Vantage CNM 2.0

Centralized Network Management

User's Guide

Version 2.0.00.61.00
April 2004

Copyright

Refer to the appendices for open sourced software announcements.

ZyXEL Limited Warranty

ZyXEL warrants that (a) the Vantage CNM 2.0 software (henceforth called the SOFTWARE) will perform substantially in accordance with the accompanying written materials for a period of ninety (90) days from the date of receipt, and (b) any Support Services provided by ZyXEL shall be substantially as described in applicable written materials provided to you by ZyXEL, and ZyXEL support engineers will make commercially reasonable efforts to solve any problem issues. To the extent allowed by applicable law, implied warranties on the SOFTWARE, if any, are limited to ninety (90) days.

CUSTOMER REMEDIES.

ZyXEL's and its suppliers' entire liability and your exclusive remedy shall be, at ZyXEL's option, either (a) return of the price paid, if any, or (b) repair or replacement of the SOFTWARE that does not meet ZyXEL's Limited Warranty and which is returned to ZyXEL with a copy of your receipt. This Limited Warranty is void if failure of the SOFTWARE has resulted from accident, abuse, or misapplication. Any replacement SOFTWARE will be warranted for the remainder of the original warranty period or thirty (30) days, whichever is longer. Outside Taiwan, neither these remedies nor any product support services offered by ZyXEL are available without proof of purchase from an authorized international source.

NO OTHER WARRANTIES.

To the maximum extent permitted by applicable law, ZyXEL and its suppliers disclaim all other warranties and conditions, either express or implied, including, but not limited to, implied warranties of merchantability, fitness for a particular purpose, title, and non-infringement, with regard to the SOFTWARE, and the provision of or failure to provide Support Services. This limited warranty gives you specific legal rights. You may have others, which vary from state/jurisdiction to state/jurisdiction.

Please read the license screen in the installation wizard. You must accept the terms of the license in order to install Vantage CNM.

Customer Support

Please have the following information ready when you contact customer support.

- Warranty Information.
- Date that you received your software.
- Brief description of the problem and the steps you took to solve it.

METHOD / LOCATION	SUPPORT E-MAIL SALES E-MAIL	TELEPHONE[1] FAX[1]	WEB SITE FTP SITE	REGULAR MAIL
WORLDWIDE	support@zyxel.com.tw sales@zyxel.com.tw	+886-3-578-3942 +886-3-578-2439	www.zyxel.com www.europe.zyxel.com ftp.zyxel.com ftp.europe.zyxel.com	ZyXEL Communications Corp. 6 Innovation Road II Science Park Hsinchu 300 Taiwan
NORTH AMERICA	support@zyxel.com sales@zyxel.com	+1-800-255-4101 +1-714-632-0882 +1-714-632-0858	www.us.zyxel.com ftp.us.zyxel.com	ZyXEL Communications Inc. 1130 N. Miller St. Anaheim CA 92806-2001 U.S.A.
GERMANY	support@zyxel.de sales@zyxel.de	+49-2405-6909-0 +49-2405-6909-99	www.zyxel.de	ZyXEL Deutschland GmbH. Adenauerstr. 20/A2 D-52146 Wuerselen Germany
FRANCE	info@zyxel.fr	+33 (0)4 72 52 97 97 +33 (0)4 72 52 19 20	www.zyxel.fr	ZyXEL France 1 rue des Vergers Bat. 1 / C 69760 Limonest France
SPAIN	support@zyxel.es sales@zyxel.es	+34 902 195 420 +34 913 005 345	www.zyxel.es	ZyXEL Communications Alejandro Villegas 33 1º, 28043 Madrid Spain
DENMARK	support@zyxel.dk sales@zyxel.dk	+45 39 55 07 00 +45 39 55 07 07	www.zyxel.dk	ZyXEL Communications A/S Columbusvej 5 2860 Soeborg Denmark
NORWAY	support@zyxel.no sales@zyxel.no	+47 22 80 61 80 +47 22 80 61 81	www.zyxel.no	ZyXEL Communications A/S Nils Hansens vei 13 0667 Oslo Norway
SWEDEN	support@zyxel.se sales@zyxel.se	+46 31 744 7700 +46 31 744 7701	www.zyxel.se	ZyXEL Communications A/S Sjöporten 4, 41764 Göteborg Sweden
FINLAND	support@zyxel.fi sales@zyxel.fi	+358-9-4780-8411 +358-9-4780 8448	www.zyxel.fi	ZyXEL Communications Oy Malminkaari 10 00700 Helsinki Finland

[1] "+" is the (prefix) number you enter to make an international telephone call.

Table of Contents

List of Figures

List of Tables

Preface

Introducing Vantage Centralized Network Management (CNM) 2.0

Vantage Centralized Network Management 2.0 is a cost-effective, browser-based global management solution that allows an administrator from any location to easily configure, manage, monitor and troubleshoot ZyXEL devices located worldwide.

Vantage CNM allows you to effectively separate usage and management of ZyXEL's comprehensive range of broadband security devices.

Related Documentation

- Support Disk

  Refer to the included CD for support documents.

- Quick Start Guide

  The Quick Start Guide is designed to help you get up and running right away. It contains a detailed easy-to-follow connection diagram, default settings, handy checklists and information on setting up your network and configuring for Internet access.

- Web Configurator Online Help

  Click a screen's help button for screen descriptions and supplementary information.

- Certifications

  Refer to the product page at www.zyxel.com for information on product certifications.

- ZyXEL Glossary and Web Site

  Please refer to www.zyxel.com for an online glossary of networking terms and additional support documentation.

Syntax Conventions

- This manual may refer to Vantage Centralized Network Management 2.0 simply as Vantage CNM or Vantage.
- The version number on the title page is the Vantage version that is documented in this User's Guide.
- "Enter" means for you to type one or more characters and press the carriage return. "Select" or "Choose" means for you to use one of the predefined choices.
- The choices of a menu item are in **Bold Arial** font.
- Mouse action sequences are denoted using a ">". For example, "click **Configuration > LAN > IP Alias** means first click **Configuration,** then click **LAN** and finally click **IP Alias**.
- For brevity's sake, we will use "e.g." as shorthand for "for instance" and "i.e." for "that is" or "in other words" throughout this manual.

1 Introducing Vantage

This chapter introduces Vantage key features and Vantage requirements.

1.1 Key Features

1.1.1 Object Tree View

The object tree has three defined views letting you view the devices directly as you configure them. The views are Account (arranged by customer name), Type (arranged by device type) and Main View up to seven layers deep. The object tree also allows you to create your own logical views (organizing them by geographic region etc. for example). Status icons in the tree let you know immediately if a device that has gone down, is currently being configured or there is a fatal alarm associated with the device.

1.1.2 Flexible Friendly Device Registration

Use the registration wizard to register a single device or multiple devices by importing an XML registration file. This means that any customer's network can be brought under Vantage control in the time it takes to run a wizard.

1.1.3 Building Blocks

Use BBs (building block) to rapidly configure both existing and new devices by reusing multiple configurations, a device's single configuration or a configuration component, ensuring absolute consistency across devices. As you use Vantage longer, it will become even easier to use as you build up valuable BB repositories.

1.1.4 Multiple Domain Administration

Associate administrators to domains that you specify in the object tree allowing efficient division of labor with maximum independence. Furthermore, multiple administrators may manage one domain, each with different privileges allowing autonomy while collaboratively managing the same network(s).

1.1.5 Complete Device Configuration

Use the Vantage configuration menus to configure its features including LAN, WAN, NAT, firewall, VPN, static routes, wireless etc. You may also directly access any device's web configurator from the object tree by simply right-clicking on it, giving you total control over any device within Vantage.

1.1.6 Configuration Synchronization

Make sure a device configuration within Vantage is absolutely consistent with its actual configuration at any time by using the Vantage synchronization screen. This means that local configuration changes can be detected by selecting the Vantage Synchronize menu, therefore allowing flexibility with control.

1.1.7 Firewall

Create consistent device firewall policies by reusing successful configurations in other ZyXEL devices. Ensure consistency and compliance with all security policies as well as constantly monitor all devices and act immediately if things go wrong.

1.1.8 One-Click VPN

Graphically create VPN (Virtual Private Networking) tunnels between devices by simply clicking a device and dragging a "tunnel" to another device. Pre-configured tunnel settings mean that even non-technical administrators can set up and manage tunnels with minimum effort.

1.1.9 Configuration File Management

Back up, restore and reset to factory default any device's configuration file from one location.

1.1.10 Firmware Upgrade

Batch download device firmware from Vantage (after downloading the firmware from a website) to multiple devices located anywhere, minimizing time, effort and room for error as well as ensuring firmware consistency across devices. Device owners can be notified automatically and reports can be generated detailing any device's firmware upload history.

1.1.11 Monitoring and Notifications

Use the **Status Monitor** to give real time messages (of who has logged in for example) and the alarm screens to know what is going on in your management domain. Alarms are warnings of hardware failure, security breaches, attacks or illegal Vantage login attempts. You can configure Vantage to notify you by e-mail in the event a device goes down or has triggered an alarm. You can also configure Vantage to automatically notify device owners and other administrators when a configuration (such as firmware upgrade) is going to take place.

1.1.12 Logs

Logs detail information pertaining to customer accounts, devices and Vantage that is essential for troubleshooting or historical analysis. Logs and alarms facilitate the secure, smooth operation of all Vantage-registered ZyXEL devices across the globe.

1.1.13 Data Maintenance

Back up all Vantage configurations including firmware uploaded to the Vantage server, creating various Vantage "snap shots" that may be restored at a later date.

1.1.14 Vantage System Management

Configure Vantage server public IP address, FTP, syslog, mail servers, set a management idle timeout and protect Vantage from brute-force password dictionary attacks in the Vantage system menus. Furthermore, you may pre-configure notification recipients and alter Administrator privileges from here, making Vantage a truly global tool.

1.1.15 License Management

Simply login into www.myZyXEL.com to acquire a new activation key when you purchase an expansion license letting you manage yet even more devices with Vantage CNM 2.0.

1.2 Vantage Requirements and Installation

For Vantage setup requirements, access and installation, see the *Quick Start Guide*.

2 GUI Introduction

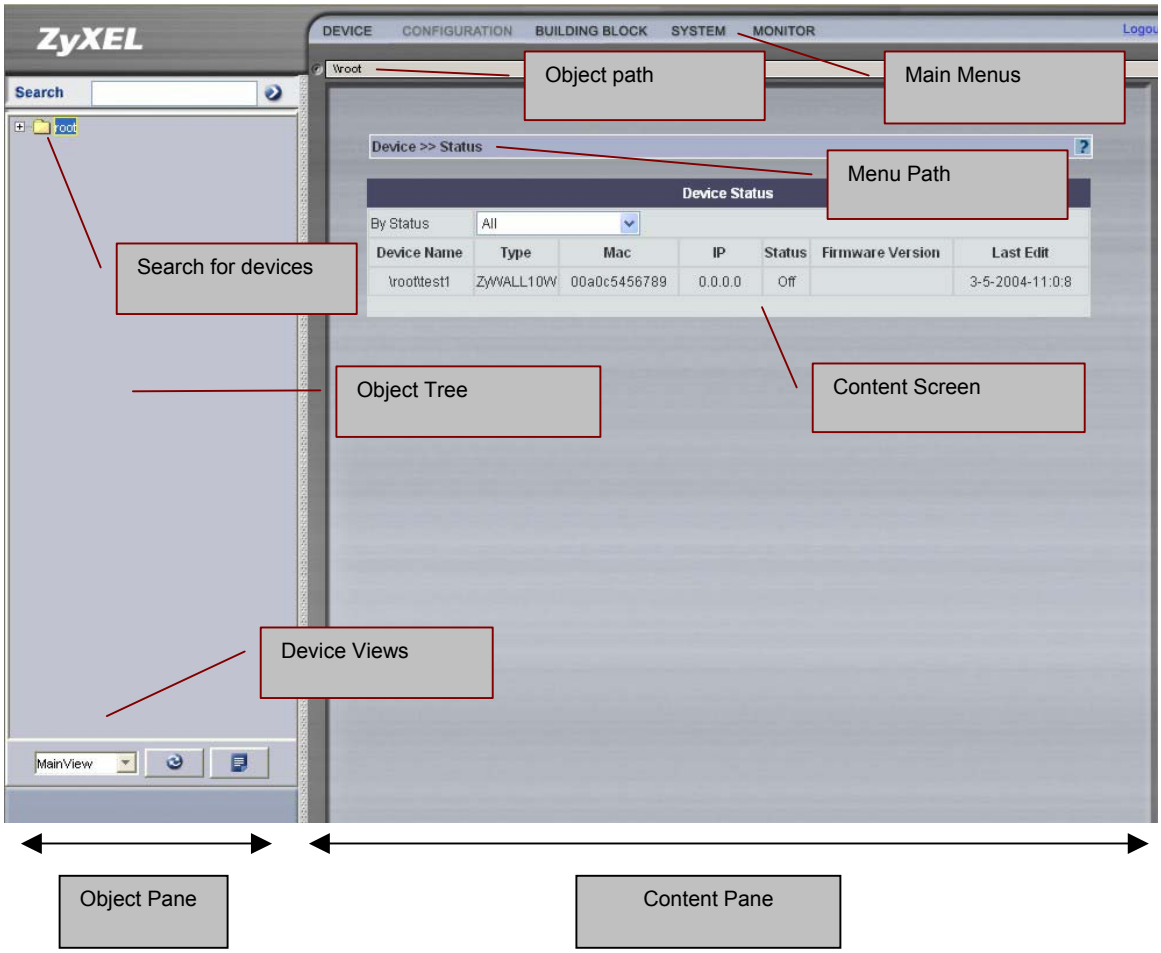


Figure 2-1 Main Screen

2.1 Main Menu Components

The main screen consists of two non-resizable panes; the object pane and the content pane.

2.2 Object Pane

The bottom of the object pane consists of an object tree view types list box where you can select a logical view of the devices. The top of the object pane has a **Search** function where you can search for devices.

2.2.1 Object Tree View Types

The **View** list box contains three default views called (device) **TypeView, AccountView** and **MainView.** You can also create custom views.

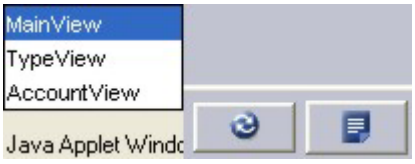


Figure 2-2 Object Tree View Types

- In the **MainView**, you may create group folders and account folders up to seven layers deep and add devices to each layer correspondingly. You can only configure devices in the main view.
- The **TypeView** view lists devices by model type.
- The **AccountView** allows for a one-layer automated view of each customer's account and the device(s) that they own.
- You can also create custom views by clicking the detail icon to display the next screen. The custom view name then appears in this list box. In custom views, you may create group folders and account folders up to seven layers deep.

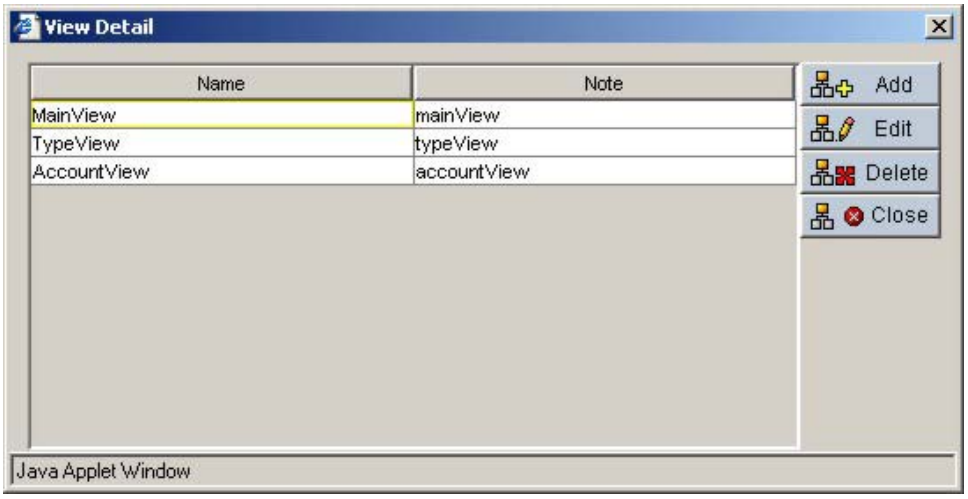


Figure 2-3 Details Screen

Click **Add** in this screen to create a new custom view, such as by geographic area. Give the view a unique name and write a note to further describe it. To edit or delete an existing view, select the target view in *Figure 2-3* and then click **Edit** or **Delete**. Click **Close** to close the screen.

2.2.2 Searches

Select a folder first to define the scope of the search. Search for devices by device name or MAC address within the selected folder in the Object tree. Results are displayed in the same split window.

2.2.3 Folders

A folder is a logical grouping of devices. There are two types of folders, **Account** and **Group**. All devices in an **Account** folder belong to that account. When you create a folder you are requested to give a name. A device can only be owned by one customer and a customer can own many devices. A **Group** folder may contain devices belonging to different accounts.

Folder right-click options are (in **MainView** only):

Figure 2-4 Folder Right-Click Options

1. **Add device.** Displays an **Add devices** screen from which you can select devices not yet mapped to another folder.

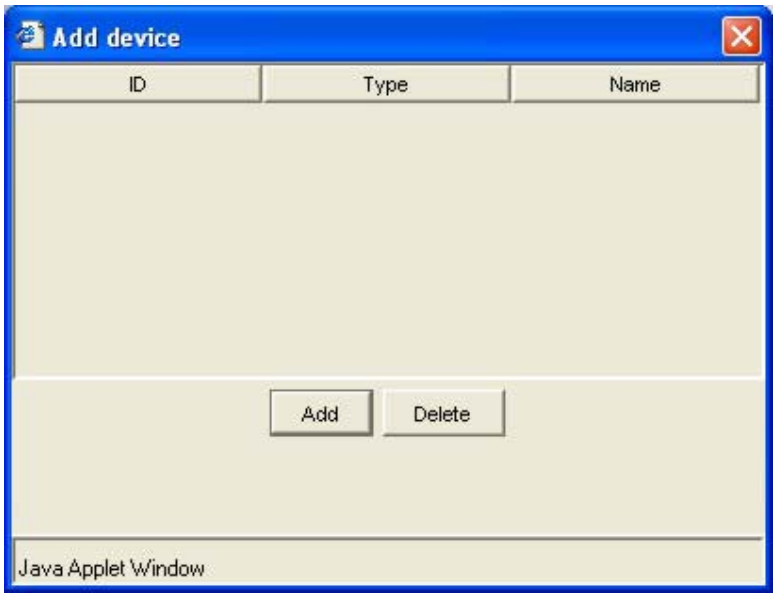


Figure 2-5 Add Devices

2. **Delete**.
   - This option displays a screen asking you if you want to delete the root folder and un-map the devices within the folder to the **Add devices** screen or
   - Delete the folder and un-map the devices within the folder. The device is still registered with Vantage but no longer associated with the folder. The latter action also disables Vantage within the device.
3. **Associate.** Links an administrator to this folder. This folder and all sub-folders are in this administrator's domain. The administrator cannot manage nor see folders or BBs outside this domain.

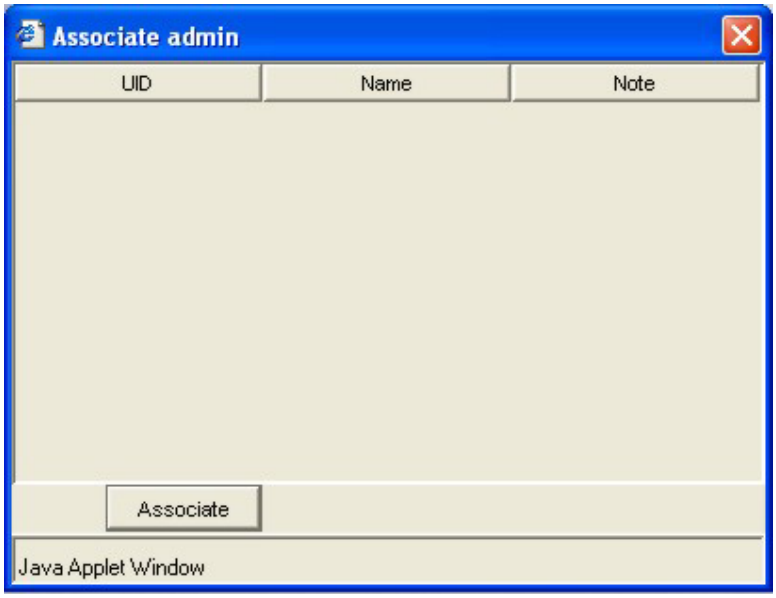


Figure 2-6 Associate Administrators

An administrator icon appears on the folder when you associate an administrator with a folder. To disassociate the administrator from this folder, right-click to select the icon and **UnAssociate**.

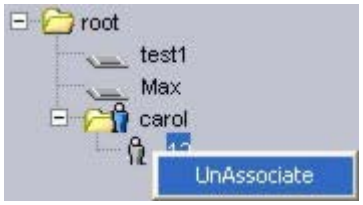


Figure 2-7 Associated Administrator Right-Click Options

4. **Add folder**. Add a new generic folder (**Group**) or customer folder (**Account**) where all devices within the folder belong to one customer. You can configure the **Account** folder to display the name of the customer on the folder in the object tree (see **Configuration > General > Customer Information**).

   When you add a folder, you must enter a new folder group name.

Figure 2-8 Add New Folder Group Name

5. **Alarm**.

Alarms are real-time warnings of hardware failure, security breaches, attacks or illegal Vantage login attempts. Click a folder; select **Alarm** and **Locate** to find alarms associated with devices within this folder.

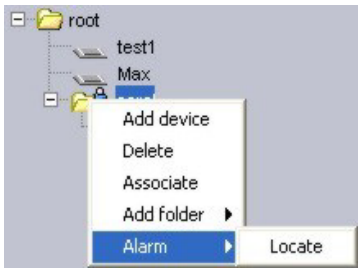


Figure 2-9 Account Folder Alarm Right-Click Options

2.2.4 Devices

Right-click a device options are:

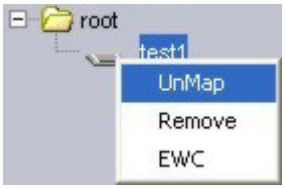


Figure 2-10 Device Right-Click Options

1. **Unmap**. The device disappears from the tree and goes to the available pool screen from which you can map. Devices display Device name. MAC address and device type.
2. **Remove**. Delete the device registration from Vantage. Vantage disables CNM in the device.
3. **EWC**. Click this to open the device's embedded web configurator. If you know the password you can log in directly and configure any item. You should synchronize with Vantage afterwards.

2.3 Content Pane

2.3.1 Object Path

The Object Path shows the folder or parent folder of the device you have clicked in the Object tree, for example "\root\zywall2".

2.3.2 Menu Path

The Menu Path shows what menu you have clicked from the drop-down menu, for example "Configuration > WAN".

2.3.3 Menu Overview

The following is an overview of the Vantage menus:

- All monitor menus are pop-up menus.
- You can only configure a single device at any one time.
- Some menus are not accessible because administrators do not have permission.
- Vantage can "remember" device and configuration menus. If for example, you select device A, then select DMZ in the **Configuration File** menu and then change to device B. The configuration DMZ will appear for device B. If device B does not have a DMZ, then the **Device > Status** screen will appear.

- If the selected device does not have a certain configuration, DMZ or wireless for example, then DMZ or WLAN will appear grayed out in the **Configuration** menu list. If this happens and you cannot access the last click menu, then you will be redirected to **Device > Status** page by default.
- If you click an administrator icon in the object tree, the **System > Administrators** menus will appear.

You can only configure a single device at one time.

Table 2-1Menus Overview

Device	Configuration	Building Block	System	Monitor	Logout
Status	Select Device BB	Device BB	Administrators	Alarm	Logout
Registration	General	Configuration BB	Status	Firmware Report	
Synchronize	LAN	Component BB	Upgrade	Status Monitor	
Firmware Mgmt	WLAN		License	VPN Editor	
Firmware Upgrade	DMZ		Preferences		
Configuration File	WAN		Maintenance		
	NAT		Address Book		
	Static route		Certificate Mgmt		
	VPN		Logs		
	Firewall		About		
	Device Log				
	ADSL Monitor				
	Device Alarm				

2.3.4 Procedure For Configuring A Device

The default when you first enter Vantage is the root node in the object tree and **Device >Status** menu.

1. Select a device in the object pane.

2. Select an item from a drop-down menu (Device, Configuration, Building Block, System or Monitor). If the selected device does not have a certain configuration, DMZ or wireless for example, then DMZ or WLAN will appear grayed out in the Configuration menu list.

3. That menu for the selected device then appears in the Content pane.

Context-Sensitive Menus

Some context-sensitive menus appear with the words “Java Applet Window” as follows:

Figure 2-11 Java Applet Window

If you do not want to see "Java Applet Window" in context-sensitive menus, then do the following:

Step 1. On the Vantage CNM server, go to Vantage CNM 2.0 installation directory\utilities (the default installation path is C:\Program Files\ZyXEL\Vantage CNM 2.0\utilities) and copy the "java.policy" file.

Step 2. On the Vantage CNM client computer, go to the Java plug-in installation directory\j2re1.4.1\lib\security\ (the default installation path is C:\Program Files\Java\j2re1.4.1\lib\security). You should see a (different) "java.policy" file there.

Step 3. Replace the "java.policy" file found in step 2 with the one copied in step 1.

It is not advisable to replace this file if other applications use the Java plug-in. Vantage CNM 2.0 functions normally whether the replacement is made or not.

2.4 Icon Key

Table 2-2 Object Tree Icons

ICON	DESCRIPTION
	This is an account folder where you can see the devices and folders inside and which contain some devices with an alarm.
	This is an account folder where you can see the devices and folders inside.
	This is an account folder where you cannot see the device inside and which contains some devices with an alarm.
	This is an account folder where you cannot see the devices inside.
	This is an open group folder, which contains some devices and folders with an alarm.
	This is an open group folder.
	This is a closed group folder, which contains some devices with an alarm.
	This is an administrator currently logged in.
	This is an administrator that has logged out.
	This is a ZyWALL device turned off.
	This is a ZyWALL device that has firmware uploading.
	This is a ZyWALL device that has an alarm that is turned on.

	This is a ZyWALL device turned off with an alarm and will have a firmware upload.
	This is a ZyWALL device turned on.
	This is a ZyWALL device with an alarm.
	This is a ZyWALL device turned on with an alarm and has firmware uploading.
	This is a ZyWALL device and has firmware uploading.
	This is a Prestige device turned off.
	This is a Prestige device turned off with an alarm.
	This is a Prestige device turned off with an alarm and will have a firmware upload.
	This is a Prestige device turned off and will have a firmware upload.
	This is a Prestige device that has an alarm that is turned on.
	This is a Prestige device with an alarm.
	This is a Prestige device with an alarm and has firmware uploading.
	This is a Prestige device with firmware uploading.
	Click this icon to refresh the current topology tree.
	Click this icon to view the topology detail information for the current user.

Table 2-3 Pop-up Menus Icons

	Click this icon to **Add** a new topology view.
	Click this icon to **Edit** the selected topology view.
	Click this icon to **Delete** the selected topology view.
	Click this icon to **Close** the popup dialog.

Table 2-4 Content Pane Icons

ICON	DESCRIPTION
	Click **Apply** the current configuration settings and apply to the server.
	Click **Save** the current configuration settings but not apply to the server. The configuration can be cancelled.
	Click **Back** to go to the previous page.
	Click **Next** to navigate to the next page.
	Click to **Reset** the current page
	Click **OK** to apply the configuration.

Yes	Click **Yes** to confirm your configuration edit.
No	Click **No** to cancel the configuration edit.
Finish	Click **Finish** to complete the whole configuration.
Cancel	Click to **Cancel** the configuration and return to the previous page.
Retrieve	Click **Retrieve** to get the logs from a device.
	Click this icon to choose from an existing BB.
	Click this icon to save a new BB.
	Click this icon to choose from an existing personal profile.
	Click this icon to save as a new personal profile.
Advanced	Click **Advanced** to show more details and configure.
Ckeck..	Click **Check** to view the status.
	This icon represents a Fatal error.
	This icon represents a Major error.
	This icon represents a Minor error.
	This icon represents a Warning error.
	This icon represents a Web Help link.
	This is a checkbox that allows you to make multiple selections from a group.
	This is a radio button allows you to make one selection from a group.
3	Type text in a text box.
Pick One	Choose from a list of pre-defined choices from a list box.
Browse...	This is a Browse icon allowing you to select a file external to Vantage.

TABLE 2-5 VPN Editor Icons

ICON	DESCRIPTION
Add	**Add** a new tunnel.
Edit	**Edit** the selected tunnel.
Delete	**Delete** the selected tunnel.
Map	Upload a map file to the VPN editor.
Save	**Save** the graphical tunnel depiction.

	**Force** deletes the selected tunnel even if the selected tunnel is active.
	**Refresh** the VPN monitor.
	**Delete** erases the selected tunnel if it is not active.
	The ZyXEL device is turned on.
	The ZyXEL device is turned off.

3 The Device Menus

3.1 Device Menus Overview

The **Device** menus allow you to register your device, synchronize devices, and manage firmware and configuration files.

3.2 Device Main Screen

Device Status is the default first screen you see; the default folder in the Object pane is “root”.

Figure 3-1 Device > Status > Main Screen

The following table describes the fields in this screen

Table 3-1 Device > Status > Main Screen

LABEL	DESCRIPTION
By Status	Select a filter status from the drop-down list box to choose which devices to view within the folder. You can view devices by: All: You can view all devices. On: You can view all devices that are online and Vantage is successfully communicating with. Off: You can view all devices that are offline. On_Alarm: You can view all devices that have an alarm that is turned on. Off_Alarm: You can view all devices that have an alarm that is turned off. On_Firmware: You can view all devices that have firmware uploading. Off_Firmware: You can view all devices that will have a firmware upload. After they are turned on Vantage will wait up to twenty minutes to upload the firmware. On_Alarm_Firmware: You can view all devices that have an alarm that is turned on and have firmware uploading. Off_Alarm_Firmware: You can view all devices that have an alarm that is turned off and will have a firmware upload.
Device Name	This field displays the user-defined name, for example, “Dev1”.
Type	This field displays the ZyXEL device model.

MAC	This field displays the LAN MAC address of the ZyXEL device.
IP	This field displays the IP address of the ZyXEL device.
Status	This field displays the operating status of the ZyXEL device. **Off** indicates the ZyXEL device is not currently connected to the network. **On** indicates the ZyXEL device is connected to the network.
Firmware Version	This field displays the device firmware network operating system (NOS) version number and date.
Last Edit	This shows the date the screen was last edited.

3.3 Device Status

In the **Device** menus, select single devices only in the Object pane when you select the **Synchronize** and **Configuration File** menu options. You may select both folders and devices for all other **Device** menu options.

Click a device, for example "test1" in the following screen and then select the Device drop down menus and click Status. This is a read-only screen showing device summary information.

Figure 3-2 Device > Status > Single Device

The following table describes the fields in this screen

Table 3-2 Device > Status > Single Device

LABEL	DESCRIPTION
Device Name	This field displays the user-defined name, for example, "test1".
Type	This field displays the ZyXEL device model.
MAC	This field displays the LAN MAC address of the ZyXEL device.
IP	This field displays the IP address of the ZyXEL device.
Status	This field displays the operating status of the ZyXEL device. **Off** indicates the ZyXEL device is not currently connected to the network. **On** indicates the ZyXEL device is connected to the network.
Firmware Version	This field displays the device firmware network operating system (NOS) version number and date.
Last Edit	This shows the date the screen was last edited.

3.4 Device Registration

Register devices with Vantage using the device registration wizard. Select a folder (not a device) in the object tree to have the new devices automatically mapped to that folder.

Figure 3-3 Device > Registration Wizard > Account Association

- Click **Yes** to display the next wizard screen (in the Content pane). Choose the device owner for this new device(s). This device should then appear under the correct customer in the **AccountView**.
- Click **No** to jump to *Figure 3-5*. If you already selected an Account folder in the object tree, then the owner name is pre-selected here.

Figure 3-4 Device > Registration > Owner Selection

In the following screen select a radio button to either:

- Manually add: When you choose this option, you must enter the information shown in *Figure 3-6* for a single device at a time.
- Import from an XML batch registration file: choose this option if you want to input a batch of devices in one go. Go to the XML folder within the Vantage CNM Installation directory (C:\Program Files\ZyXEL\Vantage CNM 2.0\xml by default). Choose the 4-devices or 100-ZyWALL10W templates and modify accordingly.

Click **Next** to proceed to the next registration screen.

Figure 3-5 Device > Registration > Wizard Choices

3.4.1 Manual Option

Use the following screen to enter device information, get device configurations and set encryption options.

You do not need to add NAT or firewall rules when you encrypt this traffic.

To set the encryption mode on the ZyXEL device, do the following:

1. Go to CI (Command Interface) mode (SMT 24.8 for devices with SMT menus)
2. Type 'CNM encrymode X' where:

Value of X	Encryption Mode
0	None
1	DES
2	3DES

3. To set the encryption key on the ZyXEL device, type 'CNM encrykey xxxxxxxxx' where ‘xxxxxxxxx’ is the alphanumeric encryption key (“0” to “9”, “a” to “z” or “A” to “Z”) in the Vantage server.

Figure 3-6 Device > Registration > Manual Registration

The following table describes the fields in this screen

Table 3-3 Device > Registration > Manual Registration

LABEL	DESCRIPTION
MAC (Hex)	Enter the LAN MAC address of the ZyXEL device (without colons) in this field. Vantage uses the MAC address to identify the ZyXEL device, so make sure it is entered correctly.
Name	Enter a unique name here for the ZyXEL device for identification purposes. The device name cannot exceed ten characters.
Device Type	Select the ZyXEL device type from the pull-down menu.
Set Vantage CNM configuration to device	Select the radio button to have Vantage first get the WAN configuration from the device. The device will then be reset including VPN. The pre-edited configuration will then be set to the device except for VPN.
Get configuration from the device	Select the radio button to have Vantage first get the WAN configuration from the device. Vantage then pulls all other current configurations from the device. The device configuration "overwrites" Vantage configurations.
Encryption Methods	The encryption options at the time of writing are DES and 3DES. Choose from None (no encryption), DES or 3DES. The ZyXEL device must be set to the same encryption mode (and have the same encryption key) as the Vantage server.
Encryption Key	Type an eight-character alphanumeric (“0” to “9”, “a” to “z” or "A" to "Z") for DES encryption and a 24-character alphanumeric (“0” to “9”, “a” to “z” or "A" to "Z") for 3DES encryption.
Back	Click **Back** to return to the previous screen.
Finish	Click **Finish** to go to the **Device Registration Finished** screen.

3.4.2 Import From an Batch XML Registration File

Use this method when you want to register a batch of ZyXEL devices at one time. The file should be in XML format containing the fields shown in the manual registration screen for each device.

Go to “vantage installed path\xml\” to see two XML templates (one for Prestige and one for ZyWALL) that you may use to create an XML batch registration file.

After you have completed the XML import file, click **Browse** to locate it in the next screen and then click **Next** to display the XML file information.

Figure 3-7 Registration Wizard: Configuration File

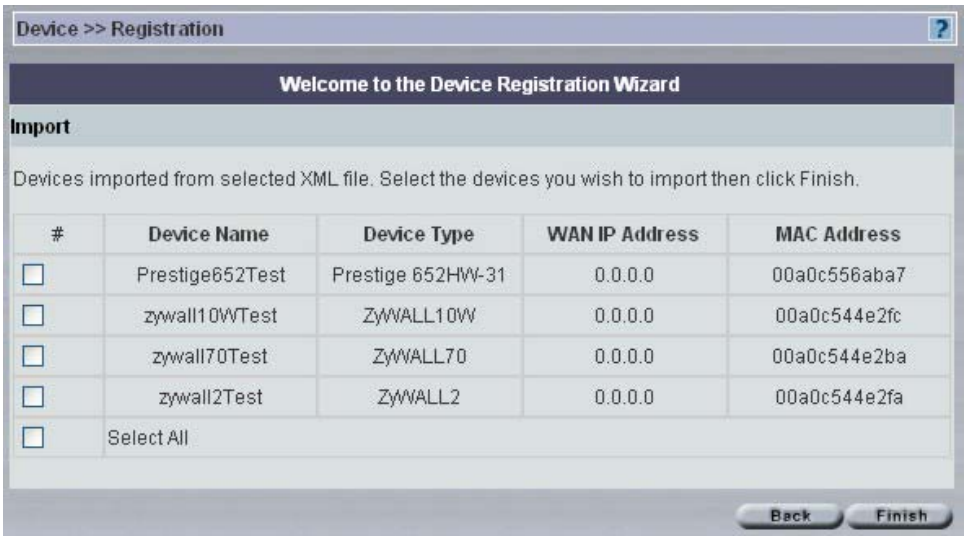


Figure 3-8 Registration

Devices imported from the selected XML files are displayed in this screen.

Select the devices that you wish to import and then click the **Finish** button.

Select All devices to import all devices that are displayed in this screen.

Click **Finish** to go to a **Device Registration Finished** screen showing what files you have successfully registered.

Figure 3-9 Registration Wizard: Finish

3.5 Device – Vantage Data Inconsistency: Synchronize

Click **Device > Synchronize** to have Vantage check for data inconsistencies in the selected object. Data inconsistencies may occur if device configurations are made directly to the device instead of in Vantage.

3.5.1 Vantage – Device Override Criteria

Vantage CNM Override Device

Select the radio button and click apply to have Vantage first get the WAN configuration from the device. The device will then be reset including VPN. The pre-edited configuration will then be set to the device except for VPN.

Device Override Vantage CNM

Select the radio button and click apply to have Vantage first get the WAN configuration from the device. Vantage then pulls all other current configurations from the device. The device configuration "overwrites" Vantage configurations.

Daily Operations

Normal operation is that Vantage overwrites device configurations. However, use the **Synchronize Settings** menu to decide what to do in case device data inconsistencies occur.

Select a device and then click **Device > Synchronize Settings**. A screen displays showing which configuration menus are out-of-synch. Access the device web configurator to view discrepancy details between corresponding configurations. When you understand the discrepancy, you can then decide to allow Vantage to override the device configuration or vice-versa.

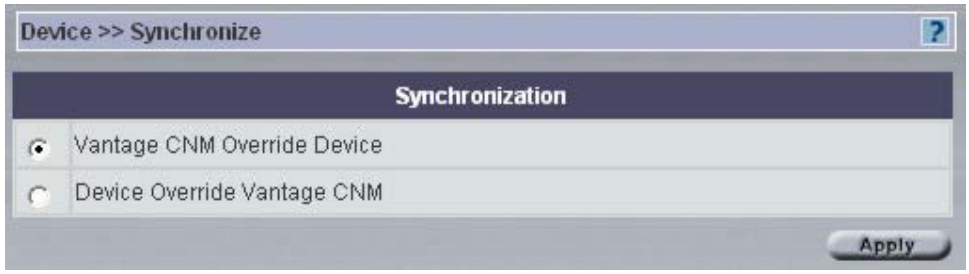


Figure 3-10 Device > Synchronize

3.6 Firmware Management

Use the **Firmware Management** screen to download ZyXEL device firmware from the ZyXEL FTP site to Vantage. After you download it to Vantage, you can then upload it from Vantage to the target devices.

All firmware is downloaded to one repository within Vantage. There is no domain-specific repository within Vantage for firmware downloads.

You cannot edit an existing firmware in Vantage; you can only delete it.

Administrators should subscribe to the ZyXEL mailing lists to be regularly informed of new firmware versions.

Click **Device > Firmware Management** to display the next screen.

Figure 3-11 Device > Firmware Management

The following table describes the fields in this screen

Table 3-4 Device > Firmware Management

TYPE	DESCRIPTION
Index	This is the file list number.

FW Alias	This is the firmware file name.
Device Type	This field displays the model. You must upload firmware to the correct model. For example firmware for P650R-11 is not compatible with the P650R-13 model. Vantage should automatically detect firmware for the device selected. Uploading incorrect firmware may damage the device.
FW Version	This field displays ZyNOS (ZyXEL network operating System) firmware version.
FW Release Date	This field displays the date the firmware was created.
Administrator	This field displays the administrator who downloaded this firmware file to Vantage.
ZyXEL Download Website	Click this hyperlink to go to the ZyXEL Website and download firmware to your computer. Firmware is uploaded to your device in the following manner • download from the website to your computer • upload from your computer to the Vantage • upload from Vantage to your selected device.
Add	Click **Add** to proceed to the next screen.
Delete	Click to delete a selected firmware from your Vantage firmware management.

3.6.1 Add Firmware Screen

Click **Add** in **Firmware Management** to view the next screen that allows you to select a "firmware zip" file. Upload the "firmware zip" file to Vantage. This "firmware zip" file contains more than the firmware. It contains:

- The device firmware ("bin" file extension). Only this firmware file is actually downloaded to the device.
- The device default configuration file ("config" file extension).
- Device firmware release notes ("doc" file extension) highlighting
- Boot module with "bm" file extension
- A file with "XML" file extension. Vantage uses the XML file to gather the device type, firmware version and release date information.

Click **Add** in *Figure 3-11* to display the next screen. Type the file name and path or browse to where you saved the file. You may create a firmware alias for the selected zip in this screen.

Figure 3-12 Device > Firmware Management > Add Firmware

3.7 Device Firmware Upgrade

Use the **Device Firmware Upgrade** screen to download firmware to devices from Vantage.

You may upgrade firmware to several homogeneous devices at the same time. Vantage can upload firmware from 20 to 50 devices at a time depending on your network bandwidth. You can upload firmware in the **Main View** or in **Type View**.

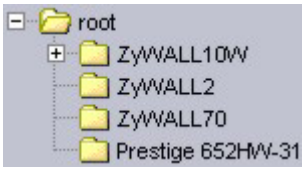


Figure 3-13 TypeView

3.7.1 Firmware Upgrade Select Product Line and Mode

If you select a device in the object tree Figure 3-15 will be shown, otherwise the following screen will be displayed. Use this screen to select the product line and model name of devices that you want to download firmware to from Vantage.

1. Pick a product line.
2. Pick a model name.

Click **Next** to proceed to the Firmware Upgrade screen.

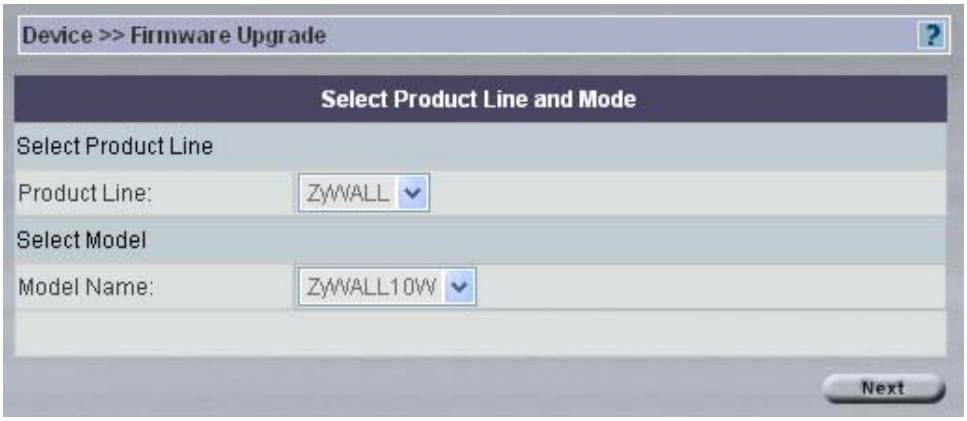


Figure 3-14 Firmware Upgrade > Select Product Line and Mode

3.7.2 Firmware Upgrade Process

Firmware Upgrade Process

1. Select Firmware by picking a node.
2. Select the candidate devices (of that model type for the node selected).

Click **Upgrade** to begin the device upgrade process

Figure 3-15 Device > Firmware Upgrade

See *Table 3-4* for field descriptions. Click **Upgrade** to begin the device upgrade process.

3.7.3 Advisory Notes on Firmware Upgrade

- It is advisable to upgrade firmware during periods of low network activity, since each device must restart after firmware upload.
- You should also notify device owners before you begin the upload. See the **System > Preferences > Notifications** screen.

3.8 Configuration File

Use these screens to manage, back up and restore configuration files ("Configuration" files).

Select the device and then click **Device > Configuration File**.

You can create your own configuration file alias in Vantage. This may make it easier to distinguish multiple configuration files for the same device.

3.8.1 Configuration File Management

Use this screen to view and delete configuration files uploaded to Vantage. You can view the configuration file name, a description of it, the date it was backed up and which administrator backed it up.

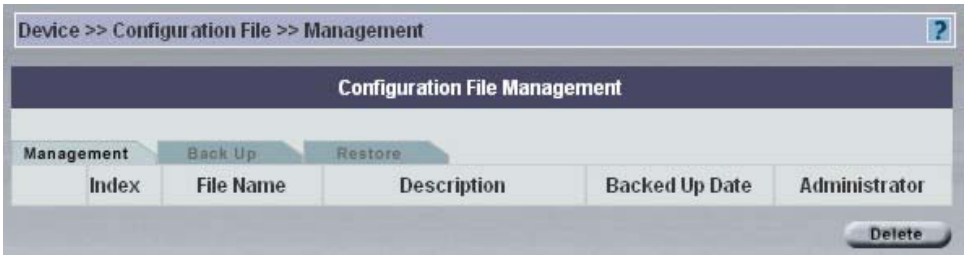


Figure 3-16 Device > Configuration File > Management

The following table describes the fields in this screen

Table 3-5 Device > Configuration File > Management

TYPE	DESCRIPTION
Index	This displays a number assigned to the file
File Name	This displays the name given to the configuration file.
Description	This displays a description that was entered at the time of file backup or file restoration.
Backed Up Date	This field displays the date of back up of a configuration file.
Administrator	This field displays the administrator who performed the backup or restoration of the configuration file.
Delete	Select the checkbox and click **Delete** to remove a selected firmware from your Vantage firmware management.

3.8.2 Configuration File Backup

Select a device and then use the **Backup** screen to save that device's configuration file to either Vantage or your computer (from which you're accessing Vantage).

Once your 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.

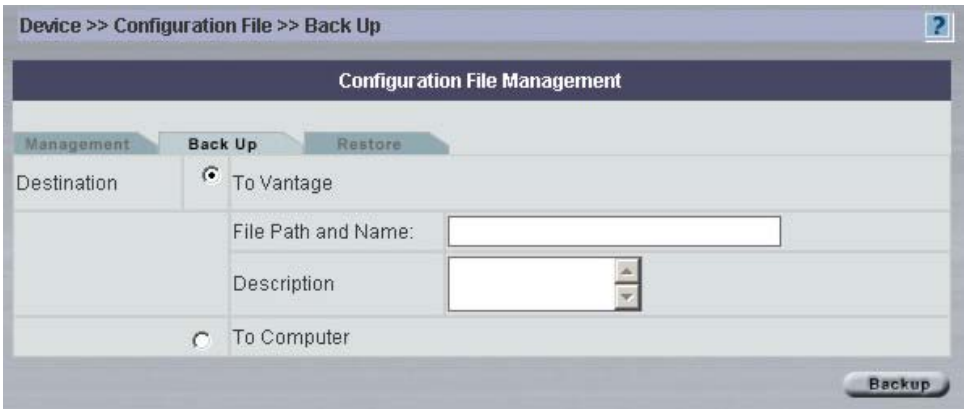


Figure 3-17 Device > Configuration File > Back Up

The following table describes the fields in this screen

Table 3-6 Device > Configuration File > Back Up

TYPE	DESCRIPTION
Destination	Select the radio button to give the download destination to Vantage.
File Path and Name	Type in the location of the file you want to upload in this field.
Description	Type a description of the file backup.
To Computer	Select the radio button to give the download destination to your computer.
Back Up	Click the Backup button to proceed to a dialog box where your configuration is saved to your computer.

3.8.3 Configuration File Restore

Use the **Restore** screen to overwrite a devices current configuration with a previously saved backup file or the default configuration file from either Vantage or your computer (from which you're accessing Vantage). Be sure to upload the correct Configuration file for the device.

Make sure you restore a configuration file to the correct model or you may damage the device.

If you restore a configuration file to a device other than the one intended, you may lock out the device. The configuration file contains the WAN configuration.

Figure 3-18 Device > Configuration File > Upload

Table 3-7 Device > Configuration File > Upload

TYPE	DESCRIPTION
Resource	Select this radio button to upload a configuration file From Vantage.
File Name	Select a file from the drop-down list box.
From Computer	Select this radio button to upload a configuration file From your Computer.
File Path and Name	Type in the location of the file you want to upload in this field or click Browse ... to find it.
Upload	Click Upload to begin the upload process.

4 Configuration > Select Device BB & General

This section shows you how to use the select device building block screen and how to configure the General menus.

These screens will vary depending on which model you're configuring.

When you click a configuration menu, the screen shows the current device configuration.

If you're unfamiliar with ZyXEL device configurations, please consult your device User's Guide.

Configuration > General can be saved as one **Configuration BB**.

4.1 Select Device BB

This screen essentially allows you copy a device's total configuration (except WAN, NAT and VPN) and paste it to another device.

4.1.1 Procedure to Copy and Paste a Device's Configuration

1. Select the device from which you want to copy its configuration.
2. Click **Configuration** > **Select Device BB** to display the next screen.
3. Click the "Save as a BB" icon ( ) and save it as a new BB with a unique device BB name.
4. Select the device to which you want to paste this configuration.
5. Click **Configuration** > **Select Device BB** to display the next screen.
6. Click the "Load a BB" icon ( ) and select the BB you just saved.
7. Click the **Apply** button to save that configuration to the device.
8. This device configuration can then be further fine-tuned using the regular configuration menus and saved as another new device BB.

Figure 4-1 Select Device BB

4.2 Configuration General Screens

Click **Configuration > General** to configure **System**, **DDNS**, **Time Setting** and **Owner Info**. The **System** tab is shown next.

4.2.1 System

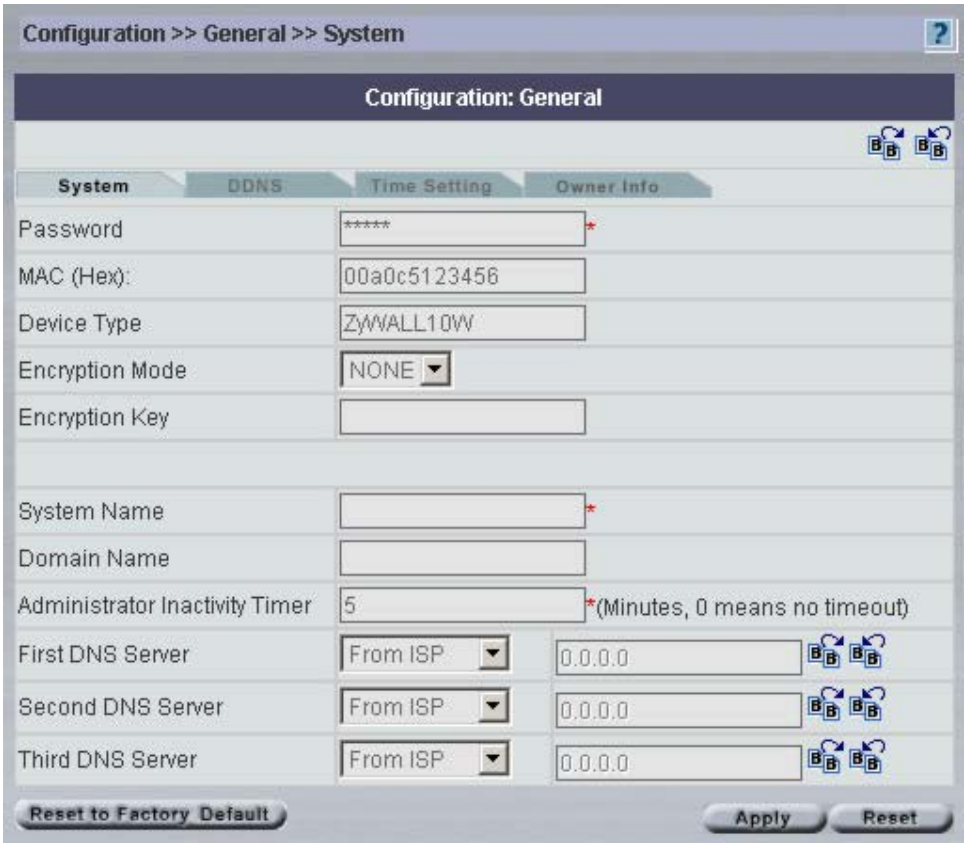


Figure 4-2 Configuration > General > System – ZyWALL

The following table describes the fields in this screen

Table 4-1 Configuration > General > System – ZyWALL

FIELD	DESCRIPTION
Password	Enter the password used to access the device.
MAC (Hex)	This field displays the LAN MAC address of the ZyXEL device. Vantage uses the MAC address to identify the ZyXEL device. This is entered when you manually register the ZyXEL device.
Device Type	This field displays the ZyXEL device type selected in the object tree.

Table 4-1 Configuration > General > System – ZyWALL

<table>
<tr><th>FIELD</th><th>DESCRIPTION</th></tr>
<tr><td>Encryption Mode</td><td>You may choose to encrypt traffic between the ZyXEL device and the Vantage server here. Choose from None (no encryption), DES or 3DES. The ZyXEL device must be set to the same encryption mode (and have the same encryption key) as the Vantage server.
You do not need to add NAT or firewall rules when you encrypt this traffic.
To set the encryption mode on the ZyXEL device, do the following:
1. Go to CI mode (SMT 24.8 for devices with SMT menus)
2. Type 'CNM encrymode X' where:
<table>
<tr><th>Value of X</th><th>Encryption Mode</th></tr>
<tr><td>0</td><td>None</td></tr>
<tr><td>1</td><td>DES</td></tr>
<tr><td>2</td><td>3DES</td></tr>
</table>
</td></tr>
<tr><td>Encryption Key</td><td>Type an eight-character alphanumeric (“0” to “9”, “a” to “z”) for DES encryption and a 24-character alphanumeric (“0” to “9”, “a” to “z”) for 3DES encryption. To set the encryption key on the ZyXEL device, type
'CNM encrykey xxxxxxxxx' where ‘xxxxxxxxx’ is the hexadecimal secret key number you used in the Vantage server.</td></tr>
<tr><td>System Name</td><td>Enter a unique name here for the ZyXEL device for identification purposes. The device name cannot exceed 31 characters.</td></tr>
<tr><td>Domain Name</td><td>The Domain Name entry is what is propagated to the DHCP clients on the LAN side of the target device. If you leave this blank, the domain name obtained by the device via DHCP from the ISP is used.</td></tr>
<tr><td>Administrator Inactivity Timer</td><td>Set how long a management session can remain idle before it expires. After it expires, you have to (default five minutes) log back into the device.</td></tr>
<tr><td>First DNS Server

Second DNS Server

Third DNS Server</td><td>DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. These DNS servers refer to the device system DNS server. The device uses a system DNS server (in the order you specify here) to resolve domain names for VPN, DDNS and the timeserver.
Select From ISP if the ISP dynamically assigns the device DNS server information. The text box to the right then displays the (read-only) DNS server IP address that the ISP assigns.
Select User-Defined if you want to assign the DNS server IP address yourself. Enter the DNS server's IP address in the field to the right or select from an IP address component BB.
Select None if you do not want to configure device system DNS servers. If you do not configure a system DNS server, you must use IP addresses when configuring VPN and DDNS.</td></tr>
<tr><td>Reset to Factory Default</td><td>Click this button to upload the factory-default configuration file of the device.</td></tr>
<tr><td>Apply</td><td>Click Apply to apply your changes in this screen.</td></tr>
<tr><td>Reset</td><td>Click Reset to begin configuring the screen afresh.</td></tr>
</table>

4.2.2 DDNS

Use this screen to configure your DNS parameters

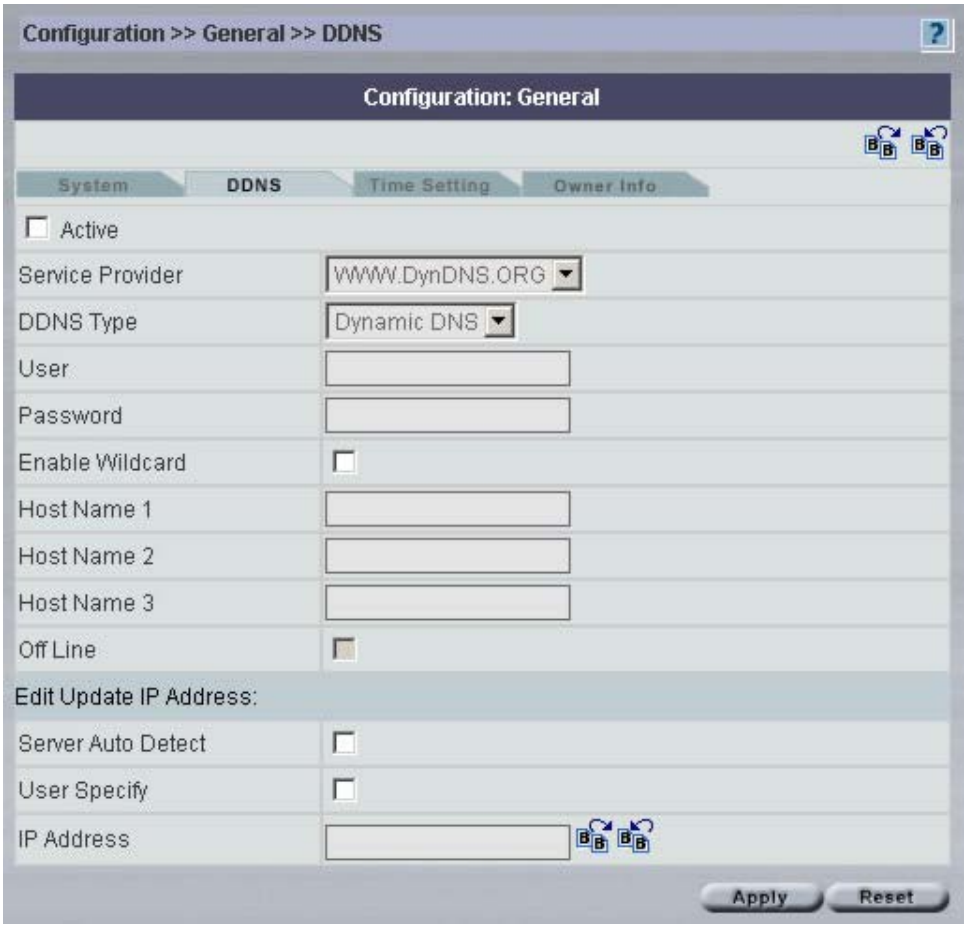


Figure 4-3 Configuration > General > DDNS

The following table describes the fields in this screen

Table 4-2 Configuration > General > DDNS

LABEL	DESCRIPTION
Active	Select this check box to use dynamic DNS.
Service Provider	Select the name of your Dynamic DNS service provider.
DDNS Type	Select the type of service that you are registered for from your Dynamic DNS service provider.
User	Enter your user name.
Password	Enter the password assigned to you.
Enable Wildcard	Select the check box to enable DYNDNS Wildcard.
Host Names 1~3	Enter the host names in the three fields provided. You can specify up to two host names in each field separated by a comma (",").

Table 4-2 Configuration > General > DDNS

LABEL	DESCRIPTION
Off Line	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.
Edit Update IP Address:	
Server Auto Detect	Select this option to update the IP address of the host name(s) automatically by the DDNS server. It is recommended that you select this option.
User Specify	Select this option to update the IP address of the host name(s) to the IP address specified below. Use this option if you have a static IP address.
IP Address	Enter the IP address if you select the **User Specify** option.
E-Mail (Prestige Only)	Type the e-mail address here or select from a previously created e-mail component BB. You may also save a newly entered e-mail address as a new e-mail component BB.
Apply	Click **Apply** to save your changes back to the device.
Reset	Click **Reset** to begin configuring this screen afresh.

