Table 52 SECURITY > CERTIFICATES > My Certificates > Details (continued)

LABEL	DESCRIPTION
Serial Number	This field displays the certificate's identification number given by the certification authority or generated by the ZyXEL Device.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), Organizational Unit (OU), Organization (O) and Country (C).
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as Common Name, Organizational Unit, Organization and Country. With self-signed certificates, this is the same as the **Subject Name** field.
Signature Algorithm	This field displays the type of algorithm that was used to sign the certificate. The ZyXEL Device uses rsa-pkcs1-sha1 (RSA public-private key encryption algorithm and the SHA1 hash algorithm). Some certification authorities may use rsa-pkcs1-md5 (RSA public-private key encryption algorithm and the MD5 hash algorithm).
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.
Key Algorithm	This field displays the type of algorithm that was used to generate the certificate's key pair (the ZyXEL Device uses RSA encryption) and the length of the key set in bits (1024 bits for example).
Subject Alternative Name	This field displays the certificate owner's IP address (IP), domain name (DNS) or e-mail address (EMAIL).
Key Usage	This field displays for what functions the certificate's key can be used. For example, "DigitalSignature" means that the key can be used to sign certificates and "KeyEncipherment" means that the key can be used to encrypt text.
Basic Constraint	This field displays general information about the certificate. For example, Subject Type=CA means that this is a certification authority's certificate and "Path Length Constraint=1" means that there can only be one certification authority in the certificate's path.
MD5 Fingerprint	This is the certificate's message digest that the ZyXEL Device calculated using the MD5 algorithm.
SHA1 Fingerprint	This is the certificate's message digest that the ZyXEL Device calculated using the SHA1 algorithm.
Certificate in PEM (Base-64) Encoded Format	This read-only text box displays the certificate or certification request in Privacy Enhanced Mail (PEM) format. PEM uses 64 ASCII characters to convert the binary certificate into a printable form. You can copy and paste a certification request into a certification authority's web page, an e-mail that you send to the certification authority or a text editor and save the file on a management computer for later manual enrollment. You can copy and paste a certificate into an e-mail to send to friends or colleagues or you can copy and paste a certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example).
Apply	Click **Apply** to save your changes back to the ZyXEL Device. You can only change the name, except in the case of a self-signed certificate, which you can also set to be the default self-signed certificate that signs the imported trusted remote host certificates.
Cancel	Click **Cancel** to quit and return to the **My Certificates** screen.

11.7 My Certificate Export

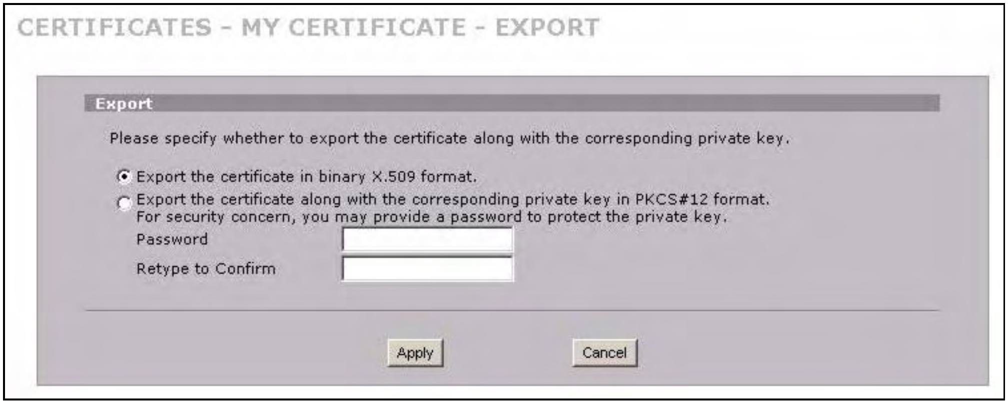
Click **SECURITY > CERTIFICATES > My Certificates** and then a certificate's export icon to open the **My Certificate Export** screen. Follow the instructions in this screen to choose the file format to use for saving the certificate from the ZyXEL Device to a computer.

11.7.1 Certificate File Export Formats

You can export a certificate in one of these file formats:

- Binary X.509: This is an ITU-T recommendation that defines the formats for X.509 certificates.
- Binary PKCS#12: This is a format for transferring public key and private key certificates. The private key in a PKCS #12 file is within a password-encrypted envelope. The file's password is not connected to your certificate's public or private passwords. Exporting a PKCS #12 file creates this and you must provide it to decrypt the contents when you import the file into the ZyXEL Device.

Figure 123 SECURITY > CERTIFICATES > My Certificates > Export



CERTIFICATES - MY CERTIFICATE - EXPORT

Export

Please specify whether to export the certificate along with the corresponding private key.

● Export the certificate in binary X.509 format.

○ Export the certificate along with the corresponding private key in PKCS#12 format.
For security concern, you may provide a password to protect the private key.

Password

Retype to Confirm

The following table describes the labels in this screen.

Table 53 SECURITY > CERTIFICATES > My Certificates > Export

LABEL	DESCRIPTION
Export the certificate in binary X.509 format.	Binary X.509 is an ITU-T recommendation that defines the formats for X.509 certificates.
Export the certificate along with the corresponding private key in PKCS#12 format.	PKCS#12 is a format for transferring public key and private key certificates. You can also password-encrypt the private key in the PKCS #12 file. The file's password is not connected to your certificate's public or private passwords.
Password	Type the file's password to use for encrypting the private key. The password is optional, although you must specify one if you want to be able to import the PKCS#12 format certificate into Netscape version 7.2.
Retype to confirm	Type the password to make sure that you have entered it correctly.
Apply	Click **Apply** and then **Save** in the **File Download** screen. The **Save As** screen opens, browse to the location that you want to use and click **Save**.
Cancel	Click **Cancel** to quit and return to the **My Certificates** screen.

11.8 My Certificate Import

Click **SECURITY** > **CERTIFICATES** > **My Certificates** and then **Import** to open the **My Certificate Import** screen. Follow the instructions in this screen to save an existing certificate from a computer to the ZyXEL Device.

You can only import a certificate that matches a corresponding certification request that was generated by the ZyXEL Device (the certification request contains the private key). The certificate you import replaces the corresponding request in the **My Certificates** screen.
One exception is that you can import a PKCS#12 format certificate without a corresponding certification request since the certificate includes the private key.

You must remove any spaces from the certificate's filename before you can import it.

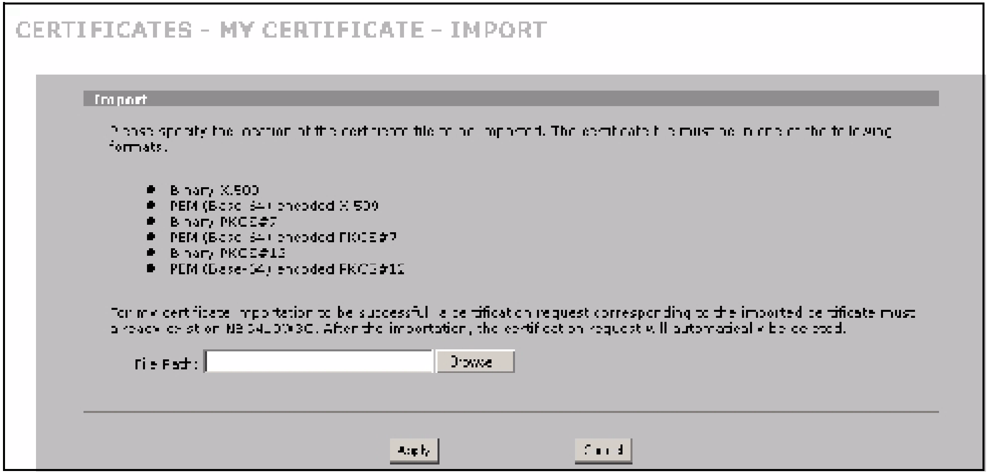
11.8.1 Certificate File Formats

The certification authority certificate that you want to import has to be in one of these file formats:

- Binary X.509: This is an ITU-T recommendation that defines the formats for X.509 certificates.
- PEM (Base-64) encoded X.509: This Privacy Enhanced Mail format uses 64 ASCII characters to convert a binary X.509 certificate into a printable form.
- Binary PKCS#7: This is a standard that defines the general syntax for data (including digital signatures) that may be encrypted. The ZyXEL Device currently allows the importation of a PKS#7 file that contains a single certificate.
- PEM (Base-64) encoded PKCS#7: This Privacy Enhanced Mail (PEM) format uses 64 ASCII characters to convert a binary PKCS#7 certificate into a printable form.
- Binary PKCS#12: This is a format for transferring public key and private key certificates. The private key in a PKCS #12 file is within a password-encrypted envelope. The file's password is not connected to your certificate's public or private passwords. Exporting a PKCS #12 file creates this and you must provide it to decrypt the contents when you import the file into the ZyXEL Device.

Be careful to not convert a binary file to text during the transfer process. It is easy for this to occur since many programs use text files by default.

Figure 124 SECURITY > CERTIFICATES > My Certificates > Import



CERTIFICATES - MY CERTIFICATE - IMPORT

Please specify the location of the certificate file to be imported. The certificate file must be in one of the following formats.

- Binary X.509
- PEM (Base-64) encoded X.509
- Binary PKCS#7
- PEM (Base-64) encoded PKCS#7
- Binary PKCS#12
- PEM (Base-64) encoded PKCS#12

For my certificate importation to be successful, a certification request corresponding to the imported certificate must already exist on NBG410W3G. After the importation, the certification request will automatically be deleted.

File Path:

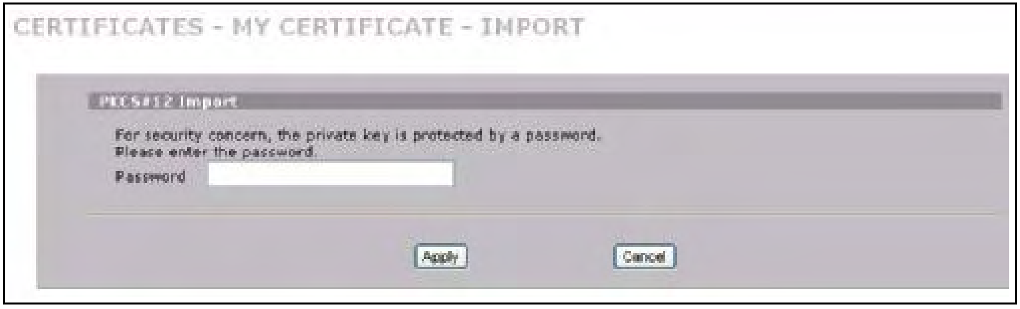
The following table describes the labels in this screen.

Table 54 SECURITY > CERTIFICATES > My Certificates > Import

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click **Browse** to find it.
Browse	Click **Browse** to find the certificate file you want to upload.
Apply	Click **Apply** to save the certificate on the ZyXEL Device.
Cancel	Click **Cancel** to quit and return to the **My Certificates** screen.

When you import a binary PKCS#12 format certificate, another screen displays for you to enter the password.

Figure 125 SECURITY > CERTIFICATES > My Certificates > Import: PKCS#12



CERTIFICATES - MY CERTIFICATE - IMPORT

For security concern, the private key is protected by a password.
Please enter the password.

Password

The following table describes the labels in this screen.

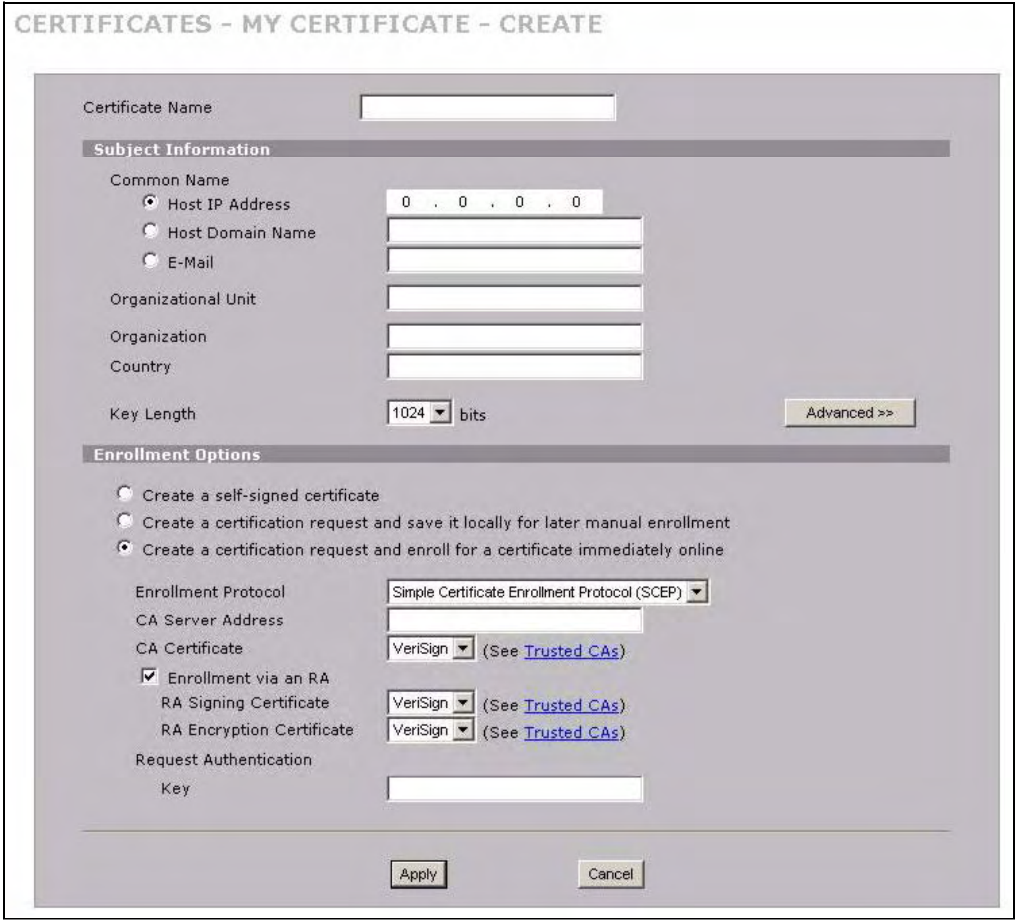
Table 55 SECURITY > CERTIFICATES > My Certificates > Import: PKCS#12

LABEL	DESCRIPTION
Password	Type the file’s password that was created when the PKCS #12 file was exported.
Apply	Click **Apply** to save the certificate on the ZyXEL Device.
Cancel	Click **Cancel** to quit and return to the **My Certificates** screen.

11.9 My Certificate Create

Click **SECURITY** > **CERTIFICATES** > **My Certificates > Create** to open the **My Certificate Create** screen. Use this screen to have the ZyXEL Device create a self-signed certificate, enroll a certificate with a certification authority or generate a certification request.

Figure 126 SECURITY > CERTIFICATES > My Certificates > Create (Basic)



CERTIFICATES - MY CERTIFICATE - CREATE

Certificate Name

Subject Information

Common Name
- ● Host IP Address 0 . 0 . 0 . 0
- ○ Host Domain Name
- ○ E-Mail

Organizational Unit

Organization

Country

Key Length 1024 bits

Enrollment Options

- ○ Create a self-signed certificate
- ○ Create a certification request and save it locally for later manual enrollment
- ● Create a certification request and enroll for a certificate immediately online

Enrollment Protocol: Simple Certificate Enrollment Protocol (SCEP)

CA Server Address

CA Certificate: VeriSign (See Trusted CAs)

☑ Enrollment via an RA

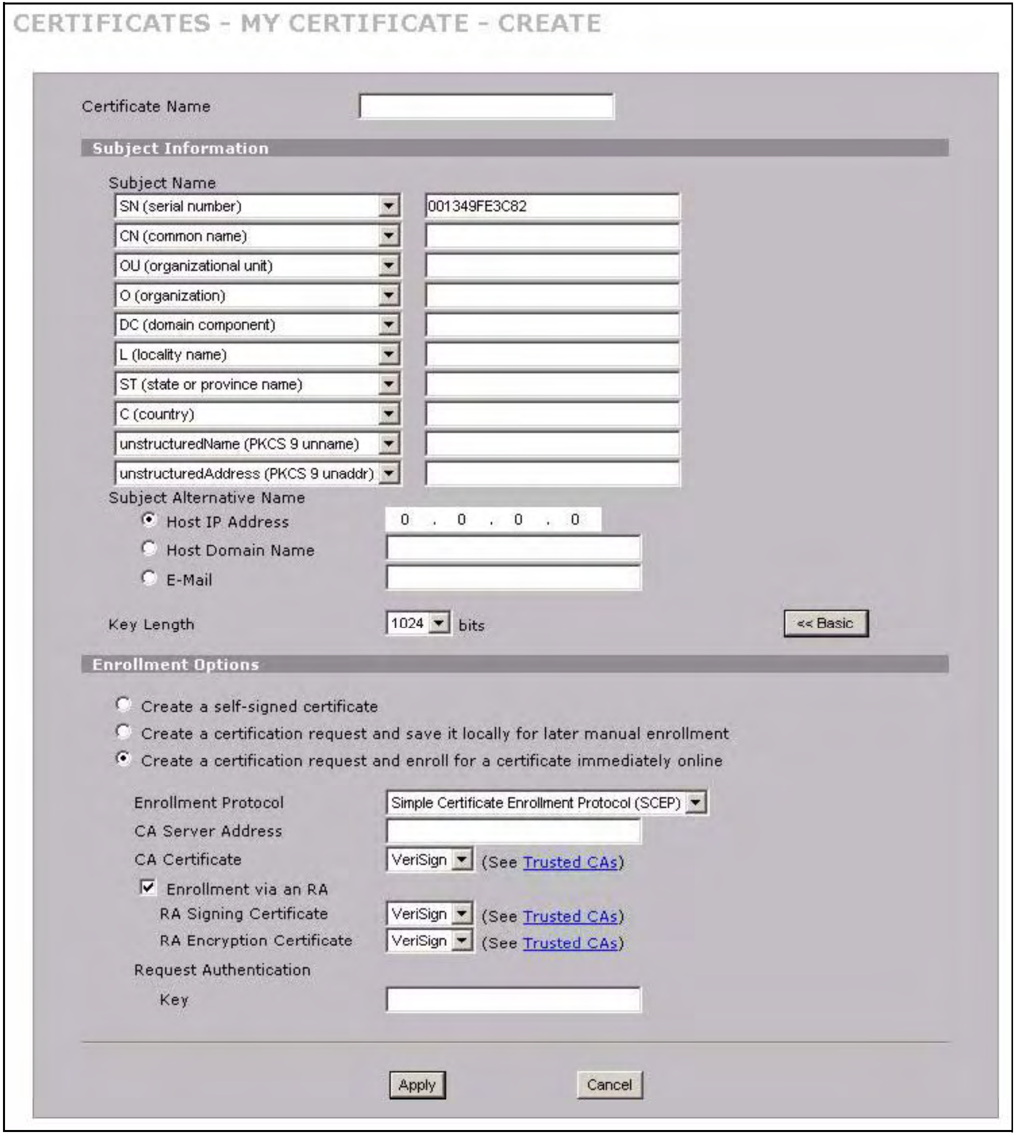
RA Signing Certificate: VeriSign (See Trusted CAs)

RA Encryption Certificate: VeriSign (See Trusted CAs)

Request Authentication

Key

Figure 127 SECURITY > CERTIFICATES > My Certificates > Create (Advanced)



CERTIFICATES - MY CERTIFICATE - CREATE

Certificate Name

Subject Information

Subject Name

SN (serial number) 001349FE3C82
CN (common name)
OU (organizational unit)
O (organization)
DC (domain component)
L (locality name)
ST (state or province name)
C (country)
unstructuredName (PKCS 9 unname)
unstructuredAddress (PKCS 9 unaddr)

Subject Alternative Name
● Host IP Address 0 . 0 . 0 . 0
○ Host Domain Name
○ E-Mail

Key Length 1024 bits

Enrollment Options

○ Create a self-signed certificate
○ Create a certification request and save it locally for later manual enrollment
● Create a certification request and enroll for a certificate immediately online

Enrollment Protocol Simple Certificate Enrollment Protocol (SCEP)
CA Server Address
CA Certificate VeriSign (See Trusted CAs)
☑ Enrollment via an RA
RA Signing Certificate VeriSign (See Trusted CAs)
RA Encryption Certificate VeriSign (See Trusted CAs)
Request Authentication
Key

The following table describes the labels in this screen.

Table 56 SECURITY > CERTIFICATES > My Certificates > Create

LABEL	DESCRIPTION
Certificate Name	Type up to 31 ASCII characters (not including spaces) to identify this certificate.
Subject Information	Use these fields to record information that identifies the owner of the certificate. You do not have to fill in every field, but the **Common Name** is mandatory if you click **<< Basic**. The certification authority may add fields (such as a serial number) to the subject information when it issues a certificate. It is recommended that each certificate have unique subject information.
The fields below display when you click **<< Basic**.	

Table 56 SECURITY > CERTIFICATES > My Certificates > Create (continued)

LABEL	DESCRIPTION
Common Name	Select a radio button to identify the certificate's owner by IP address, domain name or e-mail address. Type the IP address (in dotted decimal notation), domain name or e-mail address in the field provided. The domain name or e-mail address can be up to 31 ASCII characters. The domain name or e-mail address is for identification purposes only and can be any string.
Organizational Unit	Type up to 63 characters to identify the organizational unit or department to which the certificate owner belongs. You may use any character, including spaces, but the ZyXEL Device drops trailing spaces.
Organization	Type up to 63 characters to identify the company or group to which the certificate owner belongs. You may use any character, including spaces, but the ZyXEL Device drops trailing spaces.
Country	Type up to 63 characters to identify the nation where the certificate owner is located. You may use any character, including spaces, but the ZyXEL Device drops trailing spaces.
The fields below display when you click **Advanced >>**.	
Subject Name	You must configure at least one of these fields. Select an item from the drop-down list box and enter the corresponding information in the field to the right. **SN (serial number)** - select this and enter the certificate's identification number, such as the ZyXEL Device's MAC address. You can use up to 63 characters. **CN (common name)** - select this and enter a name to identify the owner of the certificate. You can use up to 63 characters. **OU (organizational unit)** - select this and enter a unit within the organization to identify the owner of the certificate. You can use up to 63 characters. **O (organization)** - select this and enter an organization to identify the owner of the certificate. You can use up to 63 characters. **DC (domain component)** - select this and enter the domain component of a domain to identify the owner of the certificate. For example, if the domain is zyxel.com, the domain component is "zyxel" or "com". You can use up to 63 characters. **L (locality name)** - select this and enter the place where the owner of the certificate resides, such as a city or county. You can use up to 63 characters. **ST (state or province name)** - select this and enter the state or province in which the owner of the certificate resides. You can use up to 63 characters. **C (country)** - select this and enter the name of the country at which the owner of the certificate resides. You can use up to 63 characters. **unstructuredName (PKCS 9 unname)** - select this and enter the name of the owner of the certificate as an unstructured ASCII string. You can use up to 63 characters. Check with the certificate's issuing certification authority for their interpretation in this field if you select to apply to a certification authority for a certificate. **unstructuredAddress (PKCS 9 unaddr)** - select this and enter the address of the owner of the certificate as an unstructured ASCII string. You can use up to 63 characters. Check with the certificate's issuing certification authority for their interpretation in this field if you select to apply to a certification authority for a certificate. **MAILTO (PKCS 9 email address)** - select this and enter the email address of the owner of the certificate. You can use up to 63 characters. Check with the certificate's issuing certification authority for their interpretation in this field if you select to apply to a certification authority for a certificate.

Table 56 SECURITY > CERTIFICATES > My Certificates > Create (continued)

LABEL	DESCRIPTION
Subject Alternative Name	Select a radio button to identify the certificate's owner by IP address, domain name or e-mail address. Type the IP address (in dotted decimal notation), domain name or e-mail address in the field provided. The domain name or e-mail address can be up to 31 ASCII characters. The domain name or e-mail address is for identification purposes only and can be any string.
Key Length	Select a number from the drop-down list box to determine how many bits the key should use (512 to 2048). The longer the key, the more secure it is. A longer key also uses more PKI storage space.
<< Basic/Advanced >>	Click **<< Basic** to configure basic subject information. Click **Advanced >>** to configure more subject information for a certificate.
Enrollment Options	These radio buttons deal with how and when the certificate is to be generated.
Create a self-signed certificate	Select **Create a self-signed certificate** to have the ZyXEL Device generate the certificate and act as the Certification Authority (CA) itself. This way you do not need to apply to a certification authority for certificates.
Create a certification request and save it locally for later manual enrollment	Select **Create a certification request and save it locally for later manual enrollment** to have the ZyXEL Device generate and store a request for a certificate. Use the **My Certificate Details** screen to view the certification request and copy it to send to the certification authority. Copy the certification request from the **My Certificate Details** screen (see Section 11.6 on page 200) and then send it to the certification authority.
Create a certification request and enroll for a certificate immediately online	Select **Create a certification request and enroll for a certificate immediately online** to have the ZyXEL Device generate a request for a certificate and apply to a certification authority for a certificate. You must have the certification authority's certificate already imported in the **Trusted CAs** screen. When you select this option, you must select the certification authority's enrollment protocol and the certification authority's certificate from the drop-down list boxes and enter the certification authority's server address. You also need to fill in the **Reference Number** and **Key** if the certification authority requires them.
Enrollment Protocol	Select the certification authority's enrollment protocol from the drop-down list box. **Simple Certificate Enrollment Protocol (SCEP)** is a TCP-based enrollment protocol that was developed by VeriSign and Cisco. **Certificate Management Protocol (CMP)** is a TCP-based enrollment protocol that was developed by the Public Key Infrastructure X.509 working group of the Internet Engineering Task Force (IETF) and is specified in RFC 2510.
CA Server Address	Enter the IP address (or URL) of the certification authority server.
CA Certificate	Select the certification authority's certificate from the **CA Certificate** drop-down list box. You must have the certification authority's certificate already imported in the **Trusted CAs** screen. Click **Trusted CAs** to go to the **Trusted CAs** screen where you can view (and manage) the ZyXEL Device's list of certificates of trusted certification authorities.
Enrollment via an RA	If you select **Create a certification request and enroll for a certificate immediately online**, you can select this option to apply for a certificate through a RA (Registration Authority). The RA is an intermediary authorized by a CA to verify each subscriber's identity and forward the requests to the CA. After the CA signs and issues the certificates, the RA distributes the certificates to the subscribers.

Table 56 SECURITY > CERTIFICATES > My Certificates > Create (continued)

LABEL	DESCRIPTION
RA Signing Certificate	If you select **Enrollment via an RA**, select the CA's RA signing certificate from the drop-down list box. You must have the certificate already imported in the **Trusted CAs** screen. Click **Trusted CAs** to go to the **Trusted CAs** screen where you can view (and manage) the ZyXEL Device's list of certificates of trusted certification authorities.
RA Encryption Certificate	If you select **Enrollment via an RA**, select the CA's RA encryption certificate from the drop-down list box. You must have the certificate already imported in the **Trusted CAs** screen. Click **Trusted CAs** to go to the **Trusted CAs** screen where you can view (and manage) the ZyXEL Device's list of certificates of trusted certification authorities.
Request Authentication	When you select **Create a certification request and enroll for a certificate immediately online**, the certification authority may want you to include a reference number and key to identify you when you send a certification request. Fill in both the **Reference Number** and the **Key** fields if your certification authority uses CMP enrollment protocol. Just fill in the **Key** field if your certification authority uses the SCEP enrollment protocol.
Reference Number	Enter the reference number that the certification authority gave you. You can use up to 31 ASCII printable characters. Spaces are allowed.
Key	Type the key that the certification authority gave you. You can use up to 31 ASCII printable characters. Spaces are allowed.
Apply	Click **Apply** to begin certificate or certification request generation.
Cancel	Click **Cancel** to quit and return to the **My Certificates** screen.

After you click **Apply** in the **My Certificate Create** screen, you see a screen that tells you the ZyXEL Device is generating the self-signed certificate or certification request.

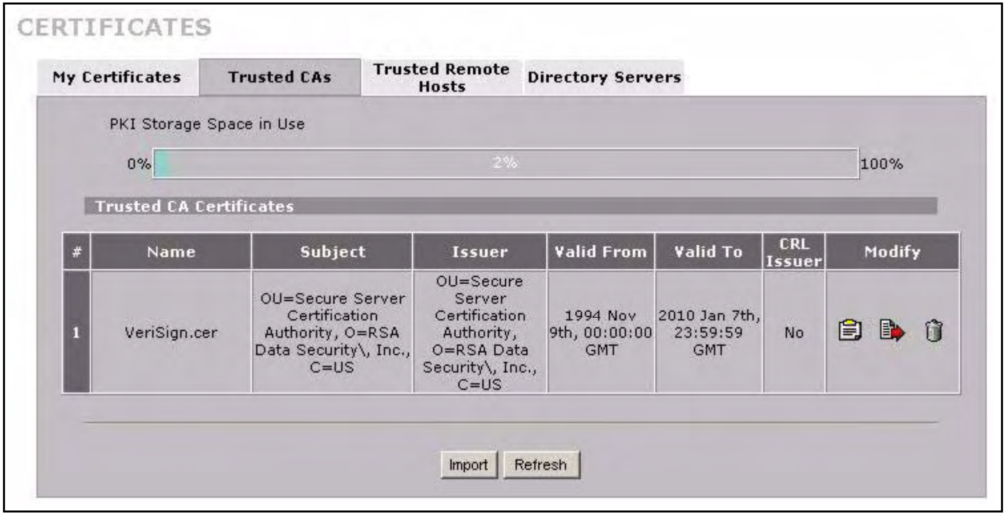
After the ZyXEL Device successfully enrolls a certificate or generates a certification request or a self-signed certificate, you see a screen with a **Return** button that takes you back to the **My Certificates** screen.

If you configured the **My Certificate Create** screen to have the ZyXEL Device enroll a certificate and the certificate enrollment is not successful, you see a screen with a **Return** button that takes you back to the **My Certificate Create** screen. Click **Return** and check your information in the **My Certificate Create** screen. Make sure that the certification authority information is correct and that your Internet connection is working properly if you want the ZyXEL Device to enroll a certificate online.

11.10 Trusted CAs

Click **SECURITY** > **CERTIFICATES** > **Trusted CAs** to open the **Trusted CAs** screen. This screen displays a summary list of certificates of the certification authorities that you have set the ZyXEL Device to accept as trusted. The ZyXEL Device accepts any valid certificate signed by a certification authority on this list as being trustworthy; thus you do not need to import any certificate that is signed by one of these certification authorities.

Figure 128 SECURITY > CERTIFICATES > Trusted CAs



PKI Storage Space in Use

0% 2% 100%

Trusted CA Certificates

#	Name	Subject	Issuer	Valid From	Valid To	CRL Issuer	Modify
1	VeriSign.cer	OU=Secure Server Certification Authority, O=RSA Data Security\, Inc., C=US	OU=Secure Server Certification Authority, O=RSA Data Security\, Inc., C=US	1994 Nov 9th, 00:00:00 GMT	2010 Jan 7th, 23:59:59 GMT	No	

The following table describes the labels in this screen.

Table 57 SECURITY > CERTIFICATES > Trusted CAs

LABEL	DESCRIPTION
PKI Storage Space in Use	This bar displays the percentage of the ZyXEL Device's PKI storage space that is currently in use. When the storage space is almost full, you should consider deleting expired or unnecessary certificates before adding more certificates.
#	This field displays the certificate index number. The certificates are listed in alphabetical order.
Name	This field displays the name used to identify this certificate.
Subject	This field displays identifying information about the certificate's owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). It is recommended that each certificate have unique subject information.
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as a common name, organizational unit or department, organization or company and country. With self-signed certificates, this is the same information as in the **Subject** field.
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.
CRL Issuer	This field displays **Yes** if the certification authority issues CRL (Certificate Revocation Lists) for the certificates that it has issued and you have selected the- **Check incoming certificates issued by this CA against a CRL** check box in the certificate's details screen to have the ZyXEL Device check the CRL before trusting any certificates issued by the certification authority. Otherwise the field displays **No**.

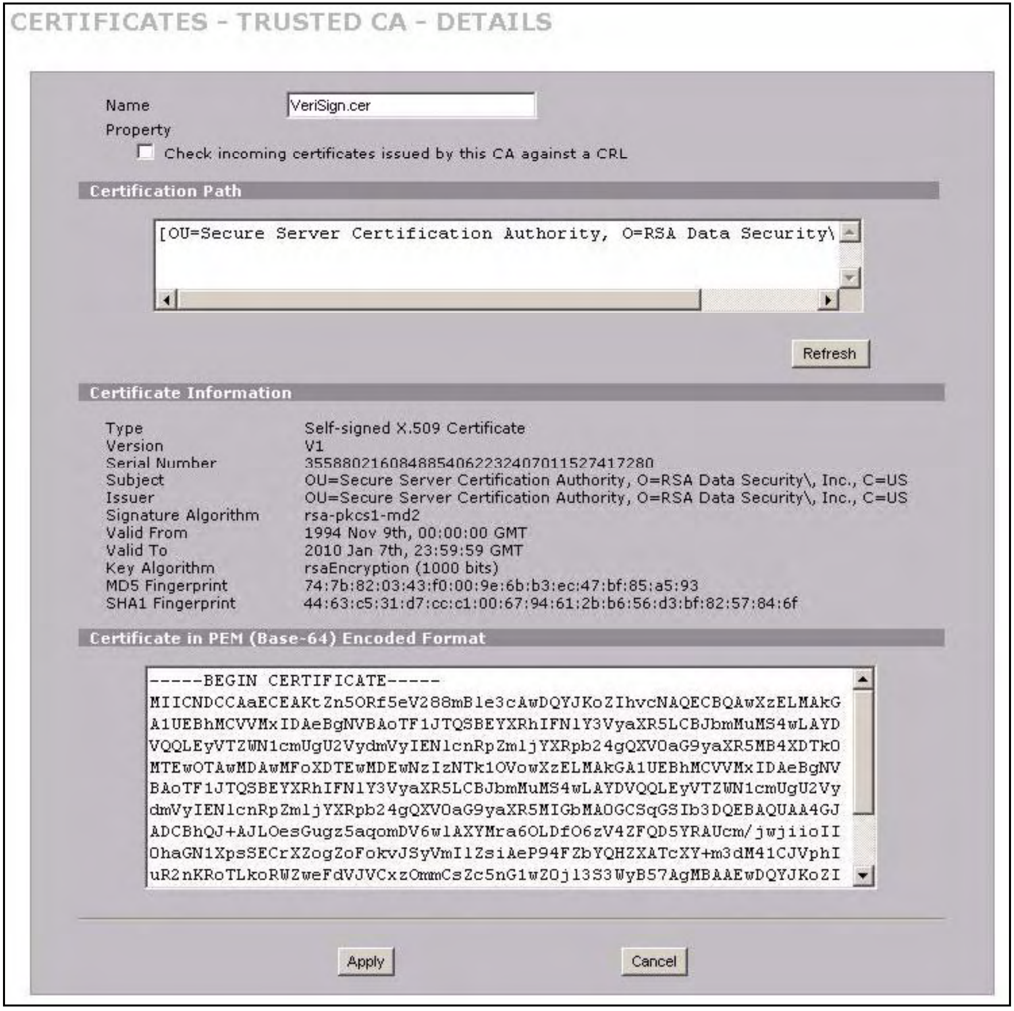
Table 57 SECURITY > CERTIFICATES > Trusted CAs (continued)

LABEL	DESCRIPTION
Modify	Click the details icon to open a screen with an in-depth list of information about the certificate. Use the export icon to save the certificate to a computer. Click the icon and then **Save** in the **File Download** screen. The **Save As** screen opens, browse to the location that you want to use and click **Save**. Click the delete icon to remove the certificate. A window displays asking you to confirm that you want to delete the certificates. Note that subsequent certificates move up by one when you take this action.
Import	Click **Import** to open a screen where you can save the certificate of a certification authority that you trust, from your computer to the ZyXEL Device.
Refresh	Click this button to display the current validity status of the certificates.

11.11 Trusted CA Details

Click **SECURITY** > **CERTIFICATES** > **Trusted CAs** to open the **Trusted CAs** screen. Click the details icon to open the **Trusted CA Details** screen. Use this screen to view in-depth information about the certification authority’s certificate, change the certificate’s name and set whether or not you want the ZyXEL Device to check a certification authority’s list of revoked certificates before trusting a certificate issued by the certification authority.

Figure 129 SECURITY > CERTIFICATES > Trusted CAs > Details



CERTIFICATES - TRUSTED CA - DETAILS

Name VeriSign.cer

Property

□ Check incoming certificates issued by this CA against a CRL

Certification Path

```
[OU=Secure Server Certification Authority, O=RSA Data Security\
```

Certificate Information

Type	Self-signed X.509 Certificate
Version	V1
Serial Number	3558802160848854062232407011527417280
Subject	OU=Secure Server Certification Authority, O=RSA Data Security\, Inc., C=US
Issuer	OU=Secure Server Certification Authority, O=RSA Data Security\, Inc., C=US
Signature Algorithm	rsa-pkcs1-md2
Valid From	1994 Nov 9th, 00:00:00 GMT
Valid To	2010 Jan 7th, 23:59:59 GMT
Key Algorithm	rsaEncryption (1000 bits)
MD5 Fingerprint	74:7b:82:03:43:f0:00:9e:6b:b3:ec:47:bf:85:a5:93
SHA1 Fingerprint	44:63:c5:31:d7:cc:c1:00:67:94:61:2b:b6:56:d3:bf:82:57:84:6f

Certificate in PEM (Base-64) Encoded Format

```
-----BEGIN CERTIFICATE-----
MIICNDCCAaECEAKtZn5ORf5eV288mBle3cAwDQYJKoZIhvcNAQECBQAwXzELMAkG
A1UEBhMCVVMxIDAeBgNVBAoTF1JTQSBEYXRhIFNlY3VyaXR5LCBJbmMuMS4wLAYD
VQQLEyVTZWN1cmUgU2VydmVyIENlcnRpZmljYXRpb24gQXV0aG9yaXR5MB4XDTk0
MTEwOTAwMDAwMFoXDTEwMDEwNzIzNTk1OVowXzELMAkGA1UEBhMCVVMxIDAeBgNV
BAoTF1JTQSBEYXRhIFNlY3VyaXR5LCBJbmMuMS4wLAYDVQQLEyVTZWN1cmUgU2Vy
dmVyIENlcnRpZmljYXRpb24gQXV0aG9yaXR5MIGbMA0GCSqGSIb3DQEBAQUAA4GJ
ADCBhQJ+AJLOesGugz5aqomDV6wlAXYMra6OLDfO6zV4ZFQD5YRAUcm/jwjiioII
0haGN1XpsSECrXZogZoFokvJSyVmIlZsiAeP94FZbYQHZXATcXY+m3dM41CJVphI
uR2nKRoTLkoRWZweFdVJVCxzOmmCsZc5nG1wZ0jl3S3WyB57AgMBAAEwDQYJKoZI
```

The following table describes the labels in this screen.

Table 58 SECURITY > CERTIFICATES > Trusted CAs > Details

LABEL	DESCRIPTION
Name	This field displays the identifying name of this certificate. If you want to change the name, type up to 31 characters to identify this key certificate. You may use any character (not including spaces).
Property Check incoming certificates issued by this CA against a CRL	Select this check box to have the ZyXEL Device check incoming certificates that are issued by this certification authority against a Certificate Revocation List (CRL). Clear this check box to have the ZyXEL Device not check incoming certificates that are issued by this certification authority against a Certificate Revocation List (CRL).

Table 58 SECURITY > CERTIFICATES > Trusted CAs > Details (continued)

LABEL	DESCRIPTION
Certification Path	Click the **Refresh** button to have this read-only text box display the end entity's certificate and a list of certification authority certificates that shows the hierarchy of certification authorities that validate the end entity's certificate. If the issuing certification authority is one that you have imported as a trusted certification authority, it may be the only certification authority in the list (along with the end entity's own certificate). The ZyXEL Device does not trust the end entity's certificate and displays "Not trusted" in this field if any certificate on the path has expired or been revoked.
Refresh	Click **Refresh** to display the certification path.
Certificate Information	These read-only fields display detailed information about the certificate.
Type	This field displays general information about the certificate. CA-signed means that a Certification Authority signed the certificate. Self-signed means that the certificate's owner signed the certificate (not a certification authority). X.509 means that this certificate was created and signed according to the ITU-T X.509 recommendation that defines the formats for public-key certificates.
Version	This field displays the X.509 version number.
Serial Number	This field displays the certificate's identification number given by the certification authority.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), Organizational Unit (OU), Organization (O) and Country (C).
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as Common Name, Organizational Unit, Organization and Country. With self-signed certificates, this is the same information as in the **Subject Name** field.
Signature Algorithm	This field displays the type of algorithm that was used to sign the certificate. Some certification authorities use rsa-pkcs1-sha1 (RSA public-private key encryption algorithm and the SHA1 hash algorithm). Other certification authorities may use rsa-pkcs1-md5 (RSA public-private key encryption algorithm and the MD5 hash algorithm).
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.
Key Algorithm	This field displays the type of algorithm that was used to generate the certificate's key pair (the ZyXEL Device uses RSA encryption) and the length of the key set in bits (1024 bits for example).
Subject Alternative Name	This field displays the certificate's owner's IP address (IP), domain name (DNS) or e-mail address (EMAIL).
Key Usage	This field displays for what functions the certificate's key can be used. For example, "DigitalSignature" means that the key can be used to sign certificates and "KeyEncipherment" means that the key can be used to encrypt text.
Basic Constraint	This field displays general information about the certificate. For example, Subject Type=CA means that this is a certification authority's certificate and "Path Length Constraint=1" means that there can only be one certification authority in the certificate's path.

Table 58 SECURITY > CERTIFICATES > Trusted CAs > Details (continued)

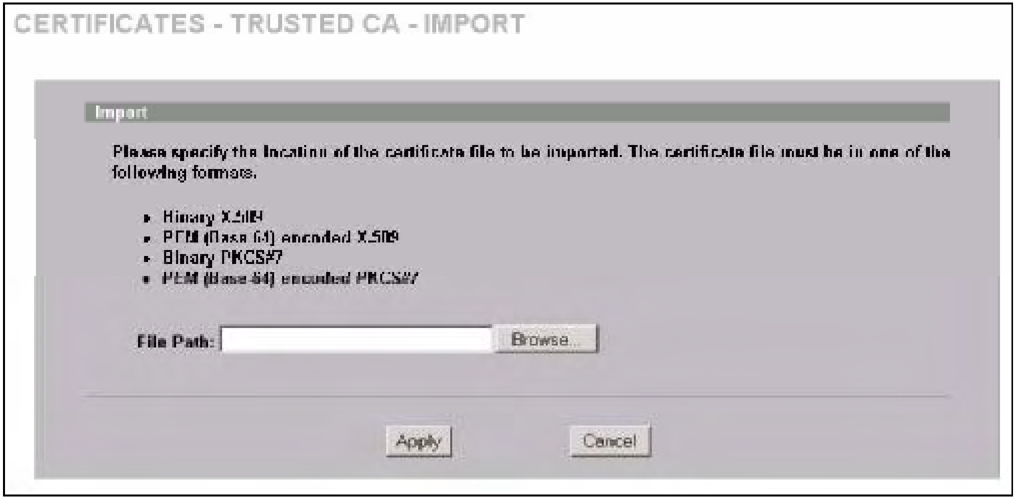
LABEL	DESCRIPTION
CRL Distribution Points	This field displays how many directory servers with Lists of revoked certificates the issuing certification authority of this certificate makes available. This field also displays the domain names or IP addresses of the servers.
MD5 Fingerprint	This is the certificate's message digest that the ZyXEL Device calculated using the MD5 algorithm. You can use this value to verify with the certification authority (over the phone for example) that this is actually their certificate.
SHA1 Fingerprint	This is the certificate's message digest that the ZyXEL Device calculated using the SHA1 algorithm. You can use this value to verify with the certification authority (over the phone for example) that this is actually their certificate.
Certificate in PEM (Base-64) Encoded Format	This read-only text box displays the certificate or certification request in Privacy Enhanced Mail (PEM) format. PEM uses 64 ASCII characters to convert the binary certificate into a printable form. You can copy and paste the certificate into an e-mail to send to friends or colleagues or you can copy and paste the certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example).
Apply	Click **Apply** to save your changes back to the ZyXEL Device. You can only change the name and/or set whether or not you want the ZyXEL Device to check the CRL that the certification authority issues before trusting a certificate issued by the certification authority.
Cancel	Click **Cancel** to quit and return to the **Trusted CAs** screen.

11.12 Trusted CA Import

Click **SECURITY** > **CERTIFICATES** > **Trusted CAs** to open the **Trusted CAs** screen and then click **Import** to open the **Trusted CA Import** screen. Follow the instructions in this screen to save a trusted certification authority's certificate from a computer to the ZyXEL Device. The ZyXEL Device trusts any valid certificate signed by any of the imported trusted CA certificates.

You must remove any spaces from the certificate's filename before you can import the certificate.

Figure 130 SECURITY > CERTIFICATES > Trusted CAs > Import



CERTIFICATES - TRUSTED CA - IMPORT

Import

Please specify the location of the certificate file to be imported. The certificate file must be in one of the following formats.

- Binary X.509
- PEM (Base-64) encoded X.509
- Binary PKCS#7
- PEM (Base-64) encoded PKCS#7

The following table describes the labels in this screen.

Table 59 SECURITY > CERTIFICATES > Trusted CAs Import

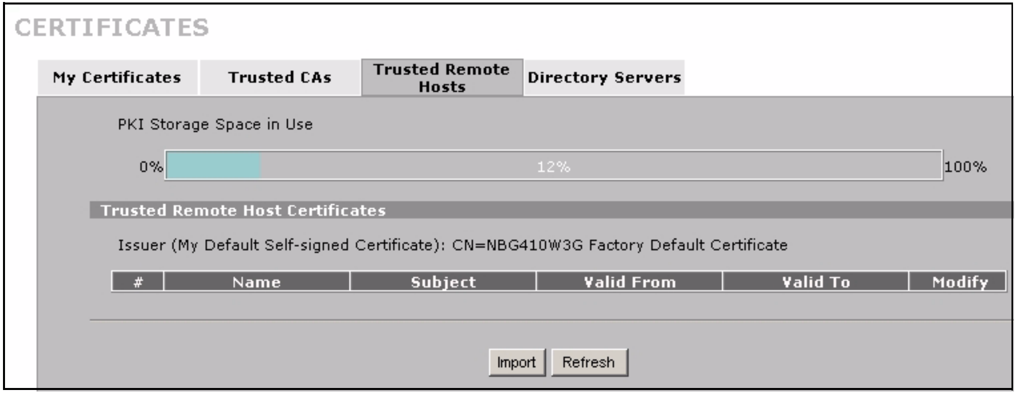
LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click **Browse** to find it.
Browse	Click **Browse** to find the certificate file you want to upload.
Apply	Click **Apply** to save the certificate on the ZyXEL Device.
Cancel	Click **Cancel** to quit and return to the **Trusted CAs** screen.

11.13 Trusted Remote Hosts

Click **SECURITY** > **CERTIFICATES** > **Trusted Remote Hosts** to open the **Trusted Remote Hosts** screen. This screen displays a list of the certificates of peers that you trust but which are not signed by one of the certification authorities on the **Trusted CAs** screen.

You do not need to add any certificate that is signed by one of the certification authorities on the **Trusted CAs** screen since the ZyXEL Device automatically accepts any valid certificate signed by a trusted certification authority as being trustworthy.

Figure 131 SECURITY > CERTIFICATES > Trusted Remote Hosts



Issuer (My Default Self-signed Certificate): CN=NBG410W3G Factory Default Certificate

The following table describes the labels in this screen.

Table 60 SECURITY > CERTIFICATES > Trusted Remote Hosts

LABEL	DESCRIPTION
PKI Storage Space in Use	This bar displays the percentage of the ZyXEL Device's PKI storage space that is currently in use. When the storage space is almost full, you should consider deleting expired or unnecessary certificates before adding more certificates.
Issuer (My Default Self-signed Certificate)	This field displays identifying information about the default self-signed certificate on the ZyXEL Device that the ZyXEL Device uses to sign the trusted remote host certificates.
#	This field displays the certificate index number. The certificates are listed in alphabetical order.
Name	This field displays the name used to identify this certificate.
Subject	This field displays identifying information about the certificate's owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). It is recommended that each certificate have unique subject information.
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.
Modify	Click the details icon to open a screen with an in-depth list of information about the certificate. Use the export icon to save the certificate to a computer. Click the icon and then **Save** in the **File Download** screen. The **Save As** screen opens, browse to the location that you want to use and click **Save**. Click the delete icon to remove the certificate. A window displays asking you to confirm that you want to delete the certificate. Note that subsequent certificates move up by one when you take this action.
Import	Click **Import** to open a screen where you can save the certificate of a remote host (which you trust) from your computer to the ZyXEL Device.
Refresh	Click this button to display the current validity status of the certificates.

11.14 Trusted Remote Hosts Import

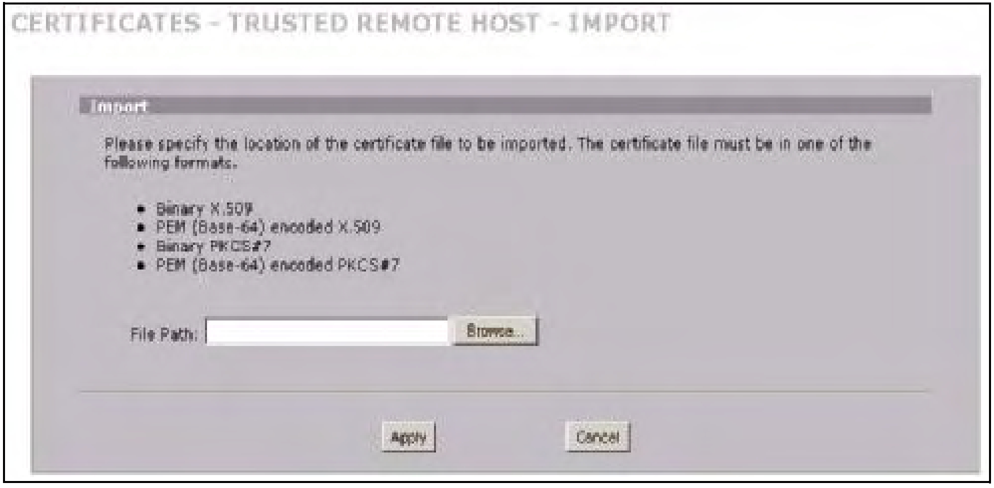
Click **SECURITY** > **CERTIFICATES** > **Trusted Remote Hosts** to open the **Trusted Remote Hosts** screen and then click **Import** to open the **Trusted Remote Host Import** screen.

You may have peers with certificates that you want to trust, but the certificates were not signed by one of the certification authorities on the **Trusted CAs** screen. Follow the instructions in this screen to save a peer's certificates from a computer to the ZyXEL Device.

You do not need to add any certificate that is signed by one of the certification authorities on the **Trusted CAs** screen since the ZyXEL Device automatically accepts any valid certificate signed by a trusted certification authority as being trustworthy.

The trusted remote host certificate must be a self-signed certificate; and you must remove any spaces from its filename before you can import it.

Figure 132 SECURITY > CERTIFICATES > Trusted Remote Hosts > Import



CERTIFICATES - TRUSTED REMOTE HOST - IMPORT

Import

Please specify the location of the certificate file to be imported. The certificate file must be in one of the following formats.

- Binary X.509
- PEM (Base-64) encoded X.509
- Binary PKCS#7
- PEM (Base-64) encoded PKCS#7

File Path: Browse...

The following table describes the labels in this screen.

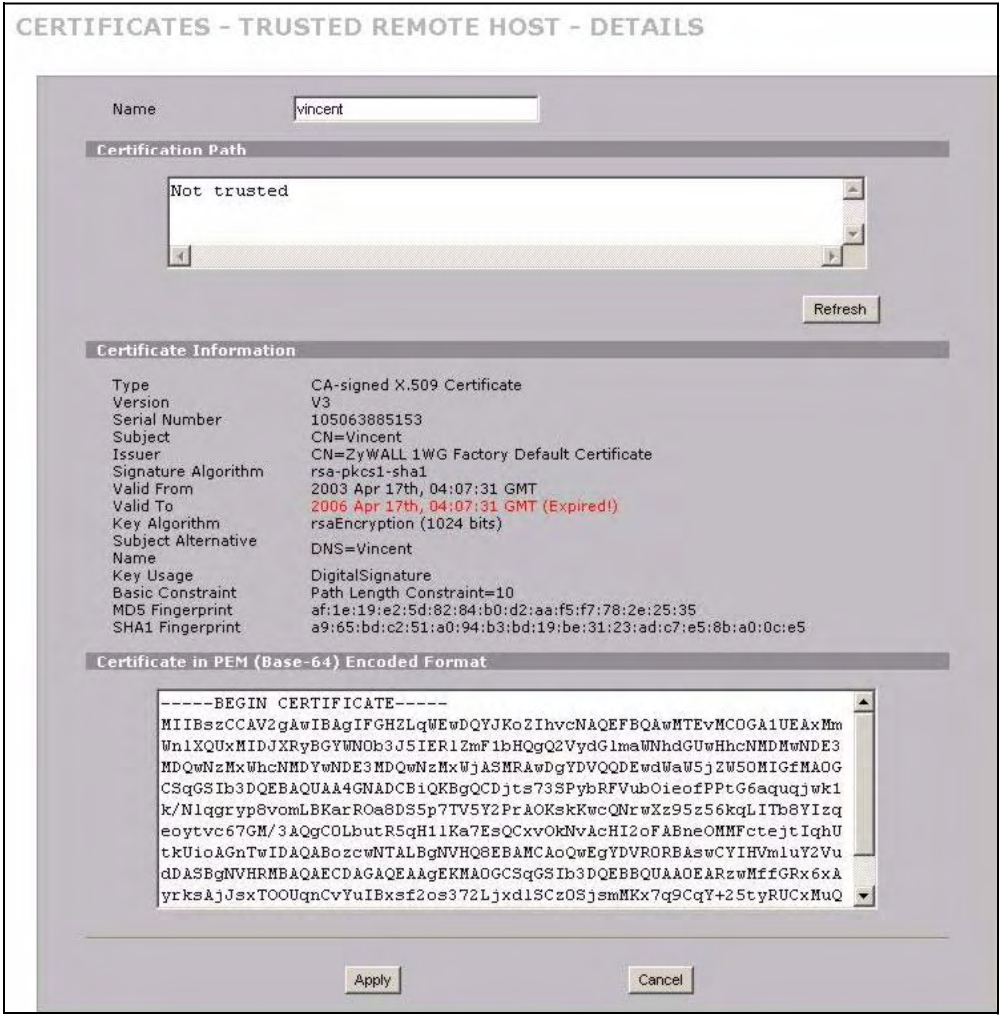
Table 61 SECURITY > CERTIFICATES > Trusted Remote Hosts > Import

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click **Browse** to find it.
Browse	Click **Browse** to find the certificate file you want to upload.
Apply	Click **Apply** to save the certificate on the ZyXEL Device.
Cancel	Click **Cancel** to quit and return to the **Trusted Remote Hosts** screen.

11.15 Trusted Remote Host Certificate Details

Click **SECURITY** > **CERTIFICATES** > **Trusted Remote Hosts** to open the **Trusted Remote Hosts** screen. Click the details icon to open the **Trusted Remote Host Details** screen. You can use this screen to view in-depth information about the trusted remote host's certificate and/or change the certificate's name.

Figure 133 SECURITY > CERTIFICATES > Trusted Remote Hosts > Details



CERTIFICATES - TRUSTED REMOTE HOST - DETAILS

Name: vincent

Certification Path

```
Not trusted
```

Certificate Information

Type	CA-signed X.509 Certificate
Version	V3
Serial Number	105063885153
Subject	CN=Vincent
Issuer	CN=ZyWALL 1WG Factory Default Certificate
Signature Algorithm	rsa-pkcs1-sha1
Valid From	2003 Apr 17th, 04:07:31 GMT
Valid To	2006 Apr 17th, 04:07:31 GMT (Expired!)
Key Algorithm	rsaEncryption (1024 bits)
Subject Alternative Name	DNS=Vincent
Key Usage	DigitalSignature
Basic Constraint	Path Length Constraint=10
MD5 Fingerprint	af:1e:19:e2:5d:82:84:b0:d2:aa:f5:f7:78:2e:25:35
SHA1 Fingerprint	a9:65:bd:c2:51:a0:94:b3:bd:19:be:31:23:ad:c7:e5:8b:a0:0c:e5

Certificate in PEM (Base-64) Encoded Format

```
-----BEGIN CERTIFICATE-----
MIIBszCCAV2gAwIBAgIFGHZLqWEwDQYJKoZIhvcNAQEFBQAwMTEvMC0GA1UEAxMm
WnlXQUxMIDJXRyBGYWN0b3J5IERlZmF1bHQgQ2VydGlmaWNhdGUwHhcNMDMwNDE3
MDQwNzMxWhcNMDYwNDE3MDQwNzMxWjASMRAwDgYDVQQDEwdWaW5jZW50MIGfMA0G
CSqGSIb3DQEBAQUAA4GNADCBiQKBgQCDjts73SPybRFVubOieofPPtG6aquqjwk1
k/NlqgryP8vomLBKarROa8DS5p7TV5Y2PrAOKskKwcQNrwXz95z56kqLITb8YIzq
eoytvc67GM/3AQgCOLbutR5qH1lKa7EsQCxvOkNvAcHI2oFABneOMMFctejtIqhU
tkUioAGnTwIDAQABozcwNTALBgNVHQ8EBAMCAoQwEgYDVR0RBAswCYIHVmluY2Vu
dDASBgNVHRMBAQAECDAGAQEAAgEKMA0GCSqGSIb3DQEBBQUAA0EARzwMffGRx6xA
yrksAjJsxTOOUqnCvYuIBxsf2os372LjxdlSCz0SjsmMKx7q9CqY+25tyRUCxMuQ
```

The following table describes the labels in this screen.

Table 62 SECURITY > CERTIFICATES > Trusted Remote Hosts > Details

LABEL	DESCRIPTION
Name	This field displays the identifying name of this certificate. If you want to change the name, type up to 31 characters to identify this key certificate. You may use any character (not including spaces).
Certification Path	Click the **Refresh** button to have this read-only text box display the end entity's own certificate and a list of certification authority certificates in the hierarchy of certification authorities that validate a certificate's issuing certification authority. For a trusted host, the list consists of the end entity's own certificate and the default self-signed certificate that the ZyXEL Device uses to sign remote host certificates.
Refresh	Click **Refresh** to display the certification path.
Certificate Information	These read-only fields display detailed information about the certificate.
Type	This field displays general information about the certificate. With trusted remote host certificates, this field always displays CA-signed. The ZyXEL Device is the Certification Authority that signed the certificate. X.509 means that this certificate was created and signed according to the ITU-T X.509 recommendation that defines the formats for public-key certificates.
Version	This field displays the X.509 version number.
Serial Number	This field displays the certificate's identification number given by the device that created the certificate.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), Organizational Unit (OU), Organization (O) and Country (C).
Issuer	This field displays identifying information about the default self-signed certificate on the ZyXEL Device that the ZyXEL Device uses to sign the trusted remote host certificates.
Signature Algorithm	This field displays the type of algorithm that the ZyXEL Device used to sign the certificate, which is rsa-pkcs1-sha1 (RSA public-private key encryption algorithm and the SHA1 hash algorithm).
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.
Key Algorithm	This field displays the type of algorithm that was used to generate the certificate's key pair (the ZyXEL Device uses RSA encryption) and the length of the key set in bits (1024 bits for example).
Subject Alternative Name	This field displays the certificate's owner's IP address (IP), domain name (DNS) or e-mail address (EMAIL).
Key Usage	This field displays for what functions the certificate's key can be used. For example, "DigitalSignature" means that the key can be used to sign certificates and "KeyEncipherment" means that the key can be used to encrypt text.
Basic Constraint	This field displays general information about the certificate. For example, Subject Type=CA means that this is a certification authority's certificate and "Path Length Constraint=1" means that there can only be one certification authority in the certificate's path.

