LAN-Cell 3

4G / 3G Cellular Router + VPN + Firewall

User's Guide

Version 5.4

proxicast®

CONTENTS

Document Revision History

April 29, 2014	Version 5.4:	Added Guest Hotspot, Wi-Fi Client Static IP, IPSec Split Tunneling
February 1, 2013	Version 5.2:	Revised for latest firmware features and Modem-SAFE base
April 2, 2012	Version 5.1:	Initial release

Related Documents & Resources

LAN-Cell 3 Quick Start Guide
http://www.proxicast.com/support/files/LAN-Cell-3-QuickStartGuide.pdf

LAN-Cell 3 Firmware Release Notes
http://www.proxicast.com/support/files/Release-Notes.pdf

LAN-Cell 3 Application Tech Notes
http://www.proxicast.com/support/TechNotes.htm

Proxicast Knowledgebase
http://www.proxicast.com/AbsoluteFM/afmmain.aspx

Tips for Verizon Wireless Modems
http://www.proxicast.com/support/files/LC3-Tips-Verzion-Wireless.pdf

LAN-Cell 3 Accessories
http://www.proxicast.com/shopping/index.php

About This User's Guide

Intended Audience

This manual is intended for user who need to configure the LAN-Cell 3 using the device's embedded web interface. You should have at least a basic knowledge of TCP/IP networking concepts and topology.

Related Documentation

- **Quick Start Guide**

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

- **Firmware Release Notes**

  Every new LAN-Cell firmware release includes a description of the new features and improvements.

- **Proxicast Support Web Site**

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

Syntax Conventions

- The LAN-Cell 3 may be referred to as the "LAN-Cell", the "device" or the "system".
- The LAN-Cell 3's wired Ethernet WAN interface may be referred to as "WAN", "Wired WAN" "Ethernet WAN", "WAN (Ethernet)" or "WAN 1".
- The LAN-Cell's USB modem interface may be referred to was "Cellular", "CELL", "USB", WAN (USB Modem)" or "WAN 2"
- Product labels, screen names, field labels and field choices are all in **bold** font.
- A key stroke is denoted by square brackets and uppercase text, for example, [ENTER] means the "enter" or "return" key on your keyboard.
- "Enter" means for you to type one or more characters and then press the [ENTER] key. "Select" or "choose" means for you to use one of the predefined choices.
- A right angle bracket (>) within a screen name denotes a mouse click. For example, **Management > Log** means you first click **Management** menu, then the **Log** sub menu to get to that screen.
- The example screens shown in the User's Guide may differ slightly from the actual screens on the LAN-Cell, depending on the firmware version the LAN-Cell is running.

Safety Warnings

- Do NOT use this product near water.
- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do NOT store things on the device.
- Do NOT install, use, or service this device during a thunderstorm.
- Connect ONLY suitable accessories to the device.
- Do NOT open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. ONLY qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Use ONLY an appropriate power adaptor or cord for your device.
- Connect the power adaptor or cord to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe).
- Do NOT allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Do NOT use the device if the power adaptor or cord is damaged as it might cause electrocution.
- Do not use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.
- Do NOT obstruct the device ventilation slots, as insufficient airflow may harm your device.
- Antenna Warning! This device meets ETSI and FCC certification requirements when using the included antenna(s).
- If you wall mount your device, make sure that no electrical lines, gas or water pipes will be damaged.

This product is recyclable. Dispose of it properly.

CHAPTER 1: INTRODUCTION

The LAN-Cell 3 is Proxicast's third generation of enterprise-grade secure cellular gateways. This model features customer accessible and removable "4G/3G" USB cellular modems -- the same ones commonly used to provide high-speed 4G/3G cellular connectivity to laptops. The USB modem seamlessly becomes a WAN interface for the LAN-Cell's router and is fully integrated with all of the LAN-Cell's security, performance, and management capabilities.

As with its predecessors, the LAN-Cell 3 is loaded with security features including VPN, firewall and access control. The LAN-Cell 3 adds improved throughput, support for 4G cellular modems, bandwidth management, NAT, port forwarding, policy routing, DHCP server and many other powerful features required for complex and demanding applications.

The LAN-Cell 3 also has a built-in IEEE 802.11 b/g/n Wi-Fi radio that functions as both an access point and a WAN bridge. This allows Wi-Fi devices to securely communicate with the LAN-Cell and access the wired network or Internet. It also enables the LAN-Cell to use available Wi-Fi networks for even higher speed Internet access.

The LAN-Cell 3's all metal construction coupled with its unique Multi-Function Mounting System and patent-pending Modem-SAFE^{TM} system make it the perfect choice for applications where a high-performance, secure, reliable and rugged cellular router is required.

1.1 Key Features

- **Multiple Broadband WAN Connections (4G/3G + 802.11 b/g/n + xDSL/cable modem)**

  The LAN-Cell 3 supports multiple broadband technologies, including 4G/3G, 802.11 b/g/n and xDSL/cable modems. You can create a mobile broadband connection using a 4G/3G modem or switch to fixed line connection using a xDSL/cable modem. It also supports the latest 802.11n technology for Wi-Fi on the WAN.

- **4G/3G USB Modem Support**

  With support for over 100 different 4G/3G USB modems on dozens of mobile networks worldwide, the LAN-Cell 3 allows you to use your existing 4G/3G modem and service provider to create a mobile broadband sharing connection. (Find the list of currently compatible modems on our web site.)

- **Dual WAN Load Balance and Failover**

  Proxicast's LAN-Cell 3 supports load balancing and failover functions between fixed-line (xDSL/cable modem), Wi-Fi, and 4G/3G service, offering non-stop network connectivity.

- **IPsec Server & Client**

  The LAN-Cell 3's embedded IPSec VPN features allow remote users to make secure connections to devices which normally cannot run VPN software. The LAN-Cell can also establish site-to-site IPSec tunnels to existing corporate VPN servers for enterprise-level data security.

- **Quality of Service (Bandwidth Management)**

  Proxicast's LAN-Cell 3 is able to automatically monitor your bandwidth usage, prioritize traffic, and allocate bandwidth to all applications and users. At the same time, it also is able to provide users with the freedom to customize their bandwidth allocation to meet special requirements. Policy-based bandwidth allocation and routing give the user complete control over how WAN resources are utilized.

- **Industrial Design**

  Designed specifically for industrial and mobile applications, the LAN-Cell 3's rugged steel chassis and unique Multi-Function Mounting Base provide physical security along with conveniences such as power-locking, cable management and our patent-pending Modem-LOCK USB modem retention system.

- **Energy Efficient**

  The LAN-Cell 3's low power consumption SOC chip makes it ideal for solar or battery-powered installations.

1.2 Package Contents

- LAN-Cell 3
- Multi-Function Mounting Base with Modem-SAFE
- 120/240 VAC to 12 VDC Power Adapter
- 2x 3 dBi Wi-Fi Antennas
- 1x CAT5e Cable
- 1x USB Cable
- 3x Velcro Strips
- 4x Rubber Feet
- Mounting Hardware Kit
- Quick Start Guide

CHAPTER 2: HARDWARE

2.1 Front LEDs

Figure 1: LAN-Cell 3 Front Panel

LABEL	LED STATE	DESCRIPTION
MODEM		USB 2.0 port for 4G/3G USB modems only
USB	Flashing	USB modem is initializing – or – USB modem is not registered on the carrier network – or – There is no compatible cellular service available at the current location
	Solid	USB modem has made a connection & has been assigned an IP address
Wi-Fi	Solid	The LAN-Cell's internal Wi-Fi radio is enabled
OS	Solid	An internal OS error has occurred
PWR	Solid	Power is on
STAT	Flashing	Power-on Self Test is in progress (approx. 60 sec)
	Solid	LAN-Cell is at normal operational status
WAN	Solid	Link Status on the wired WAN Ethernet port
	Flashing	Data activity on the wired WAN Ethernet port
LAN 1-4	Solid	Link Status on the corresponding LAN Ethernet port
	Flashing	Data activity on the corresponding LAN Ethernet port
EJECT USB		Press & hold for 5 seconds. Wait for LED to stop flashing. Remove USB modem.
RESET		Press & hold for 5 seconds until the STAT LED begins to flash. Wait for STAT LED to stay on solid. This returns the LAN-Cell to its factory default settings: LAN IP = 192.168.1.1:8080 Username/Password = admin/1234

2.2 Rear Panel

Figure 2: LAN-Cell 3 Rear Panel

LABEL	DESCRIPTION
Wi-Fi (B)*	Attach one of the supplied cylindrical Wi-Fi antennas to this RP-SMA (reverse polarity) connector if using the LAN-Cell's integrated 802.11 b/g/n radio.
LAN 1-4 (yellow)	Connect equipment to these ports with Ethernet cables. These ports are auto-negotiating (supporting 10, 100, 1000 Mbps) and auto-sensing (adjusts to the Ethernet cable type: straight-through vs. cross-over).
WAN (blue)	Connect a cable/DSL modem or other 10/100/1000 Ethernet-based WAN equipment to this auto-sensing/auto-negotiating port.
PWR	Connect the included 12V DC power adapter to this jack. This is a 2.1mm center pin positive connector.
ON/OFF	Power Switch. To prevent accidental disengagement of the switch, install the Power Switch cover included with the Multi-Function Mounting Base.
Wi-Fi (A)*	Attach one of the supplied cylindrical Wi-Fi antennas to this RP-SMA (reverse polarity) connector if using the LAN-Cell's integrated 802.11 b/g/n radio. If using only 1 antenna, use jack A.

* Attaching other types of antennas (such antennas with standard SMA, TNC or FME connectors) to this jack may damage the antennas and/or Wi-Fi antenna jack!

2.3 Multi-Function Mounting Base

The LAN-Cell 3's Multi-Function Mounting provides:

A. Wall and deck mounting options

B. Multiple external antenna mounting points

C. Cable management tie-down posts

D. Power switch & reset button protection features

E. Modem-SAFE™ USB modem mounting system

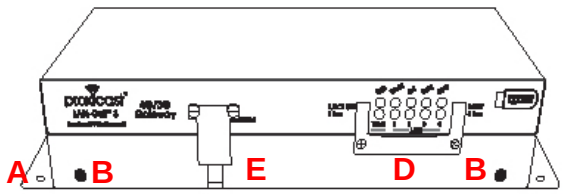


Figure 3: Mounting Base Front

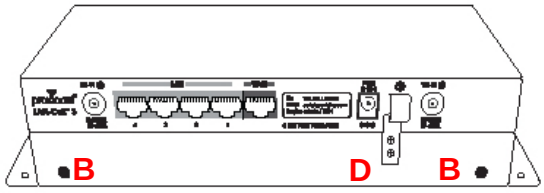


Figure 4: Mounting Base Rear

2.4 Modem-SAFE™

The LAN-Cell 3's patent-pending Modem-SAFE system is a mechanism for securing a USB modem to prevent it from being removed or coming loose in mobile applications. The slotted mounting plate and Velcro strip design allows for infinite flexibility in mounting a wide variety of USB modems.

Note: At this time, the Novatel USB551L, MC679 and MC545 modems are known to be incompatible with the Modem-SAFE base due to the design of their USB connector and its limited operating angle.

Assembling the Mounting Base:

- Insert a Velcro strip through the slotted mounting plate with the wide "cat-ear" end pointing up and with the loop (soft) side facing you (Figure 5).

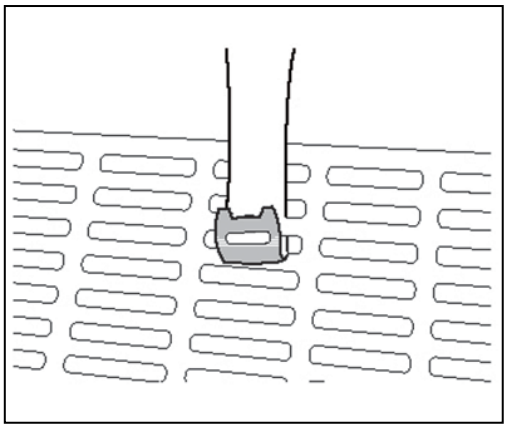


Figure 5: Inserting Velcro Strip

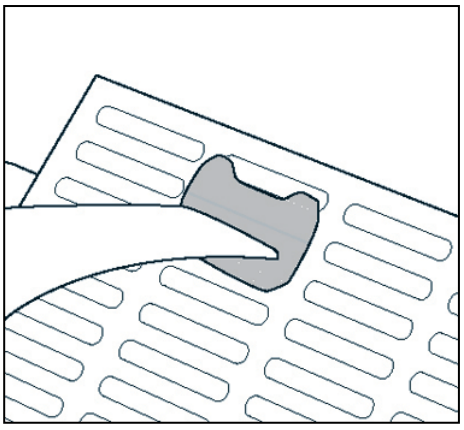


Figure 6: Locking Velcro Strip

- Loop the tapered end of the Velcro strip up through an adjacent slot and secure through the hole in the top of the Velcro strip (Figure 6). It is critical that you pull the strip tightly against the mounting plate. Hold the wide-end of the Velcro strip against the mounting plate for leverage when cinching this loop.
- Attach the right-angled male-to-female USB adapter to the USB modem. Also attach the external antenna pigtail to the USB modem. External modem antennas are highly recommended when using the Modem-SAFE base.
- Place the USB modem onto the plate and loop the strip over the modem and back under the plate. The hook (rough) side of the Velcro should be against the body of the USB modem. Pull tightly to secure (Figure 7).

Note: Different modem models require different placement on the slotted mounting plate. Modems with external antenna connectors on the top or bottom should be oriented so that the antenna connector is pointing away from the slotted plate.

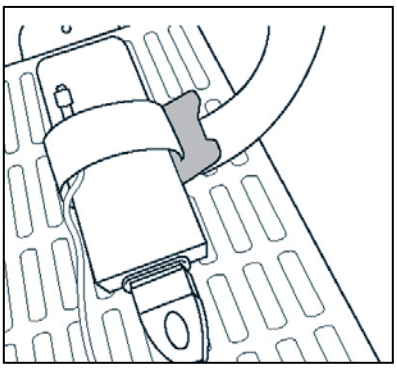


Figure 7: Cinching the Modem

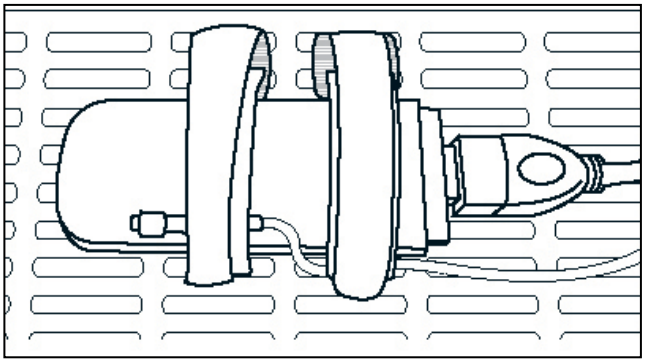


Figure 8: Modem Locked to Plate

- Repeat as necessary (Figure 8). For most USB modems, two Velcro strips are sufficient. Pull the ends of the Velcro straps tightly up through the slots and secure onto the top of the first loop of Velcro.

- Align the top of the Multi-Function base so that the vertical slot is facing the LAN-Cell 3's LEDs and the three cable tie posts are facing the Ethernet ports. Attach the top of base to the bottom of the LAN-Cell 3 using the 4 corner screw holes and the provided #6-32 screws.
- Place the slotted mounting plate assembly into the base and secure to the LAN-Cell 3 (Figure 9).

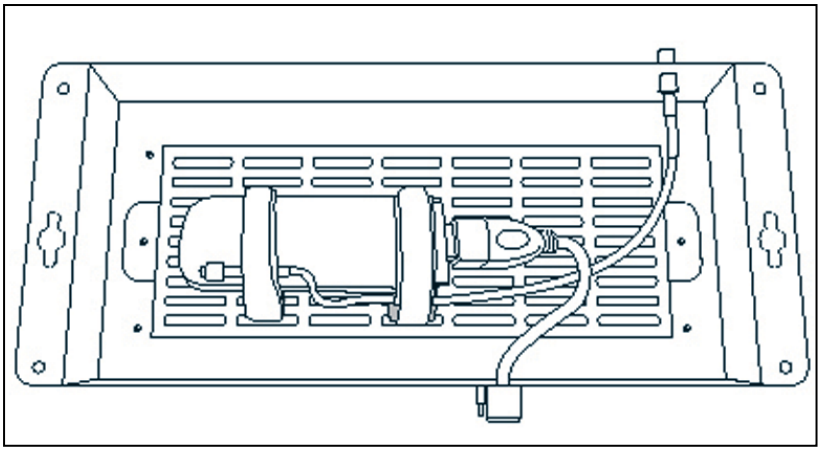


Figure 9: Assembled Modem-LOCK

- Attach the USB cable to the front USB jack and the external modem antenna to one of the four "D" holes in the base (Figure 9).
- Place the bottom cover over the base assembly and secure with screws on each side of the base.
- Optionally install the button covers over the front Reset and rear Power switches to prevent accidental activation of these buttons.

2.5 Hardware Setup

2.5.1 Power On

Plug one end of the provided power adapter into LAN-Cell 3's DC power port and the other end into a power outlet. Depress the Power push-button on the rear of the unit. After about 60 seconds, the LAN-Cell 3 will be operational when its PWR LED and STAT LED are both constantly on.

2.5.2 Install LAN Connection

Plug one end of an Ethernet cable into your computer's network port and the other end into one of LAN-Cell 3's four LAN ports on the rear panel. The corresponding LAN LED will be green and will flash indicating LAN traffic.

2.5.3 Install WAN Connection

Choose one or more ways to connect LAN-Cell 3 to the Internet.

A. Connect via 3G/4G USB Modem
   Plug a supported 3G/4G USB modem into LAN-Cell 3's USB port on the front panel.

B. Connect via xDSL, cable modem or other wired Ethernet service
   Plug an Ethernet cable from your Ethernet WAN device (e.g. DSL modem) into LAN-Cell 3's WAN port on the rear panel.

The LAN-Cell 3 supports 2 simultaneous WAN connections for both fail-over and load-balancing operations.

2.5.4 Install Wi-Fi Connection

Attach the 2 RP-SMA antennas to the A & B Wi-Fi antenna jacks on the rear panel. These antennas provide both Wi-Fi service to LAN devices and can be configured as an optional WAN connection in place of a wired Ethernet WAN connection.

CHAPTER 3: ACCESSING THE LAN-CELL 3

Initial setup of the LAN-Cell 3 must be done using an Ethernet cable – the internal Wi-Fi Access Point is disabled by default as a security precaution.

Configure your PC to receive an automatic its IP address information automatically (DHCP) or set your PC's IP address to 192.168.1.2, netmask= 255.255.255.0 and default gateway=192.168.1.1. If you are unfamiliar with how to configure your PC's TCP/IP settings, please refer to the Appendix.

3.1 Start-up and Login

Open any Web browser. In the address box, enter [HTTP://192.168.1.1:8080]

When you successfully connect to the configuration interface for LAN-Cell 3, the login screen will appear (Figure 10). Enter your username as [admin] and your password as [1234]. These are filled in initially as a convenience. You will then see the LAN-Cell 3's Router Status page (Figure 11). Changing the login password is highly recommended. See the **Admin > Management** screen.

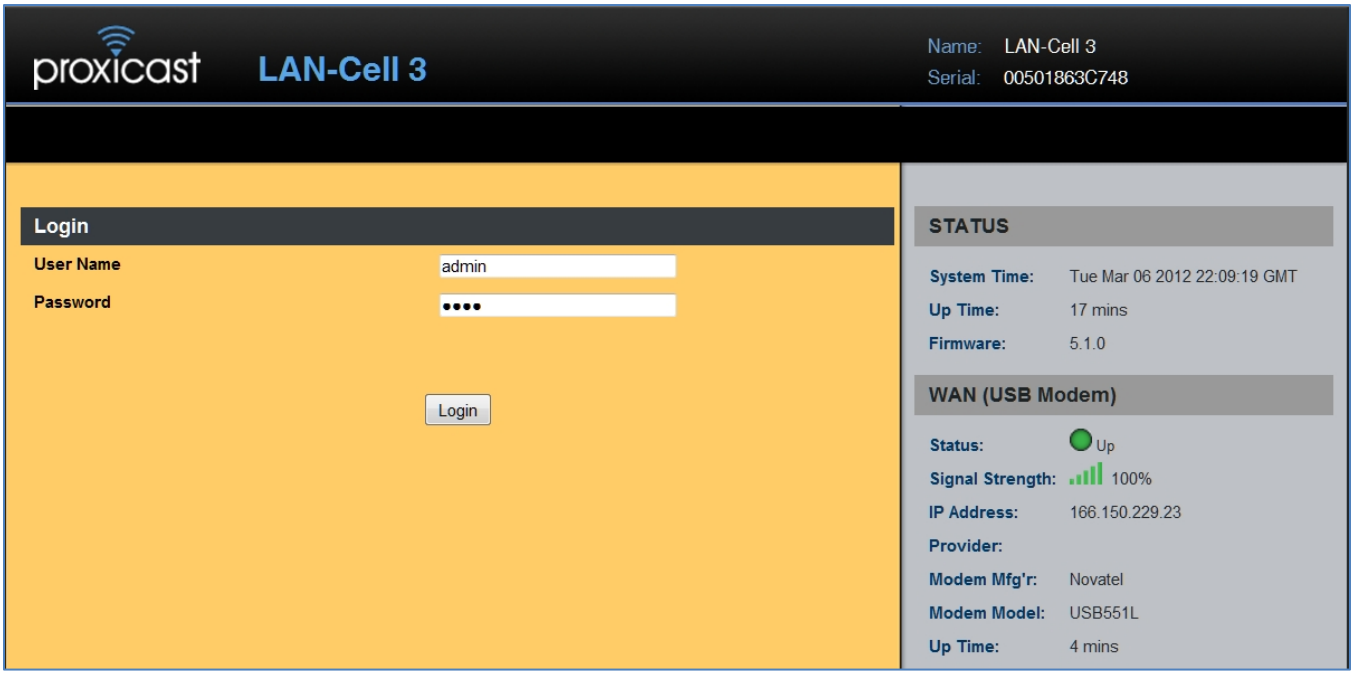


Figure 10: LAN-Cell 3 Login Screen

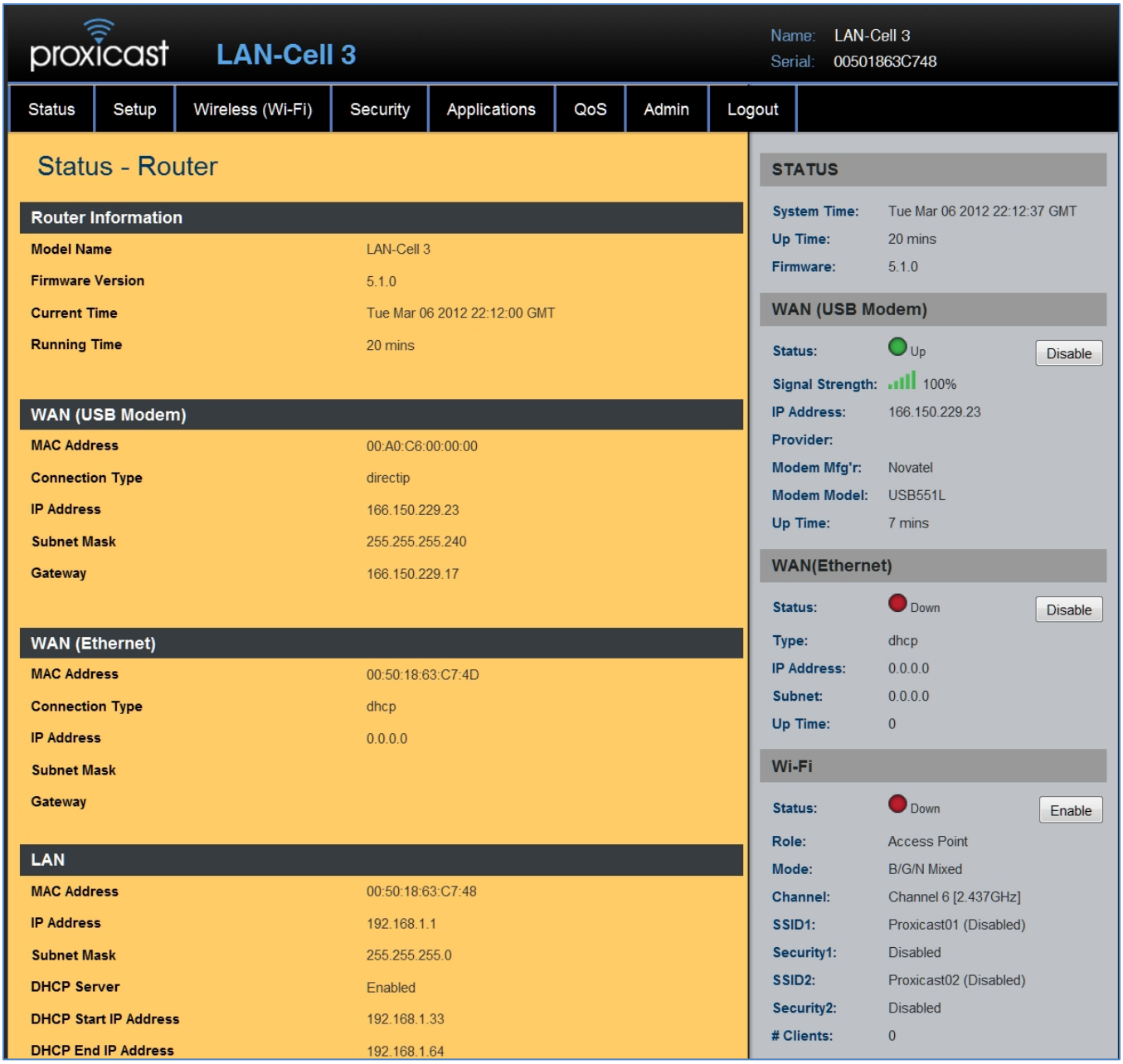


Figure 11: Router Status Screen

3.2 Navigating the User Interface

The LAN-Cell's web management interface is divided into 3 sections (Figure 12):

1. Drop-down Navigation Menus
2. The Status Summary Column
3. Configuration Parameters

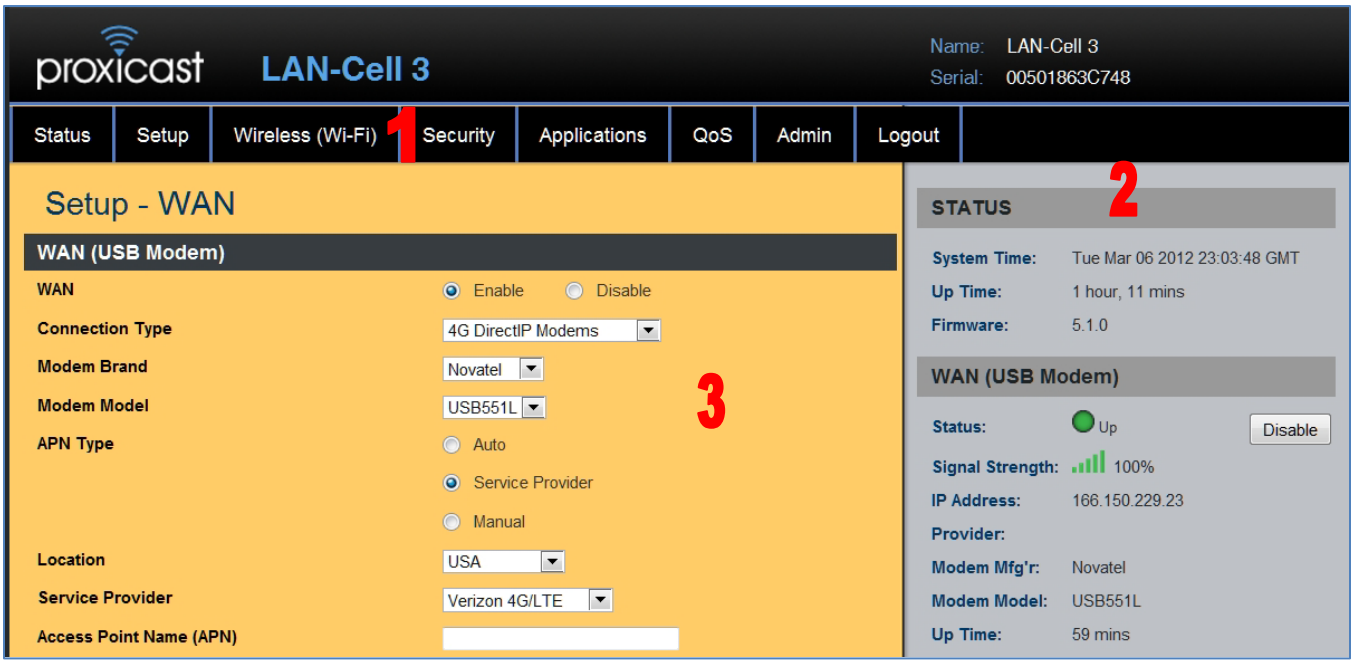


Figure 12: LAN-Cell 3 Screen Layout

To expand a drop-down menu, click on the menu title. Then select the desired sub-menu. Chapters 5 through 11 provide details on each of the LAN-Cell 3's menu options.

The Status Summary column is shown on the right side of every screen to provide a quick overview of the LAN-Cell's key operating parameters. The Enable/Disable buttons allow you to easily change an interface's status.

Configuration parameters are entered on the main panel of each screen. Screens are divided into logical parameters groupings labeled with black bands.

3.3 Menu Structure

Status	Provides real-time and historical information about the LAN-Cell's operation.
Setup	Changes the LAN-Cell's LAN, WAN, DHCP, DDNS, Time and other settings. WAN configures the USB modem and wired Ethernet connections. WAN Advanced configures fail-over modes and related settings.
Wireless (Wi-Fi)	Configures the LAN-Cell's embedded 802.11 b/g/n Wi-Fi radio.
Security	Includes screens for configuring the LAN-Cell's firewall, filtering, and VPN features.
Applications	Port-Forwarding, DMZ and other application-specific settings.
QoS	Enables Quality-of-Service (bandwidth management) and performance enhancing features.
Admin	Includes system management, firmware updates, utilities and system event logging.

CHAPTER 4: QUICK SETUP

4.1 USB Modem Configuration

The LAN-Cell 3 auto-recognizes and configures itself for over 100 different USB modem models on dozens of cellular service provider networks. Please refer to the *LAN-Cell 3 Firmware Release Notes* for the list of currently supported modems.

The USB modem may need to be activated with a cellular service provider before it can used in the LAN-Cell 3 Follow the service provider or modem manufacturer's instructions for activating, testing, and updating the firmware on the USB modem before attempting to use it in the LAN-Cell 3.

Some modems require cellular service provider specific settings to be entered on the LAN-Cell 3's **Setup > WAN** screen. If the USB modem and carrier settings are not auto-detected, obtain the following information from the service provider:

Parameter	Your Cellular Carrier's Settings
Modem Manufacturer*	The original equipment manufacturer, not the ISP's brand
Modem Model #*	The original equipment manufacturers' model
APN†	
Authentication Type	
Username / Password	
ISP Access #Φ	#777 for CDMA, *99# for GSM
PIN Code‡	

* This information is often on the modem's label; sometimes under a removable cover.

† APN applies only to GSM carriers. Many GSM carriers operate different APNs for different types of data service plans.

Φ The LAN-Cell does not use the phone number assigned to the USB modem. That number is used only by the provider.

‡ The 4 digit PIN code field is required only if the SIM/RUIM is has been locked.

On the **Setup > WAN** screen (Figure 13), begin by selecting the USB modem brand and model. Next select the location, service provider name and specific APN setting (if required). If you are using a "custom" APN, select the Manual option and enter the custom APN value in the Access Point Name field.

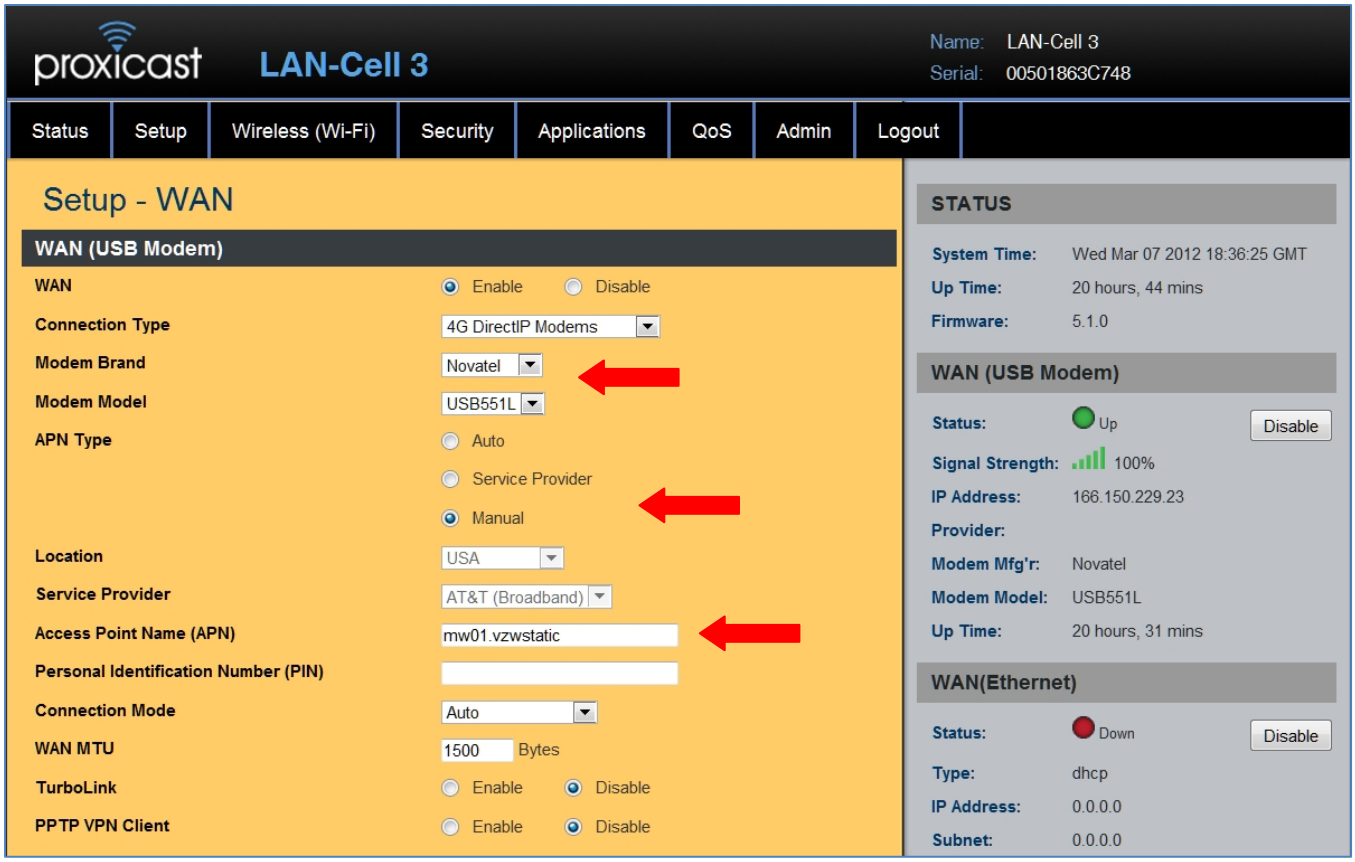


Figure 13: USB Modem Setup

Proxicast recommends implementing the WAN Fail-Over Connectivity Check found on the **Setup > WAN Advanced** screen for maximum 4G/3G connection reliability. By default, this feature is enabled and configured to ping a high-availability server.