4.2.3 Time Setting

Use this screen to configure your time settings.

Figure 4-4 Configuration > General > Time Setting

The following table describes the fields in this screen

Table 4-3 Configuration > General > Time Setting

LABEL	DESCRIPTION

Table 4-3 Configuration > General > Time Setting

LABEL	DESCRIPTION
Time Protocol (or Use Time Server when Bootup)	Select the time service protocol that your timeserver sends when you turn on the device. Not all timeservers 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). Select **None** to enter the time and date manually.
Time Server Address	Enter the IP address of your timeserver. Check with your ISP/network administrator if you are unsure of this information (the default is tick.stdtime.gov.tw).
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	Select this option if you use daylight savings time. 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.
Start Date	Enter the month and day that your daylight-savings time starts on if you selected **Daylight Savings**.
End Date	Enter the month and day that your daylight-savings time ends on if you selected **Daylight Savings**.
Calibrate (Prestige only)	Select the check box to have your Prestige use the timeserver (that you configured above) to set its internal system clock.
Apply	Click **Apply** to save your changes back to the device.
Reset	Click **Reset** to begin configuring this screen afresh.

4.2.4 Owner Info

The address book is the equivalent of a device owner BB. You can select from previous entries or save as new entries.

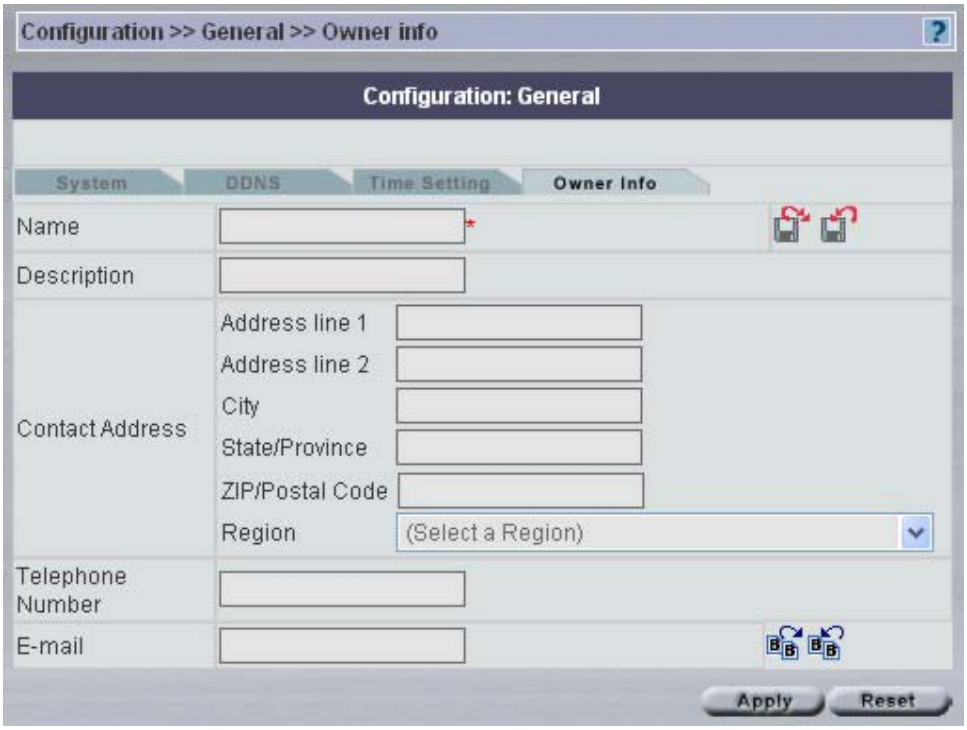


Figure 4-5 Configuration > General > Owner Info

The following table describes the fields in this screen

Table 4-4 Configuration > General > Owner Info

TYPE	DESCRIPTION
Name	Type the full name of the owner of this device.
Description	Type some extra information about this customer.
Contact Address	Type the complete customer mailing address here.
Address 1, 2	Type the customer's building number, street and city zone (if applicable) here.
City	Type the full city or town name.
StateProvince	Type the state or province.
ZIP/Postal Code	Type the zip or postal code here.
Region	Select the country or region from the list.
Telephone Number	Type the customer's telephone number including country code and area code here.
E-mail	Type the customer's e-mail address here or select from a previously created e-mail component BB. You may also save a newly entered e-mail address as a new e-mail component BB.
Apply	Click **Apply** to create the BB. This BB is then available in the BB pool for this domain.
Reset	Click **Reset** to begin configuring the screen afresh.

5 Configuration > LAN

5.1 LAN Overview

The **Configuration: LAN** screen varies depending on the device type shown.

Local Area Network (LAN) is a shared communication system to which many computers are attached. Use the LAN screens to configure a LAN DHCP server, manage IP addresses, and partition a physical network into logical networks.

5.2 DHCP Setup

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a server. You can configure the ZyXEL device as a DHCP server or disable it. When configured as a server, the ZyXEL device provides the 4444444444444444444444/IP configuration for the clients. If set to **None**, DHCP service will be disabled and you must have another DHCP server on your LAN, or else the computer must be manually configured.

5.2.1 IP Pool Setup

The ZyXEL device is pre-configured with a pool of 32 IP addresses starting from 192.168.1.33 to 192.168.1.64. This configuration leaves 31 IP addresses (excluding the ZyXEL device itself) in the lower range for other server computers, for instance, servers for mail, FTP, TFTP, web, etc., that you may have.

5.2.2 DNS Servers

Use the **LAN IP** screen to configure the DNS server information that the ZyXEL device sends to the DHCP client devices on the LAN.

5.3 LAN TCP/IP

The ZyXEL device has built-in DHCP server capability that assigns IP addresses and DNS servers to systems that support DHCP client capability.

5.3.1 Factory LAN Defaults

The LAN parameters of the ZyXEL device are preset in the factory with the following values:

- IP address of 192.168.1.1 with subnet mask of 255.255.255.0 (24 bits)
- DHCP server enabled with 32 client IP addresses starting from 192.168.1.33.

These parameters should work for the majority of installations. If your ISP gives you explicit DNS server address(es), read the embedded web configurator help regarding what fields need to be configured.

5.3.2 IP Address and Subnet Mask

Refer to the *IP Address and Subnet Mask* section in the **Wizard Setup** chapter for this information.

5.3.3 RIP Setup

RIP (Routing Information Protocol, RFC 1058 and RFC 1389) allows a router to exchange routing information with other routers. **RIP Direction** controls the sending and receiving of RIP packets. When set to **Both** or **Out**

Only, the ZyXEL device will broadcast its routing table periodically. When set to **Both** or **In Only**, it will incorporate the RIP information that it receives; when set to **None**, it will not send any RIP packets and will ignore any RIP packets received.

RIP Version controls the format and the broadcasting method of the RIP packets that the ZyXEL device sends (it recognizes both formats when receiving). **RIP-1** is universally supported; but **RIP-2** carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology.

Both **RIP-2B** and **RIP-2M** send routing data in RIP-2 format; the difference being that **RIP-2B** uses subnet broadcasting while **RIP-2M** uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also.

By default, **RIP Direction** is set to **Both** and **RIP Version** to **RIP-1**.

5.3.4 Multicast

Traditionally, IP packets are transmitted in one of either two ways - Unicast (1 sender - 1 recipient) or Broadcast (1 sender - everybody on the network). Multicast delivers IP packets to a group of hosts on the network - not everybody and not just 1.

IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see sections 4 and 5 of RFC 2236. The class D IP address is used to identify host groups and can be in the range 224.0.0.0 to 239.255.255.255. The address 224.0.0.0 is not assigned to any group and is used by IP multicast computers. The address 224.0.0.1 is used for query messages and is assigned to the permanent group of all IP hosts (including gateways). All hosts must join the 224.0.0.1 group in order to participate in IGMP. The address 224.0.0.2 is assigned to the multicast routers group.

The ZyXEL device supports both IGMP version 1 (**IGMP-v1**) and IGMP version 2 (**IGMP-v2**). At start up, the ZyXEL device queries all directly connected networks to gather group membership. After that, the ZyXEL device periodically updates this information. IP multicasting can be enabled/disabled on the ZyXEL device LAN and/or WAN interfaces in the web configurator (**LAN**; **WAN**). Select **None** to disable IP multicasting on these interfaces.

5.4 Configuring LAN IP – ZyWALL

Select a device and then click **Configuration > LAN**. **IP** is the first tab.

Figure 5-1 Configuration > LAN > IP – ZyWALL

The following table describes the fields in this screen

Table 5-1 Configuration > LAN > IP – ZyWALL

LABEL	DESCRIPTION
DHCP Mode	DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients (computers) to obtain TCP/IP configuration at startup from a server.. When configured as a server, the ZyXEL device provides TCP/IP configuration for the clients. If not, DHCP service is disabled and you must have another DHCP server on your LAN, or else the computer must be manually configured. When set as a server, fill in the rest of the DHCP setup fields.
IP Pool Starting Address	This field specifies the first of the contiguous addresses in the IP address pool.
Pool Size	This field specifies the size, or count of the IP address pool.

Table 5-1 Configuration > LAN > IP – ZyWALL

LABEL	DESCRIPTION
First DNS Server Second DNS Server Third DNS Server	DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. The ZyXEL device passes a DNS (Domain Name System) server IP address (in the order you specify here) to the DHCP clients. The ZyXEL device only passes this information to the LAN DHCP clients when you select **DHCP Server**. If you don't select **DHCP Server**, DHCP service is disabled and you must have another DHCP sever on your LAN, or else the computers must have their DNS server addresses manually configured. Select **From ISP** if an ISP dynamically assigns DNS server information (and the ZyXEL device's WAN IP address). The field to the right displays the (read-only) DNS server IP address that the ISP assigns. Select **User-Defined** if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose **User-Defined**, but leave the IP address set to 0.0.0.0, **User-Defined** changes to **None** after you click **Apply**. If you set a second choice to **User-Defined**, and enter the same IP address, the second **User-Defined** changes to **None** after you click **Apply**. Select **DNS Relay** to have the ZyXEL device act as a DNS proxy. The ZyXEL device's LAN IP address displays in the field to the right (read-only). The ZyXEL device tells the DHCP clients on the LAN that the ZyXEL device itself is the DNS server. When a computer on the LAN sends a DNS query to the ZyXEL device, the ZyXEL device forwards the query to the ZyXEL device's system DNS server (configured in the **SYSTEM General** screen) and relays the response back to the computer. You can only select **DNS Relay** for one of the three servers; if you select **DNS Relay** for a second or third DNS server, that choice changes to **None** after you click **Apply**. Select **None** if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a machine in order to access it.
TCP/IP	
IP Address	Type the IP address of the ZyXEL device in dotted decimal notation. 192.168.1.1 is the factory default.
IP Subnet Mask	The subnet mask specifies the network number portion of an IP address. The ZyXEL device automatically calculates the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the ZyXEL device, which is 255.255.255.0.
RIP Direction	RIP (Routing Information Protocol, RFC1058 and RFC 1389) allows a router to exchange routing information with other routers. The **RIP Direction** field controls the sending and receiving of RIP packets. Select the RIP direction from **Both**/**In Only**/**Out Only**/**None**. When set to **Both** or **Out Only**, the ZyXEL device broadcasts its routing table periodically. When set to **Both** or **In Only**, it incorporates the RIP information that it receives; when set to **None**, it does not send any RIP packets and ignores any RIP packets received. **Both** is the default.
RIP Version	The **RIP Version** field controls the format and the broadcasting method of the RIP packets that the ZyXEL device sends (it recognizes both formats when receiving). **RIP-1** is universally supported but RIP-2 carries more information. **RIP-1** is probably adequate for most networks, unless you have an unusual network topology. Both **RIP-2B** and **RIP-2M** sends the routing data in RIP-2 format; the difference being that **RIP-2B** uses subnet broadcasting while **RIP-2M** uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also. By default, RIP direction is set to **Both** and the **Version** set to **RIP-1**.

Table 5-1 Configuration > LAN > IP – ZyWALL

LABEL	DESCRIPTION
Multicast	Select **IGMP V-1** or **IGMP V-2** or **None**. IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see *sections 4 and 5 of RFC 2236*.
Windows Networking (NetBIOS over TCP/IP): NetBIOS (Network Basic Input/Output System) are TCP or UDP broadcast packets that enable a computer to connect to and communicate with a LAN. For some dial-up services such as PPPoE or PPTP, NetBIOS packets cause unwanted calls. However it may sometimes be necessary to allow NetBIOS packets to pass through to the WAN in order to find a computer on the WAN.	
Allow From LAN to WAN	Select this option to forward NetBIOS packets from the LAN port to the WAN port.
Apply	Click **Apply** to save your changes back to the ZyXEL device.
Reset	Click **Reset** to begin configuring this screen afresh.

5.5 Configuring LAN IP - Prestige

Select a device, and then click **Configuration > LAN**. **IP** is the only tab used for an ADSL device.

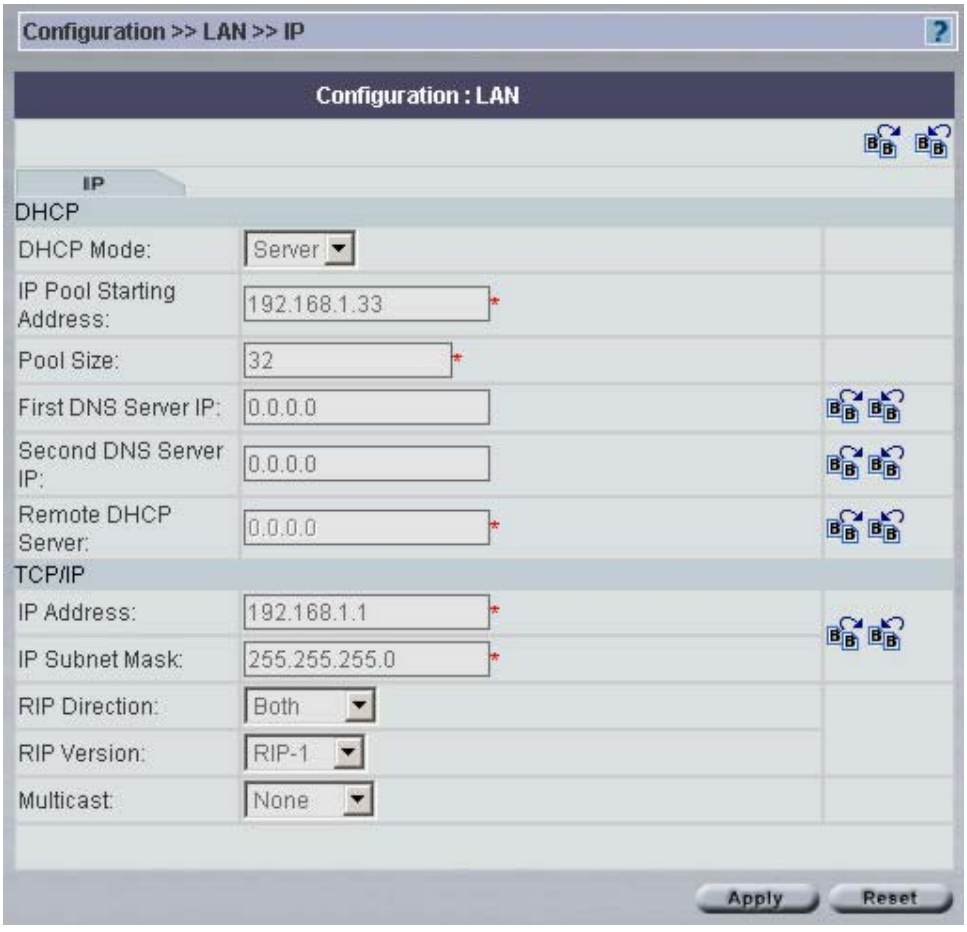


Figure 5-2 Configuration > LAN > IP – Prestige

Table 5-2 Configuration > LAN > IP – Prestige

LABEL	DESCRIPTION
DHCP Mode	DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients (computers) to obtain TCP/IP configuration at startup from a server. Select **None** if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a machine in order to access it. When configured as a **Server**, the ZyXEL device provides TCP/IP configuration for the clients. When set as a **Server**, fill in the rest of the DHCP setup fields. Select **Relay** to have the ZyXEL device act as a DNS proxy. The ZyXEL device tells the DHCP clients on the LAN that the ZyXEL device itself is the DNS server. When a computer on the LAN sends a DNS query to the ZyXEL device, the ZyXEL device forwards the query to the ZyXEL device's system DNS server and relays the response back to the computer. You can select **Relay** and enter an IP Pool Starting Address. The First DNS Server IP and Second DNS Server IP will appear as read only fields.
IP Pool Starting Address	This field specifies the first of the contiguous addresses in the IP address pool.
Pool Size	This field specifies the size, or count of the IP address pool.
First DNS Server IP Second DNS Server IP	The ZyWALL passes a DNS (Domain Name System) server IP address (in the order you specify here) to the DHCP clients. Type your First DNS Server IP and Second DNS Server IP addresses in these fields.
Remote DHCP Server	If **Relay** is selected in the DHCP field above, then type the IP address of the actual, remote DHCP server here.
TCP/IP	
IP Address	Type the IP address of the ZyXEL device in dotted decimal notation. 192.168.1.1 is the factory default.
IP Subnet Mask	The subnet mask specifies the network number portion of an IP address. The ZyXEL device automatically calculates the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the ZyXEL device, which is 255.255.255.0.
RIP Direction	RIP (Routing Information Protocol, RFC1058 and RFC 1389) allows a router to exchange routing information with other routers. The **RIP Direction** field controls the sending and receiving of RIP packets. Select the RIP direction from **Both**/**In Only**/**Out Only**/**None**. When set to **Both** or **Out Only**, the ZyXEL device broadcasts its routing table periodically. When set to **Both** or **In Only**, it incorporates the RIP information that it receives; when set to **None**, it does not send any RIP packets and ignores any RIP packets received. **Both** is the default.
RIP Version	The **RIP Version** field controls the format and the broadcasting method of the RIP packets that the ZyXEL device sends (it recognizes both formats when receiving). **RIP-1** is universally supported but RIP-2 carries more information. **RIP-1** is probably adequate for most networks, unless you have an unusual network topology. Both **RIP-2B** and **RIP-2M** sends the routing data in RIP-2 format; the difference being that **RIP-2B** uses subnet broadcasting while **RIP-2M** uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also. By default, RIP direction is set to **Both** and the **Version** set to **RIP-1**.

Table 5-2 Configuration > LAN > IP – Prestige

LABEL	DESCRIPTION
Multicast	Select **IGMP V-1** or **IGMP V-2** or **None**. IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see *sections 4 and 5 of RFC 2236*.
Apply	Click **Apply** to save your changes back to the ZyXEL device.
Reset	Click **Reset** to begin configuring this screen afresh.

5.6 Configuring LAN Static DHCP – ZyWALL

This table allows you to assign IP addresses on the LAN to specific individual computers based on their MAC Addresses.

Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02.

Select a device, and then click **Configuration > LAN > Static DHCP**.

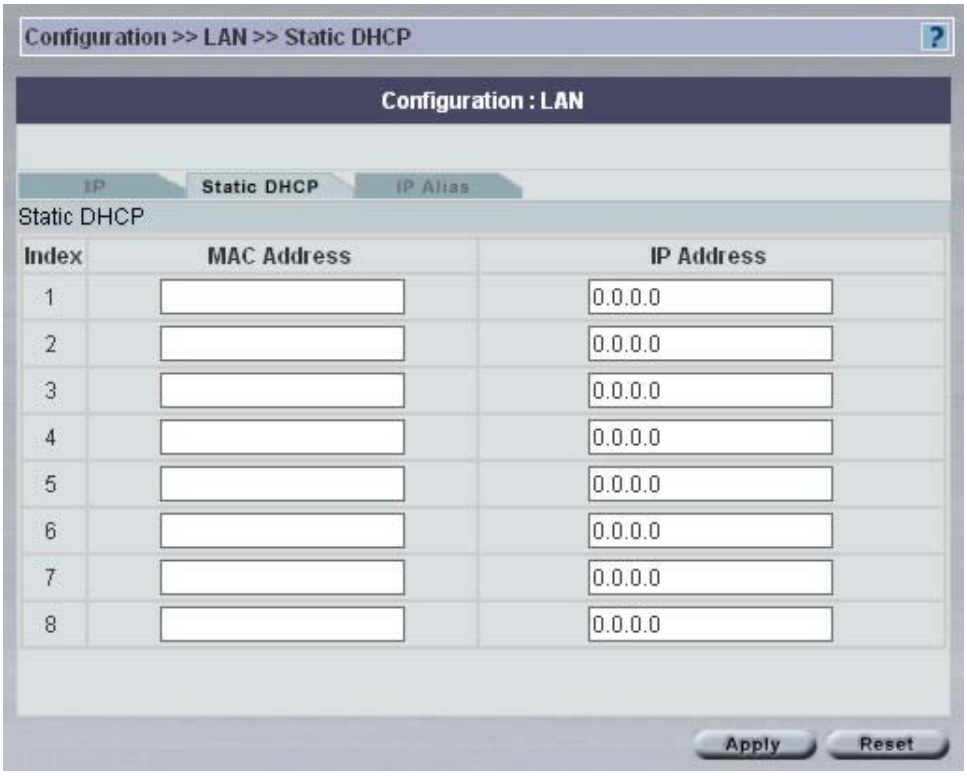


Figure 5-3 Configuration > LAN > Static DHCP – ZyWALL

The following table describes the fields in this screen

Table 5-3 Configuration > LAN > Static DHCP – ZyWALL

LABEL	DESCRIPTION

Table 5-3 Configuration > LAN > Static DHCP – ZyWALL

LABEL	DESCRIPTION
Index	This is the index number of the Static IP table entry (row).
MAC Address	This is the MAC address of a computer on the device's LAN.
IP Address	This is the IP address to be assigned to the device with the MAC address above.
Apply	Click **Apply** to save your changes back to the ZyXEL device.
Reset	Click **Reset** to begin configuring this screen afresh.

5.7 Configuring LAN IP Alias – ZyWALL

IP Alias allows you to partition a physical network into different logical networks over the same Ethernet interface. The ZyXEL device lets you configure logical LAN interfaces via its single physical Ethernet interface with the device itself being the gateway for each LAN network.

When you use IP alias, you can also configure firewall rules to control access between the LAN's logical networks (subnets).

Select a device, and then click **Configuration > LAN > IP Alias**.

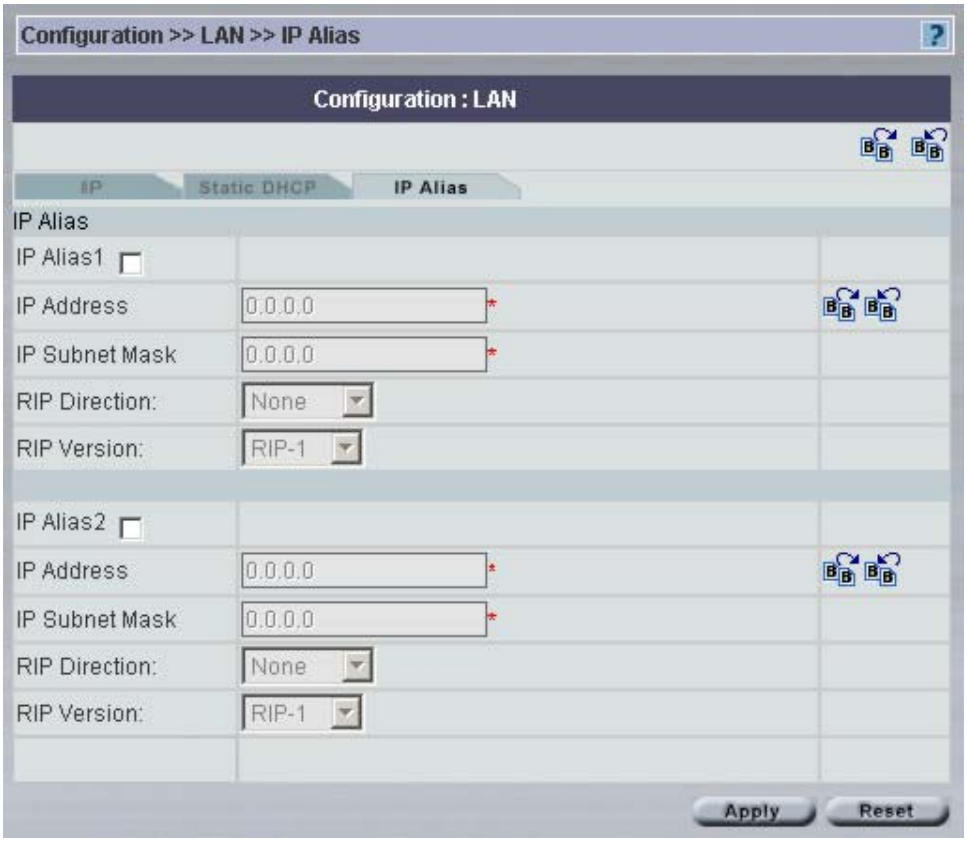


Figure 5-4 Configuration > LAN > IP Alias

The following table describes the fields in this screen

Table 5-4 Configuration > LAN > IP Alias

LABEL	DESCRIPTION
IP Alias 1,2	Select the check box to configure another LAN network for the ZyXEL device.
IP Address	Enter the IP address of the ZyXEL device in dotted decimal notation.
IP Subnet Mask	The ZyXEL device automatically calculates the subnet mask based how many aliases you select. See also the appendices for more information on IP subnetting.
RIP Direction	RIP (Routing Information Protocol, RFC1058 and RFC 1389) allows a router to exchange routing information with other routers. The **RIP Direction** field controls the sending and receiving of RIP packets. Select the RIP direction from **Both**/**In Only**/**Out Only**/**None**. When set to **Both** or **Out Only**, the ZyXEL device broadcasts its routing table periodically. When set to **Both** or **In Only**, it incorporates the RIP information that it receives; when set to **None**, it does not send any RIP packets and ignores any RIP packets received.
RIP Version	The **RIP Version** field controls the format and the broadcasting method of the RIP packets that the ZyXEL device sends (it recognizes both formats when receiving). **RIP-1** is universally supported but RIP-2 carries more information. **RIP-1** is probably adequate for most networks, unless you have an unusual network topology. Both **RIP-2B** and **RIP-2M** sends the routing data in RIP-2 format; the difference being that **RIP-2B** uses subnet broadcasting while **RIP-2M** uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also. By default, RIP direction is set to **Both** and the Version set to **RIP-1**.
Apply	Click **Apply** to save your changes back to the ZyXEL device.
Reset	Click **Reset** to begin configuring this screen afresh.

6 Configuration > WLAN

This chapter shows the wireless LAN screens.

6.1 Wireless LAN Overview

This section introduces the wireless LAN (WLAN) and some basic scenarios.

6.1.1 Additional Installation Requirements for using 802.1x

- A computer with an IEEE 802.11b wireless LAN card.
- A computer equipped with a web browser (with JavaScript enabled) and/or Telnet.
- A wireless client computer must be running IEEE 802.1x-compliant software. Currently, this is offered in Windows XP.
- An optional network RADIUS server for remote user authentication and accounting.

6.2 Wireless LAN Basics

This section provides background information on WLAN.

6.2.1 Channel

IEEE 802.11b wireless devices use radio frequencies called channels. Choose the radio channel depending on your geographical area. Adjacent Access Points (APs) should use different channels to reduce crosstalk. Crosstalk occurs when radio signals from access points overlap and cause interference that degrades performance.

6.2.2 ESS ID

Extended Service Set (ESS) is defined as one or more APs acting as a bridge between a wired LAN and the associated wireless clients. The ESS ID is a unique ID given to the APs and the wireless clients that participate in the same wireless network. You can think of the ESS ID as being similar to a workgroup name in a Microsoft network.

6.2.3 RTS/CTS

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

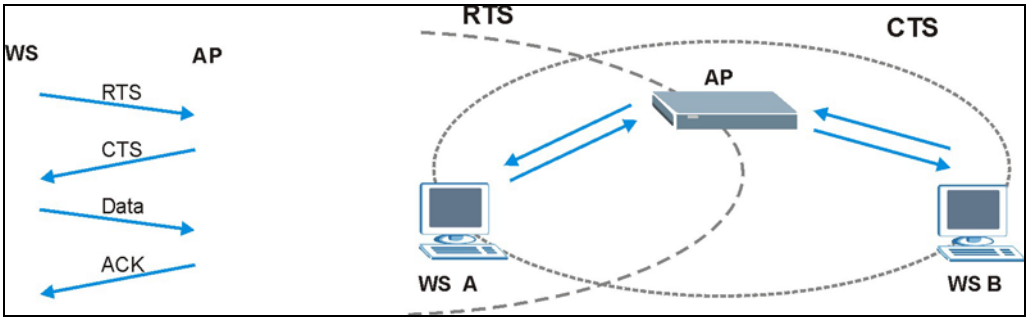


Figure 6-1 RTS Threshold

Wireless stations (WS) A and B do not hear each other. They can hear the AP. When station A sends data to the ZyXEL device, it might not know that the station B is already using the channel. If these two stations send data at the same time, collisions may occur when both sets of data arrive at the AP at the same time, resulting in a loss of messages for both stations.

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

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

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

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

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

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

6.2.4 Fragmentation Threshold

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

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

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

6.2.5 WEP

WEP provides a mechanism for encrypting data using encryption keys. Both the AP and the wireless stations must use the same WEP key to encrypt and decrypt data. The ZyXEL device allows you to configure up to four 64-bit or 128-bit WEP keys, but only one key can be enabled at any one time.

6.3 Configuring Wireless LAN

If you are configuring the ZyXEL device from a computer connected to the wireless LAN and you change the ZyXEL device's ESSID or WEP settings, you will lose your wireless connection when you press **Apply** to confirm. You must then change the wireless settings of your computer to match the ZyXEL device's new settings.

Select a device, and then click **Configuration > WLAN**. **Wireless** is the first screen.

6.3.1 WLAN Wireless

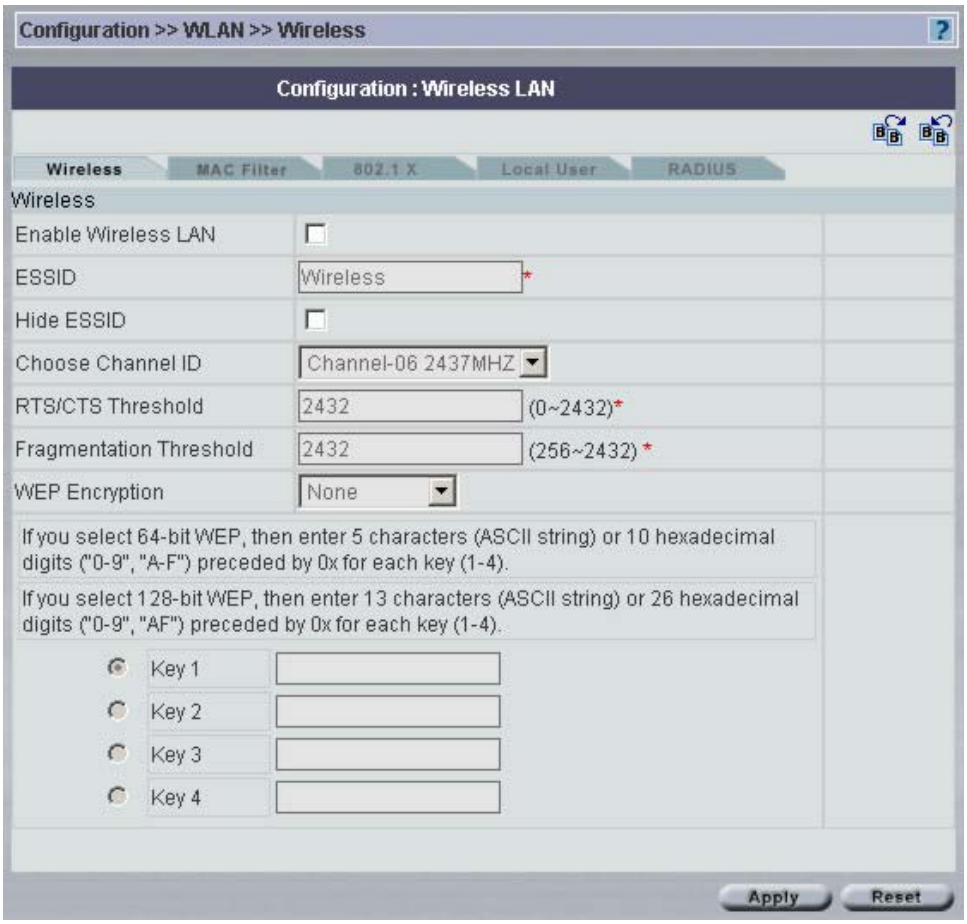


Figure 6-2 Configuration > WLAN > Wireless

The following table describes the fields in this screen

Table 6-1 Configuration > WLAN > Wireless

LABEL	DESCRIPTION
Enable Wireless LAN	The wireless LAN is turned off by default; before you enable the wireless LAN you should configure some security by setting MAC filters and/or 802.1x security; otherwise your wireless LAN will be vulnerable upon enabling it. Select the check box to enable the wireless LAN.
ESSID	(Extended Service Set IDentification) The ESSID identifies the Service Set the station is to connect to. Wireless clients associating to the Access Point must have the same ESSID. Enter a descriptive name (up to 32 characters) for the wireless LAN.
Hide ESSID	Select to hide the ESSID in the outgoing beacon frame so a station cannot obtain the ESSID through passive scanning.
Choose Channel ID	This allows you to set the operating frequency/channel depending on your particular region. Select a channel from the drop-down list box. CH01 2412 MHz / CH02 2417 MHz ~ CH11 2462 MHz (North America/FCC) CH01 2412 MHz / CH02 2417 MHz ~ CH13 2472 MHz (Europe CE/ ETSI) CH01 2412 MHz / CH02 2417 MHz ~ Ch14 2484 MHz (Japan) CH10 2457 MHz / CH11 2462 MHz (Spain)
RTS/CTS Threshold	(Request To Send) The threshold (number of bytes) for enabling RTS/CTS handshake. Data with its frame size larger than this value will perform the RTS/CTS handshake. Setting this attribute to be larger than the maximum MSDU (MAC service data unit) size turns off the RTS/CTS handshake. Setting this attribute to zero turns on the RTS/CTS handshake. Enter a value between **0** and **2432**.
Fragmentation Threshold	The threshold (number of bytes) for the fragmentation boundary for directed messages. It is the maximum data fragment size that can be sent. Enter a value between **256** and **2432**.
WEP Encryption	WEP (Wired Equivalent Privacy) provides data encryption to prevent unauthorized wireless stations from accessing data transmitted over the wireless network. Select **Disable** to allow wireless clients to communicate with the access points without any data encryption. Select **64-bit WEP** or **128-bit WEP** to enable data encryption. Although WEP is functional at 5.5 and 11 Mbps, there is significant performance degradation when using WEP at these rates.
Key 1 to Key 4	If you chose **64-bit WEP** in the **WEP Encryption** field, then enter any 5 characters (ASCII string) or 10 hexadecimal characters ("0-9", "A-F") preceded by 0x for each key. If you chose **128-bit WEP** in the **WEP Encryption** field, then enter 13 characters (ASCII string) or 26 hexadecimal characters ("0-9", "A-F") preceded by 0x for each key. There are four data encryption keys to secure your data from eavesdropping by unauthorized wireless users. The values for the keys must be set up exactly the same on the access points as they are on the wireless client computers.
Apply	Click **Apply** to save your changes back to the ZyXEL device.
Reset	Click **Reset** to begin configuring this screen afresh.

6.4 Configuring MAC Filter

The MAC filter screen allows you to configure the ZyXEL device to give exclusive access to specific devices (**Allow Association**) or exclude specific devices from accessing the ZyXEL device (**Deny Association**). The Prestige can be configured to give exclusive access to up to 32 devices or exclude up to 32 devices from accessing the Prestige. The ZyWALL can be configured to give exclusive access to up to 12 devices or exclude up to 12 devices from accessing the ZyWALL. Every Ethernet device has a unique MAC (Media Access

Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02. You need to know the MAC address of the devices to configure this screen.

Select a device and then click **Configuration > WLAN** > **MAC Filter**. The screen appears as shown next.

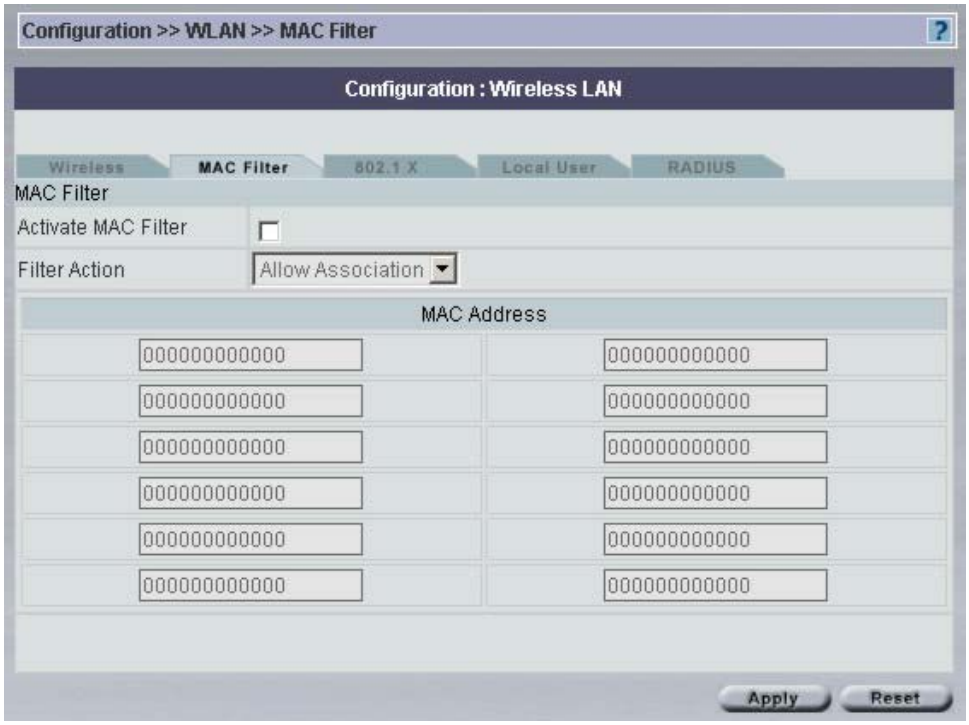


Figure 6-3 Configuration > WLAN > MAC Filter

Table 6-2 Configuration > WLAN > MAC Filter

LABEL	DESCRIPTION
Activate MAC Filter	Enable MAC address filtering to have the router allow or deny access to wireless stations based on MAC addresses. Disable MAC address filtering to have the router not perform MAC filtering on the wireless stations.
Filter Action	Define the filter action for the list of MAC addresses in the MAC address filter table. Select **Deny Association** to block access to the router, MAC addresses not listed will be allowed to access the router. Select **Allow Association** to permit access to the router, MAC addresses not listed will be denied access to the router.
MAC Address	Enter the MAC addresses (in XXXXXXXXXXXX format) of the client computers that are allowed or denied access to the ZyXEL device in these address fields.
Apply	Click **Apply** to save your changes back to the ZyXEL device.
Reset	Click **Reset** to begin configuring this screen afresh.

6.5 802.1x Overview

The IEEE 802.1x standard outlines enhanced security methods for both the authentication of wireless stations and encryption key management. Authentication can be done using the local user database internal to the ZyXEL device or an external RADIUS server for an unlimited number of users.

6.5.1 Configuring 802.1x – ZyWALL

Select a ZyWALL device and then click **Configuration > WLAN** > **802.1x**. The screen appears as shown next.

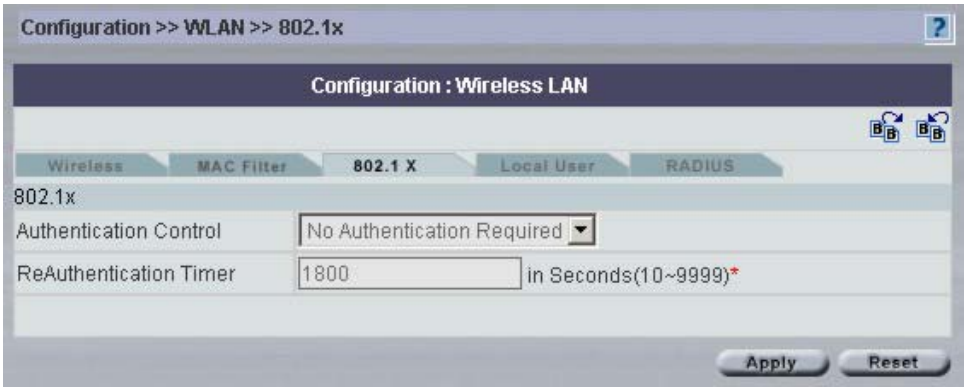


Figure 6-4 Configuration > WLAN > 802.1x – ZyWALL

The following table describes the fields in this screen

Table 6-3 Configuration > WLAN > 802.1x – ZyWALL

LABEL	DESCRIPTION
Authentication Control	Select **Authentication Required** to authenticate all wireless clients before they can access the wired network. Select **No Authentication Required** to allow all wireless clients to access your wired network without authentication. Select **No Access** to deny all wireless clients access to your wired network.
Reauthentication Timer	Specify the time interval between the RADIUS server's authentication checks of wireless users connected to the network. This field is activated only when you select **Authentication Required** in the **Authentication Type** field.
Apply	Click **Apply** to save your changes back to the ZyXEL device.
Reset	Click **Reset** to begin configuring this screen afresh.

6.5.2 Configuring 802.1x – Prestige

Select a Prestige device and then click **Configuration > WLAN** > **802.1x**. The screen appears as shown next.

Figure 6-5 Configuration > WLAN > 802.1x – Prestige

The following table describes the fields in this screen

Table 6-4 Configuration > WLAN > 802.1x – Prestige

LABEL	DESCRIPTION
Authentication Control	Select **Authentication Required** to authenticate all wireless clients before they can access the wired network. Select **No Authentication Required** to allow all wireless clients to access your wired network without authentication. Select **No Access** to deny all wireless clients access to your wired network.
Reauthentication Timer	Specify the time interval between the RADIUS server's authentication checks of wireless users connected to the network. This field is activated only when you select **Authentication Required** in the **Authentication Type** field.
Idle Timeout	The Prestige automatically disconnects a wireless station from the wired network after a period of inactivity. The wireless station needs to enter the username and password again before access to the wired network is allowed. This field is activated only when you select **Authentication Required** in the **Wireless Port Control** field. The default time interval is **3600** seconds (or 1 hour).

Table 6-4 Configuration > WLAN > 802.1x – Prestige

LABEL	DESCRIPTION
Authentication Databases	The authentication database contains wireless station login information. The local user database is the built-in database on the Prestige. The RADIUS is an external server. Use this drop-down list box to select which database the Prestige should use (first) to authenticate a wireless station. Before you specify the priority, make sure you have set up the corresponding database correctly first. Select **Local User Database Only** to have the Prestige just check the built-in user database on the Prestige for a wireless station's username and password. Select **RADIUS Only** to have the Prestige just check the user database on the specified RADIUS server for a wireless station's username and password. Select **Local first, then RADIUS** to have the Prestige first check the user database on the Prestige for a wireless station's username and password. If the user name is not found, the Prestige then checks the user database on the specified RADIUS server. Select **RADIUS first, then Local** to have the Prestige first check the user database on the specified RADIUS server for a wireless station's username and password. If the Prestige cannot reach the RADIUS server, the Prestige then checks the local user database on the Prestige. When the user name is not found or password does not match in the RADIUS server, the Prestige will not check the local user database and the authentication fails.
Apply	Click **Apply** to save your changes back to the ZyXEL device.
Reset	Click **Reset** to begin configuring this screen afresh.

6.6 Local User Database

By storing user profiles locally on the ZyXEL device, the ZyXEL device is able to authenticate VPN extended authentication clients or wireless clients without interacting with a network RADIUS server. However, there is a limit on the number of users you may authenticate in this way.

6.6.1 Configuring Local User Database

Select a device and then click **Configuration > WLAN** > **Local User Database**. The screen appears as shown next.

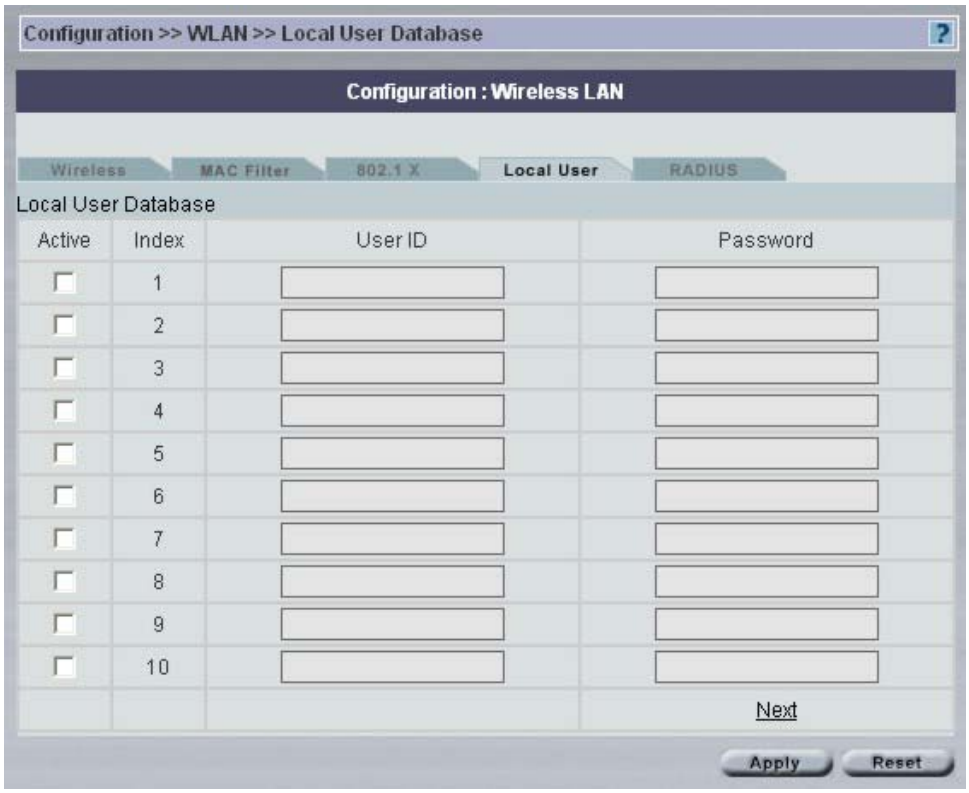


Figure 6-6 Configuration > WLAN > Local User

The following table describes the labels in this screen.

Table 6-5 Configuration > WLAN > Local User

LABEL	DESCRIPTION
Active	Select this check box to enable the user profile.
Index	This is the local user index number.
User ID	Enter the user name of the user profile.
Password	Enter a password up to 31 characters long for this user profile.
Next	Select Next to view the next page of **Local User Database** entries.
Apply	Click **Apply** to save your changes back to the ZyXEL device.
Reset	Click **Reset** to begin configuring this screen afresh.

6.6.2 RADIUS

RADIUS is based on a client-sever model that supports authentication and accounting, where access point is the client and the server is the RADIUS server. The RADIUS server handles the following tasks among others:

- **Authentication**

  Determines the identity of the users.

- **Accounting**

  Keeps track of the client's network activity.

RADIUS user is a simple package exchange in which the ZyXEL device acts as a message relay between the wireless client and the network RADIUS server.

Types of RADIUS Messages

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

- **Access-Request**

  Sent by the ZyXEL device requesting authentication.

- **Access-Reject**

  Sent by a RADIUS server rejecting access.

- **Access-Accept**

  Sent by a RADIUS server allowing access.

- **Access-Challenge**

  Sent by a RADIUS server requesting more information in order to allow access. The access point sends a proper response from the user and then sends another Access-Request message.

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

- **Accounting-Request**

  Sent by the ZyXEL device requesting accounting.

- **Accounting-Response**

  Sent by the RADIUS server to indicate that it has started or stopped accounting.

In order to ensure network security, the ZyXEL device and the RADIUS server use a shared secret key, which is a password, they both know. The key is not sent over the network. In addition to the shared key, password information exchanged is also encrypted to protect the network from unauthorized access.

6.6.3 EAP Authentication Overview

EAP (Extensible Authentication Protocol) is an authentication protocol that runs on top of the IEEE802.1x transport mechanism in order to support multiple types of user authentication. By using EAP to interact with an EAP-compatible RADIUS server, the access point helps a wireless station and a RADIUS server perform authentication.

The type of authentication you use depends on the RADIUS server or the AP. The ZyXEL device supports EAP-TLS and EAP-TTLS with RADIUS.

The ZyXEL device supports EAP-MD5 (Message-Digest Algorithm 5) with the local user database.

The details below provide a general description of how IEEE 802.1x EAP authentication works. For an example list of EAP-MD5 authentication steps, see the IEEE 802.1x chapter in the *Appendices*.

- The wireless station sends a “start” message to the ZyXEL device.
- The ZyXEL device sends a “request identity” message to the wireless station for identity information.
- The wireless station replies with identity information, including username and password.

- The RADIUS server checks the user information against its user profile database and determines whether or not to authenticate the wireless station.

6.7 Configuring RADIUS

Use the **RADIUS** screen if you want to use an external server to perform authentication.

Select a device, then click **Configuration > WLAN** > **RADIUS**. The screen appears as shown next.

Figure 6-7 Configuration > WLAN > RADIUS

The following table describes the fields in this screen

Table 6-6 Configuration > WLAN > RADIUS

LABEL	DESCRIPTION
Activate Authentication	Enable this feature to have the ZyXEL device use an external authentication server in performing user authentication. Disable this feature if you will not use an external authentication server. If you disable this feature, you can still set the ZyXEL device to perform user authentication using the local user database.
Server IP	Enter the IP address of the external authentication server in dotted decimal notation.
Port	The default port of the RADIUS server for authentication is **1812**. You need not change this value unless your network administrator instructs you to do so with additional information.
Key	Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external authentication server and the access points. The key is not sent over the network. This key must be the same on the external authentication server and ZyXEL device.
Activate Accounting	Enable this feature to do user accounting through an external authentication server.

Table 6-6 Configuration > WLAN > RADIUS

LABEL	DESCRIPTION
Server IP	Enter the IP address of the external accounting server in dotted decimal notation.
Port	The default port of the RADIUS server for accounting is **1813**. You need not change this value unless your network administrator instructs you to do so with additional information.
Key	Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external accounting server and the access points. The key is not sent over the network. This key must be the same on the external accounting server and ZyXEL device.
Apply	Click **Apply** to save your changes back to the ZyXEL device.
Reset	Click **Reset** to begin configuring this screen afresh.

7 Configuration > DMZ

7.1 DMZ Overview

The DeMilitarized Zone (DMZ) auto-negotiating 10/100 Mbps Ethernet port provides a way for public servers (Web, e-mail, FTP, etc.) to be visible to the outside world (while still being protected from DoS (Denial of Service) attacks such as SYN flooding and Ping of Death). These public servers can also still be accessed from the secure LAN.

By default the firewall allows traffic between the WAN and the DMZ, traffic from the DMZ to the LAN is denied, and traffic from the LAN to the DMZ is allowed. Internet users can have access to host servers on the DMZ but no access to the LAN, unless special filter rules allowing access were configured by the administrator or the user is an authorized remote user.

It is highly recommended that you connect all of your public servers to the DMZ port. If you have more than one public server, connect a hub to the DMZ port.

It is also highly recommended that you keep all sensitive information off of the public servers connected to the DMZ port. Store sensitive information on LAN computers.

7.2 DMZ Addresses

You can assign public or private IP addresses to computers connected to the DMZ port.

With public IP addresses, the WAN and DMZ ports must use public IP addresses that are on separate subnets. See the appendices for information on IP subnetting.

If the DMZ computers use private IP addresses, go to the **WAN IP** screen and select **SUA Only** or **Full Feature** in the **Network Address Translation** field. Configure NAT mapping rules for the private IP addresses of the computers on the DMZ.

7.3 Configuring DMZ

Select a ZyWALL device and from the **Configuration Screen**, click **DMZ**. The screen appears as shown next.

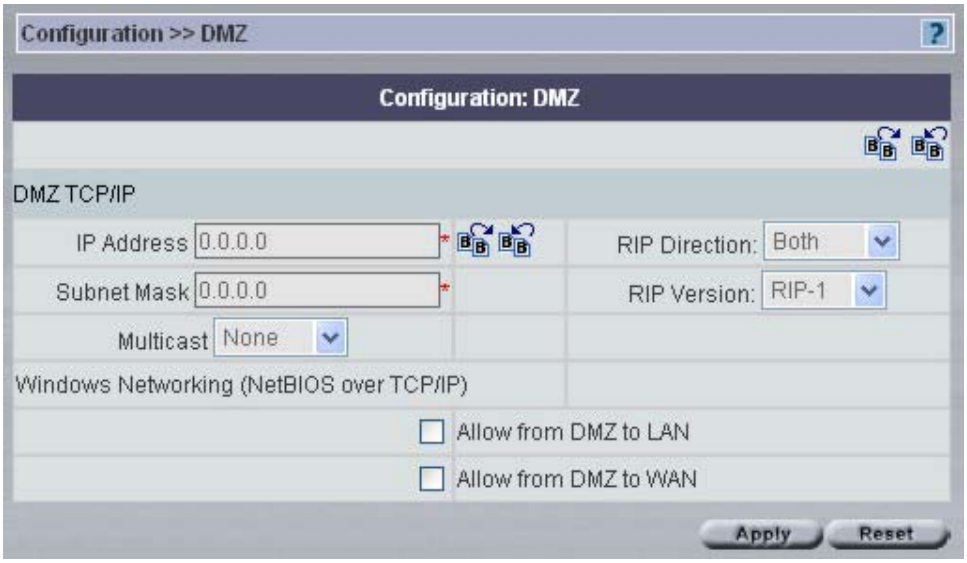


Figure 7-1 Configuration > DMZ

The following table describes the labels in this screen.

Table 7-1 Configuration > DMZ

LABEL	DESCRIPTION
DMZ TCP/IP	
IP Address	Type the IP address of your ZyWALL in dotted decimal notation 192.168.1.1 (factory default).
Subnet Mask	The subnet mask specifies the network number portion of an IP address. Your ZyWALL will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the ZyWALL 255.255.255.0.
RIP Direction	RIP (Routing Information Protocol, RFC1058 and RFC 1389) allows a router to exchange routing information with other routers. The **RIP Direction** field controls the sending and receiving of RIP packets. Select the RIP direction from **Both**/**In Only**/**Out Only**/**None**. When set to **Both** or **Out Only**, the ZyWALL will broadcast its routing table periodically. When set to **Both** or **In Only**, it will incorporate the RIP information that it receives; when set to **None**, it will not send any RIP packets and will ignore any RIP packets received. Both is the default.
RIP Version	The **RIP Version** field controls the format and the broadcasting method of the RIP packets that the ZyWALL sends (it recognizes both formats when receiving). **RIP-1** is universally supported but RIP-2 carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology. Both **RIP-2B** and **RIP-2M** sends the routing data in RIP-2 format; the difference being that **RIP-2B** uses subnet broadcasting while **RIP-2M** uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also. By default, RIP direction is set to **Both** and the Version set to **RIP-1**.

Table 7-1 Configuration > DMZ

LABEL	DESCRIPTION
Multicast	Select **IGMP V-1** or **IGMP V-2** or **None**. IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see *sections 4 and 5 of RFC 2236*.
Windows Networking (NetBIOS over TCP/IP)	
Allow from DMZ to LAN	Click this option to forward NetBIOS packets from the DMZ port to the LAN port.
Allow from DMZ to WAN	Click this option to forward NetBIOS packets from the DMZ port to the WAN port.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to refresh the current screen.

8 Configuration > WAN

You will see different WAN screens depending on whether you're configuring a ZyWALL or Prestige device.

Be extremely vigilant when configuring a device's WAN as an incorrect configuration could result in the device being inaccessible from Vantage (or by the web configurator from the WAN) and may necessitate a site visit to correct.

8.1 General WAN – ZyWALL

TCP/IP Priority (Metric)

The metric represents the "cost of transmission". A router determines the best route for transmission by choosing a path with the lowest "cost". RIP routing uses hop count as the measurement of cost, with a minimum of "1" for directly connected networks. The number must be between "1" and "15"; a number greater than "15" means the link is down. The smaller the number, the lower the "cost".

The metric sets the priority for the ZyXEL device's routes to the Internet. If any two of the default routes have the same metric, the ZyXEL device uses the following pre-defined priorities:

1. Normal route: designated by the ISP.
2. Traffic-redirect route. Traffic redirect forwards WAN traffic to a backup gateway when the ZyXEL device cannot connect to the Internet through its normal gateway. Connect the backup gateway on the WAN so that the ZyXEL device still provides firewall protection.
3. Dial-backup route.

For example, if the normal route has a metric of "1" and the traffic-redirect route has a metric of "2" and dial-backup route has a metric of "3", then the normal route acts as the primary default route. If the normal route fails to connect to the Internet, the ZyXEL device tries the traffic-redirect route next. In the same manner, the ZyXEL device uses the dial-backup route if the traffic-redirect route also fails.

If you want the dial-backup route to take first priority over the traffic-redirect route or even the normal route, all you need to do is set the dial-backup route's metric to "1" and the others to "2" (or greater).

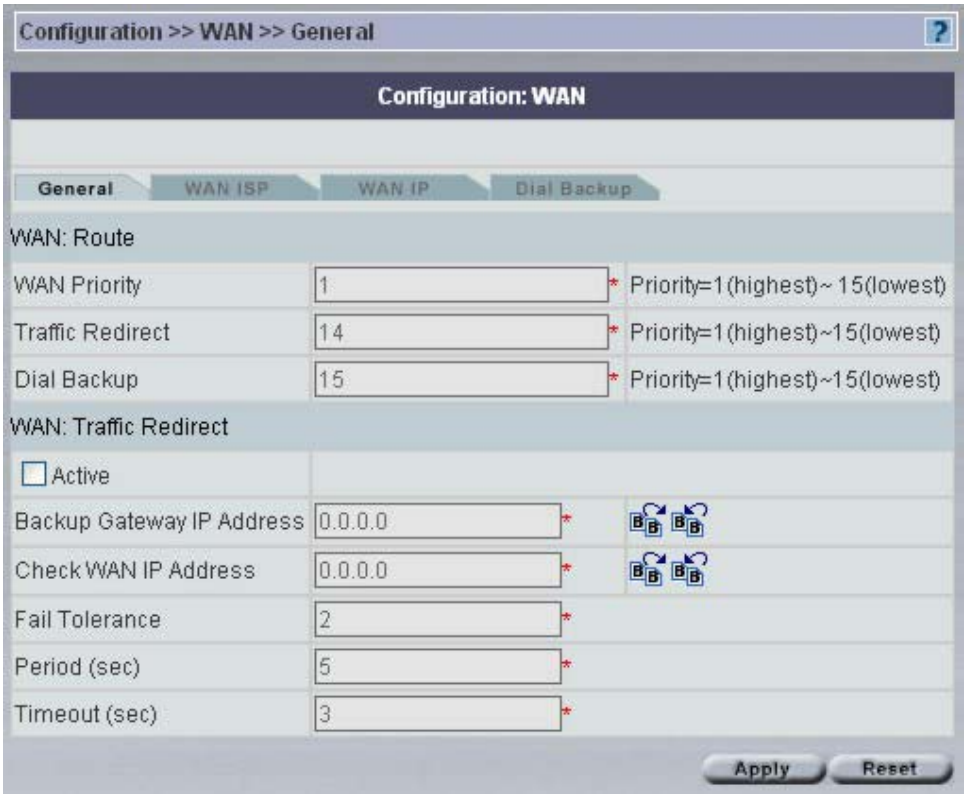


Figure 8-1 Configuration > WAN > General – ZyWALL

The following table describes the fields in this screen

Table 8-1 Configuration > WAN > General – ZyWALL

LABEL	DESCRIPTION
WAN: Route	
WAN Traffic Redirect Dial Backup	The default WAN connection is "1' as your broadband connection via the WAN port should always be your preferred method of accessing the WAN. The default priority of the routes is **WAN**, **Traffic Redirect** and then **Dial Backup** (dial backup does not apply to all ZyXEL device models): You have two choices for an auxiliary connection in the event that your regular WAN connection goes down. If **Dial Backup** is preferred to **Traffic Redirect**, then type "14" in the **Dial Backup Priority (metric)** field (and leave the **Traffic Redirect Priority (metric)** at the default of "15").
WAN: Traffic Redirect	
Active	Select this check box to have the ZyXEL device use traffic redirect if the normal WAN connection goes down.
Backup Gateway IP Address	Type the IP address of your backup gateway in dotted decimal notation. The ZyXEL device automatically forwards traffic to this IP address if the ZyXEL device's Internet connection terminates.