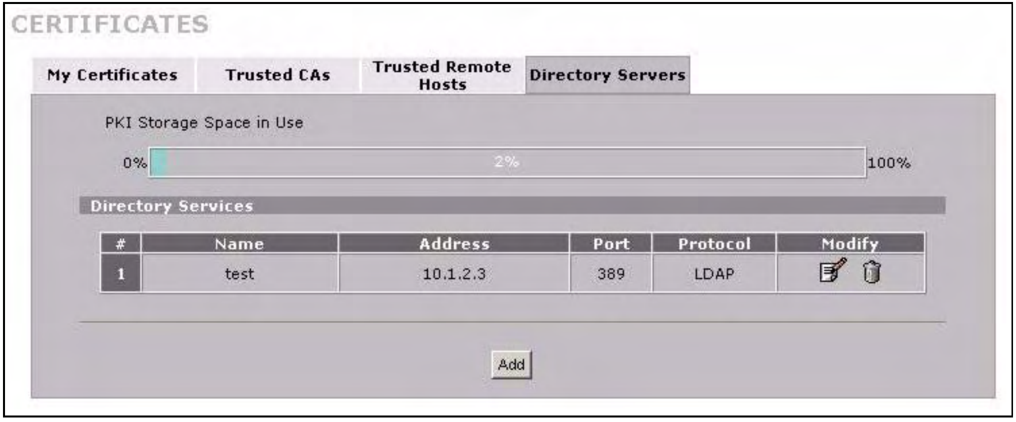
Table 62 SECURITY > CERTIFICATES > Trusted Remote Hosts > Details (continued)

LABEL	DESCRIPTION
MD5 Fingerprint	This is the certificate's message digest that the ZyXEL Device calculated using the MD5 algorithm. The ZyXEL Device uses one of its own self-signed certificates to sign the imported trusted remote host certificates. This changes the fingerprint value displayed here (so it does not match the original). See Section 11.3 on page 196 for how to verify a remote host's certificate before you import it into the ZyXEL Device.
SHA1 Fingerprint	This is the certificate's message digest that the ZyXEL Device calculated using the SHA1 algorithm. The ZyXEL Device uses one of its own self-signed certificates to sign the imported trusted remote host certificates. This changes the fingerprint value displayed here (so it does not match the original). See Section 11.3 on page 196 for how to verify a remote host's certificate before you import it into the ZyXEL Device.
Certificate in PEM (Base-64) Encoded Format	This read-only text box displays the certificate or certification request in Privacy Enhanced Mail (PEM) format. PEM uses 64 ASCII characters to convert the binary certificate into a printable form. You can copy and paste the certificate into an e-mail to send to friends or colleagues or you can copy and paste the certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example).
Apply	Click **Apply** to save your changes back to the ZyXEL Device. You can only change the name of the certificate.
Cancel	Click **Cancel** to quit configuring this screen and return to the **Trusted Remote Hosts** screen.

11.16 Directory Servers

Click **SECURITY** > **CERTIFICATES** > **Directory Servers** to open the **Directory Servers** screen. This screen displays a summary list of directory servers (that contain lists of valid and revoked certificates) that have been saved into the ZyXEL Device. If you decide to have the ZyXEL Device check incoming certificates against the issuing certification authority's list of revoked certificates, the ZyXEL Device first checks the server(s) listed in the **CRL Distribution Points** field of the incoming certificate. If the certificate does not list a server or the listed server is not available, the ZyXEL Device checks the servers listed here.

Figure 134 SECURITY > CERTIFICATES > Directory Servers



#	Name	Address	Port	Protocol	Modify
1	test	10.1.2.3	389	LDAP	

The following table describes the labels in this screen.

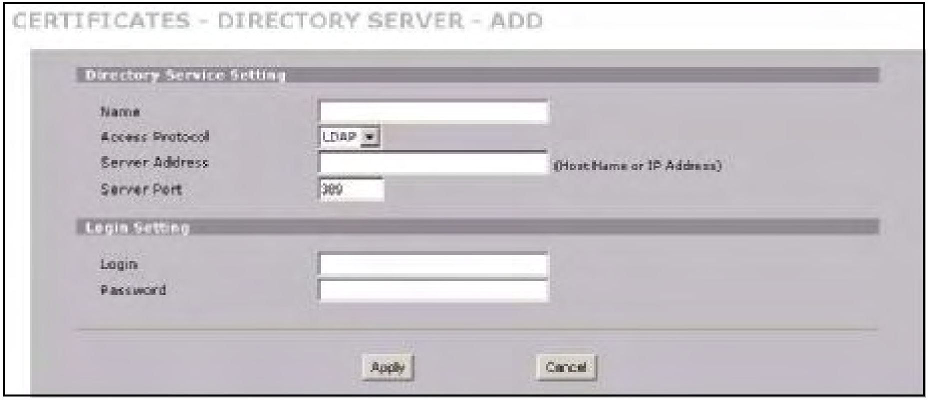
Table 63 SECURITY > CERTIFICATES > Directory Servers

LABEL	DESCRIPTION
PKI Storage Space in Use	This bar displays the percentage of the ZyXEL Device’s PKI storage space that is currently in use. When the storage space is almost full, you should consider deleting expired or unnecessary certificates before adding more certificates.
#	The index number of the directory server. The servers are listed in alphabetical order.
Name	This field displays the name used to identify this directory server.
Address	This field displays the IP address or domain name of the directory server.
Port	This field displays the port number that the directory server uses.
Protocol	This field displays the protocol that the directory server uses.
Modify	Click the details icon to open a screen where you can change the information about the directory server. Click the delete icon to remove the directory server entry. A window displays asking you to confirm that you want to delete the directory server. Note that subsequent certificates move up by one when you take this action.
Add	Click **Add** to open a screen where you can configure information about a directory server so that the ZyXEL Device can access it.

11.17 Directory Server Add or Edit

Click **SECURITY** > **CERTIFICATES** > **Directory Servers** to open the **Directory Servers** screen. Click **Add** (or the details icon) to open the **Directory Server Add** screen. Use this screen to configure information about a directory server that the ZyXEL Device can access.

Figure 135 SECURITY > CERTIFICATES > Directory Server > Add



CERTIFICATES - DIRECTORY SERVER - ADD

Directory Service Setting

Name

Access Protocol: LDAP

Server Address (Host Name or IP Address)

Server Port: 389

Login Setting

Login

Password

The following table describes the labels in this screen.

Table 64 SECURITY > CERTIFICATES > Directory Server > Add

LABEL	DESCRIPTION
Directory Service Setting	
Name	Type up to 31 ASCII characters (spaces are not permitted) to identify this directory server.

Table 64 SECURITY > CERTIFICATES > Directory Server > Add

LABEL	DESCRIPTION
Access Protocol	Use the drop-down list box to select the access protocol used by the directory server. **LDAP** (Lightweight Directory Access Protocol) is a protocol over TCP that specifies how clients access directories of certificates and lists of revoked certificates.[A]
Server Address	Type the IP address (in dotted decimal notation) or the domain name of the directory server.
Server Port	This field displays the default server port number of the protocol that you select in the **Access Protocol** field. You may change the server port number if needed, however you must use the same server port number that the directory server uses. 389 is the default server port number for LDAP.
Login Setting	
Login	The ZyXEL Device may need to authenticate itself in order to assess the directory server. Type the login name (up to 31 ASCII characters) from the entity maintaining the directory server (usually a certification authority).
Password	Type the password (up to 31 ASCII characters) from the entity maintaining the directory server (usually a certification authority).
Apply	Click **Apply** to save your changes back to the ZyXEL Device.
Cancel	Click **Cancel** to quit configuring this screen and return to the **Directory Servers** screen.

[A] At the time of writing, LDAP is the only choice of directory server access protocol.

PART V
Advanced

12

Network Address Translation (NAT)

This chapter discusses how to configure NAT on the ZyXEL Device.

12.1 NAT Overview

NAT (Network Address Translation - NAT, RFC 1631) is the translation of the IP address of a host in a packet. For example, the source address of an outgoing packet, used within one network is changed to a different IP address known within another network.

12.1.1 NAT Definitions

Inside/outside denotes where a host is located relative to the ZyXEL Device. For example, the computers of your subscribers are the inside hosts, while the web servers on the Internet are the outside hosts.

Global/local denotes the IP address of a host in a packet as the packet traverses a router. For example, the local address refers to the IP address of a host when the packet is in the local network, while the global address refers to the IP address of the host when the same packet is traveling in the WAN side.

Note that inside/outside refers to the location of a host, while global/local refers to the IP address of a host used in a packet. Thus, an inside local address (ILA) is the IP address of an inside host in a packet when the packet is still in the local network, while an inside global address (IGA) is the IP address of the same inside host when the packet is on the WAN side. The following table summarizes this information.

Table 65 NAT Definitions

TERM	DESCRIPTION
Inside	This refers to the host on the LAN.
Outside	This refers to the host on the WAN.
Local	This refers to the packet address (source or destination) as the packet travels on the LAN.
Global	This refers to the packet address (source or destination) as the packet travels on the WAN.

NAT never changes the IP address (either local or global) of an **outside** host.

12.1.2 What NAT Does

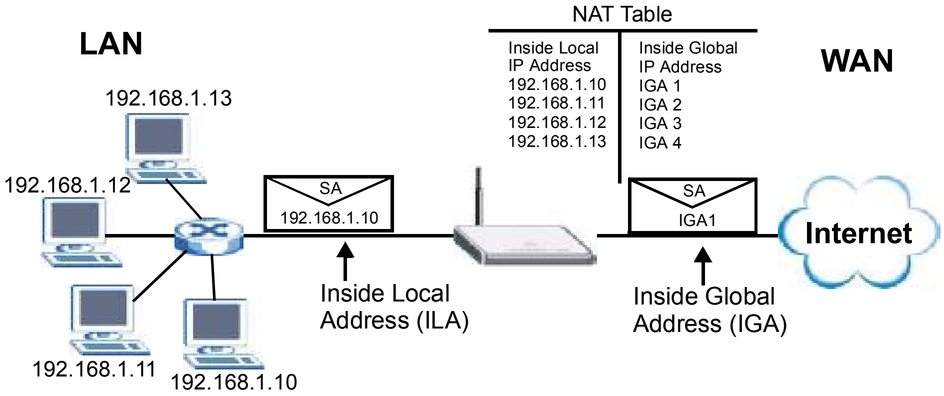
In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address) back to the inside local address before forwarding it to the original inside host. Note that the IP address (either local or global) of an outside host is never changed.

The global IP addresses for the inside hosts can be either static or dynamically assigned by the ISP. In addition, you can designate servers (for example a web server and a telnet server) on your local network and make them accessible to the outside world. Although you can make designated servers on the LAN accessible to the outside world, it is strongly recommended that you attach those servers to the DMZ port instead. If you do not define any servers (for Many-to-One and Many-to-Many Overload mapping), NAT offers the additional benefit of firewall protection. With no servers defined, your ZyXEL Device filters out all incoming inquiries, thus preventing intruders from probing your network. For more information on IP address translation, refer to RFC 1631, The IP Network Address Translator (NAT).

12.1.3 How NAT Works

Each packet has two addresses – a source address and a destination address. For outgoing packets, the ILA (Inside Local Address) is the source address on the LAN, and the IGA (Inside Global Address) is the source address on the WAN. For incoming packets, the ILA is the destination address on the LAN, and the IGA is the destination address on the WAN. NAT maps private (local) IP addresses to globally unique ones required for communication with hosts on other networks. It replaces the original IP source address (and TCP or UDP source port numbers for Many-to-One and Many-to-Many Overload NAT mapping) in each packet and then forwards it to the Internet. The ZyXEL Device keeps track of the original addresses and port numbers so incoming reply packets can have their original values restored. The following figure illustrates this.

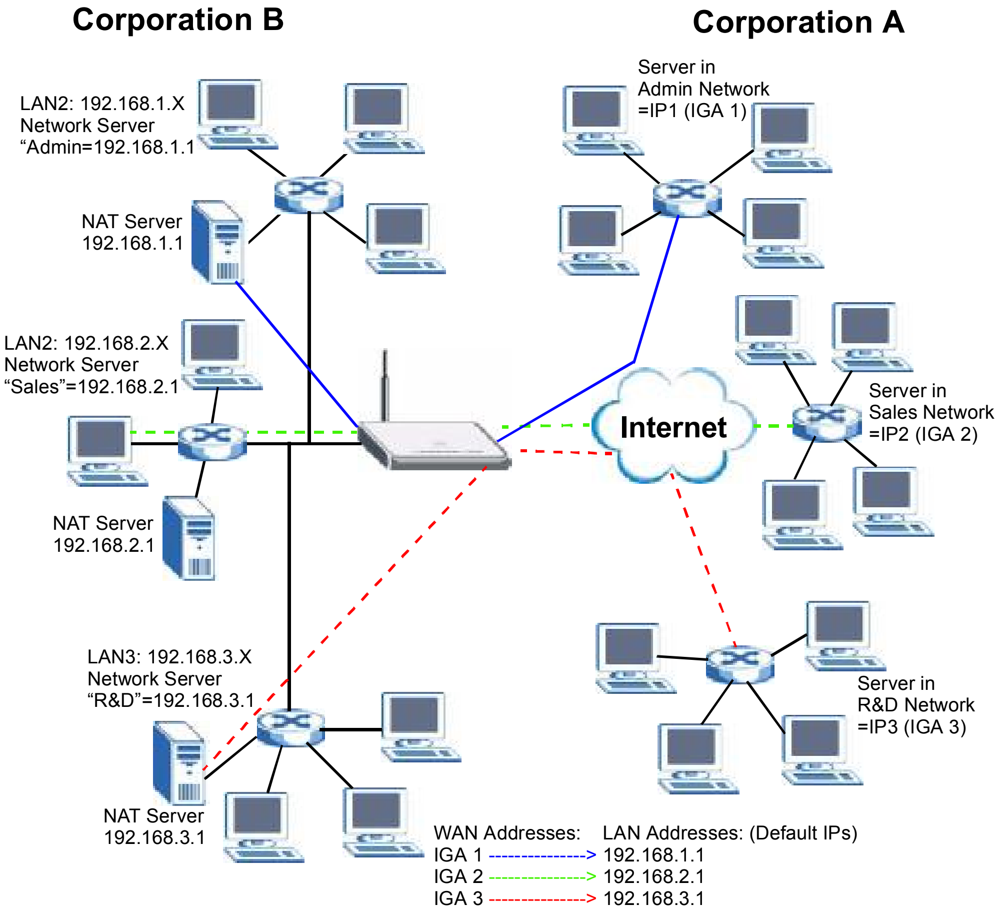
Figure 136 How NAT Works



12.1.4 NAT Application

The following figure illustrates a possible NAT application, where three inside LANs (logical LANs using IP Alias) behind the ZyXEL Device can communicate with three distinct WAN networks. More examples follow at the end of this chapter.

Figure 137 NAT Application With IP Alias



12.1.5 Port Restricted Cone NAT

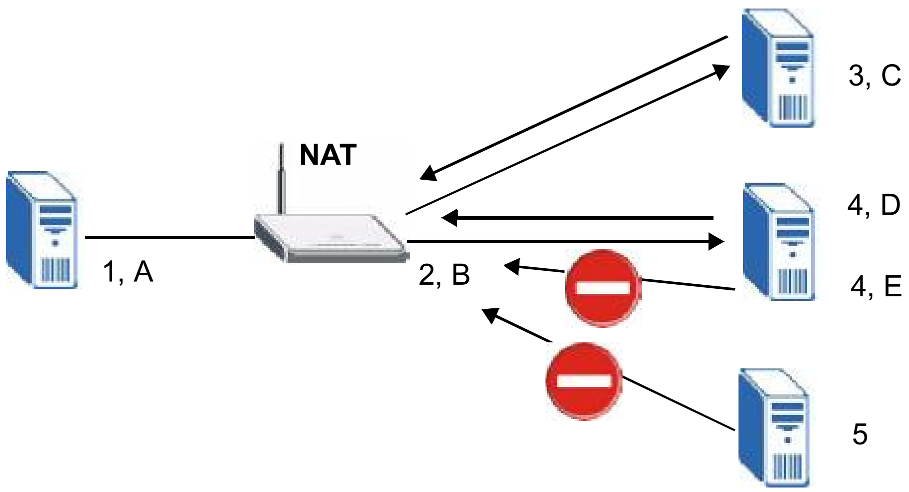
ZyXEL Device ZyNOS version 4.00 and later uses port restricted cone NAT. Port restricted cone NAT maps all outgoing packets from an internal IP address and port to a single IP address and port on the external network. In the following example, the ZyXEL Device maps the source address of all packets sent from internal IP address **1** and port **A** to IP address **2** and port **B** on the external network. A host on the external network (IP address **3** and Port **C** for example) can only send packets to the internal host if the internal host has already sent a packet to the external host's IP address and port.

A server with IP address **1** and port **A** sends packets to IP address **3**, port **C** and IP address **4**, port **D**. The ZyXEL Device changes the server's IP address to **2** and port to **B**.

Since **1**, **A** has already sent packets to **3**, **C** and **4**, **D,** they can send packets back to **2**, **B** and the ZyXEL Device will perform NAT on them and send them to the server at IP address **1**, port **A**.

Packets have not been sent from **1**, **A** to **4**, **E** or **5**, so they cannot send packets to **1**, **A**.

Figure 138 Port Restricted Cone NAT Example



12.1.6 NAT Mapping Types

NAT supports five types of IP/port mapping. They are:

- **One to One**: In One-to-One mode, the ZyXEL Device maps one local IP address to one global IP address.
- **Many to One**: In Many-to-One mode, the ZyXEL Device maps multiple local IP addresses to one global IP address. This is equivalent to SUA (i.e., PAT, port address translation), ZyXEL's Single User Account feature (the **SUA** option).
- **Many to Many Overload**: In Many-to-Many Overload mode, the ZyXEL Device maps the multiple local IP addresses to shared global IP addresses.
- **Many One to One**: In Many-One-to-One mode, the ZyXEL Device maps each local IP address to a unique global IP address.
- **Server**: This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world although, it is highly recommended that you use the DMZ port for these servers instead.

Port numbers do **not** change for **One-to-One** and **Many-One-to-One** NAT mapping types.

The following table summarizes the NAT mapping types.

Table 66 NAT Mapping Types

TYPE	IP MAPPING
One-to-One	ILA1 ←→ IGA1

Many-to-One (SUA/PAT)	ILA1 ←→ IGA1
	ILA2 ←→ IGA1
	…

Many-to-Many Overload	ILA ←→ IGA1
	ILA2 ←→ IGA2
	ILA3 ←→ IGA1
	ILA4 ←→ IGA2
	…

Many-One-to-One	ILA1 ←→ IGA1
	ILA2 ←→ IGA2
	ILA3 ←→ IGA3
	…

Server	Server 1 IP ←→ IGA1 Server 2 IP ←→ IGA1 Server 3 IP ←→ IGA1

12.2 Using NAT

You must create a firewall rule in addition to setting up SUA/NAT, to allow traffic from the WAN to be forwarded through the ZyXEL Device.

12.2.1 SUA (Single User Account) Versus NAT

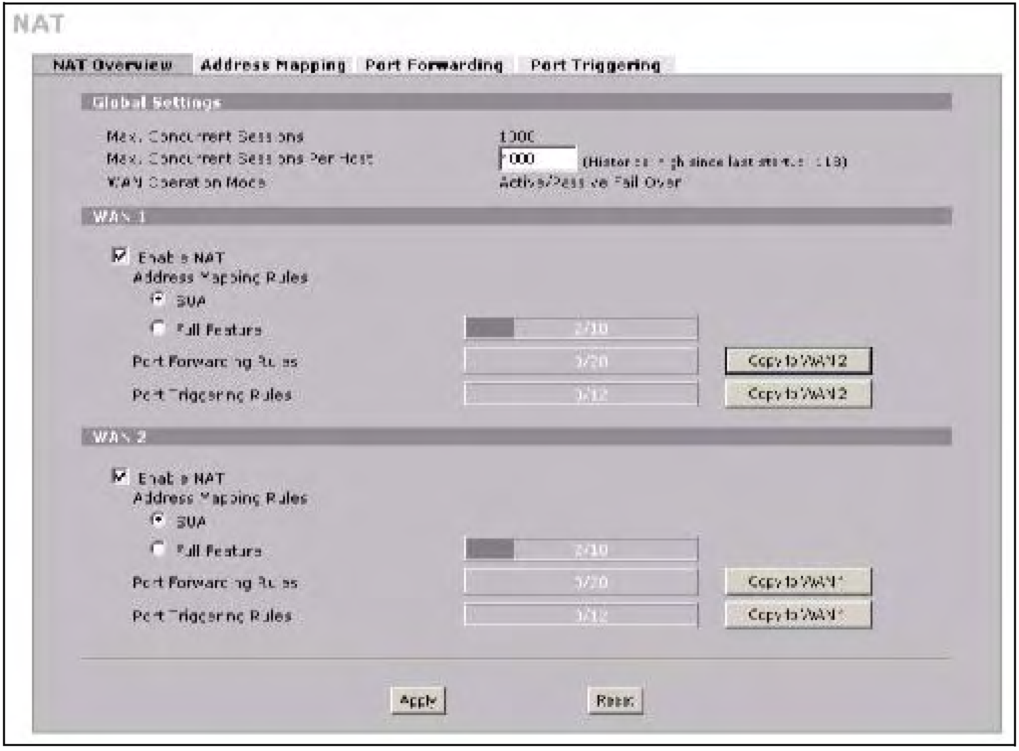
SUA (Single User Account) is a ZyNOS implementation of a subset of NAT that supports two types of mapping, **Many-to-One** and **Server**. The ZyXEL Device also supports **Full Feature** NAT to map multiple global IP addresses to multiple private LAN IP addresses of clients or servers using mapping types. Select either **SUA** or **Full Feature** in **NAT Overview**.

Selecting **SUA** means (latent) multiple WAN-to-LAN and WAN-to-DMZ address translation. That means that computers on your DMZ with public IP addresses will still have to undergo NAT mapping if you're using **SUA** NAT mapping. If this is not your intention, then select **Full Feature** NAT and don't configure NAT mapping rules to those computers with public IP addresses on the DMZ.

12.3 NAT Overview Screen

Click **ADVANCED > NAT** to open the **NAT Overview** screen.

Figure 139 ADVANCED > NAT > NAT Overview



NAT

NAT Overview | Address Mapping | Port Forwarding | Port Triggering

Global Settings

Max. Concurrent Sessions 1000

Max. Concurrent Sessions Per Host 1000 (History high since last start: 13)

WAN Operation Mode Active/Passive Fail Over

WAN 1

☑ Enable NAT

Address Mapping Rules

● SUA

○ Full Feature 2/10

Port Forwarding Rules 0/20 Copy to WAN 2

Port Triggering Rules 0/12 Copy to WAN 2

WAN 2

☑ Enable NAT

Address Mapping Rules

● SUA

○ Full Feature 2/10

Port Forwarding Rules 0/20 Copy to WAN 1

Port Triggering Rules 0/12 Copy to WAN 1

Apply Reset

The following table describes the labels in this screen.

Table 67 ADVANCED > NAT > NAT Overview

LABEL	DESCRIPTION
Global Settings	
Max. Concurrent Sessions	This read-only field displays the highest number of NAT sessions that the ZyXEL Device will permit at one time.
Max. Concurrent Sessions Per Host	Use this field to set the highest number of NAT sessions that the ZyXEL Device will permit a host to have at one time.
WAN Operation Mode	This read-only field displays the operation mode of the ZyXEL Device's WAN interfaces.
WAN 1, 2	
Enable NAT	Select this check box to turn on the NAT feature for the WAN interface. Clear this check box to turn off the NAT feature for the WAN interface.
Address Mapping Rules	Select **SUA** if you have just one public WAN IP address for your ZyXEL Device. This lets the ZyXEL Device use its permanent, pre-defined NAT address mapping rules. Select **Full Feature** if you have multiple public WAN IP addresses for your ZyXEL Device. This lets the ZyXEL Device use the address mapping rules that you configure. This is the equivalent of what used to be called full feature NAT or multi-NAT. The bar displays how many of the ZyXEL Device's possible address mapping rules are configured. The first number shows how many address mapping rules are configured on the ZyXEL Device. The second number shows the maximum number of address mapping rules that can be configured on the ZyXEL Device.

Table 67 ADVANCED > NAT > NAT Overview (continued)

LABEL	DESCRIPTION
Port Forwarding Rules	The bar displays how many of the ZyXEL Device's possible port forwarding rules are configured. The first number shows how many port forwarding rules are configured on the ZyXEL Device. The second number shows the maximum number of port forwarding rules that can be configured on the ZyXEL Device.
Port Triggering Rules	The bar displays how many of the ZyXEL Device's possible trigger port rules are configured. The first number shows how many trigger port rules are configured on the ZyXEL Device. The second number shows the maximum number of trigger port rules that can be configured on the ZyXEL Device.
Copy to WAN 2 (and Copy to WAN 1)	Click **Copy to WAN 2** (or **Copy to WAN 1**) to duplicate this WAN interface's NAT port forwarding or trigger port rules on the other WAN interface. Note: Using the copy button overwrites the other WAN interface's existing rules. The copy button is best suited for initial NAT configuration where you have configured NAT port forwarding or trigger port rules for one interface and want to use similar rules for the other WAN interface. You can use the other NAT screens to edit the NAT rules after you copy them from one WAN interface to the other.
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to begin configuring this screen afresh.

12.4 NAT Address Mapping

Click **ADVANCED** > **NAT** > **Address Mapping** to open the following screen.

12.4.1 What NAT Does

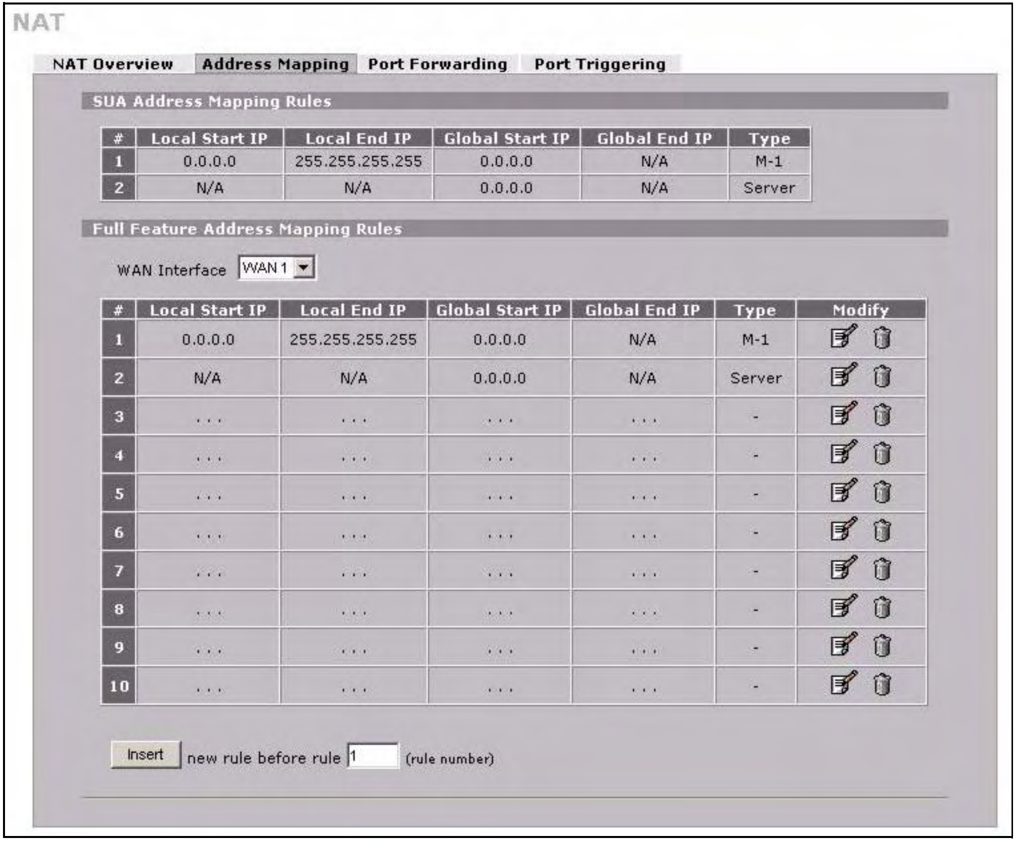
In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address) back to the inside local address before forwarding it to the original inside host. Note that the IP address (either local or global) of an outside host is never changed.

See Section 12.1 on page 225 for more on NAT.

Use this screen to change your ZyXEL Device’s address mapping settings.

Ordering your rules is important because the ZyXEL Device applies the rules in the order that you specify. When a rule matches the current packet, the ZyXEL Device takes the corresponding action and the remaining rules are ignored. If there are any empty rules before your new configured rule, your configured rule will be pushed up by that number of empty rules. For example, if you have already configured rules 1 to 6 in your current set and now you configure rule number 9. In the set summary screen, the new rule will be rule 7, not 9. Now if you delete rule 4, rules 5 to 7 will be pushed up by 1 rule, so old rules 5, 6 and 7 become new rules 4, 5 and 6.

Figure 140 ADVANCED > NAT > Address Mapping



SUA Address Mapping Rules

#	Local Start IP	Local End IP	Global Start IP	Global End IP	Type
1	0.0.0.0	255.255.255.255	0.0.0.0	N/A	M-1
2	N/A	N/A	0.0.0.0	N/A	Server

Full Feature Address Mapping Rules

WAN Interface: WAN 1

#	Local Start IP	Local End IP	Global Start IP	Global End IP	Type	Modify
1	0.0.0.0	255.255.255.255	0.0.0.0	N/A	M-1	✎ 🗑
2	N/A	N/A	0.0.0.0	N/A	Server	✎ 🗑
3	...	...	...	...	-	✎ 🗑
4	...	...	...	...	-	✎ 🗑
5	...	...	...	...	-	✎ 🗑
6	...	...	...	...	-	✎ 🗑
7	...	...	...	...	-	✎ 🗑
8	...	...	...	...	-	✎ 🗑
9	...	...	...	...	-	✎ 🗑
10	...	...	...	...	-	✎ 🗑

Insert new rule before rule 1 (rule number)

The following table describes the labels in this screen.

Table 68 ADVANCED > NAT > Address Mapping

LABEL	DESCRIPTION
SUA Address Mapping Rules	This read-only table displays the default address mapping rules.
Full Feature Address Mapping Rules	
WAN Interface	Select the WAN interface for which you want to view or configure address mapping rules.
#	This is the rule index number.
Local Start IP	This refers to the Inside Local Address (ILA), which is the starting local IP address. If the rule is for all local IP addresses, then this field displays 0.0.0.0 as the **Local Start IP** address. Local IP addresses are **N/A** for **Server** port mapping.
Local End IP	This is the end Inside Local Address (ILA). If the rule is for all local IP addresses, then this field displays 255.255.255.255 as the **Local End IP** address. This field is **N/A** for **One-to-One** and **Server** mapping types.
Global Start IP	This refers to the Inside Global IP Address (IGA), that is the starting global IP address. 0.0.0.0 is for a dynamic IP address from your ISP with **Many-to-One** and **Server** mapping types.

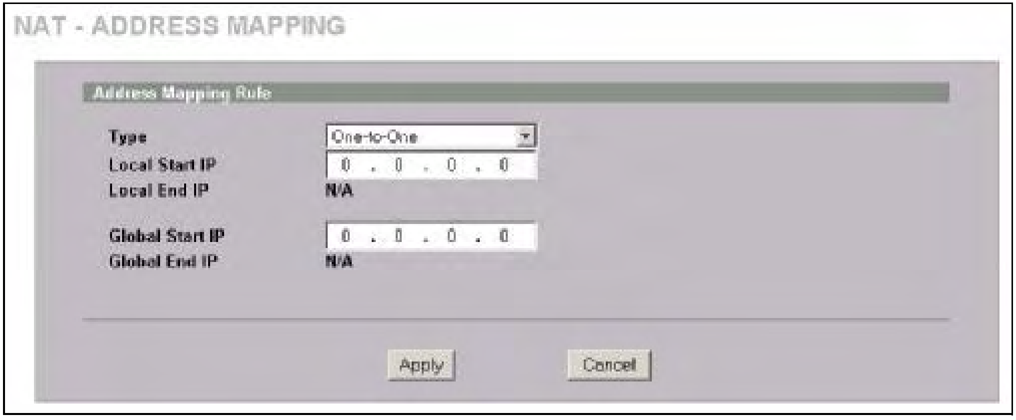
Table 68 ADVANCED > NAT > Address Mapping (continued)

LABEL	DESCRIPTION
Global End IP	This is the ending Inside Global Address (IGA). This field is **N/A** for **One-to-One**, **Many-to-One** and **Server** mapping types.
Type	1. **One-to-One** mode maps one local IP address to one global IP address. Note that port numbers do not change for the One-to-One NAT mapping type. 2. **Many-to-One** mode maps multiple local IP addresses to one global IP address. This is equivalent to SUA (i.e., PAT, port address translation), ZyXEL's Single User Account feature that previous ZyXEL routers supported only. 3. **Many-to-Many Overload** mode maps multiple local IP addresses to shared global IP addresses. 4. **Many One-to-One** mode maps each local IP address to unique global IP addresses. 5. **Server** allows you to specify inside servers of different services behind the NAT to be accessible to the outside world.
Modify	Click the edit icon to go to the screen where you can edit the address mapping rule. Click the delete icon to delete an existing address mapping rule. A window display asking you to confirm that you want to delete the address mapping rule. Note that subsequent address mapping rules move up by one when you take this action.
Insert	Click **Insert** to insert a new mapping rule before an existing one.

12.4.2 NAT Address Mapping Edit

Click the edit icon to display the **NAT Address Mapping Edit** screen. Use this screen to edit an address mapping rule. See Section 12.1 on page 225 for information on NAT and address mapping.

Figure 141 ADVANCED > NAT > Address Mapping > Edit



NAT - ADDRESS MAPPING

Address Mapping Rule

Type: One-to-One

Local Start IP: 0 . 0 . 0 . 0

Local End IP: N/A

Global Start IP: 0 . 0 . 0 . 0

Global End IP: N/A

The following table describes the labels in this screen.

Table 69 ADVANCED > NAT > Address Mapping > Edit

LABEL	DESCRIPTION
Type	Choose the port mapping type from one of the following. 1. **One-to-One**: One-to-One mode maps one local IP address to one global IP address. Note that port numbers do not change for One-to-One NAT mapping type. 2. **Many-to-One**: Many-to-One mode maps multiple local IP addresses to one global IP address. This is equivalent to SUA (i.e., PAT, port address translation), ZyXEL's Single User Account feature. 3. **Many-to-Many Overload**: Many-to-Many Overload mode maps multiple local IP addresses to shared global IP addresses. 4. **Many One-to-One**: Many One-to-One mode maps each local IP address to unique global IP addresses. 5. **Server**: This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world.
Local Start IP	This is the starting Inside Local IP Address (ILA). Local IP addresses are **N/A** for **Server** port mapping.
Local End IP	This is the end Inside Local IP Address (ILA). If your rule is for all local IP addresses, then enter 0.0.0.0 as the **Local Start IP** address and 255.255.255.255 as the **Local End IP** address. This field is **N/A** for **One-to-One** and **Server** mapping types.
Global Start IP	This is the starting Inside Global IP Address (IGA). Enter **0.0.0.0** here if you have a dynamic IP address from your ISP.
Global End IP	This is the ending Inside Global IP Address (IGA). This field is **N/A** for **One-to-One**, **Many-to-One** and **Server** mapping types.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

12.5 Port Forwarding

A port forwarding set is a list of inside (behind NAT on the LAN) servers, for example, web or FTP, that you can make visible to the outside world even though NAT makes your whole inside network appear as a single computer to the outside world.

You may enter a single port number or a range of port numbers to be forwarded, and the local IP address of the desired server. The port number identifies a service; for example, web service is on port 80 and FTP on port 21. In some cases, such as for unknown services or where one server can support more than one service (for example both FTP and web service), it might be better to specify a range of port numbers. You can allocate a server IP address that corresponds to a port or a range of ports.

Many residential broadband ISP accounts do not allow you to run any server processes (such as a Web or FTP server) from your location. Your ISP may periodically check for servers and may suspend your account if it discovers any active services at your location. If you are unsure, refer to your ISP.

12.5.1 Default Server IP Address

In addition to the servers for specified services, NAT supports a default server IP address. A default server receives packets from ports that are not specified in this screen.

If you do not assign a **Default Server** IP address, the ZyXEL Device discards all packets received for ports that are not specified here or in the remote management setup.

12.5.2 Port Forwarding: Services and Port Numbers

The ZyXEL Device provides the additional safety of the DMZ ports for connecting your publicly accessible servers. This makes the LAN more secure by physically separating it from your public servers.

Use the **Port Forwarding** screen to forward incoming service requests to the server(s) on your local network.

The most often used port numbers are shown in the following table. Please refer to RFC 1700 for further information about port numbers.

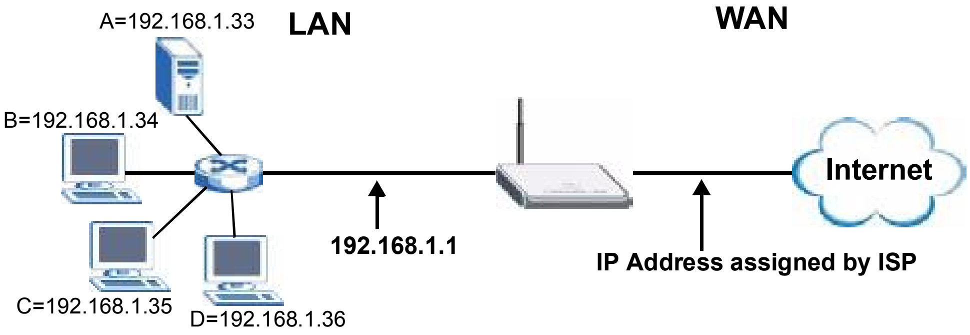
Table 70 Services and Port Numbers

SERVICES	PORT NUMBER
ECHO	7
FTP (File Transfer Protocol)	21
SMTP (Simple Mail Transfer Protocol)	25
DNS (Domain Name System)	53
Finger	79
HTTP (Hyper Text Transfer protocol or WWW, Web)	80
POP3 (Post Office Protocol)	110
NNTP (Network News Transport Protocol)	119
SNMP (Simple Network Management Protocol)	161
SNMP trap	162
PPTP (Point-to-Point Tunneling Protocol)	1723

12.5.3 Configuring Servers Behind Port Forwarding (Example)

Let's say you want to assign ports 21-25 to one FTP, Telnet and SMTP server (**A** in the example), port 80 to another (**B** in the example) and assign a default server IP address of 192.168.1.35 to a third (**C** in the example). You assign the LAN IP addresses and the ISP assigns the WAN IP address. The NAT network appears as a single host on the Internet.

Figure 142 Multiple Servers Behind NAT Example



12.5.4 NAT and Multiple WAN

The ZyXEL Device has two WAN interfaces. You can configure port forwarding and trigger port rule sets for the first WAN interface and separate sets of rules for the second WAN interface.

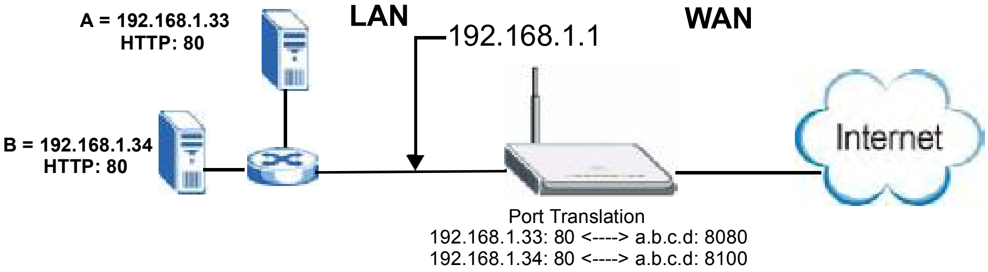
12.5.5 Port Translation

The ZyXEL Device can translate the destination port number or a range of port numbers of packets coming from the WAN to another destination port number or range of port numbers on the local network. When you use port forwarding without port translation, a single server on the local network can use a specific port number and be accessible to the outside world through a single WAN IP address. When you use port translation with port forwarding, multiple servers on the local network can use the same port number and still be accessible to the outside world through a single WAN IP address.

The following example has two web servers on a LAN. Server **A** uses IP address 192.168.1.33 and server **B** uses 192.168.1.34. Both servers use port 80. The letters a.b.c.d represent the WAN port's IP address. The ZyXEL Device translates port 8080 of traffic received on the WAN port (IP address a.b.c.d) to port 80 and sends it to server **A** (IP address 192.168.1.33). The ZyXEL Device also translates port 8100 of traffic received on the WAN port (also IP address a.b.c.d) to port 80, but sends it to server **B** (IP address 192.168.1.34).

In this example, anyone wanting to access server A from the Internet must use port 8080. Anyone wanting to access server B from the Internet must use port 8100.

Figure 143 Port Translation Example



12.6 Port Forwarding Screen

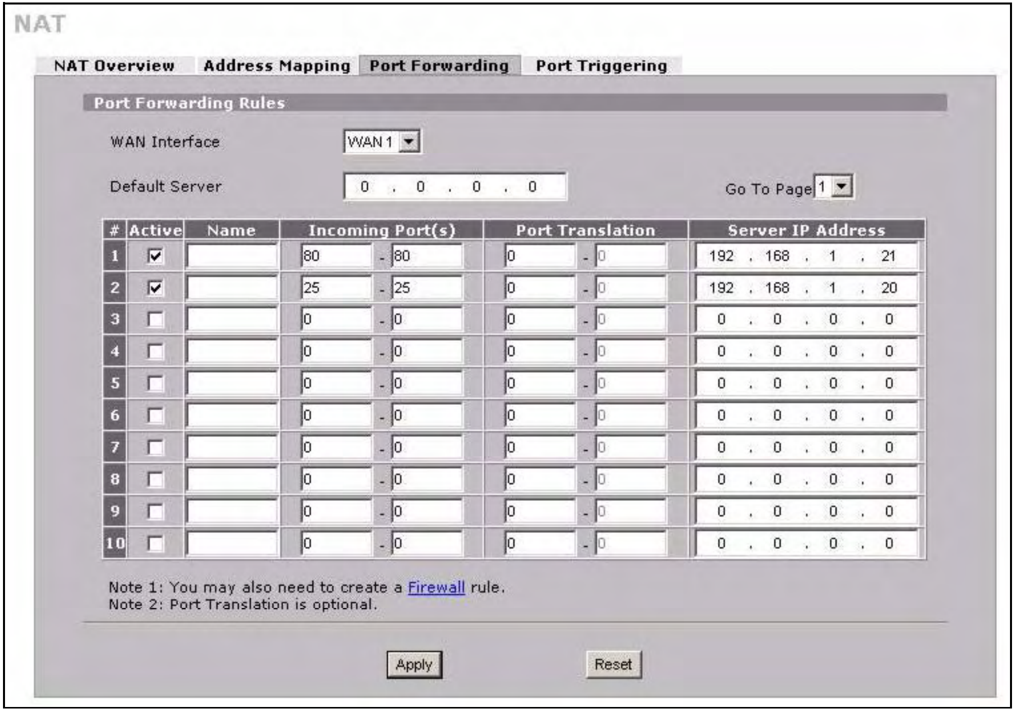
Click **ADVANCED** > **NAT** > **Port Forwarding** to open the **Port Forwarding** screen.

If you do not assign a **Default Server** IP address, the ZyXEL Device discards all packets received for ports that are not specified here or in the remote management setup.

Refer to Figure 70 on page 236 for port numbers commonly used for particular services.

The last port forwarding rule is reserved for Roadrunner services. The rule is activated only when you set the **WAN Encapsulation** to **Ethernet** and the **Service Type** to something other than **Standard**.

Figure 144 ADVANCED > NAT > Port Forwarding



Port Forwarding Rules

WAN Interface: WAN 1

Default Server: 0 . 0 . 0 . 0

Go To Page: 1

#	Active	Name	Incoming Port(s)		Port Translation		Server IP Address
1	☑		80	80	0	0	192 . 168 . 1 . 21
2	☑		25	25	0	0	192 . 168 . 1 . 20
3	□		0	0	0	0	0 . 0 . 0 . 0
4	□		0	0	0	0	0 . 0 . 0 . 0
5	□		0	0	0	0	0 . 0 . 0 . 0
6	□		0	0	0	0	0 . 0 . 0 . 0
7	□		0	0	0	0	0 . 0 . 0 . 0
8	□		0	0	0	0	0 . 0 . 0 . 0
9	□		0	0	0	0	0 . 0 . 0 . 0
10	□		0	0	0	0	0 . 0 . 0 . 0

Note 1: You may also need to create a Firewall rule.
Note 2: Port Translation is optional.

The following table describes the labels in this screen.

Table 71 ADVANCED > NAT > Port Forwarding

LABEL	DESCRIPTION
WAN Interface	Select the WAN interface for which you want to view or configure address mapping rules.
Default Server	In addition to the servers for specified services, NAT supports a default server. A default server receives packets from ports that are not specified in this screen. If you do not assign a **Default Server** IP address, the ZyXEL Device discards all packets received for ports that are not specified here or in the remote management setup.
Go To Page	Choose a page from the drop-down list box to display the corresponding summary page of the port forwarding servers.
#	This is the number of an individual port forwarding server entry.
Active	Select this check box to enable the port forwarding server entry. Clear this check box to disallow forwarding of these ports to an inside server without having to delete the entry.
Name	Enter a name to identify this port-forwarding rule.
Incoming Port(s)	Enter a port number here. To forward only one port, enter it again in the second field. To specify a range of ports, enter the last port to be forwarded in the second field.
Port Translation	Enter the port number here to which you want the ZyXEL Device to translate the incoming port. For a range of ports, you only need to enter the first number of the range to which you want the incoming ports translated, the ZyXEL Device automatically calculates the last port of the translated port range.
Server IP Address	Enter the inside IP address of the server here.
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to begin configuring this screen afresh.

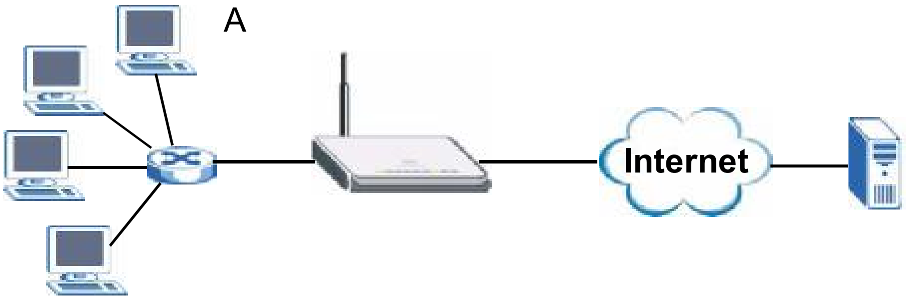
12.7 Port Triggering

Some services use a dedicated range of ports on the client side and a dedicated range of ports on the server side. With regular port forwarding you set a forwarding port in NAT to forward a service (coming in from the server on the WAN) to the IP address of a computer on the client side (LAN). The problem is that port forwarding only forwards a service to a single LAN IP address. In order to use the same service on a different LAN computer, you have to manually replace the LAN computer's IP address in the forwarding port with another LAN computer's IP address.

Trigger port forwarding solves this problem by allowing computers on the LAN to dynamically take turns using the service. The ZyXEL Device records the IP address of a LAN computer that sends traffic to the WAN to request a service with a specific port number and protocol (a "trigger" port). When the ZyXEL Device's WAN port receives a response with a specific port number and protocol ("incoming" port), the ZyXEL Device forwards the traffic to the LAN IP address of the computer that sent the request. After that computer’s connection for that service closes, another computer on the LAN can use the service in the same manner. This way you do not need to configure a new IP address each time you want a different LAN computer to use the application.

For example:

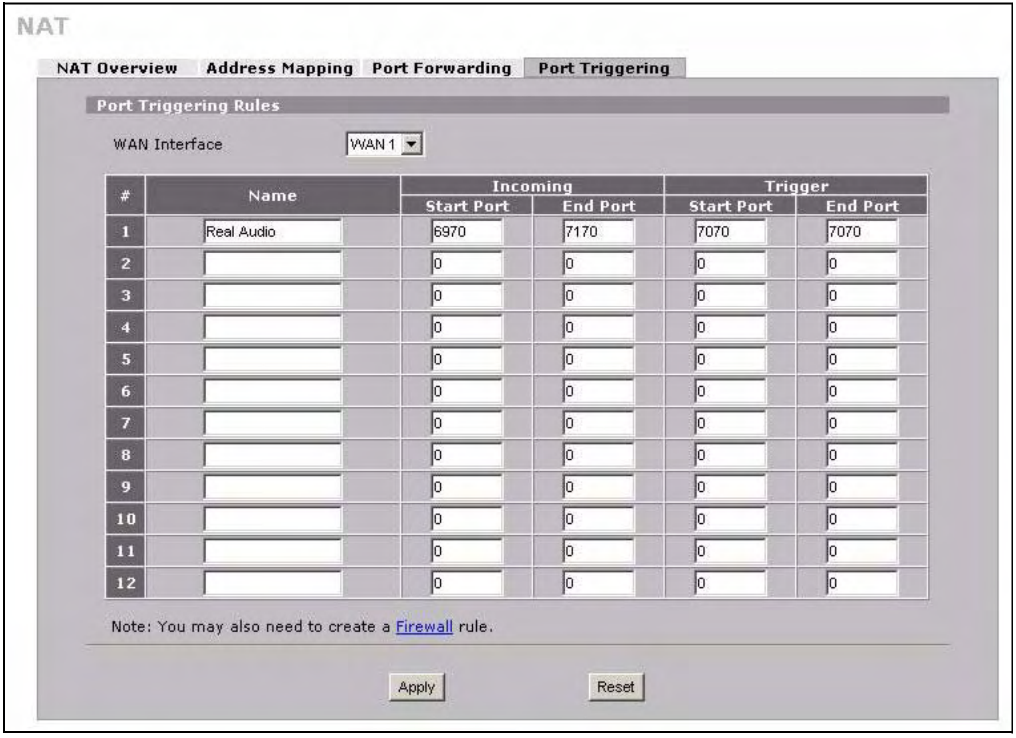
Figure 145 Trigger Port Forwarding Process: Example



1 Jane (A) requests a file from the Real Audio server (port 7070).
2 Port 7070 is a “trigger” port and causes the ZyXEL Device to record Jane’s computer IP address. The ZyXEL Device associates Jane's computer IP address with the "incoming" port range of 6970-7170.
3 The Real Audio server responds using a port number ranging between 6970-7170.
4 The ZyXEL Device forwards the traffic to Jane’s computer IP address.
5 Only Jane can connect to the Real Audio server until the connection is closed or times out. The ZyXEL Device times out in three minutes with UDP (User Datagram Protocol) or two hours with TCP/IP (Transfer Control Protocol/Internet Protocol).

Click **ADVANCED** > **NAT** > **Port Triggering** to open the following screen. Use this screen to change your ZyXEL Device’s trigger port settings.

Figure 146 ADVANCED > NAT > Port Triggering



Port Triggering Rules

WAN Interface: WAN 1

#	Name	Incoming		Trigger	
		Start Port	End Port	Start Port	End Port
1	Real Audio	6970	7170	7070	7070
2		0	0	0	0
3		0	0	0	0
4		0	0	0	0
5		0	0	0	0
6		0	0	0	0
7		0	0	0	0
8		0	0	0	0
9		0	0	0	0
10		0	0	0	0
11		0	0	0	0
12		0	0	0	0

Note: You may also need to create a Firewall rule.

The following table describes the labels in this screen.

Table 72 ADVANCED > NAT > Port Triggering

LABEL	DESCRIPTION
WAN Interface	Select the WAN interface for which you want to view or configure address mapping rules.
#	This is the rule index number (read-only).
Name	Type a unique name (up to 15 characters) for identification purposes. All characters are permitted - including spaces.
Incoming	Incoming is a port (or a range of ports) that a server on the WAN uses when it sends out a particular service. The ZyXEL Device forwards the traffic with this port (or range of ports) to the client computer on the LAN that requested the service.
Start Port	Type a port number or the starting port number in a range of port numbers.
End Port	Type a port number or the ending port number in a range of port numbers.
Trigger	The trigger port is a port (or a range of ports) that causes (or triggers) the ZyXEL Device to record the IP address of the LAN computer that sent the traffic to a server on the WAN.
Start Port	Type a port number or the starting port number in a range of port numbers.
End Port	Type a port number or the ending port number in a range of port numbers.
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to begin configuring this screen afresh.

13

Static Route

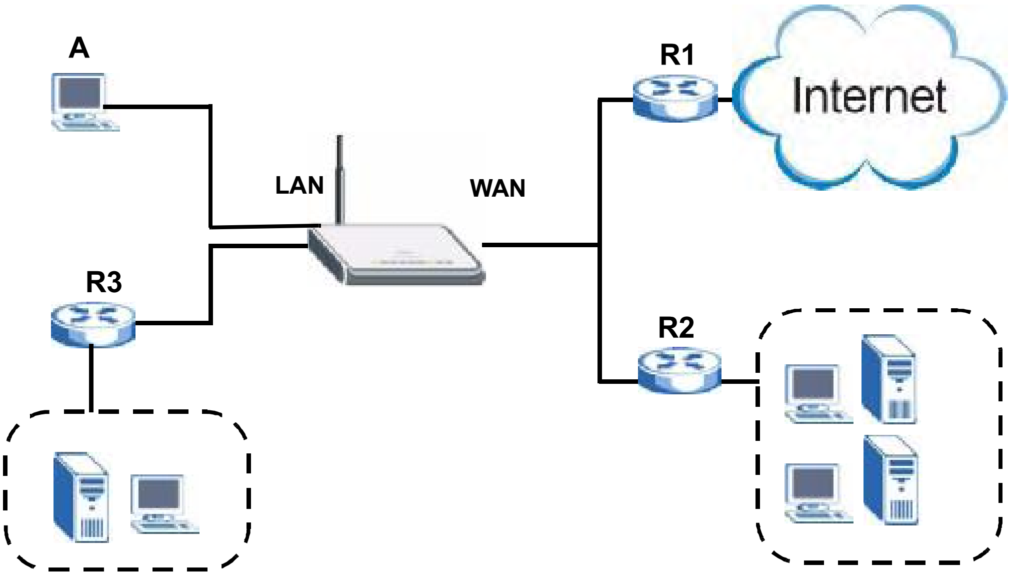
This chapter shows you how to configure static routes for your ZyXEL Device.

13.1 IP Static Route

The ZyXEL Device usually uses the default gateway to route outbound traffic from local computers to the Internet. To have the ZyXEL Device send data to devices not reachable through the default gateway, use static routes.

For example, the next figure shows a computer (**A**) connected to the ZyXEL Device's LAN interface. The ZyXEL Device routes most traffic from **A** to the Internet through the default gateway (**R1**). You create one static route to connect to services offered by your ISP behind router **R2**. You create another static route to communicate with a separate network behind a router (**R3**) connected to the LAN.

Figure 147 Example of Static Routing Topology



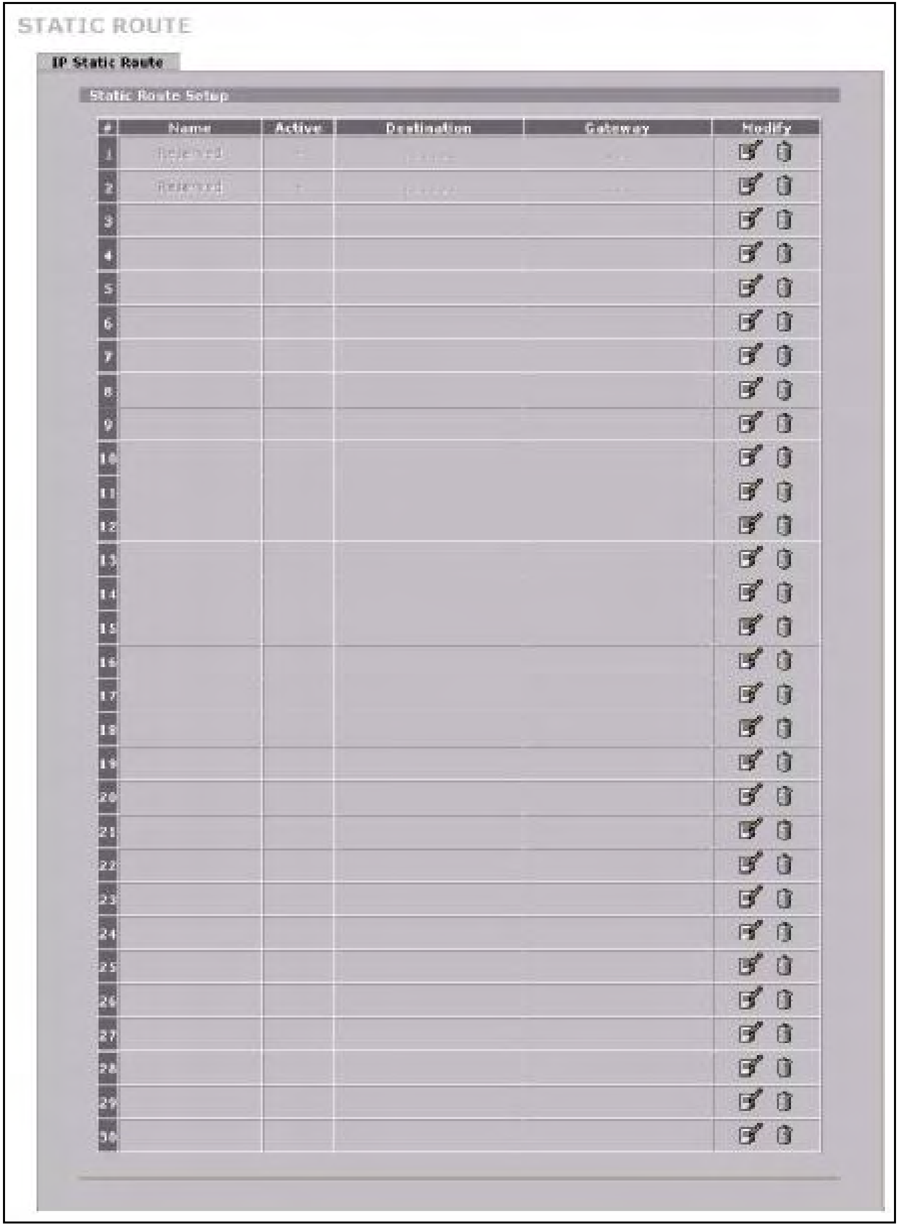
13.2 IP Static Route

Click **ADVANCED** > **STATIC ROUTE** to open the **IP Static Route** screen.

The first two static route entries are for default WAN 1 and WAN 2 routes on a ZyXEL Device with multiple WAN interfaces. You cannot modify or delete a static default route.

The default route is disabled after you change the static WAN IP address to a dynamic WAN IP address.

Figure 148 ADVANCED > STATIC ROUTE > IP Static Route



STATIC ROUTE

IP Static Route

Static Route Setup

#	Name	Active	Destination	Gateway	Modify
1	Reserved	-	[illegible]	[illegible]	✎ 🗑
2	Reserved	-	[illegible]	[illegible]	✎ 🗑
3					✎ 🗑
4					✎ 🗑
5					✎ 🗑
6					✎ 🗑
7					✎ 🗑
8					✎ 🗑
9					✎ 🗑
10					✎ 🗑
11					✎ 🗑
12					✎ 🗑
13					✎ 🗑
14					✎ 🗑
15					✎ 🗑
16					✎ 🗑
17					✎ 🗑
18					✎ 🗑
19					✎ 🗑
20					✎ 🗑
21					✎ 🗑
22					✎ 🗑
23					✎ 🗑
24					✎ 🗑
25					✎ 🗑
26					✎ 🗑
27					✎ 🗑
28					✎ 🗑
29					✎ 🗑
30					✎ 🗑

The following table describes the labels in this screen.

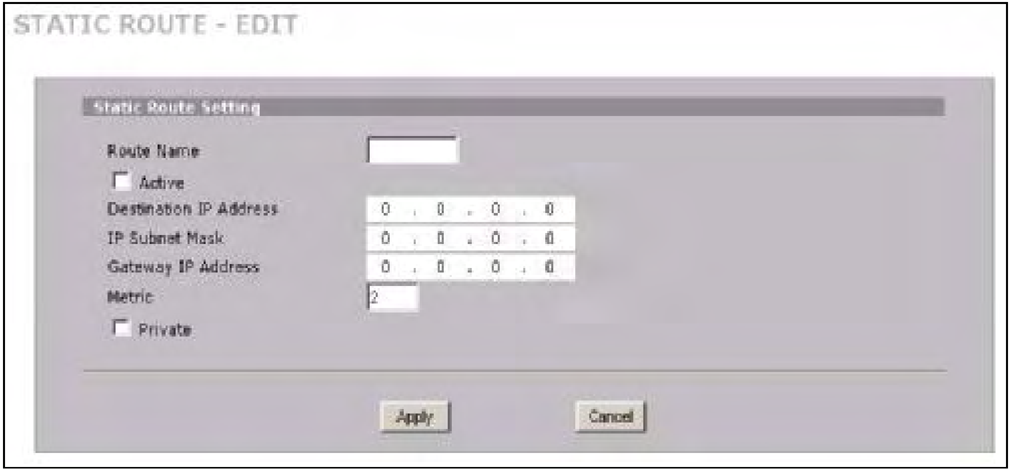
Table 73 ADVANCED > STATIC ROUTE > IP Static Route

LABEL	DESCRIPTION
#	This is the number of an individual static route.
Name	This is the name that describes or identifies this route.
Active	This field shows whether this static route is active (**Yes**) or not (**No**).
Destination	This parameter specifies the IP network address of the final destination. Routing is always based on network number.
Gateway	This is the IP address of the gateway. The gateway is a router or switch on the same network segment as the ZyXEL Device's interface. The gateway helps forward packets to their destinations.
Modify	Click the edit icon to go to the screen where you can set up a static route on the ZyXEL Device. Click the delete icon to remove a static route from the ZyXEL Device. A window displays asking you to confirm that you want to delete the route.

