



Read and  
Retain for  
Future  
Reference

**Cooper Bussmann**  
**615M-1**  
**Cellular Data Modem & IP Router Series**  
**User Manual**  
Version 1.0

## Modem Use

The 615M-1 Series modems are designed and intended for use in fixed and mobile applications. “Fixed” assumes the device is physically secured at one location and not easily moved to another location. Always keep the cellular antenna a distance of at least 20 cm (8 in.) from anyone’s head or body while the modem is in use. This modem is designed for use in applications that observe the 20 cm separation distance.

## Interference Issues

Avoid possible radio frequency (RF) interference by following these guidelines:

- The use of cellular telephones or devices in aircraft is illegal. Use in aircraft may endanger operation and disrupt the cellular network. Failure to observe this restriction may result in suspension or denial of cellular services to the offender, legal action or both.
- Do not operate in the vicinity of gasoline or diesel fuel pumps unless use has been approved and authorized.
- Do not operate in locations where the device could interfere with medical equipment that may be in use.
- Do not operate in fuel depots, chemical plants, or blasting areas unless use has been approved and authorized.
- Use care if operating in the vicinity of protected personal medical devices, such as hearing aids and pacemakers.
- Operation in the presence of other electronic equipment may cause interference if the equipment is incorrectly protected. Follow the installation recommendations provided by the equipment manufacturers.

## Mobile Application Safety

- Do not change parameters or perform other maintenance on the 615M-1 modem while driving.
- Road safety is crucial. Observe national regulations for cellular telephones and devices while in vehicles.
- Avoid potential interference with vehicle electronics by correctly installing the 615M-1 modem. ELPRO recommends installation by a professional.

## UL Listed Models



When operating at elevated temperature extremes, the surface may exceed +70°C. For user safety, the 615M-1 should be installed in a restricted access location.



The SIM/SVC connectors are used for maintenance purposes only.

**WARNING – EXPLOSION HAZARD, do not connect while circuit is live unless the area is known to be non-hazardous.**

## Important Notice

ELPRO reserves the right to modify the equipment, its specification, or this manual without prior notice in the interest of improving performance, reliability, or servicing. At the time of publication all data is correct for the operation of the equipment at the referenced voltage and/or temperature. Performance data indicates typical values related to the particular product.

No part of this documentation or information supplied may be divulged to any third party without the express written consent of ELPRO. Products offered may contain software which is proprietary to ELPRO. The offer or supply of these products and services does not include or infer any transfer of ownership.

## Release Notice

This is the April 2013 release of the *615M-1 Cellular Data Modem & IP Router Series Manual* version 1.0, which relates to version 5.0.2e modem firmware.

## Follow Instructions

Read this entire manual and all other publications pertaining to the work to be performed before installing, operating, or servicing this equipment. Practice all plant and safety instructions and precautions. Failure to follow the instructions can cause personal injury and/or property damage.

## Proper Use

Any unauthorized modifications to or use of this equipment outside its specified mechanical, electrical, or other operating limits may cause personal injury and/or property damage, including damage to the equipment. Any such unauthorized modifications: (1) constitute “misuse” and/or “negligence” within the meaning of the product warranty, thereby excluding warranty coverage for any resulting damage; and (2) invalidate product certifications or listings.

# CONTENTS

---

<b>Chapter 1 - INTRODUCTION</b> .....	<b>5</b>	<b>Chapter 4 - IP ADDRESSING</b> .....	<b>58</b>
1.1 Module Identification .....	5	4.1 Overview .....	58
1.2 Features and Benefits .....	5	4.2 IP Addressing Tutorial .....	58
1.3 General Specifications .....	6	4.3 Private vs. Public IP Addresses .....	58
1.4 Mechanical Specifications .....	8	4.4 Port Forwarding .....	59
1.5 Order Information .....	9	4.5 DMZ .....	59
1.6 External Connectors .....	10	4.6 Friendly IP Address .....	60
1.7 Antenna .....	11	<b>Chapter 5 - IPSEC AND VPN PASS-THROUGH</b>	
1.8 Power Cable Pinout .....	11	<b>DEPLOYMENT GUIDE</b> .....	<b>61</b>
1.9 RS-232 Serial Port Integration Parameters ..	12	7.1 Benefits of IPsec .....	61
<b>Chapter 2 - GETTING STARTED</b> .....	<b>13</b>	7.2 615M-1 Configured IPsec Client .....	61
2.1 Package Contents .....	13	Cisco Router-VPN Server Configuration ..	62
2.2 Device Connections .....	13	615M-1-IPSEC Client Configuration .....	62
2.3 LAN Configuration .....	14	7.3 615M-1 Configured VPN Pass-through .....	63
2.4 Cellular Connections .....	15	615M-1-VPN Pass-Through Configuration ..	64
<b>Chapter 3 - 615M-1 WEB INTERFACE</b> .....	<b>16</b>	<b>Chapter 8 - USER I/O PORT</b> .....	<b>65</b>
3.1 Logging on to the Web Interface .....	16	8.1 Circuit for Analog Inputs .....	66
3.2 Unit Status .....	17	8.2 Simplified Circuit for Digital Input/Outputs ..	66
Status .....	17	8.3 Simplified Circuit for Mechanical Relays .....	67
Identity .....	20	8.4 Inserting Wires into User Port Connector .....	67
Basic Settings .....	20	<b>Appendix A - GLOSSARY</b> .....	<b>68</b>
3.3 Cell Connection – 615M-1 .....	22		
Carrier .....	22		
GSM Settings .....	23		
CDMA Settings .....	24		
System Monitor .....	27		
Dynamic DNS .....	28		
3.4 LAN Settings .....	30		
MAC Filtering .....	33		
IP Filtering .....	34		
3.5 Router .....	37		
Port Forwarding .....	37		
Static Routes .....	38		
3.6 Security .....	39		
PPTP .....	40		
IPsec .....	41		
GRE .....	44		
3.7 Serial .....	44		
External Serial .....	44		
3.8 Diagnostics .....	48		
SNMP .....	48		
Logging .....	50		
3.9 I/O Settings .....	51		
Status .....	51		
Settings .....	52		
Labels .....	56		
3.10 Firmware Update .....	56		

## CHAPTER 1 - INTRODUCTION

The 615M-1 Series from ELPRO is the ideal solution for a wide range of cellular data network serial and Ethernet connectivity requirements. All 615M-1 Series feature both high-speed 3G HSPA and EVDO cellular communications in a single device, with full GSM and CDMA backward compatibility. The 615M-1 delivers two LAN, one serial, and Rx diversity connections.

The **GSM** mode features a Tri-Band UMTS/HSUPA (850/1900/2100) and Quad-Band GSM/GPRS network support with data rates up to 14.4Mbps downlink and 5.76Mbps uplink for HSPA, and is backward compatible to HSUPA, HSDPA, EDGE and GPRS, dependent on carrier service availability.

The **CDMA** mode features EV-DO Rev A speeds with data rates up to 3.1Mbps downlink and 1.8Mbps uplink, and is backward compatible to EV-DO Rev 0 and 1xRTT, dependent on carrier service availability. This occurs automatically to the level of service available. Dual Band Digital CDMA 800MHz and CDMA PCS 1900MHz models supports packet-switched services.

### 1.1 Module Identification

The module identification label is located on the bottom of your 615M-1 device. This label contains the product part number, the serial number, FCC and IC identifications, as well as carrier specific information that is required when activating your data account.

The module identification label contains information for GSM and CDMA:

- The **GSM** information contains an International Mobile Equipment Identity (IMEI) number in decimal format. This number is used by the GSM network only to identify and validate the device. It has no permanent or semi-permanent relation to the subscriber.
- The **CDMA** information contains the device MEID numbers. This number is required by your cellular carrier when activating your data contract. The MEID number is provided in both decimal and hexadecimal formats. The format required for activation is carrier dependent.

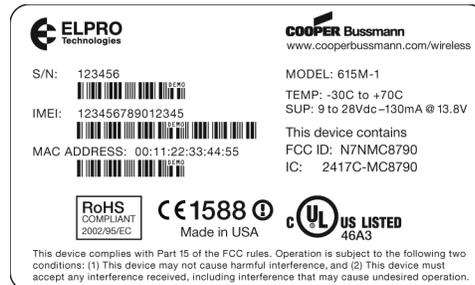


Figure 1 Module Identification Label

### 1.2 Features and Benefits

The 615M-1 Series provides the following features and benefits:

- Multiple carriers in a single device.
- Supports dynamic or static IP.
- Inbound and outbound Ethernet routing.
- DHCP server and inbound port mapping/translation (port forwarding).
- Firewall configuration for increased network security.
- Diversity antenna port/auxiliary port for increased receive sensitivity.
- Local or remote configuration using HTML web server.

- TCP/IP packet assembler and dis-assembler for serial connected devices.
- Inbound IP termination with static IP.
- Modem Domain Names with dynamic DNS.
- Internet access and web browsing via Ethernet connector.
- VPN support.
- On-board 1.8/3V SIM socket (active only for GSM).

### 1.3 General Specifications

Product specifications are subject to change without notice.

Table 1

Specifications	
<b>Transmitter/Receiver</b>	
Frequency	Quad-band 850/900/1900/2100 MHz/AWS <sup>(1,2)</sup> Quad-band 850/900/1800/1900 MHz <sup>(3,4)</sup> 800 MHz Cellular/1900 MHz PCS/2100 MHz <sup>(5)</sup> 800 MHz Cellular/1900 MHz PCS/2100 MHz <sup>(6)</sup> 800 MHz Cellular/1900 MHz PCS <sup>(7)</sup>
Transmit Power (Max)	250 mW <sup>(1,2)</sup> ; 2 W <sup>(3,4)</sup> ; 250 mW <sup>(5,6,7)</sup>
Transmission	UMTS, HSPA, EDGE, GPRS, EVDO Rev A (IS-856-A), 1xEVDO Rev 0 (IS-856), 1xRTT (IS-2000)
Modulation	UMTS, HSPA, EDGE, GPRS, EVDO Rev A (IS-856-A), 1xEVDO Rev 0 (IS-856), 1xRTT (IS-2000)
Receive Sensitivity	-109 dBm <sup>(1)</sup> ; -109 dBm <sup>(2)</sup> ; -105 dBm <sup>(3,4)</sup> ; -107 dBm <sup>(5,6,7)</sup>
Channel Spacing	5 MHz <sup>(1,2)</sup> ; 10 MHz <sup>(2)</sup> ; 1.25 MHz <sup>(5,6,7)</sup>
Data Rate	Downlink up to 384 kbps; Uplink up to 384 kbps <sup>(1)</sup> Downlink up to 14.4 Mbps ; Uplink up to 5.76 Mbps <sup>(2)</sup> Downlink up to 236 kbps; Uplink up to 236 kbps <sup>(3)</sup> Downlink up to 115 kbps; Uplink up to 115 kbps <sup>(4)</sup> Downlink up to 3.1 Mbps; Uplink up to 1.8 Mbps <sup>(5)</sup> Downlink up to 2.4 Mbps; Uplink up to 153.6 kbps <sup>(6)</sup> Downlink up to 153.6 kbps; Uplink up to 153.6 kbps <sup>(7)</sup>
Range (LoS)	Cellular depends on service provider
Antenna Connector	2 x Female SMA Standard Polarity <sup>(1,2,3,4,5,6,7)</sup>
<b>Input/Output</b>	
Discrete Input	ON 2.3 Vdc, OFF 0.7 Vdc, 5.5 Vdc max <sup>(8)</sup>
Discrete Output	NPN Transistor close to Digital Ground, Pull down 100-ohm <sup>(8)</sup>
Relay Outputs	Max voltage 30 Vdc, Max current 1 A <sup>(8)</sup>
Analog Inputs	Voltage input range 0 – 30 Vdc, Accuracy +/-0.2 Vdc <sup>(8)</sup>
<b>Ethernet Port</b>	
Ethernet Port	10/100baseT; RJ45 Connector – 2 x IEEE 802.3 (auto MDIX)

## Cooper Bussmann 615M-1 Cellular Data Modem and IP Router Series Manual

Specifications	
Link Activity	Activity LED
<b>Serial</b>	
RS232	DB9 Female DCE
Data Rate (Bps)	1200, 2400, 4800, 9600, 14400, 19200, 38400, 57600, 76800, 115200 bps
Serial Settings	8 Data Bits; No Stop/1 Start/Parity (Configurable)
<b>Protocols and Configuration</b>	
Protocols Supported	TCP/IP, UDP, ARP, ICMP, FTP, TFTP, TELNET, PING, GPS-NMEA (optional), DHCP; MAC Filtering (Whitelist), IP Filtering (Blacklist), DMZ, Dynamic DNS, Port Forwarding; SNMP, HTTP embedded web server; IPsec, GRE Tunneling, PPTP, VPN, RADIUS/802.1x
User Configuration	Configuration and Firmware upgrades via HTTP/OTA (Over-the-Air)
Configurable Parameters	Client/Router, Serial Client Server Simultaneous RS232 connection
Security	VPN, SIM Card PIN, RADIUS, IPsec
Bandwidth Protection	MAC Address—Whitelist/Blacklist, IP Filtering—Whitelist/Blacklist
Network Management	SNMP V2c, V3
<b>LED Indication/Diagnostics</b>	
LED Indication	RSSI; SVC; NET; GPS; AUX
Reported Diagnostics	Diagnostics available through web pages
<b>Compliance</b>	
EMC	FCC Part 15; Industry Canada; CE; A-Tick
RF (Radio)	EN 300 328; FCC Part 15
Hazardous Area	Class I, Division 2
Safety	IEC 60950-1
UL	UL Listed
Environmental	MIL-STD-810F
Approvals	PTCRB, Carrier Specific Approvals
<b>General</b>	
Size	109 x 153 x 45 mm (4.3 in x 6 in x 1.8 in)
Housing	Powder-coated Aluminum
Mounting	DIN Rail, Panel Mount (optional)
Terminal Blocks	I/O: Removable terminal block, Screwless push-in wire, 18 - 28 AWG
Temperature Rating	-30 to +70°C; -22 to +158°F
Humidity Rating	5 – 95% RH Non-condensing
Weight	1.13 kg (2.5 lb)

Specifications	
<b>Power Supply</b>	
Nominal Supply	9 to 28 Vdc; Under/Over Voltage Protection and Reverse Polarity Molex 43025-0400 4-pin locking connector
Average Current Draw	130 mA @ 13.8 Vdc (Idle)
Transmit Current Draw	350 mA @ 13.8 Vdc
<p><b>NOTE</b> Specifications subject to change.</p> <p><sup>1</sup> UMTS  <sup>2</sup> HSPA  <sup>3</sup> EDGE  <sup>4</sup> GPRS  <sup>5</sup> EVDO Rev A (IS-856-A)  <sup>6</sup> 1xEVDO Rev 0 (IS-856)  <sup>7</sup> 1xRTT (IS-2000)  <sup>8</sup> Access via SNMP only</p>	

### 1.4 Mechanical Specifications

This section describes the exterior dimensions of the 615M-1 modem. A DIN rail mounting plate (not shown) is provided with the modem, and needs to be fitted to the modem using the screws and toothed washers provided, as described in the installation instructions. The mounting plate can be used to secure the modem to any surface that can be drilled for such purpose.

The following drawings may be used as layout reference before proceeding with the mounting process.

