# EtherLINQ

## 4G/LTE Ethernet Router

## with WiFi, VPN & Firewall

# *User's Guide*

**Version 5.2**

proxicast®

# CONTENTS

# Document Revision History

| | |
|---|---|
| June 3, 2019 | Version 5.2: Updated for firmware v5.2.x new/revised features |
| July 25, 2018 | Version 5.1: Initial release |

# Related Documents & Resources

**EtherLINQ Quick Start Guide**

http://www.proxicast.com/support/files/EtherLINQ-3-QuickStartGuide.pdf

**EtherLINQ Technical Support (Documentation, Firmware Updates, KnowledgeBase)**

https://support.proxicast.com

**EtherLINQ Accessories**

https://shop.proxicast.com

# About This User's Guide

## Intended Audience

This manual is intended for users who need to configure the EtherLINQ 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 EtherLINQ firmware release includes a description of the new features and improvements.

- **Proxicast Support Web Site**

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

## Syntax Conventions

- The EtherLINQ may be referred to as the "EtherLINQ", the "device", the "router", or the "system".
- The EtherLINQ's wired Ethernet WAN interface may be referred to as "WAN", "Wired WAN" "Ethernet WAN", "WAN (Ethernet)" or "WAN 1".
- 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.
- The example screens shown in the User's Guide may differ slightly from the actual screens on the EtherLINQ, depending on the firmware version the EtherLINQ 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 adapter or cord for your device.
- Connect the power adapter 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 adapter or cord and do NOT place the product where anyone can walk on the power adapter or cord.
- Do NOT use the device if the power adapter 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 EtherLINQ is Proxicast’s fourth generation of enterprise-grade secure cellular gateways. This series features an embedded LTE cellular modem. The internal modem seamlessly becomes a WAN interface for the EtherLINQ’s router and is fully integrated with all of the EtherLINQ’s security, performance, and management capabilities.

As with its predecessors, the EtherLINQ is loaded with security features including VPN, firewall and access control. The EtherLINQ adds improved throughput and reliability, NAT, port forwarding, DHCP server, an integrated USB Webcam server, serial device server, GPS functionality (in some models) and many other powerful features required for complex and demanding applications.

The EtherLINQ also has a built-in IEEE 802.11 b/g/n WiFi radio that functions as an access point. This allows WiFi devices to securely communicate with the EtherLINQ and access the wired network or Internet.

The EtherLINQ’s all metal construction make it the perfect choice for applications where a high-performance, secure, reliable and rugged cellular router is required.

## 1.1 Key Features

1. **WAN Failover**
   Proxicast’s EtherLINQ supports failover between fixed-line Ethernet (e.g. xDSL/cable modem) WANs and its internal LTE modem offering non-stop network connectivity. Users can define which WAN interface has priority and the parameters for failover and fall-back actions.

2. **IPSec Server & Client**
   The EtherLINQ’s embedded IPSec VPN features allow remote users to make secure connections to devices which normally cannot run VPN software. The EtherLINQ can also establish site-to-site IPSec tunnels to existing corporate VPN servers for enterprise-level data security.

3. **NAT-Router, IP Pass-Through (Bridge) and Virtual Cable Mode Operations**
   The EtherLINQ can be configured as a traditional NAT router serving as a LAN gateway device. Optionally, it can be configured as a Bridge to provide direct Internet connectivity to a single device (Ethernet or WiFi). The EtherLINQ also supports Proxicast’s unique “Virtual Cable Mode” operation – a special virtual private networking technology that tunnels through any intervening network topologies to make devices connected to the EtherLINQ appear as if they are wired directly to devices connected to a remote EtherLINQ (or PocketPORT).

4. **WiFi Access Point**

   The EtherLINQ includes an 802.11 b/g/n compliant access point bridged to its LAN so that both wired the wireless devices can share the EtherLINQ’s WAN connection.

5. **USB Webcam & Serial Device Servers**

   The EtherLINQ includes 2 application servers – one for USB web cameras and one for USB serial devices. Basic video capabilities can be easily added to remote installation; with an RS-232/422 to USB adapter, legacy serial devices can also be accessed.

6. **GPS Server**

   Certain EtherLINQ models include GPS functionality to both serve and push NMEA data streams to geoposition-enabled applications.

7. **Dynamic Feature Control**

   Administrators can enable / disable various EtherLINQ features as necessary for additional security.

8. **Industrial Design**

   Designed specifically for industrial and mobile applications, the EtherLINQ’s rugged steel chassis and Kensington Lock slot provide physical security along with conveniences such as a locking power supply and removable screw-down mounting tabs.

9. **Energy Efficient**

   The EtherLINQ’s low power consumption SOC chip makes it ideal for solar or battery-powered installations, consuming less than 3 W under normal operating conditions.

## 1.2 Package Contents

- 1x EtherLINQ
- 1x 120/240 VAC to 12 VDC Locking Power Adapter
- 2x 5 dBi LTE Antennas (Flat)
- 2x 5 dBi WiFi Antennas (Round)
- 1x SIM Adapter Kit
- 1x 8 GB microSD Card (installed)
- 1x CAT5e Cable
- 4x Rubber Feet
- 1x Mounting Hardware Kit
- 1x Quick Start Guide

# CHAPTER 2: HARDWARE

## 2.1 Front LEDs

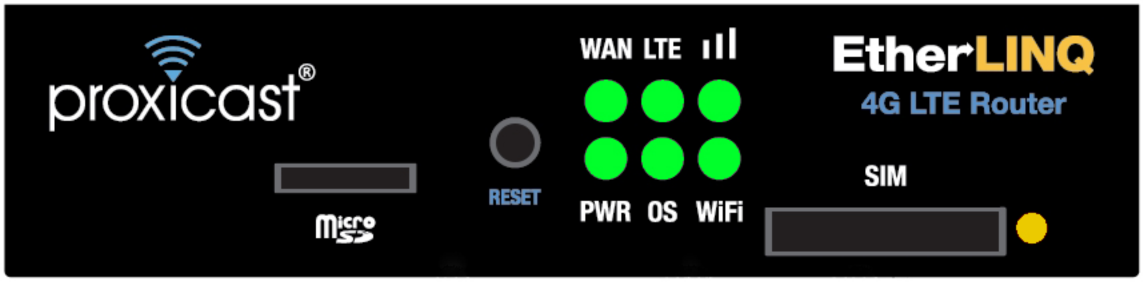


**Figure 1: EtherLINQ Front Panel**

| LABEL | LED STATE | DESCRIPTION |
|---|---|---|
| **MicroSD** | | Slot for microSD cards. Must be formatted for the FAT32 file system. |
| **RESET** | | Press & hold for 2 seconds until the OS LED begins to flash. This places the EtherLINQ in CONFIGURATION MODE and forces the LAN IP = 192.168.1.1:8080 (see *Chapter 16: CONFIGURATION MODE)*<br>Press & hold for 10 seconds until the top row of LEDs flash in sequence. Wait for the OS LED to stay on solid. This returns the EtherLINQ to its factory default settings: LAN IP = 192.168.1.1:8080 ~ Username/Password = admin/1234 |
| **WAN** | Solid | The wired WAN Ethernet port is the active WAN |
| | Flashing | The wired WAN Ethernet port is attempting to connect |
| **LTE** | Solid | The LTE Modem is the active WAN |
| | Flashing | The LTE Modem is attempting to connect |
| **Bars** | Off | The LTE Modem is not receiving a cellular signal |
| | 1 Hz | The LTE signal is POOR |
| | 10 Hz | The LTE signal is GOOD |
| | Solid | The LTE signal is EXCELLENT |
| **PWR** | Solid | Power is on |
| **OS** | Flashing | The EtherLINQ is booting up, performing an internal function or in Configuration Mode |
| | Solid | The EtherLINQ is operating normally |
| **WiFi** | Solid | The EtherLINQ's internal WiFi radio is enabled |
| **SIM** | | Press yellow button on the right to eject the SIM tray. The EtherLINQ uses "mini" (2FF) sized SIMs. Adapters are provided for Micro (3FF) and Nano (4FF) sized SIMs. |

## 2.2 Rear Panel

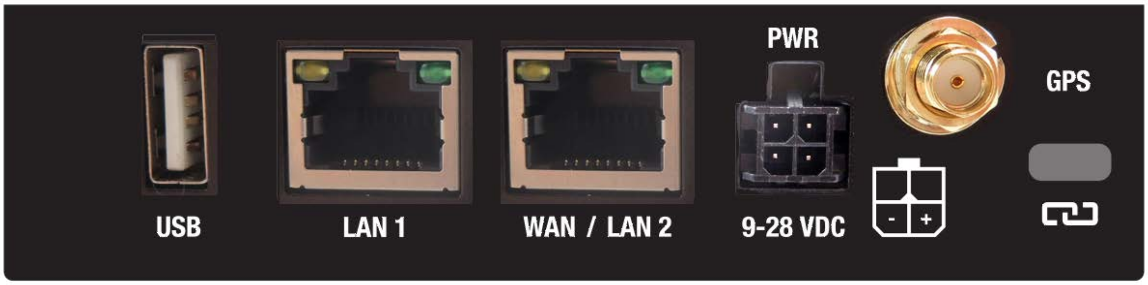


**Figure 2: EtherLINQ Rear Panel**

| LABEL | DESCRIPTION |
|---|---|
| **USB** | USB 2.0 port for webcams, USB serial devices and flash drives |
| **LAN 1** | Connect equipment to this port with an Ethernet cable |
| **WAN / LAN 2** | Connect a cable/DSL modem or other Ethernet-based WAN equipment to this port. Can also be defined as a second LAN port via a software setting. |
| **PWR** | Connect the included 12V DC power adapter to this jack |
| **GPS** | Connect an external GPS antenna to this SMA Female jack |
| **LOCK** | Kensington Lock port |

## 2.3 Hardware Setup

### 2.3.1 Attach Antennas

Attach the flat paddle shaped antennas to the MAIN and AUX SMA Female jacks on the left and right sides of the EtherLINQ along the Gold LTE banner. Attach the 2 round antennas to the MAIN and AUX RP-SMA Female jacks on the left and right sides along the Blue WiFi banner.

### 2.3.2 Install LAN Connection

Plug one end of an Ethernet cable into your computer's network port and the other end into the EtherLINQ's LAN 1 port on the rear panel.

### 2.3.3 Install WAN Connection (optional)

To use an external WAN connection such as a xDSL, cable modem or other wired Ethernet service as either primary or backup, connect an Ethernet cable from the output of the Ethernet WAN device to EtherLINQ's WAN port on the rear panel.

### 2.3.4 Insert SIM Card

Press the eject button to the right of the SIM card holder to eject the tray. Insert an active SIM card with the gold pins facing up and the diagonal notch on the front left. Replace the tray with the pins facing up and insert fully.

### 2.3.5 Power On

Plug one end of the provided power adapter into EtherLINQ's DC power port and the other end into an AC power outlet. After about 60 seconds, the EtherLINQ will be operational when its PWR LED and OS LED are both constantly on.

# CHAPTER 3: ACCESSING THE ETHERLINQ

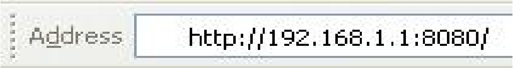
Initial setup of the EtherLINQ can be done using an Ethernet cable or via the internal WiFi Access Point.

Configure your PC to receive 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.

To connect via WiFi, scan for a network named "EtherLINQ-nnnn" where nnnn are the last 4 characters of the EtherLINQ's serial number. The default security mode is WPA2-PSK and the default password is the 8 digit number printed on the EtherLINQ's label.

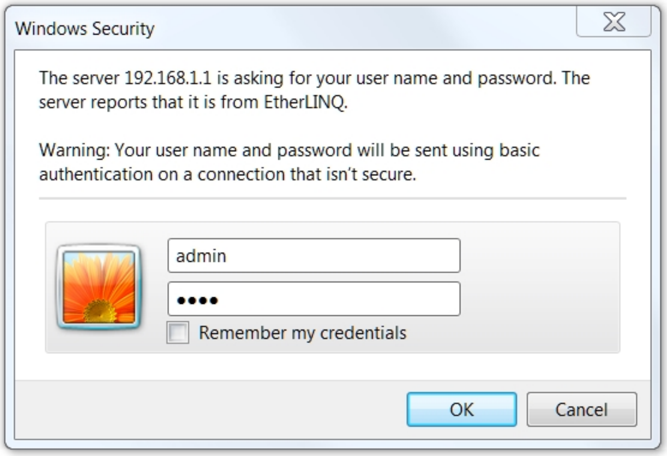
## 3.1 Start-up and Login

Open any web browser. In the address box, enter http://192.168.1.1:8080 or http://*serial#*.etherlinq.net:8080 where *serial#* is the 12 character serial number of the EtherLINQ printed on the bottom label (e.g. 001B39123456).



Address http://192.168.1.1:8080/

When you successfully connect to the configuration interface for EtherLINQ, the login screen will appear (Figure 3). Enter your username as [admin] and your password as [1234]. The EtherLINQ's Status page (Figure 4) will then be displayed. Changing the login password is highly recommended. See the **Advanced** tab.



Windows Security

The server 192.168.1.1 is asking for your user name and password. The server reports that it is from EtherLINQ.

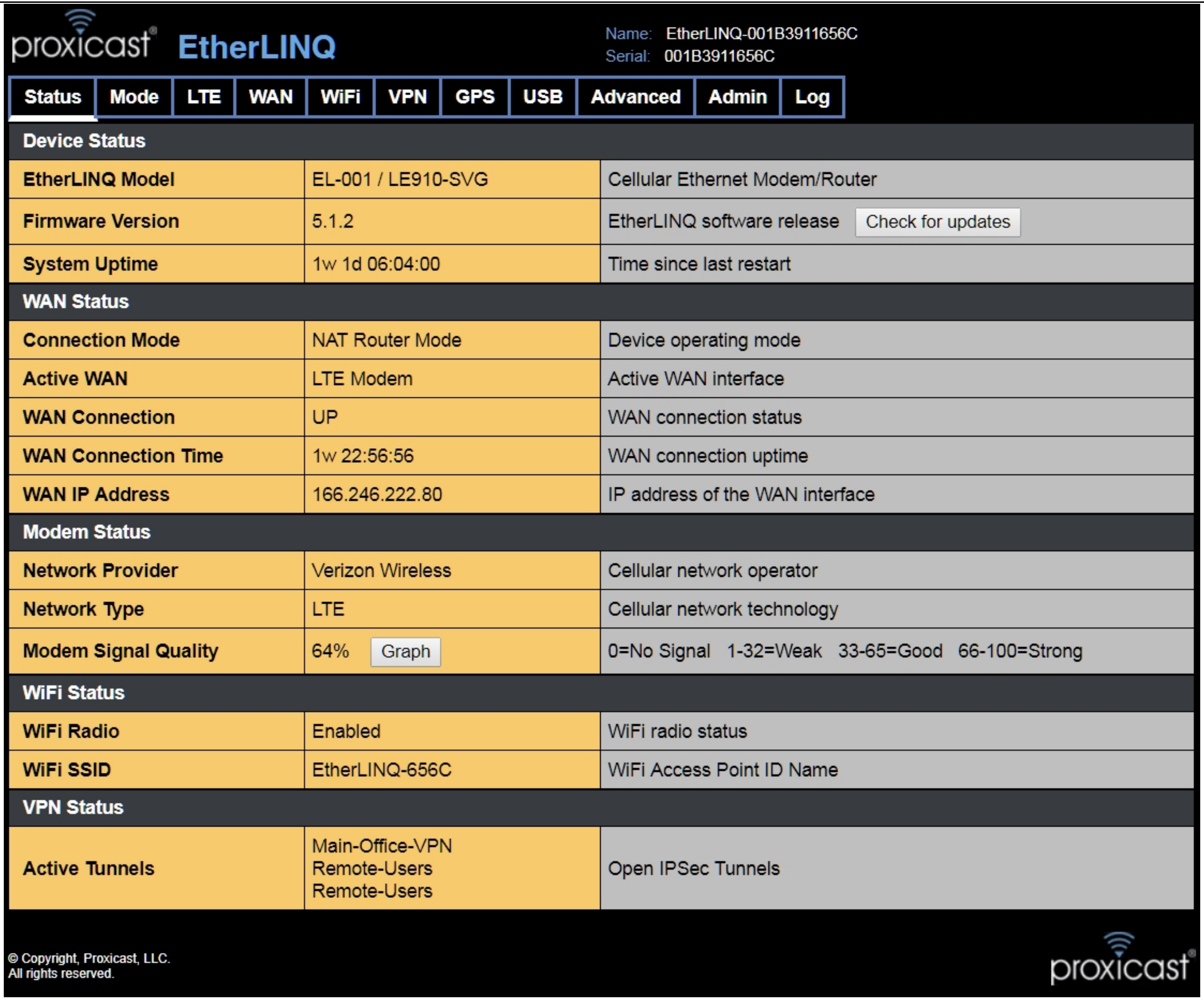
Warning: Your user name and password will be sent using basic authentication on a connection that isn't secure.

admin

••••

□ Remember my credentials

**Figure 3: EtherLINQ Login Screen**



Name: EtherLINQ-001B3911656C
Serial: 001B3911656C

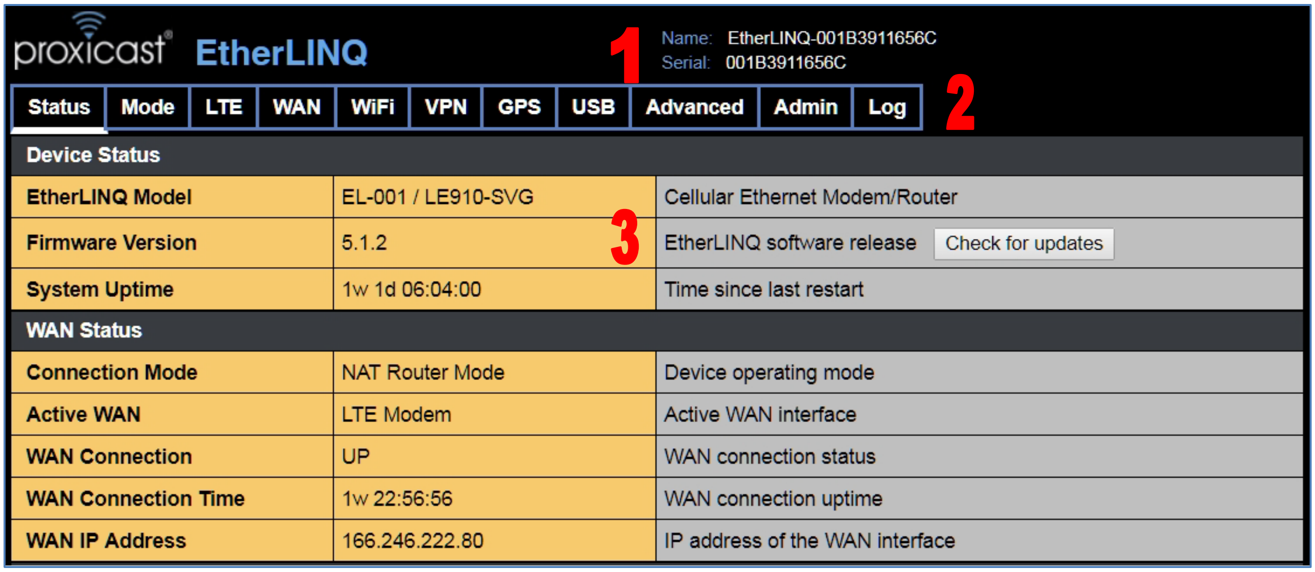
| Device Status | | |
|---|---|---|
| EtherLINQ Model | EL-001 / LE910-SVG | Cellular Ethernet Modem/Router |
| Firmware Version | 5.1.2 | EtherLINQ software release |
| System Uptime | 1w 1d 06:04:00 | Time since last restart |
| **WAN Status** | | |
| Connection Mode | NAT Router Mode | Device operating mode |
| Active WAN | LTE Modem | Active WAN interface |
| WAN Connection | UP | WAN connection status |
| WAN Connection Time | 1w 22:56:56 | WAN connection uptime |
| WAN IP Address | 166.246.222.80 | IP address of the WAN interface |
| **Modem Status** | | |
| Network Provider | Verizon Wireless | Cellular network operator |
| Network Type | LTE | Cellular network technology |
| Modem Signal Quality | 64% | 0=No Signal 1-32=Weak 33-65=Good 66-100=Strong |
| **WiFi Status** | | |
| WiFi Radio | Enabled | WiFi radio status |
| WiFi SSID | EtherLINQ-656C | WiFi Access Point ID Name |
| **VPN Status** | | |
| Active Tunnels | Main-Office-VPN<br>Remote-Users<br>Remote-Users | Open IPSec Tunnels |

**Figure 4: Router Status Screen**

## 3.2 Navigating the User Interface

The EtherLINQ's web management interface is divided into 3 sections (Figure 5):

1. Page Header
2. Navigation Menu Tabs
3. Configuration Parameters



| Device Status | | |
|---|---|---|
| EtherLINQ Model | EL-001 / LE910-SVG | Cellular Ethernet Modem/Router |
| Firmware Version | 5.1.2 | EtherLINQ software release |
| System Uptime | 1w 1d 06:04:00 | Time since last restart |
| **WAN Status** | | |
| Connection Mode | NAT Router Mode | Device operating mode |
| Active WAN | LTE Modem | Active WAN interface |
| WAN Connection | UP | WAN connection status |
| WAN Connection Time | 1w 22:56:56 | WAN connection uptime |
| WAN IP Address | 166.246.222.80 | IP address of the WAN interface |

**Figure 5: EtherLINQ Screen Layout**

The page header always displays the EtherLINQ's System Name and Serial Number. The System Name can be changed by clicking on the current value or on the **Advanced** tab.

Each menu tab is a collection of related system parameters and/or statistics. To select a menu tab, click on the menu tab title. The currently selected tab is indicated with a white bar at the bottom. Chapters 5 through 15 provide details on each of the EtherLINQ's menu options.

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

## 3.3 Top Level Menu Structure

| | |
|---|---|
| **Status** | Provides real-time and historical information about the EtherLINQ's operation |
| **Mode** | Changes the EtherLINQ's Operating Mode, either "NAT Router" (default), "IP Pass-Through" (bridge) or "Virtual Cable" mode |
| **LTE** | Configures the EtherLINQ's embedded LTE modem *(select models)* |
| **WAN** | Configures the EtherLINQ's wired Ethernet WAN port |
| **WiFi** | Configures the EtherLINQ's embedded 802.11 b/g/n WiFi radio *(select models)* |
| **VPN** | Create and manage IPSec VPN settings *(select models)* |
| **GPS** | Enable and configure the EtherLINQ's embedded GPS Server *(select models)* |

| | |
|---|---|
| **USB** | Enable and configure the EtherLINQ's embedded USB Webcam server and USB Serial Port server |
| **Advanced** | Manages advanced settings such as passwords, ports, reboot, DDNS and syslog |
| **Admin** | Includes system management, firmware updates, system utilities, and diagnostic functions |
| **Log** | View the system event log |

**NOTE:** The available menu tabs may vary between EtherLINQ models and depend upon which services have been licensed and activated for each serial number.

# CHAPTER 4: QUICK SETUP

For many non-remote access applications, the EtherLINQ's default settings are sufficient.

| | |
|---|---|
| **LAN IP Address** | 192.168.1.1<br>Subnet mask = 255.255.255.0 |
| **HTTP Management Access** | admin / 1234 on port 8080 |
| **Operating Mode** | NAT Router |
| **LAN DHCP Server** | Enabled |
| **WAN Priority** | 1. Ethernet WAN<br>2. LTE WAN |
| **Ethernet WAN** | DHCP Client Enabled |
| **LTE APN** | Carrier Default |
| **WiFi Access Point** | Enabled<br>SSID = *EtherLINQ-nnnn* where nnnn are the last 4 characters of the serial number<br>WPA2 Password = 8 digit number printed on EtherLINQ label |
| **Security** | All TCP/UDP ports closed. Remote Management disabled |

Press the RESET button for 10 seconds to return the EtherLINQ to these settings.

See Section *A.8: EtherLINQ Default Settings* for a complete list of the EtherLINQ's default values.

## 4.1 Quick Setup

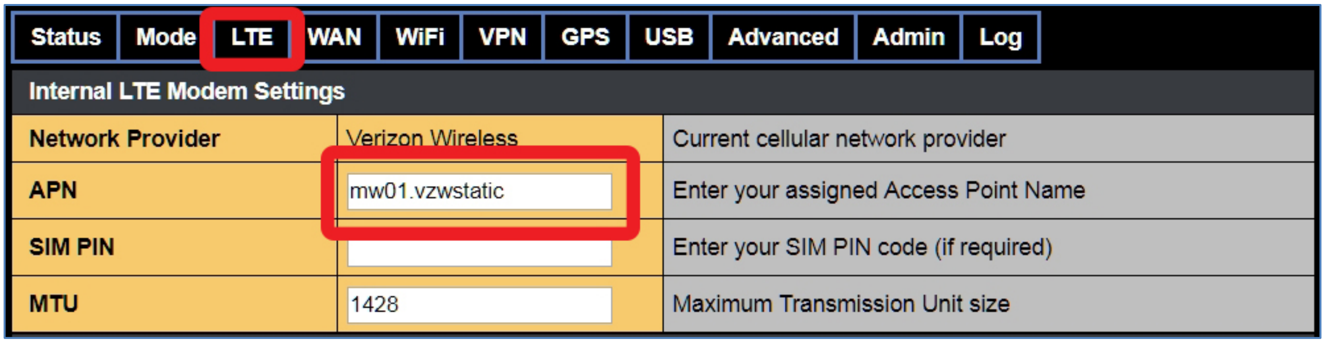
1. Power off the EtherLINQ.
2. For LTE connections: press the yellow eject button next to the SIM slot and remove the SIM tray. Place an active[1] SIM in the tray and carefully insert the tray back into the EtherLINQ.
3. For wired WAN connections: connect an Ethernet cable from your WAN access device (modem) to the EtherLINQ's WAN port.
4. Power on the EtherLINQ.

If you are using your cellular carrier's default APN (e.g. *broadband* for AT&T or *vzwinternet* for Verizon), the

[1] SIMs must be provisioned by the cell carrier prior to use in the EtherLINQ. Check with your cellular service provider regarding the correct service plan and Access Point Name (APN) required for your application. To activate a SIM, you will need the IMEI number of the EtherLINQ modem printed on the bottom label.

EtherLINQ will automatically connect to the cellular network with this value.

If you are using a different APN (e.g. *i2gold* for AT&T, *xxnn.vzwstatic* for Verizon or a custom APN), access the EtherLINQ's management pages via a web browser at http://192.168.1.1:8080. Click on the **LTE** tab and enter the correct APN, then click the **Save & Apply** button at the bottom of the page.



| Internal LTE Modem Settings | | |
|---|---|---|
| Network Provider | Verizon Wireless | Current cellular network provider |
| APN | mw01.vzwstatic | Enter your assigned Access Point Name |
| SIM PIN | | Enter your SIM PIN code (if required) |
| MTU | 1428 | Maximum Transmission Unit size |

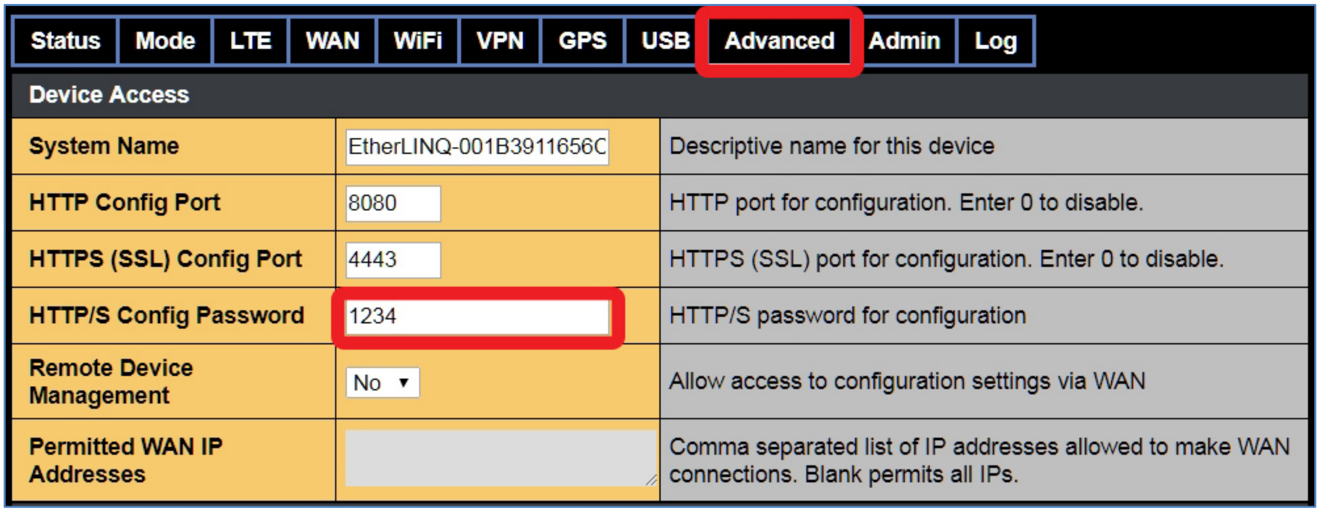
**Figure 6: Set LTE APN Value**

The EtherLINQ will connect to the new APN when it reboots. With the Ethernet WAN and/or LTE Modem configuration complete, DHCP-enabled Ethernet LAN and WiFi devices connected to the EtherLINQ will have access to the Internet.

