# *LAN-Cell Gateway Series*

***Secure Cellular Data Gateway***

# *User's Guide*

Version 3.62

July 2004

proxicast™

# 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, LAN-Cell, ProxiOS, 1x Mobile Gateway, 1xMG, and the Proxicast logo are all trademarks/servicemarks of Proxicast, LLC. All other products and company names mentioned in this publication are the property of their respective copyright and/or trademark holders and are used for identification purposes only. The Proxicast LAN-Cell 1x Mobile Gateway is currently patent pending.

# Federal Communications Commission (FCC) Interference Statement

This device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference.
2. This device must accept any interference received, including interference that may cause undesired operations.

Portions of this equipment have 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 commercial environment. This equipment 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.

If this equipment does cause harmful interference to radio/television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and the receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

## Notice

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment. Use only the accessories, attachments, and power supplies provided by the manufacturer – connecting non-approved antennas or power supplies to the LAN-Cell may damage the unit or cause interference and will void your warranty.

## Certifications

**Assembled from Tested Components**
(Complete System Not Tested)

**FOR HOME OR OFFICE USE**

**Contains FCC ID: P4MDT2000DUAL**

# 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 of character 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.

**Online Registration**

Register online registration at www.Proxicast.com for free future product updates and information.

# Customer Support

When you contact your customer support representative please have the following information ready:

- Product model and serial number.
- Warranty Information.
- Date that you received your device.
- Brief description of the problem and the steps you took to solve it.

# Table of Contents

# List of Figures

# List of Tables

# Preface

## About This User's Manual

Congratulations on your purchase of the LAN-Cell Gateway Series. This manual is designed to guide you through the configuration of your LAN-Cell for its various applications.

**Use the web configurator, System Management Terminal (SMT) or command interpreter interface to configure your LAN-Cell. Not all features can be configured through all interfaces.**

The web configurator parts of this guide contain background information on features configurable by the web configurator and the SMT. The SMT parts of this guide contain background information solely on features not configurable by the web configurator.

This manual may refer to the LAN-Cell Gateway Series as the LAN-Cell.

## Related Documentation

- **Support Disk**
  Refer to the included CD for support documents.
- **Quick Start Guide**
  The Quick Start Guide is designed to help you get up and running right away. It contains a detailed easy-to-follow connection diagram, default settings, handy checklists and information on setting up your network and configuring for Internet access.
- **Web Configurator Online Help**
  Embedded web help for descriptions of individual screens and supplementary information.
- **Certifications**
  Refer to the product page at www.Proxicast.com for information on product certifications.
- **Proxicast Support Web Site**
  Please refer to www.Proxicast.com for additional support documentation.

## Syntax Conventions

- The version number on the title page is the latest firmware version that is documented in this *User's Guide*. Earlier versions may also be included.
- "Enter" means for you to type one or more characters and press the carriage return. "Select" or "Choose" means for you to use one of the predefined choices.
- The SMT menu titles and labels are in **Bold Times New Roman** font. Command and arrow keys are enclosed in square brackets. [ENTER] means the Enter, or carriage return key; [ESC] means the Escape key and [SPACE BAR] means the Space Bar.
- The choices of a menu item are in **Bold Arial** font.
- Mouse action sequences are denoted using a comma. For example, "click the Apple icon, **Control Panels** and then **Modem**" means first click the Apple icon, then point your mouse pointer to **Control Panels** and then click **Modem**.
- For brevity's sake, we will use "e.g." as a shorthand for "for instance" and "i.e." for "that is" or "in other words" throughout this manual.

## Graphics Icons Key

| | | |
|---|---|---|
|  LAN-Cell |  Computer |  Notebook Computer |
|  Server |  Modem |  DSLAM (Digital Subscriber Line Access Multiplexer) |
|  Firewall |  Router |  Switch |
|  Wireless Signal | | |

# Part I:

## Getting Started

This part helps you get to know your LAN-Cell, introduces the web configurator and covers how to configure the Setup screens.

# Chapter 1
# Getting to Know Your LAN-Cell

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

## 1.1 Introducing the LAN-Cell

The LAN-Cell is an ideal secure gateway for all data passing between the Internet and your LAN using either the integrated wireless modem, or an external DSL/Cable modem or Ethernet connection.

By integrating NAT, firewall and VPN capability, the LAN-Cell is a complete security solution that protects your Intranet and efficiently manages data traffic on your network.

## 1.2 Features

### 1.2.1 Physical Features

#### 4-Port Switch

A combination of switch and router makes your LAN-Cell a cost-effective and viable network solution. You can connect up to four computers to the LAN-Cell without the cost of a hub. Use a hub to add more than four computers to your LAN.

#### Auto-negotiating 10/100 Mbps Ethernet LAN

The LAN interfaces automatically detect if they are on a 10 or a 100 Mbps Ethernet.

#### Auto-sensing 10/100 Mbps Ethernet LAN

The LAN interfaces automatically adjust to either a crossover or straight-through Ethernet cable.

#### Cellular Modem

The LAN-Cell's integrated cellular modem can be used as the primary WAN interface or it can be configured as a back-up connection when/if ever the broadband connection to the WAN port fails or is unavailable.

#### Ethernet WAN Connection

The LAN-Cell's integrated Ethernet WAN port can be used as the primary WAN interface when connected to an existing LAN or external DSL or Cable Modem.  It can also be configured as a back-up connection when/if ever the Cellular Modem connection to the WAN port fails or is unavailable.

#### Auto-negotiating 10/100 Mbps Ethernet WAN

The 10/100 Mbps Ethernet WAN port attaches to the Internet via broadband modem or router and automatically detects if it's on a 10 or a 100 Mbps Ethernet.

#### Time and Date

The LAN-Cell allows you to get the current time and date from an external server when you turn on your LAN-Cell. You can also set the time manually.

#### Reset Button

The LAN-Cell reset button is built into the front panel. Use this button to restore the factory default password to 1234; IP address to 192.168.1.1, subnet mask to 255.255.255.0 and DHCP server enabled with a pool size of "1" and address 192.168.1.33.

### 1.2.2 Non-Physical Features

#### IPSec VPN Capability

Establish Virtual Private Network (VPN) tunnels to connect computers to your company network using data encryption and the Internet; thus providing secure communications 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.

**The LAN-Cell supports two simultaneous VPN connections.**

#### X-Auth (Extended Authentication)

X-Auth provides added security for VPN by requiring each VPN client to use a username and password.

#### Certificates

The LAN-Cell can use certificates (also called digital IDs) to authenticate users. Certificates are based on public-private key pairs. Certificates provide a way to exchange public keys for use in authentication.

#### SSH

The LAN-Cell uses the SSH (Secure Shell) secure communication protocol to provide secure encrypted communication between two hosts over an unsecured network.

#### HTTPS

HyperText Transfer Protocol over Secure Socket Layer, or HTTP over SSL is a web protocol that encrypts and decrypts web sessions. Use HTTPS for secure web configurator access to the LAN-Cell.

#### Firewall

The LAN-Cell has a stateful inspection firewall with DoS (Denial of Service) protection. By default, when the firewall is activated, all incoming traffic from the WAN to the LAN is blocked unless it is initiated from the LAN. The LAN-Cell firewall supports TCP/UDP inspection, DoS detection and protection, real time alerts, reports and logs.

#### Brute-Force Password Guessing Protection

The LAN-Cell has a special protection mechanism to discourage brute-force password guessing attacks on the LAN-Cell's management interfaces. You can specify a wait-time that must expire before entering a fourth password after three incorrect passwords have been entered. Please see the appendices for details about this feature.

#### Content Filtering

The LAN-Cell can block web features such as ActiveX controls, Java applets and cookies, as well as disable web proxies. The LAN-Cell can block specific URLs by using the keyword feature. It also allows the administrator to define time periods and days during which content filtering is enabled.

#### Packet Filtering

The packet filtering mechanism blocks unwanted traffic from entering/leaving your network.

#### Call Scheduling

Configure call time periods to restrict and allow access for users on remote nodes.

#### PPPoE

PPPoE facilitates the interaction of a host with an Internet modem to achieve access to high-speed data networks via a familiar "dial-up networking" user interface.

#### PPPoE Pass-through

A computer on the LAN-side of the LAN-Cell can initiate a PPPoE session independently of any PPPoE sessions running on the LAN-Cell itself. These "bridged" PPPoE sessions are not restricted to the number of PPPoE sessions allowed on the WAN side.

### 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 a TCP/IP-based network.

PPTP supports on-demand, multi-protocol and virtual private networking over public networks, such as the Internet. The LAN-Cell supports one PPTP server connection at any given time.

### Dynamic DNS Support

With Dynamic DNS (Domain Name System) support, you can have a static hostname alias for a dynamic IP address, allowing the host to be more easily accessible from various locations on the Internet. You must register for this service with DynDNS.ORG, a Dynamic DNS service provider.

### IP Multicast

Deliver IP packets to a specific group of hosts using IP multicast. IGMP (Internet Group Management Protocol) is the protocol used to support multicast groups. The latest version is version 2 (see RFC 2236); the LAN-Cell supports both versions 1 and 2.

### IP Alias

IP Alias allows you to partition a physical network into logical networks over the same Ethernet interface. The LAN-Cell supports three logical LAN interfaces via its single physical Ethernet LAN interface with the LAN-Cell itself as the gateway for each LAN network.

### SNMP

SNMP (Simple Network Management Protocol) is a protocol used for exchanging management information between network devices. SNMP is a member of the TCP/IP protocol suite. Your 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).

### Network Address Translation (NAT)

NAT (Network Address Translation - NAT, RFC 1631) allows the translation of multiple IP addresses used within one network to different IP addresses known within another network.

### Traffic Redirect

Traffic Redirect forwards WAN traffic to a backup gateway when the LAN-Cell cannot connect to the Internet, thus acting as an auxiliary backup when your regular WAN connection fails.

### Port Forwarding

Use this feature to forward incoming service requests to a server on your local network. 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.

### DHCP (Dynamic Host Configuration Protocol)

DHCP (Dynamic Host Configuration Protocol) allows the individual client computers to obtain the TCP/IP configuration at start-up from a centralized DHCP server. The LAN-Cell has built-in DHCP server capability, enabled by default, which means it can assign IP addresses, an IP default gateway and DNS servers to all systems that support the DHCP client. The LAN-Cell can also act as a surrogate DHCP server (**DHCP Relay**) where it relays IP address assignment from another DHCP server to the clients.

### Shared Internet Access

Computers connected to the LAN-side of the LAN-Cell can have simultaneous access to the Internet. Inactive connections can be dropped after a specified idle timeout (see Configuring WAN ISP).

### Full Network Management

The embedded web configurator is an all-platform web-based utility that allows you to easily access the LAN-Cell's management settings and configure the firewall. The LAN-Cell also provides the SMT (System Management Terminal) interface. The SMT is a menu-driven interface that you can access from a terminal emulator over a telnet connection.

### RoadRunner Support

In addition to standard cable modem services, the LAN-Cell supports Time Warner's RoadRunner Service.

### Logging and Tracing

- Built-in message logging and packet tracing.
- Unix syslog facility support.
- Firewall logs.
- Content filtering logs.

### Upgrade LAN-Cell Firmware

The firmware of the LAN-Cell can be upgraded via the LAN or remotely over a WAN connection.

### Embedded FTP and TFTP Servers

The LAN-Cell's embedded FTP and TFTP Servers enable fast firmware upgrades as well as configuration file backups and restoration.

## 1.3 Applications for the LAN-Cell

Here are some examples of what you can do with your LAN-Cell. See www.proxicast.com for additional examples and technical notes on how to configure your LAN-Cell for different scenarios.

- Access Remote Equipment for Data Collection, Control or Monitoring over a Cellular Data Network

  The LAN-Cell can be configured to be "always connected" to a Cellular Data Network. Using either static IP addresses from the cellular carrier (or the LAN-Cell's optional Dynamic DNS feature), you can access any devices attached to the LAN-side of the remote LAN-Cell unit. The LAN-Cell can easily by powered by solar cells for truly remote applications.

- Mobile Workgroups

  Corporate IT departments can provide their mobile workgroups (e.g. construction trailers, temporary locations, client sites, etc.) with an extension of the corporate network. The LAN-Cell can be configured with the same security, content management, and access control policies implemented elsewhere on the corporate network. The LAN-Cell's integrated VPN client feature can provide secure access to corporate systems without special software or configuration on each remote LAN computer.

- High Availability Internet Connection

  The LAN-Cell's ability to automatically redirect WAN-bound traffic to its Ethernet WAN, Cellular Modem, or alternate router interfaces enables it to cost-effectively provide a high degree of Internet access connectivity without manual intervention.

- Secure Cellular Data Access

  The LAN-Cell's built-in VPN client and encryption technology allows you to design and deploy secure data access applications over the public Internet and cellular carrier wireless networks.

- Mixed Ethernet and Serial Device Connections

  Using external serial-to-Ethernet converters and the built-in 4-port 10/100 Ethernet Switch, the LAN-Cell can consolidate multiple serial and Ethernet-based devices into a single WAN/Cellular connection.

- In-Vehicle Applications

  The LAN-Cell is ideal for providing a complete LAN + Cellular Internet Access solution for data-intensive vehicles such as emergency response vans, public safety equipment, watercraft, and insurance adjusters.

# Chapter 2
# Introducing the Web Configurator

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

## 2.1 Web Configurator Overview

The embedded web configurator allows you to manage the LAN-Cell from anywhere through a browser such as Microsoft Internet Explorer or Netscape Navigator. Use Internet Explorer 6.0 and later or Netscape Navigator 7.0 and later versions with JavaScript enabled. It is recommended that you set your screen resolution to 1024 by 768 pixels.

## 2.2 Accessing the LAN-Cell Web Configurator

**Step 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*).

**Step 2.** Launch your web browser.

**Step 3.** Type "192.168.1.1" as the URL.

**Step 4.** Type "1234" (default) as the password and click **Login**. In some versions, the default password appears automatically - if this is the case, click **Login**.

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

**Step 6.** 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.

**Step 7.** You should now see the **MAIN MENU** screen (see *Figure 2-1*).

## 2.3 Resetting the LAN-Cell

If you forget your password or cannot access the SMT menu, you will need to reload the factory-default configuration file or use the **RESET** button located on the front panel 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. Also, the password will be reset to "1234".

### 2.3.1 Procedure To Use The Reset Button

**Step 1.** Make sure the **POWER** LED is on (not blinking) before you begin this procedure.

**Step 2.** Use a paper clip or similar object to press and hold the recessed **RESET** button for 5 seconds. If the **POWER** LED begins to blink, the defaults have been restored and the LAN-Cell restarts.

## 2.4 Navigating the LAN-Cell Web Configurator

We use the LAN-Cell Gateway Web screens in this guide as an example. Screens vary slightly for different LAN-Cell models. The following summarizes how to navigate the web configurator from the **MAIN MENU** screen.

**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.**

**Follow the instructions you see in the MAIN MENU screen or click the icon (located in the top right corner of most screens) to view online help.**

**The icon does not appear in the MAIN MENU screen.**

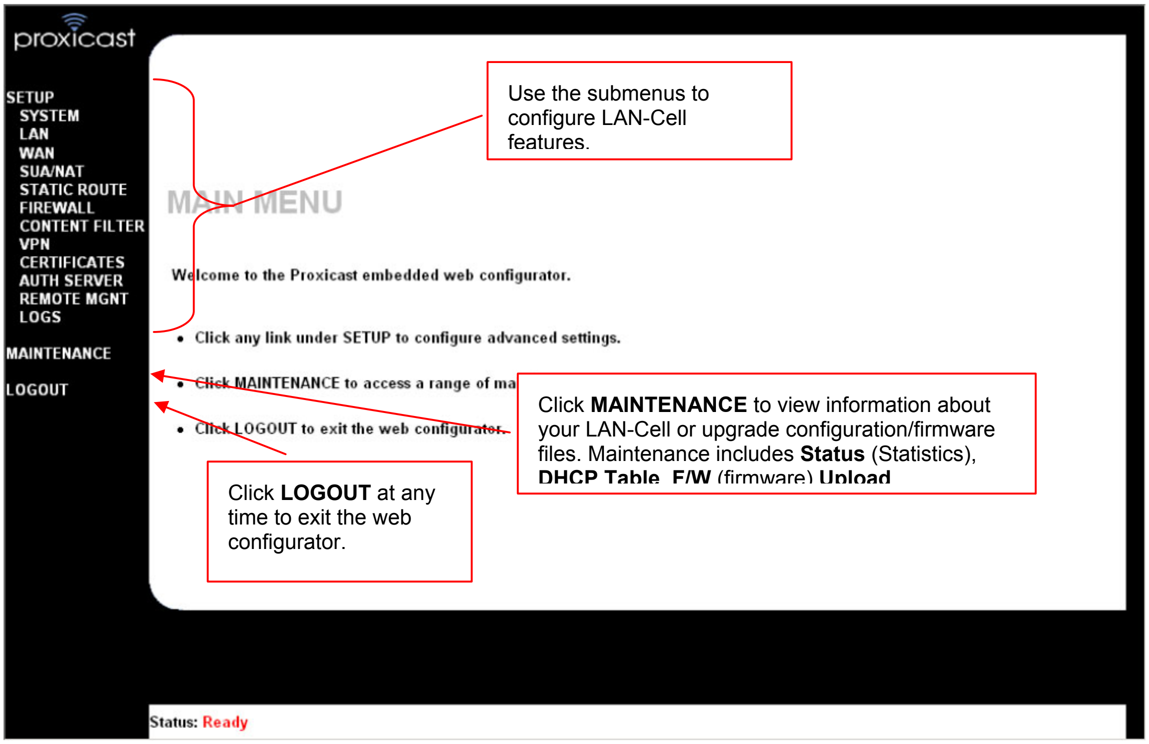



**Figure 2-1 The MAIN MENU Screen of the Web Configurator**

The following table describes the sub-menus.

**Table 2-1 Web Configurator Screens Summary**

| LINK | TAB | FUNCTION |
|---|---|---|
| SYSTEM | General | Use this screen to configure general system settings. |
| | DDNS | Use this screen to configure Dynamic Domain Name System settings. |
| | Password | Use this screen to change your password. |
| | Time Setting | Use this screen to change your LAN-Cell's time and date. |
| LAN | IP | 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. |
| WAN | Route | This screen allows you to configure route priority and traffic redirect properties. |
| | WAN ISP | Use this screen to configure Internet Service Provider parameters. |
| | WAN IP | Use this screen to configure WAN IP address settings. |
| | WAN MAC | Use this screen to configure WAN MAC address settings. |
| | Traffic Redirect | Use this screen to configure your traffic redirect properties and parameters. |
| | Cellular Modem | Use this screen to configure the cellular modem WAN connection. |
| SUA/NAT | SUA Server | Use this screen to configure servers behind the LAN-Cell. |
| | Address Mapping | Use this screen to configure network address translation mapping rules. |
| | Trigger Port | Use this screen to change your LAN-Cell's trigger port settings. |
| STATIC ROUTE | IP Static Route | Use this screen to configure IP static routes. |
| FIREWALL | Summary | This screen shows a summary of the firewall rules, and allows you to edit/add firewall rules. |
| | Attack Alert | Use this screen to configure the threshold for DoS attacks. |
| CONTENT FILTER | General | This screen allows you to enable content filtering and block certain web features. |
| | Categories | Use this screen to select which categories of web pages to filter out, as well as to register for external database content filtering and view reports. |
| | Customization | Use this screen to customize the content filter list. |
| VPN | VPN Rules | Use this screen to configure VPN connections and view the rule summary. |
| | SA Monitor | Use this screen to display and manage active VPN connections. |
| | Global Setting | Use this screen to allow NetBIOS packets through the VPN connections. |
| 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. |

**Table 2-1 Web Configurator Screens Summary**

| LINK | TAB | FUNCTION |
|---|---|---|
| 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. |
| REMOTE MGNT | WWW | Use this screen to configure through which interface(s) and from which IP address(es) users can use HTTPS (LAN-Cell Gateway only) 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. |
| | Security | Use this screen to set whether or not the LAN-Cell responds to ICMP pings and/or requests for unauthorized services. |
| 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. |
| | Reports | Use this screen to have the LAN-Cell record and display the network usage reports. |
| MAINTENANCE | Status | This screen contains administrative and system-related information. Use this screen to access statistics. |
| | DHCP Table | This screen shows current DHCP Client information of all network clients using the LAN-Cell's DHCP server. |
| | F/W Upload | Use this screen to upload firmware to your LAN-Cell |
| | Configuration | 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. |
| LOGOUT | | Click this label to exit the web configurator. |

# Part II:

## System and LAN

This part covers configuration of the system and LAN screens.

# Chapter 3
# System Screens

*This chapter provides information on the System screens.*

## 3.1 Configuring General Setup

Click **SYSTEM** to open the **General** screen.

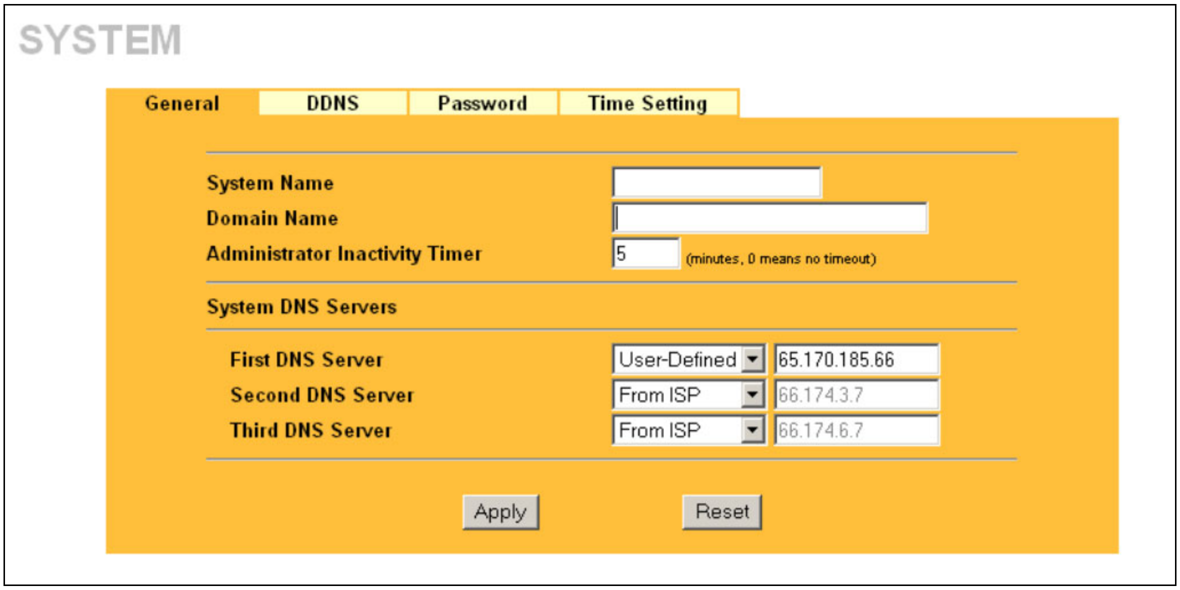



**Figure 3-1 System General Setup**

The following table describes the fields in this screen.

**Table 3-1 System General Setup**

| LABEL | DESCRIPTION |
|---|---|
| System Name | Choose a descriptive name for identification purposes. This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted. |
| Domain Name | Enter the domain name (if you know it) here. If you leave this field blank, the ISP may assign a domain name via DHCP.<br>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). |
| System DNS Servers (if applicable)<br>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 here) to resolve domain names for VPN, DDNS and the time server.<br>If you are using the Dynamic DNS feature, we recommend setting at least the first DNS Server to a known static IP address so that the dyndns.org server can be located when a new connection is established. | |

**Table 3-1 System General Setup**

| LABEL | DESCRIPTION |
|---|---|
| First DNS Server<br><br>Second DNS Server<br><br>Third DNS Server | Select **From ISP** if your ISP dynamically assigns DNS server information (and the LAN-Cell's WAN IP address). The field to the right displays the (read-only) DNS server IP address that the ISP assigns.<br>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**.<br>Select **None** if you do not want to configure DNS servers. If you do not configure a system DNS server, you must use IP addresses when configuring VPN, DDNS and the time server. |
| Apply | Click **Apply** to save your changes back to the LAN-Cell. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

# 3.2 Dynamic DNS

Dynamic DNS allows you to update your current dynamic IP address with a dynamic DNS service so that anyone can contact you (in NetMeeting, CU-SeeMe, etc.). You can also access your FTP server or Web site on computers attached to the LAN-Cell Gateway 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.

You need to register a dynamic DNS account with www.dyndns.org to obtain a username and password.

## 3.2.1 DYNDNS Wildcard

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

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

# 3.3 Configuring Dynamic DNS

To change your LAN-Cell's DDNS, click **SYSTEM**, then the **DDNS** tab. The screen appears as shown.

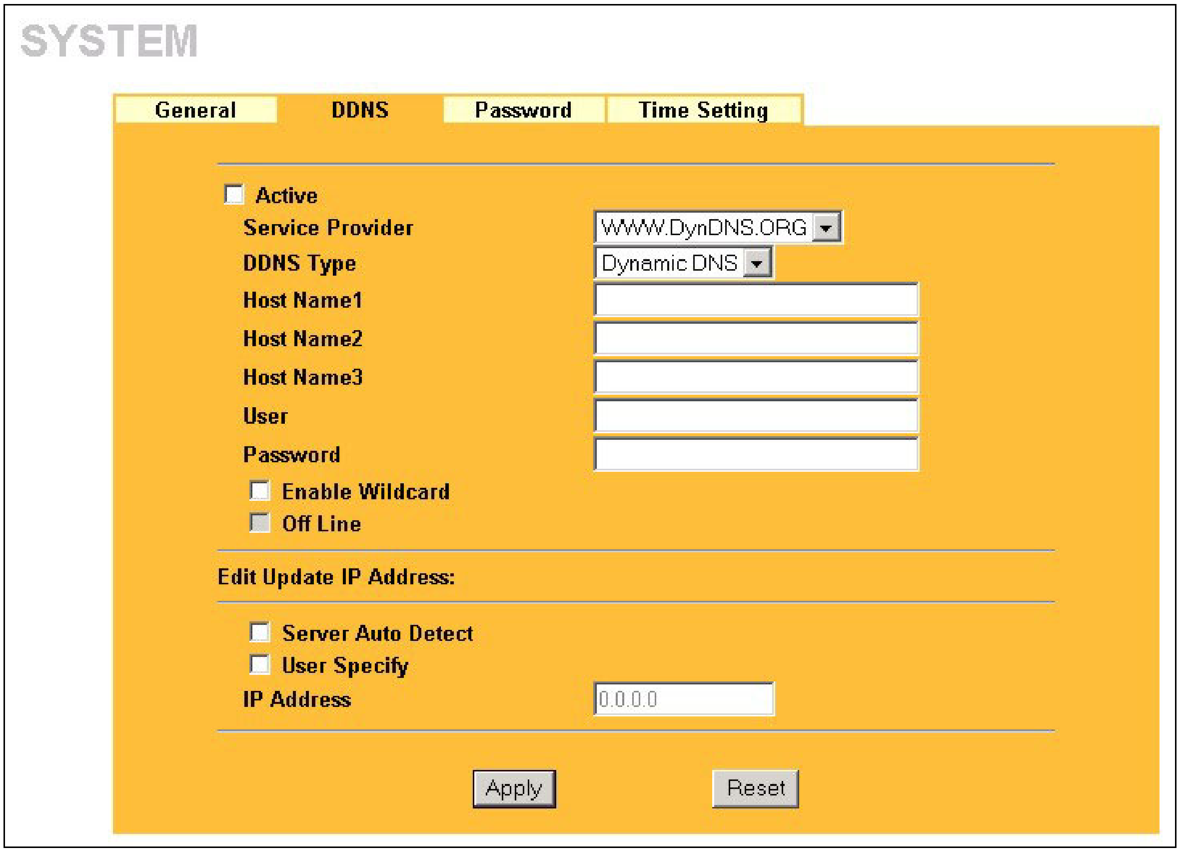



**Figure 3-2 DDNS**

The following table describes the fields in this screen.

**Table 3-2 DDNS**

| LABEL | DESCRIPTION |
|---|---|
| Active | Select this check box to use dynamic DNS. |
| Service Provider | Select the name of your Dynamic DNS service provider. |
| DDNS Type | Select the type of service that you are registered for from your Dynamic DNS service provider. |
| Host Names 1~3 | Enter the host names in the three fields provided. You can specify up to two host names in each field separated by a comma (","). |
| User | Enter your user name. |
| Password | Enter the password assigned to you. |
| Enable Wildcard | Select the check box to enable DYNDNS Wildcard. |
| Off Line | This option is available when **CustomDNS** is selected in the **DDNS Type field**. Check with your Dynamic DNS service provider to have traffic redirected to a URL (that you can specify) while you are off line. |
| Server Auto Detect | Select this option to update the IP address of the host name(s) automatically by the DDNS server. It is recommended that you select this option. |
| User Specify | Select this option to update the IP address of the host name(s) to the IP address specified below. Use this option if you have a static IP address. |
| IP Addr | Enter the IP address if you select the **User Specify** option. |
| Apply | Click **Apply** to save your changes back to the LAN-Cell. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 3.4 Configuring Password

To change your LAN-Cell's password (recommended), click **SYSTEM**, then the **Password** tab. The screen appears as shown. This screen allows you to change the LAN-Cell's password.

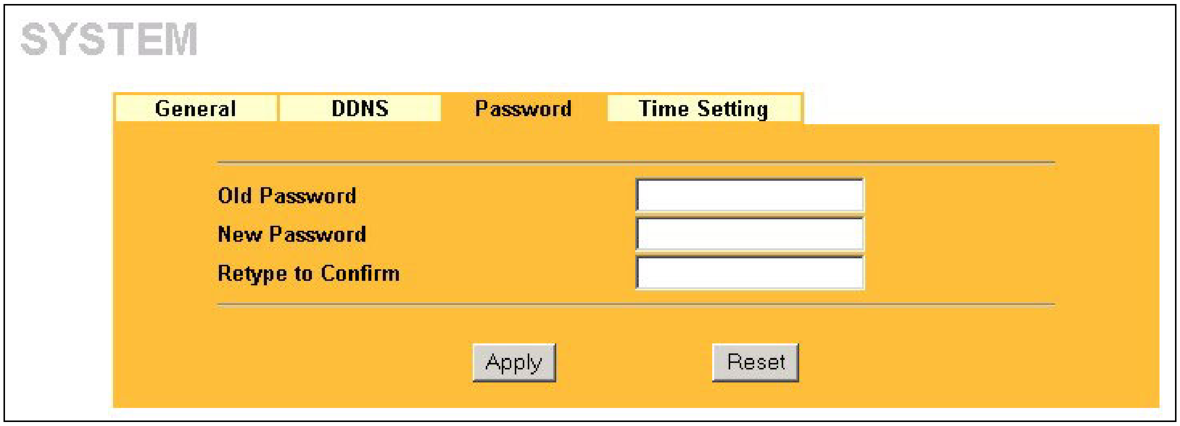



**Figure 3-3 Password**

The following table describes the fields in this screen.

**Table 3-3 Password**

| LABEL | DESCRIPTION |
|---|---|
| Old Password | Type the default password or the existing password you use to access the system in this field. |
| New Password | Type the new password in this field. |
| Retype to Confirm | Type the new password again in this field. |
| Apply | Click **Apply** to save your changes back to the LAN-Cell. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 3.5 Pre-defined NTP Time Servers List

The LAN-Cell uses the following pre-defined list of NTP time servers if you do not specify a time server or it cannot synchronize with the time server you specified.

**The LAN-Cell can use this pre-defined list of time servers regardless of the** Time Protocol **you select.**

When the LAN-Cell uses the pre-defined list of NTP time servers, it randomly selects one server and tries to synchronize with 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 servers have been tried.

**Table 3-4 Default Time Servers**

| |
|---|
| ntp1.cs.wisc.edu |
| ntp1.gbg.netnod.se |
| ntp2.cs.wisc.edu |
| tock.usno.navy.mil |
| ntp3.cs.wisc.edu |
| ntp.cs.strath.ac.uk |
| ntp1.sp.se |
| time1.stupi.se |
| tick.stdtime.gov.tw |

**Table 3-4 Default Time Servers**

| |
|---|
| tock.stdtime.gov.tw |
| time.stdtime.gov.tw |

## 3.6 Configuring Time Setting

To change your LAN-Cell's time and date, click **SYSTEM**, then the **Time Setting** tab. The screen appears as shown. Use this screen to configure the LAN-Cell's time based on your local time zone.

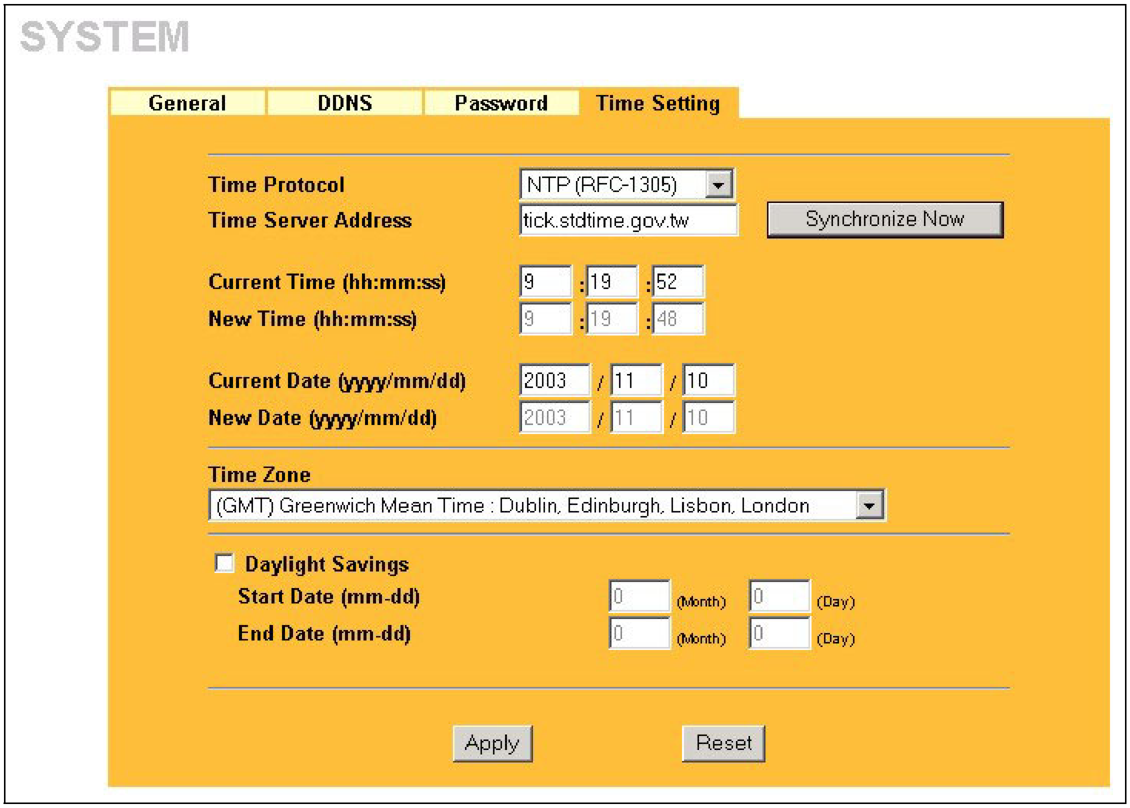



**Figure 3-4 Time Setting**

The following table describes the fields in this screen.

**Table 3-5 Time Setting**

| LABEL | DESCRIPTION |
|---|---|
| Time Protocol | Select the time service protocol that your time server sends when you turn on the LAN-Cell. 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.<br>The main differences between them are the format.<br>**Daytime (RFC-867)** format is day/month/year/time zone of the server.<br>**Time (RFC-868)** format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0.<br>The default, **NTP (RFC-1305),** is similar to Time (RFC-868).<br>Select **None** to enter the time and date manually. |
| Time Server Address | Enter the address of your time server. Check with your ISP/network administrator if you are unsure of this information (the default is tick.stdtime.gov.tw). |
| Synchronize Now | Click this button to get the time and date from the time server you specified above. |
| Current Time | This field displays the time of your LAN-Cell.<br>Each time you reload this page, the LAN-Cell synchronizes the time with the time server. |

**Table 3-5 Time Setting**

| LABEL | DESCRIPTION |
|---|---|
| New Time | This field displays the last updated time from the time server.<br>When you select **None** in the **Time Protocol** field, enter the new time in this field and then click **Apply**. |
| Current Date | This field displays the date of your LAN-Cell.<br>Each time you reload this page, the LAN-Cell synchronizes the time with the time server. |
| New Date | This field displays the last updated date from the time server.<br>When you select **None** in the **Time Protocol** field, enter the new date in this field and then click **Apply**. |
| Time Zone | Choose the time setting of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT). |
| Daylight Savings | Select this option if you use daylight savings time. Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening. |
| Start Date | Enter the month and day that your daylight-savings time starts on if you selected **Daylight Savings**. |
| End Date | Enter the month and day that your daylight-savings time ends on if you selected **Daylight Savings**. |
| Apply | Click **Apply** to save your changes back to the LAN-Cell. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

# Chapter 4
# LAN Screens

*This chapter describes how to configure LAN settings.*

## 4.1 LAN Overview

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

## 4.2 DHCP Setup

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

### 4.2.1 IP Pool Setup

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

## 4.3 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. Let's say you select 192.168.1 as the network number; which 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.

## 4.4 DNS Server Address Assignment

Use DNS (Domain Name System) to map 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 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, enter them in the DNS Server fields in DHCP Setup.
2. If the ISP did not give you DNS server information, leave the DNS Server fields in DHCP Setup set to 0.0.0.0 for the ISP to dynamically assign the DNS server IP addresses.

## 4.5 LAN TCP/IP

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

### 4.5.1 Factory LAN Defaults

The LAN parameters of the LAN-Cell are preset in the factory with the following values:

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

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

### 4.5.2 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**.

### 4.5.3 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.

## 4.6 Configuring IP

Click **LAN** to open the **IP** screen.

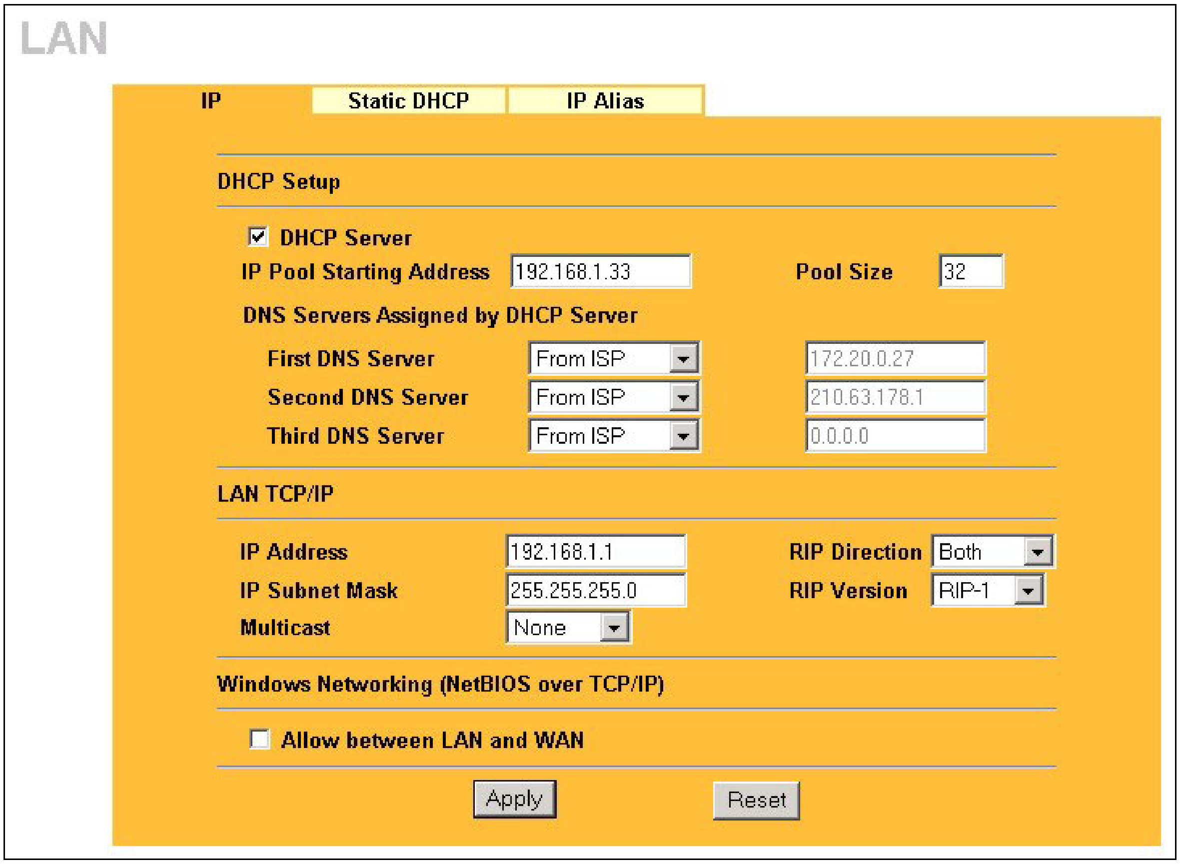



**Figure 4-1 IP**

The following table describes the fields in this screen.

**Table 4-1 IP**

| LABEL | DESCRIPTION |
|---|---|
| DHCP Setup | |
| DHCP Server | 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 the **DHCP Server** check box selected. Clear it to disable the LAN-Cell acting as a DHCP server. When configured as a server, the LAN-Cell provides TCP/IP configuration for the clients. If not, DHCP service is disabled and you must have another DHCP server on your LAN, or else the workstation must be manually configured. When set as a server, fill in the following four fields. |
| IP Pool Starting Address | This field specifies the first of the contiguous addresses in the IP address pool. The default is 192.168.1.33. |
| Pool Size | This field specifies the size, or count, of the IP address pool. The default is 32. |
| Primary/Secondary DNS Servers | Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the subnet mask. Leave these entries at 0.0.0.0 if they are provided by a WAN DHCP server. |
| 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. |
| IP Subnet Mask | The subnet mask specifies the network number portion of an IP address. Your LAN-Cell 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 4-1 IP**

| 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. **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*. |
| Windows Networking (NetBIOS over TCP/IP) | |
| Allow between LAN and WAN | Select this check box to forward NetBIOS packets from the LAN to the WAN and from the 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.<br>Clear this check box to block all NetBIOS packets going from the LAN to the WAN and from the WAN to the LAN. |
| Apply | Click **Apply** to save your changes back to the LAN-Cell. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 4.7 Configuring Static DHCP

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

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

To change your LAN-Cell's Static DHCP settings, click **LAN**, then the **Static DHCP** tab. The screen appears as shown.

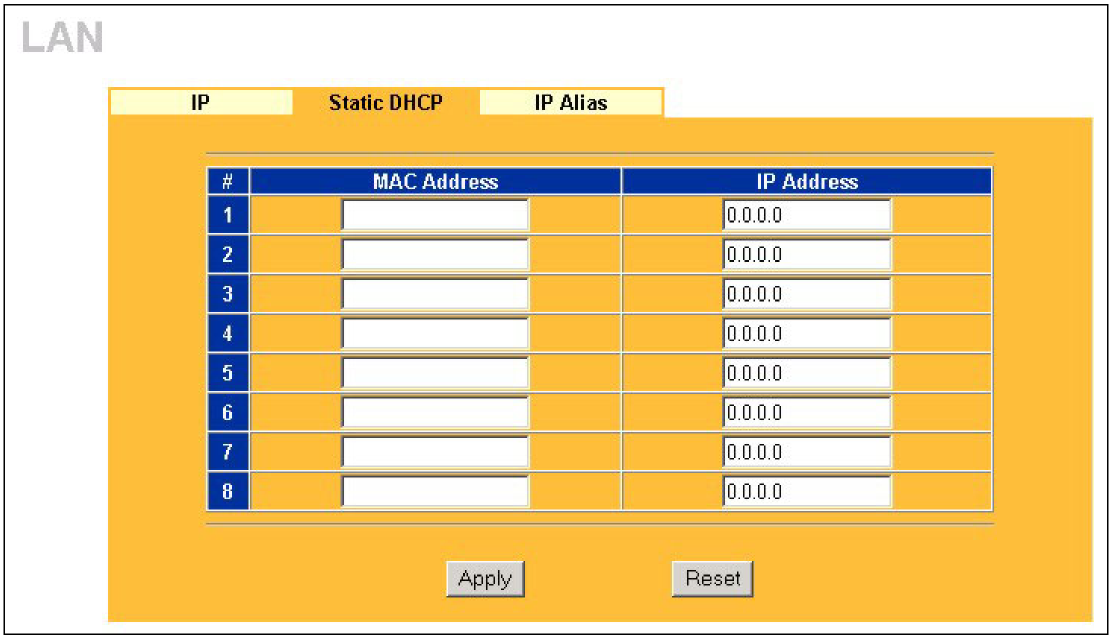



**Figure 4-2 Static DHCP**

The following table describes the fields in this screen.

**Table 4-2 Static DHCP**

| LABEL | DESCRIPTION |
|---|---|
| **#** | This is the index number of the Static IP table entry (row). |
| MAC Address | Type the MAC address (with colons) of a computer on your LAN. |
| IP Address | Type the IP address to be assigned to the device with the MAC address entered above. |
| Apply | Click **Apply** to save your changes back to the LAN-Cell. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 4.8 Configuring IP Alias

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

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

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

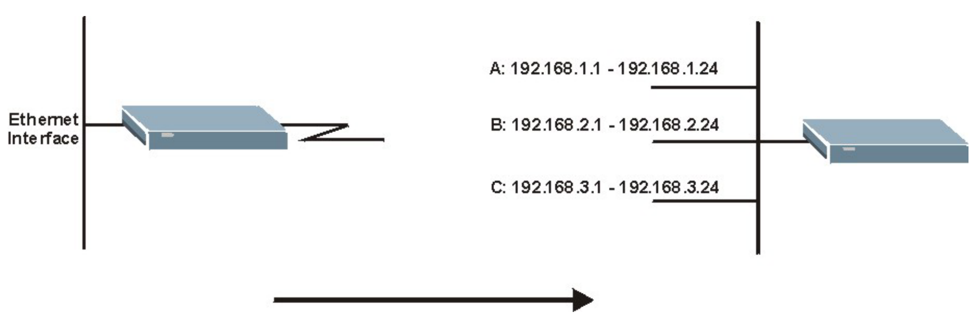



**Figure 4-3 Partitioned Logical Networks**

To change your LAN-Cell's IP alias settings, click **LAN**, then the **IP Alias** tab. The screen appears as shown.

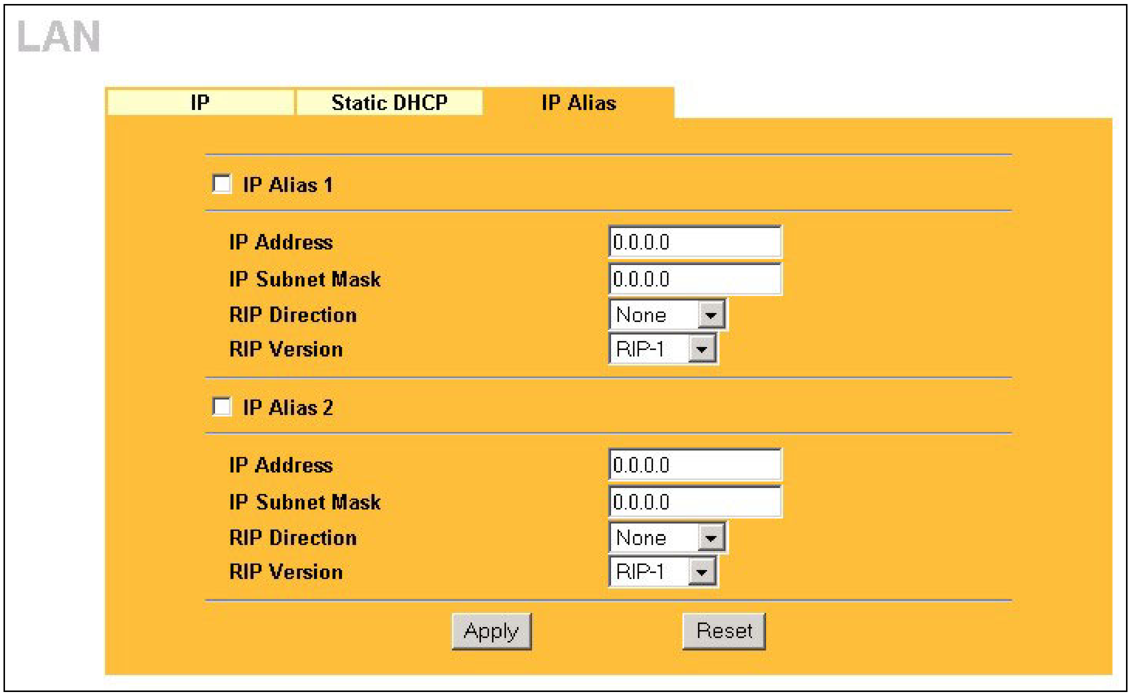



**Figure 4-4 IP Alias**

The following table describes the fields in this screen.

**Table 4-3 IP Alias**

| LABEL | DESCRIPTION |
|---|---|
| IP Alias 1,2 | Select the check box to configure another LAN 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 | 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. |

# Part III:

## WAN & Cellular Modem

This part covers configuration of the WAN & Cellular Modem screens.

# Chapter 5
# WAN Screens

*This chapter describes how to configure WAN settings.*

## 5.1 TCP/IP Priority (Metric)

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

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

1. **WAN**: designated by the ISP (see *section 5.4*) or a static route (see the IP Static Route Setup chapter)
2. **Traffic Redirect** (see *section 5.7*)
3. **Cellular Modem** (see *section 5.8*)

For example, if **WAN** has a metric of "1" and **Traffic Redirect** has a metric of "2" and **Cellular Modem** has a metric of "3", the **WAN** connection acts as the primary default route. If the **WAN** route fails to connect to the Internet, the LAN-Cell tries **Traffic Redirect** next. In the same manner, the LAN-Cell uses **Cellular Modem** if **Traffic Redirect** also fails.

If you want **Cellular Modem** to take first priority over **Traffic Redirect** or even **WAN**, all you need to do is set **Cellular Modem**'s metric to "1" and the others to "2" (or greater).

Click **WAN** to open the **Route** screen.

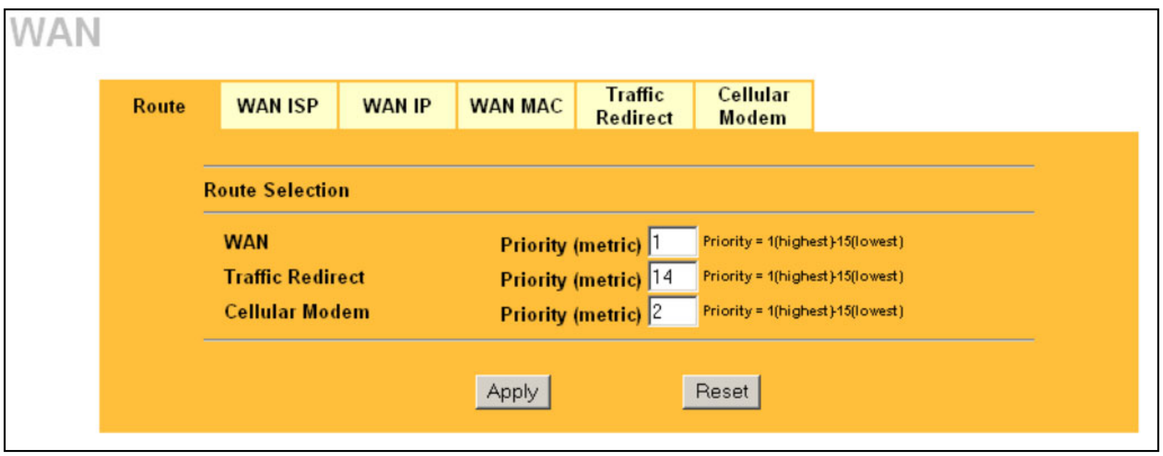



**Figure 5-1 WAN Setup: Route**

**Table 5-1 WAN Setup: Route**

| LABEL | DESCRIPTION |
|---|---|
| WAN | The default WAN connection is "1" as your broadband connection via the WAN port should always be your preferred method of accessing the WAN. The default priority of the routes is **WAN**, **Traffic Redirect** and then **Cellular Modem**: |
| Traffic Redirect | You have two choices for an auxiliary connection (**Traffic Redirect** and **Cellular Modem**) in the event that your regular WAN connection goes down. If **Cellular Modem** is preferred to **Traffic Redirect**, then type "14" in the **Cellular Modem Priority (metric)** field (and leave the **Traffic Redirect Priority (metric)** at the default of "15"). |
| Cellular Modem | If you want the Cellular modem connection to be the primary means for WAN communications, then set the Priority of **Cellular Modem** to "1" and set **WAN** & **Traffic Redirect** to numbers between "2" and "14". |
| Apply | Click **Apply** to save your changes back to the LAN-Cell. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 5.2 WAN IP Address 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 5-2 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.**

### 5.2.1 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:A0:C5:00:00:02.

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 (configuration file). It will not change unless you change the setting or upload a different "rom" file.

Your LAN-Cell's WAN Port is set at half-duplex mode as most cable/DSL modems only support half-duplex mode. Make sure your modem is in half-duplex mode. Your LAN-Cell supports full duplex mode on the LAN side.

**Table 5-3 Example of Network Properties for LAN Servers with Fixed IP Addresses**

| | |
|---|---|
| Choose an IP address | 192.168.1.2-192.168.132; 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 Configuring WAN ISP

To change your LAN-Cell's WAN ISP settings, click **WAN**, then the **WAN ISP** tab. The screen differs by the encapsulation.

### 5.3.1 Ethernet Encapsulation

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

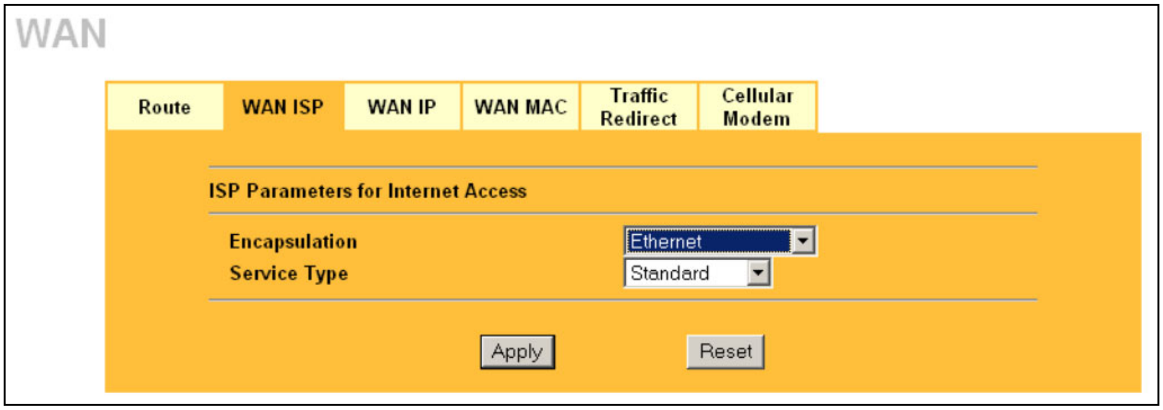



**Figure 5-2 Ethernet Encapsulation**

The following table describes the fields in this screen.

**Table 5-4 Ethernet Encapsulation**

| LABEL | DESCRIPTION |
|---|---|
| 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**.<br>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. |
| Login Server (Telia Login only) | Type the domain name of the Telia login server, for example "login1.telia.com". |
| 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. |
| 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 Draft standard (RFC 2516) specifying how a personal computer (PC) interacts with a broadband modem (DSL, cable, wireless, etc.) connection. The **PPPoE** option is for a dial-up connection using PPPoE.

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

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

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

By implementing PPPoE directly on the 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.

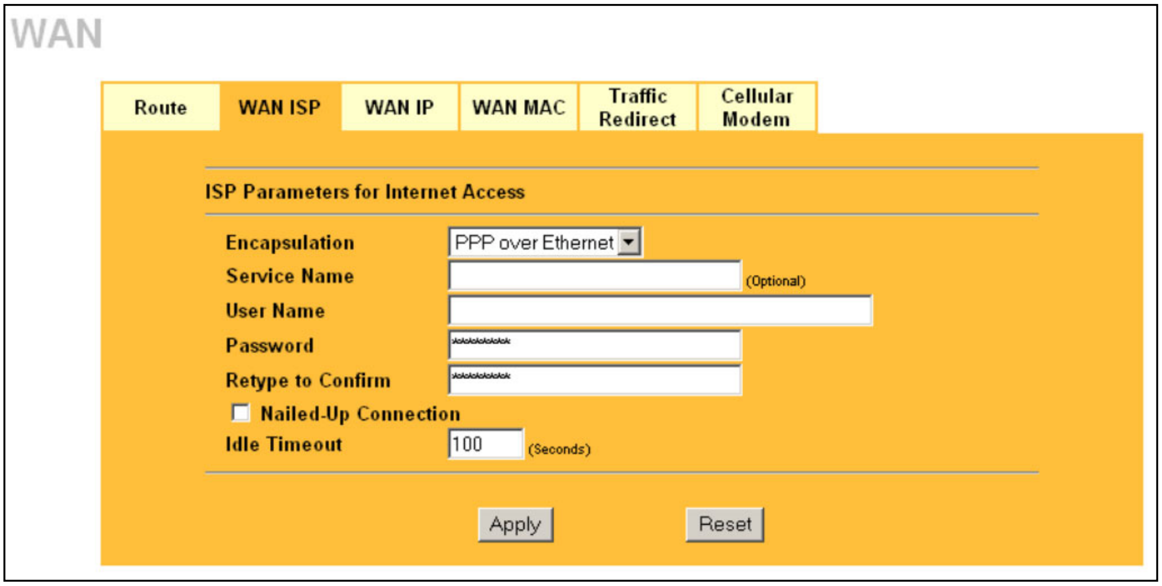



**Figure 5-3 PPPoE Encapsulation**

The following table describes the fields in this screen.

**Table 5-5 PPPoE Encapsulation**

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

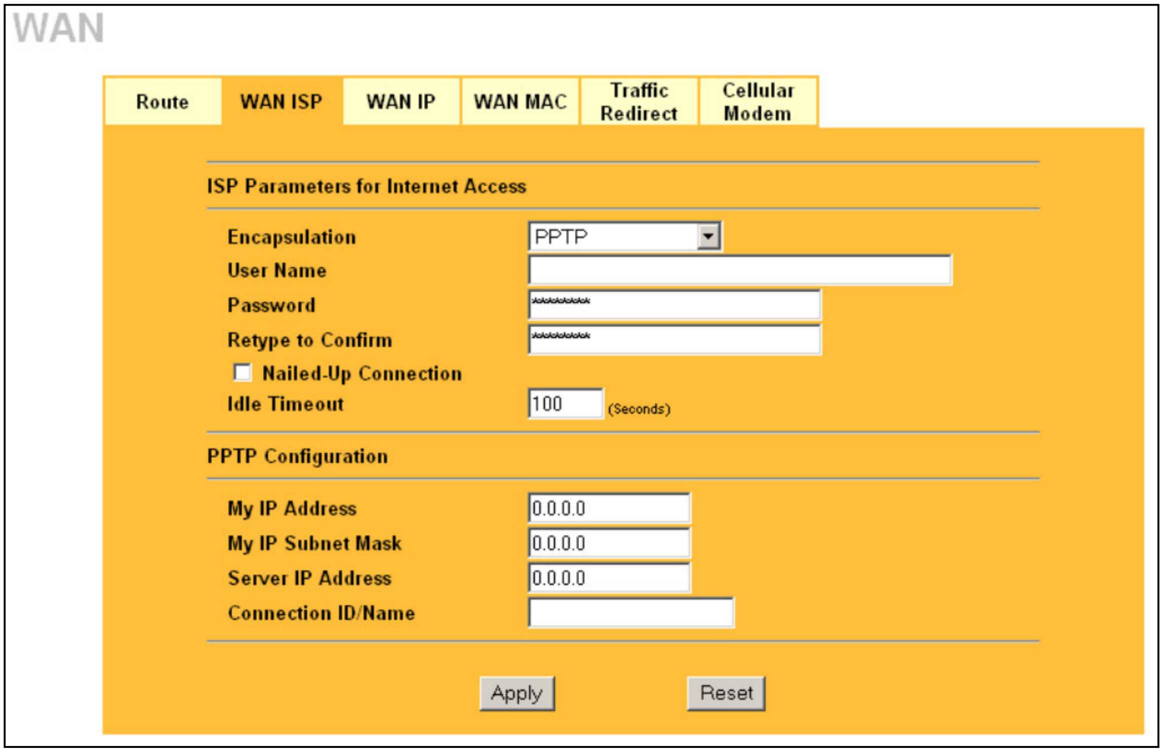



**Figure 5-4 PPTP Encapsulation**

The following table describes the fields in this screen.

**Table 5-6 PPTP Encapsulation**

| LABEL | DESCRIPTION |
|---|---|
| ISP Parameters for Internet Access | |
| 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 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 is correctly. |
| Nailed-up Connection | Select **Nailed-Up Connection** if you do not want the connection to time out. |
| Idle Timeout | This value specifies the time in seconds that elapses before the 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. |
| Apply | Click **Apply** to save your changes back to the LAN-Cell. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 5.4 Configuring WAN IP

To change your LAN-Cell's WAN IP settings, click **WAN**, then the **WAN IP** tab. This screen varies according to the type of encapsulation you select.

If your ISP did *not* assign you a fixed IP address, click **Get automatically from ISP (Default)**;otherwise click **Use fixed IP Address** and enter the IP address in the following field.

**When** Network Address Translation **is set to** Full Feature**, but there is no NAT rule configured, the warning message** "Warning! No NAT rule configured in system" **appears in the status bar.**

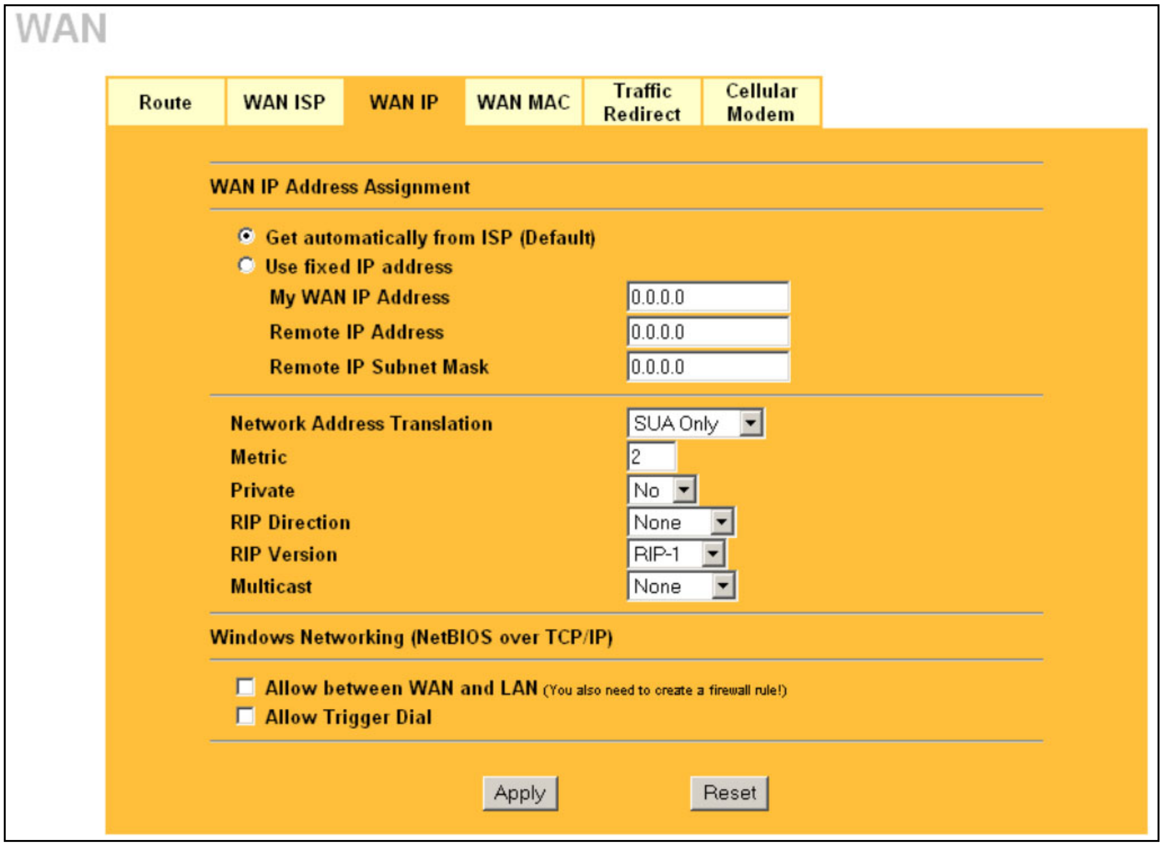



**Figure 5-5 IP Setup**

The following table describes the fields in this screen.

**Table 5-7 IP Setup**

| LABEL | DESCRIPTION |
|---|---|
| WAN IP Address Assignment | |
| Get automatically from ISP | Select this option If your ISP did not assign you a fixed IP address. This is the default selection. |
| Use fixed IP address | Select this option If the ISP assigned a fixed IP address. |
| My WAN IP Address (or IP Address) | Enter your WAN IP address in this field if you selected **Use Fixed IP Address.** |
| My WAN IP Subnet Mask (Ethernet encapsulation only) | Type your network's IP subnet mask. |
| Remote IP Address (or Gateway IP Address) | Type the IP address of the remote network or 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. |

**Table 5-7 IP Setup**

| LABEL | DESCRIPTION |
|---|---|
| Remote IP Subnet Mask (PPPoE and PPTP encapsulation) | When using a LAN to LAN application, type the IP subnet mask of the destination network. 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. |
| 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).<br>Choose **None** to disable NAT**.**<br>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**.<br>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!<br>For more information about NAT refer to the *NAT* chapter in this *User's Guide*. |
| Metric (PPPoE and PPTP only) | This field sets this route's priority among the routes the LAN-Cell uses.<br>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". |
| Private (PPPoE and PPTP only) | 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 | 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.<br>Choose **Both**, **None**, **In Only** or **Out Only**.<br>When set to **Both** or **Out Only**, the LAN-Cell will broadcast its routing table periodically.<br>When set to **Both** or **In Only**, the LAN-Cell will incorporate RIP information that it receives.<br>When set to **None**, the LAN-Cell will not send any RIP packets and will ignore any RIP packets received.<br>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).<br>Choose **RIP-1**, **RIP-2B** or **RIP-2M**.<br>**RIP-1** is universally supported; but **RIP-2** carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology. Both **RIP-2B** and **RIP-2M** sends the routing data in RIP-2 format; the difference being that RIP-2B uses subnet broadcasting while RIP-2M uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also. By default, the **RIP Version** field is set to **RIP-1**. |
| Multicast | Choose **None** (default), **IGMP-V1** or **IGMP-V2**. IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see sections 4 and 5 of RFC 2236. |
| Windows Networking (NetBIOS over TCP/IP): Windows Networking (NetBIOS over TCP/IP): NetBIOS (Network Basic Input/Output System) are TCP or UDP broadcast packets that enable a computer to connect to and communicate with a LAN. For some dial-up services such as PPPoE or PPTP, NetBIOS packets cause unwanted calls. | |

**Table 5-7 IP Setup**

| LABEL | DESCRIPTION |
|---|---|
| Allow between WAN and LAN | Select this check box to forward NetBIOS packets from the LAN to the WAN and from the 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.<br>Clear this check box to block all NetBIOS packets going from the LAN to the WAN and from the WAN to the LAN. |
| 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. |

## 5.5 Configuring WAN MAC

To change your LAN-Cell's WAN MAC settings, click **WAN**, then the **WAN MAC** tab. The screen appears as shown.

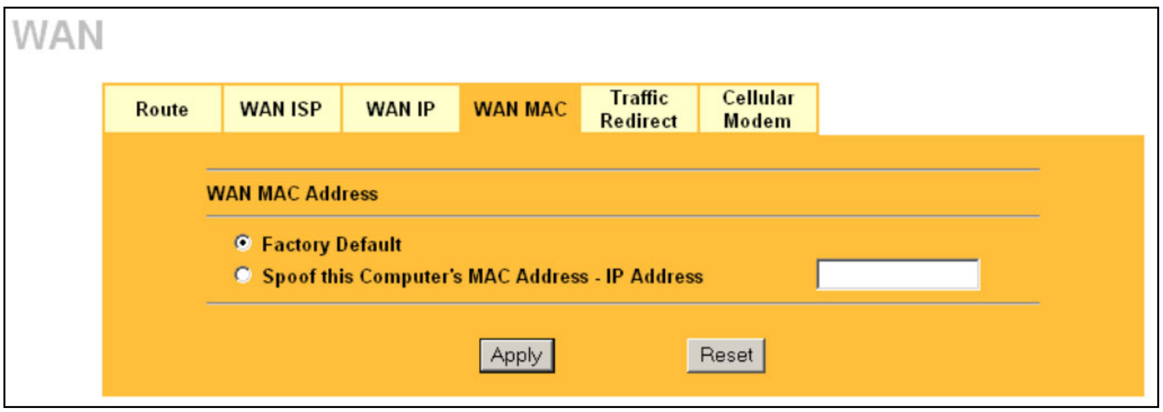



**Figure 5-6 MAC Setup**

The MAC address screen allows users to configure the WAN port's MAC Address by either using the factory default or cloning the MAC address from a computer on your LAN. Choose **Factory Default** to select the factory assigned default MAC Address.

Otherwise, click **Spoof this computer's MAC address - IP Address** 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 (configuration file). It will not change unless you change the setting or upload a different ROM file.

## 5.6 Traffic Redirect

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

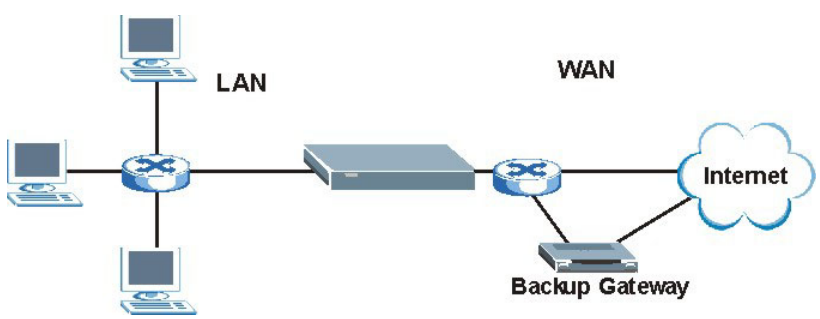



**Figure 5-7 Traffic Redirect Setup Example**

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

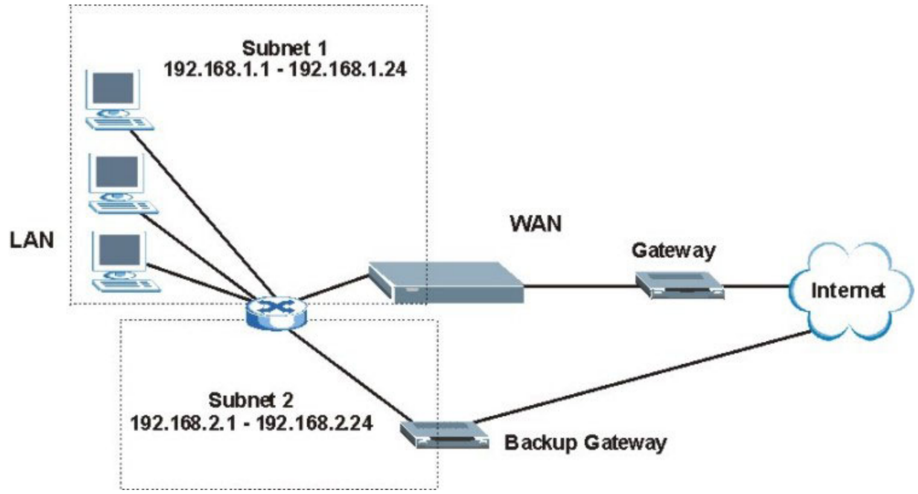



**Figure 5-8 Traffic Redirect LAN Setup**

## 5.7 Configuring Traffic Redirect

To change your LAN-Cell's Traffic Redirect settings, click **WAN**, then the **Traffic Redirect** tab. The screen appears as shown.

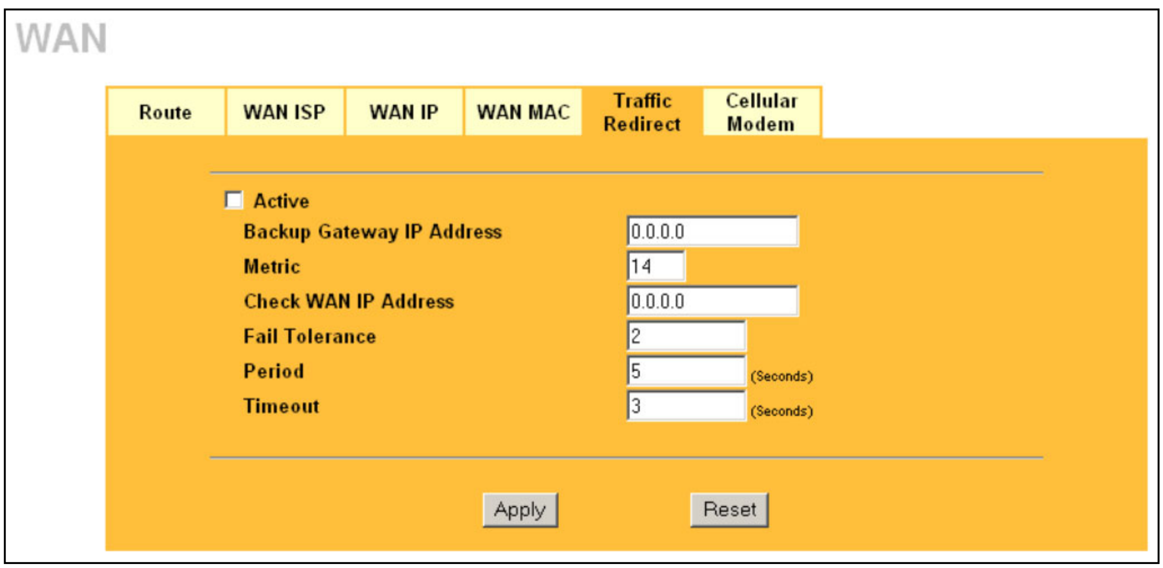



**Figure 5-9 Traffic Redirect**

The following table describes the fields in this screen.

**Table 5-8 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. |
| Metric | This field sets this route's priority among the routes the LAN-Cell uses.<br>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". |

**Table 5-8 Traffic Redirect**

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

## 5.8 Configuring Cellular Modem

To change your LAN-Cell's Cellular Modem settings, click **WAN**, then the **Cellular Modem** tab. The screen appears as shown.