4.2 WAN Configuration

The bottom half of the **SETUP > WAN** screen (Figure 14) is used to configure the LAN-Cell 3's Wired Ethernet WAN interface. For most Ethernet connections, the default DHCP client mode is sufficient. If your WAN interface has been assigned a static IP address, select "Static IP" from the Connection Type drop-down and enter the appropriate TCP/IP setting values. If your Ethernet connection uses the PPPoE protocol, select that Connection Type and enter your login information.

The LAN-Cell 3's Wi-Fi radio can also be used in place of the wired Ethernet WAN connection. For more information on this option, see Section 6.1.6.

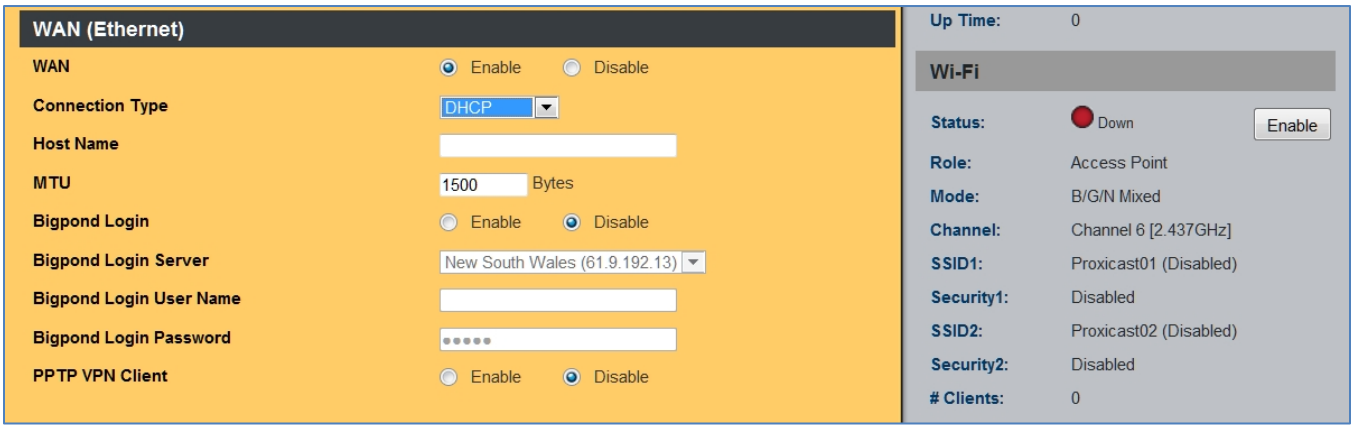


Figure 14: Ethernet WAN Setup

4.3 LAN Configuration

If you need to change the LAN-Cell 3's default LAN subnet (192.168.1.1 / 255.255.255.0), go to the **Setup > LAN** screen (Figure 15) and enter the IP address to assign to the LAN-Cell and select the desired subnet mask from the drop-down list. The LAN-Cell's DHCP server will automatically adjust to serve addresses from the new subnet.

Figure 15: Ethernet LAN Setup

4.4 Wi-Fi Configuration

The LAN-Cell 3's internal 802.11 b/g/n Wi-Fi radio is disabled by default as a security precaution. To provide laptops, tablets and other Wi-Fi devices with Internet connectivity through the LAN-Cell, go to the **Wireless (Wi-Fi) > Basic** screen (Figure 16) and enable the wireless connection.

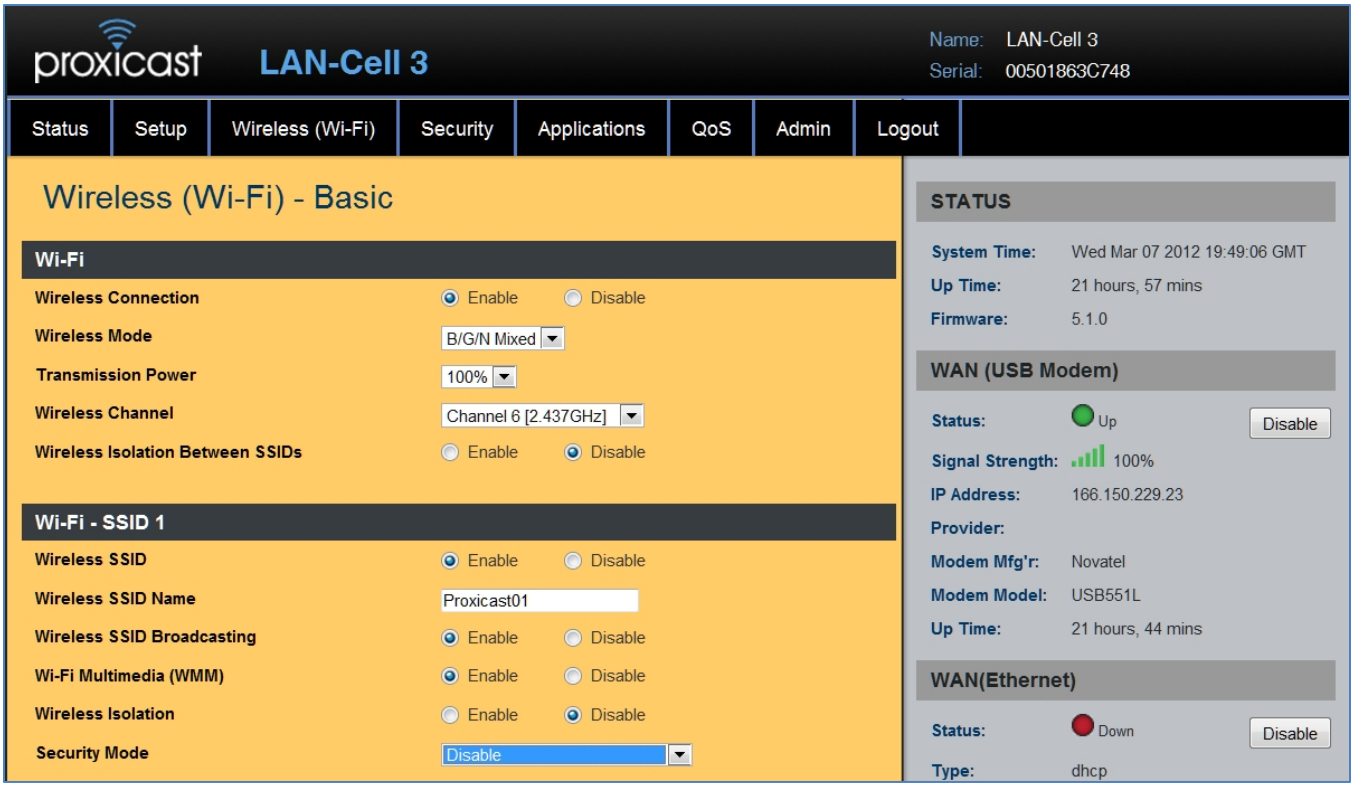


Figure 16: Wi-Fi Basic Setup

Only SSID1 will be enabled by default. You may change the SSID Name to suit your preference. We strongly recommend that you change the Security Mode to prevent authorized access to your Internet connection. The LAN-Cell 3 also supports a second SSID. This is most often used when you wish to provide “guest” access to your Internet service, but maintain guest devices on a different LAN subnet than your other devices.

4.5 Password

To change the LAN-Cell 3’s default password, select the **Admin > Management** screen (Figure 17). Enter the new password (case sensitive) and re-enter the value to confirm.

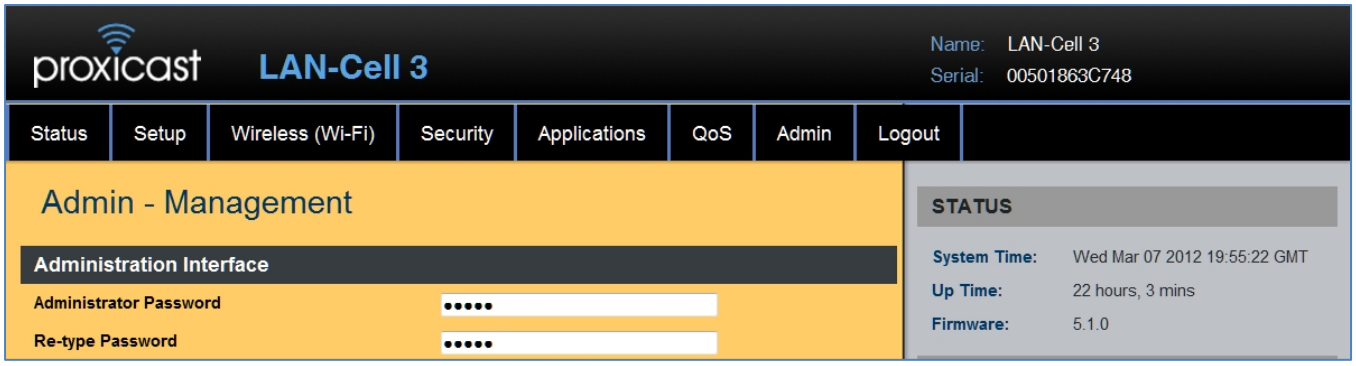


Figure 17: Changing the Admin Password

CHAPTER 5: STATUS MENU

5.1 Router

Router Information	
Model Name	LAN-Cell 3
Firmware Version	5.1.0
Current Time	Wed Mar 07 2012 20:07:30 GMT
Running Time	22 hours, 15 mins

WAN (USB Modem)	
MAC Address	00:A0:C6:00:00:00
Connection Type	directip
IP Address	166.150.229.23
Subnet Mask	255.255.255.240
Gateway	166.150.229.17

WAN (Ethernet)	
MAC Address	00:50:18:63:C7:4D
Connection Type	dhcp
IP Address	0.0.0.0
Subnet Mask	
Gateway	

LAN	
MAC Address	00:50:18:63:C7:48
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
DHCP Server	Enabled
DHCP Start IP Address	192.168.1.33
DHCP End IP Address	192.168.1.64

Figure 18: Router Status

5.1.1 Router Information

Model Name	Product model name is shown.
Firmware Version	The firmware version this device is running.
Current Time	Current system time
Running Time	The period of time LAN-Cell 3 has been running.

5.1.2 WAN (USB Modem)

MAC Address	MAC Address of the USB Modem (Direct IP modems only)
Connection Type	The current connection type (wwan or DirectIP)
IP Address	WAN IP address
Subnet Mask	Subnet mask
Gateway	IP address of the remote gateway

5.1.3 WAN (Ethernet)

MAC Address	MAC Address of the WAN port
Connection Type	The current connection type (PPPoE, Static IP, and DHCP)
IP Address	WAN IP address
Subnet Mask	Subnet mask
Gateway	IP address of the remote gateway

5.1.4 LAN

MAC Address	MAC Address of the LAN switch
IP Address	Internal IP Address of the LAN-Cell 3
Subnet Mask	Subnet mask in the internal network
DHCP Service	DHCP service enabled or disabled
DHCP Start IP Address	DHCP Start IP address
DHCP End IP Address	DHCP End IP address
Max DHCP Clients	The maximum IP addressed which can be assigned to PCs connecting to the network

5.1.5 Wi-Fi

Wireless Channel	Wireless Channel in use (default is 6)
Wireless SSID 1	SSID1 of the LAN-Cell
MAC Address 1	MAC Address for SSID1
Wireless SSID 2	SSID2 of the LAN-Cell
MAC Address 2	MAC Address for SSID2

5.2 Traffic

Click on **Status > Traffic** and then choose the graph scale from two hours, one day, one week, and one month. You will see the graph in Figure 19. You can monitor your download and upload throughput.

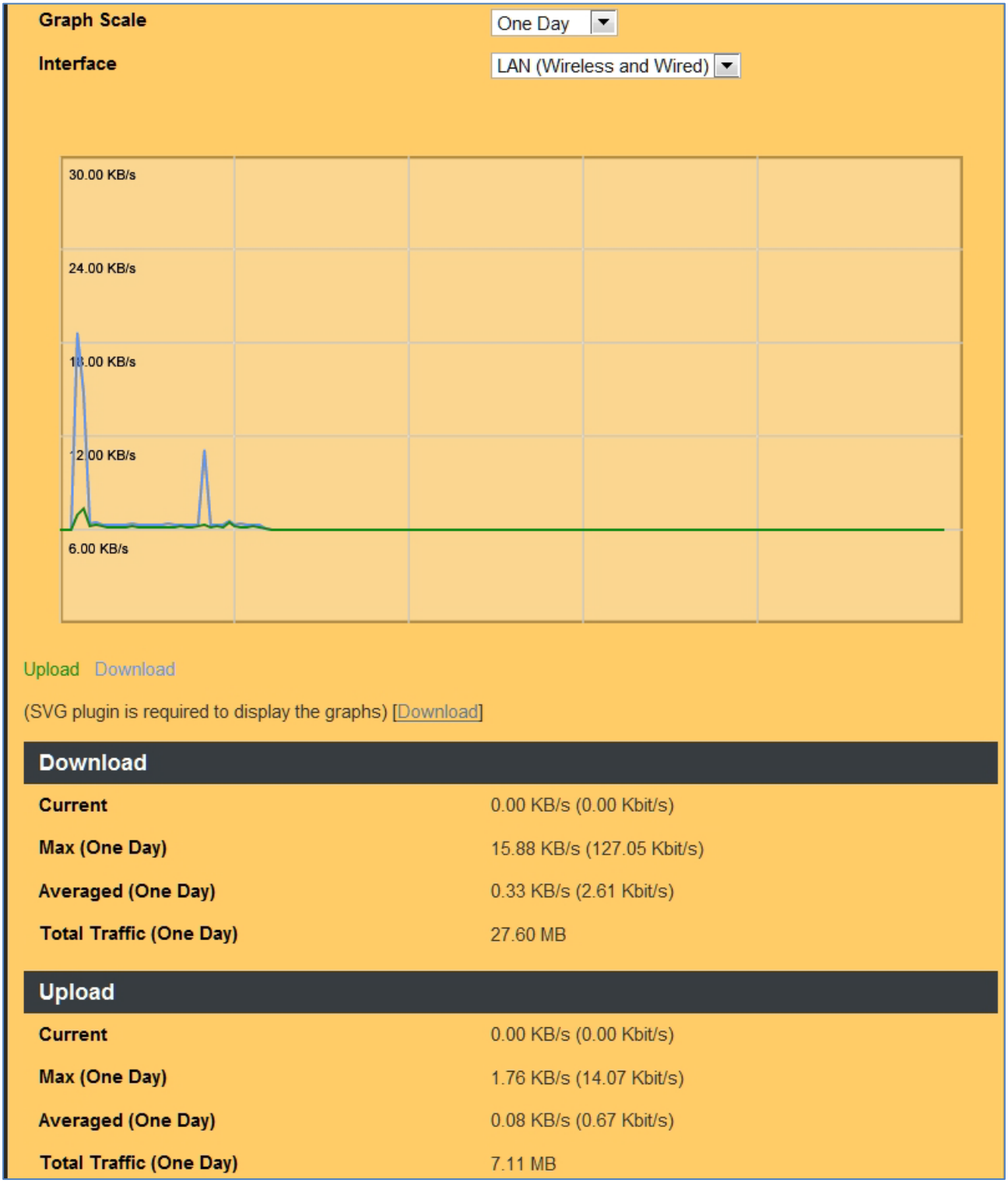
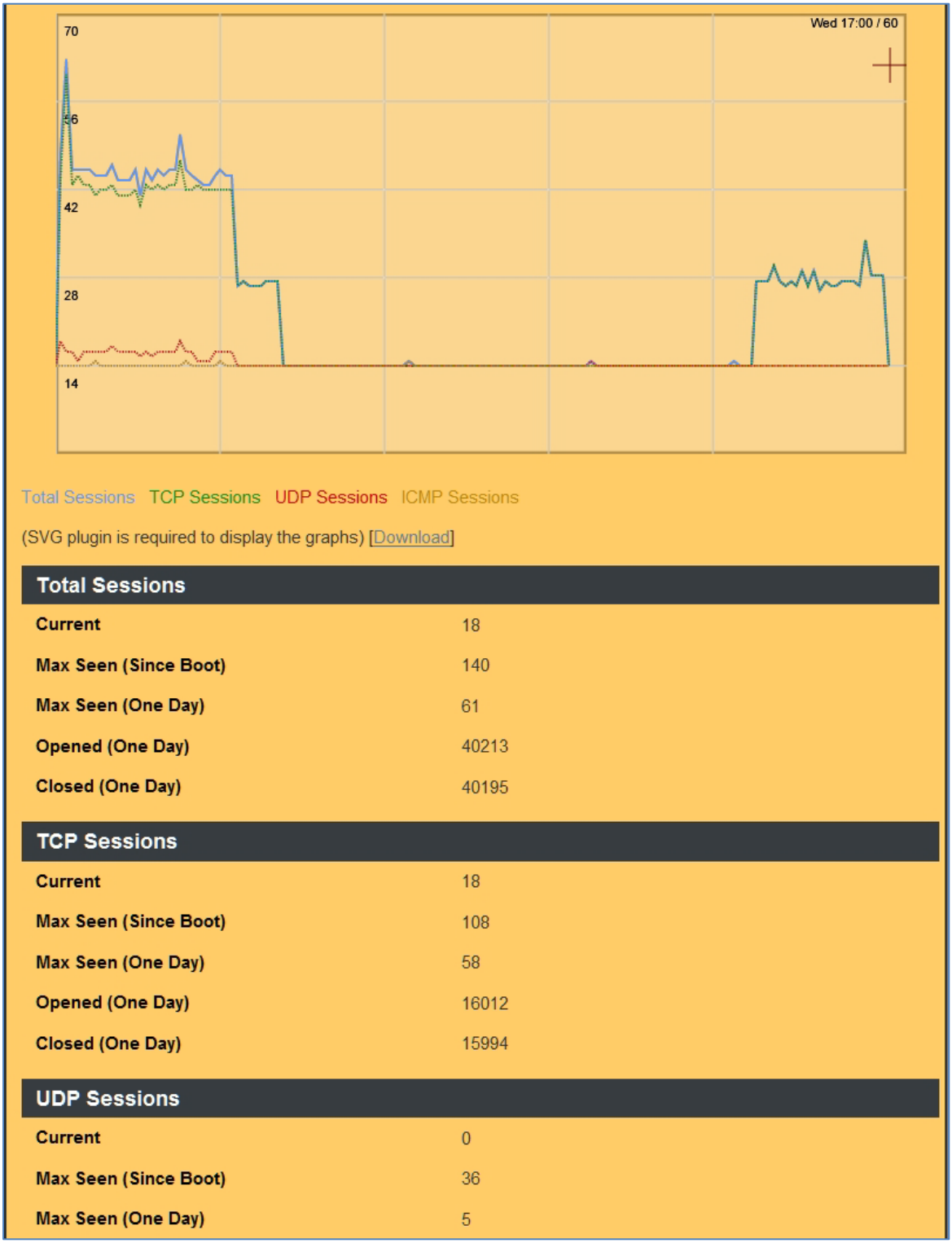


Figure 19: Traffic Status Graph

5.3 Session

Click on Status > Session and choose the graph scale from two hours, one day, one week, and one month. You will now see the graph in Figure 20. TCP, UDP, ICMP, and total session information is displayed.



Total Sessions	
Current	18
Max Seen (Since Boot)	140
Max Seen (One Day)	61
Opened (One Day)	40213
Closed (One Day)	40195

TCP Sessions	
Current	18
Max Seen (Since Boot)	108
Max Seen (One Day)	58
Opened (One Day)	16012
Closed (One Day)	15994

UDP Sessions	
Current	0
Max Seen (Since Boot)	36
Max Seen (One Day)	5

Figure 20: Session Status

5.4 User/DHCP

Displays a table of the system LAN users and their IP addresses, MAC addresses and remaining DHCP lease times.

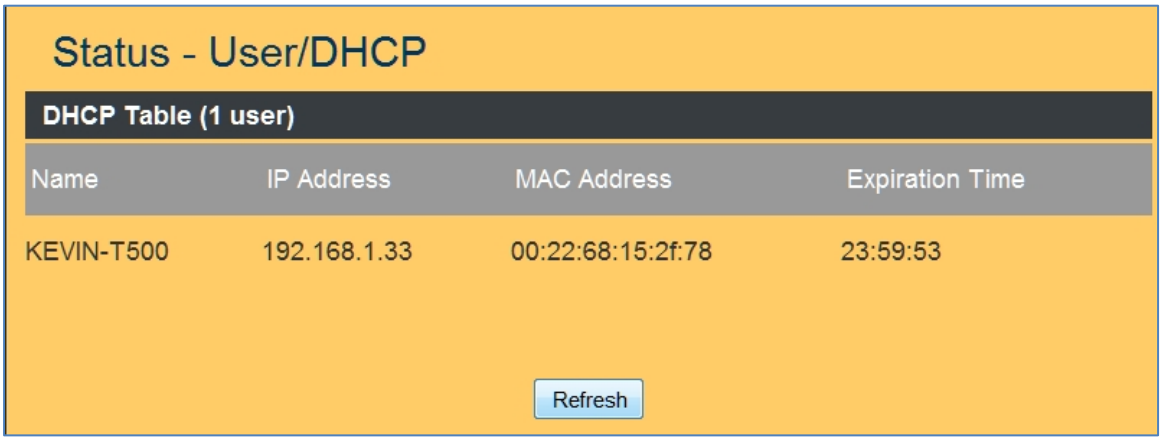


Figure 21: User/DHCP Status

Name	DHCP client name
IP Address	IP address which is assigned to this client
MAC Address	MAC address of this client
Expiration Time	The remaining time of the IP assignment

5.5 Current Users

Displays a table of the system LAN and WAN users and their IP addresses.

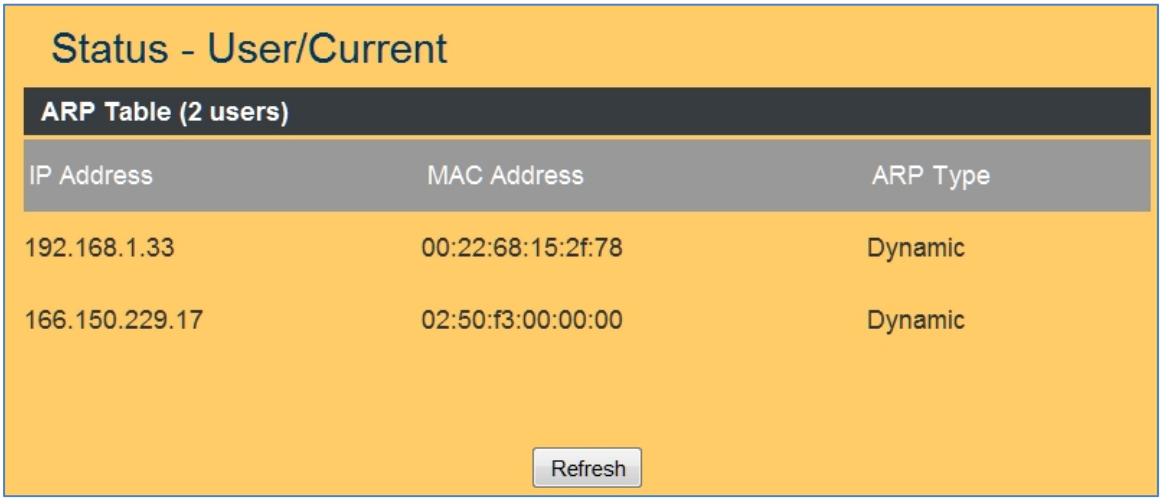


Figure 22: Current Users

IP Address	IP address assigned by Static ARP matching
MAC Address	MAC address in the Static ARP matching
ARP Type	Static or dynamic

CHAPTER 6: SETUP MENU

6.1 WAN

6.1.1 WAN (USB Modem)

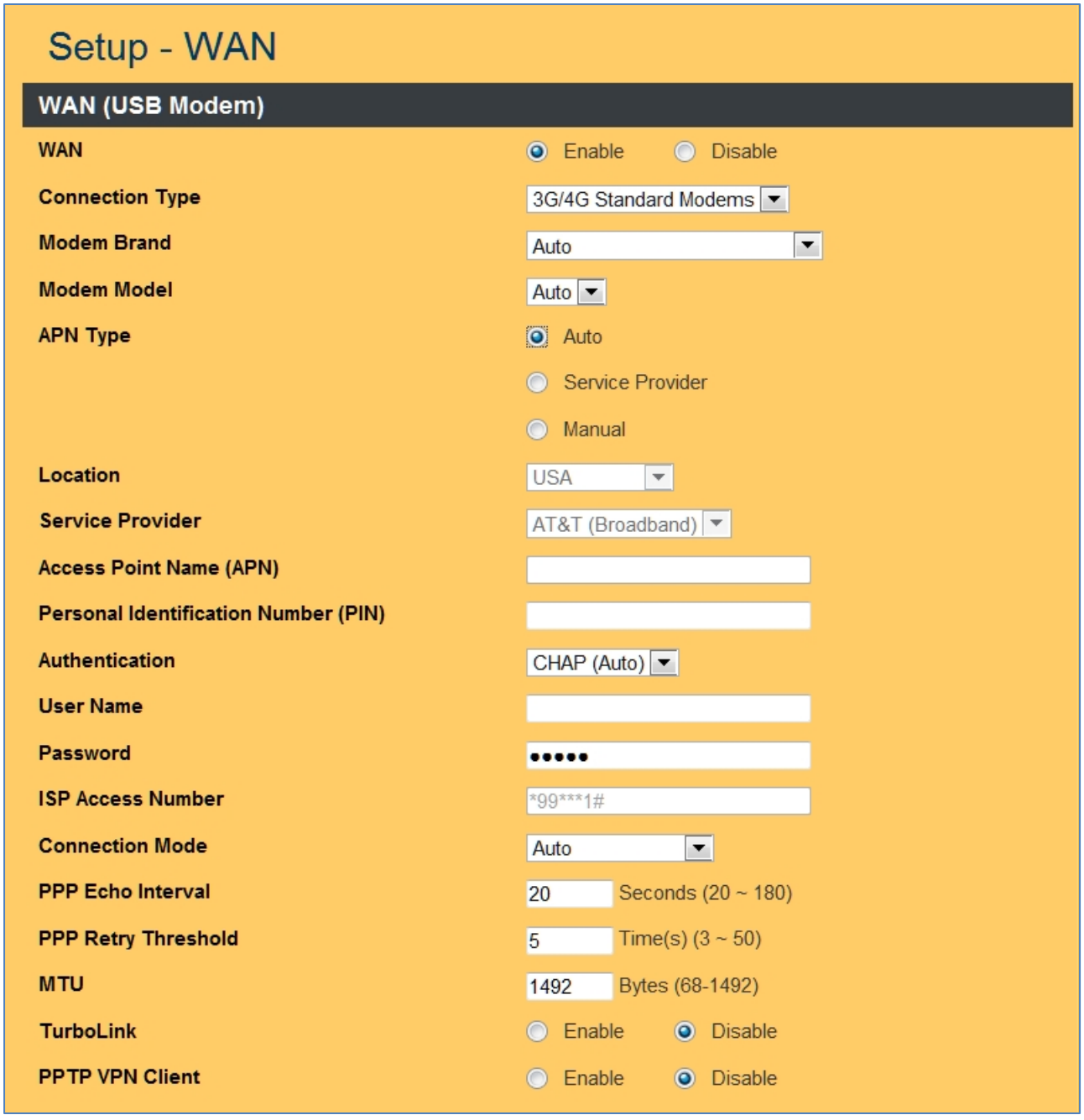


Figure 23: Setup WAN USB Modem

WAN	Select Enable/Disable to enable/disable USB WAN
Connection Type	PPP or DirectIP modems
Modem Brand	Choose your modem's brand. Select Auto for automatic detection.
Modem Model	Choose your modem's model number. Select Auto for automatic detection.
APN Type	Choose Auto to use an APN preo-programmed into your USB modem. Select by Service Provider for to the ISP you use, or otherwise choose Manual to assign desired APN.
Location	Choose your country.
Service Provider	Choose your cellular service provider and the Access Point Name (APN) will be automatically assigned.
Access Point Name (APN)	Enter APN string offered by the ISP if you select Manual for APN Type. Leave this field blank if your ISP does not use APN's (e.g. CDMA networks).
Personal Identification Number (PIN)	Enter PIN code required by your modem. Leave it blank if a PIN code has not been assigned.
Authentication Type	Typically "Auto" or select CHAP/PAP/None as required.
User Name	The user name required by the ISP (blank if your ISP doesn't require a username).
Password	The password required by the ISP (blank if your ISP doesn't require a username).
ISP Access Number	Enter ISP Access Number required by the ISP to connect to their data network (GSM default *99***1# CDMA default #777). DO NOT enter the phone number assigned to the USB modem.
Connection Mode	Typically "Auto" or can be used to force the modem to operate in a specific mode (if supported by the modem).
PPP Echo Interval	PPP echo will ensure whether the link is still up or not (default interval 20 seconds)
PPP Retry Threshold	When PPP echo retry exceeds PPP Retry Threshold (default 5 times), the connection is recognized as down.
MTU	PPP maximum transmission unit: up to 1492 bytes (PPP's header is 8 bytes).
TurboLink	Although typically not required, enable "TurboLink" to improve the connection stability. (Please note that TurboLink function will increase your 3G/4G data usage)
PPTP VPN Client	Enable to allow the USB WAN to make a client connection to a remote PPTP server. If enabled, enter the PPTP username, password, VPN host IP address and MPPE128 parameters required for the PPTP VPN connection.

6.1.2 WAN (Ethernet)

LAN-Cell 3 supports four WAN connection types in addition to the USB Modem: DHCP, Static, PPPoE, Wi-Fi-Client. Select the appropriate connection type from the pull-down menu. The screen will expose the related fields for each type of WAN connection.

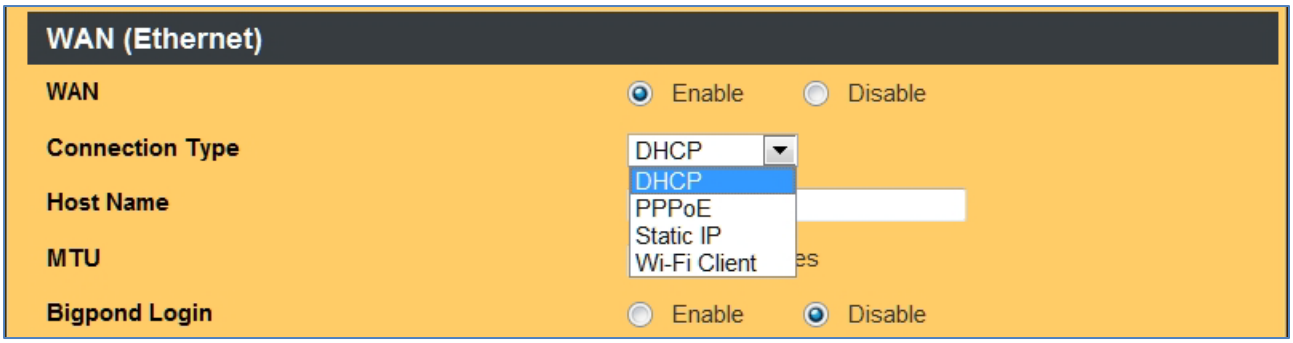


Figure 24: WAN (Ethernet) Connection Types

6.1.3 DHCP (automatic IP address assignment)

The IP address is automatically assigned to you by your ISP (most common Ethernet WAN option).

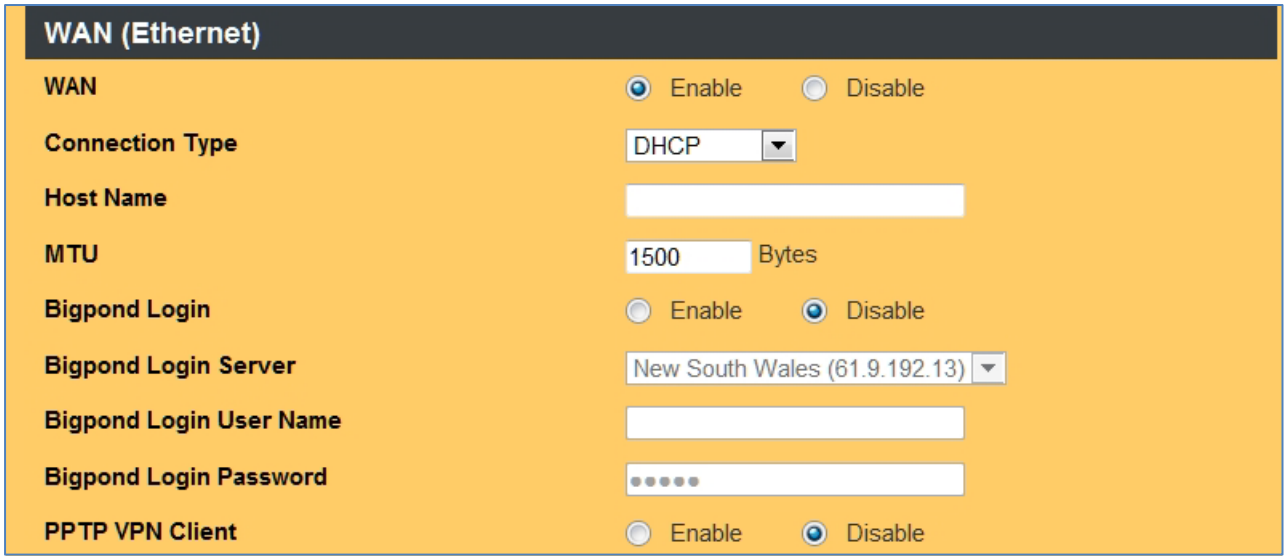


Figure 25: Setup WAN Ethernet DHCP

WAN	Select Enable/Disable to enable/disable WAN
Connection Type	DHCP
Host Name	Some ISP and DHCP servers ask for the Host Name of the DHCP client before assigning an IP address. In this case, enter your Host Name.
MTU	Maximum Transmission Unit (1500 is the default for Ethernet)
Bigpond Login	If you are using the “Bigpond” system, please enable this item
Bigpond Login Server	Please choose the Bigpond server.
Bigpond Login User Name	Please enter your User Name provided by Bigpond
Bigpond Login Password	Please enter your Password provided by Bigpond
PPTP VPN Client	Enable to allow the WAN to make a client connection to a remote PPTP server. If enabled, enter the PPTP username, password, VPN host IP address and MPPE128 parameters required for the PPTP VPN connection.