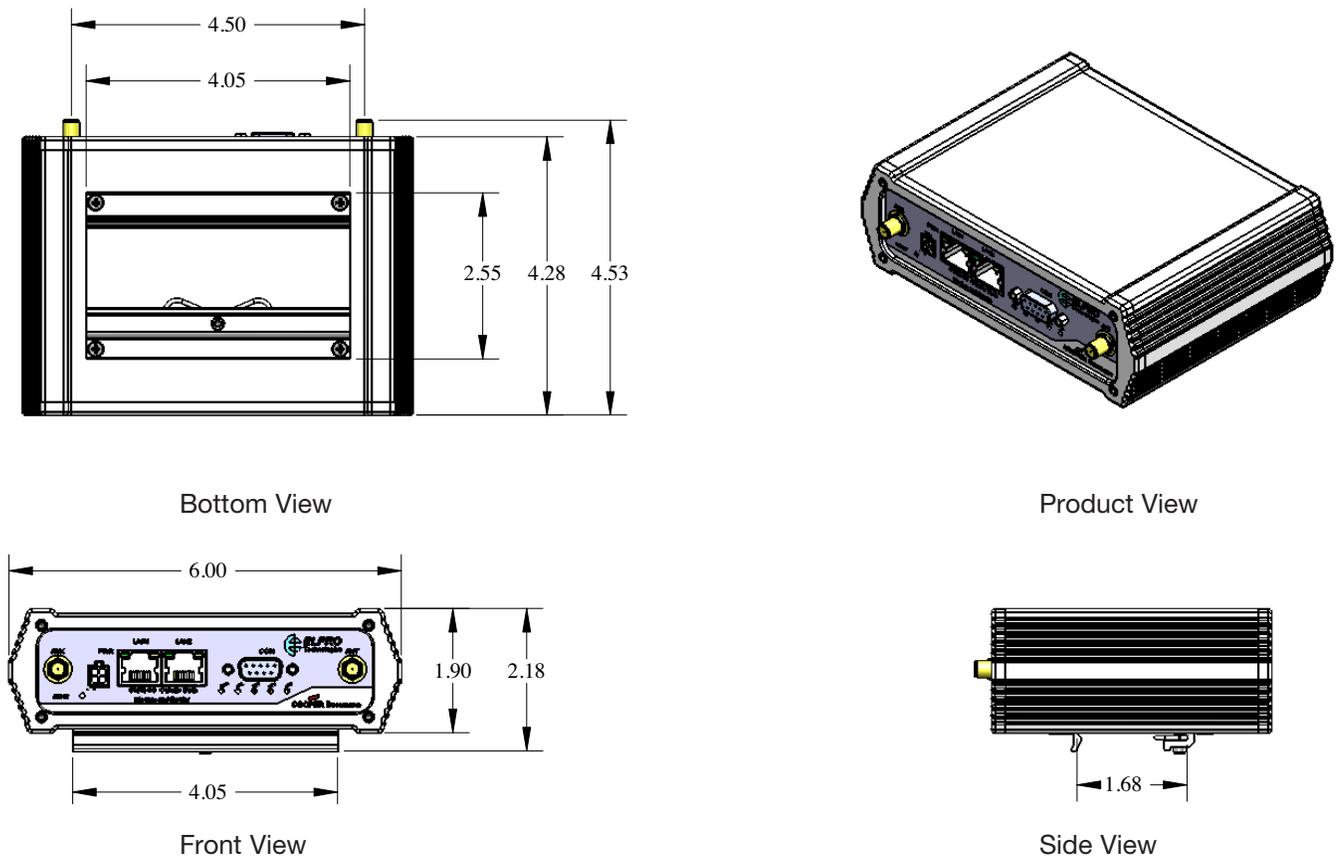


Figure 2 615M-1 Mechanical Drawings

## 1.5 Order Information

Table 2

Order Code	Description
615M-1	3G Modem, GSM/CDMA

Table 3

Product Code	Description	Data Sheet
<b>Antennas–Cellular</b>		
WHGSM-3	Cellular Antenna, 130 mm (5 in.), SMA Male, Magnetic Base Mount, 2 dBi gain	7941
<b>Cables</b>		
CC3/10-SMA	Coaxial Cable Kit, 3 m (9.8 ft)/10 m (32 ft), N-type to SMA	7932 7947
CCTAIL-SMA-F/M	Coaxial Cable Tail, 600 mm (24 in.), SMA to N-type Female or Male	7951
SER-RJ45	Configuration Cable, RS232 Serial, DB9 Female to RJ45	7956
SER-DB9NULL	RS232 Serial, Null Modem	7988
ETH-C5X	Ethernet Cable, 1.8 m (6 ft), Crossover, RJ45 to RJ45	7952
ETH-C5A	Ethernet Cable, 1.8 m (6 ft), Direct, RJ45 to RJ45	7953
<b>Surge Diverters</b>		
CSD-SMA-2500	SMA Surge Diverter for use with CC10, CC20 - SMA	7959
CSD-N-6000	Coaxial Surge Diverter, Bulkhead N Female to N Female	7960
IOP32D	Signal Surge Diverter, 2 wire/4 wire	7961
<b>Power Supply</b>		
PS-WW-XP	100Vac Input Power Supply	7934
PS-DINAC-12DC-OK	DIN Rail Power Supply, 100 - 250 Vac, 12 Vdc/2.5 A	7935
PS-DINAC-24DC-OK	DIN Rail Power Supply, 100 - 250 Vac, 24 Vdc/2A	7958
<b>Mounting Brackets</b>		
BR-615-DINCLIP	DIN Rail Mount Kit for 615M-xx Series	7986
BR-615-PLATE	Panel Mounting Plate Kit: for 615M-xx Series	7987

## 1.6 External Connectors

Table 4 describes the external connectors for the 615M-1 modem.

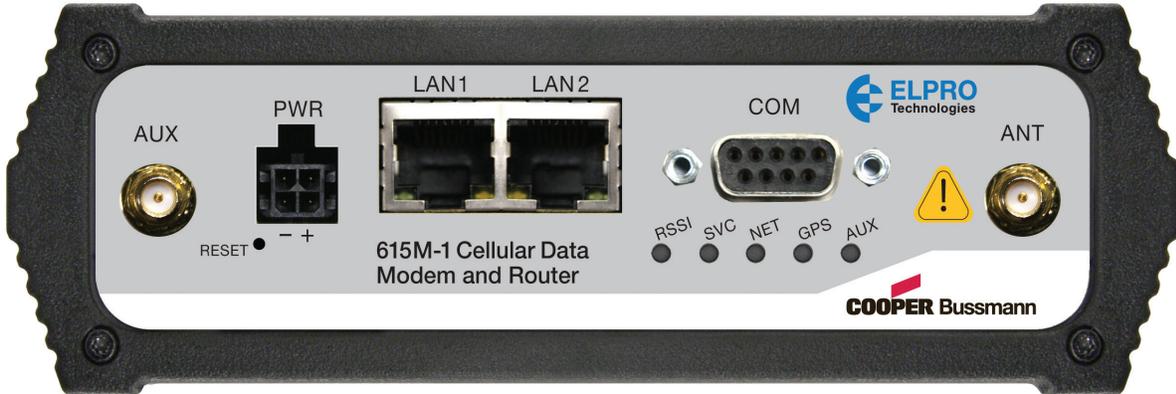


Figure 3 Front Panel Connections

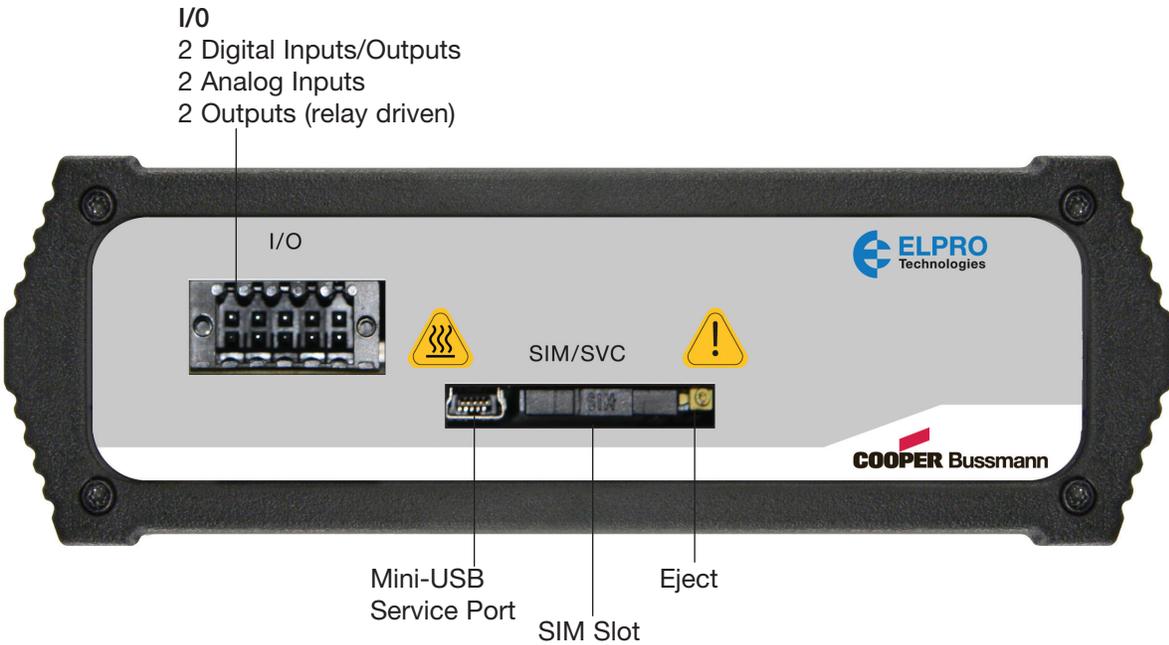


Figure 4 Rear Panel Connections

Table 4 External Connectors

Panel Indicator	Connection	Description
COM	RS-232	Serial to IP conversion use
ANT	SMA	Primary RF antenna
AUX	SMA	Cellular diversity
LAN 1, LAN 2	RJ-45	Interface for Ethernet connection to devices
SIM/SVC	USB Mini	Available for ELPRO support use only

Panel Indicator	Connection	Description
RESET		Hold for one second to reset unit. Hold for at least 4 sec to reconfigure the unit to its factory default settings.
PWR Jack	Molex 43025-0400; Power – bottom pins	Interface for power plug (9-28 Vdc) Top pins are not available for use.
SIM/SVC	SIM Card socket	Interface for SIM card. Your wireless service provider will supply the SIM card with your wireless service contract.

Table 5 Status LEDs

Function	Off	Green	Flash Green	Red	Flash Red	Amber	Flash Amber
RSSI		Strong		Weak/None		Medium	
SVC		3G	3G/NC		NC	2G	2G/NC
NET	No Connectivity		RX Data		TX Data		RX/TX
Aux	Disabled	Good		Failed			

If SVC is solid on, the modem is connected to the Internet. If SVC is flashing, the modem is trying to connect to the network. NET indicates the direction of data. At boot, the LEDs act differently than described in Table 5. The boot sequence for LEDs is as follows:

All Red, All Amber, All Green, All Flash Green 3 times. Boot sequence is complete.

## 1.7 Antenna

The primary antenna connections are SMA female connectors, and must be used with antenna with SMA male connectors. When using a direct mount or rubber duck antenna, choose the antenna specific to your band requirements. Mounting options and cable lengths are user’s choice and application specific.

The AUX antenna connector is installed on all standard models and can be used for diversity. The diversity port supports two bands, Cellular (850 MHz), and PCS(1900 MHz). Connect a dual band cellular antenna to this port to implement RX diversity on the unit and increase receive sensitivity on the cellular network.

## 1.8 Power Cable Pinout

The 615M-1 ships with a 6 ft power cable that does not require a fuse. The ignition sense line should be shorted to Vin/Vbattery.

Table 6

Pin	Signal	Color Mobile	Color Fixed
1	VIN/VBatt	Red	Red
2	Ground	Blue	Black
3	Ignition Sense	White	White
4	No Connect	NA	NA

## 1.9 RS-232 Serial Port Integration Parameters

Table 7 provides the serial cable design information to integrate the 615M-1 modem into your system. Table 8 provides the default RS-232 communication parameters. This modem can be connected to a PC with a straight-through serial modem cable.

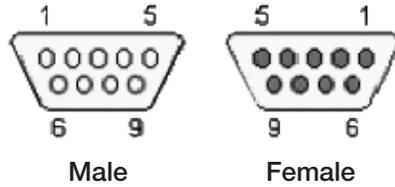


Figure 5 DE-9 Connectors

Table 7 Standard RS-232 DE-9 Pin Out

Pin	Name	Direction	Description
1	CD	Output	Carrier Detect
2	RX	Output	Receive Data
3	TX	Input	Transmit Data
4	DTR	Input	Data Terminal Ready
5	GND		System Ground
6	DSR	Output	Data Set Ready
7	RTS	Input	Request to Send
8	CTS	Output	Clear to Send
9	RI	Output	Ring Indicator
NOTE Port is a DCE.			

Table 8 Default RS-232 Communication Parameters

Bits Per Second	115,200
Data Bits	8
Parity	None
Stop Bits	1
Flow Control	None

## CHAPTER 2 - GETTING STARTED

### 2.1 Package Contents

The 615M-1 Modem package contains the following:

- 615M-1 Modem
- Power Cable
- Information Card

### 2.2 Device Connections

Use the following steps to connect devices to the modem and connect the modem to power.

1. (GSM Users) Insert the SIM card into the SIM/SVC slot (see Figure 6).



Figure 6 Inserting SIM Card

2. Connect an antenna to the ANT connector on the front panel of the 615M-1 modem.
3. Connect an Ethernet cable into the LAN 1 port and plug the other end into the network port on your PC.
4. Connect the Power Adapter to the modem PWR port and plug into a proper AC power socket.

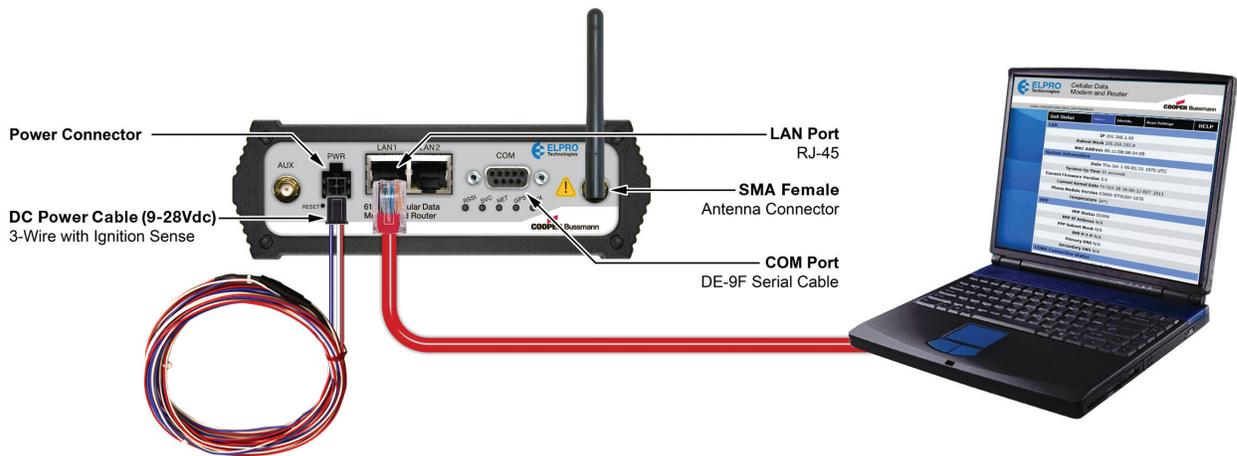


Figure 7 Connecting to Power and PC

## 2.3 LAN Configuration

The modem is configured via internal web pages.

For Windows XP users:

1. Choose **Start-->Control Panel-->Network Connections**.
2. Right-click Local Area Connection and click **Properties**.
3. Click **Internet Protocol (TCP/IP)** and click **Properties**.
4. On the **General** tab, select the options “Obtain an IP address automatically” and “Obtain DNS server address automatically.”
5. Click **OK** to complete the TCP/IP configuration.

For Windows 7 users:

1. Choose **Start-->Control Panel-->Network and Sharing Center**.
2. Select **Change Adapter Setting**.
3. Right-click Local Area Connection, click **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.
4. On the **General** tab, select the options “Obtain an IP address automatically” and “Obtain DNS server address automatically.”
5. Click **OK** to complete TCP/IP configuration.