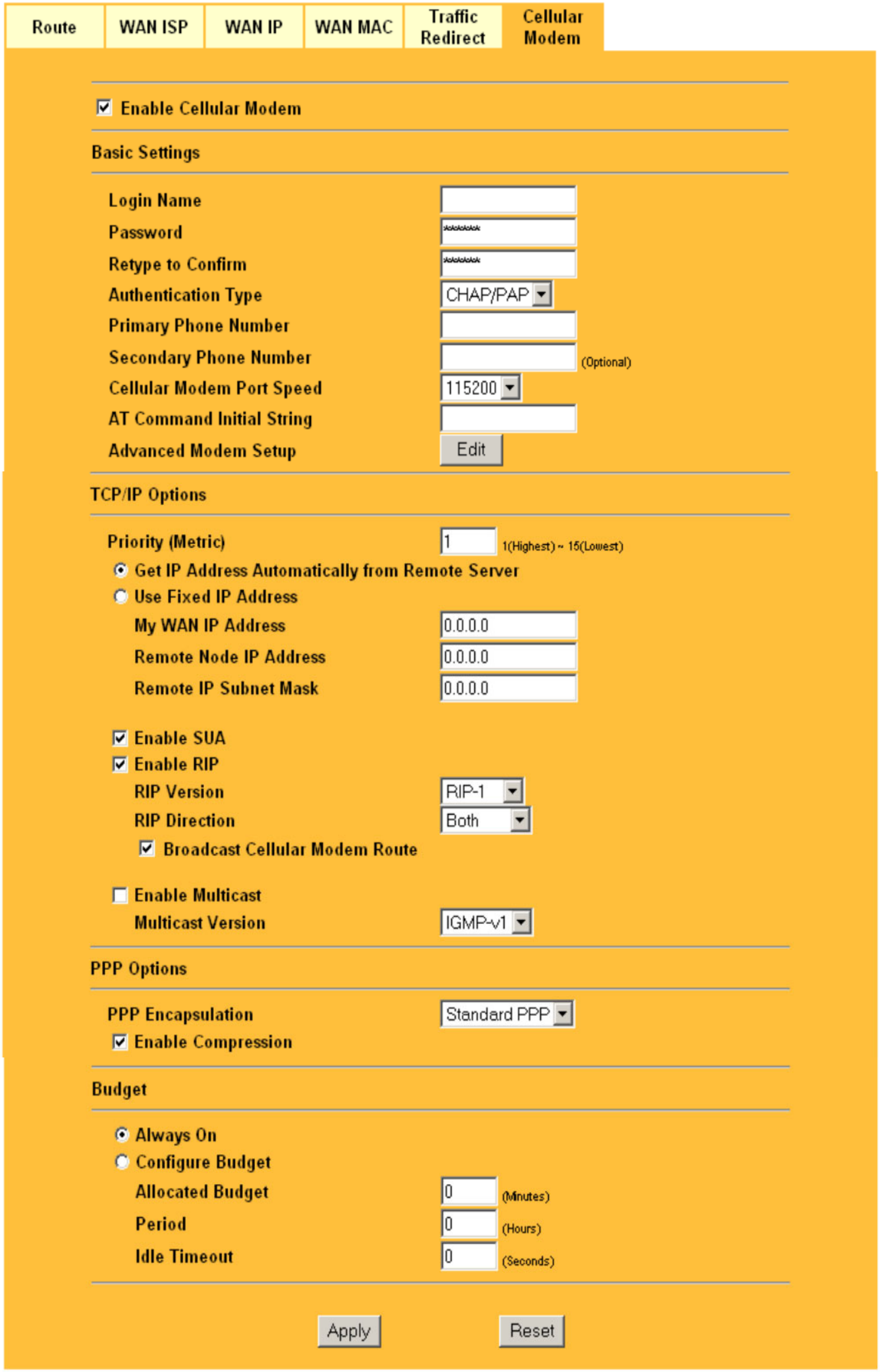



**Figure 5-10 Cellular Modem Setup**

The following table describes the labels in this screen.

**Table 5-9 Cellular Modem Setup**

| LABEL | DESCRIPTION |
|---|---|
| Enable Cellular Modem | Select this check box to turn on Cellular Modem. |
| Basic Settings | |
| 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:<br>**CHAP/PAP** - Your LAN-Cell accepts either CHAP or PAP when requested by this remote node.<br>**CHAP** - Your LAN-Cell accepts CHAP only.<br>**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 networks require dialing the pound sign # before the phone number for cellular calls. Include a # symbol at the beginning of the phone numbers as required. |
| Cellular Modem Port Speed | The LAN-Cell's connection to its internal cellular modem is fixed at **115200** bps. Do not alter this setting or the LAN-Cell will not function properly. |
| AT Command Initial String | Depending upon your application requirements, additional commands may be required during cellular modem initialization. Please refer to the appropriate *Application Note* for examples of typical cellular modem initialization strings. |
| Advanced Modem Setup | Click **Edit** to display the **Advanced Setup** screen and edit the details of your Cellular Modem setup. |
| TCP/IP Options | |
| Priority (Metric) | This field sets this route's priority among the three routes the LAN-Cell uses (normal, traffic redirect and Cellular Modem). Type a number (1 to 15) to set the priority of the Cellular Modem route for data transmission. The smaller the number, the higher the priority.<br>If the three routes have the same metrics, the priority of the routes is as follows: **WAN**, **Traffic Redirect**, **Cellular Modem**. |
| 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. |
| Remote Node IP Address | Leave this field set to 0.0.0.0 (default) to have the ISP or other remote router dynamically (automatically) send its IP address if you do not know it. Type the remote gateway's IP address here if you know it (static). |
| Remote IP Subnet Mask | Leave this field set to 0.0.0.0 (default) to have the ISP or other remote router dynamically send its subnet mask if you do not know it. Type the remote gateway's subnet mask here if you know it (static). |

**Table 5-9 Cellular Modem Setup**

| LABEL | DESCRIPTION |
|---|---|
| Enable SUA | Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network to a different IP address known within another network.<br>**SUA** (Single User Account) is a subset of NAT that supports two types of mapping: Many-to-One and Server. When you select this option the LAN-Cell will use Address Mapping Set 255 in the SMT (see the section on menu 15.1 for more information).<br>Select the check box to enable SUA. Clear the check box to disable SUA so the LAN-Cell does not perform any NAT mapping for the Cellular Modem 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).<br>Choose **RIP-1**, **RIP-2B** or **RIP-2M**.<br>**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. |
| 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.<br>Choose **Both**, **In Only** or **Out Only**.<br>When set to **Both** or **Out Only**, the LAN-Cell will broadcast its routing table periodically.<br>When set to **Both** or **In Only**, the LAN-Cell will incorporate RIP information that it receives. |
| Broadcast Cellular Modem 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*. |
| PPP Options | |
| PPP Encapsulation | The LAN-Cell's internal modem supports only **Standard PPP**. Do not alter this setting. |
| Enable Compression | Select this check box to turn on stac compression. |
| Budget | |
| Always On | Select this check box to have the Cellular Modem connection on all of the time. |
| Configure Budget | Select this check box to have the Cellular Modem connection on during the time that you select. |
| Allocated Budget | Type the amount of time (in minutes) that the Cellular Modem 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 Cellular Modem connection. This option applies only when the LAN-Cell initiates the call. The Cellular Modem 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. |

## 5.9 Advanced Modem Setup

The LAN-Cell's internal modem is factory configured to work with the default Advanced Modem Setup values. We recommend that you do not change these values unless instructed to do so by an *Application Note*, or Technical Support.

## 5.10 Configuring Advanced Modem Setup

Click the **Edit** button in the **Cellular Modem** screen to display the **Advanced Setup** screen shown next.

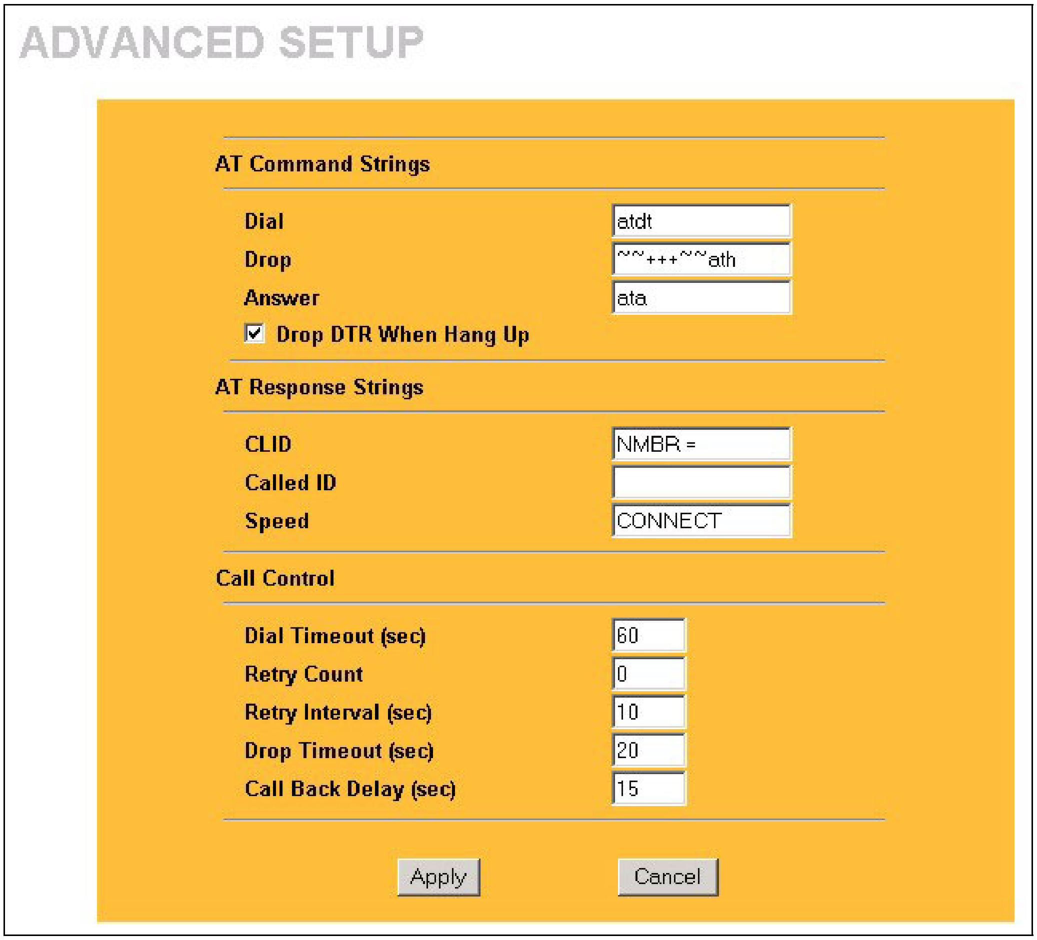



**Figure 5-11 Advanced Setup**

The following table describes the labels in this screen.

**Table 5-10 Advanced Setup**

| LABEL | DESCRIPTION | EXAMPLE |
|---|---|---|
| AT Command Strings | | |
| Dial | The AT Command string to make a call. | atdt |
| Drop | The AT Command string to drop a call. "~" represents a one second wait. | ~~+++~~ath |
| Answer | The AT Command string to answer a call. | ata |
| Drop DTR When Hang Up | Should always be enabled. | |
| AT Response Strings | | |

**Table 5-10 Advanced Setup**

| LABEL | DESCRIPTION | EXAMPLE |
|---|---|---|
| CLID | 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 cellular modem. CLID is required for CLID authentication. | NMBR |
| Called ID | The keyword preceding the dialed number. | |
| Speed | The keyword preceding the connection speed. | CONNECT |
| Call Control | | |
| Dial Timeout (sec) | Number of seconds for the LAN-Cell to try to set up an outgoing call before timing out (stopping). | 60 |
| Retry Count | Number of times for the LAN-Cell to retry a busy or no-answer phone number before blacklisting the number. | 0 |
| Retry Interval (sec) | 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. | 10 |
| Drop Timeout (sec) | Number of seconds for the LAN-Cell to wait before dropping the DTR signal if it does not receive a positive disconnect confirmation. | 20 |
| Call Back Delay (sec) | Number of seconds for the LAN-Cell to wait between dropping a callback request call and dialing the corresponding callback call. | 15 |
| Apply | Click **Apply** to save your changes back to the LAN-Cell. | |
| Cancel | Click **Cancel** to exit this screen without saving. | |

# Part IV:

## NAT and Static Route

This part covers Network Address Translation and setting up static routes.

# Chapter 6
# Network Address Translation (NAT)

*This chapter discusses how to configure NAT on the LAN-Cell.*

## 6.1 NAT Overview

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

### 6.1.1 NAT Definitions

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 6-1 NAT Definitions**

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

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

### 6.1.2 What NAT Does

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

The global IP addresses for the inside hosts can be either static or dynamically assigned by the ISP. In addition, you can designate servers (for example a web server and a telnet server) on your local network and make them accessible to the outside world. You can make designated servers on the LAN accessible to the outside world. 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)*.

### 6.1.3 How NAT Works

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

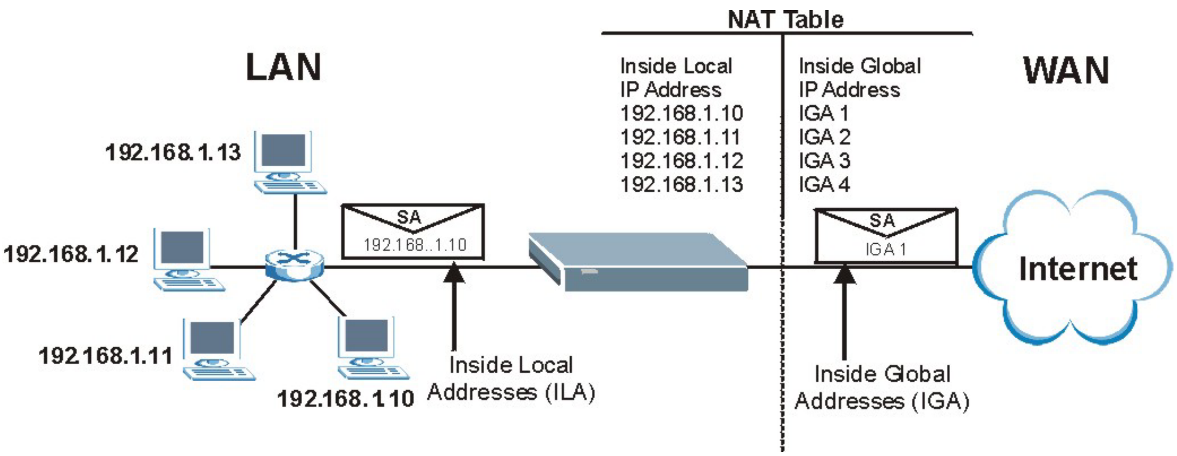



**Figure 6-1 How NAT Works**

### 6.1.4 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.

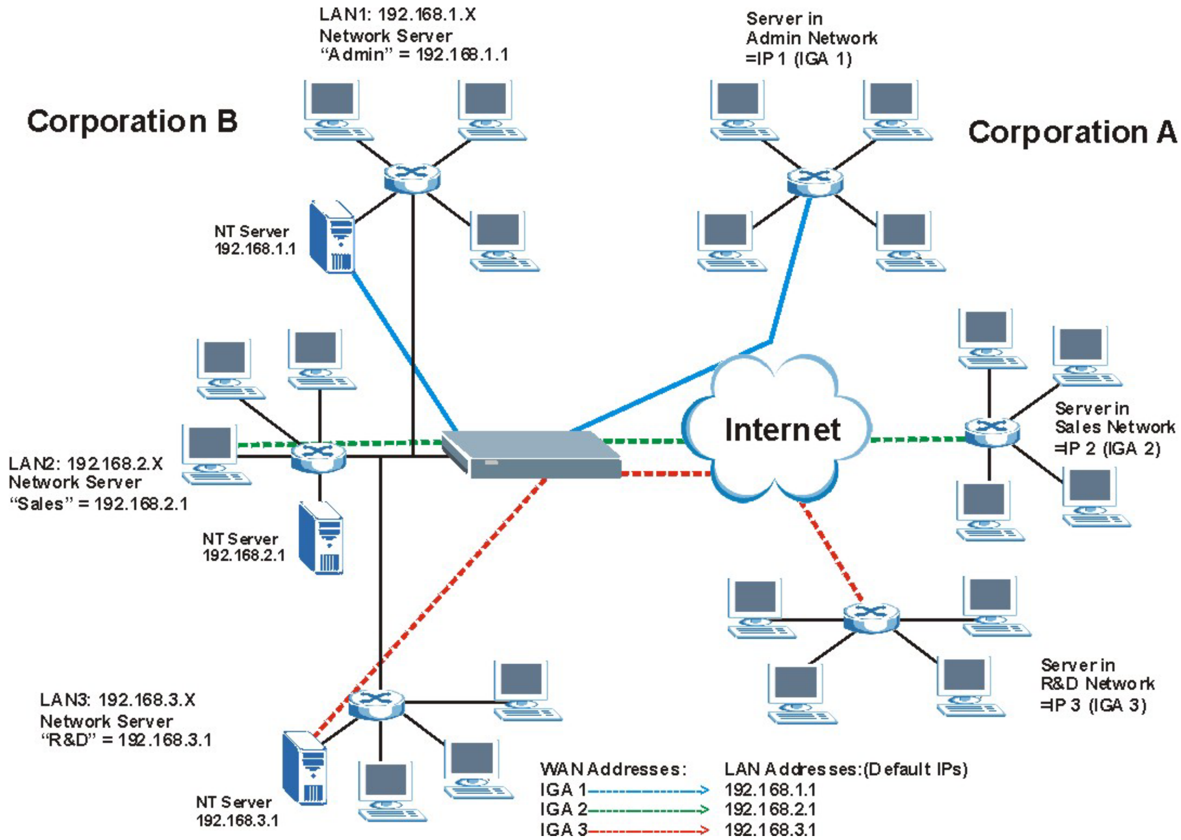



**Figure 6-2 NAT Application With IP Alias**

### 6.1.5 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), the Single User Account feature (the SUA Only 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. Port numbers do **not** change for **One-to-One** and **Many-One-to-One** NAT mapping types.

**TABLE 6-2 NAT MAPPING TYPES**

| TYPE | IP MAPPING | SMT ABBREVIATION |
|---|---|---|
| One-to-One | ILA1←→ IGA1 | 1-1 |
| Many-to-One (SUA/PAT) | ILA1←→ IGA1<br>ILA2←→ IGA1<br>… | M-1 |

**TABLE 6-2 NAT MAPPING TYPES**

| TYPE | IP MAPPING | SMT ABBREVIATION |
|---|---|---|
| Many-to-Many Overload | ILA1←→ IGA1<br>ILA2←→ IGA2<br>ILA3←→ IGA1<br>ILA4←→ IGA2<br>… | M-M Ov |
| Many-One-to-One | ILA1←→ IGA1<br>ILA2←→ IGA2<br>ILA3←→ IGA3<br>… | M-1-1 |
| Server | Server 1 IP←→ IGA1<br>Server 2 IP←→ IGA1<br>Server 3 IP←→ IGA1 | Server |

The following table summarizes these types.

# 6.2 Using NAT

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

## 6.2.1 SUA (Single User Account) Versus NAT

SUA (Single User Account) is an 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 Only** or **Full Feature** in **WAN IP**.

# 6.3 SUA Server

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

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

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

## 6.3.1 Default Server IP Address

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

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

## 6.3.2 Port Forwarding: Services and Port Numbers

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

**Table 6-3 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 |

### 6.3.3 Configuring Servers Behind SUA (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.

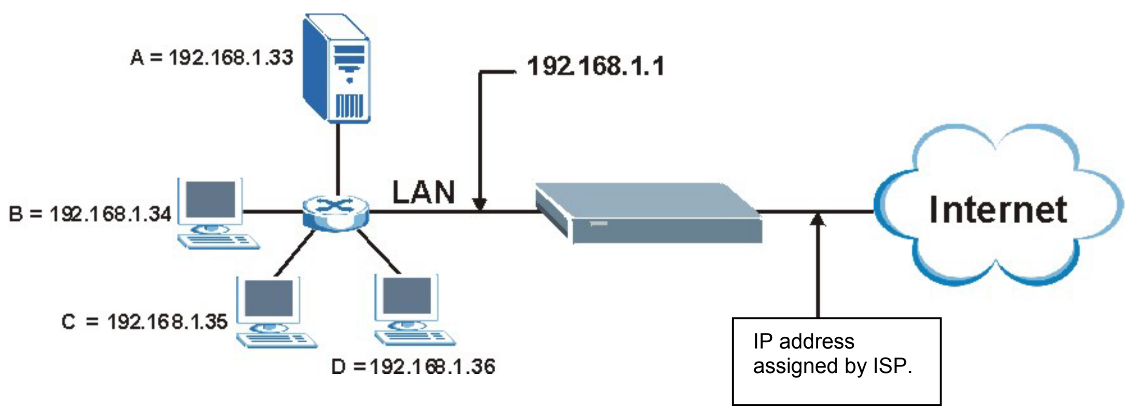



**Figure 6-3 Multiple Servers Behind NAT Example**

## 6.4 Configuring SUA Server

**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.**

Click **SUA/NAT** to open the **SUA Server** screen.

Refer to the firewall chapters for port numbers commonly used for particular services.

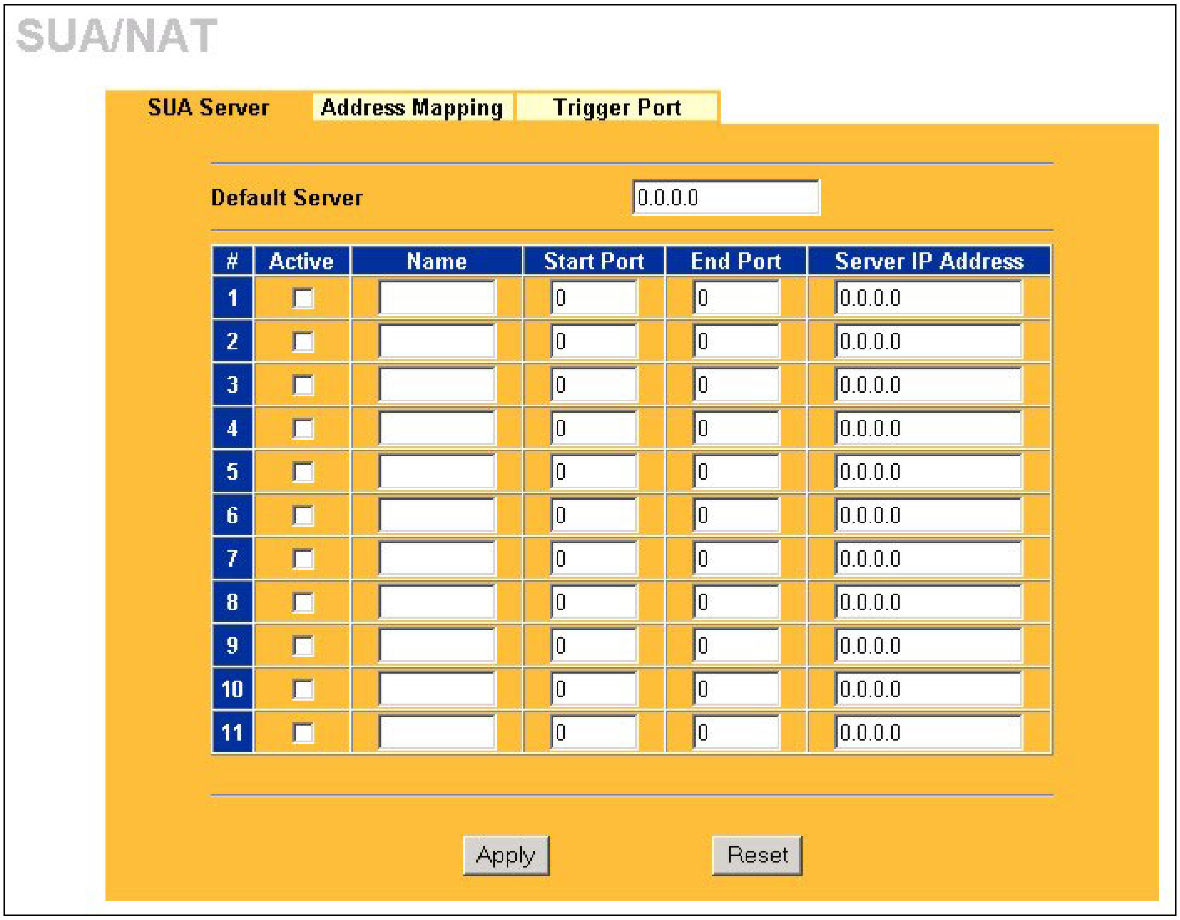



**Figure 6-4 SUA Server**

The following table describes the fields in this screen.

**Table 6-4 SUA Server**

| 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, then all packets received for ports not specified in this screen will be discarded. |
| # | Number of an individual SUA server entry. |
| Active | Select this check box to enable the SUA server entry. Clear this checkbox to disallow forwarding of these ports to an inside server without having to delete the entry. |
| Name | Enter a name to identify this port-forwarding rule. |
| Start Port | Enter a port number here. 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 No** field |
| End Port | |
| Server IP Address | Enter the inside IP address of the server here. |
| Apply | Click **Apply** to save your changes back to the LAN-Cell. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 6.5 Configuring Address Mapping

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.

To change your LAN-Cell's Address Mapping settings, click **SUA/NAT**, then the **Address Mapping** tab. The screen appears as shown.

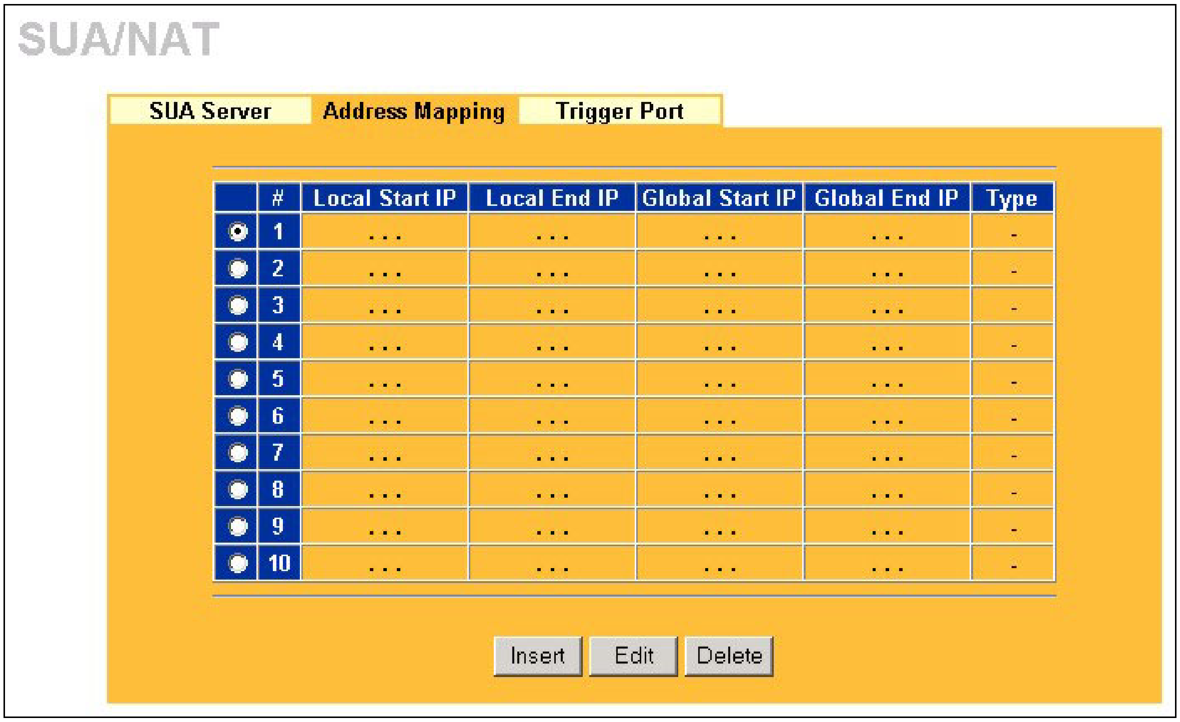



**Figure 6-5 Address Mapping**

The following table describes the fields in this screen.

**Table 6-5 Address Mapping**

| LABEL | DESCRIPTION |
|---|---|
| Local Start IP | This refers to the Inside Local Address (ILA), that is the starting local IP address. Local IP addresses are **N/A** for **Server** port mapping. |
| Local End IP | This is the end Inside Local Address (ILA). If the rule is for all local IP addresses, then this field displays 0.0.0.0 and 255.255.255.255 as the **Local End IP** address. This field is **N/A** for **One-to-One** and **Server** mapping types. |
| Global Start IP | This refers to the Inside Global IP Address (IGA). 0.0.0.0 is for a dynamic IP address from your ISP with **Many-to-One** and **Server** mapping types. |
| Global End IP | This is the ending Inside Global Address (IGA), that is the starting global IP address. 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.<br>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), the Single User Account feature.<br>3. **Many-to-Many Overload** mode maps multiple local IP addresses to shared global IP addresses.<br>4. **Many One-to-One** mode maps each local IP address to unique global IP addresses.<br>5. **Server** allows you to specify inside servers of different services behind the NAT to be accessible to the outside world. |
| Edit | Click **Edit** to go to the **Address Mapping Rule** screen. |
| Delete | Click **Delete** to delete an address mapping rule. |

**Table 6-5 Address Mapping**

| LABEL | DESCRIPTION |
|---|---|
| Insert | Click **Insert** to insert a new mapping rule before an existing one. |

### Configuring Address Mapping

To edit an Address Mapping rule, click the **Edit** button to display the screen shown next.

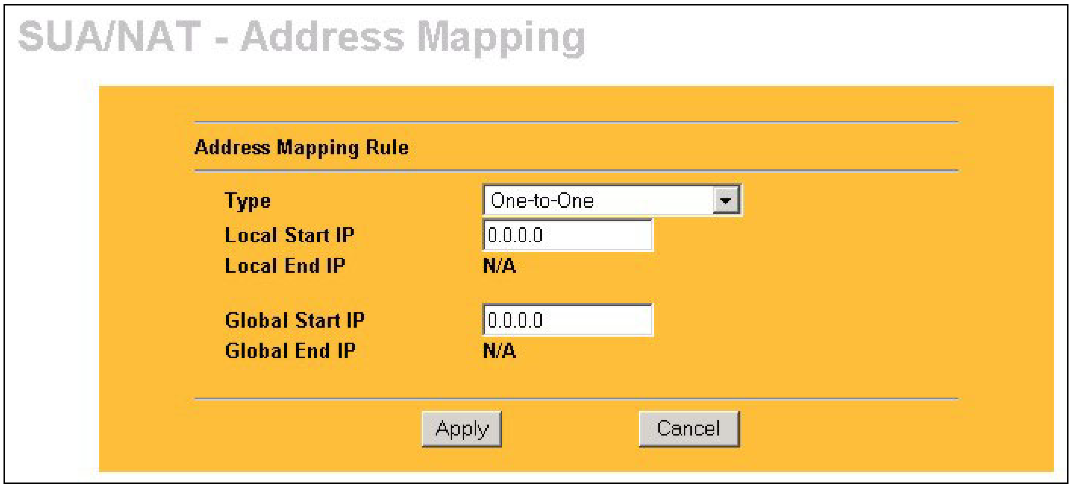



**Figure 6-6 Address Mapping Rule**

The following table describes the fields in this screen.

**Table 6-6 Address Mapping Rule**

| LABEL | DESCRIPTION |
|---|---|
| Type | Choose the port mapping type from one of the following.<br>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.<br>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), the Single User Account feature.<br>3. **Many-to-Many Ov** (Overload): Many-to-Many Overload mode maps multiple local IP addresses to shared global IP addresses.<br>4. **Many One-to-One**: Many One-to-one mode maps each local IP address to unique global IP addresses.<br>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.<br>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. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 6.6 Configuring Trigger Port

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:

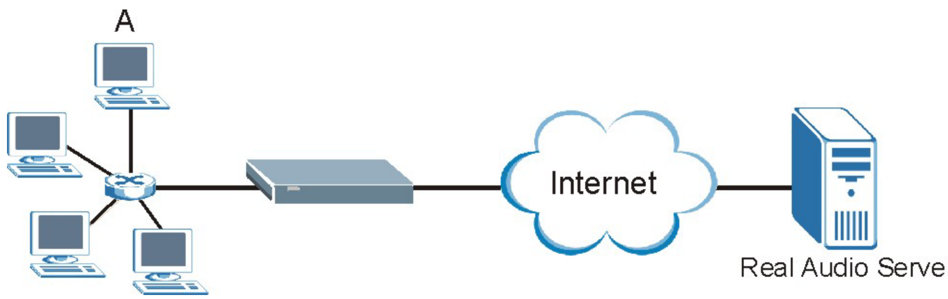



**Figure 6-7 Trigger Port Forwarding Example**

1. **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 **A**'s computer IP address. The LAN-Cell associates **A**'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 **A**'s computer IP address.

5. Only **A** 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).

To change your LAN-Cell's trigger port settings, click **SUA/NAT** and the **Trigger Port** tab. The screen appears as shown.

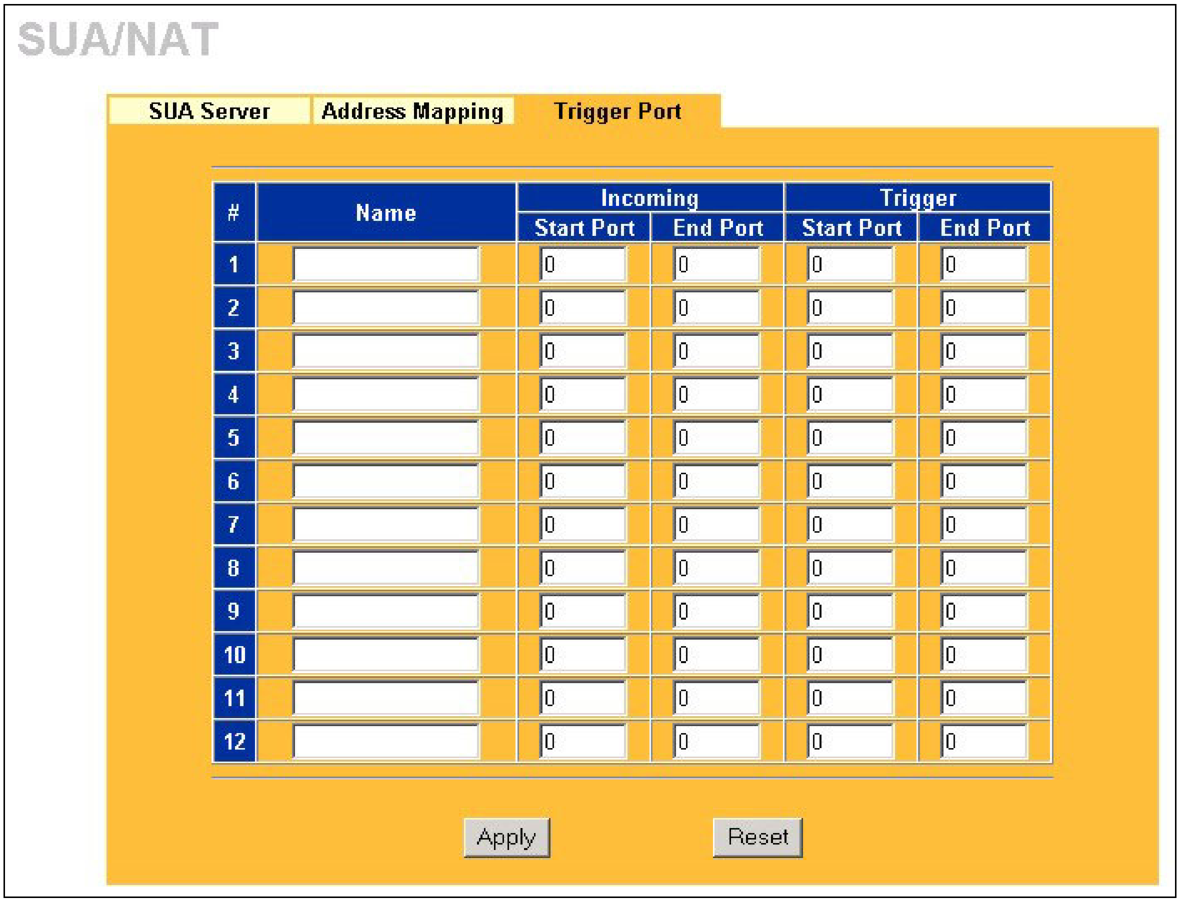



**Figure 6-8 Trigger Port**

The following table describes the fields in this screen.

**Table 6-7 Trigger Port**

| LABEL | DESCRIPTION |
|---|---|
| No. | 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. |

# Chapter 7
# Static Route Screens

*This chapter shows you how to configure static routes for your LAN-Cell.*

## 7.1 Static Route Overview

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.

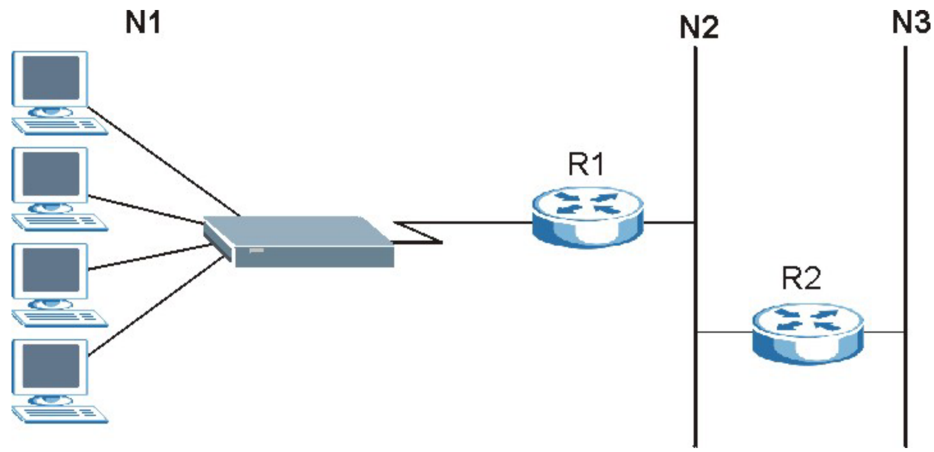



**Figure 7-1 Example of Static Routing Topology**

## 7.2 Configuring IP Static Route

Click **STATIC ROUTE** to open the **Route Entry** screen.

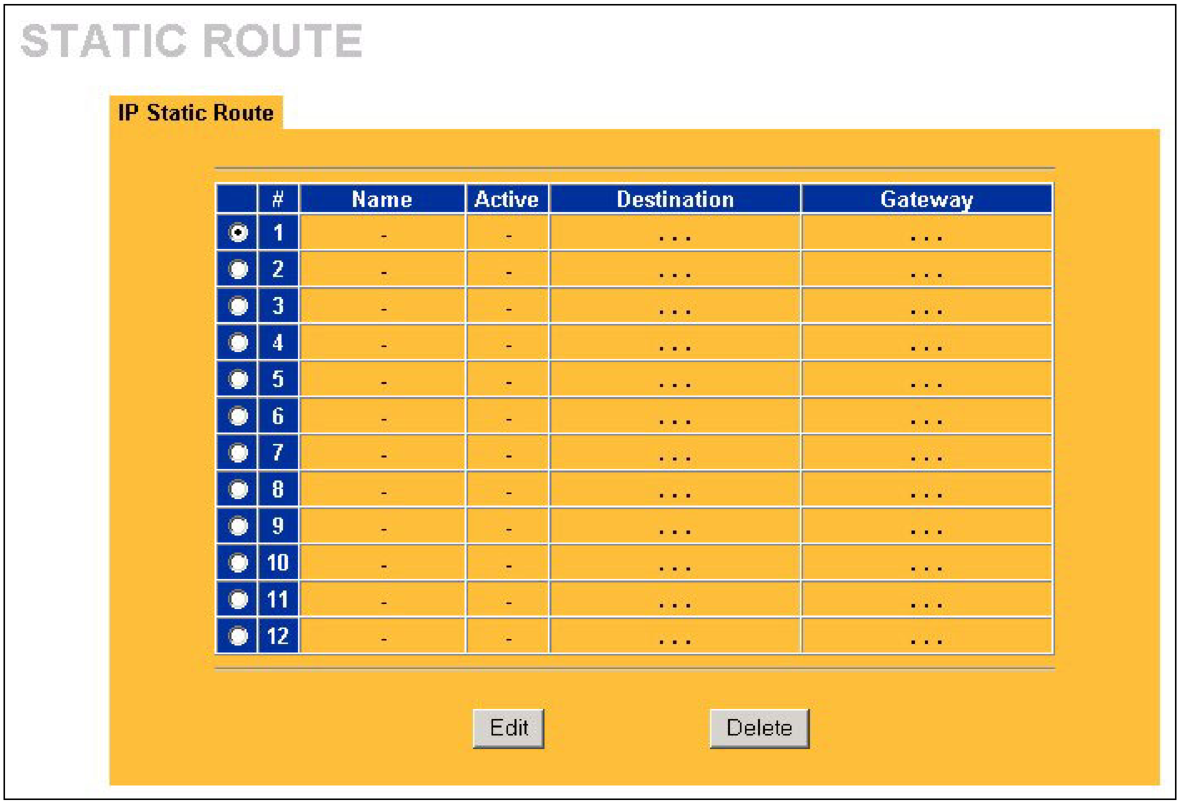



**Figure 7-2 Static Route Screen**

The following table describes the fields in this screen.

**Table 7-1 IP Static Route Summary**

| LABEL | DESCRIPTION |
|---|---|
| # | Number of an individual static route. |
| Name | Name that describes or identifies this route. |
| Active | This field shows whether this static route is active (**Yes**) or not (**No**). |
| Destination | This parameter specifies the IP network address of the final destination. Routing is always based on network number. |
| Gateway | This is the IP address of the gateway. The gateway is 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. |
| Edit | Select the radio button next to a static route index number and then click **Edit** to set up a static route on the LAN-Cell. |
| Delete | Select the radio button next to a static route index number and then click **Delete** to remove a static route on the LAN-Cell. |

### 7.2.1 Configuring Route Entry

Select a static route index number and click **Edit**. The screen shown next appears. Fill in the required information for each static route.

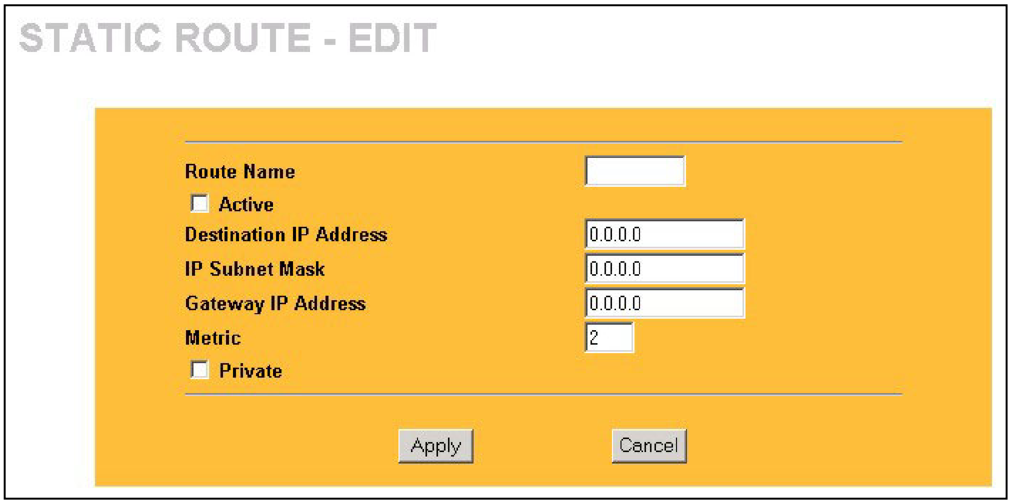



**Figure 7-3 Edit IP Static Route**

The following table describes the fields in this screen.

**Table 7-2 Edit IP Static Route**

| 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 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 | Metric represents the "cost" of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Enter a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number. |
| Private | This parameter determines if the LAN-Cell will include this route to a remote node in its RIP broadcasts.<br>Select this check box to keep this route private and not included in RIP broadcasts. Clear this checkbox to propagate this route to other hosts through RIP broadcasts. |
| Apply | Click **Apply** to save your changes back to the LAN-Cell. |
| Cancel | Click **Cancel** to exit this screen without saving. |

# Part V:

## Firewall and Content Filters

This part introduces firewalls in general and the LAN-Cell firewall.
It also explains how to configure the LAN-Cell firewall and content filtering.

# Chapter 8 Firewalls

*This chapter gives some background information on firewalls and introduces the LAN-Cell firewall.*

## 8.1 Firewall Overview

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

## 8.2 Types of Firewalls

There are three main types of firewalls:

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

### 8.2.1 Packet Filtering Firewalls

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

### 8.2.2 Application-level Firewalls

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

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

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

### 8.2.3 Stateful Inspection Firewalls

Stateful inspection firewalls restrict access by screening data packets against defined access rules. They make access control decisions based on IP address and protocol. They also "inspect" the session data to assure the integrity of the connection and to adapt to dynamic protocols. These firewalls generally provide the best speed and transparency; however, they may lack the granular application level access control or caching that some proxies support. See *section 8.5* for more information on Stateful Inspection.

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

## 8.3 Introduction to the LAN-Cell Firewall

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

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

The LAN-Cell has one Ethernet WAN port and one Ethernet LAN port, which are used to physically separate the network into two areas.

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

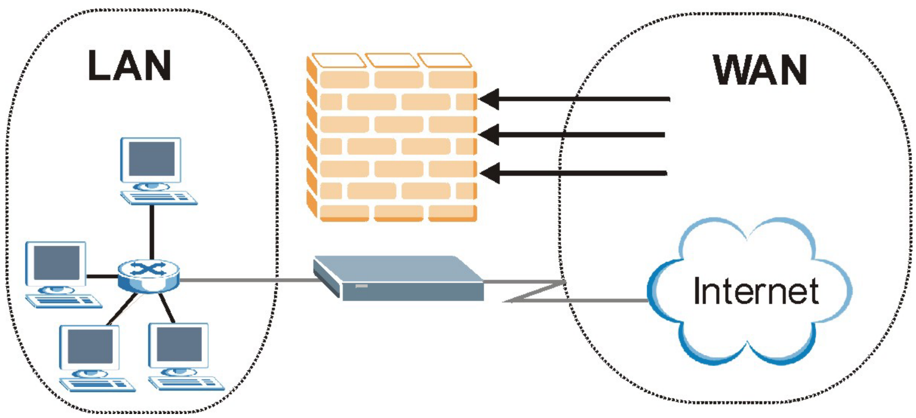



**Figure 8-1 LAN-Cell Firewall Application**

## 8.4 Denial of Service

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

### 8.4.1 Basics

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

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

Some of the most common IP ports are:

**Table 8-1 Common IP Ports**

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

### 8.4.2 Types of DoS Attacks

There are four types of DoS attacks:

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

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

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

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

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

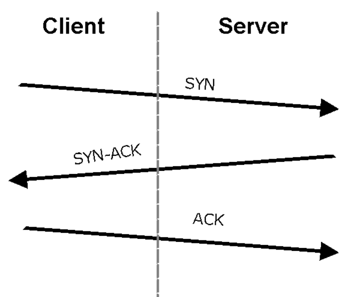



**Figure 8-2 Three-Way Handshake**

➢ 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.

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

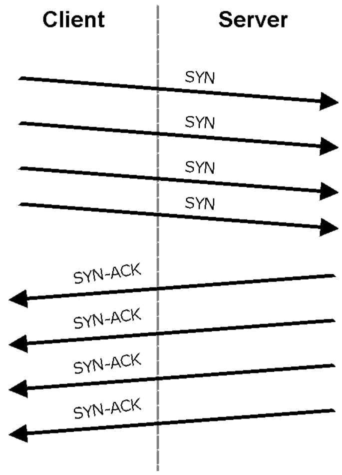



**Figure 8-3 SYN Flood**

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

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

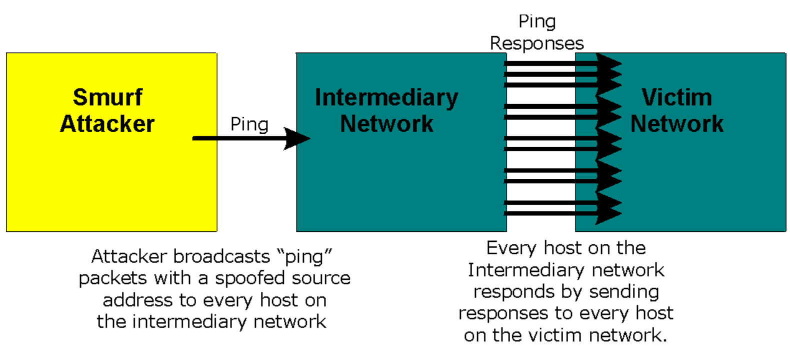



**Figure 8-4 Smurf Attack**

- ICMP Vulnerability

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

**Table 8-2 ICMP Commands That Trigger Alerts**

| | |
|---|---|
| 5 | REDIRECT |
| 13 | TIMESTAMP_REQUEST |
| 14 | TIMESTAMP_REPLY |
| 17 | ADDRESS_MASK_REQUEST |
| 18 | ADDRESS_MASK_REPLY |

- Illegal Commands (NetBIOS and SMTP)

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

**Table 8-3 Legal NetBIOS Commands**

| |
|---|
| MESSAGE: |
| REQUEST: |
| POSITIVE: |
| NEGATIVE: |
| RETARGET: |
| KEEPALIVE: |

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

**Table 8-4 Legal SMTP Commands**

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

- Traceroute

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

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

## 8.5 Stateful Inspection

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

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

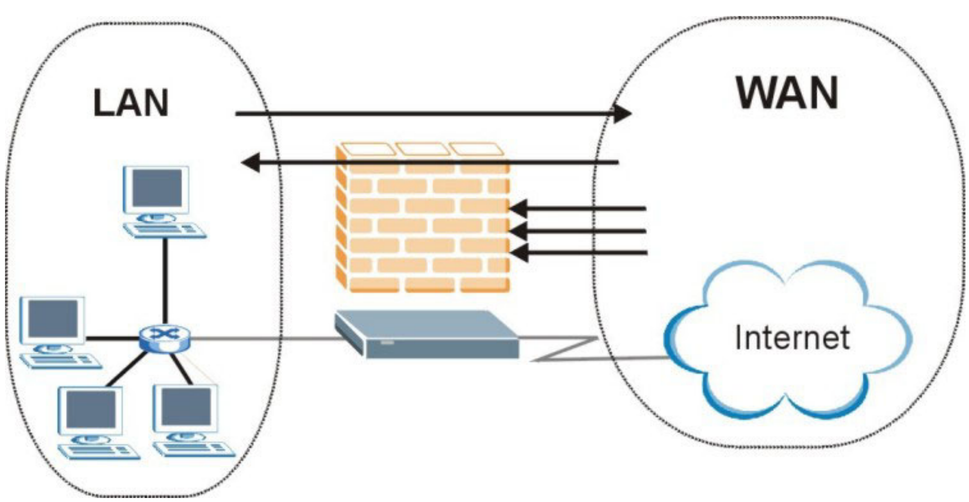



**Figure 8-5 Stateful Inspection**

The previous figure shows the LAN-Cell's default firewall rules in action as well as demonstrates how stateful inspection works. User A can initiate a Telnet session from within the LAN and responses to this request are allowed. However other Telnet traffic initiated from the WAN is blocked.

### 8.5.1 Stateful Inspection Process

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

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

### 8.5.2 Stateful Inspection and the LAN-Cell

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

i. Block all traffic of a certain type, such as IRC (Internet Relay Chat), from the LAN to the Internet.

ii. Allow certain types of traffic from the Internet to specific hosts on the LAN.

iii. Allow access to a Web server to everyone but competitors.

iv. Restrict use of certain protocols, such as Telnet, to authorized users on the LAN.

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

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

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

### 8.5.3 TCP Security

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

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

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

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

### 8.5.4 UDP/ICMP Security

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

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

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

### 8.5.5 Upper Layer Protocols

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

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

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

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

## 8.6 Guidelines For Enhancing Security With Your Firewall

1. Change the default password via SMT or web configurator.
2. Limit who can telnet into your LAN-Cell.
3. Don't enable any local service (such as SNMP or NTP) that you don't use. Any enabled service could present a potential security risk. A determined hacker might be able to find creative ways to misuse the enabled services to access the firewall or the network.
4. For local services that are enabled, protect against misuse. Protect by configuring the services to communicate only with specific peers, and protect by configuring rules to block packets for the services at specific interfaces.
5. Protect against IP spoofing by making sure the firewall is active.
6. Keep the LAN-Cell in a secured (locked) room.

## 8.7 Packet Filtering Vs Firewall

Below are some comparisons between the LAN-Cell's filtering and firewall functions.

### 8.7.1 Packet Filtering:

- The LAN-Cell 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.

#### 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.

### 8.7.2 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.

#### 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.

# Chapter 9
# Firewall Screens

*This chapter shows you how to configure your LAN-Cell firewall.*

## 9.1 Access Methods

The web configurator is, by far, the most comprehensive firewall configuration tool your LAN-Cell has to offer. For this reason, it is recommended that you configure your firewall using the web configurator. SMT screens allow you to activate the firewall. CLI commands provide limited configuration options and are only recommended for advanced users, please refer to the *Appendices* for firewall CLI commands.

## 9.2 Firewall Policies Overview

Firewall rules are grouped based on the direction of travel of packets to which they apply:

- LAN to LAN/LAN-Cell
- LAN to WAN
- WAN to LAN
- WAN to WAN/LAN-Cell

By default, the LAN-Cell's stateful packet inspection allows packets traveling in the following directions:

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

By default, the LAN-Cell's stateful packet inspection blocks packets traveling in the following directions:

- WAN to LAN
- WAN to WAN/LAN-Cell

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

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

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

For example, you may create rules to:

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

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

## 9.3 Rule Logic Overview

**Study these points carefully before configuring rules.**

### 9.3.1 Rule Checklist

1. State the intent of the rule. For example, "This restricts all IRC access from the LAN to the Internet." Or, "This allows a remote Lotus Notes server to synchronize over the Internet to an inside Notes server."
2. Is the intent of the rule to forward or block traffic?
3. What direction of traffic does the rule apply to (refer to *9.2*)?
4. What IP services will be affected?
5. What computers on the LAN are to be affected (if any)?
6. What computers on the Internet will be affected? The more specific, the better. For example, if traffic is being allowed from the Internet to the LAN, it is better to allow only certain machines on the Internet to access the LAN.

### 9.3.2 Security Ramifications

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

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

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

### 9.3.3 Key Fields For Configuring Rules

#### Action

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

**"Block" means the firewall silently discards the packet.**

#### Service

Select the service from the **Service** scrolling list box. If the service is not listed, it is necessary to first define it. See *section 9.8* for more information on predefined services.

#### Source Address

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

#### Destination Address

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

## 9.4 Connection Direction Examples

This section describes examples for firewall rules for connections going from LAN to WAN and from WAN to LAN.

LAN to LAN/LAN-Cell, WAN and WAN/LAN-Cell rules apply to packets coming in on the associated interface (LAN or WAN respectively). LAN to LAN/LAN-Cell means policies for LAN-to-LAN-Cell (the policies for managing the LAN-Cell through the LAN interface) and policies for LAN-to-LAN (the policies that control routing between two subnets on the LAN). Similarly, WAN to WAN/LAN-Cell polices apply in the same way to the WAN ports.

### 9.4.1 LAN to WAN Rules

The default rule for LAN to WAN traffic is that all users on the LAN are allowed non-restricted access to the WAN. When you configure a LAN to WAN rule, you in essence want to limit some or all users from accessing certain services on the WAN. See the following figure.

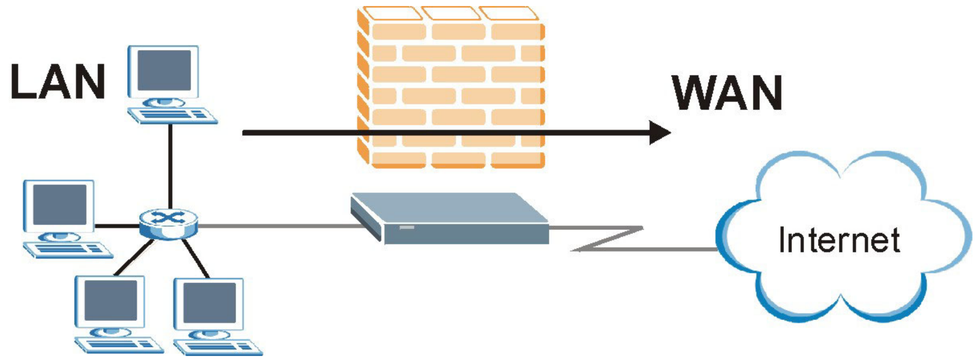



**Figure 9-1 LAN to WAN Traffic**

### 9.4.2 WAN to LAN Rules

The default rule for WAN to LAN traffic blocks all incoming connections (WAN to LAN). If you wish to allow certain WAN users to have access to your LAN, you will need to create custom rules to allow it. See the following figure.

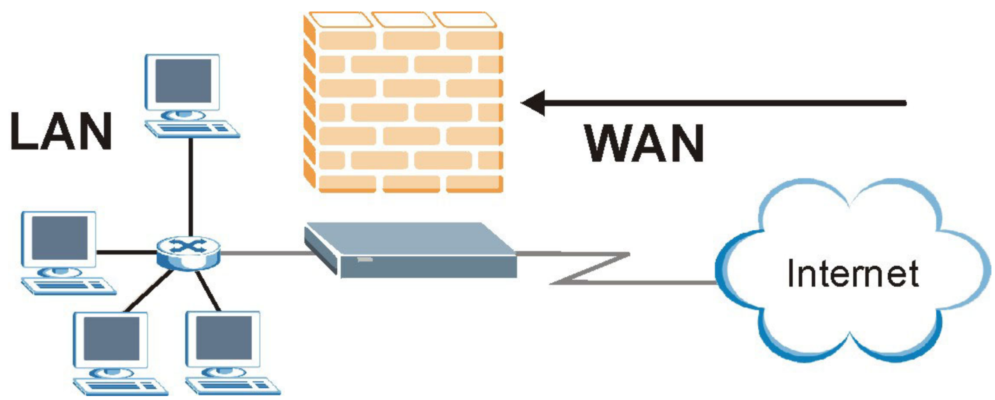



**Figure 9-2 WAN to LAN Traffic**

## 9.5 Alerts

Alerts are reports on events, such as attacks, that you may want to know about right away. You can choose to generate an alert when an attack is detected in the **Attack Alert** screen *(Figure 9-12* - check the **Generate alert when attack detected** checkbox) or when a rule is matched in the **Edit Rule** screen (see *Figure 9-4)*. Configure the **Log Settings** screen to have the LAN-Cell send an immediate e-mail message to you when an event generates an alert. Refer to the chapter on logs for details.

## 9.6 Configuring Firewall

**The ordering of your rules is very important as rules are applied in turn.**

Click FIREWALL to open the Summary screen. Enable (or activate) the firewall by selecting the Enable Firewall check box as seen in the following screen.

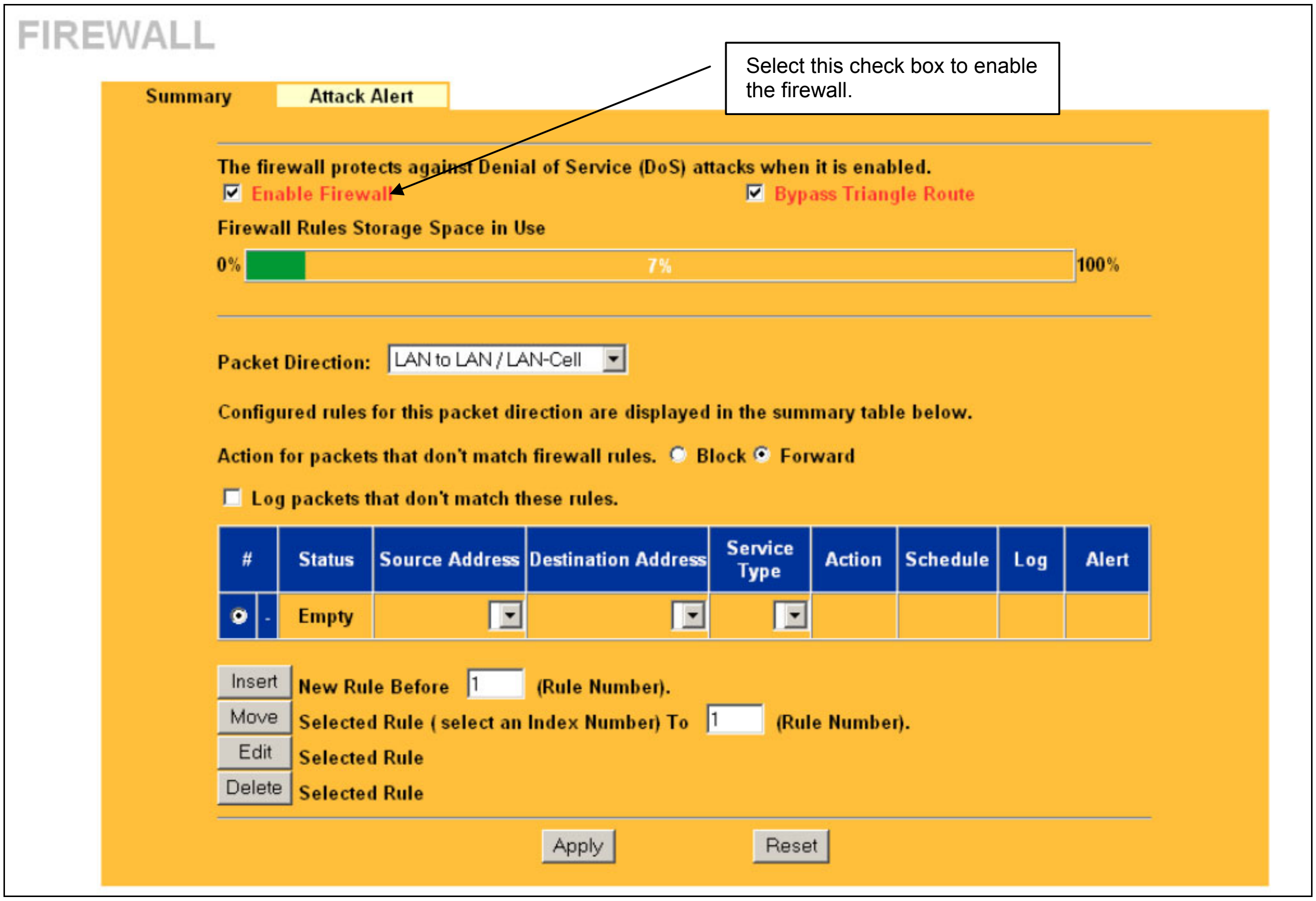



**Figure 9-3 Enabling the Firewall**

The following table describes the fields in this screen.

**Table 9-1 Firewall Rules Summary: First Screen**

| LABEL | DESCRIPTION |
|---|---|
| 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. |
| Bypass Triangle Route | Select this check box to have the LAN-Cell firewall ignore the use of triangle route topology on the network. See the *Appendices* for more on triangle route topology. |
| Firewall Rules Storage Space in Use | This read-only bar shows how much of the LAN-Cell's memory for recording firewall rules it is currently using. When you are using 80% or less of the storage space, the bar is green. When the amount of space used is over 80%, the bar is red. |

**Table 9-1 Firewall Rules Summary: First Screen**

| LABEL | DESCRIPTION |
|---|---|
| Packet Direction | Use the drop-down list box to select a direction of travel of packets (**LAN to LAN/LAN-Cell**, **LAN to WAN**, **WAN to LAN**, **WAN to WAN/LAN-Cell**) for which you want to configure firewall rules. |
| Block/ Forward | Use the option buttons to select whether to **Block** (silently discard) or **Forward** (allow the passage of) packets that are traveling in the selected direction. |
| Log | Select the check box to create a log (when the above action is taken) for packets that are traveling in the selected direction and do not match any of the rules below. |
| 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. | |
| # | This is your firewall rule number. The ordering of your rules is important as rules are applied in turn. The **Move** field below allows you to reorder your rules. |
| Status | This field displays whether a firewall is turned on (**Active**) or not (**Inactive**). Rules that have not been configured display **Empty**. |
| 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. Please note that a blank service type is equivalent to **Any**. See *Table 9-5* for more information. |
| Action | This is the specified action for that rule, either **Block** or **Forward**. Note that **Block** means the firewall silently discards the packet. |
| Schedule | This field tells you whether a schedule is specified (**Yes**) or not (**No**). |
| Log | This field shows you if a log is created for packets that match the rule (**Match**), don't match the rule (**Not Match**), both (**Both**) or no log is created (**None**). |
| Alert | This field tells you whether this rule generates an alert (**Yes**) or not (**No**) when the rule is matched. |
| Insert | Type the index number for where you want to put a rule. For example, if you type "6", your new rule becomes number 6 and the previous rule 6 (if there is one) becomes rule 7.<br>Click **Insert** to display this screen and refer to the following table for information on the fields. |
| Move | Select a rule's Index option button and type a number for where you want to put that rule. Click **Move** to move the rule to the number that you typed. The ordering of your rules is important as they are applied in order of their numbering. |
| Edit | Click **Edit** to create or edit a rule. |
| Delete | Click **Delete** to delete an existing firewall rule. Note that subsequent firewall rules move up by one when you take this action. |
| Apply | Click **Apply** to save your changes back to the LAN-Cell. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 9.6.1 Configuring Firewall Rules

Follow these directions to create a new rule.

**Step 1.** In the **Summary** screen, type the index number for where you want to put the rule. For example, if you type "6", your new rule becomes number 6 and the previous rule 6 (if there is one) becomes rule 7.

**Step 2.** Click **Insert** to display this screen and refer to the following table for information on the fields.

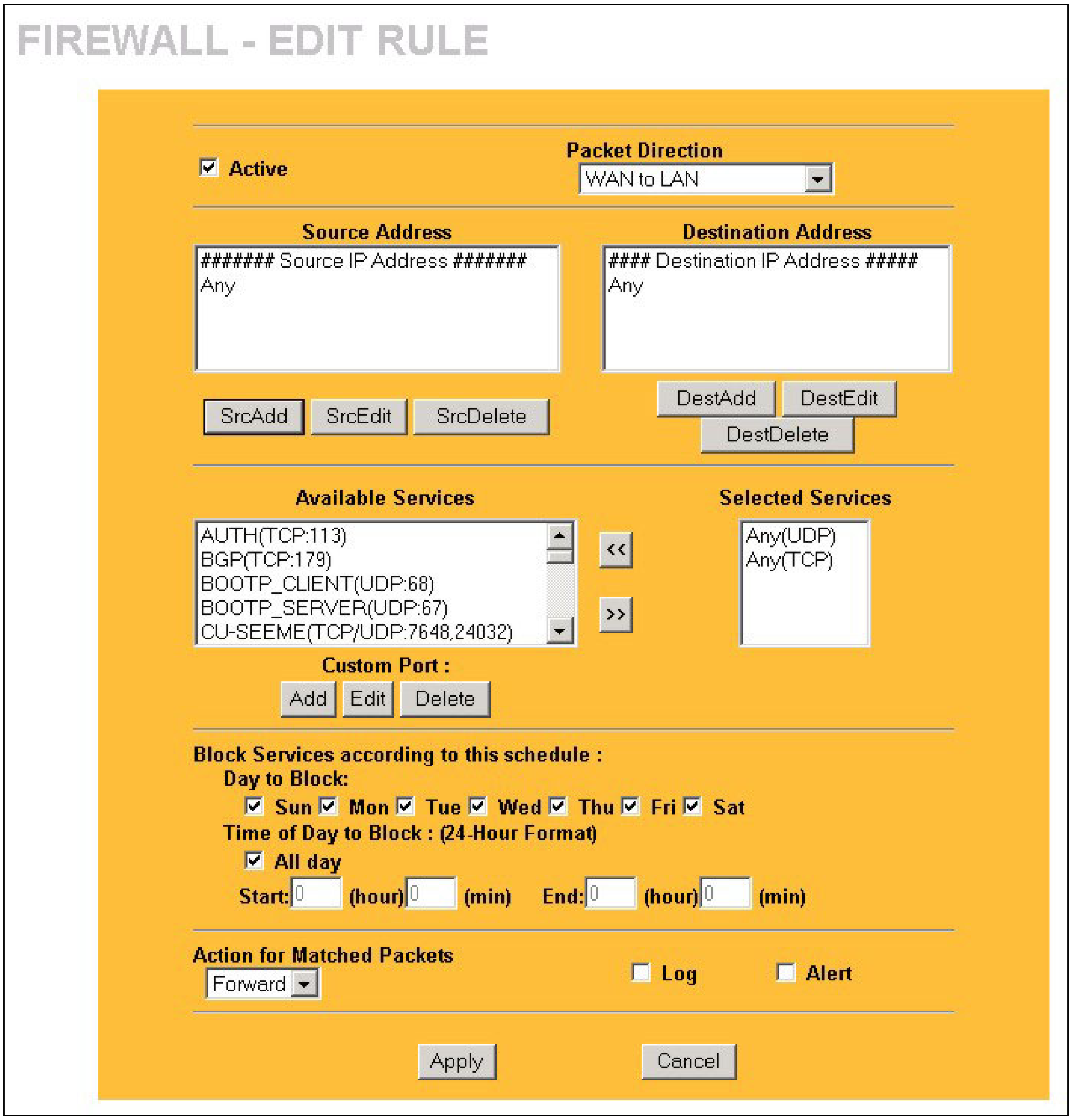



**Figure 9-4 Creating/Editing A Firewall Rule**

The following table describes the fields in this screen.

**Table 9-2 Creating/Editing A Firewall Rule**

| LABEL | DESCRIPTION |
|---|---|
| Active | Check the **Active** check box to have the LAN-Cell use this rule. Leave it unchecked if you do not want the LAN-Cell to use the rule after you apply it |
| Packet Direction | Use the drop-down list box to select the direction of packet travel to which you want to apply this firewall rule. |
| Source Address | Click **SrcAdd** to add a new address, **SrcEdit** to edit an existing one or **SrcDelete** to delete one. Please see the next section for more information on adding and editing source addresses. |

**Table 9-2 Creating/Editing A Firewall Rule**

| LABEL | DESCRIPTION |
|---|---|
| Destination Address | Click **DestAdd** to add a new address, **DestEdit** to edit an existing one or **DestDelete** to delete one. Please see the following section on adding and editing destination addresses. |
| Available/ Selected Services | Please see *Table 9-5* for more information on services available. Highlight a service from the **Available Services** box on the left, then click **>>** to add it to the **Selected Services** box on the right. To remove a service, highlight it in the **Selected Services** box on the right, then click **<<**. |
| Custom Port | |
| Add | Click this button to bring up the screen that you use to configure a new custom service that is not in the predefined list of services. |
| Edit | Select a custom service (denoted by an "*") from the **Available Services** list and click this button to edit the service. |
| Delete | Select a custom service (denoted by an "*") from the **Available Services** list and click this button to remove the service. |
| Block Services according to this schedule : | |
| Day to Block | Select everyday or the day(s) of the week to activate blocking. |
| Time of Day to Block (24-Hour Format) | Select **All Day** or enter the start and end times in the hour-minute format to activate blocking. |
| Action for Matched Packets | Use the drop down list box to select whether to discard (**Block**) or allow the passage of (**Forward**) packets that match this rule. |
| Log | This field determines if a log is created for packets that match the rule (**Match**), don't match the rule (**Not Match**), both (**Both**) or no log is created (**None**). Go to the **Log Settings** page and select the **Access Control** logs category to have the LAN-Cell record these logs. |
| Alert | Check the **Alert** check box to determine that this rule generates an alert when the rule is matched. |
| Apply | Click **Apply** to save your customized settings and exit this screen. |
| Cancel | Click **Cancel** to exit this screen without saving, |

## 9.6.2 Configuring Source and Destination Addresses

To add a new source or destination address, click **SrcAdd** or **DestAdd** from the previous screen. To edit an existing source or destination address, select it from the box and click **SrcEdit** or **DestEdit** from the previous screen**.** Either action displays the following screen.

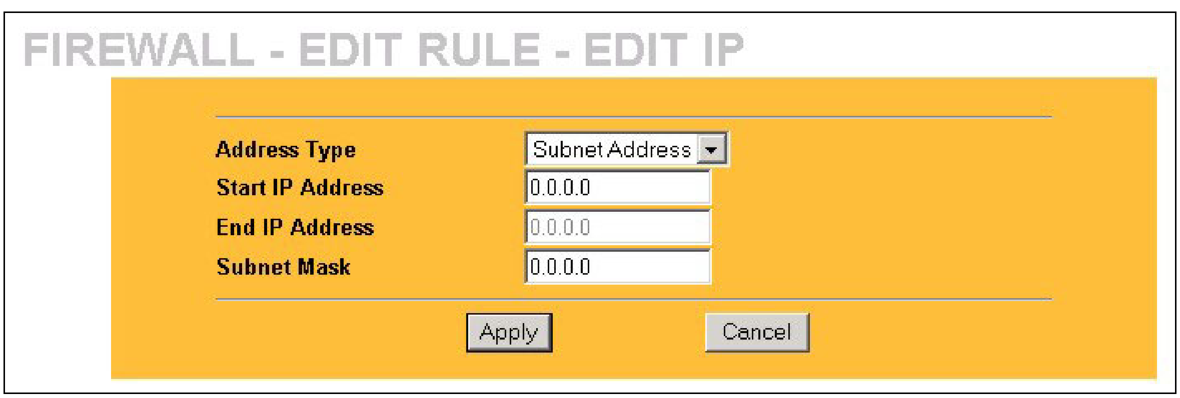



**Figure 9-5 Adding/Editing Source and Destination Addresses**

The following table describes the fields in this screen.

**Table 9-3 Adding/Editing Source and Destination Addresses**

| LABEL | DESCRIPTION |
|---|---|
| Address Type | Do you want your rule to apply to packets with a particular (single) IP, a range of IP addresses (e.g., 192.168.1.10 to 192.169.1.50), a subnet or any IP address? Select an option from the drop-down list box that includes: **Single Address**, **Range Address**, **Subnet Address** and **Any Address**. |
| Start IP Address | Enter the single IP address or the starting IP address in a range here. |
| End IP Address | Enter the ending IP address in a range here. |
| Subnet Mask | Enter the subnet mask here, if applicable. |
| Apply | Click **Apply** to save your customized settings and exit this screen. |
| Cancel | Click **Cancel** to exit this screen without saving, |

## 9.6.3 Configuring Custom Ports

Configure customized ports for services not predefined by the LAN-Cell (see *section 9.8* for a list of predefined services). For a comprehensive list of port numbers and services, visit the IANA (Internet Assigned Number Authority) web site.

Click the **Add** button under **Custom Port** while editing a firewall to configure a custom port. This displays the following screen.

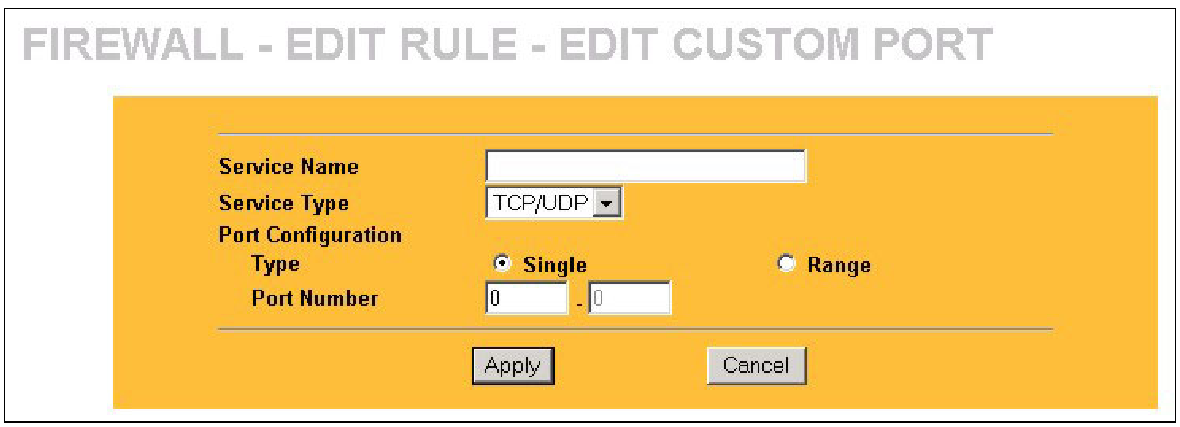



**Figure 9-6 Creating/Editing A Custom Port**

The following table describes the fields in this screen.

**Table 9-4 Creating/Editing A Custom Port**

| LABEL | DESCRIPTION |
|---|---|
| Service Name | Enter a unique name for your custom port. |
| Service Type | Choose the IP port (**TCP**, **UDP** or **Both**) that defines your customized port from the drop down list box. |
| Port Configuration | |
| Type | Select **Single** to specify one port only or **Range** to specify a span of ports that define your customized service. |
| Port Number | Enter a single port number or the range of port numbers that define your customized service. |
| Apply | Click **Apply** to save your customized settings and exit this screen. |
| Cancel | Click **Cancel** to exit this screen without saving, |

## 9.7 Example Firewall Rule

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

**Step 1.** Click the **Firewall** link and then the **Summary** tab.

**Step 2.** In the **Summary** screen, type the index number for where you want to put the rule. For example, if you type "6", your new rule becomes number 6 and the previous rule 6 (if there is one) becomes rule 7.