6.1.4 Static (Fixed IP address assignment)

The IP address, subnet mask, gateway, and DNS server are provided by your ISP.

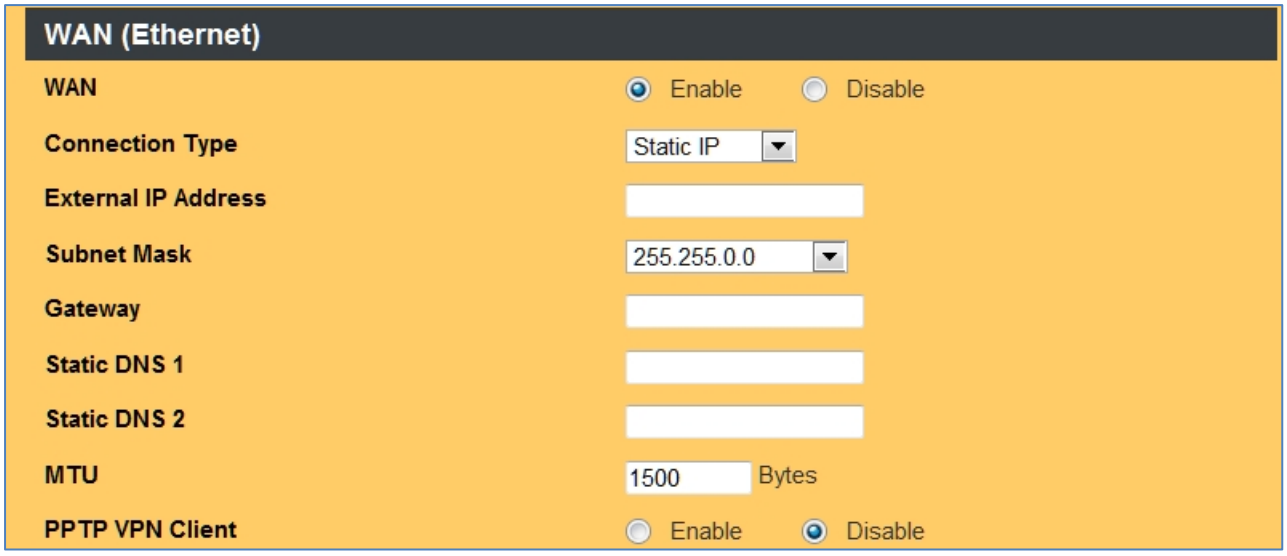


Figure 26: Setup WAN Ethernet Static IP

WAN	Select Enable / Disable to enable/disable WAN.
Connection Type	Static IP
External IP Address	The external IP addresses assigned by the ISP.
Netmask	The netmask assigned by the ISP.
Gateway	The gateway assigned by the ISP.
Static DNS 1	The static DNS 1 assigned by the ISP.
Static DNS 2	The static DNS 2 assigned by the ISP.
MTU	Maximum Transmission Unit (1500 is the default for Ethernet)
PPTP VPN Client	Enable to allow the WAN to make a client connection to a remote PPTP server. If enabled, enter the PPTP username, password, VPN host IP address and MPPE128 parameters required for the PPTP VPN connection.

6.1.5 PPPoE (connected by username/password)

If your ISP provides the username and password, please enter the information accordingly.

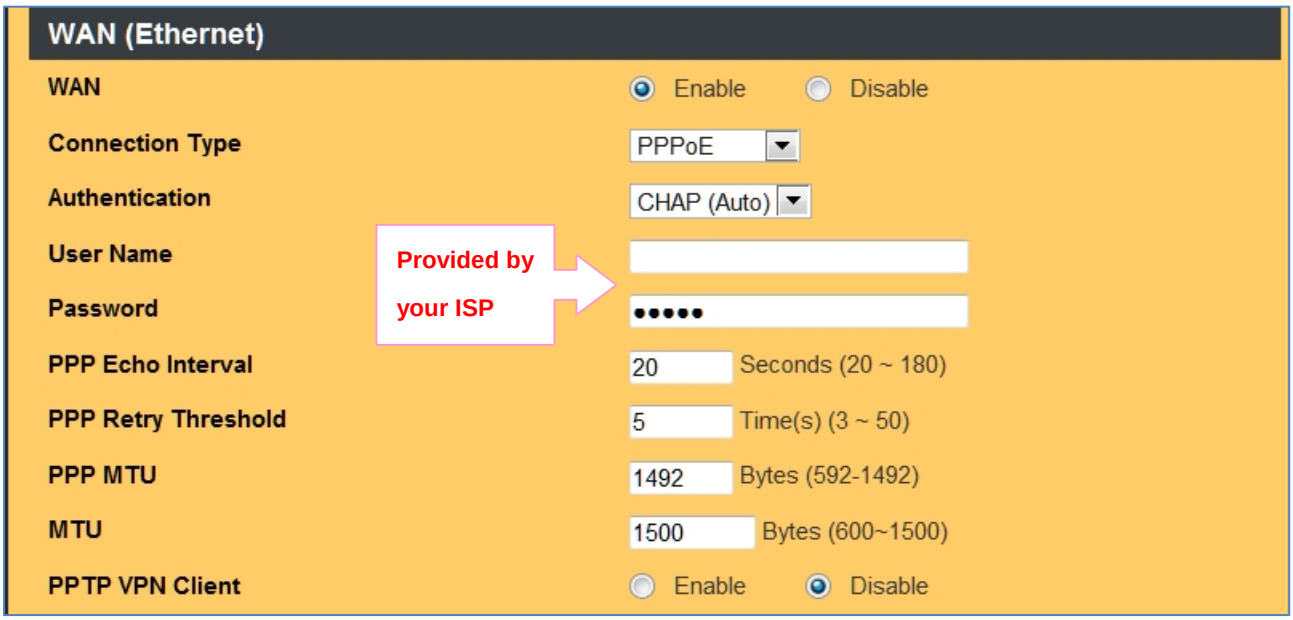


Figure 27: Setup WAN Ethernet PPPoE

WAN	Select Enable/Disable to enable/disable WAN
Connection Type	PPPoE
Authentication Type	Typically “Auto” or select CHAP/PAP/None as required.
User Name	The user name assigned by the ISP.
Password	The password assigned by the ISP.

PPP Echo Interval	PPP echo will ensure whether the link is still up or not (default interval 20 seconds)
PPP Retry Threshold	When PPP echo retry exceeds PPP Retry Threshold (default 5 times), the connection would be recognized as down.
PPP MTU	PPP maximum transmission unit: up to 1492 bytes (PPP's header is 8 bytes)(This value should be less than MTU value at least 8 bytes).
PPTP VPN Client	Enable to allow the WAN to make a client connection to a remote PPTP server. If enabled, enter the PPTP username, password, VPN host IP address and MPPE128 parameters required for the PPTP VPN connection.

6.1.6 Wi-Fi Client

The LAN-Cell 3's built-in Wi-Fi radio can be used as a WAN interface to establish a connection to an external Wi-Fi network. Whenever the LAN-Cell 3 detects the target Wi-Fi network, it will automatically make a connection to this network. This option disables the Ethernet WAN interface, but the LAN-Cell 3 can still function as a local Wi-Fi access point while connected to the remote Wi-Fi network.

Note: the LAN-Cell 3's Wi-Fi radio must first be enabled on the **Wireless (Wi-Fi) > Basic** screen.

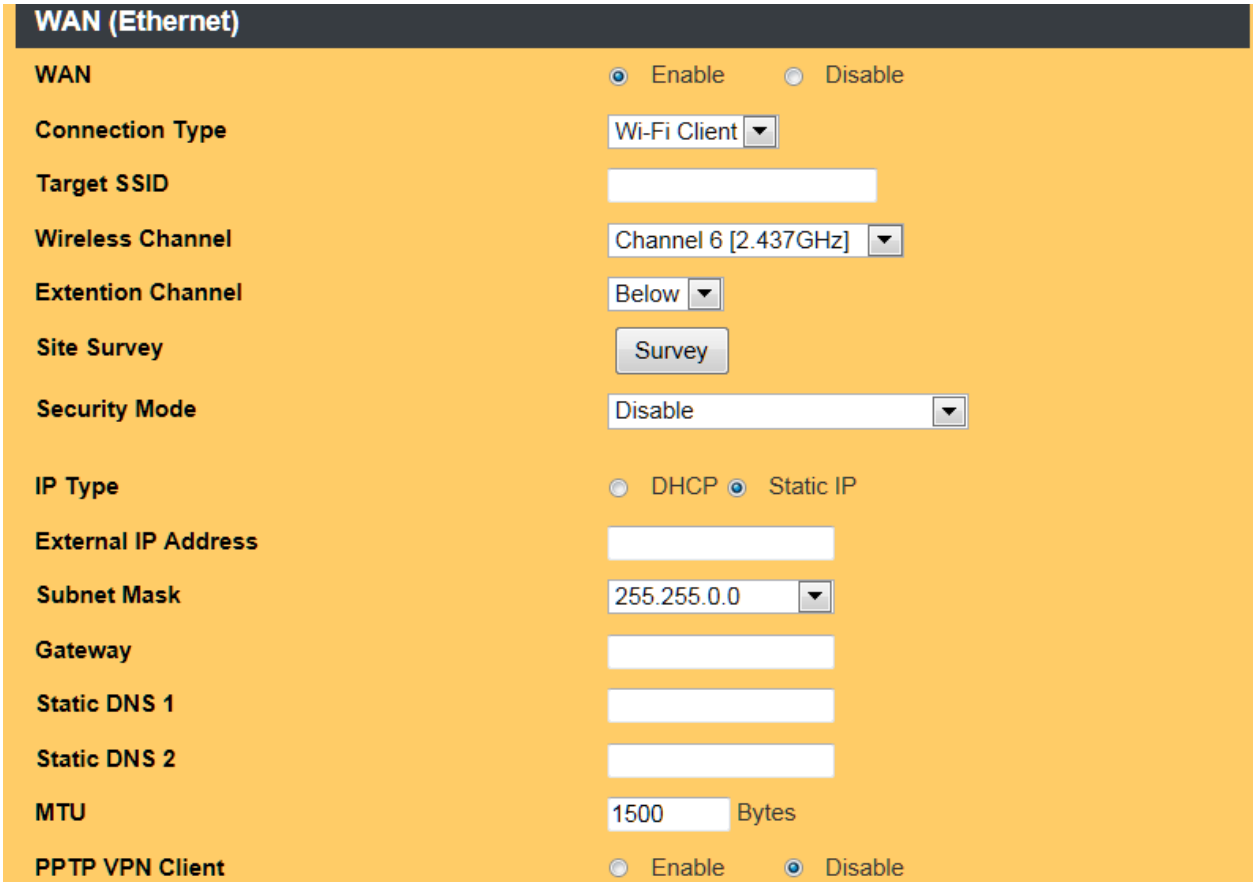


Figure 28: Setup WAN Wi-Fi Client

WAN	Select Enable/Disable to enable/disable WAN
Connection Type	Wi-Fi Client
Target SSID	Enter the SSID of the external target Wi-Fi network to connect to.
Target BSSID (MAC)	Enter the BSSID to connect to. The BSSID is optional if you set the target SSID.
Wireless Channel	Select the Wi-Fi channel number used by the target Wi-Fi network.
Extension Channel	When operating in 40 MHz mode the access point will use an extended channel either below or above the current channel. Optimal selection will depend on the channels of other networks in the area.
Site Survey	Click this button to display a table of visible Wi-Fi networks. Select the desired network from the Site Survey table and the associated SSID and channel information will be automatically entered.
Security Mode	Select the Security Mode which matches the target Wi-Fi network. Enter the associated security information (such as pre-shared keys) required by the target Wi-Fi network.
IP Type	Select DHCP if the external access point will assign IP address information to the LAN-Cell. Select Static IP to manually assign the IP information.
External IP Address	Static IP address to use with the external access point.
Subnet Mask	Subnet mask of the external access point's network.
Gateway	IP address of the Internet gateway router on the external Wi-Fi network.
Static DNS1 & DNS2	Domain name servers for the external Wi-Fi network.
MTU	Maximum Transmission Unit (1500 is the default for Ethernet)
PPTP VPN Client	Enable to allow the WAN to make a client connection to a remote PPTP server. If enabled, enter the PPTP username, password, VPN host IP address and MPPE128 parameters required for the PPTP VPN connection.

6.2 WAN Advanced

The WAN Advanced screen configures several advanced WAN settings including:

- Fail-Over
- Load Balancing
- Keep-Alive

The settings are the same for both the USB and Ethernet WAN interfaces.

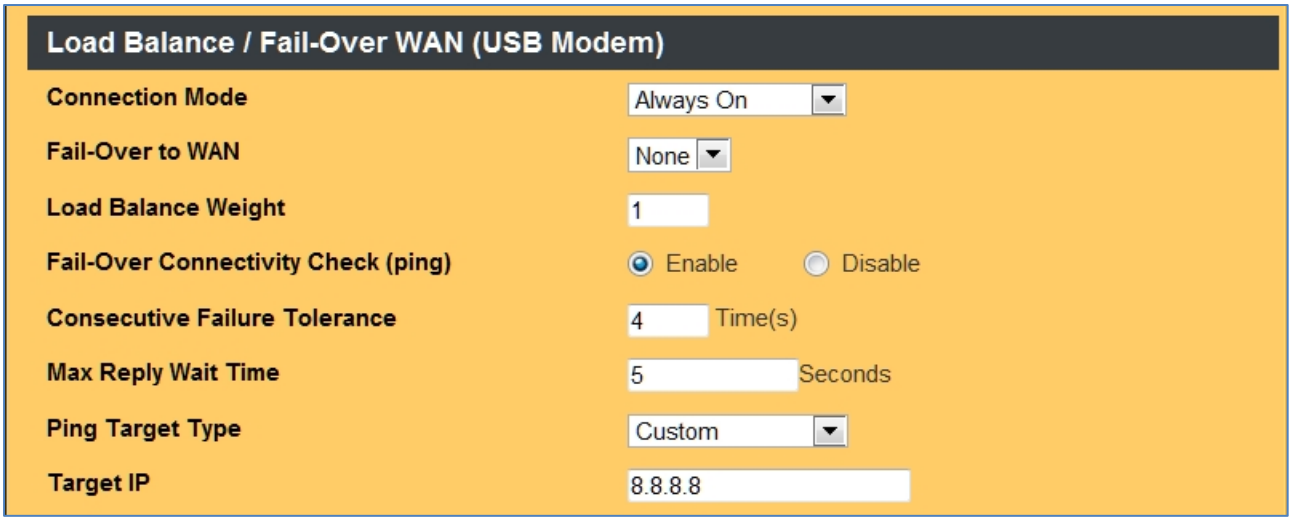


Figure 29: Setup WAN Advanced

Connection Mode	**Always On**: WAN connection is always established and routes traffic as required. **Backup Standby**: WAN connection is always established but only routes traffic when primary WAN is down (route on demand) **Backup**: WAN connection is only established and only routes traffic when primary WAN is down (connect on demand + route on demand).
Fail-Over to WAN	If one of the WAN's is marked as "Backup" or "Backup Standby", the other WAN will allow you select that WAN as the backup for the current WAN (e.g. if you want the Ethernet WAN to be primary and have it fail-over to use the USB WAN when necessary, mark the USB WAN as "Backup Standby", and select USB WAN as the "Fail-Over to WAN" for the Ethernet WAN interface.
Load Balance Weight	The weight for session-based multi-path routes. Sessions will be established in weighted round-robin fashion on the WANs as new requests are received from LAN devices. Increase the Load Balance Weight of one WAN versus the other to have a higher percentage of traffic flow out that WAN when both WANs are active. Note: finer-grained control over WAN traffic can be achieved using the **Static Routing** feature.

Fail-Over Connectivity Check (ping)	Enable/disable the use of ICMP (ping) packets to determine if a WAN interface is currently up.
Consecutive Failure Tolerance	The number of consecutive pings that must fail to be acknowledged before the interface is marked as down.
Max Reply Wait Time	The maximum number of seconds to wait for each ping to be acknowledged (maximum latency) before assuming the ping to have failed.
Ping Target Type	**Default Gateway**: sends ICMP packets to the ISP's default gateway address. Note: many ISP's do not support ICMP replies from their default gateways. **Custom**: sends ICMP packets to an IP address of your choosing.
Target IP	Enter the IP address of the custom host target to be used.

6.3 LAN

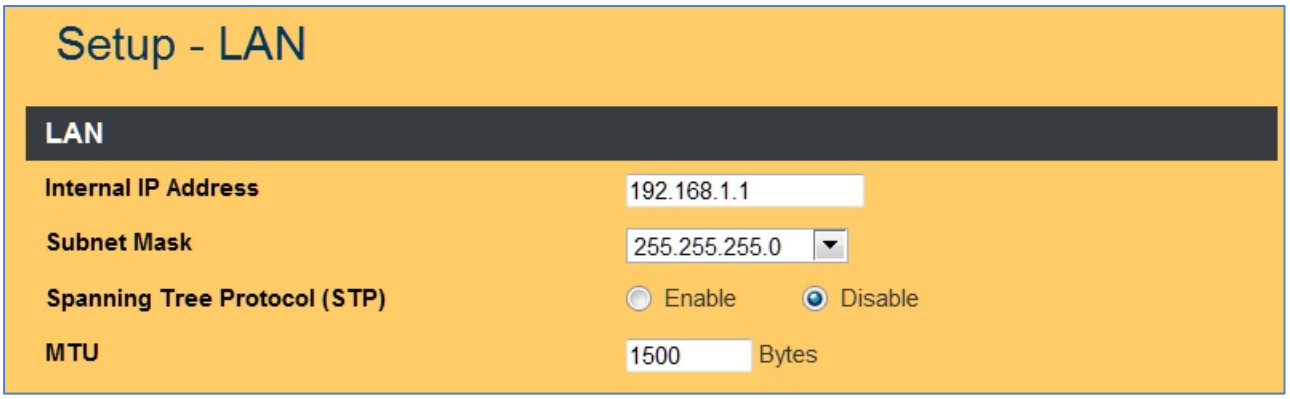


Figure 30: Setup LAN

Internal IP Address	Sets the internal LAN IP address of the LAN-Cell 3. Note: The LAN-Cell's built-in DHCP Server will automatically adjust to the IP address and subnet entered.
Subnet Mask	Select the appropriate subnet mask from the list.
Spanning Tree Protocol (STP)	Click Enable to avoid cyclic topology caused by incorrect connection of your internal network.
MTU	Maximum transmission unit: up to 1500 bytes.

6.4 Static Routing

6.4.1 Static Routing Settings

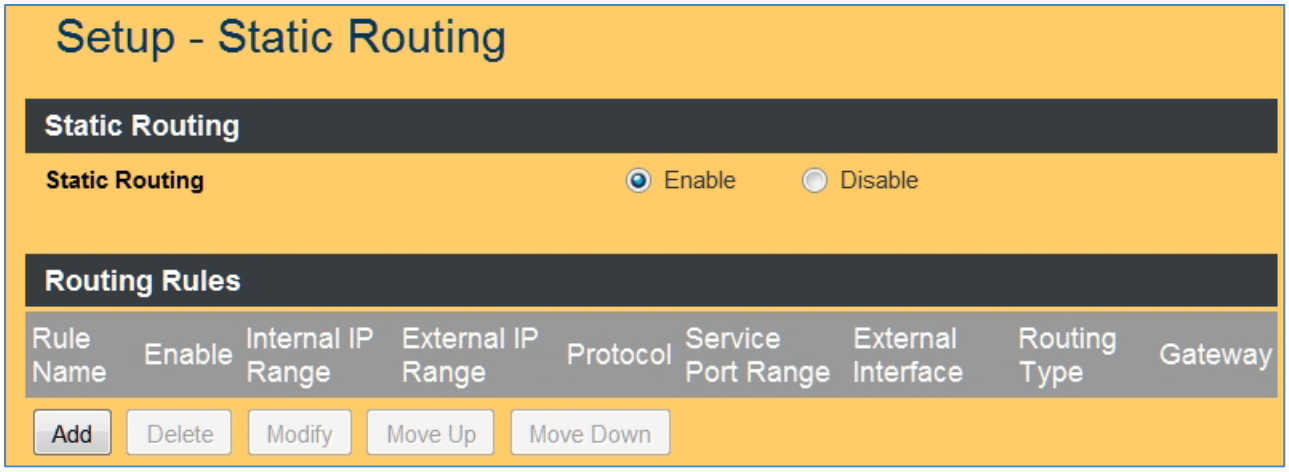


Figure 31: Setup Static Routing

Static Routing	Choose Enable/Disable to enable/disable the static routing feature.

6.4.2 Add Routing Rule

Click on the [Add] button. The screen shown in Figure 32 will open.

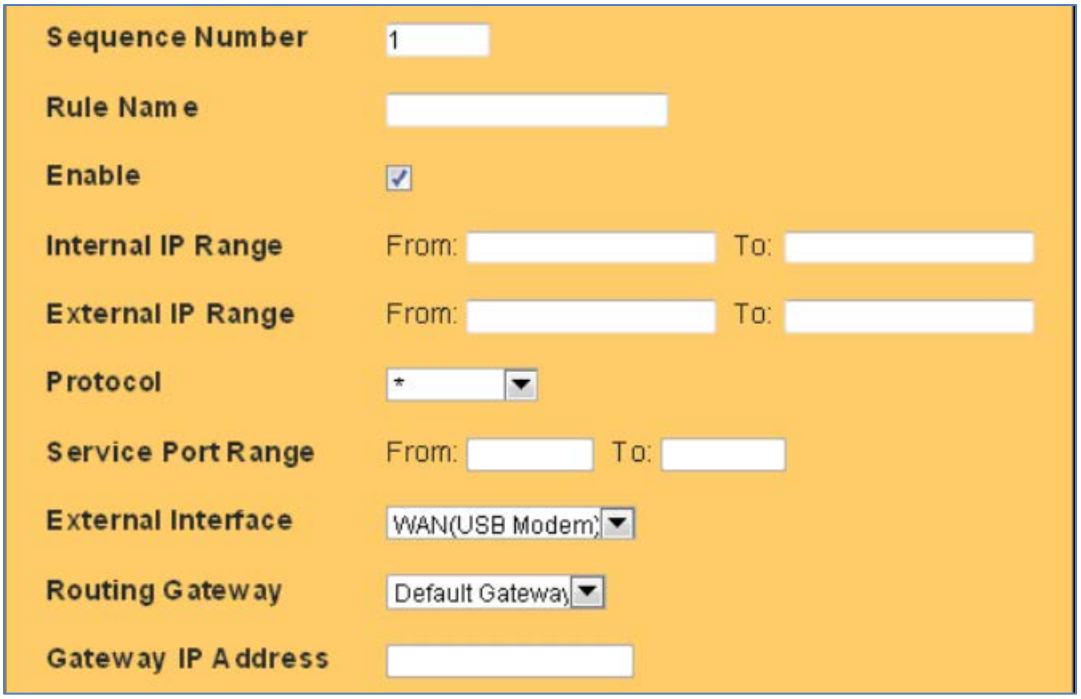


Figure 32: Add Static Routing Rule

Sequence Number	This defines the sequence of the Routing rules. If a packet fits the conditions set by the Routing rules, the packet will then be sorted according to the first Routing rule from the top of the list.
Rule Name	Descriptive name of the Routing rule. Rule names may not contain spaces.
Rule Enable	Enable/Disable this Routing rule
Internal IP Range	Set up the internal IP range for this rule.
External IP Range	Set up the external IP range for this rule.
Protocol	Set up the protocol (TCP or UDP) for the to be enabled.
Service Port Range	Set up the Service Port Range (e.g., HTTP is TCP/80) for the to be enabled.
External Interface	Select which External Interface (USB WAN, Ethernet WAN or LAN) for the packets to go through, IF the packet fits the condition of this rule. If your LAN includes another Internet gateway device, you can create a “traffic redirect” rule using the LAN interface to send selected traffic to the other gateway.
Routing Gateway	**Default Gateway**: Use the default gateway of the selected external interface. **Static Gateway**: Use the specific gateway IP address entered.
Gateway IP Address	IP address of the static gateway.

6.4.3 Static Routing Examples

This example forces all E-Mail sent through the LAN-Cell to go through the USB WAN interface exclusively. All other types of traffic is unaffected by this rule.

Rule Name	SMTP-to-USB
Enable	Enable
Internal IP Range	Blank (applied to all)
External IP Range	Blank (applied to all)
Protocol	TCP
Service Port Range	25:25 (SMTP Port:25)
External Interface	WAN USB
Routing Gateway	Default Gateway

This type of rule can be used to create policies that direct specific types of traffic to specific interfaces. It can also be used to segment the LAN traffic for load balancing and other purposes.

This example forces traffic associated with a specific test PC (192.168.1.27) on the LAN to communicate only with the Headquarters network (24.3.85.1/24) using a specific gateway address (12.85.33.147).

Rule Name	Test-PC-to-HQ
Enable	Enable
Internal IP Range	192.168.1.27 - 192.168.1.27
External IP Range	24.3.85.1 – 24.3.85.254
Protocol	*
External Interface	WAN Ethernet
Routing Gateway	Static Gateway
Gateway IP	12.85.33.147

You can combine the Static Routing Rules with the LAN-Cell 3's WAN Load-Balancing Weights and the Quality of Service (QoS) Bandwidth Management features to gain precise control over which devices and protocols use specific interface resources.

6.5 DHCP Server

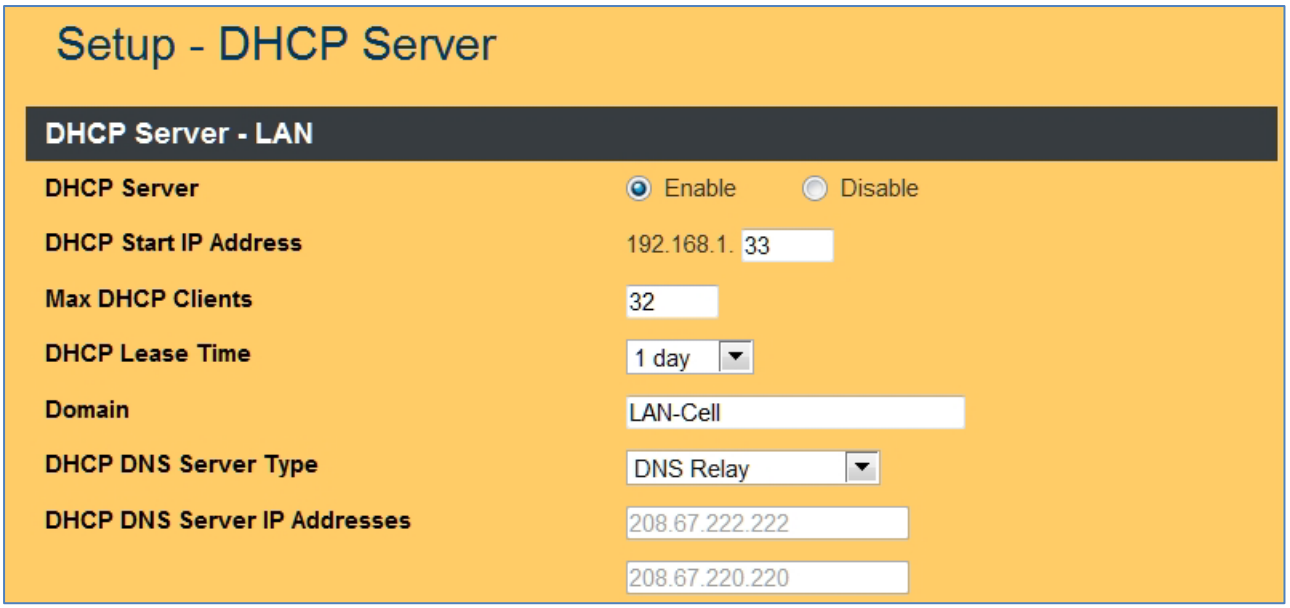


Figure 33: Setup DHCP Services

DHCP Server	Select Enable/Disable to enable/disable DHCP Server.
DHCP Starting IP Address	The DHCP starting IP address offered by the DHCP Server. The DHCP Server is limited to a Class-C (/24) subnet and automatically adopts the subnet that the LAN-Cell's LAN interface is assigned to.
Max DHCP Clients	The maximum number of the IP addresses supported by the DHCP server.
DHCP Lease Time	Please choose lease time from the selection list. You can choose 1 Hour, 3 Hours, 6 Hours, 1 Day, 3 Days, or 7 Days.
Domain	Enter a domain name if LAN devices require a domain assignment as part of the DHCP information.
DHCP DNS Server Type	**DNS Relay:** DHCP devices will be assigned the LAN-Cell's LAN IP address as their DNS Server. The LAN-Cell will relay all DNS requests to the appropriate external DNS server. This is the default and most common mode of operation. **ISP DNS Server**: The DNS Servers from WAN ISP will be relayed to DHCP clients. **OpenDNS Server**: DNS Servers operated by the OpenDNS project will be relayed to DHCP clients. **Google DNS Server**: DNS Servers operated by Google will be assigned to DHCP devices. Currently 8.8.8.8 and 8.8.4.4 are used. **Custom**: Enter the appropriate DNS addresses in the fields below. These will be relayed to DHCP devices.

6.6 DDNS

DDNS (Dynamic Domain Name Service) allows an “internet domain name” to be assigned to a computer/router which has a dynamic IP address. This makes it possible for other internet devices to connect to the computer/router without needing to trace the changing IP addresses themselves. To enable DDNS, you will first need to sign up for DDNS services from one of the supported DDNS service providers such as DynDNS.org, TZO.com or ZoneEdit.com.

DDNS is useful when combined with the virtual host and/or port-forwarding features. It allows internet users to connect to your virtual host by using a domain name, rather than an IP address. The DDNS service helps users to locate the right IP address by the domain name.

For example, assume that you wish to remotely access a web server embedded in one of your LAN devices, but you obtain a different IP address from your ISP every time you connect to the internet. In this case, you will need to enable DDNS, so users can connect to your web server through a fixed domain name without regard for the changing IP address of your WAN connection.

Note: As a service to its customers, Proxicast operates a Dynamic DNS service which is automatically updated each time a LAN-Cell WAN IP changes. The DDNS host name is the serial number of the LAN-Cell 3 in the”proxidns.com” domain. For example: 00501863C748.proxidns.com

This “permanent” DDNS name is always available but cannot be changed. To create your own hostname, register with one of the supported DDNS service providers before configuring the LAN-Cell’s DDNS settings.

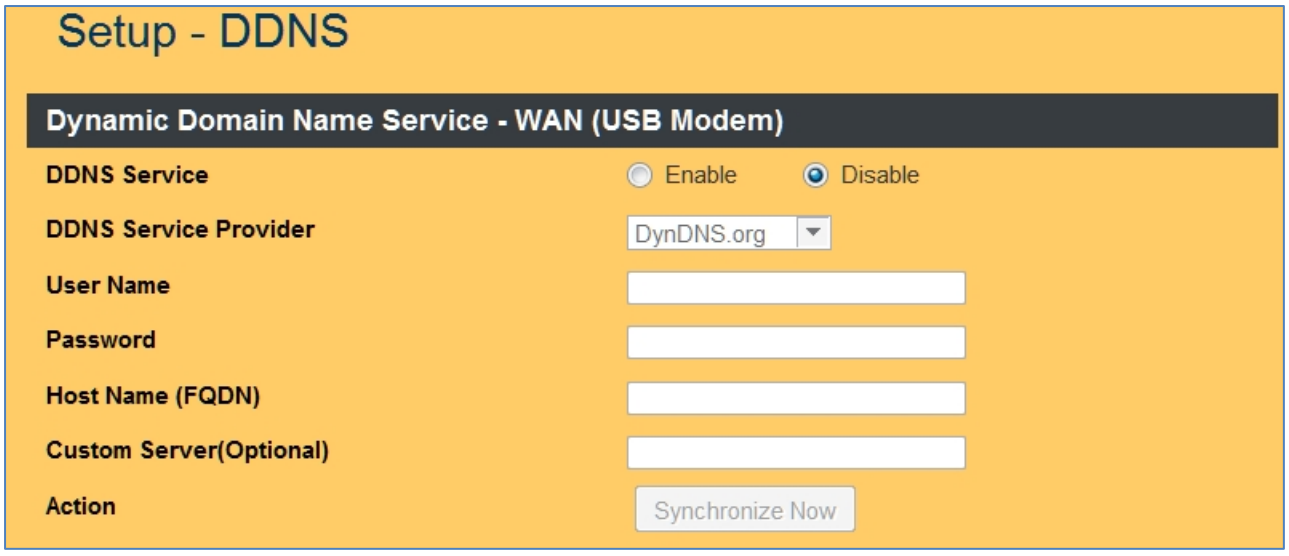


Figure 34: Setup DDNS Service

DDNS Service	Select Enable to enable DDNS service. Select Disable to disable DDNS service.
DDNS Service Provider	Select the desired DDNS service provider from the list.
User Name	Enter your username for your DDNS service provider account. We recommend avoiding special characters (#, $, &, @, etc) in your password.
Password	Enter your password for your DDNS service provider account. We recommend avoiding special characters (#, $, &, @, etc) in your password.
Host Name	Enter the full-qualified domain name (FQDN) assigned by your DDNS service provider for this specific LAN-Cell. Enter the entire domain name, e.g.: myrouter.mydomain.com You must define this hostname within your DDNS service provider account before it can be updated by the LAN-Cell. The hostname must match exactly on both the DDNS account and this screen.
Custom Server	If your DDNS service provider assigns you a custom update server, enter that value here.
Synchronize Now	Once your DDNS values have been saved, this button is enabled to force the LAN-Cell to attempt to update the DDNS service provider with the latest WAN IP address. Check the Log for full results.

The DDNS settings are the same for both the USB and Ethernet WAN interfaces. If both WAN interfaces will be operating simultaneously, enter a different hostname for each WAN interface. If the WANs are being used in fail-over (backup) mode, enter the same hostname for both interfaces.