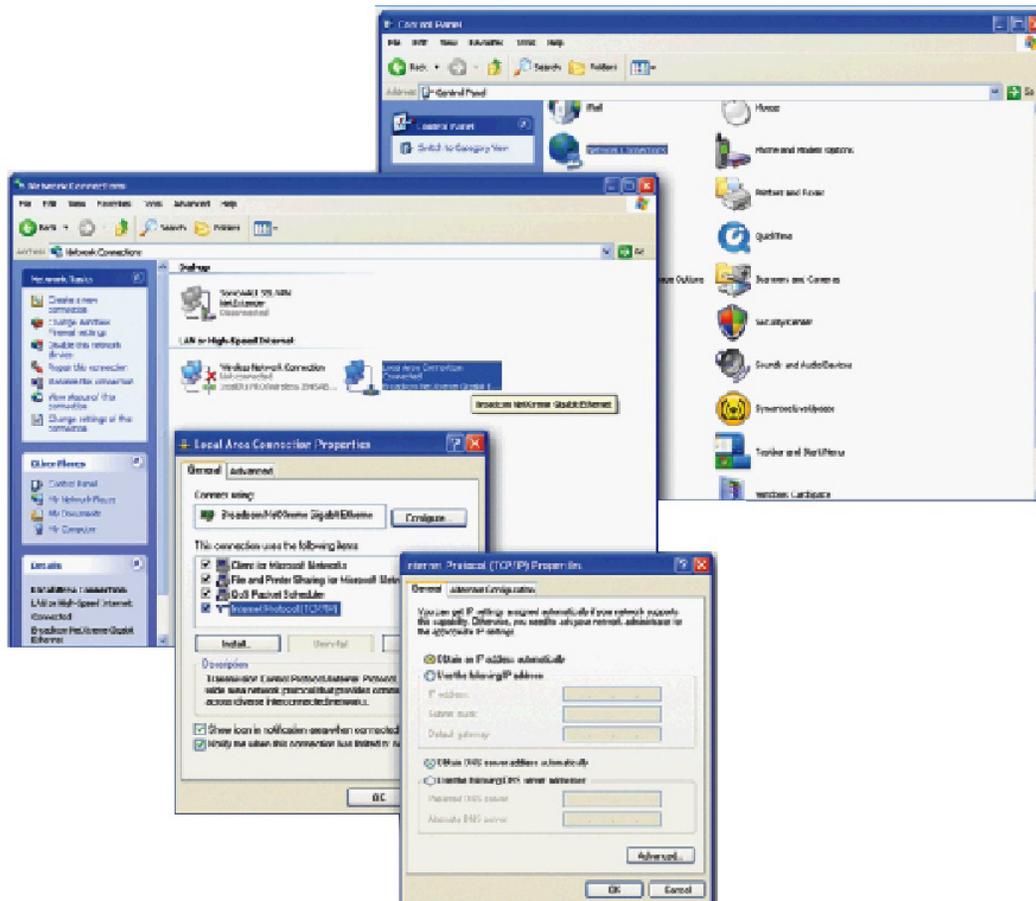


Figure 8 LAN Configuration Screens

## 2.4 Cellular Connections

Before you begin, you need an active cellular account with the carrier of your choice.

### GSM Users:

1. Insert the SIM card (gold side up) into the SIM/SVC slot in the rear of the modem.
2. Push the card completely into the slot until it clicks in place.
3. If you have already powered your device, you will need to cycle power to register the SIM for operation.

### CDMA Users:

Refer to section “Basic Settings” to provision your modem for proper operation.

## CHAPTER 3 - 615M-1 WEB INTERFACE

### 3.1 Logging on to the Web Interface

1. Start your web browser and enter 192.168.1.50 in the address bar.  
The following login screen appears.

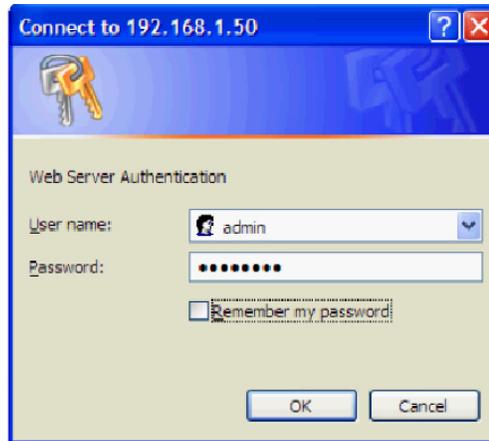


Figure 9 Login Screen

2. Enter the User Name "admin" and the Password "password."
3. Click OK.

The modem's Home Page appears. The main navigation pane (see Figure 10) is on the left side of the page, and on the right side is the content area.



Figure 10 Main Navigation Pane

### 3.2 Unit Status

Click Unit Status on the main navigation pane to access the Status, Identity, and Basic Settings pages.

#### Status

Click the Status tab on the Unit Status page to see general status information for the unit. Figures 11 and 12 show the Status content for GSM and CDMA.

Unit Status	Status	Identity	Basic Settings	HELP
<b>LAN</b>				
IP 192.168.1.50				
Subnet Mask 255.255.255.0				
MAC Address 00:11:DB:06:55:13				
<b>System Information</b>				
Date Sun Jan 4 15:20:13 1970 UTC				
System Up Time 314414 seconds				
Current Firmware Version 5.0				
Current Kernel Date Fri Oct 28 16:06:12 EDT 2011				
Phone Module Version D3200-STSUGN-1575				
Temperature 42°C				
Main Voltage 13.73				
<b>PPP</b>				
PPP Status UP				
PPP IP Address 74.198.92.13				
PPP Subnet Mask 255.255.255.252				
PPP P-T-P 74.198.92.14				
Primary DNS 64.71.255.198				
Secondary DNS 64.71.255.253				
<b>GSM Connection Status</b>				
Service Type HSPA				
MDN 15142421486				
IMEI 357485040340095				
MEID A100004BCCFB9				
IMSI 302720402528031				
Carrier				
Channel 1037				
Frequency WCDMA 850				
Roaming Not Roaming				
Signal Strength (dBm) -78 (strong)				
<input type="button" value="Refresh"/>				

Figure 11 615M-1 Unit Status–Status (GSM)

Unit Status	Status	Identity	Basic Settings	HELP
<b>LAN</b>				
IP 192.168.1.50				
Subnet Mask 255.255.255.0				
MAC Address 00:11:DB:06:54:EB				
<b>System Information</b>				
Date Thu Jan 1 00:01:31 1970 UTC				
System Up Time 92 seconds				
Current Firmware Version 5.0				
Current Kernel Date Fri Oct 28 16:06:12 EDT 2011				
Phone Module Version D3600-STSUSH-1576				
Temperature 28°C				
<b>PPP</b>				
PPP Status DOWN				
PPP IP Address N/A				
PPP Subnet Mask N/A				
PPP P-T-P N/A				
Primary DNS N/A				
Secondary DNS N/A				
<b>CDMA Connection Status</b>				
Service Type				
MDN				
MEID A100004BCD034				
MSID/MTN 2012681360				
PRL 60774				
SID 4139				
NID 65535				
Channel 0				
Frequency CDMA Band Class 0				
Roaming Roaming				
Signal Strength (dBm) -120 (poor)				
<input type="button" value="Refresh"/>				

Figure 12 615M-1 Unit Status–Status (CDMA)

## LAN

IP	Displays the LAN-side static IP information for the modem.   <b>NOTE</b> Once this IP address is changed and saved, the browser connection to the device will be lost. To continue configuration, reconnect to the (new) IP address (the address that has been entered and saved).
Subnet Mask	Displays the LAN-side subnet mask for the modem.
MAC Address	Media Access Control Address. Every Ethernet device (LAN card) has a unique hardware serial number or MAC address to identify each Network Device.

## System Information

Date	Displays the current date and time (UTC), as received from the cellular carrier. The date and time information is updated at the start of each PPP connection, and maintained internally until the modem is rebooted. If no PPP connection was made this boot cycle, the time display will not be accurate. The date is not a user-settable function—it is controlled only by the carrier-supplied date and time. Not all carriers support this function.
System Up Time	Displays the system uptime in seconds: <ul style="list-style-type: none"> <li>• 1 minute = 60 seconds</li> <li>• 1 hour = 3600 seconds</li> <li>• 1 day = 86400 seconds</li> <li>• 1 year = 31,536,000 seconds</li> </ul>
Current Firmware Version	Displays the current modem firmware version loaded. For the latest updates, visit <a href="http://www.cooperbussmann.com/wireless">www.cooperbussmann.com/wireless</a> .
Kernel Date	Displays the date of the operating system kernel running on the modem.
Phone Module Version	This version varies depending on the vendor of the radio module within the modem.
Temperature	Displays the current internal temperature of the modem, as measured by the cellular radio module.
Main Voltage	Supply voltage applied to the 615M-1.

## PPP

PPP Status	Indicates the status of the cellular connection, typically UP when connected properly.
PPP IP Address	The current IP address of the 615M-1 on the cellular network.
PPP Subnet Mask	The PPP subnet mask is typically set to 255.255.255.255, but may be different depending on the carrier.
PPP P-t-P	The point-to-point address of the gateway on the cellular network. It may be possible to ping this address to determine if a PPP IP address assigned is routable from the Internet.
Primary DNS	The Primary DNS server, as assigned by the cellular carrier, when PPP is UP.
Secondary DNS	The Secondary DNS server, as assigned by the cellular carrier when PPP is UP.

## CDMA Connection Status

<b>Service Type</b>	Determines the type of network your device has connected to (GPRS, EDGE, UMTS, HSDPA, CDMA 1xRTT, EVDO Rev0 or RevA).
<b>MEID</b>	The Electronic Serial Number is only applicable for the CDMA product line, and carrier specific (such as AllTel™, Verizon Wireless™, or Sprint™).
<b>MDN/MTN</b>	The actual phone number of the device, as supplied by the carrier. When the unit is successfully provisioned, the phone number for the user account is displayed.
<b>MIN/IMSI</b>	This number is used by the Mobile Telephone Network and will be different if ported from another carrier (it is not used by the end user of the device).
<b>PRL</b>	Preferred Roaming List, only applicable for the CDMA product line, and carrier specific (AllTel, Verizon, Sprint, and so on).
<b>SID</b>	System ID (Identity), provided by the carrier.
<b>NID</b>	Network Identifier. The NID is supplied automatically from the network.
<b>Channel</b>	Cell Site channel number at which the modem is connected. This information is useful for the carrier in the event of troubleshooting.
<b>Frequency</b>	Cellular frequency band that the modem is using. The 800 MHz and 1900 MHz frequency bands are mainly in the US and outlying areas. In some cases 900 and 1800 are seen for European or foreign carriers.
<b>Roaming</b>	Options are either “Roaming” or “Not Roaming,” and may defer from the PRL in the case of CDMA.
<b>Signal Strength (dBm)</b>	Measured in dBm, this is the Received Signal Strength Indicator (RSSI).
<b>Diagnostic</b>	If this number is less than 128, it represents the number of successful PPP connections since the modem was rebooted. If this number is 128 or greater, the Diagnostic value minus 128 equals the number of times the cellular module has been reset since the modem was rebooted.

## GSM Connection Status

<b>Service Type</b>	Determines the type of network your device has connected to; GPRS, EDGE, HSDPA, HSUPA, or HSPA. Check SIM is displayed if the SIM is invalid, missing, or if the PIN needs to be entered.
<b>MDN</b>	The Mobile Directory Number is the phone number assigned to the SIM card supplied by the carrier. The MDN may display NOT AVAILABLE if the PIN status is disabled or the MDN is unknown.
<b>IMEI</b>	The International Mobile Equipment Identity is a unique 15-digit number that serves as the serial number of the GSM module in the modem.
<b>MEID</b>	Mobile Equipment Identifier. Applies to CDMA devices only.
<b>IMSI</b>	The International Mobile Subscriber Identity is a unique number that designates the subscriber. This number is used for provisioning in network elements. The IMSI may display NOT AVAILABLE if a SIM card is not detected.
<b>Carrier</b>	Cellular provider name or code.
<b>Channel</b>	Cell Site channel number at which the modem is connected. This information is useful for the carrier in the event of troubleshooting.

- Frequency** Cellular frequency band that the modem is using. The frequency bands 800 MHz and 1900 MHz are mainly in the US and outlying areas. In some cases 900, 1800, and 2100 MHz are seen for European or foreign carriers.
- Roaming** Options are either “Roaming” or “Not Roaming.”
- Signal Strength (dBm)** Measured in dBm, this is the Received Signal Strength Indicator (RSSI).

## Identity

Click the Identity tab on the Unit Status page to view identity information for the unit.

Unit Status	Status	Identity	Basic Settings	HELP
<b>Factory Settings</b>				
Serial Number		550091		
Model Number		140-7202-110		
<b>User-defined</b>				
Unit ID				
Refresh				

Figure 13 Unit Status–Identity

## Factory Settings

- Serial Number** Unique serial number for this unit.
- Model Number** Unit model number defining its capacity and features.

## User-defined

- Unit ID** User-defined for ease of reference, used by various services.

## Basic Settings

Click the Basic Settings tab on the Unit Status page to see the unit identification number and configure power management and network time settings.

Unit Status	Status	Identity	Basic Settings	HELP
<b>Unit ID</b>				
ID		<input type="text"/>		
Cancel Save				
<b>Power Management</b>				
Shutdown Method		<input checked="" type="radio"/> Disabled <input type="radio"/> Power Off		
After Ignition Line Off		Shutdown in 60 minutes		
When Voltage Drops Below		<input type="text" value="11.0"/> Volts (set to 0 to turn off)		
Cancel Save				
<b>Network Time</b>				
NTP Client		<input checked="" type="radio"/> Disabled <input type="radio"/> Enabled		
NTP Server		<input type="text"/>		
Update Frequency		<input type="text" value="24"/> Hours (set to 0 to disable updates)		
Cancel Save				

Figure 14 Unit Status–Basic Settings

## Unit ID

**ID** This identification number serves to distinguish this unit from other units in the network. It is at the same time the “syslocation” for the SNMP facility.

## Power Management

The 615M-1 unit is designed to stay on even if the ignition is turned off. The unit can be configured to automatically shut down 1, 5, 30, 60 or 240 minutes after ignition has been turned off, or when the supply voltage drops to a certain level.

<b>Shutdown Method</b>	Disabled by default. Select “Power Off” to enable power management.
<b>After Ignition Line Off</b>	Select one of the following time intervals: 1, 5, 30, 60 or 240 minutes.
<b>When Voltage Drops Below</b>	Enter the desired voltage. Enter “0” to disable and give precedence to the time delay configured in After Ignition Time Off.

## Network Time

The 615M-1 is capable of maintaining the current time (UTC) by synchronizing itself with a Network Time Protocol (NTP) server. You may specify a server URL and how frequently the router should synchronize with the server. The router must have an Internet connection in order to synchronize with the server. Because the router does not save or track time while powered off, the time will be inaccurate until the router can connect to the server.

<b>NTP Client</b>	Disabled by default. Select “Enabled” to activate the router’s NTP client to synchronize with the specified server.
<b>NTP Server</b>	Enter the URL of the desired NTP server. Most NTP servers have a posted usage policy. A review of the usage policies and choice of an appropriate server is recommended.
<b>Update Frequency</b>	Set to 24 hours by default. Specify the frequency to synchronize the router time with the specified NTP server.

### 3.3 Cell Connection – 615M-1

Click Cell Connection on the main navigation pane to access the Carrier, UMTS, CDMA, System Monitor and Dynamic DNS settings pages.

#### Carrier

Click the Carrier tab on the Cell Connection page to change carrier settings.