13.2.1 IP Static Route Edit

Click the edit icon in the **IP Static Route** screen. The screen shown next appears. Use this screen to configure the required information for a static route.

Figure 149 ADVANCED > STATIC ROUTE > IP Static Route > Edit



STATIC ROUTE - EDIT

Static Route Setting

Route Name

□ Active

Destination IP Address 0 . 0 . 0 . 0

IP Subnet Mask 0 . 0 . 0 . 0

Gateway IP Address 0 . 0 . 0 . 0

Metric 2

□ Private

The following table describes the labels in this screen.

Table 74 ADVANCED > STATIC ROUTE > IP Static Route > Edit

LABEL	DESCRIPTION
Route Name	Enter the name of the IP static route. Leave this field blank to delete this static route.
Active	This field allows you to activate/deactivate this static route.
Destination IP Address	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
IP Subnet Mask	Enter the IP subnet mask here.

Table 74 ADVANCED > STATIC ROUTE > IP Static Route > Edit

LABEL	DESCRIPTION
Gateway IP Address	Enter the IP address of the gateway. The gateway is a router or switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations.
Metric	Metric represents the “cost” of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Enter a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.
Private	This parameter determines if the ZyXEL Device will include this route to a remote node in its RIP broadcasts. Select this check box to keep this route private and not included in RIP broadcasts. Clear this check box to propagate this route to other hosts through RIP broadcasts.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

14

DNS

This chapter shows you how to configure the DNS screens.

14.1 DNS Overview

DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a machine before you can access it. The ZyXEL Device uses a system DNS server (in the order you specify in the **DNS System** screen) to resolve domain names, for example, DDNS and the time server.

14.2 DNS Server Address Assignment

The ZyXEL Device can get the DNS server addresses in the following ways.

1 The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you DNS server addresses, manually enter them in the DNS server fields.

2 If your ISP dynamically assigns the DNS server IP addresses (along with the ZyXEL Device's WAN IP address), set the DNS server fields to get the DNS server address from the ISP.

3 You can manually enter the IP addresses of other DNS servers. These servers can be public or private. A DNS server could even be behind a remote IPSec router (see Section 14.5.1 on page 248).

14.3 DNS Servers

There are three places where you can configure DNS setup on the ZyXEL Device.

1 Use the **DNS System** screen to configure the ZyXEL Device to use a DNS server to resolve domain names for ZyXEL Device system features such as DDNS and the time server.

2 Use the **DNS DHCP** screen to configure the DNS server information that the ZyXEL Device sends to the DHCP client devices on the LAN or DMZ.

3 Use the **REMOTE MGMT DNS** screen to configure the ZyXEL Device to accept or discard DNS queries.

14.4 Address Record

An address record contains the mapping of a fully qualified domain name (FQDN) to an IP address. An FQDN consists of a host and domain name and includes the top-level domain. For example, www.zyxel.com.tw is a fully qualified domain name, where “www” is the host, “zyxel” is the second-level domain, and “com.tw” is the top level domain. mail.myZyXEL.com.tw is also a FQDN, where "mail" is the host, "myZyXEL" is the second-level domain, and "com.tw" is the top level domain.

The ZyXEL Device allows you to configure address records about the ZyXEL Device itself or another device. This way you can keep a record of DNS names and addresses that people on your network may use frequently. If the ZyXEL Device receives a DNS query for an FQDN for which the ZyXEL Device has an address record, the ZyXEL Device can send the IP address in a DNS response without having to query a DNS name server.

14.4.1 DNS Wildcard

Enabling the wildcard feature for your host causes *.yourhost.com to be aliased to the same IP address as yourhost.com. This feature is useful if you want to be able to use, for example, www.yourhost.com and still reach your hostname.

14.5 Name Server Record

A name server record contains a DNS server’s IP address. The ZyXEL Device can query the DNS server to resolve domain names for features such as DDNS and the time server. A domain zone may also be included. A domain zone is a fully qualified domain name without the host. For example, zyxel.com.tw is the domain zone for the www.zyxel.com.tw fully qualified domain name.

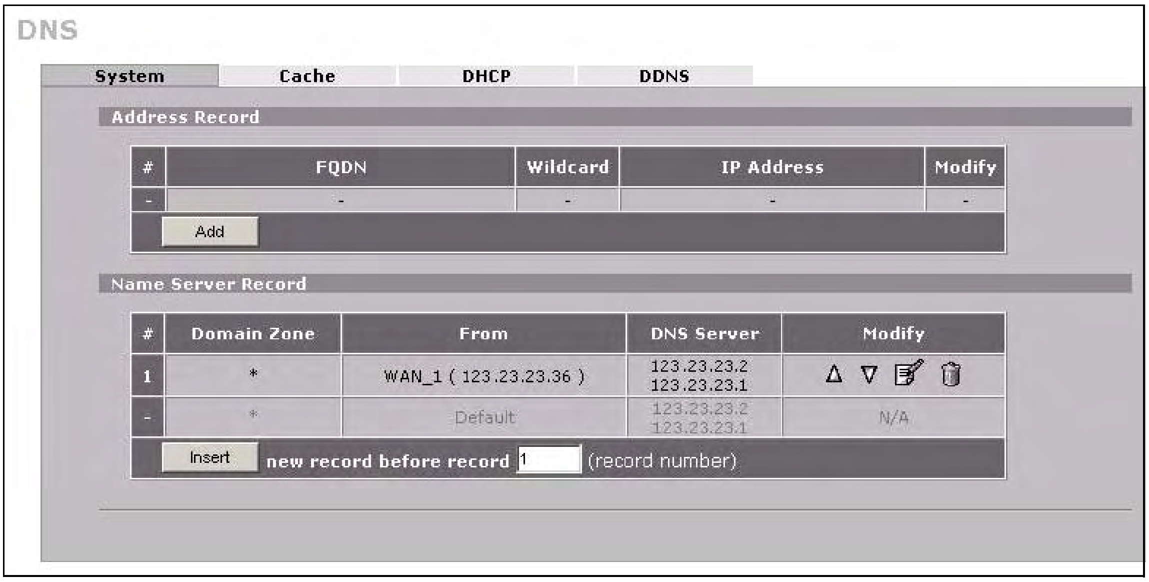
14.5.1 Private DNS Server

In cases where you want to use domain names to access Intranet servers on a remote private network that has a DNS server, you must identify that DNS server. You cannot use DNS servers on the LAN or from the ISP since these DNS servers cannot resolve domain names to private IP addresses on the remote private network.

14.6 System Screen

Click **ADVANCED** > **DNS** to display the following screen. Use this screen to configure your ZyXEL Device’s DNS address and name server records.

Figure 150 ADVANCED > DNS > System DNS



DNS

Address Record

#	FQDN	Wildcard	IP Address	Modify
-	-	-	-	-

Name Server Record

#	Domain Zone	From	DNS Server	Modify
1	*	WAN_1 (123.23.23.36)	123.23.23.2 123.23.23.1	
-	*	Default	123.23.23.2 123.23.23.1	N/A

Insert new record before record 1 (record number)

The following table describes the labels in this screen.

LABEL	DESCRIPTION
Address Record	An address record specifies the mapping of a fully qualified domain name (FQDN) to an IP address. An FQDN consists of a host and domain name and includes the top-level domain. For example, www.zyxel.com.tw is a fully qualified domain name, where “www” is the host, “zyxel” is the second-level domain, and “com.tw” is the top level domain.
#	This is the index number of the address record.
FQDN	This is a host’s fully qualified domain name.
Wildcard	This column displays whether or not the DNS wildcard feature is enabled for this domain name.
IP Address	This is the IP address of a host.
Modify	Click the edit icon to go to the screen where you can edit the record. Click the delete icon to remove an existing record. A window display asking you to confirm that you want to delete the record. Note that subsequent records move up by one when you take this action.
Add	Click **Add** to open a screen where you can add a new address record. Refer to Table 75 on page 251 for information on the fields.
Name Server Record	A name server record contains a DNS server’s IP address. The ZyXEL Device can query the DNS server to resolve domain names for features such as DDNS and the time server. When the ZyXEL Device needs to resolve a domain name, it checks it against the name server record entries in the order that they appear in this list. A “*” indicates a name server record without a domain zone. The default record is grayed out. The ZyXEL Device uses this default record if the domain name that needs to be resolved does not match any of the other name server records. A name server record with a domain zone is always put before a record without a domain zone.
#	This is the index number of the name server record.

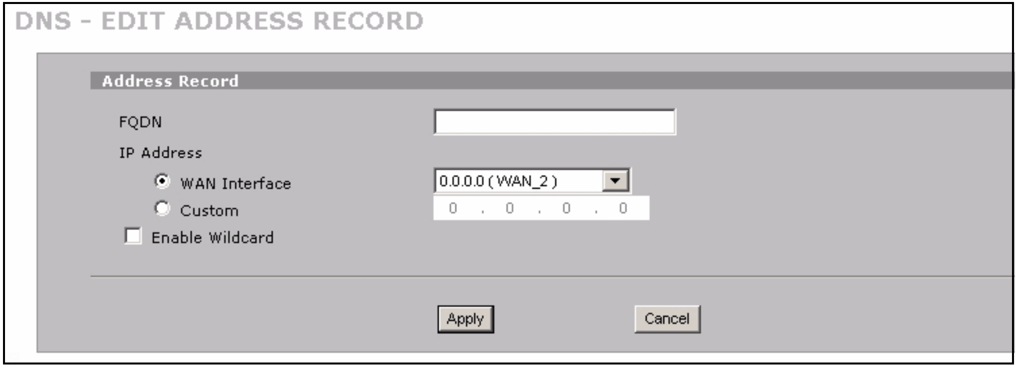
LABEL	DESCRIPTION
Domain Zone	A domain zone is a fully qualified domain name without the host. For example, zyxel.com.tw is the domain zone for the www.zyxel.com.tw fully qualified domain name.
From	This field displays whether the IP address of a DNS server is from a WAN interface (and which it is) or specified by the user.
DNS Server	This is the IP address of a DNS server.
Modify	Click a triangle icon to move the record up or down in the list. Click the edit icon to go to the screen where you can edit the record. Click the delete icon to remove an existing record. A window display asking you to confirm that you want to delete the record. Note that subsequent records move up by one when you take this action.
Insert	Click **Insert** to open a screen where you can insert a new name server record. Refer to Table 76 on page 252 for information on the fields.

14.6.1 Adding an Address Record

Click **Add** in the **System** screen to open this screen. Use this screen to add an address record.

An address record contains the mapping of a fully qualified domain name (FQDN) to an IP address. Configure address records about the ZyXEL Device itself or another device to keep a record of DNS names and addresses that people on your network may use frequently. If the ZyXEL Device receives a DNS query for an FQDN for which the ZyXEL Device has an address record, the ZyXEL Device can send the IP address in a DNS response without having to query a DNS name server. See Section 14.4 on page 248 for more on address records.

Figure 151 ADVANCED > DNS > Add (Address Record)



DNS - EDIT ADDRESS RECORD

Address Record

FQDN

IP Address

● WAN Interface 0.0.0.0 (WAN_2)

○ Custom 0 . 0 . 0 . 0

□ Enable Wildcard

The following table describes the labels in this screen.

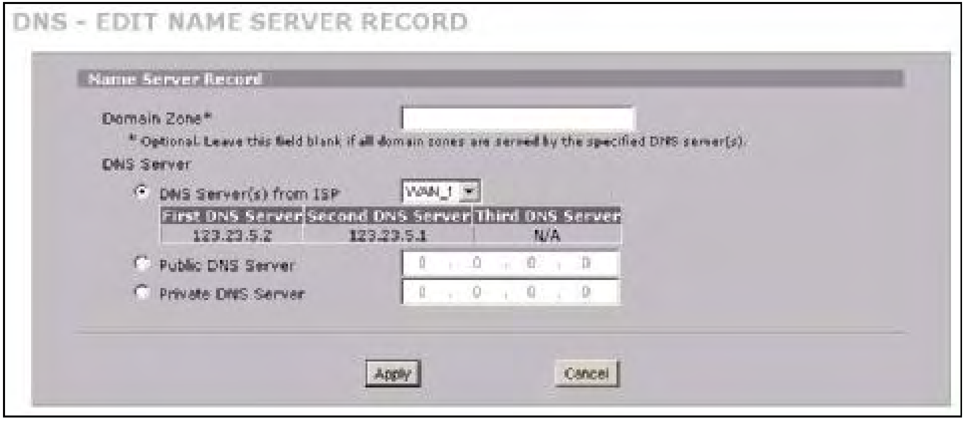
Table 75 ADVANCED > DNS > Add (Address Record)

LABEL	DESCRIPTION
FQDN	Type a fully qualified domain name (FQDN) of a server. An FQDN starts with a host name and continues all the way up to the top-level domain name. For example, www.zyxel.com.tw is a fully qualified domain name, where "www" is the host, "zyxel" is the second-level domain, and "com.tw" is the top level domain.
IP Address	If this entry is for one of the WAN ports on a ZyXEL Device with multiple WAN ports, select **WAN Interface** and select WAN 1 or WAN 2 from the drop-down list box. If this entry is for the WAN port on a ZyXEL Device with a single WAN port, select **WAN Interface**. For entries that are not for the WAN port(s), select **Custom** and enter the IP address of the host in dotted decimal notation.
Enable Wildcard	Select the check box to enable DNS wildcard.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

14.6.2 Inserting a Name Server Record

Click **Insert** in the **System** screen to open this screen. Use this screen to insert a name server record. A name server record contains a DNS server's IP address. The ZyXEL Device can query the DNS server to resolve domain names for features such as DDNS and the time server. A domain zone may also be included. A domain zone is a fully qualified domain name without the host. For example, zyxel.com.tw is the domain zone for the www.zyxel.com.tw fully qualified domain name.

Figure 152 ADVANCED > DNS > Insert (Name Server Record)



DNS - EDIT NAME SERVER RECORD

Name Server Record

Domain Zone*

* Optional. Leave this field blank if all domain zones are served by the specified DNS server(s).

DNS Server

● DNS Server(s) from ISP WAN_1

First DNS Server	Second DNS Server	Third DNS Server
123.23.5.2	123.23.5.1	N/A

○ Public DNS Server 0 . 0 . 0 . 0

○ Private DNS Server 0 . 0 . 0 . 0

The following table describes the labels in this screen.

LABEL	DESCRIPTION
Domain Zone	This field is optional. A domain zone is a fully qualified domain name without the host. For example, zyxel.com.tw is the domain zone for the www.zyxel.com.tw fully qualified domain name. For example, whenever the ZyXEL Device receives needs to resolve a zyxel.com.tw domain name, it can send a query to the recorded name server IP address. Leave this field blank if all domain zones are served by the specified DNS server(s).
DNS Server	Select the **DNS Server(s) from ISP** radio button if your ISP dynamically assigns DNS server information. You also need to select an interface through which the ISP provides the DNS server IP address(es). The interface should be activated and set as a DHCP client.The fields below display the (read-only) DNS server IP address(es) that the ISP assigns. **N/A** displays for any DNS server IP address fields for which the ISP does not assign an IP address. **N/A** displays for all of the DNS server IP address fields if the ZyXEL Device has a fixed WAN IP address. Select **Public DNS Server** if you have the IP address of a DNS server. The IP address must be public or a private address on your local LAN. Enter the DNS server's IP address in the field to the right. **Public DNS Server** entries with the IP address set to 0.0.0.0 are not allowed. Select **Private DNS Server** if the DNS server has a private IP address and is located in a local network. Enter the DNS server's IP address in the field to the right. With a private DNS server, you must also configure the first DNS server entry for the LAN or DMZ in the **DNS DHCP** screen to use **DNS Relay**. **Private DNS Server** entries with the IP address set to 0.0.0.0 are not allowed.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

14.7 DNS Cache

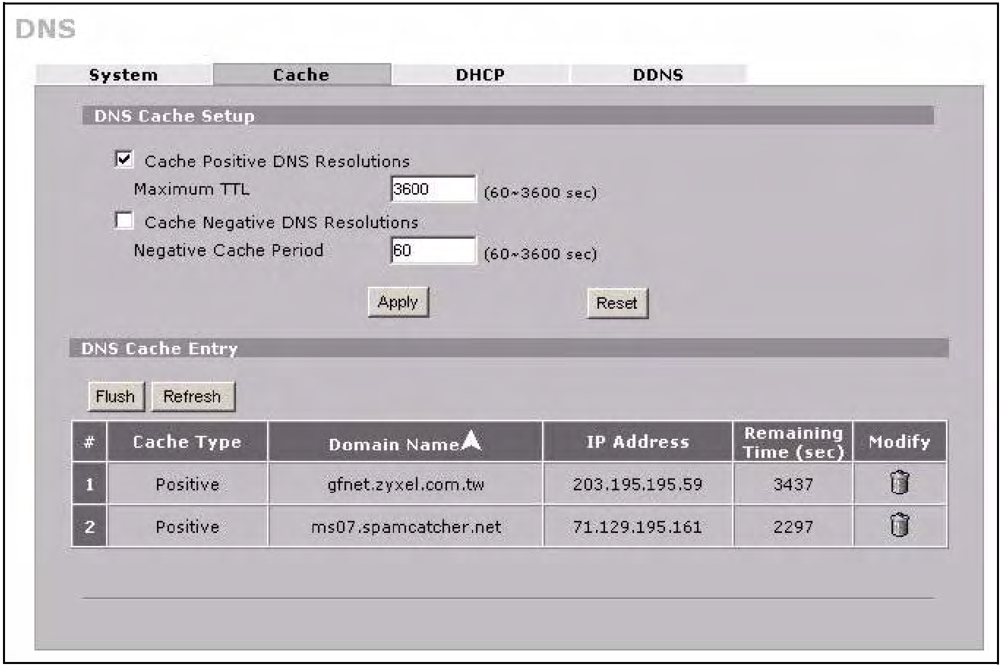
DNS cache is the temporary storage area where a router stores responses from DNS servers. When the ZyXEL Device receives a positive or negative response for a DNS query, it records the response in the DNS cache. A positive response means that the ZyXEL Device received the IP address for a domain name that it checked with a DNS server within the five second DNS timeout period. A negative response means that the ZyXEL Device did not receive a response for a query it sent to a DNS server within the five second DNS timeout period.

When the ZyXEL Device receives DNS queries, it compares them against the DNS cache before querying a DNS server. If the DNS query matches a positive entry, the ZyXEL Device responses with the IP address from the entry. If the DNS query matches a negative entry, the ZyXEL Device replies that the DNS query failed.

14.8 Configure DNS Cache

To configure your ZyXEL Device’s DNS caching, click **ADVANCED** > **DNS** > **Cache**. The screen appears as shown.

Figure 153 ADVANCED > DNS > Cache



DNS Cache Setup

☑ Cache Positive DNS Resolutions

Maximum TTL 3600 (60~3600 sec)

☐ Cache Negative DNS Resolutions

Negative Cache Period 60 (60~3600 sec)

DNS Cache Entry

#	Cache Type	Domain Name▲	IP Address	Remaining Time (sec)	Modify
1	Positive	gfnet.zyxel.com.tw	203.195.195.59	3437	🗑
2	Positive	ms07.spamcatcher.net	71.129.195.161	2297	🗑

The following table describes the labels in this screen.

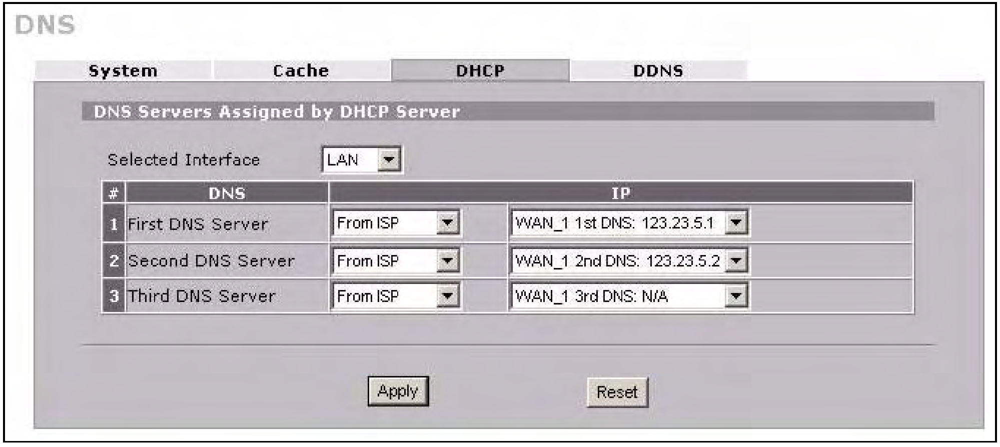
LABEL	DESCRIPTION
DNS Cache Setup	
Cache Positive DNS Resolutions	Select the check box to record the positive DNS resolutions in the cache. Caching positive DNS resolutions helps speed up the ZyXEL Device's processing of commonly queried domain names and reduces the amount of traffic that the ZyXEL Device sends out to the WAN.
Maximum TTL	Type the maximum time to live (TTL) (60 to 3600 seconds). This sets how long the ZyXEL Device is to allow a positive resolution entry to remain in the DNS cache before discarding it.
Cache Negative DNS Resolutions	Caching negative DNS resolutions helps speed up the ZyXEL Device's processing of commonly queried domain names (for which DNS resolution has failed) and reduces the amount of traffic that the ZyXEL Device sends out to the WAN.
Negative Cache Period	Type the time (60 to 3600 seconds) that the ZyXEL Device is to allow a negative resolution entry to remain in the DNS cache before discarding it.
Apply	Click **Apply** to save your changes back to the ZyXEL Device.
Reset	Click **Reset** to begin configuring this screen afresh.
DNS Cache Entry	
Flush	Click this button to clear the cache manually. After you flush the cache, the ZyXEL Device must query the DNS servers again for any domain names that had been previously resolved.
Refresh	Click this button to reload the cache.
#	This is the index number of a record.
Cache Type	This displays whether the response for the DNS request is positive or negative.
Domain Name	This is the domain name of a host.

LABEL	DESCRIPTION
IP Address	This is the (resolved) IP address of a host. This field displays **0.0.0.0** for negative DNS resolution entries.
Remaining Time (sec)	This is the number of seconds left before the DNS resolution entry is discarded from the cache.
Modify	Click the delete icon to remove the DNS resolution entry from the cache.

14.9 Configuring DNS DHCP

Click **ADVANCED** > **DNS** > **DHCP** to open the **DNS DHCP** screen shown next. Use this screen to configure the DNS server information that the ZyXEL Device sends to its LAN or DMZ DHCP clients.

Figure 154 ADVANCED > DNS > DHCP



Selected Interface: LAN

#	DNS		IP
1	First DNS Server	From ISP	WAN_1 1st DNS: 123.23.5.1
2	Second DNS Server	From ISP	WAN_1 2nd DNS: 123.23.5.2
3	Third DNS Server	From ISP	WAN_1 3rd DNS: N/A

The following table describes the labels in this screen.

LABEL	DESCRIPTION
DNS Servers Assigned by DHCP Server	The ZyXEL Device passes a DNS (Domain Name System) server IP address to the DHCP clients.
Selected Interface	Select an interface from the drop-down list box to configure the DNS servers for the specified interface.
DNS	These read-only labels represent the DNS servers.

LABEL	DESCRIPTION
IP	Select **From ISP** if your ISP dynamically assigns DNS server information (and the ZyXEL Device's WAN IP address). Use the drop-down list box to select a DNS server IP address that the ISP assigns in the field to the right. Select **User-Defined** if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose **User-Defined**, but leave the IP address set to 0.0.0.0, **User-Defined** changes to **None** after you click **Apply**. If you set a second choice to **User-Defined**, and enter the same IP address, the second **User-Defined** changes to **None** after you click **Apply**. Select **DNS Relay** to have the ZyXEL Device act as a DNS proxy. The ZyXEL Device's LAN or DMZ IP address displays in the field to the right (read-only). The ZyXEL Device tells the DHCP clients on the LAN or DMZ that the ZyXEL Device itself is the DNS server. When a computer on the LAN or DMZ sends a DNS query to the ZyXEL Device, the ZyXEL Device forwards the query to the ZyXEL Device's system DNS server (configured in the **DNS System** screen) and relays the response back to the computer. You can only select **DNS Relay** for one of the three servers; if you select DNS Relay for a second or third DNS server, that choice changes to **None** after you click **Apply**. Select **None** if you do not want to configure DNS servers. You must have another DHCP sever on your LAN, or else the computers must have their DNS server addresses manually configured. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to begin configuring this screen afresh.

14.10 Dynamic DNS

Dynamic DNS allows you to update your current dynamic IP address with one or many dynamic DNS services so that anyone can contact you (in NetMeeting, CU-SeeMe, etc.). You can also access your FTP server or Web site on your own computer using a domain name (for instance myhost.dhs.org, where myhost is a name of your choice) that will never change instead of using an IP address that changes each time you reconnect. Your friends or relatives will always be able to call you even if they don't know your IP address.

First of all, you need to have registered a dynamic DNS account with www.dyndns.org. This is for people with a dynamic IP from their ISP or DHCP server that would still like to have a domain name. The Dynamic DNS service provider will give you a password or key.

You must go to the Dynamic DNS service provider’s website and register a user account and a domain name before you can use the Dynamic DNS service with your ZyXEL Device.

14.10.1 DYNDNS Wildcard

Enabling the wildcard feature for your host causes *.yourhost.dyndns.org to be aliased to the same IP address as yourhost.dyndns.org. This feature is useful if you want to be able to use, for example, www.yourhost.dyndns.org and still reach your hostname.

If you have a private WAN IP address, then you cannot use Dynamic DNS.

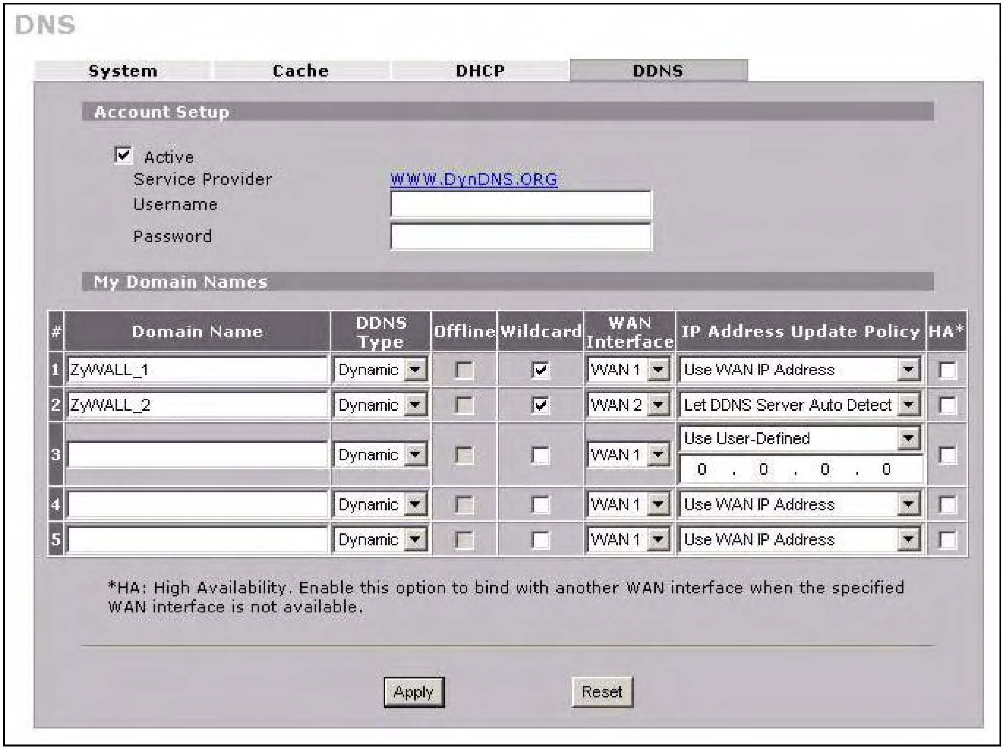
14.10.2 High Availability

A DNS server maps a domain name to a port's IP address. If that WAN port loses its connection, high availability allows the router to substitute another port's IP address for the domain name mapping.

14.11 Configuring Dynamic DNS

To change your ZyXEL Device’s DDNS, click **ADVANCED** > **DNS** > **DDNS**. The screen appears as shown.

Figure 155 ADVANCED > DNS > DDNS



☑ Active
Service Provider WWW.DynDNS.ORG
Username
Password

#	Domain Name	DDNS Type	Offline	Wildcard	WAN Interface	IP Address Update Policy	HA*
1	ZyWALL_1	Dynamic	□	☑	WAN 1	Use WAN IP Address	□
2	ZyWALL_2	Dynamic	□	☑	WAN 2	Let DDNS Server Auto Detect	□
3		Dynamic	□	□	WAN 1	Use User-Defined 0 . 0 . 0 . 0	□
4		Dynamic	□	□	WAN 1	Use WAN IP Address	□
5		Dynamic	□	□	WAN 1	Use WAN IP Address	□

*HA: High Availability. Enable this option to bind with another WAN interface when the specified WAN interface is not available.

The following table describes the labels in this screen.

LABEL	DESCRIPTION
Account Setup	
Active	Select this check box to use dynamic DNS.
Service Provider	This is the name of your Dynamic DNS service provider.

LABEL	DESCRIPTION
Username	Enter your user name. You can use up to 31 alphanumeric characters (and the underscore). Spaces are not allowed.
Password	Enter the password associated with the user name above. You can use up to 31 alphanumeric characters (and the underscore). Spaces are not allowed.
My Domain Names	
Domain Name 1~5	Enter the host names in these fields.
DDNS Type	Select the type of service that you are registered for from your Dynamic DNS service provider. Select **Dynamic** if you have the Dynamic DNS service. Select **Static** if you have the Static DNS service. Select **Custom** if you have the Custom DNS service.
Offline	This option is available when **Custom** is selected in the **DDNS Type** field. Check with your Dynamic DNS service provider to have traffic redirected to a URL (that you can specify) while you are off line.
Wildcard	Select the check box to enable DYNDNS Wildcard.
WAN Interface	Select the WAN interface to use for updating the IP address of the domain name.
IP Address Update Policy	Select **Use WAN IP Address** to have the ZyXEL Device update the domain name with the WAN interface's IP address. Select **Use User-Defined** and enter the IP address if you have a static IP address. Select **Let DDNS Server Auto Detect** only when there are one or more NAT routers between the ZyXEL Device and the DDNS server. This feature has the DDNS server automatically detect and use the IP address of the NAT router that has a public IP address. Note: The DDNS server may not be able to detect the proper IP address if there is an HTTP proxy server between the ZyXEL Device and the DDNS server.
HA	Select this check box to enable the high availability (HA) feature. High availability has the ZyXEL Device update a domain name with another interface’s IP address when the normal WAN interface does not have a connection. The ZyXEL Device will update the domain name with the IP address of whichever WAN interface has a connection, regardless of the setting in the **WAN Interface** field. Disable this feature and the ZyXEL Device will only update the domain name with an IP address of the WAN interface specified in the **WAN Interface** field. If that WAN interface does not have a connection, the ZyXEL Device will not update the domain name with another port’s IP address. Note: DDNS does not function when the ZyXEL Device uses traffic redirect.
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to begin configuring this screen afresh.

15

Remote Management

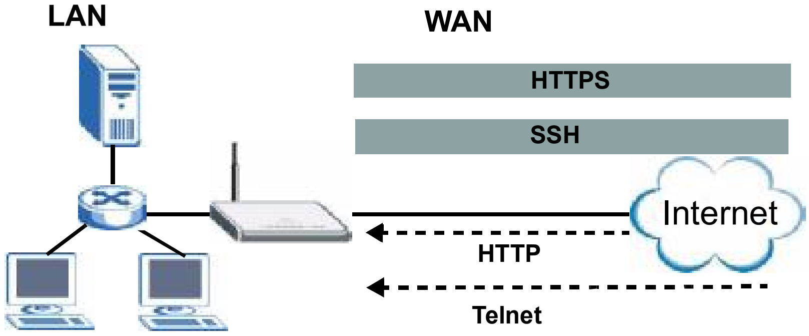
This chapter provides information on the Remote Management screens.

15.1 Remote Management Overview

Remote management allows you to determine which services/protocols can access which ZyXEL Device interface (if any) from which computers.

The following figure shows secure and insecure management of the ZyXEL Device coming in from the WAN. HTTPS and SSH access are secure. HTTP and Telnet access are not secure.

Figure 156 Secure and Insecure Remote Management From the WAN



When you configure remote management to allow management from any network except the LAN, you still need to configure a firewall rule to allow access. See Chapter 9 on page 167 for details on configuring firewall rules.

You can also disable a service on the ZyXEL Device by not allowing access for the service/ protocol through any of the ZyXEL Device interfaces.

You may only have one remote management session running at a time. The ZyXEL Device automatically disconnects a remote management session of lower priority when another remote management session of higher priority starts. The priorities for the different types of remote management sessions are as follows.

1. Console port
2. SSH

3 Telnet
4 HTTPS and HTTP

15.1.1 Remote Management Limitations

Remote management does not work when:

1 You have not enabled that service on the interface in the corresponding remote management screen.
2 You have disabled that service in one of the remote management screens.
3 The IP address in the **Secure Client IP Address** field does not match the client IP address. If it does not match, the ZyXEL Device will disconnect the session immediately.
4 There is already another remote management session with an equal or higher priority running. You may only have one remote management session running at one time.
5 There is a firewall rule that blocks it.
6 A filter is applied (through the commands) to block a Telnet, FTP or Web service.

15.1.2 System Timeout

There is a default system management idle timeout of five minutes (three hundred seconds). The ZyXEL Device automatically logs you out if the management session remains idle for longer than this timeout period. The management session does not time out when a statistics screen is polling. You can change the timeout period in the **MAINTENANCE** > **General** screen.

15.2 WWW (HTTP and HTTPS)

HTTPS (HyperText Transfer Protocol over Secure Socket Layer, or HTTP over SSL) is a web protocol that encrypts and decrypts web pages. Secure Socket Layer (SSL) is an application-level protocol that enables secure transactions of data by ensuring confidentiality (an unauthorized party cannot read the transferred data), authentication (one party can identify the other party) and data integrity (you know if data has been changed).

It relies upon certificates, public keys, and private keys (see Chapter 11 on page 195 for more information).

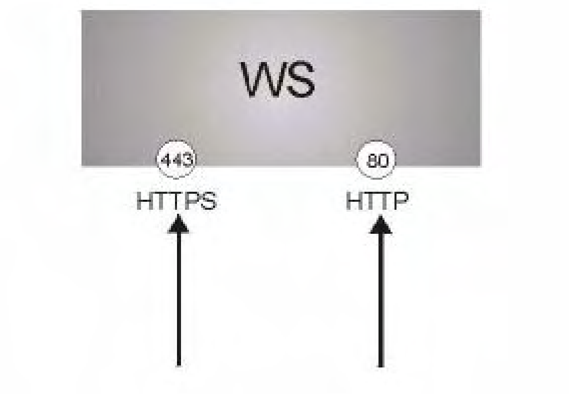
HTTPS on the ZyXEL Device is used so that you may securely access the ZyXEL Device using the web configurator. The SSL protocol specifies that the SSL server (the ZyXEL Device) must always authenticate itself to the SSL client (the computer which requests the HTTPS connection with the ZyXEL Device), whereas the SSL client only should authenticate itself when the SSL server requires it to do so (select **Authenticate Client Certificates** in the **REMOTE MGMT > WWW** screen). **Authenticate Client Certificates** is optional and if selected means the SSL-client must send the ZyXEL Device a certificate. You must apply for a certificate for the browser from a CA that is a trusted CA on the ZyXEL Device.

Please refer to the following figure.

1 HTTPS connection requests from an SSL-aware web browser go to port 443 (by default) on the ZyXEL Device's WS (web server).

2 HTTP connection requests from a web browser go to port 80 (by default) on the ZyXEL Device's WS (web server).

Figure 157 HTTPS Implementation

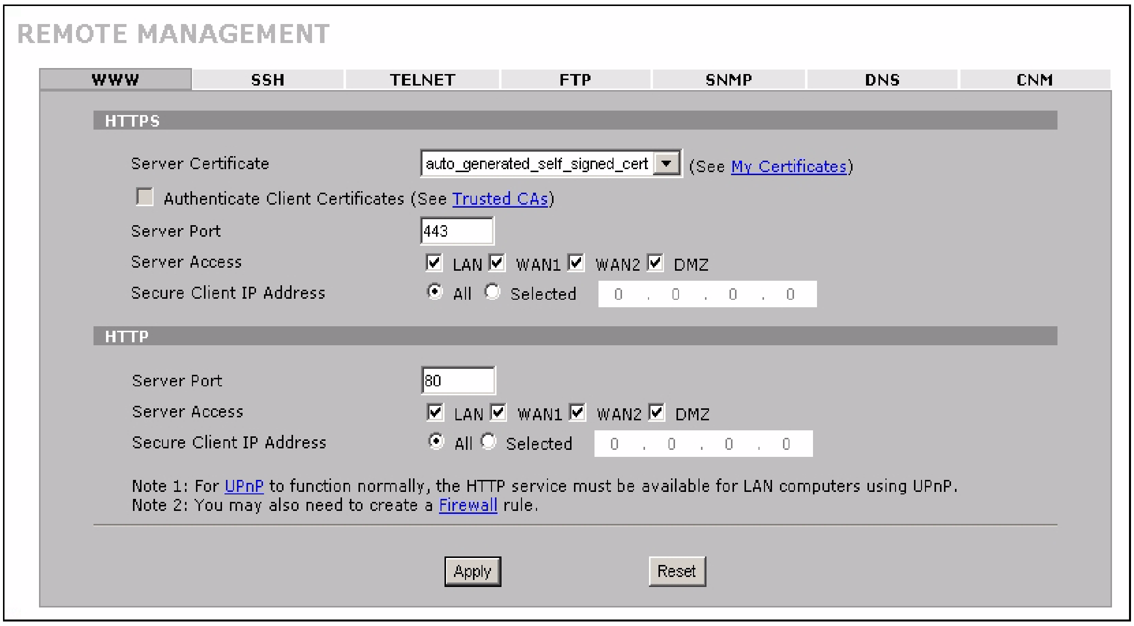


If you disable the **HTTP** service in the **REMOTE MGMT > WWW** screen, then the ZyXEL Device blocks all HTTP connection attempts.

15.3 WWW

Click **ADVANCED** > **REMOTE MGMT** to open the **WWW** screen. Use this screen to configure the ZyXEL Device's HTTP and HTTPS management settings.

Figure 158 ADVANCED > REMOTE MGMT > WWW



HTTPS

Server Certificate: auto_generated_self_signed_cert (See My Certificates)

□ Authenticate Client Certificates (See Trusted CAs)

Server Port: 443

Server Access: ☑ LAN ☑ WAN1 ☑ WAN2 ☑ DMZ

Secure Client IP Address: ● All ○ Selected 0 . 0 . 0 . 0

HTTP

Server Port: 80

Server Access: ☑ LAN ☑ WAN1 ☑ WAN2 ☑ DMZ

Secure Client IP Address: ● All ○ Selected 0 . 0 . 0 . 0

Note 1: For UPnP to function normally, the HTTP service must be available for LAN computers using UPnP.
Note 2: You may also need to create a Firewall rule.

The following table describes the labels in this screen.

Table 76 ADVANCED > REMOTE MGMT > WWW

LABEL	DESCRIPTION
HTTPS	
Server Certificate	Select the **Server Certificate** that the ZyXEL Device will use to identify itself. The ZyXEL Device is the SSL server and must always authenticate itself to the SSL client (the computer which requests the HTTPS connection with the ZyXEL Device).
Authenticate Client Certificates	Select **Authenticate Client Certificates** (optional) to require the SSL client to authenticate itself to the ZyXEL Device by sending the ZyXEL Device a certificate. To do that the SSL client must have a CA-signed certificate from a CA that has been imported as a trusted CA on the ZyXEL Device (see Appendix F on page 403 on importing certificates for details).
Server Port	The HTTPS proxy server listens on port 443 by default. If you change the HTTPS proxy server port to a different number on the ZyXEL Device, for example 8443, then you must notify people who need to access the ZyXEL Device web configurator to use "https://ZyXEL Device IP Address:**8443**" as the URL.
Server Access	Select the interface(s) through which a computer may access the ZyXEL Device using this service. You can allow only secure web configurator access by clearing all of the interface check boxes in the **HTTP Server Access** field and setting the **HTTPS Server Access** field to an interface(s).
Secure Client IP Address	A secure client is a "trusted" computer that is allowed to communicate with the ZyXEL Device using this service. Select **All** to allow any computer to access the ZyXEL Device using this service. Choose **Selected** to just allow the computer with the IP address that you specify to access the ZyXEL Device using this service.
HTTP	
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.

Table 76 ADVANCED > REMOTE MGMT > WWW (continued)

LABEL	DESCRIPTION
Server Access	Select the interface(s) through which a computer may access the ZyXEL Device using this service.
Secure Client IP Address	A secure client is a “trusted” computer that is allowed to communicate with the ZyXEL Device using this service. Select **All** to allow any computer to access the ZyXEL Device using this service. Choose **Selected** to just allow the computer with the IP address that you specify to access the ZyXEL Device using this service.
Apply	Click **Apply** to save your customized settings and exit this screen.
Reset	Click **Reset** to begin configuring this screen afresh.

15.4 HTTPS Example

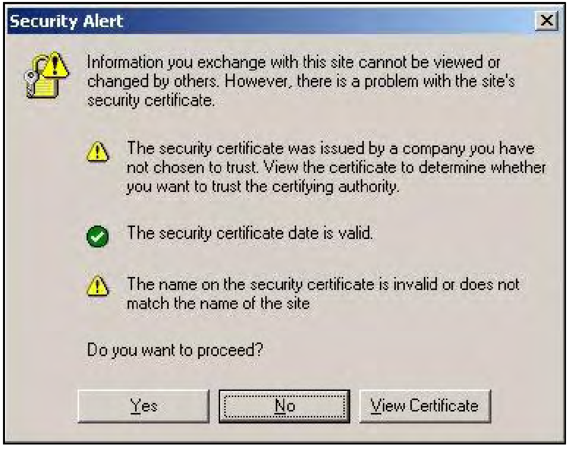
If you haven’t changed the default HTTPS port on the ZyXEL Device, then in your browser enter “https://ZyXEL Device IP Address/” as the web site address where “ZyXEL Device IP Address” is the IP address or domain name of the ZyXEL Device you wish to access.

15.4.1 Internet Explorer Warning Messages

When you attempt to access the ZyXEL Device HTTPS server, a Windows dialog box pops up asking if you trust the server certificate. Click **View Certificate** if you want to verify that the certificate is from the ZyXEL Device.

You see the following **Security Alert** screen in Internet Explorer. Select **Yes** to proceed to the web configurator login screen; if you select **No**, then web configurator access is blocked.

Figure 159 Security Alert Dialog Box (Internet Explorer)



Security Alert

Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

⚠ The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

✓ The security certificate date is valid.

⚠ The name on the security certificate is invalid or does not match the name of the site

Do you want to proceed?

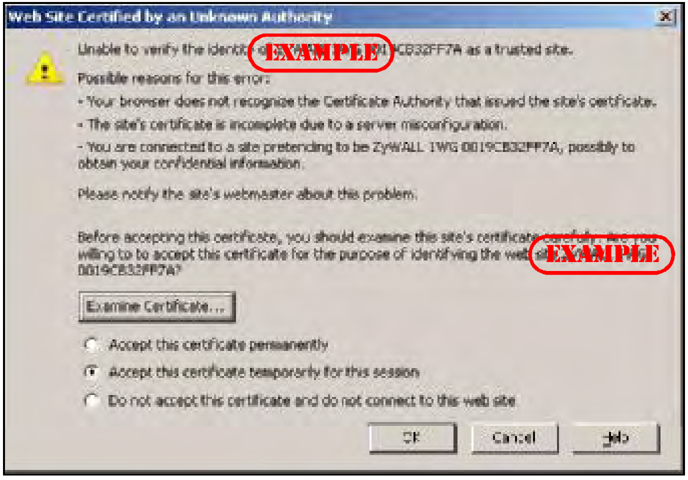
15.4.2 Netscape Navigator Warning Messages

When you attempt to access the ZyXEL Device HTTPS server, a **Website Certified by an Unknown Authority** screen pops up asking if you trust the server certificate. Click **Examine Certificate** if you want to verify that the certificate is from the ZyXEL Device.

If **Accept this certificate temporarily for this session** is selected, then click **OK** to continue in Netscape.

Select **Accept this certificate permanently** to import the ZyXEL Device's certificate into the SSL client.

Figure 160 Security Certificate 1 (Netscape)



Web Site Certified by an Unknown Authority

Unable to verify the identit EXAMPLE CB32FF7A as a trusted site.

Possible reasons for this error:

- Your browser does not recognize the Certificate Authority that issued the site's certificate.
- The site's certificate is incomplete due to a server misconfiguration.
- You are connected to a site pretending to be ZyWALL 1WG 0019CB32FF7A, possibly to obtain your confidential information.

Please notify the site's webmaster about this problem.

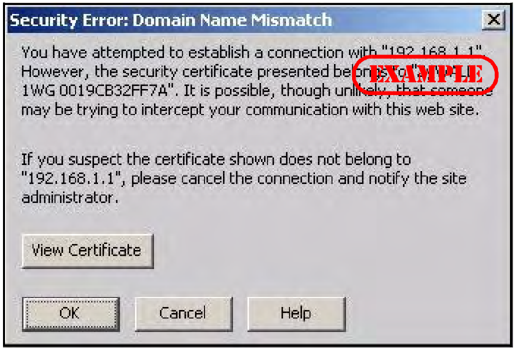
Before accepting this certificate, you should examine this site's certificate EXAMPLE willing to to accept this certificate for the purpose of identifying the web EXAMPLE 0019CB32FF7A?

○ Accept this certificate permanently

● Accept this certificate temporarily for this session

○ Do not accept this certificate and do not connect to this web site

Figure 161 Security Certificate 2 (Netscape)



Security Error: Domain Name Mismatch

You have attempted to establish a connection with "192.168.1.1". However, the security certificate presented be EXAMPLE 1WG 0019CB32FF7A". It is possible, though unlikely, that someone may be trying to intercept your communication with this web site.

If you suspect the certificate shown does not belong to "192.168.1.1", please cancel the connection and notify the site administrator.

15.4.3 Avoiding the Browser Warning Messages

The following describes the main reasons that your browser displays warnings about the ZyXEL Device's HTTPS server certificate and what you can do to avoid seeing the warnings.

- The issuing certificate authority of the ZyXEL Device's HTTPS server certificate is not one of the browser's trusted certificate authorities. The issuing certificate authority of the ZyXEL Device's factory default certificate is the ZyXEL Device itself since the certificate is a self-signed certificate.
    - For the browser to trust a self-signed certificate, import the self-signed certificate into your operating system as a trusted certificate.
    - To have the browser trust the certificates issued by a certificate authority, import the certificate authority's certificate into your operating system as a trusted certificate. Refer to Appendix F on page 403 for details.

- The actual IP address of the HTTPS server (the IP address of the ZyXEL Device's port that you are trying to access) does not match the common name specified in the ZyXEL Device's HTTPS server certificate that your browser received. Do the following to check the common name specified in the certificate that your ZyXEL Device sends to HTTPS clients.

  2a Click **REMOTE MGMT**. Write down the name of the certificate displayed in the **Server Certificate** field.

  2b Click **CERTIFICATES**. Find the certificate and check its **Subject** column. **CN** stands for certificate's common name (see Figure 164 on page 266 for an example).

Use this procedure to have the ZyXEL Device use a certificate with a common name that matches the ZyXEL Device's actual IP address. You cannot use this procedure if you need to access the WAN port and it uses a dynamically assigned IP address.

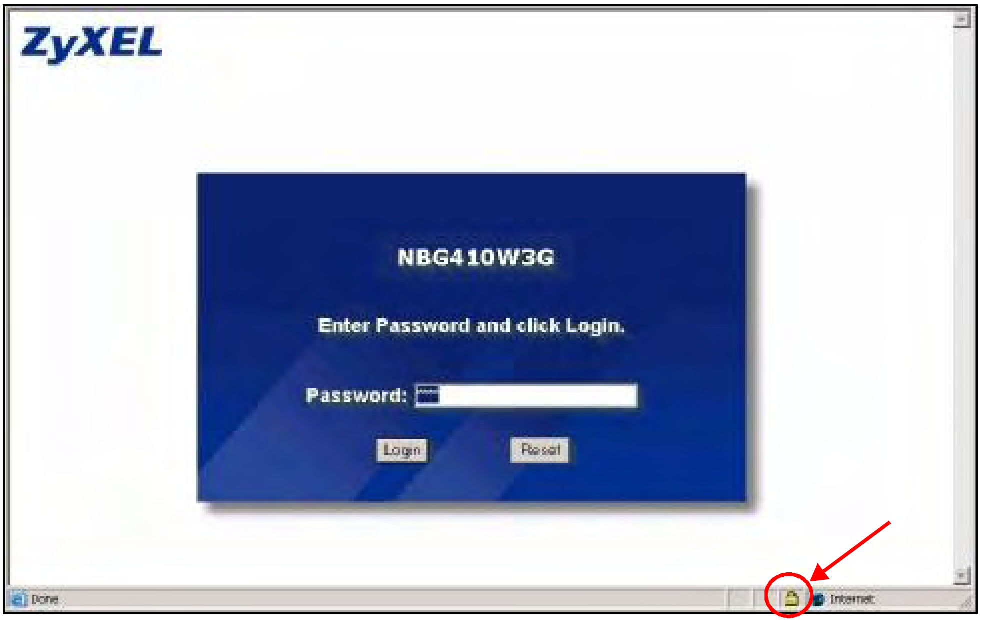
2a Create a new certificate for the ZyXEL Device that uses the IP address (of the ZyXEL Device's port that you are trying to access) as the certificate's common name. For example, to use HTTPS to access a LAN port with IP address 192.168.1.1, create a certificate that uses 192.168.1.1 as the common name.

2b Go to the remote management **WWW** screen and select the newly created certificate in the **Server Certificate** field. Click **Apply**.

15.4.4 Login Screen

After you accept the certificate, the ZyXEL Device login screen appears. The lock displayed in the bottom right of the browser status bar denotes a secure connection.

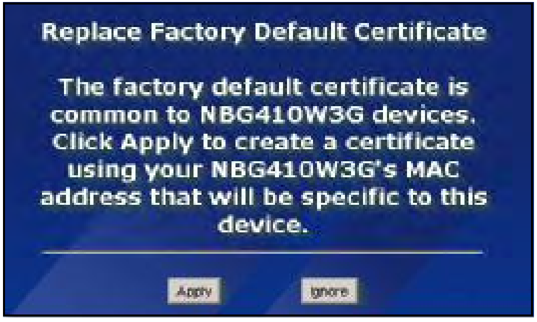
Figure 162 Example: Lock Denoting a Secure Connection



Click **Login** and you then see the next screen.

The factory default certificate is a common default certificate for all ZyXEL Device models.

Figure 163 Replace Certificate

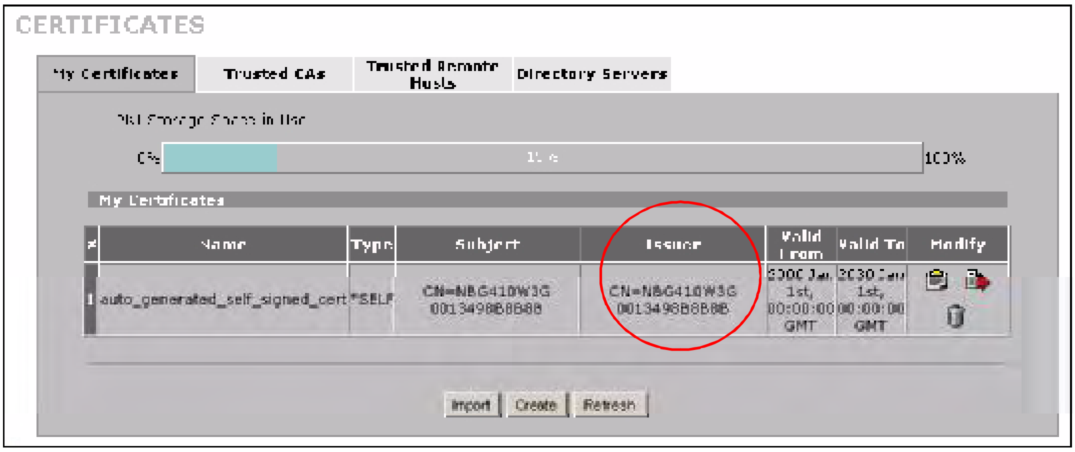


Replace Factory Default Certificate

The factory default certificate is common to NBG410W3G devices. Click Apply to create a certificate using your NBG410W3G's MAC address that will be specific to this device.

Click **Apply** in the **Replace Certificate** screen to create a certificate using your ZyXEL Device's MAC address that will be specific to this device. Click **CERTIFICATES** to open the **My Certificates** screen. You will see information similar to that shown in the following figure.

Figure 164 Device-specific Certificate



CERTIFICATES

PKI Storage Space in Use

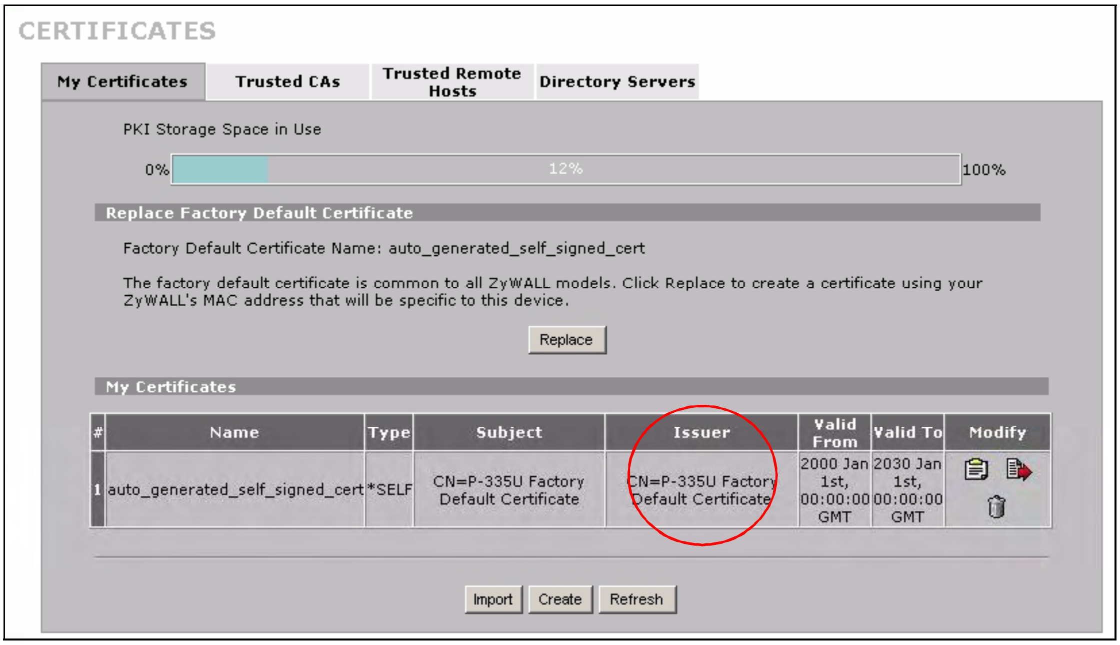
0% 11% 100%

My Certificates

#	Name	Type	Subject	Issuer	Valid From	Valid To	Modify
1	auto_generated_self_signed_cert	*SELF	CN=NBG410W3G 0013498B8B8B	CN=NBG410W3G 0013498B8B8B	2000 Jan 1st, 00:00:00 GMT	2030 Jan 1st, 00:00:00 GMT	

Click **Ignore** in the **Replace Certificate** screen to use the common ZyXEL Device certificate. You will then see this information in the **My Certificates** screen.

Figure 165 Common ZyXEL Device Certificate



CERTIFICATES

PKI Storage Space in Use

Replace Factory Default Certificate

Factory Default Certificate Name: auto_generated_self_signed_cert

The factory default certificate is common to all ZyWALL models. Click Replace to create a certificate using your ZyWALL's MAC address that will be specific to this device.

My Certificates

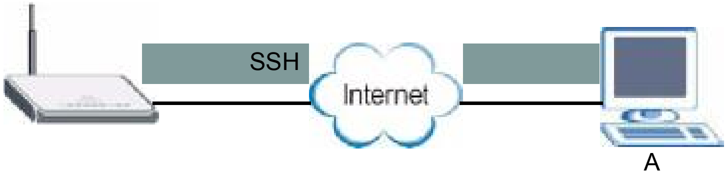
#	Name	Type	Subject	Issuer	Valid From	Valid To	Modify
1	auto_generated_self_signed_cert	*SELF	CN=P-335U Factory Default Certificate	CN=P-335U Factory Default Certificate	2000 Jan 1st, 00:00:00 GMT	2030 Jan 1st, 00:00:00 GMT	

15.5 SSH

You can use SSH (Secure SHell) to securely access the ZyXEL Device's command line interface. Specify which interfaces allow SSH access and from which IP address the access can come.

Unlike Telnet or FTP, which transmit data in plaintext (clear or unencrypted text), SSH is a secure communication protocol that combines authentication and data encryption to provide secure encrypted communication between two hosts over an unsecured network. In the following figure, computer **A** on the Internet uses SSH to securely connect to the WAN port of the ZyXEL Device for a management session.

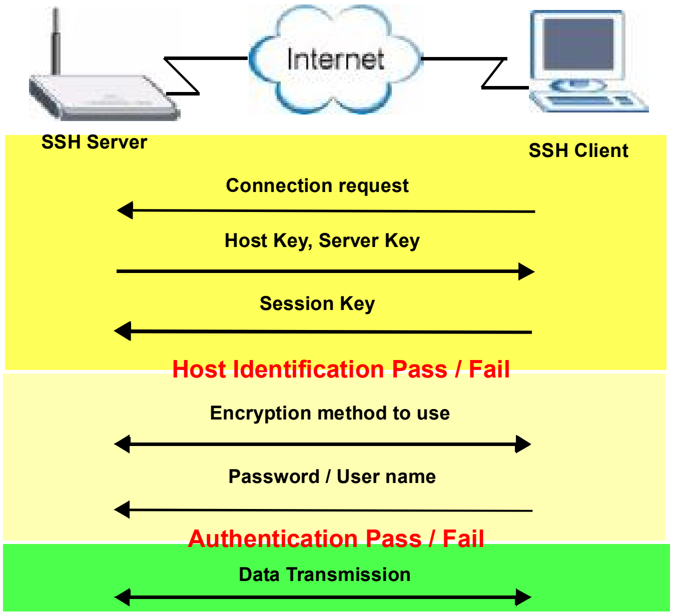
Figure 166 SSH Communication Over the WAN Example



15.6 How SSH Works

The following table summarizes how a secure connection is established between two remote hosts.

Figure 167 How SSH Works



1 Host Identification

The SSH client sends a connection request to the SSH server. The server identifies itself with a host key. The client encrypts a randomly generated session key with the host key and server key and sends the result back to the server.

The client automatically saves any new server public keys. In subsequent connections, the server public key is checked against the saved version on the client computer.

2 Encryption Method

Once the identification is verified, both the client and server must agree on the type of encryption method to use.

3 Authentication and Data Transmission

After the identification is verified and data encryption activated, a secure tunnel is established between the client and the server. The client then sends its authentication information (user name and password) to the server to log in to the server.