6.7 MAC Address Clone

Some ISPs only allow a registered MAC address to access to the internet. To bypass the requirement, you need to set up a cloned MAC address for LAN-Cell 3 using the pre-registered MAC address.

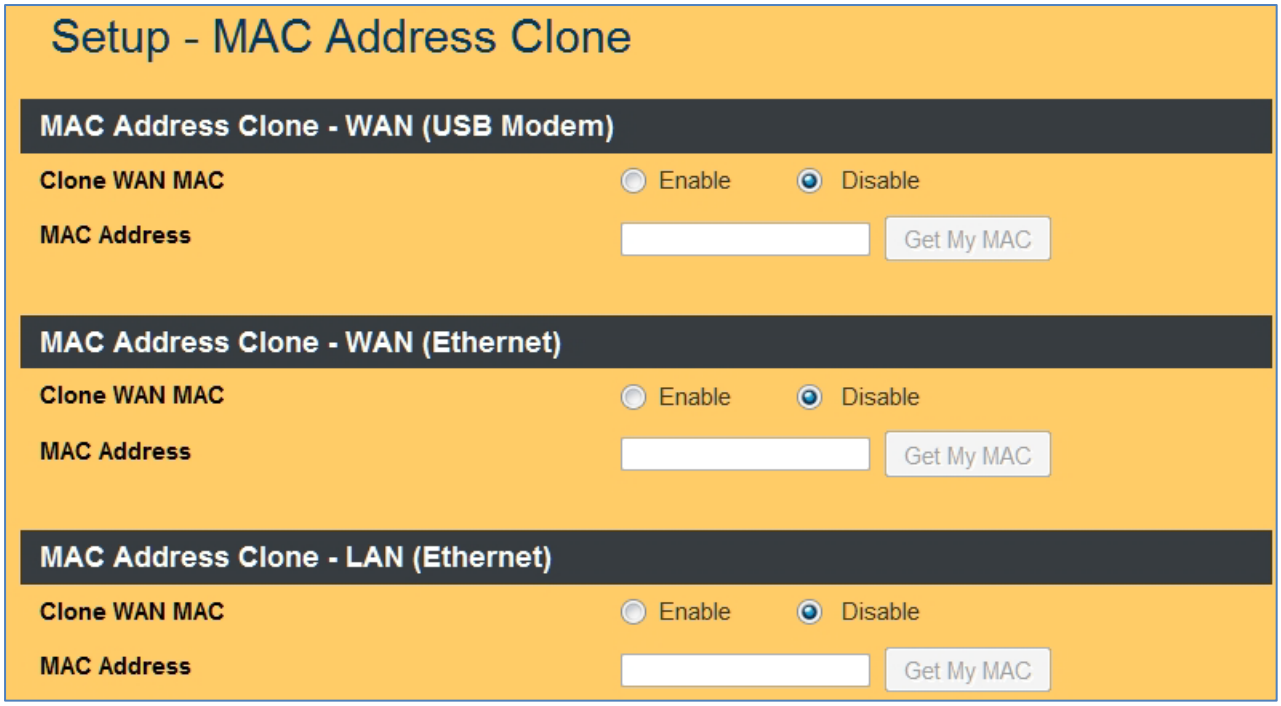


Figure 35: Setup MAC Address Clone

Clone WAN MAC	If your ISP grants access only to a fixed MAC address, select Enable. If your ISP does not enforce access control, please select Disable.
MAC Address	If the PC you use to configure LAN-Cell 3 is the device which has the MAC address authorized to access the internet, press **Get My MAC** button. Or you can type in the MAC Address which has been granted access by your ISP.

6.8 VLAN

A virtual local area network, or VLAN, is a group of hosts which communicate as if they were attached to the same broadcast domain, regardless of their physical location. A VLAN has the same attributes as a physical local area network (LAN), but it allows for end stations to be grouped together even if they are not located on the same network switch. Port-based VLAN function is provided in LAN-Cell 3 for users to assist with managing the LAN and WLAN groups, for example to reduce broadcast traffic that might be sent from the Ethernet LAN to Wi-Fi clients.

1. Click on [Add] to add a VLAN group.

2. Configure the VLAN group by simply checking the box to associate the group members

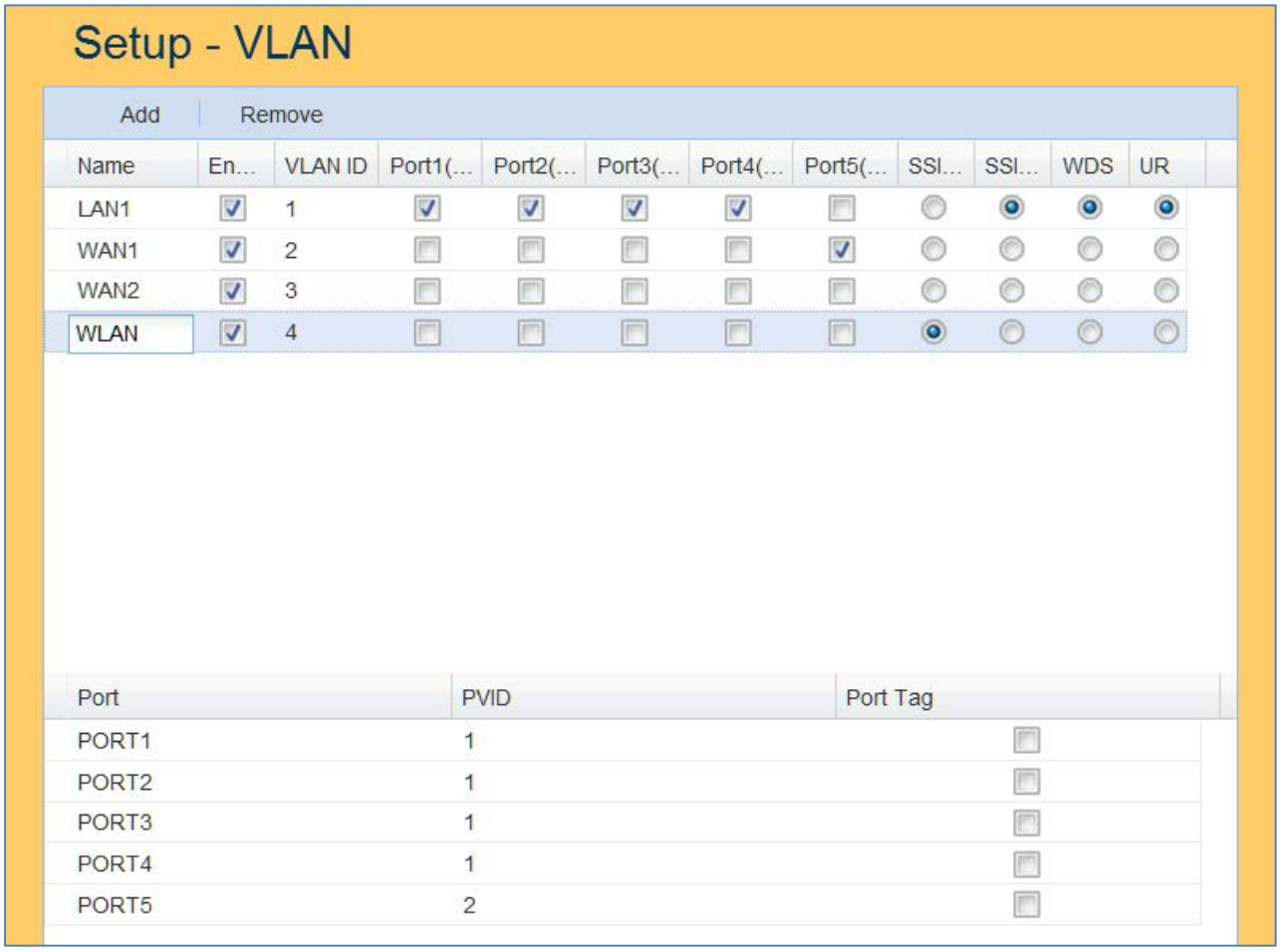


Figure 36: Setup VLANs

* A total of 16 VLAN groups can be set in the LAN-Cell 3.

** Tagged VLAN only applied to the physical ports.

*** Changing VLAN settings will cause the LAN-Cell 3 to reboot in order for the changes to take effect.

6.9 Time

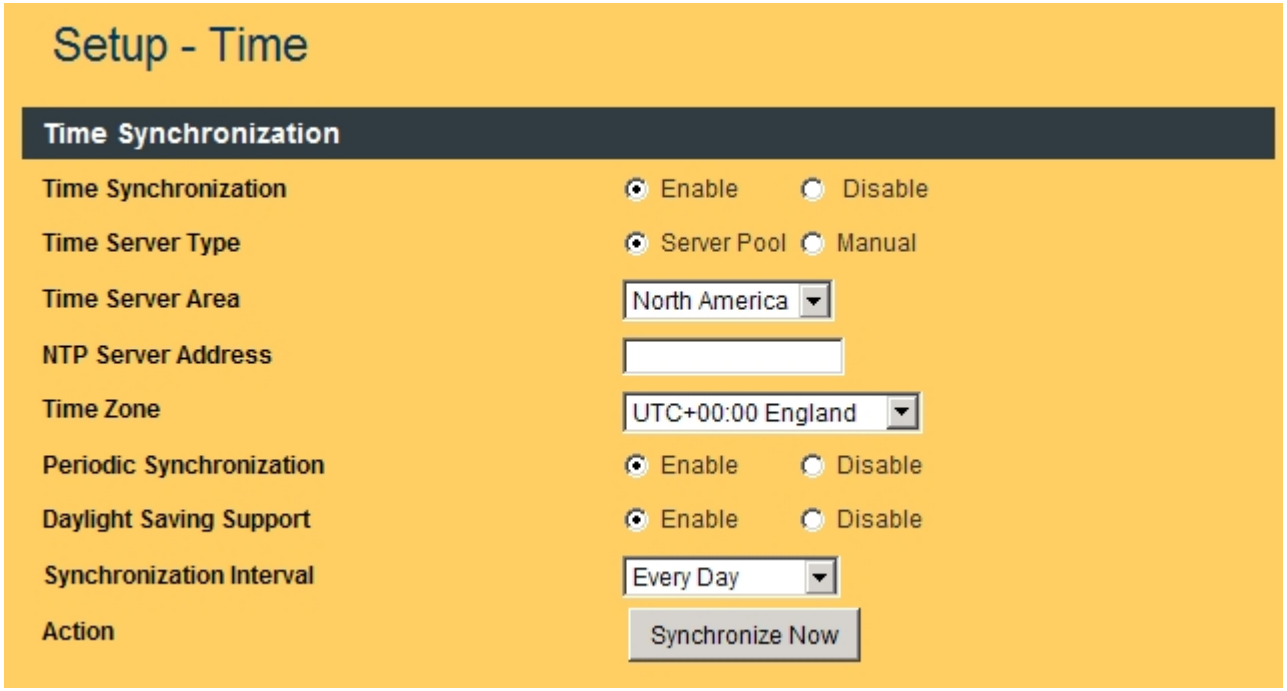


Figure 37: Setup Time Servers & Automatic Reboot

Time Synchronization	Select Enable/Disable to enable/disable Time Synchronization
Time Server Type	Select to use a pre-defined pool of time servers on the Internet or your own time server.
Time Server Area	If Server Pool is selected, choose the Time Server by location.
NTP Server Address	If Manual is selected, enter the IP address of your Time Server (NTP).
Time Zone	Select Time Zone according to your location.
Periodic Synchronization	Select Enable/Disable to enable/disable Periodic Synchronization
Daylight Savings Support	Enable/Disable automatic time adjustment for Daylight Savings Time.
Synchronization interval	Select from Every Hour, Every 6 Hours, Every 12 Hours, Every Day, and Every Week.
Action	Click the **Synchronize Now** button to contact the time server for an immediate update.

CHAPTER 7: WIRELESS (Wi-Fi) MENU

7.1 Basic Setup

The LAN-Cell 3's multiple simultaneous SSIDs provide the ability to create separate security mode and key settings for both convenience and increased protection. For example, internal users can configure their network devices to access the first SSID with the WPA2 PSK (Pre-Shared Key), while visitors can be assigned to the second SSID with a WEP key that changes periodically. In addition, the SSIDs can be isolated to prevent malicious attacks and local area network access for visitors using the second SSID. This provides an extremely convenient approach for providing access internet access for visitors while enforcing strong security protection at all times.

7.1.1 Wi-Fi Settings

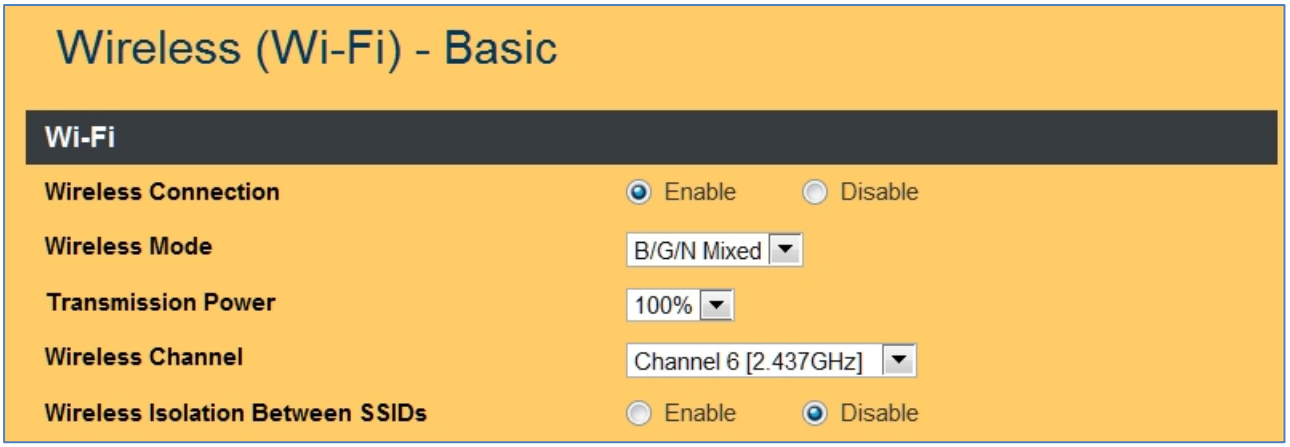


Figure 38: Setup Wi-Fi Basic

Wireless Connection	Select Enable if you would like to turn on the wireless radio. Select Disable if you would like to turn off the wireless radio.
Wireless Mode	Select the wireless mode for 802.11b/g/n or mixed use.
Transmission Power	Select the transmission power class from 10%, 25%, 50%, 75%, and 100%.
Wireless Channel	Select which Wi-Fi channel to be used. For non-US, Canada, Taiwan locations, see **Wireless > Advanced** to select the appropriate region and channel range.
Wireless Isolation Between SSIDs	Select Enable if you would like to prevent communication between the SSID's. Select Enable if you would like to allow communication between the SSID's

7.1.2 SSID Settings

Each SSID can be configured with its own attributes. Further, various security modes are available based on your needs and preference: Disable, WEP, WPA Pre-Shared Key, WPA, WPA2 Pre-Shared Key, and WPA2. However, it is important to note that all devices under the SSID must use the same security mode.

Different methods will grant different levels of security. Using encryption – where data packets are encrypted before transmission - can prevent data packets from being analyzed by un-trusted parties. However, higher the security level is, the lower the data throughput becomes.

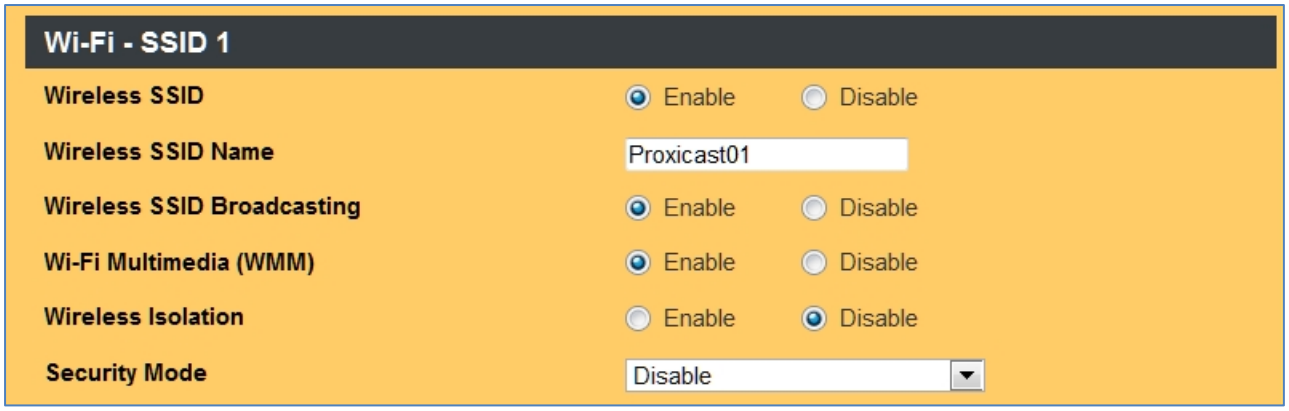


Figure 39: Wi-Fi SSID1

Wireless SSID	Select Enable if you would like to turn on this SSID. Select Disable if you would like to turn off this SSID.
Wireless SSID Name	Enter name you would like to assign to this SSID.
Wireless SSID Broadcasting	LAN-Cell 3 broadcasts SSID periodically. Select Enable to turn it on or Disable to turn it off. Enabling SSID Broadcasting makes it convenient for users to find and connect to the LAN-Cell 3. Disabling SSID broadcasting enhances the security by hiding SSID information.
Wi-Fi Multimedia (WMM)	Select Enable to prioritize different traffic types based on their characteristics. For example, VoIP or video traffic will have higher priorities over ordinary traffic.
Wireless Isolation	Select Enable if you would like to prevent access to other network devices connecting to this SSID. Select Disable if you would like to allow access to other network devices connecting to this SSID.
Security Mode	Select the desired Security Mode for this SSID and one of the following sets of additional fields will be displayed.

7.1.3 WEP

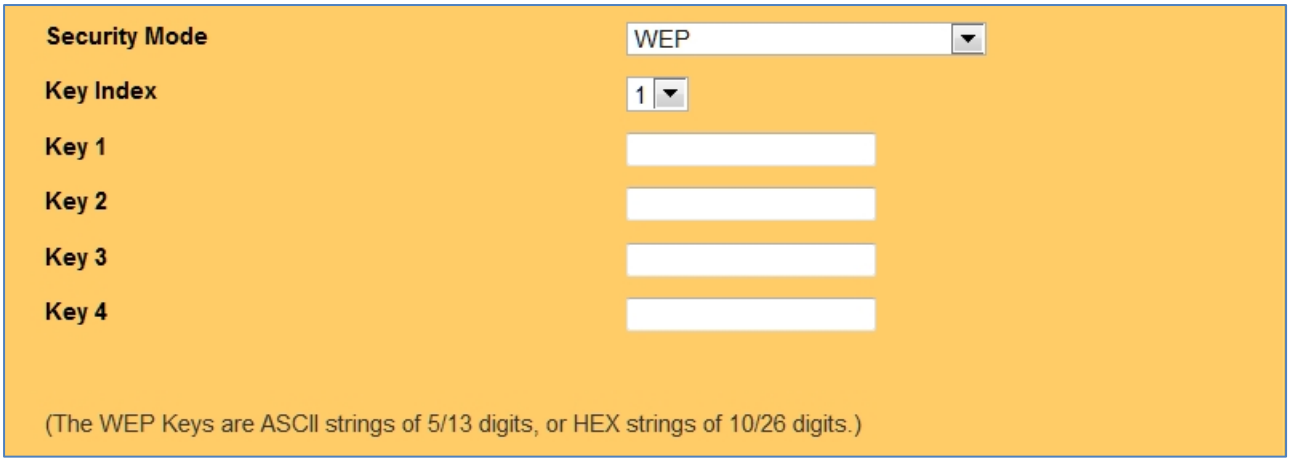


Figure 40: WEP Settings

WEP Key Index	WEP Key Index indicates which WEP key is used for data encryption.
WEP Key (1~4)	64-bit WEP: type 10 hexadecimal digits or 5 ASCII characters 128-bit WEP: type 26 hexadecimal digits or 13 ASCII characters.

7.1.4 WPA/WPA2 Pre-shared Key

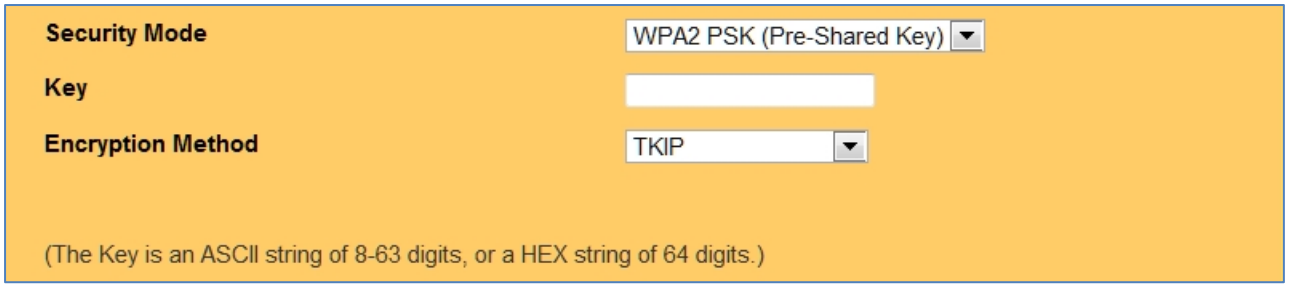


Figure 41: WPA/WPA2 PSK Settings

Key	Pre-shared Key serves as the credential for the packet encryption. This same value must be entered in all Wi-Fi devices connecting to this SSID.
Encryption Mode	TKIP & AES are supported.

7.1.5 WPA/WPA2 Radius

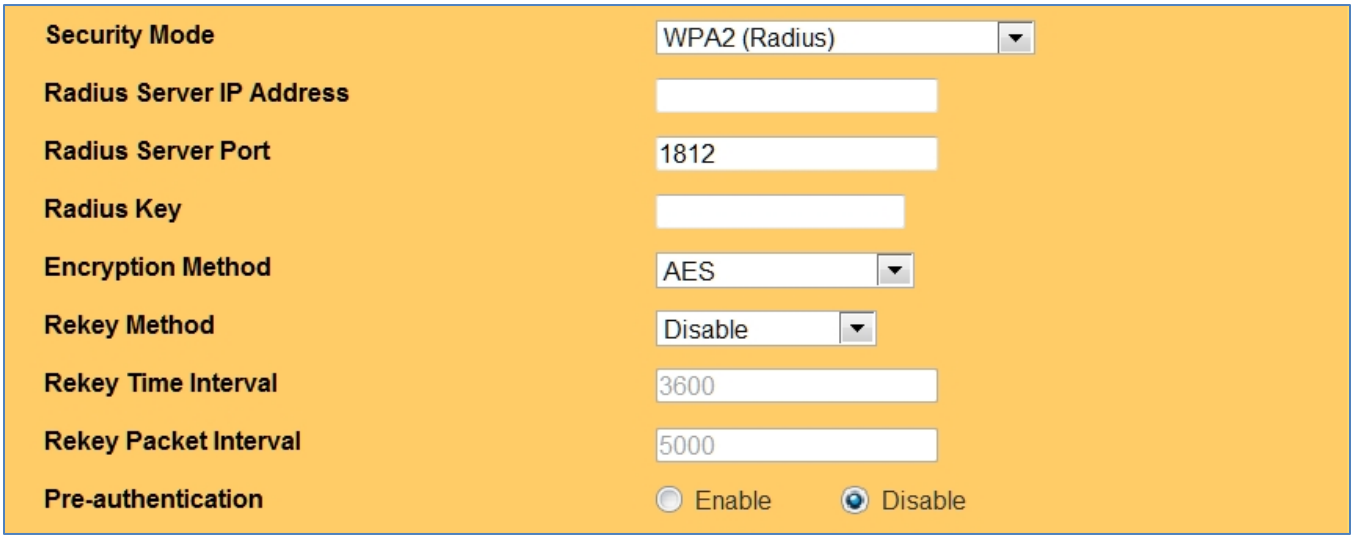


Figure 42: WPA/WPA2 Radius Settings

Radius Server IP Address	Enter the RADIUS server's IP address.
Radius Server Port	Enter the RADIUS server's port number. The default port is 1812.
Radius Key	Enter the RADIUS server's Key.
Encryption Method	Select TKIP or AES for the packet encryption.
Rekey Method	Select method for determining when new key is required.
Rekey Time Interval	Enter the frequency of key renewals in seconds.
Rekey Packet Interval	Enter the frequency of key renewals in number of packets.
Pre-authentication	Enable pre-authentication if required by your Radius server

7.1.6 SSID2 Guest LAN

Users connecting to SSID2 can be segregated into their own local area network to provide Internet service while preventing access to other devices on the primary LAN. Enter the Guest LAN starting IP address which will be assigned to the LAN-Cell, and the corresponding subnet mark. Guest Wi-Fi devices will be assigned a DHCP address in this subnet. For more flexibility in controlling guest Wi-Fi access, refer to Section 7.6: Guest Hotspot.

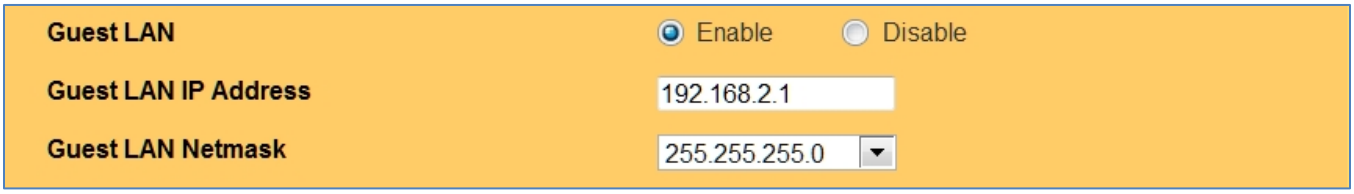


Figure 43: Wi-Fi Guest LAN

7.2 Advanced Setup

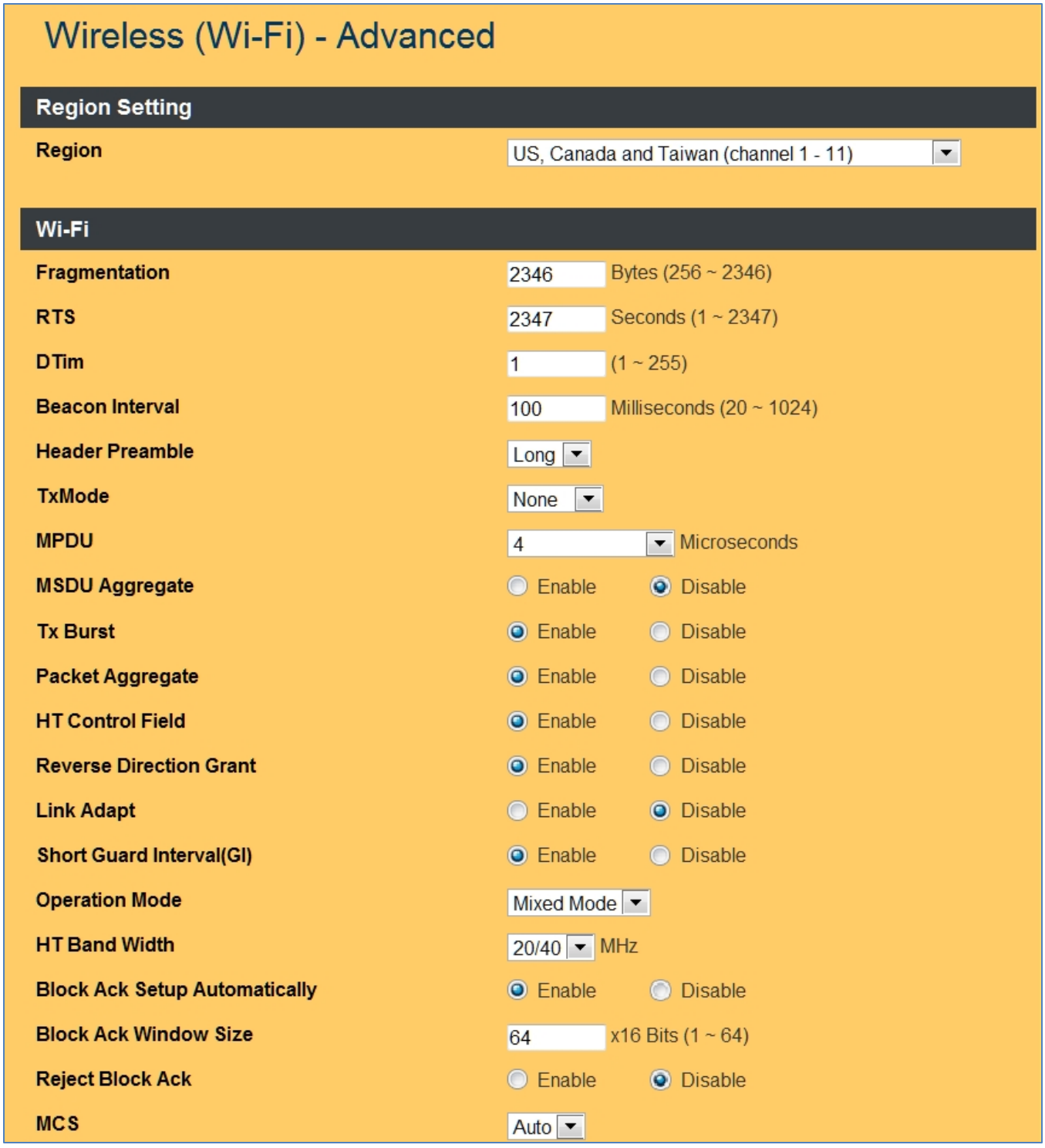


Figure 44: Wi-Fi Advanced Settings

Region	Choose the region in which the LAN-Cell is currently operating (sets channels).
Fragmentation	Enter the fragmentation bytes. The default value is 2346 bytes.
RTS	Enter the RTS seconds. The default value is 2347 seconds.
DTim	Enter the DTim seconds. The default value is 1.
Beacon Interval	Enter the interval to send a beacon. The default value is 100 milliseconds.
Header Preamble	Choose Long or Short header preamble.
TxMode	Choose different transmission mode.
MPDU	MPDU data length. The transmission rate is increased when you choose a larger number, but usually the max value will be 4 in the wireless card
MSDU Aggregate	A kind of packet aggregation method, it can improve the transmission efficiency. Please make sure you Wireless card has this function supported.
Tx Burst	Some 802.11g wireless cards support this mode. The transmission rate can be increased when this function is enabled.
Packet Aggregate	An aggregation method like A-MSDU, it can improve the transmission efficiency. Please make sure you Wireless card has this function supported.
HT Control Field	Choose Enable/Disable. It is useful when you need to debug the wireless network.
Reverse Direction Grant	Choose Enable/Disable. The response time can be shorter enable this function is enabled.
Link Adapt	Choose Enable/Disable. The function is used to dynamically change the modulation and encoding mechanism between wireless devices.
Short Guard Interval (SGI)	Choose Enable/Disable. Short GI can improve the transmission rate, but with less immunity when interference exists.
Operation Mode	Choose Mixed mode or Greenfield. You may choose Greenfield mode to increase the transmission rate when you using 802.11n wireless network only.
HT Band Width	Using HT20MHz or HT20/40MHz
Block Ack Setup Automatically	Choose Enable/Disable. If your Wi-Fi Card supports the Block Ack mechanism, it can improve the data transmission efficiency when this function is enabled.
Block Ack Window Size	Specify a Block Ack window size.
Reject Block Ack	Choose Enable to reject the request of BA from another other Wireless device.
MCS	Select transmission (connection) speed.

7.3 WDS Setup

A wireless distribution system (WDS) is a system enabling the wireless interconnection of access points in an 802.11 network. It allows a wireless network's coverage area to be expanded using multiple access points without a wired backbone to link the APs.

The LAN-Cell 3 supports 2 modes of WDS operation:

- Bridging: APs communicate only with each other and don't allow wireless clients to access them.
- Repeating: APs communicate with each other and with wireless clients.

All base stations in a wireless distribution system must be configured to use the same radio channel, method of encryption (none, WEP, or WPA) and the same encryption keys. They may be configured to different service set identifiers (SSIDs). WDS also requires every base station to be configured to forward to others in the system.

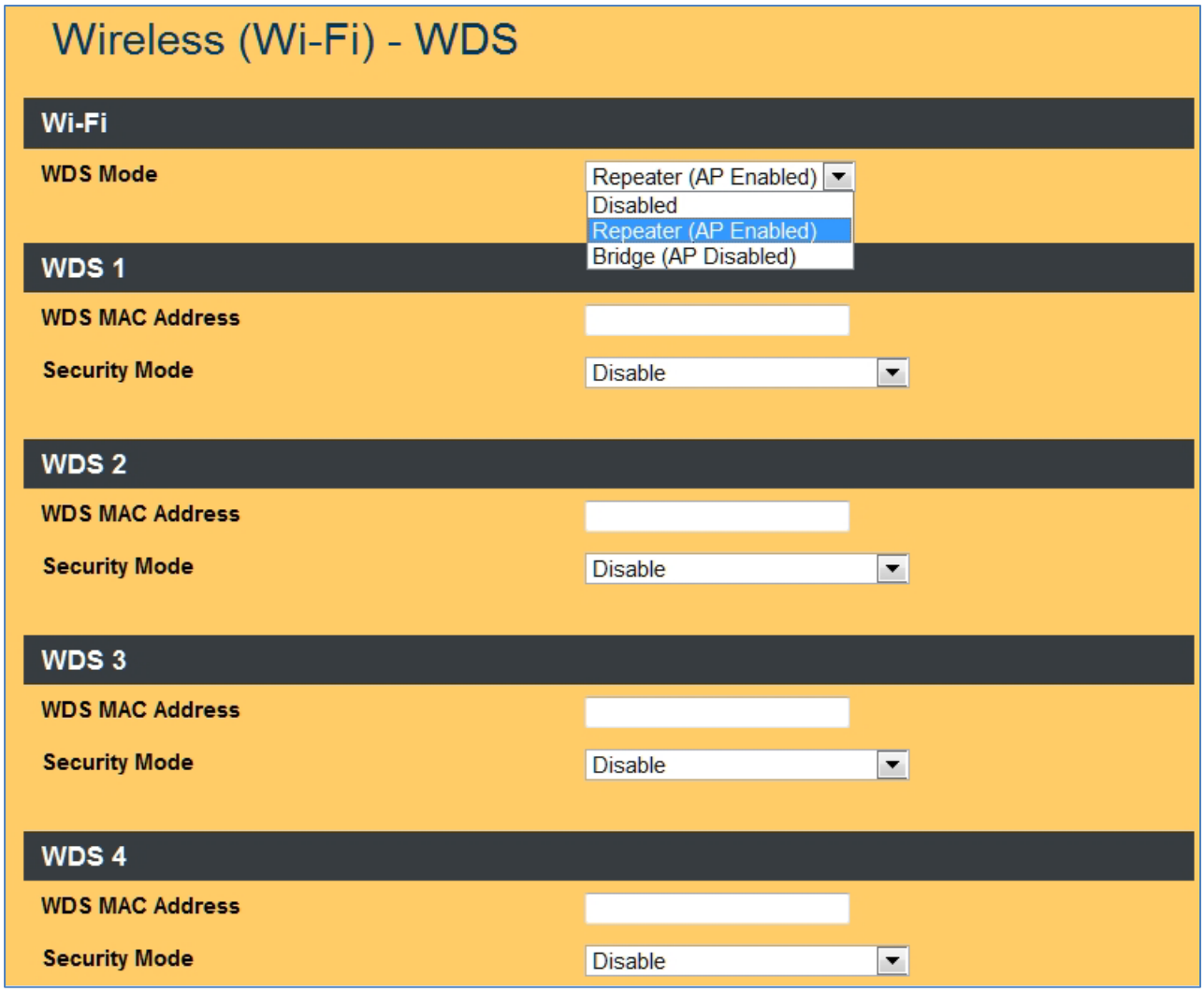


Figure 45: Wi-Fi Wireless Distribution System

WDS	Select Enable to enable WDS function. Select Disable to disable WDS function.
MAC Address [1~4]	Enter the MAC addresses of the other bridged wireless devices. Maximum of 4 devices are allowed to be bridged together.

