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 ZyXEL Device 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.

# **APPENDIX C** Setting up Your Computer's IP Address

All computers must have a 10M or 100M Ethernet adapter card and TCP/IP installed.

Windows 95/98/Me/NT/2000/XP, Macintosh OS 7 and later operating systems and all versions of UNIX/LINUX include the software components you need to install and use TCP/IP on your computer. Windows 3.1 requires the purchase of a third-party TCP/IP application package.

TCP/IP should already be installed on computers using Windows NT/2000/XP, Macintosh OS 7 and later operating systems.

After the appropriate TCP/IP components are installed, configure the TCP/IP settings in order to "communicate" with your network.

# Windows 95/98/Me

Click Start, Settings, Control Panel and double-click the Network icon to open the Network window.

Network 🔗 🗙
Configuration Identification Access Control
The following network components are installed:
LPB for TCP/IP Printing      SCom EtherLink 10/100 PCI TX NIC (3C905B-TX)      Dial-Up Adapter      USB Fast Ethernet Adapter      TCP/IP -> 3Com EtherLink 10/100 PCI TX NIC (3C905B-T
Add Remove Properties
Client for Microsoft Networks
Eile and Print Sharing Description TCP/IP is the protocol you use to connect to the Internet and wide-area networks.
OK Cancel

#### Figure 130 WIndows 95/98/Me: Network: Configuration

## **Installing Components**

The **Network** window **Configuration** tab displays a list of installed components. You need a network adapter, the TCP/IP protocol and Client for Microsoft Networks.

If you need the adapter:

- 1 In the Network window, click Add.
- 2 Select Adapter and then click Add.
- **3** Select the manufacturer and model of your network adapter and then click **OK**.

If you need TCP/IP:

- 1 In the Network window, click Add.
- 2 Select Protocol and then click Add.
- **3** Select **Microsoft** from the list of **manufacturers**.
- 4 Select TCP/IP from the list of network protocols and then click OK.

If you need Client for Microsoft Networks:

- 1 Click Add.
- **2** Select **Client** and then click **Add**.

- **3** Select **Microsoft** from the list of manufacturers.
- **4** Select **Client for Microsoft Networks** from the list of network clients and then click **OK**.
- **5** Restart your computer so the changes you made take effect.

## Configuring

- **1** In the **Network** window **Configuration** tab, select your network adapter's TCP/IP entry and click **Properties**
- 2 Click the IP Address tab.
  - If your IP address is dynamic, select **Obtain an IP address** automatically.
  - If you have a static IP address, select **Specify an IP address** and type your information into the **IP Address** and **Subnet Mask** fields.

Figure 131	Windows	95/98/Me:	TCP/IP	Properties:	IP Address
------------	---------	-----------	--------	-------------	------------

TCP/IP Properties				? ×
Bindings	Adv	anced	N	etBIOS [
DNS Configuration	Gateway	WINS Config	guration	IP Address
An IP address can If your network dor your network admi the space below.	be automat es not auton nistrator for a address aut	ically assigned natically assign an address, ar omatically	d to this c n IP addro nd then ty	computer. esses, ask upe it in
C Specify an IF	address:			
[P Address:				
S <u>u</u> bnet Mas	k:			
☑ Detect conne	ection to net	work media		
		OK		Cancel

**3** Click the **DNS** Configuration tab.

- If you do not know your DNS information, select **Disable DNS**.
- If you know your DNS information, select **Enable DNS** and type the information in the fields below (you may not need to fill them all in).

Bindings	Adv	anced	Ne	etBIOS
DNS Configuration	Gateway	WINS Conl	iguration	IP Address
Disable DNS	ļ			
C Enable DNS				
Host:		D <u>o</u> main:		
DNS Server Sea	arch Order —			
			Add	1
			<u> </u>	1
		<u>F</u>	emove	
Domain Suffix S	earch Order			
			Add	
			emove	i l
				1
		0		Cancel

Figure 132 Windows 95/98/Me: TCP/IP Properties: DNS Configuration

- 4 Click the Gateway tab.
  - If you do not know your gateway's IP address, remove previously installed gateways.
  - If you have a gateway IP address, type it in the **New gateway field** and click **Add**.
- 5 Click OK to save and close the TCP/IP Properties window.
- 6 Click OK to close the Network window. Insert the Windows CD if prompted.
- 7 Restart your computer when prompted.

