Table 96 Security > Certificates > Trusted CAs (continued)

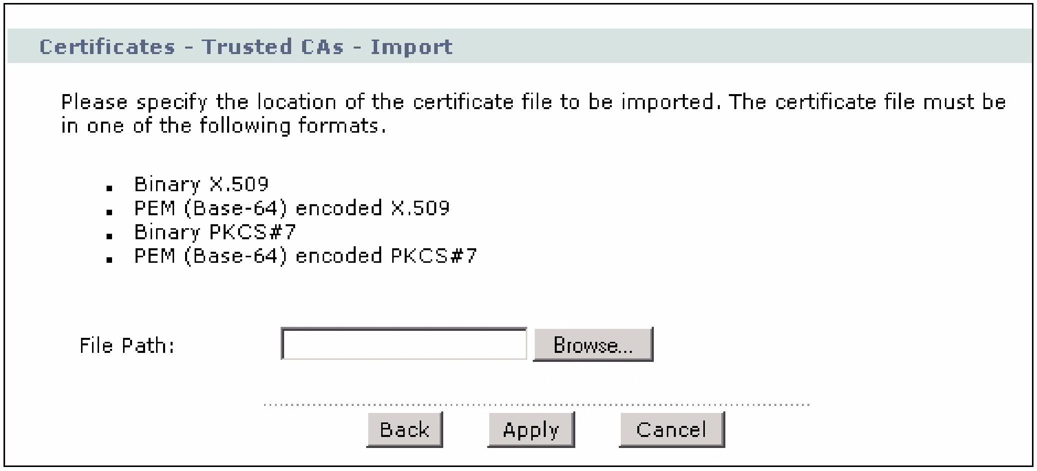
LABEL	DESCRIPTION
Subject	This field displays identifying information about the certificate's owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). It is recommended that each certificate have unique subject information.
Issuer	This field 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 Certificate Revocation Lists for the certificates that it has issued and you have selected the **Issues certificate revocation lists (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".
Modify	Click the Edit icon to open a screen with an in-depth list of information about the certificate. Click the Remove 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.

15.6 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 to the ZyXEL Device.

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

Figure 179 Security > Certificates > Trusted CA > Import



Certificates - Trusted CAs - 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: [   ]

The following table describes the labels in this screen.

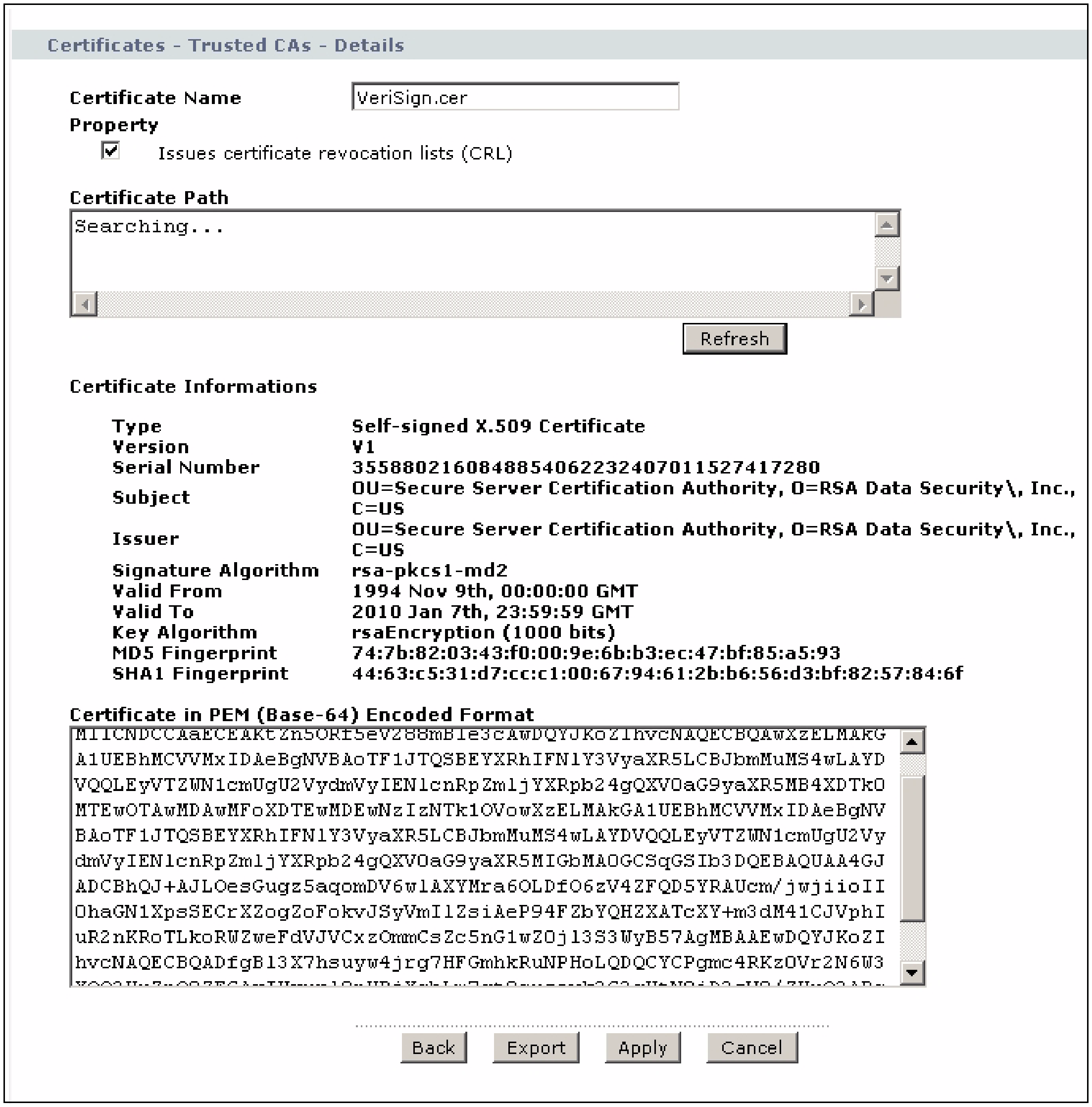
Table 97 Security > Certificates > Trusted CA > Import

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.
Back	Click **Back** to return to the previous screen.
Apply	Click **Apply** to save the certificate on the ZyXEL Device.
Cancel	Click **Cancel** to quit and return to the **Trusted CAs** screen.

15.7 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 180 Security > Certificates > Trusted CA > Details



Certificates - Trusted CAs - Details

Certificate Name: VeriSign.cer

Property

☑ Issues certificate revocation lists (CRL)

Certificate Path

```
Searching...
```

Certificate Informations

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

```
MIICNDCCAaECEAKtZn5ORf5eV288mBle3cAwDQYJKoZIhvcNAQECBQAwXzELMAkG
A1UEBhMCVVMxIDAeBgNVBAoTF1JTQSBEYXRhIFN1Y3VyaXR5LCBJbmMuMS4wLAYD
VQQLEyVTZWN1cmUgU2VydmVyIEN1cnRpZmljYXRpb24gQXV0aG9yaXR5MB4XDTk0
MTEwOTAwMDAwMFoXDTEwMDEwNzIzNTk1OVowXzELMAkGA1UEBhMCVVMxIDAeBgNV
BAoTF1JTQSBEYXRhIFN1Y3VyaXR5LCBJbmMuMS4wLAYDVQQLEyVTZWN1cmUgU2Vy
dmVyIEN1cnRpZmljYXRpb24gQXV0aG9yaXR5MIGbMA0GCSqGSIb3DQEBAQUAA4GJ
ADCBhQJ+AJLOesGugz5aqomDV6wlAXYMra6OLDfO6zV4ZFQD5YRAUcm/jwjiioII
0haGN1XpsSECrXZogZoFokvJSyVmIlZsiAeP94FZbYQHZXATcXY+m3dM41CJVphI
uR2nKRoTLkoRWZweFdVJVCxzOmmCsZc5nG1wZ0jl3S3WyB57AgMBAAEwDQYJKoZI
hvcNAQECBQADfgBl3X7hsuyw4jrg7HFGmhkRuNPHoLQDQCYCPgmc4RKz0Vr2N6W3
```

The following table describes the labels in this screen.

Table 98 Security > Certificates > Trusted CA > Details

LABEL	DESCRIPTION
Certificate 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 Issues certificate revocation lists (CRLs)	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).
Certificate 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.

Table 98 Security > Certificates > Trusted CA > Details (continued)

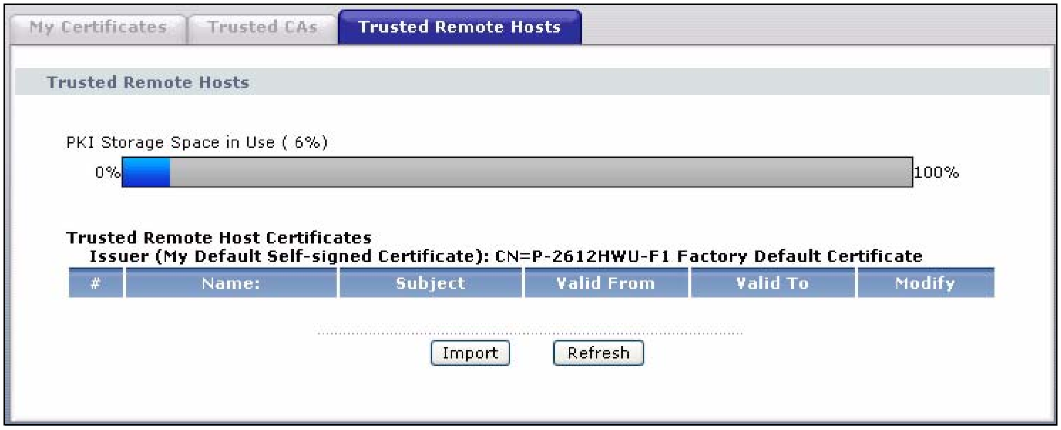
LABEL	DESCRIPTION
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.
Key Algorithm	This field displays the type of algorithm that was used to generate 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.
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).
Back	Click **Back** to return to the previous screen.
Export	Click this button 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**.
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.

15.8 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 181 Security > Certificates > Trusted Remote Hosts



Trusted Remote Hosts

PKI Storage Space in Use (6%)

Trusted Remote Host Certificates

Issuer (My Default Self-signed Certificate): CN=P-2612HWU-F1 Factory Default Certificate

#	Name:	Subject	Valid From	Valid To	Modify

The following table describes the labels in this screen.

Table 99 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. The bar turns from green to red when the maximum is being approached. When the bar is red, 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.

Table 99 Security > Certificates > Trusted Remote Hosts (continued)

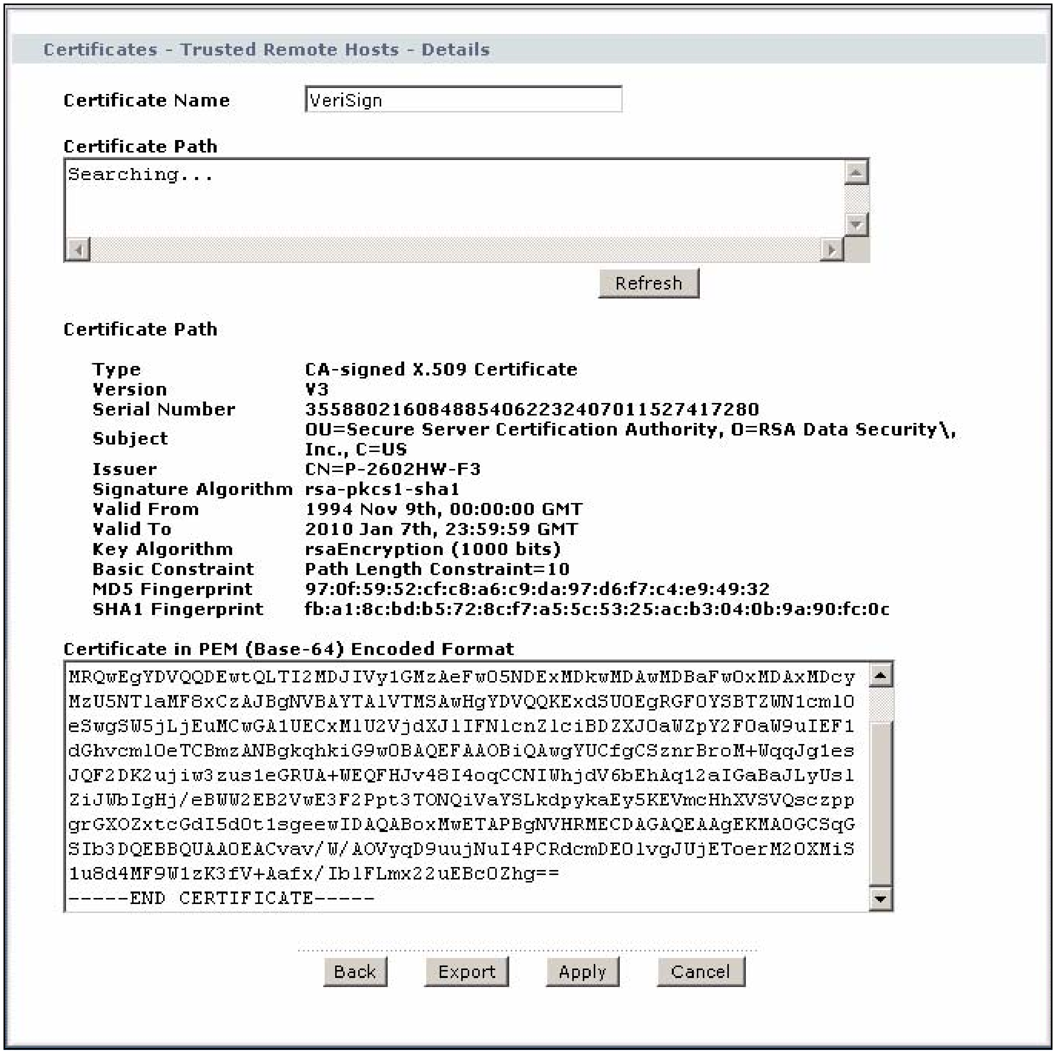
LABEL	DESCRIPTION
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.
Modify	Click the Edit icon to open a screen with an in-depth list of information about the certificate. Click the Remove 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.

15.9 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. Use this screen to view in-depth information about the trusted remote host's certificate and/or change the certificate's name.

Figure 182 Security > Certificates > Trusted Remote Hosts > Details



Certificates - Trusted Remote Hosts - Details

Certificate Name: VeriSign

Certificate Path

```
Searching...
```

Certificate Path

Type	CA-signed X.509 Certificate
Version	V3
Serial Number	3558802160848854062232407011527417280
Subject	OU=Secure Server Certification Authority, O=RSA Data Security\, Inc., C=US
Issuer	CN=P-2602HW-F3
Signature Algorithm	rsa-pkcs1-sha1
Valid From	1994 Nov 9th, 00:00:00 GMT
Valid To	2010 Jan 7th, 23:59:59 GMT
Key Algorithm	rsaEncryption (1000 bits)
Basic Constraint	Path Length Constraint=10
MD5 Fingerprint	97:0f:59:52:cf:c8:a6:c9:da:97:d6:f7:c4:e9:49:32
SHA1 Fingerprint	fb:a1:8c:bd:b5:72:8c:f7:a5:5c:53:25:ac:b3:04:0b:9a:90:fc:0c

Certificate in PEM (Base-64) Encoded Format

```
MRQwEgYDVQQDEwtQLTI2MDJIVy1GMzAeFw05NDExMDkwMDAwMDBaFw0xMDAxMDcy
MzU5NTlaMF8xCzAJBgNVBAYTAlVTMSAwHgYDVQQKExdSU0EgRGF0YSBTZWN1cml0
eSwgSW5jLjEuMCwGA1UECxMlU2VjdXJlIFNlcnZlciBDZXJ0aWZpY2F0aW9uIEF1
dGhvcml0eTCBmzANBgkqhkiG9w0BAQEFAAOBiQAwgYUCfgCSznrBroM+WqqJg1es
JQF2DK2ujiw3zus1eGRUA+WEQFHJv48I4oqCCNIWhjdV6bEhAq12aIGaBaJLyUs1
ZiJWbIgHj/eBWW2EB2VwE3F2Ppt3TONQiVaYSLkdpykaEy5KEVmcHhXVSVQsczpp
grGXOZxtcGdI5d0t1sgeewIDAQABoxMwETAPBgNVHRMECDAGAQEAAgEKMA0GCSqG
SIb3DQEBBQUAA0EACvav/W/AOVyqD9uujNuI4PCRdcmDEOlvgJUjEToerM2OXMiS
1u8d4MF9W1zK3fV+Aafx/IblFLmx22uEBc0Zhg==
-----END CERTIFICATE-----
```

The following table describes the labels in this screen.

Table 100 Security > Certificates > Trusted Remote Hosts > Details

LABEL	DESCRIPTION
Certificate 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).
Certificate 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.

Table 100 Security > Certificates > Trusted Remote Hosts > Details (continued)

LABEL	DESCRIPTION
Certificate Path	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.
MD5 Fingerprint	This is the certificate's message digest that the ZyXEL Device calculated using the MD5 algorithm. You cannot use this value to verify that this is the remote host's actual certificate because the ZyXEL Device has signed the certificate; thus causing this value to be different from that of the remote hosts actual certificate. See Section 15.1.3 on page 289 for how to verify a remote host's certificate.

Table 100 Security > Certificates > Trusted Remote Hosts > Details (continued)

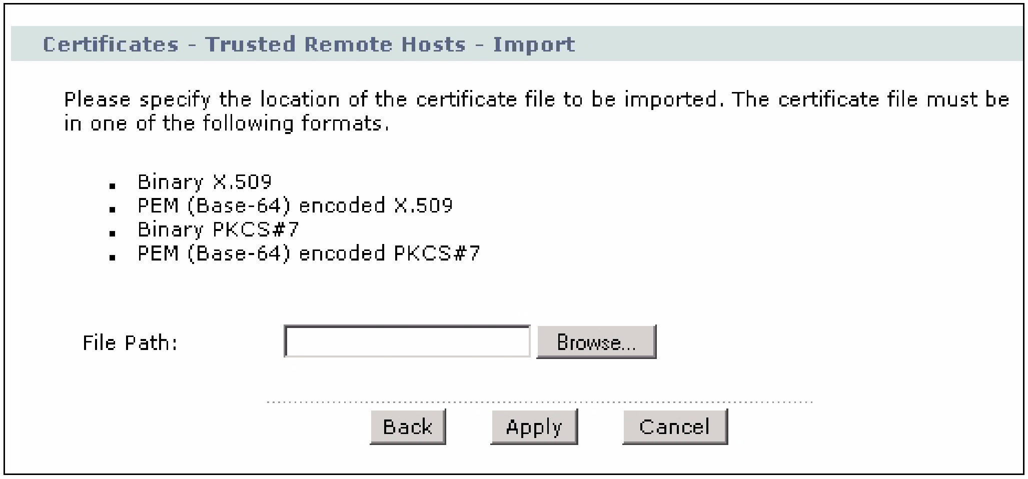
LABEL	DESCRIPTION
SHA1 Fingerprint	This is the certificate's message digest that the ZyXEL Device calculated using the SHA1 algorithm. You cannot use this value to verify that this is the remote host's actual certificate because the ZyXEL Device has signed the certificate; thus causing this value to be different from that of the remote hosts actual certificate. See Section 15.1.3 on page 289 for how to verify a remote host's 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).
Back	Click **Back** to return to the previous screen.
Export	Click this button 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**.
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.

15.10 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. Follow the instructions in this screen to save a trusted host's certificate to the ZyXEL Device.

Note: 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 183 Security > Certificates > Trusted Remote Hosts > Import



Certificates - Trusted Remote Hosts - 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 101 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.
Back	Click **Back** to return to the previous screen.
Apply	Click **Apply** to save the certificate on the ZyXEL Device.
Cancel	Click **Cancel** to quit and return to the **Trusted Remote Hosts** screen.

CHAPTER 16

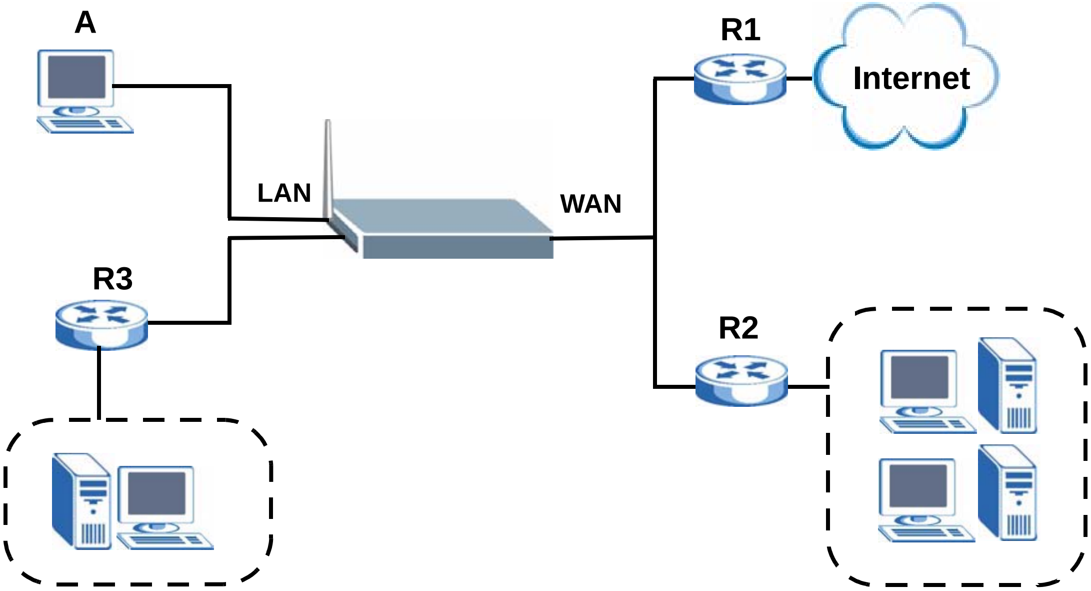
Static Route

16.1 Overview

The ZyXEL Device usually uses the default gateway to route outbound traffic from computers on the LAN 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 ZyXEL Device's 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 184 Example of Static Routing Topology



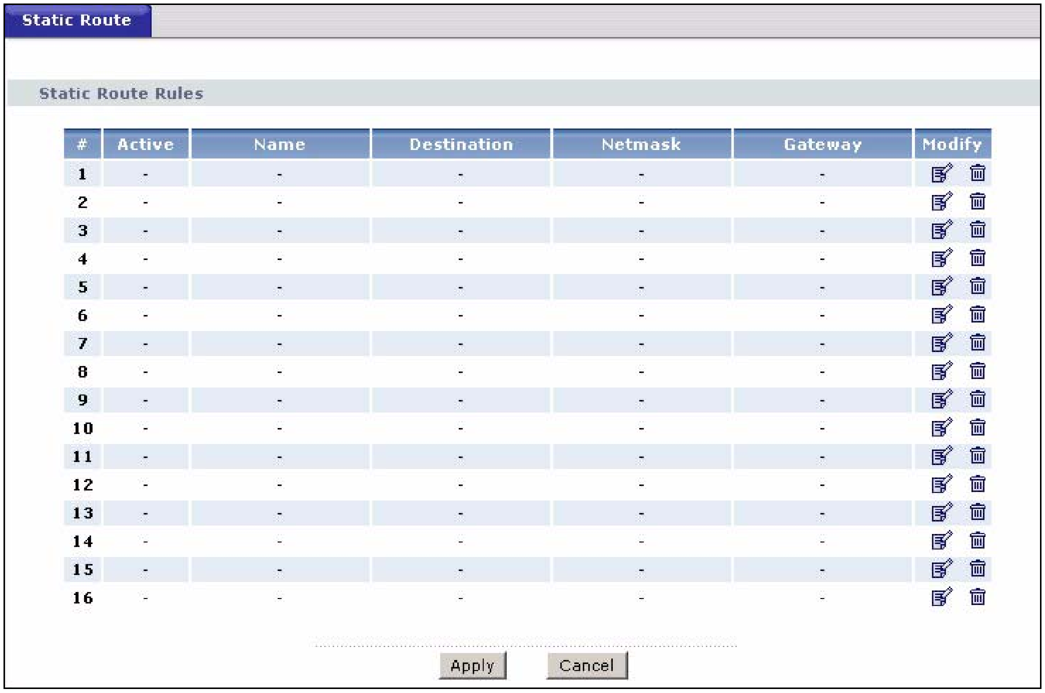
16.1.1 What You Can Do in the Static Route Screens

Use the **Static Route** screens (Section 16.2 on page 314) to view and configure IP static routes on the ZyXEL Device.

16.2 Configuring Static Route

Click **Advanced > Static Route** to open the **Static Route** screen.

Figure 185 Advanced > Static Route



Static Route Rules

#	Active	Name	Destination	Netmask	Gateway	Modify
1	-	-	-	-	-	✎ 🗑
2	-	-	-	-	-	✎ 🗑
3	-	-	-	-	-	✎ 🗑
4	-	-	-	-	-	✎ 🗑
5	-	-	-	-	-	✎ 🗑
6	-	-	-	-	-	✎ 🗑
7	-	-	-	-	-	✎ 🗑
8	-	-	-	-	-	✎ 🗑
9	-	-	-	-	-	✎ 🗑
10	-	-	-	-	-	✎ 🗑
11	-	-	-	-	-	✎ 🗑
12	-	-	-	-	-	✎ 🗑
13	-	-	-	-	-	✎ 🗑
14	-	-	-	-	-	✎ 🗑
15	-	-	-	-	-	✎ 🗑
16	-	-	-	-	-	✎ 🗑

The following table describes the labels in this screen.

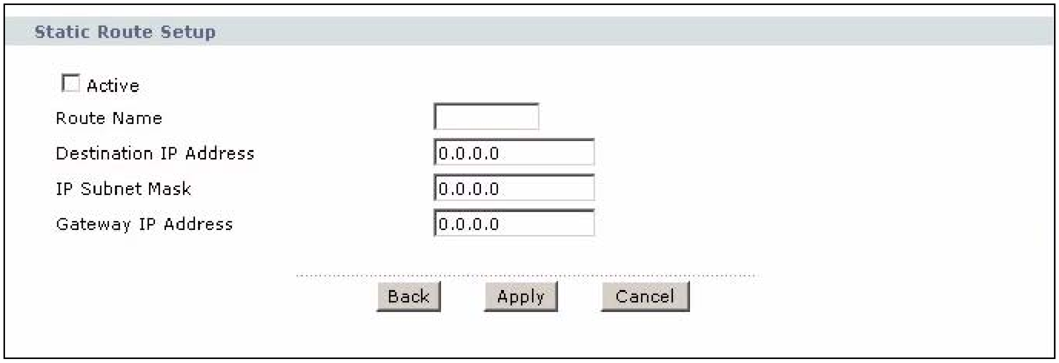
Table 102 Advanced > Static Route

LABEL	DESCRIPTION
#	This is the number of an individual static route.
Active	This field indicates whether the rule is active or not. Clear the check box to disable the rule. Select the check box to enable it.
Name	This is the name that describes or identifies this route.
Destination	This parameter specifies the IP network address of the final destination. Routing is always based on network number.
Netmask	This parameter specifies the IP network subnet mask of the final destination.
Gateway	This is 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.
Modify	Click the Edit icon to go to the screen where you can set up a static route on the ZyXEL Device. Click the Remove icon to remove a static route from the ZyXEL Device. A window displays asking you to confirm that you want to delete the route.
Apply	Click this to apply your changes to the ZyXEL Device.
Cancel	Click this to return to the previously saved configuration.

16.2.1 Static Route Edit

Select a static route index number and click **Edit**. The screen shown next appears. Use this screen to configure the required information for a static route.

Figure 186 Advanced > Static Route > Edit



Static Route Setup

☐ Active

Route Name	
Destination IP Address	0.0.0.0
IP Subnet Mask	0.0.0.0
Gateway IP Address	0.0.0.0

The following table describes the labels in this screen.

Table 103 Advanced > Static Route > Edit

LABEL	DESCRIPTION
Active	This field allows you to activate/deactivate this static route.
Route Name	Enter the name of the IP static route. Leave this field blank to delete 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.
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.
Back	Click **Back** to return to the previous screen without saving.
Apply	Click **Apply** to save your changes back to the ZyXEL Device.
Cancel	Click **Cancel** to begin configuring this screen afresh.

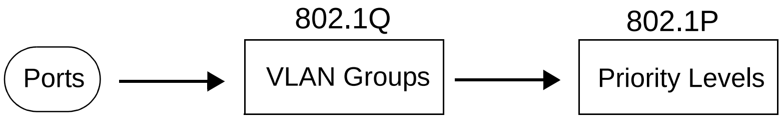
17

802.1Q/1P

17.1 Overview

A Virtual Local Area Network (VLAN) allows a physical network to be partitioned into multiple logical networks. A VLAN group can be treated as an individual device. Each group can have its own rules about where and how to forward traffic. You can assign any ports on the ZyXEL Device to a VLAN group and configure the settings for the group. You may also set the priority level for traffic transmitted through the ports.

Figure 187 802.1Q/1P



17.1.1 What You Can Do in the 802.1Q/1P Screens

- Use the **Group Setting** screen (Section 17.2 on page 324) to activate 802.1Q/1P, specify the management VLAN group, display the VLAN groups and configure the settings for each VLAN group.
- Use the **Port Setting** screen (Section 17.3 on page 327) to configure the PVID and assign traffic priority for each port.

17.1.2 What You Need to Know About 802.1Q/1P

IEEE 802.1P Priority

IEEE 802.1P specifies the user priority field and defines up to eight separate traffic types by inserting a tag into a MAC-layer frame that contains bits to define class of service.

IEEE 802.1Q Tagged VLAN

Tagged VLAN uses an explicit tag (VLAN ID) in the MAC header to identify the VLAN membership of a frame across bridges - they are not confined to the device on which they were created. The VLAN ID associates a frame with a specific VLAN and provides the information that devices need to process the frame across the network.

PVC

A virtual circuit is a logical point-to-point circuit between customer sites. Permanent means that the circuit is preprogrammed by the carrier as a path through the network. It does not need to be set up or torn down for each session.

Forwarding Tagged and Untagged Frames

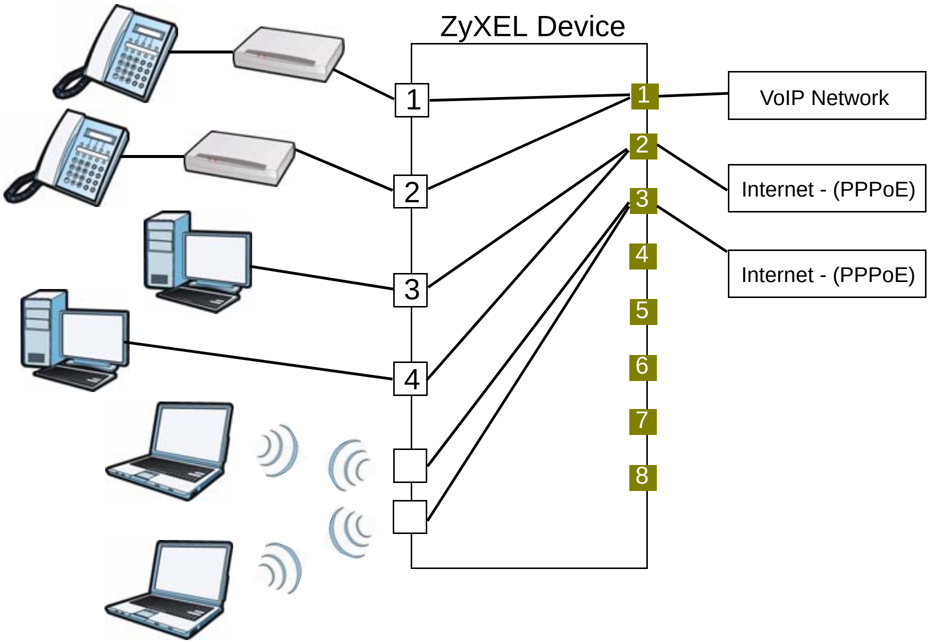
Each port on the device is capable of passing tagged or untagged frames. To forward a frame from an 802.1Q VLAN-aware device to an 802.1Q VLAN-unaware device, the ZyXEL Device first decides where to forward the frame and then strips off the VLAN tag. To forward a frame from an 802.1Q VLAN-unaware device to an 802.1Q VLAN-aware switch, the ZyXEL Device first decides where to forward the frame, and then inserts a VLAN tag reflecting the ingress port's default VID. The default PVID is VLAN 1 for all ports, but this can be changed.

Whether to tag an outgoing frame depends on the setting of the egress port on a per-VLAN, per-port basis (recall that a port can belong to multiple VLANs). If the tagging on the egress port is enabled for the VID of a frame, then the frame is transmitted as a tagged frame; otherwise, it is transmitted as an untagged frame.

17.1.3 802.1Q/1P Example

This example shows how to configure the 802.1Q/1P settings on the ZyXEL Device.

Figure 188 802.1Q/1P Example



LAN1 and LAN2 are connected to ATAs (Analog Telephone Adapters) and used for VoIP traffic. You want to set a high priority for this type of traffic, so you will group these ports into one VLAN (VLAN2) and then set them to use a PVC (PVC1) with a high priority service level. You would start with the following steps.

1 Click **Advanced** > **802.1Q/1P** > **Group Setting** > **Edit** to display the following screen.

2 In the **Name** field type VoIP to identify the group.

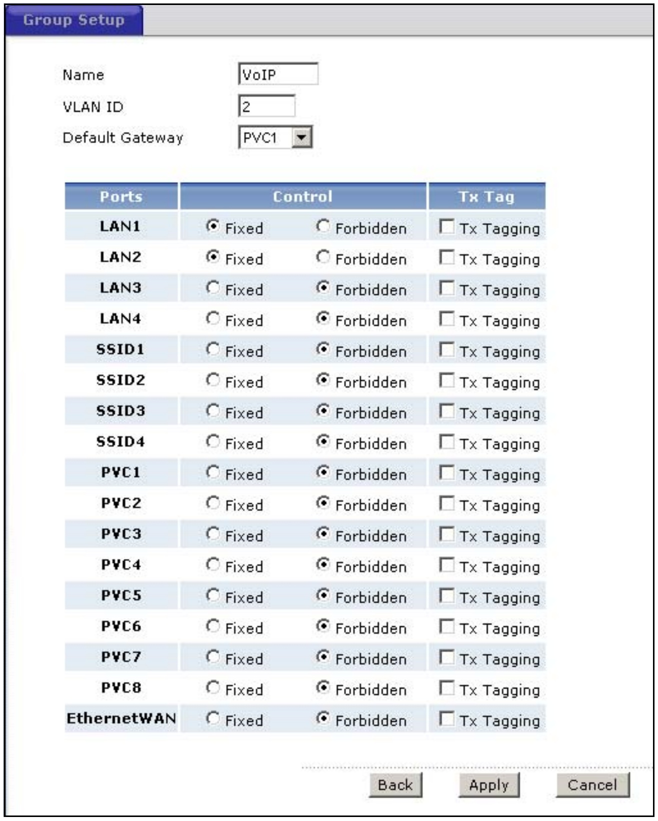
3 In the **VLAN ID** field type in 2 to identify the VLAN group.

4 Select **PVC1** from the **Default Gateway** drop-down list box.

5 In the **Control** field, select **Fixed** for LAN1, LAN2 and PVC1 to be permanent members of the VLAN group.

6 Click **Apply**.

Figure 189 Advanced > 802.1Q/1P > Group Setting > Edit: Example



Name	VoIP
VLAN ID	2
Default Gateway	PVC1

Ports	Control		Tx Tag
LAN1	● Fixed	○ Forbidden	□ Tx Tagging
LAN2	● Fixed	○ Forbidden	□ Tx Tagging
LAN3	○ Fixed	● Forbidden	□ Tx Tagging
LAN4	○ Fixed	● Forbidden	□ Tx Tagging
SSID1	○ Fixed	● Forbidden	□ Tx Tagging
SSID2	○ Fixed	● Forbidden	□ Tx Tagging
SSID3	○ Fixed	● Forbidden	□ Tx Tagging
SSID4	○ Fixed	● Forbidden	□ Tx Tagging
PVC1	○ Fixed	● Forbidden	□ Tx Tagging
PVC2	○ Fixed	● Forbidden	□ Tx Tagging
PVC3	○ Fixed	● Forbidden	□ Tx Tagging
PVC4	○ Fixed	● Forbidden	□ Tx Tagging
PVC5	○ Fixed	● Forbidden	□ Tx Tagging
PVC6	○ Fixed	● Forbidden	□ Tx Tagging
PVC7	○ Fixed	● Forbidden	□ Tx Tagging
PVC8	○ Fixed	● Forbidden	□ Tx Tagging
EthernetWAN	○ Fixed	● Forbidden	□ Tx Tagging

To set a high priority for VoIP traffic, follow these steps.

