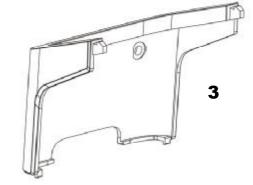
14.1 Wall-Mounting

This section shows you how to mount your MAX208M2W Series on a wall using the ZyXEL Wall-Mounting kit (not included).

14.1.1 The Wall-Mounting Kit

The wall-mounting kit contains the following parts:





- 1 Two Mortar Plugs (M4*L30 mm)
- 2 Two Screws (M4*L30 mm)
- 3 Wall-Mounting Chassis

If any parts are missing, contact your vendor.

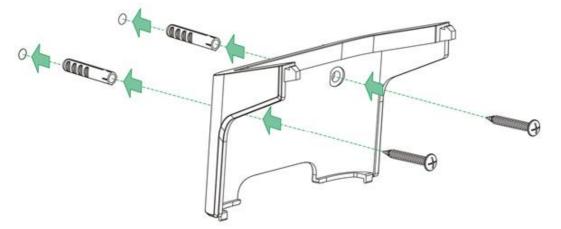
14.1.2 Instructions

To mount the MAX208M2W Series on a wall:

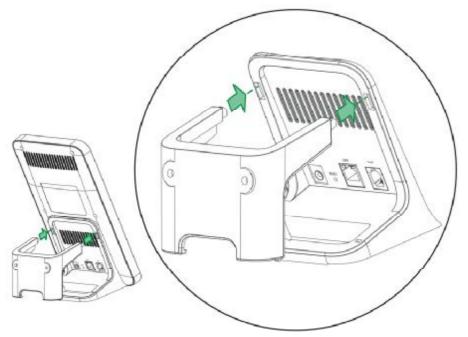
- 1 Select a position free of obstructions on a sturdy wall.
- **2** Drill two holes in the wall exactly 70 mm apart. The holes should be 6 mm wide and at least 30 mm deep.

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

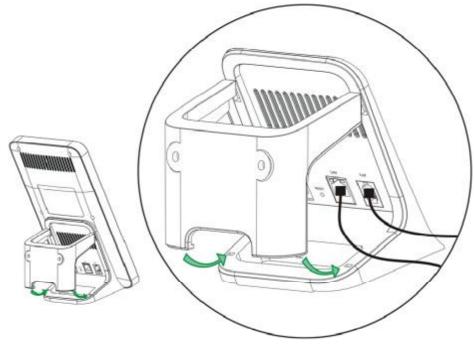
3 Attach the wall mounting chassis with the plugs and screws as shown below:



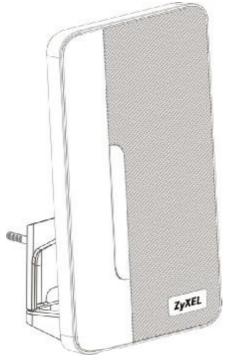
4 Connect the MAX208M2W Series to the wall mounting chassis by snapping the chassis' two upper chassis hooks into the matching holes on the MAX208M2W Series:



Do not pinch or server the cable connections between the wallmounting chassis the MAX208M2W Series. **5** Snap the lower chassis hooks into the matching holes on the MAX208M2W Series. The cable connections should come out either the left or right gaps between the wall-mounting chassis and the MAX208M2W Series



6 Once you have snapped the wall-mounting chassis in place, the MAX208M2W Series is securely fastened to the wall.



Chapter 14 Product Specifications

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 MAX208M2W Series supports EAP-TTLS authentication.

EAP-TTLS (Tunneled Transport Layer Service)

EAP-TTLS is an extension of the EAP-TLS authentication that uses certificates for only the server-side authentications to establish a secure connection (with EAP-TLS digital certifications are needed by both the server and the wireless clients for mutual authentication). Client authentication is then done by sending username and password through the secure connection, thus client identity is protected. For client authentication, EAP-TTLS supports EAP methods and legacy authentication methods such as PAP, CHAP, MS-CHAP and MS-CHAP v2.

B

Setting Up Your Computer's IP Address

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

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

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

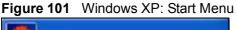
In this appendix, you can set up an IP address for:

- Windows XP/NT/2000 on page 210
- Windows Vista on page 213
- Mac OS X: 10.3 and 10.4 on page 217
- Mac OS X: 10.5 on page 221
- Linux: Ubuntu 8 (GNOME) on page 224
- Linux: openSUSE 10.3 (KDE) on page 230

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.





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





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

Figure 103 Windows XP: Control Panel > Network Connections > Properties



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

Figure 104 Windows XP: Local Area Connection Properties

ieneral	Authentica	tion Ac	lvanced			
Conne	ct using:					
11日 (11日)	Accton EN12	207D-TX	PCI Fast E	thernet.	Adapter	
This co	onnection use	es the fol	lowing iter	ns:	Config	jure
	Client for M File and Pr OoS Pool Internet Pr	inter Sha ot Schoo	aring for Mi	crosoft N	letworks	
_						
	Install		Uninstall		Proper	ties
Desc	ription					
Desc Trar wide	100	k protoc	ocol/Interr ol that pro	vides co	col. The del	fault
Desc Trar wide acro	ription Ismission Cor area netwo	k protoc terconne	ocol/Interr ol that pro cted netw	vides co orks.	col. The del mmunicatior	fault

5 The Internet Protocol TCP/IP Properties window opens.

Figure 105 Windows XP: Internet Protocol (TCP/IP) Properties

General	Alternate Configuration	
this cap		d automatically if your network supports eed to ask your network administrator for
💿 O E	otain an IP address autor	natically
OUs	e the following IP addre:	SS:
IP ac	ldress:	e e e
Subr	iet mask:	e e) (2
Defa	ult gateway:	
⊙ OŁ	otain DNS server address	s automatically
OUs	e the following DNS serv	ver addresses:
Prefe	rred DNS server:	
Alterr	nate DNS server;	
		Advanced.
		OK Can

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

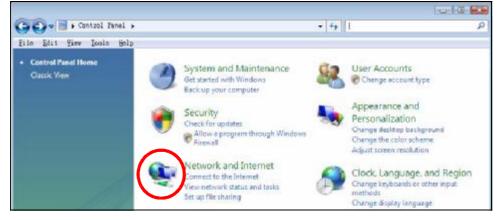
This section shows screens from Windows Vista Professional.