Make sure of the following in order for WDS to work correctly:

(1) All WDS devices must use the same radio channel.

(2) All WDS devices must use the same encryption mode and encryption keys.

7.4 Universal Repeater Setup

The Universal Repeater function is similar to WDS in that it is used to essentially enlarge the area of wireless network coverage. However, unlike WDS, Universal Repeater offers simplicity in configuration requirements, as users only need to configure the current AP as a client, and to connect it to the second AP's SSID (or BSSID). However, you need to ensure that the two APs are using the same wireless channel and security mode (and key) for Universal Repeater to work correctly.

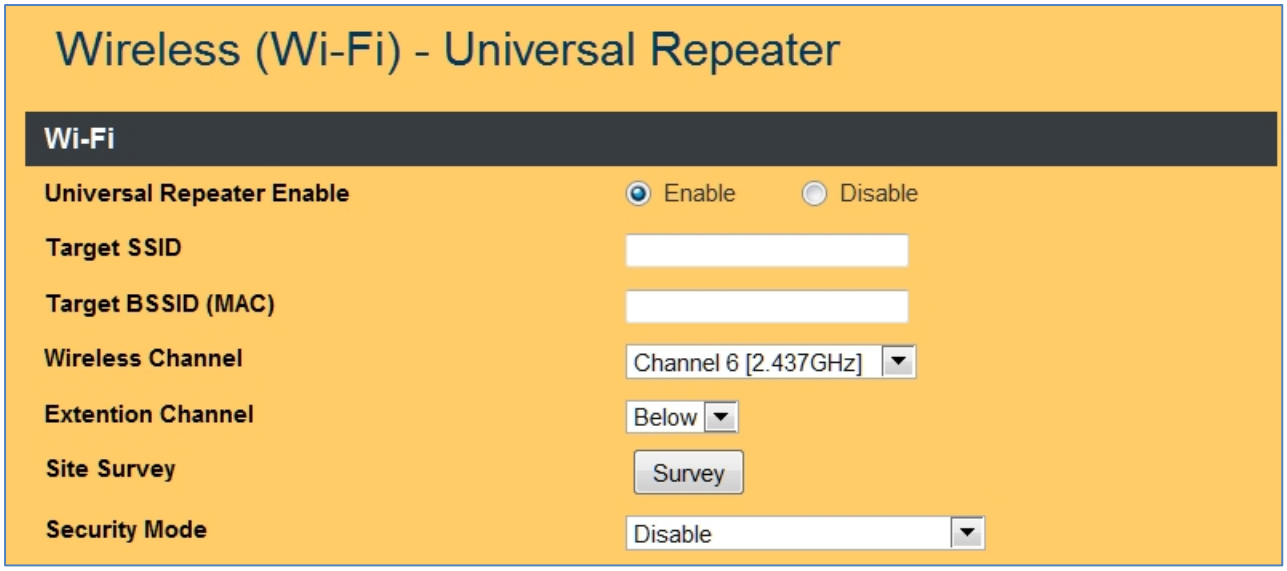


Figure 46: Wi-Fi Universal Repeater Setup

Universal Repeater	Select Enable to enable Universal Repeater. Select Disable to disable Universal Repeater.
Target SSID	Enter the target SSID to connect to.
Target BSSID (MAC)	Enter the target BSSID to connect to. The BSSID is optional if you setup the target SSID.

Security Mode	Choose the security mode the target AP uses, and enter the key if needed.
Wireless Channel	Select which Wi-Fi channel to be used. For non-US, Canada, Taiwan locations, see Wireless > Advanced to select the appropriate region and channel range.
Extension Channel	When operating in 40 MHz mode the access point will use an extended channel either below or above the current channel. Optimal selection will depend on the channels of other networks in the area.
Site Survey	Click this button to display a table of visible Wi-Fi networks. Select the desired network from the Site Survey table and the associated SSID and channel information will be automatically entered.
Security Mode	Select the Security Mode which matches the target Wi-Fi network. Enter the associated security information (such as pre-shared keys) required by the target Wi-Fi network.

7.5 WPS Setup

Wi-Fi Protected Setup (WPS) is a computing standard that allows easy establishment of a secure wireless network. Although easy to setup, WPS connections are inherently less secure than manually configured WPA/WPA2 connections. The LAN-Cell 3 supports two different types of WPS:

- PIN Method: A Personal Identification Number (PIN) is generated by the LAN-Cell. This PIN must then be entered at the "representant" of the network (other AP or client device).
- Push-Button-Method: The user simply has to push the button on the LAN-Cell 3 screen and either an actual or virtual one on the new wireless client device.

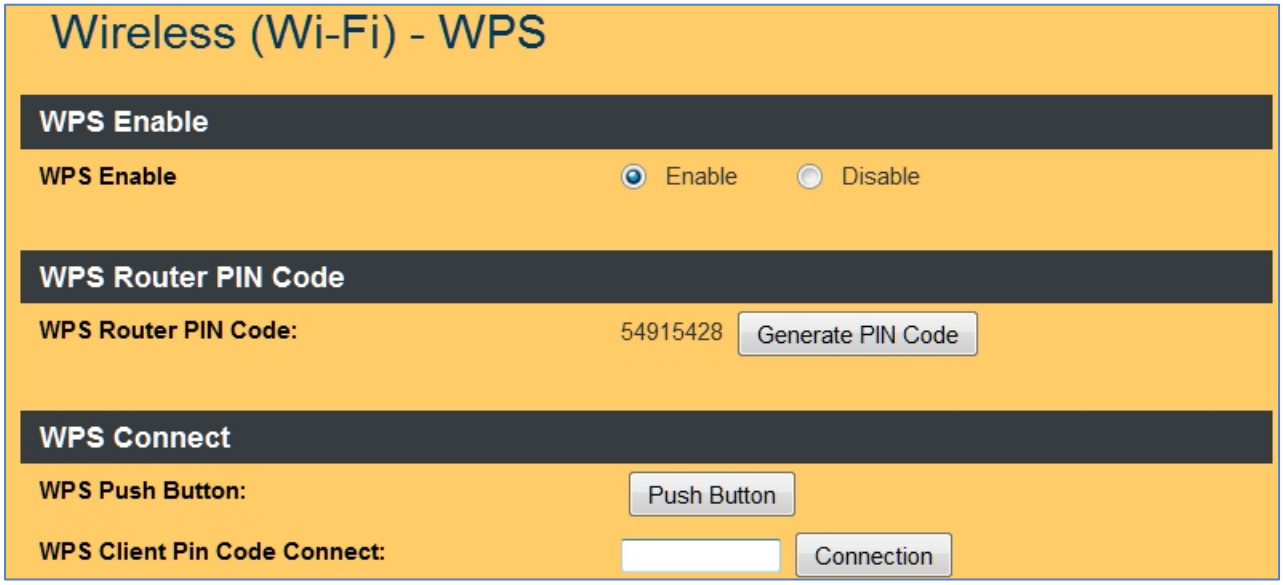


Figure 47: Wi-Fi WPS Setup

7.6 Guest Hotspot

The Guest Hotspot feature allows the LAN-Cell 3 to provide Wi-Fi access to guest wireless devices. This feature segregates the guest devices into their own subnet (like the Guest LAN feature), but also automatically redirects Wi-Fi users to a “splash” page and prevents them from accessing the Internet until they “login” to the hotspot and optionally agree to a Terms of Use.

The Guest Hotspot feature offers several additional capabilities compared to the Guest LAN feature:

- A customizable “splash” screen shown to guest users before they are allowed to access the Internet
- Optional “Terms of Use” policy agreement
- Optional username/password security for guest connections
- Optional “white list” URLs that can be accessed without authentication

Note: The Guest Hotspot feature is available in LAN-Cell 3 firmware versions 5.4.0 and later. Units upgraded to 5.4.0 or alter cannot be downgraded to firmware versions earlier than 5.4.0. Configuration files from LAN-Cell 3’s running earlier firmware versions cannot be copied to units running 5.4.0 or later (and vice-versa).

Note: To use the Guest Hotspot feature, SSID2 must be enabled and not hidden; Security Mode and Guest LAN should be disabled.

7.6.1 Guest Hotspot Setup

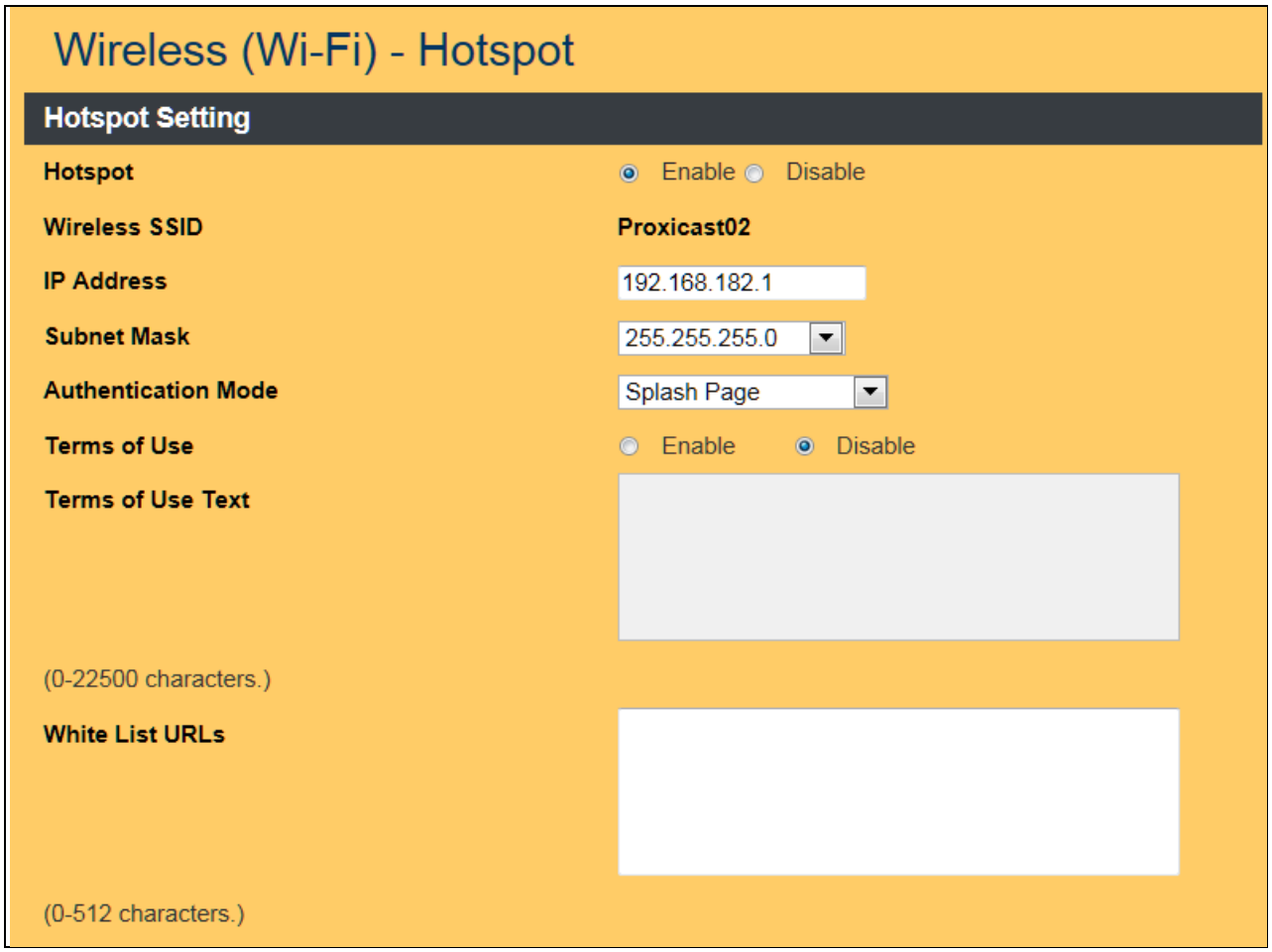


Figure 48: Guest Hotspot Setup

Hotspot	Select Enable to enable the Guest Hotspot function Select Disable to disable the Guest Hotspot function.
Wireless SSID	This is SSID #2 from the Wi-Fi Basic screen. Change SSID #2 to reflect the name to be displayed when users scan for this access point.
IP Address	Enter the IP Address to assign to the Hotspot. Guest Wi-Fi clients will be assigned a dynamic IP address starting with the next address in this subnet.
Subnet Mask	Enter the subnet mask which corresponds to the desired DHCP pool size.
Authentication Mode	**Splash Page** – redirects users to a LAN-Cell 3 generated web page which requires them to click a “login” button and optionally agree to Terms of Use. **Local User Database** – adds username/password fields to the splash page. Define allowed usernames and passwords in the table on this screen.

Terms of Use	Select Enable to add a Terms of Use link to the splash page and change the Login button text to “Login and Accept Terms”.
Term of Use Text	Text to be displayed on the Terms of Use web page. This field may contain HTML tags. **NOTE**: If pasting text from a word processor, be sure to eliminate any extended ASCII characters such as “smart quotes” or copyright/trademark symbols and replace them with their HTML equivalent.
White List URLs	List URLs (1 per line) which may be accessed without the user clicking the “login” button. Include in this list any sources of remote content (such as graphic files) which are used on the Terms of Use or Splash screens. **NOTE**: *proxicast.com* will give users access to any server in the proxicast.com domain, whereas *www.proxicast.com/graphics* would provide access only to a specific directory on the www site.

7.6.2 Hotspot Pages Setting

The default Guest Hotspot splash page layout is shown below. To change the Splash screen, select Customized and enter content into each of the fields. All fields are optional and may contain HTML tags.

Figure 49: Default Splash Screen

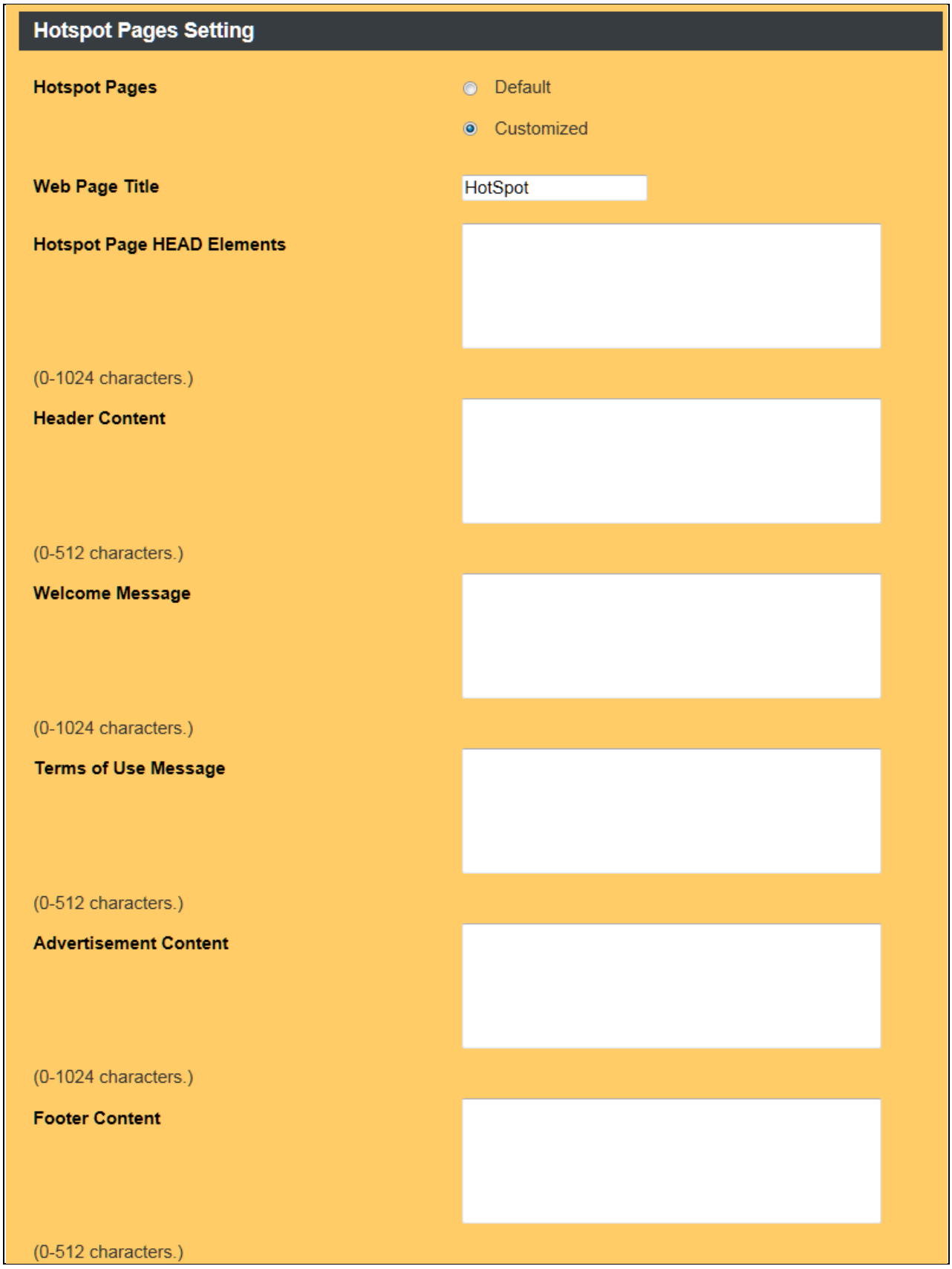


Figure 50: Hotspot Pages Setting

Web Page Title	Title text of browser's window/tab
Hotspot Page HEAD Elements	Text that will be inserted between the <HEAD> elements of the HTML splash screen. These can include CSS style definitions, javascript functions, or links to external CSS/JS files, etc. See the list of Splash screen DIV names below.
Header Content	Text shown at the top of the Splash, Terms and Success screens.
Welcome Message	Main text of the Splash screen.
Terms of Use Message	Text used to direct user's attention to the Terms of Use link.
Advertisement Content	Text below the Welcome message that can be used to display ads or any other content.
Footer Content	Text shown at the bottom of the Splash, Terms and Success screens.

The following DIV ID's are available for formatting via CSS styles on the Splash Screen. Define the desired styles in the **Hotspot Page HEAD Elements** field or in an external CSS file.

The "header", "body" and "footer" DIV ID's are repeated on the Terms of Use and Success pages.

WARNING:	A bug in Internet Explorer v9 and earlier causes IE to render any HTML entered into these fields in the router's GUI instead of displaying the raw HTML tags. Use IE10+ or a different browser to edit the Guest Hotspot page.

7.6.3 Hotspot Operation

Prior to logging in, the Wi-Fi Guest will have no access to the Internet (other than White Listed URLs). Before users can make connections with VPN clients, Android/iOS apps or other non-browser applications, they must use a web browser to access the Splash screen and login.

After logging in, the Wi-Fi Guest's browser will momentarily display a "Success" page that confirms the login and redirects the browser to the original destination web page URL.

A user can be removed from the Hotspot's authorized list by entering http://logout into their browser.

If no WAN interfaces are currently available, the Splash screen will not display - the browser will timeout.

By default. Hotspot traffic will be forwarded to any available WAN interface. To force Hotspot traffic to use only a specific WAN interface, add the Hotspot subnet to the Security>IP Access Control list as "allow" for the desired WAN and "deny" for the other WAN interface.

CHAPTER 8: SECURITY MENU

8.1 Firewall

The LAN-Cell 3 has several firewall-related security features designed to protect LAN devices from unwanted access and attack from WAN (and even other LAN) connections. By default, these WAN protections are enabled and all “inbound” connections from WAN devices are blocked, except for TCP Port 8080 which is used by the LAN-Cell 3’s web management interface. The LAN-Cell 3 will automatically open other ports for inbound access as you define VPN, Port-Forwarding, and Virtual Host rules (see the Applications menu). You do not need to explicitly define firewall rules for remote access purposes.

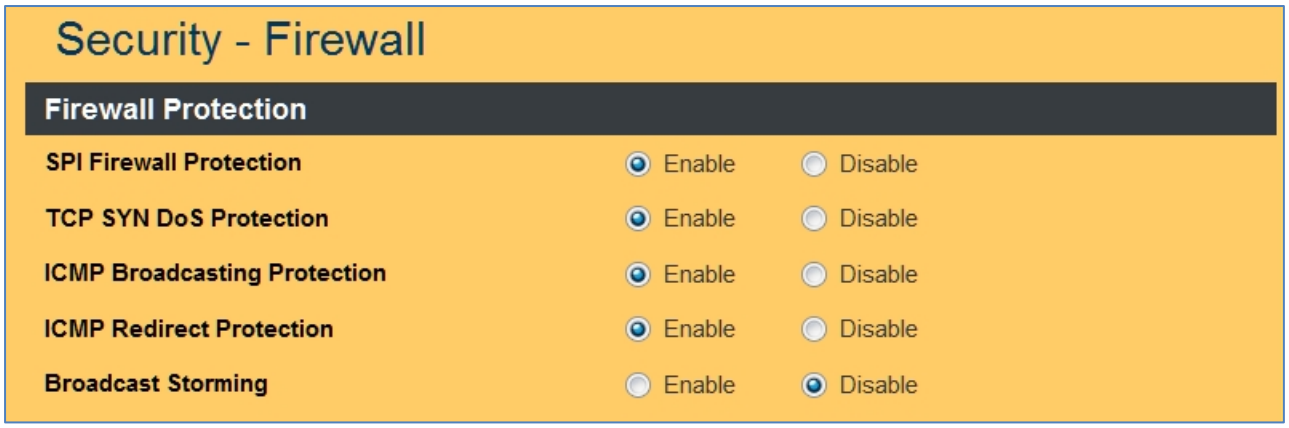


Figure 51: Firewall Setup

SPI Firewall Protection	Select Enable to enable SPI Firewall Protection. Select Disable to disable SPI Firewall Protection.
TCP SYN DoS Protection	Check to enable TCP SYN DoS Protection. Uncheck to disable TCP SYN DoS Protection. TCP SYN DoS attack sends a flood of TCP/SYN (connection requests), causing the LAN-Cell to consume computing resources (e.g. memory, CPU) to reply and continuously wait for the incoming packets. The LAN-Cell 3 is able to detect TCP SYN DoS attacks and limit the resource consumption by lowering the incoming request rate by fast recycling of the resource. Therefore, the LAN-Cell 3 is still able to serve normal traffic while it is under such an attack.

ICMP Broadcasting Protection	Check to enable ICMP Broadcasting Protection. Uncheck to disable ICMP Broadcasting Protection. ICMP broadcasting attack is a type of DoS attacks. A flood of ICMP broadcasting packets is generated and sent to LAN-Cell 3. Consequently, this LAN-Cell will experience a high number of interruptions and consumption of computing resources. The LAN-Cell 3 is able to stop responding to ICMP broadcasting echo packets in order to avoid a potential ICMP broadcasting DoS attack.
ICMP Redirect Protection	Check to enable ICMP Redirect Protection. Uncheck to disable ICMP Redirect Protection. An ICMP redirect message is a way to change the existing routing path. Generally, ICMP redirect packets should not be sent, and so when there is the occurrence that ICMP redirect packets are sent, it is important to note that it is very likely to be used as a means for a network attack.
Broadcast Storming	Check to enable Broadcast Storm Protection. Check to disable Broadcast Storm Protection. A broadcast storm is a situation in which messages are broadcast on a network, and each message prompts a receiving node to respond by broadcasting its own messages on the network that in turn prompt further responses, and so on. This snowball effect can have a serious negative impact on network performance. See also Spanning Tree Protocol to reduce broadcast loops on the LAN.

8.2 IP Access Control

IP Access Control is used to either allow or deny specific types of “outbound” connections from specific LAN IP addresses. Each rule defines a custom Access Control List (ACL) that the LAN-Cell 3 uses to determine if a packet is to be routed or not. By default, the LAN-Cell 3 allows all LAN devices to connect to all external ports on any WAN interface.

Outbound IP Access Control rules are typically used to limit end-user access to one or more Internet services that have been deemed an inappropriate use of the WAN connection. The rules can also be used to create routing policies that force specific types of traffic to flow through specific WAN interfaces (e.g. all E-Mail must go through the Ethernet WAN only).

8.2.1 IP ACL Settings

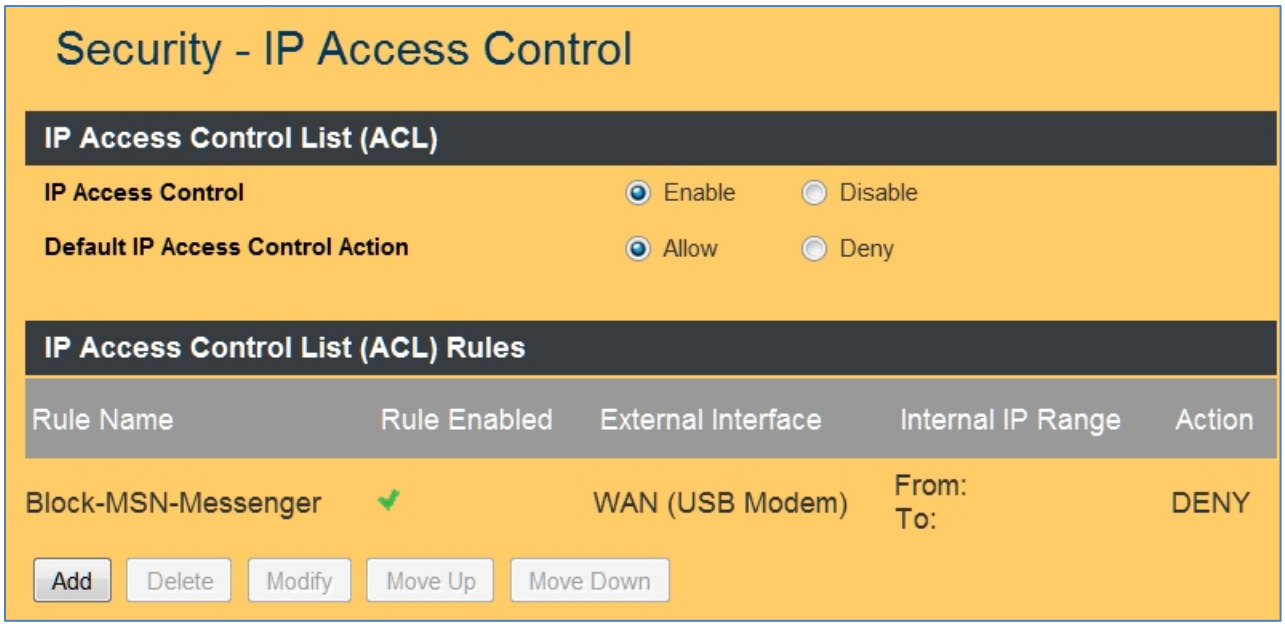


Figure 52: IP Access Control Setup

IP Access Control	Select Enable to enable ACL. Select Disable to disable ACL.
Default IP Access Control Action	Check Allow to allow LAN devices to communicate with the WAN interfaces except for the ACL rules (deny rules) defined in the table below. Check Deny to prevent LAN devices from communicating with the WAN interfaces except for the ACL rules (permit rules) defined in the table below.

8.2.2 ACL Rules

Click on the [Add] button to display the following screen:

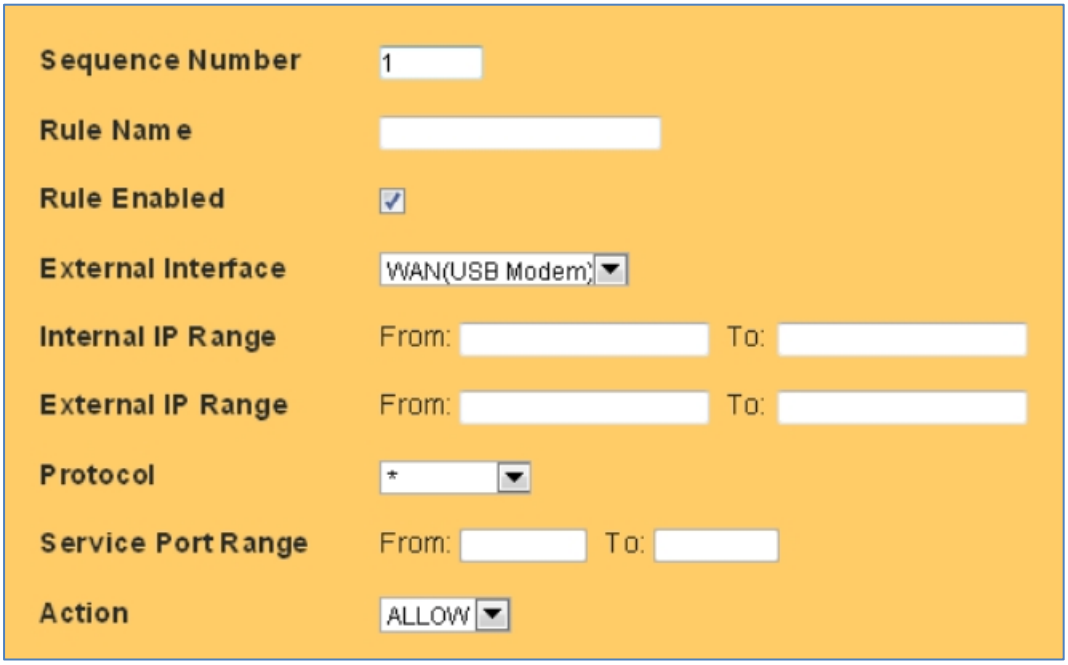


Figure 53: IP ACL Rule Setup

Sequence Number	This defines the sequence of the ACL rules. Packets are matched against the rules in the order displayed until a match is found.
Rule Name	Name of the ACL rule. No spaces are permitted.
Rule Enable	Enable/Disable this ACL rule
External Interface	Please select which External Interface (USB WAN or Ethernet WAN) you want a packet to go through, IF the packet fits the condition of this ACL rule. Select "*" to allow the LAN-Cell to determine the best available WAN interface to use.
Internal IP Range	Set up the internal IP range for this ACL rule. Only packets from devices in this range will be filtered by this rule. Leave blank to apply to all LAN devices.
External IP Range	Set up the external IP range for this ACL rule. Only packets destined for IP addresses in this range will be filtered by this rule. Leave blank to have this rule apply to all non-LAN addresses.
Protocol	Set up the protocol (TCP or UDP or both) for the ACL to be enabled. Select "*" to apply this rule to all packet types.
Service Port Range	Set up the Service Port Range (e.g., HTTP is TCP/80) for the ACL to be enabled. Leave blank to apply this rule to all ports.
Action	Select whether the LAN-Cell should ALLOW / DENY packets which match this rule.

8.2.3 IP ACL Rule Example

Assume for example that a company does not wish to allow employees to use the MSN Windows Live Messenger system over the USB WAN interface. The LAN-Cell 3 administrator can set up an ACL Deny action rejecting the traffic going out to the external IP address range used by MSN.

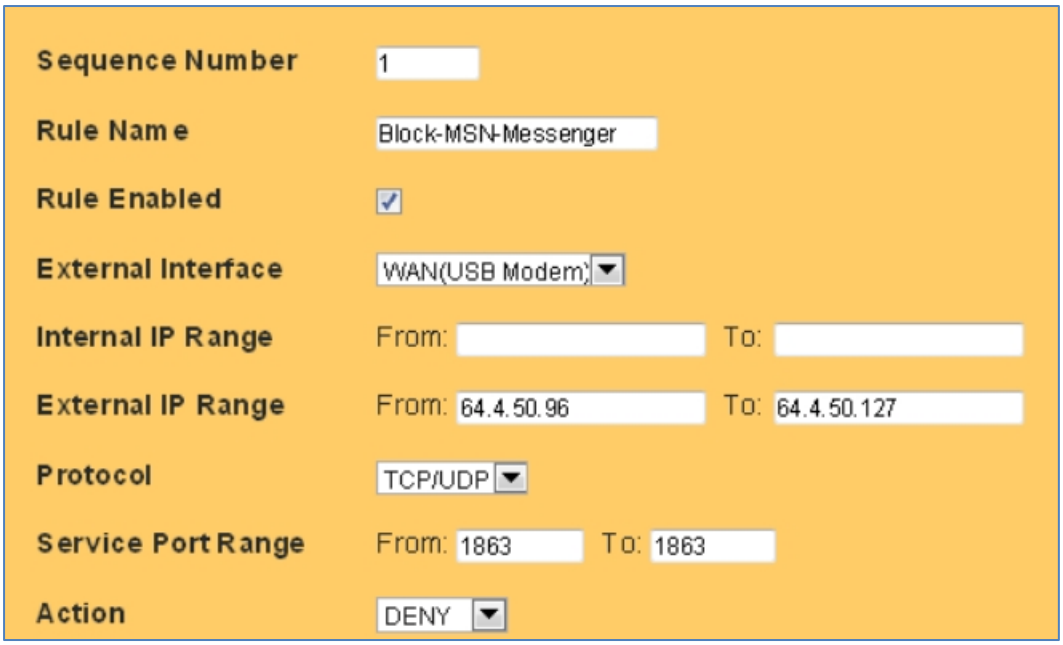


Figure 54: MSN ACL Example

Rule Name	Block-MSN-Messenger
Rule Enable	Enable
External Interface	WAN (USB Modem)
Internal IP Range	*{blank}* (applies to all LAN devices)
External IP Range	64.4.50.96 to 64.4.50.127 (IP address range for MSN server)
Protocol	TCP/UDP
Service Port Range	1863 (MSN port)
Action	DENY

8.3 Outbound MAC ACL

Similar to IP Access Control, Outbound MAC ACL Control is used to either allow or deny specific devices identified by their unique Media Access Control (MAC) addresses from making “outbound” connections. The MAC rules also enable you to “statically” assign an IP address from the LAN-Cell 3’s DHCP pool to a specific MAC address.