**Step 3.** Click **Insert** to display the firewall rule configuration screen.

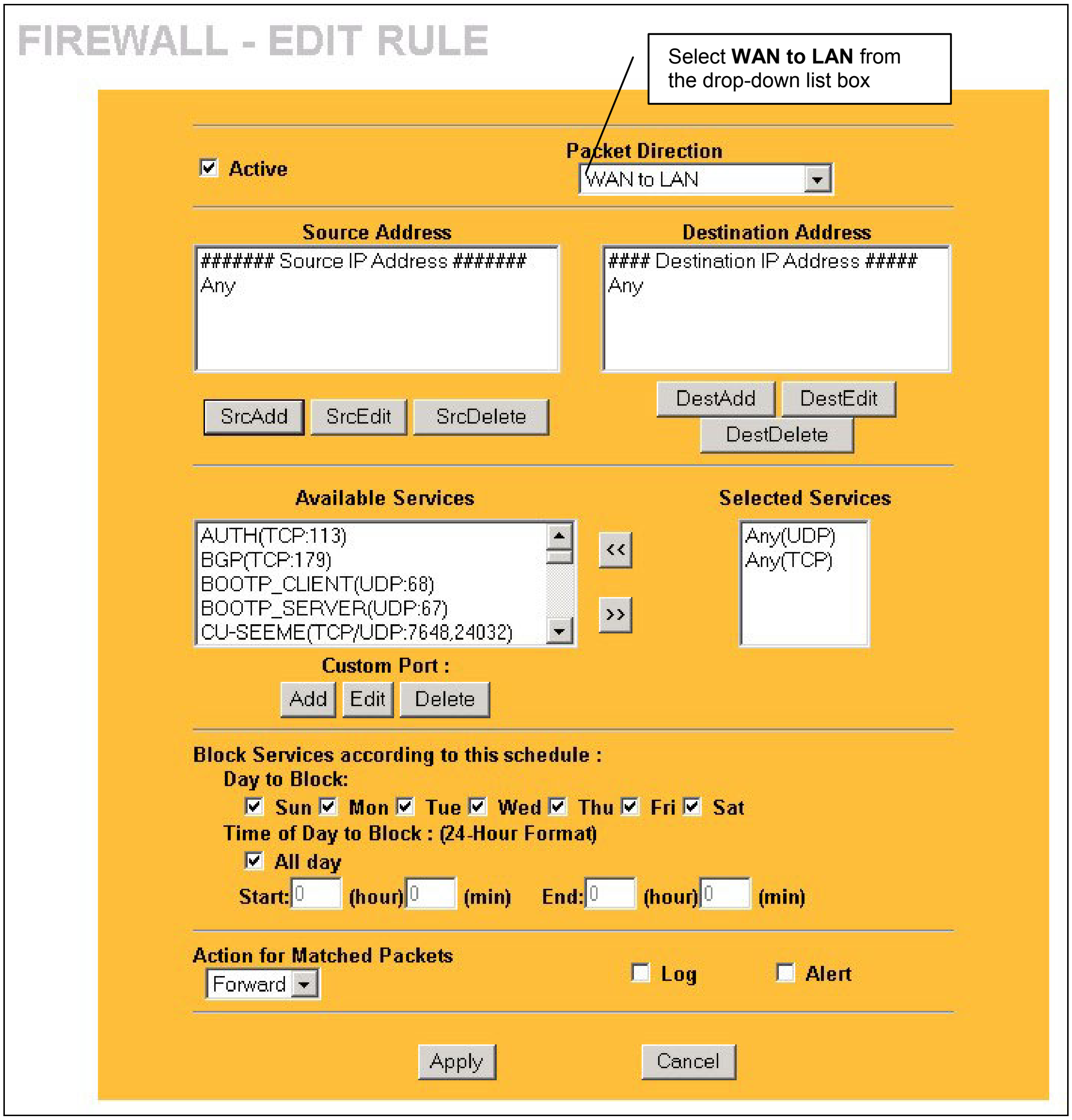



**Figure 9-7 Firewall IP Config Screen**

**Step 4.** Select **Any** in the Destination Address box and then click **DestDelete**.

**Step 5.** Click **DestAdd** under the Source Address box.

**Step 6.** Configure the **Firewall Rule Edit IP** screen as follows and click **Apply**.

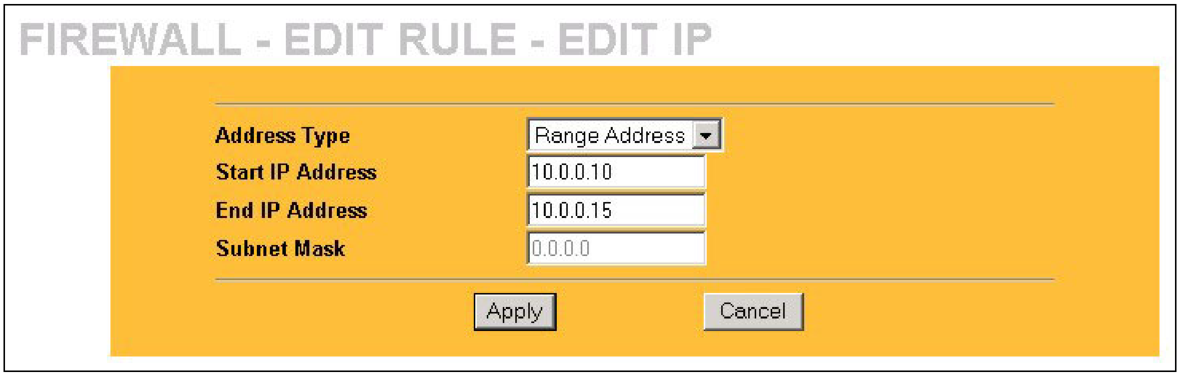



**Figure 9-8 Firewall Rule Edit IP Example**

**Step 7.** In the firewall rule configuration screen, click **Add** under **Custom Port** to open the **Edit Custom Port** screen. Configure it as follows and click **Apply**.

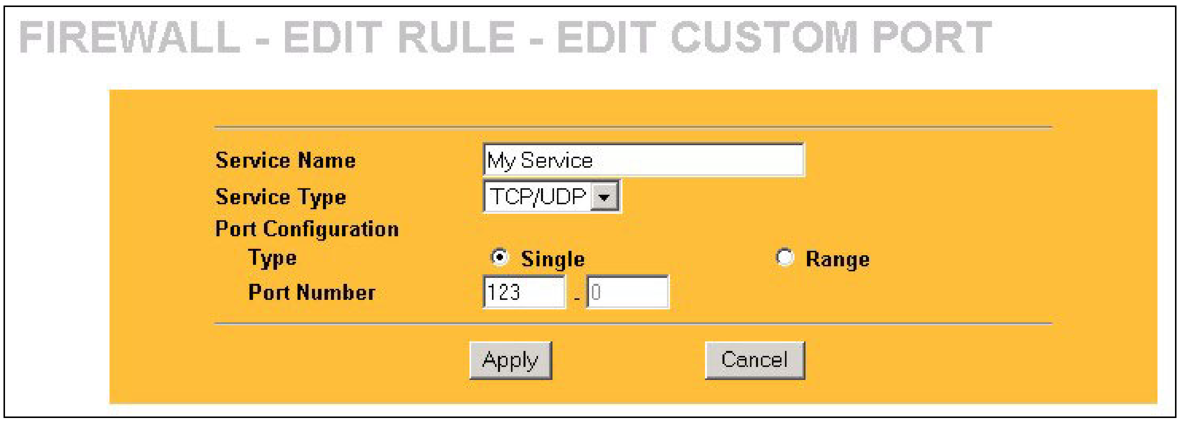



**Figure 9-9 Edit Custom Port Example**

**Step 8.** The firewall rule configuration screen displays, use the arrows between **Available Services** and **Selected Services** to configure it as follows. Click **Apply** when you are done.

**Custom ports show up with an "*" before their names in the** Services **list box and the Rule Summary list box. Click** Apply **after you've created your custom port.**

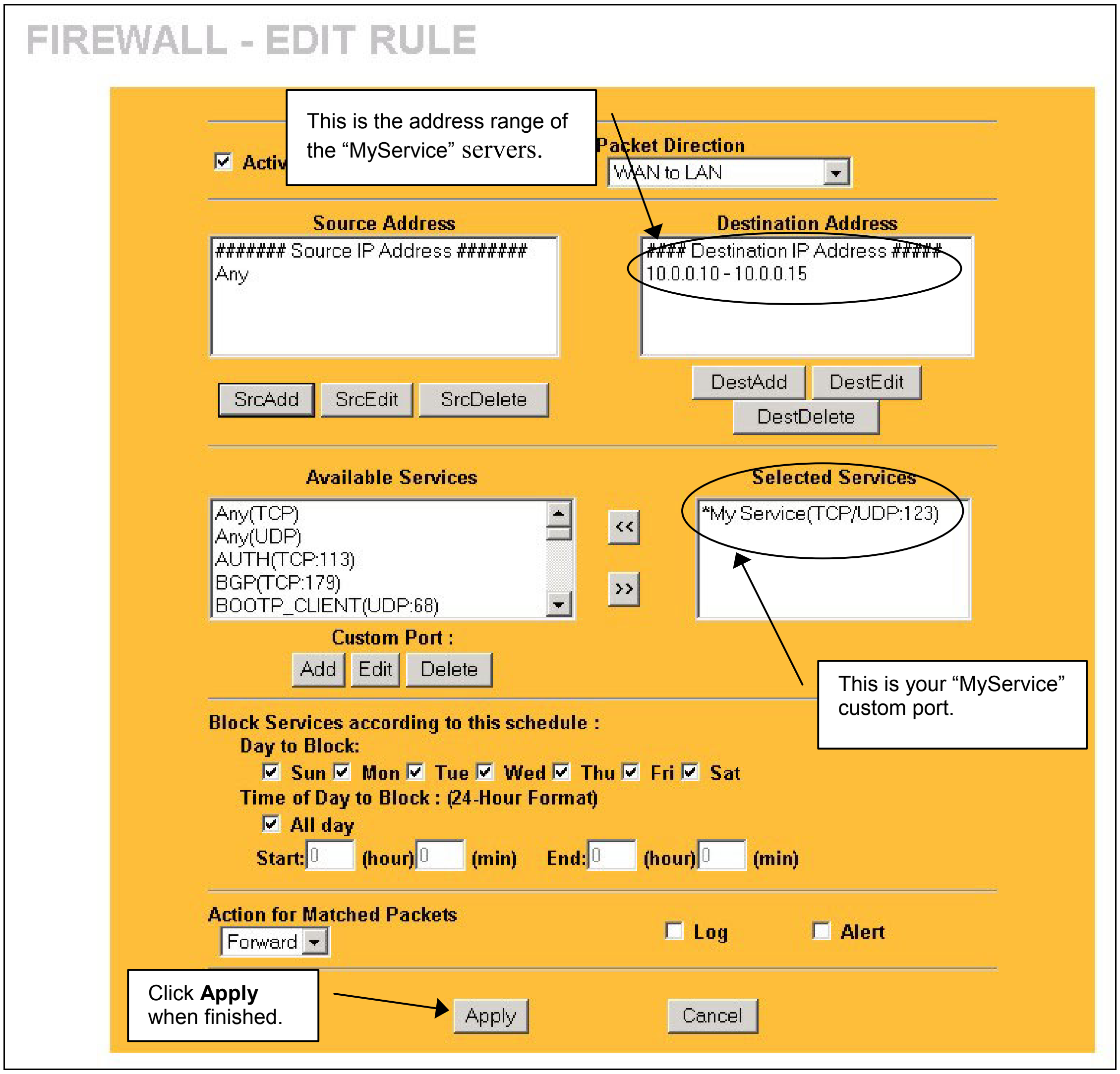



**Figure 9-10 MyService Rule Configuration**

On completing the configuration procedure for this Internet firewall rule, the **Rule Summary** screen should look like the following. Remember to click **Apply** when you have finished configuring your rule(s) to save your settings back to the LAN-Cell.

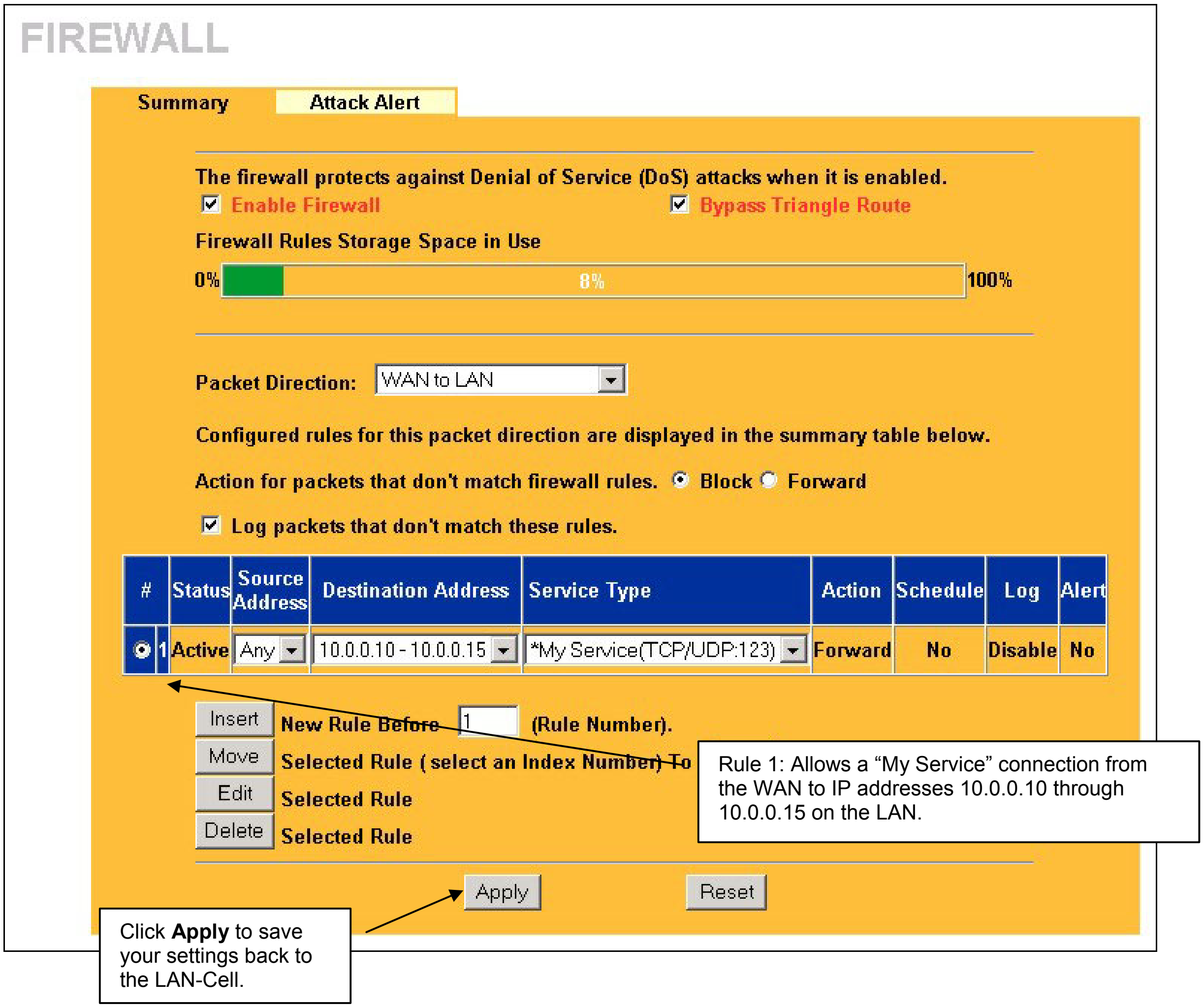



**Figure 9-11 My Service Example Rule Summary**

## 9.8 Predefined Services

The **Available Services** list box in the **Rule Config**(uration) screen (see *Figure 9-4*) displays all predefined services that the LAN-Cell already supports. Next to the name of the 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 default configuration labeled "(**DNS**)". **(UDP/TCP:53)** means UDP port 53 and TCP port 53. Custom services may also be configured using the **Custom Ports** function discussed later.

**Table 9-5 Predefined Services**

| SERVICE | DESCRIPTION |
|---|---|
| AIM/New-ICQ(TCP:5190) | AOL's Internet Messenger service, 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. |

**Table 9-5 Predefined Services**

| SERVICE | DESCRIPTION |
|---|---|
| DNS(UDP/TCP:53) | Domain Name Server, a service that matches web names (e.g. www.nortelnetworks.com) to IP numbers. |
| FINGER(TCP:79) | Finger is a UNIX or Internet related command that can be used to find out if a user is logged on. |
| FTP(TCP:20.21) | 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. |
| ICQ(UDP:4000) | This is a popular Internet chat program. |
| IKE(UDP:500) | The Internet Key Exchange algorithm is used for key distribution and management. |
| IPSEC_TUNNEL(AH:0) | The IPSEC AH (Authentication Header) tunneling protocol uses this service. |
| IPSEC_TUNNEL(ESP:0) | The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service. |
| IRC(TCP/UDP:6667) | This is another popular Internet chat program. |
| MSN Messenger(TCP:1863) | Microsoft Networks' messenger service uses this protocol. |
| MULTICAST(IGMP:0) | Internet Group Multicast Protocol is used when sending packets to a specific group of hosts. |
| 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(ICMP:0) | 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:0) | 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. |
| 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. |

**Table 9-5 Predefined Services**

| SERVICE | DESCRIPTION |
|---|---|
| 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. |

## 9.9 Configuring Attack Alert

Attack alerts are the first defense against DOS attacks. In the **Attack Alert** screen, shown later, you may choose to generate an alert whenever an attack is detected. For DoS attacks, the LAN-Cell uses thresholds to determine when to drop sessions that do not become fully established. These thresholds apply globally to all sessions.

You can use the default threshold values, or you can change them to values more suitable to your security requirements.

### 9.9.1 Threshold Values

Tune these parameters when something is not working and after you have checked the firewall counters. These default values should work fine for normal small offices with ADSL bandwidth. 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.

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), then the default values should be reduced.
You should make any changes to the threshold values before you continue configuring firewall rules.

### 9.9.2 Half-Open Sessions

An unusually high number of half-open sessions (either an absolute number or measured as the arrival rate) could indicate that a Denial of Service attack is occurring. For TCP, "half-open" means that the session has not reached the established state-the TCP three-way handshake has not yet been completed (see *Figure 8-2*). For UDP, "half-open" means that the firewall has detected no return traffic.

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.

When the number of existing half-open sessions rises above a threshold (**max-incomplete high**), the LAN-Cell starts deleting half-open sessions as required to accommodate new connection requests. The LAN-Cell continues to delete half-open requests as necessary, until the number of existing half-open sessions drops below another threshold (**max-incomplete low**).

When the rate of new connection attempts rises above a threshold (**one-minute high**), the LAN-Cell starts deleting half-open sessions as required to accommodate new connection requests. The LAN-Cell continues to delete half-open sessions as necessary, until the rate of new connection attempts drops below another threshold (**one-minute low**). The rate is the number of new attempts detected in the last one-minute sample period.

### TCP Maximum Incomplete and Blocking Period

An unusually high number of half-open sessions with the same destination host address could indicate that a Denial of Service attack is being launched against the host.

Whenever the number of half-open sessions with the same destination host address rises above a threshold (**TCP Maximum Incomplete**), the LAN-Cell starts deleting half-open sessions according to one of the following methods:

1. If the **Blocking Period** timeout is 0 (the default), then the LAN-Cell deletes the oldest existing half-open session for the host for every new connection request to the host. This ensures that the number of half-open sessions to a given host will never exceed the threshold.
2. If the **Blocking Period** timeout is greater than 0, then the LAN-Cell blocks all new connection requests to the host giving the server time to handle the present connections. The LAN-Cell continues to block all new connection requests until the **Blocking Period** expires.

The LAN-Cell also sends alerts whenever **TCP Maximum Incomplete** is exceeded. The global values specified for the threshold and timeout apply to all TCP connections. Click the **Attack Alert** tab to bring up the next screen.

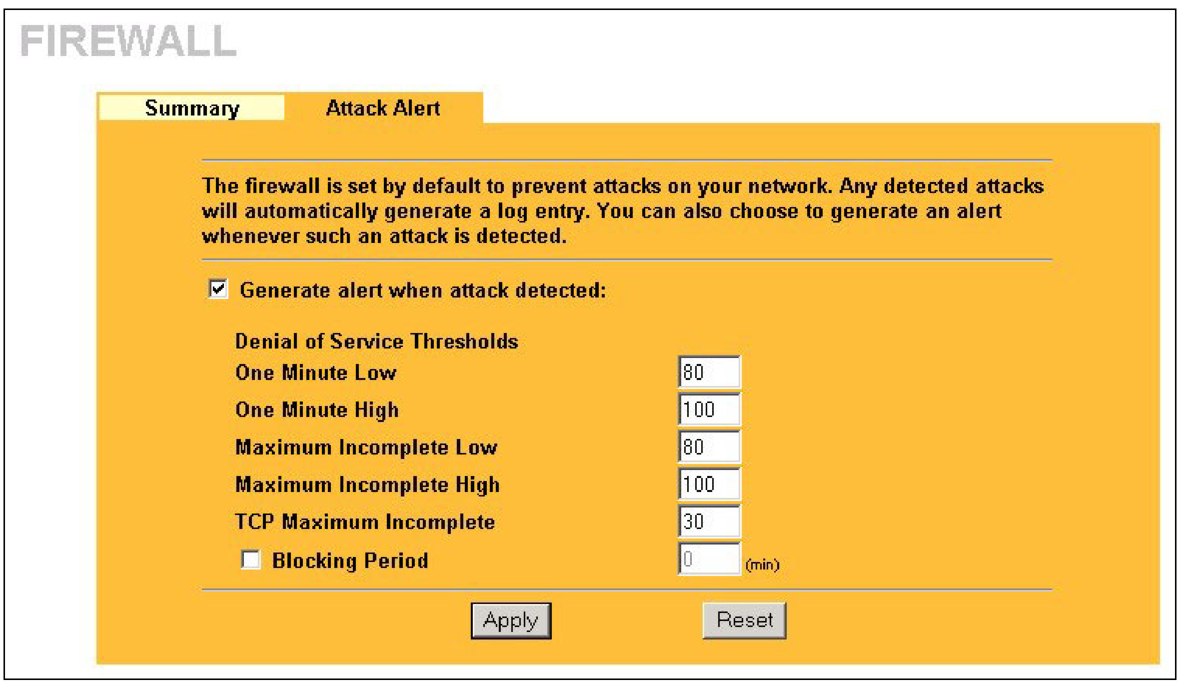



**Figure 9-12 Attack Alert**

The following table describes the fields in this screen.

**Table 9-6 Attack Alert**

| LABEL | DESCRIPTION | DEFAULT VALUES |
|---|---|---|
| Generate alert when attack detected | A detected attack automatically generates a log entry. Check this box to generate an alert (as well as a log) whenever an attack is detected. See the chapter on logs for more information on logs and alerts. | |
| Denial of Service Thresholds | | |
| One Minute Low | This is the rate of new half-open sessions 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. | 80 existing half-open sessions. |
| One Minute High | This is the rate of new half-open sessions that causes the firewall to start deleting half-open sessions. When the rate of new connection attempts rises above this number, the LAN-Cell deletes half-open sessions as required to accommodate new connection attempts. | 100 half-open sessions per minute. The above numbers cause the LAN-Cell to start deleting half-open sessions when more than 100 session establishment attempts have been detected in the last minute, and to stop deleting half-open sessions when fewer than 80 session establishment attempts have been detected in the last minute. |
| Maximum Incomplete Low | This is the number of existing half-open sessions that causes the firewall to stop deleting half-open sessions. The LAN-Cell continues to delete half-open requests as necessary, until the number of existing half-open sessions drops below this number. | 80 existing half-open sessions. |
| Maximum Incomplete High | This is the number of existing half-open sessions that causes the firewall to start deleting half-open sessions. When the number of existing half-open sessions rises above this number, the 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. | 100 existing half-open sessions. The above values causes the LAN-Cell to start deleting half-open sessions when the number of existing half-open sessions rises above 100, and to stop deleting half-open sessions with the number of existing half-open sessions drops below 80. |
| TCP Maximum Incomplete | This is the number of existing half-open TCP sessions with the same destination host IP address that causes the firewall to start dropping half-open sessions to that same destination host IP address. Enter a number between 1 and 256. As a general rule, you should choose a smaller number for a smaller network, a slower system or limited bandwidth. | 30 existing half-open TCP sessions. |
| Blocking Period | When **TCP Maximum Incomplete** is reached you can choose if the next session should be allowed or blocked. If you check **Blocking Period** any new sessions will be blocked for the length of time you specify in the next field (min) and all old incomplete sessions will be cleared during this period. If you want strong security, it is better to block the traffic for a short time, as it will give the server some time to digest the loading. | Select this check box to specify a number in minutes (min) text box. |
| (min) | Enter the length of **Blocking Period** in minutes. | 0 |
| Apply | Click **Apply** to save your changes back to the LAN-Cell. | |
| Reset | Click **Reset** to begin configuring this screen afresh. | |

# Chapter 10
# Content Filtering Screens

*This chapter provides a brief overview of content filtering using the web embedded configurator.*

## 10.1 Introduction to Content Filtering

Internet content filtering allows you to create and enforce Internet access policies tailored to their needs. Content filtering is the ability to block certain web features or specific URL keywords and should not be confused with packet filtering via SMT menu 21.1.

With content filtering, you can do the following:

### 10.1.1 Restrict Web Features

The LAN-Cell can block web features such as ActiveX controls, Java applets, cookies and disable web proxies.

### 10.1.2 Create a Filter List

You can select categories, such as pornography or racial intolerance, to block from a pre-defined list.

### 10.1.3 Filter Specific Web Sites

Your LAN-Cell can block or allow access to specific web sites based on their URLs or based on certain key words contained in web site content.

### 10.1.4 Days and Times

The LAN-Cell also allows you to define time periods and days during which the LAN-Cell performs content filtering.

## 10.2 General Content Filter Configuration

Click **CONTENT FILTER** and the screen will display as shown. Use this screen to enable content filtering, configure a schedule, and create a denial message. You can also choose specific computers to be included in or excluded from the content filtering configuration.

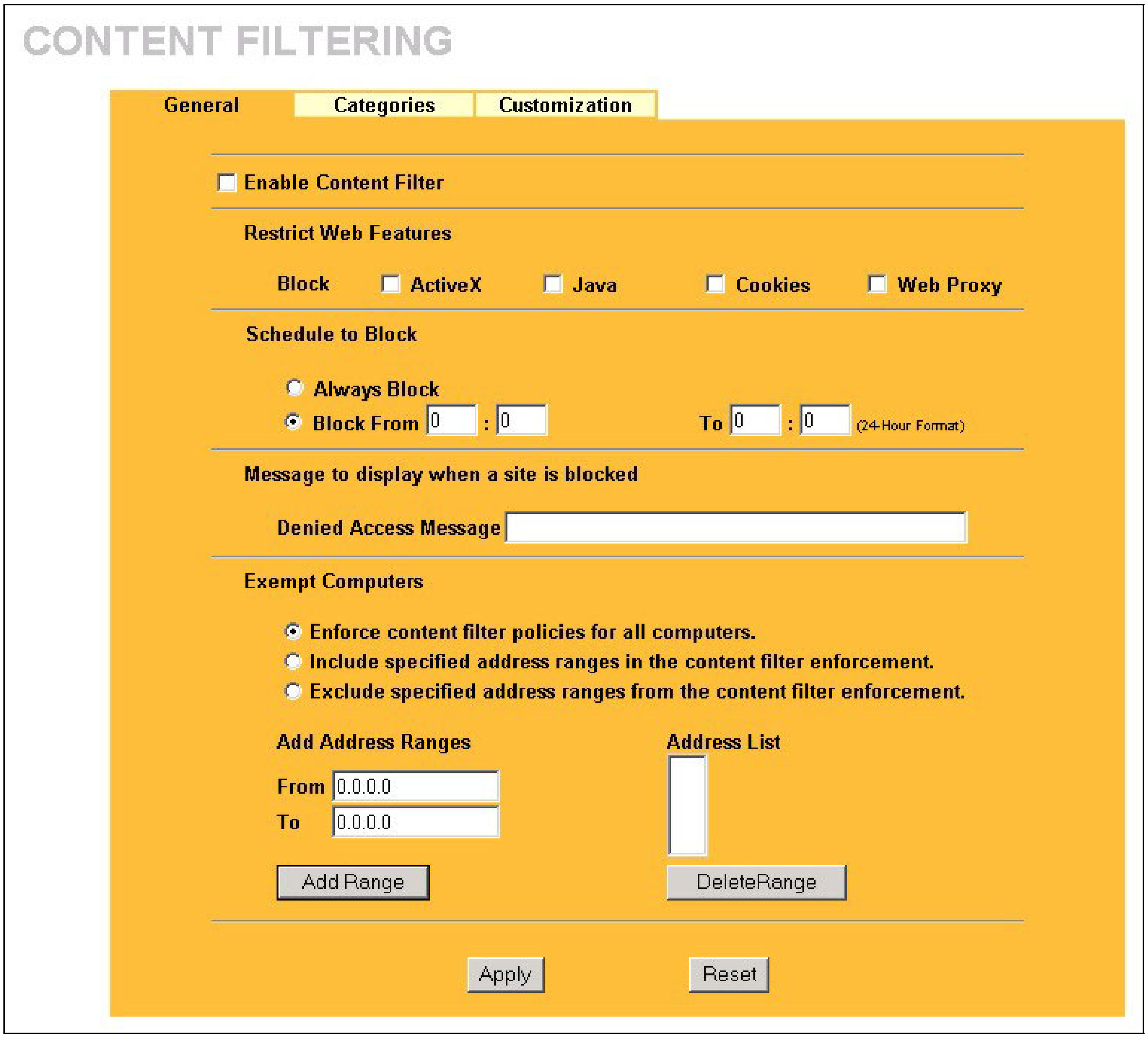



**Figure 10-1 Content Filter : General**

The following table describes the labels in this screen.

**Table 10-1 Content Filter : General**

| LABEL | DESCRIPTION |
|---|---|
| Enable Content Filter | Select this check box to enable the content filter. |
| Restrict Web Features : Select the check box(es) to restrict a feature. When you download a page containing a restricted feature, that part of the web page will appear blank or grayed out. | |
| Block<br>ActiveX | ActiveX is a tool for building dynamic and active web pages and distributed object applications. When you visit an ActiveX web site, ActiveX controls are downloaded to your browser, where they remain in case you visit the site again. |
| Java | Java is a programming language and development environment for building downloadable Web components or Internet and intranet business applications of all kinds. |
| Cookies | Cookies are files stored on a computer's hard drive. Some web servers use them to track usage and provide service based on ID. |
| Web Proxy | A server that acts as an intermediary between a user and the Internet to provide security, administrative control, and caching service. When a proxy server is located on the WAN it is possible for LAN users to circumvent content filtering by pointing to this proxy server. |

**Table 10-1 Content Filter : General**

| LABEL | DESCRIPTION |
|---|---|
| Schedule to Block : Content filtering scheduling applies to the Filter List, Customized sites and Keywords. Restricted web server data, such as ActiveX, Java, Cookies and Web Proxy are not affected. | |
| Always Block | Click this option button to have content filtering always active with Time of Day limitations not enforced. This is enabled by default. |
| Block From/To | Click this option button to have content filtering only active during the time interval specified. In the **Block From** and **To** fields, enter the time period, in 24-hour format, during which content filtering will be enforced. |
| Message to display when a site is blocked | |
| Denied Access Message | Enter a message to be displayed when a user tries to access a restricted web site. The default message is "Please contact your network administrator!!" |
| Exempt Computers | |
| Enforce content filter policies for all computers | Select this checkbox to have all users on your LAN follow content filter policies (default). |
| Include specified address ranges in the content filter | Select this checkbox to have a specific range of users on your LAN follow content filter policies. |
| Exclude specified address ranges from the content filter | Select this checkbox to exempt a specific range of users on your LAN from content filter policies. |
| Add Address Ranges | |
| From | Type the beginning IP address (in dotted decimal notation) of the specific range of users on your LAN. |
| To | Type the ending IP address (in dotted decimal notation) of the specific range of users on your LAN, then click **Add Range**. |
| Address List | This text field shows the address ranges that are blocked. |
| Add Range | Click **Add Range** after you have filled in the **From** and **To** fields above. |
| Delete Range | Click **Delete Range** after you select the range of addresses you wish to delete. |
| Apply | Click **Apply** to save your changes back to the LAN-Cell. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 10.3 Content Filtering with an External Server

Your LAN-Cell uses an application services company that provides outsourced content filtering. If you enable the content filter, your LAN-Cell will have access to an external database, which contains dynamically updated ratings of millions of web sites. This feature requires a separate subscription to the content filtering service; contact Proxicast for more information on subscribing to this service. The content filtering lookup process is described below.

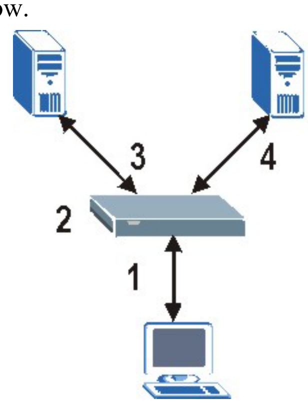



**Figure 10-2 Content Filtering Lookup Procedure**

**Step 1.** A computer sends an HTTP request to a web server.

**Step 2.** The LAN-Cell looks up the web site in its local database. If an attempt to access the web site was made in the past, a record of that web site's rating will be in the LAN-Cell's cache. The LAN-Cell will either block or forward the request based on the rating policy you configure.

If the LAN-Cell doesn't have a record of the web site, it will query the lookup server and simultaneously send the request to the web server.

**Step 3.** The lookup server sends the rating information back to the LAN-Cell, which then either forwards or blocks the web content. The web site address is then also stored in the LAN-Cell's content filtering cache.

## 10.4 Checking Content Filtering Activation

After you register for content filtering, the web site displays a registration successful web page. This does not mean the content filtering is active yet. You need to wait up to ten minutes for the content filtering to be activated.

Since there will be no activation notice, do the following:

**Step 1.** Go to your device's web configurator's **Content Filtering**, **Categories** screen.

**Step 2.** Select at least one category and click **Apply**.

**Step 3.** Enter a valid URL or IP address of a web site in the **Test if Web site is blocked** field and click the **Test Against Internet Server** button.
When content filtering is active, you should see an access blocked or access forwarded message. An error message displays if content filtering is not active.

## 10.5 Configuring Categories

To register for and configure category-based content filtering, click **CONTENT FILTER**, and then the **Categories** tab. The screen appears as shown.

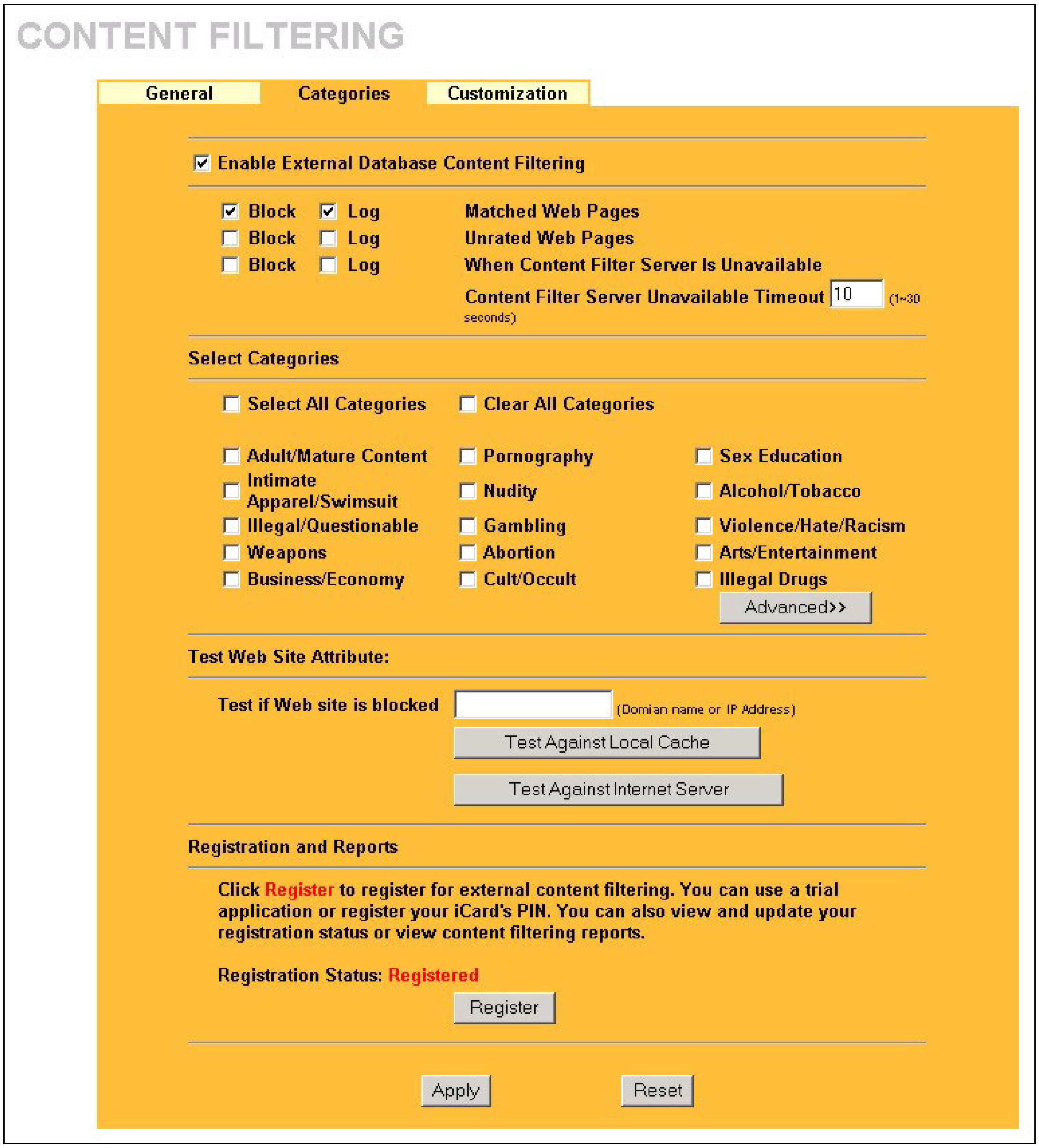



**Figure 10-3 Content Filter : Categories**

The following table describes the labels in this screen.

**Table 10-2 Content Filter : Categories**

| LABEL | DESCRIPTION |
|---|---|
| Enable Web Site Auto Categorization | Enable external database content filtering to have the LAN-Cell check an external database to find to which category a requested web page belongs. The LAN-Cell then blocks or forwards access to the web page depending on the configuration of the rest of this page. |
| Matched Web Pages | Select **Block** to prevent users from accessing web pages that match the categories that you select below.<br><br>When external database content filtering blocks access to a web page, it displays the denied access message that you configured in the **Content Filter General** screen along with the category of the blocked web page.<br><br>Select **Log** to record attempts to access prohibited web pages. |

**Table 10-2 Content Filter : Categories**

| LABEL | DESCRIPTION |
|---|---|
| Unrated Web Pages | Select **Block** to prevent users from accessing web pages that the external database content filtering has not categorized.<br>When the external database content filtering blocks access to a web page, it displays the denied access message that you configured in the **Content Filter General** screen along with the category of the blocked web page.<br>Select **Log** to record attempts to access web pages that are not categorized. |
| When Content Filter Server Is Unavailable | Select **Block** to block access to any requested web page if the external content filtering database is unavailable. The following are possible causes:<br>There is no response from the external content filtering server within the time period specified in the **Content Filter Server Unavailable Timeout** field.<br>The LAN-Cell is not able to resolve the domain name of the external content filtering database.<br>There is an error response from the external content filtering database (this can be caused by an expired content filtering registration).<br>Select **Log** to record attempts to access web pages that occur when the external content filtering database is unavailable. |
| Content Filter Server Unavailable Timeout | Specify a number of seconds (1 to 30) for the LAN-Cell to wait for a response from the external content filtering server. If there is still no response by the time this period expires, the LAN-Cell blocks or allows access to the requested web page based on the setting in the **Block When Content Filter Server Is Unavailable** field. |
| Select Categories | |
| Select All Categories | Select this check box to restrict access to all site categories listed below. |
| Clear All Categories | Select this check box to clear the selected categories below. |
| Adult/Mature Content | Selecting this category excludes pages that contain material of adult nature that does not necessarily contain excessive violence, sexual content, or nudity. These pages include very profane or vulgar content and pages that are not appropriate for children. |
| Pornography | Selecting this category excludes pages that contain sexually explicit material for the purpose of arousing a sexual or prurient interest. |
| Sex Education | Selecting this category excludes pages that provide graphic information (sometimes graphic) on reproduction, sexual development, safe sex practices, sexuality, birth control, and sexual development. It also includes pages that offer tips for better sex as well as products used for sexual enhancement. |
| Intimate Apparel/Swimsuit | Selecting this category excludes pages that contain images or offer the sale of swimsuits or intimate apparel or other types of suggestive clothing. It does not include pages selling undergarments as a subsection of other products offered. |
| Nudity | Selecting this category excludes pages containing nude or seminude depictions of the human body. These depictions are not necessarily sexual in intent or effect, but may include pages containing nude paintings or photo galleries of artistic nature. This category also includes nudist or naturist pages that contain pictures of nude individuals. |
| Alcohol/Tobacco | Selecting this category excludes pages that promote or offer the sale alcohol/tobacco products, or provide the means to create them. It also includes pages that glorify, tout, or otherwise encourage the consumption of alcohol/tobacco. It does not include pages that sell alcohol or tobacco as a subset of other products. |
| Illegal/Questionable | Selecting this category excludes pages that advocate or give advice on performing illegal acts such as service theft, evading law enforcement, fraud, burglary techniques and plagiarism. It also includes pages that provide or sell questionable educational materials, such as term papers. |

**Table 10-2 Content Filter : Categories**

| LABEL | DESCRIPTION |
|---|---|
| Gambling | Selecting this category excludes pages where a user can place a bet or participate in a betting pool (including lotteries) online. It also includes pages that provide information, assistance, recommendations, or training on placing bets or participating in games of chance. It does not include pages that sell gambling related products or machines. It also does not include pages for offline casinos and hotels (as long as those pages do not meet one of the above requirements). |
| Violence/Hate/Racism | Selecting this category excludes pages that depict extreme physical harm to people or property, or that advocate or provide instructions on how to cause such harm. It also includes pages that advocate, depict hostility or aggression toward, or denigrate an individual or group on the basis of race, religion, gender, nationality, ethnic origin, or other characteristics. |
| Weapons | Selecting this category excludes pages that sell, review, or describe weapons such as guns, knives or martial arts devices, or provide information on their use, accessories, or other modifications. It does not include pages that promote collecting weapons, or groups that either support or oppose weapons use. |
| Abortion | Selecting this category excludes pages that provide information or arguments in favor of or against abortion, describe abortion procedures, offer help in obtaining or avoiding abortion, or provide information on the effects, or lack thereof, of abortion. |
| Arts/Entertainment | Selecting this category excludes pages that promote and provide information about motion pictures, videos, television, music and programming guides, books, comics, movie theatres, galleries, artists or reviews on entertainment. |
| Business/Economy | Selecting this category excludes pages devoted to business firms, business information, economics, marketing, business management and entrepreneurship. This does not include pages that perform services that are defined in another category (such as Information Technology companies, or companies that sell travel services). |
| Cult/Occult | Selecting this category excludes pages that promote or offer methods, means of instruction, or other resources to affect or influence real events through the use of spells, curses, magic powers and satanic or supernatural beings. |
| Illegal Drugs | Selecting this category excludes pages that promote, offer, sell, supply, encourage or otherwise advocate the illegal use, cultivation, manufacture, or distribution of drugs, pharmaceuticals, intoxicating plants or chemicals and their related paraphernalia. |
| Education | Selecting this category excludes pages that offer educational information, distance learning and trade school information or programs. It also includes pages that are sponsored by schools, educational facilities, faculty, or alumni groups. |
| Cultural Institutions | Selecting this category excludes pages sponsored by cultural institutions, or those that provide information about museums, galleries, and theaters (not movie theaters). It includes groups such as 4H and the Boy Scouts of America. |
| Financial Services | Selecting this category excludes pages that provide or advertise banking services (online or offline) or other types of financial information, such as loans. It does not include pages that offer market information, brokerage or trading services. |
| Brokerage/Trading | Selecting this category excludes pages that provide or advertise trading of securities and management of investment assets (online or offline). It also includes insurance pages, as well as pages that offer financial investment strategies, quotes, and news. |
| Games | Selecting this category excludes pages that provide information and support game playing or downloading, video games, computer games, electronic games, tips, and advice on games or how to obtain cheat codes. It also includes pages dedicated to selling board games as well as journals and magazines dedicated to game playing. It includes pages that support or host online sweepstakes and giveaways. |
| Government/Legal | Selecting this category excludes pages sponsored by or which provide information on government, government agencies and government services such as taxation and emergency services. It also includes pages that discuss or explain laws of various governmental entities. |
| Military | Selecting this category excludes pages that promote or provide information on military branches or armed services. |

**Table 10-2 Content Filter : Categories**

| LABEL | DESCRIPTION |
|---|---|
| Political/Activist Groups | Selecting this category excludes pages sponsored by or which provide information on political parties, special interest groups, or any organization that promotes change or reform in public policy, public opinion, social practice, or economic activities. |
| Health | Selecting this category excludes pages that provide advice and information on general health such as fitness and well-being, personal health or medical services, drugs, alternative and complimentary therapies, medical information about ailments, dentistry, optometry, general psychiatry, self-help, and support organizations dedicated to a disease or condition. |
| Computers/Internet | Selecting this category excludes pages that sponsor or provide information on computers, technology, the Internet and technology-related organizations and companies. |
| Hacking/Proxy Avoidance | Pages providing information on illegal or questionable access to or the use of communications equipment/software, or provide information on how to bypass proxy server features or gain access to URLs in any way that bypasses the proxy server. |
| Search Engines/Portals | Selecting this category excludes pages that support searching the Internet, indices, and directories. |
| Web Communications | Selecting this category excludes pages that allow or offer Web-based communication via e-mail, chat, instant messaging, message boards, etc. |
| Job Search/Careers | Selecting this category excludes pages that provide assistance in finding employment, and tools for locating prospective employers. |
| News/Media | Selecting this category excludes pages that primarily report information or comments on current events or contemporary issues of the day. It also includes radio stations and magazines. It does not include pages that can be rated in other categories. |
| Personals/Dating | Selecting this category excludes pages that promote interpersonal relationships. |
| Reference | Selecting this category excludes pages containing personal, professional, or educational reference, including online dictionaries, maps, census, almanacs, library catalogues, genealogy-related pages and scientific information. |
| Chat/Instant Messaging | Selecting this category excludes pages that provide chat or instant messaging capabilities or client downloads. |
| Email | Selecting this category excludes pages offering web-based email services, such as online email reading, e-cards, and mailing list services. |
| Newsgroups | Selecting this category excludes pages that offer access to Usenet news groups or other messaging or bulletin board systems. |
| Religion | Selecting this category excludes pages that promote and provide information on conventional or unconventional religious or quasi-religious subjects, as well as churches, synagogues, or other houses of worship. It does not include pages containing alternative religions such as Wicca or witchcraft (Cult/Occult) or atheist beliefs (Political/Activist Groups). |
| Shopping | Selecting this category excludes pages that provide or advertise the means to obtain goods or services. It does not include pages that can be classified in other categories (such as vehicles or weapons). |
| Auctions | Selecting this category excludes pages that support the offering and purchasing of goods between individuals. This does not include classified advertisements. |
| Real Estate | Selecting this category excludes pages that provide information on renting, buying, or selling real estate or properties. |
| Society/Lifestyle | Selecting this category excludes pages providing information on matters of daily life. This does not include pages relating to entertainment, sports, jobs, sex or pages promoting alternative lifestyles such as homosexuality. Personal homepages fall within this category if they cannot be classified in another category. |
| Gay/Lesbian | Selecting this category excludes pages that provide information, promote, or cater to gay and lesbian lifestyles. This does not include pages that are sexually oriented. |

**Table 10-2 Content Filter : Categories**

| LABEL | DESCRIPTION |
|---|---|
| Restaurants/Dining/Food | Selecting this category excludes pages that list, review, discuss, advertise and promote food, catering, dining services, cooking and recipes. |
| Sports/Recreation/Hobbies | Selecting this category excludes pages that promote or provide information about spectator sports, recreational activities, or hobbies. This includes pages that discuss or promote camping, gardening, and collecting. |
| Travel | Selecting this category excludes pages that promote or provide opportunity for travel planning, including finding and making travel reservations, vehicle rentals, descriptions of travel destinations, or promotions for hotels or casinos. |
| Vehicles | Selecting this category excludes pages that provide information on or promote vehicles, boats, or aircraft, including pages that support online purchase of vehicles or parts. |
| Humor/Jokes | Selecting this category excludes pages that primarily focus on comedy, jokes, fun, etc. This may include pages containing jokes of adult or mature nature. Pages containing humorous Adult/Mature content also have an Adult/Mature category rating. |
| Streaming Media/MP3 | Selecting this category excludes pages that sell, deliver, or stream music or video content in any format, including pages that provide downloads for such viewers. |
| Software Downloads | Selecting this category excludes pages that are dedicated to the electronic download of software packages, whether for payment or at no charge. |
| Pay to Surf | Selecting this category excludes pages that pay users in the form of cash or prizes, for clicking on or reading specific links, email, or web pages. |
| For Kids | Selecting this category excludes pages designed specifically for children. |
| Web Advertisements | Selecting this category excludes pages that provide online advertisements or banners. This does not include advertising servers that serve adult-oriented advertisements. |
| Web Hosting | Selecting this category excludes pages of organizations that provide top-level domain pages, as well as web communities or hosting services. |
| Advanced/Basic | Click **Advanced** to see an expanded list of categories, or click **Basic** to see a smaller list. |
| Test Web Site Attribute | |
| Test if Web site is blocked | You can check whether or not the content filter currently blocks any given web page. Enter a web site address in the text box. |
| Test Against Local Cache | Click this button to test whether or not the web site above is saved in the LAN-Cell's database of restricted web pages. |
| Test Against Internet Server | Click this button to test whether or not the web site above is saved in the external content filter server's database of restricted web pages. |
| Registration and Reports | |
| Registration Status | This read-only field displays **Registered** if you have successfully registered the LAN-Cell for category-based content filtering (using an external database).<br>This field displays **Unregistered** if you have not successfully registered the LAN-Cell or your registration has expired.<br>**This field only displays whether or not you have successfully registered, not whether or not content filtering is active. See *section 10.4* for how to check the content filtering activation.** |

**Table 10-2 Content Filter : Categories**

| LABEL | DESCRIPTION |
|---|---|
| Register | Click **Register** to go to a web site where you can register for category-based content filtering (using an external database). Refer to the web site's on-line help for details.<br>**The web site displays a registration successful web page. It may take up to another ten minutes for content filtering to be activated. See *section 10.4* for how to check the content filtering activation.**<br>You can manage your registration status or view content filtering reports after you register this device.<br>You cannot access the web site if you have enabled content filtering in the **Content Filter General** screen and blocked access to web pages that use Java. |
| Apply | Click **Apply** to save your changes back to the LAN-Cell. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 10.6 Configuring Customization

To customize the content filter list by adding or removing specific sites from the filter list on your LAN-Cell, click **CONTENT FILTER**, then the **Customization** tab. The screen appears as shown.

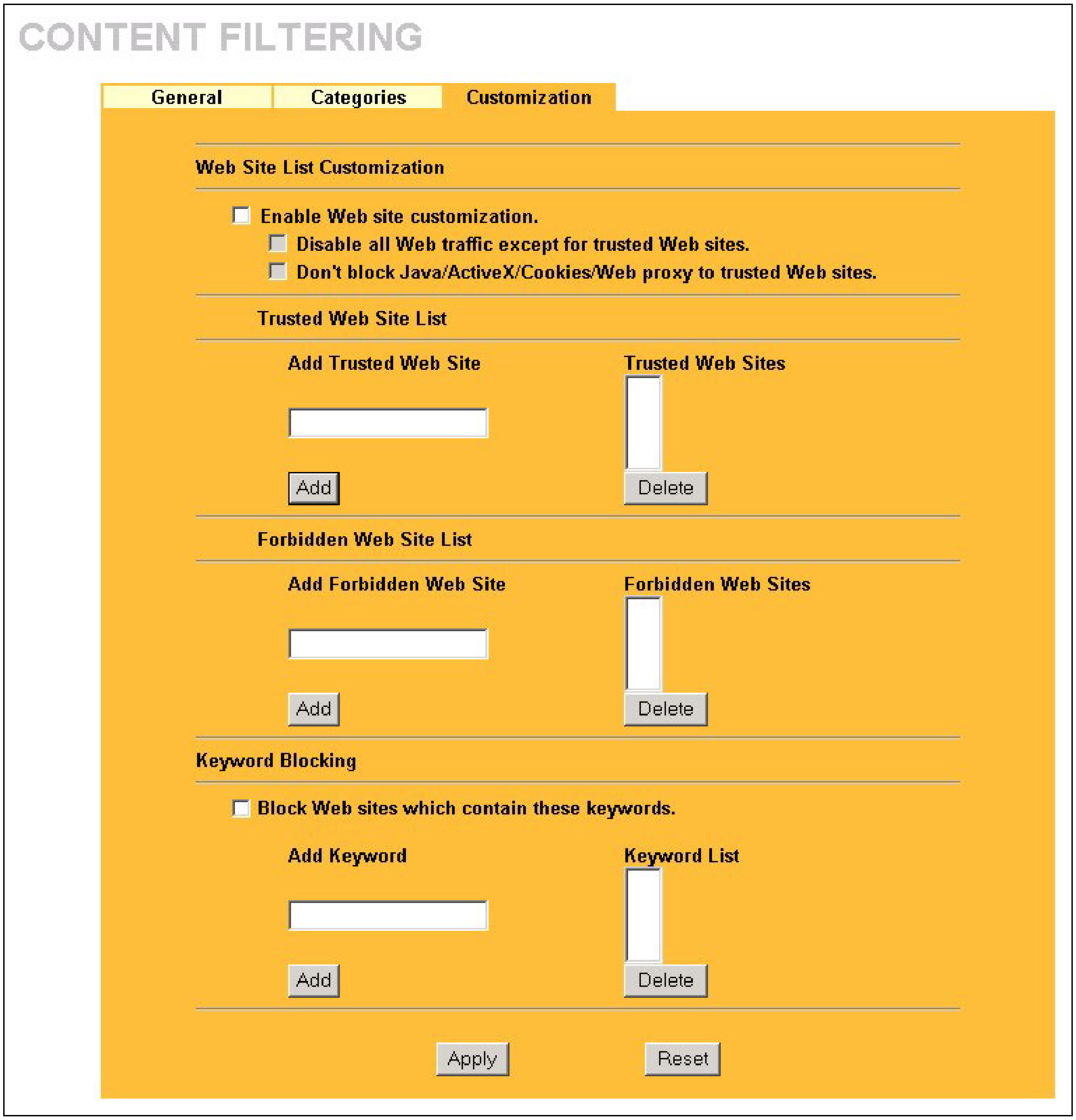



**Figure 10-4 Content Filter: Customization**

The following table describes the labels in this screen.

**Table 10-3 Content Filter : Customization**

| LABEL | DESCRIPTION |
|---|---|
| Web Site List Customization | |
| Enable Web site customization | Select this check box to allow **Trusted Domain** web sites and block **Forbidden Domain** web sites. Content filter list customization may be enabled and disabled without re-entering the site names. |
| Disable all Web traffic except for trusted Web sites | When this box is selected, the LAN-Cell only allows Web access to sites on the **Trusted Web Site** list. If they are chosen carefully, this is the most effective way to block objectionable material. |
| Don't block Java/ActiveX/Cookies/Web proxy to trusted Web sites | When this box is selected, the LAN-Cell will permit Java, ActiveX and Cookies from sites on the **Trusted Web Site** list to the LAN. In certain cases, it may be desirable to allow Java, ActiveX or Cookies from sites that are known and trusted. |

**Table 10-3 Content Filter : Customization**

| LABEL | DESCRIPTION |
|---|---|
| Trusted Web Site List | These are sites that you want to allow access to, regardless of their content rating, can be allowed by adding them to this list. You can enter up to 32 entries. |
| Add Trusted Web Site | Enter host names such as "www.good-site.com" into this text field. Do not enter the complete URL of the site – that is, do not include "http://". All subdomains are allowed. For example, entering "proxicast.com" also allows "www.proxicast.com", "partner.proxicast.com", "press.proxicast.com", etc. |
| Trusted Web Sites | This list displays the trusted web sites already added. |
| Add | Click this button when you have finished adding the host name in the text field above. |
| Delete | Select a web site name from the **Trusted Web Site List**, and then click this button to delete it from that list. |
| Forbidden Web Site List | Sites that you want to block access to, regardless of their content rating, can be allowed by adding them to this list. You can enter up to 32 entries. |
| Add Forbidden Web Site | Enter host names such as "www.bad-site.com" into this text field. Do not enter the complete URL of the site – that is, do not include "http://". All subdomains are allowed. For example, entering "bad-site.com" also blocks "www.bad-site.com", "partner.bad-site.com", "press.bad-site.com", etc. |
| Forbidden Web Sites | This list displays the forbidden web sites already added. |
| Add | Click this button when you have finished adding the host name in the text field above. |
| Delete | Select a web site name from the **Forbidden Web Site List**, and then click this button to delete it from that list. |
| Keyword Blocking | **Keyword Blocking** allows you to block websites that contain certain keywords. |
| Block Web sites which contain these keywords | Select this checkbox to enable keyword blocking. |
| Add Keyword | Enter a keyword to block. |
| Keyword List | This list displays the keywords already added. |
| Add | Click this button when you have finished adding the key words field above. |
| Delete | Select a keyword from the **Keyword List**, and then click this button to delete it from that list. |
| Apply | Click **Apply** to save your changes back to the LAN-Cell. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

# Part VI:

## VPN/IPSec

This part provides information on how to configure VPN/IPSec.

# Chapter 11
# Introduction to IPSec

*This chapter introduces the basics of IPSec VPNs.*

## 11.1 VPN Overview

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

### 11.1.1 IPSec

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

### 11.1.2 Security Association

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

### 11.1.3 Other Terminology

- **Encryption**

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

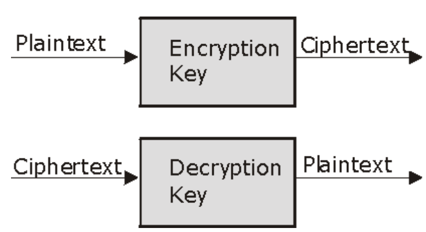



**Figure 11-1 Encryption and Decryption**

- **Data Confidentiality**

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

- **Data Integrity**

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

- **Data Origin Authentication**

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

### 11.1.4 VPN Applications

The LAN-Cell supports the following VPN applications.

- **Linking Two or More Private Networks Together**

  Connect branch offices and business partners over the Internet with significant cost savings and improved performance when compared to leased lines between sites.

- **Accessing Network Resources When NAT Is Enabled**

  When NAT is enabled, remote users are not able to access hosts on the LAN unless the host is designated a public LAN server for that specific protocol. Since the VPN tunnel terminates inside the LAN, remote users will be able to access all computers that use private IP addresses on the LAN.

- **Unsupported IP Applications**

  A VPN tunnel may be created to add support for unsupported emerging IP applications. See the chapter on *Getting to Know Your LAN-Cell* for an example of a VPN application.

## 11.2 IPSec Architecture

The overall IPSec architecture is shown as follows.

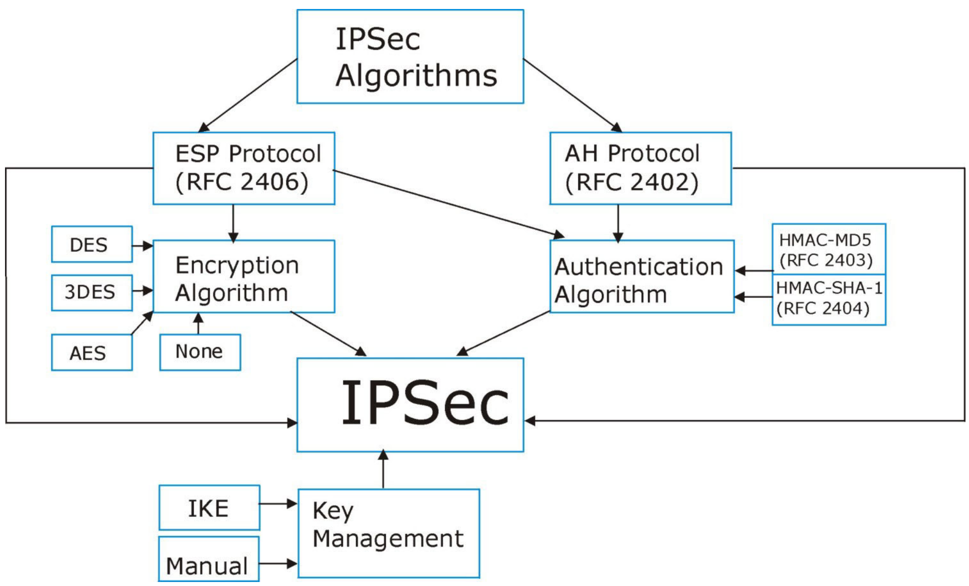



**Figure 11-2 IPSec Architecture**

### 11.2.1 IPSec Algorithms

The **ESP** (Encapsulating Security Payload) Protocol (RFC 2406) and **AH** (Authentication Header) protocol (RFC 2402) describe the packet formats and the default standards for packet structure (including implementation algorithms).

The Encryption Algorithm describes the use of encryption techniques such as DES (Data Encryption Standard) and Triple DES algorithms.

The Authentication Algorithms, HMAC-MD5 (RFC 2403) and HMAC-SHA-1 (RFC 2404, provide an authentication mechanism for the **AH** and **ESP** protocols. Please see *12.2* for more information.

### 11.2.2 Key Management

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

## 11.3 Encapsulation

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

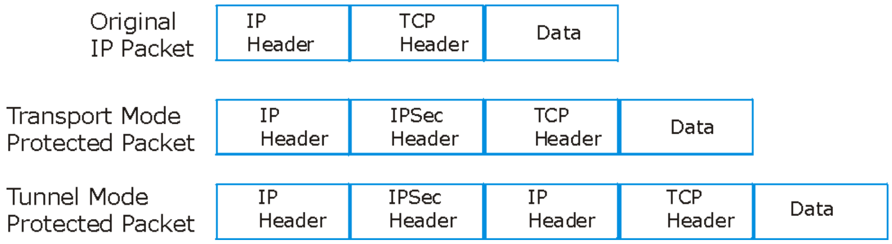



**Figure 11-3 Transport and Tunnel Mode IPSec Encapsulation**

### 11.3.1 Transport Mode

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

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

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

### 11.3.2 Tunnel Mode

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

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

## 11.4 IPSec and NAT

Read this section if you are running IPSec on a host computer behind the LAN-Cell.

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

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

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

**Tunnel** mode **ESP** with authentication is compatible with NAT because integrity checks are performed over the combination of the "original header plus original payload," which is unchanged by a NAT device. **Transport** mode **ESP** with authentication is not compatible with NAT, although NAT traversal provides a way to use **Transport** mode **ESP** when there is a NAT router between the IPSec endpoints (see *section 12.7* for details).

**Table 11-1 VPN and NAT**

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

# Chapter 12
# VPN Screens

*This chapter introduces the VPN Web configurator. See the Logs chapter for information on viewing logs and the appendix for IPSec log descriptions.*

## 12.1 VPN/IPSec Overview

Use the screens documented in this chapter to configuring and managing a VPN connection.

## 12.2 IPSec Algorithms

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

### 12.2.1 AH (Authentication Header) Protocol

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

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

### 12.2.2 ESP (Encapsulating Security Payload) Protocol

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

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

**Table 12-1 AH and ESP**

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

## 12.3 My IP Address

**My IP Address** is the WAN IP address of the LAN-Cell. The LAN-Cell has to rebuild the VPN tunnel if the **My IP Address** changes after setup.

The following applies if this field is configured as **0.0.0.0**:

- The LAN-Cell uses the current LAN-Cell WAN IP address (static or dynamic) to set up the VPN tunnel.
- If the WAN connection goes down, the LAN-Cell uses the Cellular Modem IP address for the VPN tunnel when using Cellular Modem fail-over or the LAN IP address when using traffic redirect. See the chapter on WAN for details on Cellular Modem fail-over and traffic redirect.

## 12.4 Secure Gateway Address

**Secure Gateway Address** is the WAN IP address or domain name of the remote IPSec router (secure gateway).

If the remote secure gateway has a static WAN IP address, enter it in the **Secure Gateway Address** field. You may alternatively enter the remote secure gateway's domain name (if it has one) in the **Secure Gateway Address** field.

You can also enter a remote secure gateway's domain name in the **Secure Gateway Address** field if the remote secure gateway has a dynamic WAN IP address and is using DDNS. The LAN-Cell has to rebuild the VPN tunnel each time the remote secure gateway's WAN IP address changes (there may be a delay until the DDNS servers are updated with the remote gateway's new WAN IP address).

### 12.4.1 Dynamic Secure Gateway Address

If the remote secure gateway has a dynamic WAN IP address and does not use DDNS, enter 0.0.0.0 as the secure gateway's address. In this case only the remote secure gateway can initiate SAs.

**The Secure Gateway IP Address may be configured as 0.0.0.0 only when using** IKE **key management and not** Manual **key management.**

## 12.5 Summary Screen

The following figure helps explain the main fields in the web configurator.

Local and remote IP addresses must be static.

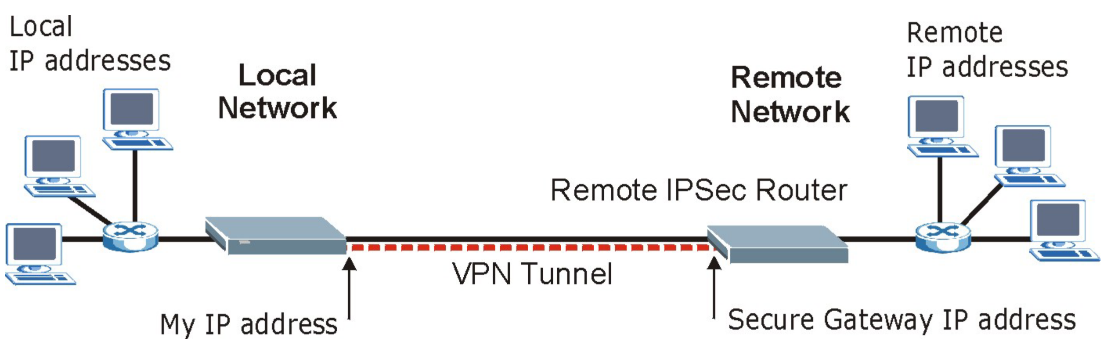



**Figure 12-1 IPSec Summary Fields**

Click **VPN** to open the **VPN Rules** screen. This is a read-only menu of your IPSec rules (tunnels). Edit or create an IPSec rule by selecting an index number and then clicking **Edit** to configure the associated submenus.

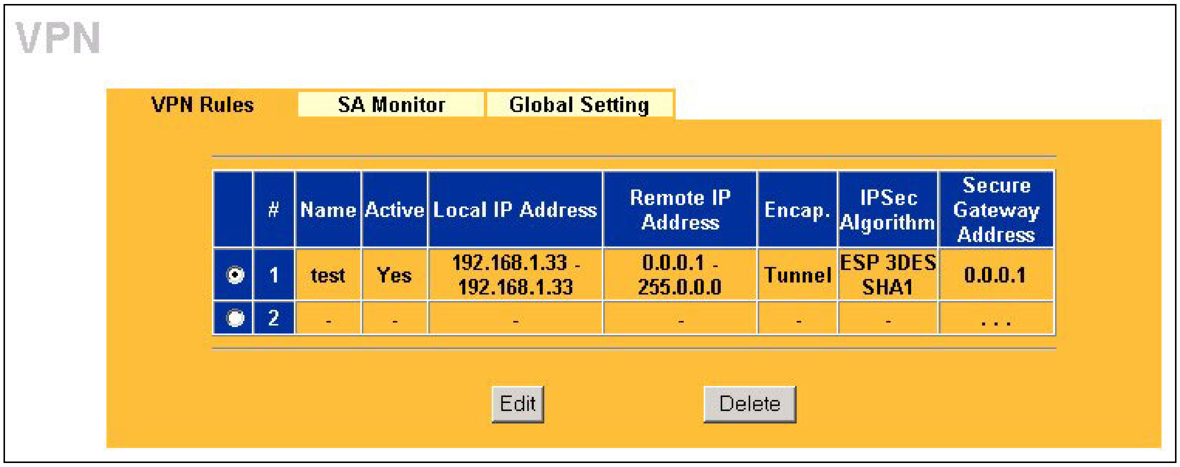



**Figure 12-2 VPN Rules**

The following table describes the fields in this screen.

**Table 12-2 VPN Rules**

| LABEL | DESCRIPTION |
|---|---|
| # | This field displays the VPN rule number. |
| Name | This field displays the identification name for this VPN policy. |
| Active | **Y** signifies that this VPN rule is active. |
| Local IP Address | This is the IP address(es) of computer(s) on your local network behind your LAN-Cell.<br>The same (static) IP address is displayed twice when the **Local Address Type** field in the **Edit VPN Rule** (or **Manual Key**) screen is configured to **Single Address**.<br>The beginning and ending (static) IP addresses, in a range of computers are displayed when the **Local Address Type** field in the **Edit VPN Rule** (or **Manual Key**) screen is configured to **Range Address**.<br>A (static) IP address and a subnet mask are displayed when the **Local Address Type** field in the **Edit VPN Rule** (or **Manual Key**) screen is configured to **Subnet Address**. |
| Remote IP Address | This is the IP address(es) of computer(s) on the remote network behind the remote IPSec router.<br>This field displays **N/A** when the **Secure Gateway Address** field displays **0.0.0.0**. In this case only the remote IPSec router can initiate the VPN.<br>The same (static) IP address is displayed twice when the **Remote Address Type** field in the **Edit VPN Rule** (or **Manual Key**) screen is configured to **Single Address**.<br>The beginning and ending (static) IP addresses, in a range of computers are displayed when the **Remote Address Type** field in the **Edit VPN Rule** (or **Manual Key**) screen is configured to **Range Address**.<br>A (static) IP address and a subnet mask are displayed when the **Remote Address Type** field in the **Edit VPN Rule** (or **Manual Key**) 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.<br>Both **AH** and **ESP** increase LAN-Cell processing requirements and communications latency (delay). |
| Secure Gateway Address | This is the static WAN IP address or URL of the remote IPSec router. This field displays **0.0.0.0** when you configure the **Secure Gateway Address** field in the **Edit VPN Rule** screen to **0.0.0.0.** |
| Edit | Click **Edit** to edit the VPN policy. |
| Delete | Click **Delete** to remove the VPN policy. |

## 12.6 Keep Alive

When you initiate an IPSec tunnel with keep alive enabled, the LAN-Cell automatically renegotiates the tunnel when the IPSec SA lifetime period expires (see *section 12.13* for more on the IPSec SA lifetime). In effect, the IPSec tunnel becomes an "always on" connection after you initiate it. Both IPSec routers must have a LAN-Cell-compatible keep alive feature enabled in order for this feature to work.

If the LAN-Cell has its maximum number of simultaneous IPSec tunnels connected to it and they all have keep alive enabled, then no other tunnels can take a turn connecting to the LAN-Cell because the LAN-Cell never drops the tunnels that are already connected. Your LAN-Cell model can support 5 simultaneous IPSec SAs.

**When there is outbound traffic with no inbound traffic, the LAN-Cell automatically drops the tunnel after two minutes.**

## 12.7 NAT Traversal

NAT traversal allows you to set up a VPN connection when there are NAT routers between IPSec routers A and B.


**Figure 12-3 NAT Router Between IPSec Routers**

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

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

### 12.7.1 NAT Traversal Configuration

For NAT traversal to work you must:

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

In order for IPSec router A (see the figure) to receive an initiating IPSec packet from IPSec router B, set the NAT router to forward UDP port 500 to IPSec router A.

### 12.7.2 X-Auth (Extended Authentication)

Extended authentication provides added security by allowing you to use usernames and passwords for VPN connections. This is especially helpful when multiple LAN-Cells use one VPN rule to connect to a single LAN-Cell. An attacker cannot make a VPN connection without a valid username and password.

The extended authentication server checks the user names and passwords of the extended authentication clients before completing the IPSec connection (see also the *Authentication Server* section).

A LAN-Cell can be an extended authentication server for some VPN connections and an extended authentication client for other VPN connections.

### 12.7.3 Remote DNS Server

In cases where you want to use domain names to access Intranet servers on a remote 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 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. In order to access computers that use private domain names on the headquarters (HQ) network, the LAN-Cell at branch office 1 uses the Intranet DNS server in headquarters. The DNS server feature for VPN does not work with Windows 2000 or Windows XP

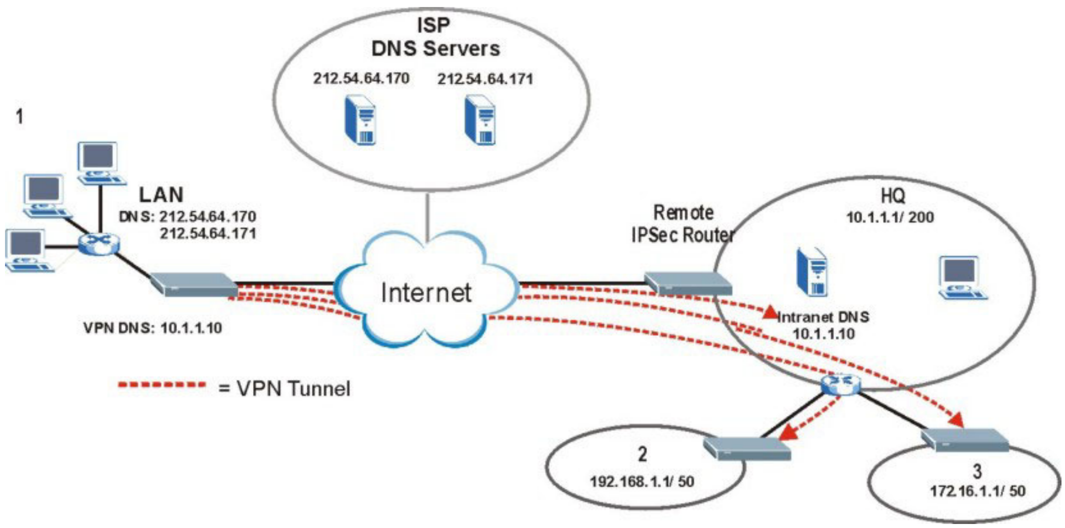



**Figure 12-4 VPN Host using Intranet DNS Server Example**

**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 network.**

## 12.8 ID Type and Content

With aggressive negotiation mode (see *section 12.12.1*), the LAN-Cell identifies incoming SAs by ID type and content since this identifying information is not encrypted. This enables the LAN-Cell to distinguish between multiple rules for SAs that connect from remote IPSec routers that have dynamic WAN IP addresses. Telecommuters can use separate passwords to simultaneously connect to the LAN-Cell from IPSec routers with dynamic IP addresses (see *section 12.18.2* for a telecommuter configuration example).

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

With main mode (see *section 12.12.2*), the ID type and content are encrypted to provide identity protection. In this case the LAN-Cell can only distinguish between up to 12 different incoming SAs that connect from remote IPSec routers that have dynamic WAN IP addresses. The LAN-Cell can distinguish up to 12 incoming SAs because you can select between three encryption algorithms (DES, 3DES and AES), two authentication algorithms (MD5 and SHA1) and two key groups (DH1 and DH2) when you configure a VPN rule (see *section 12.10*). The ID type and content act as an extra level of identification for incoming SAs.