1 Click Start > Control Panel.



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

Figure 107 Windows Vista: Control Panel

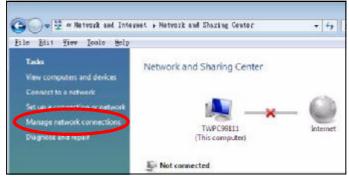


3 Click the Network and Sharing Center icon.

Figure 108 Windows Vista: Network And Internet

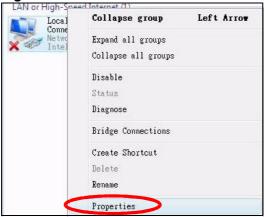


- 4 Click Manage network connections.
 - Figure 109 Windows Vista: Network and Sharing Center



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

Figure 110	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 111 Windows Vista: Local Area Connection Properties

onnect using:		
Intel(R) PRO/10	000 MT Desktop Conn	ection
		Configure
his connection uses	the following items:	-
🗹 🚚 Network Mor 🗹 🚚 File and Print		t Networks
 ✓ □ File and Print ✓ □ Internet Proto ✓ □ Internet Proto ✓ □ Internet Proto ✓ □ Link-Layer To 	nitor3 Driver er Sharing for Microsof pool Version 6 (TCP/IP poology Discovery Map opology Discovery Res	v6) v4) oper I/O Driver
 ✓ □ File and Print ✓ □ Internet Proto ✓ □ Internet Proto ✓ □ Internet Proto ✓ □ Link-Layer To 	er Sharing for Microsof peol Version & (TCP/IP peol Version 4 (TCP/IP opology Discovery Map	v6) v4) oper I/O Driver
✓ Internet Prote ✓ Internet Prote	er Sharing for Microsof cool Version S (TCP/IP cool Version 4 (TCP/IP opology Discovery Map opology Discovery Res	v6) v41 oper I/O Driver sponder

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

Figure 112 Windows Vista: Internet Protocol Version 4 (TCP/IPv4) Properties

eneral	Alternate Configuration				
his cap) get IP settings assigned a ability. Otherwise, you ne appropriate IP settings.				
0	otain an IP address autom	atically)			
© U≦	e the following IP address	1			
IP ac	ldress:	24	a i	- S	
Sybr	et mask:	4	4	÷.	
<u>D</u> efa	ult gateway:			Т	
o ot	otain DNS server address a	automatically			
	- : <u>e</u> the following DNS serve	And an			
Prefe	erred DNS server:		10		
Alter	nate DNS server:	4		<u>.</u>	
				a du	anced

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.



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

Figure 114 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 115 Mac OS X 10.4: Network Preferences Show All Network a 1 Location: Automatic : Show: Network Status Suit-in Ethernet is currently active and has the IP address 10.0.1.2. You are connected to the teternet via Built-in Ethe Built-in Ethernet leternet Sharing is on and is using AirPort to share the connection. AirPort 0 (Configure...) 1 60 sconnect... Click the lock to prevent further changes. (Assist me...) Apply Now

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

Figure 116 Mac OS X 10.4: Network Preferences > TCP/IP Tab.

		Network	Q	
t ⊫ Show All			ų	
U	ocation: Automa	itic		
	Show: Built-in	Ethernet		
TCP	IP PPPoE Ap	pleTalk Proxi	es Ethernet	
Configure IPv4:	Using DHCP	>	[0]	
IP Address:	0.0.0	1	Renew D	HCP Lease
Subnet Mask: Router:		DHCP Clie	ent ID: Of require	d)
DNS Servers:				
Search Domains:	[(Optional)
IPv6 Address:				
	Configure IPv6.			0

- **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 117 Mac OS X 10.4: Network Preferences > Ethernet

		Automatic	Location:	
		Built-in Ethernet	Show:	
	xies Ethernet	oE AppleTalk Pro	TCP/IP PP	TO
		lly	re IPv4: Manua	Configure IPv4
		0	ddress: 0.0.0.0	IP Address
			t Mask: 0.0.0.0	Subnet Mask
			Router: 0.0.0.0	Router
1			iervers:	DNS Servers
(Optiona			imains:	Search Domains
			ddress:	IPv6 Address
(ure IPv6)	Config	

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 118	Mac OS X 10.4: Network I	Jtility
------------	--------------------------	---------

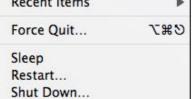
Info Netstat AppleTalk Ping Lookup	Traceroute	Whois	Finger	Port Scan
Please select a network interface for information				
Network Interface (en0)				
Internace information	Transfer :	Statistics		
Hardware Address 00:16:cb:8b:50:2e	Sent Pack	ets 20607	5	
IP Address(es) 118.169.44.203	Send Err	ors 0		
Link Speed 100 Mb	Recv Pack	ets 22626	ġ.	
Link Status Active	Recy Err	ors 0		
Vendor Marvell	Collisie	ons O		
Model Yukon Gigabit Adapter 88E8053				

Mac OS X: 10.5

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

1 Click Apple > System Preferences.

Figure 119 Mac OS X 10.5: Apple Menu Finder File Edit View About This Mac Software Update... Mac OS X Software... Dock Recent Items



2 In System Preferences, click the Network icon.

Figure 120 Mac OS X 10.5: Systems Preferences

00			System I	Preferences			
	Show All					Q	
Personal			1110				
New			H	0	Ó	Q	
Appearance	Desktop & Screen Saver	Dock	Exposé & Spaces	International	Security	Spotlight	
Hardware							
6		\bigcirc	8		0		
CDs & DVDs	Displays	Energy Saver	Keyboard & Mouse	Print & Fax	Sound		
Internet &	Network						
		Ø					
.Mac	Network	QuickTime	Sharing				
System	<u> </u>						
11		**	()	8	2	۲	
Accounts	Date & Time	Parental Controls	Software Update	Speech	Startup Disk	Time Machine	Universal Access

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

		Network	
► Show All	Ĵ		٩
	Location:	Automatic	•
Internal Modem Not Connected PPPoE Not Connected	600)	Status:	Not Connected The cable for Ethernet is connected, but your computer does not have an IP address.
Ethernet Not Connected	<>	Configure:	Using DHCP
FireWire Not Connected	¥		
AirPort	1		
		DNS Server:	
		DNS Server: Search Domains:	
		Search Domains:	WPA: ZyXEL04 Connect

- 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.

 \bullet In the ${\bf Router}$ field, enter the IP address of your MAX208M2W Series.

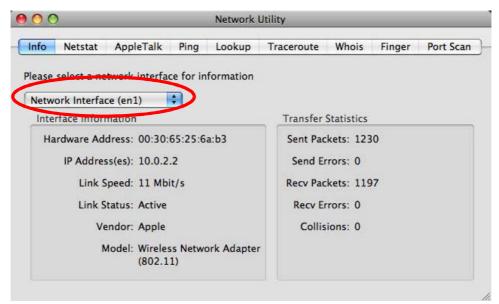
00		Network			
Show All)			٩	_
	Location:	Automatic	\$		
Internal Modem Not Connected PPPoE Not Connected	€	Status:	Not Connected The cable for Ethernet is c your computer does not h		
Ethernet Not Connected	@	Configure:	Manually	•	Ľ.
FireWire Not Connected AirPort Off	(i) 1	IP Address: Subnet Mask: Router: DNS Server: Search Domains: 802.1X:	0.0.0.0	Connect	
+ - \$-				Advanced	(

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 123 Mac OS X 10.5: Network Utility



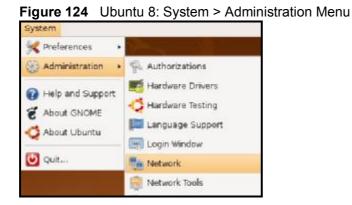
Linux: Ubuntu 8 (GNOME)

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

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

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

1 Click System > Administration > Network.



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 125 Ubuntu 8: Network Settings > Connections

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

Figure 126	Ubuntu 8: Administrator Account Aut	hentication

Authenticate	×
System policy prevents modifying the configuration	
An application is attempting to perform an that requires privileges. Authentication as users below is required to perform this acti	one of the
🔒 C.J.,,,, (chris)	:
Password for chris:	
ails	
Cancel Auth	enticate
	System policy prevents modifying the configuration An application is attempting to perform an that requires privileges. Authentication as 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 127 Ubuntu 8: Network Settings > Connections

5 The **Properties** dialog box opens.

gure 120	Ubuntu 8: Network Se eth0 Properties	
Enable I	oaming mode	
Connecti	on Settings	
Con <u>fi</u> gur	ation:	\$]
<u>I</u> P addre	ss:	
<u>S</u> ubnet	mask:	
<u>G</u> ateway	vaddress:	
	R C:	ancel

- 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.