8.3.1 MAC ACL Settings

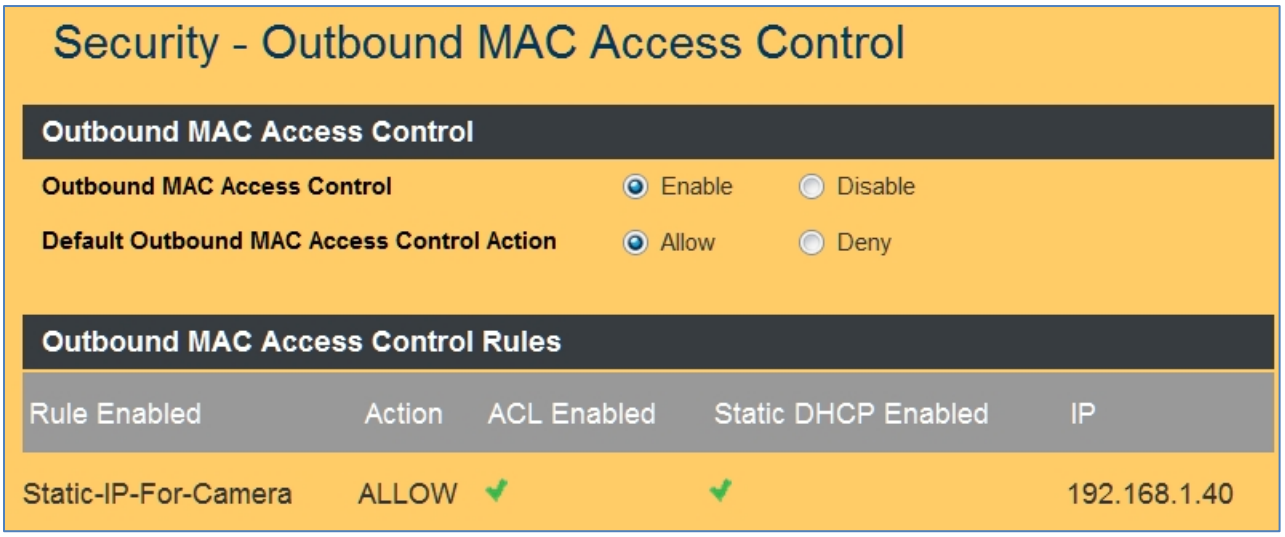


Figure 55: Outbound MAC Address Control Setup

Outbound MAC Access Control	Choose Enable/Disable to enable/disable MAC Access Control
Default Outbound MAC Access Control Action	The default ACL action of the ACL rules. When you add the individual rules, they can be viewed as exceptions and take effect relative to the default action.

8.3.2 MAC ACL Rules

Click on the [Add] button to display the following screen:

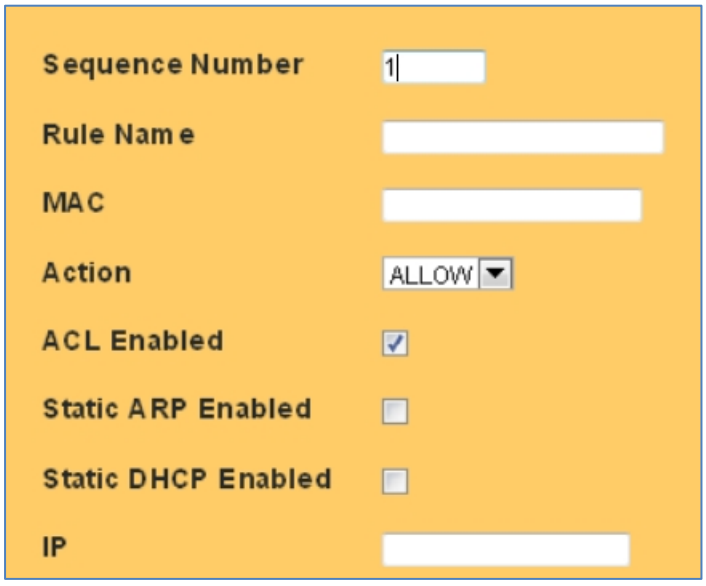


Figure 56: MAC ACL Rule Setup

Sequence Number	This defines the sequence (priority) of all the MAC ACL actions.
Rule Name	Name of the MAC access rule. Spaces are not allowed.
MAC	Set up the MAC Address to which you would like to enable the MAC ACL action. Format the MAC address as: 00:00:00:00:00:00
Action	Select whether the LAN-Cell should ALLOW / DENY packets matching this rule.
ACL Enabled	Enable/Disable this MAC access rule.
Static ARP Enabled	Enable/Disable this Static ARP rule.
Static DHCP Enabled	Enable/Disable this Static DHCP rule.
IP	The IP address to assign via static ARP or static DHCP. The address must be within the DHCP pool configured for the LAN-Cell and the DHCP Server feature must be enabled.

8.3.3 MAC ACL Rule Example

Assume that you have an IP camera that only accepts DHCP addresses and you need to assign it a static IP address (192.168.1.40) so that it can be remotely accessed.

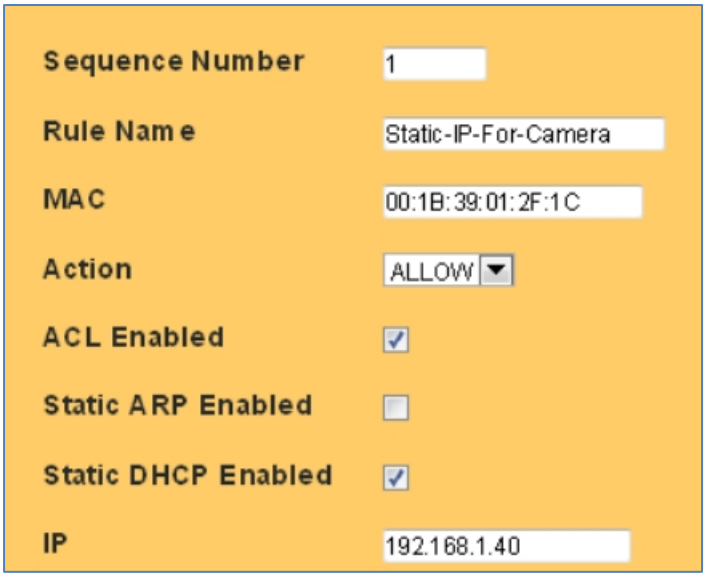


Figure 57: MAC ACL Rule Example

Sequence Number	1
Rule Name	Static-IP-For-Camera
MAC	00:1B:39:01:2F;1C
Action	Allow
ACL Enable	Enable
Static ARP Enabled	Disabled
Static DHCP Enabled	Enable
IP	192.168.1.40

8.4 OpenDNS

OpenDNS is a leading provider of security and infrastructure services including integrated Web content filtering, anti-phishing and DNS. OpenDNS services can secure networks from online threats and enforce Internet-use policies. Please refer to http://www.opendns.com for more information and to establish an account.

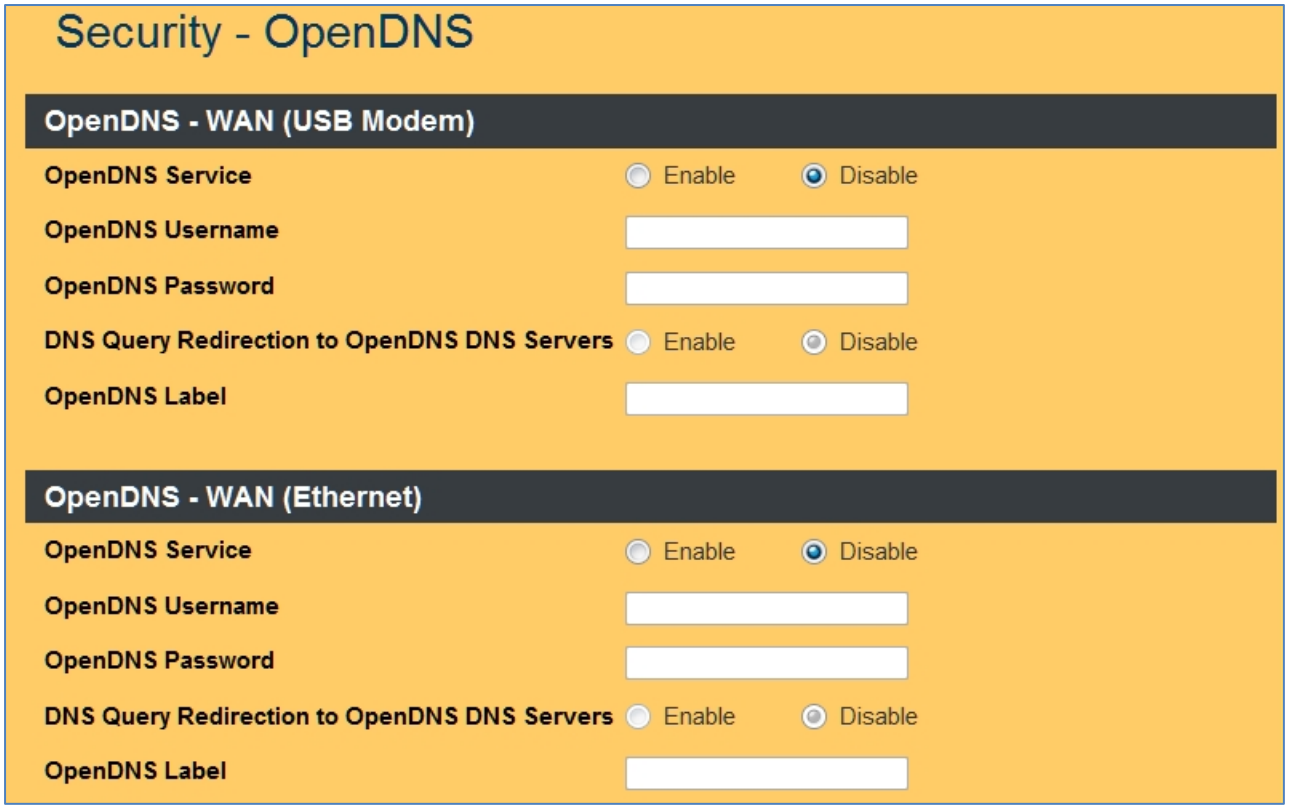


Figure 58: OpenDNS Settings

OpenDNS Service	Choose Enable/Disable to enable/disable OpenDNS
OpenDNS Username	Enter your OpenDNS user name.
OpenDNS Password	Enter your OpenDNS password.
DNS Query Redirection to OpenDNS DNS Servers	Choose Enable/Disable to enable/disable the data flow redirect to the OpenDNS Server. Users can get advanced content filtering function through this setting.
OpenDNS Label	Enter the OpenDNS Label.

8.5 Web Filtering

Web filtering allows the LAN-Cell 3 administrator to restrict access to various web resources based on keywords as well as to restrict certain types of potentially dangerous web page content such as ActiveX and Java.

8.5.1 Web Filtering Setup

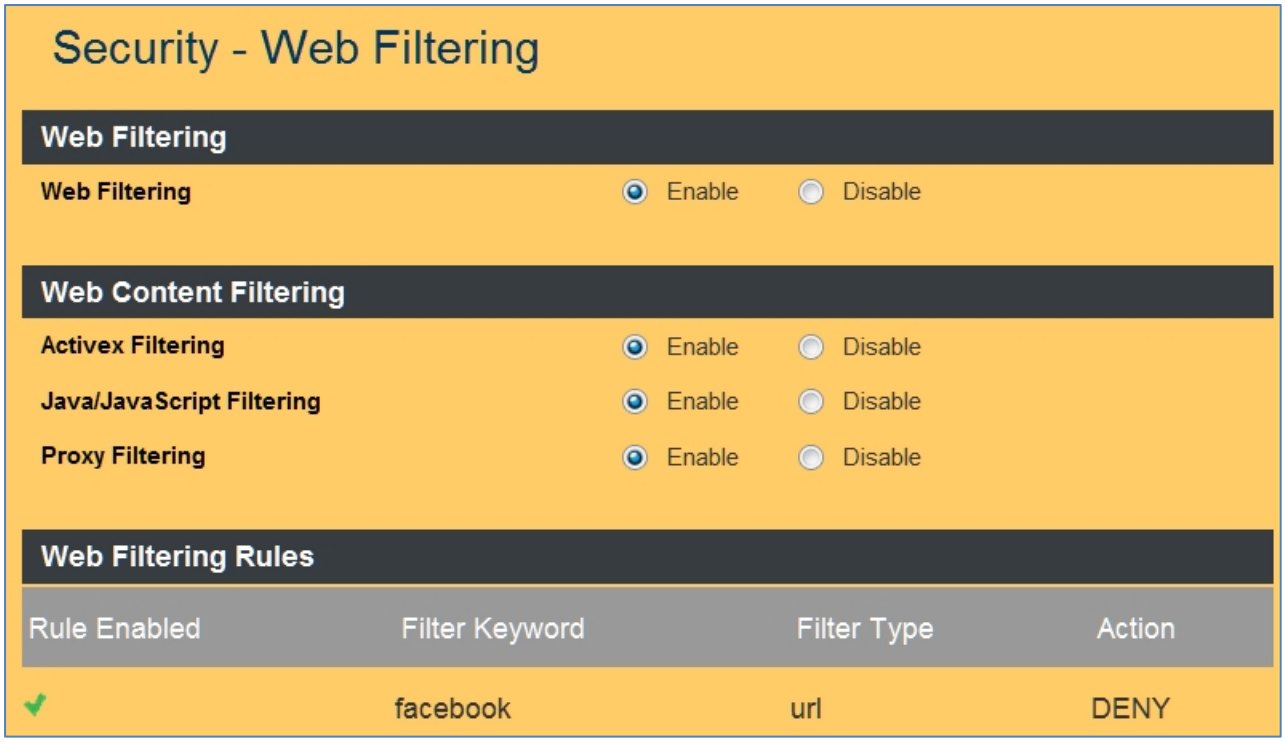


Figure 59: Web Filtering Settings

Web Filtering	Choose Enable/Disable to enable/disable Web Filtering
ActiveX Filtering	Choose Enable/Disable to enable/disable ActiveX Filtering
Java/JavaScript Filtering	Choose Enable/Disable to enable/disable Java/JavaScript Filtering
Proxy Filtering	Choose Enable/Disable to enable/disable Proxy Filtering

8.5.2 Added Web Filtering Rules

Click on the [Add] button to display the following screen:

Figure 60: Add Web Filtering Rule

Sequence Number	This defines the sequence (priority) of all the Web Filtering rules
Rule Enable	Choose Enable/Disable to enable/disable this Web Filtering rule
Filter Keyword	Enter the Keyword
Filter Type	Choose URL or Sever
Action	Select ALLOW / DENY

8.5.3 Web Filtering Rule Example

To block access to Facebook web pages, enter the following settings:

Figure 61: Web Filtering Rule Example

8.6 VPN / PPTP

The Point-to-Point Tunneling Protocol (PPTP) is a method for implementing virtual private networks. PPTP uses a control channel over TCP and a GRE tunnel operating to encapsulate PPP packets. The PPTP settings in this section define the parameters and user access rules when the LAN-Cell 3 is acting as a PPTP “server” allowing connections from remote PPTP clients such as Windows PC’s. The LAN-Cell 3 can also act as a PPTP “client” – see the PPTP section under each WAN interface.

8.6.1 VPN / PPTP Settings

Figure 62: PPTP VPN Settings

PPTP	Choose Enable/Disable to enable/disable the PPTP Server.
MTU	Enter MTU value. The default value is 1482 bytes.
VPN Start IP Address	Enter the VPN start IP address. The default value is 192.168.39.1.
Max VPN Clients	Enter the max number of VPN clients allowed.
Auto DNS	Choose Enable/Disable to enable/disable Auto DNS.
DNS	Enter the DNS server if you chose Disable for Auto DNS.
CHAP Enable	Choose Enable/Disable to enable/disable CHAP for VPN authentication.
MSCHAP Enable	Choose Enable/Disable to enable/disable MSCHAP for VPN authentication.
MSCHAP v2 Enable	Choose Enable/Disable to enable/disable MSCHAP v2 for VPN authentication.
MPP128 Enable	Choose Enable/Disable to enable/disable MPP128 encryption.
Proxy ARP Enable	Choose Enable/Disable to enable/disable Proxy ARP.
NAT Enable	Choose Enable/Disable to enable/disable NAT.

8.6.2 Add VPN / PPTP User Rule

Click on the [Add] button to display the following screen:

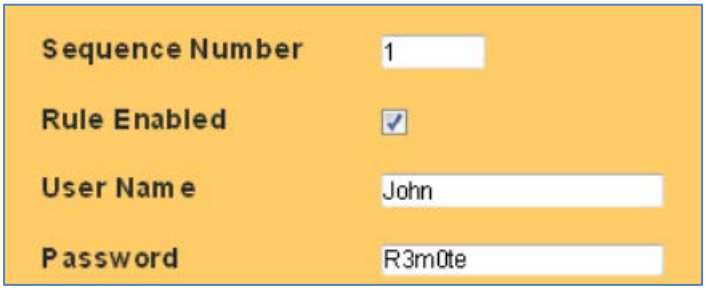


Figure 63: Add PPTP VPN User

Sequence Number	This defines the sequence of the PPTP rules.
Rule Enable	Enable/Disable this PPTP rule
User Name	Enter PPTP user name.
Password	Enter PPTP password.

8.7 VPN / IPsec

Internet Protocol Security (IPsec) is a standards-based protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session. IPsec also includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys to be used during the session.

IPsec is an extremely popular and robust end-to-end security scheme operating in the Internet Layer of the Internet Protocol Suite. It can be used to protect data flows between a pair of security gateways (Net-to-Net Mode), or between a security gateway and a remote device (Remote User Mode). The LAN-Cell 3 supports both modes and is interoperable with a wide variety of IPSec-compliant software and hardware products from numerous vendors.

When configuring an IPSec VPN connection, keep the following in mind:

- All VPN parameters much match EXACTLY between the 2 devices.
- It is helpful can have simultaneous access to the parameter and log screens of both devices during setup and testing.
- The network on the LAN side of the LAN-Cell and on the “private” side of your other VPN equipment must be on different subnets.
- Most users find it easiest to configure net-to-net VPNs if both end-points have static public IP addresses. Contact your ISP or cellular network operator to determine if static IP addresses are available. Otherwise, you will need to define a Dynamic DNS hostname for your LAN-Cell that has a dynamic IP address.
- The LAN-Cell can be either the VPN initiator or responder for net-to-net VPNs. It is the responder for Remote User VPNs.
- All intervening network hardware between the VPN end-points must support IPSec VPN pass-through and allow ESP (encrypted, Type 50) packets in addition to IKE and NAT-T requests on UDP ports 500 & 4500.
- Proxicast IPSec VPN Client for Windows is the easiest way to configure a remote user VPN tunnel on a Windows PC. A fully-functional 30 day evaluation copy can be downloaded from the Proxicast web site.
- Additional LAN-Cell VPN configuration examples are available on the Proxicast Support web site in the TechNotes and Knowledgebase areas.

8.7.1 VPN / IPsec Settings

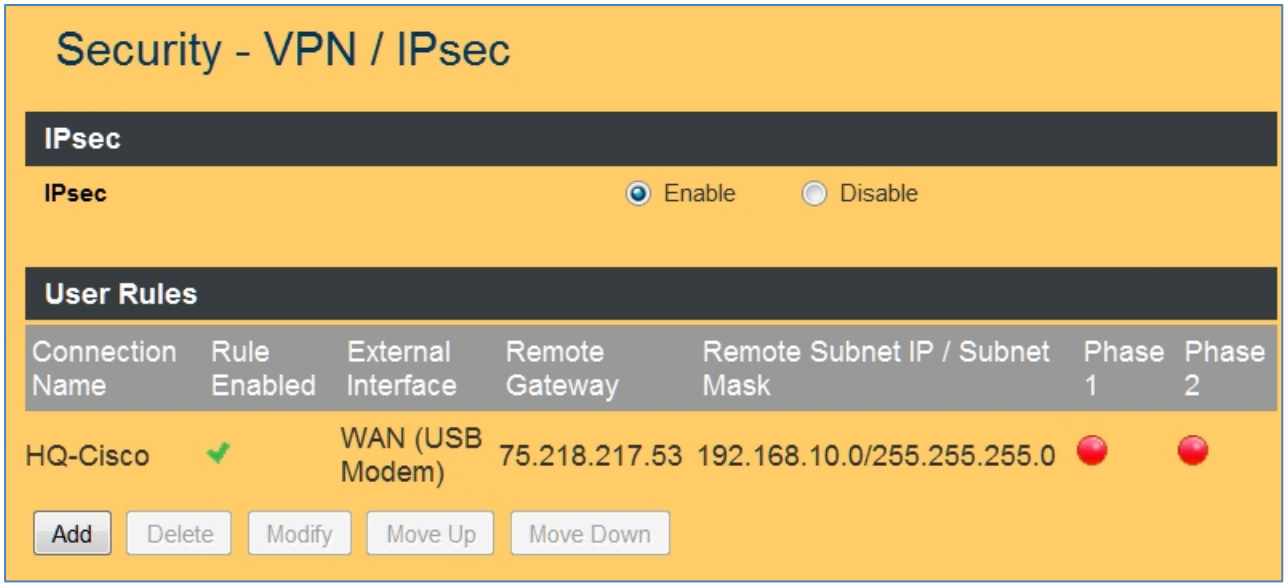


Figure 64: IPSec VPN Settings

IPsec	Select Enable/Disable to enable/disable IPsec.

8.7.2 Add VPN / IPsec Net-to-Net Rule

In this example, a Net-to-Net VPN connection will be established between an existing VPN concentrator on the Headquarters network and a LAN-Cell 3 at a remote office location.

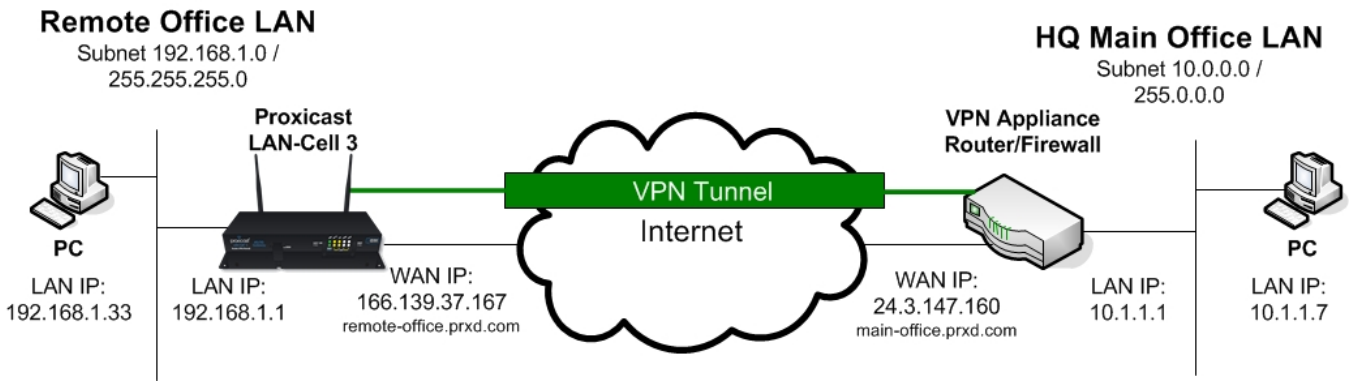


Figure 65: Net-to-Net IPSec Example

Click on the [Add] button to display the following screen:

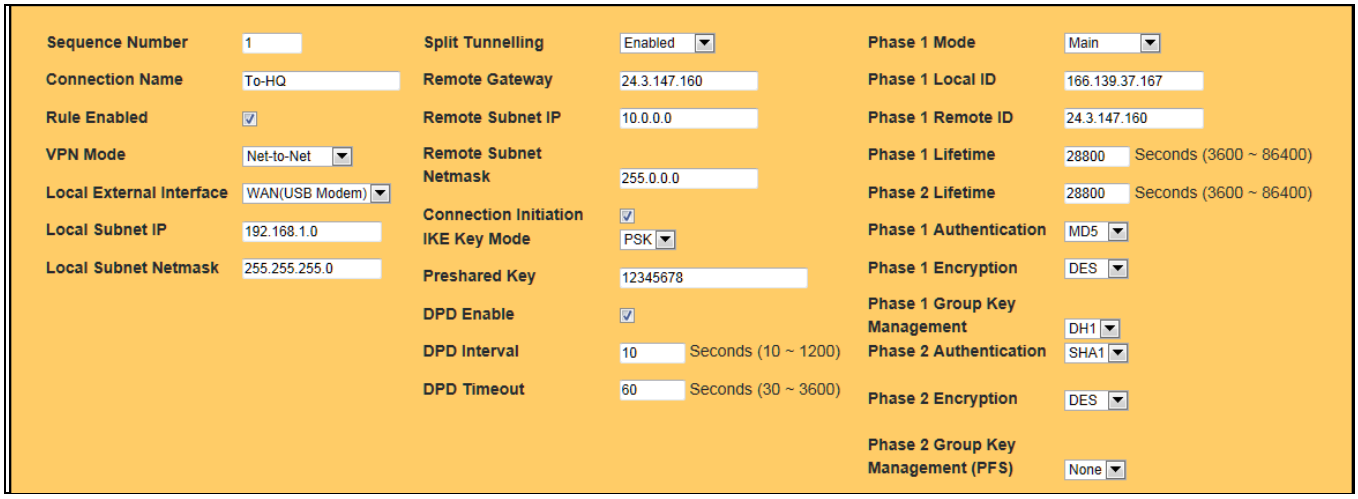


Figure 66: IPSec Net-to-Net VPN Settings

Sequence Number	This defines the sequence of the IPsec rules.
Connection Name	Name of the IPsec rule. Spaces are not permitted.
Rule Enable	Enable/Disable this IPsec rule
VPN Mode	Net-to-Net or Remote-User
Local External Interface	Choose the external WAN for this IPSec rule to use.
Local Subnet IP	Enter the subnet IP address on the LAN-side of the local LAN-Cell which will be visible to the remote VPN subnet.
Local Subnet Netmask	Enter the netmask for the local VPN gateway.
Split Tunnelling	**Enabled** = Traffic can flow to Internet addresses outside of IPSec tunnel (default). **Initiator** = The LAN-Cell 3 directs all traffic into the IPSec tunnel. The VPN device on the other side is responsible for routing the traffic to its final destination. **Responder** = The LAN-Cell 3 receives traffic from another VPN device which is forwarding all traffic through the VPN tunnel.
Remote Gateway	Enter the IP address or domain name of the remote VPN gateway. This option is required in Net-to-Net mode.
Remote Subnet IP	Enter the subnet IP address of the remote VPN gateway. This option is required in Net-to-Net mode.
Remote Subnet Netmask	Enter the subnet netmask of the remote VPN gateway. This option is required in Net-to-Net mode.
Connection Initiation	Check to force the LAN-Cell to always attempt to initiate a VPN connection to the

	remote gateway. If uncheck, the VPN will not be established unless the remote gateway initiates a connection or traffic on the local LAN subnet is destined for the remote subnet.
IKE Key Mode	At this time, only Pre-Shared Key (PSK) is supported.
Preshared Key	Enter the preshared key. The key should be at least an 8-digit ASCII string.
DPD Enable	Enable/disable Dead Peer Detection (DPD).
DPD Interval	Enter the number of seconds between checks for a dead peer.
DPD Timeout	Enter the number of seconds to wait for a response before declaring the peer dead.
Phase 1 Mode	Select Main or Aggressive Mode. Must match the setting on the remote gateway.
Phase 1 Local ID	Enter the phase 1 Local ID.
Phase 1 Remote ID	Enter the phase 1 Remote ID.
Phase 1 Lifetime	Enter the phase 1 lifetime. This value is between 3600 and 86400 seconds.
Phase 2 Lifetime	Enter the phase 2 lifetime. This value is between 3600 and 86400 seconds.
Phase 1 Authentication	Choose the phase 1 authentication as MD5 or SHA1.
Phase I Encryption	Choose the phase 1 encryption as DES, 3DES or AES.
Phase 1 Group Key Management	Choose the phase 1 group key management as DH1, DH2 or DH5.
Phase 2 Authentication	Choose the phase 2 authentication as MD5 or SHA1.
Phase 2 Encryption	Choose the phase 2 encryption as DES, 3DES or AES.
Phase 2 Group Key Management (PFS)	Choose the phase 2 group key management as DH1, DH2 or DH5. This setting is also known as Perfect Forward Secrecy.

8.7.3 Add VPN / IPsec Remote User Rule

In this example, a Remote User VPN connection will be established between with the LAN-Cell 3 functioning as the VPN Server and remote PC as the client using the Proxicast IPSec VPN Client for Windows software. The LAN-Cell has a dynamic IP address but can be accessed via its dynamic DNS name *001B39123456.proxidns.com*.

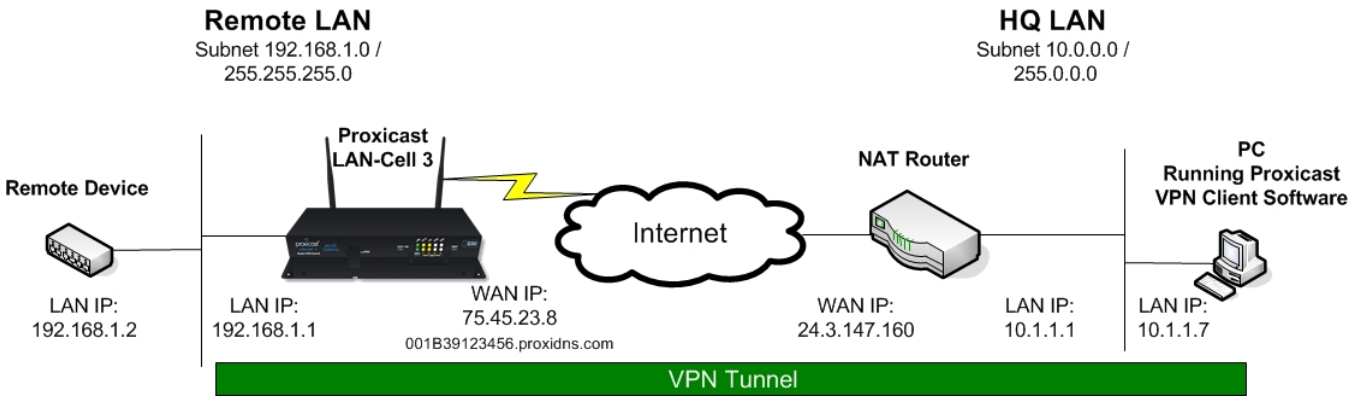


Figure 67: Remote User IPSec Example

Click on the [Add] button to display the following screen and select **VPN Mode** = Remote User:

Sequence Number	1	IKE Key Mode	PSK	Phase 1 Mode	Main
Connection Name	Remote-Users	Preshared Key	12345678	Phase 1 Local ID	
Rule Enabled	☑	DPD Enable	☑	Phase 1 Remote ID	
VPN Mode	Remote Use	DPD Interval	10 Seconds (10 ~ 1200)	Phase 1 Lifetime	28800 Seconds (3600 ~ 28800)
L2TP Enabled	☐	DPD Timeout	60 Seconds (30 ~ 3600)	Phase 2 Lifetime	28800 Seconds (3600 ~ 28800)
Local External Interface	WAN(USB Modem)			Phase 1 Authentication	MD5
Local Subnet IP	192.168.1.0			Phase 1 Encryption	DES
Local Subnet Netmask	255.255.255.0			Phase 1 Group Key Management	DH1
				Phase 2 Authentication	SHA1
				Phase 2 Encryption	DES
				Phase 2 Group Key Management (PFS)	None

Figure 68: IPSec Remote User VPN Settings

The settings for a Remote User VPN are essentially the same as for a Net-to-Net VPN except that the Remote Gateway and Network information is not required since the remote will be a single unknown IP address.

This same configuration is used if the VPN PC is directly connected to the Internet, for example via Wi-Fi hotspot or its own cellular modem card.

Note: You cannot make a Remote User VPN connection to a LAN-Cell that has a private IP address; you must request a public IP address from your ISP. If you cannot obtain a public IP address for the LAN-Cell, then you must have the LAN-Cell initiate a Net-to-Net VPN connection to another VPN server in order to remotely access devices attached to the LAN-Cell.

CHAPTER 9: APPLICATIONS MENU

9.1 Port Forwarding

The LAN-Cell 3 provides Network Address Translation (NAT) services to protect private LAN IP addresses from access by users on the external WAN. Port-Forwarding is a technique to selectively allow remote users to access selected devices and services on the private LAN.

The LAN-Cell 3 supports both Port Forwarding and Port Translation features. These features are integrated with the LAN-Cell's firewall feature. Creating new port forwarding/translation rules automatically opens the corresponding ports in the firewall – no other configuration is necessary.

The port forwarding function gives remote users access to devices on the local network via the public WAN IP address. Users can assign a specific external port range to a local server (IP address). Furthermore, users can specify a different internal port range to be associated with external ports in a port forwarding rule. When the LAN-Cell 3 receives an external request to access any one of the configured external ports, it will redirect the request to the corresponding internal server and change its destination port to one of the internal ports specified. This allows multiple LAN devices with the same port (e.g. port 80) to be accessed remotely without having to change their settings.

By enabling the DMZ Host Function, you can set up a Demilitarized Zone (DMZ) host, that is, a particular computer which is fully exposed to the Internet. This may be necessary for certain applications that use random ports or when you do not know the specific ports required for remote access.