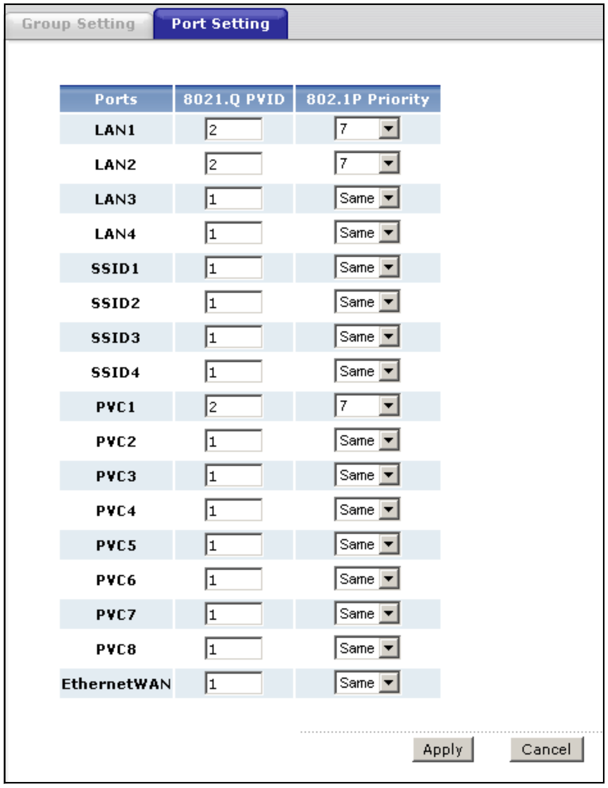
1 Click **Advanced** > **802.1Q/1P** > **Port Setting** to display the following screen.

2 Type 2 in the **802.1Q PVID** column for LAN1, LAN2 and PVC1.

3 Select **7** from the **802.1P Priority** drop-down list box for LAN1, LAN2 and PVC1.

4 Click **Apply**.

Figure 190 Advanced > 802.1Q/1P > Port Setting: Example



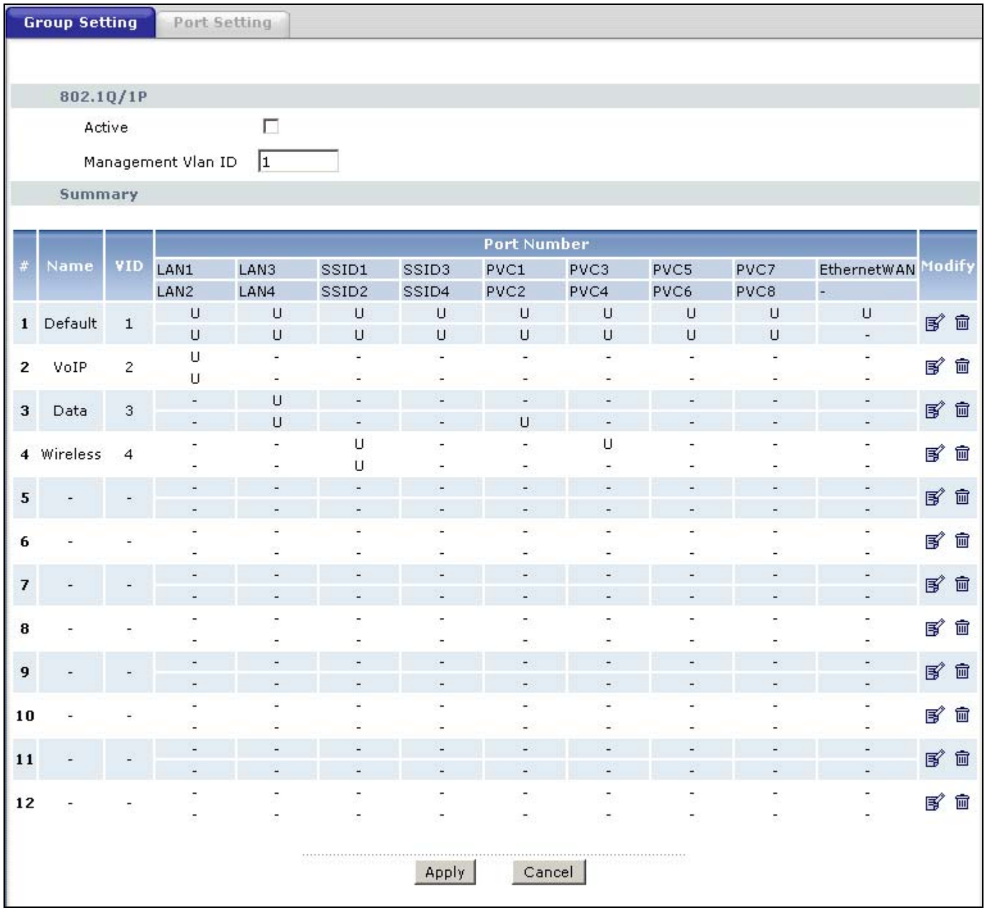
Ports	8021.Q PVID	802.1P Priority
LAN1	2	7
LAN2	2	7
LAN3	1	Same
LAN4	1	Same
SSID1	1	Same
SSID2	1	Same
SSID3	1	Same
SSID4	1	Same
PVC1	2	7
PVC2	1	Same
PVC3	1	Same
PVC4	1	Same
PVC5	1	Same
PVC6	1	Same
PVC7	1	Same
PVC8	1	Same
EthernetWAN	1	Same

Ports 3 and 4 are connected to desktop computers and are used for Internet traffic. You want to set a lower priority for this type of traffic, so you want to group these ports and PVC2 into one VLAN (VLAN3). PVC2 priority is set to low level of service.

SSID1 and SSID2 are two wireless networks. You want to create medium priority for this type of traffic, so you want to group these ports and PVC3 into one VLAN (VLAN4). PVC3 priority is set to medium level of service.

Follow the same steps as in VLAN2 to configure the settings for VLAN3 and VLAN4. The summary screen should display as follows.

Figure 191 Advanced > 802.1Q/1P > Group Setting: Example



802.1Q/1P

Active □

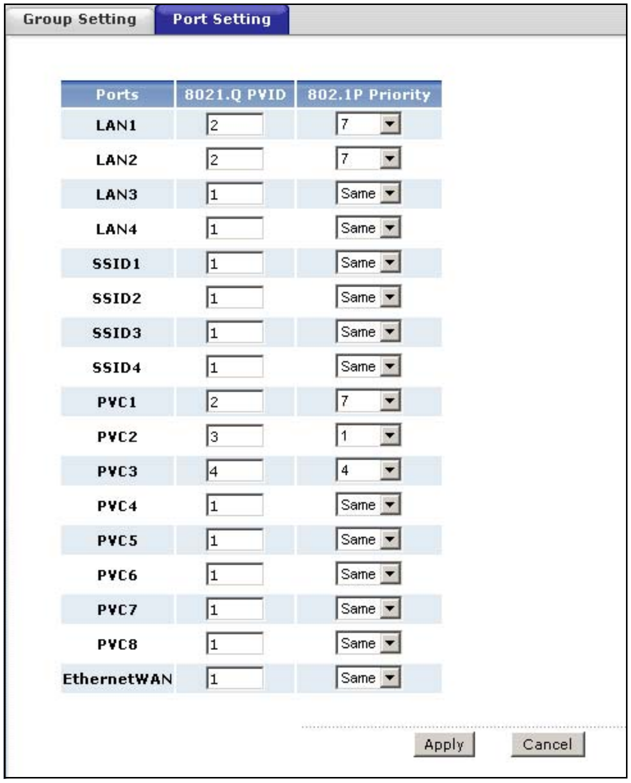
Management Vlan ID 1

Summary

#	Name	VID	Port Number									Modify
			LAN1 LAN2	LAN3 LAN4	SSID1 SSID2	SSID3 SSID4	PVC1 PVC2	PVC3 PVC4	PVC5 PVC6	PVC7 PVC8	EthernetWAN -	
1	Default	1	U U	U U	U U	U U	U U	U U	U U	U U	U -	✎ 🗑
2	VoIP	2	U U	- -	- -	- -	- -	- -	- -	- -	- -	✎ 🗑
3	Data	3	- -	U U	- -	- -	- U	- -	- -	- -	- -	✎ 🗑
4	Wireless	4	- -	- -	U U	- -	- -	U -	- -	- -	- -	✎ 🗑
5	-	-	- -	- -	- -	- -	- -	- -	- -	- -	- -	✎ 🗑
6	-	-	- -	- -	- -	- -	- -	- -	- -	- -	- -	✎ 🗑
7	-	-	- -	- -	- -	- -	- -	- -	- -	- -	- -	✎ 🗑
8	-	-	- -	- -	- -	- -	- -	- -	- -	- -	- -	✎ 🗑
9	-	-	- -	- -	- -	- -	- -	- -	- -	- -	- -	✎ 🗑
10	-	-	- -	- -	- -	- -	- -	- -	- -	- -	- -	✎ 🗑
11	-	-	- -	- -	- -	- -	- -	- -	- -	- -	- -	✎ 🗑
12	-	-	- -	- -	- -	- -	- -	- -	- -	- -	- -	✎ 🗑

The port screen should look like this.

Figure 192 Advanced > 802.1Q/1P > Port Setting: Example



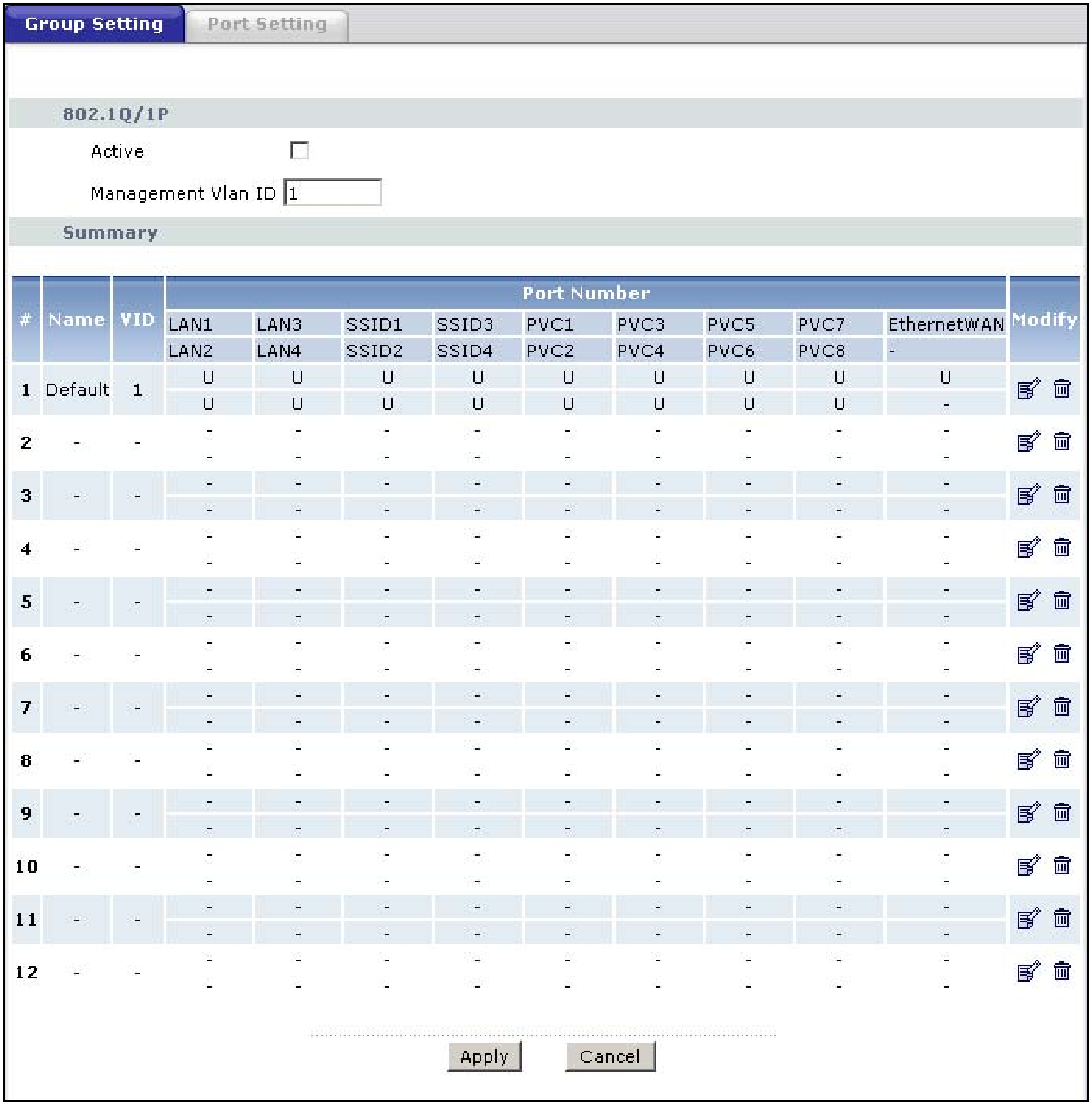
Ports	8021.Q PVID	802.1P Priority
LAN1	2	7
LAN2	2	7
LAN3	1	Same
LAN4	1	Same
SSID1	1	Same
SSID2	1	Same
SSID3	1	Same
SSID4	1	Same
PVC1	2	7
PVC2	3	1
PVC3	4	4
PVC4	1	Same
PVC5	1	Same
PVC6	1	Same
PVC7	1	Same
PVC8	1	Same
EthernetWAN	1	Same

This completes the 802.1Q/1P setup.

17.2 The 802.1Q/1P Group Setting Screen

Use this screen to activate 802.1Q/1P and display the VLAN groups. Click **Advanced > 802.1Q/1P** to display the following screen.

Figure 193 Advanced > 802.1Q/1P > Group Setting



802.1Q/1P

Active □

Management Vlan ID 1

Summary

#	Name	VID	Port Number									Modify
			LAN1	LAN3	SSID1	SSID3	PVC1	PVC3	PVC5	PVC7	EthernetWAN	
			LAN2	LAN4	SSID2	SSID4	PVC2	PVC4	PVC6	PVC8	-	
1	Default	1	U	U	U	U	U	U	U	U	U	
			U	U	U	U	U	U	U	U	-	
2	-	-	-	-	-	-	-	-	-	-	-	
			-	-	-	-	-	-	-	-	-	
3	-	-	-	-	-	-	-	-	-	-	-	
			-	-	-	-	-	-	-	-	-	
4	-	-	-	-	-	-	-	-	-	-	-	
			-	-	-	-	-	-	-	-	-	
5	-	-	-	-	-	-	-	-	-	-	-	
			-	-	-	-	-	-	-	-	-	
6	-	-	-	-	-	-	-	-	-	-	-	
			-	-	-	-	-	-	-	-	-	
7	-	-	-	-	-	-	-	-	-	-	-	
			-	-	-	-	-	-	-	-	-	
8	-	-	-	-	-	-	-	-	-	-	-	
			-	-	-	-	-	-	-	-	-	
9	-	-	-	-	-	-	-	-	-	-	-	
			-	-	-	-	-	-	-	-	-	
10	-	-	-	-	-	-	-	-	-	-	-	
			-	-	-	-	-	-	-	-	-	
11	-	-	-	-	-	-	-	-	-	-	-	
			-	-	-	-	-	-	-	-	-	
12	-	-	-	-	-	-	-	-	-	-	-	
			-	-	-	-	-	-	-	-	-	

The following table describes the labels in this screen.

Table 104 Advanced > 802.1Q/1P > Group Setting

LABEL	DESCRIPTION
802.1P/1Q	
Active	Select this check box to activate the 802.1P/1Q feature.
Management Vlan ID	Enter the ID number of a VLAN group. All interfaces (ports, SSIDs and PVCs) are in the management VLAN by default. If you disable the management VLAN, you will not be able to access the ZyXEL Device.

Table 104 Advanced > 802.1Q/1P > Group Setting (continued)

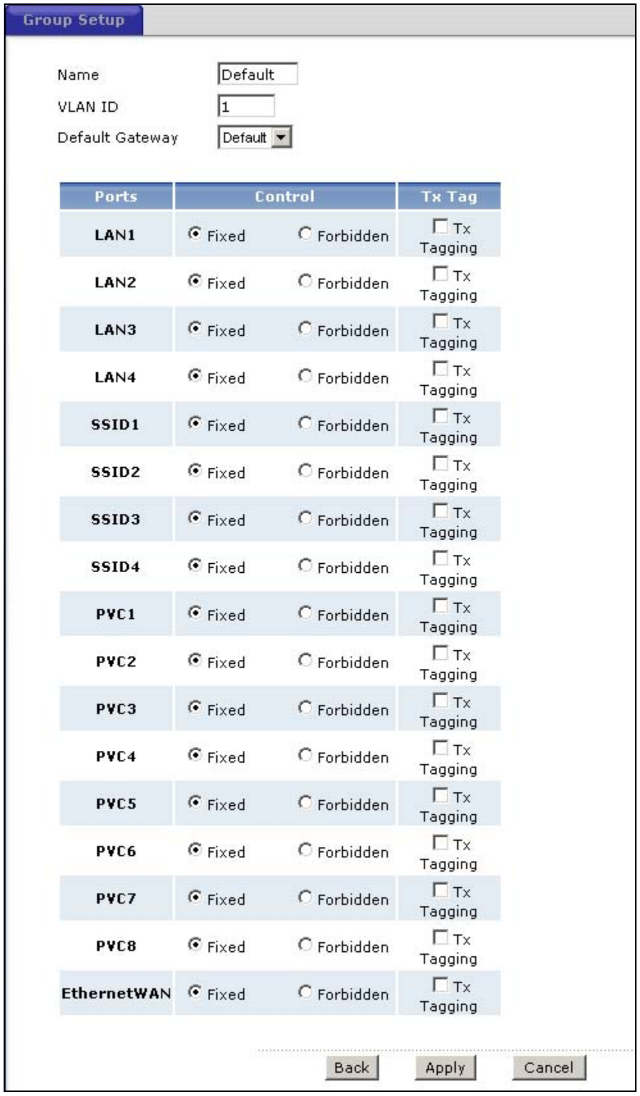
LABEL	DESCRIPTION
Summary	
#	This field displays the index number of the VLAN group.
Name	This field displays the name of the VLAN group.
VID	This field displays the ID number of the VLAN group.
Port Number	These columns display the VLAN's settings for each port. A tagged port is marked as **T**, an untagged port is marked as **U** and ports not participating in a VLAN are marked as "**–**".
Modify	Click the **Edit** button to configure the ports in the VLAN group. Click the **Remove** button to delete the VLAN group.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

17.2.1 Editing 802.1Q/1P Group Setting

Use this screen to configure the settings for each VLAN group.

In the **802.1Q/1P** screen, click the **Edit** button from the **Modify** filed to display the following screen.

Figure 194 Advanced > 802.1Q/1P > Group Setting > Edit



Name	Default
VLAN ID	1
Default Gateway	Default

Ports	Control		Tx Tag
LAN1	● Fixed	○ Forbidden	□ Tx Tagging
LAN2	● Fixed	○ Forbidden	□ Tx Tagging
LAN3	● Fixed	○ Forbidden	□ Tx Tagging
LAN4	● Fixed	○ Forbidden	□ Tx Tagging
SSID1	● Fixed	○ Forbidden	□ Tx Tagging
SSID2	● Fixed	○ Forbidden	□ Tx Tagging
SSID3	● Fixed	○ Forbidden	□ Tx Tagging
SSID4	● Fixed	○ Forbidden	□ Tx Tagging
PVC1	● Fixed	○ Forbidden	□ Tx Tagging
PVC2	● Fixed	○ Forbidden	□ Tx Tagging
PVC3	● Fixed	○ Forbidden	□ Tx Tagging
PVC4	● Fixed	○ Forbidden	□ Tx Tagging
PVC5	● Fixed	○ Forbidden	□ Tx Tagging
PVC6	● Fixed	○ Forbidden	□ Tx Tagging
PVC7	● Fixed	○ Forbidden	□ Tx Tagging
PVC8	● Fixed	○ Forbidden	□ Tx Tagging
EthernetWAN	● Fixed	○ Forbidden	□ Tx Tagging

The following table describes the labels in this screen.

Table 105 Advanced > 802.1Q/1P > Group Setting > Edit

LABEL	DESCRIPTION
Name	Enter a descriptive name for the VLAN group for identification purposes. The text may consist of up to 8 letters, numerals, “-”, “_” and “@”.
VLAN ID	Assign a VLAN ID for the VLAN group. The valid VID range is between 1 and 4094.
Default Gateway	Select the default gateway for the VLAN group.
Ports	This field displays the types of ports available to join the VLAN group.

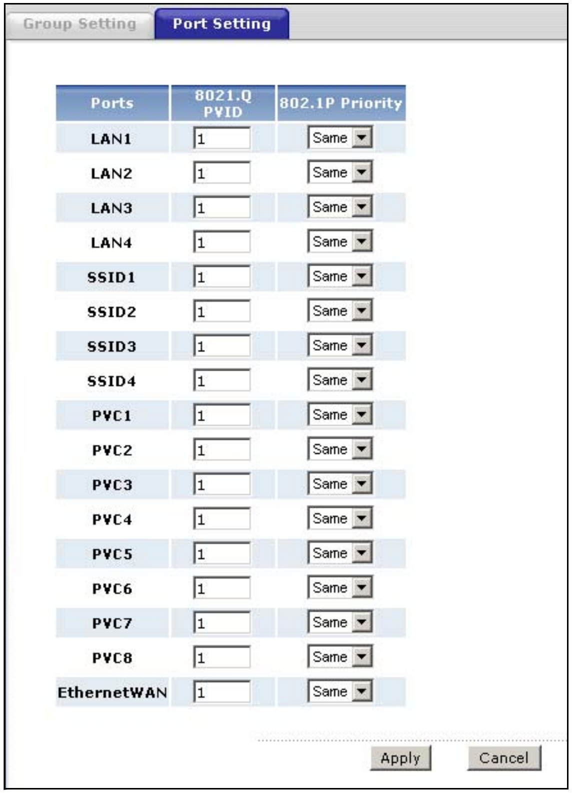
Table 105 Advanced > 802.1Q/1P > Group Setting > Edit (continued)

LABEL	DESCRIPTION
Control	Select **Fixed** for the port to be a permanent member of the VLAN group. Select **Forbidden** if you want to prohibit the port from joining the VLAN group.
Tx Tag	Select **Tx Tagging** if you want the port to tag all outgoing traffic transmitted through this VLAN. You select this if you want to create VLANs across different devices and not just the ZyXEL Device.
Back	Click this to return to the previous screen without saving.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

17.3 The 802.1Q/1P Port Setting Screen

Use this screen to configure the PVID and assign traffic priority for each port. Click **Advanced** > **802.1Q/1P** > **Port Setting** to display the following screen.

Figure 195 Advanced > 802.1Q/1P > Port Setting



Ports	8021.Q PVID	802.1P Priority
LAN1	1	Same
LAN2	1	Same
LAN3	1	Same
LAN4	1	Same
SSID1	1	Same
SSID2	1	Same
SSID3	1	Same
SSID4	1	Same
PVC1	1	Same
PVC2	1	Same
PVC3	1	Same
PVC4	1	Same
PVC5	1	Same
PVC6	1	Same
PVC7	1	Same
PVC8	1	Same
EthernetWAN	1	Same

The following table describes the labels in this screen.

Table 106 Advanced > 802.1Q/1P > Port Setting

LABEL	DESCRIPTION
Ports	This field displays the types of ports available to join the VLAN group.
802.1Q PVID	Assign a VLAN ID for the port. The valid VID range is between 1 and 4094. The ZyXEL Device assigns the PVID to untagged frames or priority-tagged frames received on this port, SSID, or PVC.
802.1P Priority	Assign a priority for the traffic transmitted through the port, SSID, or PVC. Select **Same** if you do not want to modify the priority. You may choose a priority level from **0-7**, with 0 being the lowest level and 7 being the highest level.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

18

Quality of Service (QoS)

This chapter contains information about configuring QoS, editing classifiers and viewing the ZyXEL Device's QoS packet statistics.

18.1 Overview

This chapter discusses the ZyXEL Device's **QoS** screens. Use these screens to set up your ZyXEL Device to use QoS for traffic management.

Quality of Service (QoS) refers to both a network's ability to deliver data with minimum delay, and the networking methods used to control the use of bandwidth. QoS allows the ZyXEL Device to group and prioritize application traffic and fine-tune network performance.

Without QoS, all traffic data is equally likely to be dropped when the network is congested. This can cause a reduction in network performance and make the network inadequate for time-critical application such as video-on-demand.

The ZyXEL Device assigns each packet a priority and then queues the packet accordingly. Packets assigned a high priority are processed more quickly than those with low priority if there is congestion, allowing time-sensitive applications to flow more smoothly. Time-sensitive applications include both those that require a low level of latency (delay) and a low level of jitter (variations in delay) such as Voice over IP (VoIP) or Internet gaming, and those for which jitter alone is a problem such as Internet radio or streaming video.

- See Section 18.5 on page 341 for advanced technical information on SIP.

18.1.1 What You Can Do in the QoS Screens

- Use the **General** screen (Section 18.2 on page 333) to enable QoS on the ZyXEL Device, decide allowable bandwidth using QoS and configure priority mapping settings for traffic that does not match a custom class.
- Use the **Class Setup** screen (Section 18.3 on page 335) to set up classifiers to sort traffic into different flows and assign priority and define actions to be performed for a classified traffic flow.

- Use the **Monitor** screen (Section 18.4 on page 341) to view the ZyXEL Device's QoS-related packet statistics.

18.1.2 What You Need to Know About QoS

QoS versus Cos

QoS is used to prioritize source-to-destination traffic flows. All packets in the same flow are given the same priority. CoS (class of service) is a way of managing traffic in a network by grouping similar types of traffic together and treating each type as a class. You can use CoS to give different priorities to different packet types.

CoS technologies include IEEE 802.1p layer 2 tagging and DiffServ (Differentiated Services or DS). IEEE 802.1p tagging makes use of three bits in the packet header, while DiffServ is a new protocol and defines a new DS field, which replaces the eight-bit ToS (Type of Service) field in the IP header.

Tagging and Marking

In a QoS class, you can configure whether to add or change the DSCP (DiffServ Code Point) value, IEEE 802.1p priority level and VLAN ID number in a matched packet. When the packet passes through a compatible network, the networking device, such as a backbone switch, can provide specific treatment or service based on the tag or marker.

18.1.3 QoS Class Setup Example

In the following figure, your Internet connection has an upstream transmission speed of 50 Mbps. You configure a classifier to assign the highest priority queue (6) to VoIP traffic from the LAN interface, so that voice traffic would not get delayed when there is network congestion. Traffic from the boss's IP address (192.168.1.23 for example) is mapped to queue 5. Traffic that does not match these two classes are assigned priority queue based on the internal QoS mapping table on the ZyXEL Device.

Figure 196 QoS Example

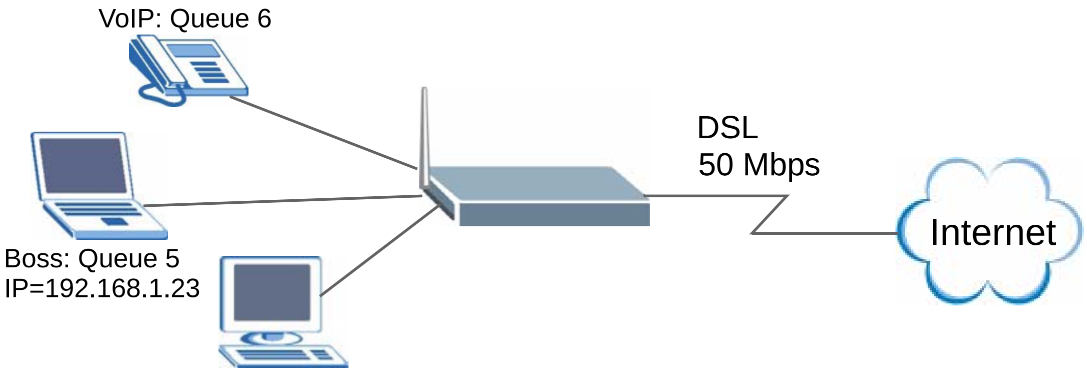
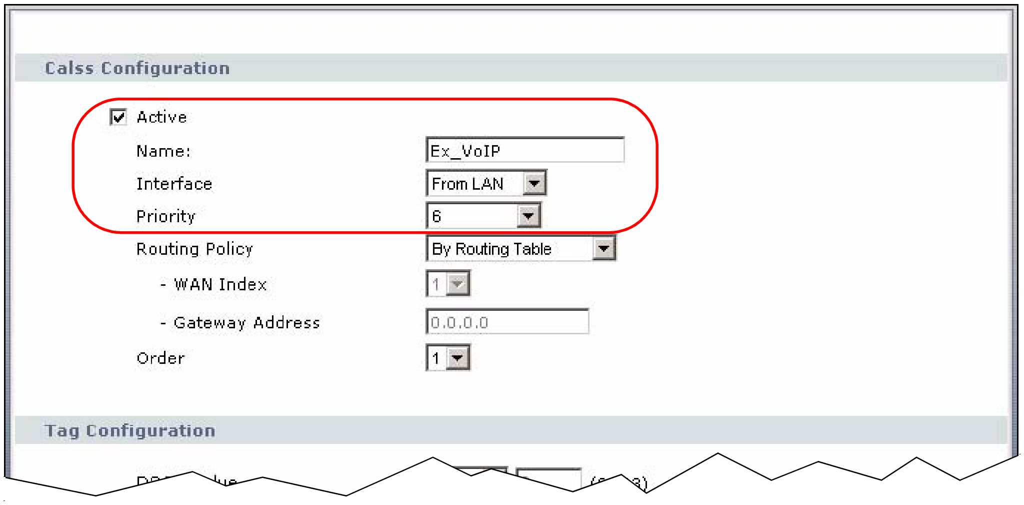


Figure 197 QoS Class Example: VoIP -1



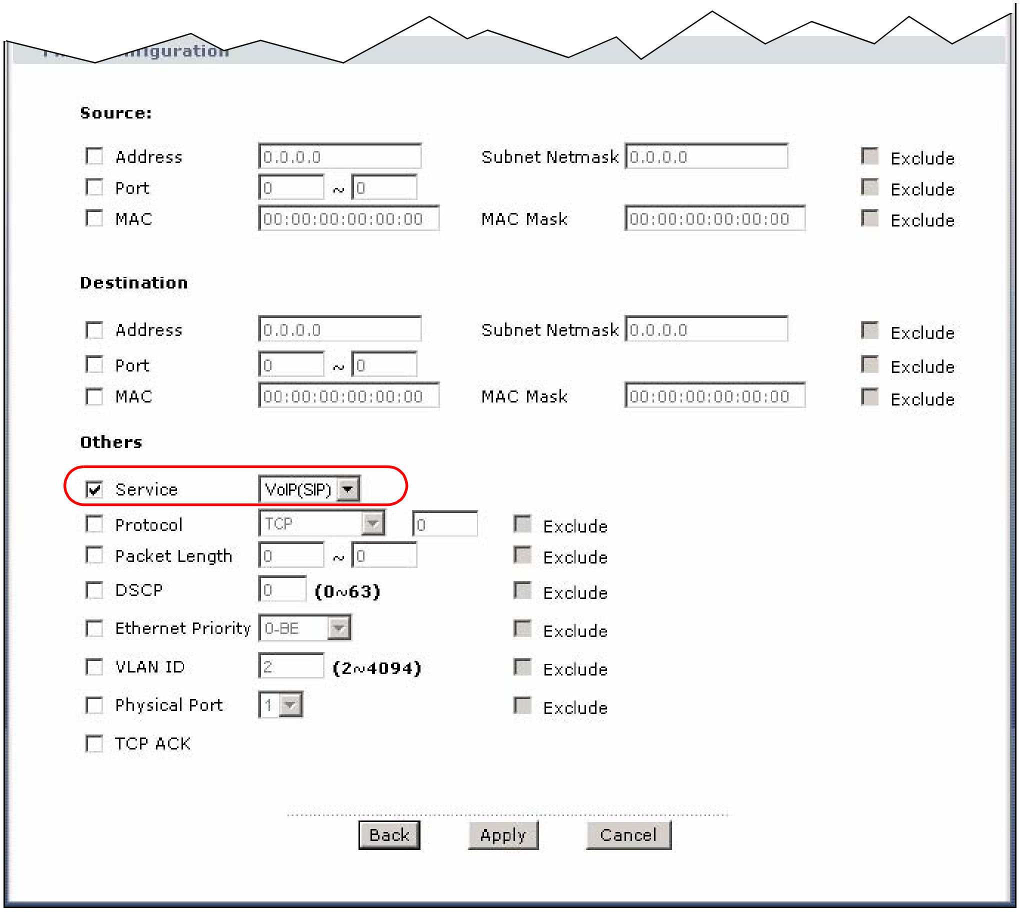
Calss Configuration

☑ Active

Name:	Ex_VoIP
Interface	From LAN
Priority	6
Routing Policy	By Routing Table
- WAN Index	1
- Gateway Address	0.0.0.0
Order	1

Tag Configuration

Figure 198 QoS Class Example: VoIP -2



Source:

☐ Address	0.0.0.0	Subnet Netmask	0.0.0.0	☐ Exclude
☐ Port	0 ~ 0			☐ Exclude
☐ MAC	00:00:00:00:00:00	MAC Mask	00:00:00:00:00:00	☐ Exclude

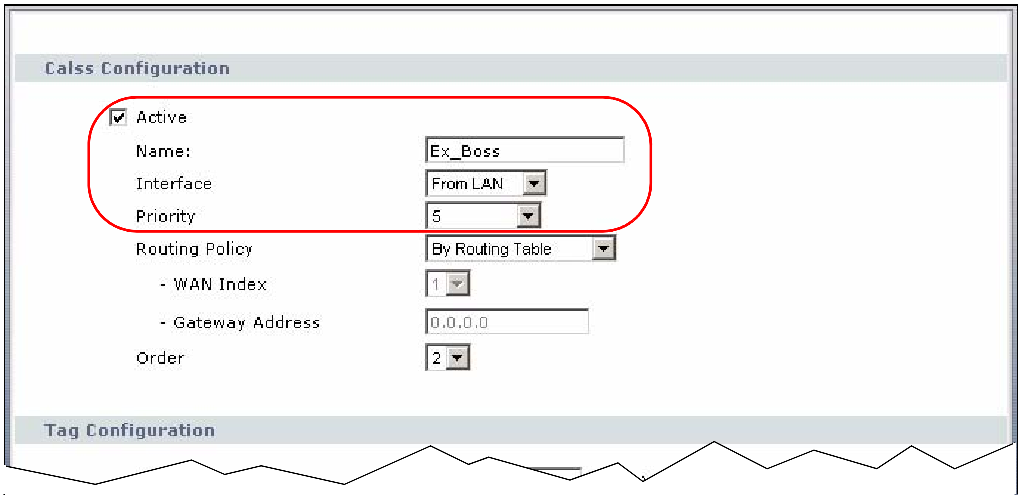
Destination

☐ Address	0.0.0.0	Subnet Netmask	0.0.0.0	☐ Exclude
☐ Port	0 ~ 0			☐ Exclude
☐ MAC	00:00:00:00:00:00	MAC Mask	00:00:00:00:00:00	☐ Exclude

Others

☑ Service	VoIP(SIP)	
☐ Protocol	TCP 0	☐ Exclude
☐ Packet Length	0 ~ 0	☐ Exclude
☐ DSCP	0 **(0~63)**	☐ Exclude
☐ Ethernet Priority	0-BE	☐ Exclude
☐ VLAN ID	2 **(2~4094)**	☐ Exclude
☐ Physical Port	1	☐ Exclude
☐ TCP ACK		

Figure 199 QoS Class Example: Boss -1

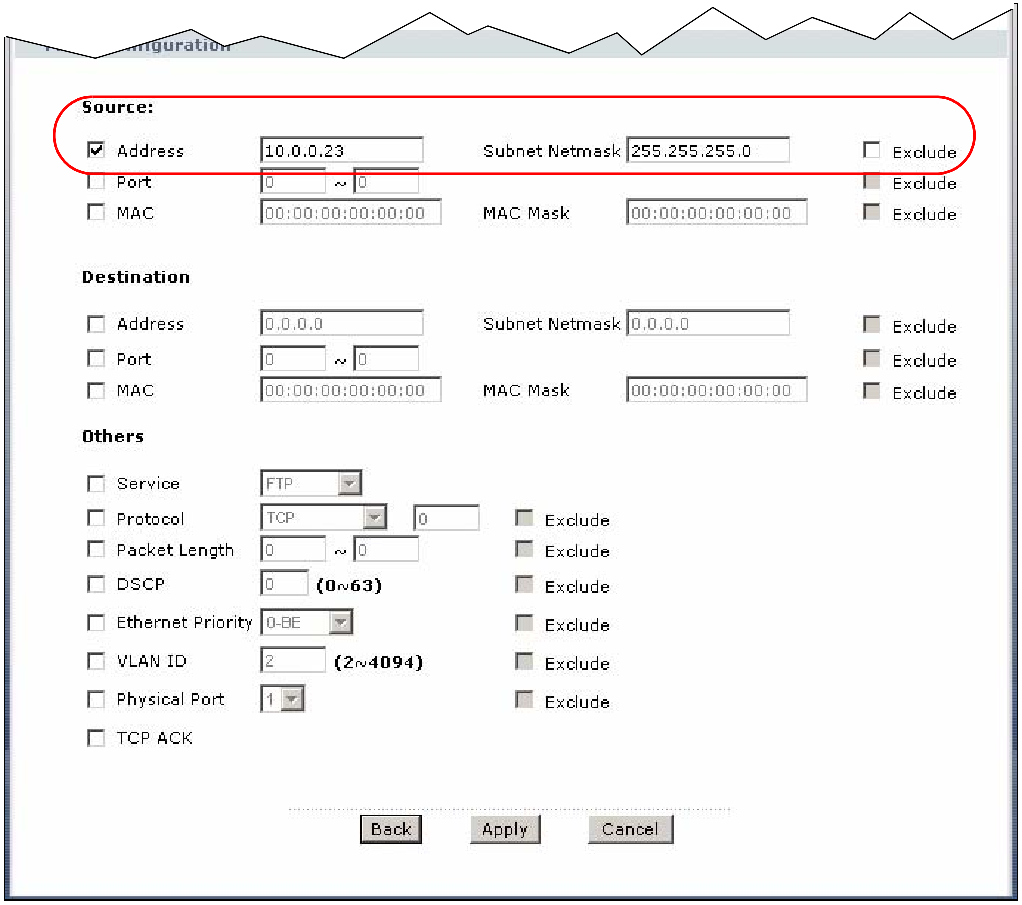


Calss Configuration

☑ Active	
Name:	Ex_Boss
Interface	From LAN
Priority	5
Routing Policy	By Routing Table
- WAN Index	1
- Gateway Address	0.0.0.0
Order	2

Tag Configuration

Figure 200 QoS Class Example: Boss -2



Source:

☑ Address	10.0.0.23	Subnet Netmask	255.255.255.0	□ Exclude
□ Port	0 ~ 0			□ Exclude
□ MAC	00:00:00:00:00:00	MAC Mask	00:00:00:00:00:00	□ Exclude

Destination

□ Address	0.0.0.0	Subnet Netmask	0.0.0.0	□ Exclude
□ Port	0 ~ 0			□ Exclude
□ MAC	00:00:00:00:00:00	MAC Mask	00:00:00:00:00:00	□ Exclude

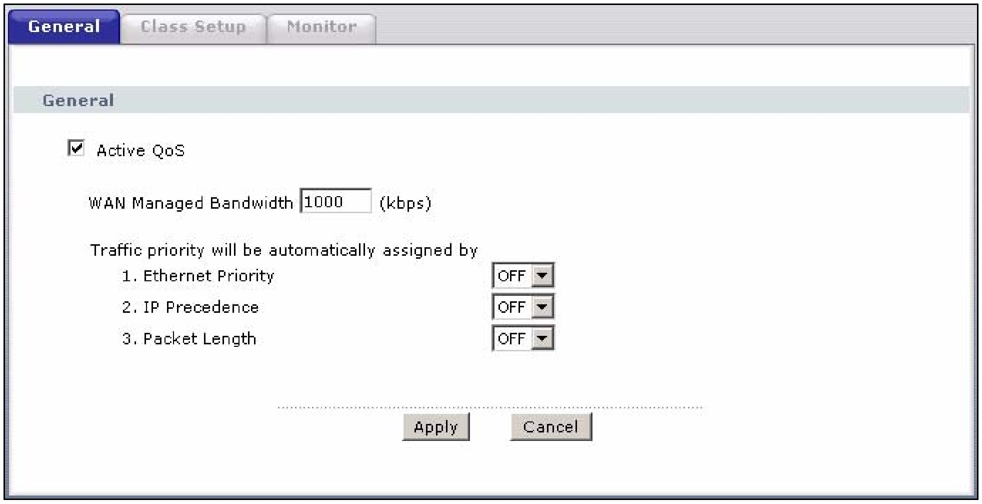
Others

□ Service	FTP		
□ Protocol	TCP	0	□ Exclude
□ Packet Length	0 ~ 0		□ Exclude
□ DSCP	0	**(0~63)**	□ Exclude
□ Ethernet Priority	0-BE		□ Exclude
□ VLAN ID	2	**(2~4094)**	□ Exclude
□ Physical Port	1		□ Exclude
□ TCP ACK			

18.2 The QoS General Screen

Click **Advanced > QoS** to open the screen as shown next. Use this screen to enable or disable QoS, and select to have the ZyXEL Device automatically assign priority to traffic according to the IEEE 802.1p priority level, IP precedence and/or packet length.