	Network Settings	2
_ocation:		: 🖪 😭 🛷
Connections	General DNS Hosts	
DNS Serve	rs	
10.0.2.3		- 문 <u>A</u> dd
		Delete
Search Dor	nains	
		- 슈dd
		Delete

Figure 129 Ubuntu 8: Network Settings > DNS

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

Verifying Settings

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

Devices - Network Tools - • × Tool Edit Help Devices Ping Netstat Traceroute Port Scan Lookup Finger Whois Network device: **₽** Ethernet Interface (eth0) \$ <u> C</u>onfigure **IP Information** Protocol IP Address Netmask / Prefix Broadcast Scope IPv4 10.0.2.15 10.0.2,255 255.255.255.0 fe80::a00:27ff:fe30:e16c 64 Link IPv6 Interface Statistics Interface Information Transmitted bytes: 684.6 KiB Hardware address: 08:00:27:30:e1:6c Multicast: Enabled Transmitted packets: 1425 1500 MTU: Transmission errors: 0 Link speed: not available Received bytes: 219.5 KiB State: Active Received packets: 1426 Reception errors: 0 Collisions: 0

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

Figure 130 Ubuntu 8: Network Tools

properly.

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 131 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 132 openSUSE 10.3: K Menu > Computer Menu



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

🕘 YaST Control Center @ li	inux-h2oz 🍥		_	×
<u>F</u> ile <u>E</u> dit <u>H</u> elp				
Software	DSL	ISDN		
Hardware				
System	Modem	Network Card		
Network Devices				
- Network Services				
1 Novell AppArmor				
Security and Users				
💥 Miscellaneous				
Search	-^-			
				1

Figure 133 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 134	openSUSE 10.3: Network	 Settings
i iguio io i		Counigo

etwork Card	Network	Setting	5		
verview					
stalled network cards.	Global Options	Overview	Hostname/DNS	Routing	
ditionally, edit their	-	40 10	P Address		
enfiguration.	Name				
dding a Network	AND PCnet - Fas	t varavi p	HGP		
and:					
ess Add to configure a					
nually.					
onfiguring or					
eleting:					
oose a network card					
en press Configure or					
change or remove. Ien press Configure or elete as desired.					
en press Configure or					
en press Configure or					
en press Configure or	AMD PCnet - F		L		
en press Configure or	AMD PCnet - F MAC : 08:00:27				
en press Configure or	MAC: 08:00:27 • Device Na	196:ed:3d Ime: eth-eti	ho		
en press Configure or	MAC: 08:00:27 Device Na Started a	1961ed:3d Ime: eth-eth utomatical	h0 yaat boot		
en press Configure or	MAC: 08:00:27 Device Na Started a	1961ed:3d Ime: eth-eth utomatical	ho		
en press Configure or	MAC: 08:00:27 Device Na Started a	1961ed:3d Ime: eth-eth utomatical	h0 yaat boot		
en press Configure or	MAC : 08:00:27 Device Na Started a IP addres	1961ed:3d Ime: eth-eth utomatical	h0 yaat boot		

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

Address Setup 🔺	Network Car	rd Setup		
Select No Address				
Setup if you do not vant any IP address	General Address	Hardware		
or this device. This is	Device Type C	enfiguration Name		
particularly useful for	Ethernet 🔻 🛛	etho		
oonding ethernet devices.	O No IP Address (for	r Bonding Devices)		
Select Dynamic	O Dynamic Address	DHCP +		
address if you do not	Statically assigned	d IP Address		
have a static IP address assigned by	IP Address	Subnet Mask	Hostname	
the system				_
administrator or your	-Additional Addresses			
cable or DSL provider.	-Additional Addition States			
You can choose one of	Alias Name: IP7	Address Netmask		
he dynamic address				
assignment method.				
Select DHCP if you have a DHCP server				
unning on your local				
etwork. Network				
addresses are then				
obtained automatically rom the server.				
To automatically				
search for free IP and hen assign it				
		Add Edit	01910	
zeroconf. To use				

Figure 135 openSUSE 10.3: Network Card Setup

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

Select **Statically assigned IP Address** if you have a static IP address. Fill in the **IP address**, **Subnet mask**, and **Hostname** fields.

7 Click Next to save the changes and close the Network Card Setup window.

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

nter the name for	Network Settings		
DNS domain that it belongs to.	Glebal Options Overview Hostn	ame/DNS Routing	
Optionally enter the name server list and	-Hostname and Domain Name Hostname	Domain Name	
omain search list.	linux-h2oz	site	
ote that the ostname is globalit pplies to all	Change Hostname via DHCP <u>W</u> rite Hostname to /etc/hosts		
terfaces, not just nis one.	Change /etc/resolv.conf manually Name Servers and Domain Search U	st	
he domain is	Name Server 1	Domain Search	
specially important if	10.0.2.3		
erver.	Name Server 2		
If you are using DHCP to get an IP address, check whether to get a hostname via DHCP.	Name Server 3		
he hostname of your ost lwhich can be	Update DNS date via DHCP		
een by issuing the osthame command) ill be set utomatically by the HCP client. You may ant to disable this ption if you connect o different networks			

Figure 136 openSUSE 10.3: Network Settings

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

Verifying Settings

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

Figure 137 openSUSE 10.3: KNetwork Manager

🗊 Enable Wireless		
🝸 Disable Wireless	😺 KNetworkManager	
✓ Switch to Online Mode	Wired Devices	5
😡 Switch to Offline Mode	🗙 Wired Network	
T Show Connection Information	🔜 Dial-Up Connections	•
💫 Configure	🍕 Options	
	🕜 <u>H</u> elp	•
	0 Quit	Ctrl+Q
		K

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

Device	Addresse 🛛 🏹 S	tatistics
	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

Figure 138 openSUSE: Connection Status - KNetwork Manager

Appendix B Setting Up Your Computer's IP Address

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

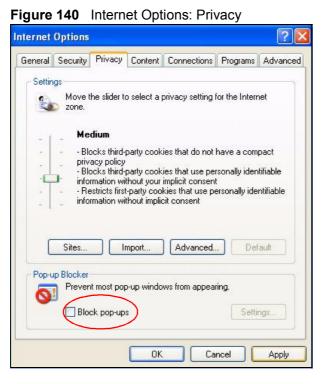
1 In Internet Explorer, select **Tools**, **Pop-up Blocker** and then select **Turn Off Pop-up Blocker**.