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

**Table 12-3 Local ID Type and Content Fields**

| LOCAL ID TYPE= | CONTENT= |
|---|---|
| IP | Type the IP address of your computer or leave the field blank to have the LAN-Cell automatically use its own IP address. |

**Table 12-3 Local ID Type and Content Fields**

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

**Table 12-4 Peer ID Type and Content Fields**

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

## 12.8.1 ID Type and Content Examples

Two IPSec routers must have matching ID type and content configuration in order to set up a VPN tunnel.

The two LAN-Cells in this example can complete negotiation and establish a VPN tunnel.

**Table 12-5 Matching ID Type and Content Configuration Example**

| LAN-CELL A | LAN-CELL B |
|---|---|
| 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 |

The two LAN-Cells in this example cannot complete their negotiation because LAN-Cell B's **Local ID type** is **IP**, but LAN-Cell A's **Peer ID type** is set to **E-mail**. An "ID mismatched" message displays in the IPSEC LOG.

**Table 12-6 Mismatching ID Type and Content Configuration Example**

| LAN-CELL A | LAN-CELL B |
|---|---|
| Local ID type: IP | **Local ID type: IP** |
| Local ID content: 1.1.1.10 | Local ID content: 1.1.1.10 |
| **Peer ID type: E-mail** | Peer ID type: IP |
| Peer ID content: aa@yahoo.com | Peer ID content: N/A |

## 12.9 Pre-Shared Key

A pre-shared key identifies a communicating party during a phase 1 IKE negotiation (see *section 12.10* for more on IKE phases). It is called "pre-shared" because you have to share it with another party before you can communicate with them over a secure connection.

## 12.10 VPN Implementation

### 12.10.1 Client to Site VPN

A client to site VPN tunnel connects a single computer behind an IPSec router to a group of computers behind the remote IPSec router.

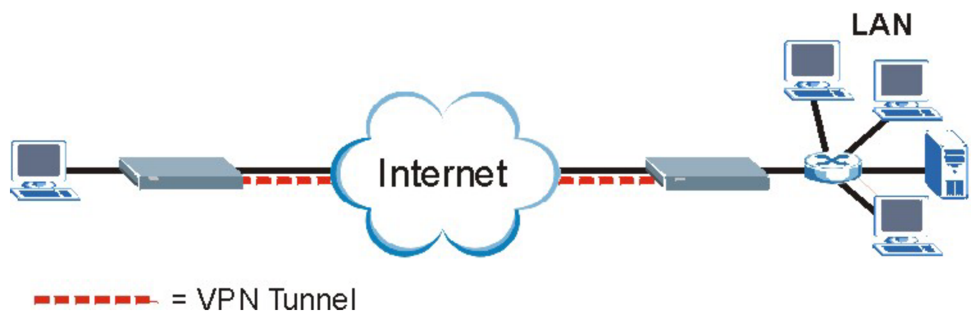



**Figure 12-5 Client-to-Site VPN Example**

### 12.10.2 Site to site VPN

A site to site VPN tunnel connects group of computers behind an IPSec router to a group of computers behind the remote IPSec router.

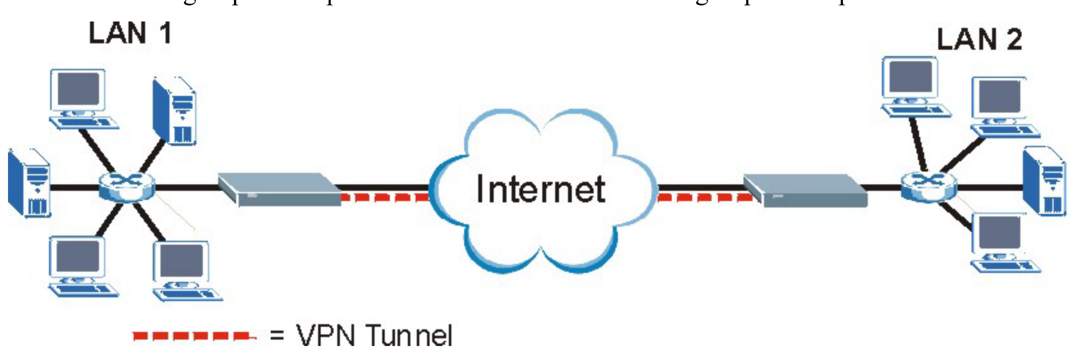



**Figure 12-6 Site-to-Site VPN Example**

## 12.11 Configuring Basic IKE VPN Rule Setup

Select one of the VPN rules in the **VPN Rules** screen and click **Edit** or click the **Rule Setup** tab on the LAN-Cell to configure the rule's settings. The basic IKE rule setup screen is shown next.

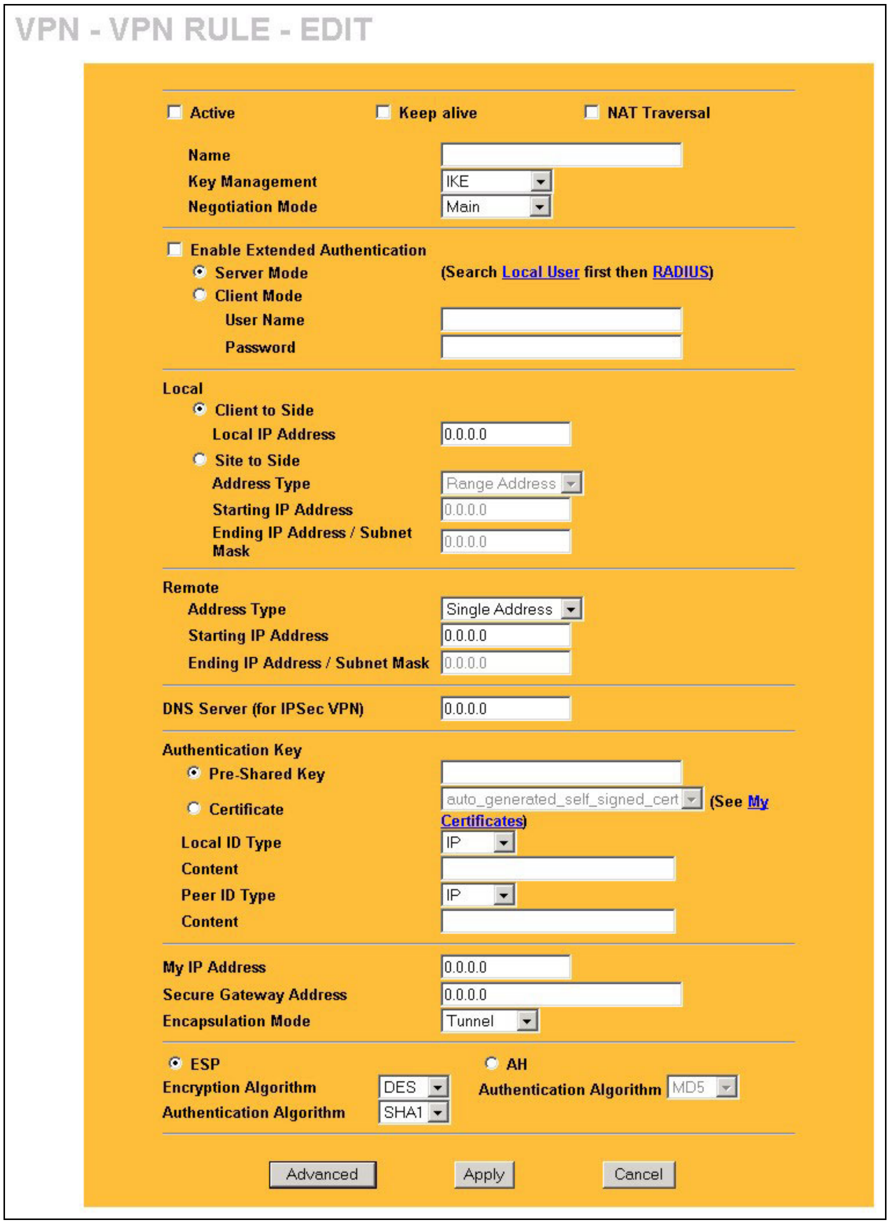



**Figure 12-7 Basic IKE VPN Rule Edit**

The following table describes the fields in this screen.

**Table 12-7 Basic IKE VPN Rule Edit**

| LABEL | DESCRIPTION |
|---|---|
| Active | Select this check box to activate this VPN tunnel. This option determines whether a VPN rule is applied before a packet leaves the firewall. |
| Keep Alive | Select this check box to turn on the keep alive feature for this SA.<br><br>Turn on Keep Alive to have the LAN-Cell automatically reinitiate the SA after the SA lifetime times out, even if there is no traffic. The remote IPSec router must also have keep alive enabled in order for this feature to work. |

**Table 12-7 Basic IKE VPN Rule Edit**

| 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.<br>The remote IPSec router must also have NAT traversal enabled.<br>You can use NAT traversal with **ESP** protocol using **Transport** or **Tunnel** mode, but not with **AH** protocol nor with manual key management. In order for an IPSec router behind a NAT router to receive an initiating IPSec packet, set the NAT router to forward UDP port 500 to the IPSec router behind the NAT router. |
| 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. |
| Key Management (or IPSec Keying Mode) | Select **IKE** or **Manual Key** from the drop-down list box. **IKE** provides more protection so it is generally recommended. **Manual Key** is a useful option for troubleshooting. |
| 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. |
| 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.<br>You must also configure the extended authentication clients' usernames and passwords in the auth server's local user database or a RADIUS server (see the *Authentication Server* section).<br>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.<br>During authentication, if the extended authentication server 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 external extended authentication server. 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. |
| 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. |

**Table 12-7 Basic IKE VPN Rule Edit**

| LABEL | DESCRIPTION |
|---|---|
| Local:<br>Local IP addresses must be static and correspond to the remote IPSec router's configured remote IP addresses.<br>Two active SAs can have the same configured 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.<br>In order to have more than one active rule with the **Secure Gateway Address** field set to **0.0.0.0**, the ranges of the local IP addresses cannot overlap between rules.<br>If you configure an active rule with **0.0.0.0** in the **Secure 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 **Secure Gateway Address** field set to **0.0.0.0**. | |
| Client to Site | Select this radio button to build a client to site VPN connection. |
| Local IP Address | Enter a static local IP address. The local IP address must correspond to the remote IPSec router's configured remote IP addresses. |
| Site to Site | Select this radio button to establish a VPN between two sites (groups of IP addresses). |
| Address Type | Use the drop-down menu to choose **Range Address** or **Subnet 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 **Range Address**, enter the beginning (static) IP address, in a range of computers on your 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 **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:<br>Remote IP addresses must be static and correspond to the remote IPSec router's configured local IP addresses. The remote fields do not apply when the **Secure Gateway Address** field is configured to **0.0.0.0**. In this case only the remote IPSec router can initiate the VPN.<br>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 menu 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. |

**Table 12-7 Basic IKE VPN Rule Edit**

| LABEL | DESCRIPTION |
| --- | --- |
| 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. |
| DNS Server (for IPSec VPN) | If there is a private DNS server that services the VPN, type its IP address here. The LAN-Cell assigns this additional DNS server to the LAN-Cell's DHCP clients that have IP addresses in this IPSec rule's range of local addresses.<br>A DNS server allows clients on the VPN to find other computers and servers on the VPN by their (private) domain names. |
| 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.<br>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.<br>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.<br>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.<br>Select **DNS** to identify this LAN-Cell by a domain name.<br>Select **E-mail** to identify this LAN-Cell by an e-mail address.<br>You do not configure the local ID type and content when you set **Authentication Method** 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 IP Address** field (refer to the **My IP Address** field description) if you configure the local **Content** field to **0.0.0.0** or leave it blank.<br>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.<br>➢ When there is a NAT router between the two IPSec routers.<br>➢ 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.<br>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. |

**Table 12-7 Basic IKE VPN Rule Edit**

<table>
<tr><th>LABEL</th><th>DESCRIPTION</th></tr>
<tr><td>Peer ID Type</td><td>Select from the following when you set Authentication Method to Pre-shared Key.<br>➢ Select IP to identify the remote IPSec router by its IP address.<br>➢ Select DNS to identify the remote IPSec router by a domain name.<br>➢ Select E-mail to identify the remote IPSec router by an e-mail address.<br>Select from the following when you set Authentication Method to Certificate.<br>➢ 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.<br>➢ 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.<br>➢ 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.<br>➢ Select Subject Name to identify the remote IPSec router by the subject name of the certificate it uses for this VPN connection.<br>➢ Select Any to have the LAN-Cell not check the remote IPSec router's ID.</td></tr>
<tr><td>Content</td><td>The configuration of the peer content depends on the peer ID type.<br>Do the following when you set Authentication Method to Pre-shared Key.<br>➢ 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 Secure Gateway Address field (refer to the Secure Gateway Address field description).<br>➢ 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.<br>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:<br>➢ When there is a NAT router between the two IPSec routers.<br>➢ When you want the LAN-Cell to distinguish between VPN connection requests that come in from remote IPSec routers with dynamic WAN IP addresses.<br>Do the following when you set Authentication Method to Certificate.<br>➢ 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 Secure Gateway Address field (refer to the Secure Gateway Address field description).<br>➢ 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.<br>➢ For Subject Name, type the subject name of the certificate the remote IPSec router will use for this VPN connection.<br>➢ For Any, the peer Content field is not available.<br>Regardless of how you configure the ID Type and Content fields, two active SAs cannot have both the local and remote IP address ranges overlap between rules.</td></tr>
</table>

**Table 12-7 Basic IKE VPN Rule Edit**

| LABEL | DESCRIPTION |
|---|---|
| My IP Address | Enter the WAN IP address of your LAN-Cell. The VPN tunnel has to be rebuilt if this IP address changes.<br>The following applies if this field is configured as **0.0.0.0**:<br>➢ The LAN-Cell uses the current LAN-Cell WAN IP address (static or dynamic) to set up the VPN tunnel.<br>➢ If the WAN connection goes down, the LAN-Cell uses the Cellular Modem IP address for the VPN tunnel when using Cellular Modem fail-over or the LAN IP address when using traffic redirect. See the chapter on WAN for details on Cellular Modem and traffic redirect. |
| Secure Gateway Address | Type the WAN IP address or the URL (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 (the **Key Management** (or **IPSec Keying Mode**) field must be set to **IKE**).<br>In order to have more than one active rule with the **Secure Gateway Address** field set to **0.0.0.0**, the ranges of the local IP addresses cannot overlap between rules.<br>If you configure an active rule with **0.0.0.0** in the **Secure 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 **Secure Gateway Address** field set to **0.0.0.0**. |
| Encapsulation Mode | Select **Tunnel** mode or **Transport** mode from the drop-down list box. |
| ESP | 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 below). |
| Encryption Algorithm | Select **DES**, **3DES**, **AES** or **NULL** from the drop-down list box.<br>When you use one of these encryption algorithms for data communications, both the sending device and the receiving device must use 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**.<br>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. |
| AH | 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 below). |
| 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. |

**Table 12-7 Basic IKE VPN Rule Edit**

| LABEL | DESCRIPTION |
|---|---|
| Advanced | Click **Advanced** to configure more detailed settings of your IKE key management. |
| Apply | Click **Apply** to save your customized settings and exit this screen. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 12.12 IKE Phases

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

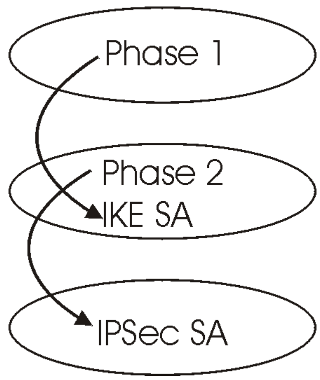



**Figure 12-8 Two Phases to Set Up the IPSec SA**

In phase 1 you must:

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

In phase 2 you must:

- Choose which protocol to use (**ESP** or **AH**) for the IKE key exchange.
- Choose an encryption algorithm.
- Choose an authentication algorithm
- Choose whether to enable Perfect Forward Secrecy (PFS) using Diffie-Hellman public-key cryptography – see *section 12.12.5*.
- Choose **Tunnel** mode or **Transport** mode.
- Set the IPSec SA lifetime. This field allows you to determine how long the IPSec SA should stay up before it times out. The LAN-Cell automatically renegotiates the IPSec SA if there is traffic when the IPSec SA lifetime period expires. The LAN-Cell also automatically renegotiates the IPSec SA if both IPSec routers have keep alive enabled, even if there is no traffic. If an IPSec SA times out, then the IPSec router must renegotiate the SA the next time someone attempts to send traffic.

### 12.12.1 X-Auth and IKE

X-Auth (Extended Authentication) inserts a new exchange between IKE phases 1 and 2 for client authentication.

### 12.12.2 Negotiation Mode

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

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

### 12.12.3 Pre-Shared Key

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

### 12.12.4 Diffie-Hellman (DH) Key Groups

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

### 12.12.5 Perfect Forward Secrecy (PFS)

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

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

## 12.13 Configuring Advanced IKE Setup

Select one of the VPN rules in the **VPN Rules** screen and click **Edit** to configure the rule's settings. The basic IKE rule setup screen opens

Set the **Key Management** (or **IPSec Keying Mode**) field to **IKE** and click the **Advanced** button to display the advanced IKE VPN rule setup screen.

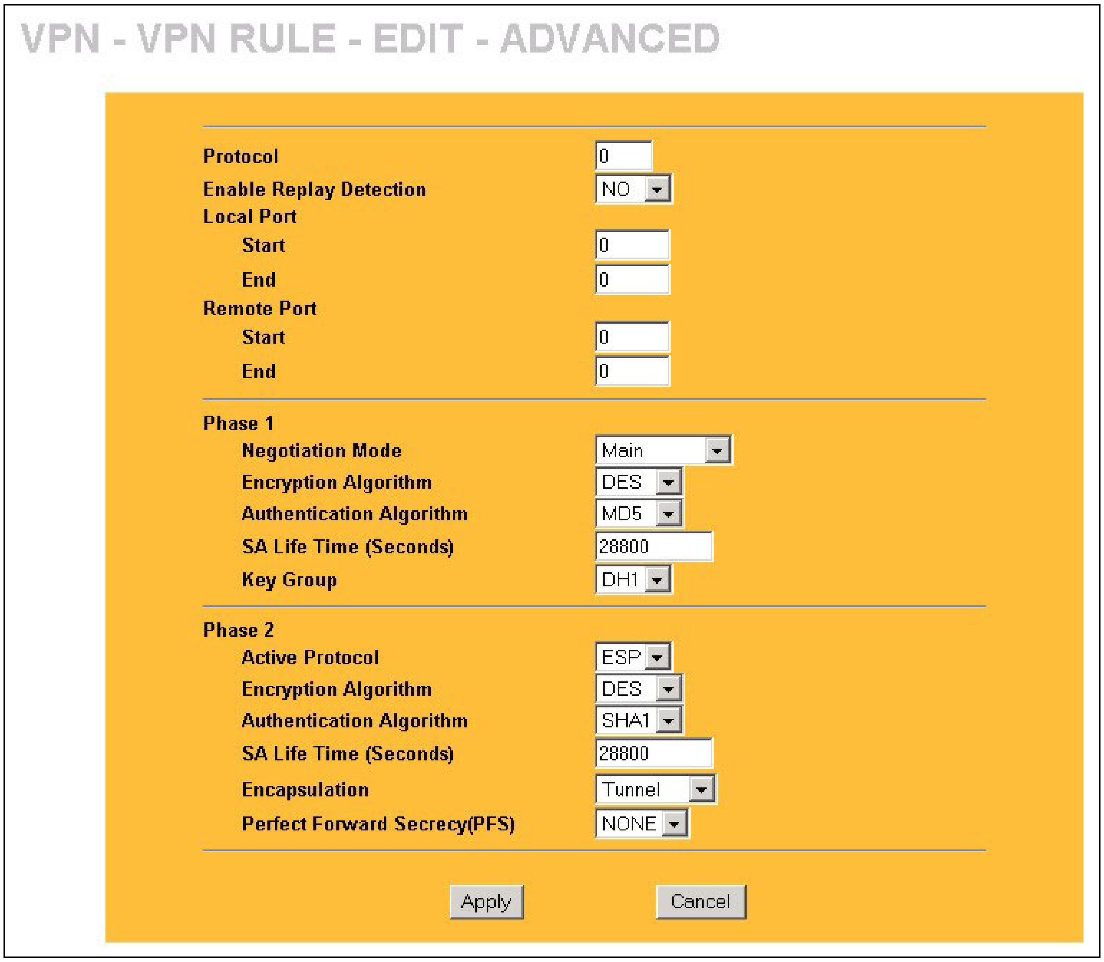



**Figure 12-9 Advanced IKE VPN Rule Setup**

The following table describes the fields in this screen.

**Table 12-8 Advanced IKE VPN Rule Setup**

| LABEL | DESCRIPTION |
|---|---|
| Protocol | Enter 1 for ICMP, 6 for TCP, 17 for UDP, etc. 0 is the default and signifies any protocol. |
| 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. Select **YES** from the drop-down menu to enable replay detection, or select **NO** to disable it. |
| Local Port | |
| Start | "0" is the default and signifies any port. Type a port number from 0 to 65535. Some of the most common IP ports are: 21, FTP; 53, DNS; 23, Telnet; 80, HTTP; 25, SMTP; 110, POP3. |
| End | Type a port number in this field to define a port range. This port number must be greater than that specified in the previous field. If **Local Port Start** is left at 0, **Local Port End** will also remain at 0. |
| Remote Port | |

**Table 12-8 Advanced IKE VPN Rule Setup**

| LABEL | DESCRIPTION |
|---|---|
| Start | Type up to 32 characters to identify this VPN policy. You may use any character, including spaces, but the LAN-Cell drops trailing spaces. |
| End | Enter a port number in this field to define a port range. This port number must be greater than that specified in the previous field. If **Remote Port Start is** left at 0, **Remote Port End** will also remain at 0. |
| Phase 1 | |
| 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 **DES**, **3DES** or **AES** from the drop-down list box.<br>When you use one of these encryption algorithms for data communications, both the sending device and the receiving device must use 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 | 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. |
| 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).<br>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 | 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. |
| Phase 2 | |
| Active Protocol | Use the drop-down list box to choose from **ESP** or **AH**. |
| Encryption Algorithm | This field is available when you select **ESP** in the **Active Protocol** field.<br>Select **DES**, **3DES**, **AES** or **NULL** from the drop-down list box.<br>When you use one of these encryption algorithms for data communications, both the sending device and the receiving device must use 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**.<br>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. |

**Table 12-8 Advanced IKE VPN Rule Setup**

| LABEL | DESCRIPTION |
|---|---|
| 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).<br>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. |
| Encapsulation | Select **Tunnel** mode or **Transport** mode from the drop-down list box. |
| Perfect Forward Secrecy (PFS) | Perfect Forward Secrecy (PFS) is disabled (**NONE**) by default in phase 2 IPSec SA setup. This allows faster IPSec setup, but is not so secure. Choose **DH1** or **DH2** from the drop-down list box 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). |
| Apply | Click **Apply** to save your changes back to the LAN-Cell and return to the **Edit VPN Rule** screen. |
| Cancel | Click **Cancel** to return to the **Edit VPN Rule** screen without saving your changes. |

# 12.14 Manual Key Setup

Manual key management is useful if you have problems with **IKE** key management.

## 12.14.1 Security Parameter Index (SPI)

An SPI is used to distinguish different SAs terminating at the same destination and using the same IPSec protocol. This data allows for the multiplexing of SAs to a single gateway. The **SPI** (Security Parameter Index) along with a destination IP address uniquely identify a particular Security Association (SA). The **SPI** is transmitted from the remote VPN gateway to the local VPN gateway. The local VPN gateway then uses the network, encryption and key values that the administrator associated with the SPI to establish the tunnel.

**Current LAN-Cell implementation assumes identical outgoing and incoming SPIs.**

# 12.15 Configuring Edit Manual Setup

To edit manual setup, click **Edit** in the **VPN Rules** screen to configure the VPN settings.

Select **Manual Key** (or **Manual**) in the **Key Management** (or **IPSec Keying Mode**) field to display the manual VPN rule setup screen.

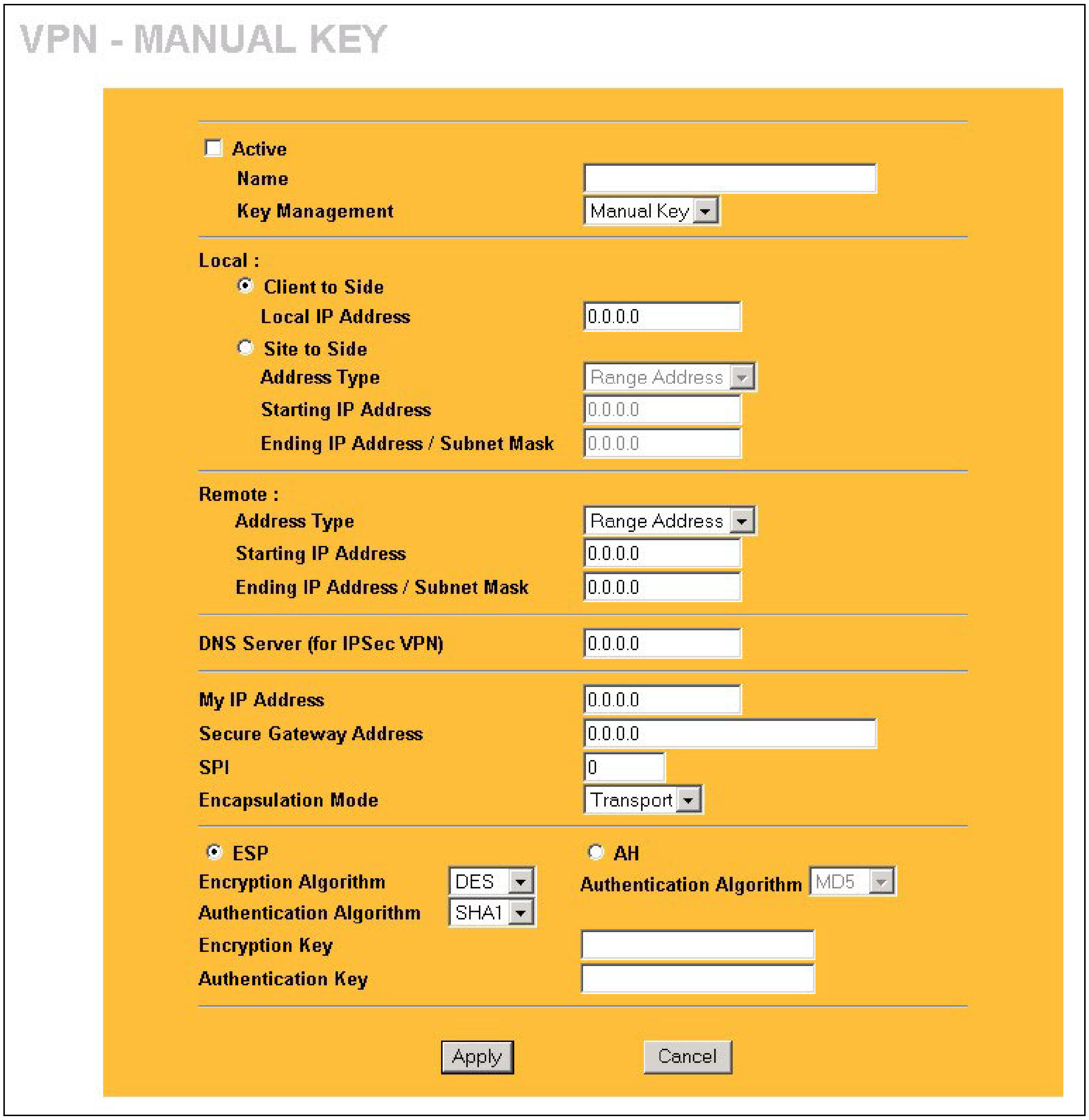



**Figure 12-10 Manual VPN Rule Setup**

The following table describes the labels in this screen.

**Table 12-9 VPN Manual Setup**

| LABEL | DESCRIPTION |
|---|---|
| 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. |
| Key Management | Select **IKE** or **Manual Key** (or **Manual**) from the drop-down list box. **Manual Key** is a useful option for troubleshooting if you have problems using **IKE** key management. |
| Local:<br>Local IP addresses must be static and correspond to the remote IPSec router's configured remote IP addresses.<br>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. | |
| Client to Site | Select this radio button to build a client to site VPN connection. |

**Table 12-9 VPN Manual Setup**

| LABEL | DESCRIPTION |
|---|---|
| Local IP Address | Enter a static local IP address. The local IP address must correspond to the remote IPSec router's configured remote IP addresses. |
| Site to Site | Select this radio button to establish a VPN between two sites (groups of IP addresses). |
| Address Type | Use the drop-down list box to choose **Range Address** or **Subnet 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 **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 **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:<br>Remote IP addresses must be static and correspond to the remote IPSec router's configured local IP addresses.<br>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. |
| DNS Server (for IPSec VPN) | If there is a private DNS server that services the VPN, type its IP address here. The LAN-Cell assigns this additional DNS server to the LAN-Cell's DHCP clients that have IP addresses in this IPSec rule's range of local addresses.<br>A DNS server allows clients on the VPN to find other computers and servers on the VPN by their (private) domain names. |
| My IP Address | Enter the WAN IP address of your LAN-Cell. The VPN tunnel has to be rebuilt if this IP address changes.<br>The following applies if this field is configured as **0.0.0.0**:<br>➢ The LAN-Cell uses the current LAN-Cell WAN IP address (static or dynamic) to set up the VPN tunnel.<br>➢ If the WAN connection goes down, the LAN-Cell uses the Cellular Modem IP address for the VPN tunnel when using Cellular Modem fail-over or the LAN IP address when using traffic redirect. See the chapter on WAN for details on Cellular Modem fail-over and traffic redirect. |
| Secure Gateway Addr | Type the WAN IP address or the URL (up to 31 characters) of the IPSec router with which you're making the VPN connection. |
| 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 12-9 VPN Manual Setup**

| LABEL | DESCRIPTION |
|---|---|
| ESP | 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). |
| Encryption Algorithm | Select **DES**, **3DES** or **NULL** from the drop-down list box.<br>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. |
| AH | 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). |
| 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 (Only with ESP) | 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. |

## 12.16 SA Monitor

In the web configurator, click **VPN** and the **SA Monitor** tab. Use this screen to display and manage your active VPN connection.

A Security Association (SA) is the group of security settings related to a specific VPN tunnel. This screen displays the active VPN connection. Use **Refresh** to display the active VPN connection. This screen is read-only. The following table describes the fields in this tab.

**When there is outbound traffic but no inbound traffic, the SA times out automatically after two minutes. A tunnel with no outbound or inbound traffic is "idle" and does not timeout until the SA lifetime period expires. See the section on keep alive to have the LAN-Cell renegotiate an IPSec SA when the SA lifetime expires, even if there is no traffic.**

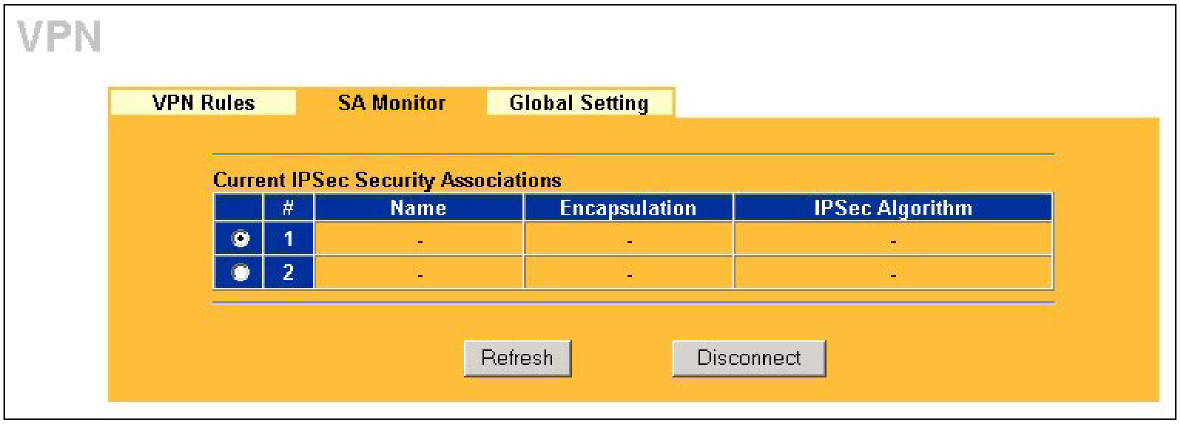



**Figure 12-11 VPN SA Monitor**

The following table describes the fields in this screen.

**Table 12-10 VPN SA Monitor**

| LABEL | DESCRIPTION |
|---|---|
| # | This is the security association index number. |
| Name | This field displays the identification name for this VPN policy. |
| Encapsulation | This field displays **Tunnel** or **Transport** mode. |
| IPSec Algorithm | This field displays the security protocols used for an SA.<br><br>Both AH and ESP increase LAN-Cell processing requirements and communications latency (delay). |
| Refresh | Click **Refresh** to display the current active VPN connection(s). This button is available when you have active VPN connections. |
| Disconnect | Select a security association index number that you want to disconnect and then click **Disconnect**. This button is available when you have active VPN connections. |

## 12.17 Global Settings

In the web configurator, click **VPN** on the navigation panel and the **Global Setting** tab. Use this screen to allow or block NetBIOS packets in the IPSec tunnels.

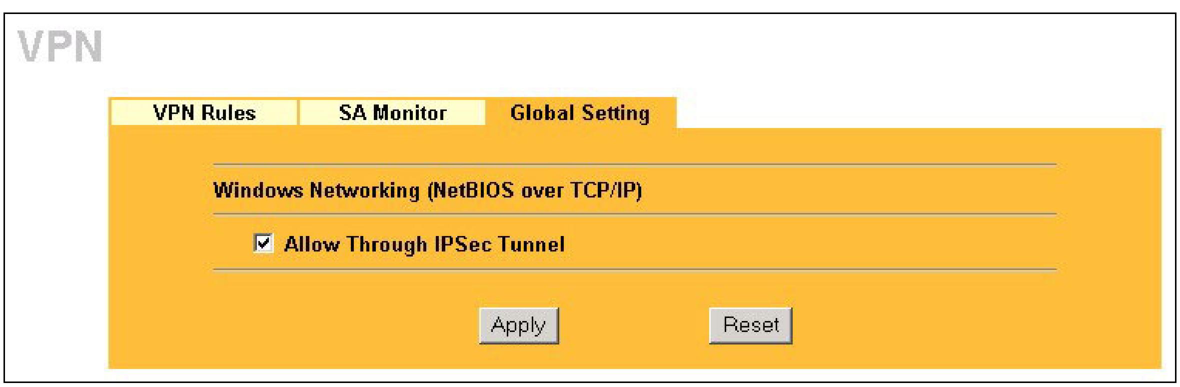



**Figure 12-12 VPN Global Setting**

The following table describes the fields in this screen.

**Table 12-11 VPN Global Setting**

| LABEL | DESCRIPTION |
|---|---|
| Windows Networking (NetBIOS over TCP/IP)<br>NetBIOS (Network Basic Input/Output System) are TCP or UDP broadcast 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. | |
| Allow Through IPSec Tunnel | Select this check box to send NetBIOS packets through the VPN connection. |
| Apply | Click **Apply** to save your customized settings and exit this screen. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 12.18 Telecommuter VPN/IPSec Examples

The following examples show how multiple telecommuters can make VPN connections to a single LAN-Cell at headquarters. The telecommuters use IPSec routers with dynamic WAN IP addresses. The LAN-Cell at headquarters has a static public IP address.

### 12.18.1 Telecommuters Sharing One VPN Rule Example

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

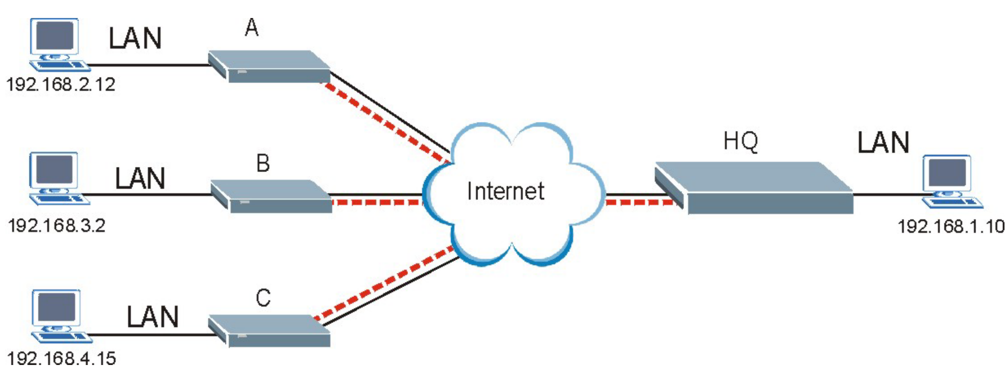



**Figure 12-13 Telecommuters Sharing One VPN Rule Example**

**Table 12-12 Telecommuters Sharing One VPN Rule Example**

| FIELDS | TELECOMMUTERS | HEADQUARTERS |
|---|---|---|
| My IP Address: | 0.0.0.0 (dynamic IP address assigned by the ISP) | Public static IP address |
| Secure Gateway IP Address: | Public static IP address | 0.0.0.0 With this IP address only the telecommuter can initiate the IPSec tunnel. |
| Local IP Address: | Telecommuter A: 192.168.2.12<br>Telecommuter B: 192.168.3.2<br>Telecommuter C: 192.168.4.15 | 192.168.1.10 |
| Remote IP Address: | 192.168.1.10 | 0.0.0.0 (N/A) |

### 12.18.2 Telecommuters Using Unique VPN Rules Example

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

With aggressive negotiation mode (see *section 12.12.1*), the LAN-Cell can use the ID types and contents to distinguish between VPN rules. Telecommuters can each use a separate VPN rule to simultaneously access a LAN-Cell at headquarters. They can use different IPSec parameters. The local IP addresses (or ranges of addresses) of the rules configured on the LAN-Cell at headquarters can overlap. The local IP addresses of the rules configured on the telecommuters' IPSec routers should not overlap.

See the following table and figure for an example where three telecommuters each use a different VPN rule for a VPN connection with a LAN-Cell located at headquarters. The LAN-Cell at headquarters (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 at headquarters can also initiate VPN connections to the telecommuters since it can find the telecommuters by resolving their domain names.

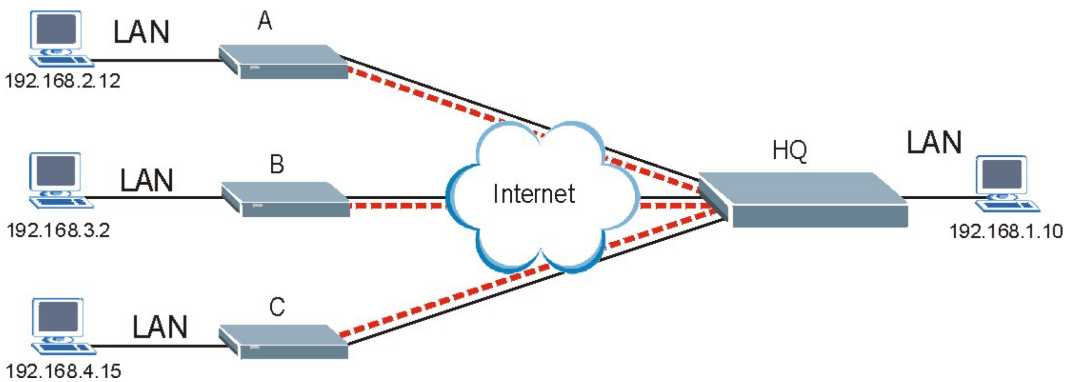



**Figure 12-14 Telecommuters Using Unique VPN Rules Example**

**Table 12-13 Telecommuters Using Unique VPN Rules Example**

| TELECOMMUTERS | HEADQUARTERS |
|---|---|
| **All Telecommuter Rules:** | **All Headquarters Rules:** |
| My IP Address 0.0.0.0 | My IP Address: bigcompanyhq.com |
| Secure Gateway Address: bigcompanyhq.com | Local IP Address: 192.168.1.10 |
| Remote 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 | |
| | |
| **Telecommuter A (telecommutera.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 | Secure Gateway Address: telecommuter1.com |
| | Remote Address 192.168.2.12 |
| | |
| **Telecommuter B (telecommuterb.dydns.org)** | **Headquarters LAN-Cell Rule 2:** |

**Table 12-13 Telecommuters Using Unique VPN Rules Example**

| TELECOMMUTERS | HEADQUARTERS |
|---|---|
| Local ID Type: DNS | Peer ID Type: DNS |
| Local ID Content: telecommuterb.com | Peer ID Content: telecommuterb.com |
| Local IP Address: 192.168.3.2 | Secure Gateway Address: telecommuterb.com |
| | Remote Address 192.168.3.2 |
| | |
| **Telecommuter C (telecommuterc.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 | Secure Gateway Address: telecommuterc.com |
| | Remote Address 192.168.4.15 |

## 12.19 VPN and Remote Management

If a VPN tunnel uses Telnet, FTP, WWW SNMP, DNS or ICMP, then you should configure remote management (**REMOTE MGNT**) to allow access for that service.

# Part VII:

## Certificates

This part provides information and configuration instructions for public-key certificates.

# Chapter 13
# Certificates

*This chapter gives background information about public-key certificates and explains how to use them.*

## 13.1 Certificates 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.

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 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).

### 13.1.1 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.

## 13.2 Self-signed Certificates

Until public-key infrastructure becomes more mature, it may not be available in some areas. You can have the LAN-Cell act as a certification authority and sign its own certificates.

## 13.3 Configuration Summary

This section summarizes how to manage certificates on the LAN-Cell.

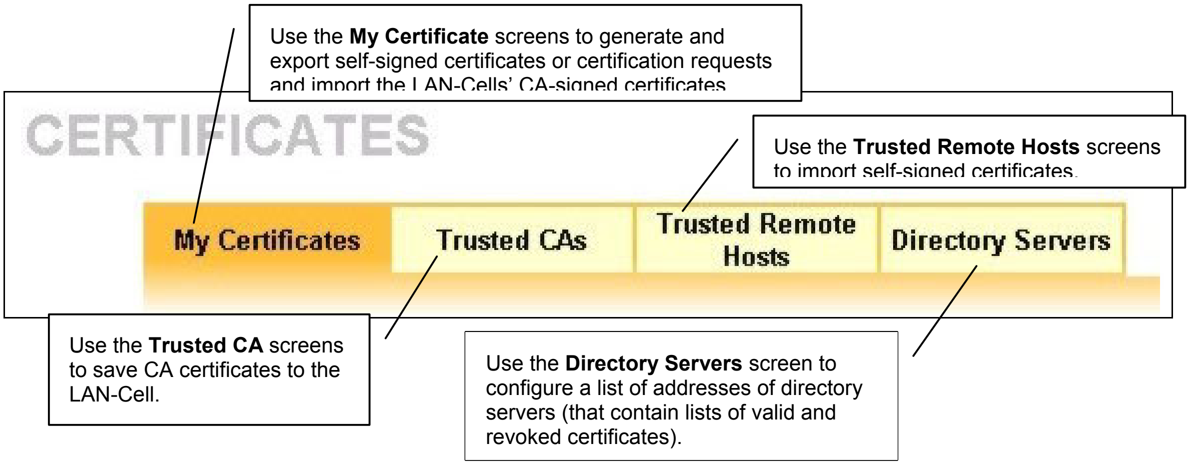



**Figure 13-1 Certificate Configuration Overview**

## 13.4 My Certificates

Click **CERTIFICATES**, **My Certificates** to open the LAN-Cell's summary list of certificates and certification requests. Certificates display in black and certification requests display in gray. See the following figure.

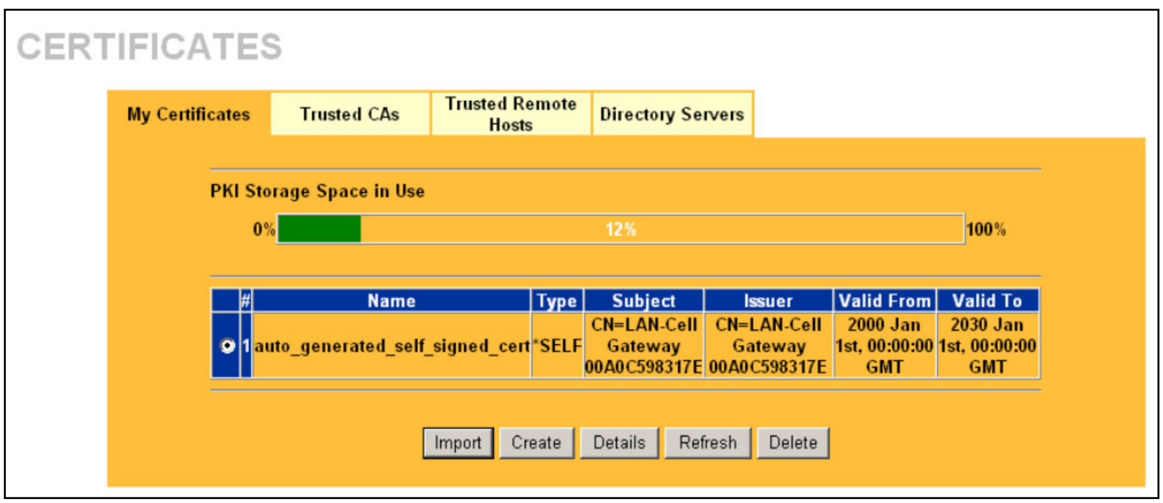



**Figure 13-2 My Certificates**

The following table describes the labels in this screen.

**Table 13-1 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 you are using 80% or less of the storage space, the bar is green. When the amount of space used is over 80%, the bar is red. When the bar is red, you should consider deleting expired or unnecessary certificates before adding more certificates. |

**Table 13-1 My Certificates**

| LABEL | DESCRIPTION |
|---|---|
| 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. **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. |
| 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. |
| Details | Select the radio button next to a certificate's index number and then click **Details** to open a screen with an in-depth list of information about that certificate. |
| Refresh | Click this button to display the current validity status of the certificates. |
| Delete | Select the radio button next to the index number of a certificate that you want to delete and then click **Delete** to remove that certificate.<br>Do the following to delete a certificate that shows ***SELF** in the **Type** field.<br>1. Make sure that no other features, such as HTTPS, VPN, SSH … are configured to use the ***SELF** certificate.<br>2. Select the radio button next to the index number of another self-signed certificate and click **Details** (see the section on the **Create** button if you need to create a self-signed certificate).<br>3. Select the **Default self-signed certificate which signs the imported remote host certificates** check box.<br>4. Click **Apply** to save the changes and return to the **My Certificates** screen.<br>5. The certificate that originally showed ***SELF** displays **SELF** and you can delete it now.<br>Note that subsequent certificates move up by one when you take this action. |

## 13.5 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.

## 13.6 Importing a Certificate

Click **CERTIFICATES**, **My Certificates** and then **Import** to open the **My Certificate Import** screen. Follow the instructions in this screen to save an existing certificate to the LAN-Cell, see the following figure.

**1. You can only import a certificate that matches a corresponding certification request that was generated by the LAN-Cell.**

**2. The certificate you import replaces the corresponding request in the** My Certificates **screen.**

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

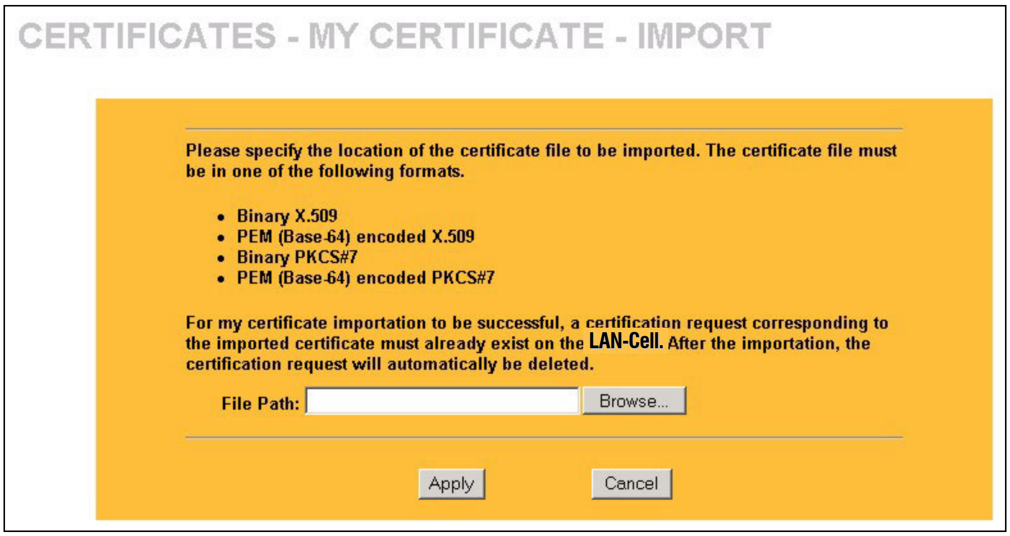



**Figure 13-3 My Certificate Import**

The following table describes the labels in this screen.

**Table 13-2 My Certificate 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. |

## 13.7 Creating a Certificate

Click **CERTIFICATES**, **My Certificates** and then **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, see the following figure.


**Figure 13-4 My Certificate Create**

The following table describes the labels in this screen.

**Table 13-3 My Certificate 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. |
| 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. |
| 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 13-3 My Certificate Create**

| 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.<br>Copy the certification request from the **My Certificate Details** screen (see section *13.8*) 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.<br>You must have the certification authority's certificate already imported in the **Trusted CAs** screen.<br>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.<br>**Simple Certificate Enrollment Protocol (SCEP)** is a TCP-based enrollment protocol that was developed by VeriSign and Cisco.<br>**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.<br>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. |
| 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 SECP enrollment protocol. |
| Key | Type the key that the certification authority gave you. |
| 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.

## 13.8 My Certificate Details

Click **CERTIFICATES**, and then **My Certificates** to open the **My Certificates** screen (see Figure 13-2). Click **Details** to open the **My Certificate Details** screen. You can use this screen to view in-depth certificate information and change the certificate's name. In the case of a self-signed certificate, you can set it to be the one that the LAN-Cell uses to sign the trusted remote host certificates that you import to the LAN-Cell.

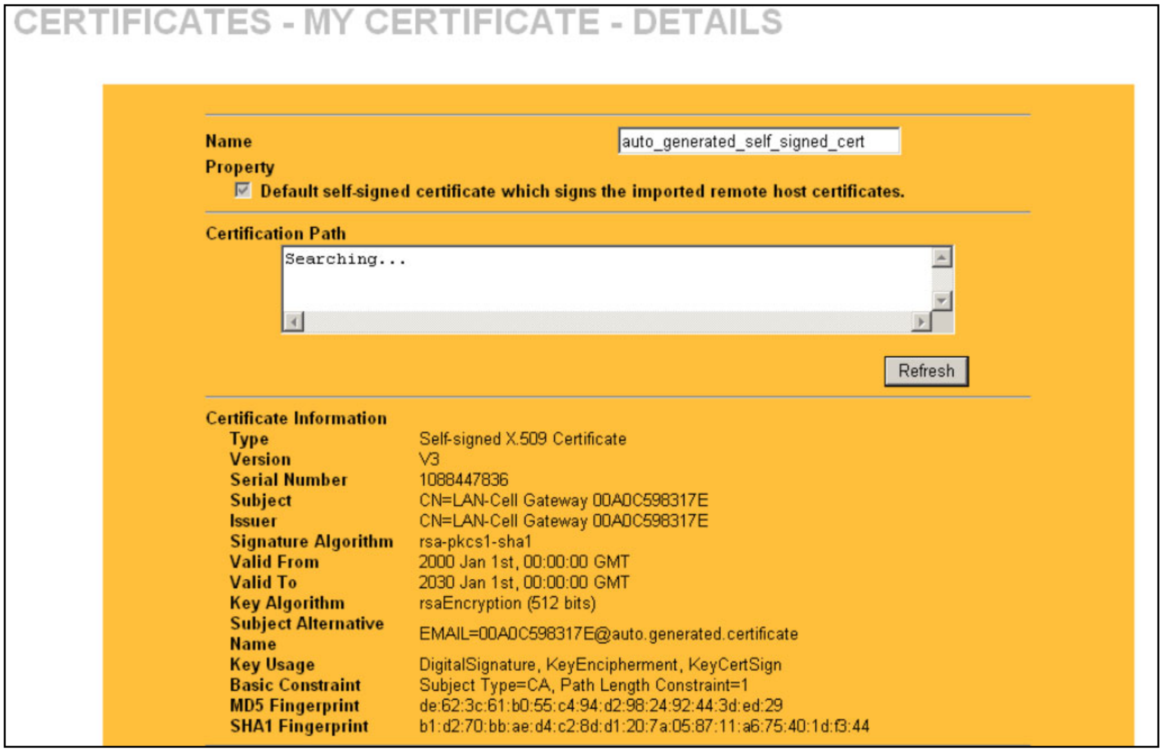



**Figure 13-5 My Certificate Details**

The following table describes the labels in this screen.

**Table 13-4 My Certificate 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<br>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.<br>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. |
| 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).<br>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. |

**Table 13-4 My Certificate Details**

| LABEL | DESCRIPTION |
|---|---|
| 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.<br>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 ras-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. |
| 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. |
| 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.<br>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.<br>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). |
| Export | Click this button and then **Save** in the **File Download** screen. The **Save As** screen opens, browse to the location that you want to use and click **Save**. |
| Apply | Click **Apply** to save your changes back to the 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. |

## 13.9 Trusted CAs

Click **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. See the following figure.

The following table describes the labels in this screen.

**Table 13-5 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 you are using 80% or less of the storage space, the bar is green. When the amount of space used is over 80%, the bar is red. When the bar is red, 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". |
| 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. |
| Details | Select the radio button next to a certificate's index number and then click **Details** to open a screen with an in-depth list of information about that certificate. |
| Refresh | Click this button to display the current validity status of the certificates. |
| Delete | Select the radio button next to the index number of a certificate that you want to delete and then click **Delete** to remove that certificate. |

## 13.10 Importing a Trusted CA's Certificate

Click **CERTIFICATES**, **Trusted CAs** to open the **Trusted CAs** screen and then click **Import** to open the **Trusted CA Import** screen. Follow the instructions in this screen to save a trusted certification authority's certificate to the LAN-Cell, see the following figure.

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

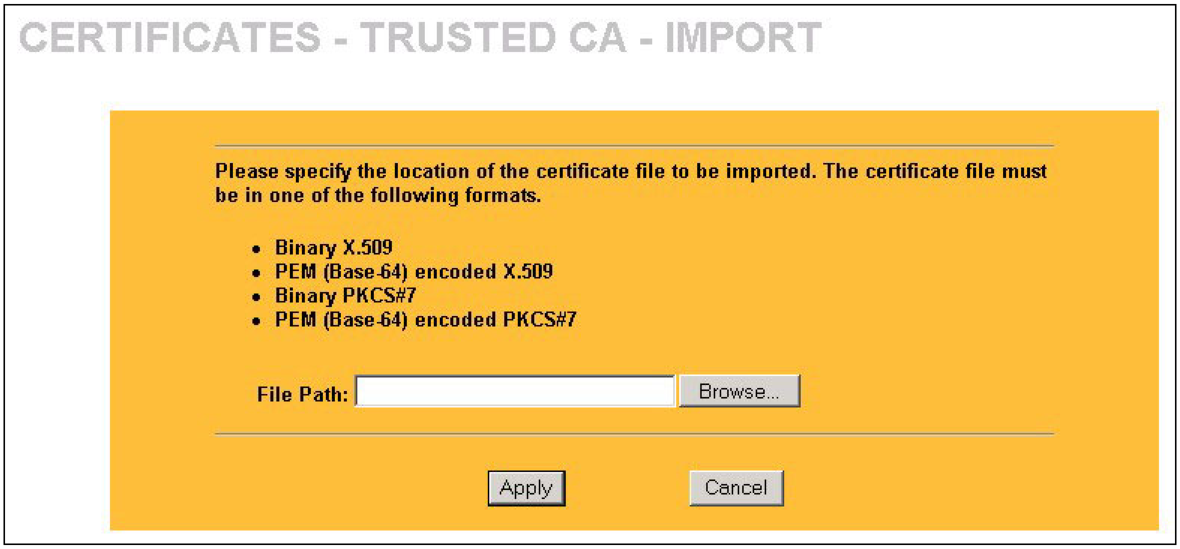



**Figure 13-6 Trusted CA Import**

The following table describes the labels in this screen.

**Table 13-6 Trusted CA Import**

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

## 13.11 Trusted CA Certificate Details

Click **CERTIFICATES**, **Trusted CAs** to open the **Trusted CAs** screen. Click **Details** 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.

The following table describes the labels in this screen.

**Table 13-7 Trusted CA 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<br>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).<br>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). |
| 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.<br>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 ras-pkcs1-md5 (RSA public-private key encryption algorithm and the MD5 hash algorithm). |
| Valid From | This field displays the date that the certificate becomes applicable. The text displays in red and includes a "Not Yet Valid!" message if the certificate has not yet become applicable. |

**Table 13-7 Trusted CA Details**

| LABEL | DESCRIPTION |
|---|---|
| Valid To | This field displays the date that the certificate expires. The text displays in red and includes an "Expiring!" or "Expired!" message if the certificate is about to expire or has already expired. |
| Key Algorithm | This field displays the type of algorithm that was used to generate the certificate's key pair (the 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. |
| 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.<br>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). |
| Export | Click this button and then **Save** in the **File Download** screen. The **Save As** screen opens, browse to the location that you want to use and click **Save**. |
| Apply | Click **Apply** to save your changes back to the 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. |

## 13.12 Trusted Remote Hosts

Click **CERTIFICATES**, **Trusted Remote Hosts** to open the **Trusted Remote Hosts** screen (see the following figure). 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.

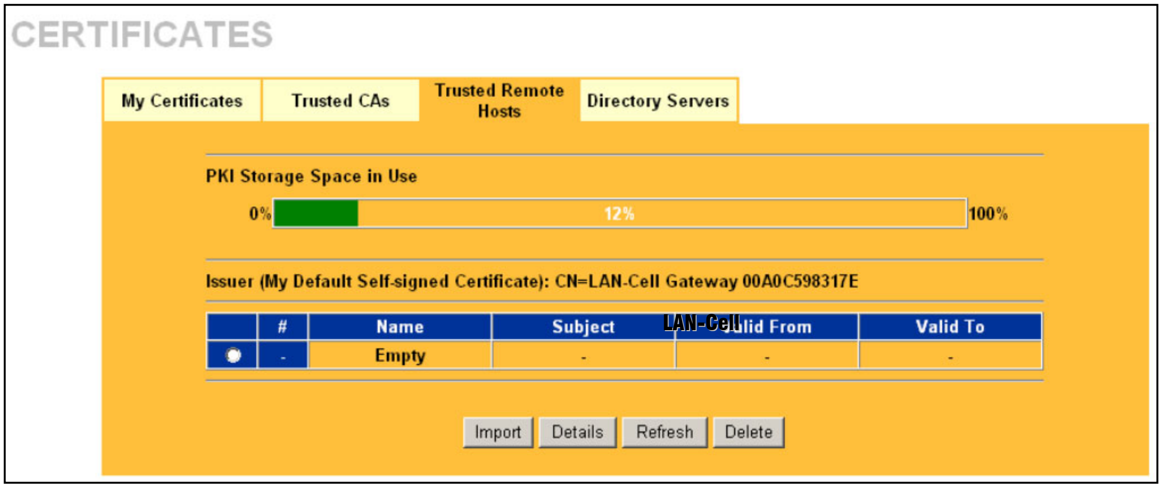



**Figure 13-7 Trusted Remote Hosts**

The following table describes the labels in this screen.

**Table 13-8 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 you are using 80% or less of the storage space, the bar is green. When the amount of space used is over 80%, the bar is red. When the bar is red, you should consider deleting expired or unnecessary certificates before adding more certificates. |
| Issuer (My Default Self-signed Certificate) | This field displays identifying information about the default self-signed certificate on the 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. |
| 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. |
| Details | Select the radio button next to a certificate's index number and then click **Details** to open a screen with an in-depth list of information about that certificate. |
| Refresh | Click this button to display the current validity status of the certificates. |
| Delete | Select the radio button next to the index number of a certificate that you want to delete and then click **Delete** to remove that certificate. |

## 13.13 Verifying a Trusted Remote Host's Certificate

Certificates issued by certification authorities have the certification authority's signature for you to check. Self-signed certificates only have the signature of the host itself. This means that you must be very careful when deciding to import (and thereby trust) a remote host's self-signed certificate.

### 13.13.1 Trusted Remote Host Certificate Fingerprints

A certificate's fingerprints are message digests calculated using the MD5 or SHA1 algorithms. The following procedure describes how to use a certificate's fingerprint to verify that you have the remote host's actual certificate.

**Step 1.** Browse to where you have the remote host's certificate saved on your computer.

**Step 2.** Make sure that the certificate has a ".cer" or ".crt" file name extension.

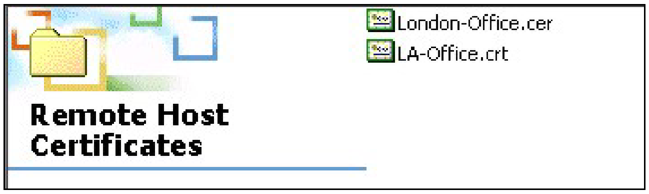



**Figure 13-9 Remote Host Certificates**

**Step 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.

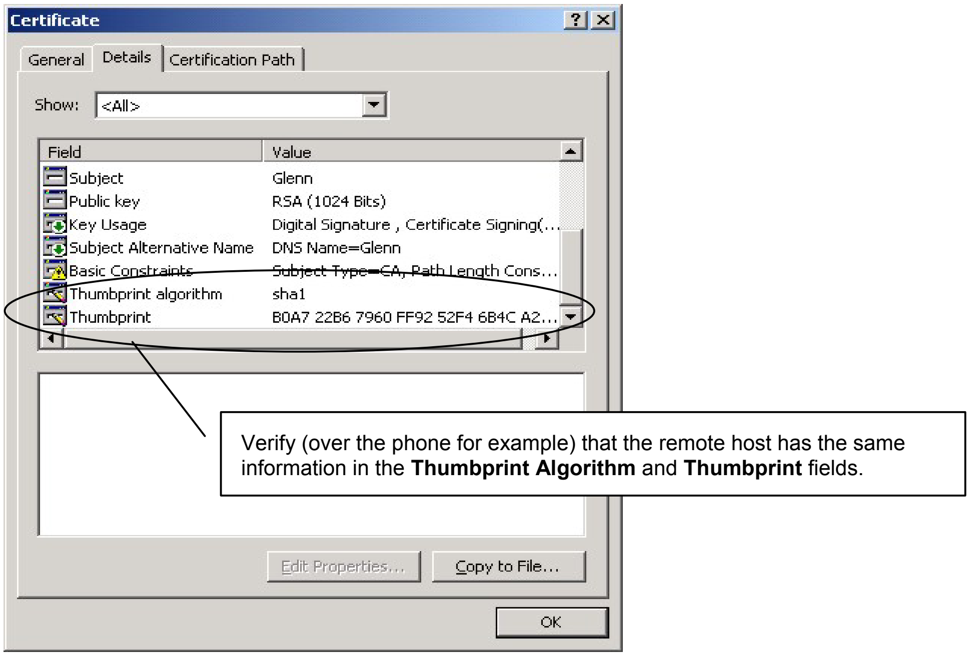



**Figure 13-10 Certificate Details**

## 13.14 Importing a Trusted Remote Host's Certificate

Click **CERTIFICATES**, **Trusted Remote Hosts** to open the **Trusted Remote Hosts** screen and then click **Import** to open the **Trusted Remote Host Import** screen. Follow the instructions in this screen to save a trusted host's certificate to the LAN-Cell, see the following figure.

**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.**

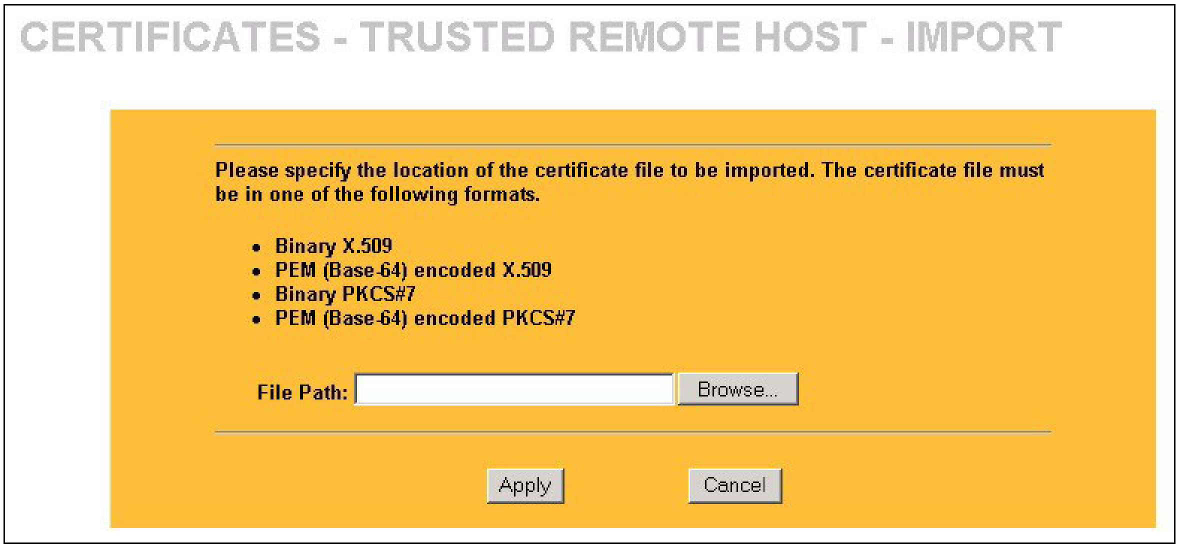



**Figure 13-8 Trusted Remote Host Import**

The following table describes the labels in this screen.

**Table 13-11 Trusted Remote Host 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. |

## 13.15 Trusted Remote Host Certificate Details

Click **CERTIFICATES**, **Trusted Remote Hosts** to open the **Trusted Remote Hosts** screen. Click **Details** 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.

The following table describes the labels in this screen.

**Table 13-12 Trusted Remote Host 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. |

**Table 13-12 Trusted Remote Host Details**

| LABEL | DESCRIPTION |
|---|---|
| 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. |
| MD5 Fingerprint | This is the certificate's message digest that the LAN-Cell calculated using the MD5 algorithm. You cannot use this value to verify that this is the remote host's actual certificate because the LAN-Cell has signed the certificate; thus causing this value to be different from that of the remote hosts actual certificate. See *section 13.13.1* for how to verify a remote host's certificate. |
| SHA1 Fingerprint | This is the certificate's message digest that the LAN-Cell calculated using the SHA1 algorithm. You cannot use this value to verify that this is the remote host's actual certificate because the LAN-Cell has signed the certificate; thus causing this value to be different from that of the remote hosts actual certificate. See *section 13.13.1* for how to verify a remote host's certificate. |
| Certificate in PEM (Base-64) Encoded Format | This read-only text box displays the certificate or certification request in Privacy Enhanced Mail (PEM) format. PEM uses 64 ASCII characters to convert the binary certificate into a printable form.<br>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). |
| Export | Click this button and then **Save** in the **File Download** screen. The **Save As** screen opens, browse to the location that you want to use and click **Save**. |
| Apply | Click **Apply** to save your changes back to the 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. |

## 13.16 Directory Servers

Click **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.

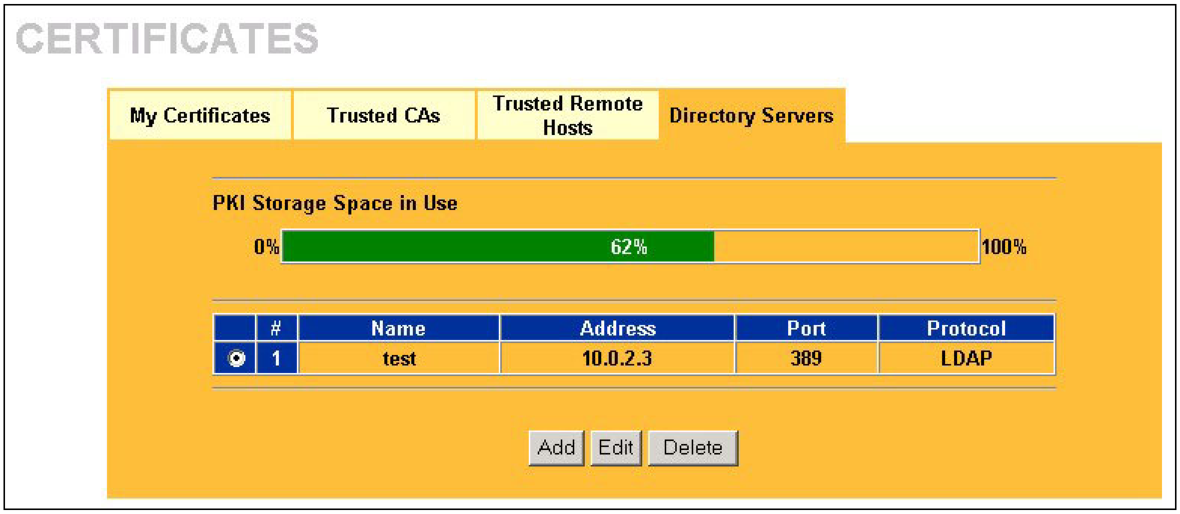



**Figure 13-9 Directory Servers**

The following table describes the labels in this screen.

**Table 13-13 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 you are using 80% or less of the storage space, the bar is green. When the amount of space used is over 80%, the bar is red. When the bar is red, 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. |
| Add | Click **Add** to open a screen where you can configure information about a directory server so that the LAN-Cell can access it. |
| Edit | Select the radio button next to a directory server's index number and then click **Edit** to open a screen where you can change the information about that directory server. |
| Delete | Select the radio button next to the index number of a directory server entry that you want to remove and then click **Delete** to remove that directory server entry. |

## 13.17 Add or Edit a Directory Server

Click **CERTIFICATES**, **Directory Servers** to open the **Directory Servers** screen. Click **Add** (or the details icon) to open the following screen. Use this screen to configure information about a directory server that the LAN-Cell can access.

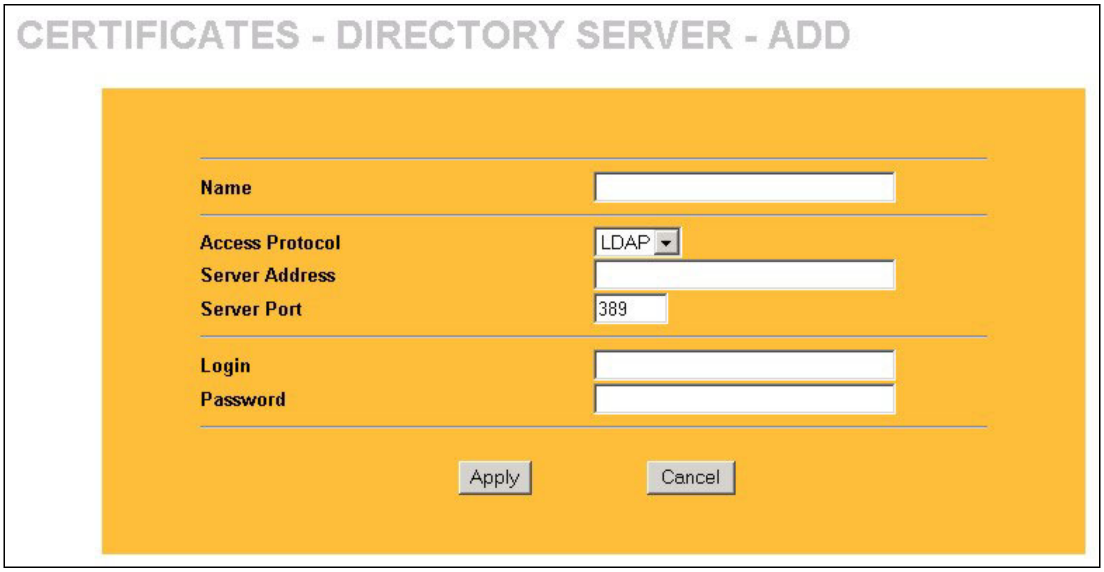



**Figure 13-10 Directory Server Add**

The following table describes the labels in this screen.

**Table 13-14 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.<br>**LDAP** (Lightweight Directory Access Protocol) is a protocol over TCP that specifies how clients access directories certificates and lists of revoked certificates.[1] |
| 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.<br>You may change the server port number if needed, however you must use the same server port number that the directory server uses.<br>**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. |

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

# Part VIII:

## Authentication Server & Remote Management

This part provides information and configuration instructions for configuration of the authentication server screens and remote management.

# Chapter 14
# Authentication Server

*This chapter discusses how to configure the authentication server on the LAN-Cell.*

## 14.1 Authentication Server Overview

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.

## 14.2 Local User Database

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

## 14.3 Configuring Local User Database

To change your LAN-Cell's local user list, click **AUTH SERVER**. The screen appears as shown.

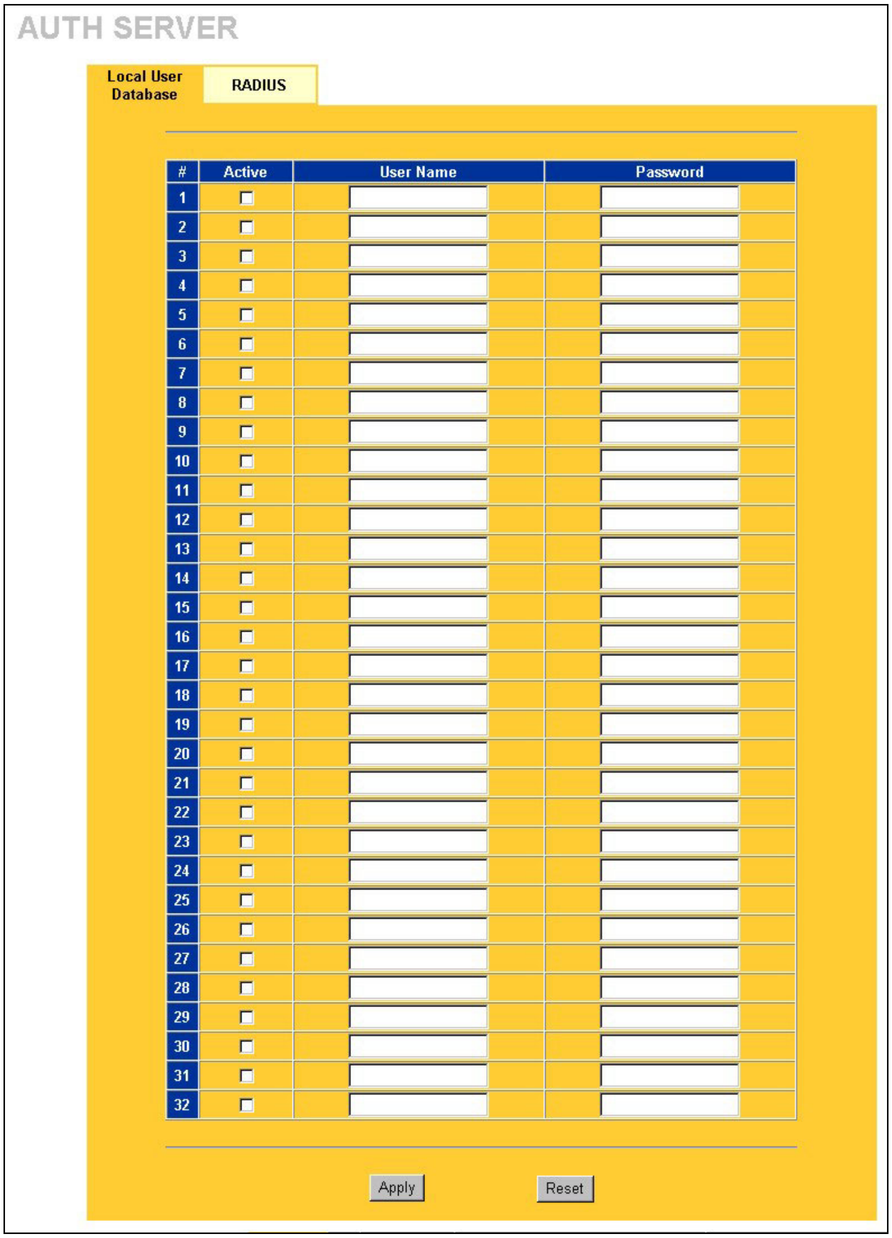



**Figure 14-1 Local User Database**

The following table describes the fields in this screen.