## **Verifying Settings**

- 1 Click Start and then Run.
- **2** In the **Run** window, type "winipcfg" and then click **OK** to open the **IP Configuration** window.
- **3** Select your network adapter. You should see your computer's IP address, subnet mask and default gateway.

# Windows 2000/NT/XP

The following example figures use the default Windows XP GUI theme.

1 Click start (Start in Windows 2000/NT), Settings, Control Panel.



Figure 133 Windows XP: Start Menu

**2** In the **Control Panel**, double-click **Network Connections** (**Network and Dial-up Connections** in Windows 2000/NT).

Figure 134 Windows XP: Control Panel



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



Figure 135 Windows XP: Control Panel: Network Connections: Properties

**4** Select **Internet Protocol (TCP/IP)** (under the **General** tab in Win XP) and then click **Properties**.

Figure 136 Windows XP: Local Area Connection Properties

占 Local	Area Connection Properties	? 🗙
General	Authentication Advanced	
Connec	t using:	
B A	accton EN1207D-TX PCI Fast Ethernet Adapter	
	Configu	ire
	File and Printer Sharing for Microsoft Networks	
	Internet Protocol (TCP/IP)	
	nstall Uninstall Properti	es
Tran: wide acros	iption smission Control Protocol/Internet Protocol. The defa area network protocol that provides communication ss diverse interconnected networks.	ult
Sho	w icon in notification area when connected	
	ОК	Cancel

- **5** The **Internet Protocol TCP/IP Properties** window opens (the **General tab** in Windows XP).
  - If you have a dynamic IP address click **Obtain an IP address** automatically.

- If you have a static IP address click Use the following IP Address and fill in the IP address, Subnet mask, and Default gateway fields.
- Click Advanced.

Figure 137	Windows	XP: Inte	ernet Pro	tocol (T	CP/IP)	Pror	perties
i iguic ior	********	//		10001 (1	O(n)	1 106	001000

ieneral A	Iternate Configuration	n				
You can g this capab the approp	et IP settings assigne ility. Otherwise, you r riate IP settings.	ed automat leed to ask	ically if y your ne	our ne twork	etwork admini	supports strator foi
📀 Obtai	n an IP address auto	matically				
Use t	he following IP addre	ess:				
IP addre	ess:					
Subnet	mask:			22		
Default	gateway:			- 63		
💿 Obtai	n DNS server addre:	ss automat	cally			
O Use t	he following DNS se	rver addre:	sses: —			
Preferre	d DNS server:		2	35	- 24	
Alternat	e DNS server:			- 53	2	
					Ac	lvanced
				ОК		Can

6 If you do not know your gateway's IP address, remove any previously installed gateways in the **IP Settings** tab and click **OK**.

Do one or more of the following if you want to configure additional IP addresses:

- In the IP Settings tab, in IP addresses, click Add.
- In **TCP/IP Address**, type an IP address in **IP address** and a subnet mask in **Subnet mask**, and then click **Add**.
- Repeat the above two steps for each IP address you want to add.
- Configure additional default gateways in the **IP Settings** tab by clicking **Add** in **Default gateways**.
- In **TCP/IP Gateway Address**, type the IP address of the default gateway in **Gateway**. To manually configure a default metric (the number of transmission hops), clear the **Automatic metric** check box and type a metric in **Metric**.
- Click Add.
- Repeat the previous three steps for each default gateway you want to add.
- Click **OK** when finished.

IP address DHCP Enabled		Subnet mask	
	Add	Edit	Remove
fault gateways: Gateway		Metric	
	Add	Edit	Remove
Automatic metric		1	

Figure 138 Windows XP: Advanced TCP/IP Properties

7 In the Internet Protocol TCP/IP Properties window (the General tab in Windows XP):

- Click **Obtain DNS server address automatically** if you do not know your DNS server IP address(es).
- If you know your DNS server IP address(es), click Use the following DNS server addresses, and type them in the Preferred DNS server and Alternate DNS server fields.