## 4.2 Password

Proxicast strongly recommends changing the EtherLINQ's default administration password.

To change the EtherLINQ's password, select the **Advanced** tab (Figure 7). Enter the new password (case sensitive) and click the **Save & Apply** button at the bottom of the page.



| Device Access | | |
|---|---|---|
| System Name | EtherLINQ-001B3911656C | Descriptive name for this device |
| HTTP Config Port | 8080 | HTTP port for configuration. Enter 0 to disable. |
| HTTPS (SSL) Config Port | 4443 | HTTPS (SSL) port for configuration. Enter 0 to disable. |
| HTTP/S Config Password | 1234 | HTTP/S password for configuration |
| Remote Device Management | No ▾ | Allow access to configuration settings via WAN |
| Permitted WAN IP Addresses | | Comma separated list of IP addresses allowed to make WAN connections. Blank permits all IPs. |

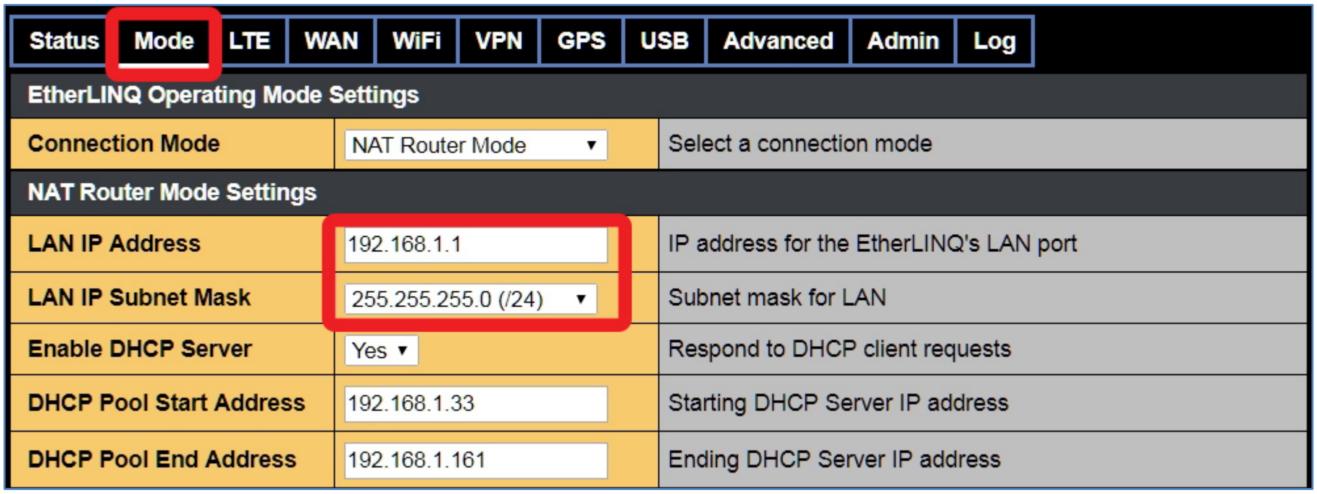
**Figure 7: Changing the Admin Password**

By default, the EtherLINQ's management interface cannot be accessed remotely over a WAN connection. To enable remote access to the management pages, choose the **Remote Device Management** option. When this option is enabled, you must change the EtherLINQ's default password.

**NOTE:** Remote Device Management is not required for remote access to devices connected to the EtherLINQ.

## 4.3 LAN Configuration

To change the EtherLINQ's default LAN subnet (192.168.1.1 / 255.255.255.0), go to the **Mode** tab (Figure 8) and enter the IP address to assign to the EtherLINQ and select the desired subnet mask from the drop-down list. The EtherLINQ's DHCP server will automatically adjust to serve addresses from the new subnet.



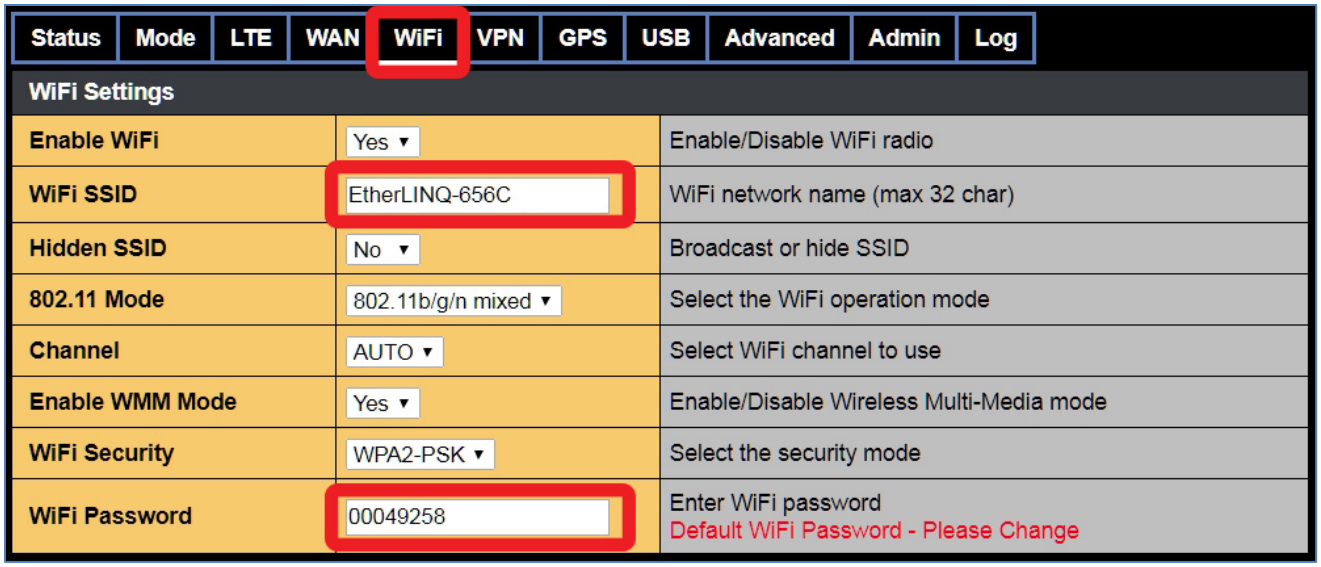
| EtherLINQ Operating Mode Settings | | |
|---|---|---|
| Connection Mode | NAT Router Mode ▾ | Select a connection mode |
| **NAT Router Mode Settings** | | |
| LAN IP Address | 192.168.1.1 | IP address for the EtherLINQ's LAN port |
| LAN IP Subnet Mask | 255.255.255.0 (/24) ▾ | Subnet mask for LAN |
| Enable DHCP Server | Yes ▾ | Respond to DHCP client requests |
| DHCP Pool Start Address | 192.168.1.33 | Starting DHCP Server IP address |
| DHCP Pool End Address | 192.168.1.161 | Ending DHCP Server IP address |

**Figure 8: Ethernet LAN Setup**

## 4.4 WiFi Configuration

Proxicast strongly recommends changing the EtherLINQ's default WiFi password.

To change the SSID value broadcast by the EtherLINQ to WiFi clients and the WPA2 access password, select the **WiFi** tab.



WiFi Settings

| | | |
|---|---|---|
| Enable WiFi | Yes ▾ | Enable/Disable WiFi radio |
| WiFi SSID | EtherLINQ-656C | WiFi network name (max 32 char) |
| Hidden SSID | No ▾ | Broadcast or hide SSID |
| 802.11 Mode | 802.11b/g/n mixed ▾ | Select the WiFi operation mode |
| Channel | AUTO ▾ | Select WiFi channel to use |
| Enable WMM Mode | Yes ▾ | Enable/Disable Wireless Multi-Media mode |
| WiFi Security | WPA2-PSK ▾ | Select the security mode |
| WiFi Password | 00049258 | Enter WiFi password<br>Default WiFi Password - Please Change |

**Figure 9: Changing the WiFi Password**

## 4.5 Accessing Remote Devices

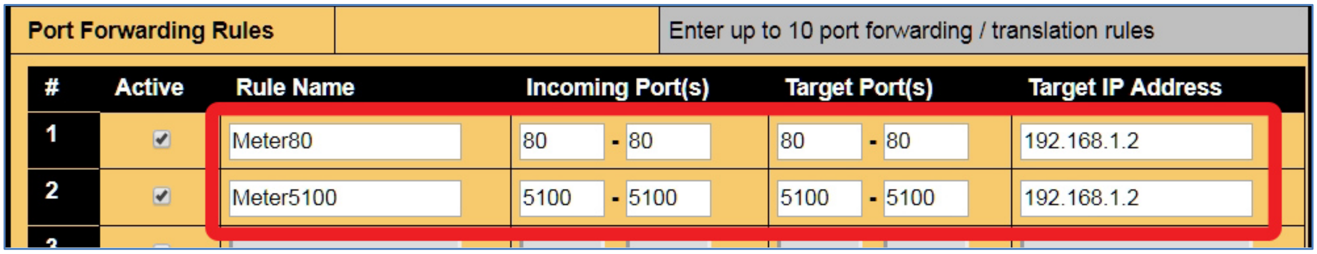
In NAT Mode, accessing devices connected to the EtherLINQ from the Internet requires three things:

1. A publically accessible WAN IP address assigned by your WAN service provider (typically a static IP)
2. A statically assigned private IP address assigned by you on the LAN device to be accessed
3. One or more port-forwarding rules defined in the EtherLINQ to direct incoming traffic to the target device

Contact your WAN/LTE provider regarding the ability for your account to be accessed remotely. See also Section *A.4 Accessing Remote Devices* for other ways to remotely access devices using the EtherLINQ.

Remotely accessible devices in NAT Mode should have their IP address set to a value outside of the EtherLINQ's DHCP pool. The LAN IP address of the EtherLINQ must be the Default Gateway address on the target device.

In the EtherLINQ, define the ports your device uses to listen for connections by selecting the **Mode** tab. Enter the port to be used on the WAN interface of the EtherLINQ (incoming) and the port used by the device you wish to connect to (target), along with the private IP address you assigned to the target device. Repeat this information for each port required by your device.



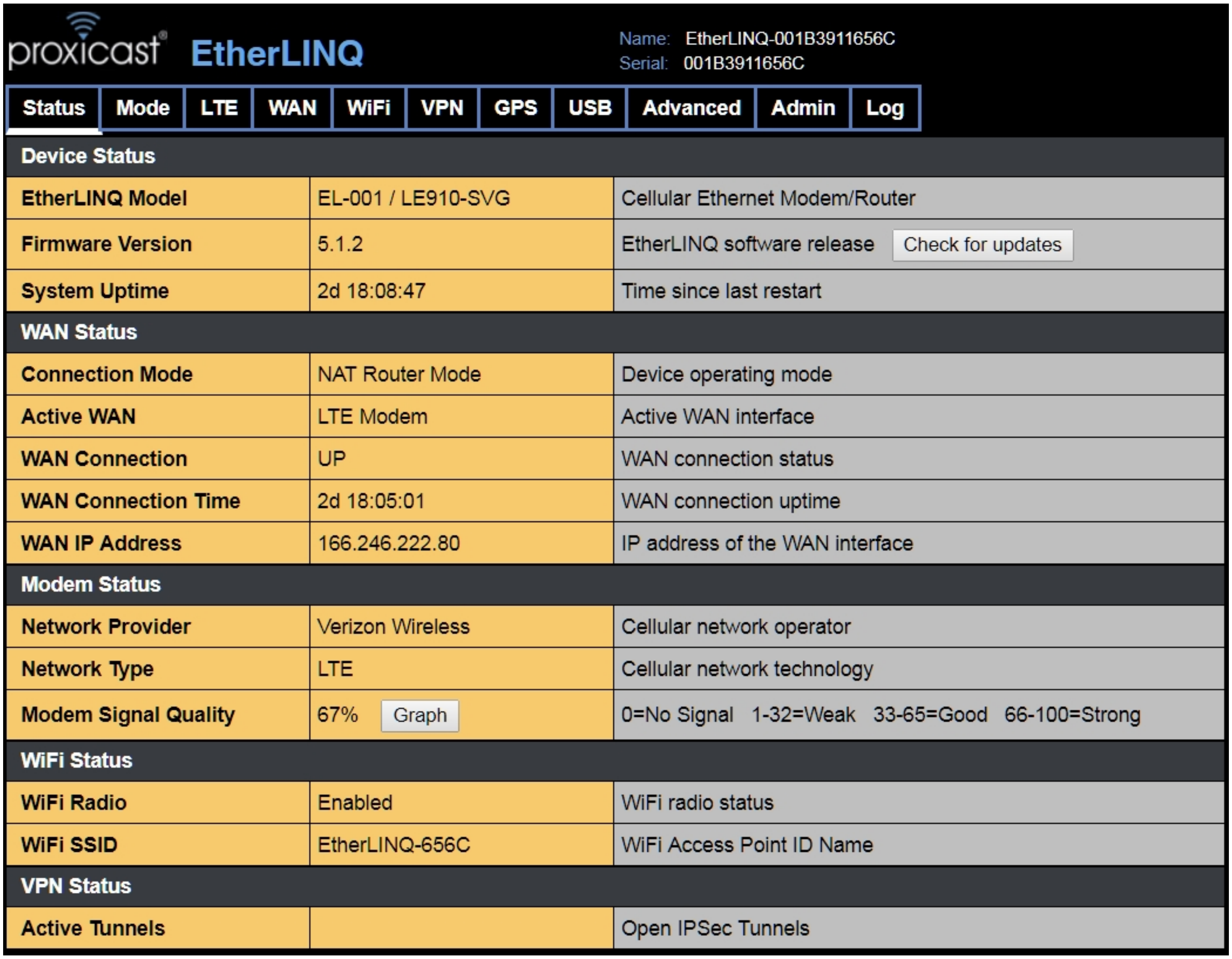
Port Forwarding Rules — Enter up to 10 port forwarding / translation rules

| # | Active | Rule Name | Incoming Port(s) | Target Port(s) | Target IP Address |
|---|---|---|---|---|---|
| 1 | ☑ | Meter80 | 80 - 80 | 80 - 80 | 192.168.1.2 |
| 2 | ☑ | Meter5100 | 5100 - 5100 | 5100 - 5100 | 192.168.1.2 |

**Figure 10: Port Forwarding Rules**

# CHAPTER 5: STATUS TAB

## 5.1 Device Status



Name: EtherLINQ-001B3911656C
Serial: 001B3911656C

| Device Status | | |
|---|---|---|
| EtherLINQ Model | EL-001 / LE910-SVG | Cellular Ethernet Modem/Router |
| Firmware Version | 5.1.2 | EtherLINQ software release Check for updates |
| System Uptime | 2d 18:08:47 | Time since last restart |
| **WAN Status** | | |
| Connection Mode | NAT Router Mode | Device operating mode |
| Active WAN | LTE Modem | Active WAN interface |
| WAN Connection | UP | WAN connection status |
| WAN Connection Time | 2d 18:05:01 | WAN connection uptime |
| WAN IP Address | 166.246.222.80 | IP address of the WAN interface |
| **Modem Status** | | |
| Network Provider | Verizon Wireless | Cellular network operator |
| Network Type | LTE | Cellular network technology |
| Modem Signal Quality | 67% Graph | 0=No Signal 1-32=Weak 33-65=Good 66-100=Strong |
| **WiFi Status** | | |
| WiFi Radio | Enabled | WiFi radio status |
| WiFi SSID | EtherLINQ-656C | WiFi Access Point ID Name |
| **VPN Status** | | |
| Active Tunnels | | Open IPSec Tunnels |

**Figure 11: Router Status**

### 5.1.1 Device Information

| | |
|---|---|
| EtherLINQ Model | Product model name. To the left of the slash is the EtherLINQ hardware version. To the right is the LTE modem module version (if present) |
| Firmware Version | The firmware version this EtherLINQ is running. Click the **Check for Updates** button to find and install new EtherLINQ firmware (see Section *Updating EtherLINQ Firmware*) |
| System Uptime | The period of time EtherLINQ has been running since its last restart |

### 5.1.2 WAN Status

| | |
|---|---|
| Connection Mode | The EtherLINQ's current operating mode |
| Active WAN | Which of the WAN interfaces is currently responsible for routing traffic |
| WAN Connection | The status (UP/DOWN) of the currently active WAN |
| WAN Connection Time | The amount of time the currently active WAN has been routing traffic |
| WAN IP Address | The public facing IP address of the currently active WAN interface |

### 5.1.3 Modem Status

| | |
|---|---|
| Network Provider | The name of the cellular service provider currently serving the EtherLINQ's internal LTE modem |
| Network Type | The type of cellular service currently available (LTE, UMTS, GSM) |
| Modem Signal Quality | An aggregate measure of the strength and quality of the signal reaching the LTE modem. Click the **GRAPH** button to see more details and a history of the signal environment (see below). |

### 5.1.4 WiFi Status

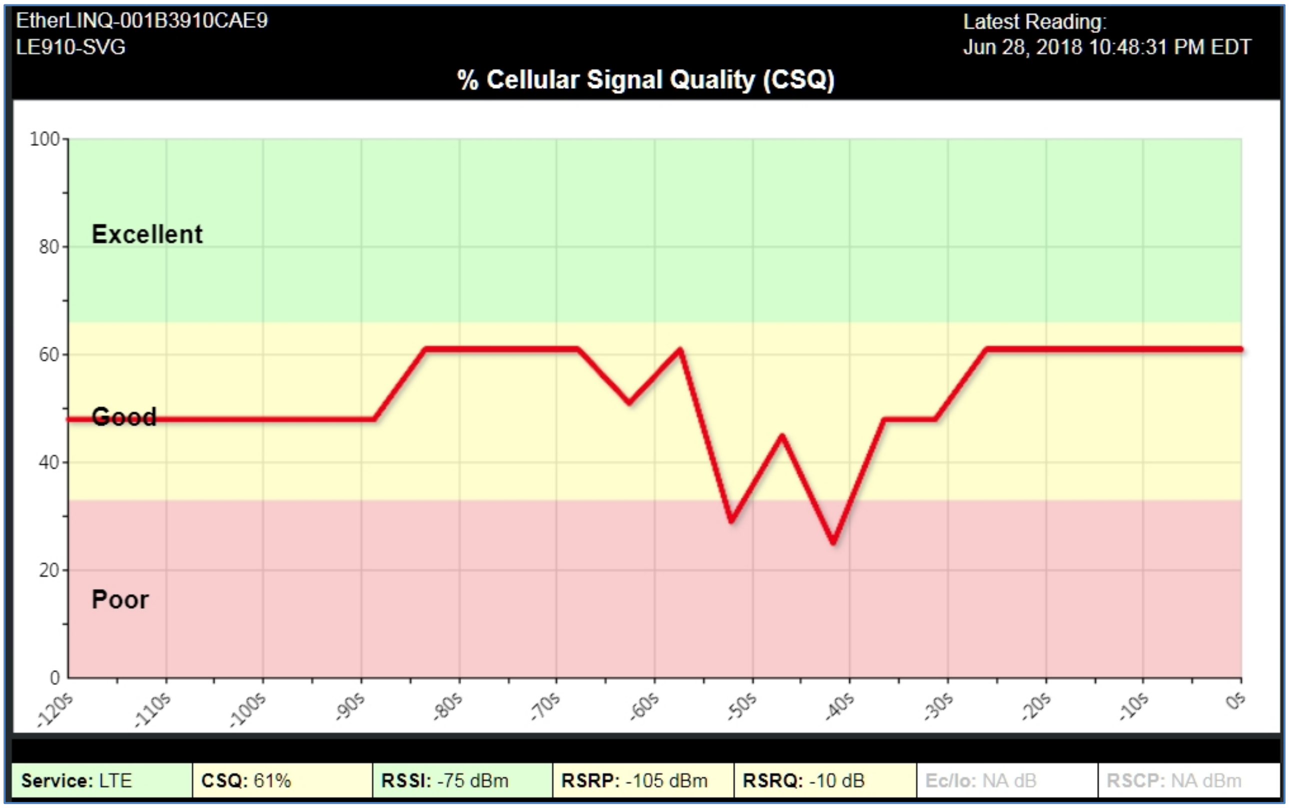
| | |
|---|---|
| WiFi Radio | Whether the EtherLINQ's WiFi radio is enabled or disabled |
| WiFi SSID | SSID of the EtherLINQ |

### 5.1.5 VPN Status

| | |
|---|---|
| Active Tunnels | Names of the currently active IPSec tunnels to/from this EtherLINQ |

## 5.2 Modem Signal Quality Graph

Click on the **Graph** button next to Modem Signal Quality and the graph in Figure 12 is displayed.



EtherLINQ-001B3910CAE9
LE910-SVG

Latest Reading:
Jun 28, 2018 10:48:31 PM EDT

% Cellular Signal Quality (CSQ)

**Service:** LTE | **CSQ:** 61% | **RSSI:** -75 dBm | **RSRP:** -105 dBm | **RSRQ:** -10 dB | **Ec/Io:** NA dB | **RSCP:** NA dBm

**Figure 12: Modem Signal Quality Graph**

The Modem Signal Quality Graph shows the current cellular signal environment for the EtherLINQ along with the overall quality measurement for the trailing 2 minutes with readings taken every 5 seconds. The graph is useful for positioning antennas and troubleshooting cellular signal related issues.

The graph is color coded to quickly indicate if a parameter is in the Excellent, Good, or Poor range. In general, reliable connection (and best throughput performance) is achieved when the signal quality remains in the Excellent or Good zones. Some fluctuation is normal.

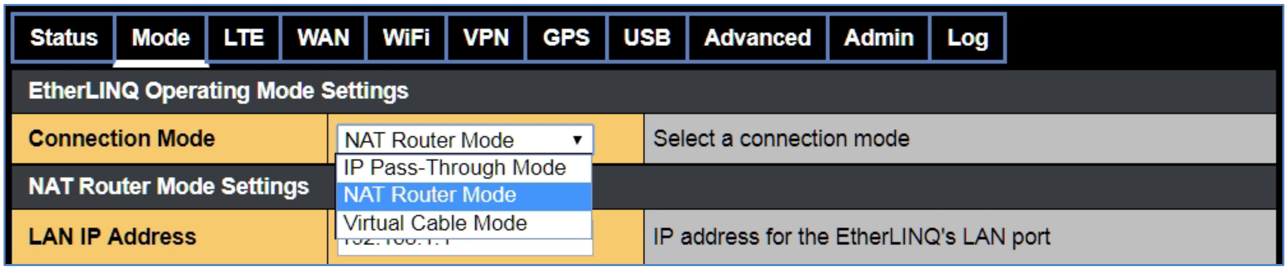
The parameters at the bottom of the graph are:

| | |
|---|---|
| Service | Radio technology currently active. Options are LTE, UMTS, GSM, UNKNOWN. |
| CSQ | Cellular Signal Quality. A composite measure of the overall signal quality expressed as a percentage. |
| RSSI | Received Signal Strength Indicator. A measurement of the amount of power in |

| | |
|---|---|
| | total radio signal received by the modem. Range is -113 dBm to -51 dBm. |
| RSRP | Reference Signal Received Power. The average power received by the modem from a single cell specific reference signal resource element spread over the full bandwidth. It is a signal strength measurement for LTE service and is not displayed for other services. Range is -140 dBm to -44 dBm. |
| RSRQ | Reference Signal Received Quality. A measurement that indicates the quality of the received reference signal relative to the RSSI and the number of resource blocks. It is a signal quality measurement for LTE service and is not displayed for other services. Range is -19.5 dB to -3 dB. |
| Ec/Io | Energy per code bit / Interference. The ratio of received power of the carrier (pilot) signal to the noise + interference. It is a signal-to-noise ratio used to measure quality of UMTS service. Ec/Io is not displayed for other services. Range is -24 dB to 0 dB. |
| RSCP | Reference Signal Code Power. Denotes the power measured by a receiver on a particular physical communication channel. It is a signal strength measurement for UMTS service and is not displayed for other services. Range is -120 dBm to -25 dBm. |

# CHAPTER 6: MODE TAB

EtherLINQ has three modes of operation which determine how the EtherLINQ behaves with regard to Internet access for LAN devices.



EtherLINQ Operating Mode Settings

| | | |
|---|---|---|
| Connection Mode | NAT Router Mode ▼ | Select a connection mode |

NAT Router Mode Settings

| | | |
|---|---|---|
| LAN IP Address | 192.168.1.1 | IP address for the EtherLINQ's LAN port |

**Figure 13: Connection Mode**

1. **NAT Router Mode** (default)

   The EtherLINQ operates as a standard Network Address Translation Router, providing private addresses via DHCP to attached Ethernet/WiFi devices and translating the IP of these devices to the single shared IP of the EtherLINQ’s WAN interface. For in-bound remote access, port forwarding/translation rules must be created for each desired port/IP combination. NAT Mode is also used when IPSec VPN connections are required.

2. **IP Pass-Through Mode**

   This mode causes the EtherLINQ to function as a “bridge” instead of a router. In this mode, the IP address of the active WAN interface is passed through to a single Ethernet (or WiFi) device attached to the EtherLINQ. The first device to request an IP from the EtherLINQ will be assigned the WAN IP, so IP Pass-Through Mode should only be used when a single device requires Internet access.

3. **Virtual Cable Mode**

   Virtual Cable Mode creates a fully encrypted point-to-point connection between two or more EtherLINQs’ and/or Proxicast PocketPORT’s. In this virtual private networking (VPN) mode, the devices connected to each of the EtherLINQ’s or PocketPORTs appear to be directly connected via an Ethernet cable. See Section *6.3 Virtual Cable Mode.*

## 6.1 NAT Router Mode

The EtherLINQ provides Network Address Translation (NAT) services to protect private LAN IP addresses from access by users on the external WAN. NAT Router Mode is the EtherLINQ's default operating mode.

NAT Router Mode allows multiple Ethernet and WiFi devices to share the EtherLINQ's active WAN interface. Up to 2 Ethernet devices can be directly connected to the EtherLINQ along with multiple WiFi devices. An Ethernet switch can also be connected to one of the EtherLINQ's LAN ports to add additional devices.