**Table 14-1 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. |

## 14.4 Configuring RADIUS

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

To set up your LAN-Cell's RADIUS server settings, click **AUTH SERVER**, then the **RADIUS** tab. The screen appears as shown.

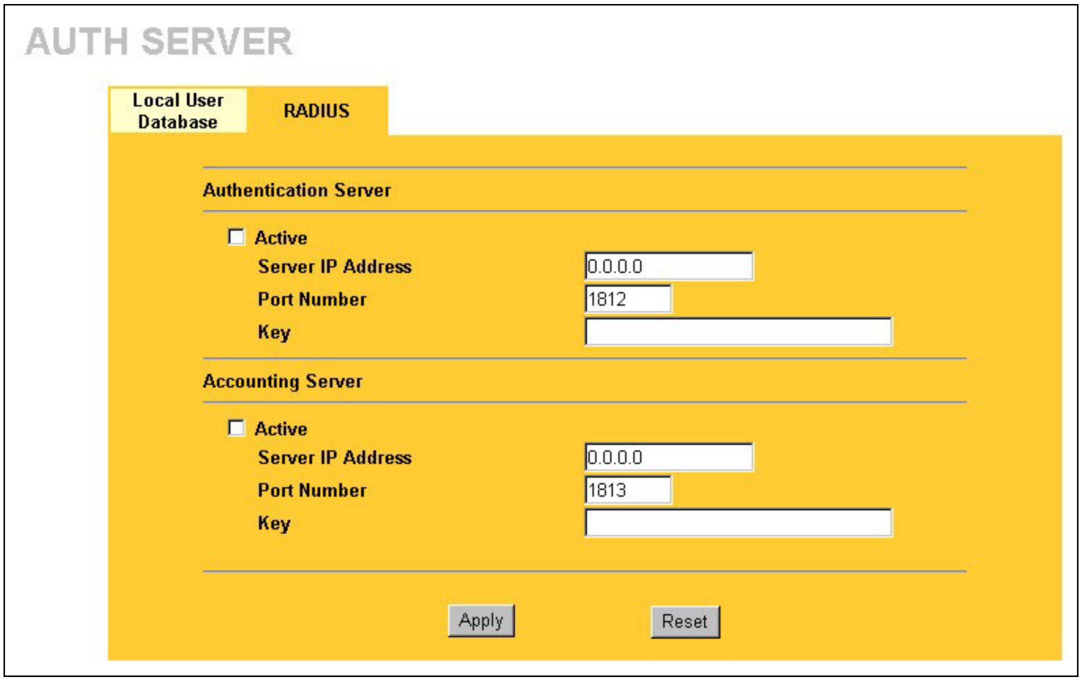



**Figure 14-2 RADIUS**

The following table describes the fields in this screen.

**Table 14-2 RADIUS**

| LABEL | DESCRIPTION |
|---|---|
| Authentication Server | |
| Active | Enable this feature to have the LAN-Cell use an external authentication server in performing user authentication.<br>Disable this feature if you will not use an external authentication server. If you disable this feature, you can still set the LAN-Cell to perform user authentication using the local user database. |
| Server 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**.<br>You need not change this value unless your network administrator instructs you to do so with additional information. |
| Key | Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external authentication server and the access points.<br>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 | Enable this feature to do user accounting through an external authentication server. |

**Table 14-2 RADIUS**

| LABEL | DESCRIPTION |
|---|---|
| Server 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**.<br><br>You need not change this value unless your network administrator instructs you to do so with additional information. |
| Key | Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external accounting server and the access points.<br><br>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. |

# Chapter 15
# Remote Management Screens

*This chapter provides information on the Remote Management screens.*

## 15.1 Remote Management Overview

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

**When you configure remote management to allow management from the WAN, you still need to configure a firewall rule to allow access. See the firewall chapters for details on configuring firewall rules.**

You may manage your LAN-Cell from a remote location via:

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

**When you Choose** WAN only **or** ALL **(LAN & WAN), you still need to configure a firewall rule to allow access.**

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

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. SSH
2. Telnet
3. HTTPS and HTTP

### 15.1.1 Remote Management Limitations

Remote management over LAN or WAN will not work when:

1. A filter in SMT 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 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.

### 15.1.2 Remote Management and NAT

When NAT is enabled:

- Use the LAN-Cell's WAN IP address when configuring from the WAN.
- Use the LAN-Cell's LAN IP address when configuring from the LAN.

### 15.1.3 System Timeout

There is a system timeout of five minutes (three hundred seconds) for the telnet/web/FTP connections. Your LAN-Cell automatically logs you out if you do nothing in this timeout period, except when it is continuously updating the status in menu 24.1 or when `sys stdio` has been changed on the command line. See the **System** screen to change the timeout period in the **Administrator Inactivity Timer** field.

## 15.2 Introduction to HTTPS

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

It relies upon certificates, public keys, and private keys (see the *Certificates* chapter 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).

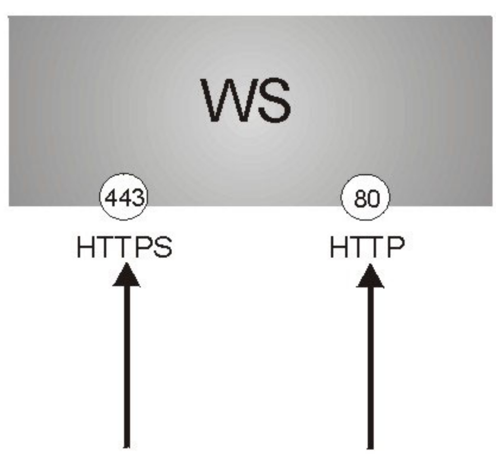



**Figure 15-1 HTTPS Implementation**

**If you disable** HTTP Server Access (Disable) **in the** REMOTE MGMT WWW **screen, then the LAN-Cell blocks all HTTP connection attempts.**

## 15.3 Configuring WWW

To change your LAN-Cell's web settings, click **REMOTE MGNT**, then the **WWW** tab. The screen appears as shown.

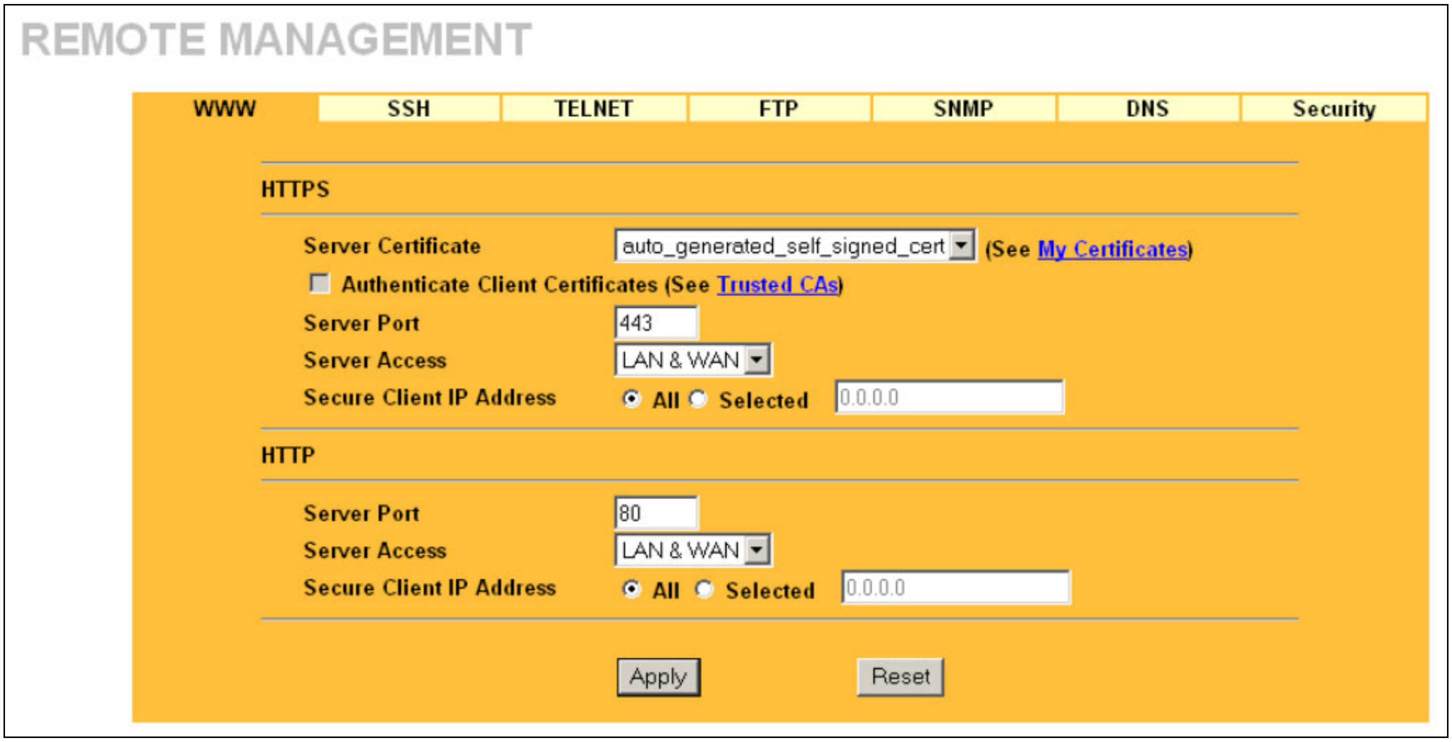



**Figure 15-2 WWW**

The following table describes the labels in this screen.

**Table 15-1 WWW**

| LABEL | DESCRIPTION |
|---|---|
| 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 the appendix 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 a LAN-Cell interface from **Server Access** on which incoming HTTPS access is allowed.<br><br>You can allow only secure web configurator access by setting the **HTTP Server Access** field to **Disable** and setting the **HTTPS Server Access** field to an interface(s). |

**Table 15-1 WWW**

| LABEL | DESCRIPTION |
|---|---|
| Secure Client IP Address | A secure client is a "trusted" computer that is allowed to communicate with the LAN-Cell using this service.<br>Select **All** to allow any computer to access the LAN-Cell using this service.<br>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.<br>Select **All** to allow any computer to access the LAN-Cell using this service.<br>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 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.

### 15.4.1 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.


**Figure 15-3 Security Alert Dialog Box (Internet Explorer)**

### 15.4.2 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 the appendix on importing certificates 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.

  **Step 1.** Click **REMOTE MGNT**. Write down the name of the certificate displayed in the **Server Certificate** field.

  **Step 2.** Click **CERTIFICATES**. Find the certificate and check its **Subject** column. **CN** stands for certificate's common name (see ***Error! Reference source not found.*** 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.

  **Step 1.** 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.

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

### 15.4.3 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.

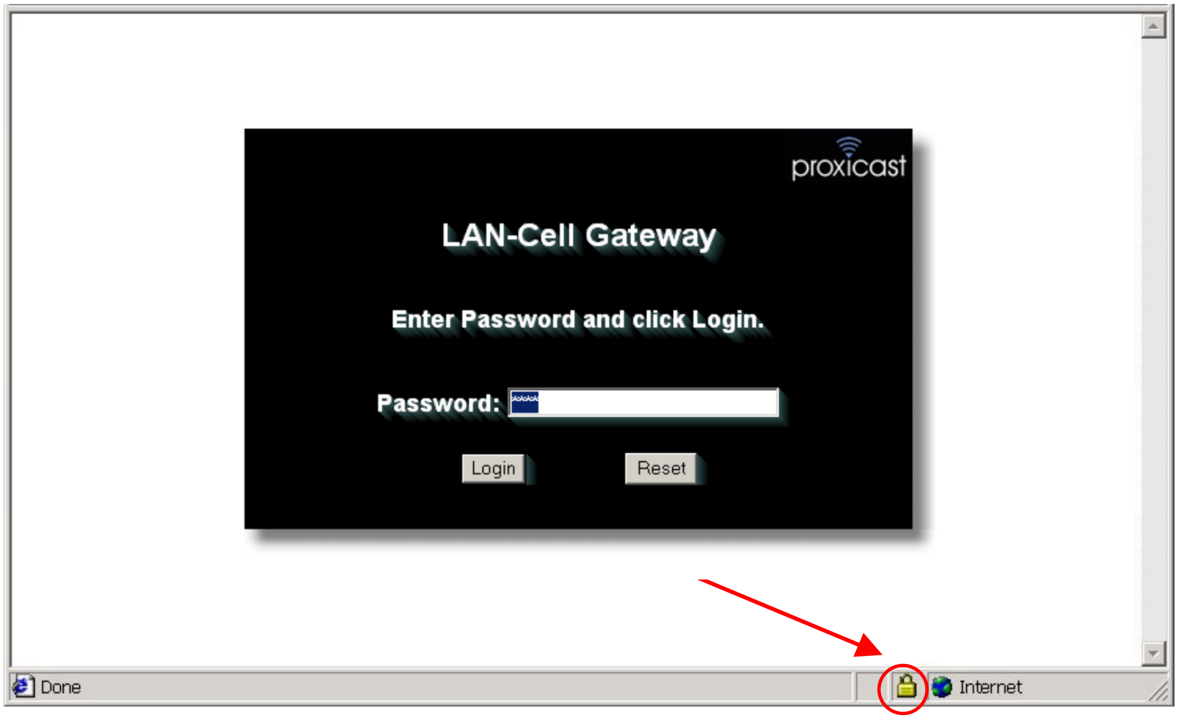



**Figure 15-4 Login Screen (Internet Explorer)**

## 15.5 SSH Overview

Unlike Telnet or FTP, which transmit data in clear text, SSH (Secure Shell) is a secure communication protocol that combines authentication and data encryption to provide secure encrypted communication between two hosts over an unsecured network.


**Figure 15-5 SSH Communication Example**

## 15.6 How SSH works

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

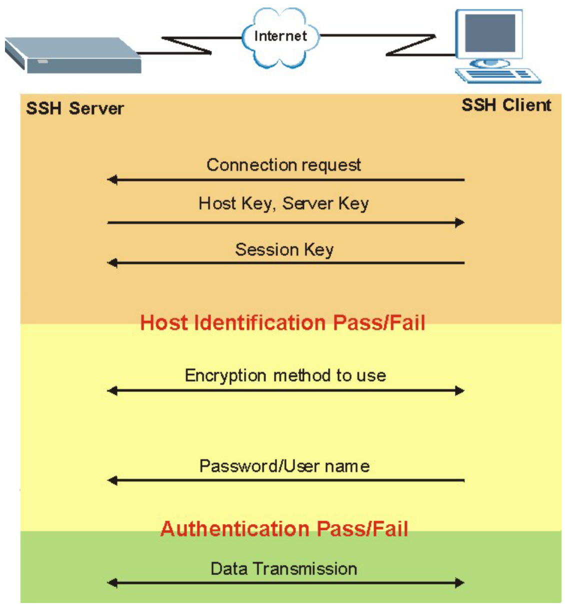



**Figure 15-6How SSH Works**

**1. Host Identification**

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

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

**2. Encryption Method**

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

**3. Authentication and Data Transmission**

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

## 15.7 SSH Implementation on the 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.

### 15.7.1 Requirements for Using SSH

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

## 15.8 Configuring SSH

To change your LAN-Cell's Secure Shell settings, click **REMOTE MGNT**, then the **SSH** tab. The screen appears as shown. This feature is not available on the LAN-Cell 2WE.

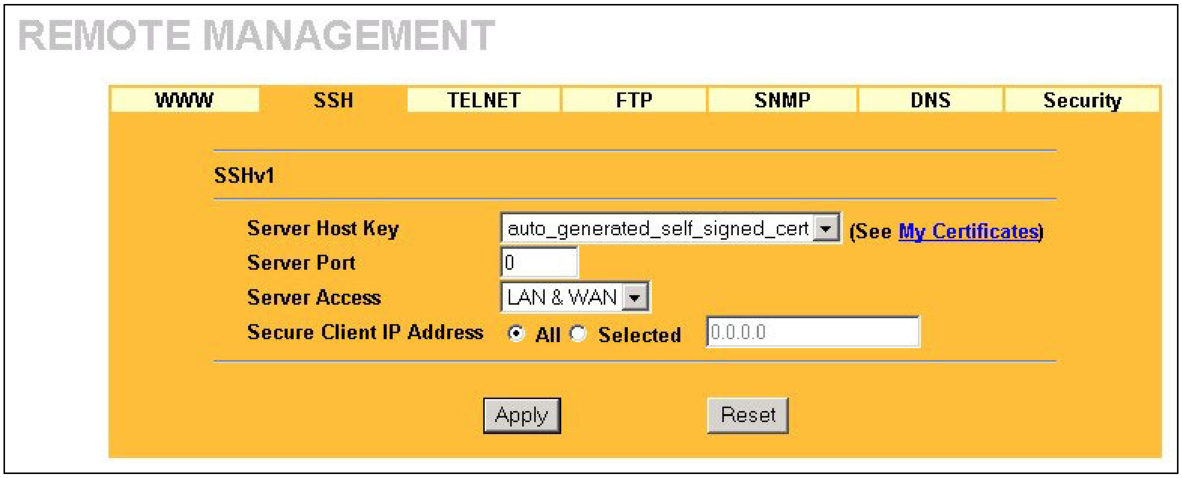



**Figure 15-7 SSH**

The following table describes the labels in this screen.

**Table 15-2 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 the *Certificates* part 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.<br>Select **All** to allow any computer to access the LAN-Cell using this service.<br>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. |

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

## 15.9 Secure Telnet Using SSH Examples

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

### 15.9.1 Example 1: Microsoft Windows

This section describes how to access the LAN-Cell using the Secure Shell Client program.

**Step 1.** Launch the SSH client and specify the connection information (IP address, port number or device name) for the LAN-Cell.

**Step 2.** Configure the SSH client to accept connection using SSH version 1.

**Step 3.** A window displays prompting you to store the host key in you computer. Click **Yes** to continue.

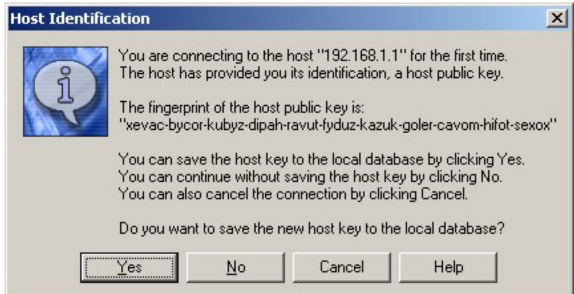



**Figure 15-8 SSH Example 1: Store Host Key**

Enter the password to log in to the LAN-Cell. The SMT main menu displays next.

## 15.9.2 Example 2: Linux

This section describes how to access the LAN-Cell using the OpenSSH client program that comes with most Linux distributions.

**Step 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.

```
$ 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
```

**Figure 15-9 SSH Example 2: Test**

**Step 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.

```
$ 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:
```

**Figure 15-10SSH Example 2: Log in**

**Step 3.** The SMT main menu displays next.

## 15.10 Secure FTP Using SSH Example

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

**Step 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].

**Step 2.** Enter the password to login to the LAN-Cell.

**Step 3.** Use the "`put`" command to upload a new firmware to the LAN-Cell.

```
$ 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
$
```

**Figure 15-11 Secure FTP: Firmware Upload Example**

## 15.11 Telnet

You can configure your LAN-Cell for remote Telnet access as shown next.

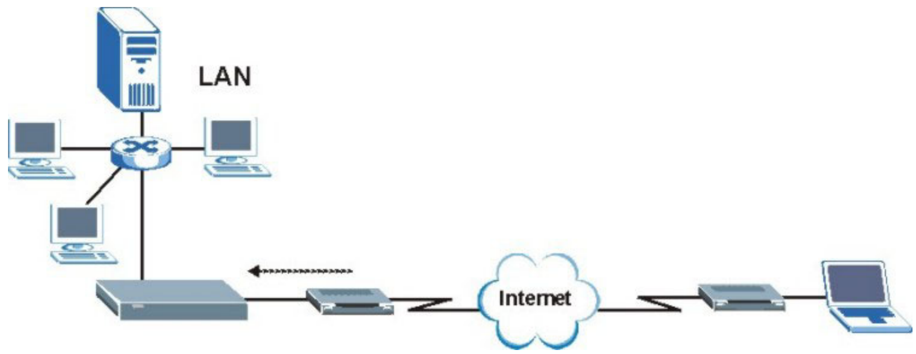



**Figure 15-12 Telnet Configuration on a TCP/IP Network**

## 15.12 Configuring TELNET

Click **REMOTE MGNT** to open the **TELNET** screen.

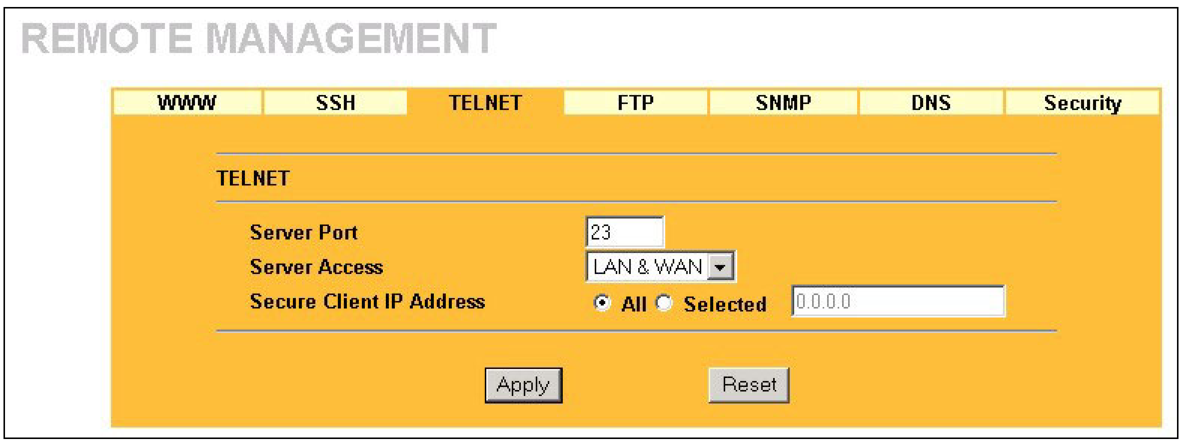



**Figure 15-13 Telnet**

The following table describes the labels in this screen.

**Table 15-3 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.<br>Select **All** to allow any computer to access the LAN-Cell using this service.<br>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. |

# 15.13 Configuring FTP

You can upload and download the LAN-Cell's firmware and configuration files using FTP, please see the 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 **REMOTE MANAGEMENT**, then the **FTP** tab. The screen appears as shown.

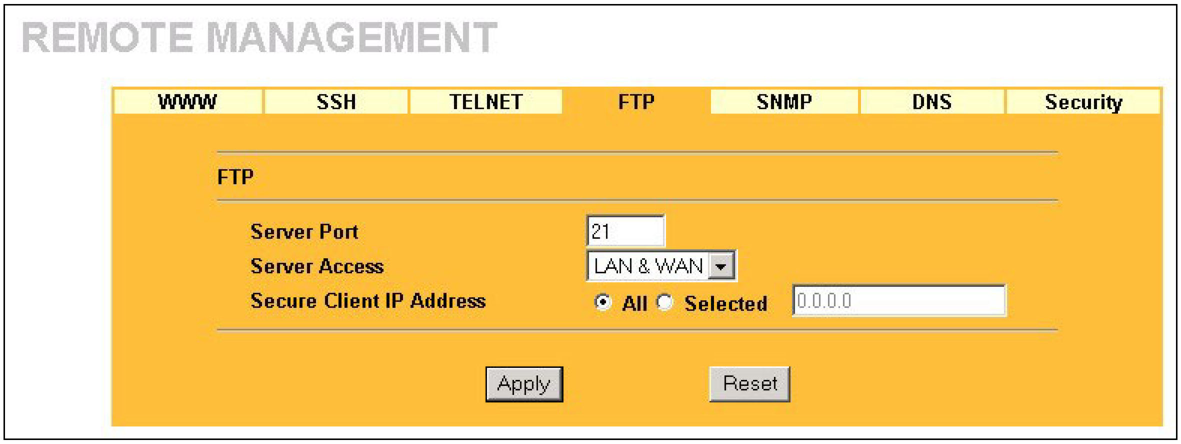



**Figure 15-14 FTP**

The following table describes the fields in this screen.

**Table 15-4 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.<br>Select **All** to allow any computer to access the LAN-Cell using this service.<br>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. |

# 15.14 Configuring SNMP

Simple Network Management Protocol is a protocol used for exchanging management information between network devices. SNMP is a member of the TCP/IP protocol suite. Your 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.

**SNMP is only available if TCP/IP is configured.**

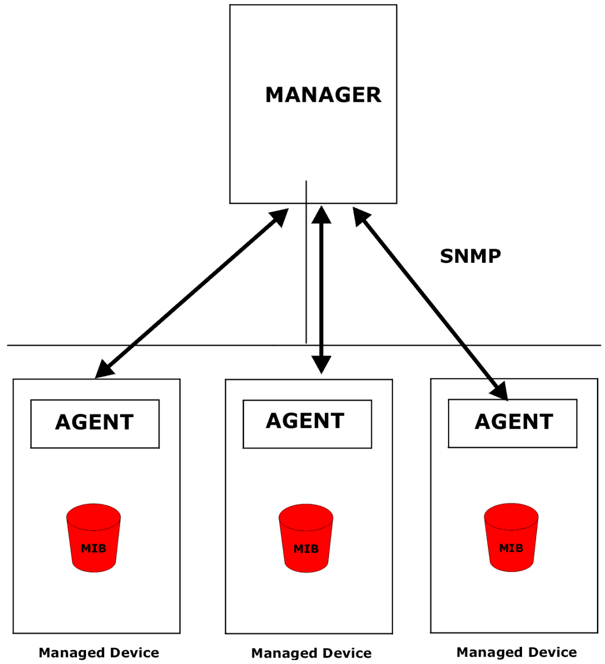



**Figure 15-15 SNMP Management Model**

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.

### 15.14.1 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.

### 15.14.2 SNMP Traps

The LAN-Cell will send traps to the SNMP manager when any one of the following events occurs:

**Table 15-5 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 MIB) | A trap is sent with the reason of restart before rebooting when the system is going to restart (warm start). |
| 6a | For intentional reboot : | A trap is sent with the message "System reboot by user!" if reboot is done intentionally, (for example, download new files, CI command "sys reboot", etc.). |
| 6b | For fatal error : | A trap is sent with the message of the fatal code if the system reboots because of fatal errors. |

## 15.14.3 REMOTE MANAGEMENT: SNMP

To change your LAN-Cell's SNMP settings, click **REMOTE MGNT**, then the **SNMP** tab. The screen appears as shown.

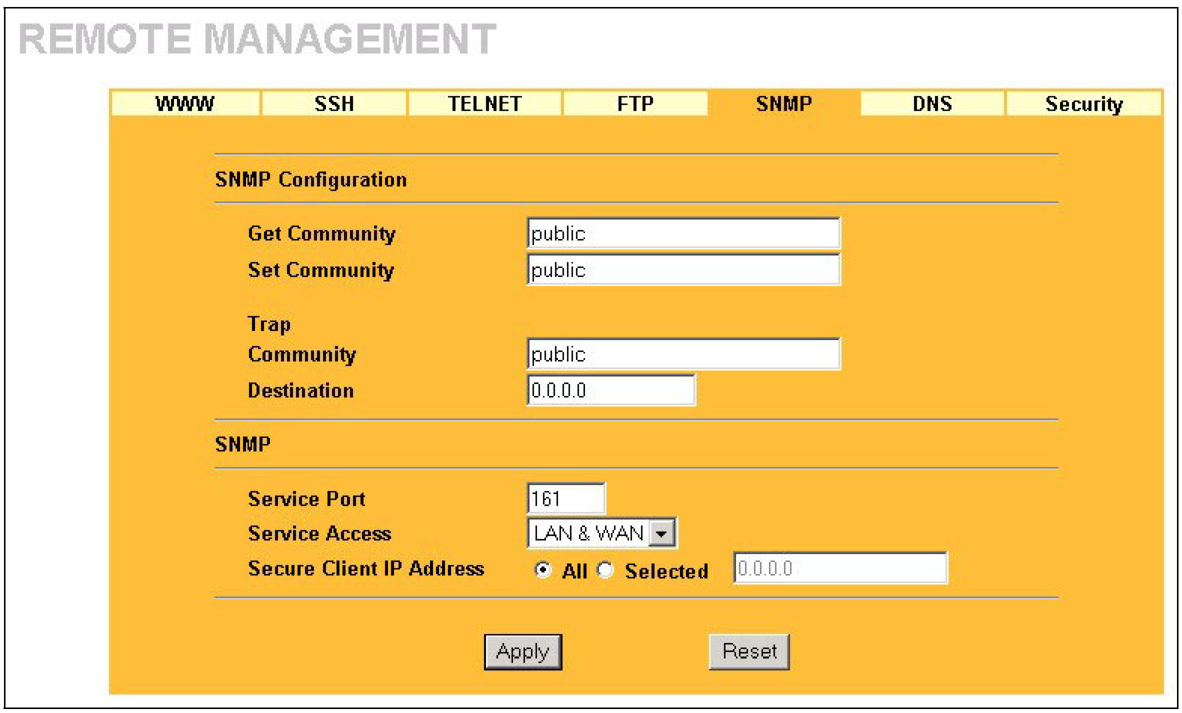



**Figure 15-16 SNMP**

The following table describes the fields in this screen.

**Table 15-6 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. |
| Trusted Host | If you enter a trusted host, your LAN-Cell will only respond to SNMP messages from this address. 0.0.0.0 (default) 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. 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.<br>Select **All** to allow any computer to access the LAN-Cell using this service.<br>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. |

## 15.15 Configuring DNS

Use DNS (Domain Name System) to map a domain name to its corresponding IP address and vice versa. Refer to the *Internet Access* chapter for more information.

To change your LAN-Cell's DNS settings, click **REMOTE MGNT**, then the **DNS** tab. The screen appears as shown.

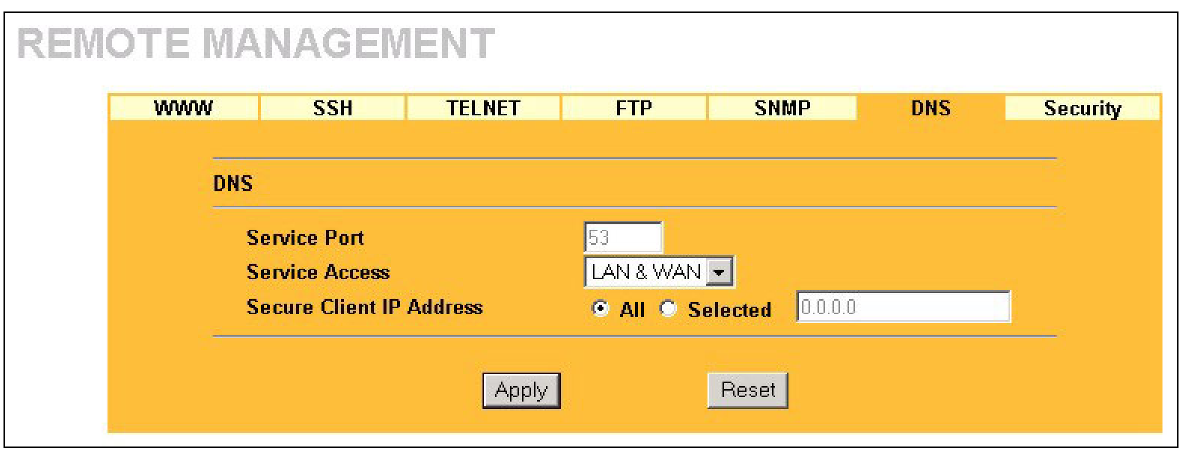



**Figure 15-17 DNS**

The following table describes the fields in this screen.

**Table 15-7 DNS**

| LABEL | DESCRIPTION |
|---|---|
| Service 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.<br>Select **All** to allow any computer to send DNS queries to the LAN-Cell.<br>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 and exit this screen. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 15.16 Configuring Security

To change your LAN-Cell's Security settings, click **REMOTE MGNT**, then the **Security** tab. The screen appears as shown.

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

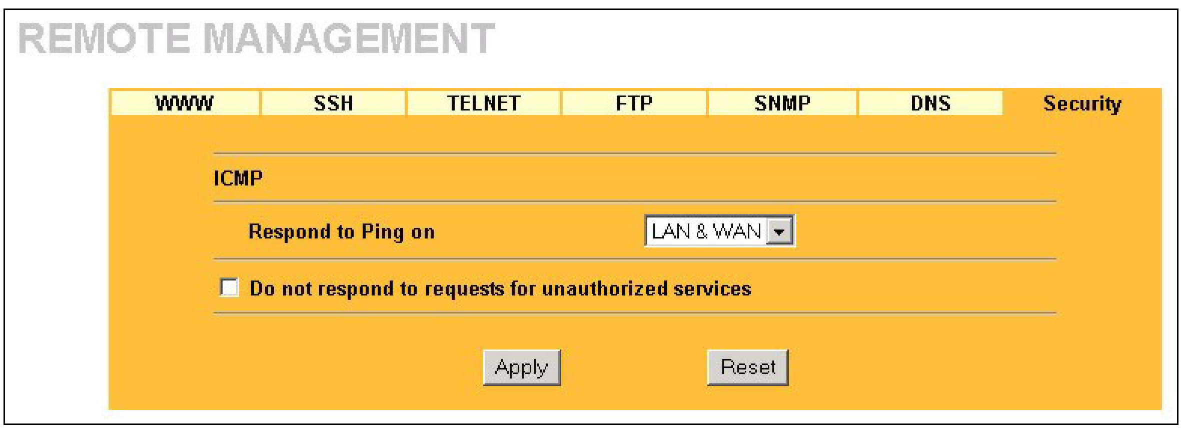



**Figure 15-18 Security**

The following table describes the fields in this screen.

**Table 15-8 Security**

| LABEL | DESCRIPTION |
|---|---|
| ICMP | Internet Control Message Protocol is a message control and error-reporting protocol between a host server and a gateway to the Internet. ICMP uses Internet Protocol (IP) datagrams, but the messages are processed by the TCP/IP software and directly apparent to the application user. |
| Respond to Ping on | The LAN-Cell will not respond to any incoming Ping requests when **Disable** is selected. Select **LAN** to reply to incoming LAN Ping requests**.** Select **WAN** to reply to incoming WAN Ping requests. Otherwise select **LAN & WAN** to reply to both incoming LAN and WAN Ping requests. |

**Table 15-8 Security**

| LABEL | DESCRIPTION |
|---|---|
| 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. By default this option is not selected and 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.<br><br>Note that the probing packets must first traverse the LAN-Cell 's firewall mechanism before reaching this anti-probing mechanism. Therefore if the firewall mechanism blocks a probing packet, the LAN-Cell reacts based on the firewall policy, which by default, is to send a TCP reset packet for a blocked TCP packet. You can use the command "sys firewall tcprst rst [on\|off]" to change this policy. When the firewall mechanism blocks a UDP packet, it drops the packet without sending a response packet. |
| Apply | Click **Apply** to save your customized settings and exit this screen. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

# Part IX:

## Logs

This part provides information and instructions for the logs and reports.

# Chapter 16
# Logs Screens

*This chapter contains information about configuring general log settings and viewing the LAN-Cell's logs. Refer to appendices for example log message explanations.*

## 16.1 Configuring View Log

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 16.2*). Options include logs about system maintenance, system errors, access control, allowed or blocked web sites, blocked web features (such as ActiveX controls, java and cookies), attacks (such as DoS) and IPSec.

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

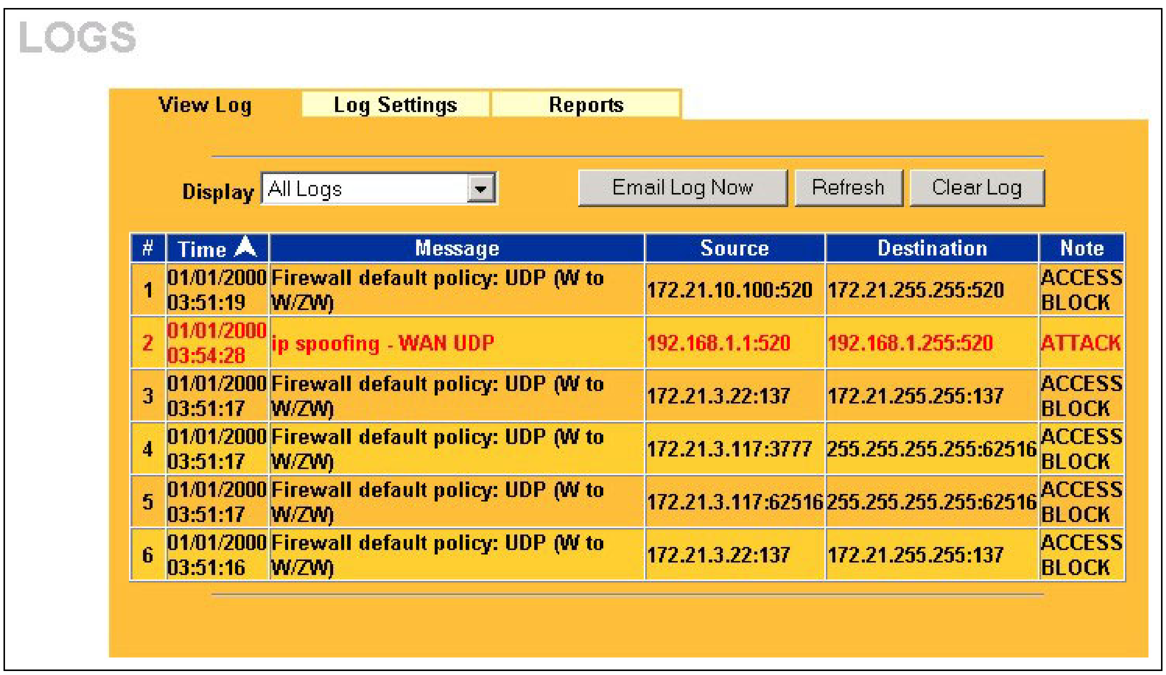



**Figure 16-1 View Log**

The following table describes the labels in this screen.

**Table 16-1 View Log**

| LABEL | DESCRIPTION |
|---|---|
| Display | The categories that you select in the **Log Settings** page (see *section 16.2*) display in the drop-down list box.<br>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. |
| Time | This field displays the time the log was recorded. See the chapter on system maintenance and information 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 **Address Info** fields in **Log Settings**, see *section 16.2*). |
| Refresh | Click **Refresh** to renew the log screen. |
| Clear Log | Click **Clear Log** to delete all the logs. |

## 16.2 Configuring Log Settings

To change your LAN-Cell's log settings, click **LOGS**, then the **Log Settings** tab. 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.

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

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

LOGS

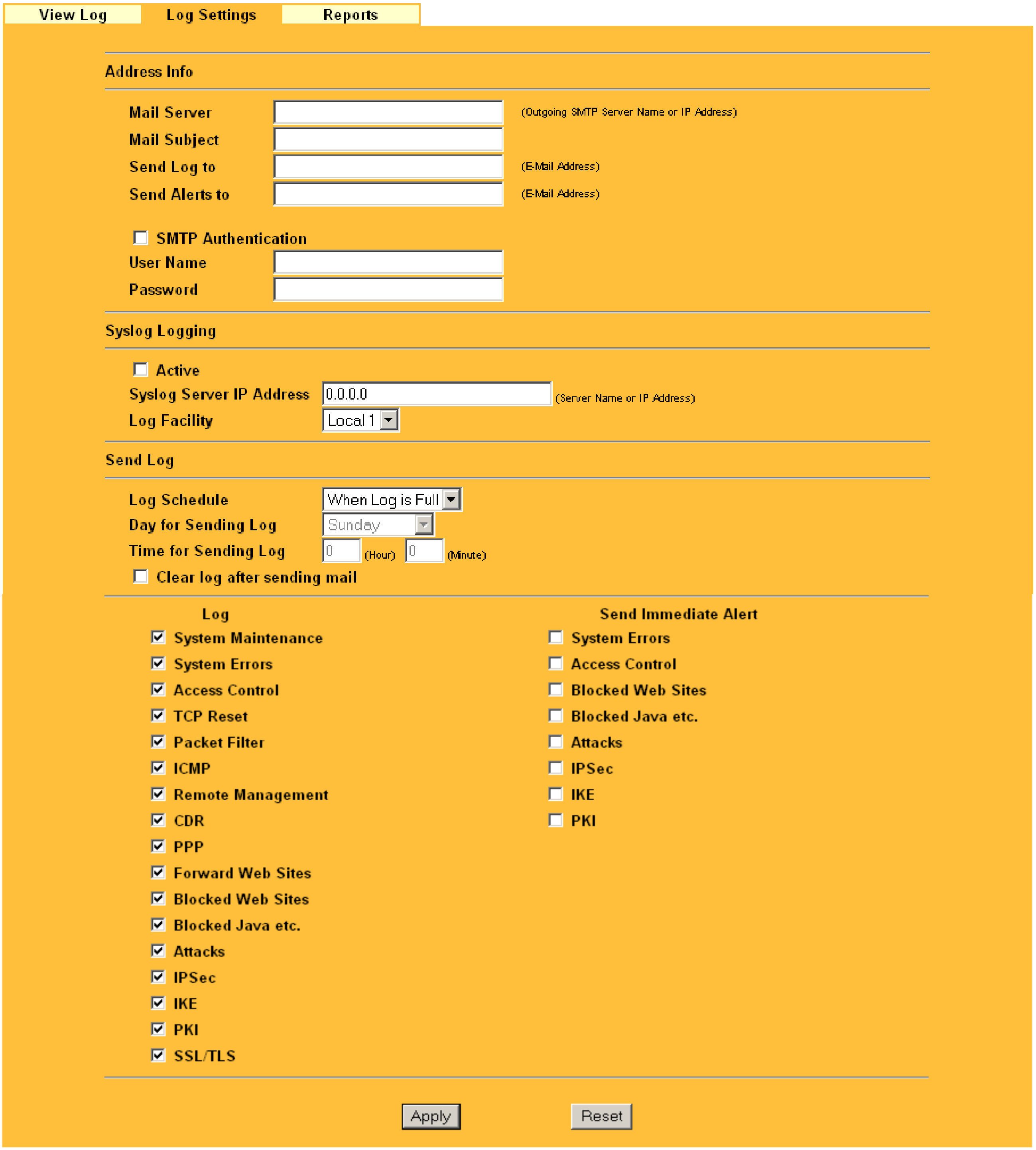



**Figure 16-2 Log Settings**

The following table describes the labels in this screen.

**Table 16-2 Log Settings**

| LABEL | DESCRIPTION |
|---|---|
| Address Info | |
| Mail Server | Enter the server name or the IP address of the mail server for the e-mail addresses specified below. If this field is left blank, logs and alert messages will not be sent via e-mail. |
| Mail Subject | Type a title that you want to be in the subject line of the log e-mail message that the LAN-Cell sends. |
| Send Log To | Logs are sent to the e-mail address specified in this field. If this field is left blank, logs will not be sent via e-mail. |
| Send Alerts To | Alerts are sent to the e-mail address specified in this field. If this field is left blank, alerts will not be sent via e-mail. |
| STMP Authentication | Check this box if your e-mail server requires SMTP Authentication to forward e-mail. |
| Username | Enter the SMTP Username required for SMTP server authentication. |
| Password | Enter the SMTP Password required for SMTP server authentication. |
| Syslog Logging | Syslog logging sends a log to an external syslog server used to store logs. |
| Active | Click **Active** to enable syslog logging. |
| Syslog Server IP Address | Enter the server 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. |
| Send Log | |
| Log Schedule | This drop-down menu is used to configure the frequency of log messages being sent as E-mail:<br>• **Daily**<br>• **Weekly**<br>• **Hourly**<br>• **When Log is Full**<br>• **None.**<br>If you select **Weekly** or **Daily**, specify a time of day when the E-mail should be sent. If you select **Weekly**, then also specify which day of the week the E-mail should be sent. If you select **When Log is Full**, an alert is sent when the log fills up. If you select **None**, no log messages are sent |
| Day for Sending Log | Use the drop down list box to select which day of the week to send the logs. |
| Time for Sending Log | Enter the time of the day in 24-hour format (for example 23:00 equals 11:00 pm) to send the logs. |
| Log | Select the categories of logs that you want to record. Logs include alerts. |
| Send Immediate Alert | Select the categories of alerts for which you want the LAN-Cell to instantly e-mail alerts to the e-mail address specified in the **Send Alerts To** field. |
| Apply | Click **Apply** to save your customized settings and exit this screen. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 16.3 Configuring Reports

To change your LAN-Cell's log reports, click **LOGS**, then the **Reports** tab. The screen appears as shown.

The **Reports** page displays which computers on the LAN send and receive the most traffic, what kinds of traffic are used the most and which web sites are visited the most often. Use the **Reports** screen to have the LAN-Cell record and display the following network usage details:

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

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

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

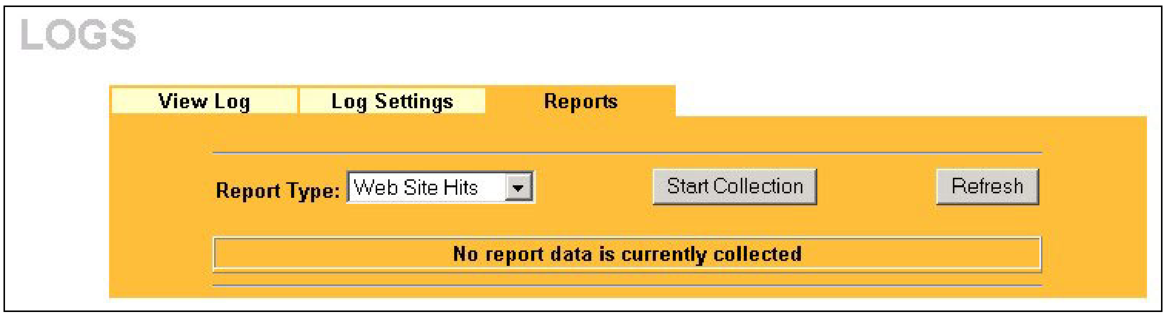



**Figure 16-3 Reports**

**Enabling the LAN-Cell's reporting function decreases the overall throughput by about 1 Mbps.**

The following table describes the labels in this screen.

**Table 16-3 Reports**

| LABEL | DESCRIPTION |
|---|---|
| Report Type | Use the drop-down list box to select the type of reports to display.<br>**Web Site Hits** displays the web sites that have been visited the most often from the LAN and how many times they have been visited.<br>**Protocol/Port** displays the protocols or service ports that have been used the most and the amount of traffic for the most used protocols or service ports.<br>**LAN IP Address** displays the LAN IP addresses to and /or from which the most traffic has been sent and how much traffic has been sent to and from those IP addresses. |
| Start Collection/ Stop Collection | The button text shows **Start Collection** when the LAN-Cell is not recording report data and **Stop Collection** when the LAN-Cell is recording report data.<br>Click **Start Collection** to have the LAN-Cell record report data.<br>Click **Stop Collection** to halt the LAN-Cell from recording more data. |
| Refresh | Click **Refresh** to update the report display. The report also refreshes automatically when you close and reopen the screen. |

**All of the recorded reports data is erased when you turn off the LAN-Cell.**

### 16.3.1 Viewing Web Site Hits

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

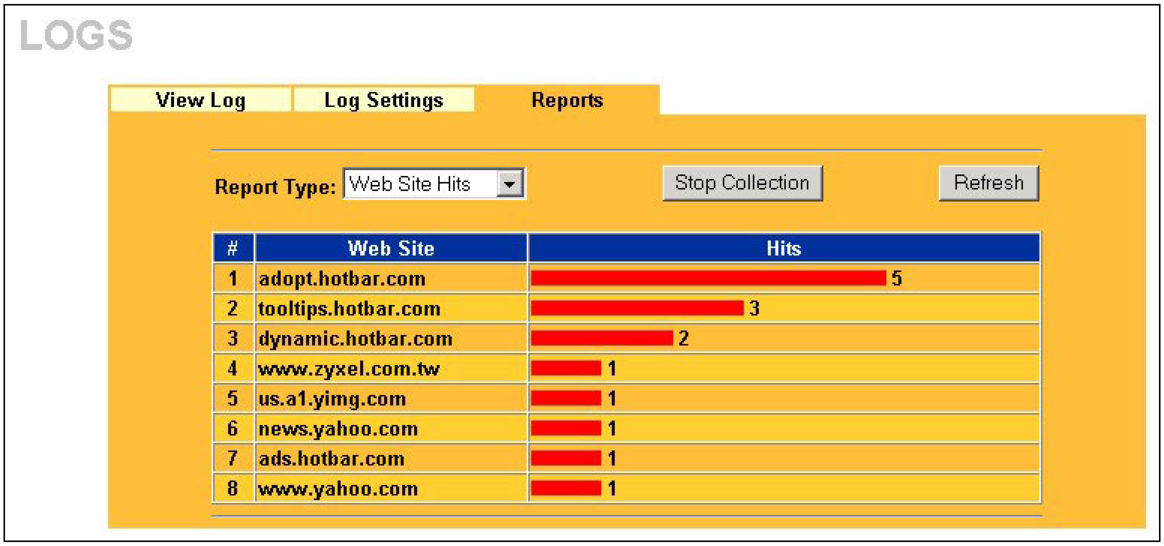



**Figure 16-4 Web Site Hits Report Example**

The following table describes the labels in this screen.

**Table 16-4 Web Site Hits Report**

| LABEL | DESCRIPTION |
|---|---|
| Web Site | This column lists the domain names of the web sites visited most often from computers on the LAN. The names are ranked by the number of visits to each web site and listed in descending order with the most visited web site listed first. The LAN-Cell counts each page viewed in a web site as another hit on the web site. |
| Hits | This column lists how many times each web site has been visited. The count starts over at 0 if a web site passes the hit count limit (see *Table 16-7 Report Specifications*). |

### 16.3.2 Viewing Protocol/Port

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

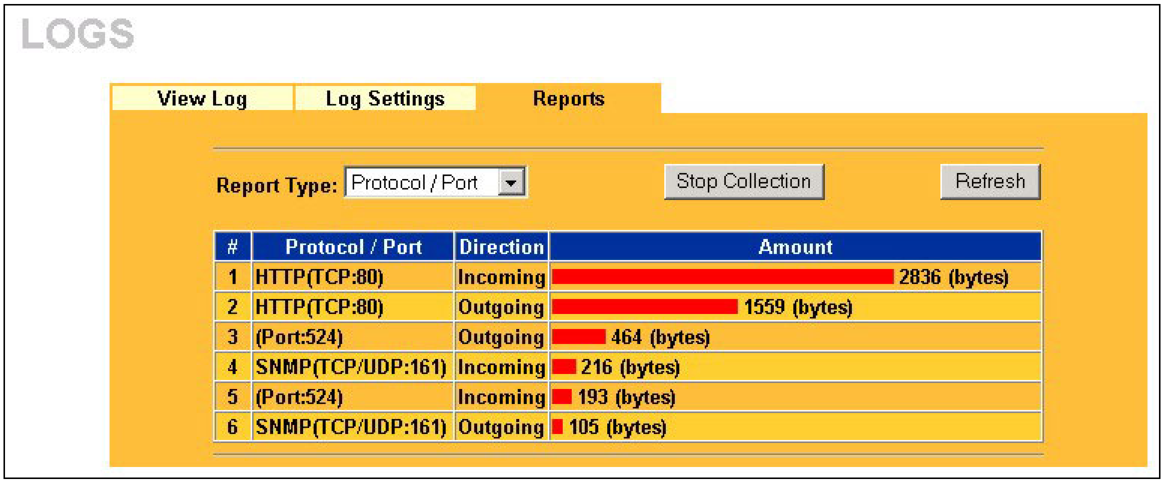



**Figure 16-5 Protocol/Port Report Example**

The following table describes the labels in this screen.

**Table 16-5 Protocol/ Port Report**

| LABEL | DESCRIPTION |
|---|---|
| Protocol/Port | This column lists the protocols or service ports for which the most traffic has gone through the LAN-Cell. The protocols or service ports are listed in descending order with the most used protocol or service port listed first. |
| Direction | This field displays **Incoming** to denote traffic that is coming in from the WAN to the LAN. This field displays **Outgoing** to denote traffic that is going out from the LAN to the WAN. |
| Amount | This column lists how much traffic has been sent and/or received for each protocol or service port. The measurement unit shown (bytes, Kbytes, Mbytes or Gbytes) varies with the amount of traffic for the particular protocol or service port. The count starts over at 0 if a protocol or port passes the bytes count limit (see *Table 16-7 Report Specifications*). |

## 16.3.3 Viewing LAN IP Address

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

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

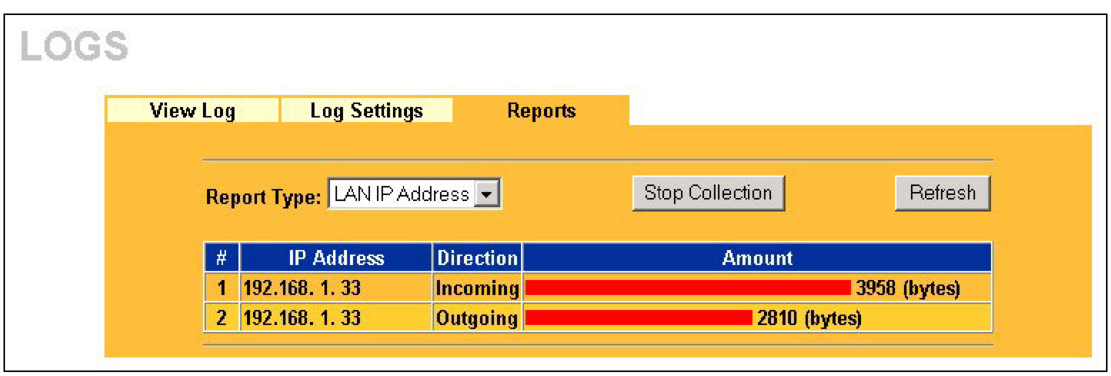



**Figure 16-6 LAN IP Address Report Example**

The following table describes the labels in this screen.

**Table 16-6 LAN IP Address Report**

| LABEL | DESCRIPTION |
|---|---|
| IP Address | This column lists the LAN IP addresses to and/or from which the most traffic has been sent. The LAN IP addresses are listed in descending order with the LAN IP address to and/or from which the most traffic was sent listed first. |
| Direction | This field displays **Incoming** to denote traffic that is coming in from the WAN to the LAN. This field displays **Outgoing** to denote traffic that is going out from the LAN to the WAN. |
| Amount | This column displays how much traffic has gone to and from the listed LAN IP addresses. The measurement unit shown (bytes, Kbytes, Mbytes or Gbytes) varies with the amount of traffic sent to and from the LAN IP address. The count starts over at 0 if the total traffic sent to and from a LAN IP passes the bytes count limit (see *Table 16-7 Report Specifications*). |

## 16.3.4 Reports Specifications

The following table lists detailed specifications on the reports feature.

**Table 16-7 Report Specifications**

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

# Part X:

## Maintenance

This part covers the maintenance screens.

# Chapter 17
# Maintenance

*This chapter displays system information such as firmware, port IP addresses and port traffic statistics.*

## 17.1 Maintenance Overview

The maintenance screens can help you view system information, upload new firmware, manage configuration and restart your LAN-Cell.

## 17.2 Status Screen

Click **MAINTENANCE** to open the **Status** screen, where you can use to monitor your LAN-Cell. Note that these fields are READ-ONLY and only used for diagnostic purposes.

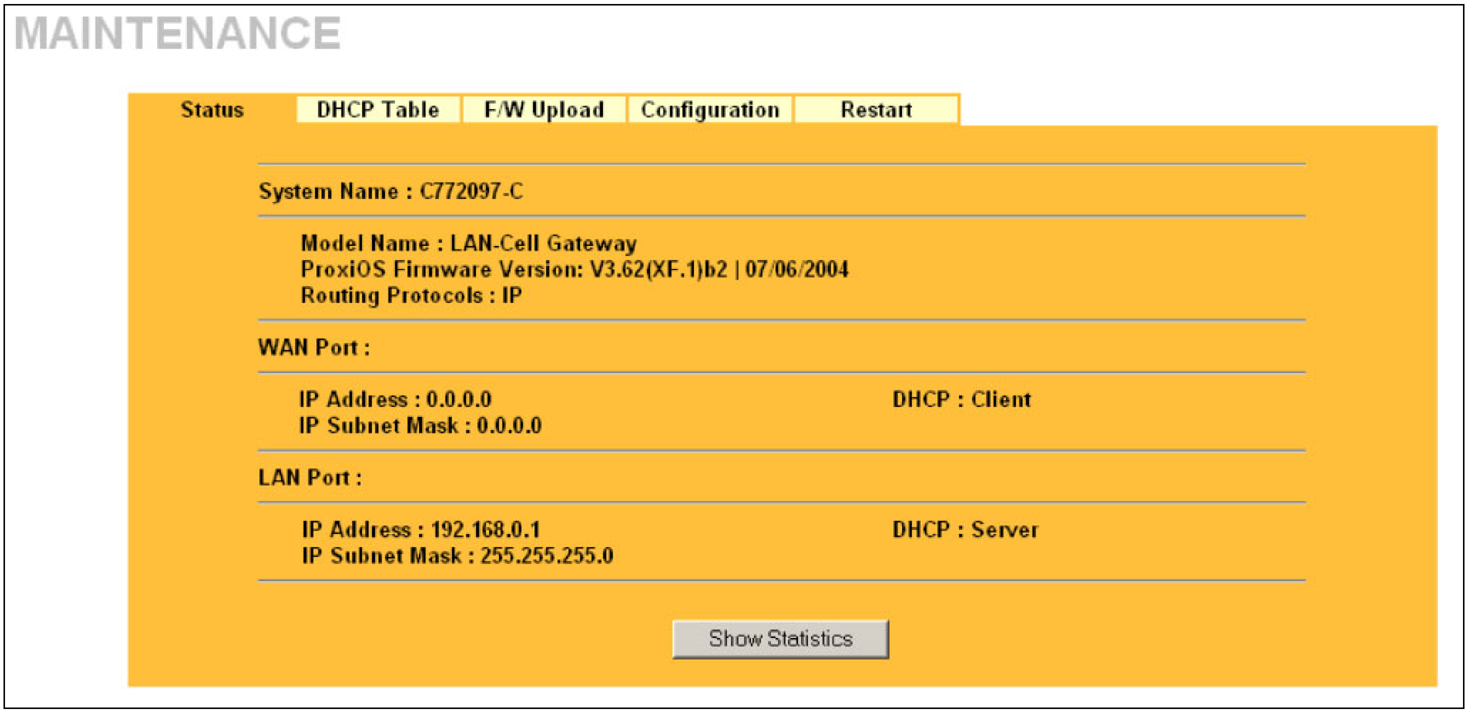



**Figure 17-1 System Status**

The following table describes the labels in this screen.

**Table 17-1 System Status**

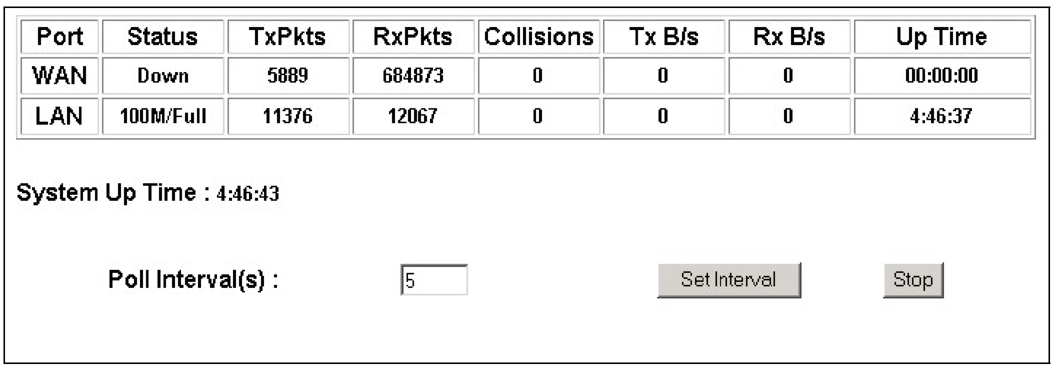
| LABEL | DESCRIPTION |
|---|---|
| System Name | This is the **System Name** you chose in the first Internet Access Wizard screen. It is for identification purposes |
| Model Name | The model name identifies your device type. The model name should also be on a sticker on your device. If you are uploading firmware, be sure to upload firmware for this exact model name. This field is not available on all models. |
| ProxiOS Firmware Version: | This Proxicast's Firmware version and the date created. |
| Routing Protocols | This shows the routing protocol - **IP** for which the LAN-Cell is configured. |
| WAN Port | |
| IP Address | This is the WAN port IP address. |

**Table 17-1 System Status**

| LABEL | DESCRIPTION |
|---|---|
| IP Subnet Mask | This is the WAN port subnet mask. |
| DHCP | This is the WAN port DHCP role - **Client** or **None**. |
| LAN Port | |
| IP Address | This is the LAN port IP address. |
| IP Subnet Mask | This is the LAN port subnet mask. |
| DHCP | This is the LAN port DHCP role – **Server** or **None**. |

## 17.2.1 System Statistics

Read-only information here includes port status and packet specific statistics. Also provided are "system up time" and "poll interval(s)". The **Poll Interval(s)** field is configurable. Note: The System Statistics Screen does not show statistics for the Cellular Modem port.



| Port | Status | TxPkts | RxPkts | Collisions | Tx B/s | Rx B/s | Up Time |
|---|---|---|---|---|---|---|---|
| WAN | Down | 5889 | 684873 | 0 | 0 | 0 | 00:00:00 |
| LAN | 100M/Full | 11376 | 12067 | 0 | 0 | 0 | 4:46:37 |



**Figure 17-2 System Status: Show Statistics**

The following table describes the labels in this screen.

**Table 17-2 System Status: Show Statistics**

| LABEL | DESCRIPTION |
|---|---|
| Port | This is the WAN or LAN port. |
| Status | This displays the port speed and duplex setting if you're using Ethernet encapsulation and **down** (line is down), **idle** (line (ppp) idle), **dial** (starting to trigger a call) and **drop** (dropping a call) if you're using PPPoE encapsulation. |
| TxPkts | This is the number of transmitted packets on this port. |
| RxPkts | This is the number of received packets on this port. |
| Collisions | This is the number of collisions 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. |

**Table 17-2 System Status: Show Statistics**

| LABEL | DESCRIPTION |
|---|---|
| Poll Interval(s) | Enter the time interval for refreshing statistics in this field. |
| Set Interval | Click this button to apply the new poll interval you entered in the **Poll Interval(s)** field. |
| Stop | Click **Stop** to stop refreshing statistics, click **Stop**. |

## 17.3 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 set to **None**, DHCP service will be disabled and you must have another DHCP server on your LAN, or else the computer must be manually configured.

Click **MAINTENANCE**, and then the **DHCP Table** tab. 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 DHCP server.

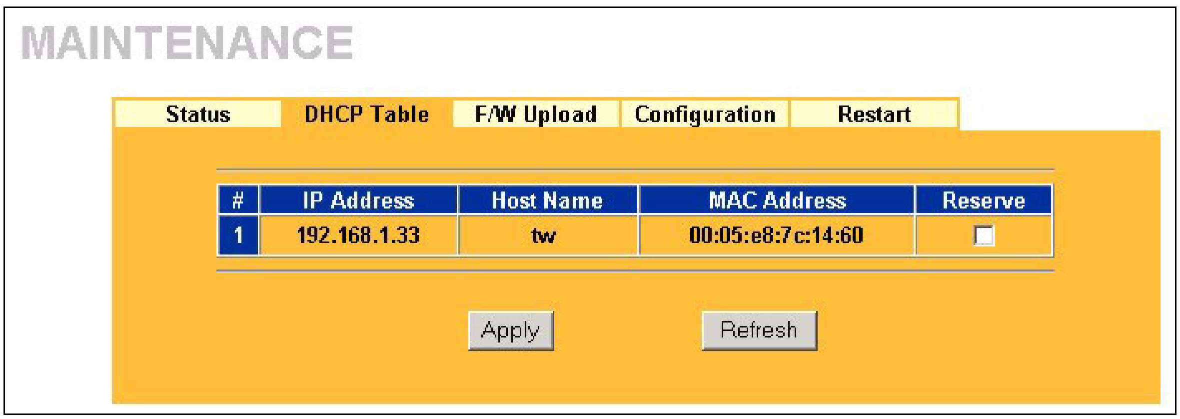



**Figure 17-3 DHCP Table**

The following table describes the labels in this screen.

**Table 17-3 DHCP Table**

| LABEL | DESCRIPTION |
|---|---|
| # | 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 | This field shows the MAC address of the computer with the name in the **Host Name** field.<br>Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02. |
| Refresh | Click **Refresh** to renew the screen. |

## 17.4 F/W Upload Screen

Find firmware at http://www.proxicast.com/ in a file that (usually) uses the system model name with a "*.bin" extension, e.g., "LAN-Cell.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 the *Firmware and Configuration File Maintenance* chapter for upgrading firmware using FTP/TFTP commands.

Click **MAINTENANCE**, and then the **F/W Upload** tab. Follow the instructions in this screen to upload firmware to your LAN-Cell.

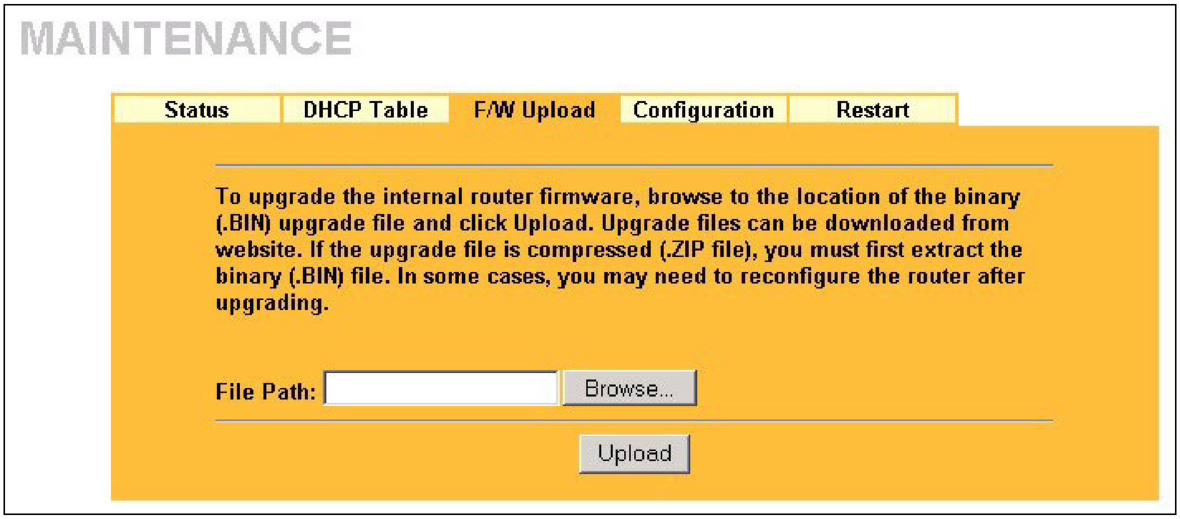



**Figure 17-4 Firmware Upload**

The following table describes the fields in this screen.

**Figure 17-5 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!**

After you see the **Firmware Upload in Process** screen, wait two minutes before logging into the LAN-Cell again.

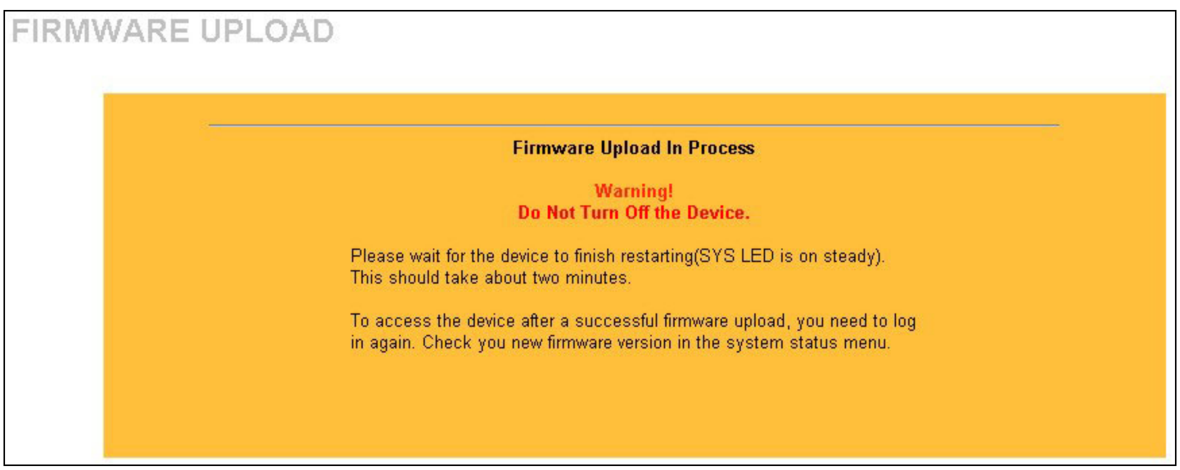



**Figure 17-6 Firmware Upload In Process**

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 17-7 Network Temporarily Disconnected**

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

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

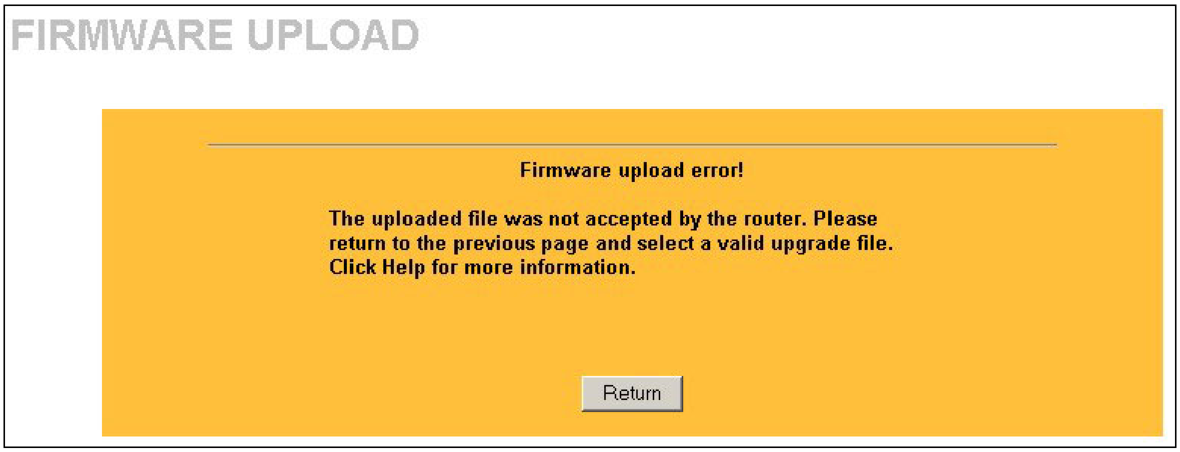



**Figure 17-8 Firmware Upload Error**

## 17.5 Configuration Screen

See the *Firmware and Configuration File Maintenance* chapter for transferring configuration files using FTP/TFTP commands.

Click **MAINTENANCE**, and then the **Configuration** tab. Information related to factory defaults, backup configuration, and restoring configuration appears as shown next.

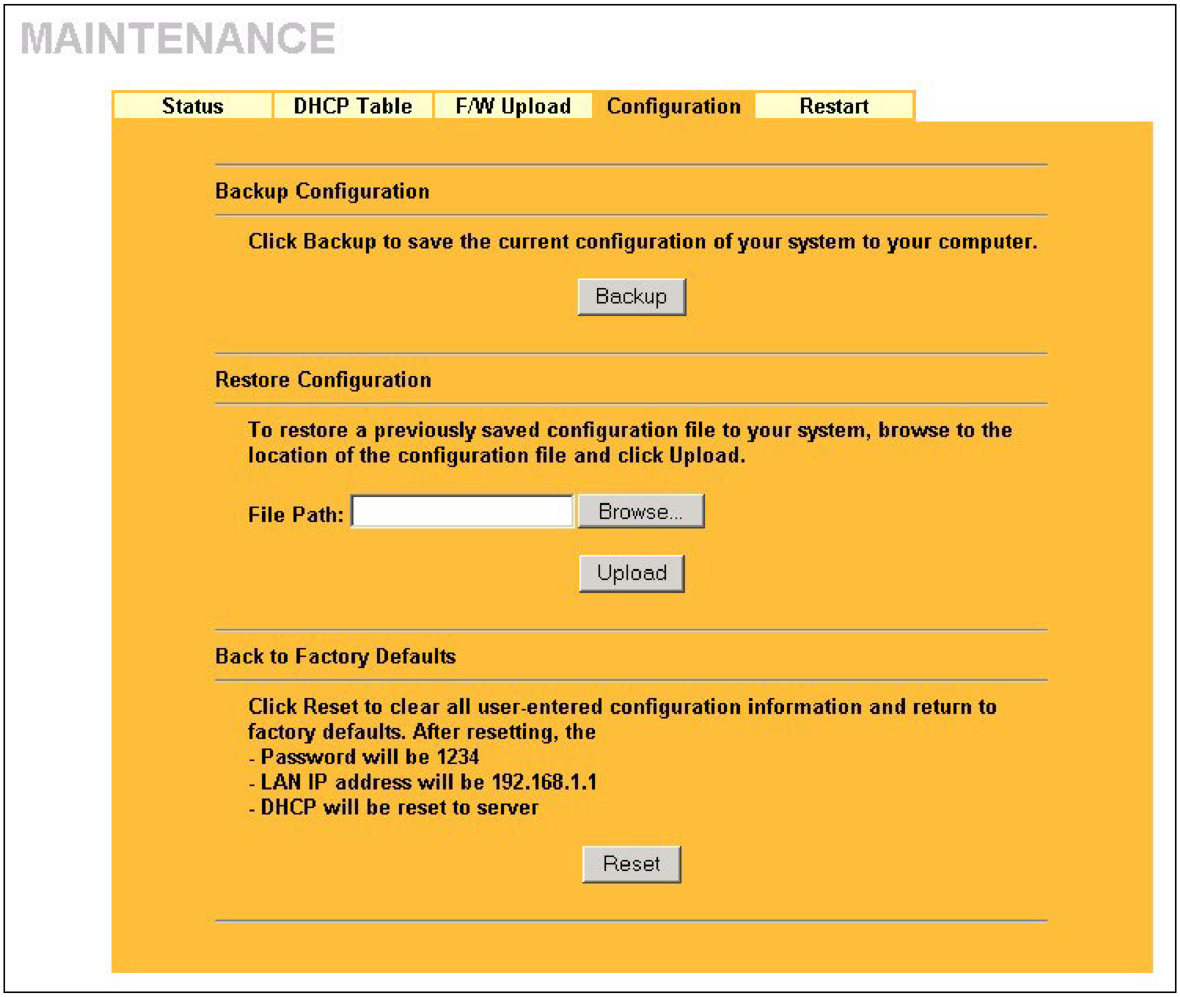



**Figure 17-9 Configuration**

### 17.5.1 Backup Configuration

Backup Configuration allows you to backup (save) the current system (LAN-Cell) configuration to your computer. Backup is highly recommended once your LAN-Cell is functioning properly.

Click **Backup** to save your current LAN-Cell configuration to your computer.

### 17.5.2 Restore Configuration

Restore Configuration allows you to restore a previously saved configuration file from your computer to your LAN-Cell.

**Table 17-4 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 device while configuration file upload is in progress.**

After you see a "configuration upload successful" screen, you must then wait one minute before logging into the device again.

