LAN-Cell 2

3G Cellular Router + VPN + Firewall

User's Guide

Version 4.02
November 2008
Edition 2

proxicast®

www.proxicast.com

Contents Overview

Table of Contents

About This User's Guide

Intended Audience

This manual is intended for people who want to configure the LAN-Cell 2 using the web configurator or System Management Terminal (SMT). You should have at least a basic knowledge of TCP/IP networking concepts and topology.

Related Documentation

- Quick Start Guide

  The Quick Start Guide is designed to help you get up and running right away. It contains information on setting up your network and configuring for Internet access.
- Web Configurator Online Help

  Embedded web help for descriptions of individual screens and supplementary information.
- Support Disk

  Refer to the included CD for additional support documents.
- Proxicast Support Web Site

  Please refer to support.proxicast.com for additional support documentation and access to our Knowledgebase.

Document Conventions

Warnings and Notes

These are how warnings and notes are shown in this User's Guide.

Warnings tell you about things that could harm you or your device.

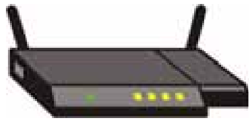
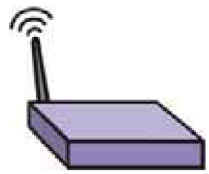
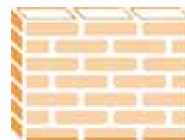
Notes tell you other important information (for example, other things you may need to configure or helpful tips) or recommendations.

Syntax Conventions

- The LAN-Cell 2 may be referred to as the "LAN-Cell", the "device" or the "system" in this User's Guide.
- The LAN-Cell's wired Ethernet WAN interface may be referred to as "WAN", "Wired WAN" or "WAN 1".
- The LAN-Cell's PC-Card modem 3G cellular interface may be referred to was "Cellular", "CELL", or "WAN 2"
- Product labels, screen names, field labels and field choices are all in **bold** font.
- A key stroke is denoted by square brackets and uppercase text, for example, [ENTER] means the "enter" or "return" key on your keyboard.
- "Enter" means for you to type one or more characters and then press the [ENTER] key. "Select" or "choose" means for you to use one of the predefined choices.
- A right angle bracket (>) within a screen name denotes a mouse click. For example, **Maintenance > Log > Log Setting** means you first click **Maintenance** in the navigation panel, then the **Log** sub menu and finally the **Log Setting** tab to get to that screen.
- Units of measurement may denote the "metric" value or the "scientific" value. For example, "k" for kilo may denote "1000" or "1024", "M" for mega may denote "1000000" or "1048576" and so on.
- "e.g.," is a shorthand for "for instance", and "i.e.," means "that is" or "in other words".
- The example screens shown in the User's Guide may differ slightly from the actual screens on the LAN-Cell, depending on the firmware version the LAN-Cell is running.

Icons Used in Figures

Figures in this User’s Guide may use the following generic icons. The LAN-Cell icon is not an exact representation of your device.

LAN-Cell 	Computer 	Notebook computer 
Server 	Wi-Fi Access Point 	Firewall 
Telephone 	Switch 	Router 

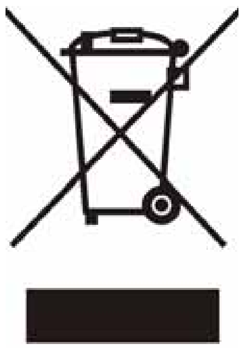
Safety Warnings

For your safety, be sure to read and follow all warning notices and instructions.

- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do NOT store things on the device.
- Do NOT install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- Do NOT open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. ONLY qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Use ONLY an appropriate power adaptor or cord for your device.
- Connect the power adaptor or cord to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe).
- Not to remove the plug and plug into a wall outlet by itself; always attach the plug to the power supply first before insert into the wall.
- Do NOT allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Do NOT use the device if the power adaptor or cord is damaged as it might cause electrocution.
- If the power adaptor or cord is damaged, remove it from the power outlet.
- Do NOT attempt to repair the power adaptor or cord. Contact your local vendor to order a new one.
- Do not use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.
- CAUTION: RISK OF EXPLOSION IF BATTERY (on the motherboard) IS REPLACED BY AN INCORRECT TYPE. DISPOSE OF USED BATTERIES ACCORDING TO THE INSTRUCTIONS. Dispose them at the applicable collection point for the recycling of electrical and electronic equipment. For detailed information about recycling of this product, please contact your local city office, your household waste disposal service or the store where you purchased the product.
- Do NOT obstruct the device ventilation slots, as insufficient airflow may harm your device.

- Antenna Warning! This device meets ETSI and FCC certification requirements when using the included antenna(s).
- If you wall mount your device, make sure that no electrical lines, gas or water pipes will be damaged.

This product is recyclable. Dispose of it properly.



PART I
Introduction

1

Getting to Know Your LAN-Cell 2

This chapter introduces the main features and applications of the LAN-Cell 2.

1.1 LAN-Cell 2: 3G Cellular Router + VPN + Firewall Overview

The LAN-Cell 2 is Proxicast's second generation of enterprise-grade secure cellular gateways. This model features customer accessible and removeable "3G" PC-Card (PCMCIA) cellular modems -- the same ones commonly used to provide high-speed 3G cellular connectivity to laptops. The 3G PC-Card modem seamlessly becomes a WAN interface for the LAN-Cell's router and is fully integrated with all of the LAN-Cell's security, performance, and management capabilities.

As in earlier LAN-Cell models, the LAN-Cell 2 is loaded with security features including VPN, firewall and X.509 PKI certificates. The LAN-Cell 2's De-Militarized Zone (DMZ) increases LAN security by providing separate ports for connecting publicly accessible servers. The LAN-Cell provide the option to change port roles from LAN to DMZ.

The LAN-Cell 2 adds bandwidth management, NAT, port forwarding, policy routing, DHCP server, Cell-Sentry^{TM} data budgeting and many other powerful features required for complex and demanding applications.

The LAN-Cell 2 also has a built-in Wi-Fi access point that allows IEEE 802.11a, IEEE 802.11b or IEEE 802.11g compatible clients to securely communicate with the LAN-Cell and access the wired network or Internet. You can use the Wi-Fi access point as part of the LAN, DMZ or WLAN.

The LAN-Cell 2's all metal construction coupled with its unique Card-Lock^{TM} and Card-Guard^{TM} systems make it the perfect choice for applications where a high-performance, secure, reliable and rugged cellular router is required.

See Chapter 44 on page 575 for a complete list of features.

1.2 Ways to Manage the LAN-Cell

Use any of the following methods to manage the LAN-Cell.

- Web Configurator. This is recommended for everyday management of the LAN-Cell using a (supported) web browser.
- SMT. System Management Terminal is a text-based configuration menu that you can use to configure your device.
- FTP for firmware upgrades and configuration backup/restore.

- Command Line Interface. Line commands are mostly used for troubleshooting by service engineers and also provide access to some of the LAN-Cell's more advanced features.
- SNMP. The device can be monitored by an SNMP manager. See the SNMP chapter in this User's Guide.

1.3 Good Habits for Managing the LAN-Cell

Do the following things regularly to make the LAN-Cell more secure and to manage the LAN-Cell more effectively.

- Change the password. Use a password that's not easy to guess and that consists of different types of characters, such as numbers and letters.
- Write down the password and put it in a safe place.
- Back up the configuration (and make sure you know how to restore it). Restoring an earlier working configuration may be useful if the device becomes unstable or even crashes. If you forget your password, you will have to reset the LAN-Cell to its factory default settings. If you backed up an earlier configuration file, you would not have to totally re-configure the LAN-Cell. You could simply restore your last configuration.

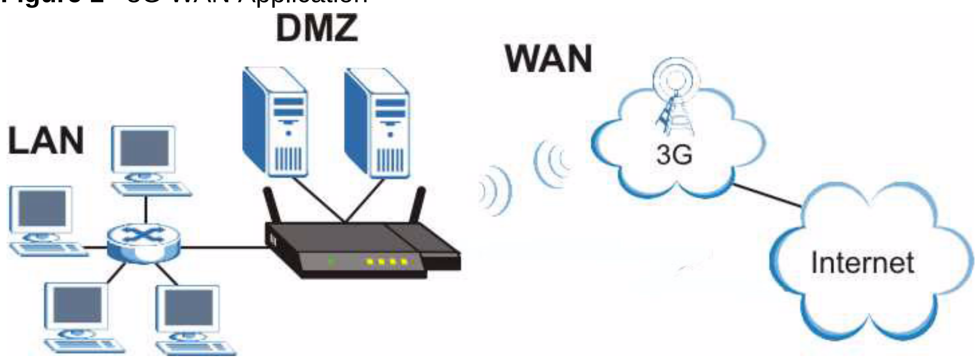
1.4 Applications for the LAN-Cell

Here are some examples of what you can do with your LAN-Cell.

1.4.1 3G WAN Applications

Insert a 3G PC-Card modem to have the LAN-Cell wirelessly access the Internet via a 3G celluar network. Use this connection to provide Internet access to LAN devices such as PCs and ATMs, or to provide access to remote equipment such as weather stations and security systems. See Section 5.4 on page 114 for more information about 3G Cellular WAN support.

Figure 1 3G WAN Application



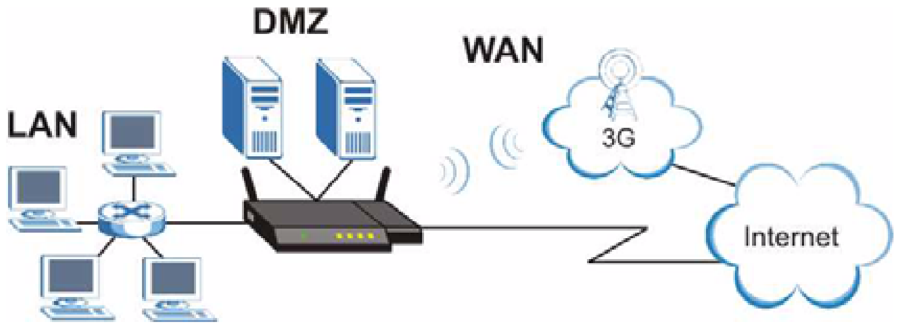
1.4.2 Redundant Secure Broadband Internet Access via Ethernet or Cellular

Connect the LAN-Cell's Ethernet WAN port to your existing Internet access gateway (company network, or your cable or DSL modem for example). Connect computers or servers to the LAN, DMZ or WLAN ports for shared Internet access.

With both the primary WAN (physical WAN port) and 3G WAN connections enabled, you can set one of the WAN connections as an automatic fail-over backup connection or use load balancing to improve quality of service and maximize bandwidth utilization.

The LAN-Cell guarantees not only high speed Internet access, but secure internal network protection and traffic management as well.

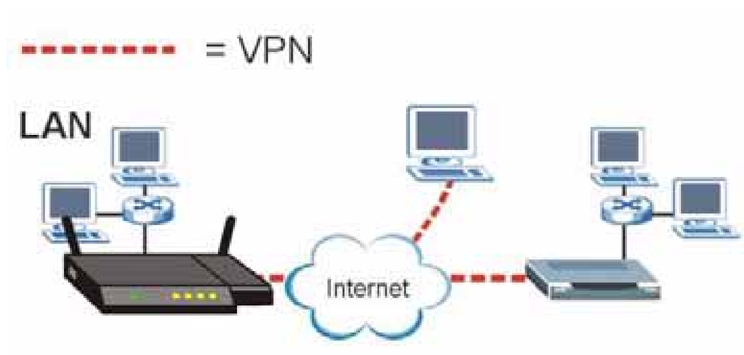
Figure 2 Redundant Internet Access via Ethernet or Cellular



1.4.3 VPN Application

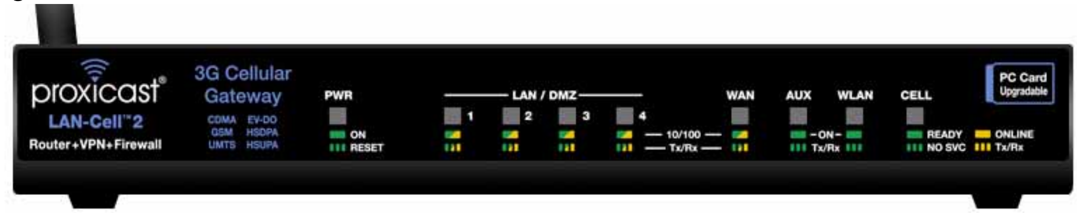
The LAN-Cell's built-in VPN feature is an ideal cost-effective way to securely connect branch offices, business partners and telecommuters over the Internet without the need (and expense) for leased lines between sites. You can make connections via the LAN-Cell's cellular, wired WAN, or dial-backup interfaces to ensure VPN connectivity regardless of the communication service available.

Figure 3 VPN Application



1.5 Front Panel Indicators

Figure 4 Front Panel



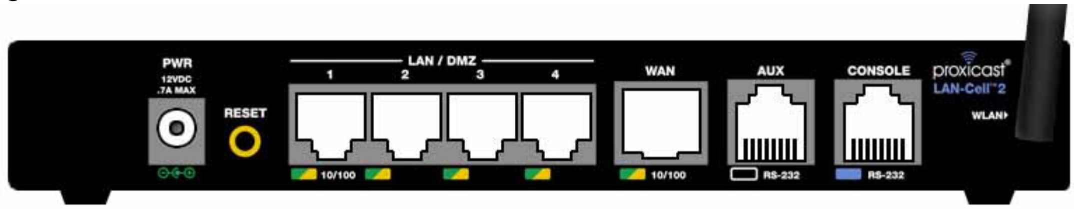
The following table describes the LAN-Cell's front panel indicator lights.

Table 1 Front Panel Lights

LED	COLOR	STATUS	DESCRIPTION
PWR		Off	The LAN-Cell is turned off.
	Green	On	The LAN-Cell is ready and running.
		Flashing	Power-on Self Test is in progress. (approximately 60 sec)
	Red	On	The power to the LAN-Cell is too low.
LAN/DMZ 1-4		Off	The LAN/DMZ is not connected.
	Green	On	The LAN-Cell has a successful 10Mbps Ethernet connection.
		Flashing	The 10M LAN is sending or receiving packets.
	Orange	On	The LAN-Cell has a successful 100Mbps Ethernet connection.
		Flashing	The 100M LAN is sending or receiving packets.
WAN		Off	The WAN connection is not ready, or has failed.
	Green	On	The LAN-Cell has a successful 10Mbps WAN connection.
		Flashing	The 10M WAN is sending or receiving packets.
	Orange	On	The LAN-Cell has a successful 100Mbps WAN connection.
		Flashing	The 100M WAN is sending or receiving packets.
AUX	Green	Off	The dial backup port is not connected to a remote server.
		On	The dial backup port is connected to a remote server.
		Flashing	The dial backup port is sending or receiving packets.
WLAN	Green	Off	The wireless LAN is not ready, or has failed.
		On	The wireless LAN is ready.
		Flashing	The wireless LAN is sending or receiving packets.
CELL		Off	There is no 3G card inserted in the LAN-Cell.
	Green	Flashing	3G card is initializing OR is not registered on the carrier network OR there is no compatible cellular service available.
		On	A 3G card ready to make a connection (dial).
	Orange	On	The 3G WAN connection is established.
		Flashing	The 3G WAN is sending or receiving packets.
	Green/ Orange	Flashing	Cellular signal strength or quality is Poor. Connections may be unreliable.

1.6 Rear Panel Connections

Figure 5 Rear Panel



The following table describes the LAN-Cell 2's rear panel connections.

Table 2 Rear Panel Connections

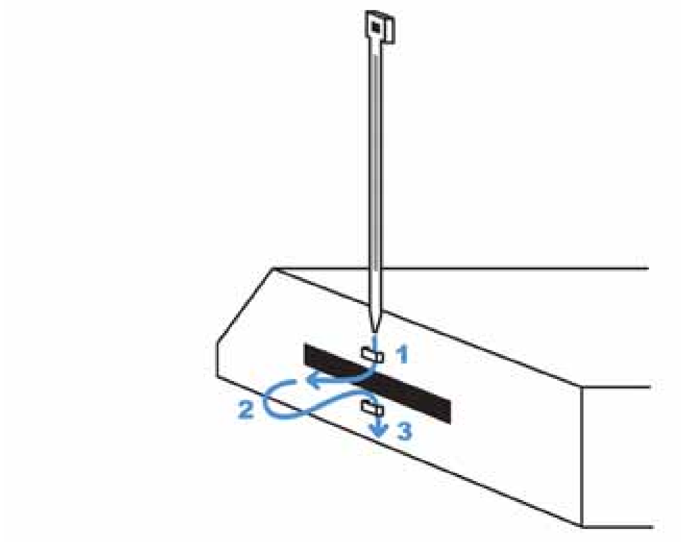
LABEL	DESCRIPTION
PWR	Connect the included 12V DC power adapter to this power jack.
RESET	To erase all user-entered settings, press & hold the reset button with a small object such as a paperclip for approximately 10 seconds until the PWR LED begins to flash. This returns the LAN-Cell to its factory default settings (LAN IP = 192.168.1.1 Password = 1234).
LAN/DMZ 1-4	Connect computer equipment to these ports with Ethernet cables. These ports are auto-negotiating (can connect at 10 or 100 Mbps) and auto-sensing (automatically adjust to the type of Ethernet cable you use, straight-through or crossover). Set the ports as LAN or DMZ in the web configurator.
WAN	Connect a cable/DSL modem or other 10/100 Ethernet-based WAN equipment to this port.
AUX	Connect an analog modem's RS-232 interface to the AUX port using the **Black** dial backup cable. The AUX port is used only to provide modem dial-backup support for the wired WAN and Cellular Modem interfaces. The default AUX port communication parameters are: 115200 bps, no parity, 8 data bits, 1 stop bit, hardware flow control..
CONSOLE	Use the **Blue** serial cable to connect a terminal or PC-terminal emulation program to the LAN-Cell for diagnostic access. The default Console Port communication parameters are: 9600 bps, no parity, 8 data bits, 1 stop bit, no flow control.
WLAN	Attach the supplied cylindrical Wi-Fi antenna to this SMA-RP (reverse polarity) connector if you will be using the LAN-Cell's integrated 802.11 a/b/g/ access point. **Attaching other types of antennas (such antennas with standard SMA, TNC or FME connectors) to this jack may damage the antennas and/or WLAN antenna jack!**
3G CARD SLOT	Insert an activated 3G PC-Card cellular modem into the slot on the right side of the LAN-Cell. **Always power off the LAN-Cell before inserting or removing PC-Cards, otherwise damage to the LAN Cell or the PC-Card may result**.

1.7 Card-Lock

The LAN-Cell 2's Card-Lock system provides a mechanism for securing the PC Card modem to prevent it from coming loose in mobile applications.

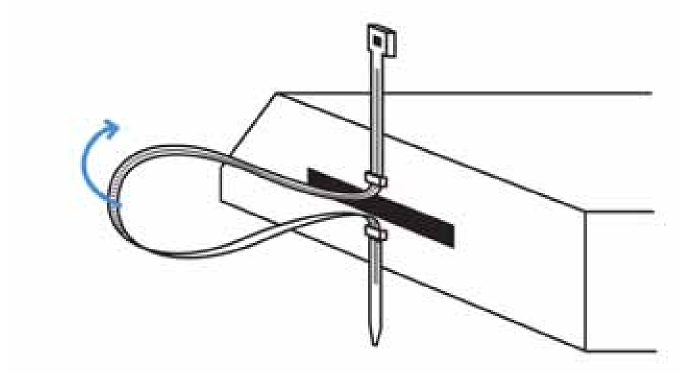
1 Insert a cable-tie through the two Card-Lock brackets above and below the PC-Card slot (Figure 6) leaving enough slack to accommodate the portion of the PC-Card that extends outside of the LAN-Cell.

Figure 6 Card-Lock Step 1



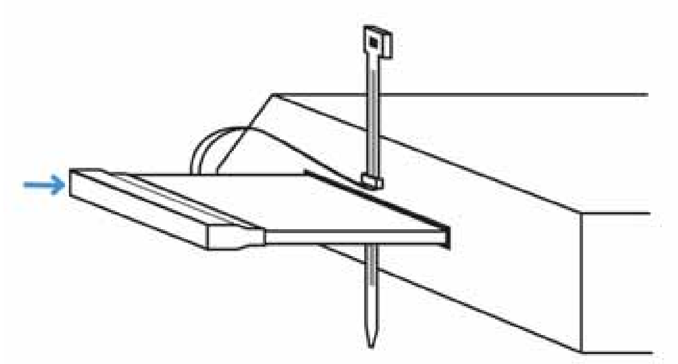
2 Rotate the loop toward the front of the LAN-Cell (Figure 7).

Figure 7 Card-Lock Step 2



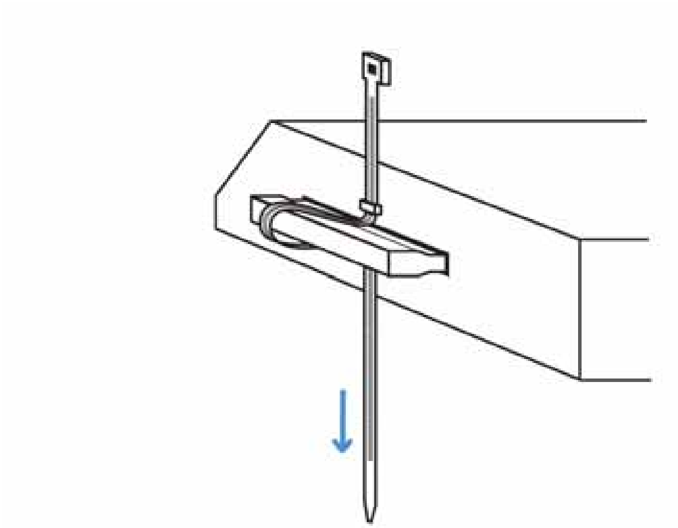
3 Insert the PC-Card modem into the card slot, keeping the cable-tie loop toward the front of the LAN-Cell (Figure 8).

Figure 8 Card-Lock Step 3



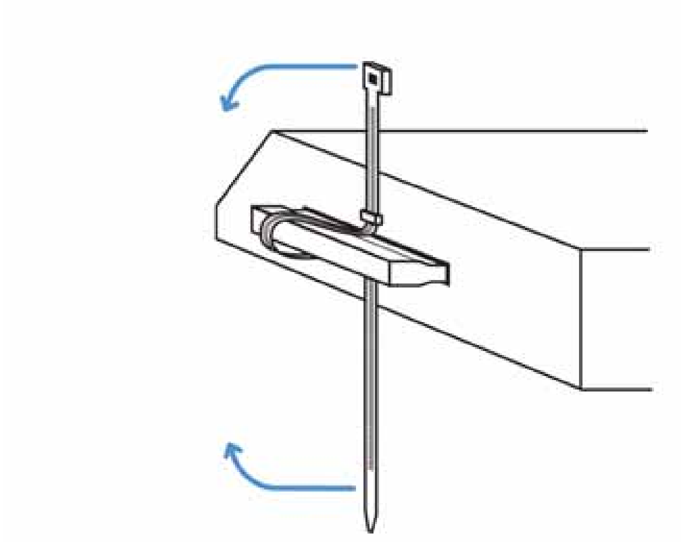
4 Once the PC-Card is inserted, slide the loop over the protruding end of the card and pull the bottom of the cable-tie straight down to tighten the loop against the card (Figure 9).

Figure 9 Card-Lock Step 4



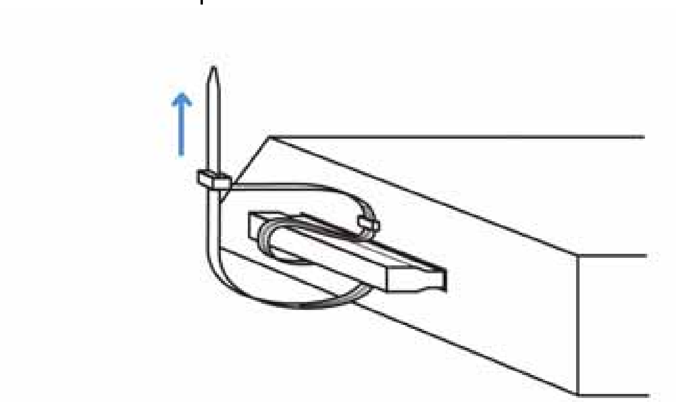
5 Bring the bottom of the cable-tie up to secure it with the cable-tie lock (Figure 10).

Figure 10 Card-Lock Step 5



6 Tighten the cable-tie against the PC Card (Figure 11).

Figure 11 Card-Lock Step 6



You may also wish to lock the PC Card's external antenna "pig-tail" cable inside the cable-tie loop to minimize movement of the antenna cable.

2

Introducing the Web Configurator & Home Screen

This chapter describes how to access the LAN-Cell web configurator and provides an overview of its screens.

2.1 Web Configurator Overview

The web configurator is an HTML-based management interface that allows easy LAN-Cell setup and management via Internet browser. Use Internet Explorer 6.0 and later or Netscape Navigator 7.0 and later versions. The recommended screen resolution is 1024 by 768 pixels.

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

- Web browser pop-up windows from your device. Web pop-up blocking is enabled by default in Windows XP SP (Service Pack) 2.
- JavaScripts (enabled by default).
- Java permissions (enabled by default).

See Appendix A on page 583 if you want to make sure these functions are allowed in Internet Explorer or Netscape Navigator.

2.2 Accessing the LAN-Cell Web Configurator

By default, the packets from WLAN to WLAN/LAN-Cell are dropped and users cannot configure the LAN-Cell wirelessly. We do not recommend configuring the LAN-Cell via a WLAN connection.

1. Make sure your LAN-Cell hardware is properly connected and prepare your computer/computer network to connect to the LAN-Cell (refer to the Quick Start Guide).
2. Launch your web browser.
3. Type "192.168.1.1" as the URL. The LAN-Cell Login screen will appear Figure 12)

Figure 12 Web Configurator Login Screen

4 Type "1234" (default) as the password and click **Login**.

5 You should see a screen (Figure 13) asking you to change your password (highly recommended). Type a new password (and retype it to confirm) and click **Apply** or click **Ignore**.

Figure 13 Change Password Screen

6 Click **Apply** in the **Replace Certificate** screen (Figure 14) to create a certificate using your LAN-Cell's MAC address that will be specific to this device.

If you do not replace the default certificate here or in the **CERTIFICATES** screen, this screen displays every time you access the web configurator.

Figure 14 Replace Certificate Screen

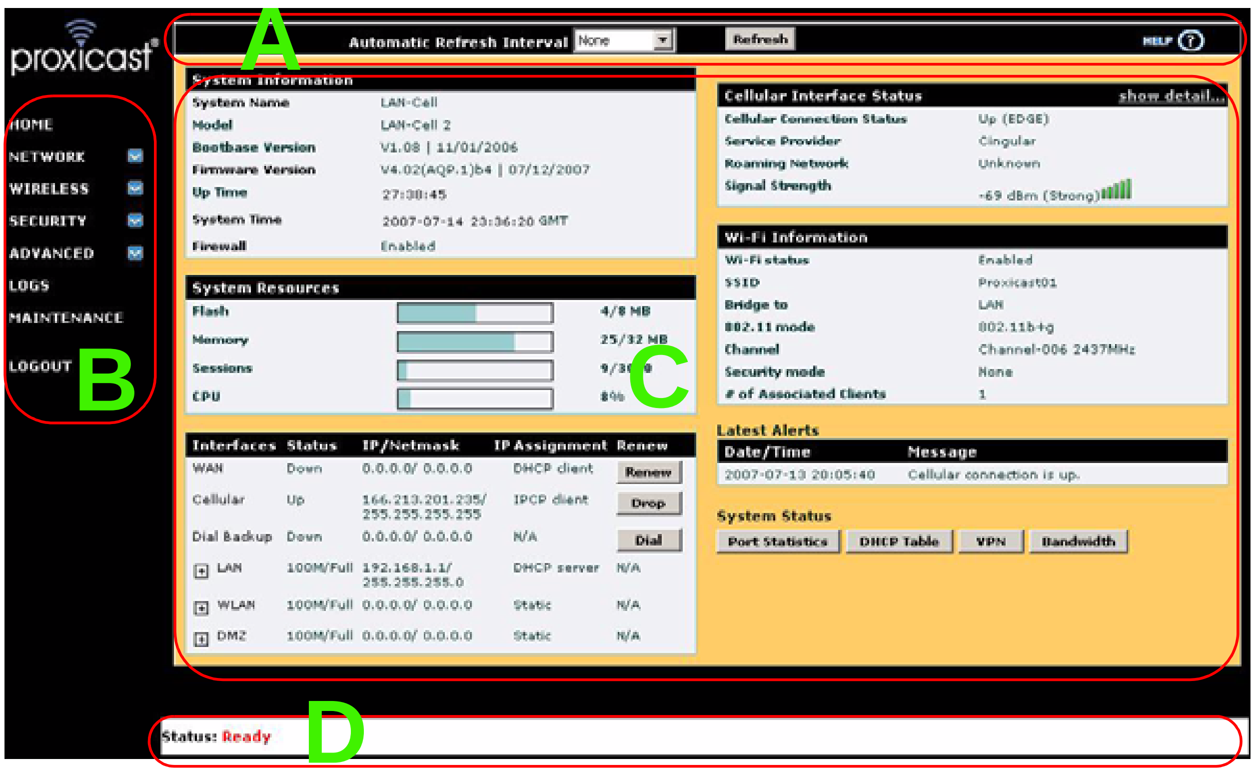
7 You should now see the **HOME** screen (see Figure 16 on page 41).

The management session automatically times out when the time period set in the **Administrator Inactivity Timer** field expires (default five minutes). Simply log back into the LAN-Cell if this happens to you.

2.3 Navigating the LAN-Cell Web Configurator

The following summarizes how to navigate the web configurator from the **HOME** screen.

Figure 15 HOME Screen



As illustrated above, the main screen is divided into these parts:

- **A** - Title Bar
- **B** - Navigation Panel
- **C** - Main Window
- **D** - Status Bar

2.3.1 Title Bar

The title bar contains the Help icon in the upper right corner.

2.3.2 Navigation Panel

The following table describes the sub-menus on the left side navigation panel.

Table 3 Screens Summary

LINK	TAB	FUNCTION
HOME		This screen shows the LAN-Cell's general device and network status information. Use this screen to access the wizards, statistics and DHCP table.
NETWORK		
LAN	LAN	Use this screen to configure LAN DHCP and TCP/IP settings.
	Static DHCP	Use this screen to assign fixed IP addresses on the LAN.
	IP Alias	Use this screen to partition your LAN interface into subnets.
	Port Roles	Use this screen to change the LAN/DMZ/WLAN port roles.
WAN	General	This screen allows you to configure load balancing, route priority and traffic redirect properties.
	WAN	Use this screen to configure the WAN connection for Internet access.
	Cellular	Use this screen to configure the Cellular connection for Internet access.
	Traffic Redirect	Use this screen to configure your traffic redirect properties and parameters.
	Dial Backup	Use this screen to configure the backup WAN dial-up connection.
DMZ	DMZ	Use this screen to configure your DMZ connection.
	Static DHCP	Use this screen to assign fixed IP addresses on the DMZ.
	IP Alias	Use this screen to partition your DMZ interface into subnets.
	Port Roles	Use this screen to change the LAN/DMZ/WLAN port roles on the LAN-Cell.
WLAN	WLAN	Use this screen to configure your WLAN connection.
	Static DHCP	Use this screen to assign fixed IP addresses on the WLAN.
	IP Alias	Use this screen to partition your WLAN interface into subnets.
	Port Roles	Use this screen to change the LAN/DMZ/WLAN port roles on the LAN-Cell.
WIRELESS		
CELLULAR		Use this screen to configure the Cellular connection for Internet access.
Wi-Fi	Wi-Fi Configuration	Use this screen to configure the internal Wi-Fi Access Point settings.
	Security	Use this screen to configure the WLAN security settings.
	MAC Filter	Use this screen to change MAC filter settings on the LAN-Cell
SECURITY		

Table 3 Screens Summary (continued)

LINK	TAB	FUNCTION
FIREWALL	Default Rule	Use this screen to activate/deactivate the firewall and the direction of network traffic to which to apply the rule
	Rule Summary	This screen shows a summary of the firewall rules, and allows you to edit/add a firewall rule.
	Anti-Probing	Use this screen to change your anti-probing settings.
	Threshold	Use this screen to configure the threshold for DoS attacks.
	Service	Use this screen to configure custom services.
VPN WIZARD		Use this Wizard to be prompted through the process of setting up a basic IPSec VPN connection.
VPN CONFIG	VPN Rules (IKE)	Use this screen to configure VPN connections using IKE key management and view the rule summary.
	VPN Rules (Manual)	Use this screen to configure VPN connections using manual key management and view the rule summary.
	SA Monitor	Use this screen to display and manage active VPN connections.
	Global Setting	Use this screen to configure the IPSec timer settings.
CERTIFICATES	My Certificates	Use this screen to view a summary list of certificates and manage certificates and certification requests.
	Trusted CAs	Use this screen to view and manage the list of the trusted CAs.
	Trusted Remote Hosts	Use this screen to view and manage the certificates belonging to the trusted remote hosts.
	Directory Servers	Use this screen to view and manage the list of the directory servers.
AUTH SERVER	Local User Database	Use this screen to configure the local user account(s) on the LAN-Cell.
	RADIUS	Configure this screen to use an external server to authenticate wireless and/or VPN users.
ADVANCED		
NAT	NAT Overview	Use this screen to enable NAT.
	Address Mapping	Use this screen to configure network address translation mapping rules.
	Port Forwarding	Use this screen to configure servers behind the LAN-Cell.
	Port Triggering	Use this screen to change your LAN-Cell’s port triggering settings.
DNS	System	Use this screen to configure the address and name server records.
	Cache	Use this screen to configure the DNS resolution cache.
	DHCP	Use this screen to configure LAN/DMZ/WLAN DNS information.
	DDNS	Use this screen to set up dynamic DNS.

Table 3 Screens Summary (continued)

LINK	TAB	FUNCTION
REMOTE MGMT	WWW	Use this screen to configure through which interface(s) and from which IP address(es) users can use HTTPS or HTTP to manage the LAN-Cell.
	SSH	Use this screen to configure through which interface(s) and from which IP address(es) users can use Secure Shell to manage the LAN-Cell.
	TELNET	Use this screen to configure through which interface(s) and from which IP address(es) users can use Telnet to manage the LAN-Cell.
	FTP	Use this screen to configure through which interface(s) and from which IP address(es) users can use FTP to access the LAN-Cell.
	SNMP	Use this screen to configure your LAN-Cell's settings for Simple Network Management Protocol management.
	DNS	Use this screen to configure through which interface(s) and from which IP address(es) users can send DNS queries to the LAN-Cell.
STATIC ROUTE	IP Static Route	Use this screen to configure IP static routes.
POLICY ROUTE	Policy Route Summary	Use this screen to view a summary list of all the policies and configure policies for use in IP policy routing.
BW MGMT	Summary	Use this screen to enable bandwidth management on an interface.
	Class Setup	Use this screen to set up the bandwidth classes.
	Monitor	Use this screen to view the LAN-Cell's bandwidth usage and allotments.
Custom APP	Custom App	Use this screen to specify port numbers for the LAN-Cell to monitor for FTP, HTTP, SMTP, POP3, H323, and SIP traffic.
ALG	ALG	Use this screen to allow certain applications to pass through the LAN-Cell.
LOGS	View Log	Use this screen to view the logs for the categories that you selected.
	Log Settings	Use this screen to change your LAN-Cell's log settings.
MAINTENANCE	General	This screen contains administrative.
	Password	Use this screen to change your password.
	Time and Date	Use this screen to change your LAN-Cell's time and date.
	F/W Upload	Use this screen to upload firmware to your LAN-Cell
	Backup & Restore	Use this screen to backup and restore the configuration or reset the factory defaults to your LAN-Cell.
	Restart	This screen allows you to reboot the LAN-Cell without turning the power off.
	Diagnostics	Use this screen to have the LAN-Cell generate and send diagnostic files by e-mail and/or the console port.
LOGOUT		Click this label to exit the web configurator.

2.3.3 Main Window

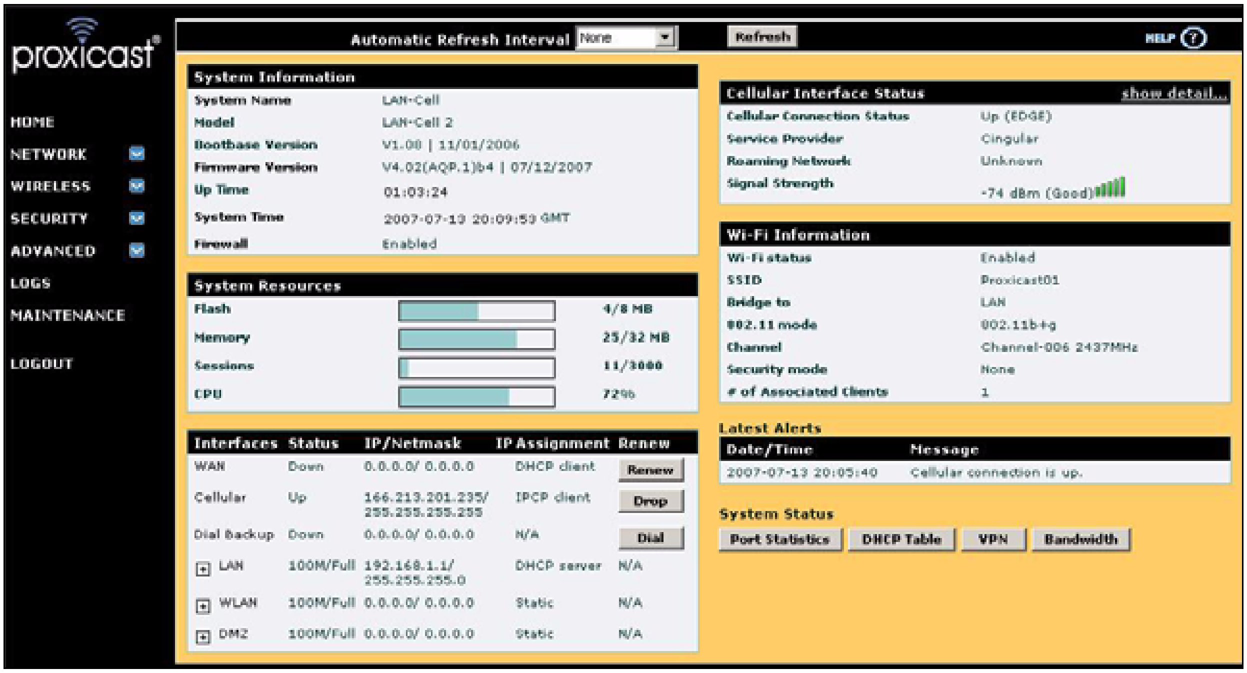
The main window shows the screen you select in the navigation panel. It is discussed in more detail in the rest of this document.

Right after you log in, the **HOME** screen is displayed.

2.3.4 HOME Screen

This screen displays general status information about the LAN-Cell.

Figure 16 Web Configurator HOME Screen



The following table describes the labels in this screen.

Table 4 Web Configurator HOME Screen

LABEL	DESCRIPTION
Automatic Refresh Interval	Select a number of seconds or **None** from the drop-down list box to update all screen statistics automatically at the end of every time interval or to not update the screen statistics.
Refresh	Click this button to update the status screen statistics immediately.
System Information	
System Name	This is the **System Name** you enter in the **MAINTENANCE > General** screen. It is for identification purposes. Click the field label to go to the screen where you can specify a name for this LAN-Cell.
Model	This is the model name of your LAN-Cell.
Bootbase Version	This is the bootbase version and the date created.
Firmware Version	This is the ProxiOS Firmware version and the date created. ProxiOS is Proxicast's proprietary Network Operating System design. Click the field label to go to the screen where you can upload a new firmware file.
Up Time	This field displays how long the LAN-Cell has been running since it last started up. The LAN-Cell starts up when you turn it on, when you restart it (**MAINTENANCE > Restart**), or when you reset it (see Section A. on page 50).

Table 4 Web Configurator HOME Screen (continued)

LABEL	DESCRIPTION
System Time	This field displays your LAN-Cell’s present date (in yyyy-mm-dd format) and time (in hh:mm:ss format) along with the difference from the Greenwich Mean Time (GMT) zone. The difference from GMT is based on the time zone. It is also adjusted for Daylight Saving Time if you set the LAN-Cell to use it. Click the field label to go to the screen where you can modify the LAN-Cell’s date and time settings.
Firewall	This displays whether or not the LAN-Cell’s firewall is activated. Click the field label to go to the screen where you can turn the firewall on or off.
System Resources	
Flash	The first number shows how many megabytes of the flash the LAN-Cell is using.
Memory	The first number shows how many megabytes of the heap memory the LAN-Cell is using. Heap memory refers to the memory that is not used by ProxiOS and is thus available for running processes like NAT, VPN and the firewall. The second number shows the LAN-Cell's total heap memory (in megabytes). The bar displays what percent of the LAN-Cell's heap memory is in use. The bar turns from green to red when the maximum is being approached.
Sessions	The first number shows how many sessions are currently open on the LAN-Cell. This includes all sessions that are currently traversing the LAN-Cell, terminating at the LAN-Cell or Initiated from the LAN-Cell The second number is the maximum number of sessions that can be open at one time. The bar displays what percent of the maximum number of sessions is in use. The bar turns from green to red when the maximum is being approached.
CPU	This field displays what percentage of the LAN-Cell’s processing ability is currently used. When this percentage is close to 100%, the LAN-Cell is running at full load, and the throughput is not going to improve anymore. If you want some applications to have more throughput, you should turn off other applications (for example, using bandwidth management.
Interfaces	This is the port type. Click "+" to expand or "-" to collapse the IP alias drop-down lists. Hold your cursor over an interface’s label to display the interface’s MAC Address. Click an interface’s label to go to the screen where you can configure settings for that interface.
Status	For the LAN, DMZ and WLAN ports, this displays the port speed and duplex setting. Ethernet port connections can be in half-duplex or full-duplex mode. Full-duplex refers to a device's ability to send and receive simultaneously, while half-duplex indicates that traffic can flow in only one direction at a time. The Ethernet port must use the same speed or duplex mode setting as the peer Ethernet port in order to connect. For the WAN interface(s) and the Dial Backup port, it displays the port speed and duplex setting if you’re using Ethernet encapsulation or the remote node name (configured through the SMT) for a PPP connection and **Down** (line is down or not connected), **Idle** (line (ppp) idle), **Dial** (starting to trigger a call) or **Drop** (dropping a call) if you’re using PPPoE encapsulation.
IP/Netmask	This shows the port’s IP address and subnet mask.

Table 4 Web Configurator HOME Screen (continued)

LABEL	DESCRIPTION
IP Assignment	For the WAN, if the LAN-Cell gets its IP address automatically from an ISP, this displays **DHCP client** when you're using Ethernet encapsulation and **IPCP Client** when you're using PPPoE or PPTP encapsulation. **Static** displays if the WAN port is using a manually entered static (fixed) IP address. For the LAN, WLAN or DMZ, **DHCP server** displays when the LAN-Cell is set to automatically give IP address information to the computers connected to the LAN. **DHCP relay** displays when the LAN-Cell is set to forward IP address assignment requests to another DHCP server. Static displays if the LAN port is using a manually entered static (fixed) IP address. In this case, you must have another DHCP server on your LAN, or else the computers must be manually configured. For the dial backup port, this shows **N/A** when dial backup is disabled and **IPCP client** when dial backup is enabled.
Renew	If you are using Ethernet encapsulation and the WAN port is configured to get the IP address automatically from the ISP, click **Renew** to release the WAN port's dynamically assigned IP address and get the IP address afresh. Click **Dial** to dial up the PPTP, PPPoE or dial backup connection. Click **Drop** to disconnect the PPTP, PPPoE, 3G WAN or dial backup connection.
Cellular Interface Status The fields below shows up on the LAN-Cell with a 3G card inserted.	
Cellular Connection Status	This displays **Down** when the 3G connection is down or not activated. This displays **Idle** when the 3G connection is idle. This displays **Init** when the LAN-Cell is initializing the 3G card. This displays **Drop** when the LAN-Cell is dropping a call. This also displays whether the LAN-Cell is connected to a **UMTS/HSDPA**, **GPRS/EDGE** or **CDMA/EV-DO** network.
Service Provider	This displays the name of your network service provider or **Limited Service** when the signal strength is too low.
Roaming Network	Name of 3G Operator currently providing service when roaming off of the 3G card's "Home" network.
Signal Strength	This displays the strength of the signal. The signal strength mainly depends on the antenna output power and the distance between your LAN-Cell and the service provider's base station.
Last Connection Up Time	This displays how long the 3G connection has been up.
Tx Bytes	This displays the total number of data frames transmitted.
Rx Bytes	This displays the total number of data frames received.
Remaining Budget Bytes	This field is available only when you enable budget control in the Cellular screen. This shows how much data (in bytes) can still be transmitted through the cellular connection before the LAN-Cell takes the actions you specified in the Cellular screen. Click the reset link and OK in the pop-up screen to clear all counters in the Remaining Budget Bytes and Remaining Budget Time fields.
Remaining Budget Time	This field is available only when you enable budget control in the Cellular screen. This shows the amount of time (in hours and minutes) the cellular connection can still be used before the LAN-Cell takes the actions you specified in the Cellular screen.
Cellular Card Manufacturer	This displays the manufacturer of your 3G card.
Cellular Card Model	This displays the model name of your 3G card.

Table 4 Web Configurator HOME Screen (continued)

LABEL	DESCRIPTION
Cellular Card Firmware Revision	This displays the version of the firmware currently used in the 3G card.
Cellular Card IMEI	This field is available only when you insert a GSM (Global System for Mobile Communications) or UMTS (Universal Mobile Telecommunications System) cellular card. This displays the International Mobile Equipment Identity (IMEI) which is the serial number of the GSM or UMTS cellular card. The IMEI is a unique 15-digit number used to identify a mobile device.
SIM Card IMSI	This field is available only when you insert a GSM or UMTS cellular card. This displays the International Mobile Subscriber Identity (IMSI) stored in the SIM (Subscriber Identity Module) card. The SIM card is installed in a mobile device and used for authenticating a customer to the carrier network. The IMSI is a unique 15-digit number used to identify a user on a network.
Cellular Card ESN	This field is available only when you insert a CDMA (Code Division Multiple Access) cellular card. This shows the ESN (Electronic Serial Number) of the inserted CDMA cellular card in decimal and (hexadecimal) notation. The ESN is the serial number of a CDMA cellular card and is similar to the IMEI on a GSM or UMTS cellular card.
Enter PIN code	If the PIN code you specified in the Cellular screen is not the right one for the card you inserted, this field displays allowing you to enter the correct PIN code. Enter the PIN code (four to eight digits) for the inserted cellular card.
PUK Code	If you enter the PIN code incorrectly three times, the SIM card will be blocked by your ISP and you cannot use the account to access the Internet. You should get the PUK (Personal Unblocking Key) code (four to eight digits) from your ISP. Enter the PUK code to enable the SIM card. If an incorrect PUK code is entered 10 times, the SIM card will be disabled permanently. You then need to contact your ISP for a new SIM card.
New PIN Code	Configure a PIN code for the SIM card. You can specify any four to eight digits to have a new PIN code or enter the previous PIN code.
Reset budget counters, resume budget control	This field displays if you have enabled budget control but insert a cellular card with a different user account from the one for which you configured budget control. Select this option to have the LAN-Cell do budget calculation starting from 0 but use the previous settings.
Resume budget control	This field displays if you have enabled budget control but insert a cellular card with a different user account from the one for which you configured budget control. Select this option to have the LAN-Cell keep the existing statistics and continue counting.
Disable budget control	This field displays if you have enabled budget control but insert a cellular card with a different user account from the one for which you configured budget control. Select this option to disable budget control. If you want to enable and configure new budget control settings for the new user account, go to the Cellular screen. The LAN-Cell keeps the existing statistics if you do not change the budget control settings. You could reinsert the original card and enable budget control to have the LAN-Cell continue counting the budget control statistics.
Enter modem unlock code	This field only displays when you insert a cellular card and the internal modem on the cellular card is blocked. Enter a key to enable the internal modem on your cellular card. By default, the key is the last four digits of your phone number used to dial up the cellular connection. Otherwise, you need to get the key from your service provider.

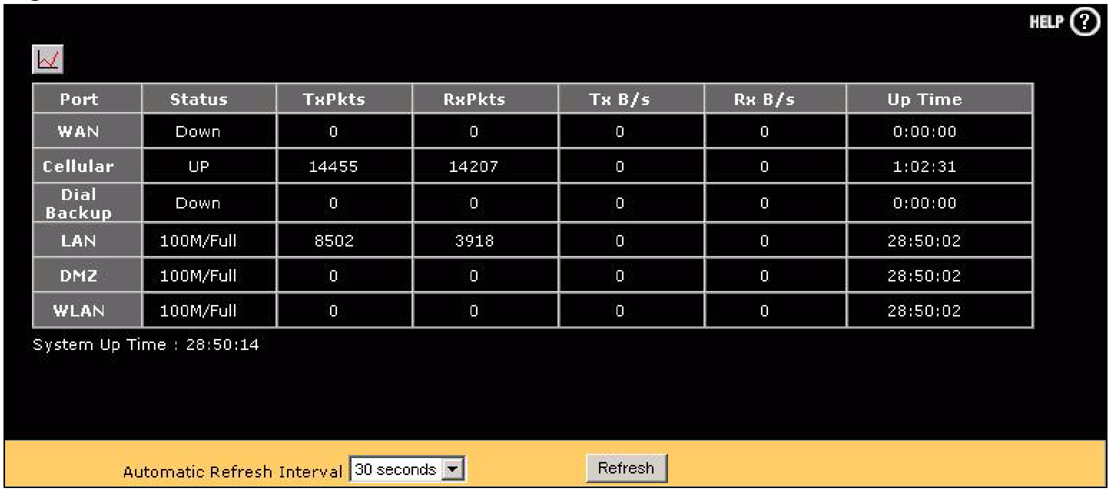
Table 4 Web Configurator HOME Screen (continued)

LABEL	DESCRIPTION
Wi-Fi Information	
Wi-Fi status	This displays whether or not the wireless LAN card is activated.
SSID	This displays a descriptive name used to identify the LAN-Cell in the wireless LAN.
Bridge To	This displays whether the wireless LAN card is used as part of the LAN, DMZ or WLAN.
802.11 Mode	This displays the wireless standard (802.11a, 802.11b, 802.11g or 802.11b+g) of the wireless LAN.
Channel	This displays the radio channel the LAN-Cell is currently using for the wireless LAN.
Security Mode	This shows the type of wireless security the LAN-Cell is using.
# of Associated Clients	This shows the number of the wireless client(s) connected to the LAN-Cell.
ALERTS	
Latest Alerts	This table displays the five most recent alerts recorded by the LAN-Cell. You can see more information in the **View Log** screen, such as the source and destination IP addresses and port numbers of the incoming packets.
Date/Time	This is the date and time the alert was recorded.
Message	This is the reason for the alert.
System Status	
Port Statistics	Click **Port Statistics** to see router performance statistics such as the number of packets sent and number of packets received for each port.
DHCP Table	Click **DHCP Table** to show current DHCP client information.
VPN	Click **VPN** to display the active VPN connections.
Bandwidth	Click **Bandwidth** to view the LAN-Cell's bandwidth usage and allotments.

2.3.5 Port Statistics

Click **Port Statistics** in the **HOME** screen. Read-only information here includes port status and packet specific statistics. The **Poll Interval(s)** field is configurable.

Figure 17 HOME > Show Statistics



The following table describes the labels in this screen.

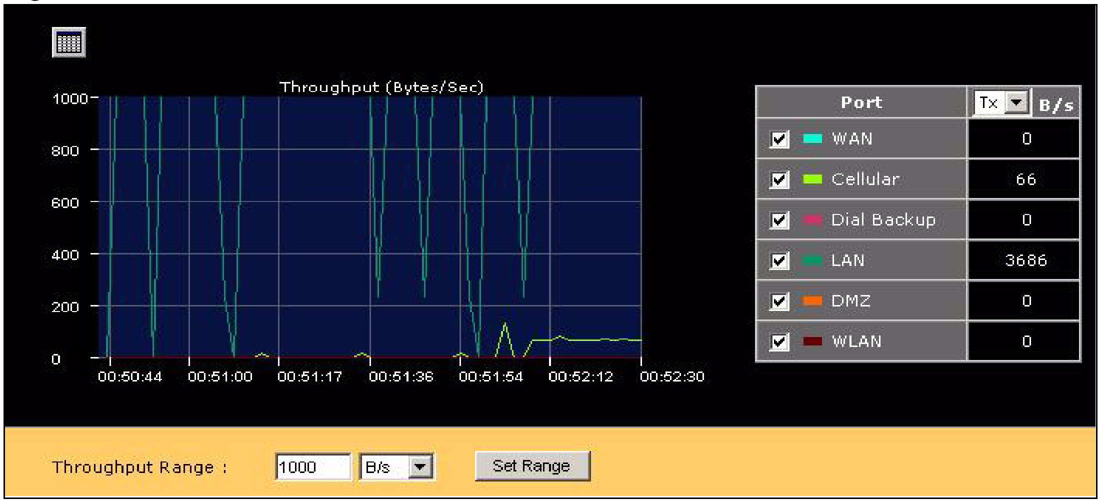
Table 5 HOME > Show Statistics

LABEL	DESCRIPTION
	Click the icon to display the chart of throughput statistics.
Port	These are the LAN-Cell's interfaces.
Status	For the WAN interface(s) and the Dial Backup port, this displays the port speed and duplex setting if you're using Ethernet encapsulation or the remote node name for a PPP connection and **Down** (line is down or not connected), **Idle** (line (ppp) idle), **Dial** (starting to trigger a call) or **Drop** (dropping a call) if you're using PPPoE encapsulation. For the LAN, DMZ and WLAN ports, this displays the port speed and duplex setting. For the WLAN card, this displays the transmission rate when WLAN is enabled or **Down** when WLAN is disabled.
TxPkts	This is the number of transmitted packets on this port.
RxPkts	This is the number of received packets on this port.
Tx B/s	This displays the transmission speed in bytes per second on this port.
Rx B/s	This displays the reception speed in bytes per second on this port.
Up Time	This is the total amount of time the line has been up.
System Up Time	This is the total time the LAN-Cell has been on.
Automatic Refresh Interval	Select a number of seconds or **None** from the drop-down list box to update all screen statistics automatically at the end of every time interval or to not update the screen statistics.
Refresh	Click this button to update the screen's statistics immediately.

2.3.6 Show Statistics: Line Chart

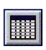
Click the icon in the **Show Statistics** screen. This screen shows you a line chart of each port's throughput statistics.

Figure 18 HOME > Show Statistics > Line Chart



The following table describes the labels in this screen.

Table 6 HOME > Show Statistics > Line Chart

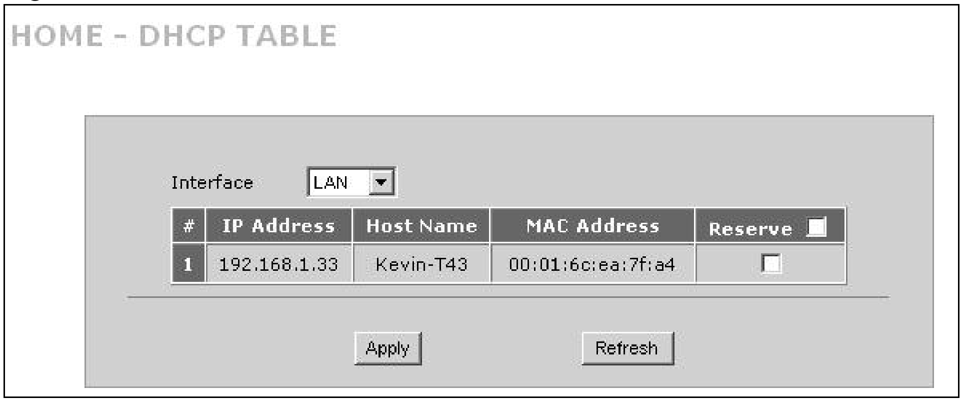
LABEL	DESCRIPTION
	Click the icon to go back to the **Show Statistics** screen.
Port	Select the check box(es) to display the throughput statistics of the corresponding interface(s).
B/s	Specify the direction of the traffic for which you want to show throughput statistics in this table. Select **Tx** to display transmitted traffic throughput statistics and the amount of traffic (in bytes). Select **Rx** to display received traffic throughput statistics and the amount of traffic (in bytes).
Throughput Range	Set the range of the throughput (in **B/s**, **KB/s** or **MB/s**) to display. Click **Set Range** to save this setting back to the LAN-Cell.

2.3.7 DHCP Table Screen

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 LAN-Cell as a DHCP server or disable it. When configured as a server, the LAN-Cell provides the TCP/IP configuration for the clients. If DHCP service is disabled, you must have another DHCP server on your LAN, or else the computer must be manually configured.

Click **Show DHCP Table** in the **HOME** screen. Read-only information here relates to your DHCP status. The DHCP table shows current DHCP client information (including **IP Address**, **Host Name** and **MAC Address**) of all network clients using the LAN-Cell's DHCP server.

Figure 19 HOME > DHCP Table



The following table describes the labels in this screen.

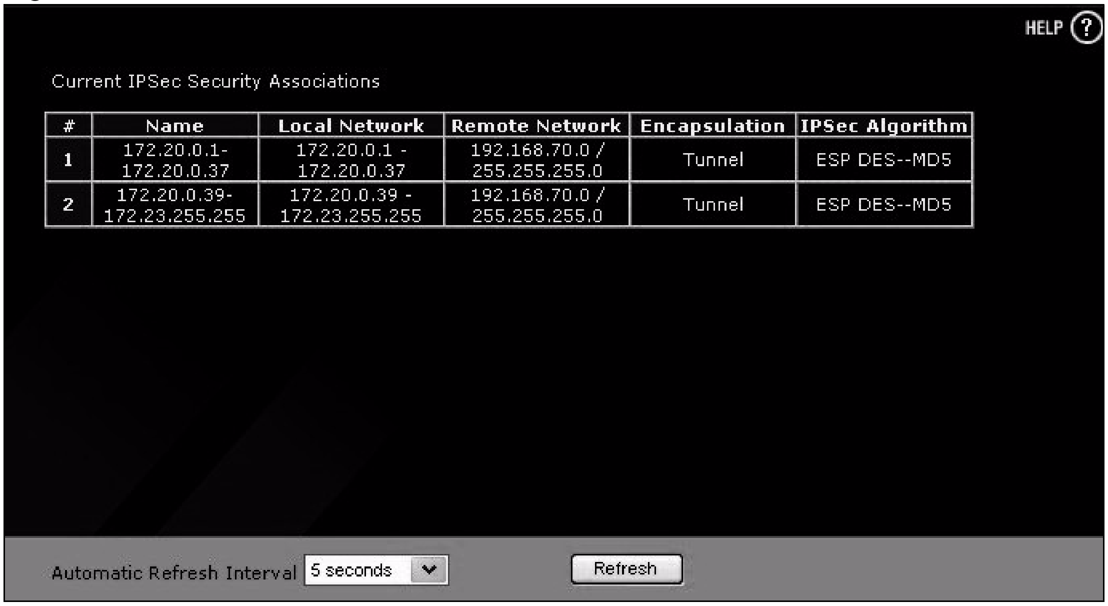
Table 7 HOME > DHCP Table

LABEL	DESCRIPTION
Interface	Select **LAN**, **DMZ** or **WLAN** to show the current DHCP client information for the specified interface.
#	This is the index number of the host computer.
IP Address	This field displays the IP address relative to the # field listed above.
Host Name	This field displays the computer host name.
MAC Address	The MAC (Media Access Control) or Ethernet address on a LAN (Local Area Network) is unique to your computer (six pairs of hexadecimal notation). A network interface card such as an Ethernet adapter has a hardwired address that is assigned at the factory. This address follows an industry standard that ensures no other adapter has a similar address.
Reserve	Select the check box in the heading row to automatically select all check boxes or select the check box(es) in each entry to have the LAN-Cell always assign the selected entry(ies)'s IP address(es) to the corresponding MAC address(es) (and host name(s)). You can select up to 128 entries in this table. After you click **Apply**, the MAC address and IP address also display in the corresponding **LAN**, **DMZ** or **WLAN Static DHCP** screen (where you can edit them).
Refresh	Click **Refresh** to reload the DHCP table.

2.3.8 VPN Status

Click **VPN** in the **HOME** screen. This screen displays read-only information about the active VPN connections. The **Poll Interval(s)** field is configurable. A Security Association (SA) is the group of security settings related to a specific VPN tunnel.

Figure 20 HOME > VPN Status



The following table describes the labels in this screen.

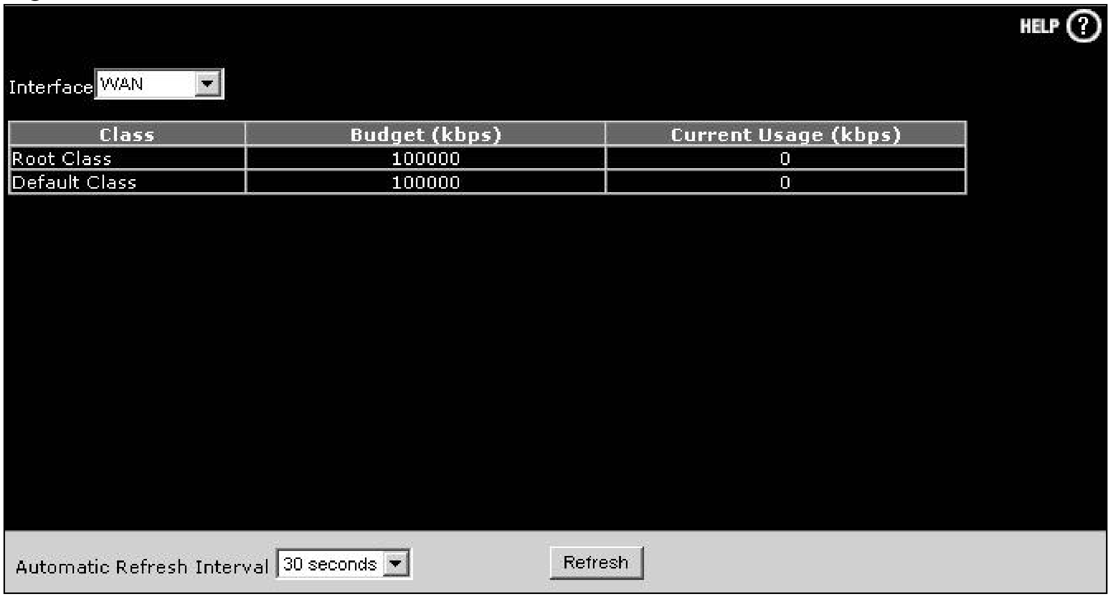
Table 8 HOME > VPN Status

LABEL	DESCRIPTION
#	This is the security association index number.
Name	This field displays the identification name for this VPN policy.
Local Network	This field displays the IP address of the computer using the VPN IPSec feature of your LAN-Cell.
Remote Network	This field displays IP address (in a range) of computers on the remote network behind the remote IPSec router.
Encapsulation	This field displays **Tunnel** or **Transport** mode.
IPSec Algorithm	This field displays the security protocols used for an SA. Both AH and ESP increase LAN-Cell processing requirements and communications latency (delay).
Automatic Refresh Interval	Select a number of seconds or **None** from the drop-down list box to update all screen statistics automatically at the end of every time interval or to not update the screen statistics.
Refresh	Click this button to update the screen's statistics immediately.

2.3.9 Bandwidth Monitor

Click **Bandwidth** in the **HOME** screen to display the bandwidth monitor. This screen displays the device's bandwidth usage and allotments.

Figure 21 Home > Bandwidth Monitor



The following table describes the labels in this screen.

Table 9 ADVANCED > BW MGMT > Monitor

LABEL	DESCRIPTION
Interface	Select an interface from the drop-down list box to view the bandwidth usage of its bandwidth classes.
Class	This field displays the name of the bandwidth class. A **Default Class** automatically displays for all the bandwidth in the **Root Class** that is not allocated to bandwidth classes. If you do not enable maximize bandwidth usage on an interface, the LAN-Cell uses the bandwidth in this default class to send traffic that does not match any of the bandwidth classes.[A]
Budget (kbps)	This field displays the amount of bandwidth allocated to the bandwidth class.
Current Usage (kbps)	This field displays the amount of bandwidth that each bandwidth class is using.
Automatic Refresh Interval	Select a number of seconds or **None** from the drop-down list box to update all screen statistics automatically at the end of every time interval or to not update the screen statistics.
Refresh	Click this button to update the screen’s statistics immediately.

A. If you allocate all the root class’s bandwidth to the bandwidth classes, the default class still displays a budget of 2 kbps (the minimum amount of bandwidth that can be assigned to a bandwidth class).

2.3.10 Status Bar

The Status Bar area displays system confirmation and error messages as you navigate through the Web Configurator. Whenever clicking “Apply” to save configuration parameters, be sure to wait for the Status Bar message “**Configuration updated successfully**” before moving to the next screen.

2.4 Resetting the LAN-Cell

If you forget your password or cannot access the web configurator, you will need to reload the factory-default configuration file or use the **RESET** button on the back of the LAN-Cell. Uploading this configuration file replaces the current configuration file with the factory-default configuration file. This means that you will lose all configurations that you had previously and the speed of the console port will be reset to the default of 9600bps with 8 data bit, no parity, one stop bit and flow control set to none. The password will be reset to 1234, also.

Make sure the **SYS** LED is on (not blinking) before you begin this procedure.

1 Press the **RESET** button for ten seconds, and then release it. If the **SYS** LED begins to blink, the defaults have been restored and the LAN-Cell restarts. Otherwise, go to step 2.
2 Turn the LAN-Cell off.
3 While pressing the **RESET** button, turn the LAN-Cell on.
4 Continue to hold the **RESET** button. The **SYS** LED will begin to blink and flicker very quickly after about 20 seconds. This indicates that the defaults have been restored and the LAN-Cell is now restarting.

Release the **RESET** button and wait for the LAN-Cell to finish restarting.

3

Tutorials: 3G Modem Setup & VPN Wizard

This chapter describes how to set up a 3G Cellular PC-Card modem WAN connection and how to configure a basic VPN using the VPN Wizard and firewall security settings.

3.1 Setting Up a 3G WAN Connection

3.1.1 Inserting a 3G PC-Card

To enable and use the 3G WAN connection, you need to insert a 3G PC-Card in the LAN-Cell.

Turn the LAN-Cell off before you install or remove a 3G card.

1 After obtaining a 3G PC-Card modem from your cellular service provider, ensure that it is properly configured and activated on their network by using the PC-Card in a Windows laptop to make a 3G network connection. PC-Card firmware updates and device activation must be done using the software tools provided by your carrier or the PC-Card manufacturer.

1 Make sure the LAN-Cell is off before inserting or removing a card (to avoid damage).

2 Slide the connector end of the 3G card firmly and completely into the slot.

3 Power on the LAN-Cell.

The LAN-Cell supports a specific list of 3G Cellular PC-Card modems including devices for GSM, GPRS, EDGE, HSDPA, HSUPA, UMTS, CDMA, 1xRTT and EV-DO carrier networks worldwide. ExpressCard modems are supported using a PC-Card to ExpressCard adapter cradle.

Refer to the firmware *Release Notes* or the Proxicast Support Web site for the list of 3G PC-Cards supported in your firmware version. Support for additional 3G cards is being added continuously and may require a firmware upgrade.

3.1.2 Configuring 3G WAN Settings

You should already have an activated user account and network access information from the service provider.

1 Click **WIRELESS** > **Cellular** on the LAN-Cell.
2 Make sure that the Cellular interface is Enabled.
3 For GSM networks such as AT&T, T-Mobile, Rogers, Vodafone, Orange, MTN, etc., enter the APN (Access Point Name) and phone number (typically *99#) that were provided by your service provider.
4 For CDMA networks such as Verizon Wireless, Sprint, Alltel, Telus, etc., the APN field is not required or displayed. The ISP access phone number is typically #777 for CDMA networks.
5 Select the authentication type used by your service provider. If it was not given, leave the field at the default (None).
6 If required by your network operator, also enter the user name, password, and PIN code used for network access. If your service provider didn't provide this information, contact your service provider.
7 If you want the Cellular WAN connection to stay connected at all times, select "Always On", otherwise indicate how long to wait before the LAN-Cell drops the 3G connection when no data activity is detected. Note: this will "hang up" the 3G connection and is not the same as the radio "Dormant State" that 3G PC-Cards go into when not transmitting data.
8 For WAN IP Address Assignment, select **Get Automatically from ISP**. This is the correct setting in most situations, even if your carrier has assigned a "static" IP address to your 3G card.
9 Click **Apply**.

Figure 22 Tutorial: WIRELESS > Cellular (3G WAN) - CDMA Example

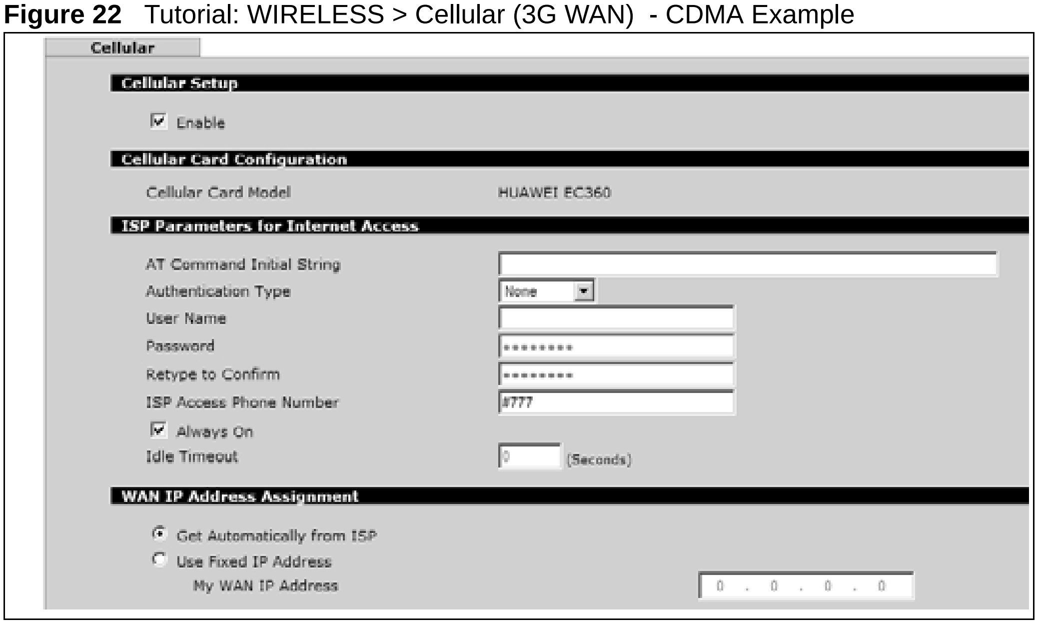
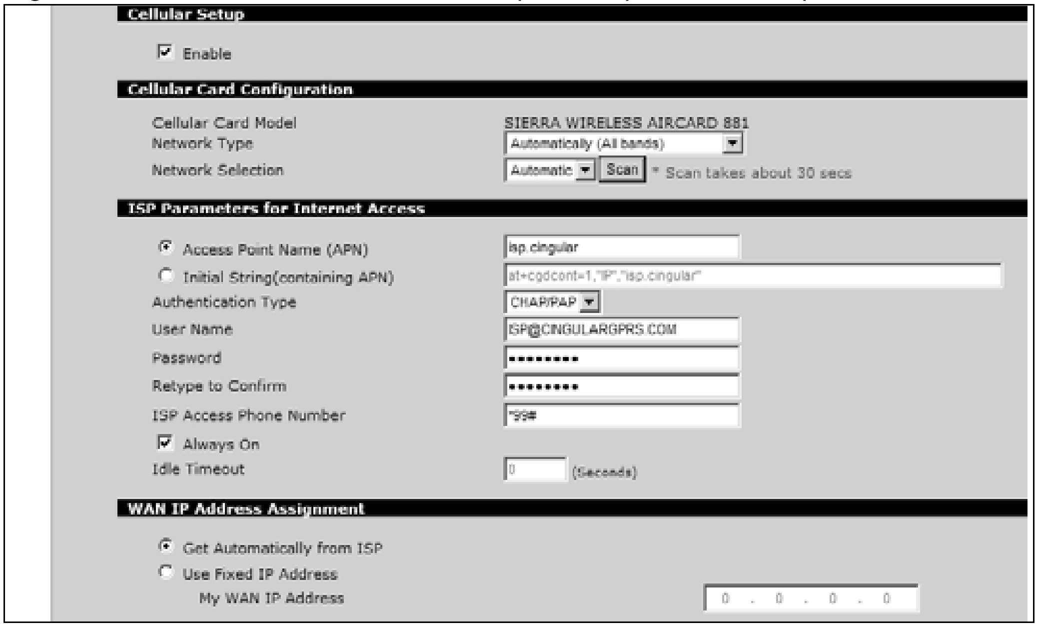


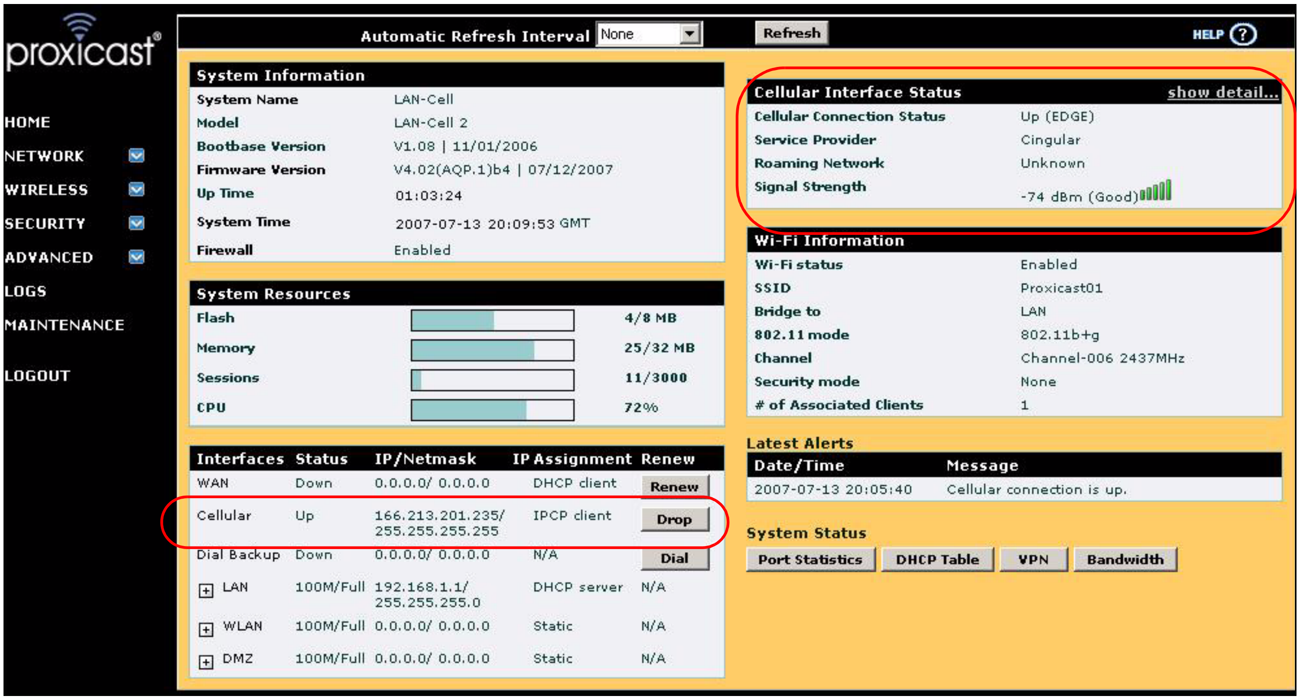
Figure 23 Tutorial: WIRELESS > Cellular (3G WAN) - GSM Example



3.1.3 Checking WAN Connections

1. Go to the web configurator’s **Home** screen.
2. In the network status table, make sure the status for **Cellular** is not **Down** and there is an IP address. If the Cellular connection is not up, make sure you have entered the correct information in the **Cellular** screen and the signal strength to the service provider’s base station is not too low.

Figure 24 Tutorial: Home



3.2 VPN Wizard Overview

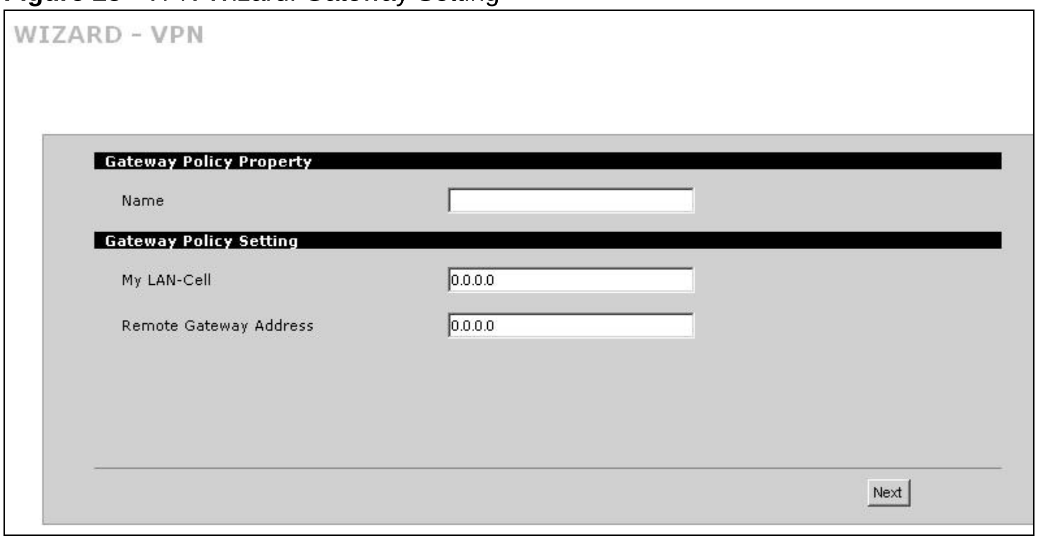
The web configurator contains a “wizard” feature to help you easily set up a basic IPSec VPN connnection.

From the left-side navigation menu, select **SECURITY** then click the **VPN Wizard** menu item to open the **VPN Wizard** screen. Use this wizard to configure a VPN connection that uses a pre-shared key. If you want to set the rule to use a certificate, please go to the **VPN Config** screens for configuration. See Section 3.2.1 on page 57.

3.2.1 VPN Wizard Gateway Setting

Use this screen to name the VPN gateway policy (IKE SA) and identify the IPSec routers at either end of the VPN tunnel.

Figure 25 VPN Wizard: Gateway Setting



The following table describes the labels in this screen.

Table 10 VPN Wizard: Gateway Setting

LABEL	DESCRIPTION
Gateway Policy Property	
Name	Type up to 32 characters to identify this VPN gateway policy. You may use any character, including spaces, but the LAN-Cell drops trailing spaces.
My LAN-Cell	Enter the WAN IP address or the domain name of your LAN-Cell or leave the field set to **0.0.0.0**. The following applies if the **My LAN-Cell** field is configured as **0.0.0.0**: When the WAN interface operation mode is set to **Active/Passive**, the LAN-Cell uses the IP address (static or dynamic) of the WAN interface that is in use. When the WAN interface operation mode is set to **Active/Active**, the LAN-Cell uses the IP address (static or dynamic) of the primary (highest priority) WAN interface to set up the VPN tunnel as long as the corresponding WAN or CELL connection is up. If the corresponding WAN or CELL connection goes down, the LAN-Cell uses the IP address of the other WAN interface. If both WAN connections go down, the LAN-Cell uses the dial backup IP address for the VPN tunnel when using dial backup or the LAN IP address when using traffic redirect. See the chapter on WAN for details on dial backup and traffic redirect.

Table 10 VPN Wizard: Gateway Setting

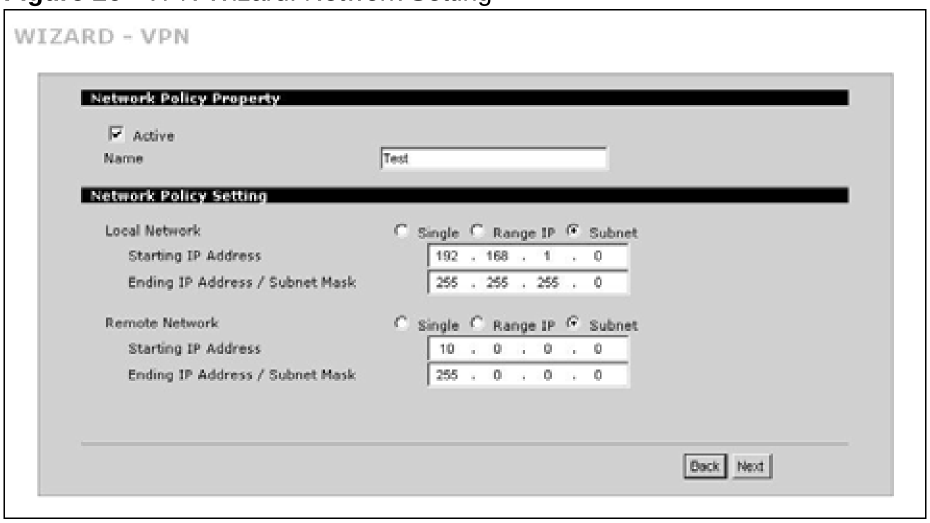
LABEL	DESCRIPTION
Remote Gateway Address	Enter the WAN IP address or domain name of the remote IPSec router (secure gateway) in the field below to identify the remote IPSec router by its IP address or a domain name. Set this field to **0.0.0.0** if the remote IPSec router has a dynamic WAN IP address.
Back	Click **Back** to return to the previous screen.
Next	Click **Next** to continue.

3.2.2 VPN Wizard Network Setting

Use this screen to name the VPN network policy (IPSec SA) and identify the devices behind the IPSec routers at either end of a VPN tunnel.

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.

Figure 26 VPN Wizard: Network Setting



The following table describes the labels in this screen.

Table 11 VPN Wizard: Network Setting

LABEL	DESCRIPTION
Network Policy Property	
Active	If the **Active** check box is selected, packets for the tunnel trigger the LAN-Cell to build the tunnel. Clear the **Active** check box to turn the network policy off. The LAN-Cell does not apply the policy. Packets for the tunnel do not trigger the tunnel.
Name	Type up to 32 characters to identify this VPN network policy. You may use any character, including spaces, but the LAN-Cell drops trailing spaces.
Network Policy Setting	

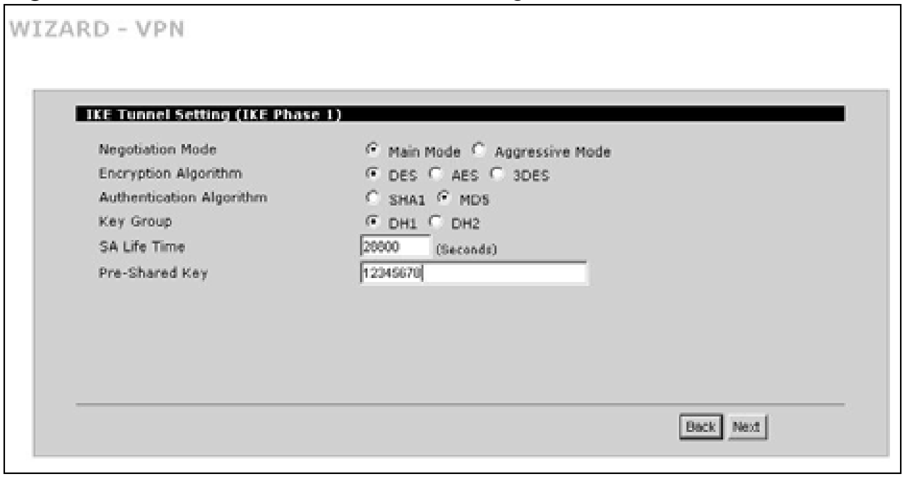
Table 11 VPN Wizard: Network Setting

LABEL	DESCRIPTION
Local Network	Local IP addresses must be static and correspond to the remote IPSec router's configured remote IP addresses. Select **Single** for a single IP address. Select **Range IP** for a specific range of IP addresses. Select **Subnet** to specify IP addresses on a network by their subnet mask.
Starting IP Address	When the **Local Network** field is configured to **Single**, enter a (static) IP address on the LAN behind your LAN-Cell. When the **Local Network** field is configured to **Range IP**, enter the beginning (static) IP address, in a range of computers on the LAN behind your LAN-Cell. When the **Local Network** field is configured to **Subnet**, this is a (static) IP address on the LAN behind your LAN-Cell.
Ending IP Address/ Subnet Mask	When the **Local Network** field is configured to **Single**, this field is N/A. When the **Local Network** field is configured to **Range IP**, enter the end (static) IP address, in a range of computers on the LAN behind your LAN-Cell. When the **Local Network** field is configured to **Subnet**, this is a subnet mask on the LAN behind your LAN-Cell.
Remote Network	Remote IP addresses must be static and correspond to the remote IPSec router's configured local IP addresses. Select **Single** for a single IP address. Select **Range IP** for a specific range of IP addresses. Select **Subnet** to specify IP addresses on a network by their subnet mask.
Starting IP Address	When the **Remote Network** field is configured to **Single**, enter a (static) IP address on the network behind the remote IPSec router. When the **Remote Network** field is configured to **Range IP**, enter the beginning (static) IP address, in a range of computers on the network behind the remote IPSec router. When the **Remote Network** field is configured to **Subnet**, enter a (static) IP address on the network behind the remote IPSec router
Ending IP Address/ Subnet Mask	When the **Remote Network** field is configured to **Single**, this field is N/A. When the **Remote Network** field is configured to **Range IP**, enter the end (static) IP address, in a range of computers on the network behind the remote IPSec router. When the **Remote Network** field is configured to **Subnet**, enter a subnet mask on the network behind the remote IPSec router.
Back	Click **Back** to return to the previous screen.
Next	Click **Next** to continue.

3.2.3 VPN Wizard IKE Tunnel Setting (IKE Phase 1)

Use this screen to specify the authentication, encryption and other settings needed to negotiate a phase 1 IKE SA.

Figure 27 VPN Wizard: IKE Tunnel Setting



The following table describes the labels in this screen.

Table 12 VPN Wizard: IKE Tunnel Setting

LABEL	DESCRIPTION
Negotiation Mode	Select **Main Mode** for identity protection. Select **Aggressive Mode** to allow more incoming connections from dynamic IP addresses to use separate passwords. Note: Multiple SAs (security associations) connecting through a secure gateway must have the same negotiation mode.
Encryption Algorithm	When **DES** is used for data communications, both sender and receiver must know the same secret key, which can be used to encrypt and decrypt the message or to generate and verify a message authentication code. 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. This implementation of **AES** uses a 128-bit key. **AES** is faster than **3DES**.
Authentication Algorithm	**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.
Key Group	You must choose a key group for phase 1 IKE setup. **DH1** (default) refers to Diffie-Hellman Group 1 a 768 bit random number. **DH2** refers to Diffie-Hellman Group 2 a 1024 bit (1Kb) random number.
SA Life Time (Seconds)	Define the length of time before an IKE SA automatically renegotiates in this field. The minimum value is 180 seconds. 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.

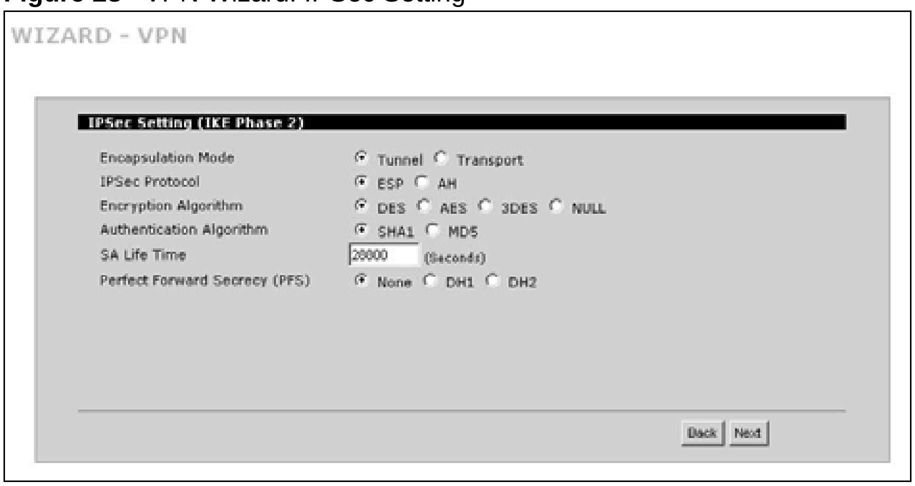
Table 12 VPN Wizard: IKE Tunnel Setting (continued)

LABEL	DESCRIPTION
Pre-Shared Key	Type your pre-shared key in this field. 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. Type from 8 to 31 case-sensitive ASCII characters or from 16 to 62 hexadecimal ("0-9", "A-F") characters. You must precede a hexadecimal key with a "0x (zero x), which is not counted as part of the 16 to 62 character range for the key. For example, in "0x0123456789ABCDEF", 0x denotes that the key is hexadecimal and 0123456789ABCDEF is the key itself. Both ends of the VPN tunnel must use the same pre-shared key. You will receive a PYLD_MALFORMED (payload malformed) packet if the same pre-shared key is not used on both ends.
Back	Click **Back** to return to the previous screen.
Next	Click **Next** to continue.

3.2.4 VPN Wizard IPSec Setting (IKE Phase 2)

Use this screen to specify the authentication, encryption and other settings needed to negotiate a phase 2 IPSec SA.

Figure 28 VPN Wizard: IPSec Setting



The following table describes the labels in this screen.

Table 13 VPN Wizard: IPSec Setting

LABEL	DESCRIPTION
Encapsulation Mode	**Tunnel** is compatible with NAT, **Transport** is not. 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. 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).
IPSec Protocol	Select the security protocols used for an SA. Both **AH** and **ESP** increase LAN-Cell processing requirements and communications latency (delay).

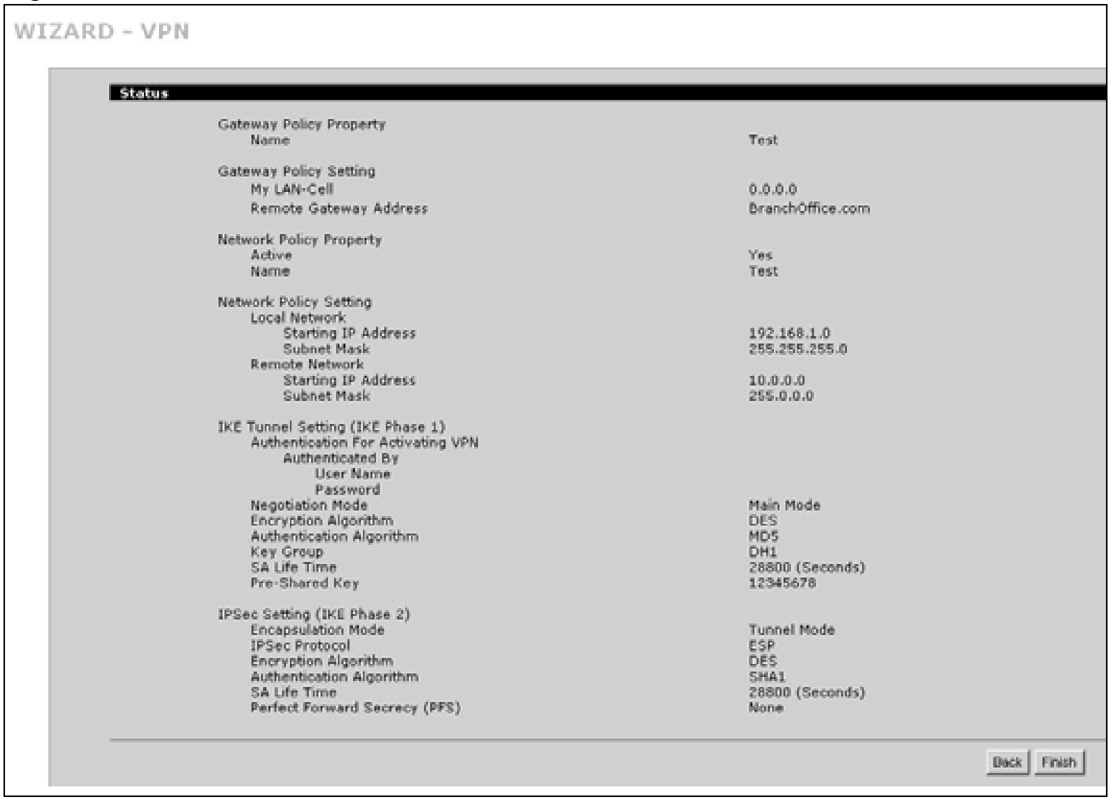
Table 13 VPN Wizard: IPSec Setting (continued)

LABEL	DESCRIPTION
Encryption Algorithm	When **DES** is used for data communications, both sender and receiver must know the same secret key, which can be used to encrypt and decrypt the message or to generate and verify a message authentication code. 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. This implementation of **AES** uses a 128-bit key. **AES** is faster than **3DES**. Select **NULL** to set up a tunnel without encryption. When you select **NULL**, you do not enter an encryption key.
Authentication Algorithm	**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.
SA Life Time (Seconds)	Define the length of time before an IKE SA automatically renegotiates in this field. The minimum value is 180 seconds. 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 Secret (PFS)	Perfect Forward Secret (PFS) is disabled (**None**) by default in phase 2 IPSec SA setup. This allows faster IPSec setup, but is not so secure. Select **DH1** or **DH2** to enable PFS. **DH1** refers to Diffie-Hellman Group 1 a 768 bit random number. **DH2** refers to Diffie-Hellman Group 2 a 1024 bit (1Kb) random number (more secure, yet slower).
Back	Click **Back** to return to the previous screen.
Next	Click **Next** to continue.

3.2.5 VPN Wizard Status Summary

This read-only screen shows the status of the current VPN setting. Use the summary table to check whether what you have configured is correct.

Figure 29 VPN Wizard: VPN Status



The following table describes the labels in this screen.

Table 14 VPN Wizard: VPN Status

LABEL	DESCRIPTION
Gateway Policy Property	
Name	This is the name of this VPN gateway policy.
Gateway Policy Setting	
My LAN-Cell	This is the WAN IP address or the domain name of your LAN-Cell.
Remote Gateway Address	This is the IP address or the domain name used to identify the remote IPSec router.
Network Policy Property	
Active	This displays whether this VPN network policy is enabled or not.
Name	This is the name of this VPN network policy.
Network Policy Setting	
Local Network	
Starting IP Address	This is a (static) IP address on the LAN behind your LAN-Cell.
Ending IP Address/ Subnet Mask	When the local network is configured for a single IP address, this field is N/A. When the local network is configured for a range IP address, this is the end (static) IP address, in a range of computers on the LAN behind your LAN-Cell. When the local network is configured for a subnet, this is a subnet mask on the LAN behind your LAN-Cell.

Table 14 VPN Wizard: VPN Status (continued)

LABEL	DESCRIPTION
Remote Network	
Starting IP Address	This is a (static) IP address on the network behind the remote IPSec router.
Ending IP Address/ Subnet Mask	When the remote network is configured for a single IP address, this field is N/A. When the remote network is configured for a range IP address, this is the end (static) IP address, in a range of computers on the network behind the remote IPSec router. When the remote network is configured for a subnet, this is a subnet mask on the network behind the remote IPSec router.
IKE Tunnel Setting (IKE Phase 1)	
Negotiation Mode	This shows **Main Mode** or **Aggressive Mode**. Multiple SAs connecting through a secure gateway must have the same negotiation mode.
Encryption Algorithm	This is the method of data encryption. Options can be **DES**, **3DES** or **AES**.
Authentication Algorithm	**MD5** (Message Digest 5) and **SHA1** (Secure Hash Algorithm) are hash algorithms used to authenticate packet data.
Key Group	This is the key group you chose for phase 1 IKE setup.
SA Life Time (Seconds)	This is the length of time before an IKE SA automatically renegotiates.
Pre-Shared Key	This is a pre-shared key identifying a communicating party during a phase 1 IKE negotiation.
IPSec Setting (IKE Phase 2)	
Encapsulation Mode	This shows **Tunnel** mode or **Transport** mode.
IPSec Protocol	**ESP** or **AH** are the security protocols used for an SA.
Encryption Algorithm	This is the method of data encryption. Options can be **DES**, **3DES**, **AES** or **NULL**.
Authentication Algorithm	**MD5** (Message Digest 5) and **SHA1** (Secure Hash Algorithm) are hash algorithms used to authenticate packet data.
SA Life Time (Seconds)	This is the length of time before an IKE SA automatically renegotiates.
Perfect Forward Secret (PFS)	Perfect Forward Secret (PFS) is disabled (**None**) by default in phase 2 IPSec SA setup. Otherwise, **DH1** or **DH2** are selected to enable PFS.
Back	Click **Back** to return to the previous screen.
Finish	Click **Finish** to complete and save the wizard setup.

3.2.6 VPN Wizard Setup Complete

Congratulations! You have successfully set up the VPN rule for your LAN-Cell. If you already had VPN rules configured, the wizard adds the new VPN rule after the last existing VPN rule.

Figure 30 VPN Wizard Setup Complete

3.3 Security Settings for VPN Traffic

The LAN-Cell can apply the firewall and content filtering to the traffic going to or from the LAN-Cell's VPN tunnels. The LAN-Cell applies the security settings to the traffic before encrypting VPN traffic that it sends out or after decrypting received VPN traffic.

The security settings apply to VPN traffic going to or from the LAN-Cell's VPN tunnels. They do not apply to other VPN traffic for which the LAN-Cell is not one of the gateways (VPN pass-through traffic).

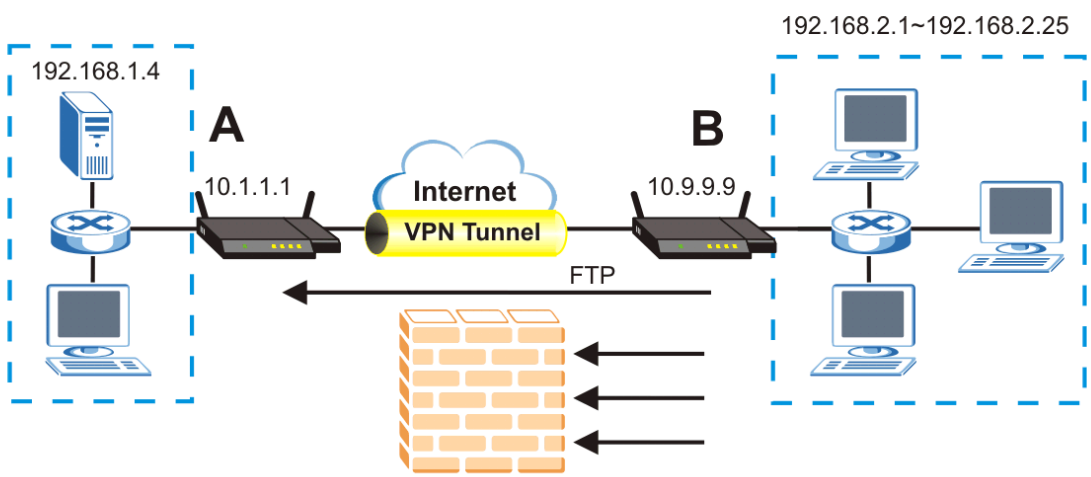
You can apply firewall security to VPN traffic based on its direction of travel. The following examples show how you do this for the firewall.

3.3.1 Firewall Rule for VPN Example

The firewall provides even more fine-tuned control for VPN tunnels. You can configure default and custom firewall rules for VPN packets.

Take the following example. You have a LAN FTP server with IP address 192.168.1.4 behind device A. You could configure a VPN rule to allow the network behind device B to access your LAN FTP server through a VPN tunnel. Now, if you don't want other services like chat or e-mail going to the FTP server, you can configure firewall rules that allow only FTP traffic to come from VPN tunnels to the FTP server. Furthermore, you can configure the firewall rule so that only the network behind device B can access the FTP server through a VPN tunnel (not other remote networks that have VPN tunnels with the LAN-Cell).

Figure 31 Firewall Rule for VPN

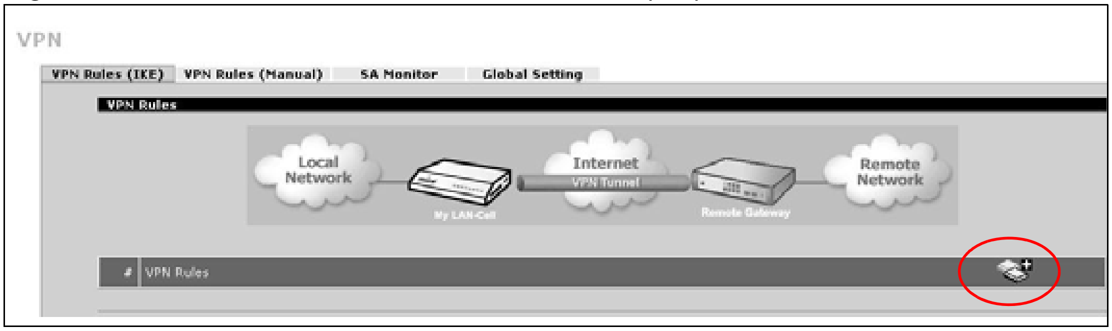


3.3.2 Configuring the VPN Rule

This section shows how to configure a VPN rule on device A to let the network behind B access the FTP server. You would also have to configure a corresponding rule on device B.

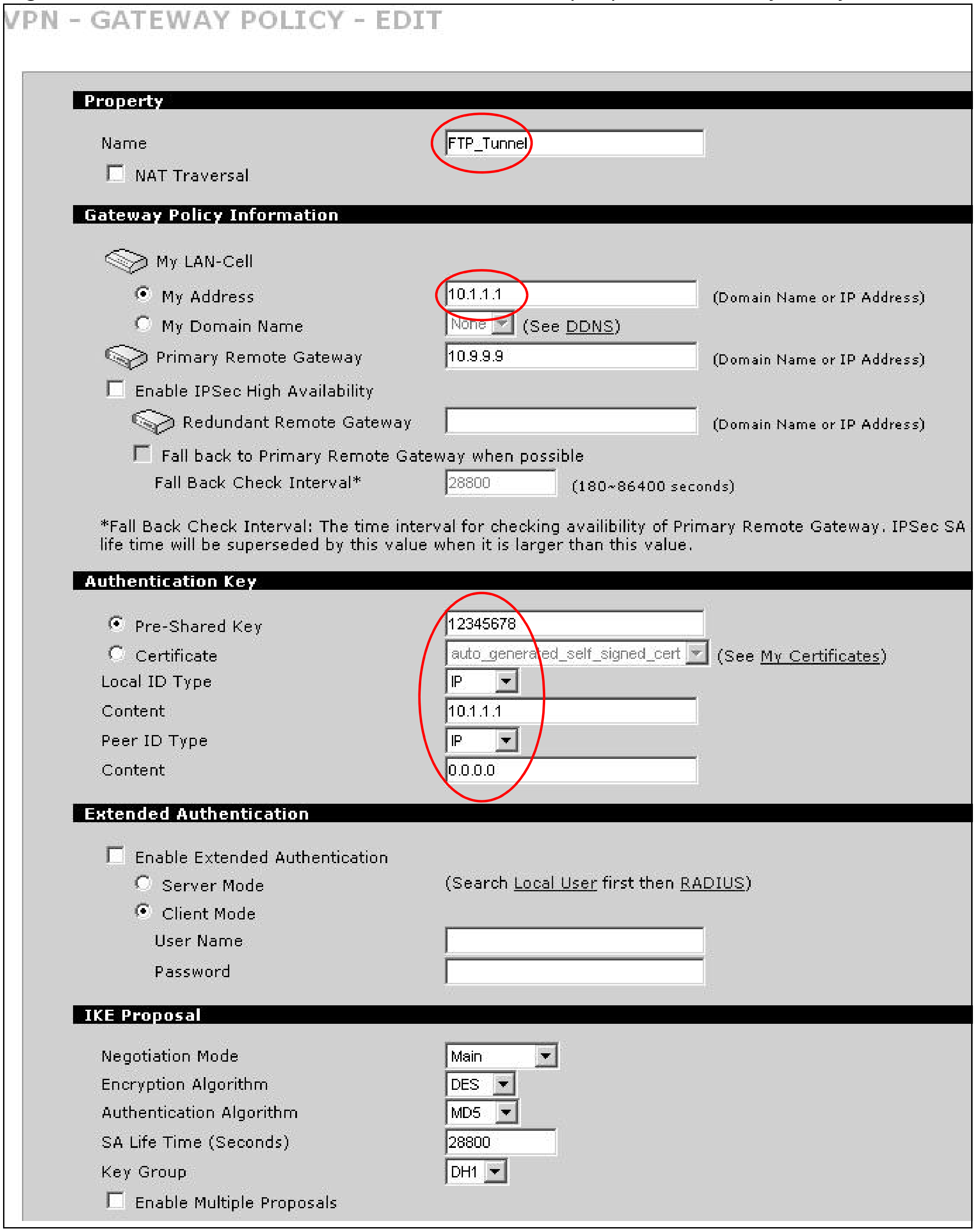
1 Click **Security** > **VPN CONFIG** to open the following screen. Click the **Add Gateway Policy** icon.

Figure 32 SECURITY > VPN CONFIG > VPN Rules (IKE)



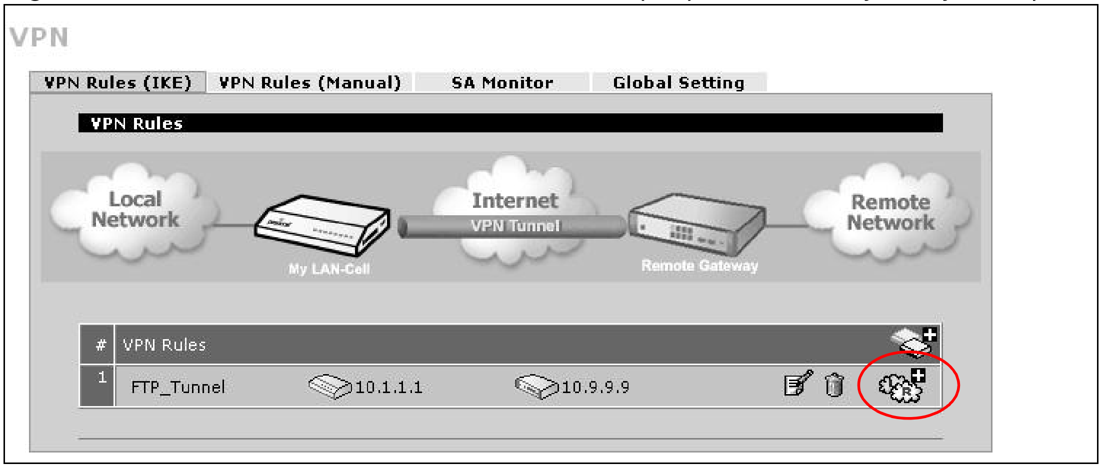
2 Use this screen to set up the connection between the routers. Configure the fields that are circled as follows and click **Apply**.

Figure 33 SECURITY > VPN CONFIG > VPN Rules (IKE)> Add Gateway Policy



3 Click the **Add Network Policy** icon.

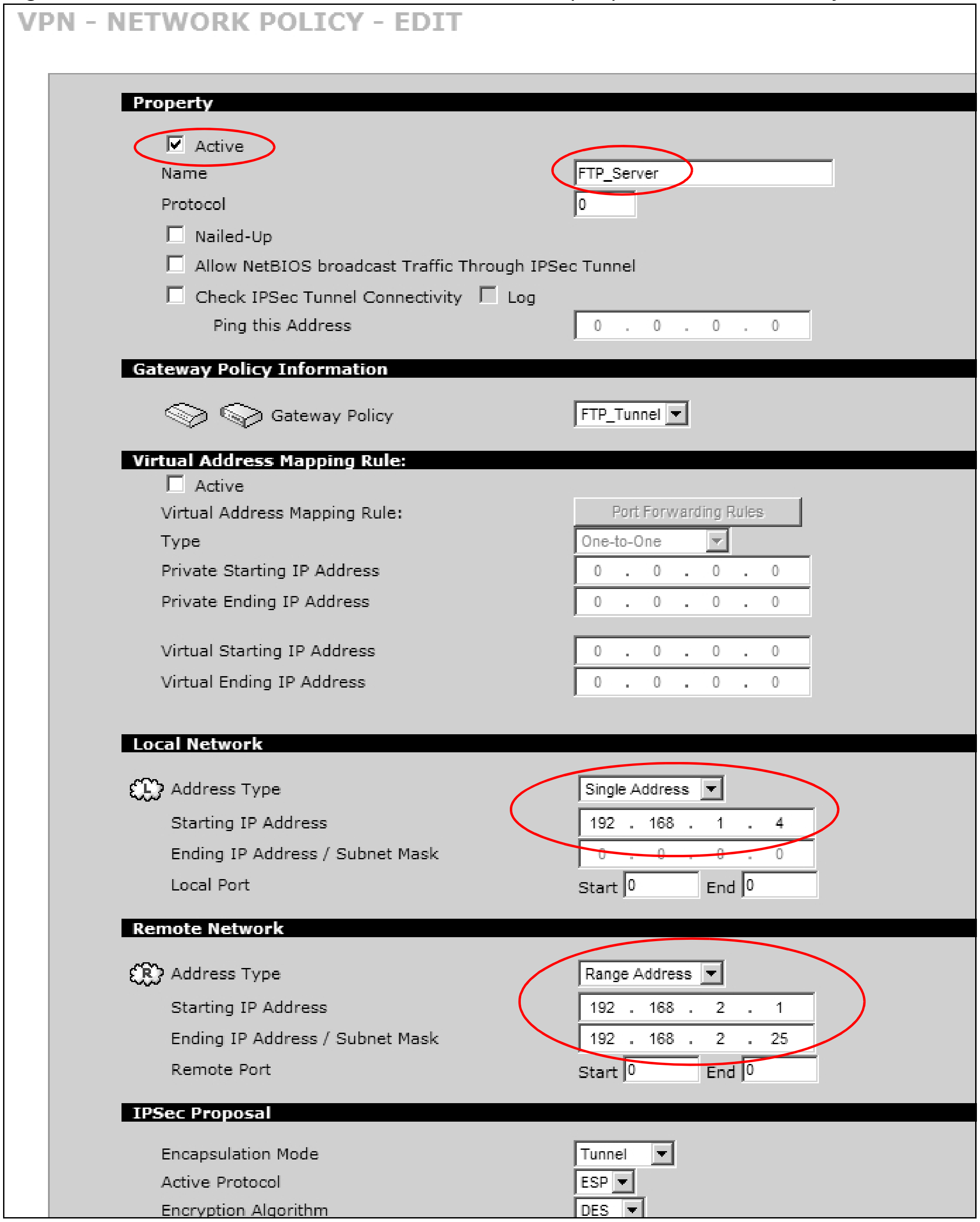
Figure 34 SECURITY > VPN CONFIG> VPN Rules (IKE): With Gateway Policy Example



4 Use this screen to specify which computers behind the routers can use the VPN tunnel. Configure the fields that are circled as follows and click **Apply**. You may notice that the example does not specify the port numbers. This is due to the following reasons.

- While FTP uses a control session on port 20, the port for the data session is not fixed. So this example uses the firewall's FTP application layer gateway (ALG) to handle this instead of specifying port numbers in this VPN network policy.
- The firewall provides better security because it operates at layer 4 and checks traffic sessions. The VPN network policy only operates at layer 3 and just checks IP addresses and port numbers.

Figure 35 SECURITY > VPN CONFIG > VPN Rules (IKE)> Add Network Policy



3.3.3 Configuring the Firewall Rules

Suppose you have several VPN tunnels but you only want to allow device B's network to access the FTP server. You also only want FTP traffic to go to the FTP server, so you want to block all other traffic types (like chat, e-mail, web and so on). The following sections show how to configure firewall rules to enforce these restrictions.

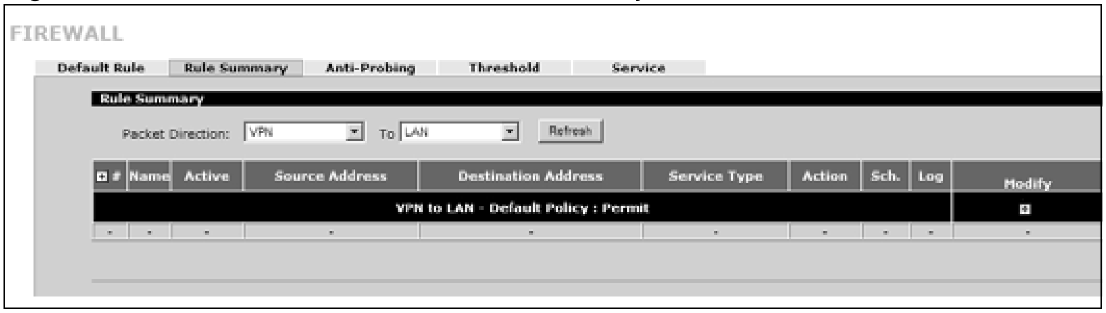
3.3.3.1 Firewall Rule to Allow Access Example

Configure a firewall rule that allows FTP access from the VPN tunnel to the FTP server.

1 Click **Security > Firewall > Rule Summary**.

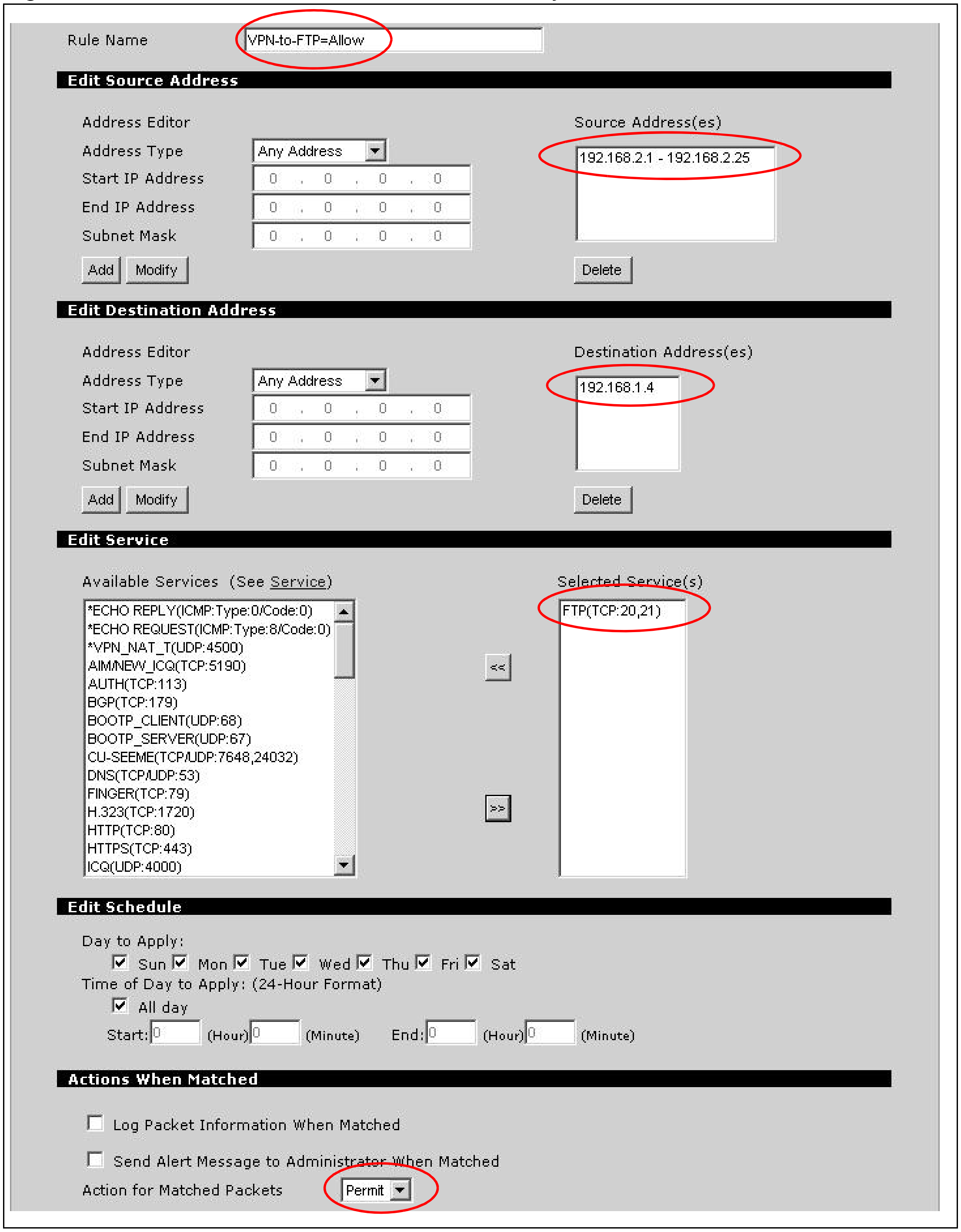
2 Select **VPN to LAN** as the packet direction and click **Refresh**.

Figure 36 SECURITY > FIREWALL > Rule Summary



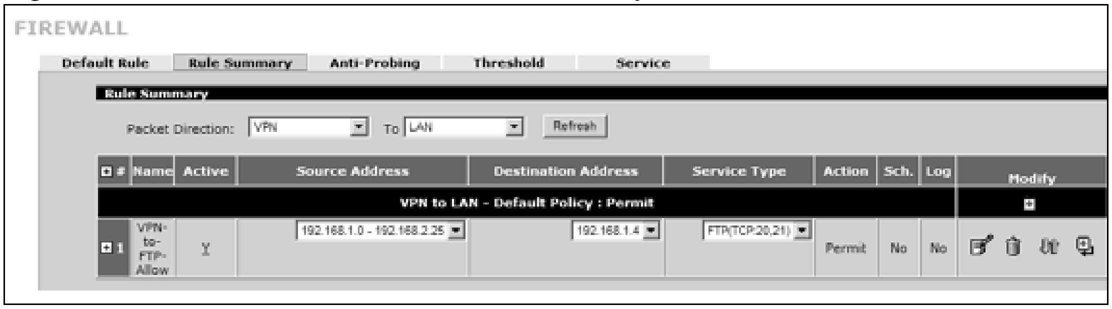
3 Insert a new by clicking the plus sign (+) under the Modify column. Define the rule as shown in the following figure and click **Apply**. The source addresses are the VPN rule's remote network and the destination address is the LAN FTP server.

Figure 37 SECURITY > FIREWALL > Rule Summary > Edit: Allow



4 The rule displays in the summary list of VPN to LAN firewall rules.

Figure 38 SECURITY > FIREWALL > Rule Summary: Allow

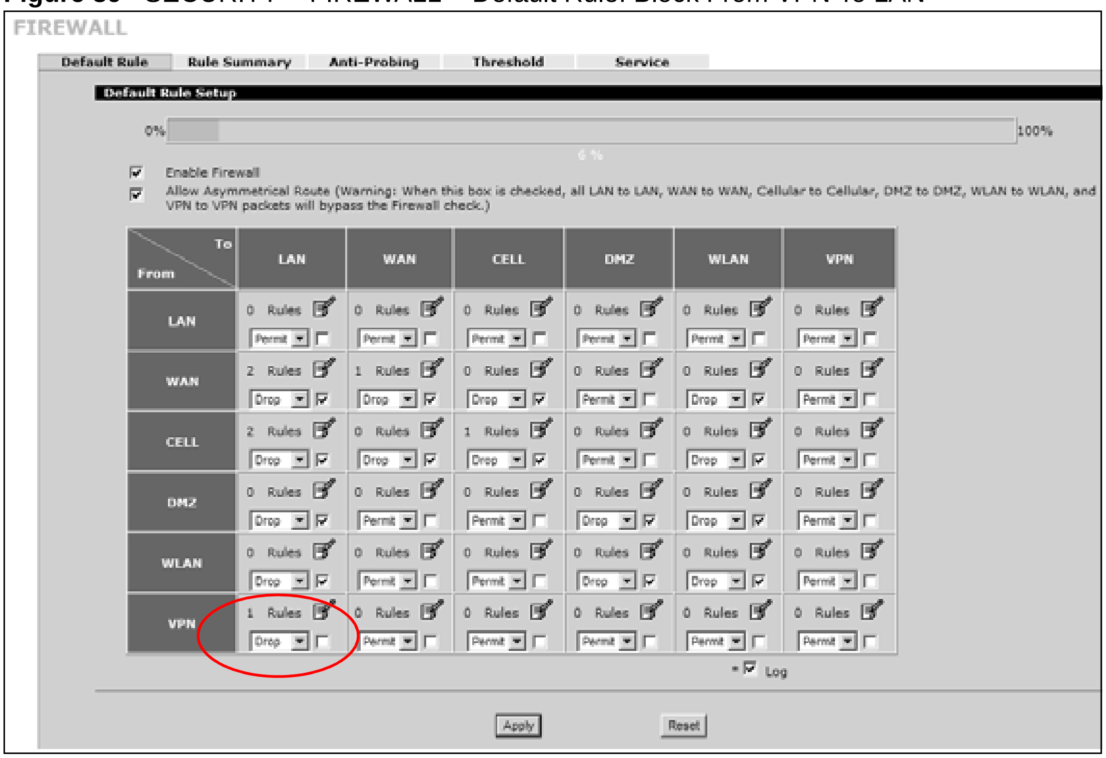


3.3.3.2 Default Firewall Rule to Block Other Access Example

Now you configure the default firewall rule to block all VPN to LAN traffic. This blocks any other types of access from VPN tunnels to the LAN FTP server. This means that you need to configure more firewall rules if you want to allow any other VPN tunnels to access the LAN.

1. Click **SECURITY** > **FIREWALL** > **Default Rule**.
2. Configure the screen as follows and click **Apply**.

Figure 39 SECURITY > FIREWALL > Default Rule: Block From VPN To LAN



PART II
Network & Wireless Menus

The WIRELESS > CELLULAR menu option is a short-cut to the WAN > CELLULAR screen.

4

LAN Screens

4.1 LAN, WAN and the LAN-Cell

This chapter describes how to configure LAN settings.

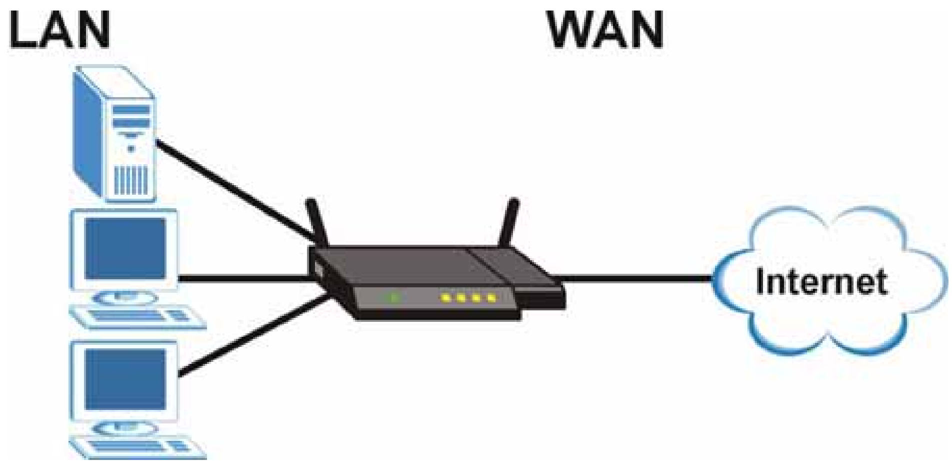
A network is a shared communication system to which many computers are attached.

The Local Area Network (LAN) includes the computers and networking devices in your home or office that you connect to the LAN-Cell's LAN ports.

The Wide Area Network (WAN) is another network (most likely the Internet) that you connect to the LAN-Cell's WAN port. See Chapter 5 on page 89 for how to use the WAN screens to set up your WAN connection.

The LAN and the WAN are two separate networks. The LAN-Cell controls the traffic that goes between them. The following graphic gives an example.

Figure 40 LAN and WAN



4.1.1 What You Can Do in The LAN Screens

- Use the **LAN** screen (Section 4.2 on page 80) to configure TCP/IP, DHCP, IP/MAC binding and NetBIOS settings on the LAN.
- Use the **Static DHCP** screen (Section 4.3 on page 83) to configure the IP addresses assigned to devices in the LAN by DHCP.
- Use the **IP Alias** screen (Section 4.4 on page 84) to configure IP alias settings on the ZLAN-Cell's LAN ports.
- Use the **Port Roles** screen (Section 4.5 on page 86) to configure LAN ports on the LAN-Cell.

4.1.2 What You Need to Know About LAN

IP Address and Subnet Mask

Similar to the way houses on a street share a common street name, so too do computers on a LAN share one common network number.

Where you obtain your network number depends on your particular situation. If the ISP or your network administrator assigns you a block of registered IP addresses, follow their instructions in selecting the IP addresses and the subnet mask.

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0 and you must enable the Network Address Translation (NAT) feature of the LAN-Cell. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told otherwise. If you select 192.168.1.0 as the network number; it covers 254 individual addresses, from 192.168.1.1 to 192.168.1.254 (zero and 255 are reserved). In other words, the first three numbers specify the network number while the last number identifies an individual computer on that network.

Once you have decided on the network number, pick an IP address that is easy to remember, for instance, 192.168.1.1, for your LAN-Cell, but make sure that no other device on your network is using that IP address.

The subnet mask specifies the network number portion of an IP address. Your LAN-Cell will compute the subnet mask automatically based on the IP address that you entered. You don't need to change the subnet mask computed by the LAN-Cell unless you are instructed to do otherwise.

Private IP Addresses

Every machine on the Internet must have a unique address. If your networks are isolated from the Internet, for example, only between your two branch offices, you can assign any IP addresses to the hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks:

- 10.0.0.0 — 10.255.255.255
- 172.16.0.0 — 172.31.255.255
- 192.168.0.0 — 192.168.255.255

You can obtain your IP address from the IANA, from an ISP or it can be assigned from a private network. If you belong to a small organization and your Internet access is through an ISP, the ISP can provide you with the Internet addresses for your local networks. On the other hand, if you are part of a much larger organization, you should consult your network administrator for the appropriate IP addresses.

Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, please refer to RFC 1597, *Address Allocation for Private Internets* and RFC 1466, *Guidelines for Management of IP Address Space.*

MAC Address

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, 00:1B:39:00:00:02.

DHCP

The LAN-Cell can use DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) to automatically assign IP addresses subnet masks, gateways, and some network information like the IP addresses of DNS servers to the computers on your LAN. You can alternatively have the LAN-Cell relay DHCP information from another DHCP server. If you disable the LAN-Cell's DHCP service, you must have another DHCP server on your LAN, or else the computers must be manually configured.

IP Pool Setup

The LAN-Cell is pre-configured with a pool of IP addresses for the computers on your LAN. See Appendix on page 575 for the default IP pool range. Do not assign your LAN computers static IP addresses that are in the DHCP pool.

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 LAN-Cell 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 LAN-Cell 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**.

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

WINS

WINS (Windows Internet Naming Service) is a Windows implementation of NetBIOS Name Server (NBNS) on Windows. It keeps track of NetBIOS computer names. It stores a mapping table of your network’s computer names and IP addresses. The table is dynamically updated for IP addresses assigned by DHCP. This helps reduce broadcast traffic since computers can query the server instead of broadcasting a request for a computer name’s IP address. In this way WINS is similar to DNS, although WINS does not use a hierarchy (unlike DNS). A network can have more than one WINS server. Samba can also serve as a WINS server.

IP Alias

IP alias allows you to partition a physical network into different logical networks over the same Ethernet interface. The LAN, DMZ or WLAN may all be partitioned in this way.

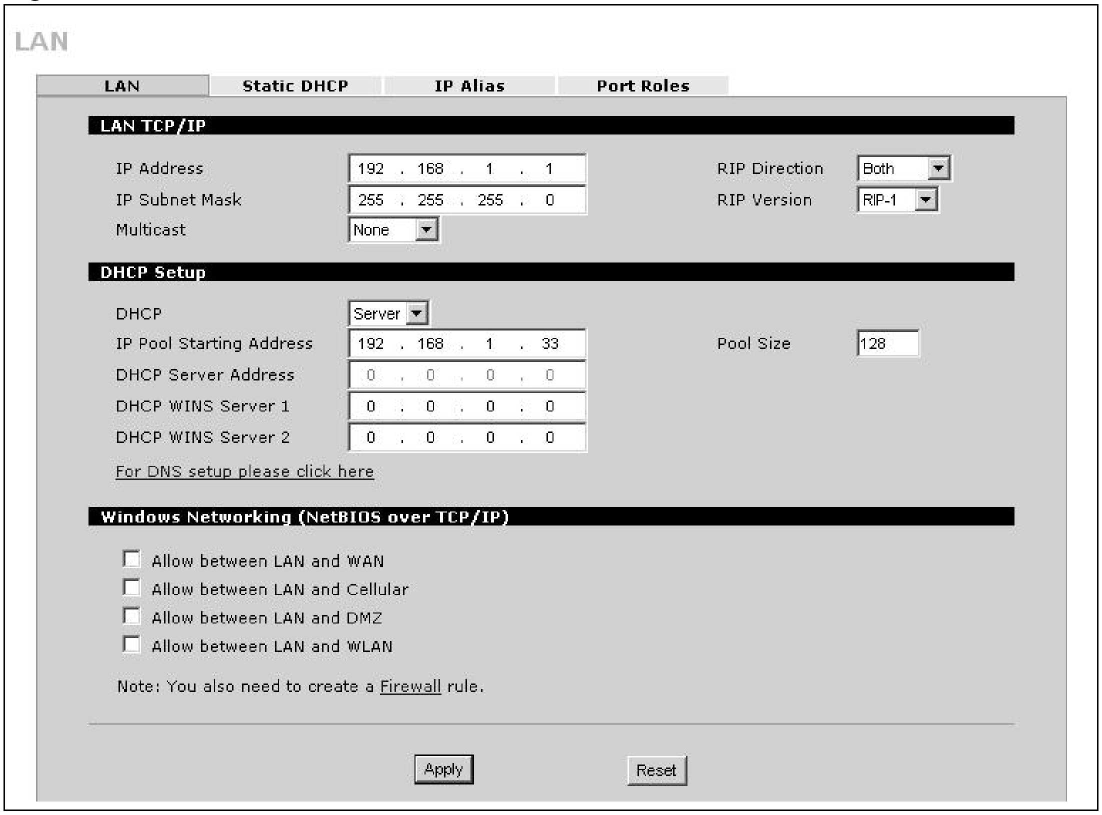
Port Roles

Port Roles allows you to set ports as part of the LAN, DMZ and/or WLAN interface.

4.2 LAN Screen

Click **NETWORK** > **LAN** to open the **LAN** screen. Use this screen to configure the LAN-Cell’s IP address and other LAN TCP/IP settings as well as the built-in DHCP server capability that assigns IP addresses and DNS servers to systems that support DHCP client capability.

Figure 41 NETWORK > LAN



The following table describes the labels in this screen.

Table 15 NETWORK > LAN

LABEL	DESCRIPTION
LAN TCP/IP	
IP Address	Type the IP address of your LAN-Cell in dotted decimal notation. 192.168.1.1 is the factory default. Alternatively, click the right mouse button to copy and/or paste the IP address.
IP Subnet Mask	The subnet mask specifies the network number portion of an IP address. Your LAN-Cell 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 LAN-Cell.
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 LAN-Cell 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.

Table 15 NETWORK > LAN (continued)

LABEL	DESCRIPTION
RIP Version	The **RIP Version** field controls the format and the broadcasting method of the RIP packets that the LAN-Cell 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**.
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*.
DHCP Setup	
DHCP	DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients (workstations) to obtain TCP/IP configuration at startup from a server. Unless you are instructed by your ISP, leave this field set to **Server**. When configured as a server, the LAN-Cell provides TCP/IP configuration for the clients. When set as a server, fill in the **IP Pool Starting Address** and **Pool Size** fields. Select **Relay** to have the LAN-Cell forward DHCP requests to another DHCP server. When set to **Relay**, fill in the **DHCP Server Address** field. Select **None** to stop the LAN-Cell from acting as a DHCP server. When you select **None**, you must have another DHCP server on your LAN, or else the computers must be manually configured.
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.
DHCP Server Address	Type the IP address of the DHCP server to which you want the LAN-Cell to relay DHCP requests. Use dotted decimal notation. Alternatively, click the right mouse button to copy and/or paste the IP address.
DHCP WINS Server 1, 2	Type the IP address of the WINS (Windows Internet Naming Service) server that you want to send to the DHCP clients. The WINS server keeps a mapping table of the computer names on your network and the IP addresses that they are currently using.
Windows Networking (NetBIOS over TCP/IP)	NetBIOS (Network Basic Input/Output System) are TCP or UDP 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 between LAN and WAN	Select this check box to forward NetBIOS packets from the LAN to WANand from WAN to the LAN. If your firewall is enabled with the default policy set to block WAN to LAN traffic, you also need to enable the default WAN to LAN firewall rule that forwards NetBIOS traffic. Clear this check box to block all NetBIOS packets going from the LAN to WAN and from WAN to the LAN.

Table 15 NETWORK > LAN (continued)

LABEL	DESCRIPTION
Allow between LAN and Cellular	Select this check box to forward NetBIOS packets from the LAN to CELL and from CELL to the LAN. If your firewall is enabled with the default policy set to block CELL to LAN traffic, you also need to enable the default CELL to LAN firewall rule that forwards NetBIOS traffic. Clear this check box to block all NetBIOS packets going from the LAN to CELL and from CELL to the LAN.
Allow between LAN and DMZ	Select this check box to forward NetBIOS packets from the LAN to the DMZ and from the DMZ to the LAN. If your firewall is enabled with the default policy set to block DMZ to LAN traffic, you also need to enable the default DMZ to LAN firewall rule that forwards NetBIOS traffic. Clear this check box to block all NetBIOS packets going from the LAN to the DMZ and from the DMZ to the LAN.
Allow between LAN and WLAN	Select this check box to forward NetBIOS packets from the LAN to the WLAN and from the WLAN to the LAN. Clear this check box to block all NetBIOS packets going from the LAN to the WLAN and from the WLAN to the LAN.
Apply	Click **Apply** to save your changes back to the LAN-Cell.
Reset	Click **Reset** to begin configuring this screen afresh.

4.3 LAN Static DHCP Screen

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

To change your LAN-Cell’s static DHCP settings, click **NETWORK** > **LAN** > **Static DHCP**. The screen appears as shown.

Figure 42 NETWORK > LAN > Static DHCP

The following table describes the labels in this screen.

Table 16 NETWORK > LAN > Static DHCP

LABEL	DESCRIPTION
#	This is the index number of the Static IP table entry (row).
MAC Address	Type the MAC address of a computer on your LAN.
IP Address	Type the IP address that you want to assign to the computer on your LAN. Alternatively, click the right mouse button to copy and/or paste the IP address.
Apply	Click **Apply** to save your changes back to the LAN-Cell.
Reset	Click **Reset** to begin configuring this screen afresh.

4.4 LAN IP Alias Screen

IP alias allows you to partition a physical network into different logical networks over the same Ethernet interface.

The LAN-Cell has a single LAN interface. Even though more than one of ports 1~4 may be in the LAN port role, they are all still part of a single physical Ethernet interface and all use the same IP address.

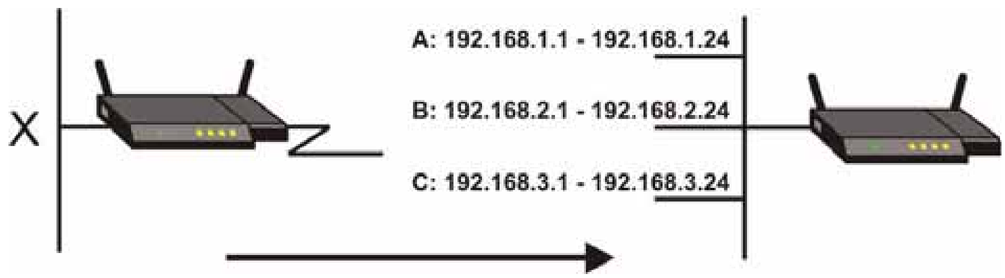
The LAN-Cell supports three logical LAN interfaces via its single physical LAN Ethernet interface. The LAN-Cell itself is the gateway for each of the logical LAN networks.

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

Make sure that the subnets of the logical networks do not overlap.

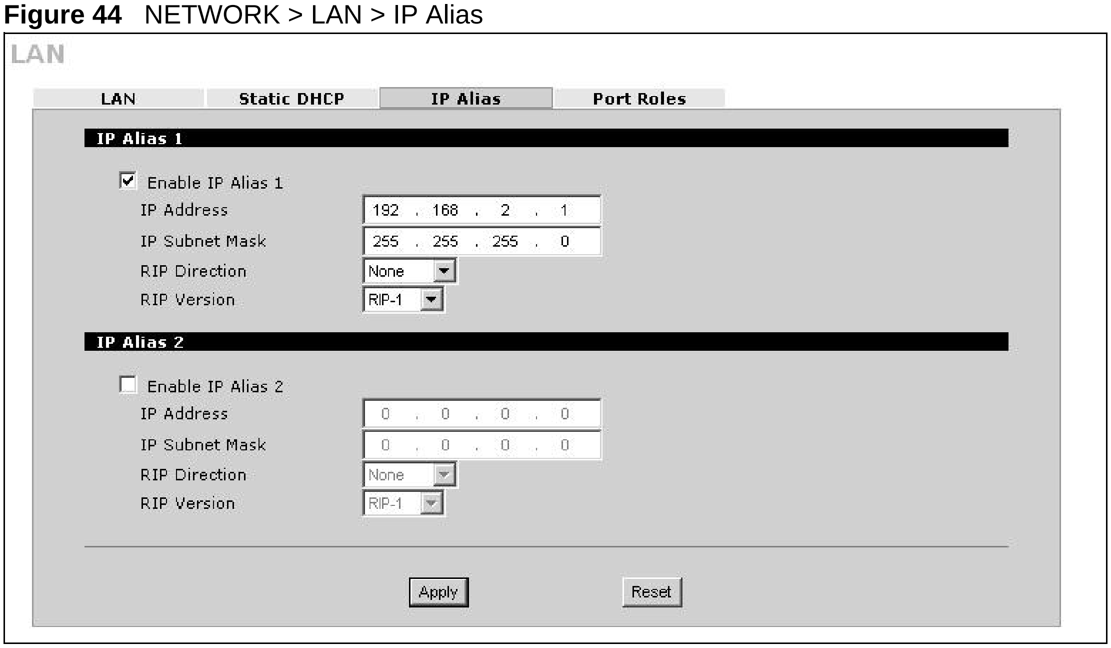
The following figure shows a LAN divided into subnets A, B, and C.

Figure 43 Physical Network & Partitioned Logical Networks



To change your LAN-Cell’s IP alias settings, click **NETWORK** > **LAN** > **IP Alias**. The screen appears as shown.

Figure 44 NETWORK > LAN > IP Alias



The following table describes the labels in this screen.

Table 17 NETWORK > LAN > IP Alias

LABEL	DESCRIPTION
Enable IP Alias 1, 2	Select the check box to configure another LAN network for the LAN-Cell.
IP Address	Enter the IP address of your LAN-Cell in dotted decimal notation. Alternatively, click the right mouse button to copy and/or paste the IP address.
IP Subnet Mask	Your LAN-Cell 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 LAN-Cell.
RIP Direction	RIP (Routing Information Protocol, RFC 1058 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 LAN-Cell 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	The **RIP Version** field controls the format and the broadcasting method of the RIP packets that the LAN-Cell 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 LAN-Cell.
Reset	Click **Reset** to begin configuring this screen afresh.

4.5 LAN Port Roles Screen

Use the **Port Roles** screen to set ports as part of the LAN, DMZ and/or WLAN interface.

Ports 1~4 on the LAN-Cell can be part of the LAN, DMZ or WLAN interface.

Do the following if you are configuring from a computer connected to a LAN, DMZ or WLAN port and changing the port's role:

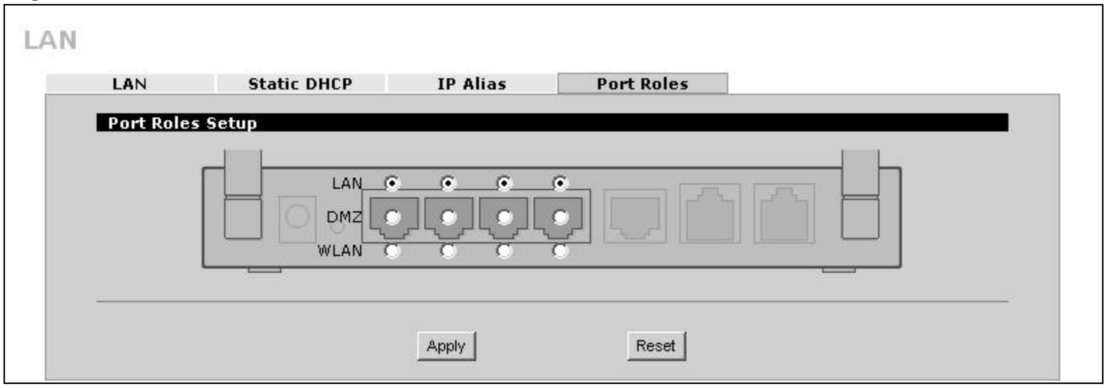
1. A port's IP address varies as its role changes, make sure your computer's IP address is in the same subnet as the LAN-Cell's LAN, DMZ or WLAN IP address.
2. Use the appropriate LAN, DMZ or WLAN IP address to access the LAN-Cell.

To change your LAN-Cell's port role settings, click **NETWORK** > **LAN** > **Port Roles**. The screen appears as shown.

The radio buttons correspond to Ethernet ports on the front panel of the LAN-Cell. On the LAN-Cell, ports 1 to 4 are all LAN ports by default.

Your changes are also reflected in the **DMZ Port Roles** and **WLAN Port Roles** screens.

Figure 45 NETWORK > LAN > Port Roles



The following table describes the labels in this screen.

Table 18 NETWORK > LAN > Port Roles

LABEL	DESCRIPTION
LAN	Select a port’s LAN radio button to use the port as part of the LAN. The port will use the LAN-Cell’s LAN IP address and MAC address.
DMZ	Select a port’s DMZ radio button to use the port as part of the DMZ. The port will use the LAN-Cell’s DMZ IP address and MAC address.
WLAN	Select a port’s WLAN radio button to use the port as part of the WLAN. The port will use the LAN-Cell’s WLAN IP address and MAC address.
Apply	Click **Apply** to save your changes back to the LAN-Cell.
Reset	Click **Reset** to begin configuring this screen afresh.

After you change the LAN/DMZ/WLAN port roles and click **Apply**, please wait for few seconds until the following screen appears. Click **Return** to go back to the **Port Roles** screen.

Figure 46 Port Roles Change Complete

5

WAN & 3G Cellular Screens

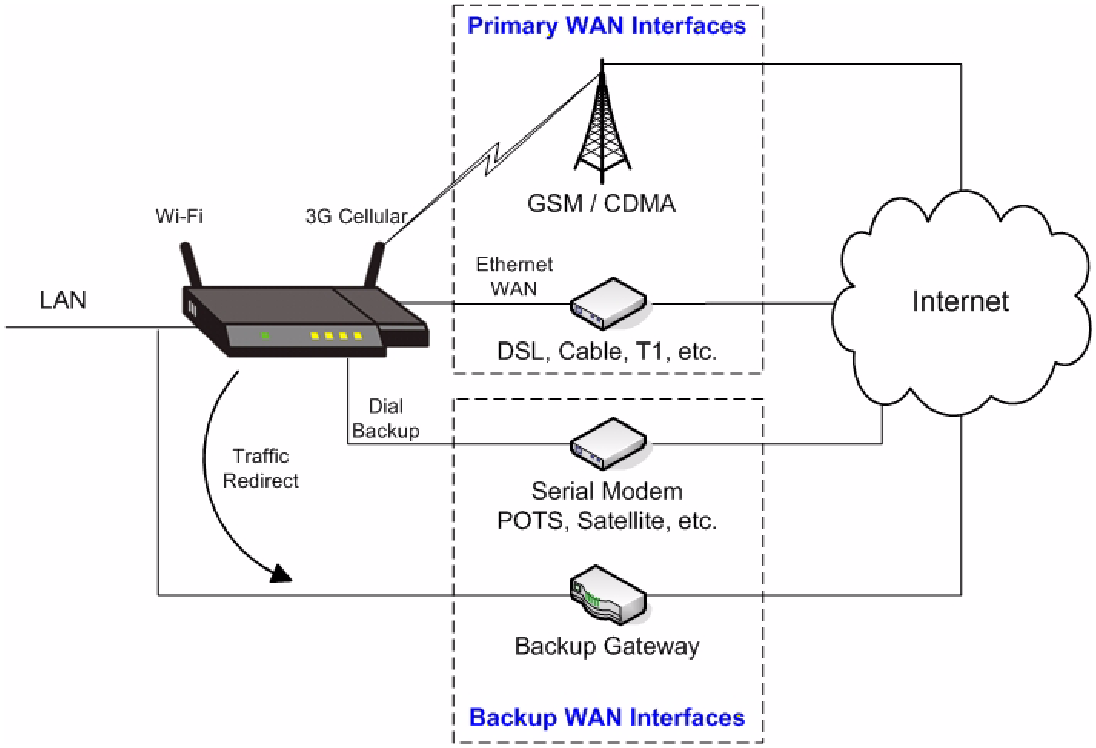
5.1 Overview

This chapter describes how to configure WAN, 3G Cellular, Dial-Backup and Traffic Redirect settings.

A WAN (Wide Area Network) connection is an outside connection to another network or the Internet. It connects your private networks such as a LAN (Local Area Network) and other networks, so that a computer in one location can communicate with computers in other locations.

The LAN-Cell 2 has two primary WAN and two backup WAN interfaces:

Figure 47 LAN-Cell 2 Primary & Backup WAN Interfaces



Primary WAN Interfaces

1. **WAN** refers to the Ethernet WAN port on the LAN-Cell which is typically connected to a DSL/cable modem, T1, or other high-speed Ethernet-based wired Internet service.
2. **CELLULAR** refers to 3G cellular (CDMA/GSM) modem cards that are inserted into the PC-Card slot on the side of the LAN-Cell.

The primary WAN interfaces can be used in either Load-Balancing or Fail-Over modes and are the most common pathways for connecting to the Internet.

Backup WAN Interfaces

1. **Dial-Backup** refers to the AUX (serial) port the LAN-Cell which can be connected to an external serial modem that responds to basic Hayes "AT" commands. The Dial-Backup port is used when the wired Ethernet WAN (or CELLULAR) interface is not available.
2. **Traffic Redirect** refers to the LAN-Cell's ability to redirect WAN-bound traffic to an independent WAN gateway located elsewhere on the Local Area Network. This is a "route of last resort" in situations where the LAN-Cell has no available WAN connections of its own.

5.1.1 What You Can Do in the WAN Screens

- Use the **General** screen (Section 5.2 on page 94) to configure load balancing, route priority, and connection test settings for the LAN-Cell.
- Use the **WAN** screen (Section 5.3 on page 103) to configure the Ethernet WAN interface for Internet access on the LAN-Cell.
- Use the **Cellular** (3G**)** screen (Section 5.4 on page 114) to configure the CELL interface for Internet access on the LAN-Cell.
- Use the **Traffic Redirect** screen (Section 5.5 on page 120) to configure an alternative gateway.
- Use the **Dial Backup** screen (Section 5.6 on page 122) to configure the backup WAN dialup connection.