15.7 SSH Implementation on the ZyXEL Device

Your ZyXEL Device supports SSH version 1.5 using RSA authentication and three encryption methods (DES, 3DES and Blowfish). The SSH server is implemented on the ZyXEL Device for remote management and file transfer on port 22. Only one SSH connection is allowed at a time.

15.7.1 Requirements for Using SSH

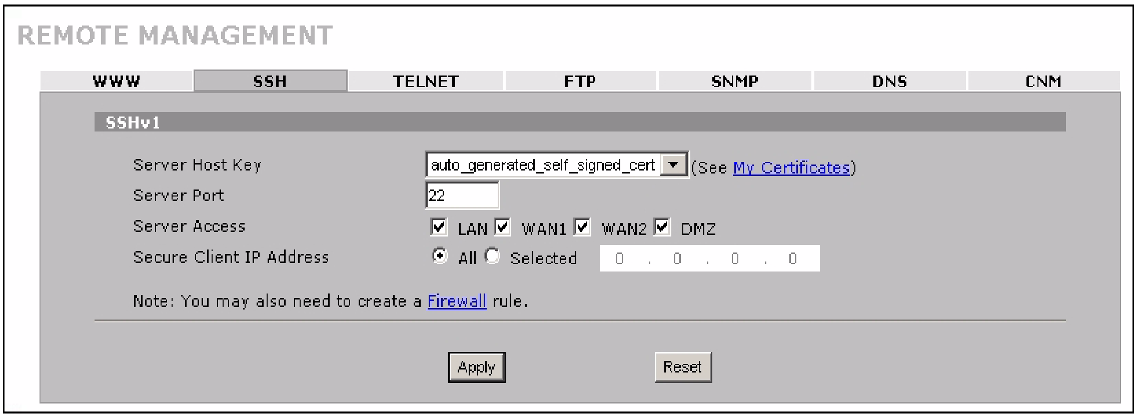
You must install an SSH client program on a client computer (Windows or Linux operating system) that is used to connect to the ZyXEL Device over SSH.

15.8 Configuring SSH

Click **ADVANCED** > **REMOTE MGMT** > **SSH** to change your ZyXEL Device's Secure Shell settings.

It is recommended that you disable Telnet and FTP when you configure SSH for secure connections.

Figure 168 ADVANCED > REMOTE MGMT > SSH



REMOTE MANAGEMENT

SSHv1

Server Host Key: auto_generated_self_signed_cert (See My Certificates)

Server Port: 22

Server Access: ☑ LAN ☑ WAN1 ☑ WAN2 ☑ DMZ

Secure Client IP Address: ● All ○ Selected 0 . 0 . 0 . 0

Note: You may also need to create a Firewall rule.

The following table describes the labels in this screen.

Table 77 ADVANCED > REMOTE MGMT > SSH

LABEL	DESCRIPTION
Server Host Key	Select the certificate whose corresponding private key is to be used to identify the ZyXEL Device for SSH connections. You must have certificates already configured in the **My Certificates** screen (Click **My Certificates** and see Chapter 11 on page 195 for details).
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Server Access	Select the interface(s) through which a computer may access the ZyXEL Device using this service.
Secure Client IP Address	A secure client is a "trusted" computer that is allowed to communicate with the ZyXEL Device using this service. Select **All** to allow any computer to access the ZyXEL Device using this service. Choose **Selected** to just allow the computer with the IP address that you specify to access the ZyXEL Device using this service.
Apply	Click **Apply** to save your customized settings and exit this screen.
Reset	Click **Reset** to begin configuring this screen afresh.

15.9 Secure Telnet Using SSH Examples

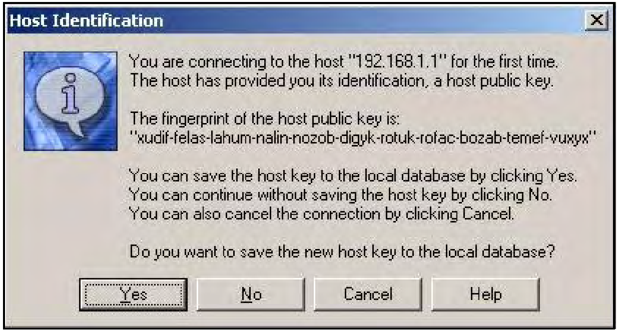
This section shows two examples using a command interface and a graphical interface SSH client program to remotely access the ZyXEL Device. The configuration and connection steps are similar for most SSH client programs. Refer to your SSH client program user's guide.

15.9.1 Example 1: Microsoft Windows

This section describes how to access the ZyXEL Device using the Secure Shell Client program.

1 Launch the SSH client and specify the connection information (IP address, port number or device name) for the ZyXEL Device.
2 Configure the SSH client to accept connection using SSH version 1.
3 A window displays prompting you to store the host key in you computer. Click **Yes** to continue.

Figure 169 SSH Example 1: Store Host Key



Host Identification

You are connecting to the host "192.168.1.1" for the first time.
The host has provided you its identification, a host public key.

The fingerprint of the host public key is:
"xudif-felas-lahum-nalin-nozob-digyk-rotuk-rofac-bozab-temef-vuxyx"

You can save the host key to the local database by clicking Yes.
You can continue without saving the host key by clicking No.
You can also cancel the connection by clicking Cancel.

Do you want to save the new host key to the local database?

Enter the password to log in to the ZyXEL Device. The CLI main menu displays next.

15.9.2 Example 2: Linux

This section describes how to access the ZyXEL Device using the OpenSSH client program that comes with most Linux distributions.

1 Test whether the SSH service is available on the ZyXEL Device.

Enter "`telnet 192.168.1.1 22`" at a terminal prompt and press [ENTER]. The computer attempts to connect to port 22 on the ZyXEL Device (using the default IP address of 192.168.1.1).

A message displays indicating the SSH protocol version supported by the ZyXEL Device.

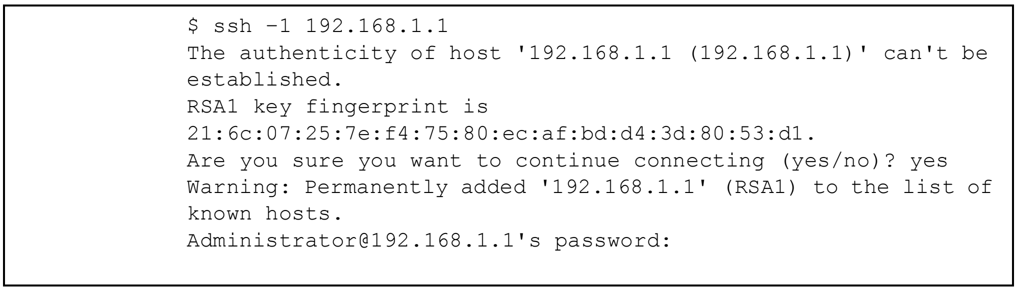
Figure 170 SSH Example 2: Test

```
$ telnet 192.168.1.1 22
Trying 192.168.1.1...
Connected to 192.168.1.1.
Escape character is '^]'.
SSH-1.5-1.0.0
```

2 Enter "`ssh -1 192.168.1.1`". This command forces your computer to connect to the ZyXEL Device using SSH version 1. If this is the first time you are connecting to the ZyXEL Device using SSH, a message displays prompting you to save the host information of the ZyXEL Device. Type "`yes`" and press **[ENTER]**.

Then enter the password to log in to the ZyXEL Device.

Figure 171 SSH Example 2: Log in



```
$ ssh -1 192.168.1.1
The authenticity of host '192.168.1.1 (192.168.1.1)' can't be
established.
RSA1 key fingerprint is
21:6c:07:25:7e:f4:75:80:ec:af:bd:d4:3d:80:53:d1.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.1.1' (RSA1) to the list of
known hosts.
Administrator@192.168.1.1's password:
```

3 The CLI main menu displays next.

15.10 Secure FTP Using SSH Example

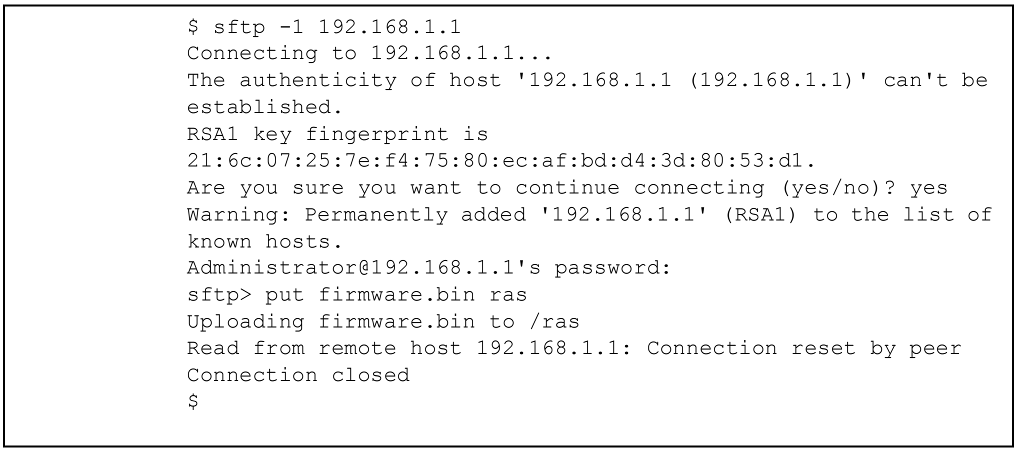
This section shows an example on file transfer using the OpenSSH client program. The configuration and connection steps are similar for other SSH client programs. Refer to your SSH client program user's guide.

1 Enter "`sftp -1 192.168.1.1`". This command forces your computer to connect to the ZyXEL Device for secure file transfer using SSH version 1. If this is the first time you are connecting to the ZyXEL Device using SSH, a message displays prompting you to save the host information of the ZyXEL Device. Type "`yes`" and press **[ENTER]**.

2 Enter the password to login to the ZyXEL Device.

3 Use the "`put`" command to upload a new firmware to the ZyXEL Device.

Figure 172 Secure FTP: Firmware Upload Example



```
$ sftp -1 192.168.1.1
Connecting to 192.168.1.1...
The authenticity of host '192.168.1.1 (192.168.1.1)' can't be
established.
RSA1 key fingerprint is
21:6c:07:25:7e:f4:75:80:ec:af:bd:d4:3d:80:53:d1.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.1.1' (RSA1) to the list of
known hosts.
Administrator@192.168.1.1's password:
sftp> put firmware.bin ras
Uploading firmware.bin to /ras
Read from remote host 192.168.1.1: Connection reset by peer
Connection closed
$
```

15.11 Telnet

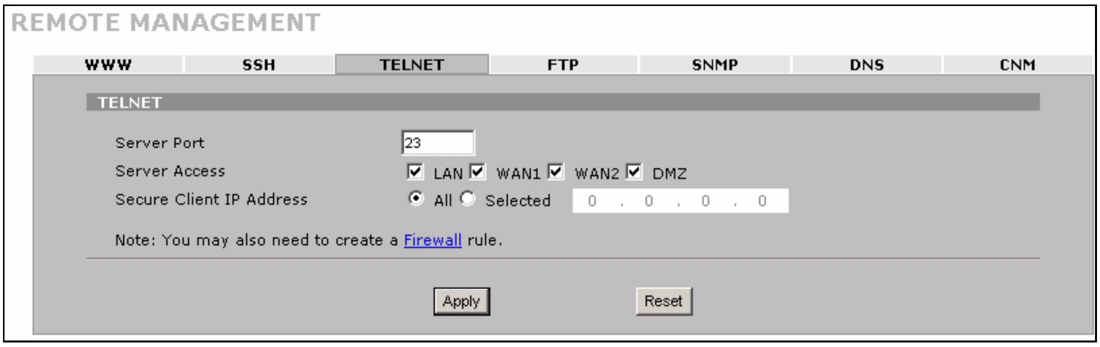
You can use Telnet to access the ZyXEL Device’s command line interface. Specify which interfaces allow Telnet access and from which IP address the access can come.

15.12 Configuring TELNET

Click **ADVANCED** > **REMOTE MGMT** > **TELNET** to open the following screen. Use this screen to specify which interfaces allow Telnet access and from which IP address the access can come.

It is recommended that you disable Telnet and FTP when you configure SSH for secure connections.

Figure 173 ADVANCED > REMOTE MGMT > Telnet



TELNET

Server Port 23

Server Access ☑ LAN ☑ WAN1 ☑ WAN2 ☑ DMZ

Secure Client IP Address ● All ○ Selected 0 . 0 . 0 . 0

Note: You may also need to create a Firewall rule.

The following table describes the labels in this screen.

Table 78 ADVANCED > REMOTE MGMT > Telnet

LABEL	DESCRIPTION
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Server Access	Select the interface(s) through which a computer may access the ZyXEL Device using this service.
Secure Client IP Address	A secure client is a "trusted" computer that is allowed to communicate with the ZyXEL Device using this service. Select **All** to allow any computer to access the ZyXEL Device using this service. Choose **Selected** to just allow the computer with the IP address that you specify to access the ZyXEL Device using this service.
Apply	Click **Apply** to save your customized settings and exit this screen.
Reset	Click **Reset** to begin configuring this screen afresh.

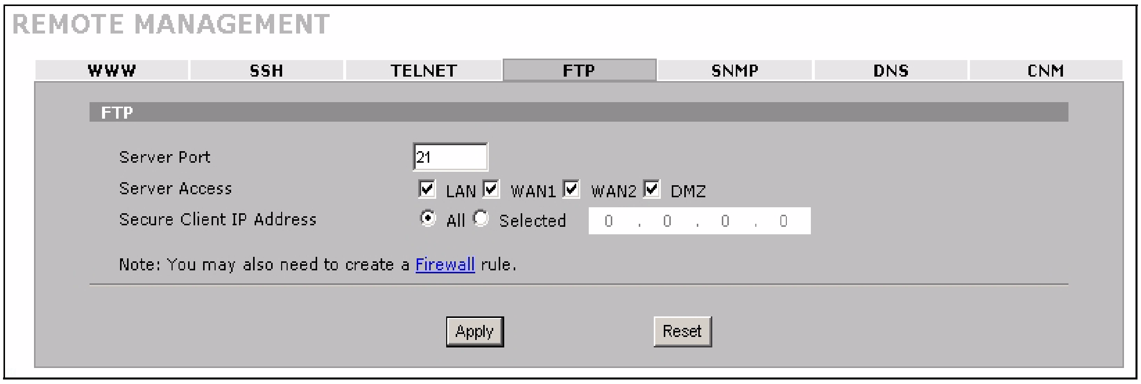
15.13 FTP

You can use FTP (File Transfer Protocol) to upload and download the ZyXEL Device's firmware and configuration files, please see the User's Guide chapter on firmware and configuration file maintenance for details. To use this feature, your computer must have an FTP client.

To change your ZyXEL Device's FTP settings, click **ADVANCED** > **REMOTE MGMT** > **FTP**. The screen appears as shown. Use this screen to specify which interfaces allow FTP access and from which IP address the access can come.

It is recommended that you disable Telnet and FTP when you configure SSH for secure connections.

Figure 174 ADVANCED > REMOTE MGMT > FTP



REMOTE MANAGEMENT

FTP

Server Port: 21

Server Access: ☑ LAN ☑ WAN1 ☑ WAN2 ☑ DMZ

Secure Client IP Address: ● All ○ Selected 0 . 0 . 0 . 0

Note: You may also need to create a Firewall rule.

The following table describes the labels in this screen.

Table 79 ADVANCED > REMOTE MGMT > FTP

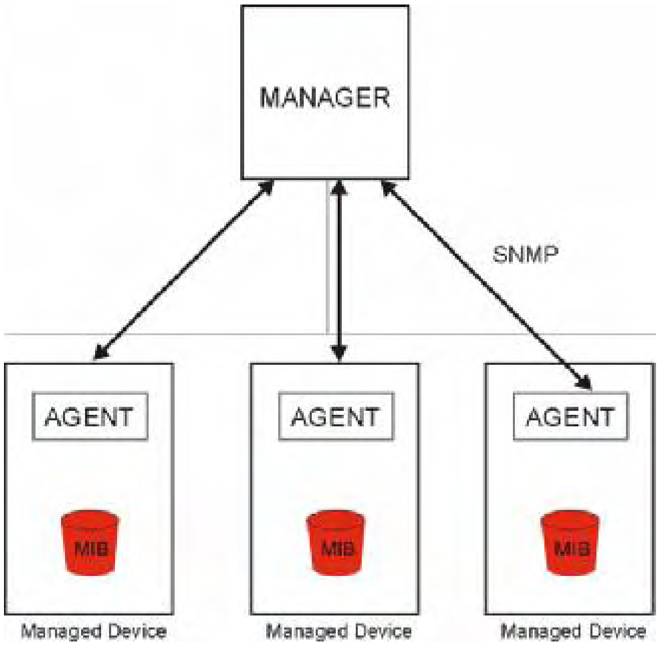
LABEL	DESCRIPTION
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Server Access	Select the interface(s) through which a computer may access the ZyXEL Device using this service.
Secure Client IP Address	A secure client is a “trusted” computer that is allowed to communicate with the ZyXEL Device using this service. Select **All** to allow any computer to access the ZyXEL Device using this service. Choose **Selected** to just allow the computer with the IP address that you specify to access the ZyXEL Device using this service.
Apply	Click **Apply** to save your customized settings.
Reset	Click **Reset** to begin configuring this screen afresh.

15.14 SNMP

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

SNMP is only available if TCP/IP is configured.

Figure 175 SNMP Management Model



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

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

The managed devices contain object variables/managed objects that define each piece of information to be collected about a device. Examples of variables include such as number of packets received, node port status etc. A Management Information Base (MIB) is a collection of managed objects. SNMP allows a manager and agents to communicate for the purpose of accessing these objects.

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

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

15.14.1 Supported MIBs

The ZyXEL Device supports MIB II that is defined in RFC-1213 and RFC-1215. The focus of the MIBs is to let administrators collect statistical data and monitor status and performance.

15.14.2 SNMP Traps

The ZyXEL Device will send traps to the SNMP manager when any one of the following events occurs:

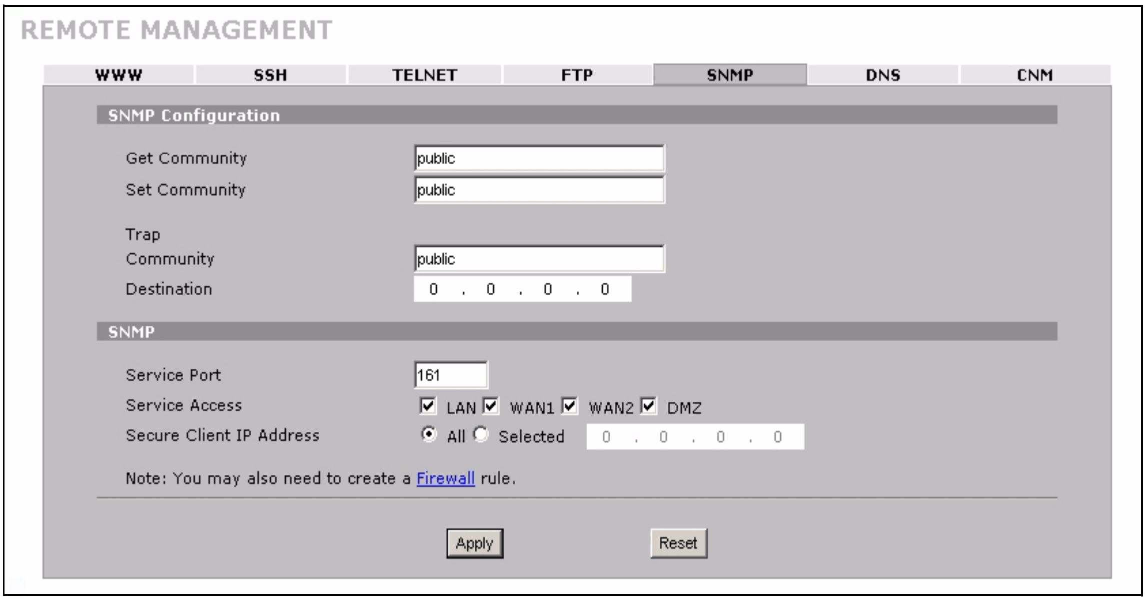
Table 80 SNMP Traps

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

15.14.3 REMOTE MANAGEMENT: SNMP

To change your ZyXEL Device's SNMP settings, click **ADVANCED** > **REMOTE MGMT** > **SNMP**. The screen appears as shown.

Figure 176 ADVANCED > REMOTE MGMT > SNMP



SNMP Configuration

Get Community	public
Set Community	public
Trap	
Community	public
Destination	0 . 0 . 0 . 0

SNMP

Service Port	161
Service Access	☑ LAN ☑ WAN1 ☑ WAN2 ☑ DMZ
Secure Client IP Address	● All ○ Selected 0 . 0 . 0 . 0

Note: You may also need to create a Firewall rule.

The following table describes the labels in this screen.

Table 81 ADVANCED > REMOTE MGMT > SNMP

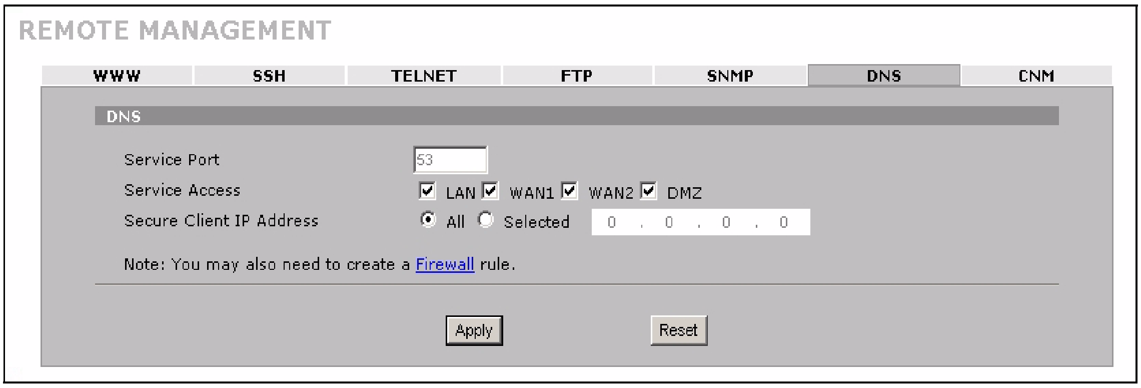
LABEL	DESCRIPTION
SNMP Configuration	
Get Community	Enter the **Get Community**, which is the password for the incoming Get and GetNext requests from the management station. The default is public and allows all requests.
Set Community	Enter the **Set community**, which is the password for incoming Set requests from the management station. The default is public and allows all requests.
Trap	
Community	Type the trap community, which is the password sent with each trap to the SNMP manager. The default is public and allows all requests.
Destination	Type the IP address of the station to send your SNMP traps to.
SNMP	
Service Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Service Access	Select the interface(s) through which a computer may access the ZyXEL Device using this service.
Secure Client IP Address	A secure client is a "trusted" computer that is allowed to communicate with the ZyXEL Device using this service. Select **All** to allow any computer to access the ZyXEL Device using this service. Choose **Selected** to just allow the computer with the IP address that you specify to access the ZyXEL Device using this service.
Apply	Click **Apply** to save your customized settings.
Reset	Click **Reset** to begin configuring this screen afresh.

15.15 DNS

Use DNS (Domain Name System) to map a domain name to its corresponding IP address and vice versa. Refer to Chapter 6 on page 111 for more information.

Click **ADVANCED** > **REMOTE MGMT** > **DNS** to change your ZyXEL Device's DNS settings. Use this screen to set from which IP address the ZyXEL Device will accept DNS queries and on which interface it can send them your ZyXEL Device's DNS settings.

Figure 177 ADVANCED > REMOTE MGMT > DNS



REMOTE MANAGEMENT

DNS

Service Port: 53

Service Access: ☑ LAN ☑ WAN1 ☑ WAN2 ☑ DMZ

Secure Client IP Address: ● All ○ Selected 0 . 0 . 0 . 0

Note: You may also need to create a Firewall rule.

The following table describes the labels in this screen.

Table 82 ADVANCED > REMOTE MGMT > DNS

LABEL	DESCRIPTION
Server Port	The DNS service port number is 53 and cannot be changed here.
Service Access	Select the interface(s) through which a computer may send DNS queries to the ZyXEL Device.
Secure Client IP Address	A secure client is a “trusted” computer that is allowed to send DNS queries to the ZyXEL Device. Select **All** to allow any computer to send DNS queries to the ZyXEL Device. Choose **Selected** to just allow the computer with the IP address that you specify to send DNS queries to the ZyXEL Device.
Apply	Click **Apply** to save your customized settings.
Reset	Click **Reset** to begin configuring this screen afresh.

15.16 Introducing Vantage CNM

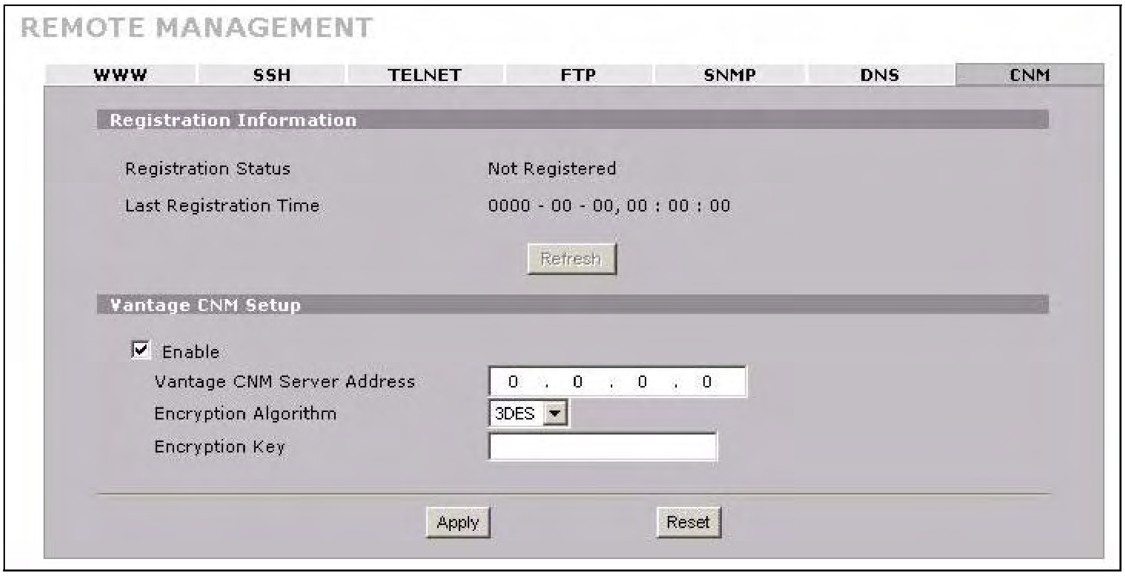
Vantage CNM (Centralized Network Management) is a browser-based global management solution that allows an administrator from any location to easily configure, manage, monitor and troubleshoot ZyXEL devices located worldwide. See the Vantage CNM User's Guide for details.

If you allow your ZyXEL Device to be managed by the Vantage CNM server, then you should not do any configurations directly to the ZyXEL Device (using either the web configurator or commands) without notifying the Vantage CNM administrator.

15.17 Configuring CNM

Vantage CNM is disabled on the device by default. Click **ADVANCED** > **REMOTE MGMT** > **CNM** to configure your device’s Vantage CNM settings.

Figure 178 ADVANCED > REMOTE MGMT > CNM



REMOTE MANAGEMENT

Registration Information

Registration Status: Not Registered

Last Registration Time: 0000 - 00 - 00, 00 : 00 : 00

Vantage CNM Setup

☑ Enable

Vantage CNM Server Address: 0 . 0 . 0 . 0

Encryption Algorithm: 3DES

Encryption Key:

The following table describes the labels in this screen.

Table 83 ADVANCED > REMOTE MGMT > CNM

LABEL	DESCRIPTION
Registration Information	
Registration Status	This read only field displays **Not Registered** when **Enable** is not selected. It displays **Registering** when the ZyXEL Device first connects with the Vantage CNM server and then **Registered** after it has been successfully registered with the Vantage CNM server. It will continue to display **Registering** until it successfully registers with the Vantage CNM server. It will not be able to register with the Vantage CNM server if: The Vantage CNM server is down. The Vantage CNM server IP address is incorrect. The Vantage CNM server is behind a NAT router or firewall that does not forward packets through to the Vantage CNM server. The encryption algorithms and/or encryption keys do not match between the ZyXEL Device and the Vantage CNM server.
Last Registration Time	This field displays the last date (year-month-date) and time (hours-minutes-seconds) that the ZyXEL Device registered with the Vantage CNM server. It displays all zeroes if it has not yet registered with the Vantage CNM server.
Refresh	Click **Refresh** to update the registration status and last registration time.
Vantage CNM Setup	
Enable	Select this check box to allow Vantage CNM to manage your ZyXEL Device.
Vantage CNM Server Address	If the Vantage server is on the same subnet as the ZyXEL Device, enter the private or public IP address of the Vantage server. If the Vantage CNM server is on a different subnet to the ZyXEL Device, enter the public IP address of the Vantage server. If the Vantage CNM server is on a different subnet to the ZyXEL Device and is behind a NAT router, enter the WAN IP address of the NAT router here.

Table 83 ADVANCED > REMOTE MGMT > CNM (continued)

LABEL	DESCRIPTION
Encryption Algorithm	The **Encryption Algorithm** field is used to encrypt communications between the ZyXEL Device and the Vantage CNM server. Choose from **None** (no encryption), **DES** or **3DES**. The **Encryption Key** field appears when you select **DES** or **3DES**. The ZyXEL Device must use the same encryption algorithm as the Vantage CNM server.
Encryption Key	Type eight alphanumeric characters ("0" to "9", "a" to "z" or "A" to "Z") when you choose the **DES** encryption algorithm and 24 alphanumeric characters ("0" to "9", "a" to "z" or "A" to "Z") when you choose the **3DES** encryption algorithm. The ZyXEL Device must use the same encryption key as the Vantage CNM server.
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to begin configuring this screen afresh.

15.17.1 Additional Configuration for Vantage CNM

If you have NAT routers or firewalls between the ZyXEL Device and the Vantage CNM server, you must configure them to forward TCP ports 8080 (HTTP), 443 (HTTPS) and 20 and 21 (FTP). They must also forward UDP ports 1864 and 1865.

16

UPnP

This chapter introduces the Universal Plug and Play feature.

16.1 Universal Plug and Play Overview

Universal Plug and Play (UPnP) is a distributed, open networking standard that uses TCP/IP for simple peer-to-peer network connectivity between devices. A UPnP device can dynamically join a network, obtain an IP address, convey its capabilities and learn about other devices on the network. In turn, a device can leave a network smoothly and automatically when it is no longer in use.

16.1.1 How Do I Know If I'm Using UPnP?

UPnP hardware is identified as an icon in the Network Connections folder (Windows XP). Each UPnP compatible device installed on your network will appear as a separate icon. Selecting the icon of a UPnP device will allow you to access the information and properties of that device.

16.1.2 NAT Traversal

UPnP NAT traversal automates the process of allowing an application to operate through NAT. UPnP network devices can automatically configure network addressing, announce their presence in the network to other UPnP devices and enable exchange of simple product and service descriptions. NAT traversal allows the following:

- Dynamic port mapping
- Learning public IP addresses
- Assigning lease times to mappings

Windows Messenger is an example of an application that supports NAT traversal and UPnP.

See Chapter 12 on page 225 for further information about NAT.

16.1.3 Cautions with UPnP

The automated nature of NAT traversal applications in establishing their own services and opening firewall ports may present network security issues. Network information and configuration may also be obtained and modified by users in some network environments.

When a UPnP device joins a network, it announces its presence with a multicast message. For security reasons, the ZyXEL Device allows multicast messages on the LAN only.

All UPnP-enabled devices may communicate freely with each other without additional configuration. Disable UPnP if this is not your intention.

16.1.4 UPnP and ZyXEL

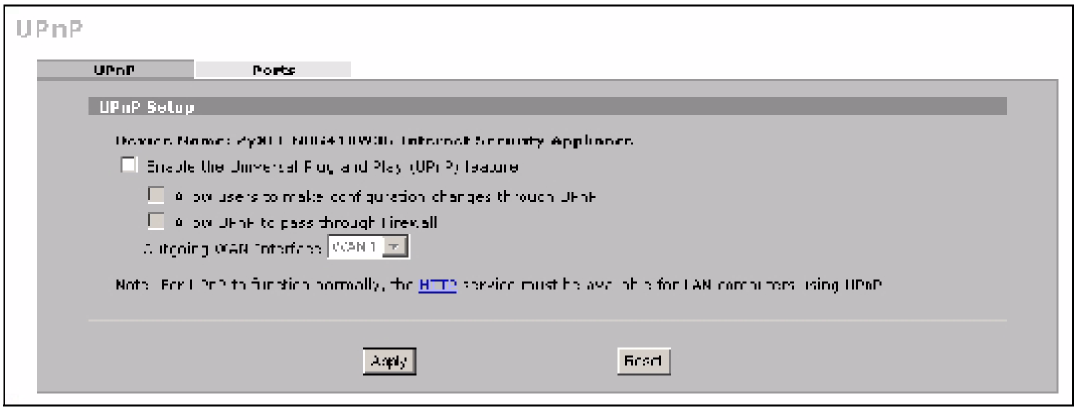
ZyXEL has achieved UPnP certification from the Universal Plug and Play Forum UPnP™ Implementers Corp. (UIC). ZyXEL's UPnP implementation supports IGD 1.0 (Internet Gateway Device).

See the following sections for examples of installing and using UPnP.

16.2 Configuring UPnP

Click **ADVANCED** > **UPnP** to display the **UPnP** screen.

Figure 179 ADVANCED > UPnP



UPnP

Device Name: ZyXEL NBG410W3G Internet Security Appliance

□ Enable the Universal Plug and Play (UPnP) feature

□ Allow users to make configuration changes through UPnP

□ Allow UPnP to pass through Firewall

Outgoing WAN Interface: WAN 1

Note: For UPnP to function normally, the HTTP service must be available for LAN computers using UPnP.

The following table describes the fields in this screen.

Table 84 ADVANCED > UPnP

LABEL	DESCRIPTION
UPnP Setup	
Device Name	This identifies the ZyXEL device in UPnP applications.
Enable the Universal Plug and Play (UPnP) feature	Select this check box to activate UPnP. Be aware that anyone could use a UPnP application to open the web configurator's login screen without entering the ZyXEL Device's IP address (although you must still enter the password to access the web configurator).
Allow users to make configuration changes through UPnP	Select this check box to allow UPnP-enabled applications to automatically configure the ZyXEL Device so that they can communicate through the ZyXEL Device, for example by using NAT traversal, UPnP applications automatically reserve a NAT forwarding port in order to communicate with another UPnP enabled device; this eliminates the need to manually configure port forwarding for the UPnP enabled application.
Allow UPnP to pass through Firewall	Select this check box to allow traffic from UPnP-enabled applications to bypass the firewall. Clear this check box to have the firewall block all UPnP application packets (for example, MSN packets).

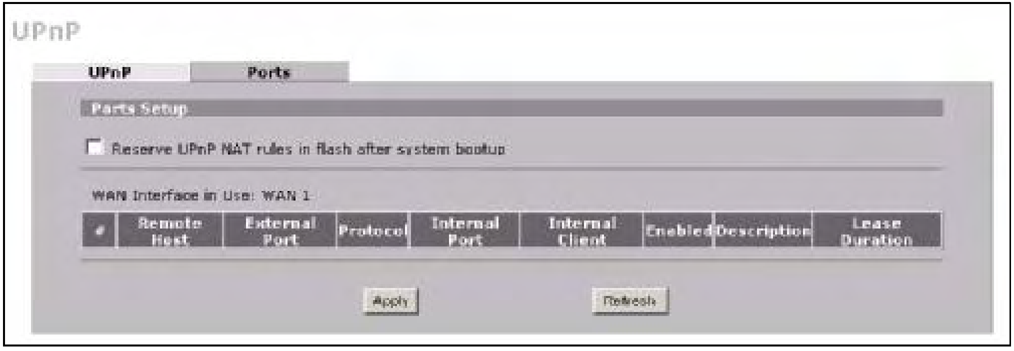
Table 84 ADVANCED > UPnP

LABEL	DESCRIPTION
Outgoing WAN Interface	Select through which WAN port you want to send out traffic from UPnP-enabled applications. If the WAN port you select loses its connection, the ZyXEL Device attempts to use the other WAN port. If the other WAN port also does not work, the ZyXEL Device drops outgoing packets from UPnP-enabled applications.
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to begin configuring this screen afresh.

16.3 Displaying UPnP Port Mapping

Click **ADVANCED** > **UPnP** > **Ports** to display the UPnP **Ports** screen. Use this screen to view the NAT port mapping rules that UPnP creates on the ZyXEL Device.

Figure 180 ADVANCED > UPnP > Ports



UPnP

UPnP | Ports

Ports Setup

☐ Reserve UPnP NAT rules in flash after system bootup

WAN Interface in Use: WAN 1

#	Remote Host	External Port	Protocol	Internal Port	Internal Client	Enabled	Description	Lease Duration

Apply | Refresh

The following table describes the labels in this screen.

Table 85 ADVANCED > UPnP > Ports

LABEL	DESCRIPTION
Reserve UPnP NAT rules in flash after system bootup	Select this check box to have the ZyXEL Device retain UPnP created NAT rules even after restarting. If you use UPnP and you set a port on your computer to be fixed for a specific service (for example FTP for file transfers), this option allows the ZyXEL Device to keep a record when your computer uses UPnP to create a NAT forwarding rule for that service.
WAN Interface in Use	This field displays through which WAN interface the ZyXEL Device is currently sending out traffic from UPnP-enabled applications. This field displays **None** when UPnP is disabled or neither of the WAN ports has a connection.
The following read-only table displays information about the UPnP-created NAT mapping rule entries in the ZyXEL Device's NAT routing table.	
#	This is the index number of the UPnP-created NAT mapping rule entry.
Remote Host	This field displays the source IP address (on the WAN) of inbound IP packets. Since this is often a wildcard, the field may be blank. When the field is blank, the ZyXEL Device forwards all traffic sent to the **External Port** on the WAN interface to the **Internal Client** on the **Internal Port**. When this field displays an external IP address, the NAT rule has the ZyXEL Device forward inbound packets to the **Internal Client** from that IP address only.

Table 85 ADVANCED > UPnP > Ports (continued)

LABEL	DESCRIPTION
External Port	This field displays the port number that the ZyXEL Device “listens” on (on the WAN port) for connection requests destined for the NAT rule’s **Internal Port** and **Internal Client**. The ZyXEL Device forwards incoming packets (from the WAN) with this port number to the **Internal Client** on the **Internal Port** (on the LAN). If the field displays “0”, the ZyXEL Device ignores the **Internal Port** value and forwards requests on all external port numbers (that are otherwise unmapped) to the **Internal Client**.
Protocol	This field displays the protocol of the NAT mapping rule (TCP or UDP).
Internal Port	This field displays the port number on the **Internal Client** to which the ZyXEL Device should forward incoming connection requests.
Internal Client	This field displays the DNS host name or IP address of a client on the LAN. Multiple NAT clients can use a single port simultaneously if the internal client field is set to 255.255.255.255 for UDP mappings.
Enabled	This field displays whether or not this UPnP-created NAT mapping rule is turned on. The UPnP-enabled device that connected to the ZyXEL Device and configured the UPnP-created NAT mapping rule on the ZyXEL Device determines whether or not the rule is enabled.
Description	This field displays a text explanation of the NAT mapping rule.
Lease Duration	This field displays a dynamic port-mapping rule’s time to live (in seconds). It displays “0” if the port mapping is static.
Apply	Click **Apply** to save your changes.
Refresh	Click **Refresh** update the screen’s table.

16.4 Installing UPnP in Windows Example

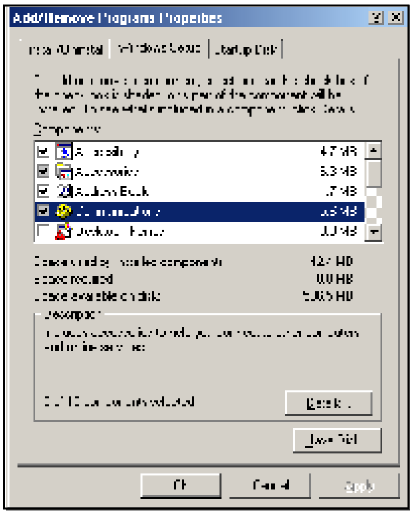
This section shows how to install UPnP in Windows Me and Windows XP.

16.4.1 Installing UPnP in Windows Me

Follow the steps below to install UPnP in Windows Me.

1 Click **Start**, **Settings** and **Control Panel**. Double-click **Add/Remove Programs**.

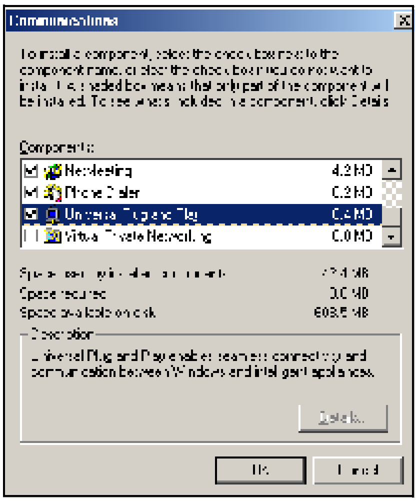
2 Click on the **Windows Setup** tab and select **Communication** in the **Components** selection box. Click **Details**.



3 In the **Communications** window, select the **Universal Plug and Play** check box in the **Components** selection box.

4 Click **OK** to go back to the **Add/Remove Programs Properties** window and click **Next**.

5 Restart the computer when prompted.


Communications
Components:
☑ NetMeeting 4.2 MB
☑ Phone Dialer 0.2 MB
☑ Universal Plug and Play 0.4 MB
☐ Virtual Private Networking 0.0 MB
Space required 0.0 MB
Description
Universal Plug and Play enables seamless connectivity and communication between Windows and intelligent appliances.
Details...
OK
Cancel

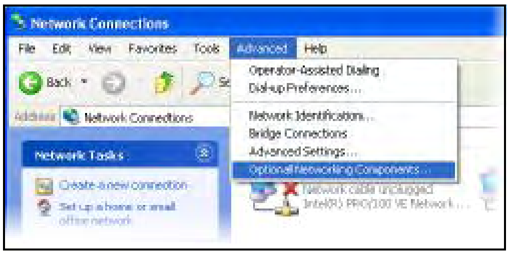
16.4.2 Installing UPnP in Windows XP

Follow the steps below to install UPnP in Windows XP.

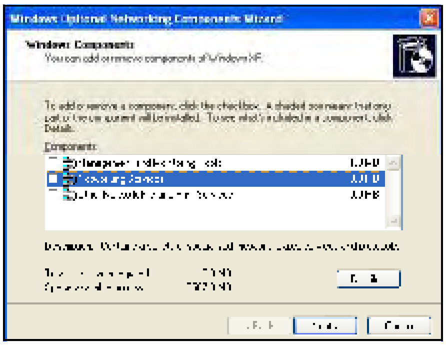
1 Click **Start**, **Settings** and **Control Panel**.

2 Double-click **Network Connections**.

3 In the **Network Connections** window, click **Advanced** in the main menu and select **Optional Networking Components ….**
The **Windows Optional Networking Components Wizard** window displays.



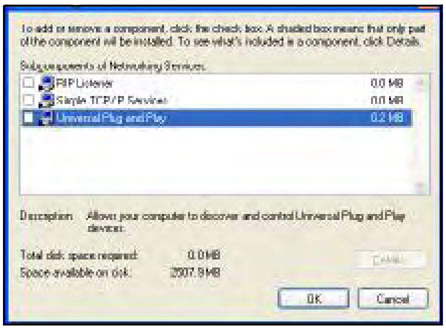
4 Select **Networking Service** in the **Components** selection box and click **Details**.


Windows Optional Networking Components Wizard

Windows Components
You can add or remove components of Windows XP.

5 In the **Networking Services** window, select the **Universal Plug and Play** check box.

6 Click **OK** to go back to the **Windows Optional Networking Component Wizard** window and click **Next**.


To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Subcomponents of Networking Services:

□ RIP Listener	0.0 MB
□ Simple TCP/IP Services	0.0 MB
□ Universal Plug and Play	0.2 MB

Description: Allows your computer to discover and control Universal Plug and Play devices.

Total disk space required: 0.0 MB
Space available on disk: 2507.9 MB

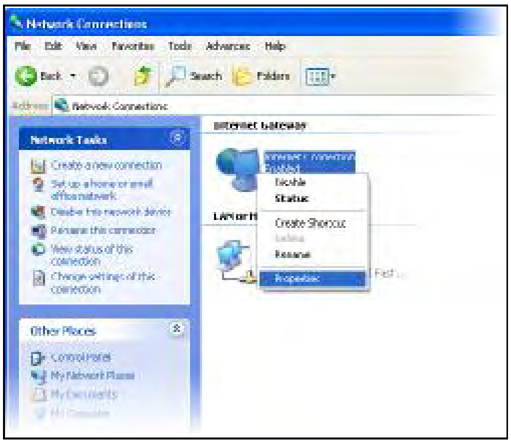
16.5 Using UPnP in Windows XP Example

This section shows you how to use the UPnP feature in Windows XP. You must already have UPnP installed in Windows XP and UPnP activated on the ZyXEL device.

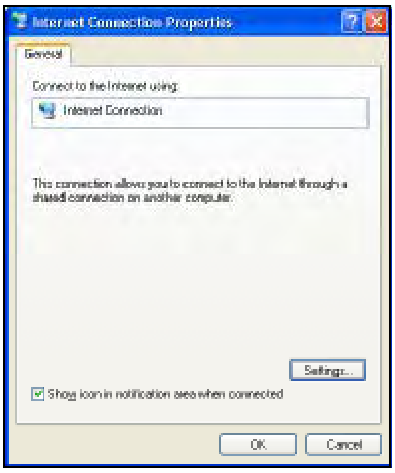
Make sure the computer is connected to a LAN port of the ZyXEL device. Turn on your computer and the ZyXEL device.

16.5.1 Auto-discover Your UPnP-enabled Network Device

1. Click **Start** and **Control Panel**. Double-click **Network Connections**. An icon displays under **Internet Gateway**.
2. Right-click the icon and select **Properties**.


Network Connections
File Edit View Favorites Tools Advanced Help
Back Search Folders
Address Network Connections
Network Tasks
Create a new connection
Set up a home or small office network
Disable this network device
Rename this connection
View status of this connection
Change settings of this connection
Other Places
Control Panel
My Network Places
My Documents
My Computer
Internet Gateway
Internet Connection Enabled
Disable
Status
Create Shortcut
Delete
Rename
Properties
LAN or High-Speed Internet

3. In the **Internet Connection Properties** window, click **Settings** to see the port mappings that were automatically created.



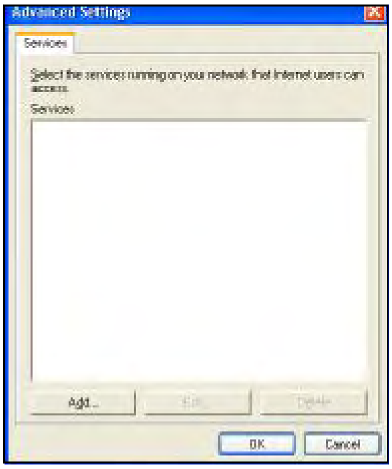
Connect to the Internet using:

Internet Connection

This connection allows you to connect to the Internet through a shared connection on another computer.

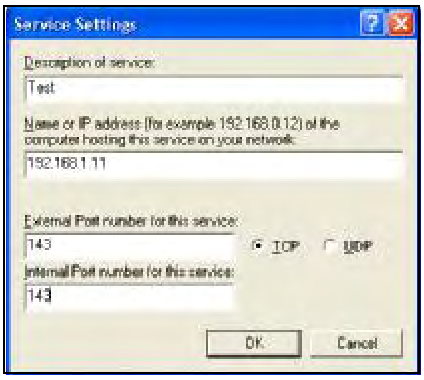
☑ Show icon in notification area when connected

You may edit or delete the port mappings or click **Add** to manually add port mappings.



Select the services running on your network that Internet users can access.

Services



Service Settings

Description of service:
Test

Name or IP address (for example 192.168.0.12) of the computer hosting this service on your network:
192.168.1.11

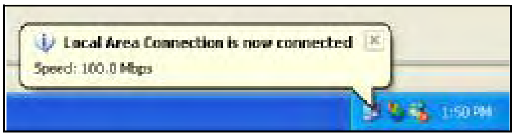
External Port number for this service:
143

● TCP ○ UDP

Internal Port number for this service:
143

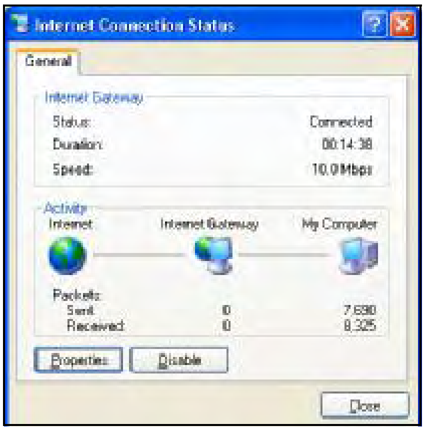
When the UPnP-enabled device is disconnected from your computer, all port mappings will be deleted automatically.

4 Select the **Show icon in notification area when connected** check box and click **OK**. An icon displays in the system tray.



Local Area Connection is now connected
Speed: 100.0 Mbps

5 Double-click the icon to display your current Internet connection status.



Internet Connection Status

General

Internet Gateway

Status:	Connected
Duration:	00:14:38
Speed:	10.0 Mbps

Activity

	Internet	Internet Gateway	My Computer
Packets:			
Sent		0	7,690
Received		0	8,325

16.5.2 Web Configurator Easy Access

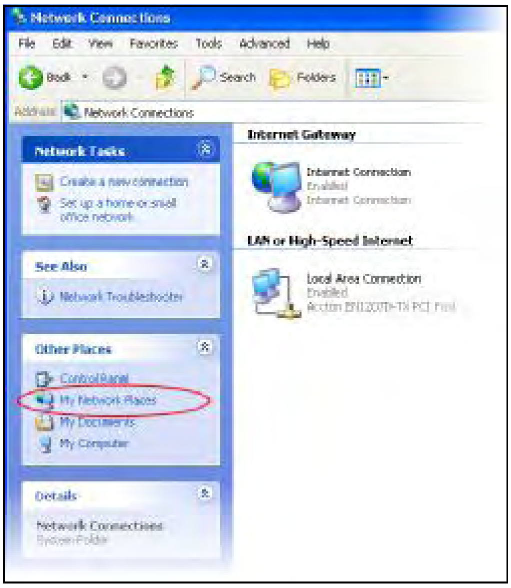
With UPnP, you can access the web-based configurator on the ZyXEL device without finding out the IP address of the ZyXEL device first. This is helpful if you do not know the IP address of the ZyXEL device.

Follow the steps below to access the web configurator.

1 Click **Start** and then **Control Panel**.

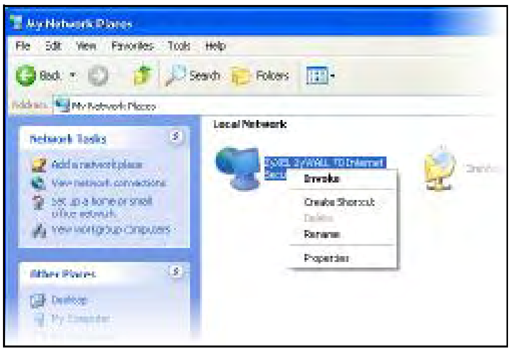
2 Double-click **Network Connections**.

3 Select **My Network Places** under **Other Places**.

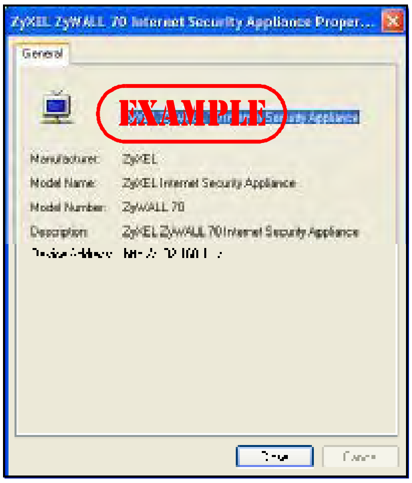


4 An icon with the description for each UPnP-enabled device displays under **Local Network**.

5 Right-click the icon for your ZyXEL device and select **Invoke**. The web configurator login screen displays.



6 Right-click the icon for your ZyXEL device and select **Properties**. A properties window displays with basic information about the ZyXEL device.



Manufacturer: ZyXEL

Model Name: ZyXEL Internet Security Appliance

Model Number: ZyWALL 70

Description: ZyXEL ZyWALL 70 Internet Security Appliance

Device Address: [illegible]

17

Custom Application

This chapter covers how to set the ZyXEL Device's to monitor custom port numbers for specific applications.

17.1 Custom Application

Use custom application to have the ZyXEL Device's ALG feature monitor traffic on custom ports, in addition to the default ports.

By default, these ZyXEL Device features monitor traffic for the following protocols on these port numbers.

- FTP: 21
- SIP: 5060
- H.323: 1720
- SMTP: 25
- POP3: 110
- HTTP: 80

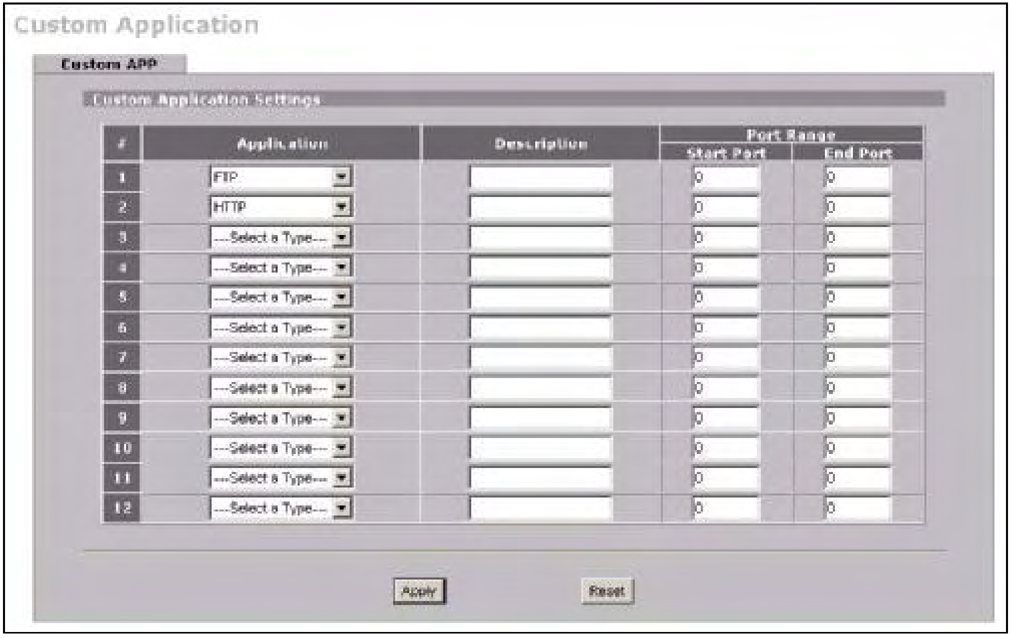
Changes in the **Custom APP** screen do not apply to the firewall.

17.2 Custom Application Configuration

Click **ADVANCED** > **Custom APP** to open the **Custom Application** screen.

This screen only specifies what port numbers the ZyXEL Device checks for specific protocol traffic. Use other screens to enable or disable the monitoring of the protocol traffic.

Figure 181 ADVANCED > Custom APP



Custom Application

Custom APP

Custom Application Settings

#	Application	Description	Port Range	
			Start Port	End Port
1	FTP		0	0
2	HTTP		0	0
3	---Select a Type---		0	0
4	---Select a Type---		0	0
5	---Select a Type---		0	0
6	---Select a Type---		0	0
7	---Select a Type---		0	0
8	---Select a Type---		0	0
9	---Select a Type---		0	0
10	---Select a Type---		0	0
11	---Select a Type---		0	0
12	---Select a Type---		0	0

The following table describes the labels in this screen.

Table 86 ADVANCED > Custom APP

LABEL	DESCRIPTION
Application	Select the application for which you want the ZyXEL Device to monitor specific ports. You can use the same application in more than one entry. To remove an entry, select **Select a Type**.
Description	Enter information about the reason for monitoring custom port numbers for this protocol.
Start Port	Enter the starting port for the range that the ZyXEL Device is to monitor for this application. If you are only entering a single port number, enter it here.
End Port	Enter the ending port for the range that the ZyXEL Device is to monitor for this application.
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to begin configuring this screen afresh.

18

ALG Screen

This chapter covers how to use the ZyXEL Device's ALG feature to allow certain applications to pass through the ZyXEL Device.

18.1 ALG Introduction

An Application Layer Gateway (ALG) manages a specific protocol (such as SIP, H.323 or FTP) at the application layer. The ZyXEL Device can function as an ALG to allow certain NAT un-friendly applications (such as SIP) to operate properly through the ZyXEL Device.

Some applications cannot operate through NAT (are NAT un-friendly) because they embed IP addresses and port numbers in their packets' data payload. The ZyXEL Device examines and uses IP address and port number information embedded in the data stream. When a device behind the ZyXEL Device uses an application for which the ZyXEL Device has ALG service enabled, the ZyXEL Device translates the device's private IP address inside the data stream to a public IP address. It also records session port numbers and dynamically creates implicit NAT port forwarding and firewall rules for the application's traffic to come in from the WAN to the LAN.

18.1.1 ALG and NAT

The ZyXEL Device dynamically creates an implicit NAT session for the application's traffic from the WAN to the LAN.

The ALG on the ZyXEL Device supports all NAT mapping types, including **One to One**, **Many to One**, **Many to Many Overload** and **Many One to One**.

18.1.2 ALG and the Firewall

The ZyXEL Device uses the dynamic port that the session uses for data transfer in creating an implicit temporary firewall rule for the session's traffic. The firewall rule only allows the session's traffic to go through in the direction that the ZyXEL Device determines from its inspection of the data payload of the application's packets. The firewall rule is automatically deleted after the application's traffic has gone through.

18.1.3 ALG and Multiple WAN

When the ZyXEL Device has two WAN interfaces and uses the second highest priority WAN interfaces as a back up, traffic cannot pass through when the primary WAN connection fails. The ZyXEL Device does not automatically change the connection to the secondary WAN interfaces.

If the primary WAN connection fails, the client needs to re-initialize the connection through the secondary WAN interfaces to have the connection go through the secondary WAN interfaces.

18.2 FTP

File Transfer Protocol (FTP) is an Internet file transfer service that operates on the Internet and over TCP/IP networks. A system running the FTP server accepts commands from a system running an FTP client. The service allows users to send commands to the server for uploading and downloading files. The FTP ALG allows TCP packets with a port 21 destination to pass through. If the FTP server is located on the LAN, you must also configure NAT port forwarding and firewall rules if you want to allow access to the server from the WAN.

18.3 H.323

H.323 is a standard teleconferencing protocol suite that provides audio, data and video conferencing. It allows for real-time point-to-point and multipoint communication between client computers over a packet-based network that does not provide a guaranteed quality of service. NetMeeting uses H.323.

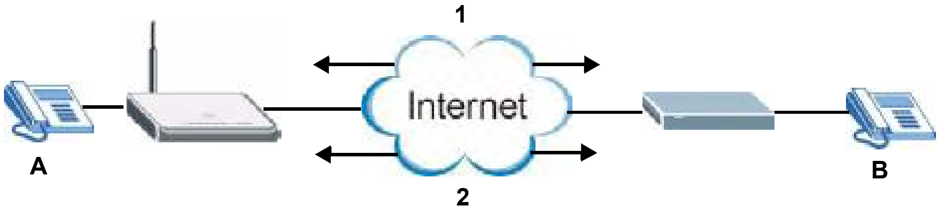
18.4 RTP

When you make a VoIP call using H.323 or SIP, the RTP (Real time Transport Protocol) is used to handle voice data transfer. See RFC 1889 for details on RTP.

18.4.1 H.323 ALG Details

- The H.323 ALG supports peer-to-peer H.323 calls.
- The H.323 ALG handles H.323 calls that go through NAT or that the ZyXEL Device routes. You can also make other H.323 calls that do not go through NAT or routing. Examples would be calls between LAN IP addresses that are on the same subnet.
- The H.323 ALG allows calls to go out through NAT. For example, you could make a call from a private IP address on the LAN to a peer device on the WAN.
- You must configure the firewall and port forwarding to allow incoming (peer-to-peer) calls from the WAN to a private IP address on the LAN or DMZ. The following example shows H.323 signaling (1) and audio (2) sessions between H.323 devices A and B.