Table 8-1 Configuration > WAN > General – ZyWALL

LABEL	DESCRIPTION
Check WAN IP Address	Configuration of this field is optional. If you do not enter an IP address here, the ZyXEL device will use the default gateway IP address. Configure this field to test the ZyXEL device's WAN accessibility. Type the IP address of a reliable nearby computer (for example, your ISP's DNS server address). If you are using PPTP or PPPoE Encapsulation, type "0.0.0.0" to configure the ZyXEL device to check the PVC (Permanent Virtual Circuit) or PPTP tunnel.
Fail Tolerance	Type the number of times the ZyXEL device may attempt and fail to connect to the Internet before traffic is forwarded to the backup gateway.
Period (sec)	Type the number of seconds for the ZyXEL device to wait between checks to see if it can connect to the WAN IP address (**Check WAN IP Address** field) or default gateway. Allow more time if your destination IP address handles lots of traffic.
Timeout (sec)	Type the number of seconds for the ZyXEL device to wait for a ping response from the IP Address in the **Check WAN IP Address** field before it times out. The WAN connection is considered "down" after the ZyXEL device times out the number of times specified in the **Fail Tolerance** field. Use a higher value in this field if your network is busy or congested.
Apply	Click **Apply** to save your changes back to the ZyXEL device.
Reset	Click **Reset** to begin configuring this screen afresh.

8.1.1 WAN ISP – ZyWALL

The screen differs by the encapsulation type chosen.

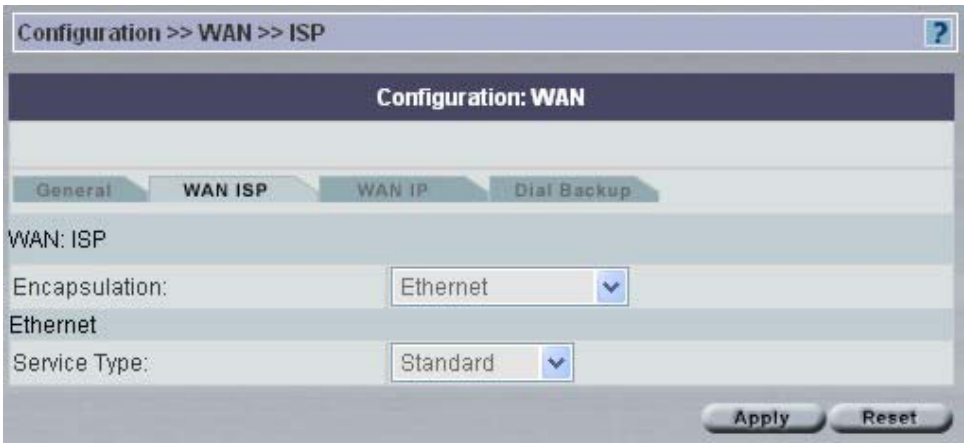


Figure 8-2 Configuration > WAN > ISP (Ethernet) – ZyWALL

Ethernet Encapsulation

The following table describes the labels in the **Ethernet** encapsulation screen.

Table 8-2 Configuration > WAN > ISP (Ethernet) – ZyWALL

LABEL	DESCRIPTION
Encapsulation	You must choose the Ethernet option when the WAN port is used as a regular Ethernet.

Table 8-2 Configuration > WAN > ISP (Ethernet) – ZyWALL

LABEL	DESCRIPTION
Service Type	Choose from **Standard**, **Telstra** (RoadRunner Telstra authentication method), **RR-Manager** (Roadrunner Manager authentication method), **RR-Toshiba** (Roadrunner Toshiba authentication method) or **Telia Login**. The following fields do not appear with the **Standard** service type.
Apply	Click **Apply** to save your changes back to the ZyXEL device.
Reset	Click **Reset** to begin configuring this screen afresh.

PPPoE Encapsulation

The ZyXEL device supports PPPoE (Point-to-Point Protocol over Ethernet). PPPoE is an IETF Draft standard (RFC 2516) specifying how a personal computer (PC) interacts with a broadband modem (DSL, cable, wireless, etc.) connection. The **PPPoE** option is for a dial-up connection using PPPoE.

For the service provider, PPPoE offers an access and authentication method that works with existing access control systems (for example Radius). PPPoE provides a login and authentication method that the existing Microsoft Dial-Up Networking software can activate, and therefore requires no new learning or procedures for Windows users.

One of the benefits of PPPoE is the ability to let you access one of multiple network services, a function known as dynamic service selection. This enables the service provider to easily create and offer new IP services for individuals.

Operationally, PPPoE saves significant effort for both you and the ISP or carrier, as it requires no specific configuration of the broadband modem at the customer site.

By implementing PPPoE directly on the ZyXEL device (rather than individual computers), the computers on the LAN do not need PPPoE software installed, since the ZyXEL device does that part of the task. Furthermore, with NAT, all of the LANs' computers will have access.

Figure 8-3 Configuration > WAN > ISP (PPPoE) – ZyWALL

The following table describes the labels in the **PPPoE** screen.

Table 8-3 Configuration > WAN > ISP (PPPoE) – ZyWALL

LABEL	DESCRIPTION
ISP Parameters for Internet Access	
Encapsulation	The PPPoE choice is for a dial-up connection using PPPoE. The router supports PPPoE (Point-to-Point Protocol over Ethernet). PPPoE is an IETF Draft standard (RFC 2516) specifying how a personal computer (PC) interacts with a broadband modem (i.e. xDSL, cable, wireless, etc.) connection. Operationally, PPPoE saves significant effort for both the end user and ISP/carrier, as it requires no specific configuration of the broadband modem at the customer site. By implementing PPPoE directly on the router rather than individual computers, the computers on the LAN do not need PPPoE software installed, since the router does that part of the task. Further, with NAT, all of the LAN's computers will have access.
Service Name	Type the PPPoE service name provided to you. PPPoE uses a service name to identify and reach the PPPoE server.
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the User Name above.
Retype to Confirm	Type your password again to make sure that you have entered it correctly.
Nailed-Up Connection	Select **Nailed-Up Connection** if you do not want the connection to time out.
Idle Timeout	This value specifies the time in seconds that elapses before the router automatically disconnects from the PPPoE server.
Apply	Click **Apply** to save your changes back to the ZyXEL device.

Table 8-3 Configuration > WAN > ISP (PPPoE) – ZyWALL

LABEL	DESCRIPTION
Reset	Click **Reset** to begin configuring this screen afresh.

PPTP Encapsulation

Point-to-Point Tunneling Protocol (PPTP) is a network protocol that enables secure transfer of data from a remote client to a private server, creating a Virtual Private Network (VPN) using TCP/IP-based networks.

PPTP supports on-demand, multi-protocol and virtual private networking over public networks, such as the Internet.

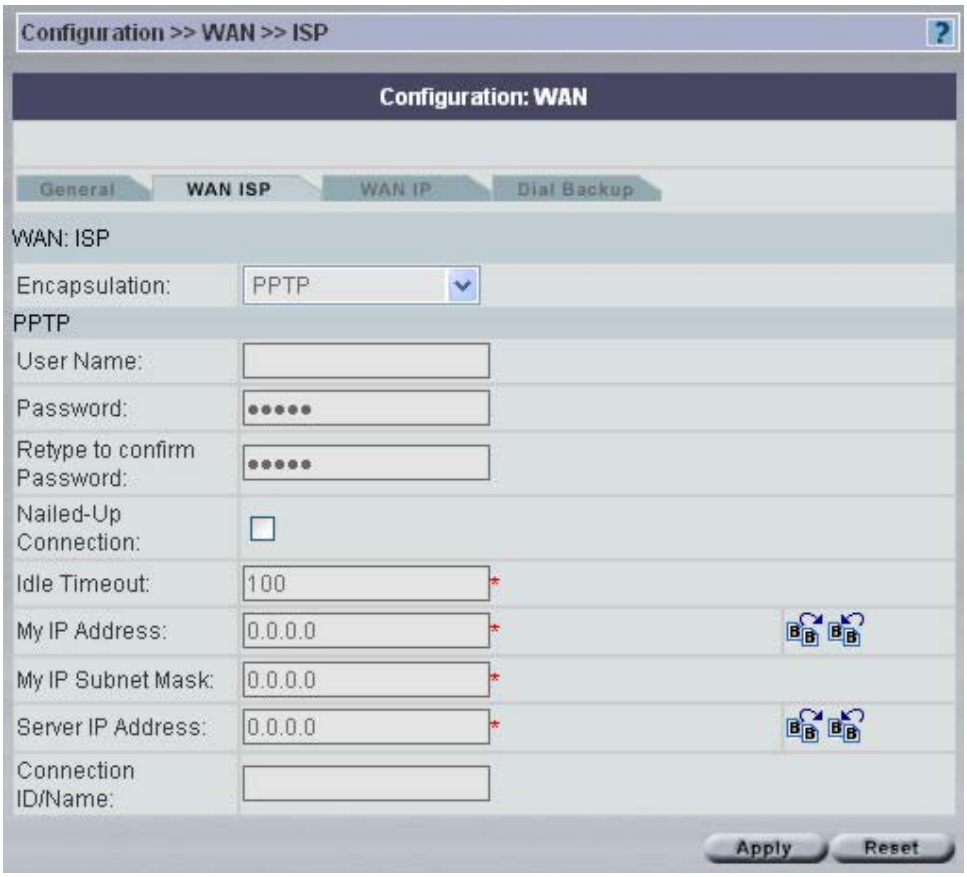


Figure 8-4 Configuration > WAN > ISP (PPTP) – ZyWALL

The following table describes the labels in the **PPTP** screen.

Table 8-4 Configuration > WAN > ISP (PPTP) – ZyWALL

LABEL	DESCRIPTION
ISP Parameters for Internet Access	

Table 8-4 Configuration > WAN > ISP (PPTP) – ZyWALL

LABEL	DESCRIPTION
Encapsulation	Point-to-Point Tunneling Protocol (PPTP) is a network protocol that enables secure transfer of data from a remote client to a private server, creating a Virtual Private Network (VPN) using TCP/IP-based networks. PPTP supports on-demand, multi-protocol, and virtual private networking over public networks, such as the Internet. The ZyXEL device supports only one PPTP server connection at any given time. To configure a PPTP client, you must configure the **User Name** and **Password** fields for a PPP connection and the PPTP parameters for a PPTP connection.
PPTP Configuration	
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the User Name above.
Retype to confirm Password	Type your password again to make sure that you have entered it correctly.
Nailed-up Connection	Select **Nailed-Up Connection** if you do not want the connection to time out.
Idle Timeout	This value specifies the time in seconds that elapses before the ZyXEL device automatically disconnects from the PPTP server.
My IP Address	Type the (static) IP address assigned to you by your ISP.
My IP Subnet Mask	The ZyXEL device will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the ZyXEL device.
Server IP Address	Type the IP address of the PPTP server.
Connection ID/Name	Type your identification name for the PPTP server.
Apply	Click **Apply** to save your changes back to the ZyXEL device.
Reset	Click **Reset** to begin configuring this screen afresh.

8.1.2 WAN IP – ZyWALL

Figure 8-5 Configuration > WAN > IP – ZyWALL

The following table describes the fields in this screen

Table 8-5 Configuration > WAN > IP – ZyWALL

LABEL	DESCRIPTION
WAN IP Address Assignment	
Get automatically from ISP	Select this option If your ISP did not assign you a fixed IP address. This is the default selection.
Use fixed IP address	Select this option If the ISP assigned a fixed IP address.
My WAN IP Address	Enter your WAN IP address in this field if you selected **Use Fixed IP Address.**
My WAN IP Subnet Mask	Enter the IP subnet mask (if your ISP gave you one) in this field if you selected **Use Fixed IP Address**.
Gateway IP Address	Enter the gateway IP address (if your ISP gave you one) in this field if you selected **Use Fixed IP Address**.

Table 8-5 Configuration > WAN > IP – ZyWALL

LABEL	DESCRIPTION
Private	This parameter determines if the ZyWALL will include the route to this remote node in its RIP broadcasts. If set to Yes, this route is kept private and not included in RIP broadcast. If No, the route to this remote node will be propagated to other hosts through RIP broadcasts.
RIP Direction	RIP (Routing Information Protocol) allows a router to exchange routing information with other routers. The **RIP Direction** field controls the sending and receiving of RIP packets. Choose **Both**, **None**, **In Only** or **Out Only**. When set to **Both** or **Out Only**, the ZyXEL device will broadcast its routing table periodically. When set to **Both** or **In Only**, the ZyXEL device will incorporate RIP information that it receives. When set to **None**, the ZyXEL device will not send any RIP packets and will ignore any RIP packets received. By default, **RIP Direction** is set to **Both**.
RIP Version	The **RIP Version** field controls the format and the broadcasting method of the RIP packets that the ZyXEL device sends (it recognizes both formats when receiving). Choose **RIP-1**, **RIP-2B** or **RIP-2M**. **RIP-1** is universally supported; but **RIP-2** carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology. Both **RIP-2B** and **RIP-2M** sends the routing data in RIP-2 format; the difference being that RIP-2B uses subnet broadcasting while RIP-2M uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also. By default, the **RIP Version** field is set to **RIP-1**.
Multicast	Choose **None** (default), **IGMP-V1** or **IGMP-V2**. IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see sections 4 and 5 of RFC 2236.
Windows Networking (NetBIOS over TCP/IP): NetBIOS (Network Basic Input/Output System) are TCP or UDP broadcast packets that enable a computer to connect to and communicate with a LAN. For some dial-up services such as PPPoE or PPTP, NetBIOS packets cause unwanted calls.	
Allow from WAN to LAN	Select this option to forward NetBIOS packets from the WAN port to the LAN port.
Allow Trigger Dial	Select this option to allow NetBIOS packets to initiate calls.
Apply	Click **Apply** to save your changes back to the ZyXEL device.
Reset	Click **Reset** to begin configuring this screen afresh.

8.1.3 Dial Backup – ZyWALL

Vantage can communicate with the device using Dial Backup if the main WAN connection goes down.

Traffic Redirect

Traffic redirect forwards WAN traffic to a backup gateway when the ZyWALL cannot connect to the Internet through its normal gateway. Connect the backup gateway on the WAN so that the ZyWALL still provides firewall protection. This feature is not available on all models.

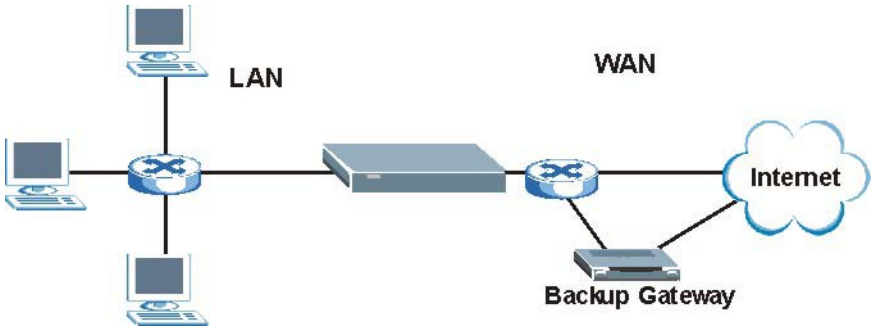


Figure 8-6 Traffic Redirect WAN Setup

The following network topology allows you to avoid triangle route security issues (see ZyWALL *Appendices*) when the backup gateway is connected to the LAN or DMZ. Use IP alias to configure the LAN into two or three logical networks with the ZyWALL itself as the gateway for each LAN network. Put the protected LAN in one subnet (Subnet 1 in the following figure) and the backup gateway in another subnet (Subnet 2). Configure a LAN to LAN/ZyWALL firewall rule that forwards packets from the protected LAN (Subnet 1) to the backup gateway (Subnet 2).

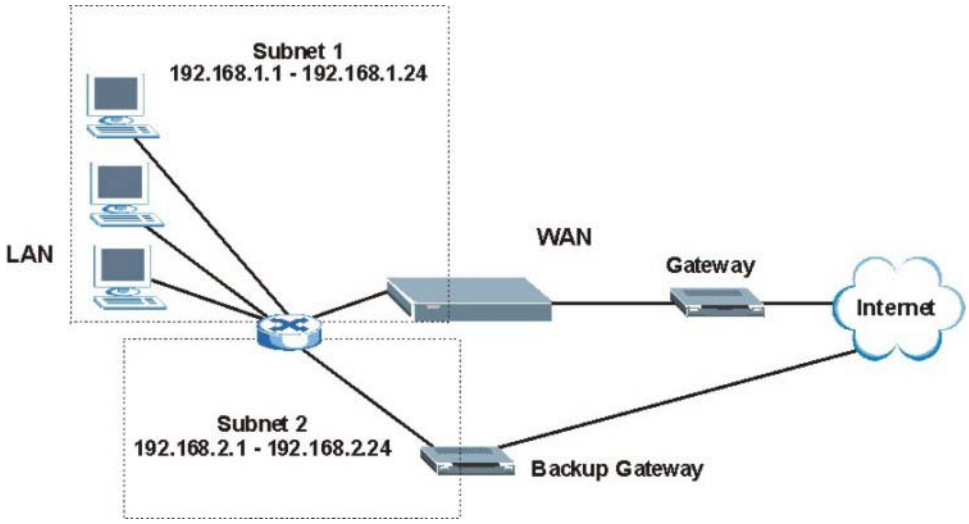


Figure 8-7 Traffic Redirect LAN Setup

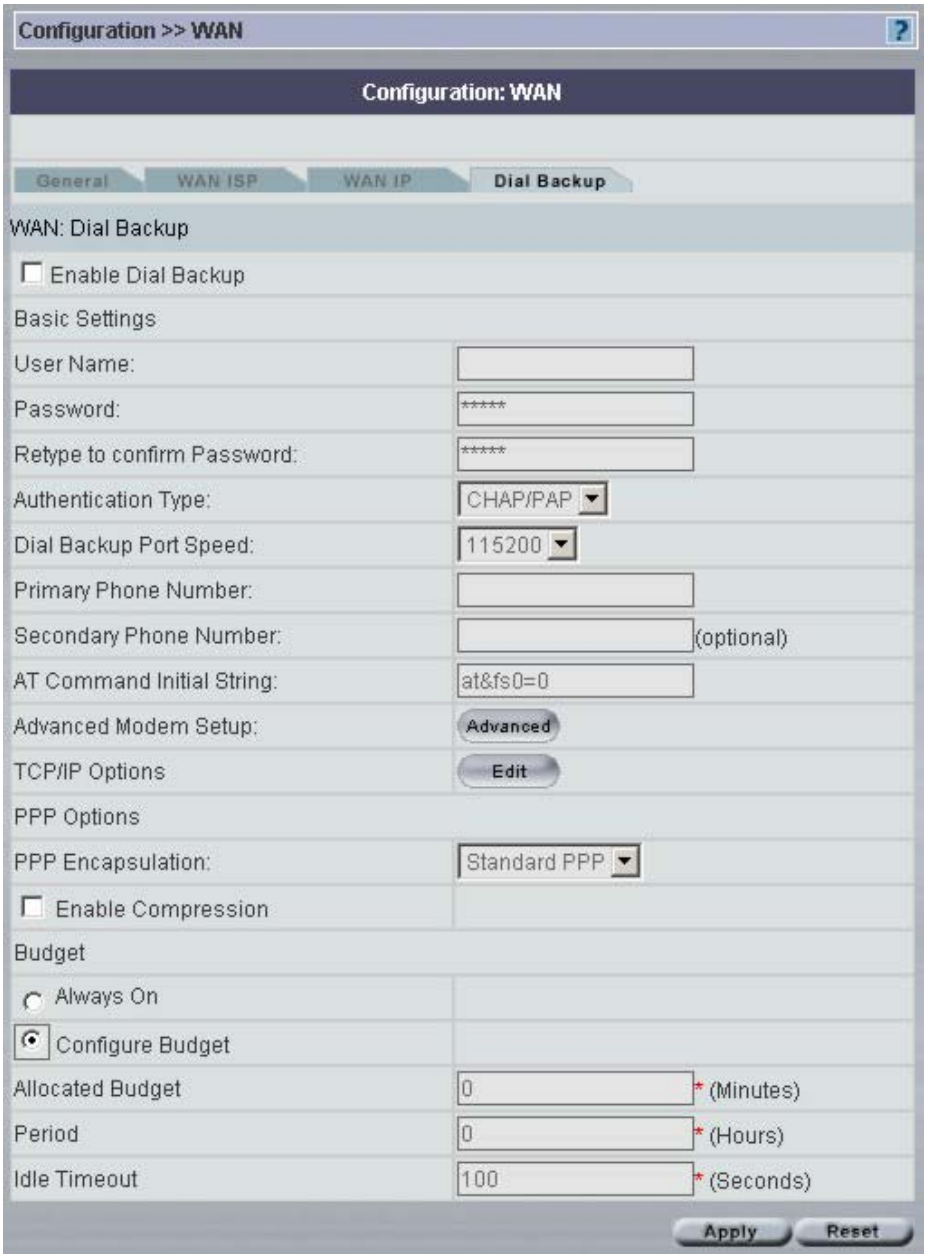


Figure 8-8 Configuration > WAN > Dial Backup – ZyWALL

The following table describes the labels in this screen.

Table 8-6 Configuration > WAN > Dial Backup – ZyWALL

LABEL	DESCRIPTION
Enable Dial Backup	Select this check box to turn on dial backup.
Basic Settings	
User Name	Type the user name assigned by your ISP.
Password	Type the password assigned by your ISP.

Table 8-6 Configuration > WAN > Dial Backup – ZyWALL

LABEL	DESCRIPTION
Retype to confirm Password	Type your password again to make sure that you have entered it correctly.
Authentication Type	Use the drop-down list box to select an authentication protocol for outgoing calls. Options are: **CHAP/PAP** - The ZyXEL device accepts either CHAP or PAP when requested by this remote node. **CHAP** - The ZyXEL device accepts CHAP only. **PAP** - The ZyXEL device accept PAP only.
Dial Backup Port Speed	Use the drop-down list box to select the speed of the connection between the Dial Backup port and the external device. Available speeds are: 9600, 19200, 38400, 57600, 115200 or 230400 bps.
Primary/ Secondary Phone Number	Type the first (primary) phone number from the ISP for this remote node. If the Primary Phone number is busy or does not answer, the ZyXEL device dials the Secondary Phone number if available. Some areas require dialing the pound sign # before the phone number for local calls. Include a # symbol at the beginning of the phone numbers as required.
AT Command Initial String	Type the AT command string to initialize the WAN device. Consult the manual of your WAN device connected to your Dial Backup port for specific AT commands.
Advanced Modem Setup	Click **Advanced** to display the **Advanced Modem Setup** screen and edit the details of your dial backup setup.
TCP/IP Options	Click **Edit** to display the **Dial Backup TCP/IP Options** screen.
PPP Options	
PPP Encapsulation	Select **CISCO PPP** from the drop-down list box if your dial backup WAN device uses Cisco PPP encapsulation, otherwise select **Standard PPP**.
Enable Compression	Select this check box to turn on stac compression.
Budget	
Always On	Select this check box to have the dial backup connection on all of the time.
Configure Budget	Select this check box to have the dial backup connection on during the time that you select.
Allocated Budget	Type the amount of time (in minutes) that the dial backup connection can be used during the time configured in the **Period** field. Set an amount that is less than the time period configured in the **Period** field.
Period	Type the time period (in hours) for how often the budget should be reset. For example, to allow calls to this remote node for a maximum of 10 minutes every hour, set the **Allocated Budget** to 10 (minutes) and the **Period** to 1 (hour).
Idle Timeout	Type the number of seconds of idle time (when there is no traffic from the ZyXEL device to the remote node) for the ZyXEL device to wait before it automatically disconnects the dial backup connection. This option applies only when the ZyXEL device initiates the call. The dial backup connection never times out if you set this field to "0" (it is the same as selecting **Always On**).
Apply	Click **Apply** to save your changes back to the ZyXEL device.
Reset	Click **Reset** to begin configuring this screen afresh.

8.1.4 Advanced Modem Setup – ZyWALL

AT Command Strings

For regular telephone lines, the default "Dial" string tells the modem that the line uses tone dialing. "ATDT" is the command for a switch that requires tone dialing. If your switch requires pulse dialing, change the string to "ATDP".

For ISDN lines, there are many more protocols and operational modes. Please consult the documentation of your TA. You may need additional commands in both "Dial" and "Init" strings.

DTR Signal

The majority of WAN devices default to hanging up the current call when the DTR (Data Terminal Ready) signal is dropped by the DTE. When the "Drop DTR When Hang Up" check box is selected, the ZyXEL device uses this hardware signal to force the WAN device to hang up, in addition to issuing the drop command "ATH".

Response Strings

The response strings tell the ZyXEL device the tags, or labels, immediately preceding the various call parameters sent from the WAN device. The response strings have not been standardized; please consult the documentation of your WAN device to find the correct tags.

Click the **Advanced** button in the **Advanced Modem Setup** in the **Dial Backup** screen to display the **Dial Backup Advanced** screen shown next.

Consult the manual of your WAN device connected to your dial backup port for specific AT commands.

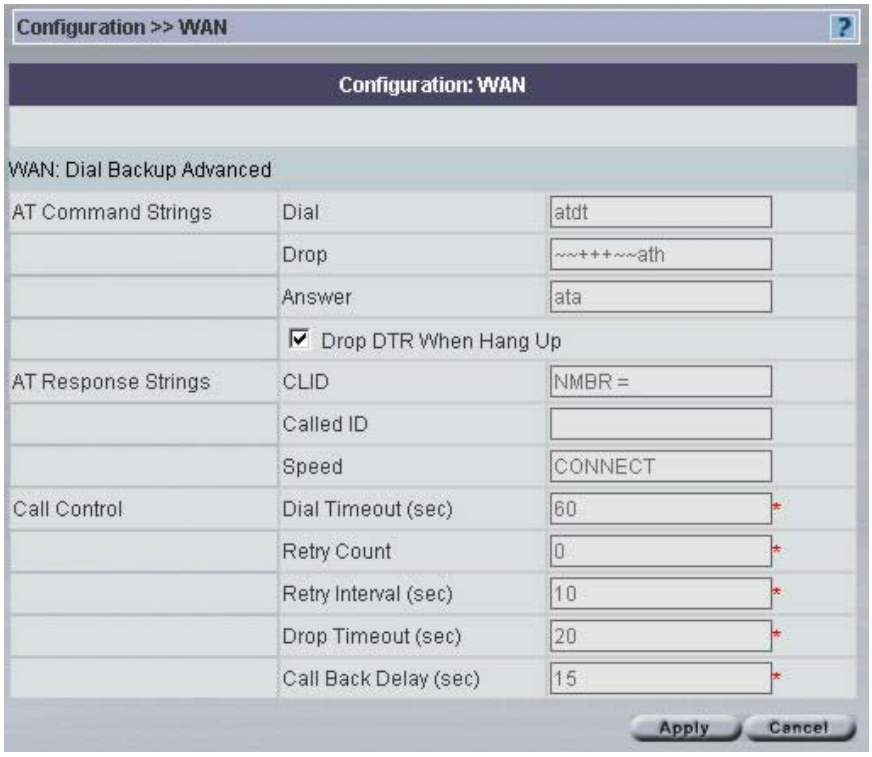


Figure 8-9 Configuration > WAN > Dial Backup > Advanced – ZyWALL

The following table describes the labels in this screen.

Table 8-7 Configuration > WAN > Dial Backup > Advanced – ZyWALL

LABEL	DESCRIPTION	EXAMPLE
AT Command Strings		
Dial	Type the AT Command string to make a call.	atdt
Drop	Type the AT Command string to drop a call. "~" represents a one second wait, for example, "~~~+++~~ath" can be used if your modem has a slow response time.	~~+++~~ath
Answer	Type the AT Command string to answer a call.	ata
Drop DTR When Hang Up	Select this check box to have the ZyXEL device drop the DTR (Data Terminal Ready) signal after the "AT Command String: Drop" is sent out.	
AT Response Strings		
CLID	Type the keyword that precedes the CLID (Calling Line Identification) in the AT response string. This lets the ZyXEL device capture the CLID in the AT response string that comes from the WAN device. CLID is required for CLID authentication.	NMBR
Called ID	Type the keyword preceding the dialed number.	
Speed	Type the keyword preceding the connection speed.	CONNECT
Call Control		
Dial Timeout (sec)	Type a number of seconds for the ZyXEL device to try to set up an outgoing call before timing out (stopping).	60
Retry Count	Type a number of times for the ZyXEL device to retry a busy or no-answer phone number before blacklisting the number.	0
Retry Interval (sec)	Type a number of seconds for the ZyXEL device to wait before trying another call after a call has failed. This applies before a phone number is blacklisted.	10
Drop Timeout (sec)	Type the number of seconds for the ZyXEL device to wait before dropping the DTR signal if it does not receive a positive disconnect confirmation.	20
Call Back Delay (sec)	Type a number of seconds for the ZyXEL device to wait between dropping a callback request call and dialing the corresponding callback call.	15
Apply	Click **Apply** to save your changes back to the ZyXEL device.	
Cancel	Click **Cancel** to begin configuring this screen afresh.	

8.1.5 Edit Dial Backup – ZyWALL

Click **Edit** in the **TCP/IP** field in *Figure 8-8* to display the next screen.

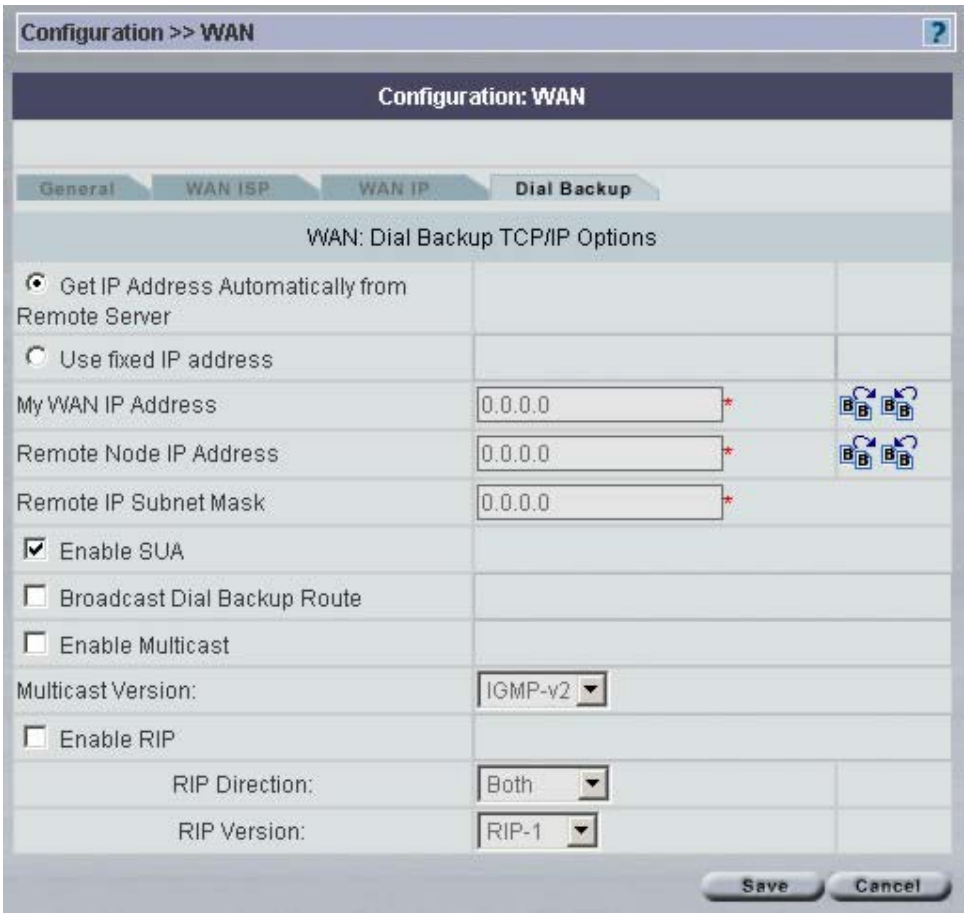


Figure 8-10 Configuration > WAN > Dial Backup > Edit – ZyWALL

The following table describes the fields in this screen

Table 8-8 Configuration > WAN > Dial Backup > Edit – ZyWALL

LABEL	DESCRIPTION
Get IP Address Automatically from Remote Server	Type the login name assigned by your ISP for this remote node.
Used Fixed IP Address	Select this check box if your ISP assigned you a fixed IP address, and then enter the IP address in the following field.
My WAN IP Address	Leave the field set to 0.0.0.0 (default) to have the ISP or other remote router dynamically (automatically) assign your WAN IP address if you do not know it. Type your WAN IP address here if you know it (static). This is the address assigned to your local ZyXEL device, not the remote router.
Remote Node IP Address	Leave this field set to 0.0.0.0 (default) to have the ISP or other remote router dynamically (automatically) send its IP address if you do not know it. Type the remote gateway's IP address here if you know it (static).
Remote IP Subnet Mask	Leave this field set to 0.0.0.0 (default) to have the ISP or other remote router dynamically send its subnet mask if you do not know it. Type the remote gateway's subnet mask here if you know it (static).

Table 8-8 Configuration > WAN > Dial Backup > Edit – ZyWALL

LABEL	DESCRIPTION
Enable SUA	Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network to a different IP address known within another network. **SUA** (Single User Account) is a subset of NAT that supports two types of mapping: Many-to-One and Server. When you select this option the ZyXEL device will use Address Mapping Set 255 in the SMT (see the section on menu 15.1 for more information). Select the check box to enable SUA. Clear the check box to disable SUA so the ZyXEL device does not perform any NAT mapping for the dial backup connection.
Broadcast Dial Backup Route	Select this check box to forward the backup route broadcasts to the WAN.
Enable Multicast	Select this check box to turn on IGMP (Internet Group Multicast Protocol). IGMP is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data.
Multicast Version	Select **IGMP-v1** or **IGMP-v2**. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see *sections 4* and *5* of *RFC 2236*.
Enable RIP	Select this check box to turn on RIP (Routing Information Protocol), which allows a router to exchange routing information with other routers.
RIP Direction	RIP (Routing Information Protocol, RFC1058 and RFC 1389) allows a router to exchange routing information with other routers. The **RIP Direction** field controls the sending and receiving of RIP packets. Select the RIP direction from **Both**/**In Only**/**Out Only**/**None**. When set to **Both** or **Out Only**, the ZyXEL device broadcasts its routing table periodically. When set to **Both** or **In Only**, it incorporates the RIP information that it receives; when set to **None**, it does not send any RIP packets and ignores any RIP packets received. **Both** is the default.
RIP Version	The **RIP Version** field controls the format and the broadcasting method of the RIP packets that the ZyXEL device sends (it recognizes both formats when receiving). **RIP-1** is universally supported but RIP-2 carries more information. **RIP-1** is probably adequate for most networks, unless you have an unusual network topology. Both **RIP-2B** and **RIP-2M** sends the routing data in RIP-2 format; the difference being that **RIP-2B** uses subnet broadcasting while **RIP-2M** uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also. By default, RIP direction is set to **Both** and the **Version** set to **RIP-1**.
Apply	Click **Apply** to save your changes back to the ZyXEL device.
Reset	Click **Reset** to begin configuring this screen afresh.

8.2 General WAN – Prestige

Traffic Shaping

Traffic Shaping is an agreement between the carrier and the subscriber to regulate the average rate and fluctuations of data transmission over an ATM network. This agreement helps eliminate congestion, which is important for transmission of real time data such as audio and video connections.

Peak Cell Rate (PCR) is the maximum rate at which the sender can send cells. This parameter may be lower (but not higher) than the maximum line speed. 1 ATM cell is 53 bytes (424 bits), so a maximum speed of 832Kbps gives a maximum PCR of 1962 cells/sec. This rate is not guaranteed because it is dependent on the line speed.

Sustained Cell Rate (SCR) is the mean cell rate of each bursty traffic source. It specifies the maximum average rate at which cells can be sent over the virtual connection. SCR may not be greater than the PCR.

Maximum Burst Size (MBS) is the maximum number of cells that can be sent at the PCR. After MBS is reached, cell rates fall below SCR until cell rate averages to the SCR again. At this time, more cells (up to the MBS) can be sent at the PCR again.

If the PCR, SCR or MBS is set to the default of "0", the system will assign a maximum value that correlates to your upstream line rate.

The following figure illustrates the relationship between PCR, SCR and MBS.

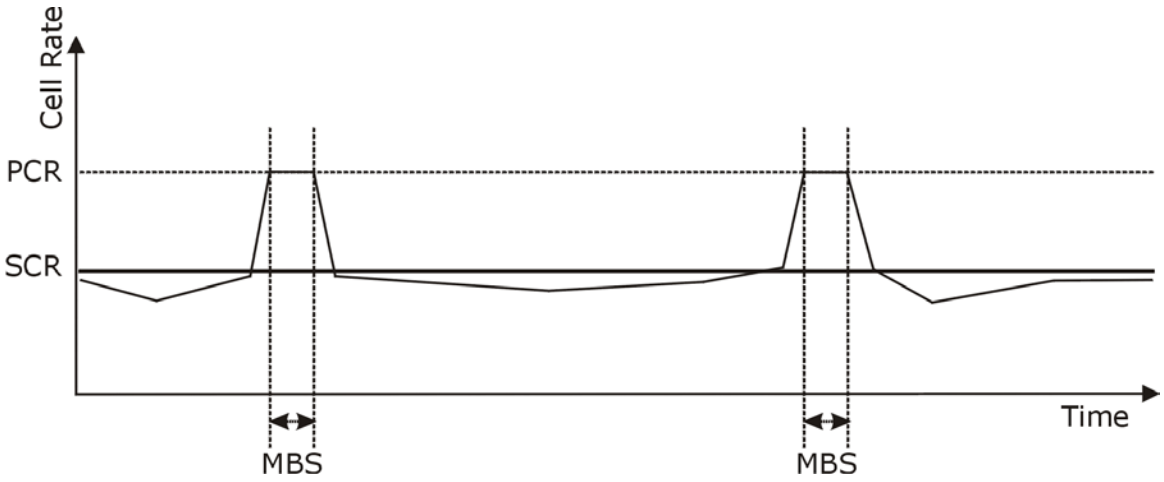


Figure 8-11 Example of Traffic Shaping

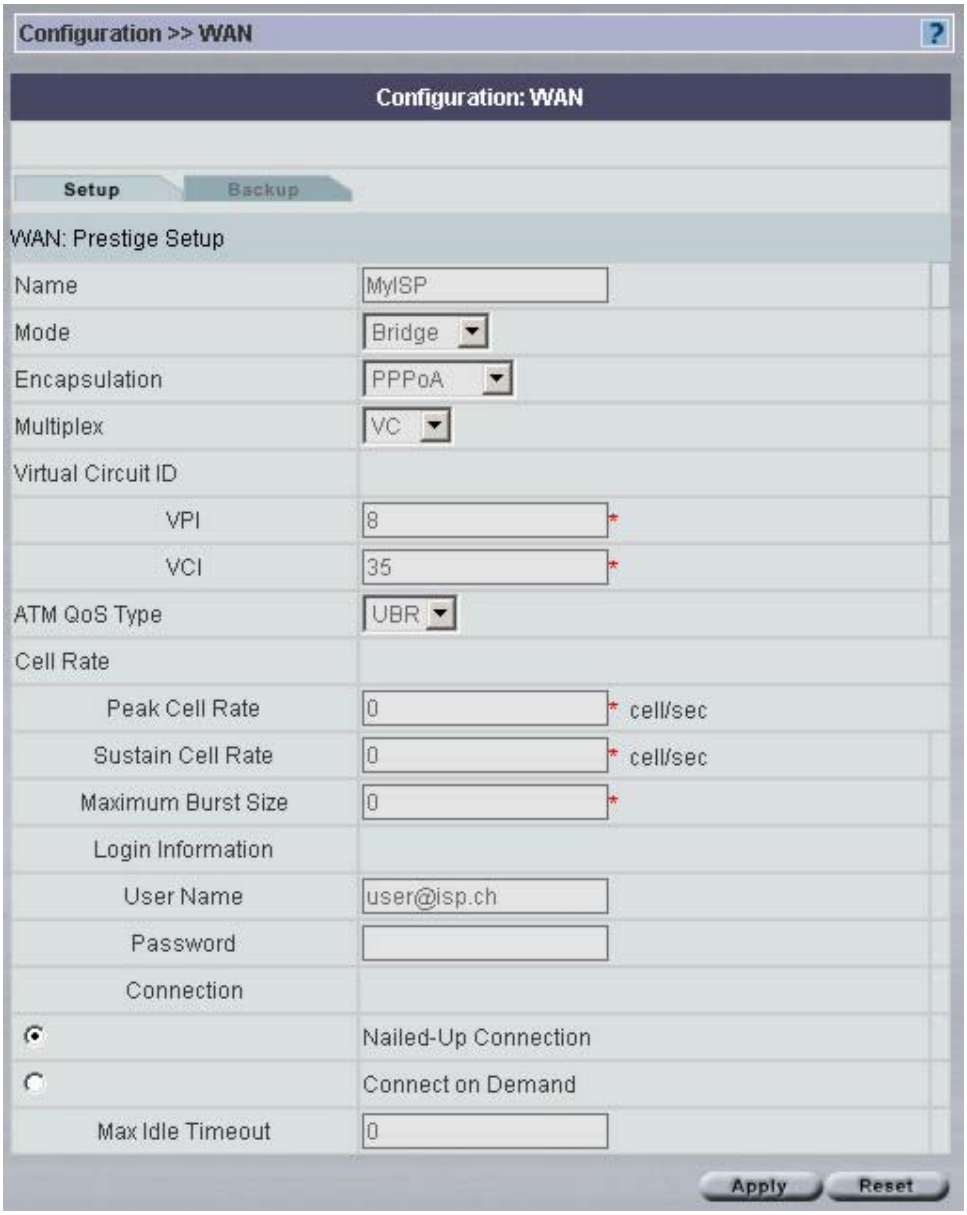


Figure 8-12 Configuration > WAN > Setup – Prestige – Bridge Mode

The following table describes the fields in this screen

Table 8-9 Configuration > WAN > Setup – Prestige – Bridge Mode

LABEL	DESCRIPTION
Name	Enter the name of your Internet Service Provider, e.g., MyISP. This information is for identification purposes only.
Mode	Select **Routing** (default) from the drop-down list box if your ISP allows multiple computers to share an Internet account. Otherwise select **Bridge**.

Table 8-9 Configuration > WAN > Setup – Prestige – Bridge Mode

LABEL	DESCRIPTION
Encapsulation	Select the method of encapsulation used by your ISP from the drop-down list box. Choices vary depending on the mode you select in the **Mode** field. If you select **Bridge** in the **Mode** field, select either **PPPoA** or **RFC 1483**. If you select **Routing** in the **Mode** field, select **PPPoA**, **RFC 1483**, **ENET ENCAP** or **PPPoE**.
Multiplex	Select the method of multiplexing used by your ISP from the drop-down list. Choices are **VC** or **LLC**.
Virtual Circuit ID	VPI (Virtual Path Identifier) and VCI (Virtual Channel Identifier) define a virtual circuit. Refer to the appendix for more information.
VPI	The valid range for the VPI is 0 to 255. Enter the VPI assigned to you.
VCI	The valid range for the VCI is 32 to 65535 (0 to 31 is reserved for local management of ATM traffic). Enter the VCI assigned to you.
ATM QoS Type	Select **CBR** (Continuous Bit Rate) to specify fixed (always-on) bandwidth for voice or data traffic. Select **UBR** (Unspecified Bit Rate) for applications that are non-time sensitive, such as e-mail. Select **VBR** (Variable Bit Rate) for bursty traffic and bandwidth sharing with other applications.
Cell Rate	Cell rate configuration often helps eliminate traffic congestion that slows transmission of real time data such as audio and video connections.
Peak Cell Rate	Divide the DSL line rate (bps) by 424 (the size of an ATM cell) to find the Peak Cell Rate (PCR). This is the maximum rate at which the sender can send cells. Type the PCR here.
Sustain Cell Rate	The Sustain Cell Rate (SCR) sets the average cell rate (long-term) that can be transmitted. Type the SCR, which must be less than the PCR. Note that system default is 0 cells/sec.
Maximum Burst Size	Maximum Burst Size (MBS) refers to the maximum number of cells that can be sent at the peak rate. Type the MBS, which is less than 65535.
Login Information	(PPPoA and PPPoE encapsulation only)
User Name	Enter the user name exactly as your ISP assigned. If assigned a name in the form user@domain where domain identifies a service name, then enter both components exactly as given.
Password	Enter the password associated with the user name above.
Connection (PPPoA and PPPoE encapsulation only)	The schedule rule(s) in the Prestige SMT menu 26 have priority over your **Connection** settings.
Nailed-Up Connection	Select **Nailed-Up Connection** when you want your connection up all the time. The Prestige will try to bring up the connection automatically if it is disconnected.
Connect on Demand	Select **Connect on Demand** when you don't want the connection up all the time and specify an idle time-out in the **Max Idle Timeout** field.

Table 8-9 Configuration > WAN > Setup – Prestige – Bridge Mode

LABEL	DESCRIPTION
Max Idle Timeout	Specify an idle time-out in the **Max Idle Timeout** field when you select **Connect on Demand**. The default setting is 0, which means the Internet session will not timeout.
Apply	Click **Apply** to save the changes.
Reset	Click **Reset** to begin configuring this screen afresh.

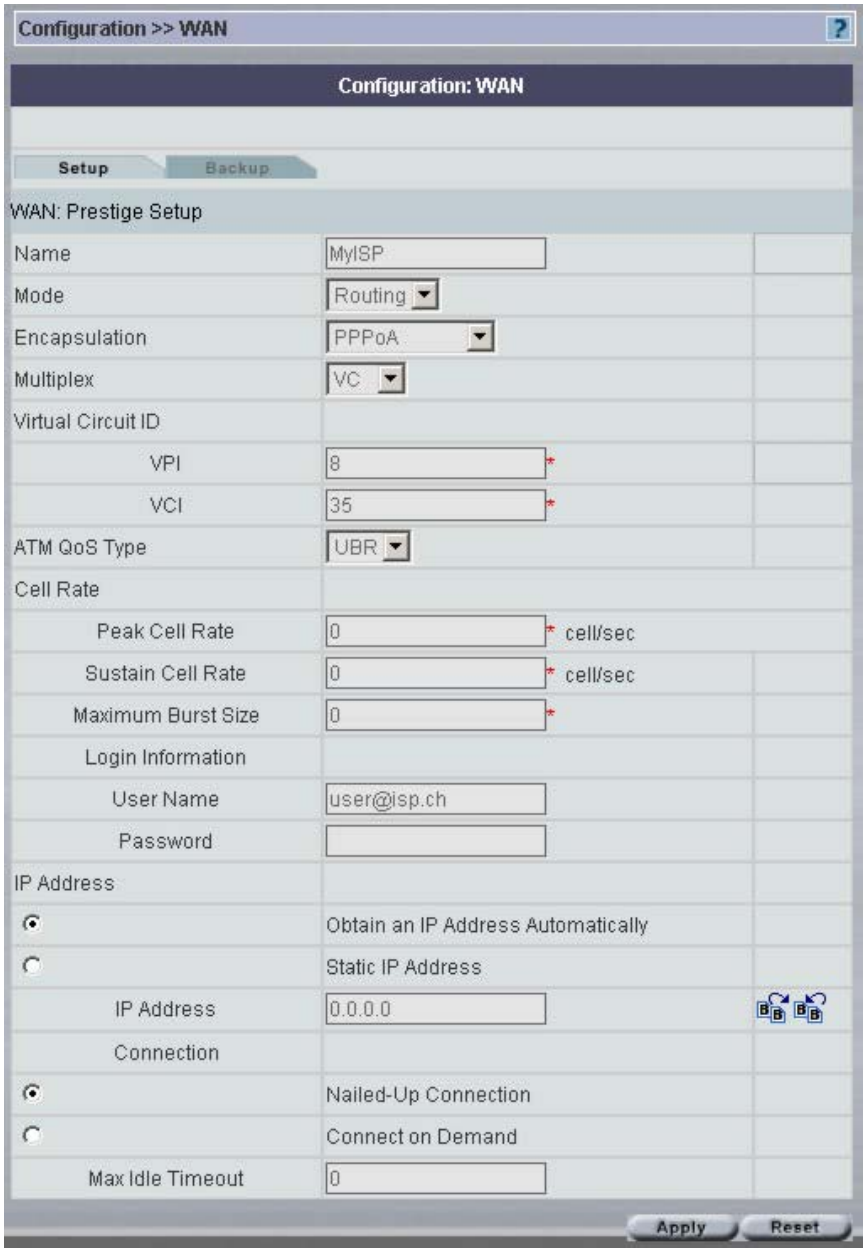


Figure 8-13 Configuration > WAN > Setup – Prestige – Routing Mode

The following table describes the fields in this screen.

Table 8-10 Configuration > WAN > Setup – Prestige – Routing Mode

LABEL	DESCRIPTION
Name	Enter the name of your Internet Service Provider, e.g., MyISP. This information is for identification purposes only.
Mode	Select **Routing** (default) from the drop-down list box if your ISP allows multiple computers to share an Internet account. Otherwise select **Bridge**.
Encapsulation	Select the method of encapsulation used by your ISP from the drop-down list box. Choices vary depending on the mode you select in the **Mode** field. If you select **Bridge** in the **Mode** field, select either **PPPoA** or **RFC 1483**. If you select **Routing** in the **Mode** field, select **PPPoA**, **RFC 1483**, **ENET ENCAP** or **PPPoE**.
Multiplex	Select the method of multiplexing used by your ISP from the drop-down list. Choices are **VC** or **LLC**.
Virtual Circuit ID	VPI (Virtual Path Identifier) and VCI (Virtual Channel Identifier) define a virtual circuit. Refer to the appendix for more information.
VPI	The valid range for the VPI is 0 to 255. Enter the VPI assigned to you.
VCI	The valid range for the VCI is 32 to 65535 (0 to 31 is reserved for local management of ATM traffic). Enter the VCI assigned to you.
ATM QoS Type	Select **CBR** (Continuous Bit Rate) to specify fixed (always-on) bandwidth for voice or data traffic. Select **UBR** (Unspecified Bit Rate) for applications that are non-time sensitive, such as e-mail. Select **VBR** (Variable Bit Rate) for bursty traffic and bandwidth sharing with other applications.
Cell Rate	Cell rate configuration often helps eliminate traffic congestion that slows transmission of real time data such as audio and video connections.
Peak Cell Rate	Divide the DSL line rate (bps) by 424 (the size of an ATM cell) to find the Peak Cell Rate (PCR). This is the maximum rate at which the sender can send cells. Type the PCR here.
Sustain Cell Rate	The Sustain Cell Rate (SCR) sets the average cell rate (long-term) that can be transmitted. Type the SCR, which must be less than the PCR. Note that system default is 0 cells/sec.
Maximum Burst Size	Maximum Burst Size (MBS) refers to the maximum number of cells that can be sent at the peak rate. Type the MBS, which is less than 65535.
Login Information	(PPPoA and PPPoE encapsulation only)
Service Name	This field is only available when **PPPoE** encapsulation is selected. Type the **PPPoE** service name provided to you. **PPPoE** uses a service name to identify and reach the **PPPoE** server.

Table 8-10 Configuration > WAN > Setup – Prestige – Routing Mode

LABEL	DESCRIPTION
PPPoE + PPPoE_Client_PC(PPPoE encapsulation only)	This field is only available when **PPPoE** encapsulation is selected. Select the checkbox to enable PPPoE passthrough. In addition to the Prestige's built-in PPPoE client, you can enable PPPoE pass through to allow up to ten hosts on the LAN to use PPPoE client software on their computers to connect to the ISP via the Prestige. Each host can have a separate account and a public WAN IP address. PPPoE pass through is an alternative to NAT for application where NAT is not appropriate.Disable PPPoE pass through if you do not need to allow hosts on the LAN to use PPPoE client software on their computers to connect to the ISP.
User Name	Enter the user name exactly as your ISP assigned. If assigned a name in the form user@domain where domain identifies a service name, then enter both components exactly as given.
Password	Enter the password associated with the user name above.
IP Address	This option is available if you select **Routing** in the **Mode** field. A static IP address is a fixed IP that your ISP gives you. A dynamic IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet. The Single User Account feature can be used with either a dynamic or static IP address. Select **Obtain an IP Address Automatically** if you have a dynamic IP address; otherwise select **Static IP Address** and type your ISP assigned IP address in the **IP Address** field below.
Connection (PPPoA and PPPoE encapsulation only)	The schedule rule(s) in SMT menu 26 have priority over your **Connection** settings.
Nailed-Up Connection	Select **Nailed-Up Connection** when you want your connection up all the time. The Prestige will try to bring up the connection automatically if it is disconnected.
Connect on Demand	Select **Connect on Demand** when you don't want the connection up all the time and specify an idle time-out in the **Max Idle Timeout** field.
Max Idle Timeout	Specify an idle time-out in the **Max Idle Timeout** field when you select **Connect on Demand**. The default setting is 0, which means the Internet session will not timeout.
Apply	Click **Apply** to save the changes.
Reset	Click **Reset** to begin configuring this screen afresh.

8.2.1 WAN Backup - Prestige

The CON/AUX port on the Prestige can be used in reserve, as a traditional dial-up connection should the WAN port connection fail. To set up the auxiliary port (AUX) for the Prestige for use in the event that the regular WAN connection is dropped, first make sure you have set up the switch and port connections.

Traffic Redirect

Traffic redirect forwards traffic to a backup gateway when the Prestige cannot connect to the Internet. An example is shown in the figure below.

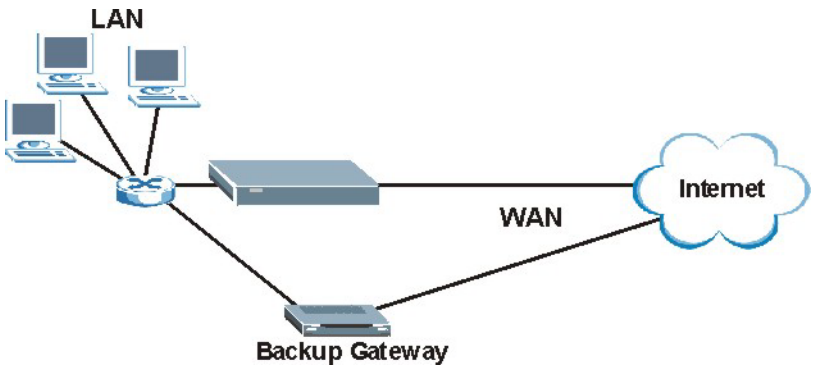


Figure 8-14 Traffic Redirect Example

The following network topology allows you to avoid triangle route security issues when the backup gateway is connected to the LAN or DMZ. Use IP alias to configure the LAN into two or three logical networks with the Prestige itself as the gateway for each LAN network. Put the protected LAN in one subnet (Subnet 1 in the following figure) and the backup gateway in another subnet (Subnet 2). Configure filters that allow packets from the protected LAN (Subnet 1) to the backup gateway (Subnet 2).

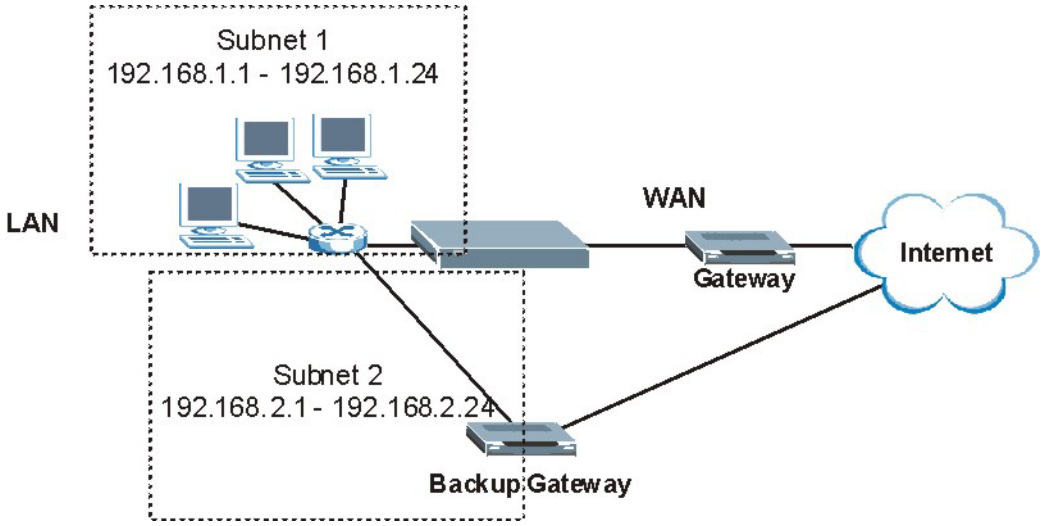


Figure 8-15 Traffic Redirect LAN Setup

8.2.2 Configuring WAN Backup - Prestige

To change your Prestige's WAN backup settings, click **WAN**, then **Backup**. The screen appears as shown.

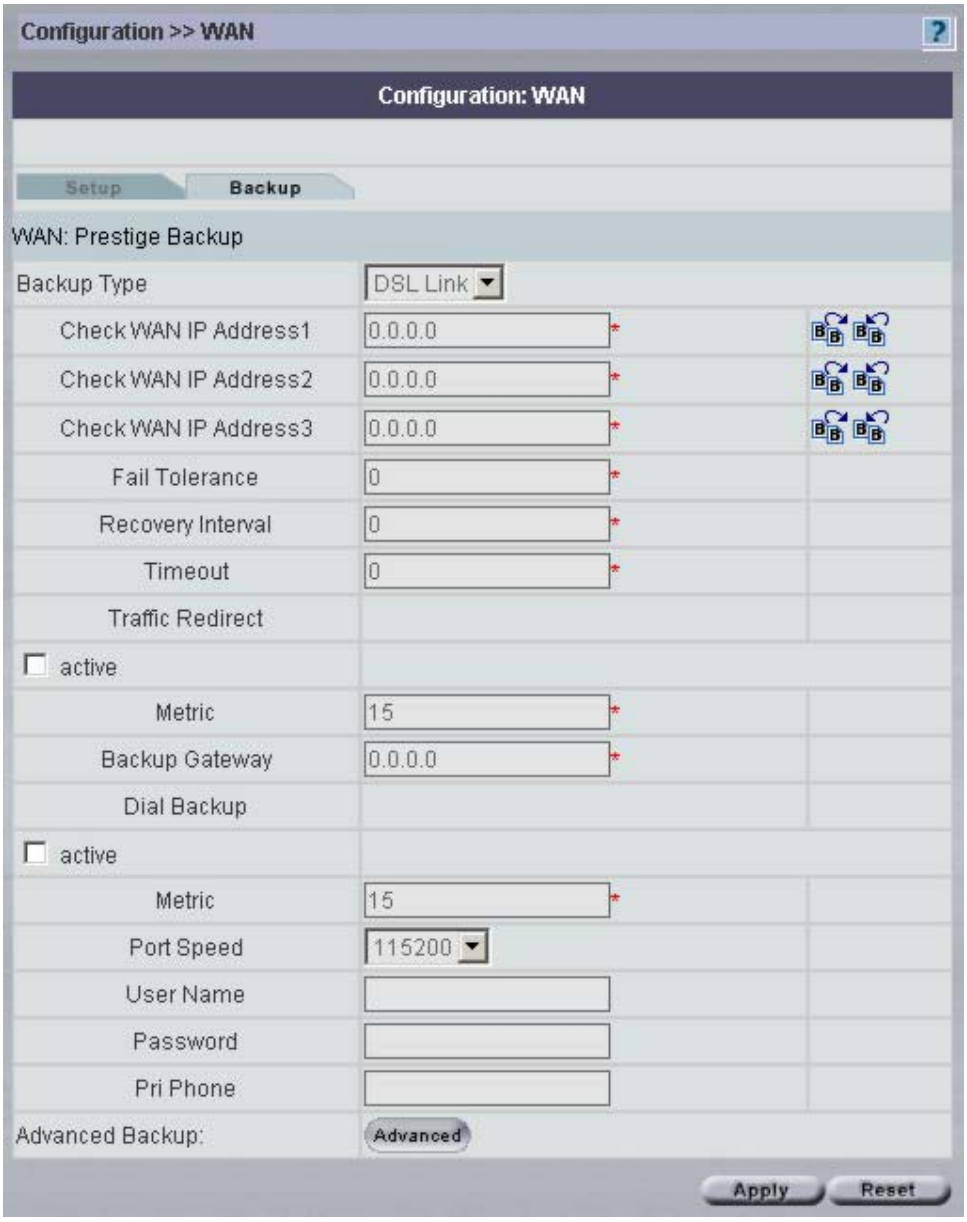


Figure 8-16 Configuration > WAN > Backup – Prestige

The following table describes the fields in this screen.