Figure 139 Pop-up Blocker

Tools	
Mail and News	•]
Pop-up Blocker	Turn Off Pop-up Blocker
Manage Add-ons Synchronize	Pop-up Blocker Settings
Windows Update	
Windows Messenger	
Internet Options	

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.



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.

igure	141	Intern	et Opt	ions: Priv	/acy	
nternet	Options					?
General	Security	Privacy	Content	Connections	Programs	Advanced
Settin	59	he slider ti	o select a	privacy setting	for the Interr	net
	- Bli priv - Bli - Info - Re	acy policy ocks third- rmation wi estricts first	party cook thout your -party coo	ies that do not ies that use pe implicit consen kies that use p cit consent	rsonally iden t	itifiable
Pop-L	Sites Ip Blocker		mport	Advanced.		ault
0	J	it most pop ck pop-up		ws from appea	ring. Setti	ngs
			ОК	Ca	ncel	Apply

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, <u>http://192.168.167.1</u>.

- 4 Click Add to move the IP address to the list of Allowed sites.
 - Figure 142 Pop-up Blocker Settings

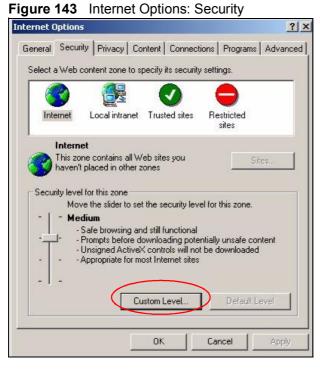
Web sites by adding the site to the list below	
Address of Web site to allow: http://192.168.1.1	Add
Allowed sites:	
	Remove
	Remove A
lotifications and Filter Level	
Play a sound when a pop-up is blocked.	
Show Information Bar when a pop-up is blocked.	
Filter Level:	

- 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.



- 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.

igure 144 Security Settings - Ja	va Scriptir
ecurity Settings	<u>? ×</u>
Settings:	
	Transfer 1
Scripting	_
Active scripting	
O Disable	
O Prompt	
Allow paste operations via script	
O Disable	
O Enable	
O Prompt	
Scripting of Java applets	
O Disable	
Enable	
O Prompt	(mark)
B User Authentication	
Reset custom settings	i
	Denot 1
Reset to: Medium	Reset
OK	Cancel

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 145 Security Settings	rity Settings - Java
Settings:	
O Disable O Enable	
Font download	
Enable O Prompt Microsoft VM	
Java permissions O Custom	
Disable Java Disable Java High safety Low safety)
Miccolloc	
Reset custom settings	
Reset to: Medium	Reset
	OK Cancel

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.

ternet Options		?
General Security Privacy Content Conr	nections Programs Ad-	vanced
<u>S</u> ettings:		
Use inline AutoComplete Use Passive FTP (for firewall and D Use smooth scrolling HTTP 1.1 settings	SL modem compatibility)	-
Use HTTP 1.1 Use HTTP 1.1 Java (Sun) Use Java 2 v1.4.1_07 for <applet></applet>		
 ➡ Microsoft VM ➡ Java console enabled (requires rest. ➡ Java logging enabled ➡ Java logging enabled ➡ JIT compiler for virtual machine enal ➡ Multimedia 		
Always show Internet Explorer (5.0 c Don't display online media content ii Enable Automatic Image Resizing	NAME AND ADDRESS OF A DECEMBER OF	J
	<u>R</u> estore Defau	ults

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.

<u>T</u> ools	<u>H</u> elp		
Web	o <u>S</u> earch	Ctrl+K	
Dow	nloads	Ctrl+J	
<u>A</u> dd	-ons		
<u>W</u> eb	Developer		۲
Erro	r <u>C</u> onsole		
Adb	lock Plus	Ctrl+Shift+A	
Pag	e <u>I</u> nfo		
튆 Eire	FTP		
Clea	ar <u>P</u> rivate Data	a Ctrl+Shift+Del	
🖾 Tab	o Mix Plus Opti	ons	
😤 Ses	sion Manager		٠
Opti	ions		

Figure 147 Mozilla Firefox: TOOLS > Options

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

Options × 100 0 宁 0 Main Tabs Content Feeds Privacy Security Advanced Block pop-up windows Exceptions... 🔽 Load images automatically Exceptions... 🔽 Enable JavaScript Advanced... 🔽 Enable Java Fonts & Colors Default font: Times New Roman ▼ Size: 16 ▼ Advanced... ⊆olors... File Types Configure how Firefox handles certain types of files Manage... OK Cancel Help

Figure 148 Mozilla Firefox Content Security

following screen.

Appendix C Pop-up Windows, JavaScript and Java Permissions

D

IP Addresses and Subnetting

This appendix introduces IP addresses and subnet masks.

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

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

Introduction to IP Addresses

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

Structure

An IP address is made up of four parts, written in dotted decimal notation (for example,). 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.

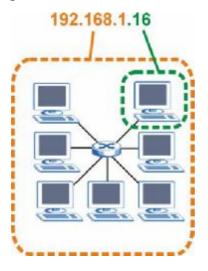


Figure 149 Network Number and Host ID

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).

	1ST OCTET:	2ND OCTET:	3RD OCTET:	4TH OCTET
	(192)	(168)	(1)	(2)
IP Address (Binary)	11000000	10101000	00000001	0000010
Subnet Mask (Binary)	11111111	11111111	11111111	00000000
Network Number	11000000	10101000	0000001	
Host ID				0000010

Table 88 IP Address Network Number and Host ID Example

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.

	BINARY				
	1ST OCTET	2ND OCTET	3RD OCTET	4TH OCTET	DECIMAL
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	255.255.255.24 8

Table 89 Subnet Masks

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:

SUBNE	TMASK	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	255.255.255.2 48	3 bits	2 ³ – 2	6

 Table 90
 Maximum Host Numbers

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.

SUBNET MASK	ALTERNATIVE NOTATION	LAST OCTET (BINARY)	LAST OCTET (DECIMAL)		
255.255.255.0	/24	0000 0000	0		
255.255.255.12 8	/25	1000 0000	128		
255.255.255.19 2	/26	1100 0000	192		
255.255.255.22 4	/27	1110 0000	224		
255.255.255.24 0	/28	1111 0000	240		
255.255.255.24 8	/29	1111 1000	248		
255.255.255.25 2	/30	1111 1100	252		

Table 91 Alternative Subnet Mask Notation

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.