If you have previously configured DNS servers, click **Advanced** and then the **DNS** tab to order them.

Internet	Protocol (TCP/IP) Properties
General	Alternate Configuration
You car this cap the app	n get IP settings assigned automatically if your network supports pability. Otherwise, you need to ask your network administrator for propriate IP settings.
💿 O t	btain an IP address automatically
OU:	se the following IP address:
IP ac	ddress:
Subr	net mask:
Defa	ault gateway:
⊙ Ot	btain DNS server address automatically
-OU:	se the following DNS server addresses:
Prefe	erred DNS server:
Alten	nate DNS server:
	Advanced
	OK Cancel

Figure 139 Windows XP: Internet Protocol (TCP/IP) Properties

- 8 Click OK to close the Internet Protocol (TCP/IP) Properties window.
- **9** Click Close (OK in Windows 2000/NT) to close the Local Area Connection Properties window.
- **10** Close the **Network Connections** window (**Network and Dial-up Connections** in Windows 2000/NT).

**11**Restart your computer (if prompted).

## **Verifying Settings**

- 1 Click Start, All Programs, Accessories and then Command Prompt.
- 2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER]. You can also open **Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab.

# Macintosh OS X

1 Click the **Apple** menu, and click **System Preferences** to open the **System Preferences** window.

#### Figure 140 Macintosh OS X: Apple Menu



**2** Click **Network** in the icon bar.

- Select Automatic from the Location list.
- Select Built-in Ethernet from the Show list.
- Click the **TCP/IP** tab.

**3** For dynamically assigned settings, select Using DHCP from the Configure list.

Figure 141 Macintosh OS X: Network

Location: Automatic	+
ow: Built-in Ethernet 😭	
ТСР/ІР РРРоЕ Арр	leTalk Proxies
Configure: Using DHCP	•
	Domain Name Servers (Optional)
IP Address: 192.168.11.12 (Provided by DHCP Server)	168.95.1.1
Subnet Mask: 255.255.254.0	
Router: 192.168.10.11	Search Domains (Optional)
DHCP Client ID: (Optional)	
Ethernet Address: 00:05:02:43:93:ff	Example: apple.com, earthlink.net

**4** For statically assigned settings, do the following:

- From the **Configure** box, select **Manually**.
- Type your IP address in the IP Address box.
- Type your subnet mask in the **Subnet mask** box.
- Type the IP address of your gateway in the **Router address** box.
- **5** Click **Apply Now** and close the window.

6 Restart your computer (if prompted).

## **Verifying Settings**

Check your TCP/IP properties in the Network window.

# Linux

This section shows you how to configure your computer's TCP/IP settings in Red Hat Linux 9.0. Procedure, screens and file location may vary depending on your Linux distribution and release version.

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

## Using the K Desktop Environment (KDE)

Follow the steps below to configure your computer IP address using the KDE.

1 Click the Red Hat button (located on the bottom left corner), select **System Setting** and click **Network**.

Figure 142 Red Hat 9.0: KDE: Network Configuration: Devices



**2** Double-click on the profile of the network card you wish to configure. The **Ethernet Device General** screen displays as shown.

Ethernet	Device	0 3
<u>G</u> eneral <u>R</u>	oute <u>H</u> ardware Device	
<u>N</u> ickname:	eth0	
Activat	e device when computer starts	
🗌 Allow a	l <u>u</u> sers to enable and disable the device	
Automa	tically obtain IP address settings with: d	hcp ≚
DHCP S	ettings	
<u>H</u> ostnar	ne (optional):	]
🛃 Auto	matically obtain <u>D</u> NS information from prov	vider
<ul> <li>Statical</li> </ul>	lv set IP addresses:	
Manual	P Address Settings	
Address	1	
<u>S</u> ubnet	Mask:	
Default	Gateway Address:	
	<i>и</i> ок	X Cancel
	¥ <u>5</u>	

Figure 143 Red Hat 9.0: KDE: Ethernet Device: General

- If you have a dynamic IP address, click **Automatically obtain IP** address settings with and select dhcp from the drop down list.
- If you have a static IP address, click **Statically set IP Addresses** and fill in the **Address**, **Subnet mask**, and **Default Gateway Address** fields.
- 3 Click OK to save the changes and close the Ethernet Device General screen.
- **4** If you know your DNS server IP address(es), click the **DNS** tab in the **Network Configuration** screen. Enter the DNS server information in the fields provided.