Table 8-11 WAN Backup – Prestige

LABEL	DESCRIPTION
Backup Type	Select the method that the Prestige uses to check the DSL connection. Select **DSL Link** to have the Prestige check if the connection to the DSLAM is up. Select **ICMP** to have the Prestige periodically ping the IP addresses configured in the **Check WAN IP Address** fields.
Check WAN IP Address1-3	Configure this field to test your Prestige's WAN accessibility. Type the IP address of a reliable nearby computer (for example, your ISP's DNS server address). **If you activate either traffic redirect or dial backup, you must configure at least one IP address here.** When using a WAN backup connection, the Prestige periodically pings the addresses configured here and uses the other WAN backup connection (if configured) if there is no response.
Fail Tolerance	Type the number of times (2 recommended) that your Prestige may ping the IP addresses configured in the **Check WAN IP Address** field without getting a response before switching to a WAN backup connection (or a different WAN backup connection).
Recovery Interval	When the Prestige is using a lower priority connection (usually a WAN backup connection), it periodically checks to whether or not it can use a higher priority connection. Type the number of seconds (30 recommended) for the Prestige to wait between checks. Allow more time if your destination IP address handles lots of traffic.
Timeout	Type the number of seconds (3 recommended) for your Prestige to wait for a ping response from one of the IP addresses in the **Check WAN IP Address** field before timing out the request. The WAN connection is considered "down" after the Prestige times out the number of times specified in the **Fail Tolerance** field. Use a higher value in this field if your network is busy or congested.
Traffic Redirect	
Active	Select this check box to have the Prestige use traffic redirect if the normal WAN connection goes down. **If you activate traffic redirect, you must configure at least one** Check WAN IP Address**.**
Metric	This field sets this route's priority among the routes the Prestige uses. The metric represents the "cost of transmission". A router determines the best route for transmission by choosing a path with the lowest "cost". RIP routing uses hop count as the measurement of cost, with a minimum of "1" for directly connected networks. The number must be between "1" and "15"; a number greater than "15" means the link is down. The smaller the number, the lower the "cost".
Backup Gateway	Type the IP address of your backup gateway in dotted decimal notation. The Prestige automatically forwards traffic to this IP address if the Prestige's Internet connection terminates.
Dial Backup	
Active	Select this check box to turn on dial backup. **If you activate dial backup, you must configure at least one** Check WAN IP Address**.**

Table 8-11 WAN Backup – Prestige

LABEL	DESCRIPTION
Metric	This field sets this route's priority among the three routes the Prestige uses (normal, traffic redirect and dial backup). Type a number (1 to 15) to set the priority of the dial backup route for data transmission. The smaller the number, the higher the priority. If the three routes have the same metrics, the priority of the routes is as follows: **WAN**, **Traffic Redirect**, **Dial Backup**.
Port Speed	Use the drop-down list box to select the speed of the connection between the dial backup port and the external device. Available speeds are: **9600**, **19200**, **38400**, **57600**, **115200** or **230400** bps.
User Name	Type the login name assigned by your ISP.
Password	Type the password assigned by your ISP.
Pri Phone #	Type the first (primary) phone number from the ISP for this remote node. Some areas require dialing the pound sign # before the phone number for local calls. Include a # symbol at the beginning of the phone numbers as required.
Advanced Backup	Click this button to display the **Advanced Backup** screen and edit more details of your WAN backup setup.
Apply	Click **Apply** to save the changes.
Reset	Click **Reset** to begin configuring this screen afresh.

8.2.3 Configuring Advanced WAN Backup – Prestige

To edit your Prestige's advanced WAN backup settings, click **WAN**, **WAN Backup** and then the **Advanced Backup** button. The screen appears as shown.

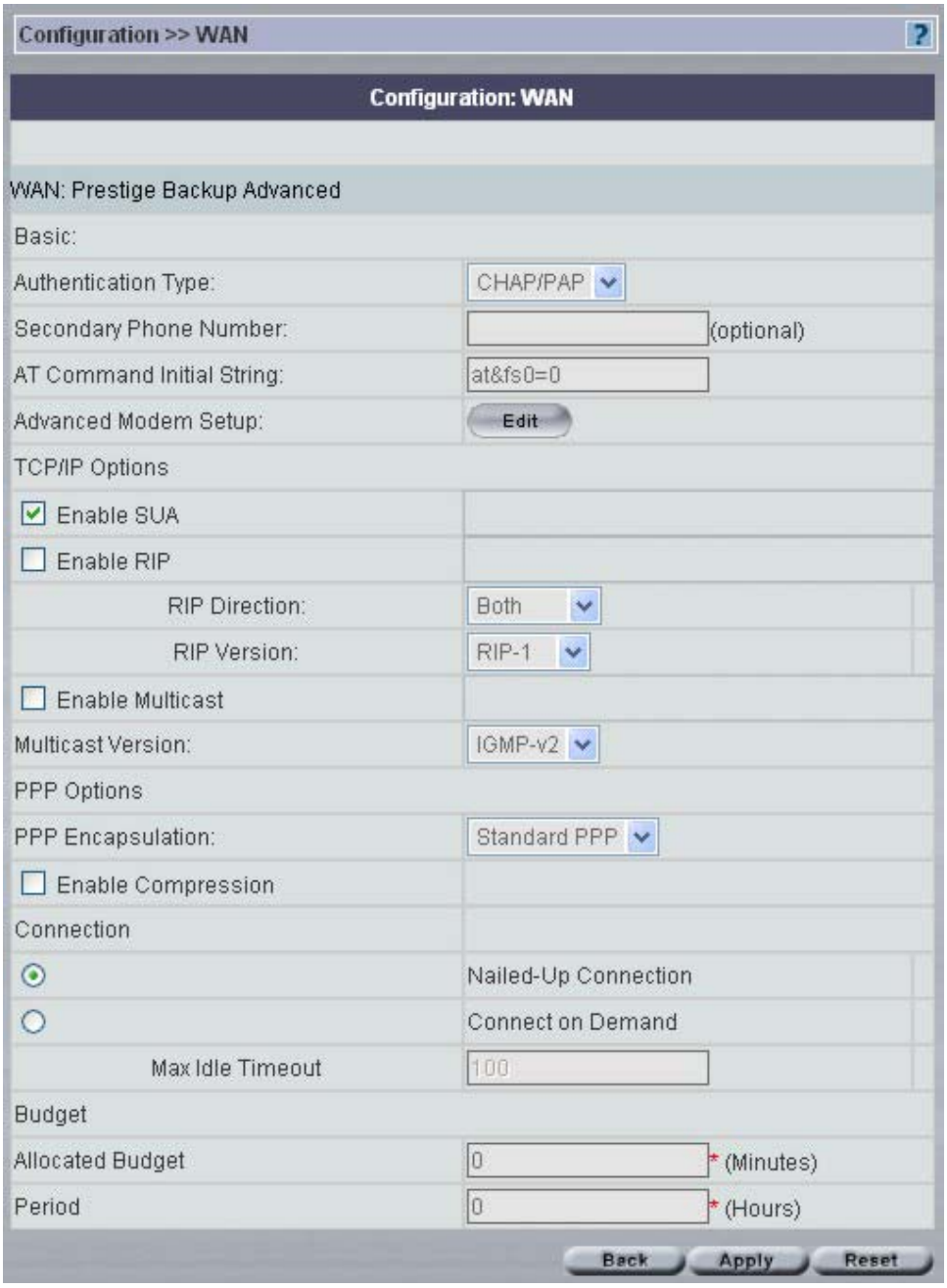


Figure 8-17 Advanced WAN Backup – Prestige

The following table describes the fields in this screen.

Table 8-12 Advanced WAN Backup – Prestige

LABEL	DESCRIPTION
Basic	
Authentication Type	Use the drop-down list box to select an authentication protocol for outgoing calls. Options are: **CHAP/PAP** - Your Prestige accepts either CHAP or PAP when requested by this remote node. **CHAP** - Your Prestige accepts CHAP only. **PAP** - Your Prestige accept PAP only.
Primary/ Secondary Phone Number	Type the first (primary) phone number from the ISP for this remote node. If the primary phone number is busy or does not answer, your Prestige dials the secondary phone number if available. Some areas require dialing the pound sign # before the phone number for local calls. Include a # symbol at the beginning of the phone numbers as required.
AT Command Initial String	Type the AT command string to initialize the WAN device. Consult the manual of your WAN device connected to your dial backup port for specific AT commands.
Advanced Modem Setup	Click the **Edit** button to display the **Advanced Modem Setup** screen and edit the details of your dial backup setup.
TCP/IP Options	
Enable SUA	Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network to a different IP address known within another network. SUA (Single User Account) is a subset of NAT that supports two types of mapping: Many-to-One and Server. When you select this option the Prestige will use Address Mapping Set 255 in the SMT (see the section on menu 15.1 for more information).
Enable RIP	Select this check box to turn on RIP (Routing Information Protocol), which allows a router to exchange routing information with other routers.
RIP Direction	RIP (Routing Information Protocol) allows a router to exchange routing information with other routers. The **RIP Direction** field controls the sending and receiving of RIP packets. Choose **Both**, **In Only** or **Out Only**. When set to **Both** or **Out Only**, the Prestige will broadcast its routing table periodically. When set to **Both** or **In Only**, the Prestige will incorporate RIP information that it receives.
RIP Version	The **RIP Version** field controls the format and the broadcasting method of the RIP packets that the Prestige sends (it recognizes both formats when receiving). Choose **RIP-1**, **RIP-2B** or **RIP-2M**. **RIP-1** is universally supported; but **RIP-2** carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology. Both **RIP-2B** and **RIP-2M** sends the routing data in RIP-2 format; the difference being that RIP-2B uses subnet broadcasting while RIP-2M uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also.

Table 8-12 Advanced WAN Backup – Prestige

LABEL	DESCRIPTION
Enable Multicast	Select this check box to turn on IGMP (Internet Group Multicast Protocol). IGMP is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data.
Multicast Version	Select **IGMP-v1** or **IGMP-v2**. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see *sections 4* and *5* of *RFC 2236*.
PPP Options	
PPP Encapsulation	Select **CISCO PPP** from the drop-down list box if your backup WAN device uses **Cisco PPP** encapsulation; otherwise select **Standard PPP**.
Enable Compression	Select this check box to enable stac compression.
Connection	
Nailed-Up Connection	Select **Nailed-Up Connection** when you want your connection up all the time. The Prestige will try to bring up the connection automatically if it is disconnected.
Connect on Demand	Select **Connect on Demand** when you don't want the connection up all the time and specify an idle time-out in the **Max Idle Timeout** field.
Max Idle Timeout	Specify an idle time-out in the **Max Idle Timeout** field when you select **Connect on Demand**. The default setting is 0, which means the Internet session will not timeout.
Budget	The configuration in the **Budget** fields has priority over your **Connection** settings.
Allocated Budget	Type the amount of time (in minutes) that the dial backup connection can be used during the time configured in the **Period** field. Set an amount that is less than the time period configured in the **Period** field. If you set the **Allocated Budget** to 0, you will not be able to use the dial backup connection.
Period	Type the time period (in hours) for how often the budget should be reset. For example, to allow calls to this remote node for a maximum of 10 minutes every hour, set the **Allocated Budget** to 10 (minutes) and the **Period** to 1 (hour). If you set the **Period** to 0, there is no budget control and the Prestige uses the **Connection** settings.
Back	Click **Back** to return to the previous screen.
Apply	Click **Apply** to save the changes.
Reset	Click **Reset** to begin configuring this screen afresh.

8.2.4 Advanced Modem Setup – Prestige

Click **Edit** in the **Advanced Modem Setup** field. See the section on ZyWALL advanced modem setup for configuration of this screen.

9 Configuration > NAT

9.1 NAT Overview

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

9.1.1 NAT Definitions

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

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

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

Table 9-1 NAT Definitions

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

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

9.1.2 What NAT Does

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

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

9.1.3 How NAT Works

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

9.1.4 NAT Mapping Types

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

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

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

The following table summarizes these types.

Table 9-2 NAT Mapping Types

TYPE	IP MAPPING	SMT ABBREVIATION
One-to-One	ILA1←→ IGA1	1-1
Many-to-One (SUA/PAT)	ILA1←→ IGA1 ILA2←→ IGA1 …	M-1
Many-to-Many Overload	ILA1←→ IGA1 ILA2←→ IGA2 ILA3←→ IGA1 ILA4←→ IGA2 …	M-M Ov

Table 9-2 NAT Mapping Types

TYPE	IP MAPPING	SMT ABBREVIATION
Many-One-to-One	ILA1←→ IGA1 ILA2←→ IGA2 ILA3←→ IGA3 …	M-1-1
Server	Server 1 IP←→ IGA1 Server 2 IP←→ IGA1 Server 3 IP←→ IGA1	Server

9.1.5 SUA (Single User Account) Versus NAT

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

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

9.2 Configuring NAT

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

Select a device and then click **Configuration > NAT**.

9.2.1 Disable NAT

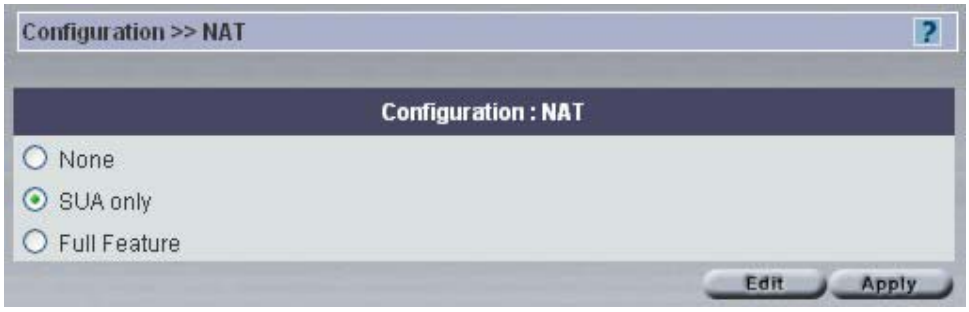


Figure 9-1 Configuration > NAT

The following table describes the fields in this screen.

Table 9-3 Configuration > NAT

LABEL	DESCRIPTION
None	Select **None** to disable NAT on the ZyXEL device

Table 9-3 Configuration > NAT

LABEL	DESCRIPTION
SUA Only	Select **SUA Only** to apply many-to-one mapping only (sufficient if the device has only one public IP address).
Full Feature	Select **Full Feature** to avail of multiple mapping types.
Edit	Click **Edit** to advance to the selected feature.
Apply	Click **Apply** to begin configuring this screen afresh.

9.3 SUA Servers

A SUA server set is a list of inside (behind NAT on the LAN) servers, for example, web or FTP, that you can make visible to the outside world even though SUA makes your whole inside network appear as a single computer to the outside world. The ZyXEL device provides the additional safety of a DMZ port for connecting your publicly accessible servers. This makes the LAN more secure by physically separating it from your public servers.

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

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

Default Server IP Address

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

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

9.3.1 Port Forwarding: Services and Port Numbers

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

The most often used port numbers are shown in the following table. Please refer to RFC 1700 for further information about port numbers. Please also refer to the Supporting CD for more examples and details on SUA/NAT.

Table 9-4 Services and Port Numbers

SERVICES	PORT NUMBER
ECHO	7
FTP (File Transfer Protocol)	21
SMTP (Simple Mail Transfer Protocol)	25

Table 9-4 Services and Port Numbers

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

9.3.2 Configuring SUA Servers – ZyWALL

Select **SUA Only** in *Figure 9-1* and then click **Edit** to bring up the next screen.

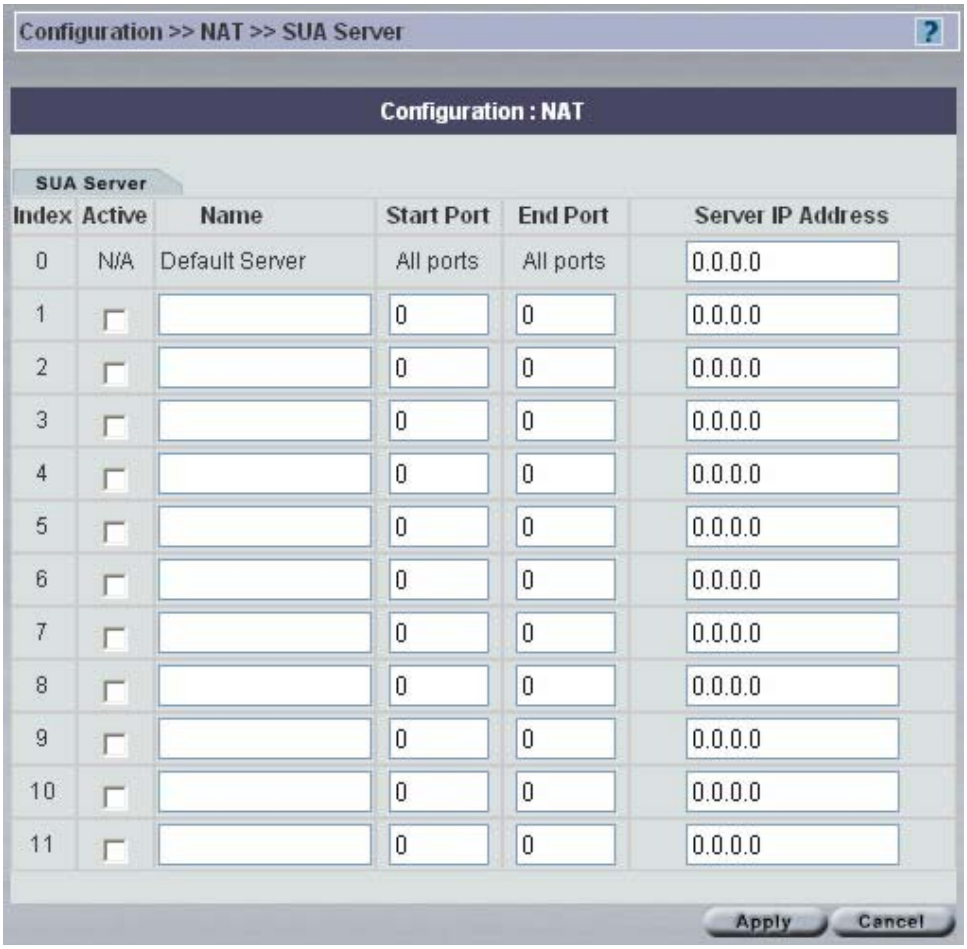


Figure 9-2 Configuration > NAT > SUA Server – ZyWALL

The following table describes the labels in this screen.

Table 9-5 Configuration > NAT > SUA Server

LABEL	DESCRIPTION
Index	This is the number of an individual SUA server entry. You may select a rule to edit or delete it.
Active	Select this check box to enable the SUA server entry. Clear this checkbox to disallow forwarding of these ports to an inside server without having to delete the entry.
Name	Type a name to identify this port-forwarding rule. To delete a SUA server entry, erase the name and click **Apply**.
Default Server	In addition to the servers for specified services, NAT supports a default server. A default server receives packets from ports that are not specified in this screen. If you do not assign a default server IP address, then all packets received for ports not specified in this screen or remote management will be discarded.
Start Port	Type the start and end port numbers that define the service that will be forwarded to the inside server specified in the next field.
End Port	
Server IP Address	Type the IP address of the inside server.
Apply	Click **Apply** to save your changes back to the ZyXEL device.
Cancel	Click **Cancel** to return to the previous screen.

Select a radio button and then click **Edit** to configure that server set.

9.3.3 Configuring SUA Servers – Prestige

Select **SUA Only** in *Figure 9-1* and then click **Edit** to bring up the next screen.

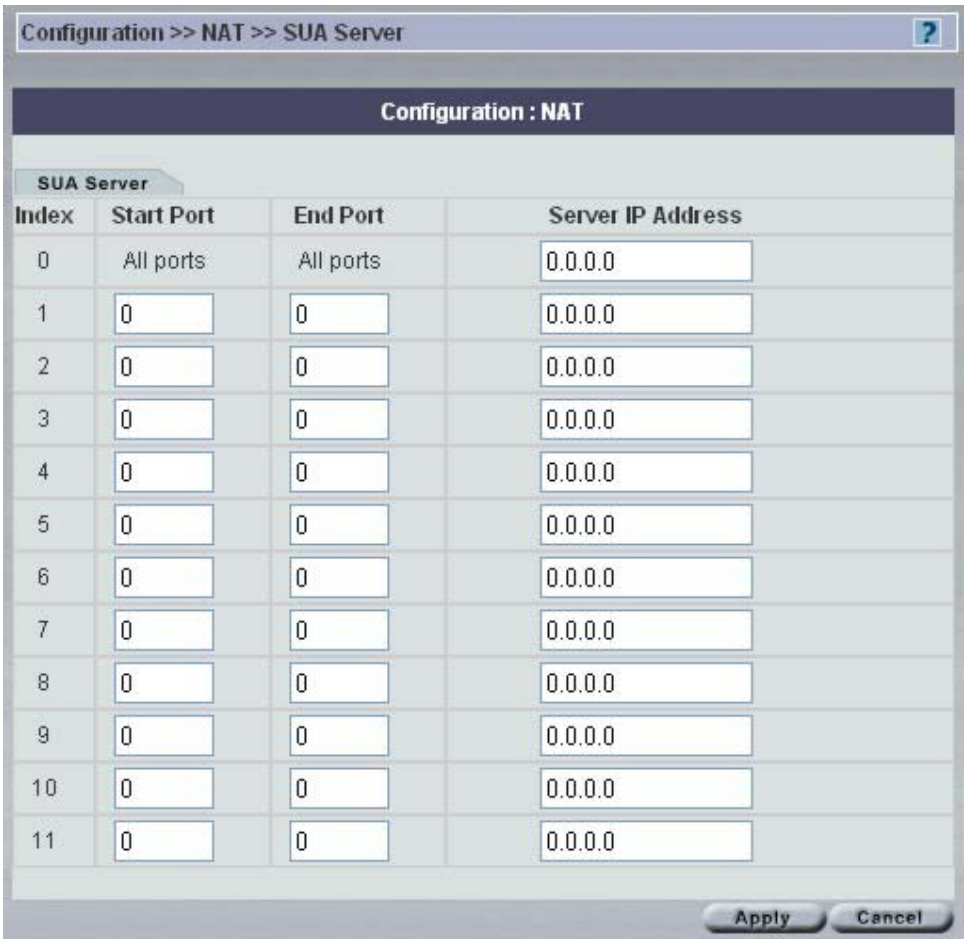


Figure 9-3 Configuration > NAT > SUA Server – Prestige

The following table describes the labels in this screen.

Table 9-6 Configuration > NAT > SUA Server – Prestige

LABEL	DESCRIPTION
Index	This is the number of an individual SUA server entry.
Default Server	In addition to the servers for specified services, NAT supports a default server. A default server receives packets from ports that are not specified in this screen. If you do not assign a default server IP address, then all packets received for ports not specified in this screen or remote management will be discarded.
Start Port	Type the start and end port numbers that define the service that will be forwarded to the inside server specified in the next field.
End Port	
Server IP Address	Type the IP address of the inside server.
Apply	Click **Apply** to save your changes back to the ZyXEL device.
Cancel	Click **Cancel** to return to the previous screen.

Select a radio button and then click **Edit** to configure that server set.

9.3.4 Full Feature Address Mapping

Select **Full Feature** in *Figure 9-1* and then click **Edit** to bring up the next screen.

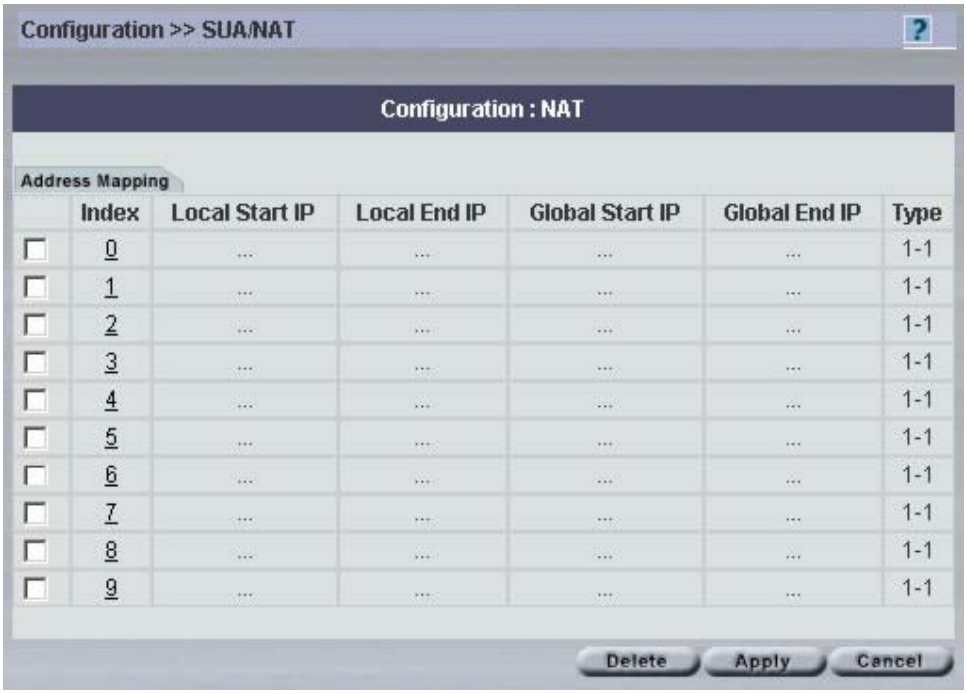


Figure 9-4 Configuration > NAT > Full Feature > Address Mapping

The following table describes the labels in this screen.

Table 9-7 Configuration > NAT > Full Feature > Address Mapping

LABEL	DESCRIPTION
Index	This is the number of an individual entry. You may select a rule to edit by going to the **Edit Address Mapping** screen for that rule.
Local Start IP	This refers to the Inside Local Address (ILA), which is the starting local IP address. Local IP addresses are **N/A** for **Server** port mapping.
Local End IP	This is the end Inside Local Address (ILA). If the rule is for all local IP addresses, then this field displays 0.0.0.0 and 255.255.255.255 as the **Local End IP** address. This field is **N/A** for **One-to-One** and **Server** mapping types.
Global Start IP	This refers to the Inside Global IP Address (IGA). 0.0.0.0 is for a dynamic IP address from your ISP with **Many-to-One** and **Server** mapping types.
Global End IP	This is the ending Inside Global Address (IGA), which is the starting global IP address. This field is **N/A** for **One-to-One**, **Many-to-One** and **Server** mapping types.

Table 9-7 Configuration > NAT > Full Feature > Address Mapping

LABEL	DESCRIPTION
Type	1. **One-to-One** mode maps one local IP address to one global IP address. Note that port numbers do not change for the One-to-one NAT mapping type. 2. **Many-to-One** mode maps multiple local IP addresses to one global IP address. This is equivalent to SUA (i.e., PAT, port address translation), ZyXEL's Single User Account feature that previous ZyXEL routers supported only. 3. **Many-to-Many Overload** mode maps multiple local IP addresses to shared global IP addresses. 4. **Many One-to-One** mode maps each local IP address to unique global IP addresses. 5. **Server** allows you to specify inside servers of different services behind the NAT to be accessible to the outside world.
Delete	Select the radio button next to a rule and click **Delete** to delete the address-mapping rule.
Apply	Click **Apply** to save your changes back to the ZyXEL device.
Cancel	Click **Cancel** to close this screen without applying any changes.

9.3.5 Edit Full Feature Address Mapping

Select a radio button from the **Address Mapping** screen and then click **Edit.** Select the mapping type and local, remote IP address ranges here.

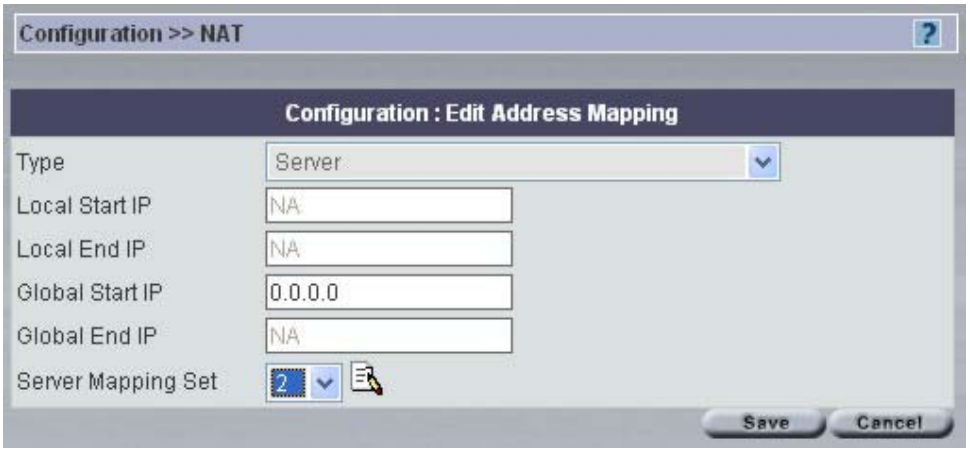


Figure 9-5 Configuration > NAT > Full Feature > Edit Address Mapping

Table 9-8 Configuration > NAT > Full Feature > Edit Address Mapping

LABEL	DESCRIPTION
Type	When you select **Type** you can choose a server mapping set. Choose the port mapping type from one of the following. 1. **One-to-One**: One-to-one mode maps one local IP address to one global IP address. Note that port numbers do not change for One-to-one NAT mapping type. 2. **Many-to-One**: Many-to-One mode maps multiple local IP addresses to one global IP address. This is equivalent to SUA (i.e., PAT, port address translation), ZyXEL's Single User Account feature. 3. **Many-to-Many Ov** (Overload): Many-to-Many Overload mode maps multiple local IP addresses to shared global IP addresses. 4. **Many One-to-One**: Many One-to-one mode maps each local IP address to unique global IP addresses. 5. **Server**: This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world.
Local Start IP	This is the starting Inside Local IP Address (ILA). Local IP addresses are **N/A** for **Server** port mapping.
Local End IP	This is the end Inside Local IP Address (ILA). If your rule is for all local IP addresses, then enter 0.0.0.0 as the **Local Start IP** address and 255.255.255.255 as the **Local End IP** address. This field is **N/A** for **One-to-One** and **Server** mapping types.
Global Start IP	This is the starting Inside Global IP Address (IGA). Enter 0.0.0.0 here if you have a dynamic IP address from your ISP.
Global End IP	This is the ending Inside Global IP Address (IGA). This field is **N/A** for **One-to-One**, **Many-to-One** and **Server** mapping types.
Server Mapping Set	This field is only available in the Prestige and when **Type** is set to **Server**. Select a number from the drop-down menu to choose a server set from the **NAT > Address Mapping** screen. Click the link to go to the **NAT > SUA Server** screen to edit a server set that you have selected in the **Server Mapping Set** field.
Save	Click **Save** to save your changes back to the ZyXEL device.
Cancel	Click **Cancel** to return to the previous screen.

9.4 Trigger Port Forwarding – ZyWALL

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

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

Trigger events only happen on outgoing data (from the ZyXEL device).

Only one LAN computer can use a trigger port (range) at a time. Therefore, if an application needs a continuous data stream, that port (range) will be tied up so that another computer on the LAN can't trigger it until that stream finishes.

9.4.1 Configuring Trigger Port

Select **Full Feature** in *Figure 9-1,* click **Edit** and then click the **Trigger Port** tab to bring up the next screen.

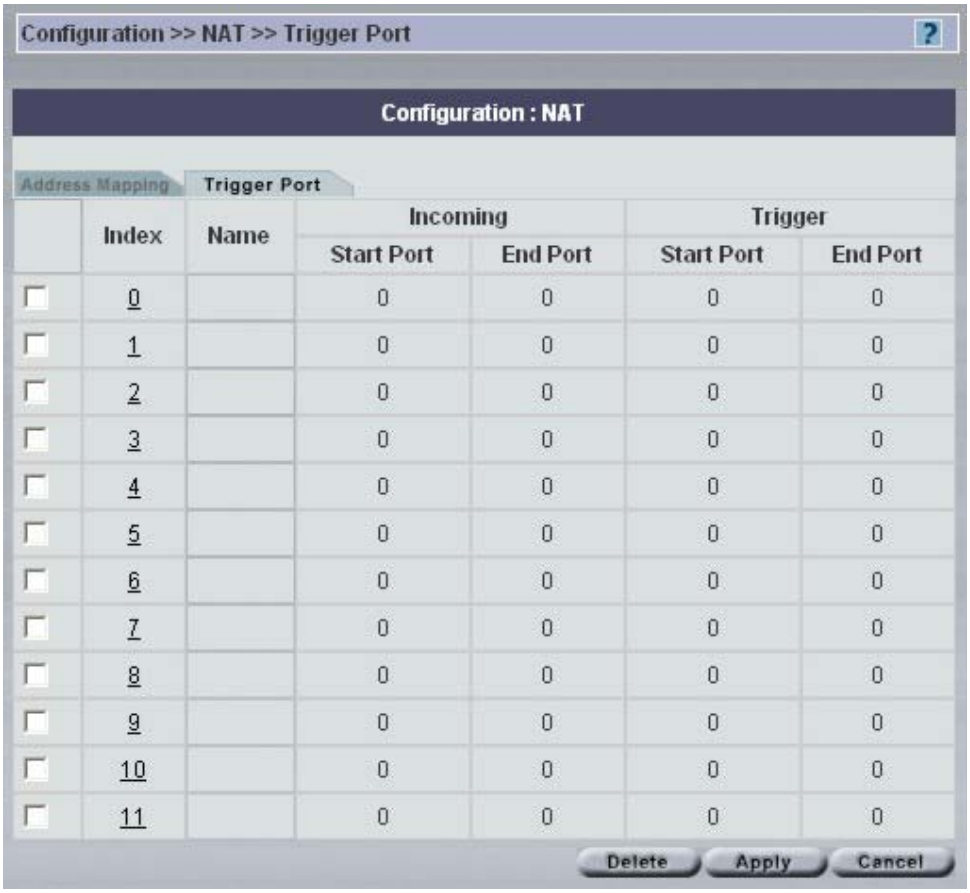


Figure 9-6 Configuration > NAT > Full Feature > Trigger Port

The following table describes the labels in this screen.

Table 9-9 Configuration > NAT > Full Feature > Trigger Port

LABEL	DESCRIPTION
Index	This is the number of an individual entry. You may select a rule to edit.
Name	This field displays a unique name (up to 15 characters) for identification purposes.
Incoming	Incoming is a port (or a range of ports) that a server on the WAN uses when it sends out a particular service. The ZyXEL device forwards the traffic with this port (or range of ports) to the client computer on the LAN that requested the service.
Start Port	This field displays a port number or the starting port number in a range of port numbers.
End Port	This field displays a port number or the ending port number in a range of port numbers.

Table 9-9 Configuration > NAT > Full Feature > Trigger Port

LABEL	DESCRIPTION
Trigger	The trigger port is a port (or a range of ports) that causes (or triggers) the ZyXEL device to record the IP address of the LAN computer that sent the traffic to a server on the WAN.
Start Port	This field displays a port number or the starting port number in a range of port numbers.
End Port	This field displays a port number or the ending port number in a range of port numbers.
Delete	Select a rule and then click **Delete** to erase it.
Apply	Click **Apply** to save your changes back to the ZyXEL device.
Cancel	Click **Cancel** to begin configuring this screen afresh.

9.4.2 Edit Trigger Port

Select an index number from the **Trigger Port** screen and then click **Edit**.

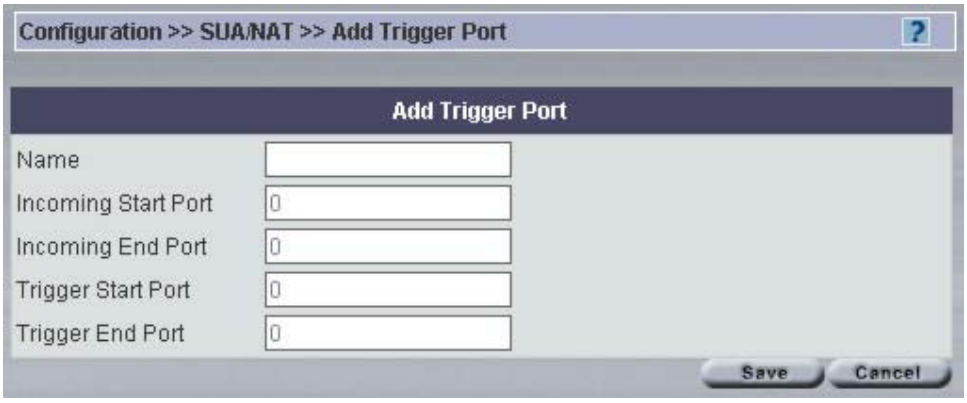


Figure 9-7 Configuration > NAT > Full Feature > Trigger Port > Edit

The following table describes the labels in this screen.

Table 9-10 Configuration > NAT > Full Feature > Trigger Port > Edit

LABEL	DESCRIPTION
Name	Type a unique name (up to 15 characters) for identification purposes. All characters are permitted - including spaces.
Incoming	Incoming is a port (or a range of ports) that a server on the WAN uses when it sends out a particular service. The ZyXEL device forwards the traffic with this port (or range of ports) to the client computer on the LAN that requested the service.
Start Port	Type a port number or the starting port number in a range of port numbers.
End Port	Type a port number or the ending port number in a range of port numbers.
Trigger	The trigger port is a port (or a range of ports) that causes (or triggers) the ZyXEL device to record the IP address of the LAN computer that sent the traffic to a server on the WAN.
Start Port	Type a port number or the starting port number in a range of port numbers.
End Port	Type a port number or the ending port number in a range of port numbers.
Save	Click **Save** to save your changes back to the ZyXEL device.
Cancel	Click **Cancel** to return to the previous screen.

10 Configuration > Static Route

This chapter shows you how to configure static route.

10.1 Static Route Overview

Each remote node specifies only the network to which the gateway is directly connected, and the ZyXEL device has no knowledge of the networks beyond

10.1.1 Static Route Summary

Select a device and then click **Configuration > Static Route**.

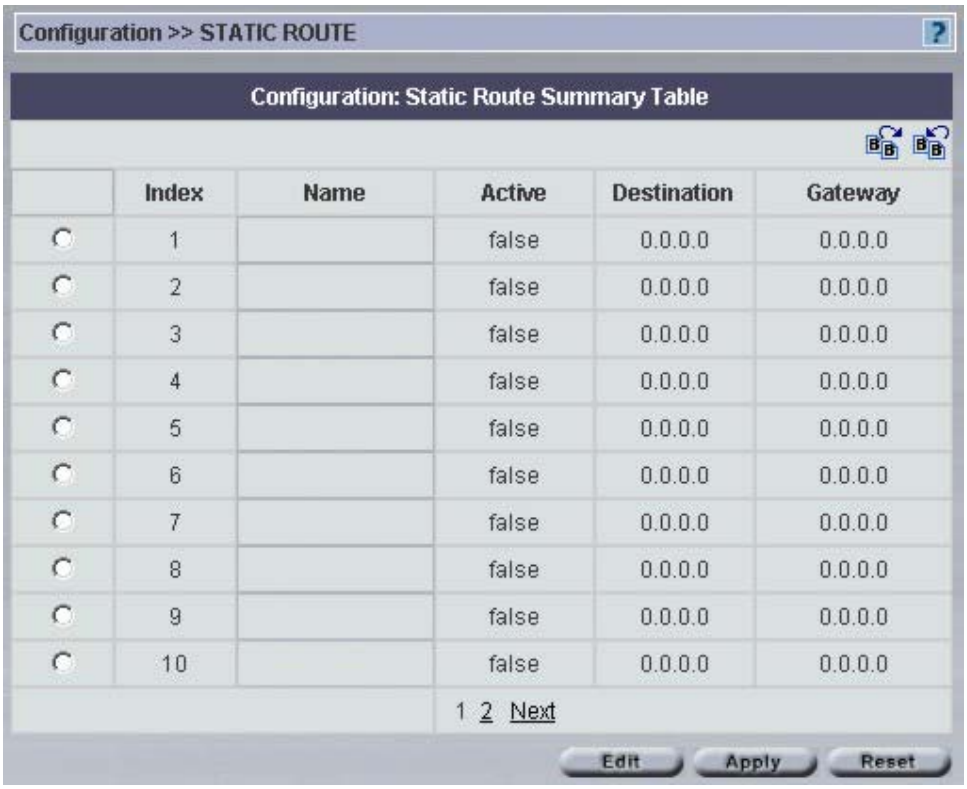


Figure 10-1 Configuration > Static Route

Table 10-1 Configuration > Static Route

LABEL	DESCRIPTION
Index	This is the number of an individual entry. You may select a rule to edit or delete it.
Name	This is the name that describes or identifies this route. To delete a static route, erase the name and then click apply.
Active	This field shows whether this static route is active or not.
Destination	This parameter specifies the IP network address of the final destination. Routing is always based on network number.

Table 10-1 Configuration > Static Route

LABEL	DESCRIPTION
Gateway	This is the IP address of the gateway. The gateway is an immediate neighbor of the ZyXEL device that will forward the packet to the destination. On the LAN, the gateway must be a router on the same segment as the ZyXEL device; over the WAN, the gateway must be the IP address of one of the remote nodes.
Next	Select a page number or **Next** to view a particular page or next page of server entries respectively.
Edit	Click a static route index number and then click **Edit** to set up a static route on the ZyXEL device.
Apply	Click **Apply** to save your changes back to the ZyXEL device.
Reset	Click **Reset** to begin configuring this screen afresh.

10.1.2 Edit Static Route

Figure 10-2 Configuration > Static Route > Edit

Table 10-2 Configuration > Static Route > Edit

LABEL	DESCRIPTION
Route Name	Enter the name of the IP static route. Leave this field blank to delete this static route.
Active	This checkbox allows you to activate/deactivate this static route.
Destination IP Address	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
IP Subnet Mask	Enter the IP subnet mask here.
Gateway IP Address	Enter the IP address of the gateway. The gateway is an immediate neighbor of the ZyXEL device that will forward the packet to the destination. On the LAN, the gateway must be a router on the same segment as the ZyXEL device; over the WAN, the gateway must be the IP address of one of the Remote Nodes.

Table 10-2 Configuration > Static Route > Edit

LABEL	DESCRIPTION
Metric	Metric represents the “cost” of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Enter a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.
Private	This parameter determines if the ZyXEL device will include this route to a remote node in its RIP broadcasts. Select this check box to keep this route private and not included in RIP broadcasts. Clear this checkbox to propagate this route to other hosts through RIP broadcasts.
Save	Click **Save** to save your changes back to the ZyXEL device.
Cancel	Click **Cancel** to return to the previous screen.

11 Configuration > VPN

This chapter shows you how to configure VPNs using Vantage.

11.1 VPN Overview

A VPN (Virtual Private Network) provides secure communications between sites without the expense of leased site-to-site lines. A secure VPN is a combination of tunneling, encryption, authentication, access control and auditing technologies/services used to transport traffic over the Internet or any insecure network that uses the TCP/IP protocol suite for communication.

11.1.1 IPSec

Internet Protocol Security (IPSec) is a standards-based VPN that offers flexible solutions for secure data communications across a public network like the Internet. IPSec is built around a number of standardized cryptographic techniques to provide confidentiality, data integrity and authentication at the IP layer.

11.1.2 Security Association

A Security Association (SA) is a contract between two parties indicating what security parameters, such as keys and algorithms they will use.

11.1.3 Encryption

Encryption is a mathematical operation that transforms data from "plaintext" (readable) to "ciphertext" (scrambled text) using a "key". The key and clear text are processed by the encryption operation, which leads to the data scrambling that makes encryption secure. Decryption is the opposite of encryption: it is a mathematical operation that transforms “ciphertext” to plaintext. Decryption also requires a key.

11.1.4 Data Confidentiality

The IPSec sender can encrypt packets before transmitting them across a network.

11.1.5 Data Integrity

The IPSec receiver can validate packets sent by the IPSec sender to ensure that the data has not been altered during transmission.

11.1.6 Data Origin Authentication

The IPSec receiver can verify the source of IPSec packets. This service depends on the data integrity service.

11.1.7 IPSec Algorithms

The **ESP** and **AH** protocols are necessary to create a Security Association (SA), the foundation of an IPSec VPN. An SA is built from the authentication provided by the **AH** and **ESP** protocols. The primary function of key management is to establish and maintain the SA between systems. Once the SA is established, the transport of data may commence.

AH (Authentication Header) Protocol

AH protocol (RFC 2402) was designed for integrity, authentication, sequence integrity (replay resistance), and non-repudiation but not for confidentiality, for which the **ESP** was designed.

In applications where confidentiality is not required or not sanctioned by government encryption restrictions, an **AH** can be employed to ensure integrity. This type of implementation does not protect the information from dissemination but will allow for verification of the integrity of the information and authentication of the originator.

ESP (Encapsulating Security Payload) Protocol

The **ESP** protocol (RFC 2406) provides encryption as well as some of the services offered by **AH**. **ESP** authenticating properties are limited compared to the **AH** due to the non-inclusion of the IP header information during the authentication process. However, **ESP** is sufficient if only the upper layer protocols need to be authenticated.

An added feature of the **ESP** is payload padding, which further protects communications by concealing the size of the packet being transmitted.

Table 11-1 AH and ESP

ESP	AH
DES (default) Data Encryption Standard (DES) is a widely used method of data encryption using a secret key. DES applies a 56-bit key to each 64-bit block of data.	**MD5** (default) MD5 (Message Digest 5) produces a 128-bit digest to authenticate packet data.
3DES Triple DES (3DES) is a variant of DES, which iterates three times with three separate keys (3 x 56 = 168 bits), effectively doubling the strength of DES.	**SHA1** SHA1 (Secure Hash Algorithm) produces a 160-bit digest to authenticate packet data.
AES Advanced Encryption Standard is a newer method of data encryption that also uses a secret key. This implementation of AES applies a 128-bit key to 128-bit blocks of data. AES is faster than 3DES.	
Select **DES** for minimal security and **3DES** or **AES** for maximum. Select **NULL** to set up a tunnel without encryption.	Select **MD5** for minimal security and **SHA-1** for maximum security.

11.1.8 Key Management

Key management allows you to determine whether to use IKE (ISAKMP) or manual key configuration in order to set up a VPN.

11.1.9 Encapsulation

The two modes of operation for IPSec VPNs are **Transport** mode and **Tunnel** mode.

Transport Mode

Transport mode is used to protect upper layer protocols and only affects the data in the IP packet. In **Transport** mode, the IP packet contains the security protocol (**AH** or **ESP**) located after the original IP header and options, but before any upper layer protocols contained in the packet (such as TCP and UDP).

With **ESP,** protection is applied only to the upper layer protocols contained in the packet. The IP header information and options are not used in the authentication process. Therefore, the originating IP address cannot be verified for integrity against the data.

With the use of **AH** as the security protocol, protection is extended forward into the IP header to verify the integrity of the entire packet by use of portions of the original IP header in the hashing process.

Tunnel Mode

Tunnel mode encapsulates the entire IP packet to transmit it securely. A **Tunnel** mode is required for gateway services to provide access to internal systems. **Tunnel** mode is fundamentally an IP tunnel with authentication and encryption. This is the most common mode of operation. **Tunnel** mode is required for gateway to gateway and host to gateway communications. **Tunnel** mode communications have two sets of IP headers:

- **Outside header**: The outside IP header contains the destination IP address of the VPN gateway.
- **Inside header**: The inside IP header contains the destination IP address of the final system behind the VPN gateway. The security protocol appears after the outer IP header and before the inside IP header.

11.1.10 IPSec and NAT

This section applies to computers running IPSec behind the ZyXEL device.

NAT is incompatible with the **AH** protocol in both **Transport** and **Tunnel** mode. An IPSec VPN using the **AH** protocol digitally signs the outbound packet, both data payload and headers, with a hash value appended to the packet. When using **AH** protocol, packet contents (the data payload) are not encrypted.

A NAT device in between the IPSec endpoints will rewrite either the source or destination address with one of its own choosing. The VPN device at the receiving end will verify the integrity of the incoming packet by computing its own hash value, and complain that the hash value appended to the received packet doesn't match. The VPN device at the receiving end doesn't know about the NAT in the middle, so it assumes that the data has been maliciously altered.

IPSec using **ESP** in **Tunnel** mode encapsulates the entire original packet (including headers) in a new IP packet. The new IP packet's source address is the outbound address of the sending VPN gateway, and its destination address is the inbound address of the VPN device at the receiving end. When using **ESP** protocol with authentication, the packet contents (in this case, the entire original packet) are encrypted. The encrypted contents, but not the new headers, are signed with a hash value appended to the packet.

Tunnel mode **ESP** with authentication is compatible with NAT because integrity checks are performed over the combination of the "original header plus original payload," which is unchanged by a NAT device. **Transport** mode **ESP** with authentication is not compatible with NAT, although NAT traversal provides a way to use **Transport** mode **ESP** when there is a NAT router between the IPSec endpoints.

Table 11-2 VPN and NAT

SECURITY PROTOCOL	MODE	NAT
AH	Transport	N
AH	Tunnel	N
ESP	Transport	N
ESP	Tunnel	Y

11.1.11 Keep Alive

When you initiate an IPSec tunnel with keep alive enabled, the ZyXEL device automatically renegotiates the tunnel when the IPSec SA lifetime period expires. In effect, the IPSec tunnel becomes an “always on” connection after you initiate it. Both IPSec routers must have a ZyXEL device-compatible keep alive feature enabled in order for this feature to work.

If the ZyXEL device has its maximum number of simultaneous IPSec tunnels connected to it and they all have keep alive enabled, then no other tunnels can take a turn connecting to the ZyXEL device because the ZyXEL device never drops the tunnels that are already connected. Check *Table 1-1 Model Specific Features* in chapter 1 to see how many simultaneous IPSec SAs the ZyXEL device model can support.

When there is outbound traffic with no inbound traffic, the ZyXEL device automatically drops the tunnel after two minutes.

11.1.12 NAT Traversal

NAT traversal allows you to set up a VPN connection when there are NAT routers between end IPSec VPN tunnel devices.

Normally you cannot set up a VPN connection with a NAT router between the two IPSec routers because the NAT router changes the header of the IPSec packet. In the previous figure, IPSec router A sends an IPSec packet in an attempt to initiate a VPN. The NAT router changes the IPSec packet's header so it does not match the header for which IPSec router B is checking. Therefore, IPSec router B does not respond and the VPN connection cannot be built.

NAT traversal solves the problem by adding a UDP port 500 header to the IPSec packet. The NAT router forwards the IPSec packet with the UDP port 500 header unchanged. IPSec router B checks the UDP port 500 header and responds. IPSec routers A and B build a VPN connection.

NAT Traversal Configuration

For NAT traversal to work you must:

- Use ESP security protocol (in either transport or tunnel mode).
- Use IKE keying mode.
- Enable NAT traversal on both IPSec endpoints.

11.1.13 ID Type and Content

With aggressive negotiation mode, the ZyXEL device identifies incoming SAs by ID type and content since this identifying information is not encrypted. This enables the ZyXEL device to distinguish between multiple rules for SAs that connect from remote IPSec routers that have dynamic WAN IP addresses. Telecommuters can use separate passwords to simultaneously connect to the ZyXEL device from IPSec routers with dynamic IP addresses.

Regardless of the ID type and content configuration, the ZyXEL device does not allow you to save multiple active rules with overlapping local and remote IP addresses.

With main mode, the ID type and content are encrypted to provide identity protection. In this case the ZyXEL device can only distinguish between up to 12 different incoming SAs that connect from remote IPSec routers that have dynamic WAN IP addresses. The ZyXEL device can distinguish up to 12 incoming SAs because you can select between three encryption algorithms (DES, 3DES and AES), two authentication algorithms (MD5 and SHA1) and two key groups (DH1 and DH2) when you configure a VPN rule. The ID type and content act as an extra level of identification for incoming SAs.

The type of ID can be a domain name, an IP address or an e-mail address. The content is the IP address, domain name, or e-mail address.

Table 11-3 Local ID Type and Content Fields

LOCAL ID TYPE	CONTENT
IP	Type the IP address of your computer or leave the field blank to have the ZyXEL device automatically use its own IP address.
DNS	Type a domain name (up to 31 characters) by which to identify this ZyXEL device.

Table 11-3 Local ID Type and Content Fields

LOCAL ID TYPE	CONTENT
E-mail	Type an e-mail address (up to 31 characters) by which to identify this ZyXEL device.
The domain name or e-mail address that you use in the **Content** field is used for identification purposes only and does not need to be a real domain name or e-mail address.	

Table 11-4 Peer ID Type and Content Fields

PEER ID TYPE	CONTENT
IP	Type the IP address of the computer with which you will make the VPN connection or leave the field blank to have the ZyXEL device automatically use the address in the **Secure Gateway** field.
DNS	Type a domain name (up to 31 characters) by which to identify the remote IPSec router.
E-mail	Type an e-mail address (up to 31 characters) by which to identify the remote IPSec router.
The domain name or e-mail address that you use in the **Content** field is used for identification purposes only and does not need to be a real domain name or e-mail address. The domain name also does not have to match the remote router's IP address or what you configure in the **Secure Gateway Addr** field below.	

11.1.14 IKE Phases

There are two phases to every IKE (Internet Key Exchange) negotiation – phase 1 (Authentication) and phase 2 (Key Exchange). A phase 1 exchange establishes an IKE SA and the second one uses that SA to negotiate SAs for IPSec.

In phase 1 you must:

- Choose a negotiation mode.
- Authenticate the connection by entering a pre-shared key.
- Choose an encryption algorithm.
- Choose an authentication algorithm.
- Choose a Diffie-Hellman public-key cryptography key group (**DH1** or **DH2**).
- Set the IKE SA lifetime. This field allows you to determine how long an IKE SA should stay up before it times out. An IKE SA times out when the IKE SA lifetime period expires. If an IKE SA times out when an IPSec SA is already established, the IPSec SA stays connected.

In phase 2 you must:

- Choose which protocol to use (**ESP** or **AH**) for the IKE key exchange.
- Choose an encryption algorithm.
- Choose an authentication algorithm
- Choose whether to enable Perfect Forward Secrecy (PFS) using Diffie-Hellman public-key cryptography. Select **None** (the default) to disable PFS.
- Choose **Tunnel** mode or **Transport** mode.
- Set the IPSec SA lifetime. This field allows you to determine how long the IPSec SA should stay up before it times out. The ZyXEL device automatically renegotiates the IPSec SA if there is traffic

when the IPSec SA lifetime period expires. The ZyXEL device also automatically renegotiates the IPSec SA if both IPSec routers have keep alive enabled, even if there is no traffic. If an IPSec SA times out, then the IPSec router must renegotiate the SA the next time someone attempts to send traffic.

11.1.15 Negotiation Mode

The phase 1 **Negotiation Mode** you select determines how the Security Association (SA) will be established for each connection through IKE negotiations.

- **Main Mode** ensures the highest level of security when the communicating parties are negotiating authentication (phase 1). It uses 6 messages in three round trips: SA negotiation, Diffie-Hellman exchange and an exchange of nonces (a nonce is a random number). This mode features identity protection (your identity is not revealed in the negotiation).
- **Aggressive Mode** is quicker than **Main Mode** because it eliminates several steps when the communicating parties are negotiating authentication (phase 1). However the trade-off is that faster speed limits its negotiating power and it also does not provide identity protection. It is useful in remote access situations where the address of the initiator is not know by the responder and both parties want to use pre-shared key authentication.

11.1.16 Diffie-Hellman (DH) Key Groups

Diffie-Hellman (DH) is a public-key cryptography protocol that allows two parties to establish a shared secret over an unsecured communications channel. Diffie-Hellman is used within IKE SA setup to establish session keys. 768-bit (Group 1 - **DH1**) and 1024-bit (Group 2 – **DH2**) Diffie-Hellman groups are supported. Upon completion of the Diffie-Hellman exchange, the two peers have a shared secret, but the IKE SA is not authenticated. For authentication, use pre-shared keys.

11.1.17 Perfect Forward Secrecy (PFS)

Enabling PFS means that the key is transient. The key is thrown away and replaced by a brand new key using a new Diffie-Hellman exchange for each new IPSec SA setup. With PFS enabled, if one key is compromised, previous and subsequent keys are not compromised, because subsequent keys are not derived from previous keys. The (time-consuming) Diffie-Hellman exchange is the trade-off for this extra security.

This may be unnecessary for data that does not require such security, so PFS is disabled (**None**) by default in the ZyXEL device. Disabling PFS means new authentication and encryption keys are derived from the same root secret (which may have security implications in the long run) but allows faster SA setup (by bypassing the Diffie-Hellman key exchange).

11.1.18 Pre-Shared Key

A pre-shared key identifies a communicating party during a phase 1 IKE negotiation. It is called “pre-shared” because you have to share it with another party before you can communicate with them over a secure connection.

11.2 VPN Tunnel Summary

Select a device and then click **Configuration > VPN**.

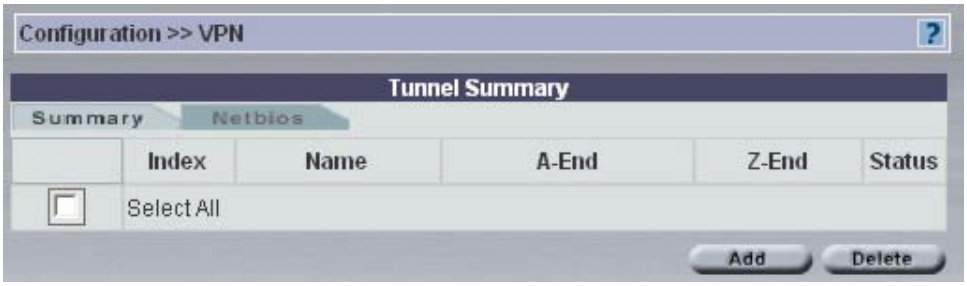


Figure 11-1 Configuration > VPN

The following table describes the labels in this screen.