Figure 201 Advanced > QoS > General



☑ Active QoS

WAN Managed Bandwidth 1000 (kbps)

Traffic priority will be automatically assigned by
1. Ethernet Priority OFF
2. IP Precedence OFF
3. Packet Length OFF

The following table describes the labels in this screen.

Table 107 Advanced > QoS > General

LABEL	DESCRIPTION
Active QoS	Select the check box to turn on QoS to improve your network performance. You can give priority to traffic that the ZyXEL Device forwards out through the WAN interface. Give high priority to voice and video to make them run more smoothly. Similarly, give low priority to many large file downloads so that they do not reduce the quality of other applications.
WAN Managed Bandwidth	Enter the amount of bandwidth for the WAN interface that you want to allocate using QoS. The recommendation is to set this speed to match the interface’s actual transmission speed. For example, set the WAN interface speed to 100000 kbps if your Internet connection has an upstream transmission speed of 100 Mbps. Setting this number higher than the interface’s actual transmission speed will stop lower priority traffic from being sent if higher priority traffic uses all of the actual bandwidth. If you set this number lower than the interface’s actual transmission speed, the ZyXEL Device will not use some of the interface’s available bandwidth.
Traffic priority will be automatically assigned by	These fields are ignored if traffic matches a class you configured in the **Class Setup** screen. If you select **ON** and traffic does not match a class configured in the **Class Setup** screen, the ZyXEL Device assigns priority to unmatched traffic based on the IEEE 802.1p priority level, IP precedence and/or packet length. See Section 18.5.4 on page 343 for more information. If you select **OFF**, traffic which does not match a class is mapped to queue two.

Table 107 Advanced > QoS > General

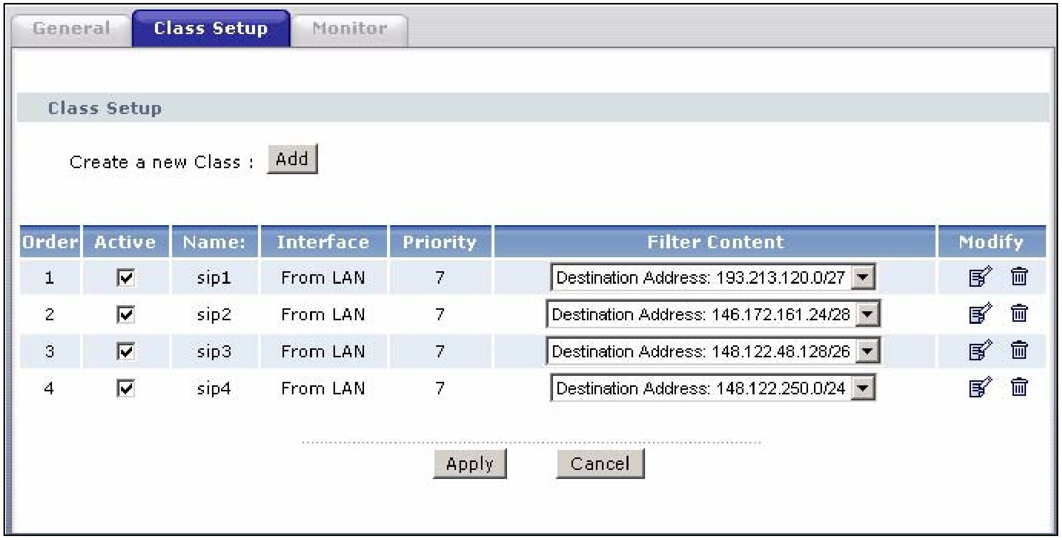
LABEL	DESCRIPTION
Apply	Click **Apply** to save your settings back to the ZyXEL Device.
Cancel	Click **Cancel** to begin configuring this screen afresh.

18.3 The Class Setup Screen

Use this screen to add, edit or delete classifiers. A classifier groups traffic into data flows according to specific criteria such as the source address, destination address, source port number, destination port number or incoming interface. For example, you can configure a classifier to select traffic from the same protocol port (such as Telnet) to form a flow.

Click **Advanced > QoS > Class Setup** to open the following screen.

Figure 202 Advanced > QoS > Class Setup



Class Setup

Create a new Class : Add

Order	Active	Name:	Interface	Priority	Filter Content	Modify
1	☑	sip1	From LAN	7	Destination Address: 193.213.120.0/27	
2	☑	sip2	From LAN	7	Destination Address: 146.172.161.24/28	
3	☑	sip3	From LAN	7	Destination Address: 148.122.48.128/26	
4	☑	sip4	From LAN	7	Destination Address: 148.122.250.0/24	

The following table describes the labels in this screen.

Table 108 Advanced > QoS > Class Setup

LABEL	DESCRIPTION
Create a new Class	Click **Add** to create a new classifier.
Order	This is the number of each classifier. The ordering of the classifiers is important as the classifiers are applied in turn.
Active	Select the check box to enable this classifier.
Name	This is the name of the classifier.
Interface	This shows the interface from which traffic of this classifier should come.

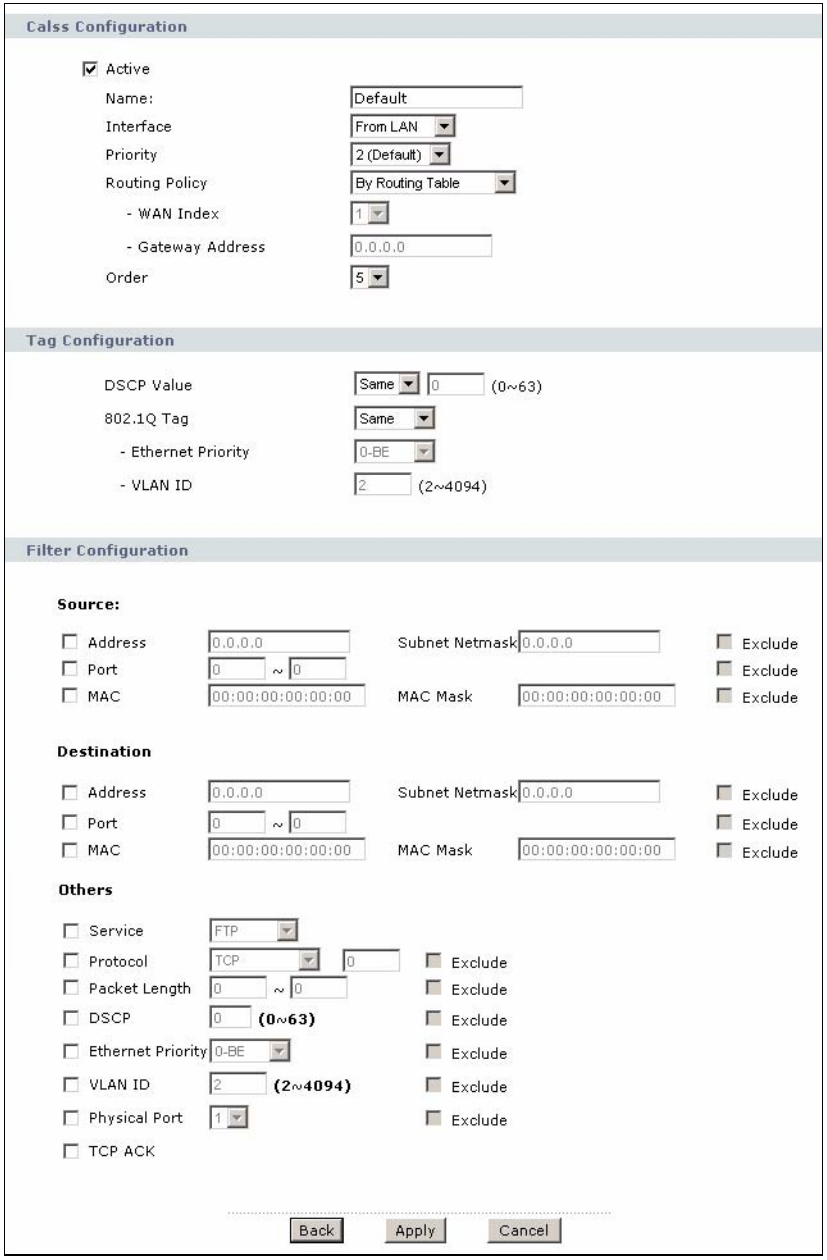
Table 108 Advanced > QoS > Class Setup (continued)

LABEL	DESCRIPTION
Priority	This is the priority assigned to traffic of this classifier.
Filter Content	This shows criteria specified in this classifier.
Modify	Click the Edit icon to go to the screen where you can edit the classifier. Click the Remove icon to delete an existing classifier.
Apply	Click **Apply** to save your changes back to the ZyXEL Device.
Cancel	Click **Cancel** to begin configuring this screen afresh.

18.3.1 The Class Configuration Screen

Click the **Add** button or the **Edit** icon in the **Modify** field to configure a classifier.

Figure 203 Advanced > QoS > Class Setup > Add



Calss Configuration

☑ Active

Name:	Default
Interface	From LAN
Priority	2 (Default)
Routing Policy	By Routing Table
- WAN Index	1
- Gateway Address	0.0.0.0
Order	5

Tag Configuration

DSCP Value	Same 0 (0~63)
802.1Q Tag	Same
- Ethernet Priority	0-BE
- VLAN ID	2 (2~4094)

Filter Configuration

Source:

□ Address	0.0.0.0	Subnet Netmask	0.0.0.0	□ Exclude
□ Port	0 ~ 0			□ Exclude
□ MAC	00:00:00:00:00:00	MAC Mask	00:00:00:00:00:00	□ Exclude

Destination

□ Address	0.0.0.0	Subnet Netmask	0.0.0.0	□ Exclude
□ Port	0 ~ 0			□ Exclude
□ MAC	00:00:00:00:00:00	MAC Mask	00:00:00:00:00:00	□ Exclude

Others

□ Service	FTP	
□ Protocol	TCP 0	□ Exclude
□ Packet Length	0 ~ 0	□ Exclude
□ DSCP	0 **(0~63)**	□ Exclude
□ Ethernet Priority	0-BE	□ Exclude
□ VLAN ID	2 **(2~4094)**	□ Exclude
□ Physical Port	1	□ Exclude
□ TCP ACK		

See Appendix E on page 557 for a list of commonly-used services. The following table describes the labels in this screen.

Table 109 Advanced > QoS > Class Setup > Add

LABEL	DESCRIPTION
Class Configuration	
Active	Select the check box to enable this classifier.
Name	Enter a descriptive name of up to 20 printable English keyboard characters, including spaces.
Interface	Select from which interface traffic of this class should come.
Priority	Select a priority level (between 0 and 7) or select **Auto** to have the ZyXEL Device map the matched traffic to a queue according to the internal QoS mapping table. See Section 18.5.4 on page 343 for more information. "0" is the lowest priority level and "7" is the highest.
Routing Policy	Select the next hop to which traffic of this class should be forwarded. Select **By Routing Table** to have the ZyXEL Device use the routing table to find a next hop and forward the matched packets automatically. Select **To Gateway Address** to route the matched packets to the router or switch you specified in the **Gateway Address** field.
WAN Index	This field in not configurable at the time of writing.
Gateway Address	Enter the IP address of the gateway, which should be a router or switch on the same segment as the ZyXEL Device’s interface(s), that can forward the packet to the destination.
Order	This shows the ordering number of this classifier. Select an existing number for where you want to put this classifier and click **Apply** to move the classifier to the number you selected. For example, if you select 2, the classifier you are moving becomes number 2 and the previous classifier 2 gets pushed down one.
Tag Configuration	
DSCP Value	Select **Same** to keep the DSCP fields in the packets. Select **Auto** to map the DSCP value to 802.1 priority level automatically. Select **Mark** to set the DSCP field with the value you configure in the field provided.

Table 109 Advanced > QoS > Class Setup > Add (continued)

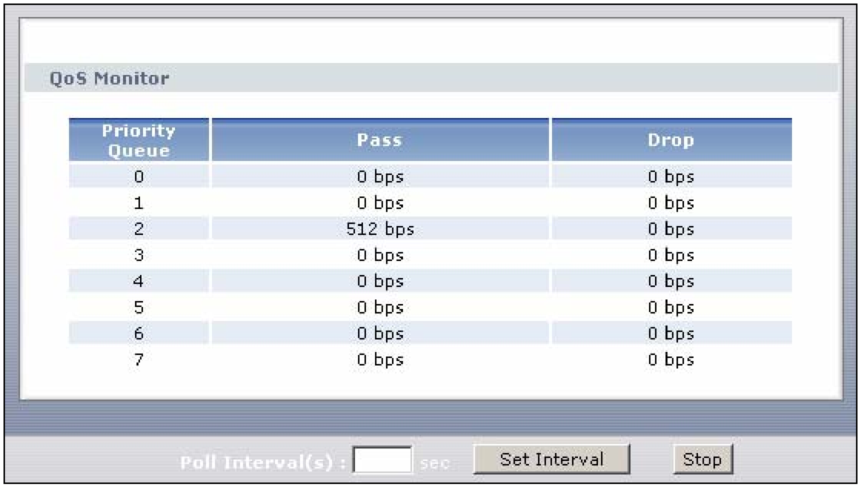
LABEL	DESCRIPTION
802.1Q Tag	Select **Same** to keep the priority setting and VLAN ID of the frames. Select **Auto** to map the 802.1 priority level to the DSCP value automatically. Select **Remove** to delete the priority queue tag and VLAN ID of the frames. Select **Mark** to replace the 802.1 priority field and VLAN ID with the value you set in the fields below. Select **Add** to treat all matched traffic untagged and add a second priority queue tag and VLAN.
Ethernet Priority	Select a priority level (between 0 and 7) from the drop down list box.
VLAN ID	Specify a VLAN ID number between 2 and 4094.
Filter Configuration	Use the following fields to configure the criteria for traffic classification.
Source	
Address	Select the check box and enter the source IP address in dotted decimal notation. A blank source IP address means any source IP address.
Subnet Netmask	Enter the source subnet mask. Refer to the appendix for more information on IP subnetting.
Port	Select the check box and enter the port number of the source. 0 means any source port number. See *Appendix E on page 557* for some common services and port numbers.
MAC	Select the check box and enter the source MAC address of the packet.
MAC Mask	Type the mask for the specified MAC address to determine which bits a packet's MAC address should match. Enter "f" for each bit of the specified source MAC address that the traffic's MAC address should match. Enter "0" for the bit(s) of the matched traffic's MAC address, which can be of any hexadecimal character(s). For example, if you set the MAC address to 00:13:49:00:00:00 and the mask to ff:ff:ff:00:00:00, a packet with a MAC address of 00:13:49:12:34:56 matches this criteria.
Exclude	Select this option to exclude the packets that match the specified criteria from this classifier.
Destination	
Address	Select the check box and enter the destination IP address in dotted decimal notation.
Subnet Netmask	Enter the destination subnet mask. Refer to the appendix for more information on IP subnetting.
Port	Select the check box and enter the port number of the destination. 0 means any source port number. See *Appendix E on page 557* for some common services and port numbers.
MAC	Select the check box and enter the destination MAC address of the packet.

Table 109 Advanced > QoS > Class Setup > Add (continued)

LABEL	DESCRIPTION
MAC Mask	Type the mask for the specified MAC address to determine which bits a packet's MAC address should match. Enter “f” for each bit of the specified destination MAC address that the traffic's MAC address should match. Enter “0” for the bit(s) of the matched traffic's MAC address, which can be of any hexadecimal character(s). For example, if you set the MAC address to 00:13:49:00:00:00 and the mask to ff:ff:ff:00:00:00, a packet with a MAC address of 00:13:49:12:34:56 matches this criteria.
Exclude	Select this option to exclude the packets that match the specified criteria from this classifier.
Others	
Service	This field simplifies classifier configuration by allowing you to select a predefined application. When you select a predefined application, you do not configure the rest of the filter fields. SIP (Session Initiation Protocol) is a signaling protocol used in Internet telephony, instant messaging and other VoIP (Voice over IP) applications. Select the check box and select **VoIP(SIP)** from the drop-down list box to configure this classifier for traffic that uses SIP. 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. Select the check box and select **FTP** from the drop-down list box to configure this classifier for FTP traffic.
Protocol	Select this option and select the protocol (**TCP** or **UDP**) or select **User defined** and enter the protocol (service type) number. 0 means any protocol number.
Packet Length	Select this option and enter the minimum and maximum packet length (from 28 to 1500) in the fields provided.
DSCP	Select this option and specify a DSCP (DiffServ Code Point) number between 0 and 63 in the field provided.
Ethernet Priority	Select this option and select a priority level (between 0 and 7) from the drop down list box. "0" is the lowest priority level and "7" is the highest.
VLAN ID	Select this option and specify a VLAN ID number between 2 and 4094.
Physical Port	Select this option and select a LAN port.
Exclude	Select this option to exclude the packets that match the specified criteria from this classifier.
TCP ACK	Select this option to set this classifier for TCP ACK (acknowledgement) packets.
Back	Click **Back** to go to the previous screen.
Apply	Click **Apply** to save your changes back to the ZyXEL Device.
Cancel	Click **Cancel** to begin configuring this screen afresh.

18.4 The QoS Monitor Screen

To view the ZyXEL Device's QoS packet statistics, click **Advanced > QoS > Monitor**. The screen appears as shown.



QoS Monitor

Priority Queue	Pass	Drop
0	0 bps	0 bps
1	0 bps	0 bps
2	512 bps	0 bps
3	0 bps	0 bps
4	0 bps	0 bps
5	0 bps	0 bps
6	0 bps	0 bps
7	0 bps	0 bps

Figure 204 Advanced > QoS > Monitor

The following table describes the labels in this screen.

Table 110 Advanced > QoS > Monitor

LABEL	DESCRIPTION
Priority Queue	This shows the priority queue number. Traffic assigned to higher index queues gets through faster while traffic in lower index queues is dropped if the network is congested.
Pass	This shows how many packets mapped to this priority queue are transmitted successfully.
Drop	This shows how many packets mapped to this priority queue are dropped.
Poll Interval(s)	Enter the time interval for refreshing statistics in this field.
Set Interval	Click this button to apply the new poll interval you entered in the **Poll Interval(s)** field.
Stop	Click **Stop** to stop refreshing statistics.

18.5 QoS Technical Reference

This section provides some technical background information about the topics covered in this chapter.

18.5.1 IEEE 802.1Q Tag

The IEEE 802.1Q standard defines an explicit VLAN tag in the MAC header to identify the VLAN membership of a frame across bridges. A VLAN tag includes the 12-bit VLAN ID and 3-bit user priority. The VLAN ID associates a frame with a specific VLAN and provides the information that devices need to process the frame across the network.

IEEE 802.1p specifies the user priority field and defines up to eight separate traffic types. The following table describes the traffic types defined in the IEEE 802.1d standard (which incorporates the 802.1p).

Table 111 IEEE 802.1p Priority Level and Traffic Type

PRIORITY LEVEL	TRAFFIC TYPE
Level 7	Typically used for network control traffic such as router configuration messages.
Level 6	Typically used for voice traffic that is especially sensitive to jitter (jitter is the variations in delay).
Level 5	Typically used for video that consumes high bandwidth and is sensitive to jitter.
Level 4	Typically used for controlled load, latency-sensitive traffic such as SNA (Systems Network Architecture) transactions.
Level 3	Typically used for “excellent effort” or better than best effort and would include important business traffic that can tolerate some delay.
Level 2	This is for “spare bandwidth”.
Level 1	This is typically used for non-critical “background” traffic such as bulk transfers that are allowed but that should not affect other applications and users.
Level 0	Typically used for best-effort traffic.

18.5.2 IP Precedence

Similar to IEEE 802.1p prioritization at layer-2, you can use IP precedence to prioritize packets in a layer-3 network. IP precedence uses three bits of the eight-bit ToS (Type of Service) field in the IP header. There are eight classes of services (ranging from zero to seven) in IP precedence. Zero is the lowest priority level and seven is the highest.

18.5.3 DiffServ

QoS is used to prioritize source-to-destination traffic flows. All packets in the flow are given the same priority. You can use CoS (class of service) to give different priorities to different packet types.

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

DSCP and Per-Hop Behavior

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

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

DSCP (6 bits)	Unused (2 bits)

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

18.5.4 Automatic Priority Queue Assignment

If you enable QoS on the ZyXEL Device, the ZyXEL Device can automatically base on the IEEE 802.1p priority level, IP precedence and/or packet length to assign priority to traffic which does not match a class.

The following table shows you the internal layer-2 and layer-3 QoS mapping on the ZyXEL Device. On the ZyXEL Device, traffic assigned to higher priority queues gets through faster while traffic in lower index queues is dropped if the network is congested.

Table 112 Internal Layer2 and Layer3 QoS Mapping

PRIORITY QUEUE	LAYER 2	LAYER 3		
	IEEE 802.1P USER PRIORITY (ETHERNET PRIORITY)	TOS (IP PRECEDENCE)	DSCP	IP PACKET LENGTH (BYTE)
0	1	0	000000	
1	2			
2	0	0	000000	>1100
3	3	1	001110 001100 001010 001000	250~1100
4	4	2	010110 010100 010010 010000	
5	5	3	011110 011100 011010 011000	<250
6	6	4	100110 100100 100010 100000	
		5	101110 101000	
7	7	6	110000 111000	
		7		

19

Dynamic DNS Setup

This chapter discusses how to configure your ZyXEL Device to use Dynamic DNS.

19.1 Overview

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 applications such as NetMeeting and CU-SeeMe). 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.

19.1.1 What You Can Do in the DDNS Screen

Use the **Dynamic DNS** screen (Section 19.2 on page 346) to enable DDNS and configure the DDNS settings on the ZyXEL Device.

19.1.2 What You Need To Know About DDNS

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.

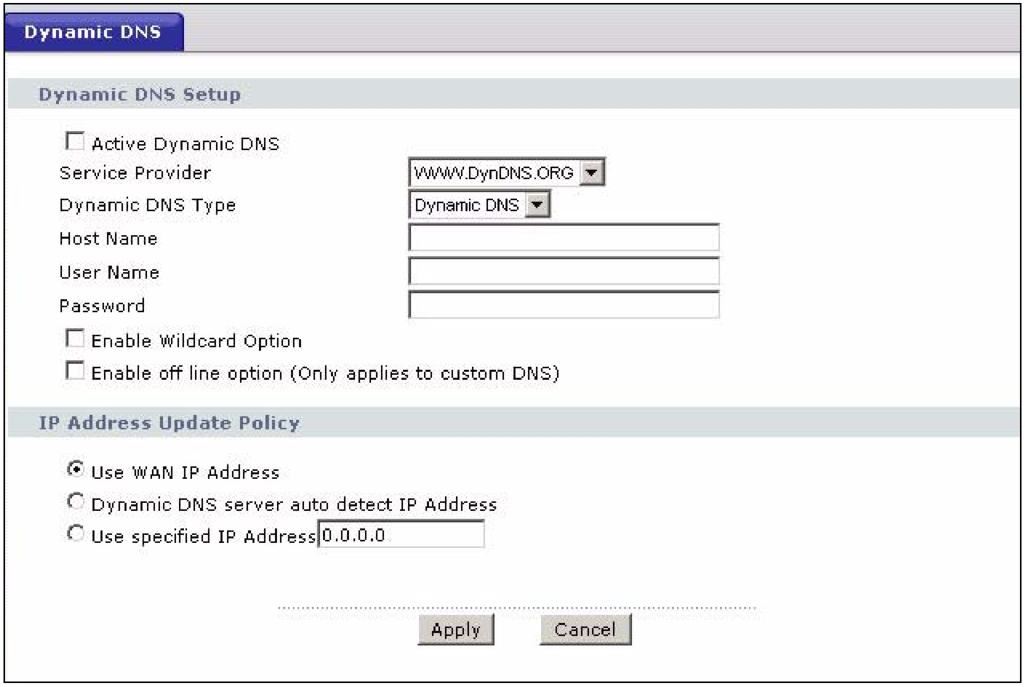
If you have a private WAN IP address, then you cannot use Dynamic DNS.

19.2 Configuring Dynamic DNS

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

See Section 19.1 on page 345 for more information.

Figure 205 Advanced > Dynamic DNS



Dynamic DNS

Dynamic DNS Setup

□ Active Dynamic DNS

Service Provider: WWW.DynDNS.ORG

Dynamic DNS Type: Dynamic DNS

Host Name:

User Name:

Password:

□ Enable Wildcard Option

□ Enable off line option (Only applies to custom DNS)

IP Address Update Policy

● Use WAN IP Address

○ Dynamic DNS server auto detect IP Address

○ Use specified IP Address 0.0.0.0

The following table describes the fields in this screen.

Table 113 Advanced > Dynamic DNS

LABEL	DESCRIPTION
Dynamic DNS Setup	
Active Dynamic DNS	Select this check box to use dynamic DNS.
Service Provider	This is the name of your Dynamic DNS service provider.
Dynamic DNS Type	Select the type of service that you are registered for from your Dynamic DNS service provider.
Host Name	Type the domain name assigned to your ZyXEL Device by your Dynamic DNS provider. You can specify up to two host names in the field separated by a comma (",").
User Name	Type your user name.
Password	Type the password assigned to you.

Table 113 Advanced > Dynamic DNS (continued)

LABEL	DESCRIPTION
Enable Wildcard Option	Select the check box to enable DynDNS Wildcard.
Enable off line option	This option is available when **CustomDNS** 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.
IP Address Update Policy	
Use WAN IP Address	Select this option to update the IP address of the host name(s) to the WAN IP address.
Dynamic DNS server auto detect IP Address	Select this option 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.
Use specified IP Address	Type the IP address of the host name(s). Use this if you have a static IP address.
Apply	Click **Apply** to save your changes back to the ZyXEL Device.
Cancel	Click **Cancel** to begin configuring this screen afresh.

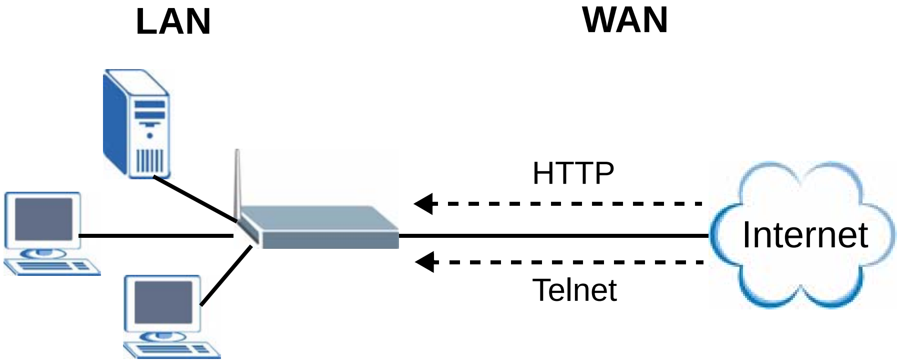
20

Remote Management Configuration

20.1 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 remote management of the ZyXEL Device coming in from the WAN.

Figure 206 Remote Management From the WAN



Note: When you configure remote management to allow management from the WAN, you still need to configure a firewall rule to allow access.

You may manage your ZyXEL Device from a remote location via:

- Internet (WAN only)
- ALL (LAN and WAN)
- LAN only,
- Neither (Disable).

Note: When you choose **WAN** only or **LAN & WAN**, you still need to configure a firewall rule to allow access.

To disable remote management of a service, select **Disable** in the corresponding **Access Status** field.

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. Telnet
2. HTTP

20.1.1 What You Can Do in the Remote Management Screens

- Use the **WWW** screen (Section 20.2 on page 351) to configure through which interface(s) and from which IP address(es) users can use HTTP to manage the ZyXEL Device.
- Use the **Telnet** screen (Section 20.3 on page 352) to configure through which interface(s) and from which IP address(es) users can use Telnet to manage the ZyXEL Device.
- Use the **FTP** screen (Section 20.4 on page 353) to configure through which interface(s) and from which IP address(es) users can use FTP to access the ZyXEL Device.
- Use the **SNMP** screen (Section 20.5 on page 354) to configure your ZyXEL Device's settings for Simple Network Management Protocol management.
- Use the **DNS** screen (Section 20.6 on page 357) to configure through which interface(s) and from which IP address(es) users can send DNS queries to the ZyXEL Device.
- Use the **ICMP** screen (Section 20.7 on page 358) to set whether or not your ZyXEL Device will respond to pings and probes for services that you have not made available.

20.1.2 What You Need to Know About Remote Management

Remote Management Limitations

Remote management does not work when:

- You have not enabled that service on the interface in the corresponding remote management screen.
- You have disabled that service in one of the remote management screens.
- The IP address in the **Secured Client IP** field does not match the client IP address. If it does not match, the ZyXEL Device will disconnect the session immediately.
- 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.
- There is a firewall rule that blocks it.

Remote Management and NAT

When NAT is enabled:

- Use the ZyXEL Device’s WAN IP address when configuring from the WAN.
- Use the ZyXEL Device’s LAN IP address when configuring from the LAN.

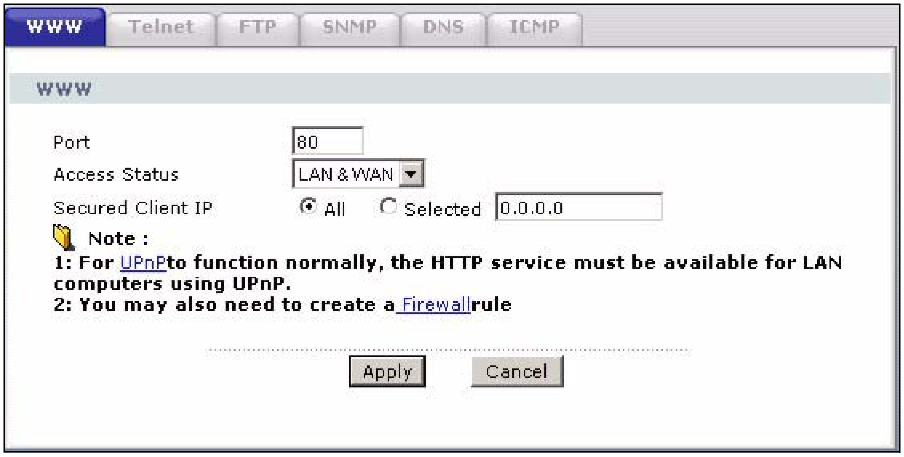
System Timeout

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.

20.2 The WWW Screen

To change your ZyXEL Device’s World Wide Web settings, click **Advanced > Remote MGMT** to display the **WWW** screen.

Figure 207 Advanced > Remote Management > WWW



WWW

Port	80
Access Status	LAN & WAN
Secured Client IP	● All ○ Selected 0.0.0.0

Note :

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

2: You may also need to create a Firewallrule

The following table describes the labels in this screen.

Table 114 Advanced > Remote Management > WWW

LABEL	DESCRIPTION
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.
Access Status	Select the interface(s) through which a computer may access the ZyXEL Device using this service.

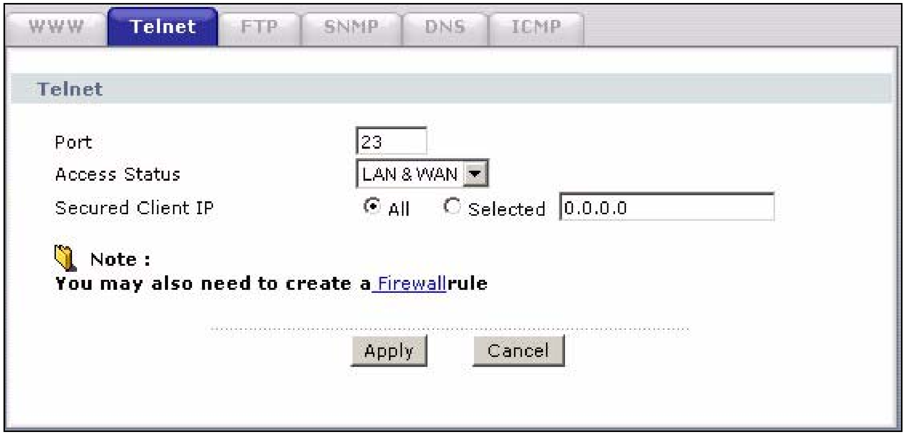
Table 114 Advanced > Remote Management > WWW

LABEL	DESCRIPTION
Secured Client IP	A secured 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 settings back to the ZyXEL Device.
Cancel	Click **Cancel** to begin configuring this screen afresh.

20.3 The Telnet Screen

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. Click **Advanced > Remote MGMT** > **Telnet** tab to display the screen as shown.

Figure 208 Advanced > Remote Management > Telnet



Port: 23
Access Status: LAN & WAN
Secured Client IP: ● 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 115 Advanced > Remote Management > Telnet

LABEL	DESCRIPTION
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.
Access Status	Select the interface(s) through which a computer may access the ZyXEL Device using this service.

Table 115 Advanced > Remote Management > Telnet

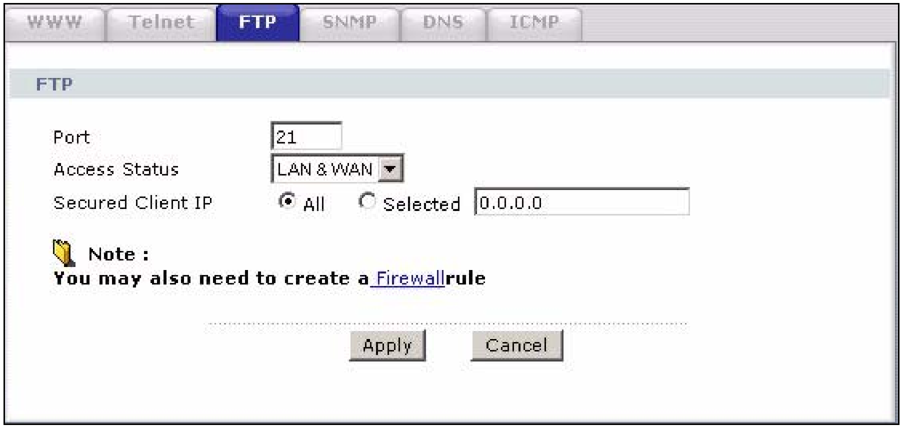
LABEL	DESCRIPTION
Secured Client IP	A secured client is a "trusted" computer that is allowed to communicate with the ZyXEL Device using this service. Select **All** to allow any computer to access the ZyXEL Device using this service. Choose **Selected** to just allow the computer with the IP address that you specify to access the ZyXEL Device using this service.
Apply	Click **Apply** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to begin configuring this screen afresh.