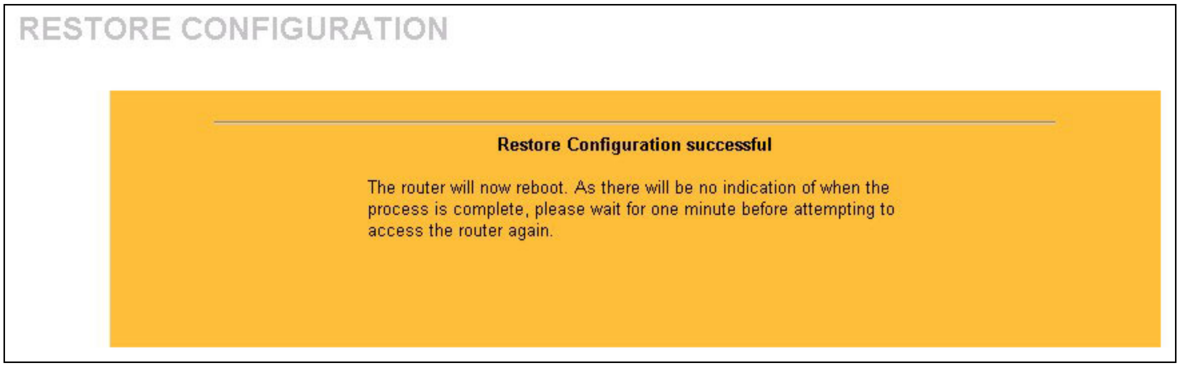



**Figure 17-10 Configuration Upload Successful**

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


**Figure 17-11 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). See your *Quick Start Guide* for details on how to set up your computer's IP address.

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

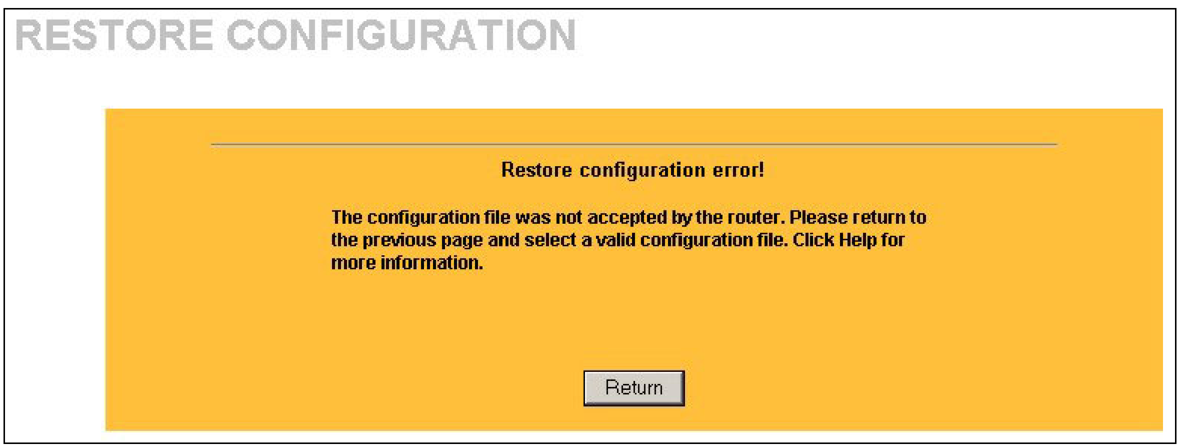



**Figure 17-12 Configuration Upload Error**

## 17.5.3 Back to Factory Defaults

Pressing the **Reset** button in this section clears all user-entered configuration information and returns the LAN-Cell to its factory defaults as shown on the screen. The following warning screen will appear.

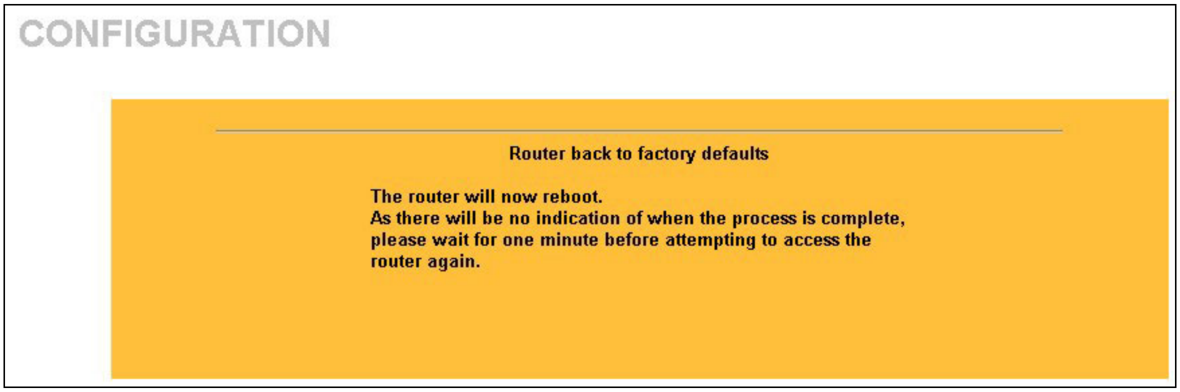



**Figure 17-13 Reset Warning Message**

You can also press the **RESET** button on the front panel for 5 seconds to reset the factory defaults of your LAN-Cell. Refer to the section on resetting the LAN-Cell for more information on the **RESET** button.

## 17.6 Restart Screen

System restart allows you to reboot the LAN-Cell without turning the power off.

Click **MAINTENANCE**, and then **Restart**. Click **Restart** to have the LAN-Cell reboot. This does not affect the LAN-Cell's configuration.

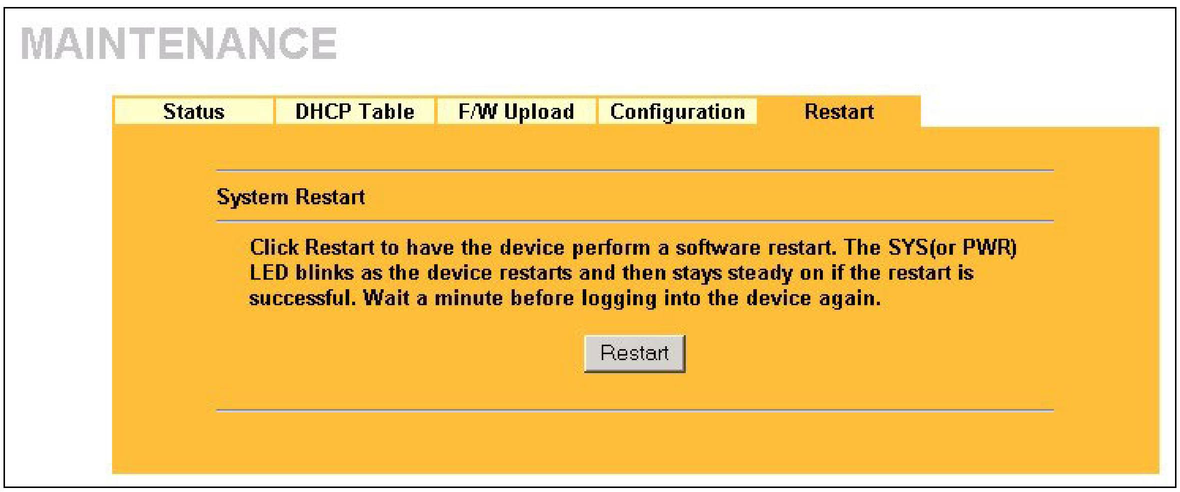



**Figure 17-14 Restart Screen**

# Part XI:

## SMT General Configuration

This part introduces the System Management Terminal and covers the General setup menu, WAN, LAN setup, and Internet access.

**See the web configurator parts of this guide for background information on features configurable by the web configurator and SMT.**

# Chapter 18
# Introducing the SMT

*This chapter explains how to access the System Management Terminal and gives an overview of its menus.*

## 18.1 Introduction to the SMT

The LAN-Cell's SMT (System Management Terminal) is a menu-driven interface that you can access over a telnet connection.

## 18.2 Accessing the SMT via Telnet

Make sure you have the physical connection properly set up as described in the hardware installation chapter.

Using Telnet client software on either computer attached the one of the LAN-Cell's LAN ports, or remotely via a WAN connection, initiate a Telnet session to the LAN-Cell's assigned IP address (or hostname if using DDNS). The default Telnet port is 23, but may be changed via the Remote Management configuration menus.

### 18.2.1 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.

```
Enter Password : XXXX
```

**Figure 18-1 Password Screen**

## 18.3 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 18-1 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. |
| 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. |

**Table 18-1 Main Menu Commands**

| OPERATION | KEYSTROKES | DESCRIPTION |
|---|---|---|
| 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. |
| Exit the SMT | Type 99, then press [ENTER]. | Type 99 at the main menu prompt and press [ENTER] to exit the SMT interface. |

## 18.3.1 Main Menu

After you enter the password, the SMT displays the **LAN-Cell Main Menu**, as shown next.

```
                    Copyright (c) 1994 - 2003 Proxicast

                           LAN-Cell 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. Internet Access Setup            24. System Maintenance
                                          26. Schedule Setup
                                          27. VPN/IPSec Setup

    Advanced Applications
      11. Remote Node Setup
      12. Static Routing Setup
      15. NAT Setup

                                          99. Exit

                      Enter Menu Selection Number:
```

**Figure 18-2 Main Menu**

We use the LAN-Cell Model 1xMG-401 menus in this guide as an example. The SMT menus for your model may vary slightly for different LAN-Cell models.  Not all LAN-Cell models contain the same features – some menu items may not be present in your specific model, but menu numbers are consistent across models to aid in user familiarity and scripting support.

The following table describes the fields in this screen.

**Table 18-2 Main Menu Summary**

| NO. | Menu Title | FUNCTION |
|---|---|---|
| 1 | General Setup | Use this menu to set up 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. |
| 3 | LAN Setup | Use this menu to apply LAN filters, configure LAN DHCP and TCP/IP settings. |
| 4 | Internet Access Setup | Configure your Internet Access setup (Internet address, gateway, login, etc.) with this menu. |

**Table 18-2 Main Menu Summary**

| NO. | Menu Title | FUNCTION |
|---|---|---|
| 11 | Remote Node 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, activate/deactivate the firewall and view the firewall log. |
| 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 and access to the Command Line Interface (sub-option #8) |
| 26 | Schedule Setup | Use this menu to schedule outgoing calls. |
| 27 | VPN/IPSec Setup | Use this menu to configure and maintain a VPN connection. |
| 99 | Exit | Use this menu to exit (necessary for remote configuration). |

## 18.4 Changing the System Password

Change the system password by following the steps shown next.

**Step 1.** Enter 23 in the main menu to open **Menu 23 - System Password** as shown next.

```
                 Menu 23 - System Password

         Old Password= ?
         New Password= ?
         Retype to confirm= ?



          Enter here to CONFIRM or ESC to CANCEL:
```

**Figure 18-3 Menu 23: System Password**

**Step 2.** Type your existing password and press [ENTER].

**Step 3.** Type your new system password and press [ENTER].

**Step 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.

## 18.5 Resetting the LAN-Cell

See the chapter that introduces the web configurator for directions on resetting the LAN-Cell.

# Chapter 19
# SMT Menu 1 - General Setup

***Menu 1 - General Setup** contains administrative and system-related information.*

## 19.1 Introduction to General Setup

**Menu 1 - General Setup** contains administrative and system-related information.

## 19.2 Configuring General Setup

**Step 1.** Enter 1 in the main menu to open **Menu 1: General Setup**.

**Step 2.** The **Menu 1 - General Setup** screen appears, as shown next. Fill in the required fields.

```
              Menu 1 - General Setup

     System Name=
     Domain Name=
     First System DNS Server= From ISP
       IP Address= N/A
     Second System DNS Server= From ISP
       IP Address= N/A
     Third System DNS Server= From ISP
       IP Address= N/A
     Edit Dynamic DNS= No


     Press ENTER to Confirm or ESC to Cancel:
```

**Figure 19-1 Menu 1: General Setup**

The following table describes the fields in this screen.

**Table 19-1 Menu 1: General Setup**

| FIELD | DESCRIPTION | EXAMPLE |
|---|---|---|
| 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-01** |
| 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.<br>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]. | |
| First System DNS Server<br>Second System DNS Server<br>Third System DNS Server | Press [SPACE BAR] to select **From ISP**, **User Defined** or **None** and press [ENTER]. | **From ISP** |
| 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. | **No** (default) |

**Table 19-1 Menu 1: General Setup**

| FIELD | DESCRIPTION | EXAMPLE |
|---|---|---|
| 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. | | |

## 19.2.1 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). Not all models have every field shown.

```
                    Menu 1.1 - Configure Dynamic DNS

     Service Provider= WWW.DynDNS.ORG
     Active= No
     DDNSType= DynamicDNS
     Host1=
     Host2=
     Host3=
     USER=
     Password= ********
     Enable Wildcard= No
     Offline= N/A
     Edit Update IP Address:
       Use Server Detected IP= No
       User Specified IP Address= No
       IP Address= N/A

                    Press ENTER to Confirm or ESC to Cancel:
```

**Figure 19-2 Configure Dynamic DNS**

Follow the instructions in the next table to configure Dynamic DNS parameters.

**Table 19-2 Configure Dynamic DNS**

| FIELD | DESCRIPTION | EXAMPLE |
|---|---|---|
| Service Provider | This is the name of your Dynamic DNS service provider. | WWW.DynDNS.ORG (default) |
| Active | Press [SPACE BAR] to select **Yes** and then press [ENTER] to make dynamic DNS active. | **Yes** |
| DDNS Type | Press [SPACE BAR] and then [ENTER] to select **DynamicDNS** if you have a dynamic IP address(es). Select **StaticDNS** if you have a static IP address(s).<br>Select **CustomDNS** to have dyns.org provide DNS service for a domain name that you already have from a source other than dyndns.org. | **DynamicDNS** (default) |
| Host1-3 | Enter your host name(s) in the fields provided. You can specify up to two host names separated by a comma in each field. | me.dyndns.org |
| USER | Enter your user name. | |
| Password | Enter the password assigned to you. | |
| Enable Wildcard | 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. | **No** |
| Offline | 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). | **Yes** |

**Table 19-2 Configure Dynamic DNS**

| FIELD | DESCRIPTION | EXAMPLE |
|---|---|---|
| Edit Update IP Address:<br>You can select **Yes** in either the **Use Server Detected IP** field or the **User Specified IP Address** field, but not both.<br>With the **Use Server Detected IP** and **User Specified IP Address** 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.<br>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. | | |
| Use Server Detected IP | Press [SPACE BAR] to select **Yes** and then press [ENTER] to have the DDNS server automatically update the IP address of the host name(s) with the public IP address that the LAN-Cell uses or is behind.<br>You can set this field to **Yes** whether the IP address is public or private, static or dynamic. | **Yes** |
| User Specified IP Address | 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.<br>Only select **Yes** if the LAN-Cell uses or is behind a static public IP address. | **No** |
| IP Address | Enter the static public IP address if you select **Yes** in the **User Specified IP Address** field. | **N/A** |
| 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.

# Chapter 20
# WAN and Cellular Modem Setup

*This chapter describes how to configure the WAN using menu 2 and the Cellular Modem using menus 2.1 and 11.1.*

## 20.1 Introduction to WAN

This chapter explains how to configure settings for your WAN port.

From the main menu, enter 2 to open menu 2.

```
                    Menu 2 - WAN Setup

               MAC Address:
                 Assigned By= Factory default
                 IP Address= N/A

               Cellular Modem:
                 Active= No
                 Phone Number=
                 Port Speed= 9600
                 AT Command String:
                   Init=
                 Edit Advanced Setup= No

           Press ENTER to Confirm or ESC to Cancel:
```

**Figure 20-1 MAC Address Cloning in WAN Setup**

The following table describes the fields in this screen.

**Table 20-1 MAC Address Cloning in WAN Setup**

| FIELD | DESCRIPTION | EXAMPLE |
|---|---|---|
| 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 workstation whose IP you give in the following field. | **IP address attached on LAN** |
| 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. | 192.168.1.35 |
| 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. | | |

## 20.2 Cellular Modem

The Cellular Modem can be configured as the primary WAN interface or it may used in reserve, as a traditional dial-up connection should the broadband connection to the WAN port fail. To set up the Cellular Modem for use in the event that the regular WAN connection is dropped, first make sure you have set up the switch and port connection (see the *Quick Start Guide*), then configure

1. Menu 2 - WAN Setup,
2. Menu 2.1 - Advanced WAN Setup and
3. Menu 11.1 - Remote Node Profile (Cellular ISP) as shown next

Refer also to the traffic redirect section for information on an alternate backup WAN connection.

## 20.3 Configuring Cellular Modem in Menu 2

From the main menu, enter 2 to open menu 2.

```
                    Menu 2 - WAN Setup

              MAC Address:
                Assigned By= Factory default
                IP Address= N/A

              Cellular Modem:
                Active= No
                Phone Number=
                Port Speed= 115200
                AT Command String:
                  Init=
                Edit Advanced Setup= No

         Press ENTER to Confirm or ESC to Cancel:
```

**Figure 20-2 Menu 2: Cellular Modem Setup**

The following table describes the fields in this menu.

**Table 20-2 Menu 2: Cellular Modem Setup**

| FIELD | DESCRIPTION | EXAMPLE |
|---|---|---|
| Cellular Modem: | | |
| Active | Use this field to turn the Cellular Modem feature on (**Yes**) or off (**No**). | **No** |
| Phone Number | Enter the telephone number assigned to your line by your telephone company. This field only accepts digits; do not include dashes and spaces. | #777 |
| Port Speed | The port speed to the Cellular Modem is fixed at 115200. Do not change this value unless instructed to do so by Proxicast Technical Support. | **115200** |
| AT Command String: | | |
| Init | Enter the AT command string to initialize the WAN device. Consult the manual of your WAN device connected to your Cellular Modem port for specific AT commands. | at&fs0=0 |
| Edit Advanced Setup | To edit the advanced setup for the Cellular Modem 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**. | **Yes** |
| 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. | | |

## 20.4 Advanced WAN Setup

To edit the advanced setup for the Cellular Modem 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].

```
                    Menu 2.1 - Advanced WAN Setup

  AT Command Strings:                    Call Control:
    Dial=                                  Dial Timeout(sec)= 0
    Drop=                                  Retry Count= 0
    Answer=                                Retry Interval(sec)= N/A
                                           Drop Timeout(sec)= 0
  Drop DTR When Hang Up= No                Call Back Delay(sec)= 0

  AT Response Strings:
    CLID=
    Called Id=
    Speed=


                   Press ENTER to Confirm or ESC to Cancel:
```

**Figure 20-3 Menu 2.1 Advanced WAN Setup**

The following table describes fields in this menu.

**Table 20-3 Advanced WAN Port Setup: AT Commands Fields**

| FIELD | DESCRIPTION | DEFAULT |
|---|---|---|
| AT Command Strings: | | |
| Dial | Enter the AT Command string to make a call. | atdt |
| 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. | +++ath |
| Answer | Enter the AT Command string to answer a call. | ata |
| 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. Do not change this value unless instructed to do so by Proxicast Technical Support. | YES |
| 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. | NMBR = |
| Called Id | Enter the keyword preceding the dialed number. | TO |
| Speed | Enter the keyword preceding the connection speed. | CONNECT |

**Table 20-4 Advanced WAN Port Setup: Call Control Parameters**

| FIELD | DESCRIPTION | DEFAULT |
|---|---|---|
| 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. | 60 seconds |
| Retry Count | Enter a number of times for the LAN-Cell to retry a busy or no-answer phone number before blacklisting the number. | 0 to disable the blacklist control |
| 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. | |

**Table 20-4 Advanced WAN Port Setup: Call Control Parameters**

| FIELD | DESCRIPTION | DEFAULT |
|---|---|---|
| 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. | 20 seconds |
| 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. | 15 seconds |

## 20.5 Remote Node Profile (Cellular ISP)

Enter **2** in **Menu 11 Remote Node Setup** to open **Menu 11.1 Remote Node Profile (Cellular ISP)** (shown below) and configure the setup for your Cellular Modem port connection.

```
                Menu 11.1 - Remote Node Profile (Cellular ISP)

   Rem Node Name= ?                    Edit PPP Options= No
   Active= Yes                         Rem IP Addr= ?
                                       Edit IP= No
   Outgoing:                           Edit Script Options= No
     My Login=
     My Password= ********             Telco Option:
     Retype to Confirm= ********         Allocated Budget(min)= 0
     Authen= CHAP/PAP                      Period(hr)= 0
     Pri Phone #= ?                      Nailed-Up Connection= No
     Sec Phone #=
                                       Session Options:
                                         Edit Filter Sets= No
                                         Idle Timeout(sec)= 100


                  Press ENTER to Confirm or ESC to Cancel:
```

**Figure 20-4 Menu 11.1 Remote Node Profile (Cellular ISP)**

The following table describes the fields in this menu.

**Table 20-5 Menu 11.1 Remote Node Profile (Cellular ISP)**

| FIELD | DESCRIPTION | EXAMPLE |
|---|---|---|
| Rem Node Name | Enter a descriptive name for the remote node. This field can be up to eight characters. | LAoffice |
| Active | Press [SPACE BAR] and then [ENTER] to select **Yes** to enable the remote node or **No** to disable the remote node. | **Yes** |
| Outgoing | | |
| My Login | Enter the login name assigned by your ISP for this remote node. | jim |
| 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.<br>Options for this field are:<br>**CHAP**/**PAP** - Your LAN-Cell will accept either **CHAP** or **PAP** when requested by this remote node.<br>**CHAP** - accept CHAP only.<br>**PAP** - accept PAP only. | **CHAP/PAP** |

**Table 20-5 Menu 11.1 Remote Node Profile (Cellular ISP)**

| FIELD | DESCRIPTION | EXAMPLE |
|---|---|---|
| Pri Phone #<br>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 cellular systems require dialing the pound sign # before the phone number. Include a # symbol at the beginning of the phone numbers as required. | #777 |
| Edit PPP Options | Move the cursor to this field and use the space bar to select [Yes] and press [Enter] to edit the PPP options for this remote node. This brings you to Menu 11.2 - Remote Node PPP Options (see *section 20.6*). | **No** (default) |
| Rem IP Addr | Leave the field set to 0.0.0.0 (default) if the remote gateway has a dynamic IP address. Enter the remote gateway's IP address here if it is static. | 0.0.0.0 (default) |
| Edit IP | This field leads to a "hidden" menu. Press [SPACE BAR] to select **Yes** and press [ENTER] to go to M**enu 11.3 - Remote Node Network Layer Options**. See *section 20.7* for more information. | **No** (default) |
| Edit Script Options | Press [SPACE BAR] to select **Yes** and press [ENTER] to edit the AT script for the Cellular Modem remote node (**Menu 11.4 - Remote Node Script**). See *section 20.8* for more information. | **No** (default) |
| 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. | 0 (default) |
| 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). | 0 (default) |
| Nailed-Up Connection | Press [SPACE BAR] to select **Yes** to set this connection to always be on, regardless of whether or not there is any traffic. Select **No** to have this connection act as a dial-up connection. | **No** (default) |
| Session Options | | |
| Edit Filter sets | This field leads to another "hidden" menu. Use [SPACE BAR] to select **Yes** and press [ENTER] to open menu 11.5 to edit the filter sets. See *section 20.9* for more details. | **No** (default) |
| 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. | 100 seconds (default) |
| 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. | | |

## 20.6 Editing PPP Options

The LAN-Cell's dial back-up feature uses PPP. To edit the remote node PPP Options, move the cursor to the **[Edit PPP Options]** field in Menu 11.1 - Remote Node Profile, and use the space bar to select **[Yes].** Press [Enter] to open Menu 11.2 as shown next.

```
                Menu 11.2 - Remote Node PPP Options

           Encapsulation= Standard PPP
           Compression= No



            Enter here to CONFIRM or ESC to CANCEL:
```

**Figure 20-5 Menu 11.2: Remote Node PPP Options**

This table describes the Remote Node PPP Options Menu, and contains instructions on how to configure the PPP options fields.

**Figure 20-6 Menu 11.2: Remote Node PPP Options**

| FIELD | DESCRIPTION | EXAMPLE |
|---|---|---|
| Encapsulation | Press [SPACE BAR] and then [ENTER] to select **CISCO PPP** if your Cellular Modem WAN device uses Cisco PPP encapsulation, otherwise select **Standard PPP**. | **Standard PPP** (default) |
| Compression | Press [SPACE BAR] and then [ENTER] to select **Yes** to enable or **No** to disable Stac compression. | **No** (default) |
| 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. | | |

## 20.7 Editing TCP/IP Options

Move the cursor to the **Edit IP** field in menu 11.1, then press [SPACE BAR] to select **Yes**. Press [ENTER] to open **Menu 11.3 - Remote Node Network Layer Options**.

```
Menu 11.3 - Remote Node Network Layer Options

  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
  Metric= 15
  Private= No
  RIP Direction= None
    Version= N/A
  Multicast= None


   Enter here to CONFIRM or ESC to CANCEL:
```

**Figure 20-7 Menu 11.3: Remote Node Network Layer Options**

The following table describes the fields in this menu.

**Table 20-6 Menu 11.3: Remote Node Network Layer Options**

| FIELD | DESCRIPTION | EXAMPLE |
|---|---|---|
| Rem IP Address | Leave this field set to 0.0.0.0 to have the ISP or other remote router dynamically (automatically) send its IP address if you do not know it. Enter the remote gateway's IP address here if you know it (static). | 0.0.0.0 (default) |
| Rem Subnet Mask | Leave this field set to 0.0.0.0 to have the ISP or other remote router dynamically send its subnet mask if you do not know it. Enter the remote gateway's subnet mask here if you know it (static). | 0.0.0.0 (default) |
| 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).<br>This is the address assigned to your local LAN-Cell, not the remote router. | 0.0.0.0 (default) |

**Table 20-6 Menu 11.3: Remote Node Network Layer Options**

| FIELD | DESCRIPTION | EXAMPLE |
|---|---|---|
| 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).<br>Press [SPACE BAR] and then [ENTER] to select either **Full Feature, None** or **SUA Only.**<br>Choose **None** to disable NAT**.**<br>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**.<br>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!<br>See the Network Address Translation (NAT) chapter for a full discussion on this feature. | **None** (default) |
| 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. | 2 |
| 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. | **No** (default) |
| RIP Direction | Press [SPACE BAR] and then [ENTER] to select the **RIP Direction** from **Both/ None/In Only**/**Out Only** and **None**. | **Both** (default) |
| Version | Press [SPACE BAR] and then [ENTER] to select the RIP version from **RIP-1/RIP-2B/RIP-2M.** | **RIP-1** |
| 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 the LAN Setup chapter for more information on this feature. | **None** (default) |
| 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. | | |

## 20.8 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.

```
                    Menu 11.4 - 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:
```

**Figure 20-8 Menu 11.4: Remote Node Script**

The following table describes the fields in this menu.

**Table 20-7 Menu 11.4: Remote Node Script**

| FIELD | DESCRIPTION | EXAMPLE |
|---|---|---|
| Active | Press [SPACE BAR] and then [ENTER] to select either **Yes** to enable the AT strings or **No** to disable them. | **No** (default) |
| 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. | 0.0.0.0 |

## 20.9 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 11.5 - Remote Node Filter**.

Use menu 11.5 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 the *Filters* chapter for more information on defining the filters.

```
                    Menu 11.5 - 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:
```

**Figure 20-9 Menu 11.5: Cellular Modem Remote Node Filter**

# Chapter 21
# LAN Setup

*This chapter describes how to configure the LAN using **Menu 3: LAN Setup**.*

## 21.1 Introduction to LAN Setup

This chapter describes how to configure the LAN-Cell for LAN connections.

## 21.2 Accessing the LAN Menus

From the main menu, enter 3 to open **Menu 3 – LAN Setup**.

```
                    Menu 3 - LAN Setup

          1. LAN Port Filter Setup
          2. TCP/IP and DHCP Setup


          5. Wireless LAN Setup


               Enter Menu Selection Number:
```

**Figure 21-1 Menu 3: LAN Setup**

## 21.3 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.

```
               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:
```

**Figure 21-2 Menu 3.1: LAN Port Filter Setup**

## 21.4 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.

```
                    Menu 3 - LAN Setup

          1. LAN Port Filter Setup
          2. TCP/IP and DHCP Setup




               Enter Menu Selection Number:
```

**Figure 21-3 Menu 3: TCP/IP and DHCP Setup**

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.

```
                 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= 32           IP Subnet Mask= 255.255.255.0
First DNS Server= From ISP             RIP Direction= Both
  IP Address= N/A                        Version= RIP-1
Second DNS Server= From ISP            Multicast= None
  IP Address= N/A                      Edit IP Alias= No
Third DNS Server= From ISP
  IP Address= N/A

                   Press ENTER to Confirm or ESC to Cancel:
```

Size of the IP Pool

IP addresses of the DNS servers

**Figure 21-4 Menu 3.2: TCP/IP and DHCP Ethernet Setup**

Follow the instructions in the next table on how to configure the DHCP fields.

**Table 21-1 DHCP Ethernet Setup Menu Fields**

| FIELD | DESCRIPTION | EXAMPLE |
|---|---|---|
| DHCP | This field enables/disables the DHCP server.<br>If set to **Server**, your LAN-Cell will act as a DHCP server.<br>If set to **None**, the DHCP server will be disabled.<br><br>When set to **Server**, the following items need to be set: | **Server** |
| Client IP Pool: | | |
| Starting Address | This field specifies the first of the contiguous addresses in the IP address pool. | 192.168.1.33 |
| Size of Client IP Pool | This field specifies the size, or count of the IP address pool. | 32 |
| First DNS Server<br>Second DNS Server<br>Third DNS Server | Press [SPACE BAR] to select **From ISP**, **User Defined**, **DNS Relay** or **None** and press [ENTER].<br>The DNS servers are passed to the DHCP clients along with the IP address and the subnet mask | **From ISP** |

Use the instructions in the following table to configure TCP/IP parameters for the LAN port.

**Table 21-2 LAN TCP/IP Setup Menu Fields**

| FIELD | DESCRIPTION | EXAMPLE |
|---|---|---|
| TCP/IP Setup: | | |
| IP Address | Enter the IP address of your LAN-Cell in dotted decimal notation | 192.168.1.1 (default) |
| 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. | 255.255.255.0 |
| RIP Direction | Press [SPACE BAR] and then [ENTER] to select the RIP direction. Options are: **Both**, **In Only**, **Out Only** or **None**. | **Both** (default) |
| Version | Press [SPACE BAR] and then [ENTER] to select the RIP version. Options are: **RIP-1**, **RIP-2B** or **RIP-2M**. | **RIP-1** (default) |
| 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. | **None** |
| 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 | **Yes** |
| 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. | | |

## 21.4.1 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.

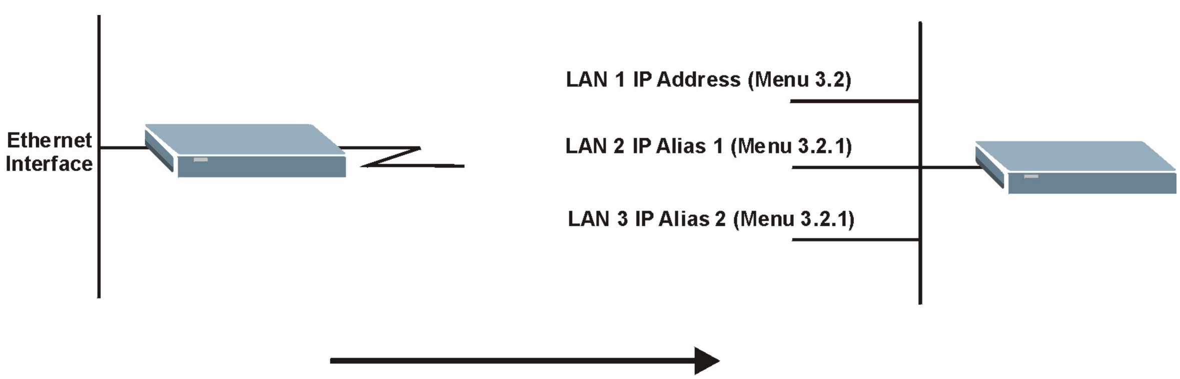



**Figure 21-5 Partitioned Logical Network**

You must 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 configure the second and third network.

Press [ENTER] to open **Menu 3.2.1 - IP Alias Setup**, as shown next.

```
Menu 3.2.1 - 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:
```

**Figure 21-6 Menu 3.2.1: IP Alias Setup**

Use the instructions in the following table to configure IP Alias parameters.

**Table 21-3 Menu 3.2.1: IP Alias Setup**

| FIELD | DESCRIPTION | DEFAULT |
|---|---|---|
| IP Alias 1, 2 | Choose **Yes** to configure the LAN network for the LAN-Cell. | **Yes** |
| IP Address | Enter the IP address of your LAN-Cell in dotted decimal notation. | 192.168.2.1 |
| 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. | 255.255.255.0 |
| RIP Direction | Press [SPACE BAR] and then [ENTER] to select the RIP direction. Options are **Both**, **In Only, Out Only** or **None**. | **None** |
| Version | Press [SPACE BAR] and then [ENTER] to select the RIP version. Options are **RIP-1**, **RIP-2B** or **RIP-2M**. | **RIP-1** |
| Incoming Protocol Filters | Enter the filter set(s) you wish to apply to the incoming traffic between this node and the LAN-Cell. | 1 |
| Outgoing Protocol Filters | Enter the filter set(s) you wish to apply to the outgoing traffic between this node and the LAN-Cell. | 2 |
| 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. | | |

# Chapter 22
# Internet Access

*This chapter shows you how to configure your LAN-Cell for Internet access via the Ethernet WAN port.*

## 22.1 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.

## 22.2 Ethernet Encapsulation

If you choose **Ethernet** in menu 4 you will see the next screen.

```
                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:
```

**Figure 22-1 Menu 4: Internet Access Setup (Ethernet)**

The following table describes this screen.

**Table 22-1 Menu 4: Internet Access Setup (Ethernet)**

| FIELD | DESCRIPTION |
|---|---|
| ISP's Name | Enter the name of your Internet Service Provider, e.g., myISP. This information is for identification purposes only. |
| 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 service type 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 | Enter the password associated with the login name above. |
| 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. |

**Table 22-1 Menu 4: Internet Access Setup (Ethernet)**

| FIELD | DESCRIPTION |
|---|---|
| Relogin Every (min) | This field is available when you select **Telia Login** in the **Service Type** field.<br>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. |
| Gateway IP Address | Enter the gateway IP address associated with your static IP. |
| Network Address Translation | Please see the NAT chapter for a more detailed discussion on the Network Address Translation feature. The choices are **Full Feature**, **None** or **SUA Only**. |
| 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. | |

## 22.3 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 LAN-Cell supports only one PPTP server connection at any given time.**

### 22.3.1 Configuring the PPTP Client

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 -Internet Access Setup** to choose **PPTP** as your encapsulation option. This brings up the following screen.

```
                    Menu 4 - Internet Access Setup

          ISP's Name= ChangeMe
          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:
```

**Figure 22-2 Internet Access Setup (PPTP)**

The following table contains instructions about the new fields when you choose **PPTP** in the **Encapsulation** field in menu 4.

**Table 22-2 New Fields in Menu 4 (PPTP) Screen**

| FIELD | DESCRIPTION | EXAMPLE |
|---|---|---|
| Encapsulation | Press [SPACE BAR] and then press [ENTER] to choose **PPTP**. The encapsulation method influences your choices for the **IP Address** field. | **PPTP** |
| Idle Timeout | This value specifies the time, in seconds, that elapses before the LAN-Cell automatically disconnects from the PPTP server. | 100 (default) |

## 22.4 PPPoE Encapsulation

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

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

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

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

By implementing PPPoE directly on the 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.

### 22.4.1 Configuring the PPPoE Client

If you enable PPPoE in menu 4, you will see the next screen. For more information on PPPoE, please see the appendix.

```
          Menu 4 - Internet Access Setup

     ISP's Name= ChangeMe
     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:
```

**Figure 22-3 Internet Access Setup (PPPoE)**

The following table contains instructions about the new fields when you choose **PPPoE** in the **Encapsulation** field in menu 4.

**Table 22-3 New Fields in Menu 4 (PPPoE) screen**

| FIELD | DESCRIPTION | EXAMPLE |
|---|---|---|
| Encapsulation | Press [SPACE BAR] and then press [ENTER] to choose **PPPoE**. The encapsulation method influences your choices in the **IP Address** field. | **PPPoE** |
| Idle Timeout | This value specifies the time in seconds that elapses before the LAN-Cell automatically disconnects from the PPPoE server. | 100 (default) |

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.

## 22.5 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.**

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 *firewall chapters* for more information on the firewall.

# Part XII:

## SMT Advanced Applications

This part covers setting up remote nodes, IP static routes and Network Address Translation. It also covers the SMT firewall menu, filters, SNMP, schedules and VPN setup.

**See the web configurator parts of this guide for background information on features configurable by web configurator and SMT.**

# Chapter 23
# Remote Node Setup

*This chapter shows you how to configure a remote node.*

## 23.1 Introduction to Remote Node Setup

A remote node is required for placing calls to a 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 Internet access, you are actually configuring a remote node. The following describes how to configure **Menu 11.1 Remote Node Profile**, **Menu 11.3 - Remote Node Network Layer Options** and **Menu 11.5 - Remote Node Filter**.

## 23.2 Remote Node Setup

From the main menu, select menu option 11 to open **Menu 11 Remote Node Setup** (shown below). Configure the setup for your regular ISP.

### 23.2.1 Ethernet Encapsulation

There are two variations of menu 11.1 depending on whether you choose **Ethernet Encapsulation** or **PPPoE 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.

```
                Menu 11.1 - Remote Node Profile

Rem Node Name= ChangeMe              Route= IP
Active= Yes

Encapsulation= Ethernet              Edit IP= No
Service Type= Standard               Session Options:
Service Name= N/A                      Edit Filter Sets= No
Outgoing:
  My Login= N/A
  My Password= N/A                   Edit Traffic Redirect= No
  Retype to Confirm= N/A
  Server= N/A
  Relogin Every (min)=  N/A


              Press ENTER to Confirm or ESC to Cancel:
```

**Figure 23-1Menu 11.1: Remote Node Profile for Ethernet Encapsulation**

The following table describes the fields in this screen.

**Table 23-1 Menu 11.1: Remote Node Profile for Ethernet Encapsulation**

| FIELD | DESCRIPTION | EXAMPLE |
|---|---|---|
| Rem Node Name | Enter a descriptive name for the remote node. This field can be up to eight characters. | LAoffice |
| Active | Press [SPACE BAR] and then [ENTER] to select **Yes** (activate remote node) or **No** (deactivate remote node). | **Yes** |

**Table 23-1 Menu 11.1: Remote Node Profile for Ethernet Encapsulation**

| FIELD | DESCRIPTION | EXAMPLE |
|---|---|---|
| Encapsulation | **Ethernet** is the default encapsulation. Press [SPACE BAR] and then [ENTER] to change to **PPPoE** or **PPTP** encapsulation. | **Ethernet** |
| Service Type | Press [SPACE BAR] and then [ENTER] to select from **Standard**, **RR-Toshiba** (RoadRunner Toshiba authentication method) or **RR-Manager** (RoadRunner Manager authentication method). Choose one of the RoadRunner methods if your ISP is Time Warner's RoadRunner; otherwise choose **Standard**. | **Standard** |
| Service Name | If you are using **PPPoE** encapsulation, then type the name of your PPPoE service here. Only valid with **PPPoE** encapsulation. | poellc |
| 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. | jim |
| 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. | ***** |
| 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.<br>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** |
| Edit IP | This field leads to a "hidden" menu. Press [SPACE BAR] to select **Yes** and press [ENTER] to go to M**enu 11.3 - Remote Node Network Layer Options**. | **No** (default) |
| Session Options | | |
| Edit Filter sets | This field leads to another "hidden" menu. Use [SPACE BAR] to select **Yes** and press [ENTER] to open menu 11.5 to edit the filter sets. See the *Remote Node Filter* section for more details. | **No** (default) |
| Edit Traffic Redirect | Press [SPACE BAR] to select **Yes** or **No**.<br>Select **No** (default) if you do not want to configure this feature.<br>Select **Yes** and press [ENTER] to configure **Menu 11.6 — Traffic Redirect Setup**. | **No** (default) |
| 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. | | |

### 23.2.2 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. Please see the appendix for more information on 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=
   My Password= ********                Nailed-Up Connection= No
   Retype to Confirm= ********
   Authen= CHAP/PAP
                                      Session Options:
                                        Edit Filter Sets= No
                                        Idle Timeout(sec)= 100

                                      Edit Traffic Redirect= No

               Press ENTER to Confirm or ESC to Cancel:
```

**Figure 23-2 Menu 11.1: Remote Node Profile for PPPoE Encapsulation**

### 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.

### Nailed-Up Connection

A 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 a nailed-up 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. A nailed-up connection can be very expensive for obvious reasons.

Do not specify a nailed-up 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 23-1*.

### Metric

See the *Metric* section in the *WAN and Cellular Modem Setup* chapter for details on the **Metric** field.

**Table 23-2 Fields in Menu 11.1 (PPPoE Encapsulation Specific)**

| FIELD | DESCRIPTION | EXAMPLE |
|---|---|---|
| Authen | This field sets the authentication protocol used for outgoing calls.<br>Options for this field are:<br>**CHAP**/**PAP** - Your LAN-Cell will accept either **CHAP** or **PAP** when requested by this remote node.<br>**CHAP** - accept CHAP only.<br>**PAP** - accept PAP only. | **CHAP/PAP** |
| 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. | 0<br>(default) |

**Table 23-2 Fields in Menu 11.1 (PPPoE Encapsulation Specific)**

| FIELD | DESCRIPTION | EXAMPLE |
|---|---|---|
| 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). | 0 (default) |
| Schedules | You can apply up to four schedule sets here. For more details please refer to the *Call Schedule Setup* chapter. | |
| Nailed-Up Connection | This field specifies if you want to make the connection to this remote node a nailed-up connection. More details are given earlier in this section. | **No** (default) |
| Session Options | | |
| Idle Timeout (sec) | 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. | 100 seconds (default) |

## 23.2.3 PPTP Encapsulation

If you change the Encapsulation to **PPTP** in menu 11.1, then you will see the next screen. Please see the appendix for information on 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:
  Service Name= N/A                       Allocated Budget(min)= 0
  Outgoing:                               Period(hr)= 0
    My Login=                             Schedules=
    My Password= ********                 Nailed-Up Connection= 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=                 Edit Traffic Redirect= No

                 Press ENTER to Confirm or ESC to Cancel:
```

**Figure 23-3 Menu 11.1: Remote Node Profile for PPTP Encapsulation**

The next table shows how to configure fields in menu 11.1 not previously discussed.

**Table 23-3 Fields in Menu 11.1 (PPTP Encapsulation)**

| FIELD | DESCRIPTION | EXAMPLE |
|---|---|---|
| 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. | **PPTP** |
| PPTP: | | |
| My IP Addr | Enter the IP address of the WAN Ethernet port. | 10.0.0.140 |
| My IP Mask | Enter the subnet mask of the WAN Ethernet port. | 255.255.255.0 |
| My Server IP Addr | Enter the IP address of the ANT modem. | 10.0.0.138 |

**Table 23-3 Fields in Menu 11.1 (PPTP Encapsulation)**

| FIELD | DESCRIPTION | EXAMPLE |
|---|---|---|
| Connection ID/Name | Enter the connection ID or connection name in the ANT. It must follow the "c:id" and "n:name" format.<br>This field is optional and depends on the requirements of your DSL modem. | N:My ISP |

## 23.3 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 11.3 - Network Layer Options**.

```
Menu 11.3 - 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= 1
  Private=
  RIP Direction= None
    Version= N/A
  Multicast= None

   Enter here to CONFIRM or ESC to CANCEL:
```

**Figure 23-4 Menu 11.3: Remote Node Network Layer Options for Ethernet Encapsulation**

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 screen.

**Table 23-4 Remote Node Network Layer Options Menu Fields**

| FIELD | DESCRIPTION | EXAMPLE |
|---|---|---|
| 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. | **Dynamic** (default) |
| (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.<br>Note that this is the address assigned to your local LAN-Cell, not the remote router. | |

**Table 23-4 Remote Node Network Layer Options Menu Fields**

| FIELD | DESCRIPTION | EXAMPLE |
|---|---|---|
| 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).<br>Choose **None** to disable NAT**.**<br>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**.<br>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!<br>See the *NAT chapter* for a full discussion on this feature. | **SUA Only** (default) |
| Metric | Enter a number from 1 to 15 to set this route's priority among the LAN-Cell's routes (see the *Metric* section in the *WAN and Cellular Modem Setup* chapter) The smaller the number, the higher priority the route has. | 1 |
| 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. | **No** |
| RIP Direction | Press [SPACE BAR] and then [ENTER] to select the RIP direction from **Both**/ **None**/**In Only**/**Out Only**. See the *LAN Setup* chapter 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. | **None** (default) |
| Version | Press [SPACE BAR] and then [ENTER] to select the RIP version from **RIP-1**/**RIP-2B**/**RIP-2M** or **None**. | N/A |
| 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] to enable IP Multicasting or select **None** to disable it. See the *LAN Setup* chapter for more information on this feature. | **None** (default) |
| 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. | | |

## 23.4 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 11.5 - Remote Node Filter**.

Use menu 11.5 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 the Filters chapter. For PPPoE or PPTP encapsulation, you have the additional option of specifying remote node call filter sets.

```
                 Menu 11.5 - 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 23-5 Menu 11.5: Remote Node Filter (Ethernet Encapsulation)**

```
                 Menu 11.5 - 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:
```

**Figure 23-6 Menu 11.5: Remote Node Filter (PPPoE or PPTP Encapsulation)**

## 23.5 Traffic Redirect

To configure the parameters for traffic redirect, enter 11 from the main menu to display **Menu 11.1—Remote Node Profile** as shown next.

```
                    Menu 11.1 - Remote Node Profile

   Rem Node Name= ChangeMe              Route= IP
   Active= Yes

   Encapsulation= Ethernet              Edit IP= No
   Service Type= Standard               Session Options:
   Service Name= N/A                      Edit Filter Sets= No
   Outgoing:
     My Login= N/A
     My Password= N/A                   Edit Traffic Redirect= Yes
     Retype to Confirm= N/A
     Server= N/A
     Relogin Every (min)= N/A


               Press ENTER to Confirm or ESC to Cancel:
```

**Figure 23-7 Menu 11.1: Remote Node Profile**

To configure traffic redirect properties, press [SPACE BAR] to select **Yes** in the **Edit Traffic Redirect** field and then press [ENTER].

**Table 23-5 Menu 11.1: Remote Node Profile (Traffic Redirect Field)**

| FIELD | DESCRIPTION | EXAMPLE |
|---|---|---|
| Edit Traffic Redirect | Press [SPACE BAR] to select **Yes** or **No**.<br>Select **No** (default) if you do not want to configure this feature. | **Yes** |

**Table 23-5 Menu 11.1: Remote Node Profile (Traffic Redirect Field)**

| FIELD | DESCRIPTION | EXAMPLE |
|---|---|---|
| | Select **Yes** and press [ENTER] to configure **Menu 11.6 — Traffic Redirect Setup**. | |
| Press [ENTER] at the message "Press ENTER to Confirm..." to save your configuration, or press [ESC] at any time to cancel. | | |

## 23.5.1 Traffic Redirect Setup

Configure parameters that determine when the LAN-Cell will forward WAN traffic to the backup gateway using **Menu 11.6 — Traffic Redirect Setup**.

```
                Menu 11.6 - Traffic Redirect Setup

             Active= No
             Configuration:
               Backup Gateway IP Address= 0.0.0.0
               Metric= 14
               Check WAN IP Address= 0.0.0.0
                 Fail Tolerance= 2
                 Period(sec)= 5
                 Timeout(sec)= 3


             Press ENTER to Confirm or ESC to Cancel:
```

**Figure 23-8 Menu 11.6: Traffic Redirect Setup**

The following table describes the fields in this screen.

**Table 23-6 Menu 11.6: Traffic Redirect Setup**

| FIELD | DESCRIPTION | EXAMPLE |
|---|---|---|
| Active | Press [SPACE BAR] and select **Yes** (to enable) or **No** (to disable) traffic redirect setup. The default is **No**.<br>When the **Active** field is **Yes**, you must configure every field in this screen unless you are using PPPoE or PPTP encapsulation (except **Check WAN IP Address** and **Timeout**).<br>If you don't configure these fields and are using PPTP or PPPoE encapsulation, then the LAN-Cell checks the PPPoE channel or PPTP tunnel to determine if the WAN connection is down. | **Yes** |
| Configuration: | | |
| Backup Gateway IP Address | Enter the IP address of your backup gateway in dotted decimal notation.<br>The LAN-Cell automatically forwards traffic to this IP address if the LAN-Cell's Internet connection terminates. | 0.0.0.0 |
| Metric | Enter a number from 1 to 15 to set this route's priority among the LAN-Cell's routes (see the *Metric* section in the *WAN and Cellular Modem Setup* chapter) The smaller the number, the higher priority the route has. | 15 (default) |
| Check WAN IP Address | Enter the IP address of a reliable nearby computer (for example, your ISP's DNS server address) to test your LAN-Cell's WAN accessibility.<br>The LAN-Cell uses the default gateway IP address if you do not enter an IP address here.<br>If you are using PPTP or PPPoE Encapsulation, enter "0.0.0.0" to configure the LAN-Cell to check the PVC (Permanent Virtual Circuit) or PPTP tunnel. | 0.0.0.0 |
| Fail Tolerance | Enter the number of times your LAN-Cell may attempt and fail to connect to the Internet before traffic is forwarded to the backup gateway. Two to five is usually a good number. | 2 |

**Table 23-6 Menu 11.6: Traffic Redirect Setup**

| FIELD | DESCRIPTION | EXAMPLE |
|---|---|---|
| Period (sec) | Enter the time interval (in seconds) between WAN connection checks. Five to 60 is usually a good number. | 5 |
| Timeout (sec) | Enter the number of seconds the LAN-Cell waits for a ping response from the IP Address in the **Check WAN IP Address** field before it times out. The number in this field should be less than the number in the **Period** field. Three to 50 is usually a good number.<br>The WAN connection is considered "down" after the LAN-Cell times out the number of times specified in the **Fail Tolerance** field. | 3 |

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.

# Chapter 24
# IP Static Route Setup

*This chapter shows you how to configure static routes with your LAN-Cell.*

## 24.1 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.

```
                    Menu 12 - IP Static Route Setup

                           1. ________
                           2. ________
                           3. ________
                           4. ________
                           5. ________
                           6. ________
                           7. ________
                           8. ________
                           9. ________
                           10. ________
                           11. ________
                           12. ________


                     Enter selection number:
```

**Figure 24-1 Menu 12: IP Static Route Setup**

Now, enter the index number of the static route that you want to configure.

```
                       Menu 12.1 - Edit IP Static Route

                   Route #: 1
                   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:
```

**Figure 24-2 Menu 12. 1: Edit IP Static Route**

`The following table describes the IP Static Route Menu fields.

**Table 24-1 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. |

**Table 24-1 Menu 12. 1: Edit IP Static Route**

| FIELD | DESCRIPTION |
|---|---|
| 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 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 the *Metric* section in the *WAN and Cellular Modem Setup* chapter). 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.

# Chapter 25
# Network Address Translation (NAT)

*This chapter discusses how to configure NAT on the LAN-Cell.*

## 25.1 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.**

### 25.1.1 SUA (Single User Account) Versus NAT

SUA (Single User Account) is an implementation of a subset of NAT that supports two types of mapping, **Many-to-One** and **Server**. See *section 25.2.1* 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.

1. **Choose** SUA Only **if you have just one public WAN IP address for your LAN-Cell.**
2. **Choose** Full Feature **if you have multiple public WAN IP addresses for your LAN-Cell.**

### 25.1.2 Applying NAT

You apply NAT via menus 4 or 11.3 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 - Internet Access Setup.**

```
          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:
```

**Figure 25-1 Menu 4: Applying NAT for Internet Access**

The following figure shows how you apply NAT to the remote node in menu 11.1.

**Step 1.** Enter 11 from the main menu.

**Step 2.** Move the cursor to the **Edit IP** field, press [SPACE BAR] to select **Yes** and then press [ENTER] to bring up **Menu 11.3 - Remote Node Network Layer Options.**

```
Menu 11.3 - 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
  Metric= 1
  Private=
  RIP Direction= None
    Version= N/A
  Multicast= None


   Enter here to CONFIRM or ESC to CANCEL:
```

**Figure 25-2 Menu 11.3: Applying NAT to the Remote Node**

The following table describes the fields in this screen.

**Table 25-1 Applying NAT in Menus 4 & 11.3**

| FIELD | DESCRIPTION | OPTIONS |
|---|---|---|
| Network Address Translation | When you select this option the SMT will use Address Mapping Set 1 (menu 15.1 - see *section 25.2.1* for further discussion). You can configure any of the mapping types described in the *Web Configurator User's Guide.* Choose **Full Feature** if you have multiple public WAN IP addresses for your LAN-Cell.<br>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 25.2.1*). Choose **SUA Only** if you have just one public WAN IP address for your LAN-Cell. | **SUA Only** |

## 25.2 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. When you select **Full Feature** in menu 4 or 11.3, the SMT will use **Set 1**. When you select **SUA Only**, the SMT will use the pre-configured **Set 255** (read only).

The server set is a list of LAN 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 the chapter on NAT web configurator screens for further information on these menus. To configure NAT, enter 15 from the main menu to bring up the following screen.

```
        Menu 15 - NAT Setup

   1. Address Mapping Sets
   2. Port Forwarding Setup
   3. Trigger Port Setup



  Enter Menu Selection Number:
```

**Figure 25-3 Menu 15: NAT Setup**

**Configure LAN IP addresses in NAT menus 15.1 and 15.2.**

### 25.2.1 Address Mapping Sets

Enter 1 to bring up **Menu 15.1 — Address Mapping Sets**.

```
                    Menu 15.1 - Address Mapping Sets

                  1.
                255. SUA (read only)




                     Enter Menu Selection Number:
```

**Figure 25-4 Menu 15.1: Address Mapping Sets**

### SUA Address Mapping Set

Enter 255 to display the next screen (see also *section 25.1.1)*. The fields in this menu cannot be changed.

```
          Menu 15.1.1 - 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:
```

**Figure 25-5 Menu 15.1.255: SUA Address Mapping Rules**

The following table explains the fields in this screen.

**Menu 15.1.255 is read-only.**

**Table 25-2 SUA Address Mapping Rules**

| FIELD | DESCRIPTION | EXAMPLE |
|---|---|---|
| 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. | SUA |
| Idx | This is the index or rule number. | 1 |
| Local Start IP | **Local Start IP** is the starting local IP address (ILA). | 0.0.0.0 |
| 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. | 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**. | 0.0.0.0 |
| 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. | Server |

**Table 25-2 SUA Address Mapping Rules**

| FIELD | DESCRIPTION | EXAMPLE |
|---|---|---|
| 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. | | |

## 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.**

```
        Menu 15.1.1 - Address Mapping Rules

 Set Name= ?

Idx  Local Start IP   Local End IP     Global Start IP  Global End IP    Type
---  ---------------  ---------------  ---------------  ---------------  ------
 1.
 2.
 3.
 4.
 5.
 6.
 7.
 8.
 9.
10.

                  Action= None          Select Rule= N/A

                  Press ENTER to Confirm or ESC to Cancel:
```

**Figure 25-6 Menu 15.1.1: First Set**

**The Type, Local and Global Start/End IPs are configured in menu 15.1.1.1 (described later) and the values are displayed here.**

## 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 25-3 Fields in Menu 15.1.1**

| FIELD | DESCRIPTION | EXAMPLE |
|---|---|---|
| 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. | NAT_SET |
| 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. | **Edit** |
| 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. | 1 |

**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.**

```
     Menu 15.1.1.1 Address Mapping Rule

Type= One-to-One

Local IP:
  Start=
  End  = N/A

Global IP:
  Start=
  End  = N/A


                Press ENTER to Confirm or ESC to Cancel:
```

**Figure 25-7 Menu 15.1.1.1: Editing/Configuring an Individual Rule in a Set**

The following table describes the fields in this screen.

**Table 25-4 Menu 15.1.1.1: Editing/Configuring an Individual Rule in a Set**

| FIELD | DESCRIPTION | EXAMPLE |
|---|---|---|
| Type | Press [SPACE BAR] and then [ENTER] to select from a total of five types. These are the mapping types discussed in the *Web Configurator User's* Guide. **Server** allows you to specify multiple servers of different types behind NAT to this computer. See *section 25.4.3* for an example. | **One-to-One** |
| 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). | 0.0.0.0 |
| 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. | N/A |
| Global IP | | |

**Table 25-4 Menu 15.1.1.1: Editing/Configuring an Individual Rule in a Set**

| FIELD | DESCRIPTION | EXAMPLE |
|---|---|---|
| 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**. | 0.0.0.0 |
| End | Enter the ending global IP address (IGA). This field is **N/A** for **One-to-One**, **Many-to-One** and **Server types**. | N/A |

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.

## 25.3 Configuring a Server behind NAT

Follow these steps to configure a server behind NAT:

**Step 1.** Enter 15 in the main menu to go to **Menu 15 - NAT Setup.**

**Step 2.** Enter 2 to go to **Menu 15.2 - NAT Server Setup**.

**Step 3.** Enter a port number in an unused **Start Port No** field. To forward only one port, enter it again in the **End Port No** field. To specify a range of ports, enter the last port to be forwarded in the **End Port No** field.

**Step 4.** 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.

**Step 5.** 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.

```
                    Menu 15.2 - NAT Server Setup

         Rule   Start Port No.   End Port No.   IP Address
        ---------------------------------------------------
           1.     Default          Default        0.0.0.0
           2.       21               25           192.168.1.33
           3.       0                0            0.0.0.0
           4.       0                0            0.0.0.0
           5.       0                0            0.0.0.0
           6.       0                0            0.0.0.0
           7.       0                0            0.0.0.0
           8.       0                0            0.0.0.0
           9.       0                0            0.0.0.0
          10.       0                0            0.0.0.0
          11.       0                0            0.0.0.0
          12.       0                0            0.0.0.0

              Press ENTER to Confirm or ESC to Cancel:
```

**Figure 25-8 Menu 15.2: NAT Server Setup**

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.

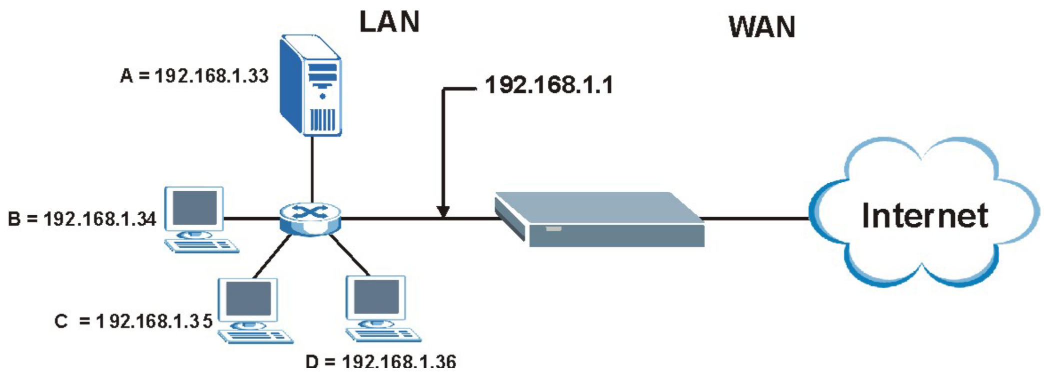



**Figure 25-9 Multiple Servers Behind NAT Example**

## 25.4 General NAT Examples

The following are some examples of NAT configuration.

### 25.4.1 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.

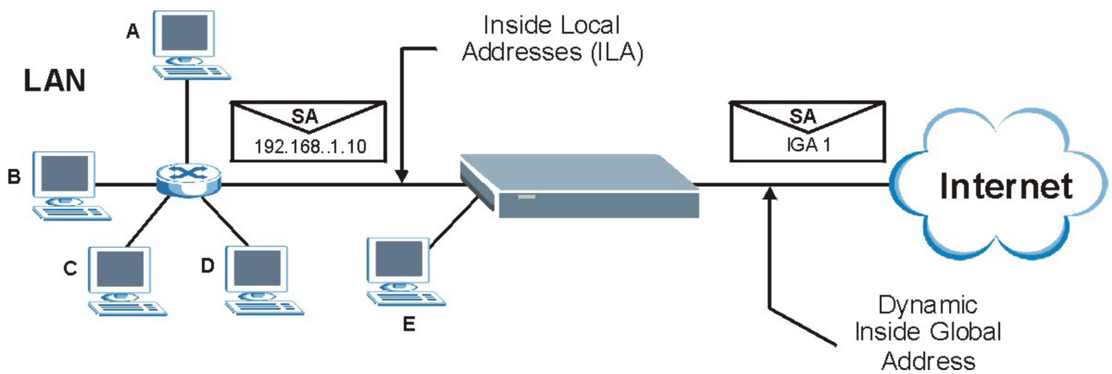



**Figure 25-10 NAT Example 1**

```
                    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:
```

**Figure 25-11 Menu 4: Internet Access & NAT Example**

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 25.4.* 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.

## 25.4.2 Example 2: Internet Access with an Inside Server

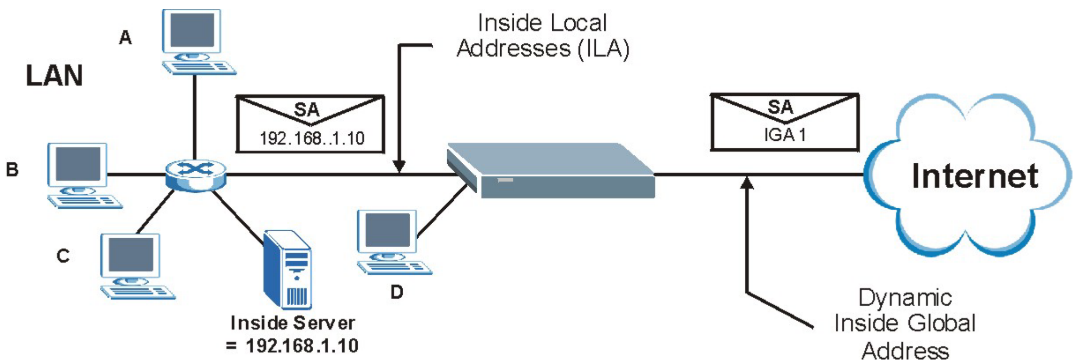



**Figure 25-12 NAT Example 2**

In this case, you do exactly as above (use the convenient pre-configured **SUA Only** set) and also go to menu 15.2 to specify the Inside Server behind the NAT as shown in the next figure.

```
                    Menu 15.2 - NAT Server Setup

        Rule   Start Port No.   End Port No.   IP Address
       ---------------------------------------------------
          1.    Default          Default        192.168.1.10
          2.      0                0            0.0.0.0
          3.      0                0            0.0.0.0
          4.      0                0            0.0.0.0
          5.      0                0            0.0.0.0
          6.      0                0            0.0.0.0
          7.      0                0            0.0.0.0
          8.      0                0            0.0.0.0
          9.      0                0            0.0.0.0
         10.      0                0            0.0.0.0
         11.      0                0            0.0.0.0
         12.      0                0            0.0.0.0

              Press ENTER to Confirm or ESC to Cancel:
```

**Figure 25-13 Menu 15.2: Specifying an Inside Server**

## 25.4.3 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 LAN-Cell. 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.

**Rule 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).

**Rule 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).

**Rule 3.** Map the other outgoing LAN traffic to IGA3 (**Many : 1** mapping).

**Rule 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:

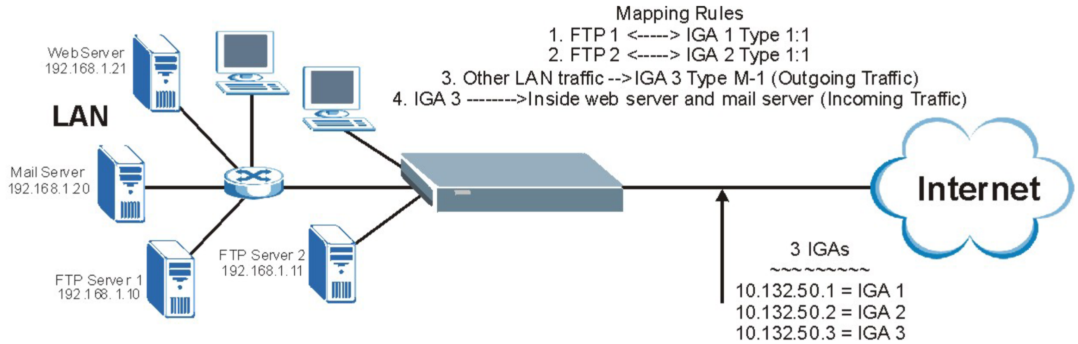



**Figure 25-14 NAT Example 3**

**Step 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 25-15*.

**Step 2.** Then enter 15 from the main menu.

**Step 3.** Enter 1 to configure the Address Mapping Sets.

**Step 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.

**Step 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 25-16).*

**Step 6.** Repeat the previous step for rules 2 to 4 as outlined above.

**Step 7.** When finished, menu 15.1.1 should look like as shown in *Figure* 25-17.

```
              Menu 11.3 - 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
                     Metric= 1
                     Private=
                     RIP Direction= None
                       Version= N/A
                     Multicast= None


                      Enter here to CONFIRM or ESC to CANCEL:
```

**Figure 25-15 Example 3: Menu 11.3**

The following figure shows how to configure the first rule.

```
     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

               Press ENTER to Confirm or ESC to Cancel:
```

**Figure 25-16 Example 3: Menu 15.1.1.1**

```
                    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= None          Select Rule= N/A

                   Press ENTER to Confirm or ESC to Cancel:
```

**Figure 25-17 Example 3: Final Menu 15.1.1**

Now configure the IGA3 to map to our web server and mail server on the LAN.

**Step 8.** Enter 15 from the main menu.

**Step 9.** Now enter 2 from this menu and configure it as shown in *Figure 25-18*.

```
                 Menu 15.2 - NAT Server Setup


         Rule   Start Port No.   End Port No.   IP Address
        ---------------------------------------------------
           1.     Default          Default        0.0.0.0
           2.       80               80           192.168.1.21
           3.       25               25           192.168.1.20
           4.       0                0            0.0.0.0
           5.       0                0            0.0.0.0
           6.       0                0            0.0.0.0
           7.       0                0            0.0.0.0
           8.       0                0            0.0.0.0
           9.       0                0            0.0.0.0
          10.       0                0            0.0.0.0
          11.       0                0            0.0.0.0
          12.       0                0            0.0.0.0

              Press ENTER to Confirm or ESC to Cancel:
```

**Figure 25-18 Example 3: Menu 15.2**

### 25.4.4 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.

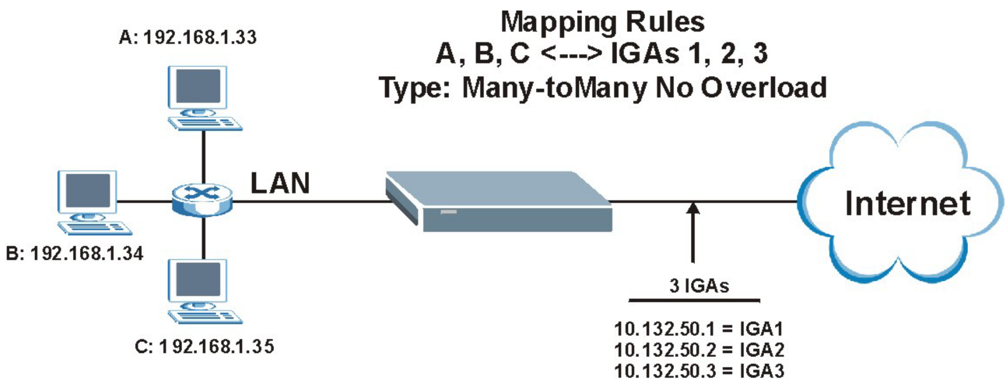



**Figure 25-19 NAT Example 4**

---

**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.

```
              Menu 15.1.1.4 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  = 10.132.20.3


                 Press ENTER to Confirm or ESC to Cancel:
```

**Figure 25-20 Example 4: Menu 15.1.1.1: Address Mapping Rule**

After you've configured your rule, you should be able to check the settings in menu 15.1.1 as shown next.

```
                        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= None            Select Rule= N/A
                   Press ENTER to Confirm or ESC to Cancel:
```

**Figure 25-21 Example 4: Menu 15.1.1: Address Mapping Rules**

## 25.5 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.

### 25.5.1 Trigger Port Forwarding Process

The following is an example of trigger port forwarding.

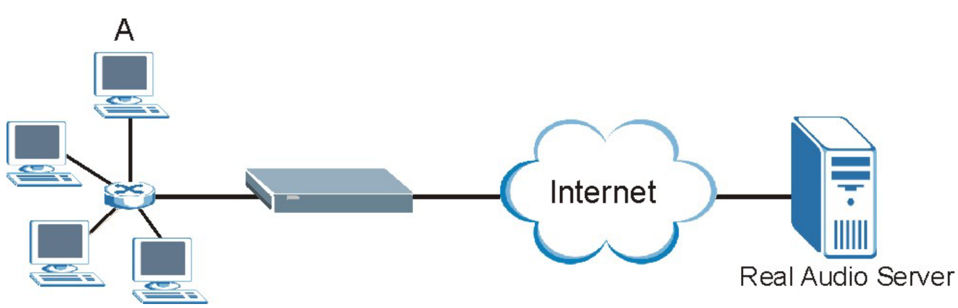



**Figure 25-22 Trigger Port Forwarding Process: Example**

1. **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 **A**'s computer IP address. The LAN-Cell associates **A**'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 **A**'s computer IP address.
5. Only **A** 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).

## 25.5.2 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 Port Setup**, shown next.

```
                    Menu 15.3 - 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:
```

**Figure 25-23 Menu 15.3: Trigger Port Setup**

The following table describes the fields in this screen.

**Table 25-5 Menu 15.3: Trigger Port Setup**

| FIELD | DESCRIPTION | EXAMPLE |
|---|---|---|
| Rule | This is the rule index number. | 1 |
| Name | Enter a unique name for identification purposes. You may enter up to 15 characters in this field. All characters are permitted - including spaces. | Real Audio |
| 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. | 6970 |
| End Port | Enter a port number or the ending port number in a range of port numbers. | 7170 |
| 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. | 7070 |

**Table 25-5 Menu 15.3: Trigger Port Setup**

| FIELD | DESCRIPTION | EXAMPLE |
|---|---|---|
| End Port | Enter a port number or the ending port number in a range of port numbers. | 7070 |

Press [ENTER] at the message "Press ENTER to Confirm..." to save your configuration, or press [ESC] at any time to cancel.

# Chapter 26
# Introducing the Firewall

*This chapter shows you how to get started with the firewall.*

## 26.1 Using SMT Menus

From the main menu enter 21 to go to **Menu 21 - Filter Set and Firewall Configuration** to display the screen shown next**.**

```
                    Menu 21 - Filter and Firewall Setup

                 1. Filter Setup
                 2. Firewall Setup



                        Enter Menu Selection Number:
```

**Figure 26-1 Menu 21: Filter and Firewall Setup**

### 26.1.1 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.

```
                     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.
```

**Figure 26-2 Menu 21.2: Firewall Setup**

**Configure the firewall rules using the web configurator or CLI commands.**

# Chapter 27
# Filter Configuration

*This chapter shows you how to create and apply filters.*

## 27.1 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.

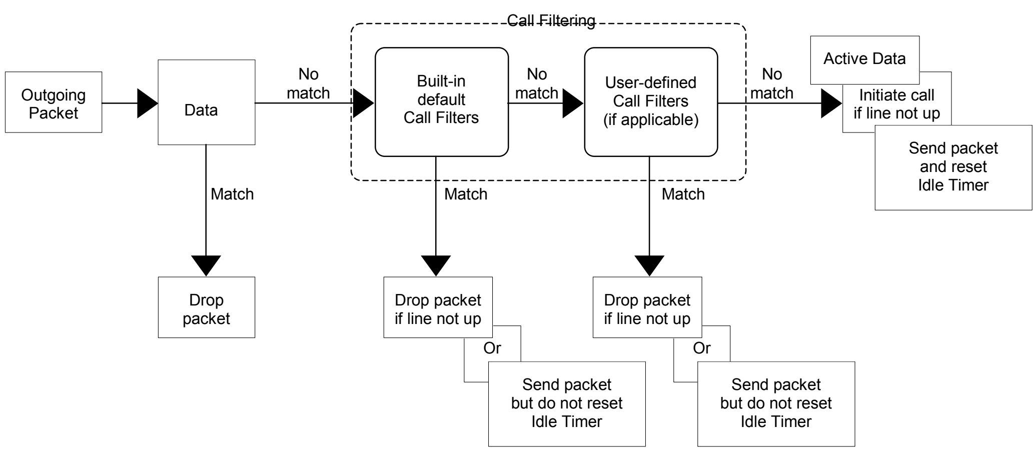



**Figure 27-1 Outgoing Packet Filtering Process**

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.

### 27.1.1 Filter Structure

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 27-6* for the logic flow when executing an IP filter.

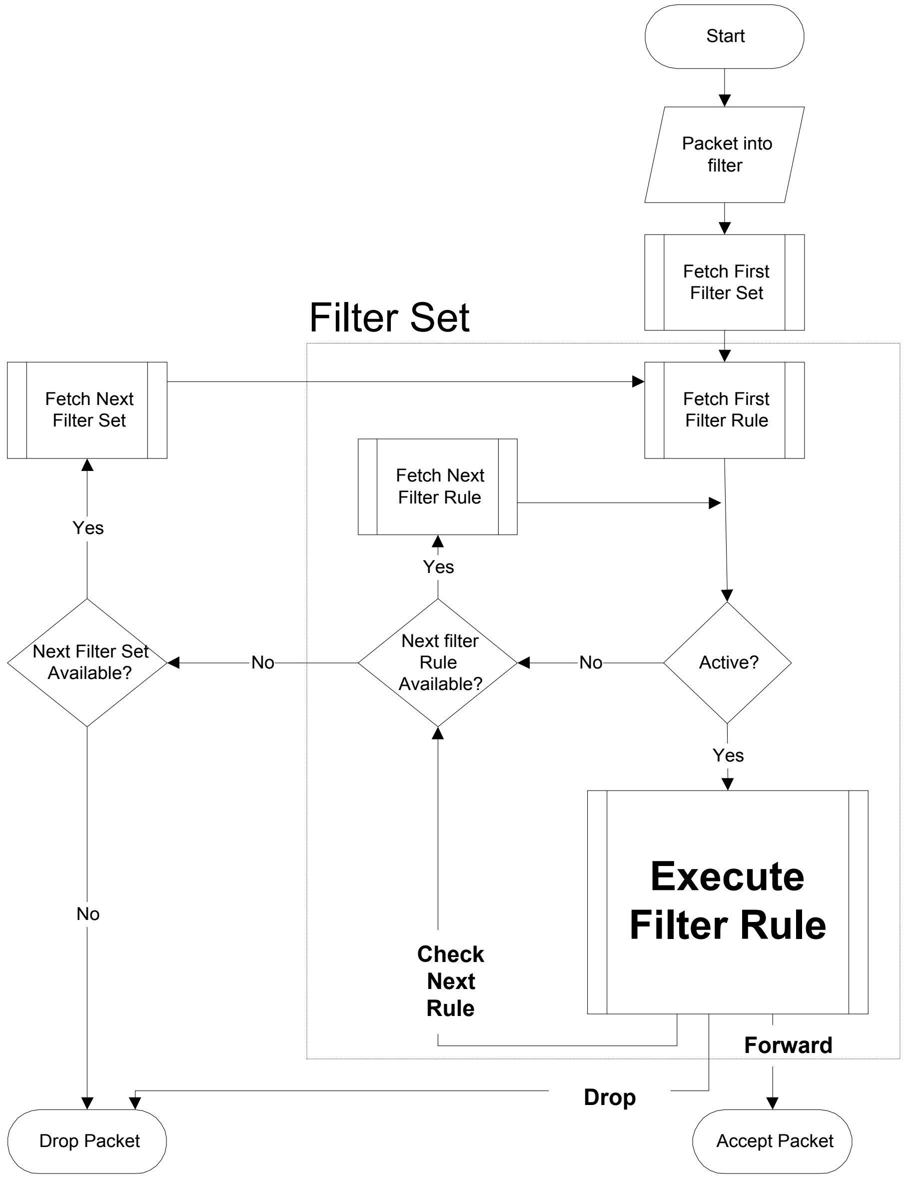



**Figure 27-2 Filter Rule Process**

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.

## 27.2 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.

**Step 1.** Enter 21 in the main menu to open menu 21.