9.1.1 Port Forward Settings

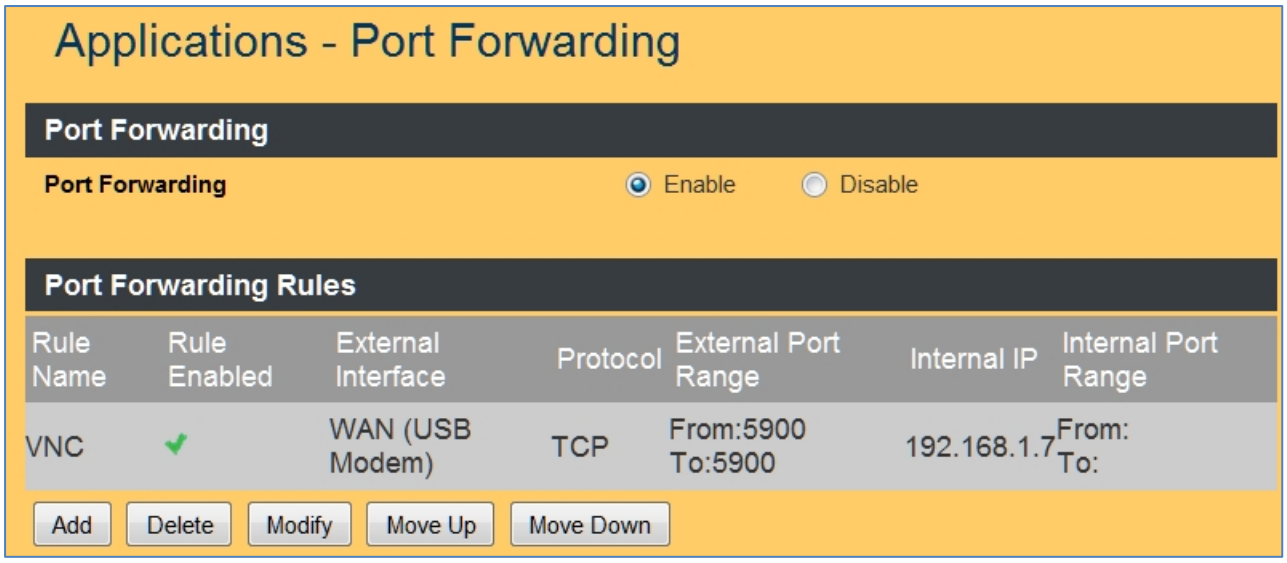


Figure 69: Port Forwarding Settings

Port Forwarding	Select Enable / Disable to enable/disable Port Forwarding

9.1.2 Add Port Range Forwarding Rule

Click on the [Add] button to display the following screen:

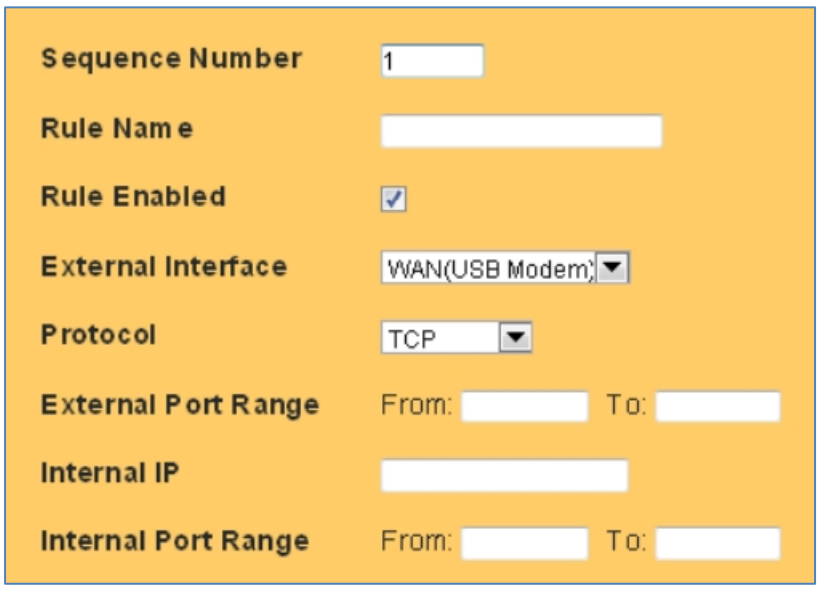


Figure 70: Add Port Forward Rule

Sequence Number	This defines the sequences (priorities) of the port forwarding rules. If a packet fits the conditions set up by the port forwarding rules, the packet will then be forwarded according to the first matching rule in the sequence.
Rule Name	Enter the name of the port forwarding rule. Must not contain spaces.
Rule Enabled	Check/Uncheck to enable/disable this port forwarding rule.
External Interface	Choose USB or Ethernet WAN as the External port forwarding interface. Each WAN interface must have its own port forwarding rules, so duplicate rules if using the LAN-Cell in a WAN fail-over configuration.
Protocol	Choose TCP, UDP or TCP/UDP for the rule to be applied.
External Port Range	Set up the External Port Range for the rule to capture.
Internal IP	Set up the Internal IP (single address) where incoming packets will be directed when the rule is matched.
Internal Port Range	Set up the Internal Port Range where the rule will send matched packets. The internal and external port ranges must contain the same number of ports, but can be different to enable port translation.

9.1.3 DMZ Settings

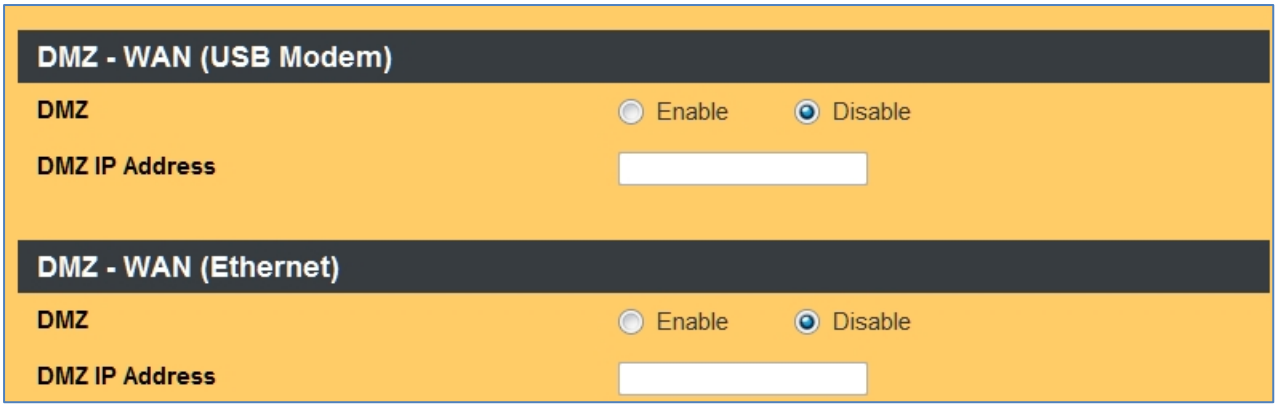


Figure 71: DMZ Settings

DMZ	Select Enable to enable DMZ function. Select Disable to disable DMZ function.
DMZ IP Address	Enter the IP address of a particular host on the LAN which will receive all the packets originally going to the corresponding WAN port / Public IP. **Note:** Be sure to add a Port Forward rule for the LAN-Cell 3's remote management interface port (default=8080) before forwarding all WAN packets to a DMZ host.

9.2 Virtual Hosts

Virtual Hosts function similarly to DMZ hosts, except that Virtual Hosts enable different WAN IP addresses to be mapped to different LAN IP addresses. This is most useful when your WAN has been assigned multiple static public IP addresses (not common for cellular connections). If you have only 1 WAN IP address, use DMZ.

9.2.1 Virtual Host Settings

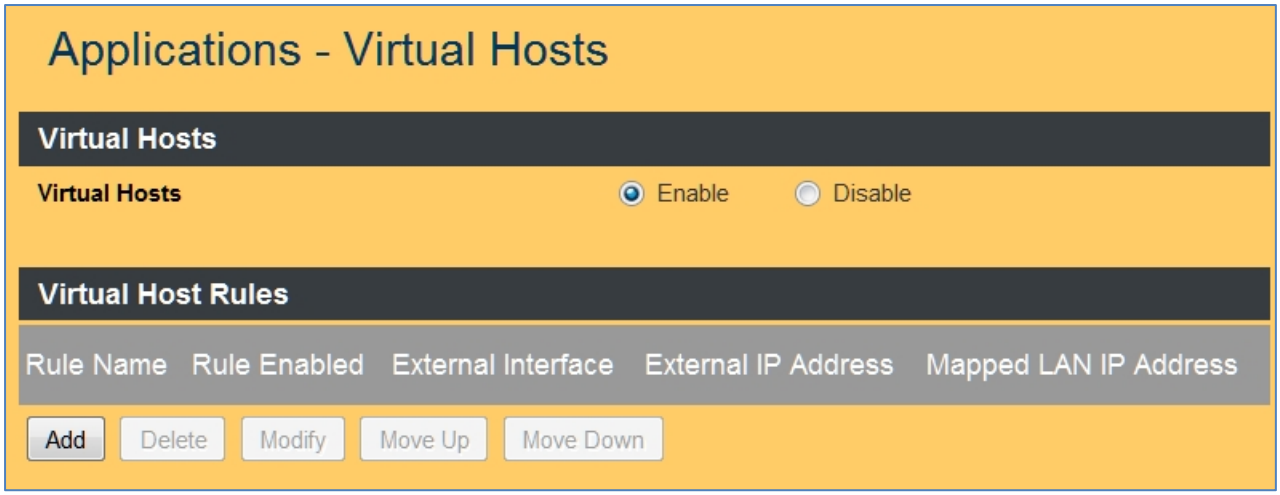


Figure 72: Virtual Host Settings

Virtual Hosets	Select Enable / Disable to enable/disable Virtual Hosts

9.2.2 Add a Virtual Host Rule

Click on the [Add] button to display the following screen:

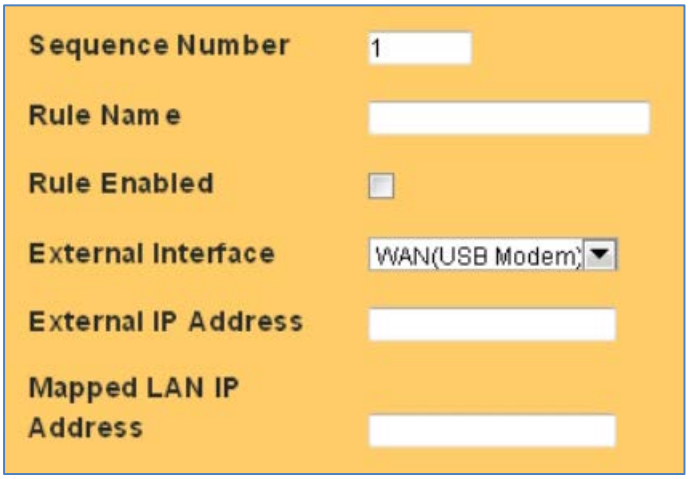


Figure 73: Virtual Host Rule

Sequence Number	This defines the sequences (priorities) of the Virtual Host rules.
Rule Name	Enter the name of the Virtual Host rule. Must not contain spaces.
Rule Enabled	Check/Uncheck to enable/disable this rule.
External Interface	Choose USB or Ethernet WAN as the External interface
External IP Address	Enter one of the IP addresses assigned to the WAN by your ISP.
Mapped LAN IP Address	Enter the Internal LAN IP (single address) where incoming packets will be directed when the rule is matched.

9.3 Streaming / Pass-Through

You can enhance your media streaming quality by enabling RTSP, MSS, and H.323 protocols. Also, the LAN-Cell 3's VPN Pass-through functionality can also be enabled on this screen. All of these features are enabled by default. Disable unused settings to reduce system overhead.

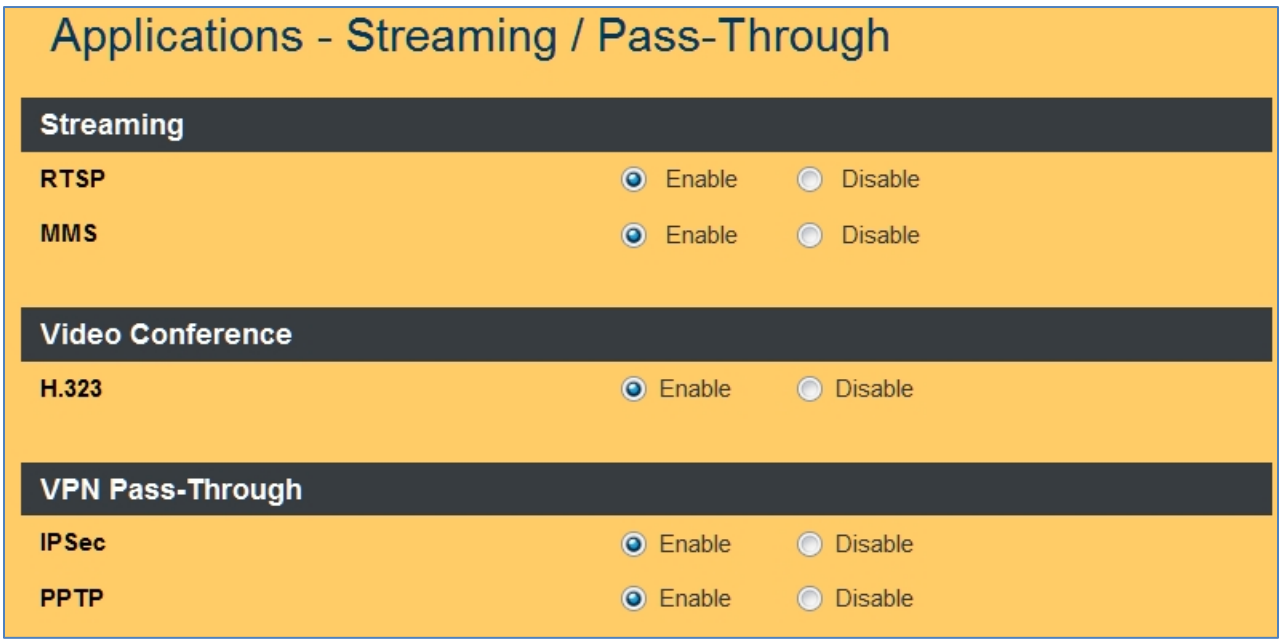


Figure 74: Application / Streaming Setup

RTSP	Select Enable/Disable to enable/disable RTSP
MMS	Select Enable/Disable to enable/disable MMS
H.323	Select Enable/Disable to enable/disable H.323
IPSec Pass-through	Select Enable/Disable to enable/disable IPSec Pass-through
PPTP Pass-through	Select Enable/Disable to enable/disable PPTP Pass-through

9.4 UPnP

Universal Plug and Play (UPnP) is a set of networking protocols that permits networked devices, such as personal computers, printers, Internet gateways, Wi-Fi access points and mobile devices to seamlessly discover each other's presence on the network and establish functional network services for communications.

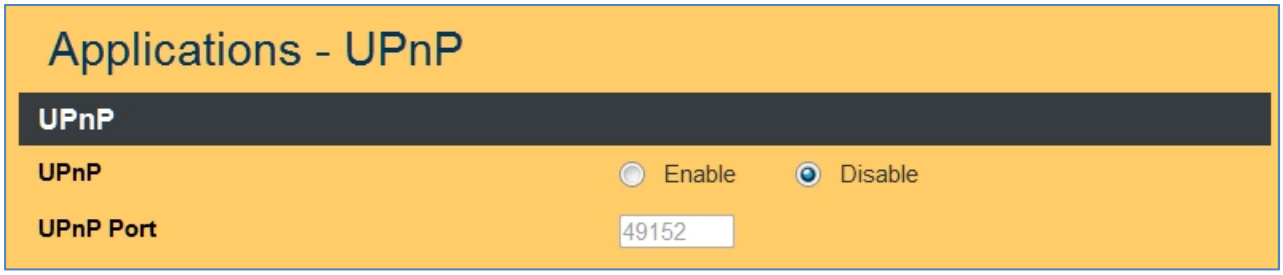


Figure 75: UPnP Setup

UPnP	Select Enable/Disable to enable/disable UPnP
UPnP Port	Enter the number for UPnP port.

CHAPTER 10: QUALITY OF SERVICE (QoS) MENU

10.1 Bandwidth Management

The LAN-Cell 3's Bandwidth Management feature provides two powerful and unique mechanisms to manage bandwidth: Static Bandwidth Management (SBM) and Dynamic Bandwidth Management (DBM). SBM provides users with the option to allocate a fixed amount of bandwidth for a specific computer or a particular application, while DBM intellectually manages the rest of the bandwidth while all the time satisfying the complicated bandwidth requirements/settings of SBM.

10.1.1 Bandwidth Management Settings

To effectively utilize the Bandwidth Management system, you must accurately specify the bandwidth available on a WAN interface. Bandwidth Management then allocates bandwidth according to this information. You can obtain the maximum bandwidth information from your ISP, or use a "speed-test" web-site application to determine your typical actual bandwidth available. Bandwidth Management will be more effective if you are conservative when specifying the maximum bandwidth per interface.

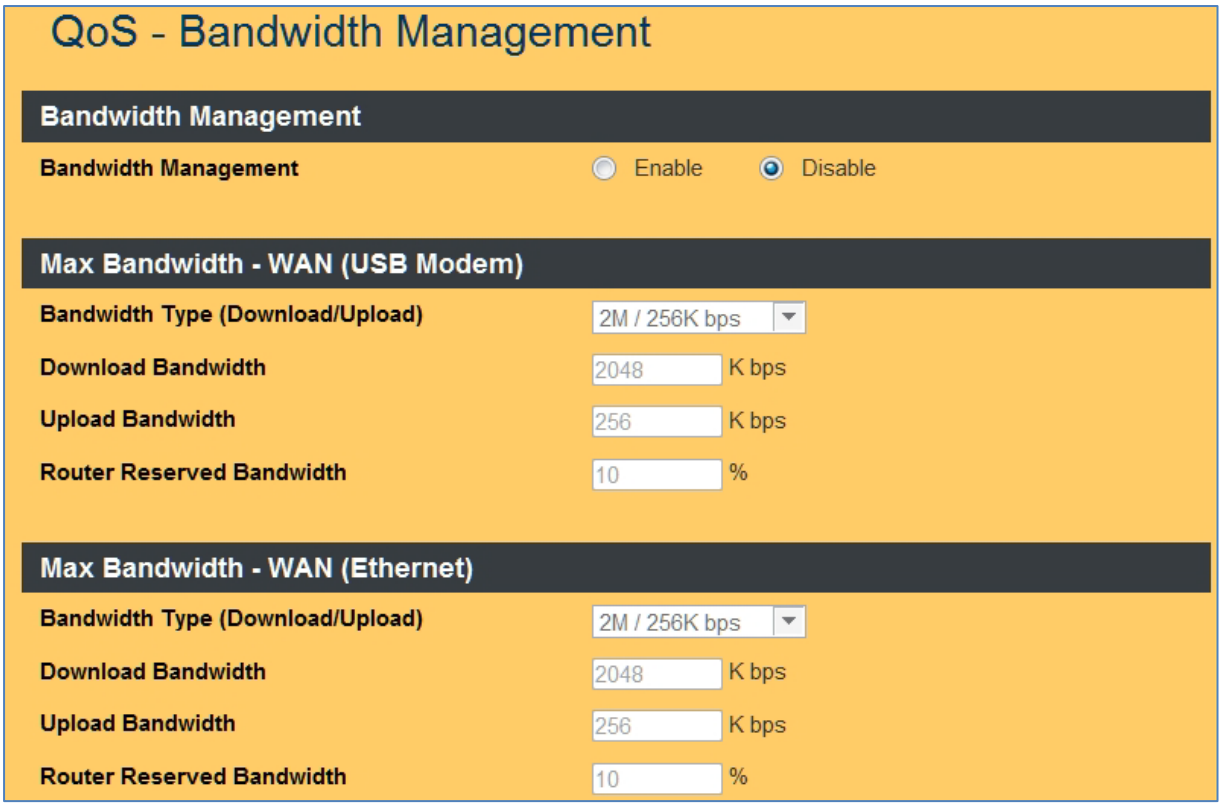


Figure 76: Bandwidth Management Setup

Bandwidth Management	Select Enable/Disable to enable/disable Bandwidth Management.
Bandwidth Type (Download/Upload)	Select the correct bandwidth type according to your Internet service subscription. If the bandwidth type is not available on the list, select Custom.
Download Bandwidth	Enter the value to customize download bandwidth. Note that the value is specified in kilobits per second (Kbps). Multiply kilobytes/sec (KB/s) by 8 to get Kbps. Divide megabytes/sec (MB/s) by 1000 to get Kbps.
Upload Bandwidth	Enter the value to customize upload bandwidth.
Router Reserved Bandwidth	Enter the value to provide bandwidth buffer for the LAN-Cell 3's use. Do not set this value to 0 or the LAN-Cell may become inaccessible during periods of heavy traffic.

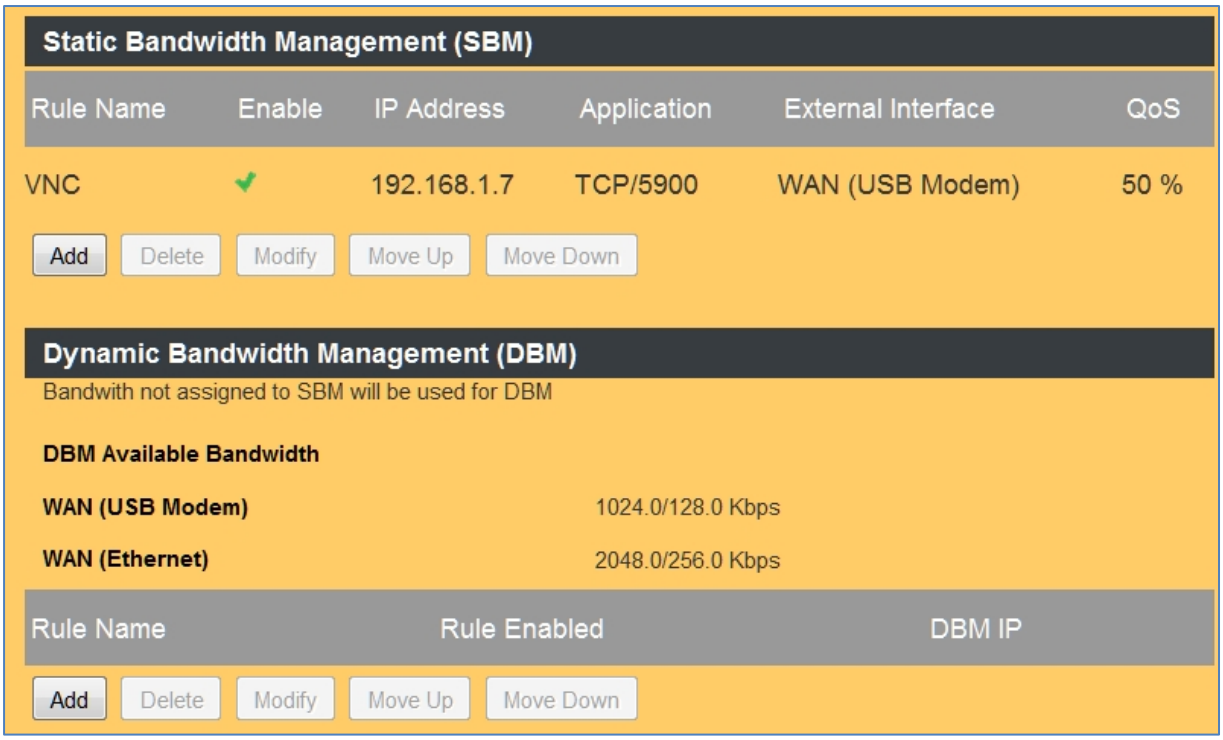


Figure 77: Bandwidth Management Rules

10.1.2 Add SBM Rules

Click on the [Add] button to display the following screen:

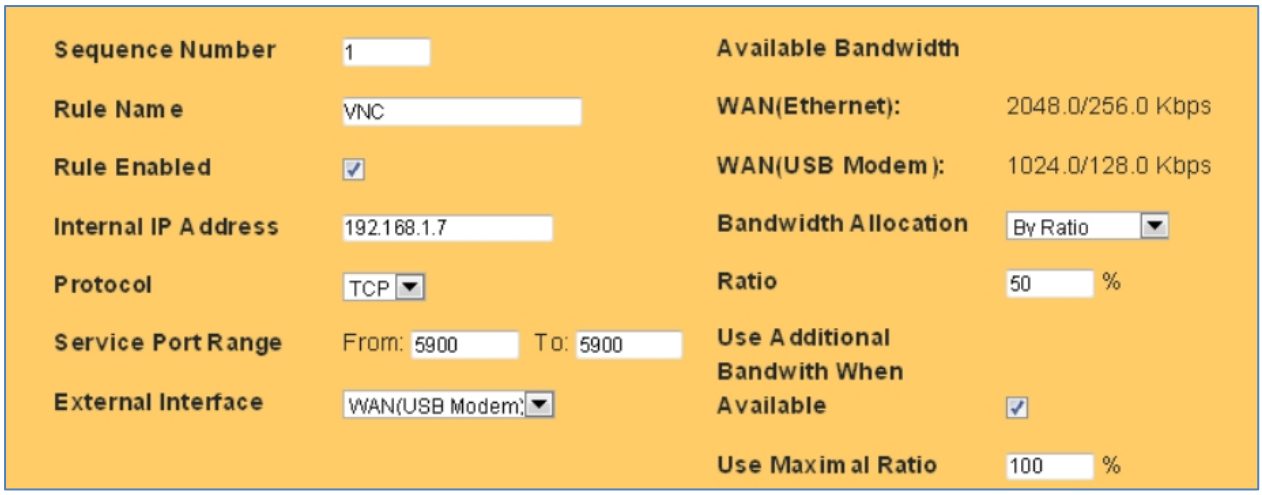


Figure 78: Add Static Bandwidth Rule

In this example, 50% of the bandwidth on the USB WAN interface is being dedicated to the VNC application (TCP Port 5900). If the interface is less than 50% loaded, VNC will be allocated additional bandwidth up to the maximum available but will never be restricted to less than half of the available bandwidth, assuring reasonable performance for this application regardless of any WAN traffic.

Sequence Number	This defines the sequence of the SBM rules. If a packet fits the conditions set by the SBM rules, the packet will then be sorted according to the first SBM rule from the top of the list.
Rule Name	Name of the SBM rule. Spaces are not allowed.
Rule Enable	Enable/Disable this SBM rule.
Internal IP	The internal LAN IP address for this SBM rule.
Protocol	Set up the protocol (TCP or UDP) for the rule.
External Interface	Select which External Interface (USB WAN or Ethernet WAN) you want a packet to go through, IF the packet fits the condition of this SBM rule.
Service Port Range	Set up the Service Port Range for the SBM rule.
Bandwidth Allocation	Select allocation by Ratio or By Bandwidth.
Ratio	The portion of the external interface's bandwidth to be allocated to this rule.
Download	Enter the reserved download bandwidth.
Upload	Enter the reserved upload bandwidth.

Use Additional Bandwidth when Available	Check this box if you wish to allow the traffic matching this SBM rule to be able to utilize the whole bandwidth when the bandwidth is idle.
Use Maximal Ratio	Percentage of the WAN interface's total bandwidth to apply to this rule.

10.1.3 Add DBM Rules

Dynamic Bandwidth Rules define which LAN IP addresses are to be included in the dynamic bandwidth allocation scheme. The default is all LAN IP addresses; however in for some applications you may wish to limit the IPs included in DBM. You may create a maximum of 16 DBM rules.

Click on the [Add] button to display the following screen:

Figure 79: Add Dynamic Bandwidth Rule

Sequence Number	This defines the sequence of the DBM rules.
Rule Name	Name of the DBM rule. Spaces are not allowed.
Rule Enable	Enable/Disable this DBM rule
Internal IP Range	Set up the internal IP range for this DBM rule.

10.2 Throughput Optimizer

The LAN-Cell 3's Throughput Optimizer feature transmits the defined high-priority packets types to optimize network utilization and minimize delays. All of the pre-defined packet types are enabled for optimization by default. Disable them only if performance of other applications is adversely affected.

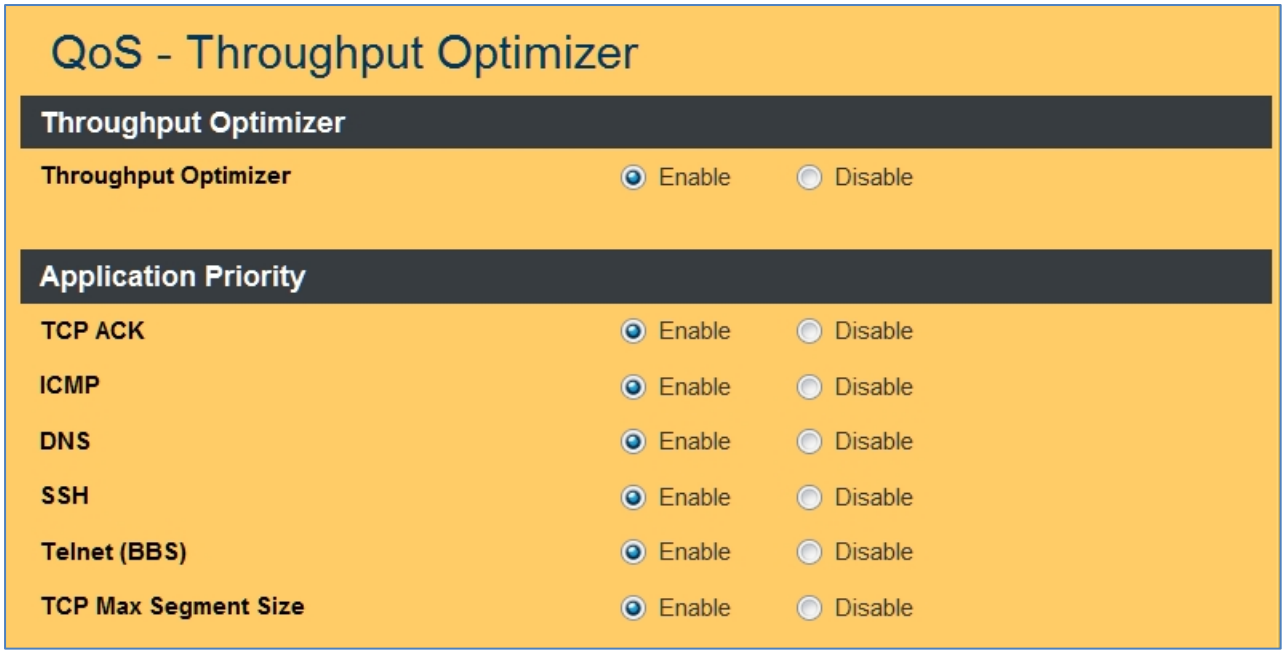


Figure 80: Throughput Optimizer Settings

Throughput Optimzer	Select Enable/Disable to enable/disable the Throughput Optimizer.
TCP ACK	Select Enable/Disable to enable/disable TCP ACK priority
ICMP	Select Enable/Disable to enable/disable ICMP priority
DNS	Select Enable/Disable to enable/disable DNS priority
SSH	Select Enable/Disable to enable/disable SSH priority
Telnet (BBS)	Select Enable/Disable to enable/disable Telnet (BBS) priority
TCP Max Segment Size	Select Enable/Disable to enable/disable TCP Max Segment Size

10.3 Ultra-NAT

Network Address Translation (NAT) is often a performance bottleneck in routers and firewalls. Generic routers are generally insufficient when dealing with a high-speed broadband network. Ultra-NAT is designed to solve this problem by accelerating NAT performance allowing the LAN-Cell 3 to maximize the higher speed networks and to reserve system performance for other features such as ACL and VPN servers.

The LAN-Cell 3 also has a hardware acceleration feature that can improve NAT performance; however, Hardware NAT acceleration cannot be enabled if any of the following features are also enabled:

- Bandwidth Management
- Web Filtering
- Wi-Fi Universal Repeater
- VPN/PPTP

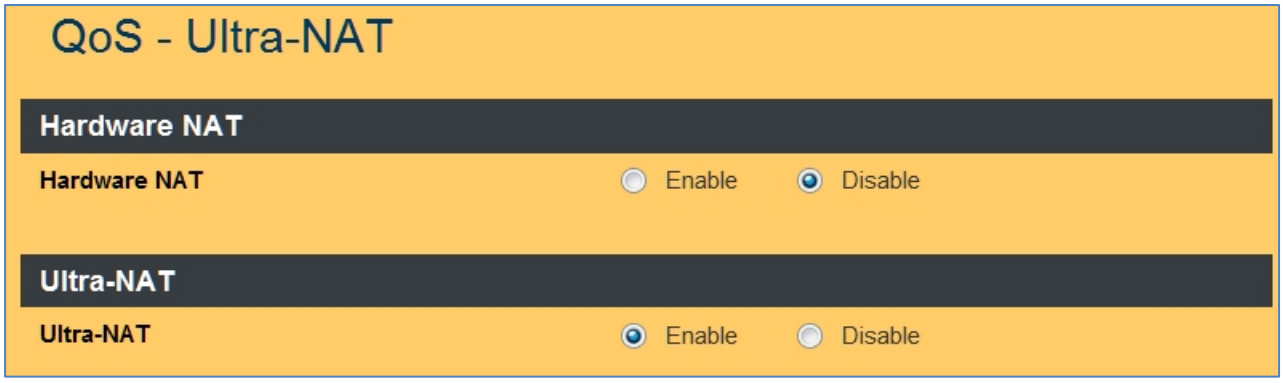


Figure 81: Ultra-NAT Settings

Hardware NAT	Select Enable/Disable to enable/disable Hardware NAT acceleration.
Ultra-NAT	Select Enable/Disable to enable/disable Ultra-NAT.

10.4 Session Manager

Session manager will automatically recycle old/dead sessions to get better connection efficiency. Users can choose the recycle rate to optimize the connection efficiency especially for applications which rapidly open and close many ports (e.g. P2P downloads, games, etc.)

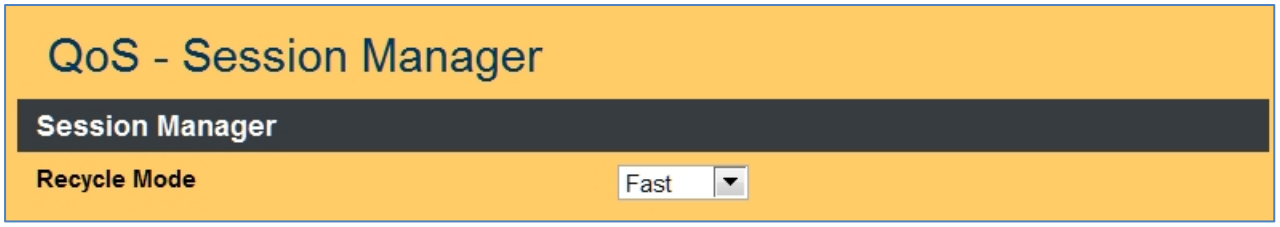


Figure 82: Session Manager Settings

Recycle Mode	Select Fast/Regular/Slow recycle rate

CHAPTER 11: ADMIN MENU

11.1 System Management

The Management screen is used to perform various administrative tasks on the LAN-Cell 2 such as changing the login password, saving and restoring system settings, scheduling a reboot, and performing firmware upgrades.