5.1.2 What You Need To Know About WAN

Encapsulation Method

Encapsulation is used to include data from an upper layer protocol into a lower layer protocol. To set up a WAN connection to the Internet, you need to use the same encapsulation method used by your ISP (Internet Service Provider).

If your ISP offers a dial-up Internet connection using PPPoE (PPP over Ethernet) or PPPoA, they may also provide a username and password (and service name) for user authentication.

WAN IP Address

The WAN IP address is an IP address for the LAN-Cell, which makes it accessible from an outside network. It is used by the LAN-Cell to communicate with other devices in other networks. It can be static (fixed) or dynamically assigned by the ISP each time the LAN-Cell tries to access the Internet.

If your ISP assigns you a static WAN IP address, they should also assign you the subnet mask and DNS server IP address(es) (and a gateway IP address if you use the Ethernet or ENET ENCAP encapsulation method).

Most Cellular Network Operators provide WAN IP addresses using a form of Dynamic Host Control Protocol (DHCP), even if your WAN IP address is “static”. In these cases, configure the Cellular WAN IP Address Assignment as “Get Automatically from ISP”.

Multiple WAN Interfaces

You can use a second WAN connection for load sharing to increase overall network throughput or as a backup to enhance network reliability.

The LAN-Cell has one Ethernet WAN port. Inserting a 3G card adds a second WAN (Cellular) interface. You can connect one interface to one ISP (or network) and connect the other to a second ISP (or network).

If one WAN interface's connection goes down, the LAN-Cell can automatically send its traffic through the other WAN interface when the WAN interfaces are configured for Fail-Over Mode. See Chapter 5 on page 92 for details.

Optionally, the LAN-Cell can balance the load between the two WAN interfaces (see Section on page 92).

You can use policy routing to specify the WAN interface that specific services go through. An ISP may give traffic from certain (more expensive) connections priority over the traffic from other accounts. You could route delay intolerant traffic (like voice over IP calls) through this kind of connection. Other traffic could be routed through a cheaper broadband Internet connection that does not provide priority service. The LAN-Cell's NAT feature allows you to configure sets of rules for one WAN interface and separate sets of rules for the other WAN interface. Refer to Chapter 13 on page 289 for details.

The LAN-Cell's DDNS lets you select which WAN interface you want to use for each individual domain name. The DDNS high availability feature lets you have the LAN-Cell use the other WAN interface for a domain name if the configured WAN interface's connection goes down. See DDNS on page 309 for details.

When configuring a VPN rule, you have the option of selecting one of the LAN-Cell's domain names in the **My Address** field.

Load Balancing Introduction

On the LAN-Cell, load balancing is the process of dividing traffic loads between the two WAN interfaces (or ports). This allows you to improve quality of services and maximize bandwidth utilization.

See also policy routing to provide quality of service by dedicating a route for a specific traffic type and bandwidth management to specify a set amount of bandwidth for a specific traffic type on an interface.

Load Balancing Algorithms

The LAN-Cell uses three load balancing methods (least load first, weighted round robin and spillover) to decide which WAN interface the traffic for a session[1] (from the LAN) uses.

The following sections describe each load balancing method. The available bandwidth you configure on the LAN-Cell refers to the actual bandwidth provided by the ISP and the measured bandwidth refers to the bandwidth an interface is currently using.

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".

1. The metric sets the priority for the LAN-Cell's routes to the Internet. Each route must have a unique metric.
2. The priorities of the WAN interface routes must always be higher than the dial-backup and traffic redirect route priorities.

Lets say that you have the WAN operation mode set to active/passive, meaning the LAN-Cell will use the second highest priority WAN interface as a back up. The WAN route has a metric of "2", the Cellular route has a metric of "3", the traffic-redirect route has a metric of "14" and the dial-backup route has a metric of "15". In this case, the WAN route acts as the primary default route. If the WAN route fails to connect to the Internet, the LAN-Cell tries the Cellular route next. If the Cellular route fails, the LAN-Cell tries the traffic-redirect route. In the same manner, the LAN-Cell uses the dial-backup route if the traffic-redirect route also fails.

1. In the load balancing section, a session may refer to normal connection-oriented, UDP and SNMP2 traffic.

The dial-backup or traffic redirect routes cannot take priority over the WAN and Cellular routes.

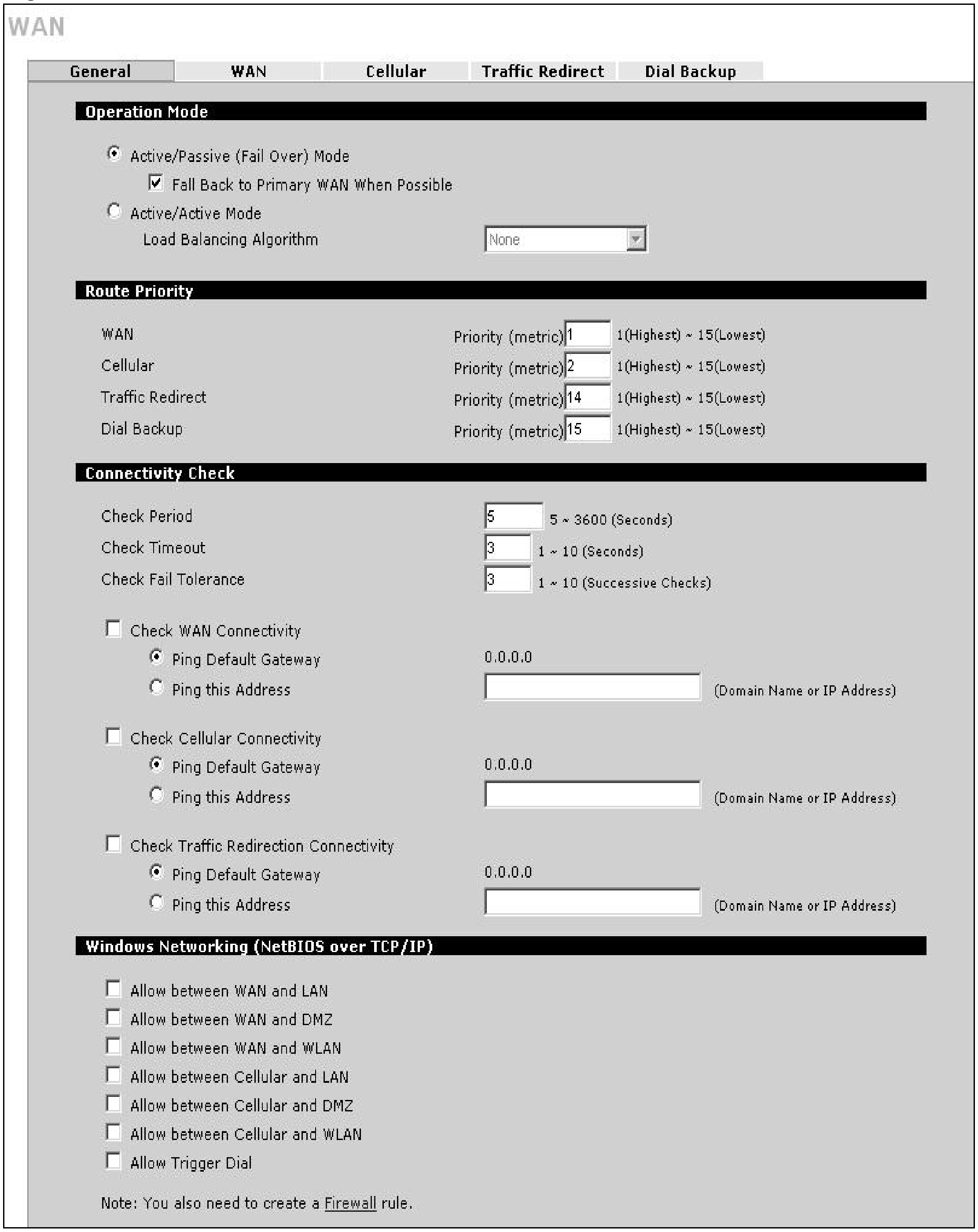
WAN Continuity Check

TThe LAN-Cell can periodically generate ICMP (ping) traffic to test the connection status of the Ethernet WAN, Cellular WAN or Traffic Redirect ports. This feature is useful for detecting “dead-peer” situations or other conditions where the WAN interface is not forwarding traffic even though the physical status of the interface is “up”. WAN Connectivity Check is most useful for “Always-On” WAN connections.

5.2 WAN General Screen

Click **NETWORK** > **WAN** to open the **General** screen. Use this screen to configure load balancing, route priority and traffic redirect properties.

Figure 48 NETWORK > WAN General



The following table describes the labels in this screen.

Table 19 NETWORK > WAN General

LABEL	DESCRIPTION
Active/Passive (Fail Over) Mode	Select the Active/Passive (fail over) operation mode to have the LAN-Cell use the second highest priority WAN interface as a back up. This means that the LAN-Cell will normally use the highest priority (primary) WAN interface (depending on the priorities you configure in the **Route Priority** fields). The LAN-Cell will switch to the secondary (second highest priority) WAN interface when the primary WAN interface's connection fails.
Fall Back to Primary WAN When Possible	This field determines the action the LAN-Cell takes after the primary WAN interface fails and the LAN-Cell starts using the secondary WAN interface. Select this check box to have the LAN-Cell change back to using the primary WAN interface when the LAN-Cell can connect through the primary WAN interface again. Clear this check box to have the LAN-Cell continue using the secondary WAN interface, even after the LAN-Cell can connect through the primary WAN interface again. The LAN-Cell continues to use the secondary WAN interface until it's connection fails (at which time it will change back to using the primary WAN interface if its connection is up.
Active/Active Mode	Select **Active/Active Mode** to have the LAN-Cell use both of the WAN interfaces at the same time and allow you to enable load balancing.
Load Balancing Algorithm	Select **Least Load First**, **Weighted Round Robin** or **Spillover** to activate load balancing and set the related fields. Otherwise, select **None**. Refer to Section 5.2.1 on page 97 for load balancing configuration.
Route Priority	
WAN Cellular Traffic Redirect Dial Backup	The default WAN connection is "1' as your broadband connection via the WAN interface should always be your preferred method of accessing the WAN. The LAN-Cell switches from the WAN interface to the Cellular if the WAN interface's connection fails and then back to WAN interface when the WAN interface's connection comes back up. The default priority of the routes is **WAN**, **Cellular**, **Traffic Redirect** and then **Dial Backup**: You have three choices for an auxiliary connection (**Cellular**, **Traffic Redirect** and **Dial Backup**) 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"). The **Dial Backup** field is available only when you enable the corresponding dial backup feature in the **Dial Backup** screen.
Connectivity Check	
Check Period	The LAN-Cell tests a WAN connection by periodically sending a ping to either the default gateway or the address in the **Ping this Address** field. Type a number of seconds (5 to 3600) to set the time interval between checks. Allow more time if your destination IP address handles lots of traffic.
Check Timeout	Type the number of seconds (1 to 10) for your LAN-Cell to wait for a response to the ping before considering the check to have failed. This setting must be less than the **Check Period**. Use a higher value in this field if your network is busy or congested.
Check Fail Tolerance	Type how many WAN connection checks can fail (1-10) before the connection is considered "down" (not connected). The LAN-Cell still checks a "down" connection to detect if it reconnects.

Table 19 NETWORK > WAN General (continued)

LABEL	DESCRIPTION
Check WAN/ Cellular Connectivity	Select the check box to have the LAN-Cell periodically test the respective WAN interface's connection. Select **Ping Default Gateway** to have the LAN-Cell ping the WAN interface's default gateway IP address. Select **Ping this Address** and enter a domain name or IP address of a reliable nearby computer (for example, your ISP's DNS server address) to have the LAN-Cell ping that address. For a domain name, use up to 63 alphanumeric characters (hyphens, periods and the underscore are also allowed) without spaces.
Check Traffic Redirection Connectivity	Select the check box to have the LAN-Cell periodically test the traffic redirect connection. Select **Ping Default Gateway** to have the LAN-Cell ping the backup gateway's IP address. Select **Ping this Address** and enter a domain name or IP address of a reliable nearby computer (for example, your ISP's DNS server address) to have the LAN-Cell ping that address. For a domain name, use up to 63 alphanumeric characters (hyphens, periods and the underscore are also allowed) without spaces.
Windows Networking (NetBIOS over TCP/IP):	NetBIOS (Network Basic Input/Output System) are TCP or UDP 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 between WAN and LAN	Select this check box to forward NetBIOS packets from WAN to the LAN port and from the LAN port to WAN. If your firewall is enabled with the default policy set to block WAN to LAN traffic, you also need to enable the default WAN to LAN firewall rule that forwards NetBIOS traffic. Clear this check box to block all NetBIOS packets going from WAN to the LAN port and from LAN port to WAN.
Allow between WAN and DMZ	Select this check box to forward NetBIOS packets from WAN to the DMZ port and from the DMZ port to WAN. Clear this check box to block all NetBIOS packets going from WAN to the DMZ port and from DMZ port to WAN.
Allow between WAN and WLAN	Select this check box to forward NetBIOS packets from WAN to the WLAN port and from the WLAN port to WAN. Clear this check box to block all NetBIOS packets going from WANto the WLAN port and from WLAN port to WAN.
Allow between Cellular and LAN	Select this check box to forward NetBIOS packets from Cellular to the LAN port and from the LAN port to Cellular. If your firewall is enabled with the default policy set to block Cellular to LAN traffic, you also need to enable the default Cellular to LAN firewall rule that forwards NetBIOS traffic. Clear this check box to block all NetBIOS packets going from Cellular to the LAN port and from LAN port to Cellular.
Allow between Cellular and DMZ	Select this check box to forward NetBIOS packets from Cellular to the DMZ port and from the DMZ port to Cellular. Clear this check box to block all NetBIOS packets going from Cellular to the DMZ port and from DMZ port to Cellular.
Allow between WAN and WLAN	Select this check box to forward NetBIOS packets from Cellular to the WLAN port and from the WLAN port to Cellular. Clear this check box to block all NetBIOS packets going from Cellular to the WLAN port and from WLAN port to Cellular.
Allow Trigger Dial	Select this option to allow NetBIOS packets to initiate calls.
Apply	Click **Apply** to save your changes back to the LAN-Cell.
Reset	Click **Reset** to begin configuring this screen afresh.

5.2.1 Configuring Load Balancing

To configure load balancing on the LAN-Cell, click **NETWORK** > **WAN** in the navigation panel. The **WAN General** screen displays by default. Select **Active/Active Mode** under **Operation Mode** to enable load balancing on the LAN-Cell.

The **WAN General** screen varies depending on what you select in the **Load Balancing Algorithm** field.

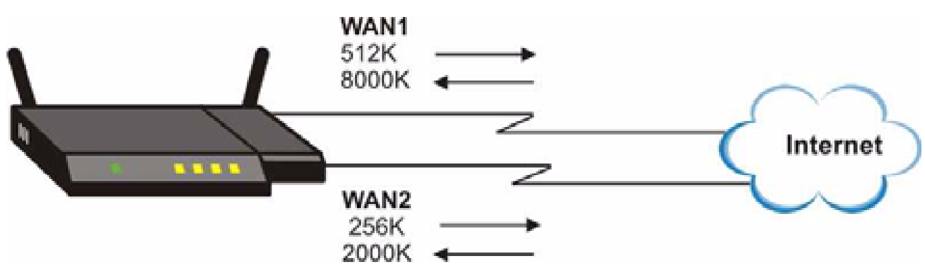
5.2.1.1 Least Load First

The least load first algorithm uses the current (or recent) outbound and/or inbound bandwidth utilization of each WAN interface as the load balancing criteria for making decisions on how how to route traffic. The outbound bandwidth utilization is defined as the measured outbound throughput over the available outbound bandwidth. The inbound bandwidth utilization is defined as the measured inbound throughput over the available inbound bandwidth. The two ratios are indexes used to calculate which WAN interface is less utilized at the time. A new LAN-originated session is distributed to the less utilized WAN interface.

5.2.1.2 Example 1

The following figure depicts an example where both the WAN interfaces on the LAN-Cell are connected to the Internet. The configured available outbound bandwidths for WAN and Cellular are 512K and 256K respectively.

Figure 49 Least Load First Example



If the outbound bandwidth utilization is used as the load balancing index and the measured outbound throughput of WAN is 412K and Cellular is 198K, the LAN-Cell calculates the load balancing index as shown in the table below.

Since Cellular has a smaller load balancing index (meaning that it is less utilized than WAN), the LAN-Cell will send the subsequent new session traffic through Cellular.

Table 20 Least Load First: Example 1

INTERFACE	OUTBOUND		LOAD BALANCING INDEX (M/A)
	AVAILABLE (A)	MEASURED (M)	
WAN	512 K	412 K	0.8
Cellular	256 K	198 K	0.77

5.2.1.3 Example 2

This example uses the same network scenario as in Figure 49 on page 97, but uses both the outbound and inbound bandwidth utilization in calculating the load balancing index. If the measured inbound stream throughput for both WAN and Cellular is 1600K, the LAN-Cell calculates the average load balancing indices as shown in the table below.

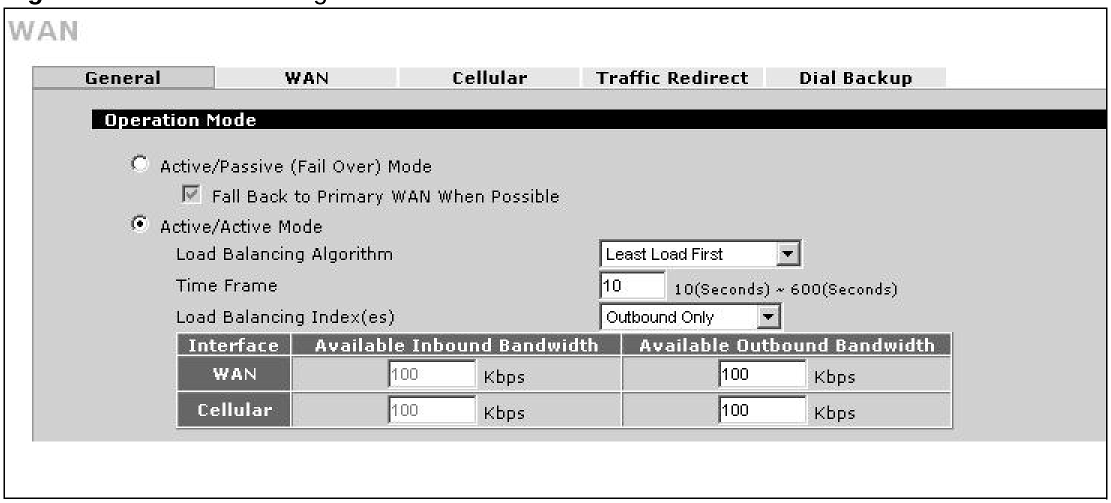
Since WAN has a smaller load balancing index (meaning that it is less utilized than Cellular), the LAN-Cell will send the next new session traffic through WAN.

Table 21 Least Load First: Example 2

INTERFACE	OUTBOUND		INBOUND		AVERAGE LOAD BALANCING INDEX (OM / OA + IM / IA) / 2
	AVAILABLE (OA)	MEASURED (OM)	AVAILABLE (IA)	MEASURED (IM)	
WAN	512 K	412 K	8000 K	1600 K	(0.8 + 0.2) / 2 = 0.5
Cellular	256 K	198 K	2000 K	1600 K	(0.77 + 0.8) / 2 = 0.79

To configure **Least Load First**, select **Least Load First** in the **Load Balancing Algorithm** field.

Figure 50 Load Balancing: Least Load First



The following table describes the related fields in this screen.

Table 22 Load Balancing: Least Load First

LABEL	DESCRIPTION
Active/Active Mode	Select **Active/Active Mode** and set the related fields to enable load balancing on the LAN-Cell.
Load Balancing Algorithm	Set the load balancing method to **Least Load First**.
Time Frame	You can set the LAN-Cell to get the measured bandwidth using the average bandwidth in the specified time interval. Enter the time interval between 10 and 600 seconds.
Load Balancing Index(es)	Specify the direction of the traffic utilization you want the LAN-Cell to use in calculating the load balancing index. Select **Outbound Only**, **Inbound Only** or **Outbound + Inbound**.
Interface	This field displays the name of the WAN interface (**WAN** and **Cellular**).

Table 22 Load Balancing: Least Load First (continued)

LABEL	DESCRIPTION
Available Inbound Bandwidth	This field is applicable when you select **Outbound + Inbound** or **Inbound Only** in the **Load Balancing Index(es)** field. Specify the inbound (or downstream) bandwidth (in kilo bites per second) for the interface. This should be the actual downstream bandwidth that your ISP provides.
Available Outbound Bandwidth	This field is applicable when you select **Outbound + Inbound** or **Outbound Only** in the **Load Balancing Index(es)** field. Specify the outbound (or upstream) bandwidth (in kilo bites per second) for the interface. This should be the actual upstream bandwidth that your ISP provides.

5.2.1.4 Weighted Round Robin

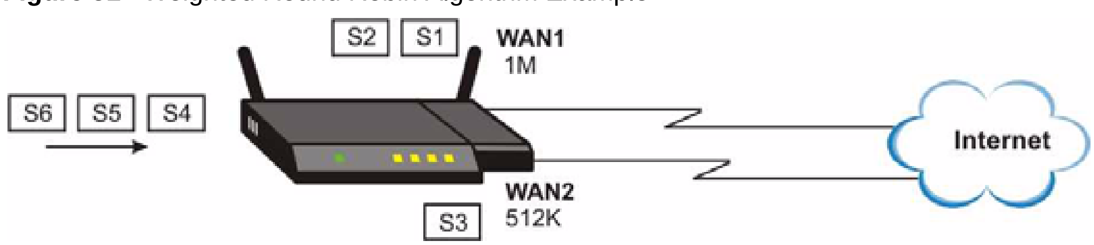
Round Robin routes traffic on a rotating basis and is activated only when a WAN interface has more traffic than the configured available bandwidth. On the LAN-Cell with two WAN interfaces, an amount of traffic is sent through the first interface. The second interface is also given an equal amount of traffic, and then the same amount of traffic is sent through the first interface again; and so on. This works in a looping fashion until there is no outgoing traffic.

Similar to the Round Robin (RR) algorithm, the Weighted Round Robin (WRR) algorithm sets the LAN-Cell to send traffic through each WAN interface in turn. In addition, the WAN interfaces are assigned weights. An interface with a larger weight gets more of the traffic than an interface with a smaller weight.

This algorithm is best suited for situations when the bandwidths set for the two WAN interfaces are different.

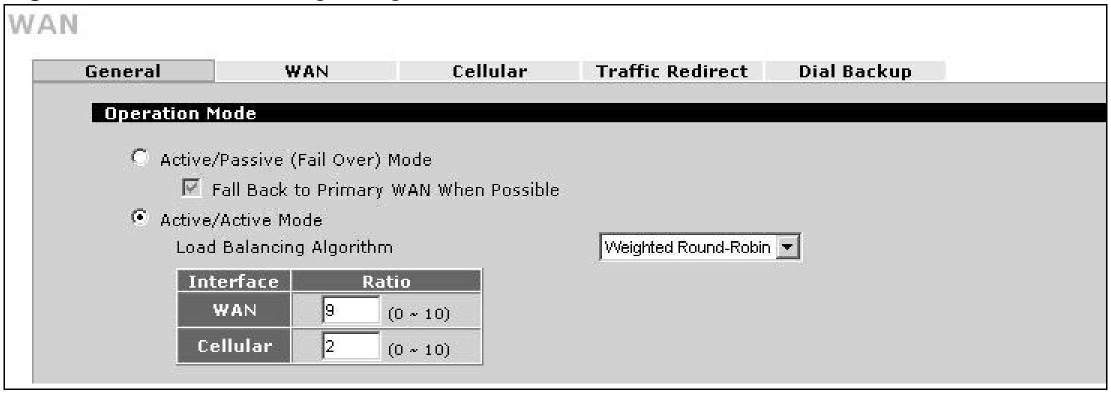
For example, in the figure below, the configured available bandwidth of WAN is 1M and Cellular is 512K. You can set the LAN-Cell to distribute the network traffic between the two interfaces by setting the weight of WAN and Cellular to 2 and 1 respectively. The LAN-Cell assigns the traffic of two sessions to WAN for every one session's traffic assigned to Cellular.

Figure 51 Weighted Round Robin Algorithm Example



To load balance using the weighted round robin method, select **Weighted Round Robin** in the **Load Balancing Algorithm** field.

Figure 52 Load Balancing: Weighted Round Robin



The following table describes the related fields in this screen.

Table 23 Load Balancing: Weighted Round Robin

LABEL	DESCRIPTION
Active/Active Mode	Select **Active/Active Mode** and set the related fields to enable load balancing on the LAN-Cell.
Load Balancing Algorithm	Set the load balancing method to **Weighted Round Robin**.
Interface	This field displays the name of the WAN interface (**WAN** and **Cellular**).
Ratio	Specify the weight for the interface. Enter 0 to set the LAN-Cell not to send traffic load to the interface. The higher the number, the bigger the weight (the more traffic sent).

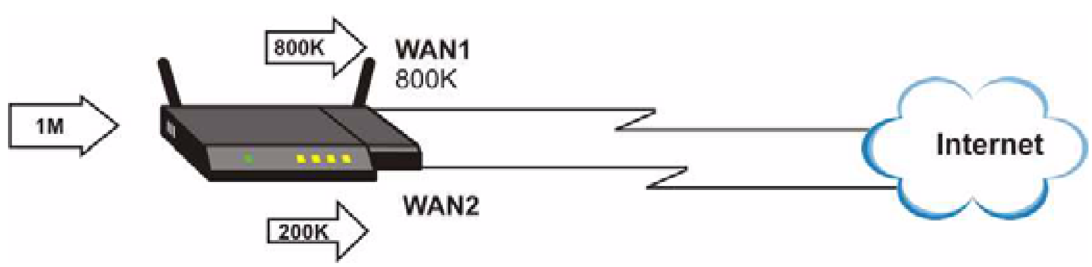
5.2.1.5 Spillover

With the spillover load balancing algorithm, the LAN-Cell sends network traffic to the primary interface until the maximum allowable load is reached, then the LAN-Cell sends the excess network traffic of new sessions to the secondary WAN interface. Configure the **Route Priority** metrics in the **WAN General** screen to determine the primary and secondary WANs.

In cases where the primary WAN interface uses an unlimited access Internet connection and the secondary WAN uses a per-use timed access plan, the LAN-Cell will only use the secondary WAN interface when the traffic load reaches the upper threshold on the primary WAN interface. This allows you to fully utilize the bandwidth of the primary WAN interface while avoiding overloading it and reducing Internet connection fees at the same time.

In the following example figure, the upper threshold of the primary WAN interface is set to 800K. The LAN-Cell sends network traffic of a new session that exceeds this limit to the secondary WAN interface.

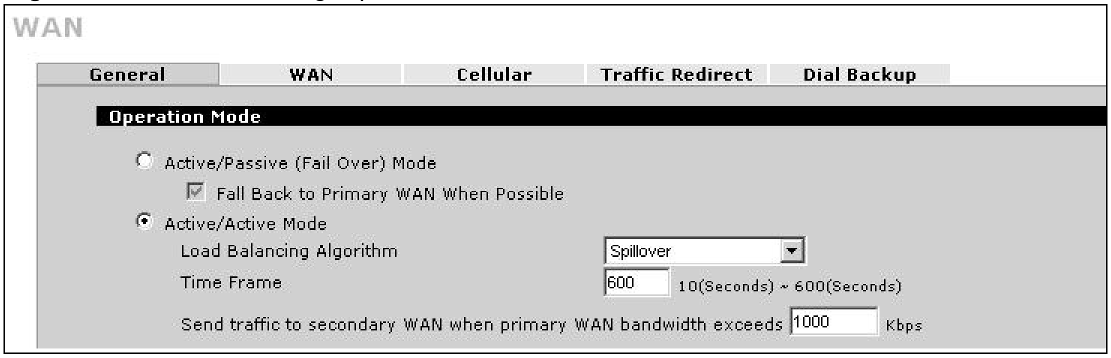
Figure 53 Spillover Algorithm Example



To load balance using the spillover method, select **Spillover** in the **Load Balancing Algorithm** field.

Configure the **Route Priority** metrics in the **WAN General** screen to determine the primary and secondary WANs. By default, WAN is the primary WAN and Cellular is the secondary WAN.

Figure 54 Load Balancing: Spillover



The following table describes the related fields in this screen.

Table 24 Load Balancing: Spillover

LABEL	DESCRIPTION
Active/Active Mode	Select **Active/Active Mode** and set the related fields to enable load balancing on the LAN-Cell.
Load Balancing Algorithm	Set the load balancing method to **Spillover**.
Time Frame	You can set the LAN-Cell to get the measured bandwidth using the average bandwidth in the specified time interval. Enter the time interval between 10 and 600 seconds.
Send traffic to secondary WAN when primary WAN bandwidth exceeds	Specify the maximum allowable bandwidth on the primary WAN. Once this maximum bandwidth is reached, the LAN-Cell sends the new session traffic that exceeds this limit to the secondary WAN. The LAN-Cell continues to send traffic of existing sessions to the primary WAN.

5.2.2 WAN Connectivity Check

The WAN Connectivity Check feature will drop the specified interface if the indicated “peer” IP address (or FQDN) does not respond to a sequence of ICMP packets. If the WAN Operation Mode is “Fail-Over”, then traffic will be directed to the next highest priority WAN interface. The LAN-Cell will periodically check the status of the down WAN interface and bring the interface back up to check if the peer IP address has begun to respond again.

WAN Connectivity can be used to create a “heart-beat” for the LAN-Cell. When a WAN interface is marked “Always-On”, direct the ICMP packets to the IP address (or FQDN) of a network monitoring application to monitor the status of the LAN-Cell’s WAN interface. This can also be used to “keep-alive” some WAN connections or applications if required.

See Table 19 on page 95 for details on configuring the WAN Connectivity Check feature.

Some ISP's (including most cellular carriers) do not acknowledge ICMP packets on their default gateways. Choose a different IP address to check.

When selecting an IP address for WAN Connectivity to check, choose either a device whose status is under your control or is well known. You can use a fully qualified domain name (FQDN) to send packets to the virtual IP address of a host with a high-availability connection to the Internet. If the IP address or host specified stops responding to ICMP packets the LAN-Cell's WAN port will also go down.

WAN Connectivity Check packets may increase the amount of data usage on your WAN ISP account (including 3G). If your ISP limits the amount of traffic allowed, consider the impact of using WAN Connectivity Check on your traffic allowance or use Cell-Sentry (Section 5.4.2 on page 118) to monitor usage.

5.3 WAN Screen

To change your LAN-Cell's WAN ISP, IP and MAC settings, click **NETWORK** > **WAN** > **WAN**. The screen differs by the encapsulation.

The WAN and Cellular IP addresses of a LAN-Cell with multiple WAN interfaces must be on different subnets.

WAN IP Assignment

Every computer on the Internet must have a unique IP address. If your networks are isolated from the Internet, for instance, only between your two branch offices, you can assign any IP addresses to the hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks.

Table 25 Private IP Address Ranges

10.0.0.0	-	10.255.255.255
172.16.0.0	-	172.31.255.255
192.168.0.0	-	192.168.255.255

You can obtain your IP address from the IANA, from an ISP or have it assigned by a private network. If you belong to a small organization and your Internet access is through an ISP, the ISP can provide you with the Internet addresses for your local networks. On the other hand, if you are part of a much larger organization, you should consult your network administrator for the appropriate IP addresses.

Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, please refer to RFC 1597, Address Allocation for Private Internets and RFC 1466, Guidelines for Management of IP Address Space.

DNS Server Address Assignment

Use DNS (Domain Name System) to map a domain name to its corresponding IP address and vice versa, for instance, the IP address of www.proxicast.com is 63.135.115.22. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it.

The LAN-Cell can get the DNS server addresses in the following ways.

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

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

3 You can manually enter the IP addresses of other DNS servers. These servers can be public or private. A DNS server could even be behind a remote IPSec router (see Section on page 308).

WAN MAC Address

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, 00:1B:39:00:00:02.

You can configure the WAN port's MAC address by either using the factory default or cloning the MAC address from a computer on your LAN. Once it is successfully configured, the address will be copied to the "rom" file (ProxiOS configuration file). It will not change unless you change the setting or upload a different "rom" file.

Table 26 Example of Network Properties for LAN Servers with Fixed IP Addresses

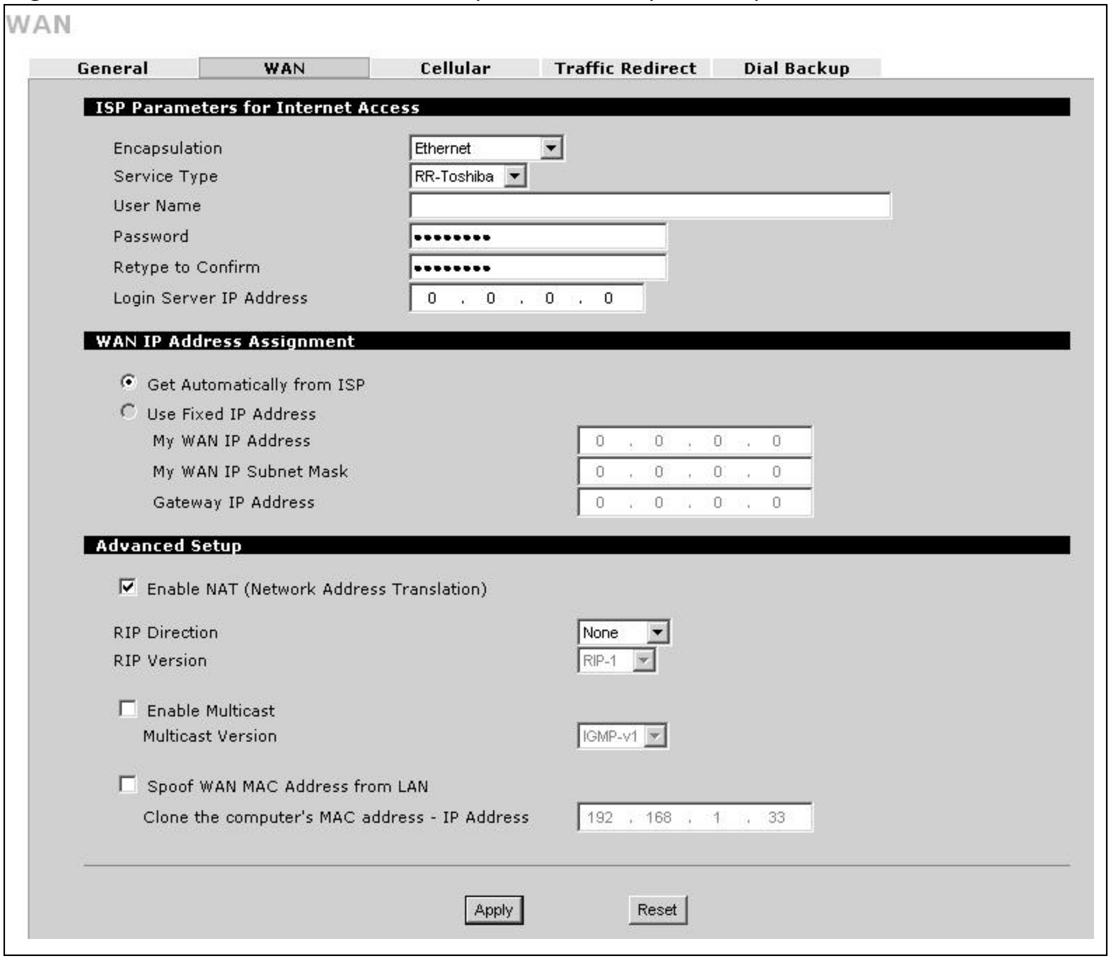
Choose an IP address	192.168.1.2-192.168.1.32; 192.168.1.65-192.168.1.254.
Subnet mask	255.255.255.0
Gateway (or default route)	192.168.1.1(LAN-Cell LAN IP)

5.3.1 WAN Ethernet Encapsulation

For ISPs (such as Telstra) that send UDP heartbeat packets to verify that the customer is still online, please create a **WAN-to-WAN/LAN-Cell** firewall rule for those packets. Contact your ISP to find the correct port number.

The screen shown next is for **Ethernet** encapsulation.

Figure 55 NETWORK > WAN > WAN (Ethernet Encapsulation)



The following table describes the labels in this screen.

Table 27 NETWORK > WAN > WAN (Ethernet Encapsulation)

LABEL	DESCRIPTION
ISP Parameters for Internet Access	
Encapsulation	You must choose the **Ethernet** option when the WAN port is used as a regular Ethernet.
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.
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 is correctly.
Login Server IP Address	Type the authentication server IP address here if your ISP gave you one. This field is not available for Telia Login.
Login Server (Telia Login only)	Type the domain name of the Telia login server, for example login1.telia.com.

Table 27 NETWORK > WAN > WAN (Ethernet Encapsulation) (continued)

LABEL	DESCRIPTION
Relogin Every(min) (Telia Login only)	The Telia server logs the LAN-Cell out if the LAN-Cell does not log in periodically. Type the number of minutes from 1 to 59 (30 default) for the LAN-Cell to wait between logins.
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**.
Advanced Setup	
Enable NAT (Network Address Translation)	Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network (for example a private IP address used in a local network) to a different IP address known within another network (for example a public IP address used on the Internet). Select this check box to enable NAT.
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 LAN-Cell will broadcast its routing table periodically. When set to **Both** or **In Only**, the LAN-Cell will incorporate RIP information that it receives. When set to **None**, the LAN-Cell 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 LAN-Cell 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**.
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.

Table 27 NETWORK > WAN > WAN (Ethernet Encapsulation) (continued)

LABEL	DESCRIPTION
Multicast Version	Choose **None** (default), **IGMP-V1** or **IGMP-V2**. IGMP (Internet Group Multicast Protocol) is a session-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.
Spoof WAN MAC Address from LAN	You can configure the WAN port's MAC address by either using the factory assigned default MAC Address or cloning the MAC address of a computer on your LAN. By default, the LAN-Cell uses the factory assigned MAC Address to identify itself on the WAN. Otherwise, select the check box next to **Spoof WAN MAC Address from LAN** and enter the IP address of the computer on the LAN whose MAC you are cloning. Once it is successfully configured, the address will be copied to the rom file (ProxiOS configuration file). It will not change unless you change the setting or upload a different ROM file.
Clone the computer’s MAC address – IP Address	Enter the IP address of the computer on the LAN whose MAC you are cloning. If you clone the MAC address of a computer on your LAN, it is recommended that you clone the MAC address prior to hooking up the WAN port.
Apply	Click **Apply** to save your changes back to the LAN-Cell.
Reset	Click **Reset** to begin configuring this screen afresh.

5.3.2 PPPoE Encapsulation

The LAN-Cell supports PPPoE (Point-to-Point Protocol over Ethernet). PPPoE is an IETF 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).

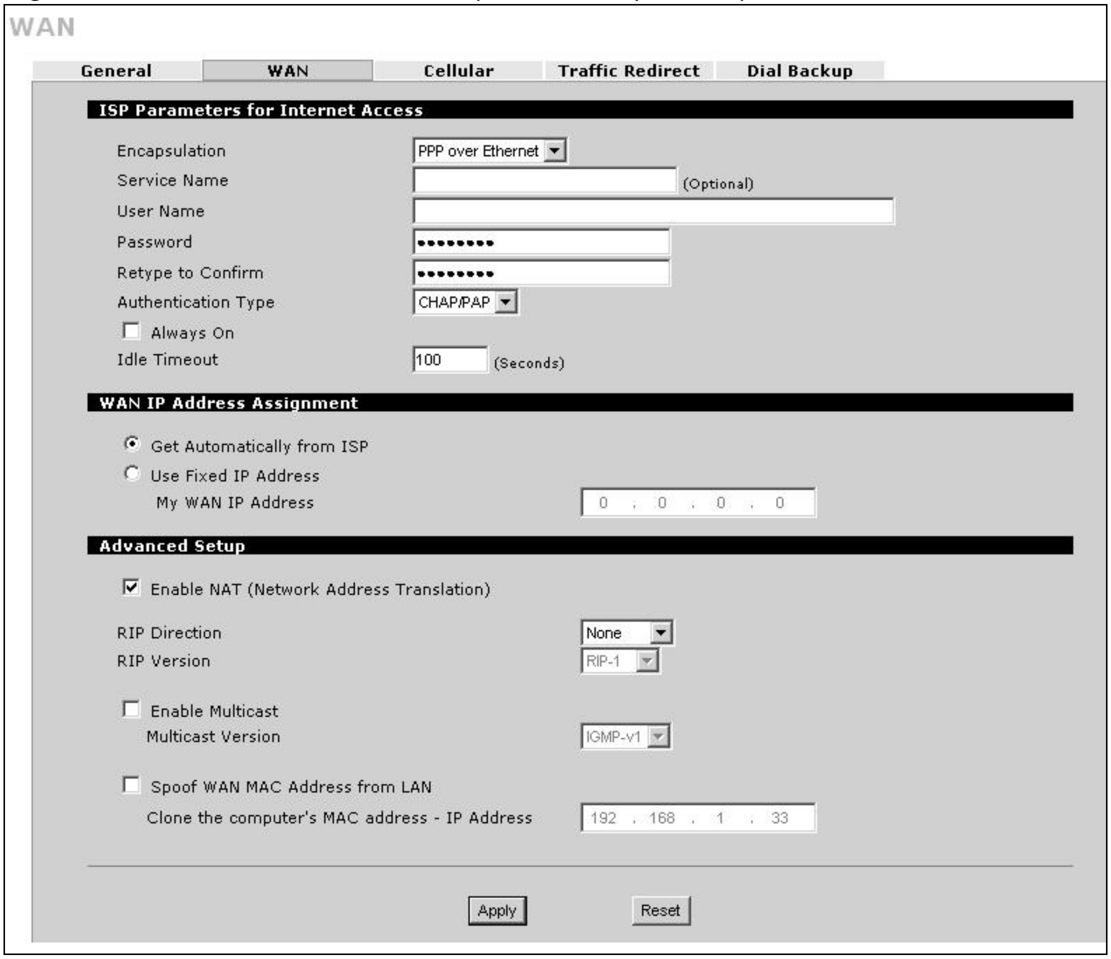
One of the benefits of PPPoE is the ability to let you access one of multiple network services, a function known as dynamic service selection. This enables the service provider to easily create and offer new IP services for individuals.

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 LAN-Cell (rather than individual computers), the computers on the LAN do not need PPPoE software installed, since the LAN-Cell does that part of the task. Furthermore, with NAT, all of the LANs’ computers will have access.

The screen shown next is for **PPPoE** encapsulation.

Figure 56 NETWORK > WAN > WAN (PPPoE Encapsulation)



The following table describes the labels in this screen.

Table 28 NETWORK > WAN > WAN (PPPoE Encapsulation)

LABEL	DESCRIPTION
ISP Parameters for Internet Access	
Encapsulation	Select **PPPoE** for a dial-up connection using PPPoE.
Service Name	Type the PPPoE service name provided to you by your ISP. 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 is correctly.
Authentication Type	The LAN-Cell supports PAP (Password Authentication Protocol) and CHAP (Challenge Handshake Authentication Protocol). CHAP is more secure than PAP; however, PAP is readily available on more platforms. Use the drop-down list box to select an authentication protocol for outgoing calls. Options are: **CHAP/PAP** - Your LAN-Cell accepts either CHAP or PAP when requested by this remote node. **CHAP** - Your LAN-Cell accepts CHAP only. **PAP** - Your LAN-Cell accepts PAP only.

Table 28 NETWORK > WAN > WAN (PPPoE Encapsulation) (continued)

LABEL	DESCRIPTION
Nailed-Up	Select **Nailed-Up** if you do not want the connection to time out.
Idle Timeout	This value specifies the time in seconds that elapses before the LAN-Cell automatically disconnects from the PPPoE server.
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.**
Advanced Setup	
Enable NAT (Network Address Translation)	Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network (for example a private IP address used in a local network) to a different IP address known within another network (for example a public IP address used on the Internet). Select this checkbox to enable NAT. For more information about NAT see Chapter 13 on page 289.
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 LAN-Cell will broadcast its routing table periodically. When set to **Both** or **In Only**, the LAN-Cell will incorporate RIP information that it receives. When set to **None**, the LAN-Cell 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 LAN-Cell 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**.
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	Choose **None** (default), **IGMP-V1** or **IGMP-V2**. IGMP (Internet Group Multicast Protocol) is a session-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.

Table 28 NETWORK > WAN > WAN (PPPoE Encapsulation) (continued)

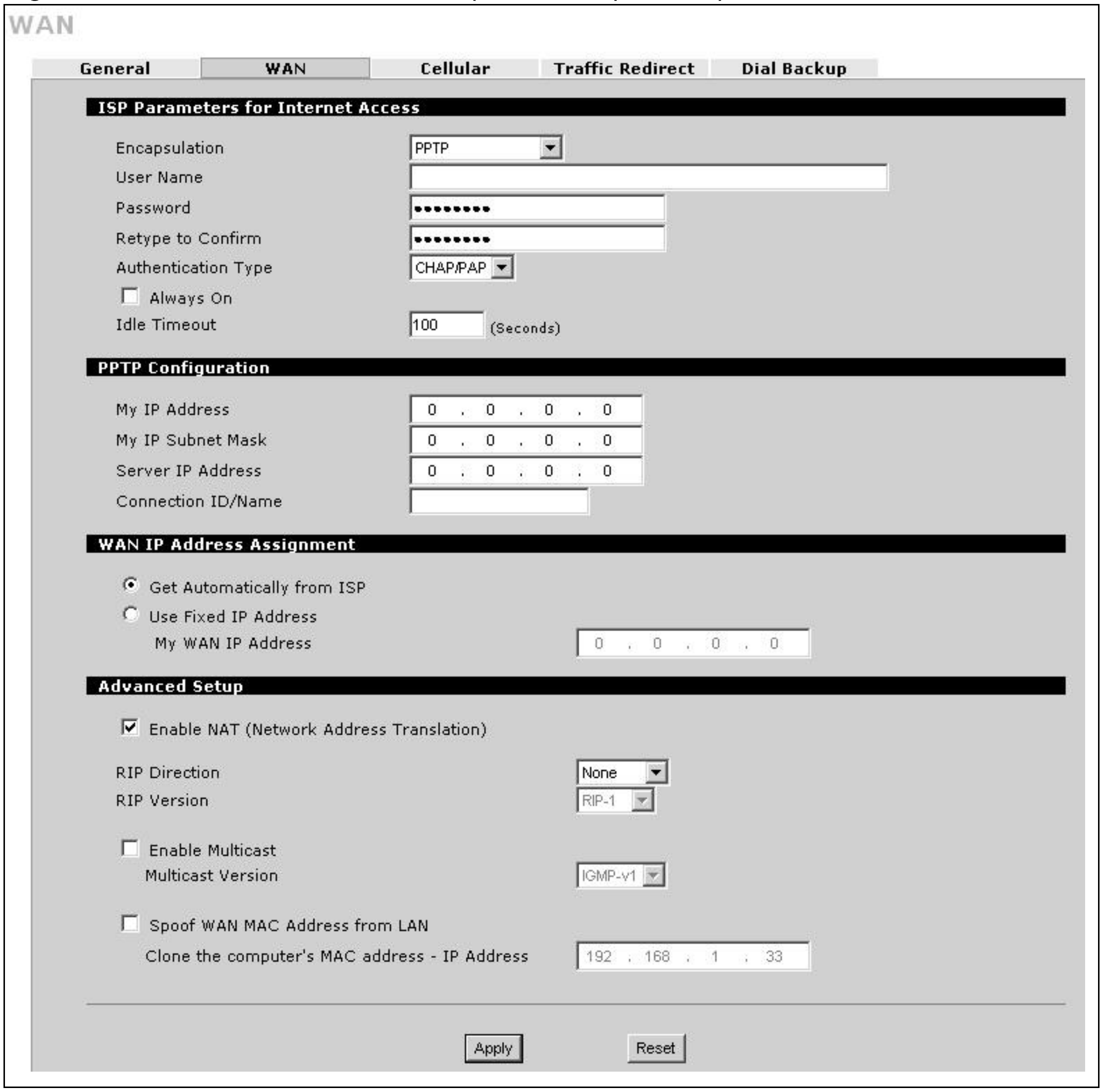
LABEL	DESCRIPTION
Spoof WAN MAC Address from LAN	You can configure the WAN port's MAC address by either using the factory assigned default MAC Address or cloning the MAC address of a computer on your LAN. By default, the LAN-Cell uses the factory assigned MAC Address to identify itself on the WAN. Otherwise, select the check box next to **Spoof WAN MAC Address from LAN** and enter the IP address of the computer on the LAN whose MAC you are cloning. Once it is successfully configured, the address will be copied to the rom file (ProxiOS configuration file). It will not change unless you change the setting or upload a different ROM file.
Clone the computer's MAC address – IP Address	Enter the IP address of the computer on the LAN whose MAC you are cloning. If you clone the MAC address of a computer on your LAN, it is recommended that you clone the MAC address prior to hooking up the WAN port.
Apply	Click **Apply** to save your changes back to the LAN-Cell.
Reset	Click **Reset** to begin configuring this screen afresh.

5.3.3 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. The screen shown next is for **PPTP** encapsulation.

Figure 57 NETWORK > WAN > WAN (PPTP Encapsulation)



The following table describes the labels in this screen.

Table 29 NETWORK > WAN > WAN (PPTP Encapsulation)

LABEL	DESCRIPTION
ISP Parameters for Internet Access	
Encapsulation	Set the encapsulation method to **PPTP**. The LAN-Cell 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.
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.

Table 29 NETWORK > WAN > WAN (PPTP Encapsulation) (continued)

LABEL	DESCRIPTION
Authentication Type	The LAN-Cell supports PAP (Password Authentication Protocol) and CHAP (Challenge Handshake Authentication Protocol). CHAP is more secure than PAP; however, PAP is readily available on more platforms. Use the drop-down list box to select an authentication protocol for outgoing calls. Options are: **CHAP/PAP** - Your LAN-Cell accepts either CHAP or PAP when requested by this remote node. **CHAP** - Your LAN-Cell accepts CHAP only. **PAP** - Your LAN-Cell accepts PAP only.
Nailed-up	Select **Nailed-Up** if you do not want the connection to time out.
Idle Timeout	This value specifies the time in seconds that elapses before the LAN-Cell automatically disconnects from the PPTP server.
PPTP Configuration	
My IP Address	Type the (static) IP address assigned to you by your ISP.
My IP Subnet Mask	Your LAN-Cell 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 LAN-Cell.
Server IP Address	Type the IP address of the PPTP server.
Connection ID/ Name	Type your identification name for the PPTP server.
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**.
Advanced Setup	
Enable NAT (Network Address Translation)	Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network (for example a private IP address used in a local network) to a different IP address known within another network (for example a public IP address used on the Internet). Select this checkbox to enable NAT. For more information about NAT see Chapter 13 on page 289.
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 LAN-Cell will broadcast its routing table periodically. When set to **Both** or **In Only**, the LAN-Cell will incorporate RIP information that it receives. When set to **None**, the LAN-Cell will not send any RIP packets and will ignore any RIP packets received. By default, **RIP Direction** is set to **Both**.

Table 29 NETWORK > WAN > WAN (PPTP Encapsulation) (continued)

LABEL	DESCRIPTION
RIP Version	The **RIP Version** field controls the format and the broadcasting method of the RIP packets that the LAN-Cell 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**.
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	Choose **None** (default), **IGMP-V1** or **IGMP-V2**. IGMP (Internet Group Multicast Protocol) is a session-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.
Spoof WAN MAC Address from LAN	You can configure the WAN port's MAC address by either using the factory assigned default MAC Address or cloning the MAC address of a computer on your LAN. By default, the LAN-Cell uses the factory assigned MAC Address to identify itself on the WAN. Otherwise, select the check box next to **Spoof WAN MAC Address from LAN** and enter the IP address of the computer on the LAN whose MAC you are cloning. Once it is successfully configured, the address will be copied to the rom file (ProxiOS configuration file). It will not change unless you change the setting or upload a different ROM file.
Clone the computer's MAC address – IP Address	Enter the IP address of the computer on the LAN whose MAC you are cloning. If you clone the MAC address of a computer on your LAN, it is recommended that you clone the MAC address prior to hooking up the WAN port.
Apply	Click **Apply** to save your changes back to the LAN-Cell.
Reset	Click **Reset** to begin configuring this screen afresh.

5.4 Cellular (3G WAN) Screen

3G (Third Generation) is a digital, packet-switched wireless technology. Bandwidth usage is optimized as multiple users share the same channel and bandwidth is only allocated to users when they send data. It allows fast transfer of voice and non-voice data and provides broadband Internet access to mobile devices.

If the signal strength of a 3G network is too low, the 3G card may switch to an available 2.5G or 2.75G network.

To change your LAN-Cell's 3G WAN settings, click **NETWORK** > **WAN** > **Cellular**.

The actual data rate you obtain varies depending the 3G card you use, the signal strength to the service provider’s base station, etc.

Turn the LAN-Cell off before you install or remove a 3G card.

The WAN and Cellular IP addresses of the LAN-Cell must be on different subnets.

The WIRELESS > CELLULAR menu in the Navigation Panel is a short-cut directly to the Cellular WAN parameter screen (Figure 58 on page 115).

5.4.1 Configuring 3G Network Access Parameters

Figure 58 NETWORK > WAN > Cellular (3G WAN) (CDMA)

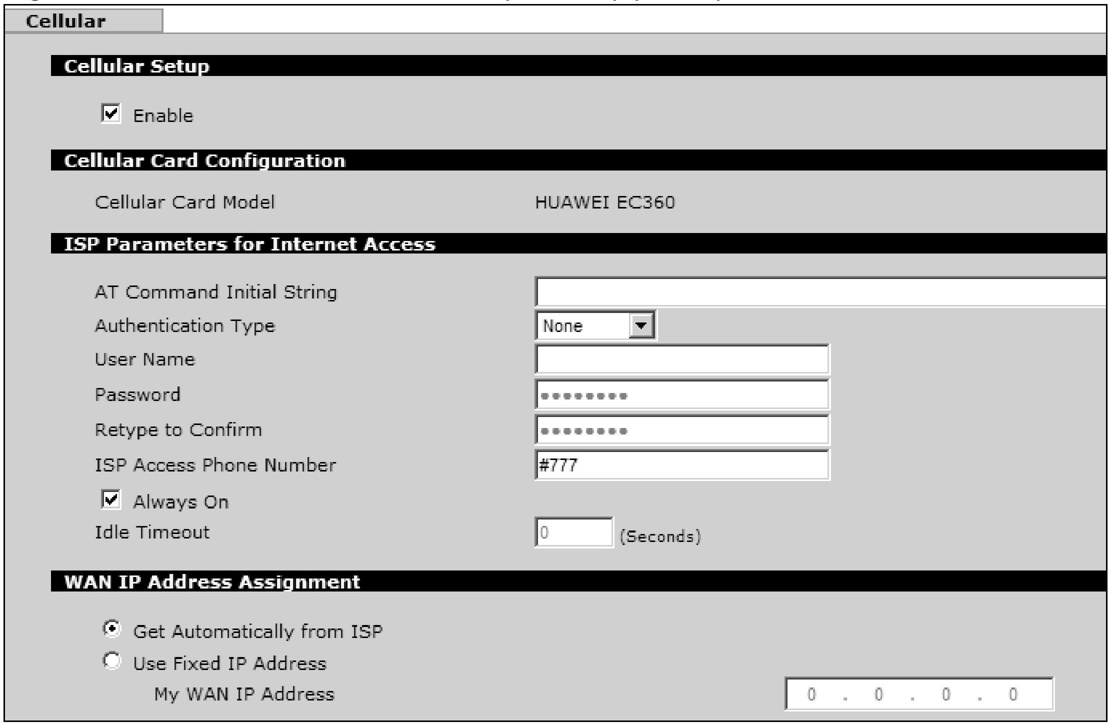
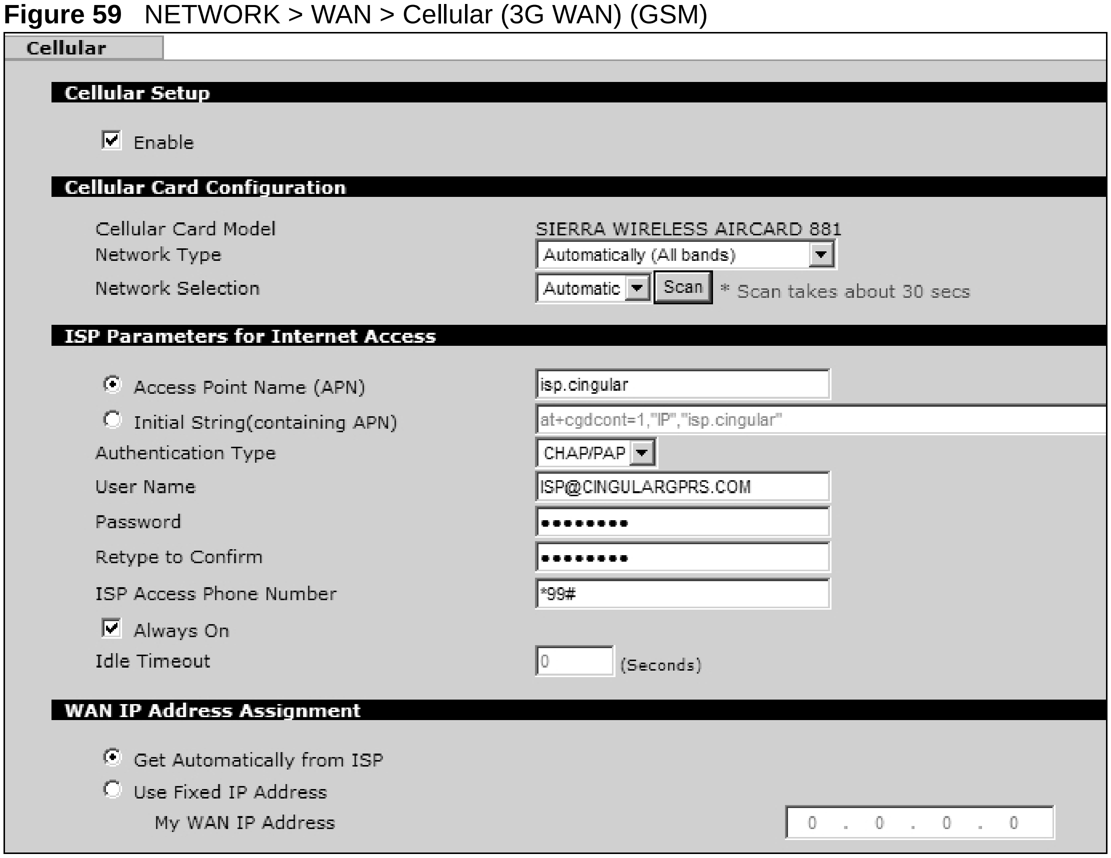


Figure 59 NETWORK > WAN > Cellular (3G WAN) (GSM)



The following table describes the labels in this screen.

Table 30 NETWORK > WAN > Cellular (3G WAN)

LABEL	DESCRIPTION
Cellular Card Configuration	
Cellular Card Model	This displays the manufacturer and model name of your 3G card if you inserted one in the LAN-Cell. Otherwise, it displays **Not Installed**.
Network Type	Select the type of the network (UMTS/HSDPA only, GPRS/EDGE only, GSM all or WCDMA all) to which you want the card to connect. Otherwise, select Automatically to have the card connect to an available network using the default settings on the cellular card. The types of the network vary depending on the cellular card you inserted. This setting is saved to the flash of your cellular card. This field is not available if you insert a CDMA cellular card.
Network Selection	Select a service provider to which you want the card to connect. Otherwise, select Automatic to have the LAN-Cell use the default settings on the cellular card and connect to your service provider's base station. This shows Automatic only by default. Click Scan to have the LAN-Cell search for and display the available service providers. This field resets to the default setting (Automatic) if the LAN-Cell restarts. This field is not available if you insert a CDMA cellular card.
ISP Parameters for Internet Access	
Access Point Name (APN)	Enter the APN (Access Point Name) provided by your service provider. Connections with different APNs may provide different services (such as Internet access or MMS (Multi-Media Messaging Service)) and charge method. You can enter up to 31 ASCII printable characters. Spaces are allowed.
Initial String (containing APN)	Select this option and enter the initial string and APN if you know how to configure or your ISP provides a string, which would include the APN, to initialize the cellular card. You can enter up to 72 ASCII printable characters. Spaces are allowed. This field is available only when you insert a GSM cellular card.
AT Command Initial String	Enter the AT command initial string provided by your ISP to initialize the cellular card. If it was not given, leave the field at the default. You can enter up to 72 ASCII printable characters. Spaces are allowed. This field is available when you insert a CDMA cellular card.
Authentication Type	The LAN-Cell supports PAP (Password Authentication Protocol) and CHAP (Challenge Handshake Authentication Protocol). CHAP is more secure than PAP; however, PAP is readily available on more platforms. Use the drop-down list box to select an authentication protocol for outgoing calls. Options are: CHAP/PAP - Your LAN-Cell accepts either CHAP or PAP when requested by the ISP. CHAP - Your LAN-Cell accepts CHAP only. PAP - Your LAN-Cell accepts PAP only. None - Your LAN-Cell does not send your user name and password for authentication. The user name and password fields are grayed out. Select this option if your ISP did not give you a user name and password.
User Name	Type the user name (of up to 31 ASCII printable characters) given to you by your service provider.
Password	Type the password (of up to 31 ASCII printable characters) associated with the user name above.
Retype to Confirm	Type your password again to make sure that you have entered is correctly.

Table 30 NETWORK > WAN > Cellular (3G WAN) (continued)

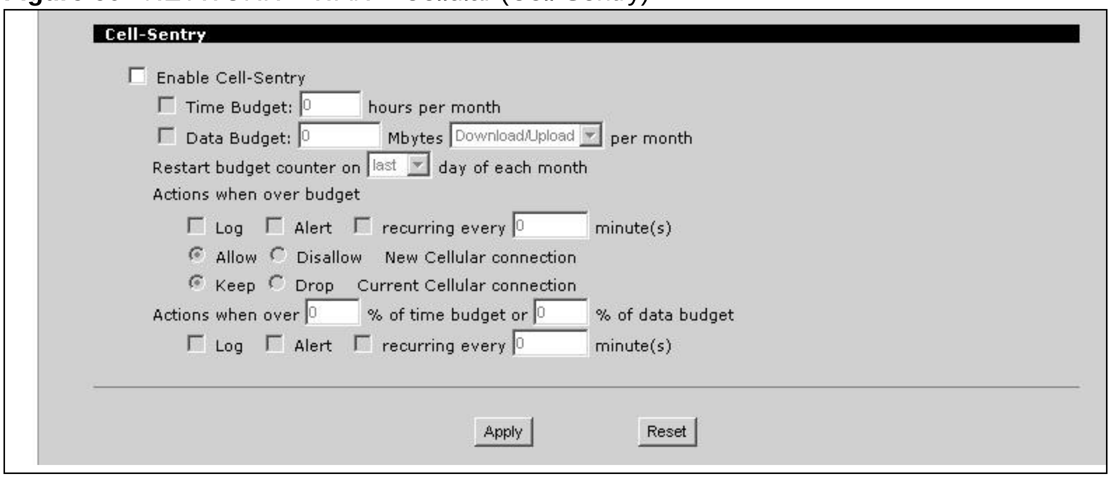
LABEL	DESCRIPTION
PIN Code	Enter the PIN (Personal Identification Number) code (four to eight digits, 0000 for example) provided by your ISP. If you enter the PIN code incorrectly, the cellular card may be blocked by your ISP and you cannot use the account to access the Internet. If your ISP disabled PIN code authentication, enter an arbitrary number. This field is available only when you insert a GSM cellular card. .
ISP Access Phone Number	Enter the phone number (dial string) used to dial up a connection to your service provider's base station. Your ISP should provide the dial string. By default, *99# is the dial string for GSM-based networks and #777 is the dial string for CDMA-based networks.
Always On	Select **Always On** if you do not want the connection to time out.
Idle Timeout	This value specifies the time in seconds that elapses before the LAN-Cell automatically disconnects from the ISP.
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 and is the correct choice for most cellular ISPs, even when a “static” IP is assigned to the 3G card.
Use Fixed IP Address	Select this option If the ISP assigned a fixed IP address, subnet mask and default gateway. This is not commonly used by 3G cellular network operators, even when a “static” IP is assigned to the 3G card.
My WAN IP Address	Enter your WAN IP address in this field if you selected **Use Fixed IP Address**.
Advanced Setup	
Enable NAT (Network Address Translation)	Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network (for example a private IP address used in a local network) to a different IP address known within another network (for example a public IP address used on the Internet). Select this checkbox to enable NAT. For more information about NAT see Chapter 13 on page 289.
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	Choose **None** (default), **IGMP-V1** or **IGMP-V2**. IGMP (Internet Group Multicast Protocol) is a session-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 LAN-Cell.
Reset	Click **Reset** to begin configuring this screen afresh.

5.4.2 Configuring Cell-Sentry Budget Control

Cell-Sentry enables you to monitor and/or limit the amount of usage on the Cellular WAN interface. This feature enables you to utilize a carrier's lower cost data service plans and ensures that you do not exceed your plan allowance.

Actual usage statistics on the carrier's 3G network may differ from the LAN-Cell's counters. Set your budget limits lower than the maximum allowed on your plan.

Figure 60 NETWORK > WAN > Cellular (Cell-Sentry)



The following table describes the labels in this screen.

Table 31 NETWORK > WAN > Cellular (Cell-Sentry)

LABEL	DESCRIPTION
Enable Cell-Sentry	Select this check box to set a monthly limit for the user account of the installed cellular card. You must insert a cellular card before you enable budget control on the LAN-Cell. You can set a limit on the total traffic and/or call time. The LAN-Cell takes the actions you specified when a limit is exceeded during the month.
Time Budget	Select this check box and specify the amount of time (in hours) that the cellular connection can be used within one month. If you change the value after you configure and enable budget control, the LAN-Cell resets the statistics.
Data Budget	Select this check box and specify how much downstream and/or upstream data (in Mbytes) can be transmitted via the cellular connection within one month. Select **Download** to set a limit on the downstream traffic (from the ISP to the LAN-Cell). Select **Upload** to set a limit on the upstream traffic (from the LAN-Cell to the ISP). Select **Download/Upload** to set a limit on the total traffic in both directions. If you change the value after you configure and enable budget control, the LAN-Cell resets the statistics.

Table 31 NETWORK > WAN > Cellular (Cell-Sentry) (continued)

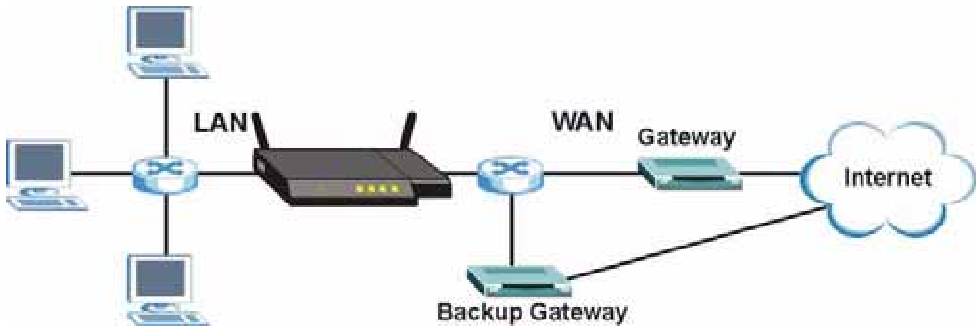
LABEL	DESCRIPTION
Restart budget counter on	Select the date on which the LAN-Cell resets the budget every month. If the date you selected is not available in a month, such as 30th or 31th, the LAN-Cell resets the budget on the last day of the month. To more closely match your ISP's usage counters, set this value to the date of your monthly billing cycle.
Actions when over budget	Specify the actions the LAN-Cell takes when the time or data limit is exceeded. Select **Log** to create a log entry. Select **Alert** to create an alert. This option is available only when you select Log. If you select Log, you can also select recurring every to have the LAN-Cell send the log for this event periodically and specify how often (from 1 to 4600 minutes) to send a log. Select **Allow** to permit new cellular connections or **Disallow** to drop/block new cellular connections. Select **Keep** to maintain the existing cellular connection or **Drop** to disconnect it. You cannot select Allow and Drop at the same time. If you select Disallow and Keep, the LAN-Cell allows you to transmit data using the current connection, but you cannot build a new connection if the existing connection is disconnected.
Actions when over % of time budget or % of data budget	Specify the actions the LAN-Cell takes when the specified percentage of time budget or data limit is exceeded. Enter a number from 1 to 99 in the percentage fields. If you change the value after you configure and enable budget control, the LAN-Cell resets the statistics. Select **Log** to create a log entry. Select **Alert** to create an alert. This option is available only when you select Log. If you select Log, you can also select recurring every to have the LAN-Cell send the log for this event periodically and specify how often (from 1 to 4600 minutes) to send a log.
Apply	Click **Apply** to save your changes back to the LAN-Cell.
Reset	Click **Reset** to begin configuring this screen afresh.

To have the LAN-Cell send you an E-Mail when Cell-Sentry detects a specified threshold, be sure to configure the LAN-Cell's Log/Alert E-Mail feature (Section 21.3 on page 377).

5.5 Traffic Redirect Screen

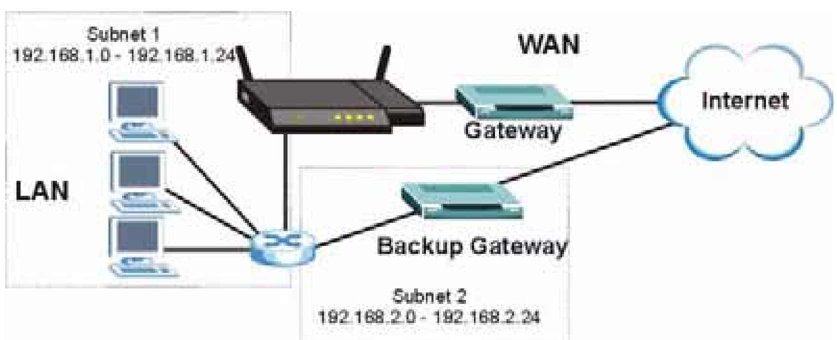
Traffic redirect forwards WAN traffic to a backup gateway when the LAN-Cell cannot connect to the Internet through its normal gateway. Connect the backup gateway on the WAN so that the LAN-Cell still provides firewall protection for the LAN.

Figure 61 Traffic Redirect WAN Setup



IP alias 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 LAN-Cell 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/LAN-Cell firewall rule that forwards packets from the protected LAN (Subnet 1) to the backup gateway (Subnet 2).

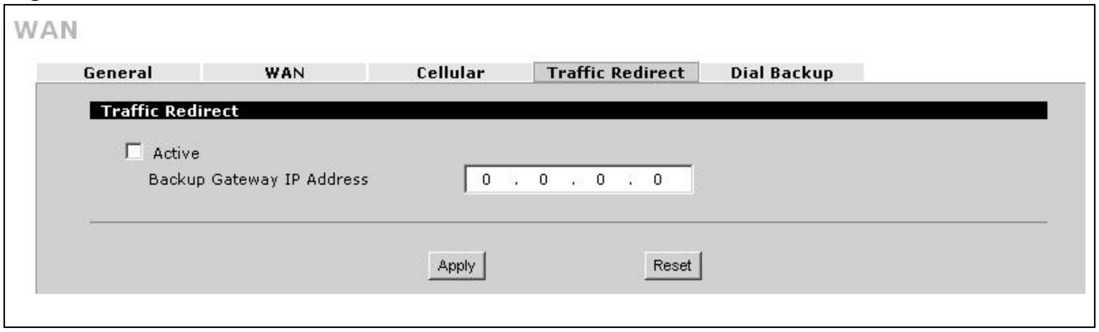
Figure 62 Traffic Redirect LAN Setup



5.5.1 Configuring Traffic Redirect

To change your LAN-Cell's traffic redirect settings, click **NETWORK** > **WAN** > **Traffic Redirect**. The screen appears as shown.

Figure 63 NETWORK > WAN > Traffic Redirect



The following table describes the labels in this screen.

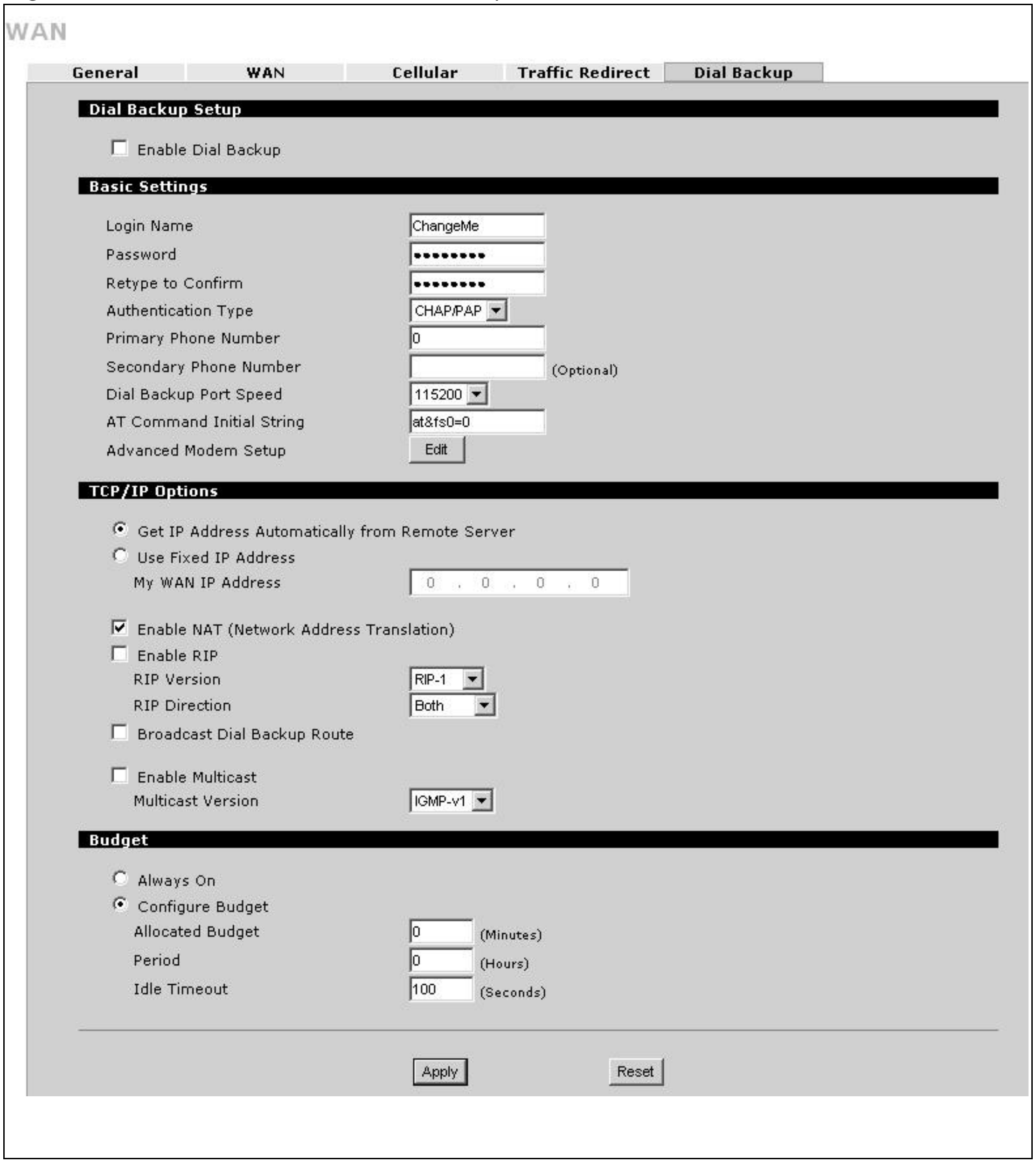
Table 32 NETWORK > WAN > Traffic Redirect

LABEL	DESCRIPTION
Active	Select this check box to have the LAN-Cell 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 LAN-Cell automatically forwards traffic to this IP address if the LAN-Cell's Internet connection terminates.
Apply	Click **Apply** to save your changes back to the LAN-Cell.
Reset	Click **Reset** to begin configuring this screen afresh.

5.6 Dial Backup Screen

Click **NETWORK** > **WAN** > **Dial Backup** to display the **Dial Backup** screen. Use this screen to configure the backup WAN dial-up connection.

Figure 64 NETWORK > WAN > Dial Backup



The following table describes the labels in this screen.

Table 33 NETWORK > WAN > Dial Backup

LABEL	DESCRIPTION
Dial Backup Setup	
Enable Dial Backup	Select this check box to turn on dial backup.
Basic Settings	

Table 33 NETWORK > WAN > Dial Backup (continued)

LABEL	DESCRIPTION
Login Name	Type the login name assigned by your ISP.
Password	Type the password assigned by your ISP.
Retype to Confirm	Type your password again to make sure that you have entered is correctly.
Authentication Type	Use the drop-down list box to select an authentication protocol for outgoing calls. Options are: **CHAP/PAP** - Your LAN-Cell accepts either CHAP or PAP when requested by this remote node. **CHAP** - Your LAN-Cell accepts CHAP only. **PAP** - Your LAN-Cell accepts 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 LAN-Cell 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.
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.
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 **Edit** to display the **Advanced Setup** screen and edit the details of your dial backup setup.
TCP/IP Options	
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, 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 LAN-Cell, not the remote router.
Enable NAT (Network Address Translation)	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. Select the check box to enable NAT. Clear the check box to disable NAT so the LAN-Cell does not perform any NAT mapping for the dial backup connection.
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 Version	The **RIP Version** field controls the format and the broadcasting method of the RIP packets that the LAN-Cell 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 33 NETWORK > WAN > Dial Backup (continued)

LABEL	DESCRIPTION
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 LAN-Cell will broadcast its routing table periodically. When set to **Both** or **In Only**, the LAN-Cell will incorporate RIP information that it receives.
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*.
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 LAN-Cell to the remote node) for the LAN-Cell to wait before it automatically disconnects the dial backup connection. This option applies only when the LAN-Cell 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 LAN-Cell.
Reset	Click **Reset** to begin configuring this screen afresh.

The Dial-Backup Budget is unrelated to the Cell-Sentry Budget.

5.6.1 Advanced Modem Setup

5.6.1.1 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.

5.6.1.2 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 LAN-Cell uses this hardware signal to force the WAN device to hang up, in addition to issuing the drop command ATH.

5.6.1.3 Response Strings

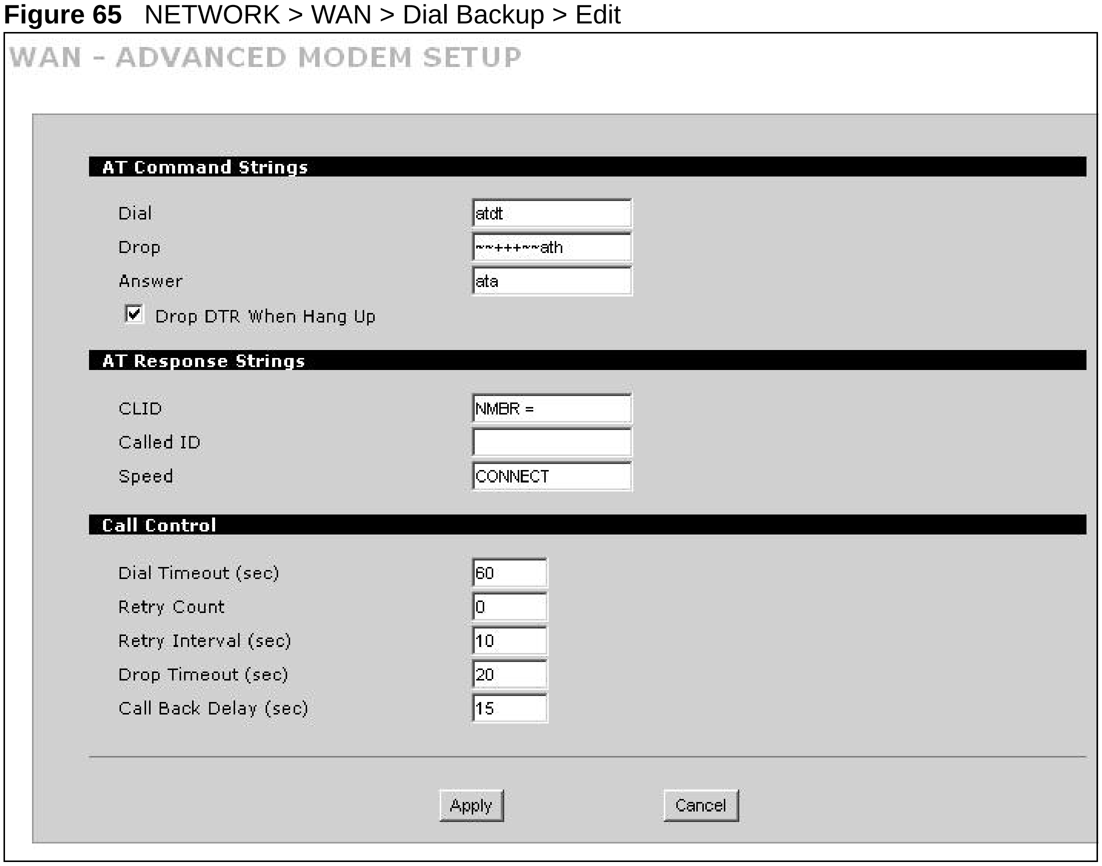
The response strings tell the LAN-Cell the tags, or labels, immediately preceding the various call parameters sent from the WAN device. The response strings have not been standardized; please consult the documentation of your WAN device to find the correct tags.

5.6.2 Configuring Advanced Modem Setup

Click the **Edit** button in the **Dial Backup** screen to display the **Advanced Setup** screen.

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

Figure 65 NETWORK > WAN > Dial Backup > Edit



The following table describes the labels in this screen.

Table 34 NETWORK > WAN > Dial Backup > Edit

LABEL	DESCRIPTION
AT Command Strings	
Dial	Type the AT Command string to make a call.
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.
Answer	Type the AT Command string to answer a call.
Drop DTR When Hang Up	Select this check box to have the LAN-Cell 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 LAN-Cell capture the CLID in the AT response string that comes from the WAN device. CLID is required for CLID authentication.
Called ID	Type the keyword preceding the dialed number.
Speed	Type the keyword preceding the connection speed.
Call Control	
Dial Timeout (sec)	Type a number of seconds for the LAN-Cell to try to set up an outgoing call before timing out (stopping).
Retry Count	Type a number of times for the LAN-Cell to retry a busy or no-answer phone number before blacklisting the number.
Retry Interval (sec)	Type a number of seconds for the LAN-Cell to wait before trying another call after a call has failed. This applies before a phone number is blacklisted.
Drop Timeout (sec)	Type the number of seconds for the LAN-Cell to wait before dropping the DTR signal if it does not receive a positive disconnect confirmation.
Call Back Delay (sec)	Type a number of seconds for the LAN-Cell to wait between dropping a callback request call and dialing the corresponding callback call.
Apply	Click **Apply** to save your changes back to the LAN-Cell.
Cancel	Click **Cancel** to exit this screen without saving.

6

DMZ Screens

6.1 Overview

The DeMilitarized Zone (DMZ) 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.

6.1.1 What You Can Do in the DMZ Screens

- Use the **DMZ** screen (Section 6.2 on page 129) to configure TCP/IP, DHCP, IP/MAC binding and NetBIOS settings on the DMZ.
- Use the **Static DHCP** screen (Section 6.3 on page 132) to configure the IP addresses assigned to devices in the DMZ by DHCP.
- Use the **IP Alias** screen (Section 6.4 on page 133) to configure IP alias settings on the LAN-Cell's DMZ ports.
- Use the **Port Roles** screen (Section 6.5 on page 135) to configure DMZ ports on the LAN-Cell.

6.1.2 What You Need To Know About DMZ

DMZ and Security

It is highly recommended that you connect all of your public servers to the DMZ port(s).

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.

DMZ and Firewall Rules

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.

DMZ and NAT

See Chapter 13 on page 289 for an overview of NAT.

If you do not configure SUA NAT or any full feature NAT mapping rules for the public IP addresses on the DMZ, the LAN-Cell will route traffic to the public IP addresses on the DMZ without performing NAT. This may be useful for hosting servers for NAT unfriendly applications.

If the DMZ computers use private IP addresses, use NAT if you want to make them publicly accessible.

DHCP

Like the LAN, the LAN-Cell can also assign TCP/IP configuration via DHCP to computers connected to the DMZ ports.

See Section 4.3 on page 83 for more information on DHCP.

IP Alias

See Section 4.4 on page 84 for more information on IP alias.

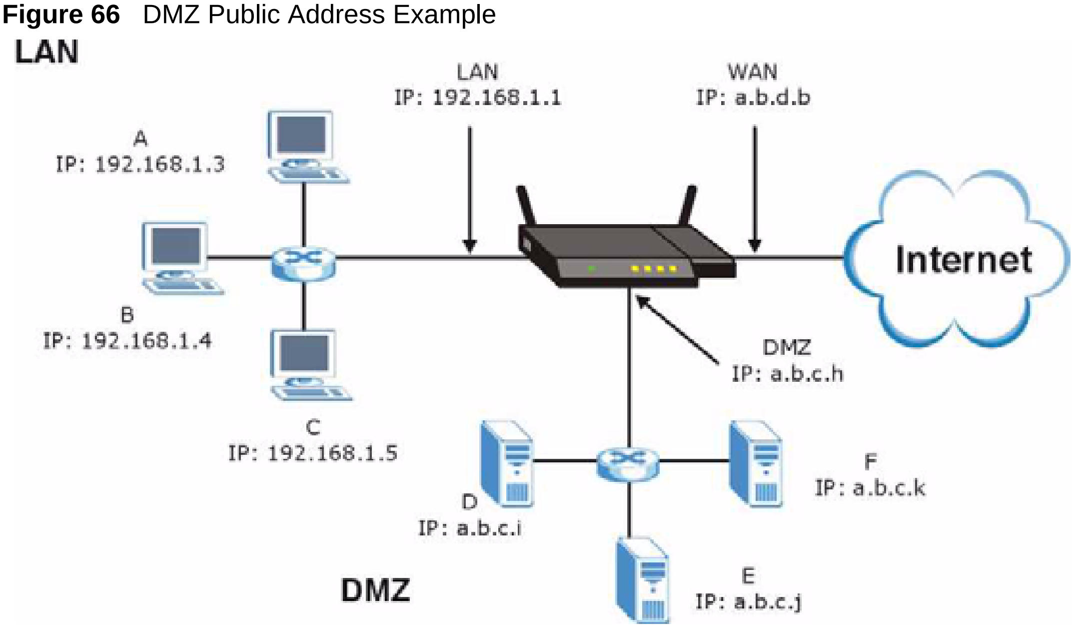
Port Roles

See Section 4.5 on page 86 for more information on port roles.

6.1.3 DMZ Public IP Address Example

The following figure shows a simple network setup with public IP addresses on the WAN and DMZ and private IP addresses on the LAN. Lower case letters represent public IP addresses (like a.b.c.d for example). The LAN port and connected computers (A through C) use private IP addresses that are in one subnet. The DMZ port and connected servers (D through F) use public IP addresses that are in another subnet. The public IP addresses of the DMZ and WAN ports are in separate subnets.

Figure 66 DMZ Public Address Example

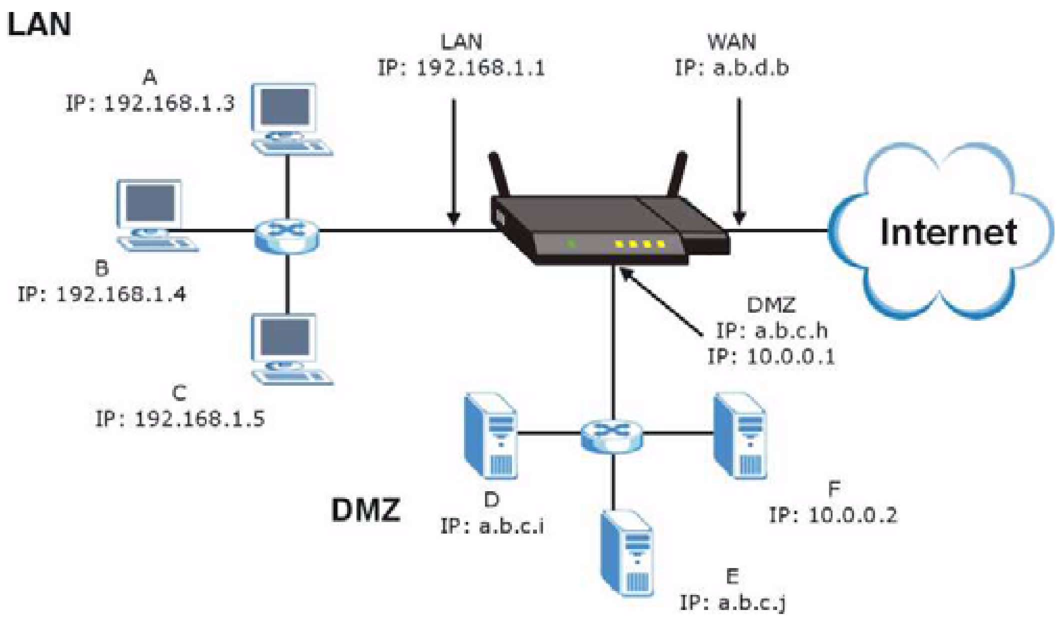


6.1.4 DMZ Private and Public IP Address Example

The following figure shows a network setup with both private and public IP addresses on the DMZ. Lower case letters represent public IP addresses (like a.b.c.d for example). The LAN port and connected computers (A through C) use private IP addresses that are in one subnet. The DMZ port and server F use private IP addresses that are in one subnet. The private IP addresses of the LAN and DMZ are on separate subnets. The DMZ port and connected servers (D and E) use public IP addresses that are in one subnet. The public IP addresses of the DMZ and WAN are on separate subnets.

Configure one subnet (either the public or the private) in the **Network > DMZ** screen (see Figure 68 on page 130) and configure the other subnet in the **Network > DMZ > IP Alias** screen (see Figure 6.4 on page 133) to use this kind of network setup. You also need to configure NAT for the private DMZ IP addresses.

Figure 67 DMZ Private and Public Address Example

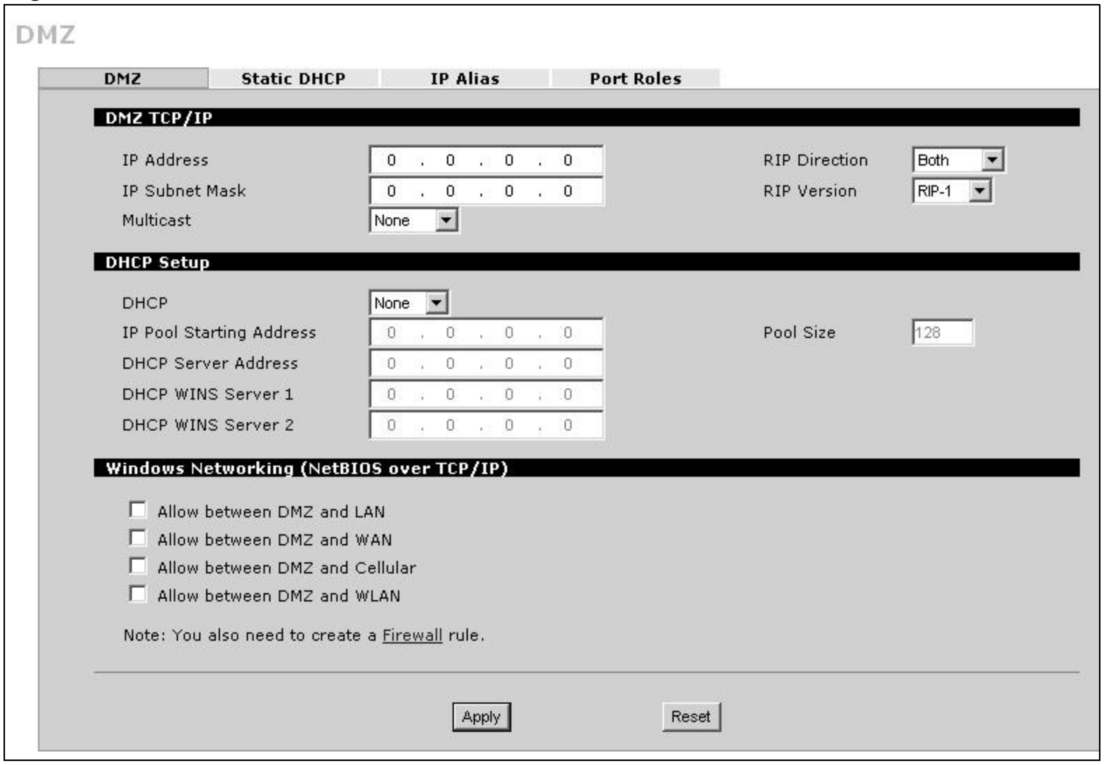


6.2 DMZ Screen

The DMZ and the connected computers can have private or public IP addresses. When the DMZ uses public IP addresses, the WAN and DMZ ports must use public IP addresses that are on separate subnets. See Appendix C on page 605 for information on IP subnetting.

From the main menu, click **NETWORK** > **DMZ** to open the **DMZ** screen. The screen appears as shown next.

Figure 68 NETWORK > DMZ



The following table describes the labels in this screen.

Table 35 NETWORK > DMZ

LABEL	DESCRIPTION
DMZ TCP/IP	
IP Address	Type the IP address of your LAN-Cell's DMZ port in dotted decimal notation. Note: Make sure the IP addresses of the LAN, WAN, WLAN and DMZ are on separate subnets.
IP Subnet Mask	The subnet mask specifies the network number portion of an IP address. Your LAN-Cell 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 LAN-Cell 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 LAN-Cell 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.

Table 35 NETWORK > DMZ (continued)

LABEL	DESCRIPTION
RIP Version	The **RIP Version** field controls the format and the broadcasting method of the RIP packets that the LAN-Cell 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**.
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*.
DHCP Setup	
DHCP	DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients (workstations) to obtain TCP/IP configuration at startup from a server. Unless you are instructed by your ISP, leave this field set to **Server**. When configured as a server, the LAN-Cell provides TCP/IP configuration for the clients. When set as a server, fill in the **IP Pool Starting Address** and **Pool Size** fields. Select **Relay** to have the LAN-Cell forward DHCP requests to another DHCP server. When set to **Relay**, fill in the **DHCP Server Address** field. Select **None** to stop the LAN-Cell from acting as a DHCP server. When you select **None**, you must have another DHCP server on your LAN, or else the computers must be manually configured.
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.
DHCP Server Address	Type the IP address of the DHCP server to which you want the LAN-Cell to relay DHCP requests. Use dotted decimal notation. Alternatively, click the right mouse button to copy and/or paste the IP address.
DHCP WINS Server 1, 2	Type the IP address of the WINS (Windows Internet Naming Service) server that you want to send to the DHCP clients. The WINS server keeps a mapping table of the computer names on your network and the IP addresses that they are currently using.
Windows Networking (NetBIOS over TCP/IP)	
Allow between DMZ and LAN	Select this check box to forward NetBIOS packets from the LAN to the DMZ and from the DMZ to the LAN. If your firewall is enabled with the default policy set to block DMZ to LAN traffic, you also need to configure a DMZ to LAN firewall rule that forwards NetBIOS traffic. Clear this check box to block all NetBIOS packets going from the LAN to the DMZ and from the DMZ to the LAN.
Allow between DMZ and WAN	Select this check box to forward NetBIOS packets from the DMZ to WANand from WAN to the DMZ. Clear this check box to block all NetBIOS packets going from the DMZ to WAN and from WAN to the DMZ.

Table 35 NETWORK > DMZ (continued)

LABEL	DESCRIPTION
Allow between DMZ and Cellular	Select this check box to forward NetBIOS packets from the DMZ to CELL and from CELL to the DMZ. Clear this check box to block all NetBIOS packets going from the DMZ to CELL and from CELL to the DMZ.
Allow between DMZ and WLAN	Select this check box to forward NetBIOS packets from the WLAN to the DMZ and from the DMZ to the WLAN. If your firewall is enabled with the default policy set to block DMZ to WLAN traffic and WLAN to DMZ traffic, you also need to configure DMZ to WLAN and WLAN to DMZ firewall rules that forward NetBIOS traffic. Clear this check box to block all NetBIOS packets going from the WLAN to the DMZ and from the DMZ to the WLAN.
Apply	Click **Apply** to save your changes back to the LAN-Cell.
Reset	Click **Reset** to begin configuring this screen afresh.

6.3 DMZ Static DHCP Screen

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

To change your LAN-Cell’s static DHCP settings on the DMZ, click **NETWORK** > **DMZ** > **Static DHCP**. The screen appears as shown.

Figure 69 NETWORK > DMZ > Static DHCP

The following table describes the labels in this screen.

Table 36 NETWORK > DMZ > Static DHCP

LABEL	DESCRIPTION
#	This is the index number of the Static IP table entry (row).
MAC Address	Type the MAC address of a computer on your DMZ.
IP Address	Type the IP address that you want to assign to the computer on your DMZ. Alternatively, click the right mouse button to copy and/or paste the IP address.
Apply	Click **Apply** to save your changes back to the LAN-Cell.
Reset	Click **Reset** to begin configuring this screen afresh.

6.4 DMZ IP Alias Screen

The LAN-Cell has a single DMZ interface. Even though more than one of ports 1~4 may be in the DMZ port role, they are all still part of a single physical Ethernet interface and all use the same IP address.

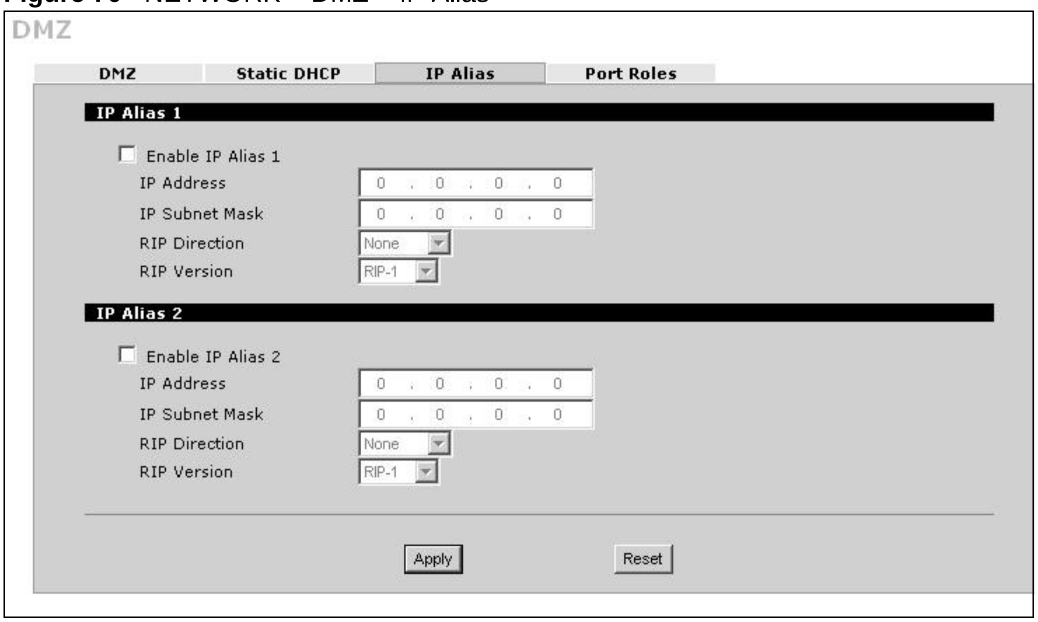
The LAN-Cell supports three logical DMZ interfaces via its single physical DMZ Ethernet interface. The LAN-Cell itself is the gateway for each of the logical DMZ networks.

The IP alias IP addresses can be either private or public regardless of whether the physical DMZ interface is set to use a private or public IP address. Use NAT if you want to make DMZ computers with private IP addresses publicly accessible (see Chapter 13 on page 289 for more information). When you use IP alias, you can have the DMZ use both public and private IP addresses at the same time.

Make sure that the subnets of the logical networks do not overlap.

To change your LAN-Cell’s IP alias settings, click **NETWORK** > **DMZ** > **IP Alias**. The screen appears as shown.

Figure 70 NETWORK > DMZ > IP Alias



The following table describes the labels in this screen.

Table 37 NETWORK > DMZ > IP Alias

LABEL	DESCRIPTION
Enable IP Alias 1, 2	Select the check box to configure another DMZ network for the LAN-Cell.
IP Address	Enter the IP address of your LAN-Cell in dotted decimal notation. Note: Make sure the IP addresses of the LAN, WAN, WLAN and DMZ are on separate subnets.
IP Subnet Mask	Your LAN-Cell 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 LAN-Cell.

Table 37 NETWORK > DMZ > IP Alias (continued)

LABEL	DESCRIPTION
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 LAN-Cell 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	The **RIP Version** field controls the format and the broadcasting method of the RIP packets that the LAN-Cell 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 LAN-Cell.
Reset	Click **Reset** to begin configuring this screen afresh.

6.5 DMZ Port Roles

Use the **Port Roles** screen to set ports as part of the LAN, DMZ and/or WLAN interface.

Ports 1~4 on the LAN-Cell can be part of the LAN, DMZ or WLAN interface.

Do the following if you are configuring from a computer connected to a LAN, DMZ or WLAN port and changing the port's role:

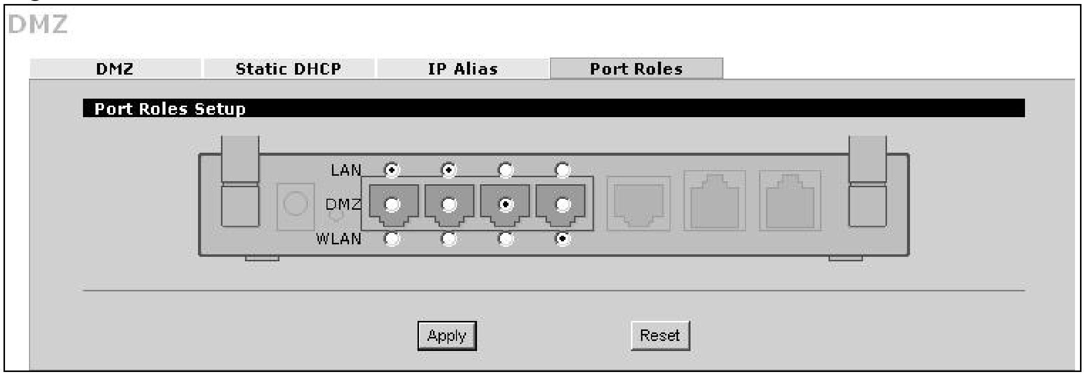
1. A port's IP address varies as its role changes, make sure your computer's IP address is in the same subnet as the LAN-Cell's LAN, DMZ or WLAN IP address.
2. Use the appropriate LAN, DMZ or WLAN IP address to access the LAN-Cell.

To change your LAN-Cell’s port role settings, click **NETWORK** > **DMZ** > **Port Roles**. The screen appears as shown.

The radio buttons correspond to Ethernet ports on the front panel of the LAN-Cell. On the LAN-Cell, ports 1 to 4 are all LAN ports by default.

Your changes are also reflected in the **LAN** and/or **WLAN Port Roles** screens.

Figure 71 NETWORK > DMZ > Port Roles



The following table describes the labels in this screen.

Table 38 NETWORK > DMZ > Port Roles

LABEL	DESCRIPTION
LAN	Select a port's LAN radio button to use the port as part of the LAN. The port will use the LAN-Cell's LAN IP address and MAC address.
DMZ	Select a port's DMZ radio button to use the port as part of the DMZ. The port will use the LAN-Cell's DMZ IP address and MAC address.
WLAN	Select a port's WLAN radio button to use the port as part of the WLAN. The port will use the LAN-Cell's WLAN IP address and MAC address.
Apply	Click **Apply** to save your changes back to the LAN-Cell.
Reset	Click **Reset** to begin configuring this screen afresh.

7

Wireless LAN (WLAN) Screens

7.1 Overview

In addition to the LAN and DMZ logical networks, the LAN-Cell also provides a Wireless LAN (WLAN) logical network that can be used to segregate traffic for policy routing, security or other management purposes.

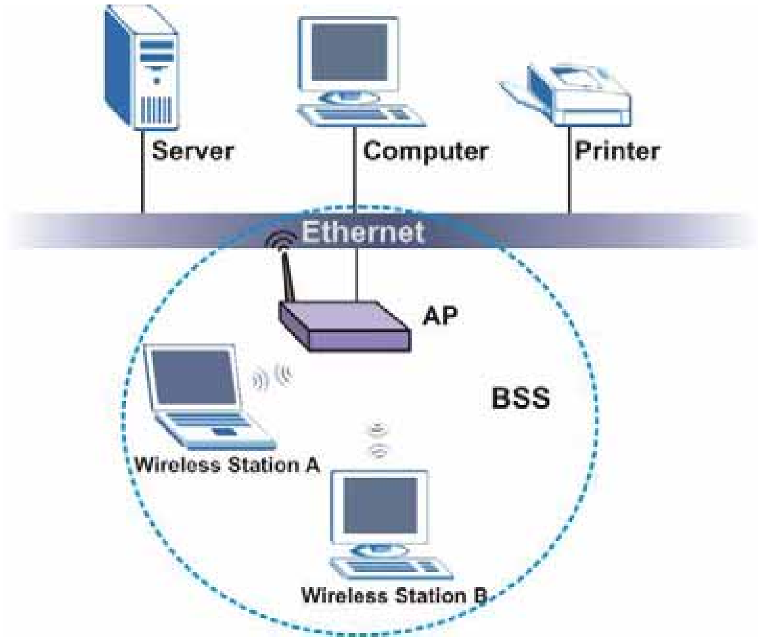
This chapter discusses how to configure the wireless LAN subnet on the LAN-Cell.

A wireless LAN can be as simple as two computers with wireless LAN adapters communicating in a peer-to-peer network or as complex as a number of computers with wireless LAN adapters communicating through access points which bridge network traffic to the wired LAN.

To add a wireless network to the LAN-Cell, you can either activate the LAN-Cell's internal 802.11 a/b/g Wi-Fi Access Point or connect an external Access Point to a LAN-Cell Ethernet port and define that port as a WLAN role.

The following figure provides an example of a wireless network.

Figure 72 Example of a Wireless Network



The wireless network is the part in the blue circle. In this wireless network, devices A and B are called wireless clients. The wireless clients use the access point (AP) to interact with other devices (such as the printer) or with the Internet. Your LAN-Cell is the AP.

Every wireless network must follow these basic guidelines.

- Every wireless client in the same wireless network must use the same SSID.

  The SSID is the name of the wireless network. It stands for Service Set IDentity.
- If two wireless networks overlap, they should use different channels.

  Like radio stations or television channels, each wireless network uses a specific channel, or frequency, to send and receive information.
- Every wireless client in the same wireless network must use security compatible with the AP.

7.1.1 What You Can Do in the WLAN Screens

- Use the **WLAN** screen (Section 7.2 on page 139) to configure TCP/IP, DHCP, IP/MAC binding and NetBIOS settings on the WLAN.
- Use the **Static DHCP** screen (Section 7.3 on page 141) to configure the IP addresses assigned to devices in the LAN by DHCP.
- Use the **IP Alias** screen (Section 7.4 on page 142) to configure IP alias settings on the LAN-Cell's LAN ports.
- Use the **Port Roles** screen (Section 7.5 on page 144) to set a port to be part of the WLAN and connect an Access Point (AP) to the WLAN interface to extend the LAN-Cell's wireless LAN coverage.

7.1.2 What You Need to Know About Wireless LAN

DHCP

Like the LAN, the LAN-Cell can also assign TCP/IP configuration via DHCP to computers connected to the WLAN ports.

See Section 4.3 on page 83 for more information on DHCP.

IP Alias

IP alias allows you to partition a physical network into different logical networks over the same Ethernet interface. See Section 4.4 on page 84 for more information on IP alias.

Port Roles

Use port roles to set ports as part of the LAN, DMZ and/or WLAN interface. See Section 4.5 on page 86 for more information on port roles.

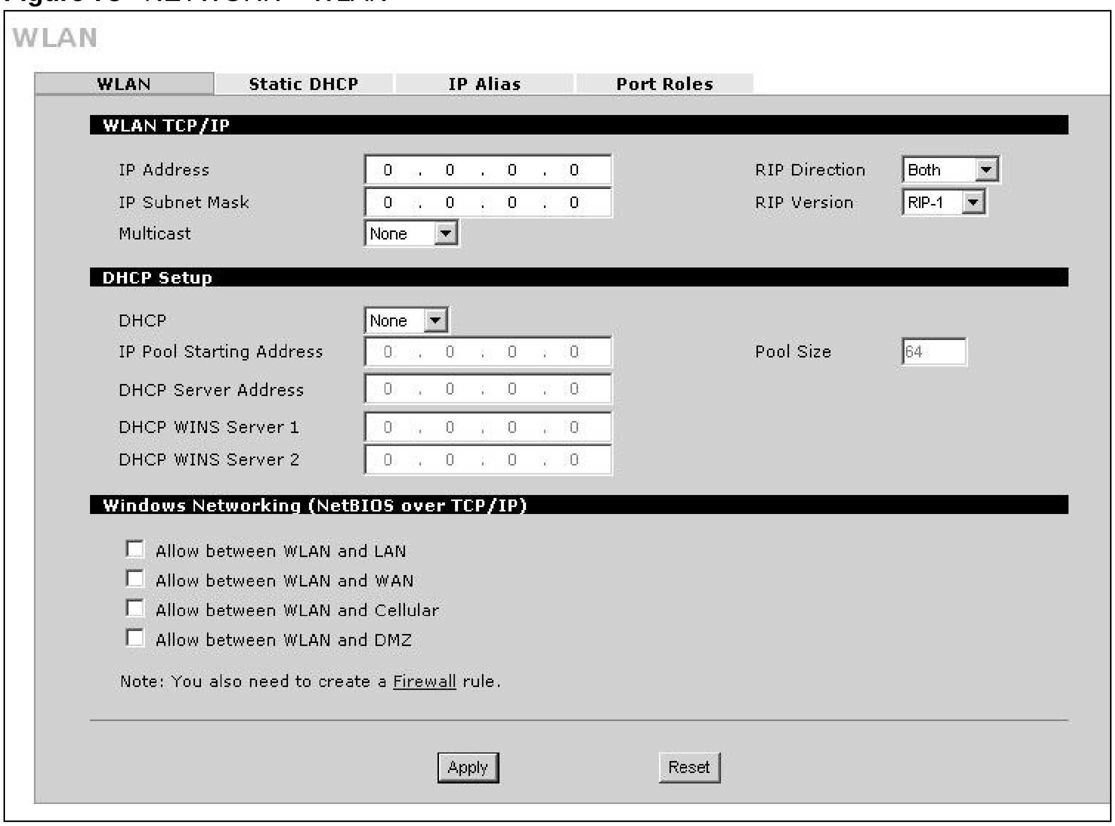
See Appendix E on page 617 for more detailed information on WLANs.

7.2 WLAN Screen

The built-in Wi-Fi access point is used as part of the LAN by default. You can use the **Port Roles** screen (see Figure 77 on page 145) to set a port to be part of the WLAN. Then connect an external access point (AP) to it to extend the LAN-Cell's wireless LAN coverage.

Click **NETWORK** > **WLAN** to open the **WLAN** screen to configure the IP address for LAN-Cell's WLAN interface, other TCP/IP and DHCP settings.

Figure 73 NETWORK > WLAN



The following table describes the labels in this screen.

Table 39 NETWORK > WLAN

LABEL	DESCRIPTION
WLAN TCP/IP	
IP Address	Type the IP address of your LAN-Cell's WLAN interface in dotted decimal notation. Alternatively, click the right mouse button to copy and/or paste the IP address. Note: Make sure the IP addresses of the LAN, WAN, WLAN and DMZ are on separate subnets.

Table 39 NETWORK > WLAN (continued)

LABEL	DESCRIPTION
IP Subnet Mask	The subnet mask specifies the network number portion of an IP address. Your LAN-Cell 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 LAN-Cell.
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 LAN-Cell 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 LAN-Cell 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**.
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*.
DHCP Setup	
DHCP	DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients (workstations) to obtain TCP/IP configuration at startup from a server. Unless you are instructed by your ISP, leave this field set to **Server**. When configured as a server, the LAN-Cell provides TCP/IP configuration for the clients. When set as a server, fill in the **IP Pool Starting Address** and **Pool Size** fields. Select **Relay** to have the LAN-Cell forward DHCP requests to another DHCP server. When set to **Relay**, fill in the **DHCP Server Address** field. Select **None** to stop the LAN-Cell from acting as a DHCP server. When you select **None**, you must have another DHCP server on your WLAN, or else the computers must be manually configured.
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.
DHCP Server Address	Type the IP address of the DHCP server to which you want the LAN-Cell to relay DHCP requests. Use dotted decimal notation. Alternatively, click the right mouse button to copy and/or paste the IP address.
DHCP WINS Server 1, 2	Type the IP address of the WINS (Windows Internet Naming Service) server that you want to send to the DHCP clients. The WINS server keeps a mapping table of the computer names on your network and the IP addresses that they are currently using.
Windows Networking (NetBIOS over TCP/IP)	NetBIOS (Network Basic Input/Output System) are TCP or UDP 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.

Table 39 NETWORK > WLAN (continued)

LABEL	DESCRIPTION
Allow between WLAN and LAN	Select this check box to forward NetBIOS packets from the WLAN to the LAN and from the LAN to the WLAN. Clear this check box to block all NetBIOS packets going from the LAN to the WLAN and from the WLAN to the LAN.
Allow between WLAN and WAN	Select this check box to forward NetBIOS packets from the WLAN to WAN and from WAN to the WLAN. Clear this check box to block all NetBIOS packets going from the WLAN to WAN and from WAN to the WLAN.
Allow between WLAN and Cellular	Select this check box to forward NetBIOS packets from the WLAN to CELL and from CELL to the WLAN. Clear this check box to block all NetBIOS packets going from the WLAN to CELL and from CELL to the WLAN.
Allow between WLAN and DMZ	Select this check box to forward NetBIOS packets from the WLAN to the DMZ and from the DMZ to the WLAN. If your firewall is enabled with the default policy set to block WLAN to DMZ traffic and DMZ to WLAN traffic, you also need to configure WLAN to DMZ and DMZ to WLAN firewall rules that forward NetBIOS traffic. Clear this check box to block all NetBIOS packets going from the WLAN to the DMZ and from the DMZ to the WLAN.
Apply	Click **Apply** to save your changes back to the LAN-Cell.
Reset	Click **Reset** to begin configuring this screen afresh.

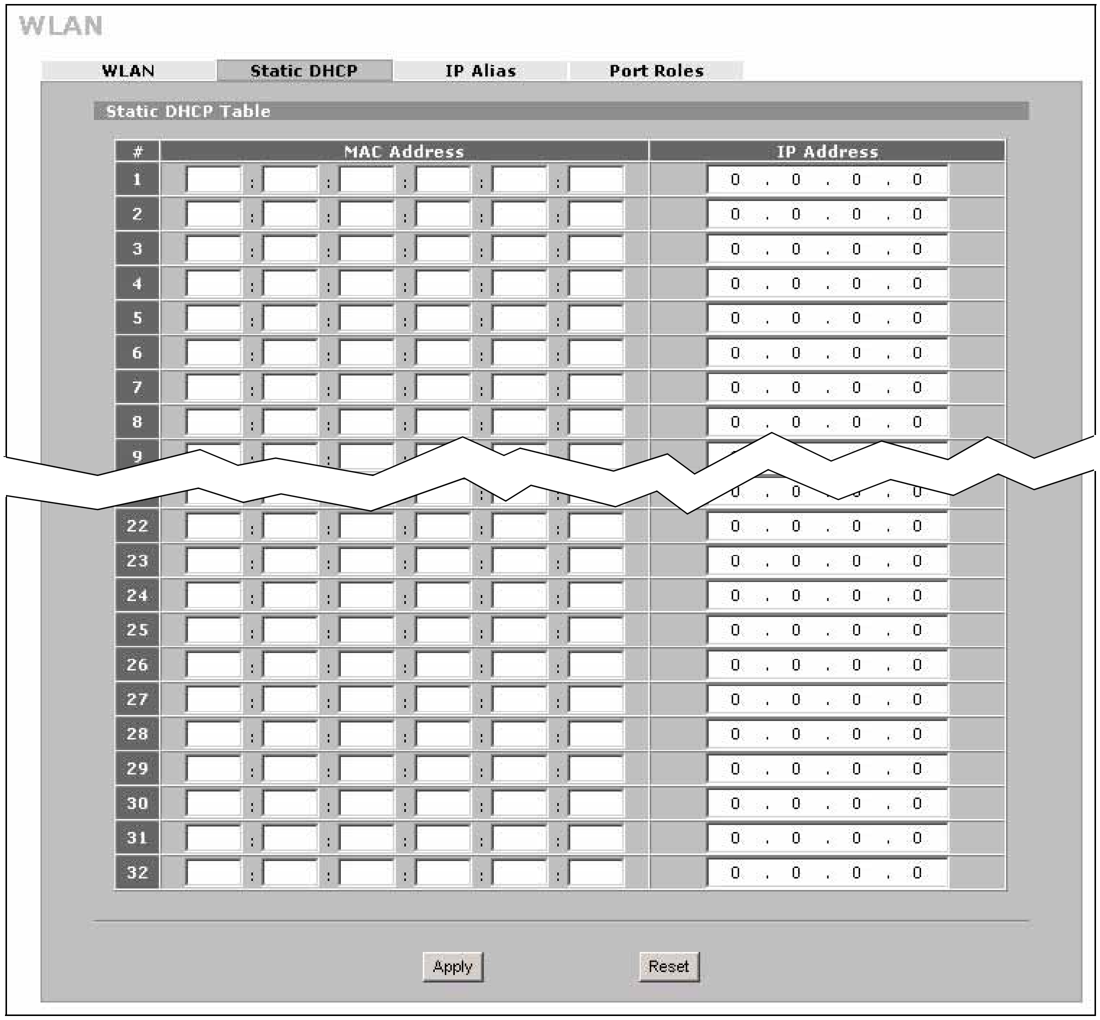
7.3 WLAN Static DHCP Screen

This table allows you to assign IP addresses on the WLAN 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, 00:1B:39:00:00:02.

To change your LAN-Cell’s WLAN static DHCP settings, click **NETWORK** >**WLAN** > **Static DHCP**. The screen appears as shown.

Figure 74 NETWORK > WLAN > Static DHCP



The following table describes the labels in this screen.

Table 40 NETWORK > WLAN > Static DHCP

LABEL	DESCRIPTION
#	This is the index number of the Static IP table entry (row).
MAC Address	Type the MAC address of a computer on your WLAN.
IP Address	Type the IP address that you want to assign to the computer on your WLAN. Alternatively, click the right mouse button to copy and/or paste the IP address.
Apply	Click **Apply** to save your changes back to the LAN-Cell.
Reset	Click **Reset** to begin configuring this screen afresh.

7.4 WLAN IP Alias Screen

IP alias allows you to partition a physical network into different logical networks over the same Ethernet interface.

The LAN-Cell has a single WLAN interface. Even though more than one of ports 1~4 may be in the WLAN port role, they are all still part of a single physical Ethernet interface and all use the same IP address.

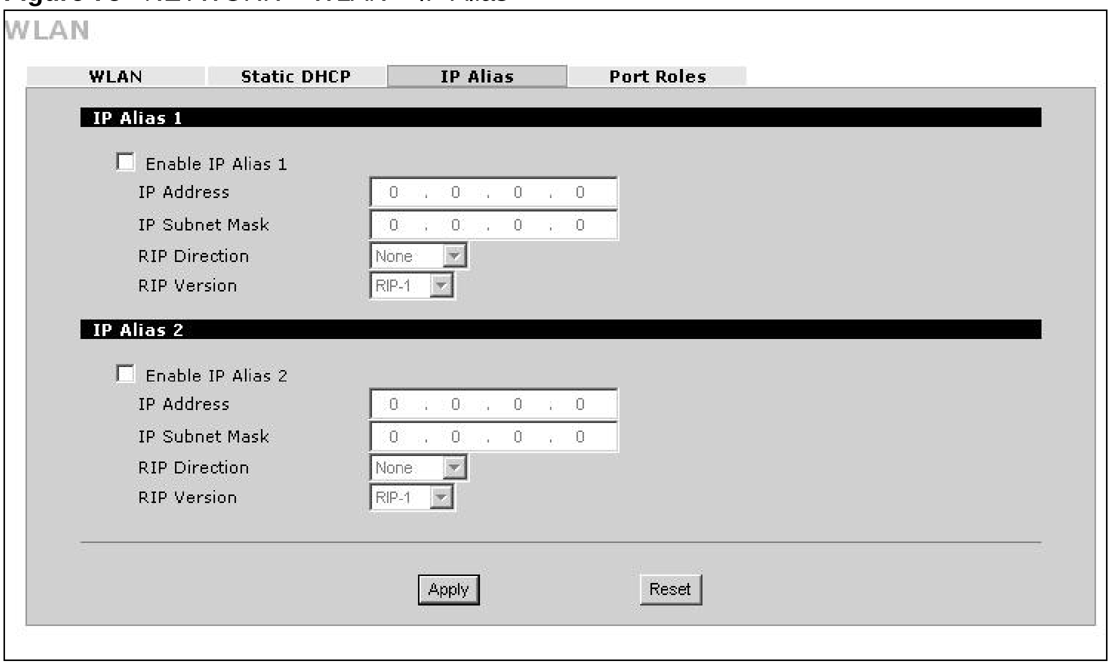
The LAN-Cell supports three logical WLAN interfaces via its single physical WLAN Ethernet interface. The LAN-Cell itself is the gateway for each of the logical WLAN networks.

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

Make sure that the subnets of the logical networks do not overlap.

To change your LAN-Cell’s IP alias settings, click **NETWORK** > **WLAN** > **IP Alias**. The screen appears as shown.

Figure 75 NETWORK > WLAN > IP Alias



The following table describes the labels in this screen.

Table 41 NETWORK > WLAN > IP Alias

LABEL	DESCRIPTION
Enable IP Alias 1, 2	Select the check box to configure another WLAN network for the LAN-Cell.
IP Address	Enter the IP address of your LAN-Cell in dotted decimal notation. Alternatively, click the right mouse button to copy and/or paste the IP address.
IP Subnet Mask	Your LAN-Cell 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 LAN-Cell.

Table 41 NETWORK > WLAN > IP Alias (continued)

LABEL	DESCRIPTION
RIP Direction	RIP (Routing Information Protocol, RFC 1058 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 LAN-Cell 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	The **RIP Version** field controls the format and the broadcasting method of the RIP packets that the LAN-Cell 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 LAN-Cell.
Reset	Click **Reset** to begin configuring this screen afresh.

7.5 WLAN Port Roles Screen

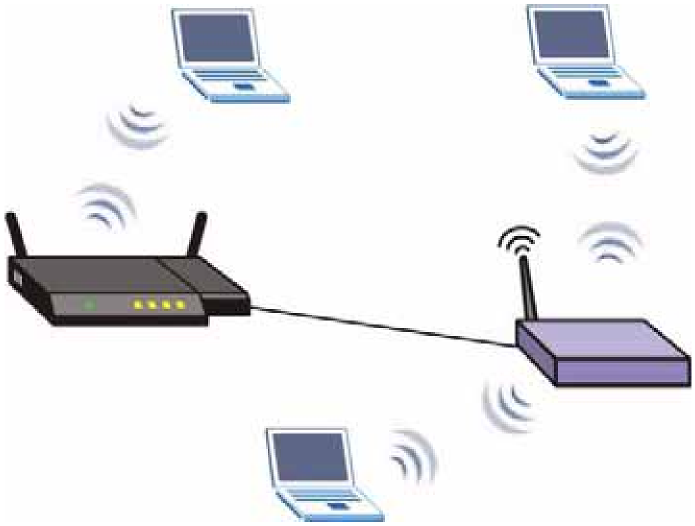
Use the **Port Roles** screen to set ports as part of the LAN, DMZ and/or WLAN interface.

Ports 1~4 on the LAN-Cell can be part of the LAN, DMZ or WLAN interface.

Connect external wireless LAN Access Points (APs) to WLAN interfaces to extend the LAN-Cell's wireless LAN coverage. The WLAN port role allows the LAN-Cell's firewall to treat traffic from connected APs as part of the LAN-Cell's WLAN. You can specify firewall rules for traffic going to or from the WLAN. The WLAN includes the LAN-Cell's own WLAN and the Ethernet ports in the WLAN port role.

The following figure shows the LAN-Cell with the interanl Wi-Fi AP enabled and an external AP connected to an Ethernet port in the WLAN port role.

Figure 76 WLAN Port Role Example



Do the following if you are configuring from a computer connected to a LAN, DMZ or WLAN port and changing the port's role:

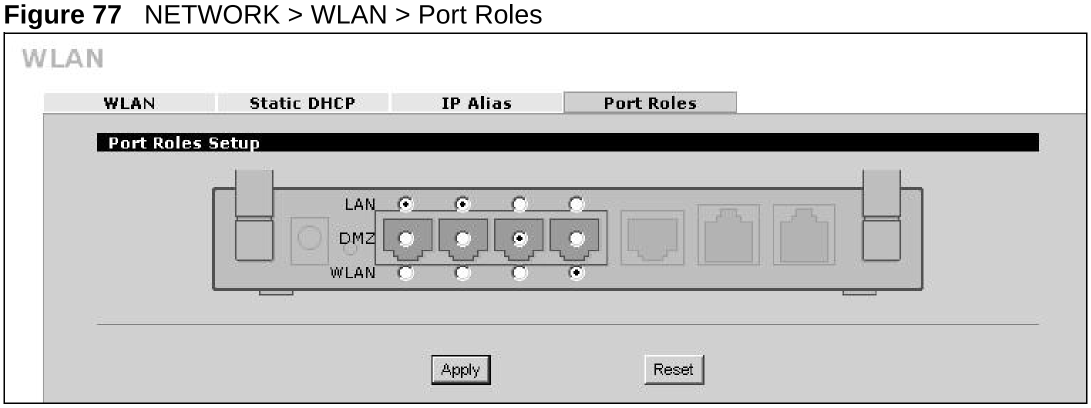
1. A port's IP address varies as its role changes, make sure your computer's IP address is in the same subnet as the LAN-Cell's LAN, DMZ or WLAN IP address.
2. Use the appropriate LAN, DMZ or WLAN IP address to access the LAN-Cell.

To change your LAN-Cell’s port role settings, click **NETWORK** > **WLAN** > **Port Roles**. The screen appears as shown.

The radio buttons correspond to Ethernet ports on the front panel of the LAN-Cell. On the LAN-Cell, ports 1 to 4 are all LAN ports by default.

Your changes are also reflected in the **LAN** and/or **DMZ Port Roles** screen.

Figure 77 NETWORK > WLAN > Port Roles



The following table describes the labels in this screen.

Table 42 NETWORK > WLAN > Port Roles

LABEL	DESCRIPTION
LAN	Select a port's LAN radio button to use the port as part of the LAN. The port will use the LAN IP address.
DMZ	Select a port's DMZ radio button to use the port as part of the DMZ. The port will use the DMZ IP address.
WLAN	Select a port's WLAN radio button to use the port as part of the WLAN. The port will use the WLAN IP address.
Apply	Click **Apply** to save your changes back to the LAN-Cell.
Reset	Click **Reset** to begin configuring this screen afresh.

After you change the LAN/DMZ/WLAN port roles and click **Apply**, please wait for few seconds until the following screen appears. Click **Return** to go back to the **Port Roles** screen.

Figure 78 NETWORK > WLAN > Port Roles: Change Complete

7.6 Wireless Security Overview

The following sections introduce different types of wireless security you can set up in the wireless network.

7.6.1 SSID

Normally, the AP acts like a beacon and regularly broadcasts the SSID in the area. You can hide the SSID instead, in which case the AP does not broadcast the SSID. In addition, you should change the default SSID to something that is difficult to guess.

This type of security is fairly weak, however, because there are ways for unauthorized devices to get the SSID. In addition, unauthorized devices can still see the information that is sent in the wireless network.

7.6.2 MAC Address Filter

Every wireless client has a unique identification number, called a MAC address.[2] A MAC address is usually written using twelve hexadecimal characters[3]; for example, 001B39000002 or 00:1B:39:00:00:02. To get the MAC address for each wireless client, see the appropriate User's Guide or other documentation.

You can use the MAC address filter to tell the AP which wireless clients are allowed or not allowed to use the wireless network. If a wireless client is allowed to use the wireless network, it still has to have the correct settings (SSID, channel, and security). If a wireless client is not allowed to use the wireless network, it does not matter if it has the correct settings.

This type of security does not protect the information that is sent in the wireless network. Furthermore, there are ways for unauthorized devices to get the MAC address of an authorized wireless client. Then, they can use that MAC address to use the wireless network.

7.6.3 User Authentication

You can make every user log in to the wireless network before they can use it. This is called user authentication. However, every wireless client in the wireless network has to support IEEE 802.1x to do this.

For wireless networks, there are two typical places to store the user names and passwords for each user.

- In the AP: this feature is called a local user database or a local database.
- In a RADIUS server: this is a server used in businesses more than in homes.

---

2. Some wireless devices, such as scanners, can detect wireless networks but cannot use wireless networks. These kinds of wireless devices might not have MAC addresses.
3. Hexadecimal characters are 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, and F.

If your AP does not provide a local user database and if you do not have a RADIUS server, you cannot set up user names and passwords for your users.

Unauthorized devices can still see the information that is sent in the wireless network, even if they cannot use the wireless network. Furthermore, there are ways for unauthorized wireless users to get a valid user name and password. Then, they can use that user name and password to use the wireless network.

Local user databases also have an additional limitation that is explained in the next section.

7.6.4 Encryption

Wireless networks can use encryption to protect the information that is sent in the wireless network. Encryption is like a secret code. If you do not know the secret code, you cannot understand the message.

The types of encryption you can choose depend on the type of user authentication. (See Section 7.6.3 on page 147 for information about this.)

Table 43 Types of Encryption for Each Type of Authentication

	No Authentication	RADIUS Server
Weakest	No Security	
	Static WEP	
		802.1x +Static WEP
	WPA-PSK	WPA
Strongest	WPA2-PSK or WPA2-PSK-Mix	WPA2 or WPA2-Mix

For example, if the wireless network has a RADIUS server, you can choose **WPA** or **WPA2**. If users do not log in to the wireless network, you can choose no encryption, **Static WEP**, **WPA-PSK**, or **WPA2-PSK**.

Usually, you should set up the strongest encryption that every wireless client in the wireless network supports. For example, suppose the AP does not have a local user database, and you do not have a RADIUS server. Therefore, there is no user authentication. Suppose the wireless network has two wireless clients. Device A only supports WEP, and device B supports WEP and WPA. Therefore, you should set up **Static WEP** in the wireless network.

Note: It is recommended that wireless clients use **WPA-PSK**, **WPA**, or stronger encryption. IEEE 802.1x and WEP encryption are better than none at all, but it is still possible for unauthorized devices to figure out the original information pretty quickly.

It is not possible to use **WPA-PSK**, **WPA** or stronger encryption with a local user database. In this case, it is better to set up stronger encryption with no authentication than to set up weaker encryption with the local user database.

If some wireless clients support WPA and some support WPA2, you should set up **WPA2-PSK-Mix** or **WPA2-Mix** (depending on the type of wireless network login) in the LAN-Cell.

Many types of encryption use a key to protect the information in the wireless network. The longer the key, the stronger the encryption. Every wireless client in the wireless network must have the same key.

7.6.5 Additional Installation Requirements for Using 802.1x

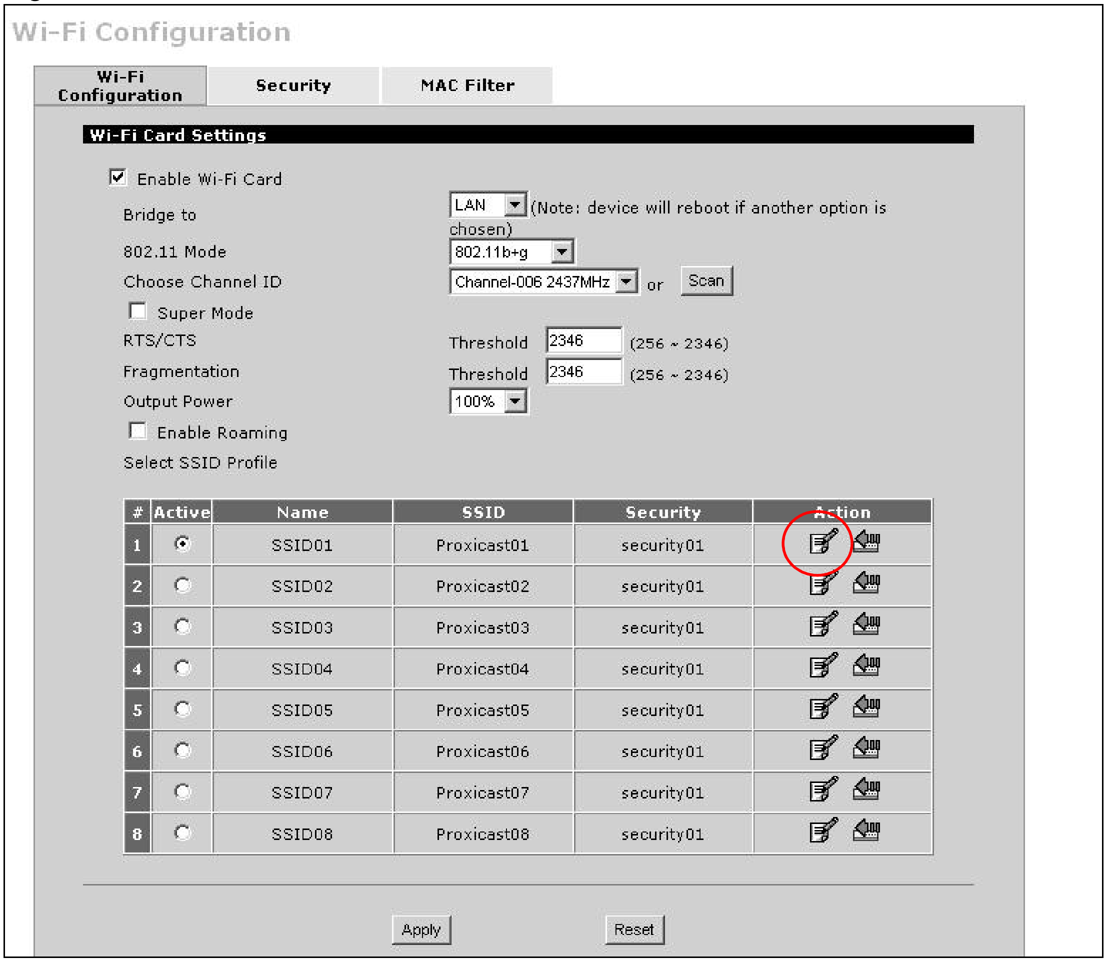
- A computer with an IEEE 802.11a/b/g wireless LAN card.
- A computer equipped with a web browser (with JavaScript enabled) and/or Telnet.
- A wireless station must be running IEEE 802.1x-compliant software. Currently, this is offered in Windows XP.
- An optional network RADIUS server for remote user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

7.7 Internal Wi-Fi Access Point Setup

If you are configuring the LAN-Cell from a computer connected to the wireless LAN and you change the LAN-Cell’s SSID or security 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 LAN-Cell’s new settings.

Click **WIRELESS** > **Wi-Fi** to open the **Wi-Fi Configuraton** screen.

Figure 79 WIRELESS > Wi-Fi



The following table describes the labels in this screen.

Table 44 WIRELESS > Wi-Fi

LABEL	DESCRIPTION
Enable Wi-Fi Card	The internal Wi-Fi access point 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.
Bridge to	Select **LAN** to use the Wi-Fi card as part of the LAN. Select **DMZ** to use the Wi-Fi card as part of the DMZ. Select **WLAN** to use the Wi-Fi card as part of the WLAN. The LAN-Cell restarts after you change the Wi-Fi card setting. Note: If you set the Wi-Fi card to be part of the LAN or DMZ, you can still use wireless access. The firewall will treat the Wi-Fi card as part of the LAN or DMZ respectively.
802.11 Mode	Select **802.11b Only** to allow only IEEE 802.11b compliant WLAN devices to associate with the LAN-Cell. Select **802.11g Only** to allow only IEEE 802.11g compliant WLAN devices to associate with the LAN-Cell. Select **802.11b+g** to allow both IEEE802.11b and IEEE802.11g compliant WLAN devices to associate with the LAN-Cell. The transmission rate of your LAN-Cell might be reduced. Select **802.11a Only** to allow only IEEE 802.11a compliant WLAN devices to associate with the LAN-Cell.
Choose Channel ID	Set the operating frequency/channel depending on your particular region. To manually set the LAN-Cell to use a channel, select a channel from the drop-down list box. To have the LAN-Cell automatically select a channel, click **Scan** instead.
Scan	Click this button to have the LAN-Cell automatically select the wireless channel with the lowest interference.
Super Mode	Select this to improve data throughput on the WLAN by enabling fast frame and packet bursting. At the time of writing, this works only when the wireless client is using an Atheros card.
RTS/CTS Threshold	This is the threshold (number of bytes) for enabling RTS/CTS handshake. Data with a 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. Enter a value between **256** and **2346**. If you select **Super Mode**, this field is grayed out and the LAN-Cell uses 2346 automatically.
Fragmentation Threshold	This is 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 **2346**. If you select **Super Mode**, this field is grayed out and the LAN-Cell uses 2346 automatically.
Output Power	Set the output power of the LAN-Cell in this field. If there is a high density of APs in an area, decrease the output power to reduce interference with other APs. Select one of the following **100%** (full power), **50%**, **25%**, **12.5%** or **min** (minimum). See the product specifications for more information on your LAN-Cell's output power.
Enable Roaming	Roaming allows wireless stations to switch from one access point to another as they move from one coverage area to another. Select this checkbox to enable roaming on the LAN-Cell if you have two or more LAN-Cells on the same subnet. Note: All APs on the same subnet and the wireless clients must have the same SSID to allow roaming.

Table 44 WIRELESS > Wi-Fi (continued)

LABEL	DESCRIPTION
Select SSID Profile	An SSID profile is the set of parameters relating to one of the LAN-Cell's BSSs. The SSID (Service Set IDentifier) identifies the Service Set with which a wireless client is associated. Wireless clients associating with the access point (AP) must have the same SSID. Note: If you are configuring the LAN-Cell from a computer connected to the wireless LAN and you change the LAN-Cell's SSID or security 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 LAN-Cell's new settings.
#	This field displays the index number of each SSID profile.
Active	Choose a profile to apply to your wireless network by selecting its radio button.
Name	This field displays the identification name of each SSID profile on the LAN-Cell.
SSID	This field displays the name of the wireless profile on the network. When a wireless client scans for an AP to associate with, this is the name that is broadcast and seen in the wireless client utility.
Security	This field indicates which security profile is currently associated with each SSID profile. See Section 7.8 on page 153 for more information.
Action	Click the **Edit** icon next to the profile you want to configure and go to the SSID configuration screen. Click the **Reset Default** icon to clear all user-entered configuration information and return the SSID profile to its factory defaults.
Apply	Click **Apply** to save your changes back to the LAN-Cell.
Reset	Click **Reset** to begin configuring this screen afresh.

7.7.1 SSID Profile

Configure wireless network security by configuring and applying an SSID profile. You can configure multiple profiles but you can only apply one to your network.

Use the **Wi-Fi Configuration** screen to see information about the SSID profiles on the LAN-Cell, and use the **Wi-Fi CONFIGURATION** > **Edit** screen to configure the SSID profiles.

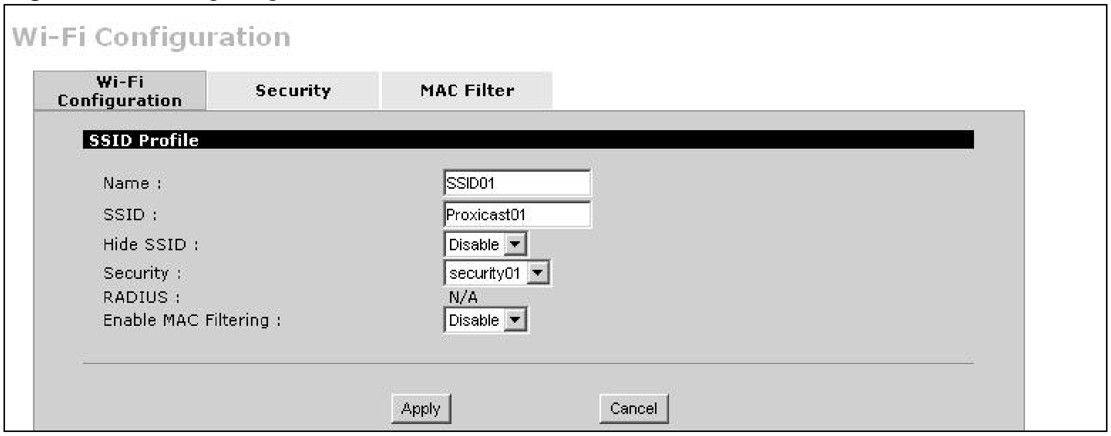
Each SSID profile references the settings configured in the following screens:

- **Wi-Fi CONFIGURATION** > **Security** (one of the security profiles).
- **AUTH SERVER** > **RADIUS** (the RADIUS server settings).
- **Wi-Fi CONFIGURATION** > **MAC Filter** (the MAC filter list, if activated in the SSID profile).

Configure the fields in the above screens to use the settings in an SSID profile.

In the **Wi-Fi CONFIGURATION** screen, click the **Edit** icon next to an SSID profile to display the following screen.

Figure 80 Configuring SSID



The following table describes the labels in this screen.

Table 45 Configuring SSID

LABEL	DESCRIPTION
Name	Enter a name (up to 32 printable 7-bit ASCII characters) identifying this profile.
SSID	When a wireless client scans for an AP to associate with, this is the name that is broadcast and seen in the wireless client utility. Enter a descriptive name (up to 32 printable 7-bit ASCII characters) for the wireless LAN.
Hide SSID	Select **Disable** if you want the LAN-Cell to broadcast this SSID (a wireless client scanning for an AP will find this SSID). Alternatively, select **Enable** to have the LAN-Cell hide this SSID (a wireless client scanning for an AP will not find this SSID).
Security	Select a security profile to use with this SSID profile. See Section 7.8 on page 153 for more information.
RADIUS	This displays **N/A** if the security profile you selected does not use RADIUS authentication. See Section 7.8 on page 153 for more information. This displays **Radius Configuration** if you select a security profile that uses RADIUS authentication. Click **Radius Configuration** to go to the **RADIUS** screen where you can view and/or change the RADIUS settings. See Section 12.3 on page 285 for more information.
Enable MAC Filtering	Select **Enable** from the drop down list box to activate MAC address filtering.
Apply	Click **Apply** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving.

7.8 Configuring Wireless Security

Click **WIRELESS** > **Wi-Fi** > **Security** to open the **Security** screen. Use this screen to create security profiles. A security profile is a group of configuration settings which can be assigned to an SSID profile in the **Wi-Fi Configuration** screen.

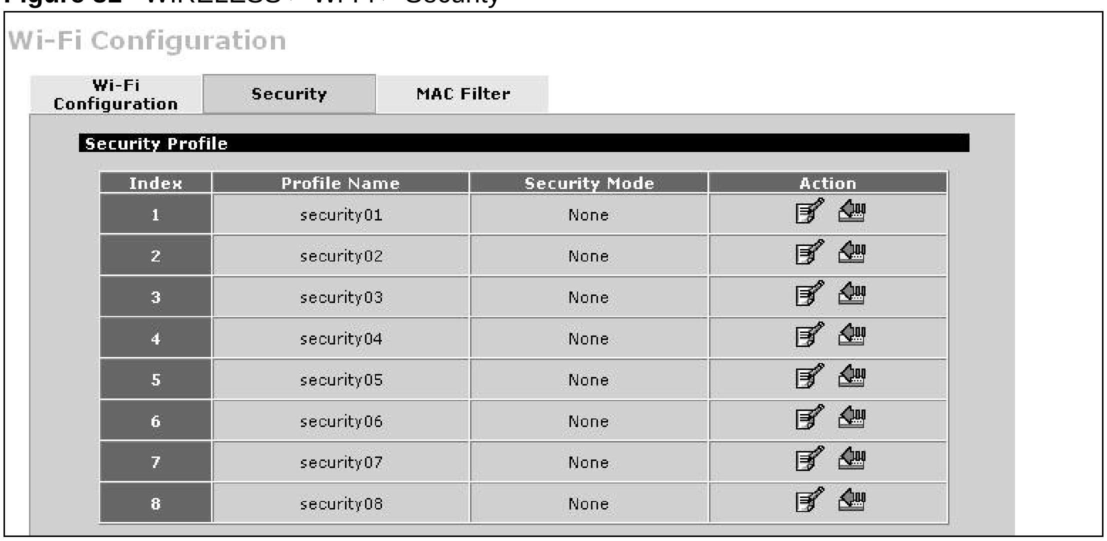
The screen changes when you configure a security profile and varies according to the security modes you select.

The following table describes the security modes you can configure.

Table 46 Security Modes

SECURITY MODE	DESCRIPTION
None	Select this to have no data encryption.
WEP	Select this to use WEP encryption.
802.1x-Only	Select this to use 802.1x authentication with no data encryption.
802.1x-Static64	Select this to use 802.1x authentication with a static 64bit WEP key and an authentication server.
802.1x-Static128	Select this to use 802.1x authentication with a static 128bit WEP key and an authentication server.
WPA	Select this to use WPA.
WPA-PSK	Select this to use WPA with a pre-shared key.
WPA2	Select this to use WPA2.
WPA2-MIX	Select this to use either WPA2 or WPA depending on which security mode the wireless client uses.
WPA2-PSK	Select this to use WPA2 with a pre-shared key.
WPA2-PSK-MIX	Select this to use either WPA-PSK or WPA2-PSK depending on which security mode the wireless client uses.

Figure 81 WIRELESS > Wi-Fi > Security



The following table describes the labels in this screen.

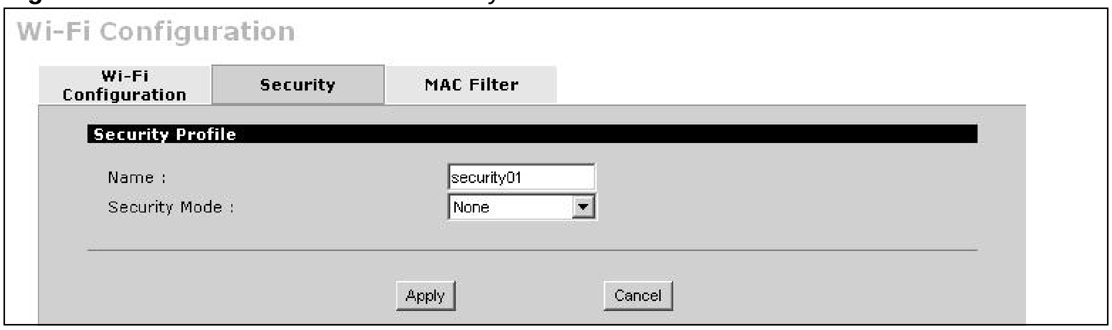
Table 47 WIRELESS > Wi-Fi > Security

LABEL	DESCRIPTION
Security Profile	
Index	This is the index number of the security profile.
Profile Name	This field displays a name given to a security profile in the **Security** configuration screen.
Security Mode	This field displays the security mode this security profile uses.
Action	Click the **Edit** icon to configure security settings for that profile. Click the **Reset Default** icon to clear all user-entered configuration information and return the security profile to its factory defaults.