Figure 15 Cell Connection–Carrier

#### Carrier

- Active Carrier** Selects the carrier and credentials to use for data calls. The Secondary Carrier cannot be selected if it is None. Changing carriers takes time, and the page may take up to one minute to refresh after Save is clicked.
- Primary Carrier** A list of carriers and their cellular protocols (UMTS/CDMA) and regions (Global, North America, Europe). Select the appropriate carrier (it cannot be the same as the Secondary Carrier). UMTS carriers require that a proper SIM be installed.
- Secondary Carrier** A list of carriers and their cellular protocols (UMTS/CDMA) and regions (Global, North America, Europe) or None. Select the appropriate carrier. It cannot be the same as the Primary Carrier. UMTS carriers require that a proper SIM be installed.
- Auto Connect** When set to Enable, it allows the modem to automatically dial the connection when the modem is powered. When set to Disable, the modem does not automatically dial the connection to the cellular provider and does not attempt to automatically re-connect when the connection has dropped.

#### Primary/Secondary Carrier

- Carrier APN** This field is visible only when the corresponding carrier supports UMTS. Enter the APN provided by the carrier.
- User** Sets the user name required by the cellular provider. Leave blank if not required.



**Warning:** If used in combination with this modem’s VPN Server, this user name and password will also be valid on this modem’s VPN Server.

<b>Password</b>	Sets the password required by the cellular provider. Leave blank if not required.
<b>Authentication Protocols</b>	Selects the authentication protocol used. If Auto is selected, the 615M-1 will negotiate a protocol with the cell tower. If Use Only is chosen, then the 615M-1 will only accept requests for the specified protocols.

## GSM Settings

Click the GSM Settings tab on the Cell Connection page to change GSM settings. The fields are only enabled if the Active Carrier supports GSM. You can choose a specific Band of operation and change various Subscriber Identity Module (SIM) settings.

The SIM, a detachable smart card containing a user’s subscription information, is one of the key features of GSM. This card allows a user to retain his or her information after switching handsets. The SIM has a security feature which, when enabled, requires a user to enter a valid PIN before the modem will connect to the cellular network.

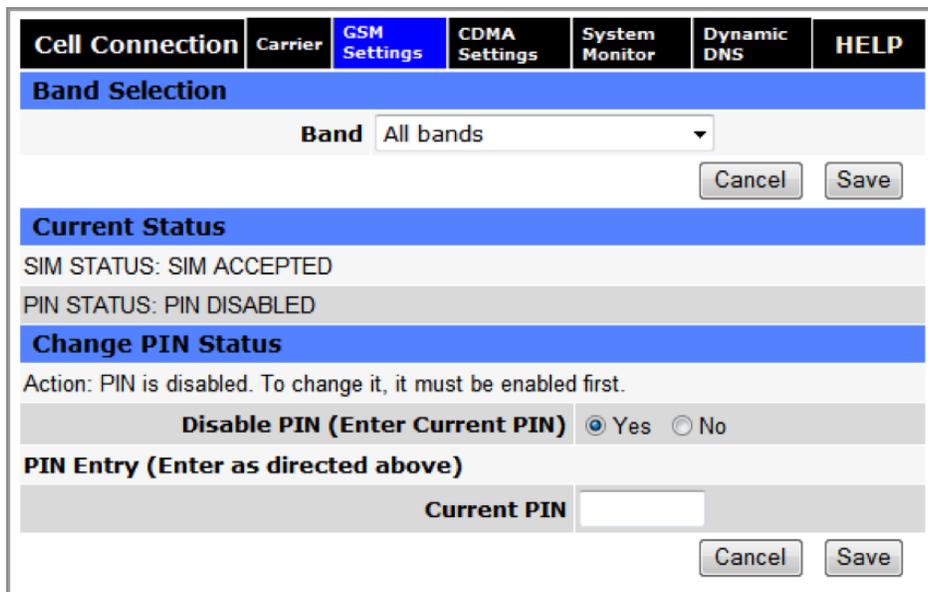


Figure 16 Cell Connection–GSM Settings

### Band Selection

<b>Band</b>	A list of frequency bands appropriate for the Active Carrier. Select a specific band or (recommended) select All Bands.
-------------	---

### Current Status

<b>SIM STATUS</b>	“SIM ACCEPTED” is displayed if a valid SIM card is inserted properly into the modem. “NO SIM, Insert Valid SIM and Press Reset” is displayed if the SIM card is invalid or missing.
<b>PIN STATUS</b>	“PIN DISABLED” is displayed when the PIN security is not enabled.

### Change PIN Status – Disable PIN

<b>Action</b>	“PIN disabled. To change it, it must be enabled first” is displayed when PIN security is not enabled.
---------------	---

### Disable PIN (Enter Current PIN)

Select “Yes” to disable the PIN security feature. Select “No” to enable PIN security for the modem. After selecting No, enter the current PIN in the Current PIN field. Click Save to finish enabling PIN security.

“PIN ACCEPTED” is displayed when the PIN security is enabled.

**Action** You may change only one of the following three options at a time. Three choices are given to Remember, Disable, or Change the PIN security settings.

### Remember PIN (Enter Current PIN)

Selecting Yes allows the modem to remember the security PIN, making it unnecessary to enter the PIN each time the modem tries to connect to the network. Selecting “No” will set the modem to not remember the current PIN, requiring the user to enter the PIN when requested.

### Disable PIN (Enter Current PIN)

Selecting “Yes” will disable the PIN security feature; the current PIN will need to be entered to allow disabling. Selecting “No” will not disable the PIN security feature.

### Change PIN (Enter Current PIN, New PIN, and Confirm PIN)

Selecting “Yes” will allow the user to change the current PIN to a new one. Selecting “No” will not require the user to change the PIN in the New PIN and Confirm PIN fields. After making changes, click Save to save the settings.

“PIN Entry Required” is displayed when the PIN security is enabled and set not to remember the PIN.

“Unknown” is displayed if the SIM card is not detected.

“SIM Invalid” is displayed if the SIM card is not detected.

**PIN** A field is provided for the user to enter the valid PIN. The user has three opportunities to enter the correct PIN.

### Change PIN Status – PIN Entry

**Current PIN** Enter the current valid PIN if PIN security is enabled. This field is also used to enable PIN security after selecting “No” to Disable PIN security.

**New PIN** Enter the new PIN (only if PIN security is enabled).

**Confirm New PIN** Re-enter the new PIN to confirm it (only if PIN security is enabled).

## CDMA Settings

Click the CDMA Settings tab on the Cell Connection page to change CDMA settings. The fields on this page are only enabled if the Active Carrier supports CDMA. You can choose a specific Band of operation and provision a new modem.

When a new modem is powered up for the first time, most of the provisioning information is blank or has information that needs to be changed. The device is usually shipped with the radio ready to be provisioned on a cellular carrier’s network. Features called Over-The-Air Service Provisioning (OTASP) and Open Mobile Alliance Device Management (OMA-DM) are supported, which allow the cellular providers to program the modem with specific information to activate the account.

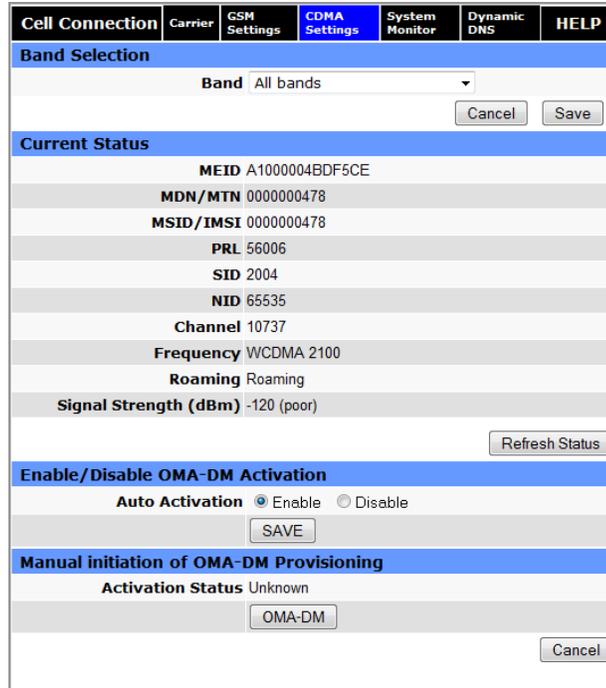


Figure 17 Cell Connection–CDMA Provisioning

### Band Selection

**Band** A list of frequency bands appropriate for the Active Carrier. Select a specific band or (recommended) select All Bands.

### Current Status

- MEID** The Mobile Equipment Identifier is used by the cellular carrier as the means to identify the cellular module. This is the identifier used to set up the user account with the cellular provider.
- MDN/MTN** The actual phone number of the device as supplied by the carrier. When the unit is successfully provisioned, the phone number for the user account is displayed.
- MIN/IMSI** This number is used by the Mobile Telephone Network, and will be different if ported from another carrier (not used by end user of device).
- PRL** The Preferred Roaming List is only applicable to the CDMA product line and is carrier specific (AllTel, Verizon, Sprint, and so on).
- SID** System ID (Identity), provided by the carrier.
- NID** Network Identifier, this is supplied automatically by the network.
- Channel** Cell Site channel number to which the modem is connected. This number may be useful to the cellular provider for troubleshooting purposes.
- Frequency** Cellular frequency band the modem is using. The 800 MHz and 1900 MHz bands are mainly in the US and outlying areas. In some cases, 900 and 1800 is seen for European or foreign carriers.

<b>Roaming</b>	Indicates Roaming or Not Roaming. Roaming means that service is being provided by an alternate carrier who has a roaming agreement with your contracted carrier. While Roaming, additional charges may apply. For provisioning, the unit must be Not Roaming.
<b>Signal Strength (dBm)</b>	Measured in dBm, this is the Received Signal Strength Indicator (RSSI). For provisioning, the signal strength should be greater than -95 dBm.

### Enable/Disable OMA-DM Activation

This section is only displayed for units that are capable of automatic (OMA-DM) provisioning. Sprint supports OMA-DM. You may choose to enable or disable automatic provisioning and save your setting. If enabled, and the unit is not provisioned (activated), each time at power-on (only) the unit will attempt an auto-activation. This capability is dependent on whether it is offered by your cellular carrier.

<b>Auto-Activation</b>	Select "Enable" to direct an unprovisioned unit to attempt OMA-DM activation once per power-up. Click Save to save the setting after making a change.
------------------------	---

### Manual Initiation of OMA-DM Provisioning

This section is only displayed for units that are capable of automatic (OMA-DM) provisioning. The activation status is displayed, and a button is provided to direct the unit to begin an OMA-DM provisioning attempt. Depending on changes to your carrier's network, it may be necessary to re-provision a unit that has already been activated. The OMA-DM capability is dependent on whether it is offered by your cellular carrier.

<b>Activation Status</b>	Displays the device activation status (Activated or Not Activated).
<b>OMA-DM</b>	Click the OMA-DM button to trigger an OMA-DM provisioning attempt.
<b>Activation Type</b>	This section is displayed for units that are not capable of automatic (OMA-DM) provisioning. Availability of OMA-DM is carrier dependent. For carriers that do not support OMA-DM, the provisioning process must be triggered by entering carrier specific information and clicking the carrier specified button (OTASP).
<b>Command (OTASP Only)</b>	The dial command used for provisioning the modem. For OTASP the number is *22899.
<b>OTASP</b>	Click the OTASP button to start the provisioning process for units using Verizon.

## System Monitor

Click the System Monitor tab on the Cell Connection page to access the configuration of additional self-monitoring for the modem in order to determine when service provider connections may have been terminated.

Cell Connection	Carrier	GSM Settings	CDMA Settings	System Monitor	Dynamic DNS	HELP
<b>Cell Connection Monitor</b>						
<b>Reset on Signal Loss</b> <input type="radio"/> Enabled <input checked="" type="radio"/> Disabled						
<b>Signal Loss Timeout</b> <input type="text" value="90"/> (90-65535) seconds						
<input type="button" value="Cancel"/> <input type="button" value="Save"/>						
<b>Periodic Reset Timer</b>						
<b>Periodic Reset Type</b> <input checked="" type="radio"/> Interval <input type="radio"/> Scheduled <input type="radio"/> Disabled						
<b>Interval Length</b> <input type="text" value="4320"/> (0=disabled, 15-65535) mins						
<b>Scheduled Time</b> <input type="checkbox"/> S <input type="checkbox"/> M <input type="checkbox"/> T <input type="checkbox"/> W <input type="checkbox"/> Th <input type="checkbox"/> F <input type="checkbox"/> S <input type="checkbox"/> All						
<input type="text" value="00"/> : <input type="text" value="00"/> UTC (00:00 - 23:59)						
<input type="button" value="Cancel"/> <input type="button" value="Save"/>						
<b>Periodic PING Settings</b>						
<b>Destination Address</b> <input type="text"/>						
<b>Secondary Address</b> <input type="text"/>						
<b>Periodic PING Timer</b> <input type="text" value="0"/> (0, 60-3600) in 10 sec steps, 0=disable						
<b>Fail Count</b> <input type="text" value="5"/> (3-10)						
<input type="button" value="Cancel"/> <input type="button" value="Save"/>						
<b>WAN Data Usage Estimates</b>						
<b>Rx Bytes</b> 13810933						
<b>Rx Packets</b> 210753						
<b>Rx Errors</b> 0						
<b>Rx Packets Dropped</b> 0						
<b>Tx Bytes</b> 469917609						
<b>Tx Packets</b> 356346						
<b>Tx Errors</b> 0						
<b>Tx Packets Dropped</b> 0						
<input type="button" value="Clear"/>						

Figure 18 Cell Connection–System Monitor

### Cell Connection Monitor

**Reset on Extended Loss** Fixed-point connections expect to have consistent access to the cellular network, as compared to mobile connections that may temporarily lose access depending on coverage. This option causes the modem to reset if the cell connection is lost for more than the Signal Loss Timeout specified.

**Signal Loss Timeout** When Reset on Signal Loss is enabled, enter a timeout period between 90 and 65535 seconds.

### Periodic Reset Timer

**Periodic Reset Type** Sets the Periodic Modem Reset timer to an Interval of time, a Scheduled day, or disables the timer.

**Interval Length** Sets the Periodic Modem Reset time from 15 to 65,535 min. The Periodic Reset is disabled when set to 0. Default is set to 4320 min (approximately 3 days).

**Scheduled Time** Sets the Periodic Modem Reset to occur at the specified time. Select specific days of week or select “All” for daily reset. Time is specified as Local Time, based on the location of the modem itself. The modem’s current time is shown on the home page.

## Periodic Ping Settings

The Periodic Ping can be used to actively check that a currently established data connection with the cellular carrier is still valid. If enabled and the cellular connection is UP, pings are output and the response is monitored as specified by the following settings. Periodic Ping is not active when the cell connection is DOWN.

<b>Destination Address</b>	You may enter an accessible IP address or URL that will respond to a ping command.
<b>Secondary Address</b>	You may enter an accessible IP address or URL that will respond to a ping command. This address will be used if the entered number of consecutive ping failures using the first address is reached.
<b>Periodic Ping Timer</b>	You may enter an interval in increments of 10 seconds. The modem will ping the destination at that interval. Enter 0 to disable this feature.
<b>Fall Count</b>	The modem will reset if the number of consecutive ping failures is equal to or greater than the fall count and the secondary address is being used. Otherwise the modem will switch from the first address to the secondary address for the ping test.

## WAN Data Usage Estimates

This section tracks the data received from and transmitted to the cellular network. This is a tool that may be used to estimate network usage. These totals are tracked by the router. Your carrier maintains separate statistics from which your billing is determined. One way to use this tool is to track usage over a fairly short period of typical usage. The total then can be extrapolated to estimate longer time periods. This router updates these statistics once approximately every 30 seconds. Click Clear to reset the totals to 0.