Figure 144 Red Hat 9.0: KDE: Network Configuration: DNS

<u>-</u> ile <u>P</u> rofile	<u>H</u> elp				
New Edit	<u>С</u> ору	Delete			
Dev <u>i</u> ces Hard <u>w</u> a	are D <u>N</u> S	H <u>o</u> sts			
You m 1.4:3:2 1.3:5:5:4 1.3:5:5:4 Hostname:	ay config servers, o look up	gure the sys and search o other host	stem's hos domain. N s on the ne	name, doma ame servers twork.	ain, are
Primary DNS:					
<u>S</u> econdary DNS					
<u>T</u> ertiary DNS:					
DNS Search Pat	th:				

**5** Click the **Devices** tab.

6 Click the Activate button to apply the changes. The following screen displays. Click Yes to save the changes in all screens.

Figure 145 Red Hat 9.0: KDE: Network Configuration: Activate

💙 Questi	on		×
?	You have made some changes in your configuration. To activate the network device eth0, the changes have saved.	to b	2
	Do you want to continue?		
	× <u>N</u> o	<u>Y</u> es	]

7 After the network card restart process is complete, make sure the **Status** is **Active** in the **Network Configuration** screen.

## **Using Configuration Files**

Follow the steps below to edit the network configuration files and set your computer IP address.

- 1 Assuming that you have only one network card on the computer, locate the ifconfigeth0 configuration file (where eth0 is the name of the Ethernet card). Open the configuration file with any plain text editor.
  - If you have a dynamic IP address, enter **dhcp** in the BOOTPROTO= field. The following figure shows an example.

Figure 146 Red Hat 9.0: Dynamic IP Address Setting in ifconfig-eth0



• If you have a static IP address, enter **static** in the BOOTPROTO= field. Type IPADDR= followed by the IP address (in dotted decimal notation) and type NETMASK= followed by the subnet mask. The following example shows an example where the static IP address is 192.168.1.10 and the subnet mask is 255.255.255.0. Figure 147 Red Hat 9.0: Static IP Address Setting in ifconfig-eth0

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=static
IPADR=192.168.1.10
NETMASK=255.255.255.0
USERCTL=n0
PEERDNS=yes
TYPE=Ethernet
```

2 If you know your DNS server IP address(es), enter the DNS server information in the resolv.conf file in the /etc directory. The following figure shows an example where two DNS server IP addresses are specified.

Figure 148 Red Hat 9.0: DNS Settings in resolv.conf

```
nameserver 172.23.5.1
nameserver 172.23.5.2
```

**3** After you edit and save the configuration files, you must restart the network card. Enter./network restart in the /etc/rc.d/init.d directory. The following figure shows an example.

Figure 149 Red Hat 9.0: Restart Ethernet Card

```
[root@localhost init.d]# network restart
Shutting down interface eth0: [OK]
Shutting down loopback interface: [OK]
Setting network parameters: [OK]
Bringing up loopback interface: [OK]
Bringing up interface eth0: [OK]
```

## **Verifying Settings**

Enter ifconfig in a terminal screen to check your TCP/IP properties.

Figure 150 Red Hat 9.0: Checking TCP/IP Properties