7.8.1 No Security

If you do not enable any wireless security on your LAN-Cell, your network is accessible to any wireless networking device within range.

Figure 82 WIRELESS > Wi-Fi > Security: None



The following table describes the wireless LAN security labels in this screen.

Table 48 WIRELESS > Wi-Fi > Security: None

LABEL	DESCRIPTION
Name	Type a name (up to 32 printable 7-bit ASCII characters) to identify this security profile.
Security Mode	Select **None** to allow wireless clients to communicate with the access points without any data encryption.
Apply	Click **Apply** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving.

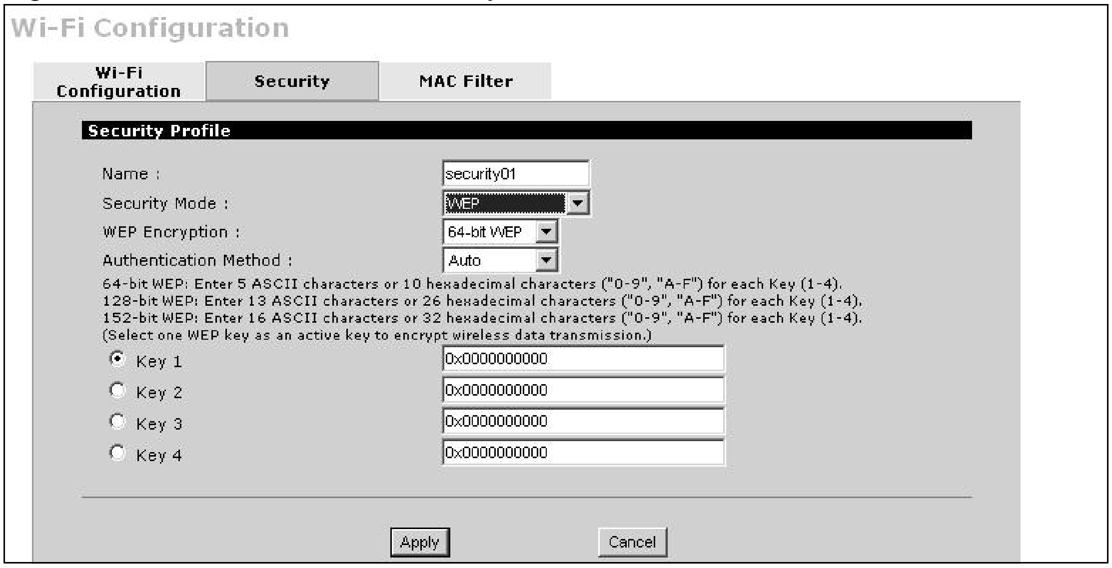
7.8.2 Static WEP

Static 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.

Your LAN-Cell allows you to configure up to four 64-bit, 128-bit or 152-bit WEP keys, but only one key can be used at any one time.

In order to configure and enable WEP encryption, click **WIRELESS** > **Wi-Fi** > **Security** > **Edit**.

Figure 83 WIRELESS > Wi-Fi > Security: WEP



The following table describes the labels in this screen.

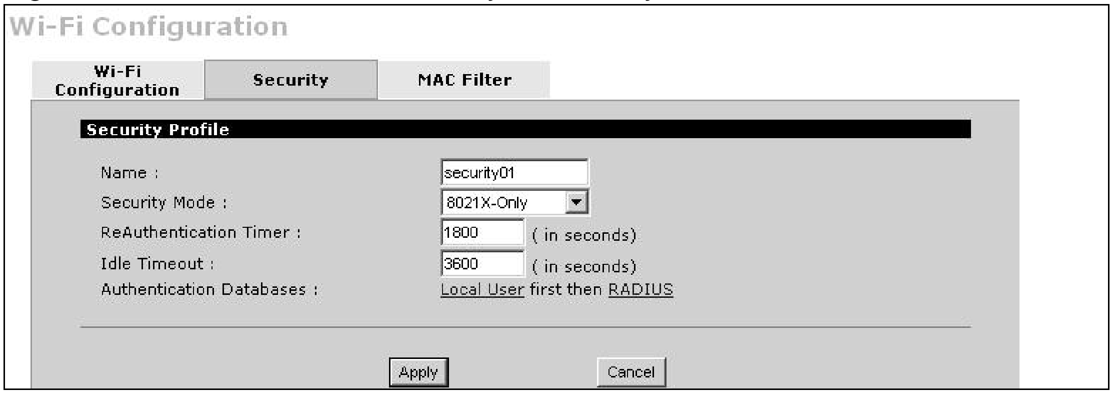
Table 49 WIRELESS > Wi-Fi > Security: WEP

LABEL	DESCRIPTION
Name	Type a name to identify this security profile.
Security Mode	Select **WEP** from the drop-down list.
WEP Encryption	WEP (Wired Equivalent Privacy) provides data encryption to prevent unauthorized wireless stations from accessing data transmitted over the wireless network. Select **64-bit WEP**, **128-bit WEP** or **152-bit WEP** to enable data encryption.
Authentication Method	Select **Shared-Key** to have the LAN-Cell use the default WEP key to authenticate the wireless client to the LAN-Cell. Select **Auto** to have the LAN-Cell switch between the shared-key and open system (the wireless clients and AP do not share a secret key for authentication) modes automatically. The default setting is **Auto**.
Key 1 to Key 4	The WEP keys are used to encrypt data. Both the LAN-Cell and the wireless clients must use the same WEP key for data transmission. If you chose **64-bit WEP** in the **WEP Encryption** field, then enter any 5 ASCII characters 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 ASCII characters or 26 hexadecimal characters ("0-9", "A-F") preceded by 0x for each key. If you chose **152-bit WEP** in the **WEP Encryption** field, then enter 16 ASCII characters or 32 hexadecimal characters ("0-9", "A-F") preceded by 0x for each key. You can configure up to four keys, but only one key can be activated at any one time. The default key is key 1.
Apply	Click **Apply** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving.

7.8.3 IEEE 802.1x Only

Click the **WIRELESS** > **Wi-Fi** > **Security** > **Edit**. Select **8021X-Only** from the **Security Mode** list.

Figure 84 WIRELESS > Wi-Fi > Security: 802.1x Only



The following table describes the labels in this screen.

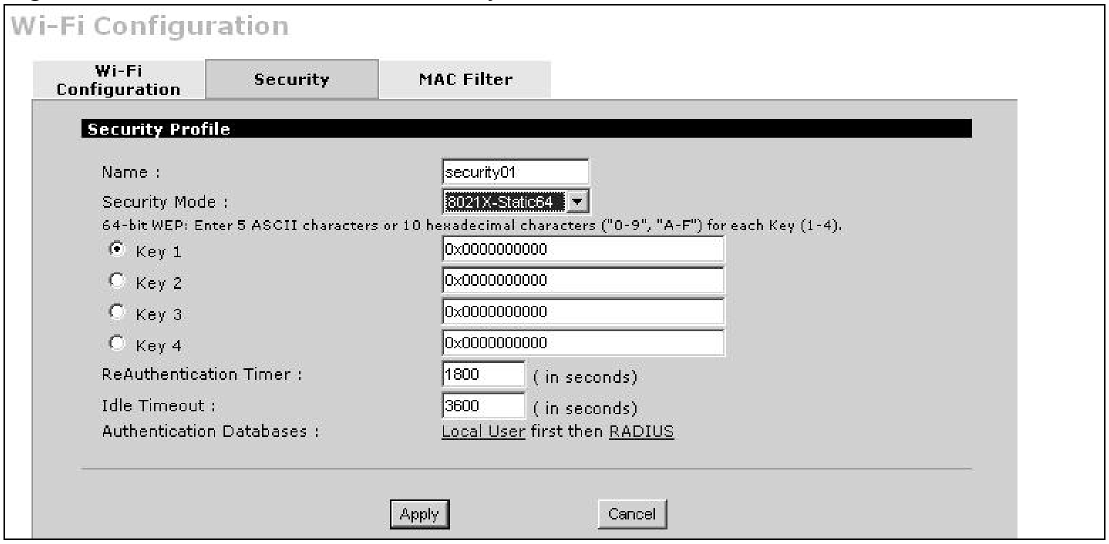
Table 50 WIRELESS > Wi-Fi > Security: 802.1x Only

LABEL	DESCRIPTION
Name	Type a name to identify this security profile.
Security Mode	Select **8021X-Only** from the drop-down list.
ReAuthentication Timer	Specify how often wireless clients have to resend user names and passwords in order to stay connected. Enter a time interval between 600 and 65535 seconds. If wireless client authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.
Idle Timeout	The LAN-Cell automatically disconnects a wireless client from the wireless network after a period of inactivity. The wireless client needs to send the username and password again before it can use the wireless network again. Some wireless clients may prompt users for a username and password; other clients may use saved login credentials. In either case, there is usually a short delay while the wireless client logs in to the wireless network again. This value is usually smaller when the wireless network is keeping track of how much time each wireless client is connected to the wireless network (for example, using an authentication server). If the wireless network is not keeping track of this information, you can usually set this value higher to reduce the number of delays caused by logging in again. Enter a time interval between 600 and 65535 seconds.
Authentication Databases	Click **Local User** to go to the **Local User Database** screen where you can view and/or edit the list of users and passwords. Click **RADIUS** to go to the **RADIUS** screen where you can configure the LAN-Cell to check an external RADIUS server.
Apply	Click **Apply** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving.

7.8.4 IEEE 802.1x + Static WEP

Click the **WIRELESS** > **Wi-Fi** > **Security** > **Edit**. Select **8021X-Static 64** or **8021X-Static128** in the **Security Mode** field to display the following screen.

Figure 85 WIRELESS > Wi-Fi > Security: 802.1x + Static WEP



The following table describes the labels in this screen.

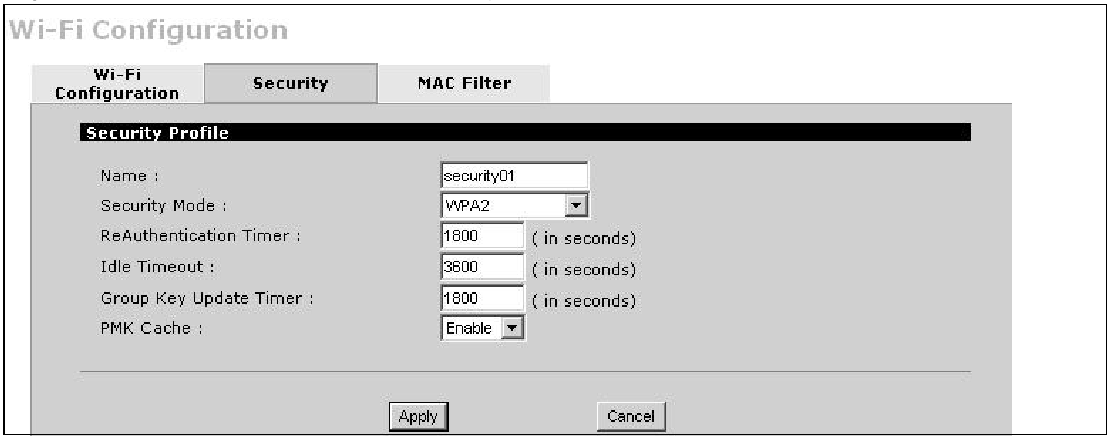
Table 51 WIRELESS > Wi-Fi > Security: 802.1x + Static WEP

LABEL	DESCRIPTION
Name	Type a name to identify this security profile.
Security Mode	Select **8021X-Static64** or **8021X-Static128** from the drop-down list.
Key 1 to Key 4	If you chose **8021X-Static64** in the **Security Mode** 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 **8021X-Static128** in the **Security Mode** 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 clients.
ReAuthentication Timer	Specify how often wireless clients have to resend user names and passwords in order to stay connected. Enter a time interval between 600 and 65535 seconds. If wireless client authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.
Idle Timeout	The LAN-Cell automatically disconnects a wireless client from the wireless network after a period of inactivity. The wireless client needs to send the username and password again before it can use the wireless network again. Some wireless clients may prompt users for a username and password; other clients may use saved login credentials. In either case, there is usually a short delay while the wireless client logs in to the wireless network again. This value is usually smaller when the wireless network is keeping track of how much time each wireless client is connected to the wireless network (for example, using an authentication server). If the wireless network is not keeping track of this information, you can usually set this value higher to reduce the number of delays caused by logging in again. Enter a time interval between 600 and 65535 seconds.
Authentication Databases	Click **Local User** to go to the **Local User Database** screen where you can view and/or edit the list of users and passwords. Click **RADIUS** to go to the **RADIUS** screen where you can configure the LAN-Cell to check an external RADIUS server.
Apply	Click **Apply** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving.

7.8.5 WPA, WPA2, WPA2-MIX

Click **WIRELESS** > **Wi-Fi** > **Security** > **Edit**. Select **WPA**, **WPA2** or **WPA2-MIX** from the **Security Mode** list.

Figure 86 WIRELESS > Wi-Fi > Security: WPA, WPA2 or WPA2-MIX



The following table describes the labels in this screen.

Table 52 WIRELESS > Wi-Fi > Security: WPA, WPA2 or WPA2-MIX

LABEL	DESCRIPTION
Name	Type a name to identify this security profile.
Security Mode	Select **WPA**, **WPA2** or **WPA2-MIX** from the drop-down list.
ReAuthentication Timer	Specify how often wireless clients have to resend user names and passwords in order to stay connected. Enter a time interval between 600 and 65535 seconds. If wireless client authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.
Idle Timeout	The LAN-Cell automatically disconnects a wireless client from the wireless network after a period of inactivity. The wireless client needs to send the username and password again before it can use the wireless network again. Some wireless clients may prompt users for a username and password; other clients may use saved login credentials. In either case, there is usually a short delay while the wireless client logs in to the wireless network again. This value is usually smaller when the wireless network is keeping track of how much time each wireless client is connected to the wireless network (for example, using an authentication server). If the wireless network is not keeping track of this information, you can usually set this value higher to reduce the number of delays caused by logging in again. Enter a time interval between 600 and 65535 seconds.
Group Key Update Timer	The **Group Key Update Timer** is the rate at which the AP sends a new group key out to all clients. The re-keying process is the WPA equivalent of automatically changing the WEP key for an AP and all stations in a WLAN on a periodic basis. Setting of the **Group Key Update Timer** is also supported in **WPA(2)-PSK** mode.
PMK Cache	This field is available only when you select **WPA2** or **WPA2-MIX**. When a wireless client moves from one AP's coverage area to another, it performs an authentication procedure (exchanging security information) with the new AP. Instead of re-authenticating a client each time it returns to the AP's coverage area, which can cause delays to time-sensitive applications, the AP and the client can store (or "cache") and use information about their previous authentication. Select **Enable** to allow PMK (Pairwise Master Key) caching, or **Disable** to switch this feature off.

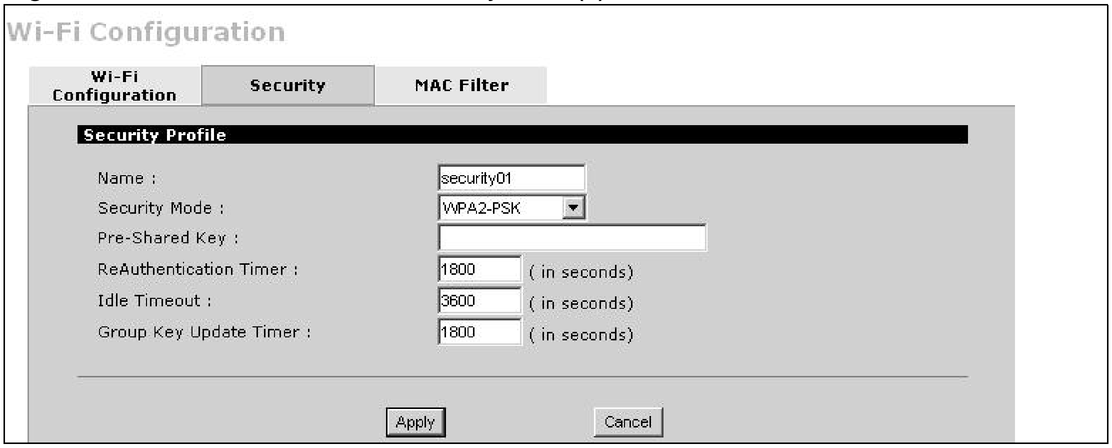
Table 52 WIRELESS > Wi-Fi > Security: WPA, WPA2 or WPA2-MIX (continued)

LABEL	DESCRIPTION
Apply	Click **Apply** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving.

7.8.6 WPA-PSK, WPA2-PSK, WPA2-PSK-MIX

Click **WIRELESS** > **Wi-Fi** > **Security** > **Edit**. Select **WPA-PSK**, **WPA2-PSK** or **WPA2-PSK-MIX** from the **Security Mode** list.

Figure 87 WIRELESS > Wi-Fi > Security: WPA(2)-PSK



The following table describes the labels in this screen.

Table 53 WIRELESS > Wi-Fi > Security: WPA(2)-PSK

LABEL	DESCRIPTION
Name	Type a name to identify this security profile.
Security Mode	Select **WPA-PSK**, **WPA2-PSK** or **WPA2-PSK-MIX** from the drop-down list.
Pre-Shared Key	The encryption mechanisms used for **WPA(2)** and **WPA(2)-PSK** are the same. The only difference between the two is that **WPA(2)-PSK** uses a simple common password, instead of user-specific credentials. Type a pre-shared key from 8 to 63 case-sensitive ASCII characters (including spaces and symbols).
ReAuthentication Timer	Specify how often wireless clients have to resend user names and passwords in order to stay connected. Enter a time interval between 600 and 65535 seconds. If wireless client authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.
Idle Timeout	The LAN-Cell automatically disconnects a wireless client from the wireless network after a period of inactivity. The wireless client needs to send the username and password again before it can use the wireless network again. Some wireless clients may prompt users for a username and password; other clients may use saved login credentials. In either case, there is usually a short delay while the wireless client logs in to the wireless network again. This value is usually smaller when the wireless network is keeping track of how much time each wireless client is connected to the wireless network (for example, using an authentication server). If the wireless network is not keeping track of this information, you can usually set this value higher to reduce the number of delays caused by logging in again. Enter a time interval between 600 and 65535 seconds.

Table 53 WIRELESS > Wi-Fi > Security: WPA(2)-PSK (continued)

LABEL	DESCRIPTION
Group Key Update Timer	The **Group Key Update Timer** is the rate at which the AP sends a new group key out to all clients. The re-keying process is the WPA equivalent of automatically changing the WEP key for an AP and all stations in a WLAN on a periodic basis. Setting of the **Group Key Update Timer** is also supported in **WPA(2)-PSK** mode.
Apply	Click **Apply** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving.

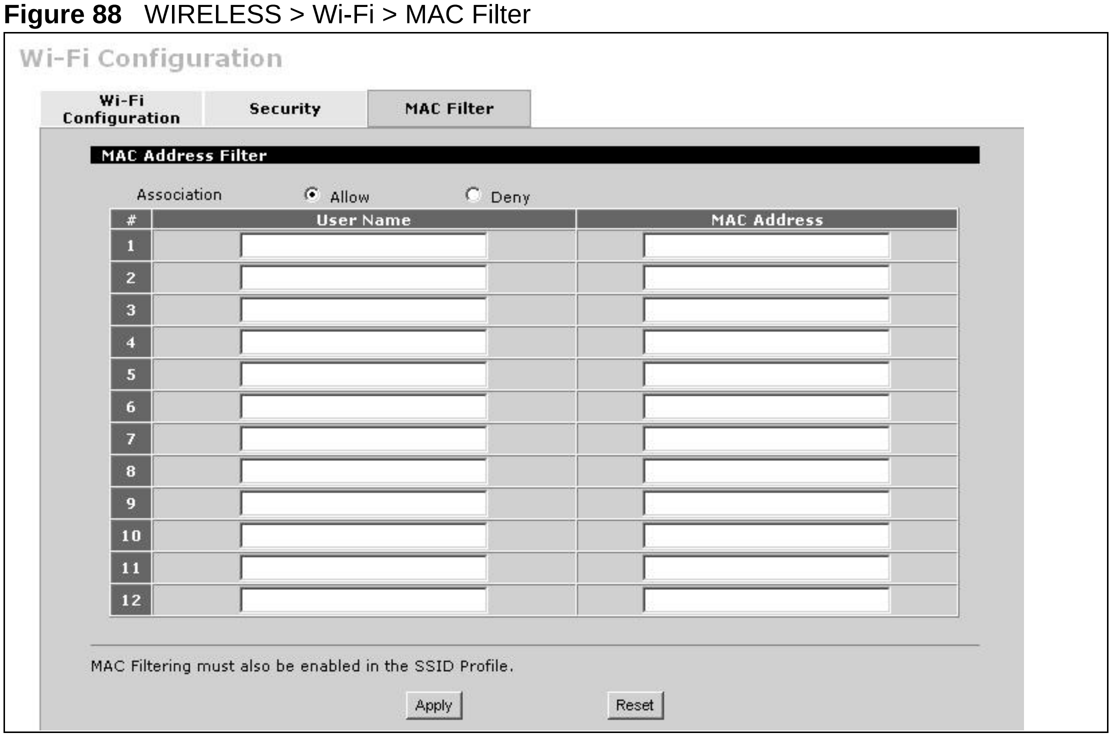
7.9 MAC Filter

The MAC filter screen allows you to configure the LAN-Cell to give exclusive access to specific devices (**Allow**) or exclude specific devices from accessing the LAN-Cell (**Deny**). 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, 00:1B:39:00:00:02. You need to know the MAC addresses of the devices to configure this screen.

To change your LAN-Cell's MAC filter settings, click the **WIRELESS** > **Wi-Fi** > **MAC Filter**. The screen appears as shown.

To activate MAC filtering on a profile, select **Enable** from the **Enable MAC Filtering** drop-down list box in the **Wi-Fi > Edit** screen and click **Apply**.

Figure 88 WIRELESS > Wi-Fi > MAC Filter



The following table describes the labels in this menu.

Table 54 WIRELESS > Wi-Fi > MAC Filter

LABEL	DESCRIPTION
Association	Define the filter action for the list of MAC addresses in the MAC address filter table. Select **Deny** to block access to the router, MAC addresses not listed will be allowed to access the router. Select **Allow** to permit access to the router, MAC addresses not listed will be denied access to the router.
#	This is the index number of the MAC address.
User Name	Enter a descriptive name for the MAC address.
MAC Address	Enter the MAC addresses (in XX:XX:XX:XX:XX:XX format) of the wireless stations that are allowed or denied access to the LAN-Cell in these address fields.
Apply	Click **Apply** to save your changes back to the LAN-Cell.
Reset	Click **Reset** to begin configuring this screen afresh.

7.10 Country Codes

The radio channel frequencies allocated for 802.11 wireless devices differ slightly in various countries. The LAN-Cell's internal 802.11 access point's default settings utilize channels which are appropriate for North America. If you will be deploying the LAN-Cell outside of North America, you must change the LAN-Cell's Country Code in order to modify the 802.11 access point's channel frequencies for your local region.

Failure to use the correct Country Code may cause unintended interference or prevent other 802.11 equipment from connecting to the LAN-Cell and may violate local communication regulations.

To change the LAN-Cell's Country Code:

1. Refer to Appendix E on page 631 to find the code for your Country/Region.
2. Using either the Console Port or a Telnet/SSH session, log into the System Management Terminal (SMT). Refer to Chapter 23 Introducing the SMT.
3. Select Menu 24 (System Maintenance), then Menu 8 (Command Interpreter Mode).
4. At the command line prompt, enter the command: `sys countrycode NNN` where NNN is the 3 digit country code value from Table 257 on page 631.
5. Press `[ENTER]` to save the new country code value.
6. Type `sys countrycode [ENTER]` to confirm the new country code value.
7. Return to the **Wi-Fi Configuration** screen and select the appropriate 802.11 channel.

If you reset the LAN-Cell to its Factory Default settings, you must reset the Country Code using the procedure above.

8

Wi-Fi Screens

8.1 Overview

In these screens you can configure wireless settings for the LAN-Cell's internal Wi-Fi 802.11 a/b/g wireless access point.

8.1.1 What You Can Do in the Wi-Fi Screens

- Use the **Wi-Fi Configuration** screen (Section 8.2 on page 166) to configure wireless network settings such as SSID for the LAN-Cell.
- Use the **Security** screen (Section 8.3 on page 169) to configure wireless security settings for the LAN-Cell.
- Use the **MAC Filter** screen (Section 8.5 on page 178) to set the LAN-Cell to allow or disallow access to devices on your wireless network based on their MAC address.

8.1.2 What You Need to Know About Wireless LAN

Wireless Security

The following sections introduce different types of wireless security you can set up in the wireless network.

SSID

Normally, the AP acts like a beacon and regularly broadcasts the SSID in the area. You can hide the SSID instead, in which case the AP does not broadcast the SSID. In addition, you should change the default SSID to something that is difficult to guess.

This type of security is fairly weak, however, because there are ways for unauthorized devices to get the SSID. In addition, unauthorized devices can still see the information that is sent in the wireless network.

MAC Address Filter

Every wireless client has a unique identification number, called a MAC address.[4] A MAC address is usually written using twelve hexadecimal characters[5]; for example, 001B39000002 or 00:1B:39:00:00:02. To get the MAC address for each wireless client, see the appropriate User's Guide or other documentation.

You can use the MAC address filter to tell the AP which wireless clients are allowed or not allowed to use the wireless network. If a wireless client is allowed to use the wireless network, it still has to have the correct settings (SSID, channel, and security). If a wireless client is not allowed to use the wireless network, it does not matter if it has the correct settings.

This type of security does not protect the information that is sent in the wireless network. Furthermore, there are ways for unauthorized devices to get the MAC address of an authorized wireless client. Then, they can use that MAC address to use the wireless network.

User Authentication

You can make every user log in to the wireless network before they can use it. This is called user authentication. However, every wireless client in the wireless network has to support IEEE 802.1x to do this.

For wireless networks, there are two typical places to store the user names and passwords for each user.

- In the AP: this feature is called a local user database or a local database.
- In a RADIUS server: this is a server used in businesses more than in homes.

If your AP does not provide a local user database and if you do not have a RADIUS server, you cannot set up user names and passwords for your users.

Unauthorized devices can still see the information that is sent in the wireless network, even if they cannot use the wireless network. Furthermore, there are ways for unauthorized wireless users to get a valid user name and password. Then, they can use that user name and password to use the wireless network.

Local user databases also have an additional limitation that is explained in the next section.

Encryption

Wireless networks can use encryption to protect the information that is sent in the wireless network. Encryption is like a secret code. If you do not know the secret code, you cannot understand the message.

4. Some wireless devices, such as scanners, can detect wireless networks but cannot use wireless networks. These kinds of wireless devices might not have MAC addresses.
5. Hexadecimal characters are 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, and F.

The types of encryption you can choose depend on the type of user authentication. (See Section on page 164 for information about this.)

Table 55 Types of Encryption for Each Type of Authentication

	No Authentication	RADIUS Server
Weakest	No Security	
	Static WEP	
		802.1x +Static WEP
	WPA-PSK	WPA
Strongest	WPA2-PSK or WPA2-PSK-Mix	WPA2 or WPA2-Mix

For example, if the wireless network has a RADIUS server, you can choose **WPA** or **WPA2**. If users do not log in to the wireless network, you can choose no encryption, **Static WEP**, **WPA-PSK**, or **WPA2-PSK**.

Usually, you should set up the strongest encryption that every wireless client in the wireless network supports. For example, suppose the AP does not have a local user database, and you do not have a RADIUS server. Therefore, there is no user authentication. Suppose the wireless network has two wireless clients. Device A only supports WEP, and device B supports WEP and WPA. Therefore, you should set up **Static WEP** in the wireless network.

Note: It is recommended that wireless clients use **WPA-PSK**, **WPA**, or stronger encryption. IEEE 802.1x and WEP encryption are better than none at all, but it is still possible for unauthorized devices to figure out the original information pretty quickly.

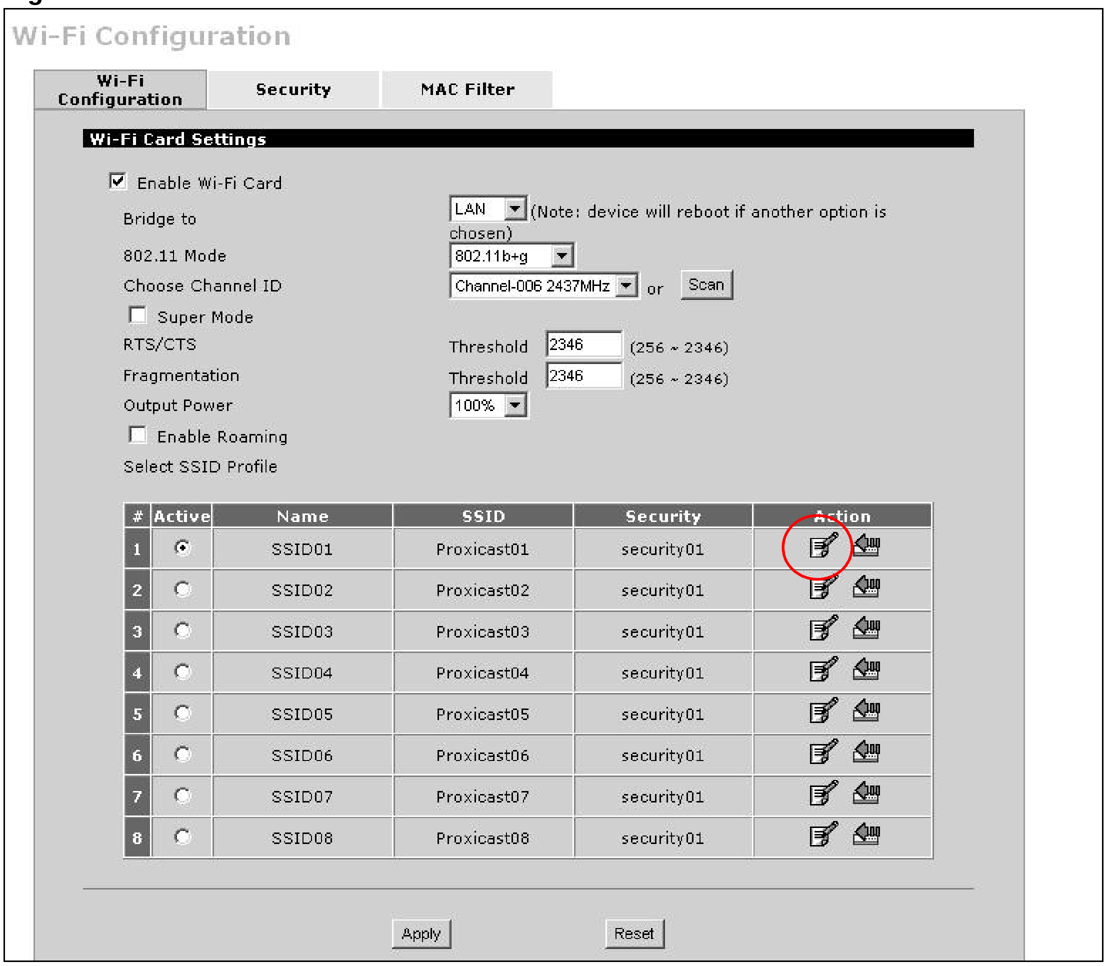
It is not possible to use **WPA-PSK**, **WPA** or stronger encryption with a local user database. In this case, it is better to set up stronger encryption with no authentication than to set up weaker encryption with the local user database.

8.2 Wi-Fi Configuration Screen

If you are configuring the LAN-Cell from a computer connected to the wireless LAN and you change the LAN-Cell's SSID or security 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 LAN-Cell's new settings.

Click **WIRELESS** > **Wi-Fi** to open the **Wi-Fi Configuraton** screen.

Figure 89 WIRELESS > Wi-Fi



The following table describes the labels in this screen.

Table 56 WIRELESS > Wi-Fi

LABEL	DESCRIPTION
Enable Wi-Fi Card	The internal Wi-Fi access point 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.
Bridge to	Select **LAN** to use the Wi-Fi card as part of the LAN. Select **DMZ** to use the Wi-Fi card as part of the DMZ. Select **WLAN** to use the Wi-Fi card as part of the WLAN. The LAN-Cell restarts after you change the Wi-Fi card setting. Note: If you set the Wi-Fi card to be part of the LAN or DMZ, you can still use wireless access. The firewall will treat the Wi-Fi card as part of the LAN or DMZ respectively.
802.11 Mode	Select **802.11b Only** to allow only IEEE 802.11b compliant WLAN devices to associate with the LAN-Cell. Select **802.11g Only** to allow only IEEE 802.11g compliant WLAN devices to associate with the LAN-Cell. Select **802.11b+g** to allow both IEEE802.11b and IEEE802.11g compliant WLAN devices to associate with the LAN-Cell. The transmission rate of your LAN-Cell might be reduced. Select **802.11a Only** to allow only IEEE 802.11a compliant WLAN devices to associate with the LAN-Cell.
Choose Channel ID	Set the operating frequency/channel depending on your particular region. To manually set the LAN-Cell to use a channel, select a channel from the drop-down list box. To have the LAN-Cell automatically select a channel, click **Scan** instead.
Scan	Click this button to have the LAN-Cell automatically select the wireless channel with the lowest interference.
Super Mode	Select this to improve data throughput on the WLAN by enabling fast frame and packet bursting. At the time of writing, this works only when the wireless client is using an Atheros card.
RTS/CTS Threshold	This is the threshold (number of bytes) for enabling RTS/CTS handshake. Data with a 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. Enter a value between **256** and **2346**. If you select **Super Mode**, this field is grayed out and the LAN-Cell uses 2346 automatically.
Fragmentation Threshold	This is 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 **2346**. If you select **Super Mode**, this field is grayed out and the LAN-Cell uses 2346 automatically.
Output Power	Set the output power of the LAN-Cell in this field. If there is a high density of APs in an area, decrease the output power to reduce interference with other APs. Select one of the following **100%** (full power), **50%**, **25%**, **12.5%** or **min** (minimum). See the product specifications for more information on your LAN-Cell's output power.
Enable Roaming	Roaming allows wireless stations to switch from one access point to another as they move from one coverage area to another. Select this checkbox to enable roaming on the LAN-Cell if you have two or more LAN-Cells on the same subnet. Note: All APs on the same subnet and the wireless clients must have the same SSID to allow roaming.

Table 56 WIRELESS > Wi-Fi (continued)

LABEL	DESCRIPTION
Select SSID Profile	An SSID profile is the set of parameters relating to one of the LAN-Cell's BSSs. The SSID (Service Set IDentifier) identifies the Service Set with which a wireless client is associated. Wireless clients associating with the access point (AP) must have the same SSID. Note: If you are configuring the LAN-Cell from a computer connected to the wireless LAN and you change the LAN-Cell's SSID or security 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 LAN-Cell's new settings.
#	This field displays the index number of each SSID profile.
Active	Choose a profile to apply to your wireless network by selecting its radio button.
Name	This field displays the identification name of each SSID profile on the LAN-Cell.
SSID	This field displays the name of the wireless profile on the network. When a wireless client scans for an AP to associate with, this is the name that is broadcast and seen in the wireless client utility.
Security	This field indicates which security profile is currently associated with each SSID profile. See Section 8.3 on page 169 for more information.
Action	Click the **Edit** icon next to the profile you want to configure and go to the SSID configuration screen. Click the **Reset Default** icon to clear all user-entered configuration information and return the SSID profile to its factory defaults.
Apply	Click **Apply** to save your changes back to the LAN-Cell.
Reset	Click **Reset** to begin configuring this screen afresh.

8.2.1 SSID Profile

Configure wireless network security by configuring and applying an SSID profile. You can configure multiple profiles but you can only apply one to your network.

Use the **Wi-Fi Configuration** screen to see information about the SSID profiles on the LAN-Cell, and use the **Wi-Fi CONFIGURATION** > **Edit** screen to configure the SSID profiles.

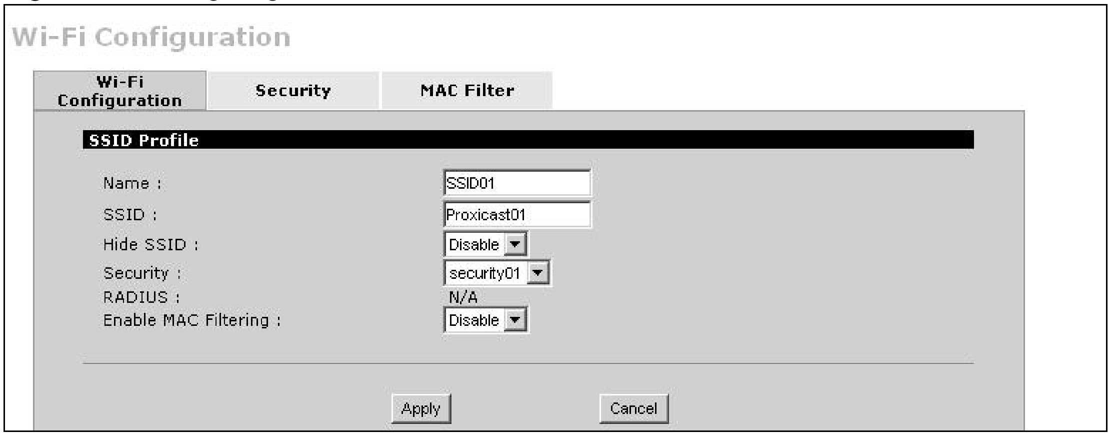
Each SSID profile references the settings configured in the following screens:

- **Wi-Fi CONFIGURATION** > **Security** (one of the security profiles).
- **AUTH SERVER** > **RADIUS** (the RADIUS server settings).
- **Wi-Fi CONFIGURATION** > **MAC Filter** (the MAC filter list, if activated in the SSID profile).

Configure the fields in the above screens to use the settings in an SSID profile.

In the **Wi-Fi CONFIGURATION** screen, click the **Edit** icon next to an SSID profile to display the following screen.

Figure 90 Configuring SSID



The following table describes the labels in this screen.

Table 57 Configuring SSID

LABEL	DESCRIPTION
Name	Enter a name (up to 32 printable 7-bit ASCII characters) identifying this profile.
SSID	When a wireless client scans for an AP to associate with, this is the name that is broadcast and seen in the wireless client utility. Enter a descriptive name (up to 32 printable 7-bit ASCII characters) for the wireless LAN.
Hide SSID	Select **Disable** if you want the LAN-Cell to broadcast this SSID (a wireless client scanning for an AP will find this SSID). Alternatively, select **Enable** to have the LAN-Cell hide this SSID (a wireless client scanning for an AP will not find this SSID).
Security	Select a security profile to use with this SSID profile. See Section 8.3 on page 169 for more information.
RADIUS	This displays **N/A** if the security profile you selected does not use RADIUS authentication. See Section 12.3 on page 285 for more information. This displays **Radius Configuration** if you select a security profile that uses RADIUS authentication. Click **Radius Configuration** to go to the **RADIUS** screen where you can view and/or change the RADIUS settings. See Section 12.3 on page 285 for more information.
Enable MAC Filtering	Select **Enable** from the drop down list box to activate MAC address filtering.
Apply	Click **Apply** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving.

8.3 Wireless Security Screen

Click **WIRELESS** > **Wi-Fi** > **Security** to open the **Security** screen. Use this screen to create security profiles. A security profile is a group of configuration settings which can be assigned to an SSID profile in the **Wi-Fi Configuration** screen.

The screen changes when you configure a security profile and varies according to the security modes you select.

The following table describes the security modes you can configure.

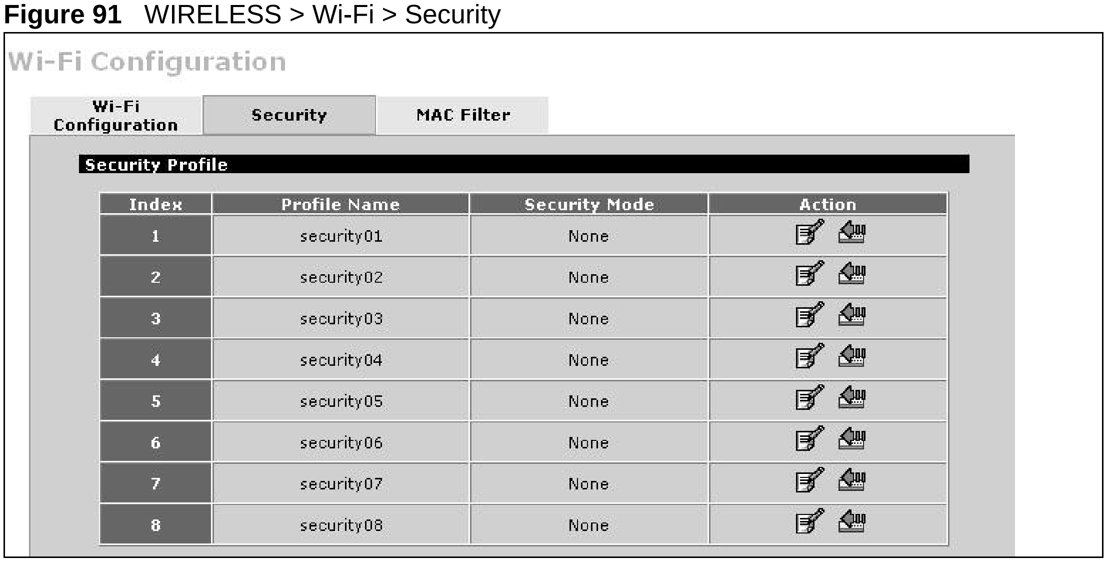
Table 58 Security Modes

SECURITY MODE	DESCRIPTION
None	Select this to have no data encryption.
WEP	Select this to use WEP encryption.
802.1x-Only	Select this to use 802.1x authentication with no data encryption.
802.1x-Static64	Select this to use 802.1x authentication with a static 64bit WEP key and an authentication server.
802.1x-Static128	Select this to use 802.1x authentication with a static 128bit WEP key and an authentication server.
WPA	Select this to use WPA.
WPA-PSK	Select this to use WPA with a pre-shared key.
WPA2	Select this to use WPA2.
WPA2-MIX	Select this to use either WPA2 or WPA depending on which security mode the wireless client uses.
WPA2-PSK	Select this to use WPA2 with a pre-shared key.
WPA2-PSK-MIX	Select this to use either WPA-PSK or WPA2-PSK depending on which security mode the wireless client uses.

If some wireless clients support WPA and some support WPA2, you should set up **WPA2-PSK-Mix** or **WPA2-Mix** (depending on the type of wireless network login) in the LAN-Cell.

Many types of encryption use a key to protect the information in the wireless network. The longer the key, the stronger the encryption. Every wireless client in the wireless network must have the same key.

Figure 91 WIRELESS > Wi-Fi > Security



The following table describes the labels in this screen.

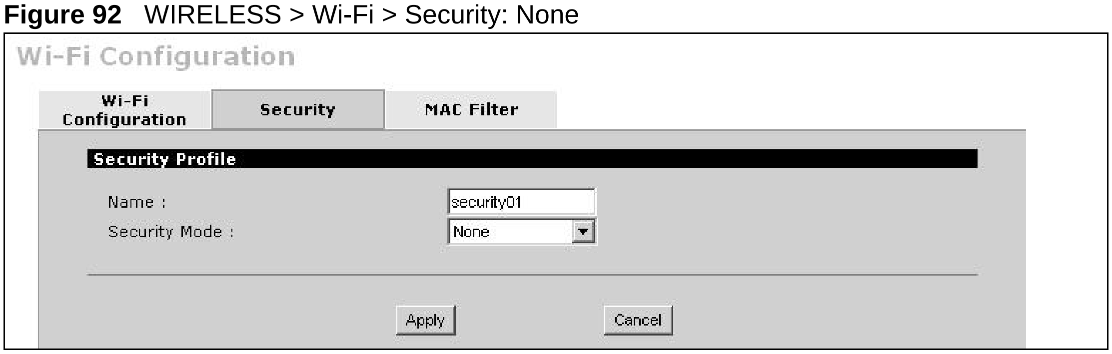
Table 59 WIRELESS > Wi-Fi > Security

LABEL	DESCRIPTION
Security Profile	
Index	This is the index number of the security profile.
Profile Name	This field displays a name given to a security profile in the **Security** configuration screen.
Security Mode	This field displays the security mode this security profile uses.
Action	Click the **Edit** icon to configure security settings for that profile. Click the **Reset Default** icon to clear all user-entered configuration information and return the security profile to its factory defaults.

8.3.1 No Security

If you do not enable any wireless security on your LAN-Cell, your network is accessible to any wireless networking device within range.

Figure 92 WIRELESS > Wi-Fi > Security: None



The following table describes the wireless LAN security labels in this screen.

Table 60 WIRELESS > Wi-Fi > Security: None

LABEL	DESCRIPTION
Name	Type a name (up to 32 printable 7-bit ASCII characters) to identify this security profile.
Security Mode	Select **None** to allow wireless clients to communicate with the access points without any data encryption.
Apply	Click **Apply** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving.

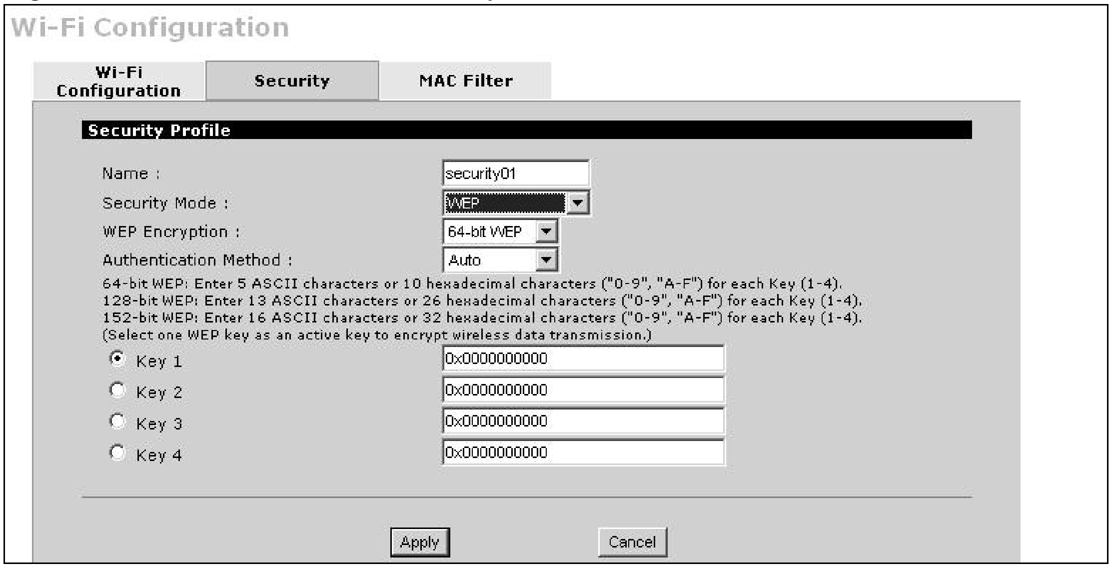
8.3.2 Static WEP

Static 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.

Your LAN-Cell allows you to configure up to four 64-bit, 128-bit or 152-bit WEP keys, but only one key can be used at any one time.

In order to configure and enable WEP encryption, click **WIRELESS** > **Wi-Fi** > **Security** > **Edit**.

Figure 93 WIRELESS > Wi-Fi > Security: WEP



The following table describes the labels in this screen.

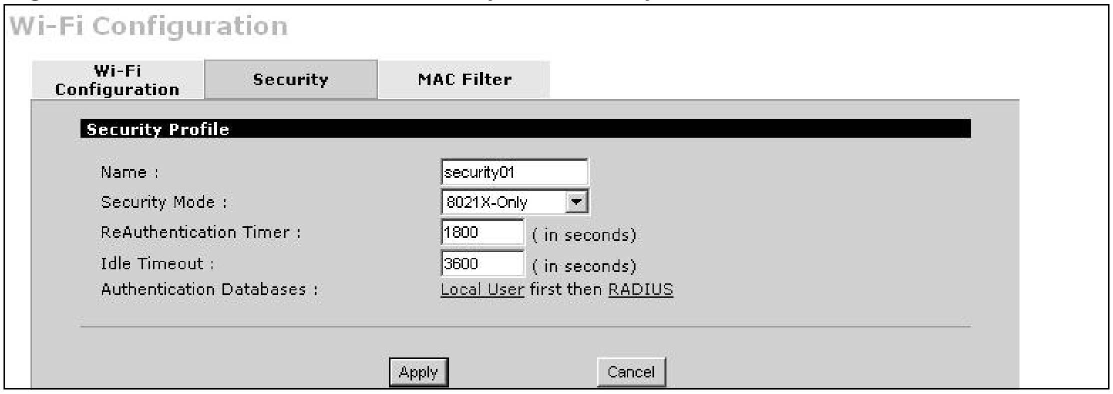
Table 61 WIRELESS > Wi-Fi > Security: WEP

LABEL	DESCRIPTION
Name	Type a name to identify this security profile.
Security Mode	Select **WEP** from the drop-down list.
WEP Encryption	WEP (Wired Equivalent Privacy) provides data encryption to prevent unauthorized wireless stations from accessing data transmitted over the wireless network. Select **64-bit WEP**, **128-bit WEP** or **152-bit WEP** to enable data encryption.
Authentication Method	Select **Shared-Key** to have the LAN-Cell use the default WEP key to authenticate the wireless client to the LAN-Cell. Select **Auto** to have the LAN-Cell switch between the shared-key and open system (the wireless clients and AP do not share a secret key for authentication) modes automatically. The default setting is **Auto**.
Key 1 to Key 4	The WEP keys are used to encrypt data. Both the LAN-Cell and the wireless clients must use the same WEP key for data transmission. If you chose **64-bit WEP** in the **WEP Encryption** field, then enter any 5 ASCII characters 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 ASCII characters or 26 hexadecimal characters ("0-9", "A-F") preceded by 0x for each key. If you chose **152-bit WEP** in the **WEP Encryption** field, then enter 16 ASCII characters or 32 hexadecimal characters ("0-9", "A-F") preceded by 0x for each key. You can configure up to four keys, but only one key can be activated at any one time. The default key is key 1.
Apply	Click **Apply** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving.

8.3.3 IEEE 802.1x Only

Click the **WIRELESS** > **Wi-Fi** > **Security** > **Edit**. Select **8021X-Only** from the **Security Mode** list.

Figure 94 WIRELESS > Wi-Fi > Security: 802.1x Only



The following table describes the labels in this screen.

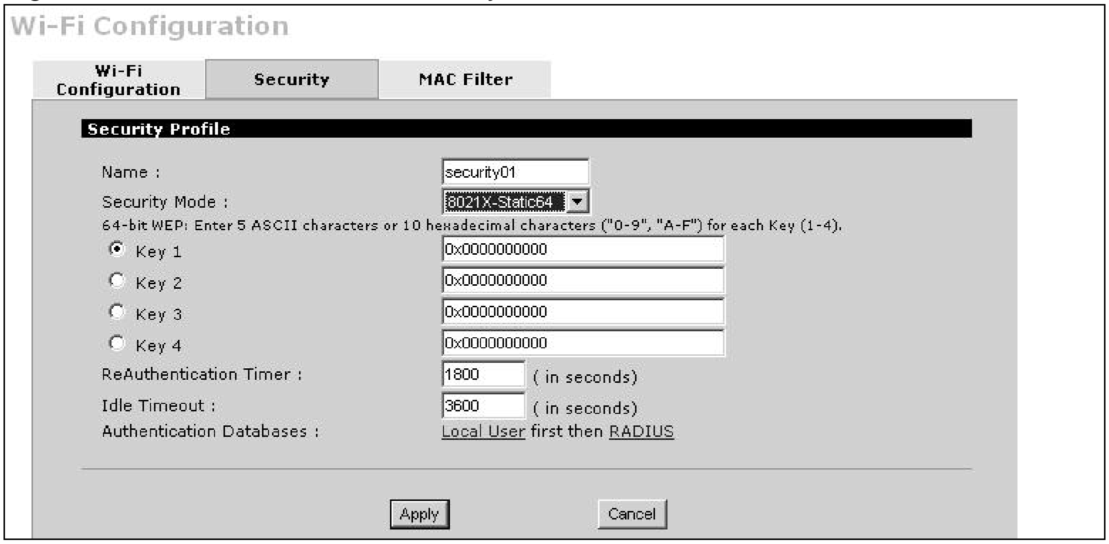
Table 62 WIRELESS > Wi-Fi > Security: 802.1x Only

LABEL	DESCRIPTION
Name	Type a name to identify this security profile.
Security Mode	Select **8021X-Only** from the drop-down list.
ReAuthentication Timer	Specify how often wireless clients have to resend user names and passwords in order to stay connected. Enter a time interval between 600 and 65535 seconds. If wireless client authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.
Idle Timeout	The LAN-Cell automatically disconnects a wireless client from the wireless network after a period of inactivity. The wireless client needs to send the username and password again before it can use the wireless network again. Some wireless clients may prompt users for a username and password; other clients may use saved login credentials. In either case, there is usually a short delay while the wireless client logs in to the wireless network again. This value is usually smaller when the wireless network is keeping track of how much time each wireless client is connected to the wireless network (for example, using an authentication server). If the wireless network is not keeping track of this information, you can usually set this value higher to reduce the number of delays caused by logging in again. Enter a time interval between 600 and 65535 seconds.
Authentication Databases	Click **Local User** to go to the **Local User Database** screen where you can view and/or edit the list of users and passwords. Click **RADIUS** to go to the **RADIUS** screen where you can configure the LAN-Cell to check an external RADIUS server.
Apply	Click **Apply** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving.

8.3.4 IEEE 802.1x + Static WEP

Click the **WIRELESS** > **Wi-Fi** > **Security** > **Edit**. Select **8021X-Static 64** or **8021X-Static128** in the **Security Mode** field to display the following screen.

Figure 95 WIRELESS > Wi-Fi > Security: 802.1x + Static WEP



The following table describes the labels in this screen.

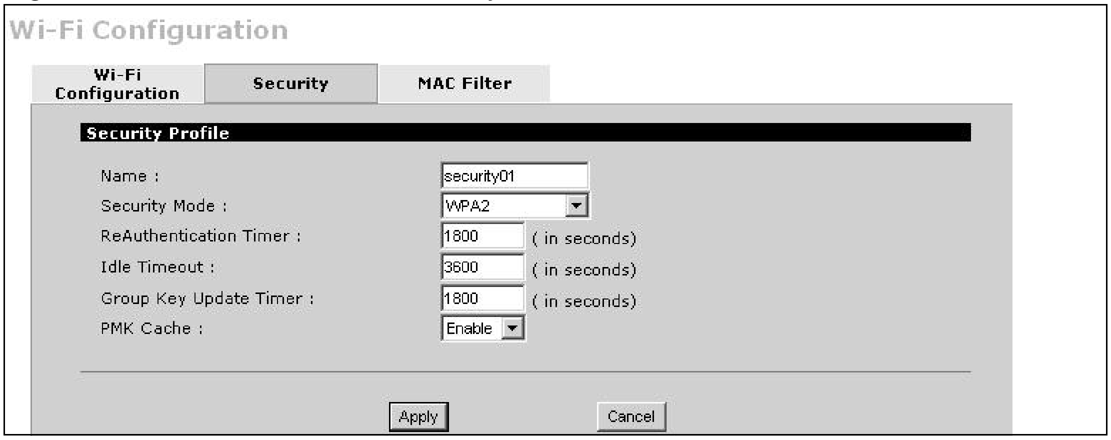
Table 63 WIRELESS > Wi-Fi > Security: 802.1x + Static WEP

LABEL	DESCRIPTION
Name	Type a name to identify this security profile.
Security Mode	Select **8021X-Static64** or **8021X-Static128** from the drop-down list.
Key 1 to Key 4	If you chose **8021X-Static64** in the **Security Mode** 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 **8021X-Static128** in the **Security Mode** 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 clients.
ReAuthentication Timer	Specify how often wireless clients have to resend user names and passwords in order to stay connected. Enter a time interval between 600 and 65535 seconds. If wireless client authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.
Idle Timeout	The LAN-Cell automatically disconnects a wireless client from the wireless network after a period of inactivity. The wireless client needs to send the username and password again before it can use the wireless network again. Some wireless clients may prompt users for a username and password; other clients may use saved login credentials. In either case, there is usually a short delay while the wireless client logs in to the wireless network again. This value is usually smaller when the wireless network is keeping track of how much time each wireless client is connected to the wireless network (for example, using an authentication server). If the wireless network is not keeping track of this information, you can usually set this value higher to reduce the number of delays caused by logging in again. Enter a time interval between 600 and 65535 seconds.
Authentication Databases	Click **Local User** to go to the **Local User Database** screen where you can view and/or edit the list of users and passwords. Click **RADIUS** to go to the **RADIUS** screen where you can configure the LAN-Cell to check an external RADIUS server.
Apply	Click **Apply** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving.

8.3.5 WPA, WPA2, WPA2-MIX

Click **WIRELESS** > **Wi-Fi** > **Security** > **Edit**. Select **WPA**, **WPA2** or **WPA2-MIX** from the **Security Mode** list.

Figure 96 WIRELESS > Wi-Fi > Security: WPA, WPA2 or WPA2-MIX



The following table describes the labels in this screen.

Table 64 WIRELESS > Wi-Fi > Security: WPA, WPA2 or WPA2-MIX

LABEL	DESCRIPTION
Name	Type a name to identify this security profile.
Security Mode	Select **WPA**, **WPA2** or **WPA2-MIX** from the drop-down list.
ReAuthentication Timer	Specify how often wireless clients have to resend user names and passwords in order to stay connected. Enter a time interval between 600 and 65535 seconds. If wireless client authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.
Idle Timeout	The LAN-Cell automatically disconnects a wireless client from the wireless network after a period of inactivity. The wireless client needs to send the username and password again before it can use the wireless network again. Some wireless clients may prompt users for a username and password; other clients may use saved login credentials. In either case, there is usually a short delay while the wireless client logs in to the wireless network again. This value is usually smaller when the wireless network is keeping track of how much time each wireless client is connected to the wireless network (for example, using an authentication server). If the wireless network is not keeping track of this information, you can usually set this value higher to reduce the number of delays caused by logging in again. Enter a time interval between 600 and 65535 seconds.
Group Key Update Timer	The **Group Key Update Timer** is the rate at which the AP sends a new group key out to all clients. The re-keying process is the WPA equivalent of automatically changing the WEP key for an AP and all stations in a WLAN on a periodic basis. Setting of the **Group Key Update Timer** is also supported in **WPA(2)-PSK** mode.
PMK Cache	This field is available only when you select **WPA2** or **WPA2-MIX**. When a wireless client moves from one AP's coverage area to another, it performs an authentication procedure (exchanging security information) with the new AP. Instead of re-authenticating a client each time it returns to the AP's coverage area, which can cause delays to time-sensitive applications, the AP and the client can store (or "cache") and use information about their previous authentication. Select **Enable** to allow PMK (Pairwise Master Key) caching, or **Disable** to switch this feature off.

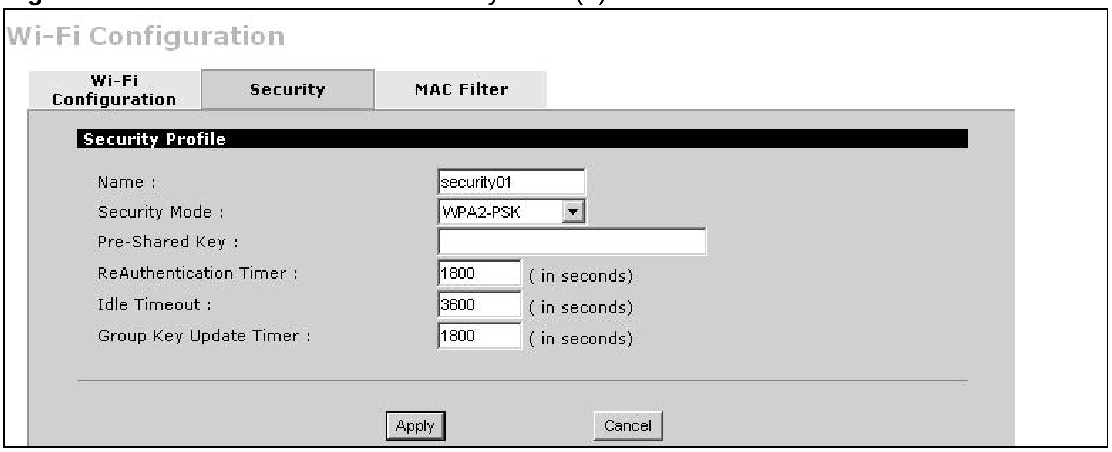
Table 64 WIRELESS > Wi-Fi > Security: WPA, WPA2 or WPA2-MIX (continued)

LABEL	DESCRIPTION
Apply	Click **Apply** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving.

8.3.6 WPA-PSK, WPA2-PSK, WPA2-PSK-MIX

Click **WIRELESS** > **Wi-Fi** > **Security** > **Edit**. Select **WPA-PSK**, **WPA2-PSK** or **WPA2-PSK-MIX** from the **Security Mode** list.

Figure 97 WIRELESS > Wi-Fi > Security: WPA(2)-PSK



The following table describes the labels in this screen.

Table 65 WIRELESS > Wi-Fi > Security: WPA(2)-PSK

LABEL	DESCRIPTION
Name	Type a name to identify this security profile.
Security Mode	Select **WPA-PSK**, **WPA2-PSK** or **WPA2-PSK-MIX** from the drop-down list.
Pre-Shared Key	The encryption mechanisms used for **WPA(2)** and **WPA(2)-PSK** are the same. The only difference between the two is that **WPA(2)-PSK** uses a simple common password, instead of user-specific credentials. Type a pre-shared key from 8 to 63 case-sensitive ASCII characters (including spaces and symbols).
ReAuthentication Timer	Specify how often wireless clients have to resend user names and passwords in order to stay connected. Enter a time interval between 600 and 65535 seconds. If wireless client authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.
Idle Timeout	The LAN-Cell automatically disconnects a wireless client from the wireless network after a period of inactivity. The wireless client needs to send the username and password again before it can use the wireless network again. Some wireless clients may prompt users for a username and password; other clients may use saved login credentials. In either case, there is usually a short delay while the wireless client logs in to the wireless network again. This value is usually smaller when the wireless network is keeping track of how much time each wireless client is connected to the wireless network (for example, using an authentication server). If the wireless network is not keeping track of this information, you can usually set this value higher to reduce the number of delays caused by logging in again. Enter a time interval between 600 and 65535 seconds.

Table 65 WIRELESS > Wi-Fi > Security: WPA(2)-PSK (continued)

LABEL	DESCRIPTION
Group Key Update Timer	The **Group Key Update Timer** is the rate at which the AP sends a new group key out to all clients. The re-keying process is the WPA equivalent of automatically changing the WEP key for an AP and all stations in a WLAN on a periodic basis. Setting of the **Group Key Update Timer** is also supported in **WPA(2)-PSK** mode.
Apply	Click **Apply** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving.

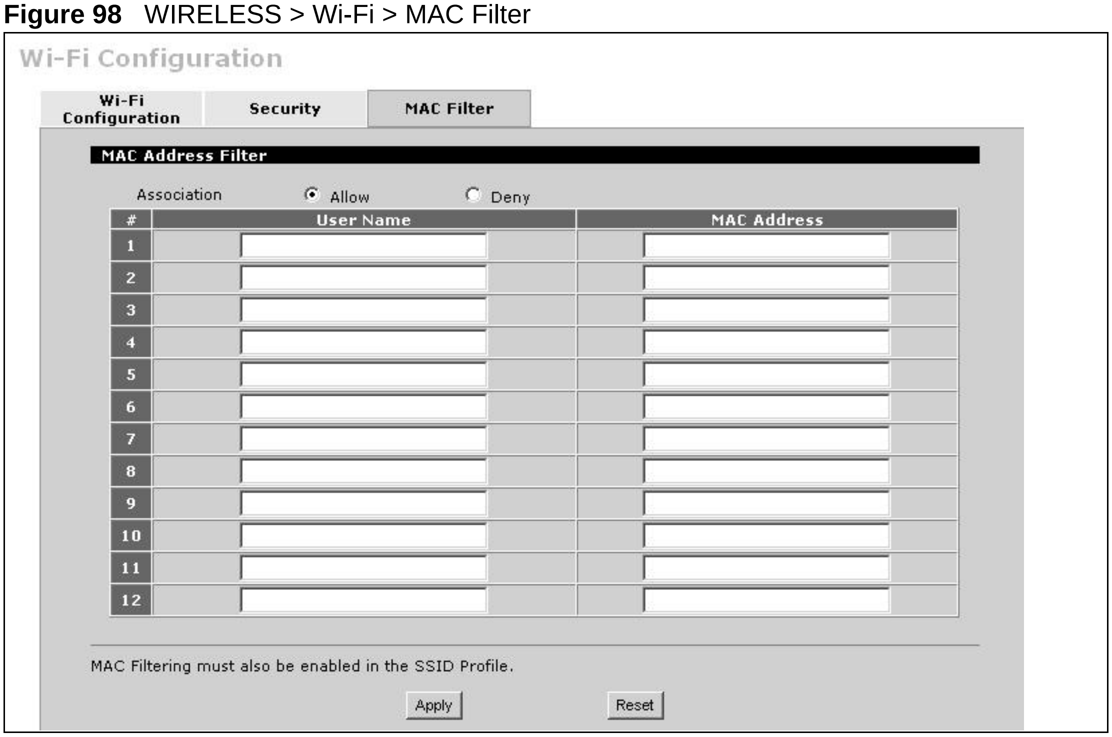
8.4 MAC Filter Screen

The MAC filter screen allows you to configure the LAN-Cell to give exclusive access to specific devices (**Allow**) or exclude specific devices from accessing the LAN-Cell (**Deny**). 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, 00:1B:39:00:00:02. You need to know the MAC addresses of the devices to configure this screen.

To change your LAN-Cell's MAC filter settings, click the **WIRELESS** > **Wi-Fi** > **MAC Filter**. The screen appears as shown.

To activate MAC filtering on a profile, select **Enable** from the **Enable MAC Filtering** drop-down list box in the **Wi-Fi > Edit** screen and click **Apply**.

Figure 98 WIRELESS > Wi-Fi > MAC Filter



The following table describes the labels in this menu.

Table 66 WIRELESS > Wi-Fi > MAC Filter

LABEL	DESCRIPTION
Association	Define the filter action for the list of MAC addresses in the MAC address filter table. Select **Deny** to block access to the router, MAC addresses not listed will be allowed to access the router. Select **Allow** to permit access to the router, MAC addresses not listed will be denied access to the router.
#	This is the index number of the MAC address.
User Name	Enter a descriptive name for the MAC address.
MAC Address	Enter the MAC addresses (in XX:XX:XX:XX:XX:XX format) of the wireless stations that are allowed or denied access to the LAN-Cell in these address fields.
Apply	Click **Apply** to save your changes back to the LAN-Cell.
Reset	Click **Reset** to begin configuring this screen afresh.

8.5 Country Codes

The radio channel frequencies allocated for 802.11 wireless devices differ slightly in various countries. The LAN-Cell's internal 802.11 access point's default settings utilize channels which are appropriate for North America. If you will be deploying the LAN-Cell outside of North America, you must change the LAN-Cell's Country Code in order to modify the 802.11 access point's channel frequencies for your local region.

Failure to use the correct Country Code may cause unintended interference or prevent other 802.11 equipment from connecting to the LAN-Cell and may violate local communication regulations.

To change the LAN-Cell's Country Code:

1 Refer to Appendix E on page 631 to find the code for your Country/Region.
2 Using either the Console Port or a Telnet/SSH session, log into the System Management Terminal (SMT). Refer to Chapter 23 Introducing the SMT.
3 Select Menu 24 (System Maintenance), then Menu 8 (Command Interpreter Mode).
4 At the command line prompt, enter the command: `sys countrycode NNN` where NNN is the 3 digit country code value from Table 257 on page 631.
5 Press `[ENTER]` to save the new country code value.
6 Type `sys countrycode [ENTER]` to confirm the new country code value.
7 Return to the **Wi-Fi Configuration** screen and select the appropriate 802.11 channel.

If you reset the LAN-Cell to its Factory Default settings, you must reset the Country Code using the procedure above.

PART III
Security Menu

9

Firewall Screens

9.1 Overview

A *firewall* is a system or group of systems that enforces an access-control policy between two networks. It is generally a mechanism used to protect a trusted network from an untrusted network.

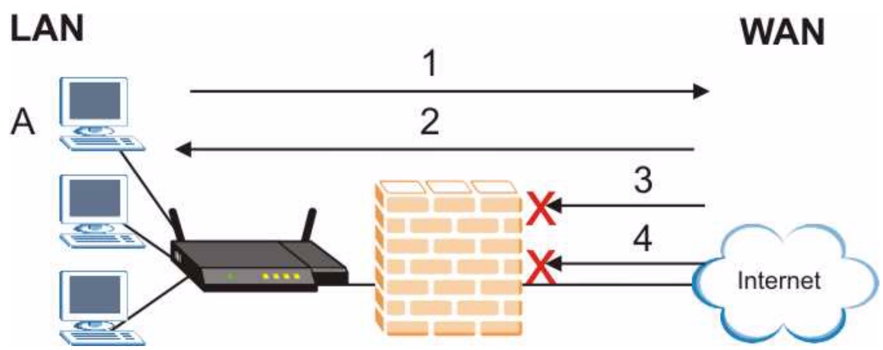
The LAN-Cell physically separates the LAN, DMZ, WLAN and the WAN and acts as a secure gateway for all data passing between the networks. The LAN-Cell protects against Denial of Service (DoS) attacks, prevents theft, destruction and modification of data, and logs events.

Enable the firewall to protect your LAN computers from attacks by hackers on the Internet and control access between the LAN, DMZ, WLAN and WAN. By default the firewall:

- allows traffic that originates from your LAN computers to go to all of the networks.
- blocks traffic that originates on the other networks from going to the LAN.
- allows traffic that originates on from WAN or CELL to access the default LAN-Cell Remote Management service ports (http/https, telent/ssh, ftp, snmp)
- allows traffic that originates on the WLAN to go to the WAN.
- allows traffic that originates on the WAN to go to the DMZ and protects your DMZ computers against DoS attacks.
- allows VPN traffic between any of the networks.

The following figure illustrates the default firewall action. User A can initiate an IM (Instant Messaging) session from the LAN to the WAN (1). Return traffic for this session is also allowed (2). However other traffic initiated from the WAN is blocked (3 and 4).

Figure 99 Default Firewall Action



Your customized rules take precedence and override the LAN-Cell's default settings. The LAN-Cell checks the source IP address, destination IP address and IP protocol type of network traffic against the firewall rules (in the order you list them). When the traffic matches a rule, the LAN-Cell takes the action specified in the rule.

9.1.1 What You Can Do in the Firewall Screens

- Use the Default Rule screens (Section 9.3 on page 184) to configure general firewall settings that apply when no specific rules have been matched.
- Use the Rule Summary screens (Section 9.4 on page 186) to configure firewall rules.
- Use the Anti-Probing screen (Section 9.5 on page 191) to specify which of the LAN-Cell's interfaces will respond to Ping requests and whether or not the LAN-Cell is to respond to probing for unused ports.
- Use the Threshold screen (Section 9.6 on page 192) to configure DoS thresholds and actions to be taken when a threshold is reached.
- Use the Service screen (Section 9.7 on page 194) to configure custom services for use in firewall rules or view the services that are predefined in the LAN-Cell.

9.1.2 What You Need To Know About The LAN-Cell Firewall

Packet Direction

Packets have source and destination address headers. You can set what the LAN-Cell does with packets traveling in a specific direction (including going to/coming from a VPN tunnel) that do not match any of the firewall rules. See also Packet Direction Examples on page 200.

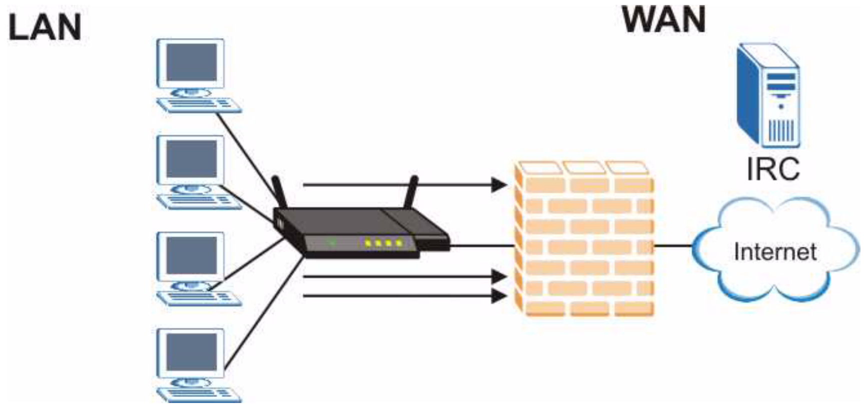
Asymmetrical Routes

Asymmetrical routes only apply if you have another gateway on your LAN and the firewall is enabled. If return traffic is routed through the LAN gateway (instead of the LAN-Cell), then the LAN-Cell may reset the 'incomplete' connection. When you enable asymmetrical routes, interface to same interface traffic (for example WAN to WAN, VPN to VPN and so on) is not checked by the firewall. See Asymmetrical Routes on page 206 for information on how to use IP alias instead of asymmetrical routes.

9.2 Firewall Rules Example

Suppose that your company decides to block all of the LAN users from using IRC (Internet Relay Chat) through the Internet. To do this, you would configure a LAN to WAN firewall rule that blocks IRC traffic from any source IP address from going to any destination address. You do not need to specify a schedule since you need the firewall rule to always be in effect. The following figure shows the results of this rule.

Figure 100 Blocking All LAN to WAN IRC Traffic Example



Your firewall would have the following configuration.

Table 67 Blocking All LAN to WAN IRC Traffic Example

#	SOURCE	DESTINATION	SCHEDULE	SERVICE	ACTION
1	Any	Any	Any	IRC	Drop
Default	Any	Any	Any	Any	Allow

- The first row blocks LAN access to the IRC service on the WAN.
- The second row is the firewall's default policy that allows all traffic from the LAN to go to the WAN.

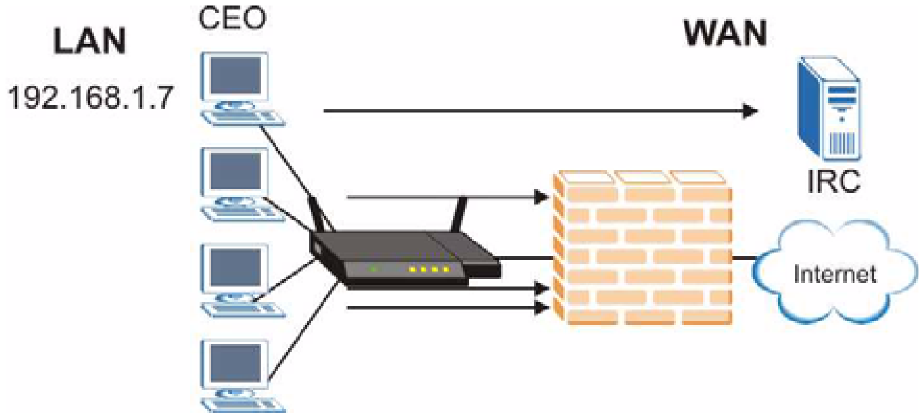
The LAN-Cell applies the firewall rules in order. So for this example, when the LAN-Cell receives traffic from the LAN, it checks it against the first rule. If the traffic matches (if it is IRC traffic) the firewall takes the action in the rule (drop) and stops checking the firewall rules. Any traffic that does not match the first firewall rule will match the default rule and the LAN-Cell forwards it.

Now suppose that your company wants to let the CEO use IRC. You can configure a LAN to WAN firewall rule that allows IRC traffic from the IP address of the CEO's computer. In order to make sure that the CEO's computer always uses the same IP address, make sure it either:

- has a static IP address,
- or you configure a static DHCP entry for it so the LAN-Cell always assigns it the same IP address (see Section 4.3 on page 83 for information on static DHCP).

Now you configure a LAN to WAN firewall rule that allows IRC traffic from the IP address of the CEO's computer (192.168.1.7 for example) to go to any destination address. You do not need to specify a schedule since you want the firewall rule to always be in effect. The following figure shows the results of your two custom rules.

Figure 101 Limited LAN to WAN IRC Traffic Example



Your firewall would have the following configuration.

Table 68 Limited LAN to WAN IRC Traffic Example

#	SOURCE	DESTINATION	SCHEDULE	SERVICE	ACTION
1	192.168.1.7	Any	Any	IRC	Allow
2	Any	Any	Any	IRC	Drop
Default	Any	Any	Any	Any	Allow

- The first row allows the LAN computer at IP address 192.168.1.7 to access the IRC service on the WAN.
- The second row blocks LAN access to the IRC service on the WAN.
- The third row is (still) the firewall's default policy of allowing all traffic from the LAN to go to the WAN.

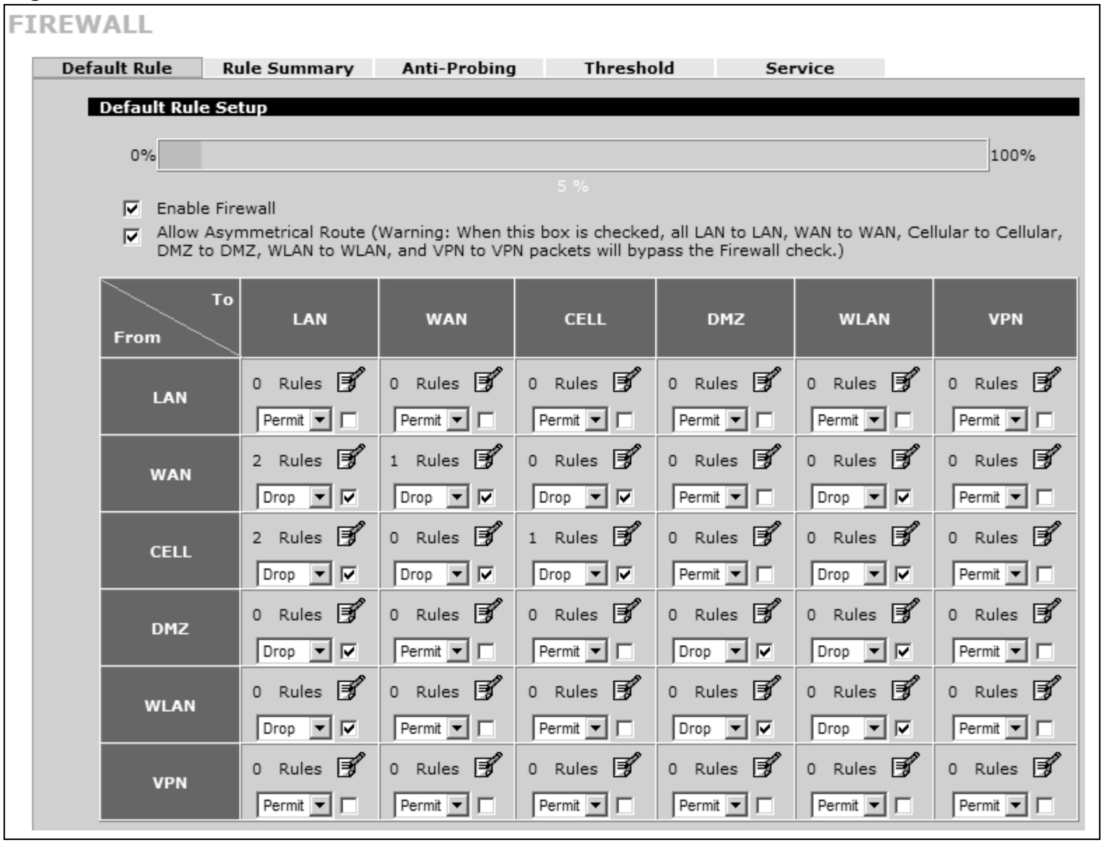
The rule for the CEO must come before the rule that blocks all LAN to WAN IRC traffic. If the rule that blocks all LAN to WAN IRC traffic came first, the CEO's IRC traffic would match that rule and the LAN-Cell would drop it and not check any other firewall rules.

9.3 Firewall Default Rule

Click **SECURITY** > **FIREWALL** to open the **Default Rule** screen.

Use this screen to configure general firewall settings for the LAN-Cell.

Figure 102 SECURITY > FIREWALL > Default Rule



The following table describes the labels in this screen.

Table 69 SECURITY > FIREWALL > Default Rule

LABEL	DESCRIPTION
0-100%	This bar displays the percentage of the LAN-Cell's firewall rules storage space that is currently in use. When the storage space is almost full, you should consider deleting unnecessary firewall rules before adding more firewall rules.
Enable Firewall	Select this check box to activate the firewall. The LAN-Cell performs access control and protects against Denial of Service (DoS) attacks when the firewall is activated. Note: When you activate the firewall, all current connections through the LAN-Cell are dropped when you apply your changes.
Allow Asymmetrical Route	If an alternate gateway on the LAN has an IP address in the same subnet as the LAN-Cell's LAN IP address, return traffic may not go through the LAN-Cell. This is called an asymmetrical or "triangle" route. This causes the LAN-Cell to reset the connection, as the connection has not been acknowledged. Select this check box to have the LAN-Cell permit the use of asymmetrical route topology on the network (not reset the connection). Note: Allowing asymmetrical routes may let traffic from the WAN go directly to the LAN without passing through the LAN-Cell. A better solution is to use IP alias to put the LAN-Cell and the backup gateway on separate subnets. See Asymmetrical Routes and IP Alias on page 206 for an example.

Table 69 SECURITY > FIREWALL > Default Rule (continued)

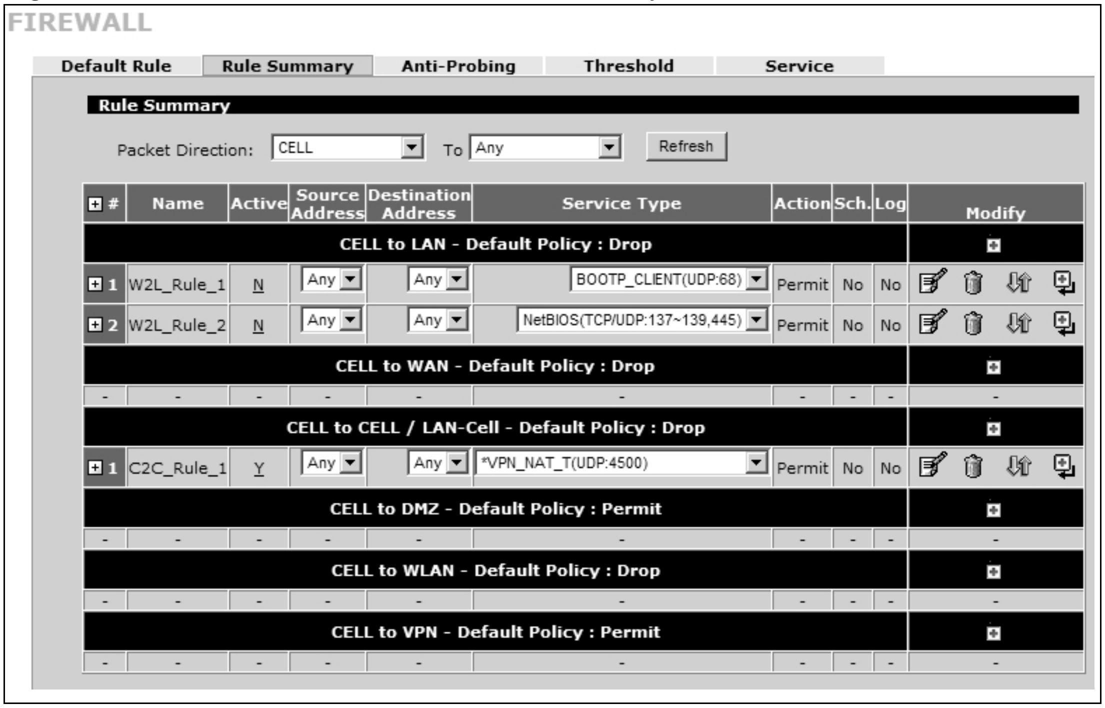
LABEL	DESCRIPTION
From, To	Set the firewall’s default actions based on the direction of travel of packets. Click the edit icon to go to a summary screen of the rules for that packet direction. Here are some example descriptions of the directions of travel. **From LAN To LAN** means packets traveling from a computer on one LAN subnet to a computer on another LAN subnet on the LAN interface of the LAN-Cell or the LAN-Cell itself. The LAN-Cell does not apply the firewall to packets traveling from a LAN computer to another LAN computer on the same subnet. **From CELL To LAN** means packets that originates from the 3G Cellular connection and are destined for devices on the private LAN subnet. **From WAN To LAN** means packets that originates from the wired Ethernet WAN port (or serial Dial-Backup port) and are destined for devices on the private LAN subnet. In fail-over operation, you will typically define the same firewall rules for both the WAN and CELL packet sources. **From VPN** means traffic that came into the LAN-Cell through a VPN tunnel and is going to the selected “to” interface. For example, **From VPN To LAN** specifies the VPN traffic that is going to the LAN. The LAN-Cell applies the firewall to the traffic after decrypting it. **To VPN** is traffic that comes in through the selected “from” interface and goes out through any VPN tunnel. For example, **From LAN To VPN** specifies the traffic that is coming from the LAN and going out through a VPN tunnel. The LAN-Cell applies the firewall to the traffic before encrypting it. **From VPN To VPN** means traffic that comes in through a VPN tunnel and goes out through (another) VPN tunnel or terminates at the LAN-Cell. This is the case when the LAN-Cell is the hub in a hub-and-spoke VPN. This is also the case if you allow someone to use a service (like Telnet or HTTP) through a VPN tunnel to manage the LAN-Cell. The LAN-Cell applies the firewall to the traffic after decrypting it. Note: The VPN connection directions apply to the traffic going to or from the LAN-Cell’s VPN tunnels. They do not apply to other VPN traffic for which the LAN-Cell is not one of the gateways (VPN pass-through traffic). Here are the default actions from which you can select. Select **Drop** to silently discard the packets without sending a TCP reset packet or an ICMP destination-unreachable message to the sender. Select **Reject** to deny the packets and send a TCP reset packet (for a TCP packet) or an ICMP destination-unreachable message (for a UDP packet) to the sender. Select **Permit** to allow the passage of the packets. The firewall rules for the WAN port with a higher route priority also apply to the dial backup connection.
Log	Select the check box next to a direction of packet travel to create a log when the above action is taken for packets that are traveling in that direction and do not match any of your customized rules.
Apply	Click **Apply** to save your changes back to the LAN-Cell.
Reset	Click **Reset** to begin configuring this screen afresh.

9.4 Firewall Rule Summary Screen

Click **SECURITY** > **FIREWALL** > **Rule Summary** to open the screen. This screen displays a list of the configured firewall rules.

The ordering of your rules is very important as rules are applied in the order that they are listed.

Figure 103 SECURITY > FIREWALL > Rule Summary



The following table describes the labels in this screen.

Table 70 SECURITY > FIREWALL > Rule Summary

LABEL	DESCRIPTION
Packet Direction	Use the drop-down list boxes and click **Refresh** to select a direction of travel of packets for which you want to display firewall rules. **To edit firewall rules for packets destined for one of the LAN-Cell's internal interfaces (such as a Remote Management port -- see page 319), select the same interface name in the Source and Destination drop-down listboxes (e.g. CELL to CELL) or select ANY as the Destination to see all rules that apply from the indicated source .** The VPN connection directions apply to the traffic going to or from the LAN-Cell's VPN tunnels. They do not apply to other VPN traffic for which the LAN-Cell is not one of the gateways (VPN pass-through traffic).
+/-	In the heading row, click + to expand or - to collapse the Source Address, Destination Address and Service Type drop down lists for all of the displayed rules.
Default Policy	This field displays the default action and log policy you selected in the **Default Rule** screen for the packet direction shown in the field above.
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.	

Table 70 SECURITY > FIREWALL > Rule Summary

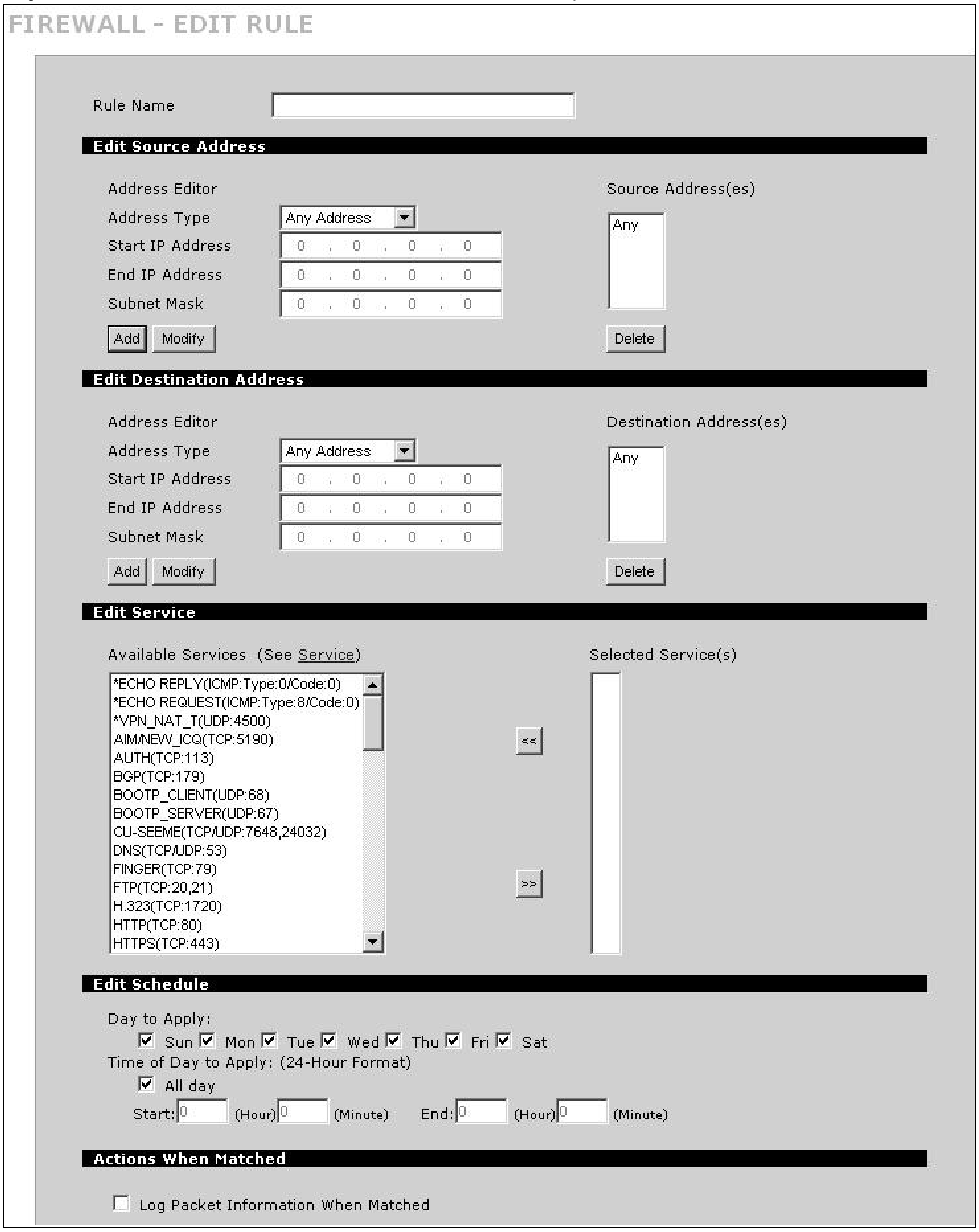
LABEL	DESCRIPTION
#	This is your firewall rule number. The ordering of your rules is important as rules are applied in turn. Click + to expand or - to collapse the **Source Address**, **Destination Address** and **Service Type** drop down lists.
Name	This is the name of the firewall rule.
Active	This field displays whether a firewall is turned on (**Y**) or not (**N**).
Source Address	This drop-down list box displays the source addresses or ranges of addresses to which this firewall rule applies. Please note that a blank source or destination address is equivalent to **Any**.
Destination Address	This drop-down list box displays the destination addresses or ranges of addresses to which this firewall rule applies. Please note that a blank source or destination address is equivalent to **Any**.
Service Type	This drop-down list box displays the services to which this firewall rule applies. See Appendix D on page 613 for a list of common services.
Action	This field displays whether the firewall silently discards packets (**Drop**), discards packets and sends a TCP reset packet or an ICMP destination-unreachable message to the sender (**Reject**) or allows the passage of packets (**Permit**).
Sch.	This field tells you whether a schedule is specified (**Yes**) or not (**No**).
Log	This field shows you whether a log is created when packets match this rule (**Yes**) or not (**No**).
Modify	Click the edit icon to go to the screen where you can edit the rule. Click the delete icon to delete an existing firewall rule. A window display asking you to confirm that you want to delete the firewall rule. Note that subsequent firewall rules move up by one when you take this action.

9.4.1 Firewall Edit Rule

In the Rule Summary screen, click the edit icon or the insert icon to display the Firewall Edit Rule screen.

Use this screen to create or edit a firewall rule. Refer to the following table for information on the labels.

Figure 104 SECURITY > FIREWALL > Rule Summary > Edit



The following table describes the labels in this screen.

Table 71 SECURITY > FIREWALL > Rule Summary > Edit

LABEL	DESCRIPTION
Rule Name	Enter a descriptive name of up to 31 printable ASCII characters (except Extended ASCII characters) for the firewall rule. Spaces are allowed.
Edit Source/Destination Address	
Address Type	Do you want your rule to apply to packets with a particular (single) IP, a range of IP addresses (for example 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.
Subnet Mask	Enter the subnet mask here, if applicable.
Add	Click **Add** to add a new address to the **Source** or **Destination Address(es)** box. You can add multiple addresses, ranges of addresses, and/or subnets.
Modify	To edit an existing source or destination address, select it from the box and click **Modify**.
Delete	Highlight an existing source or destination address from the **Source** or **Destination Address(es)** box above and click **Delete** to remove it.
Edit Service	
Available/ Selected Services	Highlight a service from the **Available Services** box on the left, then click **>>** to add it to the **Selected Service(s)** box on the right. To remove a service, highlight it in the **Selected Service(s)** box on the right, then click **<<**. Next to the name of a service, two fields appear in brackets. The first field indicates the IP protocol type (TCP, UDP, or ICMP). The second field indicates the IP port number that defines the service. (Note that there may be more than one IP protocol type). For example, look at the DNS entry, (UDP/TCP:53) means UDP port 53 and TCP port 53. Click the **Service** link to go to the **Service screen where you can** configure custom service ports. See Appendix D on page 613 for a list of commonly used services and port numbers. You can use the [CTRL] key and select multiple services at once.
Edit Schedule	
Day to Apply	Select everyday or the day(s) of the week to apply the rule.
Time of Day to Apply (24-Hour Format)	Select **All Day** or enter the start and end times in the hour-minute format to apply the rule.
Actions When Matched	
Log Packet Information When Matched	This field determines if a log for packets that match the rule is created (**Yes**) or not (**No**). Go to the **Log Settings** page and select the **Access Control** logs category to have the LAN-Cell record these logs.
Send Alert Message to Administrator When Matched	Select the check box to have the LAN-Cell generate an alert when the rule is matched.

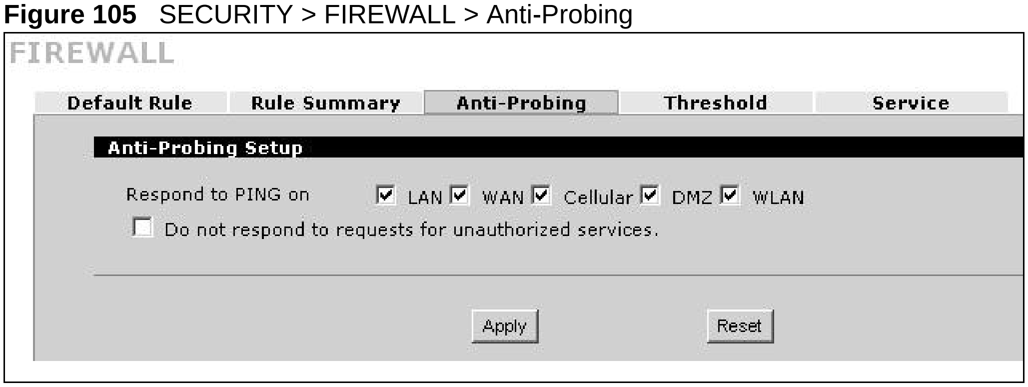
Table 71 SECURITY > FIREWALL > Rule Summary > Edit

LABEL	DESCRIPTION
Action for Matched Packets	Use the drop-down list box to select what the firewall is to do with packets that match this rule. Select **Drop** to silently discard the packets without sending a TCP reset packet or an ICMP destination-unreachable message to the sender. Select **Reject** to deny the packets and send a TCP reset packet (for a TCP packet) or an ICMP destination-unreachable message (for a UDP packet) to the sender. Select **Permit** to allow the passage of the packets. Note: You also need to configure NAT port forwarding (or full featured NAT address mapping rules) if you want to allow computers on the WAN to access devices on the LAN. Note: You may also need to configure the remote management settings if you want to allow a WAN computer to manage the LAN-Cell or restrict management from the LAN.
Apply	Click **Apply** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving.

9.5 Anti-Probing Screen

Click **SECURITY** > **FIREWALL** > **Anti-Probing** to open the following screen. Configure this screen to help keep the LAN-Cell hidden from probing attempts. You can specify which of the LAN-Cell's interfaces will respond to Ping requests and whether or not the LAN-Cell is to respond to probing for unused ports.

Figure 105 SECURITY > FIREWALL > Anti-Probing



The following table describes the labels in this screen.

Table 72 SECURITY > FIREWALL > Anti-Probing

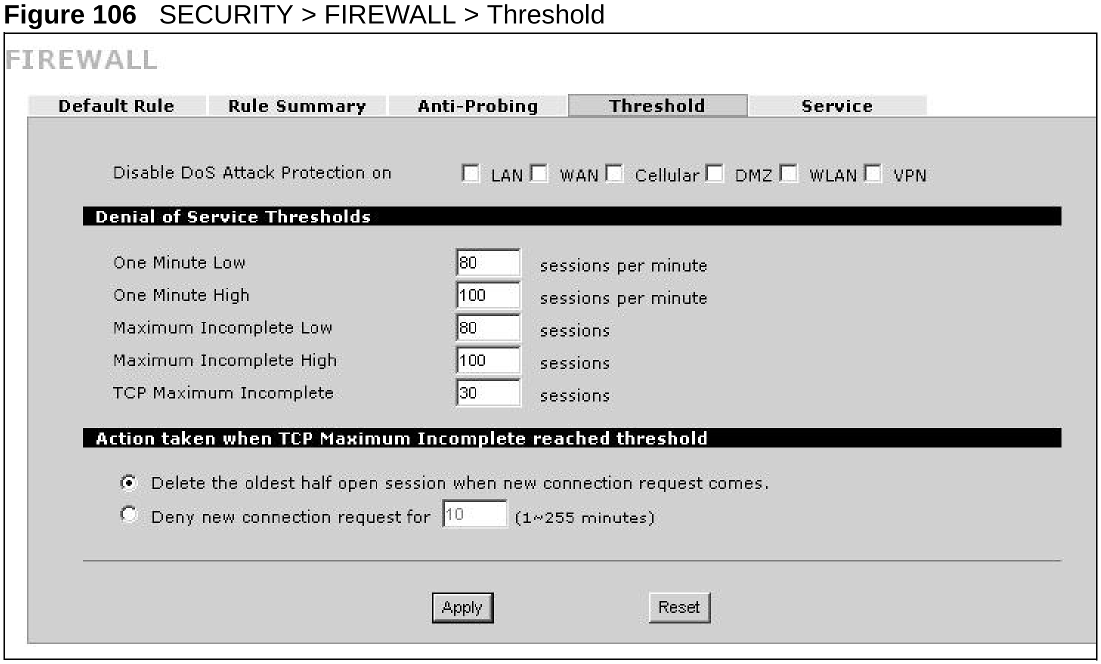
LABEL	DESCRIPTION
Respond to PING on	Select the check boxes of the interfaces that you want to reply to incoming Ping requests. Clear an interface's check box to have the LAN-Cell not respond to any Ping requests that come into that interface.
Do not respond to requests for unauthorized services.	Select this option to prevent hackers from finding the LAN-Cell by probing for unused ports. If you select this option, the LAN-Cell will not respond to port request(s) for unused ports, thus leaving the unused ports and the LAN-Cell unseen. If this option is not selected, the LAN-Cell will reply with an ICMP port unreachable packet for a port probe on its unused UDP ports and a TCP reset packet for a port probe on its unused TCP ports. Note that the probing packets must first traverse the LAN-Cell's firewall rule checks before reaching this anti-probing mechanism. Therefore if a firewall rule stops a probing packet, the LAN-Cell reacts based on the firewall rule to either send a TCP reset packet for a blocked TCP packet (or an ICMP port-unreachable packet for a blocked UDP packets) or just drop the packets without sending a response packet.
Apply	Click **Apply** to save your changes back to the LAN-Cell.
Reset	Click **Reset** to begin configuring this screen afresh.

9.6 Threshold Screen

For DoS attacks, the LAN-Cell uses thresholds to determine when to start dropping sessions that do not become fully established (half-open sessions). These thresholds apply globally to all sessions. See Threshold Values on page 207 for more information on DoS thresholds.

Click **SECURITY** > **FIREWALL** > **Threshold** to bring up the next screen. The global values specified for the threshold and timeout apply to all TCP connections.

Figure 106 SECURITY > FIREWALL > Threshold



The following table describes the labels in this screen.

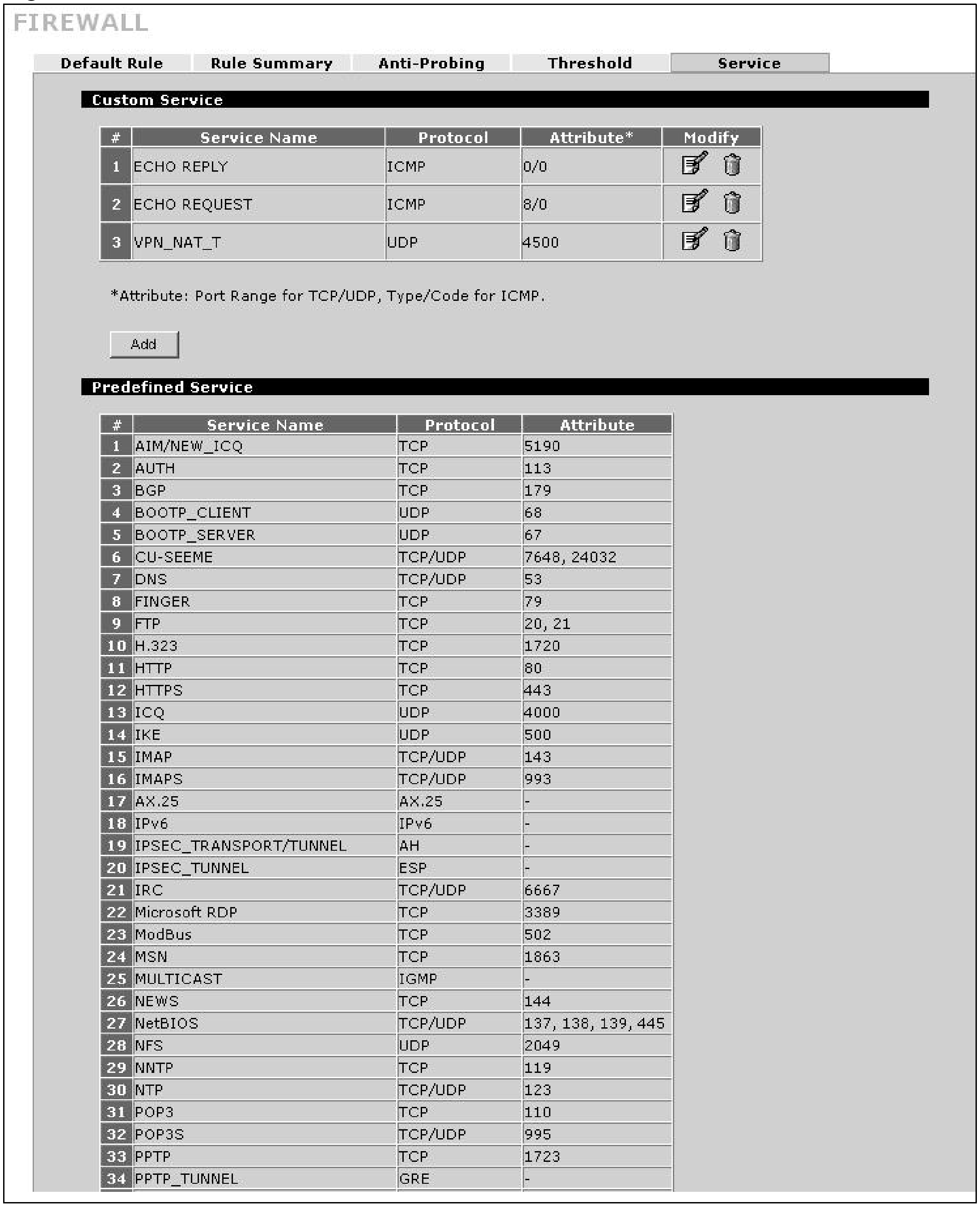
Table 73 SECURITY > FIREWALL > Threshold

LABEL	DESCRIPTION
Disable DoS Attack Protection on	Select the check boxes of any interfaces (or all VPN tunnels) for which you want the LAN-Cell to not use the Denial of Service protection thresholds. This disables DoS protection on the selected interface (or all VPN tunnels). You may want to disable DoS protection for an interface if the LAN-Cell is treating valid traffic as DoS attacks. Another option would be to raise the thresholds.
Denial of Service Thresholds	The LAN-Cell measures both the total number of existing half-open sessions and the rate of session establishment attempts. Both TCP and UDP half-open sessions are counted in the total number and rate measurements. Measurements are made once a minute.
One Minute Low	This is the rate of new half-open sessions per minute that causes the firewall to stop deleting half-open sessions. The LAN-Cell continues to delete half-open sessions as necessary, until the rate of new connection attempts drops below this number.
One Minute High	This is the rate of new half-open sessions per minute that causes the firewall to start deleting half-open sessions. When the rate of new connection attempts rises above this number, the LAN-Cell deletes half-open sessions as required to accommodate new connection attempts. For example, if you set the one minute high to 100, the LAN-Cell starts deleting half-open sessions when more than 100 session establishment attempts have been detected in the last minute. It stops deleting half-open sessions when the number of session establishment attempts detected in a minute goes below the number set as the one minute low.
Maximum Incomplete Low	This is the number of existing half-open sessions that causes the firewall to stop deleting half-open sessions. The LAN-Cell continues to delete half-open requests as necessary, until the number of existing half-open sessions drops below this number.
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 LAN-Cell deletes half-open sessions as required to accommodate new connection requests. Do not set **Maximum Incomplete High** to lower than the current **Maximum Incomplete Low** number. For example, if you set the maximum incomplete high to 100, the LAN-Cell starts deleting half-open sessions when the number of existing half-open sessions rises above 100. It stops deleting half-open sessions when the number of existing half-open sessions drops below the number set as the maximum incomplete low.
TCP Maximum Incomplete	An unusually high number of half-open sessions with the same destination host address could indicate that a DoS attack is being launched against the host. Specify 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. The LAN-Cell sends alerts whenever the **TCP Maximum Incomplete** is exceeded.
Action taken when TCP Maximum Incomplete reached threshold	Select the action that LAN-Cell should take when the TCP maximum incomplete threshold is reached. You can have the LAN-Cell either: Delete the oldest half open session when a new connection request comes. or Deny new connection requests for the number of minutes that you specify (between 1 and 256).
Apply	Click **Apply** to save your changes back to the LAN-Cell.
Reset	Click **Reset** to begin configuring this screen afresh.

9.7 Service Screen

Click **SECURITY > FIREWALL** > **Service** to open the screen as shown next. Use this screen to configure custom services for use in firewall rules or view the services that are predefined in the LAN-Cell.

Figure 107 SECURITY > FIREWALL > Service



#	Service Name	Protocol	Attribute*	Modify
1	ECHO REPLY	ICMP	0/0	
2	ECHO REQUEST	ICMP	8/0	
3	VPN_NAT_T	UDP	4500	

*Attribute: Port Range for TCP/UDP, Type/Code for ICMP.

Add

Predefined Service

#	Service Name	Protocol	Attribute
1	AIM/NEW_ICQ	TCP	5190
2	AUTH	TCP	113
3	BGP	TCP	179
4	BOOTP_CLIENT	UDP	68
5	BOOTP_SERVER	UDP	67
6	CU-SEEME	TCP/UDP	7648, 24032
7	DNS	TCP/UDP	53
8	FINGER	TCP	79
9	FTP	TCP	20, 21
10	H.323	TCP	1720
11	HTTP	TCP	80
12	HTTPS	TCP	443
13	ICQ	UDP	4000
14	IKE	UDP	500
15	IMAP	TCP/UDP	143
16	IMAPS	TCP/UDP	993
17	AX.25	AX.25	-
18	IPv6	IPv6	-
19	IPSEC_TRANSPORT/TUNNEL	AH	-
20	IPSEC_TUNNEL	ESP	-
21	IRC	TCP/UDP	6667
22	Microsoft RDP	TCP	3389
23	ModBus	TCP	502
24	MSN	TCP	1863
25	MULTICAST	IGMP	-
26	NEWS	TCP	144
27	NetBIOS	TCP/UDP	137, 138, 139, 445
28	NFS	UDP	2049
29	NNTP	TCP	119
30	NTP	TCP/UDP	123
31	POP3	TCP	110
32	POP3S	TCP/UDP	995
33	PPTP	TCP	1723
34	PPTP_TUNNEL	GRE	-

The following table describes the labels in this screen.

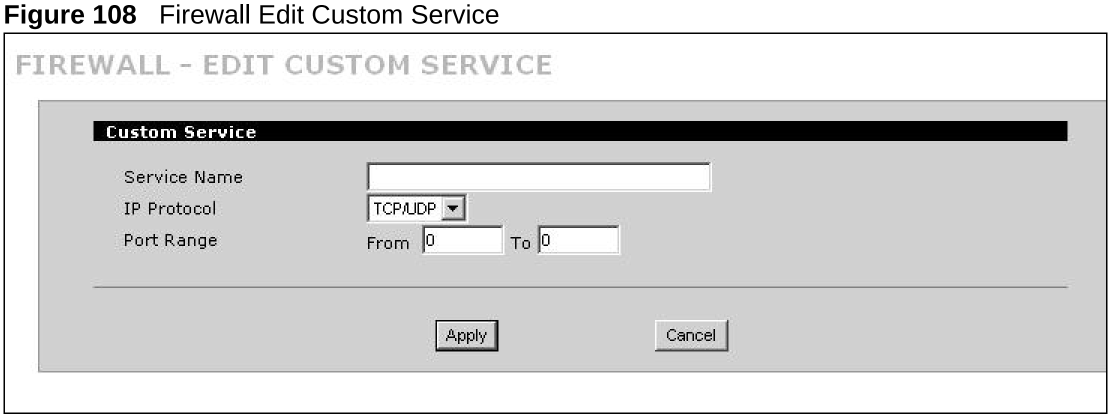
Table 74 SECURITY > FIREWALL > Service

LABEL	DESCRIPTION
Custom Service	This table shows all configured custom services.
#	This is the index number of the custom service.
Service Name	This is the name of the service.
Protocol	This is the IP protocol type. If you selected **Custom**, this is the IP protocol value you entered.
Attribute	This is the IP port number or ICMP type and code that defines the service.
Modify	Click the edit icon to go to the screen where you can edit the service. Click the delete icon to remove an existing service. A window displays asking you to confirm that you want to delete the service. Note that subsequent services move up by one when you take this action.
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.
Predefined Service	This table shows all the services that are already configured for use in firewall rules. See Appendix D on page 613 for a list of common services.
#	This is the index number of the predefined service.
Service Name	This is the name of the service.
Protocol	This is the IP protocol type. There may be more than one IP protocol type.
Attribute	This is the IP port number or ICMP type and code that defines the service.

9.7.1 Firewall Edit Custom Service

Click **SECURITY** > **FIREWALL** > **Service** > **Add** to display the following screen. Use this screen to configure a custom service entry not is not predefined in the LAN-Cell. See Appendix D on page 613 for a list of commonly used services and port numbers.

Figure 108 Firewall Edit Custom Service



The following table describes the labels in this screen.

Table 75 SECURITY > FIREWALL > Service > Add

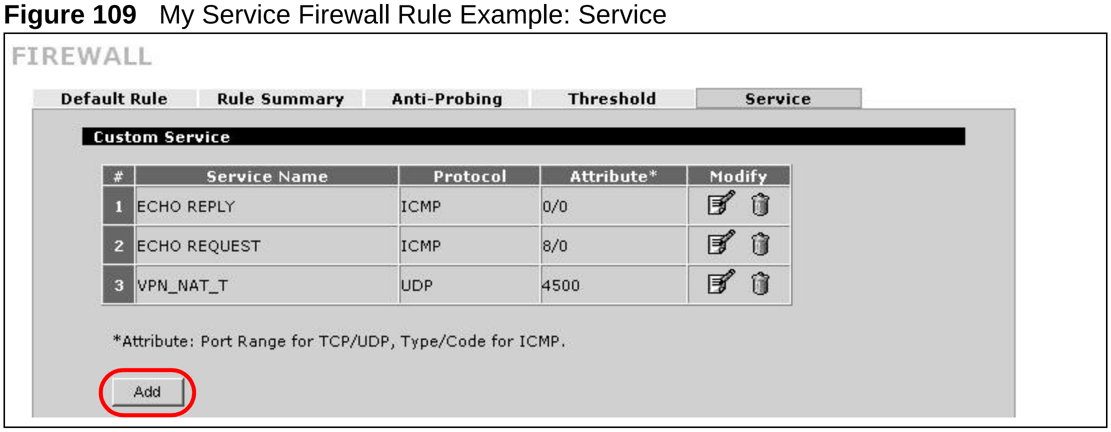
LABEL	DESCRIPTION
Service Name	Enter a descriptive name of up to 31 printable ASCII characters (except Extended ASCII characters) for the custom service. You cannot use the "(" character. Spaces are allowed.
IP Protocol	Choose the IP protocol (**TCP**, **UDP**, **TCP/UDP**, **ICMP** or **Custom**) that defines your customized service from the drop down list box. If you select **Custom**, specify the protocol's number. For example, ICMP is 1, TCP is 6, UDP is 17 and so on.
Port Range	Enter the port number (from 1 to 255) that defines the customized service To specify one port only, enter the port number in the **From** field and enter it again in the **To** field. To specify a span of ports, enter the first port in the **From** field and enter the last port in the **To** field.
Type/Code	This field is available only when you select **ICMP** in the **IP Protocol** field. The ICMP messages are identified by their types and in some cases codes. Enter the type number in the **Type** field and select the **Code** radio button and enter the code number if any.
Apply	Click **Apply** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving.

9.7.2 My Service Firewall Rule Example

The following Internet firewall rule example allows a hypothetical My Service connection from the Internet.

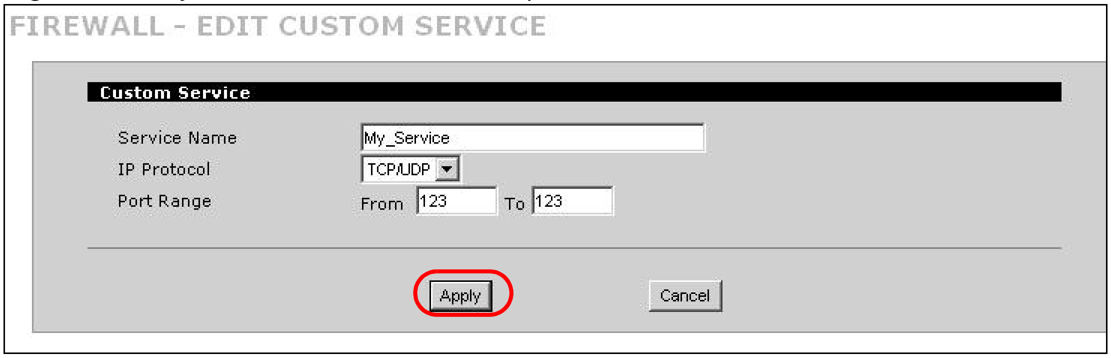
1 In the **Service** screen, click **Add** to open the **Edit Custom Service** screen.

Figure 109 My Service Firewall Rule Example: Service



2 Configure it as follows and click **Apply**.

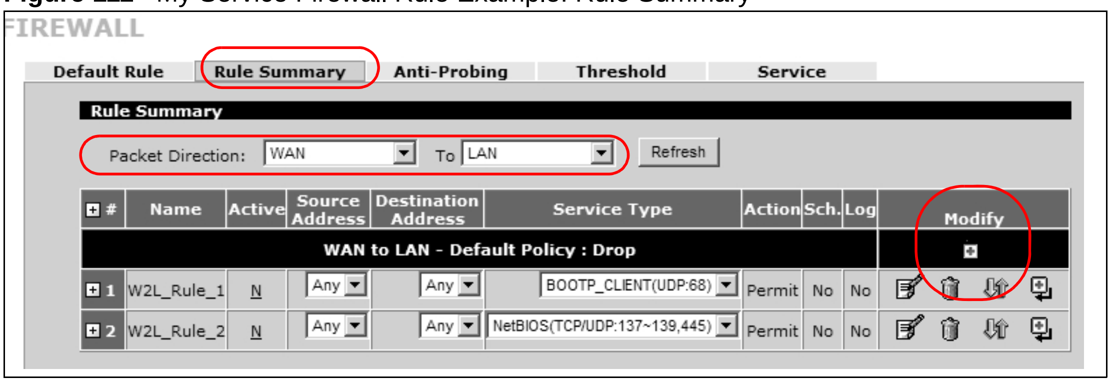
Figure 110 My Service Firewall Rule Example: Edit Custom Service



3 Click **Rule Summary**. Select **WAN to LAN** from the **Packet Direction** drop-down list boxes and click **Refresh**.

4 Click the insert icon (+) at the top of the row (Modify column) to create the new firewall rule before the others.

Figure 111 My Service Firewall Rule Example: Rule Summary

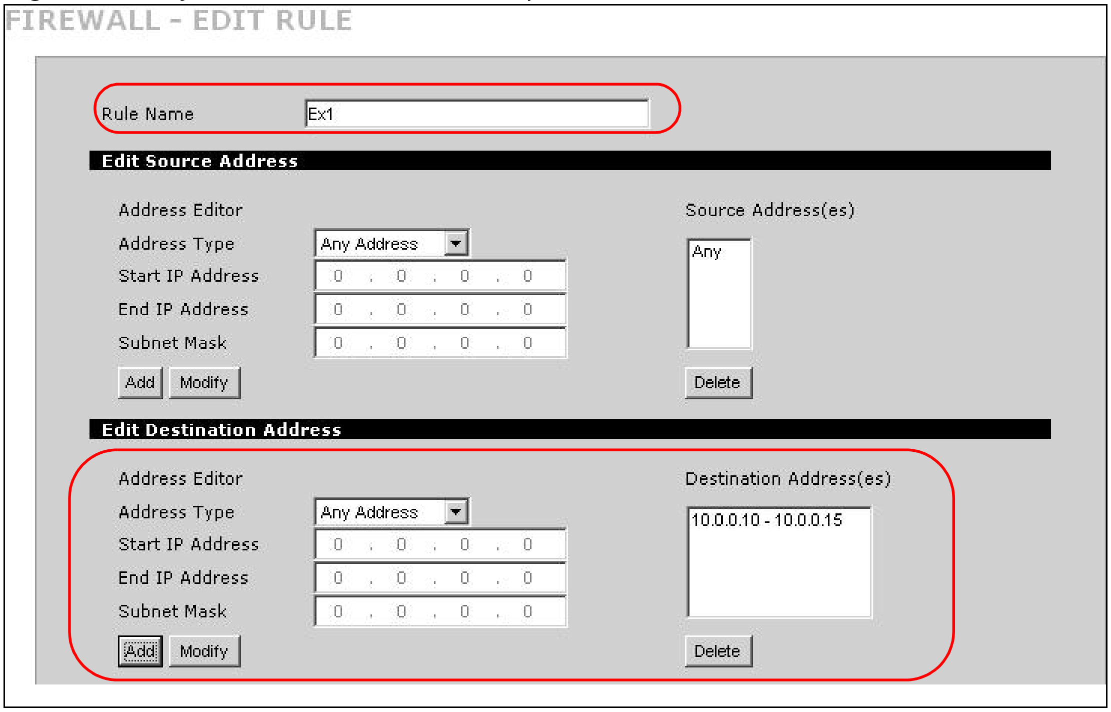


5 The **Edit Rule** screen displays. Enter the name of the firewall rule.

6 Select **Any** in the **Destination Address(es)** box and then click **Delete**.

7 Configure the destination address fields as follows and click **Add**.

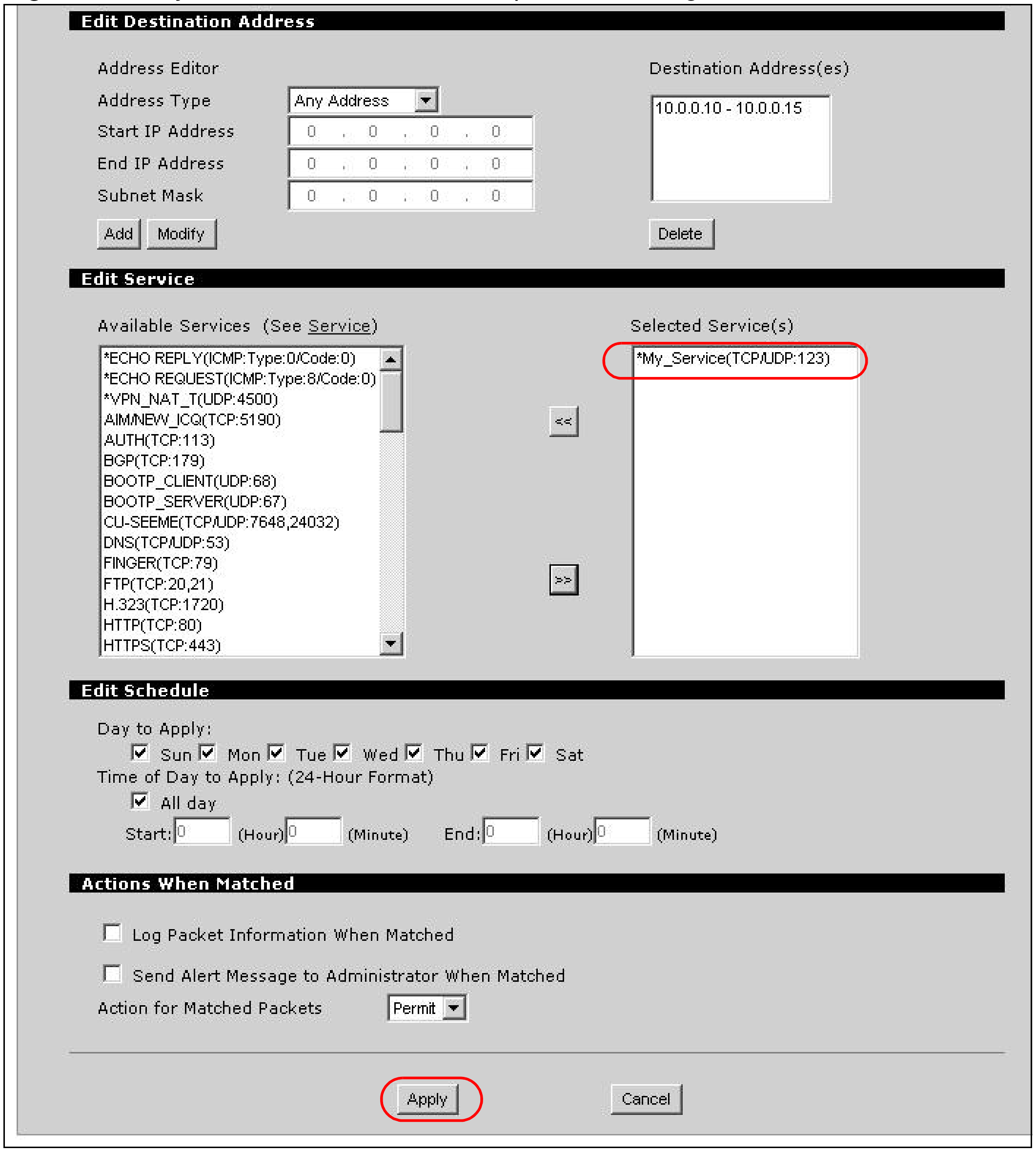
Figure 112 My Service Firewall Rule Example: Rule Edit



8 In the **Edit Rule** screen, use the arrows between **Available Services** and **Selected Service(s)** to configure it as follows. Click **Apply** when you are done.

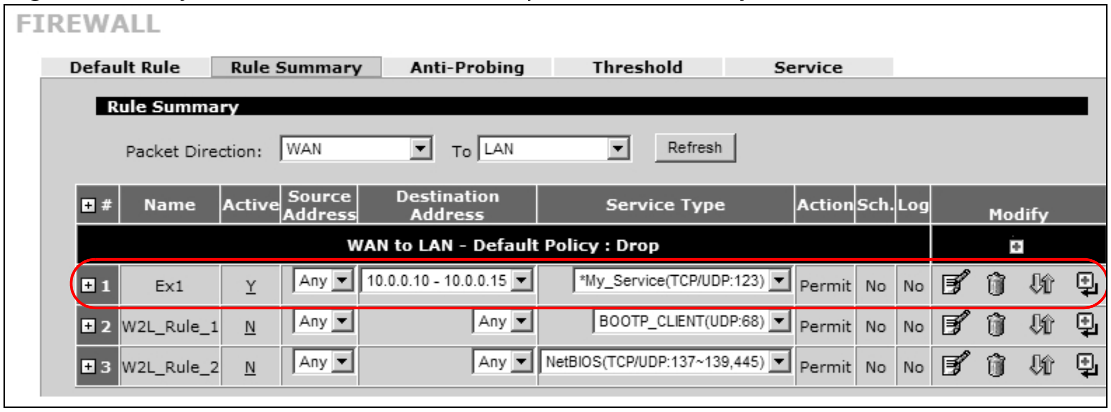
Custom services show up with an * before their names in the **Services** list box and the **Rule Summary** list box.

Figure 113 My Service Firewall Rule Example: Rule Configuration



Rule 1 allows a My Service connection from the WAN to IP addresses 10.0.0.10 through 10.0.0.15 on the LAN.

Figure 114 My Service Firewall Rule Example: Rule Summary



9.8 Firewall Technical Reference

This technical reference contains the the following sections:

- Packet Direction Examples
- Asymmetrical Routes
- DoS Firewall Thresholds
- Security Considerations

Packet Direction Examples

Firewall rules are grouped based on the direction of travel of packets to which they apply. This section gives some examples of why you might configure firewall rules for specific connection directions.

By default, the LAN-Cell allows packets traveling in the following directions:

- LAN to LAN These rules specify which computers on the LAN can manage the LAN-Cell (remote management) and communicate between networks or subnets connected to the LAN interface (IP alias).

You can also configure the remote management settings to allow only a specific computer to manage the LAN-Cell.

- LAN to WAN
- LAN to CELL

These rules specify which computers on the LAN can access which computers or services connected to WAN or CELL interfaces. See Section 9.2 on page 182 for an example.

By default, the LAN-Cell drops packets traveling in the following directions.

- WAN to LAN
- CELL to LAN

These rules specify which computers connected on a remote WAN or CELL connection can access which computers or services on the LAN. For example, you may create rules to:

- Allow certain types of traffic, such as Lotus Notes database synchronization, from specific hosts on the Internet to specific hosts on the LAN.
- Allow public access to a Web server on your protected network. You could also block certain IP addresses from accessing it.

> You also need to configure NAT port forwarding (or full featured NAT address mapping rules) to allow computers on the WAN to access devices on the LAN. See Section 13.4.1 on page 296 for an example.

- WAN to WAN
- CELl to CELL

By default the LAN-Cell stops computers connected to WAN or CELL from using the LAN-Cell as a gateway to communicate with other computers on the WAN. By default, the LAN-Cell does accept traffic from the WAN or CELL interfaces destined for one of the LAN-Cell's default Remote Management ports, to establish a VPN connection, or to pass VPN_NAT and BootP packets.

> If you change the default Remote Management ports, you also need to configure the firewall rules WAN-to-WAN/LAN-Cell and/or CELL-to-CELL/LAN-Cell to allow traffic to flow to the new management ports.

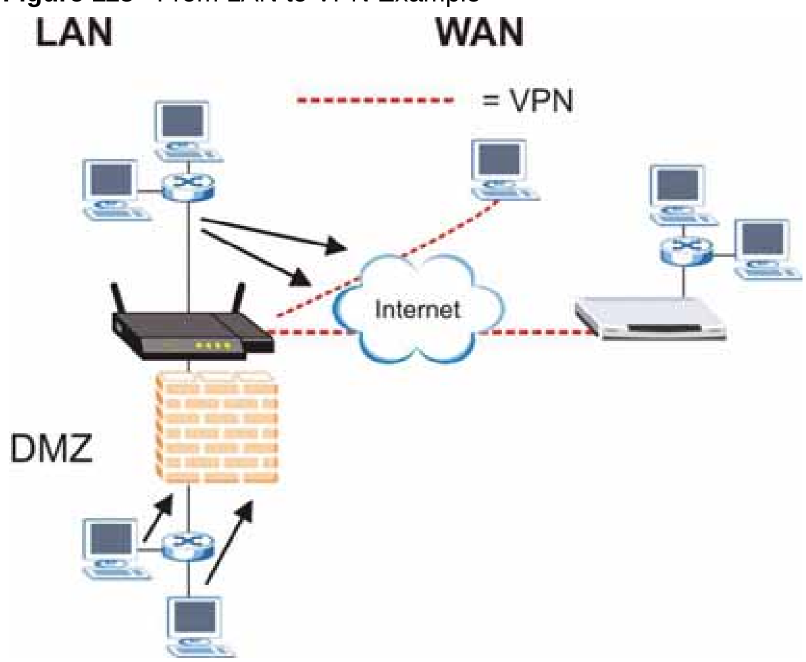
See Chapter 3 on page 53 for information about packets traveling to or from the VPN tunnels.

To VPN Packet Direction

The LAN-Cell can apply firewall rules to traffic before encrypting it to send through a VPN tunnel. **To VPN** means traffic that comes in through the selected "from" interface and goes out through any of the LAN-Cell's VPN tunnels. For example, **From LAN To VPN** specifies the traffic that is coming from the LAN and going out through any of the LAN-Cell's VPN tunnels.

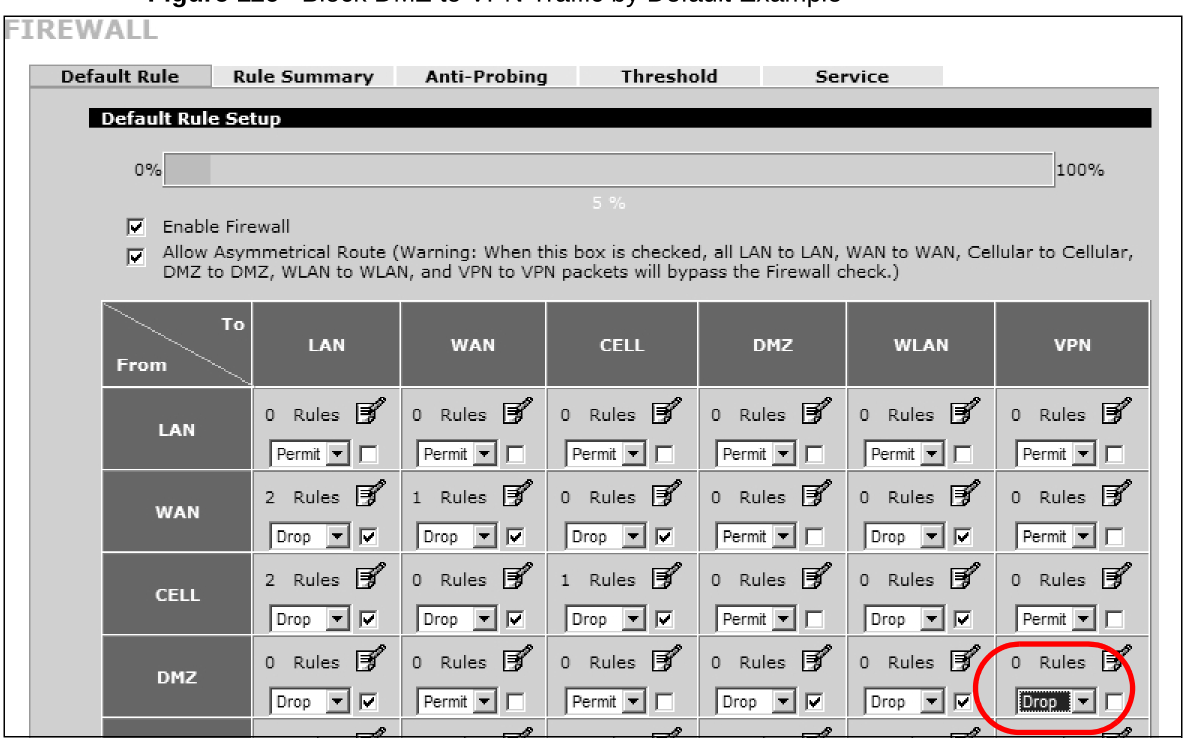
For example, by default the **From LAN To VPN** default firewall rule allows traffic from the LAN computers to go out through any of the LAN-Cell's VPN tunnels. You could configure the **From DMZ To VPN** default rule to set the LAN-Cell to silently block traffic from the DMZ computers from going out through any of the LAN-Cell's VPN tunnels.

Figure 115 From LAN to VPN Example



In order to do this, you would configure the **SECURITY** > **FIREWALL** > **Default Rule** screen as follows.

Figure 116 Block DMZ to VPN Traffic by Default Example

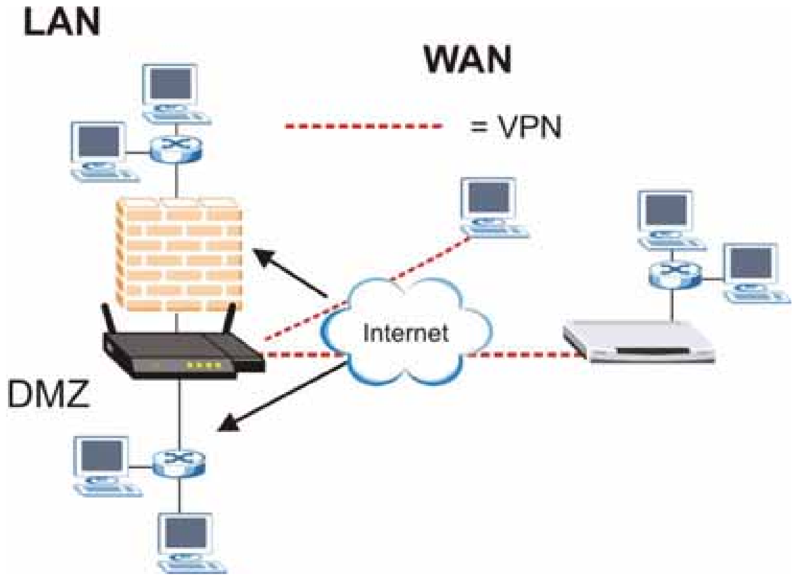


From VPN Packet Direction

You can also apply firewall rules to traffic that comes in through the LAN-Cell's VPN tunnels. The LAN-Cell decrypts the VPN traffic and then applies the firewall rules. **From VPN** means traffic that came into the LAN-Cell through a VPN tunnel and is going to the selected "to" interface.

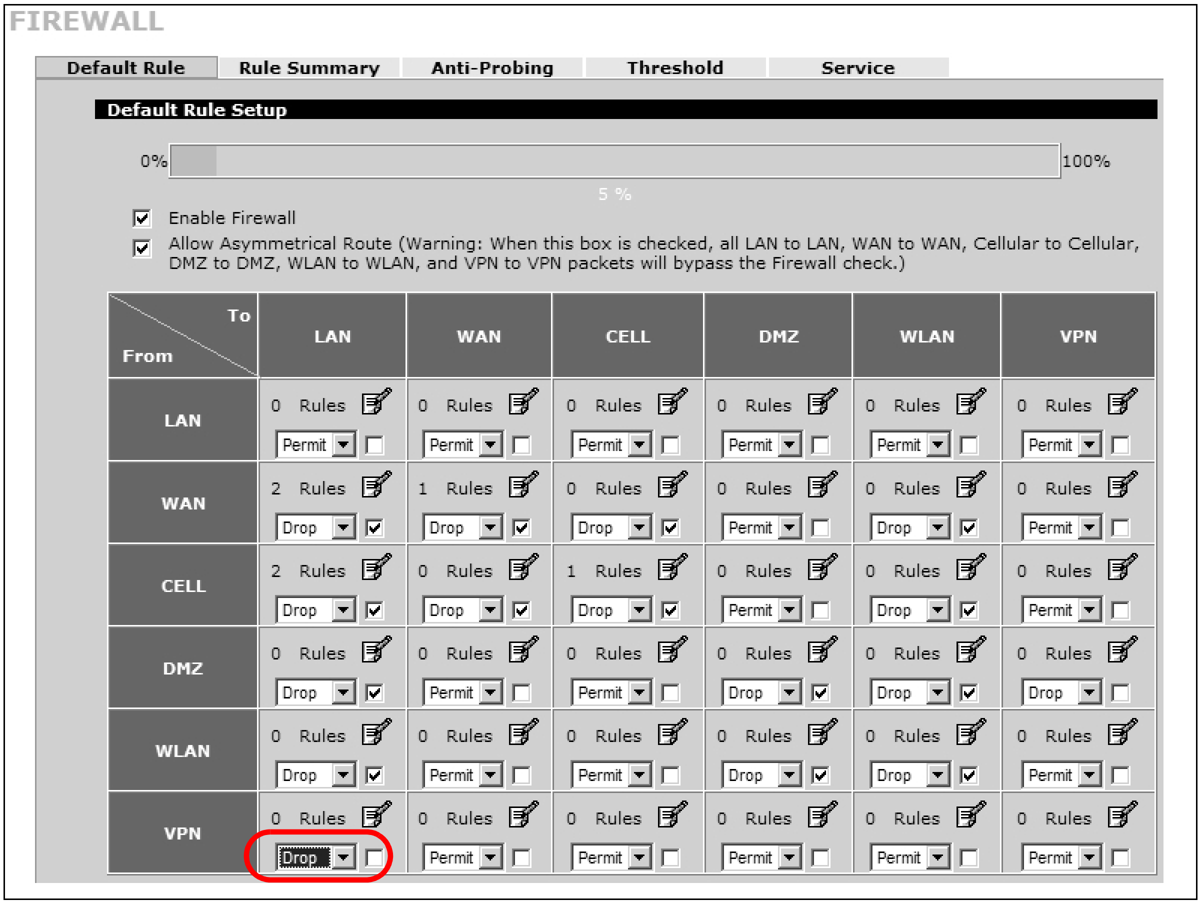
For example, by default the firewall allows traffic from any VPN tunnel to go to any of the LAN-Cell's interfaces, the LAN-Cell itself and other VPN tunnels. You could edit the **From VPN To LAN** default firewall rule to silently block traffic from the VPN tunnels from going to the LAN computers.

Figure 117 From VPN to LAN Example



In order to do this, you would configure the **SECURITY** > **FIREWALL** > **Default Rule** screen as follows.

Figure 118 Block VPN to LAN Traffic by Default Example

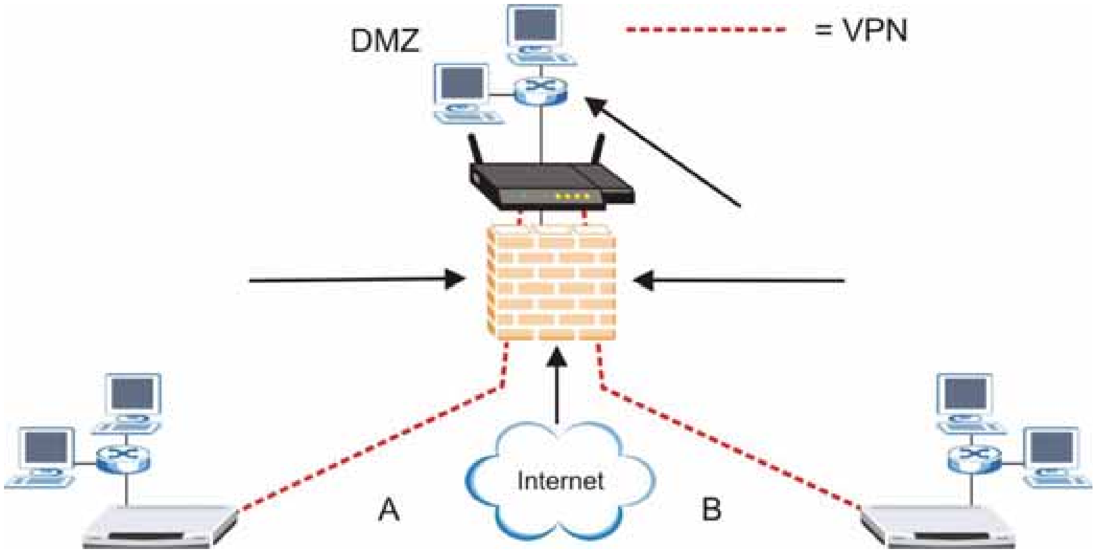


From VPN To VPN Packet Direction

From VPN To VPN firewall rules apply to traffic that comes in through one of the LAN-Cell's VPN tunnels and terminates at the LAN-Cell (like for remote management) or goes out through another of the LAN-Cell's VPN tunnels (this is called hub-and-spoke VPN, see Section 10.9 on page 238 for details). The LAN-Cell decrypts the traffic and applies the firewall rules before re-encrypting it or allowing the traffic to terminate at the LAN-Cell.

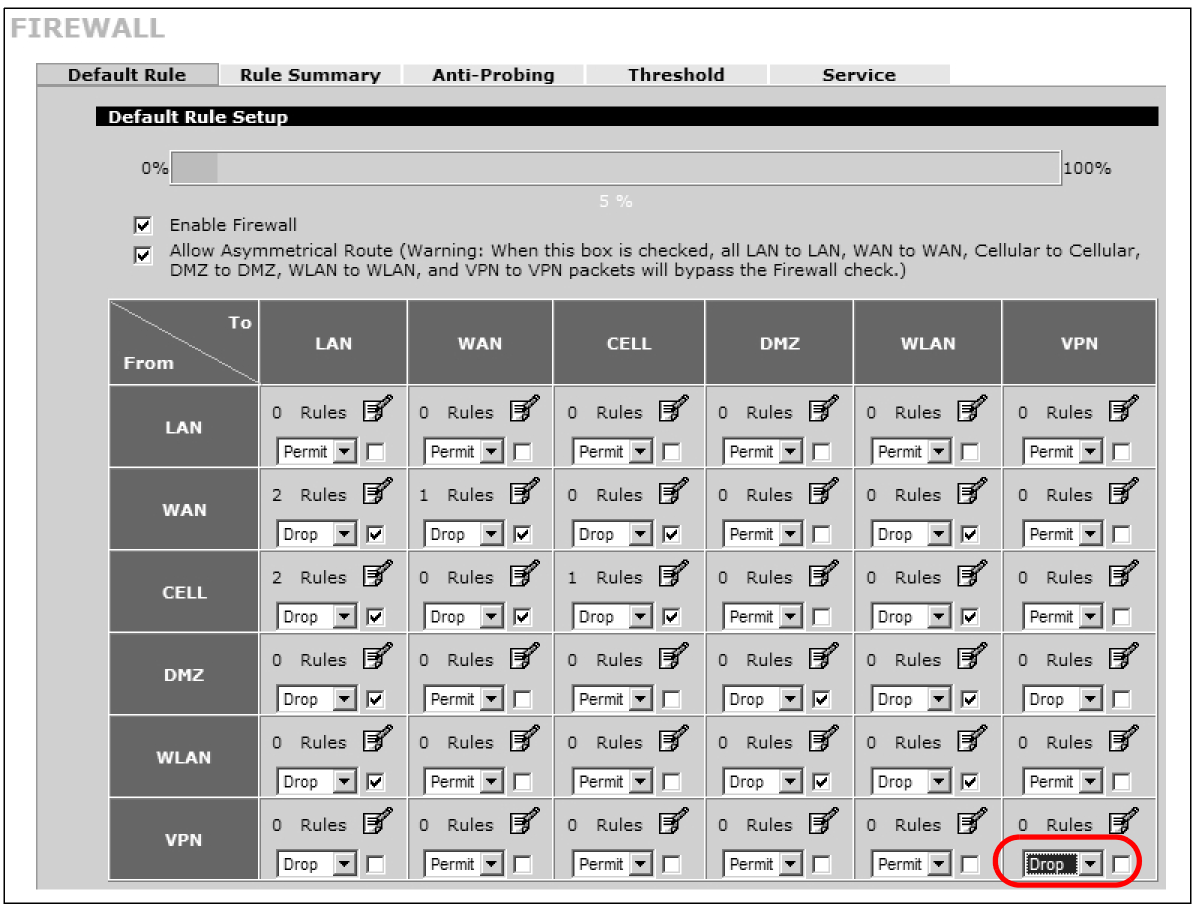
In the following example, the **From VPN To VPN** default firewall rule silently blocks the traffic that the LAN-Cell receives from any VPN tunnel (either A or B) that is destined for the other VPN tunnel or the LAN-Cell itself. VPN traffic destined for the DMZ is allowed through.

Figure 119 From VPN to VPN Example



You would configure the **SECURITY** > **FIREWALL** > **Default Rule** screen as follows.