20.4 The FTP Screen

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.

Figure 209 Advanced > Remote Management > FTP



Port: 21

Access Status: LAN & WAN

Secured Client IP: ● 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 116 Advanced > Remote Management > FTP

LABEL	DESCRIPTION
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.
Access Status	Select the interface(s) through which a computer may access the ZyXEL Device using this service.

Table 116 Advanced > Remote Management > FTP

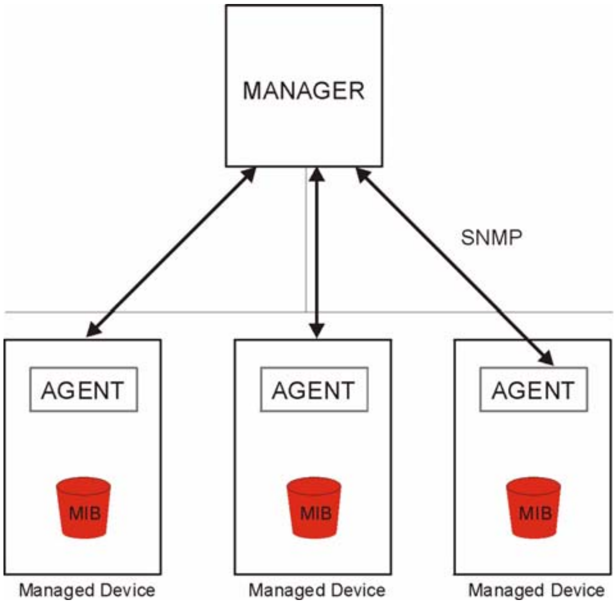
LABEL	DESCRIPTION
Secured Client IP	A secured client is a “trusted” computer that is allowed to communicate with the ZyXEL Device using this service. Select **All** to allow any computer to access the ZyXEL Device using this service. Choose **Selected** to just allow the computer with the IP address that you specify to access the ZyXEL Device using this service.
Apply	Click **Apply** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to begin configuring this screen afresh.

20.5 The SNMP Screen

Simple Network Management Protocol (SNMP) is a protocol used for exchanging management information between network devices. SNMP is a member of the TCP/IP protocol suite. Your 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) and version two (SNMPv2). The next figure illustrates an SNMP management operation.

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

Figure 210 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 and node port status. 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.

Supported MIBs

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

SNMP Traps

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

Table 117 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).

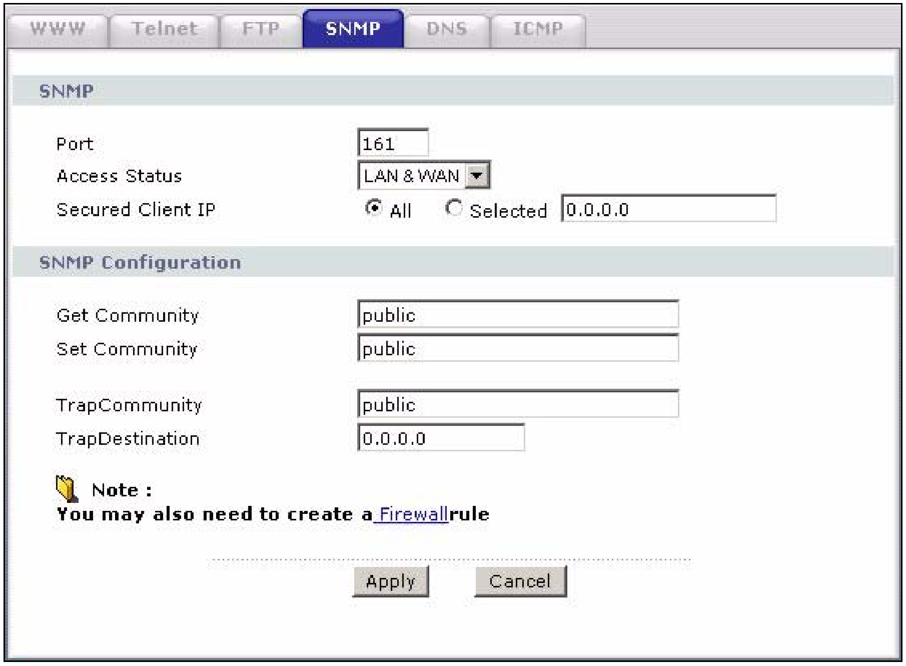
Table 117 SNMP Traps

TRAP #	TRAP NAME	DESCRIPTION
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").
6b	For fatal error:	A trap is sent with the message of the fatal code if the system reboots because of fatal errors.

20.5.1 Configuring SNMP

To change your ZyXEL Device’s SNMP settings, click **Advanced > Remote MGMT > SNMP**. The screen appears as shown.

Figure 211 Advanced > Remote Management > SNMP



SNMP

Port: 161
Access Status: LAN & WAN
Secured Client IP: ● All ○ Selected 0.0.0.0

SNMP Configuration

Get Community: public
Set Community: public

TrapCommunity: public
TrapDestination: 0.0.0.0

Note :
You may also need to create a Firewall rule

The following table describes the labels in this screen.

Table 118 Advanced > Remote Management > SNMP

LABEL	DESCRIPTION
SNMP	
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.
Access Status	Select the interface(s) through which a computer may access the ZyXEL Device using this service.

Table 118 Advanced > Remote Management > SNMP

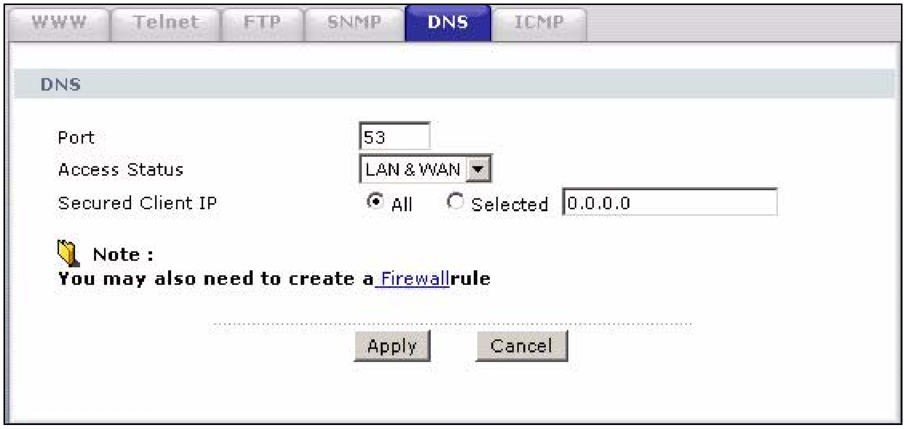
LABEL	DESCRIPTION
Secured Client IP	A secured client is a "trusted" computer that is allowed to communicate with the ZyXEL Device using this service. Select **All** to allow any computer to access the ZyXEL Device using this service. Choose **Selected** to just allow the computer with the IP address that you specify to access the ZyXEL Device using this service.
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.
Apply	Click **Apply** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to begin configuring this screen afresh.

20.6 The DNS Screen

Use DNS (Domain Name System) to map a domain name to its corresponding IP address and vice versa. Refer to Chapter 7 on page 117 for background 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. This feature is not available when the ZyXEL Device is set to bridge mode.

Figure 212 Remote Management: DNS



Port: 53
Access Status: LAN & WAN
Secured Client IP: ● 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 119 Remote Management: DNS

LABEL	DESCRIPTION
Port	The DNS service port number is 53 and cannot be changed here.
Access Status	Select the interface(s) through which a computer may send DNS queries to the ZyXEL Device.
Secured Client IP	A secured 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 and exit this screen.
Cancel	Click **Cancel** to begin configuring this screen afresh.

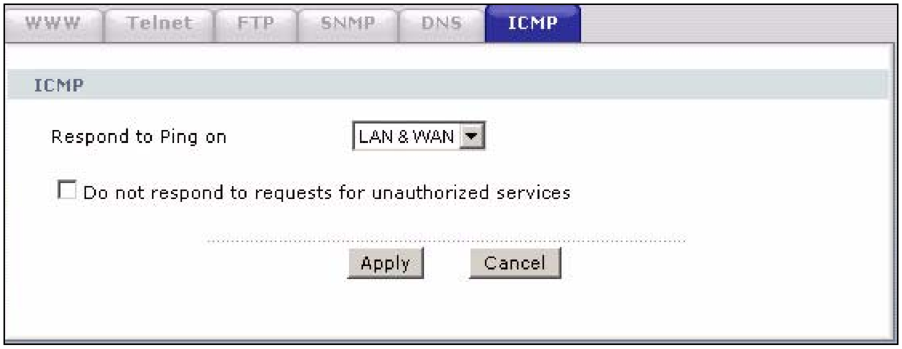
20.7 The ICMP Screen

To change your ZyXEL Device’s security settings, click **Advanced > Remote MGMT** > **ICMP**. The screen appears as shown.

If an outside user attempts to probe an unsupported port on your ZyXEL Device, an ICMP response packet is automatically returned. This allows the outside user to know the ZyXEL Device exists. Your ZyXEL Device supports anti-probing, which prevents the ICMP response packet from being sent. This keeps outsiders from discovering your ZyXEL Device when unsupported ports are probed.

Note: If you want your device to respond to pings and requests for unauthorized services, you may also need to configure the firewall anti probing settings to match.

Figure 213 Advanced > Remote Management > ICMP



ICMP

Respond to Ping on: LAN & WAN

□ Do not respond to requests for unauthorized services

The following table describes the labels in this screen.

Table 120 Advanced > Remote Management > ICMP

LABEL	DESCRIPTION
ICMP	Internet Control Message Protocol is a message control and error-reporting protocol between a host server and a gateway to the Internet. ICMP uses Internet Protocol (IP) datagrams, but the messages are processed by the TCP/IP software and directly apparent to the application user.
Respond to Ping on	The ZyXEL Device will not respond to any incoming Ping requests when **Disable** is selected. • Select **LAN** to reply to incoming LAN Ping requests. • Select **WAN** to reply to incoming WAN Ping requests. • Select **LAN & WAN** to reply to both incoming LAN and WAN Ping requests. • Select **WLAN & WAN** to reply to both incoming WLAN and WAN Ping requests. • Select **WLAN & LAN** to reply to both incoming WLAN and LAN Ping requests. • Select **WLAN** to reply to incoming WLAN Ping requests.
Do not respond to requests for unauthorized services	Select this option to prevent hackers from finding the ZyXEL Device by probing for unused ports. If you select this option, the ZyXEL Device will not respond to port request(s) for unused ports, thus leaving the unused ports and the ZyXEL Device unseen. If this option is not selected, the ZyXEL Device will reply with an ICMP port unreachable packet for a port probe on its unused UDP ports and a TCP reset packet for a port probe on its unused TCP ports. Note that the probing packets must first traverse the ZyXEL Device's firewall rule checks before reaching this anti-probing mechanism. Therefore if a firewall rule stops a probing packet, the ZyXEL Device reacts based on the firewall rule to either send a TCP reset packet for a blocked TCP packet (or an ICMP port-unreachable packet for a blocked UDP packets) or just drop the packets without sending a response packet.

Table 120 Advanced > Remote Management > ICMP

LABEL	DESCRIPTION
Apply	Click **Apply** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to begin configuring this screen afresh.

Universal Plug-and-Play (UPnP)

21.1 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.

21.1.1 What You Can Do in the UPnP Screen

Use the **UPnP** screen (Section 21.2 on page 363) to enable UPnP on the ZyXEL Device and allow UPnP-enabled applications to automatically configure the ZyXEL Device.

21.1.2 What You Need to Know About UPnP

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.

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 the NAT chapter for more information on NAT.

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.

UPnP and ZyXEL

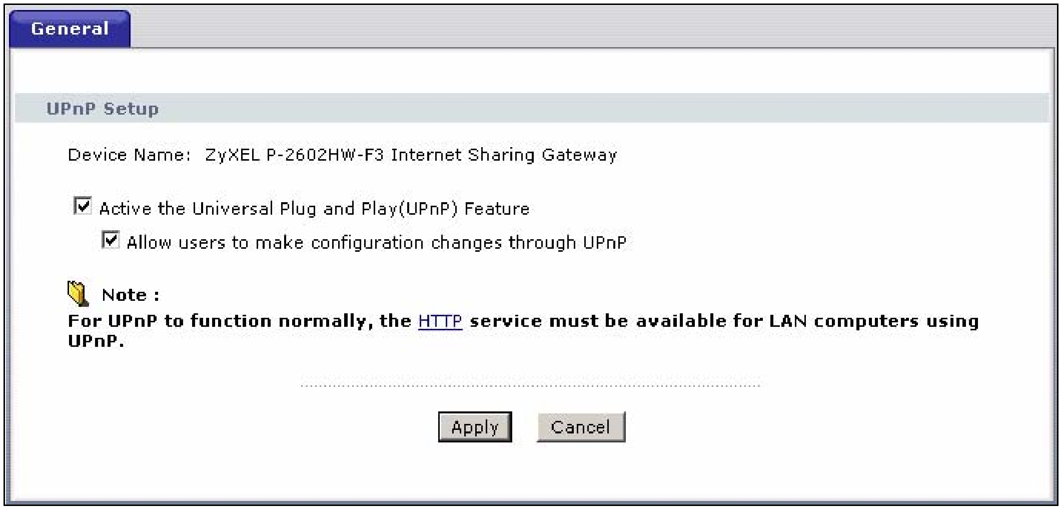
ZyXEL has achieved UPnP certification from the Universal Plug and Play Forum UPnP™ Implementers Corp. (UIC). ZyXEL's UPnP implementation supports Internet Gateway Device (IGD) 1.0.

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

21.2 The UPnP Screen

Click **Advanced > UPnP** to display the screen shown next. See Section 21.1 on page 361 for more information.

Figure 214 Advanced > UPnP > General



Device Name: ZyXEL P-2602HW-F3 Internet Sharing Gateway

☑ Active the Universal Plug and Play(UPnP) Feature

☑ Allow users to make configuration changes through UPnP

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 121 Advanced > UPnP > General

LABEL	DESCRIPTION
Active 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.
Apply	Click **Apply** to save the setting to the ZyXEL Device.
Cancel	Click **Cancel** to return to the previously saved settings.

21.3 Installing UPnP in Windows Example

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

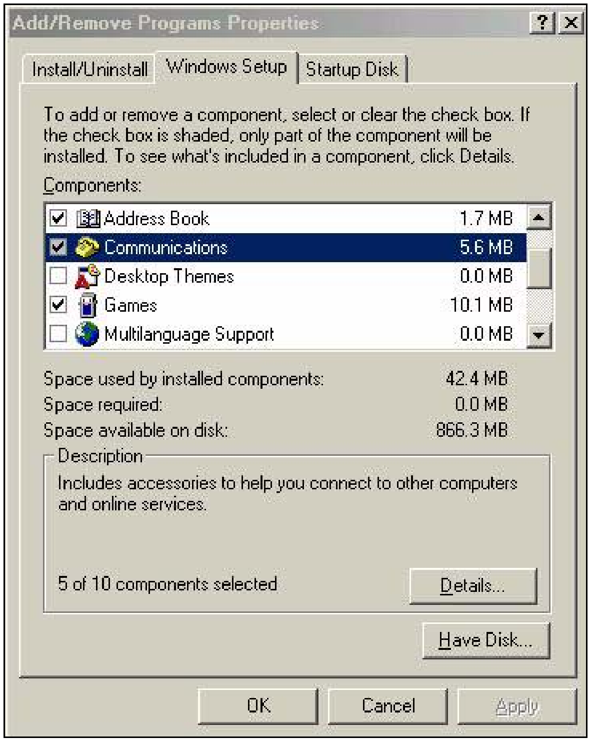
Installing UPnP in Windows Me

Follow the steps below to install the UPnP in Windows Me.

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

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

Figure 215 Add/Remove Programs: Windows Setup: Communication



To add or remove a component, select or clear the check box. If the check box is shaded, only part of the component will be installed. To see what's included in a component, click Details.

Components:

☑	Address Book	1.7 MB
☑	Communications	5.6 MB
□	Desktop Themes	0.0 MB
☑	Games	10.1 MB
□	Multilanguage Support	0.0 MB

Space used by installed components:	42.4 MB
Space required:	0.0 MB
Space available on disk:	866.3 MB

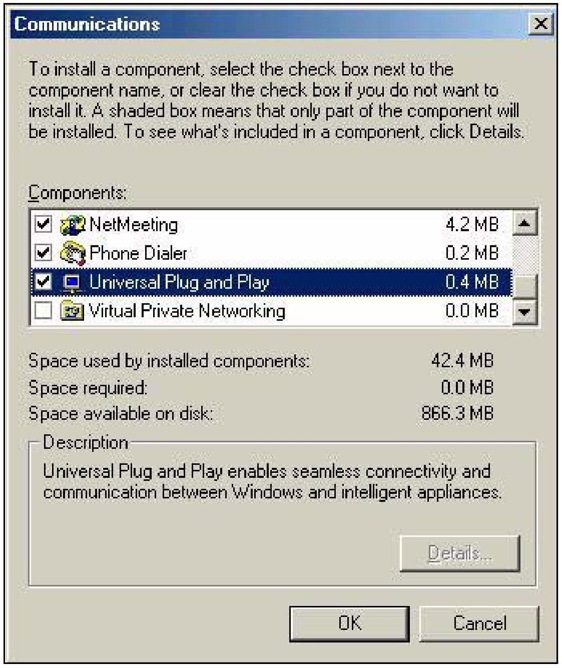
Description

Includes accessories to help you connect to other computers and online services.

5 of 10 components selected

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

Figure 216 Add/Remove Programs: Windows Setup: Communication: Components



Communications

To install a component, select the check box next to the component name, or clear the check box if you do not want to install it. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Components:

☑	NetMeeting	4.2 MB
☑	Phone Dialer	0.2 MB
☑	Universal Plug and Play	0.4 MB
□	Virtual Private Networking	0.0 MB

Space used by installed components:	42.4 MB
Space required:	0.0 MB
Space available on disk:	866.3 MB

Description

Universal Plug and Play enables seamless connectivity and communication between Windows and intelligent appliances.

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

5 Restart the computer when prompted.

Installing UPnP in Windows XP

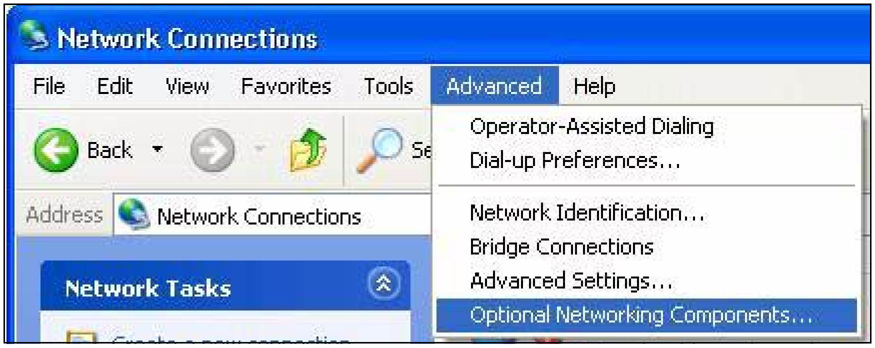
Follow the steps below to install the UPnP in Windows XP.

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

2 Double-click **Network Connections**.

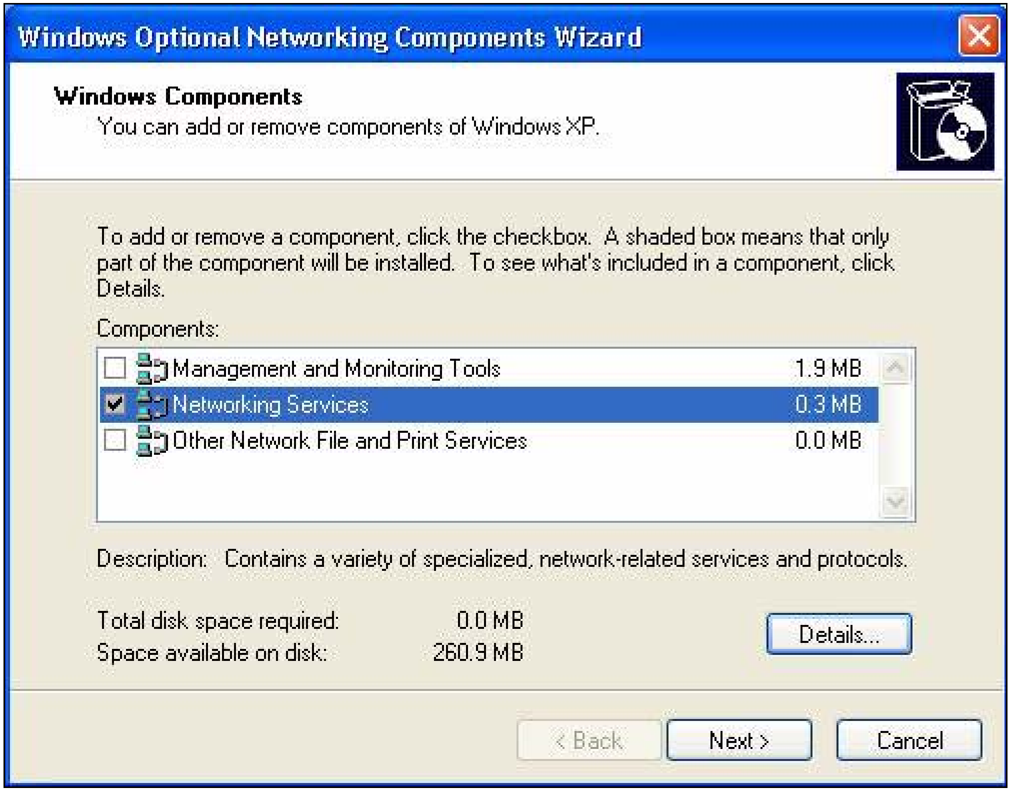
3 In the **Network Connections** window, click **Advanced** in the main menu and select **Optional Networking Components ...**.

Figure 217 Network Connections



4 The **Windows Optional Networking Components Wizard** window displays. Select **Networking Service** in the **Components** selection box and click **Details**.

Figure 218 Windows Optional Networking Components Wizard



Windows Optional Networking Components Wizard

Windows Components

You can add or remove components of Windows XP.

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

Components:

□	Management and Monitoring Tools	1.9 MB
☑	Networking Services	0.3 MB
□	Other Network File and Print Services	0.0 MB

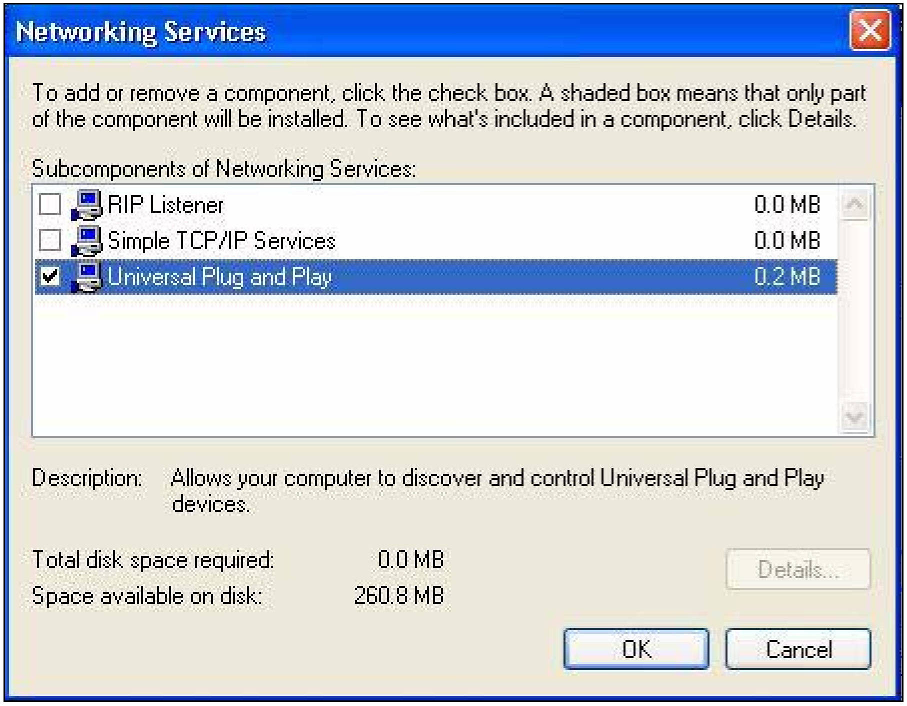
Description: Contains a variety of specialized, network-related services and protocols.

Total disk space required: 0.0 MB

Space available on disk: 260.9 MB

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

Figure 219 Networking Services



Networking Services

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: 260.8 MB

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

21.4 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.

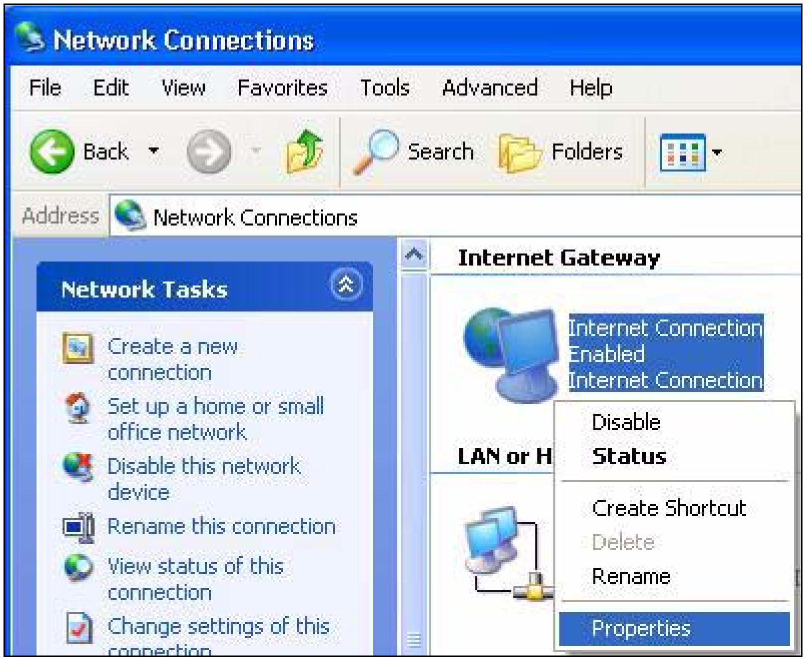
Make sure the computer is connected to a LAN port of the ZyXEL Device. Turn on your computer and the ZyXEL Device.

Auto-discover Your UPnP-enabled Network Device

1 Click **Start** and **Control Panel**. Double-click **Network Connections**. An icon displays under Internet Gateway.

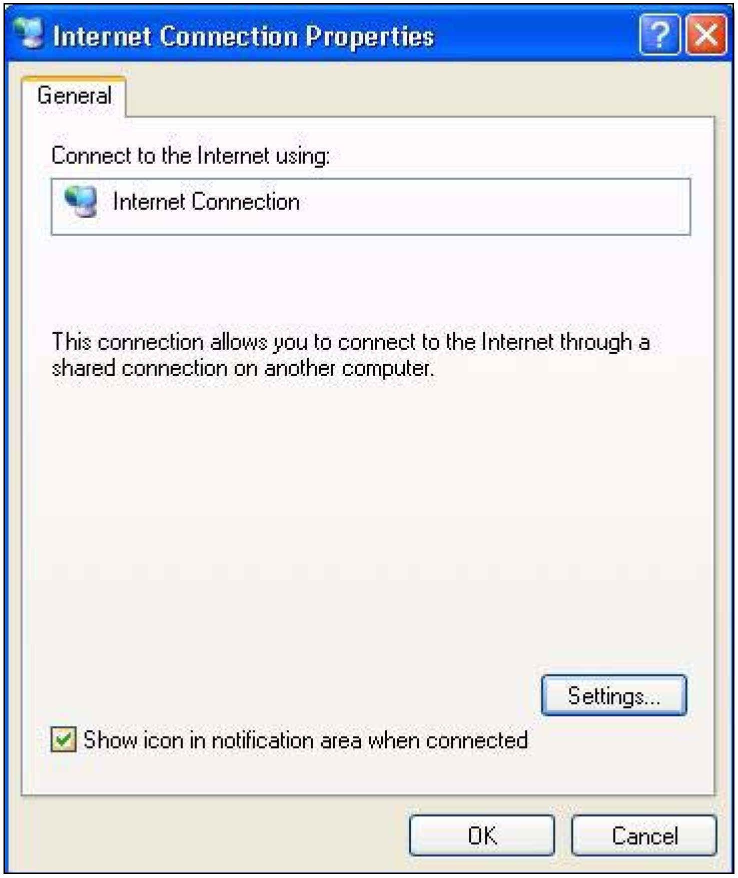
2 Right-click the icon and select **Properties**.

Figure 220 Network Connections



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

Figure 221 Internet Connection Properties



Connect to the Internet using:

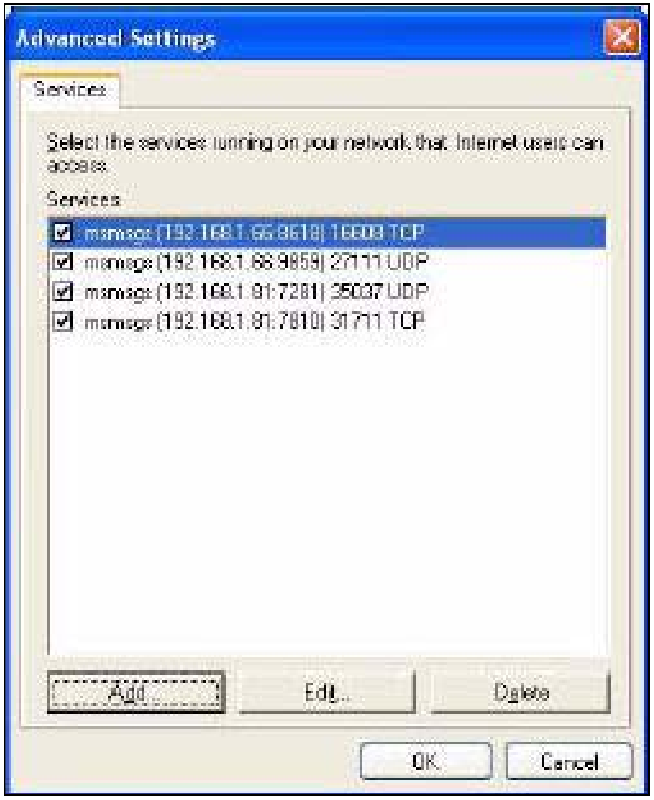
Internet Connection

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

☑ Show icon in notification area when connected

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

Figure 222 Internet Connection Properties: Advanced Settings



Advanced Settings

Services

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

Services

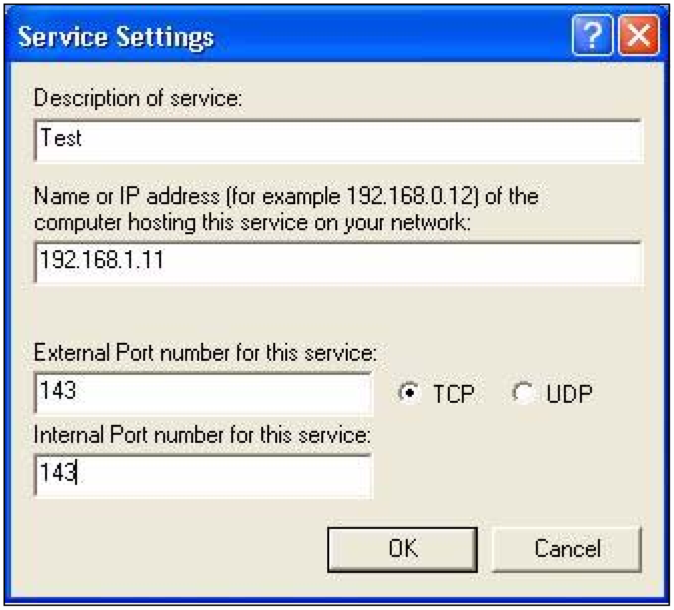
☑ msmsgs (192.168.1.66:8618) 16608 TCP

☑ msmsgs (192.168.1.66:9859) 27111 UDP

☑ msmsgs (192.168.1.81:7281) 35037 UDP

☑ msmsgs (192.168.1.81:7810) 31711 TCP

Figure 223 Internet Connection Properties: Advanced Settings: Add



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

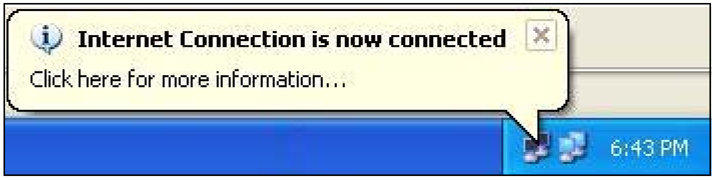
External Port number for this service:
143 ● TCP ○ UDP

Internal Port number for this service:
143

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

6 Select **Show icon in notification area when connected** option and click **OK**. An icon displays in the system tray.

Figure 224 System Tray Icon

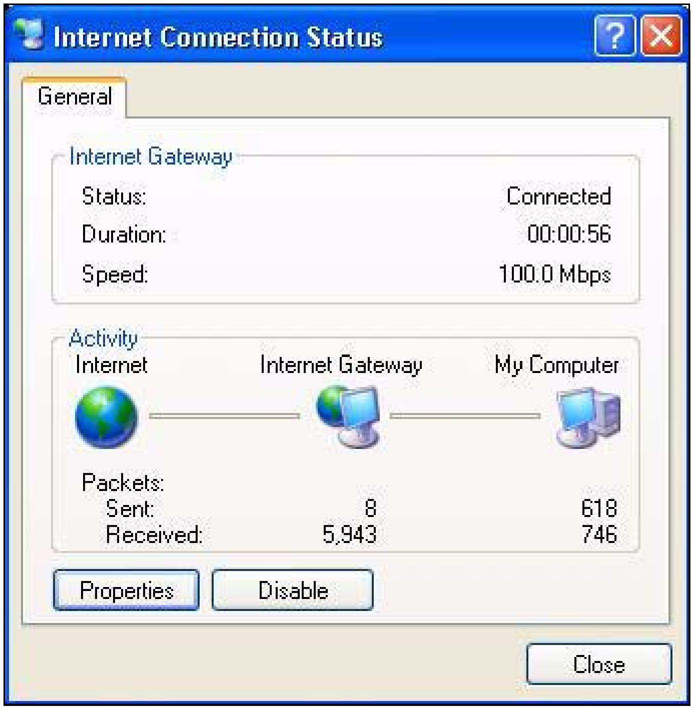


Internet Connection is now connected

Click here for more information...

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

Figure 225 Internet Connection Status



Internet Connection Status

Internet Gateway

Status: Connected

Duration: 00:00:56

Speed: 100.0 Mbps

Activity

Packets:	Internet Gateway	My Computer
Sent:	8	618
Received:	5,943	746

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 comes helpful if you do not know the IP address of the ZyXEL Device.

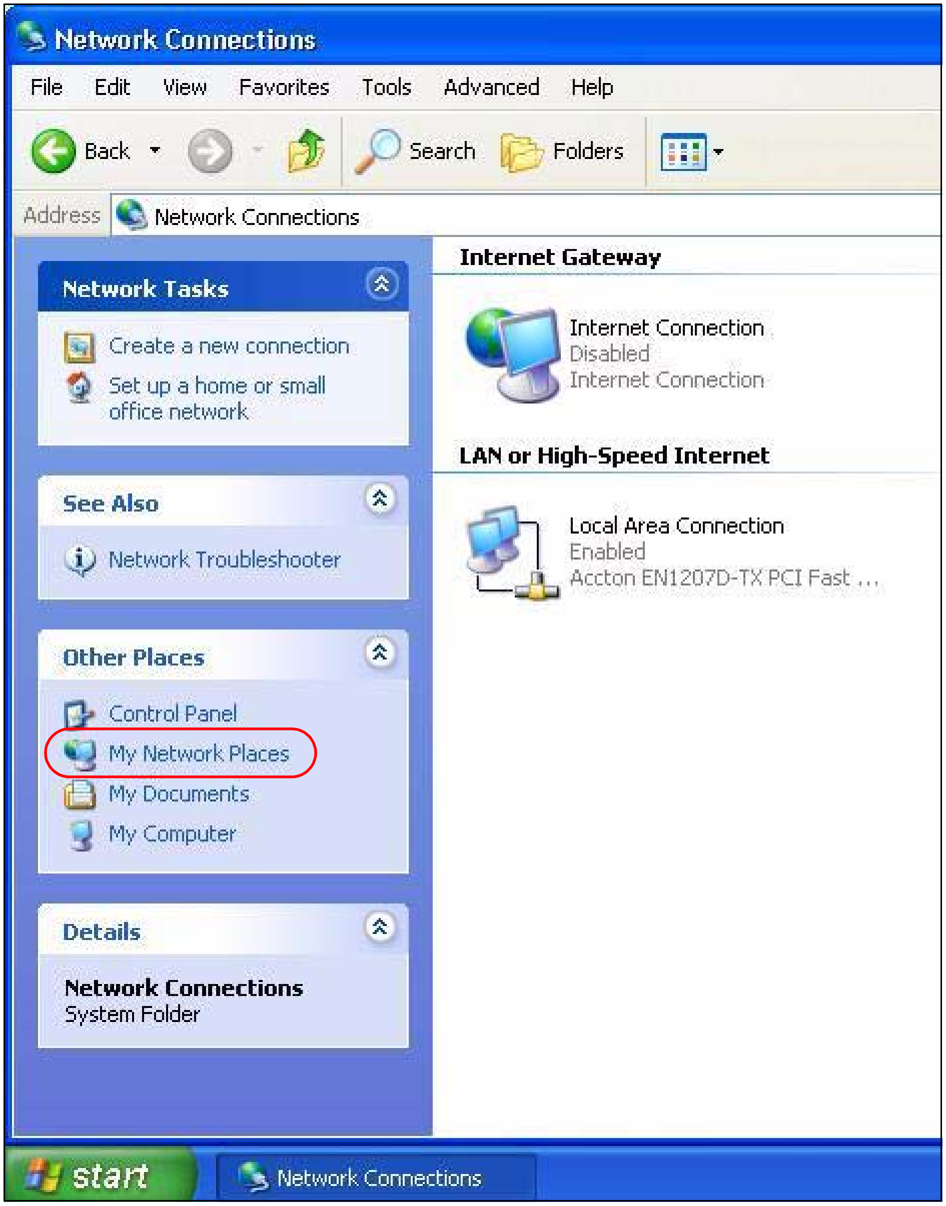
Follow the steps below to access the web configurator.