```
[root@localhost]# ifconfig
eth0 Link encap:Ethernet HWaddr 00:50:BA:72:5B:44
    inet addr:172.23.19.129 Bcast:172.23.19.255 Mask:255.255.255.0
    UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
    RX packets:717 errors:0 dropped:0 overruns:0 frame:0
    TX packets:13 errors:0 dropped:0 overruns:0 carrier:0
    collisions:0 txqueuelen:100
    RX bytes:730412 (713.2 Kb) TX bytes:1570 (1.5 Kb)
    Interrupt:10 Base address:0x1000
[root@localhost]#
```

# **APPENDIX D** IP Addresses and Subnetting

This appendix introduces IP addresses and subnet masks.

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

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

# Introduction to IP Addresses

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

# Structure

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

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

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





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 "subnetwork".

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: (192)	2ND OCTET: (168)	3RD OCTET: (1)	4TH OCTET (2)
IP Address (Binary)	11000000	10101000	0000001	00000010
Subnet Mask (Binary)	11111111	11111111	11111111	0000000
Network Number	11000000	10101000	00000001	
Host ID				00000010

 Table 95
 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	0000000	00000000	0000000	255.0.0.0
16-bit mask	11111111	11111111	00000000	0000000	255.255.0.0
24-bit mask	11111111	11111111	11111111	0000000	255.255.255.0
29-bit mask	11111111	11111111	11111111	11111000	255.255.255.248

Table 96 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:

SUBNET MASK		HOST ID SIZE		MAXIMUM NUMBER OF HOSTS
8 bits	255.0.0.0	24 bits	2 <sup>24</sup> – 2	16777214
16 bits	255.255.0.0	16 bits	2 <sup>16</sup> – 2	65534
24 bits	255.255.255.0	8 bits	2 <sup>8</sup> – 2	254
29 bits	255.255.255.248	3 bits	2 <sup>3</sup> – 2	6

Table 97 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
255.255.255.128	/25	1000 0000	128

 Table 98
 Alternative Subnet Mask Notation

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

**Table 98** Alternative Subnet Mask Notation (continued)

# 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.





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 subnetworks, A and B.



Figure 153 Subnetting Example: After Subnetting

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

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

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

# **Example: Four Subnets**

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).

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address (Decimal)	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	<b>00</b> 000000
Subnet Mask (Binary)	11111111.1111111.11111111.	11000000
Subnet Address: 192.168.1.0	Lowest Host ID: 192.168.1.1	
Broadcast Address: 192.168.1.63	Highest Host ID: 192.168.1.62	

Table	99	Subnet 1

Table Too Sublet 2				
IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE		
IP Address	192.168.1.	64		
IP Address (Binary)	11000000.10101000.00000001.	<b>01</b> 000000		
Subnet Mask (Binary)	11111111.1111111.11111111.	11000000		
Subnet Address: 192.168.1.64	Lowest Host ID: 192.168.1.65			
Broadcast Address: 192.168.1.127	Highest Host ID: 192.168.1.126			

#### Table 100 Subnet 2

#### Table 101Subnet 3

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	<b>10</b> 000000
Subnet Mask (Binary)	11111111.1111111.11111111.	<b>11</b> 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 102Subnet 4

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	192
IP Address (Binary)	11000000.10101000.00000001.	11000000
Subnet Mask (Binary)	11111111.1111111.11111111.	11000000
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

#### Table 103 Eight Subnets

SUBNET	SUBNET ADDRESS	FIRST ADDRESS	LAST ADDRESS	BROADCAST ADDRESS
5	128	129	158	159
6	160	161	190	191
7	192	193	222	223
8	224	225	254	255

 Table 103
 Eight Subnets (continued)

# **Subnet Planning**

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

 Table 104
 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

 Table 105
 16-bit Network Number Subnet Planning

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
14	255.255.255.252 (/30)	16384	2
15	255.255.255.254 (/31)	32768	1

 Table 105