Figure 120 Block VPN to VPN Traffic by Default Example



From \ To	LAN	WAN	CELL	DMZ	WLAN	VPN
LAN	0 Rules, Permit, ☐	0 Rules, Permit, ☐	0 Rules, Permit, ☐	0 Rules, Permit, ☐	0 Rules, Permit, ☐	0 Rules, Permit, ☐
WAN	2 Rules, Drop, ☑	1 Rules, Drop, ☑	0 Rules, Drop, ☑	0 Rules, Permit, ☐	0 Rules, Drop, ☑	0 Rules, Permit, ☐
CELL	2 Rules, Drop, ☑	0 Rules, Drop, ☑	1 Rules, Drop, ☑	0 Rules, Permit, ☐	0 Rules, Drop, ☑	0 Rules, Permit, ☐
DMZ	0 Rules, Drop, ☑	0 Rules, Permit, ☐	0 Rules, Permit, ☐	0 Rules, Drop, ☑	0 Rules, Drop, ☑	0 Rules, Drop, ☐
WLAN	0 Rules, Drop, ☑	0 Rules, Permit, ☐	0 Rules, Permit, ☐	0 Rules, Drop, ☑	0 Rules, Drop, ☑	0 Rules, Permit, ☐
VPN	0 Rules, Drop, ☐	0 Rules, Permit, ☐	0 Rules, Permit, ☐	0 Rules, Permit, ☐	0 Rules, Permit, ☐	0 Rules, Drop, ☐

Asymmetrical Routes

If an alternate gateway on the LAN has an IP address in the same subnet as the LAN-Cell's LAN IP address, return traffic may not go through the LAN-Cell. This is called an asymmetrical or "triangle" route. This causes the LAN-Cell to reset the connection, as the connection has not been acknowledged.

You can have the LAN-Cell permit the use of asymmetrical route topology on the network (not reset the connection).

Allowing asymmetrical routes may let traffic from the WAN go directly to the LAN without passing through the LAN-Cell. A better solution is to use IP alias to put the LAN-Cell and the backup gateway on separate subnets.

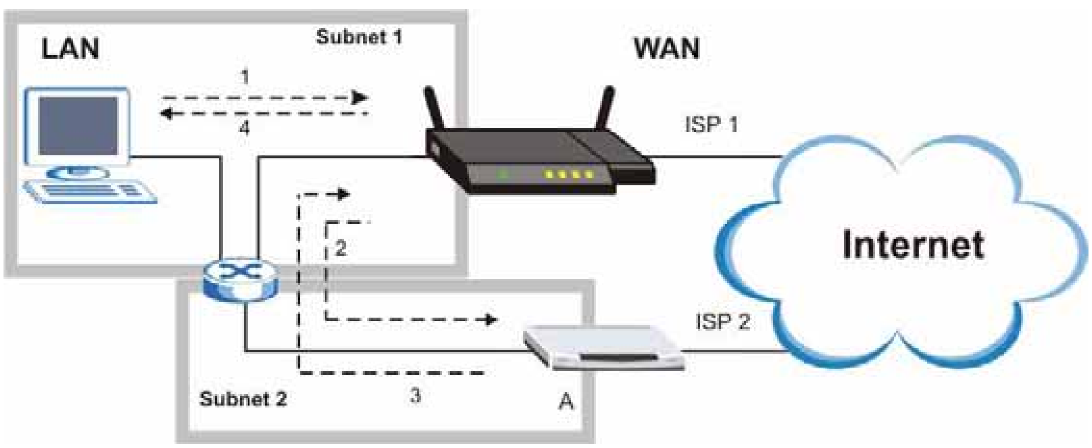
Asymmetrical Routes and IP Alias

You can use IP Alias instead of allowing asymmetrical routes. IP Alias allow you to partition your network into logical sections over the same interface.

By putting your LAN and Gateway **A** in different subnets, all returning network traffic must pass through the LAN-Cell to your LAN. The following steps describe such a scenario.

1. A computer on the LAN initiates a connection by sending a SYN packet to a receiving server on the WAN.
2. The LAN-Cell reroutes the packet to Gateway **A**, which is in **Subnet 2**.
3. The reply from the WAN goes to the LAN-Cell.
4. The LAN-Cell then sends it to the computer on the LAN in **Subnet 1**.

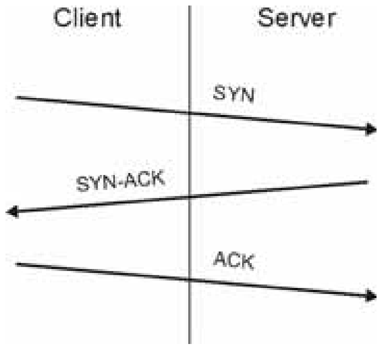
Figure 121 Using IP Alias to Solve the Triangle Route Problem



DoS Firewall Thresholds

For TCP, half-open means that the session has not reached the established state-the TCP three-way handshake has not yet been completed. 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.

Figure 122 Three-Way Handshake



For UDP, half-open means that the firewall has detected no return traffic. An unusually high number (or arrival rate) of half-open sessions could indicate a DoS attack.

Threshold Values

If everything is working properly, you probably do not need to change the threshold settings as the default threshold values should work for most small offices. Tune these parameters when you believe the LAN-Cell has been receiving DoS attacks that are not recorded in the logs or the logs show that the LAN-Cell is classifying normal traffic as DoS attacks. Factors influencing choices for threshold values are:

1 The maximum number of opened sessions.
2 The minimum capacity of server backlog in your LAN network.
3 The CPU power of servers in your LAN network.
4 Network bandwidth.
5 Type of traffic for certain servers.

Reduce the threshold values if your network is slower than average for any of these factors (especially if you have servers that are slow or handle many tasks and are often busy).

If you often use P2P applications such as file sharing with eMule or eDonkey, it’s recommended that you increase the threshold values since lots of sessions will be established during a small period of time and the LAN-Cell may classify them as DoS attacks.

Security Considerations

Incorrectly configuring the firewall may block valid access or introduce security risks to the LAN-Cell and your protected network. Use caution when creating or deleting firewall rules and test your rules after you configure them.

Consider these security ramifications before creating a 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?

10

IPSec VPN Config Screens

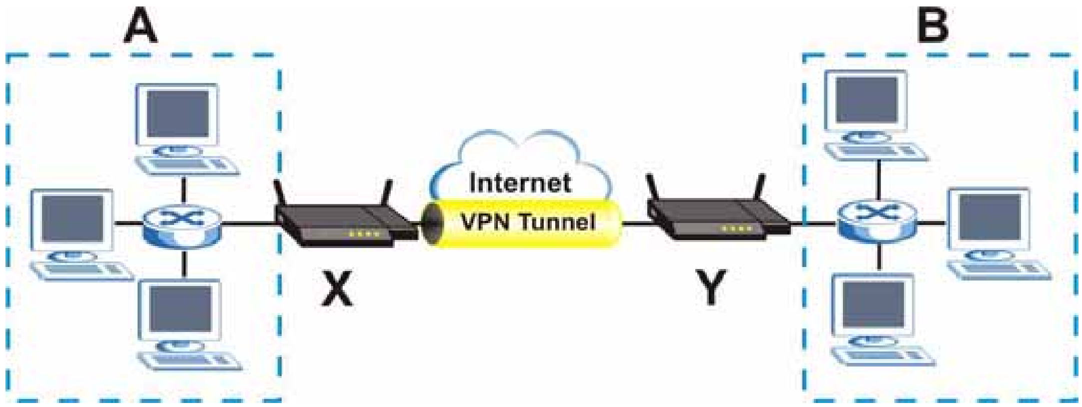
10.1 IPSec VPN Overview

A virtual private network (VPN) 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. It is used to transport traffic over the Internet or any insecure network that uses TCP/IP for communication.

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.

The following figure provides one perspective of a VPN tunnel.

Figure 123 VPN: Example



The VPN tunnel connects the LAN-Cell (**X**) and the remote IPSec router (**Y**). These routers then connect the local network (**A**) and remote network (**B**).

10.1.1 What You Can Do in the IPSec VPN Screens

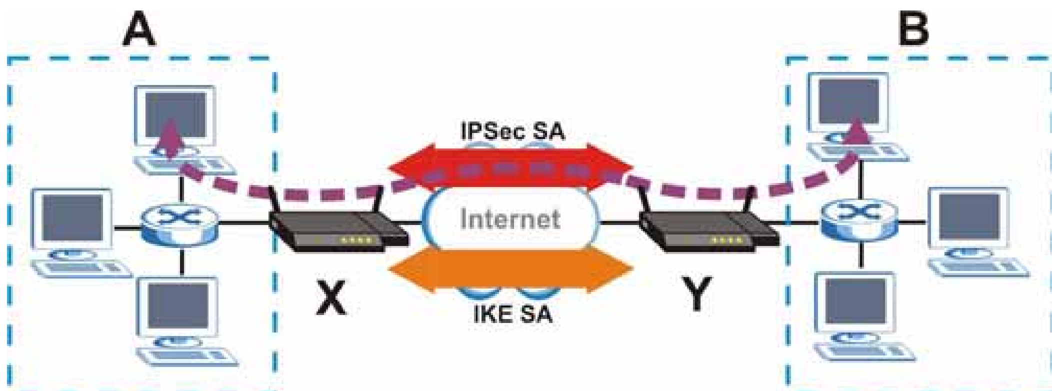
- Use the **VPN Rules (IKE)** screens (see Section 10.2 on page 212) to manage the LAN-Cell's list of VPN rules (tunnels) that use IKE SAs.
- Use the **VPN Rules (Manual)** screens (see Section 10.3 on page 227) to manage the LAN-Cell's list of VPN rules (tunnels) that use manual keys. You may want to configure a VPN rule that uses manual key management if you are having problems with IKE key management.
- Use the **SA Monitor** screen (see Section 10.5 on page 231) to display and manage active VPN connections.

- Use the VPN Global Setting screen (Section 10.6 on page 232) to change settings that apply to all of your VPN tunnels.

10.1.2 What You Need to Know About IPSec VPN

A VPN tunnel is usually established in two phases. Each phase establishes a security association (SA), a contract indicating what security parameters the LAN-Cell and the remote IPSec router will use. The first phase establishes an Internet Key Exchange (IKE) SA between the LAN-Cell and remote IPSec router. The second phase uses the IKE SA to securely establish an IPSec SA through which the LAN-Cell and remote IPSec router can send data between computers on the local network and remote network. The following figure illustrates this.

Figure 124 VPN: IKE SA and IPSec SA



In this example, a computer in network **A** is exchanging data with a computer in network **B**. Inside networks **A** and **B**, the data is transmitted the same way data is normally transmitted in the networks. Between routers **X** and **Y**, the data is protected by tunneling, encryption, authentication, and other security features of the IPSec SA. The IPSec SA is established securely using the IKE SA that routers **X** and **Y** established first.

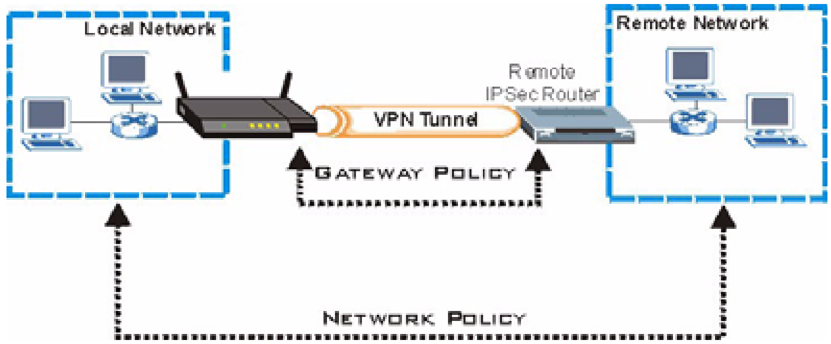
The rest of this section discusses IKE SA and IPSec SA in more detail.

Gateway and Network Policies

A VPN (Virtual Private Network) tunnel gives you a secure connection to another computer or network.

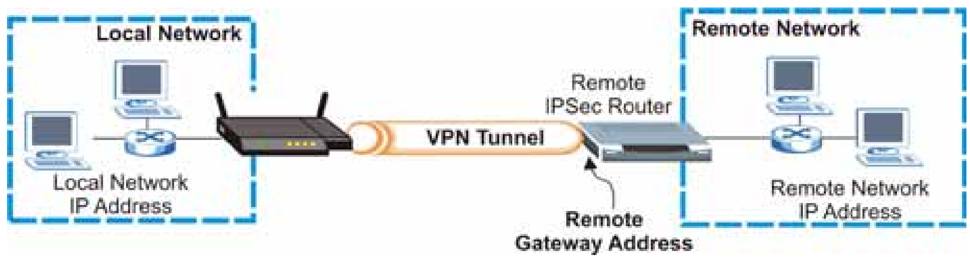
- A gateway policy contains the IKE SA settings. It identifies the IPSec routers at either end of a VPN tunnel.
- A network policy contains the IPSec SA settings. It specifies which devices (behind the IPSec routers) can use the VPN tunnel.

Figure 125 Gateway and Network Policies



This figure helps explain the main fields in the VPN setup.

Figure 126 IPSec Fields Summary



Negotiation Mode

It takes several steps to establish an IKE SA. The negotiation mode determines the number of steps to use. There are two negotiation modes--main mode and aggressive mode. Main mode provides better security, while aggressive mode is faster.

Both routers must use the same negotiation mode.

These modes are discussed in more detail in Section on page 247. Main mode is used in various examples in the rest of this section.

IP Addresses of the LAN-Cell and Remote IPSec Router

In the LAN-Cell, you have to specify the IP addresses of the LAN-Cell and the remote IPSec router to establish an IKE SA.

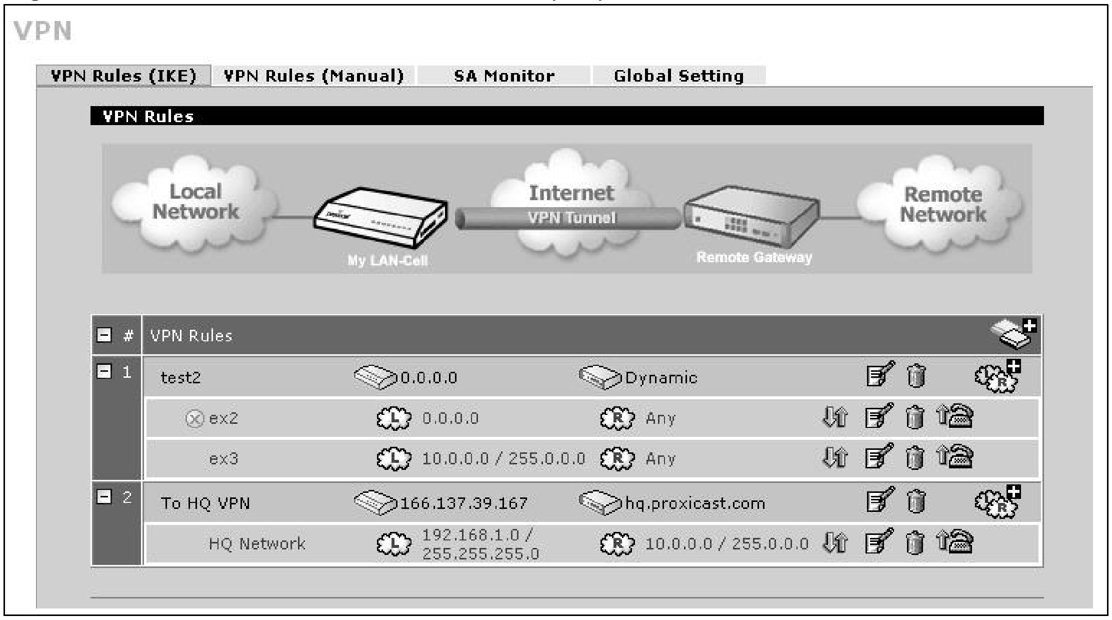
You can usually provide a static IP address or a domain name for the LAN-Cell. Sometimes, your LAN-Cell might also offer another alternative, such as using the IP address of a port or interface.

You can usually provide a static IP address or a domain name for the remote IPSec router as well. Sometimes, you might not know the IP address of the remote IPSec router (for example, telecommuters). In this case, you can still set up the IKE SA, but only the remote IPSec router can initiate an IKE SA.

10.2 VPN Rules (IKE) Screen

Click **SECURITY** > **VPN** to display the **VPN Rules (IKE)** screen. Use this screen to manage the LAN-Cell’s list of VPN rules (tunnels) that use IKE SAs.

Figure 127 SECURITY > VPN > VPN Rules (IKE)



The following table describes the labels in this screen.

Table 76 SECURITY > VPN > VPN Rules (IKE)

LABEL	DESCRIPTION
VPN Rules	These VPN rules define the settings for creating VPN tunnels for secure connection to other computers or networks.
	Click this icon to add a VPN gateway policy (or IPSec rule).
Gateway Policies	The first row of each VPN rule represents the gateway policy. The gateway policy identifies the IPSec routers at either end of a VPN tunnel (**My LAN-Cell** and **Remote Gateway**) and specifies the authentication, encryption and other settings needed to negotiate a phase 1 IKE SA (click the edit icon to display the other settings).
 My LAN-Cell	This represents your LAN-Cell. The WAN IP address, domain name or dynamic domain name of your LAN-Cell.
 Remote Gateway	This represents the remote secure gateway. The IP address, domain name or dynamic domain name of the remote IPSec router displays if you specify it, otherwise **Dynamic** displays.
	Click this icon to add a VPN network policy.
Network Policies	The subsequent rows in a VPN rule are network policies. A network policy identifies the devices behind the IPSec routers at either end of a VPN tunnel and specifies the authentication, encryption and other settings needed to negotiate a phase 2 IPSec SA.
 Local Network	This is the network behind the LAN-Cell. A network policy specifies which devices (behind the IPSec routers) can use the VPN tunnel.

Table 76 SECURITY > VPN > VPN Rules (IKE) (continued)

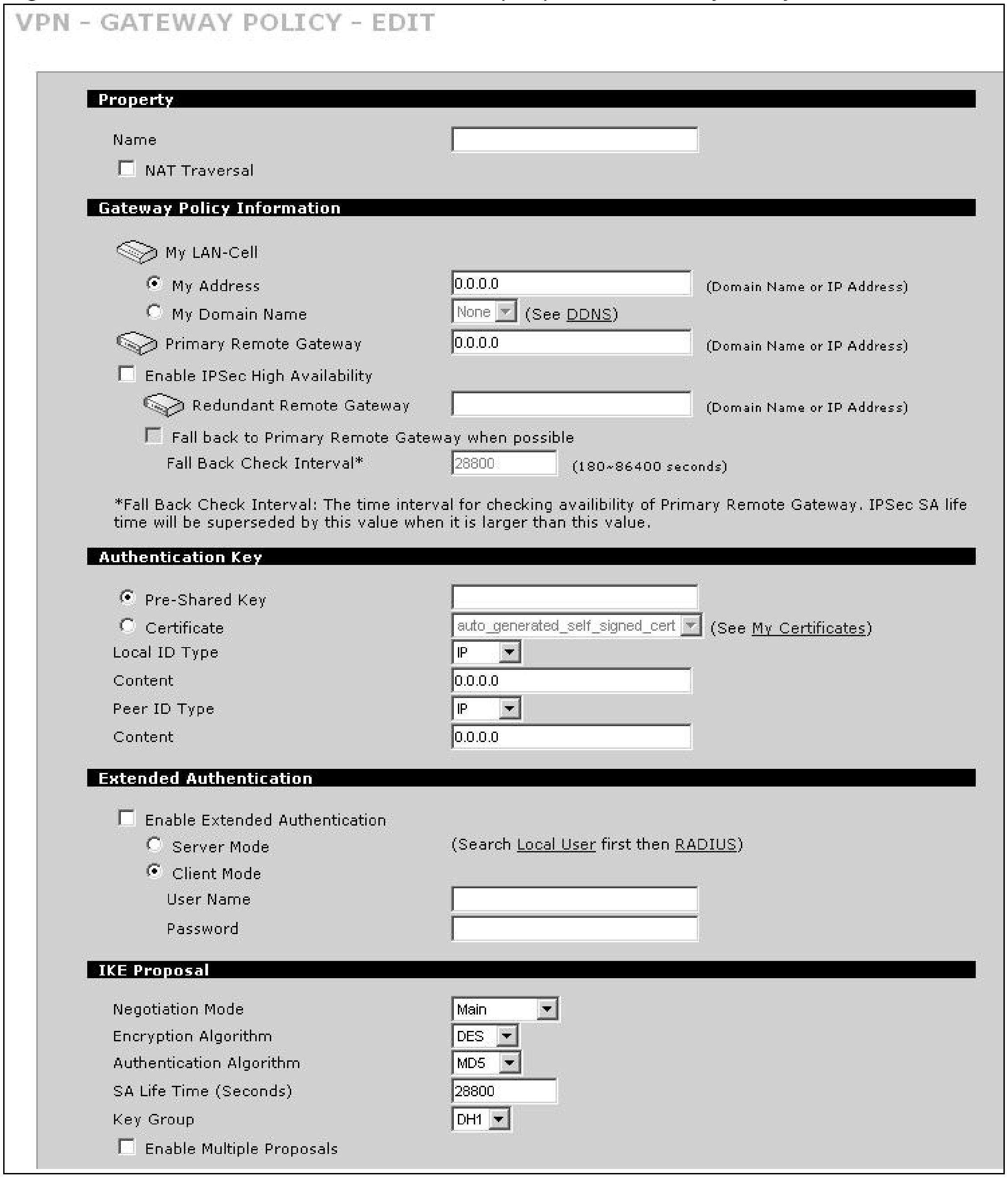
LABEL	DESCRIPTION
 Remote Network	This is the remote network behind the remote IPsec router.
	Click this icon to display a screen in which you can associate a network policy to a gateway policy.
	Click this icon to display a screen in which you can change the settings of a gateway or network policy.
	Click this icon to delete a gateway or network policy. The LAN-Cell automatically moves the associated network policy(ies) to the recycle bin.
	Click this icon to establish a VPN connection to a remote network.
	Click this icon to drop a VPN connection to a remote network.
Y/N	This field displays whether a network policy is turned on (**Y**) or not (**N**). Click the letter to change it to the other state.
Recycle Bin	The recycle bin appears when you have any network policies that are not associated to a gateway policy. When you delete a gateway, the LAN-Cell automatically moves the associated network policy(ies) to the recycle bin. You can also manually move a network policy that you do not need (but may want to use again later) to the recycle bin. Click the network policy's move or edit icon and set it's Gateway Policy to Recycle Bin.

10.2.1 VPN Rules (IKE) Gateway Policy Edit Screen

In the **VPN Rule (IKE)** screen, click the add gateway policy () icon or the edit () icon to display the **VPN-Gateway Policy -Edit** screen.

Use this screen to configure a VPN gateway policy. The gateway policy identifies the IPSec routers at either end of a VPN tunnel (**My LAN-Cell** and **Remote Gateway**) and specifies the authentication, encryption and other settings needed to negotiate a phase 1 IKE SA.

Figure 128 SECURITY > VPN > VPN Rules (IKE) > Edit Gateway Policy



The following table describes the labels in this screen.

Table 77 SECURITY > VPN > VPN Rules (IKE) > Edit Gateway Policy

LABEL	DESCRIPTION
Property	
Name	Type up to 32 characters to identify this VPN gateway policy. You may use any character, including spaces, but the LAN-Cell drops trailing spaces.

Table 77 SECURITY > VPN > VPN Rules (IKE) > Edit Gateway Policy (continued)

LABEL	DESCRIPTION
NAT Traversal	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. Note: The remote IPSec router must also have NAT traversal enabled. See Section on page 248 for more information. 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 ports 500 and 4500 to the IPSec router behind the NAT router.
Gateway Policy Information	
My LAN-Cell	This field identifies the WAN IP address or domain name of the LAN-Cell. You can select **My Address** and enter the LAN-Cell's static WAN IP address (if it has one) or leave the field set to 0.0.0.0. The LAN-Cell uses its current WAN IP address (static or dynamic) in setting up the VPN tunnel if you leave this field as **0.0.0.0**. If the WAN connection goes down, the LAN-Cell uses the dial backup IP address for the VPN tunnel when using dial backup or the LAN IP address when using traffic redirect. Otherwise, you can select **My Domain Name** and choose one of the dynamic domain names that you have configured (in the **DDNS** screen) to have the LAN-Cell use that dynamic domain name's IP address. The VPN tunnel has to be rebuilt if the **My LAN-Cell** IP address changes after setup.
Primary Remote Gateway	Type the WAN IP address or the domain name (up to 31 characters) of the IPSec router with which you're making the VPN connection. Set this field to **0.0.0.0** if the remote IPSec router has a dynamic WAN IP address. In order to have more than one active rule with the **Remote Gateway Address** field set to **0.0.0.0**, the ranges of the local IP addresses cannot overlap between rules. If you configure an active rule with **0.0.0.0** in the **Remote Gateway Address** field and the LAN's full IP address range as the local IP address, then you cannot configure any other active rules with the **Remote Gateway Address** field set to **0.0.0.0**.
Enable IPSec High Availability	Turn on the high availability feature to use a redundant (backup) VPN connection to another WAN interface on the remote IPSec router if the primary (regular) VPN connection goes down. The remote IPSec router must have a second WAN connection in order for you to use this. To use this, you must identify both the primary and the redundant remote IPSec routers by WAN IP address or domain name (you cannot set either to **0.0.0.0**).
Redundant Remote Gateway	Type the WAN IP address or the domain name (up to 31 characters) of the backup IPSec router to use when the LAN-Cell cannot not connect to the primary remote gateway.
Fall back to Primary Remote Gateway when possible	Select this to have the LAN-Cell change back to using the primary remote gateway if the connection becomes available again.
Fall Back Check Interval*	Set how often the LAN-Cell should check the connection to the primary remote gateway while connected to the redundant remote gateway. Each gateway policy uses one or more network policies. If the fall back check interval is shorter than a network policy's SA life time, the fall back check interval is used as the check interval and network policy SA life time. If the fall back check interval is longer than a network policy's SA life time, the SA lifetime is used as the check interval and network policy SA life time.

Table 77 SECURITY > VPN > VPN Rules (IKE) > Edit Gateway Policy (continued)

LABEL	DESCRIPTION
Authentication Key	
Pre-Shared Key	Select the **Pre-Shared Key** radio button and type your pre-shared key in this field. 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. Type from 8 to 31 case-sensitive ASCII characters or from 16 to 62 hexadecimal ("0-9", "A-F") characters. You must precede a hexadecimal key with a "0x (zero x), which is not counted as part of the 16 to 62 character range for the key. For example, in "0x0123456789ABCDEF", 0x denotes that the key is hexadecimal and 0123456789ABCDEF is the key itself. Both ends of the VPN tunnel must use the same pre-shared key. You will receive a PYLD_MALFORMED (payload malformed) packet if the same pre-shared key is not used on both ends.
Certificate	Select the **Certificate** radio button to identify the LAN-Cell by a certificate. Use the drop-down list box to select the certificate to use for this VPN tunnel. You must have certificates already configured in the **My Certificates** screen. Click **My Certificates** to go to the **My Certificates** screen where you can view the LAN-Cell's list of certificates.
Local ID Type	Select **IP** to identify this LAN-Cell by its IP address. Select **DNS** to identify this LAN-Cell by a domain name. Select **E-mail** to identify this LAN-Cell by an e-mail address. You do not configure the local ID type and content when you set **Authentication Key** to **Certificate**. The LAN-Cell takes them from the certificate you select.
Content	When you select **IP** in the **Local ID Type** field, type the IP address of your computer in the local **Content** field. The LAN-Cell automatically uses the IP address in the **My LAN-Cell** field (refer to the **My** LAN-Cell field description) 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. 1. When there is a NAT router between the two IPSec routers. 2. 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. When you select **DNS** or **E-mail** in the **Local ID Type** field, type a domain name or e-mail address by which to identify this LAN-Cell in the local **Content** field. 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.
Peer ID Type	Select from the following when you set **Authentication Key** to **Pre-shared Key**. Select **IP** to identify the remote IPSec router by its IP address. Select **DNS** to identify the remote IPSec router by a domain name. Select **E-mail** to identify the remote IPSec router by an e-mail address. Select from the following when you set **Authentication Key** to **Certificate**. Select **IP** to identify the remote IPSec router by the IP address in the subject alternative name field of the certificate it uses for this VPN connection. Select **DNS** to identify the remote IPSec router by the domain name in the subject alternative name field of the certificate it uses for this VPN connection. Select **E-mail** to identify the remote IPSec router by the e-mail address in the subject alternative name field of the certificate it uses for this VPN connection. Select **Subject Name** to identify the remote IPSec router by the subject name of the certificate it uses for this VPN connection. Select **Any** to have the LAN-Cell not check the remote IPSec router's ID.

Table 77 SECURITY > VPN > VPN Rules (IKE) > Edit Gateway Policy (continued)

LABEL	DESCRIPTION
Content	The configuration of the peer content depends on the peer ID type. Do the following when you set **Authentication Key** to **Pre-shared Key**. For **IP**, type the IP address of the computer with which you will make the VPN connection. If you configure this field to **0.0.0.0** or leave it blank, the LAN-Cell will use the address in the **Remote Gateway Address** field (refer to the **Remote Gateway Address** field description). For **DNS** or **E-mail**, type a domain name or e-mail address by which to identify the remote IPSec router. 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. It is recommended that you type an IP address other than **0.0.0.0** or use the **DNS** or **E-mail** ID type in the following situations: 1. When there is a NAT router between the two IPSec routers. 2. When you want the LAN-Cell to distinguish between VPN connection requests that come in from remote IPSec routers with dynamic WAN IP addresses. Do the following when you set **Authentication Key** to **Certificate**. 1. For **IP**, type the IP address from the subject alternative name field of the certificate the remote IPSec router will use for this VPN connection. If you configure this field to **0.0.0.0** or leave it blank, the LAN-Cell will use the address in the **Remote Gateway Address** field (refer to the **Remote Gateway Address** field description). 2. For **DNS** or **E-mail**, type the domain name or e-mail address from the subject alternative name field of the certificate the remote IPSec router will use for this VPN connection. 3. For **Subject Name**, type the subject name of the certificate the remote IPSec router will use for this VPN connection. Use up to255 ASCII characters including spaces. 4. For **Any**, the peer **Content** field is not available. 5. Regardless of how you configure the **ID Type** and **Content** fields, two active IPSec SAs cannot have both the local and remote IP address ranges overlap between rules.
Extended Authentication	
Enable Extended Authentication	Select this check box to activate extended authentication.
Server Mode	Select **Server Mode** to have this LAN-Cell authenticate extended authentication clients that request this VPN connection. You must also configure the extended authentication clients' usernames and passwords in the authentication server's local user database or a RADIUS server (see Chapter 12 on page 283). Click **Local User** to go to the **Local User Database** screen where you can view and/or edit the list of user names and passwords. Click **RADIUS** to go to the **RADIUS** screen where you can configure the LAN-Cell to check an external RADIUS server. During authentication, if the LAN-Cell (in server mode) does not find the extended authentication clients' user name in its internal user database and an external RADIUS server has been enabled, it attempts to authenticate the client through the RADIUS server.
Client Mode	Select **Client Mode** to have your LAN-Cell use a username and password when initiating this VPN connection to the extended authentication server LAN-Cell. Only a VPN extended authentication client can initiate this VPN connection.
User Name	Enter a user name for your LAN-Cell to be authenticated by the VPN peer (in server mode). The user name can be up to 31 case-sensitive ASCII characters, but spaces are not allowed. You must enter a user name and password when you select client mode.

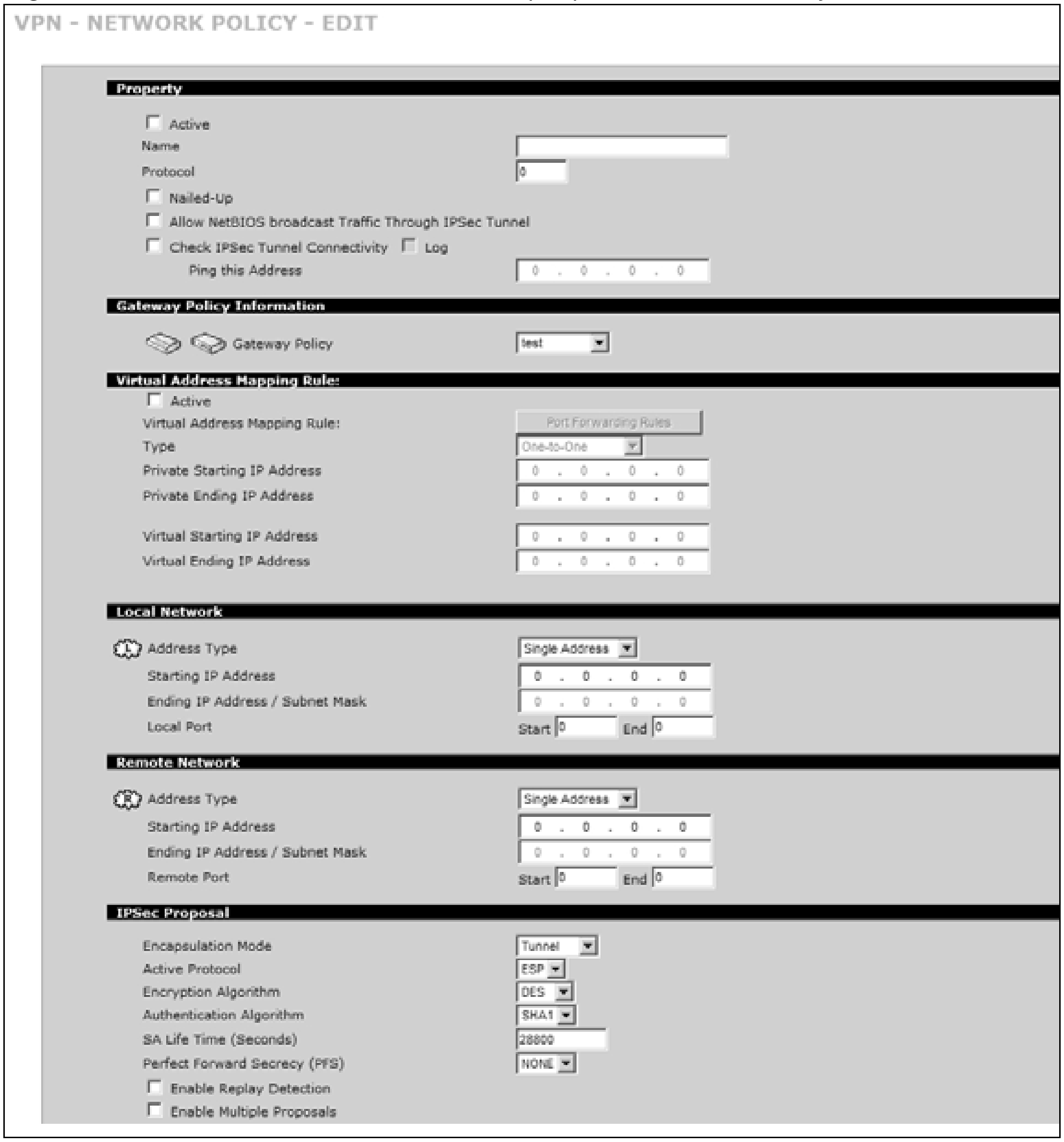
Table 77 SECURITY > VPN > VPN Rules (IKE) > Edit Gateway Policy (continued)

LABEL	DESCRIPTION
Password	Enter the corresponding password for the above user name. The password can be up to 31 case-sensitive ASCII characters, but spaces are not allowed.
IKE Proposal	
Negotiation Mode	Select **Main** or **Aggressive** from the drop-down list box. Multiple SAs connecting through a secure gateway must have the same negotiation mode.
Encryption Algorithm	Select which key size and encryption algorithm to use in the IKE SA. Choices are: DES - a 56-bit key with the DES encryption algorithm 3DES - a 168-bit key with the DES encryption algorithm AES - a 128-bit key with the AES encryption algorithm The LAN-Cell and the remote IPSec router must use the same algorithms and keys. Longer keys require more processing power, resulting in increased latency and decreased throughput.
Authentication Algorithm	Select which hash algorithm to use to authenticate packet data in the IKE SA. Choices are **SHA1** and **MD5**. **SHA1** is generally considered stronger than **MD5**, but it is also slower.
SA Life Time (Seconds)	Define the length of time before an IKE SA automatically renegotiates in this field. It may range from 180 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	Select which Diffie-Hellman key group (DH*x*) you want to use for encryption keys. Choices are: **DH1** - use a 768-bit random number **DH2** - use a 1024-bit random number
Enable Multiple Proposals	Select this to allow the LAN-Cell to use any of its phase 1 key groups and encryption and authentication algorithms when negotiating an IKE SA. When you enable multiple proposals, the LAN-Cell allows the remote IPSec router to select which phase 1 key groups and encryption and authentication algorithms to use for the IKE SA, even if they are less secure than the ones you configure for the VPN rule. Clear this to have the LAN-Cell use only the configured phase 1 key groups and encryption and authentication algorithms when negotiating an IKE SA.
Associated Network Policies	The following table shows the policy(ies) you configure for this rule. To add a VPN policy, click the add network policy ( ) icon in the **VPN Rules (IKE)** screen (see Figure 127 on page 212). Refer to Section 10.2.2 on page 219 for more information.
#	This field displays the policy index number.
Name	This field displays the policy name.
Local Network	This field displays one or a range of IP address(es) of the computer(s) behind the LAN-Cell.
Remote Network	This field displays one or a range of IP address(es) of the remote network behind the remote IPsec router.
Apply	Click **Apply** to save your changes back to the LAN-Cell.
Cancel	Click **Cancel** to exit this screen without saving.

10.2.2 VPN Rules (IKE): Network Policy Edit

Click **SECURITY** > **VPN** and the add network policy ( ) icon in the **VPN Rules (IKE)** screen to display the **VPN-Network Policy -Edit** screen. Use this screen to configure a network policy. A network policy identifies the devices behind the IPSec routers at either end of a VPN tunnel and specifies the authentication, encryption and other settings needed to negotiate a phase 2 IPSec SA.

Figure 129 SECURITY > VPN > VPN Rules (IKE) > Edit Network Policy



The following table describes the labels in this screen.

Table 78 SECURITY > VPN > VPN Rules (IKE) > Edit Network Policy

LABEL	DESCRIPTION
Active	If the **Active** check box is selected, packets for the tunnel trigger the LAN-Cell to build the tunnel. Clear the **Active** check box to turn the network policy off. The LAN-Cell does not apply the policy. Packets for the tunnel do not trigger the tunnel. If you clear the **Active** check box while the tunnel is up (and click **Apply**), you turn off the network policy and the tunnel goes down.
Name	Type a name to identify this VPN network policy. You may use any character, including spaces, but the LAN-Cell drops trailing spaces.
Protocol	Enter 1 for ICMP, 6 for TCP, 17 for UDP, etc. 0 is the default and signifies any protocol.
Nailed-Up	Select this check box to turn on the nailed up feature for this SA. Turn on nailed up to have the LAN-Cell automatically reinitiate the SA after the SA lifetime times out, even if there is no traffic. The LAN-Cell also reinitiates the SA when it restarts. The LAN-Cell also rebuilds the tunnel if it was disconnected due to the output or input idle timer.
Allow NetBIOS Traffic Through IPSec Tunnel	NetBIOS (Network Basic Input/Output System) are TCP or UDP packets that enable a computer to connect to and communicate with a LAN. 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 this check box to send NetBIOS packets through the VPN connection.
Check IPSec Tunnel Connectivity	Select the check box and configure an IP address in the **Ping this Address** field to have the LAN-Cell periodically test the VPN tunnel to the remote IPSec router. The LAN-Cell pings the IP address every minute. The LAN-Cell starts the IPSec connection idle timeout timer when it sends the ping packet. If there is no traffic from the remote IPSec router by the time the timeout period expires, the LAN-Cell disconnects the VPN tunnel.
Log	Select this check box to set the LAN-Cell to create logs when it cannot ping the remote device.
Ping this Address	If you select **Check IPSec Tunnel Connectivity**, enter the IP address of a computer at the remote IPSec network. The computer's IP address must be in this IP policy's remote range (see the **Remote Network** fields).
Gateway Policy Information	
Gateway Policy	Select the gateway policy with which you want to use the VPN policy.
Virtual Address Mapping Rule	
Active	Enable this feature to have the LAN-Cell use virtual (translated) IP addresses for the local network for the VPN connection. You do not configure the Local Network fields when you enable virtual address mapping. Virtual address mapping allows local and remote networks to have overlapping IP addresses. Virtual address mapping (NAT over IPSec) translates the source IP addresses of computers on your local network to other (virtual) IP addresses before sending the packets to the remote IPSec router. This translation hides the source IP addresses of computers in the local network.
Port Forwarding Rules	If you are configuring a **Many-to-One** rule, click this button to go to a screen where you can configure port forwarding for your VPN tunnels. The VPN network policy port forwarding rules let the LAN-Cell forward traffic coming in through the VPN tunnel to the appropriate IP address.

Table 78 SECURITY > VPN > VPN Rules (IKE) > Edit Network Policy (continued)

LABEL	DESCRIPTION
Type	Select **One-to-One** to translate a single (static) IP address on your LAN to a single virtual IP address. Select **Many-to-One** to translate a range of (static) IP addresses on your LAN to a single virtual IP address. Many-to-one rules are for traffic going out from your LAN, through the VPN tunnel, to the remote network. Use port forwarding rules to allow incoming traffic from the remote network. Select **Many One-to-One** to translate a range of (static) IP addresses on your LAN to a range of virtual IP addresses.
Private Starting IP Address	Specify the IP addresses of the devices behind the LAN-Cell that can use the VPN tunnel. When you select **One-to-One** in the Type field, enter the (static) IP address of a computer on the LAN behind your LAN-Cell. When you select **Many-to-One** or **Many One-to-One** in the Type field, enter the beginning (static) IP address in a range of computers on the LAN behind your LAN-Cell.
Private Ending IP Address	When you select **Many-to-One** or **Many One-to-One** in the Type field, enter the ending (static) IP address in a range of computers on the LAN behind your LAN-Cell.
Virtual Starting IP Address	Enter the (static) IP addresses that represent the translated private IP addresses. These must correspond to the remote IPSec router's configured remote IP addresses. When you select **One-to-One** or **Many-to-One** in the Type field, enter an IP address as the translated IP address. Many-to-one rules are only for traffic going to the remote network. Use port forwarding rules to allow incoming traffic from the remote network. When you select **Many One-to-One** in the Type field, enter the beginning IP address of a range of translated IP addresses.
Virtual Ending IP Address	When you select **Many One-to-One** in the Type field, enter the ending (static) IP address of a range of translated IP addresses. The size of the private address range must be equal to the size of the translated virtual address range.
Local Network	
Local Network	Local 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.
Address Type	Use the drop-down list box to choose **Single Address**, **Range Address**, or **Subnet Address**. Select **Single Address** for a single IP address. Select **Range Address** for a specific range of IP addresses. Select **Subnet Address** to specify IP addresses on a network by their subnet mask.
Starting IP Address	When the **Address Type** field is configured to **Single Address**, enter a (static) IP address on the LAN behind your LAN-Cell. When the **Address Type** field is configured to **Range Address**, enter the beginning (static) IP address, in a range of computers on the LAN behind your LAN-Cell. When the **Address Type** field is configured to **Subnet Address**, this is a (static) IP address on the LAN behind your LAN-Cell.
Ending IP Address/ Subnet Mask	When the **Address Type** field is configured to **Single Address**, this field is N/A. When the **Address Type** field is configured to **Range Address**, enter the end (static) IP address, in a range of computers on the LAN behind your LAN-Cell. When the **Address Type** field is configured to **Subnet Address**, this is a subnet mask on the LAN behind your LAN-Cell.

Table 78 SECURITY > VPN > VPN Rules (IKE) > Edit Network Policy (continued)

LABEL	DESCRIPTION
Local Port	0 is the default and signifies any port. Type a port number from 0 to 65535 in the **Start** and **End** fields. Some of the most common IP ports are: 21, FTP; 53, DNS; 23, Telnet; 80, HTTP; 25, SMTP; 110, POP3.
Remote Network	
Remote Network	Remote IP addresses must be static and correspond to the remote IPSec router's configured local 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.
Address Type	Use the drop-down list box to choose **Single Address**, **Range Address**, or **Subnet Address**. Select **Single Address** with a single IP address. Select **Range Address** for a specific range of IP addresses. Select **Subnet Address** to specify IP addresses on a network by their subnet mask.
Starting IP Address	When the **Address Type** field is configured to **Single Address**, enter a (static) IP address on the network behind the remote IPSec router. When the Addr Type field is configured to **Range Address**, enter the beginning (static) IP address, in a range of computers on the network behind the remote IPSec router. When the **Address Type** field is configured to **Subnet Address**, enter a (static) IP address on the network behind the remote IPSec router.
Ending IP Address/ Subnet Mask	When the **Address Type** field is configured to **Single Address**, this field is N/A. When the **Address Type** field is configured to **Range Address**, enter the end (static) IP address, in a range of computers on the network behind the remote IPSec router. When the **Address Type** field is configured to **Subnet Address**, enter a subnet mask on the network behind the remote IPSec router.
Remote Port	0 is the default and signifies any port. Type a port number from 0 to 65535 in the **Start** and **End** fields. Some of the most common IP ports are: 21, FTP; 53, DNS; 23, Telnet; 80, HTTP; 25, SMTP; 110, POP3.
IPSec Proposal	
Encapsulation Mode	Select **Tunnel** mode or **Transport** mode.
Active Protocol	Select the security protocols used for an SA. Both **AH** and **ESP** increase processing requirements and communications latency (delay).
Encryption Algorithm	Select which key size and encryption algorithm to use in the IKE SA. Choices are: **NULL** - no encryption key or algorithm **DES** - a 56-bit key with the DES encryption algorithm **3DES** - a 168-bit key with the DES encryption algorithm **AES** - a 128-bit key with the AES encryption algorithm The LAN-Cell and the remote IPSec router must use the same algorithms and keys. Longer keys require more processing power, resulting in increased latency and decreased throughput.
Authentication Algorithm	Select which hash algorithm to use to authenticate packet data in the IPSec SA. Choices are **SHA1** and **MD5**. **SHA1** is generally considered stronger than **MD5**, but it is also slower.
SA Life Time (Seconds)	Define the length of time before an IPSec SA automatically renegotiates in this field. The minimum value is 180 seconds. 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.

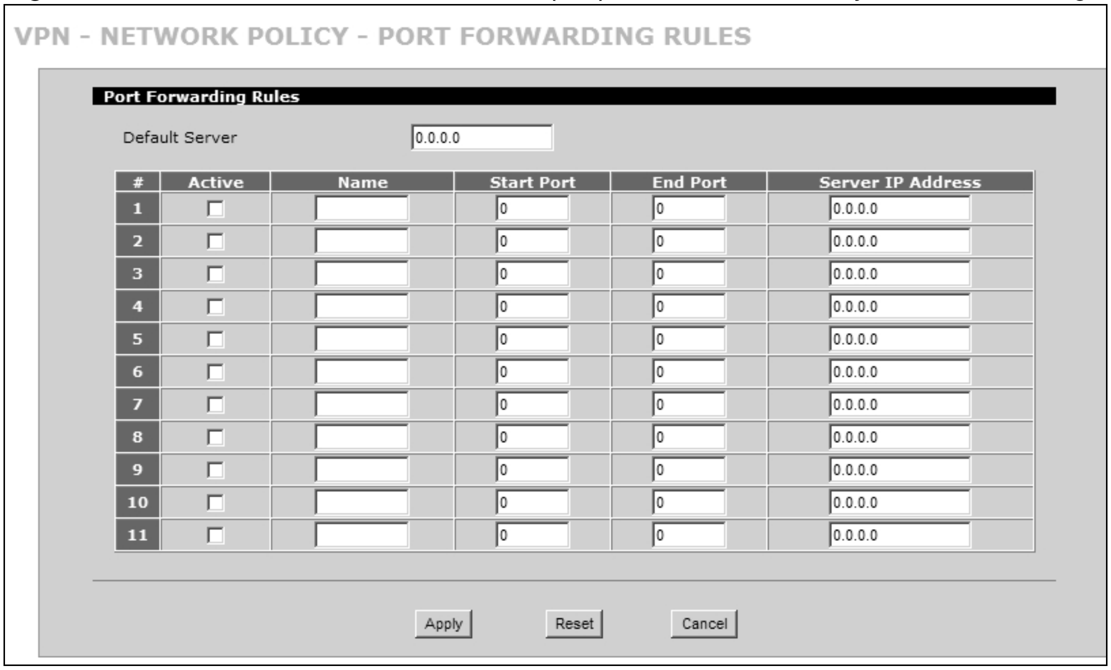
Table 78 SECURITY > VPN > VPN Rules (IKE) > Edit Network Policy (continued)

LABEL	DESCRIPTION
Perfect Forward Secret (PFS)	Select whether or not you want to enable Perfect Forward Secrecy (PFS) and, if you do, which Diffie-Hellman key group to use for encryption. Choices are: **NONE** - disable PFS **DH1** - enable PFS and use a 768-bit random number **DH2** - enable PFS and use a 1024-bit random number PFS changes the root key that is used to generate encryption keys for each IPSec SA. It is more secure but takes more time.
Enable Replay Detection	As a VPN setup is processing intensive, the system is vulnerable to Denial of Service (DOS) attacks. The IPSec receiver can detect and reject old or duplicate packets to protect against replay attacks. Enable replay detection by selecting this check box.
Enable Multiple Proposals	Select this to allow the LAN-Cell to use any of its phase 2 encryption and authentication algorithms when negotiating an IPSec SA. When you enable multiple proposals, the LAN-Cell allows the remote IPSec router to select which phase 2 encryption and authentication algorithms to use for the IPSec SA, even if they are less secure than the ones you configure for the VPN rule. Clear this to have the LAN-Cell use only the configured phase 2 encryption and authentication algorithms when negotiating an IPSec SA.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to discard all changes and return to the main VPN screen.

10.2.3 Network Policy Edit: Port Forwarding Screen

Click **SECURITY > VPN** and the add network polic) icon in the **VPN Rules (IKE)** screen to display the **VPN-Network Policy -Edit** screen. Then, under **Virtual Address Mapping Rule**, select **Many-to-One** as the **Type** and click the **Port Forwarding Rules** button to open the following screen. Use this screen to configure port forwarding for your VPN tunnels to let the LAN-Cell forward traffic coming in through the VPN tunnel to the appropriate IP address on the LAN.

Figure 130 SECURITY > VPN > VPN Rules (IKE) > Edit Network Policy > Port Forwarding



The following table describes the labels in this screen.

Table 79 SECURITY > VPN > VPN Rules (IKE) > Edit Network Policy > Port Forwarding

LABEL	DESCRIPTION
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, all packets received for ports not specified in this screen are discarded.
#	This is the number of an individual port forwarding server entry.
Active	Select this check box to enable the port forwarding server entry. Clear this check box to disallow forwarding of these ports to an inside server without having to delete the entry.
Name	Enter a name to identify this port-forwarding rule.
Start Port	Type a port number in this field. To forward only one port, type the port number again in the **End Port** field. To forward a series of ports, type the start port number here and the end port number in the **End Port** field.
End Port	Type a port number in this field. To forward only one port, type the port number in the **Start Port** field above and then type it again in this field. To forward a series of ports, type the last port number in a series that begins with the port number in the **Start Port** field above.
Server IP Address	Type your server IP address in this field.
Apply	Click **Apply** to save your changes back to the LAN-Cell.
Reset	Click **Reset** to begin configuring this screen afresh.

10.2.4 VPN Rules (IKE): Network Policy Move Screen

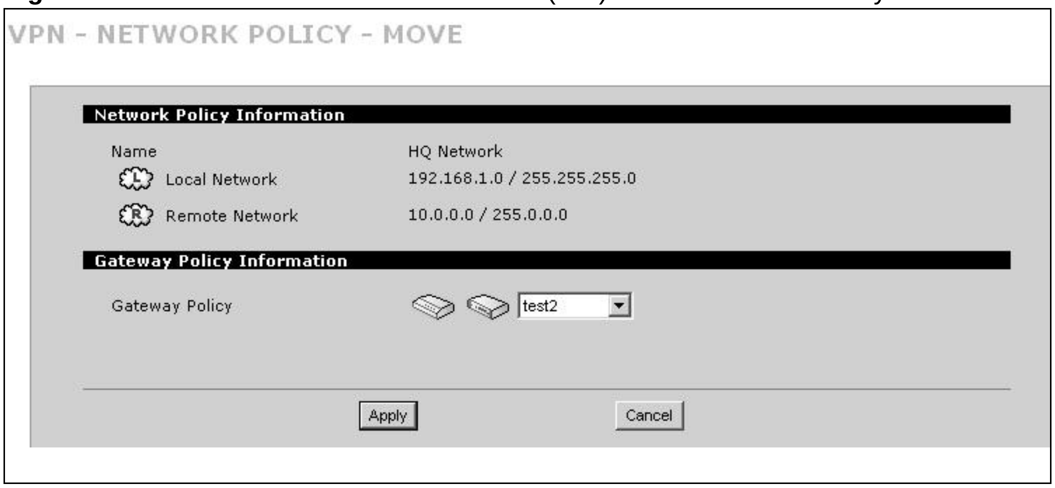
Click the move ( ) icon in the **VPN Rules (IKE)** screen to display the **VPN Rules (IKE): Network Policy Move** screen.

A VPN (Virtual Private Network) tunnel gives you a secure connection to another computer or network. Each VPN tunnel uses a single gateway policy and one or more network policies.

- The gateway policy contains the IKE SA settings. It identifies the IPSec routers at either end of a VPN tunnel.
- The network policy contains the IPSec SA settings. It specifies which devices (behind the IPSec routers) can use the VPN tunnel.

Use this screen to associate a network policy to a gateway policy.

Figure 131 SECURITY > VPN > VPN Rules (IKE) > Move Network Policy



The following table describes the labels in this screen.

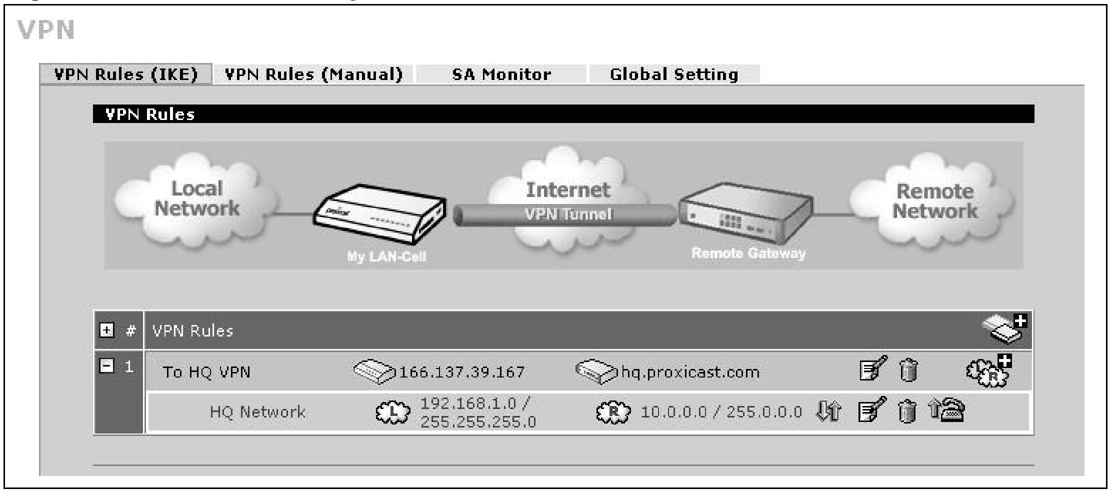
Table 80 SECURITY > VPN > VPN Rules (IKE) > Move Network Policy

LABEL	DESCRIPTION
Network Policy Information	The following fields display the general network settings of this VPN policy.
Name	This field displays the policy name.
Local Network	This field displays one or a range of IP address(es) of the computer(s) behind the LAN-Cell.
Remote Network	This field displays one or a range of IP address(es) of the remote network behind the remote IPsec router.
Gateway Policy Information	
Gateway Policy	Select the name of a VPN rule (or gateway policy) to which you want to associate this VPN network policy. If you do not want to associate a network policy to any gateway policy, select **Recycle Bin** from the drop-down list box. The **Recycle Bin** gateway policy is a virtual placeholder for any network policy(ies) without an associated gateway policy. When there is a network policy in **Recycle Bin**, the **Recycle Bin** gateway policy automatically displays in the **VPN Rules (IKE)** screen.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to discard all changes and return to the main VPN screen.

10.2.5 Dialing the VPN Tunnel via Web Configurator

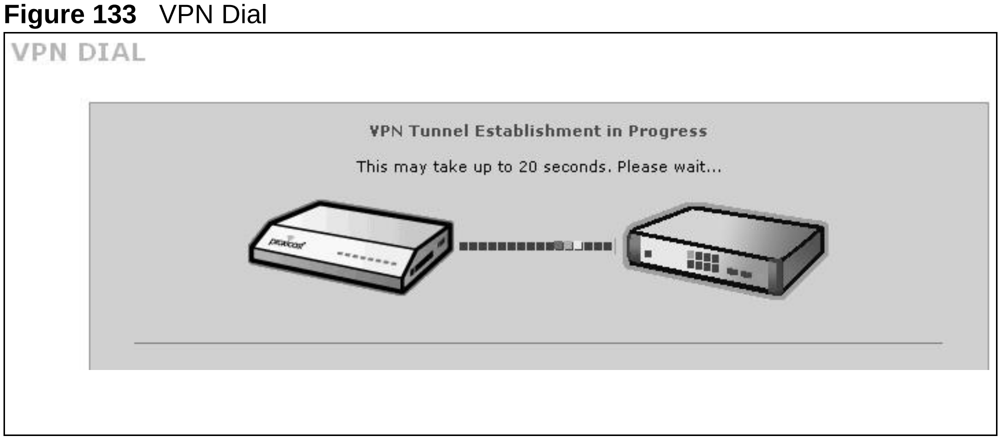
To test whether the IPSec routers can build the VPN tunnel, click the dial ( ) icon in the **VPN Rules (IKE)** screen to have the IPSec routers set up the tunnel. If you find a disconnect ( ) icon next to the rule you just created in the **VPN Rules (IKE)** screen, the LAN-Cell automatically built the VPN tunnel. Go to the **SA Monitor** screen to view a list of connected VPN tunnels. See Section 10.5 on page 231 for more information.

Figure 132 VPN Rule Configured



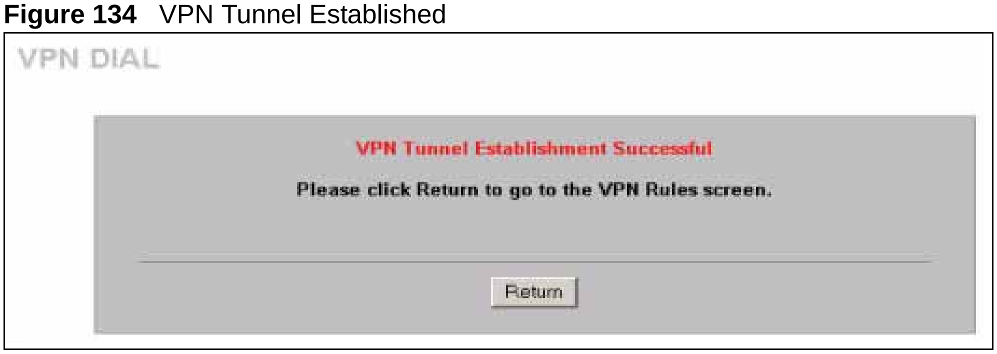
The following screen displays.

Figure 133 VPN Dial



This screen displays later if the IPSec routers can build the VPN tunnel.

Figure 134 VPN Tunnel Established



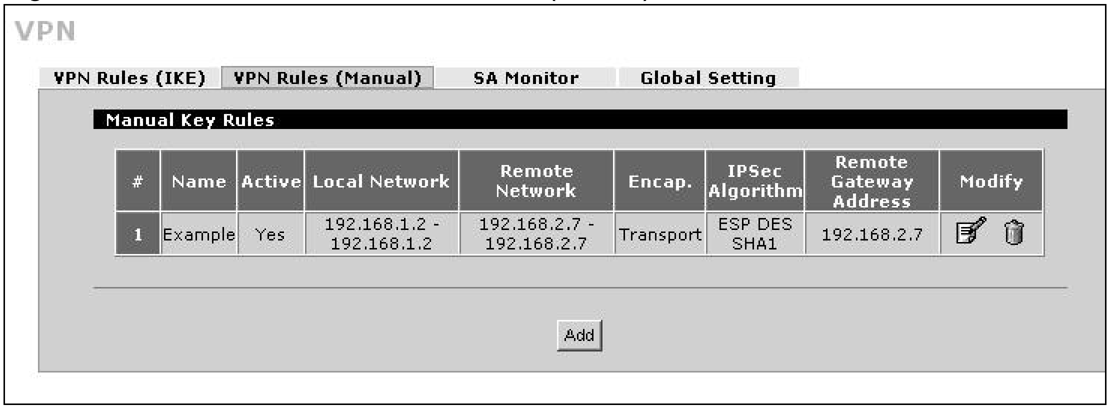
10.3 VPN Rules (Manual)

Refer to Figure 126 on page 211 for a graphical representation of the fields in the web configurator.

Click **SECURITY** > **VPN** > **VPN Rules (Manual)** to open the **VPN Rules (Manual)** screen.

Use this screen to manage the LAN-Cell's list of VPN rules (tunnels) that use manual keys. You may want to configure a VPN rule that uses manual key management if you are having problems with IKE key management.

Figure 135   SECURITY > VPN > VPN Rules (Manual)



The following table describes the labels in this screen.

Table 81   SECURITY > VPN > VPN Rules (Manual)

LABEL	DESCRIPTION
#	This is the VPN policy index number.
Name	This field displays the identification name for this VPN policy.
Active	This field displays whether the VPN policy is active or not. A **Yes** signifies that this VPN policy is active. **No** signifies that this VPN policy is not active.
Local Network	This is the IP address(es) of computer(s) on your local network behind your LAN-Cell. The same (static) IP address is displayed twice when the **Local Network Address Type** field in the **VPN - Manual Key - Edit** screen is configured to **Single Address**. The beginning and ending (static) IP addresses, in a range of computers are displayed when the **Local Network Address Type** field in the **VPN - Manual Key - Edit** screen is configured to **Range Address**. A (static) IP address and a subnet mask are displayed when the **Local Network Address Type** field in the **VPN - Manual Key - Edit** screen is configured to **Subnet Address**.

Table 81 SECURITY > VPN > VPN Rules (Manual) (continued)

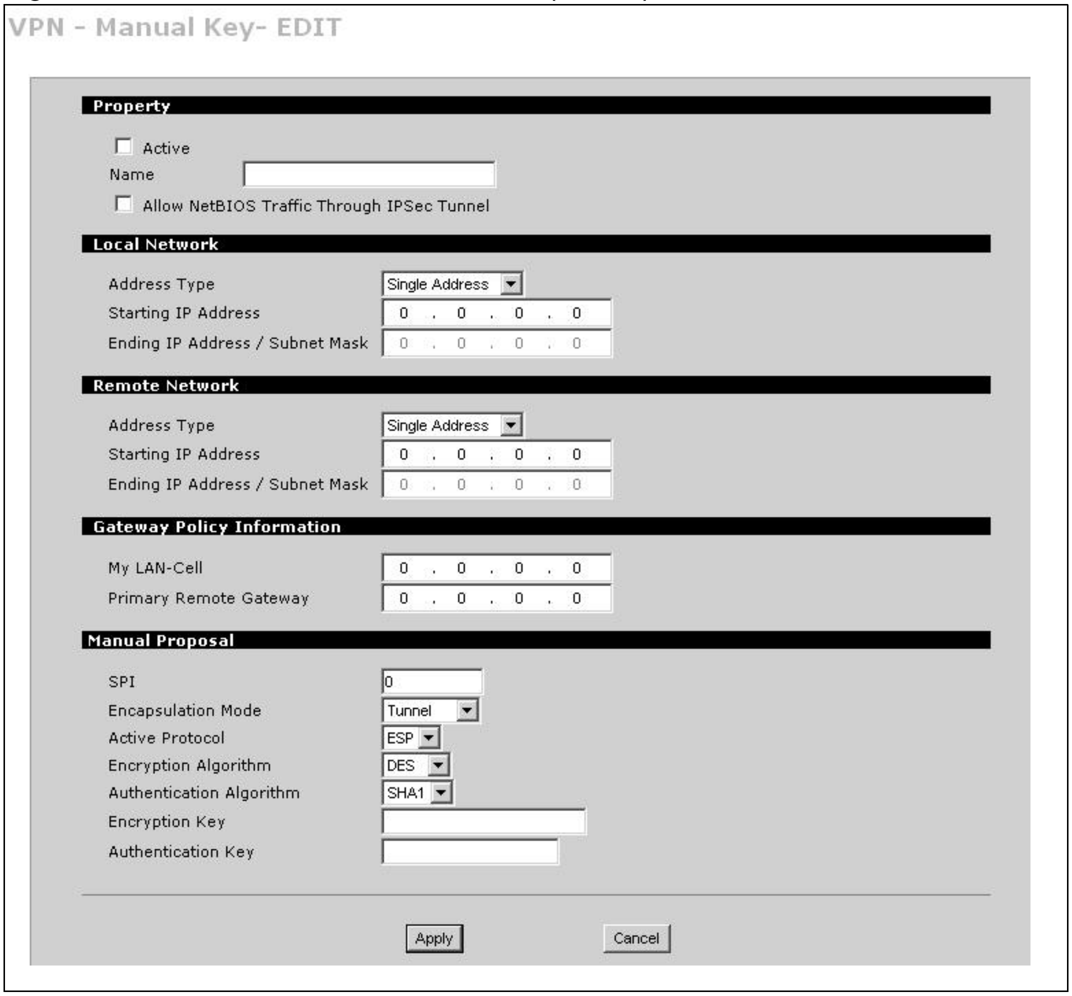
LABEL	DESCRIPTION
Remote Network	This is the IP address(es) of computer(s) on the remote network behind the remote IPSec router. This field displays **N/A** when the **Remote Gateway Address** field displays **0.0.0.0**. In this case only the remote IPSec router can initiate the VPN. The same (static) IP address is displayed twice when the **Remote Network Address Type** field in the **VPN - Manual Key - Edit** screen is configured to **Single Address**. The beginning and ending (static) IP addresses, in a range of computers are displayed when the **Remote Network Address Type** field in the **VPN - Manual Key - Edit** screen is configured to **Range Address**. A (static) IP address and a subnet mask are displayed when the **Remote Network Address Type** field in the **VPN - Manual Key - Edit** screen is configured to **Subnet Address**.
Encap.	This field displays **Tunnel** or **Transport** mode (**Tunnel** is the default selection).
IPSec Algorithm	This field displays the security protocols used for an SA. Both **AH** and **ESP** increase LAN-Cell processing requirements and communications latency (delay).
Remote Gateway Address	This is the static WAN IP address or domain name of the remote IPSec router.
Modify	Click the edit icon to edit the VPN policy. Click the delete icon to remove the VPN policy. A window displays asking you to confirm that you want to delete the VPN rule. When a VPN policy is deleted, subsequent policies move up in the page list.
Add	Click **Add** to add a new VPN policy.

10.4 VPN Rules (Manual): Edit Screen

Click the **Add** button or the edit icon on the **VPN Rules (Manual)** screen to open the following screen. Use this screen to configure VPN rules that use manual keys. Manual key management is useful if you have problems with IKE key management.

See Section on page 253 for more information about IPSec SAs using manual keys.

Figure 136 SECURITY > VPN > VPN Rules (Manual) > Edit



The following table describes the labels in this screen.

Table 82 SECURITY > VPN > VPN Rules (Manual) > Edit

LABEL	DESCRIPTION
Property	
Active	Select this check box to activate this VPN policy.
Name	Type up to 32 characters to identify this VPN policy. You may use any character, including spaces, but the LAN-Cell drops trailing spaces.
Allow NetBIOS Traffic Through IPSec Tunnel	NetBIOS (Network Basic Input/Output System) are TCP or UDP 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 this check box to send NetBIOS packets through the VPN connection.
Local Network	Local 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 82 SECURITY > VPN > VPN Rules (Manual) > Edit (continued)

LABEL	DESCRIPTION
Address Type	Use the drop-down list box to choose **Single Address**, **Range Address**, or **Subnet Address**. Select **Single Address** for a single IP address. Select **Range Address** for a specific range of IP addresses. Select **Subnet Address** to specify IP addresses on a network by their subnet mask.
Starting IP Address	When the **Address Type** field is configured to **Single Address**, enter a (static) IP address on the LAN behind your LAN-Cell. When the **Address Type** field is configured to **Range Address**, enter the beginning (static) IP address, in a range of computers on the LAN behind your LAN-Cell. When the **Address Type** field is configured to **Subnet Address**, this is a (static) IP address on the LAN behind your LAN-Cell.
Ending IP Address/Subnet Mask	When the **Address Type** field is configured to **Single Address**, this field is N/A. When the **Address Type** field is configured to **Range Address**, enter the end (static) IP address, in a range of computers on the LAN behind your LAN-Cell. When the **Address Type** field is configured to **Subnet Address**, this is a subnet mask on the LAN behind your LAN-Cell.
Remote Network	Remote IP addresses must be static and correspond to the remote IPSec router's configured local 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.
Address Type	Use the drop-down list box to choose **Single Address**, **Range Address**, or **Subnet Address**. Select **Single Address** with a single IP address. Select **Range Address** for a specific range of IP addresses. Select **Subnet Address** to specify IP addresses on a network by their subnet mask.
Starting IP Address	When the **Address Type** field is configured to **Single Address**, enter a (static) IP address on the network behind the remote IPSec router. When the Addr Type field is configured to **Range Address**, enter the beginning (static) IP address, in a range of computers on the network behind the remote IPSec router. When the **Address Type** field is configured to **Subnet Address**, enter a (static) IP address on the network behind the remote IPSec router.
Ending IP Address/Subnet Mask	When the **Address Type** field is configured to **Single Address**, this field is N/A. When the **Address Type** field is configured to **Range Address**, enter the end (static) IP address, in a range of computers on the network behind the remote IPSec router. When the **Address Type** field is configured to **Subnet Address**, enter a subnet mask on the network behind the remote IPSec router.
Gateway Policy Information	
My LAN-Cell	Enter the WAN IP address or the domain name of your LAN-Cell or leave the field set to **0.0.0.0**. The LAN-Cell uses its current WAN IP address (static or dynamic) in setting up the VPN tunnel if you leave this field as **0.0.0.0**. If the WAN connection goes down, the LAN-Cell uses the dial backup IP address for the VPN tunnel when using dial backup or the LAN IP address when using traffic redirect. The VPN tunnel has to be rebuilt if this IP address changes.
Primary Remote Gateway	Type the WAN IP address or the domain name (up to 31 characters) of the IPSec router with which you're making the VPN connection.
Manual Proposal	
SPI	Type a unique **SPI** (Security Parameter Index) from one to four characters long. Valid Characters are "0, 1, 2, 3, 4, 5, 6, 7, 8, and 9".
Encapsulation Mode	Select **Tunnel** mode or **Transport** mode from the drop-down list box.

Table 82 SECURITY > VPN > VPN Rules (Manual) > Edit (continued)

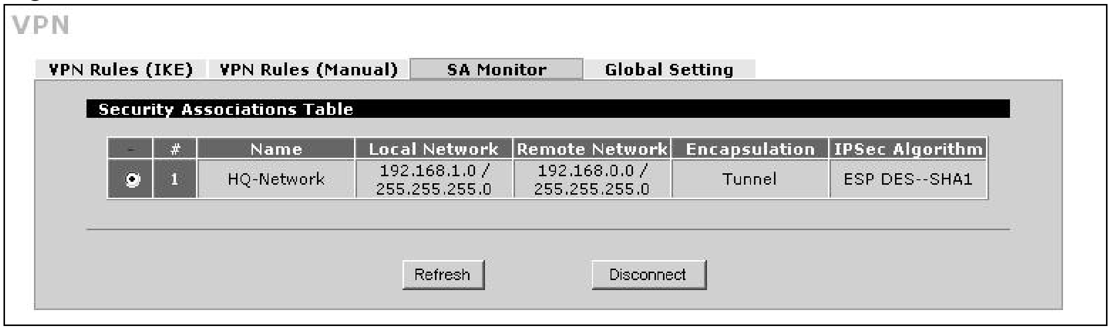
LABEL	DESCRIPTION
Active Protocol	Select **ESP** if you want to use ESP (Encapsulation Security Payload). The ESP protocol (RFC 2406) provides encryption as well as some of the services offered by **AH**. If you select **ESP** here, you must select options from the **Encryption Algorithm** and **Authentication Algorithm** fields (described next). 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 (described next).
Encryption Algorithm	Select **DES**, **3DES** or **NULL** from the drop-down list box. When **DES** is used for data communications, both sender and receiver must know the **Encryption Key**, which can be used to encrypt and decrypt the message or to generate and verify a message authentication code. 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	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 is applicable when you select **ESP** in the **Active Protocol** field above. With **DES**, type a unique key 8 characters long. With **3DES**, type a unique key 24 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 LAN-Cell.
Cancel	Click **Cancel** to exit this screen without saving.

10.5 VPN SA Monitor Screen

In the web configurator, click **SECURITY** > **VPN** > **SA Monitor**. Use this screen to display and manage active VPN connections.

A Security Association (SA) is the group of security settings related to a specific VPN tunnel. This screen displays active VPN connections. Use **Refresh** to display active VPN connections.

Figure 137 SECURITY > VPN > SA Monitor



The following table describes the labels in this screen.

Table 83 SECURITY > VPN > SA Monitor

LABEL	DESCRIPTION
#	This is the security association index number.
Name	This field displays the identification name for this VPN policy.
Local Network	This field displays the IP address of the computer using the VPN IPSec feature of your LAN-Cell.
Remote Network	This field displays IP address (in a range) of computers on the remote network behind the remote IPSec router.
Encapsulation	This field displays **Tunnel** or **Transport** mode.
IPSec Algorithm	This field displays the security protocols used for an SA. Both AH and ESP increase LAN-Cell processing requirements and communications latency (delay).
Refresh	Click **Refresh** to display the current active VPN connection(s).
Disconnect	Select a security association index number that you want to disconnect and then click **Disconnect**.

10.6 VPN Global Setting Screen

Use this screen to change settings that apply to all of your VPN tunnels.

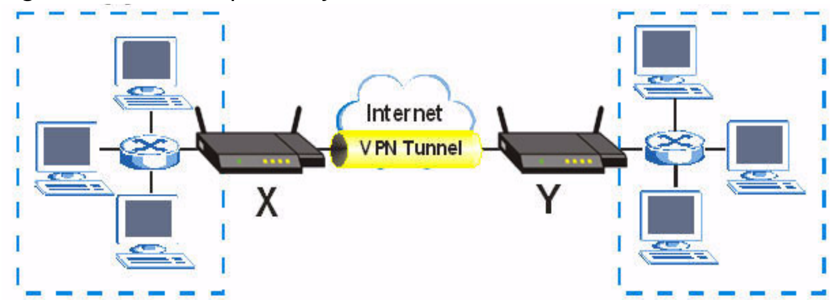
Local and Remote IP Address Conflict Resolution

Normally, you do not configure your local VPN policy rule’s IP addresses to overlap with the remote VPN policy rule’s IP addresses (see Virtual Address Mapping on page 251). For example, you usually would not configure both with 192.168.1.0. However, overlapping local and remote network IP addresses can occur with dynamic VPN rules or IP alias.

Dynamic VPN Rule

Local and remote network IP addresses can overlap when you configure a dynamic VPN rule for a remote site (see Figure 138). For example, when you configure LAN-Cell X, you configure the local network as 192.168.1.0/24 and the remote network as any (0.0.0.0). The “any” includes all possible IP addresses. It will forward traffic from network A to network B even if both the sender (for example 192.168.1.8) and the receiver (for example 192.168.1.9) are in network A. Note that the remote access can still use the VPN tunnel to access computers on LAN-Cell X’s network.

Figure 138 Overlap in a Dynamic VPN Rule



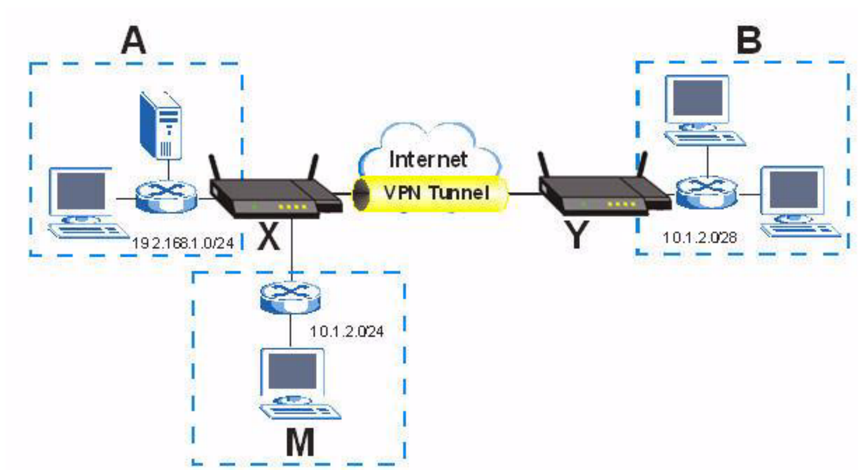
- Enabling the **VPN Global Setting** option box **Do not apply VPN Rules to overlapped local and remote address ranges** causes the LAN-Cell check if a packet's destination is also at the local network before forwarding the packet. If it is, the LAN-Cell sends the traffic to the local network.
- Disabling the option box disables the checking for local network IP addresses and sends traffic for all overlapping addresses to the remote network. This will disable your ability to access the LAN-Cell from the local subnet.

IP Alias

You could have an IP alias network that overlaps with the VPN remote network (see Figure 139). For example, you have an IP alias network M (10.1.2.0/24) in LAN-Cell X's LAN. For the VPN rule, you configure the VPN network as follows.

- Local IP address start: 192.168.1.1, end: 192.168.1.254
- Remote IP address start: 10.1.2.240, end: 10.1.2.254
- IP addresses 10.1.2.240 to 10.1.2.254 overlap.

Figure 139 Overlap in IP Alias and VPN Remote Networks

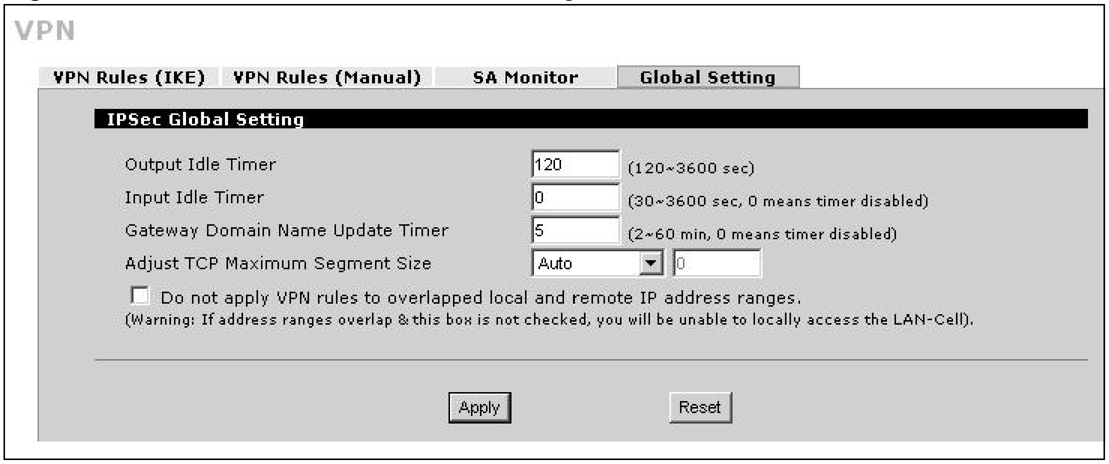


In this case, if you want to send packets from network **A** to an overlapped IP (ex. 10.1.2.241) that is in the IP alias network **M**, you have to enable **Do not apply VPN Rules to overlapped local and remote address ranges**.

10.6.1 Configuring the Global Setting Screen

Click **SECURITY** > **VPN** > **Global Setting** to open the **VPN Global Setting** screen.

Figure 140 SECURITY > VPN > Global Setting



The following table describes the labels in this screen.

Table 84 SECURITY > VPN > Global Setting

LABEL	DESCRIPTION
Output Idle Timer	When traffic is sent to a remote IPSec router from which no reply is received after the specified time period, the LAN-Cell checks the VPN connectivity. If the remote IPSec router does not reply, the LAN-Cell automatically disconnects the VPN tunnel. Enter the time period (between 120 and 3600 seconds) to wait before the LAN-Cell checks all of the VPN connections to remote IPSec routers. Enter **0** to disable this feature.
Input Idle Timer	When no traffic is received from a remote IPSec router after the specified time period, the LAN-Cell checks the VPN connectivity. If the remote IPSec router does not reply, the LAN-Cell automatically disconnects the VPN tunnel. Enter the time period (between 30 and 3600 seconds) to wait before the LAN-Cell checks all of the VPN connections to remote IPSec routers. Enter **0** to disable this feature.

Table 84 SECURITY > VPN > Global Setting (continued)

LABEL	DESCRIPTION
Gateway Domain Name Update Timer	If you use dynamic domain names in VPN rules to identify the LAN-Cell and/or the remote IPSec router, the IP address mapped to the domain name can change. The VPN tunnel stops working after the IP address changes. Any users of the VPN tunnel are disconnected until the LAN-Cell gets the new IP address from a DNS server and rebuilds the VPN tunnel. Enter the time period (between 2 and 60 minutes) to set how often the LAN-Cell queries a DNS server to update the IP address and domain name mapping. If the query returns a new IP address for a dynamic domain name, the LAN-Cell disconnects the VPN tunnel. The LAN-Cell rebuilds the VPN tunnel (using the new IP address) immediately if the IPSec SA is set to nailed up. Otherwise the LAN-Cell rebuilds the VPN tunnel when there are packets for it or you manually dial it. If the LAN-Cell and all of the remote IPSec routers use static IP addresses or regular domain names, you can enter **0** to disable this feature.
Adjust TCP Maximum Segment Size	The TCP packets are larger after the LAN-Cell encrypts them for VPN. The LAN-Cell fragments packets that are larger than a connection's MTU (Maximum Transmit Unit). In most cases you should leave this set to **Auto**. The LAN-Cell automatically sets the Maximum Segment Size (MSS) of the TCP packets that are to be encrypted by VPN based on the encapsulation type. Select **Off** to not adjust the MSS for the encrypted TCP packets. If your network environment causes fragmentation issues that are affecting your throughput performance, you can manually set a smaller MSS for the TCP packets that are to be encrypted by VPN. Select **User-Defined** and specify a size from 0~1460 bytes. 0 has the LAN-Cell use the auto setting.
Do not apply VPN Rules to overlapped local and remote address ranges	When you configure a VPN rule, the LAN-Cell checks to make sure that the IP addresses in the local and remote networks do not overlap. Select this check box to disable the check if you need to configure a VPN policy with overlapping local and remote IP addresses. Note: If a VPN policy's local and remote IP addresses overlap, you may not be able to access the device on your LAN because the LAN-Cell automatically triggers a VPN tunnel to the remote device with the same IP address.
Apply	Click **Apply** to save your changes back to the LAN-Cell.
Reset	Click **Reset** to begin configuring this screen afresh.

10.7 Mobile User VPN/IPSec Examples

The following examples show how multiple mobile users can make VPN connections to a single LAN-Cell. The mobile users use IPSec routers (or IPSec client software) with dynamic WAN IP addresses. The LAN-Cell has a static public IP address.

Remote users (or routers) must use IPSec-compliant software or hardware to establish a VPN connection with the LAN-Cell. Refer to Proxicast's Knowledgebase and TechNotes for examples of configuring specific VPN client software packages and devices.

10.7.1 Mobile Users Sharing One VPN Rule Example

See the following figure and table for an example configuration that allows multiple mobile users (**A**, **B** and **C** in the figure) to use one VPN rule to simultaneously access a LAN-Cell (**HQ** in the figure). The mobile users do not have domain names mapped to the WAN IP addresses of their IPSec routers. The mobile users must all use the same IPSec parameters but the local IP addresses (or ranges of addresses) should not overlap.

Figure 141 Mobile Users Sharing One VPN Rule Example

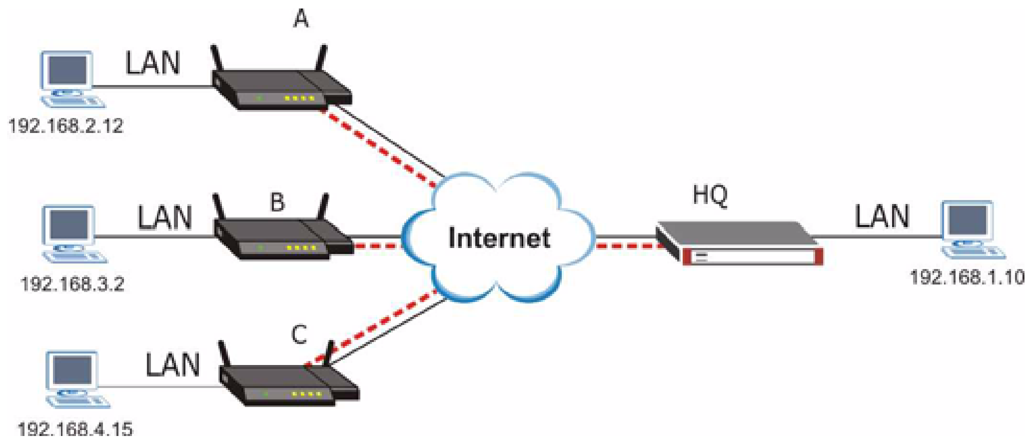


Table 85 Mobile Users Sharing One VPN Rule Example

FIELDS	MOBILE USER	HEADQUARTERS
My LAN-Cell:	0.0.0.0 (dynamic IP address assigned by the ISP)	Public static IP address
Remote Gateway Address:	Public static IP address	0.0.0.0 With this IP address only the user can initiate the IPSec tunnel.
Local Network - Single IP Address:	User A: 192.168.2.12 User B: 192.168.3.2 User C: 192.168.4.15	192.168.1.10
Remote Network - Single IP Address:	192.168.1.10	Not Applicable

10.7.2 Mobile Users Using Unique VPN Rules Example

In this example the mobile users (A, B and C in the figure) use IPSec routers (or VPN client software) with domain names that are mapped to their dynamic WAN IP addresses (use Dynamic DNS to do this).

With aggressive negotiation mode (see Section on page 247), the LAN-Cell can use the ID types and contents to distinguish between VPN rules. Mobile users can each use a separate VPN rule to simultaneously access the LAN-Cell. They can use different IPSec parameters. The local IP addresses (or ranges of addresses) of the rules configured on the LAN-Cell can overlap. The local IP addresses of the rules configured on the mobile users' IPSec routers should not overlap.

See the following table and figure for an example where three mobile users each use a different VPN rule for a VPN connection with a LAN-Cell. The LAN-Cell (HQ in the figure) identifies each incoming SA by its ID type and content and uses the appropriate VPN rule to establish the VPN connection.

The LAN-Cell can also initiate VPN connections to the mobile users since it can find the users by resolving their domain names.

Figure 142 Mobile Users Using Unique VPN Rules Example

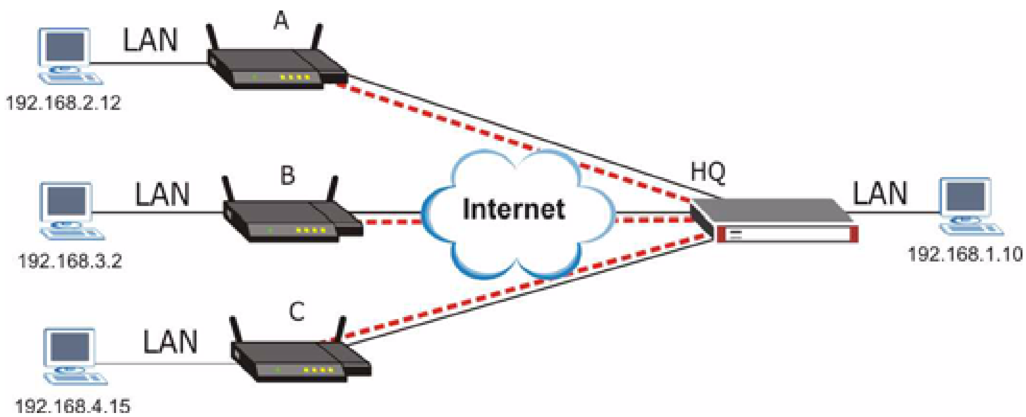


Table 86 Mobile Users Using Unique VPN Rules Example

MOBILE USERS	HEADQUARTERS
All Mobile User Rules:	All Headquarters Rules:
My LAN-Cell 0.0.0.0	My LAN-Cell: bigcompanyhq.com
Remote Gateway Address: bigcompanyhq.com	Local Network - Single IP Address: 192.168.1.10
Remote Network - Single IP Address: 192.168.1.10	Local ID Type: E-mail
Peer ID Type: E-mail	Local ID Content: bob@bigcompanyhq.com
Peer ID Content: bob@bigcompanyhq.com	
User A (UserA.dydns.org)	Headquarters LAN-Cell Rule 1:
Local ID Type: IP	Peer ID Type: IP
Local ID Content: 192.168.2.12	Peer ID Content: 192.168.2.12
Local IP Address: 192.168.2.12	Remote Gateway Address: UserA.dydns.org
	Remote Address 192.168.2.12
User B (UserB.dydns.org)	Headquarters LAN-Cell Rule 2:

Table 86 Mobile Users Using Unique VPN Rules Example

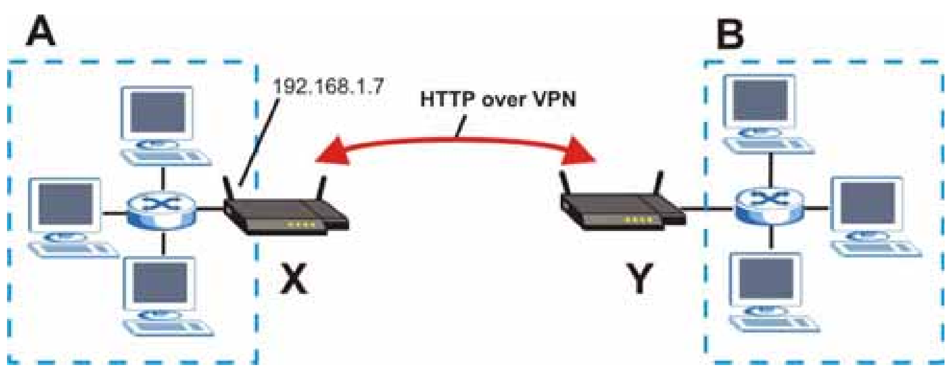
MOBILE USERS	HEADQUARTERS
Local ID Type: DNS	Peer ID Type: DNS
Local ID Content: UserB.com	Peer ID Content: UserB.com
Local IP Address: 192.168.3.2	Remote Gateway Address: UserB.dydns.org
	Remote Address 192.168.3.2
User C (UserC.dydns.org)	Headquarters LAN-Cell Rule 3:
Local ID Type: E-mail	Peer ID Type: E-mail
Local ID Content: myVPN@myplace.com	Peer ID Content: myVPN@myplace.com
Local IP Address: 192.168.4.15	Remote Gateway Address: UserC.dydns.org
	Remote Address 192.168.4.15

10.8 VPN and Remote Management

You can allow someone to use a service (like Telnet or HTTP) through a VPN tunnel to manage the LAN-Cell. One of the LAN-Cell's ports must be part of the VPN rule's local network. This can be the LAN-Cell's LAN port if you do not want to allow remote management on the WAN port. You also have to configure remote management (**REMOTE MGMT**) to allow management access for the service through the specific port (see Chapter 15 on page 319).

In the following example, the VPN rule's local network (A) includes the LAN-Cell's LAN IP address of 192.168.1.7. Someone in the remote network (B) can use a service (like HTTP for example) through the VPN tunnel to access the LAN-Cell's LAN interface. Remote management must also be configured to allow HTTP access on the LAN-Cell's LAN interface.

Figure 143 VPN for Remote Management Example

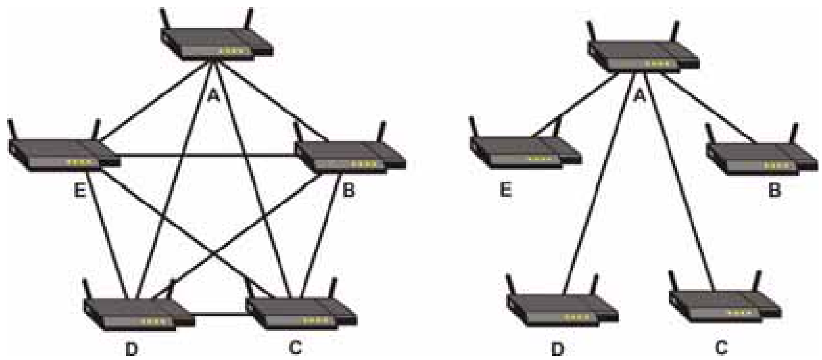


10.9 Hub-and-spoke VPN

Hub-and-spoke VPN connects VPN tunnels to form one secure network.

Figure 144 on page 239 shows some example network topologies. In the first (fully-meshed) approach, there is a VPN connection between every pair of routers. In the second (hub-and-spoke) approach, there is a VPN connection between each spoke router (**B**, **C**, **D**, and **E**) and the hub router (**A**). The hub router routes VPN traffic between the spoke routers and itself.

Figure 144 VPN Topologies



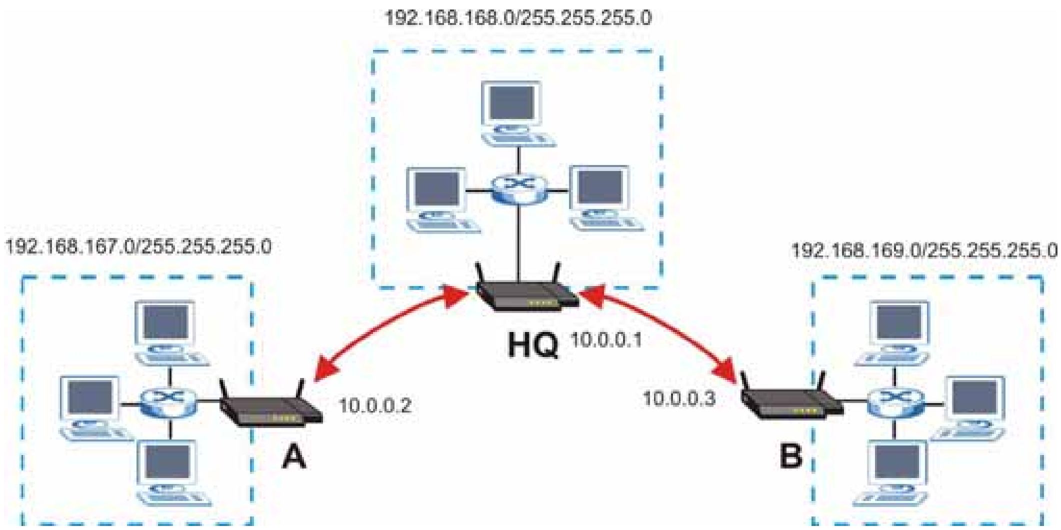
Hub-and-spoke VPN reduces the number of VPN connections that you have to set up and maintain in the network. Small office or telecommuter IPSec routers that support a limited number of VPN tunnels are also able to use VPN to connect to more networks. Hub-and-spoke VPN makes it easier for the hub router to manage the traffic between the spoke routers. If you have the spoke routers access the Internet through the hub-and-spoke VPN tunnel, the hub router can also provide content filtering, IDP, anti-spam and anti-virus protection for the spoke routers.

You should not use a hub-and-spoke VPN in every situation, however. The hub router is a single point of failure, so a hub-and-spoke VPN may not be appropriate if the connection between the spoke routers cannot be down occasionally (for maintenance, for example). In addition, there is a significant burden on the hub router. It receives VPN traffic from one spoke, decrypts it, inspects it to find out where to send it, encrypts it, and sends it to the appropriate spoke. Therefore, a hub-and-spoke VPN is more suitable when there is a minimum amount of traffic between spoke routers.

10.9.1 Hub-and-spoke VPN Example

The following figure shows a basic hub-and-spoke VPN. Branch office A uses one VPN rule to access both the headquarters (HQ) network and branch office B’s network. Branch office B uses one VPN rule to access both the headquarters and branch office A’s networks.

Figure 145 Hub-and-spoke VPN Example



10.9.2 Hub-and-spoke Example VPN Rule Addresses

The VPN rules for this hub-and-spoke example would use the following address settings.

Branch Office A:

- Remote Gateway: 10.0.0.1
- Local IP address: 192.168.167.0/255.255.255.0
- Remote IP address: 192.168.168.0~192.168.169.255

Headquarters:

Rule 1:

- Remote Gateway: 10.0.0.2
- Local IP address: 192.168.168.0~192.168.169.255
- Remote IP address:192.168.167.0/255.255.255.0

Rule 2:

- Remote Gateway: 10.0.0.3
- Local IP address: 192.168.167.0~192.168.168.255
- Remote IP address: 192.168.169.0/255.255.255.0

Branch Office B:

- Remote Gateway: 10.0.0.1
- Local IP address: 192.168.169.0/255.255.255.0
- Remote IP address: 192.168.167.0~192.168.168.255

10.9.3 Hub-and-spoke VPN Requirements and Suggestions

Consider the following when implementing a hub-and-spoke VPN.

The local IP addresses configured in the VPN rules cannot overlap

The hub router must have at least one separate VPN rule for each spoke. In the local IP address, specify the IP addresses of the hub-and-spoke networks with which the spoke is to be able to have a VPN tunnel. This may require you to use more than one VPN rule.

If you want to have the spoke routers access the Internet through the hub-and-spoke VPN tunnel, set the VPN rules in the spoke routers to use 0.0.0.0 (any) as the remote IP address.

Make sure that your **From VPN** and **To VPN** firewall rules do not block the VPN packets.

10.10 VPN Troubleshooting

If the IPSec tunnel does not build properly, the problem is likely a configuration error at one of the IPSec routers. Log into the web configurators of both IPSec routers.
Check the settings in each field methodically and slowly.

VPN Log

The system log can often help to identify a configuration problem.
Use the web configurator **LOGS Log Settings** screen to enable IKE and IPSec logging at both ends, clear the log and then build the tunnel.

View the log via the web configurator **LOGS View Log** screen or type `sys log disp` from SMT **Menu 24.8**. See Section on page 381 for information on the log messages.

Figure 146 VPN Log Example

```
LAN-Cell> sys log disp ike ipsec

#  .time                 source                  destination           notes
    message
  0|01/11/2001 18:47:22 |5.6.7.8               |5.1.2.3               |IKE
    Rule [ex-1] Tunnel built successfully
  1|01/11/2001 18:47:22 |5.6.7.8               |5.1.2.3               |IKE
    The cookie pair is : 0xDAC0B43FBDE154F5 / 0xC5156C099C3F7DCA
  2|01/11/2001 18:47:22 |5.6.7.8               |5.1.2.3               |IKE
    Send:[HASH]
  3|01/11/2001 18:47:22 |5.6.7.8               |5.1.2.3               |IKE
    The cookie pair is : 0xDAC0B43FBDE154F5 / 0xC5156C099C3F7DCA
  4|01/11/2001 18:47:22 |5.6.7.8               |5.1.2.3               |IKE
    Adjust TCP MSS to 1398
  5|01/11/2001 18:47:22 |5.1.2.3               |5.6.7.8               |IKE
    Recv:[HASH][SA][NONCE][ID][ID]
  6|01/11/2001 18:47:22 |5.1.2.3               |5.6.7.8               |IKE
    The cookie pair is : 0xDAC0B43FBDE154F5 / 0xC5156C099C3F7DCA
  7|01/11/2001 18:47:21 |5.6.7.8               |5.1.2.3               |IKE
    IKE Packet Retransmit
  8|01/11/2001 18:47:21 |5.6.7.8               |5.1.2.3               |IKE
    The cookie pair is : 0xDAC0B43FBDE154F5 / 0xC5156C099C3F7DCA
  9|01/11/2001 18:47:17 |5.6.7.8               |5.1.2.3               |IKE
    Send:[HASH][SA][NONCE][ID][ID]
 10|01/11/2001 18:47:17 |5.6.7.8               |5.1.2.3               |IKE
    The cookie pair is : 0xDAC0B43FBDE154F5 / 0xC5156C099C3F7DCA
 11|01/11/2001 18:47:17 |5.6.7.8               |5.1.2.3               |IKE
    Start Phase 2: Quick Mode
 12|01/11/2001 18:47:17 |5.6.7.8               |5.1.2.3               |IKE
    The cookie pair is : 0xDAC0B43FBDE154F5 / 0xC5156C099C3F7DCA
 13|01/11/2001 18:47:17 |5.6.7.8               |5.1.2.3               |IKE
    Phase 1 IKE SA process done
 14|01/11/2001 18:47:17 |5.6.7.8               |5.1.2.3               |IKE
    The cookie pair is : 0xDAC0B43FBDE154F5 / 0xC5156C099C3F7DCA
 15|01/11/2001 18:47:17 |5.1.2.3               |5.6.7.8               |IKE
    Recv:[ID][HASH][NOTFY:INIT_CONTACT]9C3F7DCA
 16|01/11/2001 18:47:17 |5.1.2.3               |5.6.7.8               |IKE
    The cookie pair is : 0xDAC0B43FBDE154F5 / 0xC5156C099C3F7DCA
 17|01/11/2001 18:47:15 |5.6.7.8               |5.1.2.3               |IKE
    Send:[ID][HASH][NOTFY:INIT_CONTACT]9C3F7DCA
```

10.10.1 IPSec Debug

If you are having difficulty building an IPSec tunnel to a non-Proxicast IPSec router, advanced users may wish to examine the IPSec debug feature (in the commands).

If any of your VPN rules have an active network policy set to nailed-up, using the IPSec debug feature may cause the LAN-Cell to continuously display new information. Type `ipsec debug level 0` and press [ENTER] to stop it.

Figure 147 IKE/IPSec Debug Example

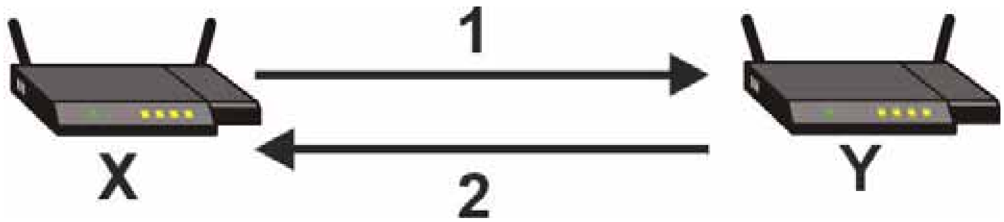
```
LAN-Cell> ipsec debug
type            level           display
LAN-Cell> ipsec debug type
<0:Disable | 1:Original on|off | 2:IKE on|off | 3: IPSec [SPI]|on|off |
4:XAUTH on|off | 5:CERT on|off | 6: All>
LAN-Cell> ipsec debug level
<0:None | 1:User | 2:Low | 3:High>

LAN-Cell> ipsec debug type 1 on
LAN-Cell> ipsec debug type 2 on
LAN-Cell> ipsec debug level 3

LAN-Cell> ipsec dial 1
get_ipsec_sa_by_policyIndex():
Start dialing for tunnel <rule# 1>...
ikeStartNegotiate(): saIndex<0>
peerIp<5.1.2.3> protocol: <IPSEC_ESP>(3)

   peer Ip <5.1.2.3> initiator(): type<IPSEC_ESP>, exch<Main>

   initiator :
   protocol: IPSEC_ESP, exchange mode: Main mode  find_ipsec_sa():
      find ipsec saNot found

      Not found  isadb_is_outstanding_req():
      isakmp is outstanding req : SA not found
isadb_create_entry():  >> INITIATOR

  isadb_get_entry_by_addr():
      Get IKE entry by address:   SA not found

      SA not found  ISAKMP SA created for peer <BRANCH> size<900>

      ISAKMP SA created for peer <BRANCH> size<900>  ISAKMP SA built,
ikePeer.s0

      ISAKMP SA built, index = 0isadb_create_entry(): done

      create IKE entry doneinitiator(): find myIpAddr = 0.0.0.0, use
<5.6.7.8> r
```

10.11 IPSec VPN Technical Reference

IKE SA Proposal

The IKE SA proposal is used to identify the encryption algorithm, authentication algorithm, and Diffie-Hellman (DH) key group that the LAN-Cell and remote IPSec router use in the IKE SA. In main mode, this is done in steps 1 and 2, as illustrated below.

Figure 148 IKE SA: Main Negotiation Mode, Steps 1 - 2: IKE SA Proposal



The LAN-Cell sends one or more proposals to the remote IPSec router. (In some devices, you can set up only one proposal.) Each proposal consists of an encryption algorithm, authentication algorithm, and DH key group that the LAN-Cell wants to use in the IKE SA. The remote IPSec router selects an acceptable proposal and sends the accepted proposal back to the LAN-Cell. If the remote IPSec router rejects all of the proposals (for example, if the VPN tunnel is not configured correctly), the LAN-Cell and remote IPSec router cannot establish an IKE SA.

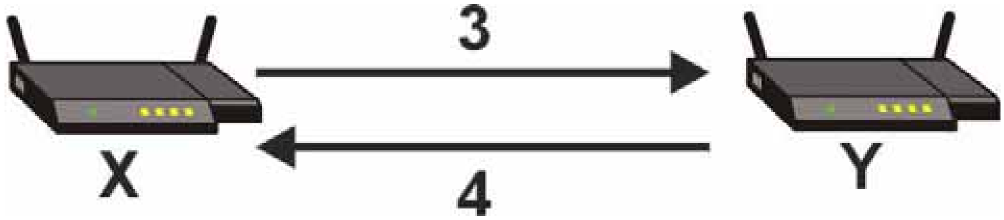
Both routers must use the same encryption algorithm, authentication algorithm, and DH key group.

See the field descriptions for information about specific encryption algorithms, authentication algorithms, and DH key groups. See Section on page 244 for more information about DH key groups.

Diffie-Hellman (DH) Key Exchange

The LAN-Cell and the remote IPSec router use a DH key exchange to establish a shared secret, which is used to generate encryption keys for IKE SA and IPSec SA. In main mode, the DH key exchange is done in steps 3 and 4, as illustrated below.

Figure 149 IKE SA: Main Negotiation Mode, Steps 3 - 4: DH Key Exchange



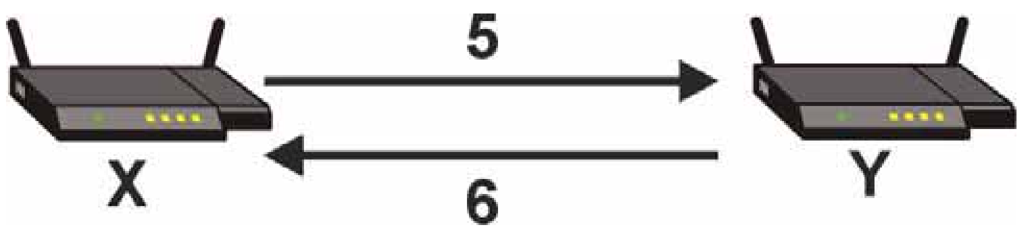
The DH key exchange is based on DH key groups. Each key group is a fixed number of bits long. The longer the key, the more secure the encryption keys, but also the longer it takes to encrypt and decrypt information. For example, DH2 keys (1024 bits) are more secure than DH1 keys (768 bits), but DH2 encryption keys take longer to encrypt and decrypt.

Authentication

Before the LAN-Cell and remote IPSec router establish an IKE SA, they have to verify each other's identity. This process is based on pre-shared keys and router identities.

In main mode, the LAN-Cell and remote IPSec router authenticate each other in steps 5 and 6, as illustrated below. Their identities are encrypted using the encryption algorithm and encryption key the LAN-Cell and remote IPSec router selected in previous steps.

Figure 150 IKE SA: Main Negotiation Mode, Steps 5 - 6: Authentication



The LAN-Cell and remote IPSec router use a pre-shared key in the authentication process, though it is not actually transmitted or exchanged.

The LAN-Cell and the remote IPSec router must use the same pre-shared key.

Router identity consists of ID type and ID content. The ID type can be IP address, domain name, or e-mail address, and the ID content is a specific IP address, domain name, or e-mail address. The ID content is only used for identification; the IP address, domain name, or e-mail address that you enter does not have to actually exist.

The LAN-Cell and the remote IPSec router each has its own identity, so each one must store two sets of information, one for itself and one for the other router. Local ID type and ID content refers to the ID type and ID content that applies to the router itself, and peer ID type and ID content refers to the ID type and ID content that applies to the other router in the IKE SA.

The LAN-Cell's local and peer ID type and ID content must match the remote IPSec router's peer and local ID type and ID content, respectively.

In the following example, the ID type and content match so the LAN-Cell and the remote IPSec router authenticate each other successfully.

Table 87 VPN Example: Matching ID Type and Content

LAN-CELL	REMOTE IPSEC ROUTER
Local ID type: E-mail	Local ID type: IP
Local ID content: tom@yourcompany.com	Local ID content: 1.1.1.2
Peer ID type: IP	Peer ID type: E-mail
Peer ID content: 1.1.1.2	Peer ID content: tom@yourcompany.com

In the following example, the ID type and content do not match so the authentication fails and the LAN-Cell and the remote IPSec router cannot establish an IKE SA.

Table 88 VPN Example: Mismatching ID Type and Content

LAN-CELL	REMOTE IPSEC ROUTER
Local ID type: E-mail	Local ID type: IP
Local ID content: tom@yourcompany.com	Local ID content: **1.1.1.2**
Peer ID type: IP	Peer ID type: E-mail
Peer ID content: **1.1.1.15**	Peer ID content: tom@yourcompany.com

It is also possible to configure the LAN-Cell to ignore the identity of the remote IPSec router. In this case, you usually set the peer ID type to **Any**. This is not as secure as other peer ID types, however.

Certificates

It is also possible for the LAN-Cell and remote IPSec router to authenticate each other with certificates. In this case, the authentication process is different.

- Instead of using the pre-shared key, the LAN-Cell and remote IPSec router check each other's certificates.
- The local ID type and ID content come from the certificate. On the LAN-Cell, you simply select which certificate to use.
- If you set the peer ID type to **Any**, the LAN-Cell authenticates the remote IPSec router using the trusted certificates and trusted CAs you have set up. Alternatively, if you want to use a specific certificate to authenticate the remote IPSec router, you can use the information in the certificate to specify the peer ID type and ID content.

You must set up the certificates for the LAN-Cell and remote IPSec router before you can use certificates in IKE SA. See Chapter 11 on page 255 for more information about certificates.

Extended Authentication

Extended authentication is often used when multiple IPSec routers use the same VPN tunnel to connect to a single IPSec router. For example, this might be used with telecommuters. Extended authentication occurs right after the authentication described in Section on page 245.

In extended authentication, one of the routers (the LAN-Cell or the remote IPSec router) provides a user name and password to the other router, which uses a local user database and/or an external server to verify the user name and password. If the user name or password is wrong, the routers do not establish an IKE SA.

You can set up the LAN-Cell to provide a user name and password to the remote IPSec router, or you can set up the LAN-Cell to check a user name and password that is provided by the remote IPSec router.

Negotiation Mode

There are two negotiation modes: main mode and aggressive mode. Main mode provides better security, while aggressive mode is faster.

Main mode takes six steps to establish an IKE SA.

Steps 1-2: The LAN-Cell sends its proposals to the remote IPSec router. The remote IPSec router selects an acceptable proposal and sends it back to the LAN-Cell.

Steps 3-4: The LAN-Cell and the remote IPSec router participate in a Diffie-Hellman key exchange, based on the accepted DH key group, to establish a shared secret.

Steps 5-6: Finally, the LAN-Cell and the remote IPSec router generate an encryption key from the shared secret, encrypt their identities, and exchange their encrypted identity information for authentication.

In contrast, aggressive mode only takes three steps to establish an IKE SA.

Step 1: The LAN-Cell sends its proposals to the remote IPSec router. It also starts the Diffie-Hellman key exchange and sends its (unencrypted) identity to the remote IPSec router for authentication.

Step 2: The remote IPSec router selects an acceptable proposal and sends it back to the LAN-Cell. It also finishes the Diffie-Hellman key exchange, authenticates the LAN-Cell, and sends its (unencrypted) identity to the LAN-Cell for authentication.

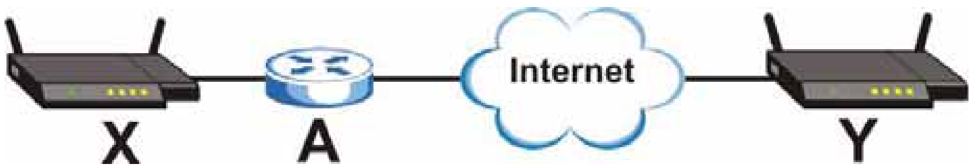
Step 3: The LAN-Cell authenticates the remote IPSec router and confirms that the IKE SA is established.

Aggressive mode does not provide as much security as main mode because the identity of the LAN-Cell and the identity of the remote IPSec router are not encrypted. It is usually used when the address of the initiator is not known by the responder and both parties want to use pre-shared keys for authentication (for example, telecommuters).

VPN, NAT, and NAT Traversal

In the following example, there is another router (**A**) between router **X** and router **Y**.

Figure 151 VPN/NAT Example



If router **A** does NAT, it might change the IP addresses, port numbers, or both. If router **X** and router **Y** try to establish a VPN tunnel, the authentication fails because it depends on this information. The routers cannot establish a VPN tunnel.

Most routers like router **A** now have an IPSec pass-through feature. This feature helps router **A** recognize VPN packets and route them appropriately. If router **A** has this feature, router **X** and router **Y** can establish a VPN tunnel as long as the active protocol is ESP. (See Section on page 252 for more information about active protocols.)

If router A does not have an IPSec pass-through or if the active protocol is AH, you can solve this problem by enabling NAT traversal. In NAT traversal, router **X** and router **Y** add an extra header to the IKE SA and IPSec SA packets. If you configure router **A** to forward these packets unchanged, router **X** and router **Y** can establish a VPN tunnel.

You have to do the following things to set up NAT traversal.

- Enable NAT traversal on the LAN-Cell and remote IPSec router.
- Configure the NAT router to forward packets with the extra header unchanged. (See the field description for detailed information about the extra header.)

The extra header may be UDP port 500 or UDP port 4500, depending on the standard(s) the LAN-Cell and remote IPSec router support.

Additional IPSec VPN Topics

This section discusses other IPSec VPN topics that apply to either IKE SAs or IPSec SAs or both. Relationships between the topics are also highlighted.

SA Life Time

SAs have a lifetime that specifies how long the SA lasts until it times out. When an SA times out, the LAN-Cell automatically renegotiates the SA in the following situations:

- There is traffic when the SA life time expires
- The IPSec SA is configured on the LAN-Cell as nailed up (see below)

Otherwise, the LAN-Cell must re-negotiate the SA the next time someone wants to send traffic.

If the IKE SA times out while an IPSec SA is connected, the IPSec SA stays connected.

An IPSec SA can be set to **nailed up**. Normally, the LAN-Cell drops the IPSec SA when the life time expires or after two minutes of outbound traffic with no inbound traffic. If you set the IPSec SA to nailed up, the LAN-Cell automatically renegotiates the IPSec SA when the SA life time expires, and it does not drop the IPSec SA if there is no inbound traffic.

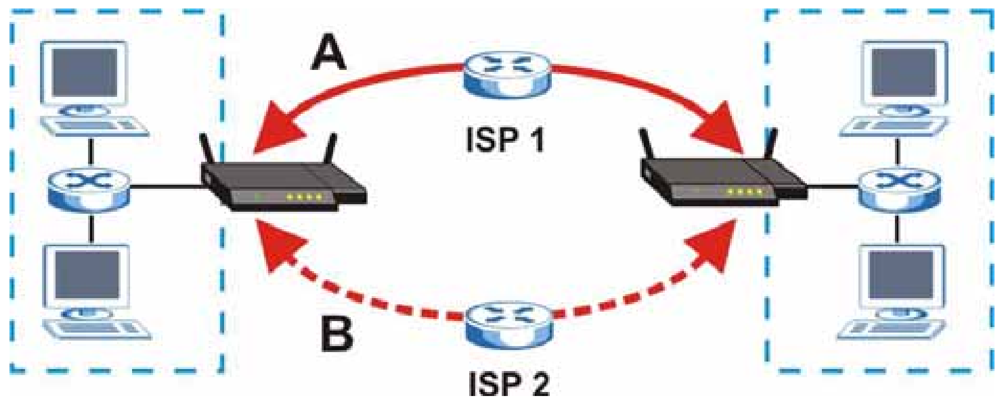
The SA life time and nailed up settings only apply if the rule identifies the remote IPSec router by a static IP address or a domain name. If the **Remote Gateway Address** field is set to **0.0.0.0**, the LAN-Cell cannot initiate the tunnel (and cannot renegotiate the SA).

IPSec High Availability

IPSec high availability (also known as VPN high availability) allows you to use a redundant (backup) VPN connection to another WAN interface on the remote IPSec router if the primary (regular) VPN connection goes down.

In the following figure, if the primary VPN tunnel (A) goes down, the LAN-Cell uses the redundant VPN tunnel (B).

Figure 152 IPSec High Availability



When setting up a IPSec high availability VPN tunnel, the remote IPSec router:

- Must have multiple WAN connections
- Only needs the configure one corresponding IPSec rule
- Should only have IPSec high availability settings in its corresponding IPSec rule if your LAN-Cell has multiple WAN connections

- Should ideally identify itself by a domain name or dynamic domain name (it must otherwise have My Address set to 0.0.0.0)
- Should use a WAN connectivity check to this LAN-Cell's WAN IP address

If the remote IPSec router is not a LAN-Cell, you may also want to avoid setting the IPSec rule to nailed up.

Encryption and Authentication Algorithms

In most LAN-Cells, you can select one of the following encryption algorithms for each proposal. The encryption algorithms are listed here in order from weakest to strongest.

- Data Encryption Standard (DES) is a widely used (but breakable) method of data encryption. It applies a 56-bit key to each 64-bit block of data.
- Triple DES (3DES) is a variant of DES. It iterates three times with three separate keys, effectively tripling the strength of DES.
- Advanced Encryption Standard (AES) is a newer method of data encryption that also uses a secret key. AES applies a 128-bit key to 128-bit blocks of data. It is faster than 3DES.

Use the commands to have the AES encryption apply 192-bit or 256-bit keys to 128-bit blocks of data.

You can select one of the following authentication algorithms for each proposal. The algorithms are listed here in order from weakest to strongest.

- MD5 (Message Digest 5) produces a 128-bit digest to authenticate packet data.
- SHA1 (Secure Hash Algorithm) produces a 160-bit digest to authenticate packet data.

IPSec SA Overview

Once the LAN-Cell and remote IPSec router have established the IKE SA, they can securely negotiate an IPSec SA through which to send data between computers on the networks.

The IPSec SA stays connected even if the underlying IKE SA is not available anymore.

This section introduces the key components of an IPSec SA.

Local Network and Remote Network

In IPSec SA, the local network, the one(s) connected to the LAN-Cell, may be called the local policy. Similarly, the remote network, the one(s) connected to the remote IPSec router, may be called the remote policy.

Virtual Address Mapping

Virtual address mapping (NAT over IPSec) changes the source IP addresses of packets from your local devices to virtual IP addresses before sending them through the VPN tunnel.

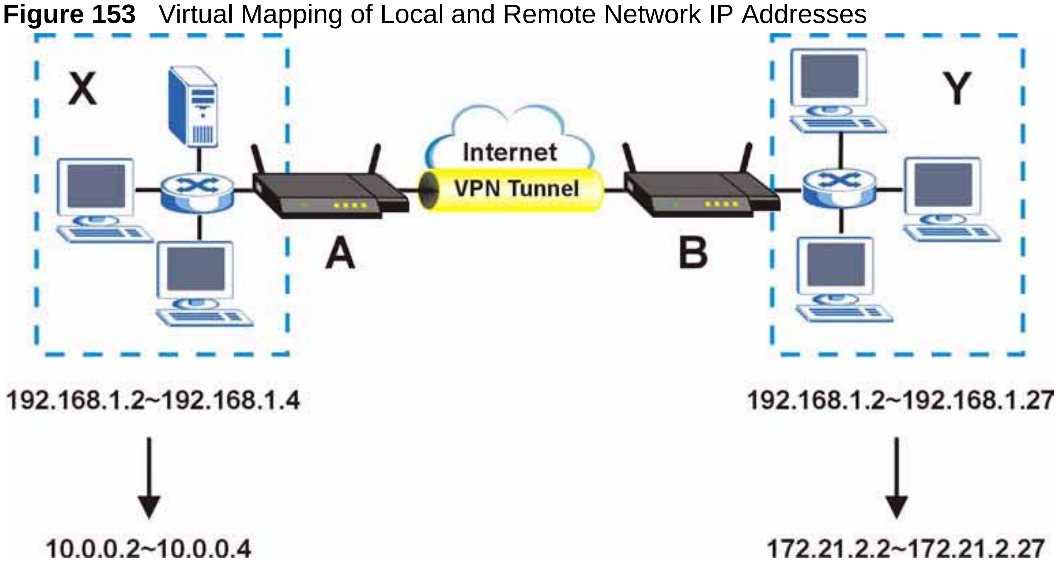
Avoiding Overlapping Local And Remote Network IP Addresses

If both IPSec routers support virtual address mapping, you can access devices on both networks, even if their IP addresses overlap. You map the LAN-Cell's local network addresses to virtual IP addresses and map the remote IPSec router's local IP addresses to other (nonoverlapping) virtual IP addresses.

The following diagram shows an example of using virutal address mapping to avoid overlapping local and remote IP addresses. You can set up virtual address mapping on both IPSec routers to allow computers on network **X** to access network **X** and network **Y** computers with the same IP address.

- You set LAN-Cell **A** to change the source IP addresses of packets from local network **X** (192.168.1.2 to 192.168.1.4) to virtual IP addresses 10.0.0.2 to 10.0.0.4 before sending them through the VPN tunnel.
- You set LAN-Cell **B** to change the source IP addresses of packets from the remote network **Y** (192.168.1.2 to 192.168.1.27) to virtual IP addresses 172.21.2.2 to 172.21.2.27 before sending them through the VPN tunnel.
- On LAN-Cell **A**, you specify 172.21.2.2 to 172.21.2.27 as the remote network. On LAN-Cell **B**, you specify 10.0.0.2 to 10.0.0.4 as the remote network.

Figure 153 Virtual Mapping of Local and Remote Network IP Addresses



Computers on network **X** use IP addresses 192.168.1.2 to 192.168.1.4 to access local network devices and IP addresses 172.21.2.2 to 172.21.2.27 to access the remote network devices.

Computers on network **Y** use IP addresses 192.168.1.2 to 192.168.1.27 to access local network devices and IP addresses 10.0.0.2 to 10.0.0.4 to access the remote network devices.

Active Protocol

The active protocol controls the format of each packet. It also specifies how much of each packet is protected by the encryption and authentication algorithms. IPSec VPN includes two active protocols, AH (Authentication Header, RFC 2402) and ESP (Encapsulating Security Payload, RFC 2406).

The LAN-Cell and remote IPSec router must use the same active protocol.

Usually, you should select ESP. AH does not support encryption, and ESP is more suitable with NAT.

Encapsulation

There are two ways to encapsulate packets. Usually, you should use tunnel mode because it is more secure. Transport mode is only used when the IPSec SA is used for communication between the LAN-Cell and remote IPSec router (for example, for remote management), not between computers on the local and remote networks.

The LAN-Cell and remote IPSec router must use the same encapsulation.

These modes are illustrated below.

Figure 154 VPN: Transport and Tunnel Mode Encapsulation

Original Packet	IP Header	TCP Header	Data		
Transport Mode Packet	IP Header	AH/ESP Header	TCP Header	Data	
Tunnel Mode Packet	IP Header	AH/ESP Header	IP Header	TCP Header	Data

In tunnel mode, the LAN-Cell uses the active protocol to encapsulate the entire IP packet. As a result, there are two IP headers:

- Outside header: The outside IP header contains the IP address of the LAN-Cell or remote IPSec router, whichever is the destination.
- Inside header: The inside IP header contains the IP address of the computer behind the LAN-Cell or remote IPSec router. The header for the active protocol (AH or ESP) appears between the IP headers.

In transport mode, the encapsulation depends on the active protocol. With AH, the LAN-Cell includes part of the original IP header when it encapsulates the packet. With ESP, however, the LAN-Cell does not include the IP header when it encapsulates the packet, so it is not possible to verify the integrity of the source IP address.

IPSec SA Proposal and Perfect Forward Secrecy

An IPSec SA proposal is similar to an IKE SA proposal (see Section on page 244), except that you also have the choice whether or not the LAN-Cell and remote IPSec router perform a new DH key exchange every time an IPSec SA is established. This is called Perfect Forward Secrecy (PFS).

If you enable PFS, the LAN-Cell and remote IPSec router perform a DH key exchange every time an IPSec SA is established, changing the root key from which encryption keys are generated. As a result, if one encryption key is compromised, other encryption keys remain secure.

If you do not enable PFS, the LAN-Cell and remote IPSec router use the same root key that was generated when the IKE SA was established to generate encryption keys.

The DH key exchange is time-consuming and may be unnecessary for data that does not require such security.

IPSec SA Using Manual Keys

You might set up an IPSec SA using manual keys when you want to establish a VPN tunnel quickly, for example, for troubleshooting. You should only do this as a temporary solution, however, because it is not as secure as a regular IPSec SA.

In IPSec SAs using manual keys, the LAN-Cell and remote IPSec router do not establish an IKE SA. They only establish an IPSec SA. As a result, an IPSec SA using manual keys has some characteristics of IKE SA and some characteristics of IPSec SA. There are also some differences between IPSec SA using manual keys and other types of SA.

IPSec SA Proposal Using Manual Keys

In IPSec SA using manual keys, you can only specify one encryption algorithm and one authentication algorithm. You cannot specify several proposals. There is no DH key exchange, so you have to provide the encryption key and the authentication key the LAN-Cell and remote IPSec router use.

The LAN-Cell and remote IPSec router must use the same encryption key and authentication key.

Authentication and the Security Parameter Index (SPI)

For authentication, the LAN-Cell and remote IPSec router use the SPI, instead of pre-shared keys, ID type and content. The SPI is an identification number.

The LAN-Cell and remote IPSec router must use the same SPI.

11

Certificates Screens

11.1 Overview

The LAN-Cell 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.

11.1.1 What You Can Do in the Certificate Screens

- Use the **My Certificate** screens (see Section 11.2 on page 257) to generate and export self-signed certificates or certification requests and import the LAN-Cell's CA-signed certificates.
- Use the **Trusted CA** screens (see Section 11.6 on page 269) to save the certificates of trusted CAs to the LAN-Cell. You can also export the certificates to a computer.
- Use the **Trusted Remote Hosts** screens (see Section 11.9 on page 274) to import selfsigned certificates from trusted remote hosts.
- Use the **Directory Servers** screen (see Section 11.12 on page 279) to configure a list of addresses of directory servers (that contain lists of valid and revoked certificates).

11.1.2 What You Need to Know About Certificates

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 LAN-Cell 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-private 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 LAN-Cell 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 LAN-Cell 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 LAN-Cell 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).

Advantages of Certificates

Certificates offer the following benefits.

- The LAN-Cell 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.

Self-signed Certificates

You can have the LAN-Cell act as a certification authority and sign its own certificates.

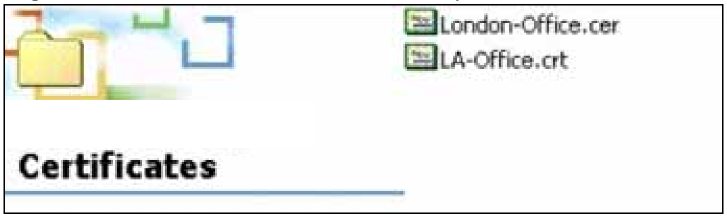
Verifying a Certificate

Before you import a trusted CA or trusted remote host certificate into the LAN-Cell, you should verify that you have the actual certificate. This is especially true of trusted CA certificates since the LAN-Cell also trusts any valid certificate signed by any of the imported trusted CA certificates.

A certificate’s fingerprints are message digests calculated using the MD5 or SHA1 algorithms. You can use a certificate’s fingerprint to verify it. The following procedure describes how to check a certificate’s fingerprint to verify that you have the actual certificate.

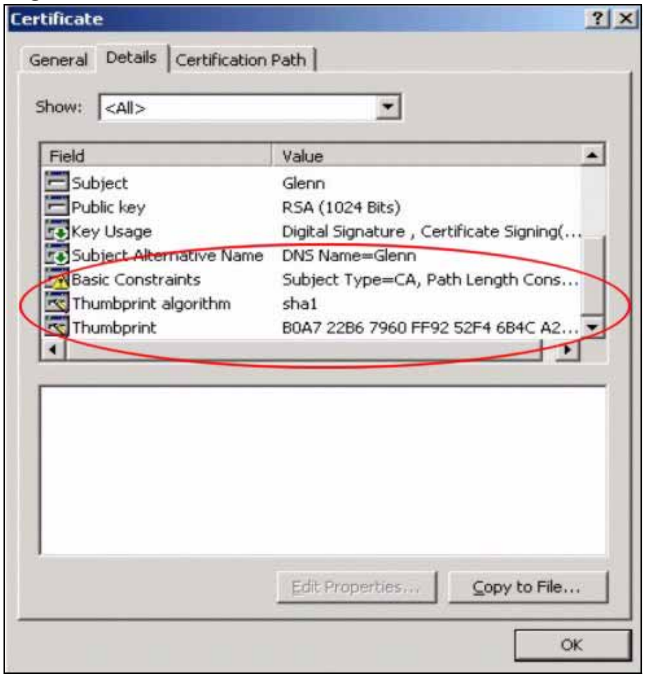
1. Browse to where you have the certificate saved on your computer.
2. Make sure that the certificate has a “.cer” or “.crt” file name extension.

Figure 155 Certificates on Your Computer



3 Double-click the certificate's icon to open the **Certificate** window. Click the **Details** tab and scroll down to the **Thumbprint Algorithm** and **Thumbprint** fields.

Figure 156 Certificate Details

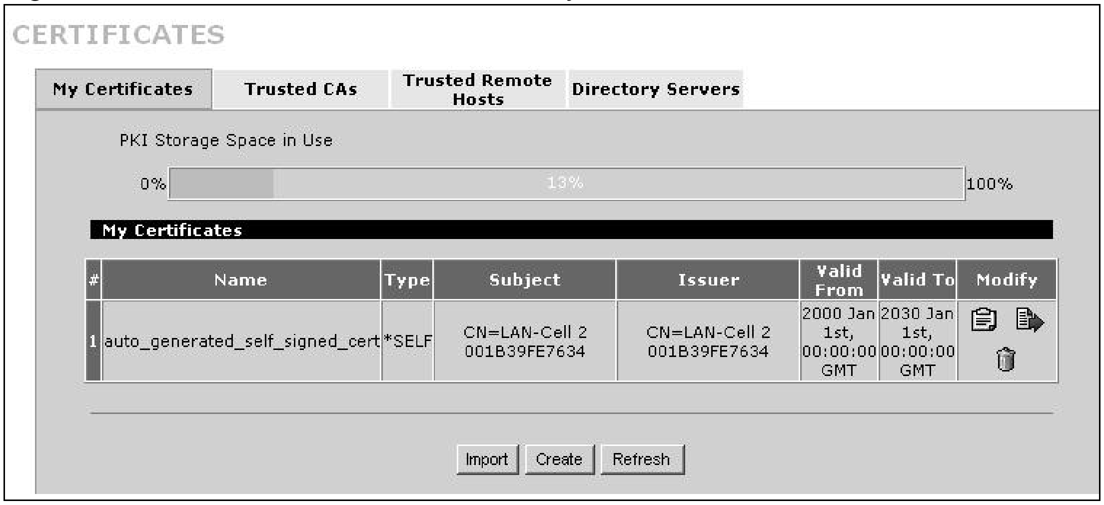


4 Use a secure method to verify that the certificate owner has the same information in the **Thumbprint Algorithm** and **Thumbprint** fields. The secure method may very based on your situation. Possible examples would be over the telephone or through an HTTPS connection.

11.2 My Certificates Screen

Click **SECURITY** > **CERTIFICATES** > **My Certificates** to open the **My Certificates** screen. This is the LAN-Cell's summary list of certificates and certification requests. Certificates display in black and certification requests display in gray.

Figure 157 SECURITY > CERTIFICATES > My Certificates



The following table describes the labels in this screen.

Table 89 SECURITY > CERTIFICATES > My Certificates

LABEL	DESCRIPTION
PKI Storage Space in Use	This bar displays the percentage of the LAN-Cell's PKI storage space that is currently in use. When the storage space is almost full, you should consider deleting expired or unnecessary certificates before adding more certificates.
Replace	This button displays when the LAN-Cell has the factory default certificate. The factory default certificate is common to all LAN-Cells that use certificates. Proxicast recommends that you use this button to replace the factory default certificate with one that uses your LAN-Cell's MAC address.
#	This field displays the certificate index number. The certificates are listed in alphabetical order.
Name	This field displays the name used to identify this certificate. It is recommended that you give each certificate a unique name.
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 LAN-Cell 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.
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.

Table 89 SECURITY > CERTIFICATES > My Certificates (continued)

LABEL	DESCRIPTION
Modify	Click the details icon to open a screen with an in-depth list of information about the certificate (or certification request). Click the export icon to save the certificate to a computer. For a certification request, click the export icon and then **Save** in the **File Download** screen. The **Save As** screen opens, browse to the location that you want to use and click **Save**. Click the delete icon to remove the certificate (or certification request). A window displays asking you to confirm that you want to delete the certificate. You cannot delete a certificate that one or more features is configured to use. Do the following to delete a certificate that shows ***SELF** in the **Type** field. 1. Make sure that no other features, such as HTTPS, VPN, SSH are configured to use the ***SELF** certificate. 2. Click the details icon next to another self-signed certificate (see the description on the **Create** button if you need to create a self-signed certificate). 3. Select the **Default self-signed certificate which signs the imported remote host certificates** check box. 4. Click **Apply** to save the changes and return to the **My Certificates** screen. 5. The certificate that originally showed ***SELF** displays **SELF** and you can delete it now. Note that subsequent certificates move up by one when you take this action
Import	Click **Import** to open a screen where you can save the certificate that you have enrolled from a certification authority from your computer to the LAN-Cell.
Create	Click **Create** to go to the screen where you can have the LAN-Cell generate a certificate or a certification request.
Refresh	Click **Refresh** to display the current validity status of the certificates.

11.2.1 My Certificate Details Screen

Click **SECURITY** > **CERTIFICATES** > **My Certificates** to open the **My Certificates** screen (see Figure 157 on page 258). Click the details icon to open the **My Certificate Details** screen. You can use this screen to view in-depth certificate information and change the certificate’s name.

If it is a self-signed certificate, you can also set the LAN-Cell to use the certificate to sign the imported trusted remote host certificates.

Figure 158 SECURITY > CERTIFICATES > My Certificates > Details

The following table describes the labels in this screen.

Table 90 SECURITY > CERTIFICATES > My Certificates > Details

LABEL	DESCRIPTION
Name	This field displays the identifying name of this certificate. If you want to change the name, type up to 31 characters to identify this certificate. You may use any character (not including spaces).
Property Default self-signed certificate which signs the imported remote host certificates.	Select this check box to have the LAN-Cell use this certificate to sign the trusted remote host certificates that you import to the LAN-Cell. This check box is only available with self-signed certificates. If this check box is already selected, you cannot clear it in this screen, you must select this check box in another self-signed certificate's details screen. This automatically clears the check box in the details screen of the certificate that was previously set to sign the imported trusted remote host certificates.

Table 90 SECURITY > CERTIFICATES > My Certificates > Details (continued)

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

Table 90 SECURITY > CERTIFICATES > My Certificates > Details (continued)

LABEL	DESCRIPTION
SHA1 Fingerprint	This is the certificate's message digest that the LAN-Cell calculated using the SHA1 algorithm.
Certificate in PEM (Base-64) Encoded Format	This read-only text box displays the certificate or certification request in Privacy Enhanced Mail (PEM) format. PEM uses 64 ASCII characters to convert the binary certificate into a printable form. You can copy and paste a certification request into a certification authority's web page, an e-mail that you send to the certification authority or a text editor and save the file on a management computer for later manual enrollment. You can copy and paste a certificate into an e-mail to send to friends or colleagues or you can copy and paste a certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example).
Apply	Click **Apply** to save your changes back to the LAN-Cell. You can only change the name, except in the case of a self-signed certificate, which you can also set to be the default self-signed certificate that signs the imported trusted remote host certificates.
Cancel	Click **Cancel** to quit and return to the **My Certificates** screen.

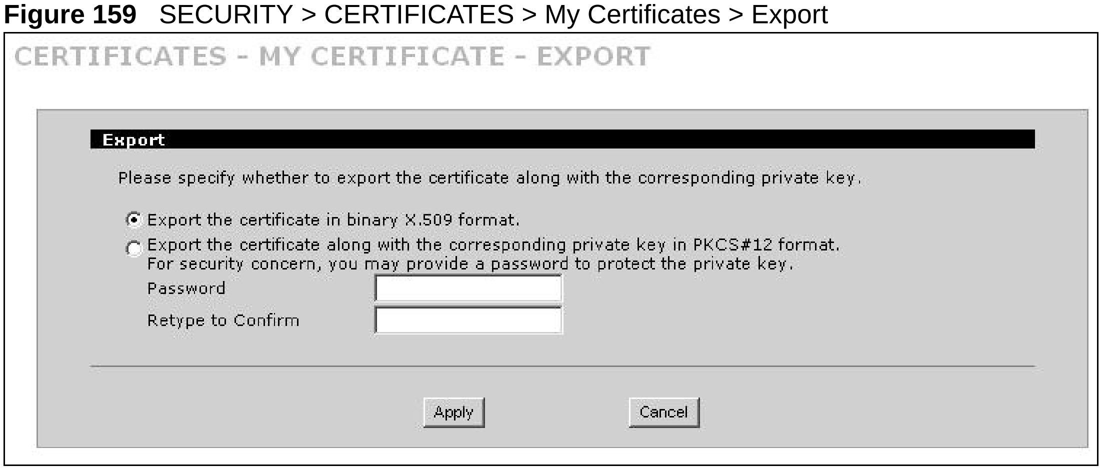
11.3 My Certificate Export Screen

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

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

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

Figure 159 SECURITY > CERTIFICATES > My Certificates > Export



The following table describes the labels in this screen.

Table 91 SECURITY > CERTIFICATES > My Certificates > Export

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

11.4 My Certificate Import Screen

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

You can only import a certificate that matches a corresponding certification request that was generated by the LAN-Cell (the certification request contains the private key). The certificate you import replaces the corresponding request in the **My Certificates** screen.

One exception is that you can import a PKCS#12 format certificate without a corresponding certification request since the certificate includes the private key.

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

Certificate File Formats

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

- Binary X.509: This is an ITU-T recommendation that defines the formats for X.509 certificates.
- PEM (Base-64) encoded X.509: This Privacy Enhanced Mail format uses 64 ASCII characters to convert a binary X.509 certificate into a printable form.
- Binary PKCS#7: This is a standard that defines the general syntax for data (including digital signatures) that may be encrypted. The LAN-Cell currently allows the importation of a PKS#7 file that contains a single certificate.

- PEM (Base-64) encoded PKCS#7: This Privacy Enhanced Mail (PEM) format uses 64 ASCII characters to convert a binary PKCS#7 certificate into a printable form.
- Binary PKCS#12: This is a format for transferring public key and private key certificates. The private key in a PKCS #12 file is within a password-encrypted envelope. The file's password is not connected to your certificate's public or private passwords. Exporting a PKCS #12 file creates this and you must provide it to decrypt the contents when you import the file into the LAN-Cell.

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

Figure 160 SECURITY > CERTIFICATES > My Certificates > Import

The following table describes the labels in this screen.

Table 92 SECURITY > CERTIFICATES > My Certificates > Import

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

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

Figure 161 SECURITY > CERTIFICATES > My Certificates > Import: PKCS#12

The following table describes the labels in this screen.

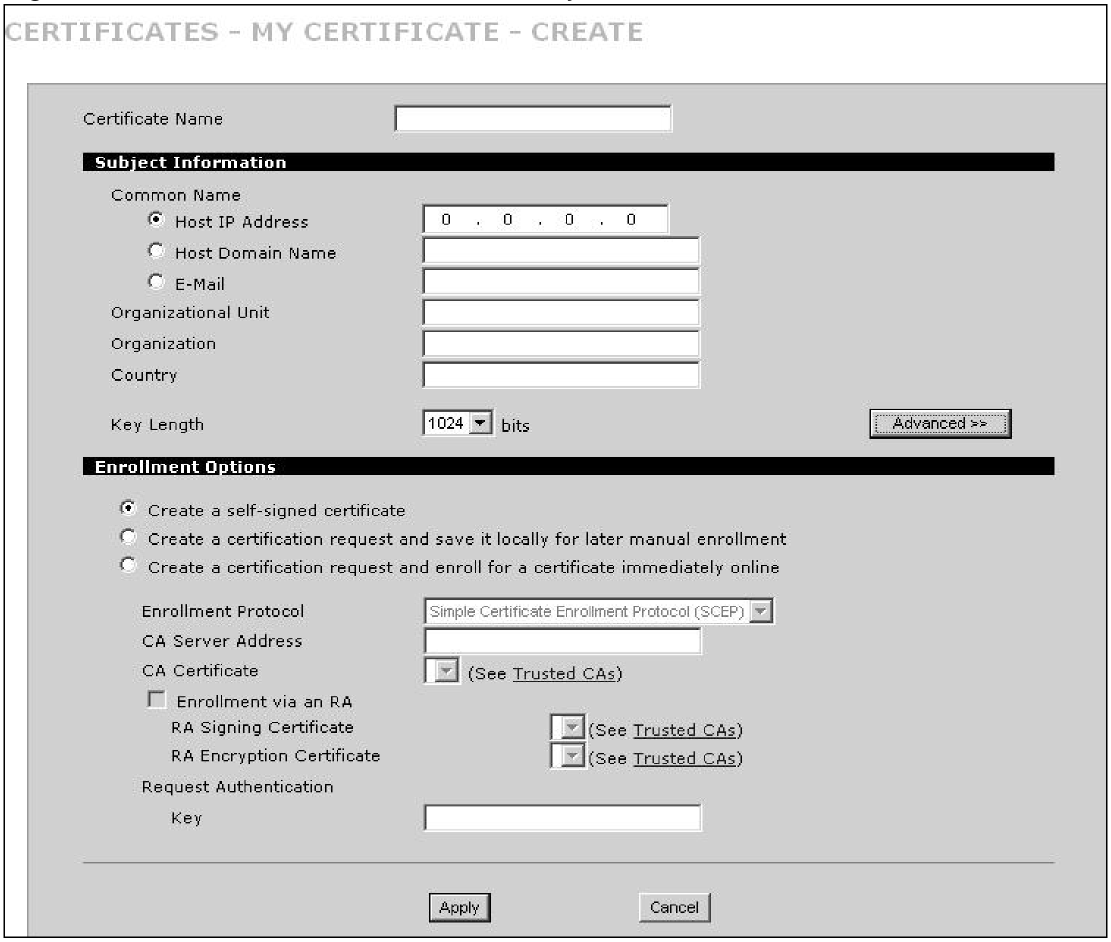
Table 93 SECURITY > CERTIFICATES > My Certificates > Import: PKCS#12

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

11.5 My Certificate Create Screen

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

Figure 162 SECURITY > CERTIFICATES > My Certificates > Create



The following table describes the labels in this screen.

Table 94 SECURITY > CERTIFICATES > My Certificates > Create

LABEL	DESCRIPTION
Certificate Name	Type up to 31 ASCII characters (not including spaces) to identify this certificate.
Subject Information	Use these fields to record information that identifies the owner of the certificate. You do not have to fill in every field, although the **Common Name** is mandatory. The certification authority may add fields (such as a serial number) to the subject information when it issues a certificate. It is recommended that each certificate have unique subject information.
Common Name	Select a radio button to identify the certificate’s owner by IP address, domain name or e-mail address. Type the IP address (in dotted decimal notation), domain name or e-mail address in the field provided. The domain name or e-mail address can be up to 31 ASCII characters. The domain name or e-mail address is for identification purposes only and can be any string.
Organizational Unit	Type up to 127 characters to identify the organizational unit or department to which the certificate owner belongs. You may use any character, including spaces, but the LAN-Cell drops trailing spaces.
Organization	Type up to 127 characters to identify the company or group to which the certificate owner belongs. You may use any character, including spaces, but the LAN-Cell drops trailing spaces.

Table 94 SECURITY > CERTIFICATES > My Certificates > Create (continued)

LABEL	DESCRIPTION
Country	Type up to 127 characters to identify the nation where the certificate owner is located. You may use any character, including spaces, but the LAN-Cell drops trailing spaces.
Key Length	Select a number from the drop-down list box to determine how many bits the key should use (512 to 2048). The longer the key, the more secure it is. A longer key also uses more PKI storage space.
The fields below display when you click **Advanced >>.**	
Subject Name	You must configure at least one of these fields. Select an item from the drop-down list box and enter the corresponding information in the field to the right. **SN** (serial number) - select this and enter the certificate's identification number, such as the LAN-Cell's MAC address. You can use up to 63 characters. **CN** (common name) - select this and enter a name to identify the owner of the certificate. You can use up to 63 characters. **OU** (organizational unit) - select this and enter a unit within the organization to identify the owner of the certificate. You can use up to 63 characters. **O** (organization) - select this and enter an organization to identify the owner of the certificate. You can use up to 63 characters. **DC** (domain component) - select this and enter the domain component of a domain to identify the owner of the certificate. For example, if the domain is proxicast.com, the domain component is "proxicast" or "com". You can use up to 63 characters. **L** (locality name) - select this and enter the place where the owner of the certificate resides, such as a city or county. You can use up to 63 characters. **ST** (state or province name) - select this and enter the state or province in which the owner of the certificate resides. You can use up to 63 characters. **C** (country) - select this and enter the name of the country at which the owner of the certificate resides. You can use up to 63 characters. **unstructuredName** (PKCS 9 unname) - select this and enter the name of the owner of the certificate as an unstructured ASCII string. You can use up to 63 characters. Check with the certificate's issuing certification authority for their interpretation in this field if you select to apply to a certification authority for a certificate. **unstructuredAddress** (PKCS 9 unaddr) - select this and enter the address of the owner of the certificate as an unstructured ASCII string. You can use up to 63 characters. Check with the certificate's issuing certification authority for their interpretation in this field if you select to apply to a certification authority for a certificate. **MAILTO** (PKCS 9 email address) - select this and enter the email address of the owner of the certificate. You can use up to 63 characters. Check with the certificate's issuing certification authority for their interpretation in this field if you select to apply to a certification authority for a certificate.
Subject Alternative Name	Select a radio button to identify the certificate's owner by IP address, domain name or e-mail address. Type the IP address (in dotted decimal notation), domain name or e-mail address in the field provided. The domain name or e-mail address can be up to 31 ASCII characters. The domain name or e-mail address is for identification purposes only and can be any string.
Enrollment Options	These radio buttons deal with how and when the certificate is to be generated.
Create a self-signed certificate	Select **Create a self-signed certificate** to have the LAN-Cell generate the certificate and act as the Certification Authority (CA) itself. This way you do not need to apply to a certification authority for certificates.