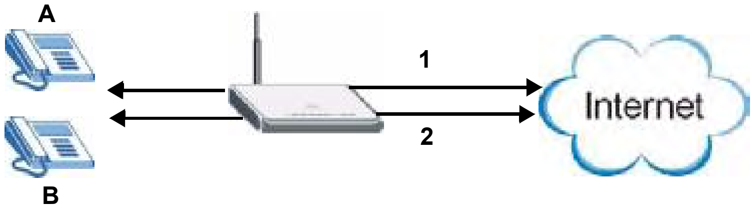
Figure 182 H.323 ALG Example



- With multiple WAN IP addresses on the ZyXEL Device, you can configure different firewall and port forwarding rules to allow incoming calls from each WAN IP address to go to a specific IP address on the LAN or DMZ.

  For example, you configure firewall and port forwarding rules to allow LAN IP address **A** to receive calls through public WAN IP address **1**. You configure different firewall and port forwarding rules to allow LAN IP address **B** to receive calls through public WAN IP address **2**.

Figure 183 H.323 with Multiple WAN IP Addresses



- The H.323 ALG operates on TCP packets with a port 1720 destination.
- The ZyXEL Device allows H.323 audio connections.

18.5 SIP

The Session Initiation Protocol (SIP) is an application-layer control (signaling) protocol that handles the setting up, altering and tearing down of voice and multimedia sessions over the Internet. SIP is used in VoIP (Voice over IP), the sending of voice signals over the Internet Protocol.

SIP signaling is separate from the media for which it handles sessions. The media that is exchanged during the session can use a different path from that of the signaling. SIP handles telephone calls and can interface with traditional circuit-switched telephone networks.

18.5.1 STUN

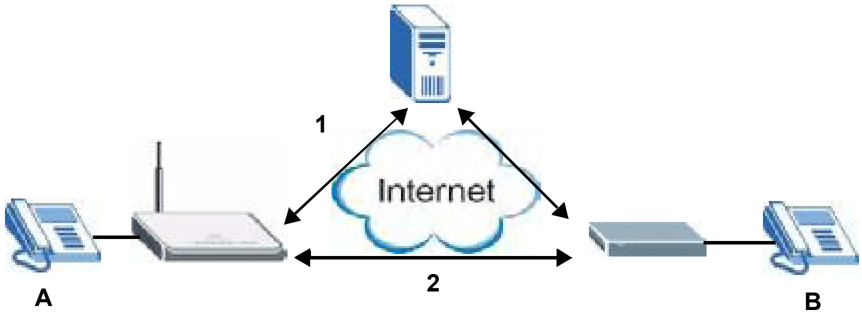
STUN (Simple Traversal of User Datagram Protocol (UDP) through Network Address Translators) allows the VoIP device to find the presence and types of NAT routers and/or firewalls between it and the public Internet. STUN also allows the VoIP device to find the public IP address that NAT assigned, so the VoIP device can embed it in the SIP data stream. See RFC 3489 for details on STUN. You do not need to use STUN for devices behind the ZyXEL Device if you enable the SIP ALG.

18.5.2 SIP ALG Details

- SIP clients can be connected to the LAN or DMZ. A SIP server must be on the WAN.
- You can make and receive calls between the LAN and the WAN, between the DMZ and the WAN. You cannot make a call between the LAN and the LAN, between the LAN and the DMZ, between the DMZ and the DMZ, and so on.
- The SIP ALG allows UDP packets with a port 5060 destination to pass through.
- The ZyXEL Device allows SIP audio connections.

The following example shows SIP signaling (**1**) and audio (**2**) sessions between SIP clients **A** and **B** and the SIP server.

Figure 184 SIP ALG Example



18.5.3 SIP Signaling Session Timeout

Most SIP clients have an “expire” mechanism indicating the lifetime of signaling sessions. The SIP user agent 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 calls during the ZyXEL Device SIP timeout default (60 minutes), the ZyXEL Device SIP ALG drops any incoming calls after the timeout period.

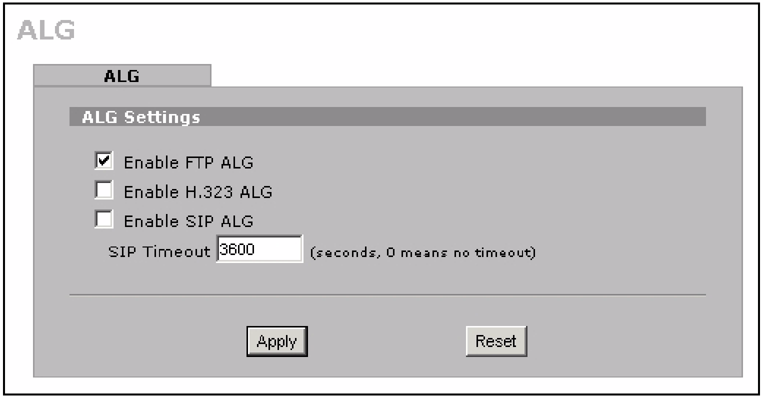
18.5.4 SIP Audio Session Timeout

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.

18.6 ALG Screen

Click **ADVANCED** > **ALG** to open the **ALG** screen. Use the **ALG** screen to turn individual ALGs off or on and set the SIP timeout.

Figure 185 ADVANCED > ALG



ALG

ALG Settings

☑ Enable FTP ALG

□ Enable H.323 ALG

□ Enable SIP ALG

SIP Timeout 3600 (seconds, 0 means no timeout)

The following table describes the labels in this screen.

Table 87 ADVANCED > ALG

LABEL	DESCRIPTION
Enable FTP ALG	Select this check box to allow FTP sessions to pass through the ZyXEL Device. FTP (File Transfer Program) is a program that enables fast transfer of files, including large files that may not be possible by e-mail.
Enable H.323 ALG	Select this check box to allow H.323 sessions to pass through the ZyXEL Device. H.323 is a protocol used for audio communications over networks.
Enable SIP ALG	Select this check box to allow SIP sessions to pass through the ZyXEL Device. SIP is a signaling protocol used in VoIP (Voice over IP), the sending of voice signals over Internet Protocol.
SIP Timeout	Most SIP clients have an “expire” mechanism indicating the lifetime of signaling sessions. The SIP user agent 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 calls during the ZyXEL Device SIP timeout (default 60 minutes), the ZyXEL Device SIP ALG drops any incoming calls after the timeout period. Enter the SIP signaling session timeout value.
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to begin configuring this screen afresh.

PART VI
Logs and Maintenance

19

Logs Screens

This chapter contains information about configuring general log settings and viewing the ZyXEL Device’s logs. Refer to Section 19.5 on page 312 for example log message explanations.

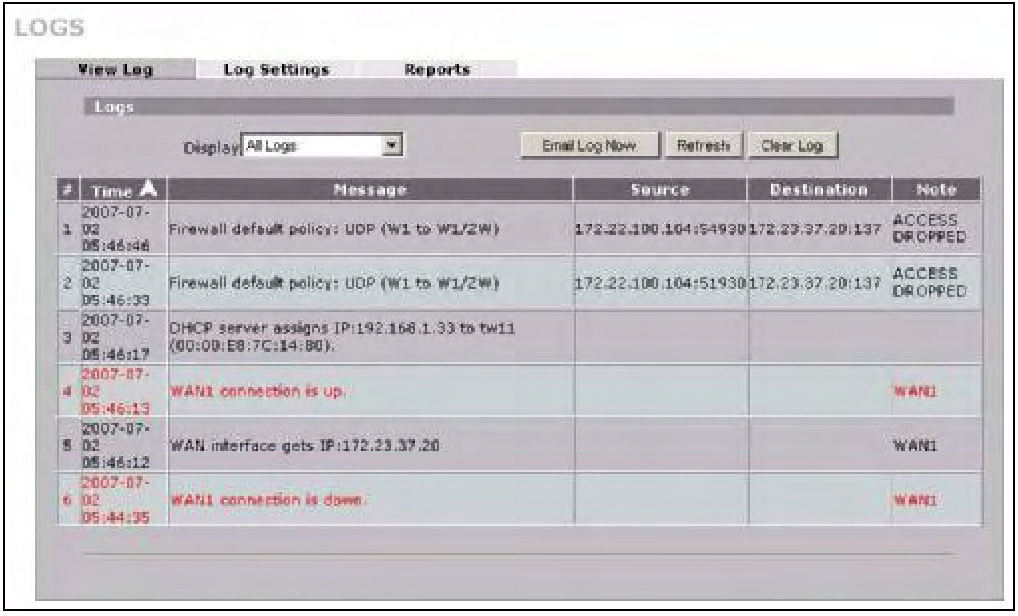
19.1 Configuring View Log

The web configurator allows you to look at all of the ZyXEL Device’s logs in one location.

Click **LOGS** to open the **View Log** screen. Use the **View Log** screen to see the logs for the categories that you selected in the **Log Settings** screen (see Section 19.3 on page 304). Options include logs about system maintenance, system errors, access control, allowed or blocked web sites, blocked web features (such as ActiveX controls, java and cookies), attacks (such as DoS) and IPSec.

Log entries in red indicate system error logs. The log wraps around and deletes the old entries after it fills. Click a column heading to sort the entries. A triangle indicates ascending or descending sort order.

Figure 186 LOGS > View Log



Display: All Logs

#	Time ▲	Message	Source	Destination	Note
1	2007-07-02 05:46:46	Firewall default policy: UDP (W1 to W1/2W)	172.22.100.104:54930	172.23.37.20:137	ACCESS DROPPED
2	2007-07-02 05:46:33	Firewall default policy: UDP (W1 to W1/2W)	172.22.100.104:51930	172.23.37.20:137	ACCESS DROPPED
3	2007-07-02 05:46:17	DHCP server assigns IP:192.168.1.33 to tw11 (00:00:E8:7C:14:80).			
4	2007-07-02 05:46:13	WAN1 connection is up.			WAN1
5	2007-07-02 05:46:12	WAN interface gets IP:172.23.37.20			WAN1
6	2007-07-02 05:44:35	WAN1 connection is down.			WAN1

The following table describes the labels in this screen.

Table 88 LOGS > View Log

LABEL	DESCRIPTION
Display	The categories that you select in the **Log Settings** page (see Section 19.3 on page 304) display in the drop-down list box. Select a category of logs to view; select **All Logs** to view logs from all of the log categories that you selected in the **Log Settings** page.
#	This field displays the log number.
Time	This field displays the time the log was recorded. See Section 20.4 on page 327 to configure the ZyXEL Device's time and date.
Message	This field states the reason for the log.
Source	This field lists the source IP address and the port number of the incoming packet.
Destination	This field lists the destination IP address and the port number of the incoming packet.
Note	This field displays additional information about the log entry.
Email Log Now	Click **Email Log Now** to send the log screen to the e-mail address specified in the **Log Settings** page (make sure that you have first filled in the **E-mail Log Settings** fields in **Log Settings**, see Section 19.3 on page 304).
Refresh	Click **Refresh** to renew the log screen.
Clear Log	Click **Clear Log** to delete all the logs.

19.2 Log Description Example

The following is an example of how a log displays in the command line interpreter and a description of the sample log. Refer to the Section 19.5 on page 312 for more log message descriptions and the appendix for details on using the command line interpreter to display logs.

```
#   .time                   source                   destination
notes

     message

  5|06/08/2004 05:58:20 |172.21.4.187:137       |172.21.255.255:137
|ACCESS BLOCK

     Firewall default policy: UDP (W to W/ZW)
```

Table 89 Log Description Example

LABEL	DESCRIPTION
#	This is log number five.
time	The log was generated on June 8, 2004 at 5:58 and 20 seconds AM.
source	The log was generated due to a NetBIOS packet sent from IP address 172.21.4.187 port 137.
destination	The NetBIOS packet was sent to the 172.21.255.255 subnet port 137. This was a NetBIOS UDP broadcast packet meant to discover devices on the network.

Table 89 Log Description Example

LABEL	DESCRIPTION
notes	The ZyXEL Device blocked the packet.
message	The ZyXEL Device blocked the packet in accordance with the firewall’s default policy of blocking sessions that are initiated from the WAN. “UDP” means that this was a User Datagram Protocol packet. “W to W/ZW” indicates that the packet was traveling from the WAN to the WAN or the ZyXEL Device.

19.2.1 About the Certificate Not Trusted Log

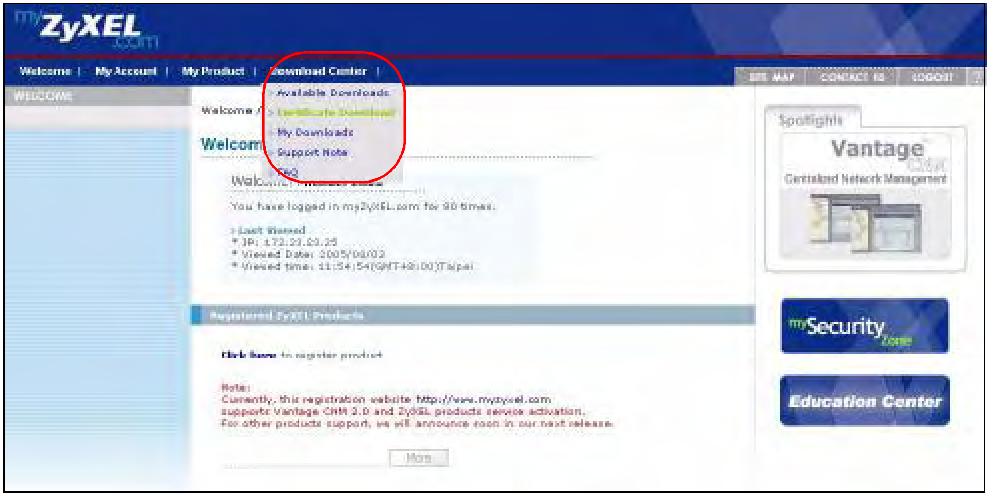
myZyXEL.com and the update server use certificates signed by VeriSign to identify themselves. If the ZyXEL Device does not have a CA certificate signed by VeriSign as a trusted CA, the ZyXEL Device will not trust the certificate from myZyXEL.com and the update server. The ZyXEL Device will generate a log like "Due to error code(11), cert not trusted: SSL/TLS peer certif..." for every time it attempt to establish a (HTTPS) connection with myZyXEL.com and the update server. The V4.00 default configuration file includes a trusted CA certificate signed by VeriSign. If you upgraded to ZyNOS V4.00 firmware without uploading the V4.00 default configuration file, you can download a CA certificate signed by VeriSign from myZyXEL.com and import it into the ZyXEL Device as a trusted CA. This will stop the ZyXEL Device from generating this log every time it attempts to connect with myzyxel.com and the update server.

Follow the steps below to download the certificate from myZyXEL.com.

1 Go to http://www.myZyXEL.com and log in with your account.

2 Click **Download Center** and then **Certificate Download**.

Figure 187 myZyXEL.com: Download Center



You have logged in myZyXEL.com for 90 times.

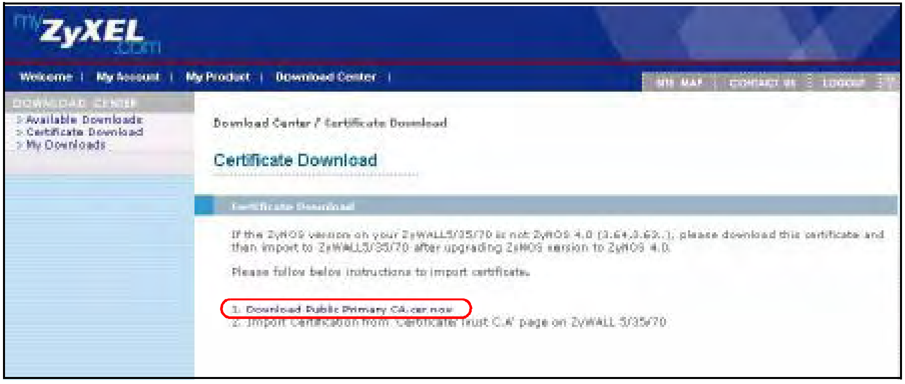
Last Viewed
* IP: 172.23.23.25
* Viewed Date: 2005/03/03
* Viewed time: 11:54:54(GMT+08:00)Taipei

Click here to register product

Note:
Currently, this registration website http://www.myzyxel.com supports Vantage CNM 2.0 and ZyXEL products service activation.
For other products support, we will announce soon in our next release.

3 Click the link in the **Certificate Download** screen.

Figure 188 myZyXEL.com: Certificate Download



If the ZyNOS version on your ZyWALL5/35/70 is not ZyNOS 4.0 (3.64,3.62..), please download this certificate and then import to ZyWALL5/35/70 after upgrading ZyNOS version to ZyNOS 4.0.

Please follow below instructions to import certificate.

1. Download Public Primary CA.cer now
2. Import Certification from 'Certificate Trust C.A' page on ZyWALL 5/35/70

19.3 Configuring Log Settings

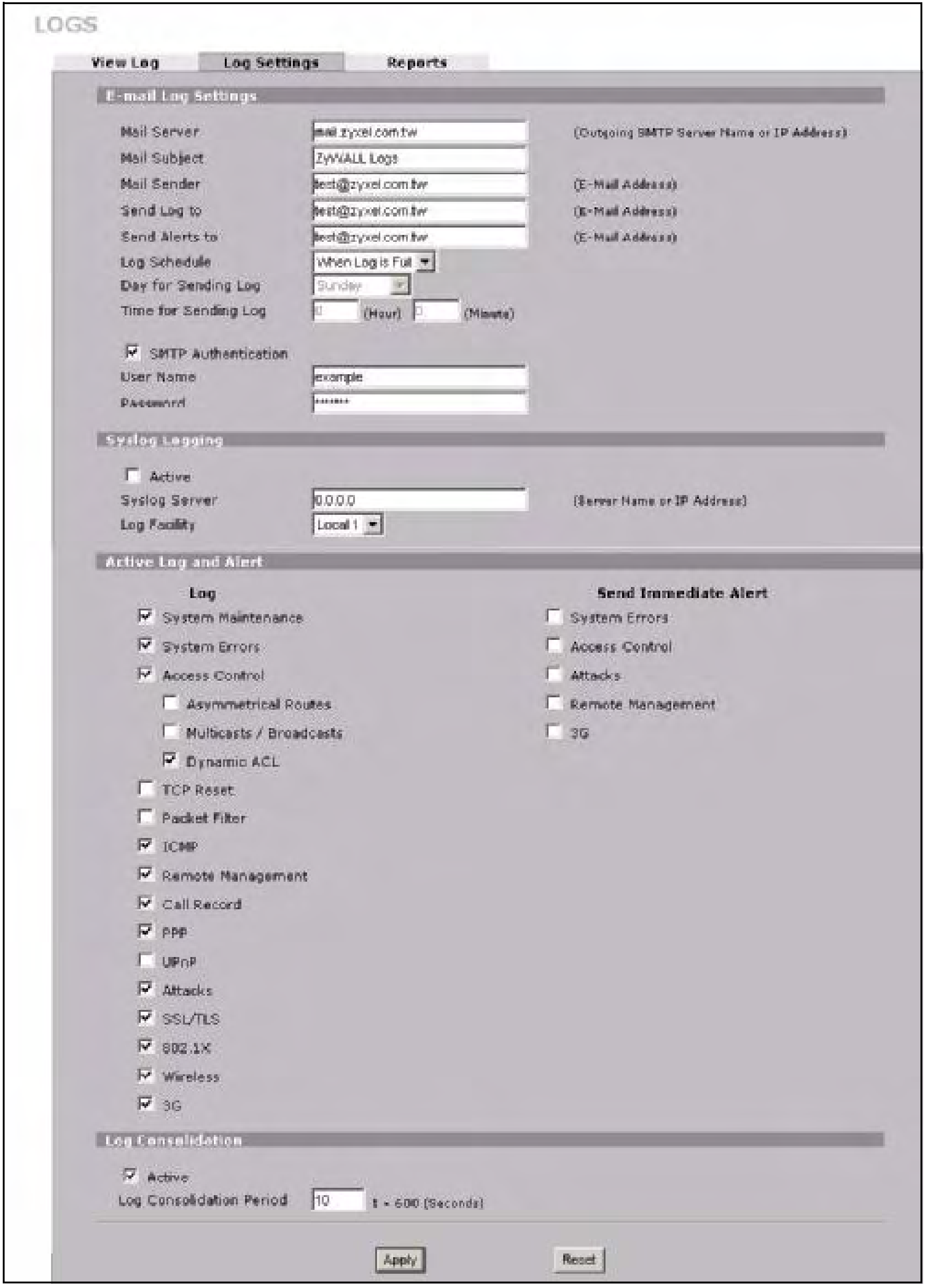
To change your ZyXEL Device’s log settings, click **LOGS** > **Log Settings**. The screen appears as shown.

Use the **Log Settings** screen to configure to where the ZyXEL Device is to send logs; the schedule for when the ZyXEL Device is to send the logs and which logs and/or immediate alerts the ZyXEL Device is to send.

An alert is a type of log that warrants more serious attention. They include system errors, attacks (access control) and attempted access to blocked web sites or web sites with restricted web features such as cookies, active X and so on. Some categories such as **System Errors** consist of both logs and alerts. You may differentiate them by their color in the **View Log** screen. Alerts display in red and logs display in black.

Alerts are e-mailed as soon as they happen. Logs may be e-mailed as soon as the log is full (see **Log Schedule**). Selecting many alert and/or log categories (especially **Access Control**) may result in many e-mails being sent.

Figure 189 LOGS > Log Settings



LOGS

View Log | Log Settings | Reports

E-mail Log Settings

Mail Server	mail.zyxel.com.tw	(Outgoing SMTP Server Name or IP Address)
Mail Subject	ZyWALL Logs	
Mail Sender	test@zyxel.com.tw	(E-Mail Address)
Send Log to	test@zyxel.com.tw	(E-Mail Address)
Send Alerts to	test@zyxel.com.tw	(E-Mail Address)
Log Schedule	When Log is Full ▾	
Day for Sending Log	Sunday ▾	
Time for Sending Log	0 (Hour) 0 (Minute)	

☑ SMTP Authentication

User Name	example
Password	*******

Syslog Logging

☐ Active

Syslog Server	0.0.0.0	(Server Name or IP Address)
Log Facility	Local 1 ▾	

Active Log and Alert

Log	Send Immediate Alert
☑ System Maintenance	☐ System Errors
☑ System Errors	☐ Access Control
☑ Access Control	☐ Attacks
☐ Asymmetrical Routes	☐ Remote Management
☐ Multicasts / Broadcasts	☐ 3G
☑ Dynamic ACL	
☐ TCP Reset	
☐ Packet Filter	
☑ ICMP	
☑ Remote Management	
☑ Call Record	
☑ PPP	
☐ UPnP	
☑ Attacks	
☑ SSL/TLS	
☑ 802.1X	
☑ Wireless	
☑ 3G	

Log Consolidation

☑ Active

Log Consolidation Period 10 1 ~ 600 (Seconds)

Apply Reset

The following table describes the labels in this screen.

Table 90 LOGS > Log Settings

LABEL	DESCRIPTION
E-mail Log Settings	
Mail Server	Enter the server name or the IP address of the mail server for the e-mail addresses specified below. If this field is left blank, logs and alert messages will not be sent via e-mail.
Mail Subject	Type a title that you want to be in the subject line of the log e-mail message that the ZyXEL Device sends.
Mail Sender	Enter the e-mail address that you want to be in the from/sender line of the log e-mail message that the ZyXEL Device sends. If you activate SMTP authentication, the e-mail address must be able to be authenticated by the mail server as well.
Send Log To	Logs are sent to the e-mail address specified in this field. If this field is left blank, logs will not be sent via e-mail.
Send Alerts To	Alerts are sent to the e-mail address specified in this field. If this field is left blank, alerts will not be sent via e-mail.
Log Schedule	This drop-down menu is used to configure the frequency of log messages being sent as E-mail: **Daily** **Weekly** **Hourly** **When Log is Full** **None**. If you select **Weekly** or **Daily**, specify a time of day when the E-mail should be sent. If you select **Weekly**, then also specify which day of the week the E-mail should be sent. If you select **When Log is Full**, an alert is sent when the log fills up. If you select **None**, no log messages are sent.
Day for Sending Log	Use the drop down list box to select which day of the week to send the logs.
Time for Sending Log	Enter the time of the day in 24-hour format (for example 23:00 equals 11:00 pm) to send the logs.
SMTP Authentication	SMTP (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. Select the check box to activate SMTP authentication. If mail server authentication is needed but this feature is disabled, you will not receive the e-mail logs.
User Name	Enter the user name (up to 31 characters) (usually the user name of a mail account).
Password	Enter the password associated with the user name above.
Syslog Logging	Syslog allows you to send system logs to a server. Syslog logging sends a log to an external syslog server.
Active	Click **Active** to enable syslog logging.
Syslog Server	Enter the server name or IP address of the syslog server that will log the selected categories of logs.
Log Facility	Select a location from the drop down list box. The log facility allows you to log the messages to different files in the syslog server. Refer to the documentation of your syslog program for more details.
Active Log and Alert	
Log	Select the categories of logs that you want to record. Logs include alerts.

Table 90 LOGS > Log Settings (continued)

LABEL	DESCRIPTION
Send Immediate Alert	Select the categories of alerts for which you want the ZyXEL Device to instantly e-mail alerts to the e-mail address specified in the **Send Alerts To** field.
Log Consolidation	
Active	Some logs (such as the Attacks logs) may be so numerous that it becomes easy to ignore other important log messages. Select this check box to merge logs with identical messages into one log. You can use the `sys log consolidate msglist` command to see what log messages will be consolidated.
Log Consolidation Period	Specify the time interval during which the ZyXEL Device merges logs with identical messages into one log.
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to begin configuring this screen afresh.

19.4 Configuring Reports

The **Reports** screen displays which computers on the LAN or DMZ send and receive the most traffic, what kinds of traffic are used the most and which web sites are visited the most often. The ZyXEL Device can record and display the following network usage details:

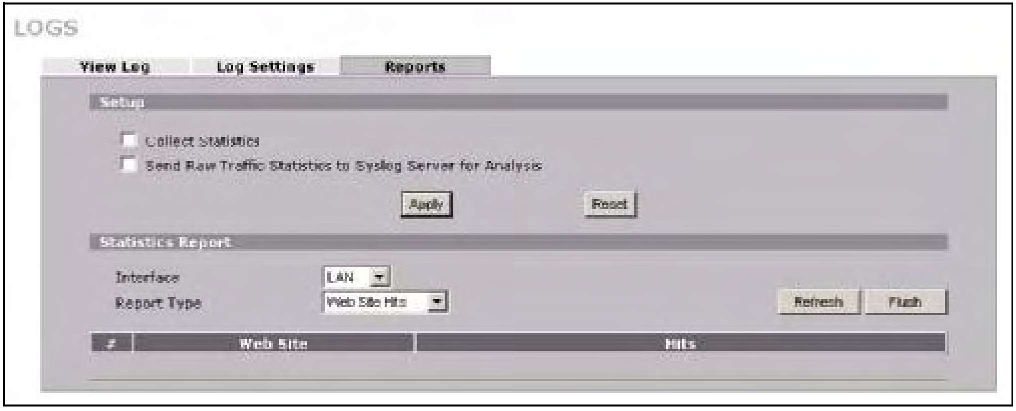
- Web sites visited the most often
- Number of times the most visited web sites were visited
- The most-used protocols or service ports
- The amount of traffic for the most used protocols or service ports
- The LAN or DMZ IP addresses to and/or from which the most traffic has been sent
- How much traffic has been sent to and from the LAN or DMZ IP addresses to and/or from which the most traffic has been sent

✍ The web site hit count may not be 100% accurate because sometimes when an individual web page loads, it may contain references to other web sites that also get counted as hits.

The ZyXEL Device records web site hits by counting the HTTP GET packets. Many web sites include HTTP GET references to other web sites and the ZyXEL Device may count these as hits, thus the web hit count is not (yet) 100% accurate.

Click **LOGS > Reports** to display the following screen.

Figure 190 LOGS > Reports



Enabling the ZyXEL Device's reporting function decreases the overall throughput by about 1 Mbps.

The following table describes the labels in this screen.

Table 91 LOGS > Reports

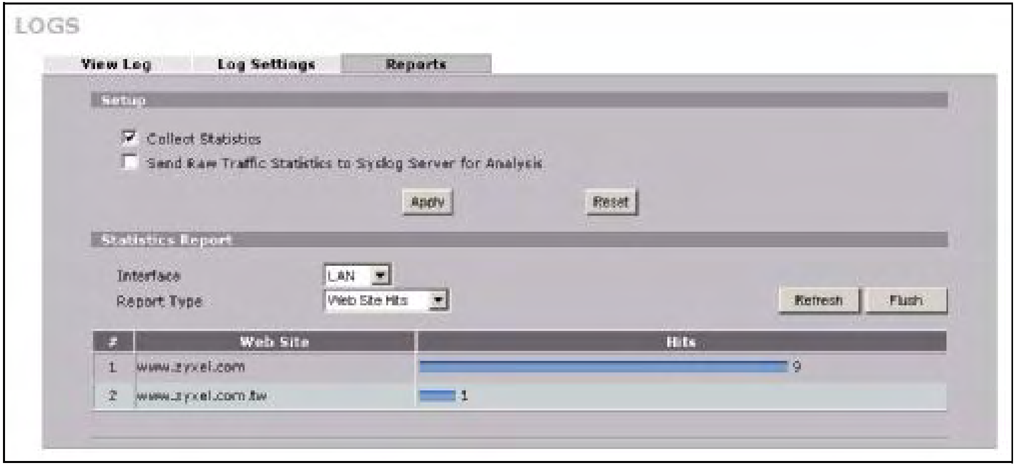
LABEL	DESCRIPTION
Collect Statistics	Select the check box and click **Apply** to have the ZyXEL Device record report data.
Send Raw Traffic Statistics to Syslog Server for Analysis	Select the check box and click **Apply** to have the ZyXEL Device send unprocessed traffic statistics to a syslog server for analysis. You must have the syslog server already configured in the **Log Settings** screen.
Apply	Click **Apply** to save your changes to the ZyXEL Device.
Reset	Click **Reset** to begin configuring this screen afresh.
Interface	Select on which interface (**LAN** or **DMZ**) the logs will be collected. The logs on the DMZ or LAN IP alias 1 and 2 are also recorded.
Report Type	Use the drop-down list box to select the type of reports to display. **Web Site Hits** displays the web sites that have been visited the most often from the LAN and how many times they have been visited. **Protocol/Port** displays the protocols or service ports that have been used the most and the amount of traffic for the most used protocols or service ports. **Host IP Address** displays the LAN or DMZ IP addresses to and /or from which the most traffic has been sent and how much traffic has been sent to and from those IP addresses.
Refresh	Click **Refresh** to update the report display. The report also refreshes automatically when you close and reopen the screen.
Flush	Click **Flush** to discard the old report data and update the report display.

All of the recorded reports data is erased when you turn off the ZyXEL Device.

19.4.1 Viewing Web Site Hits

In the **Reports** screen, select **Web Site Hits** from the **Report Type** drop-down list box to have the ZyXEL Device record and display which web sites have been visited the most often and how many times they have been visited.

Figure 191 LOGS > Reports: Web Site Hits Example



☑ Collect Statistics
□ Send Raw Traffic Statistics to Syslog Server for Analysis

Interface: LAN
Report Type: Web Site Hits

#	Web Site	Hits
1	www.zyxel.com	9
2	www.zyxel.com.tw	1

The following table describes the label in this screen.

Table 92 LOGS > Reports: Web Site Hits Report

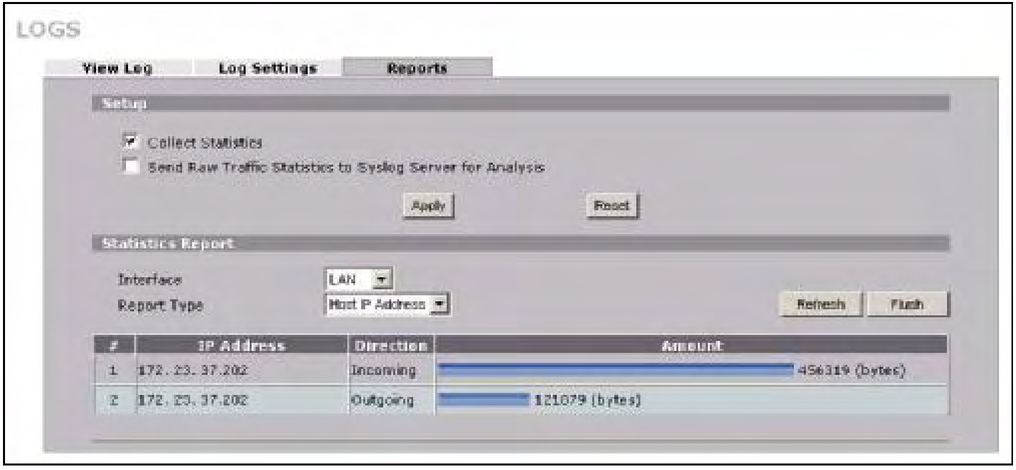
LABEL	DESCRIPTION
Web Site	This column lists the domain names of the web sites visited most often from computers on the LAN or DMZ. The names are ranked by the number of visits to each web site and listed in descending order with the most visited web site listed first. The ZyXEL Device counts each page viewed in a web site as another hit on the web site.
Hits	This column lists how many times each web site has been visited. The count starts over at 0 if a web site passes the hit count limit (see Table 95 on page 312).

19.4.2 Viewing Host IP Address

In the **Reports** screen, select **Host IP Address** from the **Report Type** drop-down list box to have the ZyXEL Device record and display the LAN or DMZ IP addresses that the most traffic has been sent to and/or from and how much traffic has been sent to and/or from those IP addresses.

Computers take turns using dynamically assigned LAN or DMZ IP addresses. The ZyXEL Device continues recording the bytes sent to or from a LAN or DMZ IP address when it is assigned to a different computer.

Figure 192 LOGS > Reports: Host IP Address Example



☑ Collect Statistics

□ Send Raw Traffic Statistics to Syslog Server for Analysis

Interface: LAN

Report Type: Host IP Address

#	IP Address	Direction	Amount
1	172.23.37.202	Incoming	456319 (bytes)
2	172.23.37.202	Outgoing	121079 (bytes)

The following table describes the labels in this screen.

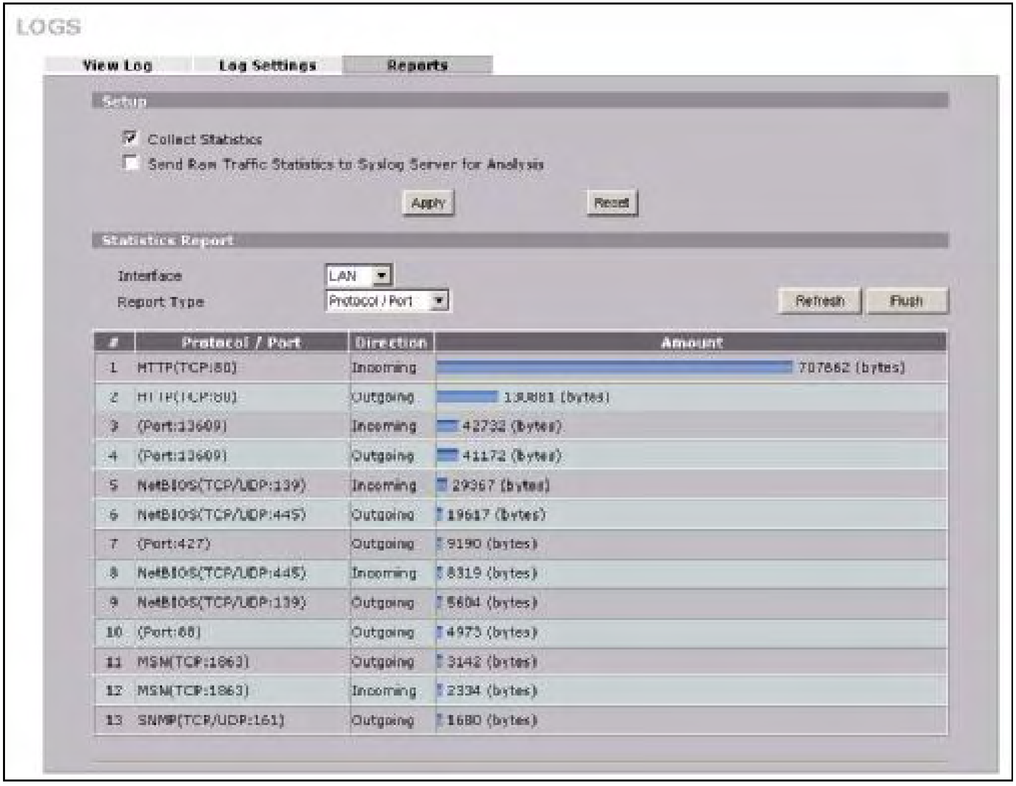
Table 93 LOGS > Reports: Host IP Address

LABEL	DESCRIPTION
IP Address	This column lists the LAN or DMZ IP addresses to and/or from which the most traffic has been sent. The LAN or DMZ IP addresses are listed in descending order with the LAN or DMZ IP address to and/or from which the most traffic was sent listed first.
Direction	This field displays **Incoming** to denote traffic that is coming in from the WAN to the LAN or DMZ. This field displays **Outgoing** to denote traffic that is going out from the LAN or DMZ to the WAN.
Amount	This column displays how much traffic has gone to and from the listed LAN or DMZ IP addresses. The measurement unit shown (bytes, Kbytes, Mbytes or Gbytes) varies with the amount of traffic sent to and from the LAN or DMZ IP address. The count starts over at 0 if the total traffic sent to and from a LAN or DMZ IP passes the bytes count limit (see Table 95 on page 312).

19.4.3 Viewing Protocol/Port

In the **Reports** screen, select **Protocol/Port** from the **Report Type** drop-down list box to have the ZyXEL Device record and display which protocols or service ports have been used the most and the amount of traffic for the most used protocols or service ports.

Figure 193 LOGS > Reports: Protocol/Port Example



☑ Collect Statistics

☐ Send Raw Traffic Statistics to Syslog Server for Analysis

Interface: LAN

Report Type: Protocol / Port

#	Protocol / Port	Direction	Amount
1	HTTP(TCP:80)	Incoming	707862 (bytes)
2	HTTP(TCP:80)	Outgoing	138881 (bytes)
3	(Port:13609)	Incoming	42732 (bytes)
4	(Port:13609)	Outgoing	41172 (bytes)
5	NetBIOS(TCP/UDP:139)	Incoming	29367 (bytes)
6	NetBIOS(TCP/UDP:445)	Outgoing	19617 (bytes)
7	(Port:427)	Outgoing	9190 (bytes)
8	NetBIOS(TCP/UDP:445)	Incoming	8319 (bytes)
9	NetBIOS(TCP/UDP:139)	Outgoing	5604 (bytes)
10	(Port:68)	Outgoing	4973 (bytes)
11	MSN(TCP:1863)	Outgoing	3142 (bytes)
12	MSN(TCP:1863)	Incoming	2334 (bytes)
13	SNMP(TCP/UDP:161)	Outgoing	1680 (bytes)

The following table describes the labels in this screen.

Table 94 LOGS > Reports: Protocol/ Port

LABEL	DESCRIPTION
Protocol/Port	This column lists the protocols or service ports for which the most traffic has gone through the ZyXEL Device. The protocols or service ports are listed in descending order with the most used protocol or service port listed first.
Direction	This field displays **Incoming** to denote traffic that is coming in from the WAN to the LAN or DMZ. This field displays **Outgoing** to denote traffic that is going out from the LAN or DMZ to the WAN.
Amount	This column lists how much traffic has been sent and/or received for each protocol or service port. The measurement unit shown (bytes, Kbytes, Mbytes or Gbytes) varies with the amount of traffic for the particular protocol or service port. The count starts over at 0 if a protocol or port passes the bytes count limit (see Table 95 on page 312).

19.4.4 System Reports Specifications

The following table lists detailed specifications on the reports feature.

Table 95 Report Specifications

LABEL	DESCRIPTION
Number of web sites/protocols or ports/IP addresses listed:	20
Hit count limit:	Up to 2^{32} hits can be counted per web site. The count starts over at 0 if it passes four billion.
Bytes count limit:	Up to 2^{64} bytes can be counted per protocol/port or LAN IP address. The count starts over at 0 if it passes 2^{64} bytes.

19.5 Log Descriptions

This section provides descriptions of example log messages.

Table 96 System Maintenance Logs

LOG MESSAGE	DESCRIPTION
`Time calibration is successful`	The router has adjusted its time based on information from the time server.
`Time calibration failed`	The router failed to get information from the time server.
`WAN interface gets IP: %s`	A WAN interface got a new IP address from the DHCP, PPPoE, PPTP or dial-up server.
`DHCP client IP expired`	A DHCP client's IP address has expired.
`DHCP server assigns %s`	The DHCP server assigned an IP address to a client.
`Successful WEB login`	Someone has logged on to the router's web configurator interface.
`WEB login failed`	Someone has failed to log on to the router's web configurator interface.
`Successful TELNET login`	Someone has logged on to the router via telnet.
`TELNET login failed`	Someone has failed to log on to the router via telnet.
`Successful FTP login`	Someone has logged on to the router via FTP.
`FTP login failed`	Someone has failed to log on to the router via FTP.
`NAT Session Table is Full!`	The maximum number of NAT session table entries has been exceeded and the table is full.
`Starting Connectivity Monitor`	Starting Connectivity Monitor.
`Time initialized by Daytime Server`	The router got the time and date from the Daytime server.
`Time initialized by Time server`	The router got the time and date from the time server.
`Time initialized by NTP server`	The router got the time and date from the NTP server.

Table 96 System Maintenance Logs (continued)

LOG MESSAGE	DESCRIPTION
`Connect to Daytime server fail`	The router was not able to connect to the Daytime server.
`Connect to Time server fail`	The router was not able to connect to the Time server.
`Connect to NTP server fail`	The router was not able to connect to the NTP server.
`Too large ICMP packet has been dropped`	The router dropped an ICMP packet that was too large.
`Configuration Change: PC = 0x%x, Task ID = 0x%x`	The router is saving configuration changes.
`Successful SSH login`	Someone has logged on to the router’s SSH server.
`SSH login failed`	Someone has failed to log on to the router’s SSH server.
`Successful HTTPS login`	Someone has logged on to the router's web configurator interface using HTTPS protocol.
`HTTPS login failed`	Someone has failed to log on to the router's web configurator interface using HTTPS protocol.
`DNS server %s was not responding to last 32 consecutive queries…`	The specified DNS server did not respond to the last 32 consecutive queries.
`DDNS update IP:%s (host %d) successfully`	The device updated the IP address of the specified DDNS host name.
`SMTP successfully`	The device sent an e-mail.

Table 97 System Error Logs

LOG MESSAGE	DESCRIPTION
`%s exceeds the max. number of session per host!`	This attempt to create a NAT session exceeds the maximum number of NAT session table entries allowed to be created per host.
`setNetBIOSFilter: calloc error`	The router failed to allocate memory for the NetBIOS filter settings.
`readNetBIOSFilter: calloc error`	The router failed to allocate memory for the NetBIOS filter settings.
`WAN connection is down.`	A WAN connection is down. You cannot access the network through this interface.
`DHCP Server cannot assign the static IP %S (out of range).`	The LAN subnet, LAN alias 1, or LAN alias 2 was changed and the specified static DHCP IP addresses are no longer valid.
`The DHCP static IP %s is conflict.`	The static DHCP IP address conflicts with another host.
`SMTP fail (%s)`	The device failed to send an e-mail (error message included).
`SMTP authentication fail (%s)`	The device failed to authenticate with the SMTP server (error message included).

Table 98 Access Control Logs

LOG MESSAGE	DESCRIPTION
`Firewall default policy: [ TCP | UDP | IGMP | ESP | GRE | OSPF ] <Packet Direction>`	Attempted TCP/UDP/IGMP/ESP/GRE/OSPF access matched the default policy and was blocked or forwarded according to the default policy's setting.
`Firewall rule [NOT] match:[ TCP | UDP | IGMP | ESP | GRE | OSPF ] <Packet Direction>, <rule:%d>`	Attempted TCP/UDP/IGMP/ESP/GRE/OSPF access matched (or did not match) a configured firewall rule (denoted by its number) and was blocked or forwarded according to the rule.
`Triangle route packet forwarded: [ TCP | UDP | IGMP | ESP | GRE | OSPF ]`	The firewall allowed a triangle route session to pass through.
`Packet without a NAT table entry blocked: [ TCP | UDP | IGMP | ESP | GRE | OSPF ]`	The router blocked a packet that didn't have a corresponding NAT table entry.
`Router sent blocked web site message: TCP`	The router sent a message to notify a user that the router blocked access to a web site that the user requested.
`Exceed maximum sessions per host (%d).`	The device blocked a session because the host's connections exceeded the maximum sessions per host.
`Firewall allowed a packet that matched a NAT session: [ TCP | UDP ]`	A packet from the WAN (TCP or UDP) matched a cone NAT session and the device forwarded it to the LAN.

Table 99 TCP Reset Logs

LOG MESSAGE	DESCRIPTION
`Under SYN flood attack, sent TCP RST`	The router sent a TCP reset packet when a host was under a SYN flood attack (the TCP incomplete count is per destination host.)
`Exceed TCP MAX incomplete, sent TCP RST`	The router sent a TCP reset packet when the number of TCP incomplete connections exceeded the user configured threshold. (the TCP incomplete count is per destination host.) Note: Refer to **TCP Maximum Incomplete** in the **Firewall Attack Alerts** screen.
`Peer TCP state out of order, sent TCP RST`	The router sent a TCP reset packet when a TCP connection state was out of order.Note: The firewall refers to RFC793 Figure 6 to check the TCP state.
`Firewall session time out, sent TCP RST`	The router sent a TCP reset packet when a dynamic firewall session timed out. The default timeout values are as follows: ICMP idle timeout: 3 minutes UDP idle timeout: 3 minutes TCP connection (three way handshaking) timeout: 270 seconds TCP FIN-wait timeout: 2 MSL (Maximum Segment Lifetime set in the TCP header). TCP idle (established) timeout (s): 150 minutes TCP reset timeout: 10 seconds

Table 99 TCP Reset Logs (continued)

LOG MESSAGE	DESCRIPTION
`Exceed MAX incomplete, sent TCP RST`	The router sent a TCP reset packet when the number of incomplete connections (TCP and UDP) exceeded the user-configured threshold. (Incomplete count is for all TCP and UDP connections through the firewall.)Note: When the number of incomplete connections (TCP + UDP) > "Maximum Incomplete High", the router sends TCP RST packets for TCP connections and destroys TOS (firewall dynamic sessions) until incomplete connections < "Maximum Incomplete Low".
`Access block, sent TCP RST`	The router sends a TCP RST packet and generates this log if you turn on the firewall TCP reset mechanism (via CI command: "sys firewall tcprst").

Table 100 Packet Filter Logs

LOG MESSAGE	DESCRIPTION
`[ TCP | UDP | ICMP | IGMP | Generic ] packet filter matched (set: %d, rule: %d)`	Attempted access matched a configured filter rule (denoted by its set and rule number) and was blocked or forwarded according to the rule.

For type and code details, see Table 110 on page 321.

Table 101 ICMP Logs

LOG MESSAGE	DESCRIPTION
`Firewall default policy: ICMP <Packet Direction>, <type:%d>, <code:%d>`	ICMP access matched the default policy and was blocked or forwarded according to the user's setting.
`Firewall rule [NOT] match: ICMP <Packet Direction>, <rule:%d>, <type:%d>, <code:%d>`	ICMP access matched (or didn't match) a firewall rule (denoted by its number) and was blocked or forwarded according to the rule.
`Triangle route packet forwarded: ICMP`	The firewall allowed a triangle route session to pass through.
`Packet without a NAT table entry blocked: ICMP`	The router blocked a packet that didn't have a corresponding NAT table entry.
`Unsupported/out-of-order ICMP: ICMP`	The firewall does not support this kind of ICMP packets or the ICMP packets are out of order.
`Router reply ICMP packet: ICMP`	The router sent an ICMP reply packet to the sender.

Table 102 Remote Management Logs

LOG MESSAGE	DESCRIPTION
`Remote Management: FTP denied`	Attempted use of FTP service was blocked according to remote management settings.
`Remote Management: TELNET denied`	Attempted use of TELNET service was blocked according to remote management settings.
`Remote Management: HTTP or UPnP denied`	Attempted use of HTTP or UPnP service was blocked according to remote management settings.
`Remote Management: WWW denied`	Attempted use of WWW service was blocked according to remote management settings.

Table 102 Remote Management Logs

LOG MESSAGE	DESCRIPTION
`Remote Management: HTTPS denied`	Attempted use of HTTPS service was blocked according to remote management settings.
`Remote Management: SSH denied`	Attempted use of SSH service was blocked according to remote management settings.
`Remote Management: ICMP Ping response denied`	Attempted use of ICMP service was blocked according to remote management settings.
`Remote Management: SNMP denied`	Attempted use of SNMP service was blocked according to remote management settings.
`Remote Management: DNS denied`	Attempted use of DNS service was blocked according to remote management settings.

Table 103 CDR Logs

LOG MESSAGE	DESCRIPTION
`board %d line %d channel %d, call %d, %s C01 Outgoing Call dev=%x ch=%x %s`	The router received the setup requirements for a call. “call” is the reference (count) number of the call. “dev” is the device type (3 is for dial-up, 6 is for PPPoE, 10 is for PPTP). "channel" or “ch” is the call channel ID. For example, "board 0 line 0 channel 0, call 3, C01 Outgoing Call dev=6 ch=0 "Means the router has dialed to the PPPoE server 3 times.
`board %d line %d channel %d, call %d, %s C02 OutCall Connected %d %s`	The PPPoE, PPTP or dial-up call is connected.
`board %d line %d channel %d, call %d, %s C02 Call Terminated`	The PPPoE, PPTP or dial-up call was disconnected.

Table 104 PPP Logs

LOG MESSAGE	DESCRIPTION
`ppp:LCP Starting`	The PPP connection’s Link Control Protocol stage has started.
`ppp:LCP Opening`	The PPP connection’s Link Control Protocol stage is opening.
`ppp:CHAP Opening`	The PPP connection’s Challenge Handshake Authentication Protocol stage is opening.
`ppp:IPCP Starting`	The PPP connection’s Internet Protocol Control Protocol stage is starting.
`ppp:IPCP Opening`	The PPP connection’s Internet Protocol Control Protocol stage is opening.
`ppp:LCP Closing`	The PPP connection’s Link Control Protocol stage is closing.
`ppp:IPCP Closing`	The PPP connection’s Internet Protocol Control Protocol stage is closing.

Table 105 UPnP Logs

LOG MESSAGE	DESCRIPTION
`UPnP pass through Firewall`	UPnP packets can pass through the firewall.

For type and code details, see Table 110 on page 321.

Table 106 Attack Logs

LOG MESSAGE	DESCRIPTION
`attack [ TCP | UDP | IGMP | ESP | GRE | OSPF ]`	The firewall detected a TCP/UDP/IGMP/ESP/GRE/OSPF attack.
`attack ICMP (type:%d, code:%d)`	The firewall detected an ICMP attack.
`land [ TCP | UDP | IGMP | ESP | GRE | OSPF ]`	The firewall detected a TCP/UDP/IGMP/ESP/GRE/OSPF land attack.
`land ICMP (type:%d, code:%d)`	The firewall detected an ICMP land attack.
`ip spoofing - WAN [ TCP | UDP | IGMP | ESP | GRE | OSPF ]`	The firewall detected an IP spoofing attack on the WAN port.
`ip spoofing - WAN ICMP (type:%d, code:%d)`	The firewall detected an ICMP IP spoofing attack on the WAN port.
`icmp echo : ICMP (type:%d, code:%d)`	The firewall detected an ICMP echo attack.
`syn flood TCP`	The firewall detected a TCP syn flood attack.
`ports scan TCP`	The firewall detected a TCP port scan attack.
`teardrop TCP`	The firewall detected a TCP teardrop attack.
`teardrop UDP`	The firewall detected an UDP teardrop attack.
`teardrop ICMP (type:%d, code:%d)`	The firewall detected an ICMP teardrop attack.
`illegal command TCP`	The firewall detected a TCP illegal command attack.
`NetBIOS TCP`	The firewall detected a TCP NetBIOS attack.
`ip spoofing - no routing entry [ TCP | UDP | IGMP | ESP | GRE | OSPF ]`	The firewall classified a packet with no source routing entry as an IP spoofing attack.
`ip spoofing - no routing entry ICMP (type:%d, code:%d)`	The firewall classified an ICMP packet with no source routing entry as an IP spoofing attack.
`vulnerability ICMP (type:%d, code:%d)`	The firewall detected an ICMP vulnerability attack.
`traceroute ICMP (type:%d, code:%d)`	The firewall detected an ICMP traceroute attack.
`ports scan UDP`	The firewall detected a UDP port scan attack.
`Firewall sent TCP packet in response to DoS attack TCP`	The firewall sent TCP packet in response to a DoS attack
`ICMP Source Quench ICMP`	The firewall detected an ICMP Source Quench attack.
`ICMP Time Exceed ICMP`	The firewall detected an ICMP Time Exceed attack.
`ICMP Destination Unreachable ICMP`	The firewall detected an ICMP Destination Unreachable attack.
`ping of death. ICMP`	The firewall detected an ICMP ping of death attack.
`smurf ICMP`	The firewall detected an ICMP smurf attack.

Table 106 Attack Logs (continued)

LOG MESSAGE	DESCRIPTION
`IP address in FTP port command is different from the client IP address. It maybe a bounce attack.`	The IP address in an FTP port command is different from the client IP address. It may be a bounce attack.
`Fragment packet size is smaller than the MTU size of output interface.`	The fragment packet size is smaller than the MTU size of output interface.

Table 107 3G Logs

LOG MESSAGE	DESCRIPTION
`SIM/3G interface mismatch: %s.`	The ID number of the currently selected interface or SIM card is different from the previous one configured for budget control.
`Preconfigured SIM card/3G interface doesn’t match inserted card. Might need to reconfigure budget control settings.`	The 3G interface is different from the previous one configured for budget control. You may need to reconfigure budget control settings specific to the current user account.
`Budget counters are reset, budget control is resumed.`	The ZyXEL Device restarted budget calculation from 0 after resetting the existing statistics.
`Budget control is resumed.`	The ZyXEL Device kept the existing budget control statistics and continue a counting.
`Budget control is disabled.`	Budget control is deactivated for the user account of the 3G interface on the ZyXEL Device.
`Skip 3G SIM authentication because 3G configuration is not set.`	The ZyXEL Device skipped SIM card authentication because the PIN code is not specified or SIM card authentication is disabled.
`3G SIM authentication failed because of no response from SIM card.`	SIM card authentication failed because the ZyXEL Device received a SIM busy message three times when querying for the card status.
`3G SIM card PIN code is incorrect.`	The specified PIN code does not match the 3G interface.
`SIM card not inserted or damaged.`	There is no SIM card inserted or the SIM card is damaged.
`3G connection has been dropped - %s.`	The 3G connection has been dropped due to the specific reason, such as idle timeout, manual disconnection, failure to get an IP address, switching to WAN 1, ping check failure, connection reset, and so on.
`Warning: (%IMSI% or %ESN%) Over time budget! (budget = %CONFIGURED_BUDGET% hours, used = %USED_VOLUME%(2 decimals) hours).`	This shows that the preconfigured time budget was exceeded. This also displays the ID number of the selected 3G interface or SIM card and the 3G connection’s usage time in hours.
`Warning: (%IMSI% or %ESN%) Over %THRESHOLD%% of time budget (%REMAIN_BUDGET%(2 decimals) hours remain in %CONFIGURED_BUDGET% hours budget).`	This shows that the specified percentage of the time budget was exceeded. This also displays the ID number of the selected 3G interface or SIM card and the amount of time (in hours) the 3G connection can still be used.

Table 107 3G Logs (continued)

LOG MESSAGE	DESCRIPTION
`Warning: (%ESN% or %IMSI%) Over data budget! (budget =%CONFIGURED_BUDGET%(2 decimals Mbytes, used = %USED_VOLUME%(2 decimals) Mbytes).`	This shows that the preconfigured data limit was exceeded. The ID number of the selected 3G interface or SIM card is displayed. The amount of data (in Mbytes) sent and/or received (depending on your configuration) through the 3G connection is also displayed.
`Warning: (%ESN% or %IMSI%) Over %THRESHOLD%% of data budget (%REMAIN_BUDGET%(2 decimals) Mbytes remain in %CONFIGURED_BUDGET% Mbytes budget).`	This shows that the specified percentage of data limit was exceeded. This also displays the ID number of the selected 3G interface or SIM card and how much data (in Mbytes) can still be transmitted through the 3G connection.

Table 108 PKI Logs

LOG MESSAGE	DESCRIPTION
`Enrollment successful`	The SCEP online certificate enrollment was successful. The Destination field records the certification authority server IP address and port.
`Enrollment failed`	The SCEP online certificate enrollment failed. The Destination field records the certification authority server's IP address and port.
`Failed to resolve <SCEP CA server url>`	The SCEP online certificate enrollment failed because the certification authority server's address cannot be resolved.
`Enrollment successful`	The CMP online certificate enrollment was successful. The Destination field records the certification authority server's IP address and port.
`Enrollment failed`	The CMP online certificate enrollment failed. The Destination field records the certification authority server's IP address and port.
`Failed to resolve <CMP CA server url>`	The CMP online certificate enrollment failed because the certification authority server's IP address cannot be resolved.
`Rcvd ca cert: <subject name>`	The router received a certification authority certificate, with subject name as recorded, from the LDAP server whose IP address and port are recorded in the Source field.
`Rcvd user cert: <subject name>`	The router received a user certificate, with subject name as recorded, from the LDAP server whose IP address and port are recorded in the Source field.
`Rcvd CRL <size>: <issuer name>`	The router received a CRL (Certificate Revocation List), with size and issuer name as recorded, from the LDAP server whose IP address and port are recorded in the Source field.
`Rcvd ARL <size>: <issuer name>`	The router received an ARL (Authority Revocation List), with size and issuer name as recorded, from the LDAP server whose address and port are recorded in the Source field.
`Failed to decode the received ca cert`	The router received a corrupted certification authority certificate from the LDAP server whose address and port are recorded in the Source field.
`Failed to decode the received user cert`	The router received a corrupted user certificate from the LDAP server whose address and port are recorded in the Source field.
`Failed to decode the received CRL`	The router received a corrupted CRL (Certificate Revocation List) from the LDAP server whose address and port are recorded in the Source field.

Table 108 PKI Logs (continued)

LOG MESSAGE	DESCRIPTION
`Failed to decode the received ARL`	The router received a corrupted ARL (Authority Revocation List) from the LDAP server whose address and port are recorded in the Source field.
`Rcvd data <size> too large! Max size allowed: <max size>`	The router received directory data that was too large (the size is listed) from the LDAP server whose address and port are recorded in the Source field. The maximum size of directory data that the router allows is also recorded.
`Cert trusted: <subject name>`	The router has verified the path of the certificate with the listed subject name.
`Due to <reason codes>, cert not trusted: <subject name>`	Due to the reasons listed, the certificate with the listed subject name has not passed the path verification. The recorded reason codes are only approximate reasons for not trusting the certificate. Please see Table 113 on page 320 for the corresponding descriptions of the codes.

CODE	DESCRIPTION
1	Algorithm mismatch between the certificate and the search constraints.
2	Key usage mismatch between the certificate and the search constraints.
3	Certificate was not valid in the time interval.
4	(Not used)
5	Certificate is not valid.
6	Certificate signature was not verified correctly.
7	Certificate was revoked by a CRL.
8	Certificate was not added to the cache.
9	Certificate decoding failed.
10	Certificate was not found (anywhere).
11	Certificate chain looped (did not find trusted root).
12	Certificate contains critical extension that was not handled.
13	Certificate issuer was not valid (CA specific information missing).
14	(Not used)
15	CRL is too old.
16	CRL is not valid.
17	CRL signature was not verified correctly.
18	CRL was not found (anywhere).
19	CRL was not added to the cache.
20	CRL decoding failed.
21	CRL is not currently valid, but in the future.
22	CRL contains duplicate serial numbers.
23	Time interval is not continuous.
24	Time information not available.
25	Database method failed due to timeout.
26	Database method failed.

CODE	DESCRIPTION
27	Path was not verified.
28	Maximum path length reached.