<b>Rx Bytes</b>	The total number of bytes received by the modem from the cell network. All statistics are cleared automatically when this count exceeds 1 billion (1,000,000,000).
<b>Rx Packets</b>	The total number of TCP and UDP packets received by the modem from the cell network.
<b>Rx Errors</b>	The number of corrupted TCP and UDP packets received by the modem from the cell network.
<b>Rx Packets Dropped</b>	The number of TCP and UDP packets received by the modem from the cell network that were not accepted. This may occur due to memory or throughput problems.
<b>Tx Bytes</b>	The total number of bytes transmitted by the modem to the cell network. All statistics are cleared automatically when this count exceeds 1 billion (1,000,000,000).
<b>Tx Packets</b>	The total number of TCP and UDP packets transmitted by the modem to the cell network.
<b>Tx Errors</b>	The number of corrupted TCP and UDP packets received by the modem that were meant to be transmitted on the cell network.
<b>Tx Packets Dropped</b>	The number of TCP and UDP packets received by the modem for transmit to the cell network that were not accepted. This may occur due to memory or throughput problems.
<b>Clear</b>	Click Clear to reset the totals to 0. These totals are NOT cleared by a modem reboot.

## Dynamic DNS

Click the Dynamic DNS tab on the Cell Connection page to configure dynamic DNS. Dynamic DNS is a system that allows the domain name data of a computer with a varying (dynamic) IP address held in a name server to be updated in real time, making it possible to establish connections to that machine without the need to track the actual IP address. A number of providers offer Dynamic DNS services (DDNS), free or for a charge. For example, a free service provided by NO-IP allows users to setup between one and five host names on a domain name provided by NO-IP. NO-IP is the default DNS service.

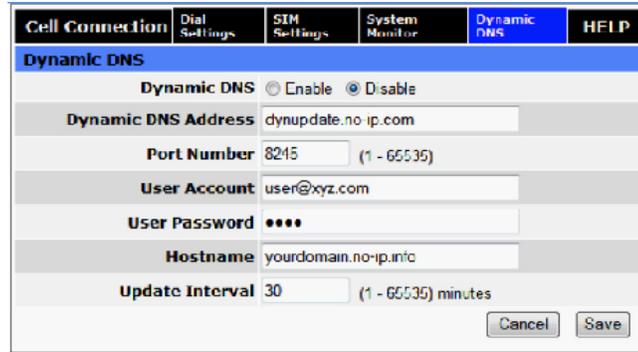


Figure 19 Cell Connection–Dynamic DNS

## Dynamic DNS

### Dynamic DNS

Selecting “Enable” allows the modem to provide the selected service dynamic IP address information. Selecting “Disable” stops any IP information from being sent to the selected service.

### Dynamic DNS Address

The Internet address to which the Dynamic DNS information is to be communicated. Default is dynupdate.no-ip.com.

### Port Number

The port number for the Internet address given above. Default is 8245.

### User Account

The user name used when setting up the account. Used to login to the Dynamic DNS service.

### User Password

The password associated with the user name account.

### Hostname

The hostname identified to the Dynamic DNS service. For example, http://test.myserver.com.

### Update Interval

Sets the interval at which the modem will update the Dynamic DNS server of its carrier assigned IP address. The update interval can be between 0 to 65,535 minutes. It is recommended that the update interval be set as long as necessary. Each update is considered a data call by the cellular provider and could deplete low usage data plan minutes.

### Save

Click Save for changes to take effect.

### 3.4 LAN Settings

Click LAN Settings on the main navigation pane to access LAN configuration settings and the MAC and IP filtering.

LAN	LAN Settings	MAC Filtering	IP Filtering	HELP
<b>LAN Settings</b>				
Ethernet IP Address	192 . 168 . 1 . 50			
Ethernet Subnet Mask	255 . 255 . 255 . 0			
LAN Masquerade	<input checked="" type="radio"/> Enable <input type="radio"/> Disable			
Bind Services to Eth IP	<input type="radio"/> Enable <input checked="" type="radio"/> Disable			
<b>DNS Resolving</b>				
DNS Auto	<input checked="" type="radio"/> Enable <input type="radio"/> Disable			
DNS Server 1 IP Address	192 . 168 . 1 . 50			
DNS Server 2 IP Address	0 . 0 . 0 . 0			
<b>DHCP Configuration</b>				
DHCP	<input checked="" type="radio"/> Enable <input type="radio"/> Disable			
DHCP start range	192 . 168 . 1 . 120			
DHCP end range	192 . 168 . 1 . 200			
DHCP Lease Time	86400 (seconds)			
<b>Remote Administration</b>				
Web Server Port	80 (1 - 65534)			
Remote Configure	<input checked="" type="radio"/> Enable <input type="radio"/> Disable			
Incoming Port	8080 (1 - 65534)			
Admin Password	<input type="text"/>			
Confirm Password	<input type="text"/>			
Friendly IP Address	0 . 0 . 0 . 0 /			
Apply Friendly IP Address	<input type="checkbox"/> Remote Administration <input type="checkbox"/> SSH <input type="checkbox"/> Telnet <input type="checkbox"/> SNMP			
SSH Port	50022 (1 - 65534, 0 to block)			
Telnet Port	23 (1 - 65534, 0 to block)			
SNMP Port	161 (1 - 65534, 0 to block)			
<b>RADIUS Settings</b>				
RADIUS Authentication	<input type="radio"/> Enable <input checked="" type="radio"/> Disable			
Server IP Address	0 . 0 . 0 . 0			
Server Port	1812			
Server Secret	<input type="text"/>			
Confirm Secret	<input type="text"/>			
Timeout	2			
Retries	2			
				Cancel Save

Figure 20 LAN-LAN Settings

#### LAN Settings

**Ethernet IP Address** This sets the IP address of this device and is the address used to access the configuration pages. If the IP address changes, you will need to re-enter the new IP address in your browser to access the configuration pages. The default IP address is 192.168.1.50 and should be changed for security purposes.

**Ethernet Subnet Mask** Sets the subnet mask for the LAN side of the modem to the device.

- LAN Masquerade** When enabled, the 615M-1 masquerades all Ethernet traffic to the LAN, making all WAN traffic appear as if it originated from the 615M-1. This can be useful in applications where there is equipment on the local LAN that cannot cope with connections from multiple Host IP addresses.
- Bind Services to Eth IP** UDP datagrams or TCP sockets from services inside the 615M-1 (Serial, IO, GPS) normally appear to come from the interface (LAN or WAN) closest to the destination. Enable this option to force the source address to be the LAN Ethernet IP address. This can be useful if packets are being sent through a VPN tunnel. Note that outside of a tunnel, Network Address Translation (NAT) may still force the source address to be rewritten to the WAN address.

## DNS Resolving

- DNS Auto** Selecting “Enable” allows the servers designated as DNS Server 1 or 2 to automatically resolve domain names to IP addresses. These servers communicate with name servers by sending DNS queries and heeding DNS responses. Selecting “Disable” does not allow DNS Server 1 or 2 to resolve domain names.
- DNS Server 1 IP Address** The Ethernet IP address of the preferred DNS server. The default address is 192.168.1.50, the same as the LAN Ethernet IP Address for the modem. If the LAN Ethernet IP Address changes, the DNS Server 1 address will automatically change to the same.
- DNS Server 2 IP Address** Ethernet address of the alternate DNS server. The default is set to 0.0.0.0.

## DHCP Configuration

- DHCP** Dynamic Host Configuration Protocol, a protocol used by client devices that are connected to the LAN port of this device to automatically obtain an IP address assigned by this device. Selecting “Enable” configures this device to assign IP addresses to client devices taken from a pool specified by the values entered in the DHCP start range and DHCP end range. Selecting “Disable” turns off this DHCP server functionality.
- DHCP start range** DHCP server starting IP address. The default is set as 192.168.1.100.
- DHCP end range** DHCP server ending IP address. The maximum usable number is 253.
- DHCP Lease Time** Sets the duration (in seconds) that the connected device is allowed to keep the assigned IP address. In many cases it is possible for the device to receive the same IP address after the lease time expires.

## Remote Administration

- Web Server Port** Enter the port number to be used by the web server.
- Remote Configure** Selecting “Enable” allows remote access to the modem’s configuration pages through the cellular network connection. Selecting “Disable” turns off the ability to remotely access the modem’s configuration pages.
- Incoming Port** Sets the port number used to remotely configure the modem. (Remote Configuration is unavailable if the Incoming Port number also appears in an entry in Router | Port Forwarding | IP Mapping Table.)
- Admin Password** Sets the password required for remote configuration.
- Confirm Password** Re-enter the Admin Password to confirm the correct spelling.

<b>Friendly IP Address</b>	Specifies the IP address from which remote administration is permitted. Entering 0.0.0.0 will allow any IP address. Leave the fifth box blank (after the /) if specifying a specific IP, or 0.0.0.0. A subnet mask may be entered in the fifth box. The mask indicates how many bits of the IP address to match. The mask can be a value from 1 to 32.
<b>Apply Friendly IP Address</b>	Selecting the checkbox for a service allows remote access to the service only from the friendly IP address. Clearing the checkbox for a service allows any IP address access to the service.
<b>SSH, Telnet, and SNMP Ports</b>	Enter the port number that will be used for remote access to the service. Entering zero for the port number will block remote access to the service. Once a service is blocked (0 entered) or moved to another port, the default port number (such as 23 for Telnet) can be used in a Port Forwarding rule to provide access to a user device located behind the modem. Port Forwarding has precedence. Therefore, if the SSH, Telnet or SNMP port also appears as an Incoming Port in an entry in Router   Port Forwarding   IP Mapping Table, that service will be unavailable.

## RADIUS Settings

<b>RADIUS Authentication</b>	Enables or disables RADIUS authentication for web page access.
<b>Server IP Address</b>	The IP address of the RADIUS server.
<b>Server Port</b>	The port of the server.
<b>Server Secret</b>	Sets the secret to use with the server.
<b>Confirm Secret</b>	Re-enter the Server Secret to confirm the correct spelling.
<b>Timeout</b>	Specifies how many seconds to wait before a retry.
<b>Retries</b>	Specifies how many times to retry authenticating with the server before giving up.
<b>Save and Cancel</b>	After modifying settings, either click Save to keep the currently displayed value for each parameter or click Cancel to discard the changes and return to the last saved parameters. Once Save is clicked, Cancel cannot be used to return to previous settings.

## MAC Filtering

Click the MAC Filtering tab on the LAN page to configure MAC filtering, which allows up to five unique device MAC addresses to have access to the network.

Figure 21 LAN–MAC Filtering

### MAC Filtering

<b>MAC Filtering</b>	Allows you to Enable or Disable MAC filtering.
<b>Allowed MAC Address</b>	Enter the MAC address for a device to be allowed on the network.
<b>Comment</b>	Use this field to add a name describing the device that is using the allowed MAC address.
<b>Clear</b>	Click Clear to remove the MAC address from the list of allowed addresses.
<b>Save and Cancel</b>	Click Save to save the changes, or click Cancel to discard the changes.

## IP Filtering

Click the IP Filtering tab on the LAN page to add or change IP filters.

The screenshot shows the 'IP Filtering' configuration interface. At the top, there are navigation tabs: LAN, LAN Settings, MAC Filtering, IP Filtering (highlighted), and HELP. Below the tabs, the 'IP Filtering' section is active, with 'Enable' selected and 'Disable' unselected. There are 'Cancel' and 'Save' buttons. The 'Add Custom IP Filters' section contains several fields: Filter Number (1-20), Source IP Address, Destination IP Address, Protocol (Any, ICMP, TCP, UDP, Other), Source Port, Destination Port, Direction (Any, WAN to LAN), and Action (Keep, Drop). Each field has an 'Exclude' checkbox. 'Clear' and 'Add' buttons are at the bottom. A table titled 'Custom IP Filters' is empty, showing columns: No, Src IP, Dst IP, Proto, Src Port, Dst Port, Dir, Act.

Figure 22 LAN-IP Filtering

You can enter up to 20 IP filters. Each IP filter is identified by a unique number (from 1 to 20). An IP packet passes through the filtering logic when the “IP Filtering” option is enabled and one of the following conditions apply:

- The IP packet is received on one of the interfaces and is destined to the 615M-1 unit,  
OR
- The IP packet is sent by the 615M-1 unit,  
OR
- The IP packet is forwarded by the 615M-1 unit.

The filtering logic is as follows:

```

if exists(filter[1]) AND match(packet, filter[1]) then apply(action[1])
else if exists(filter[2]) AND match(packet, filter[2]) then apply(action[2])
else if exists(filter[3]) AND match(packet, filter[3]) then apply(action[3])
...
else if exists(filter[20]) AND match(packet, filter[20]) then apply(action[20])
else process packet normally.
    
```

Where:

```

exists(filter[n]) -> The user as defined filter number n.
match(packet, filter[n]) -> The IP packet matches filter number n.
apply(action[n]) -> The action identified in filter number n.
    
```

## IP Filters

**IP Filtering** Allows you to enable or disable IP filters. When “Enable” is selected, the custom IP filters you have entered are taken into account when processing IP packets. The predefined IP filters are also be taken into account. When “Disable” is selected, is no IP filtering.

### Add Custom IP Filters

**Filter Number** Each IP filter is identified by a unique number from 1 to 20.

**Source IP Address** Specifies the source IP address.

**Any**—Any source IP Address will satisfy this criteria.

**Specific**—A specific Host IP address.

**Range**—A range of IP addresses.

When “Exclude” is selected, in order for the packet to match with the criteria it must NOT have the specified source IP address (or NOT be within the given source IP address range).

**Destination IP Address** Specifies the destination address.

**Any**—Any destination IP Address will satisfy this criteria.

**Specific**—A specific Host IP address.

**Range**—A range of IP addresses.

When “Exclude” is selected, in order for the packet to match with this criteria it must NOT have this destination IP address (or NOT be in the given destination IP address range).

**Protocol** **Any**—Any protocol number.  
**ICMP**—The ICMP protocol (1).  
**TCP**—The TCP protocol (6).  
**UDP**—The UDP protocol (17).  
**Other**—Any other IP protocol.

When “Exclude” is selected, in order for the packet to match with this criteria it must NOT have this protocol number.

<b>Source Port</b>	<p><b>Any</b>—Any source port number. <b>Specific</b>—Select a specific source port number. <b>Range</b>—Select a range of source port number.</p> <p>When “Exclude” is selected, in order for the packet to match with this criteria it must NOT have this source port number (or NOT be in the given source port number range).</p>
<b>Destination Port</b>	<p><b>Any</b>—Any destination port number. <b>Specific</b>—Select a specific destination port number. <b>Range</b>—Select a range of destination port number.</p> <p>When “Exclude” is selected, in order for the packet to match with this criteria it must NOT have this destination port number (or NOT be in the given destination port number range).</p>
<b>Direction</b>	<p>The direction corresponds to the path taken by the IP packet inside the 615M-1 unit.</p> <ul style="list-style-type: none"><li>• An IP packet can <b>TERMINATE</b> inside the 615M-1 unit. <b>WAN to 615M-1</b>—The IP packet is received from the WAN (cellular) interface and is destined to the 615M-1 unit. <b>LAN to 615M-1</b>—The IP packet is received from the LAN interface and is destined to the 615M-1 unit.</li><li>• An IP packet can <b>ORIGINATE</b> from the 615M-1 unit. <b>615M-1 to WAN</b>—The IP packet is sent by the 615M-1 unit to the WAN (cellular) interface <b>615M-1 to LAN</b>—The IP packet is sent by the 615M-1 unit to the LAN interface.</li><li>• An IP packet can be <b>FORWARDED</b> by the 615M-1 unit. <b>WAN to LAN</b>—The IP packet is received on the WAN (cellular) interface and forwarded to the LAN interface. <b>LAN to WAN</b>—The IP packet is received on the LAN interface and forwarded to the WAN (cellular) interface.</li></ul> <p>When “Exclude” is selected, in order for the packet to match with this criteria it must NOT be processed in the given direction.</p>
<b>Action</b>	<p><b>Keep</b>—If IP filtering is enabled and an IP packet matches all criteria in the IP filter, keep the IP packet (continue normal processing of the IP packet).</p> <p><b>Drop</b>—If IP filtering is enabled and an IP packet matches all criteria in the IP filter, drop the IP packet.</p>
<b>Custom IP Filters</b>	
<b>Del</b>	Click Del to delete the filter.