Table 94 SECURITY > CERTIFICATES > My Certificates > Create (continued)

LABEL	DESCRIPTION
Create a certification request and save it locally for later manual enrollment	Select **Create a certification request and save it locally for later manual enrollment** to have the LAN-Cell generate and store a request for a certificate. Use the **My Certificate Details** screen to view the certification request and copy it to send to the certification authority. Copy the certification request from the **My Certificate Details** screen (see Section 11.2.1 on page 259) and then send it to the certification authority.
Create a certification request and enroll for a certificate immediately online	Select **Create a certification request and enroll for a certificate immediately online** to have the LAN-Cell generate a request for a certificate and apply to a certification authority for a certificate. You must have the certification authority's certificate already imported in the **Trusted CAs** screen. When you select this option, you must select the certification authority's enrollment protocol and the certification authority's certificate from the drop-down list boxes and enter the certification authority's server address. You also need to fill in the **Reference Number** and **Key** if the certification authority requires them.
Enrollment Protocol	Select the certification authority's enrollment protocol from the drop-down list box. **Simple Certificate Enrollment Protocol (SCEP)** is a TCP-based enrollment protocol that was developed by VeriSign and Cisco. **Certificate Management Protocol (CMP)** is a TCP-based enrollment protocol that was developed by the Public Key Infrastructure X.509 working group of the Internet Engineering Task Force (IETF) and is specified in RFC 2510.
CA Server Address	Enter the IP address (or URL) of the certification authority server.
CA Certificate	Select the certification authority's certificate from the **CA Certificate** drop-down list box. You must have the certification authority's certificate already imported in the **Trusted CAs** screen. Click **Trusted CAs** to go to the **Trusted CAs** screen where you can view (and manage) the LAN-Cell's list of certificates of trusted certification authorities.
Enrollment via an RA	If you select **Create a certification request and enroll for a certificate immediately online**, you can select this option to apply for a certificate through a RA (Registration Authority). The RA is an intermediary authorized by a CA to verify each subscriber's identity and forward the requests to the CA. After the CA signs and issues the certificates, the RA distributes the certificates to the subscribers.
RA Signing Certificate	If you select **Enrollment via an RA**, select the CA's RA signing certificate from the drop-down list box. You must have the certificate already imported in the **Trusted CAs** screen. Click **Trusted CAs** to go to the **Trusted CAs** screen where you can view (and manage) the LAN-Cell's list of certificates of trusted certification authorities.
RA Encryption Certificate	If you select **Enrollment via an RA**, select the CA's RA encryption certificate from the drop-down list box. You must have the certificate already imported in the **Trusted CAs** screen. Click **Trusted CAs** to go to the **Trusted CAs** screen where you can view (and manage) the LAN-Cell's list of certificates of trusted certification authorities.
Request Authentication	When you select **Create a certification request and enroll for a certificate immediately online**, the certification authority may want you to include a reference number and key to identify you when you send a certification request. Fill in both the **Reference Number** and the **Key** fields if your certification authority uses CMP enrollment protocol. Just fill in the **Key** field if your certification authority uses the SCEP enrollment protocol.
Key	Type the key that the certification authority gave you.

Table 94 SECURITY > CERTIFICATES > My Certificates > Create (continued)

LABEL	DESCRIPTION
Apply	Click **Apply** to begin certificate or certification request generation.
Cancel	Click **Cancel** to quit and return to the **My Certificates** screen.

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

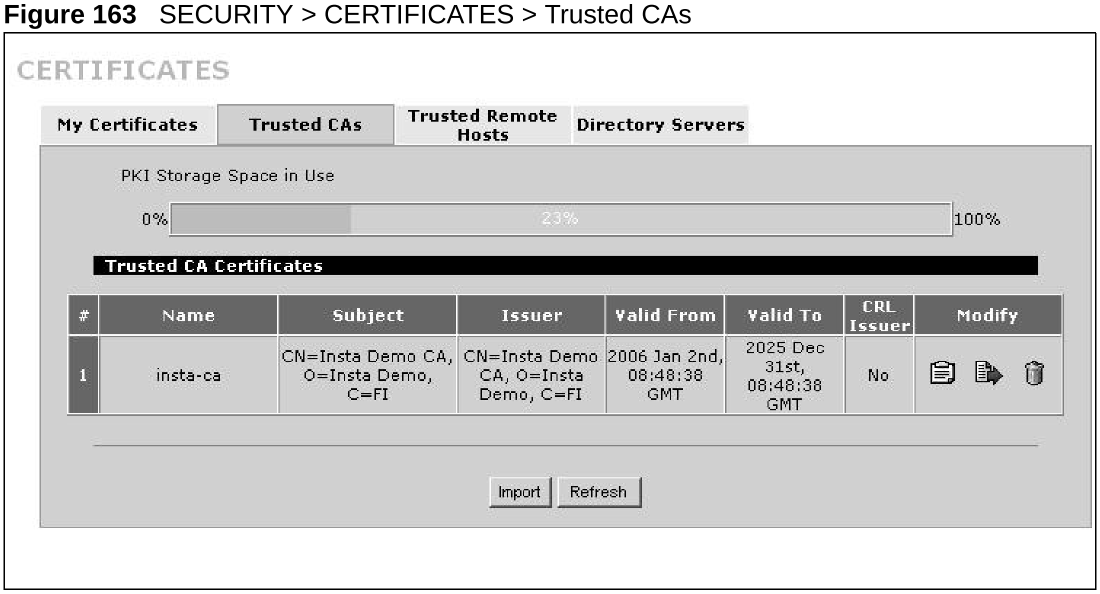
After the LAN-Cell successfully enrolls a certificate or generates a certification request or a self-signed certificate, you see a screen with a **Return** button that takes you back to the **My Certificates** screen.

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

11.6 Trusted CAs Screen

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

Figure 163 SECURITY > CERTIFICATES > Trusted CAs



The following table describes the labels in this screen.

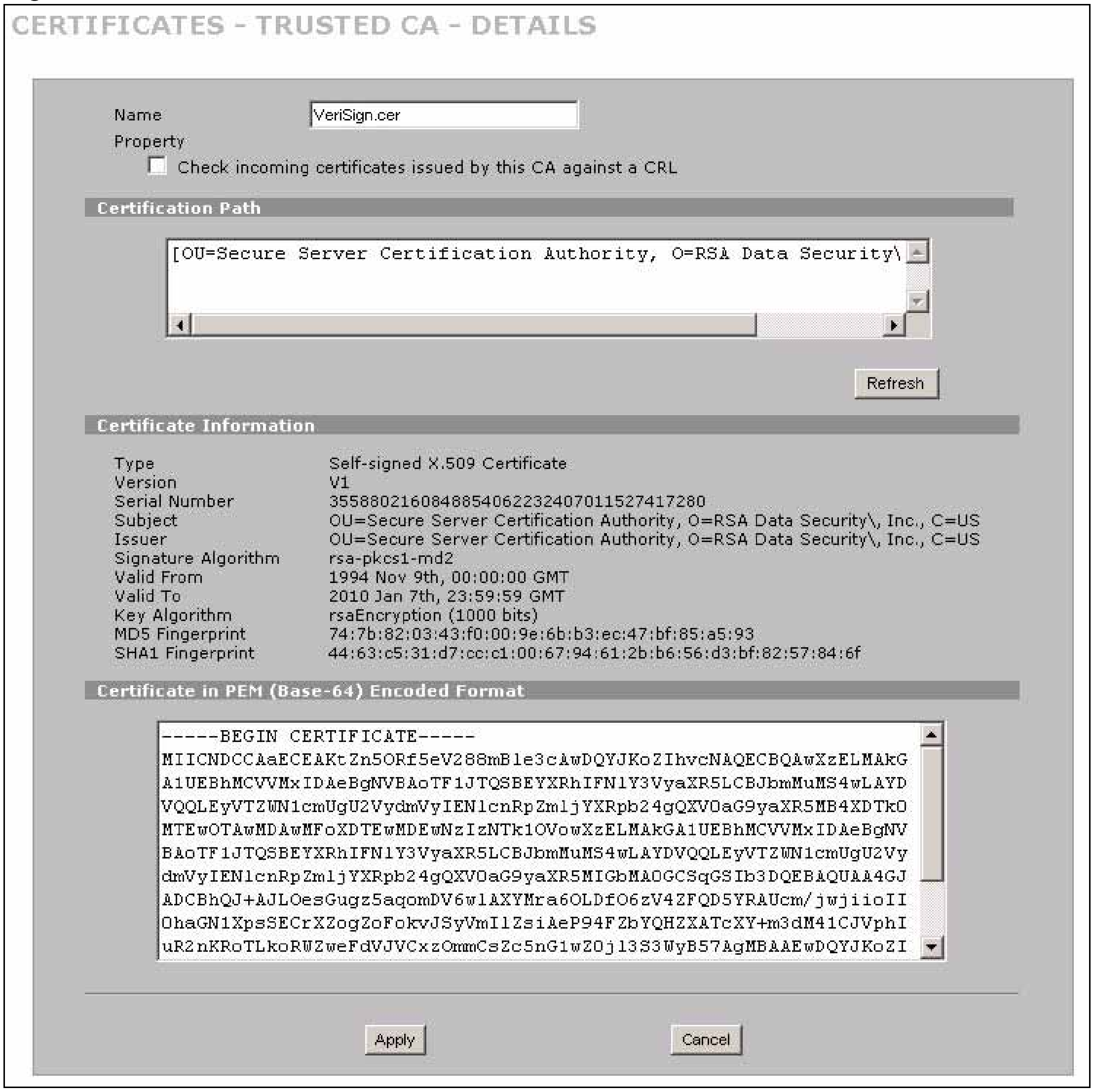
Table 95 SECURITY > CERTIFICATES > Trusted CAs

LABEL	DESCRIPTION
PKI Storage Space in Use	This bar displays the percentage of the LAN-Cell's PKI storage space that is currently in use. When the storage space is almost full, you should consider deleting expired or unnecessary certificates before adding more certificates.
#	This field displays the certificate index number. The certificates are listed in alphabetical order.
Name	This field displays the name used to identify this certificate.
Subject	This field displays identifying information about the certificate's owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). It is recommended that each certificate have unique subject information.
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as a common name, organizational unit or department, organization or company and country. With self-signed certificates, this is the same information as in the **Subject** field.
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.
CRL Issuer	This field displays Yes if the certification authority issues Certificate Revocation Lists for the certificates that it has issued and you have selected the **Issues certificate revocation lists (CRL)** check box in the certificate's details screen to have the LAN-Cell check the CRL before trusting any certificates issued by the certification authority. Otherwise the field displays "No".
Modify	Click the details icon to open a screen with an in-depth list of information about the certificate. Use the export icon to save the certificate to a computer. Click the icon and then **Save** in the **File Download** screen. The **Save As** screen opens, browse to the location that you want to use and click **Save**. Click the delete icon to remove the certificate. A window displays asking you to confirm that you want to delete the certificates. Note that subsequent certificates move up by one when you take this action.
Import	Click **Import** to open a screen where you can save the certificate of a certification authority that you trust, from your computer to the LAN-Cell.
Refresh	Click this button to display the current validity status of the certificates.

11.7 Trusted CA Details Screen

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

Figure 164 SECURITY > CERTIFICATES > Trusted CAs > Details



The following table describes the labels in this screen.

Table 96 SECURITY > CERTIFICATES > Trusted CAs > Details

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

Table 96 SECURITY > CERTIFICATES > Trusted CAs > Details (continued)

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

Table 96 SECURITY > CERTIFICATES > Trusted CAs > Details (continued)

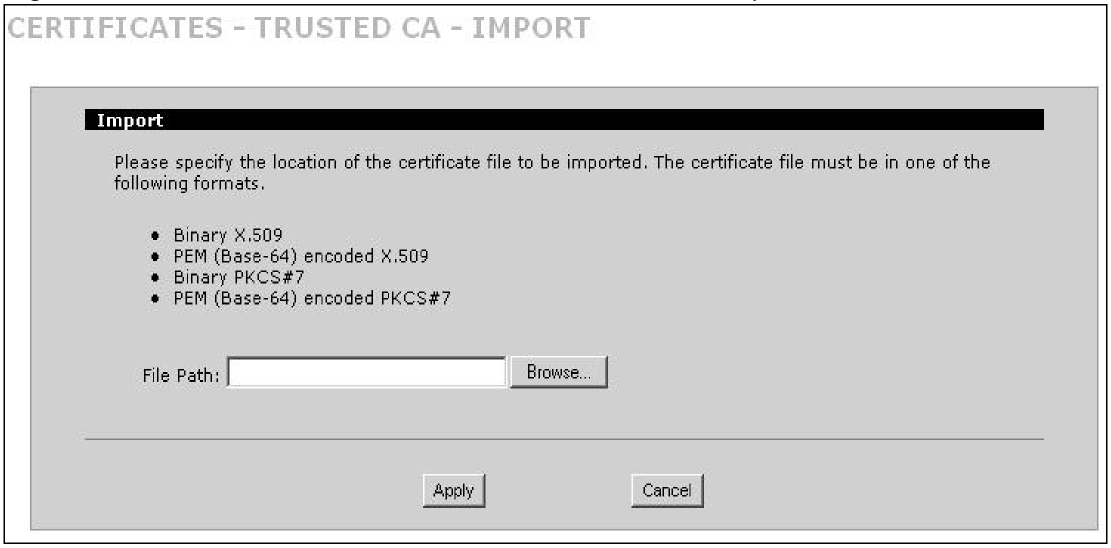
LABEL	DESCRIPTION
CRL Distribution Points	This field displays how many directory servers with Lists of revoked certificates the issuing certification authority of this certificate makes available. This field also displays the domain names or IP addresses of the servers.
MD5 Fingerprint	This is the certificate's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

11.8 Trusted CA Import Screen

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

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

Figure 165 SECURITY > CERTIFICATES > Trusted CAs > Import



The following table describes the labels in this screen.

Table 97 SECURITY > CERTIFICATES > Trusted CAs Import

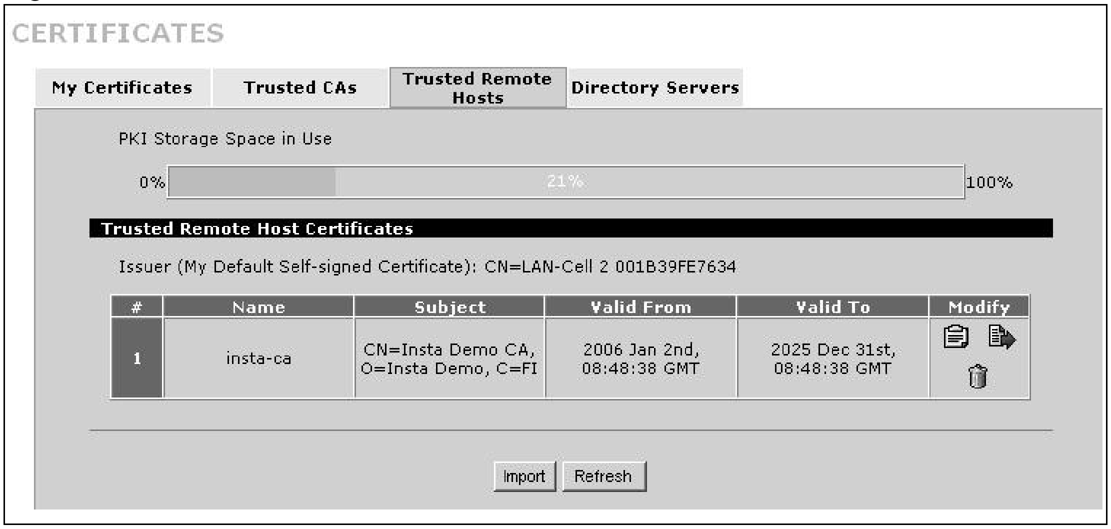
LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click **Browse** to find it.
Browse	Click **Browse** to find the certificate file you want to upload.
Apply	Click **Apply** to save the certificate on the LAN-Cell.
Cancel	Click **Cancel** to quit and return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

11.9 Trusted Remote Hosts Screen

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

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

Figure 166 SECURITY > CERTIFICATES > Trusted Remote Hosts



The following table describes the labels in this screen.

Table 98 SECURITY > CERTIFICATES > Trusted Remote Hosts

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

11.10 Trusted Remote Hosts Import Screen

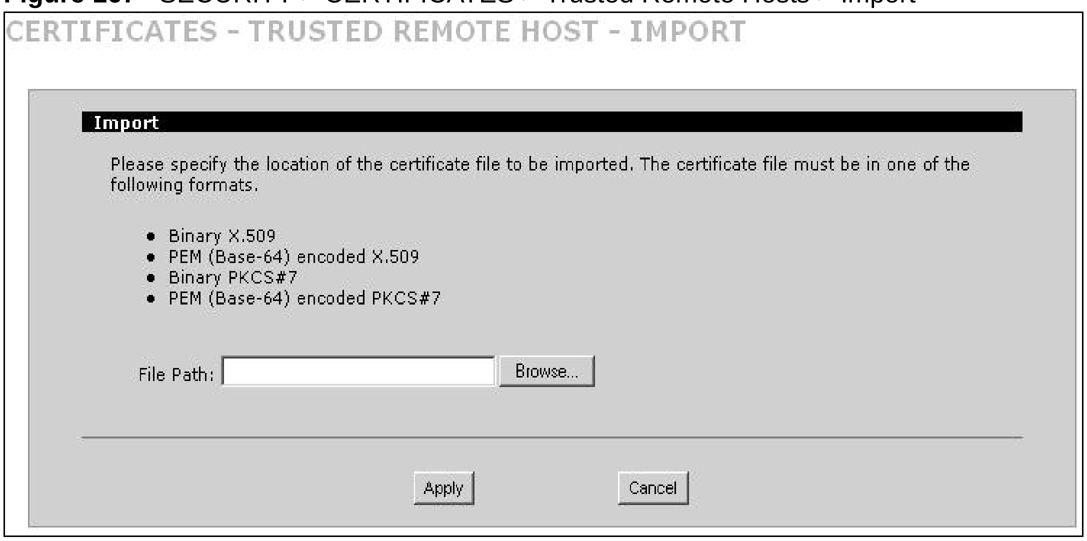
Click **SECURITY** > **CERTIFICATES** > **Trusted Remote Hosts** to open the **Trusted Remote Hosts** screen and then click **Import** to open the **Trusted Remote Host Import** screen.

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

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

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

Figure 167 SECURITY > CERTIFICATES > Trusted Remote Hosts > Import



The following table describes the labels in this screen.

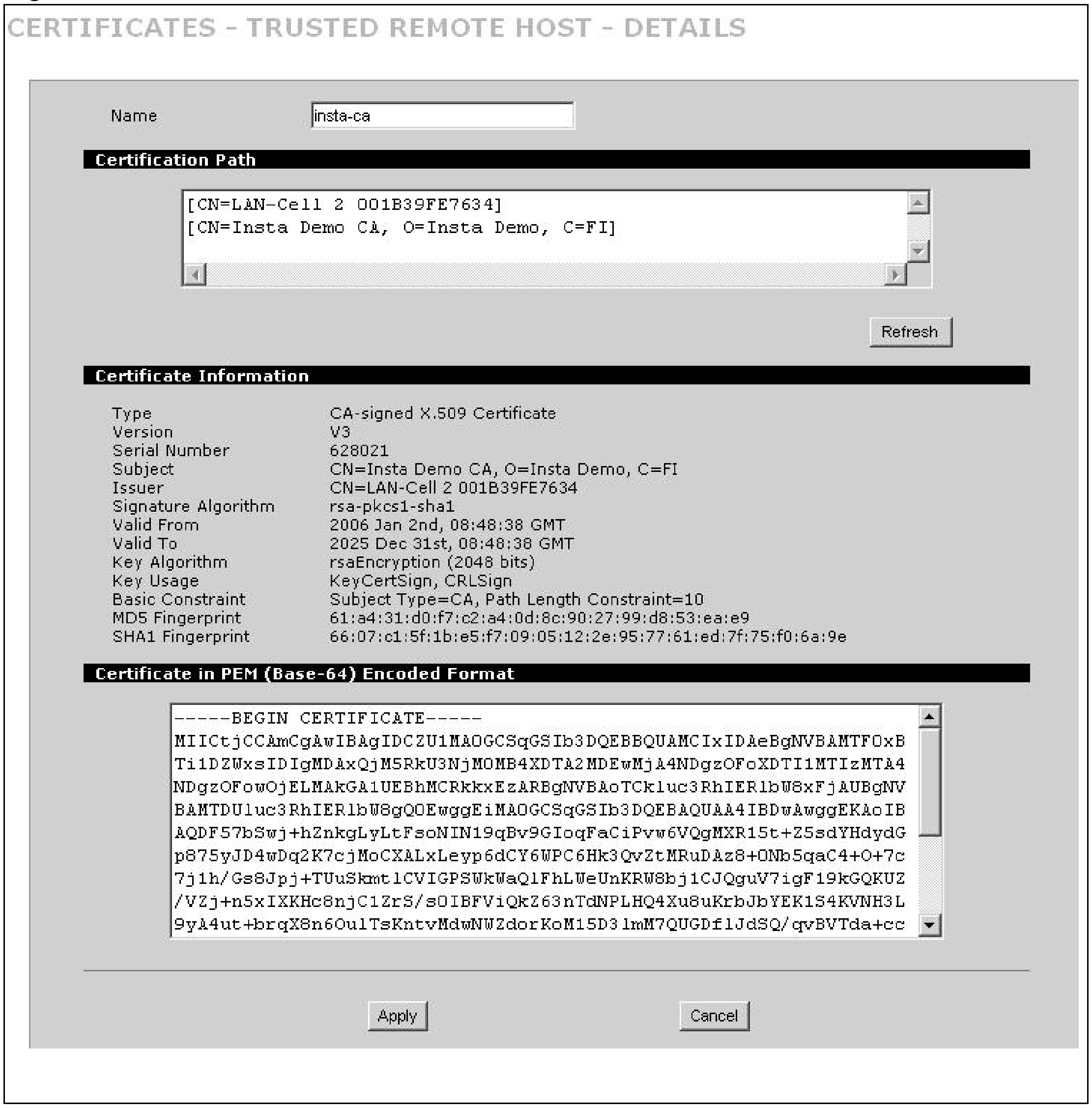
Table 99 SECURITY > CERTIFICATES > Trusted Remote Hosts > Import

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

11.11 Trusted Remote Host Certificate Details Screen

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

Figure 168 SECURITY > CERTIFICATES > Trusted Remote Hosts > Details



The following table describes the labels in this screen.

Table 100 SECURITY > CERTIFICATES > Trusted Remote Hosts > Details

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

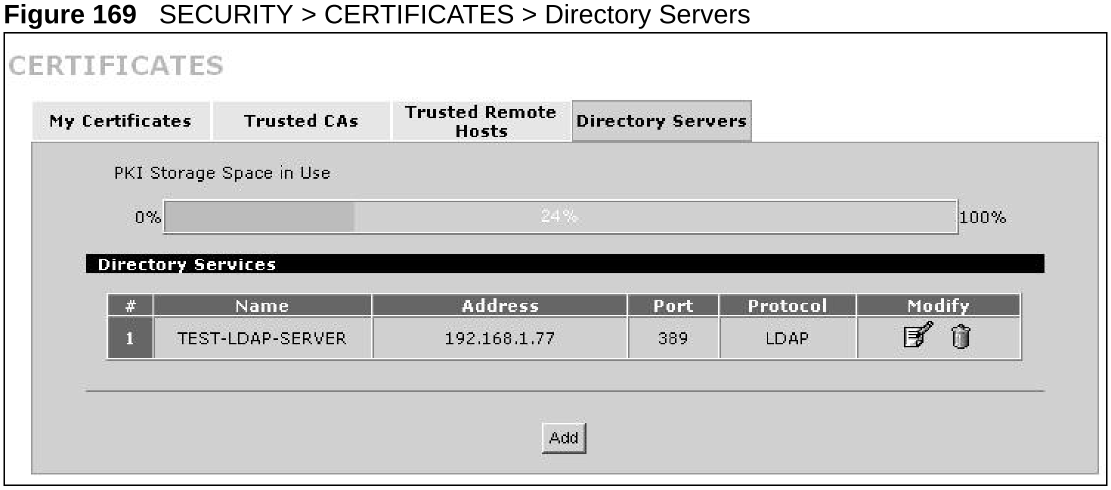
Table 100 SECURITY > CERTIFICATES > Trusted Remote Hosts > Details (continued)

LABEL	DESCRIPTION
MD5 Fingerprint	This is the certificate's message digest that the LAN-Cell calculated using the MD5 algorithm. The LAN-Cell uses one of its own self-signed certificates to sign the imported trusted remote host certificates. This changes the fingerprint value displayed here (so it does not match the original). See Section on page 256 for how to verify a remote host's certificate before you import it into the LAN-Cell.
SHA1 Fingerprint	This is the certificate's message digest that the LAN-Cell calculated using the SHA1 algorithm. The LAN-Cell uses one of its own self-signed certificates to sign the imported trusted remote host certificates. This changes the fingerprint value displayed here (so it does not match the original). See Section on page 256 for how to verify a remote host's certificate before you import it into the LAN-Cell.
Certificate in PEM (Base-64) Encoded Format	This read-only text box displays the certificate or certification request in Privacy Enhanced Mail (PEM) format. PEM uses 64 ASCII characters to convert the binary certificate into a printable form. You can copy and paste the certificate into an e-mail to send to friends or colleagues or you can copy and paste the certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example).
Apply	Click **Apply** to save your changes back to the LAN-Cell. You can only change the name of the certificate.
Cancel	Click **Cancel** to quit configuring this screen and return to the **Trusted Remote Hosts** screen.

11.12 Directory Servers Screen

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

Figure 169 SECURITY > CERTIFICATES > Directory Servers



The following table describes the labels in this screen.

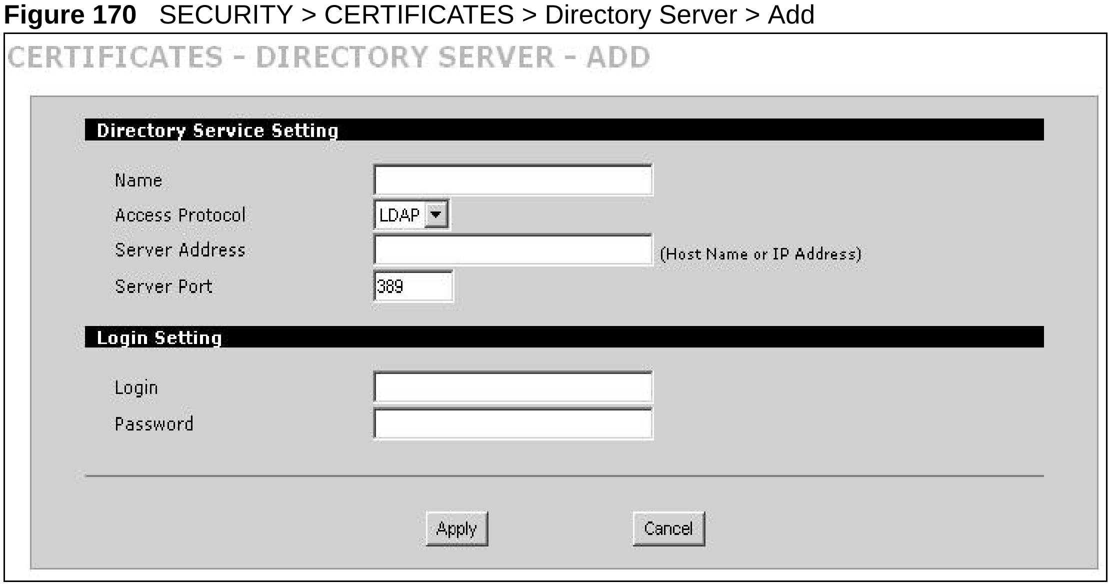
Table 101 SECURITY > CERTIFICATES > Directory Servers

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

11.13 Directory Server Add or Edit Screen

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

Figure 170 SECURITY > CERTIFICATES > Directory Server > Add



The following table describes the labels in this screen.

Table 102 SECURITY > CERTIFICATES > Directory Server > Add

LABEL	DESCRIPTION
Directory Service Setting	
Name	Type up to 31 ASCII characters (spaces are not permitted) to identify this directory server.
Access Protocol	Use the drop-down list box to select the access protocol used by the directory server. **LDAP** (Lightweight Directory Access Protocol) is a protocol over TCP that specifies how clients access directories of certificates and lists of revoked certificates.[A]
Server Address	Type the IP address (in dotted decimal notation) or the domain name of the directory server.
Server Port	This field displays the default server port number of the protocol that you select in the **Access Protocol** field. You may change the server port number if needed, however you must use the same server port number that the directory server uses. 389 is the default server port number for LDAP.
Login Setting	
Login	The LAN-Cell may need to authenticate itself in order to assess the directory server. Type the login name (up to 31 ASCII characters) from the entity maintaining the directory server (usually a certification authority).
Password	Type the password (up to 31 ASCII characters) from the entity maintaining the directory server (usually a certification authority).
Apply	Click **Apply** to save your changes back to the LAN-Cell.
Cancel	Click **Cancel** to quit configuring this screen and return to the **Directory Servers** screen.

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

12

Authentication Server Screens

12.1 Overview

This chapter discusses how to configure the LAN-Cell's authentication server feature.

A LAN-Cell set to be a VPN extended authentication server can use either the local user database internal to the LAN-Cell or an external RADIUS server for an unlimited number of users. The LAN-Cell uses the same local user database for VPN extended authentication and wireless LAN security. See Appendix E on page 617 for more information about RADIUS.

12.1.1 What You Can Do in the Authentication Server Screens

- Use the **Local User Database** Screen (Section 12.2 on page 284) to configure your LAN-Cell's list of local user profiles.
- Use the **RADIUS** Screen (Section 12.3 on page 285) to configure external RADIUS server settings.

12.1.2 What You Need To Know About Authentication Server

Local User Database

By storing user profiles locally on the LAN-Cell, your LAN-Cell is able to authenticate users without interacting with a network RADIUS server. However, there is a limit on the number of users you may authenticate in this way.

RADIUS

The LAN-Cell can use an external RADIUS server to authenticate an unlimited number of users. RADIUS is based on a client-server model that supports authentication and accounting, where access point is the client and the server is the RADIUS server.

- • Authentication

  Determines the identity of the users.
- • Accounting

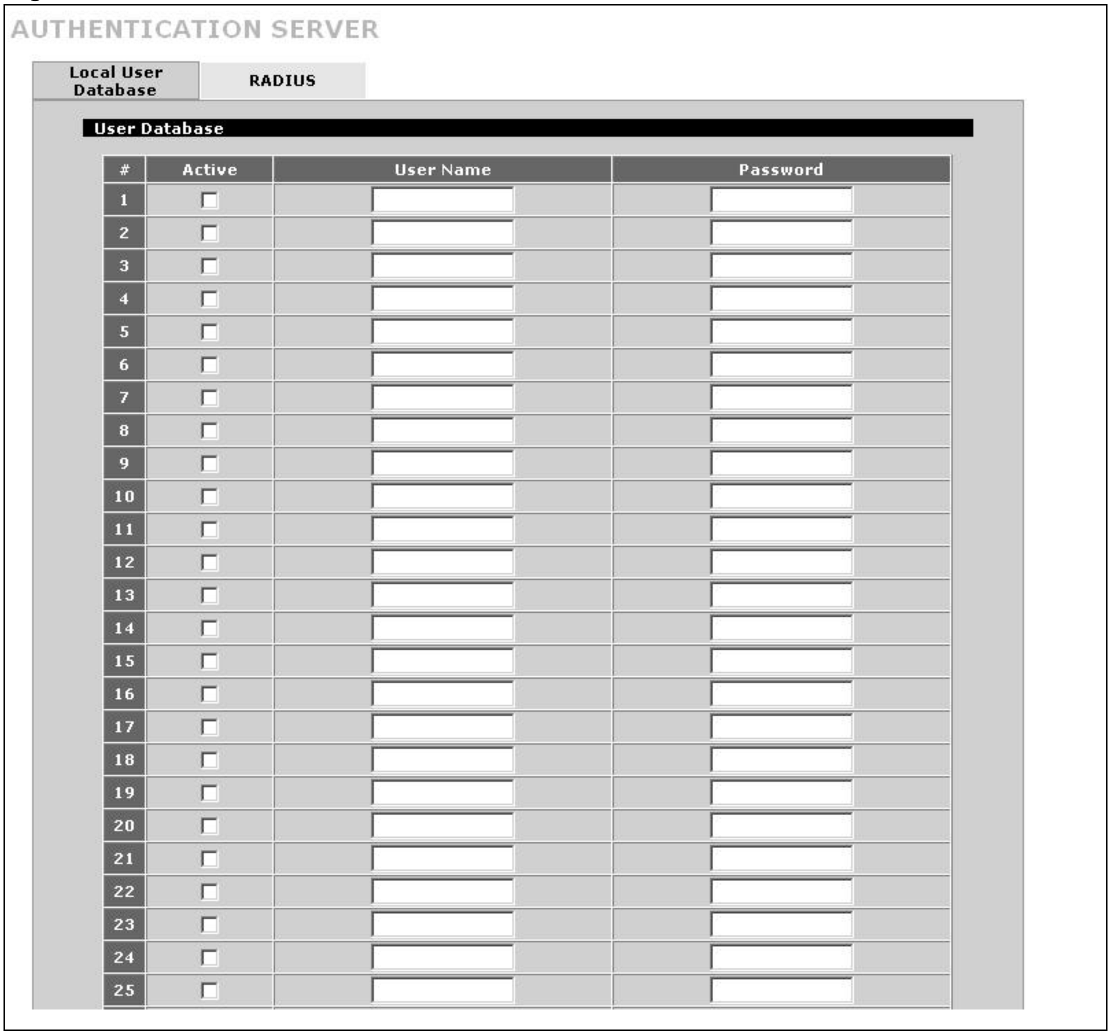
  Keeps track of the client's network activity.

RADIUS user is a simple package exchange in which your LAN-Cell acts as a message relay between the wireless station and the network RADIUS server.

12.2 Local User Database Screen

Click **SECURITY** > **AUTH SERVER** to open the **Local User Database** screen. The local user database is a list of user profiles stored on the LAN-Cell. The LAN-Cell can use this list of user profiles to authenticate users. Use this screen to change your LAN-Cell's list of user profiles.

Figure 171 SECURITY > AUTH SERVER > Local User Database



The following table describes the labels in this screen.

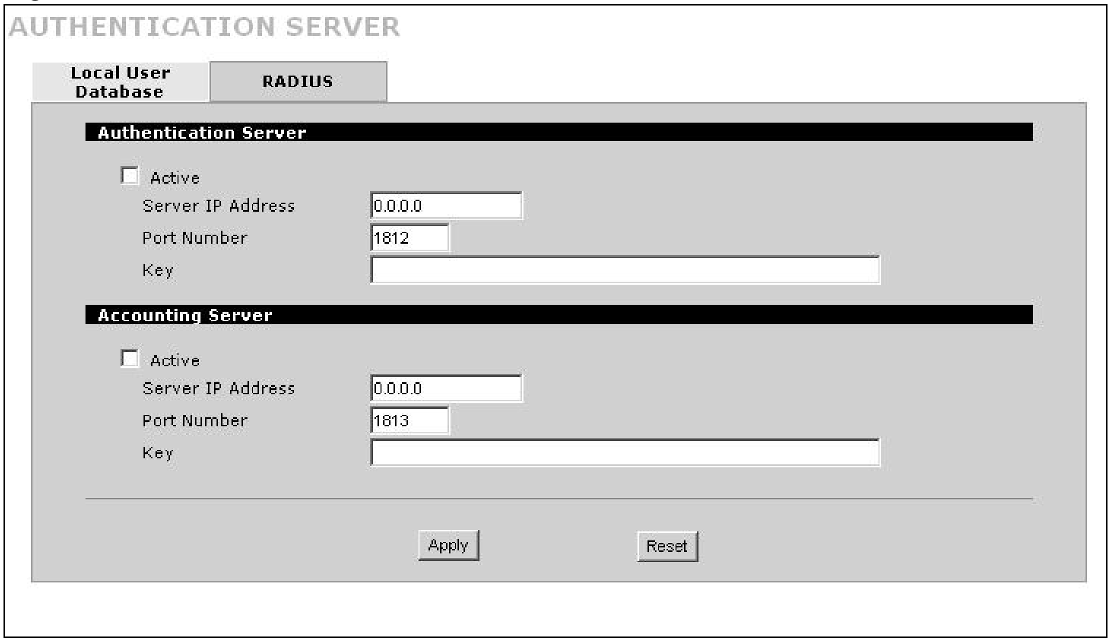
Table 103 SECURITY > AUTH SERVER > Local User Database

LABEL	DESCRIPTION
Active	Select this check box to enable the user profile.
User Name	Enter the user name of the user profile.
Password	Enter a password up to 31 characters long for this user profile.
Apply	Click **Apply** to save your changes back to the LAN-Cell.
Reset	Click **Reset** to begin configuring this screen afresh.

12.3 RADIUS Screen

Click **SECURITY** > **AUTH SERVER** > **RADIUS** to open the **RADIUS** screen. Configure this screen to use an external RADIUS server to authenticate users.

Figure 172 SECURITY > AUTH SERVER > RADIUS



The following table describes the labels in this screen.

Table 104 SECURITY > AUTH SERVER > RADIUS

LABEL	DESCRIPTION
Authentication Server	
Active	Select the check box to enable user authentication through an external authentication server. Clear the check box to enable user authentication using the local user profile on the LAN-Cell.
Server IP Address	Enter the IP address of the external authentication server in dotted decimal notation.
Port Number	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 LAN-Cell. The key is not sent over the network. This key must be the same on the external authentication server and LAN-Cell.
Accounting Server	
Active	Select the check box to enable user accounting through an external authentication server.
Server IP Address	Enter the IP address of the external accounting server in dotted decimal notation.
Port Number	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.

Table 104 SECURITY > AUTH SERVER > RADIUS

LABEL	DESCRIPTION
Key	Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external accounting server and the LAN-Cell. The key is not sent over the network. This key must be the same on the external accounting server and LAN-Cell.
Apply	Click **Apply** to save your changes back to the LAN-Cell.
Reset	Click **Reset** to begin configuring this screen afresh.

PART IV

Advanced Menu

13

Network Address Translation (NAT) Screens

13.1 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.

13.1.1 What You Can Do in the NAT Screens

- Use the **NAT Overview** screen (Section 13.2 on page 290) to configure global NAT settings and enable NAT on a WAN interface.
- Use the **Address Mapping** screens (Section 13.3 on page 292**)** to change your LAN-Cell's address mapping settings.
- Click **Port Forwarding** screens (Section 13.4 on page 295) to make servers with private IP addresses on your network (behind NAT) visible to the outside world.
- Click **Port Triggering** screens (Section 13.5 on page 300) to change your LAN-Cell's trigger port settings.

13.1.2 What You Need To Know About NAT

NAT Mapping Types

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

- **One to One**: In One-to-One mode, the LAN-Cell maps one local IP address to one global IP address.
- **Many to One**: In Many-to-One mode, the LAN-Cell maps multiple local IP addresses to one global IP address. This is equivalent to SUA (i.e., PAT, port address translation), Proxicast's Single User Account feature (the **SUA** option).
- **Many to Many Overload**: In Many-to-Many Overload mode, the LAN-Cell maps the multiple local IP addresses to shared global IP addresses.
- **Many One to One**: In Many-One-to-One mode, the LAN-Cell 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.

The following table summarizes the NAT mapping types.

Table 105 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	ILA ←→ IGA1 ILA2 ←→ IGA2 ILA3 ←→ IGA1 ILA4 ←→ IGA2 …	M-M Ov
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

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

SUA (Single User Account) Versus NAT

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

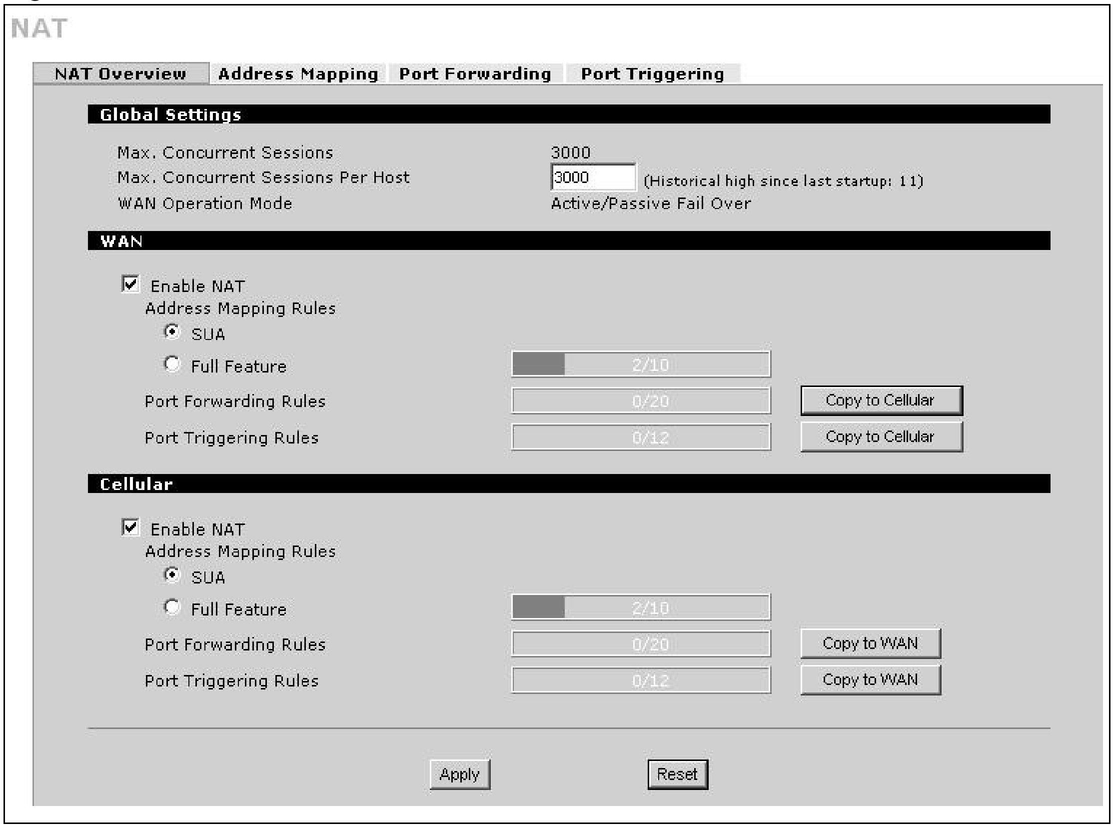
Selecting **SUA** means (latent) multiple WAN-to-LAN and WAN-to-DMZ address translation. That means that computers on your DMZ with public IP addresses will still have to undergo NAT mapping if you're using **SUA** NAT mapping. If this is not your intention, then select **Full Feature** NAT and don't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

13.2 NAT Overview Screen

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

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

Figure 173 ADVANCED > NAT > NAT Overview



The following table describes the labels in this screen.

Table 106 ADVANCED > NAT > NAT Overview

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

Table 106 ADVANCED > NAT > NAT Overview (continued)

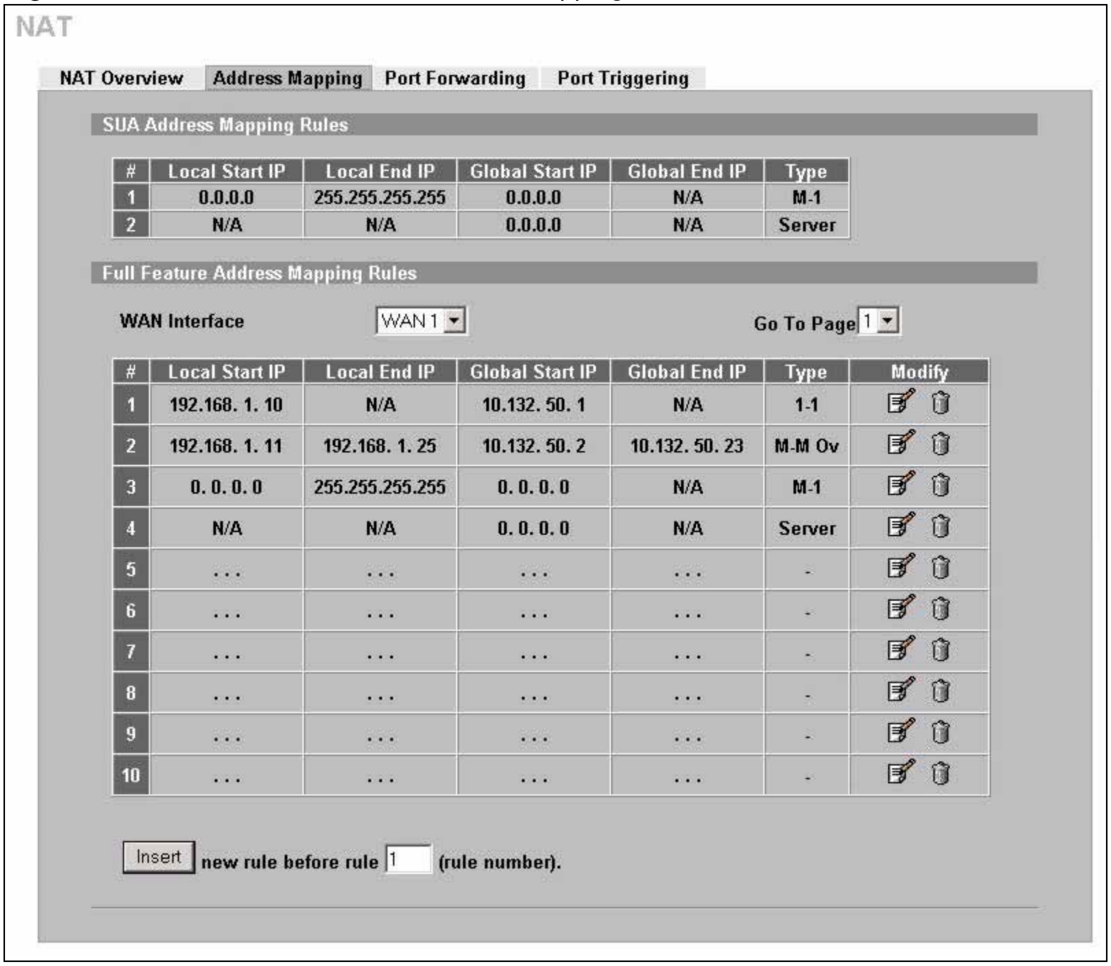
LABEL	DESCRIPTION
Port Forwarding Rules	The bar displays how many of the LAN-Cell's possible port forwarding rules are configured. The first number shows how many port forwarding rules are configured on the LAN-Cell. The second number shows the maximum number of port forwarding rules that can be configured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

13.3 NAT Address Mapping

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

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

Figure 174 ADVANCED > NAT > Address Mapping



The following table describes the labels in this screen.

Table 107 ADVANCED > NAT > Address Mapping

LABEL	DESCRIPTION
SUA Address Mapping Rules	This read-only table displays the default address mapping rules.
Full Feature Address Mapping Rules	
WAN Interface	Select the WAN interface for which you want to view or configure address mapping rules.
Go To Page	Choose a page from the drop-down list box to display the corresponding summary page of address mapping rules.
#	This is the rule index number.
Local Start IP	This refers to the Inside Local Address (ILA), which is the starting local IP address. If the rule is for all local IP addresses, then this field displays 0.0.0.0 as the **Local Start IP** address. Local IP addresses are **N/A** for **Server** port mapping.
Local End IP	This is the end Inside Local Address (ILA). If the rule is for all local IP addresses, then this field displays 255.255.255.255 as the **Local End IP** address. This field is **N/A** for **One-to-One** and **Server** mapping types.

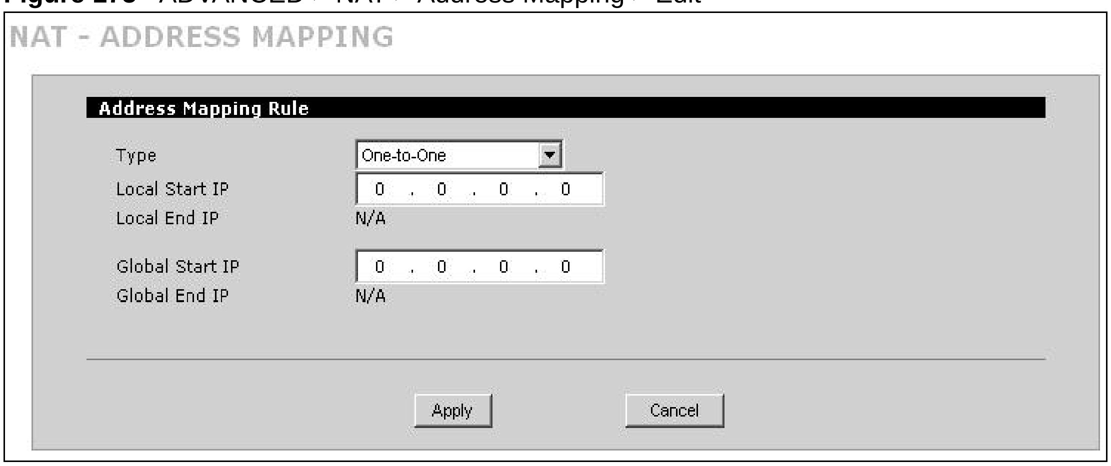
Table 107 ADVANCED > NAT > Address Mapping (continued)

LABEL	DESCRIPTION
Global Start IP	This refers to the Inside Global IP Address (IGA), that is the starting global IP address. 0.0.0.0 is for a dynamic IP address from your ISP with **Many-to-One** and **Server** mapping types.
Global End IP	This is the ending Inside Global Address (IGA). This field is **N/A** for **One-to-One**, **Many-to-One** and **Server** mapping types.
Type	1. **One-to-One** mode maps one local IP address to one global IP address. Note that port numbers do not change for the One-to-One NAT mapping type. 2. **Many-to-One** mode maps multiple local IP addresses to one global IP address. This is equivalent to SUA (i.e., PAT, port address translation), Proxicast's Single User Account feature that previous Proxicast routers supported only. 3. **Many-to-Many Overload** mode maps multiple local IP addresses to shared global IP addresses. 4. **Many One-to-One** mode maps each local IP address to unique global IP addresses. 5. **Server** allows you to specify inside servers of different services behind the NAT to be accessible to the outside world.
Modify	Click the edit icon to go to the screen where you can edit the address mapping rule. Click the delete icon to delete an existing address mapping rule. A window display asking you to confirm that you want to delete the address mapping rule. Note that subsequent address mapping rules move up by one when you take this action.
Insert	Click **Insert** to insert a new mapping rule before an existing one.

13.3.1 NAT Address Mapping Edit

Click the **Edit** button to display the **NAT Address Mapping Edit** screen. Use this screen to edit an address mapping rule. See Section 13.3 on page 292 for information on NAT and address mapping.

Figure 175 ADVANCED > NAT > Address Mapping > Edit



The following table describes the labels in this screen.

Table 108 ADVANCED > NAT > Address Mapping > Edit

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

13.4 Port Forwarding

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

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

Many 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

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

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

Port Forwarding: Services and Port Numbers

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

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

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

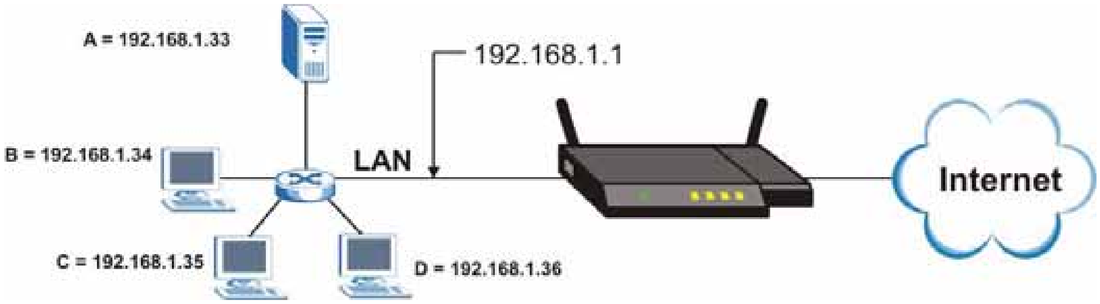
Table 109 Services and Port Numbers

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

13.4.1 Configuring Servers Behind Port Forwarding (Example)

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

Figure 176 Multiple Servers Behind NAT Example



NAT and Multiple WAN

The LAN-Cell has two WAN interfaces (wired + cellular). You can configure port forwarding and trigger port rule sets for the first WAN interface and separate sets of rules for the second WAN interface.

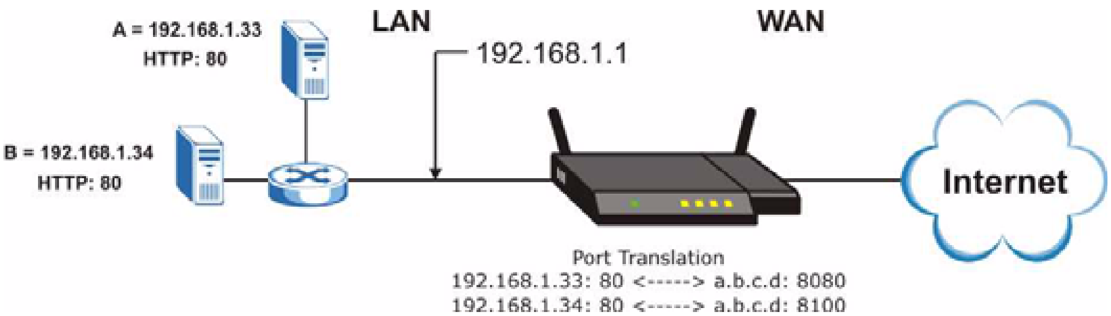
Port Translation

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

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

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

Figure 177 Port Translation Example



13.4.2 Port Forwarding Screen

Click **ADVANCED** > **NAT** > **Port Forwarding** to open the **Port Forwarding** screen. Refer to Figure 109 on page 296 for port numbers commonly used for particular services.

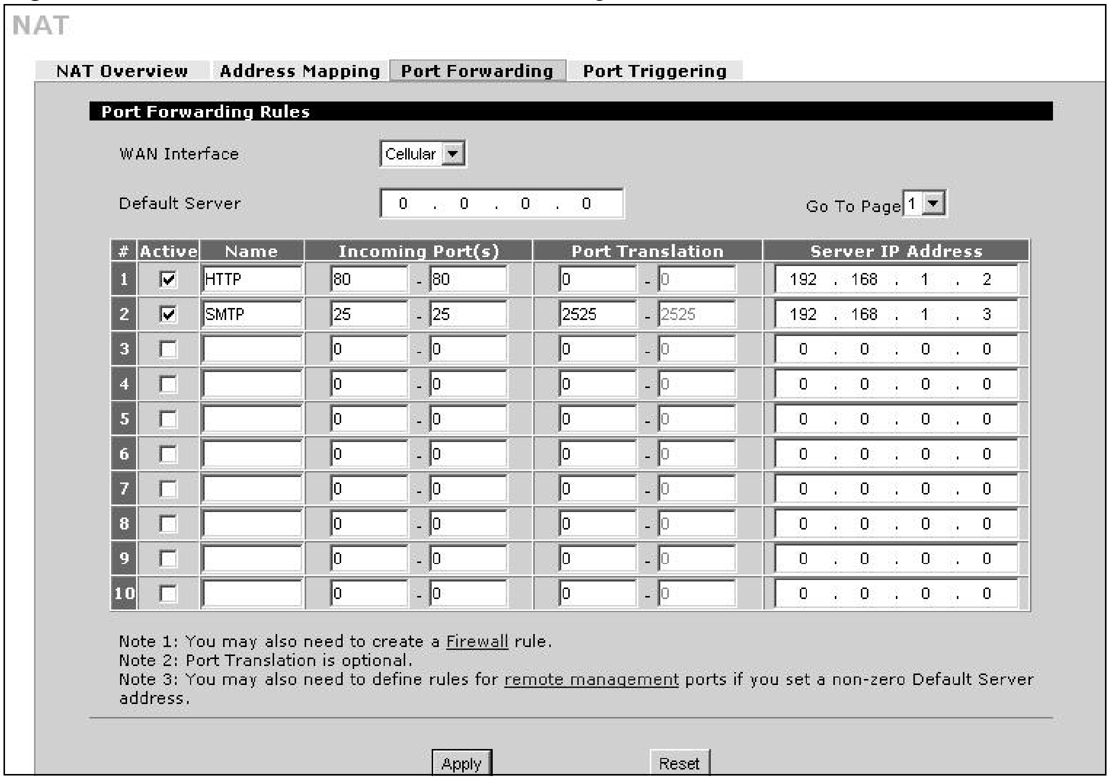
Remember to define the appropriate **Firewall Rules** to allow the ports listed on the **Port Forwarding Screen** through the correct WAN and LAN/DMZ interfaces (e.g. WAN-to-LAN and Cell-to-LAN or WAN-to-DMZ and Cell-to-DMZ rules).

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

In general, if you wish to access the LAN-Cell for remote management through the WAN or CELLULAR interfaces, do not define a NAT **Default Server**. Use the Port Forwarding Rules, Remote Management Ports, and Firewall Rules to define WAN-based remote access to the LAN-Cell.

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

Figure 178 ADVANCED > NAT > Port Forwarding



The following table describes the labels in this screen.

Table 110 ADVANCED > NAT > Port Forwarding

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

Table 110 ADVANCED > NAT > Port Forwarding

LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes back to the LAN-Cell.
Reset	Click **Reset** to begin configuring this screen afresh.

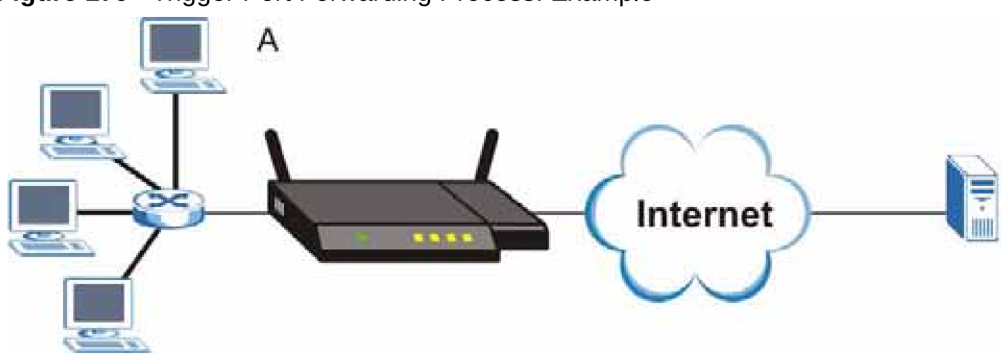
13.5 Port Triggering

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

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

For example:

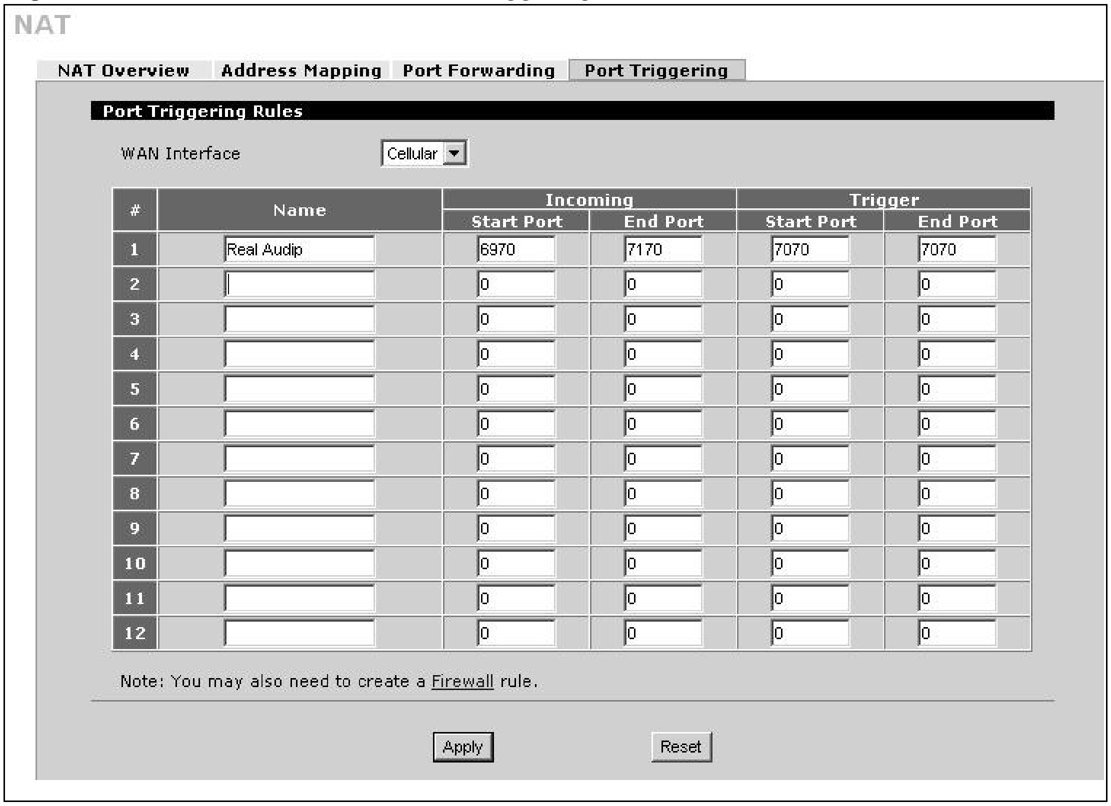
Figure 179 Trigger Port Forwarding Process: Example



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

Click **ADVANCED** > **NAT** > **Port Triggering** to open the following screen. Use this screen to change your LAN-Cell's trigger port settings.

Figure 180 ADVANCED > NAT > Port Triggering



The following table describes the labels in this screen.

Table 111 ADVANCED > NAT > Port Triggering

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

13.6 NAT Technical Reference

This technical reference contains the following sections:

- Inside/outside and Global/locall
- What NAT Does
- How NAT Works
- NAT Application
- Port Restricted Cone NAT

Inside/outside and Global/local

Inside/outside denotes where a host is located relative to the LAN-Cell. 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 112 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.

What NAT Does

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

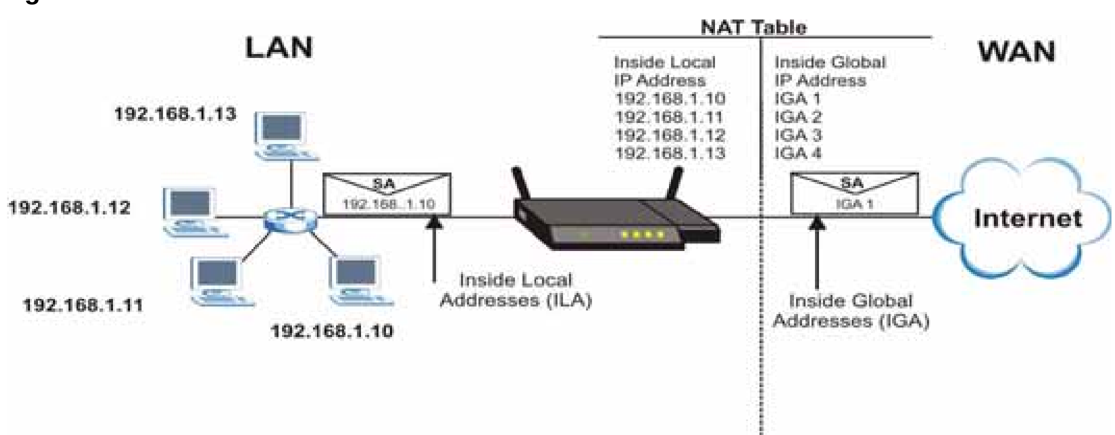
The global IP addresses for the inside hosts can be either static or dynamically assigned by the ISP. In addition, you can designate servers (for example a web server and a telnet server) on your local network and make them accessible to the outside world. Although you can make designated servers on the LAN accessible to the outside world, it is strongly recommended that you attach those servers to the DMZ port instead. If you do not define any servers (for Many-to-One and Many-to-Many Overload mapping), NAT offers the additional benefit of firewall protection. With no servers defined, your LAN-Cell 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).

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 LAN-Cell keeps track of the original addresses and port numbers so incoming reply packets can have their original values restored. The following figure illustrates this.

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

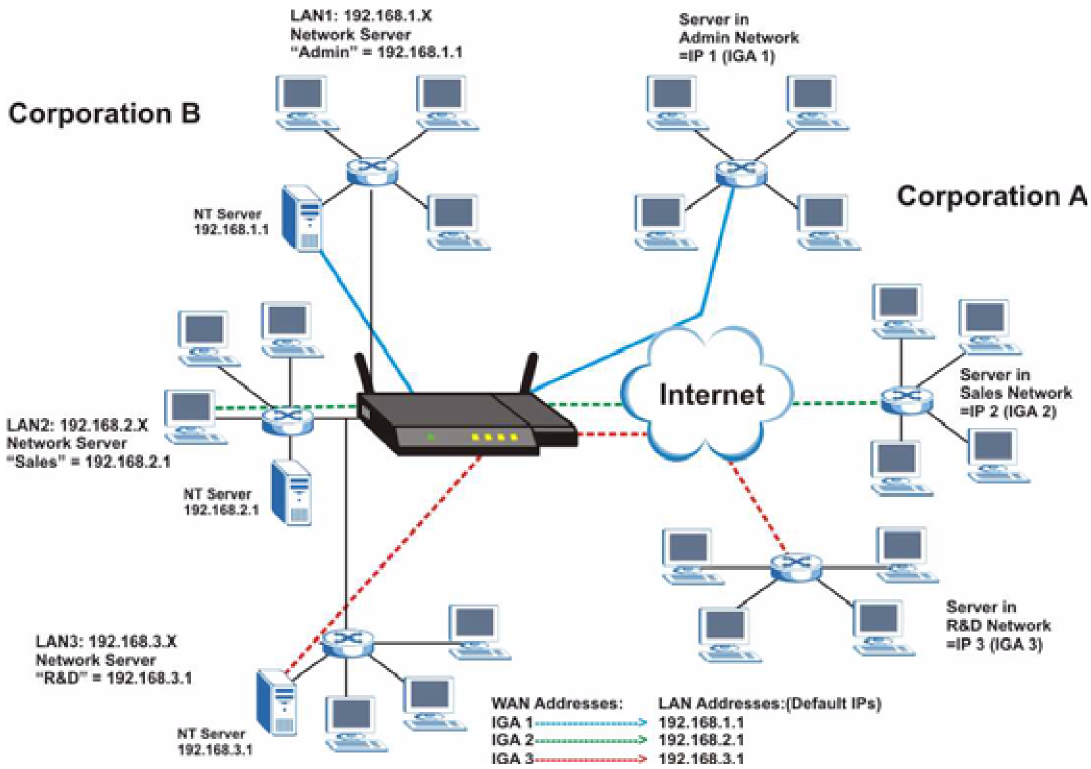
Figure 181 How NAT Works



NAT Application

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

Figure 182 NAT Application With IP Alias



Port Restricted Cone NAT

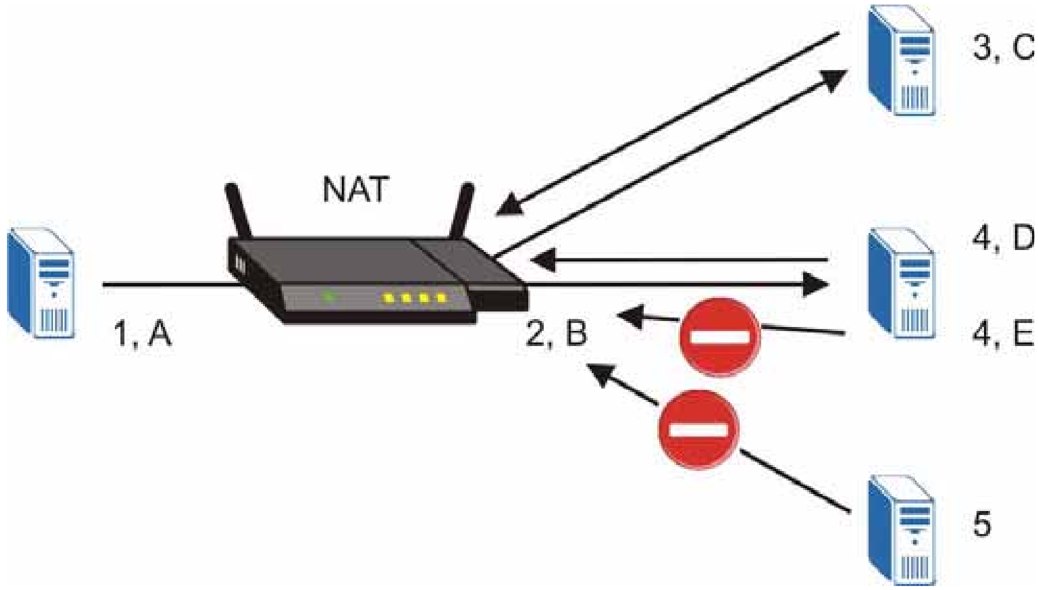
LAN-Cell ProxiOS version 4.00 and later uses port restricted cone NAT. Port restricted cone NAT maps all outgoing packets from an internal IP address and port to a single IP address and port on the external network. In the following example, the LAN-Cell maps the source address of all packets sent from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

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

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

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

Figure 183 Port Restricted Cone NAT Example



14

DNS Screens

14.1 Overview

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

14.1.1 What You Can Do in the DNS Screens

- Use the System screen (Section 14.2 on page 309) to configure the LAN-Cell to use a DNS server to resolve domain names for LAN-Cell system features like VPN, DDNS and the time server.
- Use the Add Address Record screen (Section 14.2.1 on page 311) to add an address record.
- Use the Insert Name Server Record screen (Section 14.2.2 on page 312) to insert a name server record.
- Use the Cache screen (Section 14.3 on page 313) to configure the LAN-Cell's DNS caching settings.
- Use the DHCP screen (Section 14.5 on page 315) to configure the DNS server information that the LAN-Cell sends to its LAN, DMZ or WLAN DHCP clients.
- Use the DDNS screen (Section on page 309) to change your LAN-Cell's DDNS (Dynamic DNS) settings.

14.1.2 What You Need To Know About DNS

DNS Server Address Assignment

The LAN-Cell can get the DNS server addresses in the following ways.

1. The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you DNS server addresses, manually enter them in the DNS server fields.
2. If your ISP dynamically assigns the DNS server IP addresses (along with the LAN-Cell's WAN IP address), set the DNS server fields to get the DNS server address from the ISP.
3. You can manually enter the IP addresses of other DNS servers. These servers can be public or private. A DNS server could even be behind a remote IPSec router (see Section on page 308).

DNS Servers

There are three places where you can configure DNS setup on the LAN-Cell.

1. Use the **DNS System** screen to configure the LAN-Cell to use a DNS server to resolve domain names for LAN-Cell system features like VPN, DDNS and the time server.
2. Use the **DNS DHCP** screen to configure the DNS server information that the LAN-Cell sends to the DHCP client devices on the LAN, DMZ or WLAN.
3. Use the **REMOTE MGMT DNS** screen to configure the LAN-Cell to accept or discard DNS queries.

Address Record

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

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

DNS Wildcard

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

Name Server Record

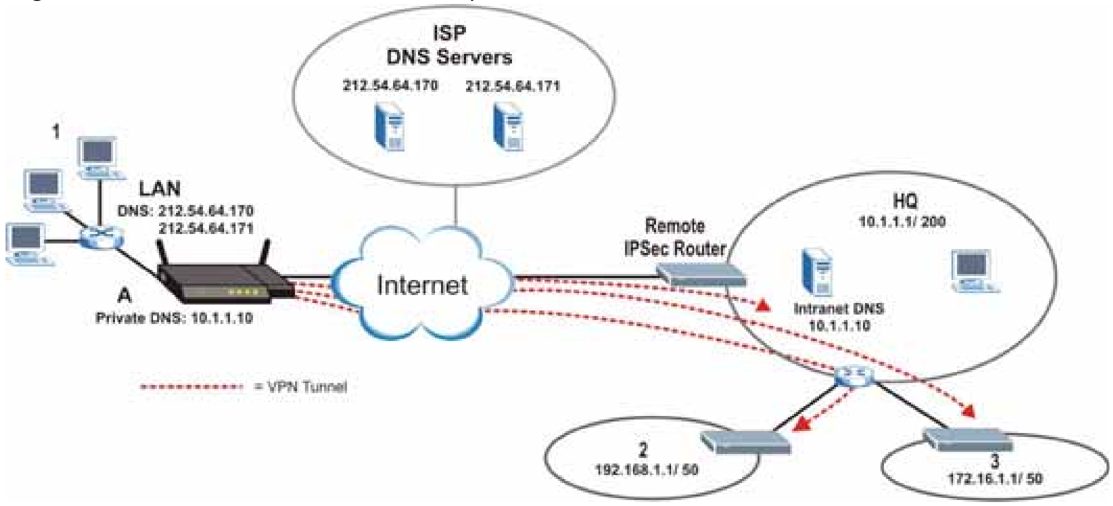
A name server record contains a DNS server’s IP address. The LAN-Cell can query the DNS server to resolve domain names for features like VPN, DDNS and the time server. A domain zone may also be included. A domain zone is a fully qualified domain name without the host. For example, proxicast.com is the domain zone for the www.proxicast.com fully qualified domain name.

Private DNS Server

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

The following figure depicts an example where three VPN tunnels are created from LAN-Cell A; one to branch office **2**, one to branch office **3** and another to headquarters (**HQ**). In order to access computers that use private domain names on the **HQ** network, the LAN-Cell at branch office **1** uses the Intranet DNS server in headquarters.

Figure 184 Private DNS Server Example



If you do not specify an Intranet DNS server on the remote network, then the VPN host must use IP addresses to access the computers on the remote private network.

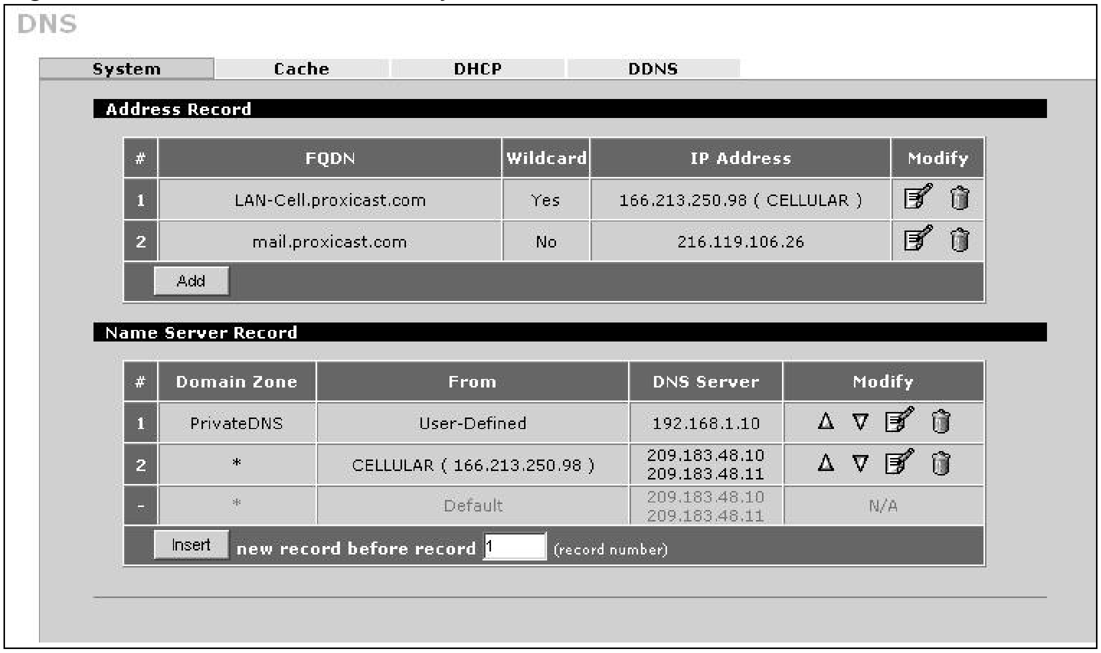
DDNS

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

14.2 System Screen

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

Figure 185 ADVANCED > DNS > System DNS



The following table describes the labels in this screen.

Table 113 ADVANCED > DNS > System DNS

LABEL	DESCRIPTION
Address Record	An address record specifies the mapping of a fully qualified domain name (FQDN) to an IP address. An FQDN consists of a host and domain name and includes the top-level domain. For example, www.proxicast.com is a fully qualified domain name, where “www” is the host, “proxicast” is the second-level domain, and “.com” is the top level domain.
#	This is the index number of the address record.
FQDN	This is a host’s fully qualified domain name.
Wildcard	This column displays whether or not the DNS wildcard feature is enabled for this domain name.
IP Address	This is the IP address of a host.
Modify	Click the edit icon to go to the screen where you can edit the record. Click the delete icon to remove an existing record. A window display asking you to confirm that you want to delete the record. Note that subsequent records move up by one when you take this action.
Add	Click **Add** to open a screen where you can add a new address record. Refer to Table 114 on page 312 for information on the fields.
Name Server Record	A name server record contains a DNS server’s IP address. The LAN-Cell can query the DNS server to resolve domain names for features like VPN, DDNS and the time server. When the LAN-Cell needs to resolve a domain name, it checks it against the name server record entries in the order that they appear in this list. A “*” indicates a name server record without a domain zone. The default record is grayed out. The LAN-Cell uses this default record if the domain name that needs to be resolved does not match any of the other name server records. A name server record with a domain zone is always put before a record without a domain zone.
#	This is the index number of the name server record.

Table 113 ADVANCED > DNS > System DNS

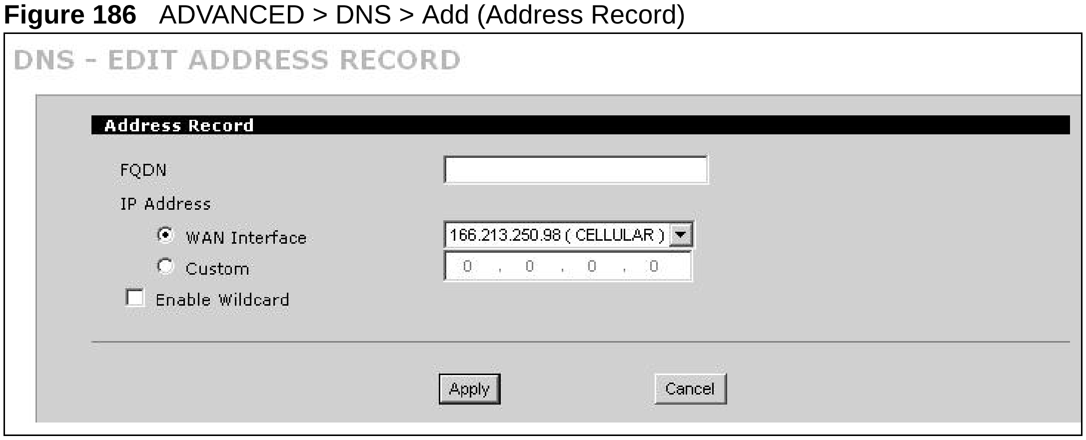
LABEL	DESCRIPTION
Domain Zone	A domain zone is a fully qualified domain name without the host. For example, proxicast.com is the domain zone for the www.proxicast.com fully qualified domain name.
From	This field displays whether the IP address of a DNS server is from a WAN interface (and which it is) or specified by the user.
DNS Server	This is the IP address of a DNS server.
Modify	Click a triangle icon to move the record up or down in the list. Click the edit icon to go to the screen where you can edit the record. Click the delete icon to remove an existing record. A window display asking you to confirm that you want to delete the record. Note that subsequent records move up by one when you take this action.
Insert	Click **Insert** to open a screen where you can insert a new name server record. Refer to Table 115 on page 313 for information on the fields.

14.2.1 Adding an Address Record

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

An address record contains the mapping of a fully qualified domain name (FQDN) to an IP address. Configure address records about the LAN-Cell itself or another device to keep a record of DNS names and addresses that people on your network may use frequently. If the LAN-Cell receives a DNS query for an FQDN for which the LAN-Cell has an address record, the LAN-Cell can send the IP address in a DNS response without having to query a DNS name server. See Section on page 308 for more on address records.

Figure 186 ADVANCED > DNS > Add (Address Record)



The following table describes the labels in this screen.

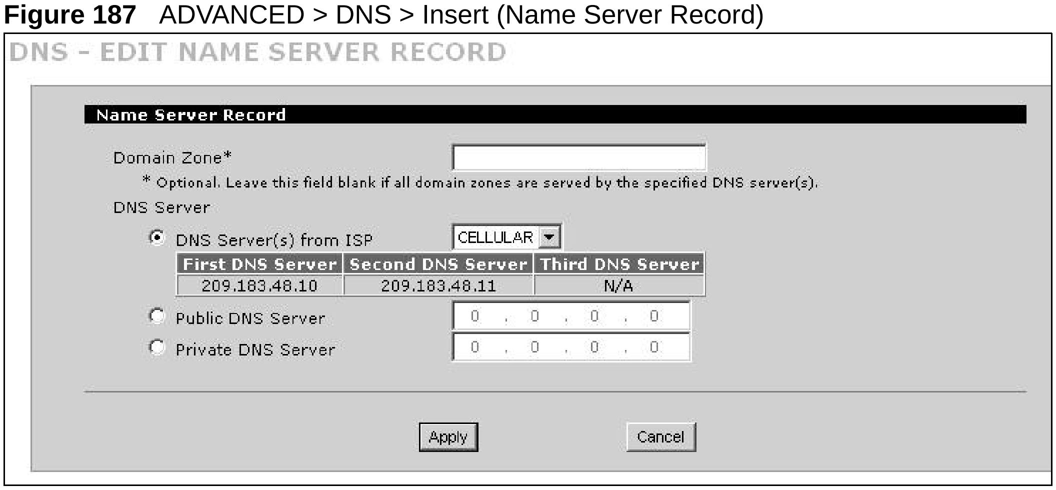
Table 114 ADVANCED > DNS > Add (Address Record)

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

14.2.2 Inserting a Name Server Record

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

Figure 187 ADVANCED > DNS > Insert (Name Server Record)



The following table describes the labels in this screen.

Table 115 ADVANCED > DNS > Insert (Name Server Record)

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

14.3 DNS Cache

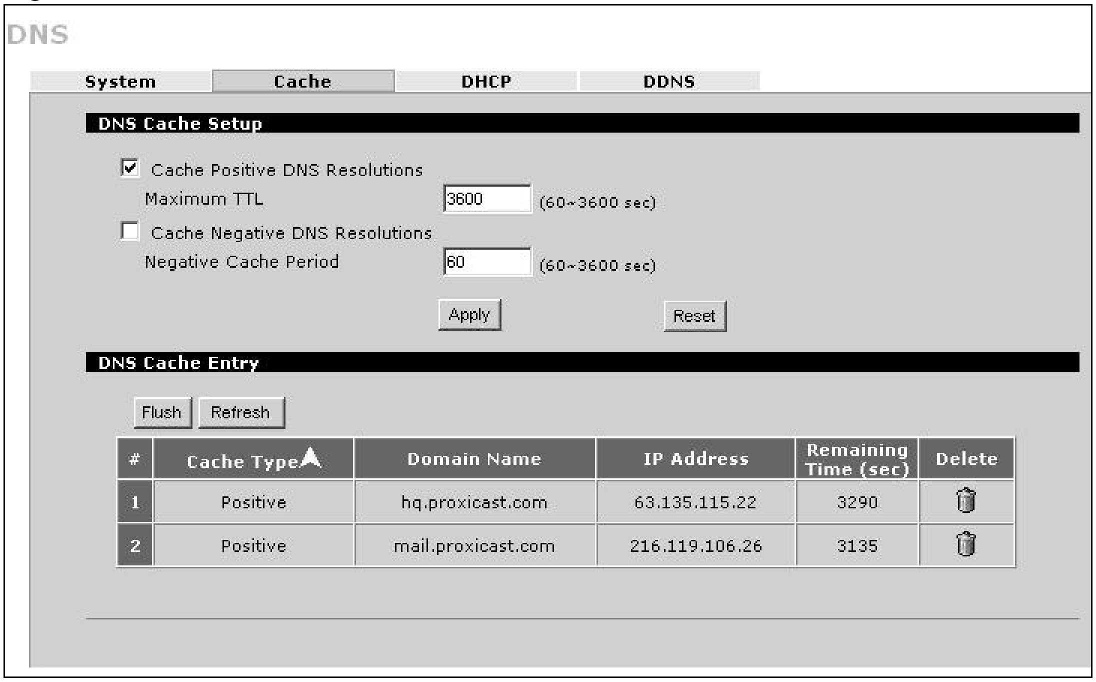
DNS cache is the temporary storage area where a router stores responses from DNS servers. When the LAN-Cell receives a positive or negative response for a DNS query, it records the response in the DNS cache. A positive response means that the LAN-Cell received the IP address for a domain name that it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

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

14.4 Configure DNS Cache

To configure your LAN-Cell's DNS caching, click **ADVANCED** > **DNS** > **Cache**. The screen appears as shown.

Figure 188 ADVANCED > DNS > Cache



The following table describes the labels in this screen.

Table 116 ADVANCED > DNS > Cache

LABEL	DESCRIPTION
DNS Cache Setup	
Cache Positive DNS Resolutions	Select the check box to record the positive DNS resolutions in the cache. Caching positive DNS resolutions helps speed up the LAN-Cell's processing of commonly queried domain names and reduces the amount of traffic that the LAN-Cell sends out to the WAN.
Maximum TTL	Type the maximum time to live (TTL) (60 to 3600 seconds). This sets how long the LAN-Cell is to allow a positive resolution entry to remain in the DNS cache before discarding it.
Cache Negative DNS Resolutions	Caching negative DNS resolutions helps speed up the LAN-Cell's processing of commonly queried domain names (for which DNS resolution has failed) and reduces the amount of traffic that the LAN-Cell sends out to the WAN.
Negative Cache Period	Type the time (60 to 3600 seconds) that the LAN-Cell is to allow a negative resolution entry to remain in the DNS cache before discarding it.
Apply	Click **Apply** to save your changes back to the LAN-Cell.
Reset	Click **Reset** to begin configuring this screen afresh.
DNS Cache Entry	
Flush	Click this button to clear the cache manually. After you flush the cache, the LAN-Cell must query the DNS servers again for any domain names that had been previously resolved.
Refresh	Click this button to reload the cache.
#	This is the index number of a record.
Cache Type	This displays whether the response for the DNS request is positive or negative.
Domain Name	This is the domain name of a host.
IP Address	This is the (resolved) IP address of a host. This field displays **0.0.0.0** for negative DNS resolution entries.

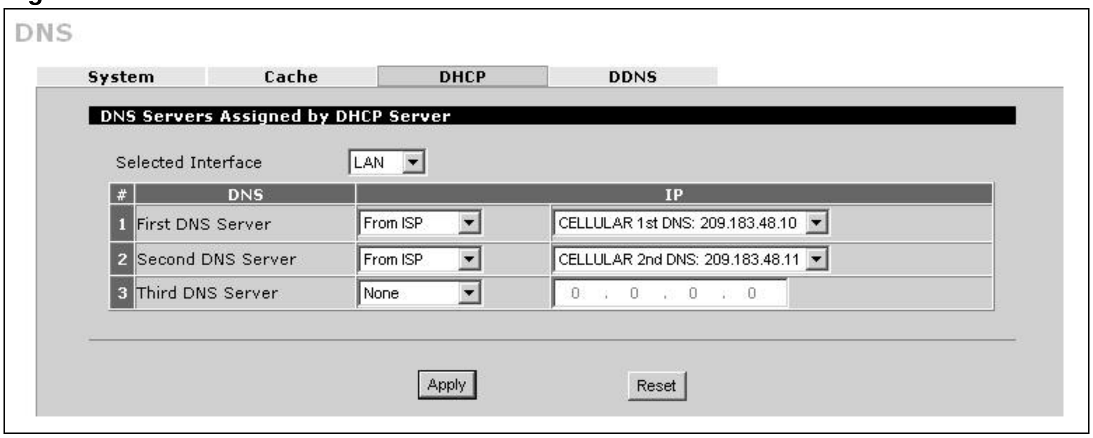
Table 116 ADVANCED > DNS > Cache

LABEL	DESCRIPTION
Remaining Time (sec)	This is the number of seconds left before the DNS resolution entry is discarded from the cache.
Modify	Click the delete icon to remove the DNS resolution entry from the cache.

14.5 Configuring DNS DHCP

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

Figure 189 ADVANCED > DNS > DHCP



The following table describes the labels in this screen.

Table 117 ADVANCED > DNS > DHCP

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

Table 117 ADVANCED > DNS > DHCP

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

14.6 DDNS Screen

First, you need to have registered a dynamic DNS account with one of the supported DDNS Service Providers. This is for users with a dynamic IP from their ISP or DHCP server that would still like to have a domain name. The Dynamic DNS service provider will give you a password or key.

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

DYNDNS Wildcard

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

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

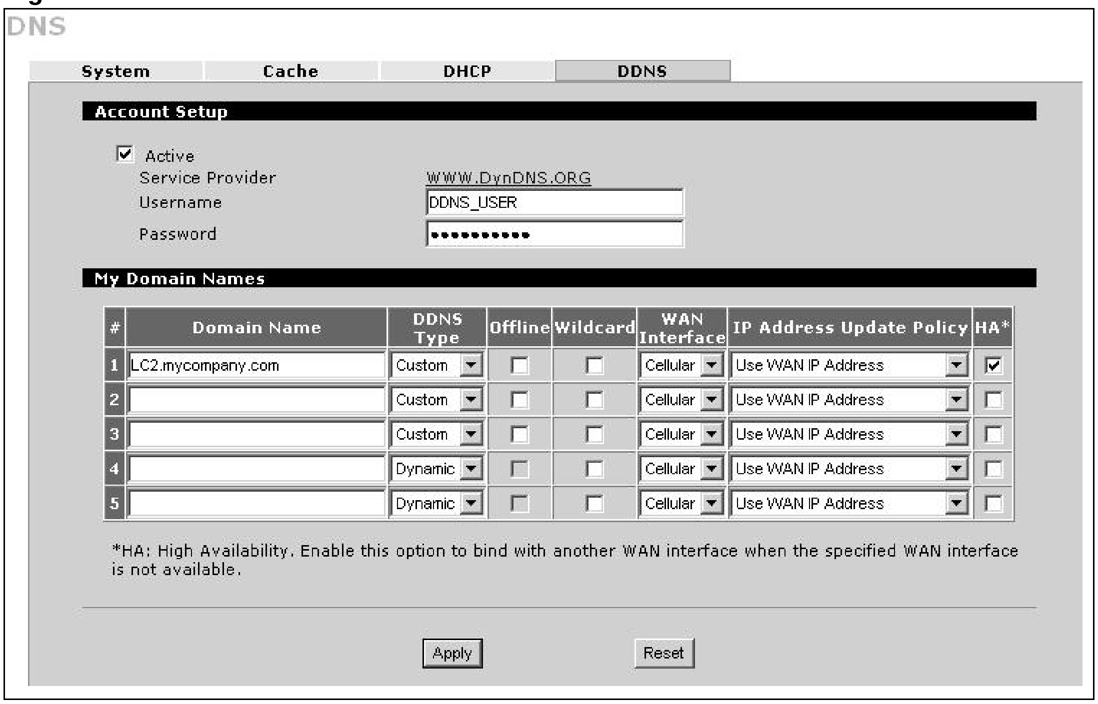
High Availability

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

14.7 Configuring Dynamic DNS

To change your LAN-Cell's DDNS, click **ADVANCED** > **DNS** > **DDNS**. The screen appears as shown.

Figure 190 ADVANCED > DNS > DDNS



The following table describes the labels in this screen.

Table 118 ADVANCED > DNS > DDNS

LABEL	DESCRIPTION
Account Setup	
Active	Select this check box to use dynamic DNS.
Service Provider	This is the name of your Dynamic DNS service provider.
Username	Enter your user name. You can use up to 31 alphanumeric characters (and the underscore). Spaces are not allowed.
Password	Enter the password associated with the user name above. You can use up to 31 alphanumeric characters (and the underscore). Spaces are not allowed.
My Domain Names	
Domain Name 1~5	Enter the host names in these fields. Enter a Fully Qualified Domain Name (FQDN) that matches the host name set up in your DynDNS account.

Table 118 ADVANCED > DNS > DDNS

LABEL	DESCRIPTION
DDNS Type	Select the type of service that you are registered for from your Dynamic DNS service provider. Select **Dynamic** if you have the Dynamic DNS service. Select **Static** if you have the Static DNS service. Select **Custom** if you have the Custom DNS service.
Offline	This option is available when **Custom** is selected in the **DDNS Type** field. Check with your Dynamic DNS service provider to have traffic redirected to a URL (that you can specify) while you are off line.
Wildcard	Select the check box to enable DYNDNS Wildcard.
WAN Interface	Select the WAN interface to use for updating the IP address of the domain name.
IP Address Update Policy	Select **Use WAN IP Address** to have the LAN-Cell update the domain name with the WAN interface's IP address. Select **Use User-Defined** and enter the IP address if you have a static IP address. Select **Let DDNS Server Auto Detect** only when there are one or more NAT routers between the LAN-Cell and the DDNS server. This feature has the DDNS server automatically detect and use the IP address of the NAT router that has a public IP address. Note: The DDNS server may not be able to detect the proper IP address if there is an HTTP proxy server between the LAN-Cell and the DDNS server.
HA	Select this check box to enable the high availability (HA) feature. High availability has the LAN-Cell update a domain name with another interface’s IP address when the normal WAN interface does not have a connection. If the WAN interface specified in the **WAN Interface** field does not have a connection, the LAN-Cell will attempt to use the IP address of another WAN interface to update the domain name. When the WAN interfaces are in the active/passive operating mode, the LAN-Cell will update the domain name with the IP address of whichever WAN interface has a connection, regardless of the setting in the **WAN Interface** field. Disable this feature and the LAN-Cell will only update the domain name with an IP address of the WAN interface specified in the **WAN Interface** field. If that WAN interface does not have a connection, the LAN-Cell will not update the domain name with another port’s IP address. Note: If you enable high availability, DDNS can also function when the LAN-Cell uses the dial backup port. DDNS does not function when the LAN-Cell uses traffic redirect.
Apply	Click **Apply** to save your changes back to the LAN-Cell.
Reset	Click **Reset** to begin configuring this screen afresh.

15

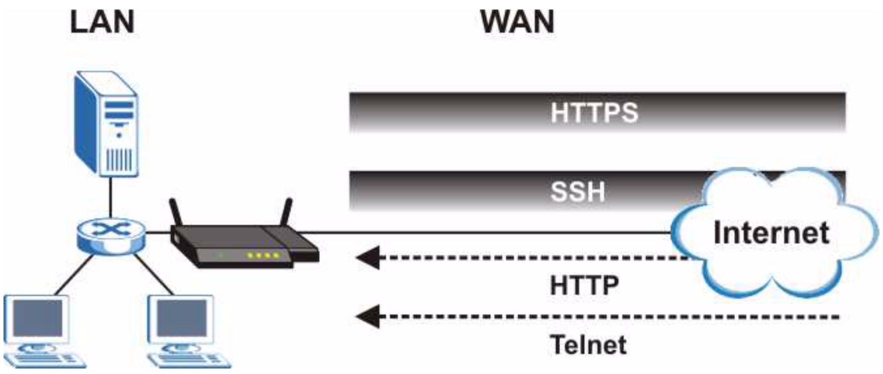
Remote Management Screens

15.1 Overview

This chapter provides information on the Remote Management screens. Remote management allows you to determine which services/protocols can access which LAN-Cell interface (if any) from which computers.

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

Figure 191 Secure and Insecure Remote Management From the WAN



15.1.1 What You Can Do in the Remote Management Screens

- Use the **WWW** screen (Section 15.4 on page 327) to configure the LAN-Cell's HTTP and HTTPS management settings.
- Use the **SSH** screen (Section 15.6 on page 330) to configure the LAN-Cell's Secure Shell settings.
- Use the **Telnet** screen (Section 15.8 on page 331) to specify which interfaces allow Telnet access and from which IP address the access can come.
- Use the **FTP** screen (Section 15.9 on page 332) to specify which interfaces allow FTP access and from which IP address the access can come.
- Use the **SNMP** screen (Section 15.10 on page 333) to configure the LAN-Cell's SNMP settings.
- Use the **DNS** screen (Section 15.11 on page 336) to set from which IP address the LAN-Cell will accept DNS queries and on which interface it can send them your LAN-Cell's DNS settings.

15.1.2 What You Need To Know About Remote Management

Firewall Rules

When you configure remote management to allow management from any network except the LAN, you still need to configure a firewall rule to allow access. See Chapter 9 on page 181 for details on configuring firewall rules.

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

Remote Management Sessions

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

1 Console port
2 SSH
3 Telnet
4 HTTPS and HTTP

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

Remote Management Limitations

Remote management does not work when:

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

System Timeout

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

15.2 Remote Management Examples

15.2.1 HTTPS Example

If you haven't changed the default HTTPS port on the LAN-Cell, then in your browser enter "https://LAN-Cell IP Address/" as the web site address where "LAN-Cell IP Address" is the IP address or domain name of the LAN-Cell you wish to access.

15.2.1.1 Internet Explorer Warning Messages

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

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

Other web browsers present similar Security Alerts when first accessing the LAN-Cell's HTTPS server.

Figure 192 Security Alert Dialog Box (Internet Explorer)

15.2.1.2 Avoiding the Browser Warning Messages

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

- The issuing certificate authority of the LAN-Cell's HTTPS server certificate is not one of the browser's trusted certificate authorities. The issuing certificate authority of the LAN-Cell's factory default certificate is the LAN-Cell itself since the certificate is a self-signed certificate.
  - For the browser to trust a self-signed certificate, import the self-signed certificate into your operating system as a trusted certificate.
  - To have the browser trust the certificates issued by a certificate authority, import the certificate authority's certificate into your operating system as a trusted certificate. Refer to Appendix G on page 629 for details.

- The actual IP address of the HTTPS server (the IP address of the LAN-Cell's port that you are trying to access) does not match the common name specified in the LAN-Cell's HTTPS server certificate that your browser received. Do the following to check the common name specified in the certificate that your LAN-Cell sends to HTTPS clients.
  6a Click **REMOTE MGMT**. Write down the name of the certificate displayed in the **Server Certificate** field.
  6b Click **CERTIFICATES**. Find the certificate and check its **Subject** column. **CN** stands for certificate's common name (see Figure 195 on page 323 for an example).

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

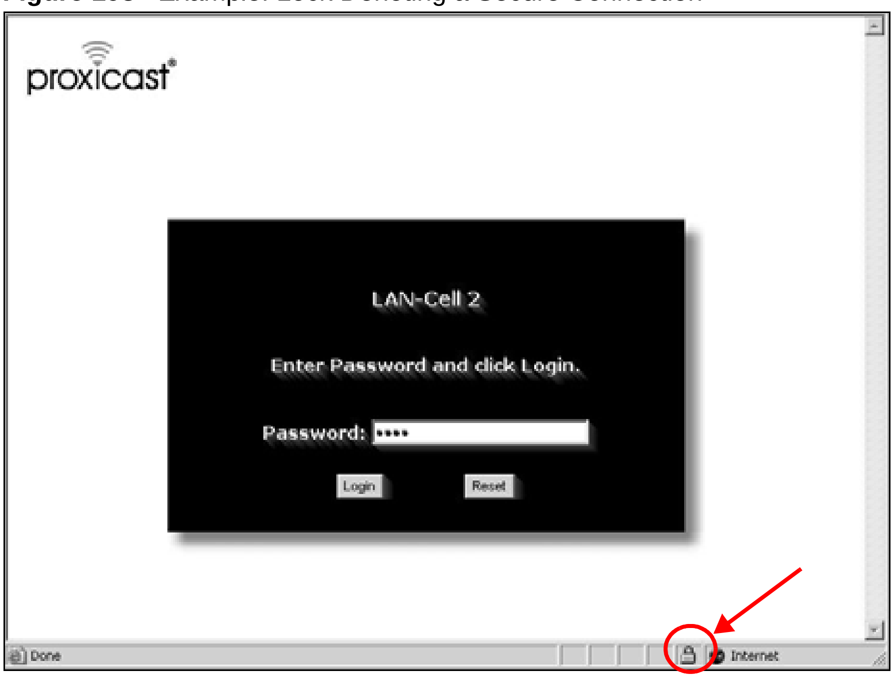
6a Create a new certificate for the LAN-Cell that uses the IP address (of the LAN-Cell's port that you are trying to access) as the certificate's common name. For example, to use HTTPS to access a LAN port with IP address 192.168.1.1, create a certificate that uses 192.168.1.1 as the common name.

6b Go to the remote management **WWW** screen and select the newly created certificate in the **Server Certificate** field. Click **Apply**.

15.2.1.3 Login Screen

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

Figure 193 Example: Lock Denoting a Secure Connection



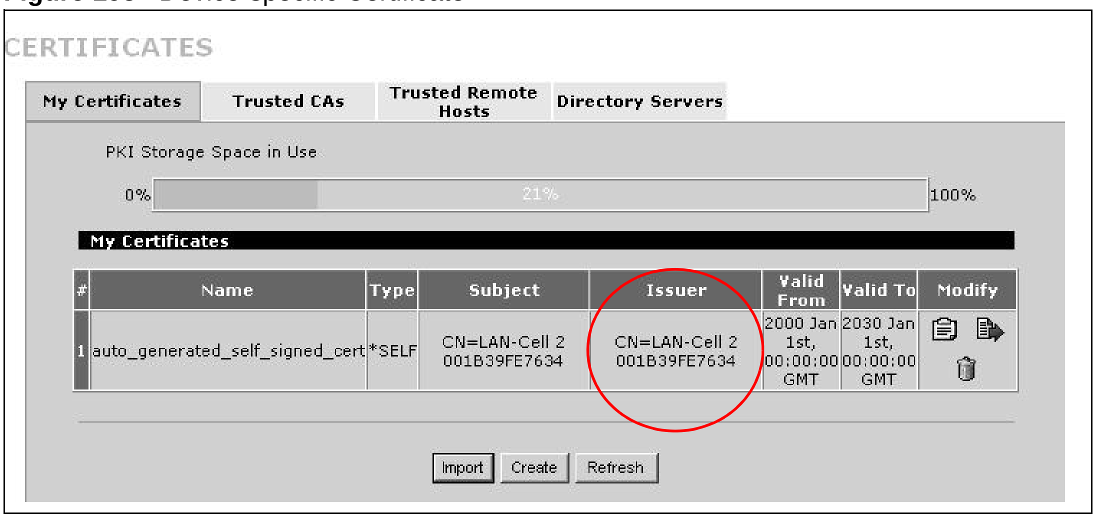
Click **Login** and you then see the next screen.

The factory default certificate is a common default certificate for all LAN-Cell models.

Figure 194 Replace Certificate

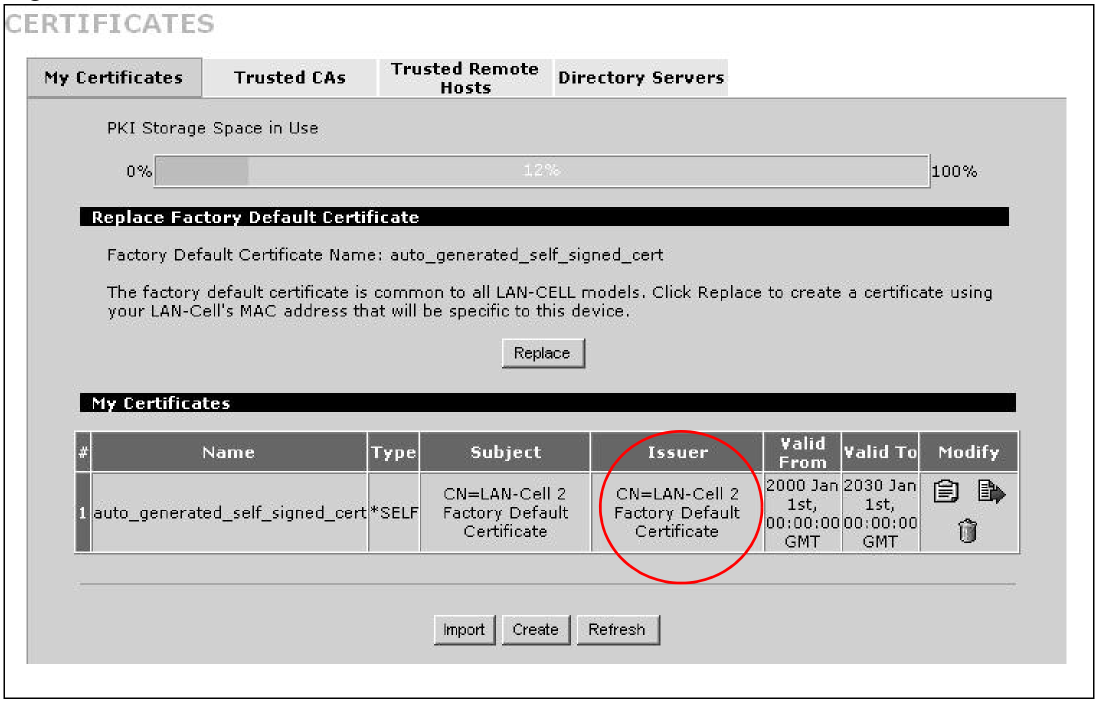
Click **Apply** in the **Replace Certificate** screen to create a certificate using your LAN-Cell’s MAC address that will be specific to this device. Click **CERTIFICATES** to open the **My Certificates** screen. You will see information similar to that shown in the following figure.

Figure 195 Device-specific Certificate



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

Figure 196 Common LAN-Cell Certificate



15.2.2 Secure Telnet Using SSH Examples

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

15.2.2.1 Example 1: Microsoft Windows

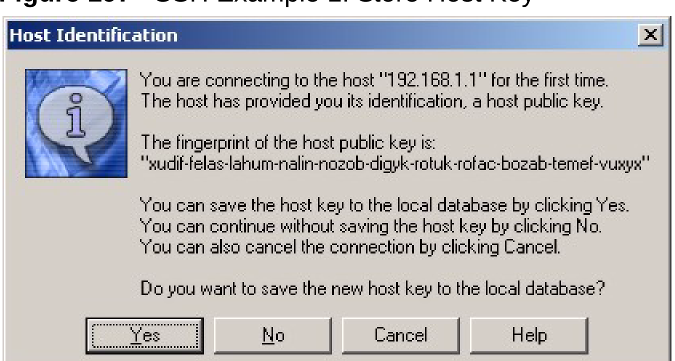
This section describes how to access the LAN-Cell using the Secure Shell Client program.

1 Launch the SSH client and specify the connection information (IP address, port number or device name) for the LAN-Cell.

2 Configure the SSH client to accept connection using SSH version 1.

3 A window displays prompting you to store the host key in you computer. Click **Yes** to continue.

Figure 197 SSH Example 1: Store Host Key



Enter the password to log in to the LAN-Cell. The SMT main menu displays next.

15.2.2.2 Example 2: Linux

This section describes how to access the LAN-Cell using the OpenSSH client program that comes with most Linux distributions.

1 Test whether the SSH service is available on the LAN-Cell.

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

A message displays indicating the SSH protocol version supported by the LAN-Cell.

Figure 198 SSH Example 2: Test

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

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

Then enter the password to log in to the LAN-Cell.

Figure 199 SSH Example 2: Log in

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

3 The SMT main menu displays next.

15.2.2.3 Secure FTP Using SSH Example

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

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

2 Enter the password to login to the LAN-Cell.

3 Use the “`put`” command to upload a new firmware to the LAN-Cell.

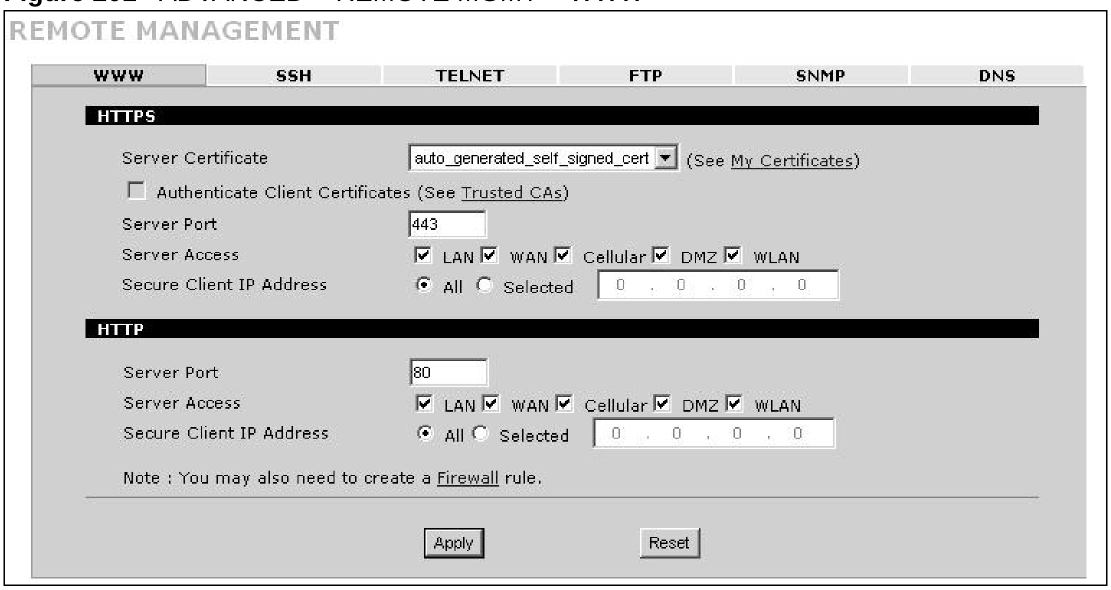
Figure 200 Secure FTP: Firmware Upload Example

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

15.3 WWW

Click **ADVANCED** > **REMOTE MGMT** to open the **WWW** screen. Use this screen to configure the LAN-Cell’s HTTP and HTTPS management settings.

Figure 201 ADVANCED > REMOTE MGMT > WWW



The following table describes the labels in this screen.

Table 119 ADVANCED > REMOTE MGMT > WWW

LABEL	DESCRIPTION
HTTPS	
Server Certificate	Select the **Server Certificate** that the LAN-Cell will use to identify itself. The LAN-Cell is the SSL server and must always authenticate itself to the SSL client (the computer which requests the HTTPS connection with the LAN-Cell).
Authenticate Client Certificates	Select **Authenticate Client Certificates** (optional) to require the SSL client to authenticate itself to the LAN-Cell by sending the LAN-Cell a certificate. To do that the SSL client must have a CA-signed certificate from a CA that has been imported as a trusted CA on the LAN-Cell (see Appendix G on page 629 on importing certificates for details).
Server Port	The HTTPS proxy server listens on port 443 by default. If you change the HTTPS proxy server port to a different number on the LAN-Cell, for example 8443, then you must notify people who need to access the LAN-Cell web configurator to use "https://LAN-Cell IP Address:**8443**" as the URL.
Server Access	Select the interface(s) through which a computer may access the LAN-Cell using this service. You can allow only secure web configurator access by clearing all of the interface check boxes in the **HTTP Server Access** field and setting the **HTTPS Server Access** field to an interface(s).
Secure Client IP Address	A secure client is a "trusted" computer that is allowed to communicate with the LAN-Cell using this service. Select **All** to allow any computer to access the LAN-Cell using this service. Choose **Selected** to just allow the computer with the IP address that you specify to access the LAN-Cell using this service.
HTTP	
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Server Access	Select the interface(s) through which a computer may access the LAN-Cell using this service.
Secure Client IP Address	A secure client is a "trusted" computer that is allowed to communicate with the LAN-Cell using this service. Select **All** to allow any computer to access the LAN-Cell using this service. Choose **Selected** to just allow the computer with the IP address that you specify to access the LAN-Cell using this service.
Apply	Click **Apply** to save your customized settings and exit this screen.
Reset	Click **Reset** to begin configuring this screen afresh.

15.4 The WWW (HTTP and HTTPS) Screen

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

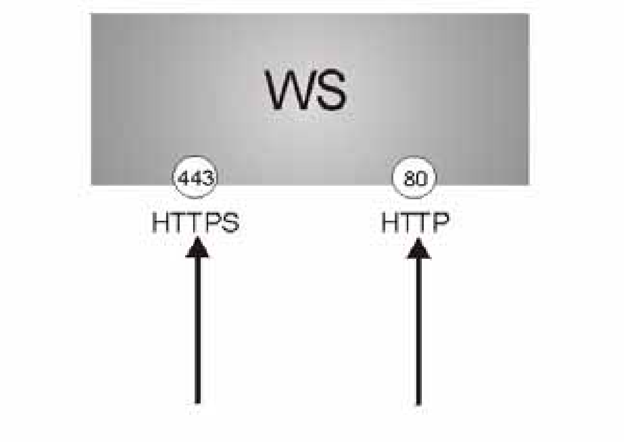
It relies upon certificates, public keys, and private keys (see Chapter 11 on page 255 for more information).

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

Please refer to the following figure.

1. HTTPS connection requests from an SSL-aware web browser go to port 443 (by default) on the LAN-Cell's WS (web server).
2. HTTP connection requests from a web browser go to port 80 (by default) on the LAN-Cell's WS (web server).

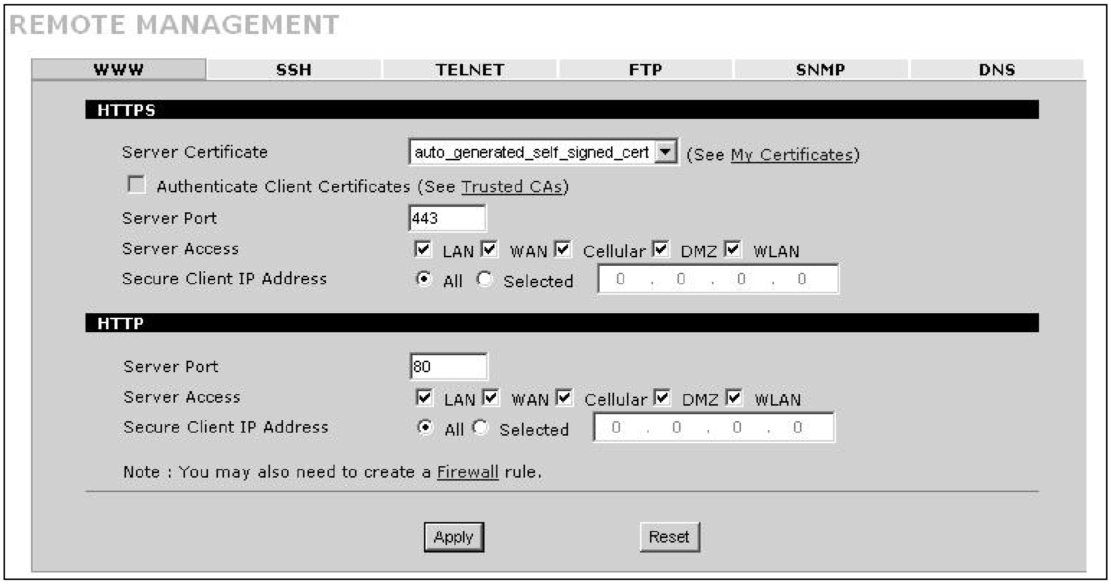
Figure 202 HTTPS Implementation



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

15.5 Configuring the WWW Screen

Click **ADVANCED** > **REMOTE MGMT** to open the **WWW** screen. ADVANCED > REMOTE MGMT > WWW



The following table describes the labels in this screen.

Table 120 ADVANCED > REMOTE MGMT > WWW

LABEL	DESCRIPTION
HTTPS	
Server Certificate	Select the **Server Certificate** that the LAN-Cell will use to identify itself. The LAN-Cell is the SSL server and must always authenticate itself to the SSL client (the computer which requests the HTTPS connection with the LAN-Cell).
Authenticate Client Certificates	Select **Authenticate Client Certificates** (optional) to require the SSL client to authenticate itself to the LAN-Cell by sending the LAN-Cell a certificate. To do that the SSL client must have a CA-signed certificate from a CA that has been imported as a trusted CA on the LAN-Cell (see Appendix G on page 629 on importing certificates for details).
Server Port	The HTTPS proxy server listens on port 443 by default. If you change the HTTPS proxy server port to a different number on the LAN-Cell, for example 8443, then you must notify people who need to access the LAN-Cell web configurator to use "https://LAN-Cell IP Address:**8443**" as the URL.
Server Access	Select the interface(s) through which a computer may access the LAN-Cell using this service. You can allow only secure web configurator access by clearing all of the interface check boxes in the **HTTP Server Access** field and setting the **HTTPS Server Access** field to an interface(s).
Secure Client IP Address	A secure client is a "trusted" computer that is allowed to communicate with the LAN-Cell using this service. Select **All** to allow any computer to access the LAN-Cell using this service. Choose **Selected** to just allow the computer with the IP address that you specify to access the LAN-Cell using this service.
HTTP	
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.

Table 120 ADVANCED > REMOTE MGMT > WWW (continued)

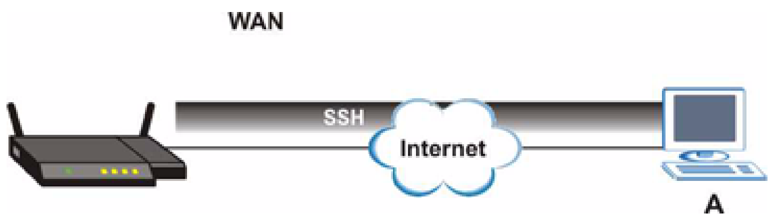
LABEL	DESCRIPTION
Server Access	Select the interface(s) through which a computer may access the LAN-Cell using this service.
Secure Client IP Address	A secure client is a “trusted” computer that is allowed to communicate with the LAN-Cell using this service. Select **All** to allow any computer to access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

15.6 The SSH Screen

You can use SSH (Secure SHell) to securely access the LAN-Cell’s SMT or command line interface. Specify which interfaces allow SSH access and from which IP address the access can come.

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

Figure 203 SSH Communication Over the WAN Example



SSH Implementation on the LAN-Cell

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

Requirements for Using SSH

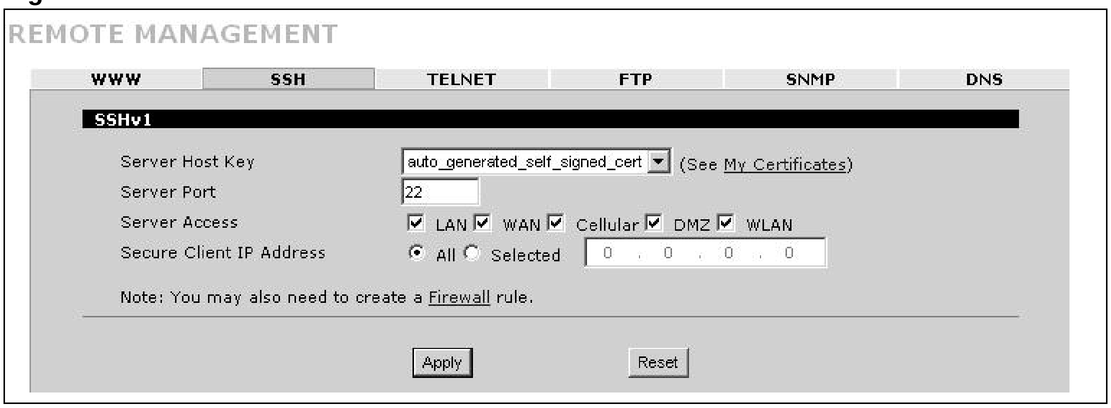
You must install an SSH client program on a client computer (Windows or Linux operating system) that is used to connect to the LAN-Cell over SSH.

15.7 Configuring the SSH Screen

Click **ADVANCED** > **REMOTE MGMT** > **SSH** to change your LAN-Cell's Secure Shell settings.

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

Figure 204 ADVANCED > REMOTE MGMT > SSH



The following table describes the labels in this screen.

Table 121 ADVANCED > REMOTE MGMT > SSH

LABEL	DESCRIPTION
Server Host Key	Select the certificate whose corresponding private key is to be used to identify the LAN-Cell for SSH connections. You must have certificates already configured in the **My Certificates** screen (Click **My Certificates** and see Chapter 11 on page 255 for details).
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Server Access	Select the interface(s) through which a computer may access the LAN-Cell using this service.
Secure Client IP Address	A secure client is a "trusted" computer that is allowed to communicate with the LAN-Cell using this service. Select **All** to allow any computer to access the LAN-Cell using this service. Choose **Selected** to just allow the computer with the IP address that you specify to access the LAN-Cell using this service.
Apply	Click **Apply** to save your customized settings and exit this screen.
Reset	Click **Reset** to begin configuring this screen afresh.

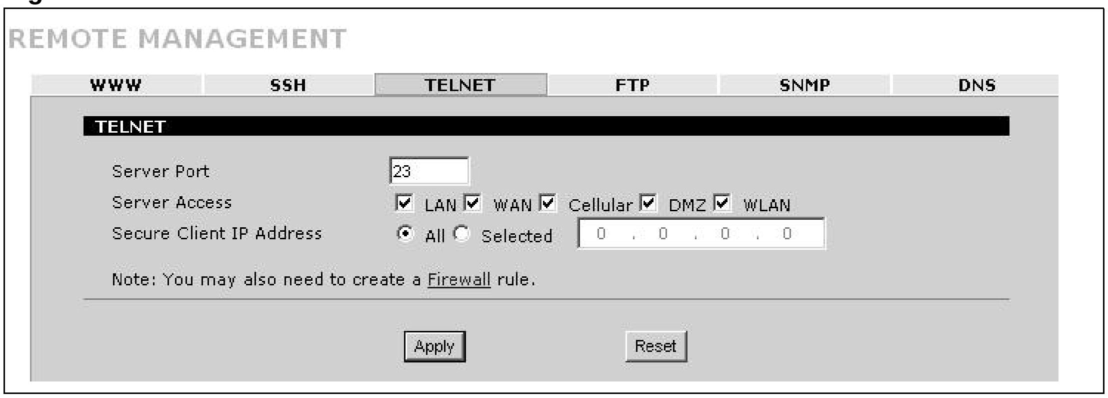
15.8 Telnet Screen

You can use Telnet to access the LAN-Cell's SMT or command line interface. Specify which interfaces allow Telnet access and from which IP address the access can come.

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

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

Figure 205 ADVANCED > REMOTE MGMT > Telnet



The following table describes the labels in this screen.

Table 122 ADVANCED > REMOTE MGMT > Telnet

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

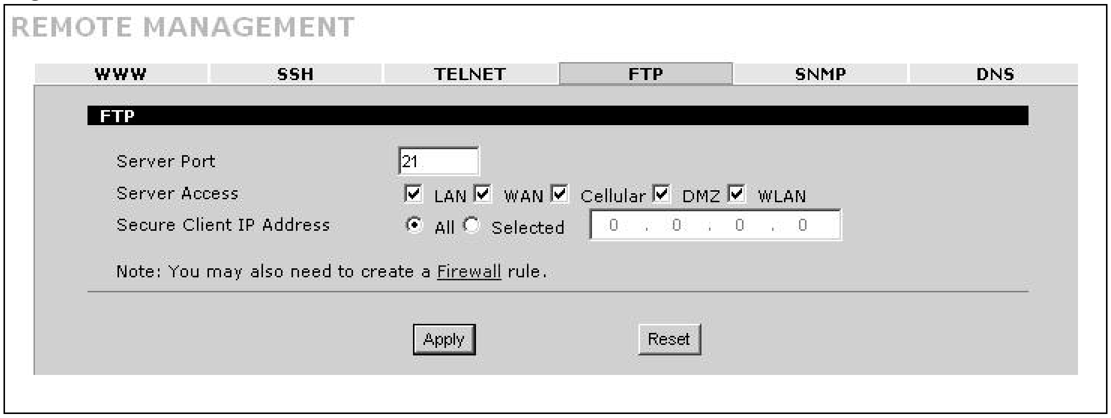
15.9 FTP Screen

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

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

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

Figure 206 ADVANCED > REMOTE MGMT > FTP



The following table describes the labels in this screen.

Table 123 ADVANCED > REMOTE MGMT > FTP

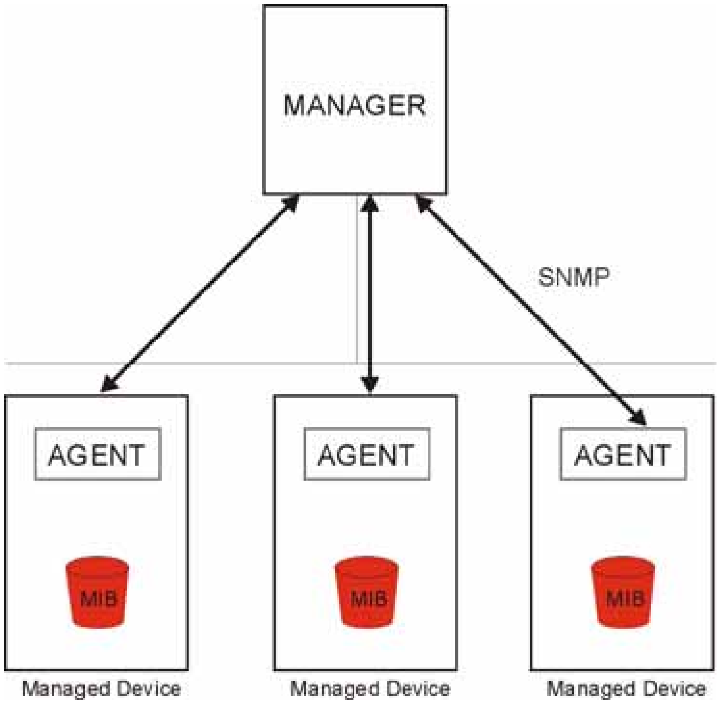
LABEL	DESCRIPTION
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Server Access	Select the interface(s) through which a computer may access the LAN-Cell using this service.
Secure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

15.10 SNMP Screen

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

SNMP is only available if TCP/IP is configured.

Figure 207 SNMP Management Model



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

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

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

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

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

Supported MIBs

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

SNMP Traps

The LAN-Cell will send traps to the SNMP manager when any one of the following events occurs:

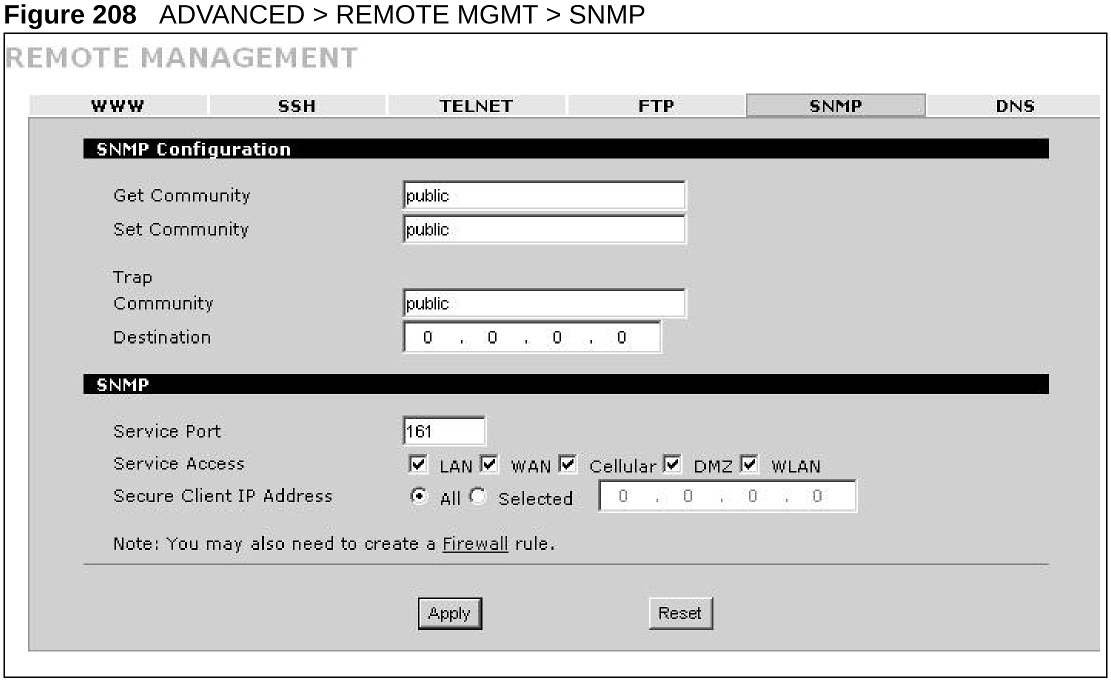
Table 124 SNMP Traps

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

15.10.1 Configuring the SNMP Screen

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

Figure 208 ADVANCED > REMOTE MGMT > SNMP



The following table describes the labels in this screen.

Table 125 ADVANCED > REMOTE MGMT > SNMP

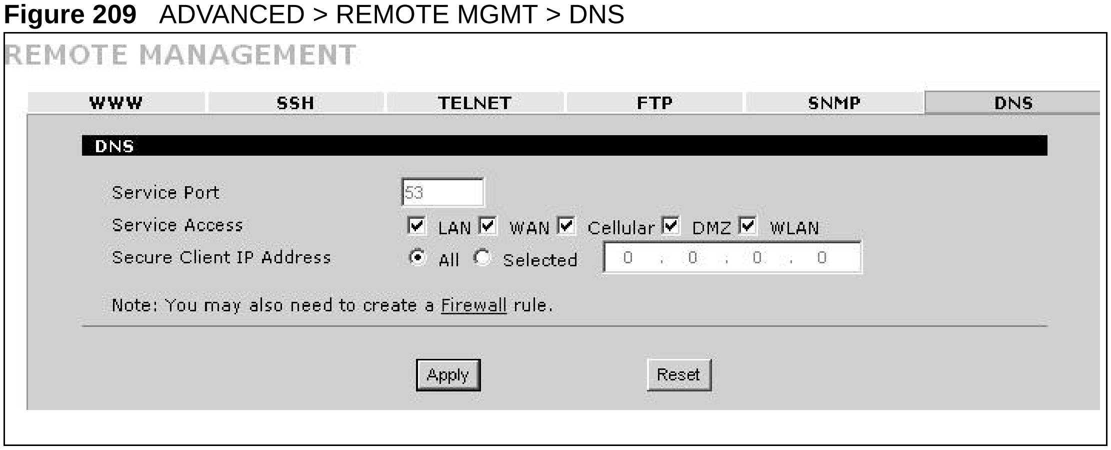
LABEL	DESCRIPTION
SNMP Configuration	
Get Community	Enter the **Get Community**, which is the password for the incoming Get and GetNext requests from the management station. The default is public and allows all requests.
Set Community	Enter the **Set community**, which is the password for incoming Set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

15.11 DNS Screen

Use DNS (Domain Name System) to map a domain name to its corresponding IP address and vice versa. Refer to Chapter 5 on page 89 for more information.

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

Figure 209 ADVANCED > REMOTE MGMT > DNS



The following table describes the labels in this screen.

Table 126 ADVANCED > REMOTE MGMT > DNS

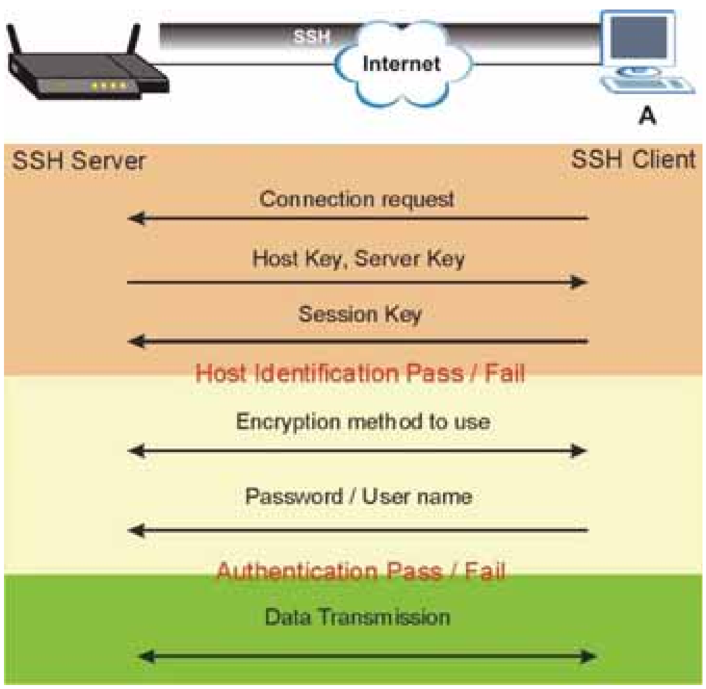
LABEL	DESCRIPTION
Server Port	The DNS service port number is 53 and cannot be changed here.
Service Access	Select the interface(s) through which a computer may send DNS queries to the LAN-Cell.
Secure Client IP Address	A secure client is a “trusted” computer that is allowed to send DNS queries to the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

15.12 Remote Management Technical Reference

How SSH Works

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

Figure 210 How SSH Works



1 Host Identification

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

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

2 Encryption Method

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

3 Authentication and Data Transmission

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

16

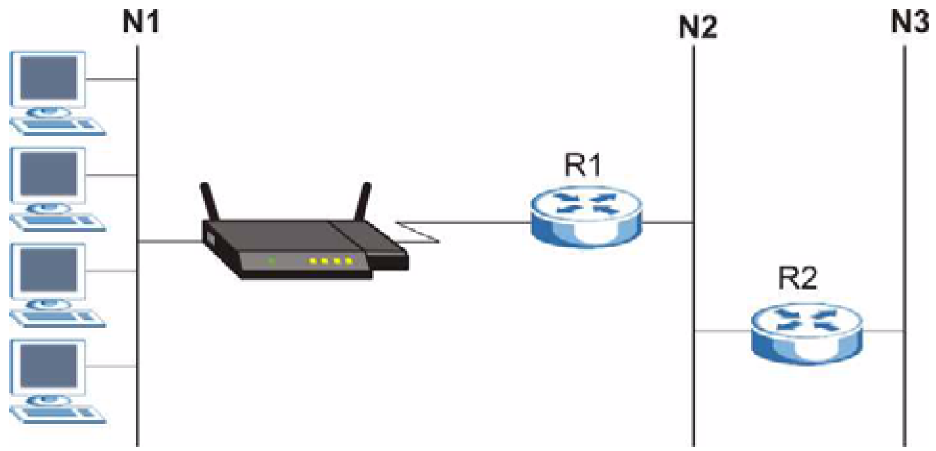
Static Route Screens

16.1 Overview

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

Each remote node specifies only the network to which the gateway is directly connected, and the LAN-Cell has no knowledge of the networks beyond. For instance, the LAN-Cell knows about network N2 in the following figure through remote node Router 1. However, the LAN-Cell is unable to route a packet to network N3 because it doesn't know that there is a route through the same remote node Router 1 (via gateway Router 2). The static routes are for you to tell the LAN-Cell about the networks beyond the remote nodes.

Figure 211 Example of Static Routing Topology



16.1.1 What You Can Do in the Static Route Screens

- Use the **IP Static Route** screen (Section 16.2 on page 339) to display the current static route entries.
- Use the **IP Static Route Edit** screen (Section 16.2.1 on page 341) to configure the required information for a static route.

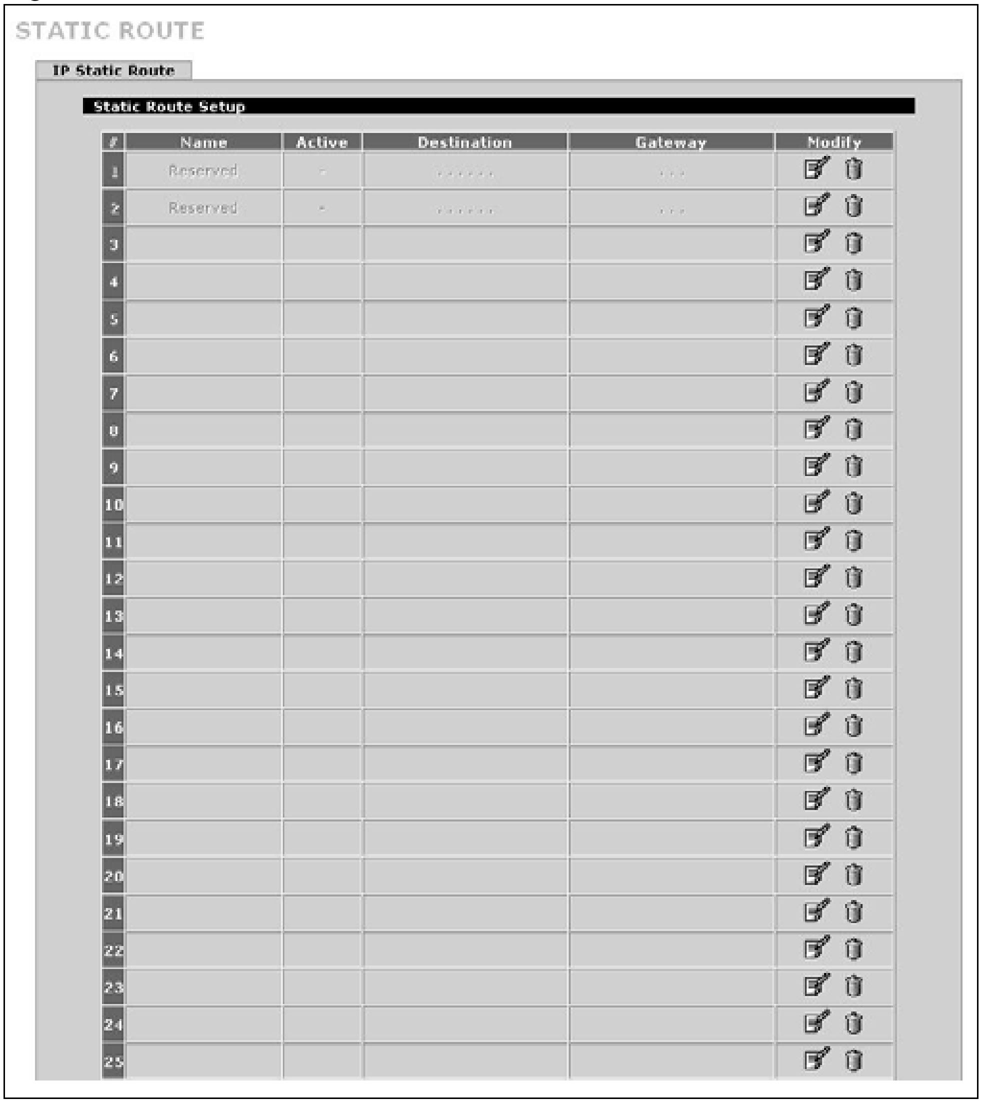
16.2 IP Static Route Screen

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

The first two static route entries are for default WAN and Cellular routes on a LAN-Cell with multiple WAN interfaces. You cannot modify or delete a static default route.

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

Figure 212 ADVANCED > STATIC ROUTE > IP Static Route



The following table describes the labels in this screen.

Table 127 ADVANCED > STATIC ROUTE > IP Static Route

LABEL	DESCRIPTION
#	This is the number of an individual static route.
Name	This is the name that describes or identifies this route.
Active	This field shows whether this static route is active (**Yes**) or not (**No**).
Destination	This parameter specifies the IP network address of the final destination. Routing is always based on network number.

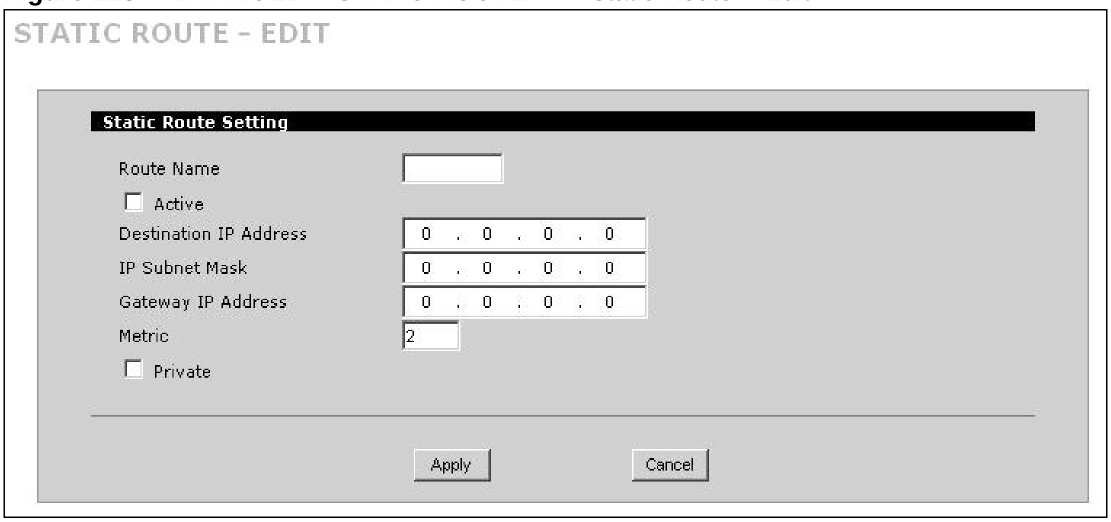
Table 127 ADVANCED > STATIC ROUTE > IP Static Route

LABEL	DESCRIPTION
Gateway	This is the IP address of the gateway. The gateway is a router or switch on the same network segment as the LAN-Cell's interface. The gateway helps forward packets to their destinations.
Modify	Click the edit icon to go to the screen where you can set up a static route on the LAN-Cell. Click the delete icon to remove a static route from the LAN-Cell. A window displays asking you to confirm that you want to delete the route.

16.2.1 IP Static Route Edit Screen

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

Figure 213 ADVANCED > STATIC ROUTE > IP Static Route > Edit



The following table describes the labels in this screen.

Table 128 ADVANCED > STATIC ROUTE > IP Static Route > Edit

LABEL	DESCRIPTION
Route Name	Enter the name of the IP static route. Leave this field blank to delete this static route.
Active	This field allows you to activate/deactivate this static route.
Destination IP Address	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
IP Subnet Mask	Enter the IP subnet mask here.
Gateway IP Address	Enter the IP address of the gateway. The gateway is a router or switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations.
Metric	Metric represents the "cost" of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Enter a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.

Table 128 ADVANCED > STATIC ROUTE > IP Static Route > Edit

LABEL	DESCRIPTION
Private	This parameter determines if the LAN-Cell will include this route to a remote node in its RIP broadcasts. Select this check box to keep this route private and not included in RIP broadcasts. Clear this check box to propagate this route to other hosts through RIP broadcasts.
Apply	Click **Apply** to save your changes back to the LAN-Cell.
Cancel	Click **Cancel** to exit this screen without saving.

17

Policy Route Screens

17.1 Overview

Traditionally, routing is based on the destination address only and the LAN-Cell takes the shortest path to forward a packet. IP Policy Routing (IPPR) provides a mechanism to override the default routing behavior and alter the packet forwarding based on the policy defined by the network administrator. Policy-based routing is applied to incoming packets on a per interface basis, prior to the normal routing.

17.1.1 What You Can Do in the Policy Route Screens

- Use the **Policy Route Summary** screen (Section 17.2 on page 344) to display the current policy route entries.
- Use the **Policy Route Edit** screen (Section 17.3 on page 345) to configure a policy route to override the default.

17.1.2 What You Need To Know About Policy Route

Benefits

- Source-Based Routing – Network administrators can use policy-based routing to direct traffic from different users through different connections.
- Quality of Service (QoS) – Organizations can differentiate traffic by setting the precedence or ToS (Type of Service) values in the IP header at the periphery of the network to enable the backbone to prioritize traffic.
- Cost Savings – IPPR allows organizations to distribute interactive traffic on high-bandwidth, high-cost paths while using low-cost paths for batch traffic.
- Load Sharing – Network administrators can use IPPR to distribute traffic among multiple paths.

Routing Policy

Individual routing policies are used as part of the overall IPPR process. A policy defines the matching criteria and the action to take when a packet meets the criteria. The action is taken only when all the criteria are met. The criteria include the source address and port, IP protocol (ICMP, UDP, TCP, etc.), destination address and port, ToS and precedence (fields in the IP header) and length. The inclusion of length criterion is to differentiate between interactive and bulk traffic. Interactive applications, e.g., telnet, tend to have short packets, while bulk traffic, e.g., file transfer, tends to have large packets.

The actions that can be taken include:

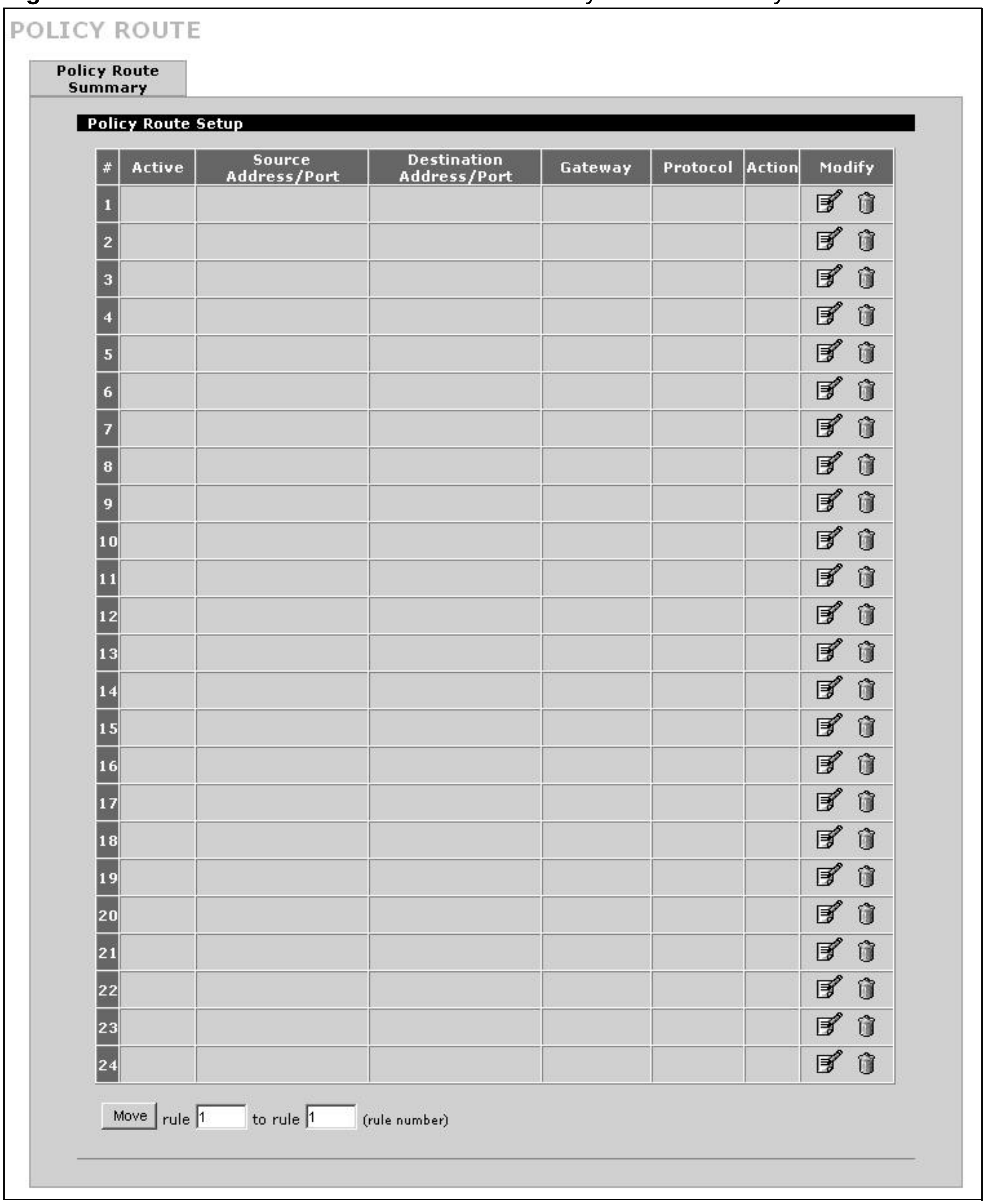
- Routing the packet to a different gateway (and hence the outgoing interface).
- Setting the ToS and precedence fields in the IP header.

