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 72
 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 WiMAX Device.

Once you have decided on the network number, pick an IP address for your WiMAX Device 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 WiMAX Device 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 WiMAX Device 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 122 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 123 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 124 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 <a href="https://">https://</a> or there is a sealed padlock icon (

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

- Internet Explorer on page 206
- Firefox on page 216
- Opera on page 222
- Konqueror on page 230

# **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 125	Internet Explorer 7: Certification E	Error
------------	--------------------------------------	-------

* *	Certificate Error: Navigation Blocked
3	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 126 Internet Explorer 7: Certification Error

Solution to this website (not recommended).

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

Figure 127 Internet Explorer 7: Certificate Error



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

Figure 128 Internet Explorer 7: Certificate

Certificate	Information
This CA Root cert install this certific Authorities store.	ficate is not trusted. To enable trust, ate in the Trusted Root Certification
Issued to: n	sa2401
Issued by: n	sa2401
Valid from 5	20/2008 to 5/20/2011

5 In the Certificate Import Wizard, click Next.

Figure 129 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 130 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	
O Place all certificates in the following store	
Certificate store;	
Browse	
Rade Next > Case	

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

Figure 131 Internet Explorer 7: Certificate Import Wizard

Place all certificates in the following store	
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 132 Internet Explorer 7: Select Certificate Store

Select the certificate store you want to use.    Personal  Persona	
Personal     Trusted Root Certification Authorities     Enterprise Trust     Intermediate Certification Authorities     Active Directory User Object	^
Trusted Root Certification Authorities     Interprise Trust     Interprise Trust     Intermediate Certification Authorities	
Enterprise Trust     Intermediate Certification Authorities     Active Directory Lloss Object	
Intermediate Certification Authorities	
D Active Directory Lleer Object	
Acuve Directory User Object	
🕀 🦳 Trusted Publishers	$\mathbf{M}$
< · · · · · · · · · · · · · · · · · · ·	

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

Figure 133 Internet Explorer 7: Certificate Import Wizard



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

Figure 134 Internet Explorer 7: Security Warning

Security	Warning
<u>.</u>	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): 35D 1C9AC DBC0E654 FE327C71 464D 154B 242E5B93 Warning: If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you dick "Yes" you acknowledge this risk.
	Do you want to install this certificate? Yes No

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

Figure 135 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 136 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 137 Internet Explorer 7: Public Key Certificate File



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

Figure 138 Internet Explorer 7: Open File - Security Warning

Open Fil	e - Security Warning	×
Do you	want to open this file?	
( and a	Name: CA.cer	
	Publisher: Unknown Publisher	
	Type: Security Certificate	
	From: D:\Documents and Settings\13435\Desktop	
	Open Cancel	
🗹 Alway	rs ask before opening this file	
1	While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do r open this software. What's the risk?	not

**3** Refer to steps 4-12 in the Internet Explorer procedure beginning on page 206 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 139 Internet Explorer 7: Tools Menu



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

Figure 140 Internet Explorer 7: Internet Options

nternet Options		? 🛛
General Security Privacy	Content Connections	Programs Advanced
Content Advisor Ratings help you viewed on this c	u control the Internet cor computer.	ntent that can be
	Enable	Settings
Certificates Use certificates	for encrypted connection	ns and identification.
Clear SSL state	Certificates	Publishers
AutoComplete AutoComplete s on webpages ar for you	tores previous entries nd suggests matches	Settings
Feeds Feeds Provide u websites that ca Explorer and oth	pdated content from an be read in Internet her programs.	Settings
	ок	Cancel Apply

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



Figure 141 Internet Explorer 7: Certificates

4 In the Certificates confirmation, click Yes.

Figure 142 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 143 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 F0BC9989 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 144 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.  Foosbille masces 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 miccorfiguration.  - The site's certificate is momplete due to a server miccorfiguration.  - The site's certificate is momplete due to a server miccorfiguration.  - The site's certificate is momplete due to a server miccorfiguration.  - The site's certificate is this webmacter about this problem.  Rease notify the site's webmacter about this problem.  Every excepting this certificate, you should examine the site's certificate carefully. Are you willing to a scope this certificate for the purpose of identifying the Web site 172.20.37.202?  Example Certificate  - Accept this certificate permanently - security this certificate and do not connect to this Web site  - Cancel