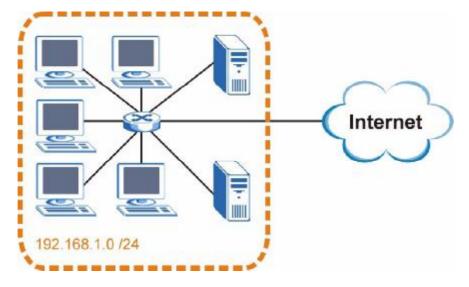
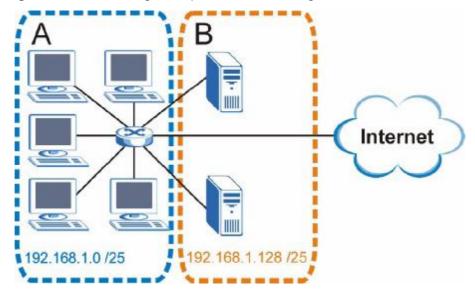


Figure 150 Subnetting Example: Before Subnetting

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, \bf{A} and \bf{B} .





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

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 92 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 00000
Subnet Mask (Binary)	11111111.11111111.11111111.	11 000000
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 93Subnet 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 94 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 95Subnet 4

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	192
IP Address (Binary)	11000000.10101000.00000001	11000000
Subnet Mask (Binary)	111111111.11111111111111111	11 000000

 Table 95
 Subnet 4 (continued)

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

Example: Eight Subnets

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

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

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

 Table 96
 Eight Subnets

Subnet Planning

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

Table 97 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.

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

 Table 98
 16-bit Network Number Subnet Planning

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 MAX208M2W Series.

Once you have decided on the network number, pick an IP address for your MAX208M2W Series 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 MAX208M2W Series 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 MAX208M2W Series 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.

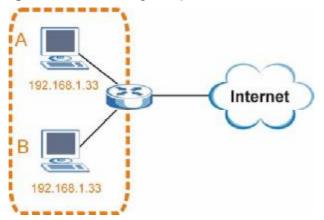


Figure 152 Conflicting Computer IP Addresses Example

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.

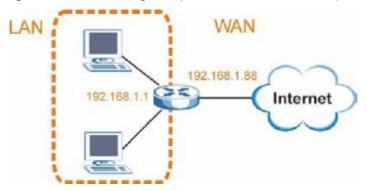


Figure 153 Conflicting Computer IP Addresses Example

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.

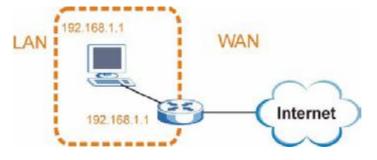


Figure 154 Conflicting Computer and Router IP Addresses Example

Ε

Importing Certificates

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

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

Many ZyXEL products, such as the NSA-2401, issue their own public key certificates. These can be used by web browsers on a LAN or WAN to verify that they are in fact connecting to the legitimate device and not one masquerading as it. However, because the certificates were not issued by one of the several organizations officially recognized by the most common web browsers, you will need to import the ZyXEL-created certificate into your web browser and flag that certificate as a trusted authority.

Note: You can see if you are browsing on a secure website if the URL in your web browser's address bar begins with https:// or there is a sealed padlock icon (

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

- Internet Explorer on page 260
- Firefox on page 270
- Opera on page 276
- 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 155 Internet Explorer 7: Certification Error

* *	Certificate Error: Navigation Blocked
8	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.
	Ø Click here to close this webpage.
	Continue to this website (not recommended).
	More information

2 Click Continue to this website (not recommended).

Figure 156 Internet Explorer 7: Certification Error

Solution to this website (not recommended).

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

Figure 157 Internet Explorer 7: Certificate Error



4 In the Certificate dialog box, click Install Certificate.

Figure 158 Internet Explorer 7: Certificate

	ormation
	ate is not trusted. To enable trust, a in the Trusted Root Certification
Issued to: rsa2	401
Issued by: nsa2	401
Valid from \$/20/	2006 to 5/20/2011

5 In the Certificate Import Wizard, click Next.

Figure 159 Internet Explorer 7: Certificate Import Wizard



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

Figure 160 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	
OPlace all certificates in the following store	
Certificate store:	
Browse	
< Back Next > Cance	:

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

Figure 161 Internet Explorer 7: Certificate Import Wizard

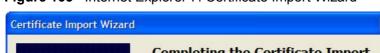
• Place all certificates in the following s	tore
Certificate store:	
	Browse

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

Figure 162 Internet Explorer 7: Select Certificate Store

Personal Trusted Root Certification Authorities Enterprise Trust	_
🗄 🧰 Enterprise Trust	
	*
🗉 🦲 Intermediate Certification Authorities	3
🗉 🦲 Active Directory User Object	
🕀 🦳 Trusted Publishers	×
< III	>

9 In the Completing the Certificate Import Wizard screen, click Finish.
 Figure 163 Internet Explorer 7: Certificate Import Wizard





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

Figure 164 Internet Explorer 7: Security Warning

Security	Warning				
1	You are about to install a certificate from a certification authority (CA) daiming 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. certificate with an unconfirmed thumbprint is a security risk. If you click "yes" you acknowledge this					
	Do you want to install this certificate?				

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

Figure 165 Internet Explorer 7: Certificate Import Wizard



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

Figure 166 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?
View certificates

Installing a Stand-Alone Certificate File in Internet Explorer

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

1 Double-click the public key certificate file.

Figure 167 Internet Explorer 7: Public Key Certificate File



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

Figure 168 Internet Explorer 7: Open File - Security Warning

Open Fil	e - 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				
Open Cancel 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 nopen this software. What's the risk?	not			

3 Refer to steps 4-12 in the Internet Explorer procedure beginning on page 260 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 169 Internet Explorer 7: Tools Menu



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

Figure 170 Internet Explorer 7: Internet Options

iternet O	ptions		?	
General S	ecurity Privaty	Content Connections	Programs Advanced	
Content /		control the Internet cor mputer.	ntent that can be	
		Enable	Settings	
Certificat		or encrypted connection	ns and identification.	
C	ear SSL state	Certificates	Publishers	
AutoCom	AutoComplete st	ores previous entries d suggests matches	Settings	
Feeds Feeds provide updated content from websites that can be read in Internet Explorer and other programs.				
		ОК С	ancel 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**.

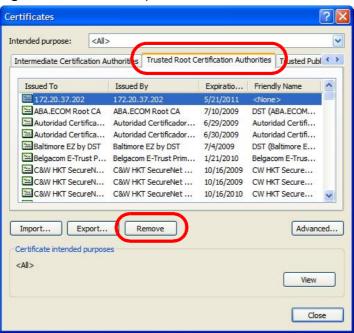


Figure 171 Internet Explorer 7: Certificates

4 In the Certificates confirmation, click Yes.

Figure 172 Internet Explorer 7: Certificates

Certific	ates 🛛 🕅
	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 173 Internet Explorer 7: Root Certificate Store

Root Ce	rtificate Store
1	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 (sha 1) : DC44635D 10FE2D0D E76A72ED 002B9AF7 677EB0E9 Thumbprint (md5) : 65F5E948 F0BC9998 50803387 C6A18384 Yes No

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 174 Firefox 2: Website Certified by an Unknown Authority