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

2 Double-click **Network Connections**.

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

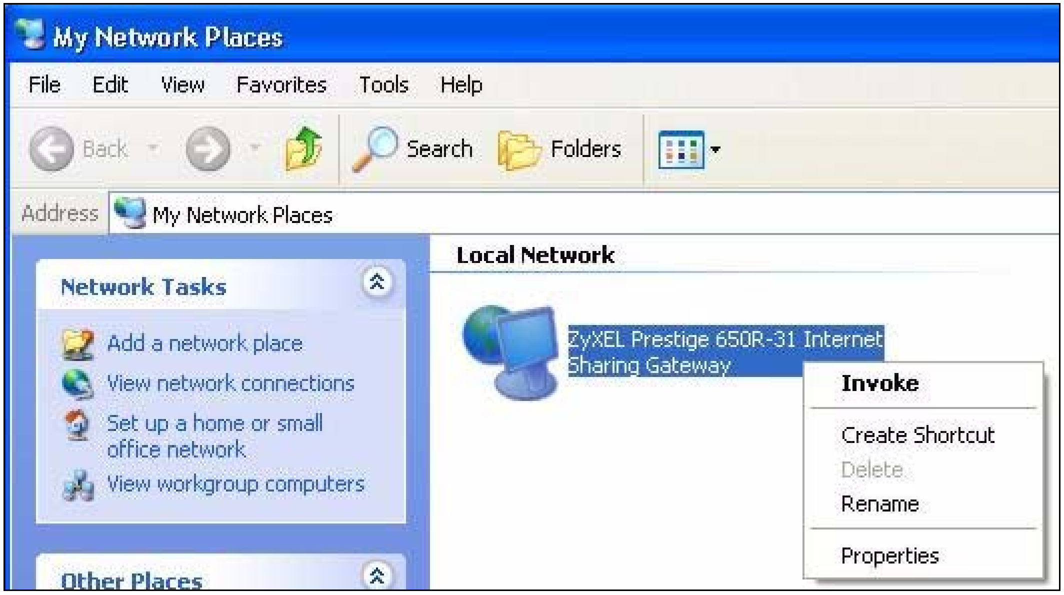
Figure 226 Network Connections



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

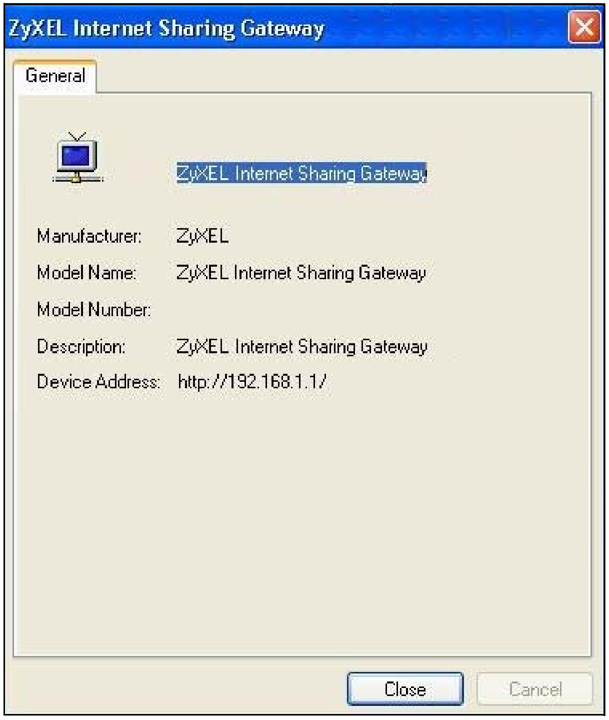
5 Right-click on the icon for your ZyXEL Device and select **Invoke**. The web configurator login screen displays.

Figure 227 Network Connections: My Network Places



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

Figure 228 Network Connections: My Network Places: Properties: Example



ZyXEL Internet Sharing Gateway

Manufacturer: ZyXEL

Model Name: ZyXEL Internet Sharing Gateway

Model Number:

Description: ZyXEL Internet Sharing Gateway

Device Address: http://192.168.1.1/

22

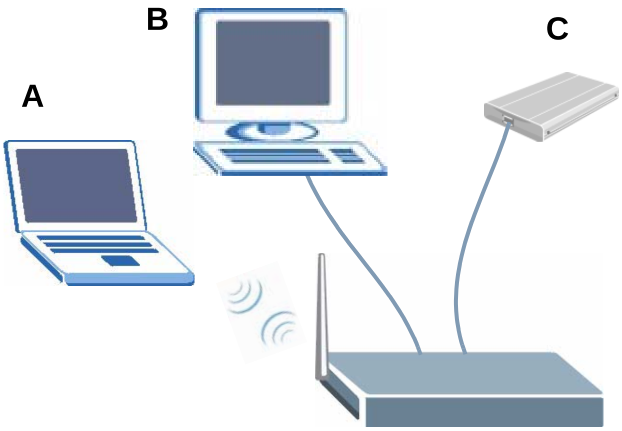
File Sharing

22.1 Overview

Share files on a USB memory stick or hard drive connected to your ZyXEL Device with users on your network.

The following figure is an overview of the ZyXEL Device's file server feature. Computers **A** and **B** can access files on a USB device (**C**) which is connected to the ZyXEL Device.

Figure 229 File Sharing Overview



- See Section 22.1.2 on page 376 for an explanation of file-sharing terms.
- See Section 22.1.4 on page 377 for file-sharing examples.

22.1.1 What You Can Do in the File-Sharing Screens

- Use the **Server Settings** screen (Section 22.2 on page 381) to configure your file-sharing server.
- Use the **User Name and Password** screen (Section 22.3 on page 383) to set up and edit a file-sharing account.
- Use the **Share Configuration** screen (Section 22.4 on page 384) to configure your the file path of your shares.

22.1.2 What You Need to Know About File-Sharing

User Account

This gives you access to the file-sharing server. It includes your user name and password.

Workgroup name

This is the name given to a set of computers that are connected on a network and share resources such as a printer or files. Windows automatically assigns the workgroup name when you set up a network.

Shares

When settings are set to default, each USB device connected to the ZyXEL Device is given a folder, called a “share”. If a USB hard drive connected to the ZyXEL Device has more than one partition, then each partition will be allocated a share. You can also configure a “share” to be a sub-folder or file on the USB device.

File Systems

A file system is a way of storing and organizing files on your hard drive and storage device. Often different operating systems such as Windows or Linux have different file systems. The file-sharing feature on your ZyXEL Device supports File Allocation Table (FAT) and FAT32 file systems.

Common Internet File System

The ZyXEL Device uses Common Internet File System (CIFS) protocol for its file sharing functions. CIFS compatible computers can access the USB file storage devices connected to the ZyXEL Device. CIFS protocol is supported on Microsoft Windows, Linux Samba and other operating systems (refer to your systems specifications for CIFS compatibility).

File Transfer Protocol

This is a method of transferring data from one computer to another over a network such as the Internet.

22.1.3 Before You Begin

Make sure the ZyXEL Device is connected to your network and turned on.

1 Connect the USB device to one of the ZyXEL Device’s USB ports. Make sure the ZyXEL Device is connected to your network.

2 The ZyXEL Device detects the USB device and makes its contents available for browsing. If you are connecting a USB hard drive that comes with an external power supply, make sure it is connected to an appropriate power source that is on.

Note: If your USB device cannot be detected by ZyXEL Device, see the troubleshooting for suggestions.

22.1.4 File-Sharing Examples

In this section you can:

- Set up File-Sharing
- Share Your Files

22.1.4.1 Set Up File-Sharing

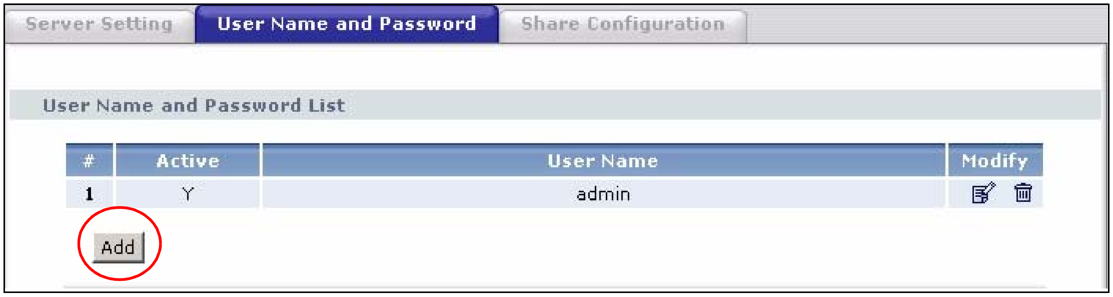
To set up file-sharing you need to set up a user account, enable file-sharing and set up your share(s).

Set up a User Account

Before you can share files you need a user account.

1 Click **Advanced > File Sharing > User Name and Password** to display the following screen. Click **Add** to set up a user name and password.

Figure 230 Advanced > File-Sharing > User Name and Password Example

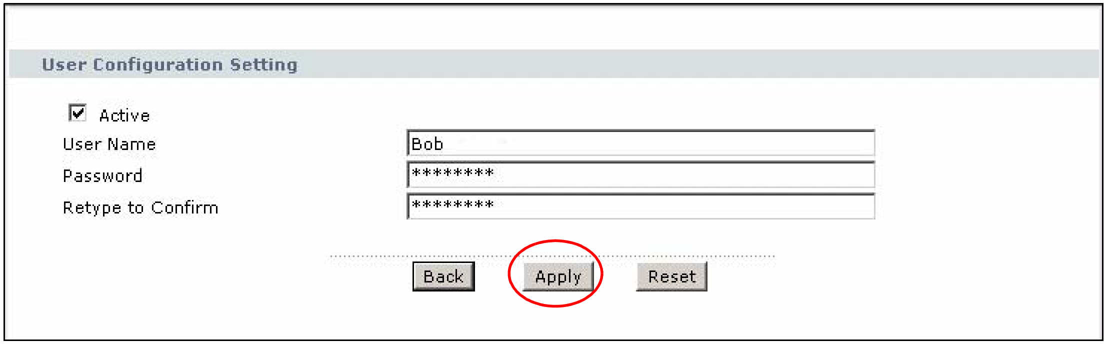


User Name and Password List

#	Active	User Name	Modify
1	Y	admin	📝 🗑

2 The following screen appears. Select **Active**, and enter a user name and password as shown in the example screen below. Click **Apply** to save your settings.

Figure 231 Advanced > File-Sharing > User Name and Password: Add Example



User Configuration Setting

☑ Active

User Name	Bob
Password	********
Retype to Confirm	********

3 This sets up your user account, now you are ready to set up file-sharing on your ZyXEL Device.

Set up File-Sharing on Your ZyXEL Device

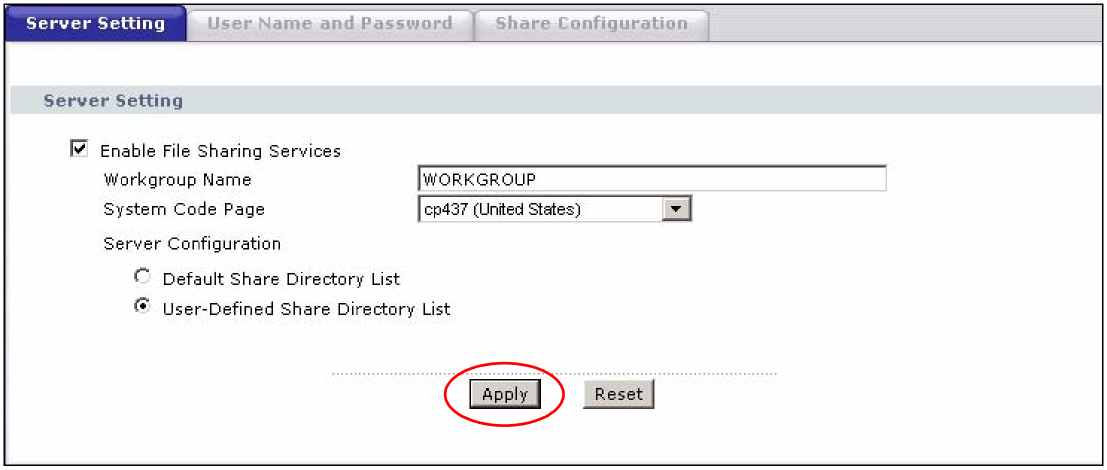
You also need to set up file-sharing on your ZyXEL Device in order to share files.

1 Go to **Advanced > File Sharing > Server Setting** to enter a workgroup name and select the type of characters used in your USB device, as shown in the screen below.

- If you want to use default share names, select **Default Share Directory List** in this screen.
- If you want to use your own share names and add, modify or delete shares, select **User-Defined Share Directory List** in this screen, as shown in the example screen below.

2 Click **Apply** to save your settings.

Figure 232 Advanced > File Sharing > Server Setting Example



Server Setting

☑ Enable File Sharing Services

Workgroup Name	WORKGROUP
System Code Page	cp437 (United States)

Server Configuration

○ Default Share Directory List

● User-Defined Share Directory List

3 This sets up the file-sharing server.

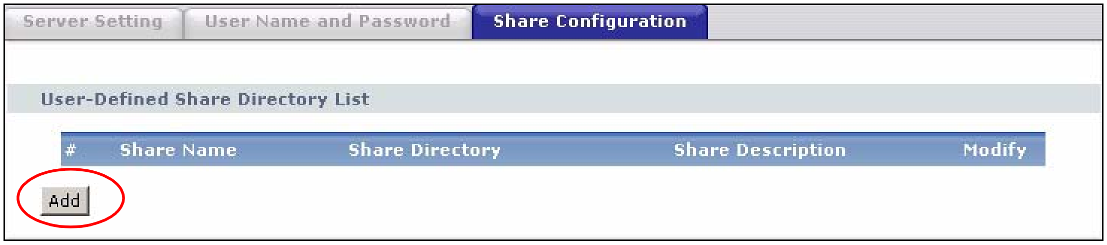
- If you have selected **Default Share Directory List**, you are ready to file-share. Go to Section 22.1.4.2 on page 380 for an example on sharing your files.
- If you have selected **User-Defined Share Directory List**, go to the next section to set up your shares.

Set up Your Share(s)

If you have selected **User-Defined Share Directory List** when you set up your file-sharing server, you can add, edit or delete your shares.

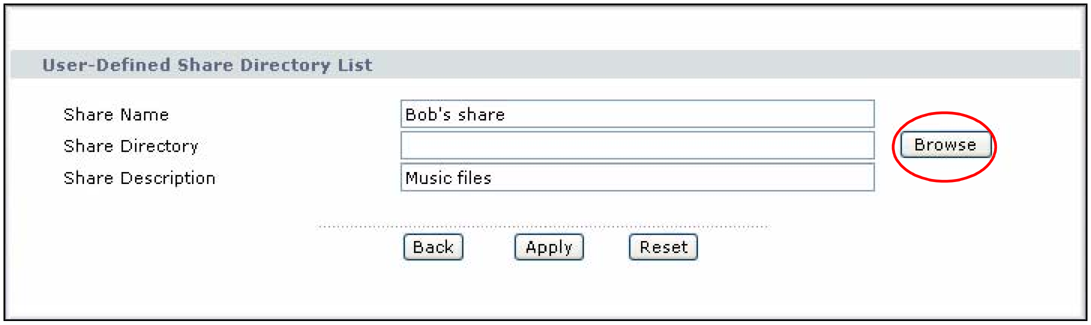
1 Go to **Advanced > File Sharing > Share Configuration** and click **Add** as shown in the following screen.

Figure 233 Advanced > File Sharing > Share Configuration Example


Server Setting
User Name and Password
Share Configuration
User-Defined Share Directory List
# Share Name Share Directory Share Description Modify
Add

2 Set up a file path for the server to find your shares. In the screen that appears, type the name of your share and a description as shown in the following example screen. Click **Browse**.

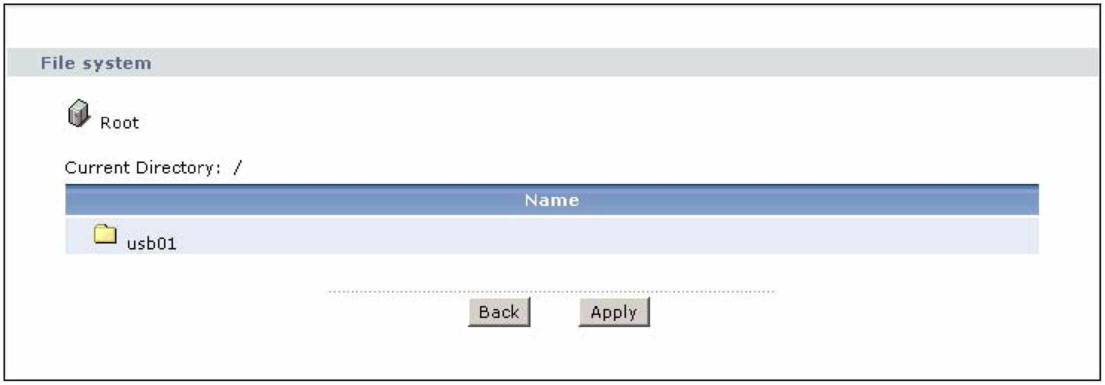
Figure 234 Advanced > File Sharing > Share Configuration: Add Example


User-Defined Share Directory List

Share Name	Bob's share
Share Directory	
Share Description	Music files

3 Another screen appears, letting you set the file path of your share. Click **Apply**.

Figure 235 Advanced > File Sharing > Share Configuration: Add: Browse Example



4 You are now ready to file-share. Go to Section 22.1.4.2 on page 380 to share your files.

22.1.4.2 Access Your Shared Files From a Computer

You can use Windows to access the file storage devices connected to the ZyXEL Device.

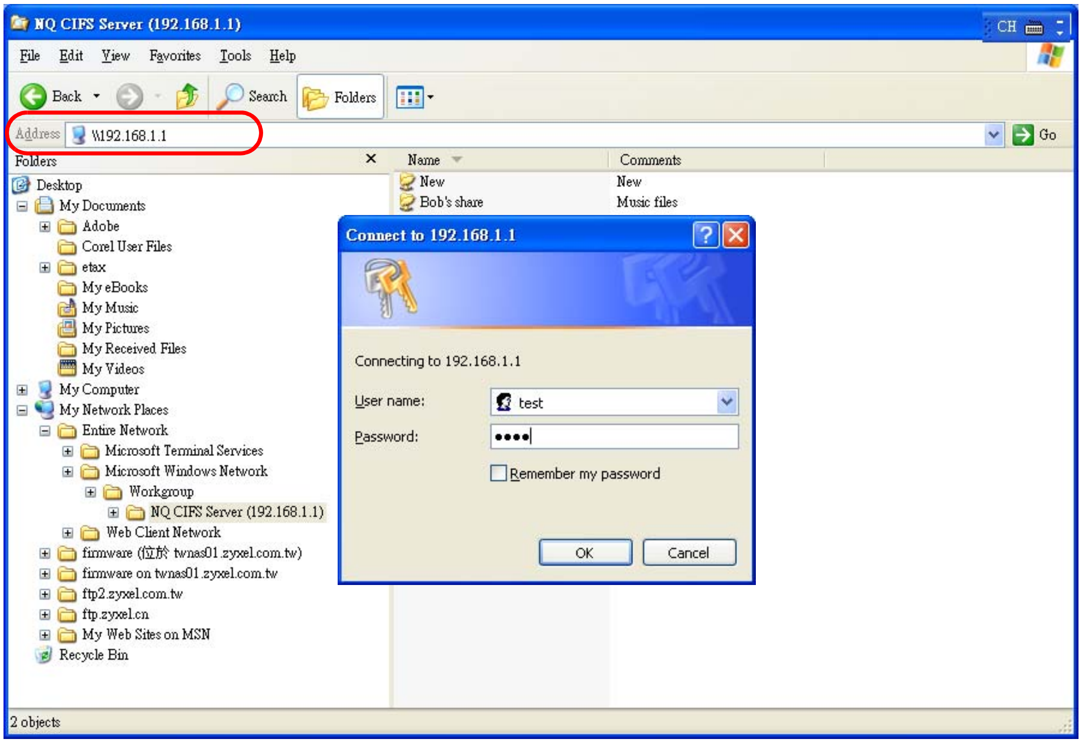
Note: The examples in this User's Guide show you how to use Microsoft's Windows XP to browse your shared files. Refer to your operating system's documentation for how to browse your file structure.

Use Windows Explorer to Share Files

Open Windows Explorer to access Bob's Share using Windows Explorer browser.

1 In Windows Explorer's Address bar type a double backslash "\\" followed by the IP address of the ZyXEL Device (the default IP address of the ZyXEL Device is 192.168.1.1) and press [ENTER]. A screen asking for password authentication appears. Type the user name and password and click **OK**.

Figure 236 File Sharing via Windows Explorer



Connecting to 192.168.1.1

User name: test

Password: ••••

☐ Remember my password

Note: Once you login to the file "Bob's Share" via your ZyXEL Device, you do not have to relogin unless you restart your computer.

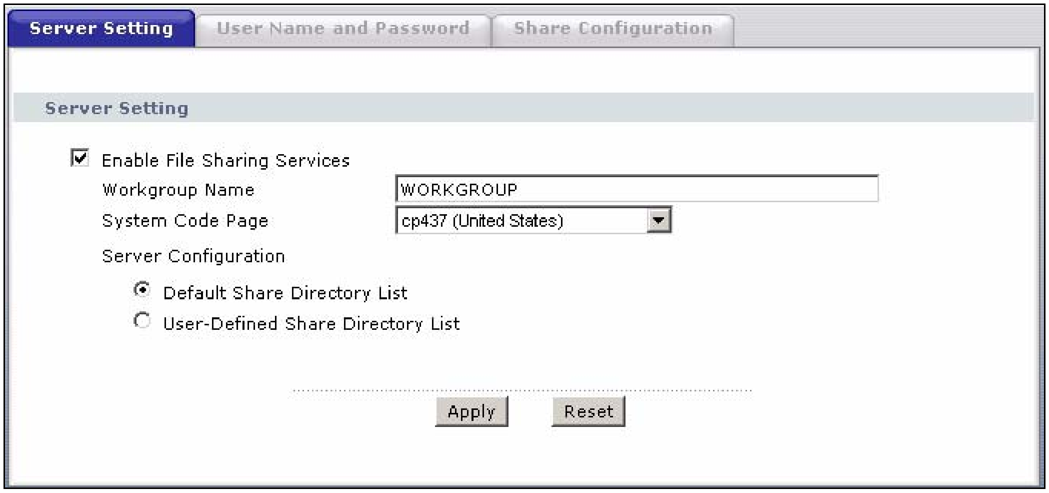
22.2 The Server Settings Screen

In the **Server Settings** screen you need to configure your ZyXEL Device's **Workgroup Name**.

The ZyXEL Device will not be able to join the workgroup if your local area network has restrictions set up that do not allow devices to join a workgroup. In this case, contact your network administrator.

Use this screen to set up file sharing via the ZyXEL Device. To access this screen, click **Advanced > File Sharing**.

Figure 237 File Sharing > Server Configuration



☑ Enable File Sharing Services

Workgroup Name: WORKGROUP

System Code Page: cp437 (United States)

Server Configuration

● Default Share Directory List

○ User-Defined Share Directory List

Each field is described in the following table.

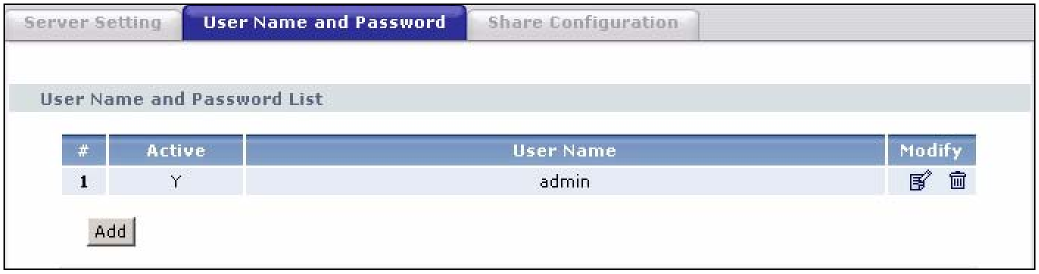
Table 122 File Sharing > Server Configuration

LABEL	DESCRIPTION
Enable File Sharing Services	Select this to enable file sharing through the ZyXEL Device.
Workgroup Name	You can add the ZyXEL Device to an existing or a new workgroup on your network. Enter the name of the workgroup which your ZyXEL Device automatically joins. You can set the ZyXEL Device's workgroup name to be exactly the same as the workgroup name to which your computer belongs to.
System Code Page	Select the character set of the files contained on your storage device. For example, if your files were created on an operating system which used the Russian alphabet, select **cp866 (Russian)**. If the file or folder names on your USB storage device appear as unrecognizable (or jumbled) characters, you should double check this setting to make sure it is set correctly.
Server Configuration	Select **Default Share Directory List** to use the preset share names. Select **User-Defined Share Directory List** to use your own share names and set access levels.
Apply	Click this to save your changes to the ZyXEL Device.
Reset	Click this to set every field in this screen to its last-saved value.

22.3 The User Name and Password Screen

Use this screen to configure a user account. To access this screen, click **Advanced > File Sharing > User Name and Password**.

Figure 238 File Sharing > User Name and Password



User Name and Password List

#	Active	User Name	Modify
1	Y	admin	

Each field is described in the following table.

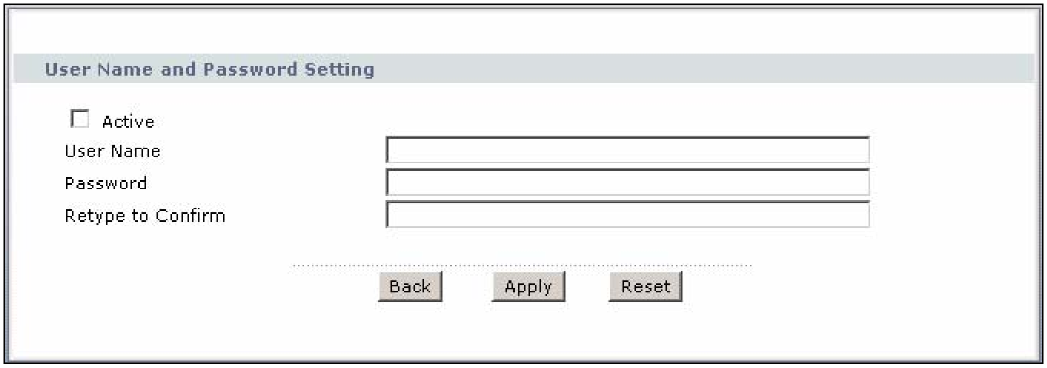
Table 123 File Sharing > User Name and Password

LABEL	DESCRIPTION
#	This is a read-only index number of the user name on the ZyXEL Device.
Active	This shows whether the user name is active (able to access shares via the ZyXEL Device) or inactive (unable to access shares via the ZyXEL Device).
User Name	This field shows the list of user names already configured on the ZyXEL Device.
Modify	Click the Edit icon to change the settings of an existing user account. Click the Remove icon to delete this entry in the list.
Add	Click this button to configure another user name and include it in the list.

22.3.1 Add or Edit a User Account

Use this screen to add or edit a user account. To access this screen, click **Advanced > File Sharing > User Configuration** and click the **Edit** icon in the **Modify** column or the **Add** button.

Figure 239 File Sharing > User Configuration > Add/Edit



User Name and Password Setting

□ Active

User Name

Password

Retype to Confirm

Each field is described in the following table.

Table 124 File Sharing > User Configuration > Add/Edit

LABEL	DESCRIPTION
Active	Select this to set whether the user name is active (able to access shares via the ZyXEL Device) or inactive (unable to access shares via the ZyXEL Device).
User Name	This field is not configurable if you click the Edit icon in the **Modify** column to configure an existing user account. Enter the user name of the account. The user name can be 31 alpha-numeric characters long.
Password	Enter the password for this account. The password can be 31 alpha-numeric characters long.
Retype to Confirm	Retype the password.
Back	Click this button to return to the previous screen without saving your settings.
Apply	Click this to save your changes to the ZyXEL Device.
Reset	Click this to set the fields in this screen to their defaults.

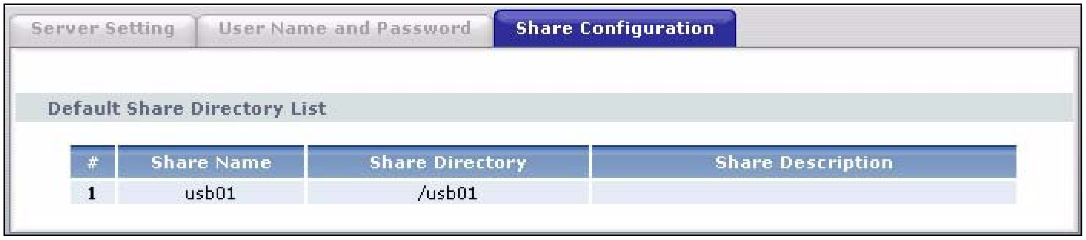
22.4 The Share Configuration Screen

Two possible screens appear depending on your **Server Configuration** settings in the **Server Setting** screen. See Section 22.2 on page 381 for details.

22.4.1 Default Share Directory List

If you selected **Default Share Directory List** in the **Server Settings** screen, the following screen appears when you click **Advanced > File Sharing > Share Configuration**.

Figure 240 File Sharing > Share Configuration: Default



#	Share Name	Share Directory	Share Description
1	usb01	/usb01	

Each field is described in the following table.

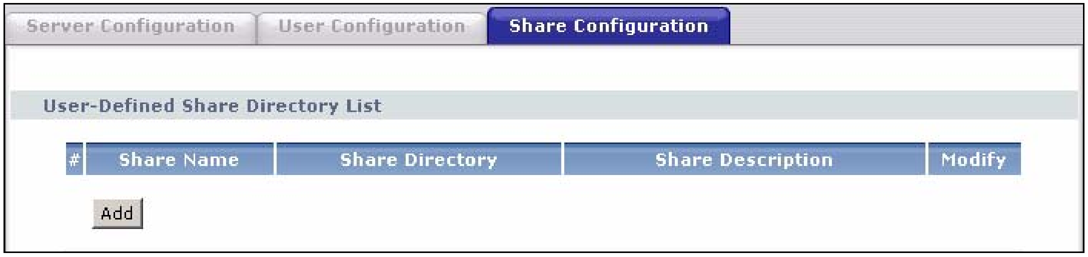
Table 125 File Sharing > Share Configuration: Default

LABEL	DESCRIPTION
Default Share Directory List	These fields identify the default shares on the ZyXEL Device.
#	This is a read-only index number of the default share on the ZyXEL Device. When more than one USB disk (or a USB hard drive with multiple shares) is connected to the ZyXEL Device this index number identifies the different disks. The first disk connected is 1, the second 2 and so on.
Share Name	This field displays the default share names on the ZyXEL Device.
Share Directory	This field displays the share directories (folders) on the ZyXEL Device. These are the directories (folders) you can enter when you browse to your USB storage device.

22.4.2 User-Defined Share Directory List

If you selected **User-Defined Directory List** in the **Server Settings** screen, the following screen appears when you click **Advanced > File Sharing > Share Configuration**.

Figure 241 File Sharing > Share Configuration: User-Defined



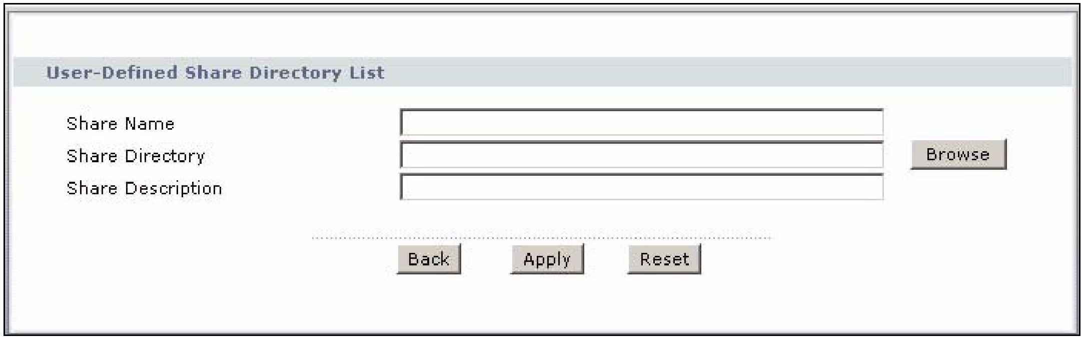
Each field is described in the following table.

Table 126 File Sharing > Share Configuration: User-Defined

LABEL	DESCRIPTION
User-Defined Share Directory List	These fields identify the shares you configured on the ZyXEL Device.
#	This is a read-only index number of the user-defined share on the ZyXEL Device.
Share Name	This field displays the user-defined share name on the ZyXEL Device.
Share Directory	This field displays the user-defined share directories (folders) on the ZyXEL Device. These are the directories (folders) you can enter when you browse to your USB storage device.
Share Description	This field displays information about the share. You can add share descriptions to user-defined shares in the **Share Configuration Add / Edit** screen.
Modify	Click the **Edit** icon to change the settings of an existing user-defined share. Click the **Remove** icon to delete this share in the list.
Add	Click this to set up a new user-defined share on the ZyXEL Device.

22.4.3 Add or Edit a User-Defined Share

Figure 242 File Sharing > Share Configuration: User-Defined > Add/Edit



Each field is described in the following table.

Table 127 File Sharing > Share Configuration: User-Defined > Add/Edit

LABEL	DESCRIPTION
Share Name	Enter the name you want the user-defined share to have in the network.
Share Directory	Manually enter the file path for the user-defined share, or click the **Browse** button.
Browse	Click this button to select the file path for the user-defined share directory. This is the folder that will be visible to a user browsing to the USB storage device. A user can access any files and sub-folders in this folder.

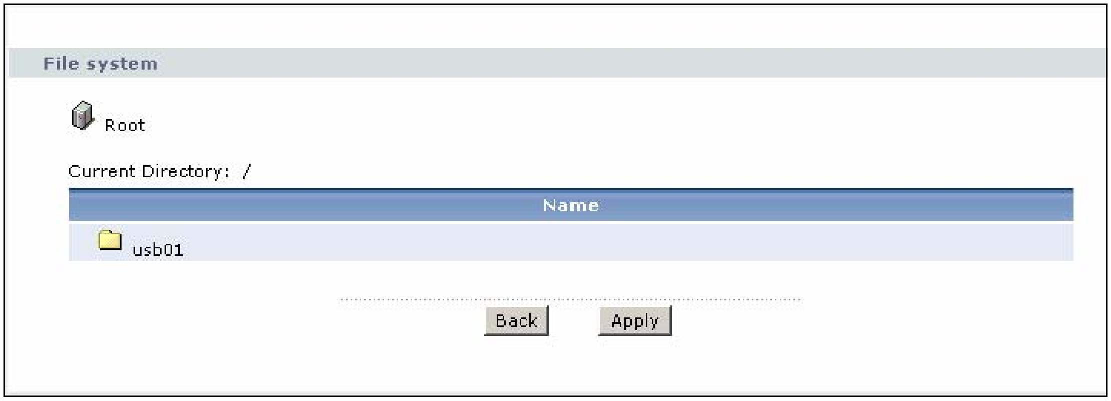
Table 127 File Sharing > Share Configuration: User-Defined > Add/Edit

LABEL	DESCRIPTION
Share Description	You can either enter a short description of the share, or leave this field blank.
Back	Click this button to return to the previous screen without saving your settings.
Apply	Click this button to save your settings.
Reset	Click this button to return all fields in this screen to their previous values.

22.4.4 Browse

To select the file path for the user-defined share directory, click **Browse** in the **Share Configuration Add/Edit** screen.

Figure 243 File Sharing > Share Configuration: User-Defined > Browse



File system

Root

Current Directory: /

Name
usb01

Each field is described in the following table.