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

Figure 145 Firefox 2: Page Info

Г

rage into	
eneral Borms Unks Media Security	
Web Site Identity Verified	
The web site 172.20.37.202 supports authentic viewing. The dentity of this web site has been authority you trust for this purpose.	cation for the page you are verified by ZyXEL, a certificate
Vew the security certificate the identity.	at verifies the web site's
Connection Encrypted: High-grade Encry The page you are viewing was encrypted befor	ption (AES-256 256 bit) e being transmitted over the
Internet.	
Encryption makes it very difficult for unauthoriz traveling between computers. It is therefore ve this page as it traveled across the network.	ed people to view information ery unlikely that anyone read

## 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 146 Firefox 2: Tools Menu

Tools	
Web <u>S</u> earch	Ctrl+K
<u>D</u> ownloads <u>A</u> dd-ons	C#l+J
Java Console	
Error Console	
Page <u>I</u> nfo	
Clear <u>P</u> rivate Da	ta Ctrl+Shift+Del
Options	2
	r 10

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

Figure 147 Firefox 2: Options

Options							
Main	Tabs	Content	Feeds	Privacy	Security	Advanced	
General	letwork U	odate Encry	yption	Thirdey	Security	Autoriced	
Protoc	cols Ise SSL <u>3</u> .0	8		🔽 Use	tls <u>1</u> .0		
Certifi	icates a web site	requires a c	ertificate:				
O S	elect one a	utomatically	Ask	me every t	ime		
View	Certificate	<u>R</u> evoo	ation Lists	Verific	ation	ecurit <u>y</u> Devices	
			1	01			-
				UK			ab

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

Figure 148	Firefox 2: Certificate Manager
------------	--------------------------------

uposes	

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

Figure 149 Firefox 2: Select File

Select File con	taining Web Sit	e certificate to import			? 🔀
Look in:	🞯 Desktop		~	0 0 🖻 🖽	]+
Desktop Desktop My Computer My Network Places	My Computer My Documents My Network Pla CA.cer	aces			
	File name:	CA.cer		~	Open
	Files of type:	Certificate Files		*	Cancel

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 150 Firefox 2: Tools Menu



In the Options dialog box, click ADVANCED > Encryption > View Certificates.
 Figure 151 Firefox 2: Options

4			5	6		<b>{</b>	
Main T	Tabs	Content	Feeds	Privacy	Security	Advanced	
Ceperal Netw	ork Lir	data Encr	votion	1			
	IN OF	Juane   Lines	/p doit				
Protocols	-						-
Use S	SSL <u>3</u> .0			🗹 Use	TLS <u>1</u> .0		
Certificate	es		_				
When a w	eb site	requires a c	ertificate:				
O Selec	t one a	utomatically	Ask	me every t	ime		
View Cer	rtificate	<u>Revo</u>	cation Lists	<u>V</u> erific	ation S	ecurity Devices	
View Cer	rtificate	Revo	cation Lists	<u>V</u> erific	ation	ecurity Devices	
View Cer	rtificate	<u>R</u> evo	cation Lists	: <u>V</u> erific	ation S	ecurity Devices	
View Cer	rtificate	<u>R</u> evo	cation Lists	<u>V</u> erific	ation S	ecurit <u>y</u> Devices	
View Cer	rtificate	Revo	cation Lists	: <u>V</u> erific	ation	ecurit <u>y</u> Devices	
View Cer	rtificate	Revo	cation Lists	<u>v</u> erific	ation S	ecurit <u>y</u> Devices	
View Cer	rtificate	Revo	cation Lists	<u>V</u> erific	ation S	ecurit <u>y</u> Devices	
View Cer	rtificate	Revo	cation Lists	) <u>V</u> erific	ation S	ecurit <u>y</u> Devices	

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 152 Firefox 2: Certificate Manager

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

Figure 153 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.

The root certifica this certificate. A	te for this server is r ccept/install?	not registered. You	may install
172.20.37.202			View
- The root certific Opera. Opera ca	cate from "172, 20, 3 innot decide if this ce	7.202" is not known ertificate can be tru	to 🔺 sted.