Websit	e Certified by an Unknown Authority 🛛 🔛 🔛
4	Unable to verify the identity of 172.20.37.202 as a busited site. Fossible mascens for this error: - Your browner does not recognise the Certificate Authority that issued the site's certificate. - The site's certificate is momplete due to a server misconfiguration. - The site's certificate is momplete due to a server misconfiguration. - The site's certificate is momplete due to a server misconfiguration. - The site's certificate is momplete due to a server misconfiguration. - The site's certificate is momplete due to a server misconfiguration. - The site's certificate is momplete due to a server misconfiguration. Fease notify the site's webmacter about this problem. Every except the certificate, you should examine the site's certificate certified, Are you willing to to accept this certificate for the purpose of identifying the Web site 172.20.37.202? Examine Certificate O Accept this certificate permanently Carcel Carcel Carcel

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 175 Firefox 2: Page Info

Page Info	
neral Borns Unix Media Becurity	
Web Site Identity Verified	
The web site 172.20.37.203 supports authenticat viewing. The identity of this web site has been ver authority you trust for this purpose.	
Vew the security certificate that identity.	verifies this web site's
Connection Encrypted: High-grade Encrypt	
The page you are viewing was encrypted before b Internet.	reing transmitted over the
Broyption makes it very difficult for unauthorized traveling between computers. It is therefore very this page as it traveled across the network.	

Installing a Stand-Alone Certificate File in Firefox

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

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

Figure 176 Firefox 2: Tools Menu

Tools			
Web <u>S</u> earch	Ctrl+K		
<u>D</u> ownloads <u>A</u> dd-ons	Cttl+J		
Java Console			
Error Console			
Page <u>I</u> nfo			
Clear Private Data Ctrl+Shift+Del			
Options	- k-		
	. n		

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

Figure 177 Firefox 2: Options

Options						
Main Tabs	Content	Feeds	Privacy	Security	Advanced	
General Network U			Flivacy	Security	Auvanceu	
Protocols)		🗹 Use	tls <u>1</u> .0		
Certificates	e requires a o	ertificate:				
Select one						- II
View Certificat	es Revoc	ation Lists	Verific	ation	ecurit <u>y</u> Devices	
		1	ОК	Can	icel H	lelp
				18 G		

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

Figure 178	Firefox 2:	Certificate Manager
------------	------------	---------------------

Certificate Name	Purposes	E.

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

Figure 179 Firefox 2: Select File

taining Web S	ite certificate to impor	t			? 🔀
Desktop		~	GØ	19 📖	-
My Documen	ts				
File name:	CA.cer			~	Open
	My Compute My Documen My Network I	Pesktop My Computer My Documents My Network Places CA.cer	My Computer My Documents My Network Places CA.cer	Pesktop My Computer My Documents My Network Places CA.cer File name: CA.cer	Pesktop My Computer My Documents My Network Places CA.cer File name: CA.cer

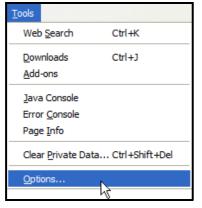
5 The next time you visit the web site, click the padlock in the address bar to open the Page Info > Security window to see the web page's security information.

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 180 Firefox 2: Tools Menu



In the Options dialog box, click ADVANCED > Encryption > View Certificates.
 Figure 181 Firefox 2: Options

Options							
十	(aa)		3	6	2	<u></u>	
Main	Tabs	Content	Feeds	Privacy	Security	Advanced	
General	Network	pdale Encr	yption				
- Proto	cols —						
v v	lse SSL <u>3</u> .0			🗹 Use	TLS 1.0		
0 s		e requires a construction of the second		me every f		ecurit <u>y</u> Devices	
				Ок	Car	icel +	Help

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

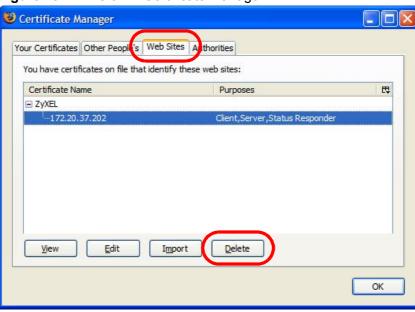


Figure 182 Firefox 2: Certificate Manager

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

Figure 183 Firefox 2: Delete Web Site Certificates



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

Opera

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

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

this certificate. A	te for this server is r ccept/install?	not registered. You i	may inst <mark>a</mark> ll
172.20.37.202			View
	ate from "172.20.3 nnot decide if this ce		
operar opera ca			

Figure 184 Opera 9: Certificate signer not found

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

Figure 185 Opera 9: Security information

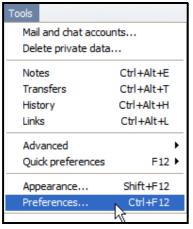


Installing a Stand-Alone Certificate File in Opera

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

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

Figure 186 Opera 9: Tools Menu

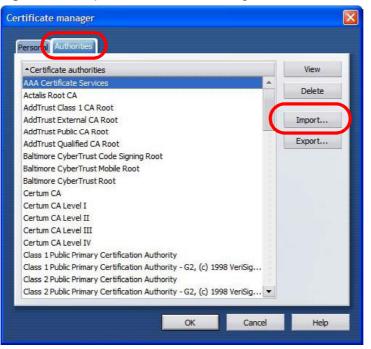


Tabs Choose a master password to protect personal certificates Browsing	
Browsing	
Notifications Set master password	
Content Fonts Ask for password Downloads	
Programs Every time needed	
History Use as master password for e-mail and Wand	
Cookies Enable Fraud Protection	
Manage certificates	
Toolbars Shortcuts Voice	
Security protocols	

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

3 In the Certificates Manager, click Authorities > Import.

Figure 188 Opera 9: Certificate manager



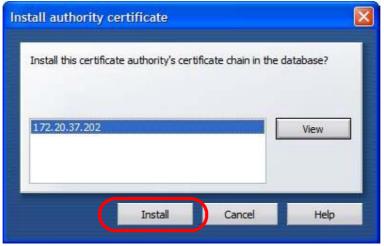
4 Use the **Import certificate** dialog box to locate the certificate and then click **Open.**

Import certifica	ate						? 🛛
Look in:	Besktop		~	GØ	E.	•	
Desktop My Computer My Network Places	My Computer My Documents My Network Pla	ices					
	File name:	CA.cer			~		Open
	Files of type:	X509 (*.ca)			~		Cancel

Figure 189 Opera 9: Import certificate

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

Figure 190 Opera 9: Install authority certificate



6 Next, click OK.

Figure 191 Opera 9: Install authority certificate



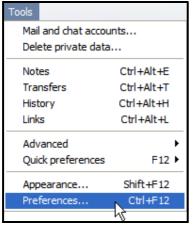
7 The next time you visit the web site, click the padlock in the address bar to open the **Security information** window to view the web page's security details.