IPPR follows the existing packet filtering facility of RAS in style and in implementation.

17.2 Policy Route Summary Screen

Click **ADVANCED** > **POLICY ROUTE** to open the **Policy Route Summary** screen.

Figure 214 ADVANCED > POLICY ROUTE > Policy Route Summary



The following table describes the labels in this screen.

Table 129 ADVANCED > POLICY ROUTE > Policy Route Summary

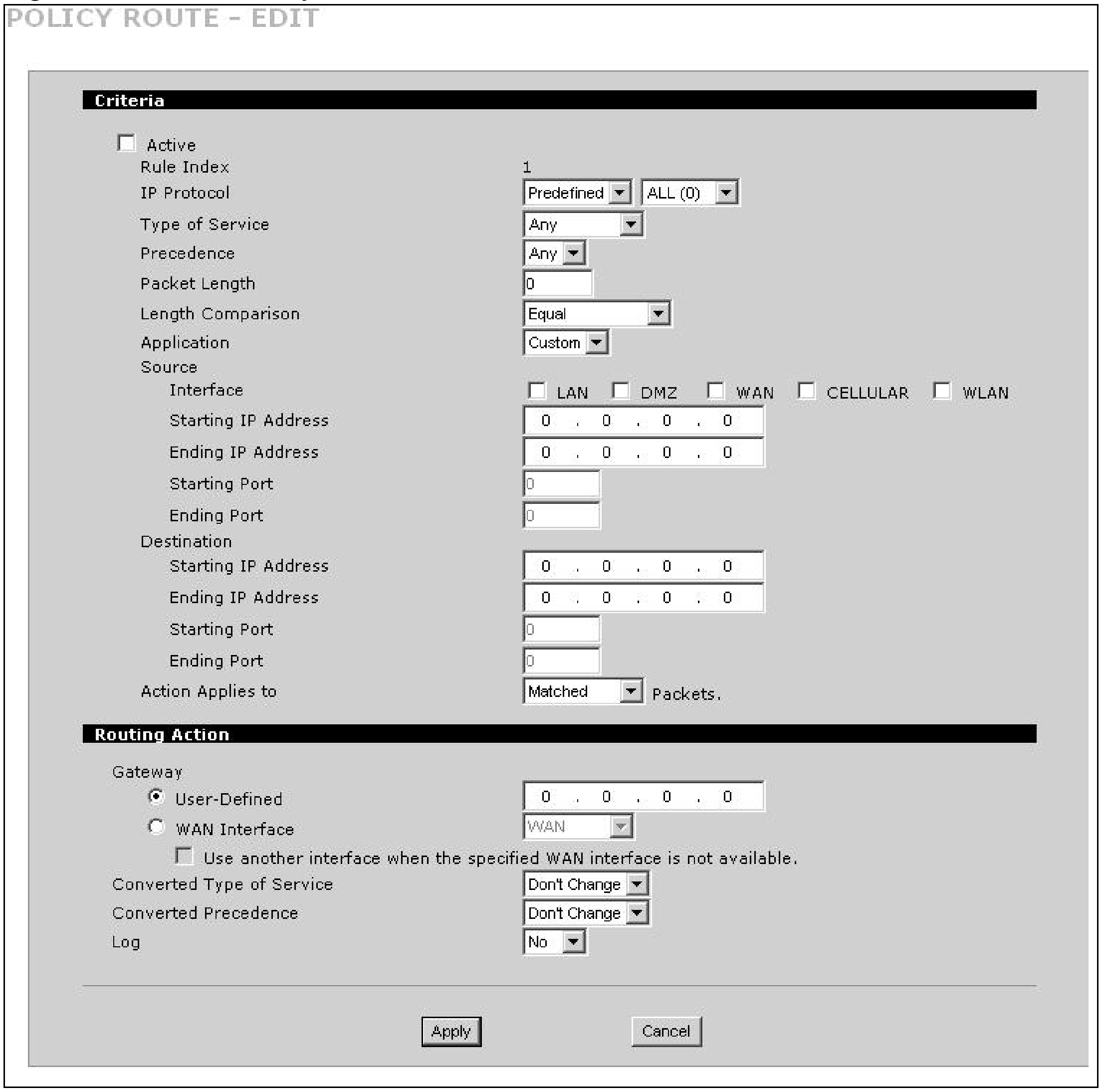
LABEL	DESCRIPTION
#	This is the number of an individual policy route.
Active	This field shows whether the policy is active or inactive.
Source Address/Port	This is the source IP address range and/or port number range.
Destination Address/Port	This is the destination IP address range and/or port number range.
Gateway	Enter the IP address of the gateway. The gateway is a router or switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations.
Protocol	This is the IP protocol and can be **ALL(0)**, **ICMP(1)**, **IGMP(2)**, **TCP(6)**, **UDP(17)**, **GRE(47)**, **ESP(50)** or **AH(51)**.
Action	This field specifies whether action should be taken on criteria **Matched** or **Not Matched**.
Modify	Click the edit icon to go to the screen where you can edit the routing policy on the LAN-Cell. Click the delete icon to remove an existing routing policy from the LAN-Cell. A window display asking you to confirm that you want to delete the routing policy.
Move	Type a policy route's index number and the 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.

17.3 Policy Route Edit Screen

Click **ADVANCED** > **POLICY ROUTE** to open the **Policy Route Summary** screen. Then click the edit icon to open the **Edit IP Policy Route** screen.

Use this screen to configure a policy route to override the default (shortest path) routing behavior and forward packets based on the criteria you specify. A policy route defines the matching criteria and the action to take when a packet meets the criteria. The action is taken only when all the criteria are met. Policy-based routing is applied to incoming packets on a per interface basis before normal routing. The LAN-Cell does not perform normal routing on packets that match any of the policy routes.

Figure 215 Edit IP Policy Route



The following table describes the labels in this screen.

Table 130 ADVANCED > POLICY ROUTE > Edit

LABEL	DESCRIPTION
Criteria	
Active	Select the check box to activate the policy.
Rule Index	This is the index number of the policy route.
IP Protocol	Select **Predefined** and then the IP protocol from **ALL(0)**, **ICMP(1)**, **IGMP(2)**, **TCP(6)**, **UDP(17)**, **GRE(47)**, **ESP(50)** or **AH(51)**. Otherwise, select **Custom** and enter a number from 0 to 255.
Type of Service	Prioritize incoming network traffic by choosing from **Any**, **Normal**, **Min Delay**, **Max Thruput**, **Max Reliable** or **Mix Cost**.
Precedence	Precedence value of the incoming packet. Select a value from **0** to **7** or **Any**.
Packet Length	Type a length of packet (in bytes). The operators in the **Len Compare** field apply to incoming packets of this length.

Table 130 ADVANCED > POLICY ROUTE > Edit (continued)

LABEL	DESCRIPTION
Length Comparison	Choose from **Equal**, **Not Equal**, **Less**, **Greater**, **Less or Equal** or **Greater or Equal**.
Application	Select a predefined application (**FTP**, **H.323** or **SIP**) for the policy rule. If you do not want to use a predefined application, select **Custom**. You can also configure the source and destination port numbers if you set **IP protocol** to **TCP** or **UDP**. **FTP** (File Transfer Program) is a program to enable fast transfer of files, including large files that may not be possible by e-mail. Select **FTP** to configure the policy rule for TCP packets with a port 21 destination. **H.323** is a protocol used for multimedia communications over networks, for example NetMeeting. Select **H.323** to configure the policy rule for TCP packets with a port 1720 destination. Note: If you select **H.323**, make sure you also use the **ALG** screen to turn on the H.323 ALG. **SIP** (Session Initiation Protocol) is a signaling protocol used in Internet telephony, instant messaging, events notification and conferencing. The LAN-Cell supports SIP traffic pass-through. Select **SIP** to configure the policy rule for UDP packets with a port 5060 destination. Note: If you select **SIP**, make sure you also use the **ALG** screen to turn on the SIP ALG.
Source	
Interface	Use the check box to select **LAN**, **DMZ**, **WAN**, **CELL** and/or **WLAN**.
Starting IP Address	Enter the source starting IP address.
Ending IP Address	Enter the source ending IP address.
Starting Port	Enter the source starting port number. This field is applicable only when you select **TCP** or **UDP** in the **IP Protocol** field and **Custom** in the **Application** field.
Ending Port	Enter the source ending port number. This field is applicable only when you select **TCP** or **UDP** in the **IP Protocol** field and **Custom** in the **Application** field.
Destination	
Starting IP Address	Enter the destination starting IP address.
Ending IP Address	Enter the destination ending IP address.
Starting Port	Enter the destination starting port number. This field is applicable only when you select **TCP** or **UDP** in the **IP Protocol** field and **Custom** in the **Application** field.
Ending Port	Enter the destination ending port number. This field is applicable only when you select **TCP** or **UDP** in the **IP Protocol** field and **Custom** in the **Application** field.
Action Applies to	Specifies whether action should be taken on criteria **Matched** or **Not Matched**.
Routing Action	

Table 130 ADVANCED > POLICY ROUTE > Edit (continued)

LABEL	DESCRIPTION
Gateway	Select **User-Defined** and enter the IP address of the gateway if you want to specify the IP address of the gateway. The gateway is an immediate neighbor of your LAN-Cell that will forward the packet to the destination. The gateway must be a router on the same segment as your LAN-Cell's LAN or WAN interface. Select **WAN Interface** to have the LAN-Cell send traffic that matches the policy route through a specific WAN interface. Select the WAN interface from the drop-down list box. Select the **Use another interface when the specified WAN interface is not available.** check box to have the LAN-Cell send traffic that matches the policy route through the other WAN interface if it cannot send the traffic through the WAN interface you selected. This option is only available when you select **WAN Interface**.
Converted Type of Service	Set the new TOS value of the outgoing packet. Prioritize incoming network traffic by choosing **Don’t Change**, **Normal**, **Min Delay**, **Max Thruput**, **Max Reliable** or **Min Cost**.
Converted Precedence	Set the new outgoing packet precedence value. Values are **0** to **7** or **Don’t Change**.
Log	Select **Yes** from the drop-down list box to make an entry in the system log when a policy is executed.
Apply	Click **Apply** to save your changes back to the LAN-Cell.
Cancel	Click **Cancel** to exit this screen without saving.

18

Bandwidth Management Screens

18.1 Overview

Bandwidth management allows you to allocate an interface's outgoing capacity to specific types of traffic. It can also help you make sure that the LAN-Cell forwards certain types of traffic (especially real-time applications) with minimum delay. With the use of real-time applications such as Voice-over-IP (VoIP) increasing, the requirement for bandwidth allocation is also increasing.

Bandwidth management addresses questions such as:

- Who gets how much access to specific applications?
- What priority level should you give to each type of traffic?
- Which traffic must have guaranteed delivery?
- How much bandwidth should be allotted to guarantee delivery?

Bandwidth management also allows you to configure the allowed output for an interface to match what the network can handle. This helps reduce delays and dropped packets at the next routing device. For example, you can set the WAN interface speed to 1024 kbps (or less) if the broadband device connected to the WAN port has an upstream speed of 1024 kbps.

18.1.1 What You Can Do in the Bandwidth Management Screens

- Use the **Summary** screen (Section 18.2 on page 354) to enable bandwidth management on an interface and set the maximum allowed bandwidth for that interface.
- Use the **Class Setup** screen (Section 18.3 on page 356) to view the configured bandwidth classes by individual interface and to to set up a bandwidth class's name, bandwidth allotment, and bandwidth filter.
- Use the **Monitor** screen (Section 18.4 on page 362) to view the device's bandwidth usage and allotments.

18.1.2 What You Need to Know About Bandwidth Management

Bandwidth Classes and Filters

Use bandwidth classes and sub-classes to allocate specific amounts of bandwidth capacity (bandwidth budgets). Configure a bandwidth filter to define a bandwidth class (or sub-class) based on a specific application and/or subnet. Use the **Class Setup** screen (see Section 18.3.1 on page 357) to set up a bandwidth class's name, bandwidth allotment, and bandwidth filter. You can configure up to one bandwidth filter per bandwidth class. You can also configure bandwidth classes without bandwidth filters. However, it is recommended that you configure sub-classes with filters for any classes that you configure without filters. The LAN-Cell leaves the bandwidth budget allocated and unused for a class that does not have a filter or sub-classes with filters. View your configured bandwidth classes and sub-classes in the **Class Setup** screen (see Section 18.3 on page 356 for details).

The total of the configured bandwidth budgets for sub-classes cannot exceed the configured bandwidth budget speed of the parent class.

Proportional Bandwidth Allocation

Bandwidth management allows you to define how much bandwidth each class gets; however, the actual bandwidth allotted to each class decreases or increases in proportion to actual available bandwidth.

Application-based Bandwidth Management

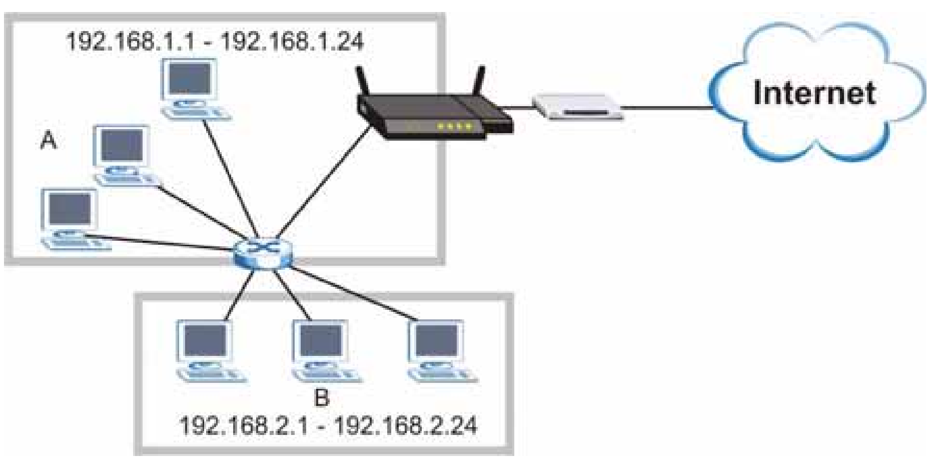
You can create bandwidth classes based on individual applications (like VoIP, Web, FTP, E-mail and Video for example).

Subnet-based Bandwidth Management

You can create bandwidth classes based on subnets.

The following figure shows LAN subnets. You could configure one bandwidth class for subnet A and another for subnet B.

Figure 216 Subnet-based Bandwidth Management Example



Scheduler

The scheduler divides up an interface's bandwidth among the bandwidth classes. The LAN-Cell has two types of scheduler: fairness-based and priority-based.

Priority-based Scheduler

With the priority-based scheduler, the LAN-Cell forwards traffic from bandwidth classes according to the priorities that you assign to the bandwidth classes. The larger a bandwidth class's priority number is, the higher the priority. Assign real-time applications (like those using audio or video) a higher priority number to provide smoother operation.

Fairness-based Scheduler

The LAN-Cell divides bandwidth equally among bandwidth classes when using the fairness-based scheduler; thus preventing one bandwidth class from using all of the interface's bandwidth.

Maximize Bandwidth Usage

The maximize bandwidth usage option allows the LAN-Cell to divide up any available bandwidth on the interface (including unallocated bandwidth and any allocated bandwidth that a class is not using) among the bandwidth classes that require more bandwidth.

When you enable maximize bandwidth usage, the LAN-Cell first makes sure that each bandwidth class gets up to its bandwidth allotment. Next, the LAN-Cell divides up an interface's available bandwidth (bandwidth that is unbudgeted or unused by the classes) depending on how many bandwidth classes require more bandwidth and on their priority levels. When only one class requires more bandwidth, the LAN-Cell gives extra bandwidth to that class.

When multiple classes require more bandwidth, the LAN-Cell gives the highest priority classes the available bandwidth first (as much as they require, if there is enough available bandwidth), and then to lower priority classes if there is still bandwidth available. The LAN-Cell distributes the available bandwidth equally among classes with the same priority level.

18.1.3 Bandwidth Management Examples

18.1.3.1 Application and Subnet-based Bandwidth Management Example

You could also create bandwidth classes based on a combination of a subnet and an application. The following example table shows bandwidth allocations for application specific traffic from separate LAN subnets.

Table 131 Application and Subnet-based Bandwidth Management Example

TRAFFIC TYPE	FROM SUBNET A	FROM SUBNET B
VoIP	64 Kbps	64 Kbps
Web	64 Kbps	64 Kbps
FTP	64 Kbps	64 Kbps
E-mail	64 Kbps	64 Kbps
Video	64 Kbps	64 Kbps

18.1.3.2 Maximize Bandwidth Usage Example

If you configure both maximize bandwidth usage (on the interface) and bandwidth borrowing (on individual sub-classes), the LAN-Cell functions as follows.

1 The LAN-Cell sends traffic according to each bandwidth class's bandwidth budget.
2 The LAN-Cell assigns a parent class's unused bandwidth to its sub-classes that have more traffic than their budgets and have bandwidth borrowing enabled. The LAN-Cell gives priority to sub-classes of higher priority and treats classes of the same priority equally.
3 The LAN-Cell assigns any remaining unused or unbudgeted bandwidth on the interface to any class that requires it. The LAN-Cell gives priority to classes of higher priority and treats classes of the same level equally.
4 If the bandwidth requirements of all of the traffic classes are met and there is still some unbudgeted bandwidth, the LAN-Cell assigns it to traffic that does not match any of the classes.

18.1.3.3 Over Allotment of Bandwidth Example

It is possible to set the bandwidth management speed for an interface higher than the interface's actual transmission speed. Higher priority traffic gets to use up to its allocated bandwidth, even if it takes up all of the interface's available bandwidth. This could stop lower priority traffic from being sent. The following is an example.

Table 132 Over Allotment of Bandwidth Example

BANDWIDTH CLASSES, ALLOTMENTS		PRIORITIES
Actual outgoing bandwidth available on the interface: 1000 kbps		
Root Class: 1500 kbps (same as Speed setting)	VoIP traffic (Service = SIP): 500 Kbps	7
	NetMeeting traffic (Service = H.323): 500 kbps	7
	FTP (Service = FTP): 500 Kbps	3

If you use VoIP and NetMeeting at the same time, the device allocates up to 500 Kbps of bandwidth to each of them before it allocates any bandwidth to FTP. As a result, FTP can only use bandwidth when VoIP and NetMeeting do not use all of their allocated bandwidth.

Suppose you try to browse the web too. In this case, VoIP, NetMeeting and FTP all have higher priority, so they get to use the bandwidth first. You can only browse the web when VoIP, NetMeeting, and FTP do not use all 1000 Kbps of available bandwidth.

18.1.3.4 Maximize Bandwidth Usage Example

Here is an example of a LAN-Cell that has maximize bandwidth usage enabled on an interface. The following table shows each bandwidth class's bandwidth budget. The classes are set up based on subnets. The interface is set to 10240 kbps. Each subnet is allocated 2048 kbps. The unbudgeted 2048 kbps allows traffic not defined in any of the bandwidth filters to go out when you do not select the maximize bandwidth option.

Table 133 Maximize Bandwidth Usage Example

BANDWIDTH CLASSES AND ALLOTMENTS	
Root Class: 10240 kbps	Administration: 2048 kbps
	Sales: 2048 kbps
	Marketing: 2048 kbps
	Research: 2048 kbps

The LAN-Cell divides up the unbudgeted 2048 kbps among the classes that require more bandwidth. If the administration department only uses 1024 kbps of the budgeted 2048 kbps, the LAN-Cell also divides the remaining 1024 kbps among the classes that require more bandwidth. Therefore, the LAN-Cell divides a total of 3072 kbps of unbudgeted and unused bandwidth among the classes that require more bandwidth.

18.1.3.5 Priority-based Allotment of Unused and Unbudgeted Bandwidth Example

The following table shows the priorities of the bandwidth classes and the amount of bandwidth that each class gets.

Table 134 Priority-based Allotment of Unused and Unbudgeted Bandwidth Example

BANDWIDTH CLASSES, PRIORITIES AND ALLOTMENTS	
Root Class: 10240 kbps	Administration: Priority 4, 1024 kbps
	Sales: Priority 6, 3584 kbps
	Marketing: Priority 6, 3584 kbps
	Research: Priority 5, 2048 kbps

Suppose that all of the classes except for the administration class need more bandwidth.

- Each class gets up to its budgeted bandwidth. The administration class only uses 1024 kbps of its budgeted 2048 kbps.
- The sales and marketing are first to get extra bandwidth because they have the highest priority (6). If they each require 1536 kbps or more of extra bandwidth, the LAN-Cell divides the total 3072 kbps total of unbudgeted and unused bandwidth equally between the sales and marketing departments (1536 kbps extra to each for a total of 3584 kbps for each) because they both have the highest priority level.
- Research requires more bandwidth but only gets its budgeted 2048 kbps because all of the unbudgeted and unused bandwidth goes to the higher priority sales and marketing classes.

18.1.3.6 Fairness-based Allotment of Unused and Unbudgeted Bandwidth Example

The following table shows the amount of bandwidth that each class gets.

Table 135 Fairness-based Allotment of Unused and Unbudgeted Bandwidth Example

BANDWIDTH CLASSES AND ALLOTMENTS	
Root Class: 10240 kbps	Administration: 1024 kbps
	Sales: 3072 kbps
	Marketing: 3072 kbps
	Research: 3072 kbps

Suppose that all of the classes except for the administration class need more bandwidth.

- Each class gets up to its budgeted bandwidth. The administration class only uses 1024 kbps of its budgeted 2048 kbps.
- The LAN-Cell divides the total 3072 kbps total of unbudgeted and unused bandwidth equally among the other classes. 1024 kbps extra goes to each so the other classes each get a total of 3072 kbps.

18.1.3.7 Reserving Bandwidth for Non-Bandwidth Class Traffic Example

Do the following three steps to configure the LAN-Cell to allow bandwidth for traffic that is not defined in a bandwidth filter.

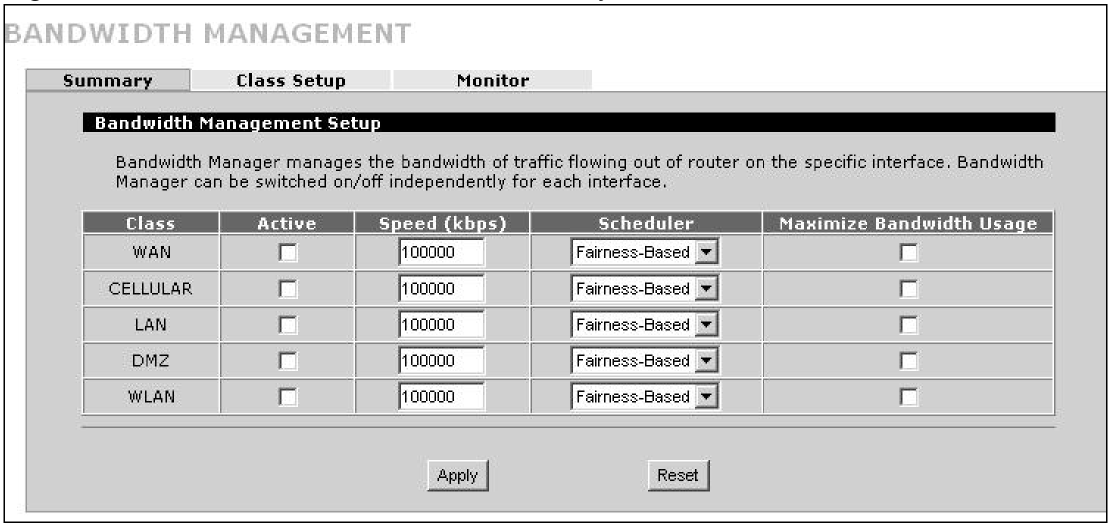
1. Leave some of the interface's bandwidth unbudgeted.
2. Do not enable the interface's **Maximize Bandwidth Usage** option.
3. Do not enable bandwidth borrowing on the sub-classes that have the root class as their parent (see Section on page 357).

18.2 Bandwidth Management Summary Screen

Click **ADVANCED** > **BW MGMT** to open the **Summary** screen.

Enable bandwidth management on an interface and set the maximum allowed bandwidth for that interface.

Figure 217 ADVANCED > BW MGMT > Summary



The following table describes the labels in this screen.

Table 136 ADVANCED > BW MGMT > Summary

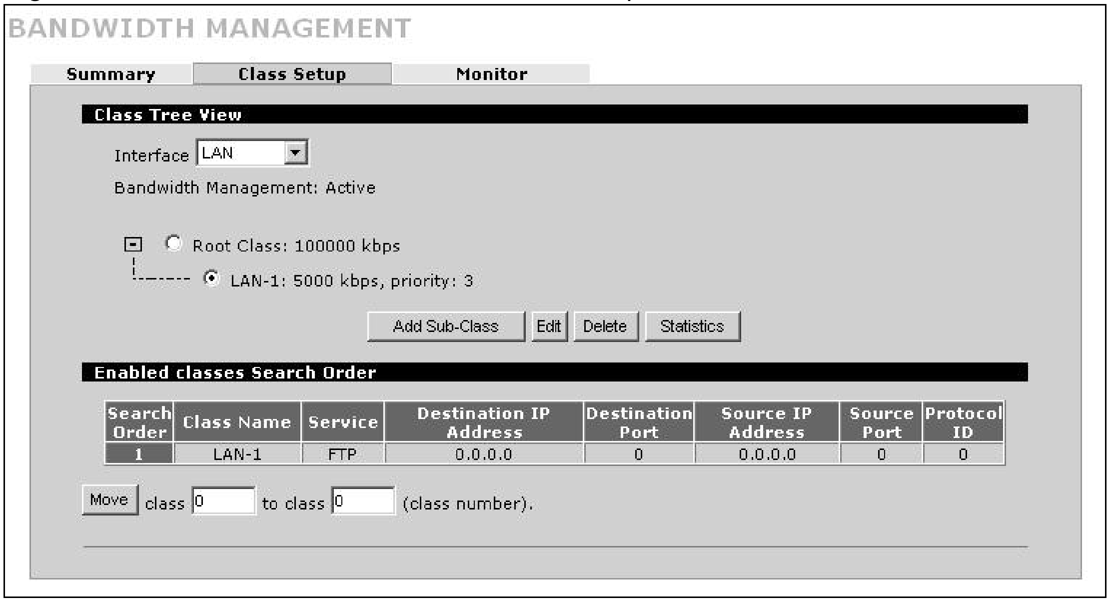
LABEL	DESCRIPTION
Class	These read-only labels represent the physical interfaces. Select an interface's check box to enable bandwidth management on that interface. Bandwidth management applies to all traffic flowing out of the router through the interface, regardless of the traffic's source. Traffic redirect or IP alias may cause LAN-to-LAN or DMZ-to-DMZ traffic to pass through the LAN-Cell and be managed by bandwidth management.
Active	Select an interface's check box to enable bandwidth management on that interface.
Speed (kbps)	Enter the amount of bandwidth for this interface that you want to allocate using bandwidth management. This appears as the bandwidth budget of the interface's root class (see Section 18.3 on page 356). The recommendation is to set this speed to match what the device connected to the port can handle. For example, set the WAN interface speed to 1000 kbps if the broadband device connected to the WAN port has an upstream speed of 1000 kbps. The recommendation is to set this speed to match the interface's actual transmission speed. For example, set the WAN interface speed to 1000 kbps if your Internet connection has an upstream transmission speed of 1 Mbps. You can set this number higher than the interface's actual transmission speed. This will stop lower priority traffic from being sent if higher priority traffic uses all of the actual bandwidth. You can also set this number lower than the interface's actual transmission speed. If you do not enable **Max Bandwidth Usage**, this will cause the LAN-Cell to not use some of the interface's available bandwidth.
Scheduler	Select either **Priority-Based** or **Fairness-Based** from the drop-down menu to control the traffic flow. Select **Priority-Based** to give preference to bandwidth classes with higher priorities. Select **Fairness-Based** to treat all bandwidth classes equally. See Section on page 351.
Maximize Bandwidth Usage	Select this check box to have the LAN-Cell divide up all of the interface's unallocated and/or unused bandwidth among the bandwidth classes that require bandwidth. Do not select this if you want to reserve bandwidth for traffic that does not match a bandwidth class (see Section 18.1.3 on page 351) or you want to limit the speed of this interface (see the **Speed** field description).
Apply	Click **Apply** to save your changes back to the LAN-Cell.
Reset	Click **Reset** to begin configuring this screen afresh.

18.3 Class Setup Screen

The **Class Setup** screen displays the configured bandwidth classes by individual interface. Select an interface and click the buttons to perform the actions described next. Click "+" to expand the class tree or click "-" to collapse the class tree. Each interface has a permanent root class. The bandwidth budget of the root class is equal to the speed you configured on the interface (see Section 18.2 on page 354 to configure the speed of the interface). Configure sub-class layers for the root class.

To add or delete child classes on an interface, click **ADVANCED** > **BW MGMT** > **Class Setup**. The screen is shown here with example classes.

Figure 218 ADVANCED > BW MGMT > Class Setup



The following table describes the labels in this screen.

Table 137 ADVANCED > BW MGMT > Class Setup

LABEL	DESCRIPTION
Interface	Select an interface for which you want to set up bandwidth management classes. Bandwidth management controls outgoing traffic on an interface, not incoming. So, in order to limit the download bandwidth of the LAN users, set the bandwidth management class on the LAN. In order to limit the upload bandwidth, set the bandwidth management class on the corresponding WAN interface.
Bandwidth Management	This field displays whether bandwidth management on the interface you selected in the field above is enabled (**Active**) or not (**Inactive**).
	After you select an interface, the bandwidth management classes configured for the interface display. The name, bandwidth and priority display for each class. "borrow" also displays if the class is set to use bandwidth from its parent class if the parent class is not using up its bandwidth budget.
Add Sub-Class	Click **Add Sub-class** to add a sub-class.
Edit	Click **Edit** to configure the selected class. You cannot edit the root class.
Delete	Click **Delete** to delete the class and all its sub-classes. You cannot delete the root class.
Statistics	Click **Statistics** to display the status of the selected class.

Table 137 ADVANCED > BW MGMT > Class Setup (continued)

LABEL	DESCRIPTION
Enabled classes Search Order	This list displays the interface’s active bandwidth management classes (the ones that have the bandwidth filter enabled). The LAN-Cell applies the classes in the order that they appear here. Once a connection matches a bandwidth management class, the LAN-Cell applies the class’s rules and does not check the connection against any other bandwidth management classes.
Search Order	This is the index number of an individual bandwidth management class.
Class Name	This is the name that identifies a bandwidth management class.
Service	This is the service that this bandwidth management class is configured to manage.
Destination IP Address	This is the destination IP address for connections to which this bandwidth management class applies.
Destination Port	This is the destination port for connections to which this bandwidth management class applies.
Source IP Address	This is the source IP address for connections to which this bandwidth management class applies.
Source Port	This is the source port for connections to which this bandwidth management class applies.
Protocol ID	This is the protocol ID (service type) number for connections to which this bandwidth management class applies. For example: 1 for ICMP, 6 for TCP or 17 for UDP.
Move	Type a class’s index number and the number for where you want to put that class. Click **Move** to move the class to the number that you typed. The ordering of your classes is important as they are applied in order of their numbering.

18.3.1 Bandwidth Manager Class Configuration

Configure a bandwidth management class in the **Class Setup** screen. You must use the **Summary** screen to enable bandwidth management on an interface before you can configure classes for that interface.

Bandwidth Borrowing

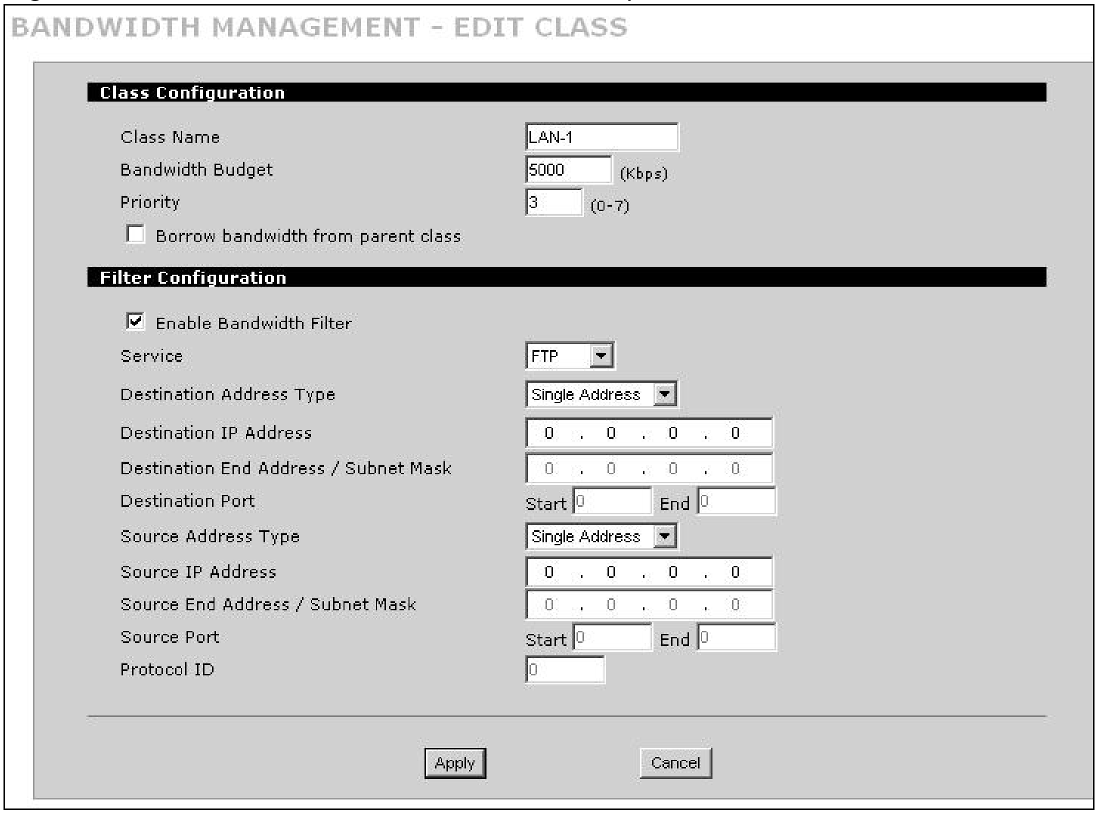
Bandwidth borrowing allows a sub-class to borrow unused bandwidth from its parent class, whereas maximize bandwidth usage allows bandwidth classes to borrow any unused or unbudgeted bandwidth on the whole interface.

Enable bandwidth borrowing on a sub-class to allow the sub-class to use its parent class’s unused bandwidth. A parent class’s unused bandwidth is given to the highest priority sub-class first. The sub-class can also borrow bandwidth from a higher parent class (grandparent class) if the sub-class’s parent class is also configured to borrow bandwidth from its parent class. This can go on for as many levels as are configured to borrow bandwidth from their parent class (see Section 18.3.1.1 on page 360).

The total of the bandwidth allotments for sub-classes cannot exceed the bandwidth allotment of their parent class. The LAN-Cell uses the scheduler to divide a parent class’s unused bandwidth among the sub-classes.

Click **ADVANCED** > **BW MGMT** > **Class Setup** > **Add Sub-Class** or **Edit** to open the following screen. Use this screen to add a child class.

Figure 219 ADVANCED > BW MGMT > Class Setup > Add Sub-Class



The following table describes the labels in this screen.

Table 138 ADVANCED > BW MGMT > Class Setup > Add Sub-Class

LABEL	DESCRIPTION
Class Configuration	
Class Name	Use the auto-generated name or enter a descriptive name of up to 20 alphanumeric characters, including spaces.
Bandwidth Budget (kbps)	Specify the maximum bandwidth allowed for the class in kbps. The recommendation is a setting between 20 kbps and 20000 kbps for an individual class.
Priority	Enter a number between 0 and 7 to set the priority of this class. The higher the number, the higher the priority. The default setting is 3.
Borrow bandwidth from parent class	Select this option to allow a sub-class to borrow bandwidth from its parent class if the parent class is not using up its bandwidth budget. Bandwidth borrowing is governed by the priority of the sub-classes. That is, a sub-class with the highest priority (7) is the first to borrow bandwidth from its parent class. Do not select this for the classes directly below the root class if you want to leave bandwidth available for other traffic types (see Section 18.1.3 on page 351) or you want to set the interface's speed to match what the next device in network can handle (see the **Speed** field description in Table 136 on page 355).
Filter Configuration	

Table 138 ADVANCED > BW MGMT > Class Setup > Add Sub-Class (continued)

LABEL	DESCRIPTION
Enable Bandwidth Filter	Select **Enable Bandwidth Filter** to have the LAN-Cell use this bandwidth filter when it performs bandwidth management. You must enter a value in at least one of the following fields (other than the **Subnet Mask** fields which are only available when you enter the destination or source IP address).
Service	This field simplifies bandwidth class configuration by allowing you to select a predefined application. When you select a predefined application, you do not configure the rest of the bandwidth filter fields (other than enabling or disabling the filter). **FTP** (File Transfer Program) is a program to enable fast transfer of files, including large files that may not be possible by e-mail. Select FTP from the drop-down list box to configure the bandwidth filter for TCP packets with a port 21 destination. **H.323** is a protocol used for multimedia communications over networks, for example NetMeeting. Select **H.323** from the drop-down list box to configure the bandwidth filter for TCP packets with a port 1720 destination. Note: If you select **H.323**, make sure you also use the **ALG** screen to turn on the H.323 ALG. **SIP** (Session Initiation Protocol) is a signaling protocol used in Internet telephony, instant messaging, events notification and conferencing. The LAN-Cell supports SIP traffic pass-through. Select **SIP** from the drop-down list box to configure this bandwidth filter for UDP packets with a port 5060 destination. This option makes it easier to manage bandwidth for SIP traffic and is useful for example when there is a VoIP (Voice over Internet Protocol) device on your LAN. Note: If you select **SIP**, make sure you also use the **ALG** screen to turn on the SIP ALG. Select **Custom** from the drop-down list box if you do not want to use a predefined application for the bandwidth class. When you select **Custom**, you need to configure at least one of the following fields (other than the **Subnet Mask** fields which you only enter if you also enter a corresponding destination or source IP address).
Destination Address Type	Do you want your rule to apply to packets coming going to a particular (single) IP, a range of IP addresses (for example 192.168.1.10 to 192.169.1.50) or a subnet? Select **Single Address, Range Address** or **Subnet Address**.
Destination IP Address	Enter the single IP address or the starting IP address in a range here.
Destination End Address / Subnet Mask	If you are configuring a range of IP addresses, enter the ending IP address here. If you are configuring a subnet of addresses, enter the subnet mask here. Refer to Appendix C on page 605 for more information on IP subnetting.
Destination Port	Enter the starting and ending destination port numbers. Enter the same port number in both fields to specify a single port number. See Appendix D on page 613 for a table of services and port numbers.
Source Address Type	Do you want your rule to apply to packets coming from a particular (single) IP, a range of IP addresses (for example 192.168.1.10 to 192.169.1.50) or a subnet? Select **Single Address, Range Address** or **Subnet Address**.
Source IP Address	Enter the single IP address or the starting IP address in a range here.

Table 138 ADVANCED > BW MGMT > Class Setup > Add Sub-Class (continued)

LABEL	DESCRIPTION
Source End Address / Subnet Mask	If you are configuring a range of IP addresses, enter the ending IP address here. If you are configuring a subnet of addresses, enter the subnet mask here. Refer to Appendix C on page 605 for more information on IP subnetting.
Source Port	Enter the starting and ending destination port numbers. Enter the same port number in both fields to specify a single port number. See Appendix D on page 613 for a table of services and port numbers.
Protocol ID	Enter the protocol ID (service type) number, for example: 1 for ICMP, 6 for TCP or 17 for UDP.
Apply	Click **Apply** to save your changes back to the LAN-Cell.
Cancel	Click **Cancel** to exit this screen without saving.

Table 139 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

18.3.1.1 Bandwidth Borrowing Example

Here is an example of bandwidth management with classes configured for bandwidth borrowing. The classes are set up based on departments and individuals within certain departments.

Refer to the product specifications in the appendix to see how many class levels you can configure on your LAN-Cell.

Table 140 Bandwidth Borrowing Example

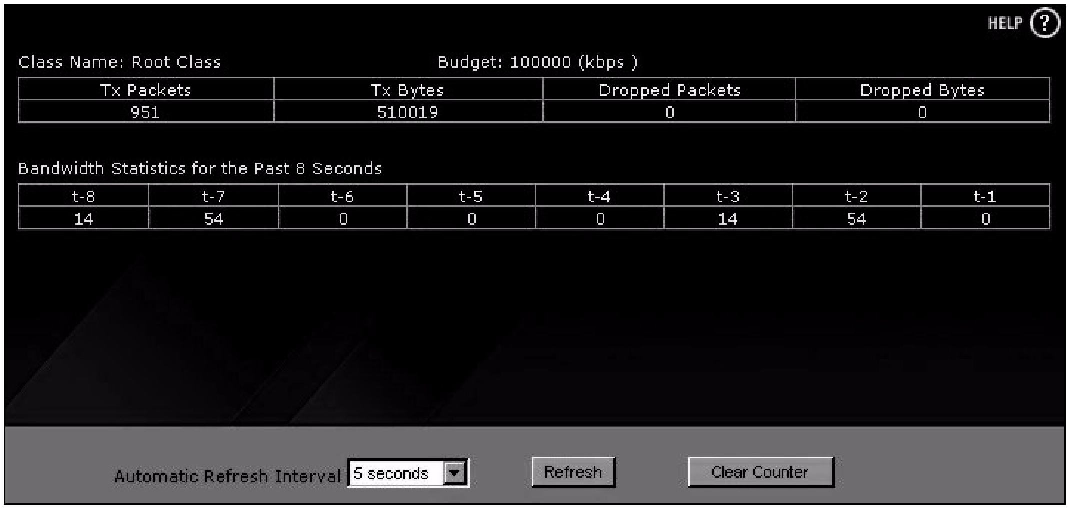
BANDWIDTH CLASSES AND BANDWIDTH BORROWING SETTINGS			
Root Class:	Administration: Borrowing Enabled		
	Sales: Borrowing Disabled	Sales USA: Borrowing Enabled	Bill: Borrowing Enabled
			Amy: Borrowing Disabled
		Sales Asia: Borrowing Disabled	Tina: Borrowing Enabled
			Fred: Borrowing Disabled
	Marketing: Borrowing Enabled		
	Research: Borrowing Enabled	Software: Borrowing Enabled	
		Hardware: Borrowing Enabled	

- The Bill class can borrow unused bandwidth from the Sales USA class because the Bill class has bandwidth borrowing enabled.
- The Bill class can also borrow unused bandwidth from the Sales class because the Sales USA class also has bandwidth borrowing enabled.
- The Bill class cannot borrow unused bandwidth from the Root class because the Sales class has bandwidth borrowing disabled.
- The Amy class cannot borrow unused bandwidth from the Sales USA class because the Amy class has bandwidth borrowing disabled.
- The Research Software and Hardware classes can both borrow unused bandwidth from the Research class because the Research Software and Hardware classes both have bandwidth borrowing enabled.
- The Research Software and Hardware classes can also borrow unused bandwidth from the Root class because the Research class also has bandwidth borrowing enabled.

18.3.2 Bandwidth Management Statistics Screen

Click **ADVANCED** > **BW MGMT** > **Class Setup** > **Statistics** to open the **Bandwidth Management Statistics** screen. This screen displays the selected bandwidth class's bandwidth usage and allotments.

Figure 220 ADVANCED > BW MGMT > Class Setup > Statistics



The following table describes the labels in this screen.

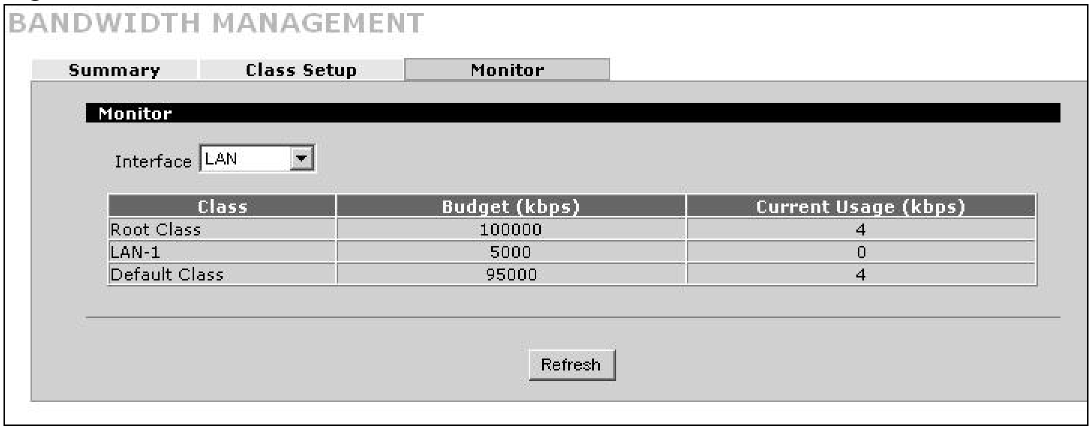
Table 141 ADVANCED > BW MGMT > Class Setup > Statistics

LABEL	DESCRIPTION
Class Name	This field displays the name of the class the statistics page is showing.
Budget (kbps)	This field displays the amount of bandwidth allocated to the class.
Tx Packets	This field displays the total number of packets transmitted.
Tx Bytes	This field displays the total number of bytes transmitted.
Dropped Packets	This field displays the total number of packets dropped.
Dropped Bytes	This field displays the total number of bytes dropped.
Bandwidth Statistics for the Past 8 Seconds (t-8 to t-1)	
This field displays the bandwidth statistics (in bps) for the past one to eight seconds. For example, t-1 means one second ago.	
Automatic Refresh Interval	Select a number of seconds or **None** from the drop-down list box to update all screen statistics automatically at the end of every time interval or to not update the screen statistics.
Refresh	Click this button to update the screen’s statistics immediately.
Clear Counter	Click **Clear Counter** to clear all of the bandwidth management statistics.

18.4 Bandwidth Manager Monitor

Click **ADVANCED** > **BW MGMT** > **Monitor** to open the following screen. Use this screen to view the device’s bandwidth usage and allotments.

Figure 221 ADVANCED > BW MGMT > Monitor



The following table describes the labels in this screen.

Table 142 ADVANCED > BW MGMT > Monitor

LABEL	DESCRIPTION
Interface	Select an interface from the drop-down list box to view the bandwidth usage of its bandwidth classes.
Class	This field displays the name of the bandwidth class. A **Default Class** automatically displays for all the bandwidth in the **Root Class** that is not allocated to bandwidth classes. If you do not enable maximize bandwidth usage on an interface, the LAN-Cell uses the bandwidth in this default class to send traffic that does not match any of the bandwidth classes.[A]
Budget (kbps)	This field displays the amount of bandwidth allocated to the bandwidth class.
Current Usage (kbps)	This field displays the amount of bandwidth that each bandwidth class is using.
Refresh	Click **Refresh** to update the page.

A. If you allocate all the root class's bandwidth to the bandwidth classes, the default class still displays a budget of 2 kbps (the minimum amount of bandwidth that can be assigned to a bandwidth class).

19

ALG Screens

19.1 Overview

This chapter covers how to use the LAN-Cell's ALG feature to allow certain applications to pass through the LAN-Cell.

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

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

To configure the ALG screen proceed to Section 19.2 on page 369.

19.1.1 What You Need to Know About ALG

ALG and NAT

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

The ALG on the LAN-Cell supports all NAT mapping types, including **One to One**, **Many to One**, **Many to Many Overload** and **Many One to One**.

ALG and the Firewall

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

ALG and Multiple WAN

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

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

When the LAN-Cell uses both of the WAN interfaces at the same time, you can configure routing policies to specify the WAN interfaces that the connection's traffic is to use.

FTP

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

H.323

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

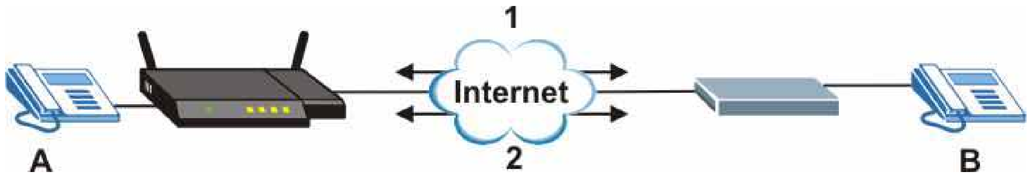
RTP

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

H.323 ALG Details

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

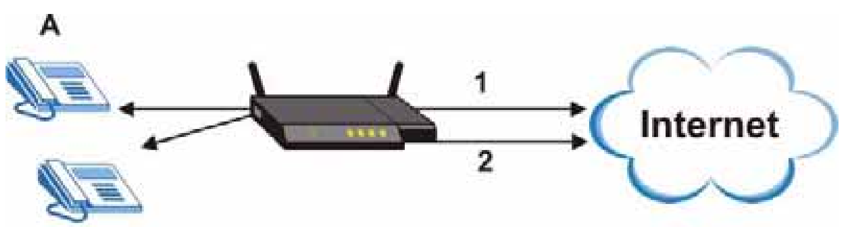
Figure 222 H.323 ALG Example



- With multiple WAN IP addresses on the LAN-Cell, you can configure different firewall and port forwarding rules to allow incoming calls from each WAN IP address to go to a specific IP address on the LAN, DMZ or WLAN. Use policy routing to have the H.323 calls from each of those LAN, DMZ or WLAN IP addresses go out through the same WAN IP address that calls come in on. The policy routing lets the LAN-Cell correctly forward the return traffic for the calls initiated from the LAN IP addresses.

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

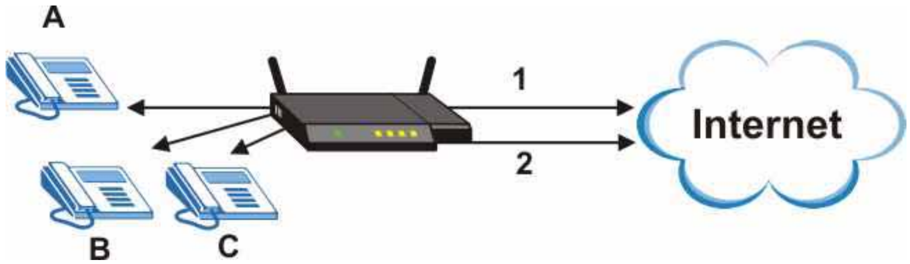
Figure 223 H.323 with Multiple WAN IP Addresses



- When you configure the firewall and port forwarding to allow calls from the WAN to a specific IP address on the LAN, you can also use policy routing to have H.323 calls from other LAN, DMZ or WLAN IP addresses go out through a different WAN IP address. The policy routing lets the LAN-Cell correctly forward the return traffic for the calls initiated from the LAN, DMZ or WLAN IP addresses.

  For example, you configure the firewall and port forwarding to allow LAN IP address **A** to receive calls from the Internet through WAN IP address **1**. You also use a policy route to have LAN IP address **A** make calls out through WAN IP address **1**. Configure another policy route to have H.323 calls from LAN IP addresses **B** and **C** go out through WAN IP address **2**. Even though only LAN IP address **A** can receive incoming calls from the Internet, LAN IP addresses **B** and **C** can still make calls out to the Internet.

Figure 224 H.323 Calls from the WAN with Multiple Outgoing Calls



- The H.323 ALG operates on TCP packets with a port 1720 destination.
- The LAN-Cell allows H.323 audio connections.
- The LAN-Cell can also apply bandwidth management to traffic that goes through the H.323 ALG.

SIP

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

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

STUN

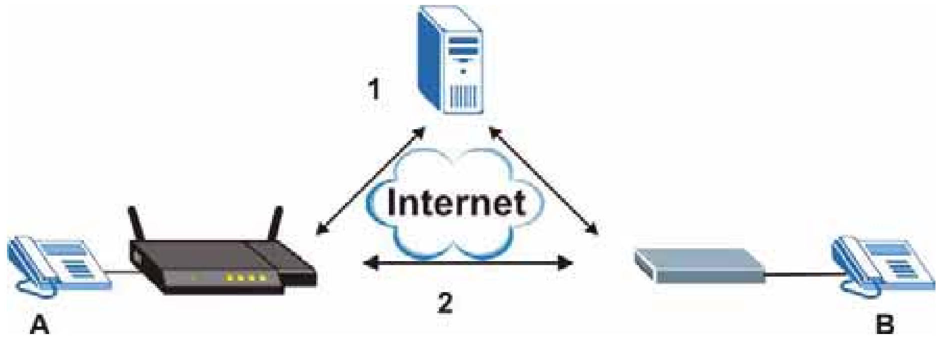
STUN (Simple Traversal of User Datagram Protocol (UDP) through Network Address Translators) allows the VoIP device to find the presence and types of NAT routers and/or firewalls between it and the public Internet. STUN also allows the VoIP device to find the public IP address that NAT assigned, so the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

SIP ALG Details

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

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

Figure 225 SIP ALG Example



SIP Signaling Session Timeout

Most SIP clients have an “expire” mechanism indicating the lifetime of signaling sessions. The SIP user agent sends registration packets to the SIP server periodically and keeps the session alive in the LAN-Cell.

If the SIP client does not have this mechanism and makes no calls during the LAN-Cell SIP timeout default (60 minutes), the LAN-Cell SIP ALG drops any incoming calls after the timeout period.

SIP Audio Session Timeout

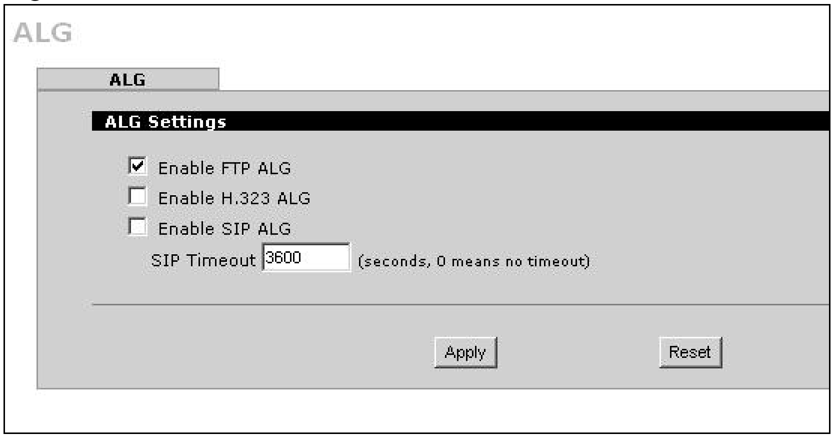
If no voice packets go through the SIP ALG before the timeout period (default 5 minutes) expires, the SIP ALG does not drop the call but blocks all voice traffic and deletes the audio session. You cannot hear anything and you will need to make a new call to continue your conversation.

19.2 ALG Screen

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

If the LAN-Cell provides an ALG for a service, you must enable the ALG in order to perform bandwidth management on that service’s traffic.

Figure 226 ADVANCED > ALG



The following table describes the labels in this screen.

Table 143 ADVANCED > ALG

LABEL	DESCRIPTION
Enable FTP ALG	Select this check box to allow FTP sessions to pass through the LAN-Cell. FTP (File Transfer Program) is a program that enables fast transfer of files, including large files that may not be possible by e-mail.
Enable H.323 ALG	Select this check box to allow H.323 sessions to pass through the LAN-Cell. H.323 is a protocol used for audio communications over networks.
Enable SIP ALG	Select this check box to allow SIP sessions to pass through the LAN-Cell. SIP is a signaling protocol used in VoIP (Voice over IP), the sending of voice signals over Internet Protocol.
SIP Timeout	Most SIP clients have an "expire" mechanism indicating the lifetime of signaling sessions. The SIP user agent sends registration packets to the SIP server periodically and keeps the session alive in the LAN-Cell. If the SIP client does not have this mechanism and makes no calls during the LAN-Cell SIP timeout (default 60 minutes), the LAN-Cell SIP ALG drops any incoming calls after the timeout period. Enter the SIP signaling session timeout value.
Apply	Click **Apply** to save your changes back to the LAN-Cell.
Reset	Click **Reset** to begin configuring this screen afresh.

20

Custom Application Screens

20.1 Overview

Use custom application to have the LAN-Cell's ALG and content filtering features monitor traffic on custom ports, in addition to the default ports.

Use the Custom App screen (Section 26.1 on page 471) to configure custom application settings on the LAN-Cell.

20.1.1 What You Need to Know About Custom Application

Default Ports

By default, these LAN-Cell features monitor traffic for the following protocols on these port numbers.

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

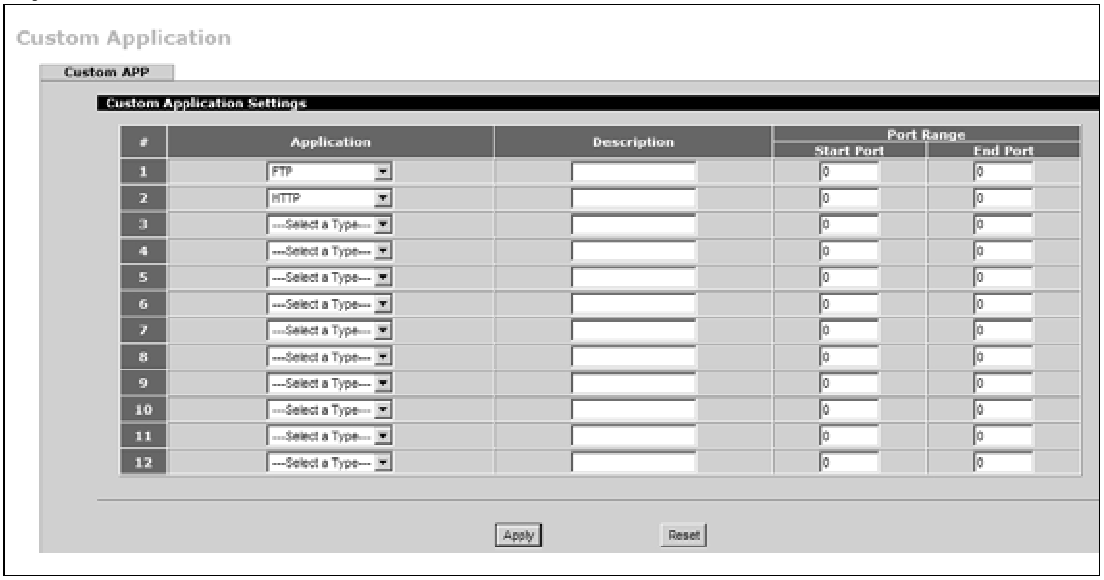
20.2 The Custom Application Screen

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

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

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

Figure 227 ADVANCED > Custom APP



The following table describes the labels in this screen.

Table 144 ADVANCED > ALG

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

PART V
Logs and Maintenance Menus

21

Logs Screens

21.1 Overview

This chapter contains information about configuring general log settings and viewing the LAN-Cell's logs. Refer to Section on page 381 for example log message explanations. The logs cover categories such as system maintenance, system errors, access control, attacks (such as DoS) and IPSec.

21.1.1 What You Can Do in the Log Screens

- Use the **View Log** screen (Section 21.2 on page 375) to see the logs for the categories that you selected in the **Log Settings** screen.
- Use the **Log Settings** screen (Section 21.3 on page 377) to configure to where the LAN-Cell is to send logs; the schedule for when the LAN-Cell is to send the logs and which logs and/or immediate alerts the LAN-Cell is to send.

21.1.2 What You Need To Know About Logs

Alerts and Logs

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

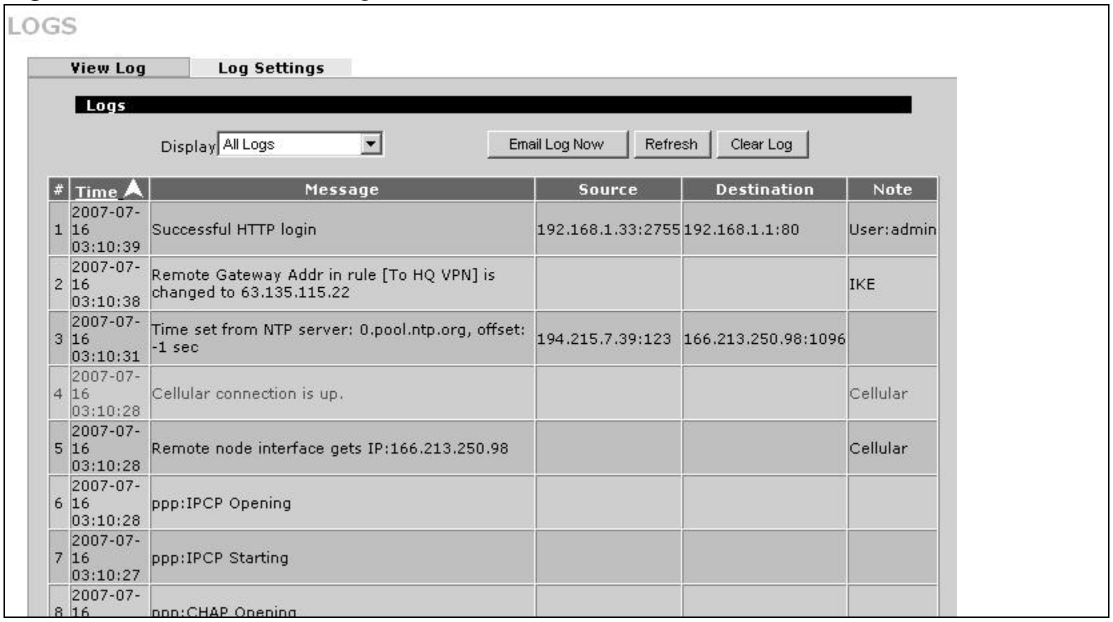
21.2 View Log Screen

The web configurator allows you to look at all of the LAN-Cell's logs in one location.

Click **LOGS** to open the **View Log** screen. Use the **View Log** screen to see the logs for the categories that you selected in the **Log Settings** screen (see Section 21.3 on page 377). Options include logs about system maintenance, system errors, access control, attacks (such as DoS) and IPSec.

When the log is full it will begin to delete older entries as it adds new ones. You can configure the LAN-Cell to E-mail you the log when it is full in the **Log Settings** screen. Click a column heading to sort the entries by the relevant attribute. A triangle indicates ascending or descending sort order.

Figure 228 LOGS > View Log



The following table describes the labels in this screen.

Table 145 LOGS > View Log

LABEL	DESCRIPTION
Display	The categories that you select in the **Log Settings** page (see Section 21.3 on page 377) display in the drop-down list box. Select a category of logs to view; select **All Logs** to view logs from all of the log categories that you selected in the **Log Settings** page.
#	This field displays the log number.
Time	This field displays the time the log was recorded. See Section 22.4 on page 399 to configure the LAN-Cell's time and date.
Message	This field states the reason for the log.
Source	This field lists the source IP address and the port number of the incoming packet.
Destination	This field lists the destination IP address and the port number of the incoming packet.
Note	This field displays additional information about the log entry.
Email Log Now	Click **Email Log Now** to send the log screen to the e-mail address specified in the **Log Settings** page (make sure that you have first filled in the **E-mail Log Settings** fields in **Log Settings**, see Section 21.3 on page 377).
Refresh	Click **Refresh** to renew the log screen.
Clear Log	Click **Clear Log** to delete all the logs.

21.2.1 Log Description Example

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

```
#  .time                  source                 destination
notes
    message
  5|06/08/2004 05:58:20 |172.21.4.187:137      |172.21.255.255:137
|ACCESS BLOCK
    Firewall default policy: UDP (W to W/LC)
```

Table 146 Log Description Example

LABEL	DESCRIPTION
#	This is log number five.
time	The log was generated on June 8, 2004 at 5:58 and 20 seconds AM.
source	The log was generated due to a NetBIOS packet sent from IP address 172.21.4.187 port 137.
destination	The NetBIOS packet was sent to the 172.21.255.255 subnet port 137. This was a NetBIOS UDP broadcast packet meant to discover devices on the network.
notes	The LAN-Cell blocked the packet.
message	The LAN-Cell blocked the packet in accordance with the firewall’s default policy of blocking sessions that are initiated from the WAN. “UDP” means that this was a User Datagram Protocol packet. “W to W/LC” indicates that the packet was traveling from the WAN to the WAN or the LAN-Cell.

21.3 Log Settings Screen

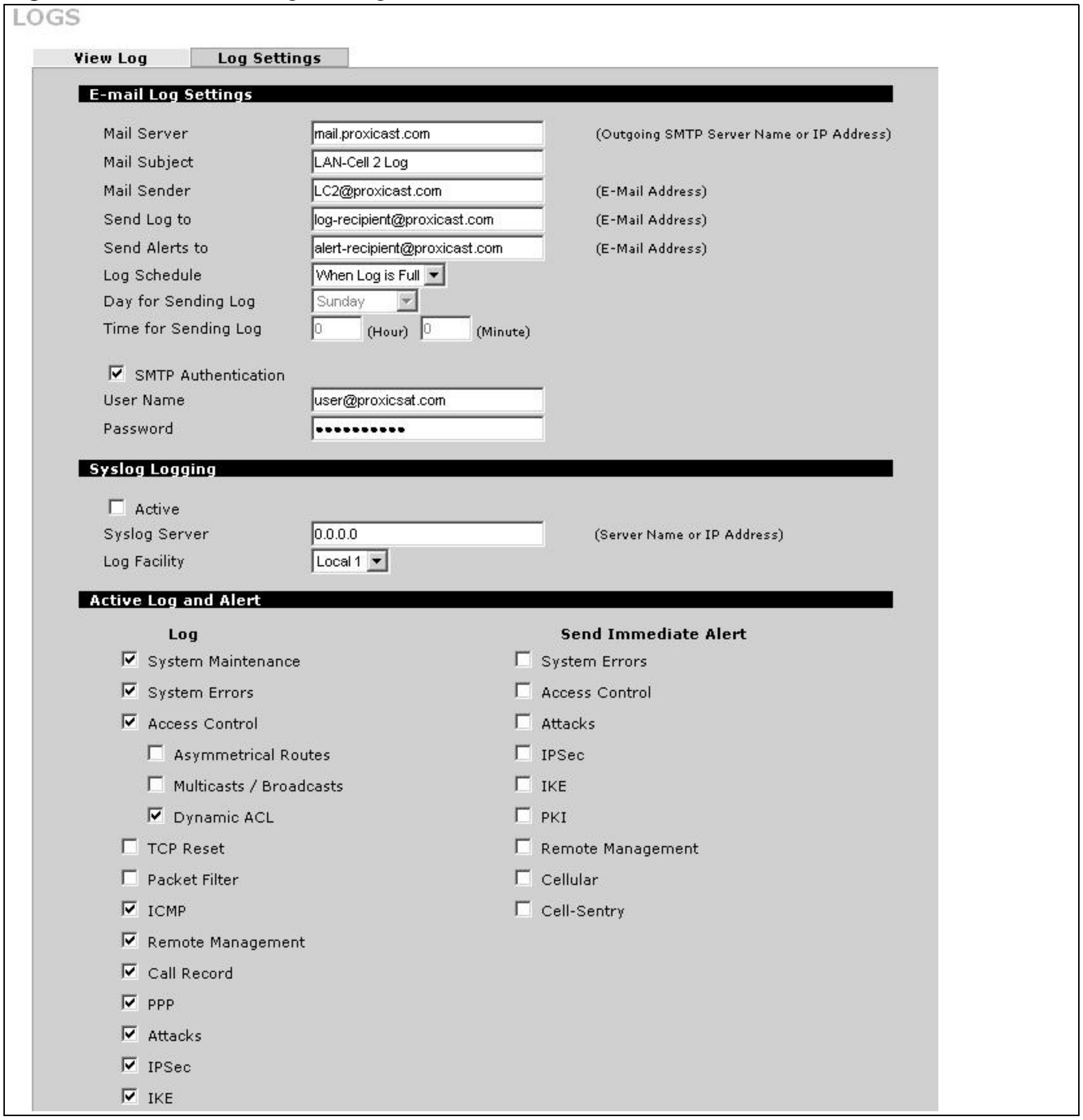
To change your LAN-Cell’s log settings, click **LOGS** > **Log Settings**. The screen appears as shown.

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

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.

Alerts can only be sent via SMTP, however, some cellular phone and pager service providers allow e-mail messages sent to specific addresses to be redirected as SMS or pager messages to mobile devices. Contact your service provider for more information.

Figure 229   LOGS > Log Settings



The following table describes the labels in this screen.

Table 147 LOGS > Log Settings

LABEL	DESCRIPTION
E-mail Log Settings	
Mail Server	Enter the server name or the IP address of the mail server for the e-mail addresses specified below. If this field is left blank, logs and alert messages will not be sent via e-mail.
Mail Subject	Type a title that you want to be in the subject line of the log e-mail message that the LAN-Cell sends.
Mail Sender	Enter the e-mail address that you want to be in the from/sender line of the log e-mail message that the LAN-Cell sends. If you activate SMTP authentication, the e-mail address must be able to be authenticated by the mail server as well.
Send Log To	Logs are sent to the e-mail address specified in this field. If this field is left blank, logs will not be sent via e-mail.
Send Alerts To	Alerts are sent to the e-mail address specified in this field. If this field is left blank, alerts will not be sent via e-mail.
Log Schedule	This drop-down menu is used to configure the frequency of log messages being sent as E-mail: **Daily** **Weekly** **Hourly** **When Log is Full** **None**. If you select **Weekly** or **Daily**, specify a time of day when the E-mail should be sent. If you select **Weekly**, then also specify which day of the week the E-mail should be sent. If you select **When Log is Full**, an alert is sent when the log fills up. If you select **None**, no log messages are sent.
Day for Sending Log	Use the drop down list box to select which day of the week to send the logs.
Time for Sending Log	Enter the time of the day in 24-hour format (for example 23:00 equals 11:00 pm) to send the logs.
SMTP Authentication	SMTP (Simple Mail Transfer Protocol) is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another. Select the check box to activate SMTP authentication. If mail server authentication is needed but this feature is disabled, you will not receive the e-mail logs.
User Name	Enter the user name (up to 63 characters) (usually the user name of a mail account).
Password	Enter the password associated with the user name above.
Syslog Logging	Syslog allows you to send system logs to a server. Syslog logging sends a log to an external syslog server.
Active	Click **Active** to enable syslog logging.
Syslog Server	Enter the server name or IP address of the syslog server that will log the selected categories of logs.
Log Facility	Select a location from the drop down list box. The log facility allows you to log the messages to different files in the syslog server. Refer to the documentation of your syslog program for more details.
Active Log and Alert	
Log	Select the categories of logs that you want to record. Logs include alerts.

Table 147 LOGS > Log Settings (continued)

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

21.4 Logs Technical Reference

Log Descriptions

This section provides descriptions of example log messages.

Table 148 System Maintenance Logs

LOG MESSAGE	DESCRIPTION
`Time calibration is successful`	The router has adjusted its time based on information from the time server.
`Time calibration failed`	The router failed to get information from the time server.
`WAN interface gets IP: %s`	A WAN interface got a new IP address from the DHCP, PPPoE, PPTP or dial-up server.
`DHCP client IP expired`	A DHCP client's IP address has expired.
`DHCP server assigns %s`	The DHCP server assigned an IP address to a client.
`Successful SMT login`	Someone has logged on to the router's SMT interface.
`SMT login failed`	Someone has failed to log on to the router's SMT interface.
`Successful WEB login`	Someone has logged on to the router's web configurator interface.
`WEB login failed`	Someone has failed to log on to the router's web configurator interface.
`Successful TELNET login`	Someone has logged on to the router via telnet.
`TELNET login failed`	Someone has failed to log on to the router via telnet.
`Successful FTP login`	Someone has logged on to the router via FTP.
`FTP login failed`	Someone has failed to log on to the router via FTP.
`NAT Session Table is Full!`	The maximum number of NAT session table entries has been exceeded and the table is full.
`Starting Connectivity Monitor`	Starting Connectivity Monitor.
`Time initialized by Daytime Server`	The router got the time and date from the Daytime server.
`Time initialized by Time server`	The router got the time and date from the time server.
`Time initialized by NTP server`	The router got the time and date from the NTP server.
`Connect to Daytime server fail`	The router was not able to connect to the Daytime server.
`Connect to Time server fail`	The router was not able to connect to the Time server.
`Connect to NTP server fail`	The router was not able to connect to the NTP server.
`Too large ICMP packet has been dropped`	The router dropped an ICMP packet that was too large.
`SMT Session Begin`	An SMT management session has started.
`SMT Session End`	An SMT management session has ended.
`Configuration Change: PC = 0x%x, Task ID = 0x%x`	The router is saving configuration changes.

Table 148 System Maintenance Logs (continued)

LOG MESSAGE	DESCRIPTION
Successful SSH login	Someone has logged on to the router's SSH server.
SSH login failed	Someone has failed to log on to the router's SSH server.
Successful HTTPS login	Someone has logged on to the router's web configurator interface using HTTPS protocol.
HTTPS login failed	Someone has failed to log on to the router's web configurator interface using HTTPS protocol.
DNS server %s was not responding to last 32 consecutive queries…	The specified DNS server did not respond to the last 32 consecutive queries.
DDNS update IP:%s (host %d) successfully	The device updated the IP address of the specified DDNS host name.
SMTP successfully	The device sent an e-mail.

Table 149 System Error Logs

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

Table 150 Access Control Logs

LOG MESSAGE	DESCRIPTION
Firewall default policy: [TCP | UDP | IGMP | ESP | GRE | OSPF] <Packet Direction>	Attempted TCP/UDP/IGMP/ESP/GRE/OSPF access matched the default policy and was blocked or forwarded according to the default policy's setting.
Firewall rule [NOT] match:[TCP | UDP | IGMP | ESP | GRE | OSPF] <Packet Direction>, <rule:%d>	Attempted TCP/UDP/IGMP/ESP/GRE/OSPF access matched (or did not match) a configured firewall rule (denoted by its number) and was blocked or forwarded according to the rule.

Table 150 Access Control Logs (continued)

LOG MESSAGE	DESCRIPTION
`Triangle route packet forwarded: [ TCP | UDP | IGMP | ESP | GRE | OSPF ]`	The firewall allowed a triangle route session to pass through.
`Packet without a NAT table entry blocked: [ TCP | UDP | IGMP | ESP | GRE | OSPF ]`	The router blocked a packet that didn't have a corresponding NAT table entry.
`Router sent blocked web site message: TCP`	The router sent a message to notify a user that the router blocked access to a web site that the user requested.
`Exceed maximum sessions per host (%d).`	The device blocked a session because the host's connections exceeded the maximum sessions per host.
`Firewall allowed a packet that matched a NAT session: [ TCP | UDP ]`	A packet from the WAN (TCP or UDP) matched a cone NAT session and the device forwarded it to the LAN.

Table 151 TCP Reset Logs

LOG MESSAGE	DESCRIPTION
`Under SYN flood attack, sent TCP RST`	The router sent a TCP reset packet when a host was under a SYN flood attack (the TCP incomplete count is per destination host.)
`Exceed TCP MAX incomplete, sent TCP RST`	The router sent a TCP reset packet when the number of TCP incomplete connections exceeded the user configured threshold. (the TCP incomplete count is per destination host.) Note: Refer to **TCP Maximum Incomplete** in the **Firewall Attack Alerts** screen.
`Peer TCP state out of order, sent TCP RST`	The router sent a TCP reset packet when a TCP connection state was out of order.Note: The firewall refers to RFC793 Figure 6 to check the TCP state.
`Firewall session time out, sent TCP RST`	The router sent a TCP reset packet when a dynamic firewall session timed out. The default timeout values are as follows: ICMP idle timeout: 3 minutes UDP idle timeout: 3 minutes TCP connection (three way handshaking) timeout: 270 seconds TCP FIN-wait timeout: 2 MSL (Maximum Segment Lifetime set in the TCP header). TCP idle (established) timeout (s): 150 minutes TCP reset timeout: 10 seconds
`Exceed MAX incomplete, sent TCP RST`	The router sent a TCP reset packet when the number of incomplete connections (TCP and UDP) exceeded the user-configured threshold. (Incomplete count is for all TCP and UDP connections through the firewall.)Note: When the number of incomplete connections (TCP + UDP) > “Maximum Incomplete High”, the router sends TCP RST packets for TCP connections and destroys TOS (firewall dynamic sessions) until incomplete connections < “Maximum Incomplete Low”.
`Access block, sent TCP RST`	The router sends a TCP RST packet and generates this log if you turn on the firewall TCP reset mechanism (via CI command: "sys firewall tcprst").

Table 152 Packet Filter Logs

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

For type and code details, see Table 163 on page 392.

Table 153 ICMP Logs

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

Table 154 CDR Logs

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

Table 155 PPP Logs

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

Table 155 PPP Logs (continued)

LOG MESSAGE	DESCRIPTION
`ppp:IPCP Opening`	The PPP connection's Internet Protocol Control Protocol stage is opening.
`ppp:LCP Closing`	The PPP connection's Link Control Protocol stage is closing.
`ppp:IPCP Closing`	The PPP connection's Internet Protocol Control Protocol stage is closing.

Table 156 Attack Logs

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

Table 156 Attack Logs (continued)

LOG MESSAGE	DESCRIPTION
`ICMP Source Quench ICMP`	The firewall detected an ICMP Source Quench attack.
`ICMP Time Exceed ICMP`	The firewall detected an ICMP Time Exceed attack.
`ICMP Destination Unreachable ICMP`	The firewall detected an ICMP Destination Unreachable attack.
`ping of death. ICMP`	The firewall detected an ICMP ping of death attack.
`smurf ICMP`	The firewall detected an ICMP smurf attack.
`IP address in FTP port command is different from the client IP address. It maybe a bounce attack.`	The IP address in an FTP port command is different from the client IP address. It may be a bounce attack.
`Fragment packet size is smaller than the MTU size of output interface.`	The fragment packet size is smaller than the MTU size of output interface.

Table 157 Remote Management Logs

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

Table 158 IPSec Logs

LOG MESSAGE	DESCRIPTION
`Discard REPLAY packet`	The router received and discarded a packet with an incorrect sequence number.
`Inbound packet authentication failed`	The router received a packet that has been altered. A third party may have altered or tampered with the packet.
`Receive IPSec packet, but no corresponding tunnel exists`	The router dropped an inbound packet for which SPI could not find a corresponding phase 2 SA.

Table 158 IPSec Logs (continued)

LOG MESSAGE	DESCRIPTION
`Rule <%d> idle time out, disconnect`	The router dropped a connection that had outbound traffic and no inbound traffic for a certain time period. You can use the "ipsec timer chk_conn" CI command to set the time period. The default value is 2 minutes.
`WAN IP changed to <IP>`	The router dropped all connections with the “MyIP” configured as “0.0.0.0” when the WAN IP address changed.
`Inbound packet decryption failed`	Please check the algorithm configuration.
`Cannot find outbound SA for rule <%d>`	A packet matches a rule, but there is no phase 2 SA for outbound traffic.
`Rule [%s] sends an echo request to peer`	The device sent a ping packet to check the specified VPN tunnel's connectivity.
`Rule [%s] receives an echo reply from peer`	The device received a ping response when checking the specified VPN tunnel's connectivity.

Table 159 IKE Logs

LOG MESSAGE	DESCRIPTION
`Active connection allowed exceeded`	The IKE process for a new connection failed because the limit of simultaneous phase 2 SAs has been reached.
`Start Phase 2: Quick Mode`	Phase 2 Quick Mode has started.
`Verifying Remote ID failed:`	The connection failed during IKE phase 2 because the router and the peer’s Local/Remote Addresses don’t match.
`Verifying Local ID failed:`	The connection failed during IKE phase 2 because the router and the peer’s Local/Remote Addresses don’t match.
`IKE Packet Retransmit`	The router retransmitted the last packet sent because there was no response from the peer.
`Failed to send IKE Packet`	An Ethernet error stopped the router from sending IKE packets.
`Too many errors! Deleting SA`	An SA was deleted because there were too many errors.
`Phase 1 IKE SA process done`	The phase 1 IKE SA process has been completed.
`Duplicate requests with the same cookie`	The router received multiple requests from the same peer while still processing the first IKE packet from the peer.
`IKE Negotiation is in process`	The router has already started negotiating with the peer for the connection, but the IKE process has not finished yet.
`No proposal chosen`	Phase 1 or phase 2 parameters don’t match. Please check all protocols / settings. Ex. One device being configured for 3DES and the other being configured for DES causes the connection to fail.
`Local / remote IPs of incoming request conflict with rule <%d>`	The security gateway is set to “0.0.0.0” and the router used the peer’s “Local Address” as the router’s “Remote Address”. This information conflicted with static rule #d; thus the connection is not allowed.
`Cannot resolve Secure Gateway Addr for rule <%d>`	The router couldn’t resolve the IP address from the domain name that was used for the secure gateway address.
`Peer ID: <peer id> <My remote type> -<My local type>`	The displayed ID information did not match between the two ends of the connection.

Table 159 IKE Logs (continued)

LOG MESSAGE	DESCRIPTION
`vs. My Remote <My remote> - <My remote>`	The displayed ID information did not match between the two ends of the connection.
`vs. My Local <My local>-<My local>`	The displayed ID information did not match between the two ends of the connection.
`Send <packet>`	A packet was sent.
`Recv <packet>`	IKE uses ISAKMP to transmit data. Each ISAKMP packet contains many different types of payloads. All of them show in the LOG. Refer to RFC2408 – ISAKMP for a list of all ISAKMP payload types.
`Recv <Main or Aggressive> Mode request from <IP>`	The router received an IKE negotiation request from the peer address specified.
`Send <Main or Aggressive> Mode request to <IP>`	The router started negotiation with the peer.
`Invalid IP <Peer local> / <Peer local>`	The peer's "Local IP Address" is invalid.
`Remote IP <Remote IP> / <Remote IP> conflicts`	The security gateway is set to "0.0.0.0" and the router used the peer's "Local Address" as the router's "Remote Address". This information conflicted with static rule #d; thus the connection is not allowed.
`Phase 1 ID type mismatch`	This router's "Peer ID Type" is different from the peer IPSec router's "Local ID Type".
`Phase 1 ID content mismatch`	This router's "Peer ID Content" is different from the peer IPSec router's "Local ID Content".
`No known phase 1 ID type found`	The router could not find a known phase 1 ID in the connection attempt.
`ID type mismatch. Local / Peer: <Local ID type/Peer ID type>`	The phase 1 ID types do not match.
`ID content mismatch`	The phase 1 ID contents do not match.
`Configured Peer ID Content: <Configured Peer ID Content>`	The phase 1 ID contents do not match and the configured "Peer ID Content" is displayed.
`Incoming ID Content: <Incoming Peer ID Content>`	The phase 1 ID contents do not match and the incoming packet's ID content is displayed.
`Unsupported local ID Type: <%d>`	The phase 1 ID type is not supported by the router.
`Build Phase 1 ID`	The router has started to build the phase 1 ID.
`Adjust TCP MSS to %d`	The router automatically changed the TCP Maximum Segment Size value after establishing a tunnel.
`Rule <%d> input idle time out, disconnect`	The tunnel for the listed rule was dropped because there was no inbound traffic within the idle timeout period.
`XAUTH succeed! Username: <Username>`	The router used extended authentication to authenticate the listed username.
`XAUTH fail! Username: <Username>`	The router was not able to use extended authentication to authenticate the listed username.
`Rule[%d] Phase 1 negotiation mode mismatch`	The listed rule's IKE phase 1 negotiation mode did not match between the router and the peer.

Table 159 IKE Logs (continued)

LOG MESSAGE	DESCRIPTION
`Rule [%d] Phase 1 encryption algorithm mismatch`	The listed rule’s IKE phase 1 encryption algorithm did not match between the router and the peer.
`Rule [%d] Phase 1 authentication algorithm mismatch`	The listed rule’s IKE phase 1 authentication algorithm did not match between the router and the peer.
`Rule [%d] Phase 1 authentication method mismatch`	The listed rule’s IKE phase 1 authentication method did not match between the router and the peer.
`Rule [%d] Phase 1 key group mismatch`	The listed rule’s IKE phase 1 key group did not match between the router and the peer.
`Rule [%d] Phase 2 protocol mismatch`	The listed rule’s IKE phase 2 protocol did not match between the router and the peer.
`Rule [%d] Phase 2 encryption algorithm mismatch`	The listed rule’s IKE phase 2 encryption algorithm did not match between the router and the peer.
`Rule [%d] Phase 2 authentication algorithm mismatch`	The listed rule’s IKE phase 2 authentication algorithm did not match between the router and the peer.
`Rule [%d] Phase 2 encapsulation mismatch`	The listed rule’s IKE phase 2 encapsulation did not match between the router and the peer.
`Rule [%d]> Phase 2 pfs mismatch`	The listed rule’s IKE phase 2 perfect forward secret (PFS) setting did not match between the router and the peer.
`Rule [%d] Phase 1 ID mismatch`	The listed rule’s IKE phase 1 ID did not match between the router and the peer.
`Rule [%d] Phase 1 hash mismatch`	The listed rule’s IKE phase 1 hash did not match between the router and the peer.
`Rule [%d] Phase 1 preshared key mismatch`	The listed rule’s IKE phase 1 pre-shared key did not match between the router and the peer.
`Rule [%d] Tunnel built successfully`	The listed rule’s IPSec tunnel has been built successfully.
`Rule [%d] Peer's public key not found`	The listed rule’s IKE phase 1 peer’s public key was not found.
`Rule [%d] Verify peer's signature failed`	The listed rule’s IKE phase 1verification of the peer’s signature failed.
`Rule [%d] Sending IKE request`	IKE sent an IKE request for the listed rule.
`Rule [%d] Receiving IKE request`	IKE received an IKE request for the listed rule.
`Swap rule to rule [%d]`	The router changed to using the listed rule.
`Rule [%d] Phase 1 key length mismatch`	The listed rule’s IKE phase 1 key length (with the AES encryption algorithm) did not match between the router and the peer.
`Rule [%d] phase 1 mismatch`	The listed rule’s IKE phase 1 did not match between the router and the peer.
`Rule [%d] phase 2 mismatch`	The listed rule’s IKE phase 2 did not match between the router and the peer.

Table 159 IKE Logs (continued)

LOG MESSAGE	DESCRIPTION
`Rule [%d] Phase 2 key length mismatch`	The listed rule's IKE phase 2 key lengths (with the AES encryption algorithm) did not match between the router and the peer.
`Remote Gateway Addr in rule [%s] is changed to %s"`	The IP address for the domain name of the peer gateway in the listed rule changed to the listed IP address.
`New My LAN-Cell Addr in rule [%s] is changed to %s`	The IP address for the domain name of the LAN-Cell in the listed rule changed to the listed IP address.
`Remote Gateway Addr has changed, tunnel [%s] will be deleted`	The listed tunnel will be deleted because the remote gateway's IP address changed.
`My LAN-Cell Addr has changed, tunnel [%s] will be deleted`	The listed tunnel will be deleted because the LAN-Cell's IP address changed.

Table 160 PKI Logs

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

Table 160 PKI Logs (continued)

LOG MESSAGE	DESCRIPTION
`Failed to decode the received CRL`	The router received a corrupted CRL (Certificate Revocation List) from the LDAP server whose address and port are recorded in the Source field.
`Failed to decode the received ARL`	The router received a corrupted ARL (Authority Revocation List) from the LDAP server whose address and port are recorded in the Source field.
`Rcvd data <size> too large! Max size allowed: <max size>`	The router received directory data that was too large (the size is listed) from the LDAP server whose address and port are recorded in the Source field. The maximum size of directory data that the router allows is also recorded.
`Cert trusted: <subject name>`	The router has verified the path of the certificate with the listed subject name.
`Due to <reason codes>, cert not trusted: <subject name>`	Due to the reasons listed, the certificate with the listed subject name has not passed the path verification. The recorded reason codes are only approximate reasons for not trusting the certificate. Please see Table 161 on page 391 for the corresponding descriptions of the codes.

Table 161 Certificate Path Verification Failure Reason Codes

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

Table 161 Certificate Path Verification Failure Reason Codes

CODE	DESCRIPTION
23	Time interval is not continuous.
24	Time information not available.
25	Database method failed due to timeout.
26	Database method failed.
27	Path was not verified.
28	Maximum path length reached.

Table 162 ACL Setting Notes

PACKET DIRECTION	DIRECTION	DESCRIPTION
(L to W)	LAN to WAN	ACL set for packets traveling from the LAN to the WAN.
(W to L)	WAN to LAN	ACL set for packets traveling from the WAN to the LAN.
(D to L)	DMZ to LAN	ACL set for packets traveling from the DMZ to the LAN.
(D to W)	DMZ to WAN	ACL set for packets traveling from the DMZ to the WAN.
(W to D)	WAN to DMZ	ACL set for packets traveling from the WAN to the DMZ.
(L to D)	LAN to DMZ	ACL set for packets traveling from the LAN to the DMZ.
(L to L/LC)	LAN to LAN/LAN-Cell	ACL set for packets traveling from the LAN to the LAN or the LAN-Cell.
(W to W/LC)	WAN to WAN/ LAN-Cell	ACL set for packets traveling from the WAN to the WAN or the LAN-Cell.
(D to D/LC)	DMZ to DMZ/ LAN-Cell	ACL set for packets traveling from the DMZ to the DM or the LAN-Cell.
(L to WL)	LAN to WLAN	ACL set for packets traveling from the LAN to the WLAN.
(WL to L)	WLAN to LAN	ACL set for packets traveling from the WLAN to the LAN.
(W to WL)	WAN to WLAN	ACL set for packets traveling from the WAN to the WLAN.
(WL to W)	WLAN to WAN	ACL set for packets traveling from the WLAN to the WAN.
(D to WL)	DMZ to WLAN	ACL set for packets traveling from the DMZ to the WLAN.
(WL to D)	WLAN to DMZ	ACL set for packets traveling from the WLAN to the DMZ.
(WL to WL)	WLAN to WLAN/ LAN-Cell	ACL set for packets traveling from the WLAN to the WLAN or the LAN-Cell.

Table 163 ICMP Notes

TYPE	CODE	DESCRIPTION
0		Echo Reply
	0	Echo reply message
3		Destination Unreachable
	0	Net unreachable
	1	Host unreachable
	2	Protocol unreachable

Table 163 ICMP Notes (continued)

TYPE	CODE	DESCRIPTION
	3	Port unreachable
	4	A packet that needed fragmentation was dropped because it was set to Don't Fragment (DF)
	5	Source route failed
4		Source Quench
	0	A gateway may discard internet datagrams if it does not have the buffer space needed to queue the datagrams for output to the next network on the route to the destination network.
5		Redirect
	0	Redirect datagrams for the Network
	1	Redirect datagrams for the Host
	2	Redirect datagrams for the Type of Service and Network
	3	Redirect datagrams for the Type of Service and Host
8		Echo
	0	Echo message
11		Time Exceeded
	0	Time to live exceeded in transit
	1	Fragment reassembly time exceeded
12		Parameter Problem
	0	Pointer indicates the error
13		Timestamp
	0	Timestamp request message
14		Timestamp Reply
	0	Timestamp reply message
15		Information Request
	0	Information request message
16		Information Reply
	0	Information reply message

Syslog Logs

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

Table 164 Syslog Logs

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

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

Table 165 RFC-2408 ISAKMP Payload Types

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

Table 165 RFC-2408 ISAKMP Payload Types (continued)

LOG DISPLAY	PAYLOAD TYPE
DEL	Delete
VID	Vendor ID

22

Maintenance Screens

22.1 Overview

This chapter displays information on the maintenance screens. The maintenance screens can help you view system information, upload new firmware, manage configuration and restart your LAN-Cell.

22.1.1 What You Can Do in the Maintenance Screens

- Use the **General Setup** screen (Section 22.2 on page 397) to configure administrative and system-related information.
- Use the **Password** screen (Section 22.3 on page 398) to change the LAN-Cell's management password.
- Use the **Time and Date** screen (Section 22.4 on page 399) to configure the LAN-Cell's time based on your local time zone.
- Use the **F/W Upload** screen (Section 22.5 on page 403) to upgrade the LAN-Cell's firmware.
- Use the **Backup and Restore** screen (Section 22.6 on page 405) to backup and restore the LAN-Cell configuration file and to reset the device to factory settings.
- Use the **Restart** screen (Section 22.7 on page 407) to reboot the LAN-Cell device.
- Use the **Diagnostics** screen (Section 22.8 on page 408) to have the LAN-Cell generate and send diagnostic files by e-mail and/or the console port.

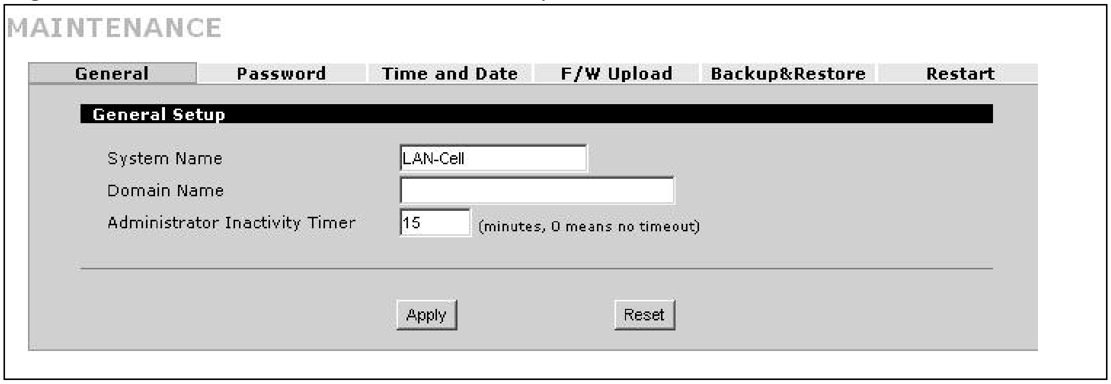
22.2 General Setup Screen

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

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

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

Figure 230 MAINTENANCE > General Setup



The following table describes the labels in this screen.

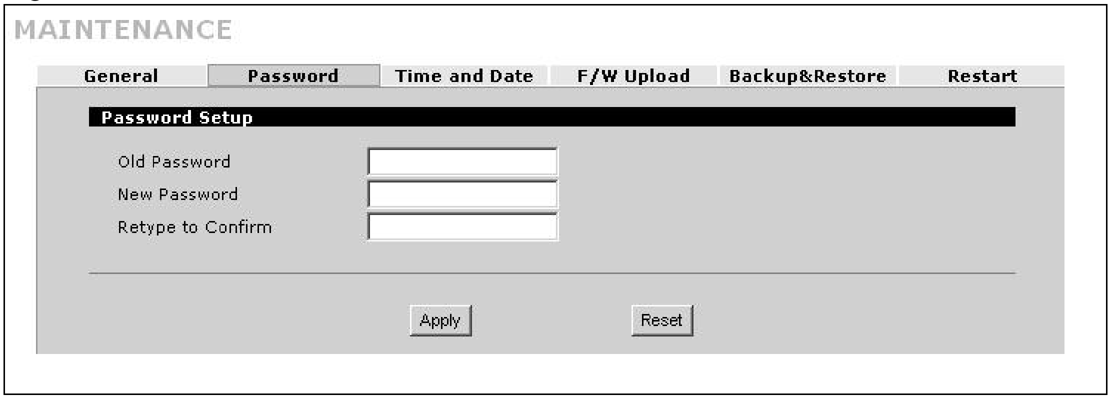
Table 166 MAINTENANCE > General Setup

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

22.3 Password Screen

Click **MAINTENANCE** > **Password** to open the following screen. Use this screen to change the LAN-Cell's management password.

Figure 231 MAINTENANCE > Password



The following table describes the labels in this screen.

Table 167 MAINTENANCE > Password

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

22.4 Time and Date Screen

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

Pre-defined NTP Time Server Pools

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

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

The LAN-Cell can use the NTP time server pools regardless of the time protocol you select.

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

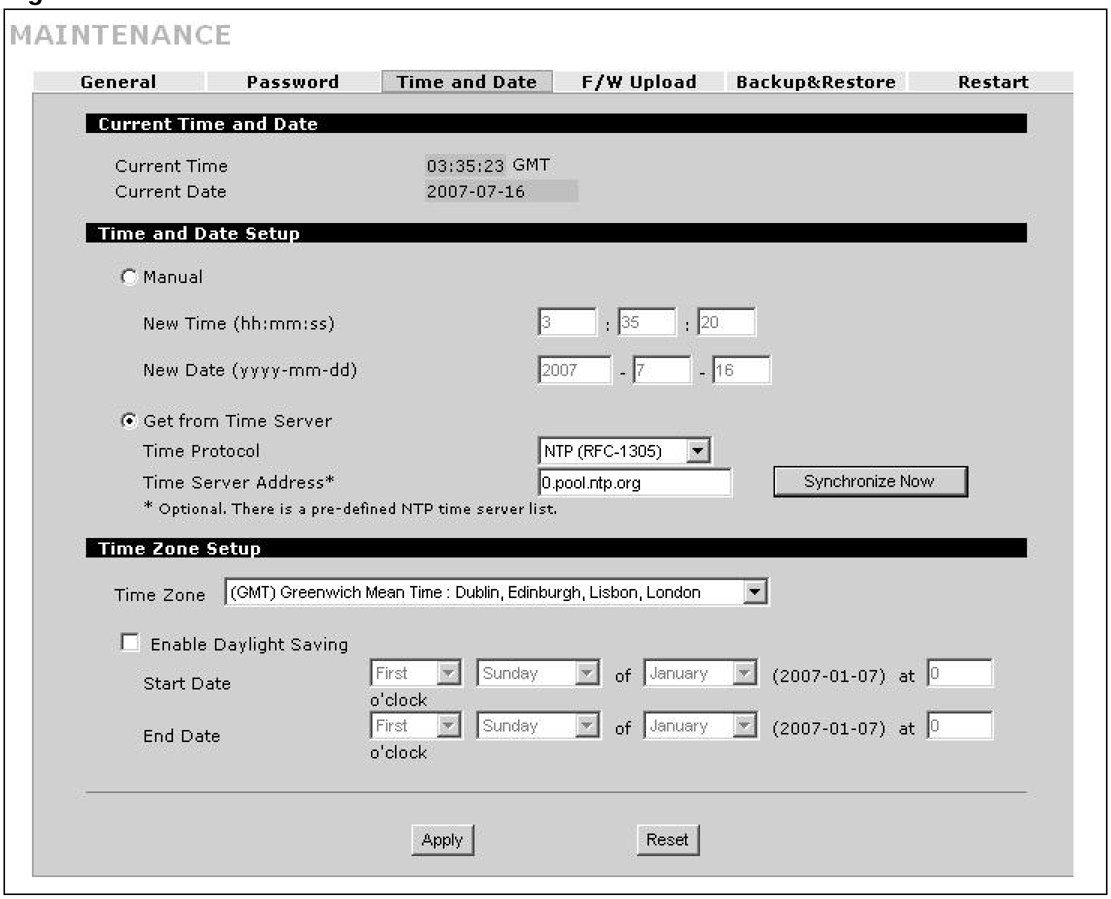
Resetting the Time

The LAN-Cell resets the time in the following instances:

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

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

Figure 232 MAINTENANCE > Time and Date



The following table describes the labels in this screen.

Table 168 MAINTENANCE > Time and Date

LABEL	DESCRIPTION
Current Time and Date	
Current Time	This field displays the LAN-Cell's present time.

Table 168 MAINTENANCE > Time and Date (continued)

LABEL	DESCRIPTION
Current Date	This field displays the LAN-Cell's present date.
Time and Date Setup	
Manual	Select this radio button to enter the time and date manually. If you configure a new time and date, Time Zone and Daylight Saving at the same time, the new time and date you entered has priority and the Time Zone and Daylight Saving settings do not affect it.
New Time (hh:mm:ss)	This field displays the last updated time from the time server or the last time configured manually. When you set **Time and Date Setup** to **Manual**, enter the new time in this field and then click **Apply**.
New Date (yyyy-mm-dd)	This field displays the last updated date from the time server or the last date configured manually. When you set **Time and Date Setup** to **Manual**, enter the new date in this field and then click **Apply**.
Get from Time Server	Select this radio button to have the LAN-Cell get the time and date from the time server you specified below.
Time Protocol	Select the time service protocol that your time server uses. Not all time servers support all protocols, so you may have to check with your ISP/network administrator or use trial and error to find a protocol that works. The main difference between them is the format. **Daytime (RFC 867)** format is day/month/year/time zone of the server. **Time (RFC 868)** format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0. The default, **NTP (RFC 1305)**, is similar to **Time (RFC 868)**.
Time Server Address	Enter the IP address or URL of your time server. Check with your ISP/network administrator if you are unsure of this information.
Synchronize Now	Click this button to have the LAN-Cell get the time and date from a time server (see the **Time Server Address** field). This also saves your changes (including the time server address).
Time Zone Setup	
Time Zone	Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
Enable Daylight Saving	Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening. Select this option if you use Daylight Saving Time.
Start Date	Configure the day and time when Daylight Saving Time starts if you selected **Enable Daylight Saving**. The **o'clock** field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time starts in most parts of the United States on the first Sunday of April. Each time zone in the United States starts using Daylight Saving Time at 2 A.M. local time. So in the United States you would select **Second**, **Sunday**, **March** and type 2 in the **o'clock** field. Daylight Saving Time starts in the European Union on the last Sunday of March. All of the time zones in the European Union start using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select **Last**, **Sunday**, **March**. The time you type in the **o'clock** field depends on your time zone. In Germany for instance, you would type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).

Table 168 MAINTENANCE > Time and Date (continued)

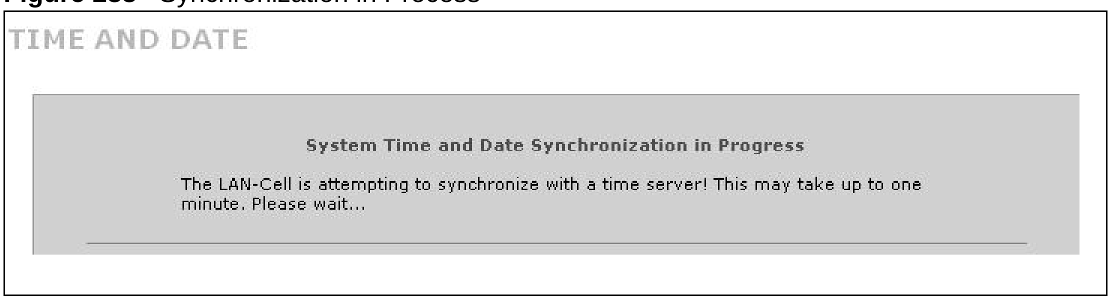
LABEL	DESCRIPTION
End Date	Configure the day and time when Daylight Saving Time ends if you selected **Enable Daylight Saving**. The **o'clock** field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time ends in the United States on the last Sunday of October. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So in the United States you would select **First**, **Sunday**, **November** and type 2 in the **o'clock** field. Daylight Saving Time ends in the European Union on the last Sunday of October. All of the time zones in the European Union stop using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select **Last**, **Sunday**, **October**. The time you type in the **o'clock** field depends on your time zone. In Germany for instance, you would type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
Apply	Click **Apply** to save your changes back to the LAN-Cell.
Reset	Click **Reset** to begin configuring this screen afresh.

22.4.1 Time Server Synchronization Example

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

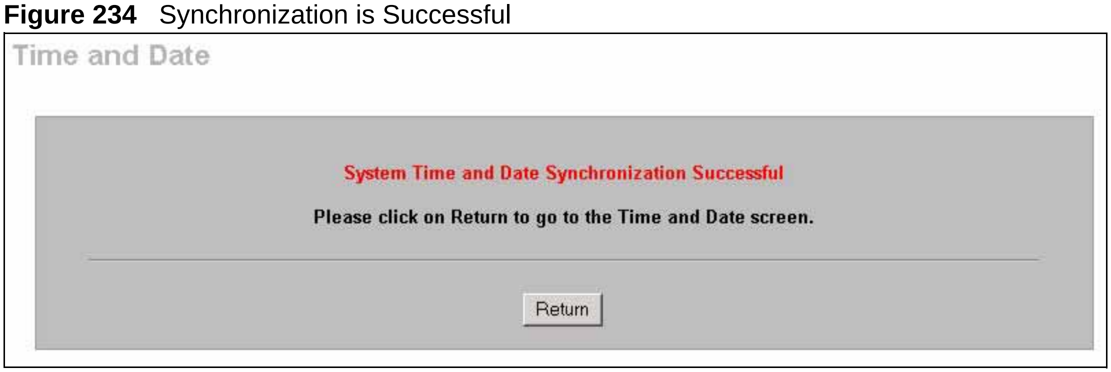
When the **System Time and Date Synchronization in Process** screen appears, wait up to one minute.

Figure 233 Synchronization in Process



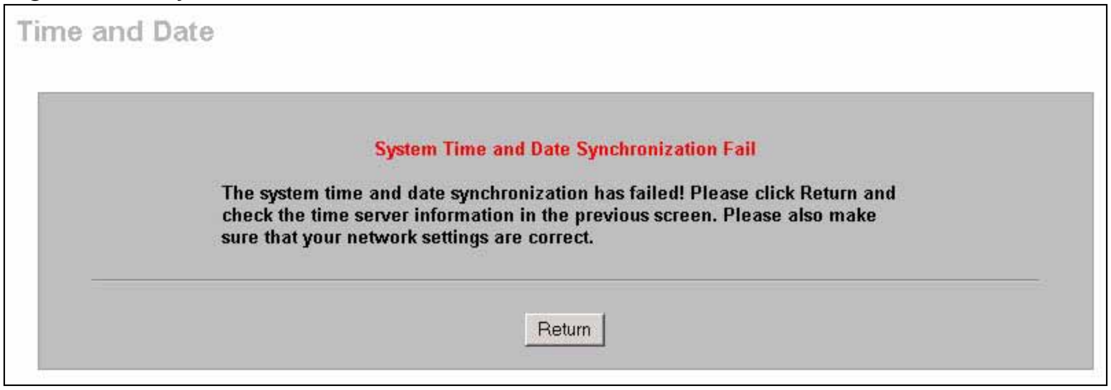
Click the **Return** button to go back to the **Time and Date** screen after the time and date is updated successfully.

Figure 234 Synchronization is Successful



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

Figure 235 Synchronization Fail



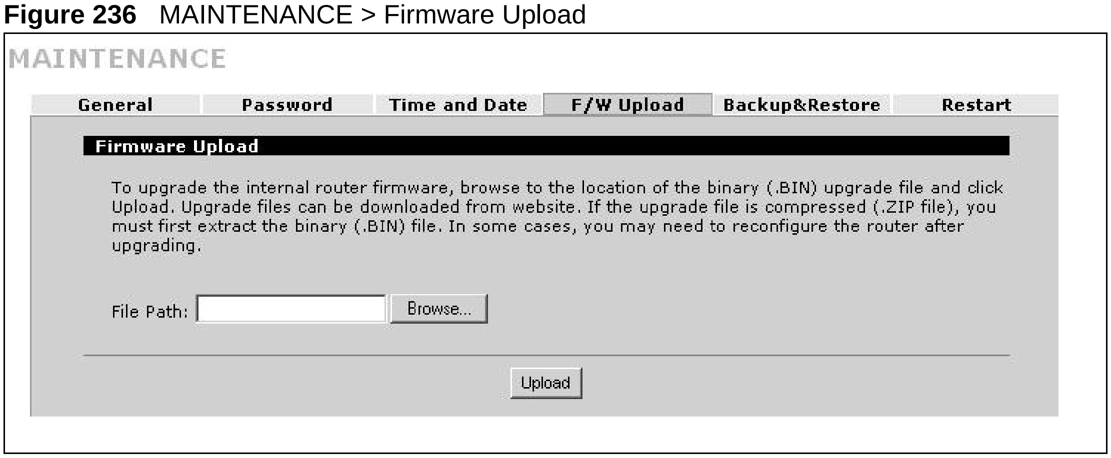
22.5 F/W Upload Screen

Find firmware at support.proxicast.com in a file that (usually) uses the firmware version number as the filename with a .bin extension, for example, "402XF1.bin". The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot. See Section 38.5 on page 537 for upgrading firmware using FTP/TFTP commands.

Click **MAINTENANCE** > **F/W UPLOAD**. Follow the instructions in this screen to upload firmware to your LAN-Cell.

Only upload firmware for your specific model!

Figure 236 MAINTENANCE > Firmware Upload



The following table describes the labels in this screen.

Table 169 MAINTENANCE > Firmware Upload

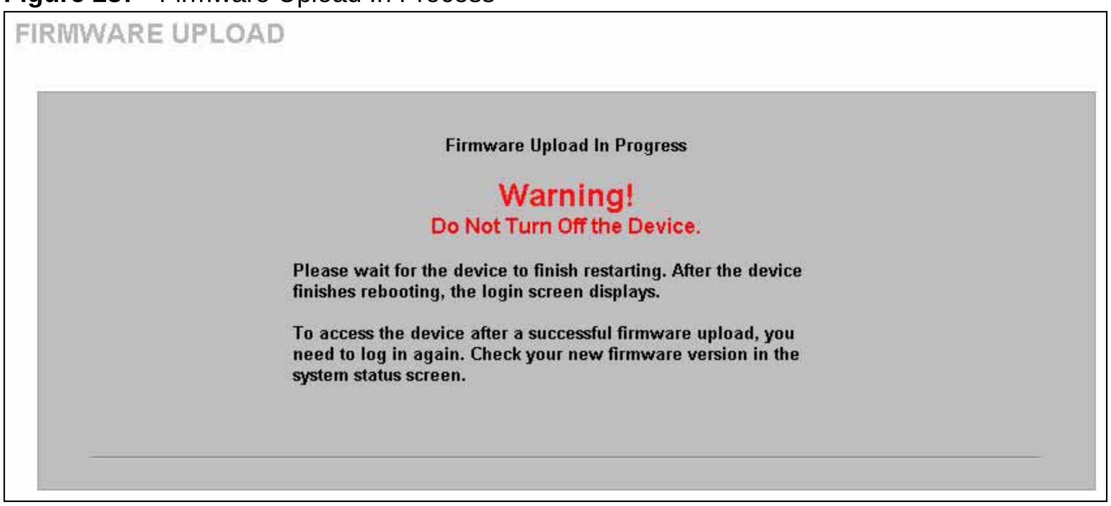
LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click **Browse ...** to find it.
Browse...	Click **Browse...** to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click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

Do not turn off the LAN-Cell while firmware upload is in progress!

When possible, perform firmware upgrades using a LAN-attached PC rather than an 802.11 client or over one of the WAN/Cellular ports.

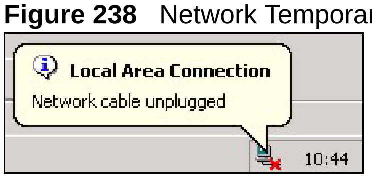
After you see the **Firmware Upload in Process** screen, wait two minutes before logging into the LAN-Cell again.

Figure 237 Firmware Upload In Process



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

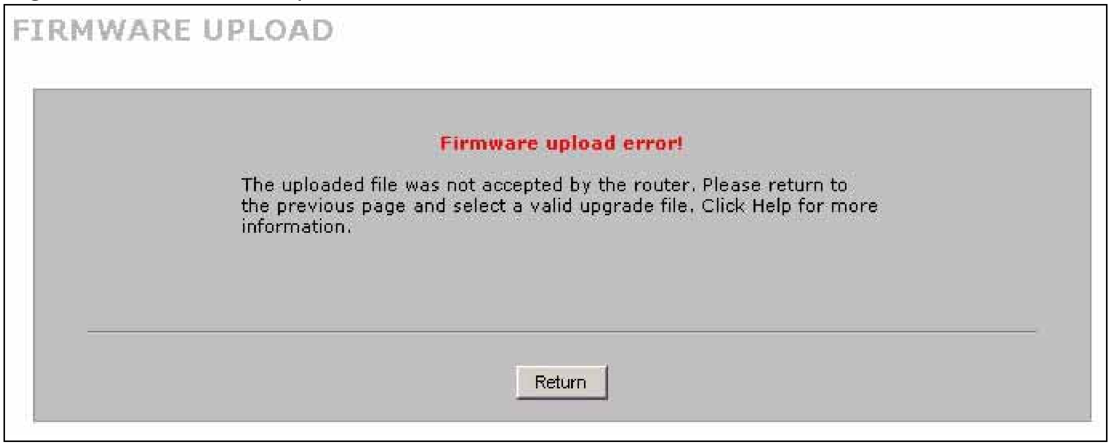
Figure 238 Network Temporarily Disconnected



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

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

Figure 239 Firmware Upload Error

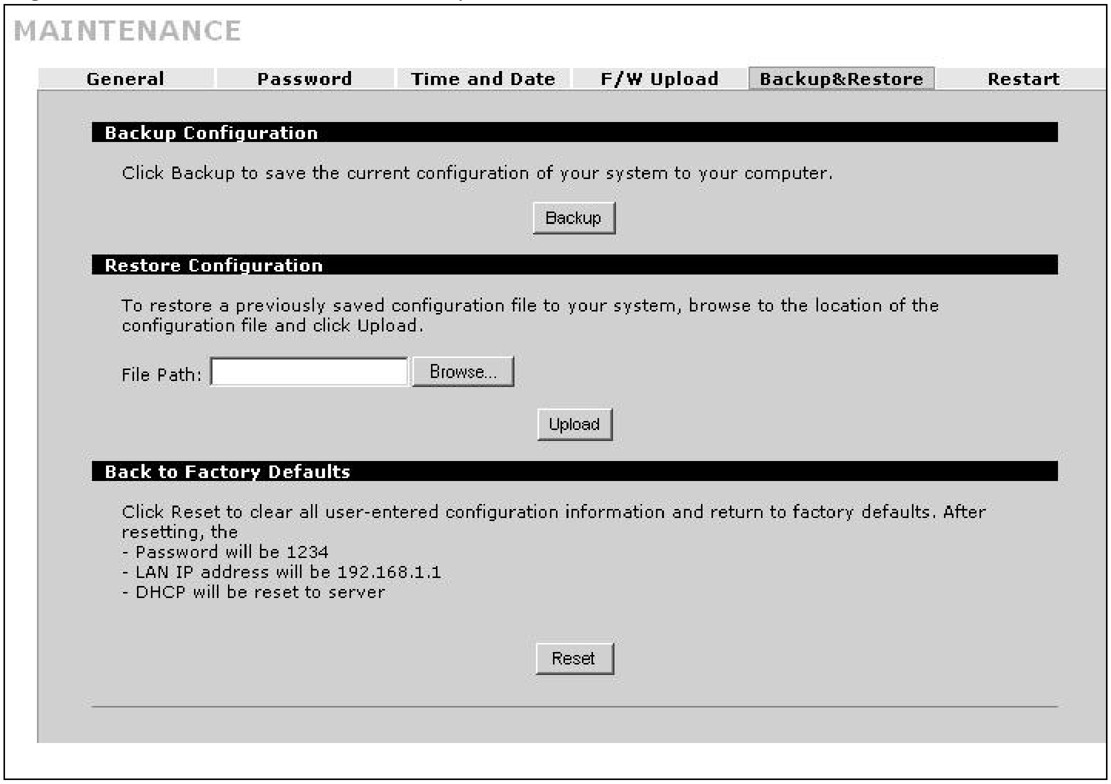


22.6 Backup and Restore Screen

See Section 38.5 on page 537 for transferring configuration files using FTP/TFTP commands.

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

Figure 240 MAINTENANCE > Backup and Restore



Backup Configuration

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

Click **Backup** to save the LAN-Cell's current configuration to your computer.

Restore Configuration

Load a configuration file from your computer to your LAN-Cell.

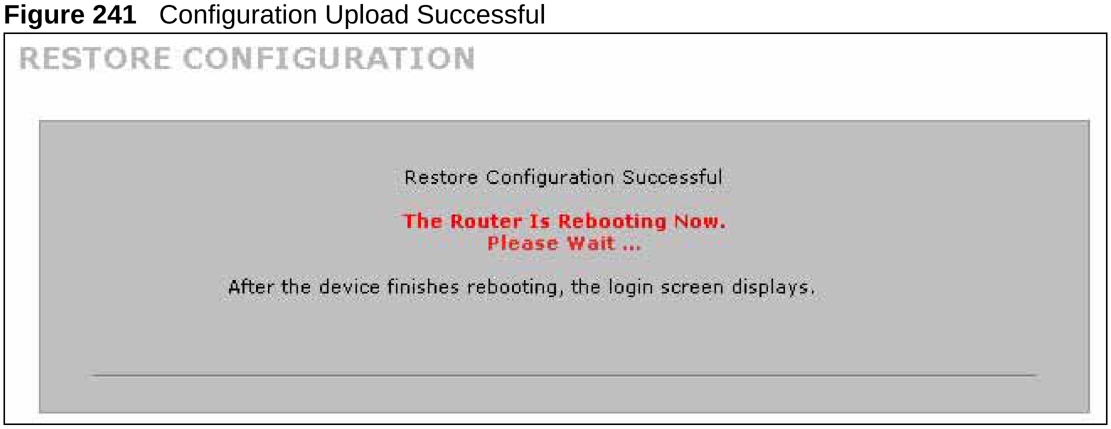
Table 170 Restore Configuration

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

Do not turn off the LAN-Cell while configuration file upload is in progress.

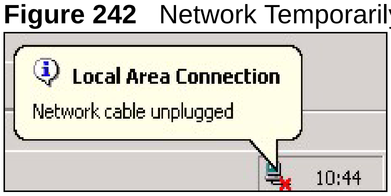
After you see a "restore configuration successful" screen, you must then wait one minute before logging into the LAN-Cell again.

Figure 241 Configuration Upload Successful



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

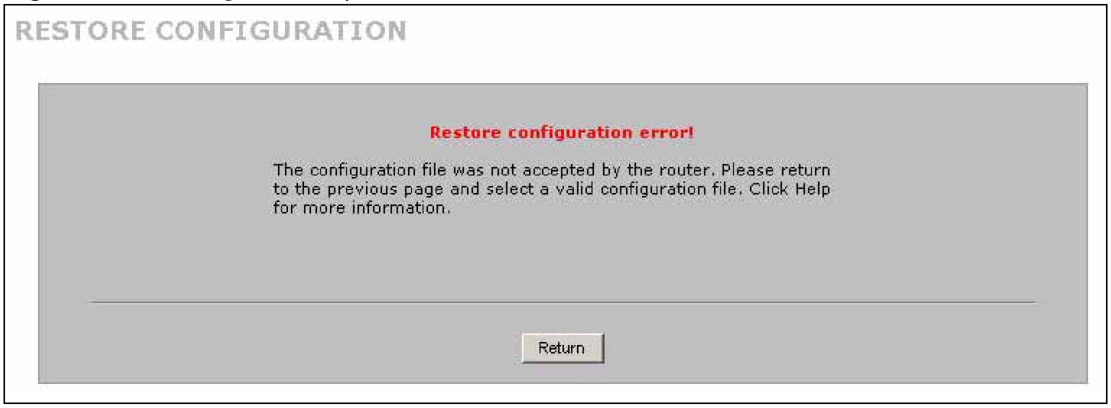
Figure 242 Network Temporarily Disconnected



If you uploaded the default configuration file you may need to change the IP address of your computer to be in the same subnet as that of the default device IP address (192.168.1.1).

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

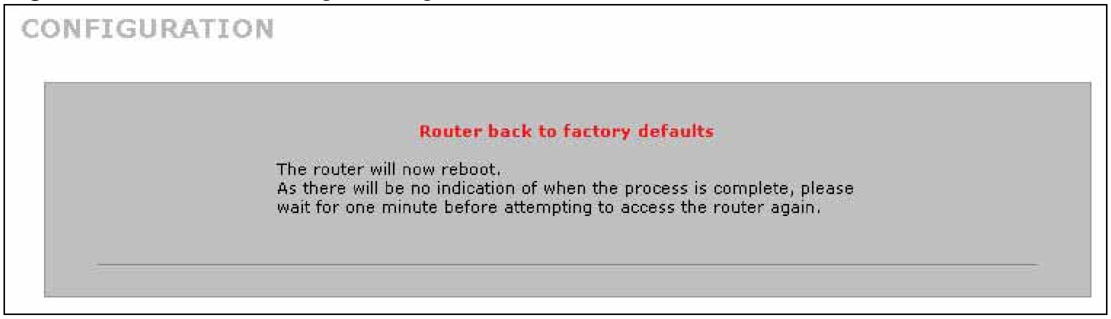
Figure 243 Configuration Upload Error



Back to Factory Defaults

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

Figure 244 Reset Warning Message



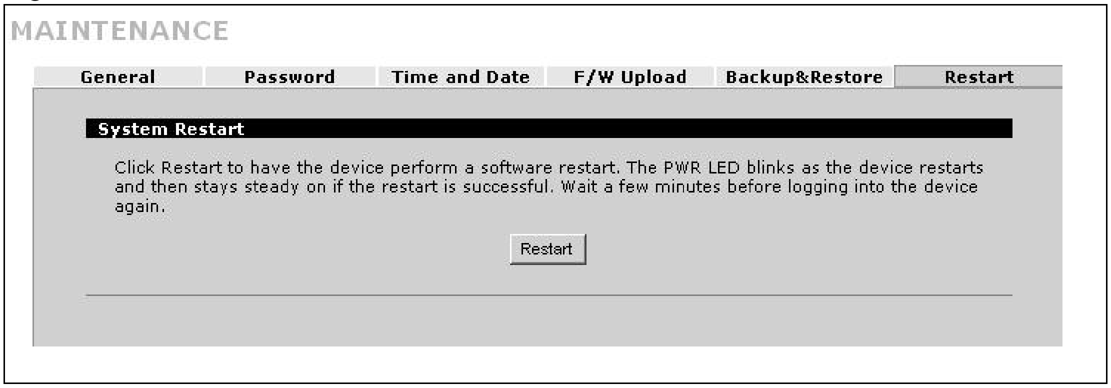
You can also press the hardware **RESET** button to reset the factory defaults of your LAN-Cell. Refer to Section 2.4 on page 51 for more information on the **RESET** button.

22.7 Restart Screen

System restart allows you to reboot the LAN-Cell without turning the power off.

Click **MAINTENANCE** > **Restart**. Click **Restart** to have the LAN-Cell reboot. Restart is different than Reset. Reset returns the device to its default configuration.

Figure 245 MAINTENANCE > Restart



22.8 The Diagnostics Screen

Use the **Diagnostics** screen to have the LAN-Cell generate and send diagnostic files by e-mail and/or the console port. The diagnostics files contain the LAN-Cell's configuration and diagnostic information. You may need to generate this file and send it to customer support during troubleshooting.

Click **MAINTENANCE** > **Diagnostics** to open the following screen.

The LAN-Cell sends only one diagnosis mail within five minutes (unless you click **Perform Diagnostics Now**).

Figure 246 MAINTENANCE > Diagnostics

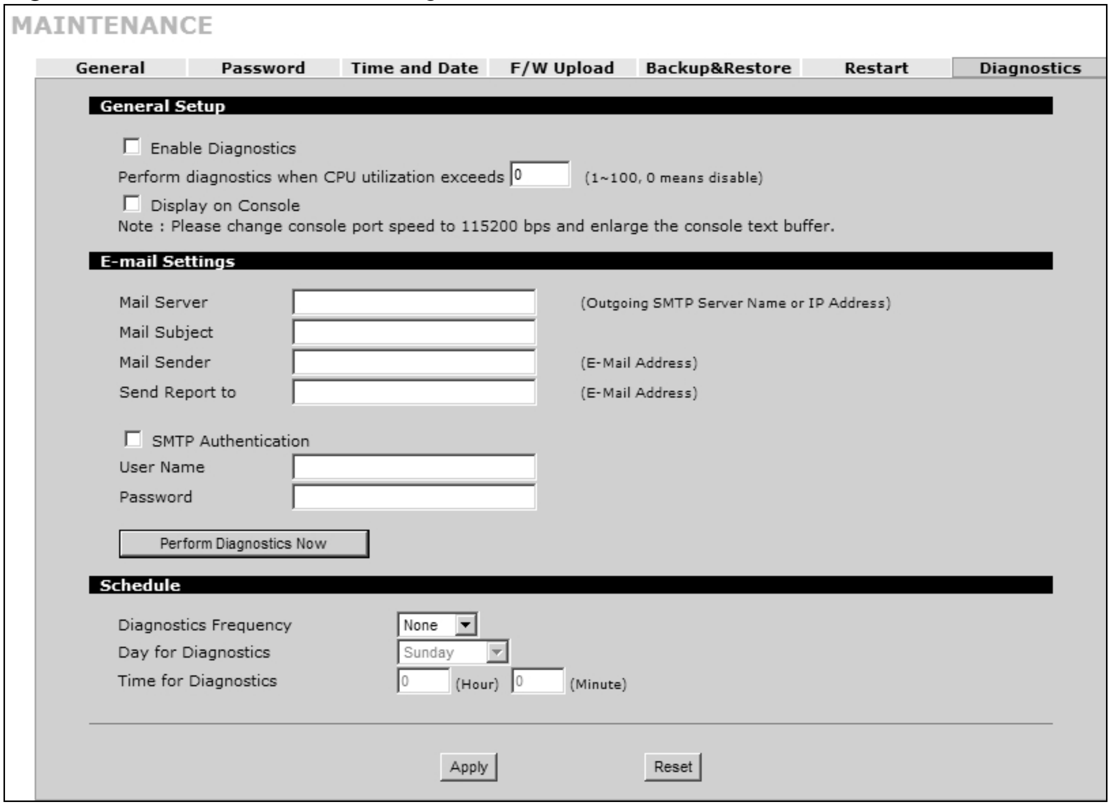


Table 171 MAINTENANCE > Diagnostics

LABEL	DESCRIPTION
Enable Diagnostics	Select this option to turn on the diagnostics feature.
Perform diagnostics when CPU utilization exceeds	Set the LAN-Cell to generate and send a diagnostic file every time the CPU usage exceeds the specified percent for more than 60 seconds. Enter 0 to have the LAN-Cell not generate and send diagnostic files based on CPU usage going over a specific level.
Display on Console	Check this box to have the diagnostic information sent to the LAN-Cell's console port. Change the port speed of your terminal device attached to the console port to 115200 bps before enabling console reporting of diagnostic files.
Send Diagnostic Report by E-Mail	
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, diagnostic files will not be sent via e-mail.
Mail Subject	Type a title that you want to be in the subject line of the diagnostic e-mail message that the LAN-Cell sends.
Mail Sender	Enter the e-mail address that you want to be in the from/sender line of the diagnostic e-mail message that the LAN-Cell sends. If you activate SMTP authentication, the e-mail address must be able to be authenticated by the mail server as well.
Send Log To	Diagnostic files are sent to the e-mail address specified in this field. If this field is left blank, diagnostic files will not be sent via e-mail.

Table 171 MAINTENANCE > Diagnostics (continued)

LABEL	DESCRIPTION
SMTP Authentication	SMTP (Simple Mail Transfer Protocol) is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another. Select the check box to activate SMTP authentication. If mail server authentication is needed but this feature is disabled, you will not receive the e-mail diagnostic files.
User Name	Enter the user name (up to 63 characters) (usually the user name of a mail account).
Password	Enter the password associated with the user name above.
Perform Diagnostics Now	Click this button to generate and send a diagnostic file immediately, instead of based on a time period or CPU usage level.
Schedule Diagnostics	
Periodic Diagnostics	Use these fields to set the LAN-Cell to generate and send diagnostic files at regular intervals. Even if you enable both CPU utilization-based and periodic diagnosis, the LAN-Cell only sends one diagnostic file within five minutes (unless you click **Perform Diagnostics Now**).
Diagnostics Frequency	Set how often the LAN-Cell generates and sends diagnostic files. Hourly Daily Weekly **None**. If you select **Daily** or **Weekly**, specify a time of day for the LAN-Cell to generate and send diagnostic files. If you select **Weekly**, then also specify which day of the week. Select **None** to have the LAN-Cell not generate and send diagnostic files based on a time period.
Day for Diagnostics	Use the drop down list box to select which day of the week to generate and send diagnostic files.
Time for Diagnostics	Enter the time of day in 24-hour format (for example 23:00 equals 11:00 pm) to generate and send diagnostic files.
Apply	Click **Apply** to save your changes back to the LAN-Cell.
Reset	Click **Reset** to begin configuring this screen afresh.

Part VI
System Management Terminal

23

Introducing the SMT

This chapter explains how to access the System Management Terminal and gives an overview of its menus.

23.1 Introduction to the SMT

The LAN-Cell's SMT (System Management Terminal) is a menu-driven interface that you can access from a terminal emulator through the console port or over a telnet/SSH connection. This chapter shows you how to access the SMT (System Management Terminal) menus via console port, how to navigate the SMT and how to configure SMT menus.

23.2 Accessing the SMT via the Console Port

Make sure you have the physical connection properly set up as described in the Quick Start Guide.

When configuring using the console port, you need a computer equipped with communications software configured to the following parameters:

- VT100 terminal emulation.
- 9600 Baud.
- No parity, 8 data bits, 1 stop bit, flow control set to none.

23.2.1 Initial Screen

When you turn on your LAN-Cell, it performs several internal tests as well as line initialization.

After the tests, the LAN-Cell asks you to press [ENTER] to continue, as shown next.

Figure 247 Initial Screen

```
Copyright (c) 1994 - 2007 Proxicast LLC

initialize ch =0, ethernet address: 00:1B:39:01:23:45
initialize ch =1, ethernet address: 00:1B:39:01:23:46
initialize ch =2, ethernet address: 00:1B:39:01:23:47
initialize ch =3, ethernet address: 00:1B:39:01:23:48
initialize ch =4, ethernet address: 00:00:00:00:00:00
AUX port init . done
Modem init . inactive

Press ENTER to continue...
```

23.2.2 Entering the Password

The login screen appears after you press [ENTER], prompting you to enter the password, as shown below.

For your first login, enter the default password “1234”. As you type the password, the screen displays an “X” for each character you type.

Please note that if there is no activity for longer than five minutes after you log in, your LAN-Cell will automatically log you out and display a blank screen. If you see a blank screen, press [ENTER] to bring up the login screen again.

Figure 248 Password Screen

```
Enter Password : XXXX
```

23.3 Navigating the SMT Interface

The SMT is an interface that you use to configure your LAN-Cell.

Several operations that you should be familiar with before you attempt to modify the configuration are listed in the table below.

Table 172 Main Menu Commands

OPERATION	KEYSTROKES	DESCRIPTION
Move down to another menu	[ENTER]	To move forward to a submenu, type in the number of the desired submenu and press [ENTER].
Move up to a previous menu	[ESC]	Press the [ESC] key to move back to the previous menu.
Move to a “hidden” menu	Press [SPACE BAR] to change No to Yes then press [ENTER].	Fields beginning with “Edit” lead to hidden menus and have a default setting of No. Press [SPACE BAR] to change No to Yes, and then press [ENTER] to go to a “hidden” menu.

Table 172 Main Menu Commands

OPERATION	KEYSTROKES	DESCRIPTION
Move the cursor	[ENTER] or [UP]/ [DOWN] arrow keys	Within a menu, press [ENTER] to move to the next field. You can also use the [UP]/[DOWN] arrow keys to move to the previous and the next field, respectively. When you are at the top of a menu, press the [UP] arrow key to move to the bottom of a menu.
Entering information	Fill in, or press [SPACE BAR], then press [ENTER] to select from choices.	You need to fill in two types of fields. The first requires you to type in the appropriate information. The second allows you to cycle through the available choices by pressing [SPACE BAR].
Required fields	<? >	All fields with the symbol <?> must be filled in order be able to save the new configuration.
N/A fields	<N/A>	Some of the fields in the SMT will show a <N/A>. This symbol refers to an option that is Not Applicable.
Save your configuration	[ENTER]	Save your configuration by pressing [ENTER] at the message “Press ENTER to confirm or ESC to cancel”. Saving the data on the screen will take you, in most cases to the previous menu. Make sure you save your settings in each screen that you configure.
Exit the SMT	Type 99, then press [ENTER].	Type 99 at the main menu prompt and press [ENTER] to exit the SMT interface.

23.3.1 Main Menu

After you enter the password, the SMT displays the **LAN-Cell Main Menu**, as shown next.

Figure 249 Main Menu

```
               Copyright (c) 1994 - 2007 Proxicast LLC

                       LAN-Cell 2 Main Menu

     Getting Started                    Advanced Management
       1. General Setup                   21. Filter and Firewall Setup
       2. WAN Setup                       22. SNMP Configuration
       3. LAN Setup                       23. System Password
       4. Ethernet WAN Setup              24. System Maintenance
       5. DMZ Setup                       25. IP Routing Policy Setup
       6. Route Setup                     26. Schedule Setup
       7. WLAN Setup                      33. Cellular Card Command Mode
     Advanced Applications
       11. WAN ISP SETUP
       12. Static Routing Setup
       15. NAT Setup
                                          99. Exit



                          Enter Menu Selection Number:
```

SMT menu numbers are not sequential. SMT menu numbering has been maintained for backward compatibility with previous LAN-Cell models and customer scripting support.

The following table describes the fields in this menu.

Table 173 Main Menu Summary

NO.	MENU TITLE	FUNCTION
1	General Setup	Use this menu to set up device mode, dynamic DNS and administrative information.
2	WAN Setup	Use this menu to clone a MAC address from a computer on your LAN and configure the backup WAN dial-up connection. You can also use this menu to configure 3G modem setting on the LAN-Cell.
3	LAN Setup	Use this menu to apply LAN filters, configure LAN DHCP and TCP/IP settings.
4	Ethernet WAN Setup	Configure your Ethernet WAN access setup (Internet address, gateway, login, etc.) with this menu.
5	DMZ Setup	Use this menu to apply DMZ filters, and configure DHCP and TCP/IP settings for the DMZ port.
6	Route Setup	Use this menu to configure your WAN route assessment, traffic redirect properties and failover parameters.
7	WLAN Setup	Use this menu to configure WLAN DHCP and TCP/IP settings for the wireless LAN interface.
11	WAN ISP Setup	Use this menu to configure detailed remote node settings (your ISP is also a remote node) as well as apply WAN filters.
12	Static Routing Setup	Configure IP static routes in this menu.
15	NAT Setup	Use this menu to configure Network Address Translation.
21	Filter and Firewall Setup	Configure filters and activate/deactivate the firewall.
22	SNMP Configuration	Use this menu to configure SNMP-related parameters.
23	System Password	Change your password in this menu (recommended).
24	System Maintenance	From displaying system status to uploading firmware, this menu provides comprehensive system maintenance.
25	IP Routing Policy Setup	Configure and display policies for use in IP policy routing.
26	Schedule Setup	Use this menu to schedule outgoing calls.
33	Cellular Card Command Mode	When the 3G cellular modem card is not in an active data session, this menu provides access to the modem's command line interface (if supported by the 3G card). Refer to the 3G card manufacturer's documentation for applicable commands in this mode. Type `[EXIT]` to return to the SMT.
99	Exit	Use this menu to exit (necessary for remote configuration).

23.3.2 SMT Menus Overview

The following table gives you an overview of your LAN-Cell's various SMT menus.

Table 174 SMT Menus Overview

MENUS	SUB MENUS		
1 General Setup	1.1 Configure Dynamic DNS	1.1.1 DDNS Host Summary	1.1.1 DDNS Edit Host
2 WAN Setup	2.1 Advanced WAN Setup		
3 LAN Setup	3.1 LAN Port Filter Setup		
	3.2 TCP/IP and DHCP Ethernet Setup	3.2.1 IP Alias Setup	
4 Ethernet WAN Setup			
5 DMZ Setup	5.1 DMZ Port Filter Setup		
	5.2 TCP/IP and DHCP Ethernet Setup	5.2.1 IP Alias Setup	
6 Route Setup	6.1 Route Assessment		
	6.2 Traffic Redirect		
	6.3 Route Failover		
7 WLAN Setup	7.2 TCP/IP and DHCP Ethernet Setup	7.2.1 IP Alias Setup	
11 WAN ISP Setup	11.1 Remote Node Profile (WAN)	11.1.2 Remote Node Network Layer Options	
		11.1.4 Remote Node Filter	
		11.1.5 Traffic Redirect Setup (for the LAN-Cell 5 only)	
	11.2 Remote Node Profile (Cellular 3G WAN)	11.2.2 Remote Node Network Layer Options	
		11.2.3 Remote Node Script	
		11.2.4 Remote Node Filter	
	11.3 Remote Node Profile (Dial Backup ISP)	11.3.1 Remote Node PPP Options	
		11.3.2 Remote Node Network Layer Options	
		11.3.3 Remote Node Script	
		11.3.4 Remote Node Filter	
12 Static Routing Setup	12.1 Edit Static Route Setup		
15 NAT Setup	15.1 Address Mapping Sets	15.1.x Address Mapping Rules	15.1.x.x Address Mapping Rule
	15.2 NAT Server Sets	15.2.x NAT Server Setup	15.2.x.x - NAT Server Configuration
	15.3 Trigger Ports	15.3.x Trigger Port Setup	

Table 174 SMT Menus Overview (continued)

MENUS	SUB MENUS		
21 Filter and Firewall Setup	21.1 Filter Set Configuration	21.1.x Filter Rules Summary	21.1.x.x Generic Filter Rule
			21.1.x.x TCP/IP Filter Rule
	21.2 Firewall Setup		
22 SNMP Configuration			
23 System Password			
24 System Maintenance	24.1 System Status		
	24.2 System Information and Console Port Speed	24.2.1 System Information	
		24.2.2 Console Port Speed	
	24.3 Log and Trace	24.3.1 View Error Log	
		24.3.2 Syslog Logging	
		24.3.4 Call-Triggering Packet	
	24.4 Diagnostic		
	24.5 Backup Configuration		
	24.6 Restore Configuration		
	24.7 Upload Firmware	24.7.1 Upload System Firmware	
		24.7.2 Upload System Configuration File	
	24.8 Command Interpreter Mode		
	24.9 Call Control	24.9.1 Budget Management	
		24.9.2 Call History	
	24.10 Time and Date Setting		
	24.11 Remote Management Setup		
25 IP Routing Policy Summary	25.1 IP Routing Policy Setup	25.1.1 IP Routing Policy Setup	
26 Schedule Setup	26.1 Schedule Set Setup		

23.4 Changing the System Password

Change the system password by following the steps shown next.

1 Enter 23 in the main menu to open **Menu 23 - System Password** as shown next.

Figure 250 Menu 23: System Password

```
                    Menu 23 - System Password

          Old Password= ?
          New Password= ?
          Retype to confirm= ?



           Enter here to CONFIRM or ESC to CANCEL:
```

2 Type your existing password and press [ENTER].
3 Type your new system password and press [ENTER].
4 Re-type your new system password for confirmation and press [ENTER].

Note that as you type a password, the screen displays an “x” for each character you type.

23.5 Resetting the LAN-Cell

See Section 2.4 on page 51 for directions on resetting the LAN-Cell.

24

General Setup

Menu 1 - General Setup contains administrative and system-related information.

24.1 Introduction to General Setup

Menu 1 - General Setup contains administrative and system-related information.

24.2 Configuring General Setup

1 Enter 1 in the main menu to open **Menu 1 - General Setup**.
2 The **Menu 1 - General Setup** screen appears, as shown next. Fill in the required fields.

Figure 251 Menu 1: General Setup

```
                    Menu 1 - General Setup

                    System Name= LAN-Cell
                    Domain Name=


                    Edit Dynamic DNS= No


                    Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this menu.

Table 175 Menu 1: General Setup

FIELD	DESCRIPTION
System Name	Choose a descriptive name for identification purposes. It is recommended you enter your computer's "Computer name" in this field. This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted. "LAN-Cell" is filled in by default.
Domain Name	Enter the domain name (if you know it) here. If you leave this field blank, the ISP may assign a domain name via DHCP. You can go to menu 24.8 and type "sys domain name" to see the current domain name used by your router. The domain name entered by you is given priority over the ISP assigned domain name. If you want to clear this field just press [SPACE BAR] and then [ENTER].

Table 175 Menu 1: General Setup (continued)

FIELD	DESCRIPTION
Edit Dynamic DNS	Press [SPACE BAR] and then [ENTER] to select **Yes** or **No** (default). Select **Yes** to configure **Menu 1.1: Configure Dynamic DNS** discussed next.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm…" to save your configuration, or press [ESC] at any time to cancel.	

24.2.1 Configuring Dynamic DNS

To configure Dynamic DNS, go to **Menu 1 - General Setup** and press [SPACE BAR] to select **Yes** in the **Edit Dynamic DNS** field. Press [ENTER] to display **Menu 1.1 - Configure Dynamic DNS** (shown next).

Figure 252 Menu 1.1: Configure Dynamic DNS

```
               Menu 1.1 - Configure Dynamic DNS

                   Service Provider= WWW.DynDNS.ORG
                   Active= No
                   Username=
                   Password= ********
                   Edit Host= No


                  Press ENTER to Confirm or ESC to Cancel:
```

Follow the instructions in the next table to configure Dynamic DNS parameters.

Table 176 Menu 1.1: Configure Dynamic DNS

FIELD	DESCRIPTION
Service Provider	This is the name of your Dynamic DNS service provider.
Active	Press [SPACE BAR] to select **Yes** and then press [ENTER] to make dynamic DNS active.
Username	Enter your user name.
Password	Enter the password assigned to you.
Edit Host	Press [SPACE BAR] and then [ENTER] to select **Yes** if you want to configure a DDNS host.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm…" to save your configuration, or press [ESC] at any time to cancel.	

24.2.1.1 Editing DDNS Host

To configure a DDNS host, follow the procedure below.

1. Enter 1 in the main menu to open **Menu 1 - General Setup**.
2. Press [SPACE BAR] to select **Yes** in the **Edit Dynamic DNS** field. Press [ENTER] to display **Menu 1.1 - Configure Dynamic DNS**.
3. Press [SPACE BAR] and then [ENTER] to select **Yes** in the **Edit Host** field. Press [ENTER] to display **Menu 1.1.1 - DDNS Host Summary**.

Figure 253 Menu 1.1.1: DDNS Host Summary

```
                 Menu 1.1.1 DDNS Host Summary

     #                        Summary
     --- - -------------------------------------------------------
     01    Hostname=LC2.proxicast.com,
             Type=Dynamic,WC=Yes,Offline=No,Policy=DDNS Server
           Detect, WAN, HA=Yes
     02    _______________________________________________________
           _______________________________________________________
     03    _______________________________________________________
           _______________________________________________________
     04    _______________________________________________________
           _______________________________________________________
     05    _______________________________________________________
           _______________________________________________________


                 Select Command= None           Select Rule= N/A
                       Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this screen.

Table 177 Menu 1.1.1: DDNS Host Summary

FIELD	DESCRIPTION
#	This is the DDNS host index number.
Summary	This displays the details about the DDNS host.
Select Command	Press [SPACE BAR] to choose from **None**, **Edit**, **Delete**, **Next Page** or **Previous Page** and then press [ENTER]. You must select a DDNS host in the next field when you choose the **Edit** or **Delete** commands. Select **None** and then press [ENTER] to go to the "Press ENTER to Confirm…" prompt. Use **Edit** to create or edit a rule. Use **Delete** to remove a rule. To edit or delete a DDNS host, first make sure you are on the correct page. When a rule is deleted, subsequent rules do not move up in the page list. Select **Next Page** or **Previous Page** to view the next or previous page of DDNS hosts (respectively).
Select Rule	Type the DDNS host index number you wish to edit or delete and then press [ENTER].
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm…" to save your configuration, or press [ESC] at any time to cancel.	

4 Select **Edit** in the **Select Command** field; type the index number of the DDNS host you want to configure in the **Select Rule** field and press [ENTER] to open **Menu 1.1.1 - DDNS Edit Host** (see the next figure).

Figure 254 Menu 1.1.1: DDNS Edit Host

```
                        Menu 1.1.1 - DDNS Edit Host

            Hostname= LC2.proxicast.com
            DDNS Type= DynamicDNS
            Enable Wildcard Option= Yes
            Enable Off Line Option= N/A
            Bind WAN= 1
            HA= Yes
            IP Address Update Policy:
              Let DDNS Server Auto Detect= Yes
              Use User-Defined= N/A
              Use WAN IP Address= N/A


                           Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this screen.

Table 178 Menu 1.1.1: DDNS Edit Host

FIELD	DESCRIPTION
Host Name	Enter your host name in this field.
DDNS Type	Press [SPACE BAR] and then [ENTER] to select **DynamicDNS** if you have the Dynamic DNS service. Select **StaticDNS** if you have the Static DNS service. Select **CustomDNS** if you have the Custom DNS service.
Enable Wildcard Option	Your LAN-Cell supports DYNDNS Wildcard. Press [SPACE BAR] and then [ENTER] to select **Yes** or **No**. This field is **N/A** when you choose DDNS client as your service provider.
Enable Off Line Option	This field is only available when **CustomDNS** is selected in the **DDNS Type** field. Press [SPACE BAR] and then [ENTER] to select **Yes**. When **Yes** is selected, http://www.dyndns.org/ traffic is redirected to a URL that you have previously specified (see www.dyndns.org for details).
Bind WAN	Enter the WAN interface to use for updating the IP address of the domain name.
HA	Press [SPACE BAR] and then [ENTER] to select **Yes** to enable the high availability (HA) feature. If the WAN interface specified in the **Bind WAN** field does not have a connection, the LAN-Cell will attempt to use the IP address of another WAN interface to update the domain name. When the WAN interfaces are in the active/passive operating mode, the LAN-Cell will update the domain name with the IP address of whichever WAN interface has a connection, regardless of the setting in the **Bind WAN** field. Clear this check box and the LAN-Cell will not update the domain name with an IP address if the WAN interface specified in the **Bind WAN** field does not have a connection. Note: If you enable high availability, DDNS can also function when the LAN-Cell uses the dial backup port. DDNS does not function when the LAN-Cell uses traffic redirect. Refer to Section on page 317 for detailed information.

Table 178 Menu 1.1.1: DDNS Edit Host (continued)

FIELD	DESCRIPTION
IP Address Update Policy:	You can select **Yes** in either the **Let DDNS Server Auto Detect** field (recommended) or the **Use User-Defined** field, but not both. With the **Let DDNS Server Auto Detect** and **Use User-Defined** fields both set to **No**, the DDNS server automatically updates the IP address of the host name(s) with the LAN-Cell's WAN IP address. DDNS does not work with a private IP address. When both fields are set to **No**, the LAN-Cell must have a public WAN IP address in order for DDNS to work.
Let DDNS Server Auto Detect	Only select this option when there are one or more **NAT** routers between the LAN-Cell and the DDNS server. Press [SPACE BAR] to select **Yes** and then press [ENTER] to have the DDNS server automatically detect and use the IP address of the NAT router that has a public IP address. Note: The DDNS server may not be able to detect the proper IP address if there is an HTTP proxy server between the LAN-Cell and the DDNS server.
Use User-Defined	Press [SPACE BAR] to select **Yes** and then press [ENTER] to update the IP address of the host name(s) to the IP address specified below. Only select **Yes** if the LAN-Cell uses or is behind a static public IP address.
Use WAN IP Address	Enter the static public IP address if you select **Yes** in the **Use User-Defined** field.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm…" to save your configuration, or press [ESC] at any time to cancel.	

The IP address updates when you reconfigure menu 1 or perform DHCP client renewal.

25

WAN, 3G and Dial Backup Setup

This chapter describes how to configure the WAN using menu 2 and dial-backup using menus 2.1 and 11.1.

25.1 Introduction to WAN, 3G WAN and Dial Backup Setup

This chapter explains how to configure settings for your WAN interface(s), a 3G WAN connection and a dial backup connection using the SMT menus.

25.2 WAN Setup

From the main menu, enter 2 to open menu 2.

Figure 255 MAC Address Cloning in WAN Setup

```
                    Menu 2 - WAN Setup

              WAN MAC Address:
                Assigned By= Factory default
                IP Address= N/A

              Dial-Backup:
                Active= No
                Port Speed= 115200
                AT Command String:
                  Init= at&fs0=0
                Edit Advanced Setup= No

              Cellular Modem Setup:
                Init= Configure APN
                APN = internet
                PIN code=


         Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this screen.