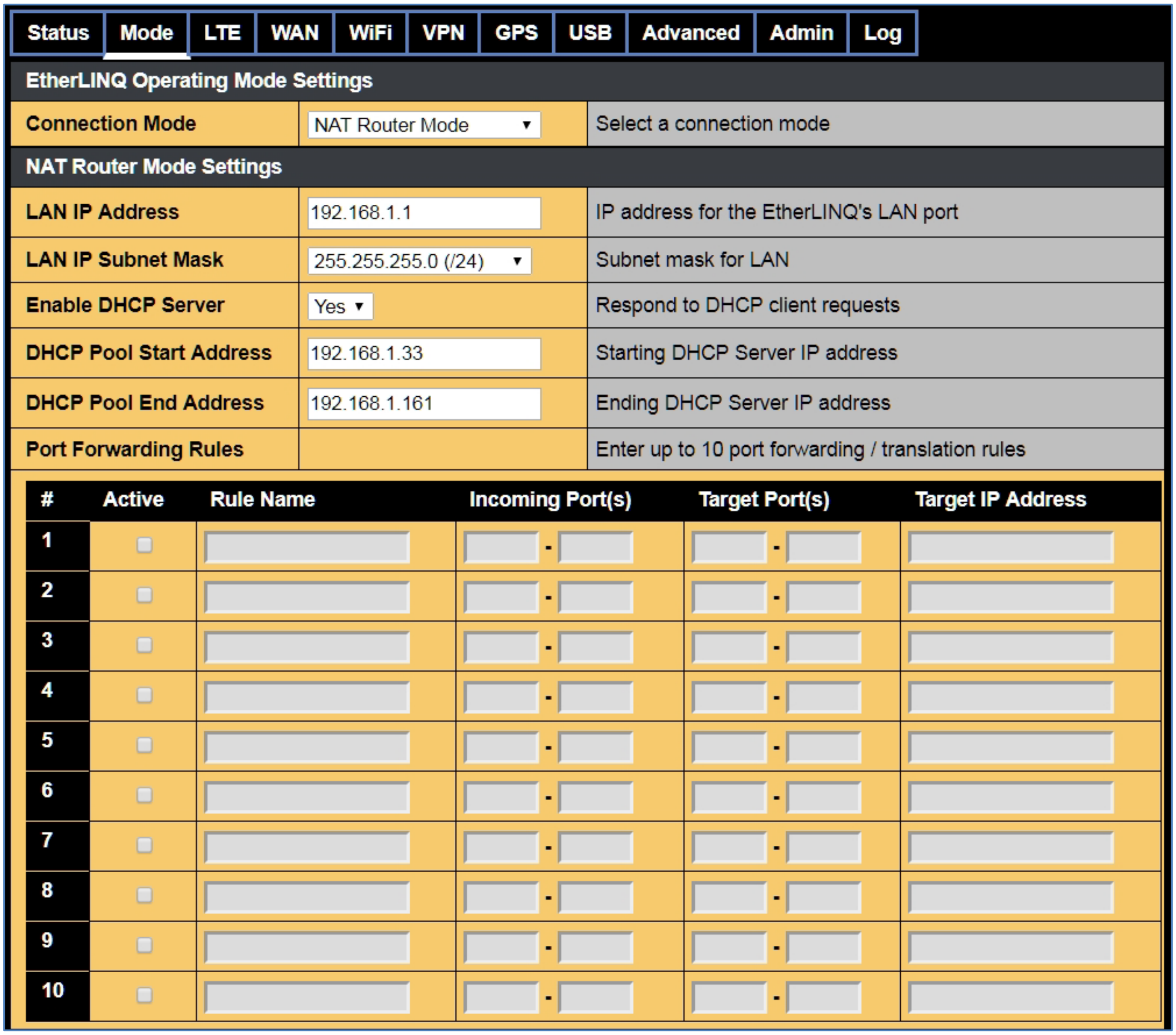
If necessary, the EtherLINQ's LAN IP address and DHCP Server settings can be changed to match those required for your application.

**NOTE:** Regardless of the NAT Router Mode LAN IP Address setting, the EtherLINQ's LAN IP address will always be 192.168.1.1 when in Configuration Mode (See *Chapter 16: CONFIGURATION MODE)*.

By default, the EtherLINQ blocks all incoming traffic from the WAN interfaces. Port-Forwarding is a technique to selectively allow access to selected devices and services on the private LAN. The EtherLINQ supports both Port Forwarding and Port Translation. These features are integrated with the EtherLINQ's firewall. 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 or DNS name. You can assign a specific external port range to a local server (IP address). Furthermore, you can specify a different internal port range to be associated with external ports in a port forwarding rule. When the EtherLINQ 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.

**NOTE:** To allow remote administrative access to the EtherLINQ, you must enable Remote Device Management on the **Advanced** tab (See *Chapter 13: ADVANCED TAB*). No port forwarding rules are required.



EtherLINQ Operating Mode Settings

| | | |
|---|---|---|
| Connection Mode | NAT Router Mode ▾ | Select a connection mode |

NAT Router Mode Settings

| | | |
|---|---|---|
| LAN IP Address | 192.168.1.1 | IP address for the EtherLINQ's LAN port |
| LAN IP Subnet Mask | 255.255.255.0 (/24) ▾ | Subnet mask for LAN |
| Enable DHCP Server | Yes ▾ | Respond to DHCP client requests |
| DHCP Pool Start Address | 192.168.1.33 | Starting DHCP Server IP address |
| DHCP Pool End Address | 192.168.1.161 | Ending DHCP Server IP address |
| Port Forwarding Rules | | Enter up to 10 port forwarding / translation rules |

| # | Active | Rule Name | Incoming Port(s) | Target Port(s) | Target IP Address |
|---|---|---|---|---|---|
| 1 | ☐ | | - | - | |
| 2 | ☐ | | - | - | |
| 3 | ☐ | | - | - | |
| 4 | ☐ | | - | - | |
| 5 | ☐ | | - | - | |
| 6 | ☐ | | - | - | |
| 7 | ☐ | | - | - | |
| 8 | ☐ | | - | - | |
| 9 | ☐ | | - | - | |
| 10 | ☐ | | - | - | |

**Figure 14: NAT Router Mode**

| | |
|---|---|
| LAN IP Address | Sets the internal LAN IP address of the EtherLINQ.<br>Note: The EtherLINQ's built-in DHCP Server will automatically adjust to the IP address and subnet entered. |
| LAN IP Subnet Mask | Select the appropriate subnet mask from the list. |
| Enable DHCP Server | The DHCP Server function can be enabled or disabled. If disabled, you must statically assign an IP address, subnet mask and default gateway (the LAN IP of the EtherLINQ) to all connected LAN/WiFi devices. |
| DHCP Pool Start Address | The DHCP starting IP address offered by the DHCP Server. |
| DHCP Pool End Address | The DHCP ending IP address offered by the DHCP Server.<br>**NOTE:** The EtherLINQ does not offer IP addresses in any particular order within the defined pool. |

| | |
|---|---|
| Port Forwarding Rules | Up to 10 Port Forwarding / Port Translation rules can be defined to direct where incoming traffic on various ports is routed. The EtherLINQ routes both TCP and UDP traffic on the designated ports. There is only one set of Port Forwarding Rules – the rules are applied to whichever WAN interface is currently active. |
| Active | Check this box to make the rule active and unlock the rule's data fields. Inactive rules will not be enforced but are saved in the EtherLINQ's configuration. |
| Rule Name | Any alphanumeric string used to identify the rule for your own purposes. |
| Incoming Port(s) | Define the port number(s) that will be exposed on the WAN interface. You will append one of these port numbers after the EtherLINQ's WAN IP or DDNS in order to access the corresponding LAN / WiFi device's IP address.<br>The incoming and target port ranges must contain the same number of ports, but can be different to enable port translation. Incoming port ranges may not overlap. |
| Target Port(s) | By default, the Incoming Ports are copied to the Target Ports. To perform "port translation" and have the EtherLINQ route traffic from an incoming port to a different port on the target device, set the Target Ports to the ports that the target device is actually listening on. |
| Target IP Address | The IP address of the LAN device to receive incoming traffic. Assigning a static IP address to port forwarding targets is recommended since DHCP does not guarantee the same IP address each time. The target device must also have its default gateway value set to the EtherLINQ's LAN IP address.<br>**NOTE:** The number of Incoming Ports and Target Ports much match on each rule and may not overlap with any other rules or include any of the EtherLINQ reserved ports (see Section *EtherLINQ Default Settings, page 75*). |

**NOTE:** Each port forwarding rule applies to both TCP and UDP traffic on the indicated port number.

## EXAMPLE:

Consider the network configuration shown in Figure 15 with the EtherLINQ operating in NAT Router Mode. To remotely access either the Meter or Controller from the Internet, port-forwarding rules must be configured.

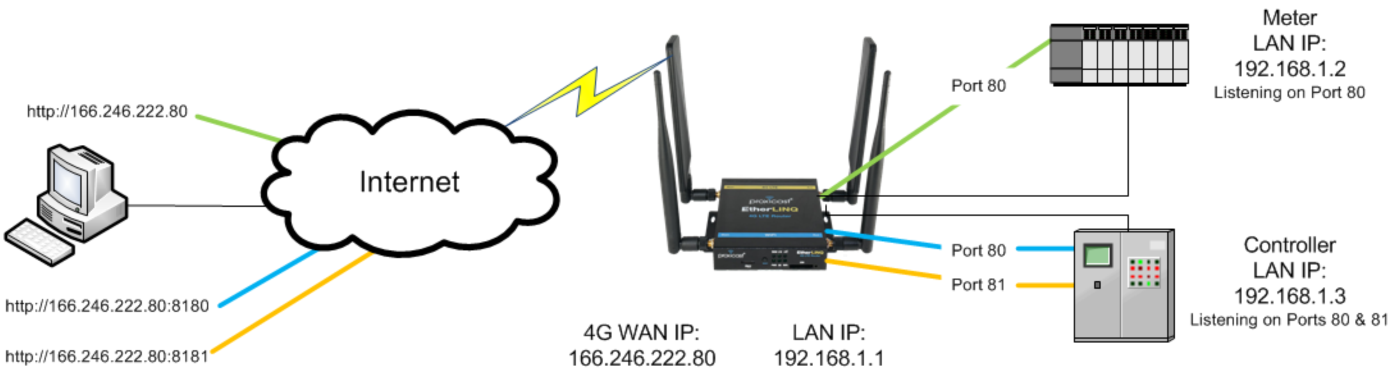
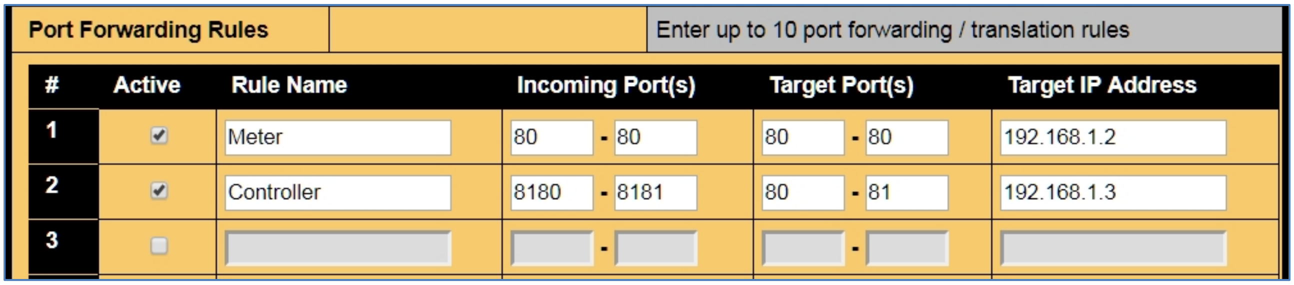


**Figure 15: NAT Router Mode Example**

Figure 16 shows the two required Port Forwarding Rules. Rule # 1 named “Meter” is for a device which has an embedded web server listening on port 80. This is the only port needed for this device, so the Incoming and Target ports are all set to “80”. A Target IP Address of 192.168.1.2 was statically assigned to the meter along with a subnet mask of 255.255.255.0 and a default gateway of 192.168.1.1 (see LAN IP settings above).



Port Forwarding Rules

Enter up to 10 port forwarding / translation rules

| # | Active | Rule Name | Incoming Port(s) | Target Port(s) | Target IP Address |
|---|---|---|---|---|---|
| 1 | ☑ | Meter | 80 - 80 | 80 - 80 | 192.168.1.2 |
| 2 | ☑ | Controller | 8180 - 8181 | 80 - 81 | 192.168.1.3 |
| 3 | ☐ |  | - | - |  |

**Figure 16: Port Forwarding & Translation Rules**

Rules #2 is for a programmable logic controller that has 2 listening ports. One is for an embedded web server listening on port 80; the other is a control interface on port 81. Since port 80 is already in use by the meter’s web server (rule #1), a different range of incoming ports to use must be defined, and the EtherLINQ must translate those ports into the ones used by the controller. In the example, ports 8180 and 8181 get translated to ports 80 and 81 respectively when sent to the controller at 1921.68.1.3.

To access the Meter, use the EtherLINQ’s public IP address. To access the Controller, use the EtherLINQ’s public IP address with either :8180 or :8181 appended to it depending on which Controller port you need to access (e.g. http://166.246.222.80:8180).

## 6.2 IP Pass-Through (Bridge) Mode

IP Pass-Through / Bridge Mode is the simplest way to use the EtherLINQ. In this mode, the EtherLINQ is essentially “invisible” to the Ethernet devices attached to it. The EtherLINQ makes a WAN connection and passes the IP address received from the WAN interface to the device attached to the LAN Ethernet port. Typically, only 1 Ethernet device is attached to the EtherLINQ when operating in IP Pass-Through/Bridge Mode - the first device to request an IP from the EtherLINQ will be assigned the WAN IP.

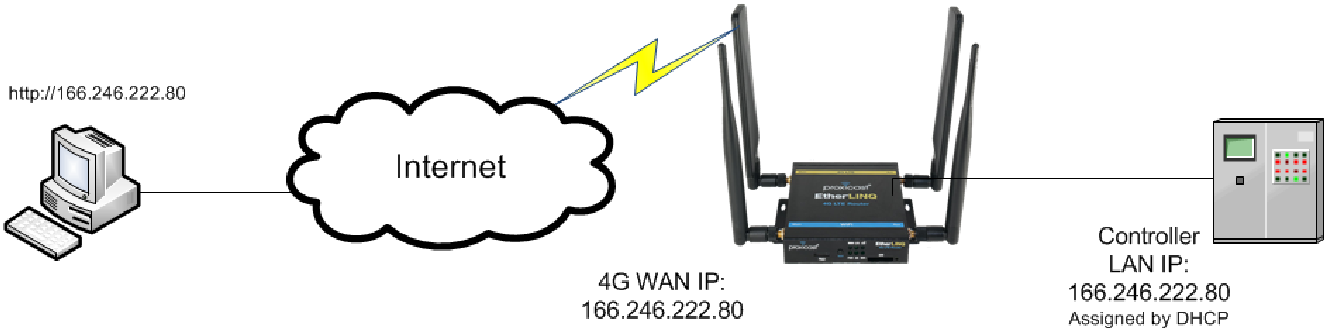
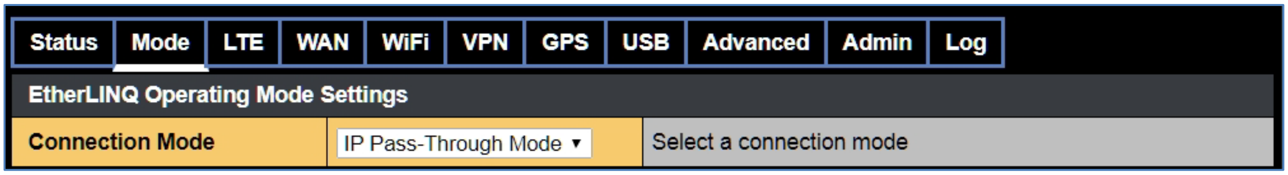


**Figure 17: IP Pass-Through Mode Example**

Configure the attached Ethernet device for DHCP to automatically receive its IP configuration information (IP address, subnet mask and default gateway)[2]. Once the EtherLINQ receives the IP information from the WAN, it will respond to DHCP requests from the Ethernet device with the cellular IP data. You may need to release and renew the Ethernet device’s IP setting in order to obtain the correct cellular values.

If the WAN IP changes, the Ethernet port’s Link Status line is “winked” to signal the attached LAN device that it needs to request a new IP address from the EtherLINQ.

Use IP Pass-Through Mode when you simply want to connect a single Ethernet device to the Internet and have the Ethernet device receive an IP address from the cellular network. It is also possible to pass the WAN IP address to a WiFi attached device. Remotely access the Ethernet device using the public IP address of the EtherLINQ.



EtherLINQ Operating Mode Settings

| | | |
|---|---|---|
| Connection Mode | IP Pass-Through Mode ▼ | Select a connection mode |

**Figure 18: IP Pass-Through Mode**

[2] A common question is “where does the static IP address from the cellular provider get entered?” The static LTE address is not entered into either the EtherLINQ or the target device – all cellular “static IP” addresses are issued via DHCP, so the target device must be set to request an IP address when the EtherLINQ is operating in IP Pass-Through Mode.

**NOTE:** Port Forwarding and Firewall rules do not apply in IP Pass-Through Mode; the LAN device is fully exposed to the WAN interface, so ensure that the device has the necessary security protections installed.

## 6.3 Virtual Cable Mode

A unique feature of the EtherLINQ is “Virtual Cable Mode” (VCM). In this mode, two or more EtherLINQ’s (and/or PocketPORT’s) act as a very long virtual Ethernet cable. The intervening WAN networks are completely transparent; the ends appear to be directly connected via cable. Any application that works over a direct Ethernet cable also works over Virtual Cable.

Virtual Cable Mode is especially useful for software applications that expect external LAN hardware to be on the same physical Ethernet segment (i.e. “flat networks”). For example, some PLC programming and monitoring applications broadcast probe packets to locate their associated hardware. These packets typically do not traverse routed networks or the Internet, but will be forwarded to the remote equipment when it is connected via Virtual Cable Mode, even across a cellular Internet connection.

The EtherLINQ uses end-to-end encryption on all Virtual Cable connections. Networks are protected by a shared password (pre-shared key), known only to the participating nodes. No software needs to be installed on any end device, so users can comply with security policies regarding third-party software installations. Closed systems such as cameras and PLC’s can have fully protected connections over the Internet even though they can’t run VPN software. Virtual Cable Mode is completely self-contained and autonomous.

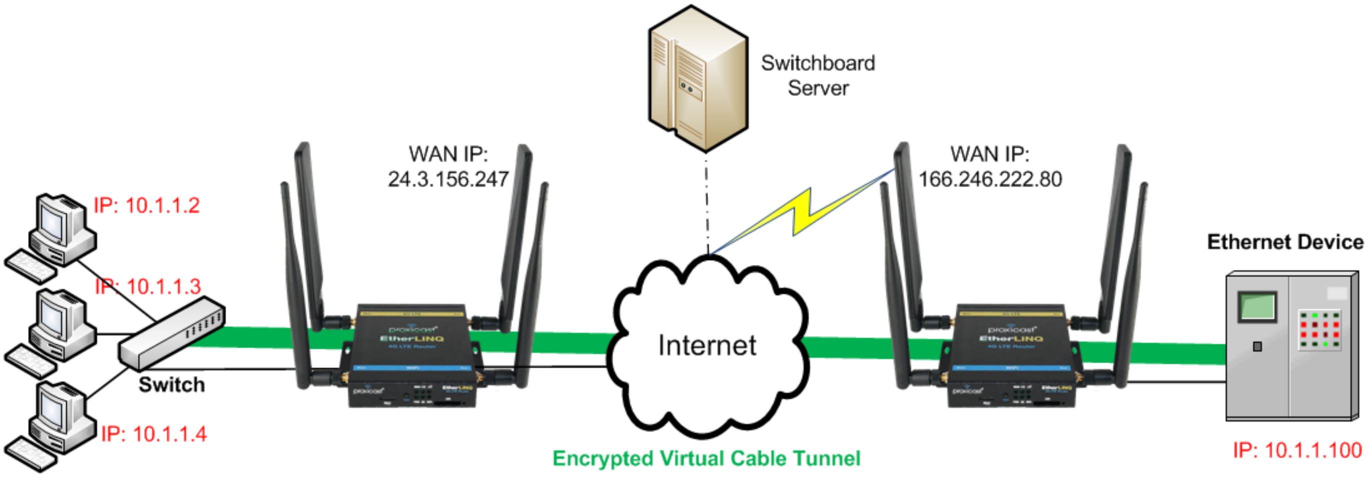


**Figure 19: Virtual Cable Mode Example**

Unlike traditional VPNs where the networks on each side of a connection are in different subnets, the network addresses on both sides of a Virtual Cable connection must be in the same subnet (see red IP addresses in Figure 19). When in Virtual Cable Mode, LAN IP, DHCP and Port-Forwarding settings from NAT Router Mode do not apply.

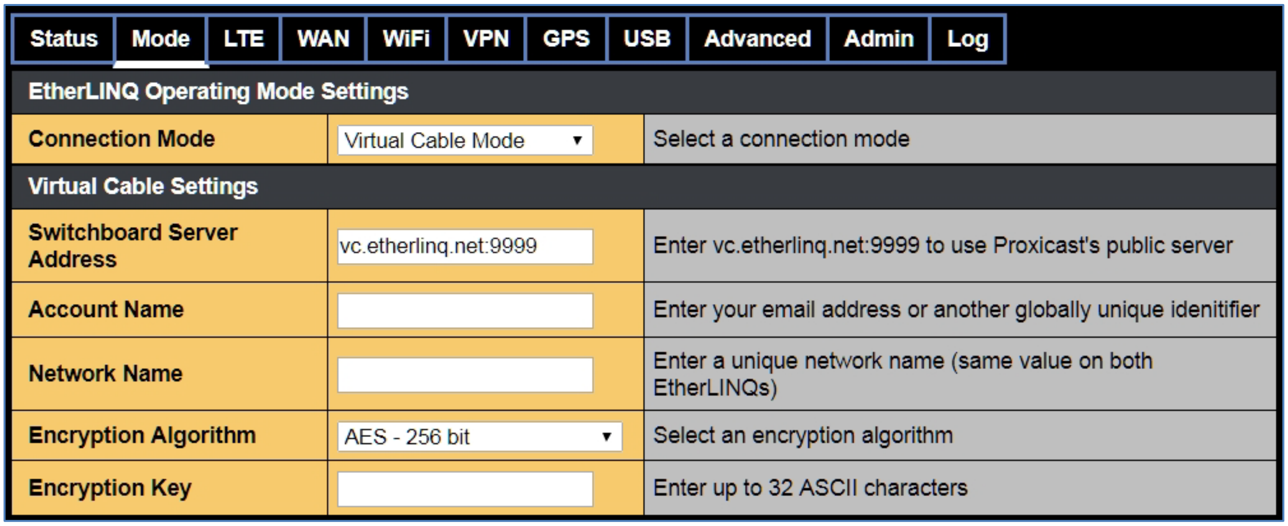
Virtual Cable Mode operates primarily as a peer-to-peer network connection. A central “Switchboard” service is used as a directory lookup so that devices can locate each other initially. Once a two-way connection is established, traffic moves directly between the peers. In instances where firewalls block inbound traffic between the devices, the Switchboard server acts as a “relay” by creating reverse tunnels to the end-points and routing traffic through the tunnels. The Switchboard server does not hold a copy of the encryption key, so data packets remain fully secure until they reach their final destination.

Proxicast maintains a public virtual cable switchboard server (vc.etherlinq.net) for use by our customers. All customer data and connections are encrypted and secured and the high-performance switchboard server has a 150 Mbps connection to the Internet. Customers connecting a large number of EtherLINQ’s to a single Virtual Cable network may wish to license the Switchboard server for hosting their own network.

Devices attached to routers operating in Virtual Cable Mode are only accessible by other devices that are part of the same Virtual Cable network; they cannot be accessed remotely via the Internet. One-to-One, One-to-Many, and Many-to-Many connections are supported. All Virtual Cable routers that need to communicate with each other must have the same Account Name, Network Name, Encryption Type and Key.

**NOTE:** All Ethernet frames and broadcast traffic are passed to all nodes of the network. Connecting a large number of devices to Virtual Cable routers can create high WAN usage which may impact cost & speed.

The EtherLINQ’s Virtual Cable Mode is fully interoperable with Virtual Cable Mode on Proxicast’s PocketPORT.



| | | |
|---|---|---|
| **EtherLINQ Operating Mode Settings** | | |
| **Connection Mode** | Virtual Cable Mode ▼ | Select a connection mode |
| **Virtual Cable Settings** | | |
| **Switchboard Server Address** | vc.etherlinq.net:9999 | Enter vc.etherlinq.net:9999 to use Proxicast's public server |
| **Account Name** | | Enter your email address or another globally unique idenitifier |
| **Network Name** | | Enter a unique network name (same value on both EtherLINQs) |
| **Encryption Algorithm** | AES - 256 bit ▼ | Select an encryption algorithm |
| **Encryption Key** | | Enter up to 32 ASCII characters |

**Figure 20: Virtual Cable Mode**

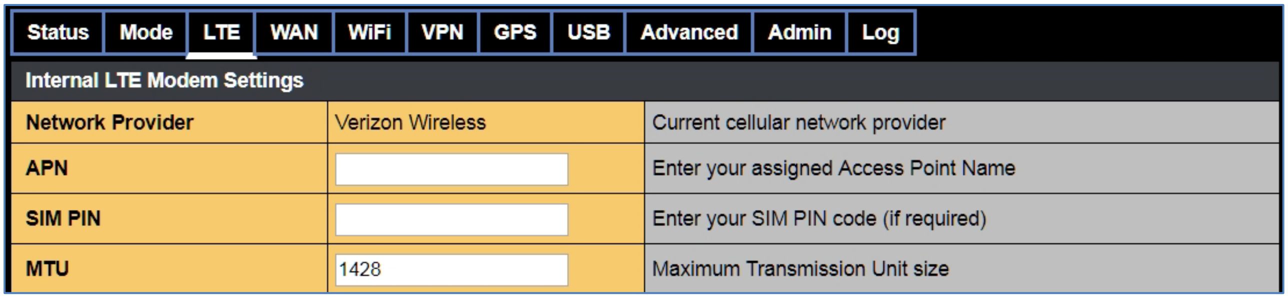
| | |
|---|---|
| Switchboard Server Address | Enter the IP address or FQDN of the Switchboard server and the server's listening port. To use Proxicast's public Switchboard, enter vc.etherlinq.net:9999 |
| Account Name | Any alphanumeric string to identify you uniquely to the Switchboard server. We recommend using your email address. No pre-registration is required; simply enter your selected Account Name. |
| Network Name | Any alphanumeric string to identify the group of devices which are to communicate with each other under your account. Only devices that have the same Network Name can communicate. You may create multiple networks under the same Switchboard account. |
| Encryption Algorithm | Select the Encryption Algorithm to be applied to data packets. AES-256 with an ASCII key is the default. You may also select AES-256 with a 64 hexadecimal key. TwoFish-256 is available for compatibility with Proxicast's PocketPORT devices. |
| Encryption Key | Enter either the ASCII or HEX encryption key to be used. |

**NOTE:** Virtual Cable Mode throughput performance can be increased by not providing a Network Password value on each EtherLINQ. This disables encryption – all data will be transferred between nodes in its native format. All nodes must have the same (or no) Network Password in order to communicate.

# CHAPTER 7: LTE TAB

The **LTE** tab configures the EtherLINQ's internal LTE modem. In many cases, the EtherLINQ is able to automatically determine the correct LTE settings based on the cellular carrier and SIM. The default settings can be overridden on this screen.

## 7.1 LTE Setup



| Internal LTE Modem Settings | | |
|---|---|---|
| Network Provider | Verizon Wireless | Current cellular network provider |
| APN | | Enter your assigned Access Point Name |
| SIM PIN | | Enter your SIM PIN code (if required) |
| MTU | 1428 | Maximum Transmission Unit size |

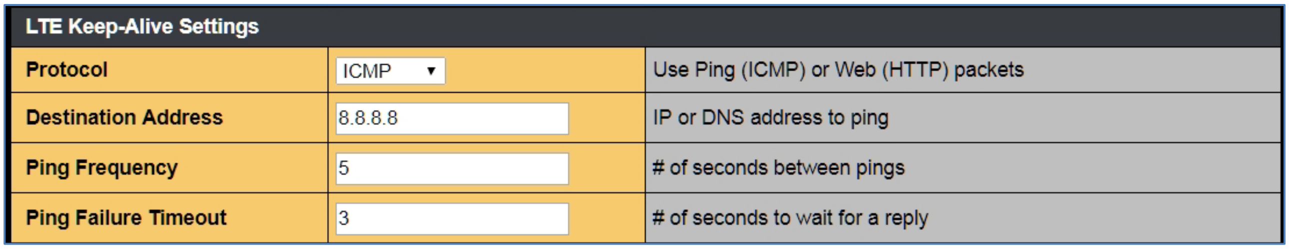
**Figure 21: LTE Settings**

| | |
|---|---|
| Network Provider<br>(read only) | The name of the cellular service provider currently providing service to the EtherLINQ. This value is automatically determined by the LTE module and may change when roaming on to a different carrier. |
| Access Point Name (APN) | Enter the APN string assigned to your SIM by your service provider. Different APN values provide different levels of service and functionality. Contact your service provider for the correct APN for your account. |
| SIM PIN | If you have assigned a 4 digit PIN to secure your SIM, enter the PIN here. |
| MTU | Enter the appropriate Maximum Transmission Unit (MTU) size for your service provider's network. In most cases, the default value is appropriate. |

## 7.2 LTE Keep-Alive

LTE Keep-Alive settings configure the EtherLINQ's "Auto Ping" feature which periodically sends traffic to a destination on the WAN to monitor the WAN connection's status. The default values are appropriate in most situations.