Figure 154 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 155 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 156 Opera 9: Tools Menu



NG	
eneral Wand S	earch Web pages Advanced
Tabs	Choose a master password to protect personal certificates
Browsing Notifications	Set master password
Content Fonts Downloads	Ask for password
Programs	Every time needed
History	Use as master password for e-mail and Wand
Security	
vetwork	Manage certificates
Toolbars Shortcuts Voice	Constituent
	Security protocols

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

3 In the Certificates Manager, click Authorities > Import.

Figure 158 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		~	O Ø	10	•
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 159 Opera 9: Import certificate

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

Figure 160 Opera 9: Install authority certificate



6 Next, click OK.

Figure 161 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 162 Opera 9: Tools Menu



2 In Preferences, ADVANCED > Security > Manage certificates.

Figure 163 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 <del>Cookies</del>	Use as master password for e-mail and Wand Enable Fraud Protection
Network	Manage certificates
Toolbars Shortcuts	

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



Figure 164 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 165 Konqueror 3.5: Server Authentication



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

Figure 166 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 167 Konqueror 3.5: KDE SSL Information

C KOLE SSLE Inter	mation - Kongueror vection is secured with St	શ	ан у 1
Chains			Y
reer tertficate:		15 50 81	
Organization Organizationia Country: Common marte	298=1 unt: X*2200 US 172 20.07.202	Organization Organizational unit Country Common name	∆y%=L X*2200 US 172.20 07.202
i Pladressi IP addressi Cerificate state: Valid from Valid until Serial numbers MDS digest: Cipher in use: Datails SSL version Cipher strength:	172.23.37.202 https://172.23.37.202/k Certificate is self-signed Wednesday 21 May 200 Saturday 21 May 2011 0 111.3932119356989422 3F:9A-76:6E:A9:F5:07:41 DHE-RSA-AE5256-SHA St TJSU/55LV3 256 bits used of a 256 H	nginwap.html and thus insy not be th 6 06:42:35 am GMT 16 42:35 am GMT 18 42:35 am GMT 18 42:45 am GMT 18 42:45 am GMT 18 51 42:45 am GMT 19 51 51 51 51 51 51 51 51 51 51 51 51 51	istworthy. 19 =AES(258) Mac=SHA1

## 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 168 Konqueror 3.5: Public Key Certificate File



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

Figure 169 Konqueror 3.5: Certificate Import Result



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

🔲 Kleopatra 🍥				×
<u>Eile V</u> iew <u>C</u> ertificates C <u>R</u> Ls <u>T</u> ools <u>S</u> e	ttings <u>H</u> elp			
Search:		In Local Certificate	es 🔻	0
Subject	Issuer	Serial		
CN=10R-CA 1:PN,0=Bundesnetzagentur,C CN=11R-CA 1:PN,0=Bundesnetzagentur,C CN=172.20.37.202,0U=XYZ200,0=ZYZEL, CN=6R-Ca 1:PN,NAMEDISTINGUISHER=1,0 CN=7R-CA 1:PN,0=Regulierungsbehörde f CN=9R-CA 1:PN,0=Regulierungsbehörde f CN=CA Cert Signing Authority,EMAIL=supp CN=D-TRUST Qualified Root CA 1 2006:PN, CN=S-TRUST Qualified Root CA 2006-001:P	CN=10R-CA 1:PN,0=B CN=11R-CA 1:PN,0=B CN=6R-Ca 1:PN,NAME CN=7R-CA 1:PN,NAME CN=8R-CA 1:PN,0=Re CN=9R-CA 1:PN,0=Re CN=0-CA Cert Signing A CN=D-TRUST Qualifie CN=D-TRUST Qualifie CN=S-TRUST Qualifie	. 2A 2D 009A 32D1 00C4 01 02 00 00B95F 00B95F 00B9 00DF		
11 Keys.				

Figure 170 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 171 Konqueror 3.5: Settings Menu

<u>S</u> ettings		
T Hide Menubar Toolbars	Ctrl+M	•
🔀 F <u>u</u> ll Screen Mode	Ctrl+Shift+F	
Save View Changes per <u>F</u> older <u>R</u> emove Folder Properties		
Load <u>V</u> iew Profile <u>S</u> ave View Profile "Web Browsing" C <u>o</u> nfigure View Profiles		•
Configure <u>Extensions</u> Configure Spell Checking Configure Shortcuts Configure Toolbars		
👒 <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 172 Konqueror 3.5: Configure

Cookies	SSL OpenSSL Your Certificates Authentica	tion Peer SSL Certificates SLL Signer
	Organization Common Name	Export
Cache	ZyREL 172.20.37.202	Bemove
362		Wently
Proxy		
CRS	15	
Stylesheets	Organization: ZiREL	Organization ZVX
<u>A</u>	Organizational unit: XYZ200	Prosnizational unit, XYZ
Crypto	Valid from: Waitmanday 22 May 2008 05 42 35 at	m GMT
-	Valid until Saturday 21 May 2011 06:42:35 am 1	SMT
rowser Identification	Cache	Policy
200	Permanently	Accept
352	O Until O Reject	
Plugins	BLOLING LEOP AN	C Brompt
<b>Ø</b>	MDS digest: 3F:9A:76:6E:A9:F5:07:41:8E:4C:88:88	RA2:D3:F0:2F

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

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

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.zyxel.com</u> ) to IP numbers.