Table 128 File Sharing > Share Configuration: User-Defined > Browse

LABEL	DESCRIPTION
File System	Use this section to set up the directory path for the share.
Parent Directory	Click the **Parent Directory** icon (⏫) to go up one level.
Current Directory	This field displays the file path of the share. This is the folder that will be visible to a user browsing to the USB storage device. A user can access any files and sub-folders in this folder.
Name	This displays the name of the folder in the **Current Directory** of the connected USB storage device. Click on a folder name to add that folder to the directory path for the share
Back	Click this button to return to the previous screen without saving your settings.
Apply	Click this button to save your settings.

CHAPTER 23

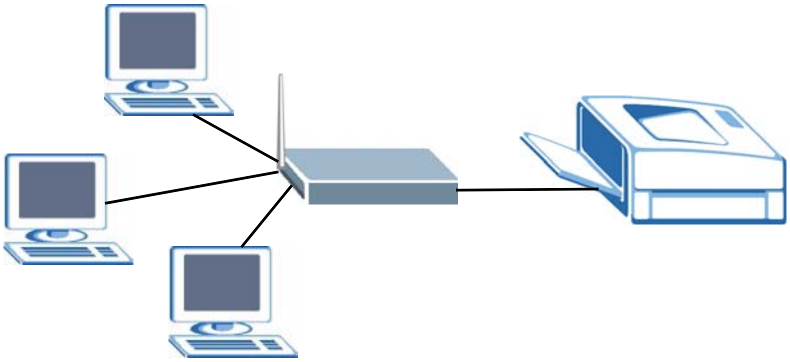
Sharing a USB Printer

This chapter describes how you can share a USB printer via your ZyXEL Device.

23.1 Overview

The ZyXEL Device allows you to share a USB printer on your LAN. You can do this by connecting a USB printer to one of the USB ports on the ZyXEL Device and then configuring a TCP/IP port on the computers connected to your network.

Figure 244 Sharing a USB Printer



23.1.1 What You Need to Know About Printer Sharing

Print Server

This is a computer or other device which manages one or more printers, and which sends print jobs to each printer from the computer itself or other devices.

Operating System

An operating system (OS) is the interface which helps you manage a computer. Common examples are Microsoft Windows, Mac OS or Linux.

TCP/IP

TCP/IP (Transmission Control Protocol/ Internet Protocol) is a set of communications protocols that most of the Internet runs on.

Port

A port maps a network service such as http to a process running on your computer, such as a process run by your web browser. When traffic from the Internet is received on your computer, the port number is used to identify which process running on your computer it is intended for.

Line Printer Remote Protocol

The Line Printer Remote (LPR) Protocol is software that provides printer spooling and print-server features using TCP/IP to connect printers and computers on a network.

Supported OSs

Your operating system must support TCP/IP ports for printing and be compatible with the LPR protocol.

The following OSs support ZyXEL Device's printer sharing feature.

- Microsoft Windows 95, Windows 98 SE (Second Edition), Windows Me, Windows NT 4.0, Windows 2000, Windows XP or Macintosh OS X.

23.1.2 Before You Begin

To configure the print server you need the following:

- Your ZyXEL Device must be connected to your computer and any other devices on your network. The USB printer must be connected to your ZyXEL Device.
- A USB printer with the driver already installed on your computer.
- The computers on your network must have the printer software already installed before they can create a TCP/IP port for printing via the network. Follow your printer manufacturers instructions on how to install the printer software on your computer.

Note: Your printer's installation instructions may ask that you connect the printer to your computer. Connect your printer to the ZyXEL Device instead.

23.1.3 What You Can Do with Printer Sharing

In this section you can:

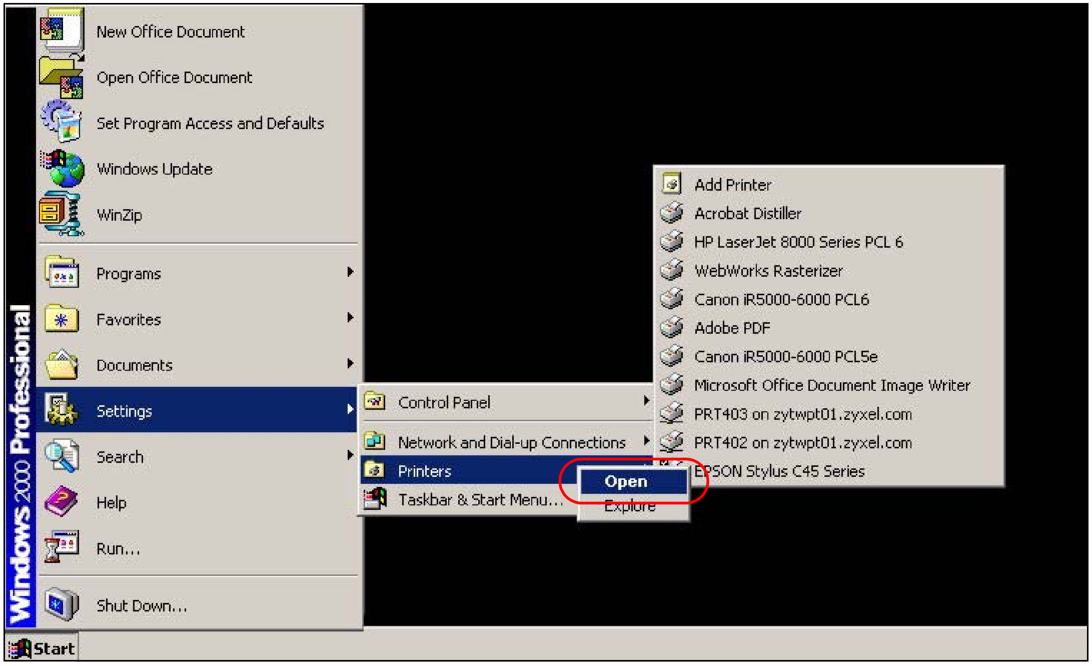
- Configure a TCP/IP Printer Port
- Add a New Printer Using Windows
- Add a New Printer Using Macintosh OS X

Configure a TCP/IP Printer Port

This example shows how you can configure a TCP/IP printer port. This example is done using the Windows 2000 Professional operating system. Some menu items may look different on your operating system. The TCP/IP port must be configured with the IP address of the ZyXEL Device and must use the LPR protocol to communicate with the printer. Consult your operating systems documentation for instructions on how to do this or follow the instructions below if you have a Windows 2000/XP operating system.

1 Click **Start** > **Settings**, then right click on **Printers** and select **Open**.

Figure 245 Open Printers Window

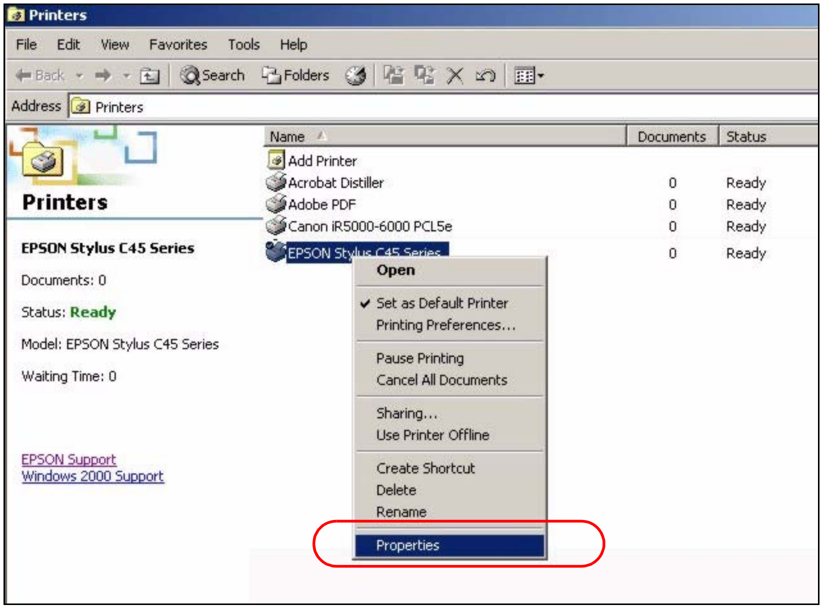


The **Printers** folder opens up. First you need to open up the properties windows for the printer you want to configure a TCP/IP port.

2 Locate your printer.

3 Right click on your printer and select **Properties**.

Figure 246 Open Printer Properties



Printers

EPSON Stylus C45 Series

Documents: 0

Status: Ready

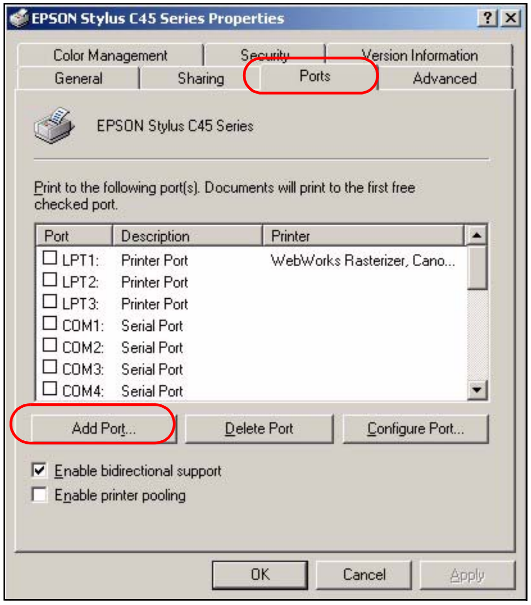
Model: EPSON Stylus C45 Series

Waiting Time: 0

Name	Documents	Status
Add Printer		
Acrobat Distiller	0	Ready
Adobe PDF	0	Ready
Canon iR5000-6000 PCL5e	0	Ready
EPSON Stylus C45 Series	0	Ready

4 Select the **Ports** tab and click **Add Port...**

Figure 247 Printer Properties Window



EPSON Stylus C45 Series

Print to the following port(s). Documents will print to the first free checked port.

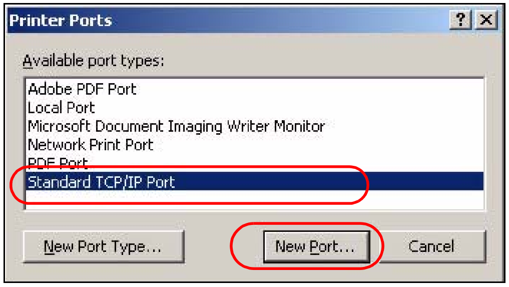
Port	Description	Printer
□ LPT1:	Printer Port	WebWorks Rasterizer, Cano...
□ LPT2:	Printer Port	
□ LPT3:	Printer Port	
□ COM1:	Serial Port	
□ COM2:	Serial Port	
□ COM3:	Serial Port	
□ COM4:	Serial Port	

☑ Enable bidirectional support

□ Enable printer pooling

5 A **Printer Ports** window appears. Select **Standard TCP/IP Port** and click **New Port...**.

Figure 248 Add a Port Window



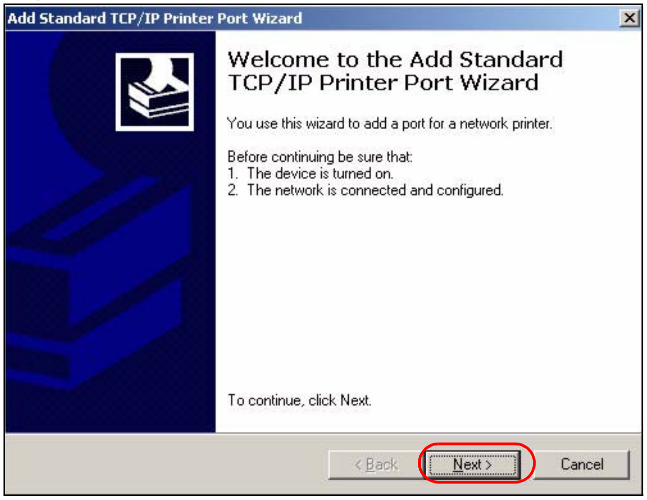
Printer Ports

Available port types:

Adobe PDF Port
Local Port
Microsoft Document Imaging Writer Monitor
Network Print Port
PDF Port
Standard TCP/IP Port

6 **Add Standard TCP/IP Printer Port Wizard** window opens up. Click **Next** to start configuring the printer port.

Figure 249 Add a Port Wizard



Add Standard TCP/IP Printer Port Wizard

Welcome to the Add Standard TCP/IP Printer Port Wizard

You use this wizard to add a port for a network printer.

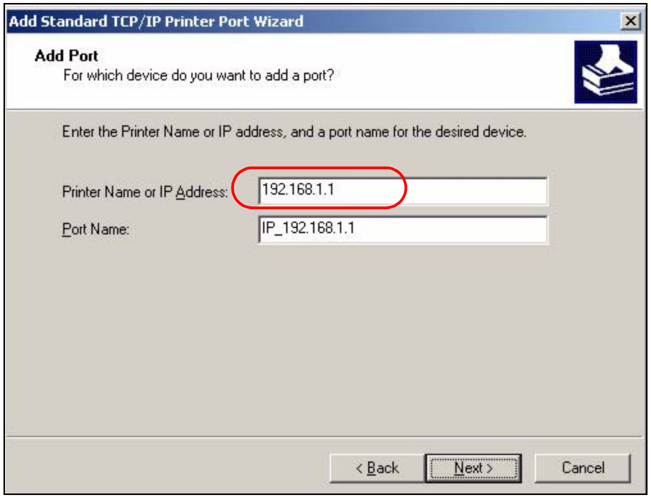
Before continuing be sure that:
1. The device is turned on.
2. The network is connected and configured.

To continue, click Next.

7 Enter the IP address of the ZyXEL Device to which the printer is connected in the **Printer Name or IP Address:** field. In our example we use the default IP address of the ZyXEL Device, 192.168.1.1. The **Port Name** field updates automatically to reflect the IP address of the port. Click **Next**.

Note: The computer from which you are configuring the TCP/IP printer port must be on the same LAN in order to use the printer sharing function.

Figure 250 Enter IP Address of the ZyXEL Device


Add Standard TCP/IP Printer Port Wizard
Add Port
For which device do you want to add a port?
< Back
Next >
Cancel

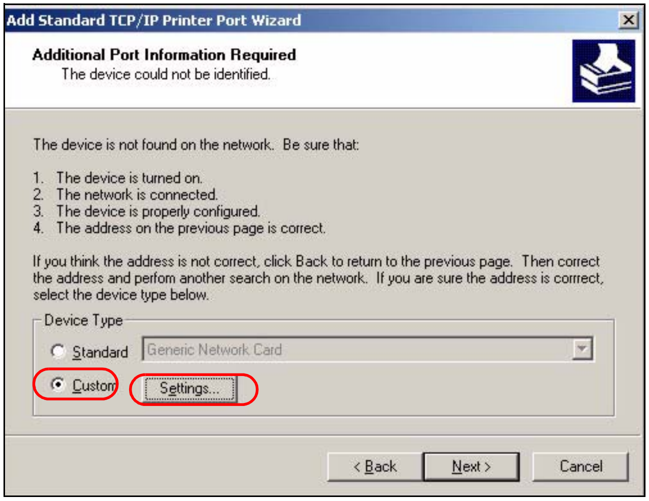
Enter the Printer Name or IP address, and a port name for the desired device.

Printer Name or IP Address: 192.168.1.1

Port Name: IP_192.168.1.1

8 Select **Custom** under **Device Type** and click **Settings**.

Figure 251 Custom Port Settings


Add Standard TCP/IP Printer Port Wizard
Additional Port Information Required
The device could not be identified.
Device Type
Settings...
< Back
Next >
Cancel

The device is not found on the network. Be sure that:

1. The device is turned on.
2. The network is connected.
3. The device is properly configured.
4. The address on the previous page is correct.

If you think the address is not correct, click Back to return to the previous page. Then correct the address and perfom another search on the network. If you are sure the address is correct, select the device type below.

○ Standard Generic Network Card

● Custom

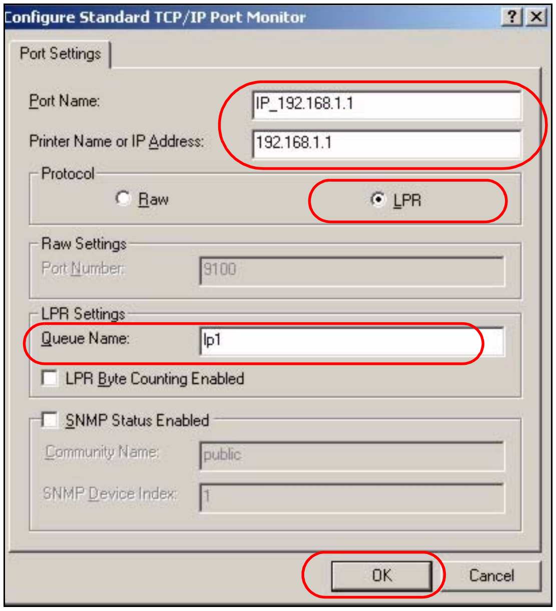
9 Confirm the IP address of the ZyXEL Device in the IP Address field.

10 Select **LPR** under **Protocol**.

11 Type the LPR queue name of your printer model in the **Queue Name** field and click **OK**. Refer to your printer documentation for the LPR queue name. Some

printer models accept any name you want to use, in this case you can enter a short descriptive name for the **Queue Name**.

Figure 252 Custom Port Settings



Configure Standard TCP/IP Port Monitor

Port Settings

Port Name: IP_192.168.1.1

Printer Name or IP Address: 192.168.1.1

Protocol: ○ Raw ● LPR

Raw Settings

Port Number: 9100

LPR Settings

Queue Name: lp1

□ LPR Byte Counting Enabled

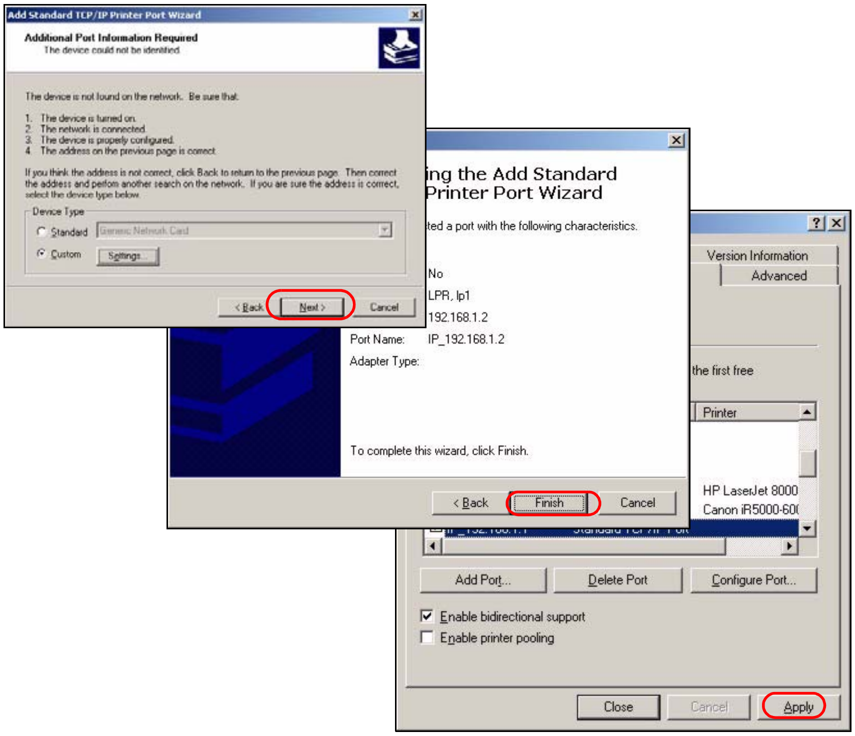
□ SNMP Status Enabled

Community Name: public

SNMP Device Index: 1

12 Continue through the wizard, apply your settings and close the wizard window.

Figure 253 Finish Adding the TCP/IP Port



Add Standard TCP/IP Printer Port Wizard

Additional Port Information Required

The device could not be identified.

The device is not found on the network. Be sure that:

1. The device is turned on.
2. The network is connected.
3. The device is properly configured.
4. The address on the previous page is correct.

If you think the address is not correct, click Back to return to the previous page. Then correct the address and perform another search on the network. If you are sure the address is correct, select the device type below.

Device Type

○ Standard Generic Network Card

● Custom Settings...

ing the Add Standard Printer Port Wizard

ted a port with the following characteristics.

No

LPR, lp1

192.168.1.2

Port Name: IP_192.168.1.2

Adapter Type:

To complete this wizard, click Finish.

☑ Enable bidirectional support

□ Enable printer pooling

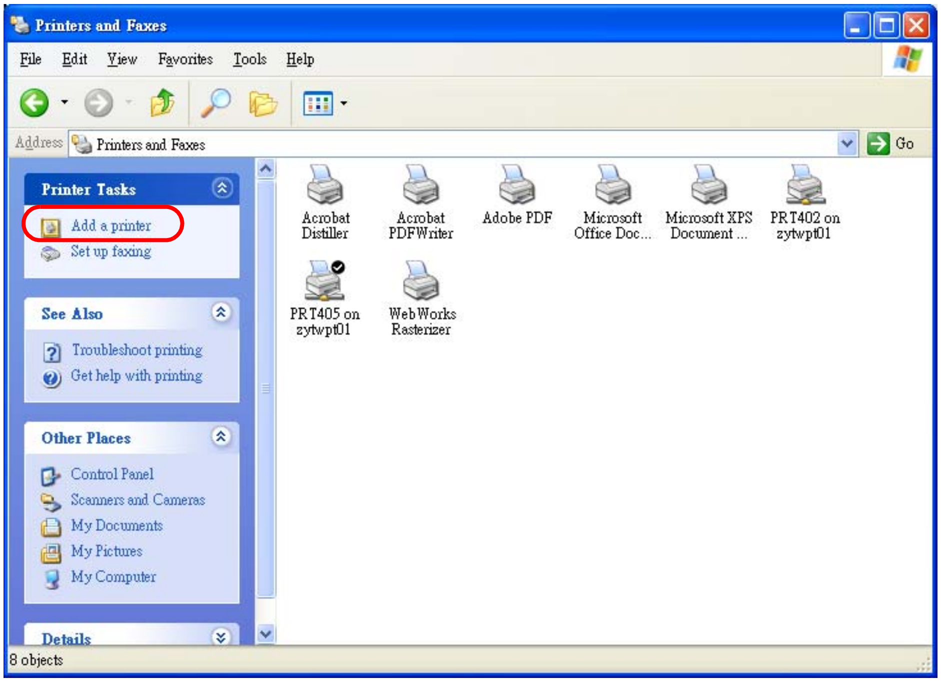
13 Repeat steps 1 to 12 to add this printer to other computers on your network.

Add a New Printer Using Windows

This example shows how to connect a printer to your ZyXEL Device using the Windows XP Professional operating system. Some menu items may look different on your operating system.

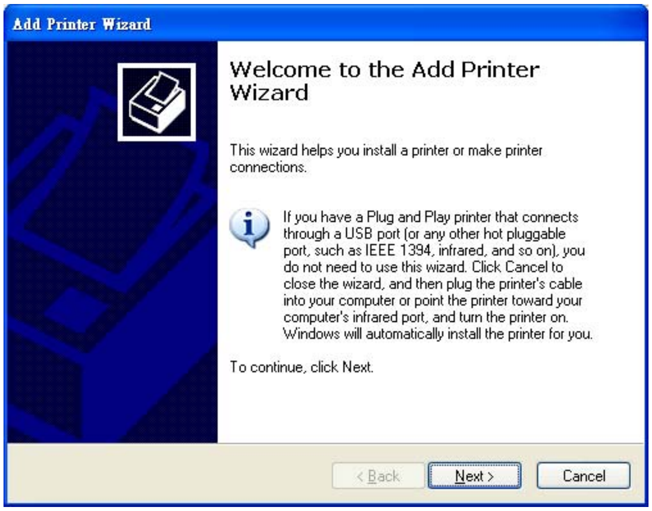
1 Click **Start** > **Control Panel** > **Printers and Faxes** to open the **Printers and Faxes** screen. Click **Add a Printer**.

Figure 254 Printers Folder



2 The **Add Printer Wizard** screen displays. Click **Next**.

Figure 255 Add Printer Wizard: Welcome



Welcome to the Add Printer Wizard

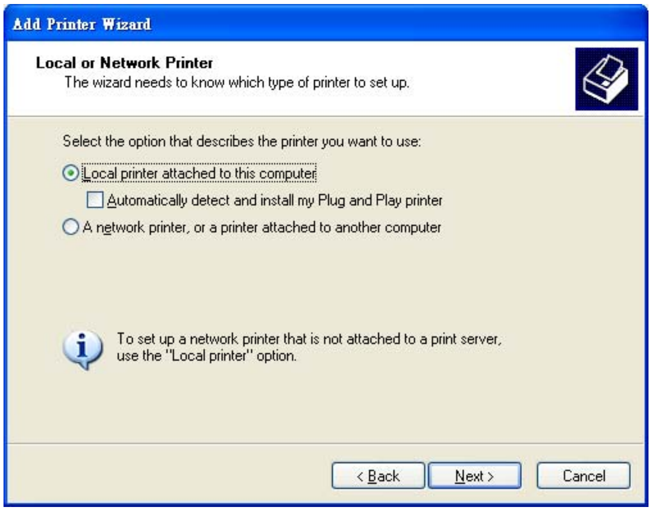
This wizard helps you install a printer or make printer connections.

If you have a Plug and Play printer that connects through a USB port (or any other hot pluggable port, such as IEEE 1394, infrared, and so on), you do not need to use this wizard. Click Cancel to close the wizard, and then plug the printer's cable into your computer or point the printer toward your computer's infrared port, and turn the printer on. Windows will automatically install the printer for you.

To continue, click Next.

3 Select **Local printer attached to this computer** and click **Next**.

Figure 256 Add Printer Wizard: Local or Network Printer



Add Printer Wizard

Local or Network Printer

The wizard needs to know which type of printer to set up.

Select the option that describes the printer you want to use:

● Local printer attached to this computer

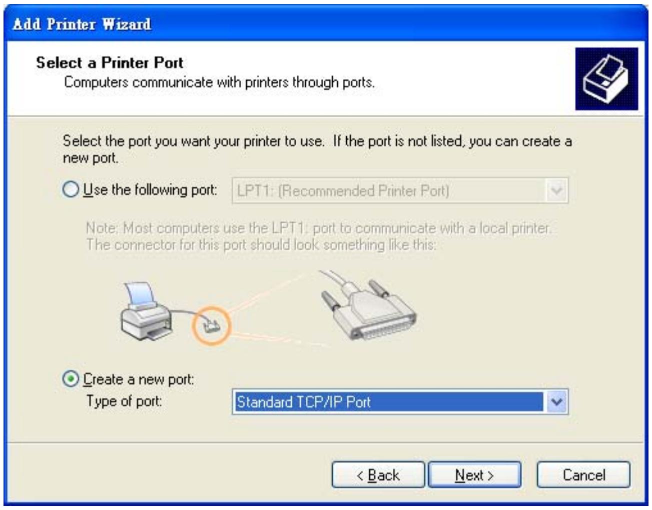
□ Automatically detect and install my Plug and Play printer

○ A network printer, or a printer attached to another computer

To set up a network printer that is not attached to a print server, use the "Local printer" option.

4 Select **Create a new port** and **Standard TCP/IP Port**. Click **Next**.

Figure 257 Add Printer Wizard: Select the Printer Port



Add Printer Wizard

Select a Printer Port

Computers communicate with printers through ports.

Select the port you want your printer to use. If the port is not listed, you can create a new port.

○ Use the following port: LPT1: (Recommended Printer Port)

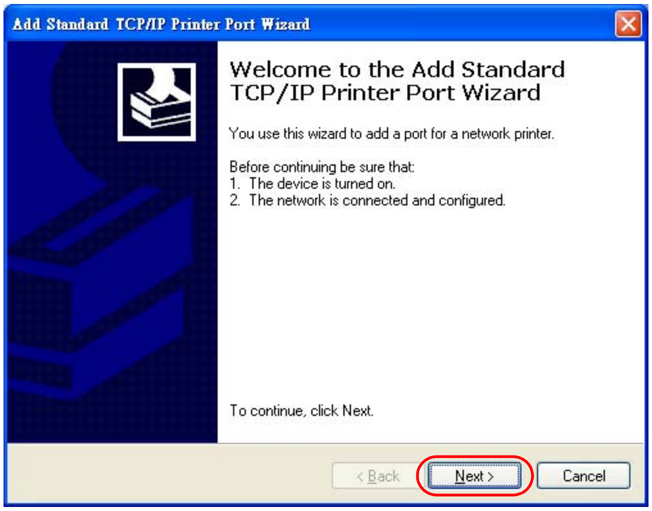
Note: Most computers use the LPT1: port to communicate with a local printer. The connector for this port should look something like this:

● Create a new port:

Type of port: Standard TCP/IP Port

5 **Add Standard TCP/IP Printer Port Wizard** window opens up. Click **Next** to start configuring the printer port.

Figure 258 Add a Port Wizard



Add Standard TCP/IP Printer Port Wizard

Welcome to the Add Standard TCP/IP Printer Port Wizard

You use this wizard to add a port for a network printer.

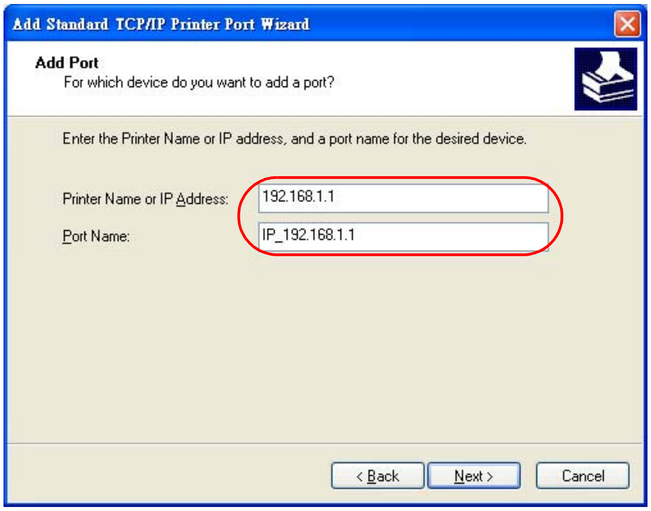
Before continuing be sure that:
1. The device is turned on.
2. The network is connected and configured.

To continue, click Next.

6 Enter the IP address of the ZyXEL Device to which the printer is connected in the **Printer Name or IP Address:** field. In our example we use the default IP address of the ZyXEL Device, 192.168.1.1. The **Port Name** field updates automatically to reflect the IP address of the port. Click **Next**.

Note: The computer from which you are configuring the TCP/IP printer port must be on the same LAN in order to use the printer sharing function.

Figure 259 Enter IP Address of the ZyXEL Device



Add Standard TCP/IP Printer Port Wizard

Add Port
For which device do you want to add a port?

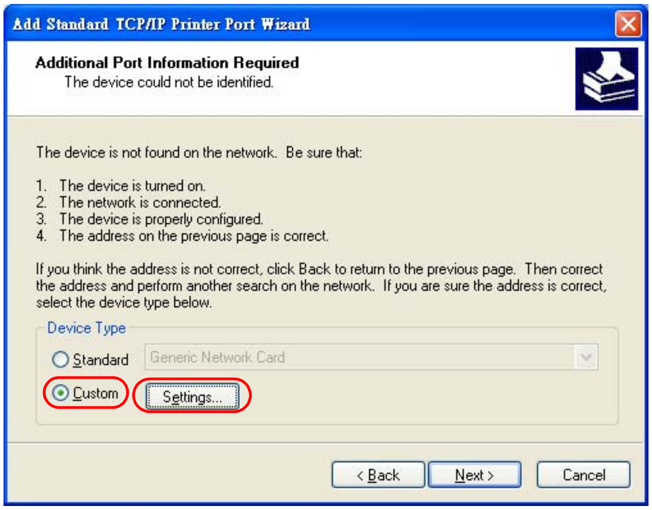
Enter the Printer Name or IP address, and a port name for the desired device.

Printer Name or IP Address: 192.168.1.1

Port Name: IP_192.168.1.1

7 Select **Custom** under **Device Type** and click **Settings**.

Figure 260 Custom Port Settings



Add Standard TCP/IP Printer Port Wizard

Additional Port Information Required

The device could not be identified.

The device is not found on the network. Be sure that:

1. The device is turned on.
2. The network is connected.
3. The device is properly configured.
4. The address on the previous page is correct.

If you think the address is not correct, click Back to return to the previous page. Then correct the address and perform another search on the network. If you are sure the address is correct, select the device type below.

Device Type

○ Standard Generic Network Card

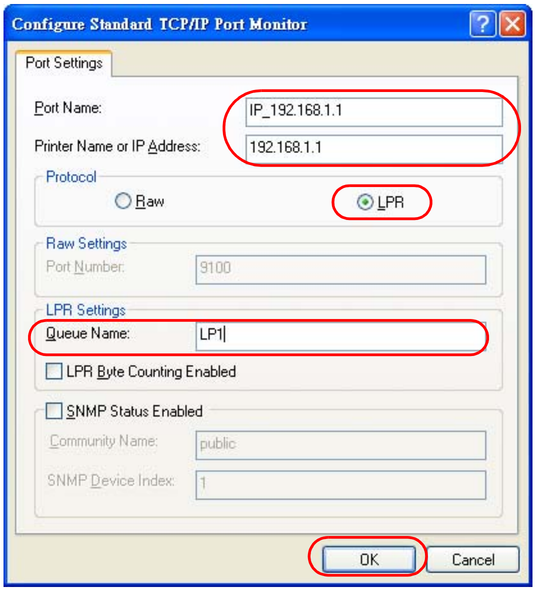
● Custom Settings...

8 Confirm the IP address of the ZyXEL Device in the Printer **Name or IP Address** field.

9 Select **LPR** under **Protocol**.

10 Type **LP1** in the **Queue Name** field and click **OK** to go back to the previous screen and click **Next**.

Figure 261 Custom Port Settings



Configure Standard TCP/IP Port Monitor

Port Settings

Port Name: IP_192.168.1.1

Printer Name or IP Address: 192.168.1.1

Protocol

○ Raw ● LPR

Raw Settings

Port Number: 9100

LPR Settings

Queue Name: LP1

□ LPR Byte Counting Enabled

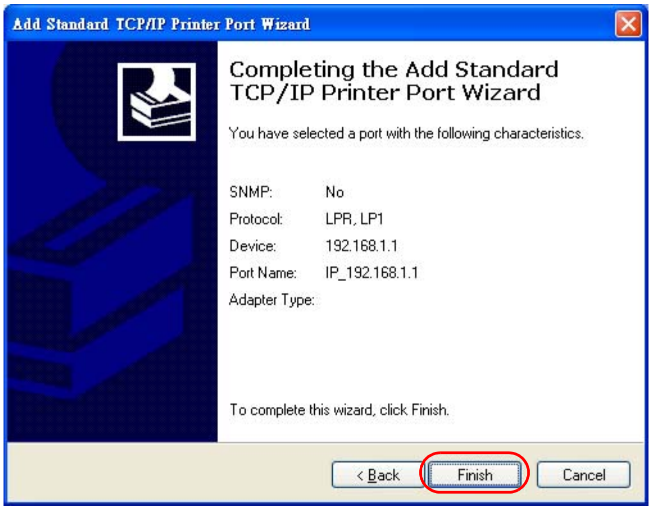
□ SNMP Status Enabled

Community Name: public

SNMP Device Index: 1

11 Click **Finish** to close the wizard window.

Figure 262 Finish Adding the TCP/IP Port



Add Standard TCP/IP Printer Port Wizard

Completing the Add Standard TCP/IP Printer Port Wizard

You have selected a port with the following characteristics.

SNMP:	No
Protocol:	LPR, LP1
Device:	192.168.1.1
Port Name:	IP_192.168.1.1
Adapter Type:	

To complete this wizard, click Finish.

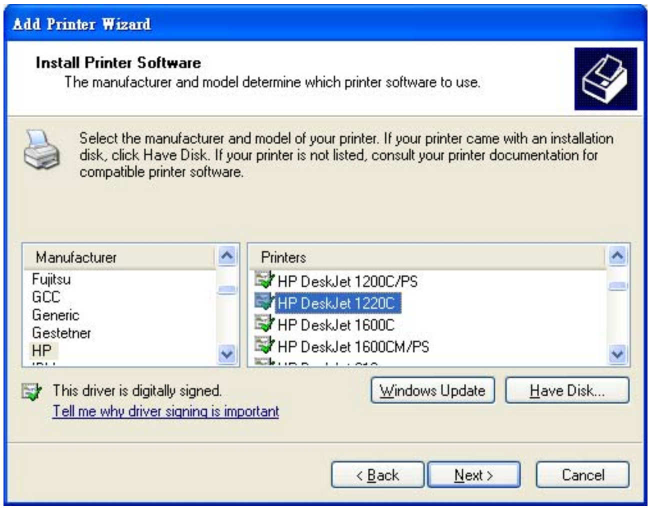
12 Select the make of the printer that you want to connect to the print server in the **Manufacturer** list of printers.

13 Select the printer model from the list of **Printers**.

14 If your printer is not displayed in the list of **Printers**, you can insert the printer driver installation CD/disk or download the driver file to your computer, click **Have Disk…** and install the new printer driver.

15 Click **Next** to continue.

Figure 263 Add Printer Wizard: Printer Driver



Add Printer Wizard

Install Printer Software

The manufacturer and model determine which printer software to use.

Select the manufacturer and model of your printer. If your printer came with an installation disk, click Have Disk. If your printer is not listed, consult your printer documentation for compatible printer software.