When the EtherLINQ detects a cellular connection failure based on the Auto Ping settings, it will drop the connection and attempt to switch to the wired WAN interface. It will also restart the cellular connection and switch back to LTE when a connection is available unless the wired WAN has higher priority or is disabled. If the Reboot on Disconnect parameter (see **Advanced** Tab) is enabled, the EtherLINQ will reboot instead of switching interfaces.



LTE Keep-Alive Settings

| | | |
|---|---|---|
| Protocol | ICMP ▾ | Use Ping (ICMP) or Web (HTTP) packets |
| Destination Address | 8.8.8.8 | IP or DNS address to ping |
| Ping Frequency | 5 | # of seconds between pings |
| Ping Failure Timeout | 3 | # of seconds to wait for a reply |

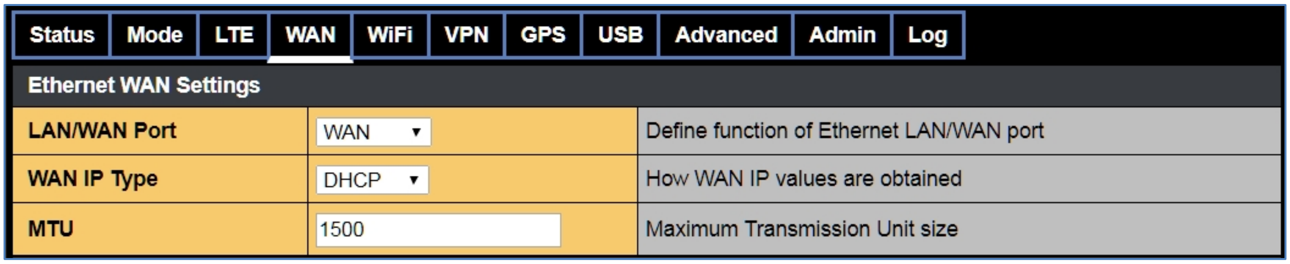
**Figure 22: LTE Keep-Alive Settings**

| | |
|---|---|
| Protocol | ICMP (ping) or HTTP packets can be used as the data for Keep-Alive. ICMP packets are faster but may be blocked and only determine if a remote host is online. HTTP packets can be used to test if a remote host is responding on port 80 with value HTTP. Select “Disabled” to disable the LTE Keep-Alive function completely and send no WAN test traffic. |
| Destination Address | Enter the IP address or FQDN of the remote host to receive Keep-Alive traffic |
| Ping Frequency | Delay time between sending Keep-Alive packets |
| Ping Failure Timeout | Maximum number of seconds to wait for each ping/HTTP to be acknowledged (maximum latency) before assuming the ping to have failed |
| Fault Tolerance | Number of consecutive pings that must fail to be acknowledged before the interface is marked as down |

# CHAPTER 8: WAN TAB

The **WAN** tab configures the EtherLINQ’s WAN Ethernet port and how the EtherLINQ responds when a WAN interface goes down.

## 8.1 WAN Setup

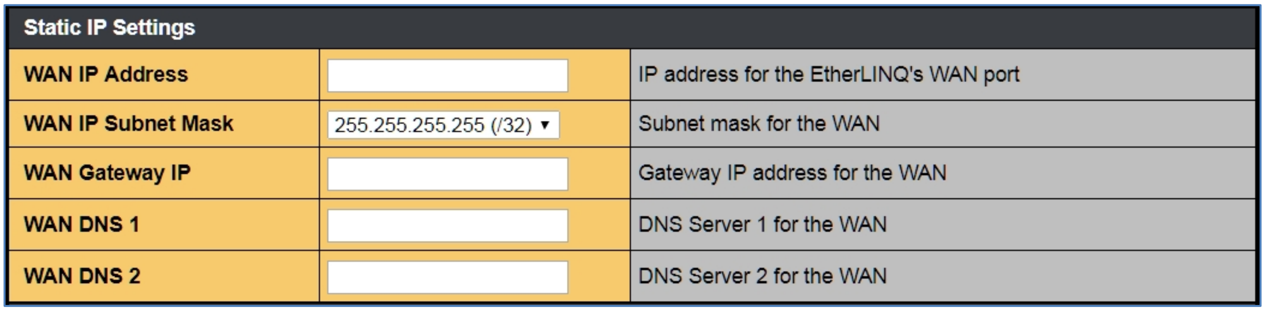


Ethernet WAN Settings

| | | |
|---|---|---|
| LAN/WAN Port | WAN ▾ | Define function of Ethernet LAN/WAN port |
| WAN IP Type | DHCP ▾ | How WAN IP values are obtained |
| MTU | 1500 | Maximum Transmission Unit size |

**Figure 23: WAN Setup**

| | |
|---|---|
| LAN/WAN Port | The LAN/WAN Ethernet port can be configured as a WAN port, a second LAN Ethernet port or the port can be disabled entirely |
| WAP IP Type | When operating as a WAN port (default), select whether the WAN requests a DHCP address assignment or assign a static IP address to the WAN interface. When Static IP is selected, additional fields as shown in Figure 24 are displayed. |
| MTU | Maximum transmission unit size: up to 1500 bytes |



Static IP Settings

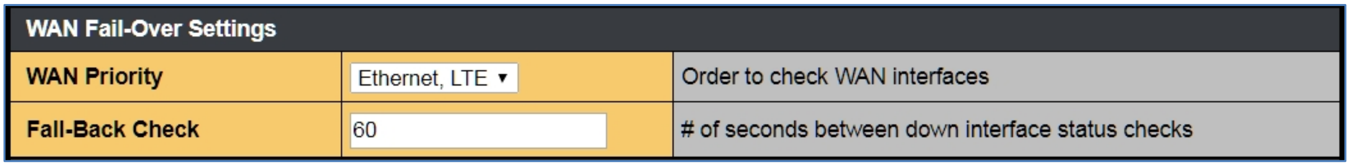
| | | |
|---|---|---|
| WAN IP Address | | IP address for the EtherLINQ's WAN port |
| WAN IP Subnet Mask | 255.255.255.255 (/32) ▾ | Subnet mask for the WAN |
| WAN Gateway IP | | Gateway IP address for the WAN |
| WAN DNS 1 | | DNS Server 1 for the WAN |
| WAN DNS 2 | | DNS Server 2 for the WAN |

**Figure 24: WAN Static IP Settings**

| | |
|---|---|
| WAN IP Address | Sets the desired WAN IP address for the EtherLINQ. The WAN subnet must be different from the LAN subnet. |
| WAN Subnet Mask | Select the appropriate subnet mask from the list |
| WAN Gateway IP | Enter the remote gateway address for the WAN interface |
| WAN DNS 1 | Enter the primary DNS Server for the WAN interface |
| WAN DNS 2 | Enter the secondary DNS Server for the WAN interface |

## 8.2 WAN Fail-Over

Sets which order the EtherLINQ uses to make WAN connections and how often the EtherLINQ attempts to re-establish a connection to the primary interface.



| WAN Fail-Over Settings | | |
|---|---|---|
| WAN Priority | Ethernet, LTE ▾ | Order to check WAN interfaces |
| Fall-Back Check | 60 | # of seconds between down interface status checks |

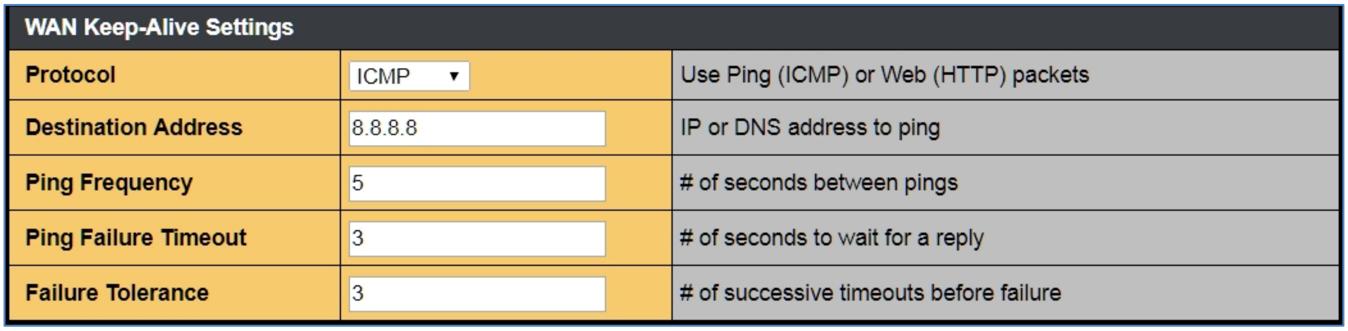
**Figure 25: WAN Fail-Over Settings**

| | |
|---|---|
| WAN Priority | Options are LTE preferred over Ethernet and Ethernet preferred over LTE. Only 1 WAN interface may be active at a time. |
| Fall-Back Check | Number of seconds the EtherLINQ waits before checking if a “down” WAN interface is available |

## 8.3 WAN Keep-Alive

WAN Keep-Alive settings configure the EtherLINQ’s “Auto Ping” feature which periodically sends traffic to a destination on the WAN to monitor the WAN connection’s status. The default values are appropriate in most situations.

When the EtherLINQ detects a WAN connection failure based on the Auto Ping settings, it will drop the connection and attempt to switch to the LTE modem. It will also restart the WAN connection and switch back to the wired WAN when a connection is available unless the LTE modem has higher priority or is not configured. If the Reboot on Disconnect parameter (see **Advanced t**ab) is enabled, the EtherLINQ will reboot instead of switching interfaces.



| WAN Keep-Alive Settings | | |
|---|---|---|
| Protocol | ICMP ▾ | Use Ping (ICMP) or Web (HTTP) packets |
| Destination Address | 8.8.8.8 | IP or DNS address to ping |
| Ping Frequency | 5 | # of seconds between pings |
| Ping Failure Timeout | 3 | # of seconds to wait for a reply |
| Failure Tolerance | 3 | # of successive timeouts before failure |

**Figure 26: WAN Keep-Alive Settings**

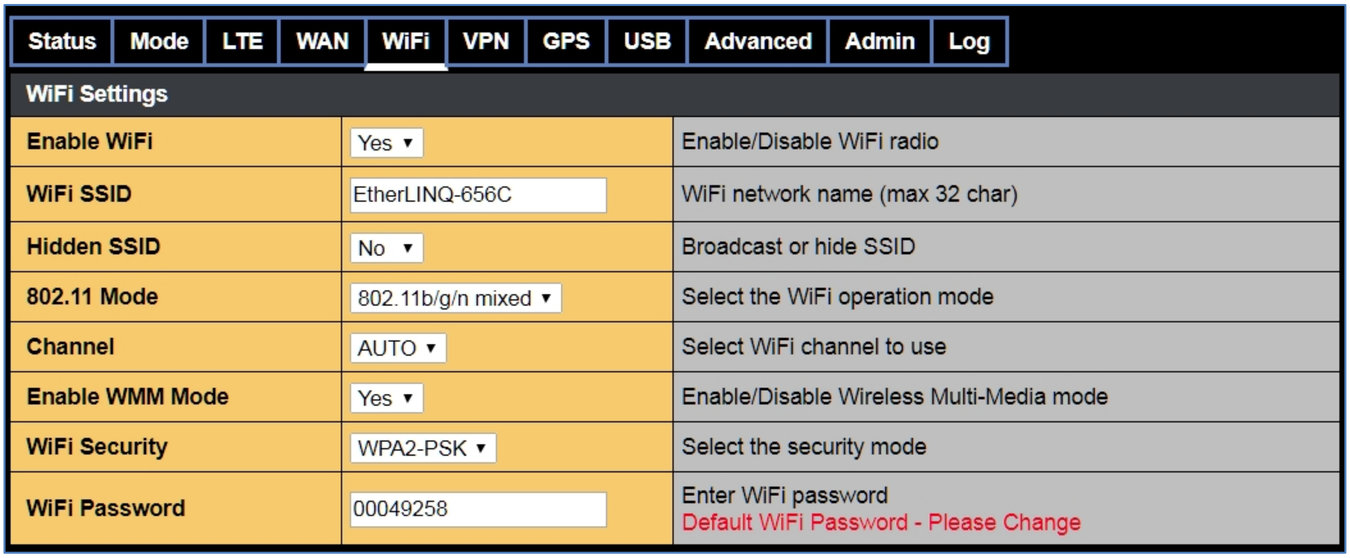
| | |
|---|---|
| Protocol | ICMP (ping) or HTTP packets can be used as the data for Keep-Alive. ICMP packets are faster but may be blocked and only determine is a remote host is |

| | |
|---|---|
| | online. HTTP packets can be used to test if a remote host is responding on port 80 with value HTTP. Select “Disabled” to disable the WAN Keep-Alive function completely and send no WAN test traffic. |
| Destination Address | Enter the IP address or FQDN of the remote host to receive Keep-Alive traffic |
| Ping Frequency | Delay time between sending Keep-Alive packets |
| Ping Failure Timeout | Maximum number of seconds to wait for each ping/HTTP to be acknowledged (maximum latency) before assuming the ping to have failed |
| Fault Tolerance | Number of consecutive pings that must fail to be acknowledged before the interface is marked as down |

# CHAPTER 9: WIFI TAB

The **WiFi** tab configures the EtherLINQ's Access Point feature on WiFi-enabled EtherLINQ models. The Access Point is bridged to the EtherLINQ's LAN -- WiFi devices are assigned IP addresses from the LAN DHCP pool.

The WiFi Access Point is enabled by default. The default SSID is "EtherLINQ-" + the last 4 characters of the EtherLINQ's serial number. The default WiFi password is unique to each serial number and is printed on the bottom label of the EtherLINQ.



WiFi Settings

| | | |
|---|---|---|
| Enable WiFi | Yes ▾ | Enable/Disable WiFi radio |
| WiFi SSID | EtherLINQ-656C | WiFi network name (max 32 char) |
| Hidden SSID | No ▾ | Broadcast or hide SSID |
| 802.11 Mode | 802.11b/g/n mixed ▾ | Select the WiFi operation mode |
| Channel | AUTO ▾ | Select WiFi channel to use |
| Enable WMM Mode | Yes ▾ | Enable/Disable Wireless Multi-Media mode |
| WiFi Security | WPA2-PSK ▾ | Select the security mode |
| WiFi Password | 00049258 | Enter WiFi password<br>Default WiFi Password - Please Change |

**Figure 27: WiFi Setup**

| | |
|---|---|
| Enable WiFi | The WiFi Access Point feature can be enabled or disabled.<br>NOTE: It is possible to completely remove the WiFi functionality from the EtherLINQ. See *Section 14.1.2 Activating & Deactivating Features*. |
| WiFi SSID | The descriptive name which is displayed when WiFi clients search for available access points |
| Hidden SSID | Enable/Disable broadcasting of the SSID. Disabling SSID broadcasting enhances the security by hiding SSID information and requiring users to enter the SSID manually when connecting to the access point. |
| 802.11 Mode | Select the combination of 802.11 radio protocols to use |
| Channel | Select the 802.11 radio channel to use. Select AUTO to have the EtherLINQ determine the best channel to use based on the local radio environment. |
| Enable WMM Mode | Enable/Disable Wireless Multi-Media mode. For example, VoIP or video traffic will have higher priorities over ordinary traffic. |
| WiFi Security | Select the security protocol that WiFi clients must use to authenticate |

| | |
|---|---|
| WiFi Password | Enter the password protocol that WiFi clients must use to authenticate to the access point. For WEP, passwords must be 5 or 13 characters; for WPA/WPA2, passwords must be between 8 and 63 characters. |

The WiFi Access Point can be enabled in all three EtherLINQ operating modes. However, in IP Pass-Through Mode, only 1 device can obtain the WAN IP address. In Virtual Cable Mode, a separate DHCP server would be required on the LAN or all WiFi devices would have to have statically assigned LAN IPs.

# CHAPTER 10: VPN TAB

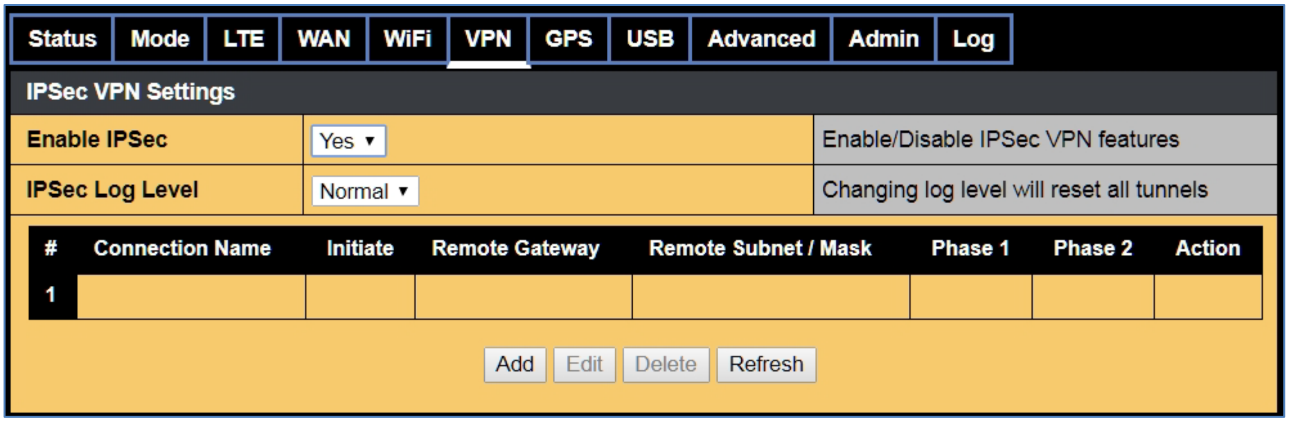
Internet Protocol Security (IPSec) is a standards-based protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session. IPSec also includes protocols for establishing mutual authentication between agents at the beginning of 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 EtherLINQ supports both modes and is interoperable with a wide variety of IPSec-compliant software and hardware products from numerous vendors. IPSec is only available when the EtherLINQ is operating in NAT Router Mode.

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 EtherLINQ and on the “private” side of the other VPN equipment must be on <u>different</u> 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, use a Dynamic DNS hostname for your EtherLINQ that has a dynamic <u>public</u> IP address (See *Section 13.3 Dynamic DNS*).
- The EtherLINQ can be either the VPN initiator or responder for net-to-net VPNs. It is the responder for Remote User VPNs. If the EtherLINQ has only a *private* WAN IP address, the EtherLINQ <u>must initiate</u> all IPSec connections (Remote User Mode is not possible with private WAN IP addresses). Consult the documentation of the VPN server the EtherLINQ will communicate with regarding configuration of private IP end-points.
- 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 EtherLINQ VPN configuration examples are available on the Proxicast Support web site in the TechNotes and Knowledgebase areas.

## 10.1 IPSec VPN Settings



IPSec VPN Settings

| | | |
|---|---|---|
| Enable IPSec | Yes ▾ | Enable/Disable IPSec VPN features |
| IPSec Log Level | Normal ▾ | Changing log level will reset all tunnels |

| # | Connection Name | Initiate | Remote Gateway | Remote Subnet / Mask | Phase 1 | Phase 2 | Action |
|---|---|---|---|---|---|---|---|
| 1 | | | | | | | |

**Figure 28: IPSec VPN Connections**

### Fields

| | |
|---|---|
| IPSec | Select Enable/Disable to enable/disable IPSec.<br>**NOTE:** It is possible to completely remove the IPSec functionality from the EtherLINQ. See *Section 14.1.2 Activating & Deactivating Features*. |
| IPSec Log Level | Normal for routine use; Debug for additional information on tunnel activity.<br>**NOTE:** Debug will quickly fill up the system log. |
| Connection Name | User-defined string to identify a specific tunnel |
| Initiate | How the tunnel was initiated (Auto, on Traffic detection, Manual, Disabled) |
| Remote Gateway | IP/FQDN of the remote IPSec end-point |
| Remote Subnet / Mask | IP subnet & netmask of the LAN connected to the remote IPSec end-point |
| Phase 1 | Status of IPSec Phase 1 negotiations (🔴 = Down, 🟢 = Up) |
| Phase 2 | Status of IPSec Phase 2 negotiations (🔴 = Down, 🟢 = Up) |
| Action | Forcibly Open or Close the tunnel |

### Buttons

| | |
|---|---|
| Add | Click **Add** to create a new IPSec connection rule |
| Edit | Highlight the desired connection and click **Edit** to modify the connection parameters. You may also double-click the row to edit. |
| Delete | Highlight a connection and click **Delete** to remove the selected rule |
| Refresh | Forcibly refresh the status of all tunnels |

## 10.2 Add an 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 EtherLINQ at a remote office location.

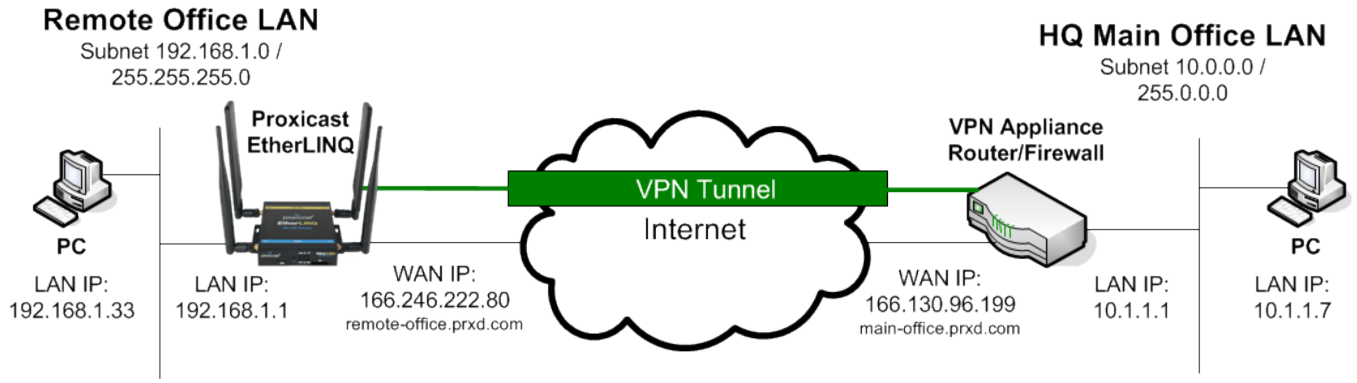
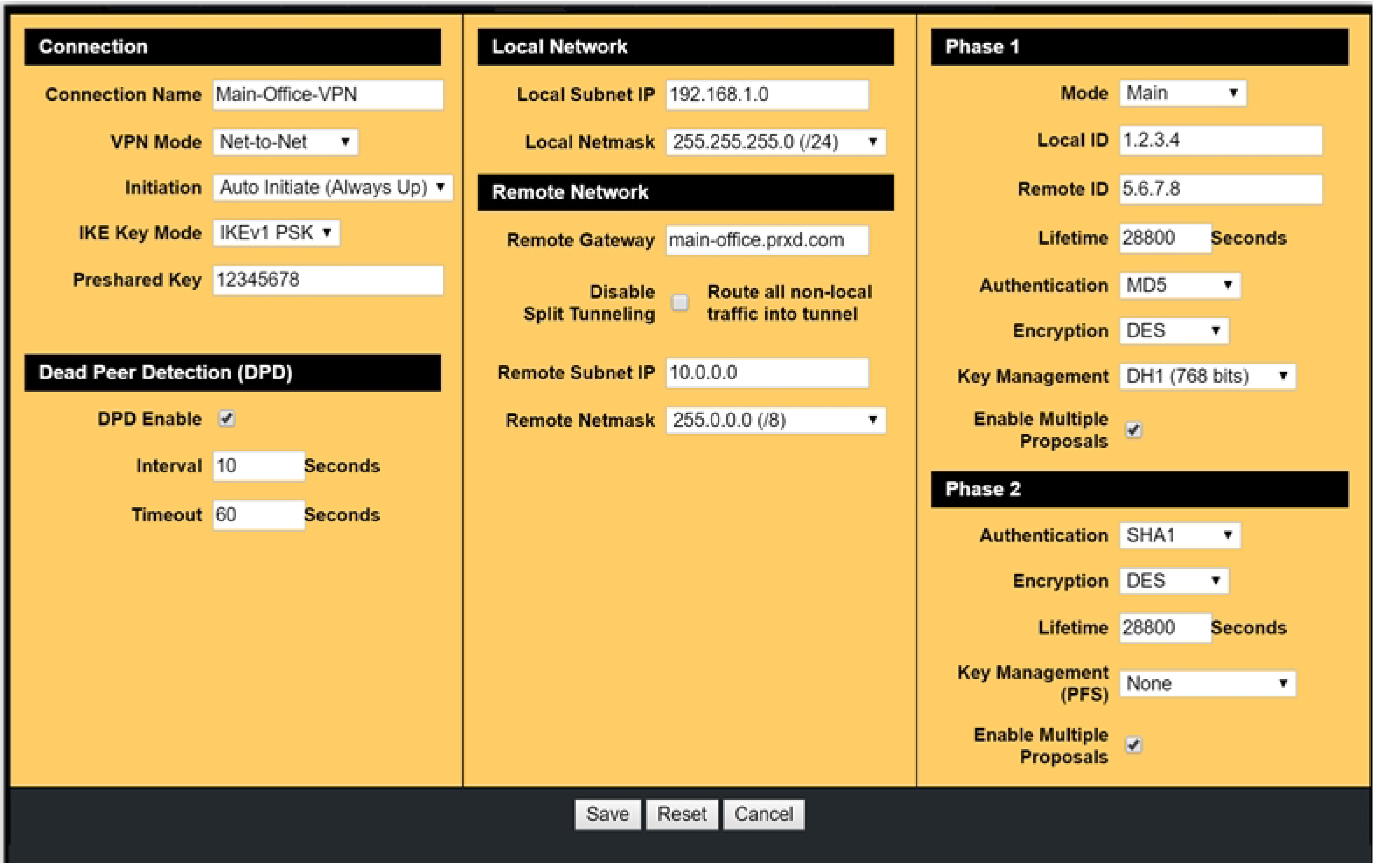


**Figure 29: Net-to-Net IPSec Example**

Click on the **Add** button to display the following screen:



**Connection**

- Connection Name: Main-Office-VPN
- VPN Mode: Net-to-Net
- Initiation: Auto Initiate (Always Up)
- IKE Key Mode: IKEv1 PSK
- Preshared Key: 12345678

**Dead Peer Detection (DPD)**

- DPD Enable: ☑
- Interval: 10 Seconds
- Timeout: 60 Seconds

**Local Network**

- Local Subnet IP: 192.168.1.0
- Local Netmask: 255.255.255.0 (/24)

**Remote Network**

- Remote Gateway: main-office.prxd.com
- Disable Split Tunneling: ☐ Route all non-local traffic into tunnel
- Remote Subnet IP: 10.0.0.0
- Remote Netmask: 255.0.0.0 (/8)

**Phase 1**

- Mode: Main
- Local ID: 1.2.3.4
- Remote ID: 5.6.7.8
- Lifetime: 28800 Seconds
- Authentication: MD5
- Encryption: DES
- Key Management: DH1 (768 bits)
- Enable Multiple Proposals: ☑

**Phase 2**

- Authentication: SHA1
- Encryption: DES
- Lifetime: 28800 Seconds
- Key Management (PFS): None
- Enable Multiple Proposals: ☑

**Figure 30: IPSec Net-to-Net VPN Settings**

### Connection

| | |
|---|---|
| Connection Name | User defined name for the IPSec rule. Spaces are not permitted. |
| VPN Mode | Net-to-Net |
| Initiation | **Auto Initiate (Always Up)**: forces the EtherLINQ to always attempt to initiate a VPN connection to the remote gateway. If the connection drops, the EtherLINQ will continuously attempt to reconnect.<br>**Initiate on Traffic:** IPSec tunnel will only be established when the EtherLINQ detects traffic that is destined for the LAN subnet behind the remote gateway.<br>**Manual Connection:** to establish an IPSec tunnel, the user must click the **Open** button on the VPN settings screen.<br>**Disabled:** this IPSec tunnel will be ignored. |
| IKE Key Mode | IKEv1 and IKEv2 Pre-Shared Key (PSK) are supported. |
| Preshared Key | Enter the preshared key. The key should be at least an 8-digit ASCII string. |

**NOTE:** If the remote VPN gateway will be responsible for initiating the VPN connection, select Manual for the EtherLINQ's Initiation Mode. Only one VPN device should act as the initiator.