 16-bit Network Number Subnet Planning (continued)

# **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 ZyXEL Device.

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

# APPENDIX E SIP Passthrough

# Enabling/Disabling the SIP ALG

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

# **Signaling Session Timeout**

Most SIP clients have an "expire" mechanism indicating the lifetime of signaling sessions. The SIP UA sends registration packets to the SIP server periodically and keeps the session alive in the ZyXEL Device.

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

# **Audio Session Timeout**

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

# APPENDIX F Services

The following table lists some commonly-used services and their associated protocols and port numbers.

- 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**.
  - 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	TCP	5190	AOL's Internet Messenger service.
AUTH	TCP	113	Authentication protocol used by some servers.
BGP	TCP	179	Border Gateway Protocol.
BOOTP_CLIENT	UDP	68	DHCP Client.
BOOTP_SERVER	UDP	67	DHCP Server.
CU-SEEME	TCP/UDP TCP/UDP	7648 24032	A popular videoconferencing solution from White Pines Software.
DNS	TCP/UDP	53	Domain Name Server, a service that matches web names (e.g. <u>www.zyxel.com</u> ) to IP numbers.
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	TCP	20	File Transfer Program, a program to enable
	TCP	21	tast transfer of files, including large files that may not be possible by e-mail.
H.323	TCP	1720	NetMeeting uses this protocol.

### Table 106 Examples of Services

NAME	PROTOCOL	PORT(S)	DESCRIPTION	
HTTP	TCP	80	Hyper Text Transfer Protocol - a client/ server protocol for the world wide web.	
HTTPS	TCP	443	HTTPS is a secured http session often used in e-commerce.	
ICMP	User-Defined	1	Internet Control Message Protocol is often used for diagnostic purposes.	
ICQ	UDP	4000	This is a popular Internet chat program.	
IGMP (MULTICAST)	User-Defined	2	Internet Group Multicast 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.	
IMAP4	TCP	143	The Internet Message Access Protocol is used for e-mail.	
IMAP4S	TCP	993	This is a more secure version of IMAP4 that runs over SSL.	
IRC	TCP/UDP	6667	This is another popular Internet chat program.	
MSN Messenger	TCP	1863	Microsoft Networks' messenger service uses this protocol.	
NetBIOS	TCP/UDP TCP/UDP TCP/UDP TCP/UDP	137 138 139 445	The Network Basic Input/Output System is used for communication between computers in a LAN.	
NEW-ICQ	TCP	5190	An Internet chat program.	
NEWS	TCP	144	A protocol for news groups.	
NFS	UDP	2049	Network File System - NFS is a client/ server distributed file service that provides transparent file sharing for network environments.	
NNTP	TCP	119	Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service.	
PING	User-Defined	1	Packet INternet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable.	
POP3	TCP	110	Post Office Protocol version 3 lets a client computer get e-mail from a POP3 server through a temporary connection (TCP/IP or other).	
POP3S	TCP	995	This is a more secure version of POP3 that runs over SSL.	
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.	

 Table 106
 Examples of Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION	
RCMD	TCP	512	Remote Command Service.	
REAL_AUDIO	TCP	7070	A streaming audio service that enables real time sound over the web.	
REXEC	TCP	514	Remote Execution Daemon.	
RLOGIN	TCP	513	Remote Login.	
ROADRUNNER	TCP/UDP	1026	This is an ISP that provides services mainly for cable modems.	
RTELNET	TCP	107	Remote Telnet.	
RTSP	TCP/UDP	554	The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.	
SFTP	TCP	115	The Simple File Transfer Protocol is an old way of transferring files between computers.	
SMTP	TCP	25	Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another.	
SMTPS	TCP	465	This is a more secure version of SMTP that runs over SSL.	
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.	
SSDP	UDP	1900	The Simple Service Discovery Protocol supports Universal Plug-and-Play (UPnP).	
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.	
TFTP	UDP	69	Trivial File Transfer Protocol is an Internet file transfer protocol similar to FTP, but uses the UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol).	