Table 11-5 Configuration > VPN

LABEL	DESCRIPTION
Index	This is the VPN policy index number
Name	This field displays the identification name for this VPN policy.
A-End/Z-End	For the Vantage manager there is no “local” or “remote”. A-End and Z-End are the end devices where the VPN tunnel terminates. These fields display the device administrators at both ends of a VPN tunnel respectively. If one end of the tunnel cannot be managed (the device exists in another administrators domain and cannot be seen), “Unknown-ZyXEL-Device” is displayed in this field. If you configure a Single-Side-VPN tunnel then a “Non-ZyXEL-Device” is supported at the Z-End.
Status	This field displays whether the VPN tunnel is active or not.
Add	Click **Add** to create a new VPN tunnel or to modify an existing one.
Delete	Select a rule and then click **Delete** to erase it. All rules can be deleted if you check the **Select All** checkbox and click **Delete**.

11.2.1 Add a VPN Tunnel

You can create a “single-ended” VPN tunnel using Vantage by selecting **N/A** from the **Remote Device** field. This allows you to create a VPN tunnel between a ZyXEL device and another IPSec router. You must make sure the remote IPSec router VPN settings correspond to the ZyXEL device VPN settings.

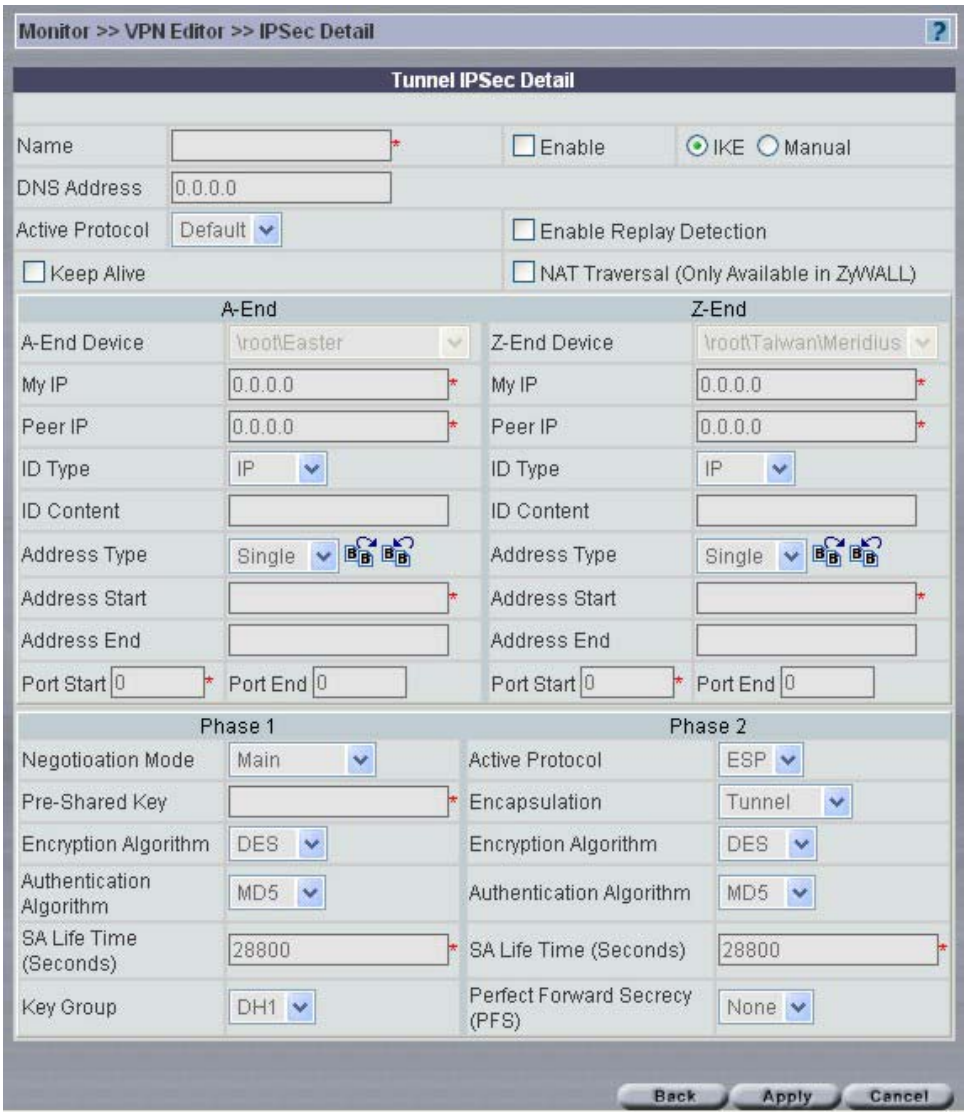


Figure 11-2 Configuration > VPN > Tunnel IPSec Detail

The following table describes the labels in this screen.

Table 11-6 Configuration > VPN > Tunnel IPSec Detail

FIELD	DESCRIPTION
Name	This is a VPN name for identification purposes.
Enable	Select this checkbox to make the VPN rule active.
IKE/Manual	Select either **IKE** or **Manual** to manage encryption keys. If you select the **IKE** method, you must configure the IKE fields. **Manual** is useful for troubleshooting if you have problems using **IKE** key management.
DNS Address	Type a domain name (up to 31 characters) by which to identify the local or remote IPSec router.

Table 11-6 Configuration > VPN > Tunnel IPSec Detail

FIELD	DESCRIPTION
Active Protocol	The **ESP** and **AH** protocols are necessary to create a Security Association (SA), the foundation of an IPSec VPN. **AH** protocol (RFC 2402) was designed for integrity, authentication, sequence integrity (replay resistance), and non-repudiation but not for confidentiality, for which the **ESP** was designed. The **ESP** protocol (RFC 2406) provides encryption as well as some of the services offered by **AH**. **ESP** authenticating properties are limited compared to the **AH** due to the non-inclusion of the IP header information during the authentication process.
Enable Replay Detection	
Keep Alive	When you initiate an IPSec tunnel with keep alive enabled, the ZyXEL device automatically renegotiates the tunnel when the IPSec SA lifetime period expires. In effect, the IPSec tunnel becomes an “always on” connection after you initiate it. Both IPSec routers must have a ZyXEL device-compatible keep alive feature enabled in order for this feature to work. If the ZyXEL device has its maximum number of simultaneous IPSec tunnels connected to it and they all have keep alive enabled, then no other tunnels can take a turn connecting to the ZyXEL device because the ZyXEL
A-End/Z-End	
NAT Traversal (Only Available in ZyWALL)	Select this check box to enable NAT traversal. NAT traversal allows you to set up a VPN connection when there are NAT routers between the two IPSec routers. The remote IPSec router must also have NAT traversal enabled. You can use NAT traversal with ESP protocol using Transport or Tunnel mode, but not with AH protocol nor with manual key management. In order for an IPSec router behind a NAT router to receive an initiating IPSec packet, set the NAT router to forward UDP port 500 to the IPSec router behind the NAT router.
A-End/Z-End Device	Select the name of the ZyXEL device from the pull-down list.
My IP	This is the IP address of the local and remote computer(s) of the VPN tunnel.
Peer IP	Type the IP address of the computer with which you will make the VPN connection or leave the field blank to have the ZyXEL device automatically use the address in the **Secure Gateway** field.
ID Type	Select **IP** to identify this ZyXEL device by its IP address. Select **DNS** to identify this ZyXEL device by a domain name. Select **E-mail** to identify this ZyXEL device by an e-mail address. You do not configure the local ID type and content when you set **Authentication Method** to **Certificate**. The ZyXEL device takes them from the certificate you select.

Table 11-6 Configuration > VPN > Tunnel IPSec Detail

FIELD	DESCRIPTION
ID Content	When you select **IP** in the **Local ID Type** field, type the IP address of your computer. The ZyXEL device uses the IP address in the **My IP Address** field if you configure the local **Content** field to **0.0.0.0** or leave it blank. It is recommended that you type an IP address other than **0.0.0.0** in the local **Content** field or use the **DNS** or **E-mail** ID type in the following situations. ➢ When there is a NAT router between the two IPSec routers. ➢ When you want the remote IPSec router to be able to distinguish between VPN connection requests that come in from IPSec routers with dynamic WAN IP addresses. ➢ With **DNS** or **E-mail** in the **Local ID Type** field, type a domain name or e-mail address by which to identify this ZyXEL device. Use up to 31 ASCII characters including spaces, although trailing spaces are truncated. The domain name or e-mail address is for identification purposes only and can be any string.
Address Type	This is the IP address(es) of computer(s) the A-end or Z-end of the VPN tunnel. The same (static) IP address is displayed twice in the **Address Start** and **Address End** fields when the **Address Type** field is configured to **Single**. The beginning and ending (static) IP addresses, in a range of computers are displayed when the **Address Type** is configured to **Range**. A (static) IP address and a subnet mask are displayed when the **Address Type** field is configured to **Subnet**. **These addresses cannot be automatically generated by Vantage.**
Address Start	Enter the beginning IP address of the computers behind the ZyXEL device.
Address End	Enter the ending IP address of the computers behind the ZyXEL device.
Port Start	**0** is the default and signifies any port. Some of the most common IP ports are: 21, FTP; 53, DNS; 23, Telnet; 80, HTTP; 25, SMTP; 110, POP3 Type a port number from 0 to 65535 for the starting port in a range.
Port End	Type the same port number as above to specify a single port. Type a port number greater than the start port number to specify the end port in a port range.
Phase 1	There are two phases to every IKE (Internet Key Exchange) negotiation – phase 1 (Authentication) and phase 2 (Key Exchange). A phase 1 exchange establishes an IKE SA and the second one uses that SA to negotiate SAs for IPSec.
Negotiation Mode	Select either **Main** or **Aggressive**. Aggressive mode is quicker than Main mode because it eliminates several steps when the communicating parties are negotiating authentication (phase 1). However the trade-off is that faster speed limits its negotiating power and it also does not provide identity protection. It is useful in remote access situations where the address of the initiator is not know by the responder and both parties want to use pre-shared key authentication.

Table 11-6 Configuration > VPN > Tunnel IPSec Detail

FIELD	DESCRIPTION
Pre-Shared key	A pre-shared key identifies a communicating party during a phase 1 IKE negotiation. It is called “pre-shared” because you have to share it with another party before you can communicate with them over a secure connection. ZyXEL gateways authenticate an IKE VPN session by matching pre-shared keys. Enter from 8 up to 31 characters. Any character may be used, including spaces, but trailing spaces are truncated. Multiple SAs connecting through a secure gateway must have the same pre-shared key.
Encryption Algorithm	Select an encryption algorithm from the pull-down menu. You can select either **DES** or **3DES**. **3DES** is more powerful but increases latency.
Authentication Algorithm	The Authentication Algorithms, HMAC-MD5 (RFC 2403) and HMAC-SHA-1 (RFC 2404, provide an authentication mechanism for the AH and ESP protocols. Select **MD5** for minimal security and **SHA-1** for maximum security. **MD5** (Message Digest 5) produces a 128-bit digest to authenticate packet data. **SHA-1** (Secure Hash Algorithm) produces a 160-bit digest to authenticate packet data.
SA Life Time (Seconds)	Define the length of time before an IKE Security Association automatically renegotiates in this field. It may range from 60 to 3,000,000 seconds (almost 35 days). A short SA Life Time increases security by forcing the two VPN gateways to update the encryption and authentication keys. However, every time the VPN tunnel renegotiates, all users accessing remote resources are temporarily disconnected.
Key Group	Diffie-Hellman (DH) is a public-key cryptography protocol that allows two parties to establish a shared secret over an unsecured communications channel. Diffie-Hellman is used within IKE SA setup to establish session keys. 768-bit (Group 1 - DH1) and 1024-bit (Group 2 – DH2) Diffie-Hellman groups are supported. Upon completion of the Diffie-Hellman exchange, the two peers have a shared secret, but the IKE SA is not authenticated. For authentication, use pre-shared keys.
Phase 2	There are two phases to every IKE (Internet Key Exchange) negotiation – phase 1 (Authentication) and phase 2 (Key Exchange). A phase 1 exchange establishes an IKE SA and the second one uses that SA to negotiate SAs for IPSec.
Active Protocol	The **ESP** and **AH** protocols are necessary to create a Security Association (SA), the foundation of an IPSec VPN. **AH** protocol (RFC 2402) was designed for integrity, authentication, sequence integrity (replay resistance), and non-repudiation but not for confidentiality, for which the **ESP** was designed. The **ESP** protocol (RFC 2406) provides encryption as well as some of the services offered by **AH**. **ESP** authenticating properties are limited compared to the **AH** due to the non-inclusion of the IP header information during the authentication process.

Table 11-6 Configuration > VPN > Tunnel IPSec Detail

FIELD	DESCRIPTION
Encapsulation	In **Transport** mode, the IP packet contains the security protocol (**AH** or **ESP**) located after the original IP header and options, but before any upper layer protocols contained in the packet (such as TCP and UDP). With ESP, protection is applied only to the upper layer protocols contained in the packet. The IP header information and options are not used in the authentication process. Therefore, the originating IP address cannot be verified for integrity against the data. With the use of **AH** as the security protocol, protection is extended forward into the IP header to verify the integrity of the entire packet by use of portions of the original IP header in the hashing process. **Tunnel** mode encapsulates the entire IP packet to transmit it securely. **Tunnel** mode is required for gateway services to provide access to internal systems. **Tunnel** mode is fundamentally an IP tunnel with authentication and encryption. This is the most common mode of operation
Encryption Algorithm	Select an encryption algorithm from the pull-down menu. You can select either **DES** or **3DES**. **3DES** is more powerful but increases latency.
Authentication Algorithm	The Authentication Algorithms, HMAC-MD5 (RFC 2403) and HMAC-SHA-1 (RFC 2404, provide an authentication mechanism for the **AH** and **ESP** protocols. Select **MD5** for minimal security and **SHA-1** for maximum security. **MD5** (Message Digest 5) produces a 128-bit digest to authenticate packet data. **SHA-1** (Secure Hash Algorithm) produces a 160-bit digest to authenticate packet data.
SA Life Time (Seconds)	Define the length of time before an IKE Security Association automatically renegotiates in this field. It may range from 60 to 3,000,000 seconds (almost 35 days). A short SA Life Time increases security by forcing the two VPN gateways to update the encryption and authentication keys. However, every time the VPN tunnel renegotiates, all users accessing remote resources are temporarily disconnected.
Perfect Forward Secrecy (PFS)	Choose whether to enable Perfect Forward Secrecy (**PFS**) using Diffie-Hellman public-key cryptography. Enabling **PFS** means that the key is transient. A brand new key using a new Diffie-Hellman exchange replaces the key for each new IPSec SA. With PFS enabled, if one key is compromised, previous and subsequent keys are not compromised, because subsequent keys are not derived from previous keys. The (time-consuming) Diffie-Hellman exchange is the trade-off for this extra security. Disabling PFS means new authentication and encryption keys are derived from the same root secret (which may have security implications in the long run) but allows faster SA setup (by bypassing the Diffie-Hellman key exchange).
Apply	Click **Apply** to apply your changes in this screen.
Cancel	Click **Cancel** to close this screen without applying any changes.

11.2.2 Edit a VPN Tunnel

Select a checkbox next to a VPN summary in *Figure 11-1* to proceed to the next screen.

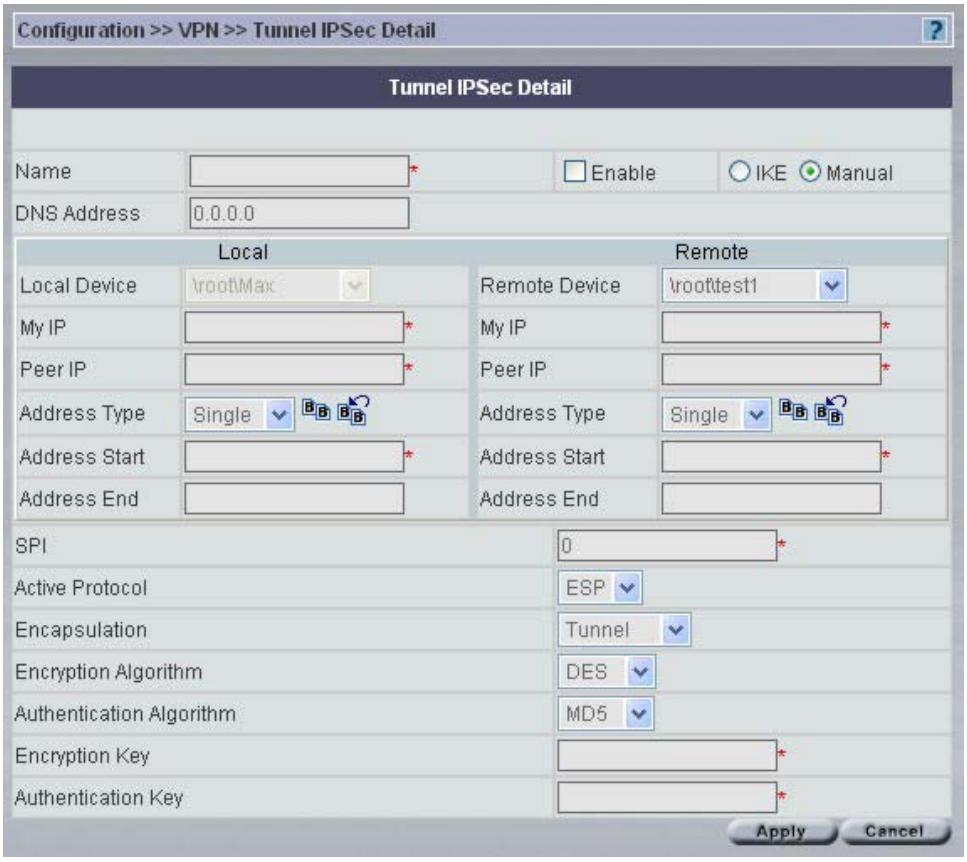


Figure 11-3 Configuration > VPN > Tunnel IPSec Detail – Edit

The following table describes the labels in this screen.

Table 11-7 Configuration > VPN > Tunnel IPSec Detail – Edit

LABEL	DESCRIPTION
Name	Type up to 32 characters to identify this VPN policy. You may use any character, including spaces, but the ZyXEL device drops trailing spaces.
Enable	Select this check box to activate this VPN policy.
IKE / Manual	Select **IKE** or **Manual**. **Manual** is a useful option for troubleshooting if you have problems using **IKE** key management.
DNS Address	Type a domain name (up to 31 characters) by which to identify the local or remote IPSec router.
A-End / Z-End	Local / Remote IP addresses must be static and correspond to the remote IPSec router's configured remote IP addresses. Two active SAs cannot have the local and remote IP address(es) both the same. Two active SAs can have the same local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time.

Table 11-7 Configuration > VPN > Tunnel IPSec Detail – Edit

LABEL	DESCRIPTION
A-End / Z-End Device	Select the name of the ZyXEL device from the pull-down list.
My IP	This is the IP address of the local and remote computer(s) of the VPN tunnel.
Peer IP	Type the IP address of the computer with which you will make the VPN connection or leave the field blank to have the ZyXEL device automatically use the address in the **Secure Gateway** field.
Address Start	When the **Address Type** field is configured to **Single**, enter a (static) IP address on the LAN behind the ZyXEL device. When the **Address Type** field is configured to **Range**, enter the beginning (static) IP address, in a range of computers on the LAN behind the ZyXEL device. When the **Address Type** field is configured to **Subnet**, this is a (static) IP address on the LAN behind the ZyXEL device.
Address End	When the **Address Type** field is configured to **Single**, this field is N/A. When the **Address Type** field is configured to **Range**, enter the end (static) IP address, in a range of computers on the LAN behind the ZyXEL device. When the **Address Type** field is configured to **Subnet**, this is a subnet mask on the LAN behind the ZyXEL device.
SPI	Type a number (base 10) from 1 to 999999 for the Security Parameter Index.
Active Protocol	Select ESP if you want to use ESP (Encapsulation Security Payload). The ESP protocol (RFC 2406) provides encryption as well as some of the services offered by AH. If you select ESP here, you must select options from the **Encryption Algorithm** and **Authentication Algorithm** fields. Select **AH** if you want to use AH (Authentication Header Protocol). The AH protocol (RFC 2402) was designed for integrity, authentication, sequence integrity (replay resistance), and non-repudiation but not for confidentiality, for which the ESP was designed. If you select **AH** here, you must select options from the **Authentication Algorithm** field.
Encapsulation	Select **Tunnel** mode or **Transport** mode from the drop-down list box.
Encryption Algorithm	Select **DES**, **3DES** or **NULL** from the drop-down list box. When you use **DES** or **3DES**, both sender and receiver must know the **Encryption Key**, which can be used to encrypt and decrypt the messages. The DES encryption algorithm uses a 56-bit key. Triple DES (**3DES**) is a variation on DES that uses a 168-bit key. As a result, **3DES** is more secure than **DES**. It also requires more processing power, resulting in increased latency and decreased throughput. Select **NULL** to set up a tunnel without encryption. When you select **NULL**, you do not enter an encryption key.
Authentication Algorithm	When you use **SHA1** or **MD5**, both sender and receiver must know the **Authentication Key**, which can be used to generate and verify a message authentication code. Select **SHA1** or **MD5** from the drop-down list box. **MD5** (Message Digest 5) and **SHA1** (Secure Hash Algorithm) are hash algorithms used to authenticate packet data. The **SHA1** algorithm is generally considered stronger than **MD5**, but is slower. Select **MD5** for minimal security and **SHA-1** for maximum security.
Encryption Key	This field only applies when you select **ESP**. With **DES**, type a unique key 8 ASCII characters long. With **3DES**, type a unique key 24 ASCII characters long. Any characters may be used, including spaces, but trailing spaces are truncated.
Authentication Key	Type a unique authentication key to be used by IPSec if applicable. Enter 16 characters for **MD5** authentication or 20 characters for **SHA-1** authentication. Any characters may be used, including spaces, but trailing spaces are truncated.
Apply	Click **Apply** to save your changes back to the ZyXEL device.
Cancel	Click **Cancel** to begin configuring this screen afresh.

11.3 VPN and NetBIOS

NetBIOS (Network Basic Input/Output System) are TCP or UDP broadcast packets that enable a computer to find other computers. It may sometimes be necessary to allow NetBIOS packets to pass through VPN tunnels in order to allow local computers to find computers on the remote network and vice versa.

Select a device, click **Configuration > VPN** and then click the NetBIOS tab to bring up the next screen

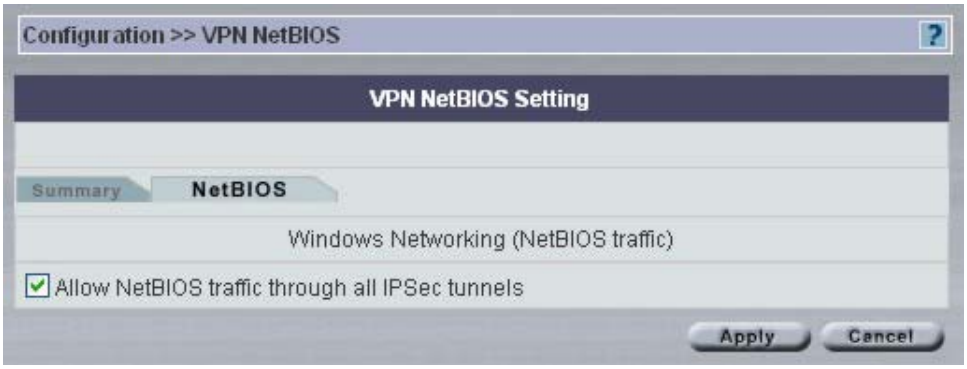


Figure 11-4 Configuration > VPN > NetBIOS

The following table describes the labels in this screen.

Table 11-8 Configuration > VPN > NetBIOS

LABEL	DESCRIPTION
Windows Networking (NetBIOS traffic)	
Allow NetBIOS traffic through all IPSec tunnels	Select the check box to permit NetBIOS packets through the VPN connection.
Apply	Click **Apply** to save your changes back to the ZyXEL device.
Cancel	Click **Cancel** to begin configuring this screen afresh.

12 Configuration > Firewall

This chapter shows you how to configure firewall for your devices.

12.1 Firewall Overview

Originally, the term *firewall* referred to a construction technique designed to prevent the spread of fire from one room to another. The networking term "firewall" is a system or group of systems that enforces an access-control policy between two networks. It may also be defined as a mechanism used to protect a trusted network from an untrusted network. Of course, firewalls cannot solve every security problem. A firewall is *one* of the mechanisms used to establish a network security perimeter in support of a network security policy. It should never be the *only* mechanism or method employed. For a firewall to guard effectively, you must design and deploy it appropriately. This requires integrating the firewall into a broad information-security policy. In addition, specific policies must be implemented within the firewall itself.

12.2 Types of Firewalls

There are three main types of firewalls:

1. Packet Filtering Firewalls
2. Application-level Firewalls
3. Stateful Inspection Firewalls

12.2.1 Packet Filtering Firewalls

Packet filtering firewalls restrict access based on the source/destination computer network address of a packet and the type of application.

12.2.2 Application-level Firewalls

Application-level firewalls restrict access by serving as proxies for external servers. Since they use programs written for specific Internet services, such as HTTP, FTP and telnet, they can evaluate network packets for valid application-specific data. Application-level gateways have a number of general advantages over the default mode of permitting application traffic directly to internal hosts:

i. Information hiding prevents the names of internal systems from being made known via DNS to outside systems, since the application gateway is the only host whose name must be made known to outside systems.

ii. Robust authentication and logging pre-authenticates application traffic before it reaches internal hosts and causes it to be logged more effectively than if it were logged with standard host logging. Filtering rules at the packet filtering router can be less complex than they would be if the router needed to filter application traffic and direct it to a number of specific systems. The router need only allow application traffic destined for the application gateway and reject the rest.

12.2.3 Stateful Inspection Firewalls

Stateful inspection firewalls restrict access by screening data packets against defined access rules. They make access control decisions based on IP address and protocol. They also "inspect" the session data to assure the integrity of the connection and to adapt to dynamic protocols. These firewalls generally provide the best speed and transparency; however, they may lack the granular application level access control or caching that some proxies support.

Firewalls, of one type or another, have become an integral part of standard security solutions for enterprises.

12.3 Introduction to ZyXEL's Firewall

The ZyXEL device firewall is a stateful inspection firewall and is designed to protect against Denial of Service attacks when activated (in SMT menu 21.2 or in the web configurator). The ZyXEL device's purpose is to allow a private Local Area Network (LAN) to be securely connected to the Internet. The ZyXEL device can be used to prevent theft, destruction and modification of data, as well as log events, which may be important to the security of your network. The ZyXEL device also has packet-filtering capabilities.

The ZyXEL device is installed between the LAN and a broadband modem connecting to the Internet. This allows it to act as a secure gateway for all data passing between the Internet and the LAN.

- The WAN (Wide Area Network) port attaches to the broadband modem (cable or ADSL) connecting to the Internet.
- The LAN (Local Area Network) port attaches to a network of computers, which needs security from the outside world. These computers will have access to Internet services such as e-mail, FTP, and the World Wide Web. However, "inbound access" will not be allowed unless the remote host is authorized to use a specific service.

12.4 Denial of Service

Denials of Service (DoS) attacks are aimed at devices and networks with a connection to the Internet. Their goal is not to steal information, but to disable a device or network so users no longer have access to network resources. The ZyXEL device is pre-configured to automatically detect and thwart all known DoS attacks.

12.4.1 Basics

Computers share information over the Internet using a common language called TCP/IP. TCP/IP, in turn, is a set of application protocols that perform specific functions. An "extension number", called the "TCP port" or "UDP port" identifies these protocols, such as HTTP (Web), FTP (File Transfer Protocol), POP3 (E-mail), etc. For example, Web traffic by default uses TCP port 80.

When computers communicate on the Internet, they are using the client/server model, where the server "listens" on a specific TCP/UDP port for information requests from remote client computers on the network. For example, a Web server typically listens on port 80. Please note that while a computer may be intended for use over a single port, such as Web on port 80, other ports are also active. If the person configuring or managing the computer is not careful, a hacker could attack it over an unprotected port.

Some of the most common IP ports are:

Table 12-1 Common IP Ports

21	FTP	53	DNS
23	Telnet	80	HTTP
25	SMTP	110	POP3

12.4.2 Types of DoS Attacks

There are four types of DoS attacks:

1. Those that exploit bugs in a TCP/IP implementation.
2. Those that exploit weaknesses in the TCP/IP specification.
3. Brute-force attacks that flood a network with useless data.

4. IP Spoofing.

1. "**Ping of Death**" and "**Teardrop**" attacks exploit bugs in the TCP/IP implementations of various computer and host systems.

   Ping of Death uses a "ping" utility to create an IP packet that exceeds the maximum 65,536 bytes of data allowed by the IP specification. The oversize packet is then sent to an unsuspecting system. Systems may crash, hang or reboot.

   Teardrop attack exploits weaknesses in the reassembly of IP packet fragments. As data is transmitted through a network, IP packets are often broken up into smaller chunks. Each fragment looks like the original IP packet except that it contains an offset field that says, for instance, "This fragment is carrying bytes 200 through 400 of the original (non fragmented) IP packet." The Teardrop program creates a series of IP fragments with overlapping offset fields. When these fragments are reassembled at the destination, some systems will crash, hang, or reboot.

2. Weaknesses in the TCP/IP specification leave it open to "**SYN Flood**" and "**LAND**" attacks. These attacks are executed during the handshake that initiates a communication session between two applications.

   Under normal circumstances, the application that initiates a session sends a SYN (synchronize) packet to the receiving server. The receiver sends back an ACK (acknowledgment) packet and its own SYN, and then the initiator responds with an ACK (acknowledgment). After this handshake, a connection is established.

   SYN Attack floods a targeted system with a series of SYN packets. Each packet causes the targeted system to issue a SYN-ACK response. While the targeted system waits for the ACK that follows the SYN-ACK, it queues up all outstanding SYN-ACK responses on what is known as a backlog queue. SYN-ACKs are moved off the queue only when an ACK comes back or when an internal timer (which is set at relatively long intervals) terminates the three-way handshake. Once the queue is full, the system will ignore all incoming SYN requests, making the system unavailable for legitimate users.

   In a **LAND Attack**, hackers flood SYN packets into the network with a spoofed source IP address of the targeted system. This makes it appear as if the host computer sent the packets to itself, making the system unavailable while the target system tries to respond to itself.

3. A **brute-force** attack, such as a "Smurf" attack, targets a feature in the IP specification known as directed or subnet broadcasting, to quickly flood the target network with useless data. A Smurf hacker floods a router with Internet Control Message Protocol (ICMP) echo request packets (pings). Since the destination IP address of each packet is the broadcast address of the network, the router will broadcast the ICMP echo request packet to all hosts on the network. If there are numerous hosts, this will create a large amount of ICMP echo request and response traffic. If a hacker chooses to spoof the source IP address of the ICMP echo request packet, the resulting ICMP traffic will not only clog up the "intermediary" network, but will also congest the network of the spoofed source IP address, known as the "victim" network. This flood of broadcast traffic consumes all available bandwidth, making communications impossible.

- ICMP Vulnerability

  ICMP is an error-reporting protocol that works in concert with IP. The following ICMP types trigger an alert:

Table 12-2 ICMP Commands That Trigger Alerts

5	REDIRECT
13	TIMESTAMP_REQUEST
14	TIMESTAMP_REPLY
17	ADDRESS_MASK_REQUEST

Table 12-2 ICMP Commands That Trigger Alerts

18	ADDRESS_MASK_REPLY

- Illegal Commands (NetBIOS and SMTP)

  The only legal NetBIOS commands are the following - all others are illegal.

Table 12-3 Legal NetBIOS Commands

MESSAGE:
REQUEST:
POSITIVE:
NEGATIVE:
RETARGET:
KEEPALIVE:

All SMTP commands are illegal except for those displayed in the following tables.

Table 12-4 Legal SMTP Commands

AUTH	DATA	EHLO	ETRN	EXPN	HELO	HELP	MAIL	NOOP
QUIT	RCPT	RSET	SAML	SEND	SOML	TURN	VRFY	

- Traceroute

  Traceroute is a utility used to determine the path a packet takes between two endpoints. Sometimes when a packet filter firewall is configured incorrectly an attacker can traceroute the firewall gaining knowledge of the network topology inside the firewall.

4. Often, many DoS attacks also employ a technique known as "**IP Spoofing**" as part of their attack. IP Spoofing may be used to break into systems, to hide the hacker's identity, or to magnify the effect of the DoS attack. IP Spoofing is a technique used to gain unauthorized access to computers by tricking a router or firewall into thinking that the communications are coming from within the trusted network. To engage in IP spoofing, a hacker must modify the packet headers so that it appears that the packets originate from a trusted host and should be allowed through the router or firewall. The ZyXEL device blocks all IP Spoofing attempts.

12.5 Stateful Inspection

With stateful inspection, fields of the packets are compared to packets that are already known to be trusted. For example, if you access some outside service, the proxy server remembers things about your original request, like the port number and source and destination addresses. This “remembering” is called *saving the state.* When the outside system responds to your request, the firewall compares the received packets with the saved state to determine if they are allowed in. The ZyXEL device uses stateful packet inspection to protect the private LAN from hackers and vandals on the Internet. By default, the ZyXEL device’s stateful inspection allows all communications to the Internet that originate from the LAN, and blocks all traffic to the LAN that originates from the Internet. In summary, stateful inspection:

- Allows all sessions originating from the LAN (local network) to the WAN (Internet).
- Denies all sessions originating from the WAN to the LAN.

12.5.1 Stateful Inspection Process

In this example, the following sequence of events occurs when a TCP packet leaves the LAN network through the firewall's WAN interface. The TCP packet is the first in a session, and the packet's application layer protocol is configured for a firewall rule inspection:

1. The packet travels from the firewall's LAN to the WAN.
2. The packet is evaluated against the interface's existing outbound access list, and the packet is permitted (a denied packet would simply be dropped at this point).
3. The packet is inspected by the firewall to determine and record information about the state of the packet's connection. This information is recorded in a new state table entry created for the new connection. If there is not a firewall rule for this packet and it is not an attack, then **Firewall Summary** screen's **Action for packets that don't match firewall rules** field determines the action for this packet.
4. Based on the obtained state information, a firewall rule creates a temporary access list entry that is inserted at the beginning of the WAN interface's inbound extended access list. This temporary access list entry is designed to permit inbound packets of the same connection as the outbound packet just inspected.
5. The outbound packet is forwarded out through the interface.
6. Later, an inbound packet reaches the interface. This packet is part of the connection previously established with the outbound packet. The inbound packet is evaluated against the inbound access list, and is permitted because of the temporary access list entry previously created.
7. The packet is inspected by a firewall rule, and the connection's state table entry is updated as necessary. Based on the updated state information, the inbound extended access list temporary entries might be modified, in order to permit only packets that are valid for the current state of the connection.
8. Any additional inbound or outbound packets that belong to the connection are inspected to update the state table entry and to modify the temporary inbound access list entries as required, and are forwarded through the interface.
9. When the connection terminates or times out, the connection's state table entry is deleted and the connection's temporary inbound access list entries are deleted.

12.5.2 Stateful Inspection and the ZyXEL device

Additional rules may be defined to extend or override the default rules. For example, a rule may be created which will:

1. Block all traffic of a certain type, such as IRC (Internet Relay Chat), from the LAN to the Internet.
2. Allow certain types of traffic from the Internet to specific hosts on the LAN.
3. Allow access to a Web server to everyone but competitors.
4. Restrict use of certain protocols, such as Telnet, to authorized users on the LAN.

These custom rules work by evaluating the network traffic's Source IP address, Destination IP address, IP protocol type, and comparing these to rules set by the administrator.

The ability to define firewall rules is a very powerful tool. Using custom rules, it is possible to disable all firewall protection or block all access to the Internet. Use extreme caution when creating or deleting firewall rules. Test changes after creating them to make sure they work correctly.

Below is a brief technical description of how these connections are tracked. Connections may either be defined by the upper protocols (for instance, TCP), or by the ZyXEL device itself (as with the "virtual connections" created for UDP and ICMP).

12.5.3 TCP Security

The ZyXEL device uses state information embedded in TCP packets. The first packet of any new connection has its SYN flag set and its ACK flag cleared; these are "initiation" packets. All packets that do not have this flag structure are called "subsequent" packets, since they represent data that occurs later in the TCP stream.

If an initiation packet originates on the WAN, this means that someone is trying to make a connection from the Internet into the LAN. Except in a few special cases (see "Upper Layer Protocols" shown next), these packets are dropped and logged.

If an initiation packet originates on the LAN, this means that someone is trying to make a connection from the LAN to the Internet. Assuming that this is an acceptable part of the security policy (as is the case with the default policy), the connection will be allowed. A cache entry is added which includes connection information such as IP addresses, TCP ports, sequence numbers, etc.

When the ZyXEL device receives any subsequent packet (from the Internet or from the LAN), its connection information is extracted and checked against the cache. A packet is only allowed to pass through if it corresponds to a valid connection (that is, if it is a response to a connection which originated on the LAN).

12.5.4 UDP/ICMP Security

UDP and ICMP do not themselves contain any connection information (such as sequence numbers). However, at the very minimum, they contain an IP address pair (source and destination). UDP also contains port pairs, and ICMP has type and code information. All of this data can be analyzed in order to build "virtual connections" in the cache.

For instance, any UDP packet that originates on the LAN will create a cache entry. Its IP address and port pairs will be stored. For a short period of time, UDP packets from the WAN that have matching IP and UDP information will be allowed back in through the firewall.

A similar situation exists for ICMP, except that the ZyXEL device is even more restrictive. Specifically, only outgoing echoes will allow incoming echo replies, outgoing address mask requests will allow incoming address mask replies, and outgoing timestamp requests will allow incoming timestamp replies. No other ICMP packets are allowed in through the firewall, simply because they are too dangerous and contain too little tracking information. For instance, ICMP redirect packets are never allowed in, since they could be used to reroute traffic through attacking machines.

12.5.5 Upper Layer Protocols

Some higher layer protocols (such as FTP and RealAudio) utilize multiple network connections simultaneously. In general terms, they usually have a "control connection" which is used for sending commands between endpoints, and then "data connections" which are used for transmitting bulk information.

Consider the FTP protocol. A user on the LAN opens a control connection to a server on the Internet and requests a file. At this point, the remote server will open a data connection from the Internet. For FTP to work properly, this connection must be allowed to pass through even though a connection from the Internet would normally be rejected.

In order to achieve this, the ZyXEL device inspects the application-level FTP data. Specifically, it searches for outgoing "PORT" commands, and when it sees these; it adds a cache entry for the anticipated data connection. This can be done safely, since the PORT command contains address and port information, which can be used to uniquely identify the connection.

Any protocol that operates in this way must be supported on a case-by-case basis. You can use the web configurator's Custom Ports feature to do this.

12.6 Firewall Policies Overview

Firewall rules are grouped based on the direction of travel of packets to which they apply: The following example is for a ZyWALL 100 device.

- LAN to LAN/ZyWALL
- LAN to WAN
- LAN to DMZ
- WAN to LAN
- WAN to WAN/ZyWALL
- WAN to DMZ
- DMZ to LAN
- DMZ to WAN
- DMZ to DMZ/ZyWALL

DMZ is not available on all models.

By default, the ZyXEL device's stateful packet inspection allows packets traveling in the following directions:

- LAN to LAN/ZyWALL
  This allows computers on the LAN to manage the ZyWALL and communicate between networks or subnets connected to the LAN interface.
- LAN to WAN
- LAN to DMZ
- WAN to DMZ
- DMZ to WAN

By default, the ZyXEL device's stateful packet inspection blocks packets traveling in the following directions:

- WAN to LAN
- WAN to WAN/ZyWALL

  This prevents computers on the WAN from using the ZyXEL device as a gateway to communicate with other computers on the WAN and/or managing the ZyXEL device.
- DMZ to LAN
- DMZ to DMZ/ZyWALL

  This prevents computers on the DMZ from communicating between networks or subnets connected to the DMZ interface and/or managing the ZyXEL device.

You may define additional rules and sets or modify existing ones but please exercise extreme caution in doing so.

If you configure firewall rules without a good understanding of how they work, you might inadvertently introduce security risks to the firewall and to the protected network. Make sure you test your rules after you configure them.

For example, you may create rules to:

- Block certain types of traffic, such as IRC (Internet Relay Chat), from the LAN to the Internet.
- Allow certain types of traffic, such as Lotus Notes database synchronization, from specific hosts on the Internet to specific hosts on the LAN.
- Allow everyone except your competitors to access a Web server.
- Restrict use of certain protocols, such as Telnet, to authorized users on the LAN.

These custom rules work by comparing the Source IP address, Destination IP address and IP protocol type of network traffic to rules set by the administrator. Your customized rules take precedence and override the ZyXEL device's default rules.

12.7 Rule Logic Overview

Study these points carefully before configuring rules.

12.7.1 Rule Checklist

1. State the intent of the rule. For example, "This restricts all IRC access from the LAN to the Internet." Or, "This allows a remote Lotus Notes server to synchronize over the Internet to an inside Notes server."
2. Is the intent of the rule to forward or block traffic?
3. What direction of traffic does the rule apply to?
4. What IP services will be affected?
5. What computers on the LAN or DMZ are to be affected (if any)?
6. What computers on the Internet will be affected? The more specific, the better. For example, if traffic is being allowed from the Internet to the LAN, it is better to allow only certain machines on the Internet to access the LAN.

12.7.2 Security Ramifications

Once the logic of the rule has been defined, it is critical to consider the security ramifications created by the rule:

1. Does this rule stop LAN users from accessing critical resources on the Internet? For example, if IRC is blocked, are there users that require this service?
2. Is it possible to modify the rule to be more specific? For example, if IRC is blocked for all users, will a rule that blocks just certain users be more effective?
3. Does a rule that allows Internet users access to resources on the LAN create a security vulnerability? For example, if FTP ports (TCP 20, 21) are allowed from the Internet to the LAN, Internet users may be able to connect to computers with running FTP servers.
4. Does this rule conflict with any existing rules?

Once these questions have been answered, adding rules is simply a matter of plugging the information into the correct fields in the web configurator screens.

12.7.3 Key Fields For Configuring Rules

Action

Should the action be to **Block** or **Forward**?

"Block" means the firewall silently discards the packet.

Service

Select the service from the **Service** scrolling list box. If the service is not listed, it is necessary to first define it.

Source Address

What is the connection's source address; is it on the LAN, DMZ or WAN? Is it a single IP, a range of IPs or a subnet?

Destination Address

What is the connection's destination address; is it on the LAN, DMZ or WAN? Is it a single IP, a range of IPs or a subnet?

12.7.4 Alerts

Alerts are reports on events, such as attacks, that you may want to know about right away. You can choose to generate an alert when an attack is detected by selecting the **Generate alert when attack detected** checkbox.

Configure the **Log Settings** screen to have the ZyXEL device send an immediate e-mail message to you when an event generates an alert. Refer to the chapter on logs for details.

12.7.5 Services and Port Numbers

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

Table 12-5 Services and Port Numbers

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

12.8 Firewall Configuration

12.8.1 Firewall Summary

Ordering Rules

When you click Add, a new rule is always appended to the end of the list. Use the **Move selected item to beginning index number** textbox and **Move** button to put a single rule in a different place.

Select a device and then click **Configuration > Firewall**.

Figure 12-1 Configuration >Firewall

The following table describes the labels in this screen.

Table 12-6 Configuration >Firewall

LABEL	DESCRIPTION
Enable Firewall	Select this check box to activate the firewall. The ZyXEL device performs access control and protects against Denial of Service (DoS) attacks when the firewall is activated.
Bypass Triangle Route	Select this check box to have the ZyXEL device firewall ignore the use of triangle route topology on the network. See the *Appendices* for more on triangle route topology.
Attack Detected Alert	Select this checkbox to have the ZyXEL device generate an alert when it identifies an attack.
DoS Settings	Click the DoS settings link to configure global firewall Denial of Services settings.
Packet Direction	Use the drop-down list box to select a direction of travel of packets for which you want to configure firewall rules.
Log packets that don't match these rules.	Select the check box to create a log (when the above action is taken) for packets that are traveling in the selected direction and do not match any of the rules below.
Action for packets that don't match firewall rules	Select whether to **Block** (silently discard) or **Forward** (allow the passage of) packets that don't match any of the firewall rules you configured.
The following read-only fields summarize the rules you have created that apply to traffic traveling in the selected packet direction. The firewall rules that you configure (summarized below) take priority over the general firewall action settings above. Select an ACL hyperlink to edit that ACL rule.	
Index	This is your firewall rule number. Select a rule hyperlink to edit that rule. The ordering of your rules is important as rules are applied in turn. The **Move** field below allows you to reorder your rules.
Source	This field lists the source IP address of the incoming packet.
Destination	This field lists the destination IP address of the outgoing packet.

Table 12-6 Configuration >Firewall

LABEL	DESCRIPTION
Services	This field displays the available services that may be added in from the **Selected Services** in the **Firewall Rule** screen.
Action	This field displays whether the rule allows (**Forward**) or discards (**Block**) packets that match this rule.
Log	This field shows you if a log is created for packets that match the rule (**Match**), don't match the rule (**Not Match**), both (**Both**) or no log is created (**None**).
Alert	This field tells you whether this rule generates an alert (**Yes**) or not (**No**) when the rule is matched.
Move	Select a rule's Index option button and type a number for where you want to put that rule. Click **Move** to move the rule to the number that you typed. The ordering of your rules is important as they are applied in order of their numbering.
Apply	Click **Apply** to save your changes back to the ZyXEL device.
Add	Click **Add** to create a new firewall rule.
Delete	Select a rule index and then click **Delete** to delete an existing firewall rule. Note that subsequent firewall rules move up by one when you take this action.

12.8.2 DoS Settings

Click the DoS settings link to configure global firewall Denial of Services settings.

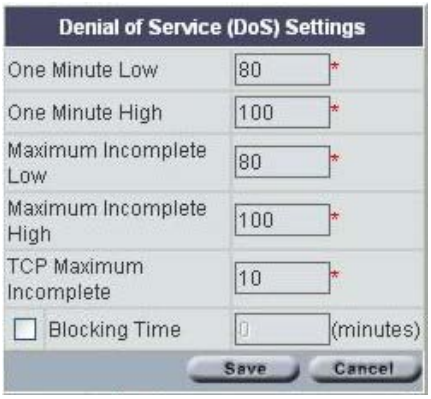


Figure 12-2 Configuration > Firewall > DoS Settings

The following table describes the labels in this screen.

Table 12-7 Configuration > Firewall > DoS Settings

LABEL	DESCRIPTION	EXAMPLE VALUES
One Minute Low	This is the rate of new half-open sessions that causes the firewall to stop deleting half-open sessions. The ZyXEL device continues to delete half-open sessions as necessary, until the rate of new connection attempts drops below this number.	80 existing half-open sessions.

Table 12-7 Configuration > Firewall > DoS Settings

LABEL	DESCRIPTION	EXAMPLE VALUES
One Minute High	This is the rate of new half-open sessions that causes the firewall to start deleting half-open sessions. When the rate of new connection attempts rises above this number, the ZyXEL device deletes half-open sessions as required to accommodate new connection attempts.	100 half-open sessions per minute. The above numbers cause the ZyXEL device to start deleting half-open sessions when more than 100 session establishment attempts have been detected in the last minute, and to stop deleting half-open sessions when fewer than 80 session establishment attempts have been detected in the last minute.
Maximum Incomplete Low	This is the number of existing half-open sessions that causes the firewall to stop deleting half-open sessions. The ZyXEL device continues to delete half-open requests as necessary, until the number of existing half-open sessions drops below this number.	80 existing half-open sessions.
Maximum Incomplete High	This is the number of existing half-open sessions that causes the firewall to start deleting half-open sessions. When the number of existing half-open sessions rises above this number, the ZyXEL device deletes half-open sessions as required to accommodate new connection requests. Do not set **Maximum Incomplete High** to lower than the current **Maximum** I**ncomplete Low** number.	100 existing half-open sessions. The above values causes the ZyXEL device to start deleting half-open sessions when the number of existing half-open sessions rises above 100, and to stop deleting half-open sessions with the number of existing half-open sessions drops below 80.
TCP Maximum Incomplete	This is the number of existing half-open TCP sessions with the same destination host IP address that causes the firewall to start dropping half-open sessions to that same destination host IP address. Enter a number between 1 and 256. As a general rule, you should choose a smaller number for a smaller network, a slower system or limited bandwidth.	10 existing half-open TCP sessions
Blocking Time	When **TCP Maximum Incomplete** is reached you can choose if the next session should be allowed or blocked. If you check **Blocking Time** any new sessions will be blocked for the length of time you specify in the next field (min) and all old incomplete sessions will be cleared during this period. If you want strong security, it is better to block the traffic for a short time, as it will give the server some time to digest the loading.	Select this check box to specify a number in minutes (min) text box.
(minutes)	Enter the length of **Blocking Time** in minutes.	0
Save	Click **Save** to save your changes and return to the previous screen.	
Cancel	Click **Cancel** to return to the previous screen.	

12.8.3 Add/Edit a Firewall Rule

Each device has a different number of rules and custom ports; see the device *User Guide* for more details.

In *Figure 12-1*, select an existing rule to edit it or click **Add** to create a new firewall rule.

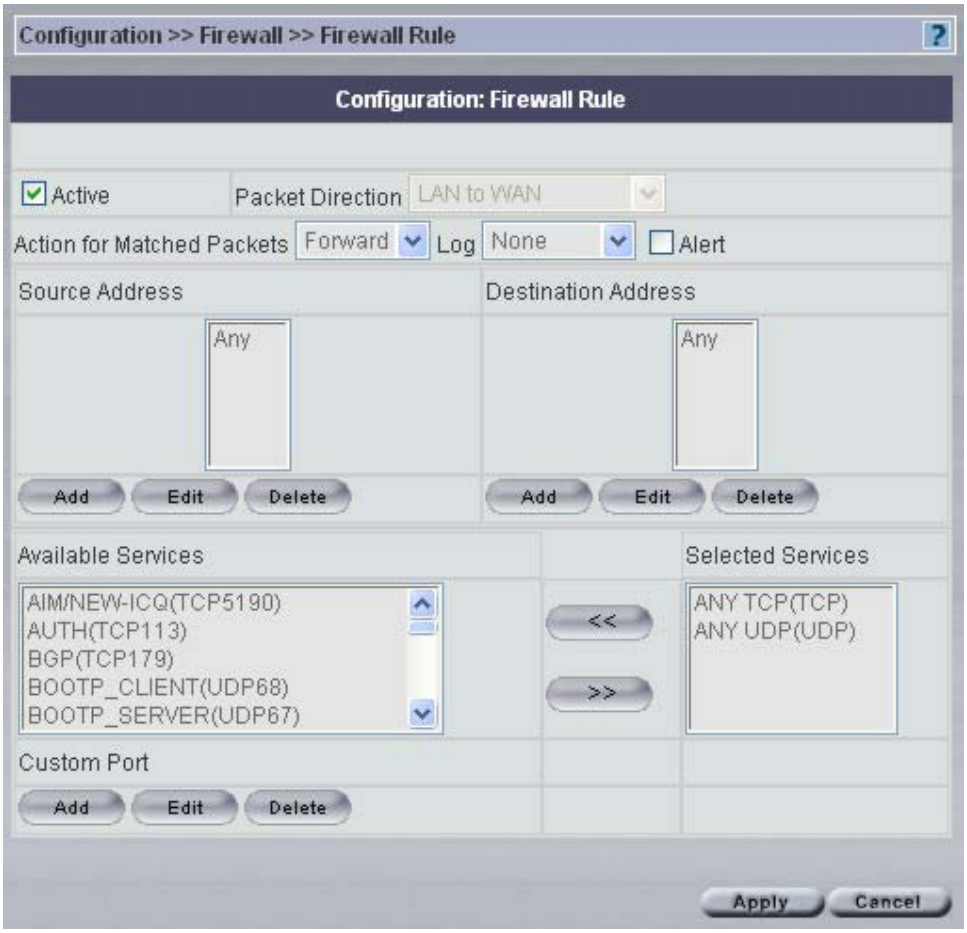


Figure 12-3 Configuration >Firewall > Edit

The following table describes the labels in this screen.

Table 12-8 Configuration >Firewall > Edit

LABEL	DESCRIPTION
Active	Check the **Active** check box to have the ZyXEL device use this rule. Leave it unchecked if you do not want the ZyXEL device to use the rule after you apply it
Packet Direction	Use the drop-down list box to select the direction of packet travel to which you want to apply this firewall rule.
Action for matched packets	Select whether to **Block** (silently discard) or **Forward** (allow the passage of) packets that are traveling in the selected direction.
Log	This field determines if a log is created for packets that match the rule (**Match**), don't match the rule (**Not Match**), both (**Both**) or no log is created (**None**). Go to the **Log Settings** page and select the **Access Control** logs category to have the ZyXEL device record these logs.
Alert	Check the **Alert** check box to determine that this rule generates an alert when the rule is matched.
Source Address	Click **Add** to add a new address, **Edit** to edit an existing one or **Delete** to delete one. Please see the next section for more information on adding and editing source addresses.

Table 12-8 Configuration >Firewall > Edit

LABEL	DESCRIPTION
Destination Address	Click **Add** to add a new address, **Edit** to edit an existing one or **Delete** to delete one. Please see the following section on adding and editing destination addresses.
Available/ Selected Services	Highlight a service from the **Available Services** box on the left, then click **>>** to add it to the **Selected Services** box on the right. To remove a service, highlight it in the **Selected Services** box on the right, then click **<<**.
Custom Port	
Add	Click this button to bring up the screen that you use to configure a new custom service that is not in the predefined list of services.
Edit	Select a custom service (denoted by an "*") from the **Available Services** list and click this button to edit the service.
Delete	Select a custom service (denoted by an "*") from the **Available Services** list and click this button to remove the service.
Apply	Click **Apply** to save the current rule setting to the device.
Cancel	Click **Cancel** to exit this screen without saving,

12.8.4 Add/Edit Source/Destination IP Addresses

Click **Add** or **Edit** under **Source Address** or **Destination Address** to add or edit a source or destination IP address.

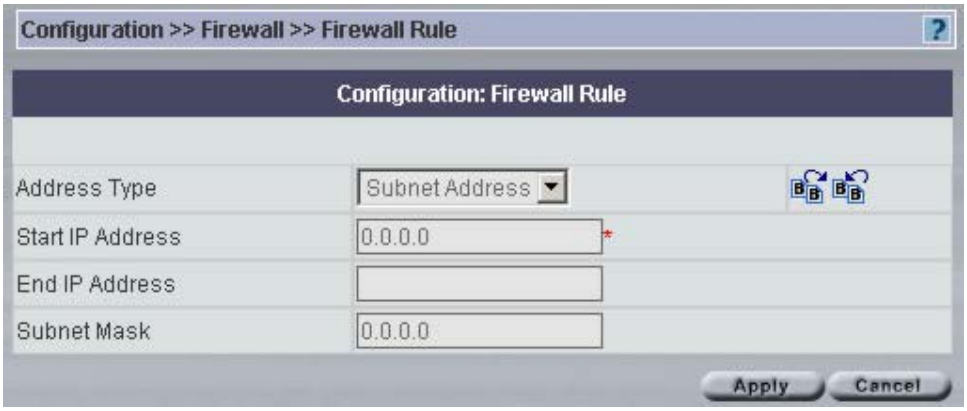


Figure 12-4 Configuration >Firewall > IP Address

The following table describes the labels in this screen.

Table 12-9 Configuration >Firewall > IP Address

LABEL	DESCRIPTION
Address Type	Do you want your rule to apply to packets with a particular (single) IP, a range of IP addresses (e.g., 192.168.1.10 to 192.169.1.50), a subnet or any IP address? Select an option from the drop-down list box that includes: **Single Address**, **Range Address**, **Subnet Address** and **Any Address**.
Start IP Address	Enter the single IP address or the starting IP address in a range here.
End IP Address	Enter the ending IP address in a range here.

Table 12-9 Configuration >Firewall > IP Address

LABEL	DESCRIPTION
Subnet Mask	Enter the subnet mask here, if applicable.
Apply	Click **Apply** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving.

12.8.5 Custom Ports

Configure customized ports for services not predefined by the ZyXEL device. For a comprehensive list of port numbers and services, visit the IANA (Internet Assigned Number Authority) web site.

Click **Add** or **Edit** under **Custom Port** to add or edit a custom port.

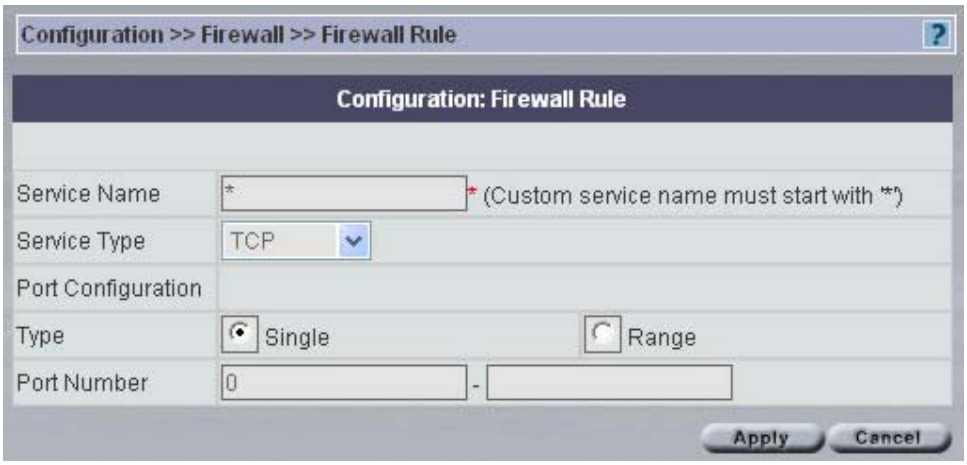


Figure 12-5 Firewall Custom Port

The following table describes the labels in this screen.

Table 12-10 Firewall Custom Port

LABEL	DESCRIPTION
Service Name	Enter a unique name for your custom port. All custom ports must begin with "*" to identify it as such in the Available Services list box in *Figure 12-3*.
Service Type	Choose the IP port (**TCP**, **UDP** or **Both**) that defines your customized port from the drop down list box.
Port Configuration Type	Click **Single** to specify one port only or **Range** to specify a span of ports that define your customized service.
Port Number	Enter a single port number or the range of port numbers that define your customized service.
Apply	Click **Apply** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving,

13 Configuration > Device Log

Use these screens to configure device logs. Not all devices have the centralized feature.

13.1 Device Logs

Select a device and then click **Configuration > Device Log**.

Figure 13-1 Configuration > Device Log > Device

The following table describes the labels in this screen.

Table 13-1 Configuration > Device Log > Device

LABEL	DESCRIPTION
Select Time Period	Select the time period (Last Day, Last 2 Days...Last 7 Days) for which you wish to view logs.
Src	This field lists the source IP address and the port number of the incoming packet.
Dest	This field lists the destination IP address and the port number of the packet.
Time	This field displays the time the log was recorded. See the chapter on system maintenance and information to configure the ZyXEL device's time and date.
Content	This field states the reason for the log.
Note	This field displays a short description.
Retrieve	Click **Retrieve** to renew the logs displayed for the selected device.
Purge	Click **Purge** to erase the logs displayed for the selected device. Only an administrator with the correct permissions that can see the device can purge the logs.
Report	Click **Report** to generate a report on the logs for the time period selected and the current page displayed only.

13.2 Device Logging Options

Use the **Logging Options** screen to configure to where the ZyXEL device is to send logs; the schedule for when the ZyXEL device is to send the logs and which logs and/or immediate alerts the ZyXEL device is to send.

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

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

To change a ZyXEL devices log settings, select a device, click **Configuration > Device Log** and then click the **Log Settings** tab. The screen appears as shown next.