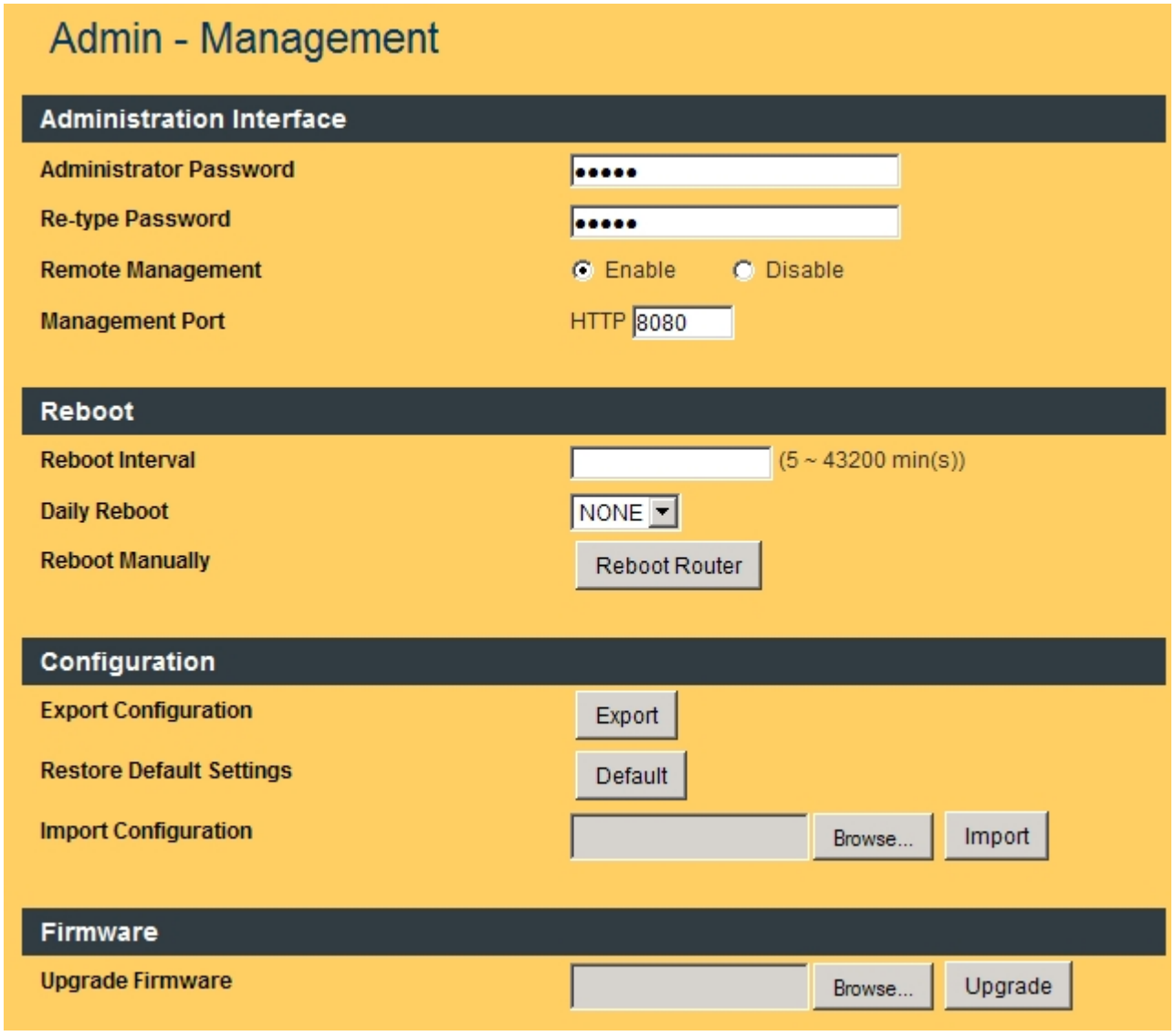


Figure 83: System Management Settings

Administrator Password	Maximum input is 36 alphanumeric characters (case sensitive)
Re-type Password	Enter the password again to confirm.
Remote Management	Select Enable to enable Remote Management. Select Disable to disable Remote Management If remote management is enabled, users may access the LAN-Cell's web configuration screens via a WAN (Internet) connection.
Management Port	HTTP port which to which remote LAN-Cell administrators connect. (Default port is 8080)
Reboot Router	Press the Reboot Router button to initiate an immediate reboot of the LAN-Cell. See the **Setup > Time** screen to configured regularly scheduled reboots.
Reboot Interval	Enter the number of minutes of run-time before the LAN-Cell 3 automatically reboots. The Interval count-down timer will restart once the LAN-Cell 3 has finished rebooting. Leave this field blank to disable the automatic reboot Interval timer.
Daily Reboot	Enter the time of day (based on the LAN-Cell's current time) at which the LAN-Cell 2 will automatically restart. Set this value to NONE to disable the daily reboot timer.
Export Configuration	Click Export to save the current configuration settings to a file.
Restore Default Configuration	Click Restore to restore the LAN-Cell 3 to its factory default system settings: LAN IP = 192.168.1.1:8080 Username/Password = admin/1234
Import Configuration	Click Browse and Import to load a previously saved configuration file.
Upgrade Firmware	Click Browse and Upgrade to load a firmware upgrade image.

Note: You can combine the Interval and Daily reboot timers to have the LAN-Cell 3 restart under conditions. For example you may desire the LAN-Cell to restart every 8 hours and always at 1 AM UTC so that you have at least one known reboot time. If the Daily Timer is used, do not set the Interval timer greater than 1440 minutes (24 hours).

11.2 SNMP

Simple Network Management Protocol (SNMP) is an Internet-standard protocol for monitoring and managing devices on IP networks. It is used by network management systems to monitor network-attached devices for conditions that warrant administrative attention. The SNMP Management Information Base (MIB) for the LAN-Cell 3 is available on the Proxicast Support web site.

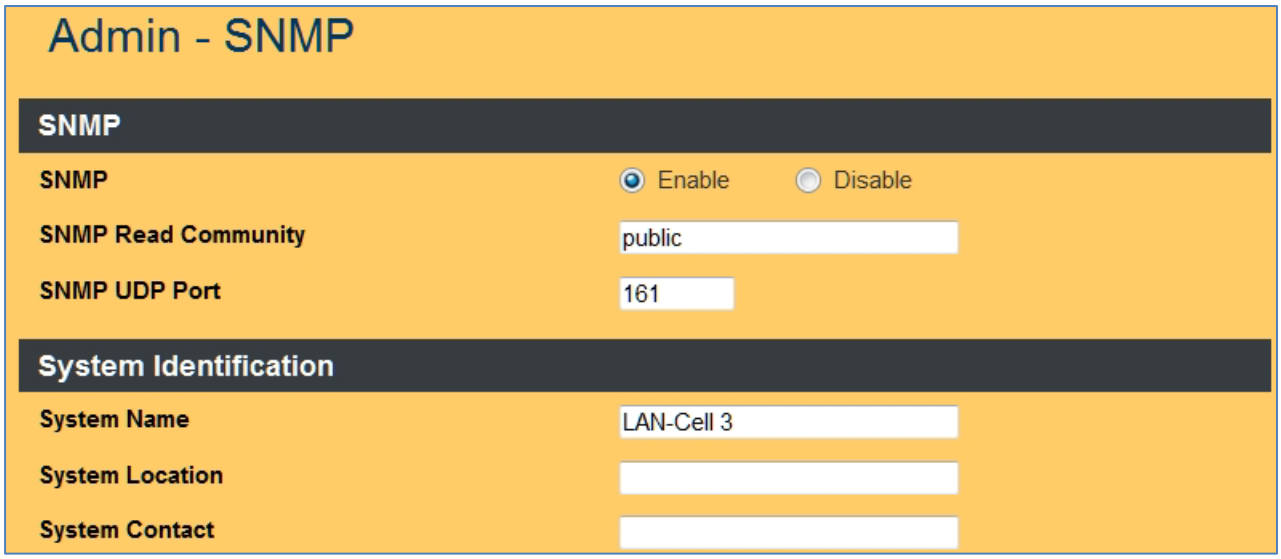


Figure 84: SNMP Settings

SNMP	Choose Enable/Disable to enable/disable the SNMP agent.
SNMP Read Community	The Community String required for read access to SNMP values. Default value is “public”. At this time, only read access is permitted.
SNMP UDP Port	UDP port on which the SNMP agent is listening.
System Name	String (25 characters) which identifies this specific LAN-Cell 3 device. Value is displayed on the upper right of the LAN-Cell’s management pages and returned as OID: 1.3.6.1.2.1.1.5.0
System Location	String (25 characters) which can be used to identify the location of this LAN-Cell. Returned as OID: 1.3.6.1.2.1.1.6.0
System Contact	String (25 characters) which can be used to identify the contact information for this LAN-Cell. Returned as OID: 1.3.6.1.2.1.1.4.0

11.3 System Utilities

The System Utilities screen provides several useful tools for network and device diagnostics.

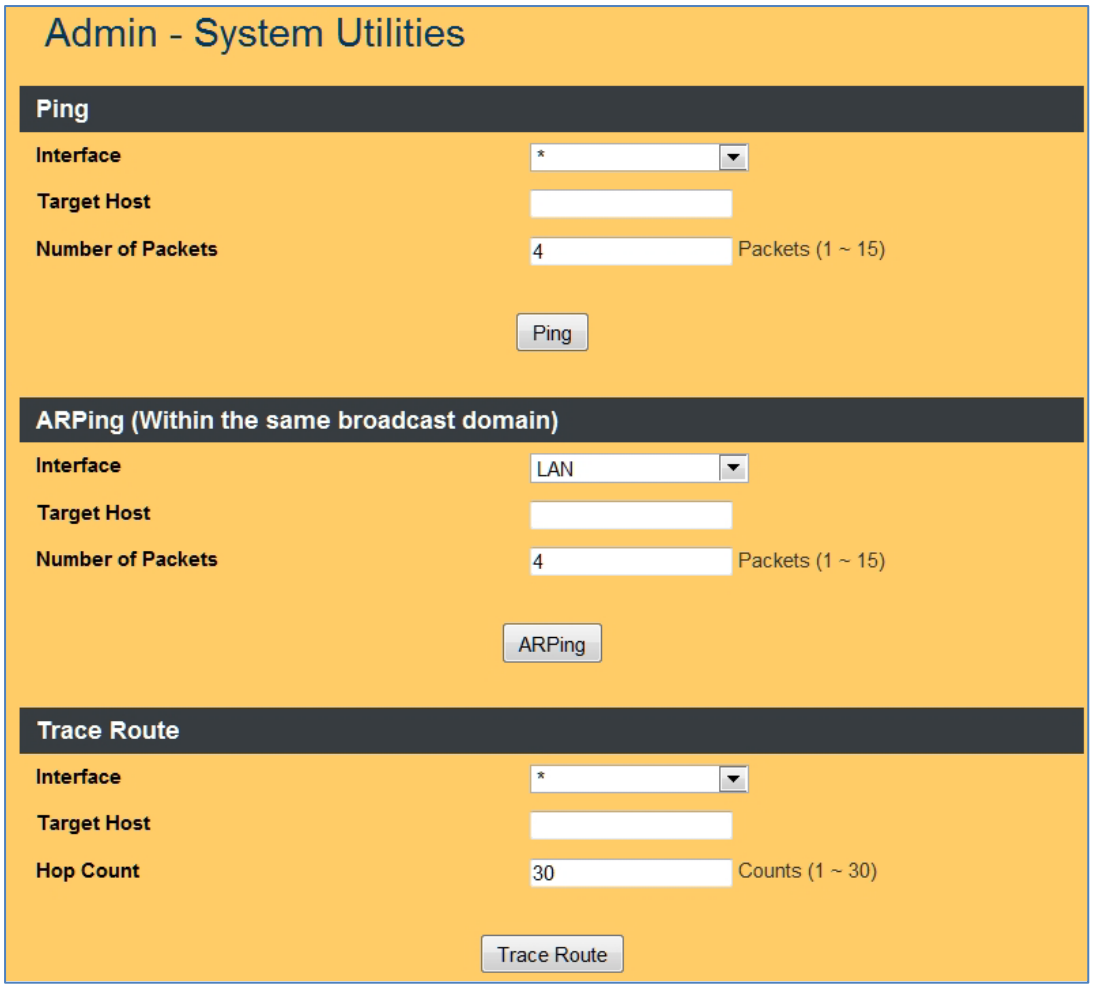


Figure 85: System Utilities

11.3.1 Ping (ICMP)

The Ping utility sends a series of ICMP packets to a designated IP address to test communications with that IP.

Interface	Select the interface through which to send the ping, ie. LAN, WAN. Selecting "*" will send the ping to the best available interface based on the LAN-Cell 3's current routing table.
Target Host	Enter the IP address to send the ping to.
Number of Packets	Specify the number of ICMP packets to send out.
Ping	Press the button to send ping ing packets.

11.3.2 ARPing

Similar to “ping” the ARPing utility is used to discover hosts on a network. The utility tests whether a given IP address is in use on the local network, and can get additional information about the device using that address. ARPing operates at layer 2 (or the link layer of the OSI model) - using the Address Resolution Protocol (ARP) for probing hosts.

Interface	Select the interface through which to send the ARPing.
Target Host	Enter the IP address to send the ARPing to.
Number of Packets	Specify the number of packets to send out.
ARPing	Press the button to send ARPing packets.

11.3.3 Trace Route

Trace Route is a network diagnostic tool for displaying the route (path) and measuring transit delays of packets across an IP network. Trace Route sends a sequence of ICMP echo request packets addressed to a destination host. Trace Route uses the returned ICMP messages to produce a list of that the packets have traversed. The timestamp values returned for each router along the path are the delay (aka latency) values measured in milliseconds for each packet. The Trace Route results are displayed in the Results Window.

Interface	Select the interface that Trace Route should use. Selecting “*” will send the ICMP requests to the best available interface based on the LAN-Cell 3’s current routing table.
Target Host	Enter the destination IP address / domain name to trace.
Hop Count	Specify the maximum number of hops for before Trrace Route deems the target host ot be unreachable.
Trace route	Press the tab to start the “Trace Route” actions

11.3.4 USB Modem Command

The System Utilities page also contains a tool for sending “AT” commands directly to the attached USB modem and viewing the results. This tool is designed primarily for Proxicast Technical Support’s use when diagnosing modem issues. Commands can only be sent to the modem when the USB WAN interface does not have an active connection (IP address) on a cellular network, therefore this tool cannot be used remotely.

11.4 Log

11.4.1 System Log

The System Log records various events that have occurred during the LAN-Cell 3's operation. Events are divided into classes to make it easier to review specific event chains. Events are displayed in reverse chronological order (newest events are at the top of the log). The LAN-Cell 3 has a limited amount of space available for log events – the oldest events are overwritten when the log is full. See the Syslog feature below for storing system log events over longer periods of time. The **Refresh** button updates the log display with the latest events. The **Clear** button erases the entire system log.

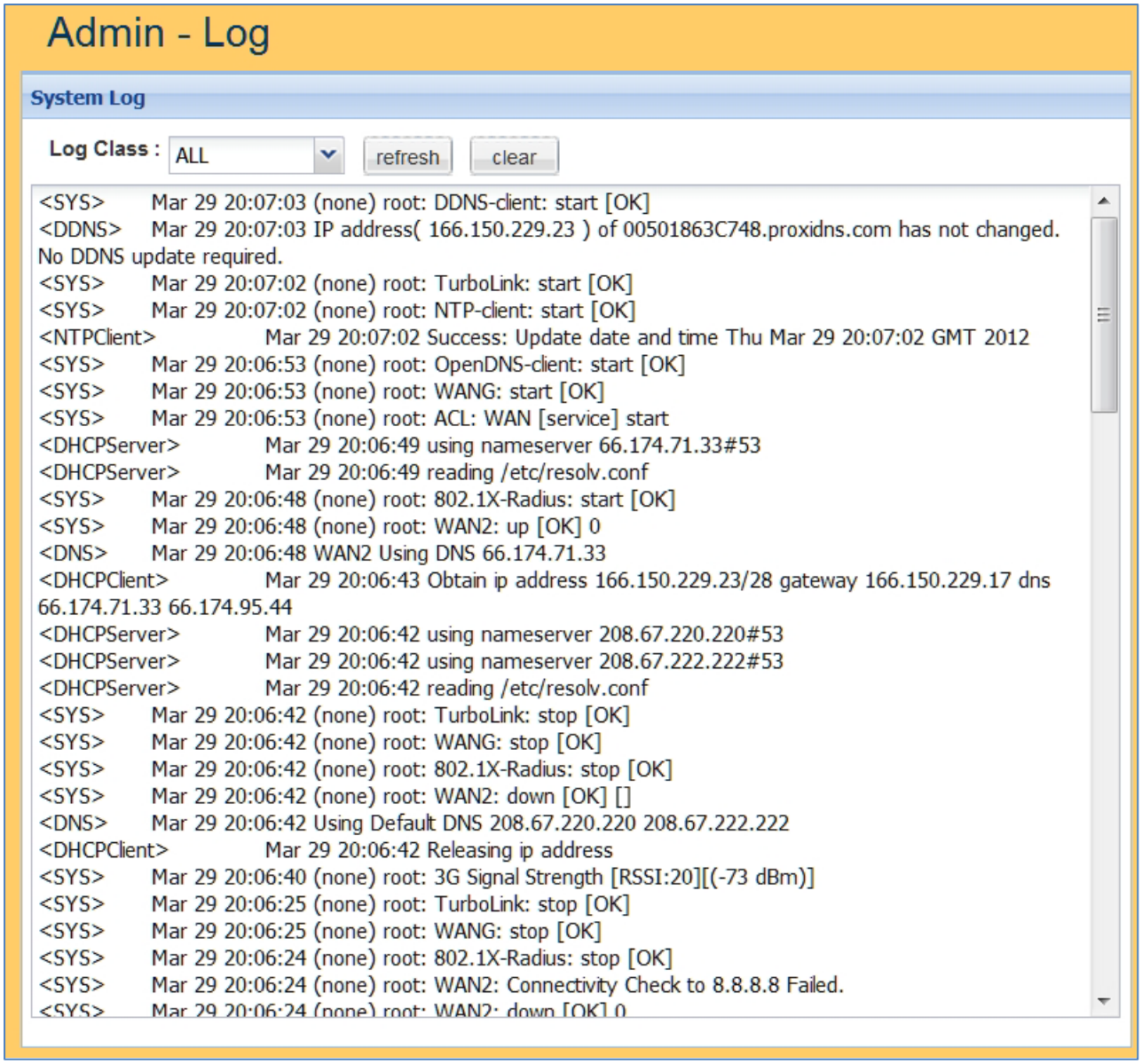


Figure 86: System Logging

11.4.2 Syslog

Syslog is a standard mechanism for transmitting and storing system log information from a device to a remote server. The LAN-Cell 3 can send its system event logs to another system which is running a Syslog server. The Syslog server can alert administrators of events and store event logs over long periods of time.

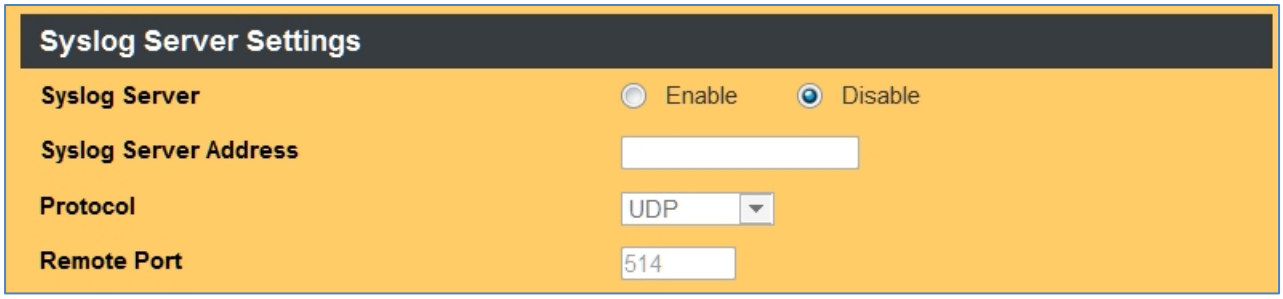


Figure 87: Syslog Settings

Syslog Sever	Choose Enable/Disable to enable/disable the Syslog function.
Syslog Server Address	The IP address or fully qualified domain name of the Syslog server which will receive event messages.
Protocol	The IP protocol that the Syslog server expects messages to use.
Remote Port	The port number that the remote Syslog server is listening on (default is UDP:514)

APPENDIX

Common Tasks

HOW TO	WHERE	ACTION
Change the LAN-Cell's IP address/subnet	Setup > LAN	Enter the IP address to assign to the LAN-Cell and select the subnet mask for the LAN. The DHCP Server will automatically adjust.
Configure the USB modem	Setup > WAN	Select the modem model and service provider from the drop-down lists or override the settings using Manual mode.
Enable Wi-Fi	Wireless > Basic	Enable the Wi-Fi radio and configure the Access Point's SSID and security settings.
Forward ports to LAN devices	Applications > Port Forwarding	Click the **Add** button to create a new port-forward/translation rule.
Set up a VPN	Security > VPN	Select either the PPTP or IPSec menus to create the corresponding VPN.
Connect to a remote Wi-Fi network	Setup > WAN	Change the Connection Type of the Ethernet WAN to **Wi-Fi Client** and enter the connection details for the remote Wi-Fi network. Wi-Fi must first be enabled via Wireless > Basic
Configure Dynamic DNS settings	Setup > DDNS	Select the preferred DDNS service provider and enter the required login information and host name. Each LAN-Cell 3 also has a unique permanent DNS name: *serial#.proxidns.com*
Configure WAN keep-alive & fail-over	Setup > WAN Advanced	Set primary WAN, fail-over target and tolerance parameters to periodically send pings to detect WAN failures.
Restart Periodically	Admin > Management	Select the frequency for the LAN-Cell 3 to automatically reboot.
Change the default unit name	Admin > SNMP	Enter the System Identification parameters.
Change the default password	Admin > Management	Passwords are case sensitive. The username cannot be changed from "admin" however, multiple users may log in concurrently.
Update Firmware	Admin > Management	Download firmware updates from http://support.proxicast.com

Troubleshooting

PROBLEM	CORRECTIVE ACTION
None of the LEDs turn on	Ensure that the correct power adapter is connected to the LAN-Cell and plugged in to an appropriate power source. If the LEDs still do not turn on, there may be a hardware failure.
Cannot access the LAN-Cell from a PC on the LAN	Check the cable between the computer (or hub/switch) and the LAN-Cell. Check that the corresponding LAN port LED is ON. Configure the PC to receive its IP settings via DHCP (automatic assignment). Confirm that any other network interfaces on the PC (such as Wi-Fi) are disabled. Wi-Fi cannot be used for the initial configuration of the LAN-Cell – the internal Wi-Fi Access Point is disabled by default.
Cannot ping any computer on the LAN	If the LAN LEDs are off, check the cable connections. Verify that the IP address and subnet of the LAN-Cell is in the same range as the computers on the LAN and that the LAN-Cell is the gateway for all LAN devices.
USB modem does not initialize (USB LED continues to flash)	Confirm that the USB modem has been activated by the cellular carrier. Follow their instructions for activating the modem using a Windows PC. Ensure that the SIM/RUIM card (if required) is properly inserted. Network registration may take several minutes. Confirm that the USB modem is supported by the LAN-Cell's current firmware version.
Cannot make (or maintain) a cellular data connection when cellular signal is present (i.e. no USB WAN IP address)	Confirm that the USB modem's APN, Username, Password, Authentication Type, PIN and ISP Access Phone Number settings are correct for the cellular provider. Confirm that the USB modem has been provisioned with the correct type of Internet access data service. Confirm that the USB modem has been activated by the carrier and/or by using a Windows PC. Consult the manufacturer's documentation for the USB modem regarding its LED status indicators.

PROBLEM	CORRECTIVE ACTION
Wrong type of 4G/3G WAN IP address is assigned (i.e. dynamic instead of static or private instead of public)	The IP address assigned to the LAN-Cell's WAN interface is controlled by the cellular service provider. Confirm that the account has been provisioned for the proper type of IP address and that the connection parameters match those required by the service provider. "Static" cellular IP addresses are assigned by the carrier via a DHCP process – the static cellular IP address is not configured in the LAN-Cell in advance.
Cellular Signal Strength is low	Cellular data connections may be unreliable if the signal strength is poor (< 20%). Check that the proper external antenna is securely attached to the USB modem. Use a USB extension cable to locate the USB modem to a more favorable location. Move the LAN-Cell to a location where the carrier's signal is stronger or use a higher-gain antenna or amplifier.
Cannot get a WAN IP address from the Ethernet WAN ISP	The WAN IP address is provided after the ISP verifies the MAC address, host name or User ID. Confirm the verification method used by the ISP and configure the corresponding fields. Check the LAN-Cell's connection to the wired WAN (cable/DSL modem). Check whether the Ethernet WAN connection requires a crossover or straight cable. Check the settings in the WAN screens, especially the fail-over/load balancing parameters.
Wi-Fi clients periodically disconnect, esp. when LAN-Cell configuration parameters are updated	Some updates to the LAN-Cell's configuration require that the Wi-Fi Access Point be reinitialized, causing client connections to drop. Configure Wi-Fi clients to automatically reconnect to the LAN-Cell. Upgrade the firmware and driver software on Wi-Fi client devices to the latest version.
After pressing RESET, cannot make a cellular connection	The RESET button returns the LAN-Cell to its factory default settings including clearing any cellular modem parameters. The USB modem settings may have to be manually reconfigured if the modem is not auto-detected.

Common Carrier Specific Issues

CARRIER	COMMENT
Verizon Wireless 4G/LTE	By default Verizon Wireless' 4G/LTE network provides NAT'd private IP addresses (10.x.x.x). This prevents all Internet initiated inbound connections from reaching the LAN-Cell. Use the LAN-Cell's VPN features to make an outbound connection to a VPN server on another network. Static public IP addresses which allow inbound initiated connections are available for an additional fee. To avoid address conflicts, do not use 10.x.x.x addressing on the LAN Cell's LAN subnet if you have a dynamic IP from Verizon.
Verizon Wireless 3G/CDMA 4G/LTE	Verizon Wireless' default gateways do not respond to ICMP (ping) packets. Do not select the "Default Gateway" option under **Setup > WAN Advanced > Fail-Over**; select another public IP address.
AT&T Wireless	The "broadband" and "isp.cingular" APN's block <u>all</u> packets originating from the Internet. To access the LAN-Cell or other equipment remotely, request that AT&T provide access to the "internet" APN, or another APN which offers *mobile terminated data service*. Or use the LAN-Cell's VPN features to make an outbound connection to a VPN server on another network. Do not select the "Default Gateway" option under **Setup > WAN Advanced > Fail-Over**; select another public IP address. Public static IP addresses which allow inbound initiated connections are available on the AT&T Wireless network for an additional fee.
Sprint	Sprint blocks access to ports 80 & 5000 (and perhaps others) from Internet addresses. Move LAN devices to different port numbers or use the LAN-Cell's Port Forwarding feature to redirect open public ports to the blocked ports on the LAN.

Specifications

Physical	
Dimensions **with Modem-SAFE** **Mounting Base**	9.1 x 4.4 x 1.0 in 23.1x 11.2 x 2.5 cm (excluding modem) 10.3 x 5.25 x 2.4 in 26.2 x 13.4 x 6.1 cm Mounting template is available for download from: http://www.proxicast.com/support/files/LAN-Cell-3-Mounting-Template.pdf
Weight **with Mounting Base**	1.5 lbs (0.7 kg) (excluding modem) 3.2 lbs (1.4 kg) (excluding modem)
Power Specification	12V DC @ 1.5 A (max) 2.1 mm jack (center pin positive)
Power Consumption	4W Typical; 8W Max
Operating Temp.	-22 to 140 F (-30~60 C)
Operating Humidity	10%~90%
Chassis	18 ga. Steel. Desktop & Removable Multi-Function Mounting Base (included). Patent-pending USB Modem-SAFE USB modem storage system. Cable management and external antenna mounting features.
Certifications	EMC: FCC ID: PBLCDE570AM FCC Part 15 Class B, CE-EMC Class B, C-Tick Class B, VCCI Class B Safety: CSA International, CE EN60950-1 (UL60950-1, CSA60950-1, EN60950-1, IEC60950-1) -- RoHS
Connectors	
LAN/DMZ	4 LAN/DMZ auto-negotiating, auto MDI/MDI-X 10/100/1000 Mbps RJ45 Ethernet ports.
WAN	One auto-negotiating, auto MDI/MDI-X 10/100/1000 Mbps RJ-45 Ethernet port
USB 2.0	For installing 4G/3G USB modems
Power Switch	On/Off
Reset Button	Restores factory default settings
USB Eject	Safely ejects USB modem
Wi-Fi	
Technology	802.11 b/g/n 300 Mbps max
Operating Modes	Access Point, Repeater, Client, WPS, WDS, WMM
SSIDs	2 (isolated) with Guest LAN option
Security	WPA, WPA2, WPA-PSK, WPA2-PSK, WEP 64 /128-bit, 802.1x
Antennas	MIMO 2x2 Two 3 dBi rubber duck style swivel 802.11 b/g/n antenna (SMA-RP Female). The Wi-Fi antenna jacks on the LAN-Cell are SMA-RP Male

Software Functions	
4G / 3G Features	Plug & Play for Most CDMA/GSM/LTE Modems Over 130 USB Modems Supported Pre-defined Service Provider Profiles WAN to 3G/4G Fail-Over and Fall-Back 3G/4G Keep-Alive Packets Multiple External Antennas Supported
Networking	LAN DHCP Server, Cache, Proxy Server, Relay WAN DHCP Static IP, PPPoE, Wi-Fi Client WAN Fail-over Detection Limits & Controls WAN Load Balancing (Ethernet + USB) Static Routing L3 / L4 IP/Port Policy-based Routing Port-Forwarding VLAN Support Spanning Tree Protocol Support Dynamic DNS (DynDNS, NoIP, TZO, etc) Permanent DNS Address (serial#.proxidns.com) Bandwidth Mgmt. & Throughput Optimization Content Filtering (OpenDNS) NTP Time Service Support
VPN Features	IPSec Server and Client Modes Site-to-Site & Remote User Access Tunnels 32 Simultaneous IPSec Tunnels AES/1DES/DES Encryption SHA1/MD5 Authentication Dead Peer Detection (DPD) PPTP Server Mode (32 simultaneous clients) MS-CHAPv2 & MPPE 128 bit security
Security Features	Stateful Packet Inspection (SPI) Firewall Anti-DoS and Anti-spoofing Protection L2 / L3 / L4 ACL Filtering Static DHCP and static ARP IP-MAC binding DMZ and Port Forwarding (virtual server
System Management	Web-based Management (Local & Remote) Tablet Friendly GUI Configuration Backup and Restore

	Firmware Upgrade and Downgrade SNMP Support Syslog Support Real-Time Logging Scheduled System Restarts Ping, ARPing, Traceroute Utilities

LAN-Cell 3 Default Settings

LAN IP Address	192.168.1.1
HTTP Management Access	admin / 1234 on port 8080
LAN DHCP Server	192.168.1.33 to .65 Subnet mask 255.255.255.0
USB 4G/3G WAN	Auto Detect & Configure
Ethernet WAN	DHCP Client Enabled
Wi-Fi Access Point	Disabled
DNS Host Name	*serial#.*proxidns.com

Press the RESET button for 5 seconds to return the LAN-Cell to these settings.

Legal Information

Copyright

Disclaimer

Proxicast does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. Proxicast further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Trademarks

Proxicast is a registered trademark and ProxiOS (Proxicast Network Operating System), LAN-Cell, Card-Guard, Cell-Lock, Modem-LOCK, PocketPORT and Cell-Sentry are trademarks of Proxicast, LLC. Other trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

Certifications

Federal Communications Commission (FCC) Interference Statement

Contains FCC ID: PBLCDE570AM

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

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

This device has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This device generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

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

- 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.

FCC Radiation Exposure Statement

- This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
- IEEE 802.11b, g and n operation of this product in the U.S.A. is firmware-limited to channels 1 through 11.
- To comply with FCC RF exposure compliance requirements, a separation distance of at least 20 cm must be maintained between the antenna of this device and all persons.

Notices

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment. This device has been designed for the WLAN 2.4 GHz networks throughout the EC region and Switzerland, with restrictions in France. This Class B digital apparatus complies with Canadian ICES-003. Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

Proxicast Limited Warranty

Proxicast warrants to the original end user (purchaser) that this product is free from any defects in materials or workmanship for a period of up to one year from the date of purchase. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, Proxicast will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal value, and will be solely at the discretion of Proxicast. This warranty shall not apply if the product is modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. Proxicast shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact Proxicast's Service Center for your Return Material Authorization number (RMA). Products must be returned Postage Prepaid. It is recommended that the unit be insured when shipped. Any returned products without proof of purchase or those with an out-dated warranty will be repaired or replaced (at the discretion of Proxicast) and the customer will be billed for parts and labor. All repaired or replaced products will be shipped by Proxicast to the corresponding return address, Postage Paid. This warranty gives you specific legal rights, and you may also have other rights that vary from country to country.

Customer Support

Online Web Support

Please refer to support.proxicast.com for additional support documentation and access to our Knowledgebase which contains many resources such as.TechNotes, Frequently Asked Questions, sample configurations and firmware updates.

E-Mail Support

Support E-mail: support@proxicast.com

Please provide the following information when you contact customer support:

- Product model and serial number.
- Current firmware version running on the device
- Date that you received your device.
- Brief description of the problem and the steps you took to solve it.

Corporate Headquarters (Worldwide Customer Support)

- Sales E-mail: sales@proxicast.com
- Telephone: 877-777-7694 (412-213-0018)
- Fax: 412-492-9386
- Web Site: www.proxicast.com
- Regular Mail & RMA Shipments:
  Proxicast, LLC 312 Sunnyfield Drive, Suite 200 Glenshaw, PA 15116-1936 USA

Return Merchandise Authorizations (RMA)

If you need to return a product for service, you must contact Customer Support and request an RMA Number. Returns will not be accepted without an RMA Number on the outside of the shipment.

Please return only the main product unit (no accessories) unless otherwise directed by Customer Support.

Securely pack and insure the product. Return shipping costs are the responsibility of the customer.

INDEX

M

N

O

P

Q

R

S

T

U

V

W