VDOLIVE	TCP UDP	7000 user- defined	A videoconferencing solution. The UDP port number is specified in the application.	

Table 106	Examples of Services	(continued)
-----------	----------------------	-------------

# Index

# A

AAA 72 about this User's Guide 27 AbS 111 accounting server see AAA ACK message 106 activity 72 address resolution protocol (ARP) 87 advanced encryption standard see AES AES 221 AK 221 ALG 99, 217 alternative subnet mask notation 239 analysis-by-synthesis 111 antenna 215 any IP 216 note 87 application layer gateway 99, 109, 217 Application Layer Gateway. See ALG. authentication 65, 72, 73, 219 inner 222 types 222 authentication key see AK authentication server see AAA authorization 219 authorization request and reply 221 authorization server see AAA auto firmware upgrade 216 auto-discovering UPnP-enabled network devices 167 automatic log out 35 auto-provisioning 216

# В

base station see BS BS 71 links 71 BYE request 106

## С

call hold 122, 124 call service mode 122, 124 call transfer 123, 124 call waiting 123, 124 CBC-MAC 221 CCMP 219, 221 CD 27 cell 71 certificate 219 verification 221 certifications 4 notices 5 viewing 5 chaining 221 chaining message authentication see CCMP change password at login 34 circuit-switched telephone networks 105 Class of Service (CoS) 113 clicks 111 client server SIP 106 client-server protocol 106 CMAC see MAC code 219 codec 110 coder/decoder 110 comfort noise 121 comfort noise generation 217 computer IP address 223 computer name 197 configuration 27 configuration upload successful 195 connections 27, 31 contact information 9 copyright 3 CoS 113 counter mode see CCMP

coverage area 71 cryptography 219 customer support 9

# D

data encryption 219, 221 data flow 221 data rate 215 daytime RFC 867 203 decoder 110 decryption 219, 221 default LAN IP address 33 device name 175 DHCP 197, 198, 217 DHCP client 217 DHCP clients 197 DHCP relay 217 DHCP server 217 DIAMETER 72 differentiated services 113 DiffServ 113 DiffServ Code Point (DSCP) 113 DiffServ code point (DSCP) 113 DiffServ marking rule 113 digital ID 219 dimensions 215 disclaimer 3 DL frequency 78 domain name 197 download frequency see DL frequency DS field 113 DSCPs 113 DTMF 111 dual-tone multi-frequency see DTMF duplex 215 dynamic DNS 198, 217 dynamic host configuration protocol 217 dynamic jitter buffer 217

## Ε

EAP 72 echo cancellation 121, 217 encoding 219 encrypted traffic 221 encryption 219, 221 environmental specifications 215 ethernet 215 ethernet encapsulation 97 europe type call service mode 122 extensible authorization protocol see EAP External Antenna 216

## F

FCC interference statement 4 firewall 131, 132 firmware 191 firmware upload 192 firmware upload error 193 flash key 122 flashing 122 frequency band 78 scanning 78 frequency pairs 111 frequency ranges 78 FTP 153, 198 FTP restrictions 153

# G

G.168 **121**, **217** G.711 **110** G.729 **111** Graphical User Interface (GUI) **29** graphics icons key **28** 

# Η

hardware 27, 31 HTTP 191 humidity 215 hybrid waveform codec 111 hypertext transfer protocol 191

## I

IANA 244 icons 28 identity 72, 219 idle timeout 154 IEEE 802.16 71, 219 IEEE 802.16e 27, 71 IEEE 802.1Q VLAN 113 IGD 1.0 164 inner authentication 222 install UPnP 164 Windows Me 164 Windows XP 166 installation 27, 31 interface 215 interference 206 Internet access 72, 216 Internet access wizard setup 49 Internet Assigned Numbers Authority See IANA 244 Internet gateway device 164 Internet service provider see ISP Internet Telephony Service Provider 30 Internet telephony service provider 105 interoperability 71 introduction 29 IP alias 217 IP policy routing (IPPR) 217 **IP-PBX 105** ISP 41 **ITSP 105** ITU-T 121

### J

jitter buffer 217

## Κ

key 65, 73, 219 key request and reply 221

## L

language 27 link quality troubleshooting 206 listening port 118 log out 35

## Μ

MAC 221 **MAN 71** management information base (MIB) 157 manual site survey 78 media access protocol 215 message authentication code see MAC message integrity 221 message waiting indication 111 Metropolitan Area Network see MAN microwave 71 mobile station see MS modulation 215 mouse action sequences 27 MS 71 multimedia 105 multiple PVC support 217 multiple SIP accounts 217 MWI 111