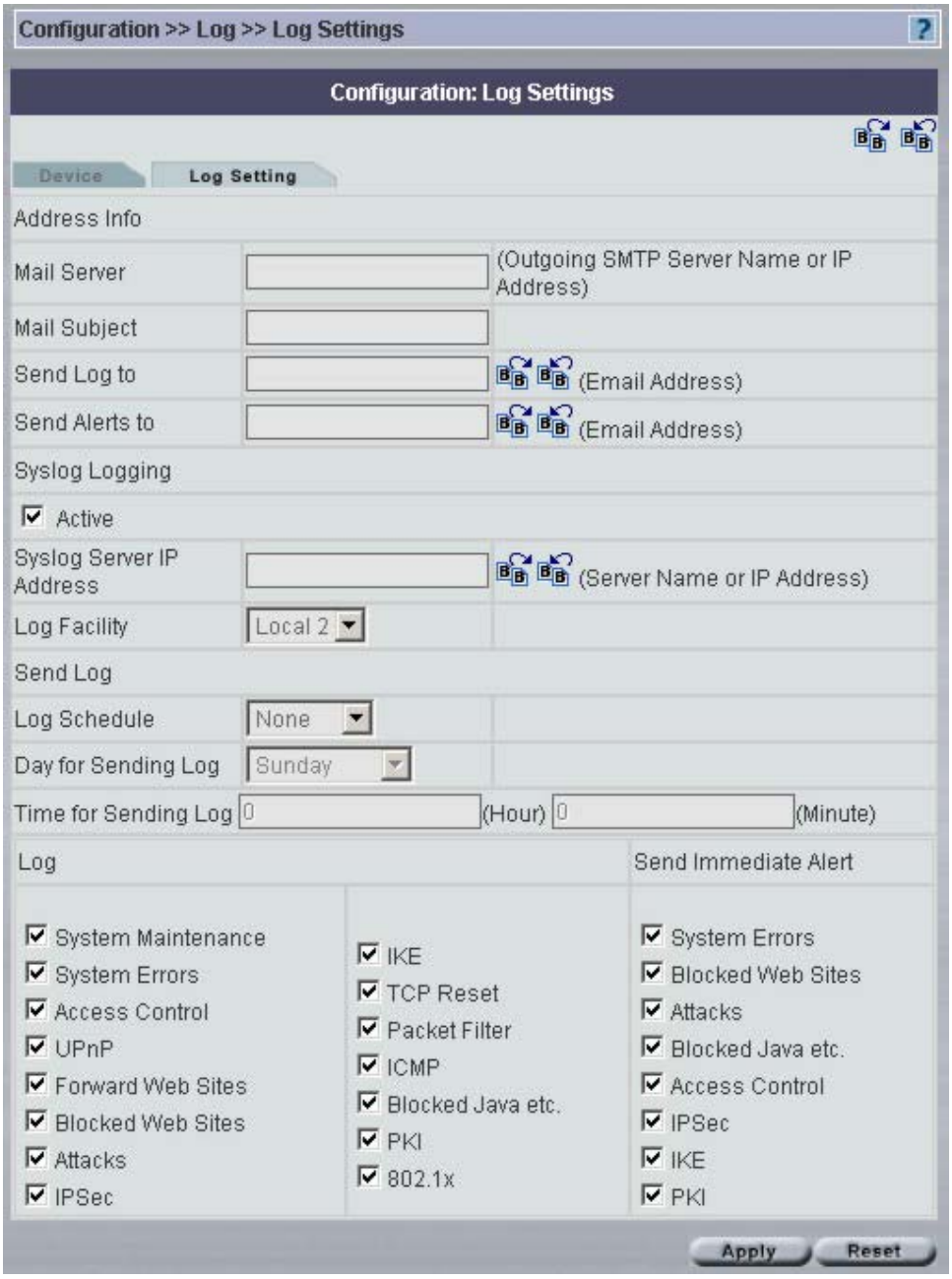


Figure 13-2 Configuration > Device Logs > Log Settings

The following table describes the labels in this screen.

Table 13-2 Configuration > Device Logs > Log Settings

LABEL	DESCRIPTION

Table 13-2 Configuration > Device Logs > Log Settings

LABEL	DESCRIPTION
Address Info	
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.
Send Log To	Logs are sent to the e-mail address specified in this field. If this field is left blank, logs will not be sent via e-mail.
Send Alerts To	Alerts are sent to the e-mail address specified in this field. If this field is left blank, alerts will not be sent via e-mail.
Syslog Logging	Syslog logging sends a log to an external syslog server used to store logs.
Active	Click **Active** to enable syslog logging.
Syslog Server IP Address	Enter the server IP address of the syslog server that will log the selected categories of logs. The device syslog server must be the same as the Vantage syslog server.
Log Facility	Select a location from the drop down list box. The log facility allows you to log the messages to different files in the syslog server. Refer to the documentation of your syslog program for more details.
Send Log	
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.
Log	Select the categories of logs that you want to record. Logs include alerts.
Send Immediate Alert	Select the categories of alerts for which you want the ZyXEL device to instantly e-mail alerts to the e-mail address specified in the **Send Alerts To** field.
Apply	Click **Apply** to save your customized settings and exit this screen.
Reset	Click **Reset** to begin configuring this screen afresh.

13.3 Purge Logs

Click **Purge** to remove logs from the Vantage database. A report of purged logs can be e-mailed and/or downloaded to your computer.

Figure 13-3 Purge Device Logs

The following table describes the labels in this screen.

Table 13-3 Purge Device Logs

LABEL	DESCRIPTION
Send e-mail report to	Select the checkbox and enter valid e-mail address(es) of those who should receive a report on logs that have been purged. Separate more than one email address by a comma.
Export Report	Select this checkbox to send a report on logs that have been purged, to the e-mail addresses defined in notifications.
Apply	Click **Apply** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to begin configuring this screen afresh.

14 Configuration > ADSL Monitor

Use this screen to monitor your ADSL link.

14.1 Introduction

The Prestige is an ADSL device compatible with the ADSL/ADSL2/ADSL2+ standards. Maximum data rates attainable by the Prestige for each standard are shown in the next table.

Table 14-1 ADSL STANDARDS

DATA RATE / STANDARD	UPSTREAM	DOWNSTREAM
ADSL	832 kbps	8Mbps
ADSL2	3.5Mbps	12Mbps
ADSL2+	3.5Mbps	24Mbps

14.2 Configuring ADSL Monitor

Select an ADSL device and click **Configuration > ADSL Monitor**.

Click a label to have the information displayed in the text box.

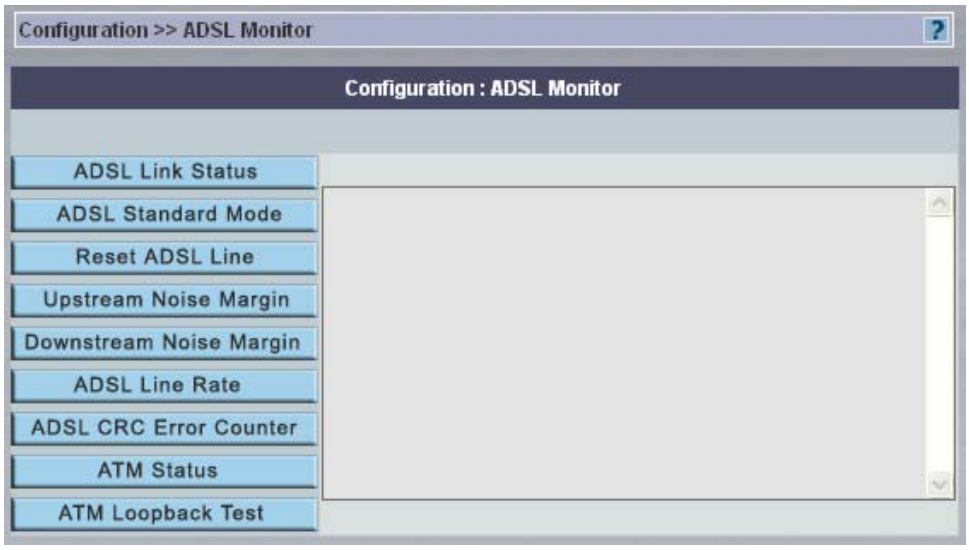


Figure 14-1 Configuration > ADSL Monitor

The following table describes the labels in this screen.

Table 14-2 Configuration > ADSL Monitor

LABEL	DESCRIPTION
ADSL Link Status	This is the status of your ADSL link.
ADSL Standard Mode	This refers to the operational protocol the Prestige and the DSLAM (Digital Subscriber Line Access Multiplexer) are using. **The standard the ISP supports determines the maximum upstream and downstream speeds attainable. Actual speeds attained also depend on the distance from your ISP, noise, line quality, etc.**
Reset ADSL Line	Click this button to reinitialize the ADSL line. The large text box above then displays the progress and results of this operation, for example: "Start to reset ADSL Loading ADSL modem F/W... Reset ADSL Line Successfully!"
Upstream Noise Margin	Click this button to display the upstream noise margin.
Downstream Noise Margin	Click this button to display the downstream noise margin.
ADSL Line Rate	Click this button to display the upstream and downstream rates of your ADSL link.
ADSL CRC Error Counter	Click this computer to have your device perform a Cyclic Redundancy Checksum. The Prestige sends a sequence of bits to every block of data or frame. This is called a frame check sequence (FCS). The receiving computer uses a predetermined number to divide the frame. If there is a remainder, then the frame is considered corrupted and a retransmission is requested.
ATM Status	Click this button to view ATM status.
ATM Loopback Test	Click this button to start the ATM loopback test. Make sure you have configured at least one PVC with proper VPIs/VCIs before you begin this test. The Prestige sends an OAM F5 packet to the DSLAM/ATM switch and then returns it (loops it back) to the Prestige. The ATM loopback test is useful for troubleshooting problems with the DSLAM and ATM network.

15 Configuration > Device Alarms

Use these screens to view and manage device alarms.

15.1 Device Alarms

Select a domain in the object tree to view alarms for that domain.

Alarms are time-critical information that the ZyXEL device automatically sends out at the time of occurrence.

15.1.1 Alarm Classifications

There are four alarm severity classifications.

Table 15-1 Alarm Severity

SEVERITY	DESCRIPTION
All	This displays all alarm severities.
Fatal	This is an alarm such as unrecoverable hardware failure.
Major	This is an alarm such as an attack.
Minor	This is an alarm such as a recoverable hardware error.
Warning	This is an alarm such as an illegal Vantage login attempt.

15.1.2 Alarm States

When an alarm is received by Vantage, it can be in one of three states:

Table 15-2 Alarm States

STATE	DESCRIPTION
Active	This is the initial state of an alarm, which means this alarm is new and no one has assumed responsibility for handling it yet.
Acknowledged	This means that one administrator has decided to respond to the cause of this alarm. Other administrators see that person's name in their alarm screen and so duplicate effort in solving the same problem is avoided.
Cleared	After the administrator has solved the cause of the alarm, he/she can clear the alarm. When an alarm is cleared, it is removed from the current alarm screen and becomes an historical alarm.

15.1.3 Current Alarms Screen

This screen includes filters for time, alarm type, alarm severity type and the administrator who responded to the alarm.

You may also configure to have administrators automatically e-mailed when an alarm occurs in the **System > Preferences >Notifications** screen (see *18.3.4)*. Alarm becomes historical after selecting **Clear**.

Figure 15-1 Configuration > Device Alarms >Current

The following table describes the labels in this screen.

Table 15-3 Configuration > Device Alarms >Current

LABEL	DESCRIPTION
Select Time Period	Select the time period (24, 48 or 72 hours) for which you wish to view logs.
Select Severity of Alarm	Select the severity of the alarm (see above) for which you wish to view logs.
Select Responder	Select **All** or **root** to display all of the administrators or root administrators that have responded to the cause of this alarm. Other administrators see that person's name in their alarm screen and so duplicate effort in solving the same problem is avoided.
Index	This is a number assigned to an alarm record.
Type	The field displays the categories that you select in the **Log Settings** page.
Severity	This field displays the alarm severity. See the alarm classifications above.
Time	This field displays the time the log was recorded.
Status	This field states the reason for the log.
Responder	This field displays the administrator who has responded to the alarm.
Response Time	This field displays the time of response since an administrator first received the alarm.
Description	This field displays a brief explanation of the administrator's response.
Retrieve	Click **Retrieve** to renew the logs displayed for the selected device.
Respond	Click **Respond** to create a response to an alarm.
Clear	Click **Clear** to erase the logs displayed for the selected device. Only the "root" administrator can clear logs.
Report	Click **Report** to generate a report on the logs for the time period selected.

15.1.4 Historical Alarms Screen

This screen displays a history of device alarm logs.

Figure 15-2 Configuration > Device Alarms > Historical

The following table describes the labels in this screen.

Table 15-4 Configuration > Device Alarms > Historical

LABEL	DESCRIPTION
Select Time Period	Select the time period (24, 48 or 72 hours) for which you wish to view logs.
Select Severity of Alarm	Select the severity of the alarm (see above) for which you wish to view logs.
Select Responder	Select **All** or **root** to display all of the administrators or root administrators that have responded to the cause of this alarm. Other administrators see that person's name in their alarm screen and so duplicate effort in solving the same problem is avoided.
Index	This is a number assigned to an alarm record.
Type	The field displays the categories that you select in the **Log Settings** page.
Severity	This field displays the alarm severity. See the alarm classifications above.
Time	This field displays the time the log was recorded.
Status	This field states the reason for the log.
Responder	This field displays the administrator who has responded to the alarm.
Response Time	This field displays the time of response since an administrator first received the alarm.
Description	This field displays a brief explanation of the administrator's response.
Retrieve	Click **Retrieve** for Vantage to pull the selected logs from the selected device.

16 Building Block

16.1 BB Categories

A BB is a building block used to build a device configuration using Vantage CNM.

- A device BB is a combination of configuration BBs, which vary by model. A device can have only one Device BB. You can select any device and save its configuration as a BB ready to be applied to another device (of the same model series). This allows rapid configuration of new devices as you can essentially copy one device's configuration to another.
- Configuration BBs may vary by model. For example, you should not apply a Prestige firewall BB to a ZyWALL.
- A configuration BB is the template of a single configuration menu item, such as **Configuration > General**. You can create a new configuration BB or save an existing configuration item as a BB and it is then available to apply to other devices of the same type.
- A component BB is the template a portion of a configuration menu item, such as IP address, e-mail address, etc.

16.2 BB Properties

You can only view (and use) BBs in your own domain. You cannot view other administrator's BBs, including BBs created by the root administrator. When creating new BBs from old ones use the save as icon ( ) to save as a new BB.

If you modify a BB, changes only affect new device configurations that use this BB and not previous ones.

16.3 Configuring Device BB Menus

You don't have to select a folder or device in the object tree first; click a BB category such as **Building Block > Device BB**.

Figure 16-1 Building Block > Device BB

The following table describes the fields in this screen

Table 16-1 Building Block > Device BB

TYPE	DESCRIPTION
Index	This is the building block list number.

Table 16-1 Building Block > Device BB

TYPE	DESCRIPTION
Name	A building block should have a unique name. Click this hyperlink to go to a BB info screen that allows you to edit the name and add some extra description of the BB.
Type	This field displays the device model, for example, ZyWALL70.
Note	This field displays some extra description of the BB
Add	Click to proceed to the next screen.
Delete	Click to delete a selected device BB.

16.3.1 Editing an Existing BB

Editing an existing does not influence devices already configured with that BB. Click a **Name** hyperlink to go to that Device BB. Change the name and type some extra description of the BB.

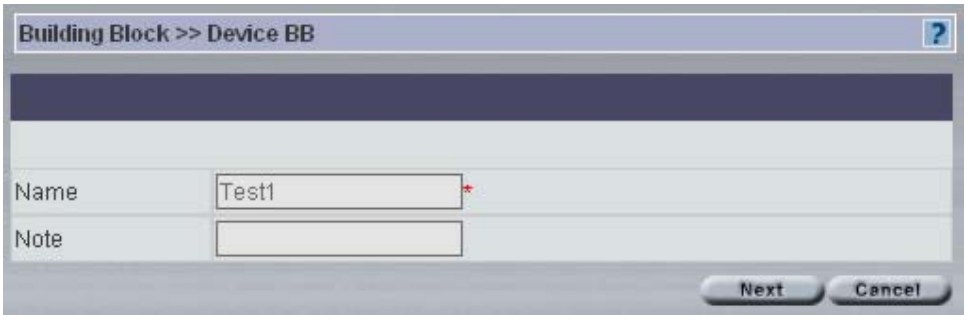


Figure 16-2 Building Block > Device BB > Edit

The following table describes the fields in this screen

Table 16-2 Building Block > Device BB > Edit

TYPE	DESCRIPTION
Name	Type a unique name for the building block.
Note	Type some extra description of the BB
Next	Click to proceed to the following screen
Cancel	Click to return to the previous screen.

16.3.2 Device BB Configuration Select

Select one of the hyperlink configuration menus to configure your BB Device LAN, WLAN etc. Click **Finish** to complete the setup. Click **Cancel** to return to the previous screen.

Figure 16-3 Building Block > Device BB > Edit > Configuration

16.3.3 Adding a New BB

Click **Add** from *Figure 16-1*.The next screen asks you what model type BB you want to add. This should be the same as the model types supported by Vantage.

Figure 16-4 Building Block > Device BB > Add

Table 16-3 Building Block > Device BB > Add

TYPE	DESCRIPTION
Name	Type a unique name for the building block.
Device	Select the device model.
Note	Type some extra description of the BB
Next	Click to proceed to the following screen
Cancel	Click to return to the previous screen.

16.4 Configuration BBs

There are two model series. ZyWALL and Prestige. Each series has its own BB set.

Click **Building Block > Configuration BB**.

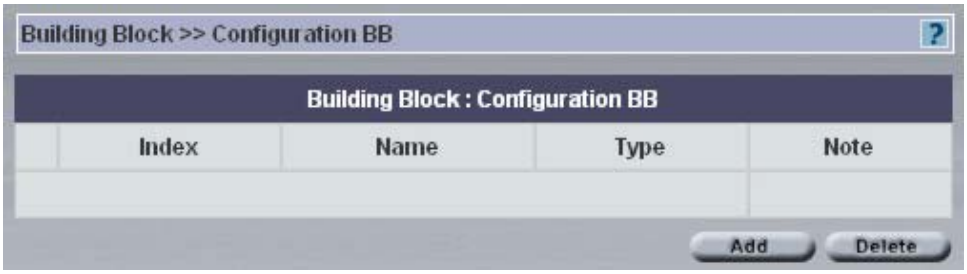


Figure 16-5 Building Block > Configuration

The following table describes the fields in this screen

Table 16-4 Building Block > Configuration

TYPE	DESCRIPTION
Index	This is the building block list number.
Name	A building block should have a unique name. Click this hyperlink to go to a BB info screen that allows you to edit the name and add some extra description of the BB.
Type	This field displays the configuration type, for example, ZyWALL LAN.
Note	This field displays some extra description of the BB
Add	Click to proceed to the next screen.
Delete	Click to delete a selected device BB.

16.4.1 Editing a Configuration BB

Type a **Name** to identify your existing or new **Configuration BB**. When you edit a Configuration BB, you can configure the BB configuration by selecting the hyperlink to the configuration screen.

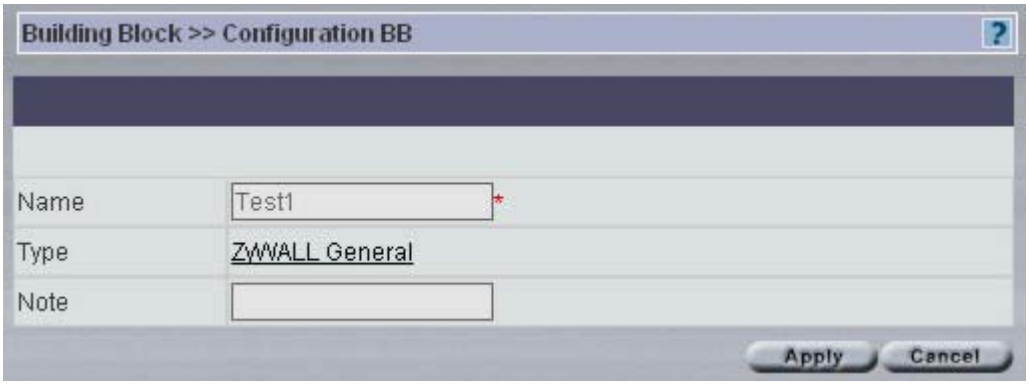


Figure 16-6 Building Block > Configuration BB > Edit

The following table describes the fields in this screen

Table 16-5 Building Block > Configuration BB > Edit

TYPE	DESCRIPTION
Name	Type a unique name for the building block.
Type	Select the configuration hyperlink.

Note	Type some extra description of the BB.
Apply	Click to **Apply** your changes to the BB configuration.
Cancel	Click **Cancel** to return to the previous screen.

16.4.2 Adding a Configuration BB

Click Add from *Figure 16-5*. Type a **Name** to identify your existing or new **Configuration BB**. When you add a new Configuration BB, you must choose what device type and BB configuration type you wish to add, from the **Device** and **Type** list boxes respectively.

Figure 16-7 Building Block > Configuration BB > Add

The following table describes the fields in this screen

Table 16-6 Building Block > Configuration BB > Add

TYPE	DESCRIPTION
Name	Type a unique name for the building block.
Device	Select the model series. The configuration BB's available differ for each series.
Type	Select the configuration. Choices available depend on the model series selected.
Note	Type some extra description of the BB
Next	Click **Next** to create the BB. This BB is then available in the BB pool for this domain.
Cancel	Click **Cancel** to begin configuring the screen afresh.

16.5 Component BBs

Current component BB types are IP address and e-mail address. Click **Building Block > Component BB** to see the following screen.

Figure 16-8 Building Block > Component BB

The following table describes the fields in this screen

Table 16-7 Building Block > Component BB

TYPE	DESCRIPTION
Index	This is the building block list number.
Name	A building block should have a unique name. Click this hyperlink to go to a BB info screen that allows you to edit the name, type and add some extra description of the BB.
Type	This field displays the component type, for example, E-mail.
Note	This field displays some extra description of the BB
Add	Click to proceed to the next screen.
Delete	Click to delete a selected device BB.

To create new component BBs, go to the configuration menus and "save as" from there for the component type selected.

16.5.1 Editing a Component BB

Type a **Name** to identify your existing or new **Component BB**. When you edit a Component BB, you can configure the BB configuration by selecting the hyperlink to the configuration screen.

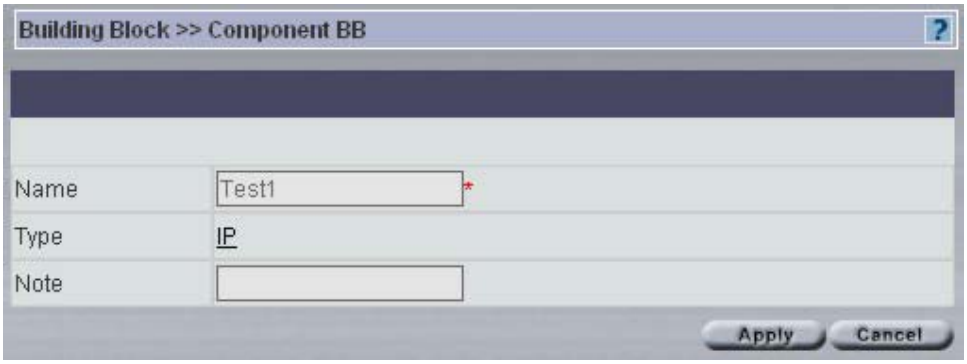


Figure 16-9 Building Block > Component BB > Edit

The following table describes the fields in this screen

Table 16-8 Building Block > Component BB > Edit

TYPE	DESCRIPTION
Name	Type a unique name for the building block.
Type	Select the configuration hyperlink.
Note	Type some extra description of the BB.
Apply	Click to **Apply** your changes to the BB component.
Cancel	Click **Cancel** to return to the previous screen.

16.5.2 Adding a Component BB

Type a **Name** to identify your existing or new **Component BB**. When you add a new Configuration BB, you must choose an IP or E-mail BB info type you wish to add.

Figure 16-10 Building Block > Component BB > Add

The following table describes the fields in this screen

Table 16-9 Building Block > Component > Add

TYPE	DESCRIPTION
Name	Type a unique name for the building block.
Type	Select from **IP** or **E-mail**.
Note	Type some extra description of the BB
Next	Click **Next** to proceed to the next screen.
Cancel	Click **Cancel** to begin configuring the screen afresh.

Adding a Component BB – IP Type

If you select **IP** in the **Type** field in the **BB Info** screen and select **Next,** you will to the next screen, where you must enter your **IP Type, Start** and **End IP/Subnet Mask** details.

Figure 16-11 Building Block > Component BB > Add > IP Address

The following table describes the fields in this screen

Table 16-10 IP Building Block > Component BB > Add > IP Address

TYPE	DESCRIPTION
IP Type	Select from **Single, Range** or **Subnet**.
Start IP	Type the IP address or the first IP address in a range.
End IP/Subnet Mask	Type the last IP address in a range or the subnet mask. See the appendices for information on IP subnetting
Apply	Click **Apply** to create the BB. This BB is then available in the BB pool for this domain.
Reset	Click **Reset** to begin configuring the screen afresh.

Adding a Component BB – E-mail Type

If you select **E-mail** in the **Type** field in the **BB Info** screen and select **Next,** you will to the next screen, where you must enter your **E-Mail Address**.

Figure 16-12 Building Block > Component BB > Add > E-Mail Address

The following table describes the fields in this screen

Table 16-11 Building Block > Component BB > Add > E-Mail Address

TYPE	DESCRIPTION
E-mail Address	Type the e-mail address in standard you@here.xx format.
Apply	Click **Apply** to create the BB. This BB is then available in the BB pool for this domain.
Reset	Click **Reset** to begin configuring the screen afresh.

17 System > Administrators

Use these screens to manage Vantage administrators.

17.1 Introduction to Administrators

An Administrator can only be associated to one management domain. To change an Administrator's management domain, you must first disassociate her from an existing domain before associating to the new domain.

Once an Administrator account has been created, her account name (UID) cannot be changed, but the password can. New administrators must change their password after first login and then regularly at three month intervals. Administrators should periodically change their passwords. The "root" Administrator can enforce periodic Administrator password changes in the **Force Administrator Password Change every 90 Days** in the **System Preferences > User Access** screen.

You can create (and manage) administrators within your domain. You cannot delete an Administrator if that Administrator has "child Administrators" (you will see a warning message). You must first delete the "child Administrators".

17.1.1 Administrator Types

There are four types of administrators, "root", "super", "normal" and "custom". Only "root" can do everything including managing the Vantage system. "Super" and "normal" are predefined administrator profiles that come with a default set of permissions. You can alter "normal" permissions but not "super" permissions in the **System > Preferences** screen. "Custom" administrators have no predefined permissions. Permissions allow for efficient division of labor without the danger of overlap or conflict.

Predefined permissions can only be re-defined by the Administrator who created the Administrator account. When an Administrator is logged in, his permission set, personal details not management domain (disassociate) cannot be changed unless "root" forcibly logs her out first.

"Root" Administrator

The default system name (and password) when you first log in is "root". This is a default system Administrator account, which cannot be deleted by anyone from the system. "root's" details are viewable by others, but not editable.

1. Only one "root" administrator can exist.
2. Only "root" can change her own personal information except for UID (User Identification).
3. Only "root" can see all other Administrators. Other Administrators can only see Administrators within their domain.

"Super" Administrators

"Super" Administrators are Administrators created using the "Super" User Group (see *Figure 18-10*). They are the next most powerful type Administrator next to "root".

1. Super users have all permissions except "System Management". "System Management" is defined as follows:
    - Vantage Upgrade
    - License
    - Preference

- Log option and purge log
- Maintenance

2. "Super" permissions are pre-defined in Vantage and are not editable by Vantage Administrators.

3. A "super" Administrator cannot edit any Vantage system settings, but can view (read only) Vantage system status and Vantage logs (but cannot purge or change log options).

4. "Super" Administrators at same management level can't disassociate each other from that management level.

"Normal" Administrators

These administrators have default permissions enabled as shown on the screen. Some permissions are not allowed. The Administrator who creates the "Normal" Administrator determines which of the enabled permissions to disable. "Normal" Administrators cannot associate nor disassociate other Administrators.

"Custom" Administrators

These administrators have no privileges enabled by default. Some permissions are not allowed. The Administrator who creates the "custom administrator" determines which of the allowable permissions to enable.

17.2 Configuring Administrators

Select a folder in the object pane and then click **System > Administrators** to display a list of all administrators configured for this domain and "root".

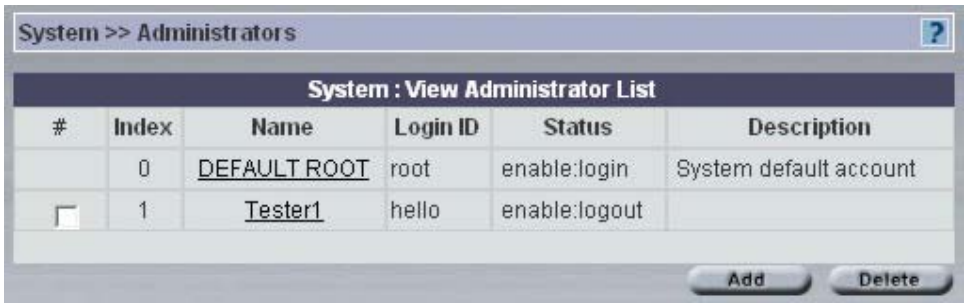


Figure 17-1 System > View Administrator List

The following table describes the fields in this screen.

Table 17-1 System > View Administrator List

LABEL	DESCRIPTION
#	Select the checkbox and enter a valid e-mail address of the person who should receive a report on logs that have been purged.
Index	This is the administrator index number.
Name	This is the administrator name for identification purposes.
Login ID	This is the administrator login name associated with the password that you log into Vantage with. The Login ID is displayed in the object tree when you associate an administrator to a folder. The Login ID cannot be changed after an Administrator account is created but her name can be.
Status	This field displays if this Administrator is currently logged in or not.
Description	This field displays extra information on this Administrator.

Table 17-1 System > View Administrator List

LABEL	DESCRIPTION
Add	Click **Add** to create a new Administrator if you have this permission.
Delete	Select an Administrator(s) and then click **Delete** to erase that Administrator account from Vantage.

17.3 Vantage Upgrade

Upgraded Vantage software may be for bug fixes, increased ZyXEL device support or new Vantage modules. You should perform system maintenance (backup) before upgrading software.

17.3.1 Upgrade Procedure

Click **System > Upgrade** to start the upgrade procedure.

A warning screen appears if there are administrators logged into Vantage. Click **OK** to view the **Online Administrators** screen.

You must request all administrators to log out before you can proceed with upgrading Vantage CNM software.

A list of Vantage administrators that are logged into Vantage is shown.

The administrator details include an administrator **Index** number, **Name** and **Phone** number (if configured).

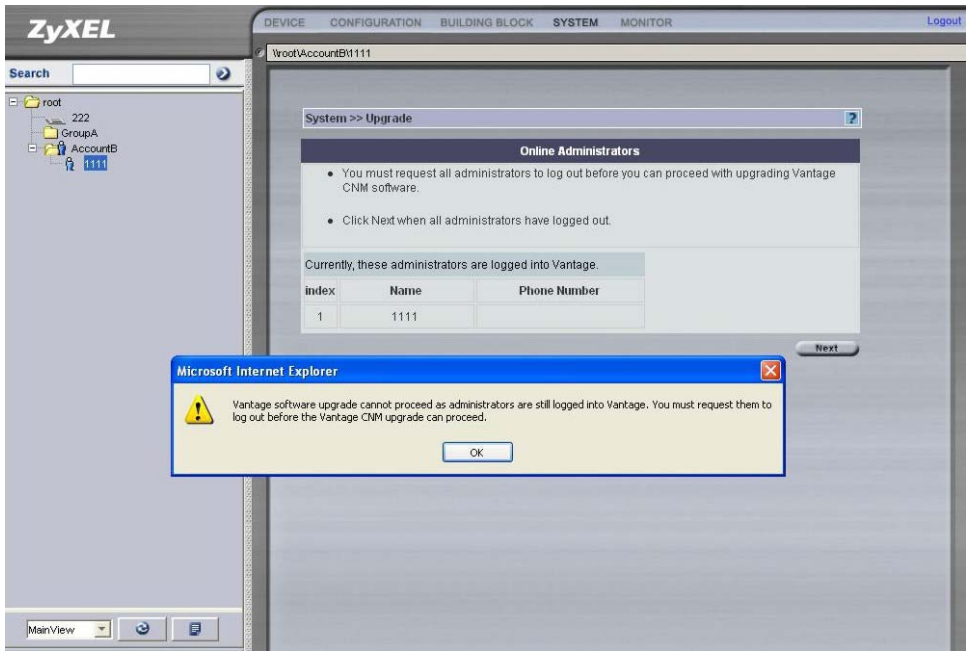


Figure 17-2 System > Upgrade > Online Administrators

Click **Next** when all administrators have logged out.

If an administrator has not logged out, Vantage will not let you continue. A warning screen will re-appear reminding you to notify them to log out.

You should have already downloaded the upgraded Vantage software from the ZyXEL website. The next screen asks you to **Browse** to the location on your computer where you have previously downloaded the software upgrade file. The software upgrade file has a .zip extension. Click **Next** to proceed.

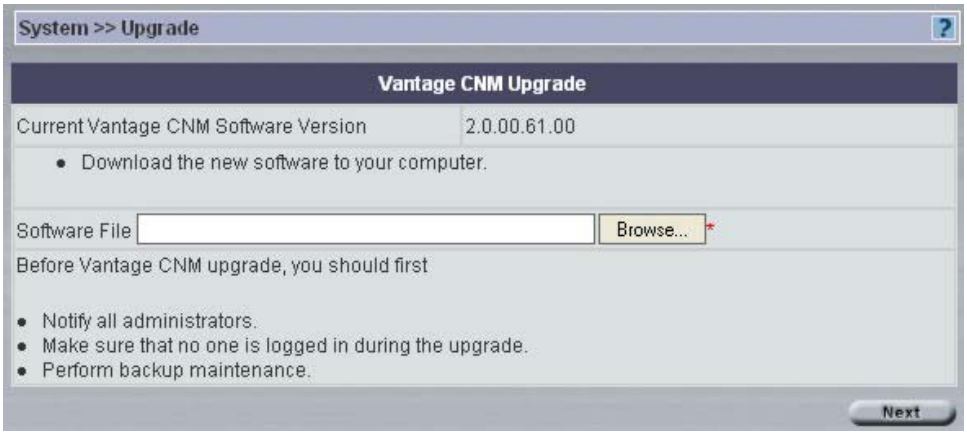


Figure 17-3 System > Upgrade > Vantage Upgrade

The next screen reminds you that Vantage will restart automatically after you start the upgrade and asks you if you are sure you want to continue with the Vantage upgrade now. Click **Yes** to continue.

Figure 17-4 System > Upgrade > Vantage Upgrade > Next

You must wait while Vantage CNM is upgrading.

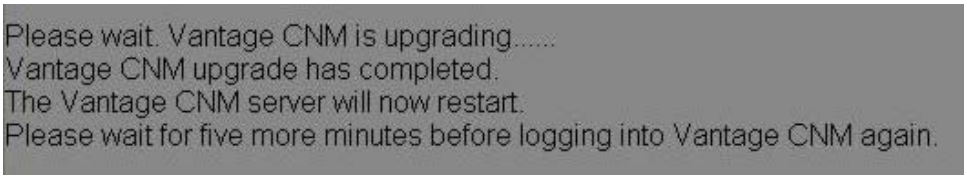


Figure 17-5 System > Upgrading

After you upgrade Vantage CNM software, the Vantage CNM server will restart automatically. Wait for about five more minutes before you log into Vantage again.

17.3.2 Version Format

Vantage CNM software version format is as follows:

A.B.CD.EF.GH

The following table details the format of this version code.

The version code of the Vantage CNM 2.0 for Windows XP SP1 without a patch is **2.0.00.61.00**.

Table 17-2 Version A.B.CD.EF.GH	
CODE	**DESCRIPTION**
A	This represents a major upgrade such as major new features or upgrade modules.
B	This represents a non-major upgrade such as new features and increased ZyXEL device support..
CD	This is the project code number.
EF	This represents the code for the operating system on which you can install this version of Vantage.
GH	This number changes for patch upgrades.

17.4 Creating an Administrator Account

Click **Add** to create a new Administrator account or select and existing Administrator account to edit it.

17.4.1 Administrator Details

Only “root” may create or edit her administrator details and create other administrators at the same (root) level. Other administrators can only create administrators for a level below them.

Figure 17-6 System > Administrator Details

The following table describes the fields in this screen.

Table 17-3 System > Administrator Details

LABEL	DESCRIPTION
Name	Type the administrator name used for identification purposes.
Login ID	Type the administrator login name associated with the password that you log into Vantage with. The Login ID is displayed in the object tree when you associate an administrator to a folder. The Login ID cannot be changed after an Administrator account is created but her name can be.
Password	Type a password associated with the Login ID above.
Password Retype	Type the same password again here to make sure that the one you typed above was typed as intended.
E-mail Address	Type a valid e-mail address for this Administrator.
Contact Address	Type a mailing address for this Administrator.
Telephone Number	Type the complete telephone number including area codes for this Administrator.
Note	Type some extra information about this Administrator here.
Apply	Click **Apply** to save your settings in Vantage.
Cancel	Click **Cancel** to go back to the previous screen without saving any changes.

17.4.2 Administrator Permissions

You may select which permissions (privileges) an administrator may have from the next screen. See *section 17.1* for more information.

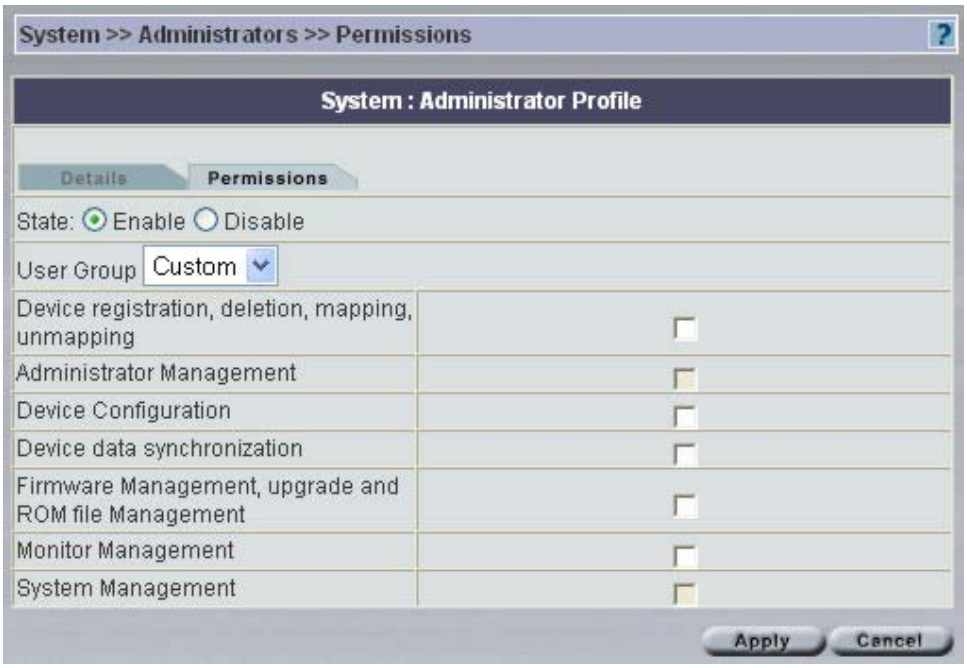


Figure 17-7 System > Administrator Permissions

The following table describes the fields in this screen.

Table 17-4 System > Administrator Permissions

LABEL	DESCRIPTION
State	Select **Disable** to prohibit Administrator access to Vantage without deleting her profile.
User Group	A “user group” is a pre-defined Administrator permission set. Select from **Custom**, **Super** and **Normal**. **Super** and **Normal** “user groups” permission sets are not editable, **Custom** “user group” permissions are editable. See *section 17.1* for more information. You may select the following permissions for **Custom**.
Device registration, deletion, mapping, unmapping	This permission allows the Administrator to register and delete devices as well as associate and disassociate devices to a folder.
Administrator Management	This permission allows the Administrator to create, edit and delete Administrators as well as associate and disassociate Administrators to a folder.
Device Configuration	This permission allows the Administrator access to all the **System > Configuration** screens.
Device data synchronization	This permission allows the Administrator access to the Device > Synchronize screen. See that screen information in this User’s Guide for more details.
Firmware Management, upgrade and ROM file Management	This permission allows the Administrator to upload device firmware and configuration files to Vantage, download device firmware and configuration files as well as remove them from Vantage.
Monitor Management	This permission allows the Administrator access to the Monitor screens.
System Management	System Management is defined as follows: ➢ Vantage Upgrade ➢ License ➢ Preference ➢ Log option and purge log ➢ Maintenance
Apply	Click **Apply** to save your settings in Vantage.
Cancel	Click **Cancel** to begin configuring the screen afresh.

18 Other System Screens

Only the root administrator can view the **System > Upgrade** to **System > Data Maintenance** screens as only the root administrator can perform these duties.

18.1 Status

Click **System > Status** to view the current Vantage system status. This is a read-only screen.

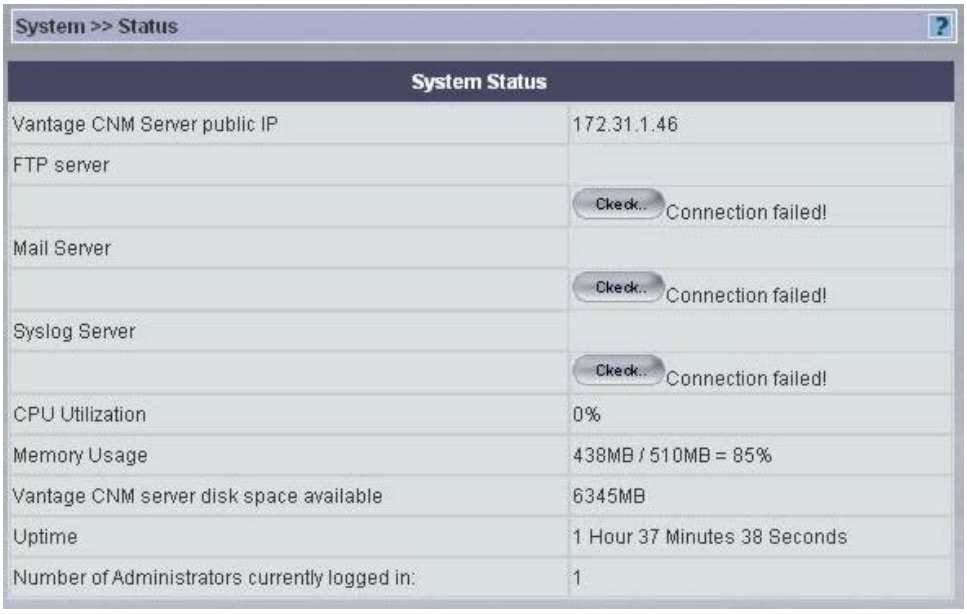


Figure 18-1 System > Vantage Status

The following table describes the fields in this screen.

Table 18-1 System > Vantage Status

LABEL	DESCRIPTION
Vantage CNM Server public IP	This field displays the IP address of the communications server. If the COM server is on the same computer as Vantage, then this address is the same IP address as that of the Vantage server computer.
FTP server	This field displays the IP address of the FTP server. Click the **Check** button to test if the connection to the server is up.
Mail Server	This field displays the IP address of the Mail Server. Click the **Check** button to test if the connection to the server is up.
Syslog Server	This field displays the IP address of the Syslog Server. Click the **Check** button to test if the connection to the server is up.
CPU Utilization	This field displays the Vantage server CPU processing power usage. Heavy usage may necessitate upgrading to a more powerful CPU.
Memory Usage	This field displays the Vantage server memory usage. Heavy usage may necessitate installing more RAM.

Table 18-1 System > Vantage Status

LABEL	DESCRIPTION
Vantage server disk space available	This field displays the Vantage server hard drive free space. Heavy usage may necessitate buying another hard drive or purging old logs and alerts.
Uptime	This field displays how long Vantage has been on since the last start up.
Number of Administrators currently logged in	This field displays the number of Administrators currently logged into Vantage.

18.2 License Management

You need a license key to generate an **Activation Key** and **Server Set Key** (at www.myZyZEL.com) in order to be able to use Vantage. See the *Quick Start Guide* for more information on generating keys at www.myZyXEL.com.

You get an initial license key when you first buy Vantage and after that you may buy expansion license keys in order to be able to manage more ZyXEL devices with Vantage.

Click **Vantage > License** to display the next screen.

Figure 18-2 System > License > License Management

The following table describes the fields in this screen.

Table 18-2 System > License > License Management

LABEL	DESCRIPTION
Number of devices allowed with this license	This field displays the number of devices you are allowed to manage with this license. If you want to manage more devices, you need to purchase another license.
Current number of devices being managed	This field displays the number of devices currently registered with Vantage.
Activation Key	This key is generated in the myZyXEL.com website from the **Authentication Code**.
Authentication Code	This read-only field displays an automatically generated code after you have installed Vantage. Use this key to obtain an **Activation Key** and a **Service Set Key** from the myZyXEL.com website.
Service Set Key	This key is generated in the myZyXEL.com website. It identifies the set of licenses activated on a product.

Table 18-2 System > License > License Management

LABEL	DESCRIPTION
Upgrade	Click **Upgrade** to proceed to the next screen.
Reset	Click **Reset** to begin configuring the screen afresh.

18.2.1 License Upgrade

Click **Upgrade** in *Table 18-2* to display this screen.

Figure 18-3 System > License > License Management > Upgrade

The following table describes the fields in this screen.

Table 18-3 System > License > License Management > Upgrade

LABEL	DESCRIPTION
Activation Key	Copy and paste or type the **Activation Key** that is generated in the myZyXEL.com website.
Service Set Key	Copy and paste or type the **Service Set Key** that is generated in the myZyXEL.com website.
Apply	Click **Apply** to begin the license upgrade process. Vantage must have an Internet connection.
Cancel	Click **Cancel** to return to the previous screen.

18.3 System >Preferences

System preferences are global Vantage server settings.

Vantage Server Public IP Address

If you change the Vantage server public IP Address, then each (Vantage-registered) device's Manager IP address must change too.

Step 1. Go to the **System>Preferences>Server** screen.

Step 2. Enter the new IP address in the **Vantage CNM Public IP** field and **Apply**.

Step 3. To change all registered devices' Manager IP address to the new IP address, you must do *one* of the following:

- Manually restart each device and wait about 5 minutes until the device registers with Vantage.
- Access each device's command line interface and enter "CNM managerIp x.x.x.x" where "x.x.x.x" is the new Vantage CNM public IP address.

Step 4. Restart Vantage CNM; you don't have to restart the computer on which Vantage CNM is installed. Right-click the Vantage icon in the system tray and select **STOP**.

Figure 18-4 Vantage Icon - Stop

Right-click the icon again and select **START**.

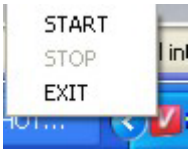


Figure 18-5 Vantage Icon - Start

Step 5. When you register new devices with Vantage, make sure the new device can ping the Vantage server (the new **Vantage CNM Public IP** address) and then set the device's Manager IP address correspondingly.

18.3.1 Servers

You can configure these servers as you install Vantage (in the installation wizard) or after you install it in this screen.

Configure the Vantage CNM public IP server address, FTP server (for firmware upload), syslog server (for logs) and mail server (for Vantage notifications and reports) in this screen. These IP addresses will be the same as the Vantage server computer if they are all on the same computer.

The FTP server is used for file transfers, such as firmware upgrade.

The SMTP server is used for e-mail notifications.

The syslog server is used to receive logs. The syslog server you configure for a device and the syslog server you configure for Vantage MUST be the same.

You should know each server's IP address, username and password. File transfers (FTP), e-mail notifications (SMTP) or log reports (syslog) will not work in Vantage if these are incorrectly configured.

See the *User's Guide appendices* for examples of setting up syslog and FTP servers. The syslog server must be either a Linux syslog server or Kiwi for Windows[2]. Vantage communicates with a Linux syslog server using SSH, so you must enable the SSH daemon on the Linux syslog server. Vantage communicates with a Windows (Kiwi) syslog server using Telnet, so you must enable Telnet on the Windows (Kiwi) syslog server. See the *Quick Start Guide* for information on configuring the Linux syslog server to send logs to Vantage.

[2] Only these syslog servers are supported at the time of writing.

Figure 18-6 System > Preferences > Server

The following table describes the fields in this screen.

Table 18-4 System > Preferences > Server

LABEL	DESCRIPTION
Vantage CNM server public IP	Select the check box to make the IP address editable.
IP Address	Type the IP address of the communications server.
FTP Server	The FTP server is used for file uploads to and from Vantage. Select the checkbox to activate the fields below.
IP Address	Type the IP address of the FTP server here.
User Name	Type your login name to this FTP server.
Password	Type the FTP server password associated with the login name.
Syslog Server	The FTP server is used for Vantage logs. Select the checkbox to activate the fields below.
IP Address	Type the IP address of the syslog server here.
User Name	Type your login name to this syslog server.
Password	Type the syslog server password associated with the login name.
Syslog Server OS	Choose Linux if your syslog server is Linux-based and choose Windows if your syslog server is Windows-based.

Table 18-4 System > Preferences > Server

LABEL	DESCRIPTION
System Log Path	This displays the file path of your syslog server.
Mail Server	The mail (SMTP) server is used to send Vantage notifications. Select the checkbox to activate the fields below.
IP Address	Type the IP address of the mail server here.
User Name	Type your login name to this mail server.
Password	Type the mail server password associated with the login name.
Apply	Click **Apply** to save your settings in Vantage.
Reset	Click **Reset** to begin configuring the screen afresh.

18.3.2 User Access

A "User" is an administrator. Set the maximum number of administrators allowed to log into Vantage at one time, Vantage idle timeout (so one administrator does not unwittingly hog resources by not logging out) and a brute force password protection mechanism in this screen.

Brute-Force Password Guessing Protection is a protection mechanism to discourage brute-force password guessing attacks on a device's management interface. You can specify a wait-time that must expire before entering a fourth password after three incorrect passwords have been entered.

You can also force all administrators to periodically change their passwords in this screen.

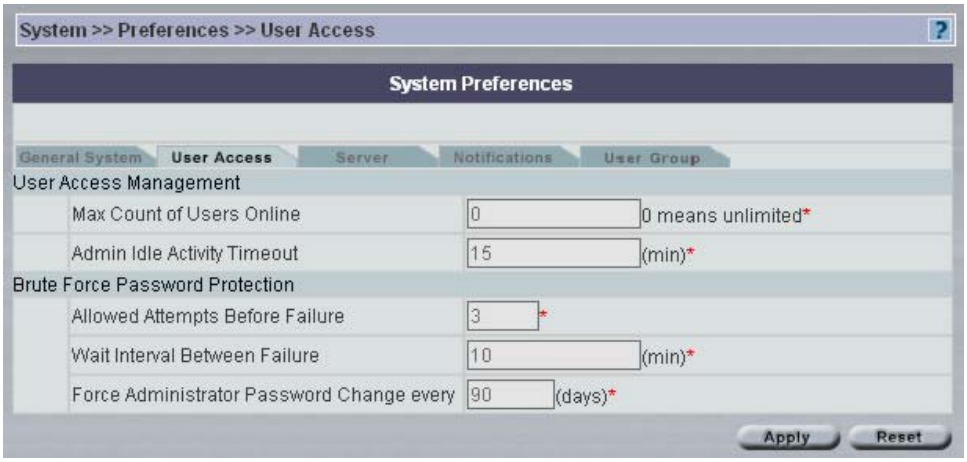


Figure 18-7 System > Preferences > User Access

The following table describes the fields in this screen.

Table 18-5 System > Preferences > User Access

LABEL	DESCRIPTION
Max Count of Users Online	Type the maximum number of administrators allowed to log into Vantage at any one time.
Admin Idle Activity Timeout	Type the length of time an Administrator can leave the Vantage web configurator idle before he is automatically logged out.

Table 18-5 System > Preferences > User Access

LABEL	DESCRIPTION
Brute Force Password Protection	Configure the next two fields to apply this.
Allowed Attempts Before Failure	Type the number of times an incorrect password may be entered before a login failure is returned.
Wait Interval Between Failure	Type the wait time before allowing another login in after a login failure is returned.
Force Administrator Password Change every	Type how often all Administrators must change their Vantage login passwords. If an Administrator does not change her password within this time, then the old password expires.
Apply	Click **Apply** to save your settings in Vantage.
Reset	Click **Reset** to begin configuring the screen afresh.

18.3.3 General Vantage Preferences

See *section 17.1.1* for more information on the root administrator. This is a read only screen.

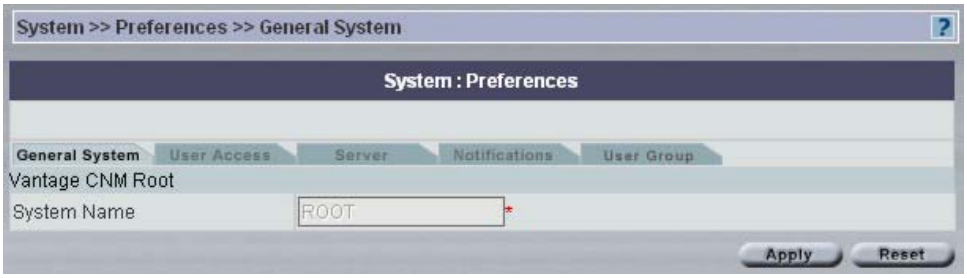


Figure 18-8 System > Preferences > General System

The following table describes the fields in this screen.

Table 18-6 System > Preferences > General System

LABEL	DESCRIPTION
Vantage CNM Root	This refers to the root of the object tree.
System Name	The root of the object tree is called “root” by default.
Apply	You cannot edit this screen.
Reset	You cannot edit this screen.

18.3.4 Notifications

Use this screen to decide who should receive e-mails for events that may warrant immediate attention such as firmware upgrade or device logs and/or alarms. **Device Owner** is a variable that refers to the e-mail address of the device owner (configured in **Configuration > General > Owner Info** screen).

Use e-mail component BBs (building block) to rapidly configure both existing and new system notification entries.

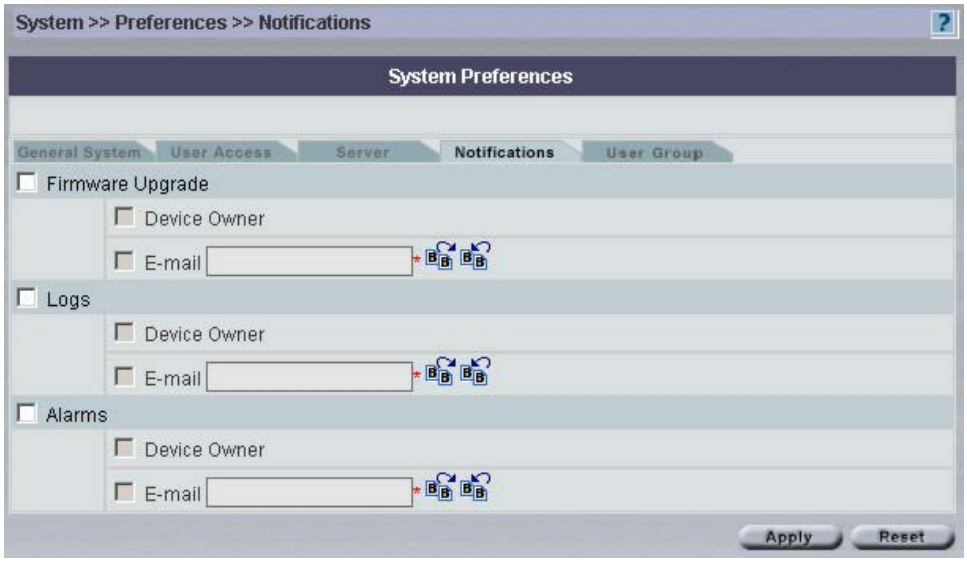


Figure 18-9 System > Preferences > Notifications

The following table describes the fields in this screen.

Table 18-7 System > Preferences > Notifications

LABEL	DESCRIPTION
Firmware Upgrade	Set who should be notified when you upload firmware to a device.
Device Owner	Select to have an e-mail automatically sent to the selected device owner e-mail address (configured in **Configuration > General > Owner Info**).
E-mail	Select a BB or enter multiple e-mail addresses separated by commas.
Logs	Set who should receive e-mailed logs.
Device Owner	Select to have an e-mail automatically sent to the selected device owner e-mail address (configured in **Configuration > General > Owner Info**).
E-mail	Select a BB or enter multiple e-mail addresses separated by commas.
Alarms	Set who should receive e-mailed alarms.
Device Owner	Select to have an e-mail automatically sent to the selected device owner e-mail address (configured in **Configuration > General > Owner Info**).
E-mail	Select a BB or enter multiple e-mail addresses separated by commas.
Apply	Click **Apply** to save your settings in Vantage.
Reset	Click **Reset** to begin configuring the screen afresh.

18.3.5 Vantage Permissions

"Root" may choose what default permissions are associated with the **Normal** permissions template here. "Root" can also create and delete new permission templates here.

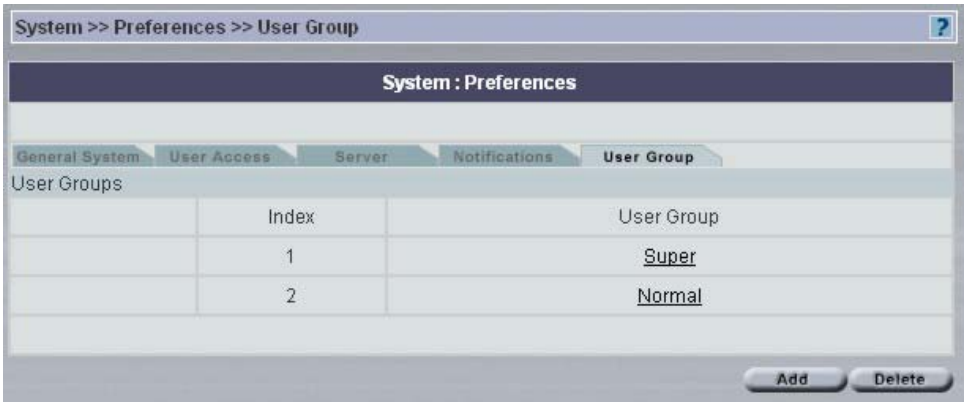


Figure 18-10 System > Preferences > Permissions

The following table describes the fields in this screen.

Table 18-8 System > Preferences > Permissions

LABEL	DESCRIPTION
Index	This is the template index number. 1 and 2 are default templates.
User Group	This field displays the template name (**User Group**).
Add	Click **Add** to create a new template.
Delete	Click **Delete** to remove a newly created template.

18.3.6 Add Permission Template

Create a new administrator permission template by clicking **Add** in the previous screen to display the next one as shown.

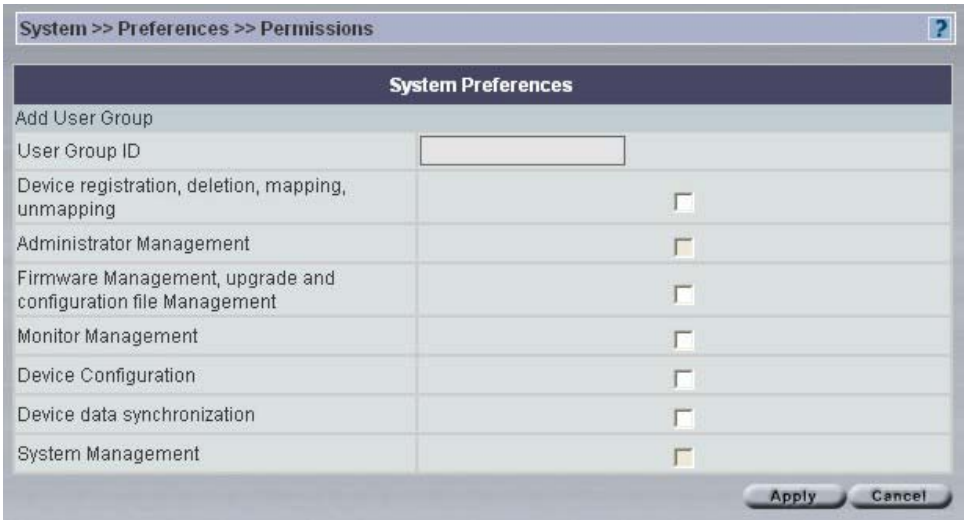


Figure 18-11 System > Preferences > Permissions > Add

The following table describes the fields in this screen.