Removing a Certificate in Opera

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

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

Figure 192 Opera 9: Tools Menu



2 In Preferences, ADVANCED > Security > Manage certificates.

Figure 193 Opera 9: Preferences

Tabs Browsing	Choose a master password to protect personal certificates
Notifications	Set master password
Content Fonts Downloads	Ask for password
Programs	Every time needed
History Cookies Security	Use as master password for e-mail and Wand Enable Fraud Protection
Network	Manage certificates
Toolbars Shortcuts Voice	

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

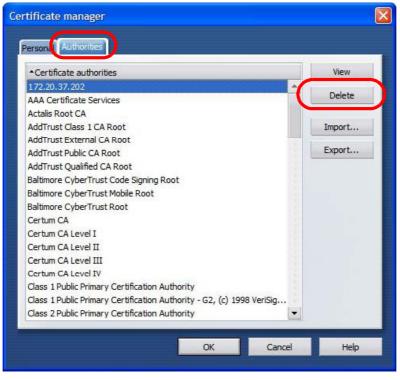


Figure 194 Opera 9: Certificate manager

- **4** The next time you go to the web site that issued the public key certificate you just removed, a certification error appears.
 - Note: There is no confirmation when you delete a certificate authority, so be absolutely certain that you want to go through with it before clicking the button.

Konqueror

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

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

Figure 195 Konqueror 3.5: Server Authentication



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

Figure 196 Konqueror 3.5: Server Authentication



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

Figure 197 Konqueror 3.5: KDE SSL Information

a have more	mation - Konqueror	e L	7 a
Chains			
reer tertToate:		15 50 81	
Organization Organization a Country: Common marter	2)Xel unt: XMZ200 US 172 20.07.202	Orgenization Orgenizationel unit Country Common name	UE
URL: Certificate state: Valid from Valid untili Serial number: MDS digest: Cipher in use: Details: SSL version:	172.23.37.202 https://172.23.37.202/o Centificate is self-signed Wednesday 21 May 2000 Saturday 21 May 2001 Saturday 2001 Saturd	and thus may not be tru 8 06:42:35 am GMT 6 42:35 am GMT 8 8:8E:4C:88:88:A2:D3:F0:2 SLV3 Ki=DH ALI=RSA Enc	ι. Έ

Installing a Stand-Alone Certificate File in Konqueror

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

1 Double-click the public key certificate file.

Figure 198 Konqueror 3.5: Public Key Certificate File



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

Figure 199 Konqueror 3.5: Certificate Import Result



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

Search: Subject	Issuer	Serial	i
CN=10R-CA 1:PN,0=Bundesnetzagentur,C CN=11R-CA 1:PN,0=Bundesnetzagentur,C	CN=10R-CA 1:PN,0=B	2A	
N=172.20.37.202,0U=XYZ200,0=ZyXEL, N=6R-Ca 1:PN,NAMEDISTINGUISHER=1,0	CN=172.20.37.202,0	009A	
N=7R-CA 1:PN,NAMEDISTINGUISHER=1,0 N=8R-CA 1:PN,0=Regulierungsbehörde f			
N=9R-CA 1:PN,0=Regulierungsbehörde f N=CA Cert Signing Authority,EMAIL=supp			
N=D-TRUST Qualified Root CA 1 2006:PN, N=D-TRUST Qualified Root CA 2 2006:PN,	CN=D-TRUST Qualifie	00B95F	
CN=S-TRUST Qualified Root CA 2006-001:P			

Figure 200 Konqueror 3.5: Kleopatra

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

Removing a Certificate in Konqueror

This section shows you how to remove a public key certificate in Konqueror 3.5.

1 Open Konqueror and click Settings > Configure Konqueror.

Figure 201 Konqueror 3.5: Settings Menu

<u>S</u> ettings	
🎟 Hide <u>M</u> enubar	Ctrl+M
<u>T</u> oolbars	•
🔀 F <u>u</u> ll Screen Mode	Ctrl+Shift+F
Save View Changes per Eolder	
<u>Remove Folder Properties</u>	
Load <u>∨</u> iew Profile	•
Save View Profile "Web Browsing".	
Configure View Profiles	
Configure <u>E</u> xtensions	
🍄 Co <u>n</u> figure Spell Checking	
🌦 Configure S <u>h</u> ortcuts	
🐁 Configure Tool <u>b</u> ars	
🔌 <u>C</u> onfigure Konqueror	

- 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 202 Konqueror 3.5: Configure

Cookies	SSL OpenSSL Your Certificates Authentication	Peer SSL Certificates S&L Signe
	Organization Common Name	Export
Cache	ZyKEL 172.20.37.202	Berrow
364		Venty
Proxy		
CRS	1	
Stylesheets	-	9
<u>A</u>	Organization: ZyXEL Organizational unit: XYZ200	Organization Zyl
	Country III	Organizational unit: XYZ
Crypto	Valid from: Wednesday 23 May 2008 06:42:35 am 6	TM
-	Valid until Saturday 21 May 2011 06:42:35 am GM	
rowser Identification	Cache	Policy
(Vice	Permanently	@ Accept
	O yndi	O Reject
Plugins	in or in the owned	C Prompt
2	UPERALDPLANESS. HLP	T C Doubt
2	MD5 digest: 3F:9A:76:6E:A9:F5:07:41:8E:4C:8B:8B:A3	ND/SED-2E

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.

Appendix E Importing Certificates

F

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.

NAME	PROTOCOL	PORT(S)	DESCRIPTION
AH (IPSEC_TUNNEL)	User-Defined	51	The IPSEC AH (Authentication Header) tunneling protocol uses this service.
AIM/New-ICQ	ТСР	5190	AOL's Internet Messenger service. It is also used as a listening port by ICQ.
AUTH	ТСР	113	Authentication protocol used by some servers.
BGP	ТСР	179	Border Gateway Protocol.
BOOTP_CLIENT	UDP	68	DHCP Client.
BOOTP_SERVER	UDP	67	DHCP Server.
CU-SEEME	ТСР	7648	A popular videoconferencing solution
	UDP	24032	from White Pines Software.
DNS	TCP/UDP	53	Domain Name Server, a service that matches web names (for example <u>www.zvxel.com</u>) to IP numbers.

 Table 99
 Commonly Used Services

Table 99 Commonly Used Services (continue)
--

NAME	PROTOCOL	PORT(S)	DESCRIPTION
ESP (IPSEC_TUNNEL)	User-Defined	50	The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service.
FINGER	ТСР	79	Finger is a UNIX or Internet related command that can be used to find out if a user is logged on.
FTP	тср	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	ТСР	1720	NetMeeting uses this protocol.
HTTP	ТСР	80	Hyper Text Transfer Protocol - a client/server protocol for the world wide web.
HTTPS	ТСР	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	ТСР	1863	Microsoft Networks' messenger service uses this protocol.
NEW-ICQ	ТСР	5190	An Internet chat program.
NEWS	ТСР	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	ТСР	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	ТСР	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).

NAME	PROTOCOL	PORT(S)	DESCRIPTION
РРТР	ТСР	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	ТСР	512	Remote Command Service.
REAL_AUDIO	ТСР	7070	A streaming audio service that enables real time sound over the web.
REXEC	ТСР	514	Remote Execution Daemon.
RLOGIN	ТСР	513	Remote Login.
RTELNET	ТСР	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	ТСР	115	Simple File Transfer Protocol.
SMTP	ТСР	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	ТСР	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	ТСР	23	Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems.