Table 109 ACL Setting Notes

PACKET DIRECTION	DIRECTION	DESCRIPTION
(L to W)	LAN to WAN	ACL set for packets traveling from the LAN to the WAN.
(W to L)	WAN to LAN	ACL set for packets traveling from the WAN to the LAN.
(D to L)	DMZ to LAN	ACL set for packets traveling from the DMZ to the LAN.
(D to W)	DMZ to WAN	ACL set for packets traveling from the DMZ to the WAN.
(W to D)	WAN to DMZ	ACL set for packets traveling from the WAN to the DMZ.
(L to D)	LAN to DMZ	ACL set for packets traveling from the LAN to the DMZ.
(L to L/ZW)	LAN to LAN/ ZyXEL Device	ACL set for packets traveling from the LAN to the LAN or the ZyXEL Device.
(W to W/ZW)	WAN to WAN/ ZyXEL Device	ACL set for packets traveling from the WAN to the WAN or the ZyXEL Device.
(D to D/ZW)	DMZ to DMZ/ ZyXEL Device	ACL set for packets traveling from the DMZ to the DM or the ZyXEL Device.

Table 110 ICMP Notes

TYPE	CODE	DESCRIPTION
0		Echo Reply
	0	Echo reply message
3		Destination Unreachable
	0	Net unreachable
	1	Host unreachable
	2	Protocol unreachable
	3	Port unreachable
	4	A packet that needed fragmentation was dropped because it was set to Don't Fragment (DF)
	5	Source route failed
4		Source Quench
	0	A gateway may discard internet datagrams if it does not have the buffer space needed to queue the datagrams for output to the next network on the route to the destination network.
5		Redirect
	0	Redirect datagrams for the Network
	1	Redirect datagrams for the Host
	2	Redirect datagrams for the Type of Service and Network
	3	Redirect datagrams for the Type of Service and Host
8		Echo

Table 110 ICMP Notes (continued)

TYPE	CODE	DESCRIPTION
	0	Echo message
11		Time Exceeded
	0	Time to live exceeded in transit
	1	Fragment reassembly time exceeded
12		Parameter Problem
	0	Pointer indicates the error
13		Timestamp
	0	Timestamp request message
14		Timestamp Reply
	0	Timestamp reply message
15		Information Request
	0	Information request message
16		Information Reply
	0	Information reply message

19.6 Syslog Logs

There are two types of syslog: event logs and traffic logs. The device generates an event log when a system event occurs, for example, when a user logs in or the device is under attack. The device generates a traffic log when a "session" is terminated. A traffic log summarizes the session's type, when it started and stopped the amount of traffic that was sent and received and so on. An external log analyzer can reconstruct and analyze the traffic flowing through the device after collecting the traffic logs.

Table 111 Syslog Logs

LOG MESSAGE	DESCRIPTION
`Event Log: <Facility*8 + Severity>Mon dd hr:mm:ss hostname src="<srcIP:srcPort>" dst="<dstIP:dstPort>" msg="<msg>" note="<note>" devID="<mac address>" cat="<category>"`	This message is sent by the system ("RAS" displays as the system name if you haven't configured one) when the router generates a syslog. The facility is defined in the web **MAIN MENU** > **LOGS** > **Log Settings** page. The severity is the log's syslog class. The definition of messages and notes are defined in the other log tables. The "devID" is the MAC address of the router's LAN port. The "cat" is the same as the category in the router's logs.
`Traffic Log: <Facility*8 + Severity>Mon dd hr:mm:ss hostname src="<srcIP:srcPort>" dst="<dstIP:dstPort>" msg="Traffic Log" note="Traffic Log" devID="<mac address>" cat="Traffic Log" duration=seconds sent=sentBytes rcvd=receiveBytes dir="<from:to>" protoID=IPProtocolID proto="serviceName" trans="IPSec/Normal"`	This message is sent by the device when the connection (session) is closed. The facility is defined in the Log Settings screen. The severity is the traffic log type. The message and note always display "Traffic Log". The "proto" field lists the service name. The "dir" field lists the incoming and outgoing interfaces ("LAN:LAN", "LAN:WAN", "LAN:DMZ", "LAN:DEV" for example).
`Event Log: <Facility*8 + Severity>Mon dd hr:mm:ss hostname src="<srcIP:srcPort>" dst="<dstIP:dstPort>" ob="<0|1>" ob_mac="<mac address>" msg="<msg>" note="<note>" devID="<mac address>" cat="<category>"`	This message is sent by the device ("RAS" displays as the system name if you haven't configured one) at the time when this syslog is generated. The facility is defined in the web **MAIN MENU** > **LOGS** > **Log Settings** page. The severity is the log's syslog class. The definition of messages and notes are defined in the other log tables. OB is the Out Break flag and the mac address of the Out Break PC.
`Event Log: <Facility*8 + Severity>Mon dd hr:mm:ss hostname src="<srcIP:srcPort>" dst="<dstIP:dstPort>" ob="0|1" ob_mac="<mac address>" msg="<msg>" note="<note>" devID="<mac address>" cat="Anti Virus" encode="< uu | b64 >"`	This message is sent by the device ("RAS" displays as the system name if you haven't configured one) at the time when this syslog is generated. The facility is defined in the web **MAIN MENU** > **LOGS** > **Log Settings** page. The severity is the log's syslog class. The "encode" message indicates the mail attachments encoding method. The definition of messages and notes are defined in the Anti-Virus log descriptions.

Table 111 Syslog Logs (continued)

LOG MESSAGE	DESCRIPTION
`Event Log: <Facility*8 + Severity>Mon dd hr:mm:ss hostname src="<srcIP:srcPort>" dst="<dstIP:dstPort>" ob="<0|1>" ob_mac="<mac address>" msg="<msg>" note="<note>" devID="<mac address>" cat="IDP" class="<idp class>" sid="<idp sid> act="<idp action>" count="1"`	This message is sent by the device ("RAS" displays as the system name if you haven't configured one) at the time when this syslog is generated. The facility is defined in the web **MAIN MENU** > **LOGS** > **Log Settings** page. The severity is the log's syslog class. The definition of messages and notes are defined in the IDP log descriptions.
`Event Log: <Facility*8 + Severity>Mon dd hr:mm:ss hostname src="<srcIP:srcPort>" dst="<dstIP:dstPort>" ob="<0|1>" ob_mac="<mac address>" msg="<msg>" note="<note>" devID="<mac address>" cat="Anti Spam" 1stReIP="<IP>"`	This message is sent by the device ("RAS" displays as the system name if you haven't configured one) at the time when this syslog is generated. The facility is defined in the web **MAIN MENU** > **LOGS** > **Log Settings** page. The severity is the log's syslog class. 1stReIP is the IP address of the first mail relay server. The definition of messages and notes are defined in the Anti-Spam log descriptions.

The following table shows RFC-2408 ISAKMP payload types that the log displays. Please refer to the RFC for detailed information on each type.

Table 112 RFC-2408 ISAKMP Payload Types

LOG DISPLAY	PAYLOAD TYPE
`SA`	Security Association
`PROP`	Proposal
`TRANS`	Transform
`KE`	Key Exchange
`ID`	Identification
`CER`	Certificate
`CER_REQ`	Certificate Request
`HASH`	Hash
`SIG`	Signature
`NONCE`	Nonce
`NOTFY`	Notification
`DEL`	Delete
`VID`	Vendor ID

20

Maintenance

This chapter displays information on the maintenance screens.

20.1 Maintenance Overview

The maintenance screens can help you view system information, upload new firmware, manage configuration and restart your ZyXEL Device.

20.2 General Setup and System Name

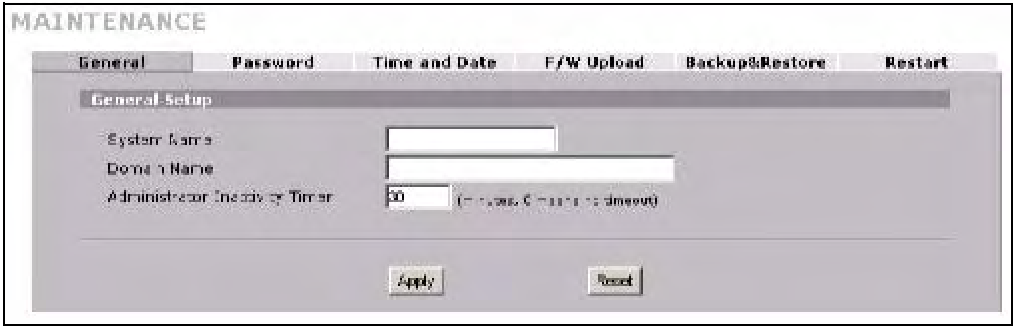
General Setup contains administrative and system-related information. **System Name** is for identification purposes. However, because some ISPs check this name you should enter your computer's "Computer Name".

- In Windows 95/98 click **Start**, **Settings**, **Control Panel**, **Network**. Click the Identification tab, note the entry for the **Computer Name** field and enter it as the **System Name**.
- In Windows 2000, click **Start**, **Settings**, **Control Panel** and then double-click **System**. Click the **Network Identification** tab and then the **Properties** button. Note the entry for the **Computer name** field and enter it as the **System Name**.
- In Windows XP, click **Start**, **My Computer**, **View system information** and then click the **Computer Name** tab. Note the entry in the **Full computer name** field and enter it as the ZyXEL Device **System Name**.

20.2.1 General Setup

Click **MAINTENANCE** to open the **General** screen. Use this screen to configure administrative and system-related information.

Figure 194 MAINTENANCE > General Setup



General Setup

System Name

Domain Name

Administrator Inactivity Timer 30 (minutes, 0 means no timeout)

The following table describes the labels in this screen.

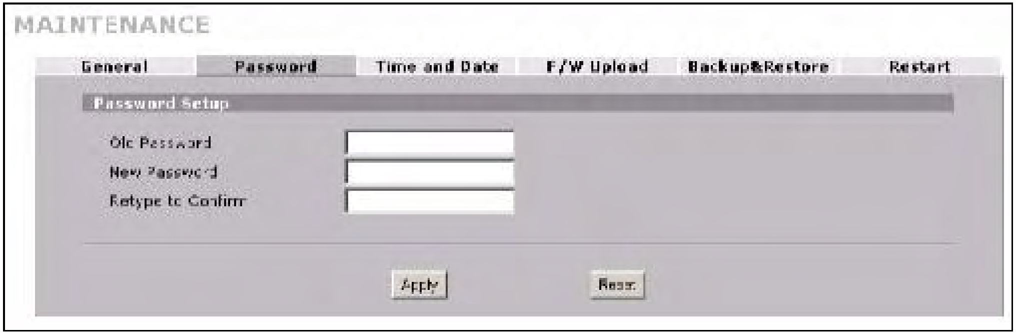
Table 113 MAINTENANCE > General Setup

LABEL	DESCRIPTION
General Setup	
System Name	Choose a descriptive name for identification purposes. It is recommended you enter your computer's "Computer name" in this field. This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted.
Domain Name	The **Domain Name** entry is what is propagated to the DHCP clients on the LAN. If you leave this blank, the domain name obtained by DHCP from the ISP is used. While you must enter the host name (System Name), the domain name can be assigned from the ZyXEL Device via DHCP. Enter the domain name (if you know it) here. If you leave this field blank, the ISP may assign a domain name via DHCP. The domain name entered by you is given priority over the ISP assigned domain name.
Administrator Inactivity Timer	Type how many minutes a management session (via the web configurator) can be left idle before the session times out. The default is 5 minutes. After it times out you have to log in with your password again. Very long idle timeouts may have security risks. A value of "0" means a management session never times out, no matter how long it has been left idle (not recommended).
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to begin configuring this screen afresh.

20.3 Configuring Password

Click **MAINTENANCE** > **Password** to open the following screen. Use this screen to change the ZyXEL Device's management password.

Figure 195 MAINTENANCE > Password



The following table describes the labels in this screen.

Table 114 MAINTENANCE > Password

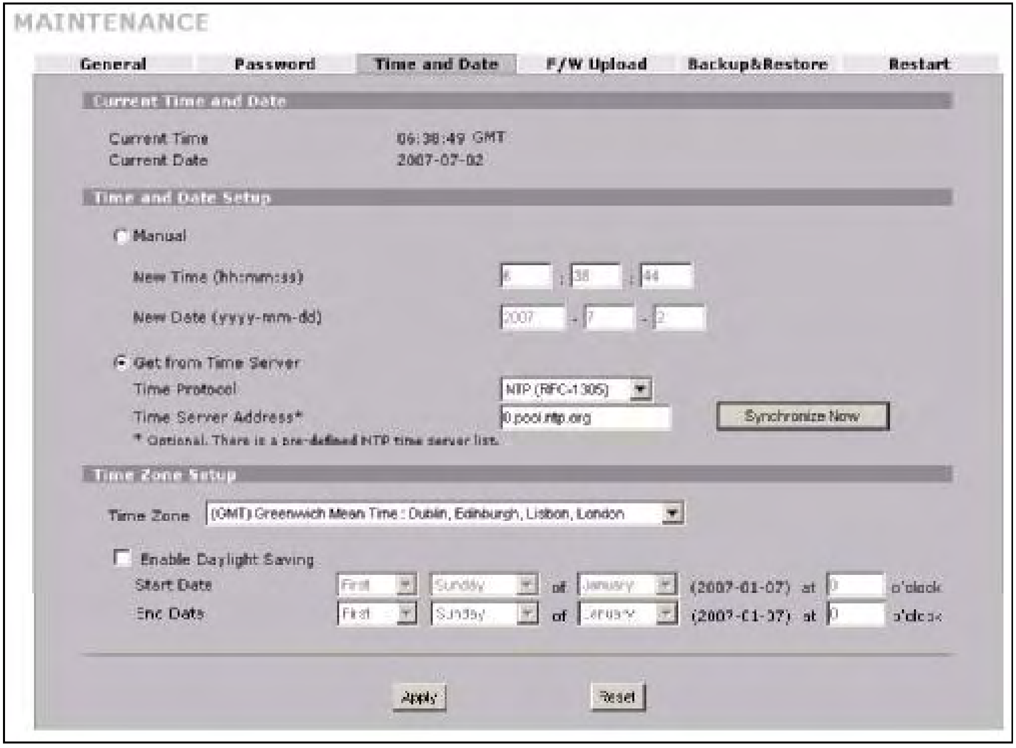
LABEL	DESCRIPTION
Old Password	Type the default password or the existing password you use to access the system in this field. If you forget the password, you may have to use the hardware **RESET** button. This restores the default password of 1234.
New Password	Type your new system password (up to 30 characters). Note that as you type a password, the screen displays a (*) for each character you type.
Retype to Confirm	Type the new password again for confirmation.
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to begin configuring this screen afresh.

20.4 Time and Date

The ZyXEL Device's Real Time Chip (RTC) keeps track of the time and date. There is also a software mechanism to set the time manually or get the current time and date from an external server when you turn on your ZyXEL Device.

To change your ZyXEL Device's time and date, click **MAINTENANCE** > **Time and Date**. The screen appears as shown. Use this screen to configure the ZyXEL Device's time based on your local time zone.

Figure 196 MAINTENANCE > Time and Date



MAINTENANCE

Current Time and Date

Current Time 06:38:49 GMT

Current Date 2007-07-02

Time and Date Setup

○ Manual

New Time (hh:mm:ss) 6 : 38 : 44

New Date (yyyy-mm-dd) 2007 - 7 - 2

● Get from Time Server

Time Protocol NTP (RFC-1305)

Time Server Address* 0.pool.ntp.org

* Optional. There is a pre-defined NTP time server list.

Time Zone Setup

Time Zone (GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London

□ Enable Daylight Saving

Start Date First Sunday of January (2007-01-07) at 0 o'clock

End Date First Sunday of January (2007-01-07) at 0 o'clock

The following table describes the labels in this screen.

Table 115 MAINTENANCE > Time and Date

LABEL	DESCRIPTION
Current Time and Date	
Current Time	This field displays the ZyXEL Device's present time.
Current Date	This field displays the ZyXEL Device's present date.
Time and Date Setup	
Manual	Select this radio button to enter the time and date manually. If you configure a new time and date, Time Zone and Daylight Saving at the same time, the new time and date you entered has priority and the Time Zone and Daylight Saving settings do not affect it.
New Time (hh:mm:ss)	This field displays the last updated time from the time server or the last time configured manually. When you set **Time and Date Setup** to **Manual**, enter the new time in this field and then click **Apply**.
New Date (yyyy-mm-dd)	This field displays the last updated date from the time server or the last date configured manually. When you set **Time and Date Setup** to **Manual**, enter the new date in this field and then click **Apply**.
Get from Time Server	Select this radio button to have the ZyXEL Device get the time and date from the time server you specified below.

Table 115 MAINTENANCE > Time and Date (continued)

LABEL	DESCRIPTION
Time Protocol	Select the time service protocol that your time server uses. Not all time servers support all protocols, so you may have to check with your ISP/network administrator or use trial and error to find a protocol that works. The main difference between them is the format. **Daytime (RFC 867)** format is day/month/year/time zone of the server. **Time (RFC 868)** format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0. The default, **NTP (RFC 1305)**, is similar to **Time (RFC 868)**.
Time Server Address	Enter the IP address or URL of your time server. Check with your ISP/network administrator if you are unsure of this information.
Synchronize Now	Click this button to have the ZyXEL Device get the time and date from a time server (see the **Time Server Address** field). This also saves your changes (including the time server address).
Time Zone Setup	
Time Zone	Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
Enable Daylight Saving	Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening. Select this option if you use Daylight Saving Time.
Start Date	Configure the day and time when Daylight Saving Time starts if you selected **Enable Daylight Saving**. The **o'clock** field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time starts in most parts of the United States on the second Sunday of March. Each time zone in the United States starts using Daylight Saving Time at 2 A.M. local time. So in the United States you would select **Second**, **Sunday**, **March** and type 2 in the **o'clock** field. Daylight Saving Time starts in the European Union on the last Sunday of March. All of the time zones in the European Union start using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select **Last**, **Sunday**, **March**. The time you type in the **o'clock** field depends on your time zone. In Germany for instance, you would type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
End Date	Configure the day and time when Daylight Saving Time ends if you selected **Enable Daylight Saving**. The **o'clock** field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time ends in the United States on the first Sunday of November. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So in the United States you would select **First**, **Sunday**, **November** and type 2 in the **o'clock** field. Daylight Saving Time ends in the European Union on the last Sunday of October. All of the time zones in the European Union stop using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select **Last**, **Sunday**, **October**. The time you type in the **o'clock** field depends on your time zone. In Germany for instance, you would type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to begin configuring this screen afresh.

20.5 Pre-defined NTP Time Server Pools

When you turn on the ZyXEL Device for the first time, the date and time start at 2000-01-01 00:00:00. The ZyXEL Device then attempts to synchronize with an NTP time server from one of the 0.pool.ntp.org, 1.pool.ntp.org or 2.pool.ntp.org NTP time server pools. These are virtual clusters of time servers that use a round robin method to provide different NTP servers to clients.

The ZyXEL Device continues to use the NTP time server pools if you do not specify a time server or it cannot synchronize with the time server you specified.

The ZyXEL Device can use the NTP time server pools regardless of the time protocol you select.

When the ZyXEL Device uses the NTP time server pools, it randomly selects one pool and tries to synchronize with a server in it. If the synchronization fails, then the ZyXEL Device goes through the rest of the list in order from the first one tried until either it is successful or all the pre-defined NTP time server pools have been tried.

20.5.1 Resetting the Time

The ZyXEL Device resets the time in the following instances:

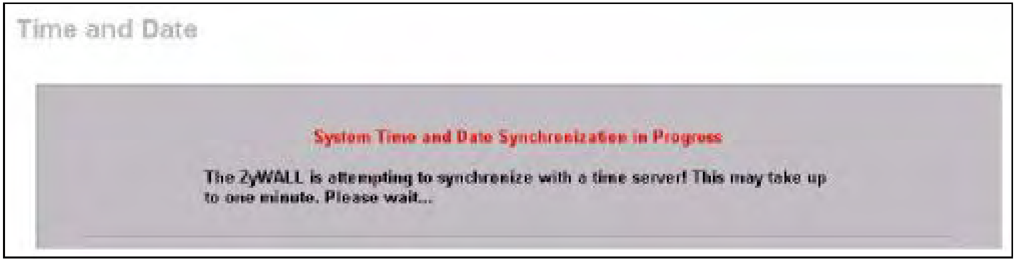
- When you click **Synchronize Now**.
- On saving your changes.
- When the ZyXEL Device starts up.
- 24-hour intervals after starting.

20.5.2 Time Server Synchronization

Click the **Synchronize Now** button to get the time and date from the predefined time server or the time server you specified in the **Time Server Address** field.

When the **System Time and Date Synchronization in Process** screen appears, wait up to one minute.

Figure 197 Synchronization in Process



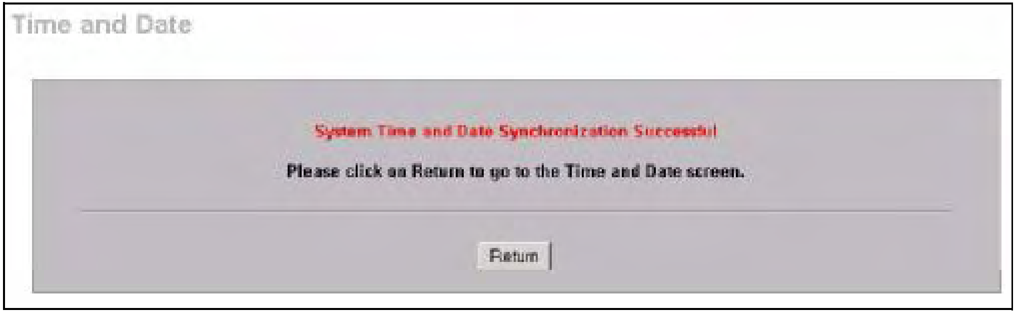
Time and Date

System Time and Date Synchronization in Progress

The ZyWALL is attempting to synchronize with a time server! This may take up to one minute. Please wait...

Click the **Return** button to go back to the **Time and Date** screen after the time and date is updated successfully.

Figure 198 Synchronization is Successful



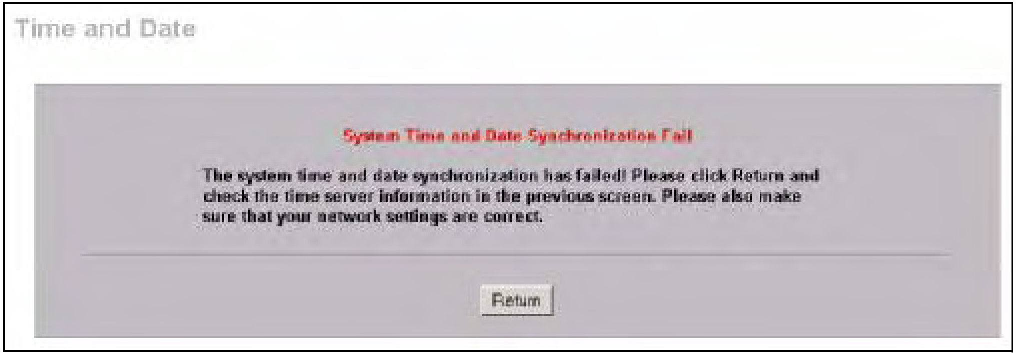
Time and Date

System Time and Date Synchronization Successful

Please click on Return to go to the Time and Date screen.

If the update was not successful, the following screen appears. Click **Return** to go back to the **Time and Date** screen.

Figure 199 Synchronization Fail



Time and Date

System Time and Date Synchronization Fail

The system time and date synchronization has failed! Please click Return and check the time server information in the previous screen. Please also make sure that your network settings are correct.

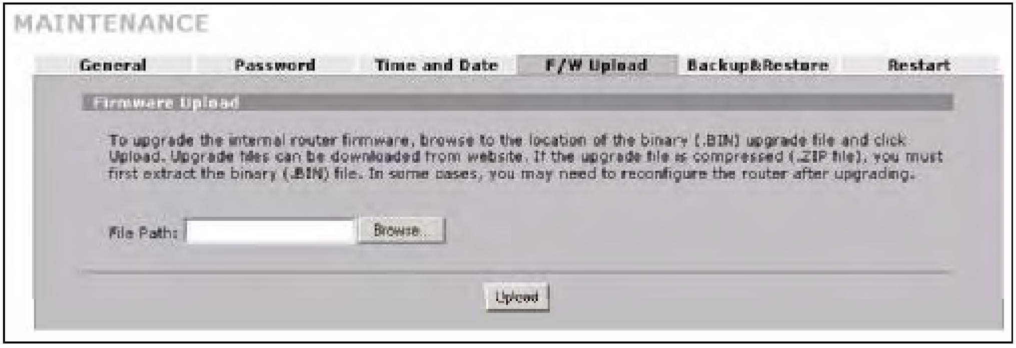
20.6 F/W Upload Screen

Find firmware at www.zyxel.com in a file that (usually) uses the system model name with a .bin extension, for example, "NBG410W3G.bin". The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot.

Click **MAINTENANCE** > **F/W UPLOAD**. Follow the instructions in this screen to upload firmware to your ZyXEL Device.

Only upload firmware for your specific model!

Figure 200 MAINTENANCE > Firmware Upload



To upgrade the internal router firmware, browse to the location of the binary (.BIN) upgrade file and click Upload. Upgrade files can be downloaded from website. If the upgrade file is compressed (.ZIP file), you must first extract the binary (.BIN) file. In some cases, you may need to reconfigure the router after upgrading.

File Path: Browse...

Upload

The following table describes the labels in this screen.

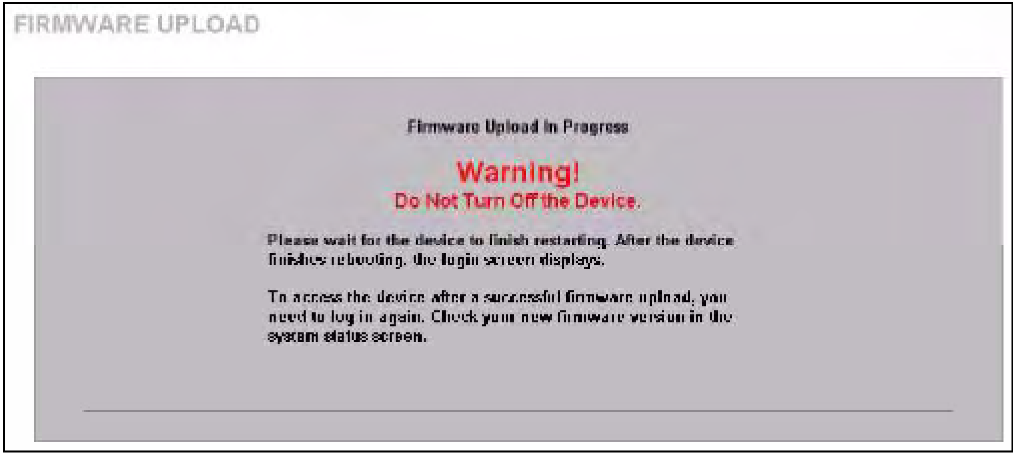
Table 116 MAINTENANCE > Firmware Upload

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click **Browse ...** to find it.
Browse...	Click **Browse...** to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click **Upload** to begin the upload process. This process may take up to two minutes.

Do not turn off the ZyXEL Device while firmware upload is in progress!

After you see the **Firmware Upload in Process** screen, wait two minutes before logging into the ZyXEL Device again.

Figure 201 Firmware Upload In Process



Firmware Upload In Progress

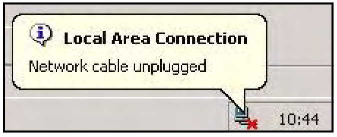
Warning!
Do Not Turn Off the Device.

Please wait for the device to finish restarting. After the device finishes rebooting, the login screen displays.

To access the device after a successful firmware upload, you need to log in again. Check your new firmware version in the system status screen.

The ZyXEL Device automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 202 Network Temporarily Disconnected



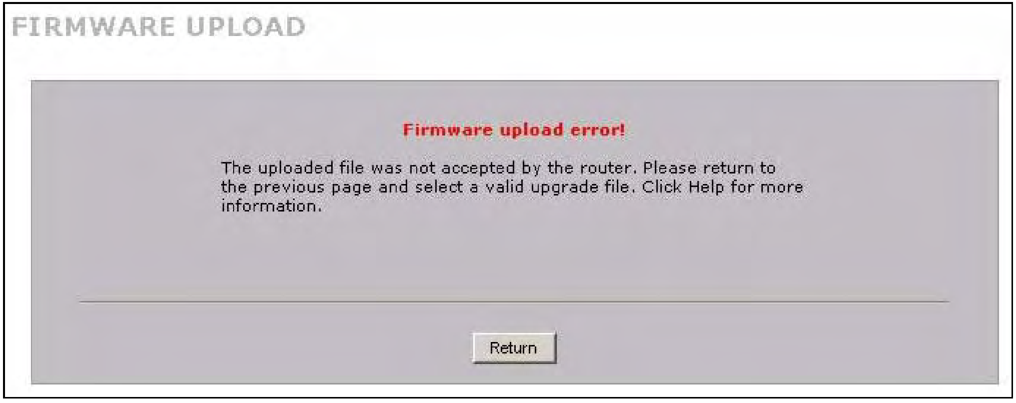
Local Area Connection

Network cable unplugged

After two minutes, log in again and check your new firmware version in the **HOME** screen.

If the upload was not successful, the following screen will appear. Click **Return** to go back to the **F/W Upload** screen.

Figure 203 Firmware Upload Error



FIRMWARE UPLOAD

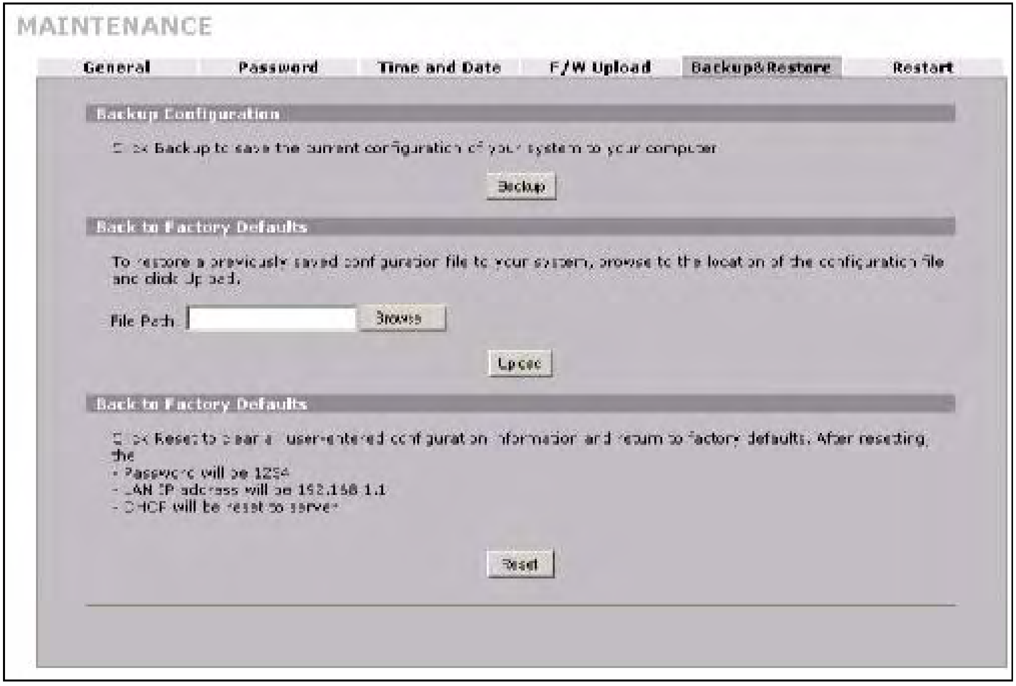
Firmware upload error!

The uploaded file was not accepted by the router. Please return to the previous page and select a valid upgrade file. Click Help for more information.

20.7 Backup and Restore

Click **MAINTENANCE** > **Backup & Restore**. Information related to factory defaults, backup configuration, and restoring configuration appears as shown next.

Figure 204 MAINTENANCE > Backup and Restore



Backup Configuration

Click Backup to save the current configuration of your system to your computer

Back to Factory Defaults

To restore a previously saved configuration file to your system, browse to the location of the configuration file and click Upload.

File Path

Back to Factory Defaults

Click Reset to clear all user-entered configuration information and return to factory defaults. After resetting, the
- Password will be 1234
- LAN IP address will be 192.168.1.1
- DHCP will be reset to server

20.7.1 Backup Configuration

Backup configuration allows you to back up (save) the ZyXEL Device’s current configuration to a file on your computer. Once your ZyXEL Device is configured and functioning properly, it is highly recommended that you back up your configuration file before making configuration changes. The backup configuration file will be useful in case you need to return to your previous settings.

Click **Backup** to save the ZyXEL Device’s current configuration to your computer.

20.7.2 Restore Configuration

Load a configuration file from your computer to your ZyXEL Device.

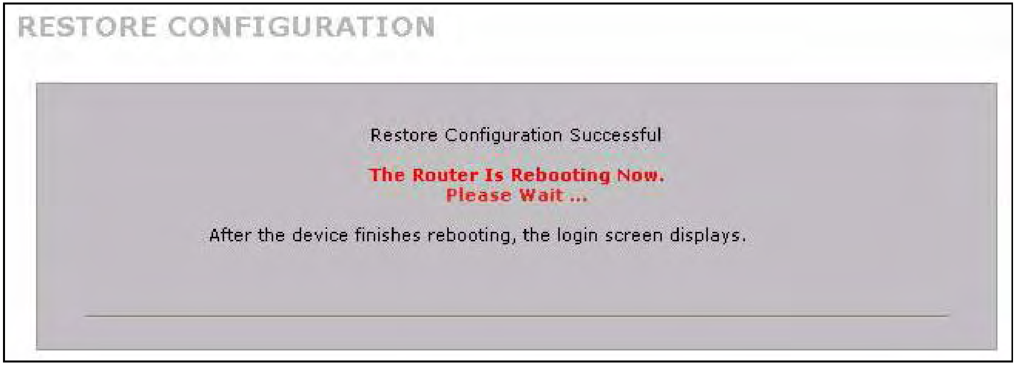
Table 117 Restore Configuration

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click **Browse ...** to find it.
Browse...	Click **Browse...** to find the file you want to upload. Remember that you must decompress compressed (.ZIP) files before you can upload them.
Upload	Click **Upload** to begin the upload process.

Do not turn off the ZyXEL Device while configuration file upload is in progress.

After you see a “restore configuration successful” screen, you must then wait one minute before logging into the ZyXEL Device again.

Figure 205 Configuration Upload Successful



RESTORE CONFIGURATION

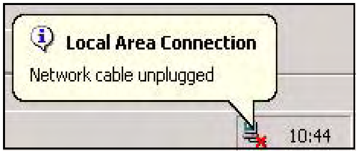
Restore Configuration Successful

The Router Is Rebooting Now.
Please Wait ...

After the device finishes rebooting, the login screen displays.

The ZyXEL Device automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 206 Network Temporarily Disconnected



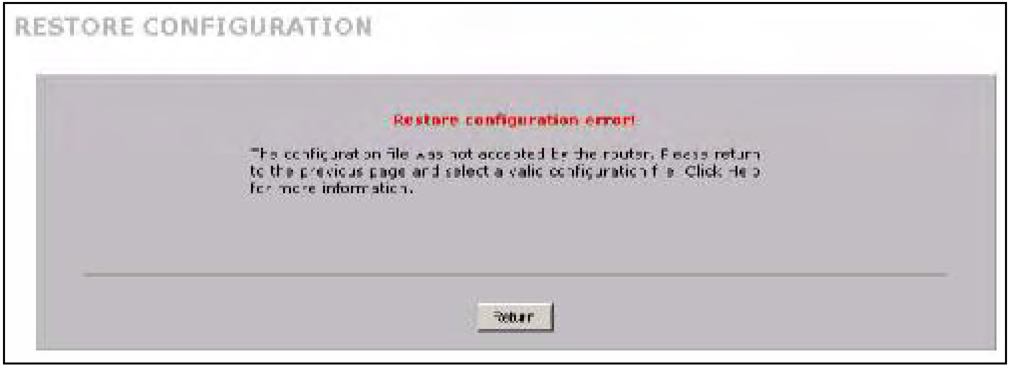
Local Area Connection

Network cable unplugged

If you uploaded the default configuration file you may need to change the IP address of your computer to be in the same subnet as that of the default device IP address (192.168.1.1). See your Quick Start Guide for details on how to set up your computer’s IP address.

If the upload was not successful, the following screen will appear. Click **Return** to go back to the **Configuration** screen.

Figure 207 Configuration Upload Error



RESTORE CONFIGURATION

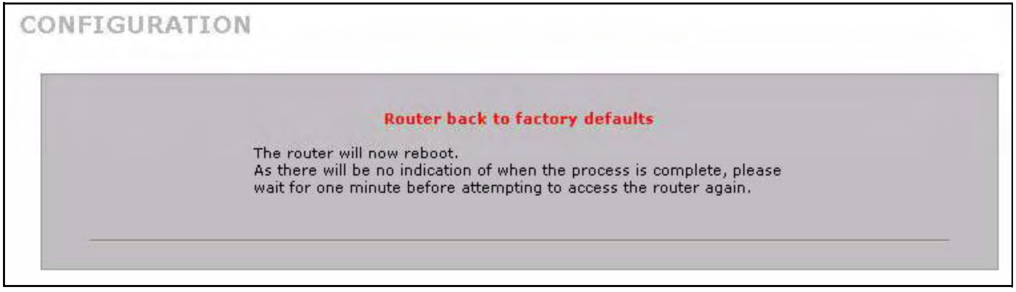
Restore configuration error!

The configuration file was not accepted by the router. Please return to the previous page and select a valid configuration file. Click Help for more information.

20.7.3 Back to Factory Defaults

Click the **Reset** button to clear all user-entered configuration information and return the ZyXEL Device to its factory defaults as shown on the screen. The following warning screen appears.

Figure 208 Reset Warning Message



Router back to factory defaults

The router will now reboot.
As there will be no indication of when the process is complete, please wait for one minute before attempting to access the router again.

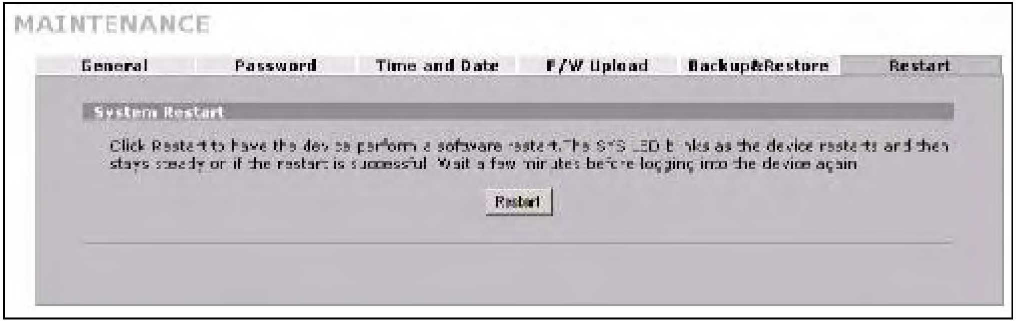
You can also press the hardware **RESET** button to reset the factory defaults of your ZyXEL Device. Refer to Section 2.3 on page 45 for more information on the **RESET** button.

20.8 Restart Screen

System restart allows you to reboot the ZyXEL Device without turning the power off.

Click **MAINTENANCE** > **Restart**. Click **Restart** to have the ZyXEL Device reboot. Restart is different to reset; (see Section 20.7.3 on page 335) reset returns the device to its default configuration.

Figure 209 MAINTENANCE > Restart



Click Restart to have the device perform a software restart. The SYS LED blinks as the device restarts and then stays steady on if the restart is successful. Wait a few minutes before logging into the device again.

PART VII

Troubleshooting and Specifications

21

Troubleshooting

This chapter offers some suggestions to solve problems you might encounter. The potential problems are divided into the following categories.

- Power, Hardware Connections, and LEDs
- ZyXEL Device Access and Login
- Internet Access
- 3G Connection

21.1 Power, Hardware Connections, and LEDs

The ZyXEL Device does not turn on. None of the LEDs turn on.

1. Make sure the ZyXEL Device is turned on.
2. Make sure you are using the power adaptor or cord included with the ZyXEL Device.
3. Make sure the power adaptor is connected to the ZyXEL Device and plugged in to an appropriate power source. Make sure the power source is turned on.
4. Turn the ZyXEL Device off and on or disconnect and re-connect the power adaptor to the ZyXEL Device.
5. If the problem continues, contact the vendor.

One of the LEDs does not behave as expected.

1. Make sure you understand the normal behavior of the LED. See Section 1.5.1 on page 39.
2. Check the hardware connections. See the Quick Start Guide.
3. Inspect your cables for damage. Contact the vendor to replace any damaged cables.
4. Turn the ZyXEL Device off and on or disconnect and re-connect the power adaptor to the ZyXEL Device.
5. If the problem continues, contact the vendor.

21.2 ZyXEL Device Access and Login

I forgot the LAN IP address for the ZyXEL Device.

1 The default LAN IP address is **192.168.1.1**.
2 Use the console port to log in to the ZyXEL Device.
3 If you changed the IP address and have forgotten it, you might get the IP address of the ZyXEL Device by looking up the IP address of the default gateway for your computer. To do this in most Windows computers, click **Start** > **Run**, enter **cmd**, and then enter **ipconfig**. The IP address of the **Default Gateway** might be the IP address of the ZyXEL Device (it depends on the network), so enter this IP address in your Internet browser.
4 If this does not work, you have to reset the device to its factory defaults. See Section 2.3 on page 45.

I forgot the password.

1 The default password is **1234**.
2 If this does not work, you have to reset the device to its factory defaults. See Section 2.3 on page 45.

I cannot see or access the **Login** screen in the web configurator.

1 Make sure you are using the correct IP address.
- The default LAN IP address is 192.168.1.1.
- Use the ZyXEL Device’s LAN IP address when configuring from the LAN.
- Use the ZyXEL Device’s WAN IP address when configuring from the WAN.
- If you changed the LAN IP address (Section 5.7 on page 104), use the new IP address.
- If you changed the LAN IP address and have forgotten it, see the troubleshooting suggestions for I forgot the LAN IP address for the ZyXEL Device.

2 Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and Section 1.5.1 on page 39.
3 Make sure your Internet browser does not block pop-up windows and has JavaScripts and Java enabled. See Appendix A on page 353.
4 Make sure your computer's Ethernet adapter is installed and functioning properly.
5 Make sure your computer is in the same subnet as the ZyXEL Device. (If you know that there are routers between your computer and the ZyXEL Device, skip this step.)

- If there is a DHCP server on your network, make sure your computer is using a dynamic IP address. See Appendix B on page 361. Your ZyXEL Device is a DHCP server by default.

6 Reset the device to its factory defaults, and try to access the ZyXEL Device with the default IP address. See Section 2.3 on page 45.

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

Advanced Suggestions

- Try to access the ZyXEL Device using another service, such as Telnet. If you can access the ZyXEL Device, check the remote management settings, and firewall rules to find out why the ZyXEL Device does not respond to HTTP.
- If your computer is connected to the **WAN** port or is connected wirelessly, use a computer that is connected to a **LAN** port.
- You may also need to clear your Internet browser's cache.

  In Internet Explorer, click **Tools** and then **Internet Options** to open the **Internet Options** screen.

  In the **General** tab, click **Delete** Files. In the pop-up window, select the **Delete all offline content** check box and click **OK**. Click **OK** in the **Internet Options** screen to close it.
- If you disconnect your computer from one device and connect it to another device that has the same IP address, your computer's ARP (Address Resolution Protocol) table may contain an entry that maps the management IP address to the previous device's MAC address).

  In Windows, use **arp -d** at the command prompt to delete all entries in your computer's ARP table.

I can see the **Login** screen, but I cannot log in to the ZyXEL Device.

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

2 You cannot log in to the web configurator while someone is using Telnet, or the console port to access the ZyXEL Device. Log out of the ZyXEL Device in the other session, or ask the person who is logged in to log out.

3 Turn the ZyXEL Device off and on or disconnect and re-connect the power adaptor or cord to the ZyXEL Device.

4 If this does not work, you have to reset the device to its factory defaults. See Section 2.3 on page 45.

I cannot Telnet to the ZyXEL Device.

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

I cannot use FTP to upload / download the configuration file. / I cannot use FTP to upload new firmware.

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

21.3 Internet Access

I cannot get a WAN IP address from the ISP.

1 The ISP provides the WAN IP address after authenticating you. Authentication may be through the user name and password, the MAC address or the host name.

  The username and password apply to PPPoE and PPPoA encapsulation only. Make sure that you have entered the correct **Service Type**, **User Name** and **Password** (be sure to use the correct casing). Refer to the WAN setup chapter (web configurator).

2 Disconnect all the cables from your device, and follow the directions in the Quick Start Guide again.

3 If the problem continues, contact your ISP.

I cannot access the Internet.

1 Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and Section 1.5.1 on page 39.

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

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

4 Disconnect all the cables from your device, and follow the directions in the Quick Start Guide again.

5 If the problem continues, contact your ISP.

I cannot access the Internet anymore. I had access to the Internet (with the ZyXEL Device), but my Internet connection is not available anymore.

1 Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and Section 1.5.1 on page 39.
2 If you use PPPoA or PPPoE encapsulation, check the idle time-out setting. Refer to the Chapter 6 on page 111.
3 Reboot the ZyXEL Device.
4 If the problem continues, contact your ISP.

The Internet connection is slow or intermittent.

1 There might be a lot of traffic on the network. Look at the LEDs, and check Section 1.5.1 on page 39. If the ZyXEL Device is sending or receiving a lot of information, try closing some programs that use the Internet, especially peer-to-peer applications.
2 Check the signal strength. If the signal strength is low, try moving the ZyXEL Device closer to the AP if possible, and look around to see if there are any devices that might be interfering with the wireless network (for example, microwaves, other wireless networks, and so on).
3 Reboot the ZyXEL Device.
4 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

21.4 3G Connection

The 3G OPERATION LED is off.

- Check the 3G SIM card is correctly inserted. See the Quick Start Guide for instructions.
- Check your 3G settings are correctly configured in the 3G screen, including your PIN, user name and password (if required) and telephone number (required). Use the information provided by your 3G ISP for your 3G user account.
- If you have used a different 3G SIM card with this device previously, the 3G card may have stored the settings for your previous SIM card. Ensure you have entered the correct settings for your current SIM card and click **Apply**.
- Check that you have selected the correct 3G interface in the **3G (WAN2**) screen.
- Check the **HOME** screen. An error message displays in the **HOME** screen if you have entered the incorrect PIN in the **3G (WAN2)** screen.
- Check your 3G connection status in the **HOME** screen. If WAN2 has no IP address, click **Dial** to request your 3G ISP for an IP address.
- Check your 3G account status with your 3G service provider.

? The 3G SIGNAL STRENGTH LED shows the 3G signal is weak or not available.

- Check that your 3G service provider has coverage in your area.
- Check that in the **3G (WAN2)** screen you have selected the correct 3G service for your area. In some areas certain kinds of 3G may not be available.
- Move the ZyXEL Device away from any structures such as large buildings or tunnels that may be blocking the 3G signal.
- Move the ZyXEL Device away from devices that cause radio signal interference, such as microwave ovens and high voltage power lines.
- Check that the ZyXEL Device’s antenna is fully extended and is pointing upwards.

? The 3G OPERATION LED is on but my 3G connection is slow or non-existent.

- Check that WAN2 has an IP address in the **HOME** page. Click **Dial** (several times if necessary) to obtain a WAN2 IP address.
- Try moving to an area with better reception. If the signal quality is poor, the 3G modem will time out before obtaining an IP address.
- Check that you have enabled NAT in the **3G (WAN2)** screen.
- Actual download speeds usually differ from maximum advertised speeds. Typical data rates are as follows. If your average download speeds are much lower then the typical data rates given below, check the **3G SIGNAL STRENGTH** LED.
  - If the **3G SIGNAL STRENGTH** LED shows a weak signal, follows\ the suggestions given in The 3G SIGNAL STRENGTH LED shows the 3G signal is weak or not available.
  - If it shows a strong signal, contact your 3G service provider for more help.

Table 118 Typical 3G transmission speeds

PACKET DATA SERVICE		THEORETICAL MAXIMUM DATA RATE	TYPICAL DATA RATE
EDGE	Upload	236 kbps	100~130 kbps
	Download	236 kbps	100~130 kbps
UMTS	Upload	384 kbps	100~300 kbps
	Download	384 kbps	100~300 kbps
HSDPA	Upload	384 kbps	100~300 kbps
	Download	3.6 Mbps	Up to 2 Mbps

22

Product Specifications

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

22.1 General ZyXEL Device Specifications

The following tables summarize the ZyXEL Device's hardware and firmware features.

Table 119 Hardware Specifications

Dimensions	190 (W) x 150 (D) x 33 (H) mm
Weight	380 g
Power Specification	12V DC 1.5 A
Ethernet Interface	
LAN/DMZ	Four LAN/DMZ auto-negotiating, auto MDI/MDI-X 10/100 Mbps RJ-45 Ethernet ports.
WAN	One auto-negotiating, auto MDI/MDI-X 10/100 Mbps RJ-45 Ethernet port.
Reset Button	Restores factory default settings.
Internal 3G module	SierraWireless MC8775 (NBG410W3G only)
USB slot	The USB port is reserved for future usage. It cannot transmit signals simultaneously with the internal 3G module.
SIM Card Slot	For installing a 3G SIM card (NBG410W3G only).
Antenna	NBG410W3G: One internal 3.6 dBi antenna One external 850/900/1800/1900/2100 MHz 3G antenna NBG412W3G: One external 3.6 dBi antenna
Distance between the centers of the holes (for wall mounting) on the device's back.	165.75 mm
Screw size for wall-mounting	M 4*10 Tap Screw, see Figure 210 on page 348.
Operation Environment	Temperature: 0º C ~ 40º C Humidity: 20% ~ 95% (non-condensing)
Storage Environment	Temperature: -30º ~ 60º C Humidity: 20% ~ 95% RH (non-condensing)
Certifications	EMC: FCC Part 15 Class B, CE-EMC Class B, C-Tick Class B Safety: CSA International, (UL60950-1, CSA60950-1, EN60950-1, IEC60950-1)

Table 120 Firmware Specifications

FEATURE	DESCRIPTION
Default IP Address	192.168.1.1
Default Subnet Mask	255.255.255.0 (24 bits)
Default Password	1234
Default DHCP Pool	192.168.1.33 to 192.168.1.160
Device Management	Use the web configurator to easily configure the rich range of features on the ZyXEL Device.
3G (2.5G) Functionality	Supports UMTS, HSDPA, UMTS, EDGE 3G and GPRS 2.5G standards.
Wi-Fi Functionality	Allows the IEEE 802.11b and/or IEEE 802.11g wireless clients to connect to the ZyXEL Device wirelessly. Enable wireless security (WEP, WPA(2), WPA(2)-PSK) and/or MAC filtering to protect your wireless network.
Firmware Upgrade	Download new firmware (when available) from the ZyXEL web site and use the web configurator, an FTP or a TFTP tool to put it on the ZyXEL Device. Note: Only upload firmware for your specific model!
Configuration Backup & Restoration	Make a copy of the ZyXEL Device's configuration. You can put it back on the ZyXEL Device later if you decide to revert back to an earlier configuration.
Network Address Translation (NAT)	Each computer on your network must have its own unique IP address. Use NAT to convert your public IP address(es) to multiple private IP addresses for the computers on your network.
Port Forwarding	If you have a server (mail or web server for example) on your network, you can use this feature to let people access it from the Internet.
DHCP (Dynamic Host Configuration Protocol)	Use this feature to have the ZyXEL Device assign IP addresses, an IP default gateway and DNS servers to computers on your network.
Dynamic DNS Support	With Dynamic DNS (Domain Name System) support, you can use a fixed URL, www.zyxel.com for example, with a dynamic IP address. You must register for this service with a Dynamic DNS service provider.
IP Multicast	IP multicast is used to send traffic to a specific group of computers. The ZyXEL Device supports versions 1 and 2 of IGMP (Internet Group Management Protocol) used to join multicast groups (see RFC 2236).
IP Alias	IP alias allows you to subdivide a physical network into logical networks over the same Ethernet interface with the ZyXEL Device itself as the gateway for each subnet.
Time and Date	Get the current time and date from an external server when you turn on your ZyXEL Device. You can also set the time manually. These dates and times are then used in logs.
Logging and Tracing	Use packet tracing and logs for troubleshooting. You can send logs from the ZyXEL Device to an external syslog server.
PPPoE	PPPoE mimics a dial-up Internet access connection.
PPTP Encapsulation	Point-to-Point Tunneling Protocol (PPTP) enables secure transfer of data through a Virtual Private Network (VPN). The ZyXEL Device supports one PPTP connection at a time.
Universal Plug and Play (UPnP)	A UPnP-enabled device can dynamically join a network, obtain an IP address and convey its capabilities to other devices on the network.

Table 120 Firmware Specifications

FEATURE	DESCRIPTION
RoadRunner Support	The ZyXEL Device supports Time Warner's RoadRunner Service in addition to standard cable modem services.
Firewall	You can configure firewall on the ZyXEL Device for secure Internet access. When the firewall is on, by default, all incoming traffic from the Internet to your network is blocked unless it is initiated from your network. This means that probes from the outside to your network are not allowed, but you can safely browse the Internet and download files for example.
Remote Management	This allows you to decide whether a service (HTTP or FTP traffic for example) from a computer on a network (LAN or WAN for example) can access the ZyXEL Device.

Table 121 Feature Specifications

FEATURE	SPECIFICATION
Local User Database Entries	32
Static DHCP Table Entries	32
Static Routes	30
Concurrent Sessions (NAT sessions)	3,000
Address Mapping Rules	10
Port Forwarding Rules	20
DNS Address Record Entries	30
DNS Name Server Record Entries	16
Firewall Throughput (with NAT)	12 Mbps
Output Power (Maximum)	IEEE 802.11b: 16 dBm at 11 Mbps CCK, QPSK, BPSK IEEE 802.11g: 13 dBm at 54 Mbps OFDM

22.2 Wall-mounting Instructions

Complete the following steps to hang your ZyXEL Device on a wall.

See Table 119 on page 345 for the size of screws to use and how far apart to place them.

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

2 Drill two holes for the screws.

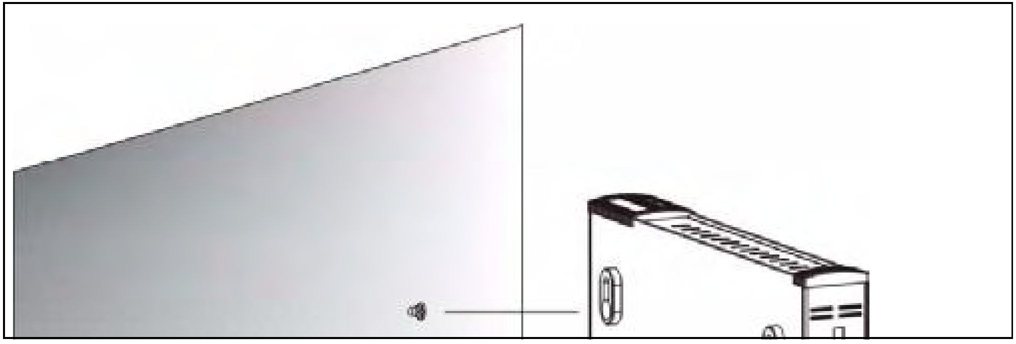
Be careful to avoid damaging pipes or cables located inside the wall when drilling holes for the screws.

3 Do not insert the screws all the way into the wall. Leave a small gap of about 0.5 cm between the heads of the screws and the wall.

4 Make sure the screws are snugly fastened to the wall. They need to hold the weight of the ZyXEL Device with the connection cables.

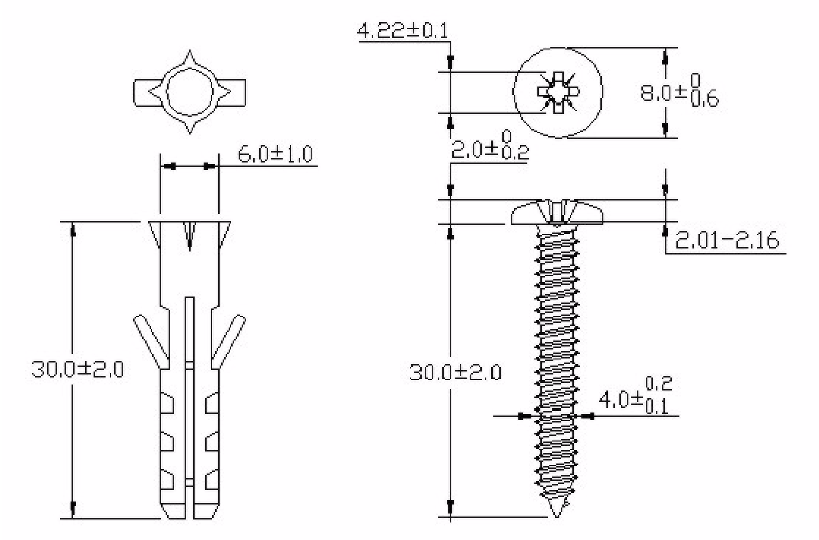
5 Align the holes on the back of the ZyXEL Device with the screws on the wall. Hang the ZyXEL Device on the screws.

Figure 210 Wall-mounting Example



The following are dimensions of an M4 tap screw and masonry plug used for wall mounting. All measurements are in millimeters (mm).

Figure 211 Masonry Plug and M4 Tap Screw



22.3 Power Adaptor Specifications

NORTH AMERICAN PLUG STANDARDS	
AC POWER ADAPTOR MODEL	PSA18R-120P (ZA)-R
INPUT POWER	100-240VAC, 50/60HZ, 0.5A
OUTPUT POWER	12VDC, 1.5A
POWER CONSUMPTION	18 W MAX.
SAFETY STANDARDS	UL, CUL (UL 60950-1 FIRST EDITIONCSA C22.2 NO. 60950-1-03 1ST.)

EUROPEAN PLUG STANDARDS	
AC POWER ADAPTOR MODEL	PSA18R-120P (ZE)-R
INPUT POWER	100-240VAC, 50/60HZ, 0.5A
OUTPUT POWER	12VDC, 1.5A
POWER CONSUMPTION	18 W MAX.
SAFETY STANDARDS	TUV, CE (EN 60950-1)

UNITED KINGDOM PLUG STANDARDS	
AC POWER ADAPTOR MODEL	PSA18R-120P (ZK)-R
INPUT POWER	100-240VAC, 50/60HZ, 0.5A
OUTPUT POWER	12VDC, 1.5A
POWER CONSUMPTION	18 W MAX.
SAFETY STANDARDS	TUV (BS EN 60950-1)

PART VIII

Appendices and Index

The appendices provide general information. Some details may not apply to your ZyXEL Device.

A

Pop-up Windows, JavaScripts and Java Permissions

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

- Web browser pop-up windows from your device.
- JavaScripts (enabled by default).
- Java permissions (enabled by default).

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

Internet Explorer Pop-up Blockers

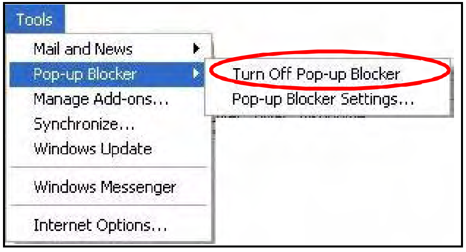
You may have to disable pop-up blocking to log into your device.

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 212 Pop-up Blocker

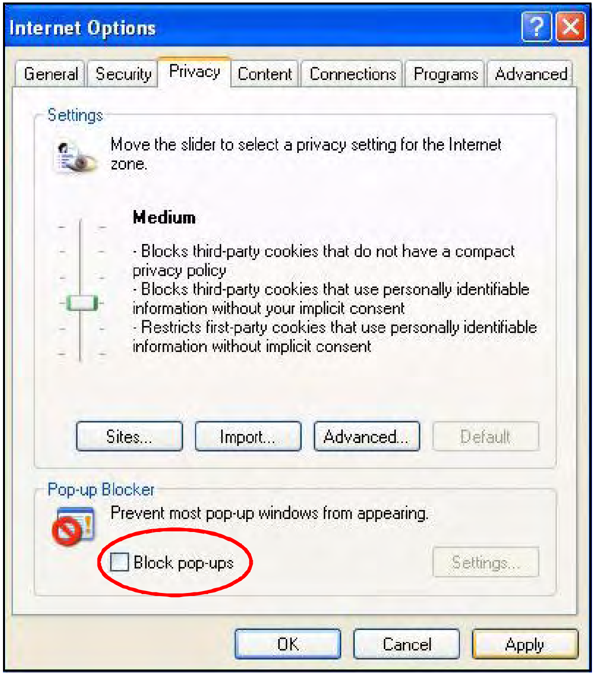


You can also check if pop-up blocking is disabled in the **Pop-up Blocker** section in the **Privacy** tab.