Table 18-9 System > Preferences > Permissions > Add

LABEL	DESCRIPTION
Add User Group	
User Group ID	Enter the new template name (**User Group**) in this field.
Device registration, deletion, mapping, unmapping	This field allows the Administrator to register and delete devices as well as associate and disassociate devices to a folder.
Firmware Management, upgrade and configuration file Management	This field allows the Administrator to upload device firmware and configuration files to Vantage, download device firmware and configuration files as well as remove them from Vantage.
Monitor Management	This field allows the Administrator access to the Monitor screens.
Device Configuration	This field allows the Administrator access to all the **System > Configuration** screens.
Device data synchronization	This field allows the Administrator access to the Device > Synchronize screen. See that screen information in this User's Guide for more details.
System Management	System Management is defined as follows: ➢ Vantage Upgrade ➢ License ➢ Preference ➢ Log option and purge log ➢ Maintenance
Apply	Click **Apply** to save your settings in Vantage.
Cancel	Click **Cancel** to begin configuring the screen afresh.

18.4 System Maintenance

Use the **Maintenance** screens to manage, back up and restore Vantage system backup files. Data maintenance includes device firmware and configuration files you have uploaded to the Vantage server. You can back up or restore to your computer or Vantage. You can choose what domain to back up by selecting a folder in the object tree.

18.4.1 System Maintenance Management

Use this screen to delete previous (old) system backups.

Figure 18-12 System > Maintenance > Management

The following table describes the fields in this screen.

Table 18-10 System > Maintenance > Management

LABEL	DESCRIPTION
Index	This field displays the system backup file index number.
Name	This field displays the system backup file name.
Description	This field displays some extra description of the system backup file.
Backed Up Date	This field displays the date the system backup file was created.
Administrator	This field displays who created the system backup file.
Delete	Select a system backup file and then click **Delete** to remove it from Vantage.

18.4.2 Back Up System Maintenance

Use this screen to save your current Vantage system to the Vantage server or your computer. You can enter extra information on the file in the **Description** text box.

Backup configuration allows you to back up (save) the current configuration to a file on your computer. Once your 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. You should perform system backup before you upgrade Vantage software.

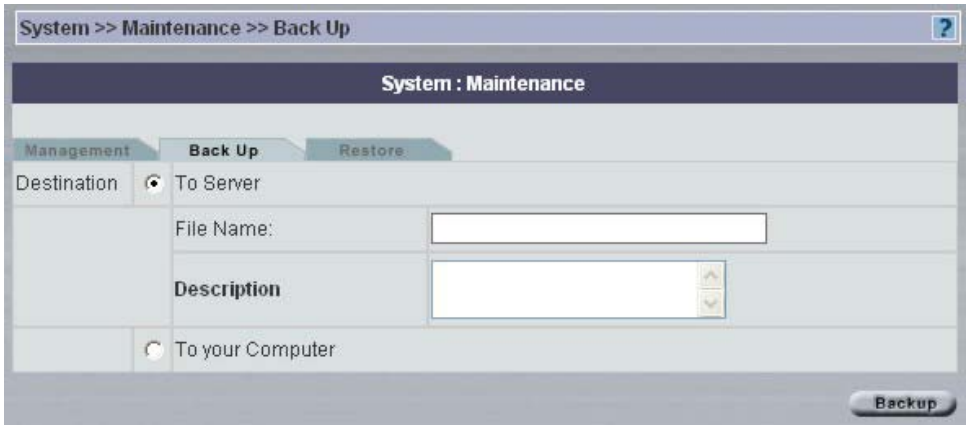


Figure 18-13 System > Maintenance > Backup

The following table describes the fields in this screen.

Table 18-11 System > Maintenance > Backup

LABEL	DESCRIPTION
Destination	Select the radio button to give the download destination to server.
To Server	Select this option to back up the file to the Vantage CNM server.
File Name	Type in the location of the file you want to upload in this field.
Description	Type a description of the file backup.
To your Computer	Select the radio button to give the download destination to your computer.
Backup	Click this button to perform the file backup.

18.4.3 Restore System Maintenance

Use this screen to restore a previously saved system backup (from your computer or Vantage) to Vantage.

Figure 18-14 System > Maintenance > Restore

The following table describes the fields in this screen.

Table 18-12 System > Maintenance > Restore

LABEL	DESCRIPTION
Destination	Select this radio button to upload a configuration file **From Server**.
From Server	Select this option to restore the file from the Vantage CNM server.
File Name	Select a file from the drop-down list box.
From Your Computer	Select this radio button to upload a configuration file From **Your Computer**.
File Name	Type in the location of the file you want to upload in this field or click **Browse** ... to find it.
Restore	Click **Restore** to begin the upload process.

18.5 Address Book

An address book is a list of personal details of people such as device owners and administrators. Click **System > Address Book** to display the next screen.

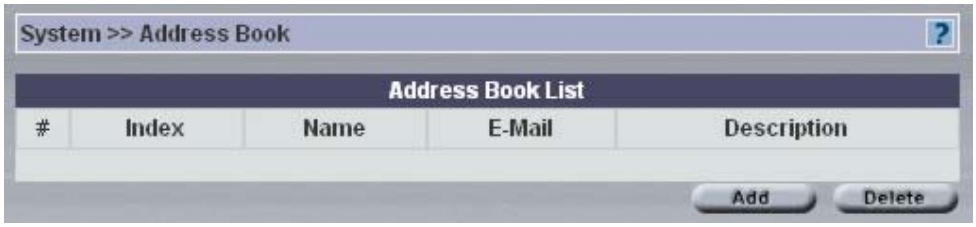


Figure 18-15 System > Address Book

The following table describes the labels in this screen.

Table 18-13 System > Address Book

LABEL	DESCRIPTION
#	This is a number defining an address book entry.
Index	This field displays the address book entry index number.
Name	This field displays the person's name.
Email	This field displays the person's e-mail address.
Description	This field displays some extra information about the person.
Add	Click **Add** to create a new customer record.
Delete	Select a system backup file and then click **Delete** to remove it from Vantage.

18.5.1 Address Book Add/Edit

From *Figure 18-15* click **Add** to create a new entry or click an existing entry hyperlink to edit it.

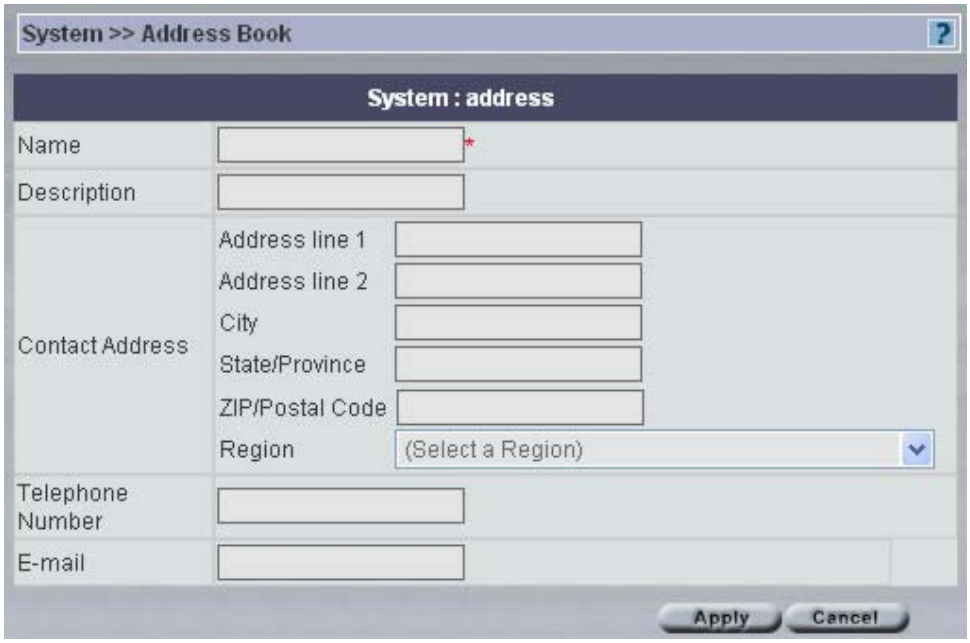


Figure 18-16 System > Address Book Add/Edit

The following table describes the labels in this screen.

Table 18-14 System > Address Book Add/Edit

LABEL	DESCRIPTION
Name	Type the person's name.
Description	Type some extra information about the person.
Contact Address	Type a mailing address for this person.
Telephone Number	Type the complete telephone number including area codes for this person.
E-mail	Type the person's e-mail address.
Apply	Click **Apply** to create a new address book record.

Table 18-14 System > Address Book Add/Edit

LABEL	DESCRIPTION
Cancel	Click **Cancel** to return to the previous screen.

18.6 Certificate Mgmt

18.6.1 Certificates Overview – ZyXEL device

The ZyXEL device can use certificates (also called digital IDs) to authenticate users. Certificates are based on public-private key pairs. A certificate contains the certificate owner's identity and public key. Certificates provide a way to exchange public keys for use in authentication.

A Certification Authority (CA) issues certificates and guarantees the identity of each certificate owner. There are commercial certification authorities like CyberTrust or VeriSign and government certification authorities. You can use the ZyXEL device to generate certification requests that contain identifying information and public keys and then send the certification requests to a certification authority.

In public-key encryption and decryption, each host has two keys. One key is public and can be made openly available; the other key is private and must be kept secure. Public-key encryption in general works as follows.

1. Tim wants to send a private message to Jenny. Tim generates a public key pair. What is encrypted with one key can only be decrypted using the other.
2. Tim keeps the private key and makes the public key openly available.
3. Tim uses his private key to encrypt the message and sends it to Jenny.
4. Jenny receives the message and uses Tim's public key to decrypt it.
5. Additionally, Jenny uses her own private key to encrypt a message and Tim uses Jenny's public key to decrypt the message.

The ZyXEL device uses certificates based on public-key cryptology to authenticate users attempting to establish a connection, not to encrypt the data that you send after establishing a connection. The method used to secure the data that you send through an established connection depends on the type of connection. For example, a VPN tunnel might use the triple DES encryption algorithm.

The certification authority uses its private key to sign certificates. Anyone can then use the certification authority's public key to verify the certificates.

A certification path is the hierarchy of certification authority certificates that validate a certificate. The ZyXEL device does not trust a certificate if any certificate on its path has expired or been revoked.

Certification authorities maintain directory servers with databases of valid and revoked certificates. A directory of certificates that have been revoked before the scheduled expiration is called a CRL (Certificate Revocation List). The ZyXEL device can check a peer's certificate against a directory server's list of revoked certificates. The framework of servers, software, procedures and policies that handles keys is called PKI (public-key infrastructure).

18.6.2 Advantages of Certificates

Certificates offer the following benefits.

The ZyXEL device only has to store the certificates of the certification authorities that you decide to trust, no matter how many devices you need to authenticate.

Key distribution is simple and very secure since you can freely distribute public keys and you never need to transmit private keys.

18.6.3 Current Certification Information

You can view your current certificate information in the following screen, including certificate name, type, origin and duration of validity.

Figure 18-17 System > Certificate Management > Information

The following table describes the labels in this screen.

Table 18-15 System > Certificate Management > Information

LABEL	DESCRIPTION
Current Certificate Information	
Certificate Name	This field displays the name used to identify this certificate. It is recommended that you give each certificate a unique name.
Certificate Type	This field displays what kind of certificate this is. **REQ** represents a certification request and is not yet a valid certificate. Send a certification request to a certification authority, which then issues a certificate. Use the **My Certificate** Import screen to import the certificate and replace the request. **SELF** represents a self-signed certificate. ***SELF** represents the default self-signed certificate, which the ZyXEL device uses to sign imported trusted remote host certificates. **CERT** represents a certificate issued by a certification authority.
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.

Table 18-15 System > Certificate Management > Information

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.
Create CSR	Click **Create CSR** to go create a certificate.
Import Certificate	Click **Import Certificate** to go to the Import Certificate screen.

18.6.4 Create a Certificate

You can create certificates by entering the requested information into the fields below. Then click **Apply**.

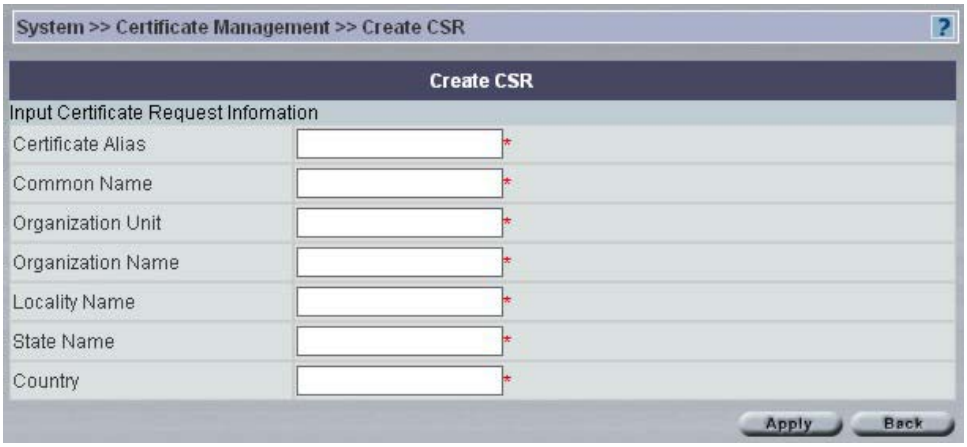


Figure 18-18 System > Certificate Management > Create CSR

The following table describes the labels in this screen.

Table 18-16 System > Certificate Management > Create CSR

LABEL	DESCRIPTION
Input Certificate Request Information	
Certificate Alias	Type a name to identify the certificate.
Common Name	Type a name to identify the certificates owner.
Organization Unit	Type the organization unit or department in this field.
Organization Name	Type the organization name or company in this field.
Locality Name	Type your company location; number, street etc.
State Name	Type the **State** or county where your company is located.
Country	Type the **Country** where your company is located.
Apply	Click **Apply** to save these changes.
Back	Click **Back** to return to the previous screen.

18.6.5 Importing Certificates

In the following screen, you can **Browse** for a certificate that has already been downloaded to your computer. Select **Apply** to complete the certificate import.

Figure 18-19 System > Certificate Management > Import Certificate

The following table describes the labels in this screen.

Table 18-17 System > Certificate Management > Import Certificate

LABEL	DESCRIPTION
Input Certificate	
Input Your Certificate Path	Type in the location of the certificate you want to upload in this field or click **Browse** ... to find it.
Apply	Click **Apply** to save these changes.
Back	Click **Back** to return to the previous screen.

18.7 Vantage Logs

Use these screens to view and configure Vantage system log preferences.

18.7.1 CNM Server

You can view system logs for previous day, the last two days or up to one week here.

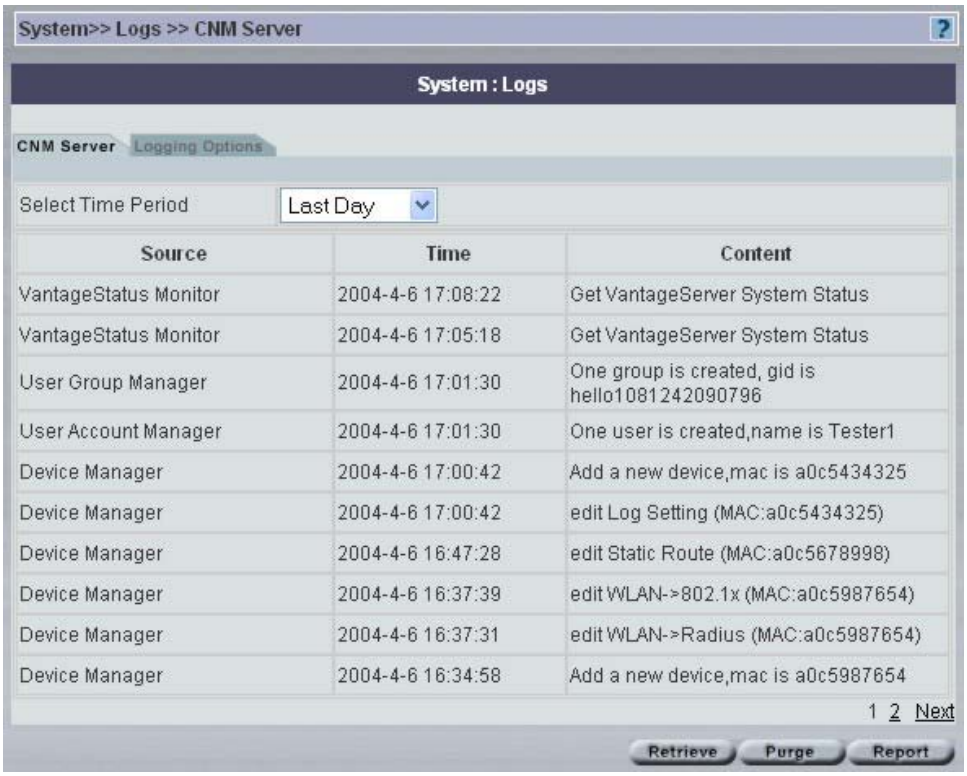


Figure 18-20 System > Logs > CNM Server

The following table describes the labels in this screen.

Table 18-18 System > Logs > CNM Server

LABEL	DESCRIPTION
Select Time Period	Select the time period for which you wish to view Vantage logs
Source	This field displays the source of the Vantage log.
Time	This field displays the date the Vantage log occurred.
Content	This field displays a message describing for the log.
Retrieve	Click **Retrieve** for Vantage to pull the logs from the selected device.
Purge	Select **Purge** to delete system logs from the Vantage server.
Report	Click **Report** to generate a report on the logs for the time period selected.

18.7.2 Vantage Logging Options

Select what type of system logs you wish to log as shown in the following screen.

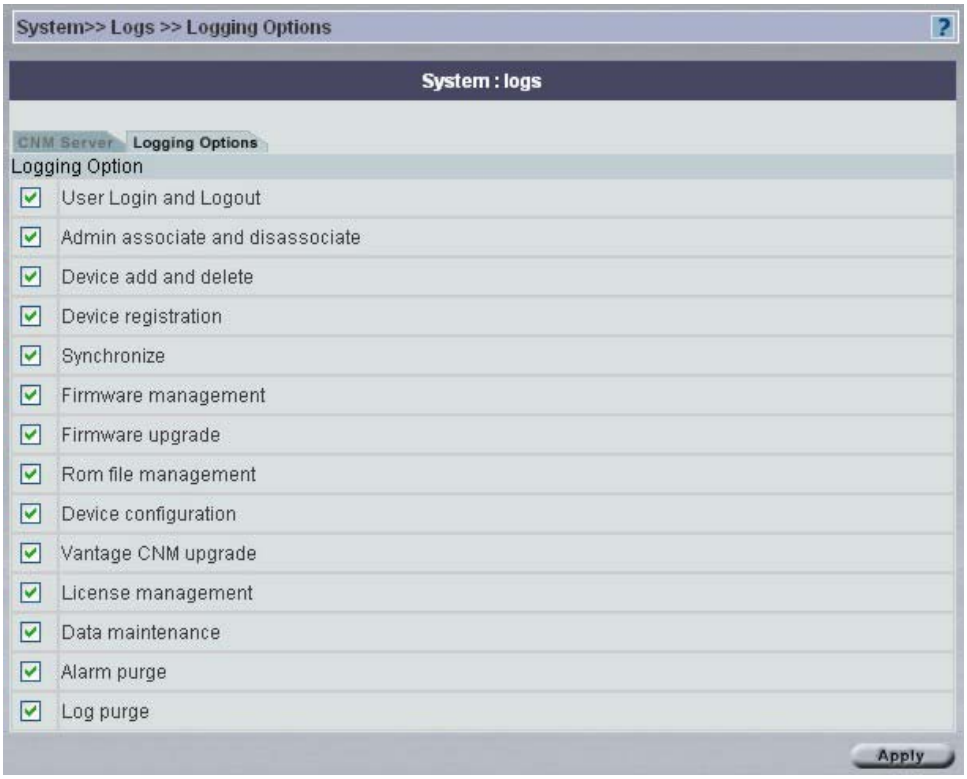


Figure 18-21 System > Logging Options

18.8 About Vantage

The **About** screen provides some basic information about Vantage as shown in the following screen.

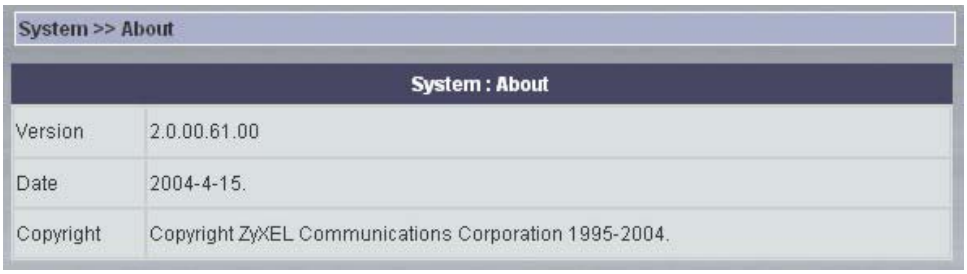


Figure 18-22 System > About Vantage

19 Monitor > Alarms

This chapter describes the monitor alarms.

19.1 Alarms

Select a domain in the object tree to view alarms for that domain.

Alarms are time-critical information that the ZyXEL device automatically sends out at the time of occurrence.

19.1.1 Alarm Types

There are three types of alarms.

Table 19-1 Types of Alarms

TYPE	DESCRIPTION
All	This displays all types of alarms.
Device	This is an alarm such as hardware failure or the network connection is down.
CNM	This is an alarm such as server communication error or illegal Vantage login attempt.

19.1.2 Alarm Classifications

There are four alarm severity classifications.

Table 19-2 Alarm Severity

SEVERITY	DESCRIPTION
All	This displays all alarm severities.
Fatal	This is an alarm such as unrecoverable hardware failure.
Major	This is an alarm such as an attack.
Minor	This is an alarm such as a recoverable hardware error.
Warning	This is an alarm such as an illegal Vantage login attempt.

19.1.3 Alarm States

When an alarm is received by Vantage, it can be in one of three states:

Table 19-3 Alarm States

STATE	DESCRIPTION
Active	This is the initial state of an alarm, which means this alarm is new and no one has assumed responsibility for handling it yet.
Acknowledged	This means that one administrator has decided to respond to the cause of this alarm. Other administrators see that person's name in their alarm screen and so duplicate effort in solving the same problem is avoided.

Table 19-3 Alarm States

STATE	DESCRIPTION
Cleared	After the administrator has solved the cause of the alarm, he/she can clear the alarm. When an alarm is cleared, it is removed from the current alarm screen and becomes an historical alarm.

19.1.4 Current Alarms Screen

View recent alarms and who has taken care of or is taking care of them in this screen.

You may also configure to have administrators automatically e-mailed when an alarm occurs in the **System > Preferences >Notifications** screen (see *18.3.4)*. Alarm becomes historical after selecting **Clear**.

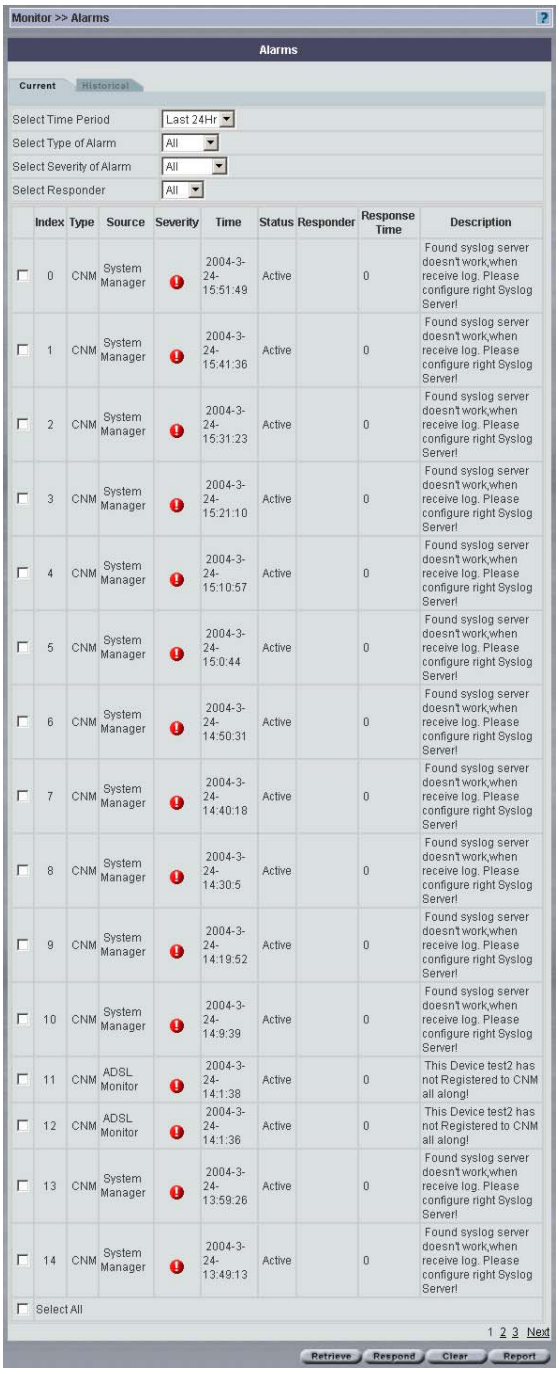


Figure 19-1 Monitor > Current Alarms

Table 19-4 Monitor > Current Alarms

STATE	DESCRIPTION
Select Time Period	Select the time period for which you wish to view alarms.
Select Type of Alarm	Select the type of alarm you wish to view, see *Table 19-1.*
Select Severity of Alarm	Select the type of alarm you wish to view, see *Table 19-2*.
Select Responder	Select the administrator to view the alarms that that administrator has responded to.
Checkbox/Select All	Select a checkbox(es) and then click **Clear** to erase those alarms.
Index	This is the alarm index number.
Type	This is the type of alarm: see *Table 19-1.*
Severity	This is the alarm severity: see *Table 19-2* and *Table 2-4*.
Time	This is the time the alarm occurred.
Status	This is the state of the alarm: see *Table 19-3*.
Responder	This is the administrator who responded to the alarm.
Response Time	This is the time the alarm occurred.
Description	This is the reason the alarm occurred.
Retrieve	Click **Retrieve** for Vantage to display the most recent alarms. These alarms may be displayed in another page.
Respond	Select an alarm and then click **Respond** to take responsibility for finding the cause of this alarm.
Clear	Select an alarm(s) and click **Clear** to erase this alarm(s).
Report	Click **Report** to generate a report on the alarms currently being viewed.

19.1.5 Historical Alarms

Historical alarms are alarms that have been cleared by an administrator.

This screen includes viewing filters for time, alarm type, alarm severity type and the administrator who responded to the alarm here.

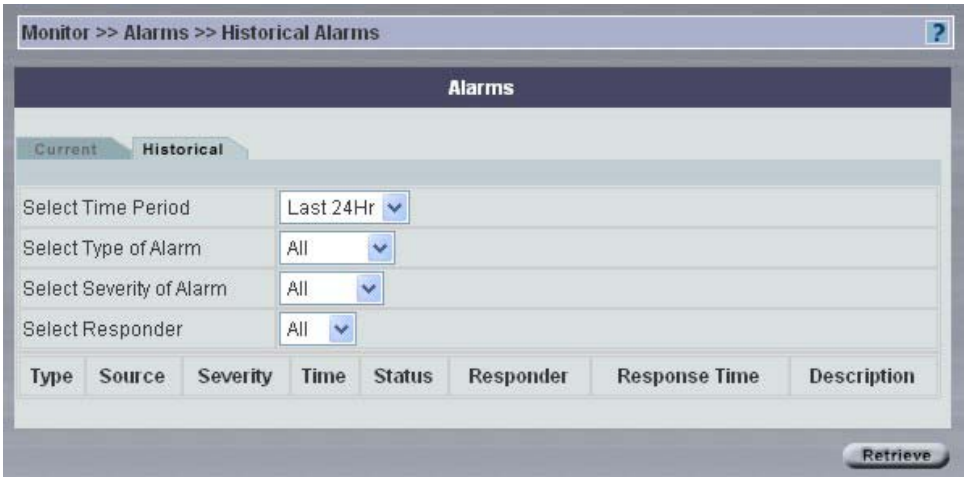


Figure 19-2 Monitor > Historical Alarms

See *Table 19-4* for more information on fields in this table.

20 Other Monitor Screens

"Firmware Upgrade" means that Vantage signals the device to request a firmware FTP upload from Vantage.

20.1 Firmware Upgrade Report

Details of firmware uploaded to Vantage are shown as in the next screen.

Figure 20-1 Monitor > Firmware Upgrade Report

The following table describes the labels in this screen.

Table 20-1 Monitor > Firmware Upgrade Report

LABEL	DESCRIPTION
Index	This is the upgrade list number.
Administrator	This displays the administrator who performed the upgrade.
Action Time	This displays the time at which the upgrade was performed.
Description	This displays a description entered in data maintenance prior to uploading.
Purge	Select **Purge** to delete selected reports from the Vantage server.

20.2 Status Monitor

This is a real time message monitor that displays messages such as urgent alerts and when an administrator has logged in or logged out. Click **Monitor > Status Monitor** and wait for Vantage to retrieve information and display it.

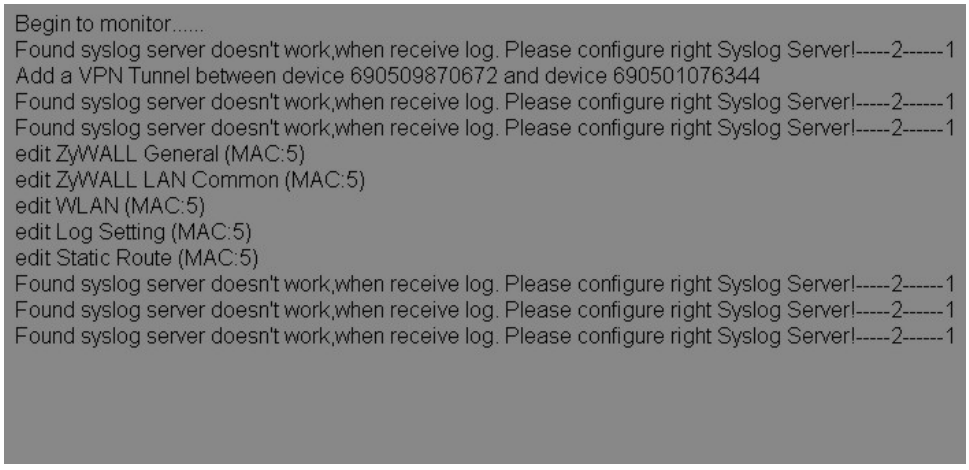


Figure 20-2 Monitor > Monitor Status

20.3 VPN Editor

This is a graphical VPN editor screen where you can click and drag VPN tunnels (single-click VPN) and also view individual tunnel details.

See *Table 2-5* for a description of the icons used in the VPN Editor.

20.3.1 Graphical VPN Tunnel Creation

Configure IPSec tunnels graphically as follows

Step 1. Drag the ZyXEL device icons around the screen as you please. Drag them apart to view each device more clearly. Save this view by clicking **Save**.

Step 2. Right-click a ZyXEL device (A-End) and select **VPN** in the popup menu. Click the ZyXEL device again and drag (you should see a red line) to another ZyXEL device (Z-End), then release the mouse button.

Step 3. You see the **Tunnel IPSec Detail** screen as shown next. Note that information in some fields has been automatically generated for you when you configure VPN this way. See *Table 11-6* for information on configuring this screen. At minimum, you must fill in the fields with the red asterisks. You can accept (or change) the automatically configured information in the other fields to set up the tunnel.

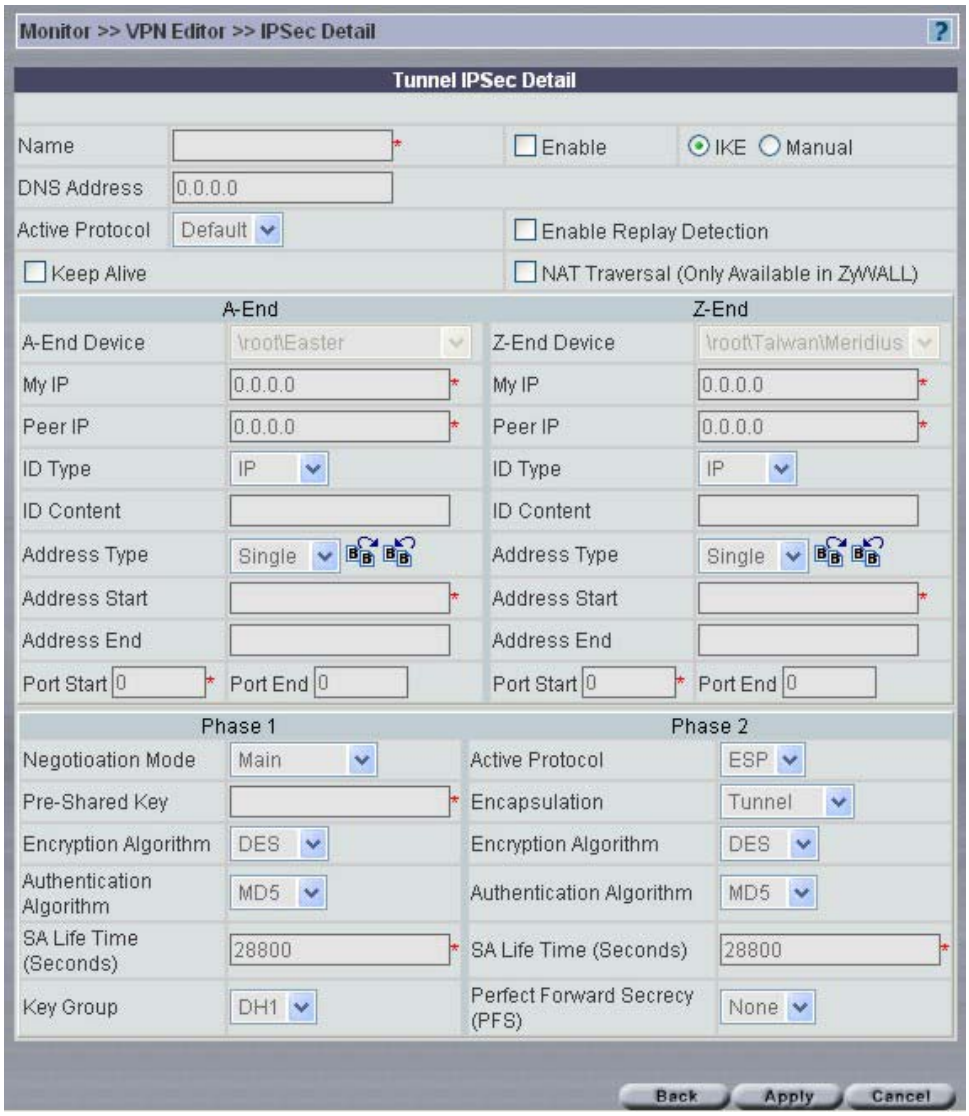


Figure 20-3 Monitor > VPN Editor > Tunnel IPSec Detail

Step 4. See Table 11-6 for more information on the fields in this screen. Click **Apply** to go to a **Tunnel Summary** screen.

The **Tunnel Summary** shows the **Name** of your tunnel, **A-End** and **Z-End** devices and the current tunnel **Status**.

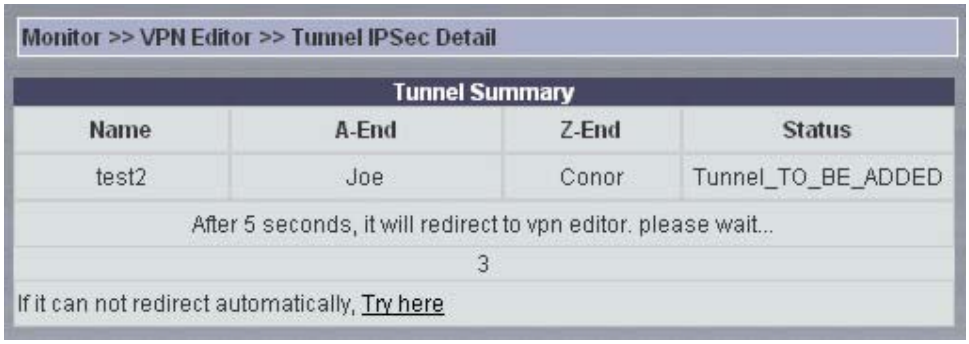


Figure 20-4 Configuration > VPN - Example Tunnel Summary

If you are not redirected, click the **Try here** hyperlink to go to the next screen.

The **Tunnel Summary** details are added to the top of the **IPSec Summary**, see *Figure 20-5* in the order they are configured (last tunnel appears last in the list).

20.3.2 Tunnel Graphical Depictions

A gray dashed line means that the Vantage server has not yet synchronized VPN tunnel information with both devices. This may be because Vantage has not so far communicated with one of the devices.

A gray solid line means that the VPN tunnel is set up between the devices but the tunnel is not active yet (no traffic).

A green solid line means an active tunnel (with traffic) between the ZyXEL devices.

The icons are dragged apart and dashed lines indicating VPN Tunnels are created after configuring the **Tunnel IPSec Detail** screen.

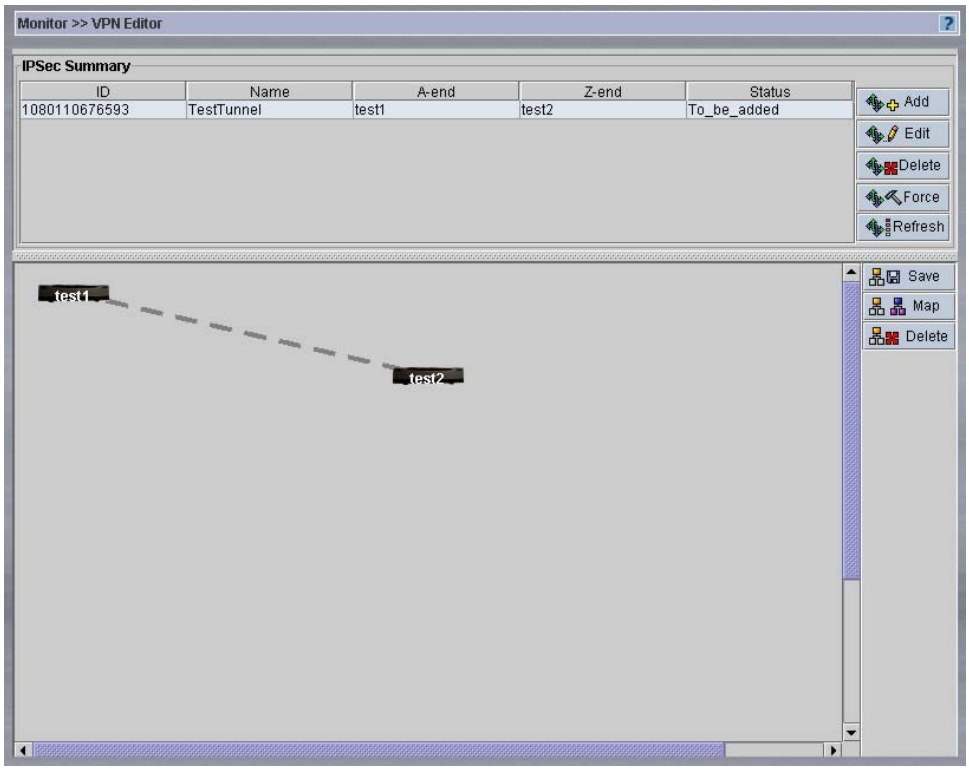


Figure 20-5 Monitor > VPN Monitor – Tunnel Graphics

To further aid the graphical depiction, click the **Map** button to upload a background image such as a map.

20.3.3 Map

Click the **Map** button in the IPSec **Summary** to upload a background gif (only) image. Type a file and path name or browse for your required file. Click **Upload**.

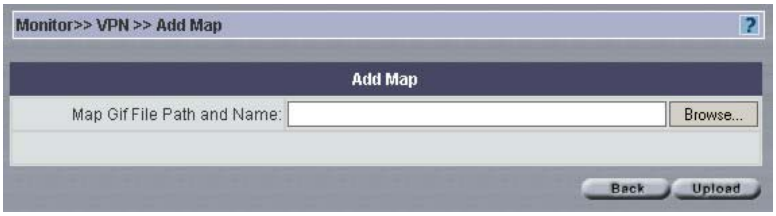
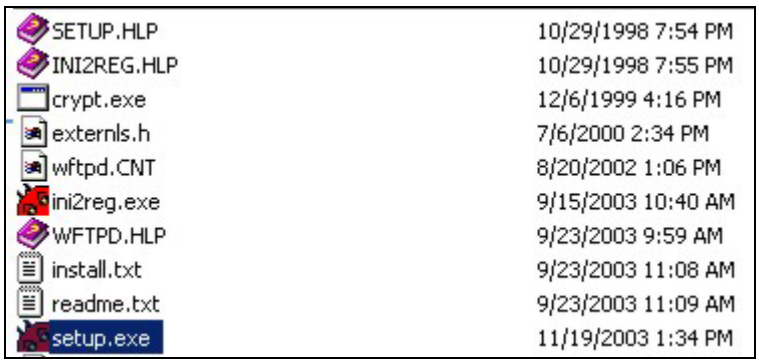


Figure 20-6 Monitor > VPN > Add MAP

Appendix A
FTP Server (WFTPD) Setup Example

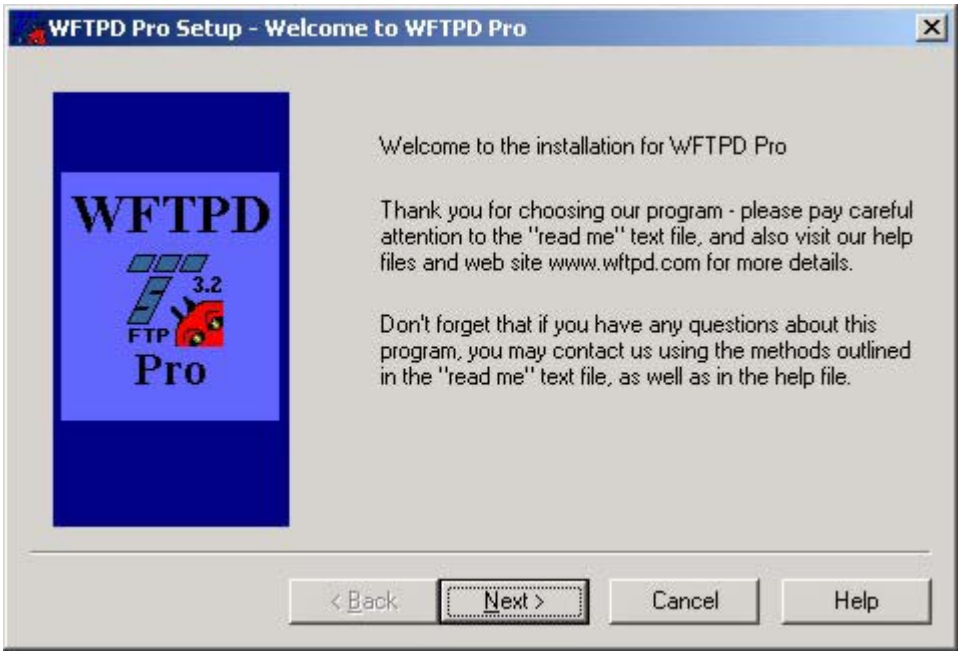
Step 1. Download the WFTPD software from www.wftpd.com to where you want to install it.

Step 2. Double-click setup.exe to begin the wizard.



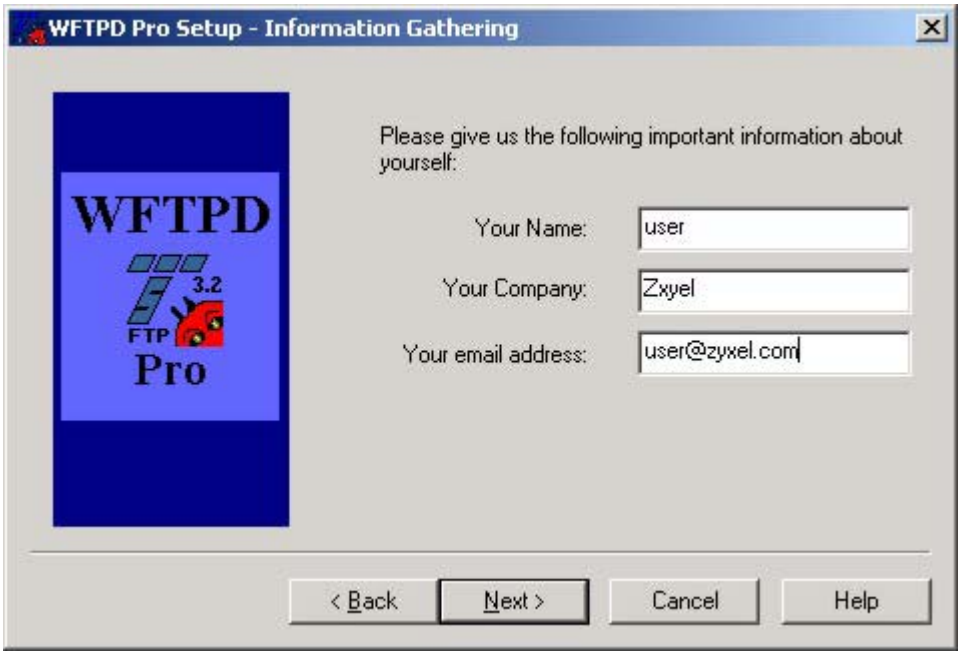
Setup

Step 3. Click **Next** to begin and then follow the wizard prompts.



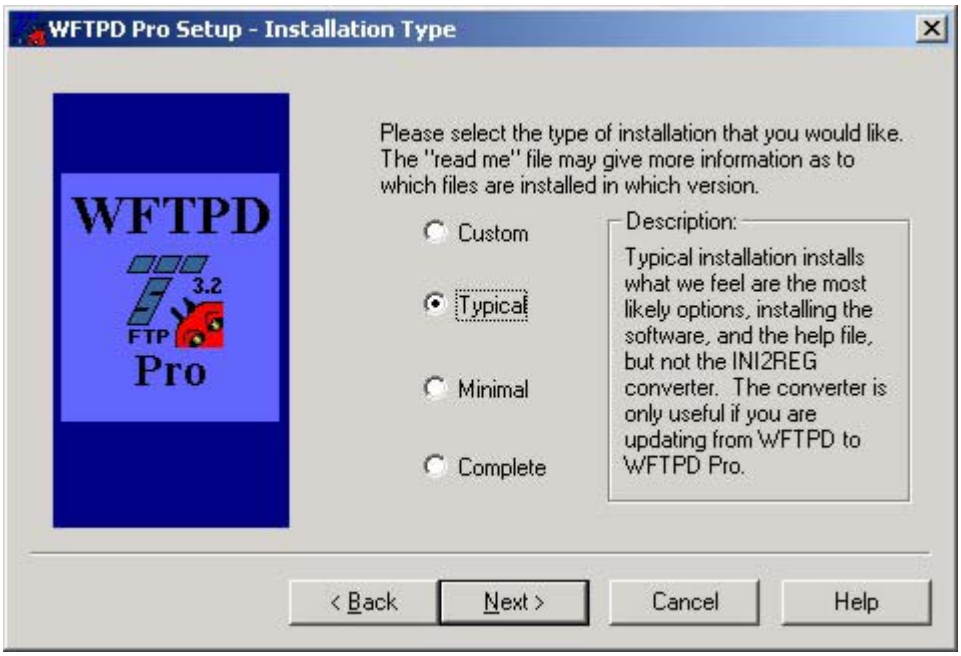
Wizard 1

Step 4. Enter your details here as shown and click **Next.**



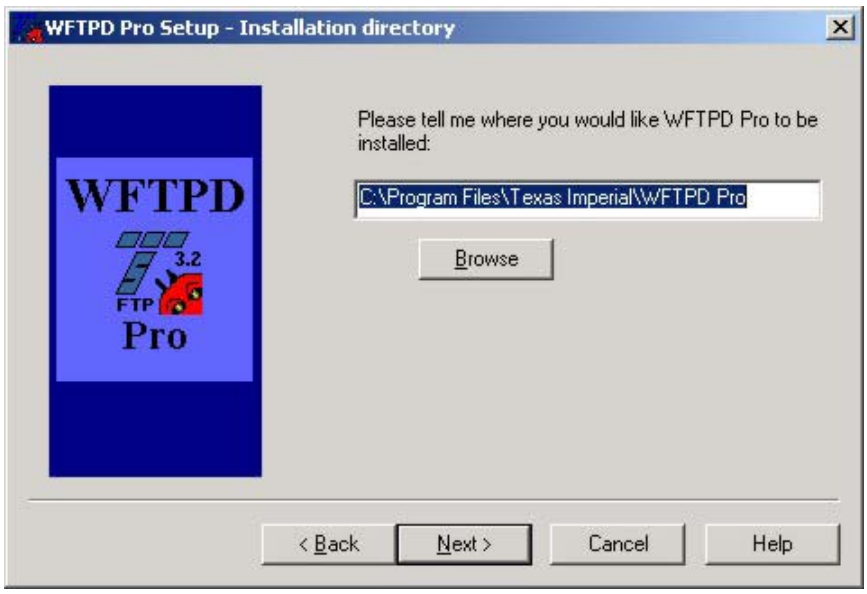
Information

Step 5. Select the installation type and click **Next**.



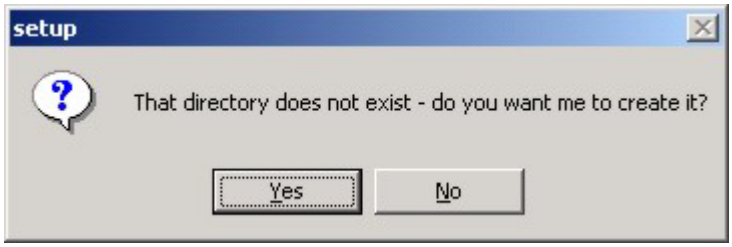
Installation Type

Step 6. Select where to install WFTPD Pro and click **Next**.



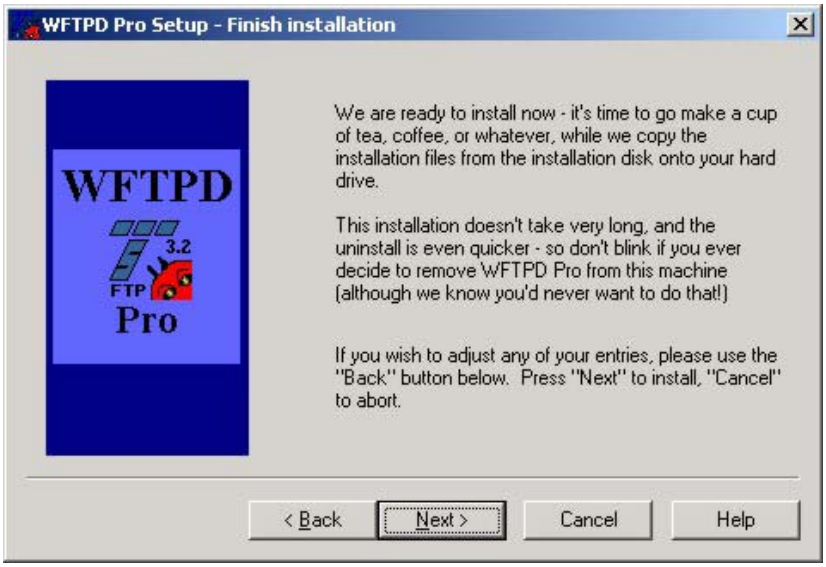
Installation Directory

Step 7. You are prompted to create the directory if it doesn't already exist. Click **Yes** to create a new directory.



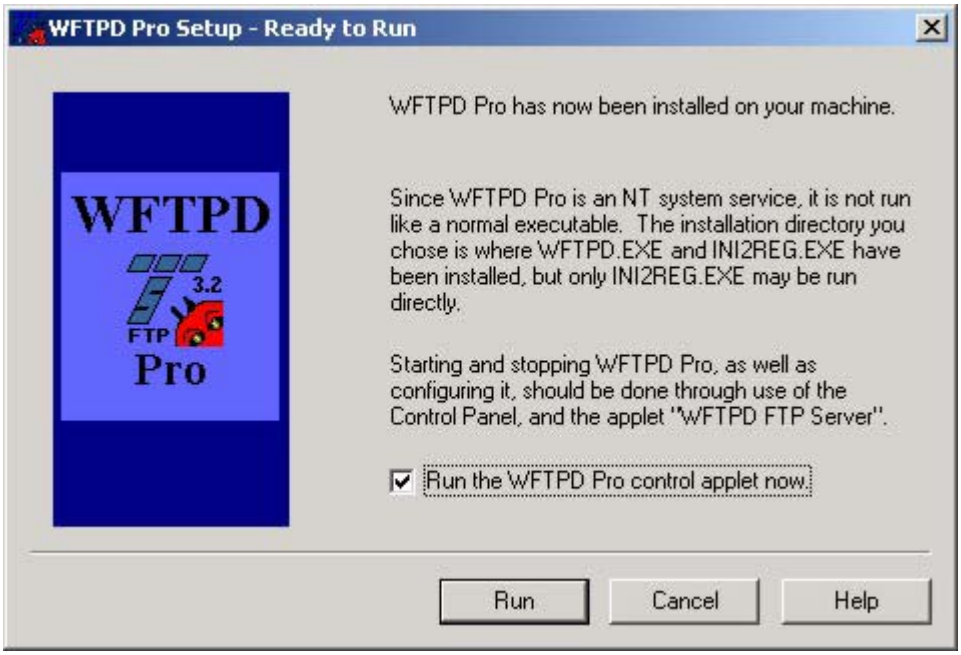
Create Directory

Step 8. Click **Next** to begin the installation.



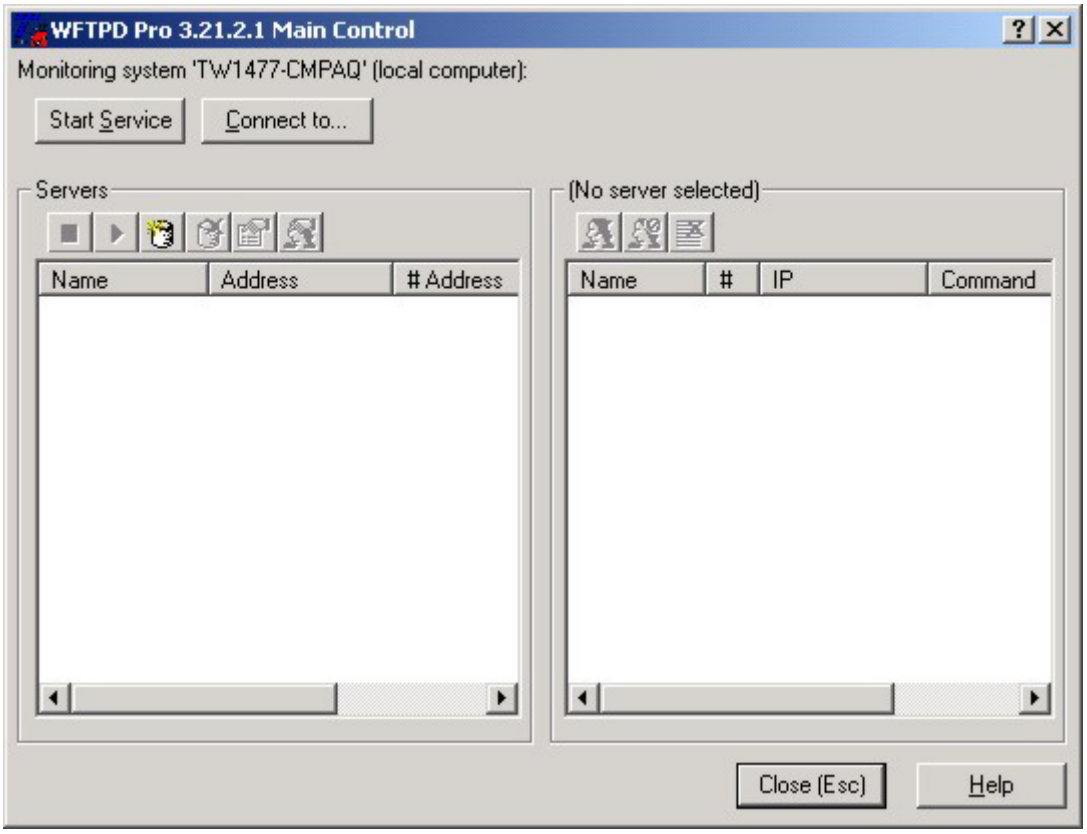
Begin Installation

Step 9. WFTPD has been installed. Click **Run** to start it. Make sure the check box is selected.



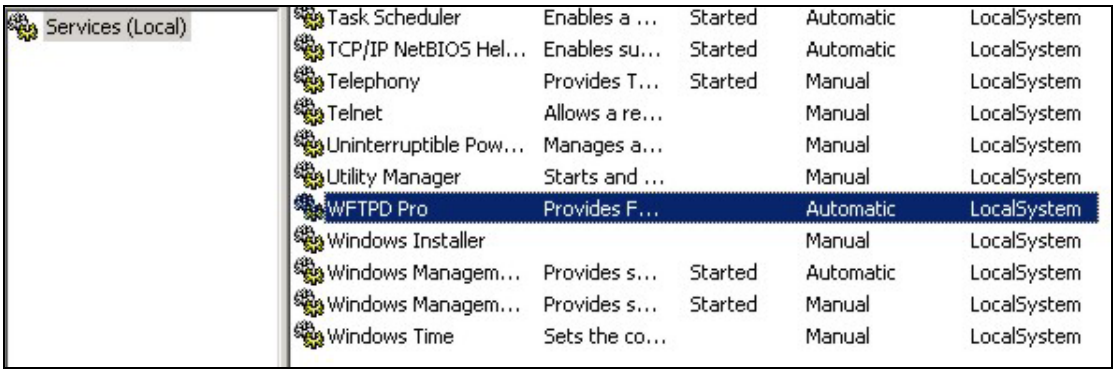
Run WFTPD

Step 10. Click **Start Service** form the WFTPD main screen.