Table 99 Commonly Used Services (continued)

Table 99 Commonly Osed Services (continued)			
NAME	PROTOCOL	PROTOCOL PORT	(S) DESCRIPTION
TFTP	UDP	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	ТСР	ТСР 7000	Another videoconferencing solution.

 Table 99
 Commonly Used Services (continued)

G

Legal Information

Copyright

Copyright © 2011 by ZyXEL Communications Corporation.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of ZyXEL Communications Corporation.

Published by ZyXEL Communications Corporation. All rights reserved.

Disclaimers

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

Your use of the MAX208M2W Series is subject to the terms and conditions of any related service providers.

Do not use the MAX208M2W Series for illegal purposes. Illegal downloading or sharing of files can result in severe civil and criminal penalties. You are subject to the restrictions of copyright laws and any other applicable laws, and will bear the consequences of any infringements thereof. ZyXEL bears NO responsibility or liability for your use of the download service feature.

Trademarks

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

Certifications

Federal Communications Commission (FCC) Interference Statement

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

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

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

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

IMPORTANT NOTE:

Radiation Exposure Statement:

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

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



依據 低功率電波輻射性電機管理辦法

第十二條 經型式認證合格之低功率射頻電機,非經許可,公司、商號或使用 者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。 第十四條 低功率射頻電機之使用不得影響飛航安全及干擾合法通信;經發現 有干擾現象時,應立即停用,並改善至無干擾時方得繼續使用。 前項合法通信,指依電信規定作業之無線電信。低功率射頻電機須忍 受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

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

Notices

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

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

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

Viewing Certifications

- 1 Go to <u>http://www.zyxel.com</u>.
- 2 Select your product on the ZyXEL home page to go to that product's page.
- **3** Select the certification you wish to view from this page.

ZyXEL Limited Warranty

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

Note

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

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

Registration

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

Index

Α

AAA 70 AbS 134 accounting server see AAA ACK message 155 activity 70 Advanced Encryption Standard see AES AES 207 ALG 92 alternative subnet mask notation 250 analysis-by-synthesis 134 Application Layer Gateway see ALG authentication 70, 205 inner 208 key server 70 types 208 authorization 205 request and reply 207 server 70 auto-discovery UPnP 118

CBC-MAC 207 CCMP 205, 207 cell 69 certificates 205 CA 71 formats 72 verification 207 certification notices 297 viewing 297 Certification Authority, see CA chaining 207 chaining message authentication see CCMP circuit-switched telephone networks 133 Class of Service (CoS) 134 client-server protocol 155 SIP 155 CMAC see MAC codec 133 comfort noise 157 copyright 295 CoS 134 counter mode see CCMP coverage area 69 cryptography 205

В

base station see BS BS 69–70 links 70 BYE request 155

С

CA 71, 72

D

data 205–207 decryption 205 encryption 205 flow 207 DHCP 89 server 89 diameter 70 Differentiated Services see DiffServ DiffServ 134 DiffServ Code Point (DSCP) 134 marking rule 138 digital ID 72, 205 DS field 137 DSCP see DiffServ DTMF 143 dual-tone multi-frequency see DTMF Dynamic Host Configuration Protocol see DHCP

Е

EAP 70 EAP (Extensible Authentication Protocol) 72 EAP-TLS 72 EAP-TTLS 72 echo cancellation 157 encryption 205–207 traffic 207 Ethernet encapsulation 91 Extensible Authorization Protocol see EAP

F

FCC interference statement 296 firewall 127 FTP 161 restrictions 161

G

G.168 **157** G.711 **134** G.729 **134**

300

Η

hybrid waveform codec 134

IANA 256 identity 70, 205 idle timeout 162 IEEE 802.16 69, 205 IEEE 802.16e 69 IGD 1.0 93 inner authentication 208 Internet access 70 gateway device 93 Internet Assigned Numbers Authority see IANA 256 Internet Telephony Service Provider see ITSP interoperability 69 IP-PBX 133 **ITSP 133** ITU-T 157

Κ

key 205 request and reply 207

Μ

MAC 207 MAN 69 Management Information Base (MIB) 164 Message Authentication Code see MAC message integrity 207 Metropolitan Area Network see MAN microwave 69, 70 mobile station see MS MS 70 multimedia 135

Ν

NAT 255 and remote management 162 server sets 91 traversal 93 NAT routers 141 network activity 70 services 70 network address translators 141

0

OK response 155 outbound proxy 142 SIP 142 outbound proxy server 142

Ρ

pattern-spotting 207 PBX services 133 PCM 134 peer-to-peer calls 142 per-hop behavior 137 PHB (per-hop behavior) 138 phone services 143 PKMv2 70, 205, 208 plain text encryption 207 Privacy Key Management see PKM private key 205 product registration 298 proxy server SIP 140 public certificate 207 public key 205 pulse code modulation 134 push button 104

Q

QoS 134 quality of service

R

RADIUS 70, 72, 206 Message Types 206 Messages 206 Shared Secret Key 206 Real-time Transport Protocol see RTP register server SIP 140 registration product 298 related documentation 3 remote management and NAT 162 remote management limitations 161 required bandwidth 134 RFC 1889 135 RFC 3489 141 RTP 135

S

safety warnings 7 secure communication 205 secure connection 70 security 205 security association 207 see SA see QoS server, outbound proxy 142

Index

services 70 Session Initiation Protocol see SIP silence suppression 157 silent packets 157 SIP 134 account 140 ACK message 155 ALG 92, 142 Application Layer Gateway, see ALG BYE request 155 call progression 154 client 155 client server 155 identities 140 INVITE request 155 number 140 OK response 155 proxy server 140 register server 140 servers 155 service domain 140 URI 140 user agent 140 SIP outbound proxy 142 **SNMP 162** manager 164 sound quality 134 SS 69, 70 STUN 141, 142 subnet 247 mask 248 subnetting 250 subscriber station see SS supplementary phone services 143 syntax conventions 5 system timeout 162

Т

tampering TCP/IP configuration 89 TEK 207 TFTP restrictions 161 TLS 205

ToS 134 Touch Tone® 143 transport encryption key see TEK transport layer security see TLS trigger port forwarding process 113 TTLS 205, 208 tunneled TLS see TTLS Type of Service 134

U

unauthorized device 205 uniform resource identifier 140 Universal Plug and Play see UPnP UPnP 92 application 93 auto-discovery 118 security issues 93 Windows XP 116 use NAT 141 user agent, SIP 140 user authentication 205

V

```
VAD 157
verification 207
voice
activity detection 157
coding 133
mail 133
Voice over IP
see VoIP
VoIP 133
```

W

waveform codec 134 WiFi Protected Setup, see WPS WiMAX 69-70 security 207 WiMAX Forum 69 Wireless Interoperability for Microwave Access see WiMAX wireless LAN WPS 104 adding stations 104 push button 104 Wireless Metropolitan Area Network see MAN wireless network access 69 standard 69 wireless security 205 wizard setup 31 WPS 104 adding stations 104 push button 104

Index