### Dead Peer Detection

| | |
|---|---|
| DPD Enable | Enable/disable Dead Peer Detection (DPD). |
| DPD Interval | Number of seconds between checks for a dead peer. |
| DPD Timeout | Number of seconds to wait for a response before declaring the peer dead. |

### Local Network

| | |
|---|---|
| Local Subnet IP | Enter the subnet IP address on the LAN-side of the local EtherLINQ which will be visible to the remote VPN subnet.<br>**NOTE:** Enter the subnet address and not the LAN IP of the EtherLINQ. E.g. if the EtherLINQ's IP is 192.168.1.1 / 255.255.255.0, enter 192.168.1.**0** as the subnet IP. |
| Local Subnet Netmask | Netmask for the LAN subnet entered above. |

### Remote Network

| | |
|---|---|
| Remote Gateway | Enter the IP address or fully qualified domain name of the remote VPN gateway. This option is required in Net-to-Net mode. |
| Disable Split Tunneling | **Unchecked:** Traffic can flow to Internet addresses outside of IPSec tunnel (default).<br>**Checked:** The EtherLINQ directs all traffic into the IPSec tunnel. The VPN device on the other side is responsible for routing the traffic to its final destination. |

| | |
|---|---|
| Remote Subnet IP | Enter the subnet IP address of the remote VPN gateway. This option is required in Net-to-Net mode.<br>**NOTE:** Enter the subnet address and not the LAN IP behind the remote VPN gateway. E.g. if the remote VPN gateway's IP is 10.1.1.1/ 255.0.0.0, enter **10.0.0.0** as the subnet IP. |
| Remote Subnet Netmask | Subnet netmask of the remote VPN gateway. This option is required in Net-to-Net mode. |

## Phase 1

| | |
|---|---|
| Mode | Select Main or Aggressive Mode. Must match the setting on the remote gateway. |
| Local ID | Enter the phase 1 Local ID |
| Remote ID | Enter the phase 1 Remote ID |
| Lifetime | Enter the phase 1 lifetime (between 3600 and 86400 seconds) |
| Authentication | Choose the phase 1 authentication |
| Encryption | Choose the phase 1 encryption |
| Key Management | Choose the phase 1 group key management |
| Enable Multiple Proposals | Check to allow the EtherLINQ to offer multiple combinations of authentication, encryption and key management to the remote VPN gateway. Selecting this option can overcome mismatches between the VPN devices if the remote VPN gateway also supports multiple proposals. |

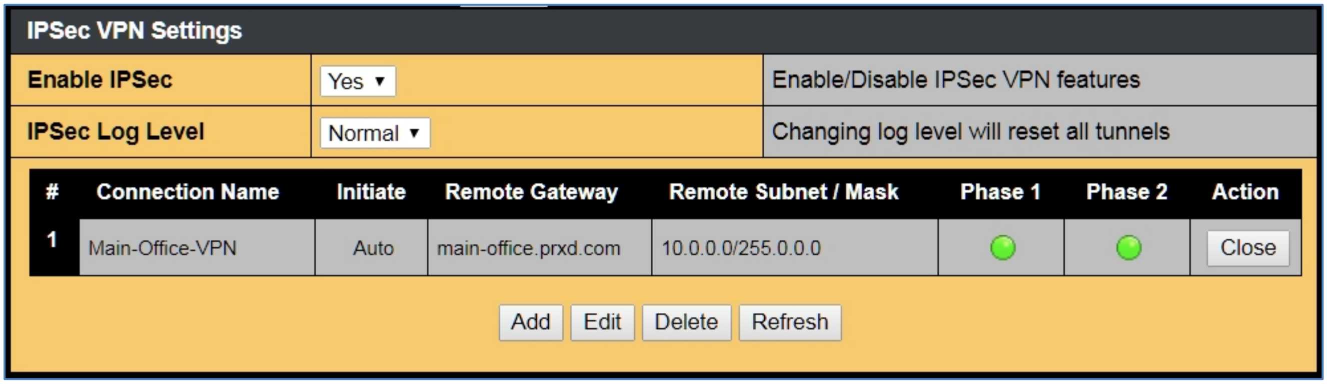
**NOTE:** For IKEv1, if the Local and Remote ID values are blank, the EtherLINQ uses its own public WAN IP address as the Local ID and the IP address of the remote VPN gateway as the Remote ID. If the remote VPN gateway has a dynamic IP address, or you use a FQDN to reference it, or it is behind a NAT firewall, Local and Remote ID values may be required on both VPN end-points.

For IKEv2, Local and Remote ID values are required.

## Phase 2

| | |
|---|---|
| Lifetime | Enter the phase 2 lifetime (between 3600 and 86400 seconds) |
| Authentication | Choose the phase 2 authentication |
| Encryption | Choose the phase 2 encryption |
| Key Management (PFS) | Choose the phase 2 group key management. This setting is also known as Perfect Forward Secrecy. |
| Enable Multiple Proposals | Check to allow the EtherLINQ to offer multiple combinations of authentication, |

| | |
|---|---|
| | encryption and key management to the remote VPN gateway. Selecting this option can overcome mismatches between the VPN devices if the remote VPN gateway also supports multiple proposals. |



IPSec VPN Settings

| | | |
|---|---|---|
| Enable IPSec | Yes ▾ | Enable/Disable IPSec VPN features |
| IPSec Log Level | Normal ▾ | Changing log level will reset all tunnels |

| # | Connection Name | Initiate | Remote Gateway | Remote Subnet / Mask | Phase 1 | Phase 2 | Action |
|---|---|---|---|---|---|---|---|
| 1 | Main-Office-VPN | Auto | main-office.prxd.com | 10.0.0.0/255.0.0.0 | ● | ● | Close |

**Figure 31: IPSec VPN Network Connections Status**

## 10.3 Add an IPSec Remote User Rule

In this example, a Remote User VPN connection will be established between with the EtherLINQ functioning as the VPN Server and remote PC as the client using the Proxicast IPSec VPN Client for Windows software.

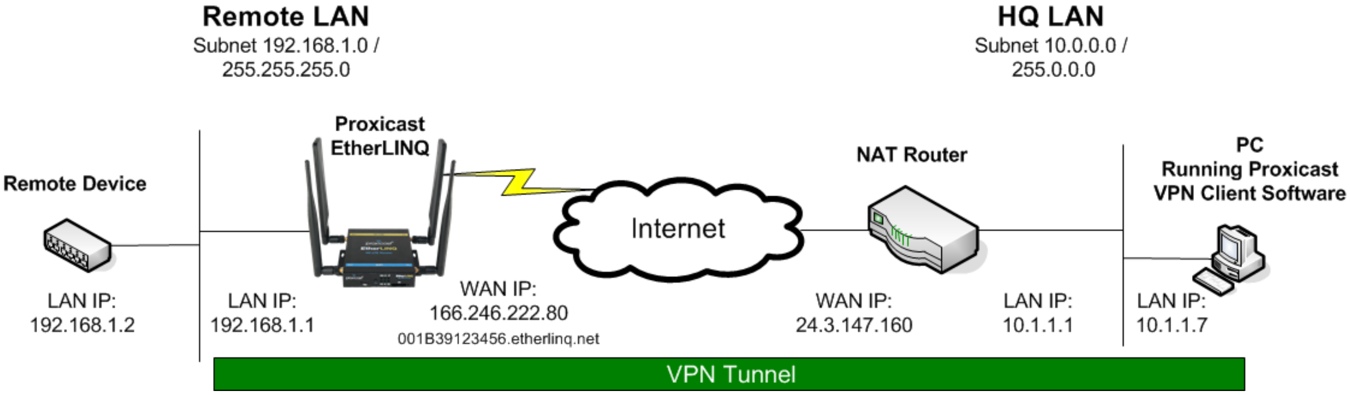
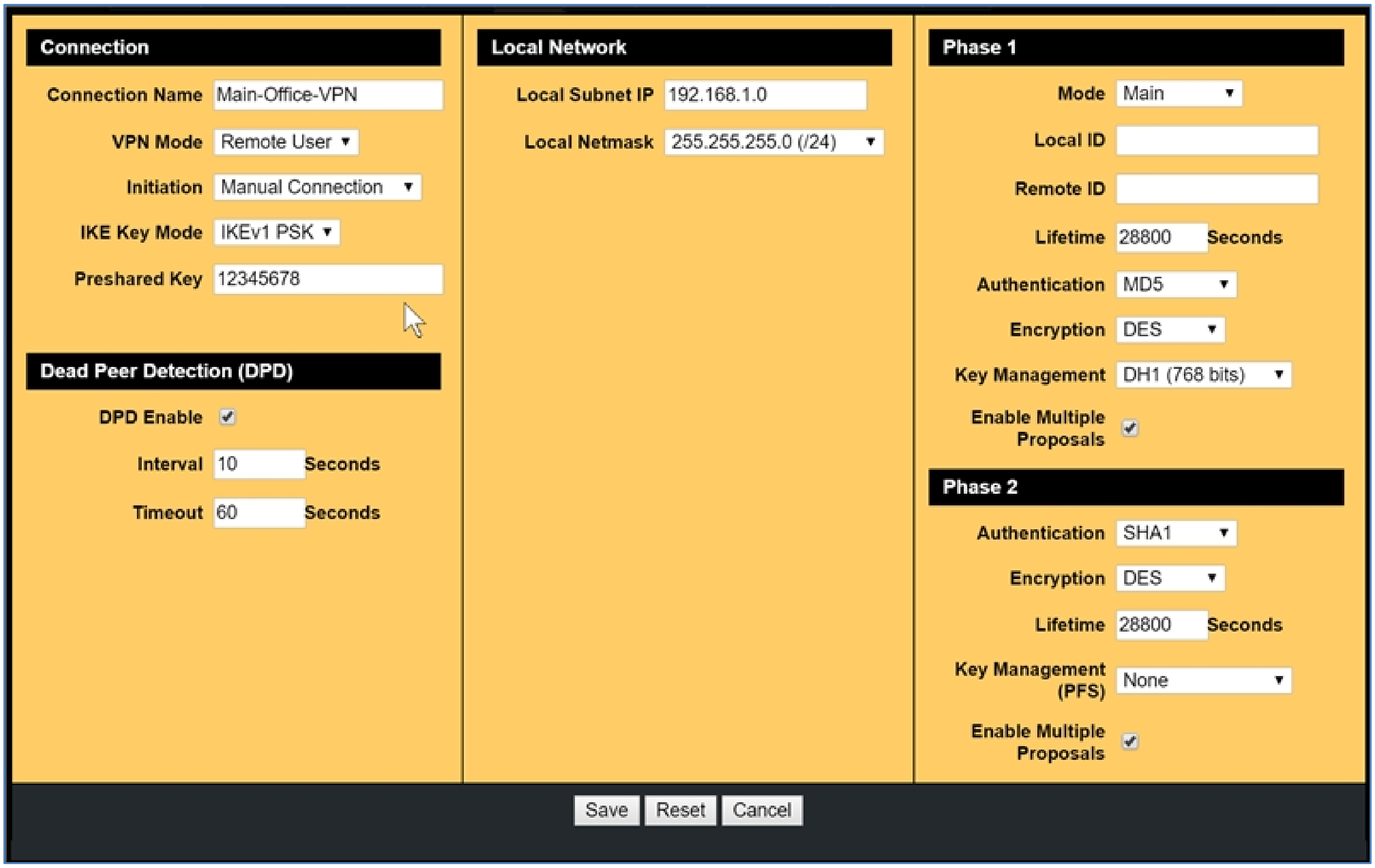


**Figure 32: Remote User IPSec Example**

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



Connection

Connection Name: Main-Office-VPN

VPN Mode: Remote User

Initiation: Manual Connection

IKE Key Mode: IKEv1 PSK

Preshared Key: 12345678

Dead Peer Detection (DPD)

DPD Enable ☑

Interval: 10 Seconds

Timeout: 60 Seconds

Local Network

Local Subnet IP: 192.168.1.0

Local Netmask: 255.255.255.0 (/24)

Phase 1

Mode: Main

Local ID:

Remote ID:

Lifetime: 28800 Seconds

Authentication: MD5

Encryption: DES

Key Management: DH1 (768 bits)

Enable Multiple Proposals ☑

Phase 2

Authentication: SHA1

Encryption: DES

Lifetime: 28800 Seconds

Key Management (PFS): None

Enable Multiple Proposals ☑

**Figure 33: 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 client will be a single unknown IP address.

Multiple VPN clients can share a single Remote User VPN rule on the EtherLINQ if all clients are to have access to the same subnet on the EtherLINQ's LAN.

**Note:** You cannot make a Remote User VPN connection to an EtherLINQ that has a private IP address; you must request a public IP address from your ISP. If a public IP address for the EtherLINQ cannot be obtained, then the EtherLINQ must initiate a Net-to-Net VPN connection to another VPN server in order to remotely access devices attached to the EtherLINQ; or use the EtherLINQ's Virtual Cable Mode (see *Section 6.3 Virtual Cable Mode*)

## Connection

| | |
|---|---|
| Connection Name | User defined name for the IPSec rule. Spaces are not permitted. |
| VPN Mode | Remote-User |
| Initiation | **Manual Connection:** an IPSec tunnel will be created when a remote VPN client |

| | |
|---|---|
| | makes a valid connection request; the EtherLINQ cannot make a connection to a remote client.<br>**Disabled:** this IPSec tunnel will be ignored. |
| IKE Key Mode | IKEv1 and IKEv2 Pre-Shared Key (PSK) are supported. |
| Preshared Key | Enter the preshared key. The key should be at least an 8-digit ASCII string. |

### Dead Peer Detection

| | |
|---|---|
| DPD Enable | Enable/disable Dead Peer Detection (DPD). |
| DPD Interval | Number of seconds between checks for a dead peer |
| DPD Timeout | Number of seconds to wait for a response before declaring the peer dead |

### Local Network

| | |
|---|---|
| Local Subnet IP | Enter the subnet IP address on the LAN-side of the local EtherLINQ which will be visible to the remote VPN client.<br>**NOTE:** Enter the subnet address and not the LAN IP of the EtherLINQ. E.g. if the EtherLINQ's IP is 192.168.1.1 / 255.255.255.0, enter 192.168.1.**0** as the subnet IP. |
| Local Subnet Netmask | Netmask for the LAN subnet entered above. |

### Phase 1

| | |
|---|---|
| Mode | Select Main or Aggressive Mode. Must match the setting on the remote client. |
| Local ID | Enter the phase 1 Local ID |
| Remote ID | Enter the phase 1 Remote ID |
| Lifetime | Enter the phase 1 lifetime (between 3600 and 86400 seconds) |
| Authentication | Choose the phase 1 authentication |
| Encryption | Choose the phase 1 encryption |
| Key Management | Choose the phase 1 group key management |
| Enable Multiple Proposals | Check to allow the EtherLINQ to offer multiple combinations of authentication, encryption and key management to the remote VPN client. Selecting this option can overcome mismatches between the VPN devices if the remote VPN client also supports multiple proposals. |

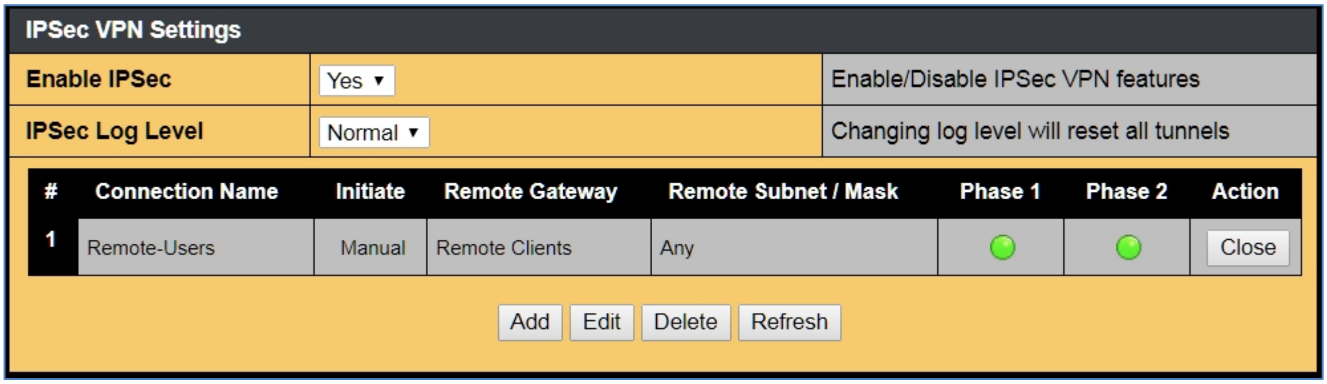
**NOTE:** For IKEv1, if the Local and Remote ID values are blank, the EtherLINQ uses its own public WAN IP address as the Local ID and the IP address of the remote VPN client as the Remote ID. If the remote client has a dynamic IP address, or you use a FQDN to reference it, or it is behind a NAT firewall, Local and Remote ID values may be required on both VPN end-points.

For IKEv2, Local and Remote ID values are required.

### Phase 2

| | |
|---|---|
| Lifetime | Enter the phase 2 lifetime (between 3600 and 86400 seconds) |
| Authentication | Choose the phase 2 authentication |
| Encryption | Choose the phase 2 encryption |
| Key Management (PFS) | Choose the phase 2 group key management. This setting is also known as Perfect Forward Secrecy. |
| Enable Multiple Proposals | Check to allow the EtherLINQ to offer multiple combinations of authentication, encryption and key management to the remote VPN client. Selecting this option can overcome mismatches between the VPN devices if the remote VPN client also supports multiple proposals. |

## 10.4 IPSec Tunnel Status



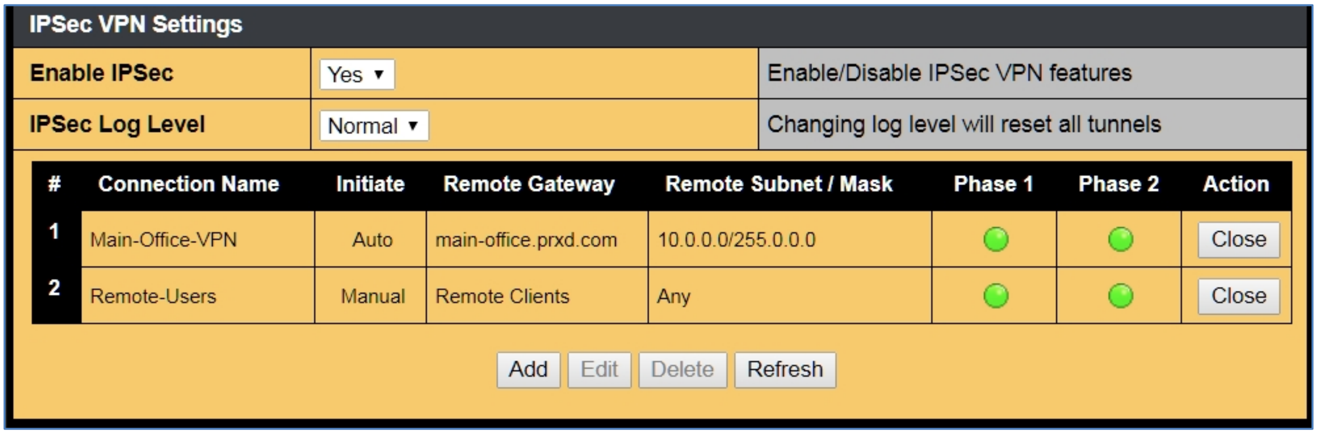
IPSec VPN Settings

| | | |
|---|---|---|
| Enable IPSec | Yes ▾ | Enable/Disable IPSec VPN features |
| IPSec Log Level | Normal ▾ | Changing log level will reset all tunnels |

| # | Connection Name | Initiate | Remote Gateway | Remote Subnet / Mask | Phase 1 | Phase 2 | Action |
|---|---|---|---|---|---|---|---|
| 1 | Remote-Users | Manual | Remote Clients | Any | ● | ● | Close |

**Figure 34: IPSec VPN Remote User Connection Status**

Multiple Net-to-Net and Remote User rules may be active at the same time to support both fixed and mobile VPN end-points.



IPSec VPN Settings

| | | |
|---|---|---|
| Enable IPSec | Yes ▾ | Enable/Disable IPSec VPN features |
| IPSec Log Level | Normal ▾ | Changing log level will reset all tunnels |

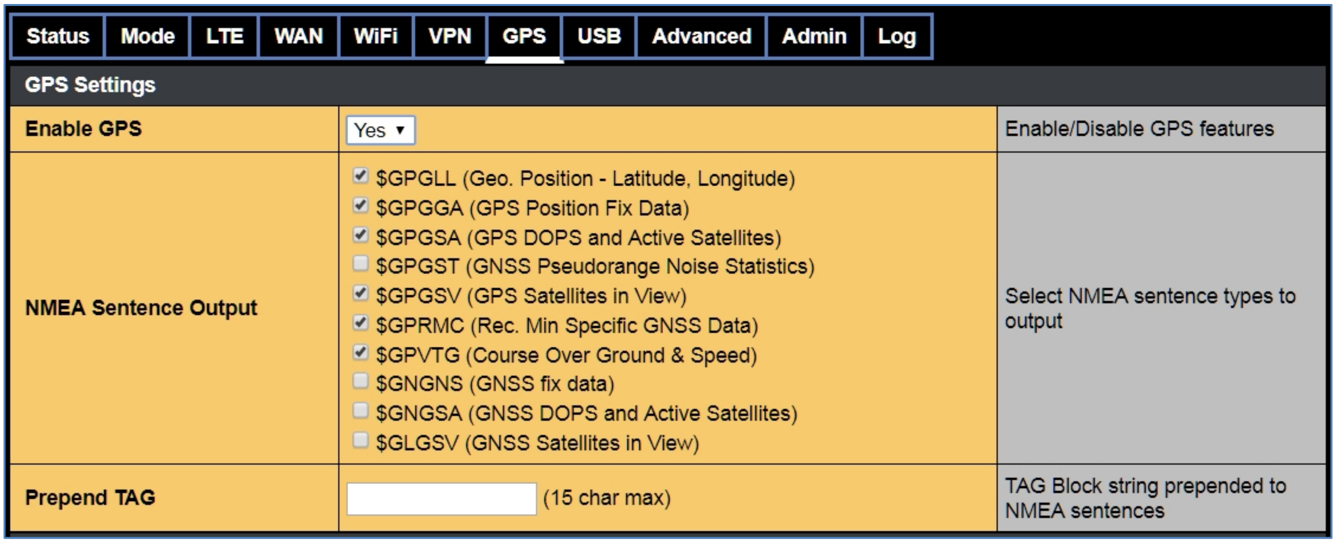
| # | Connection Name | Initiate | Remote Gateway | Remote Subnet / Mask | Phase 1 | Phase 2 | Action |
|---|---|---|---|---|---|---|---|
| 1 | Main-Office-VPN | Auto | main-office.prxd.com | 10.0.0.0/255.0.0.0 | ● | ● | Close |
| 2 | Remote-Users | Manual | Remote Clients | Any | ● | ● | Close |

Figure 35: IPSec VPN Connection Status

# CHAPTER 11: GPS TAB

On GPS equipped EtherLINQ models, the **GPS** tab configures the GPS receiver and determines how GPS data is made available to remote GPS applications. The EtherLINQ's GPS receiver outputs data in National Marine Electronics Association (NMEA) 0183 standard format (datum WGS-84). GPS data is derived solely from GPS satellites – an external GPS antenna is required. Positional data is updated once per second (1 Hz).

## 11.1 GPS Setup



GPS Settings

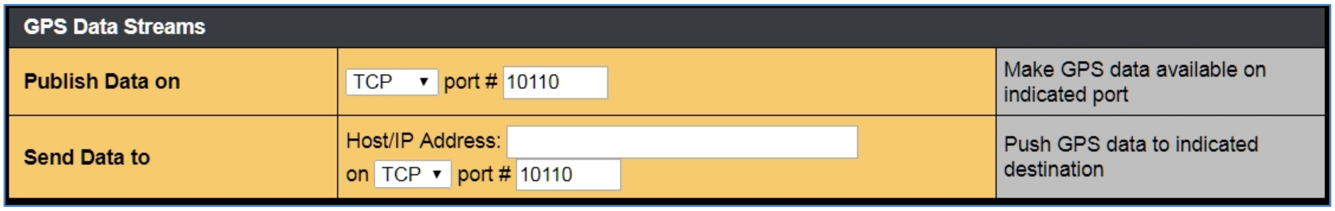
| | | |
|---|---|---|
| **Enable GPS** | Yes ▾ | Enable/Disable GPS features |
| **NMEA Sentence Output** | ☑ $GPGLL (Geo. Position - Latitude, Longitude)<br>☑ $GPGGA (GPS Position Fix Data)<br>☑ $GPGSA (GPS DOPS and Active Satellites)<br>□ $GPGST (GNSS Pseudorange Noise Statistics)<br>☑ $GPGSV (GPS Satellites in View)<br>☑ $GPRMC (Rec. Min Specific GNSS Data)<br>☑ $GPVTG (Course Over Ground & Speed)<br>□ $GNGNS (GNSS fix data)<br>□ $GNGSA (GNSS DOPS and Active Satellites)<br>□ $GLGSV (GNSS Satellites in View) | Select NMEA sentence types to output |
| **Prepend TAG** | (15 char max) | TAG Block string prepended to NMEA sentences |

**Figure 36: GPS Setup**

| | |
|---|---|
| Enable GPS | The GPS feature can be enabled or disabled.<br>**NOTE:** It is possible to completely remove the GPS functionality from the EtherLINQ. See *Section 14.1.2 Activating & Deactivating Features*. |
| NMEA Sentence Output | Select the combination of NMEA sentences to be output. Available NMEA sentences may vary by EtherLINQ model. |
| Prepend TAG | Up to 15 characters can be prepended to each NMEA sentence to uniquely identify the data stream from this EtherLINQ. |

## 11.2 GPS Data Streams

The EtherLINQ can simultaneously make GPS data available on a specified port so that remote GPS applications can retrieve the data stream and the EtherLINQ can push the GPS data stream to a specific remote host device for further processing.



GPS Data Streams

| | | |
|---|---|---|
| **Publish Data on** | TCP ▾ port # 10110 | Make GPS data available on indicated port |
| **Send Data to** | Host/IP Address:<br>on TCP ▾ port # 10110 | Push GPS data to indicated destination |

**Figure 37: GPS Data Streams**

| | |
|---|---|
| Publish Data on | Select the protocol (TCP or UDP) and the port number that will be used to serve the GPS data |
| Send Data to | Enter the remote host IP address or FQDN, protocol and port of where the EtherLINQ should send the GPS data stream. The host may be on either the LAN or WAN interface. |

# CHAPTER 12: USB TAB

The **USB** tab configures the EtherLINQ's two embedded USB servers on models with these features enabled:

1. USB Webcam Server
2. USB Serial Device Server

The USB Webcam Server enables the EtherLINQ to use inexpensive USB web cameras to provide basic remote video viewing capabilities. Most USB webcams are supported.

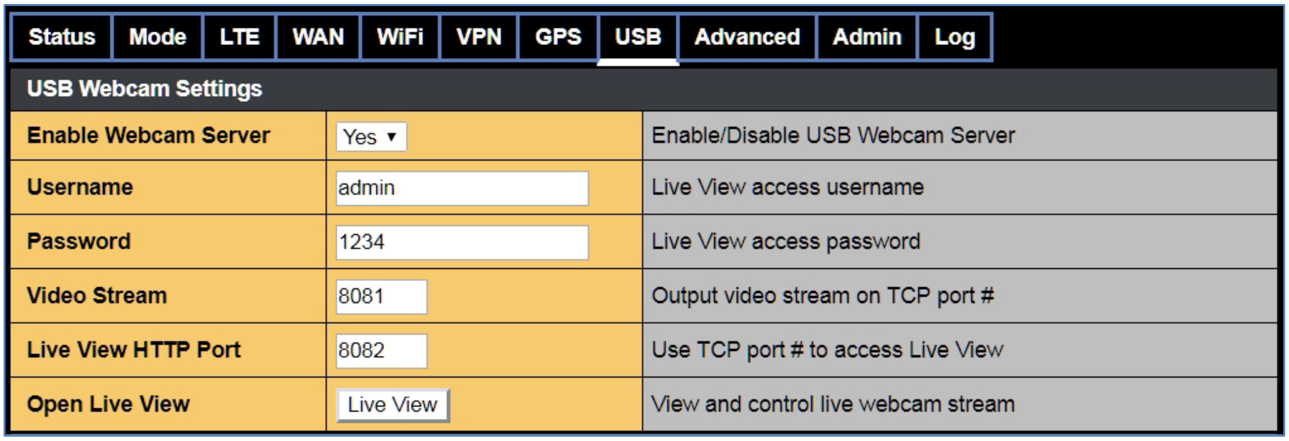
The USB Serial Device Server enables the EtherLINQ to interface with legacy serial devices to make them available over the WAN.