### 3.5 Router

Click Router on the main navigation pane to access the Port Forwarding and Static Routing pages.

#### Port Forwarding

Click the Port Forwarding tab on the Router page to configure port forwarding. Port forwarding is a technique for transmitting and receiving network traffic through a router that involves re-writing the source and/or destination IP addresses and typically the TCP/UDP port numbers of IP packets as they pass through. The various routing configurations are displayed in the IP mapping table at the bottom of the page.

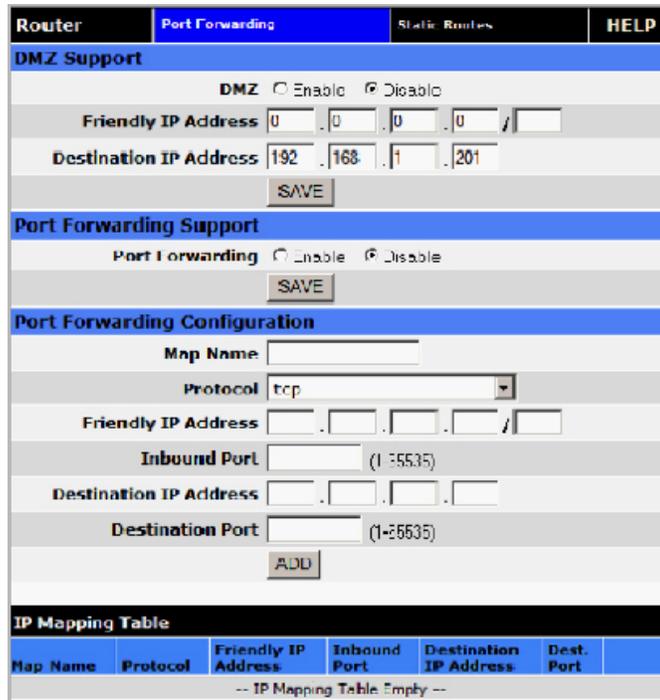


Figure 23 Router-Port Forwarding

#### DMZ Support

DMZ is a host on the internal network that has all ports exposed, except those ports forwarded otherwise.

- DMZ** Select “Enable” to allow the modem to use DMZ routes using the address set in the Destination IP Address. Select “Disable” to shut down the DMZ functionality.
- Friendly IP Address** Optionally restricts DMZ access to the specified IP address. If set to “0.0.0.0,” the DMZ is open to all incoming IP Addresses.
- Destination IP Address** The IP address that has all ports exposed, except ports defined in the Port Forwarding configuration.
- Save** Click Save for the changes to take effect.

#### Port Forwarding Configuration

- Map Name** Sets the Map Name for the IP mapping table at the bottom of the page. The Map Name can be up to ten characters in length. Do not use spaces in the character string.
- Protocol** Sets the data protocol as TCP, UDP, or All.

- Friendly IP Address** Specifies an IP address that is allowed to access the modem, or a wildcard IP address of 0.0.0.0 that allows all IP addresses to access the modem. Leave the fifth box blank (after the “/”) if specifying a specific IP, or 0.0.0.0. A subnet mask may be entered in the fifth box. The mask indicates how many bits of the IP address to match. The mask can be a value from 1 to 32.
- Inbound Port** Sets the external port number for incoming requests. (Port Forwarding rules take precedence over the services specified in LAN Settings | Remote Administration | Incoming port, SSH Port, Telnet Port or SNMP Port.)
- Destination IP Address** Sets the Local Area Network Address of the device connected to the modem’s Ethernet jack. Inbound requests will be forwarded to this IP address.
- Destination Port** Sets the Local Area Network port number used when forwarding to the destination IP address.
- Add** Click Add to save the new entry.

### Static Routes

Click the Static Routes tab on the Router page to open the static routing configuration page. Static routing refers to a manual method of setting up routing between networks. The Static Routes page allows you to create static routes and add them to the routing table, which appears at the bottom of the page.

Figure 24 Router–Static Routes

### Static Routes

- Route Name** Sets the alphanumeric identifier of the static route in the Static Route Table.
- Destination IP Address** Sets the IP address of the destination network.
- IP Subnet Mask** Sets the subnet mask of the destination network.
- Gateway** Sets PPP (this router’s wireless Internet connection), PPTP (VPN), GRE Tunnel, or the local network IP address for the gateway to the destination network.
- Gateway IP Address** The gateway IP address is only used if a local IP address was selected for the gateway. Enter the address of the local gateway.

- Metric** Sets the route priority (1 to 20). The lower the metric value the higher the route priority.
- Add** Click Add to add the configured route to the (Static) Routing Table.

### 3.6 Security

Click Security on the main navigation pane to access the PPTP, IPsec, and GRE pages.

#### Status

Click the Status tab on the Security page to see the status of the PPTP client and server and IPsec tunnels.

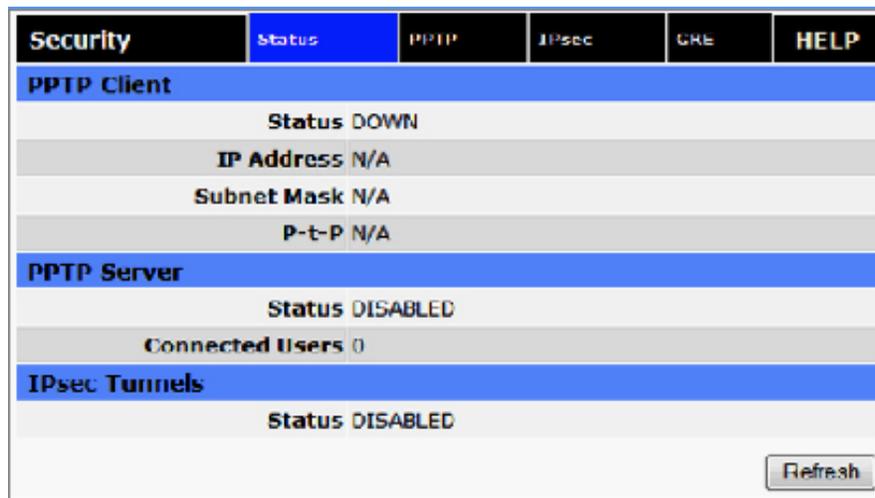


Figure 25 Security-Status

#### PPTP Client

- PPTP Client Status** Indicates the status of the PPTP Client interface, typically UP when connected properly. PPTP is the Point-to-Point Tunneling Protocol used to implement a Virtual Private Network (VPN).
- PPTP IP Address** The current IP address assigned to the modem by the VPN server.
- PPTP Subnet Mask** Indicates the status of the PPTP Client interface, usually UP when connected properly. PPTP is the Point-to-Point Tunneling Protocol used to implement a VPN.
- PPTP P-t-P** This is the LAN address of your VPN server.

#### PPTP Server

- Status** The PPTP Server is either ENABLED or DISABLED, depending on the setting selected on the Security-PPTP page.
- Connected Users** Number of users currently connected to the PPTP Server.

#### IPsec Tunnels

- Status** The number of established IPsec tunnels based on the number of tunnels Enabled on the Security-IPsec page.

## PPTP

Click the PPTP tab on the Security page to configure Point-to-Point Tunneling Protocol (PPTP), a method for implementing virtual private networks (VPN).

Figure 26 Security–PPTP

### PPTP Client Configuration

<b>PPTP Client</b>	Selecting “Enable” allows PPTP functionality. Selecting “Disable” turns off PPTP functionality.
<b>Set Default Route to PPTP</b>	Selecting “Enable” routes all IP traffic through the PPTP network. Selecting “Disable” routes only PPTP traffic through the PPTP network.
<b>PPTP Server</b>	The IP address of the virtual private network server on which to connect.
<b>Username</b>	The user name required by the VPN server.
<b>Password</b>	The password (associated with the user name) required by the VPN server.

### PPTP Server Configuration

<b>PPTP Server</b>	Selecting “Enable” starts the VPN server. Selecting “Disable” stops the VPN server.
<b>Server Local IP</b>	The IP address that clients will use to communicate with the server after they connect.
<b>Client IP Range</b>	The pool of IP addresses assigned to clients.
<b>Protocols Allowed</b>	Selecting a protocol will instruct the VPN server to accept clients who use that protocol. The server rejects clients using any of the unselected protocols.
<b>Encryption</b>	Selecting “Use MPPE” enables Microsoft Point-to-Point Encryption for communication between the server and clients. This option requires the MS-CHAP or MS-CHAPv2 protocol.

### PPTP Server User Configuration

- Full Name** This name can be used as a descriptive name for a client. It is not used by the server. No spaces are allowed in the name.
- Username** The name used by a client to log in to the server.
- Password** The password (with associated user name) used by a client to log in to the server.

### IPsec

Click the IPsec tab on the Security page to configure secured communication tunnels. The various tunnel configurations are displayed in the Tunnel Table at the bottom of the page. All tunnels are created using the ESP (Encapsulating Security Payload) protocol.

Figure 27 Security-IPsec

## IPsec Support

IPsec	Selecting “Enable” launches the IPsec process and starts all enabled tunnels. Selecting “Disable” stops all tunnels and shuts down the IPsec process. Note that all enabled tunnels are launched automatically when the unit connects to the cellular carrier.
NAT Mode	Determines how packets are addressed. Selecting “Bypass” allows packets coming from Local Subnet addresses to pass through the Network Address Translation (NAT) firewall unchanged. This may be sufficient when traffic only travels from Local Subnet to Remote Subnet. (To make sure that packets generated by 615M-1 services appear to originate from a Local Subnet address, you may need to enable the “Bind Services to Eth IP” option on the LAN Settings page.) NAT changes the source address to match the PPP IP Address shown on the Status tab of the Unit Status page. NAT-Traversal enables the NAT-T protocol which can support traffic beyond just the Local & Remote Subnets.

## Tunnel Monitor

To supplement or complement Dead Peer Detection, tunnels can be monitored by sending periodic pings, and restarting the tunnels if the pings repeatedly fail. Tunnel monitoring is controlled by the following five parameters.

IP Address 1 & IP Address 2	Up to two addresses may be entered. Tunnels are monitored only if their IP address matches the Remote IP Address or belongs to the Local Subnet or Remote Subnet. A value of 0.0.0.0 disables monitoring.
Delay	How often (in seconds) to send pings over the tunnel.
Fail count threshold	The number of successive pings that need to fail to cause the tunnel to be restarted.
Success count threshold	The number of successive pings that need to succeed for the tunnel to be considered “up” and for the process of counting failed pings to begin.

## Tunnel Configuration

Tunnel Item	Tunnel number. Starts from 1 and increments for each new tunnel. To update an existing tunnel, use its corresponding number from the tunnel table. To add a new tunnel, use the last tunnel shown in the Tunnel Table + 1.
Label	This is a label to identify a tunnel and must correspond to the name specified for the remote endpoint.
Remote IP Address	The IP address of the remote endpoint of the tunnel.
Remote Subnet	Select “None” if encrypted packets are only destined for the Remote IP Address. Use an IP address/mask if encrypted packets are also destined for the specified network that is beyond the Remote IP Address.
Local Subnet	<p> <b>IMPORTANT: The Remote Subnet and Local Subnet addresses must not overlap.</b></p> <p>Select “None” if only packets generated by 615M-1 services are to be sent over the tunnel. Select “Ethernet” if packets from the local LAN are also to be sent over the tunnel. (To make sure that packets generated by 615M-1 services appear to originate from a Local Subnet address, you may need to enable the “Bind Services to Eth IP” option on the LAN Settings page.) Use an IP address/mask if a network beyond the local LAN will be sending packets over the tunnel.</p> <p> <b>IMPORTANT: The Remote Subnet and Local Subnet addresses must not overlap.</b></p>
Phase 1 Encryption	Use AES-128, AES-256 or 3DES encryption.

<b>Phase 1 Authentication</b>	Use MD5 or SHA1 hashing.
<b>Phase 1 DH Group</b>	Negotiate (Auto) or use 768 (Group 1), 1024 (Group 2), 1536 (Group 5) or 2048 (Group 14) bit keys.
<b>Phase 1 Key Lifetime</b>	How long the keying channel of a connection should last before being renegotiated.
<b>Phase 2 Encryption</b>	Use AES-128, AES-256 or 3DES encryption.
<b>Phase 2 Authentication</b>	Use MD5 or SHA1 hashing.
<b>Phase 2 Lifetime</b>	The duration of a particular instance of a connection, from successful negotiation to expiry.
<b>Pre-shared Key</b>	Predetermined key known to both the local unit and the remote side prior to establishing the tunnel.

### Negotiation Mode

Select "Normal" to allow IPsec to negotiate some connection parameters. Select "Aggressive" to require that only those parameters selected above can be used to create the tunnel.

<b>Perfect Forward Secrecy</b>	Enable Perfect Forward Secrecy for the session keys.
<b>Dead Peer Detection Delay</b>	Tunnel keepalive time for R_U_THERE packets during idle periods.
<b>Dead Peer Detection Timeout</b>	Timeout time during tunnel idle periods where no R_U_THERE_ACK has been received.
<b>Dead Peer Detection Action</b>	Action to be taken when timeout value is reached.
<b>Add/Update</b>	Click the Add/Update to save the new entry.

### Tunnel Table

<b>Enable</b>	Click Enable to enable a tunnel. The tunnel's state is saved across resets.
<b>View</b>	Click View to open a page showing the log of the tunnel's negotiation activity.
<b>Delete</b>	Click Del to delete the tunnel.

## GRE

Click the GRE tab on the Security page to add and delete GRE (Generic Route Encapsulation) tunnels. The current tunnels are listed at the bottom of the page. Up to two networks that lie beyond the tunnel may be specified, and routes to those networks are automatically created when the tunnel is established. Static local and remote IP addresses are necessary to allow for tunnel automatic (re)connection.

Figure 28 Security–GRE

### GRE Tunnel Configuration

- Local IP Address** The local (typically WAN interface) IP address associated with the tunnel.
- Remote IP Address** The remote IP address associated with the tunnel.
- Tunnel IP Address** The IP address assigned to the tunnel interface. For example, 192.168.10.100.
- Tunnel Subnet & Mask** The tunnel subnet and mask that must include the above Tunnel IP Address. For example, 192.168.10.0/24.
- Remote User Subnet 1 & Mask** The IP network representing that of the remote user subnet, accessible via the tunnel. For example, 192.168.20.0/24.
- Remote User Subnet 2 & Mask** A possible second IP network representing another remote user subnet. For example, 192.168.15.0/24.



**NOTE** All subnets must be different from one another. If more than two remote user subnets are necessary, additional routes can be setup manually via the Router | Static Routes web page using the Tunnel IP Address as the gateway.

## 3.7 Serial

Click Serial on the main navigation pane to access the serial port configuration page.

### External Serial

Click the External Serial tab on the Serial page to configure the RS-232 Serial Port parameters and Packet Assembler and Disassembler (PAD) functionality. The PAD feature forwards requests that come in on a specific port to the Serial connector.