1 In Internet Explorer, select **Tools**, **Internet Options**, **Privacy**.

2 Clear the **Block pop-ups** check box in the **Pop-up Blocker** section of the screen. This disables any web pop-up blockers you may have enabled.

Figure 213 Internet Options: Privacy



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

Medium

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

Prevent most pop-up windows from appearing.

□ Block pop-ups

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

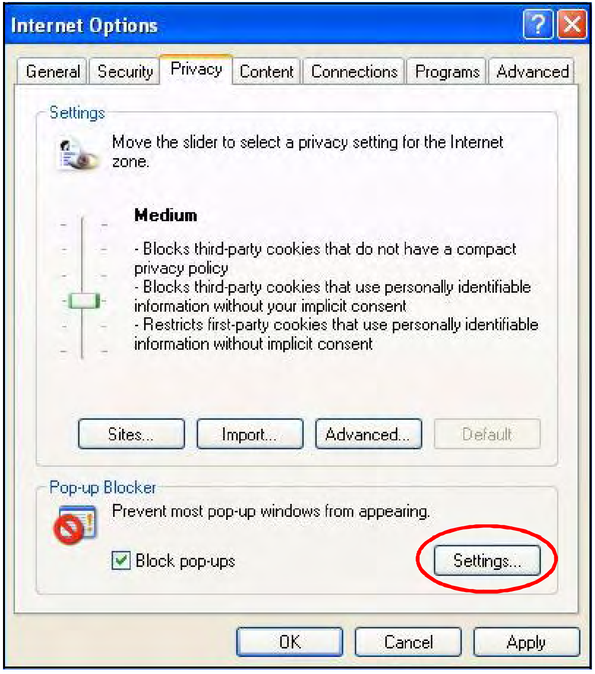
Enable Pop-up Blockers with Exceptions

Alternatively, if you only want to allow pop-up windows from your device, see the following steps.

1 In Internet Explorer, select **Tools**, **Internet Options** and then the **Privacy** tab.

2 Select **Settings…**to open the **Pop-up Blocker Settings** screen.

Figure 214 Internet Options: Privacy



Settings

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

Medium

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

Pop-up Blocker

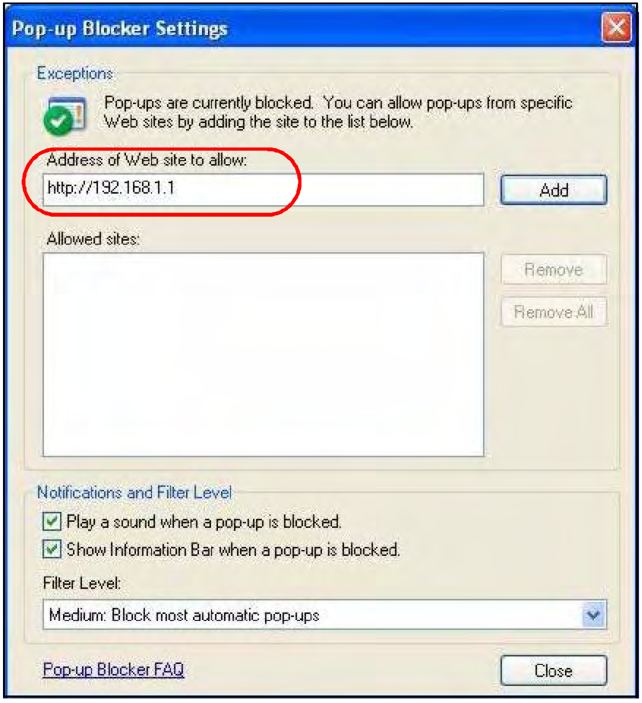
Prevent most pop-up windows from appearing.

☑ Block pop-ups

3 Type the IP address of your device (the web page that you do not want to have blocked) with the prefix “http://”. For example, http://192.168.167.1.

4 Click **Add** to move the IP address to the list of **Allowed sites**.

Figure 215 Pop-up Blocker Settings



Exceptions

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

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

Allowed sites:

Notifications and Filter Level

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

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

Filter Level: Medium: Block most automatic pop-ups

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

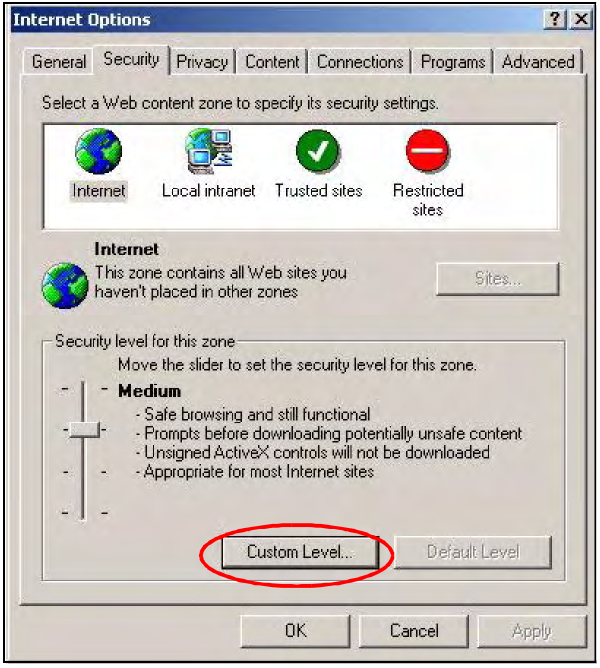
6 Click **Apply** to save this setting.

JavaScripts

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

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

Figure 216 Internet Options: Security



Select a Web content zone to specify its security settings.

Internet

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

Security level for this zone

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

Medium

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

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

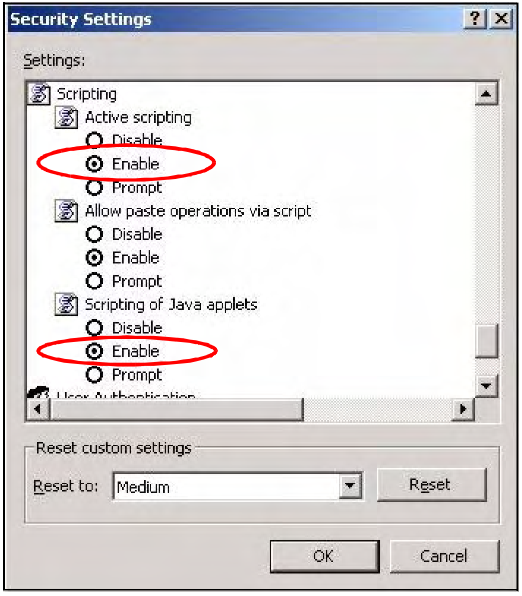
3 Scroll down to **Scripting**.

4 Under **Active scripting** make sure that **Enable** is selected (the default).

5 Under **Scripting of Java applets** make sure that **Enable** is selected (the default).

6 Click **OK** to close the window.

Figure 217 Security Settings - Java Scripting



Security Settings

Settings:

Scripting

Active scripting
- ○ Disable
- ● Enable
- ○ Prompt

Allow paste operations via script
- ○ Disable
- ● Enable
- ○ Prompt

Scripting of Java applets
- ○ Disable
- ● Enable
- ○ Prompt

User Authentication

Reset custom settings

Reset to: Medium

Java Permissions

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

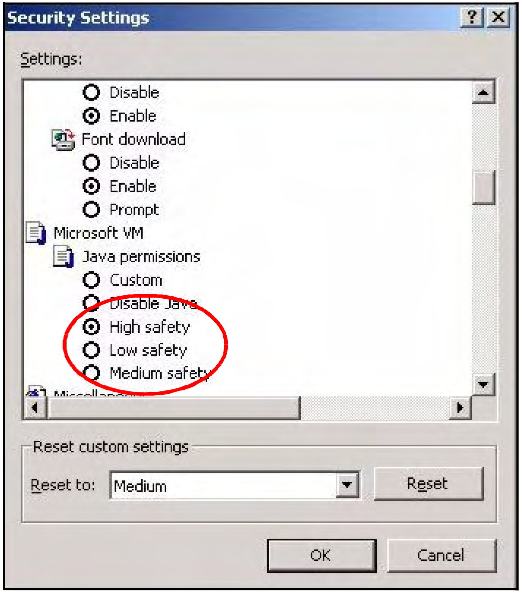
2 Click the **Custom Level...** button.

3 Scroll down to **Microsoft VM**.

4 Under **Java permissions** make sure that a safety level is selected.

5 Click **OK** to close the window.

Figure 218 Security Settings - Java



Security Settings

Settings:
- ○ Disable
- ● Enable

Font download
- ○ Disable
- ● Enable
- ○ Prompt

Microsoft VM

Java permissions
- ○ Custom
- ○ Disable Java
- ● High safety
- ○ Low safety
- ○ Medium safety

Miscellaneous

Reset custom settings

Reset to: Medium

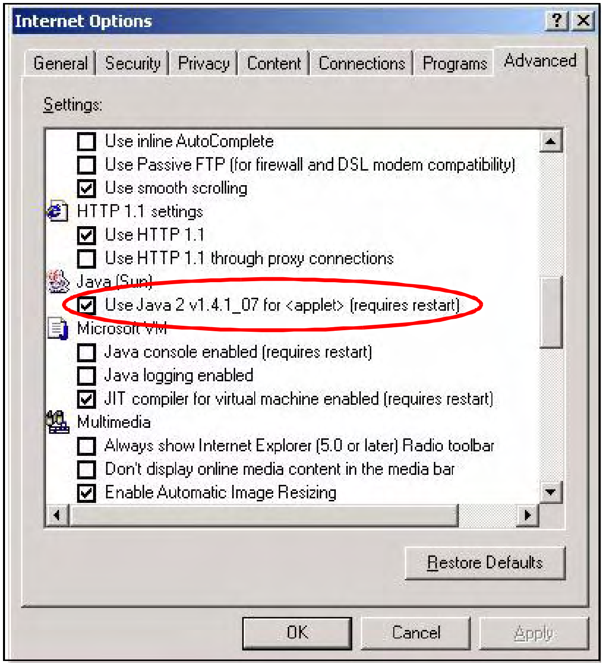
JAVA (Sun)

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

2 Make sure that **Use Java 2 for <applet>** under **Java (Sun)** is selected.

3 Click **OK** to close the window.

Figure 219 Java (Sun)



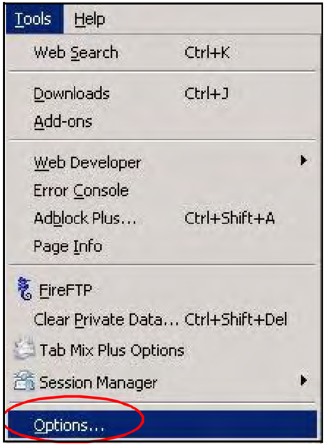
□ Use inline AutoComplete
□ Use Passive FTP (for firewall and DSL modem compatibility)
☑ Use smooth scrolling
HTTP 1.1 settings
☑ Use HTTP 1.1
□ Use HTTP 1.1 through proxy connections
Java (Sun)
☑ Use Java 2 v1.4.1_07 for <applet> (requires restart)
Microsoft VM
□ Java console enabled (requires restart)
□ Java logging enabled
☑ JIT compiler for virtual machine enabled (requires restart)
Multimedia
□ Always show Internet Explorer (5.0 or later) Radio toolbar
□ Don't display online media content in the media bar
☑ Enable Automatic Image Resizing

Mozilla Firefox

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

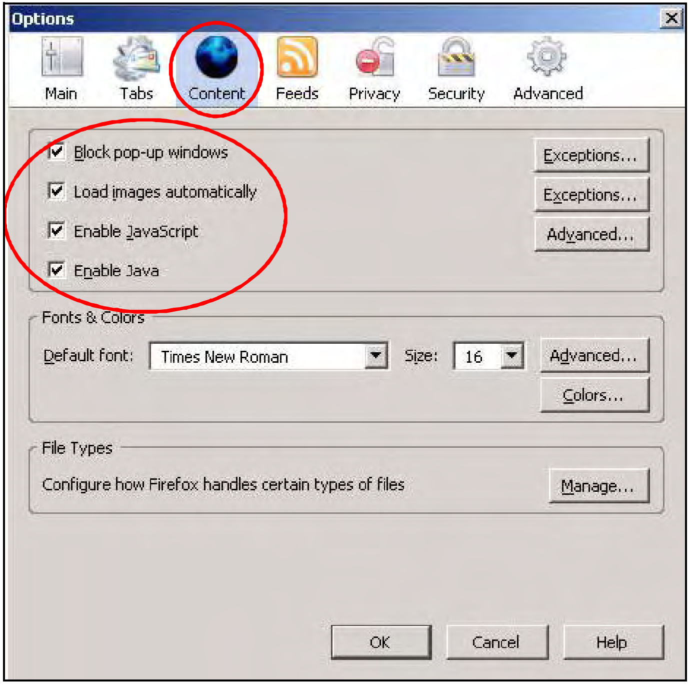
You can enable Java, Javascripts and pop-ups in one screen. Click **Tools,** then click **Options** in the screen that appears.

Figure 220 Mozilla Firefox: Tools > Options



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

Figure 221 Mozilla Firefox Content Security



☑ Block pop-up windows

☑ Load images automatically

☑ Enable JavaScript

☑ Enable Java

Default font: Times New Roman Size: 16

Configure how Firefox handles certain types of files

B

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.

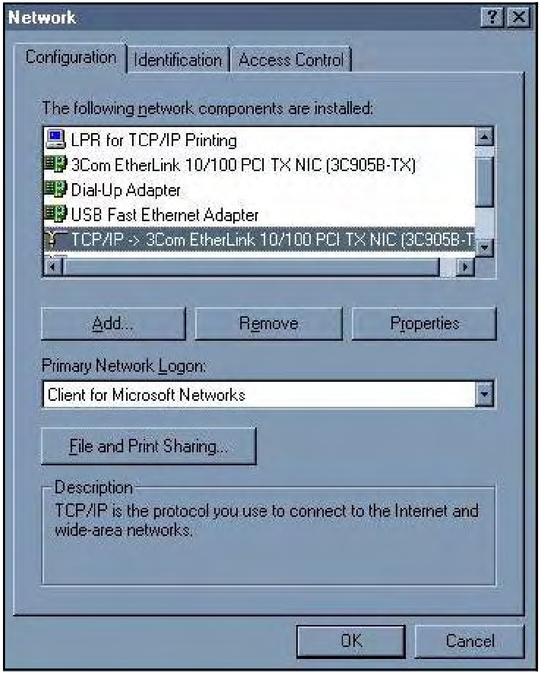
After the appropriate TCP/IP components are installed, configure the TCP/IP settings in order to "communicate" with your network.

If you manually assign IP information instead of using dynamic assignment, make sure that your computers have IP addresses that place them in the same subnet as the ZyXEL Device's LAN port.

Windows 95/98/Me

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

Figure 222 WIndows 95/98/Me: Network: Configuration



The following network components are installed:

LPR for TCP/IP Printing
3Com 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

Primary Network Logon:
Client for Microsoft Networks

Description
TCP/IP is the protocol you use to connect to the Internet and wide-area networks.

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.

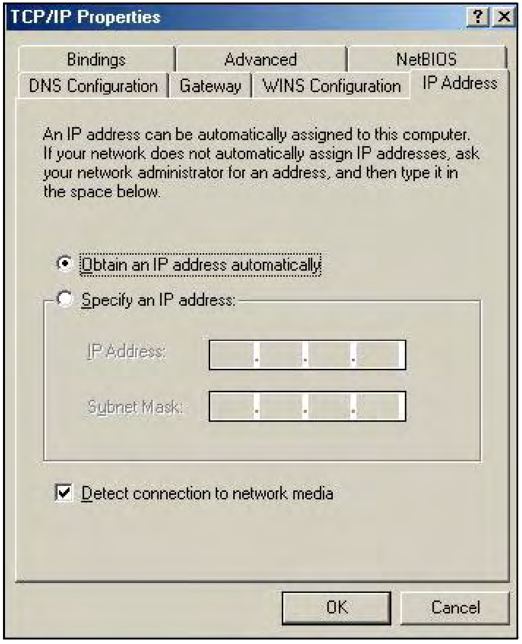
Configuring

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 223 Windows 95/98/Me: TCP/IP Properties: IP Address



TCP/IP Properties

An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.

● Obtain an IP address automatically

○ Specify an IP address:

IP Address: . . .

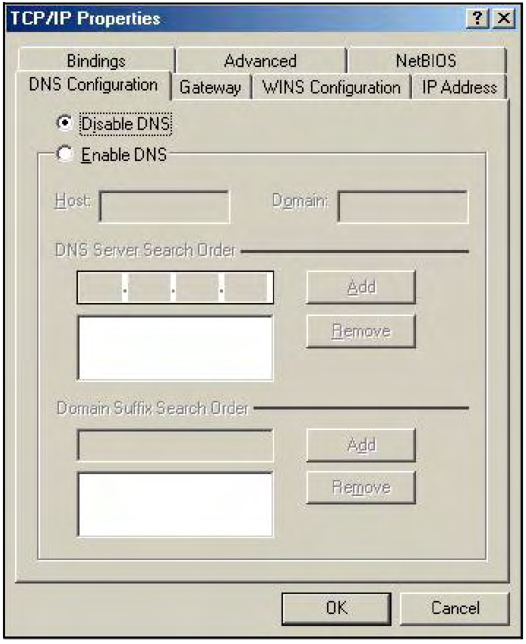
Subnet Mask: . . .

☑ Detect connection to network media

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).

Figure 224 Windows 95/98/Me: TCP/IP Properties: DNS Configuration



● Disable DNS

○ Enable DNS

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 Turn on your ZyXEL Device and 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.

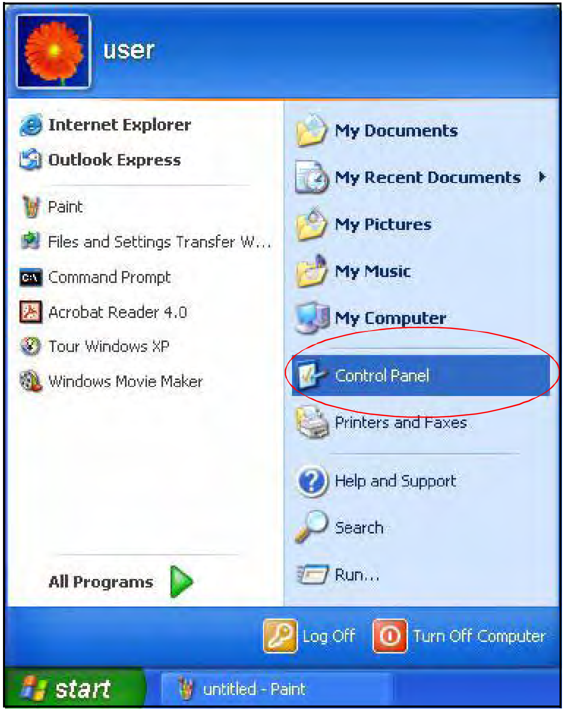
3 Select your network adapter. You should see your computer's IP address, subnet mask and default gateway.

Windows 2000/NT/XP

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

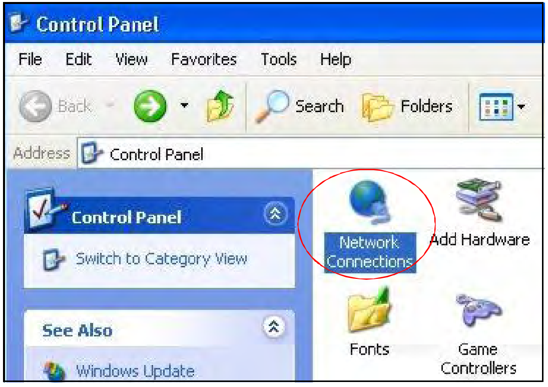
1 Click **start** (**Start** in Windows 2000/NT), **Settings**, **Control Panel**.

Figure 225 Windows XP: Start Menu



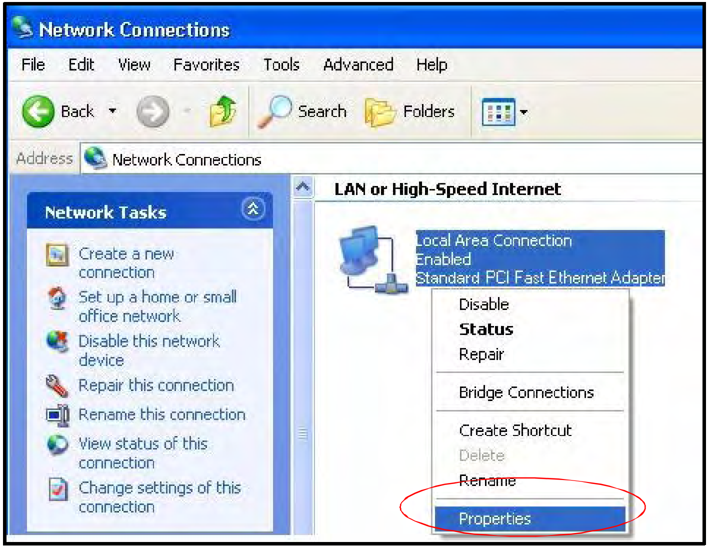
2 In the **Control Panel**, double-click **Network Connections** (**Network and Dial-up Connections** in Windows 2000/NT).

Figure 226 Windows XP: Control Panel



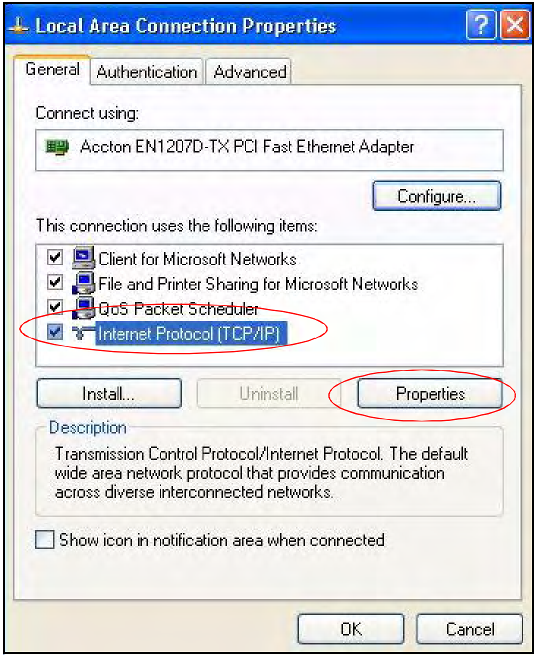
3 Right-click **Local Area Connection** and then click **Properties**.

Figure 227 Windows XP: Control Panel: Network Connections: Properties


Network Connections
File Edit View Favorites Tools Advanced Help
Back
Search
Folders
Address Network Connections
Network Tasks
Create a new connection
Set up a home or small office network
Disable this network device
Repair this connection
Rename this connection
View status of this connection
Change settings of this connection
LAN or High-Speed Internet
Local Area Connection
Enabled
Standard PCI Fast Ethernet Adapter
Disable
Status
Repair
Bridge Connections
Create Shortcut
Delete
Rename
Properties

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

Figure 228 Windows XP: Local Area Connection Properties



Connect using:

Accton EN1207D-TX PCI Fast Ethernet Adapter

This connection uses the following items:

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

Description

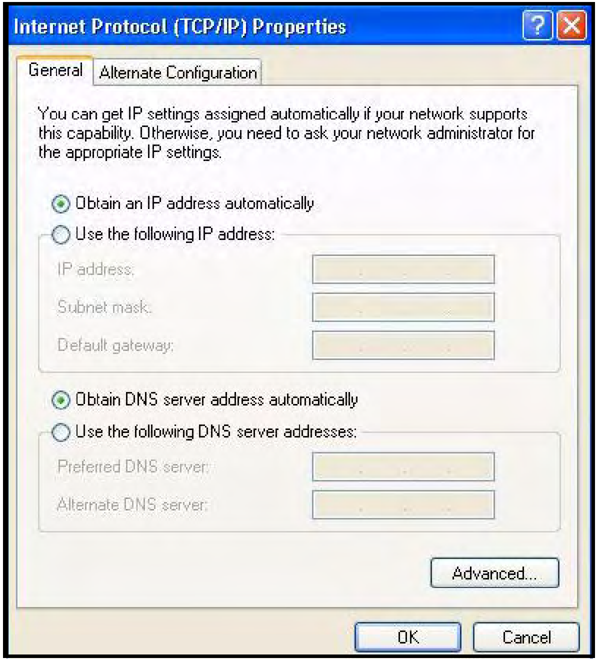
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

☐ Show icon in notification area when connected

5 The **Internet Protocol TCP/IP Properties** window opens (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 229 Windows XP: Internet Protocol (TCP/IP) Properties



Internet Protocol (TCP/IP) Properties

General | Alternate Configuration

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

● Obtain an IP address automatically

○ Use the following IP address:

IP address:

Subnet mask:

Default gateway:

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server:

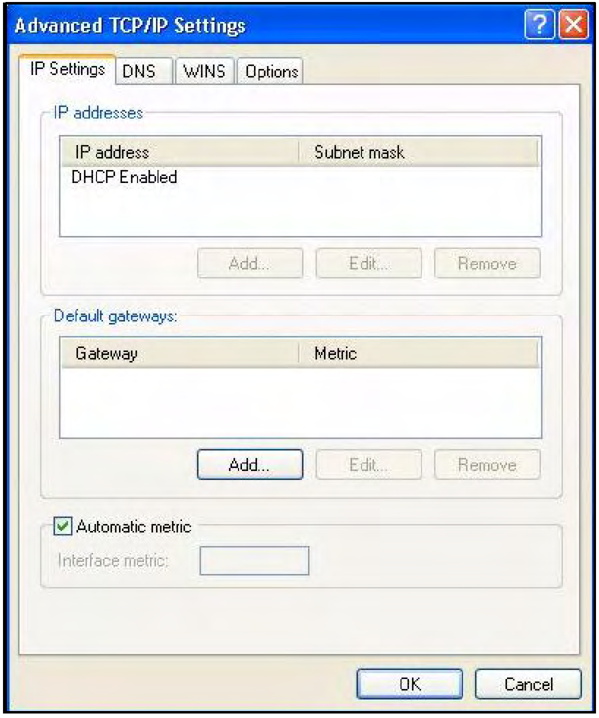
Alternate DNS server:

6 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.

Figure 230 Windows XP: Advanced TCP/IP Properties



Advanced TCP/IP Settings

IP Settings | DNS | WINS | Options

IP addresses

IP address	Subnet mask
DHCP Enabled	

Default gateways:

Gateway	Metric

☑ Automatic metric

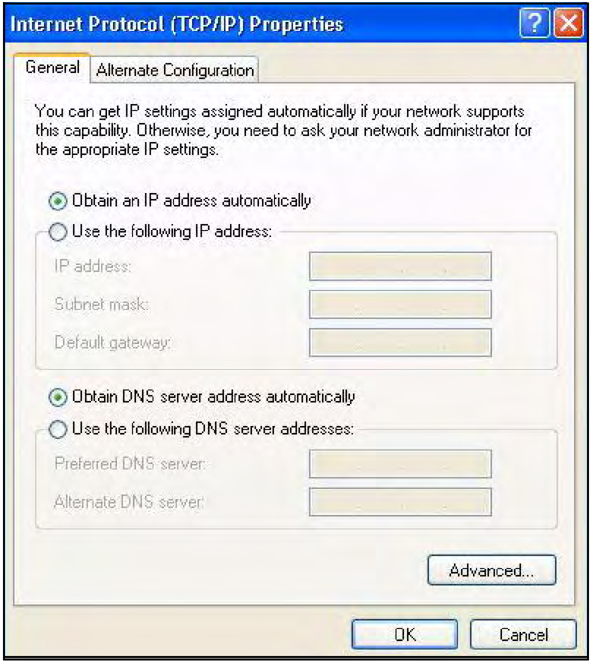
Interface metric:

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.

Figure 231 Windows XP: Internet Protocol (TCP/IP) Properties



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

● Obtain an IP address automatically

○ Use the following IP address:

IP address:

Subnet mask:

Default gateway:

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server:

Alternate DNS server:

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 Turn on your ZyXEL Device and restart your computer (if prompted).

Verifying Settings

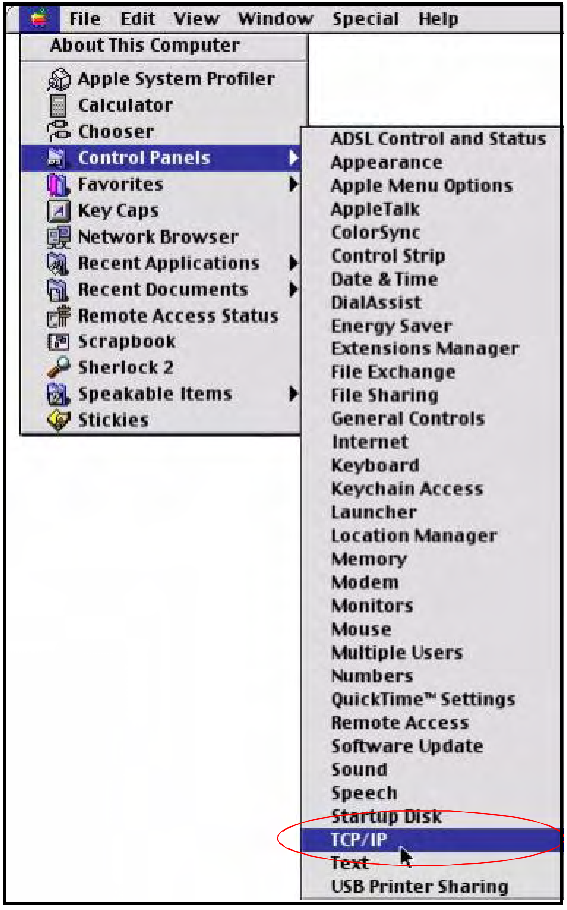
1 Click **Start**, **All Programs**, **Accessories** and then **Command Prompt**.

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 8/9

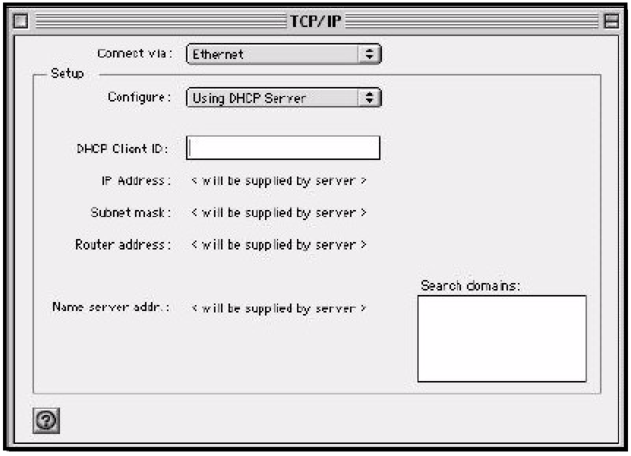
1 Click the **Apple** menu, **Control Panel** and double-click **TCP/IP** to open the **TCP/IP Control Panel**.

Figure 232 Macintosh OS 8/9: Apple Menu



2 Select **Ethernet built-in** from the **Connect via** list.

Figure 233 Macintosh OS 8/9: TCP/IP


TCP/IP

Connect via: Ethernet

Setup

Configure: Using DHCP Server

DHCP Client ID:

IP Address: < will be supplied by server >

Subnet mask: < will be supplied by server >

Router address: < will be supplied by server >

Name server addr.: < will be supplied by server >

Search domains:

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

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 ZyXEL Device in the **Router address** box.

5 Close the **TCP/IP Control Panel**.

6 Click **Save** if prompted, to save changes to your configuration.

7 Turn on your ZyXEL Device and restart your computer (if prompted).

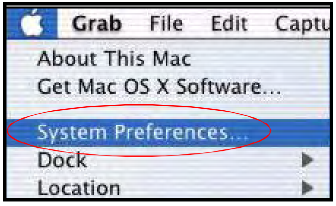
Verifying Settings

Check your TCP/IP properties in the **TCP/IP Control Panel** window.

Macintosh OS X

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

Figure 234 Macintosh OS X: Apple Menu

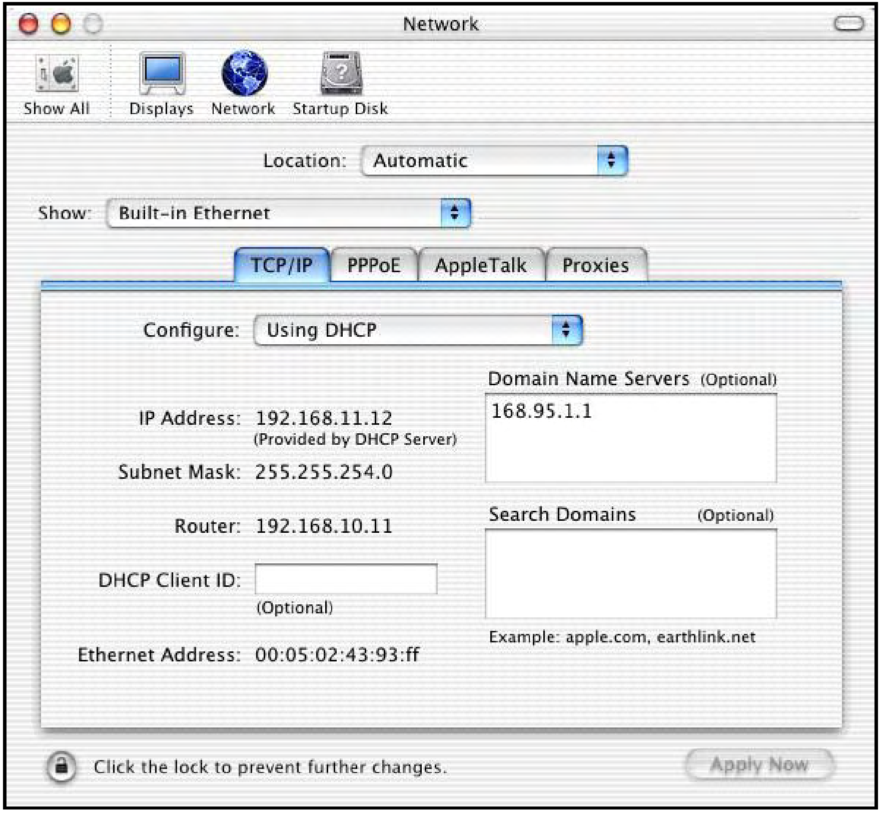


2 Click **Network** in the icon bar.

- 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 235 Macintosh OS X: Network



Location: Automatic

Show: Built-in Ethernet

Configure: Using DHCP

IP Address: 192.168.11.12
(Provided by DHCP Server)

Subnet Mask: 255.255.254.0

Router: 192.168.10.11

DHCP Client ID:
(Optional)

Ethernet Address: 00:05:02:43:93:ff

Domain Name Servers (Optional)
168.95.1.1

Search Domains (Optional)

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 ZyXEL Device in the **Router address** box.

5 Click **Apply Now** and close the window.

6 Turn on your ZyXEL Device and 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.

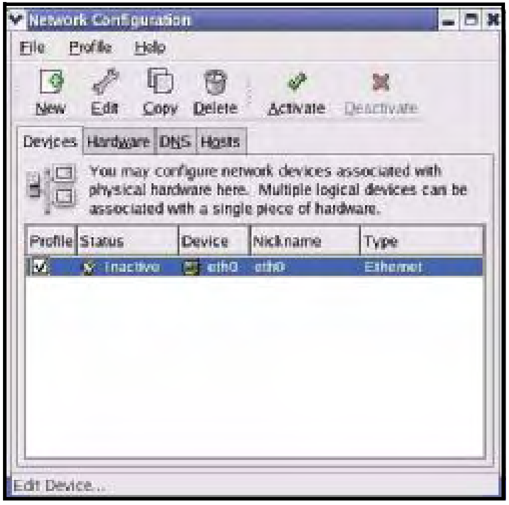
Make sure you are logged in as the root administrator.

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 236 Red Hat 9.0: KDE: Network Configuration: Devices

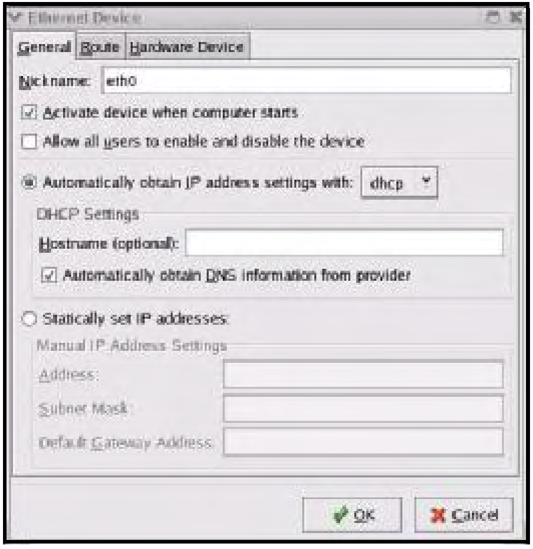


You may configure network devices associated with physical hardware here. Multiple logical devices can be associated with a single piece of hardware.

Profile	Status	Device	Nickname	Type
☑	Inactive	eth0	eth0	Ethernet

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

Figure 237 Red Hat 9.0: KDE: Ethernet Device: General



Nickname: eth0

☑ Activate device when computer starts

□ Allow all users to enable and disable the device

● Automatically obtain IP address settings with: dhcp

DHCP Settings

Hostname (optional):

☑ Automatically obtain DNS information from provider

○ Statically set IP addresses:

Manual IP Address Settings

Address:

Subnet Mask:

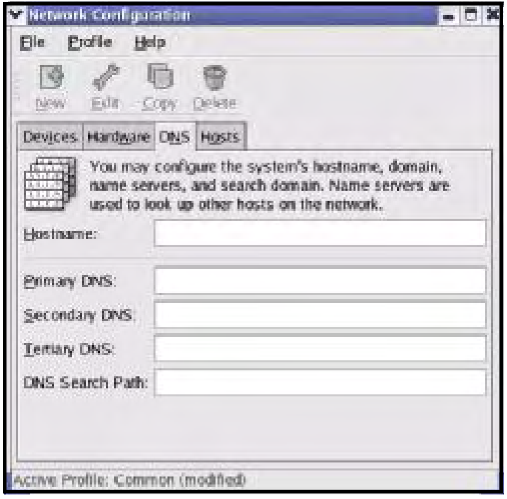
Default Gateway Address:

- 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 238 Red Hat 9.0: KDE: Network Configuration: DNS



You may configure the system's hostname, domain, name servers, and search domain. Name servers are used to look up other hosts on the network.

Hostname:

Primary DNS:

Secondary DNS:

Tertiary DNS:

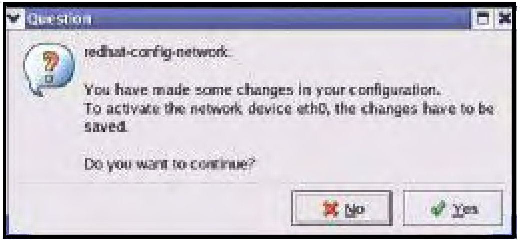
DNS Search Path:

Active Profile: Common (modified)

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 239 Red Hat 9.0: KDE: Network Configuration: Activate



redhat-config-network:

You have made some changes in your configuration.
To activate the network device eth0, the changes have to be saved.

Do you want to continue?

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 `ifconfig-eth0` 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 240 Red Hat 9.0: Dynamic IP Address Setting in ifconfig-eth0

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=dhcp
USERCTL=no
PEERDNS=yes
TYPE=Ethernet
```

- 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 241 Red Hat 9.0: Static IP Address Setting in ifconfig-eth0

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=static
IPADDR=192.168.1.10
NETMASK=255.255.255.0
USERCTL=no
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 242 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 243 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 244 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]#
```

C

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.

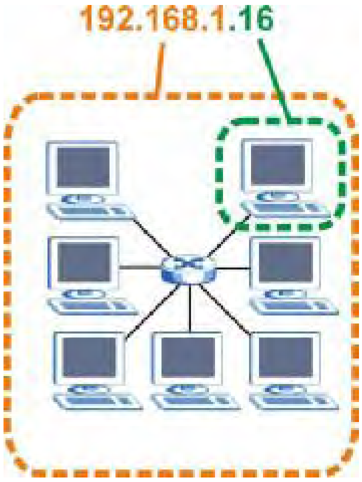
Structure

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.

Figure 245 Network Number and Host ID



How much of the IP address is the network number and how much is the host ID varies according to the subnet mask.

Subnet Masks

A subnet mask is used to determine which bits are part of the network number, and which bits are part of the host ID (using a logical AND operation). The term "subnet" is short for "sub-network".

A subnet mask has 32 bits. If a bit in the subnet mask is a "1" then the corresponding bit in the IP address is part of the network number. If a bit in the subnet mask is "0" then the corresponding bit in the IP address is part of the host ID.

The following example shows a subnet mask identifying the network number (in bold text) and host ID of an IP address (192.168.1.2 in decimal).

Table 122 IP Address Network Number and Host ID Example

	1ST OCTET: (192)	2ND OCTET: (168)	3RD OCTET: (1)	4TH OCTET (2)
IP Address (Binary)	11000000	10101000	00000001	00000010
Subnet Mask (Binary)	**11111111**	**11111111**	**11111111**	00000000
Network Number	**11000000**	**10101000**	**00000001**	
Host ID				00000010

By convention, subnet masks always consist of a continuous sequence of ones beginning from the leftmost bit of the mask, followed by a continuous sequence of zeros, for a total number of 32 bits.

Subnet masks can be referred to by the size of the network number part (the bits with a "1" value). For example, an "8-bit mask" means that the first 8 bits of the mask are ones and the remaining 24 bits are zeroes.

Subnet masks are expressed in dotted decimal notation just like IP addresses. The following examples show the binary and decimal notation for 8-bit, 16-bit, 24-bit and 29-bit subnet masks.

Table 123 Subnet Masks

	BINARY				DECIMAL
	1ST OCTET	2ND OCTET	3RD OCTET	4TH OCTET	
8-bit mask	11111111	00000000	00000000	00000000	255.0.0.0
16-bit mask	11111111	11111111	00000000	00000000	255.255.0.0
24-bit mask	11111111	11111111	11111111	00000000	255.255.255.0
29-bit mask	11111111	11111111	11111111	11111000	255.255.255.248

Network Size

The size of the network number determines the maximum number of possible hosts you can have on your network. The larger the number of network number bits, the smaller the number of remaining host ID bits.

An IP address with host IDs of all zeros is the IP address of the network (192.168.1.0 with a 24-bit subnet mask, for example). An IP address with host IDs of all ones is the broadcast address for that network (192.168.1.255 with a 24-bit subnet mask, for example).

As these two IP addresses cannot be used for individual hosts, calculate the maximum number of possible hosts in a network as follows:

Table 124 Maximum Host Numbers

SUBNET MASK		HOST ID SIZE		MAXIMUM NUMBER OF HOSTS
8 bits	255.0.0.0	24 bits	$2^{24} – 2$	16777214
16 bits	255.255.0.0	16 bits	$2^{16} – 2$	65534
24 bits	255.255.255.0	8 bits	$2^{8} – 2$	254
29 bits	255.255.255.248	3 bits	$2^{3} – 2$	6

Notation

Since the mask is always a continuous number of ones beginning from the left, followed by a continuous number of zeros for the remainder of the 32 bit mask, you can simply specify the number of ones instead of writing the value of each octet. This is usually specified by writing a "/" followed by the number of bits in the mask after the address.

For example, 192.1.1.0 /25 is equivalent to saying 192.1.1.0 with subnet mask 255.255.255.128.

The following table shows some possible subnet masks using both notations.

Table 125 Alternative Subnet Mask Notation

SUBNET MASK	ALTERNATIVE NOTATION	LAST OCTET (BINARY)	LAST OCTET (DECIMAL)
255.255.255.0	/24	0000 0000	0
255.255.255.128	/25	1000 0000	128

Table 125 Alternative Subnet Mask Notation (continued)

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

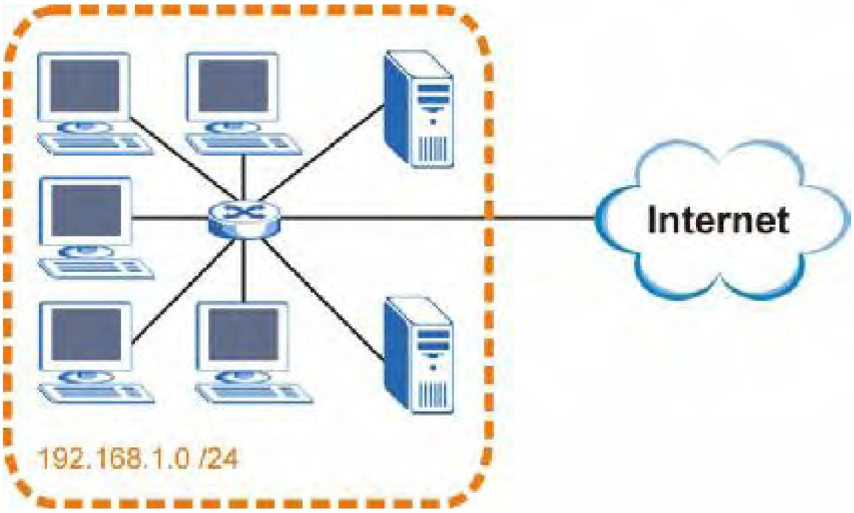
Subnetting

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 246 Subnetting Example: Before Subnetting

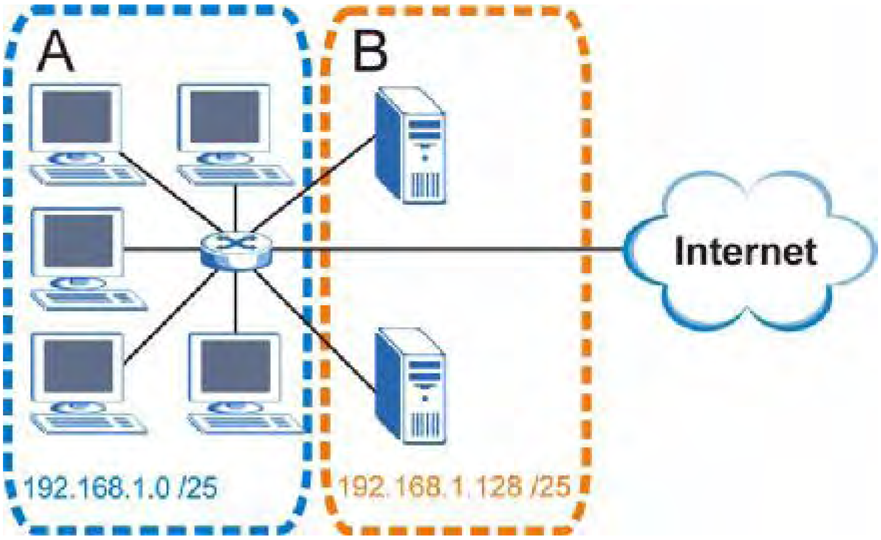


You can "borrow" one of the host ID bits to divide the network 192.168.1.0 into two separate sub-networks. The subnet mask is now 25 bits (255.255.255.128 or /25).

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

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

Figure 247 Subnetting Example: After Subnetting



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

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

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

Example: Four Subnets

The previous example illustrated using a 25-bit subnet mask to divide a 24-bit address into two subnets. Similarly, to divide a 24-bit address into four subnets, you need to “borrow” two host ID bits to give four possible combinations (00, 01, 10 and 11). The subnet mask is 26 bits (11111111.11111111.11111111.**11**000000) or 255.255.255.192.

Each subnet contains 6 host ID bits, giving 2^6 - 2 or 62 hosts for each subnet (a host ID of all zeroes is the subnet itself, all ones is the subnet's broadcast address).

Table 126 Subnet 1

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address (Decimal)	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	**00**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.0	Lowest Host ID: 192.168.1.1	
Broadcast Address: 192.168.1.63	Highest Host ID: 192.168.1.62	

Table 127 Subnet 2

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	64
IP Address (Binary)	11000000.10101000.00000001.	**01**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.64	Lowest Host ID: 192.168.1.65	
Broadcast Address: 192.168.1.127	Highest Host ID: 192.168.1.126	

Table 128 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 129 Subnet 4

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	192
IP Address (Binary)	11000000.10101000.00000001.	**11**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.192	Lowest Host ID: 192.168.1.193	
Broadcast Address: 192.168.1.255	Highest Host ID: 192.168.1.254	

Example: Eight Subnets

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

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

Table 130 Eight Subnets

SUBNET	SUBNET ADDRESS	FIRST ADDRESS	LAST ADDRESS	BROADCAST ADDRESS
1	0	1	30	31
2	32	33	62	63
3	64	65	94	95
4	96	97	126	127

Table 130 Eight Subnets (continued)

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

Subnet Planning

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

Table 131 24-bit Network Number Subnet Planning

NO. “BORROWED” HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.255.128 (/25)	2	126
2	255.255.255.192 (/26)	4	62
3	255.255.255.224 (/27)	8	30
4	255.255.255.240 (/28)	16	14
5	255.255.255.248 (/29)	32	6
6	255.255.255.252 (/30)	64	2
7	255.255.255.254 (/31)	128	1

The following table is a summary for subnet planning on a network with a 16-bit network number.

Table 132 16-bit Network Number Subnet Planning

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

Table 132 16-bit Network Number Subnet Planning (continued)

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

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.*

D

Common Services

The following table lists some commonly-used services and their associated protocols and port numbers. For a comprehensive list of port numbers, ICMP type/code numbers and services, visit the IANA (Internet Assigned Number Authority) web site.

- **Name**: This is a short, descriptive name for the service. You can use this one or create a different one, if you like.
- **Protocol**: This is the type of IP protocol used by the service. If this is **TCP/UDP**, then the service uses the same port number with TCP and UDP. If this is **USER-DEFINED**, the **Port(s)** is the IP protocol number, not the port number.
- **Port(s)**: This value depends on the **Protocol**. Please refer to RFC 1700 for further information about port numbers.
  - If the **Protocol** is **TCP**, **UDP**, or **TCP/UDP**, this is the IP port number.
  - If the **Protocol** is **USER**, this is the IP protocol number.
- **Description**: This is a brief explanation of the applications that use this service or the situations in which this service is used.

Table 133 Commonly Used Services

NAME	PROTOCOL	PORT(S)	DESCRIPTION
AH (IPSEC_TUNNEL)	User-Defined	51	The IPSEC AH (Authentication Header) tunneling protocol uses this service.
AIM/New-ICQ	TCP	5190	AOL's Internet Messenger service. It is also used as a listening port by ICQ.
AUTH	TCP	113	Authentication protocol used by some servers.
BGP	TCP	179	Border Gateway Protocol.
BOOTP_CLIENT	UDP	68	DHCP Client.
BOOTP_SERVER	UDP	67	DHCP Server.
CU-SEEME	TCP UDP	7648 24032	A popular videoconferencing solution from White Pines Software.
DNS	TCP/UDP	53	Domain Name Server, a service that matches web names (e.g. www.zyxel.com) to IP numbers.
ESP (IPSEC_TUNNEL)	User-Defined	50	The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service.
FINGER	TCP	79	Finger is a UNIX or Internet related command that can be used to find out if a user is logged on.

Table 133 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
FTP	TCP TCP	20 21	File Transfer Program, a program to enable fast transfer of files, including large files that may not be possible by e-mail.
H.323	TCP	1720	NetMeeting uses this protocol.
HTTP	TCP	80	Hyper Text Transfer Protocol - a client/ server protocol for the world wide web.
HTTPS	TCP	443	HTTPS is a secured http session often used in e-commerce.
ICMP	User-Defined	1	Internet Control Message Protocol is often used for diagnostic or routing purposes.
ICQ	UDP	4000	This is a popular Internet chat program.
IGMP (MULTICAST)	User-Defined	2	Internet Group Management Protocol is used when sending packets to a specific group of hosts.
IKE	UDP	500	The Internet Key Exchange algorithm is used for key distribution and management.
IRC	TCP/UDP	6667	This is another popular Internet chat program.
MSN Messenger	TCP	1863	Microsoft Networks' messenger service uses this protocol.
NEW-ICQ	TCP	5190	An Internet chat program.
NEWS	TCP	144	A protocol for news groups.
NFS	UDP	2049	Network File System - NFS is a client/ server distributed file service that provides transparent file sharing for network environments.
NNTP	TCP	119	Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service.
PING	User-Defined	1	Packet INternet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable.
POP3	TCP	110	Post Office Protocol version 3 lets a client computer get e-mail from a POP3 server through a temporary connection (TCP/IP or other).
PPTP	TCP	1723	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel.
PPTP_TUNNEL (GRE)	User-Defined	47	PPTP (Point-to-Point Tunneling Protocol) enables secure transfer of data over public networks. This is the data channel.
RCMD	TCP	512	Remote Command Service.
REAL_AUDIO	TCP	7070	A streaming audio service that enables real time sound over the web.
REXEC	TCP	514	Remote Execution Daemon.
RLOGIN	TCP	513	Remote Login.

Table 133 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
RTELNET	TCP	107	Remote Telnet.
RTSP	TCP/UDP	554	The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.
SFTP	TCP	115	Simple File Transfer Protocol.
SMTP	TCP	25	Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another.
SNMP	TCP/UDP	161	Simple Network Management Program.
SNMP-TRAPS	TCP/UDP	162	Traps for use with the SNMP (RFC:1215).
SQL-NET	TCP	1521	Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers.
SSH	TCP/UDP	22	Secure Shell Remote Login Program.
STRM WORKS	UDP	1558	Stream Works Protocol.
SYSLOG	UDP	514	Syslog allows you to send system logs to a UNIX server.
TACACS	UDP	49	Login Host Protocol used for (Terminal Access Controller Access Control System).
TELNET	TCP	23	Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems.
TFTP	UDP	69	Trivial File Transfer Protocol is an Internet file transfer protocol similar to FTP, but uses the UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol).
VDOLIVE	TCP	7000	Another videoconferencing solution.

E

Wireless LANs

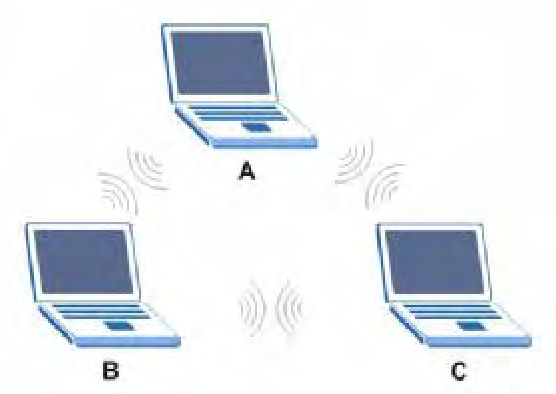
Wireless LAN Topologies

This section discusses ad-hoc and infrastructure wireless LAN topologies.

Ad-hoc Wireless LAN Configuration

The simplest WLAN configuration is an independent (Ad-hoc) WLAN that connects a set of computers with wireless adapters (A, B, C). Any time two or more wireless adapters are within range of each other, they can set up an independent network, which is commonly referred to as an ad-hoc network or Independent Basic Service Set (IBSS). The following diagram shows an example of notebook computers using wireless adapters to form an ad-hoc wireless LAN.

Figure 248 Peer-to-Peer Communication in an Ad-hoc Network

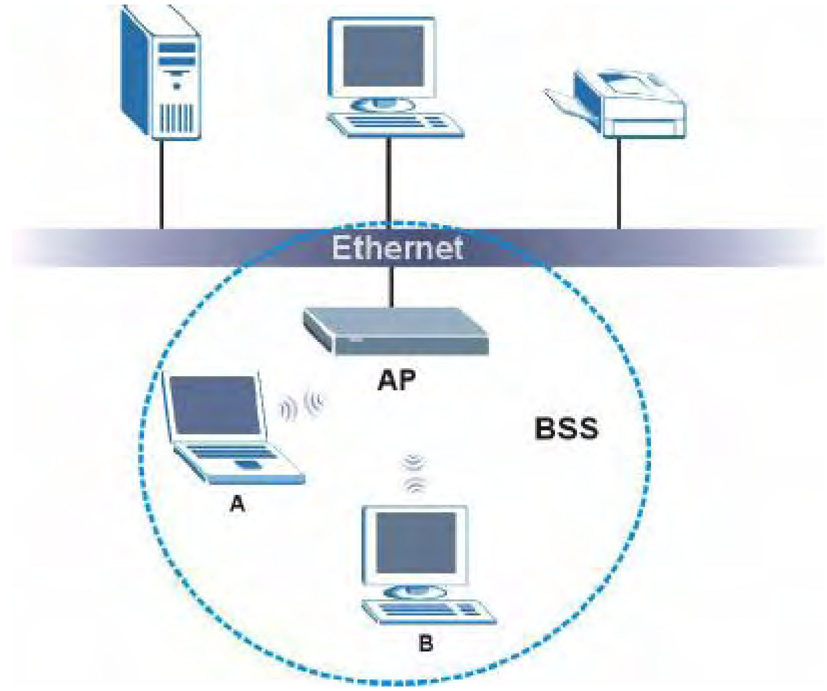


BSS

A Basic Service Set (BSS) exists when all communications between wireless clients or between a wireless client and a wired network client go through one access point (AP).

Intra-BSS traffic is traffic between wireless clients in the BSS. When Intra-BSS is enabled, wireless client **A** and **B** can access the wired network and communicate with each other. When Intra-BSS is disabled, wireless client **A** and **B** can still access the wired network but cannot communicate with each other.

Figure 249 Basic Service Set



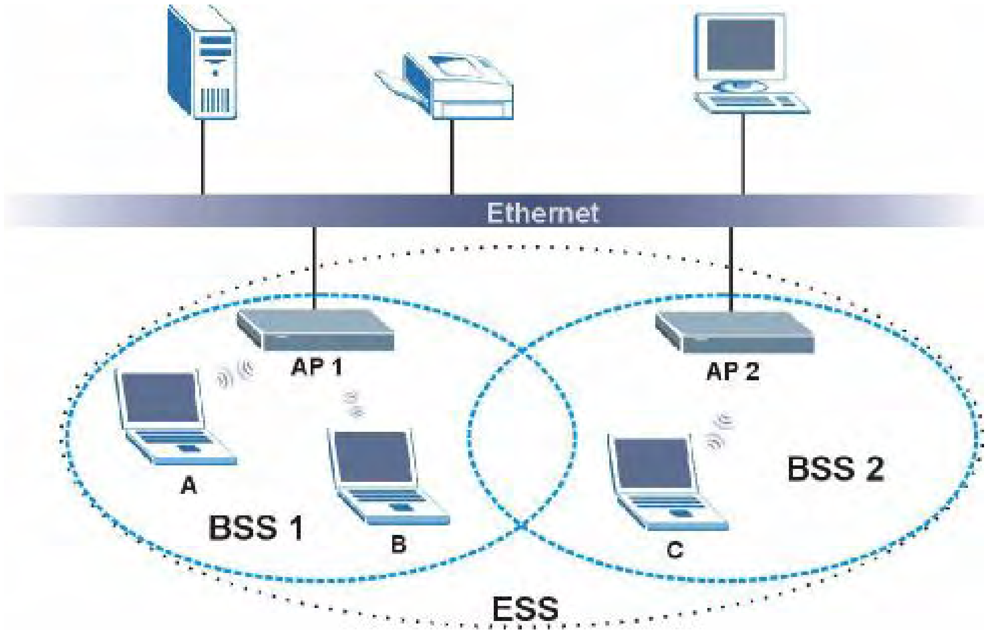
ESS

An Extended Service Set (ESS) consists of a series of overlapping BSSs, each containing an access point, with each access point connected together by a wired network. This wired connection between APs is called a Distribution System (DS).

This type of wireless LAN topology is called an Infrastructure WLAN. The Access Points not only provide communication with the wired network but also mediate wireless network traffic in the immediate neighborhood.

An ESSID (ESS IDentification) uniquely identifies each ESS. All access points and their associated wireless clients within the same ESS must have the same ESSID in order to communicate.