## 12.1 USB Webcam Setup

The USB Webcam Server uses a standard inexpensive USB web camera to take a series of MJPEG images and stream them on to a designated TCP port. The USB Webcam Server can be used to add video observation capabilities to an application environment without a significant hardware investment or using an Ethernet port.

**NOTE:** The USB Webcam Server is not intended as a substitute for high-resolution or advanced capability IP network cameras for video surveillance or similar applications. IP cameras can be connected to the EtherLINQ's LAN Ethernet port or WiFi Access Point.

The USB Webcam Server does not support video compression and is best used with low resolution images at relatively low frame rates. Audio, Pan/Tilt/Zoom and other advanced camera functions are not supported.



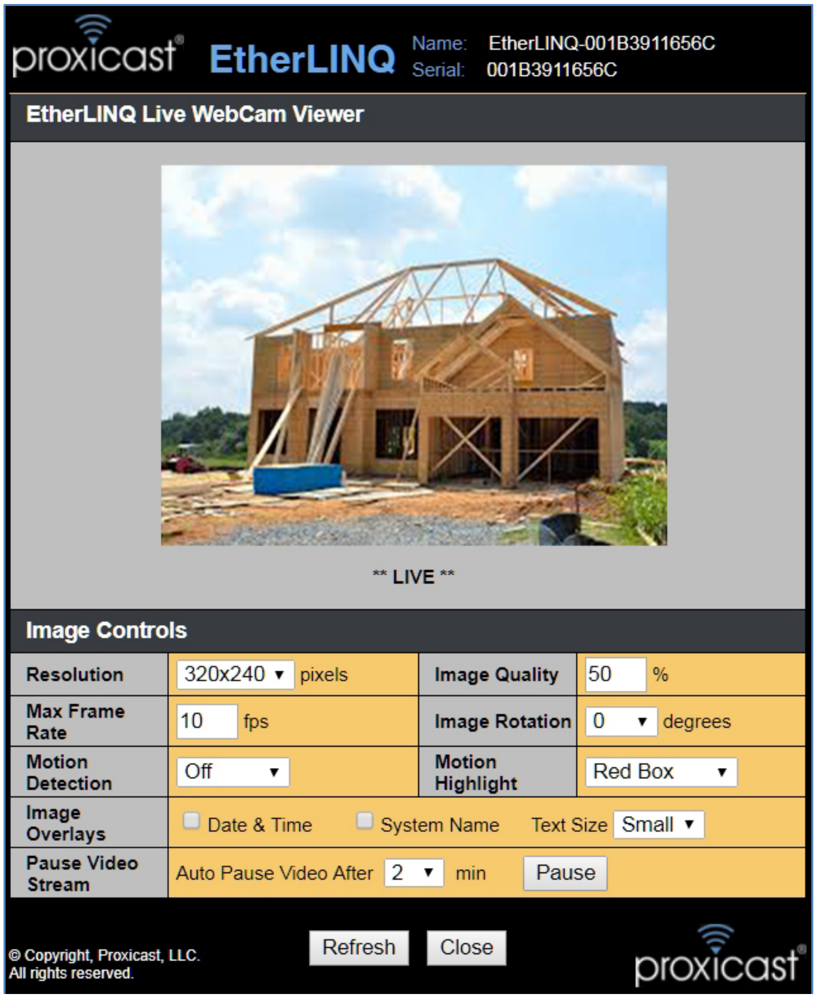
| USB Webcam Settings | | |
|---|---|---|
| Enable Webcam Server | Yes ▾ | Enable/Disable USB Webcam Server |
| Username | admin | Live View access username |
| Password | 1234 | Live View access password |
| Video Stream | 8081 | Output video stream on TCP port # |
| Live View HTTP Port | 8082 | Use TCP port # to access Live View |
| Open Live View | Live View | View and control live webcam stream |

**Figure 38: Webcam Server Setup**

| | |
|---|---|
| Enable Webcam Server | The Webcam Server feature can be enabled or disabled.<br>**NOTE:** It is possible to completely remove the Webcam Server functionality from the EtherLINQ. See *Section 14.1.2 Activating & Deactivating Features*. |
| Username | Enter the username required for authentication to the live video stream. This username can be different from the EtherLINQ's configuration username. |
| Password | Enter the password required for authentication to the live video stream. This password can be different from the EtherLINQ's configuration password. |
| Video Stream | Enter the TCP port number that will be used to output the live video stream. Third-party viewing applications such as VLC should use this port number. |
| Live View HTTP Port | Enter the TCP port number that the EtherLINQ will use to serve up its Live View video monitor application (see below) |
| Open Live View | Clicking this button will open the Live View application (Figure 39) in a new browser window |

The Live View application provides a convenient web-based tool for viewing and customizing the USB Webcam video stream. It also provides basic motion detection capabilities. Live View can be used locally or remotely (if your WAN service includes inbound connections). The video stream can also be viewed on any MJPEG capable viewer such as VLC, AnyCam, etc. including SmartPhone viewer apps. These applications may provide additional functionality such as recording.

**NOTE:** Enabling the USB Webcam Server automatically opens the Video Stream and Live View ports to the WAN and forwards those ports to the Webcam Server. No other port-forwarding/firewall rules are required.



EtherLINQ

Name: EtherLINQ-001B3911656C
Serial: 001B3911656C

EtherLINQ Live WebCam Viewer

** LIVE **

Image Controls

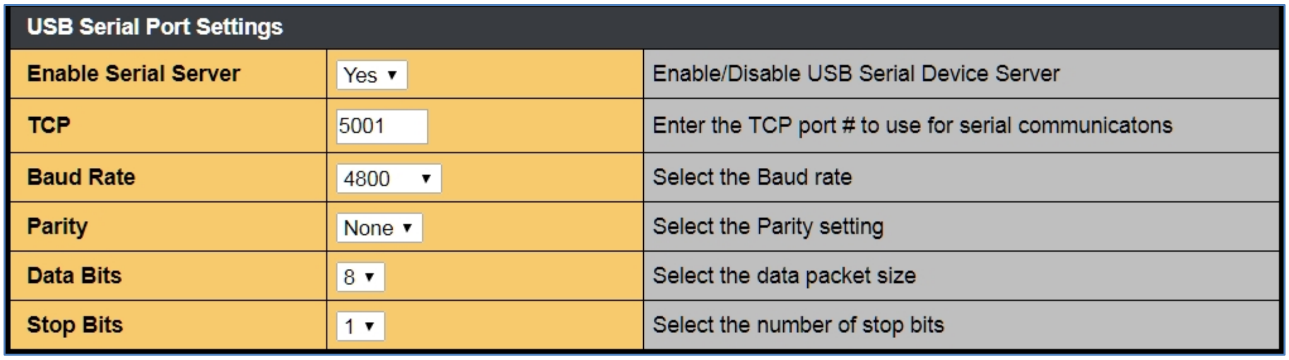
| | | | |
|---|---|---|---|
| Resolution | 320x240 ▾ pixels | Image Quality | 50 % |
| Max Frame Rate | 10 fps | Image Rotation | 0 ▾ degrees |
| Motion Detection | Off ▾ | Motion Highlight | Red Box ▾ |
| Image Overlays | □ Date & Time □ System Name Text Size Small ▾ | | |
| Pause Video Stream | Auto Pause Video After 2 ▾ min Pause | | |

© Copyright, Proxicast, LLC.
All rights reserved.

Figure 39: USB Webcam Live View Window

| | |
|---|---|
| Resolution | Camera resolution (image size). Larger images require more bandwidth and data. |
| Image Quality | Quality of the JPEG images in percent |
| Image Rotation | Rotate image 0, 90, 180 or 270 degrees |
| Motion Detection | Detect changes in pixel between images. Low/Medium/High sensitivity. High sensitivity detects motion based on fewer changed pixels. |
| Motion Highlight | Indicate changed pixels with a red or white box or cross |
| Image Overlays | Place the current Date & Time in the lower right corner of the image.<br>Place the System Name in the lower left corner of the image.<br>Specify the text size. |
| Pause Video Stream | Live View will stop streaming images after the set amount of time. This prevents excessive data usage if the Live View window is left open. |

## 12.2 USB Serial Device Server Setup



USB Serial Port Settings

| | | |
|---|---|---|
| Enable Serial Server | Yes ▾ | Enable/Disable USB Serial Device Server |
| TCP | 5001 | Enter the TCP port # to use for serial communicatons |
| Baud Rate | 4800 ▾ | Select the Baud rate |
| Parity | None ▾ | Select the Parity setting |
| Data Bits | 8 ▾ | Select the data packet size |
| Stop Bits | 1 ▾ | Select the number of stop bits |

**Figure 40: Serial Device Server Setup**

| | |
|---|---|
| Enable Serial Server | The Serial Server feature can be enabled or disabled.<br>**NOTE:** It is possible to completely remove the Serial Server functionality from the EtherLINQ. See *Section 14.1.2 Activating & Deactivating Features*. |
| TCP | TCP port number where serial data will be streamed. Remote devices must listen on this port. |
| Baud Rate | Baud rate of incoming data from the serial port |
| Parity | Parity of the incoming serial data |
| Data Bits | Number of data bits per byte of serial data |
| Stop Bits | Number stop bits per byte of serial data |

With an RS-232 to USB adapter, the EtherLINQ can be used to stream data from a serial port on a legacy device to a computer on the Internet for collection and analysis; the serial port might also be used for remote programming or diagnostics of equipment. USB devices that can directly emulate a standard serial port can be connected directly. Applications wishing to access the remote serial data stream may need to install virtual serial port drivers to translate the TCP data stream into the serial format needed by the application. See the Proxicast web site for a list of known compatible serial interface adapters and drivers.

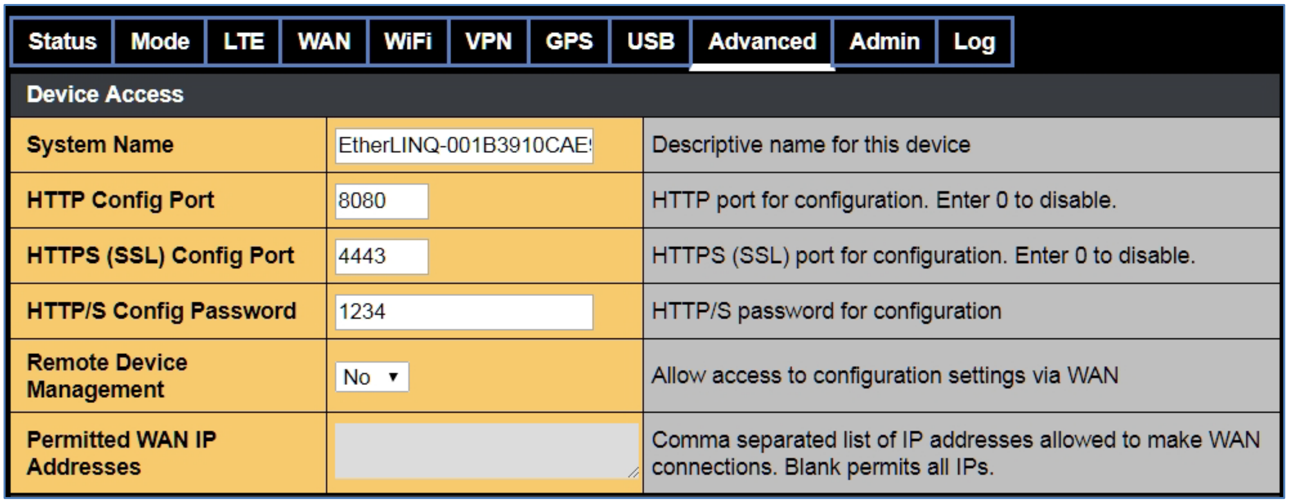
# CHAPTER 13: ADVANCED TAB

The **Advanced t**ab is a collection of functions that control how the EtherLINQ is accessed and other system capabilities:

1. Device Access
2. Scheduled Reboot
3. Dynamic DNS
4. Syslog
5. Advanced Configuration

## 13.1 Device Access

Device Access configures the System Name, management ports and restrictions for accessing the EtherLINQ.



Device Access

| | | |
|---|---|---|
| System Name | EtherLINQ-001B3910CAE! | Descriptive name for this device |
| HTTP Config Port | 8080 | HTTP port for configuration. Enter 0 to disable. |
| HTTPS (SSL) Config Port | 4443 | HTTPS (SSL) port for configuration. Enter 0 to disable. |
| HTTP/S Config Password | 1234 | HTTP/S password for configuration |
| Remote Device Management | No ▾ | Allow access to configuration settings via WAN |
| Permitted WAN IP Addresses | | Comma separated list of IP addresses allowed to make WAN connections. Blank permits all IPs. |

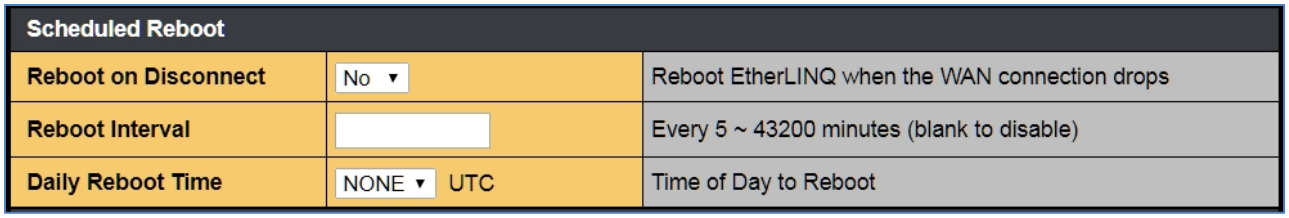
**Figure 41: Device Access Setup**

| | |
|---|---|
| System Name | String which identifies this specific EtherLINQ device. Value is displayed on the upper right of the EtherLINQ management pages. |
| HTTP Config Port | TCP port number used to access the EtherLINQ's configuration screens via HTTP. Default is port 8080. |
| HTTPS (SSL) Config Port | TCP port number used to access the EtherLINQ's configuration screens via HTTPS. Default is port 4443. |
| HTTP/S Config Password | Password required for authenticating to the EtherLINQ's management interface via HTTP or HTTPS. Default is 1234. |
| Remote Device | Enable/Disable access to the EtherLINQ's management pages from WAN devices. |

| | |
|---|---|
| Management | **NOTE 1:** Remote Device Management is DISABLED by default as a security measure to protect the EtherLINQ from Internet threats. Remote Device Management must be enabled in order to manage the EtherLINQ remotely over the Internet. The EtherLINQ configuration system is always available over the LAN interface.<br>**NOTE 2:** Enabling Remote Device Management requires that the EtherLINQ's default password to be changed. |
| Permitted WAN IP Addresses | If Remote Device Management is enabled, access to the EtherLINQ's management interface can be restricted to specific remote IP addresses. Enter a comma delimited list of permitted IP addresses. |

## 13.2 Scheduled Reboot

The EtherLINQ can reboot itself under various conditions.



**Scheduled Reboot**

| | | |
|---|---|---|
| **Reboot on Disconnect** | No ▾ | Reboot EtherLINQ when the WAN connection drops |
| **Reboot Interval** | | Every 5 ~ 43200 minutes (blank to disable) |
| **Daily Reboot Time** | NONE ▾ UTC | Time of Day to Reboot |

**Figure 42: Schedule Reboot Setup**

| | |
|---|---|
| Reboot on Disconnect | The EtherLINQ can reboot whenever it detects that a WAN interface is down. This can help re-establish WAN connections in some instances. |
| Reboot Interval | Reboots can occur on a countdown timer from the previous reboot. Use this setting to reboot at regular intervals from 5 minutes to 43,200 minutes (30 days). |
| Daily Reboot Time | The EtherLINQ can reboot every day at a selected time.<br>**NOTE:** Reboot time is always specified in UTC. |

**Note**: The Interval and Daily reboot timers can be combined. For example, the EtherLINQ can restart every 8 hours and always at 1 AM UTC so that there is at least one known reboot time. If the Daily Timer is used, do not set the Interval timer greater than 1440 minutes (24 hours).

## 13.3 **Dynamic DNS (DDNS)**

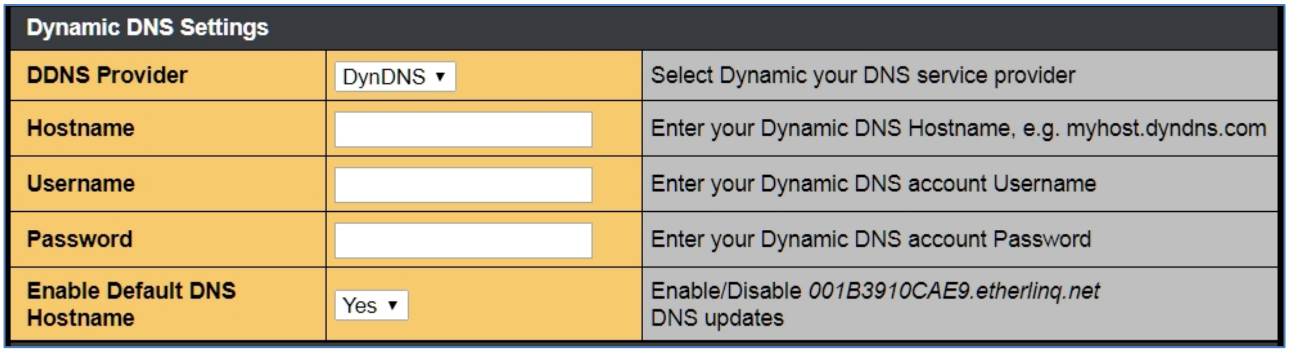
DDNS (Dynamic Domain Name Service) allows an “internet domain name” to be assigned to an EtherLINQ which has a public WAN IP address. This makes it possible for other Internet devices to connect to the EtherLINQ without needing to use the WAN IP address.

DDNS is useful when the EtherLINQ is used in IP Pass-Through or NAT Router Modes. It allows remote Internet users to connect to LAN device(s) by using a domain name, rather than an IP address. For example, assume that you wish to remotely access a web server embedded in one of your LAN devices, but the EtherLINQ obtains a different IP address from your ISP every time it connects to the Internet. In this case, DDNS allows users to connect to the web server through a fixed domain name without regard for the changing IP address of the WAN connection.

**NOTE :** DDNS only works if the WAN port receives a public (Internet routable) IP address and the ISP does not block in-bound initiated connections. Many cellular service providers are now assigning private or blocked IP addresses by default. Contact your service provider regarding the availability of a public IP address.

**NOTE :** As a service to its customers, Proxicast operates a Dynamic DNS service which is automatically updated each time an EtherLINQ WAN IP changes. The DDNS host name is the serial number of the EtherLINQ in the ”etherlinq.net” domain. For example: 001B3910CAE9.etherlinq.net.

Additionally, the EtherLINQ supports custom DDNS hostname via the DynDNS and No-IP web services. Contact these organizations to create an account and hostname.



| Dynamic DNS Settings | | |
|---|---|---|
| DDNS Provider | DynDNS ▾ | Select Dynamic your DNS service provider |
| Hostname | | Enter your Dynamic DNS Hostname, e.g. myhost.dyndns.com |
| Username | | Enter your Dynamic DNS account Username |
| Password | | Enter your Dynamic DNS account Password |
| Enable Default DNS Hostname | Yes ▾ | Enable/Disable *001B3910CAE9.etherlinq.net* DNS updates |

**Figure 43: Dynamic DNS Setup**

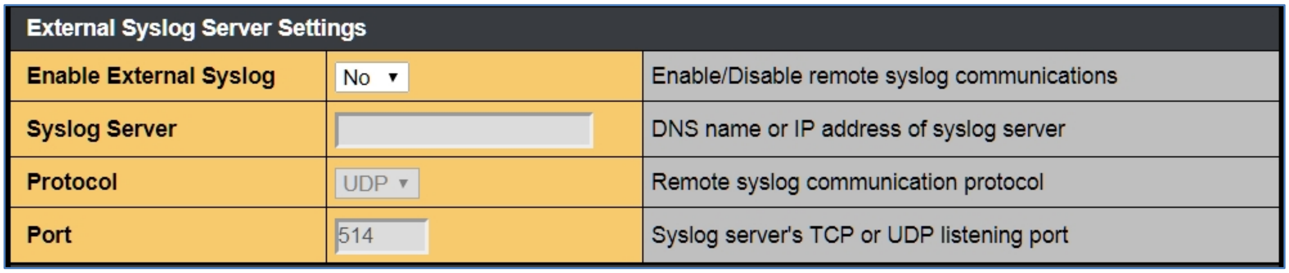
| | |
|---|---|
| DDNS Provider | DynDNS and No-IP services are supported. |
| Hostname | Enter the full-qualified domain name (FQDN) for this specific EtherLINQ as |

| | |
|---|---|
| | defined in your account at the DDNS service provider. Enter the entire domain name, e.g.: myrouter.mydomain.com<br>This hostname must be defined within your DDNS service provider account before it can be updated by the EtherLINQ. The hostname must match exactly on both the DDNS account and this field. |
| User Name | Enter the username for your DDNS service provider account. We recommend avoiding special characters (#, $, &, @, etc) in your username. |
| Enable Default DNS Hostname | Disabling this feature prevents the EtherLINQ from attempting to update Proxicast's DNS server. |

The EtherLINQ updates the DDNS service whenever the active WAN IP address changes due to WAN Fail-Over or renewal of the WAN IP address.

## 13.4 **Syslog Server**

Syslog is a standard mechanism for transmitting and storing system log information from a device to a remote server. The EtherLINQ can send its system event log 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.



**External Syslog Server Settings**

| | | |
|---|---|---|
| **Enable External Syslog** | No ▾ | Enable/Disable remote syslog communications |
| **Syslog Server** | | DNS name or IP address of syslog server |
| **Protocol** | UDP ▾ | Remote syslog communication protocol |
| **Port** | 514 | Syslog server's TCP or UDP listening port |

**Figure 44: Syslog Server Setup**

| | |
|---|---|
| Enable External Syslog | Enable/Disable the Syslog feature |
| Syslog Server | IP address or fully qualified domain name of the Syslog server which will receive event messages |
| Protocol | IP protocol (TCP or UDP) that the Syslog server expects messages to use |
| Remote Port | Port number that the remote Syslog server is listening on (default is UDP514) |

## 13.5 **Additional Configuration**

The Additional Configuration Settings field is used to send advanced configuration parameters to the EtherLINQ which are not available in the graphical user interface. Settings entered into the Additional Configuration Settings field are saved as part of the EtherLINQ's overall configuration. Refer to the TechNote *ELTN0001: EtherLINQ Command Reference* for a list of available configuration parameters and values.

Additional Configuration Settings

**Figure 45: Additional Configuration Setup**

The EtherLINQ generates the necessary basic settings on each save; additional commands are used mostly for debugging and technical support issues. However, several functions may be useful in certain common situations.

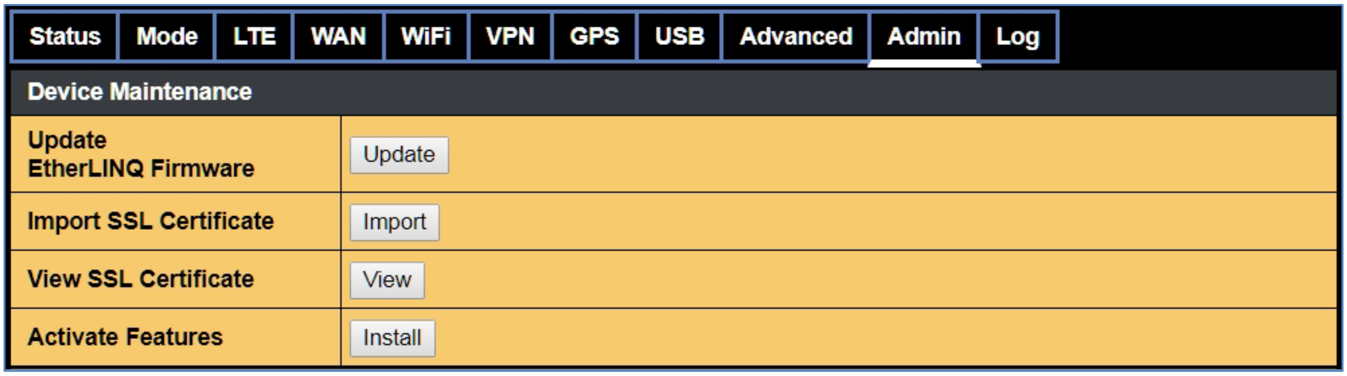
| | |
|---|---|
| DISABLERESET=1 | Prevents the hardware **Reset** button from performing a reset to factory settings when pressed for 10 seconds. The 2 second Configuration Mode press is still permitted. Useful to prevent accidental or unwanted configuration resets. |
| LOGTOSD=1 | Writes the System Event Log to the microSD card; entries are appended to the file *systemname.log* at the root of the microSD card. Allows event log entries to be recorded across system restarts. Remove the drive to examine the log file with a PC. Log files limited to 64 MB in size. |
| LOGTOUSB=1 | Writes the System Event Log to a USB flash memory drive; entries are appended to the file *systemname.log* at the root of the USB drive. Allows event log entries to be recorded across system restarts. Remove the drive to examine the log file in with a PC. Log files limited to 64 MB in size. |
| DELTACSQ=n<br>where n = 0 to 100<br>default = 10 | Log changes in Signal Quality that exceed n% of the prior value. Set higher to suppress nuisance log entries when signal strength changes dramatically; set lower to monitor signal level changes more closely. |

# CHAPTER 14: ADMIN TAB

The **Admin t**ab contains a collection of tools for administering and maintaining the EtherLINQ including firmware updates, configuration backup/restore and diagnostics.

## 14.1 Device Maintenance

This section allows users to manually upgrade EtherLINQ firmware, view and install SSL certificates and activate/deactivate optional EtherLINQ features. Each button leads to additional screens to complete the action.



| Device Maintenance | |
|---|---|
| Update<br>EtherLINQ Firmware | Update |
| Import SSL Certificate | Import |
| View SSL Certificate | View |
| Activate Features | Install |

**Figure 46: Device Maintenance Functions**

| | |
|---|---|
| Update EtherLINQ Firmware | Begins the interactive process of manually installing new EtherLINQ firmware. See *Section Chapter 1:A.6 Updating EtherLINQ Firmware* for more information. |
| Import SSL Certificate | The EtherLINQ contains a self-signed X.509 SSL certificate that is used by the internal HTTPS server. Users may import their own SSL certificates to replace the self-signed certificate. See *Section 14.1.1 SSL Certificate Format*. |
| View SSL Certificate | Displays the decoded contents of the currently active EtherLINQ SSL certificate |
| Activate Features | The EtherLINQ has a number of features that can be installed or removed. Certain EtherLINQ models may include one or more optional features; other features may require a separate license. See *Section 14.1.2 Activating & Deactivating Features*. |

### 14.1.1 SSL Certificate Format

SSL certificates to be imported into the EtherLINQ must be in PEM format and consist of the device certificate, any intermediate certificates between the device and a browser-trusted Certificate Authority, followed by the private key for the device certificate, all appended together in a single text file.