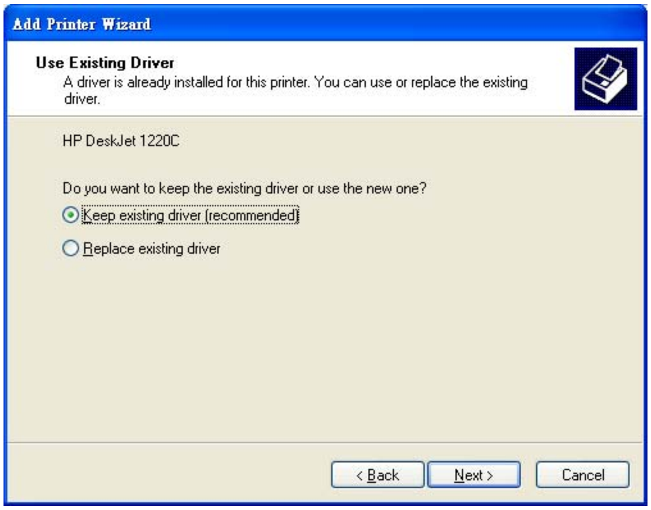
Manufacturer	Printers
Fujitsu	HP DeskJet 1200C/PS
GCC	HP DeskJet 1220C
Generic	HP DeskJet 1600C
Gestetner	HP DeskJet 1600CM/PS
HP	

This driver is digitally signed.

Tell me why driver signing is important

16 If the following screen displays, select **Keep existing driver** radio button and click **Next** if you already have a printer driver installed on your computer and you do not want to change it. Otherwise, select **Replace existing driver** to replace it with the new driver you selected in the previous screen and click **Next**.

Figure 264 Add Printer Wizard: Use Existing Driver



Add Printer Wizard

Use Existing Driver
A driver is already installed for this printer. You can use or replace the existing driver.

HP DeskJet 1220C

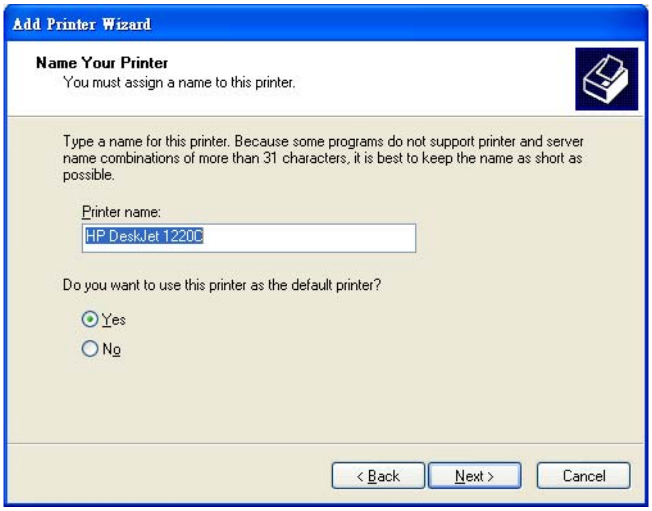
Do you want to keep the existing driver or use the new one?

● Keep existing driver (recommended)

○ Replace existing driver

17 Type a name to identify the printer and then click **Next** to continue.

Figure 265 Add Printer Wizard: Name Your Printer



Add Printer Wizard

Name Your Printer
You must assign a name to this printer.

Type a name for this printer. Because some programs do not support printer and server name combinations of more than 31 characters, it is best to keep the name as short as possible.

Printer name: HP DeskJet 1220C

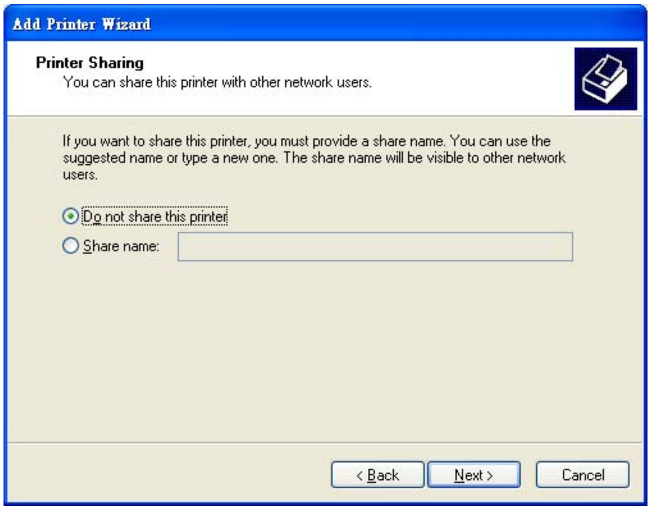
Do you want to use this printer as the default printer?

● Yes

○ No

18 The ZyXEL Device is a print server itself and you do not need to have your computer act as a print server by sharing the printer with other users in the same network; just select **Do not share this printer** and click **Next** to proceed to the following screen.

Figure 266 Add Printer Wizard: Printer Sharing



Add Printer Wizard

Printer Sharing

You can share this printer with other network users.

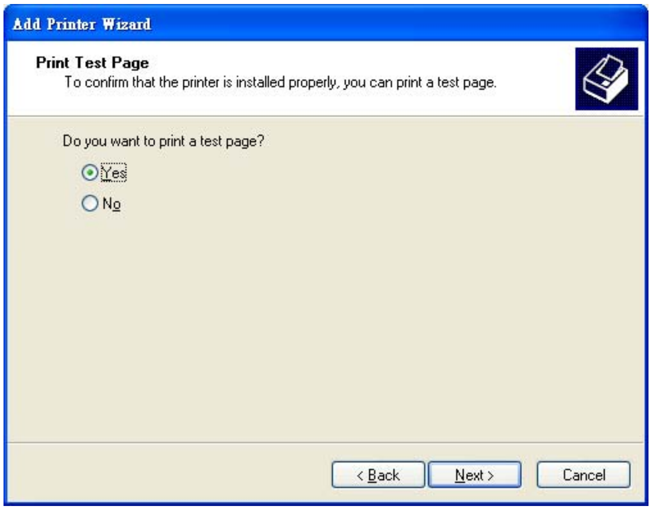
If you want to share this printer, you must provide a share name. You can use the suggested name or type a new one. The share name will be visible to other network users.

● Do not share this printer

○ Share name:

19 Select **Yes** and then click the **Next** button if you want to print a test page. A pop-up screen displays to ask if the test page printed correctly. Otherwise select **No** and then click **Next** to continue.

Figure 267 Add Printer Wizard: Print Test Page



Add Printer Wizard

Print Test Page

To confirm that the printer is installed properly, you can print a test page.

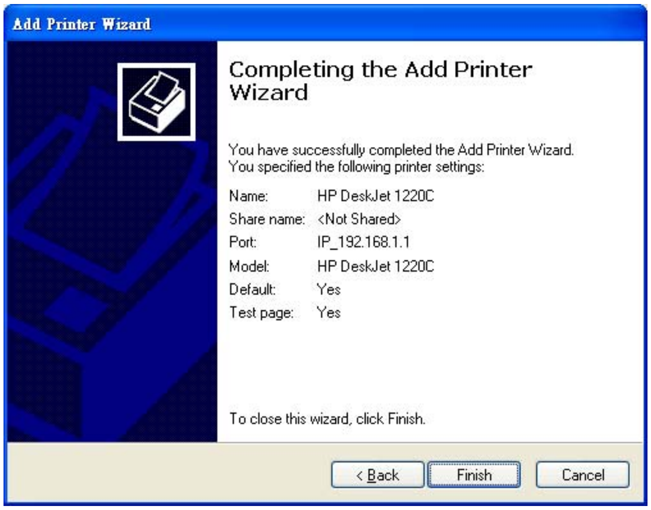
Do you want to print a test page?

● Yes

○ No

20 The following screen shows your current printer settings. Select **Finish** to complete adding a new printer.

Figure 268 Add Printer Wizard Complete



Add Printer Wizard

Completing the Add Printer Wizard

You have successfully completed the Add Printer Wizard.
You specified the following printer settings:

Name:	HP DeskJet 1220C
Share name:	<Not Shared>
Port:	IP_192.168.1.1
Model:	HP DeskJet 1220C
Default:	Yes
Test page:	Yes

To close this wizard, click Finish.

Add a New Printer Using Macintosh OS X

Complete the following steps to set up a print server driver on your Macintosh computer.

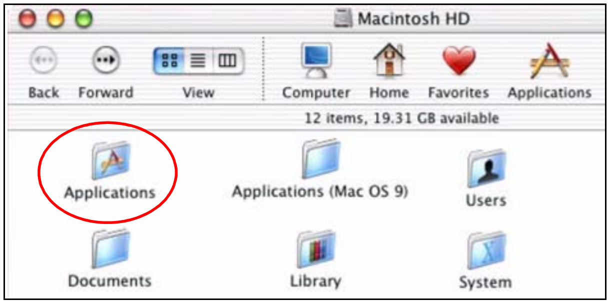
1 Click the **Print Center** icon located in the Macintosh Dock (a place holding a series of icons/shortcuts at the bottom of the desktop). Proceed to step 6 to continue. If the **Print Center** icon is not in the Macintosh Dock, proceed to the next step.

2 On your desktop, double-click the **Macintosh HD** icon to open the **Macintosh HD** window.

Figure 269 Macintosh HD

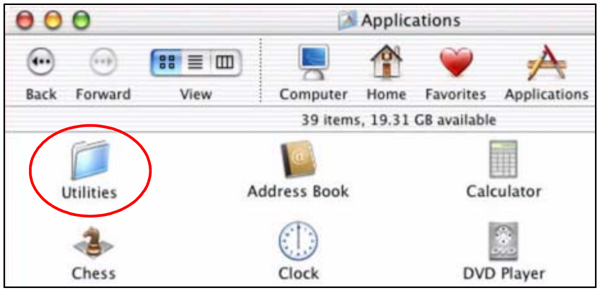
3 Double-click the **Applications** folder.

Figure 270 Macintosh HD folder



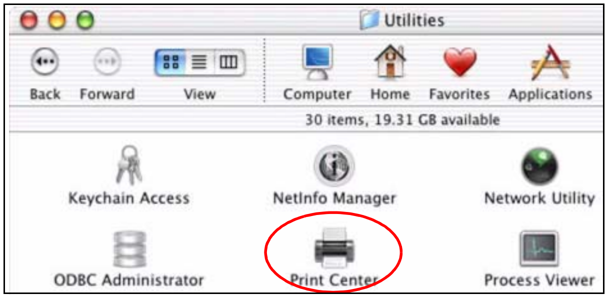
4 Double-click the **Utilities** folder.

Figure 271 Applications Folder



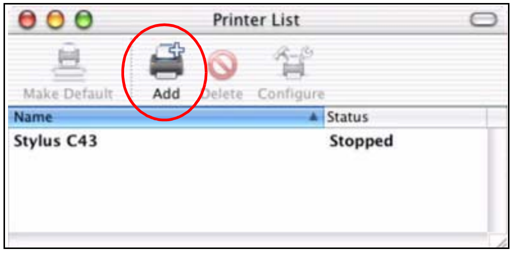
5 Double-click the **Print Center** icon.

Figure 272 Utilities Folder



6 Click the **Add** icon at the top of the screen.

Figure 273 Printer List Folder



Name	Status
Stylus C43	Stopped

7 Set up your printer in the **Printer List** configuration screen. Select **IP Printing** from the drop-down list box.

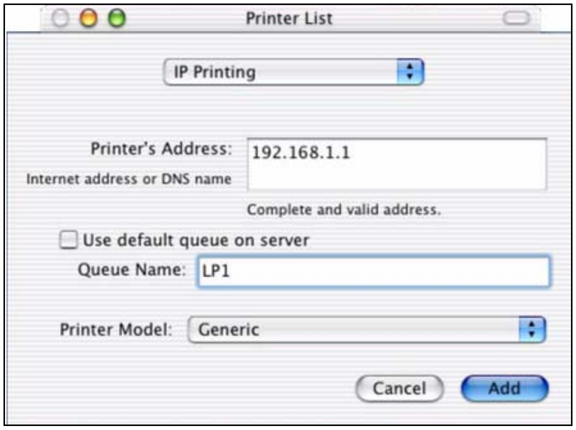
8 In the **Printer's Address** field, type the IP address of your ZyXEL Device.

9 Deselect the **Use default queue on server** check box.

10 Type **LP1** (a parallel port) in the **Queue Name** field.

11 Select your **Printer Model** from the drop-down list box. If the printer's model is not listed, select **Generic**.

Figure 274 Printer Configuration



Printer List

IP Printing

Printer's Address: 192.168.1.1

Internet address or DNS name

Complete and valid address.

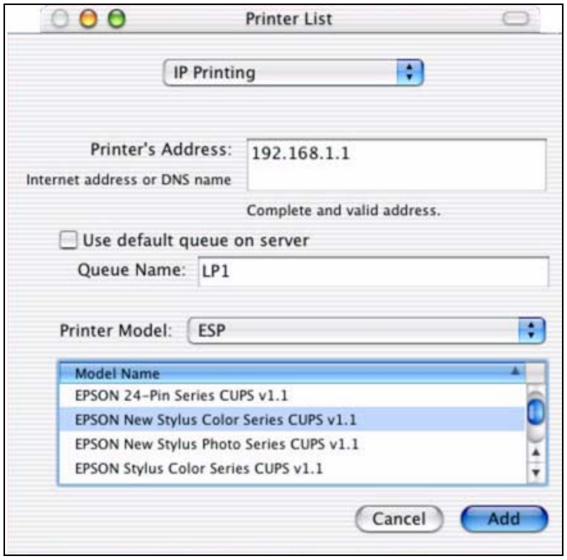
□ Use default queue on server

Queue Name: LP1

Printer Model: Generic

12 Click **Add** to select a printer model, save and close the **Printer List** configuration screen.

Figure 275 Printer Model



Printer List

IP Printing

Printer's Address: 192.168.1.1

Internet address or DNS name

Complete and valid address.

□ Use default queue on server

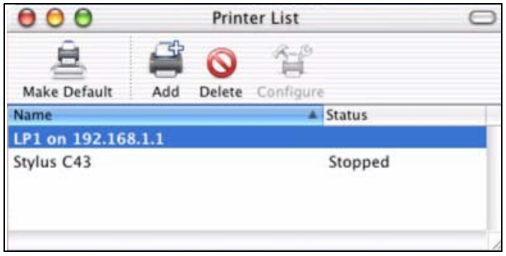
Queue Name: LP1

Printer Model: ESP

Model Name
EPSON 24-Pin Series CUPS v1.1
EPSON New Stylus Color Series CUPS v1.1
EPSON New Stylus Photo Series CUPS v1.1
EPSON Stylus Color Series CUPS v1.1

13 The **Name LP1 on 192.168.1.1** displays in the **Printer List** field. The default printer **Name** displays in bold type.

Figure 276 Print Server



Name	Status
LP1 on 192.168.1.1	
Stylus C43	Stopped

14 Your Macintosh print server driver setup is complete. You can now use the ZyXEL Device’s print server to print from a Macintosh computer.

23.2 ZyXEL Device Print Server Compatible USB Printers

The following is a list of USB printer models compatible with the ZyXEL Device print server.

Table 129 Compatible USB Printers

BRAND	MODEL
Brother	MFC7420
CANON	BJ F9000
CANON	PIXMA MP450
CANON	PIXMA MP730
CANON	PIXMA MP780
CANON	PIXMA MP830
CANON	PIXUS ip2500
CANON	PIXMA ip4200
CANON	PIXMA ip5000
CANON	PIXUS 990i
EPSON	CX3500
EPSON	CX3900
EPSON	EPL-5800
EPSON	EPL-6200L
EPSON	LP-2500
EPSON	LP-8900
EPSON	RX 510
EPSON	RX 530
EPSON	Stylus 830U
EPSON	Stylus 1270
EPSON	Stylus C43UX
EPSON	Stylus C60
EPSON	Stylus Color 670
HP	Deskjet 5550
HP	Deskjet 5652
HP	Deskjet 830C
HP	Deskjet 845C

Table 129 Compatible USB Printers (continued)

BRAND	MODEL
HP	Deskjet 1125C
HP	Deskjet 1180C
HP	Deskjet 1220C
HP	Deskjet F4185
HP	Laserjet 1200
HP	Laserjet 2200D
HP	Laserjet 2420
HP	Color Laserjet 1500L
HP	Laserjet 3015
HP	Officejet 4255
HP	Officejet 5510
HP	Officejet 5610
HP	Officejet 7210
HP	Officejet Pro L7380
HP	Photosmart 2610
HP	Photosmart 3110
HP	Photosmart 7150
HP	Photosmart 7830
HP	Photosmart C5280
HP	Photosmart D5160
HP	PSC 1350
HP	PSC 1410
IBM	Infoprint 1332
LEXMARK	Z55
LEXMARK	Z705
OKI	B4350
SAMSUNG	ML-1710
SAMSUNG	SCX-4016

PART III

Maintenance, Troubleshooting and Specifications

24

System

24.1 Overview

This chapter shows you how to configure system related settings, such as system time, password, name, the domain name and the inactivity timeout interval.

24.1.1 What You Can Do in the System Settings Screens

- Use the **General** screen (Section 24.2 on page 412) to configure system settings.
- Use the **Time Setting** screen (Section 24.3 on page 414) to set the system time.

24.1.2 What You Need to Know About System Settings

Domain Name

This is a network address that identifies the owner of a network connection. For example, in the network address “www.zyxel.com/support/files”, the domain name is “www.zyxel.com”.

DHCP

DHCP (Dynamic Host Configuration Protocol) is a method of allocating IP addresses to devices on a network from a DHCP Server. Often your ISP or a router on your network performs this function.

LAN

A LAN (local area network) is typically a network which covers a small area, made up of computers and other devices which share resources such as Internet access and printers.

24.2 The General Screen

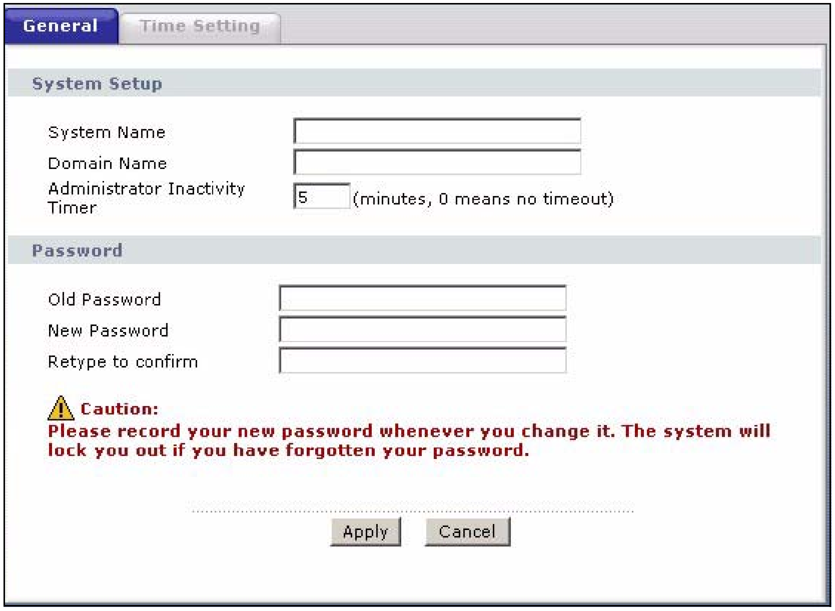
Use the **General** screen to configure system settings such as the system and domain name, inactivity timeout interval and system password.

The **System Name** is for identification purposes. However, because some ISPs check this name you should enter your computer's "Computer Name". Find the system name of your Windows computer by following one of the steps below.

- 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**.

Click **Maintenance > System** to open the **General** screen.

Figure 277 Maintenance > System > General



System Setup

System Name

Domain Name

Administrator Inactivity Timer: 5 (minutes, 0 means no timeout)

Password

Old Password

New Password

Retype to confirm

Caution:
Please record your new password whenever you change it. The system will lock you out if you have forgotten your password.

The following table describes the labels in this screen.

Table 130 Maintenance > System > General

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	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.

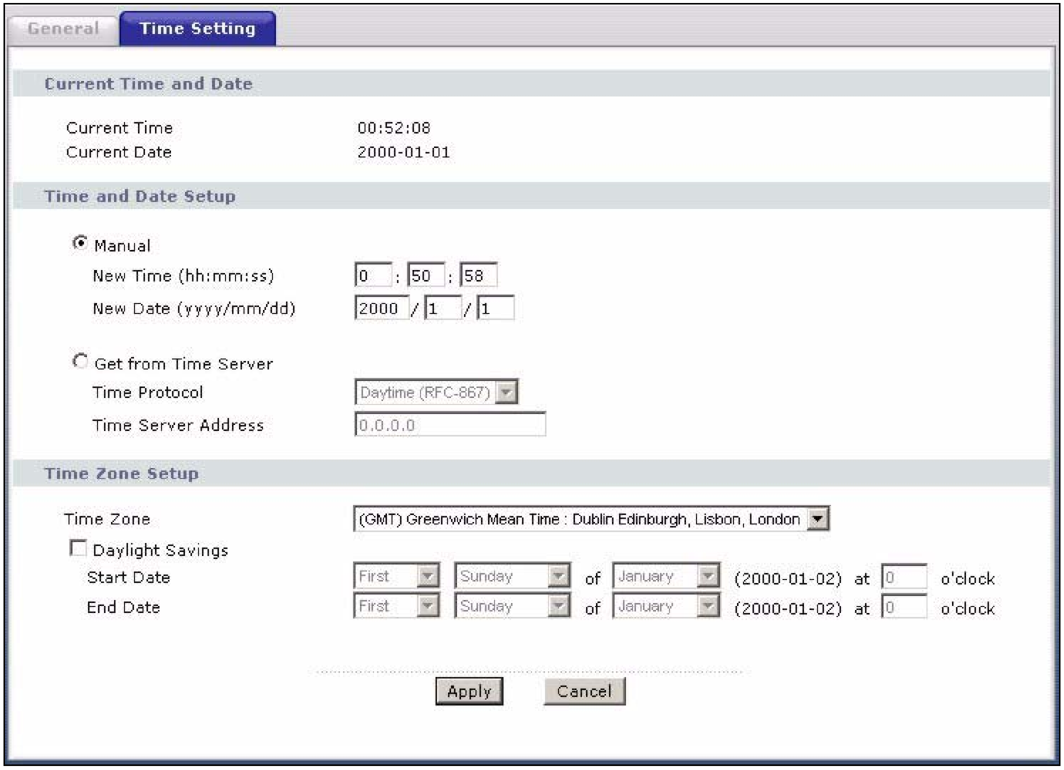
Table 130 Maintenance > System > General

LABEL	DESCRIPTION
Administrator Inactivity Timer	Type how many minutes a management session (either via the web configurator or telnet) 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).
Password	
Old Password	Type the default password or the existing password you use to access the system in this field.
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. After you change the password, use the new password to access the ZyXEL Device.
Retype to Confirm	Type the new password again for confirmation.
Apply	Click **Apply** to save your changes back to the ZyXEL Device.
Cancel	Click **Cancel** to begin configuring this screen afresh.

24.3 The Time Setting Screen

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

Figure 278 Maintenance > System > Time Setting



Current Time and Date

Current Time 00:52:08
Current Date 2000-01-01

Time and Date Setup

● Manual
New Time (hh:mm:ss) 0 : 50 : 58
New Date (yyyy/mm/dd) 2000 / 1 / 1

○ Get from Time Server
Time Protocol Daytime (RFC-867)
Time Server Address 0.0.0.0

Time Zone Setup

Time Zone (GMT) Greenwich Mean Time : Dublin Edinburgh, Lisbon, London
□ Daylight Savings
Start Date First Sunday of January (2000-01-02) at 0 o'clock
End Date First Sunday of January (2000-01-02) at 0 o'clock

The following table describes the fields in this screen.

Table 131 Maintenance > System > Time Setting

LABEL	DESCRIPTION
Current Time and Date	
Current Time	This field displays the time of your ZyXEL Device. Each time you reload this page, the ZyXEL Device synchronizes the time with the time server.
Current Date	This field displays the date of your ZyXEL Device. Each time you reload this page, the ZyXEL Device synchronizes the date with the time server.
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.

Table 131 Maintenance > System > Time Setting (continued)

LABEL	DESCRIPTION
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.
Time Protocol	Select the time service protocol that your time server sends when you turn on the ZyXEL Device. 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 (up to 20 extended ASCII characters in length) of your time server. Check with your ISP/network administrator if you are unsure of this information.
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).
Daylight Savings	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 **Daylight Savings**. 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).

Table 131 Maintenance > System > Time Setting (continued)

LABEL	DESCRIPTION
End Date	Configure the day and time when Daylight Saving Time ends if you selected **Daylight Savings**. 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 back to the ZyXEL Device.
Cancel	Click **Cancel** to begin configuring this screen afresh.

25

Logs

25.1 Overview

The web configurator allows you to choose which categories of events and/or alerts to have the ZyXEL Device log and then display the logs or have the ZyXEL Device send them to an administrator (as e-mail) or to a syslog server.

25.1.1 What You Can Do in the Log Screens

- Use the **View Log** screen (Section 25.2 on page 417) to see the logs for the categories that you selected in the **Log Settings** screen.
- Use The **Log Settings** screen (Section 25.3 on page 418) 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 record.

25.1.2 What You Need To Know About Logs

Alerts and Logs

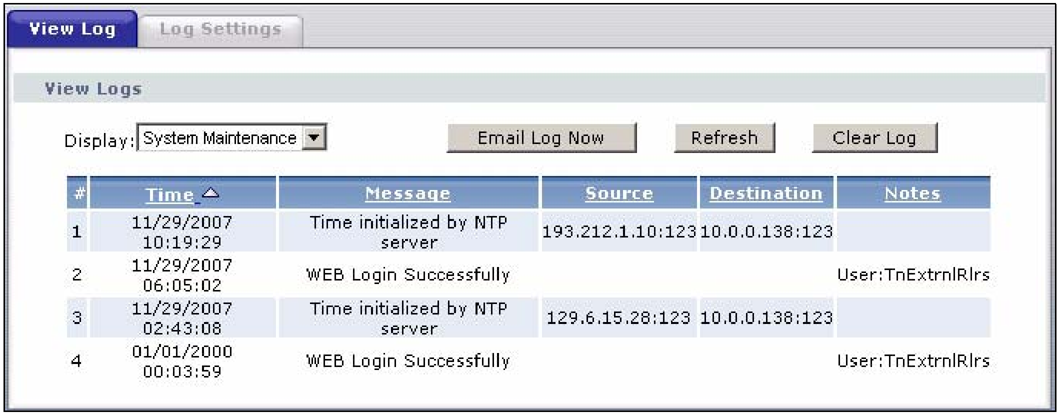
An alert is a type of log that warrants more serious attention. They include system errors, attacks (access control) and attempted access to blocked web sites. Some categories such as **System Errors** consist of both logs and alerts. You may differentiate them by their color in the **View Log** screen.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

25.2 The View Log Screen

Click **Maintenance > 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 25.3 on page 418).

Log entries in red indicate alerts. 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 279 Maintenance > Logs > View Log



Display: System Maintenance

#	Time	Message	Source	Destination	Notes
1	11/29/2007 10:19:29	Time initialized by NTP server	193.212.1.10:123	10.0.0.138:123	
2	11/29/2007 06:05:02	WEB Login Successfully			User:TnExtrnlRlrs
3	11/29/2007 02:43:08	Time initialized by NTP server	129.6.15.28:123	10.0.0.138:123	
4	01/01/2000 00:03:59	WEB Login Successfully			User:TnExtrnlRlrs

The following table describes the fields in this screen.

Table 132 Maintenance > Logs > View Log

LABEL	DESCRIPTION
Display	The categories that you select in the **Log Settings** screen 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.
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**).
Refresh	Click **Refresh** to renew the log screen.
Clear Log	Click **Clear Log** to delete all the logs.
#	This field is a sequential value and is not associated with a specific entry.
Time	This field displays the time the log was recorded.
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.
Notes	This field displays additional information about the log entry.

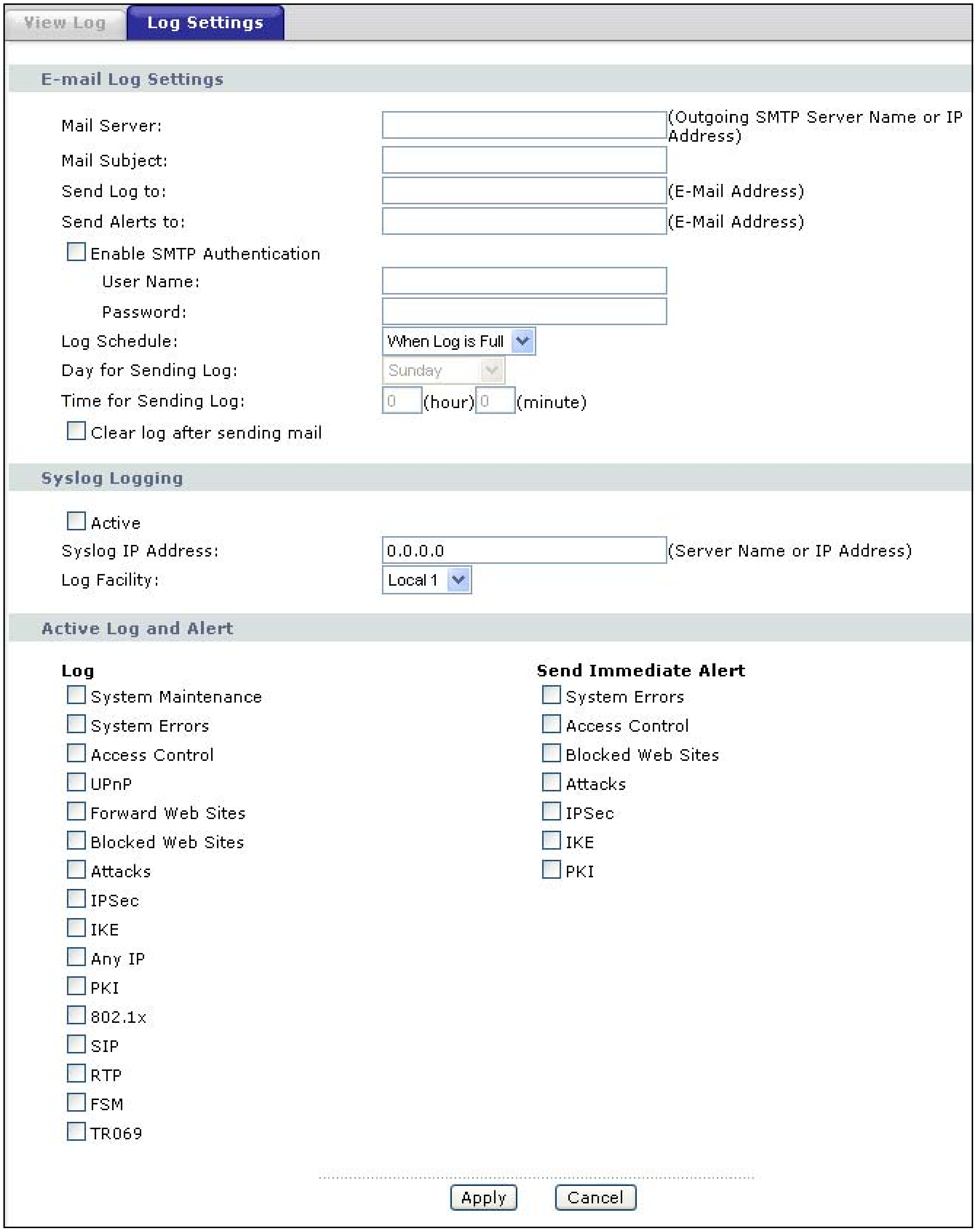
25.3 The Log Settings Screen

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 record. See Section 25.1 on page 417 for more information.

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

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

Figure 280 Maintenance > Logs > Log Settings



View Log | **Log Settings**

E-mail Log Settings

Mail Server:		(Outgoing SMTP Server Name or IP Address)
Mail Subject:		
Send Log to:		(E-Mail Address)
Send Alerts to:		(E-Mail Address)
□ Enable SMTP Authentication		
User Name:		
Password:		
Log Schedule:	When Log is Full	
Day for Sending Log:	Sunday	
Time for Sending Log:	0 (hour) 0 (minute)	
□ Clear log after sending mail		

Syslog Logging

□ Active

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

Active Log and Alert

Log

□ System Maintenance
□ System Errors
□ Access Control
□ UPnP
□ Forward Web Sites
□ Blocked Web Sites
□ Attacks
□ IPSec
□ IKE
□ Any IP
□ PKI
□ 802.1x
□ SIP
□ RTP
□ FSM
□ TR069

Send Immediate Alert

□ System Errors
□ Access Control
□ Blocked Web Sites
□ Attacks
□ IPSec
□ IKE
□ PKI

Apply | Cancel

The following table describes the fields in this screen.

Table 133 Maintenance > 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. Not all ZyXEL Device models have this field.
Send Log to	The ZyXEL Device sends logs to the e-mail address specified in this field. If this field is left blank, the ZyXEL Device does not send logs via e-mail.
Send Alerts to	Alerts are real-time notifications that are sent as soon as an event, such as a DoS attack, system error, or forbidden web access attempt occurs. Enter the E-mail address where the alert messages will be sent. Alerts include system errors, attacks and attempted access to blocked web sites. If this field is left blank, alert messages will not be sent via E-mail.
Enable 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.
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.
Clear log after sending mail	Select this to delete all the logs after the ZyXEL Device sends an E-mail of the logs.
Syslog Logging	The ZyXEL Device sends a log to an external syslog server.
Active	Click **Active** to enable syslog logging.

Table 133 Maintenance > Logs > Log Settings

LABEL	DESCRIPTION
Syslog IP Address	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 syslog server manual for more information.
Active Log and Alert	
Log	Select the categories of logs that you want to record.
Send Immediate Alert	Select log categories for which you want the ZyXEL Device to send E-mail alerts immediately.
Apply	Click **Apply** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to return to the previously saved settings.

25.4 SMTP Error Messages

If there are difficulties in sending e-mail the following error message appears.

“SMTP action request failed. ret= ??". The “??"are described in the following table.

Table 134 SMTP Error Messages

-1 means ZyXEL Device out of socket
-2 means tcp SYN fail
-3 means smtp server OK fail
-4 means HELO fail
-5 means MAIL FROM fail
-6 means RCPT TO fail
-7 means DATA fail
-8 means mail data send fail

25.4.1 Example E-mail Log

An "End of Log" message displays for each mail in which a complete log has been sent. The following is an example of a log sent by e-mail.

- You may edit the subject title.
- The date format here is Day-Month-Year.
- The date format here is Month-Day-Year. The time format is Hour-Minute-Second.

- "End of Log" message shows that a complete log has been sent.

Figure 281 E-mail Log Example

```
Subject:
        Firewall Alert From
   Date:
        Fri, 07 Apr 2000 10:05:42
   From:
        user@zyxel.com
     To:
        user@zyxel.com
  1|Apr  7 00 |From:192.168.1.1     To:192.168.1.255   |default policy  |forward
   | 09:54:03 |UDP     src port:00520 dest port:00520  |<1,00>          |
  2|Apr  7 00 |From:192.168.1.131   To:192.168.1.255   |default policy  |forward
   | 09:54:17 |UDP     src port:00520 dest port:00520  |<1,00>          |
  3|Apr  7 00 |From:192.168.1.6     To:10.10.10.10 |match           |forward
   | 09:54:19 |UDP     src port:03516 dest port:00053  |<1,01>          |
……………………………..{snip}…………………………………..
……………………………..{snip}…………………………………..
126|Apr  7 00 |From:192.168.1.1     To:192.168.1.255   |match           |forward
   | 10:05:00 |UDP     src port:00520 dest port:00520  |<1,02>          |
127|Apr  7 00 |From:192.168.1.131   To:192.168.1.255   |match           |forward
   | 10:05:17 |UDP     src port:00520 dest port:00520  |<1,02>          |
128|Apr  7 00 |From:192.168.1.1     To:192.168.1.255   |match           |forward
   | 10:05:30 |UDP     src port:00520 dest port:00520  |<1,02>          |
End of Firewall Log
```

25.5 Log Descriptions

This section provides descriptions of example log messages.

Table 135 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, 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.

Table 135 System Maintenance Logs (continued)

LOG MESSAGE	DESCRIPTION
`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.
`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.

Table 136 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.

Table 137 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.

Table 138 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.Default timeout values:ICMP idle timeout (s): 60UDP idle timeout (s): 60TCP connection (three way handshaking) timeout (s): 30TCP FIN-wait timeout (s): 60TCP idle (established) timeout (s): 3600

Table 138 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 139 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 148 on page 428.

Table 140 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 141 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 142 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 143 UPnP Logs

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

Table 144 Content Filtering Logs

LOG MESSAGE	DESCRIPTION
`%s: block keyword`	The content of a requested web page matched a user defined keyword.
`%s`	The system forwarded web content.

For type and code details, see Table 148 on page 428.

Table 145 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.

Table 146 802.1X Logs

LOG MESSAGE	DESCRIPTION
`RADIUS accepts user.`	A user was authenticated by the RADIUS Server.
`RADIUS rejects user. Pls check RADIUS Server.`	A user was not authenticated by the RADIUS Server. Please check the RADIUS Server.
`User logout because of session timeout expired.`	The router logged out a user whose session expired.

Table 146 802.1X Logs (continued)

LOG MESSAGE	DESCRIPTION
`User logout because of user deassociation.`	The router logged out a user who ended the session.
`User logout because of no authentication response from user.`	The router logged out a user from which there was no authentication response.
`User logout because of idle timeout expired.`	The router logged out a user whose idle timeout period expired.
`User logout because of user request.`	A user logged out.
`No response from RADIUS. Pls check RADIUS Server.`	There is no response message from the RADIUS server, please check the RADIUS server.
`Use RADIUS to authenticate user.`	The RADIUS server is operating as the authentication server.
`No Server to authenticate user.`	There is no authentication server to authenticate a user.