# Ν

NAT 244 and remote management 154 server sets 97 NAT routers 109 NAT traversal 163 network activity 72 network address translation (NAT) 216 network address translators 109 network disconnect 193, 195 network services 72 NTP RFC 1305 203 NTP time servers 198

# 0

OK response 106 operating humidity 215 operating temperature 215 outbound proxy 109, 110 SIP 110 outbound proxy server 110

## Ρ

pattern-spotting 221 PBX services 105 PCM 110 peer-to-peer calls 139 per-hop behavior 113 PHB (per-hop behavior) 113 phone book 139 phone services 121 physical specifications 215 PKMv2 65, 72, 73, 219, 222 plain text encryption 221 port forwarding 97 port numbers 97 services 97 port numbers 97 power 215 output 215 power supply 215 pre-defined NTP time servers list 198 preparation 29 privacy key management see PKM private key 219 product registration 8 product specifications see specifications proxy server SIP 107 **PSTN 111** public certificate 221 public key 65, 73, 219 Public Switched Telephone Network 111 pulse code modulation 110 pulse dialing 111

## Q

QoS 112, 217 quality of service see QoS Quick Start Guide 27, 31, 33

# R

radio specifications 215 RADIUS 72, 220 Shared Secret Key 221 RADIUS Message Types 220 RADIUS Messages 220 real-time transport protocol 108 reception 206 redirect server SIP 108 register server SIP 108 registration product 8 related documentation 27 remote management 153 remote management and NAT 154 remote management limitations 153 **REN 217** required bandwidth 111 reset button 35, 194 resetting the time 199 resetting your device 35 RFC 1305 203 RFC 1889 108 RFC 3489 109 RFC 3842 111 RFC 867 203 RFC 868 203 ringer equivalence number 217 RTP 108

## S

safety warnings 6 secure communication 65, 73, 219 secure connection 72 security 215, 219 security association 221 see SA see QoS see WAN server, outbound proxy 110 services 72, 97 session initiation protocol see SIP silence suppression 121, 217 silent packets 121 SIP 105 ALG 99 authentication 56 authentication password 56 SIP account 105, 217 SIP ACK message 106 SIP ALG 99, 109, 217 SIP application layer gateway 99, 217 SIP BYE request 106 SIP call progression 106 SIP client 106 SIP client server 106 SIP identities 105 SIP INVITE request 106 SIP number 56, 105 SIP OK response 106 SIP outbound proxy 110 SIP proxy server 107 SIP redirect server 108 SIP register server 108 SIP server address 56 SIP servers 106 SIP service domain 56, 106 SIP URI 105 SIP user agent 107 **SNMP 156** manager 157 MIBs 157 sound quality 110 specifications 215 physical and environmental 215 radio 215 speed dial 139 SS 71 standards 215 stateful inspection 131 storage humidity 215 storage temperature 215 **STUN 109** subnet 237 subnet mask 238

subnetting 240 subscriber station see SS supplementary phone services 121 support 27 support CD 27 syntax conventions 27 system name 197 system timeout 154

# Т

tampering TDD 215 TEK 221 telephone keys 111 temperature 215 terms 27 TFTP restrictions 153 three-way conference 123, 125 time resetting 199 time RFC 868 203 TLS 65, 73, 219 ToS 112 Touch Tone® 111 trademarks 3 transport encryption key see TEK transport layer security see TLS triangle 134 triangle route solutions 134 trigger port forwarding 98 process 98 troubleshooting link quality 206 TTLS 65, 73, 219, 222 tunneled TLS see TTLS Type of Service 112

# U

UIC 164 unauthorized device 219

uniform resource identifier 105 Universal Plug and Play 163 application 163 security issues 163 Universal Plug and Play (UPnP) 216 Universal Plug and Play Forum 164 UPnP 163, 175 auto-discovery 167 installing example 164 UPnP certification 164 USA type call service mode 124 use NAT 109 user agent, SIP 107 user authentication 219 user ID 56 user name 201

WiMAX 27, 71, 215 security 221 WiMAX Forum 71
WiMAX bandwidth 215
Wireless Interoperability for Microwave Access see WiMAX
wireless Metropolitan Area Network see MAN
wireless network 27 access 71 standard 71
wireless security 215, 219
wizard setup 49

# Ζ

ZyXEL utility 29, 31

# V

VAD 121, 217 verification 221 virtual local area network see VLAN **VLAN 113** VLAN group 113 **VLAN ID 113** VLAN ID tags 113 VLAN tags 113 voice activity detection 121, 217 voice coding 110 voice mail 105 voice over IP see VoIP VoIP 27, 105 standards compliance 217

## W

WAN 71 WAN setup 71 warranty 8 note 8 waveform codec 110 weather conditions 206 web configurator 33 weight 215 wide area network