Figure 29 Serial-External Serial

### External Serial Port Configuration

- |  |   |
|--|---|
| <b>Show Version on Boot</b>                    | When enabled, the router model number and firmware version are transmitted out the serial port upon router boot. Additionally, “OK” is transmitted when router is ready to receive data and when PPP connection is made. When disabled, these indicators are not transmitted out the serial port. |
| <b>Baud Rate, Data Bits, Stop Bits, Parity</b> | Sets the configuration of the serial port. Baud rate setting may range from 300 to 115,200 bps. The default configuration is 115,200 baud, 8 data bits, 1 stop bit, no parity.  |
| <b>Inter Character Timeout</b>                 | Sets the Inter Character Timeout from 1 to 65,535 ms.   |
| <b>DTR</b>                                     | Defines the Data Terminal Ready behavior. Refer to Table 9 for DTR descriptions.  |

Table 9 DTR Descriptions

<b>AT&amp;D0</b>	Ignore DTR.
<b>AT&amp;D2</b>	If in the Online Data State or Online Command State, upon an on-to-off transition of DTR the modem performs an orderly clear-down of the call and returns to the command state. Automatic answer is disabled while DTR remains off.
<b>AT&amp;D4</b>	The modem auto-dials the default remote station upon an off-to-on transition of DTR and enters the Online Data State. The modem ends the call and enters the command state upon an on-to-off transition of DTR.
<b>AT&amp;D5</b>	The modem auto-dials the default remote station upon an on-to-off transition of DTR and enters the Online Data State. The modem ends the call and enters the command state upon an off-to-on transition of DTR.
<b>AT&amp;D6</b>	Upon an on-to-off transition of DTR, the modem performs an orderly clear-down of any session and turns OFF the RF module. Upon an off-to-on transition of DTR, the modem turns ON the RF module and reestablishes the radio session.
<b>AT&amp;D7</b>	Upon an on-to-off transition of DTR, the modem performs an orderly clear-down of any session and turns OFF the RF module. Upon an off-to-on transition of DTR, the modem turns ON the RF module and reestablishes the radio session.
<b>AT&amp;D8</b>	The modem auto-dials the default remote station upon determining DTR is OFF and enters the Online Data State. The modem ends the call and enters the command state upon determining DTR is ON.
<b>AT&amp;D9</b>	The modem auto-dials the default remote station upon determining DTR is ON and enters the Online Data State. The modem ends the call and enters the command state upon determining DTR is OFF.

**Flow Control** Sets the Flow Control to None or Hardware control.

**DSR** Sets the Data Set Ready to Always On, On When Available, On When Connected or Always Off. The DSR parameter determines how the modem controls the state of the Data Set Ready circuit. The default value is Always Off.

**ALWAYS ON**—DSR is always on.

**ON WHEN AVAILABLE**—DSR is on when the RF signal present and phone registered on network.

**ON WHEN CONNECTED**—DSR is on when connected to CDMA.

**ALWAYS OFF**—DSR is always off.

## DCD

The DCD parameter determines how the modem controls the state of the Carrier Detect circuit and the amber DCD LED on the front panel. The default value is Connect On.

**ALWAYS ON**—DCD is always on.

**CONNECT ON**—DCD is on when connected to a remote host.

**ALWAYS OFF**—DCD is always off.

## External PAD Settings

### PAD Mode

Sets the PAD mode of the modem as a Server or Client. In Client mode, the modem will initiate an outbound connection to the Remote Host IP Address with the Outgoing Port based on the selected DTR setting. In Server mode, the modem will accept one incoming connection on the specified Incoming Port. The modem will not accept multiple incoming connections at the same time. Additional connections are arbitrated based on the Server Session Closed On and Timeout parameters.



**NOTE** It is possible to override Server mode and make an outgoing client connection using the RS-232 command set.

`atd*xxx.xxx.xxx.xxx:yyyyy`

When in server mode and no connection is active, the `atd*` command (followed by an IP address) can be issued to initiate an outbound client connection to the specified IP address and port as specified after the colon. If no port is specified, the port number used is the Outgoing Port parameter. To hang-up such a connection, 3 “+” characters must be inserted into the outgoing stream (“+++”). The modem will return to command mode once it has seen the “+++” and respond with OK. The connection can then be broken by entering “ath”. The modem will return to server mode. Such a client connection can be repeated again as necessary, as long as each connection is hung-up before a new one is made.

The modem is capable of only 1 PAD connection at a time. When a manual client connection is in progress (`atd*xxx.xxx.xxx.xxx`), a connection attempt by an incoming client may result in the disabling of the PAD function until the next device reset.

### Pad Protocol

Sets the data protocol of the PAD to TCP or UDP data. If you have set PAD Mode as Server, you can choose to support either type of client.

### Incoming Friendly IP Address

Sets the IP address of the device using the PAD functionality.

### Server Session Closed On

This option is only available if PAD mode is Server. This option sets under which condition the server will terminate an established connection. The default setting is New Client.

**NEW CLIENT**—If a different client attempts to connect, it will be successful and the current client will be forcibly disconnected without any warning. Otherwise, the current client remains connected indefinitely.

**TIMEOUT**—A new client is accepted only after a specified timeout. The duration of the timeout is specified by the Inactivity timeout, or the Hard timeout, or a combination of both.

### Server Inactivity Timeout

Time after which the current connection with the client is terminated without warning. This timeout starts over each time the client sends data to the server. This parameter is ignored if the session closes on New Client. If PAD protocol is TCP, the timeout is specified in minutes. If PAD protocol is UDP, the timeout is specified in seconds. The valid range for either is 1-65535. Setting the parameter to 0 will disable this timer.

If both Inactivity Timeout and Hard Timeout are enabled (neither is 0), a client session is terminated when either timeout is met. In this case, the value for Hard Timeout must exceed the value for Inactivity Timeout. If the Inactivity Timeout is met, the client is terminated. If the Hard Timeout is exceeded without meeting the Inactivity Timeout, the client is terminated by the Hard Timeout.

<b>Server Hard Timeout</b>	Time after which the current connection with the client will be terminated without warning. This is a fixed time from the initial connection, no matter how much or how often the client sends data to the server. This parameter is ignored if the session closes on New Client. If PAD protocol is TCP, the timeout is specified in minutes. If UDP, the timeout is specified in seconds. The valid range for either is 1-65535. Setting the parameter to 0 will disable this timer.  If both Inactivity Timeout and Hard Timeout are enabled (neither is 0), a client session is terminated when either timeout is met. In this case, the value for Hard Timeout must exceed the value for Inactivity Timeout. If the Inactivity Timeout is met, the client is terminated. If the Hard Timeout is exceeded without meeting the Inactivity Timeout, the client is terminated by the Hard Timeout.
<b>Incoming Port</b>	Sets the port number used to forward incoming requests to the serial port
<b>Outgoing Port</b>	Sets the port number used to send outgoing requests from the serial port
<b>Remote Host IP Address</b>	Sets the Server IP address to connect with when using the PAD in Client mode.
<b>TCP Client Keep Alive</b>	When in Client mode and enabled, TCP Keep Alive packets are sent from the client to the server periodically in order to detect a broken connection. The modem will automatically try to re-establish the connection if necessary. Changing this setting affects the use of TCP Keep Alive on the next client session. It will not affect an existing session.
<b>TCP Client Keep Alive Time</b>	Time in seconds between keep-alive cycles. A keep alive cycle will consist of one or more keep-alive probes separated by the keep-alive interval.
<b>TCP Client Keep Alive Probes</b>	Number of keep-alive packets that must fail before the connection is considered closed.
<b>TCP Client Keep Alive Intvl</b>	Time (in seconds) after which a keep-alive packet is considered to be failed (if not acknowledged). Another packet is sent at this time if TCP Client Keep Alive Probes limit has not been reached.
<b>PAD Long</b>	When enabled, as data passes through the PAD, a copy is stored in a log file located on the modem at /tmp/padlog. The log will stop saving data when full and data is lost at modem reset.

## 3.8 Diagnostics

Click Diagnostics on the main navigation pane to access the SNMP and Logging pages.

### SNMP

Click SNMP on the Diagnostics page to configure Simple Network Management Protocol (SNMP) functionality. SNMP is used in network management systems to monitor network-attached devices for conditions that warrant administrative attention. SNMP version v2c and v3 are supported, with the exception of INFORM.

Diagnostics	SNMP	Logging	HELP
<b>SNMP Configuration</b>			
SNMP <input type="radio"/> Enable <input checked="" type="radio"/> Disable			
Version <input checked="" type="radio"/> v2c <input type="radio"/> v3			
<b>SNMP v2c</b>			
Read-only Community Name	<input type="text" value="public"/>		
Read-write Community Name	<input type="text" value="private"/>		
<b>SNMP v3</b>			
User Name	<input type="text"/>		
Password	<input type="text"/> (min. 8 char)		
Authentication	<input checked="" type="radio"/> None <input type="radio"/> MD5		
<b>Traps</b>			
<input type="radio"/> Enable <input checked="" type="radio"/> Disable			
Server 1 Address	<input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>		
Server 1 Port	<input type="text" value="162"/> (default: 162)		
Server 2 Address	<input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>		
Server 2 Port	<input type="text" value="162"/> (default: 162)		
Server 3 Address	<input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>		
Server 3 Port	<input type="text" value="162"/> (default: 162)		
Server 4 Address	<input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>		
Server 4 Port	<input type="text" value="162"/> (default: 162)		
<input type="button" value="Download mibs.zip"/> <input type="button" value="Cancel"/> <input type="button" value="Save"/>			

Figure 30 Diagnostics–SNMP

## SNMP Configuration

**SNMP** Selecting “Enable” allows SNMP functionality. Selecting “Disable” turns off SNMP functionality.

**Version** With SNMP enabled, select the corresponding version that matches the SNMP manager.

### SNMP v2c

**Read-only Community Name** The community string used for accessing the read-only Management Information Bases (MIBs).

**Read-write Community Name** The community string used for accessing all Management Information Bases (MIBs) including writable objects.

### SNMP v3

**User Name** The user name for secure access to the Management Information Bases (MIBs) observing v3 standard.

**Password** The corresponding user password for accessing the Management Information Bases (MIBs), including writable objects.

**Authentication** Sets the authentication method for accessing the Management Information Bases (MIBs).

## Traps

<b>Traps</b>	Selecting “Enable” will allow the active trap events to be reported to the defined server(s). Selecting “Disable” deactivates events reporting. Up to four destinations can be specified.
<b>Server Address</b>	IP address of server to which the trap events will be sent.
<b>Server Port</b>	The corresponding server port to which the trap events will be sent (default 162).

## Logging

Click the Logging tab on the Diagnostics page to set up logging in order to capture the current status log of the modem. Log information is useful when contacting ELPRO Technical Support to resolve operational problems.

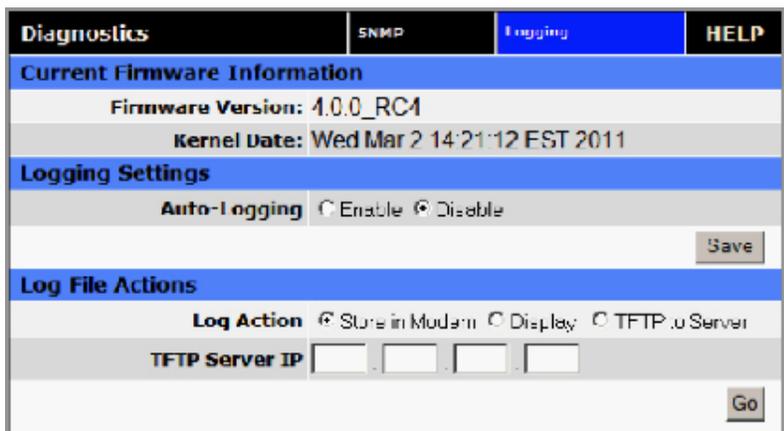


Figure 31 Diagnostics–Logging

### Current Firmware Information

<b>Version</b>	Displays the modem firmware version currently loaded in the unit.
<b>Kernel Date</b>	Displays the date of the operating system kernel the unit is running.

### Logging Settings

**AUTO-LOGGING**—Selecting “Enable” and clicking Save enables the logging capability, which saves periodic and event driven logs to permanent memory. Technical Services personnel may find such logs useful in analyzing field issues. Selecting “Disable” and clicking Save disables the logging capability. This is the default setting. To make best use of available memory it is recommended to only enable the logging capability if it is necessary to help diagnose an issue.

## Log File Actions

### Log Action

There are three available settings:

**STORE IN MODEM**—Selecting “Store in Modem” and clicking Go creates a current status log, and overwrites any previously saved log. This action save a log even if auto-logging is disabled. It is best to save the log immediately following the adverse event, and before any reboot. This log will contain only information collected since the most recent reboot of the device.

**DISPLAY**—Selecting “Display” and clicking Go displays a previously stored log directly to the web browser. You can use your mouse to select the text, and copy and paste it into a text editor to save the log on your computer.

**TFTP TO SERVER**—Selecting “TFTP to Server” and clicking Go initiates a transfer of a previously saved log file to a specified IP address using the TFTP protocol. In order for the transfer to be successful, a reachable IP address must be entered under TFTP Server IP, and the computer at that IP address must be running a TFTP Server program. Many free TFTP Servers are available for download over the Internet. Note that TFTP is different than FTP.

### TFTP Server IP

If you select “TFTP to Server” and click Go, a valid and reachable IP address must be entered here in order to complete the transfer of the saved log file using the TFTP protocol. In order for the transfer to be successful, a reachable IP address must be entered under TFTP Server IP, and the computer at that IP address must be running a TFTP Server program. Many free TFTP Servers are available for download over the Internet. Note that TFTP is different than FTP.

## 3.9 I/O Settings

Click I/O Settings on the main navigation pane to access I/O Status, Settings and Labels pages.

### Status

Click the Status Tab on the I/O Settings page to view the status of the unit’s input and output ports.

I/O Settings	status	Settings	Labels	HELP
<b>Device Input Status</b>				
Main Voltage 12.20 V				
Modem Temperature 105.00 C				
<b>Analog Input Status</b>				
Analog Input 1 0.02 V				
Analog Input 2 0.02 V				
<b>Digital Input Status</b>				
Digital Input 1 Normal				
Digital Input 2 Normal				
<b>Digital Output Status</b>				
Digital Output 1 N/A				
Digital Output 2 N/A				
<b>Relay Output Status</b>				
Relay Output 1 Open				
Relay Output 2 Open				
Refresh				

Figure 32 I/O Settings–Status

**Device Input Status**

- Main Voltage Displays current voltage applied to the unit, in Volts.
- Modem Temperature Displays temperature of the modem, in Celsius.

**Analog Input Status**

- Analog Input 1, Analog Input 2 Displays voltage of the specified analog input, in Volts.

**Digital Input Status**

- Digital Input 1, Digital Input 2 Displays the status of the specified input as Active (high state) or Normal (low state).

**Digital Output Status**

- Digital Output 1, Digital Output 2 Currently Not Available.

**Relay Output Status**

- Relay Output 1, Relay Output 2 Displays the status of the specified output as Open or Closed.

**Settings**

Click the Settings tab on the I/O Settings page to configure NMEA settings. Status Monitoring is provided via NMEA-based protocol. The 615M-1 I/O subsystem operates according to a manager/agent model. The PC-hosted manager sends requests to the 615M-1 I/O agent, which performs the required actions. The 615M-1 agent reports alarms to the PC-hosted manager.

I/O Settings	Status	Settings	Labels	HELP
<b>NMEA Connection</b>				
Manager IP address	<input checked="" type="radio"/> Auto <input type="radio"/> Manual: <input type="text"/> . <input type="text"/> . <input type="text"/> .			
Manager port	6262			
Manager connection type	<input type="radio"/> TCP <input checked="" type="radio"/> UDP			
<b>NMEA Identification</b>				
Unit ID				
Source Identification	<input checked="" type="radio"/> LAN (192.168.1.50) <input type="radio"/> WAN 0			
Source port	6263			
<b>Triggers</b>				
<b>Device</b>				
Cell Temperature	<input type="radio"/> Enable <input checked="" type="radio"/> Disable			
Threshold	Low: 0.0 C    High: 70.0 C			
<b>Analog Input</b>				
Analog Input 1	<input type="radio"/> Enable <input checked="" type="radio"/> Disable			
Threshold	Low: 0.0 V    High: 12.0 V			
Analog Input 2	<input type="radio"/> Enable <input checked="" type="radio"/> Disable			
Threshold	Low: 0.0 V    High: 12.0 V			
<b>Digital Input</b>				
Digital Input 1	<input type="radio"/> Enable <input checked="" type="radio"/> Disable			
Digital Input 2	<input type="radio"/> Enable <input checked="" type="radio"/> Disable			
<input type="button" value="Cancel"/> <input type="button" value="Save"/>				

Figure 33 I/O Settings–Settings

### NMEA Connection

<b>Manager IP address/ port</b>	The IP address and service port of the NMEA server (manager).
<b>Manager connection type</b>	The connection protocol to communicate with the NMEA server (manager).