Table 147 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.
(L to L/ZyXEL Device)	LAN to LAN/ ZyXEL Device	ACL set for packets traveling from the LAN to the LAN or the ZyXEL Device.
(W to W/ZyXEL Device)	WAN to WAN/ ZyXEL Device	ACL set for packets traveling from the WAN to the WAN or the ZyXEL Device.

Table 148 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

Table 148 ICMP Notes (continued)

TYPE	CODE	DESCRIPTION
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
	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

Table 149 Syslog Logs

LOG MESSAGE	DESCRIPTION
`<Facility*8 + Severity>Mon dd hr:mm:ss hostname src="<srcIP:srcPort>" dst="<dstIP:dstPort>" msg="<msg>" note="<note>" devID="<mac address last three numbers>" 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 various log charts throughout this appendix. The "devID" is the last three characters of the MAC address of the router's LAN port. The "cat" is the same as the category in the router's logs.

Table 150 SIP Logs

LOG MESSAGE	DESCRIPTION
`SIP Registration Success by SIP:SIP Phone Number`	The listed SIP account was successfully registered with a SIP register server.
`SIP Registration Fail by SIP:SIP Phone Number`	An attempt to register the listed SIP account with a SIP register server was not successful.
`SIP UnRegistration Success by SIP:SIP Phone Number`	The listed SIP account's registration was deleted from the SIP register server.
`SIP UnRegistration Fail by SIP:SIP Phone Number`	An attempt to delete the listed SIP account's registration from the SIP register server failed.

Table 151 RTP Logs

LOG MESSAGE	DESCRIPTION
`Error, RTP init fail`	The initialization of an RTP session failed.
`Error, Call fail: RTP connect fail`	A VoIP phone call failed because the RTP session could not be established.
`Error, RTP connection cannot close`	The termination of an RTP session failed.

Table 152 FSM Logs: Caller Side

LOG MESSAGE	DESCRIPTION
`VoIP Call Start Ph[Phone Port Number] <- Outgoing Call Number`	Someone used a phone connected to the listed phone port to initiate a VoIP call to the listed destination.
`VoIP Call Established Ph[Phone Port] -> Outgoing Call Number`	Someone used a phone connected to the listed phone port to make a VoIP call to the listed destination.
`VoIP Call End Phone[Phone Port]`	A VoIP phone call made from a phone connected to the listed phone port has terminated.

Table 153 FSM Logs: Callee Side

LOG MESSAGE	DESCRIPTION
`VoIP Call Start from SIP[SIP Port Number]`	A VoIP phone call came to the ZyXEL Device from the listed SIP number.
`VoIP Call Established Ph[Phone Port] <- Outgoing Call Number`	A VoIP phone call was set up from the listed SIP number to the ZyXEL Device.
`VoIP Call End Phone[Phone Port]`	A VoIP phone call that came into the ZyXEL Device has terminated.

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

Table 154 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

26

Call History

26.1 Overview

The ZyXEL Device keeps track of when you use the phone ports for calls.

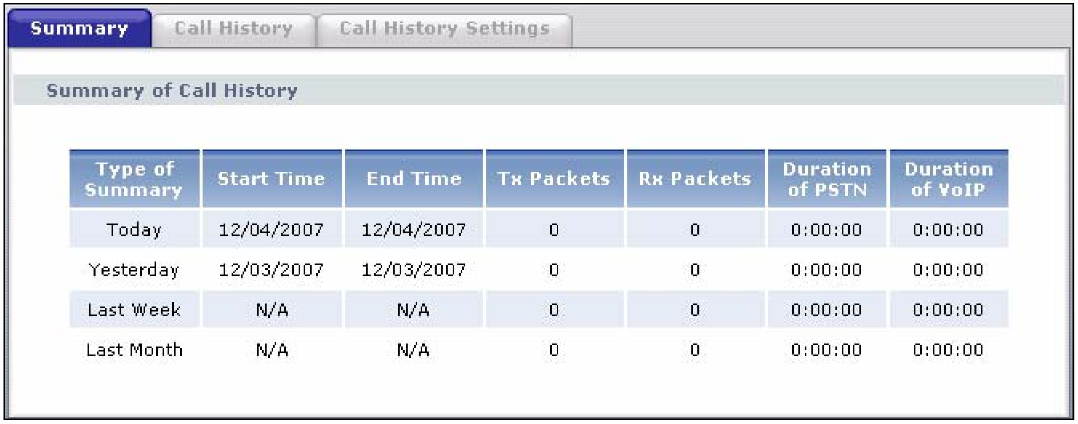
26.1.1 What You Can Do in the Call History Screens

- Use the **Summary** screen (Section 26.2 on page 433) to view a summary of the calls performed via the ZyXEL Device within a certain period.
- Use the **Call History** screen (Section 26.3 on page 434) to see the details of the calls performed on the ZyXEL Device.
- Use the **Call History Settings** screen (Section 26.4 on page 435) to configure to where the ZyXEL Device is to send call records and the schedule for when the ZyXEL Device is to send or save the call records.

26.2 Call History Summary Screen

Click **Maintenance > Call History** to open the **Summary** screen. Use the **Summary** screen to view a summary of the calls performed via the ZyXEL Device within a certain period.

Figure 282 Maintenance > Call History > Summary



Summary of Call History

Type of Summary	Start Time	End Time	Tx Packets	Rx Packets	Duration of PSTN	Duration of VoIP
Today	12/04/2007	12/04/2007	0	0	0:00:00	0:00:00
Yesterday	12/03/2007	12/03/2007	0	0	0:00:00	0:00:00
Last Week	N/A	N/A	0	0	0:00:00	0:00:00
Last Month	N/A	N/A	0	0	0:00:00	0:00:00

The following table describes the fields in this screen.

Table 155 Maintenance > Call History > Summary

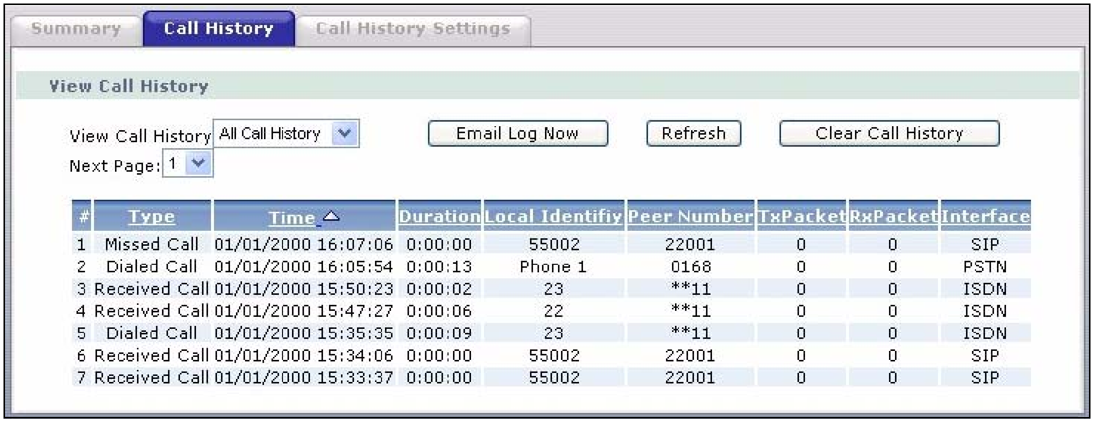
LABEL	DESCRIPTION
Type of Summary	This shows the time period.
Start Time	This shows the date when the period starts.
End Time	This shows the date when the period ends.
Tx Packets	This shows the number of voice packets the ZyXEL Device transmitted within this period.
Rx Packets	This shows the number of voice packets the ZyXEL Device received within this period.
Duration of PSTN	This shows how long the analog calls lasted within this period.
Duration of VoIP	This shows how long the Voice over Internet calls lasted within this period.

26.3 Viewing the Call History

Click **Maintenance > Call History > Call History** to open the **Call History** screen. Use the **Call History** screen to see the details of the calls performed on the ZyXEL Device.

The call history buffer can hold up to 150 entries. When the call history buffer fills, old records are deleted as new ones are added. Click a column heading to sort the entries. A triangle indicates ascending or descending sort order.

Figure 283 Maintenance > Call History > Call History



View Call History: All Call History
Next Page: 1

#	Type	Time	Duration	Local Identifiy	Peer Number	TxPacket	RxPacket	Interface
1	Missed Call	01/01/2000 16:07:06	0:00:00	55002	22001	0	0	SIP
2	Dialed Call	01/01/2000 16:05:54	0:00:13	Phone 1	0168	0	0	PSTN
3	Received Call	01/01/2000 15:50:23	0:00:02	23	**11	0	0	ISDN
4	Received Call	01/01/2000 15:47:27	0:00:06	22	**11	0	0	ISDN
5	Dialed Call	01/01/2000 15:35:35	0:00:09	23	**11	0	0	ISDN
6	Received Call	01/01/2000 15:34:06	0:00:00	55002	22001	0	0	SIP
7	Received Call	01/01/2000 15:33:37	0:00:00	55002	22001	0	0	SIP

The following table describes the fields in this screen.

Table 156 Maintenance > Call History > Call History

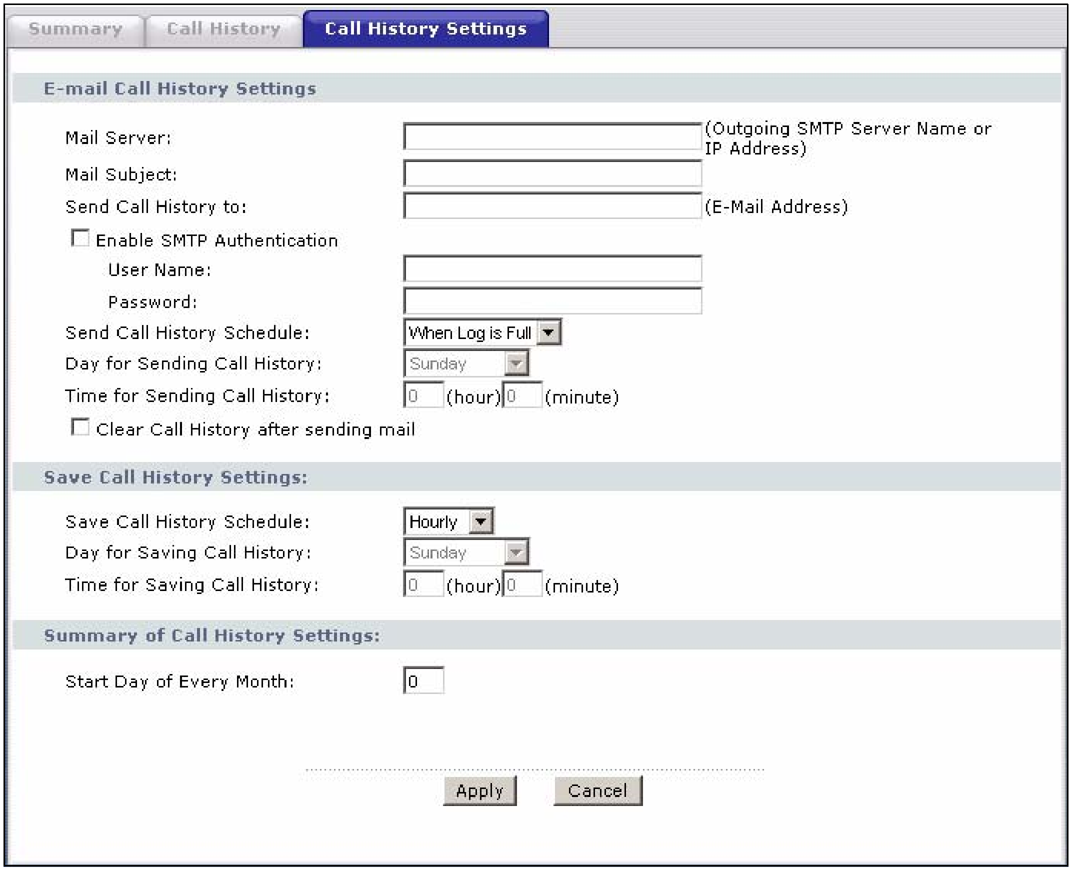
LABEL	DESCRIPTION
View Call History	Select a category of call records to view. Select **All Call History** to view any call records on the ZyXEL Device. Select **Missed Calls** to view only calls which were not answered on the ZyXEL Device. Select **Dialed Calls** to view only calls which were dialed from the ZyXEL Device. Select **Received Calls** to view only calls which were received on the ZyXEL Device
Email Log Now	Click **Email Log Now** to send the log screen to the e-mail address specified in the **Call History Settings** page (make sure that you have first filled in the **E-mail Log Settings** fields in **Call History Settings**).
Refresh	Click **Refresh** to renew the call history screen.
Clear Call History	Click **Clear Call History** to delete all call records.
Next Page	Choose a page from the drop-down list box to display the corresponding summary page of the call records.
#	This field is a sequential value and is not associated with a specific entry.
Type	This field displays the category of the call.
Time	This field displays the time the call was recorded.
Duration	This field displays how long the call lasted.
Local Identity	This field displays the phone number you used to make or receive this call.
Peer Number	This field displays the phone number you called or from which this call is made.
TxPacket	This field displays the number of packets the ZyXEL Device has transmitted for the call.
RxPacket	This field displays the number of packets the ZyXEL Device has received for the call.
Interface	This field displays the type of the call.

26.4 Configuring Call History Settings

Use the **Call History Settings** screen to configure to where the ZyXEL Device is to send call records and the schedule for when the ZyXEL Device is to send or save the call records.

To change your ZyXEL Device's call history settings, click **Maintenance > Call History > Call History Settings**. The screen appears as shown.

Figure 284 Maintenance > Call History > Call History Settings



E-mail Call History Settings

Mail Server: (Outgoing SMTP Server Name or IP Address)
Mail Subject:
Send Call History to: (E-Mail Address)
□ Enable SMTP Authentication
User Name:
Password:
Send Call History Schedule: When Log is Full
Day for Sending Call History: Sunday
Time for Sending Call History: 0 (hour) 0 (minute)
□ Clear Call History after sending mail

Save Call History Settings:

Save Call History Schedule: Hourly
Day for Saving Call History: Sunday
Time for Saving Call History: 0 (hour) 0 (minute)

Summary of Call History Settings:

Start Day of Every Month: 0

The following table describes the fields in this screen.

Table 157 Maintenance > Call History > Call History Settings

LABEL	DESCRIPTION
E-mail Call History 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. Not all ZyXEL Device have this field.
Send Call History to	The ZyXEL Device sends logs to the e-mail address specified in this field. If this field is left blank, the ZyXEL Device does not send logs via e-mail.

Table 157 Maintenance > Call History > Call History Settings

LABEL	DESCRIPTION
Enable 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 your mail server requests you to log in to receive or send e-mails. 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) that you use to log into your mail server (usually the user name of a mail account).
Password	Enter the password associated with the user name above.
Send Call History 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 Call History	Use the drop down list box to select which day of the week to send the logs.
Time for Sending Call History	Enter the time of the day in 24-hour format (for example 23:00 equals 11:00 pm) to send the logs.
Clear Call History after sending mail	Select this to delete all the logs after the ZyXEL Device sends an E-mail of the logs.
Save Call History Settings	
Save Call History Schedule	This drop-down menu is used to configure the frequency of log messages being saved: • Daily • Weekly • Hourly If you select **Weekly** or **Daily**, specify a time of day when the ZyXEL Device saves the records. If you select **Weekly**, then also specify which day of the week the ZyXEL Device saves the records.
Day for Saving Call History	Use the drop down list box to select which day of the week to save the records.
Time for Saving Call History	Enter the time of the day in 24-hour format (for example 23:00 equals 11:00 pm) to save the records.

Table 157 Maintenance > Call History > Call History Settings

LABEL	DESCRIPTION
Summary of Call History Settings	
Start Date of Every Month	Select which day of a month (from 1 to 28) on which the “Last Month” summary of call history (displays in the **Summary** screen) starts.
Apply	Click **Apply** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to return to the previously saved settings.

27

Tools

Do not interrupt the file transfer process as this may PERMANENTLY DAMAGE your ZyXEL Device.

27.1 Overview

Use the instructions in this chapter to change the device's configuration file or upgrade its firmware. After you configure your device, you can backup the configuration file to a computer. That way if you later misconfigure the device, you can upload the backed up configuration file to return to your previous settings. You can alternately upload the factory default configuration file if you want to return the device to the original default settings. The firmware determines the device's available features and functionality. You can download new firmware releases from your nearest ZyXEL FTP site (or www.zyxel.com) to use to upgrade your device's performance.

Only use firmware for your device's specific model. Refer to the label on the bottom of your ZyXEL Device.

27.1.1 What You Can Do in the Tool Screens

- Use the **Firmware Upgrade** screen (Section 27.2 on page 446) to upload firmware to your device.
- Use the **Configuration** screen (Section 27.3 on page 449) to backup and restore device configurations. You can also reset your device settings back to the factory default.
- Use the **Restart** screen (Section 27.4 on page 452) to restart your ZyXEL device.

27.1.2 What You Need To Know About Tools

Filename Conventions

The configuration file (often called the romfile or rom-0) contains the factory default settings in the menus such as password, DHCP Setup, and TCP/IP Setup. It arrives from ZyXEL with a “rom” filename extension. Once you have customized the ZyXEL Device's settings, they can be saved back to your computer under a filename of your choosing.

ZyNOS (ZyXEL Network Operating System sometimes referred to as the “ras” file) is the system firmware and has a “bin” filename extension. Find this firmware at www.zyxel.com.With many FTP and TFTP clients, the filenames are similar to those seen next.

```
ftp> put firmware.bin ras
```

This is a sample FTP session showing the transfer of the computer file "firmware.bin" to the ZyXEL Device.

```
ftp> get rom-0 config.cfg
```

This is a sample FTP session saving the current configuration to the computer file “`config.cfg`”.

If your (T)FTP client does not allow you to have a destination filename different than the source, you will need to rename them as the ZyXEL Device only recognizes “rom-0” and “ras”. Be sure you keep unaltered copies of both files for later use.

The following table is a summary. Please note that the internal filename refers to the filename on the ZyXEL Device and the external filename refers to the filename not on the ZyXEL Device, that is, on your computer, local network or FTP site and so the name (but not the extension) may vary. After uploading new firmware, see the **Status** screen to confirm that you have uploaded the correct firmware version.

Table 158 Filename Conventions

FILE TYPE	INTERNAL NAME	EXTERNAL NAME	DESCRIPTIO N
Configuration File	Rom-0	This is the configuration filename on the ZyXEL Device. Uploading the rom-0 file replaces the entire ROM file system, including your ZyXEL Device configurations, system-related data (including the default password), the error log and the trace log.	*.rom
Firmware	Ras	This is the generic name for the ZyNOS firmware on the ZyXEL Device.	*.bin

FTP Restrictions

FTP will not work when:

1. The firewall is active (turn the firewall off or create a firewall rule to allow access from the WAN).

2. You have disabled the FTP service in the **Remote Management** screen.

3. The IP you entered in the Secured Client IP field does not match the client IP. If it does not match, the device will disallow the FTP session immediately.

27.1.3 Before You Begin

- Ensure you have either created a firewall rule to allow access from the WAN or turned the firewall off, otherwise the FTP will not function.
- Make sure the FTP service has not been disabled in the Remote Management screen.

27.1.4 Tool Examples

Using FTP or TFTP to Restore Configuration

This example shows you how to restore a previously saved configuration. Note that this function erases the current configuration before restoring a previous back up configuration; please do not attempt to restore unless you have a backup configuration file stored on disk.

FTP is the preferred method for restoring your current computer configuration to your device since FTP is faster. Please note that you must wait for the system to automatically restart after the file transfer is complete.

Do not interrupt the file transfer process as this may PERMANENTLY DAMAGE your device. When the Restore Configuration process is complete, the device automatically restarts.

Restore Using FTP Session Example

Figure 285 Restore Using FTP Session Example

```
ftp> put config.rom rom-0
200 Port command okay
150 Opening data connection for STOR rom-0
226 File received OK
221 Goodbye for writing flash
ftp: 16384 bytes sent in 0.06Seconds 273.07Kbytes/sec.
ftp>quit
```

Refer to Section 27.1.2 on page 439 to read about configurations that disallow TFTP and FTP over WAN.

FTP and TFTP Firmware and Configuration File Uploads

These examples show you how to upload firmware and configuration files.

Do not interrupt the file transfer process as this may PERMANENTLY DAMAGE your device.

FTP is the preferred method for uploading the firmware and configuration. To use this feature, your computer must have an FTP client. The following sections give examples of how to upload the firmware and the configuration files.

FTP File Upload Command from the DOS Prompt Example

1. Launch the FTP client on your computer.
2. Enter “open”, followed by a space and the IP address of your device.
3. Press [ENTER] when prompted for a username.
4. Enter your password as requested (the default is “1234”).
5. Enter “bin” to set transfer mode to binary.
6. Use “put” to transfer files from the computer to the device, for example, “put firmware.bin ras” transfers the firmware on your computer (firmware.bin) to the device and renames it “ras”. Similarly, “put config.rom rom-0” transfers the configuration file on your computer (config.rom) to the device and renames it “rom-0”. Likewise “get rom-0 config.rom” transfers the configuration file on the device to your computer and renames it “config.rom.” See earlier in this chapter for more information on filename conventions.
7. Enter “quit” to exit the ftp prompt.

FTP Session Example of Firmware File Upload

Figure 286 FTP Session Example of Firmware File Upload

```
331 Enter PASS command
Password:
230 Logged in
ftp> bin
200 Type I OK
ftp> put firmware.bin ras
200 Port command okay
150 Opening data connection for STOR ras
226 File received OK
ftp: 1103936 bytes sent in 1.10Seconds 297.89Kbytes/sec.
ftp> quit
```

More commands (found in GUI-based FTP clients) are listed in this chapter.

Refer to Section 27.1.2 on page 439 to read about configurations that disallow TFTP and FTP over WAN.

TFTP File Upload

The device also supports the uploading of firmware files using TFTP (Trivial File Transfer Protocol) over LAN. Although TFTP should work over WAN as well, it is not recommended.

To use TFTP, your computer must have both telnet and TFTP clients. To transfer the firmware and the configuration file, follow the procedure shown next.

1 Use telnet from your computer to connect to the device and log in. Because TFTP does not have any security checks, the device records the IP address of the telnet client and accepts TFTP requests only from this address.

2 Enter the command “sys stdio 0” to disable the management idle timeout, so the TFTP transfer will not be interrupted. Enter “command sys stdio 5” to restore the five-minute management idle timeout (default) when the file transfer is complete.

3 Launch the TFTP client on your computer and connect to the device. Set the transfer mode to binary before starting data transfer.

4 Use the TFTP client (see the example below) to transfer files between the device and the computer. The file name for the firmware is “ras”.

Note that the telnet connection must be active and the device in CI mode before and during the TFTP transfer. For details on TFTP commands (see following example), please consult the documentation of your TFTP client program. For UNIX, use “get” to transfer from the device to the computer, “put” the other way around, and “binary” to set binary transfer mode.

TFTP Upload Command Example

The following is an example TFTP command:

```
tftp [-i] host put firmware.bin ras
```

Where “i” specifies binary image transfer mode (use this mode when transferring binary files), “host” is the device’s IP address, “put” transfers the file source on the computer (firmware.bin – name of the firmware on the computer) to the file destination on the remote host (ras - name of the firmware on the device).

Commands that you may see in GUI-based TFTP clients are listed earlier in this chapter.

Using the FTP Commands to Back Up Configuration

1 Launch the FTP client on your computer.

2 Enter “`open`”, followed by a space and the IP address of your ZyXEL Device.

3 Press [ENTER] when prompted for a username.

4 Enter your password as requested (the default is “`1234`”).

5 Enter “`bin`” to set transfer mode to binary.

6 Use “`get`” to transfer files from the ZyXEL Device to the computer, for example, “`get rom-0 config.rom`” transfers the configuration file on the ZyXEL Device to your computer and renames it “`config.rom`”. See earlier in this chapter for more information on filename conventions.

7 Enter “`quit`” to exit the ftp prompt.

FTP Command Configuration Backup Example

This figure gives an example of using FTP commands from the DOS command prompt to save your device’s configuration onto your computer.

Figure 287 FTP Session Example

```
331 Enter PASS command
Password:
230 Logged in
ftp> bin
200 Type I OK
ftp> get rom-0 zyxel.rom
200 Port command okay
150 Opening data connection for STOR ras
226 File received OK
ftp: 16384 bytes sent in 1.10Seconds 297.89Kbytes/sec.
ftp> quit
```

Configuration Backup Using GUI-based FTP Clients

The following table describes some of the commands that you may see in GUI-based FTP clients.

Table 159 General Commands for GUI-based FTP Clients

COMMAND	DESCRIPTION
Host Address	Enter the address of the host server.
Login Type	Anonymous. This is when a user I.D. and password is automatically supplied to the server for anonymous access. Anonymous logins will work only if your ISP or service administrator has enabled this option. Normal. The server requires a unique User ID and Password to login.
Transfer Type	Transfer files in either ASCII (plain text format) or in binary mode.
Initial Remote Directory	Specify the default remote directory (path).
Initial Local Directory	Specify the default local directory (path).

Backup Configuration Using TFTP

The ZyXEL Device supports the up/downloading of the firmware and the configuration file using TFTP (Trivial File Transfer Protocol) over LAN. Although TFTP should work over WAN as well, it is not recommended.

To use TFTP, your computer must have both telnet and TFTP clients. To backup the configuration file, follow the procedure shown next.

1 Use telnet from your computer to connect to the ZyXEL Device and log in. Because TFTP does not have any security checks, the ZyXEL Device records the IP address of the telnet client and accepts TFTP requests only from this address.

2 Enter command “`sys stdio 0`” to disable the management idle timeout, so the TFTP transfer will not be interrupted. Enter command “`sys stdio 5`” to restore the five-minute management idle timeout (default) when the file transfer is complete.

3 Launch the TFTP client on your computer and connect to the ZyXEL Device. Set the transfer mode to binary before starting data transfer.

4 Use the TFTP client (see the example below) to transfer files between the ZyXEL Device and the computer. The file name for the configuration file is “`rom-0`” (rom-zero, not capital o).

Note that the telnet connection must be active before and during the TFTP transfer. For details on TFTP commands (see following example), please consult the documentation of your TFTP client program. For UNIX, use "get" to transfer from the ZyXEL Device to the computer and "binary" to set binary transfer mode.

TFTP Command Configuration Backup Example

The following is an example TFTP command:

```
tftp [-i] host get rom-0 config.rom
```

where "i" specifies binary image transfer mode (use this mode when transferring binary files), "host" is the ZyXEL Device IP address, "get" transfers the file source on the ZyXEL Device (rom-0, name of the configuration file on the ZyXEL Device) to the file destination on the computer and renames it config.rom.

Configuration Backup Using GUI-based TFTP Clients

The following table describes some of the fields that you may see in GUI-based TFTP clients.

Table 160 General Commands for GUI-based TFTP Clients

COMMAND	DESCRIPTION
Host	Enter the IP address of the ZyXEL Device. 192.168.1.1 is the ZyXEL Device's default IP address when shipped.
Send/ Fetch	Use "Send" to upload the file to the ZyXEL Device and "Fetch" to back up the file on your computer.
Local File	Enter the path and name of the firmware file (*.bin extension) or configuration file (*.rom extension) on your computer.
Remote File	This is the filename on the ZyXEL Device. The filename for the firmware is "ras" and for the configuration file, is "rom-0".
Binary	Transfer the file in binary mode.
Abort	Stop transfer of the file.

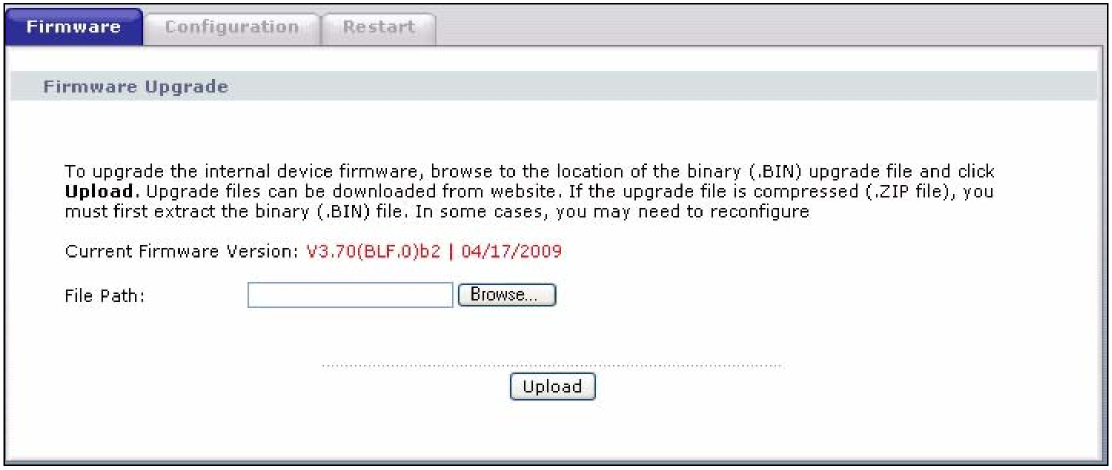
Refer to Section 27.1.2 on page 439 to read about configurations that disallow TFTP and FTP over WAN.

27.2 Firmware Upgrade Screen

Click **Maintenance > Tools** to open the **Firmware** screen. Follow the instructions in this screen to upload firmware to your ZyXEL Device. The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot. See Section on page 442 for upgrading firmware using FTP/TFTP commands.

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

Figure 288 Maintenance > Tools > Firmware Upgrade



To upgrade the internal device 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

Current Firmware Version: V3.70(BLF.0)b2 | 04/17/2009

File Path: Browse...

Upload

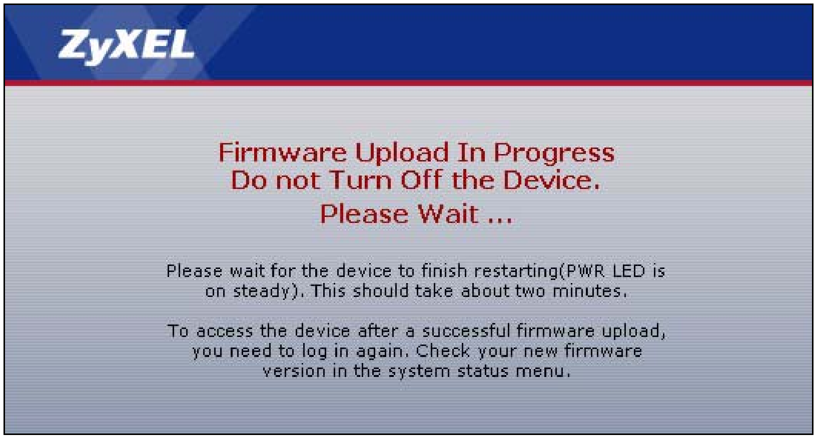
The following table describes the labels in this screen.

Table 161 Maintenance > Tools > Firmware Upgrade

LABEL	DESCRIPTION
Current Firmware Version	This is the present Firmware version and the date created.
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.

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

Figure 289 Firmware Upload In Progress



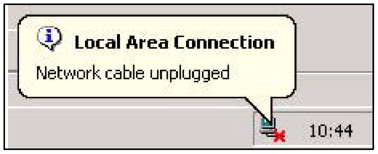
Firmware Upload In Progress
Do not Turn Off the Device.
Please Wait ...

Please wait for the device to finish restarting(PWR LED is on steady). This should take about two minutes.

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

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 290 Network Temporarily Disconnected

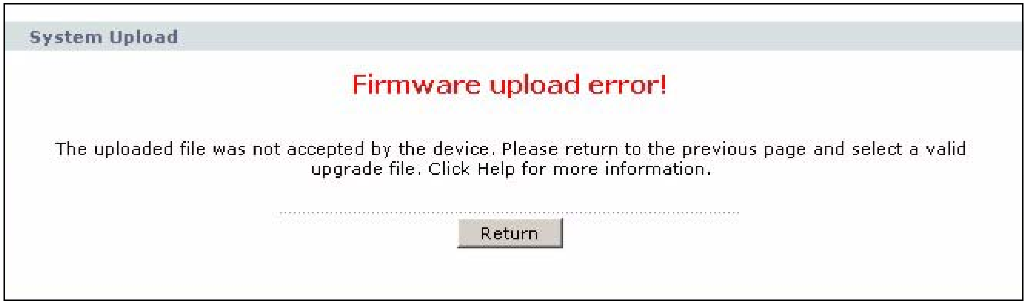


Local Area Connection
Network cable unplugged

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

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

Figure 291 Error Message



System Upload

Firmware upload error!

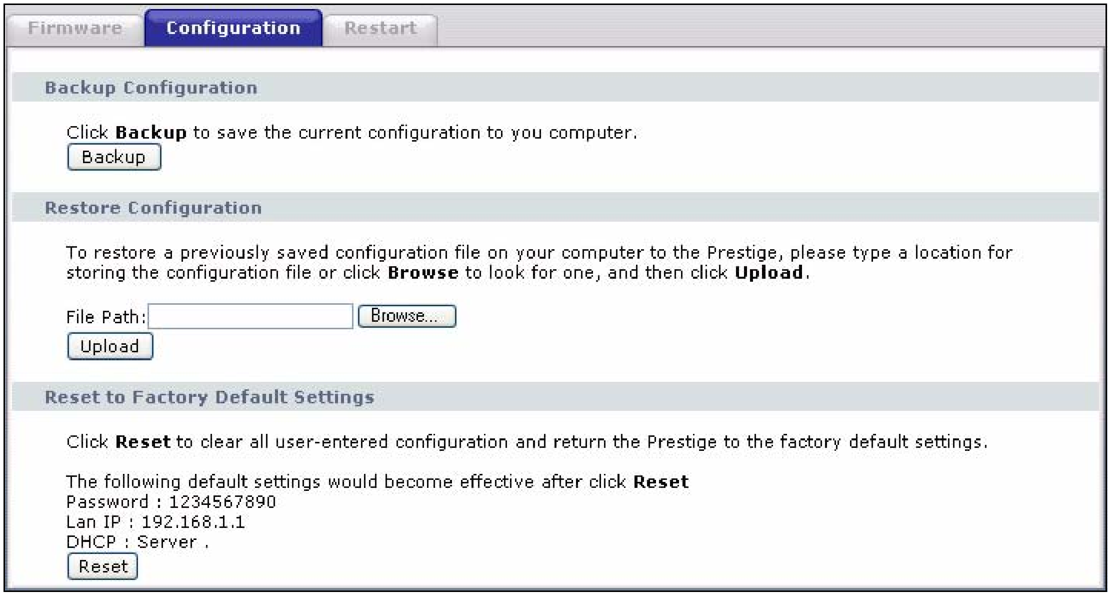
The uploaded file was not accepted by the device. Please return to the previous page and select a valid upgrade file. Click Help for more information.

27.3 The Configuration Screen

See Section 27.5 on page 452 and Section on page 441 for transferring configuration files using FTP/TFTP commands.

Click **Maintenance > Tools > Configuration**. Information related to factory defaults, backup configuration, and restoring configuration appears in this screen, as shown next.

Figure 292 Maintenance > Tools > Configuration



Backup Configuration

Click **Backup** to save the current configuration to you computer.

Restore Configuration

To restore a previously saved configuration file on your computer to the Prestige, please type a location for storing the configuration file or click **Browse** to look for one, and then click **Upload**.

File Path:

Reset to Factory Default Settings

Click **Reset** to clear all user-entered configuration and return the Prestige to the factory default settings.

The following default settings would become effective after click **Reset**
Password : 1234567890
Lan IP : 192.168.1.1
DHCP : Server .

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.

Restore Configuration

Restore Configuration allows you to upload a new or previously saved configuration file from your computer to your ZyXEL Device.

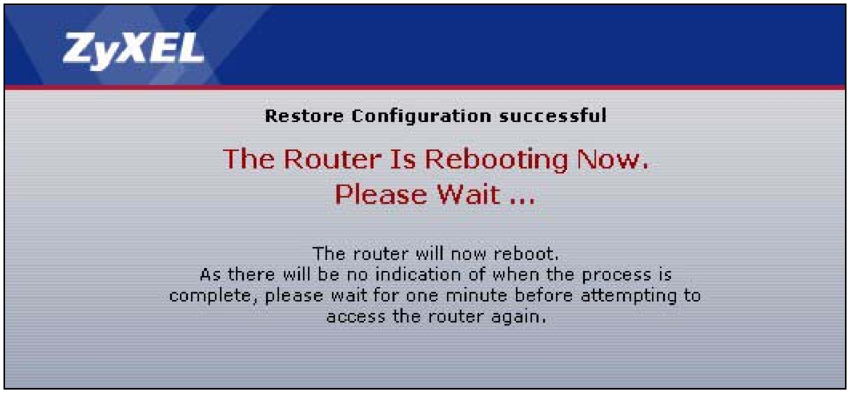
Table 162 Restore Configuration

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 293 Configuration Upload Successful



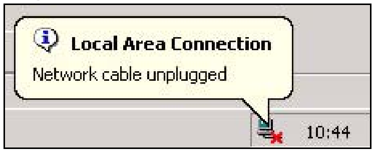
Restore Configuration successful

The Router Is Rebooting Now.
Please Wait ...

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.

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 294 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 Appendix A on page 485 for details on how to set up your computer’s IP address.