```
Menu 21 - Filter and Firewall Setup

1. Filter Setup
2. Firewall Setup



Enter Menu Selection Number:
```

**Figure 27-3 Menu 21: Filter and Firewall Setup**

**Step 2.** Enter 1 to bring up the following menu.

```
                    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:
```

**Figure 27-4 Menu 21.1: Filter Set Configuration**

**Step 3.** Select the filter set you wish to configure (1-12) and press [ENTER].

**Step 4.** Enter a descriptive name or comment in the **Edit Comments** field and press [ENTER].

**Step 5.** Press [ENTER] at the message [Press ENTER to confirm] to open **Menu 21.1.1 - 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 27-1 Abbreviations Used in the Filter Rules Summary Menu**

| FIELD | DESCRIPTION |
|---|---|
| # | The filter rule number: 1 to 6. |
| 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.<br>"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.<br>"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.<br>"F" means to forward the packet immediately and skip checking the remaining rules.<br>"D" means to drop the packet.<br>"N" means to check the next rule. |

**Table 27-1 Abbreviations Used in the Filter Rules Summary Menu**

| FIELD | DESCRIPTION |
|---|---|
| n | Action Not Matched.<br>"F" means to forward the packet immediately and skip checking the remaining rules.<br>"D" means to drop the packet.<br>"N" means to check the next rule. |

The protocol dependent filter rules abbreviation are listed as follows:

**Table 27-2 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.

## 27.2.1 Configuring a Filter Rule

To configure a filter rule, type its number in **Menu 21.1.1 - Filter Rules Summary** and press [ENTER] to open menu 21.1.1.1 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.

## 27.2.2 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 21.1.1.1 - TCP/IP Filter Rule**, as shown next.

```
                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:
```

**Figure 27-5 Menu 21.1.1.1: TCP/IP Filter Rule**

The following table describes how to configure your TCP/IP filter rule.

**Table 27-3 TCP/IP Filter Rule Menu Fields**

| FIELD | DESCRIPTION | OPTIONS |
|---|---|---|
| Active | Press [SPACE BAR] and then [ENTER] to select **Yes** to activate the filter rule or **No** to deactivate it. | **Yes**<br>**No** |
| 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. | 0-255 |
| 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. | **Yes**<br>**No** |
| Destination | | |
| IP Address | Enter the destination IP Address of the packet you wish to filter. This field is ignored if it is 0.0.0.0. | 0.0.0.0 |
| IP Mask | Enter the IP mask to apply to the **Destination: IP Addr**. | 0.0.0.0 |
| 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. | 0-65535 |
| 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 #**. | **None**<br>**Less**<br>**Greater**<br>**Equal**<br>**Not Equal** |
| Source | | |
| IP Address | Enter the source IP Address of the packet you wish to filter. This field is ignored if it is 0.0.0.0. | 0.0.0.0 |
| IP Mask | Enter the IP mask to apply to the **Source: IP Addr**. | 0.0.0.0 |
| 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. | 0-65535 |

**Table 27-3 TCP/IP Filter Rule Menu Fields**

| FIELD | DESCRIPTION | OPTIONS |
|---|---|---|
| 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 #**. | **None**<br>**Less**<br>**Greater**<br>**Equal**<br>**Not Equal** |
| 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. | **Yes**<br>**No** |
| 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.<br><br>If **More** is **Yes**, then **Action Matched** and **Action Not Matched** will be **N/A**. | **Yes**<br>**No** |
| Log | Press [SPACE BAR] and then [ENTER] to select a logging option from the following:<br>**None** – No packets will be logged.<br>**Action Matched** - Only packets that match the rule parameters will be logged.<br>**Action Not Matched** - Only packets that do not match the rule parameters will be logged.<br><br>**Both** – All packets will be logged. | **None**<br><br>**Action Matched**<br><br>**Action Not Matched**<br><br>**Both** |
| Action Matched | Press [SPACE BAR] and then [ENTER] to select the action for a matching packet. | **Check Next Rule**<br><br>**Forward**<br><br>**Drop** |
| Action Not Matched | Press [SPACE BAR] and then [ENTER] to select the action for a packet not matching the rule. | **Check Next Rule**<br><br>**Forward**<br><br>**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.

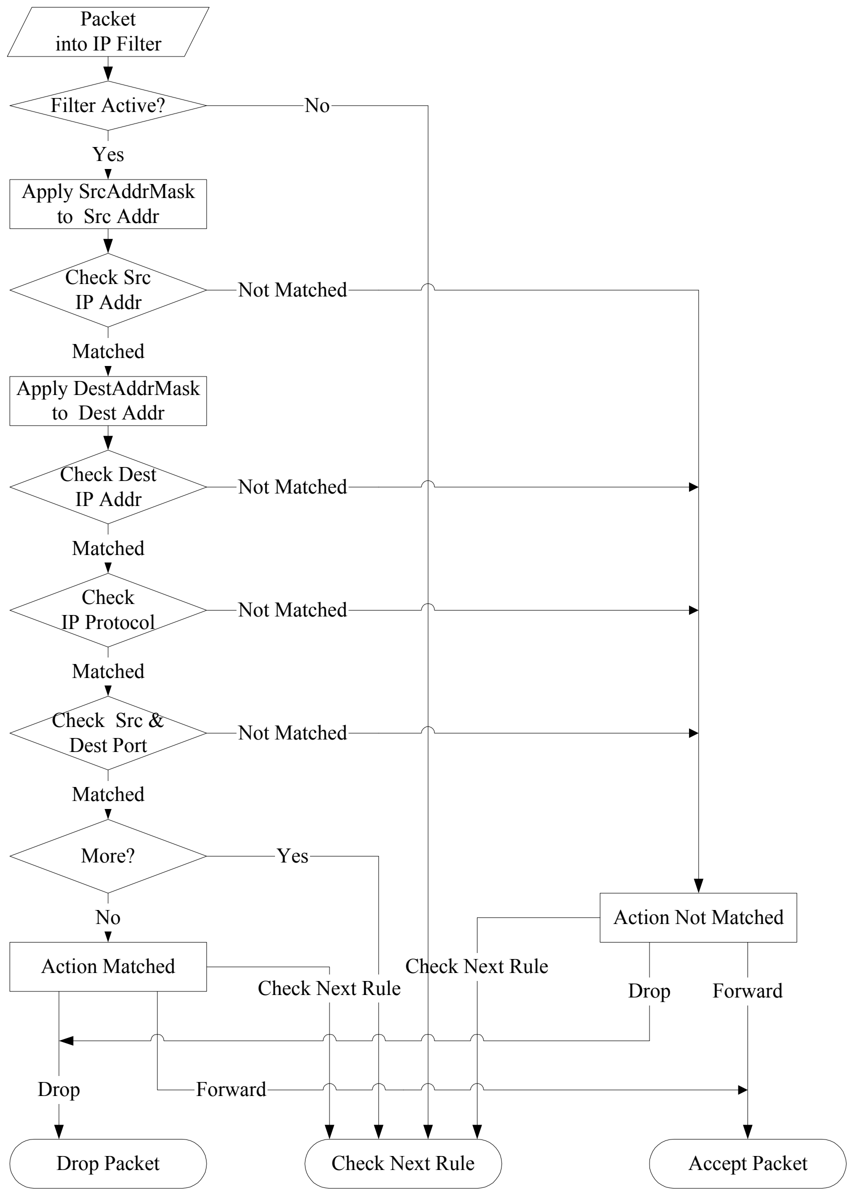



**Figure 27-6 Executing an IP Filter**

## 27.2.3 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 21.1.4.1 and press [ENTER] to open Generic Filter Rule, as shown below.

```
                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:
```

**Figure 27-7 Menu 21.1.1.1: Generic Filter Rule**

The following table describes the fields in the Generic Filter Rule menu.

**Table 27-4 Menu 21.1.1.1: Generic Filter Rule**

| FIELD | DESCRIPTION | OPTIONS |
|---|---|---|
| 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. | **Generic Filter Rule**<br>**TCP/IP Filter Rule** |
| Active | Select **Yes** to turn on the filter rule or **No** to turn it off. | **Yes / No** |
| 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. | 0-255 |
| 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. | 0-8 |
| 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.<br>If **More** is **Yes**, then Action Matched and Action Not Matched will be **No**. | **Yes**<br>**No** |
| Log | Select the logging option from the following:<br>**None** - No packets will be logged.<br>**Action Matched** - Only packets that match the rule parameters will be logged.<br>**Action Not Matched** - Only packets that do not match the rule parameters will be logged.<br>**Both** – All packets will be logged. | **None**<br>**Action Matched**<br>**Action Not Matched**<br>**Both** |
| Action Matched | Select the action for a packet matching the rule. | **Check Next Rule**<br>**Forward**<br>**Drop** |
| Action Not Matched | Select the action for a packet not matching the rule. | **Check Next Rule**<br>**Forward**<br>**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**. | | |

## 27.3 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.

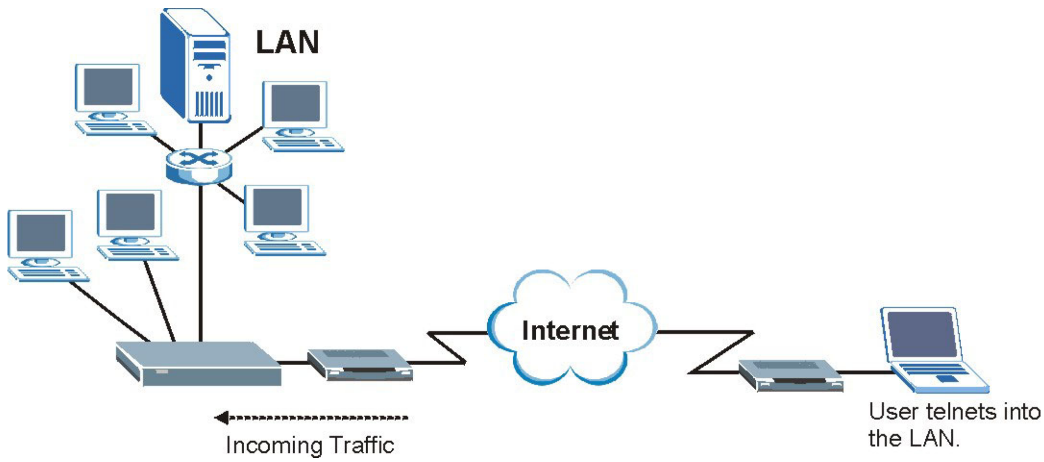



**Figure 27-8 Telnet Filter Example**

**Step 1.** Enter 21 from the main menu to open **Menu 21 - Filter and Firewall Setup**.

**Step 2.** Enter 1 to open **Menu 21.1 - Filter Set Configuration**.

**Step 3.** Enter the index of the filter set you wish to configure (say 3) and press [ENTER].

**Step 4.** Enter a descriptive name or comment in the **Edit Comments** field and press [ENTER].

**Step 5.** Press [ENTER] at the message [Press ENTER to confirm] to open **Menu 21.1.3 - Filter Rules Summary**.

**Step 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.

```
                    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.
```

Press [SPACE BAR] and then [ENTER] to choose this filter rule type. The first filter rule type determines all subsequent filter types within a set.

Select **Yes** to make the rule active.

**6** is the TCP protocol.

The port number for the telnet service (TCP protocol) is **23**. See *RFC 1060* for port numbers of well-known services.

There are no more rules to check.

Select **Equal** here as you are looking for packets going to port 23 only.

Select **Drop** here so that the packet will be dropped if its destination is the telnet port.

Select Forward here so that the packet will be forwarded if its destination is not the telnet port.

**Figure 27-9 Example Filter: Menu 21.1.3.1**

When you press [ENTER] to confirm, you will see the following screen. Note that there is only one filter rule in this set.

```
                         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
```

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).

**Figure 27-10 Example Filter Rules Summary: Menu 21.1.3**

After you've created the filter set, you must apply it.

**Step 1.** Enter 11 from the main menu to go to menu 11.

**Step 2.** Go to the **Edit Filter Sets** field, press [SPACE BAR] to select **Yes** and press [ENTER].

**Step 3.** This brings you to menu 11.5. Apply a filter set (our example filter set 3) as shown in *Figure 27-13*.

**Step 4.** Press [ENTER] to confirm after you enter the set numbers and to leave menu 11.5.

## 27.4 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.

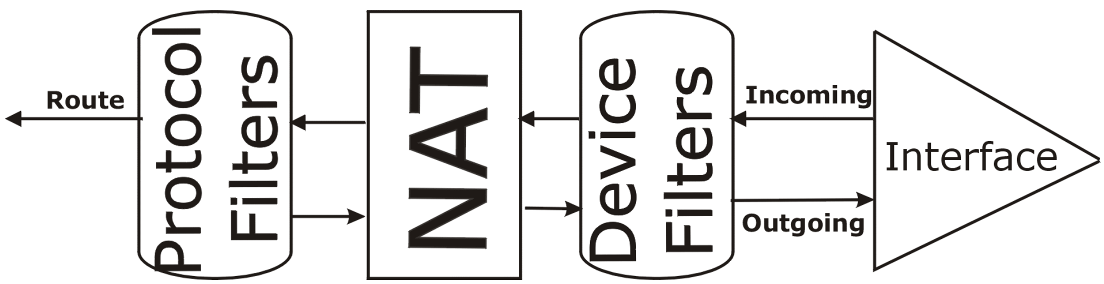



**Figure 27-11 Protocol and Device Filter Sets**

## 27.5 Firewall Versus Filters

Firewall configuration is discussed in the *firewall* chapters of this manual. Further comparisons are also made between filtering, NAT and the firewall.

## 27.6 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.**

### 27.6.1 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.

```
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:
```

**Figure 27-12 Filtering LAN Traffic**

## 27.6.2 Applying Remote Node Filters

Go to menu 11.5 (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.

```
                   Menu 11.5 - 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:
```

**Figure 27-13 Filtering Remote Node Traffic**

# Chapter 28
# SNMP Configuration

*This chapter explains SNMP configuration menu 22.*

## 28.1 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.

```
                    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:
```

**Figure 28-1 Menu 22: SNMP Configuration**

The following table describes the SNMP configuration parameters.

**Table 28-1 Menu 22: SNMP Configuration**

| FIELD | DESCRIPTION | EXAMPLE |
|---|---|---|
| Get Community | Type the Get community, which is the password for the incoming Get- and GetNext requests from the management station. | **Public** |
| Set Community | Type the Set community, which is the password for incoming Set requests from the management station. | **Public** |
| 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. | 0.0.0.0 |
| Trap<br>Community | Type the Trap community, which is the password sent with each trap to the SNMP manager. | **Public** |
| Destination | Type the IP address of the station to send your SNMP traps to. | 0.0.0.0 |
| 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. | | |

## 28.2 SNMP Traps

The LAN-Cell will send traps to the SNMP manager when any one of the following events occurs:

**Table 28-2 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 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. |

# Part XIII:

## SMT System Maintenance

This part covers system information and diagnosis, firmware and configuration file maintenance, as well as providing information on the system maintenance and information functions and how to configure remote management and VPN.

**See the web configurator parts of this guide for background information on features configurable by web configurator and SMT.**

# Chapter 29
# System Information & Diagnosis

*This chapter covers SMT menus 24.1 to 24.4.*

## 29.1 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.

```
                    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:
```

**Figure 29-1 Menu 24: System Maintenance**

## 29.2 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**Error! Reference source not found.**. 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:

**Step 1.** Enter number 24 to go to **Menu 24 - System Maintenance**.

**Step 2.** In this menu, enter 1 to open System Maintenance - Status.

**Step 3.** There are three commands in **Menu 24.1 - System Maintenance - Status**. Entering 1 drops the WAN connection, 9 resets the counters and [ESC] takes you back to the previous screen.

```
                    Menu 24.1 - System Maintenance - Status          09:41:41
                                                            Thu. Nov. 13, 2003

Port   Status        TxPkts      RxPkts    Cols    Tx B/s    Rx B/s     Up Time
 WAN   Down               0           0       0         0         0     0:00:00
 LAN   100M/Full       5818        6760       0         0         0     7:31:30

Port   Ethernet Address        IP Address           IP Mask       DHCP
 WAN  00:A0:C5:00:00:02          0.0.0.0            0.0.0.0     Client
 LAN  00:A0:C5:00:00:01      192.168.1.1      255.255.255.0     Server

     System up Time:     7:31:36

     Name:
     Routing: IP
     ProxiOS F/W Version: V3.62(WK.0)b1 | 10/24/2003

                                 Press Command:

               COMMANDS: 1-Drop WAN 9-Reset Counters   ESC-Exit
```

**Figure 29-2 Menu 24.1: System Maintenance: Status**

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 29-1 System Maintenance: Status Menu Fields**

| FIELD | DESCRIPTION |
|---|---|
| Port | Identifies a port (WAN, or LAN) on the LAN-Cell. |
| Status | Shows the port speed and duplex setting if you're using **Ethernet Encapsulation** and **Down** (line is down), **idle** (line (ppp) idle), **dial** (starting to trigger a call) and **drop** (dropping a call) if you're using **PPPoE Encapsulation**. |
| 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 shows the transmission speed in Bytes per second on this port. |
| Rx B/s | This 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. |
| Ethernet Address | This is the Ethernet 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. |
| 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<br>Name= xxx.baboo.mickey.com |
| Routing | Refers to the routing protocol used. |
| ProxiOS F/W Version | Refers to the ProxiOS (Proxicast Network Operating System) system firmware version. |
| You may enter 1 to drop the WAN connection, 9 to reset the counters or [ESC] to return to menu 24. | |

## 29.3 System Information

This section describes your system and allows you to choose different console port speeds. To get to the System Information:

**Step 1.** Enter 24 to go to **Menu 24 – System Maintenance**.

**Step 2.** Enter 2 to open Menu 24.2 - System Information

**Step 3.** From this menu you have two choices as shown in the next figure:

```
                    Menu 24.2 - System Information
                         1. System Information



                              Please enter selection:
```

**Figure 29-3 Menu 24.2: System Information**

### 29.3.1 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.

```
                  Menu 24.2.1 - System Maintenance - Information

                     Name:
                     Routing: IP
                     ProxiOS F/W Version: V3.62(WK.0)b1 | 10/24/2003
                     Country Code: 255

                     LAN
                       Ethernet Address: 00:A0:C5:00:00:01
                       IP Address: 192.168.1.1
                       IP Mask: 255.255.255.0
                       DHCP: Server


                           Press ESC or RETURN to Exit:
```

**Figure 29-4 Menu 24.2.1: System Maintenance: Information**

**Table 29-2 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<br>Name= xxx.baboo.mickey.com |
| Routing | Refers to the routing protocol used. |
| ProxiOS F/W Version | Refers to the ProxiOS (Proxicast Network Operating System) system firmware version. |
| 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. | |

## 29.4 Log and Trace

The LAN-Cell has a Syslog facility for message logging, and a trace function for viewing call-triggering packets.

```
              Menu 24.3 - System Maintenance - Log and Trace


          2. Syslog Loging
          4. Call-Triggering Packet


          Press ENTER to Confirm or ESC to Cancel
```

**Figure 29-5 Menu 24.3: System Maintenance: Log and Trace**

### 29.4.1 Syslog

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 - Unix Syslog**, as shown next.

```
                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:
```

**Figure 29-6 Menu 24.3.2: System Maintenance: Syslog**

You need to configure the syslog parameters described in the following table to activate syslog then choose what you want to log.

**Table 29-3 System Maintenance Menu Syslog Parameters**

| PARAMETER | DESCRIPTION |
|---|---|
| Syslog: | Syslog logging sends a log to an external syslog server used to store logs. |
| Active | Press [SPACE BAR] and then [ENTER] to turn syslog logging 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 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 11:19:27 192.168.202.2 Proxicast: board 0 line 0 channel 0, call 1, C01 Outgoing Call
dev=2 ch=0 40002
Jul 19 11:19:32 192.168.202.2 Proxicast: board 0 line 0 channel 0, call 1, C02 OutCall Connected
64000 40002
Jul 19 11:20:06 192.168.202.2 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 11:28:39 192.168.202.2 Proxicast: Packet Trigger: Protocol=1,
Data=4500003c100100001f010004c0a86614ca849a7b08004a5c020001006162636465666768696a6b6c6d6e6f707172
7374
Jul 19 11:28:56 192.168.202.2 Proxicast: Packet Trigger: Protocol=1,
Data=4500002c1b0140001f06b50ec0a86614ca849a7b0427001700195b3e00000000600220008cd40000020405b4
Jul 19 11:29:06 192.168.202.2 Proxicast: Packet Trigger: Protocol=1,
Data=45000028240140001f06ac12c0a86614ca849a7b0427001700195b451d1430135004000077600000
```

**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 port
Mar 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 11:42:44 192.168.202.2 Proxicast: ppp:LCP Closing
Jul 19 11:42:49 192.168.202.2 Proxicast: ppp:IPCP Closing
Jul 19 11:42:54 192.168.202.2 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)
08-01-2000       11:48:41 Local1.Notice    192.168.20.10    RAS: FW 172.21.1.80     :137  -
>172.21.1.80      :137  |UDP|default permit:<2,0>|B
08-01-2000       11:48:41 Local1.Notice    192.168.20.10    RAS: FW 192.168.77.88   :520  -
>192.168.77.88    :520  |UDP|default permit:<2,0>|B
```

```
08-01-2000       11:48:39 Local1.Notice    192.168.20.10    RAS: FW 172.21.1.50     ->172.21.1.50
|IGMP<2>|default permit:<2,0>|B
08-01-2000       11:48:39 Local1.Notice    192.168.20.10    RAS: FW 172.21.1.25     ->172.21.1.25
|IGMP<2>|default permit:<2,0>|B
```

## 29.4.2 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.

```
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...
```

**Figure 29-7 Call-Triggering Packet Example**

## 29.4.3 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.**

**Step 1.** From the main menu, select option 24 to open **Menu 24 - System Maintenance**.

**Step 2.** From this menu, select option 4. Diagnostic. This will open **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. Internet Setup Test

          System
            11. Reboot System



            Enter Menu Selection Number:

            Host IP Address= N/A
```

**Figure 29-8 Menu 24.4: System Maintenance: Diagnostic**

### 29.4.4 WAN DHCP

DHCP functionality can be enabled on the LAN or WAN as shown in Figure 29-9. 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 11.3 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.

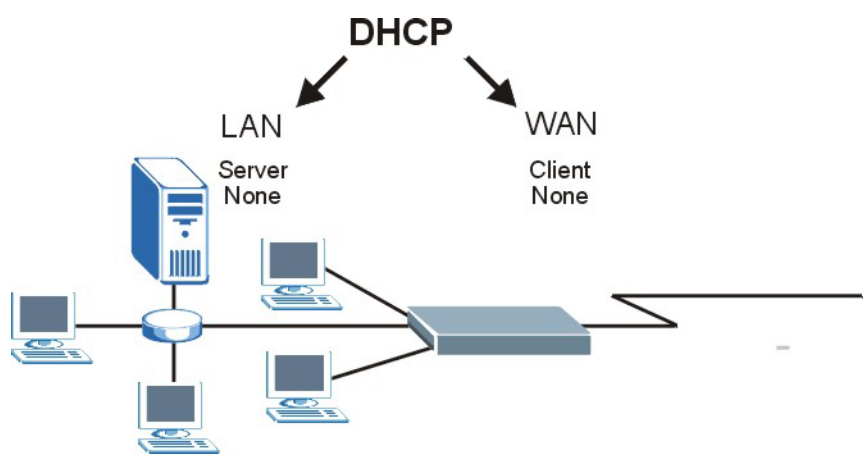



**Figure 29-9 WAN & LAN DHCP**

The following table describes the diagnostic tests available in menu 24.4 for your LAN-Cell and associated connections.

**Table 29-4 System Maintenance Menu Diagnostic**

| FIELD | DESCRIPTION |
|---|---|
| Ping Host | Enter 1 to ping any machine (with an IP address) on your LAN 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. |
| Internet Setup Test | Enter 4 to test the Internet setup. You can also test the Internet setup in **Menu 4 - Internet Access**. Please refer to the *Internet Access* chapter for more details. This feature is only available for dial-up connections using PPPoE or PPTP encapsulation. |
| Reboot System | Enter 11 to reboot the LAN-Cell. |

**Table 29-4 System Maintenance Menu Diagnostic**

| | |
|---|---|
| Host IP Address= | If you entered 1 in **Ping Host**, 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. | |

# Chapter 30
# 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.*

## 30.1 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.

## 30.2 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'ssettings, they can be saved back to your computer under a filename of your choosing.

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 **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 30-1 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), | *.rom |

**Table 30-1 Filename Conventions**

| | | | |
|---|---|---|---|
| | | the error log and the trace log. | |
| Firmware | Ras | This is the generic name for the Proxicast firmware on the LAN-Cell. | *.bin |

## 30.3 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.

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.

### 30.3.1 Backup Configuration

Follow the instructions as shown in the next screen.

```
              Menu 24.5 - System Maintenance - 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:
```

**Figure 30-1 Telnet into Menu 24.5**

### 30.3.2 Using the FTP Command from the Command Line

**Step 1.** Launch the FTP client on your computer.

**Step 2.** Enter "open", followed by a space and the IP address of your LAN-Cell.

**Step 3.** Press [ENTER] when prompted for a username.

**Step 4.** Enter your password as requested (the default is "1234").

**Step 5.** Enter "bin" to set transfer mode to binary.

**Step 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.

**Step 7.** Enter "quit" to exit the ftp prompt.

### 30.3.3 Example of FTP Commands from the Command Line

```
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
```

**Figure 30-2 FTP Session Example**

### 30.3.4 GUI-based FTP Clients

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

**Table 30-2 General Commands for GUI-based FTP Clients**

| COMMAND | DESCRIPTION |
|---|---|
| Host Address | Enter the address of the host server. |
| Login Type | Anonymous.<br>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.<br>Normal.<br>The server requires a unique User ID and Password to login. |
| Transfer Type | Transfer files in either ASCII (plain text format) or in binary mode. |
| Initial Remote Directory | Specify the default remote directory (path). |
| Initial Local Directory | Specify the default local directory (path). |

### 30.3.5 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 **Secured 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.
6. The firmware update resets the LAN-Cell's configuration to factory defaults and your specific configuration must be reloaded from a backup config file (see the README file with each firmware release for more information).

### 30.3.6 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.

**Step 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.

**Step 2.** Put the SMT in command interpreter (CI) mode by entering 8 in **Menu 24 – System Maintenance**.

**Step 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.

**Step 4.** Launch the TFTP client on your computer and connect to the LAN-Cell. Set the transfer mode to binary before starting data transfer.

**Step 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.

### 30.3.7 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.

### 30.3.8 GUI-based TFTP Clients

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

**Table 30-3 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 30.3.5* to read about configurations that disallow TFTP and FTP over WAN.

# 30.4 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.**

## 30.4.1 Restore Using FTP

For details about backup using (T)FTP please refer to earlier sections on FTP and TFTP file upload in this chapter.

```
                  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 transfer

 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:
```

**Figure 30-3 Telnet into Menu 24.6**

**Step 1.** Launch the FTP client on your computer.

**Step 2.** Enter "open", followed by a space and the IP address of your LAN-Cell.

**Step 3.** Press [ENTER] when prompted for a username.

**Step 4.** Enter your password as requested (the default is "1234").

**Step 5.** Enter "bin" to set transfer mode to binary.

**Step 6.** Find the "rom" file (on your computer) that you want to restore to your LAN-Cell.

**Step 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.

**Step 8.** Enter "quit" to exit the ftp prompt. The LAN-Cell will automatically restart after a successful restore process.

### 30.4.2 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
```

**Figure 30-4 Restore Using FTP Session Example**

Refer to *section 30.3.5* to read about configurations that disallow TFTP and FTP over WAN.

## 30.5 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 the previous *Restore Configuration* section 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.**

### 30.5.1 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.

```
            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:
```

**Figure 30-5 Telnet Into Menu 24.7.1: Upload System Firmware**

### 30.5.2 Configuration File Upload

You see the following screen when you telnet into menu 24.7.2.

```
        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:
```

**Figure 30-6 Telnet Into Menu 24.7.2: System Maintenance**

To upload the firmware and the configuration file, follow these examples

### 30.5.3 FTP File Upload Command from the DOS Prompt Example

**Step 1.** Launch the FTP client on your computer.

**Step 2.** Enter "open", followed by a space and the IP address of your LAN-Cell.

**Step 3.** Press [ENTER] when prompted for a username.

**Step 4.** Enter your password as requested (the default is "1234").

**Step 5.** Enter "bin" to set transfer mode to binary.

**Step 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.

**Step 7.** Enter "quit" to exit the ftp prompt.

### 30.5.4 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
```

**Figure 30-7 FTP Session Example of Firmware File Upload**

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

Refer to *section 30.3.5* to read about configurations that disallow TFTP and FTP over WAN.

### 30.5.5 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.

**Step 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.

**Step 2.** Put the SMT in command interpreter (CI) mode by entering 8 in **Menu 24 – System Maintenance**.

**Step 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.

**Step 4.** Launch the TFTP client on your computer and connect to the LAN-Cell. Set the transfer mode to binary before starting data transfer.

**Step 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.

### 30.5.6 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.

# Chapter 31
# System Maintenance Menus 8 to 10

*This chapter leads you through SMT menus 24.8 to 24.10.*

## 31.1 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. 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.**

```
                 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:
```

**Figure 31-1 Command Mode in Menu 24**

### 31.1.1 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.

### 31.1.2 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.

```
Copyright (c) 1994 - 2003 Proxicast
ras> ?
Valid commands are:
sys             exit            device          ether
poe             pptp            config          radius
ip              ipsec           ppp             certificates
cnm             radius          aux
ras>
```

**Figure 31-2 Valid Commands**

The following table describes some commands in this screen.

**Table 31-1 Valid Commands**

| COMMAND | DESCRIPTION |
|---|---|
| sys | The system commands display device information and configure device settings. |
| exit | This command returns you to the SMT main menu. |
| ether | These commands display Ethernet information and configure Ethernet settings. |
| aux | These commands display dial backup information and control the Cellular Modem. |
| ip | These commands display IP information and configure IP settings. |
| ipsec | These commands display IPSec information and configure IPSec settings. |
| aux | These command display and configure cellular modem (aux) settings. |

## 31.2 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.

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.

```
                Menu 24.9 - System Maintenance - Call Control

                  1. Budget Management
                  2. Call History


                        Enter Menu Selection Number:
```

**Figure 31-3 Call Control**

### 31.2.1 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.

```
                    Menu 24.9.3 - Budget Management

     Remote Node   Connection Time/Total Budget   Elapsed Time/Total Period

   1.ChangeMe               No Budget                    No Budget

   2.--------                  ---                          ---



                    Reset Node (0 to update screen):
```

**Figure 31-4 Budget Management**

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 31-2 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. | | |

### 31.2.2 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.

```
                        Menu 24.9.4 - 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):
```

**Figure 31-5 Call History**

The following table describes the fields in this screen.

**Table 31-3 Call History Fields**

| 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. | |

## 31.3 Time and Date Setting

There is 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.

```
                    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:
```

**Figure 31-6 Menu 24: System Maintenance**

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.

```
Menu 24.10 - System Maintenance - Time and Date Setting

Time Protocol= NTP (RFC-1305)
Time Server Address= tick.stdtime.gov.tw

Current Time:                        00 : 06 : 10
New Time (hh:mm:ss):                 00 : 06 : 08

Current Date:                        2000 - 01 - 01
New Date (yyyy-mm-dd):               2000 - 01 - 01

Time Zone= GMT

Daylight Saving= No
Start Date (mm-dd):                         01 - 01
End Date (mm-dd):                           01 - 01


          Press ENTER to Confirm or ESC to Cancel:
```

**Figure 31-7 Menu 24.10 System Maintenance: Time and Date Setting**

The following table describes the fields in this screen.

**Table 31-4 Menu 24.10 System Maintenance: Time and Date Setting**

| FIELD | DESCRIPTION |
|---|---|
| Time Protocol | Enter the time service protocol that your timeserver sends when you turn on the LAN-Cell. Not all timeservers support all protocols, so you may have to check with your ISP/network administrator or use trial and error to find a protocol that works. The main differences between them are the format.<br>**Daytime (RFC 867)** format is day/month/year/time zone of the server.<br>**Time (RFC-868)** format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0.<br>**NTP (RFC-1305)** the default, is similar to **Time (RFC-868)**.<br>**None** enter the time 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. The default is tick.stdtime.gov.tw |
| 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. |
| 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. |
| 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 | Enter the month and day that your daylight-savings time starts on if you selected **Yes** in the **Daylight Saving** field. |
| End Date | Enter the month and day that your daylight-savings time ends on if you selected **Yes** in the **Daylight Saving** field. |

**Table 31-4 Menu 24.10 System Maintenance: Time and Date Setting**

| FIELD | DESCRIPTION |
|---|---|
| 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. | |

## 31.3.1 Resetting the Time

The LAN-Cell resets the time in three instances:

i. On leaving menu 24.10 after making changes.

ii. When the LAN-Cell starts up, if there is a timeserver configured in menu 24.10.

iii. 24-hour intervals after starting.

# Chapter 32
# Remote Management

*This chapter covers remote management found in SMT menu 24.11.*

## 32.1 Remote Management

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

You may manage your LAN-Cell from a remote location via:

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

**When you Choose** WAN only **or** ALL **(LAN & WAN), you still need to configure a firewall rule to allow access.**

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

Enter 11 from menu 24 to bring up **Menu 24.11 – Remote Management Control**.

```
                 Menu 24.11 - Remote Management Control

   TELNET Server:     Port = 23         Access = ALL
                      Secure Client IP = 0.0.0.0
   FTP Server:        Port = 21         Access = ALL
                      Secure Client IP = 0.0.0.0
   SSH Server:        Certificate = auto_generated_self_signed_cert
                      Port = 0          Access = ALL
                      Secure Client IP = 0.0.0.0
   HTTPS Server:      Certificate = auto_generated_self_signed_cert
                      Authenticate Client Certificates = No
                      Port = 443        Access = ALL
                      Secure Client IP = 0.0.0.0
   HTTP Server:       Port = 80         Access = ALL
                      Secure Client IP = 0.0.0.0
   SNMP Service:      Port = 161        Access = ALL
                      Secure Client IP = 0.0.0.0
   DNS Service:       Port = 53         Access = ALL
                      Secure Client IP = 0.0.0.0
                 Press ENTER to Confirm or ESC to Cancel:
```

**Figure 32-1 Menu 24.11 – Remote Management Control**

The following table describes the fields in this screen.

**Table 32-1 Menu 24.11 – Remote Management Control**

| FIELD | DESCRIPTION | EXAMPLE |
|---|---|---|
| Telnet Server<br>FTP Server<br>SSH Server<br>HTTPS Server<br>HTTP Server<br>SNMP Service<br>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 remote management service. You may change the port number for a service if needed, but you must use the same port number to use that service for remote management. | 23 |
| Access | Select the access interface (if any) by pressing [SPACE BAR], then [ENTER] to choose from: **LAN only**, **WAN only**, **ALL** or **Disable**. | **LAN Only** (default) |
| 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. | 0.0.0.0 |
| Certificate | Select the certificate that the LAN-Cell will use to identify itself. | |
| 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. | | |

## 32.1.1 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 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.

# Part XIV:

## SMT Advanced Management

This part provides information on how to configure call scheduling, and VPN/IPSec.

**See the web configurator parts of this guide for background information on features configurable by web configurator and SMT.**

# Chapter 33
# Call Scheduling

*Call scheduling allows you to dictate when a remote node should be called and for how long.*

## 33.1 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.

```
                    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:
```

**Figure 33-1 Schedule Setup**

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.

```
                       Menu 26.1 - Schedule Set Setup

                Active= Yes
                Start Date(yyyy/mm/dd) = 2000 - 01 - 01
                How Often= Once
                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
```

**Figure 33-2 Schedule Set Setup**

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 33-1 Schedule Set Setup**

| FIELD | DESCRIPTION | OPTIONS |
|---|---|---|
| Active | Press [SPACE BAR] to select **Yes** or **No**. Choose **Yes** and press [ENTER] to activate the schedule set. | **Yes**<br>**No** |
| 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. | |
| 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. | **Once**<br>**Weekly** |
| 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. | |
| Weekday: | | |
| 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]. | **Yes**<br>**No**<br>**N/A** |
| Start Time | Enter the start time when you wish the schedule set to take effect in hour-minute format. | |
| Duration | Enter the maximum length of time this connection is allowed 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.<br>**Forced Down** means that the connection is blocked whether or not there is a demand call on the line.<br>**Enable Dial-On-Demand** means that this schedule permits a demand call on the line.<br>**Disable Dial-On-Demand** means that this schedule prevents a demand call on the line. | **Forced On**<br>**Forced Down**<br>**Enable Dial-On-Demand**<br>**Disable Dial-On-Demand** |
| 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.

```
                          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

                                               Edit Traffic Redirect= No


                      Press ENTER to Confirm or ESC to Cancel:
```

Apply your schedule sets here.

**Figure 33-3 Applying Schedule Set(s) to a Remote Node (PPPoE)**

You can apply up to four schedule sets, separated by commas, for one remote node. Change the schedule set numbers to your preference(s).

```
                          Menu 11.1 - Remote Node Profile

          Rem Node Name= ChangeMe              Route= IP
          Active= Yes

          Encapsulation= PPTP                  Edit IP= No
          Service Type= Standard               Telco Option:
          Service Name=N/A                       Allocated Budget(min)= 0
          Outgoing=                              Period(hr)= 0
            My Login=                            Schedules= 1,2,3,4
            My Password= ********                Nailed-up Connections=
            Authen= CHAP/PAP
                                               Session Options:
           PPTP :                                Edit Filter Sets= No
             My IP Addr=                         Idle Timeout(sec)= 100
             Server IP Addr=
             Connection ID/Name=               Edit Traffic Redirect= No


                      Press ENTER to Confirm or ESC to Cancel:
```

Apply your schedule sets here.

**Figure 33-4 Applying Schedule Set(s) to a Remote Node (PPTP)**

# Chapter 34
# VPN/IPSec Setup

*This chapter introduces the VPN SMT menus.*

## 34.1 Introduction

The VPN/IPSec main SMT menu has these main submenus:

1. Define VPN policies in menu 27.1 submenus, including security policies, endpoint IP addresses, peer IPSec router IP address and key management.
2. **Menu 27.2 - SA Monitor** allows you to manage (refresh or disconnect) your SA connections.

This is an overview of the VPN menu tree.

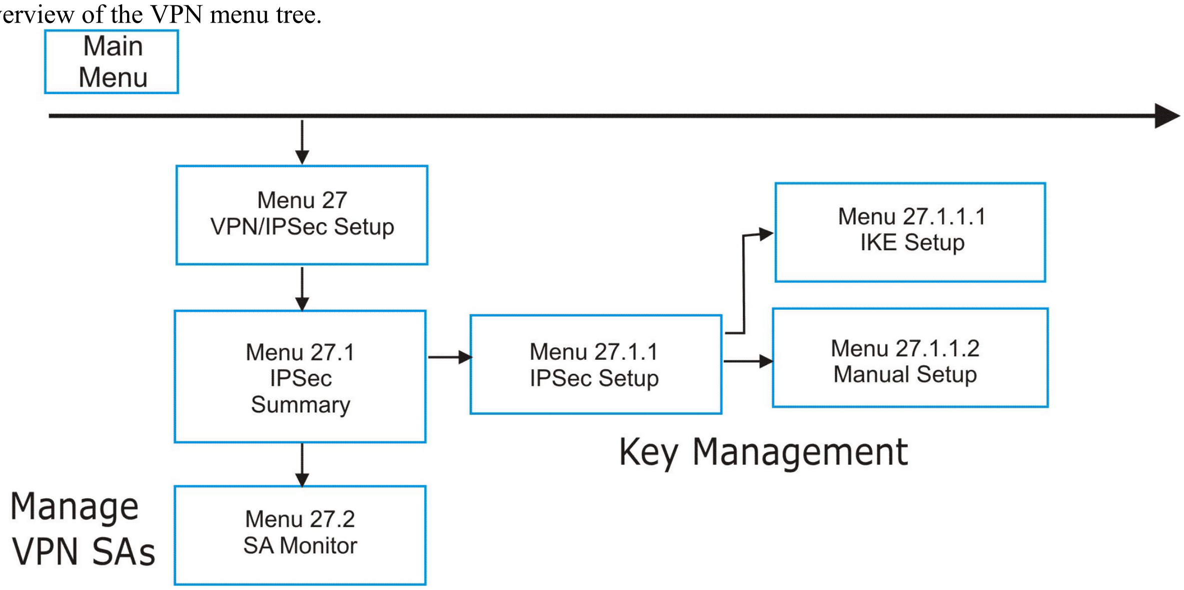



**Figure 34-1 VPN SMT Menu Tree**

From the main menu, enter 27 to display the first VPN menu (shown next).

```
                         Menu 27 - VPN/IPSec Setup

                   1. IPSec Summary
                   2. SA Monitor




                         Enter Menu Selection Number:
```

**Figure 34-2 Menu 27: VPN/IPSec Setup**

## 34.2 IPSec Summary Screen

Type 1 in menu 27 and then press [ENTER] to display **Menu 27.1 — IPSec Summary**. This is a summary read-only menu of your IPSec rules (tunnels). Edit or create an IPSec rule by selecting an index number and then configuring the associated submenus.

```
                              Menu 27.1 - IPSec Summary

 #      Name    A Local  Addr                           Encap  IPSec Algorithm
      Key Mgt     Remote Addr Start - Addr End / Mask          Secure Gw Addr
--- ---------- - -----------------   ----------------- ------ ----------------
001 taiwan     Y  192.168.1.35        192.168.1.38     Tunnel ESP DES-SHA1
    IKE           172.16.2.40         172.16.2.46             193.81.13.2
002 zw2        N  1.1.1.1             1.1.1.1          Tunnel AH  SHA1
    IKE           4.4.4.4             255.255.0.0             zw2test.zyxel






             Select Command=  None          Select Rule=  N/A

                   Press ENTER to Confirm or ESC to Cancel:
```

**Figure 34-3 Menu 27.1: IPSec Summary**

The following table describes the fields in this screen.

**Table 34-1 Menu 27.1: IPSec Summary**

| FIELD | DESCRIPTION | EXAMPLE |
|---|---|---|
| # | This is the VPN policy index number. | 1 |
| Name | This field displays the unique identification name for this VPN rule. The name may be up to 32 characters long but only 10 characters will be displayed here. | Taiwan |
| A | **Y** signifies that this VPN rule is active. | **Y** |
| Local Addr Start | When the **Addr Type** field in **Menu 27.1.1 IPSec Setup** is configured to **Single**, this is a static IP address on the LAN behind your LAN-Cell.<br><br>When the **Addr Type** field in **Menu 27.1.1 IPSec Setup** is configured to **Range**, this is the beginning (static) IP address, in a range of computers on the LAN behind your LAN-Cell.<br><br>When the **Addr Type** field in **Menu 27.1.1 IPSec Setup** is configured to **SUBNET**, this is a static IP address on the LAN behind your LAN-Cell. | 192.168.1.35 |

**Table 34-1 Menu 27.1: IPSec Summary**

| FIELD | DESCRIPTION | EXAMPLE |
|---|---|---|
| Addr End / Mask | When the **Addr Type** field in **Menu 27.1.1 IPSec Setup** is configured to **Single**, this is the same (static) IP address as in the **Local Addr Start** field.<br>When the **Addr Type** field in **Menu 27.1.1 IPSec Setup** is configured to **Range**, this is the end (static) IP address, in a range of computers on the LAN behind your LAN-Cell.<br>When the **Addr Type** field in **Menu 27.1.1 IPSec Setup** is configured to **SUBNET**, this is a subnet mask on the LAN behind your LAN-Cell. | 192.168.1.38 |
| Encap | This field displays **Tunnel** mode or **Transport** mode. See earlier for a discussion of these. You need to finish configuring the VPN policy in menu 27.1.1.1 or 27.1.1.2 if **???** is displayed. | **Tunnel** |
| IPSec Algorithm | This field displays the security protocols used for an SA. **ESP** provides confidentiality and integrity of data by encrypting the data and encapsulating it into IP packets. Encryption methods include 56-bit **DES**, 168-bit **3DES** and 128-bit **AES**. **NULL** denotes a tunnel without encryption.<br>**AH** (Authentication Header) provides strong integrity and authentication by adding authentication information to IP packets. This authentication information is calculated using header and payload data in the IP packet. This provides an additional level of security. **AH** choices are **MD5** (default - 128 bits) and **SHA -1**(160 bits)**.**<br>Both **AH** and **ESP** increase the LAN-Cell's processing requirements and communications latency (delay).<br>You need to finish configuring the VPN policy in menu 27.1.1.1 or 27.1.1.2 if **???** is displayed. | **ESP DES MD5** |
| Key Mgt | This field displays the SA's type of key management, (**IKE** or **Manual**). | **IKE** |
| Remote Addr Start | When the **Addr Type** field in **Menu 27.1.1 IPSec Setup** is configured to **Single**, this is a static IP address on the network behind the remote IPSec router.<br>When the **Addr Type** field in **Menu 27.1.1 IPSec Setup** is configured to **Range**, this is the beginning (static) IP address, in a range of computers on the network behind the remote IPSec router.<br>When the **Addr Type** field in **Menu 27.1.1 IPSec Setup** is configured to **SUBNET**, this is a static IP address on the network behind the remote IPSec router.<br>This field displays **N/A** when you configure the **Secure Gw Addr** field in SMT 27.1.1 to 0.0.0.0. | 172.16.2.40 |
| Addr End / Mask | When the **Addr Type** field in **Menu 27.1.1 IPSec Setup** is configured to **Single**, this is the same (static) IP address as in the **Remote Addr Start** field.<br>When the **Addr Type** field in **Menu 27.1.1 IPSec Setup** is configured to **Range**, this is the end (static) IP address, in a range of computers on the network behind the remote IPSec router.<br>When the **Addr Type** field in **Menu 27.1.1 IPSec Setup** is configured to **SUBNET**, this is a subnet mask on the network behind the remote IPSec router.<br>This field displays **N/A** when you configure the **Secure Gw Addr** field in SMT 27.1.1 to 0.0.0.0. | 172.16.2.46 |
| Secure GW Addr | This is the WAN IP address or the domain name (up to the first 15 characters are displayed) of the IPSec router with which you are making the VPN connection. This field displays **0.0.0.0** when you configure the **Secure Gw Addr** field in SMT 27.1.1 to 0.0.0.0. | 193.81.13.2 |

**Table 34-1 Menu 27.1: IPSec Summary**

| FIELD | DESCRIPTION | EXAMPLE |
|---|---|---|
| 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.<br>Select **None** and then press [ENTER] to go to the "Press ENTER to Confirm…" prompt.<br>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 VPN rule is deleted, subsequent rules do not move up in the page list.<br>Use **Go To Rule** to view the page where your desired rule is listed.<br>Select **Next Page** or **Previous Page** to view the next or previous page of rules (respectively). | **None** |
| Select Rule | Type the VPN rule index number you wish to edit or delete and then press [ENTER]. | 3 |
| 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. | | |

## 34.3 IPSec Setup

Select **Edit** in the **Select Command** field; type the index number of a rule in the **Select Rule** field and press [ENTER] to edit the VPN using the menu shown next.

```
                    Menu 27.1.1 - IPSec Setup

      Index #= 2         Name= zw2
      Active= No         Keep Alive= No    Nat Traversal= No
      Local ID type= IP          Content=
      My IP Addr= 0.0.0.0
      Peer ID type= IP           Content=
      Secure Gateway Address= zw2test.proxicast
      Protocol= 0        DNS Server= 0.0.0.0
      Local:  Addr Type= SINGLE
          IP Addr Start= 1.1.1.1           End/Subnet Mask= N/A
             Port Start= 0                 End= N/A
      Remote: Addr Type= SUBNET
          IP Addr Start= 4.4.4.4           End/Subnet Mask= 255.255.0.0
             Port Start= 0                 End= N/A
      Enable Replay Detection= No
      Key Management= IKE
      Edit Key Management Setup= No

                Press ENTER to Confirm or ESC to Cancel:
```

**Figure 34-4 Menu 27.1.1: IPSec Setup**

**You must also configure menu 27.1.1.1 or menu 27.1.1.2 to fully configure and use a VPN.**

The following table describes the fields in this screen.

**Table 34-2 Menu 27.1.1: IPSec Setup**

| FIELD | DESCRIPTION | EXAMPLE |
|---|---|---|
| Index | This is the VPN rule index number you selected in the previous menu. | **1** |
| Name | Enter a unique identification name for this VPN rule. The name may be up to 32 characters long but only 10 characters will be displayed in **Menu 27.1 - IPSec Summary**. | Taiwan |
| Active | Press [SPACE BAR] to choose either **Yes** or **No**. Choose **Yes** and press [ENTER] to activate the VPN tunnel. This field determines whether a VPN rule is applied before a packet leaves the firewall. | **Yes** |

**Table 34-2 Menu 27.1.1: IPSec Setup**

| FIELD | DESCRIPTION | EXAMPLE |
|---|---|---|
| Keep Alive | Press [SPACE BAR] to choose either **Yes** or **No**. Choose **Yes** and press [ENTER] to have the LAN-Cell automatically re-initiate the SA after the SA lifetime times out, even if there is no traffic. The remote IPSec router must also have keep alive enabled in order for this feature to work. | **No** |
| 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.<br>The remote IPSec router must also have NAT traversal enabled. You can use NAT traversal with **ESP** protocol using **Transport** or **Tunnel** mode, but not with **AH** protocol nor with **Manual** key management.<br>In order for an IPSec router behind a NAT router to receive an initiating IPSec packet, set the NAT router to forward UDP port 500 to the IPSec router behind the NAT router. | **No** |
| Local ID type | Press [SPACE BAR] to choose **IP**, **DNS**, or **E-mail** and press [ENTER].<br>Select **IP** to identify this LAN-Cell by its IP address.<br>Select **DNS** to identify this LAN-Cell by a domain name.<br>Select **E-mail** to identify this LAN-Cell by an e-mail address. | |
| 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 IP Address** field (refer to the My IP Address field description) if you configure the local **Content** field to **0.0.0.0** or leave it blank.<br>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.<br>➢ When there is a NAT router between the two IPSec routers.<br>➢ 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.<br>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. | |
| My IP Addr | Enter the IP address of your LAN-Cell. 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.<br>The VPN tunnel has to be rebuilt if this IP address changes. | 0.0.0.0 |
| Peer ID type | Press [SPACE BAR] to choose **IP**, **DNS**, or **E-mail** and press [ENTER].<br>Select **IP** to identify the remote IPSec router by its IP address.<br>Select **DNS** to identify the remote IPSec router by a domain name.<br>Select **E-mail** to identify the remote IPSec router by an e-mail address. | |

**Table 34-2 Menu 27.1.1: IPSec Setup**

| FIELD | DESCRIPTION | EXAMPLE |
|---|---|---|
| Content | When you select **IP** in the **Peer ID type** field, type the IP address of the computer with which you will make the VPN connection in the peer **Content** field. The LAN-Cell automatically uses the address in the **Secure Gateway Address** field (refer to the **Secure Gateway Address** field description) if you configure the peer **Content** field to **0.0.0.0** or leave it blank.<br>It is recommended that you type an IP address other than **0.0.0.0** in the peer **Content** field or use the **DNS** or **E-mail** ID type in the following situations.<br>➢ When there is a NAT router between the two IPSec routers.<br>➢ When you want the LAN-Cell to distinguish between VPN connection requests that come in from remote IPSec routers with dynamic WAN IP addresses.<br>When you select **DNS** or **E-mail** in the **Peer ID type** field, type a domain name or e-mail address by which to identify the remote IPSec router in the peer **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. | |
| Secure Gateway Address | Type the IP address or the domain name (up to 31 characters) of the IPSec router with which you're making the VPN connection.<br>Set this field to 0.0.0.0 if the remote IPSec router has a dynamic WAN IP address (the **Key Management** field must be set to **IKE**, see later). | Zw50test.com.tw |
| Protocol | Enter 1 for ICMP, 6 for TCP, 17 for UDP, etc. 0 is the default and signifies any protocol. | 0 |
| DNS Server | If there is a private DNS server that services the VPN, type its IP address here. The LAN-Cell assigns this additional DNS server to the LAN-Cell's DHCP clients that have IP addresses in this IPSec rule's range of local addresses.<br>A DNS server allows clients on the VPN to find other computers and servers on the VPN by their (private) domain names. | |
| Local | Local IP addresses must be static and correspond to the remote IPSec router's configured remote IP addresses.<br>Two active SAs can have the same configured 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.<br>In order to have more than one active rule with the **Secure Gateway Address** field set to **0.0.0.0**, the ranges of the local IP addresses cannot overlap between rules.<br>If you configure an active rule with **0.0.0.0** in the **Secure 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 **Secure Gateway Address** field set to **0.0.0.0**. | |
| Addr Type | Press [SPACE BAR] to choose **SINGLE**, **RANGE**, or **SUBNET** and press [ENTER]. Select **SINGLE** with a single IP address. Select **RANGE** for a specific range of IP addresses. Select **SUBNET** to specify IP addresses on a network by their subnet mask. | **SINGLE** |

**Table 34-2 Menu 27.1.1: IPSec Setup**

| FIELD | DESCRIPTION | EXAMPLE |
|---|---|---|
| IP Addr Start | When the **Addr Type** field is configured to **Single**, enter a static IP address on the LAN behind your LAN-Cell.<br>When the **Addr Type** field is configured to **Range**, enter the beginning (static) IP address, in a range of computers on your LAN behind your LAN-Cell.<br>When the **Addr Type** is configured to **SUBNET**, this is a (static) IP address on the LAN behind your LAN-Cell. | 192.168.1.35 |
| End/Subnet Mask | When the **Addr Type** field is configured to **Single**, this field is **N/A**.<br>When the **Addr Type** field is configured to **Range**, enter the end (static) IP address, in a range of computers on the LAN behind your LAN-Cell.<br>When the **Addr Type** field is configured to **SUBNET**, this is a subnet mask on the LAN behind your LAN-Cell. | 192.168.1.38 |
| Port Start | 0 is the default and signifies any port. Type a port number from 0 to 65535. You cannot create a VPN tunnel if you try to connect using a port number that does not match this port number or range of port numbers.<br>Some of the most common IP ports are: 21, FTP; 53, DNS; 23, Telnet; 80, HTTP; 25, SMTP; 110, POP3 | 0 |
| End | Enter a port number in this field to define a port range. This port number must be greater than that specified in the previous field. This field is **N/A** when 0 is configured in the **Port Start** field. | N/A |
| Remote | Remote IP addresses must be static and correspond to the remote IPSec router's configured local IP addresses. The remote fields are **N/A** when the **Secure Gateway Address** field is configured to 0.0.0.0.<br>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. | |
| Addr Type | Press [SPACE BAR] to choose **SINGLE**, **RANGE**, or **SUBNET** and press [ENTER]. Select **SINGLE** with a single IP address. Use **RANGE** for a specific range of IP addresses. Use **SUBNET** to specify IP addresses on a network by their subnet mask. | **SUBNET** |
| IP Addr Start | When the **Addr Type** field is configured to **Single**, enter a static IP address on the network behind the remote IPSec router.<br>When the **Addr Type** field is configured to **Range**, enter the beginning (static) IP address, in a range of computers on the network behind the remote IPSec router.<br>When the **Addr Type** field is configured to **SUBNET**, enter a static IP address on the network behind the remote IPSec router.<br>This field displays **N/A** when you configure the **Secure Gateway Address** field to 0.0.0.0. | 4.4.4.4 |
| End/Subnet Mask | When the **Addr Type** field is configured to **Single**, this field is **N/A**.<br>When the **Addr Type** field is configured to **Range**, enter the end (static) IP address, in a range of computers on the network behind the remote IPSec router.<br>When the **Addr Type** field is configured to **SUBNET**, enter a subnet mask on the network behind the remote IPSec router.<br>This field displays **N/A** when you configure the **Secure Gateway Address** field to 0.0.0.0. | 255.255.0.0 |

**Table 34-2 Menu 27.1.1: IPSec Setup**

| FIELD | DESCRIPTION | EXAMPLE |
|---|---|---|
| Port Start | 0 is the default and signifies any port. Type a port number from 0 to 65535. Someone behind the remote IPSec router cannot create a VPN tunnel when attempting to connect using a port number that does not match this port number or range of port numbers.<br>Some of the most common IP ports are: 21, FTP; 53, DNS; 23, Telnet; 80, HTTP; 25, SMTP; 110, POP3. | 0 |
| End | Enter a port number in this field to define a port range. This port number must be greater than that specified in the previous field. This field is **N/A** when 0 is configured in the **Port Start** field. | |
| 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 setting this field to **Yes**.<br>Press [SPACE BAR] to select **Yes** or **No**. Choose **Yes** and press [ENTER] to enable replay detection. | **No** |
| Key Management | Press [SPACE BAR] to choose either **IKE** or **Manual** and then press [ENTER]. **Manual** is useful for troubleshooting if you have problems using **IKE** key management. | **IKE** |
| Edit Key Management Setup | Press [SPACE BAR] to change the default **No** to **Yes** and then press [ENTER] to go to a key management menu for configuring your key management setup (described later). If you set the **Key Management** field to **IKE**, this will take you to **Menu 27.1.1.1 – IKE Setup**. If you set the **Key Management** field to **Manual**, this will take you to **Menu 27.1.1.2 – Manual Setup**. | **No** |
| 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. | | |

## 34.4 IKE Setup

To edit this menu, the **Key Management** field **Menu 27.1.1 – IPSec Setup** must be set to **IKE**. Move the cursor to the **Edit Key Management Setup** field in **Menu 27.1.1 – IPSec Setup**; press [SPACE BAR] to select **Yes** and then press [ENTER] to display **Menu 27.1.1.1 – IKE Setup**.

```
                          Menu 27.1.1.1 - IKE Setup

      Phase 1
        Negotiation Mode= Main
        Authentication Method= PreShare Key
        PSK= qwer1234
        Certificate= N/A
        Encryption Algorithm= DES
        Authentication Algorithm= MD5
        SA Life Time (Seconds)= 300
        Key Group= DH1
      Phase 2
        Active Protocol= ESP
        Encryption Algorithm= DES
        Authentication Algorithm= MD5
        SA Life Time (Seconds)= 2880
        Encapsulation= Tunnel
        Perfect Forward Secrecy (PFS)= None

                    Press ENTER to Confirm or ESC to Cancel:
Press Space Bar to Toggle.
```

**Figure 34-5 Menu 27.1.1.1: IKE Setup**

**Table 34-3 Menu 27.1.1.1: IKE Setup**

| FIELD | DESCRIPTION | EXAMPLE |
|---|---|---|
| Phase 1 | | |
| Negotiation Mode | Press [SPACE BAR] to choose from **Main** or **Aggressive** and then press [ENTER]. See earlier for a discussion of these modes. Multiple SAs connecting through a secure gateway must have the same negotiation mode. | **Main** |
| Authentication Method | Press [SPACE BAR] to choose from **PreShare Key** or **RSA SIG** and then press [ENTER]. | |
| PSK | LAN-Cell gateways authenticate an IKE VPN session by matching pre-shared keys. Pre-shared keys are best for small networks with fewer than ten nodes. Enter your pre-shared key here. Enter up to 31 characters. Any character may be used, including spaces, but trailing spaces are truncated.<br>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 | Press [SPACE BAR] to choose the certificate to use for this VPN tunnel. You must have certificates already configured in the **My Certificates** screen | |
| 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. LAN-Cell **DES** encryption algorithm uses a 56-bit key.<br>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 slightly increased latency and decreased throughput.<br>This implementation of AES uses a 128-bit key. **AES** is faster than **3DES**.<br>Press [SPACE BAR] to choose from **DES**, **3DES** or **AES** and then press [ENTER]. | **DES** |
| 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 slightly slower.<br>Press [SPACE BAR] to choose from **SHA1** or **MD5** and then press [ENTER]. | **SHA1** |
| SA Life Time (Seconds) | Define the length of time before an IKE Security Association automatically renegotiates in this field. It may range from 180 to 3,000,000 seconds (almost 35 days).<br>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. | 28800 (default) |
| 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. | **DH1** |
| Phase 2 | | |
| Active Protocol | Press [SPACE BAR] to choose from **ESP** or **AH** and then press [ENTER]. See earlier for a discussion of these protocols. | **ESP** |
| Encryption Algorithm | Press [SPACE BAR] to choose from **NULL**, **DES**, **3DES** or **AES** and then press [ENTER]. Select **NULL** to set up a tunnel without encryption. | **DES** |
| Authentication Algorithm | Press [SPACE BAR] to choose from **SHA1** or **MD5** and then press [ENTER]. | **MD5** |
| SA Life Time (Seconds) | Define the length of time before an IPSec Security Association automatically renegotiates in this field. It may range from 180 to 3,000,000 seconds (almost 35 days). | 28800 (default) |

**Table 34-3 Menu 27.1.1.1: IKE Setup**

| FIELD | DESCRIPTION | EXAMPLE |
|---|---|---|
| Encapsulation | Press [SPACE BAR] to choose from **Tunnel** mode or **Transport** mode and then press [ENTER]. See earlier for a discussion of these. | **Tunnel** |
| Perfect Forward Secrecy (PFS) | Perfect Forward Secrecy (PFS) is disabled (**None**) by default in phase 2 IPSec SA setup. This allows faster IPSec setup, but is not so secure. Press [SPACE BAR] and choose from **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). | **None** |
| 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. | | |

# 34.5 Manual Setup

You only configure **Menu 27.1.1.2 – Manual Setup** when you select **Manual** in the **Key Management** field in **Menu 27.1.1 – IPSec Setup**. Manual key management is useful if you have problems with **IKE** key management.

## 34.5.1 Active Protocol

This field is a combination of mode and security protocols used for the VPN. See the *Web Configurator User's Guide* for more information on these parameters.

**Table 34-4 Active Protocol: Encapsulation and Security Protocol**

| MODE | SECURITY PROTOCOL |
|---|---|
| Tunnel | ESP |
| Transport | AH |

## 34.5.2 Security Parameter Index (SPI)

To edit this menu, move the cursor to the **Edit Manual Setup** field in **Menu 27.1.1 – IPSec Setup** press [SPACE BAR] to select **Yes** and then press [ENTER] to go to **Menu 27.1.1.2 – Manual Setup**.

```
     Menu 27.1.1.2 - Manual Setup
Active Protocol= ESP Tunnel

ESP Setup
  SPI (Decimal)=
  Encryption Algorithm= DES
    Key1=
    Key2= N/A
    Key3= N/A
  Authentication Algorithm= MD5
    Key= N/A

AH Setup
  SPI (Decimal)= N/A
  Authentication Algorithm= N/A
    Key=

      Press ENTER to Confirm or ESC to Cancel:
```

**Figure 34-6 Menu 27.1.1.2: Manual Setup**

**Table 34-5 Menu 27.1.1.2: Manual Setup**

| FIELD | DESCRIPTION | EXAMPLE |
|---|---|---|
| Active Protocol | Press [SPACE BAR] to choose from **ESP Tunnel**, **ESP Transport**, **AH Tunnel** or **AH Transport** and then press [ENTER]. Choosing an **ESP** combination causes the **AH Setup** fields to be non-applicable (**N/A**) | **ESP Tunnel** |
| ESP Setup | The **ESP Setup** fields are **N/A** if you chose an **AH Active Protocol**. | |
| SPI (Decimal) | The **SPI** must be unique and from one to four integers ("0" to "9"). | 1234 |
| Encryption Algorithm | Press [SPACE BAR] to choose from **NULL**, **3DES** or **DES** and then press [ENTER]. Fill in the **Key1** field below when you choose **DES** and fill in fields **Key1** to **Key3** when you choose **3DES**. Select **NULL** to set up a tunnel without encryption. When you select **NULL**, you do not enter any encryption keys. | **DES** |
| Key1 | Enter a unique eight-character key. Any character may be used, including spaces, but trailing spaces are truncated.<br><br>Fill in the **Key1** field when you choose **DES** and fill in fields **Key1** to **Key3** when you choose **3DES**. | 89abcde |
| Key2 | Enter a unique eight-character key. It can be comprised of any character including spaces (but trailing spaces are truncated). | |
| Key3 | Enter a unique eight-character key. It can be comprised of any character including spaces (but trailing spaces are truncated). | |
| Authentication Algorithm | Press [SPACE BAR] to choose from **MD5** or **SHA1** and then press [ENTER]. | **MD5** |
| Key | Enter the authentication key to be used by IPSec if applicable. The key must be unique. Enter 16 characters for **MD5** authentication and 20 characters for **SHA-1** authentication. Any character may be used, including spaces, but trailing spaces are truncated. | 123456789a bcde |
| AH Setup | The **AH Setup** fields are **N/A** if you chose an **ESP Active Protocol**. | |
| SPI (Decimal) | The **SPI** must be from one to four unique decimal characters ("0" to "9") long. | **N/A** |
| Authentication Algorithm | Press [SPACE BAR] to choose from **MD5** or **SHA1** and then press [ENTER]. | **N/A** |
| Key | Enter the authentication key to be used by IPSec if applicable. The key must be unique. Enter 16 characters for **MD5** authentication and 20 characters for **SHA-1** authentication. Any character may be used, including spaces, but trailing spaces are truncated. | **N/A** |
| 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. | | |

# Chapter 35
# SA Monitor

*This chapter teaches you how to manage your SAs by using the SA Monitor in SMT menu 27.2.*

## 35.1 Introduction

A Security Association (SA) is the group of security settings related to a specific VPN tunnel. This menu (shown next) displays active VPN connections.

**When there is outbound traffic but no inbound traffic, the SA times out automatically after two minutes. A tunnel with no outbound or inbound traffic is "idle" and does not timeout until the SA lifetime period expires. See the *Web Configurator User's Guide on* keep alive to have the LAN-Cell renegotiate an IPSec SA when the SA lifetime expires, even if there is no traffic.**

## 35.2 Using SA Monitor

1. Use the **Refresh** function to display active VPN connections.
2. Use the **Disconnect** function to cut off active connections.

Type 2 in **Menu 27 - VPN/IPSec Setup**, and then press [ENTER] to go to **Menu 27.2 - SA Monitor**.

```
                              Menu 27.2 - SA Monitor

  #                  Name                        Encap.      IPSec ALgorithm
 ---   -------------------------------------   -----------   ----------------
 1          Taiwan : 3.3.3.1 - 3.3.3.3.100         Tunnel     ESP DES MD5
 2









                     Select Command= Refresh
                     Select Connection= N/A

 Press ENTER to Confirm or ESC to Cancel:
```

**Figure 35-1 Menu 27.2: SA Monitor**

**Table 35-1 Menu 27.2: SA Monitor**

| FIELD | DESCRIPTION | EXAMPLE |
|---|---|---|
| # | This is the security association index number. | |
| Name | This field displays the identification name for this VPN policy. This name is unique for each connection where the secure gateway IP address is a public static IP address.<br><br>When the secure gateway IP address is 0.0.0.0 (as discussed in the last chapter), there may be different connections using this same VPN rule. In this case, the name is followed by the remote IP address as configured in **Menu 27.1.1. – IPSec Setup**. Individual connections using the same VPN rule may be terminated without affecting other connections using the same rule. | **Taiwan** |
| Encap. | This field displays **Tunnel** mode or **Transport** mode. See previous for discussion. | **Tunnel** |
| IPSec | This field displays the security protocols used for an SA. **ESP** provides confidentiality and integrity of data by encrypting the data and encapsulating it | **ESP DES** |

# Part XV:

## General Appendices

This part provides background information about troubleshooting, setting up your computer's IP address, triangle route, how functions are related, PPPoE, PPTP, IP subnetting and safety warnings.

# Appendix A Troubleshooting

*This chapter covers potential problems and possible remedies. After each problem description, some instructions are provided to help you to diagnose and to solve the problem. Please see our included disk for further information.*

### Problems Starting Up the LAN-Cell

**Chart 1 Troubleshooting the Start-Up of Your LAN-Cell**

| PROBLEM | CORRECTIVE ACTION |
|---|---|
| None of the LEDs turn on when you turn on the LAN-Cell. | Make sure that you have the included power adaptor or cord connected to the LAN-Cell and to an appropriate power source. |
| | If the error persists, you may have a hardware problem. In this case, you should contact your vendor. |

### Problems with the Password

**Chart 2 Troubleshooting the Password**

| PROBLEM | CORRECTIVE ACTION |
|---|---|
| Cannot access the LAN-Cell. | The password field is case sensitive. Make sure that you enter the correct password using the proper casing. |
| | Use the Reset button to restore the factory default configuration file. This will restore all of the factory defaults including the password. See the *Resetting the LAN-Cell* section in the *Introducing the Web Configurator* chapter for details. |

### Problems with the LAN Interface

**Chart 3 Troubleshooting the LAN Interface**

| PROBLEM | CORRECTIVE ACTION |
|---|---|
| Cannot access the LAN-Cell from the LAN. | Check your Ethernet cable type and connections. Refer to the *Quick Start Guide* for LAN connection instructions. |
| | Make sure the computer's Ethernet adapter is installed and functioning properly. |
| Cannot ping any computer on the LAN. | Check the 10M/100M LAN LEDs on the front panel. One of these LEDs should be on. If they are off, check the cables between your LAN-Cell and hub or the station. |
| | Verify that the IP address and the subnet mask of the LAN-Cell and the computers are on the same subnet. |

### Problems with the WAN Interface

**Chart 4 Troubleshooting the WAN Interface**

| PROBLEM | CORRECTIVE ACTION |
|---|---|
| Cannot get WAN IP address from the ISP. | The ISP provides the WAN IP address after authentication. Authentication may be through the user name and password, the MAC address or the host name. Use the following corrective actions to make sure the ISP can authenticate your connection. |
| | You need a username and password if you're using PPPoE or PPTP encapsulation. Make sure that you have entered the correct **Service Type**, **User Name** and **Password** (the user name and password are case sensitive). Refer to the *WAN Screens* chapter (web configurator) or the *Internet Access* chapter (SMT). |

**Chart 4 Troubleshooting the WAN Interface**

| | |
|---|---|
| | If your ISP requires MAC address authentication, you should clone the MAC address from your computer on the LAN as the LAN-Cell's WAN MAC address. Refer to the *WAN Screens* chapter (web configurator) or the *WAN and Cellular Modem Setup* chapter (SMT). It is recommended that you clone your computer's MAC address, even if your ISP presently does not require MAC address authentication. |
| | If your ISP requires host name authentication, configure your computer's name as the LAN-Cell's system name. Refer to the *System Setup* (web configurator) Setup or the *General Setup* chapter (SMT). |

### Problems with Internet Access

**Chart 5 Troubleshooting Internet Access**

| PROBLEM | CORRECTIVE ACTION |
|---|---|
| Cannot access the Internet. | Connect your cable/DSL modem with the LAN-Cell using the appropriate cable.<br>Check with the manufacturer of your cable/DSL device about your cable requirement because some devices may require crossover cable and others a regular straight-through cable. |
| | Refer to the *WAN Screens* chapter (web configurator) or the *Internet Access* chapter (SMT) and verify your settings. |

### Problems with Remote Management

**Chart 6 Troubleshooting Telnet**

| PROBLEM | CORRECTIVE ACTION |
|---|---|
| Cannot access the LAN-Cell from the LAN or WAN. | Refer to the *Remote Management Limitations* section in the *Remote Management* chapter for scenarios when remote management may not be possible. |
| | When NAT is enabled:<br>➢ Use the LAN-Cell's WAN IP address when configuring from the WAN.<br>➢ Use the LAN-Cell's LAN IP address when configuring from the LAN. |
| | Refer to the *Problems with the LAN Interface* section for instructions on checking your LAN connection. |
| | Refer to the *Problems with the WAN Interface* section for instructions on checking your WAN connection. |

# Appendix 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.

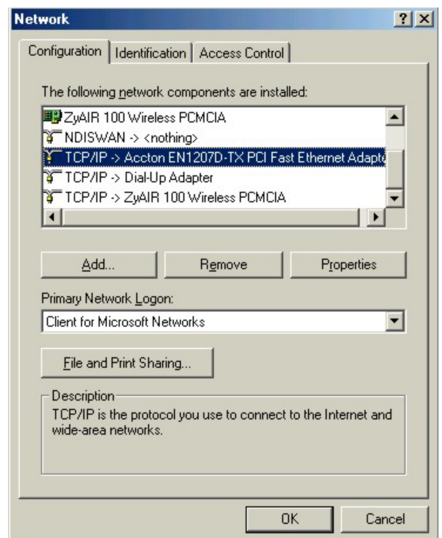
TCP/IP should already be installed on computers using Windows NT/2000/XP, Macintosh OS 7 and later operating systems.

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 (192.168.1.2 to 192.168.1.254 range with a subnet mask of 255.255.255.0.) as the default LAN-Cell's LAN port IP address (192.168.1.1).

### Windows 95/98/Me

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




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:

a. In the **Network** window, click **Add**.

b. Select **Adapter** and then click **Add**.

c. Select the manufacturer and model of your network adapter and then click **OK**.

If you need TCP/IP:

a. In the **Network** window, click **Add**.

b. Select **Protocol** and then click **Add**.

c. Select **Microsoft** from the list of **manufacturers**.

d. Select **TCP/IP** from the list of network protocols and then click **OK**.

If you need Client for Microsoft Networks:

a. Click **Add**.

b. Select **Client** and then click **Add**.

c. Select **Microsoft** from the list of manufacturers.

d. Select **Client for Microsoft Networks** from the list of network clients and then click **OK**.

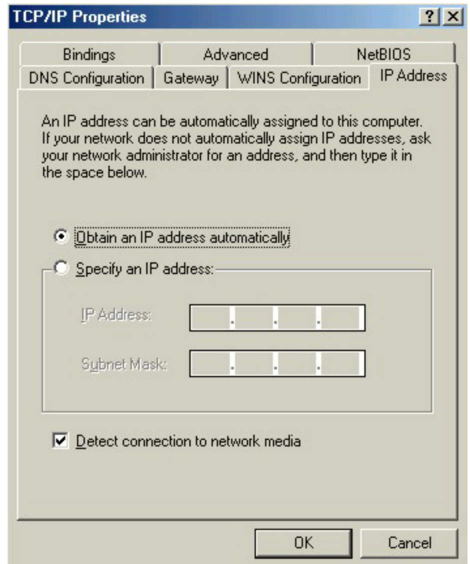
e. Restart your computer so the changes you made take effect.

In the **Network** window **Configuration** tab, select your network adapter's TCP/IP entry and click **Properties**.

1. Click the **IP Address** tab.

   -If your IP address is dynamic, select **Obtain an IP address automatically**.

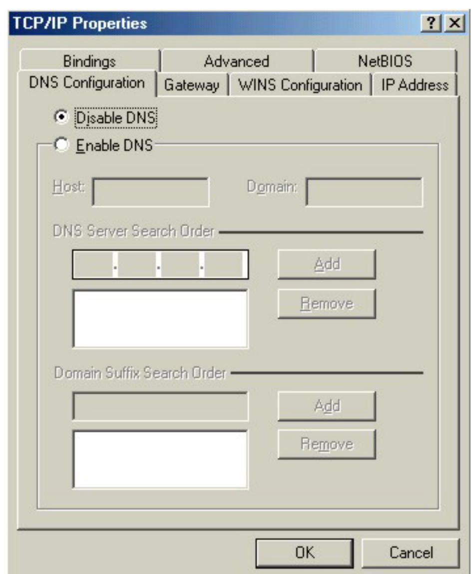
   -If you have a static IP address, select **Specify an IP address** and type your information into the **IP Address** and **Subnet Mask** fields.




2. Click the **DNS** Configuration tab.

   -If you do not know your DNS information, select **Disable DNS**.

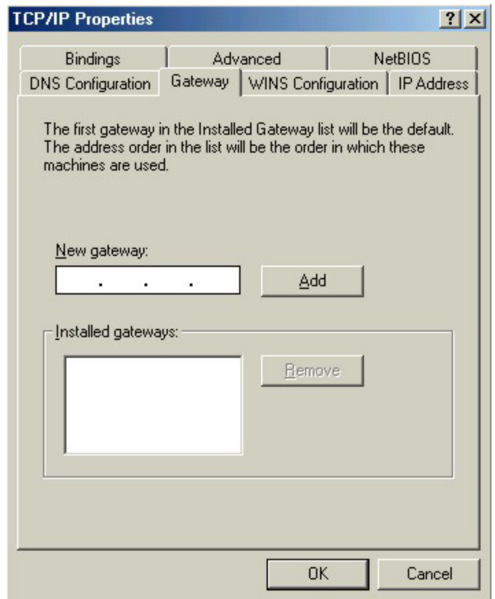
   -If you know your DNS information, select **Enable DNS** and type the information in the fields below (you may not need to fill them all in).