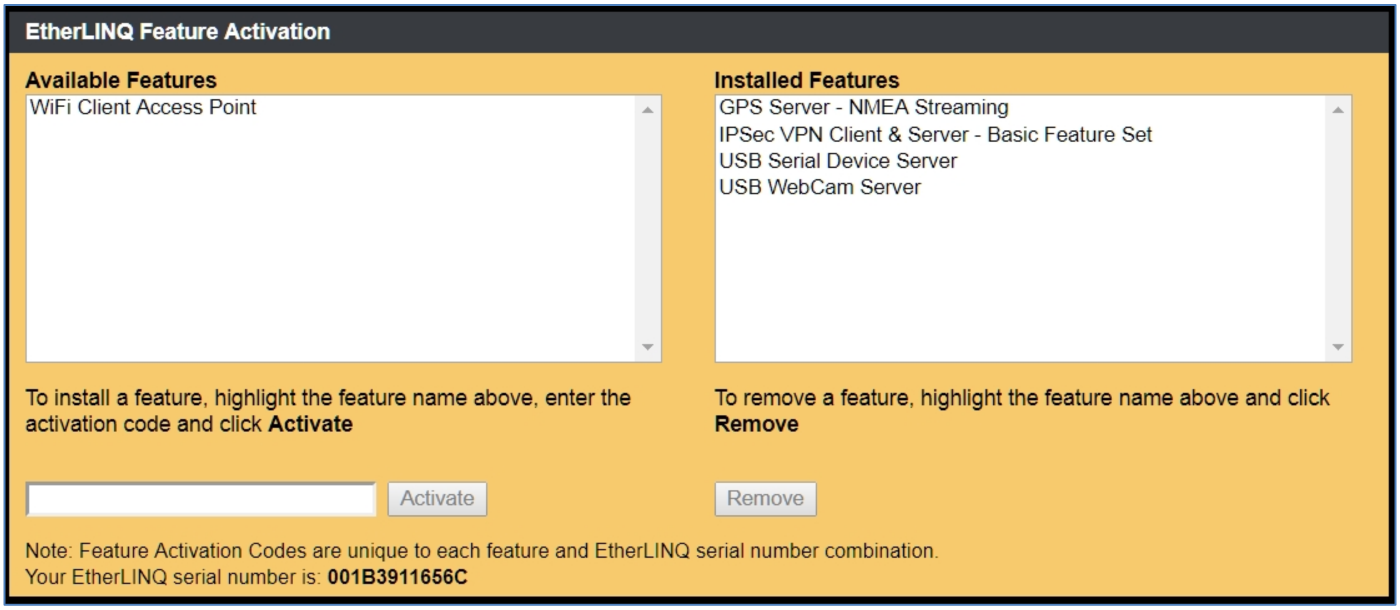
```
-----BEGIN CERTIFICATE-----
MIIGCDCCA/CgAwIBAgIQKy5u6tl1NmwUim7bo3yMBzANBgkqhkiG9w0BAQwFADCB
. . .
+AZxAeKCINT+b72x
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIFdDCCBFygAwIBAgIQJ2buVutJ846r13Ci/ITeIjANBgkqhkiG9w0BAQwFADBv
. . .
pu/xO28QOG8=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIFYDCCBEigAwIBAgIQFut20fVLtx4nwKSkqbG2kjANBgkqhkiG9w0BAQsFADCB
. . .
H6uv7JYa63uvx8imblP3FsrXcPOPayb0SRln6lrtfUoC0cJy
-----END CERTIFICATE-----
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAvR1xm2u7Yd9uKJ3JYWjGSWb0qbQd1X3pWWS6ap8WC6+dQl1e
. . .
aQDd9AdM+LPoFCcgVfaahj0gCQWYvYH2dC0i3zzp+MHQLCCq/1cGsw==
-----END RSA PRIVATE KEY-----
```

**Figure 47: SSL Certificate Example (abridged)**

### 14.1.2 Activating & Deactivating Features

Many of the EtherLINQ's non-core features can be selectively enabled or disabled as needed. For example, to prevent unauthorized use of WiFi, the entire WiFi system can be deactivated. Certain other features may not be included in a specific EtherLINQ model, but can be licensed and activated separately.

Click the **Install** button to view or change the EtherLINQ's active features (Figure 48).



EtherLINQ Feature Activation

**Available Features**

WiFi Client Access Point

**Installed Features**

GPS Server - NMEA Streaming
IPSec VPN Client & Server - Basic Feature Set
USB Serial Device Server
USB WebCam Server

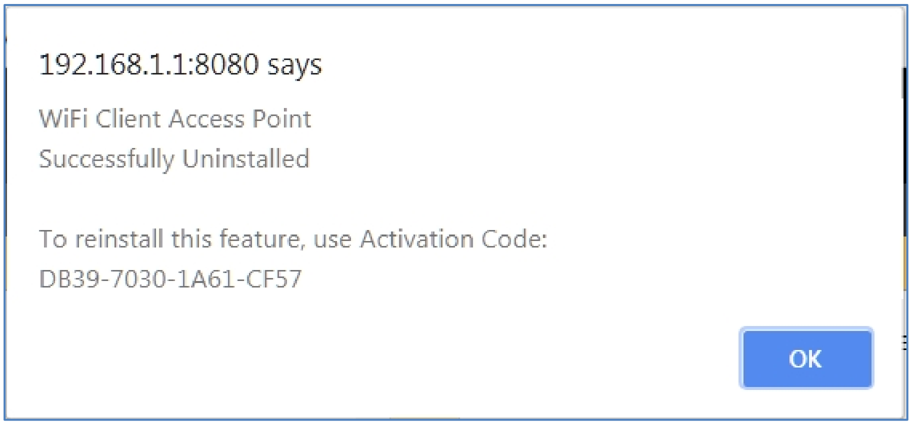
To install a feature, highlight the feature name above, enter the activation code and click **Activate**

To remove a feature, highlight the feature name above and click **Remove**

Note: Feature Activation Codes are unique to each feature and EtherLINQ serial number combination.
Your EtherLINQ serial number is: **001B3911656C**

**Figure 48: Feature Activation**

EtherLINQ features are authorized by Activation Codes which are unique to each feature/EtherLINQ serial number pair. To install a feature, highlight an Available Feature and enter its activation code. To remove a feature, highlight an Installed Feature and click the **Remove** button. The EtherLINQ will display the activation code for this feature (Figure 49) – make note of the activation code in case you need to re-activate the feature in the future. Also, if the EtherLINQ is reset to factory defaults, any activated features will be lost and must be reactivated.



192.168.1.1:8080 says

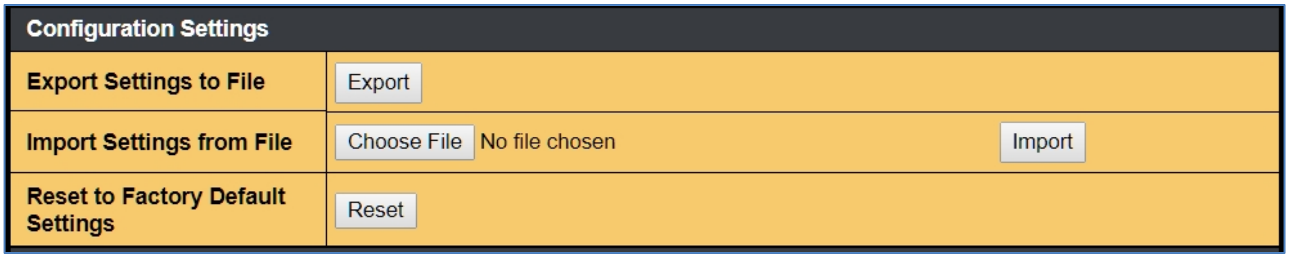
WiFi Client Access Point
Successfully Uninstalled

To reinstall this feature, use Activation Code:
DB39-7030-1A61-CF57

**Figure 49: Feature Activation Code**

## 14.2 Configuration Settings

The EtherLINQ's configuration settings can be saved to an external file and later restored. This assists with backups should the EtherLINQ be reset and can also be used to "clone" settings from one EtherLINQ to another.



| Configuration Settings | |
|---|---|
| Export Settings to File | Export |
| Import Settings from File | Choose File No file chosen Import |
| Reset to Factory Default Settings | Reset |

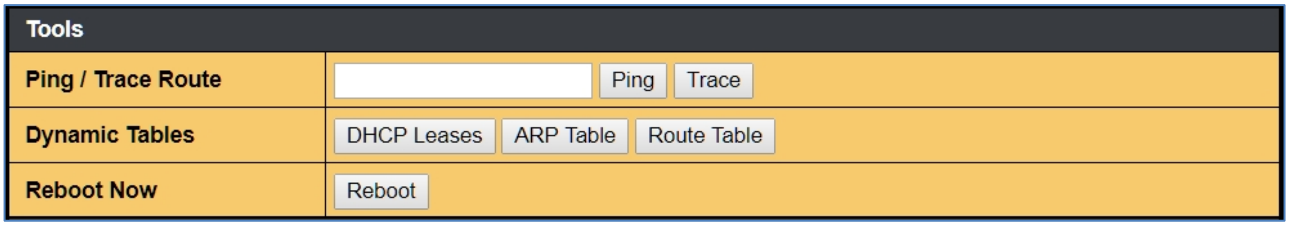
**Figure 50: Save / Restore / Reset Configuration Settings**

| | |
|---|---|
| Export Settings to File | Click to save the EtherLINQ's current settings to a file on your PC. Do not edit this file or it will not be able to be used to re-import the settings. |
| Import Settings from File | Configuration settings saved to a file by the Export process can be imported into any EtherLINQ. We recommend only importing configurations saved using the same EtherLINQ firmware revision.<br>**NOTE:** Importing a saved configuration file will cause the EtherLINQ to reboot and apply the new settings. |
| Reset to Factory Default Settings | Returns the EtherLINQ to the original factory default settings; any custom settings will be lost. This button performs the same function as pressing the physical **Reset** button on the EtherLINQ. *See Section A.8 EtherLINQ Default Settings*. |

Configuration settings may also be imported by saving the desired settings on an EtherLINQ, then using the **Export Settings to File** procedure above. Rename the output file to *EtherLINQ.cfg* and copy that file to the root of a USB drive. Insert the USB drive into a different EtherLINQ, power on that EtherLINQ and wait for the OS LED to stop flashing, then power off the EtherLINQ. When the second EtherLINQ is powered on again, it will have the settings from *EtherLINQ.cfg* file. This technique is useful for quickly cloning a large number of EtherLINQs.

## 14.3 Tools

The Tools section includes several functions for checking WAN connectivity and other EtherLINQ operating state information.



| Tools | |
|---|---|
| Ping / Trace Route | Ping Trace |
| Dynamic Tables | DHCP Leases ARP Table Route Table |
| Reboot Now | Reboot |

**Figure 51: Tools**

| | |
|---|---|
| Ping / Trace Route | Enter an IP address or FQDN in the field.<br>The **Ping** button sends 4 ICMP packets to the indicated destination.<br>The **Trace** button initiates a Trace Route command to the destination.<br>Results are displayed in an overlay window. |
| Dynamic Tables | The **DHCP Leases** button shows the devices to which the EtherLINQ has issued an IP address to via a DHCP request.<br>The **ARP Table** button displays a list of external IP and MAC addresses that have recently communicated with the EtherLINQ.<br>The **Route Table** button displays the current WAN routing information. |
| Reboot Now | This button causes the EtherLINQ to restart |

## 14.4 Debug Information

The buttons in this section provide detailed information about the internal operation of the EtherLINQ.

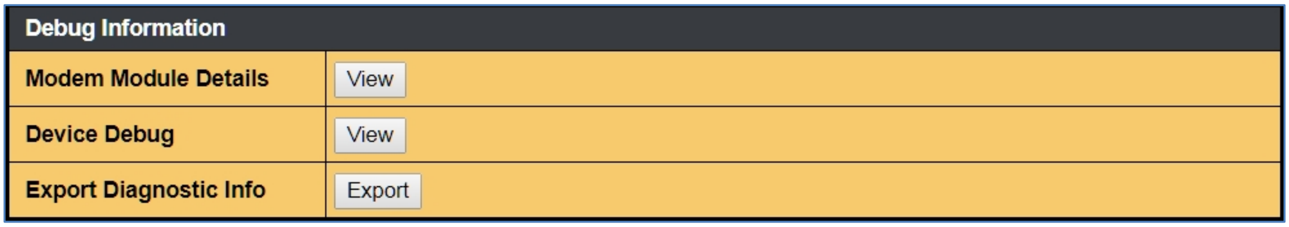


**Figure 52: Debug Functions**

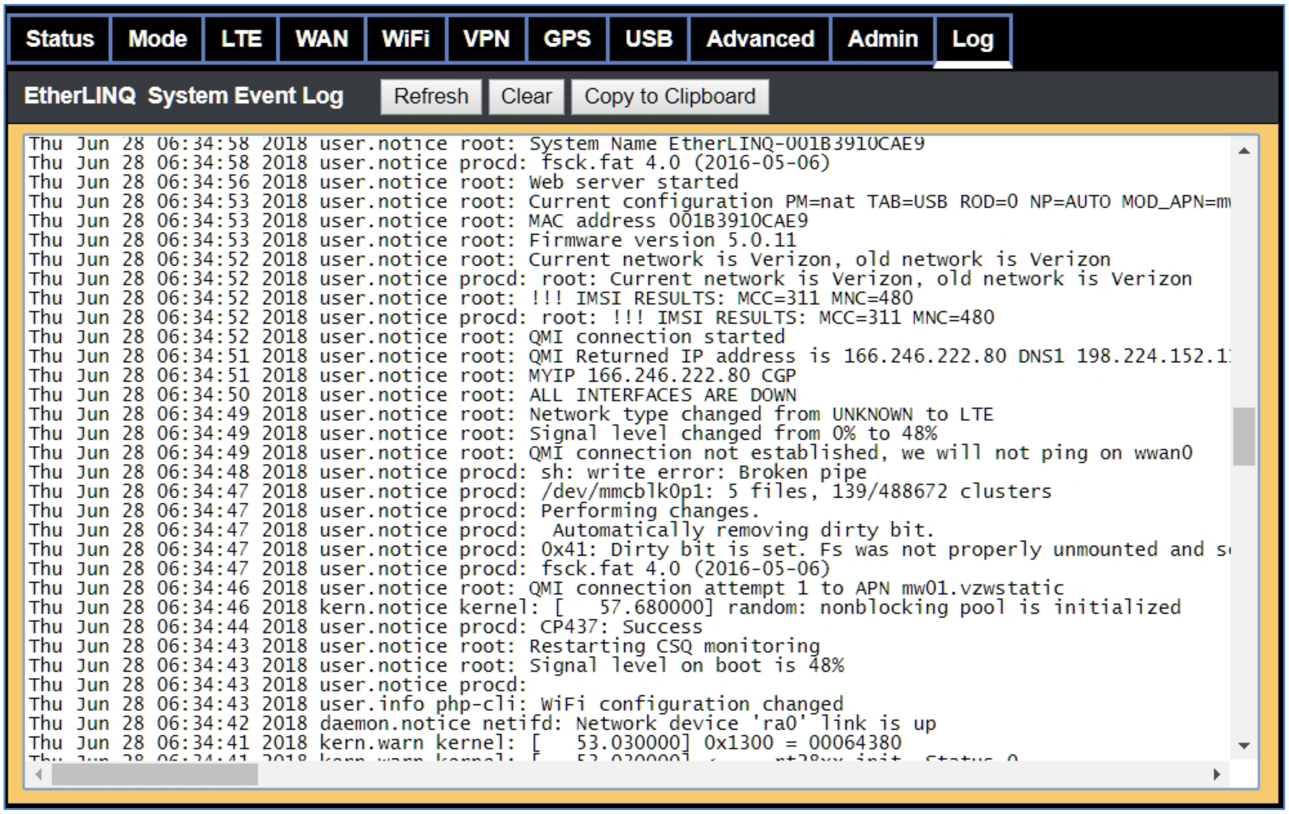
| | |
|---|---|
| Modem Module Details | Displays a screen with information about the EtherLINQ’s internal LTE modem module. This information can be helpful when troubleshooting connectivity issues. |
| Device Debug | Displays a summary of the EtherLINQ’s diagnostic and status information |
| Export Diagnostic Info | When requested by Proxicast Technical Support, use this button to produce a file on your PC with detailed diagnostic and log information. Forward the saved file to Proxicast for analysis. |

# CHAPTER 15: LOG TAB

The **Log t**ab displays the EtherLINQ's system event log history which records various events that have occurred since the last EtherLINQ reboot. The log is displayed in reverse chronological order (newest entries at the top).

The EtherLINQ has a limited amount of space available for log events – the oldest events are overwritten when the log is full. See Sections 13.4 - *Syslog Server* and *13.5:Additional Configuration* regarding techniques for storing system log events over longer periods of time. The log timestamps are always in UTC.

The **Refresh** button updates the log display with the latest events. The **Clear** button erases the entire system log. The **Copy to Clipboard** button copies the current syslog to the PC's clipboard for use in other applications.



```
Thu Jun 28 06:34:58 2018 user.notice root: System Name EtherLINQ-001B3910CAE9
Thu Jun 28 06:34:58 2018 user.notice procd: fsck.fat 4.0 (2016-05-06)
Thu Jun 28 06:34:56 2018 user.notice root: Web server started
Thu Jun 28 06:34:53 2018 user.notice root: Current configuration PM=nat TAB=USB ROD=0 NP=AUTO MOD_APN=m
Thu Jun 28 06:34:53 2018 user.notice root: MAC address 001B3910CAE9
Thu Jun 28 06:34:53 2018 user.notice root: Firmware version 5.0.11
Thu Jun 28 06:34:52 2018 user.notice root: Current network is Verizon, old network is Verizon
Thu Jun 28 06:34:52 2018 user.notice procd: root: Current network is Verizon, old network is Verizon
Thu Jun 28 06:34:52 2018 user.notice root: !!! IMSI RESULTS: MCC=311 MNC=480
Thu Jun 28 06:34:52 2018 user.notice procd: root: !!! IMSI RESULTS: MCC=311 MNC=480
Thu Jun 28 06:34:52 2018 user.notice root: QMI connection started
Thu Jun 28 06:34:51 2018 user.notice root: QMI Returned IP address is 166.246.222.80 DNS1 198.224.152.1
Thu Jun 28 06:34:51 2018 user.notice root: MYIP 166.246.222.80 CGP
Thu Jun 28 06:34:50 2018 user.notice root: ALL INTERFACES ARE DOWN
Thu Jun 28 06:34:49 2018 user.notice root: Network type changed from UNKNOWN to LTE
Thu Jun 28 06:34:49 2018 user.notice root: Signal level changed from 0% to 48%
Thu Jun 28 06:34:49 2018 user.notice root: QMI connection not established, we will not ping on wwan0
Thu Jun 28 06:34:48 2018 user.notice procd: sh: write error: Broken pipe
Thu Jun 28 06:34:47 2018 user.notice procd: /dev/mmcblk0p1: 5 files, 139/488672 clusters
Thu Jun 28 06:34:47 2018 user.notice procd: Performing changes.
Thu Jun 28 06:34:47 2018 user.notice procd:  Automatically removing dirty bit.
Thu Jun 28 06:34:47 2018 user.notice procd: 0x41: Dirty bit is set. Fs was not properly unmounted and s
Thu Jun 28 06:34:47 2018 user.notice procd: fsck.fat 4.0 (2016-05-06)
Thu Jun 28 06:34:46 2018 user.notice root: QMI connection attempt 1 to APN mw01.vzwstatic
Thu Jun 28 06:34:46 2018 kern.notice kernel: [   57.680000] random: nonblocking pool is initialized
Thu Jun 28 06:34:44 2018 user.notice procd: CP437: Success
Thu Jun 28 06:34:43 2018 user.notice root: Restarting CSQ monitoring
Thu Jun 28 06:34:43 2018 user.notice root: Signal level on boot is 48%
Thu Jun 28 06:34:43 2018 user.notice procd:
Thu Jun 28 06:34:43 2018 user.info php-cli: WiFi configuration changed
Thu Jun 28 06:34:42 2018 daemon.notice netifd: Network device 'ra0' link is up
Thu Jun 28 06:34:41 2018 kern.warn kernel: [   53.030000] 0x1300 = 00064380
Thu Jun 28 06:34:41 2018 kern.warn kernel: [   53.030000] <    rt28xx init. Status 0
```

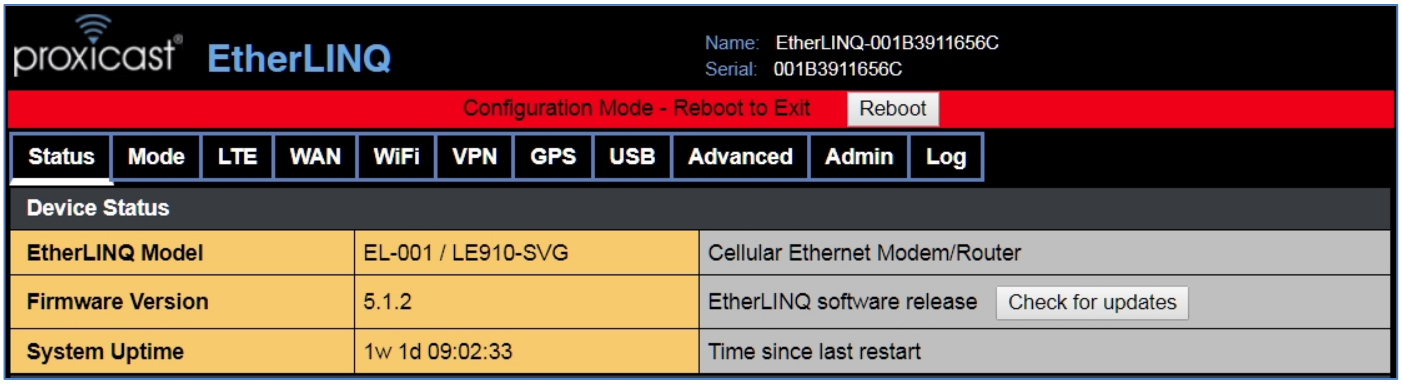
**Figure 53: System Log**

# CHAPTER 16: CONFIGURATION MODE

Configuration Mode is a mechanism for accessing the EtherLINQ via its LAN Ethernet port when it is operating in IP Pass-Through or Virtual Cable mode and thus does not have an assigned IP address. Configuration Mode can also be used when the EtherLINQ is in NAT Router mode and the LAN IP address is unknown.

To access Configuration Mode, press and hold the Reset button on the EtherLINQ's front panel for 2 seconds, until the OS LED begins to flash rapidly, then release the button. The OS LED will continue to flash as long as Configuration Mode is active.

When activated, Configuration Mode forces the EtherLINQ's LAN IP address to 192.168.1.1 and the HTTP port to 8080 (HTTPS=4443). The system password is not affected. Access the EtherLINQ at http://192.168.1.1:8080



Name: EtherLINQ-001B3911656C
Serial: 001B3911656C

Configuration Mode - Reboot to Exit

| Device Status | | |
|---|---|---|
| EtherLINQ Model | EL-001 / LE910-SVG | Cellular Ethernet Modem/Router |
| Firmware Version | 5.1.2 | EtherLINQ software release |
| System Uptime | 1w 1d 09:02:33 | Time since last restart |

**Figure 54: Configuration Mode**

Configuration Mode is indicated by a red banner across the EtherLINQ's web page header (Figure 54). Any settings may be modified while in Configuration Mode. To exit Configuration Mode and return to regular EtherLINQ operations, a system reboot is required. Press the **Reboot** button in the banner or power-cycle the EtherLINQ.

# APPENDIX

## A.1 Common Tasks

| HOW TO | WHERE | ACTION |
|---|---|---|
| Change the LAN IP Address | Mode Tab | Enter the IP address to be assigned to the EtherLINQ and select the subnet mask for the LAN. The DHCP Server will automatically adjust to the new subnet. |
| Configure the LTE APN | LTE Tab | Enter the Access Point Name (APN) assigned to your SIM. Also configure LTE Keep-Alive settings. |
| Change the WiFi Password | WiFi Tab | Configures the Access Point's SSID and security settings. |
| Forward Ports to LAN Devices | Mode Tab > NAT Router Mode | Enter up to 10 port-forward / translation rules. |
| Set up a VPN | VPN Tab | Enable IPSec and Add new rules for each VPN tunnel. |
| Configure WAN Fail-Over | WAN Tab | Set WAN priority, fail-over and connection Keep-Alive settings. |
| Restart Periodically | Advanced Tab > Scheduled Reboot | Select the frequency for the EtherLINQ to automatically reboot. |
| Change the System Name | Advanced Tab > Device Access | Enter the System Identification. |
| Change the EtherLINQ Password | Advanced Tab > Device Access | Passwords are case sensitive. The username cannot be changed from "admin" however multiple users may log in concurrently. |
| Change the Administration Ports | Advanced Tab > Device Access | HTTP and HTTPS can be assigned to any port or disabled as necessary to avoid port conflicts or increase security. |
| Backup / Restore Settings | Admin Tab > Configuration Settings | Settings can be saved or restored; EtherLINQ can be reset to factory default settings. |
| Enable Bridge Mode | Mode Tab > IP Pass-Through | Passes the WAN IP address to first LAN device that requests a DHCP address. |
| Enable Virtual Cable Mode | Mode Tab > Virtual Cable | Bridges the EtherLINQ to other EtherLINQs and PocketPORTs through any intervening network topology. |
| Update Firmware | Status Tab> Check For Updates button | Requires an active WAN connection to check the Proxicast server for updates. Manual updates can be installed via the Admin Tab. |

## A.2 Troubleshooting

| PROBLEM | CORRECTIVE ACTION |
|---|---|
| None of the LEDs turn on | Ensure that the correct power adapter is connected to the EtherLINQ 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 EtherLINQ from a PC on the LAN | Check the cable between the computer (or hub/switch) and the EtherLINQ. Check that the corresponding LAN port LED is ON.<br>Enable Configuration Mode.<br>Configure the PC to receive its IP settings via DHCP (automatic assignment).<br>Confirm that any other network interfaces on the PC (such as WiFi) are disabled. |
| Cannot ping the EtherLINQ from the LAN | If the LAN LEDs are off, check the cable connections.<br>Verify that the IP address and subnet of the EtherLINQ is in the same range as the computers on the LAN and that the EtherLINQ is the default gateway for all LAN devices. |
| Cannot make (or maintain) a cellular data connection<br>(i.e. no LTE WAN IP address) | Confirm that the SIM has been provisioned & activated with the correct type of Internet access data service.<br>Ensure that the SIM/RUIM card (if required) is properly inserted.<br>Network registration may take several minutes. |
| Cellular Signal Quality is low | Connections may be unreliable if the signal quality is < 33%.<br>Check that the proper external antenna is securely attached.<br>Use coax extension cables to locate the antennas to a more favorable location.<br>Move the EtherLINQ 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 may not be provided until after the ISP verifies the MAC address. Confirm the verification method used by the ISP.<br>Check the EtherLINQ’s connection to the wired WAN (cable/DSL modem).<br>Check whether the Ethernet WAN connection requires a crossover cable. |
| After pressing RESET, cannot make a WAN connection | The RESET button returns the EtherLINQ to its factory default settings including clearing the LTE APN and WAN parameters. |

## A.3 Common Carrier Specific Issues

| CARRIER | COMMENT |
|---|---|
| Verizon Wireless 4G/LTE | Verizon Wireless' default APN (vzwinternet) provides only NAT'd IP addresses. This prevents all Internet initiated inbound (remote access) connections from reaching the EtherLINQ.<br>Use the EtherLINQ's IPSec VPN features to make an outbound connection to a VPN server on another network or use Virtual Cable mode to connect to another EtherLINQ; or<br>Purchase a static public IP address from Verizon for an additional fee. |
| AT&T Wireless | AT&T's default APN (broadband) blocks all packets originating from the Internet. To access the EtherLINQ or other equipment remotely, request that AT&T provide you access to the i2gold APN or another APN which offers mobile terminated data service.<br>Use the EtherLINQ's IPSec VPN features to make an outbound connection to a VPN server on another network or use Virtual Cable mode to connect to another EtherLINQ; or<br>Purchase a static public IP address from AT&T for an additional fee. |

**Note for Verizon Wireless 4G/LTE Users:**

*The Verizon Wireless 4G/LTE network assigns private IP addresses by default. In order to use the Verizon Wireless 4G/LTE network for remote access and/or control applications, you must request a "static IP" address from Verizon Wireless or utilize two or more EtherLINQs in Virtual Cable Mode to create an Ethernet bridge between the devices. This is a restriction in how the Verizon Wireless 4G/LTE network is implemented and not a limitation of the EtherLINQ.*

**Note for AT&T Wireless Users:**

*The default data service plan from AT&T Wireless assigns private IP addresses to 3G/4G modems. In order to use the AT&T Wireless network for remote access and/or control applications, you must request "mobile terminated data service" from AT&T Wireless in order to obtain a public IP address. Or you may utilize two or more EtherLINQs in Virtual Cable Mode to create an Ethernet bridge between the devices. This is a restriction in how the AT&T Wireless network is implemented and not a limitation of the EtherLINQ.*

## A.4 Accessing Remote Devices

A common use for the EtherLINQ is to provide remote access to Ethernet equipment from other locations on the Internet. For IP Pass-Through/Bridge Mode and NAT Router Mode, there are three ways to remotely access Ethernet devices connected to the EtherLINQ:

1. Static IP Address
2. EtherLINQ Dynamic DNS Name
3. DynDNS Dynamic DNS Name

When operating in Virtual Cable Mode, remote devices can be accessed by their “private” IP address, just as if they were connected to the local Ethernet network.

### A.4.1 Static IP Address

Some cellular and wired Internet service providers offer a “static” or “permanent” public IP address that is assigned to the modem’s SIM card or router’s MAC address. There is often an additional fee for this feature.