Table 179 MAC Address Cloning in WAN Setup

FIELD	DESCRIPTION
WAN MAC Address	
Assigned By	Press [SPACE BAR] and then [ENTER] to choose one of two methods to assign a MAC Address. Choose **Factory Default** to select the factory assigned default MAC Address. Choose **IP address attached on LAN** to use the MAC Address of that computer whose IP you give in the following field.
IP Address	This field is applicable only if you choose the **IP address attached on LAN** method in the **Assigned By** field. Enter the IP address of the computer on the LAN whose MAC you are cloning.
When you have completed this menu, press [ENTER] at the prompt “Press ENTER to Confirm…” to save your configuration, or press [ESC] at any time to cancel.	

25.3 Dial Backup

The Dial Backup port can be used in reserve, as a traditional dial-up connection should the broadband connection to the WAN port fail. To set up the auxiliary port (Dial Backup) for use in the event that the regular WAN connection is dropped.

1. Menu 2 - WAN Setup,
2. Menu 2.1 - Advanced WAN Setup and
3. Menu 11.3 - Remote Node Profile (Backup ISP)

Refer also to the section about traffic redirect for information on an alternate backup WAN connection.

25.3.1 Configuring Dial Backup in Menu 2

From the main menu, enter 2 to open menu 2.

Figure 256 Menu 2: Dial Backup Setup

```
                    Menu 2 - WAN Setup

              WAN MAC Address:
                Assigned By= Factory default
                IP Address= N/A

              Dial-Backup:
                Active= No
                Port Speed= 115200
                AT Command String:
                  Init= at&fs0=0
                Edit Advanced Setup= No

              Cellular Modem Setup:
                Init= Configure APN
                APN = internet
                PIN code=


         Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this menu.

Table 180 Menu 2: Dial Backup Setup

FIELD	DESCRIPTION
Dial-Backup:	
Active	Use this field to turn the dial-backup feature on (**Yes**) or off (**No**).
Port Speed	Press [SPACE BAR] and then press [ENTER] 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.
AT Command String:	
Init	Enter 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.
Edit Advanced Setup	To edit the advanced setup for the Dial Backup port, move the cursor to this field; press the [SPACE BAR] to select **Yes** and then press [ENTER] to go to **Menu 2.1 - Advanced Setup**.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm…" to save your configuration, or press [ESC] at any time to cancel.	

25.3.2 Advanced WAN Setup

Consult the manual of your WAN device connected to your Dial Backup port for specific AT commands.

To edit the advanced setup for the Dial Backup port, move the cursor to the **Edit Advanced Setup** field in **Menu 2 - WAN Setup**, press the [SPACE BAR] to select **Yes** and then press [ENTER].

Figure 257 Menu 2.1: Advanced WAN Setup

```
                    Menu 2.1 - Advanced WAN Setup

     AT Command Strings:                     Call Control:
       Dial= atdt                              Dial Timeout(sec)= 60
       Drop= ~~+++~~ath                        Retry Count= 0
       Answer= ata                             Retry Interval(sec)= N/A
                                               Drop Timeout(sec)= 20
     Drop DTR When Hang Up= Yes                Call Back Delay(sec)= 15

       AT Response Strings:
         CLID= NMBR =
         Called Id=
         Speed= CONNECT

             Press ENTER to Confirm or ESC to Cancel:
```

The following table describes fields in this menu.

Table 181 Advanced WAN Port Setup: AT Commands Fields

FIELD	DESCRIPTION
AT Command Strings:	
Dial	Enter the AT Command string to make a call.
Drop	Enter the AT Command string to drop a call. “~” represents a one second wait, e.g., “~~~+++~~ath” can be used if your modem has a slow response time.
Answer	Enter the AT Command string to answer a call.
Drop DTR When Hang Up	Press the [SPACE BAR] to choose either **Yes** or **No**. When **Yes** is selected (the default), the DTR (Data Terminal Ready) signal is dropped after the “AT Command String: Drop” is sent out.
AT Response Strings:	
CLID (Calling Line Identification)	Enter the keyword that precedes the CLID (Calling Line Identification) in the AT response string. This lets the LAN-Cell capture the CLID in the AT response string that comes from the WAN device. CLID is required for CLID authentication.
Called Id	Enter the keyword preceding the dialed number.
Speed	Enter the keyword preceding the connection speed.

Table 182 Advanced WAN Port Setup: Call Control Parameters

FIELD	DESCRIPTION
Call Control	
Dial Timeout (sec)	Enter a number of seconds for the LAN-Cell to keep trying to set up an outgoing call before timing out (stopping). The LAN-Cell times out and stops if it cannot set up an outgoing call within the timeout value.
Retry Count	Enter a number of times for the LAN-Cell to retry a busy or no-answer phone number before blacklisting the number.
Retry Interval (sec)	Enter a number of seconds for the LAN-Cell to wait before trying another call after a call has failed. This applies before a phone number is blacklisted.
Drop Timeout (sec)	Enter a number of seconds for the LAN-Cell to wait before dropping the DTR signal if it does not receive a positive disconnect confirmation.
Call Back Delay (sec)	Enter a number of seconds for the LAN-Cell to wait between dropping a callback request call and dialing the co-responding callback call.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm…" to save your configuration, or press [ESC] at any time to cancel.	

25.3.3 Remote Node Profile (Backup ISP)

Enter **3** in **Menu 11 - WAN ISP Setup** to open **Menu 11.3 - Remote Node Profile (Backup ISP)** (shown below) and configure the setup for your Dial Backup port connection. Not all fields are available on all models.

Figure 258 Menu 11.3: Remote Node Profile (Backup ISP)

```
                Menu 11.3 - Remote Node Profile (Backup ISP)

     Rem Node Name=
     Active= No
                                         Edit IP= No
     Outgoing:                           Edit Script Options= No
       My Login= ChangeMe
       My Password= ********             Telco Option:
       Retype to Confirm= ********         Allocated Budget(min)= 0
       Authen= CHAP/PAP                      Period(hr)= 0
       Pri Phone #= 0                      Schedules=
       Sec Phone #=                        Always On= No

                                         Session Options:
                                           Edit Filter Sets= No
                                           Idle Timeout(sec)= 100



                  Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this menu.

Table 183 Menu 11.3: Remote Node Profile (Backup ISP)

FIELD	DESCRIPTION
Rem Node Name	Enter a descriptive name for the remote node. This field can be up to eight characters.
Active	Press [SPACE BAR] and then [ENTER] to select **Yes** to enable the remote node or **No** to disable the remote node.
Outgoing	
My Login	Enter the login name assigned by your ISP for this remote node.
My Password	Enter the password assigned by your ISP for this remote node.
Retype to Confirm	Enter your password again to make sure that you have entered is correctly.
Authen	This field sets the authentication protocol used for outgoing calls. Options for this field are: **CHAP/PAP** - Your LAN-Cell will accept either **CHAP** or **PAP** when requested by this remote node. **CHAP** - accept CHAP only. **PAP** - accept PAP only.
Pri Phone # Sec Phone #	Enter the first (primary) phone number from the ISP for this remote node. If the Primary Phone number is busy or does not answer, your LAN-Cell 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.
Edit IP	This field leads to a “hidden” menu. Press [SPACE BAR] to select **Yes** and press [ENTER] to go to **Menu 11.3.2 - Remote Node Network Layer Options**. See Section 25.3.4 on page 433 for more information.
Edit Script Options	Press [SPACE BAR] to select **Yes** and press [ENTER] to edit the AT script for the dial backup remote node (**Menu 11.3.3 - Remote Node Script**). See Section 25.3.5 on page 434 for more information.
Telco Option	
Allocated Budget	Enter the maximum number of minutes that this remote node may be called within the time period configured in the **Period** field. The default for this field is 0 meaning there is no budget control and no time limit for accessing this remote node.
Period(hr)	Enter 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).
Schedules	You can apply up to four schedule sets here. For more details please refer to Chapter 42 on page 563.
Always On	Press [SPACE BAR] to select **Yes** to set this connection to be on all the time, regardless of whether or not there is any traffic. Select **No** to have this connection act as a dial-up connection.
Session Options	
Edit Filter sets	This field leads to another “hidden” menu. Use [SPACE BAR] to select **Yes** and press [ENTER] to open menu 11.3.4 to edit the filter sets. See Section 25.3.6 on page 436 for more details.
Idle Timeout	Enter the number of seconds of idle time (when there is no traffic from the LAN-Cell to the remote node) that can elapse before the LAN-Cell automatically disconnects the PPP connection. This option only applies when the LAN-Cell initiates the call.
Once you have configured this menu, press [ENTER] at the message “Press ENTER to Confirm...” to save your configuration, or press [ESC] at any time to cancel.	

25.3.4 Editing TCP/IP Options

Move the cursor to the **Edit IP** field in menu 11.3, then press [SPACE BAR] to select **Yes**. Press [ENTER] to open **Menu 11.3.2 - Remote Node Network Layer Options**.

Figure 259 Menu 11.3.2: Remote Node Network Layer Options

```
             Menu 11.3.2 - Remote Node Network Layer Options

               IP Address Assignment= Static
               Rem IP Addr= 0.0.0.0
               Rem Subnet Mask= 0.0.0.0
               My WAN Addr= 0.0.0.0

               Network Address Translation= SUA Only
               NAT Lookup Set= 255
               Metric= 15
               Private= No
               RIP Direction= None
                 Version= N/A
               Multicast= None

                Enter here to CONFIRM or ESC to CANCEL:
```

The following table describes the fields in this menu.

Table 184 Menu 11.3.2: Remote Node Network Layer Options

FIELD	DESCRIPTION
IP Address Assignment	If your ISP did not assign you a fixed IP address, press [SPACE BAR] and then [ENTER] to select **Dynamic**, otherwise select **Static** and enter the IP address and subnet mask in the following fields.
Rem IP Address	Enter the (fixed) IP address assigned to you by your ISP (static IP address assignment is selected in the previous field).
Rem Subnet Mask	Enter the subnet mask associated with your static IP.
My WAN Addr	Leave the field set to 0.0.0.0 to have the ISP or other remote router dynamically (automatically) assign your WAN IP address if you do not know it. Enter your WAN IP address here if you know it (static). This is the address assigned to your local LAN-Cell, not the remote router.
Network Address Translation	Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network (for example a private IP address used in a local network) to a different IP address known within another network (for example a public IP address used on the Internet). Press [SPACE BAR] and then [ENTER] to select either **Full Feature**, **None** or **SUA Only**. Choose **None** to disable NAT. Choose **SUA Only** if you have a single public IP address. SUA (Single User Account) is a subset of NAT that supports two types of mapping: **Many-to-One** and **Server**. Choose **Full Feature** if you have multiple public IP addresses. **Full Feature** mapping types include: **One-to-One**, **Many-to-One** (SUA/PAT), **Many-to-Many Overload**, **Many- One-to-One** and **Server**. When you select **Full Feature** you must configure at least one address mapping set. See Chapter 13 on page 289 for a full discussion on this feature.

Table 184 Menu 11.3.2: Remote Node Network Layer Options

FIELD	DESCRIPTION
NAT Lookup Set	If you select **SUA Only** in the **Network Address Translation** field, it displays **255** and indicates the SMT will use the pre-configured **Set 255** (read only) in menu 15.1. If you select **Full Feature** or **None** in the **Network Address Translation** field, it displays **1**, **2** or **3** and indicates the SMT will use the pre-configured **Set 1** in menu 15.1 for the first WAN port, **Set 2** in menu 15.1 for the second WAN port and **Set 3** for the Backup port. Refer to Section 33.2 on page 479 for more information.
Metric	Enter a number from 1 to 15 to set this route's priority among the LAN-Cell's routes. The smaller the number, the higher priority the route has.
Private	This parameter determines if the LAN-Cell 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 broadcasts. If **No**, the route to this remote node will be propagated to other hosts through RIP broadcasts.
RIP Direction	Press [SPACE BAR] and then [ENTER] to select the **RIP Direction** from **Both**, **None**, **In Only**, **Out Only** and **None**.
Version	Press [SPACE BAR] and then [ENTER] to select the RIP version from **RIP-1**, **RIP-2B** and **RIP-2M**.
Multicast	IGMP (Internet Group Multicast Protocol) is a session-layer protocol used to establish membership in a Multicast group. The LAN-Cell supports both IGMP version 1 (**IGMP-v1**) and version 2 (**IGMP-v2**). Press the [SPACE BAR] to enable IP Multicasting or select **None** to disable it. See Section on page 80 for more information on this feature.
Once you have completed filling in **Menu 11.3.2 Remote Node Network Layer Options**, press [ENTER] at the message "Press ENTER to Confirm..." to save your configuration and return to menu 11.3, or press [ESC] at any time to cancel.	

25.3.5 Editing Login Script

For some remote gateways, text login is required before PPP negotiation is started. The LAN-Cell provides a script facility for this purpose. The script has six programmable sets; each set is composed of an 'Expect' string and a 'Send' string. After matching a message from the server to the 'Expect' field, the LAN-Cell returns the set's 'Send' string to the server.

For instance, a typical login sequence starts with the server printing a banner, a login prompt for you to enter the user name and a password prompt to enter the password:

```
Welcome to Acme, Inc.
Login: myLogin
Password:
```

To handle the first prompt, you specify "`ogin: `" as the 'Expect' string and "`myLogin`" as the 'Send' string in set 1. The reason for leaving out the leading "`L`" is to avoid having to know exactly whether it is upper or lower case. Similarly, you specify "`word: `" as the 'Expect' string and your password as the 'Send' string for the second prompt in set 2.

You can use two variables, `$USERNAME` and `$PASSWORD` (all UPPER case), to represent the actual user name and password in the script, so they will not show in the clear. They are replaced with the outgoing login name and password in the remote node when the LAN-Cell sees them in a 'Send' string. Please note that both variables must been entered exactly as shown. No other characters may appear before or after, either, i.e., they must be used alone in response to login and password prompts.

Please note that the ordering of the sets is significant, i.e., starting from set 1, the LAN-Cell will wait until the ‘Expect’ string is matched before it proceeds to set 2, and so on for the rest of the script. When both the ‘Expect’ and the ‘Send’ fields of the current set are empty, the LAN-Cell will terminate the script processing and start PPP negotiation. This implies two things: first, the sets must be contiguous; the sets after an empty one are ignored. Second, the last set should match the final message sent by the server. For instance, if the server prints:

```
login successful.
Starting PPP...
```

after you enter the password, then you should create a third set to match the final “PPP...” but without a “Send” string. Otherwise, the LAN-Cell will start PPP prematurely right after sending your password to the server.

If there are errors in the script and it gets stuck at a set for longer than the “Dial Timeout” in menu 2 (default 60 seconds), the LAN-Cell will timeout and drop the line. To debug a script, go to Menu 24.4 to initiate a manual call and watch the trace display to see if the sequence of messages and prompts from the server differs from what you expect.

Figure 260 Menu 11.3.3: Remote Node Script

```
                    Menu 11.3.3 - Remote Node Script

                   Active= No

                   Set 1:                                    Set 5:
                     Expect=                                   Expect=
                     Send=                                     Send=
                   Set 2:                                    Set 6:
                     Expect=                                   Expect=
                     Send=                                     Send=
                   Set 3:
                     Expect=
                     Send=
                   Set 4:
                     Expect=
                     Send=

              Enter here to CONFIRM or ESC to CANCEL:
```

The following table describes the fields in this menu.

Table 185 Menu 11.3.3: Remote Node Script

FIELD	DESCRIPTION
Active	Press [SPACE BAR] and then [ENTER] to select either **Yes** to enable the AT strings or **No** to disable them.
Set 1-6: Expect	Enter an Expect string to match. After matching the Expect string, the LAN-Cell returns the string in the **Send** field.
Set 1-6: Send	Enter a string to send out after the Expect string is matched.

25.3.6 Remote Node Filter

Move the cursor to the field **Edit Filter Sets** in menu 11.3, and then press [SPACE BAR] to set the value to **Yes**. Press [ENTER] to open **Menu 11.3.4 - Remote Node Filter**.

Use menu 11.3.4 to specify the filter set(s) to apply to the incoming and outgoing traffic between this remote node and the LAN-Cell to prevent certain packets from triggering calls. You can specify up to four filter sets separated by commas, for example, 1, 5, 9, 12, in each filter field. Note that spaces are accepted in this field. Please refer to Chapter 35 on page 499 for more information on defining the filters.

Figure 261 Menu 11.3.4: Remote Node Filter

```
              Menu 11.3.4 - Remote Node Filter

              Input Filter Sets:
                protocol filters=
                  device filters=
              Output Filter Sets:
                protocol filters=
                  device filters=
              Call Filter Sets:
                protocol filters=
                  device filters=


                   Enter here to CONFIRM or ESC to CANCEL:
```

25.4 3G WAN

3G (Third Generation) is a digital, packet-switched wireless technology. Bandwidth usage is optimized as multiple users share the same channel and bandwidth is only allocated to users when they send data. It allows fast transfer of voice and non-voice data and provides broadband Internet access to mobile devices. See Section 5.4 on page 114 for more information.

To set up a 3G connection, you need to configure

1. Menu 2 - WAN Setup,
2. Menu 11.2 - Remote Node Profile (Cellular 3G WAN)

25.4.1 3G Modem Setup

From the main menu, enter 2 to open menu 2.

Figure 262 3G Modem Setup in WAN Setup

```
                          Menu 2 - WAN Setup

                    WAN MAC Address:
                      Assigned By= Factory default
                      IP Address= N/A

                    Dial-Backup:
                      Active= No
                      Port Speed= 115200
                      AT Command String:
                        Init= at&fs0=0
                      Edit Advanced Setup= No

                    Cellular Modem Setup:
                      Init= Configure APN
                      APN = internet
                     PIN code=0000


               Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this screen.

Table 186 3G Modem Setup in WAN Setup

FIELD	DESCRIPTION
Cellular Modem Setup	
Init	Press [SPACEBAR] to toggle between **Configure APN** and **Configure Directly**. When selecting Configure APN, enter the appropriate APN in the next field. When selecting Configure Directly, enter the appropriate 3G modem initialization string.
APN	Enter the APN (Access Point Name) provided by your service provider. Connections with different APNs may provide different services (such as Internet access or MMS (Multi-Media Messaging Service)) and charge method. You can enter up to 31 ASCII printable characters. Spaces are allowed.
PIN Code	A PIN (Personal Identification Number) code is a key to a 3G card. Without the PIN code, you cannot use the 3G card. Enter the 4-digit PIN code (0000 for example) provided by your ISP. If you enter the PIN code incorrectly, the 3G card may be blocked by your ISP and you cannot use the account to access the Internet. If your ISP disabled PIN code authentication, enter an arbitrary number.
When you have completed this menu, press [ENTER] at the prompt “Press ENTER to Confirm…” to save your configuration, or press [ESC] at any time to cancel.	

25.4.2 Remote Node Profile (3G WAN)

Enter **2** in **Menu 11 - WAN ISP Setup** to open **Menu 11.2 - Remote Node Profile (Cellular 3G WAN)** (shown below) and configure the setup for your 3G connection.

Figure 263 Menu 11.2: Remote Node Profile (3G WAN)

```
                    Menu 11.2 - Remote Node Profile (Cellular)

     Rem Node Name= CELLULAR
     Active= Yes
                                          Edit IP= No
     Outgoing:                            Edit Script Options= No
       My Login= test
       My Password= ********
       Retype to Confirm= ********
       Authen= CHAP/PAP
       Pri Phone #= *99#
                                            Always On= No

                                          Session Options:
                                            Edit Filter Sets= No
                                            Idle Timeout(sec)= 100



                    Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this menu.

Table 187 Menu 11.2: Remote Node Profile (3G WAN)

FIELD	DESCRIPTION
Rem Node Name	Enter a descriptive name for the remote node. This field can be up to eight characters. **CELLULAR** denotes a 3G WAN connection but you can change the name.
Active	Press [SPACE BAR] and then [ENTER] to select **Yes** to enable the remote node or **No** to disable the remote node.
Outgoing	
My Login	Enter the login name assigned by your ISP for this remote node.
My Password	Enter the password assigned by your ISP for this remote node.
Retype to Confirm	Enter your password again to make sure that you have entered is correctly.
Authen	This field sets the authentication protocol used for outgoing calls. Options for this field are: **CHAP**/**PAP** - Your LAN-Cell will accept either **CHAP** or **PAP** when requested by this remote node. **CHAP** - accept CHAP only. **PAP** - accept PAP only.
Pri Phone #	Enter the phone number (dial string) used to dial up a connection to your service provider's base station. Your ISP should provide the phone number. For example, *99# is the dial string to establish a GSM connection; #777 is used for CDMA networks.
Edit IP	This field leads to a "hidden" menu. Press [SPACE BAR] to select **Yes** and press [ENTER] to go to **Menu 11.3.2 - Remote Node Network Layer Options**. See Section 25.3.4 on page 433 for more information.

Table 187 Menu 11.2: Remote Node Profile (3G WAN) (continued)

FIELD	DESCRIPTION
Edit Script Options	Press [SPACE BAR] to select **Yes** and press [ENTER] to edit the AT script for the dial backup remote node (**Menu 11.3.3 - Remote Node Script**). See Section 25.3.5 on page 434 for more information.
Always On	Press [SPACE BAR] to select **Yes** to set this connection to be on all the time, regardless of whether or not there is any traffic. Select **No** to have this connection act as a dial-up connection.
Session Options	
Edit Filter sets	This field leads to another “hidden” menu. Use [SPACE BAR] to select **Yes** and press [ENTER] to open menu 11.3.4 to edit the filter sets. See Section 25.3.6 on page 436 for more details.
Idle Timeout	Enter the number of seconds of idle time (when there is no traffic from the LAN-Cell to the remote node) that can elapse before the LAN-Cell automatically disconnects the 3G connection. .
Once you have configured this menu, press [ENTER] at the message “Press ENTER to Confirm...” to save your configuration, or press [ESC] at any time to cancel.	

26

LAN Setup

This chapter describes how to configure the LAN using **Menu 3 - LAN Setup**.

26.1 Introduction to LAN Setup

This chapter describes how to configure the LAN-Cell for LAN and wireless LAN connections.

26.2 Accessing the LAN Menus

From the main menu, enter 3 to open **Menu 3 - LAN Setup**.

Figure 264 Menu 3: LAN Setup

```
                              Menu 3 - LAN Setup

                  1. LAN Port Filter Setup
                  2. TCP/IP and DHCP Setup




                         Enter Menu Selection Number:
```

26.3 LAN Port Filter Setup

This menu allows you to specify the filter sets that you wish to apply to the LAN traffic. You seldom need to filter the LAN traffic, however, the filter sets may be useful to block certain packets, reduce traffic and prevent security breaches.

Figure 265 Menu 3.1: LAN Port Filter Setup

```
              Menu 3.1 - LAN Port Filter Setup

              Input Filter Sets:
                protocol filters=
                  device filters=
              Output Filter Sets:
                protocol filters=
                  device filters=

              Press ENTER to Confirm or ESC to Cancel:
```

26.4 TCP/IP and DHCP Ethernet Setup Menu

From the main menu, enter 3 to open **Menu 3 - LAN Setup** to configure TCP/IP (RFC 1155) and DHCP Ethernet setup.

Figure 266 Menu 3: TCP/IP and DHCP Setup

```
                   Menu 3 - LAN Setup

              1. LAN Port Filter Setup
              2. TCP/IP and DHCP Setup



                       Enter Menu Selection Number:
```

From menu 3, select the submenu option **TCP/IP and DHCP Setup** and press [ENTER]. The screen now displays **Menu 3.2 - TCP/IP and DHCP Ethernet Setup**, as shown next.

Figure 267 Menu 3.2: TCP/IP and DHCP Ethernet Setup

```
            Menu 3.2 - TCP/IP and DHCP Ethernet Setup


      DHCP= Server                      TCP/IP Setup:
      Client IP Pool:
        Starting Address= 192.168.1.33  IP Address= 192.168.1.1
        Size of Client IP Pool= 128     IP Subnet Mask= 255.255.255.0
                                        RIP Direction= Both
                                          Version= RIP-1
                                        Multicast= None
                                        Edit IP Alias= No



      DHCP Server Address= N/A



                          Press ENTER to Confirm or ESC to Cancel:
```

Follow the instructions in the next table on how to configure the DHCP fields.

Table 188 Menu 3.2: DHCP Ethernet Setup Fields

FIELD	DESCRIPTION
DHCP	This field enables/disables the DHCP server. If set to **Server**, your LAN-Cell will act as a DHCP server. If set to **None**, the DHCP server will be disabled. If set to **Relay**, the LAN-Cell acts as a surrogate DHCP server and relays requests and responses between the remote server and the clients. When set to **Server**, the following items need to be set:
Client IP Pool:	
Starting Address	This field specifies the first of the contiguous addresses in the IP address pool.
Size of Client IP Pool	This field specifies the size, or count of the IP address pool.

Table 188 Menu 3.2: DHCP Ethernet Setup Fields

FIELD	DESCRIPTION
First DNS Server Second DNS Server Third DNS Server	The LAN-Cell passes a DNS (Domain Name System) server IP address (in the order you specify here) to the DHCP clients. Select **From ISP** if your ISP dynamically assigns DNS server information (and the LAN-Cell's WAN IP address). The **IP Address** field below 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 **IP Address** field below. If you chose **User-Defined**, but leave the IP address set to 0.0.0.0, **User-Defined** changes to **None** after you save your changes. If you set a second choice to **User-Defined**, and enter the same IP address, the second **User-Defined** changes to **None** after you save your changes. Select **DNS Relay** to have the LAN-Cell act as a DNS proxy. The LAN-Cell's LAN IP address displays in the I**P Address** field below (read-only). The LAN-Cell tells the DHCP clients on the LAN that the LAN-Cell itself is the DNS server. When a computer on the LAN sends a DNS query to the LAN-Cell, the LAN-Cell forwards the query to the LAN-Cell's system DNS server (configured in menu 1) 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 save your changes. 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.
DHCP Server Address	If **Relay** is selected in the **DHCP** field above, then type the IP address of the actual, remote DHCP server here.

Use the instructions in the following table to configure TCP/IP parameters for the LAN port.

LAN and DMZ IP addresses must be on separate subnets.

Table 189 Menu 3.2: LAN TCP/IP Setup Fields

FIELD	DESCRIPTION
TCP/IP Setup:	
IP Address	Enter the IP address of your LAN-Cell in dotted decimal notation
IP Subnet Mask	Your LAN-Cell 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 LAN-Cell.
RIP Direction	Press [SPACE BAR] and then [ENTER] to select the RIP direction. Options are: **Both**, **In Only**, **Out Only** or **None**.
Version	Press [SPACE BAR] and then [ENTER] to select the RIP version. Options are: **RIP-1**, **RIP-2B** or **RIP-2M**.
Multicast	IGMP (Internet Group Multicast Protocol) is a session-layer protocol used to establish membership in a Multicast group. The LAN-Cell supports both IGMP version 1 (**IGMP-v1**) and version 2 (**IGMP-v2**). Press [SPACE BAR] and then [ENTER] to enable IP Multicasting or select **None** (default) to disable it.
Edit IP Alias	The LAN-Cell supports three logical LAN interfaces via its single physical Ethernet interface with the LAN-Cell itself as the gateway for each LAN network. Press [SPACE BAR] to select **Yes** and then press [ENTER] to display menu 3.2.1
When you have completed this menu, press [ENTER] at the prompt [Press ENTER to Confirm…] to save your configuration, or press [ESC] at any time to cancel.	

26.4.1 IP Alias Setup

IP alias allows you to partition a physical network into different logical networks over the same Ethernet interface. The LAN-Cell supports three logical LAN interfaces via its single physical Ethernet interface with the LAN-Cell itself as the gateway for each LAN network.

Use menu 3.2 to configure the first network. Move the cursor to the **Edit IP Alias** field, press [SPACE BAR] to choose **Yes** and press [ENTER] to open **Menu 3.2.1 - IP Alias Setup**, as shown next. Use this menu to configure the second and third networks.

Figure 268 Menu 3.2.1: IP Alias Setup

```
                  Menu 3.2.1 - IP Alias Setup

             IP Alias 1= Yes
               IP Address= 192.168.2.1
               IP Subnet Mask= 255.255.255.0
               RIP Direction= None
                 Version= RIP-1
               Incoming protocol filters=
               Outgoing protocol filters=
             IP Alias 2= No
               IP Address= N/A
               IP Subnet Mask= N/A
               RIP Direction= N/A
                 Version= N/A
               Incoming protocol filters= N/A
               Outgoing protocol filters= N/A


                         Enter here to CONFIRM or ESC to CANCEL:
```

Use the instructions in the following table to configure IP alias parameters.

Table 190 Menu 3.2.1: IP Alias Setup

FIELD	DESCRIPTION
IP Alias 1, 2	Choose **Yes** to configure the LAN network for the LAN-Cell.
IP Address	Enter the IP address of your LAN-Cell in dotted decimal notation.
IP Subnet Mask	Your LAN-Cell 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 LAN-Cell.
RIP Direction	Press [SPACE BAR] and then [ENTER] to select the RIP direction. Options are **Both**, **In Only**, **Out Only** or **None**.
Version	Press [SPACE BAR] and then [ENTER] to select the RIP version. Options are **RIP-1**, **RIP-2B** or **RIP-2M**.
Incoming Protocol Filters	Enter the filter set(s) you wish to apply to the incoming traffic between this node and the LAN-Cell.
Outgoing Protocol Filters	Enter the filter set(s) you wish to apply to the outgoing traffic between this node and the LAN-Cell.
When you have completed this menu, press [ENTER] at the prompt [Press ENTER to Confirm…] to save your configuration, or press [ESC] at any time to cancel.	

27

Ethernet WAN Internet Access

This chapter shows you how to configure your LAN-Cell for Internet access via the Ethernet WAN interface.

27.1 Introduction to Internet Access Setup

Use information from your ISP along with the instructions in this chapter to set up your LAN-Cell to access the Internet. There are three different menu 4 screens depending on whether you chose **Ethernet**, **PPTP** or **PPPoE** Encapsulation. Contact your ISP to determine what encapsulation type you should use.

This menu configures the wired **WAN** interface on the LAN-Cell 2. Configure the CELL interface in **Menu 11.2 - Remote Node Profile** or in the **WIRELESS > CELLULAR** screen via the web configurator.

27.2 Ethernet Encapsulation

If you choose **Ethernet** in menu 4 you will see the next menu.

Figure 269 Menu 4: Internet Access Setup (Ethernet)

```
                         Menu 4 - Ethernet WAN Setup

                    ISP's Name= WAN
                    Encapsulation= Ethernet
                      Service Type= Standard
                      My Login= N/A
                      My Password= N/A
                      Retype to Confirm= N/A
                      Login Server= N/A
                      Relogin Every (min)=  N/A
                    IP Address Assignment= Dynamic
                      IP Address= N/A
                      IP Subnet Mask= N/A
                      Gateway IP Address= N/A
                    Network Address Translation= SUA Only

                    Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this menu.

Table 191 Menu 4: Ethernet WAN Setup (Ethernet)

FIELD	DESCRIPTION
ISP's Name	This is the descriptive name of your ISP for identification purposes.
Encapsulation	Press [SPACE BAR] and then press [ENTER] to choose **Ethernet**. The encapsulation method influences your choices for the **IP Address** field.
Service Type	Press [SPACE BAR] and then [ENTER] to select **Standard**, **RR-Toshiba** (RoadRunner Toshiba authentication method), **RR-Manager** (RoadRunner Manager authentication method), **RR-Telstra** or **Telia Login**. Choose a RoadRunner flavor if your ISP is Time Warner's RoadRunner; otherwise choose **Standard**.
Note: DSL users must choose the **Standard** option only. The **My Login**, **My Password** and **Login Server** fields are not applicable in this case.	
My Login	Enter the login name given to you by your ISP.
My Password	Type your password again for confirmation.
Retype to Confirm	Enter your password again to make sure that you have entered is correctly.
Login Server	The LAN-Cell will find the RoadRunner Server IP if this field is left blank. If it does not, then you must enter the authentication server IP address.
Relogin Every (min)	This field is available when you select **Telia Login** in the **Service Type** field. The Telia server logs the LAN-Cell out if the LAN-Cell does not log in periodically. Type the number of minutes from 1 to 59 (30 recommended) for the LAN-Cell to wait between logins.
IP Address Assignment	If your ISP did not assign you a fixed IP address, press [SPACE BAR] and then [ENTER] to select **Dynamic**, otherwise select **Static** and enter the IP address and subnet mask in the following fields.
IP Address	Enter the (fixed) IP address assigned to you by your ISP (static IP address assignment is selected in the previous field).
IP Subnet Mask	Enter the subnet mask associated with your static IP.

Table 191 Menu 4: Ethernet WAN Setup (Ethernet) (continued)

FIELD	DESCRIPTION
Gateway IP Address	Enter the gateway IP address associated with your static IP.
Network Address Translation	Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network (for example a private IP address used in a local network) to a different IP address known within another network (for example a public IP address used on the Internet). Choose **None** to disable NAT. Choose **SUA Only** if you have a single public IP address. SUA (Single User Account) is a subset of NAT that supports two types of mapping: **Many-to-One** and **Server**. Choose **Full Feature** if you have multiple public IP addresses. **Full Feature** mapping types include: **One-to-One**, **Many-to-One** (SUA/PAT), **Many-to-Many Overload**, **Many- One-to-One** and **Server**. When you select **Full Feature** you must configure at least one address mapping set! Please see Chapter 13 on page 289 for a more detailed discussion on the Network Address Translation feature.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm…" to save your configuration, or press [ESC] at any time to cancel.	

27.3 Configuring the PPTP Client

The LAN-Cell supports only one PPTP server connection at any given time.

To configure a PPTP client, you must configure the **My Login** and **Password** fields for a PPP connection and the PPTP parameters for a PPTP connection.

After configuring **My Login** and **Password** for PPP connection, press [SPACE BAR] and then [ENTER] in the **Encapsulation** field in **Menu 4 -Ethernet WAN Setup** to choose **PPTP** as your encapsulation option. This brings up the following screen.

Figure 270 IEthernet WAN Setup (PPTP)

```
                    Menu 4 - Ethernet WAN Setup

               ISP's Name= WAN
               Encapsulation= PPTP
                 Service Type= N/A
                 My Login=
                 My Password= ********
                 Retype to Confirm= ********
                 Idle Timeout= 100

               IP Address Assignment= Dynamic
                 IP Address= N/A
                 IP Subnet Mask= N/A
                 Gateway IP Address= N/A
               Network Address Translation= SUA Only

               Press ENTER to Confirm or ESC to Cancel:
```

The following table contains instructions about the new fields when you choose **PPTP** in the **Encapsulation** field in menu 4.

Table 192 New Fields in Menu 4 (PPTP) Screen

FIELD	DESCRIPTION
Encapsulation	Press [SPACE BAR] and then press [ENTER] to choose **PPTP**. The encapsulation method influences your choices for the **IP Address** field.
Idle Timeout	This value specifies the time, in seconds, that elapses before the LAN-Cell automatically disconnects from the PPTP server.

27.4 Configuring the PPPoE Client

If you enable PPPoE in menu 4, you will see the next screen.

Figure 271 Ethernet WAN Setup (PPPoE)

```
                    Menu 4 - Ethernet WAN Setup

               ISP's Name= WAN
               Encapsulation= PPPoE
                 Service Type= N/A
                 My Login=
                 My Password= ********
                 Retype to Confirm= ********
                 Idle Timeout= 100

               IP Address Assignment= Dynamic
                 IP Address= N/A
                 IP Subnet Mask= N/A
                 Gateway IP Address= N/A
               Network Address Translation= SUA Only

               Press ENTER to Confirm or ESC to Cancel:
```

The following table contains instructions about the new fields when you choose **PPPoE** in the **Encapsulation** field in menu 4.

Table 193 New Fields in Menu 4 (PPPoE) screen

FIELD	DESCRIPTION
Encapsulation	Press [SPACE BAR] and then press [ENTER] to choose **PPPoE**. The encapsulation method influences your choices in the **IP Address** field.
Idle Timeout	This value specifies the time in seconds that elapses before the LAN-Cell automatically disconnects from the PPPoE server.

If you need a PPPoE service name to identify and reach the PPPoE server, please go to menu 11 and enter the PPPoE service name provided to you in the **Service Name** field.

27.5 Basic Setup Complete

Well done! You have successfully connected, installed and set up your LAN-Cell to operate on your network as well as access the Internet.

When the firewall is activated, the default policy allows all communications to the Internet that originate from the LAN, and blocks all traffic to the LAN that originates from the Internet, except for traffic to the LAN-Cell's remote management ports.

You may deactivate the firewall in menu 21.2 or via the LAN-Cell embedded web configurator. You may also define additional firewall rules or modify existing ones but please exercise extreme caution in doing so. See the chapters on firewall for more information on the firewall.

28

DMZ Setup

This chapter describes how to configure the LAN-Cell's DMZ using **Menu 5 - DMZ Setup**.

28.1 Configuring DMZ Setup

From the main menu, enter 5 to open **Menu 5 – DMZ Setup**.

Figure 272 Menu 5: DMZ Setup

```
Menu 5 - DMZ Setup

1. DMZ Port Filter Setup
2. TCP/IP and DHCP Setup

Enter Menu Selection Number:
```

28.2 DMZ Port Filter Setup

This menu allows you to specify the filter sets that you wish to apply to your public server(s) traffic.

Figure 273 Menu 5.1: DMZ Port Filter Setup

```
Menu 5.1 - DMZ Port Filter Setup

Input Filter Sets:
  protocol filters=
    device filters=
Output Filter Sets:
  protocol filters=
    device filters=

Press ENTER to Confirm or ESC to Cancel:
```

28.3 TCP/IP Setup

For more detailed information about RIP setup, IP Multicast and IP alias, please refer to Chapter 4 on page 77.

28.3.1 IP Address

From the main menu, enter 5 to open **Menu 5 - DMZ Setup** to configure TCP/IP (RFC 1155).

Figure 274 Menu 5: DMZ Setup

```
              Menu 5 - DMZ Setup

              1. DMZ Port Filter Setup
              2. TCP/IP and DHCP Setup

                      Enter Menu Selection Number:
```

From menu 5, select the submenu option **2. TCP/IP and DHCP Setup** and press [ENTER]. The screen now displays **Menu 5.2 - TCP/IP and DHCP Ethernet Setup**, as shown next.

Figure 275 Menu 5.2: TCP/IP and DHCP Ethernet Setup

```
                       Menu 5.2 - TCP/IP and DHCP Ethernet Setup


        DHCP= None                             TCP/IP Setup:
        Client IP Pool:
          Starting Address= N/A                IP Address= 10.10.2.1
          Size of Client IP Pool= N/A         IP Subnet Mask= 255.255.255.0
                                               RIP Direction= None
                                                 Version= N/A
                                               Multicast= IGMP-v2
                                               Edit IP Alias= No


        DHCP Server Address= N/A


                       Press ENTER to Confirm or ESC to Cancel:
```

The DHCP and TCP/IP setup fields are the same as the ones in **Menu 3.2 - TCP/IP and DHCP Ethernet Setup**. Each public server will need a unique IP address. Refer to Section 26.4 on page 442 for information on how to configure these fields.

DMZ, WLAN and LAN IP addresses must be on separate subnets. You must also configure NAT for the DMZ port (see Chapter 33 on page 477) in menus 15.1 and 15.2.

28.3.2 IP Alias Setup

Use menu 5.2 to configure the first network. Move the cursor to the **Edit IP Alias** field, press [SPACE BAR] to choose **Yes** and press [ENTER] to open **Menu 5.2.1 - IP Alias Setup**, as shown next. Use this menu to configure the second and third networks.

Figure 276 Menu 5.2.1: IP Alias Setup

```
              Menu 5.2.1 - IP Alias Setup

              IP Alias 1= No
                IP Address= N/A
                IP Subnet Mask= N/A
                RIP Direction= N/A
                  Version= N/A
                Incoming protocol filters= N/A
                Outgoing protocol filters= N/A
              IP Alias 2= No
                IP Address= N/A
                IP Subnet Mask= N/A
                RIP Direction= N/A
                  Version= N/A
                Incoming protocol filters= N/A
                Outgoing protocol filters= N/A

              Enter here to CONFIRM or ESC to CANCEL:
```

Refer to Table 190 on page 445 for instructions on configuring IP alias parameters.

29

Route Setup

This chapter describes how to configure the LAN-Cell's WAN Connectivity and Traffic Redirect features.

29.1 Configuring Route Setup

From the main menu, enter 6 to open **Menu 6 - Route Setup**.

Figure 277 Menu 6: Route Setup

```
              Menu 6 - Route Setup

             1. Route Assessment
             2. Traffic Redirect
             3. Route Failover


                   Enter Menu Selection Number:
```

29.2 Route Assessment

This menu allows you to configure the Ping Contintity properties.

Figure 278 Menu 6.1: Route Assessment

```
             Menu 6.1 - Route Assessment


             Probing WAN Check Point= Yes
               Use Default Gateway as Check Point= Yes
               Check Point= N/A
             Probing CELL Check Point= Yes
               Use Default Gateway as Check Point= Yes
               Check Point= N/A
             Probing Traffic Redirection Check Point= No
               Use Default Gateway as Check Point= N/A
               Check Point= N/A


             Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this menu.

Table 194 Menu 6.1: Route Assessment

FIELD	DESCRIPTION
Probing WAN/CELL Check Point	Press [SPACE BAR] and then press [ENTER] to choose **Yes** to test your LAN-Cell's WAN accessibility. If you do not select **No** in the **Use Default Gateway as Check Point** field and enter a domain name or IP address of a reliable nearby computer (for example, your ISP's DNS server address) in the **Check Point** field, the LAN-Cell will use the default gateway IP address.
Probing Traffic Redirection Check Point	Press [SPACE BAR] and then press [ENTER] to choose **Yes** to test your LAN-Cell's traffic redirect connection. If you do not select **No** in the **Use Default Gateway as Check Point** field and enter a domain name or IP address of a reliable nearby computer (for example, your ISP's DNS server address) in the **Check Point** field, the LAN-Cell will use the default gateway IP address.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm…" to save your configuration, or press [ESC] at any time to cancel.	

29.3 Traffic Redirect

To configure the parameters for traffic redirect, enter **2** in **Menu 6 - Route Setup** to open **Menu 6.2 - Traffic Redirect** as shown next.

Figure 279 Menu 6.2: Traffic Redirect

```
               Menu 6.2 - Traffic Redirect

              Active= No
              Configuration:
                Backup Gateway IP Address= 0.0.0.0
                Metric= 14



              Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this menu.

Table 195 Menu 6.2: Traffic Redirect

FIELD	DESCRIPTION
Active	Press [SPACE BAR] and select Yes (to enable) or No (to disable) traffic redirect setup. The default is No.
Backup Gateway IP Address	Enter the IP address of your backup gateway in dotted decimal notation. The LAN-Cell automatically forwards traffic to this IP address if the LAN-Cell's Internet connection terminates.
Metric	This field sets this route's priority among the routes the LAN-Cell uses. Enter a number from 1 to 15 to set this route's priority among the LAN-Cell's routes (see Section on page 92) The smaller the number, the higher priority the route has.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm…" to save your configuration, or press [ESC] at any time to cancel.	

29.4 Route Failover

This menu allows you to configure how the LAN-Cell uses the route assessment ping Connectivity check function.

Figure 280 Menu 6.3: Route Failover

```
                 Menu 6.3 - Route Failover

                 Period= 5
                 Timeout=: 3
                 Fail Tolerance= 3


                 Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this menu.

Table 196 Menu 6.3: Route Failover

FIELD	DESCRIPTION
Period	Type the number of seconds for the LAN-Cell to wait between checks to see if it can connect to the WAN IP address (in the **Check Point** field of menu 6.1) or the default gateway. Allow more time if your destination IP address handles lots of traffic.
Timeout	Type the number of seconds for your LAN-Cell to wait for a ping response from the IP address in the **Check Point** field of menu 6.1 before it times out. The WAN connection is considered "down" after the LAN-Cell 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.
Fail Tolerance	Type the number of times your LAN-Cell may attempt and fail to connect to the Internet before traffic is forwarded to the backup gateway.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm…" to save your configuration, or press [ESC] at any time to cancel.	

30

WLAN Setup

Use menu 7 to configure the IP address for LAN-Cell's WLAN interface, other TCP/IP and DHCP settings.

30.1 TCP/IP Setup

For more detailed information about RIP setup, IP Multicast and IP alias, please refer to Chapter 4 on page 77.

30.1.1 IP Address

From the main menu, enter 7 to open **Menu 7 - WLAN Setup** to configure TCP/IP (RFC 1155).

Figure 281 Menu 7: WLAN Setup

```
                  Menu 7 - WLAN Setup


              2. TCP/IP and DHCP Setup

               Enter Menu Selection Number:
```

From menu 7, select the submenu option **2. TCP/IP and DHCP Setup** and press [ENTER]. The screen now displays **Menu 7.2 - TCP/IP and DHCP Ethernet Setup**, as shown next.

Figure 282 Menu 7.2: TCP/IP and DHCP Ethernet Setup

```
                 Menu 7.2 - TCP/IP and DHCP Ethernet Setup


        DHCP= None                             TCP/IP Setup:
        Client IP Pool:
          Starting Address= N/A                IP Address= 0.0.0.0
          Size of Client IP Pool= N/A          IP Subnet Mask= 0.0.0.0
                                               RIP Direction= None
                                                 Version= N/A
                                               Multicast= IGMP-v2
                                               Edit IP Alias= No


        DHCP Server Address= N/A



                       Press ENTER to Confirm or ESC to Cancel:
```

The DHCP and TCP/IP setup fields are the same as the ones in **Menu 3.2 - TCP/IP and DHCP Ethernet Setup**. Each public server will need a unique IP address. Refer to Section 26.4 on page 442 for information on how to configure these fields.

DMZ, WLAN and LAN IP addresses must be on separate subnets. You must also configure NAT for the WLAN port (see Chapter 33 on page 477) in menus 15.1 and 15.2.

30.1.2 IP Alias Setup

You must use menu 7.2 to configure the first network. Move the cursor to the **Edit IP Alias** field, press [SPACE BAR] to choose **Yes** and press [ENTER] to configure the second and third network.

Pressing [ENTER] opens **Menu 7.2.1 - IP Alias Setup**, as shown next.

Figure 283 Menu 7.2.1: IP Alias Setup

```
                    Menu 7.2.1 - IP Alias Setup

                       IP Alias 1= No
                         IP Address= N/A
                         IP Subnet Mask= N/A
                         RIP Direction= N/A
                           Version= N/A


                       IP Alias 2= No
                         IP Address= N/A
                         IP Subnet Mask= N/A
                         RIP Direction= N/A
                           Version= N/A


               Enter here to CONFIRM or ESC to CANCEL:
```

Refer to Table 190 on page 445 for instructions on configuring IP alias parameters.

31

WAN ISP Setup

This chapter shows you how to configure a remote node to access an ISP via a WAN interface.

31.1 Introduction to WAN ISP Setup

A remote node is required for placing calls to an ISP's remote gateway. A remote node represents both the remote gateway and the network behind it across a WAN connection. Note that when you use menu 4 to set up WAN ISP access, you are actually configuring a remote node. The following describes how to configure **Menu 11.1 - Remote Node Profile**, **Menu 11.1.2 - Remote Node Network Layer Options** and **Menu 11.1.4 - Remote Node Filter**.

31.2 Remote Node Setup

From the main menu, select menu option 11 to open **Menu 11 - WAN ISP Setup** (shown below).

Enter **1** to open **Menu 11.1 - Remote Node Profile** and configure the setup for your Ethernet WAN port. Enter **2** to open **Menu 11.2 - Remote Node Profile (Cellular 3G WAN)** and configure the setup for your 3G connection. Enter **3** to open **Menu 11.3 Remote Node Profile (Backup ISP)** and configure the setup for your Dial Backup port connection (see Chapter 25 on page 427).

Figure 284 Menu 11: WAN ISP Setup

```
              Menu 11 - WAN ISP Setup

              1. WAN (ISP, SUA)
              2. CELLULAR(ISP, SUA)
              3. -Dial (BACKUP_ISP, SUA)



              Enter Node # to Edit:
```

31.3 Remote Node Profile Setup

The following explains how to configure the remote node profile menu.

31.3.1 Ethernet Encapsulation

There are three variations of menu 11.1 depending on whether you choose **Ethernet Encapsulation**, **PPPoE Encapsulation** or **PPTP Encapsulation**. You must choose the **Ethernet** option when the WAN port is used as a regular Ethernet. The first menu 11.1 screen you see is for Ethernet encapsulation shown next.

Figure 285 Menu 11.1: Remote Node Profile for Ethernet Encapsulation

```
                      Menu 11.1 - Remote Node Profile

             Rem Node Name= WAN                Route= IP
             Active= Yes

             Encapsulation= Ethernet             Edit IP= No
             Service Type= Standard              Session Options:
                                                   Schedules=
             Outgoing:                             Edit Filter Sets= No
               My Login= N/A
               My Password= N/A
               Retype to Confirm= N/A
               Server= N/A
               Relogin Every (min)=  N/A


             Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this menu.

Table 197 Menu 11.1: Remote Node Profile for Ethernet Encapsulation

FIELD	DESCRIPTION
Rem Node Name	Enter a descriptive name for the remote node. This field can be up to eight characters.
Active	Press [SPACE BAR] and then [ENTER] to select **Yes** (activate remote node) or **No** (deactivate remote node).
Encapsulation	**Ethernet** is the default encapsulation. Press [SPACE BAR] and then [ENTER] to change to **PPPoE** or **PPTP** encapsulation.
Service Type	Press [SPACE BAR] and then [ENTER] to select from **Standard**, **RR-Toshiba** (RoadRunner Toshiba authentication method), **RR-Manager** (RoadRunner Manager authentication method), **RR-Telstra** or **Telia Login**. Choose one of the RoadRunner methods if your ISP is Time Warner's RoadRunner; otherwise choose **Standard**.
Outgoing	
My Login	This field is applicable for **PPPoE** encapsulation only. Enter the login name assigned by your ISP when the LAN-Cell calls this remote node. Some ISPs append this field to the **Service Name** field above (e.g., jim@poellc) to access the PPPoE server.
My Password	Enter the password assigned by your ISP when the LAN-Cell calls this remote node. Valid for **PPPoE** encapsulation only.
Retype to Confirm	Type your password again to make sure that you have entered it correctly.

Table 197 Menu 11.1: Remote Node Profile for Ethernet Encapsulation (continued)

FIELD	DESCRIPTION
Server	This field is valid only when **RoadRunner** is selected in the **Service Type** field. The LAN-Cell will find the RoadRunner Server IP automatically if this field is left blank. If it does not, then you must enter the authentication server IP address here.
Relogin Every (min)	This field is available when you select **Telia Login** in the **Service Type** field. The Telia server logs the LAN-Cell out if the LAN-Cell does not log in periodically. Type the number of minutes from 1 to 59 (30 recommended) for the LAN-Cell to wait between logins.
Route	This field refers to the protocol that will be routed by your LAN-Cell – IP is the only option for the LAN-Cell.
Edit IP	This field leads to a “hidden” menu. Press [SPACE BAR] to select **Yes** and press [ENTER] to go to **Menu 11.1.2 - Remote Node Network Layer Options**.
Session Options	
Schedules	You can apply up to four schedule sets here. For more details please refer to Chapter 42 on page 563.
Edit Filter Sets	This field leads to another “hidden” menu. Use [SPACE BAR] to select **Yes** and press [ENTER] to open menu 11.1.4 to edit the filter sets. See Section 31.5 on page 471 for more details.
Once you have configured this menu, press [ENTER] at the message “Press ENTER to Confirm...” to save your configuration, or press [ESC] at any time to cancel.	

31.3.2 PPPoE Encapsulation

The LAN-Cell supports PPPoE (Point-to-Point Protocol over Ethernet). You can only use PPPoE encapsulation when you’re using the LAN-Cell with a DSL modem as the WAN device. If you change the Encapsulation to **PPPoE,** then you will see the next screen.

Figure 286 Menu 11.1: Remote Node Profile for PPPoE Encapsulation

```
                  Menu 11.1 - Remote Node Profile

      Rem Node Name= ChangeMe                Route= IP
      Active= Yes

      Encapsulation= PPPoE                   Edit IP= No
      Service Type= Standard                 Telco Option:
      Service Name=                            Allocated Budget(min)= 0
      Outgoing:                                Period(hr)= 0
        My Login=                              Schedules=
        My Password= ********                  Always On Connection= No
        Retype to Confirm= ********
        Authen= CHAP/PAP
                                               Session Options:
                                               Edit Filter Sets= No
                                               Idle Timeout(sec)= 100


                          Press ENTER to Confirm or ESC to Cancel:
```

31.3.2.1 Outgoing Authentication Protocol

Generally speaking, you should employ the strongest authentication protocol possible, for obvious reasons. However, some vendor's implementation includes a specific authentication protocol in the user profile. It will disconnect if the negotiated protocol is different from that in the user profile, even when the negotiated protocol is stronger than specified. If you encounter a case where the peer disconnects right after a successful authentication, please make sure that you specify the correct authentication protocol when connecting to such an implementation.

31.3.2.2 Always-On Connection

An Always-On (nailed-up) connection is a dial-up line where the connection is always up regardless of traffic demand. The LAN-Cell does two things when you specify an always-on connection. The first is that idle timeout is disabled. The second is that the LAN-Cell will try to bring up the connection when turned on and whenever the connection is down. An always-on connection can be very expensive for obvious reasons.

Do not specify an always-on connection unless your telephone company offers flat-rate service or you need a constant connection and the cost is of no concern.

The following table describes the fields not already described in Table 197 on page 466.

31.3.2.3 Metric

See Section on page 92 for details on the **Metric** field.

Table 198 Fields in Menu 11.1 (PPPoE Encapsulation Specific)

FIELD	DESCRIPTION
Service Name	If you are using **PPPoE** encapsulation, then type the name of your PPPoE service here. Only valid with **PPPoE** encapsulation.
Authen	This field sets the authentication protocol used for outgoing calls. Options for this field are: **CHAP**/**PAP** - Your LAN-Cell will accept either **CHAP** or **PAP** when requested by this remote node. **CHAP** - accept CHAP only. **PAP** - accept PAP only.
Telco Option	
Allocated Budget	The field sets a ceiling for outgoing call time for this remote node. The default for this field is 0 meaning no budget control.
Period(hr)	This field is the time period that the budget should be reset. For example, if we are allowed to call this remote node for a maximum of 10 minutes every hour, then the **Allocated Budget** is (10 minutes) and the **Period(hr)** is 1 (hour).
Schedules	You can apply up to four schedule sets here. For more details please refer to Chapter 42 on page 563.
Always On Connection	This field specifies if you want to make the connection to this remote node an always-on connection. More details are given earlier in this section.
Session Options	
Idle Timeout	Type the length of idle time (when there is no traffic from the LAN-Cell to the remote node) in seconds that can elapse before the LAN-Cell automatically disconnects the PPPoE connection. This option only applies when the LAN-Cell initiates the call.

31.3.3 PPTP Encapsulation

If you change the Encapsulation to **PPTP** in menu 11.1, then you will see the next screen.

Figure 287 Menu 11.1: Remote Node Profile for PPTP Encapsulation

```
                   Menu 11.1 - Remote Node Profile

      Rem Node Name= ChangeMe               Route= IP
      Active= Yes

      Encapsulation= PPTP                   Edit IP= No
      Service Type= Standard                Telco Option:
                                              Allocated Budget(min)= 0
      Outgoing:                               Period(hr)= 0
        My Login=                             Schedules=
        My Password= ********                 Always On Connection= No
        Retype to Confirm= ********
        Authen= CHAP/PAP
      PPTP:                                 Session Options:
        My IP Addr= 10.0.0.140                Edit Filter Sets= No
        My IP Mask= 255.255.255.0             Idle Timeout(sec)= 100
        Server IP Addr= 10.0.0.138
        Connection ID/Name=

                           Press ENTER to Confirm or ESC to Cancel:
```

The next table shows how to configure fields in menu 11.1 not previously discussed.

Table 199 Menu 11.1: Remote Node Profile for PPTP Encapsulation

FIELD	DESCRIPTION
Encapsulation	Press [SPACE BAR] and then [ENTER] to select **PPTP**. You must also go to menu 11.3 to check the IP Address setting once you have selected the encapsulation method.
My IP Addr	Enter the IP address of the WAN Ethernet port.
My IP Mask	Enter the subnet mask of the WAN Ethernet port.
Server IP Addr	Enter the IP address of the ANT modem.
Connection ID/ Name	Enter the connection ID or connection name in the ANT. It must follow the “c:id” and “n:name” format. This field is optional and depends on the requirements of your DSL modem.
Schedules	You can apply up to four schedule sets here. For more details refer to Chapter 42 on page 563.
Always On Connections	Press [SPACE BAR] and then [ENTER] to select **Yes** if you want to make the connection to this remote node an always-on connection.

31.4 Edit IP

Move the cursor to the **Edit IP** field in menu 11.1, then press [SPACE BAR] to select **Yes**. Press [ENTER] to open **Menu 11.1.2 - Remote Node Network Layer Options**. Not all fields are available on all models.

Figure 288 Menu 11.1.2: Remote Node Network Layer Options for Ethernet Encapsulation

```
               Menu 11.1.2 - Remote Node Network Layer Options

                 IP Address Assignment= Dynamic
                 Rem IP Addr= N/A
                 Rem Subnet Mask= N/A
                 My WAN Addr= N/A

                 Network Address Translation= SUA Only
                 NAT Lookup Set= 255
                 Metric= 1
                 Private= No
                 RIP Direction= None
                   Version= N/A
                 Multicast= None

                  Enter here to CONFIRM or ESC to CANCEL:
```

This menu displays the **My WAN Addr** field for **PPPoE** and **PPTP** encapsulations and **Gateway IP Addr** field for **Ethernet** encapsulation. The following table describes the fields in this menu.

Table 200 Remote Node Network Layer Options Menu Fields

FIELD	DESCRIPTION
IP Address Assignment	If your ISP did not assign you an explicit IP address, press [SPACE BAR] and then [ENTER] to select **Dynamic**; otherwise select **Static** and enter the IP address & subnet mask in the following fields.
(Rem) IP Address	If you have a static IP Assignment, enter the IP address assigned to you by your ISP.
(Rem) IP Subnet Mask	If you have a static IP Assignment, enter the subnet mask assigned to you.
Gateway IP Addr	This field is applicable to **Ethernet** encapsulation only. Enter the gateway IP address assigned to you if you are using a static IP address.
My WAN Addr	This field is applicable to **PPPoE** and **PPTP** encapsulations only. Some implementations, especially the UNIX derivatives, require the WAN link to have a separate IP network number from the LAN and each end must have a unique address within the WAN network number. If this is the case, enter the IP address assigned to the WAN port of your LAN-Cell. Note that this is the address assigned to your local LAN-Cell, not the remote router.
Network Address Translation	Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network (for example a private IP address used in a local network) to a different IP address known within another network (for example a public IP address used on the Internet). Choose **None** to disable NAT. Choose **SUA Only** if you have a single public IP address. SUA (Single User Account) is a subset of NAT that supports two types of mapping: **Many-to-One** and **Server**. Choose **Full Feature** if you have multiple public IP addresses. **Full Feature** mapping types include: **One-to-One**, **Many-to-One** (SUA/PAT), **Many-to-Many Overload**, **Many- One-to-One** and **Server**. When you select **Full Feature** you must configure at least one address mapping set. See Chapter 13 on page 289 for a full discussion on this feature.

Table 200 Remote Node Network Layer Options Menu Fields (continued)

FIELD	DESCRIPTION
NAT Lookup Set	If you select **SUA Only** in the **Network Address Translation** field, it displays **255** and indicates the SMT will use the pre-configured **Set 255** (read only) in menu 15.1. If you select **Full Feature** or **None** in the **Network Address Translation** field, it displays **1**, **2** or **3** and indicates the SMT will use the pre-configured **Set 1** in menu 15.1 for the first WAN port, **Set 2** in menu 15.1 for the second WAN port and **Set 3** for the Backup port. Refer to Section 33.2 on page 479 for more information.
Metric	Enter a number from 1 to 15 to set this route's priority among the LAN-Cell's routes (see Section on page 92). The smaller the number, the higher priority the route has.
Private	This field is valid only for PPTP/PPPoE encapsulation. This parameter determines if the LAN-Cell 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	Press [SPACE BAR] and then [ENTER] to select the RIP direction from **Both**/ **None**/**In Only**/**Out Only**. See Chapter 4 on page 77 for more information on RIP. The default for RIP on the WAN side is **None**. It is recommended that you do not change this setting.
Version	Press [SPACE BAR] and then [ENTER] to select the RIP version from **RIP-1**/**RIP-2B**/ **RIP-2M** or **None**.
Multicast	IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group. The LAN-Cell supports both IGMP version 1 (**IGMP-v1**) and version 2 (**IGMP-v2)**. Press [SPACE BAR] to enable IP Multicasting or select **None** to disable it. See Chapter 4 on page 77 for more information on this feature.
Once you have completed filling in **Menu 11.3 Remote Node Network Layer Options**, press [ENTER] at the message "Press ENTER to Confirm..." to save your configuration and return to menu 11, or press [ESC] at any time to cancel.	

31.5 Remote Node Filter

Move the cursor to the field **Edit Filter Sets** in menu 11.1, and then press [SPACE BAR] to set the value to **Yes**. Press [ENTER] to open **Menu 11.1.4 - Remote Node Filter**.

Use menu 11.1.4 to specify the filter set(s) to apply to the incoming and outgoing traffic between this remote node and the LAN-Cell to prevent certain packets from triggering calls. You can specify up to 4 filter sets separated by commas, for example, 1, 5, 9, 12, in each filter field. Note that spaces are accepted in this field. For more information on defining the filters, please refer to Chapter 35 on page 499. For PPPoE or PPTP encapsulation, you have the additional option of specifying remote node call filter sets.

Figure 289 Menu 11.1.4: Remote Node Filter (Ethernet Encapsulation)

```
              Menu 11.1.4 - Remote Node Filter

              Input Filter Sets:
                protocol filters=
                  device filters=
              Output Filter Sets:
                protocol filters=
                  device filters=

              Enter here to CONFIRM or ESC to CANCEL:
```

Figure 290 Menu 11.1.4: Remote Node Filter (PPPoE or PPTP Encapsulation)

```
              Menu 11.1.4 - Remote Node Filter

              Input Filter Sets:
                protocol filters=
                  device filters=
              Output Filter Sets:
                protocol filters=
                  device filters=
              Call Filter Sets:
                protocol filters=
                  device filters=


              Enter here to CONFIRM or ESC to CANCEL:
```

32

IP Static Route Setup

This chapter shows you how to configure static routes with your LAN-Cell.

32.1 IP Static Route Setup

Enter 12 from the main menu. Select one of the IP static routes as shown next to configure IP static routes in menu 12.1.

The first two static route entries are for default WAN and CELL routes. You cannot modify or delete a static default route.
The default route is disabled after you change the static WAN IP address to a dynamic WAN IP address.

The “-” before a route name indicates the static route is inactive.

Figure 291 Menu 12: IP Static Route Setup

```
               Menu 12 - IP Static Route Setup

              1.Reserved          16.________
              2.Reserved          17.________
              3.________          18.________
              4.________          19.________
              5.________          20.________
              6.________          21.________
              7.________          22.________
              8.________          23.________
              9.________          24.________
              10.________         25.________
              11.________         26.________
              12.________         27.________
              13.________         28.________
              14.________         29.________
              15.________         30.________

                  Enter selection number:
```

Now, enter the index number of the static route that you want to configure.

Figure 292 Menu 12. 1: Edit IP Static Route

```
              Menu 12.1 - Edit IP Static Route

              Route #: 3
              Route Name= ?
              Active= No
              Destination IP Address= ?
              IP Subnet Mask= ?
              Gateway IP Address= ?
              Metric= 2
              Private= No


              Press ENTER to CONFIRM or ESC to CANCEL:
```

`The following table describes the IP Static Route Menu fields.

Table 201 Menu 12. 1: Edit IP Static Route

FIELD	DESCRIPTION
Route #	This is the index number of the static route that you chose in menu 12.
Route Name	Enter a descriptive name for this route. This is for identification purposes only.
Active	This field allows you to activate/deactivate this static route.
Destination IP Address	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.

Table 201 Menu 12. 1: Edit IP Static Route

FIELD	DESCRIPTION
IP Subnet Mask	Enter the IP subnet mask for this destination.
Gateway IP Address	Enter the IP address of the gateway. The gateway is an immediate neighbor of your LAN-Cell that will forward the packet to the destination. On the LAN, the gateway must be a router on the same segment as your LAN-Cell; over the WAN, the gateway must be the IP address of one of the remote nodes.
Metric	Enter a number from 1 to 15 to set this route's priority among the LAN-Cell's routes (see Section on page 92). The smaller the number, the higher priority the route has.
Private	This parameter determines if the LAN-Cell 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.
Once you have completed filling in this menu, press [ENTER] at the message "Press ENTER to Confirm…" to save your configuration, or press [ESC] to cancel.	

33

Network Address Translation (NAT)

This chapter discusses how to configure NAT on the LAN-Cell.

33.1 Using NAT

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

33.1.1 SUA (Single User Account) Versus NAT

SUA (Single User Account) is a ProxiOS implementation of a subset of NAT that supports two types of mapping, **Many-to-One** and **Server**. See Section 33.2.1 on page 480 for a detailed description of the NAT set for SUA. The LAN-Cell also supports **Full Feature** NAT to map multiple global IP addresses to multiple private LAN IP addresses of clients or servers using mapping types.

Choose **SUA Only** if you have just one public WAN IP address for your LAN-Cell.
Choose **Full Feature** if you have multiple public WAN IP addresses for your LAN-Cell.

33.1.2 Applying NAT

You apply NAT via menu 4 or 11.1.2 as displayed next. The next figure shows you how to apply NAT for Internet access in menu 4. Enter 4 from the main menu to go to **Menu 4 - Ethernet WAN Setup**.

Figure 293 Menu 4: Applying NAT for Internet Access

```
              Menu 4 - Ethernet WAN Setup

              ISP's Name= ChangeMe
              Encapsulation= Ethernet
                Service Type= Standard
                My Login= N/A
                My Password= N/A
                Retype to Confirm= N/A
                Login Server= N/A
                Relogin Every (min)=  N/A
              IP Address Assignment= Dynamic
                IP Address= N/A
                IP Subnet Mask= N/A
                Gateway IP Address= N/A
              Network Address Translation= SUA Only


              Press ENTER to Confirm or ESC to Cancel:
```

The following figure shows how you apply NAT to the remote node in menu 11.1.

1 Enter 11 from the main menu.
2 Enter 1 to open **Menu 11.1 - Remote Node Profile**.
3 Move the cursor to the **Edit IP** field, press [SPACE BAR] to select **Yes** and then press [ENTER] to bring up **Menu 11.1.2 - Remote Node Network Layer Options**.

Figure 294 Menu 11.1.2: Applying NAT to the Remote Node

```
              Menu 11.1.2 - Remote Node Network Layer Options

              IP Address Assignment= Dynamic
              IP Address= N/A
              IP Subnet Mask= N/A
              Gateway IP Addr= N/A

              Network Address Translation= Full Feature
              NAT Lookup Set= 1
              Metric= 1
              Private= N/A
              RIP Direction= None
                Version= N/A
              Multicast= None


              Enter here to CONFIRM or ESC to CANCEL:
```

The following table describes the fields in this menu.

Table 202 Applying NAT in Menus 4 & 11.1.2

FIELD	DESCRIPTION	OPTIONS
Network Address Translation	When you select this option the SMT will use Address Mapping Set 1 (menu 15.1 - see Section 33.2.1 on page 480 for further discussion). You can configure any of the mapping types described in Chapter 13 on page 289. Choose **Full Feature** if you have multiple public WAN IP addresses for your LAN-Cell. When you select **Full Feature** you must configure at least one address mapping set.	Full Feature
	NAT is disabled when you select this option.	None
	When you select this option the SMT will use Address Mapping Set 255 (menu 15.1 - see Section 33.2.1 on page 480). Choose **SUA Only** if you have just one public WAN IP address for your LAN-Cell.	SUA Only

33.2 NAT Setup

Use the address mapping sets menus and submenus to create the mapping table used to assign global addresses to computers on the LAN, DMZ and WLAN. **Set 255** is used for SUA. When you select **Full Feature** in menu 4, menu 11.1.2 or menu 11.2.2, the SMT will use **Set 1** for the first WAN port and **Set 2** for the second WAN port. When you select **SUA Only**, the SMT will use the pre-configured **Set 255** (read only).

The server set is a list of LAN, DMZ and WLAN servers mapped to external ports. To use this set, a server rule must be set up inside the NAT address mapping set. Please see the section on port forwarding in Chapter 13 on page 289 for further information on these menus. To configure NAT, enter 15 from the main menu to bring up the following screen.

On the LAN-Cell, you can configure port forwarding and trigger port rules for the Ethernet WAN interface and separate sets of rules for the Cellular WAN interface.

Figure 295 Menu 15: NAT Setup

```
                        Menu 15 - NAT Setup

                            1. Address Mapping Sets
                            2. Port Forwarding Setup
                            3. Trigger Port Setup



                  Enter Menu Selection Number:
```

Configure DMZ, WLAN and LAN IP addresses in NAT menus 15.1 and 15.2. DMZ, WLAN and LAN IP addresses must be on separate subnets.

33.2.1 Address Mapping Sets

Enter 1 to bring up **Menu 15.1 - Address Mapping Sets**.

Figure 296 Menu 15.1: Address Mapping Sets

```
              Menu 15.1 - Address Mapping Sets

                      1. NAT_SET
                      2. example
                    255. SUA (read only)




              Enter Menu Selection Number:
```

33.2.1.1 SUA Address Mapping Set

Enter 255 to display the next screen (see also Section 33.1.1 on page 477). The fields in this menu cannot be changed.

Figure 297 Menu 15.1.255: SUA Address Mapping Rules

```
           Menu 15.1.255 - Address Mapping Rules

Set Name= SUA

Idx  Local Start IP   Local End IP     Global Start IP  Global End IP    Type
---  ---------------  ---------------  ---------------  ---------------  ---
1.   0.0.0.0          255.255.255.255  0.0.0.0                           M-1
2.                                    0.0.0.0                        Server
3.
4.
5.
6.
7.
8.
9.
10.

       Press ENTER to Confirm or ESC to Cancel:
```

The following table explains the fields in this menu.

Menu 15.1.255 is read-only.

Table 203 SUA Address Mapping Rules

FIELD	DESCRIPTION
Set Name	This is the name of the set you selected in menu 15.1 or enter the name of a new set you want to create.
Idx	This is the index or rule number.
Local Start IP	**Local Start IP** is the starting local IP address (ILA).
Local End IP	**Local End IP** is the ending local IP address (ILA). If the rule is for all local IPs, then the start IP is 0.0.0.0 and the end IP is 255.255.255.255.
Global Start IP	This is the starting global IP address (IGA). If you have a dynamic IP, enter 0.0.0.0 as the **Global Start IP**.
Global End IP	This is the ending global IP address (IGA).
Type	These are the mapping types discussed above. **Server** allows us to specify multiple servers of different types behind NAT to this machine. See later for some examples.
Once you have finished configuring a rule in this menu, press [ENTER] at the message “Press ENTER to Confirm…” to save your configuration, or press [ESC] to cancel.	

33.2.1.2 User-Defined Address Mapping Sets

Now look at option 1 in menu 15.1. Enter 1 to bring up this menu. Look at the differences from the previous menu. Note the extra **Action** and **Select Rule** fields mean you can configure rules in this screen. Note also that the [?] in the **Set Name** field means that this is a required field and you must enter a name for the set.

The entire set will be deleted if you leave the **Set Name** field blank and press [ENTER] at the bottom of the screen.

Figure 298 Menu 15.1.1: First Set

```
                    Menu 15.1.1 - Address Mapping Rules

  Set Name= NAT_SET

 Idx  Local Start IP   Local End IP     Global Start IP  Global End IP    Type
 ---  ---------------  ---------------  ---------------  ---------------  --
  1.  0.0.0.0          255.255.255.255  0.0.0.0                          M-1
  2.                                    0.0.0.0                        Server
  3.
  4.
  5.
  6.
  7.
  8.
  9.
 10.

                    Action= None          Select Rule= N/A

                    Press ENTER to Confirm or ESC to Cancel:
```

The Type, Local and Global Start/End IPs are configured in menu 15.1.1.1 (described later) and the values are displayed here.

33.2.1.3 Ordering Your Rules

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

Now if you delete rule 4, rules 5 to 7 will be pushed up by 1 rule, so as old rule 5 becomes rule 4, old rule 6 becomes rule 5 and old rule 7 becomes rule 6.

Table 204 Fields in Menu 15.1.1

FIELD	DESCRIPTION
Set Name	Enter a name for this set of rules. This is a required field. If this field is left blank, the entire set will be deleted.

Table 204 Fields in Menu 15.1.1 (continued)

FIELD	DESCRIPTION
Action	The default is **Edit**. **Edit** means you want to edit a selected rule (see following field). **Insert Before** means to insert a rule before the rule selected. The rules after the selected rule will then be moved down by one rule. **Delete** means to delete the selected rule and then all the rules after the selected one will be advanced one rule. **None** disables the **Select Rule** item.
Select Rule	When you choose **Edit**, **Insert Before** or **Delete** in the previous field the cursor jumps to this field to allow you to select the rule to apply the action in question.

You must press [ENTER] at the bottom of the screen to save the whole set. You must do this again if you make any changes to the set – including deleting a rule. No changes to the set take place until this action is taken.

Selecting **Edit** in the **Action** field and then selecting a rule brings up the following menu, **Menu 15.1.1.1 - Address Mapping Rule** in which you can edit an individual rule and configure the **Type**, **Local** and **Global Start/End IPs**.

An IP End address must be numerically greater than its corresponding IP Start address.

Figure 299 Menu 15.1.1.1: Editing/Configuring an Individual Rule in a Set

```
              Menu 15.1.1.1 Address Mapping Rule

                   Type= One-to-One

                   Local IP:
                     Start=
                     End  = N/A

                   Global IP:
                     Start=
                     End  = N/A

                   Server Mapping Set= N/A


              Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this menu.

Table 205 Menu 15.1.1.1: Editing/Configuring an Individual Rule in a Set

FIELD	DESCRIPTION
Type	Press [SPACE BAR] and then [ENTER] to select from a total of five types. These are the mapping types discussed in Chapter 13 on page 289. **Server** allows you to specify multiple servers of different types behind NAT to this computer. See Section 33.4.3 on page 489 for an example.
Local IP	Only local IP fields are **N/A** for server; Global IP fields MUST be set for **Server**.
Start	Enter the starting local IP address (ILA).
End	Enter the ending local IP address (ILA). If the rule is for all local IPs, then put the Start IP as 0.0.0.0 and the End IP as 255.255.255.255. This field is **N/A** for One-to-One and Server types.
Global IP	
Start	Enter the starting global IP address (IGA). If you have a dynamic IP, enter 0.0.0.0 as the **Global IP Start**. Note that **Global IP Start** can be set to 0.0.0.0 only if the types are **Many-to-One** or **Server**.
End	Enter the ending global IP address (IGA). This field is **N/A** for **One-to-One**, **Many-to-One** and **Server types**.
Server Mapping Set	This field is available only when you select **Server** in the **Type** field.
Once you have finished configuring a rule in this menu, press [ENTER] at the message "Press ENTER to Confirm…" to save your configuration, or press [ESC] to cancel.	

33.3 Configuring a Server behind NAT

Follow these steps to configure a server behind NAT:

1. Enter 15 in the main menu to go to **Menu 15 - NAT Setup.**
2. Enter 2 to open menu 15.2.

Figure 300 Menu 15.2: NAT Server Sets

```
                    Menu 15.2 - NAT Server Sets

               1. Server Set 1
               2. Server Set 2


                     Enter Set Number to Edit:
```

3. Enter 1 or 2 to go to **Menu 15.2.x - NAT Server Setup** and configure the address mapping rules for the WAN or CELL interface.

Figure 301 Menu 15.2.x: NAT Server Sets

```
                Menu 15.2.1 - NAT Server Setup

              Default Server: 0.0.0.0
          Rule  Act.   Start Port   End Port    IP Address
         ------------------------------------------------------
          001   No     0            0           0.0.0.0
          002   No     0            0           0.0.0.0
          003   No     0            0           0.0.0.0
          004   No     0            0           0.0.0.0
          005   No     0            0           0.0.0.0
          006   No     0            0           0.0.0.0
          007   No     0            0           0.0.0.0
          008   No     0            0           0.0.0.0
          009   No     0            0           0.0.0.0
          010   No     0            0           0.0.0.0


         Select Command= None           Select Rule= N/A
               Press ENTER to Confirm or ESC to Cancel:
```

4 Select **Edit Rule** in the **Select Command** field; type the index number of the NAT server you want to configure in the **Select Rule** field and press [ENTER] to open **Menu 15.2.x.x - NAT Server Configuration** (see the next figure).

Figure 302 15.2.x.x: NAT Server Configuration

```
              15.2.1.2 - NAT Server Configuration

                   Wan= 1                        Index= 2

               ------------------------------------------------

                   Name= 1

                   Active= Yes

                   Start port= 21                End port= 25

                   IP Address= 192.168.1.33

              Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this screen.

Table 206 15.2.x.x: NAT Server Configuration

FIELD	DESCRIPTION
WAN	Yyou can configure port forwarding and trigger port rules for the Ethernet WAN port and separate sets of rules for the Cellular WAN port. This is the WAN port (server set) you select in menu 15.2.
Index	This is the index number of an individual port forwarding server entry.
Name	Enter a name to identify this port-forwarding rule.
Active	Press [SPACE BAR] and then [ENTER] to select **Yes** to enable the NAT server entry.
Start Port End Port	Enter a port number in the **Start Port** field. To forward only one port, enter it again in the **End Port** field. To specify a range of ports, enter the last port to be forwarded in the **End Port** field.
IP Address	Enter the inside IP address of the server.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm…" to save your configuration, or press [ESC] at any time to cancel.	

5 Enter a port number in the **Start Port** field. To forward only one port, enter it again in the **End Port** field. To specify a range of ports, enter the last port to be forwarded in the **End Port** field.

6 Enter the inside IP address of the server in the **IP Address** field. In the following figure, you have a computer acting as an FTP, Telnet and SMTP server (ports 21, 23 and 25) at 192.168.1.33.

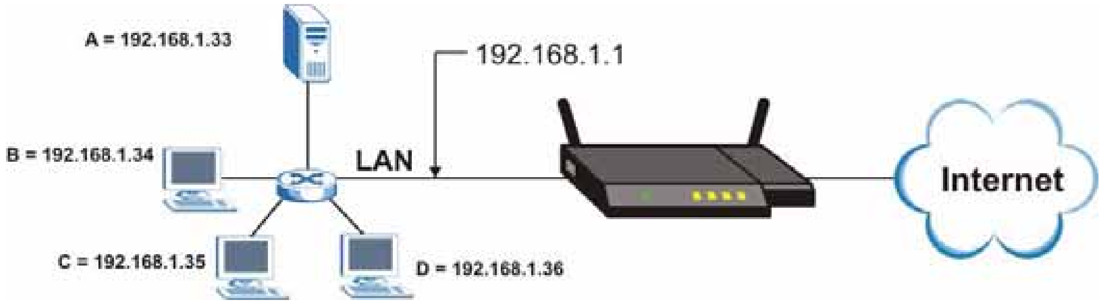
7 Press [ENTER] at the "Press ENTER to confirm …" prompt to save your configuration after you define all the servers or press [ESC] at any time to cancel.

Figure 303 Menu 15.2.1: NAT Server Setup

```
                    Menu 15.2.1 - NAT Server Setup

                  Default Server: 0.0.0.0
          Rule  Act.   Start Port   End Port    IP Address
         ---------------------------------------------------
          001   No     0            0           0.0.0.0
          002   Yes    21           25          192.168.1.33
          003   No     0            0           0.0.0.0
          004   No     0            0           0.0.0.0
          005   No     0            0           0.0.0.0
          006   No     0            0           0.0.0.0
          007   No     0            0           0.0.0.0
          008   No     0            0           0.0.0.0
          009   No     0            0           0.0.0.0
          010   No     0            0           0.0.0.0


         Select Command= None           Select Rule= N/A
               Press ENTER to Confirm or ESC to Cancel:
```

You assign the private network IP addresses. The NAT network appears as a single host on the Internet. A is the FTP/Telnet/SMTP server.

Figure 304 Server Behind NAT Example



33.4 General NAT Examples

The following are some examples of NAT configuration.

33.4.1 Internet Access Only

In the following Internet access example, you only need one rule where all your ILAs (Inside Local addresses) map to one dynamic IGA (Inside Global Address) assigned by your ISP.

Figure 305 NAT Example 1

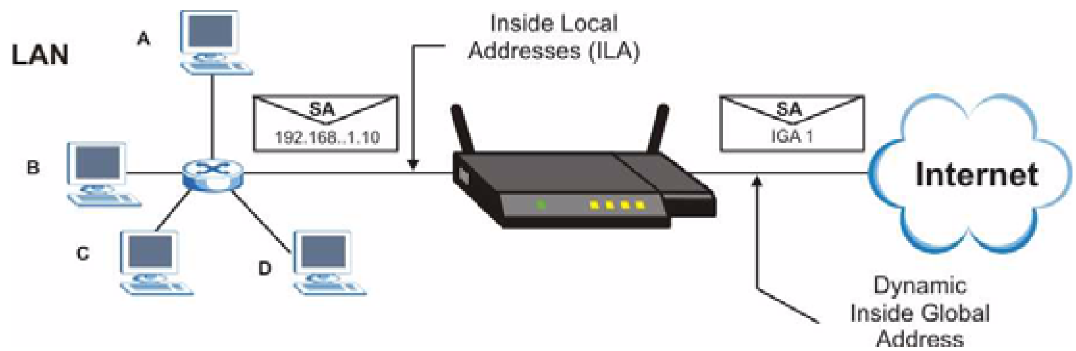


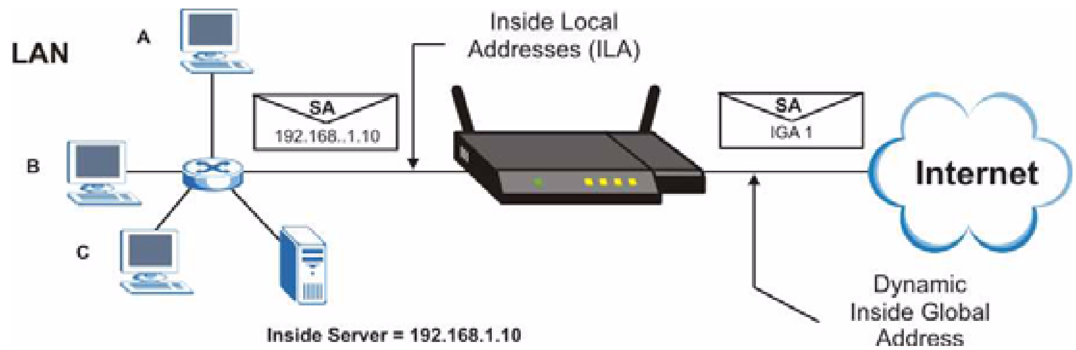
Figure 306 Menu 4: Internet Access & NAT Example

```
Menu 4 - Internet Access Setup

ISP's Name= ChangeMe
Encapsulation= Ethernet
  Service Type= Standard
  My Login= N/A
  My Password= N/A
  Retype to Confirm= N/A
  Login Server= N/A
  Relogin Every (min)=  N/A
IP Address Assignment= Dynamic
  IP Address= N/A
  IP Subnet Mask= N/A
  Gateway IP Address= N/A
Network Address Translation= SUA Only


Press ENTER to Confirm or ESC to Cancel:
```

From menu 4 shown above, simply choose the **SUA Only** option from the **Network Address Translation** field. This is the Many-to-One mapping discussed in Section 33.4 on page 487. The **SUA Only** read-only option from the **Network Address Translation** field in menus 4 and 11.3 is specifically pre-configured to handle this case.

33.4.2 Example 2: Internet Access with a Default Server

Figure 307 NAT Example 2



In this case, you do exactly as above (use the convenient pre-configured **SUA Only** set) and also go to menu 15.2.1 to specify the **Default Server** behind the NAT as shown in the next figure.

In general, if you wish to access the LAN-Cell for remote management through the WAN or CELLULAR interfaces, do not define a NAT **Default Server**. Use the Port Forwarding Rules, Remote Management Ports, and Firewall Rules to define WAN-based remote access to the LAN-Cell.

Figure 308 Menu 15.2.1: Specifying an Inside Server

```
                Menu 15.2.1 - NAT Server Setup

              Default Server: 192.168.1.10
 Rule  Act.   Start Port   End Port    IP Address
------------------------------------------------------
 001   No     0            0           0.0.0.0
 002   Yes    21           25          192.168.1.33
 003   No     0            0           0.0.0.0
 004   No     0            0           0.0.0.0
 005   No     0            0           0.0.0.0
 006   No     0            0           0.0.0.0
 007   No     0            0           0.0.0.0
 008   No     0            0           0.0.0.0
 009   No     0            0           0.0.0.0
 010   No     0            0           0.0.0.0


Select Command= None           Select Rule= N/A
      Press ENTER to Confirm or ESC to Cancel:
```

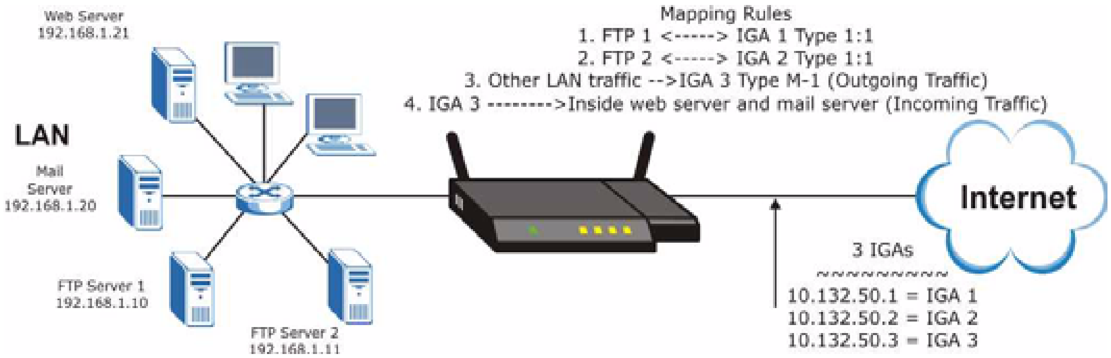
33.4.3 Example 3: Multiple Public IP Addresses With Inside Servers

In this example, there are 3 IGAs from our ISP. There are many departments but two have their own FTP server. All departments share the same router. The example will reserve one IGA for each department with an FTP server and all departments use the other IGA. Map the FTP servers to the first two IGAs and the other LAN traffic to the remaining IGA. Map the third IGA to an inside web server and mail server. Four rules need to be configured, two bi-directional and two uni-directional as follows.

1. Map the first IGA to the first inside FTP server for FTP traffic in both directions (**1 : 1** mapping, giving both local and global IP addresses).
2. Map the second IGA to our second inside FTP server for FTP traffic in both directions (**1 : 1** mapping, giving both local and global IP addresses).
3. Map the other outgoing LAN traffic to IGA3 (**Many : 1** mapping).
4. You also map your third IGA to the web server and mail server on the LAN. Type **Server** allows you to specify multiple servers, of different types, to other computers behind NAT on the LAN.

The example situation looks somewhat like this:

Figure 309 NAT Example 3



1 In this case you need to configure Address Mapping Set 1 from **Menu 15.1 - Address Mapping Sets**. Therefore you must choose the **Full Feature** option from the **Network Address Translation** field (in menu 4 or menu 11.3) in Figure 310 on page 490.
2 Then enter 15 from the main menu.
3 Enter 1 to configure the Address Mapping Sets.
4 Enter 1 to begin configuring this new set. Enter a Set Name, choose the **Edit Action** and then enter 1 for the **Select Rule** field. Press [ENTER] to confirm.
5 Select **Type** as **One-to-One** (direct mapping for packets going both ways), and enter the local **Start IP** as 192.168.1.10 (the IP address of FTP Server 1), the global **Start IP** as 10.132.50.1 (our first IGA). (See Figure 311 on page 491).
6 Repeat the previous step for rules 2 to 4 as outlined above.
7 When finished, menu 15.1.1 should look like as shown in Figure 312 on page 491.

Figure 310 Example 3: Menu 11.1.2

```
              Menu 11.1.2 - Remote Node Network Layer Options

                       IP Address Assignment= Dynamic
                       IP Address= N/A
                       IP Subnet Mask= N/A
                       Gateway IP Addr= N/A

                       Network Address Translation= SUA Only
                       Metric= 2
                       Private=
                       RIP Direction= None
                         Version= N/A
                       Multicast= None


               Enter here to CONFIRM or ESC to CANCEL:
```

The following figure shows how to configure the first rule.

Figure 311 Example 3: Menu 15.1.1.1

```
                Menu 15.1.1.1 Address Mapping Rule

                    Type= One-to-One

                    Local IP:
                      Start= 192.168.1.10
                      End   = N/A

                    Global IP:
                      Start= 10.132.50.1
                      End   = N/A

                    Server Mapping Set= N/A

                Press ENTER to Confirm or ESC to Cancel:
```

Figure 312 Example 3: Final Menu 15.1.1

```
                    Menu 15.1.1 - Address Mapping Rules

Set Name= Example3

Idx  Local Start IP   Local End IP     Global Start IP  Global End IP    Type
---  ---------------  ---------------  ---------------  ---------------  ---
 1. 192.168.1.10                       10.132.50.1                        1-1
 2  192.168.1.11                       10.132.50.2                        1-1
 3. 0.0.0.0          255.255.255.255  10.132.50.3                        M-1
 4.                                   10.132.50.3                     Server
 5.
 6.
 7.
 8.
 9.
10.

                  Action= Edit            Select Rule=

                 Press ENTER to Confirm or ESC to Cancel:
```

Now configure the IGA3 to map to our web server and mail server on the LAN.

1 Enter 15 from the main menu.
2 Enter 2 to go to menu 15.2.
3 (Enter 1 or 2 from menu 15.2) configure the menu as shown in Figure 313 on page 492.

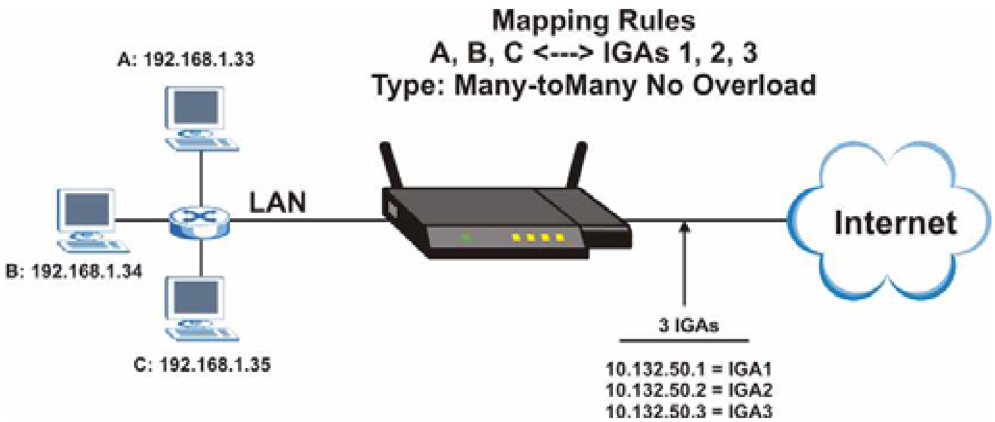
Figure 313 Example 3: Menu 15.2.1

```
                     Menu 15.2.1 - NAT Server Setup

               Default Server: 0.0.0.0
       Rule  Act.   Start Port   End Port    IP Address
      ------------------------------------------------------
       001   Yes    80           80          192.168.1.21
       002   Yes    25           25          192.168.1.20
       003   No     0            0           0.0.0.0
       004   No     0            0           0.0.0.0
       005   No     0            0           0.0.0.0
       006   No     0            0           0.0.0.0
       007   No     0            0           0.0.0.0
       008   No     0            0           0.0.0.0
       009   No     0            0           0.0.0.0
       010   No     0            0           0.0.0.0


      Select Command= None           Select Rule= N/A
            Press ENTER to Confirm or ESC to Cancel:
```

33.4.4 Example 4: NAT Unfriendly Application Programs

Some applications do not support NAT Mapping using TCP or UDP port address translation. In this case it is better to use **Many-One-to-One** mapping as port numbers do *not* change for **Many-One-to-One** (and **One-to-One**) NAT mapping types. The following figure illustrates this.

Figure 314 NAT Example 4



Other applications such as some gaming programs are NAT unfriendly because they embed addressing information in the data stream. These applications won't work through NAT even when using **One-to-One** and **Many-One-to-One** mapping types.

Follow the steps outlined in example 3 above to configure these two menus as follows.

Figure 315 Example 4: Menu 15.1.1.1: Address Mapping Rule

```
                   Menu 15.1.1.1 Address Mapping Rule

                         Type= Many-One-to-One

                         Local IP:
                           Start= 192.168.1.10
                           End  = 192.168.1.12

                         Global IP:
                           Start= 10.132.50.1
                           End  = 10.132.50.3

              Press ENTER to Confirm or ESC to Cancel:
```

After you've configured your rule, you should be able to check the settings in menu 15.1.1 as shown next.

Figure 316 Example 4: Menu 15.1.1: Address Mapping Rules

```
                 Menu 15.1.1 - Address Mapping Rules

  Set Name= Example4

Idx  Local Start IP   Local End IP     Global Start IP  Global End IP    Type
---  ---------------  ---------------  ---------------  ---------------  ---
 1.  192.168.1.10     192.168.1.12     10.132.50.1      10.132.50.3      M-1-1
 2.
 3.
 4.
 5.
 6.
 7.
 8.
 9.
10.

         Action= Edit          Select Rule=

         Press ENTER to Confirm or ESC to Cancel:
```

33.5 Trigger Port Forwarding

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 LAN-Cell 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 LAN-Cell's WAN port receives a response with a specific port number and protocol ("incoming" port), the LAN-Cell 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.

33.5.1 Two Points To Remember About Trigger Ports

1. Trigger events only happen on data that is going coming from inside the LAN-Cell and going to the outside.
2. 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.

Only one LAN computer can use a trigger port (range) at a time.

Enter 3 in menu 15 to display **Menu 15.3 - Trigger Ports**. For a LAN-Cell with multiple WAN interfaces, enter 1 or 2 from menu 15.3 to go to **Menu 15.3.1** or **Menu 15.3.2 - Trigger Port Setup** and configure trigger port rules for the first or second WAN interface.

Figure 317 Menu 15.3.1: Trigger Port Setup

```
                      Menu 15.3.1 - Trigger Port Setup

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

                           Press ENTER to Confirm or ESC to Cancel:

      HTTP:80  FTP:21  Telnet:23  SMTP:25  POP3:110  PPTP:1723
```

The following table describes the fields in this menu.

Table 207 Menu 15.3.1: Trigger Port Setup

FIELD	DESCRIPTION
Rule	This is the rule index number.
Name	Enter a unique name for identification purposes. You may enter up to 15 characters in this field. 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 LAN-Cell forwards the traffic with this port (or range of ports) to the client computer on the LAN that requested the service.
Start Port	Enter a port number or the starting port number in a range of port numbers.
End Port	Enter 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 LAN-Cell to record the IP address of the LAN computer that sent the traffic to a server on the WAN.
Start Port	Enter a port number or the starting port number in a range of port numbers.
End Port	Enter a port number or the ending port number in a range of port numbers.
Press [ENTER] at the message “Press ENTER to Confirm...” to save your configuration, or press [ESC] at any time to cancel.	

34

Firewall Status

This chapter shows you how to get started with the LAN-Cell firewall.

34.1 Firewall SMT Menus

From the main menu enter 21 to go to **Menu 21 - Filter Set and Firewall Configuration** to display the screen shown next.

Figure 318 Menu 21: Filter and Firewall Setup

```
              Menu 21 - Filter and Firewall Setup

                       1. Filter Setup
                       2. Firewall Setup


              Enter Menu Selection Number:
```

34.1.1 Activating the Firewall

Enter option 2 in this menu to bring up the following screen. Press [SPACE BAR] and then [ENTER] to select **Yes** in the **Active** field to activate the firewall. The firewall must be active to protect against Denial of Service (DoS) attacks. Use the web configurator to configure firewall rules.

Figure 319 Menu 21.2: Firewall Setup

```
                          Menu 21.2 - Firewall Setup

             The firewall protects against Denial of Service (DoS) attacks
             when it is active.

             Your network is vulnerable to attacks when the firewall is
             turned off.

             Refer to the User's Guide for details about the firewall
             default policies.

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

             Active: Yes

             You can use the Web Configurator to configure the firewall.

                      Press ENTER to Confirm or ESC to Cancel:
```

Configure the firewall rules using the web configurator or CLI commands.

35

Filter Configuration

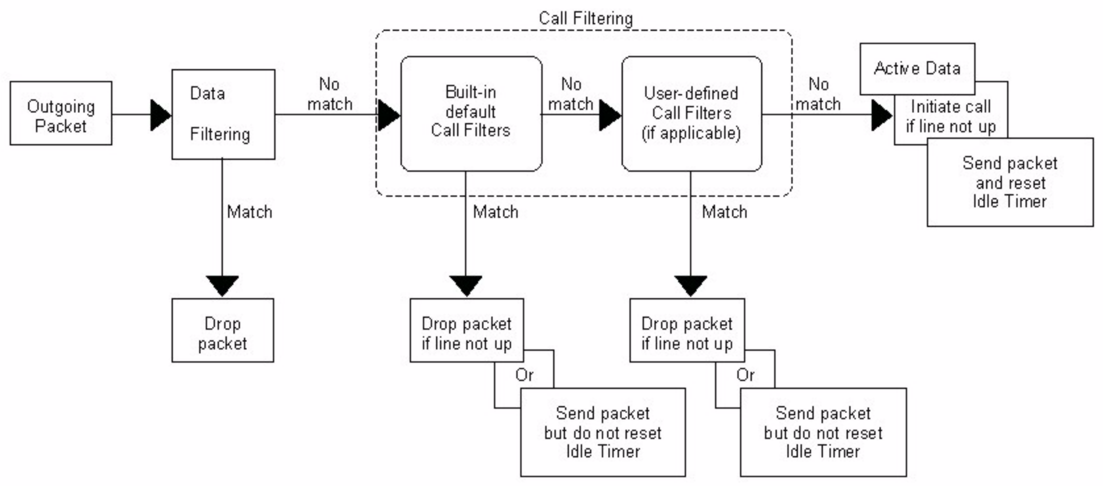
This chapter shows you how to create and apply filters.

35.1 Introduction to Filters

Your LAN-Cell uses filters to decide whether to allow passage of a data packet and/or to make a call. There are two types of filter applications: data filtering and call filtering. Filters are subdivided into device and protocol filters, which are discussed later.

Data filtering screens the data to determine if the packet should be allowed to pass. Data filters are divided into incoming and outgoing filters, depending on the direction of the packet relative to a port. Data filtering can be applied on either the WAN side or the LAN side. Call filtering is used to determine if a packet should be allowed to trigger a call. Remote node call filtering is only applicable when using PPPoE encapsulation. Outgoing packets must undergo data filtering before they encounter call filtering as shown in the following figure.

Figure 320 Outgoing Packet Filtering Process



For incoming packets, your LAN-Cell applies data filters only. Packets are processed depending upon whether a match is found. The following sections describe how to configure filter sets.

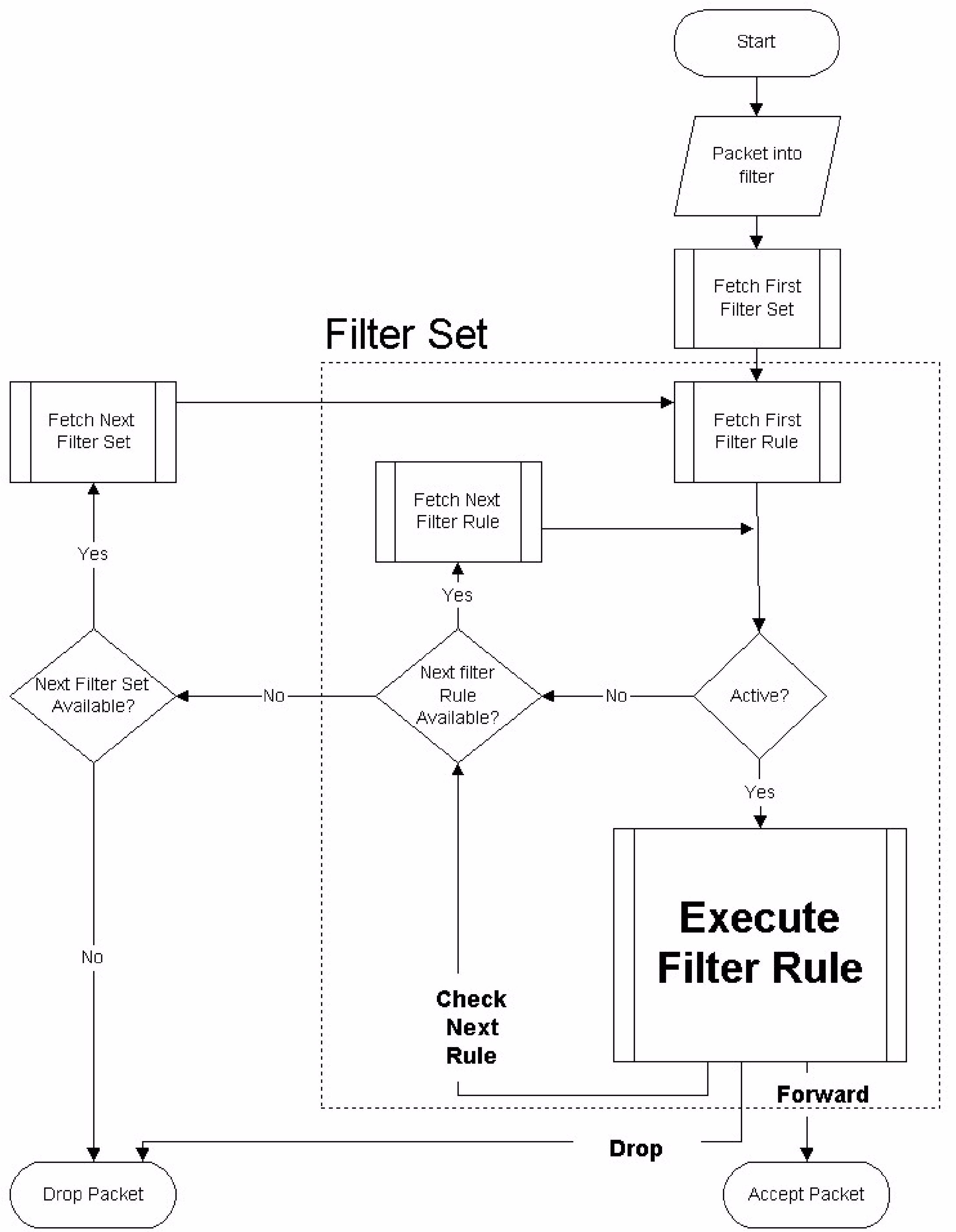
35.1.1 The Filter Structure of the LAN-Cell

A filter set consists of one or more filter rules. Usually, you would group related rules, e.g., all the rules for NetBIOS, into a single set and give it a descriptive name. The LAN-Cell allows you to configure up to twelve filter sets with six rules in each set, for a total of 72 filter rules in the system. You cannot mix device filter rules and protocol filter rules within the same set. You can apply up to four filter sets to a particular port to block multiple types of packets. With each filter set having up to six rules, you can have a maximum of 24 rules active for a single port.

Sets of factory default filter rules have been configured in menu 21 to prevent NetBIOS traffic from triggering calls and to prevent incoming telnet sessions. A summary of their filter rules is shown in the figures that follow.

The following figure illustrates the logic flow when executing a filter rule. See also Figure 325 on page 506 for the logic flow when executing an IP filter.

Figure 321 Filter Rule Process



You can apply up to four filter sets to a particular port to block multiple types of packets. With each filter set having up to six rules, you can have a maximum of 24 rules active for a single port.

35.2 Configuring a Filter Set

The LAN-Cell includes filtering for NetBIOS over TCP/IP packets by default. To configure another filter set, follow the procedure below.

1 Enter 21 in the main menu to open menu 21.

Figure 322 Menu 21: Filter and Firewall Setup

```
              Menu 21 - Filter and Firewall Setup

                       1. Filter Setup
                       2. Firewall Setup




              Enter Menu Selection Number:
```

2 Enter 1 to bring up the following menu.

Figure 323 Menu 21.1: Filter Set Configuration

```
                 Menu 21.1 - Filter Set Configuration

     Filter                                Filter
     Set #        Comments                 Set #        Comments
     ------   -----------------            ------   -----------------
      1       _______________               7       _______________
      2       _______________               8       _______________
      3       _______________               9       _______________
      4       _______________              10       _______________
      5       _______________              11       _______________
      6       _______________              12       _______________


          Enter Filter Set Number to Configure= 0

          Edit Comments= N/A

          Press ENTER to Confirm or ESC to Cancel:
```

3 Select the filter set you wish to configure (1-12) and press [ENTER].

4 Enter a descriptive name or comment in the **Edit Comments** field and press [ENTER].

5 Press [ENTER] at the message [Press ENTER to confirm] to open **Menu 21.1.x - Filter Rules Summary**.

This screen shows the summary of the existing rules in the filter set. The following tables contain a brief description of the abbreviations used in the previous menus.

Table 208 Abbreviations Used in the Filter Rules Summary Menu

FIELD	DESCRIPTION
A	Active: “Y” means the rule is active. “N” means the rule is inactive.
Type	The type of filter rule: “GEN” for Generic, “IP” for TCP/IP.
Filter Rules	These parameters are displayed here.
M	More. “Y” means there are more rules to check which form a rule chain with the present rule. An action cannot be taken until the rule chain is complete. “N” means there are no more rules to check. You can specify an action to be taken i.e., forward the packet, drop the packet or check the next rule. For the latter, the next rule is independent of the rule just checked.
m	Action Matched. “F” means to forward the packet immediately and skip checking the remaining rules. “D” means to drop the packet. “N“ means to check the next rule.
n	Action Not Matched. “F” means to forward the packet immediately and skip checking the remaining rules. “D” means to drop the packet. “N” means to check the next rule.

The protocol dependent filter rules abbreviation are listed as follows:

Table 209 Rule Abbreviations Used

ABBREVIATION	DESCRIPTION
IP	
Pr	Protocol
SA	Source Address
SP	Source Port number
DA	Destination Address
DP	Destination Port number
GEN	
Off	Offset
Len	Length

Refer to the next section for information on configuring the filter rules.

35.2.1 Configuring a Filter Rule

To configure a filter rule, type its number in **Menu 21.1.x - Filter Rules Summary** and press [ENTER] to open menu 21.1.x.x for the rule.

To speed up filtering, all rules in a filter set must be of the same class, i.e., protocol filters or generic filters. The class of a filter set is determined by the first rule that you create. When applying the filter sets to a port, separate menu fields are provided for protocol and device filter sets. If you include a protocol filter set in a device filter field or vice versa, the LAN-Cell will warn you and will not allow you to save.

35.2.2 Configuring a TCP/IP Filter Rule

This section shows you how to configure a TCP/IP filter rule. TCP/IP rules allow you to base the rule on the fields in the IP and the upper layer protocol, for example, UDP and TCP headers.

To configure TCP/IP rules, select **TCP/IP Filter Rule** from the **Filter Type** field and press [ENTER] to open **Menu 21.1.x.x - TCP/IP Filter Rule**, as shown next.

Figure 324 Menu 21.1.1.1: TCP/IP Filter Rule

```
              Menu 21.1.1.1 - TCP/IP Filter Rule

                           Filter #: 1,1
                           Filter Type= TCP/IP Filter Rule
                           Active= Yes
                           IP Protocol= 0     IP Source Route= No
                           Destination: IP Addr=
                                        IP Mask=
                                        Port #=
                                        Port # Comp= None
                                Source: IP Addr=
                                        IP Mask=
                                        Port #=
                                        Port # Comp= None
                           TCP Estab= N/A
                           More= No           Log= None
                           Action Matched= Check Next Rule
                           Action Not Matched= Check Next Rule


                           Press ENTER to Confirm or ESC to Cancel:
```

The following table describes how to configure your TCP/IP filter rule.

Table 210 Menu 21.1.1.1: TCP/IP Filter Rule

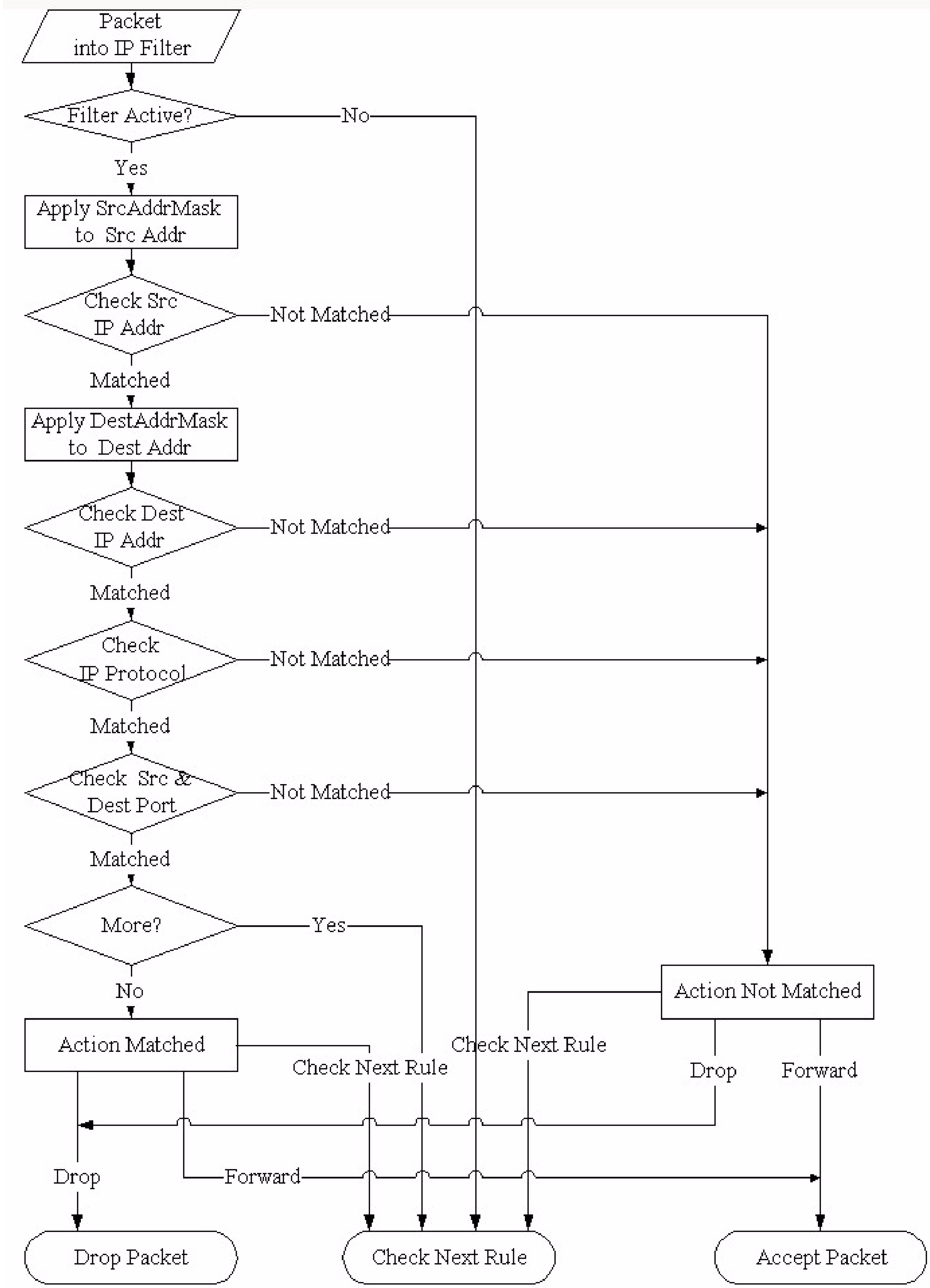
FIELD	DESCRIPTION
Active	Press [SPACE BAR] and then [ENTER] to select **Yes** to activate the filter rule or **No** to deactivate it.
IP Protocol	Protocol refers to the upper layer protocol, e.g., TCP is 6, UDP is 17 and ICMP is 1. Type a value between 0 and 255. A value of 0 matches ANY protocol.
IP Source Route	Press [SPACE BAR] and then [ENTER] to select **Yes** to apply the rule to packets with an IP source route option. Otherwise the packets must not have a source route option. The majority of IP packets do not have source route.
Destination	
IP Addr	Enter the destination IP Address of the packet you wish to filter. This field is ignored if it is 0.0.0.0.
IP Mask	Enter the IP mask to apply to the **Destination: IP Addr**.
Port #	Enter the destination port of the packets that you wish to filter. The range of this field is 0 to 65535. This field is ignored if it is 0.

Table 210 Menu 21.1.1.1: TCP/IP Filter Rule

FIELD	DESCRIPTION
Port # Comp	Press [SPACE BAR] and then [ENTER] to select the comparison to apply to the destination port in the packet against the value given in **Destination: Port #**. Options are **None**, **Equal**, **Not Equal**, **Less** and **Greater**.
Source	
IP Addr	Enter the source IP Address of the packet you wish to filter. This field is ignored if it is 0.0.0.0.
IP Mask	Enter the IP mask to apply to the **Source: IP Addr**.
Port #	Enter the source port of the packets that you wish to filter. The range of this field is 0 to 65535. This field is ignored if it is 0.
Port # Comp	Press [SPACE BAR] and then [ENTER] to select the comparison to apply to the source port in the packet against the value given in **Source: Port #**. Options are **None**, **Equal**, **Not Equal**, **Less** and **Greater**.
TCP Estab	This field is applicable only when the IP Protocol field is 6, TCP. Press [SPACE BAR] and then [ENTER] to select **Yes**, to have the rule match packets that want to establish a TCP connection (SYN=1 and ACK=0); if **No**, it is ignored.
More	Press [SPACE BAR] and then [ENTER] to select **Yes** or **No**. If **Yes**, a matching packet is passed to the next filter rule before an action is taken; if **No**, the packet is disposed of according to the action fields. If **More** is **Yes**, then **Action Matched** and **Action Not Matched** will be **N/A**.
Log	Press [SPACE BAR] and then [ENTER] to select a logging option from the following: **None** – No packets will be logged. **Action Matched** - Only packets that match the rule parameters will be logged. **Action Not Matched** - Only packets that do not match the rule parameters will be logged. **Both** – All packets will be logged.
Action Matched	Press [SPACE BAR] and then [ENTER] to select the action for a matching packet. Options are **Check Next Rule**, **Forward** and **Drop**.
Action Not Matched	Press [SPACE BAR] and then [ENTER] to select the action for a packet not matching the rule. Options are **Check Next Rule**, **Forward** and **Drop**.
When you have **Menu 21.1.1.1 - TCP/IP Filter Rule** configured, press [ENTER] at the message “Press ENTER to Confirm” to save your configuration, or press [ESC] to cancel. This data will now be displayed on **Menu 21.1.1 - Filter Rules Summary**.	

The following figure illustrates the logic flow of an IP filter.

Figure 325 Executing an IP Filter



35.2.3 Configuring a Generic Filter Rule

This section shows you how to configure a generic filter rule. The purpose of generic rules is to allow you to filter non-IP packets. For IP, it is generally easier to use the IP rules directly.

For generic rules, the LAN-Cell treats a packet as a byte stream as opposed to an IP or IPX packet. You specify the portion of the packet to check with the **Offset** (from 0) and the **Length** fields, both in bytes. The LAN-Cell applies the Mask (bit-wise ANDing) to the data portion before comparing the result against the Value to determine a match. The **Mask** and **Value** are specified in hexadecimal numbers. Note that it takes two hexadecimal digits to represent a byte, so if the length is 4, the value in either field will take 8 digits, for example, FFFFFFFF.

To configure a generic rule, select **Generic Filter Rule** in the **Filter Type** field in menu 21.1.x.x and press [ENTER] to open Generic Filter Rule, as shown below.

Figure 326 Menu 21.1.1.1: Generic Filter Rule

```
Menu 21.1.1.1 - Generic Filter Rule

Filter #: 1,1
Filter Type= Generic Filter Rule
Active= No
Offset= 0
Length= 0
Mask= N/A
Value= N/A
More= No           Log= None
Action Matched= Check Next Rule
Action Not Matched= Check Next Rule

Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in the **Generic Filter Rule** menu.

Table 211 Generic Filter Rule Menu Fields

FIELD	DESCRIPTION
Filter #	This is the filter set, filter rule co-ordinates, i.e., 2,3 refers to the second filter set and the third rule of that set.
Filter Type	Use [SPACE BAR] and then [ENTER] to select a rule type. Parameters displayed below each type will be different. TCP/IP filter rules are used to filter IP packets while generic filter rules allow filtering of non-IP packets. Options are **Generic Filter Rule** and **TCP/IP Filter Rule**.
Active	Select **Yes** to turn on the filter rule or **No** to turn it off.
Offset	Enter the starting byte of the data portion in the packet that you wish to compare. The range for this field is from 0 to 255.
Length	Enter the byte count of the data portion in the packet that you wish to compare. The range for this field is 0 to 8.
Mask	Enter the mask (in Hexadecimal notation) to apply to the data portion before comparison.
Value	Enter the value (in Hexadecimal notation) to compare with the data portion.
More	If **Yes**, a matching packet is passed to the next filter rule before an action is taken; else the packet is disposed of according to the action fields. If **More** is **Yes**, then Action Matched and Action Not Matched will be **No**.

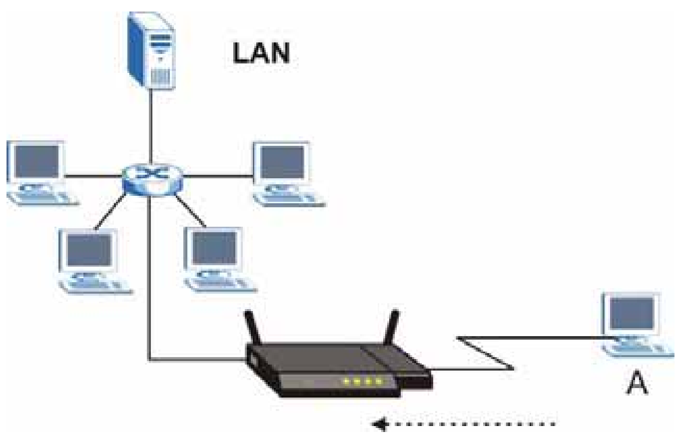
Table 211 Generic Filter Rule Menu Fields

FIELD	DESCRIPTION
Log	Select the logging option from the following: **None** - No packets will be logged. **Action Matched** - Only packets that match the rule parameters will be logged. **Action Not Matched** - Only packets that do not match the rule parameters will be logged. **Both** – All packets will be logged.
Action Matched	Select the action for a packet matching the rule. Options are **Check Next Rule**, **Forward** and **Drop**.
Action Not Matched	Select the action for a packet not matching the rule. Options are **Check Next Rule**, **Forward** and **Drop**.
Once you have completed filling in **Menu 21.1.1.1 - Generic Filter Rule**, press [ENTER] at the message "Press ENTER to Confirm" to save your configuration, or press [ESC] to cancel. This data will now be displayed on **Menu 21.1.1 - Filter Rules Summary**.	

35.3 Example Filter

Let's look at an example to block outside users from accessing the LAN-Cell via telnet. Please see our included disk for more example filters.

Figure 327 Telnet Filter Example



1 Enter 21 from the main menu to open **Menu 21 - Filter and Firewall Setup**.
2 Enter 1 to open Menu 21.1 - Filter Set Configuration.
3 Enter the index of the filter set you wish to configure (say 3) and press [ENTER].
4 Enter a descriptive name or comment in the **Edit Comments** field and press [ENTER].
5 Press [ENTER] at the message [Press ENTER to confirm] to open **Menu 21.1.3 - Filter Rules Summary**.
6 Enter 1 to configure the first filter rule (the only filter rule of this set). Make the entries in this menu as shown in the following figure.

Figure 328 Example Filter: Menu 21.1.3.1

```
                              Menu 21.1.3.1 - TCP/IP Filter Rule

              Filter #: 3,1
              Filter Type= TCP/IP Filter Rule
              Active= Yes
              IP Protocol= 6      IP Source Route= No
              Destination: IP Addr= 0.0.0.0
                           IP Mask= 0.0.0.0
                           Port #= 23
                           Port # Comp= Equal
                   Source: IP Addr= 0.0.0.0
                           IP Mask= 0.0.0.0
                           Port #= 0
                           Port # Comp= None
              TCP Estab= No
              More= No             Log= None
              Action Matched= Drop
              Action Not Matched= Forward

                       Press ENTER to Confirm or ESC to Cancel:
              Press Space Bar to Toggle.
```

The port number for the telnet service (TCP protocol) is **23**. See *RFC 1060* for port numbers of well-known services.

When you press [ENTER] to confirm, you will see the following screen. Note that there is only one filter rule in this set.

Figure 329 Example Filter Rules Summary: Menu 21.1.3

```
              Menu 21.1.3 - Filter Rules Summary

       # A Type                       Filter Rules              M m n
       - - ---- ----------------------------------------------- - - -
       1 Y IP   Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=23             N D F
       2 N
       3 N
       4 N
       5 N
       6 N


       Enter Filter Rule Number (1-6) to Configure: 1
```

This shows you that you have configured and activated (**A = Y**) a TCP/IP filter rule (**Type = IP**, **Pr = 6**) for destination telnet ports (**DP = 23**).

M = N means an action can be taken immediately. The action is to drop the packet (**m = D**) if the action is matched and to forward the packet immediately (**n = F**) if the action is not matched no matter whether there are more rules to be checked (there aren't in this example).

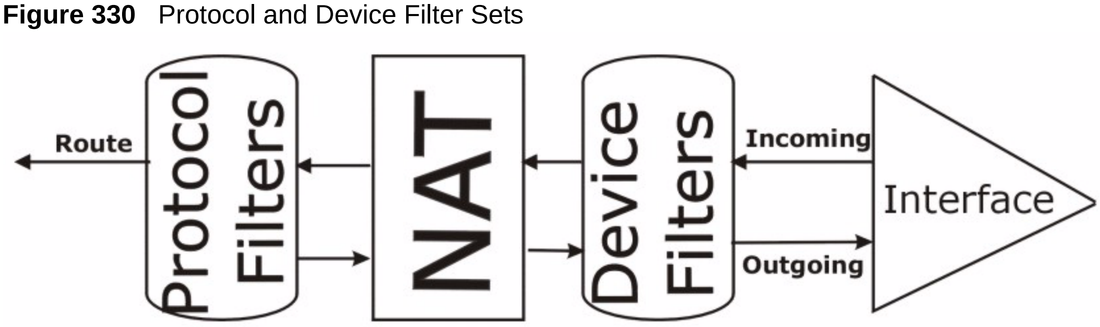
After you've created the filter set, you must apply it.

1. Enter 11 from the main menu to go to menu 11.
2. Enter 1 or 2 to open **Menu 11.x - Remote Node Profile**.
3. Go to the **Edit Filter Sets** field, press [SPACE BAR] to select **Yes** and press [ENTER].
4. This brings you to menu 11.1.4. Apply a filter set (our example filter set 3) as shown in Figure 333 on page 513.
5. Press [ENTER] to confirm after you enter the set numbers and to leave menu 11.1.4.

35.4 Filter Types and NAT

There are two classes of filter rules, **Generic Filter** (Device) rules and protocol filter (**TCP/IP**) rules. Generic filter rules act on the raw data from/to LAN and WAN. Protocol filter rules act on the IP packets. Generic and TCP/IP filter rules are discussed in more detail in the next section. When NAT (Network Address Translation) is enabled, the inside IP address and port number are replaced on a connection-by-connection basis, which makes it impossible to know the exact address and port on the wire. Therefore, the LAN-Cell applies the protocol filters to the "native" IP address and port number before NAT for outgoing packets and after NAT for incoming packets. On the other hand, the generic, or device filters are applied to the raw packets that appear on the wire. They are applied at the point when the LAN-Cell is receiving and sending the packets; i.e. the interface. The interface can be an Ethernet port or any other hardware port. The following diagram illustrates this.

Figure 330 Protocol and Device Filter Sets



35.5 Firewall Versus Filters

Below are some comparisons between the LAN-Cell's filtering and firewall functions.

35.5.1 Packet Filtering:

- The router filters packets as they pass through the router's interface according to the filter rules you designed.
- Packet filtering is a powerful tool, yet can be complex to configure and maintain, especially if you need a chain of rules to filter a service.
- Packet filtering only checks the header portion of an IP packet.

35.5.1.1 When To Use Filtering

1. To block/allow LAN packets by their MAC addresses.
2. To block/allow special IP packets which are neither TCP nor UDP, nor ICMP packets.
3. To block/allow both inbound (WAN to LAN) and outbound (LAN to WAN) traffic between the specific inside host/network "A" and outside host/network "B". If the filter blocks the traffic from A to B, it also blocks the traffic from B to A. Filters cannot distinguish traffic originating from an inside host or an outside host by IP address.
4. To block/allow IP trace route.

35.5.2 Firewall

- The firewall inspects packet contents as well as their source and destination addresses. Firewalls of this type employ an inspection module, applicable to all protocols, that understands data in the packet is intended for other layers, from the network layer (IP headers) up to the application layer.
- The firewall performs stateful inspection. It takes into account the state of connections it handles so that, for example, a legitimate incoming packet can be matched with the outbound request for that packet and allowed in. Conversely, an incoming packet masquerading as a response to a nonexistent outbound request can be blocked.
- The firewall uses session filtering, i.e., smart rules, that enhance the filtering process and control the network session rather than control individual packets in a session.
- The firewall provides e-mail service to notify you of routine reports and when alerts occur.

35.5.2.1 When To Use The Firewall

1. To prevent DoS attacks and prevent hackers cracking your network.
2. A range of source and destination IP addresses as well as port numbers can be specified within one firewall rule making the firewall a better choice when complex rules are required.
3. To selectively block/allow inbound or outbound traffic between inside host/networks and outside host/networks. Remember that filters cannot distinguish traffic originating from an inside host or an outside host by IP address.
4. The firewall performs better than filtering if you need to check many rules.
5. Use the firewall if you need routine e-mail reports about your system or need to be alerted when attacks occur.
6. The firewall can block specific URL traffic that might occur in the future. The URL can be saved in an Access Control List (ACL) database.

35.6 Applying a Filter

This section shows you where to apply the filter(s) after you design it (them). The LAN-Cell already has filters to prevent NetBIOS traffic from triggering calls, and block incoming telnet, FTP and HTTP connections.

If you do not activate the firewall, it is advisable to apply filters.

35.6.1 Applying LAN Filters

LAN traffic filter sets may be useful to block certain packets, reduce traffic and prevent security breaches. Go to menu 3.1 (shown next) and enter the number(s) of the filter set(s) that you want to apply as appropriate. You can choose up to four filter sets (from twelve) by entering their numbers separated by commas, e.g., 3, 4, 6, 11. Input filter sets filter incoming traffic to the LAN-Cell and output filter sets filter outgoing traffic from the LAN-Cell. For PPPoE or PPTP encapsulation, you have the additional option of specifying remote node call filter sets.

Figure 331 Filtering LAN Traffic

```
                    Menu 3.1 - LAN Port Filter Setup

              Input Filter Sets:
                protocol filters=
                  device filters=
              Output Filter Sets:
                protocol filters=
                  device filters=

              Press ENTER to Confirm or ESC to Cancel:
```

35.6.2 Applying DMZ Filters

DMZ traffic filter sets may be useful to block certain packets, reduce traffic and prevent security breaches. Go to menu 5.1 (shown next) and enter the number(s) of the filter set(s) that you want to apply as appropriate. You can choose up to four filter sets (from twelve) by entering their numbers separated by commas, e.g., 3, 4, 6, 11. Input filter sets filter incoming traffic to the LAN-Cell and output filter sets filter outgoing traffic from the LAN-Cell. The LAN-Cell already has filters to prevent NetBIOS traffic from triggering calls, and block incoming telnet, FTP and HTTP connections.

Figure 332 Filtering DMZ Traffic

```
                    Menu 5.1 - DMZ Port Filter Setup

              Input Filter Sets:
                protocol filters=
                  device filters=
              Output Filter Sets:
                protocol filters=
                  device filters=

              Press ENTER to Confirm or ESC to Cancel:
```

35.6.3 Applying Remote Node Filters

Go to menu 11.1.4 (shown below – note that call filter sets are only present for PPPoE encapsulation) and enter the number(s) of the filter set(s) as appropriate. You can cascade up to four filter sets by entering their numbers separated by commas. The LAN-Cell already has filters to prevent NetBIOS traffic from triggering calls, and block incoming telnet, FTP and HTTP connections.

Figure 333 Filtering Remote Node Traffic

```
                  Menu 11.1.4 - Remote Node Filter Setup

              Input Filter Sets:
                protocol filters=
                  device filters=
              Output Filter Sets:
                protocol filters=
                  device filters=

              Press ENTER to Confirm or ESC to Cancel:
```

36

SNMP Configuration

This chapter explains SNMP configuration menu 22.

36.1 SNMP Configuration

To configure SNMP, enter 22 from the main menu to display **Menu 22 - SNMP Configuration** as shown next. The "community" for **Get**, **Set** and **Trap** fields is SNMP terminology for password.

Figure 334 Menu 22: SNMP Configuration

```
              Menu 22 - SNMP Configuration

                      SNMP:
                        Get Community= public
                        Set Community= public
                        Trusted Host= 0.0.0.0
                        Trap:
                          Community= public
                          Destination= 0.0.0.0


              Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the SNMP configuration parameters.

Table 212 SNMP Configuration Menu Fields

FIELD	DESCRIPTION
Get Community	Type the Get community, which is the password for the incoming Get- and GetNext requests from the management station.
Set Community	Type the Set community, which is the password for incoming Set requests from the management station.
Trusted Host	If you enter a trusted host, your LAN-Cell will only respond to SNMP messages from this address. A blank (default) field means your LAN-Cell will respond to all SNMP messages it receives, regardless of source.
Trap	
Community	Type the Trap community, which is the password sent with each trap to the SNMP manager.

Table 212 SNMP Configuration Menu Fields (continued)

FIELD	DESCRIPTION
Destination	Type the IP address of the station to send your SNMP traps to.
When you have completed this menu, press [ENTER] at the prompt “Press [ENTER] to confirm or [ESC] to cancel” to save your configuration or press [ESC] to cancel and go back to the previous screen.	

36.2 SNMP Traps

The LAN-Cell will send traps to the SNMP manager when any one of the following events occurs:

Table 213 SNMP Traps

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

37

System Information & Diagnosis

This chapter covers SMT menus 24.1 to 24.4.

37.1 Introduction to System Status

This chapter covers the diagnostic tools that help you to maintain your LAN-Cell. These tools include updates on system status, port status and log and trace capabilities.

Select menu 24 in the main menu to open **Menu 24 - System Maintenance**, as shown below.

Figure 335 Menu 24: System Maintenance

```
              Menu 24 - System Maintenance

                 1.  System Status
                 2.  System Information and Console Port Speed
                 3.  Log and Trace
                 4.  Diagnostic
                 5.  Backup Configuration
                 6.  Restore Configuration
                 7.  Upload Firmware
                 8.  Command Interpreter Mode
                 9.  Call Control
                 10. Time and Date Setting
                 11. Remote Management Setup


              Enter Menu Selection Number:
```

37.2 System Status

The first selection, System Status, gives you information on the version of your system firmware and the status and statistics of the ports, as shown in the next figure. System Status is a tool that can be used to monitor your LAN-Cell. Specifically, it gives you information on your system firmware version, number of packets sent and number of packets received.

To get to the System Status:

1. Enter number 24 to go to **Menu 24 - System Maintenance**.
2. In this menu, enter 1 to open **Menu 24.1 - System Maintenance - Status**.

3 There are three commands in **Menu 24.1 - System Maintenance - Status**. Entering 1 or 2 drops the WAN or CELL connection, 9 resets the counters and [ESC] takes you back to the previous screen.

Figure 336 Menu 24.1: System Maintenance: Status

```
                    Menu 24.1 - System Maintenance - Status          03:13:41
                                                           Wed. Dec. 06, 2006
Port   Status       TxPkts      RxPkts    Cols    Tx B/s    Rx B/s     Up Time
WAN   100M/Full      5863       17802       0         0       128     1:31:14
CELL      Down          0           0       0         0         0     0:00:00
 LAN   100M/Full      7443        9261       0       370       128     1:31:57
WCRD   Down             1           0       0         0         0     0:00:00
 DMZ   100M/Full         0           0       0         0         0     1:31:57
WLAN   100M/Full         0           0       0         0         0     1:31:57

Port   Ethernet Address        IP Address          IP Mask       DHCP
WAN   00:13:49:00:00:02      172.23.37.10     255.255.255.0     Client
CELL  00:00:00:00:00:00           0.0.0.0           0.0.0.0       None
 LAN  00:13:49:00:00:01       192.168.1.1     255.255.255.0     Server
WLAN  00:13:49:00:00:04           0.0.0.0           0.0.0.0       None
 DMZ  00:13:49:00:00:03           0.0.0.0           0.0.0.0       None

     System up Time:     1:32:02
     Wi-Fi bridged to: LAN
                                  Press Command:

             COMMANDS: 1, 2-Drop WAN,CELL 9-Reset Counters   ESC-Exit
```

The following table describes the fields present in **Menu 24.1 - System Maintenance - Status**. These fields are READ-ONLY and meant for diagnostic purposes. The upper right corner of the screen shows the time and date according to the format you set in menu 24.10.

Table 214 System Maintenance: Status Menu Fields

FIELD	DESCRIPTION
Port	This field identifies an interface (WAN, CELL, LAN, WCRD (internal Wi-Fi AP), DMZ or WLAN) on the LAN-Cell.
Status	For the LAN, DMZ, and WLAN Interfaces, this displays the port speed and duplex setting. For the WAN interfaces, it displays the port speed and duplex setting if you're using Ethernet encapsulation or the remote node name (configured through the SMT) for a PPP connection and **Down** (line is down or not connected), **Idle** (line (ppp) idle), **Dial** (starting to trigger a call) or **Drop** (dropping a call) if you're using PPPoE encapsulation. For the Wi-Fi AP, it displays the transmission rate when WLAN is enabled or **Down** when WLAN is disabled.
TxPkts	This is the number of transmitted packets on this port.
RxPkts	This is the number of received packets on this port.
Cols	This is the number of collisions on this port.
Tx B/s	This field shows the transmission speed in Bytes per second on this port.
Rx B/s	This field shows the reception speed in Bytes per second on this port.
Up Time	This is the total amount of time the line has been up.

Table 214 System Maintenance: Status Menu Fields (continued)

FIELD	DESCRIPTION
Ethernet Address	This is the MAC address of the port listed on the left.
IP Address	This is the IP address of the port listed on the left.
IP Mask	This is the IP mask of the port listed on the left.
DHCP	This is the DHCP setting of the port listed on the left.
System up Time	This is the total time the LAN-Cell has been on.
Wi-Fi bridged to	This field shows whether the Wi-Fi AP is set to be part of the LAN, DMZ or WLAN.
You may enter 1 to drop the WAN connection, 9 to reset the counters or [ESC] to return to menu 24.	

37.3 System Information and Console Port Speed

This section describes your system and allows you to choose different console port speeds. To get to the System Information and Console Port Speed:

1. Enter 24 to go to **Menu 24 - System Maintenance**.
2. Enter 2 to open **Menu 24.2 - System Information and Console Port Speed**.
3. From this menu you have two choices as shown in the next figure:

Figure 337 Menu 24.2: System Information and Console Port Speed

```
             Menu 24.2 - System Information and Console Port Speed

                    1. System Information
                    2. Console Port Speed

             Please enter selection:
```

37.3.1 System Information

System Information gives you information about your system as shown below. More specifically, it gives you information on your routing protocol, Ethernet address, IP address, etc.

Figure 338 Menu 24.2.1: System Maintenance: Information

```
                Menu 24.2.1 - System Maintenance - Information

                   Name: LAN-Cell
                   Routing: IP
                   ProxiOS F/W Version: V4.02(AQI.0)b2 | 11/29/2006
                   Country Code: 255

                   LAN
                     Ethernet Address: 00:13:49:00:00:01
                     IP Address: 192.168.1.1
                     IP Mask: 255.255.255.0
                     DHCP: Server


                         Press ESC or RETURN to Exit:
```

The following table describes the fields in this screen.

Table 215 Fields in System Maintenance: Information

FIELD	DESCRIPTION
Name	This is the LAN-Cell's system name + domain name assigned in menu 1. For example, System Name= xxx; Domain Name= baboo.mickey.com Name= xxx.baboo.mickey.com
Routing	Refers to the routing protocol used.
ProxiOS F/W Version	Refers to the version of Proxicast's Network Operating System software.
Country Code	Refers to the country code of the firmware.
LAN	
Ethernet Address	Refers to the Ethernet MAC (Media Access Control) address of your LAN-Cell.
IP Address	This is the IP address of the LAN-Cell in dotted decimal notation.
IP Mask	This shows the IP mask of the LAN-Cell.
DHCP	This field shows the DHCP setting of the LAN-Cell.
When finished viewing, press [ESC] or [ENTER] to exit.	

37.3.2 Console Port Speed

You can change the speed of the console port through **Menu 24.2.2 – Console Port Speed**. Your LAN-Cell supports 9600 (default), 19200, 38400, 57600, and 115200 bps for the console port. Press [SPACE BAR] and then [ENTER] to select the desired speed in menu 24.2.2, as shown next.

Figure 339 Menu 24.2.2: System Maintenance: Change Console Port Speed

```
            Menu 24.2.2 - System Maintenance - Change Console Port Speed

                            Console Port Speed: 9600


                        Press ENTER to Confirm or ESC to Cancel:Press
            Space Bar to Toggle.
```

37.4 Log and Trace

There are two logging facilities in the LAN-Cell. The first is the error logs and trace records that are stored locally. The second is the UNIX syslog facility for message logging.

37.4.1 Viewing Error Log

The first place you should look for clues when something goes wrong is the error/trace log. Follow the procedure below to view the local error/trace log:

1. Select option 24 from the main menu to open **Menu 24 - System Maintenance**.
2. From menu 24, select option 3 to open **Menu 24.3 - System Maintenance - Log and Trace**.
3. Select the first option from **Menu 24.3 - System Maintenance - Log and Trace** to display the error log in the system.

After the LAN-Cell finishes displaying, you will have the option to clear the error log.

Figure 340 Menu 24.3: System Maintenance: Log and Trace

```
            Menu 24.3 - System Maintenance - Log and Trace

            1. View Error Log
            2. UNIX Syslog

            4. Call-Triggering Packet


                   Please enter selection
```

Examples of typical error and information messages are presented in the following figure.

Figure 341 Examples of Error and Information Messages

```
52 Thu Jul  1 05:54:53 2004 PP05  ERROR Wireless LAN init fail, code=15
53 Thu Jul  1 05:54:53 2004 PINI  INFO  Channel 0 ok
54 Thu Jul  1 05:54:56 2004 PP05 -WARN  SNMP TRAP 3: interface 3: link up
55 Thu Jul  1 05:54:56 2004 PP0d  INFO  LAN promiscuous mode <0>
57 Thu Jul  1 05:54:56 2004 PP0d  INFO  LAN promiscuous mode <1>
58 Thu Jul  1 05:54:56 2004 PINI  INFO  Last errorlog repeat 1 Times
59 Thu Jul  1 05:54:56 2004 PINI  INFO  main: init completed
60 Thu Jul  1 05:55:26 2004 PSSV -WARN  SNMP TRAP 0: cold start
61 Thu Jul  1 05:56:56 2004 PINI  INFO  SMT Session Begin
62 Thu Jul  1 07:50:58 2004 PINI  INFO  SMT Session End
63 Thu Jul  1 07:53:28 2004 PINI  INFO  SMT Session Begin
Clear Error Log (y/n):
```

37.4.2 Syslog Logging

The LAN-Cell uses the syslog facility to log the CDR (Call Detail Record) and system messages to a syslog server. Syslog and accounting can be configured in **Menu 24.3.2 - System Maintenance - Syslog Logging**, as shown next.

Figure 342 Menu 24.3.2: System Maintenance: Syslog Logging

```
              Menu 24.3.2 - System Maintenance - Syslog Logging

                    Syslog:
                    Active= No
                    Syslog Server IP Address= 0.0.0.0
                    Log Facility= Local 1


                Press ENTER to Confirm or ESC to Cancel:
```

You need to configure the syslog parameters described in the following table to activate syslog then choose what you want to log.

Table 216 System Maintenance Menu Syslog Parameters

FIELD	DESCRIPTION
Syslog:	
Active	Press [SPACE BAR] and then [ENTER] to turn syslog on or off.
Syslog Server IP Address	Enter the server name or IP address of the syslog server that will log the selected categories of logs.
Log Facility	Press [SPACE BAR] and then [ENTER] to select a location. 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.
When finished configuring this screen, press [ENTER] to confirm or [ESC] to cancel.	

Your LAN-Cell sends five types of syslog messages. Some examples (not all LAN-Cell specific) of these syslog messages with their message formats are shown next:

1 CDR

CDR Message Format
SdcmdSyslogSend(SYSLOG_CDR, SYSLOG_INFO, String); String = board xx line xx channel xx, call xx, str board = the hardware board ID line = the WAN ID in a board Channel = channel ID within the WAN call = the call reference number which starts from 1 and increments by 1 for each new call str = C01 Outgoing Call dev xx ch xx (dev:device No. ch:channel No.) L02 Tunnel Connected(L2TP) C02 OutCall Connected xxxx (means connected speed) xxxxx (means Remote Call Number) L02 Call Terminated C02 Call Terminated
Jul 19 11:19:27 192.168.102.2 Proxicast: board 0 line 0 channel 0, call 1, C01 Outgoing Call dev=2 ch=0 40002
Jul 19 11:19:32 192.168.102.2 Proxicast: board 0 line 0 channel 0, call 1, C02 OutCall Connected 64000 40002
Jul 19 11:20:06 192.168.102.2 Proxicast: board 0 line 0 channel 0, call 1, C02 Call Terminated

2 Packet triggered

Packet triggered Message Format
SdcmdSyslogSend(SYSLOG_PKTTRI, SYSLOG_NOTICE, String); String = Packet trigger: Protocol=xx Data=xxxxxxxxxx…..x Protocol: (1:IP 2:IPX 3:IPXHC 4:BPDU 5:ATALK 6:IPNG) Data: We will send forty-eight Hex characters to the server
Jul 19 11:28:39 192.168.102.2 Proxicast: Packet Trigger: Protocol=1,
Data=4500003c100100001f010004c0a86614ca849a7b08004a5c020001006162636465666768696a6b6c6d6e6f7071727374
Jul 19 11:28:56 192.168.102.2 Proxicast: Packet Trigger: Protocol=1, Data=4500002c1b0140001f06b50ec0a86614ca849a7b0427001700195b3e00000000600220008cd40000020405b4
Jul 19 11:29:06 192.168.102.2 Proxicast: Packet Trigger: Protocol=1, Data=450000282401400001f06ac12c0a86614ca849a7b0427001700195b451d1430135004000077600000

3 Filter log

Filter log Message Format
SdcmdSyslogSend(SYSLOG_FILLOG, SYSLOG_NOTICE, String); String = IP[Src=xx.xx.xx.xx Dst=xx.xx.xx.xx prot spo=xxxx dpo=xxxx] S04>R01mD IP[…] is the packet header and S04>R01mD means filter set 4 (S) and rule 1 (R), match (m) drop (D). Src: Source Address Dst: Destination Address prot: Protocol ("TCP","UDP","ICMP") spo: Source port dpo: Destination portMar 03 10:39:43 202.132.155.97 Proxicast: GEN[fffffffffffnordff0080] }S05>R01mF Mar 03 10:41:29 202.132.155.97 Proxicast: GEN[00a0c5f502fnord010080] }S05>R01mF Mar 03 10:41:34 202.132.155.97 Proxicast: IP[Src=192.168.2.33 Dst=202.132.155.93 ICMP]}S04>R01mF Mar 03 11:59:20 202.132.155.97 Proxicast: GEN[00a0c5f502fnord010080] }S05>R01mF Mar 03 12:00:52 202.132.155.97 Proxicast: GEN[ffffffffffff0080] }S05>R01mF Mar 03 12:00:57 202.132.155.97 Proxicast: GEN[00a0c5f502010080] }S05>R01mF Mar 03 12:01:06 202.132.155.97 Proxicast: IP[Src=192.168.2.33 Dst=202.132.155.93 TCP spo=01170 dpo=00021]}S04>R01mF

4 PPP log

PPP Log Message Format
SdcmdSyslogSend(SYSLOG_PPPLOG, SYSLOG_NOTICE, String); String = ppp:Proto Starting / ppp:Proto Opening / ppp:Proto Closing / ppp:Proto Shutdown Proto = LCP / ATCP / BACP / BCP / CBCP / CCP / CHAP/ PAP / IPCP / IPXCP Jul 19 11:42:44 192.168.102.2 Proxicast: ppp:LCP Closing Jul 19 11:42:49 192.168.102.2 Proxicast: ppp:IPCP Closing Jul 19 11:42:54 192.168.102.2 Proxicast: ppp:CCP Closing

5 Firewall log

Firewall Log Message Format

```
SdcmdSyslogSend(SYSLOG_FIREWALL, SYSLOG_NOTICE, buf);
buf = IP[Src=xx.xx.xx.xx : spo=xxxx Dst=xx.xx.xx.xx : dpo=xxxx | prot | rule | action]
Src: Source Address
spo: Source port (empty means no source port information)
Dst: Destination Address
dpo: Destination port (empty means no destination port information)
prot: Protocol ("TCP","UDP","ICMP", "IGMP", "GRE", "ESP")
rule: <a,b> where a means "set" number; b means "rule" number.
Action: nothing(N) block (B) forward (F)
08-01-200011:48:41Local1.Notice192.168.10.10RAS: FW 172.21.1.80     :137  ->172.21.1.80
:137  |UDP|default permit:<2,0>|B
08-01-200011:48:41Local1.Notice192.168.10.10RAS: FW 192.168.77.88   :520  ->192.168.77.88
:520  |UDP|default permit:<2,0>|B
08-01-200011:48:39Local1.Notice192.168.10.10RAS: FW 172.21.1.50     ->172.21.1.50
|IGMP<2>|default permit:<2,0>|B
08-01-200011:48:39Local1.Notice192.168.10.10RAS: FW 172.21.1.25     ->172.21.1.25
|IGMP<2>|default permit:<2,0>|B
```

37.4.3 Call-Triggering Packet

Call-Triggering Packet displays information about the packet that triggered a dial-out call in an easy readable format. Equivalent information is available in menu 24.1 in hex format. An example is shown next.

Figure 343 Call-Triggering Packet Example

```
IP Frame: ENET0-RECV Size:  44/  44   Time: 17:02:44.262
 Frame Type:

   IP Header:
     IP Version                = 4
     Header Length             = 20
     Type of Service           = 0x00 (0)
     Total Length              = 0x002C (44)
     Identification            = 0x0002 (2)
     Flags                     = 0x00
     Fragment Offset           = 0x00
     Time to Live              = 0xFE (254)
     Protocol                  = 0x06 (TCP)
     Header Checksum           = 0xFB20 (64288)
     Source IP                 = 0xC0A80101 (192.168.1.1)
     Destination IP            = 0x00000000 (0.0.0.0)

   TCP Header:
     Source Port               = 0x0401 (1025)
     Destination Port          = 0x000D (13)
     Sequence Number           = 0x05B8D000 (95997952)
     Ack Number                = 0x00000000 (0)
     Header Length             = 24
     Flags                     = 0x02 (....S.)
     Window Size               = 0x2000 (8192)
     Checksum                  = 0xE06A (57450)
     Urgent Ptr                = 0x0000 (0)
     Options                   =
         0000: 02 04 02 00

   RAW DATA:
    0000: 45 00 00 2C 00 02 00 00-FE 06 FB 20 C0 A8 01 01  E......... ....
     0010: 00 00 00 00 04 01 00 0D-05 B8 D0 00 00 00 00 00
................
     0020: 60 02 20 00 E0 6A 00 00-02 04 02 00
Press any key to continue...
```

37.5 Diagnostic

The diagnostic facility allows you to test the different aspects of your LAN-Cell to determine if it is working properly. Menu 24.4 allows you to choose among various types of diagnostic tests to evaluate your system, as shown next.

Follow the procedure below to get to **Menu 24.4 - System Maintenance - Diagnostic**.

1. From the main menu, select option 24 to open **Menu 24 - System Maintenance**.
2. From this menu, select option 4. Diagnostic. This will open **Menu 24.4 - System Maintenance - Diagnostic**.

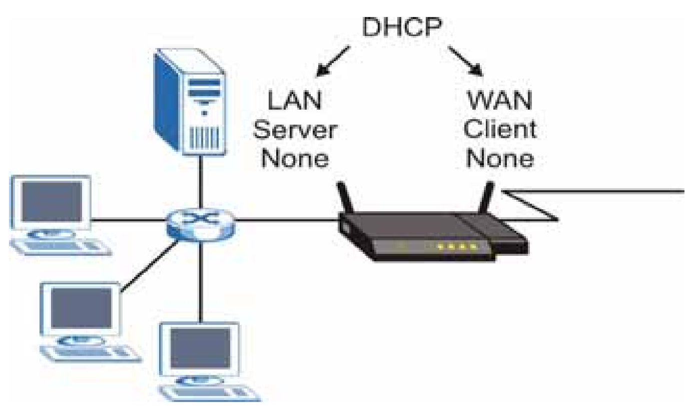
Figure 344 Menu 24.4: System Maintenance: Diagnostic

```
                Menu 24.4 - System Maintenance - Diagnostic


                 TCP/IP
                   1. Ping Host
                   2. WAN DHCP Release
                   3. WAN DHCP Renewal
                   4. PPPoE/PPTP/Cellular Setup Test

                 System
                   11. Reboot System


                    Enter Menu Selection Number:

                    WAN=
                    Host IP Address= N/A
```

37.5.1 WAN DHCP

DHCP functionality can be enabled on the LAN or WAN as shown in Figure 345 on page 527. LAN DHCP has already been discussed. The LAN-Cell can act either as a WAN DHCP client (**IP Address Assignment** field in menu 4 or menu 11.x.2 is **Dynamic** and the **Encapsulation** field in menu 4 or menu 11 is **Ethernet**) or **None**, (when you have a static IP). The **WAN Release** and **Renewal** fields in menu 24.4 conveniently allow you to release and/or renew the assigned WAN IP address, subnet mask and default gateway in a fashion similar to winipcfg.

Figure 345 WAN & LAN DHCP



The following table describes the diagnostic tests available in menu 24.4 for your LAN-Cell and associated connections.

Table 217 System Maintenance Menu Diagnostic

FIELD	DESCRIPTION
Ping Host	Enter 1 to ping any machine (with an IP address) on your LAN, DMZ, WLAN or WAN. Enter its IP address in the **Host IP Address** field below.
WAN DHCP Release	Enter 2 to release your WAN DHCP settings.
WAN DHCP Renewal	Enter 3 to renew your WAN DHCP settings.
PPPoE/PPTP/Cellular Setup Test	Enter 4 to test the Internet setup. You can also test the Internet setup in **Menu 4 - WAN ISP Setup**. Please refer to Chapter 27 on page 447 for more details. This feature is only available for a 3G connection or dial-up connections using PPPoE or PPTP encapsulation.
Reboot System	Enter 11 to reboot the LAN-Cell.
WAN	If you entered 2, 3 or 4 in the **Enter Menu Selection Number** field, enter the number of the WAN interface in this field. 1=Ethernet WAN, 2=Cellular WAN
Host IP Address	If you entered 1in the **Enter Menu Selection Number** field, then enter the IP address of the computer you want to ping in this field.
Enter the number of the selection you would like to perform or press [ESC] to cancel.	

38

Firmware and Configuration File Maintenance

This chapter tells you how to back up and restore your configuration file as well as upload new firmware and a new configuration file.

38.1 Introduction

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

38.2 Filename Conventions

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

ProxiOS (Proxicast Network Operating System sometimes referred to as the "ras" file) is the system firmware and has a "bin" filename extension. With many FTP and TFTP clients, the filenames are similar to those seen next.

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

This is a sample FTP session showing the transfer of the computer file " firmware.bin" to the LAN-Cell.

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

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

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

The following table is a summary. Please note that the internal filename refers to the filename on the LAN-Cell and the external filename refers to the filename not on the LAN-Cell, that is, on your computer, local network or FTP site and so the name (but not the extension) may vary. After uploading new firmware, see the **ProxiOS F/W Version** field in **Menu 24.2.1 - System Maintenance - Information** to confirm that you have uploaded the correct firmware version. The AT command is the command you enter after you press “y” when prompted in the SMT menu to go into debug mode.

Table 218 Filename Conventions

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

38.3 Backup Configuration

The LAN-Cell displays different messages explaining different ways to backup, restore and upload files in menus 24.5, 24.6, 24. 7.1 and 24.7.2 depending on whether you use the console port or Telnet.

Option 5 from **Menu 24 - System Maintenance** allows you to backup the current LAN-Cell configuration to your computer. Backup is highly recommended once your LAN-Cell is functioning properly. FTP is the preferred method for backing up your current configuration to your computer since it is faster. You can also perform backup and restore using menu 24 through the console port. Any serial communications program should work fine; however, you must use Xmodem protocol to perform the download/upload and you don’t have to rename the files.

Please note that terms “download” and “upload” are relative to the computer. Download means to transfer from the LAN-Cell to the computer, while upload means from your computer to the LAN-Cell.

38.3.1 Backup Configuration

Follow the instructions as shown in the next screen.

Figure 346 Telnet into Menu 24.5

```
                    Menu 24.5 - Backup Configuration

 To transfer the configuration file to your workstation, follow the
 procedure below:

    1. Launch the FTP client on your workstation.
    2. Type "open" and the IP address of your router. Then type
       "root" and SMT password as requested.
    3. Locate the 'rom-0' file.
    4. Type 'get rom-0' to back up the current router
       configuration to your workstation.