 Table 73
 Commonly Used Services

Table 73	Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
ESP (IPSEC_TUNNEL)	User-Defined	50	The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service.
FINGER	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	File Transfer Program, a program to
	ТСР	21	large files that may not be possible by e-mail.
H.323	ТСР	1720	NetMeeting uses this protocol.
НТТР	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 73
 Commonly Used Services (continued)

	NAME	PROTOCOL	PORT(S)	DESCRIPTION
	TFTP	UDP	69	Trivial File Transfer Protocol is an Internet file transfer protocol similar to FTP, but uses the UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol).
	VDOLIVE	ТСР	7000	Another videoconferencing solution.

 Table 73
 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 WiMAX Device is subject to the terms and conditions of any related service providers.

Do not use the WiMAX Device 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 Communication Commission Interference Statement**

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

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

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

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

#### **IMPORTANT NOTE:**

#### **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.



## 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>.

# A

AAA 58 accounting server see AAA activity 58 Advanced Encryption Standard see AES AES 153 ALG 80 alternative subnet mask notation 196 Application Layer Gateway see ALG authentication 58, 151 inner 154 key server 58 types 154 authorization 151 request and reply 153 server 58 auto-discovery UPnP 100

## В

base station see BS BS 57–58 links 58

# С

CA 59, 60 CBC-MAC 153 CCMP 151, 153 cell 57 certificates 151

CA 59 formats 60 verification 153 certification notices 243 viewing 243 Certification Authority, see CA chaining 153 chaining message authentication see CCMP CMAC see MAC copyright 241 counter mode see CCMP coverage area 57 cryptography 151

# D

data 151–153 decryption 151 encryption 151 flow 153 DHCP 77 server 77 diameter 58 digital ID 60, 151 Dynamic Host Configuration Protocol see DHCP

# Ε

EAP 58 EAP (Extensible Authentication Protocol) 60 EAP-TLS 60 EAP-TTLS 60 encryption 151–153 traffic **153** Ethernet encapsulation **79** Extensible Authorization Protocol see EAP

## F

FCC interference statement 242 firewall 107 FTP 113 restrictions 113

## I

IANA 202 identity 58, 151 idle timeout 114 IEEE 802.16 57, 151 IEEE 802.16e 57 IGD 1.0 81 inner authentication 154 Internet access 58 gateway device 81 Internet Assigned Numbers Authority see IANA 202 interoperability 57

# Κ

key 151 request and reply 153

## Μ

MAC 153 MAN 57 Management Information Base (MIB) 116 Message Authentication Code see MAC message integrity 153 Metropolitan Area Network see MAN microwave 57, 58 mobile station see MS MS 58

## Ν

NAT 201 and remote management 114 server sets 79 traversal 81 network activity 58 services 58

## Ρ

pattern-spotting 153 PKMv2 58, 151, 154 plain text encryption 153 Privacy Key Management see PKM private key 151 product registration 244 public certificate 153 public key 151

## R

RADIUS 58, 60, 152 Message Types 152 Messages 152 Shared Secret Key 152 registration product 244 related documentation 3 remote management and NAT 114 remote management limitations 113

## S

safety warnings 7 secure communication 151 secure connection 58 security 151 security association 153 see SA services 58 SIP ALG 80 Application Layer Gateway, see ALG **SNMP 114** manager 116 SS 57, 58 subnet 193 mask 194 subnetting 196 subscriber station see SS syntax conventions 5 system timeout 114

# Т

tampering TCP/IP configuration 77 TEK 153 TFTP restrictions 113 TLS 151 transport encryption key see TEK transport layer security see TLS trigger port forwarding process 95 TTLS 151, 154 tunneled TLS see TTLS

# U

unauthorized device 151 Universal Plug and Play see UPnP UPnP 80 application 81 auto-discovery 100 security issues 81 Windows XP 98 user authentication 151

## V

verification 153

## W

WiMAX 57–58

security 153
WiMAX Forum 57

Wireless Interoperability for Microwave Access see WiMAX
Wireless Metropolitan Area Network

see MAN
wireless network
access 57
standard 57

wireless security 151
wizard setup 27