If the SIM / MAC has been assigned a static IP address, the EtherLINQ will automatically receive that IP address when it connects to the Internet as long as the proper Access Point Name (APN) has been configured on the LTE tab (see *Chapter 7: LTE TAB*) or the correct WAN settings have been entered in the WAN tab (see *Chapter 8: WAN TAB*). Use the assigned static IP address to access remote Ethernet devices.

### A.4.2 EtherLINQ Dynamic DNS

Some Internet service providers assign a random (dynamic) public IP address to the modem every time a new connection is made. This makes it impossible to use the modem’s cellular IP address to access remote devices. The solution is a technique called “dynamic DNS”. With dynamic DNS, a unique “fully qualified domain name” (FQDN) is defined to represent the device with a dynamic IP address. Software on the EtherLINQ then updates the DNS system with the FQDN’s new IP address every time that the IP address changes.

Proxicast maintains a dynamic DNS service which assigns each EtherLINQ a unique and permanent FQDN based on the EtherLINQ’s serial number in the form: *serial#.ethelinq.net* (e.g. 001B39AB12CD.etherlinq.net). The IP address for this DNS name is updated automatically every time the EtherLINQ makes a new WAN connection.

Use this FQDN to access an Ethernet device connected to the EtherLINQ from anywhere on the Internet. For example, if the Ethernet device has an embedded web server, it can be accessed with a web browser by using the address: http://001B39AB12CD.etherlinq.net

### A.4.3 Dynamic DNS

To define your own (perhaps more memorable) FQDN, the EtherLINQ supports the widely used DynDNS.com and NoIP dynamic DNS services.

Visit DynDNS.com or NoIP.com to create a username, password and hostname. Enter these values into the Dynamic DNS section of the EtherLINQ's configuration page (see *Section 13.3Dynamic DNS (DDNS)*).

The EtherLINQ will automatically update the Dynamic DNS servers every time a new WAN IP address is assigned. Use the defined hostname (e.g. *myhost.dyndns.com*) to remotely access the Ethernet device attached to the EtherLINQ.

### A.4.4 Port Forwarding – NAT Router Mode

To remotely access an Ethernet device when operating the EtherLINQ in NAT Router Mode, the "private" IP address of the Ethernet device must be defined as the Port Forwarding target destination for the NAT Router. See *Section 6.1 NAT Router Mode* for a detailed explanation of the EtherLINQ's port-forwarding/translation features.

### A.4.5 Internet Service Provider Restrictions

Some Internet service providers assign "private" IP addresses in the ranges of:

- 10.0.0.0 – 10.255.255.255
- 172.16.0.0 – 172.31.255.255
- 192.168.0.0 – 192.168.255.255

Private IP addresses cannot be used in remote access applications (except in Virtual Cable Mode). Request that the Internet service company provide a routable "public" IP address for your modem. For LTE modems, this may involve changing the Access Point Name (APN) used to connect to the LTE network.

Also, some Internet providers may block certain (or all) "inbound" traffic from the Internet based on the type of service to which you have subscribed. Check with the service provider for more information on options for unblocking inbound connections from the Internet to the EtherLINQ. If you are unable to obtain an unblocked WAN connection, consider using Virtual Cable Mode which uses "outbound" connections to link two sites into a virtual private network.

If you can only obtain a private WAN IP address, do not use the same private subnet for the EtherLINQ LAN networks in NAT Router Mode.

## A.5 Cellular Signal Issues

**Maximizing Signal Strength**

- Place the antenna outside or near a window and as high as possible. Avoid placing in front of “Low-E” glass windows.
- Avoid interference sources such as metal enclosures, lighting fixtures, machinery, and computer/radio equipment.
- Use 2 identical antennas; if using only 1 antenna, connect it to the Main port.
- Keep antenna cabling as short as possible with the minimum number of connectors.

**Signal Quality Graph Not Visible**

- Use Internet Explorer 9+, Chrome or Firefox
- Enable Javascript support.
- Disable the browser’s prior version compatibility mode.

**Signal Strength Varies Significantly**

- Signal strength varies over time even for stationary locations due to intermittent interference, cell tower and modem power adjustments and other factors.
- A lower consistent reading is preferred over a highly variable reading that may hit higher peak values.
- The antenna may require a metal ground plane placed beneath it for proper operation.

**Signal Strength is Worse with Antenna**

- When changing antenna positions, allow 30-60 seconds for the signal strength readings to stabilize.
- Stand at least 2 feet away from the antenna.
- The lower value may be due to the modem reducing its power output to compensate for the higher gain antenna. If the reading indicates a poor signal, the antenna may be in an unfavorable location, not tuned for the cellular carrier's frequencies or there may be a short in the antenna cable or loose connection.
- The signal loss due to a long cable run or multiple connectors may be offsetting the gain from the antenna.

## A.6 Updating EtherLINQ Firmware

There are 3 methods for updating firmware on the EtherLINQ:

1. The **Check For Updates** button
2. Manual update
3. Via USB memory stick

Unless stated otherwise in the firmware release notes, upgrading the EtherLINQ's firmware will NOT erase any saved configuration settings, but a backup of the EtherLINQ's configuration before updating the firmware is highly recommended. Each EtherLINQ firmware release is independent; the latest version can be installed without installing any intervening releases.

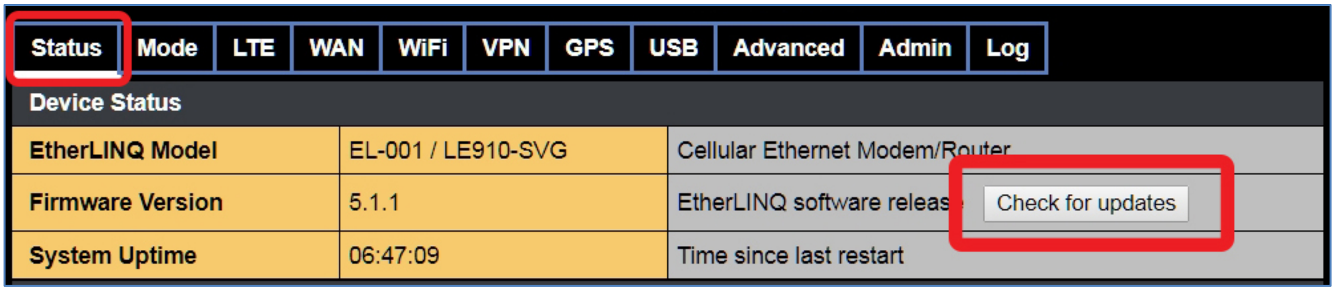
**NOTE :** While the EtherLINQ is installing new firmware, the top row of LEDs will rapidly flash in sequence and the OS LED will turn off. The firmware update process typically takes 6-7 minutes and the EtherLINQ will reboot at the end of the process.

**DO NOT POWER OFF THE ETHERLINQ DURING A FIRMWARE UPDATE**

Powering off the prematurely may permanently damage the EtherLINQ. Wait for the OS LED to remain on solid before attempting to connect to the EtherLINQ or powering the device off.

### A.6.1 Check For Updates Button

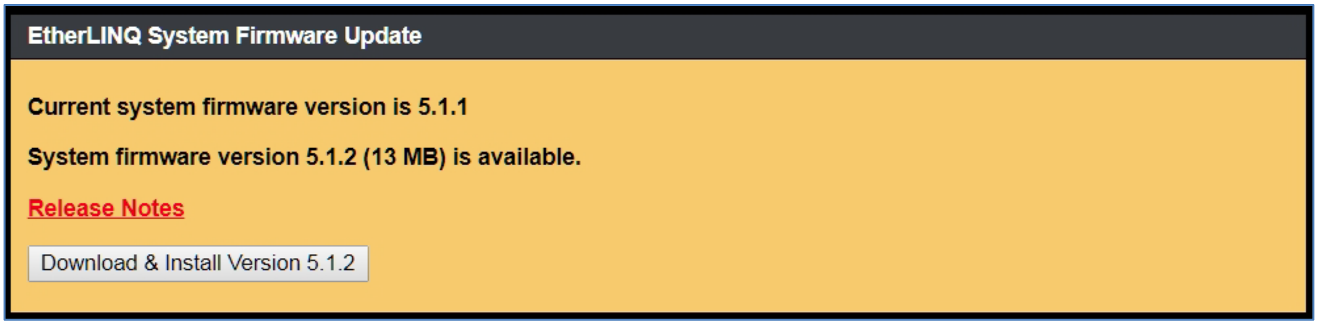
On the Status tab, the button next to the current firmware release causes the EtherLINQ to contact a Proxicast server and report if newer firmware is available. For this firmware update option, the EtherLINQ must have an active Internet connection and a FAT32 formatted microSD memory card installed.



| Device Status | | |
|---|---|---|
| EtherLINQ Model | EL-001 / LE910-SVG | Cellular Ethernet Modem/Router |
| Firmware Version | 5.1.1 | EtherLINQ software releas |
| System Uptime | 06:47:09 | Time since last restart |

**Figure 55: Check for Firmware Updates**

The EtherLINQ will display a results page indicating if newer firmware is available.



EtherLINQ System Firmware Update

Current system firmware version is 5.1.1

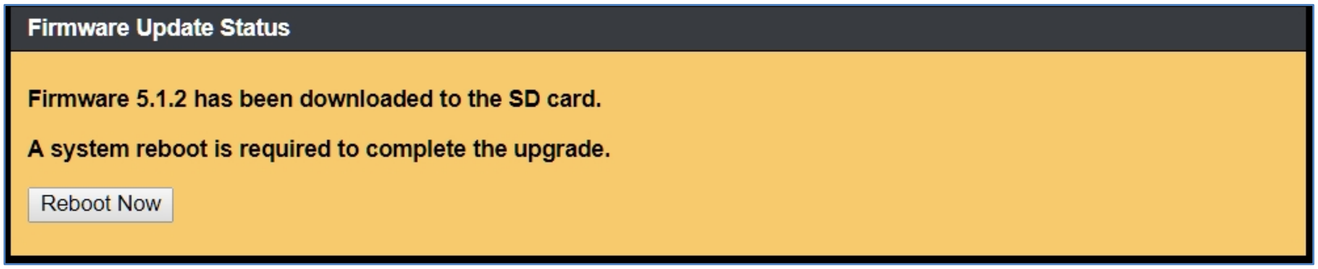
System firmware version 5.1.2 (13 MB) is available.

Release Notes

**Figure 56: Check Updates Status**

Please review the **Release Notes** link to see what changes have been incorporated into the latest EtherLINQ firmware. Click the Download & Install button to begin the firmware update process. Depending on the speed of the EtherLINQ's WAN connection, it may take several minutes for the firmware to download.

When downloading is complete, the EtherLINQ will display a confirmation page. The new firmware will be installed on the next reboot of the EtherLINQ.



Firmware Update Status

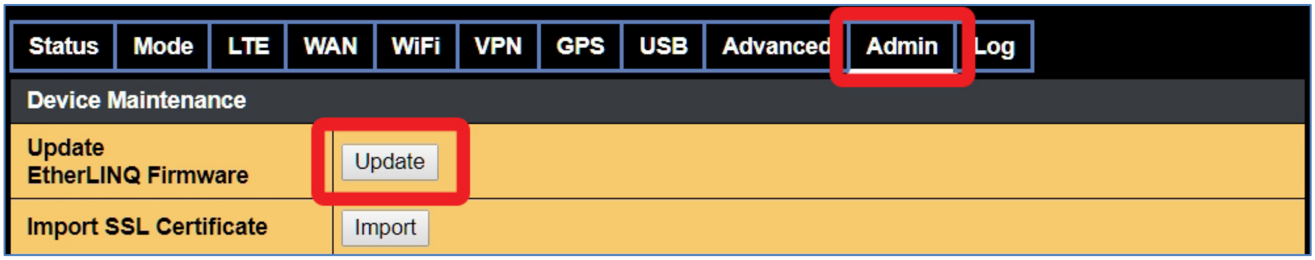
Firmware 5.1.2 has been downloaded to the SD card.

A system reboot is required to complete the upgrade.

**Figure 57: Check Updates Confirmation**

## A.6.2 Manual Firmware Update

The EtherLINQ's firmware can also be updated manually by using the firmware **Update** button on the **Admin** tab. For this option, you must first manually download the EtherLINQ firmware from the Proxicast web site. Check [http://support.proxicast.com](http://support.proxicast.com) for information on the latest EtherLINQ firmware. Both firmware updates and downgrades may be performed using this process.

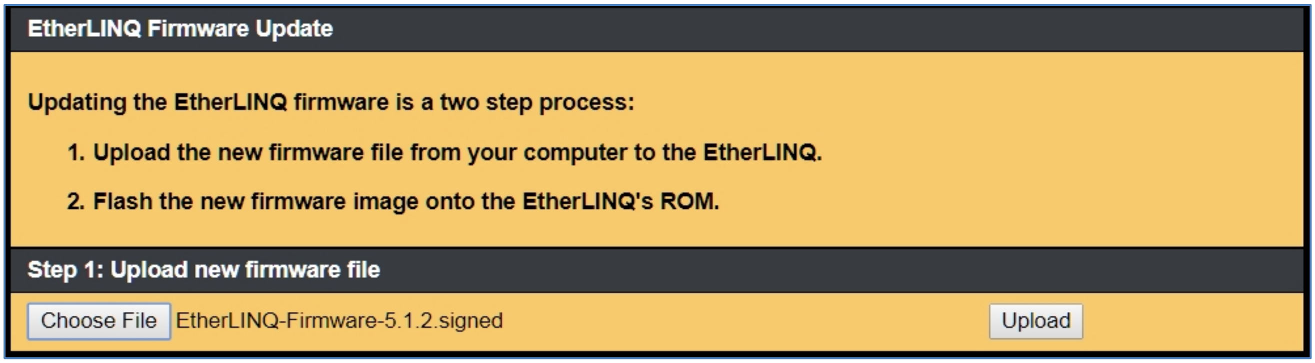


Device Maintenance

| | |
|---|---|
| Update EtherLINQ Firmware | Update |
| Import SSL Certificate | Import |

**Figure 58: Manual Firmware Update**

The **Update** button presents a dialog page to specify the location of the firmware image file that you downloaded from the Proxicast web site (click the **Choose File** button). EtherLINQ firmware image files are digitally signed to ensure that the firmware being installed is genuine Proxicast firmware. EtherLINQ firmware files have a file extension of ".signed".



EtherLINQ Firmware Update

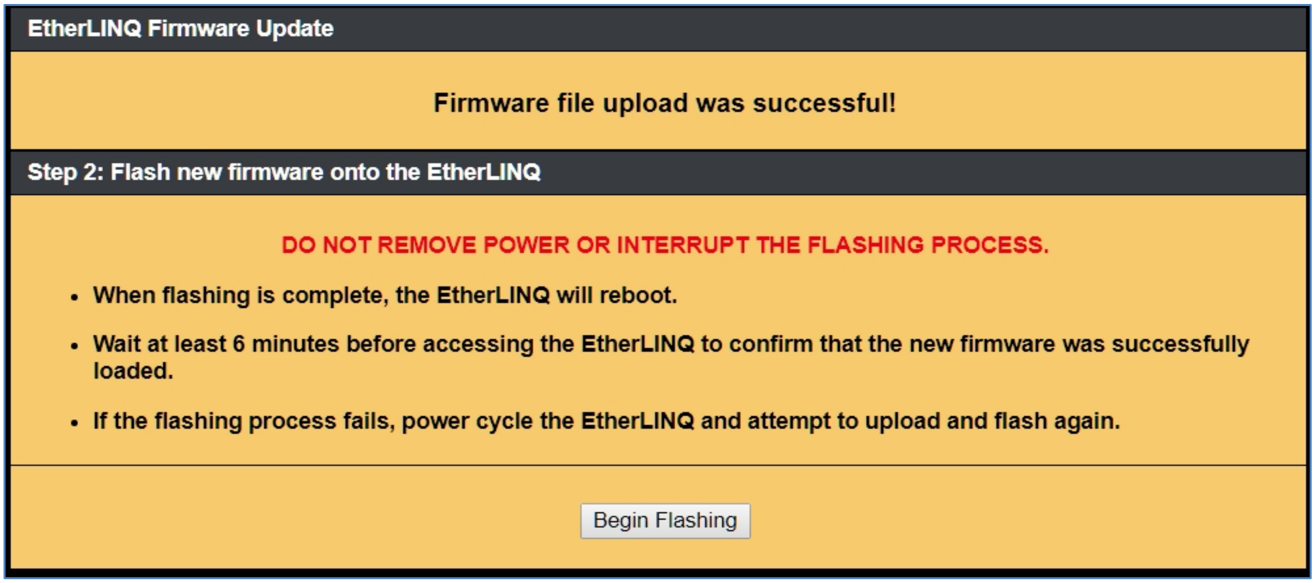
Updating the EtherLINQ firmware is a two step process:

1. Upload the new firmware file from your computer to the EtherLINQ.
2. Flash the new firmware image onto the EtherLINQ's ROM.

Step 1: Upload new firmware file

**Figure 59: Firmware File Selection**

Click the **Upload** button to transfer the firmware file into the EtherLINQ's temporary storage. A confirmation page will display; Click the **Begin Flashing** button to start the actual firmware update process.



EtherLINQ Firmware Update

Firmware file upload was successful!

Step 2: Flash new firmware onto the EtherLINQ

DO NOT REMOVE POWER OR INTERRUPT THE FLASHING PROCESS.

- When flashing is complete, the EtherLINQ will reboot.
- Wait at least 6 minutes before accessing the EtherLINQ to confirm that the new firmware was successfully loaded.
- If the flashing process fails, power cycle the EtherLINQ and attempt to upload and flash again.

**Figure 60: Firmware Flashing**

### A.6.3 Firmware Update via USB

EtherLINQ firmware can also be installed without access to the user interface via a USB memory stick (thumb drive). This allows field personal to perform updates while maintaining security; it is also a convenient way to update many EtherLINQs quickly. For this procedure a FAT32 formatted USB drive is required.

1. Download the desired EtherLINQ firmware image file from http://support.proxicast.com
2. Copy the file to the root directory of the USB drive. Only have one version of firmware file at the root.
3. Power off the EtherLINQ and insert the USB drive into the EtherLINQ's USB port
4. Power on the EtherLINQ

After several seconds, the EtherLINQ will detect the firmware file on the USB drive and begin the firmware update process. The top row of LEDs will flash rapidly in sequence. Wait for the EtherLINQ to reboot again and the OS LED to remain on solid. Then remove the USB drive.

**NOTE :** This process can only be used to install a higher numbered EtherLINQ firmware version; downgrading requires access to the EtherLINQ's user interface. The EtherLINQ will not attempt to reinstall the same firmware version should the USB drive be left in place.

## A.7 Specifications

| Physical | |
|---|---|
| **Dimensions** | 4.7 x 5.3 x 1.0 in 120 x 135 x 25 mm (excluding antennas & mounting bracket)<br>7.1 x 6.6 x 1.0 in 180 x 168 x 25 mm (including antenna & mounting bracket) |
| **Weight** | 12 oz (0.34 kg) (excluding antennas & mounting bracket)<br>18 oz (0.51 kg) (including antennas & mounting bracket) |
| **Power Specification** | 9-28 DC input (12 VDC typical) |
| **Power Consumption** | < 3W Typical |
| **Operating Temp.** | -22 to 140 F (-30~60 C) |
| **Operating Humidity** | 10%~90% |
| **Chassis** | 18 ga. Steel. Desktop & Removable Mounting Brackets (included).<br>Kensington Security Slot (lock) |
| **Certifications** | EMC: FCC ID: 2AL8JEL-001 FCC Part 15 Class B, CE-EMC Class B, C-Tick Class B, VCCI Class B<br>Safety: CSA International, CE EN60950-1 (UL60950-1, CSA60950-1, EN60950-1, IEC60950-1) – RoHS Compliant |
| **Connectors** | |
| **LAN 1** | 1 LAN auto-negotiating, auto MDI/MDI-X 10/100 Mbps RJ45 Ethernet port |
| **WAN / LAN 2** | One auto-negotiating, auto MDI/MDI-X 10/100 Mbps RJ-45 Ethernet port.<br>Software definable as a second LAN port. |
| **USB 2.0** | For USB Webcams, serial devices and firmware loading |
| **Power** | 4-pin Molex Mini-Fit with retention clip |
| **Reset Button** | Restores factory default settings & activates Configuration Mode |
| **MicroSD Slot** | For internal temporary storage |
| **SIM** | Mini SIM (2FF) for LTE modem. SIM size adapters included. |
| **Antennas Connectors** | |
| **4G/LTE** | 2x2 MIMO SMA Female antenna jacks.<br>Two 5 dBi paddle style swivel antennas (SMA Male). |
| **WiFi** | 2x2 MIMO Reverse Polarity SMA (RP-SMA) Female antenna jacks.<br>Two 5 dBi rubber duck style swivel 802.11 b/g/n antennas (RP-SMA Male). |
| **GPS**<br>(select models) | SMA Female jack.<br>Active & Passive antennas supported. |
| **WiFi** | |
| **Technology** | 802.11 b/g/n 300 Mbps max |

| | |
|---|---|
| **Operating Mode** | Access Point |
| **Security** | WPA2-PSK, WPA-PSK, WEP, None |
| **4G/LTE Modem (EtherLINQ model EL-001 / LE910-NAG)** | |
| **Module** | Telit LE910; FCC ID: RI7LE910NA |
| **Frequency Bands (MHz)** | **LTE:**<br>B17: 700<br>B5: 850<br>B4: AWS1700/2100<br>B2: 1900 |
| **Speeds (max)** | **LTE Category 3:**<br>DL up to 100 Mbps<br>UL up 50 Mbps |
| **4G/LTE Modem (EtherLINQ model EL-001 / LE910-SVG)** | |
| **Module** | Telit LE910; FCC ID: RI7LE910SV |
| **Frequency Bands (MHz)** | **LTE:**<br>B13: 700<br>B4: AWS1700/2100 |
| **Speeds (max)** | **LTE Category 3:**<br>DL up to 100 Mbps<br>UL up 50 Mbps |
| **Software Functions** | |
| **4G / LTE Features** | 4G/LTE to WAN Fail-Over and Fall-Back<br>4G/LTE Keep-Alive Packets<br>Signal Quality History Graph & Statistics<br>2x MIMO External Antennas Supported |
| **WAN Features** | Static & DHCP Address Assignment<br>Assign WAN port to LAN or Disable port<br>WAN to 4G/LTE Fail-Over and Fall-Back<br>WAN Keep-Alive Packets |
| **Networking** | LAN DHCP Server<br>WAN Fail-over Detection Limits & Controls<br>Port-Forwarding & Translation<br>IP Pass-Through (Bridge) Mode<br>Virtual Cable Mode (Ethernet over IP)<br>Dynamic DNS (DynDNS, NoIP) |

| | |
|---|---|
| | Permanent DNS Address (serial#.etherlinq.net) |
| **IPSec VPN Features** | IPSec Server and Client Modes<br>Site-to-Site & Remote User Access Tunnels<br>Unlimited Simultaneous IPSec Tunnels<br>IKEv1 & IKEv2 Internet Key Exchange<br>DES / 3DES / AES-128 / AES-192 / AES-256 Encryption<br>MD5 / SHA1 / SHA2-256 / SHA2-384 / SHA2-512 Authentication<br>Diffie-Hellmen Groups 1, 2, 5, 14, 15, 16, 17, 18<br>Dead Peer Detection (DPD) |
| **Virtual Cable Mode** | Proprietary end-to-end tunneling through any firewall or network topology.<br>Interoperable with Proxicast's PocketPORT devices in Virtual Cable Mode. |
| **Security Features** | Network Address Translation & Firewall<br>HTTPS / SSL<br>Feature Restriction<br>Digitally Signed Firmware |
| **Internal Application Servers** | Webcam, Serial Device, GPS |
| **System Management** | Web-based Management (Local & Remote)<br>Configuration Backup and Restore<br>Firmware Upgrade and Downgrade via web interface or USB drive<br>Syslog Support<br>Real-Time Logging<br>Scheduled System Restarts<br>Ping, Traceroute Utilities |

## A.8 EtherLINQ Default Settings

| | |
|---|---|
| **LAN IP Address** | 192.168.1.1<br>Subnet mask = 255.255.255.0 |
| **LAN DHCP Server** | Enabled Pool = 192.168.1.33 to .161 |
| **HTTP Management Access** | admin / 1234 on port 8080 |
| **HTTPS Management Access** | admin / 1234 on port 4443 using a self-signed SSL certificate |
| **WAN Security** | All TCP/UDP ports closed. Remote Management Disabled |
| **Operating Mode** | NAT Router |
| **WAN Priority** | 1. Ethernet WAN<br>2. LTE WAN |
| **WAN Fall-Back** | Check every 60 seconds |
| **Ethernet WAN** | DHCP Client Enabled |
| **LTE APN** | Carrier Default<br>AT&T = broadband<br>Verizon = vzwinternet<br>T-Mobile = fast.t-mobile.com |
| **LTE & WAN Keep-Alive** | ICMP Protocol (ping) to 8.8.8.8<br>Frequency = every 5 sec; Timeout = 3 sec; Tolerance = 3 consecutive failures |
| **WiFi Access Point** | Enabled<br>SSID = EtherLINQ-nnnn where nnnn are the last 4 characters of the serial #<br>WPA2 Password = 8 digit number printed on EtherLINQ label |
| **IPSec VPN** | Disabled |
| **GPS Server** | Disabled. TCP Port = 10110 |
| **USB Webcam Server** | Disabled. Video Stream Port = 8081; Live View Port = 8082 |
| **USB Serial Device Server** | Disabled. TCP Port = 5001 |
| **Scheduled Reboot** | Disabled |
| **External Syslog** | Disabled |
| **DNS Host Name** | *serial#.*etherlinq.net |
| **Reserved Ports** | 6644 & 9922 are used internally and cannot be forwarded |

Press the RESET button for 10 seconds to return the EtherLINQ to these settings.

## A.9 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), EtherLINQ, 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.

### Open Source Software

This product contains software distributed under one or more of the following open source licenses: Apache 2.0, GNU General Public License (GPL) Versions 2 and 3, GNU Lesser General Public License (LGPL), MIT License, OpenSSL License, PHP 7 License, and strongSwan License. For more information on this software, including licensing terms and your rights to access source code, contact Proxicast.

## A.10 FCC Certification

### Federal Communications Commission (FCC) Interference Statement

**FCC ID: 2AL8JEL-001**

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:
(1) This device may not cause harmful interference, and
(2) This device must accept any interference received, including interference that may cause undesired operation.

This equipment 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 equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and 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 equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance of 2 7 cm between the radiator and your body. This device and its antennas(s} must not be co-located or operating in conjunction with any other antenna or transmitter except in accordance with FCC multi-transmitter product procedures.

To comply with FCC regulations limiting both maximum RF output power and human exposure to Rf radiation, the maximum WiFi antenna gain must not exceed 7 dBi.

## FCC Caution

This device has been designed for the WLAN 2.4 GHz networks. For product available in the USA/Canada market, only channels 1-11 can be operated. Selection of other channels is not possible.

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

## A.11 Safety and Hazards

Under no circumstances should the device be used in any areas

(a) where blasting is in progress,

{b) where explosive atmospheres may be present, or

(c) that are near (1) medical or life support equipment, or (2) any equipment which may be susceptible to any form of radio interference. In such areas, the device MUST BE POWERED OFF AT All TIMES (since the device otherwise could transmit signals that might interfere with such equipment).

In addition, under no circumstances should the device be used in any aircraft, regardless of whether the aircraft is on the ground or in flight. In any aircraft, the device MUST BE POWERED OFF AT ALL TIMES since the device otherwise could transmit signals that might interfere with various onboard systems on such aircraft.

Furthermore, under no circumstances should the device be used by tile driver or operator of any vehicle. Such use of the device will detract from the driver's or operator's control of that vehicle. In some jurisdictions, use of the device white driving or operating a vehicle constitutes a civil and/or criminal offense,

Due to the nature of wireless communications, transmission and reception of data by the device can never be guaranteed, and it is possible that data communicated or transmitted wirelessly may be delayed, corrupted (i.e., contain errors}, or totally lost. The device is not intended for, and Proxicast recommends the device not be used in any critical applications where failure to transmit or receive data coul d result in property damage or loss or personal injury of any kind (including death) to the user or to any other party.

Proxicast expressly disclaims liability for damages of any kind resulting from:

(a) delays, errors, or losses of any data transmitted or received using the device; or

(b) any failure of the device to transmit or receive such data.

Purchaser agrees to indemnify Proxicast against any liability or damages caused to third parties as a result of Purchaser's misuse or misapplication of the Proxicast product.

## A.12 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.

# A.13 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