 For details on FTP commands, please consult the documentation of your FTP
 client program.  For details on backup using TFTP (note that you must
 remain in this menu to back up using TFTP), please see your router manual.


 Press ENTER to Exit:
```

38.3.2 Using the FTP Command from the Command Line

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

38.3.3 Example of FTP Commands from the Command Line

Figure 347 FTP Session Example

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

38.3.4 GUI-based FTP Clients

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

Table 219 General Commands for GUI-based FTP Clients

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

38.3.5 File Maintenance Over WAN

TFTP, FTP and Telnet over the WAN will not work when:

1. The firewall is active (turn the firewall off in menu 21.2 or create a firewall rule to allow access from the WAN).
2. You have disabled Telnet service in menu 24.11.
3. You have applied a filter in menu 3.1 (LAN) or in menu 11.5 (WAN) to block Telnet service.
4. The IP you entered in the **Secure Client IP** field in menu 24.11 does not match the client IP. If it does not match, the LAN-Cell will disconnect the Telnet session immediately.
5. You have an SMT console session running.

38.3.6 Backup Configuration Using TFTP

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

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

1. Use telnet from your computer to connect to the LAN-Cell and log in. Because TFTP does not have any security checks, the LAN-Cell records the IP address of the telnet client and accepts TFTP requests only from this address.
2. Put the SMT in command interpreter (CI) mode by entering 8 in **Menu 24 – System Maintenance**.
3. Enter command “sys stdio 0” to disable the SMT timeout, so the TFTP transfer will not be interrupted. Enter command “sys stdio 5” to restore the five-minute SMT timeout (default) when the file transfer is complete.

4 Launch the TFTP client on your computer and connect to the LAN-Cell. Set the transfer mode to binary before starting data transfer.

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

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

38.3.7 TFTP Command Example

The following is an example TFTP command:

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

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

38.3.8 GUI-based TFTP Clients

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

Table 220 General Commands for GUI-based TFTP Clients

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

Refer to Section 38.3.5 on page 532 to read about configurations that disallow TFTP and FTP over WAN.

38.3.9 Backup Via Console Port

Back up configuration via console port by following the HyperTerminal procedure shown next. Procedures using other serial communications programs should be similar.

1 Display menu 24.5 and enter “y” at the following screen.

Figure 348 System Maintenance: Backup Configuration

```
Ready to backup Configuration via Xmodem.
Do you want to continue (y/n):
```

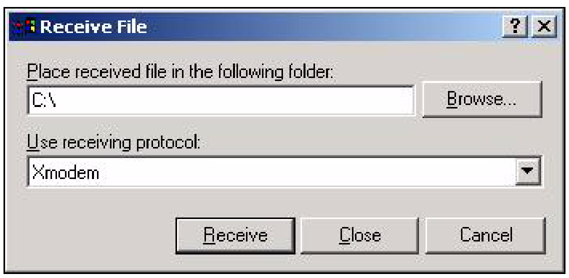
2 The following screen indicates that the Xmodem download has started.

Figure 349 System Maintenance: Starting Xmodem Download Screen

```
You can enter ctrl-x to terminate operation any
time.
Starting XMODEM download...
```

3 Run the HyperTerminal program by clicking **Transfer**, then **Receive File** as shown in the following screen.

Figure 350 Backup Configuration Example



Type a location for storing the configuration file or click **Browse** to look for one.

Choose the **Xmodem** protocol.

Then click **Receive**.

4 After a successful backup you will see the following screen. Press any key to return to the SMT menu.

Figure 351 Successful Backup Confirmation Screen

```
** Backup Configuration completed. OK.
### Hit any key to continue.###
```

38.4 Restore Configuration

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

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

WARNING!
Do not interrupt the file transfer process as this may PERMANENTLY DAMAGE YOUR LAN-Cell. When the Restore Configuration process is complete, the LAN-Cell will automatically restart.

38.4.1 Restore Using FTP

For details about backup using (T)FTP please refer to earlier sections on FTP and TFTP file upload in this chapter.

Figure 352 Telnet into Menu 24.6

```
             Menu 24.6 -- System Maintenance - Restore Configuration

     To transfer the firmware and configuration file to your workstation,
     follow the procedure below:

     1. Launch the FTP client on your workstation.
     2. Type "open" and the IP address of your router. Then type "root" and
     SMT password as requested.
     3. Type "put backupfilename rom-0" where backupfilename is the name of
     your backup configuration file on your workstation and rom-0 is the
     remote file name on the router. This restores the configuration to
     your router.
     4. The system reboots automatically after a successful file transferFor
     details on FTP commands, please consult the documentation of your
     FTPclient program.

     For details on backup using TFTP (note that you must remain in this menu
     to back up using TFTP), please see your router manual.

     Press ENTER to Exit:
```

1. Launch the FTP client on your computer.
2. Enter “open”, followed by a space and the IP address of your LAN-Cell.
3. Press [ENTER] when prompted for a username.
4. Enter your password as requested (the default is “1234”).
5. Enter “bin” to set transfer mode to binary.
6. Find the “rom” file (on your computer) that you want to restore to your LAN-Cell.
7. Use “put” to transfer files from the LAN-Cell to the computer, for example, “put config.rom rom-0” transfers the configuration file “config.rom” on your computer to the LAN-Cell. See earlier in this chapter for more information on filename conventions.

8 Enter "quit" to exit the ftp prompt. The LAN-Cell will automatically restart after a successful restore process.

38.4.2 Restore Using FTP Session Example

Figure 353 Restore Using FTP Session Example

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

Refer to Section 38.3.5 on page 532 to read about configurations that disallow TFTP and FTP over WAN.

38.4.3 Restore Via Console Port

Restore configuration via console port by following the HyperTerminal procedure shown next. Procedures using other serial communications programs should be similar.

1 Display menu 24.6 and enter "y" at the following screen.

Figure 354 System Maintenance: Restore Configuration

```
Ready to restore Configuration via Xmodem.
Do you want to continue (y/n):
```

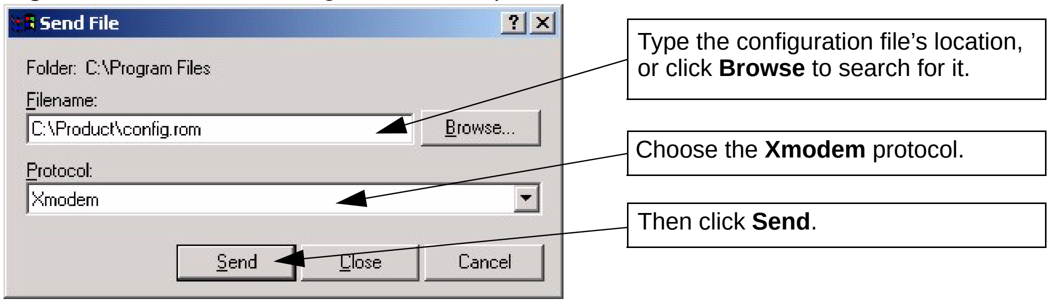
2 The following screen indicates that the Xmodem download has started.

Figure 355 System Maintenance: Starting Xmodem Download Screen

```
Starting XMODEM download (CRC mode) ...CCCCCCCCC
```

3 Run the HyperTerminal program by clicking **Transfer**, then **Send File** as shown in the following screen.

Figure 356 Restore Configuration Example



4 After a successful restoration you will see the following screen. Press any key to restart the LAN-Cell and return to the SMT menu.

Figure 357 Successful Restoration Confirmation Screen

```
Save to ROM
Hit any key to start system reboot.
```

38.5 Uploading Firmware and Configuration Files

This section shows you how to upload firmware and configuration files. You can upload configuration files by following the procedure in Section 38.4 on page 534 or by following the instructions in **Menu 24.7.2 - System Maintenance - Upload System Configuration File** (for console port).

WARNING!
Do not interrupt the file transfer process as this may PERMANENTLY DAMAGE YOUR LAN-Cell.

38.5.1 Firmware File Upload

FTP is the preferred method for uploading the firmware and configuration. To use this feature, your computer must have an FTP client.

When you telnet into the LAN-Cell, you will see the following screens for uploading firmware and the configuration file using FTP.

Figure 358 Telnet Into Menu 24.7.1: Upload System Firmware

```
          Menu 24.7.1 - System Maintenance - Upload System Firmware

     To upload the system firmware, follow the procedure below:

       1. Launch the FTP client on your workstation.
       2. Type "open" and the IP address of your system. Then type "root" and
     SMT password as requested.
       3. Type "put firmwarefilename ras" where "firmwarefilename" is the
     name of your firmware upgrade file on your workstation and "ras" is the
     remote file name on the system.
       4. The system reboots automatically after a successful firmware
     upload.

     For details on FTP commands, please consult the documentation of your
     FTP client program. For details on uploading system firmware using TFTP
     (note that you must remain on this menu to upload system firmware using
     TFTP), please see your manual.

     Press ENTER to Exit:
```

38.5.2 Configuration File Upload

You see the following screen when you telnet into menu 24.7.2.

Figure 359 Telnet Into Menu 24.7.2: System Maintenance

```
     Menu 24.7.2 - System Maintenance - Upload System Configuration File

     To upload the system configuration file, follow the procedure below:

       1. Launch the FTP client on your workstation.
       2. Type "open" and the IP address of your system. Then type "root" and
     SMT password as requested.
       3. Type "put configurationfilename rom-0" where
     "configurationfilename" is the name of your system configuration file on
     your workstation, which will be transferred to the "rom-0" file on the
     system.
       4. The system reboots automatically after the upload system
     configuration file process is complete.

     For details on FTP commands, please consult the documentation of your
     FTP client program. For details on uploading configuration file using
     TFTP (note that you must remain on this menu to upload configuration
     file using TFTP), please see your manual.

     Press ENTER to Exit:
```

To upload the firmware and the configuration file, follow these examples

38.5.3 FTP File Upload Command from the DOS Prompt Example

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

38.5.4 FTP Session Example of Firmware File Upload

Figure 360 FTP Session Example of Firmware File Upload

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

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

Refer to Section 38.3.5 on page 532 to read about configurations that disallow TFTP and FTP over WAN.

38.5.5 TFTP File Upload

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

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

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

2 Put the SMT in command interpreter (CI) mode by entering 8 in **Menu 24 – System Maintenance**.
3 Enter the command “sys stdio 0” to disable the console timeout, so the TFTP transfer will not be interrupted. Enter “command sys stdio 5” to restore the five-minute console timeout (default) when the file transfer is complete.
4 Launch the TFTP client on your computer and connect to the LAN-Cell. Set the transfer mode to binary before starting data transfer.
5 Use the TFTP client (see the example below) to transfer files between the LAN-Cell and the computer. The file name for the firmware is “ras”.

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

38.5.6 TFTP Upload Command Example

The following is an example TFTP command:

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

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

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

38.5.7 Uploading Via Console Port

FTP or TFTP are the preferred methods for uploading firmware to your LAN-Cell. However, in the event of your network being down, uploading files is only possible with a direct connection to your LAN-Cell via the console port. Uploading files via the console port under normal conditions is not recommended since FTP or TFTP is faster. Any serial communications program should work fine; however, you must use the Xmodem protocol to perform the download/upload.

38.5.8 Uploading Firmware File Via Console Port

1 Select 1 from **Menu 24.7 – System Maintenance – Upload Firmware** to display **Menu 24.7.1 - System Maintenance - Upload System Firmware**, and then follow the instructions as shown in the following screen.

Figure 361 Menu 24.7.1 As Seen Using the Console Port

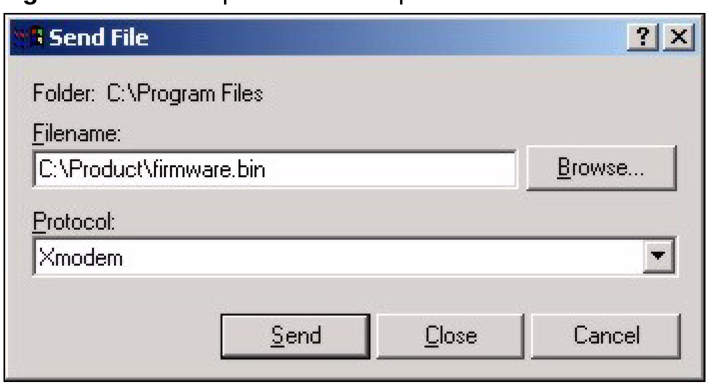
```
          Menu 24.7.1 - System Maintenance - Upload System Firmware

    To upload system firmware:
    1. Enter "y" at the prompt below to go into debug mode.
    2. Enter "atur" after "Enter Debug Mode" message.
    3. Wait for "Starting XMODEM upload" message before activating
    Xmodem upload on your terminal.
    4. After successful firmware upload, enter "atgo" to restart the router.

    Warning: Proceeding with the upload will erase the current system
    firmware.

            Do You Wish To Proceed:(Y/N)
```

2 After the "Starting Xmodem upload" message appears, activate the Xmodem protocol on your computer. Follow the procedure as shown previously for the HyperTerminal program. The procedure for other serial communications programs should be similar.

38.5.9 Example Xmodem Firmware Upload Using HyperTerminal

Click **Transfer**, then **Send File** to display the following screen.

Figure 362 Example Xmodem Upload



After the firmware upload process has completed, the LAN-Cell will automatically restart.

38.5.10 Uploading Configuration File Via Console Port

1 Select 2 from **Menu 24.7 – System Maintenance – Upload Firmware** to display **Menu 24.7.2 - System Maintenance - Upload System Configuration File**. Follow the instructions as shown in the next screen.

Figure 363 Menu 24.7.2 As Seen Using the Console Port

```
Menu 24.7.2 - System Maintenance - Upload System Configuration File

To upload system configuration file:
1. Enter "y" at the prompt below to go into debug mode.
2. Enter "atlc" after "Enter Debug Mode" message.
3. Wait for "Starting XMODEM upload" message before activating
   Xmodem upload on your terminal.
4. After successful firmware upload, enter "atgo" to restart
   the system.

Warning:
1. Proceeding with the upload will erase the current
configuration file.
2. The system's console port speed (Menu 24.2.2) may change when it is
restarted; please adjust your terminal's speed accordingly. The password
may change (menu 23), also.
3. When uploading the DEFAULT configuration file, the console
port speed will be reset to 9600 bps and the password to "1234".

         Do You Wish To Proceed:(Y/N)
```

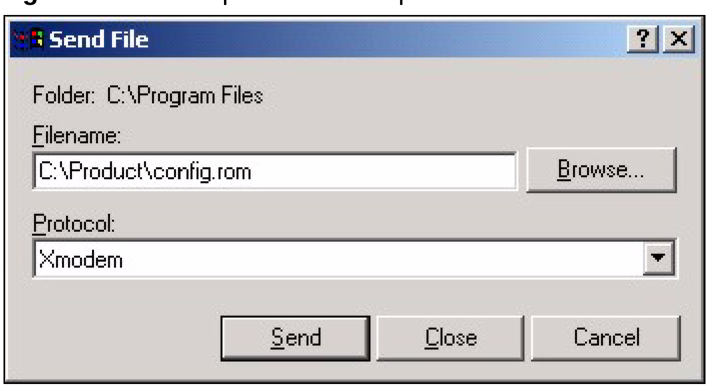
2 After the "Starting Xmodem upload" message appears, activate the Xmodem protocol on your computer. Follow the procedure as shown previously for the HyperTerminal program. The procedure for other serial communications programs should be similar.

3 Enter “atgo” to restart the LAN-Cell.

38.5.11 Example Xmodem Configuration Upload Using HyperTerminal

Click **Transfer**, then **Send File** to display the following screen.

Figure 364 Example Xmodem Upload



After the configuration upload process has completed, restart the LAN-Cell by entering “atgo”.

39

System Maint. Menus 8 to 10

This chapter leads you through SMT menus 24.8 to 24.10.

39.1 Command Interpreter Mode

The Command Interpreter (CI) is a part of the main router firmware. The CI provides much of the same functionality as the SMT, while adding some low-level setup and diagnostic functions. Enter the CI from the SMT by selecting menu 24.8. Access can be by Telnet or by a serial connection to the console port, although some commands are only available with a serial connection. See the included disk or proxicast.com for more detailed information on CI commands. Enter 8 from **Menu 24 - System Maintenance**.

Use of undocumented commands or misconfiguration can damage the unit and possibly render it unusable.

Figure 365 Command Mode in Menu 24

```
              Menu 24 - System Maintenance

                 1.  System Status
                 2.  System Information and Console Port Speed
                 3.  Log and Trace
                 4.  Diagnostic
                 5.  Backup Configuration
                 6.  Restore Configuration
                 7.  Upload Firmware
                 8.  Command Interpreter Mode
                 9.  Call Control
                 10. Time and Date Setting
                 11. Remote Management Setup


              Enter Menu Selection Number:
```

39.1.1 Command Syntax

The command keywords are in `courier new` font.

Enter the command keywords exactly as shown, do not abbreviate.

The required fields in a command are enclosed in angle brackets <>.

The optional fields in a command are enclosed in square brackets [].

The | symbol means “or”.

For example,

```
sys filter netbios config <type> <on|off>
```

means that you must specify the type of netbios filter and whether to turn it on or off.

39.1.2 Command Usage

A list of commands can be found by typing `help` or `?` at the command prompt. Always type the full command. Type `exit` to return to the SMT main menu when finished.

Figure 366 Valid Commands

```
Copyright (c) 1994 - 2007 Proxicast LLC
LAN-Cell> ?
Valid commands are:
sys             ls              exit            device
ether           aux             config          wwan
wlan            ip              ipsec           bm
certificates    8021x           radius          radserv
wcfg
LAN-Cell>
```

The following table describes some commands in this screen.

Table 221 Valid Commands

COMMAND	DESCRIPTION
sys	The system commands display device information and configure device settings.
ls	The load sharing commands allow you to configure load balancing.
exit	This command returns you to the SMT main menu.
device	The device commands deal with the dial backup connection.
ether	These commands display Ethernet information and configure Ethernet settings.
aux	These commands display dial backup information and control dial backup connections.
config	These commands configure firewall and anti-spam settings.
wwan	These commands configure the 3G cellular WAN interface
wlan	These commands configure the internal 801.11 Wi-Fi- Access Point
ip	These commands display IP information and configure IP settings.
ipsec	These commands display IPSec information and configure IPSec settings.
bm	These commands configure bandwidth management settings and display bandwidth management information.
certificates	These commands display certificate information and configure certificate settings.
8021x	These commands configure 802.1x settings and display 802.1x information.

Table 221 Valid Commands

COMMAND	DESCRIPTION
radius	These commands display remote RADIUS server access information and configure RADIUS access settings.
radserv	These command configure the Local RADIUS server settings
wcfg	These command configure the SSID & security settings of the Wi-Fi AP.

39.2 Call Control Support

The LAN-Cell provides two call control functions: budget management and call history. Please note that this menu is only applicable when **Encapsulation** is set to **PPPoE** or **PPTP** in menu 4 or menu 11.1.

Budget Management is unrelated to the Cell-Sentry budget feature. Configure Cell-Sentry budgets using the web configurator (see Section 5.4.2 on page 118)

The budget management function allows you to set a limit on the total outgoing call time of the LAN-Cell within certain times. When the total outgoing call time exceeds the limit, the current call will be dropped and any future outgoing calls will be blocked.

Call history chronicles preceding incoming and outgoing calls.

To access the call control menu, select option 9 in menu 24 to go to **Menu 24.9 - System Maintenance - Call Control**, as shown in the next table.

Figure 367 Call Control

```
              Menu 24.9 - System Maintenance - Call Control

                  1.Budget Management
                  2.Call History

              Enter Menu Selection Number:
```

39.2.1 Budget Management

Menu 24.9.1 shows the budget management statistics for outgoing calls. Enter 1 from **Menu 24.9 - System Maintenance - Call Control** to bring up the following menu. Not all fields are available on all models.

Figure 368 Budget Management

```
               Menu 24.9.1 - Budget Management

     Remote Node   Connection Time/Total Budget   Elapsed Time/Total Period

   1.WAN_1                  No Budget                  No Budget

   2.WAN_2                  No Budget                  No Budget

   3.Dial                   No Budget                  No Budget


                 Reset Node (0 to update screen):
```

The total budget is the time limit on the accumulated time for outgoing calls to a remote node. When this limit is reached, the call will be dropped and further outgoing calls to that remote node will be blocked. After each period, the total budget is reset. The default for the total budget is 0 minutes and the period is 0 hours, meaning no budget control. You can reset the accumulated connection time in this menu by entering the index of a remote node. Enter 0 to update the screen. The budget and the reset period can be configured in menu 11.1 for the remote node.

Table 222 Budget Management

FIELD	DESCRIPTION	EXAMPLE
Remote Node	Enter the index number of the remote node you want to reset (just one in this case)	1
Connection Time/ Total Budget	This is the total connection time that has gone by (within the allocated budget that you set in menu 11.1).	5/10 means that 5 minutes out of a total allocation of 10 minutes have lapsed.
Elapsed Time/Total Period	The period is the time cycle in hours that the allocation budget is reset (see menu 11.1.) The elapsed time is the time used up within this period.	0.5/1 means that 30 minutes out of the 1-hour time period has lapsed.
Enter “0” to update the screen or press [ESC] to return to the previous screen.		

39.2.2 Call History

This is the second option in **Menu 24.9 - System Maintenance - Call Control**. It displays information about past incoming and outgoing calls. Enter 2 from **Menu 24.9 - System Maintenance - Call Control** to bring up the following menu.

Figure 369 Call History

```
    Menu 24.9.2 - Call History

        Phone Number   Dir    Rate    #call   Max   Min  Total
     1.
     2.
     3.
     4.
     5.
     6.
     7.
     8.
     9.
    10.

    Enter Entry to Delete(0 to exit):
```

The following table describes the fields in this screen.

Table 223 Call History

FIELD	DESCRIPTION
Phone Number	The PPPoE service names are shown here.
Dir	This shows whether the call was incoming or outgoing.
Rate	This is the transfer rate of the call.
#call	This is the number of calls made to or received from that telephone number.
Max	This is the length of time of the longest telephone call.
Min	This is the length of time of the shortest telephone call.
Total	This is the total length of time of all the telephone calls to/from that telephone number.
You may enter an entry number to delete it or ‘”0” to exit.	

39.3 Time and Date Setting

The LAN-Cell’s Real Time Chip (RTC) keeps track of the time and date. There is also a software mechanism to set the time manually or get the current time and date from an external server when you turn on your LAN-Cell. Menu 24.10 allows you to update the time and date settings of your LAN-Cell. The real time is then displayed in the LAN-Cell error logs and firewall logs.

Select menu 24 in the main menu to open **Menu 24 - System Maintenance**, as shown next.

Figure 370 Menu 24: System Maintenance

```
                    Menu 24 - System Maintenance

               1.  System Status
               2.  System Information and Console Port Speed
               3.  Log and Trace
               4.  Diagnostic
               5.  Backup Configuration
               6.  Restore Configuration
               7.  Upload Firmware
               8.  Command Interpreter Mode
               9.  Call Control
              10. Time and Date Setting
              11. Remote Management Setup


                  Enter Menu Selection Number:
```

Enter 10 to go to **Menu 24.10 - System Maintenance - Time and Date Setting** to update the time and date settings of your LAN-Cell as shown in the following screen.

Figure 371 Menu 24.10 System Maintenance: Time and Date Setting

```
              Menu 24.10 - System Maintenance - Time and Date Setting

              Time Protocol= NTP (RFC-1305)
              Time Server Address= 0.pool.ntp.org

              Current Time:                         08 : 24 : 26
              New Time (hh:mm:ss):                  N/A  N/A  N/A

              Current Date:                         2005 - 07 - 27
              New Date (yyyy-mm-dd):                N/A    N/A  N/A

              Time Zone= GMT

              Daylight Saving= No
              Start Date (mm-nth-week-hr):          Jan. - 1st  - Sun. -  00
              End Date (mm-nth-week-hr):            Jan. - 1st  - Sun. -  00


                Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this screen.

Table 224 Menu 24.10 System Maintenance: Time and Date Setting

FIELD	DESCRIPTION
Time Protocol	Enter the time service protocol that your timeserver uses. Not all time servers support all protocols, so you may have to check with your ISP/network administrator or use trial and error to find a protocol that works. The main differences between them are 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 **Manual** to enter the new time and new date manually.
Time Server Address	Enter the IP address or domain name of your timeserver. Check with your ISP/ network administrator if you are unsure of this information.
Current Time	This field displays an updated time only when you reenter this menu.
New Time	Enter the new time in hour, minute and second format. This field is available when you select **Manual** in the **Time Protocol** field.
Current Date	This field displays an updated date only when you reenter this menu.
New Date	Enter the new date in year, month and day format. This field is available when you select **Manual** in the **Time Protocol** field.
Time Zone	Press [SPACE BAR] and then [ENTER] to set the time difference between your time zone and Greenwich Mean Time (GMT).
Daylight Saving	Daylight Saving Time 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 daylight time in the evenings. If you use daylight savings time, then choose **Yes**.
Start Date (mm-nth-week-hr)	Configure the day and time when Daylight Saving Time starts if you selected **Yes** in the **Daylight Saving** field. The **hr** field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time starts in most parts of the United States on the first Sunday of April. Each time zone in the United States starts using Daylight Saving Time at 2 A.M. local time. So in the United States you would select **Apr.**, **1st**, **Sun.** and type 02 in the **hr** field. Daylight Saving Time starts in the European Union on the last Sunday of March. All of the time zones in the European Union start using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select **Mar.**, **Last**, **Sun.** The time you type in the **hr** field depends on your time zone. In Germany for instance, you would type 02 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
End Date (mm-nth-week-hr)	Configure the day and time when Daylight Saving Time ends if you selected **Yes** in the **Daylight Saving** field. The **hr** field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time ends in the United States on the last Sunday of October. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So in the United States you would select **Oct.**, **Last**, **Sun.** and type 02 in the **hr** field. Daylight Saving Time ends in the European Union on the last Sunday of October. All of the time zones in the European Union stop using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select **Oct.**, **Last**, **Sun.** The time you type in the **hr** field depends on your time zone. In Germany for instance, you would type 02 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
Once you have filled in this menu, press [ENTER] at the message “Press ENTER to Confirm or ESC to Cancel“ to save your configuration, or press [ESC] to cancel.	

40

Remote Management

This chapter covers remote management found in SMT menu 24.11.

40.1 Remote Management

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

When you configure remote management to allow management from any network except the LAN, you still need to configure a firewall rule to allow access. See Chapter 9 on page 181 for details on configuring firewall rules.

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

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

Enter 11 from menu 24 to bring up **Menu 24.11 - Remote Management Control**.

Figure 372 Menu 24.11 – Remote Management Control

```
                 Menu 24.11 - Remote Management Control

     TELNET Server:     Port = 23         Access = Disable
                        Secure Client IP = 0.0.0.0
     FTP Server:        Port = 21         Access = LAN+WAN+DMZ+WLAN+CELL
                        Secure Client IP = 0.0.0.0
     SSH Server:        Certificate = auto_generated_self_signed_cert
                        Port = 22         Access = LAN+WAN+DMZ+WLAN+CELL
                        Secure Client IP = 0.0.0.0
     HTTPS Server:      Certificate = auto_generated_self_signed_cert
                        Authenticate Client Certificates = No
                        Port = 443        Access = LAN+WAN+DMZ+WLAN+CELL
                        Secure Client IP = 0.0.0.0
     HTTP Server:       Port = 80         Access = LAN+WAN+DMZ+WLAN+CELL
                        Secure Client IP = 0.0.0.0
     SNMP Service:      Port = 161        Access = LAN+WAN+DMZ+WLAN+CELL
                        Secure Client IP = 0.0.0.0
     DNS Service:       Port = 53         Access = LAN+WAN+DMZ+WLAN+CELL
                        Secure Client IP = 0.0.0.0

                 Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this screen.

Table 225 Menu 24.11 – Remote Management Control

FIELD	DESCRIPTION
Telnet Server FTP Server SSH Server HTTPS Server HTTP Server SNMP Service DNS Service	Each of these read-only labels denotes a service that you may use to remotely manage the LAN-Cell.
Port	This field shows the port number for the service or protocol. You may change the port number if needed, but you must use the same port number to access the LAN-Cell.
Access	Select the access interfaces (if any) by pressing [SPACE BAR], then [ENTER] to choose the correct combination or select **Disable** to prevent remote access via this port from all interfaces.
Secure Client IP	The default 0.0.0.0 allows any client to use this service to remotely manage the LAN-Cell. Enter an IP address to restrict access to a client with a matching IP address.
Certificate	Press [SPACE BAR] and then [ENTER] to select the certificate that the LAN-Cell will use to identify itself. The LAN-Cell is the SSL server and must always authenticate itself to the SSL client (the computer which requests the HTTPS connection with the LAN-Cell).

Table 225 Menu 24.11 – Remote Management Control (continued)

FIELD	DESCRIPTION
Authenticate Client Certificates	Select **Yes** by pressing [SPACE BAR], then [ENTER] to require the SSL client to authenticate itself to the LAN-Cell by sending the LAN-Cell a certificate. To do that the SSL client must have a CA-signed certificate from a CA that has been imported as a trusted CA on the LAN-Cell (see Appendix G on page 629 for details).
Once you have filled in this menu, press [ENTER] at the message "Press ENTER to Confirm or ESC to Cancel" to save your configuration, or press [ESC] to cancel.	

40.1.1 Remote Management Limitations

Remote management over LAN or WAN will not work when:

1. A filter in menu 3.1 (LAN) or in menu 11.5 (WAN) is applied to block a Telnet, FTP or Web service.
2. You have disabled that service in menu 24.11.
3. The IP address in the **Secure Client IP** field (menu 24.11) does not match the client IP address. If it does not match, the LAN-Cell will disconnect the session immediately.
4. There is an SMT console session running.
5. There is already another remote management session with an equal or higher priority running. You may only have one remote management session running at one time.
6. There is a firewall rule that blocks it.

41

IP Policy Routing

This chapter covers setting and applying policies used for IP routing.

41.1 IP Routing Policy Summary

Menu 25 shows the summary of a policy rule, including the criteria and the action of a single policy, and whether a policy is active or not. Each policy contains two lines. The former part is the criteria of the incoming packet and the latter is the action. Between these two parts, separator "|" means the action is taken on criteria matched and separator "=" means the action is taken on criteria not matched.

Figure 373 Menu 25: Sample IP Routing Policy Summary

```
                         Menu 25 - IP Routing Policy Summary

   #   A                          Criteria/Action
   --- - -------------------------------------------------------
   001 N SA=1.1.1.1-1.1.1.1 DA=2.2.2.2-2.2.2.5
         SP=20-25 DP=20-25 P=6 T=NM PR=0      |GW=192.168.1.1 T=MT PR=0
   002 N _______________________________________________________
         _______________________________________________________
   003 N _______________________________________________________
         _______________________________________________________
   004 N _______________________________________________________
         _______________________________________________________
   005 N _______________________________________________________
         _______________________________________________________
   006 N _______________________________________________________
         _______________________________________________________

                Select Command= None           Select Rule= N/A
                      Press ENTER to Confirm or ESC to Cancel:

  Press Space Bar to Toggle.
```

The following table describes the fields in this screen.

Table 226 Menu 25: Sample IP Routing Policy Summary

FIELD	DESCRIPTION
#	This is the policy index number.
A	This displays whether a policy is active (**Y**) or not (**N**).

Table 226 Menu 25: Sample IP Routing Policy Summary (continued)

FIELD	DESCRIPTION
Criteria/Action	This displays the details about to which packets the policy applies and how the policy has the LAN-Cell handle those packets. Refer to Table 227 on page 556 for detailed information.
Select Command	Press [SPACE BAR] to choose from **None**, **Edit**, **Delete**, **Go To Rule**, **Next Page** or **Previous Page** and then press [ENTER]. You must select a rule in the next field when you choose the **Edit**, **Delete** or **Go To** commands. Select **None** and then press [ENTER] to go to the "Press ENTER to Confirm…" prompt. Use **Edit** to create or edit a rule. Use **Delete** to remove a rule. To edit or delete a rule, first make sure you are on the correct page. When a rule is deleted, subsequent rules do not move up in the page list. Use **Go To Rule** to view the page where your desired rule is listed. Select **Next Page** or **Previous Page** to view the next or previous page of rules (respectively).
Select Rule	Type the policy index number you wish to edit or delete and then press [ENTER].
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm…" to save your configuration, or press [ESC] at any time to cancel.	

Table 227 IP Routing Policy Setup

ABBREVIATION	MEANING
Criterion SA	Source IP Address
SP	Source Port
DA	Destination IP Address
DP	Destination Port
P	IP layer 4 protocol number (TCP=6, UDP=17…)
T	Type of service of incoming packet
PR	Precedence of incoming packet
Action GW	Gateway IP address
T	Outgoing Type of service
P	Outgoing Precedence
Service NM	Normal
MD	Minimum Delay
MT	Maximum Throughput
MR	Maximum Reliability
MC	Minimum Cost

41.2 IP Routing Policy Setup

To setup a routing policy, perform the following procedures:

1 Type 25 in the main menu to open **Menu 25 - IP Routing Policy Summary**.

2 Select **Edit** in the **Select Command** field; type the index number of the rule you want to configure in the **Select Rule** field and press [ENTER] to open **Menu 25.1 - IP Routing Policy Setup** (see the next figure).

Figure 374 Menu 25.1: IP Routing Policy Setup

```
               Menu 25.1 - IP Routing Policy Setup

      Rule Index= 1                           Active= Yes
      Criteria:
        IP Protocol    = 6
        Type of Service= Normal               Packet length= 40
        Precedence     = 0                      Len Comp= Equal
        Source:
          addr start= 1.1.1.1                 end= 1.1.1.1
          port start= 20                      end= 25
        Destination:
          addr start= 2.2.2.2                 end= 2.2.2.5
          port start= 20                      end= 25
       Action= Matched
         Gateway Type= IP Address
         Gateway addr   = 192.168.1.1          Redirect packet= N/A
         Type of Service= Max Thruput          Log= No
         Precedence     = 0
      Edit policy to packets received from= No

                          Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this screen.

Table 228 Menu 25.1: IP Routing Policy Setup

FIELD	DESCRIPTION
Rule Index	This is the index number of the routing policy selected in **Menu 25 - IP Routing Policy Summary**.
Active	Press [SPACE BAR] and then [ENTER] to select **Yes** to activate the policy.
Criteria	
IP Protocol	Enter a number that represents an IP layer 4 protocol, for example, UDP=17, TCP=6, ICMP=1 and Don't care=0.
Type of Service	Prioritize incoming network traffic by choosing from **Don't Care**, **Normal**, **Min Delay**, **Max Thruput** or **Max Reliable**.
Precedence	Precedence value of the incoming packet. Press [SPACE BAR] and then [ENTER] to select a value from **0** to **7** or **Don't Care**.
Packet Length	Type the length of incoming packets (in bytes). The operators in the **Len Comp** (next field) apply to packets of this length.
Len Comp	Press [SPACE BAR] and then [ENTER] to choose from **Equal**, **Not Equal**, **Less**, **Greater**, **Less or Equal** or **Greater or Equal**.
Source	
addr start / end	Source IP address range from start to end.
port start / end	Source port number range from start to end; applicable only for TCP/UDP.
Destination	

Table 228 Menu 25.1: IP Routing Policy Setup

FIELD	DESCRIPTION
addr start / end	Destination IP address range from start to end.
port start / end	Destination port number range from start to end; applicable only for TCP/UDP.
Action	Specifies whether action should be taken on criteria Matched or Not Matched.
Gateway Type	Press [SPACE BAR] and then [ENTER] to select **IP Address** and enter the IP address of the gateway if you want to specify the IP address of the gateway. The gateway is an immediate neighbor of your LAN-Cell that will forward the packet to the destination. The gateway must be a router on the same segment as your LAN-Cell's LAN or WAN port. Press [SPACE BAR] and then [ENTER] to select **Remote Node** to have the LAN-Cell send traffic that matches the policy route through a specific WAN port.
Gateway addr	This field displays if you selected **IP Address** in the **Gateway Type** field. Defines the outgoing gateway address. The gateway must be on the same subnet as the LAN-Cell if it is on the LAN, otherwise, the gateway must be the IP address of a remote node. The default gateway is specified as 0.0.0.0.
Remote Node Idx	This field displays if you selected **Remote Node** in the **Gateway Type** field. Type **1** for Ethernet WAN or 2 for Cellular WAN.
Redirect Packet	This field applies if you selected **Remote Node** in the **Gateway Type** field. Press [SPACE BAR] and then [ENTER] to select **Yes** to have the LAN-Cell send traffic that matches the policy route through the other WAN interface if it cannot send the traffic through the WAN interface you selected.
Type of Service	Set the new TOS value of the outgoing packet. Prioritize incoming network traffic by choosing **Don't Care**, **Normal**, **Min Delay**, **Max Thruput**, **Max Reliable** or **Min Cost**.
Precedence	Set the new outgoing packet precedence value. Values are **0** to **7** or **Don't Care**.
Log	Press [SPACE BAR] and then [ENTER] to select **Yes** to make an entry in the system log when a policy is executed.
Edit policy to packets received from	Press [SPACE BAR] and then [ENTER] to select **Yes** or **No** (default). Select **Yes** to configure Menu 25.1.1: IP Routing Policy Setup discussed next.
When you have completed this menu, press [ENTER] at the prompt "Press [ENTER] to confirm or [ESC] to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.	

41.2.1 Applying Policy to Packets

To apply the policy to packets received on the selected interface(s), go to **Menu 25.1: IP Routing Policy Setup** and press [SPACE BAR] to select **Yes** in the **Edit policy to packets received from** field. Press [ENTER] to display **Menu 25.1.1 - IP Routing Policy Setup** (shown next).

Figure 375 Menu 25.1.1: IP Routing Policy Setup

```
               Menu 25.1.1 - IP Routing Policy Setup

                          Apply policy to packets received from:
                            LAN= No
                            DMZ= No
                            WLAN= No
                            ALL WAN= Yes
                              Selected Remote Node index= N/A

              Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this screen.

Table 229 Menu 25.1.1: IP Routing Policy Setup

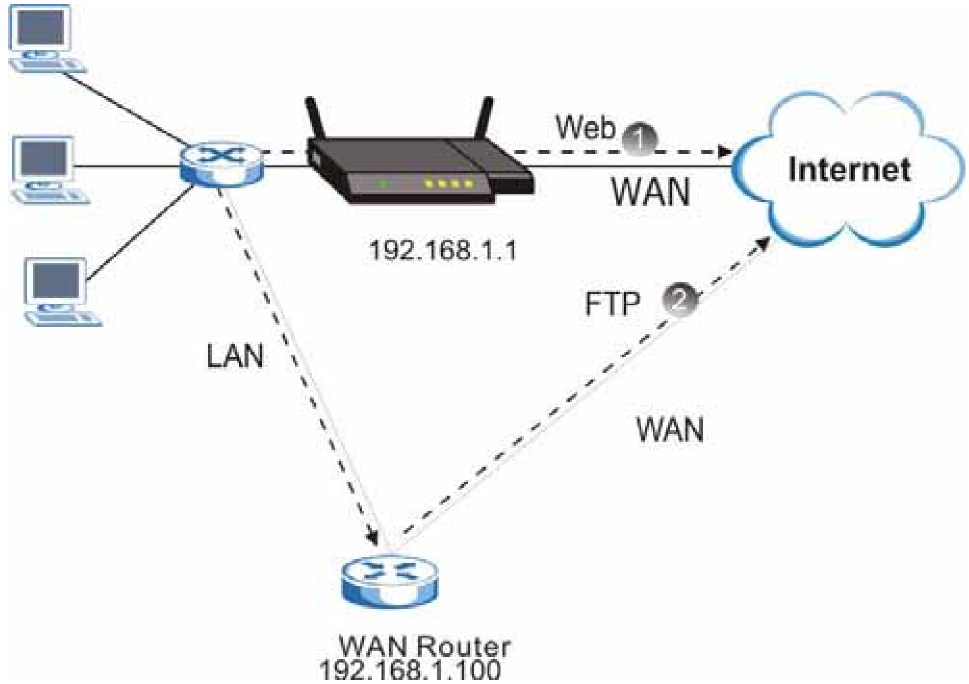
FIELD	DESCRIPTION
LAN/DMZ/WLAN/ ALL WAN	Press [SPACE BAR] to select **Yes** or **No**. Choose **Yes** and press [ENTER] to apply the policy to packets received on the specific interface(s).
Selected Remote Node index	If you select **No** in the **ALL WAN** field, enter the number of the WAN interface.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm…" to save your configuration, or press [ESC] at any time to cancel.	

41.3 IP Policy Routing Example

If a network has both Internet and remote node connections, you can route Web packets to the Internet using one policy and route FTP packets to a remote network using another policy. See the next figure.

Route 1 represents the default IP route and route 2 represents the configured IP route.

Figure 376 Example of IP Policy Routing



To force Web packets coming from clients with IP addresses of 192.168.1.33 to 192.168.1.64 to be routed to the Internet via the WAN port of the LAN-Cell, follow the steps as shown next.

1 Create a rule in **Menu 25.1 - IP Routing Policy Setup** as shown next.

Figure 377 IP Routing Policy Example 1

```
              Menu 25.1 - IP Routing Policy Setup

              Rule Index= 1                           Active= Yes
              Criteria:
                IP Protocol    = 6
                Type of Service= Don't Care           Packet length= 10
                Precedence     = Don't Care             Len Comp= Equal
                Source:
                  addr start= 192.168.1.33       end= 192.168.1.64
                  port start= 0                  end= N/A
                Destination:
                  addr start= 0.0.0.0                 end= N/A
                  port start= 80                      end= 80
              Action= Matched
                 Gateway Type= IP Address
                 Gateway addr   = 192.168.1.1          Redirect packet= N/A
                 Type of Service= Max Thruput          Log= No
                 Precedence     = 0
              Edit policy to packets received from= No

                                    Press ENTER to Confirm or ESC to Cancel:
```

2 Select **Yes** in the **LAN** field in menu 25.1.1 to apply the policy to packets received on the LAN port.

3 Check **Menu 25 - IP Routing Policy Summary** to see if the rule is added correctly.

4 Create another rule in menu 25.1 for this rule to route packets from any host (IP=0.0.0.0 means any host) with protocol TCP and port FTP access through another gateway (192.168.1.100).

Figure 378 IP Routing Policy Example 2

```
 Menu 25.1 - IP Routing Policy Setup

Rule Index= 2                               Active= No
Criteria:
  IP Protocol    = 6
  Type of Service= Don't Care               Packet length= 10
  Precedence     = Don't Care                 Len Comp= Equal
  Source:
    addr start= 0.0.0.0                     end= N/A
    port start= 0                           end= N/A
  Destination:
    addr start= 0.0.0.0                     end= N/A
    port start= 20                          end= 21
Action= Matched
   Gateway Type= IP Address
   Gateway addr   = 192.168.1.100     Redirect packet= N/A
   Type of Service= Don't Care        Log= No
   Precedence     = Don't Care
Edit policy to packets received from= No

                    Press ENTER to Confirm or ESC to Cancel:
```

5 Select **Yes** in the **LAN** field in menu 25.1.1 to apply the policy to packets received on the LAN port.

6 Check **Menu 25 - IP Routing Policy Summary** to see if the rule is added correctly.

42

Call Scheduling

Call scheduling allows you to dictate when a remote node should be called and for how long.

42.1 Introduction to Call Scheduling

The call scheduling feature allows the LAN-Cell to manage a remote node and dictate when a remote node should be called and for how long. This feature is similar to the scheduler in a videocassette recorder (you can specify a time period for the VCR to record). You can apply up to 4 schedule sets in **Menu 11.1 - Remote Node Profile**. From the main menu, enter 26 to access **Menu 26 - Schedule Setup** as shown next.

Figure 379 Schedule Setup

```
                           Menu 26 - Schedule Setup

              Schedule                      Schedule
              Set #     Name                Set #     Name
              ------    ------------------  ------    ------------------
              1         _________________   7         _________________
              2         _________________   8         _________________
              3         _________________   9         _________________
              4         _________________   10        _________________
              5         _________________   11        _________________
              6         _________________   12        _________________

              Enter Schedule Set Number to Configure= 0
              Edit Name= N/A
              Press ENTER to Confirm or ESC to Cancel:
```

Lower numbered sets take precedence over higher numbered sets thereby avoiding scheduling conflicts. For example, if sets 1, 2, 3 and 4 are applied in the remote node, then set 1 will take precedence over set 2, 3 and 4 as the LAN-Cell, by default, applies the lowest numbered set first. Set 2 will take precedence over set 3 and 4, and so on.

You can design up to 12 schedule sets but you can only apply up to four schedule sets for a remote node.

To delete a schedule set, enter the set number and press [SPACE BAR] and then [ENTER] or [DEL] in the Edit Name field.

To set up a schedule set, select the schedule set you want to setup from menu 26 (1-12) and press [ENTER] to see **Menu 26.1 - Schedule Set Setup** as shown next.

Figure 380 Schedule Set Setup

```
Menu 26.1 - Schedule Set Setup

Active= Yes
How Often= Once
Start Date(yyyy-mm-dd) = N/A
Once:
  Date(yyyy-mm-dd)= 2000 - 01 - 01
Weekdays:
  Sunday= N/A
  Monday= N/A
  Tuesday= N/A
  Wednesday= N/A
  Thursday= N/A
  Friday= N/A
  Saturday= N/A
Start Time (hh:mm)= 00 : 00
Duration (hh:mm)= 00 : 00
Action= Forced On

Press ENTER to Confirm or ESC to Cancel:
Press Space Bar to Toggle
```

If a connection has been already established, your LAN-Cell will not drop it. Once the connection is dropped manually or it times out, then that remote node can't be triggered up until the end of the **Duration**.

Table 230 Schedule Set Setup

FIELD	DESCRIPTION
Active	Press [SPACE BAR] to select **Yes** or **No**. Choose **Yes** and press [ENTER] to activate the schedule set.
How Often	Should this schedule set recur weekly or be used just once only? Press [SPACE BAR] and then [ENTER] to select **Once** or **Weekly**. Both these options are mutually exclusive. If **Once** is selected, then all weekday settings are **N/A**. When **Once** is selected, the schedule rule deletes automatically after the scheduled time elapses.
Start Date	Enter the start date when you wish the set to take effect in year -month-date format. Valid dates are from the present to 2036-February-5.
Once:	
Date	If you selected **Once** in the **How Often** field above, then enter the date the set should activate here in year-month-date format.
Weekdays:	

Table 230 Schedule Set Setup (continued)

FIELD	DESCRIPTION
Day	If you selected **Weekly** in the **How Often** field above, then select the day(s) when the set should activate (and recur) by going to that day(s) and pressing [SPACE BAR] to select **Yes**, then press [ENTER].
Start Time	Enter the start time when you wish the schedule set to take effect in hour-minute format.
Duration	The duration determines how long the LAN-Cell is to apply the action configured in the **Action** field. Enter the maximum length of time in hour-minute format.
Action	**Forced On** means that the connection is maintained whether or not there is a demand call on the line and will persist for the time period specified in the **Duration** field. **Forced Down** means that the connection is blocked whether or not there is a demand call on the line. **Enable Dial-On-Demand** means that this schedule permits a demand call on the line. **Disable Dial-On-Demand** means that this schedule prevents a demand call on the line.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm…" to save your configuration, or press [ESC] at any time to cancel.	

Once your schedule sets are configured, you must then apply them to the desired remote node(s). Enter 11 from the Main Menu and then enter the target remote node index. Press [SPACE BAR] and then [ENTER] to select **PPPoE** in the **Encapsulation** field to make the schedule sets field available as shown next.

Figure 381 Applying Schedule Set(s) to a Remote Node (PPPoE)

```
                       Menu 11.1 - Remote Node Profile

          Rem Node Name= ChangeMe        Route= IP
          Active= Yes

          Encapsulation= PPPoE           Edit IP= No
          Service Type= Standard         Telco Option:
          Service Name=                    Allocated Budget(min)= 0
          Outgoing=                        Period(hr)= 0
            My Login=                      Schedules= 1,2,3,4
            My Password= ********          Nailed-Up Connection= No
            Authen= CHAP/PAP
                                         Session Options:
                                           Edit Filter Sets= No
                                           Idle Timeout(sec)= 100


               Press ENTER to Confirm or ESC to Cancel:
```

You can apply up to four schedule sets, separated by commas, for one remote node. Change the schedule set numbers to your preference(s).

Figure 382 Applying Schedule Set(s) to a Remote Node (PPTP)

```
                          Menu 11.1 - Remote Node Profile

             Rem Node Name= ChangeMe              Route= IP
             Active= Yes

             Encapsulation= PPTP               Edit IP= No
             Service Type= Standard             Telco Option:
                                                  Allocated Budget(min)= 0
             Outgoing=                            Period(hr)= 0
               My Login=                          Schedules= 1,2,3,4
               My Password= ********              Nailed-up Connections= No
               Retype to Confirm= ********
               Authen= CHAP/PAP
             PPTP:                                Session Options:
               My IP Addr=                          Edit Filter Sets= No
               My IP Mask=                          Idle Timeout(sec)= 100
               Server IP Addr=
               Connection ID/Name=


              Press ENTER to Confirm or ESC to Cancel:
```

PART VII
Troubleshooting and Specifications

43

Troubleshooting

This chapter offers some suggestions to solve problems you might encounter.

Proxicast's web site also contains a knowledgebase of other troubleshooting, technical support, and example configuration information. Please consult support.proxicast.com for the latest LAN-Cell support information.

The potential problems are divided into the following categories.

- Power, Hardware Connections, and LEDs
- LAN-Cell Access and Login
- Internet Access

43.1 Power, Hardware Connections, and LEDs

The LAN-Cell does not turn on. None of the LEDs turn on.

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

One of the LEDs does not behave as expected.

1. Make sure you understand the normal behavior of the LED. See Section 1.5 on page 30.
2. Check the hardware connections. See the Quick Start Guide.
3. Inspect your cables for damage. Contact the vendor to replace any damaged cables.

4 Turn the LAN-Cell off and on or disconnect and re-connect the power adaptor to the LAN-Cell.
5 If the problem continues, contact the vendor.

43.2 LAN-Cell Access and Login

I forgot the LAN IP address for the LAN-Cell.

1 The default LAN IP address is **192.168.1.1**.
2 Use the console port to log in to the LAN-Cell.
3 If you changed the IP address and have forgotten it, you might get the IP address of the LAN-Cell by looking up the IP address of the default gateway for your computer. To do this in most Windows computers, click **Start** > **Run**, enter **cmd**, and then enter **ipconfig**. The IP address of the **Default Gateway** might be the IP address of the LAN-Cell (it depends on the network), so enter this IP address in your Internet browser.
4 If this does not work, you have to reset the device to its factory defaults. See Section 2.4 on page 51.

I forgot the password.

1 The default password is **1234**.
2 If this does not work, you have to reset the device to its factory defaults. See Section 2.4 on page 51.

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

1 Make sure you are using the correct IP address.
   - The default LAN IP address is 192.168.1.1.
   - Use the LAN-Cell’s LAN IP address when configuring from the LAN.
   - Use the LAN-Cell’s WAN IP address when configuring from the WAN.
   - If you changed the LAN IP address (Section 4.2 on page 80), use the new IP address.
   - If you changed the LAN IP address and have forgotten it, see the troubleshooting suggestions for I forgot the LAN IP address for the LAN-Cell.
2 Enter “HTTP://192.168.1.1” (or the current LAN IP address of the LAN-Cell) into your browsers address bar.
3 Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and Section 1.5 on page 30.

4 Make sure your Internet browser does not block pop-up windows and has JavaScripts and Java enabled. See Appendix A on page 583.
5 Make sure your computer's Ethernet adapter is installed and functioning properly.
6 Make sure your computer is in the same subnet as the LAN-Cell. (If you know that there are routers between your computer and the LAN-Cell, skip this step.)
    - If there is a DHCP server on your network, make sure your computer is using a dynamic IP address. See Appendix B on page 589. Your LAN-Cell is a DHCP server by default.
7 Reset the device to its factory defaults, and try to access the LAN-Cell with the default IP address. See Section 2.4 on page 51.
8 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

Advanced Suggestions

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

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

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

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

? I can see the **Login** screen, but I cannot log in to the LAN-Cell.

1 Make sure you have entered the user name and password correctly. The default user name is **admin**, and the default password is **1234**. These fields are case-sensitive, so make sure [Caps Lock] is not on.
2 You cannot log in to the web configurator while someone is using the SMT, Telnet, or the console port to access the LAN-Cell. Log out of the LAN-Cell in the other session, or ask the person who is logged in to log out.
3 Turn the LAN-Cell off and on or disconnect and re-connect the power adaptor or cord to the LAN-Cell.
4 If this does not work, you have to reset the device to its factory defaults. See Section 2.4 on page 51.

I cannot access the SMT. / I cannot Telnet to the LAN-Cell.

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

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

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

I receive an error when trying to upload new firmware to the LAN-Cell.

1. Firmware updates are usually delivered in ZIP archives. Unzip the archives and load the file with the ".BIN" extension.
2. Be certain that the firmware file you are loading is for your LAN-Cell model.
3. Back-up your configuration settings to a PC, press the RESET button for 10 seconds, then log back into the LAN-Cell (192.168.1.1 password = 1234). Upload the firmware then reload your saved configuration file.
4. Firmware upgrades over a WAN interface are possible, but not recommended, especially over 3G cellular WAN connections, due to high latency and the potential for interrupted communications.
5. Try performing the firmware upgrade via the Console port using FTP.

43.3 Internet Access

I cannot make a 3G cellular connection.

1 Make sure that you are using a 3G PC-Card modem that is supported in your version of the LAN-Cell's ProxiOS firmware. Check the Proxicast web site for the last firmware and 3G card support information.

1 Make sure that your 3G PC-Card modem (and SIM/RUIM card if used) is <u>associated</u> with your account at your service provider and that it is properly <u>provisioned</u> for Internet services.

2. Make sure that your 3G PC-Card modem has been properly activated on your service providers network. Use a Windows laptop to confirm that the 3G card is functioning properly on the carrier's network. Follow the carrier or card manufacturer's instructions on activating and updating the 3G card in Windows.
3. Check the APN, Username, Password, Authentication Type, and ISP Access phone number in the **WIRELESS** > **CELLULAR** screen. Refer to Section 5.4 on page 114.
4. Disconnect all the cables from your device, remove the 3G card, and follow the directions in the Quick Start Guide again.
5. If the problem continues, contact your ISP.

I cannot get a WAN IP address (or the correct IP address) from the ISP.

1. The ISP provides the WAN IP address after authenticating you. Authentication may be through the user name and password, the 3G Card's ESN, IMEI, or IMSI value, the MAC address or the host name.
2. Try using the "Get Automatically from IP" option even if you have a "static" IP address assigned by your ISP.
3. Disconnect all the cables from your device, remove the 3G card, and follow the directions in the Quick Start Guide again.
4. If the problem continues, contact your ISP.

I cannot access the Internet.

1. Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and Section 1.5 on page 30.
2. Make sure you entered your ISP account information correctly in the WAN or Cellular screens or SMT menus. These fields are case-sensitive, so make sure [Caps Lock] is not on.
3. If you are trying to access the Internet using a Wi-Fi client, make sure the settings in the Wi-Fi client are the same as the settings in the LAN-Cell's Wi-Fi AP.
4. Disconnect all the cables from your device, remove the 3G card, and follow the directions in the Quick Start Guide again.
5. If the problem continues, contact your ISP.

I cannot access the Internet anymore. I had access to the Internet (with the LAN-Cell), but my Internet connection is not available anymore.

1. Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and Section 1.5 on page 30.

2 Check the Cell-Sentry budget control. Refer to Section 5.4.2 on page 118.
3 Check the schedule rules. Refer to Chapter 42 on page 563 (SMT).
4 Reboot the LAN-Cell.
5 If the problem continues, contact your ISP.

? The Internet connection is slow or intermittent.

1 There might be a lot of traffic on the network. Look at the LEDs, and check Section 1.5 on page 30. If the LAN-Cell is sending or receiving a lot of information, try closing some programs that use the Internet, especially peer-to-peer applications.
2 Check the 3G signal strength. If the signal strength is low, try repositioning the LAN-Cell's external antenna (if used) or move the LAN-Cell to a different location. Look for any devices that might be interfering with the cellular signal (for example, microwaves, CRT's, light fixtures, other wireless networks, and so on).
3 Reboot the LAN-Cell.
4 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

Advanced Suggestions

- Check the settings for bandwidth management. If it is disabled, you might consider activating it. If it is enabled, you might consider changing the allocations.
- Contact your cellular service provider regarding coverage and signal quality at your location.
- Utilize a higher gain external antenna or amplifier.

44

Product Specifications

The following tables summarize the LAN-Cell's hardware and firmware features.

Table 231 Hardware Specifications

Dimensions	220 (W) x 137 (D) x 32 (H) mm
Weight	1.09 kg
Power Specification	12V DC. 2.1 mm jack (center pin positive)
Power Consumption	5W Typical; 8W Max
Ethernet Interface	
LAN/DMZ	Four LAN/DMZ/WLAN auto-negotiating, auto MDI/MDI-X 10/100 Mbps RJ-45 Ethernet ports.
WAN	One auto-negotiating, auto MDI/MDI-X 10/100 Mbps RJ-45 Ethernet port
Reset Button	Restores factory default settings
Console	RJ-45 port for RS-232 null modem connection
Dial Backup	RJ-45 port for RS-232 connection
PC-Card Slot	For installing a 3G card. Optional Card-Guard 3G card protection cover includes mounting hole for bulkhead SMA antenna jacks. 3G Card pig-tail connectors are available separately..
WLAN Antenna	One 2 dBi rubber duck style swivel 802.11 a/b/g antenna (SMA-RP Female). WLAN jack on the LAN-Cell is SMA-RP Male
Card-Lock	Use 18lb tensile strength (miniature) cable-ties. Max. width 0.1 in (2.5 mm)
Operation Temperature	-30º C ~ 60º C
Operation Humidity	20% ~ 92% RH (non-condensing)
Certifications	EMC: FCC Part 15 Class B, CE-EMC Class B, C-Tick Class B, VCCI Class B Safety: CSA International, CE EN60950-1 (UL60950-1, CSA60950-1, EN60950-1, IEC60950-1)

Table 232 Firmware Specifications

FEATURE	DESCRIPTION
Default IP Address	192.168.1.1
Default Subnet Mask	255.255.255.0 (24 bits)
Default Password	1234
Default DHCP Pool	192.168.1.33 to 192.168.1.160
Device Management	Use the web configurator to easily configure the rich range of features on the LAN-Cell.

Table 232 Firmware Specifications

FEATURE	DESCRIPTION
Wireless Functionality	Allow the IEEE 802.11a, IEEE 802.11b and/or IEEE 802.11g wireless clients to connect to the LAN-Cell wirelessly. Enable wireless security (WEP, WPA(2), WPA(2)-PSK) and/or MAC filtering to protect your wireless network.
Firmware Upgrade	Download new firmware (when available) from the Proxicast web site and use the web configurator, an FTP or a TFTP tool to put it on the LAN-Cell. Note: Only upload firmware for your specific model!
Configuration Backup & Restoration	Make a copy of the LAN-Cell’s configuration. You can put it back on the LAN-Cell later if you decide to revert back to an earlier configuration.
Network Address Translation (NAT)	Each computer on your network must have its own unique IP address. Use NAT to convert your public IP address(es) to multiple private IP addresses for the computers on your network.
Port Forwarding	If you have a server (mail or web server for example) on your network, you can use this feature to let people access it from the Internet.
DHCP (Dynamic Host Configuration Protocol)	Use this feature to have the LAN-Cell assign IP addresses, an IP default gateway and DNS servers to computers on your network.
Dynamic DNS Support	With Dynamic DNS (Domain Name System) support, you can use a fixed URL, www.proxicast.com for example, with a dynamic IP address. You must register for this service with a Dynamic DNS service provider.
IP Multicast	IP multicast is used to send traffic to a specific group of computers. The LAN-Cell supports versions 1 and 2 of IGMP (Internet Group Management Protocol) used to join multicast groups (see RFC 2236).
IP Alias	IP alias allows you to subdivide a physical network into logical networks over the same Ethernet interface with the LAN-Cell itself as the gateway for each subnet.
Time and Date	Get the current time and date from an external server when you turn on your LAN-Cell. You can also set the time manually. These dates and times are then used in logs.
Logging and Tracing	Use packet tracing and logs for troubleshooting. You can send logs from the LAN-Cell to an external syslog server.
PPPoE	PPPoE mimics a dial-up Internet access connection.
PPTP Encapsulation	Point-to-Point Tunneling Protocol (PPTP) enables secure transfer of data through a Virtual Private Network (VPN). The LAN-Cell supports one PPTP connection at a time.
RoadRunner Support	The LAN-Cell supports Time Warner’s RoadRunner Service in addition to standard cable modem services.
Firewall	You can configure firewall on the Proxicast Device for secure Internet access. When the firewall is on, by default, all incoming traffic from the Internet to your network is blocked unless it is initiated from your network. This means that probes from the outside to your network are not allowed, but you can safely browse the Internet and download files for example.
IPSec VPN	This allows you to establish a secure Virtual Private Network (VPN) tunnel to connect with business partners and branch offices using data encryption and the Internet without the expense of leased site-to-site lines. The LAN-Cell VPN is based on the IPSec standard and is fully interoperable with other IPSec-based VPN products.

Table 232 Firmware Specifications

FEATURE	DESCRIPTION
Bandwidth Management	You can efficiently manage traffic on your network by reserving bandwidth and giving priority to certain types of traffic and/or to particular computers.
Remote Managemet	This allows you to decide whether a service (HTTP or FTP traffic for example) from a computer on a network (LAN or WAN for example) can access the LAN-Cell.

Table 233 Feature Specifications

FEATURE	SPECIFICATION
Number of Local User Database Entries	32
Number of Static DHCP Table Entries	32
Number of Static Routes	30
Number of Policy Routes	24
Number of NAT Sessions	3,000
Number of Address Mapping Rules	10
Number of Port Forwarding Rules	20
Number of IPSec VPN Tunnels/Security Associations	5
Number of Bandwidth Management Classes	10
Number of Bandwidth Management Class Levels	1
Number of DNS Address Record Entries	30
Number of DNS Name Server Record Entries	16

Table 234 Performance

CATEGORY	PERFORMANCE
Firewall Throughput (with NAT)	24 Mbps
VPN (3DES) Throughput	24 Mbps
User Licenses	Unlimited
Concurrent Sessions	3,000
Simultaneous IPSec VPN Connections	5
Output Power (Maximum)	IEEE 802.11a: 14 dBm at 54 Mbps OFDM IEEE 802.11b: 18 dBm at 11 Mbps CCK, QPSK, BPSK IEEE 802.11g: 17 dBm at 54 Mbps OFDM

Compatible 3G Cards

Please see the Release Notes included on the LAN-Cell Documentation CD (or at support.proxicast.com) for the list of 3G PC-Card modems supported in each firmware release.

3G Card Installation

Do not insert or remove a card with the LAN-Cell turned on.

Make sure the LAN-Cell is off before inserting or removing a 3G card (to avoid damage). Slide the connector end of the card into the slot as shown next.

Power Adapter Specifications

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

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

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

AUSTRALIA AND NEW ZEALAND PLUG STANDARDS	
AC POWER ADAPTOR MODEL	PSA18R-120P (ZS)-R
INPUT POWER	100-240VAC, 50/60HZ, 0.5A
OUTPUT POWER	12VDC, 1.5A
POWER CONSUMPTION	18 W MAX.
SAFETY STANDARDS	AS/NZ60950

JAPAN PLUG STANDARDS	
AC POWER ADAPTOR MODEL	PSA18R-120P (ZA)-R
INPUT POWER	100-240VAC, 50/60HZ, 0.5A
OUTPUT POWER	12VDC, 1.5A
POWER CONSUMPTION	18 W MAX.
SAFETY STANDARDS	JET

CHINA PLUG STANDARDS	
AC POWER ADAPTOR MODEL	PSA18R-120P (ZA)-R
INPUT POWER	100-240VAC, 50/60HZ, 0.5A
OUTPUT POWER	12VDC, 1.5A
POWER CONSUMPTION	18 W MAX.
SAFETY STANDARDS	CCC

Cable Pin Assignments

In a serial communications connection, generally a computer is DTE (Data Terminal Equipment) and a modem is DCE (Data Circuit-terminating Equipment). The LAN-Cell is DCE when you connect a computer to the console port. The LAN-Cell is DTE when you connect a modem to the dial backup port.[6]

The console cable and dial backup cable each have an RJ-45 connector and a DB-9 connector. The pin layout for the DB-9 connector end of the cables is as follows.

Figure 383 Console/Dial Backup Cable DB-9 End Pin Layout

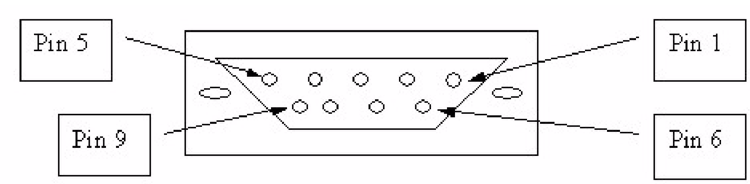


Table 235 Console Cable Pin Assignments

PIN DEFINITION	RJ-45 END	DB-9M (MALE) END
DSR	1	6
DTR	2	4
TX	3	3
RTS	4	7
GND	5	5
RX	6	2

6. Pins 2,3 and 5 are used.

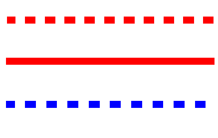
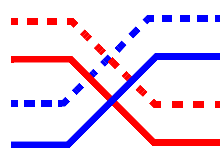
Table 235 Console Cable Pin Assignments

PIN DEFINITION	RJ-45 END	DB-9M (MALE) END
CTS	7	8
DCD	8	1
	N/A	9

Table 236 Console Cable Pin Assignments

PIN DEFINITION	RJ-45 END	DB-9M (MALE) END
DTR	1	4
DSR	2	6
RX	3	2
CTS	4	8
GND	5	5
TX	6	3
RTS	7	7
DCD	8	1
	N/A	9

Table 237 Ethernet Cable Pin Assignments

WAN / LAN ETHERNET CABLE PIN LAYOUT									
Straight-through					**Crossover**				
(Switch)			(Adapter)		(Switch)			(Switch)	
1	IRD +		1	OTD +	1	IRD +		1	IRD +
2	IRD -		2	OTD -	2	IRD -		2	IRD -
3	OTD +		3	IRD +	3	OTD +		3	OTD +
6	OTD -		6	IRD -	6	OTD -		6	OTD -

PART VIII
Appendices

A

Pop-up Windows, JavaScripts and Java Permissions

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

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

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

Internet Explorer Pop-up Blockers

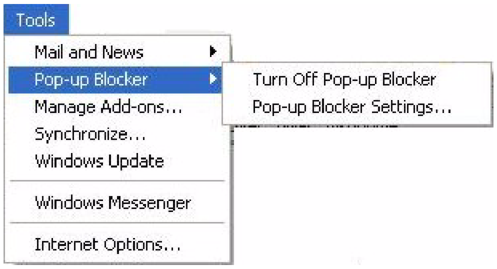
You may have to disable pop-up blocking to log into your device.

Either disable pop-up blocking (enabled by default in Windows XP SP (Service Pack) 2) or allow pop-up blocking and create an exception for your device's IP address.

Disable pop-up Blockers

1 In Internet Explorer, select **Tools**, **Pop-up Blocker** and then select **Turn Off Pop-up Blocker**.

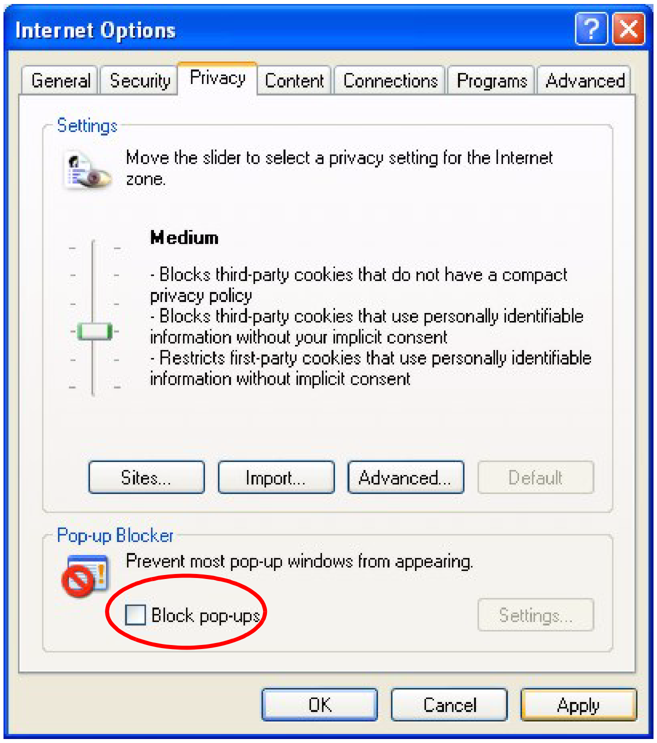
Figure 384 Pop-up Blocker



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

1 In Internet Explorer, select **Tools**, **Internet Options**, **Privacy**.
2 Clear the **Block pop-ups** check box in the **Pop-up Blocker** section of the screen. This disables any web pop-up blockers you may have enabled.

Figure 385 Internet Options



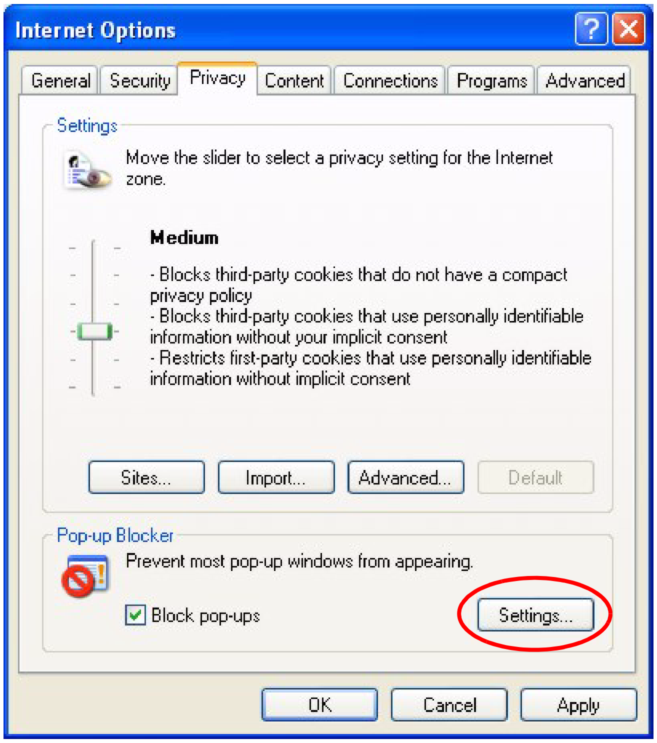
3 Click **Apply** to save this setting.

Enable pop-up Blockers with Exceptions

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

1 In Internet Explorer, select **Tools**, **Internet Options** and then the **Privacy** tab.
2 Select **Settings…**to open the **Pop-up Blocker Settings** screen.

Figure 386 Internet Options



3 Type the IP address of your device (the web page that you do not want to have blocked) with the prefix “http://”. For example, http://192.168.1.1.

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

Figure 387 Pop-up Blocker Settings

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

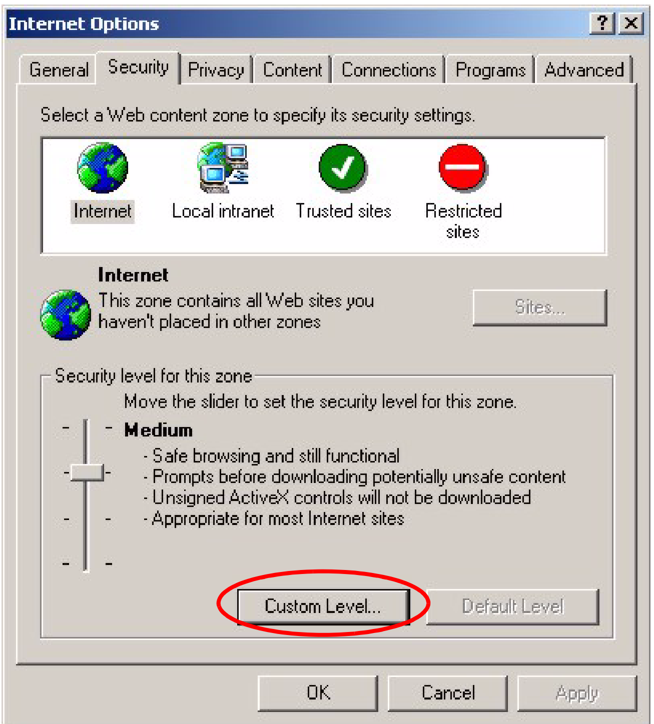
6 Click **Apply** to save this setting.

JavaScripts

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

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

Figure 388 Internet Options



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

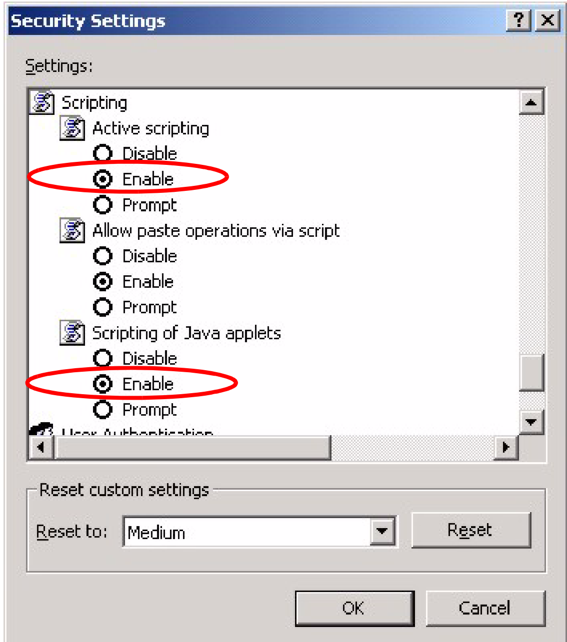
3 Scroll down to **Scripting**.

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

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

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

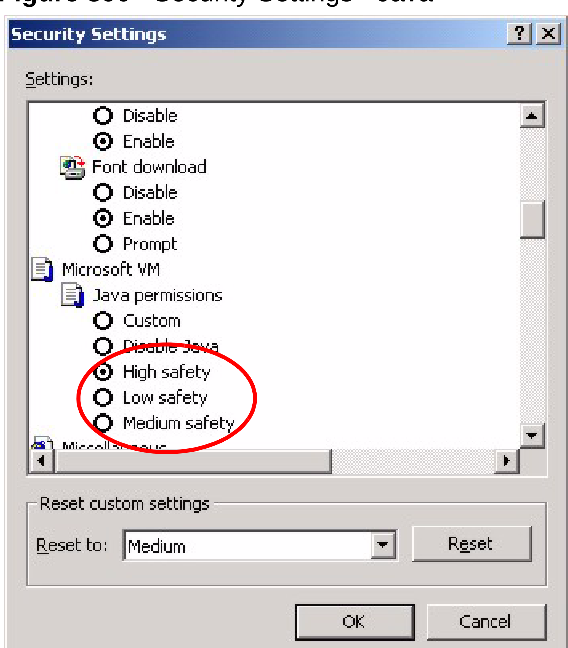
Figure 389 Security Settings - Java Scripting



Java Permissions

1 From Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.
2 Click the **Custom Level...** button.
3 Scroll down to **Microsoft VM**.
4 Under **Java permissions** make sure that a safety level is selected.
5 Click **OK** to close the window.

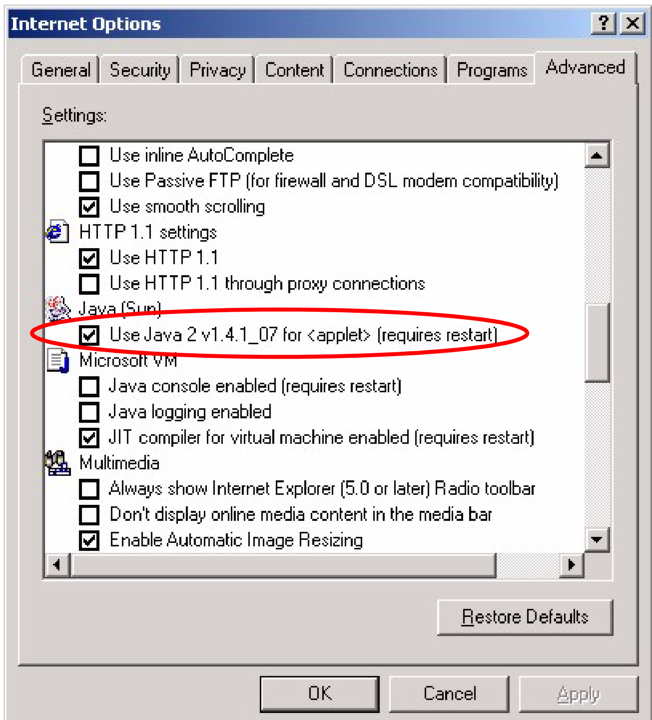
Figure 390 Security Settings - Java



JAVA (Sun)

1. From Internet Explorer, click **Tools**, **Internet Options** and then the **Advanced** tab.
2. make sure that **Use Java 2 for <applet>** under **Java (Sun)** is selected.
3. Click **OK** to close the window.

Figure 391 Java (Sun)



B

Setting up Your Computer's IP Address

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

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

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

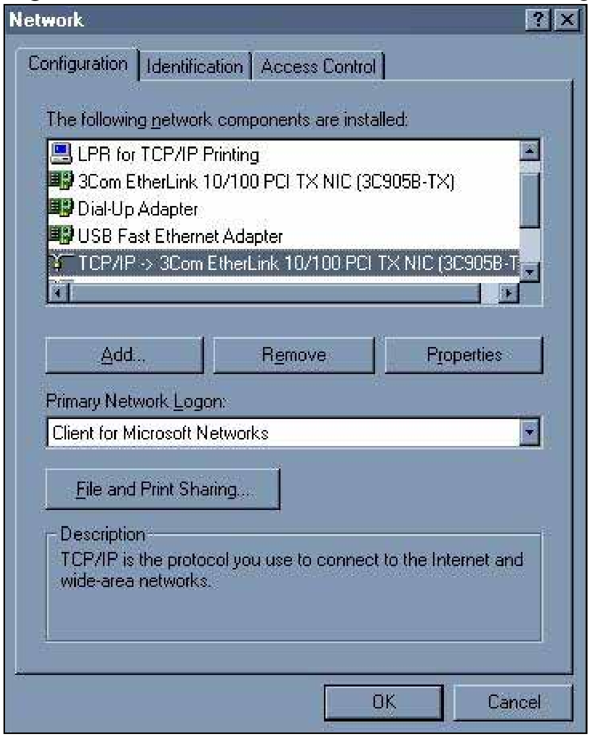
After the appropriate TCP/IP components are installed, configure the TCP/IP settings in order to "communicate" with your network.

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

Windows 95/98/Me

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

Figure 392 WIndows 95/98/Me: Network: Configuration



Installing Components

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

If you need the adapter:

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

If you need TCP/IP:

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

If you need Client for Microsoft Networks:

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

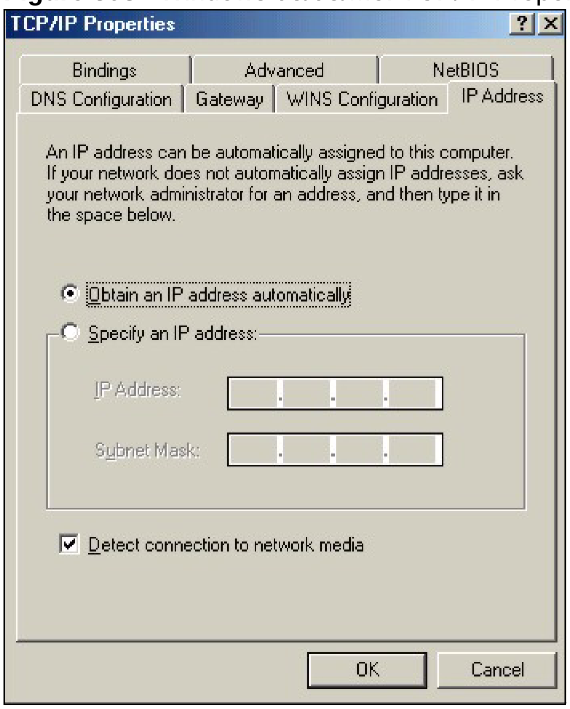
Configuring

1 In the **Network** window **Configuration** tab, select your network adapter's TCP/IP entry and click **Properties**

2 Click the **IP Address** tab.

- If your IP address is dynamic, select **Obtain an IP address automatically**.
- If you have a static IP address, select **Specify an IP address** and type your information into the **IP Address** and **Subnet Mask** fields.

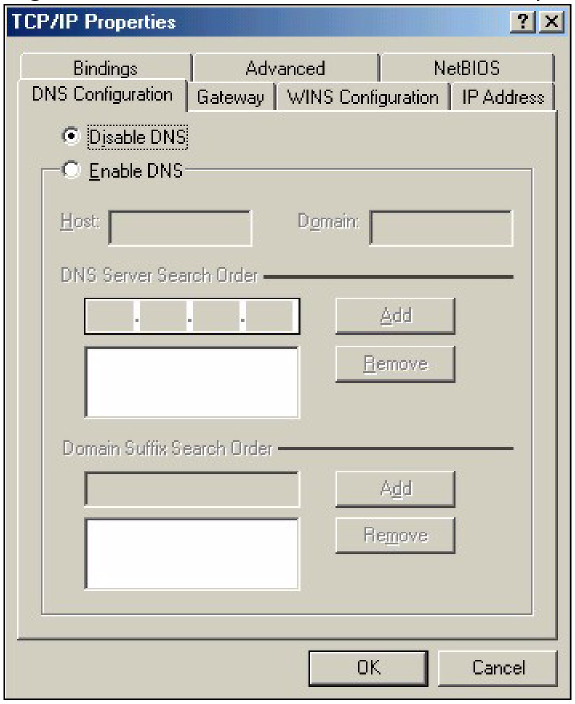
Figure 393 Windows 95/98/Me: TCP/IP Properties: IP Address



3 Click the **DNS** Configuration tab.

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

Figure 394 Windows 95/98/Me: TCP/IP Properties: DNS Configuration



4 Click the **Gateway** tab.

- If you do not know your gateway’s IP address, remove previously installed gateways.
- If you have a gateway IP address, type it in the **New gateway field** and click **Add**.

5 Click **OK** to save and close the **TCP/IP Properties** window.

6 Click **OK** to close the **Network** window. Insert the Windows CD if prompted.

7 Turn on your LAN-Cell and restart your computer when prompted.

Verifying Settings

1 Click **Start** and then **Run**.

2 In the **Run** window, type "winipcfg" and then click **OK** to open the **IP Configuration** window.

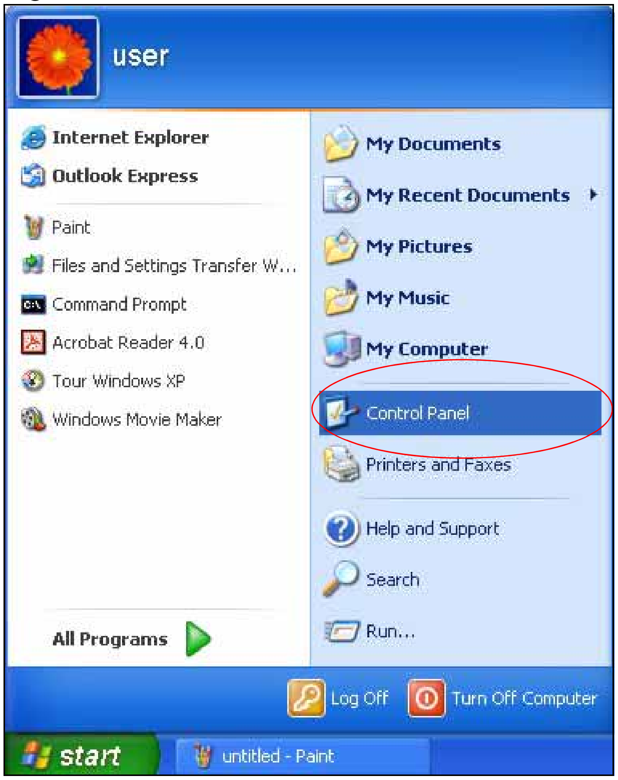
3 Select your network adapter. You should see your computer's IP address, subnet mask and default gateway.

Windows 2000/NT/XP

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

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

Figure 395 Windows XP: Start Menu

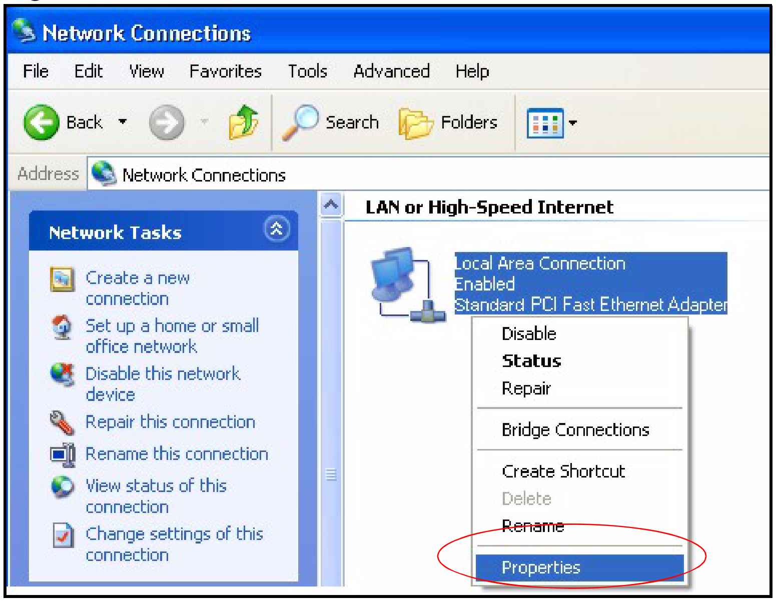


2 In the **Control Panel**, double-click **Network Connections** (**Network and Dial-up Connections** in Windows 2000/NT).

Figure 396 Windows XP: Control Panel

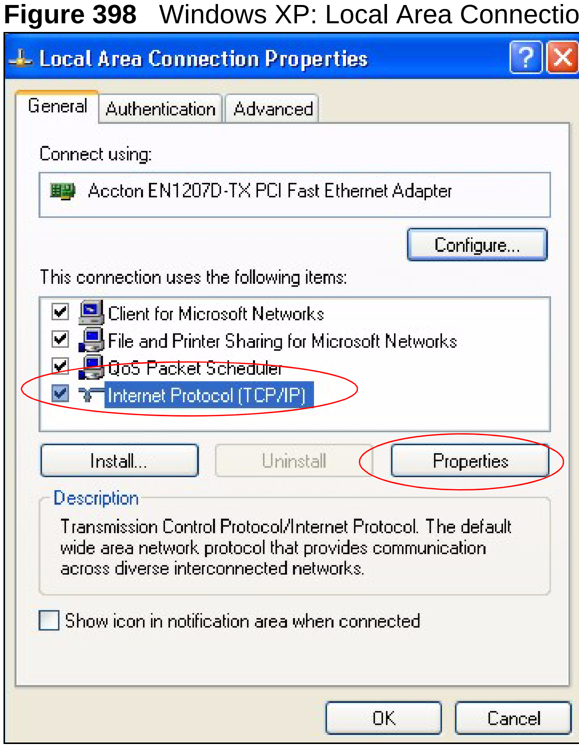
3 Right-click **Local Area Connection** and then click **Properties**.

Figure 397 Windows XP: Control Panel: Network Connections: Properties



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

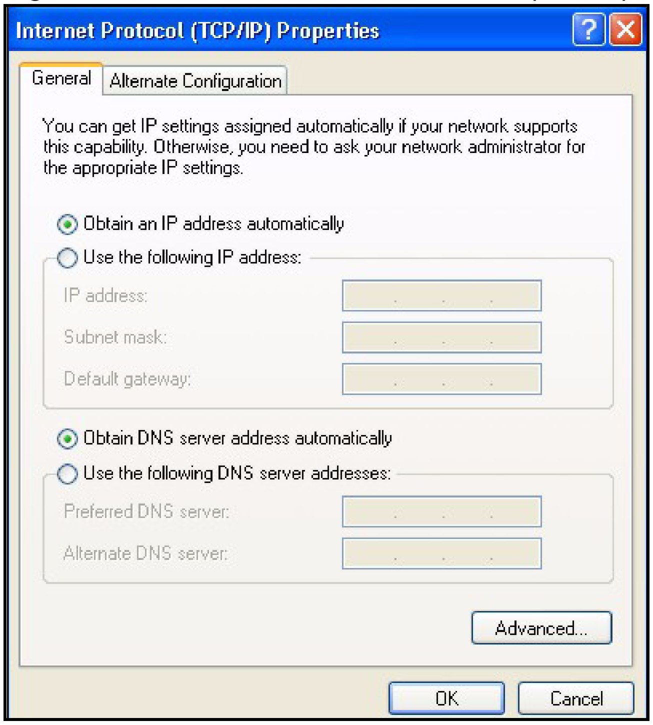
Figure 398 Windows XP: Local Area Connection Properties



5 The **Internet Protocol TCP/IP Properties** window opens (the **General tab** in Windows XP).

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

Figure 399 Windows XP: Internet Protocol (TCP/IP) Properties

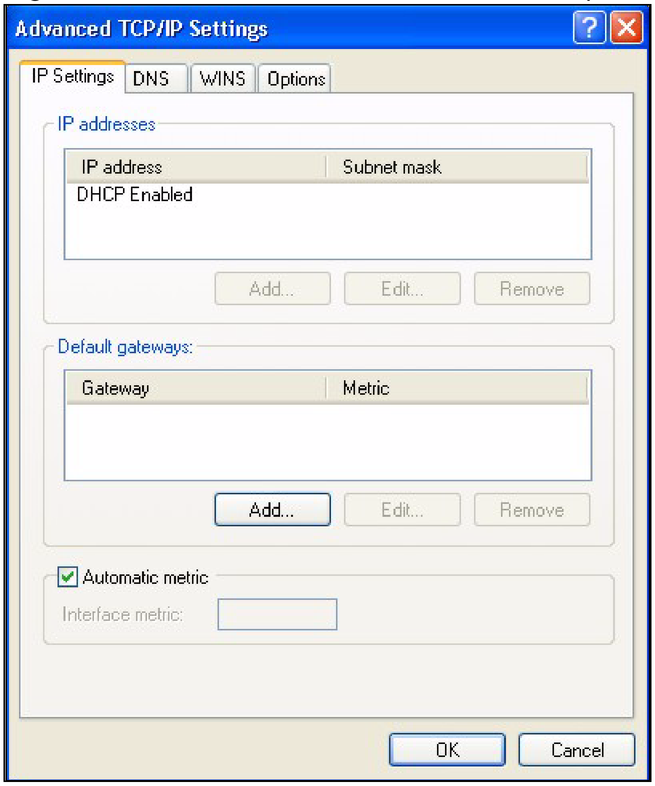


6 If you do not know your gateway's IP address, remove any previously installed gateways in the **IP Settings** tab and click **OK**.

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

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

Figure 400 Windows XP: Advanced TCP/IP Properties

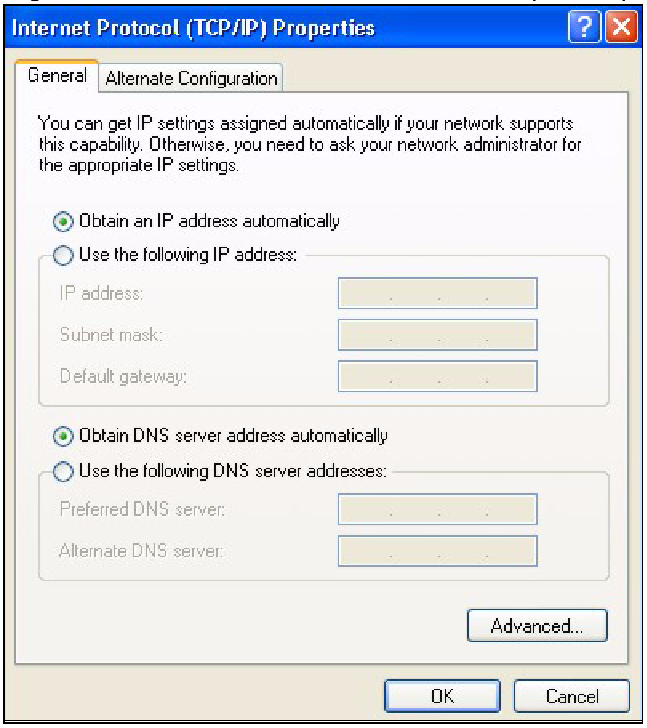


7 In the **Internet Protocol TCP/IP Properties** window (the **General** tab in Windows XP):

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

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

Figure 401 Windows XP: Internet Protocol (TCP/IP) Properties



8 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.

9 Click **Close** (**OK** in Windows 2000/NT) to close the **Local Area Connection Properties** window.

10 Close the **Network Connections** window (**Network and Dial-up Connections** in Windows 2000/NT).

11 Turn on your LAN-Cell and restart your computer (if prompted).

Verifying Settings

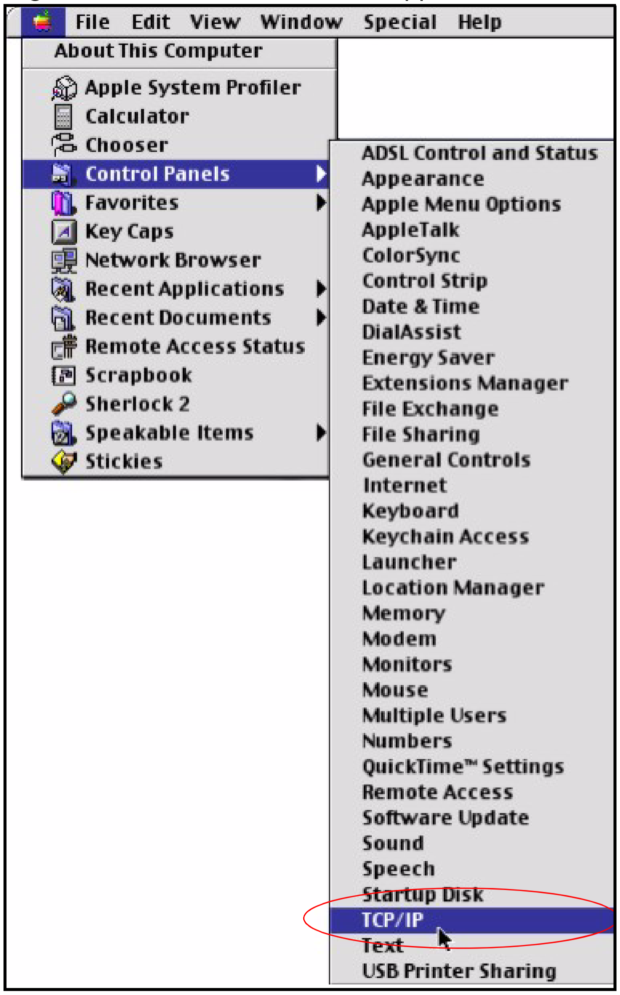
1 Click **Start**, **All Programs**, **Accessories** and then **Command Prompt**.

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

Macintosh OS 8/9

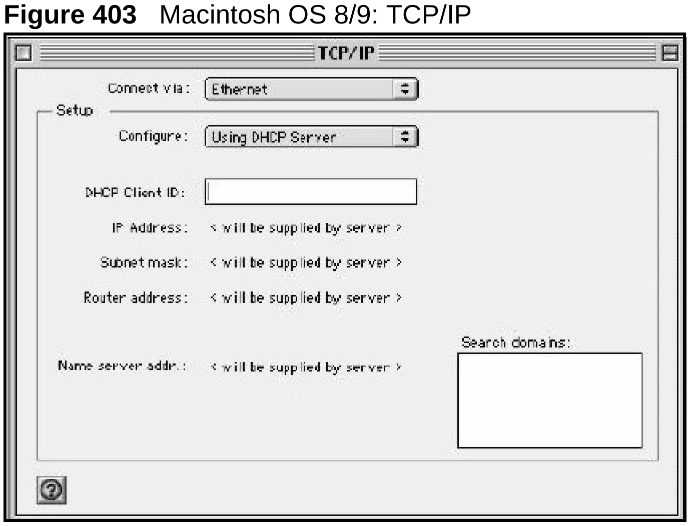
1 Click the **Apple** menu, **Control Panel** and double-click **TCP/IP** to open the **TCP/IP Control Panel**.

Figure 402 Macintosh OS 8/9: Apple Menu



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

Figure 403 Macintosh OS 8/9: TCP/IP



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

4 For statically assigned settings, do the following:

- From the **Configure** box, select **Manually**.

- Type your IP address in the **IP Address** box.
- Type your subnet mask in the **Subnet mask** box.
- Type the IP address of your LAN-Cell in the **Router address** box.

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

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

7 Turn on your LAN-Cell and restart your computer (if prompted).

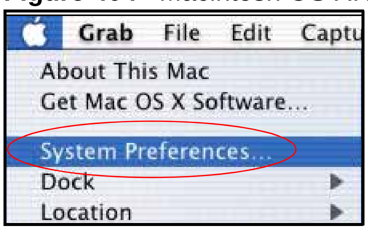
Verifying Settings

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

Macintosh OS X

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

Figure 404 Macintosh OS X: Apple Menu

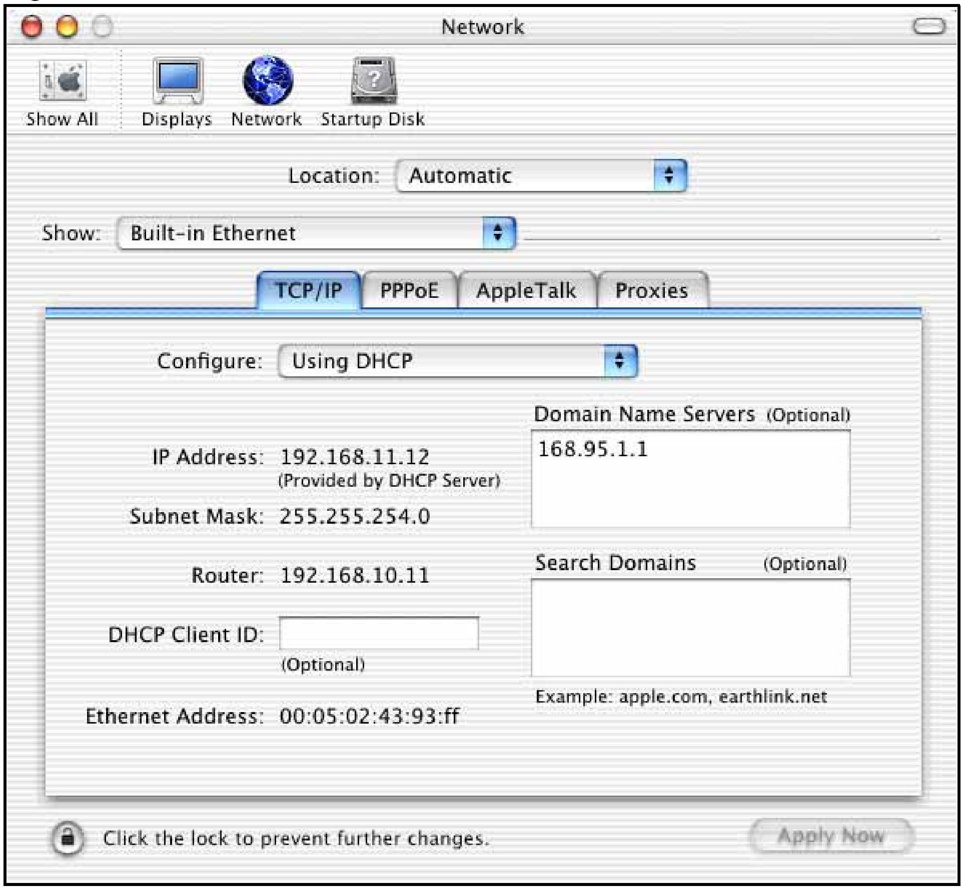


2 Click **Network** in the icon bar.

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

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

Figure 405 Macintosh OS X: Network



4 For statically assigned settings, do the following:

- From the **Configure** box, select **Manually**.
- Type your IP address in the **IP Address** box.
- Type your subnet mask in the **Subnet mask** box.
- Type the IP address of your LAN-Cell in the **Router address** box.

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

6 Turn on your LAN-Cell and restart your computer (if prompted).

Verifying Settings

Check your TCP/IP properties in the **Network** window.

Linux

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

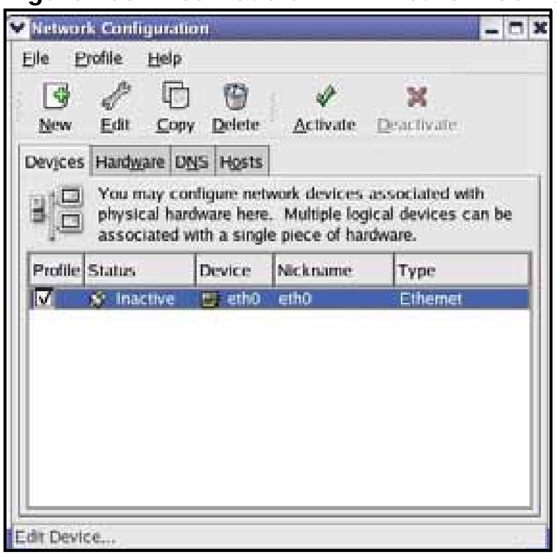
Make sure you are logged in as the root administrator.

Using the K Desktop Environment (KDE)

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

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

Figure 406 Red Hat 9.0: KDE: Network Configuration: Devices



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

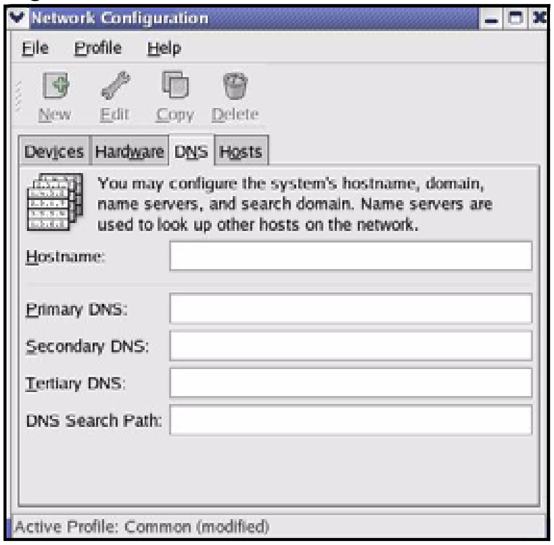
Figure 407 Red Hat 9.0: KDE: Ethernet Device: General

- If you have a dynamic IP address, click **Automatically obtain IP address settings with** and select **dhcp** from the drop down list.
- If you have a static IP address, click **Statically set IP Addresses** and fill in the **Address**, **Subnet mask**, and **Default Gateway Address** fields.

3 Click **OK** to save the changes and close the **Ethernet Device General** screen.

4 If you know your DNS server IP address(es), click the **DNS** tab in the **Network Configuration** screen. Enter the DNS server information in the fields provided.

Figure 408 Red Hat 9.0: KDE: Network Configuration: DNS



5 Click the **Devices** tab.

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

Figure 409 Red Hat 9.0: KDE: Network Configuration: Activate

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

Using Configuration Files

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

1 Assuming that you have only one network card on the computer, locate the `ifconfig-eth0` configuration file (where `eth0` is the name of the Ethernet card). Open the configuration file with any plain text editor.

- If you have a dynamic IP address, enter **dhcp** in the `BOOTPROTO=` field. The following figure shows an example.

Figure 410 Red Hat 9.0: Dynamic IP Address Setting in ifconfig-eth0

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

- If you have a static IP address, enter **`static`** in the `BOOTPROTO=` field. Type `IPADDR=` followed by the IP address (in dotted decimal notation) and type `NETMASK=` followed by the subnet mask. The following example shows an example where the static IP address is 192.168.1.10 and the subnet mask is 255.255.255.0.

Figure 411 Red Hat 9.0: Static IP Address Setting in ifconfig-eth0

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=static
IPADDR=192.168.1.10
NETMASK=255.255.255.0
USERCTL=no
PEERDNS=yes
TYPE=Ethernet
```

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

Figure 412 Red Hat 9.0: DNS Settings in resolv.conf

```
nameserver 172.23.5.1
nameserver 172.23.5.2
```

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

Figure 413 Red Hat 9.0: Restart Ethernet Card

```
[root@localhost init.d]# network restart

Shutting down interface eth0:                [OK]
Shutting down loopback interface:            [OK]
Setting network parameters:                  [OK]
Bringing up loopback interface:              [OK]
Bringing up interface eth0:                  [OK]
```

Verifying Settings

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

Figure 414 Red Hat 9.0: Checking TCP/IP Properties

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

C

IP Addresses and Subnetting

This appendix introduces IP addresses, IP address classes and subnet masks. You use subnet masks to subdivide a network into smaller logical networks.

Introduction to IP Addresses

An IP address has two parts: the network number and the host ID. Routers use the network number to send packets to the correct network, while the host ID identifies a single device on the network.

An IP address is made up of four octets, written in dotted decimal notation, for example, 192.168.1.1. (An octet is an 8-digit binary number. Therefore, each octet has a possible range of 00000000 to 11111111 in binary, or 0 to 255 in decimal.)

There are several classes of IP addresses. The first network number (192 in the above example) defines the class of IP address. These are defined as follows:

- Class A: 0 to 127
- Class B: 128 to 191
- Class C: 192 to 223
- Class D: 224 to 239
- Class E: 240 to 255

IP Address Classes and Hosts

The class of an IP address determines the number of hosts you can have on your network.

- In a class A address the first octet is the network number, and the remaining three octets are the host ID.
- In a class B address the first two octets make up the network number, and the two remaining octets make up the host ID.
- In a class C address the first three octets make up the network number, and the last octet is the host ID.

The following table shows the network number and host ID arrangement for classes A, B and C.

Table 238 Classes of IP Addresses

IP ADDRESS	OCTET 1	OCTET 2	OCTET 3	OCTET 4
Class A	**Network number**	Host ID	Host ID	Host ID

Table 238 Classes of IP Addresses (continued)

IP ADDRESS	OCTET 1	OCTET 2	OCTET 3	OCTET 4
Class B	**Network number**	**Network number**	Host ID	Host ID
Class C	**Network number**	**Network number**	**Network number**	Host ID

An IP address with host IDs of all zeros is the IP address of the network (192.168.1.0 for example). An IP address with host IDs of all ones is the broadcast address for that network (192.168.1.255 for example). Therefore, to determine the total number of hosts allowed in a network, deduct two as shown next:

- A class C address (1 host octet: 8 host bits) can have $2^8 – 2$, or 254 hosts.
- A class B address (2 host octets: 16 host bits) can have $2^{16} – 2$, or 65534 hosts.

A class A address (3 host octets: 24 host bits) can have $2^{24} – 2$ hosts, or approximately 16 million hosts.

IP Address Classes and Network ID

The value of the first octet of an IP address determines the class of an IP address as already stated. These are the details of how that range is determined.

- Class A addresses have a **0** in the leftmost bit.
- Class B addresses have a **1** in the leftmost bit and a **0** in the next leftmost bit.
- Class C addresses start with **1 1 0** in the first three leftmost bits.
- Class D addresses begin with **1 1 1 0**. Class D addresses are used for multicasting, which is used to send information to groups of computers.
- There is also a class E. It is reserved for future use.

The following table shows the allowed ranges for the first octet of each class. This range determines the number of subnets you can have in a network.

Table 239 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
Class E (reserved)	**1111**0000 to **1111**1111	240 to 255

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. 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 like IP addresses. The "natural" masks for class A, B and C IP addresses are as follows.

Table 240 "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 leftmost 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.

Table 241 Alternative Subnet Mask Notation

SUBNET MASK	SUBNET MASK "1" BITS	LAST OCTET BIT VALUE	DECIMAL
255.255.255.0	/24	0000 0000	0
255.255.255.128	/25	1000 0000	128
255.255.255.192	/26	1100 0000	192
255.255.255.224	/27	1110 0000	224
255.255.255.240	/28	1111 0000	240
255.255.255.248	/29	1111 1000	248
255.255.255.252	/30	1111 1100	252

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.

Table 242 Two Subnets Example

IP/SUBNET MASK	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”).

To make two 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 make 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.

Table 243 Subnet 1

IP/SUBNET MASK	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	

Table 244 Subnet 2

IP/SUBNET MASK	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

Table 244 Subnet 2 (continued)

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
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	

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 (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 zeroes is the subnet itself, all ones is the broadcast address on the subnet).

Table 245 Subnet 1

IP/SUBNET MASK	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	

Table 246 Subnet 2

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

Table 247 Subnet 3

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	**10**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.128	Lowest Host ID: 192.168.1.129	
Broadcast Address: 192.168.1.191	Highest Host ID: 192.168.1.190	

Table 248 Subnet 4

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

Example Eight Subnets

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

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

Table 249 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	225	254	255

The following table is a summary for class “C” subnet planning.

Table 250 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

Table 250 Class C Subnet Planning (continued)

NO. “BORROWED” HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
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 (see Table 238 on page 605) available for subnetting.

The following table is a summary for class “B” subnet planning.

Table 251 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
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

D

Common Services

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

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

Table 252 Commonly Used Services

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

Table 252 Commonly Used Services (continued)

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

Table 252 Commonly Used Services (continued)

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

E

Wireless LANs

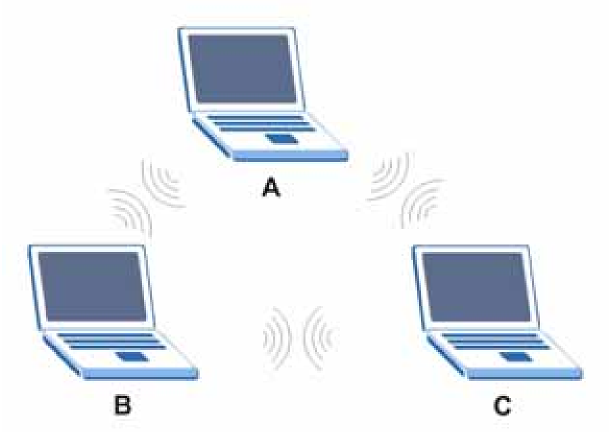
Wireless LAN Topologies

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

Ad-hoc Wireless LAN Configuration

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

Figure 415 Peer-to-Peer Communication in an Ad-hoc Network

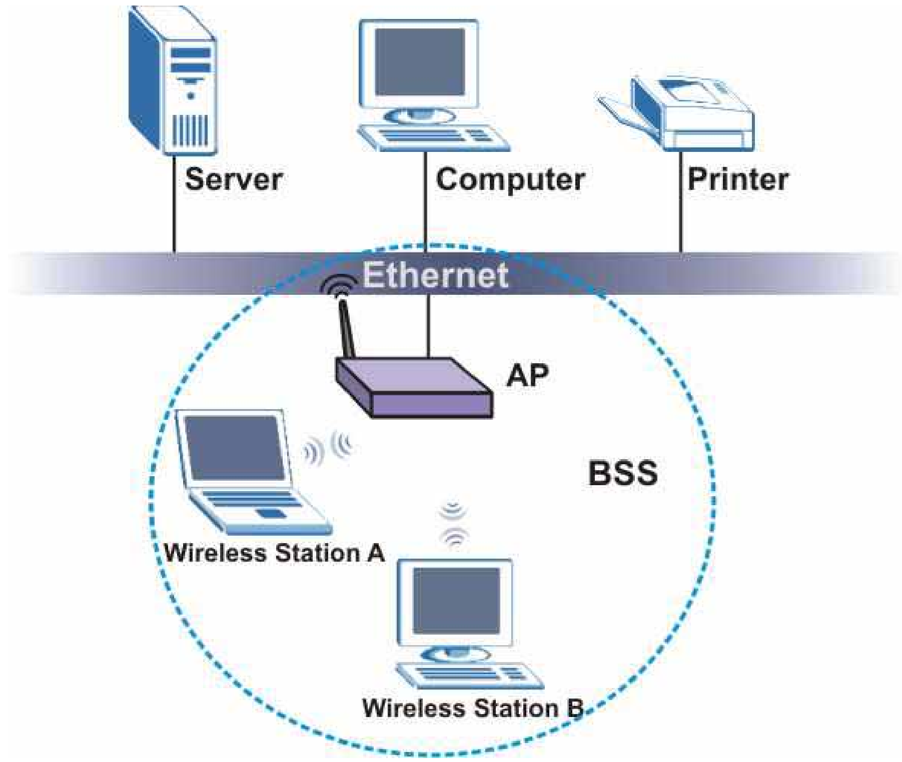


BSS

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

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

Figure 416 Basic Service Set



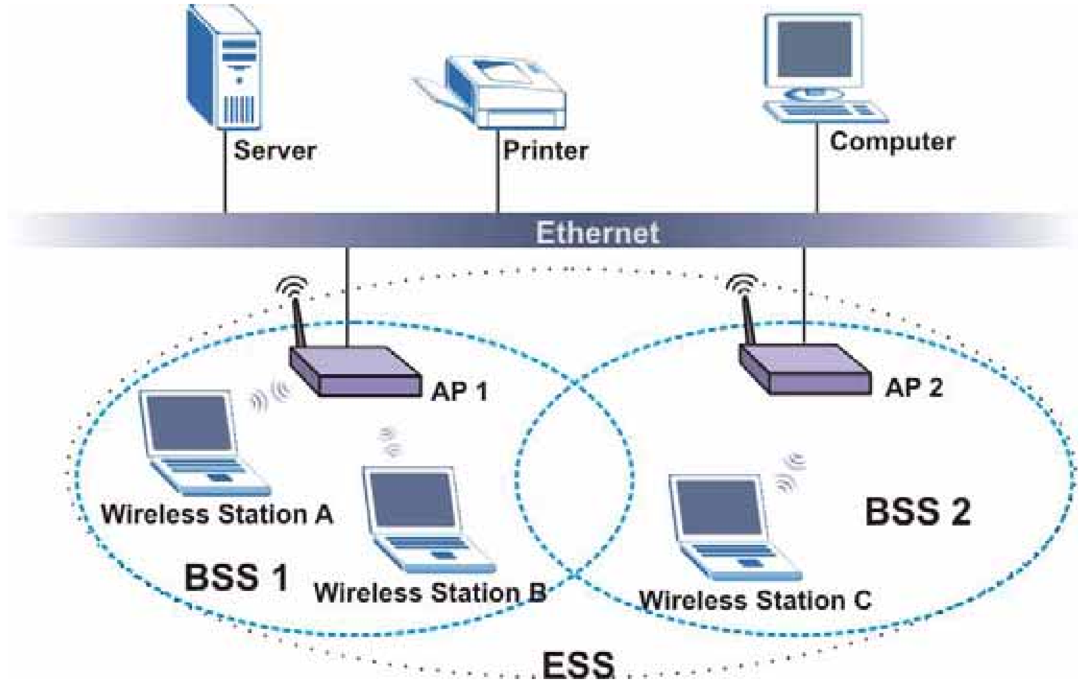
ESS

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

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

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

Figure 417 Infrastructure WLAN



Channel

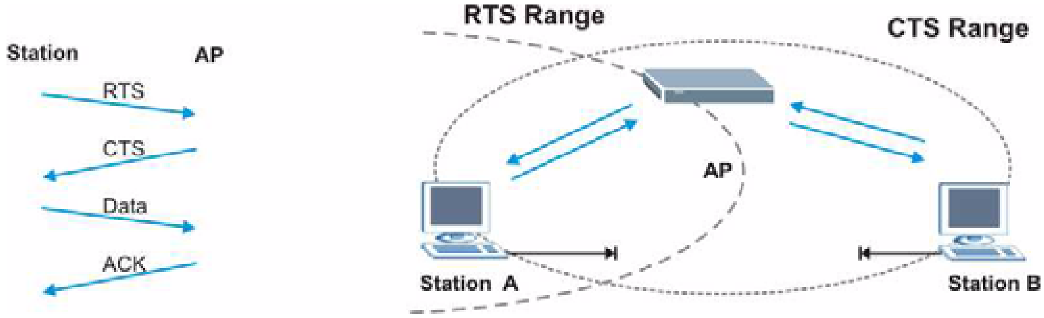
A channel is the radio frequency(ies) used by IEEE 802.11a/b/g wireless devices. Channels available depend on your geographical area. You may have a choice of channels (for your region) so you should use a different channel than an adjacent AP (access point) to reduce interference. Interference occurs when radio signals from different access points overlap causing interference and degrading performance.

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

RTS/CTS

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

Figure 418 RTS/CTS



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

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

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

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

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

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

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

Fragmentation Threshold

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

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

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

Preamble Type

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

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

Select **Long** preamble if you are unsure what preamble mode the wireless adapters support, and to provide more reliable communications in busy wireless networks.

Select **Short** preamble if you are sure the wireless adapters support it, and to provide more efficient communications.

Select **Dynamic** to have the AP automatically use short preamble when wireless adapters support it, otherwise the AP uses long preamble.

The AP and the wireless adapters MUST use the same preamble mode in order to communicate.

IEEE 802.11g Wireless LAN

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

Table 253 IEEE 802.11g

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

Wireless Security Overview

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

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

The following figure shows the relative effectiveness of these wireless security methods available on your LAN-Cell.

Table 254 Wireless Security Levels

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

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

IEEE 802.1x

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

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

RADIUS

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

- Authentication

  Determines the identity of the users.
- Authorization

Determines the network services available to authenticated users once they are connected to the network.

- Accounting

  Keeps track of the client’s network activity.

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

Types of RADIUS Messages

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

- Access-Request

  Sent by an access point requesting authentication.
- Access-Reject

  Sent by a RADIUS server rejecting access.
- Access-Accept

  Sent by a RADIUS server allowing access.
- Access-Challenge

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

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

- Accounting-Request

  Sent by the access point requesting accounting.
- Accounting-Response

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

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

Types of EAP Authentication

This section discusses some popular authentication types: EAP-MD5, EAP-TLS, EAP-TTLS, PEAP and LEAP. Your wireless LAN device may not support all authentication types.

EAP (Extensible Authentication Protocol) is an authentication protocol that runs on top of the IEEE 802.1x transport mechanism in order to support multiple types of user authentication. By using EAP to interact with an EAP-compatible RADIUS server, an access point helps a wireless station and a RADIUS server perform authentication.

The type of authentication you use depends on the RADIUS server and an intermediary AP(s) that supports IEEE 802.1x. .

For EAP-TLS authentication type, you must first have a wired connection to the network and obtain the certificate(s) from a certificate authority (CA). A certificate (also called digital IDs) can be used to authenticate users and a CA issues certificates and guarantees the identity of each certificate owner.

EAP-MD5 (Message-Digest Algorithm 5)

MD5 authentication is the simplest one-way authentication method. The authentication server sends a challenge to the wireless client. The wireless client ‘proves’ that it knows the password by encrypting the password with the challenge and sends back the information. Password is not sent in plain text.

However, MD5 authentication has some weaknesses. Since the authentication server needs to get the plaintext passwords, the passwords must be stored. Thus someone other than the authentication server may access the password file. In addition, it is possible to impersonate an authentication server as MD5 authentication method does not perform mutual authentication. Finally, MD5 authentication method does not support data encryption with dynamic session key. You must configure WEP encryption keys for data encryption.

EAP-TLS (Transport Layer Security)

With EAP-TLS, digital certifications are needed by both the server and the wireless clients for mutual authentication. The server presents a certificate to the client. After validating the identity of the server, the client sends a different certificate to the server. The exchange of certificates is done in the open before a secured tunnel is created. This makes user identity vulnerable to passive attacks. A digital certificate is an electronic ID card that authenticates the sender’s identity. However, to implement EAP-TLS, you need a Certificate Authority (CA) to handle certificates, which imposes a management overhead.

EAP-TTLS (Tunneled Transport Layer Service)

EAP-TTLS is an extension of the EAP-TLS authentication that uses certificates for only the server-side authentications to establish a secure connection. Client authentication is then done by sending username and password through the secure connection, thus client identity is protected. For client authentication, EAP-TTLS supports EAP methods and legacy authentication methods such as PAP, CHAP, MS-CHAP and MS-CHAP v2.

PEAP (Protected EAP)

Like EAP-TTLS, server-side certificate authentication is used to establish a secure connection, then use simple username and password methods through the secured connection to authenticate the clients, thus hiding client identity. However, PEAP only supports EAP methods, such as EAP-MD5, EAP-MSCHAPv2 and EAP-GTC (EAP-Generic Token Card), for client authentication. EAP-GTC is implemented only by Cisco.

LEAP

LEAP (Lightweight Extensible Authentication Protocol) is a Cisco implementation of IEEE 802.1x.

Dynamic WEP Key Exchange

The AP maps a unique key that is generated with the RADIUS server. This key expires when the wireless connection times out, disconnects or reauthentication times out. A new WEP key is generated each time reauthentication is performed.

If this feature is enabled, it is not necessary to configure a default encryption key in the Wireless screen. You may still configure and store keys here, but they will not be used while Dynamic WEP is enabled.

EAP-MD5 cannot be used with Dynamic WEP Key Exchange

For added security, certificate-based authentications (EAP-TLS, EAP-TTLS and PEAP) use dynamic keys for data encryption. They are often deployed in corporate environments, but for public deployment, a simple user name and password pair is more practical. The following table is a comparison of the features of authentication types.

Table 255 Comparison of EAP Authentication Types

	EAP-MD5	EAP-TLS	EAP-TTLS	PEAP	LEAP
Mutual Authentication	No	Yes	Yes	Yes	Yes
Certificate – Client	No	Yes	Optional	Optional	No
Certificate – Server	No	Yes	Yes	Yes	No
Dynamic Key Exchange	No	Yes	Yes	Yes	Yes
Credential Integrity	None	Strong	Strong	Strong	Moderate
Deployment Difficulty	Easy	Hard	Moderate	Moderate	Moderate
Client Identity Protection	No	No	Yes	Yes	No

WPA and WPA2

Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i standard. WPA2 (IEEE 802.11i) is a wireless security standard that defines stronger encryption, authentication and key management than WPA.

Key differences between WPA or WPA2 and WEP are improved data encryption and user authentication.

If both an AP and the wireless clients support WPA2 and you have an external RADIUS server, use WPA2 for stronger data encryption. If you don't have an external RADIUS server, you should use WPA2-PSK (WPA2-Pre-Shared Key) that only requires a single (identical) password entered into each access point, wireless gateway and wireless client. As long as the passwords match, a wireless client will be granted access to a WLAN.

If the AP or the wireless clients do not support WPA2, just use WPA or WPA-PSK depending on whether you have an external RADIUS server or not.

Select WEP only when the AP and/or wireless clients do not support WPA or WPA2. WEP is less secure than WPA or WPA2.

Encryption

Both WPA and WPA2 improve data encryption by using Temporal Key Integrity Protocol (TKIP), Message Integrity Check (MIC) and IEEE 802.1x. WPA and WPA2 use Advanced Encryption Standard (AES) in the Counter mode with Cipher block chaining Message authentication code Protocol (CCMP) to offer stronger encryption than TKIP.

TKIP uses 128-bit keys that are dynamically generated and distributed by the authentication server. AES (Advanced Encryption Standard) is a block cipher that uses a 256-bit mathematical algorithm called Rijndael. They both include a per-packet key mixing function, a Message Integrity Check (MIC) named Michael, an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism.

WPA and WPA2 regularly change and rotate the encryption keys so that the same encryption key is never used twice.

The RADIUS server distributes a Pairwise Master Key (PMK) key to the AP that then sets up a key hierarchy and management system, using the PMK to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients. This all happens in the background automatically.

The Message Integrity Check (MIC) is designed to prevent an attacker from capturing data packets, altering them and resending them. The MIC provides a strong mathematical function in which the receiver and the transmitter each compute and then compare the MIC. If they do not match, it is assumed that the data has been tampered with and the packet is dropped.

By generating unique data encryption keys for every data packet and by creating an integrity checking mechanism (MIC), with TKIP and AES it is more difficult to decrypt data on a Wi-Fi network than WEP and difficult for an intruder to break into the network.

The encryption mechanisms used for WPA(2) and WPA(2)-PSK are the same. The only difference between the two is that WPA(2)-PSK uses a simple common password, instead of user-specific credentials. The common-password approach makes WPA(2)-PSK susceptible to brute-force password-guessing attacks but it’s still an improvement over WEP as it employs a consistent, single, alphanumeric password to derive a PMK which is used to generate unique temporal encryption keys. This prevent all wireless devices sharing the same encryption keys. (a weakness of WEP)

User Authentication

WPA and WPA2 apply IEEE 802.1x and Extensible Authentication Protocol (EAP) to authenticate wireless clients using an external RADIUS database. WPA2 reduces the number of key exchange messages from six to four (CCMP 4-way handshake) and shortens the time required to connect to a network. Other WPA2 authentication features that are different from WPA include key caching and pre-authentication. These two features are optional and may not be supported in all wireless devices.

Key caching allows a wireless client to store the PMK it derived through a successful authentication with an AP. The wireless client uses the PMK when it tries to connect to the same AP and does not need to go with the authentication process again.

Pre-authentication enables fast roaming by allowing the wireless client (already connecting to an AP) to perform IEEE 802.1x authentication with another AP before connecting to it.

Wireless Client WPA Supplicants

A wireless client supplicant is the software that runs on an operating system instructing the wireless client how to use WPA. At the time of writing, the most widely available supplicant is the WPA patch for Windows XP, Funk Software's Odyssey client.

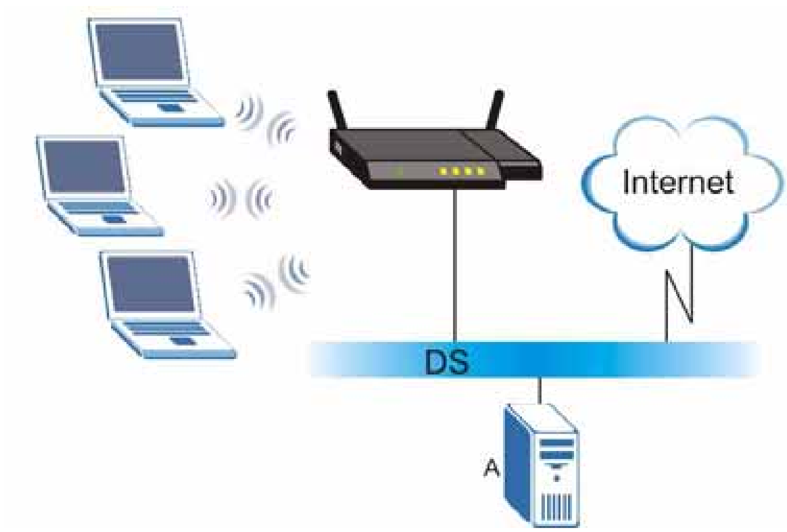
The Windows XP patch is a free download that adds WPA capability to Windows XP's built-in "Zero Configuration" wireless client. However, you must run Windows XP to use it.

WPA(2) with RADIUS Application Example

You need the IP address of the RADIUS server, its port number (default is 1812), and the RADIUS shared secret. A WPA(2) application example with an external RADIUS server looks as follows. "A" is the RADIUS server. "DS" is the distribution system.

1. The AP passes the wireless client's authentication request to the RADIUS server.
2. The RADIUS server then checks the user's identification against its database and grants or denies network access accordingly.
3. The RADIUS server distributes a Pairwise Master Key (PMK) key to the AP that then sets up a key hierarchy and management system, using the pair-wise key to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients.

Figure 419 WPA(2) with RADIUS Application Example



WPA(2)-PSK Application Example

A WPA(2)-PSK application looks as follows.

1. First enter identical passwords into the AP and all wireless clients. The Pre-Shared Key (PSK) must consist of between 8 and 63 ASCII characters or 64 hexadecimal characters (including spaces and symbols).
2. The AP checks each wireless client's password and (only) allows it to join the network if the password matches.
3. The AP and wireless clients use the pre-shared key to generate a common PMK (Pairwise Master Key).

4 The AP and wireless clients use the TKIP or AES encryption process to encrypt data exchanged between them.

Figure 420 WPA(2)-PSK Authentication

Security Parameters Summary

Refer to this table to see what other security parameters you should configure for each Authentication Method/ key management protocol type. MAC address filters are not dependent on how you configure these security features.

Table 256 Wireless Security Relational Matrix

AUTHENTICATION METHOD/ KEY MANAGEMENT PROTOCOL	ENCRYPTION METHOD	ENTER MANUAL KEY	IEEE 802.1X
Open	None	No	Disable
			Enable without Dynamic WEP Key
Open	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable
Shared	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable
WPA	TKIP/AES	No	Enable
WPA-PSK	TKIP/AES	Yes	Disable
WPA2	TKIP/AES	No	Enable
WPA2-PSK	TKIP/AES	Yes	Disable

Roaming

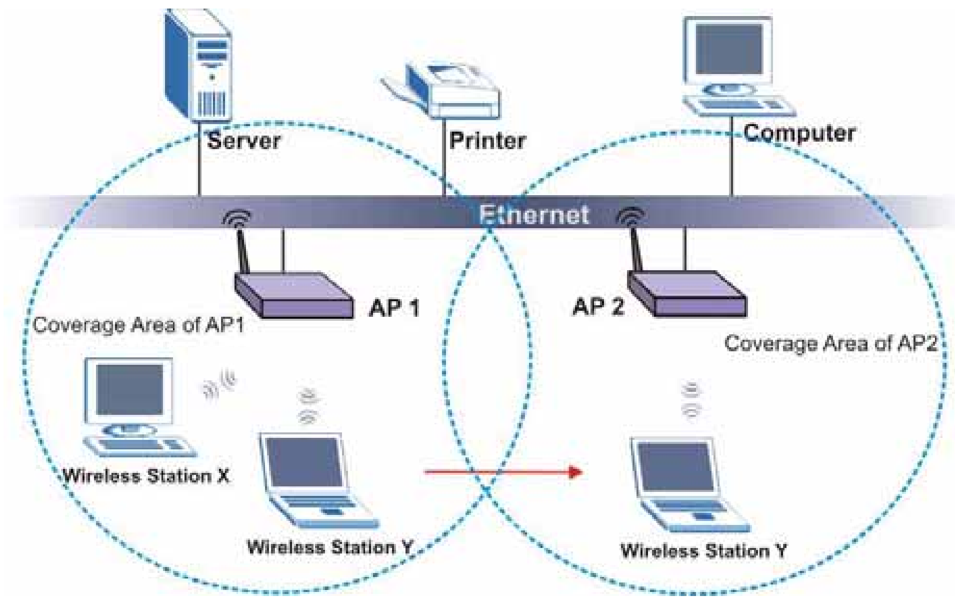
An AP creates its own wireless coverage area. A wireless station can associate with a particular access point only if it is within the access point’s coverage area.

In a network environment with multiple access points, wireless stations are able to switch from one access point to another as they move between the coverage areas. This is roaming. As the wireless station moves from place to place, it is responsible for choosing the most appropriate access point depending on the signal strength, network utilization or other factors.

The roaming feature on the access points allows the access points to relay information about the wireless stations to each other. When a wireless station moves from a coverage area to another, it scans and uses the channel of a new access point, which then informs the other access points on the LAN about the change. The new information is then propagated to the other access points on the LAN. An example is shown in Figure 421 on page 629.

If the roaming feature is not enabled on the access points, information is not communicated between the access points when a wireless station moves between coverage areas. The wireless station may not be able to communicate with other wireless stations on the network and vice versa.

Figure 421 Roaming Example



The steps below describe the roaming process.

1. Wireless station **Y** moves from the coverage area of access point **AP 1** to that of access point **AP 2**.
2. Wireless station **Y** scans and detects the signal of access point **AP 2**.
3. Wireless station **Y** sends an association request to access point **AP 2**.
4. Access point **AP 2** acknowledges the presence of wireless station **Y** and relays this information to access point **AP 1** through the wired LAN.

Requirements for Roaming

The following requirements must be met in order for wireless stations to roam between the coverage areas.

1. All the access points must be on the same subnet and configured with the same ESSID.
2. If IEEE 802.1x user authentication is enabled and to be done locally on the access point, the new access point must have the user profile for the wireless station.

3 The adjacent access points should use different radio channels when their coverage areas overlap.
4 All access points must use the same port number to relay roaming information.
5 The access points must be connected to the Ethernet and be able to get IP addresses from a DHCP server if using dynamic IP address assignment.

Antenna Overview

An antenna couples RF signals onto air. A transmitter within a wireless device sends an RF signal to the antenna, which propagates the signal through the air. The antenna also operates in reverse by capturing RF signals from the air.

Positioning the antennas properly increases the range and coverage area of a wireless LAN.

Antenna Characteristics

Frequency

An antenna in the frequency of 2.4GHz (IEEE 802.11b) or 5GHz (IEEE 802.11a) is needed to communicate efficiently in a wireless LAN.

Radiation Pattern

A radiation pattern is a diagram that allows you to visualize the shape of the antenna's coverage area.

Antenna Gain

Antenna gain, measured in dB (decibel), is the increase in coverage within the RF beam width. Higher antenna gain improves the range of the signal for better communications.

For an indoor site, each 1 dB increase in antenna gain results in a range increase of approximately 2.5%. For an unobstructed outdoor site, each 1dB increase in gain results in a range increase of approximately 5%. Actual results may vary depending on the network environment.

Antenna gain is sometimes specified in dBi, which is how much the antenna increases the signal power compared to using an isotropic antenna. An isotropic antenna is a theoretical perfect antenna that sends out radio signals equally well in all directions. dBi represents the true gain that the antenna provides.

Connector

The WLAN antenna connector on the LAN-Cell 2 is a reverse polarity SMA jack (SMA-RP Male). Connect only antennas with female reverse polarity SMA plugs (SMA-RP Female) to this jack.

Types of Antennas for WLAN

There are two types of antennas used for wireless LAN applications.

- Omni-directional antennas send the RF signal out in all directions on a horizontal plane. The coverage area is torus-shaped (like a donut) which makes these antennas ideal for a room environment. With a wide coverage area, it is possible to make circular overlapping coverage areas with multiple access points.
- Directional antennas concentrate the RF signal in a beam, like a flashlight does with the light from its bulb. The angle of the beam determines the width of the coverage pattern. Angles typically range from 20 degrees (very directional) to 120 degrees (less directional). Directional antennas are ideal for hallways and outdoor point-to-point applications.

Positioning Antennas

In general, antennas should be mounted as high as practically possible and free of obstructions. In point-to–point application, position both antennas at the same height and in a direct line of sight to each other to attain the best performance.

For omni-directional antennas mounted on a table, desk, and so on, point the antenna up. For omni-directional antennas mounted on a wall or ceiling, point the antenna down. For a single AP application, place omni-directional antennas as close to the center of the coverage area as possible.

For directional antennas, point the antenna in the direction of the desired coverage area.

Country Codes

The table below lists the 3 digit Country Code values for selecting the correct 802.11 radio channel frequencies for different countries/regions. See Section 7.10 on page 162 for instructions on changing the LAN-Cell's default country code (255 - U.S./North America).

If your country is not listed, contact Proxicast Customer Support.

Table 257 Country Codes

COUNTRY	COUNTRY CODE
Australia	244
Astria	233
Belgium	248
Brazil	208
China	222
Czech	246
Denmark	252
European CTR21	212

COUNTRY	COUNTRY CODE
Finland	240
France	219
Germany	237
Greece	247
Hong Kong	242
Hungary	229
India	214
Ireland	235
Israel	226
Italy	236
Japan	234
Malaysia	232
Morocco	239
Netherlands	253
New Zealand	243
Norway	245
Peru	209
Philippines	216
Poland	231
Portugal	220
Romania	207
Russia	230
S.Africa	254
S.Korea	217
Singapore	241
Slovak	228
Slovenia	215
Spain	213
Sweden	250
Switzerland	225
Taiwan	238
Thailand	227
Turkey	211
UAE	224
UK	249
Ukraine	221
USA / N. America	255

F

Brute-Force Password Guessing Protection

Brute-force password guessing protection allows you to specify a wait-time that must expire before entering a fourth password after three incorrect passwords have been entered.

The following describes the commands for enabling, disabling and configuring the brute-force password guessing protection mechanism for the password. See Section 39.1 on page 543 for information on the command structure.

Table 258 Brute-Force Password Guessing Protection Commands

COMMAND	DESCRIPTION
sys pwderrtm	This command displays the brute-force guessing password protection settings.
sys pwderrtm 0	This command turns off the password's protection from brute-force guessing. The brute-force password guessing protection is turned off by default.
sys pwderrtm N	This command sets the password protection to block all access attempts for N (a number from 1 to 60) minutes after the third time an incorrect password is entered.

Example

```
sys pwderrtm 5
```

This command sets the password protection to block all access attempts for five minutes after the third time an incorrect password is entered.

G

Legal Information

Copyright

Disclaimer

Proxicast does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. Proxicast further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Trademarks

Proxicast is a registered trademark and ProxiOS (Proxicast Network Operating System), LAN-Cell, Cell-Guard, Cell-Lock, and Cell-Sentry are trademarks of Proxicast, LLC. Other trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

Certifications

Federal Communications Commission (FCC) Interference Statement

The device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operations.

This device has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This device generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this device does cause harmful interference to radio/television reception, which can be determined by turning the device off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

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

FCC Radiation Exposure Statement

- This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
- For operation within 5.15 ~ 5.25GHz frequency range, it is restricted to indoor environment.
- IEEE 802.11b or 802.11g operation of this product in the U.S.A. is firmware-limited to channels 1 through 11.
- To comply with FCC RF exposure compliance requirements, a separation distance of at least 20 cm must be maintained between the antenna of this device and all persons.

Notices

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This device has been designed for the WLAN 2.4 GHz and 5 GHz networks throughout the EC region and Switzerland, with restrictions in France.

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

Proxicast Limited Warranty

Proxicast warrants to the original end user (purchaser) that this product is free from any defects in materials or workmanship for a period of up to one year from the date of purchase. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, Proxicast will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal value, and will be solely at the discretion of Proxicast. This warranty shall not apply if the product is modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. Proxicast shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact Proxicast's Service Center for your Return Material Authorization number (RMA). Products must be returned Postage Prepaid. It is recommended that the unit be insured when shipped. Any returned products without proof of purchase or those with an out-dated warranty will be repaired or replaced (at the discretion of Proxicast) and the customer will be billed for parts and labor. All repaired or replaced products will be shipped by Proxicast to the corresponding return address, Postage Paid. This warranty gives you specific legal rights, and you may also have other rights that vary from country to country.

H

Customer Support

Online Web Support

Please refer to support.proxicast.com for additional support documentation and access to our Knowledgebase which contains many resources such as.TechNotes, Frequently Asked Questions, sample configurations and firmware updates.

E-Mail Support

Support E-mail: support@proxicast.com

Please provide the following information when you contact customer support:

- Product model and serial number.
- Current firmware version running on the device
- Date that you received your device.
- Brief description of the problem and the steps you took to solve it.

Corporate Headquarters (Worldwide Customer Support)

- Sales E-mail: sales@proxicast.com
- Telephone: 877-777-7694 (412-213-0018)
- Fax: 412-492-9386
- Web Site: www.proxicast.com, support.proxicast.com
- Regular Mail & RMA Shipments:
  Proxicast, LLC
  312 Sunnyfield Drive, Suite 200
  Glenshaw, PA 15116-1936

Return Merchandise Authorizations (RMA)

If you need to return a product for service, you must contact Customer Support and request an RMA Number. Returns will not be accepted without an RMA Number on the outside of the shipment.

Please return only the main product unit (no accessories) unless otherwise directed by Proxicast Customer Support.

Securely pack and insure the product. Return shipping costs are the responsibiliy of the customer.

Index

Symbols

Numerics

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

X