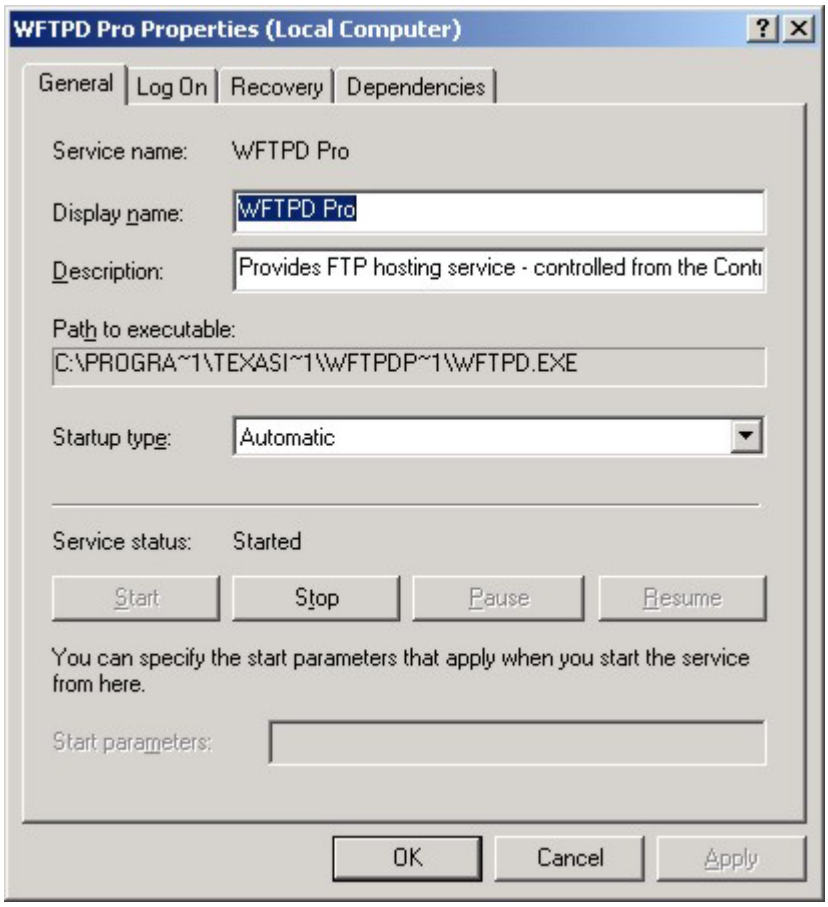
WFTPD Main Screen

Step 11. Open **Administrative Tools** in the Windows **Control Panel** and then select **Services** to see the WFTPD Pro service.



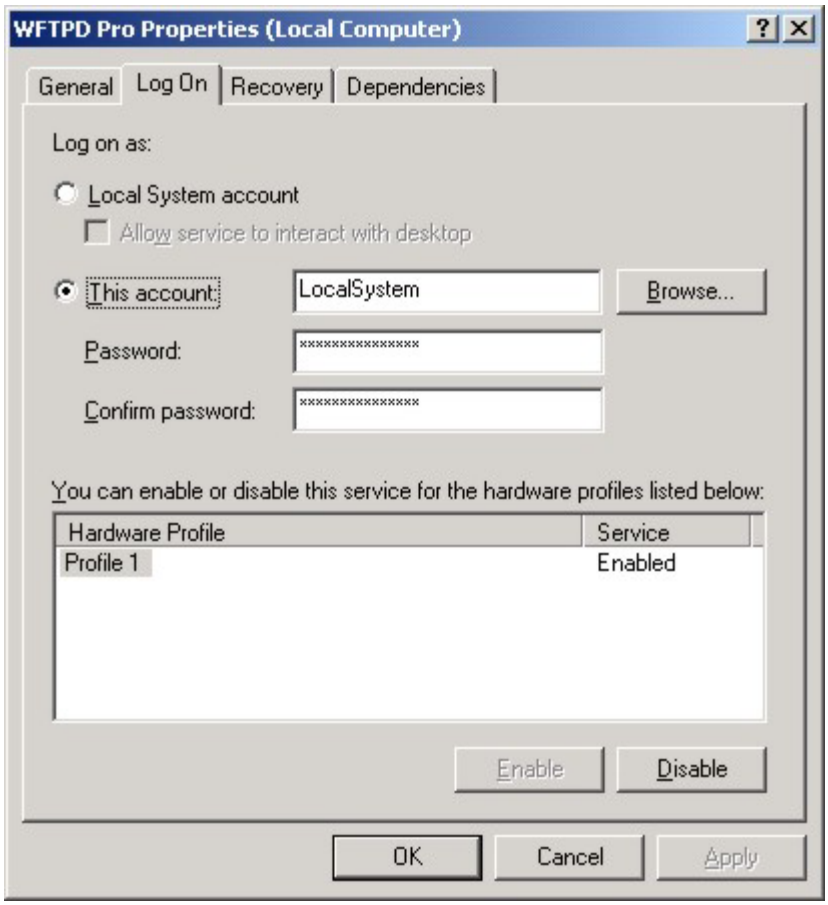
Windows Services

Step 12. Right-click **WFTPD Pro** service and then click **Properties**.



WFTPD Properties

Step 13. Click the **Log On** tab to configure a user name and password for this server. This must be the same username and password that you use in Vantage.



WFTPD Pro Log On

Appendix B
Configuring the Kiwi Syslog Daemon

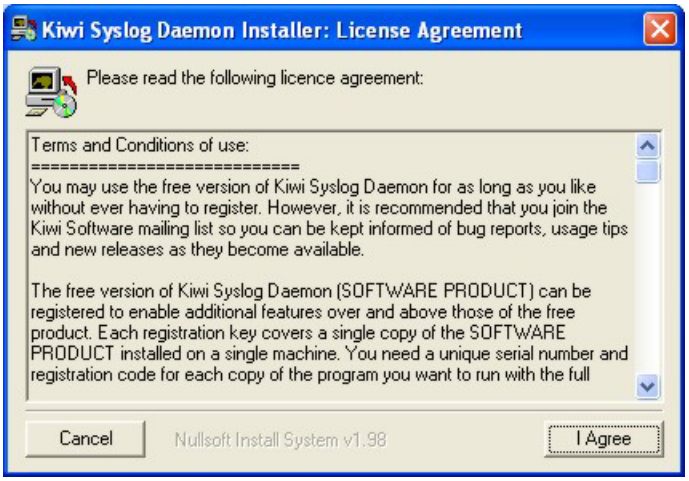
This section shows you how to install and configure the KiWi Syslog Daemon for use with Vantage CNM 2.0.

Installing the Kiwi Syslog Daemon

Follow the steps below to install the KiWi. Syslog Daemon

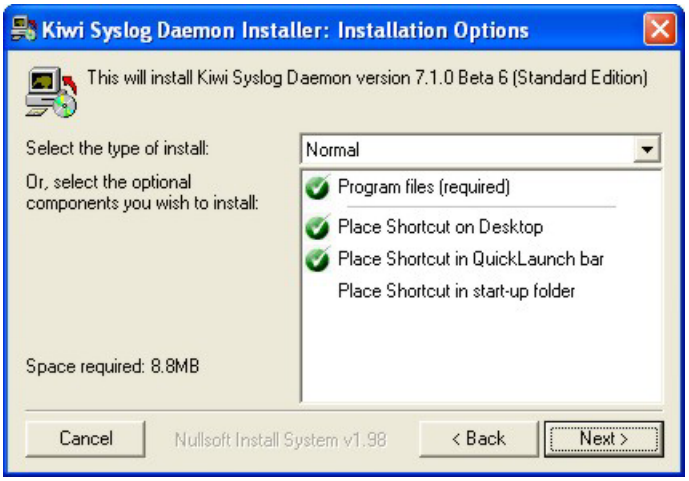
Step 1. Download the latest version of the KiWi Syslog Daemon from www.kiwisyslog.com to your computer.

Step 2. Double-click on the setup program. A screen displays as shown. Click **I Agree** to accept the license agreement.



Kiwi Syslog Daemon Installation: License Agreement

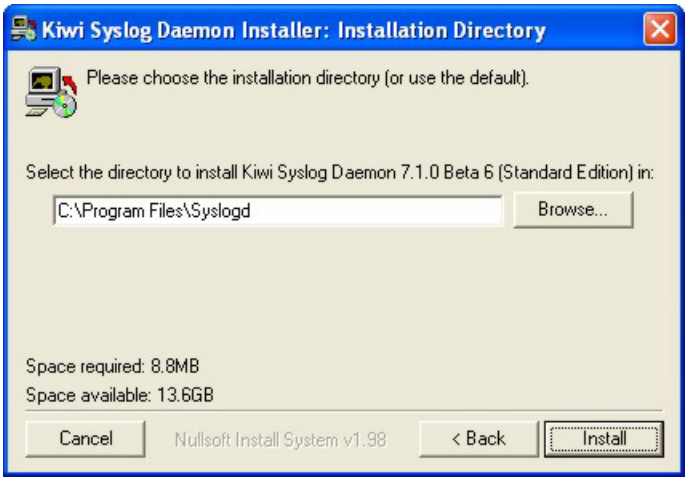
Step 3. Select the installation type (the default is **Normal**) and click **Next**.



Kiwi Installation: Installation Options

Step 4. Click **Install** to install Kiwi to the default directory.

You must install Kiwi in the C:\Program Files\Syslog **directory for the Vantage CNM 2.0 syslog function to work.**



Kiwi Installation: Installation Directory

Wait before the installation process completes.

Importing the Syslog Configuration File

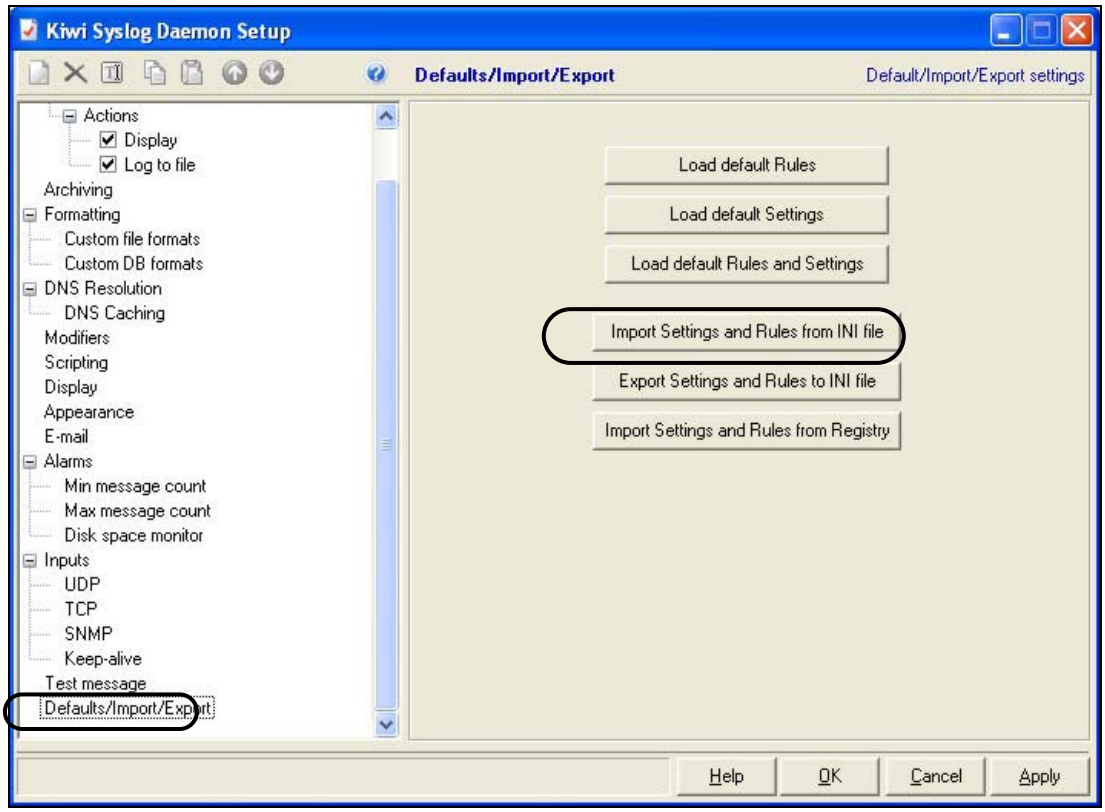
After installing the Kiwi Syslog Daemon, follow the steps below to import the configuration file.

Step 1. Copy and save the "Syslog Daemon Settings.ini" file to your computer.

Step 2. Start the Kiwi Syslog Daemon. In the main Kiwi Syslog Daemon screen, click **File**, **Setup**. A screen displays as shown.

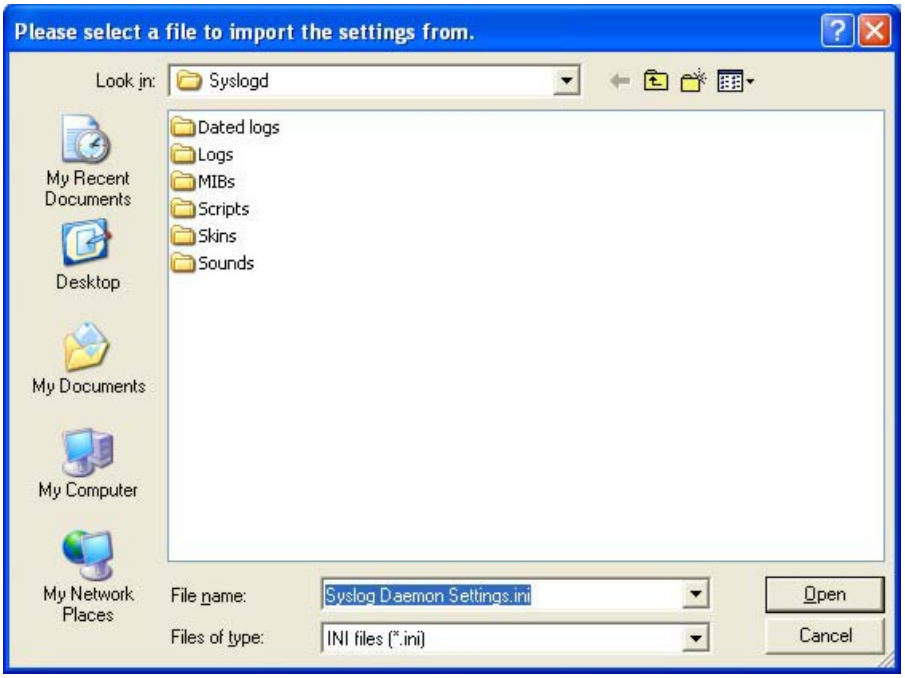
Step 5. Click **Defaults/Import/Export** under **Inputs**.

Step 6. Click **Import Settings and Rules from INI file**.



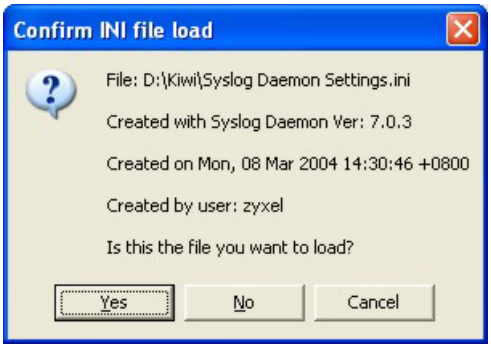
Kiwi Syslog Daemon Setup

Step 7. Locate the .ini syslog configuration file you and click **Open**.



Kiwi Syslog Daemon Setup: Import Configuration File

Step 8. Click **Yes** to confirm the configuration file import.



Kiwi Syslog Daemon Setup: Import Configuration File: Confirm

Step 9. In the **Kiwi Syslog Daemon Setup** screen, click **Apply** and then **OK** to close the screen.

You must start the Telnet service on the computer you install Kiwi.

Starting the Telnet Service

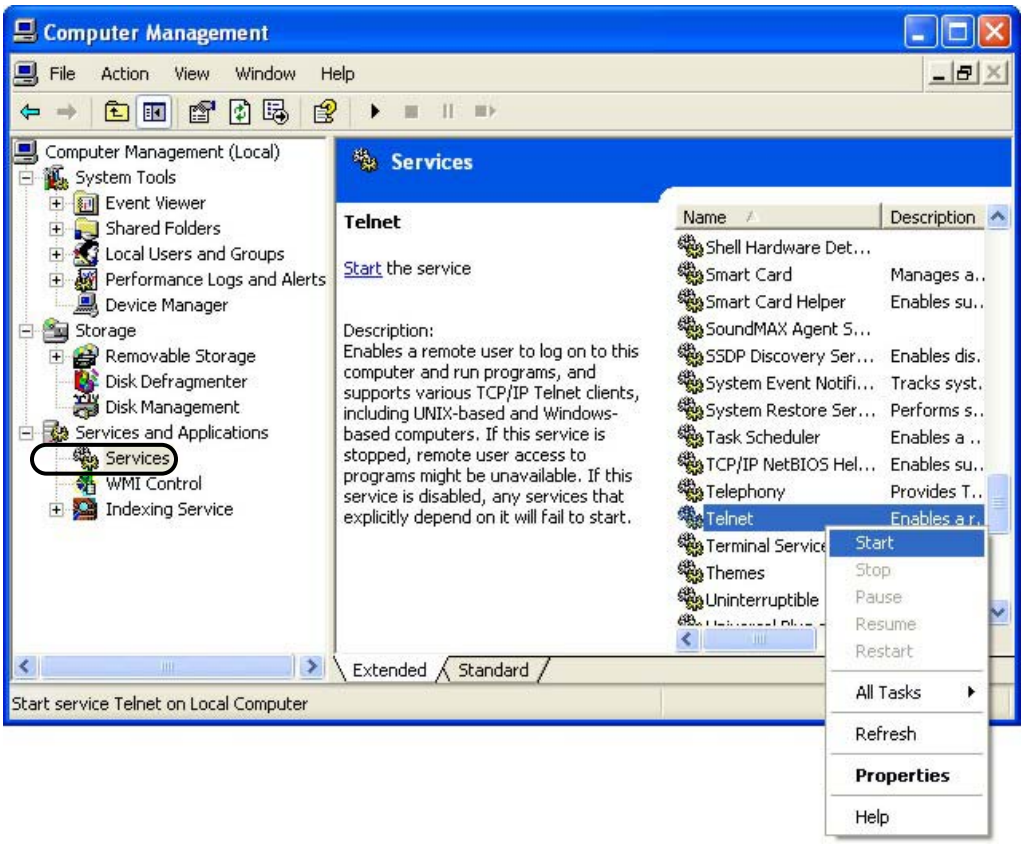
Follow the steps below to activate Telnet service for syslog logging on the computer you install Kiwi.

Step 3. Right-click on **My Computer** on the desktop and click **Manage**.

Windows XP: My Computer

Step 10. A **Computer Management** screen displays as shown next. Click **Services** under **Services and Applications** on the left panel.

Step 11. Search for the Telnet service on the right panel (you may have to scroll down the screen). Right-click on **Telnet** and click **Start** to start the Telnet service.



Windows XP: Computer Management

After you have installed and configure the Kii Syslog Daemon and started the Telnet service on the computer, configure the syslog settings in Vantage CNM 2.0. Set the syslog server username and password to be the same as the Windows username and password in the Vantage system **Server** screen.

Setting Up the Syslog Server in Vantage

Step 6. Log in to Vantage using the "root" account.

Step 7. Go to **System>Preferences>Server** screen.

Vantage System Servers

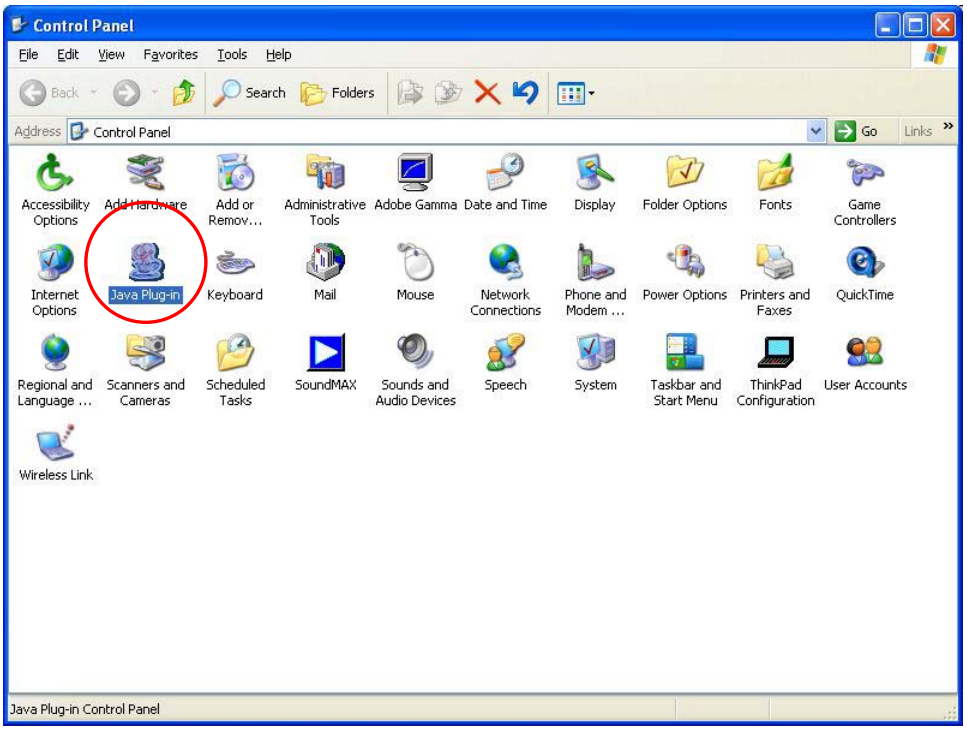
Step 8. Select **Syslog Server**, then enter the IP address of the computer on which you installed the Syslog server and the user name and password that you configured

Step 9. Click **Apply**.

Appendix C
Java Console Debug Messages

If you have problems with Vantage, customer support may ask you to find Java console debug messages. This appendix shows you how to do this.

Step 1. Click **Start**, **Control Panel** and double-click on **Java Plug-in**.

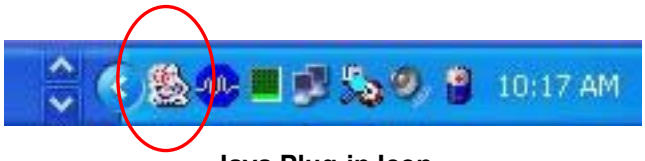


Control Panel Java Plug-in Icon

Step 2. Make sure that your settings match those of the **Basic** tab in the **Java™ Plug-in Control Panel** as shown in the following screenshot.

Java Plug-in Control Panel

Step 3. Open Internet Explorer and log into Vantage CNM 2.0. After successful login a Java plug-in icon should appear in your Windows system tray. If there is no icon present, return to step 2.

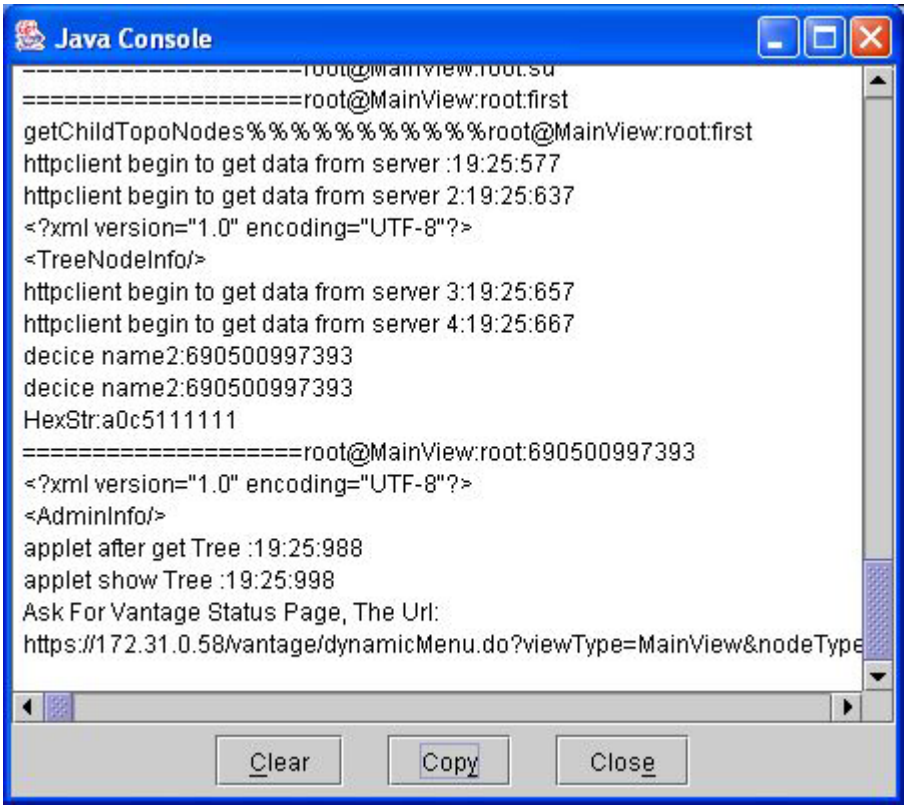


Java Plug-in Icon

Step 4. Right-click on the Java plug-in icon and select **Open Control Panel,** to view the Java Console screen.

Open Control Panel

Step 5. In the Java Console window, click **Copy**.



Java Console

Step 6. Paste this data into an e-mail and send it to customer support.

Appendix D
IP Subnetting

IP Addressing

Routers "route" based on the network number. The router that delivers the data packet to the correct destination host uses the host ID.

IP Classes

An IP address is made up of four octets (eight bits), written in dotted decimal notation, for example, 192.168.1.1. IP addresses are categorized into different classes. The class of an address depends on the value of its first octet.

- Class "A" addresses have a 0 in the left most bit. In a class "A" address the first octet is the network number and the remaining three octets make up the host ID.
- Class "B" addresses have a 1 in the left most bit and a 0 in the next left most bit. In a class "B" address the first two octets make up the network number and the two remaining octets make up the host ID.
- Class "C" addresses begin (starting from the left) with 1 1 0. In a class "C" address the first three octets make up the network number and the last octet is the host ID.
- Class "D" addresses begin with 1 1 1 0. Class "D" addresses are used for multicasting. (There is also a class "E" address. It is reserved for future use.)

Classes of IP Addresses

IP ADDRESS:		OCTET 1	OCTET 2	OCTET 3	OCTET 4
Class A	0	Network number	Host ID	Host ID	Host ID
Class B	10	Network number	Network number	Host ID	Host ID
Class C	110	Network number	Network number	Network number	Host ID

Host IDs of all zeros or all ones are not allowed.

Therefore:

- A class "C" network (8 host bits) can have 2^8 –2 or 254 hosts.
- A class "B" address (16 host bits) can have 2^{16} –2 or 65534 hosts.

A class "A" address (24 host bits) can have 2^{24} –2 hosts (approximately 16 million hosts).

Since the first octet of a class "A" IP address must contain a "0", the first octet of a class "A" address can have a value of 0 to 127.

Similarly the first octet of a class "B" must begin with "10", therefore the first octet of a class "B" address has a valid range of 128 to 191. The first octet of a class "C" address begins with "110", and therefore has a range of 192 to 223.

Allowed IP Address Range By Class

CLASS	ALLOWED RANGE OF FIRST OCTET (BINARY)	ALLOWED RANGE OF FIRST OCTET (DECIMAL)
Class A	**0**0000000 to **0**1111111	0 to 127
Class B	**10**000000 to **10**111111	128 to 191

Class C	**110**00000 to **110**11111	192 to 223
Class D	**1110**0000 to **1110**1111	224 to 239

Subnet Masks

A subnet mask is used to determine which bits are part of the network number, and which bits are part of the host ID (using a logical AND operation). A subnet mask has 32 bits; each bit of the mask corresponds to a bit of the IP address. If a bit in the subnet mask is a "1" then the corresponding bit in the IP address is part of the network number. If a bit in the subnet mask is "0" then the corresponding bit in the IP address is part of the host ID.

Subnet masks are expressed in dotted decimal notation just as IP addresses are. The "natural" masks for class A, B and C IP addresses are as follows.

"Natural" Masks

CLASS	NATURAL MASK
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

Subnetting

With subnetting, the class arrangement of an IP address is ignored. For example, a class C address no longer has to have 24 bits of network number and 8 bits of host ID. With subnetting, some of the host ID bits are converted into network number bits. By convention, subnet masks always consist of a continuous sequence of ones beginning from the left most bit of the mask, followed by a continuous sequence of zeros, for a total number of 32 bits.

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

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

The following table shows all possible subnet masks for a class "C" address using both notations.

Alternative Subnet Mask Notation

SUBNET MASK IP ADDRESS	SUBNET MASK "1" BITS	LAST OCTET BIT VALUE
255.255.255.0	/24	0000 0000
255.255.255.128	/25	1000 0000
255.255.255.192	/26	1100 0000
255.255.255.224	/27	1110 0000
255.255.255.240	/28	1111 0000
255.255.255.248	/29	1111 1000
255.255.255.252	/30	1111 1100

The first mask shown is the class "C" natural mask. Normally if no mask is specified it is understood that the natural mask is being used.

Example: Two Subnets

As an example, you have a class "C" address 192.168.1.0 with subnet mask of 255.255.255.0.

	NETWORK NUMBER	HOST ID
IP Address	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	00000000
Subnet Mask	255.255.255.	0
Subnet Mask (Binary)	11111111.11111111.11111111.	00000000

The first three octets of the address make up the network number (class "C"). You want to have two separate networks.

Divide the network 192.168.1.0 into two separate subnets by converting one of the host ID bits of the IP address to a network number bit. The "borrowed" host ID bit can be either "0" or "1" thus giving two subnets; 192.168.1.0 with mask 255.255.255.128 and 192.168.1.128 with mask 255.255.255.128.

In the following charts, shaded/bolded last octet bit values indicate host ID bits "borrowed" to form network ID bits. The number of "borrowed" host ID bits determines the number of subnets you can have. The remaining number of host ID bits (after "borrowing") determines the number of hosts you can have on each subnet.

Subnet 1

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	**0**0000000
Subnet Mask	255.255.255.	128
Subnet Mask (Binary)	11111111.11111111.11111111.	**1**0000000
Subnet Address: 192.168.1.0	Lowest Host ID: 192.168.1.1	
Broadcast Address: 192.168.1.127	Highest Host ID: 192.168.1.126	

Subnet 2

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	**1**0000000
Subnet Mask	255.255.255.	128
Subnet Mask (Binary)	11111111.11111111.11111111.	**1**0000000
Subnet Address: 192.168.1.128	Lowest Host ID: 192.168.1.129	
Broadcast Address: 192.168.1.255	Highest Host ID: 192.168.1.254	

The remaining 7 bits determine the number of hosts each subnet can have. Host IDs of all zeros represent the subnet itself and host IDs of all ones are the broadcast address for that subnet, so the actual number of hosts available on each subnet in the example above is $2^7 - 2$ or 126 hosts for each subnet.

192.168.1.0 with mask 255.255.255.128 is the subnet itself, and 192.168.1.127 with mask 255.255.255.128 is the directed broadcast address for the first subnet. Therefore, the lowest IP address that can be assigned to an actual host for the first subnet is 192.168.1.1 and the highest is 192.168.1.126. Similarly the host ID range for the second subnet is 192.168.1.129 to 192.168.1.254.

Example: Four Subnets

The above example illustrated using a 25-bit subnet mask to divide a class "C" address space into two subnets. Similarly to divide a class "C" address into four subnets, you need to "borrow" two host ID bits to give four

possible combinations of 00, 01, 10 and 11. The subnet mask is 26 bits (11111111.11111111.11111111.**11**000000) or 255.255.255.192. Each subnet contains 6 host ID bits, giving 2^6-2 or 62 hosts for each subnet (all 0's is the subnet itself, all 1's is the broadcast address on the subnet).

Subnet 1

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

Subnet 2

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

Subnet 3

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	**10**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.128	Lowest Host ID: 192.168.1.129	
Broadcast Address: 192.168.1.191	Highest Host ID: 192.168.1.190	

Subnet 4

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

Example Eight Subnets

Similarly use a 27-bit mask to create 8 subnets (001, 010, 011, 100, 101, 110).

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

Eight Subnets

SUBNET	SUBNET ADDRESS	FIRST ADDRESS	LAST ADDRESS	BROADCAST ADDRESS

1	0	1	30	31
2	32	33	62	63
3	64	65	94	95
4	96	97	126	127
5	128	129	158	159
6	160	161	190	191
7	192	193	222	223
8	224	223	254	255

The following table is a summary for class “C” subnet planning.

Class C Subnet Planning

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

Subnetting With Class A and Class B Networks.

For class “A” and class “B” addresses the subnet mask also determines which bits are part of the network number and which are part of the host ID.

A class “B” address has two host ID octets available for subnetting and a class “A” address has three host ID octets available for subnetting.

The following table is a summary for class “B” subnet planning.

Class B Subnet Planning

NO. “BORROWED” HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.128.0 (/17)	2	32766
2	255.255.192.0 (/18)	4	16382
3	255.255.224.0 (/19)	8	8190
4	255.255.240.0 (/20)	16	4094
5	255.255.248.0 (/21)	32	2046
6	255.255.252.0 (/22)	64	1022
7	255.255.254.0 (/23)	128	510
8	255.255.255.0 (/24)	256	254

Class B Subnet Planning

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
9	255.255.255.128 (/25)	512	126
10	255.255.255.192 (/26)	1024	62
11	255.255.255.224 (/27)	2048	30
12	255.255.255.240 (/28)	4096	14
13	255.255.255.248 (/29)	8192	6
14	255.255.255.252 (/30)	16384	2
15	255.255.255.254 (/31)	32768	1

Appendix E
Open Software Announcements

Notice

This Product includes Castor

Copyright (C) 1999-2001 Intalio, Inc. All Rights Reserved.

Redistribution and use of this software and associated documentation ("Software"), with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain copyright statements and notices. Redistributions must also contain a copy of this document.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The name "ExoLab" must not be used to endorse or promote products derived from this Software without prior written permission of ExoLab Group. For written permission, please contact info@exolab.org.

4. Products derived from this Software may not be called "ExoLab" nor may "ExoLab" appear in their names without prior written permission of ExoLab Group. Exolab is a registered trademark of ExoLab Group.

5.Due credit should be given to the ExoLab Group (http://www.exolab.org).

THIS SOFTWARE IS PROVIDED BY INTALIO, INC. AND CONTRIBUTORS "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF ERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED.

IN NO EVENT SHALL INTALIO, INC. OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This Product includes Junit under Common Public License Version 1.0

Common Public License Version 1.0

THE ACCOMPANYING PROGRAM IS PROVIDED UNDER THE TERMS OF THIS COMMON PUBLIC LICENSE ("AGREEMENT"). ANY USE, REPRODUCTION OR DISTRIBUTION OF THE PROGRAM CONSTITUTES RECIPIENT'S ACCEPTANCE OF THIS AGREEMENT.

1. DEFINITIONS

"Contribution" means: a) in the case of the initial Contributor, the initial code and documentation distributed under this Agreement, and b) in the case of each subsequent Contributor: i) changes to the Program, and ii) additions to the Program; where such changes and/or additions to the Program originate from and are distributed by that particular Contributor. A Contribution 'originates' from a Contributor if it was added to the Program by such Contributor itself or anyone acting on such Contributor's behalf. Contributions do not include additions to the Program which: (i) are separate modules of software distributed in conjunction with the Program under their own license agreement, and (ii) are not derivative works of the Program.

"Contributor" means any person or entity that distributes the Program.

"Licensed Patents " mean patent claims licensable by a Contributor which are necessarily infringed by the use or sale of its Contribution alone or when combined with the Program.

"Program" means the Contributions distributed in accordance with this Agreement.

"Recipient" means anyone who receives the Program under this Agreement, including all Contributors.

2. GRANT OF RIGHTS

a) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free copyright license to reproduce, prepare derivative works of, publicly display, publicly perform, distribute and sublicense the Contribution of such Contributor, if any, and such derivative works, in source code and object code form.

b) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free patent license under Licensed Patents to make, use, sell, offer to sell, import and otherwise transfer the Contribution of such Contributor, if any, in source code and object code form. This patent license shall apply to the combination of the Contribution and the Program if, at the time the Contribution is added by the Contributor, such addition of the Contribution causes such combination to be covered by the Licensed Patents. The patent license shall not apply to any other combinations which include the Contribution. No hardware per se is licensed hereunder.

c) Recipient understands that although each Contributor grants the licenses to its Contributions set forth herein, no assurances are provided by any Contributor that the Program does not infringe the patent or other intellectual property rights of any other entity. Each Contributor disclaims any liability to Recipient for claims brought by any other entity based on infringement of intellectual property rights or otherwise. As a condition to exercising the rights and licenses granted hereunder, each Recipient hereby assumes sole responsibility to secure any other intellectual property rights needed, if any. For example, if a third party patent license is required to allow Recipient to distribute the Program, it is Recipient's responsibility to acquire that license before distributing the Program.

d) Each Contributor represents that to its knowledge it has sufficient copyright rights in its Contribution, if any, to grant the copyright license set forth in this Agreement.

3. REQUIREMENTS

A Contributor may choose to distribute the Program in object code form under its own license agreement, provided that:

a) it complies with the terms and conditions of this Agreement; and

b) its license agreement: i) effectively disclaims on behalf of all Contributors all warranties and conditions, express and implied, including warranties or conditions of title and non-infringement, and implied warranties or conditions of merchantability and fitness for a particular purpose; ii) effectively excludes on

behalf of all Contributors all liability for damages, including direct, indirect, special, incidental and consequential damages, such as lost profits; iii) states that any provisions which differ from this Agreement are offered by that Contributor alone and not by any other party; and iv) states that source code for the Program is available from such Contributor, and informs licensees how to obtain it in a reasonable manner on or through a medium customarily used for software exchange.

When the Program is made available in source code form:

a) it must be made available under this Agreement; and

b) a copy of this Agreement must be included with each copy of the Program.

Contributors may not remove or alter any copyright notices contained within the Program.

Each Contributor must identify itself as the originator of its Contribution, if any, in a manner that reasonably allows subsequent Recipients to identify the originator of the Contribution.

4. COMMERCIAL DISTRIBUTION

Commercial distributors of software may accept certain responsibilities with respect to end users, business partners and the like. While this license is intended to facilitate the commercial use of the Program, the Contributor who includes the Program in a commercial product offering should do so in a manner which does not create potential liability for other Contributors. Therefore, if a Contributor includes the Program in a commercial product offering, such Contributor ("Commercial Contributor") hereby agrees to defend and indemnify every other Contributor ("Indemnified Contributor") against any losses, damages and costs (collectively "Losses") arising from claims, lawsuits and other legal actions brought by a third party against the Indemnified Contributor to the extent caused by the acts or omissions of such Commercial Contributor in connection with its distribution of the Program in a commercial product offering. The obligations in this section do not apply to any claims or Losses relating to any actual or alleged intellectual property infringement. In order to qualify, an Indemnified Contributor must: a) promptly notify the Commercial Contributor in writing of such claim, and b) allow the Commercial Contributor to control, and cooperate with the Commercial Contributor in, the defense and any related settlement negotiations. The Indemnified Contributor may participate in any such claim at its own expense.

For example, a Contributor might include the Program in a commercial product offering, Product X. That Contributor is then a Commercial Contributor. If that Commercial Contributor then makes performance claims, or offers warranties related to Product X, those performance claims and warranties are such Commercial Contributor's responsibility alone. Under this section, the Commercial Contributor would have to defend claims against the other Contributors related to those performance claims and warranties, and if a court requires any other Contributor to pay any damages as a result, the Commercial Contributor must pay those damages.

5. NO WARRANTY

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, THE PROGRAM IS PROVIDED ON AN "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, EITHER EXPRESS OR IMPLIED INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OR CONDITIONS OF TITLE, NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Each Recipient is solely responsible for determining the appropriateness of using and distributing the Program and assumes all risks associated with its exercise of rights under this Agreement, including but not limited to the risks and costs of program errors, compliance with applicable laws, damage to or loss of data, programs or equipment, and unavailability or interruption of operations.

6. DISCLAIMER OF LIABILITY

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, NEITHER RECIPIENT NOR ANY CONTRIBUTORS SHALL HAVE ANY LIABILITY FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING WITHOUT LIMITATION LOST PROFITS), HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OR DISTRIBUTION OF THE PROGRAM

OR THE EXERCISE OF ANY RIGHTS GRANTED HEREUNDER, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7. GENERAL

If any provision of this Agreement is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this Agreement, and without further action by the parties hereto, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.

If Recipient institutes patent litigation against a Contributor with respect to a patent applicable to software (including a cross-claim or counterclaim in a lawsuit), then any patent licenses granted by that Contributor to such Recipient under this Agreement shall terminate as of the date such litigation is filed. In addition, if Recipient institutes patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Program itself (excluding combinations of the Program with other software or hardware) infringes such Recipient's patent(s), then such Recipient's rights granted under Section 2(b) shall terminate as of the date such litigation is filed.

All Recipient's rights under this Agreement shall terminate if it fails to comply with any of the material terms or conditions of this Agreement and does not cure such failure in a reasonable period of time after becoming aware of such noncompliance. If all Recipient's rights under this Agreement terminate, Recipient agrees to cease use and distribution of the Program as soon as reasonably practicable. However, Recipient's obligations under this Agreement and any licenses granted by Recipient relating to the Program shall continue and survive.

Everyone is permitted to copy and distribute copies of this Agreement, but in order to avoid inconsistency the Agreement is copyrighted and may only be modified in the following manner. The Agreement Steward reserves the right to publish new versions (including revisions) of this Agreement from time to time. No one other than the Agreement Steward has the right to modify this Agreement. IBM is the initial Agreement Steward. IBM may assign the responsibility to serve as the Agreement Steward to a suitable separate entity. Each new version of the Agreement will be given a distinguishing version number. The Program (including Contributions) may always be distributed subject to the version of the Agreement under which it was received. In addition, after a new version of the Agreement is published, Contributor may elect to distribute the Program (including its Contributions) under the new version. Except as expressly stated in Sections 2(a) and 2(b) above, Recipient receives no rights or licenses to the intellectual property of any Contributor under this Agreement, whether expressly, by implication, estoppel or otherwise. All rights in the Program not expressly granted under this Agreement are reserved.

This Agreement is governed by the laws of the State of New York and the intellectual property laws of the United States of America. No party to this Agreement will bring a legal action under this Agreement more than one year after the cause of action arose. Each party waives its rights to a jury trial in any resulting litigation.

This Product includes Cryptix

Cryptix General License

Copyright (c) 1995, 1996, 1997, 1998, 1999, 2000 The Cryptix Foundation Limited. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE CRYPTIX FOUNDATION LIMITED AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE CRYPTIX FOUNDATION LIMITED OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This Product includes software of Java Software technologies.

TECHNOLOGY LICENSE FROM SUN MICROSYSTEMS, INC. TO DOUG LEA

Whereas Doug Lea desires to utlized certain Java Software technologies in the util.concurrent technology; and Whereas Sun Microsystems, Inc. (“Sun”) desires that Doug Lea utilize certain Java Software technologies in the util.concurrent technology; Therefore the parties agree as follows, effective May 31, 2002:

“Java Software technologies” means

classes/java/util/ArrayList.java, and

classes/java/util/HashMap.java.

The Java Software technologies are Copyright (c) 1994-2000 Sun Microsystems, Inc. All rights reserved.

Sun hereby grants Doug Lea a non-exclusive, worldwide, non-transferrable license to use, reproduce, create derivate works of, and distribute the Java Software and derivative works thereof in source and binary forms as part of a larger work, and to sublicense the right to use, reproduce and distribute the Java Software and Doug Lea's derivative works as the part of larger works through multiple tiers of sublicensees provided that the following conditions are met:

-Neither the name of or trademarks of Sun may be used to endorse or promote products including or derived from the Java Software technology without specific prior written permission; and

-Redistributions of source or binary code must contain the above copyright notice, this notice and the following disclaimers:

THIS SOFTWARE IS PROVIDED "AS IS," WITHOUT A WARRANTY OF ANY KIND. ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE HEREBY EXCLUDED. SUN MICROSYSTEMS, INC. AND ITS LICENSORS SHALL NOT BE LIABLE FOR ANY DAMAGES SUFFERED BY LICENSEE AS A RESULT OF USING, MODIFYING OR

DISTRIBUTING THE SOFTWARE OR ITS DERIVATIVES. IN NO EVENT WILL SUN MICROSYSTEMS, INC. OR ITS LICENSORS BE LIABLE FOR ANY LOST REVENUE, PROFIT OR DATA, OR FOR DIRECT, INDIRECT, SPECIAL, CONSEQUENTIAL, INCIDENTAL OR PUNITIVE

DAMAGES, HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY, ARISING OUT OF THE USE OF OR INABILITY TO USE SOFTWARE, EVEN IF SUN MICROSYSTEMS, INC. HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

You acknowledge that Software is not designed, licensed or intended for use in the design, construction, operation or maintenance of any nuclear facility.

signed [Doug Lea] dated

JAVA Software Technologies

JAVA(TM) 2 SOFTWARE DEVELOPMENT KIT (J2SDK), STANDARD EDITION, VERSION 1.4.1_X SUPPLEMENTAL LICENSE TERMS

These supplemental license terms ("Supplemental Terms") add to or modify the terms of the Binary Code License Agreement (collectively, the "Agreement"). Capitalized terms not defined in these Supplemental Terms shall have the same meanings ascribed to them in the Binary Code License Agreement. These Supplemental Terms shall supersede any inconsistent or conflicting terms in the Binary Code License Agreement, or in any license contained within the Software.

1. Software Internal Use and Development License Grant. Subject to the terms and conditions of this Agreement, including, but not limited to Section 4 (Java Technology Restrictions) of these Supplemental Terms, Sun grants you a non-exclusive, non-transferable, limited license without fees to reproduce internally and use internally the binary form of the Software complete and unmodified for the sole purpose of designing, developing, testing, and running your Java applets and applications intended to run on Java-enabled general purpose desktop computers and servers ("Programs").

2. License to Distribute Software. Subject to the terms and conditions of this Agreement, including, but not limited to Section 4 (Java Technology Restrictions) of these Supplemental Terms, Sun grants you a non-exclusive, non-transferable, limited license without fees to reproduce and distribute the Software, provided that (i) you distribute the Software complete and unmodified (unless otherwise specified in the applicable README file) and only bundled as part of, and for the sole purpose of running, your Programs, (ii) the Programs add significant and primary functionality to the Software, (iii) you do not distribute additional software intended to replace any omponent(s) of the Software (unless otherwise specified in the applicable README file), (iv) you do not remove or alter any proprietary legends or notices contained in the Software, (v) you only distribute the Software subject to a license agreement that protects Sun's interests consistent with the terms contained in this Agreement, and (vi) you agree.

3. License to Distribute Redistributables. Subject to the terms and conditions of this Agreement, including but not limited to Section 4 (Java Technology Restrictions) of these Supplemental Terms, Sun grants you a non-exclusive, non-transferable, limited license without fees to reproduce and distribute those files specifically identified as redistributable in the Software "README" file ("Redistributables") provided that: (i) you distribute the Redistributables complete and unmodified (unless otherwise specified in the applicable README file), and only bundled as part of Programs, (ii) you do not distribute additional software intended to supersede any component(s) of the Redistributables (unless otherwise specified in the applicable README file), (iii) you do not remove or alter any proprietary legends or notices contained in or on the Redistributables, (iv) you only distribute the Redistributables pursuant to a license agreement that protects Sun's interests consistent with the terms contained in the Agreement.

4. Java Technology Restrictions. You may not modify the Java Platform Interface ("JPI", identified as classes contained within the "java" package or any subpackages of he "java" package), by creating additional classes within the JPI or otherwise causing the addition to or modification of the classes in the JPI. In the event that you create an additional class and associated API(s) which (i) extends the functionality of the Java platform, and (ii) is exposed to third party software

developers for the purpose of developing additional software which invokes such additional API, you must promptly publish broadly an accurate specification for such API for free use by all developers. You may not create, or authorize your licensees to create, additional classes, interfaces, or subpackages that are in any way identified as "java", "javax", "sun" or similar convention as specified by Sun in any naming convention designation.

5. Notice of Automatic Software Updates from Sun. You acknowledge that the Software may automatically download, install, and execute applets, applications, software extensions, and updated versions of the Software from Sun ("Software Updates"), which may require you to accept updated terms and conditions for installation. If additional terms and conditions are not presented on installation, the Software Updates will be considered part of the Software and subject to the terms and conditions of the Agreement.

6. Notice of Automatic Downloads. You acknowledge that, by your use of the Software and/or by requesting services that require use of the Software, the Software may automatically download, install, and execute software applications from sources other than Sun ("Other Software"). Sun makes no representations of a relationship of any kind to licensors of Other Software. TO THE EXTENT NOT PROHIBITED BY LAW, IN NO EVENT WILL SUN OR ITS LICENSORS BE LIABLE FOR ANY LOST REVENUE, PROFIT OR DATA, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL OR PUNITIVE DAMAGES, HOWEVER CAUSED REGARDLESS OF THE THEORY OF LIABILITY, ARISING OUT OF OR RELATED TO THE USE OF OR INABILITY TO USE OTHER SOFTWARE, EVEN IF SUN HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7. Distribution by Publishers. This section pertains to your distribution of the Software with your printed book or magazine (as those terms are commonly used in the industry) relating to Java technology ("Publication"). Subject to and conditioned upon your compliance with the restrictions and obligations contained in the Agreement, in addition to the license granted in Paragraph 1 above, Sun hereby grants to you a non-exclusive, nontransferable limited right to reproduce complete and unmodified copies of the Software on electronic media (the "Media") for the sole purpose of inclusion and distribution with your Publication(s), subject to the following terms: (i) You may not distribute the Software on a stand-alone basis; it must be distributed with your Publication(s); (ii) You are responsible for downloading the Software from the applicable Sun web site; (iii) You must refer to the Software as JavaTM 2 Software Development Kit, Standard Edition, Version 1.4.1; (iv) The Software must be reproduced in its ent

8. Trademarks and Logos. You acknowledge and agree as between you and Sun that Sun owns the SUN, SOLARIS, JAVA, JINI, FORTE, and iPLANET trademarks and all SUN, SOLARIS, JAVA, JINI, FORTE, and iPLANET-related trademarks, service marks, logos and other brand designations ("Sun Marks"), and you agree to comply with the Sun Trademark and Logo Usage Requirements currently located at http://www.sun.com/policies/trademarks. Any use you make of the Sun Marks inures to Sun's benefit.

9. Source Code. Software may contain source code that is provided solely for reference purposes pursuant to the terms of this Agreement. Source code may not be redistributed unless expressly provided for in this Agreement.

10. Termination for Infringement. Either party may terminate this Agreement immediately should any Software become, or in either party's opinion be likely to become,the subject of a claim of infringement of any intellectual property right.

For inquiries please contact: Sun Microsystems, Inc., 4150Network Circle, Santa Clara, California 95054, U.S.A (LFI#134402/Form ID#011801)

This Product includes software of Apache Software Foundation.

Apache License

Version 2.0, January 2004

http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition,

"control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are

necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works hereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

(a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

(b) You must cause any modified files to carry prominent notices stating that You changed the files; and

(c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

(d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License. You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You

may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

Version 1.1

Redistribution and use in source and binary forms, with or without modification, are

permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

The end-user documentation included with the redistribution, if any, must include the following acknowledgment: “This product includes software developed by the Apache Software Foundation (http://www.apache.org/).” Alternately, this acknowledgment may appear in the software itself, if and wherever such third-party acknowledgments normally appear.

The names “Apache” and “Apache Software Foundation” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact apache@apache.org.

Products derived from this software may not be called “Apache”, nor may “Apache” appear in their name, without prior written permission of the Apache Software Foundation.

THIS SOFTWARE IS PROVIDED ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE APACHE SOFTWARE FOUNDATION OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This software consists of voluntary contributions made by many individuals on behalf of the Apache Software Foundation. For more information on the Apache Software Foundation, please see <http://www.apache.org/>.

Portions of this software are based upon public domain software originally written at the National Center for Supercomputing Applications, University of Illinois, Urbana-Champaign.

NOTE: Some components of the Vantage CNM software incorporate source code covered under the **Apache License**. To obtain the source code covered under the **Apache License**, please contact ZyXEL customer support.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get

it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the

same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License. In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License").

Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables. The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library. Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library. You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions: a) The modified work must itself be a software library. b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change. c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License. d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains

meaningful. (For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.) These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote

it. Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library. In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices. Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy. This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange. If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not

compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables. When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law. If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.) Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications. You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things: a) Accompany the work with the complete corresponding

machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.) b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a

copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with. c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution. d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place. e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy. For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things: a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above. b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to

refrain entirely from distribution of the Library. If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances. It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice. This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing

and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE

LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCHDAMAGES.

END OF TERMS AND CONDITIONS

This Product includes MySQl database under GPL.

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

59 Temple Place - Suite 330, Boston, MA 02111-1307, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it. For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software. Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program

proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you". Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program. You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it. Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program. In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or, c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.) The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the

scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable. If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program. If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances. It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice. This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add

an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE; THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

All other trademarks or trade names mentioned herein, if any, are the property of their respective owners.

End-User License Agreement for Vantage CNM

WARNING: ZyXEL Communications Corp. IS WILLING TO LICENSE THE ENCLOSED SOFTWARE TO YOU ONLY UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS LICENSE AGREEMENT. PLEASE READ THE TERMS CAREFULLY BEFORE COMPLETING THE INSTALLATION PROCESS AS INSTALLING THE SOFTWARE WILL INDICATE YOUR ASSENT TO THEM. IF YOU DO NOT AGREE TO THESE TERMS, THEN ZyXEL, INC. IS UNWILLING TO LICENSE THE SOFTWARE TO YOU, IN WHICH EVENT YOU SHOULD RETURN THE UNINSTALLED SOFTWARE AND PACKAGING TO THE PLACE FROM WHICH IT WAS ACQUIRED, AND YOUR MONEY WILL BE REFUNDED.

1. Grant of License for Personal Use

ZyXEL Communications Corp. ("ZyXEL") grants you a non-exclusive, non-sublicense, non-transferable license to use the program with which this license is distributed (the "Software"), including any documentation files accompanying the Software ("Documentation"), for internal business use only, for up to the number of users specified in sales order and invoice. You have the right to make one backup copy of the Software and Documentation solely for archival, back-up or disaster recovery purposes. You shall not exceed the scope of the license granted hereunder. Any rights not expressly granted by ZyXEL to you are reserved by ZyXEL, and all implied licenses are disclaimed.

2. Ownership

You have no ownership rights in the Software. Rather, you have a license to use the Software as long as this License Agreement remains in full force and effect. Ownership of the Software, Documentation and all intellectual property rights therein shall remain at all times with ZyXEL. Any other use of the Software by any other entity is strictly forbidden and is a violation of this License Agreement.

3. Copyright

The Software and Documentation contain material that is protected by United States Copyright Law and trade secret law, and by international treaty provisions. All rights not granted to you herein are expressly reserved by ZyXEL. You may not remove any proprietary notice of ZyXEL or any of its licensors from any copy of the Software or Documentation.

4. Restrictions

You may not publish, display, disclose, sell, rent, lease, modify, store, loan, distribute, or create derivative works of the Software, or any part thereof. You may not assign, sublicense, convey or otherwise transfer, pledge as security or otherwise encumber the rights and licenses granted hereunder with respect to the Software. You may not copy, reverse engineer, decompile, reverse compile, translate, adapt, or disassemble the Software, or any part thereof, nor shall you attempt to create the source code from the object code for the Software. You may not market, co-brand, private label or otherwise permit third parties to link to the Software, or any part thereof. You may not use the Software, or any part thereof, in the operation of a service bureau or for the benefit of any other person or entity. You may not cause, assist or permit any third party to do any of the foregoing.

5. Confidentiality

You acknowledge that the Software contains proprietary trade secrets of ZyXEL and you hereby agree to maintain the confidentiality of the Software using at least as great a degree of care as you use to maintain the confidentiality of your own most confidential information. You agree to reasonably communicate the terms and conditions of this License Agreement to those persons employed by you who come into contact with the Software, and to use reasonable best efforts to ensure their compliance with such terms and conditions, including, without limitation, not knowingly permitting such persons to use any portion of the Software for the purpose of deriving the source code of the Software.

6. No Warranty

THE SOFTWARE IS PROVIDED "AS IS." TO THE MAXIMUM EXTENT PERMITTED BY LAW, ZyXEL DISCLAIMS ALL WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. ZyXEL DOES NOT WARRANT THAT THE FUNCTIONS CONTAINED IN THE SOFTWARE WILL MEET ANY REQUIREMENTS OR NEEDS YOU MAY HAVE, OR THAT THE SOFTWARE WILL OPERATE ERROR FREE, OR IN AN

UNINTERUPTED FASHION, OR THAT ANY DEFECTS OR ERRORS IN THE SOFTWARE WILL BE CORRECTED, OR THAT THE SOFTWARE IS COMPATIBLE WITH ANY PARTICULAR PLATFORM. SOME JURISDICTIONS DO NOT ALLOW THE WAIVER OR EXCLUSION OF IMPLIED WARRANTIES SO THEY MAY NOT APPLY TO YOU. IF THIS EXCLUSION IS HELD TO BE UNENFORCEABLE BY A COURT OF COMPETENT JURISDICTION, THEN ALL EXPRESS AND IMPLIED WARRANTIES SHALL BE LIMITED IN DURATION TO A PERIOD OF THIRTY (30) DAYS FROM THE DATE OF PURCHASE OF THE SOFTWARE, AND NO WARRANTIES SHALL APPLY AFTER THAT PERIOD.

7. LIMITATION OF LIABILITY. To the maximum extent permitted by applicable law, in no event shall ZyXEL or its suppliers be liable for any special, incidental, indirect, or consequential damages whatsoever (including, without limitation, damages for loss of business profits, business interruption, loss of business information, or any other pecuniary loss) arising out of the use of or inability to use the SOFTWARE or the provision of or failure to provide Support Services, even if ZyXEL has been advised of the possibility of such damages. In any case, ZyXEL's entire liability under any provision of this EULA shall be limited to the greater of the amount actually paid by you for the SOFTWARE; provided, however, if you have entered into a ZyXEL Support Services Agreement, ZyXEL's entire liability regarding Support Services shall be governed by the terms of that agreement.

8. Export Restrictions

THIS LICENSE AGREEMENT IS EXPRESSLY MADE SUBJECT TO ANY APPLICABLE LAWS, REGULATIONS, ORDERS, OR OTHER RESTRICTIONS ON THE EXPORT OF THE SOFTWARE OR INFORMATION ABOUT SUCH SOFTWARE WHICH MAY BE IMPOSED FROM TIME TO TIME. YOU SHALL NOT EXPORT THE SOFTWARE, DOCUMENTATION OR INFORMATION ABOUT THE SOFTWARE AND DOCUMENTATION WITHOUT COMPLYING WITH SUCH LAWS, REGULATIONS, ORDERS, OR OTHER RESTRICTIONS. YOU AGREE TO INDEMNIFY ZyXEL AGAINST ALL CLAIMS, LOSSES, DAMAGES, LIABILITIES, COSTS AND EXPENSES, INCLUDING REASONABLE ATTORNEYS' FEES, TO THE EXTENT SUCH CLAIMS ARISE OUT OF ANY BREACH OF THIS SECTION 8.

9. Audit Rights

ZyXEL SHALL HAVE THE RIGHT, AT ITS OWN EXPENSE, UPON REASONABLE PRIOR NOTICE, TO PERIODICALLY INSPECT AND AUDIT YOUR RECORDS TO ENSURE YOUR COMPLIANCE WITH THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT.

10. Termination

This License Agreement is effective until it is terminated. You may terminate this License Agreement at any time by destroying or returning to ZyXEL all copies of the Software and Documentation in your possession or under your control. ZyXEL may terminate this License Agreement for any reason, including, but not limited to, if ZyXEL finds that you have violated any of the terms of this License Agreement. Upon notification of termination, you agree to destroy or return to ZyXEL all copies of the Software and Documentation and to certify in writing that all known copies, including backup copies, have been destroyed. All provisions relating to confidentiality, proprietary rights, and non-disclosure shall survive the termination of this Software License Agreement.

12. General

This License Agreement shall be construed, interpreted and governed by the laws of Republic of China without regard to conflicts of laws provisions thereof. The exclusive forum for any disputes arising out of or relating to this License Agreement shall be an appropriate court or Commercial Arbitration Association

sitting in ROC, Taiwan. This License Agreement shall constitute the entire Agreement between the parties hereto. This License Agreement, the rights granted hereunder, the Software and Documentation shall not be assigned by you without the prior written consent of ZyXEL. Any waiver or modification of this License Agreement shall only be effective if it is in writing and signed by both parties hereto. If any part of this License Agreement is found invalid or unenforceable by a court of competent jurisdiction, the remainder of this License Agreement shall be interpreted so as to reasonably effect the intention of the parties.