3. 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**.




4. Click **OK** to save and close the **TCP/IP Properties** window.

5. Click **OK** to close the **Network** window. Insert the Windows CD if prompted.

6. Turn on your LAN-Cell and restart your computer when prompted.

Verifying Your Computer's IP Address

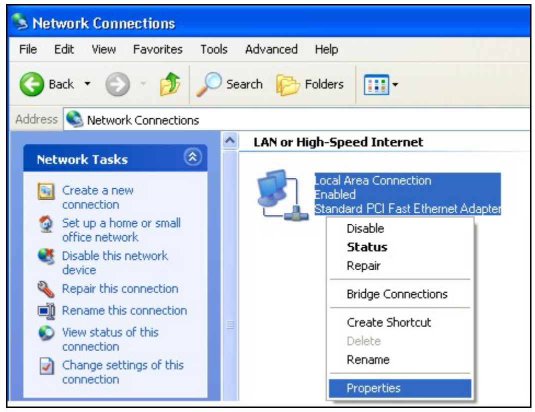
1. Click **Start** and then **Run**.
2. In the **Run** window, type "winipcfg" and then click **OK** to open the **IP Configuration** window.
3. Select your network adapter. You should see your computer's IP address, subnet mask and default gateway.

### Windows 2000/NT/XP

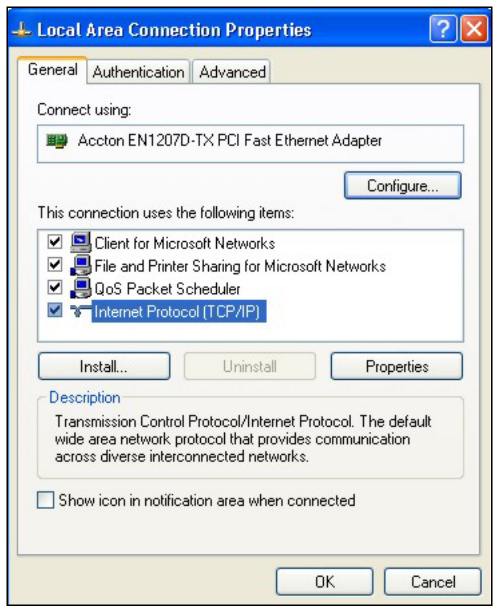
1. For Windows XP, click **Start**, **Control Panel**. In Windows 2000/NT, click **Start**, **Settings**, **Control Panel**.

2. For Windows XP, click **Network Connections**. For Windows 2000/NT, click **Network and Dial-up Connections**.


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




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

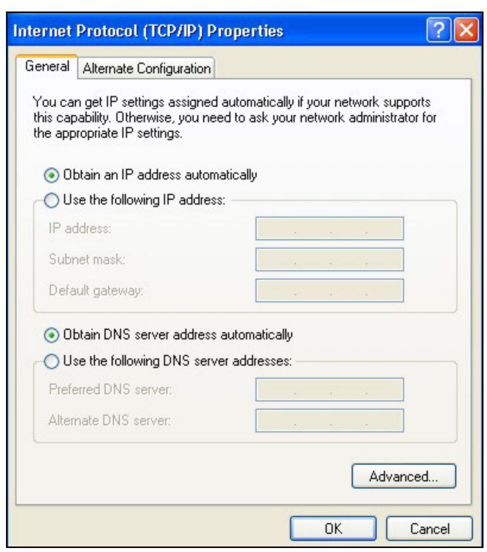



5. The **Internet Protocol TCP/IP Properties** window opens (the **General tab** in Windows XP).

   -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**.



6. -If you do not know your gateway's IP address, remove any previously installed gateways in the **IP Settin**gs 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.

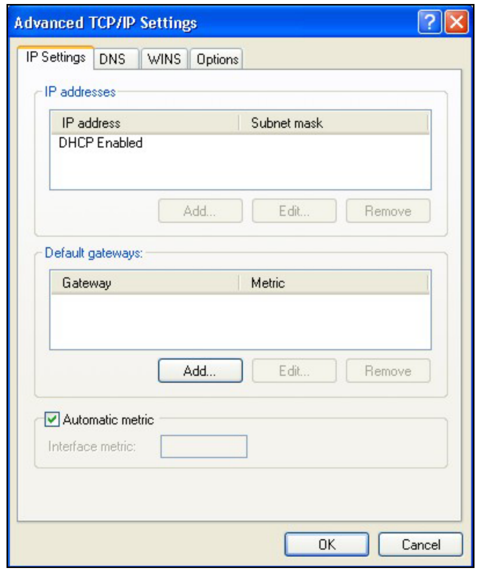
   -Configure additional default gateways in the **IP Settings** tab by clicking **Add** in **Default gateways**.

   -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.

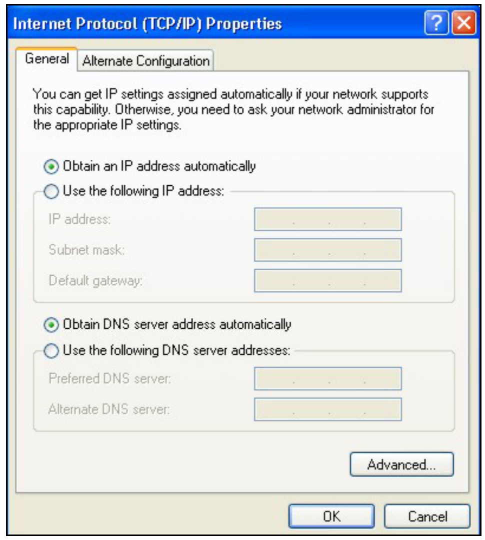


7. In the **Internet Protocol TCP/IP Properties** window (the **General tab** in Windows XP):

   -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.




8. Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.

9. Click **OK** to close the **Local Area Connection Properties** window.

10. Turn on your LAN-Cell and restart your computer (if prompted).

Checking/Modifying Your Computer's IP Address

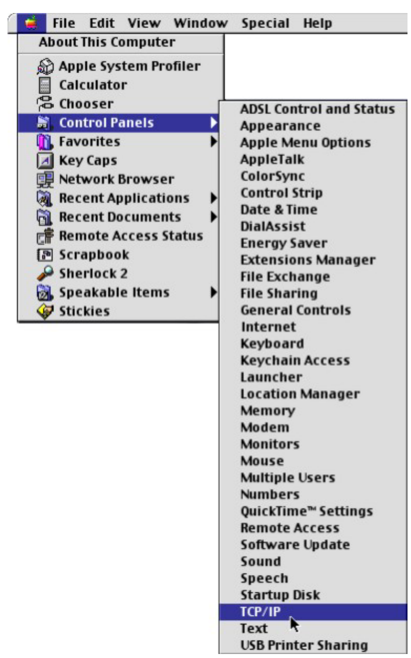
1. Click **Start**, **All Programs**, **Accessories** and then **Command Prompt**.

2. In the **Command Prompt** window, type "ipconfig" and then press [ENTER] to verify that your computer's static IP address is in the correct subnet (192.168.1.2 to 192.168.1.254 if using the default LAN-Cell LAN IP address). Alternatively, to have the LAN-Cell assign your computer a new IP address (from the IP pool), make sure your LAN-Cell is turned on, type "ipconfig/renew" and then press **ENTER**.

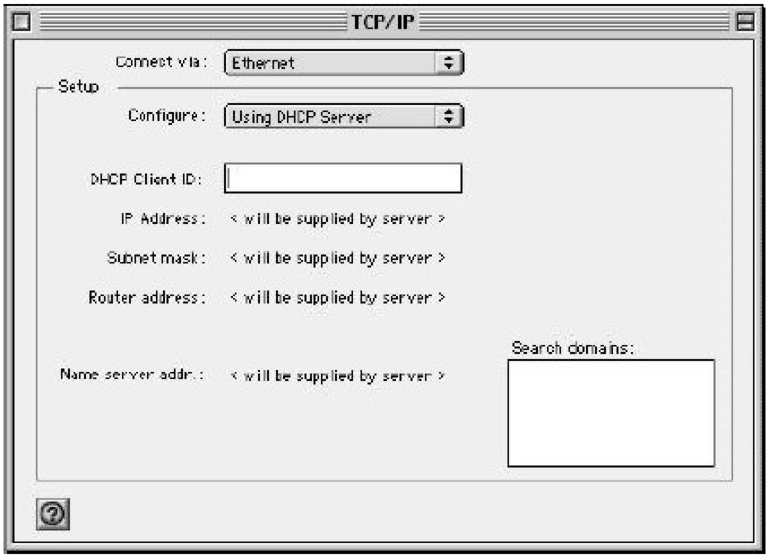
   Your computer can now communicate with the LAN-Cell using the LAN port.

### Macintosh OS 8/9

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



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




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.

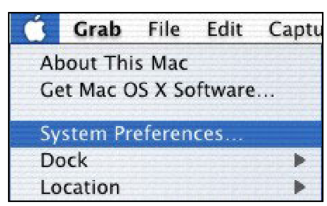
   -Type the IP address of your LAN-Cell in the **Router address** box.
5. Close the **TCP/IP Control Panel**.
6. Click **Save** if prompted, to save changes to your configuration.
7. Turn on your LAN-Cell and restart your computer (if prompted).

Verifying Your Computer's IP Address

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.

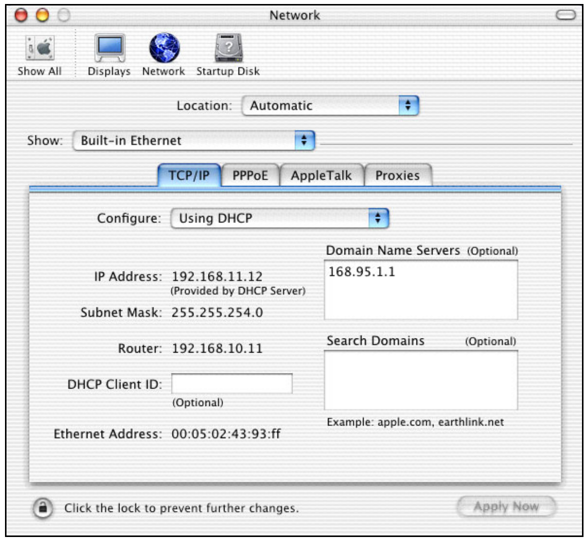


2. Click **Network** in the icon bar.

   - 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.

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 Your Computer's IP Address

**Check your TCP/IP properties in the** Network **window**

# Appendix C
# Triangle Route

### The Ideal Setup

When the firewall is on, your LAN-Cell acts as a secure gateway between your LAN and the Internet. In an ideal network topology, all incoming and outgoing network traffic passes through the LAN-Cell to protect your LAN against attacks.

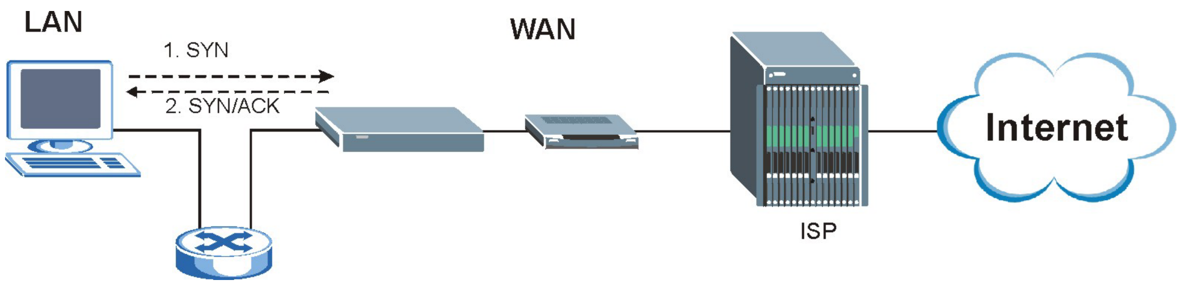



**Diagram 1 Ideal Setup**

### The "Triangle Route" Problem

A traffic route is a path for sending or receiving data packets between two Ethernet devices. Some companies have more than one alternate route to one or more ISPs. If the LAN and ISP(s) are in the same subnet, the "triangle route" problem may occur. The steps below describe the "triangle route" problem.

**Step 1.** A computer on the LAN initiates a connection by sending out a SYN packet to a receiving server on the WAN.

**Step 2.** The LAN-Cell reroutes the SYN packet through Gateway **B** on the LAN to the WAN.

**Step 3.** The reply from the WAN goes directly to the computer on the LAN without going through the LAN-Cell.

As a result, the LAN-Cell resets the connection, as the connection has not been acknowledged.

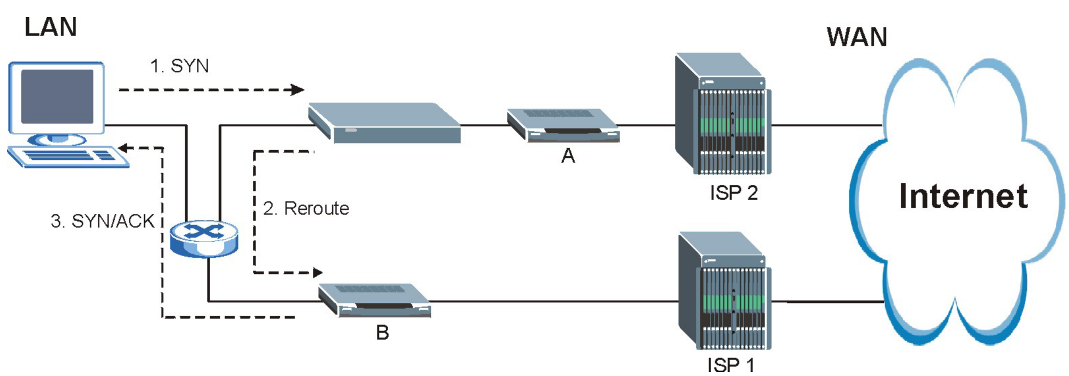



**Diagram 2 "Triangle Route" Problem**

### The "Triangle Route" Solutions

This section presents you two solutions to the "triangle route" problem.

### IP Aliasing

IP alias allows you to partition your network into logical sections over the same Ethernet interface. Your LAN-Cell supports up to three logical LAN interfaces with the LAN-Cell being the gateway for each logical network. By putting your LAN and Gateway **B** in different subnets, all returning network traffic must pass through the LAN-Cell to your LAN. The following steps describe such a scenario.

A computer on the LAN initiates a connection by sending a SYN packet to a receiving server on the WAN.

The LAN-Cell reroutes the packet to Gateway **B** which is in Subnet 2.

The reply from WAN goes through the LAN-Cell to the computer on the LAN in Subnet 1.

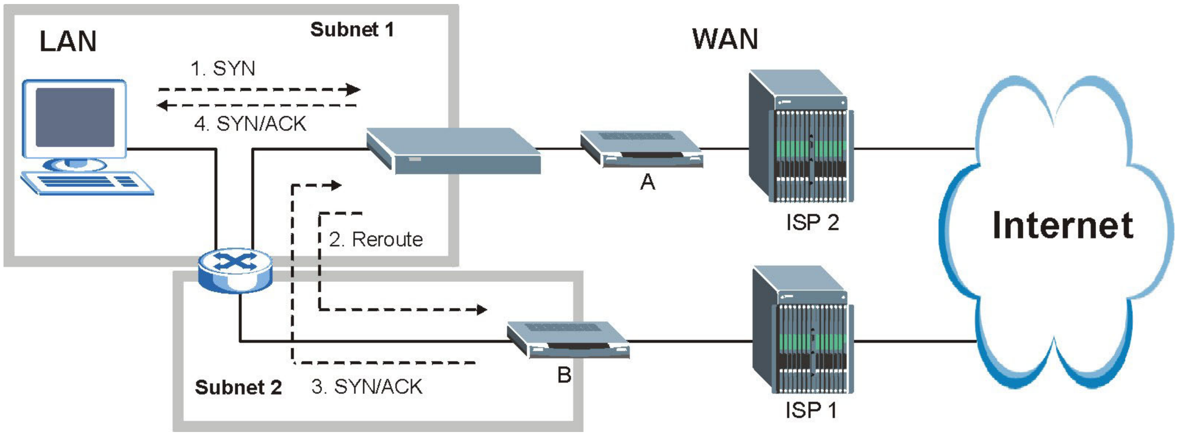



**Diagram 3 IP Alias**

### Gateways on the WAN Side

A second solution to the "triangle route" problem is to put all of your network gateways on the WAN side as the following figure shows. This ensures that all incoming network traffic passes through your LAN-Cell to your LAN. Therefore your LAN is protected.

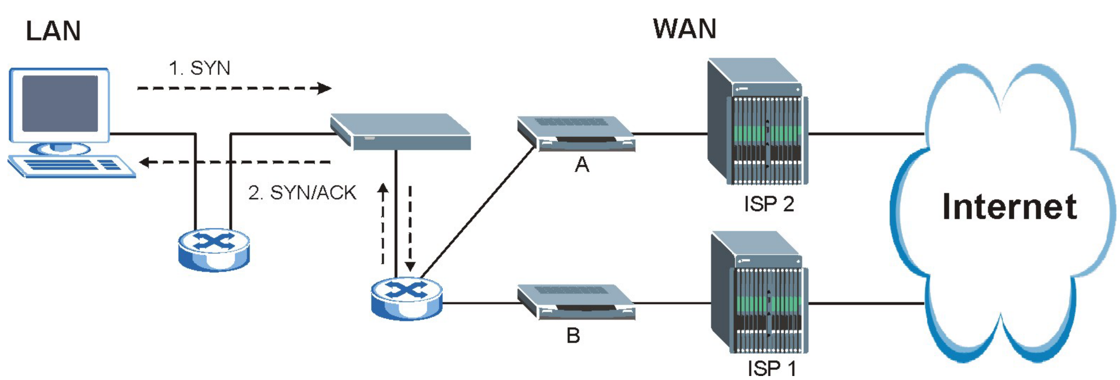



**Diagram 4 Gateways on the WAN Side**

### How To Configure Triangle Route:

**Step 1.** From the SMT main menu, enter 24.

**Step 2.** Enter "8" in menu 24 to enter CI command mode.

**Step 3.** Use the following commands to allow/disallow triangle route.

| | |
|---|---|
| `sys firewall ignore triangle all off` | This command allows triangle route. |
| `sys firewall ignore triangle all on` | This command disallows triangle route. |

# Appendix D PPPoE

## PPPoE in Action

An ADSL modem bridges a PPP session over Ethernet (PPP over Ethernet, RFC 2516) from your PC to an ATM PVC (Permanent Virtual Circuit), which connects to a DSL Access Concentrator where the PPP session terminates (see the next figure). One PVC can support any number of PPP sessions from your LAN. PPPoE provides access control and billing functionality in a manner similar to dial-up services using PPP.

## Benefits of PPPoE

PPPoE offers the following benefits:

1. It provides you with a familiar dial-up networking (DUN) user interface.
2. It lessens the burden on the carriers of provisioning virtual circuits all the way to the ISP on multiple switches for thousands of users. For GSTN (PSTN & ISDN), the switching fabric is already in place.
3. It allows the ISP to use the existing dial-up model to authenticate and (optionally) to provide differentiated services.

## Traditional Dial-up Scenario

The following diagram depicts a typical hardware configuration where the PCs use traditional dial-up networking.

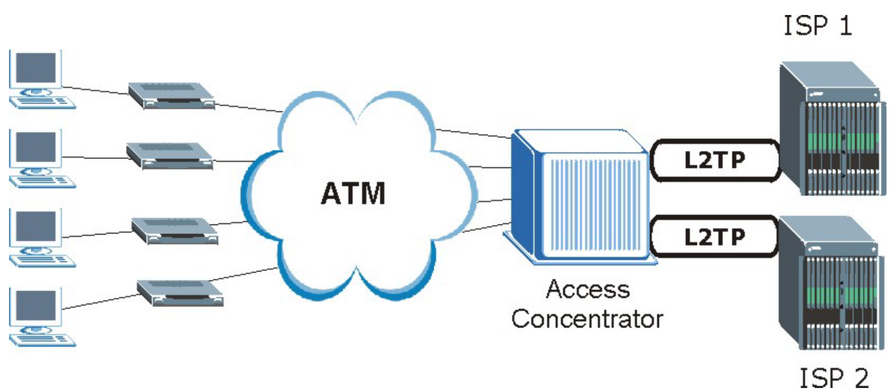



**Diagram D-1 Single-PC per Modem Hardware Configuration**

## How PPPoE Works

The PPPoE driver makes the Ethernet appear as a serial link to the PC and the PC runs PPP over it, while the modem bridges the Ethernet frames to the Access Concentrator (AC). Between the AC and an ISP, the AC is acting as a L2TP (Layer 2 Tunneling Protocol) LAC (L2TP Access Concentrator) and tunnels the PPP frames to the ISP. The L2TP tunnel is capable of carrying multiple PPP sessions.

With PPPoE, the VC (Virtual Circuit) is equivalent to the dial-up connection and is between the modem and the AC, as opposed to all the way to the ISP. However, the PPP negotiation is between the PC and the ISP.

## LAN-Cell as a PPPoE Client

When using the LAN-Cell as a PPPoE client, the PCs on the LAN see only Ethernet and are not aware of PPPoE. This alleviates the administrator from having to manage the PPPoE clients on the individual PCs.

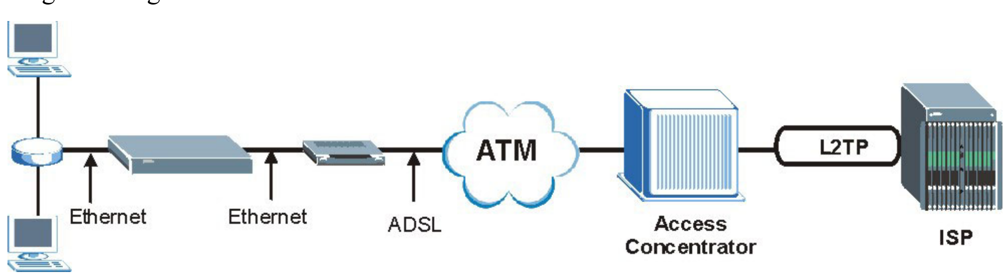



**Diagram D-2 LAN-Cell as a PPPoE Client**

# Appendix E
# PPTP

### What is PPTP?

PPTP (Point-to-Point Tunneling Protocol) is a Microsoft proprietary protocol (RFC 2637 for PPTP is informational only) to tunnel PPP frames.

### How can we transport PPP frames from a PC to a broadband modem over Ethernet?

A solution is to build PPTP into the ANT (ADSL Network Termination) where PPTP is used only over the short haul between the PC and the modem over Ethernet. For the rest of the connection, the PPP frames are transported with PPP over AAL5 (RFC 2364). The PPP connection, however, is still between the PC and the ISP. The various connections in this setup are depicted in the following diagram. The drawback of this solution is that it requires one separate ATM VC per destination.

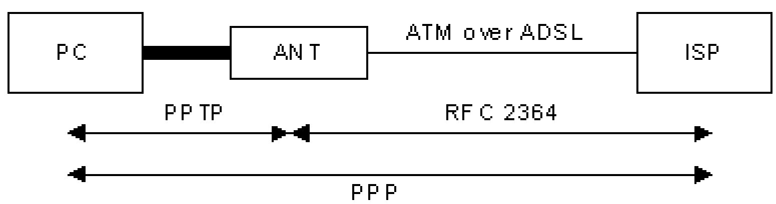



**Diagram E-1 Transport PPP frames over Ethernet**

### PPTP and the LAN-Cell

When the LAN-Cell is deployed in such a setup, it appears as a PC to the ANT.

In Windows VPN or PPTP Pass-Through feature, the PPTP tunneling is created from Windows 95, 98 and NT clients to an NT server in a remote location. The pass-through feature allows users on the network to access a different remote server using the LAN-Cell's Internet connection. In NAT mode, the LAN-Cell is able to pass the PPTP packets to the internal PPTP server (i.e. NT server) behind the NAT. Users need to forward PPTP packets to port 1723 by configuring the server in **Menu 15.2 - Server Set Setup**. In the case above as the remote PPTP Client initializes the PPTP connection, the user must configure the PPTP clients. The LAN-Cell initializes the PPTP connection hence; there is no need to configure the remote PPTP clients.

### PPTP Protocol Overview

PPTP is very similar to L2TP, since L2TP is based on both PPTP and L2F (Cisco's Layer 2 Forwarding). Conceptually, there are three parties in PPTP, namely the PNS (PPTP Network Server), the PAC (PPTP Access Concentrator) and the PPTP user. The PNS is the box that hosts both the PPP and the PPTP stacks and forms one end of the PPTP tunnel. The PAC is the box that dials/answers the phone calls and relays the PPP frames to the PNS. The PPTP user is not necessarily a PPP client (can be a PPP server too). Both the PNS and the PAC must have IP connectivity; however, the PAC must in addition have dial-up capability. The phone call is between the user and the PAC and the PAC tunnels the PPP frames to the PNS. The PPTP user is unaware of the tunnel between the PAC and the PNS.

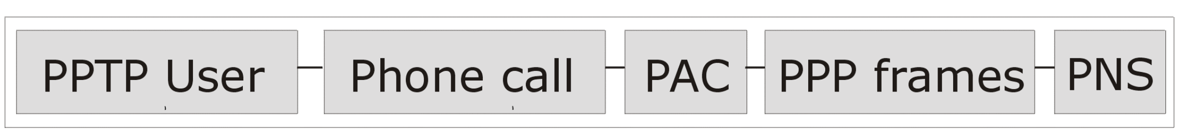



**Diagram E-2 PPTP Protocol Overview**

Microsoft includes PPTP as a part of the Windows OS. In Microsoft's implementation, the PC, and hence the LAN-Cell, is the PNS that requests the PAC (the ANT) to place an outgoing call over AAL5 to an RFC 2364 server.

### Control & PPP connections

Each PPTP session has distinct control connection and PPP data connection.

Call Connection

The control connection runs over TCP. Similar to L2TP, a tunnel control connection is first established before call control messages can be exchanged. Please note that a tunnel control connection supports multiple call sessions.

The following diagram depicts the message exchange of a successful call setup between a PC and an ANT.

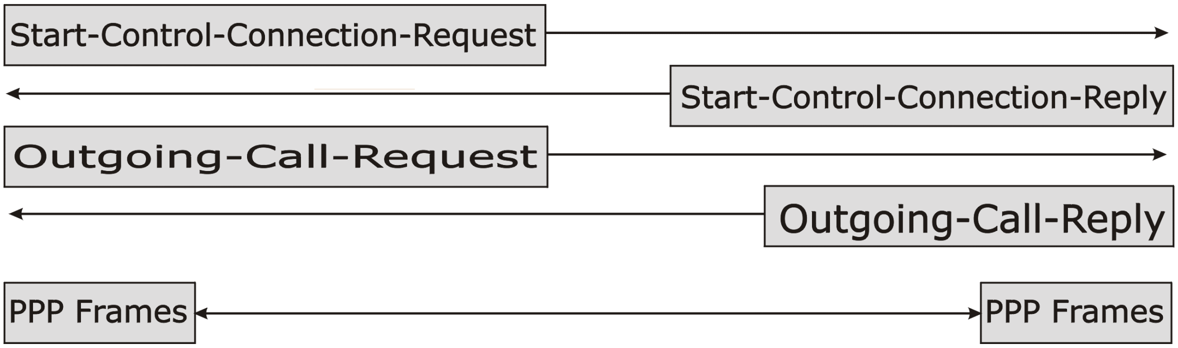



**Diagram E-3 Example Message Exchange between PC and an ANT**

**PPP Data Connection**

The PPP frames are tunneled between the PNS and PAC over GRE (General Routing Encapsulation, RFC 1701, 1702). The individual calls within a tunnel are distinguished using the Call ID field in the GRE header.

# Appendix F
# IP Subnetting

## IP Addressing

Routers "route" based on the network number. The router that delivers the data packet to the correct destination host uses the host ID.

## IP Classes

An IP address is made up of four octets (eight bits), written in dotted decimal notation, for example, 192.168.1.1. IP addresses are categorized into different classes. The class of an address depends on the value of its first octet.

- Class "A" addresses have a 0 in the left most bit. In a class "A" address the first octet is the network number and the remaining three octets make up the host ID.
- Class "B" addresses have a 1 in the left most bit and a 0 in the next left most bit. In a class "B" address the first two octets make up the network number and the two remaining octets make up the host ID.
- Class "C" addresses begin (starting from the left) with 1 1 0. In a class "C" address the first three octets make up the network number and the last octet is the host ID.
- Class "D" addresses begin with 1 1 1 0. Class "D" addresses are used for multicasting. (There is also a class "E" address. It is reserved for future use.)

**Chart F-1 Classes of IP Addresses**

| IP ADDRESS: | | OCTET 1 | OCTET 2 | OCTET 3 | OCTET 4 |
|---|---|---|---|---|---|
| Class A | 0 | Network number | Host ID | Host ID | Host ID |
| Class B | 10 | Network number | Network number | Host ID | Host ID |
| Class C | 110 | Network number | Network number | Network number | Host ID |

**Host IDs of all zeros or all ones are not allowed.**

Therefore:

- A class "C" network (8 host bits) can have $2^8 - 2$ or 254 hosts.
- A class "B" address (16 host bits) can have $2^{16} - 2$ or 65534 hosts.

A class "A" address (24 host bits) can have $2^{24} - 2$ hosts (approximately 16 million hosts).

Since the first octet of a class "A" IP address must contain a "0", the first octet of a class "A" address can have a value of 0 to 127.

Similarly the first octet of a class "B" must begin with "10", therefore the first octet of a class "B" address has a valid range of 128 to 191. The first octet of a class "C" address begins with "110", and therefore has a range of 192 to 223.

**Chart F-2 Allowed IP Address Range By Class**

| CLASS | ALLOWED RANGE OF FIRST OCTET (BINARY) | ALLOWED RANGE OF FIRST OCTET (DECIMAL) |
|---|---|---|
| Class A | **0**0000000 to **0**1111111 | 0 to 127 |
| Class B | **10**000000 to **10**111111 | 128 to 191 |
| Class C | **110**00000 to **110**11111 | 192 to 223 |
| Class D | **1110**0000 to **1110**1111 | 224 to 239 |

## Subnet Masks

A subnet mask is used to determine which bits are part of the network number, and which bits are part of the host ID (using a logical AND operation). A subnet mask has 32 bits; each bit of the mask corresponds to a bit of the IP address. If a bit in the subnet mask is a "1" then the corresponding bit in the IP address is part of the network number. If a bit in the subnet mask is "0" then the corresponding bit in the IP address is part of the host ID.

Subnet masks are expressed in dotted decimal notation just as IP addresses are. The "natural" masks for class A, B and C IP addresses are as follows.

**Chart F-3 "Natural" Masks**

| CLASS | NATURAL MASK |
|---|---|
| A | 255.0.0.0 |
| B | 255.255.0.0 |
| C | 255.255.255.0 |

### Subnetting

With subnetting, the class arrangement of an IP address is ignored. For example, a class C address no longer has to have 24 bits of network number and 8 bits of host ID. With subnetting, some of the host ID bits are converted into network number bits. By convention, subnet masks always consist of a continuous sequence of ones beginning from the left most bit of the mask, followed by a continuous sequence of zeros, for a total number of 32 bits.

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

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

The following table shows all possible subnet masks for a class "C" address using both notations.

**Chart F-4 Alternative Subnet Mask Notation**

| SUBNET MASK IP ADDRESS | SUBNET MASK "1" BITS | LAST OCTET BIT VALUE |
|---|---|---|
| 255.255.255.0 | /24 | 0000 0000 |
| 255.255.255.128 | /25 | 1000 0000 |
| 255.255.255.192 | /26 | 1100 0000 |
| 255.255.255.224 | /27 | 1110 0000 |
| 255.255.255.240 | /28 | 1111 0000 |
| 255.255.255.248 | /29 | 1111 1000 |
| 255.255.255.252 | /30 | 1111 1100 |

The first mask shown is the class "C" natural mask. Normally if no mask is specified it is understood that the natural mask is being used.

### Example: Two Subnets

As an example, you have a class "C" address 192.168.1.0 with subnet mask of 255.255.255.0.

| | NETWORK NUMBER | HOST ID |
|---|---|---|
| IP Address | 192.168.1. | 0 |
| IP Address (Binary) | 11000000.10101000.00000001. | 00000000 |
| Subnet Mask | 255.255.255. | 0 |
| Subnet Mask (Binary) | 11111111.11111111.11111111. | 00000000 |

The first three octets of the address make up the network number (class "C"). You want to have two separate networks.

Divide the network 192.168.1.0 into two separate subnets by converting one of the host ID bits of the IP address to a network number bit. The "borrowed" host ID bit can be either "0" or "1" thus giving two subnets; 192.168.1.0 with mask 255.255.255.128 and 192.168.1.128 with mask 255.255.255.128.

**In the following charts, shaded/bolded last octet bit values indicate host ID bits "borrowed" to form network ID bits. The number of "borrowed" host ID bits determines the number of subnets you can have. The remaining number of host ID bits (after "borrowing") determines the number of hosts you can have on each subnet.**

**Chart F-5 Subnet 1**

| | NETWORK NUMBER | LAST OCTET BIT VALUE |
|---|---|---|
| IP Address | 192.168.1. | 0 |
| IP Address (Binary) | 11000000.10101000.00000001. | **0**0000000 |
| Subnet Mask | 255.255.255. | 128 |
| Subnet Mask (Binary) | 11111111.11111111.11111111. | **1**0000000 |
| Subnet Address: 192.168.1.0 | Lowest Host ID: 192.168.1.1 | |
| Broadcast Address: 192.168.1.127 | Highest Host ID: 192.168.1.126 | |

**Chart F-6 Subnet 2**

| | NETWORK NUMBER | LAST OCTET BIT VALUE |
|---|---|---|
| IP Address | 192.168.1. | 128 |
| IP Address (Binary) | 11000000.10101000.00000001. | **1**0000000 |
| Subnet Mask | 255.255.255. | 128 |
| Subnet Mask (Binary) | 11111111.11111111.11111111. | **1**0000000 |
| Subnet Address: 192.168.1.128 | Lowest Host ID: 192.168.1.129 | |
| Broadcast Address: 192.168.1.255 | Highest Host ID: 192.168.1.254 | |

The remaining 7 bits determine the number of hosts each subnet can have. Host IDs of all zeros represent the subnet itself and host IDs of all ones are the broadcast address for that subnet, so the actual number of hosts available on each subnet in the example above is $2^7$ – 2 or 126 hosts for each subnet.

192.168.1.0 with mask 255.255.255.128 is the subnet itself, and 192.168.1.127 with mask 255.255.255.128 is the directed broadcast address for the first subnet. Therefore, the lowest IP address that can be assigned to an actual host for the first subnet is 192.168.1.1 and the highest is 192.168.1.126. Similarly the host ID range for the second subnet is 192.168.1.129 to 192.168.1.254.

### Example: Four Subnets

The above example illustrated using a 25-bit subnet mask to divide a class "C" address space into two subnets. Similarly to divide a class "C" address into four subnets, you need to "borrow" two host ID bits to give four possible combinations of 00, 01, 10 and 11. The subnet mask is 26 bits (11111111.11111111.11111111.**11**000000) or 255.255.255.192. Each subnet contains 6 host ID bits, giving $2^6$-2 or 62 hosts for each subnet (all 0's is the subnet itself, all 1's is the broadcast address on the subnet).

**Chart F-7 Subnet 1**

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

**Chart F-8 Subnet 2**

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

**Chart F-9 Subnet 3**

| | NETWORK NUMBER | LAST OCTET BIT VALUE |
|---|---|---|
| IP Address | 192.168.1. | 128 |
| IP Address (Binary) | 11000000.10101000.00000001. | **10**000000 |
| Subnet Mask (Binary) | 11111111.11111111.11111111. | **11**000000 |
| Subnet Address: 192.168.1.128 | Lowest Host ID: 192.168.1.129 | |
| Broadcast Address: 192.168.1.191 | Highest Host ID: 192.168.1.190 | |

**Chart F-10 Subnet 4**

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

### Example Eight Subnets

Similarly use a 27-bit mask to create 8 subnets (001, 010, 011, 100, 101, 110).

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

**Chart F-11 Eight Subnets**

| SUBNET | SUBNET ADDRESS | FIRST ADDRESS | LAST ADDRESS | BROADCAST ADDRESS |
|---|---|---|---|---|
| 1 | 0 | 1 | 30 | 31 |
| 2 | 32 | 33 | 62 | 63 |
| 3 | 64 | 65 | 94 | 95 |
| 4 | 96 | 97 | 126 | 127 |
| 5 | 128 | 129 | 158 | 159 |
| 6 | 160 | 161 | 190 | 191 |
| 7 | 192 | 193 | 222 | 223 |
| 8 | 224 | 223 | 254 | 255 |

The following table is a summary for class "C" subnet planning.

**Chart F-12 Class C Subnet Planning**

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

### Subnetting With Class A and Class B Networks.

For class "A" and class "B" addresses the subnet mask also determines which bits are part of the network number and which are part of the host ID.

A class "B" address has two host ID octets available for subnetting and a class "A" address has three host ID octets (see ***Error! Reference source not found.***) available for subnetting.

The following table is a summary for class "B" subnet planning.

**Chart F-13 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 |

# Appendix G
# Safety Warnings and Instructions

1. Be sure to read and follow all warning notices and instructions.
2. The maximum recommended ambient temperature for the LAN-Cell is 40º Celsius (104º Fahrenheit). Care must be taken to allow sufficient air circulation or space between units when the LAN-Cell is installed inside a closed rack assembly. The operating ambient temperature of the rack environment might be greater than room temperature.
3. Installation in a rack without sufficient airflow can be unsafe.
4. Racks should safely support the combined weight of all equipment.
5. The connections and equipment that supply power to the LAN-Cell should be capable of operating safely with the maximum power requirements of the LAN-Cell. In case of a power overload, the supply circuits and supply wiring should not become hazardous. The input rating of the LAN-Cell is printed on the nameplate.
6. Installation in restricted access areas must comply with Articles 110-16, 110-17, and 110-18 of the National Electrical Code, ANSI/NFPA 70.
7. Do not allow anything to rest on the power cord and do not locate the product where anyone can walk on the power cord.
8. Do not service the product by yourself. Opening or removing covers can expose you to dangerous high voltage points or other risks and will void your warranty. Refer all servicing to qualified service personnel.
9. Generally, when installed after the final configuration, the product must comply with the applicable safety standards and regulatory requirements of the country in which it is installed. If necessary, consult the appropriate regulatory agencies and inspection authorities to ensure compliance.
10. A rare condition can create a voltage potential between the earth grounds of two or more buildings. If products installed in separate building are interconnected, the voltage potential can cause a hazardous condition. Consult a qualified electrical consultant to determine whether or not this phenomenon exists and, if necessary, implement corrective action before interconnecting the products.

# Part XVI:

## Command, Log Appendices and Index

This part provides information on the command line interface, firewall and NetBIOS commands, logs and password protection. There is also an index of key terms.

# Appendix H
# Command Interpreter

The following describes how to use the command interpreter. Enter 24 in the main menu to bring up the system maintenance menu. Enter 8 to go to **Menu 24.8 - Command Interpreter Mode**. See the included disk or Proxicast.com for more detailed information on these commands.

**Use of undocumented commands or misconfiguration can damage the unit and possibly render it unusable.**

### 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.

### Command Usage

A list of valid 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.

# Appendix I
# Firewall Commands

The following describes the firewall commands. See the ***Error! Reference source not found.*** appendix for information on the command structure.

**Chart I-1** Firewall Commands

| FUNCTION | | COMMAND | DESCRIPTION |
|---|---|---|---|
| **Firewall** | | | |
| | **Set-Up** | | |
| | | `config edit firewall active <yes \| no>` | This command turns the firewall on or off. |
| | | `config retrieve firewall` | This command returns the previously saved firewall settings. |
| | | `config save firewall` | This command saves the current firewall settings. |
| | **Display** | | |
| | | `config display firewall` | This command shows the of all the firewall settings including e-mail, attack, and the sets/ rules. |
| | | `config display firewall set <set #>` | This command shows the current configuration of a set; including timeout values, name, default-permit, and etc.<br>If you don't put use a number (#) after "set", information about all of the sets/rules appears. |
| | | `config display firewall set <set #> rule <rule #>` | This command shows the current entries of a rule in a firewall rule set. |
| | | `config display firewall attack` | This command shows all of the attack response settings. |
| | | `config display firewall e-mail` | This command shows all of the e-mail settings. |
| | | `config display firewall ?` | This command shows all of the available firewall sub commands. |
| **Edit** | | | |
| | **E-mail** | `config edit firewall e-mail mail-server <ip address of mail server>` | This command sets the IP address to which the e-mail messages are sent. |
| | | `config edit firewall e-mail return-addr <e-mail address>` | This command sets the source e-mail address of the firewall e-mails. |

**Chart I-1** Firewall Commands

| FUNCTION | COMMAND | DESCRIPTION |
|---|---|---|
| | `config edit firewall e-mail email-to <e-mail address>` | This command sets the e-mail address to which the firewall e-mails are sent. |
| | `config edit firewall e-mail policy <full \| hourly \| daily \| weekly>` | This command sets how frequently the firewall log is sent via e-mail. |
| | `config edit firewall e-mail day <sunday \| monday \| tuesday \| wednesday \| thursday \| friday \| saturday>` | This command sets the day on which the current firewall log is sent through e-mail if the LAN-Call is set to send it on a weekly basis. |
| | `config edit firewall e-mail hour <0-23>` | This command sets the hour when the firewall log is sent through e- mail if the LAN-Call is set to send it on an hourly, daily or weekly basis. |
| | `config edit firewall e-mail minute <0-59>` | This command sets the minute of the hour for the firewall log to be sent via e- mail if the LAN-Call is set to send it on a hourly, daily or weekly basis. |
| **Attack** | `config edit firewall attack send-alert <yes \| no>` | This command enables or disables the immediate sending of DOS attack notification e-mail messages. |
| | `config edit firewall attack block <yes \| no>` | Set this command to yes to block new traffic after the tcp-max-incomplete threshold is exceeded. Set it to no to delete the oldest half-open session when traffic exceeds the tcp-max-incomplete threshold. |
| | `config edit firewall attack block-minute <0-255>` | This command sets the number of minutes for new sessions to be blocked when the tcp-max-incomplete threshold is reached. This command is only valid when block is set to yes. |
| | `config edit firewall attack minute-high <0-255>` | This command sets the threshold rate of new half-open sessions per minute where the LAN-Call starts deleting old half-opened sessions until it gets them down to the minute-low threshold. |
| | `config edit firewall attack minute-low <0-255>` | This command sets the threshold of half-open sessions where the LAN-Call stops deleting half-opened sessions. |
| | `config edit firewall attack max-incomplete-high <0-255>` | This command sets the threshold of half-open sessions where the LAN-Call starts deleting old half-opened sessions until it gets them down to the max incomplete low. |
| | `config edit firewall attack max-incomplete-low <0-255>` | This command sets the threshold where the LAN-Call stops deleting half-opened sessions. |
| | `config edit firewall attack tcp-max-incomplete <0-255>` | This command sets the threshold of half-open TCP sessions with the same destination where the LAN-Call starts dropping half-open sessions to that destination. |

**Chart I-1** Firewall Commands

<table>
<tr><th>FUNCTION</th><th>COMMAND</th><th>DESCRIPTION</th></tr>
<tr><td>Sets</td><td>config edit firewall set <set #> name <desired name></td><td>This command sets a name to identify a specified set.</td></tr>
<tr><td></td><td>Config edit firewall set <set #> default-permit <forward | block></td><td>This command sets whether a packet is dropped or allowed through, when it does not meet a rule within the set.</td></tr>
<tr><td></td><td>Config edit firewall set <set #> icmp-timeout <seconds></td><td>This command sets the time period to allow an ICMP session to wait for the ICMP response.</td></tr>
<tr><td></td><td>Config edit firewall set <set #> udp-idle-timeout <seconds></td><td>This command sets how long a UDP connection is allowed to remain inactive before the LAN-Call considers the connection closed.</td></tr>
<tr><td></td><td>Config edit firewall set <set #> connection-timeout <seconds></td><td>This command sets how long LAN-Call waits for a TCP session to be established before dropping the session.</td></tr>
<tr><td></td><td>Config edit firewall set <set #> fin-wait-timeout <seconds></td><td>This command sets how long the LAN-Call leaves a TCP session open after the firewall detects a FIN-exchange (indicating the end of the TCP session).</td></tr>
<tr><td></td><td>Config edit firewall set <set #> tcp-idle-timeout <seconds></td><td>This command sets how long LAN-Call lets an inactive TCP connection remain open before considering it closed.</td></tr>
<tr><td></td><td>Config edit firewall set <set #> log <yes | no></td><td>This command sets whether or not the LAN-Call creates logs for packets that match the firewall’s default rule set.</td></tr>
<tr><td>Rules</td><td>Config edit firewall set <set #> rule <rule #> permit <forward | block></td><td>This command sets whether packets that match this rule are dropped or allowed through.</td></tr>
<tr><td></td><td>Config edit firewall set <set #> rule <rule #> active <yes | no></td><td>This command sets whether a rule is enabled or not.</td></tr>
<tr><td></td><td>Config edit firewall set <set #> rule <rule #> protocol <integer protocol value ></td><td>This command sets the protocol specification number made in this rule for ICMP.</td></tr>
<tr><td></td><td>Config edit firewall set <set #> rule <rule #> log <none | match | not-match | both></td><td>This command sets the LAN-Call to log traffic that matches the rule, doesn't match, both or neither.</td></tr>
<tr><td></td><td>Config edit firewall set <set #> rule <rule #> alert <yes | no></td><td>This command sets whether or not the LAN-Call sends an alert e-mail when a DOS attack or a violation of a particular rule occurs.</td></tr>
</table>

**Chart I-1** Firewall Commands

| FUNCTION | COMMAND | DESCRIPTION |
|---|---|---|
| | `config edit firewall set <set #> rule <rule #> srcaddr-single <ip address>` | This command sets the rule to have the LAN-Call check for traffic with this individual source address. |
| | `config edit firewall set <set #> rule <rule #> srcaddr-subnet <ip address> <subnet mask>` | This command sets a rule to have the LAN-Call check for traffic from a particular subnet (defined by IP address and subnet mask). |
| | `config edit firewall set <set #> rule <rule #> srcaddr-range <start ip address> <end ip address>` | This command sets a rule to have the LAN-Call check for traffic from this range of addresses. |
| | `config edit firewall set <set #> rule <rule #> destaddr-single <ip address>` | This command sets the rule to have the LAN-Call check for traffic with this individual destination address. |
| | `config edit firewall set <set #> rule <rule #> destaddr-subnet <ip address> <subnet mask>` | This command sets a rule to have the LAN-Call check for traffic with a particular subnet destination (defined by IP address and subnet mask). |
| | `config edit firewall set <set #> rule <rule #> destaddr-range <start ip address> <end ip address>` | This command sets a rule to have the LAN-Call check for traffic going to this range of addresses. |
| | `config edit firewall set <set #> rule <rule #> TCP destport-single <port #>` | This command sets a rule to have the LAN-Call check for TCP traffic with this destination address. You may repeat this command to enter various, non-consecutive port numbers. |
| | `config edit firewall set <set #> rule <rule #> TCP destport-range <start port #> <end port #>` | This command sets a rule to have the LAN-Call check for TCP traffic with a destination port in this range. |
| | `config edit firewall set <set #> rule <rule #> UDP destport-single <port #>` | This command sets a rule to have the LAN-Call check for UDP traffic with this destination address. You may repeat this command to enter various, non-consecutive port numbers. |
| | `config edit firewall set <set #> rule <rule #> UDP destport-range <start port #> <end port #>` | This command sets a rule to have the LAN-Call check for UDP traffic with a destination port in this range. |
| **Delete** | | |
| | `config delete firewall e-mail` | This command removes all of the settings for e-mail alert. |
| | `config delete firewall attack` | This command resets all of the attack response settings to their defaults. |
| | `config delete firewall set <set #>` | This command removes the specified set from the firewall configuration. |

**Chart I-1** Firewall Commands

| FUNCTION | COMMAND | DESCRIPTION |
|---|---|---|
| | `config delete firewall set <set #> rule <rule #>` | This command removes the specified rule in a firewall configuration set. |

# Appendix J
# NetBIOS Filter Commands

The following describes the NetBIOS packet filter commands. See the ***Error! Reference source not found.*** appendix for information on the command structure.

## Introduction

NetBIOS (Network Basic Input/Output System) are TCP or UDP broadcast packets that enable a computer to connect to and communicate with a LAN.

For some dial-up services such as PPPoE or PPTP, NetBIOS packets cause unwanted calls.

You can configure NetBIOS filters to do the following:

- Allow or disallow the sending of NetBIOS packets between the LAN and the WAN.
- Allow or disallow the sending of NetBIOS packets through VPN connections.
- Allow or disallow NetBIOS packets to initiate calls.

## Display NetBIOS Filter Settings

**Diagram J-1** NetBIOS Display Filter Settings Command Example

Syntax: `sys filter netbios disp`

This command gives a read-only list of the current NetBIOS filter modes.

```
ras> sys filter netbios disp
=========== NetBIOS Filter Status ===========
        Between LAN and WAN: Block
        IPSec Packets: Forward
        Trigger Dial: Disabled
```

**Diagram J-2 NetBIOS Display Filter Settings Command Example**

The filter types and their default settings are as follows.

**Chart J-1 NetBIOS Filter Default Settings**

| NAME | DESCRIPTION | EXAMPLE |
|---|---|---|
| Between LAN and WAN | This field displays whether NetBIOS packets are blocked or forwarded between the LAN and the WAN. | Forward |
| IPSec Packets | This field displays whether NetBIOS packets sent through a VPN connection are blocked or forwarded. | Forward |
| Trigger dial | This field displays whether NetBIOS packets are allowed to initiate calls. Disabled means that NetBIOS packets are blocked from initiating calls. | Disabled |

## NetBIOS Filter Configuration

Syntax: `sys filter netbios config <type> <on|off>`

where

| | |
|---|---|
| `<type>` = | Identify which NetBIOS filter (numbered 0-3) to configure.<br>`0` = Between LAN and WAN<br>3 = IPSec packet pass through<br>4 = Trigger Dial |
| `<on\|off>` = | For types `0`, use `on` to enable the filter and block NetBIOS packets. Use `off` to disable the filter and forward NetBIOS packets.<br>For type `3`, use `on` to block NetBIOS packets from being sent through a VPN connection. Use `off` to allow NetBIOS packets to be sent through a VPN connection.<br>For type `4`, use `on` to allow NetBIOS packets to initiate dial backup calls. Use `off` to block NetBIOS packets from initiating dial backup calls. |

Example commands

Command: `sys filter netbios config 0 on`

This command blocks LAN to WAN and WAN to LAN NetBIOS packets

Command: `sys filter netbios config 3 on`

This command blocks IPSec NetBIOS packets

Command: `sys filter netbios config 4 off`

This command stops NetBIOS commands from initiating calls.

# Appendix K
# Log Descriptions

**Chart K-1 System Error Logs**

| LOG MESSAGE | DESCRIPTION |
|---|---|
| `%s exceeds the max. number of session per host!` | This attempt to create a SUA/NAT session exceeds the maximum number of SUA/NAT session table entries allowed to be created per host. |

**Chart K-2 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. |
| `DHCP client gets %s` | A DHCP client got a new IP address from the DHCP 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. |
| `SMT Login Successfully` | Someone has logged on to the router's SMT interface. |
| `SMT Login Fail` | Someone has failed to log on to the router's SMT interface. |
| `WEB Login Successfully` | Someone has logged on to the router's web configurator interface. |
| `WEB Login Fail` | Someone has failed to log on to the router's web configurator interface. |
| `TELNET Login Successfully` | Someone has logged on to the router via telnet. |
| `TELNET Login Fail` | Someone has failed to log on to the router via telnet. |
| `FTP Login Successfully` | Someone has logged on to the router via ftp. |
| `FTP Login Fail` | Someone has failed to log on to the router via ftp. |
| `NAT Session Table is Full!` | The maximum number of SUA/NAT session table entries has been exceeded and the table is full. |

**Chart K-3 Content Filtering Logs**

| CATEGORY | LOG MESSAGE | DESCRIPTION |
|---|---|---|
| URLFOR | `IP/Domain Name` | The LAN-Call allows access to this IP address or domain name and forwarded traffic addressed to the IP address or domain name. |

**Chart K-3 Content Filtering Logs**

| | | |
|---|---|---|
| URLBLK | `IP/Domain Name` | The LAN-Call blocked access to this IP address or domain name due to a forbidden keyword. All web traffic is disabled except for trusted domains, untrusted domains, or the cybernot list. |
| JAVBLK | `IP/Domain Name` | The LAN-Call blocked access to this IP address or domain name because of a forbidden service such as: ActiveX, a Java applet, a cookie, or a proxy. |

**Chart K-4 Attack Logs**

| LOG MESSAGE | DESCRIPTION |
|---|---|
| `attack TCP` | The firewall detected a TCP attack. |
| `attack UDP` | The firewall detected an UDP attack. |
| `attack IGMP` | The firewall detected an IGMP attack. |
| `attack ESP` | The firewall detected an ESP attack. |
| `attack GRE` | The firewall detected a GRE attack. |
| `attack OSPF` | The firewall detected an OSPF attack. |
| `attack ICMP (type:%d, code:%d)` | The firewall detected an ICMP attack; see the section on ICMP messages for type and code details. |
| `land TCP` | The firewall detected a TCP land attack. |
| `land UDP` | The firewall detected an UDP land attack. |
| `land IGMP` | The firewall detected an IGMP land attack. |
| `land ESP` | The firewall detected an ESP land attack. |
| `land GRE` | The firewall detected a GRE land attack. |
| `land OSPF` | The firewall detected an OSPF land attack. |
| `land ICMP (type:%d, code:%d)` | The firewall detected an ICMP land attack; see the section on ICMP messages for type and code details. |
| `ip spoofing - WAN TCP` | The firewall detected a TCP IP spoofing attack on the WAN port. |
| `ip spoofing - WAN UDP` | The firewall detected an UDP IP spoofing attack on the WAN port. |
| `ip spoofing - WAN IGMP` | The firewall detected an IGMP IP spoofing attack on the WAN port. |
| `ip spoofing - WAN ESP` | The firewall detected an ESP IP spoofing attack on the WAN port. |
| `ip spoofing - WAN GRE` | The firewall detected a GRE IP spoofing attack on the WAN port. |
| `ip spoofing - WAN OSPF` | The firewall detected an OSPF 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. See the section on ICMP messages for type and code details. |
| `icmp echo ICMP (type:%d, code:%d)` | The firewall detected an ICMP echo attack. See the section on ICMP messages for type and code details. |
| `syn flood TCP` | The firewall detected a TCP syn flood attack. |
| `ports scan TCP` | The firewall detected a TCP port scan attack. |

**Chart K-4 Attack Logs**

| LOG MESSAGE | DESCRIPTION |
|---|---|
| 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; see the section on ICMP messages for type and code details. |
| 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 | The firewall detected a TCP IP spoofing attack while the LAN-Call did not have a default route. |
| ip spoofing - no routing entry UDP | The firewall detected an UDP IP spoofing attack while the LAN-Call did not have a default route. |
| ip spoofing - no routing entry IGMP | The firewall detected an IGMP IP spoofing attack while the LAN-Call did not have a default route. |
| ip spoofing - no routing entry ESP | The firewall detected an ESP IP spoofing attack while the LAN-Call did not have a default route. |
| ip spoofing - no routing entry GRE | The firewall detected a GRE IP spoofing attack while the LAN-Call did not have a default route. |
| ip spoofing - no routing entry OSPF | The firewall detected an OSPF IP spoofing attack while the LAN-Call did not have a default route. |
| ip spoofing - no routing entry ICMP (type:%d, code:%d) | The firewall detected an ICMP IP spoofing attack while the LAN-Call did not have a default route; see the section on ICMP messages for type and code details. |
| vulnerability ICMP (type:%d, code:%d) | The firewall detected an ICMP vulnerability attack; see the section on ICMP messages for type and code details. |
| traceroute ICMP (type:%d, code:%d) | The firewall detected an ICMP traceroute attack; see the section on ICMP messages for type and code details. |

**Chart K-5 Access Logs**

| LOG MESSAGE | DESCRIPTION |
|---|---|
| Firewall default policy: TCP (set:%d) | TCP access matched the default policy of the listed ACL set and the LAN-Call blocked or forwarded it according to the ACL set's configuration. |
| Firewall default policy: UDP (set:%d) | UDP access matched the default policy of the listed ACL set and the LAN-Call blocked or forwarded it according to the ACL set's configuration. |
| Firewall default policy: ICMP (set:%d, type:%d, code:%d) | ICMP access matched the default policy of the listed ACL set and the LAN-Call blocked or forwarded it according to the ACL set's configuration. See the section on ICMP messages for type and code details. |
| Firewall default policy: IGMP (set:%d) | IGMP access matched the default policy of the listed ACL set and the LAN-Call blocked or forwarded it according to the ACL set's configuration. |
| Firewall default policy: ESP (set:%d) | ESP access matched the default policy of the listed ACL set and the LAN-Call blocked or forwarded it according to the ACL set's configuration. |

**Chart K-5 Access Logs**

| LOG MESSAGE | DESCRIPTION |
|---|---|
| Firewall default policy: GRE (set:%d) | GRE access matched the default policy of the listed ACL set and the LAN-Call blocked or forwarded it according to the ACL set's configuration. |
| Firewall default policy: OSPF (set:%d) | OSPF access matched the default policy of the listed ACL set and the LAN-Call blocked or forwarded it according to the ACL set's configuration. |
| Firewall default policy: (set:%d) | Access matched the default policy of the listed ACL set and the LAN-Call blocked or forwarded it according to the ACL set's configuration. |
| Firewall rule match: TCP (set:%d, rule:%d) | TCP access matched the listed firewall rule and the LAN-Call blocked or forwarded it according to the rule's configuration. |
| Firewall rule match: UDP (set:%d, rule:%d) | UDP access matched the listed firewall rule and the LAN-Call blocked or forwarded it according to the rule's configuration. |
| Firewall rule match: ICMP (set:%d, rule:%d, type:%d, code:%d) | ICMP access matched the listed firewall rule and the LAN-Call blocked or forwarded it according to the rule's configuration. See the section on ICMP messages for type and code details. |
| Firewall rule match: IGMP (set:%d, rule:%d) | IGMP access matched the listed firewall rule and the LAN-Call blocked or forwarded it according to the rule's configuration. |
| Firewall rule match: ESP (set:%d, rule:%d) | ESP access matched the listed firewall rule and the LAN-Call blocked or forwarded it according to the rule's configuration. |
| Firewall rule match: GRE (set:%d, rule:%d) | GRE access matched the listed firewall rule and the LAN-Call blocked or forwarded it according to the rule's configuration. |
| Firewall rule match: OSPF (set:%d, rule:%d) | OSPF access matched the listed a firewall rule and the LAN-Call blocked or forwarded it according to the rule's configuration. |
| Firewall rule match: (set:%d, rule:%d) | Access matched the listed firewall rule and the LAN-Call blocked or forwarded it according to the rule's configuration. |
| Firewall rule NOT match: TCP  (set:%d, rule:%d) | TCP access did not match the listed firewall rule and the LAN-Call logged it. |
| Firewall rule NOT match: UDP (set:%d, rule:%d) | UDP access did not match the listed firewall rule and the LAN-Call logged it. |
| Firewall rule NOT match: ICMP (set:%d, rule:%d, type:%d, code:%d) | ICMP access did not match the listed firewall rule and the LAN-Call logged it. |
| Firewall rule NOT match: IGMP (set:%d, rule:%d) | IGMP access did not match the listed firewall rule and the LAN-Call logged it. |
| Firewall rule NOT match: ESP (set:%d, rule:%d) | ESP access did not match the listed firewall rule and the LAN-Call logged it. |
| Firewall rule NOT match: GRE (set:%d, rule:%d) | GRE ac access did not match the listed firewall rule and the LAN-Call logged it. |

**Chart K-5 Access Logs**

| LOG MESSAGE | DESCRIPTION |
|---|---|
| Firewall rule NOT match: OSPF (set:%d, rule:%d) | OSPF access did not match the listed firewall rule and the LAN-Call logged it. |
| Firewall rule NOT match: (set:%d, rule:%d) | Access did not match the listed firewall rule and the LAN-Call logged it. |
| Filter default policy DROP! | TCP access matched a default filter policy and the LAN-Call dropped the packet to block access. |
| Filter default policy DROP! | UDP access matched a default filter policy and the LAN-Call dropped the packet to block access. |
| Filter default policy DROP! | ICMP access matched a default filter policy and the LAN-Call dropped the packet to block access. |
| Filter default policy DROP! | Access matched a default filter policy and the LAN-Call dropped the packet to block access. |
| Filter default policy DROP! | Access matched a default filter policy (denied LAN IP) and the LAN-Call dropped the packet to block access. |
| Filter default policy FORWARD! | TCP access matched a default filter policy. Access was allowed and the router forwarded the packet. |
| Filter default policy FORWARD! | UDP access matched a default filter policy. Access was allowed and the router forwarded the packet. |
| Filter default policy FORWARD! | ICMP access matched a default filter policy. Access was allowed and the router forwarded the packet. |
| Filter default policy FORWARD! | Access matched a default filter policy. Access was allowed and the router forwarded the packet. |
| Filter default policy FORWARD! | Access matched a default filter policy (denied LAN IP). Access was allowed and the router forwarded the packet. |
| Filter match DROP <set %d/rule %d> | TCP access matched the listed filter rule and the LAN-Call dropped the packet to block access. |
| Filter match DROP <set %d/rule %d> | UDP access matched the listed filter rule and the LAN-Call dropped the packet to block access. |
| Filter match DROP <set %d/rule %d> | ICMP access matched the listed filter rule and the LAN-Call dropped the packet to block access. |
| Filter match DROP <set %d/rule %d> | Access matched the listed filter rule and the LAN-Call dropped the packet to block access. |
| Filter match DROP <set %d/rule %d> | Access matched the listed filter rule (denied LAN IP) and the LAN-Call dropped the packet to block access. |
| Filter match FORWARD <set %d/rule %d> | TCP access matched the listed filter rule. Access was allowed and the router forwarded the packet. |
| Filter match FORWARD <set %d/rule %d> | UDP access matched the listed filter rule. Access was allowed and the router forwarded the packet. |
| Filter match FORWARD <set %d/rule %d> | ICMP access matched the listed filter rule. Access was allowed and the router forwarded the packet. |
| Filter match FORWARD <set %d/rule %d> | Access matched the listed filter rule. Access was allowed and the router forwarded the packet. |

**Chart K-5 Access Logs**

| LOG MESSAGE | DESCRIPTION |
|---|---|
| `Filter match FORWARD <set %d/rule %d>` | Access matched the listed filter rule (denied LAN IP). Access was allowed and the router forwarded the packet. |
| `(set:%d)` | With firewall messages, this is the number of the ACL policy set and denotes the packet's direction (see *Chart K-6*).<br>With filter messages, this is the number of the filter set. |
| `(rule:%d)` | With firewall messages, the firewall rule number denotes the number of a firewall rule within an ACL policy set.<br>With filter messages, this is the number of an individual filter rule. |
| `Router sent blocked web site message` | A message was sent to notify a user that the router blocked access to a requested web site |
| `Triangle route packet forwarded` | The firewall allowed a triangle route session to pass through. |
| `Firewall sent TCP packet in response to DoS attack` | The firewall detected a DoS attack and sent a TCP packet(s) in response. |
| `Firewall sent TCP reset packets` | The firewall sent out TCP reset packets. |
| `Packet without a NAT table entry blocked` | The router blocked a packet that did not have a corresponding SUA/NAT table entry. |
| `Out of order TCP handshake packet blocked` | The router blocked a TCP handshake packet that came out of the proper order |
| `Drop unsupported/out-of-order ICMP` | The LAN-Call generates this log after it drops an ICMP packet due to one of the following two reasons:<br>1. The LAN-Call does not support the ICMP packet's protocol.<br>2. The ICMP packet is an echo reply for which there was no corresponding echo request. |
| `Router sent ICMP response packet (type:%d, code:%d)` | The router sent an ICMP response packet. This packet automatically bypasses the firewall. See the section on ICMP messages for type and code details. |

**Chart K-6 ACL Setting Notes**

| ACL SET NUMBER | DIRECTION | DESCRIPTION |
|---|---|---|
| 1 | LAN to WAN | ACL set 1 for packets traveling from the LAN to the WAN. |
| 2 | WAN to LAN | ACL set 2 for packets traveling from the WAN to the LAN. |
| 7 | LAN to LAN/LAN-Call | ACL set 7 for packets traveling from the LAN to the LAN or the LAN-Call. |
| 8 | WAN to WAN/LAN-Call | ACL set 8 for packets traveling from the WAN to the WAN or the LAN-Call. |

**Chart K-7 ICMP Notes**

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

**Chart K-8 Sys log**

| LOG MESSAGE | DESCRIPTION |
|---|---|
| Mon dd hr:mm:ss hostname src="<srcIP:srcPort>" dst="<dstIP:dstPort>" msg="<msg>" note="<note>" | This message is sent by the "RAS" when this syslog is generated. The messages and notes are defined in this appendix’s other charts. |

### VPN/IPSec logs

To view the IPSec and IKE connection log, type 3 in menu 27 and press [ENTER] to display the IPSec log as shown next. The following figure shows a typical log from the initiator of a VPN connection.

```
Index:    Date/Time:              Log:
------------------------------------------------------------
 001    01 Jan 08:02:22    Send Main Mode request to <192.168.200.101>
 002    01 Jan 08:02:22    Send:<SA>
 003    01 Jan 08:02:22    Recv:<SA>
 004    01 Jan 08:02:24    Send:<KE><NONCE>
 005    01 Jan 08:02:24    Recv:<KE><NONCE>
 006    01 Jan 08:02:26    Send:<ID><HASH>
 007    01 Jan 08:02:26    Recv:<ID><HASH>
 008    01 Jan 08:02:26    Phase 1 IKE SA process done
 009    01 Jan 08:02:26    Start Phase 2: Quick Mode
 010    01 Jan 08:02:26    Send:<HASH><SA><NONCE><ID><ID>
 011    01 Jan 08:02:26    Recv:<HASH><SA><NONCE><ID><ID>
 012    01 Jan 08:02:26    Send:<HASH>
 Clear IPSec Log (y/n):
```

**Diagram K-1 Example VPN Initiator IPSec Log**

### VPN Responder IPSec Log

The following figure shows a typical log from the VPN connection peer.

```
Index:    Date/Time:              Log:
------------------------------------------------------------
 001    01 Jan 08:08:07    Recv Main Mode request from <192.168.200.100>
 002    01 Jan 08:08:07    Recv:<SA>
 003    01 Jan 08:08:08    Send:<SA>
 004    01 Jan 08:08:08    Recv:<KE><NONCE>
 005    01 Jan 08:08:10    Send:<KE><NONCE>
 006    01 Jan 08:08:10    Recv:<ID><HASH>
 007    01 Jan 08:08:10    Send:<ID><HASH>
 008    01 Jan 08:08:10    Phase 1 IKE SA process done
 009    01 Jan 08:08:10    Recv:<HASH><SA><NONCE><ID><ID>
 010    01 Jan 08:08:10    Start Phase 2: Quick Mode
 011    01 Jan 08:08:10    Send:<HASH><SA><NONCE><ID><ID>
 012    01 Jan 08:08:10    Recv:<HASH>
 Clear IPSec Log (y/n):
```

**Diagram K-2 Example VPN Responder IPSec Log**

This menu is useful for troubleshooting. A log index number, the date and time the log was created and a log message are displayed.

**Double exclamation marks (!!) denote an error or warning message.**

The following table shows sample log messages during IKE key exchange.

**A PYLD_MALFORMED packet usually means that the two ends of the VPN tunnel are not using the same pre-shared key.**

**Chart K-9 Sample IKE Key Exchange Logs**

| LOG MESSAGE | DESCRIPTION |
|---|---|
| Send <Symbol> Mode request to <IP><br>Send <Symbol> Mode request to <IP> | The LAN-Call has started negotiation with the peer. |
| Recv <Symbol> Mode request from <IP><br>Recv <Symbol> Mode request from <IP> | The LAN-Call has received an IKE negotiation request from the peer. |
| Recv:<Symbol> | IKE uses the ISAKMP protocol (refer to RFC2408 – ISAKMP) to transmit data. Each ISAKMP packet contains payloads of different types that show in the log - see Chart K-11. |
| Phase 1 IKE SA process done | Phase 1 negotiation is finished. |
| Start Phase 2: Quick Mode | Phase 2 negotiation is beginning using Quick Mode. |
| !! IKE Negotiation is in process | The LAN-Call has begun negotiation with the peer for the connection already, but the IKE key exchange has not finished yet. |
| !! Duplicate requests with the same cookie | The LAN-Call has received multiple requests from the same peer but it is still processing the first IKE packet from that peer. |
| !! No proposal chosen | The parameters configured for Phase 1 or Phase 2 negotiations don't match. Please check all protocols and settings for these phases. For example, one party may be using 3DES encryption, but the other party is using DES encryption, so the connection will fail. |
| !! Verifying Local ID failed<br>!! Verifying Remote ID failed | During IKE Phase 2 negotiation, both parties exchange policy details, including local and remote IP address ranges. If these ranges differ, then the connection fails. |
| !! Local / remote IPs of incoming request conflict with rule <#d> | If the security gateway is "0.0.0.0", the LAN-Call will use the peer's "Local Addr" as its "Remote Addr". If this IP (range) conflicts with a previously configured rule then the connection is not allowed. |
| !! Invalid IP <IP start>/<IP end> | The peer's "Local IP Addr" range is invalid. |
| !! Remote IP <IP start> / <IP end> conflicts | If the security gateway is "0.0.0.0", the LAN-Call will use the peer's "Local Addr" as its "Remote Addr". If a peer's "Local Addr" range conflicts with other connections, then the LAN-Call will not accept VPN connection requests from this peer. |
| !! Active connection allowed exceeded | The LAN-Call limits the number of simultaneous Phase 2 SA negotiations. The IKE key exchange process fails if this limit is exceeded. |
| !! IKE Packet Retransmit | The LAN-Call did not receive a response from the peer and so retransmits the last packet sent. |
| !! Failed to send IKE Packet | The LAN-Call cannot send IKE packets due to a network error. |
| !! Too many errors! Deleting SA | The LAN-Call deletes an SA when too many errors occur. |

**Chart K-9 Sample IKE Key Exchange Logs**

| LOG MESSAGE | DESCRIPTION |
|---|---|
| `!! Phase 1 ID type mismatch` | The ID type of an incoming packet does not match the local's peer ID type. |
| `!! Phase 1 ID content mismatch` | The ID content of an incoming packet does not match the local's peer ID content. |
| `!! No known phase 1 ID type found` | The ID type of an incoming packet does not match any known ID type. |
| `Peer ID: IP address type <IP address>` | The IP address type or IP address of an incoming packet does not match the peer IP address type or IP address configured on the local router. The log displays the IP address type and IP address of the incoming packet. |
| `vs. My Remote <IP address>` | The IP address type or IP address of an incoming packet does not match the peer IP address type or IP address configured on the local router. The log displays this router's configured remote IP address type or IP address that the incoming packet did not match. |
| `vs. My Local <IP address>` | The IP address type or IP address of an incoming packet does not match the peer IP address type or IP address configured on the local router. The log displays this router's configured local IP address type or IP address that the incoming packet did not match. |
| `-> <symbol>` | The router sent a payload type of IKE packet. |
| `Error ID Info` | The parameters configured for Phase 1 ID content do not match or the parameters configured for the Phase 2 ID (IP address of single, range or subnet) do not match. Please check all protocols and settings for these phases. |

The following table shows sample log messages during packet transmission.

**Chart K-10 Sample IPSec Logs During Packet Transmission**

| LOG MESSAGE | DESCRIPTION |
|---|---|
| `!! WAN IP changed to <IP>` | If the LAN-Call's WAN IP changes, all configured "My IP Addr" are changed to b "0.0.0.0". If this field is configured as 0.0.0.0, then the LAN-Call will use the current LAN-Call WAN IP address (static or dynamic) to set up the VPN tunnel. |
| `!! Cannot find IPSec SA` | The LAN-Call cannot find a phase 2 SA that corresponds with the SPI of an inbound packet (from the peer); the packet is dropped. |
| `!! Cannot find outbound SA for rule <%d>` | The packet matches the rule index number (#d), but Phase 1 or Phase 2 negotiation for outbound (from the VPN initiator) traffic is not finished yet. |
| `!! Discard REPLAY packet` | If the LAN-Call receives a packet with the wrong sequence number it will discard it. |
| `!! Inbound packet authentication failed` | The authentication configuration settings are incorrect. Please check them. |
| `!! Inbound packet decryption failed` | The decryption configuration settings are incorrect. Please check them. |
| `Rule <#d> idle time out, disconnect` | If an SA has no packets transmitted for a period of time (configurable via CI command), the LAN-Call drops the connection. |

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

**Chart K-11 RFC-2408 ISAKMP Payload Types**

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

### Log Commands

Go to the command interpreter interface (the *Command Interpreter Appendix* explains how to access and use the commands).

Configuring What You Want the LAN-Call to Log

Use the `sys logs load` command to load the log setting buffer that allows you to configure which logs the LAN-Call is to record.

Use `sys logs category` followed by a log category and a parameter to decide what to record

**Chart K-12 Log Categories and Available Settings**

| LOG CATEGORIES | AVAILABLE PARAMETERS |
|---|---|
| access | 0, 1, 2, 3 |
| attack | 0, 1, 2, 3 |
| error | 0, 1, 2, 3 |
| ike | 0, 1, 2, 3 |
| ipsec | 0, 1, 2, 3 |
| javablocked | 0, 1, 2, 3 |
| mten | 0, 1 |
| upnp | 0, 1 |
| urlblocked | 0, 1, 2, 3 |
| urlforward | 0, 1 |
| Use `0` to not record logs for that category, `1` to record only logs for that category, `2` to record only alerts for that category, and `3` to record both logs and alerts for that category. | |

Use the `sys logs save` command to store the settings in the LAN-Call (you must do this in order to record logs).

### Displaying Logs

Use the `sys logs display` command to show all of the logs in the LAN-Call's log.

Use the `sys logs category display` command to show the log settings for all of the log categories.

Use the `sys logs display [log category]` command to show the logs in an individual LAN-Call log category.

Use the `sys logs clear` command to erase all of the LAN-Call's logs.

## Log Command Example

This example shows how to set the LAN-Call to record the access logs and alerts and then view the results.

```
ras> sys logs load
ras> sys logs category access 3
ras> sys logs save
ras> sys logs display access

#  .time                  source                  destination            notes
    message
  0|11/11/2002 15:10:12 |172.22.3.80:137        |172.22.255.255:137    |ACCESS BLOCK
    Firewall default policy: UDP(set:8)
  1|11/11/2002 15:10:12 |172.21.4.17:138        |172.21.255.255:138    |ACCESS BLOCK
    Firewall default policy: UDP(set:8)
  2|11/11/2002 15:10:11 |172.17.2.1             |224.0.1.60            |ACCESS BLOCK
    Firewall default policy: IGMP(set:8)
  3|11/11/2002 15:10:11 |172.22.3.80:137        |172.22.255.255:137    |ACCESS BLOCK
    Firewall default policy: UDP(set:8)
  4|11/11/2002 15:10:10 |192.168.20.1:520       |192.168.20.255:520    |ACCESS BLOCK
    Firewall default policy: UDP(set:8)
  5|11/11/2002 15:10:10 |172.21.4.67:137        |172.21.255.255:137    |ACCESS BLOCK
```

# Appendix L
# Brute-Force Password Guessing Protection

The following describes the commands for enabling, disabling and configuring the brute-force password guessing protection mechanism for the password. See the ***Error! Reference source not found.*** appendix for information on the command structure.

**Chart L-1 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. |

# Appendix M
# Index

## K



## L



## M



## N



## O



## P



## Q



## R

## S



## T