Figure 250 Infrastructure WLAN



Channel

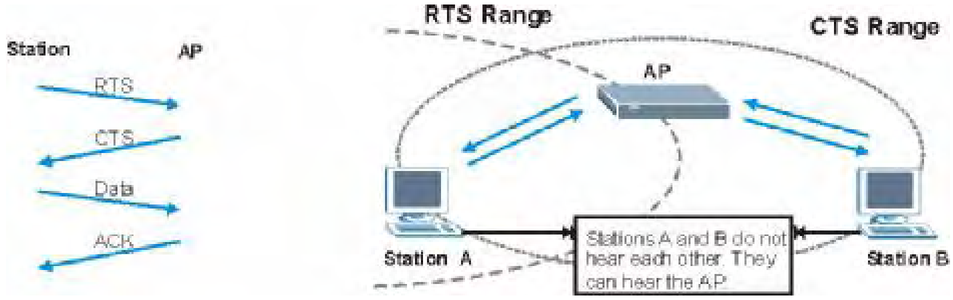
A channel is the radio frequency(ies) used by wireless devices to transmit and receive data. Channels available depend on your geographical area. You may have a choice of channels (for your region) so you should use a channel different from an adjacent AP (access point) to reduce interference. Interference occurs when radio signals from different access points overlap causing interference and degrading performance.

Adjacent channels partially overlap however. To avoid interference due to overlap, your AP should be on a channel at least five channels away from a channel that an adjacent AP is using. For example, if your region has 11 channels and an adjacent AP is using channel 1, then you need to select a channel between 6 or 11.

RTS/CTS

A hidden node occurs when two stations are within range of the same access point, but are not within range of each other. The following figure illustrates a hidden node. Both stations (STA) are within range of the access point (AP) or wireless gateway, but out-of-range of each other, so they cannot "hear" each other, that is they do not know if the channel is currently being used. Therefore, they are considered hidden from each other.

Figure 251 RTS/CTS


Station
AP
RTS
CTS
Data
ACK
RTS Range
CTS Range
AP
Station A
Stations A and B do not hear each other. They can hear the AP
Station B

When station **A** sends data to the AP, it might not know that the station **B** is already using the channel. If these two stations send data at the same time, collisions may occur when both sets of data arrive at the AP at the same time, resulting in a loss of messages for both stations.

RTS/CTS is designed to prevent collisions due to hidden nodes. An **RTS/CTS** defines the biggest size data frame you can send before an RTS (Request To Send)/CTS (Clear to Send) handshake is invoked.

When a data frame exceeds the **RTS/CTS** value you set (between 0 to 2432 bytes), the station that wants to transmit this frame must first send an RTS (Request To Send) message to the AP for permission to send it. The AP then responds with a CTS (Clear to Send) message to all other stations within its range to notify them to defer their transmission. It also reserves and confirms with the requesting station the time frame for the requested transmission.

Stations can send frames smaller than the specified **RTS/CTS** directly to the AP without the RTS (Request To Send)/CTS (Clear to Send) handshake.

You should only configure **RTS/CTS** if the possibility of hidden nodes exists on your network and the "cost" of resending large frames is more than the extra network overhead involved in the RTS (Request To Send)/CTS (Clear to Send) handshake.

If the **RTS/CTS** value is greater than the **Fragmentation Threshold** value (see next), then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS/CTS** size.

Enabling the RTS Threshold causes redundant network overhead that could negatively affect the throughput performance instead of providing a remedy.

Fragmentation Threshold

A **Fragmentation Threshold** is the maximum data fragment size (between 256 and 2432 bytes) that can be sent in the wireless network before the AP will fragment the packet into smaller data frames.

A large **Fragmentation Threshold** is recommended for networks not prone to interference while you should set a smaller threshold for busy networks or networks that are prone to interference.

If the **Fragmentation Threshold** value is smaller than the **RTS/CTS** value (see previously) you set then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS/CTS** size.

Preamble Type

Preamble is used to signal that data is coming to the receiver. Short and long refer to the length of the synchronization field in a packet.

Short preamble increases performance as less time sending preamble means more time for sending data. All IEEE 802.11 compliant wireless adapters support long preamble, but not all support short preamble.

Use long preamble if you are unsure what preamble mode other wireless devices on the network support, and to provide more reliable communications in busy wireless networks.

Use short preamble if you are sure all wireless devices on the network support it, and to provide more efficient communications.

Use the dynamic setting to automatically use short preamble when all wireless devices on the network support it, otherwise the ZyXEL Device uses long preamble.

The wireless devices MUST use the same preamble mode in order to communicate.

IEEE 802.11g Wireless LAN

IEEE 802.11g is fully compatible with the IEEE 802.11b standard. This means an IEEE 802.11b adapter can interface directly with an IEEE 802.11g access point (and vice versa) at 11 Mbps or lower depending on range. IEEE 802.11g has several intermediate rate steps between the maximum and minimum data rates. The IEEE 802.11g data rate and modulation are as follows:

Table 134 IEEE 802.11g

DATA RATE (MBPS)	MODULATION
1	DBPSK (Differential Binary Phase Shift Keyed)
2	DQPSK (Differential Quadrature Phase Shift Keying)
5.5 / 11	CCK (Complementary Code Keying)
6/9/12/18/24/36/48/54	OFDM (Orthogonal Frequency Division Multiplexing)

Wireless Security Overview

Wireless security is vital to your network to protect wireless communication between wireless clients, access points and the wired network.

Wireless security methods available on the ZyXEL Device are data encryption, wireless client authentication, restricting access by device MAC address and hiding the ZyXEL Device identity.

The following figure shows the relative effectiveness of these wireless security methods available on your ZyXEL Device.

Table 135 Wireless Security Levels

SECURITY LEVEL	SECURITY TYPE
Least Secure	Unique SSID (Default)
	Unique SSID with Hide SSID Enabled
	MAC Address Filtering
	WEP Encryption
	IEEE802.1x EAP with RADIUS Server Authentication
	Wi-Fi Protected Access (WPA)
Most Secure	WPA2

You must enable the same wireless security settings on the ZyXEL Device and on all wireless clients that you want to associate with it.

IEEE 802.1x

In June 2001, the IEEE 802.1x standard was designed to extend the features of IEEE 802.11 to support extended authentication as well as providing additional accounting and control features. It is supported by Windows XP and a number of network devices. Some advantages of IEEE 802.1x are:

- User based identification that allows for roaming.
- Support for RADIUS (Remote Authentication Dial In User Service, RFC 2138, 2139) for centralized user profile and accounting management on a network RADIUS server.
- Support for EAP (Extensible Authentication Protocol, RFC 2486) that allows additional authentication methods to be deployed with no changes to the access point or the wireless clients.

RADIUS

RADIUS is based on a client-server model that supports authentication, authorization and accounting. The access point 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 AP acts as a message relay between the wireless client and the network RADIUS server.

Types of RADIUS Messages

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user authentication:

- Access-Request

  Sent by an access point 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 access point sends a proper response from the user and then sends another Access-Request message.

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user accounting:

- Accounting-Request

  Sent by the access point 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.

Types of EAP Authentication

This section discusses some popular authentication types: EAP-MD5, EAP-TLS, EAP-TTLS, PEAP and LEAP. Your wireless LAN device may not support all authentication types.

EAP (Extensible Authentication Protocol) is an authentication protocol that runs on top of the IEEE 802.1x transport mechanism in order to support multiple types of user authentication. By using EAP to interact with an EAP-compatible RADIUS server, an access point helps a wireless station and a RADIUS server perform authentication.

The type of authentication you use depends on the RADIUS server and an intermediary AP(s) that supports IEEE 802.1x. .

For EAP-TLS authentication type, you must first have a wired connection to the network and obtain the certificate(s) from a certificate authority (CA). A certificate (also called digital IDs) can be used to authenticate users and a CA issues certificates and guarantees the identity of each certificate owner.

EAP-MD5 (Message-Digest Algorithm 5)

MD5 authentication is the simplest one-way authentication method. The authentication server sends a challenge to the wireless client. The wireless client 'proves' that it knows the password by encrypting the password with the challenge and sends back the information. Password is not sent in plain text.

However, MD5 authentication has some weaknesses. Since the authentication server needs to get the plaintext passwords, the passwords must be stored. Thus someone other than the authentication server may access the password file. In addition, it is possible to impersonate an authentication server as MD5 authentication method does not perform mutual authentication. Finally, MD5 authentication method does not support data encryption with dynamic session key. You must configure WEP encryption keys for data encryption.

EAP-TLS (Transport Layer Security)

With EAP-TLS, digital certifications are needed by both the server and the wireless clients for mutual authentication. The server presents a certificate to the client. After validating the identity of the server, the client sends a different certificate to the server. The exchange of certificates is done in the open before a secured tunnel is created. This makes user identity vulnerable to passive attacks. A digital certificate is an electronic ID card that authenticates the sender's identity. However, to implement EAP-TLS, you need a Certificate Authority (CA) to handle certificates, which imposes a management overhead.

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. 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.

PEAP (Protected EAP)

Like EAP-TTLS, server-side certificate authentication is used to establish a secure connection, then use simple username and password methods through the secured connection to authenticate the clients, thus hiding client identity. However, PEAP only supports EAP methods, such as EAP-MD5, EAP-MSCHAPv2 and EAP-GTC (EAP-Generic Token Card), for client authentication. EAP-GTC is implemented only by Cisco.

LEAP

LEAP (Lightweight Extensible Authentication Protocol) is a Cisco implementation of IEEE 802.1x.

Dynamic WEP Key Exchange

The AP maps a unique key that is generated with the RADIUS server. This key expires when the wireless connection times out, disconnects or reauthentication times out. A new WEP key is generated each time reauthentication is performed.

If this feature is enabled, it is not necessary to configure a default encryption key in the wireless security configuration screen. You may still configure and store keys, but they will not be used while dynamic WEP is enabled.

EAP-MD5 cannot be used with Dynamic WEP Key Exchange

For added security, certificate-based authentications (EAP-TLS, EAP-TTLS and PEAP) use dynamic keys for data encryption. They are often deployed in corporate environments, but for public deployment, a simple user name and password pair is more practical. The following table is a comparison of the features of authentication types.

Table 136 Comparison of EAP Authentication Types

	EAP-MD5	EAP-TLS	EAP-TTLS	PEAP	LEAP
Mutual Authentication	No	Yes	Yes	Yes	Yes
Certificate – Client	No	Yes	Optional	Optional	No
Certificate – Server	No	Yes	Yes	Yes	No
Dynamic Key Exchange	No	Yes	Yes	Yes	Yes
Credential Integrity	None	Strong	Strong	Strong	Moderate
Deployment Difficulty	Easy	Hard	Moderate	Moderate	Moderate
Client Identity Protection	No	No	Yes	Yes	No

WPA and WPA2

Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i standard. WPA2 (IEEE 802.11i) is a wireless security standard that defines stronger encryption, authentication and key management than WPA.

Key differences between WPA or WPA2 and WEP are improved data encryption and user authentication.

If both an AP and the wireless clients support WPA2 and you have an external RADIUS server, use WPA2 for stronger data encryption. If you don't have an external RADIUS server, you should use WPA2-PSK (WPA2-Pre-Shared Key) that only requires a single (identical) password entered into each access point, wireless gateway and wireless client. As long as the passwords match, a wireless client will be granted access to a WLAN.

If the AP or the wireless clients do not support WPA2, just use WPA or WPA-PSK depending on whether you have an external RADIUS server or not.

Select WEP only when the AP and/or wireless clients do not support WPA or WPA2. WEP is less secure than WPA or WPA2.

Encryption

Both WPA and WPA2 improve data encryption by using Temporal Key Integrity Protocol (TKIP), Message Integrity Check (MIC) and IEEE 802.1x. WPA and WPA2 use Advanced Encryption Standard (AES) in the Counter mode with Cipher block chaining Message authentication code Protocol (CCMP) to offer stronger encryption than TKIP.

TKIP uses 128-bit keys that are dynamically generated and distributed by the authentication server. AES (Advanced Encryption Standard) is a block cipher that uses a 256-bit mathematical algorithm called Rijndael. They both include a per-packet key mixing function, a Message Integrity Check (MIC) named Michael, an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism.

WPA and WPA2 regularly change and rotate the encryption keys so that the same encryption key is never used twice.

The RADIUS server distributes a Pairwise Master Key (PMK) key to the AP that then sets up a key hierarchy and management system, using the PMK to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients. This all happens in the background automatically.

The Message Integrity Check (MIC) is designed to prevent an attacker from capturing data packets, altering them and resending them. The MIC provides a strong mathematical function in which the receiver and the transmitter each compute and then compare the MIC. If they do not match, it is assumed that the data has been tampered with and the packet is dropped.

By generating unique data encryption keys for every data packet and by creating an integrity checking mechanism (MIC), with TKIP and AES it is more difficult to decrypt data on a Wi-Fi network than WEP and difficult for an intruder to break into the network.

The encryption mechanisms used for WPA(2) and WPA(2)-PSK are the same. The only difference between the two is that WPA(2)-PSK uses a simple common password, instead of user-specific credentials. The common-password approach makes WPA(2)-PSK susceptible to brute-force password-guessing attacks but it’s still an improvement over WEP as it employs a consistent, single, alphanumeric password to derive a PMK which is used to generate unique temporal encryption keys. This prevent all wireless devices sharing the same encryption keys. (a weakness of WEP)

User Authentication

WPA and WPA2 apply IEEE 802.1x and Extensible Authentication Protocol (EAP) to authenticate wireless clients using an external RADIUS database. WPA2 reduces the number of key exchange messages from six to four (CCMP 4-way handshake) and shortens the time required to connect to a network. Other WPA2 authentication features that are different from WPA include key caching and pre-authentication. These two features are optional and may not be supported in all wireless devices.

Key caching allows a wireless client to store the PMK it derived through a successful authentication with an AP. The wireless client uses the PMK when it tries to connect to the same AP and does not need to go with the authentication process again.

Pre-authentication enables fast roaming by allowing the wireless client (already connecting to an AP) to perform IEEE 802.1x authentication with another AP before connecting to it.

Wireless Client WPA Supplicants

A wireless client supplicant is the software that runs on an operating system instructing the wireless client how to use WPA. At the time of writing, the most widely available supplicant is the WPA patch for Windows XP, Funk Software's Odyssey client.

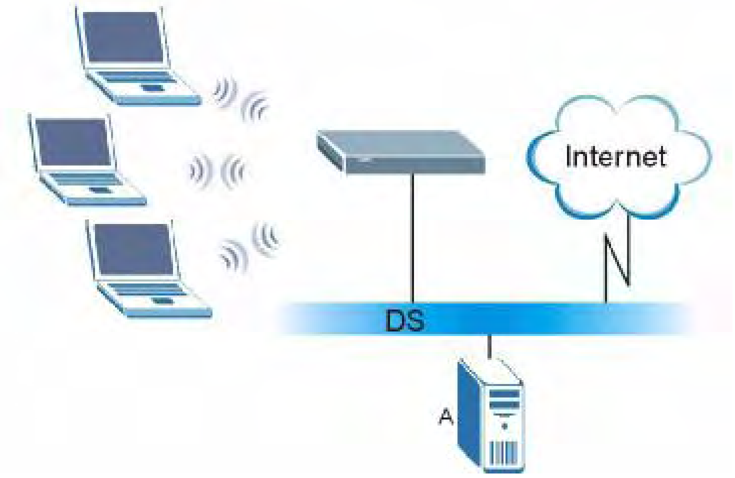
The Windows XP patch is a free download that adds WPA capability to Windows XP's built-in "Zero Configuration" wireless client. However, you must run Windows XP to use it.

WPA(2) with RADIUS Application Example

To set up WPA(2), you need the IP address of the RADIUS server, its port number (default is 1812), and the RADIUS shared secret. A WPA(2) application example with an external RADIUS server looks as follows. "A" is the RADIUS server. "DS" is the distribution system.

1 The AP passes the wireless client's authentication request to the RADIUS server.
2 The RADIUS server then checks the user's identification against its database and grants or denies network access accordingly.
3 A 256-bit Pairwise Master Key (PMK) is derived from the authentication process by the RADIUS server and the client.
4 The RADIUS server distributes the PMK to the AP. The AP then sets up a key hierarchy and management system, using the PMK to dynamically generate unique data encryption keys. The keys are used to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients.

Figure 252 WPA(2) with RADIUS Application Example



WPA(2)-PSK Application Example

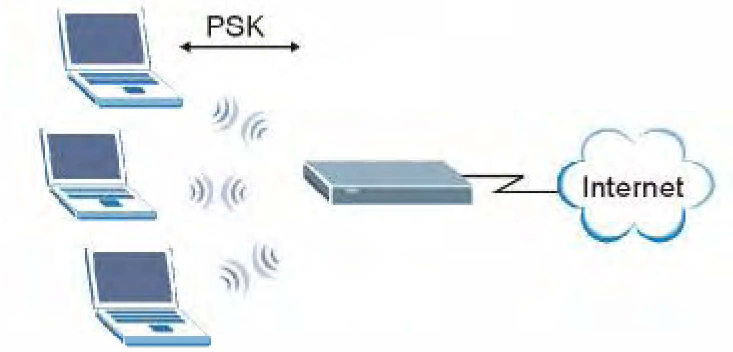
A WPA(2)-PSK application looks as follows.

1 First enter identical passwords into the AP and all wireless clients. The Pre-Shared Key (PSK) must consist of between 8 and 63 ASCII characters or 64 hexadecimal characters (including spaces and symbols).
2 The AP checks each wireless client's password and allows it to join the network only if the password matches.

3 The AP and wireless clients generate a common PMK (Pairwise Master Key). The key itself is not sent over the network, but is derived from the PSK and the SSID.

4 The AP and wireless clients use the TKIP or AES encryption process, the PMK and information exchanged in a handshake to create temporal encryption keys. They use these keys to encrypt data exchanged between them.

Figure 253 WPA(2)-PSK Authentication



Security Parameters Summary

Refer to this table to see what other security parameters you should configure for each authentication method or key management protocol type. MAC address filters are not dependent on how you configure these security features.

Table 137 Wireless Security Relational Matrix

AUTHENTICATION METHOD/ KEY MANAGEMENT PROTOCOL	ENCRYPTIO N METHOD	ENTER MANUAL KEY	IEEE 802.1X
Open	None	No	Disable
			Enable without Dynamic WEP Key
Open	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable
Shared	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable
WPA	TKIP/AES	No	Enable
WPA-PSK	TKIP/AES	Yes	Disable
WPA2	TKIP/AES	No	Enable
WPA2-PSK	TKIP/AES	Yes	Disable

Antenna Overview

An antenna couples RF signals onto air. A transmitter within a wireless device sends an RF signal to the antenna, which propagates the signal through the air. The antenna also operates in reverse by capturing RF signals from the air.

Positioning the antennas properly increases the range and coverage area of a wireless LAN.

Antenna Characteristics

Frequency

An antenna in the frequency of 2.4GHz (IEEE 802.11b and IEEE 802.11g) or 5GHz (IEEE 802.11a) is needed to communicate efficiently in a wireless LAN

Radiation Pattern

A radiation pattern is a diagram that allows you to visualize the shape of the antenna's coverage area.

Antenna Gain

Antenna gain, measured in dB (decibel), is the increase in coverage within the RF beam width. Higher antenna gain improves the range of the signal for better communications.

For an indoor site, each 1 dB increase in antenna gain results in a range increase of approximately 2.5%. For an unobstructed outdoor site, each 1dB increase in gain results in a range increase of approximately 5%. Actual results may vary depending on the network environment.

Antenna gain is sometimes specified in dBi, which is how much the antenna increases the signal power compared to using an isotropic antenna. An isotropic antenna is a theoretical perfect antenna that sends out radio signals equally well in all directions. dBi represents the true gain that the antenna provides.

Types of Antennas for WLAN

There are two types of antennas used for wireless LAN applications.

- Omni-directional antennas send the RF signal out in all directions on a horizontal plane. The coverage area is torus-shaped (like a donut) which makes these antennas ideal for a room environment. With a wide coverage area, it is possible to make circular overlapping coverage areas with multiple access points.
- Directional antennas concentrate the RF signal in a beam, like a flashlight does with the light from its bulb. The angle of the beam determines the width of the coverage pattern. Angles typically range from 20 degrees (very directional) to 120 degrees (less directional). Directional antennas are ideal for hallways and outdoor point-to-point applications.

Positioning Antennas

In general, antennas should be mounted as high as practically possible and free of obstructions. In point-to–point application, position both antennas at the same height and in a direct line of sight to each other to attain the best performance.

For omni-directional antennas mounted on a table, desk, and so on, point the antenna up. For omni-directional antennas mounted on a wall or ceiling, point the antenna down. For a single AP application, place omni-directional antennas as close to the center of the coverage area as possible.

For directional antennas, point the antenna in the direction of the desired coverage area.

F

Importing Certificates

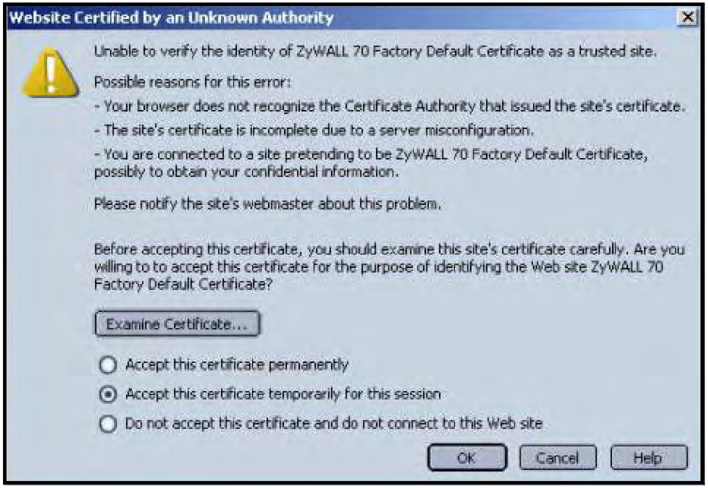
This appendix shows importing certificates examples using Internet Explorer 5.

Import ZyXEL Device Certificates into Netscape Navigator

In Netscape Navigator, you can permanently trust the ZyXEL Device's server certificate by importing it into your operating system as a trusted certification authority.

Select **Accept This Certificate Permanently** in the following screen to do this.

Figure 254 Security Certificate



Website Certified by an Unknown Authority

Unable to verify the identity of ZyWALL 70 Factory Default Certificate as a trusted site.

Possible reasons for this error:

- Your browser does not recognize the Certificate Authority that issued the site's certificate.
- The site's certificate is incomplete due to a server misconfiguration.
- You are connected to a site pretending to be ZyWALL 70 Factory Default Certificate, possibly to obtain your confidential information.

Please notify the site's webmaster about this problem.

Before accepting this certificate, you should examine this site's certificate carefully. Are you willing to to accept this certificate for the purpose of identifying the Web site ZyWALL 70 Factory Default Certificate?

Examine Certificate...

○ Accept this certificate permanently

● Accept this certificate temporarily for this session

○ Do not accept this certificate and do not connect to this Web site

OK | Cancel | Help

Importing the ZyXEL Device's Certificate into Internet Explorer

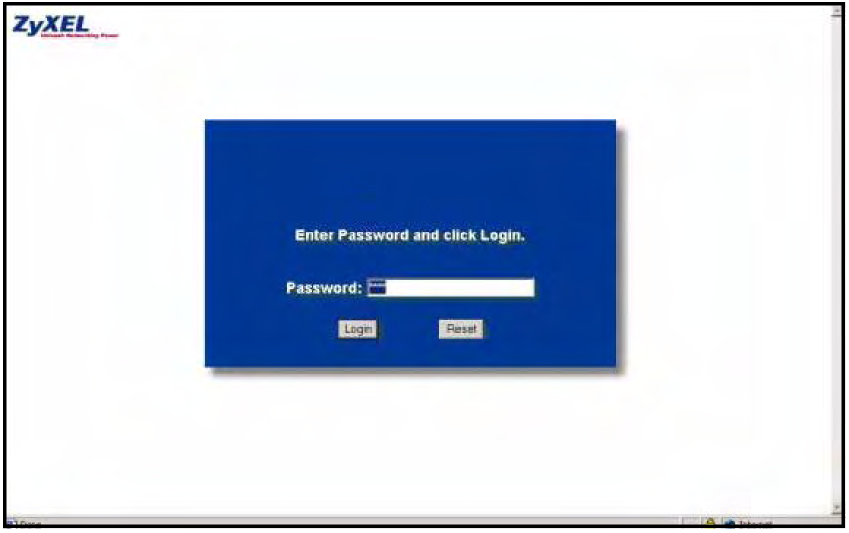
For Internet Explorer to trust a self-signed certificate from the ZyXEL Device, simply import the self-signed certificate into your operating system as a trusted certification authority.

To have Internet Explorer trust a ZyXEL Device certificate issued by a certificate authority, import the certificate authority's certificate into your operating system as a trusted certification authority.

The following example procedure shows how to import the ZyXEL Device's (self-signed) server certificate into your operating system as a trusted certification authority.

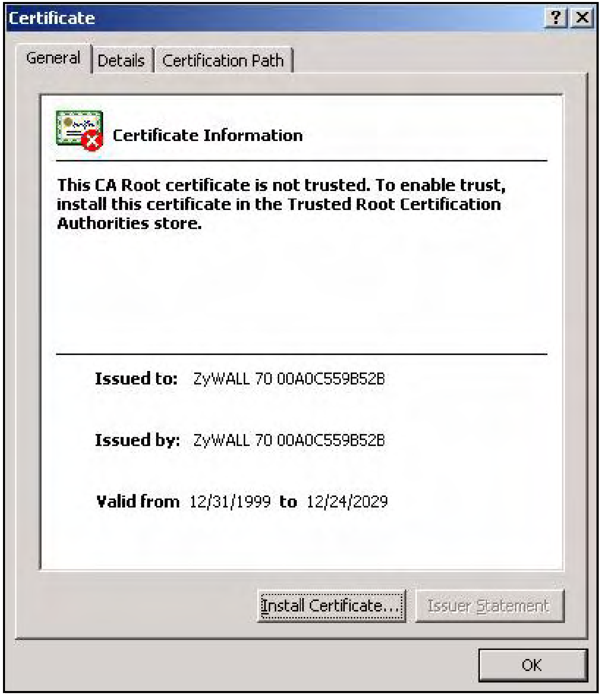
1 In Internet Explorer, double click the lock shown in the following screen.

Figure 255 Login Screen



2 Click **Install Certificate** to open the **Install Certificate** wizard.

Figure 256 Certificate General Information before Import



Certificate Information

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

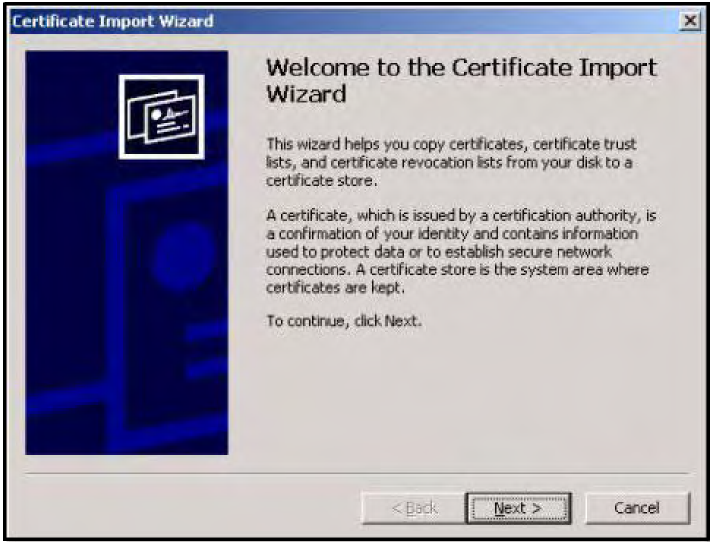
Issued to: ZyWALL 70 00A0C559B52B

Issued by: ZyWALL 70 00A0C559B52B

Valid from 12/31/1999 to 12/24/2029

3 Click **Next** to begin the **Install Certificate** wizard.

Figure 257 Certificate Import Wizard 1



Welcome to the Certificate Import Wizard

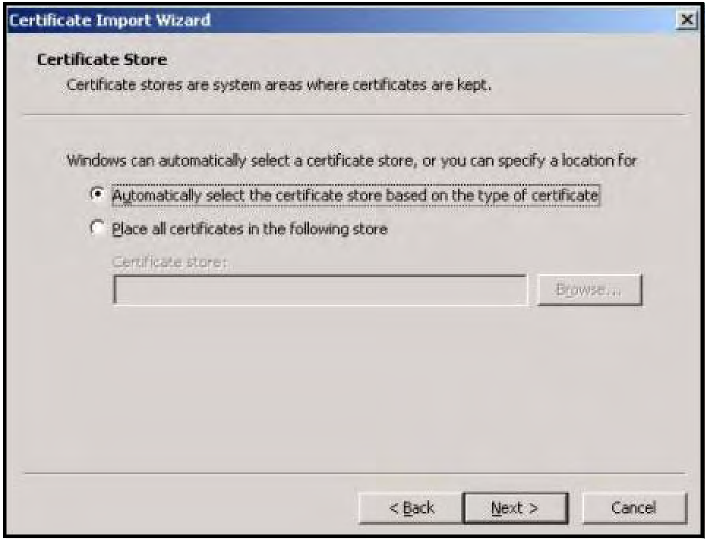
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

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

To continue, click Next.

4 Select where you would like to store the certificate and then click **Next**.

Figure 258 Certificate Import Wizard 2



Certificate Store

Certificate stores are system areas where certificates are kept.

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

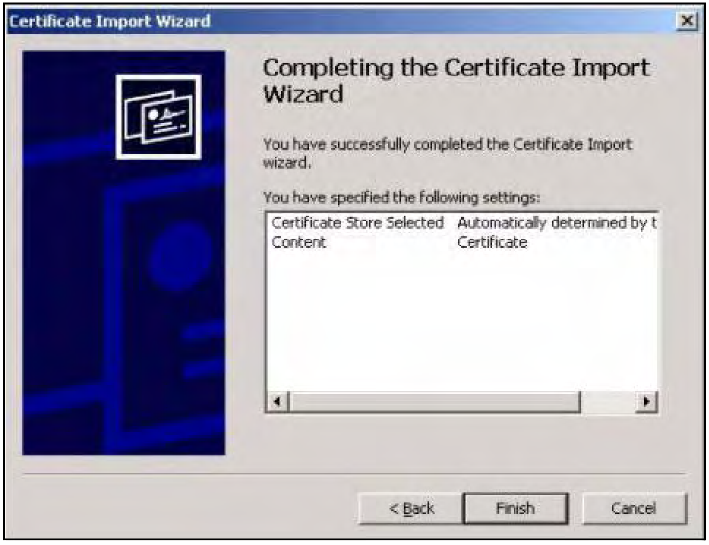
● Automatically select the certificate store based on the type of certificate

○ Place all certificates in the following store

Certificate store:

5 Click **Finish** to complete the **Import Certificate** wizard.

Figure 259 Certificate Import Wizard 3



Certificate Import Wizard

Completing the Certificate Import Wizard

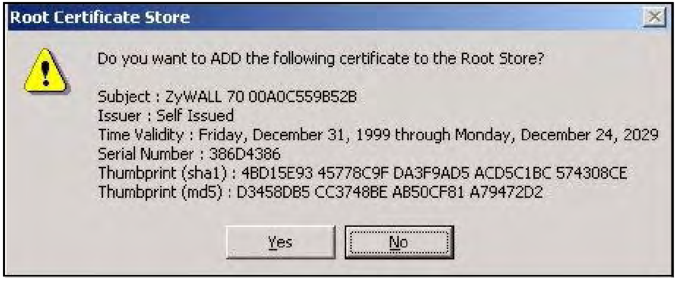
You have successfully completed the Certificate Import wizard.

You have specified the following settings:

Certificate Store Selected	Automatically determined by t
Content	Certificate

6 Click **Yes** to add the ZyXEL Device certificate to the root store.

Figure 260 Root Certificate Store

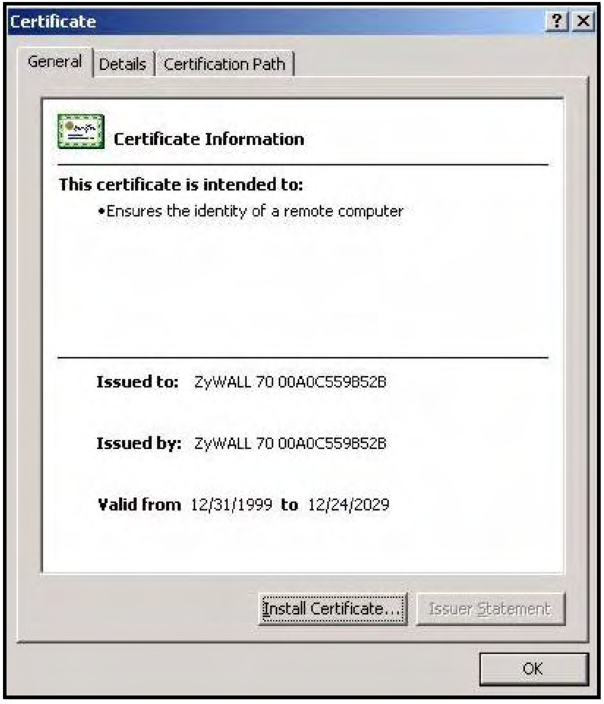


Root Certificate Store

Do you want to ADD the following certificate to the Root Store?

Subject : ZyWALL 70 00A0C559B52B
Issuer : Self Issued
Time Validity : Friday, December 31, 1999 through Monday, December 24, 2029
Serial Number : 386D4386
Thumbprint (sha1) : 4BD15E93 45778C9F DA3F9AD5 ACD5C1BC 574308CE
Thumbprint (md5) : D3458DB5 CC3748BE AB50CF81 A79472D2

Figure 261 Certificate General Information after Import



Certificate Information

This certificate is intended to:

- Ensures the identity of a remote computer

Issued to: ZyWALL 70 00A0C559B52B

Issued by: ZyWALL 70 00A0C559B52B

Valid from 12/31/1999 to 12/24/2029

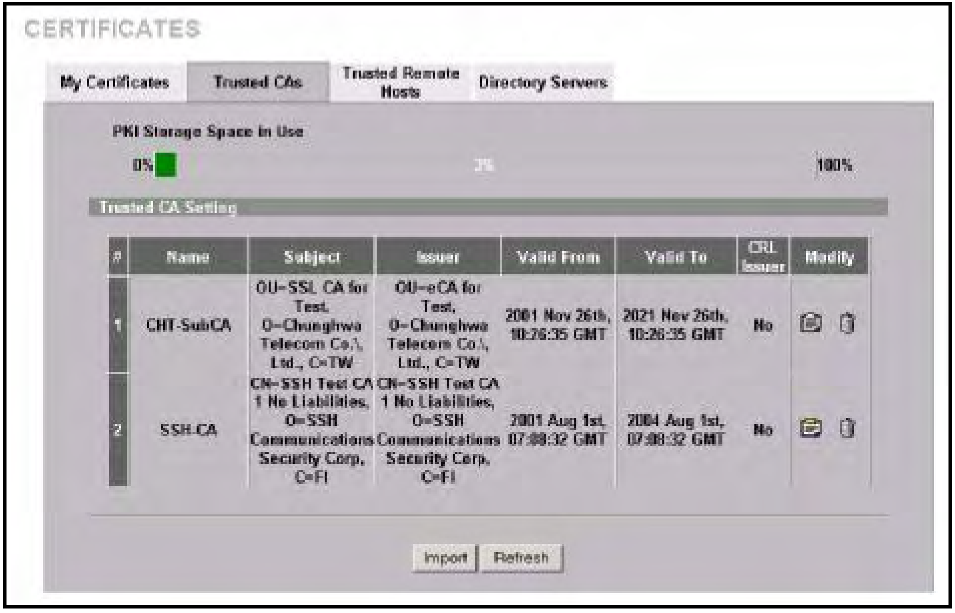
Enrolling and Importing SSL Client Certificates

The SSL client needs a certificate if **Authenticate Client Certificates** is selected on the ZyXEL Device.

You must have imported at least one trusted CA to the ZyXEL Device in order for the **Authenticate Client Certificates** to be active (see the Certificates chapter for details).

Apply for a certificate from a Certification Authority (CA) that is trusted by the ZyXEL Device (see the ZyXEL Device's **Trusted CA** web configurator screen).

Figure 262 ZyXEL Device Trusted CA Screen



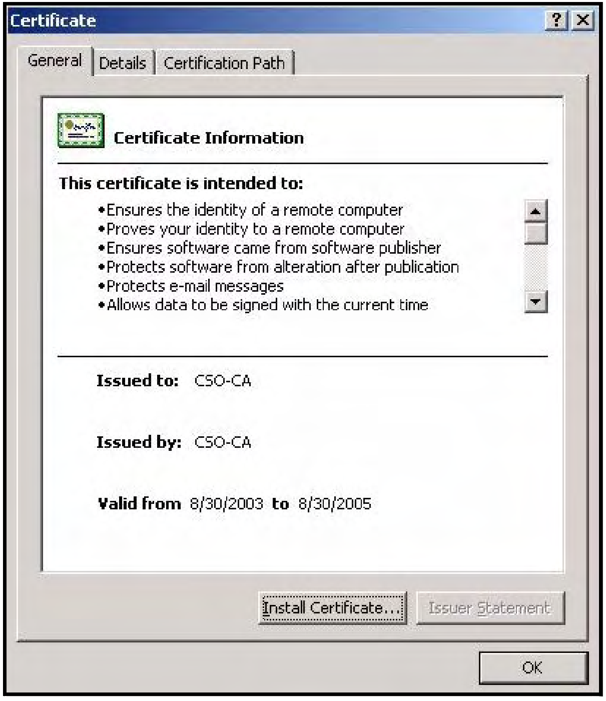
#	Name	Subject	Issuer	Valid From	Valid To	CRL Issuer	Modify
1	CHT-SubCA	OU=SSL CA for Test, O=Chunghwa Telecom Co.\, Ltd., C=TW	OU=eCA for Test, O=Chunghwa Telecom Co.\, Ltd., C=TW	2001 Nov 26th, 10:26:35 GMT	2021 Nov 26th, 10:26:35 GMT	No	
2	SSH-CA	CN=SSH Test CA 1 No Liabilities, O=SSH Communications Security Corp, C=FI	CN=SSH Test CA 1 No Liabilities, O=SSH Communications Security Corp, C=FI	2001 Aug 1st, 07:08:32 GMT	2004 Aug 1st, 07:08:32 GMT	No	

The CA sends you a package containing the CA's trusted certificate(s), your personal certificate(s) and a password to install the personal certificate(s).

Installing the CA's Certificate

1 Double click the CA's trusted certificate to produce a screen similar to the one shown next.

Figure 263 CA Certificate Example



Certificate

General | Details | Certification Path

Certificate Information

This certificate is intended to:

- Ensures the identity of a remote computer
- Proves your identity to a remote computer
- Ensures software came from software publisher
- Protects software from alteration after publication
- Protects e-mail messages
- Allows data to be signed with the current time

Issued to: CSO-CA

Issued by: CSO-CA

Valid from 8/30/2003 to 8/30/2005

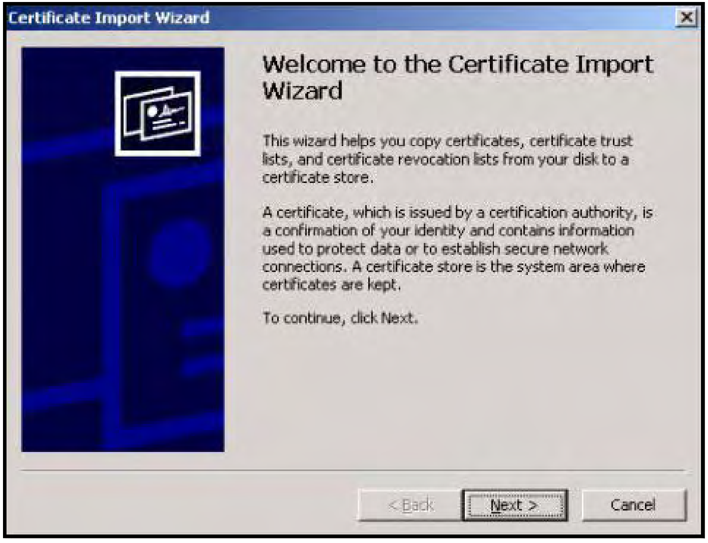
2 Click **Install Certificate** and follow the wizard as shown earlier in this appendix.

Installing Your Personal Certificate(s)

You need a password in advance. The CA may issue the password or you may have to specify it during the enrollment. Double-click the personal certificate given to you by the CA to produce a screen similar to the one shown next

1 Click **Next** to begin the wizard.

Figure 264 Personal Certificate Import Wizard 1



Certificate Import Wizard

Welcome to the Certificate Import Wizard

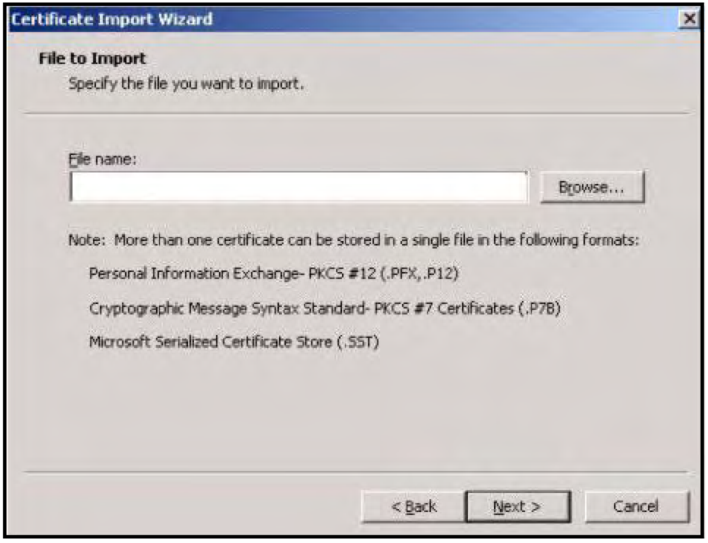
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

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

To continue, click Next.

2 The file name and path of the certificate you double-clicked should automatically appear in the **File name** text box. Click **Browse** if you wish to import a different certificate.

Figure 265 Personal Certificate Import Wizard 2



Certificate Import Wizard

File to Import

Specify the file you want to import.

File name:

Note: More than one certificate can be stored in a single file in the following formats:

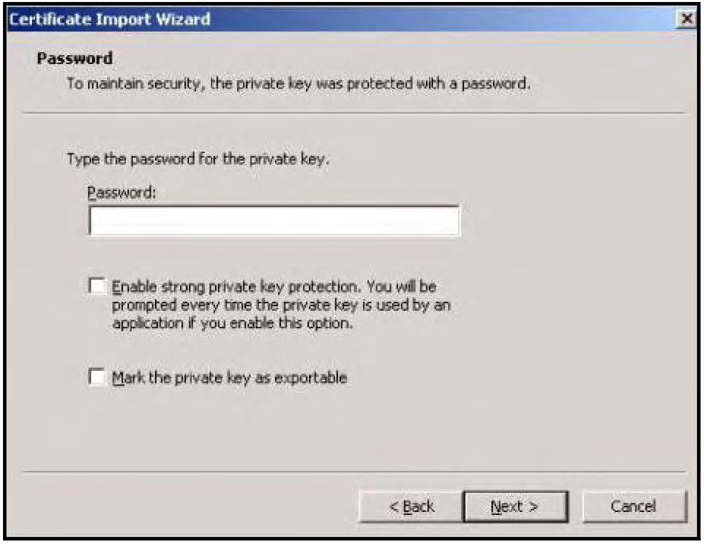
Personal Information Exchange- PKCS #12 (.PFX,.P12)

Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

3 Enter the password given to you by the CA.

Figure 266 Personal Certificate Import Wizard 3



Certificate Import Wizard

Password

To maintain security, the private key was protected with a password.

Type the password for the private key.

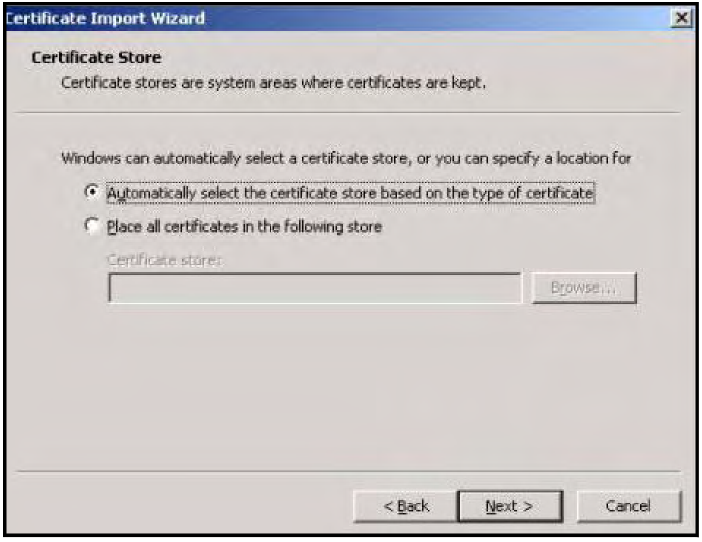
Password:

□ Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.

□ Mark the private key as exportable

4 Have the wizard determine where the certificate should be saved on your computer or select **Place all certificates in the following store** and choose a different location.

Figure 267 Personal Certificate Import Wizard 4



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

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

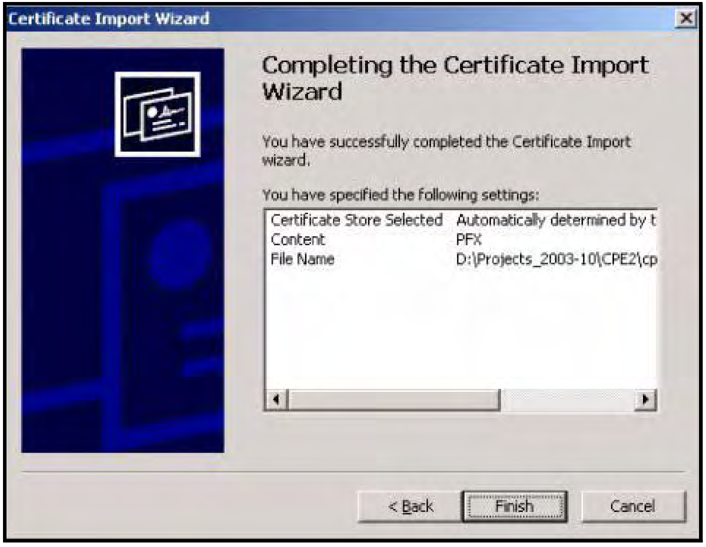
● Automatically select the certificate store based on the type of certificate

○ Place all certificates in the following store

Certificate store:

5 Click **Finish** to complete the wizard and begin the import process.

Figure 268 Personal Certificate Import Wizard 5



Certificate Import Wizard

Completing the Certificate Import Wizard

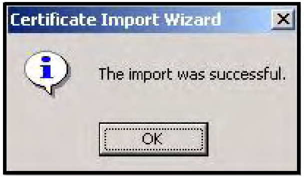
You have successfully completed the Certificate Import wizard.

You have specified the following settings:

Certificate Store Selected	Automatically determined by t
Content	PFX
File Name	D:\Projects_2003-10\CPE2\cp

6 You should see the following screen when the certificate is correctly installed on your computer.

Figure 269 Personal Certificate Import Wizard 6



Certificate Import Wizard

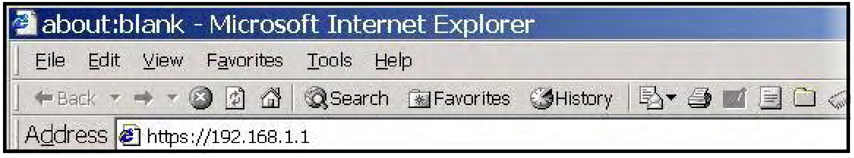
The import was successful.

Using a Certificate When Accessing the ZyXEL Device Example

Use the following procedure to access the ZyXEL Device via HTTPS.

1 Enter ‘https://ZyXEL Device IP Address/ in your browser’s web address field.

Figure 270 Access the ZyXEL Device Via HTTPS



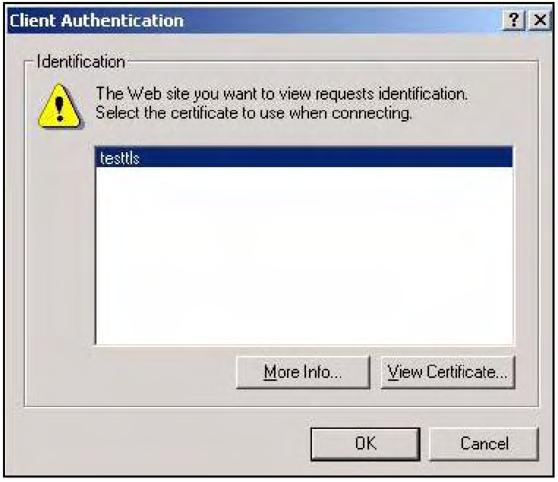
about:blank - Microsoft Internet Explorer

File Edit View Favorites Tools Help
Back Search Favorites History

Address https://192.168.1.1

2 When **Authenticate Client Certificates** is selected on the ZyXEL Device, the following screen asks you to select a personal certificate to send to the ZyXEL Device. This screen displays even if you only have a single certificate as in the example.

Figure 271 SSL Client Authentication



Client Authentication

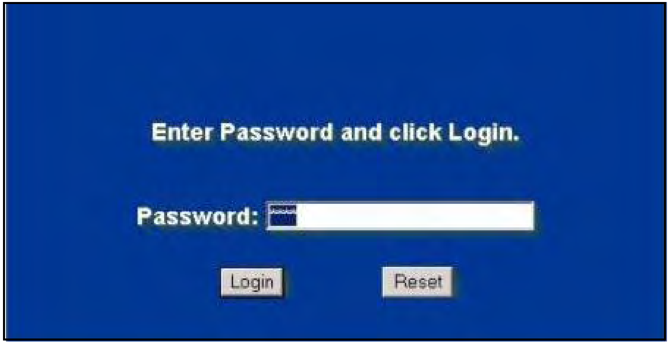
Identification

The Web site you want to view requests identification.
Select the certificate to use when connecting.

testtls

3 You next see the ZyXEL Device login screen.

Figure 272 ZyXEL Device Secure Login Screen



Enter Password and click Login.

Password:

G

Legal Information

Copyright

Disclaimer

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 ZyXEL Device is subject to the terms and conditions of any related service providers.

Trademarks

ZyNOS (ZyXEL Network Operating System) is a registered trademark of ZyXEL Communications, Inc. Other trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

Certifications

Federal Communications Commission (FCC) Interference Statement

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

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

This device has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This device generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

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

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

FCC Radiation Exposure Statement

- This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
- IEEE 802.11b or 802.11g operation of this product in the U.S.A. is firmware-limited to channels 1 through 11.
- To comply with FCC RF exposure compliance requirements, a separation distance of at least 20 cm must be maintained between the antenna of this device and all persons.

注意 ！

依據　低功率電波輻射性電機管理辦法

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

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

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

Notices

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

This device has been designed for the WLAN 2.4 GHz network throughout the EC region and Switzerland, with restrictions in France.

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

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

Viewing Certifications

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

ZyXEL Limited Warranty

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

Note

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

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

Registration

Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com for global products, or at www.us.zyxel.com for North American products.

H

Customer Support

In the event of problems that cannot be solved by using this manual, you should contact your vendor. If you cannot contact your vendor, then contact a ZyXEL office for the region in which you bought the device. Regional offices are listed below (see also http://www.zyxel.com/web/contact_us.php). Please have the following information ready when you contact an office.

Required Information

- Product model and serial number.
- Warranty Information.
- Date that you received your device.
- Brief description of the problem and the steps you took to solve it.

"+" is the (prefix) number you dial to make an international telephone call.

Corporate Headquarters (Worldwide)

- Support E-mail: support@zyxel.com.tw
- Sales E-mail: sales@zyxel.com.tw
- Telephone: +886-3-578-3942
- Fax: +886-3-578-2439
- Web: www.zyxel.com
- Regular Mail: ZyXEL Communications Corp., 6 Innovation Road II, Science Park, Hsinchu 300, Taiwan

China - ZyXEL Communications (Beijing) Corp.

- Support E-mail: cso.zycn@zyxel.cn
- Sales E-mail: sales@zyxel.cn
- Telephone: +86-010-82800646
- Fax: +86-010-82800587
- Address: 902, Unit B, Horizon Building, No.6, Zhichun Str, Haidian District, Beijing
- Web: http://www.zyxel.cn

China - ZyXEL Communications (Shanghai) Corp.

- Support E-mail: cso.zycn@zyxel.cn
- Sales E-mail: sales@zyxel.cn
- Telephone: +86-021-61199055
- Fax: +86-021-52069033

- Address: 1005F, ShengGao International Tower, No.137 XianXia Rd., Shanghai
- Web: http://www.zyxel.cn

Costa Rica

- Support E-mail: soporte@zyxel.co.cr
- Sales E-mail: sales@zyxel.co.cr
- Telephone: +506-2017878
- Fax: +506-2015098
- Web: www.zyxel.co.cr
- Regular Mail: ZyXEL Costa Rica, Plaza Roble Escazú, Etapa El Patio, Tercer Piso, San José, Costa Rica

Czech Republic

- E-mail: info@cz.zyxel.com
- Telephone: +420-241-091-350
- Fax: +420-241-091-359
- Web: www.zyxel.cz
- Regular Mail: ZyXEL Communications, Czech s.r.o., Modranská 621, 143 01 Praha 4 - Modrany, Ceská Republika

Denmark

- Support E-mail: support@zyxel.dk
- Sales E-mail: sales@zyxel.dk
- Telephone: +45-39-55-07-00
- Fax: +45-39-55-07-07
- Web: www.zyxel.dk
- Regular Mail: ZyXEL Communications A/S, Columbusvej, 2860 Soeborg, Denmark

Finland

- Support E-mail: support@zyxel.fi
- Sales E-mail: sales@zyxel.fi
- Telephone: +358-9-4780-8411
- Fax: +358-9-4780-8448
- Web: www.zyxel.fi
- Regular Mail: ZyXEL Communications Oy, Malminkaari 10, 00700 Helsinki, Finland

France

- E-mail: info@zyxel.fr
- Telephone: +33-4-72-52-97-97
- Fax: +33-4-72-52-19-20
- Web: www.zyxel.fr
- Regular Mail: ZyXEL France, 1 rue des Vergers, Bat. 1 / C, 69760 Limonest, France

Germany

- Support E-mail: support@zyxel.de
- Sales E-mail: sales@zyxel.de
- Telephone: +49-2405-6909-69
- Fax: +49-2405-6909-99
- Web: www.zyxel.de
- Regular Mail: ZyXEL Deutschland GmbH., Adenauerstr. 20/A2 D-52146, Wuerselen, Germany

Hungary

- Support E-mail: support@zyxel.hu
- Sales E-mail: info@zyxel.hu
- Telephone: +36-1-3361649
- Fax: +36-1-3259100
- Web: www.zyxel.hu
- Regular Mail: ZyXEL Hungary, 48, Zoldlomb Str., H-1025, Budapest, Hungary

India

- Support E-mail: support@zyxel.in
- Sales E-mail: sales@zyxel.in
- Telephone: +91-11-30888144 to +91-11-30888153
- Fax: +91-11-30888149, +91-11-26810715
- Web: http://www.zyxel.in
- Regular Mail: India - ZyXEL Technology India Pvt Ltd., II-Floor, F2/9 Okhla Phase -1, New Delhi 110020, India

Japan

- Support E-mail: support@zyxel.co.jp
- Sales E-mail: zyp@zyxel.co.jp
- Telephone: +81-3-6847-3700
- Fax: +81-3-6847-3705
- Web: www.zyxel.co.jp
- Regular Mail: ZyXEL Japan, 3F, Office T&U, 1-10-10 Higashi-Gotanda, Shinagawa-ku, Tokyo 141-0022, Japan

Kazakhstan

- Support: http://zyxel.kz/support
- Sales E-mail: sales@zyxel.kz
- Telephone: +7-3272-590-698
- Fax: +7-3272-590-689
- Web: www.zyxel.kz
- Regular Mail: ZyXEL Kazakhstan, 43 Dostyk Ave., Office 414, Dostyk Business Centre, 050010 Almaty, Republic of Kazakhstan

Malaysia

- Support E-mail: support@zyxel.com.my
- Sales E-mail: sales@zyxel.com.my
- Telephone: +603-8076-9933
- Fax: +603-8076-9833
- Web: http://www.zyxel.com.my
- Regular Mail: ZyXEL Malaysia Sdn Bhd., 1-02 & 1-03, Jalan Kenari 17F, Bandar Puchong Jaya, 47100 Puchong, Selangor Darul Ehsan, Malaysia

North America

- Support E-mail: support@zyxel.com
- Support Telephone: +1-800-978-7222
- Sales E-mail: sales@zyxel.com
- Sales Telephone: +1-714-632-0882
- Fax: +1-714-632-0858
- Web: www.zyxel.com
- Regular Mail: ZyXEL Communications Inc., 1130 N. Miller St., Anaheim, CA 92806-2001, U.S.A.

Norway

- Support E-mail: support@zyxel.no
- Sales E-mail: sales@zyxel.no
- Telephone: +47-22-80-61-80
- Fax: +47-22-80-61-81
- Web: www.zyxel.no
- Regular Mail: ZyXEL Communications A/S, Nils Hansens vei 13, 0667 Oslo, Norway

Poland

- E-mail: info@pl.zyxel.com
- Telephone: +48-22-333 8250
- Fax: +48-22-333 8251
- Web: www.pl.zyxel.com
- Regular Mail: ZyXEL Communications, ul. Okrzei 1A, 03-715 Warszawa, Poland

Russia

- Support: http://zyxel.ru/support
- Sales E-mail: sales@zyxel.ru
- Telephone: +7-095-542-89-29
- Fax: +7-095-542-89-25
- Web: www.zyxel.ru
- Regular Mail: ZyXEL Russia, Ostrovityanova 37a Str., Moscow 117279, Russia

Singapore

- Support E-mail: support@zyxel.com.sg
- Sales E-mail: sales@zyxel.com.sg
- Telephone: +65-6899-6678
- Fax: +65-6899-8887
- Web: http://www.zyxel.com.sg
- Regular Mail: ZyXEL Singapore Pte Ltd., No. 2 International Business Park, The Strategy #03-28, Singapore 609930

Spain

- Support E-mail: support@zyxel.es
- Sales E-mail: sales@zyxel.es
- Telephone: +34-902-195-420
- Fax: +34-913-005-345
- Web: www.zyxel.es
- Regular Mail: ZyXEL Communications, Arte, 21 5ª planta, 28033 Madrid, Spain

Sweden

- Support E-mail: support@zyxel.se
- Sales E-mail: sales@zyxel.se
- Telephone: +46-31-744-7700
- Fax: +46-31-744-7701
- Web: www.zyxel.se
- Regular Mail: ZyXEL Communications A/S, Sjöporten 4, 41764 Göteborg, Sweden

Taiwan

- Support E-mail: support@zyxel.com.tw
- Sales E-mail: sales@zyxel.com.tw
- Telephone: +886-2-27399889
- Fax: +886-2-27353220
- Web: http://www.zyxel.com.tw
- Address: Room B, 21F., No.333, Sec. 2, Dunhua S. Rd., Da-an District, Taipei

Thailand

- Support E-mail: support@zyxel.co.th
- Sales E-mail: sales@zyxel.co.th
- Telephone: +662-831-5315
- Fax: +662-831-5395
- Web: http://www.zyxel.co.th
- Regular Mail: ZyXEL Thailand Co., Ltd., 1/1 Moo 2, Ratchaphruk Road, Bangrak-Noi, Muang, Nonthaburi 11000, Thailand.

Turkey

- Support E-mail: cso@zyxel.com.tr
- Telephone: +90 212 222 55 22
- Fax: +90-212-220-2526
- Web: http:www.zyxel.com.tr
- Address: Kaptanpasa Mahallesi Piyalepasa Bulvari Ortadogu Plaza N:14/13 K:6 Okmeydani/Sisli Istanbul/Turkey

Ukraine

- Support E-mail: support@ua.zyxel.com
- Sales E-mail: sales@ua.zyxel.com
- Telephone: +380-44-247-69-78
- Fax: +380-44-494-49-32
- Web: www.ua.zyxel.com
- Regular Mail: ZyXEL Ukraine, 13, Pimonenko Str., Kiev 04050, Ukraine

United Kingdom

- Support E-mail: support@zyxel.co.uk
- Sales E-mail: sales@zyxel.co.uk
- Telephone: +44-1344-303044, 0845 122 0301 (UK only)
- Fax: +44-1344-303034
- Web: www.zyxel.co.uk
- Regular Mail: ZyXEL Communications UK Ltd., 11 The Courtyard, Eastern Road, Bracknell, Berkshire RG12 2XB, United Kingdom (UK)

Index