### NMEA Identification

<b>Unit ID</b>	The unit name to be included in the NMEA message payload.
<b>Source Identification</b>	The unit's IP address that will be included in the NMEA message payload.

### Triggers–Device

<b>Cell Temperature and Thresholds</b>	Enables or disables the NMEA alarm and notification when an analog input goes out of range.
--	---

### Triggers–Analog Input

<b>Analog Input and thresholds (1 or 2)</b>	Enables or disables the NMEA alarm and notification when an analog input goes out of range.
---	---

### Triggers–Digital Input

<b>Digital Input 1, Digital Input 2</b>	Enables or disables the NMEA alarm and notification when the input state changes.
---	---

### NMEA Message Format

This section includes the messages generated by the 615M-1 in response to an alert or acknowledge. These messages will be sent to the manager at the IP address specified.

**Alarm Message Format**

```

$IIALR,hhmmss.ss,xxx,c,s,ip;uid;txt*hh<CR><LF>
hhmmss.ss: NMEA-compliant time (UTC) of initial condition change
xxx: ASCII-encoded hex target descriptor,
    composed of three fields <F1><F2><F3>
<F1> Type of alarm message
    0 Original message for a given alarm
    1 Repetition of an event already reported
    2-F Reserved for future use
<F2> Class of I/O being operated on
    0 Digital input
    1 Analog input
    2 Digital output (contact closure)
    3-F Reserved for future use
<F3> I/O Channel number
    Digital Inputs
        0 Ignition sense
        1 DIN1
        2 DIN2
        3-F Reserved for Future use
    Analog Input
        0 CiPHR input voltage sense
        1 Modem PCB temperature sense
        2 AIN1
        3 AIN2
        4-F Reserved for Future use
    Digital Output
        0 DO1 (COM1/NO1)
        1 DO2 (COM1/NO1)
        2-F Reserved for Future use
c: NMEA-compliant alarm condition
  A = Threshold exceeded (alarm is active)
  V = Threshold not exceeded (indication of return to normal state)
s: NMEA-compliant alarm, acknowledgment state
  V = unacknowledged
ip: User-specified IP address (as configured via the 615M-1 WEB pages)
uid: Free-form text unit identifier (8 characters max)
txt: Free-form alarm/indication text (20 characters max)
hh: NMEA-compliant checksum

```

**Example: Report a temperature-back-in-range indication for the Cell module.**

```
$IIALR,135912.01,011,V,V,172.30.41.9;ADAM12;PCI TEMP NORMAL*FF<CR><LF>
```

**Example: Report a “repeat: digital input #1” alarm.**

```
$IIALR,211545.22,101,A,V,172.30.41.9;ADAM12;MAN DOWN*FF<CR><LF>
```

## ASK Message Format

```
$IIACK,xxx*hh<CR><LF>
```

```
xxx: ASCII-encoded hex target descriptor,
      composed of three fields <F1><F2><F3>
      <F1> Operation being performed
            0    Acknowledging an alarm or opening a digital output
            1    Closing a digital output
            2    Read Request for an input (analog or digital)
            3-F  Reserved for future use

      <F2> Class of I/O being operated on
            0    Digital input
            1    Analog input
            2    Digital output (contact closure)
            3-F  Reserved for future use

      <F3> I/O Channel number
            Digital Inputs
                0    Ignition sense
                1    DIN1
                2    DIN2
                3-F  Reserved for Future use

            Analog Input
                0    615M-1 input voltage sense
                1    Modem PCB temperature sense
                2    AIN1
                3    AIN2
                4-F  Reserved for Future use

            Digital Output
                0    DO1 (COM1/NO1)
                1    DO2 (COM2/NO2)
                2-F  Reserved for Future use

hh: NMEA-compliant checksum
```

**Example: Acknowledge a “Cell module temperature out of range” alarm.**

```
$IIACK,011*FF<CR><LF>
```

## Labels

Click the Labels tab on the I/O Settings page to provide a label for each diagnostic value indicating its normal and abnormal conditions.

I/O Settings	Status	Settings	Labels	HELP	
<b>NMEA Labels</b>					
<b>When In Range</b>					
Cell Temperature	<input type="text" value="CELL TEMP NORMAL"/>				
<b>When Out Of Range</b>					
Cell Temperature	<input type="text" value="CELL TEMP OOR"/>				
<b>Analog Input NMEA Labels</b>					
<b>When In Range:</b>					
Analog Input 1	<input type="text" value="A INPUT 1 NORMAL"/>				
Analog Input 2	<input type="text" value="A INPUT 2 NORMAL"/>				
<b>When Out Of Range</b>					
Analog Input 1	<input type="text" value="A INPUT 1 OOR"/>				
Analog Input 2	<input type="text" value="A INPUT 2 OOR"/>				
<b>Digital Input NMEA Labels</b>					
<b>When Inactive (notify)</b>					
Digital Input 1	<input type="text" value="D INPUT 1 NORMAL"/>				
Digital Input 2	<input type="text" value="D INPUT 2 NORMAL"/>				
<b>When Active (alarm)</b>					
Digital Input 1	<input type="text" value="D INPUT 1 ACTIVE"/>				
Digital Input 2	<input type="text" value="D INPUT 2 ACTIVE"/>				
				<input type="button" value="Cancel"/>	<input type="button" value="Save"/>

Figure 34 I/O Settings–Labels

## 3.10 Firmware Update

Click Firmware Update on the main navigation pane to download current firmware for the unit. When newer versions of the modem firmware become available, you can download the proper file from the Cooper Bussmann web site and manually update the unit by uploading the new firmware. The update file name is: `upgradeevdo.tar.gz` for the 615M-1 modem.

Firmware Update	HELP
<b>Current Firmware Information</b>	
Version: 4.1.0	
Current Kernel Date: Fri Oct 28 16:06:12 EDT 2011	
<b>Upload New Firmware</b>	
File	<input type="button" value="Browse..."/>
Progress	
<i>Note: The upgrade procedure takes approximately 3 minutes.</i>	
<input type="button" value="Upload"/>	
<b>Configuration File</b>	
File	<input type="button" value="Browse..."/>
<input type="button" value="Upload"/>	
<input type="button" value="Save"/>	

Figure 35 Firmware Update

### Current Firmware Information

<b>Version</b>	Displays the modem firmware version currently loaded in the unit.
<b>Kernel Date</b>	Displays the date of the operating system kernel the unit is running.

### Upload New Firmware

<b>File</b>	Enter the update file name, or click Browse to locate the file on your hard drive. Updates can be executed if Remote Administration is enabled.
<b>Progress</b>	Displays the update progress once Save is clicked.
<b>Upload</b>	After selecting the firmware upgrade filename, click Upload to begin the firmware upgrade process.

### Configuration File

<b>File</b>	Enter the name of the uploaded configuration file, or click Browse to locate the file in a specific folder. The file to be uploaded must be named config.xml. If multiple files need to be maintained, it is recommended that separate directories be used. The update can be executed remotely if Remote Administration is enabled.
<b>Upload</b>	After selecting the firmware configuration filename, click Upload to begin the configuration loading process.
<b>Save</b>	Returns a link to the configuration file on the unit. Right-click the link and select "Save Target As..." to save the file. The link page refreshes after 15 seconds. It is recommended that you use the specified filename to save the file. If multiple files need to be maintained, it is recommended that you use directory paths to separate the files.

## CHAPTER 4 - IP ADDRESSING

---

### 4.1 Overview

When 615M-1 cellular router is connected to a cellular carrier, it will always have two IP addresses. The first is the local area network (LAN) address. The 615M-1 can be accessed through either the LAN 1 or LAN 2 Ethernet connectors on the front panel using this IP address. This IP address is user configurable and is saved locally in the 615M-1. The factory default IP address is 192.168.1.50, with a subnet mask of 255.255.255.0.

The second 615M-1 IP address is assigned by the cellular carrier each time the 615M-1 connects to the cellular network. Often this IP address is publicly accessible from the Internet. However, in some instances the cellular carrier may assign an IP address that is protected by firewalls. When a publicly accessible IP address is assigned, data flows can be initiated from either the 615M-1 or from the Internet. When an IP address is protected by cellular firewalls, data flows can only be initiated from the 615M-1. In either case, after a data flow has been established, data is free to move in both directions.

### 4.2 IP Addressing Tutorial

The default LAN subnet of the 615M-1 consists of addresses from 192.168.1.0 to 192.168.1.255. The first and last IP address a subnet is always reserved, no matter the subnet size. The first IP address in the subnet is the Network ID. The last IP address in the subnet is the Broadcast Address.

The following example illustrates a sample 615M-1 network. The subnet consists of IP addresses ranging from 192.168.1.0 to 192.168.1.255. The subnet mask is 255.255.255.0. This is sometimes written in shorthand notation as: 192.168.1.50/24 since the subnet mask 255.255.255.0 contains 24 ones then 8 zeros when it is converted to binary.

The first address 192.168.1.0 is reserved for the Network ID. The last address 192.168.1.255 is reserved for the broadcast address. There are 254 valid IP addresses that may be assigned to hosts on the LAN network.

Ethernet Subnet Mask	255.255.255.0	
Network ID	192.168.1.0	(reserved—first IP address in subnet)
Broadcast Address:	192.168.1.255	(reserved—last IP address in subnet)
615M-1	192.168.1.50/24	
PLC/RTU #1	192.168.1.10/24	
Computer #1	192.168.1.125/24	

By changing the subnet mask, the network can be made to include as many or as few IP addresses as desired. Ethernet devices can only communicate directly to other devices that have IP addresses within the same IP subnet. For example, Computer #1 in the example above can only communicate with locally connected devices that have IP addresses between 192.168.1.1 and 192.168.1.254. When Computer #1 wants to communicate with another server on the Internet, it sends its data packet to the local gateway. In this case, the local gateway is the 615M-1 router. Since the 615M-1 has two IP addresses (each IP address is on a separate subnet), it can forward the packet from the LAN network (192.168.1.0/24) to the cellular network. The packet will continue to be forwarded in a similar fashion from subnet to subnet until it reaches its final destination.

### 4.3 Private vs. Public IP Addresses

Certain address ranges in the IPv4 address space have been reserved as private IP address. Private IP addresses can be used by anyone, without the need to register for an IP address assignment from the Internet Assigned Numbers Authority (IANA). However, private IP addresses are not routable on the Internet. Routers on the Internet will typically drop any packets that are destined for a private IP address. These addresses are reserved for local use only.

Common Private IP Address Ranges:

- 10.0.0.0 to 10.255.255.255
- 172.16.0.0 to 172.31.255.255
- 192.168.0.0 to 192.168.255.255

Devices using Private IP addresses must have a router with Network Address Translation (NAT) capability to access the Internet. By default, the 615M-1 will perform the NAT function on all outgoing traffic. The 615M-1 radio will change the source IP address from the private IP of the local host to the public IP address for the 615M-1 which was assigned by the cellular carrier. Since the outgoing packet has been modified, a remote server or website on the Internet will think the packet came directly from the 615M-1 radio. It will reply back to the cellular IP address of the 615M-1. The 615M-1 radio remembers which traffic flows have been established and routes the incoming return traffic back to the desired host device on the local area network.

### 4.4 Port Forwarding

NAT functionality is only useful for traffic flows that are initiated by the 615M-1 or by a device that is physically connected to the 615M-1. Port forwarding can be enabled to allow remote devices connecting through the Internet to initiate traffic flows with a local device connected to a 615M-1 router.

In the example configuration shown below, a host from the Internet can create either a TCP or UDP connection with the local host at 192.168.1.250 on port 7000 by sending a packet to the cellular IP address of the 615M-1 radio at port 8010. When the 615M-1 radio receives a packet destined for port 8010 it will look through the Port Forwarding table to see if a matching rule exists. It finds the rule that instructs it to forward this packet to port 7000 of IP address 192.168.1.250. The 615M-1 then modifies the destination IP address and port number before forwarding the packet on to the local area network.

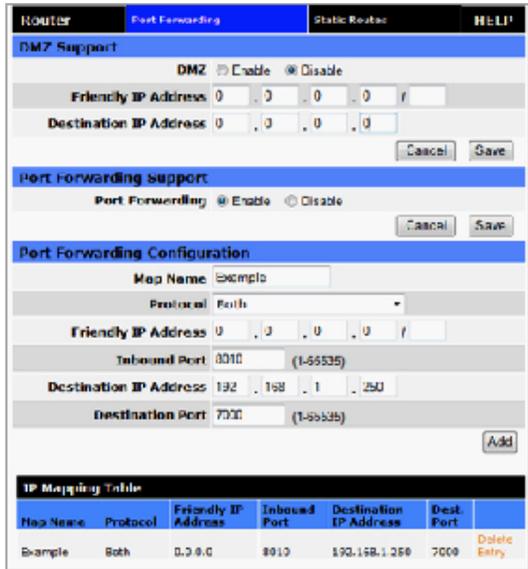


Figure 36 Port Forwarding Example

Port forwarding is essential for field applications that use polling initiated by a polling master. The port forwarding function allows the polling master to establish a data connection through the Internet. The incoming polling message is forwarded by the 615M-1 to the appropriate PLC or RTU on the 615M-1’s local area network.

### 4.5 DMZ

Alternately, DMZ can be enabled on the 615M-1 radio. When DMZ is enabled, all traffic received from the Internet and destined to the 615M-1’s cellular IP address is forwarded to the DMZ host. The IP address of the DMZ host is specified by the user. Using DMZ can eliminate the need to specify many individual port forwarding rules. However, by exposing all the ports on the local device, the local device may become more susceptible to attacks.

If specific Port Forwarding rules exist in the IP Mapping Table, these rules take precedence over the DMZ host.

## 4.6 Friendly IP Address

Friendly IP addresses can be used with either port forwarding or DMZ to provide an additional layer of security. When Friendly IP addresses are used, the 615M-1 will only forward packets to the LAN if the source IP address of the received packet matches either the specific IP address or range of IP addresses specified in the Friendly IP address field.

 This feature can be disabled by entering 0.0.0.0 in the friendly IP address field. In this case, packets from any host on the Internet can be forwarded to the LAN when either DMZ or Port Forwarding is enabled.

## CHAPTER 5 - IPSEC AND VPN PASS-THROUGH DEPLOYMENT GUIDE

This chapter provides information on building a secure IP network using IPsec and the ELPRO 615M-1 Cellular Modem. Two configuration scenarios are provided. The first scenario demonstrates the 615M-1 when used as an IPsec client. The second scenario shows the 615M-1 passing an IPsec connection from WAN to LAN (VPN pass-through). Detailed configuration examples are provided for each scenario.

### 7.1 Benefits of IPsec

Internet Protocol Security Standard (IPsec) is an industry driven standard that ensures confidentiality, integrity, and authenticity of an IP network. IPsec is a key component of this standard-based, flexible solution for deploying a network-wide policy.

There are two significant benefits to IPsec compliance for our customers—enhanced security features and interoperability.

- Enhanced security features give our customers the comfort of knowing that IP based communications are using the most secure and comprehensive standard available today for encryption and authentication.

The 615M-1 IPsec encryption support: AES-128, AES-256 and 3DES

The 615M-1 IPsec authentication support: MD5 and SHA1

All tunnels are created using the ESP (Encapsulating Security Payload) protocol.

- Protocol interoperability means that an IPsec-compliant device, such as the 615M-1, will be able to exchange keys and encrypted communications with another IPsec-compliant product such as a Cisco™ router. IPsec compliance ensures that these two different products can negotiate and maintain a secure communication with each other.

### 7.2 615M-1 Configured IPsec Client

In the following configuration examples, the 615M-1 is used as an IPsec Client to connect to a Cisco Router acting as a VPN server.

Where:

REMOTE SUBNET: 10.100.0.0/21

FIREWALL EXTERNAL IP (REMOTE IP): A.B.C.D

615M-1 PPP IP (LOCAL IP): W.X.Y.Z

LOCAL SUBNET: 10.100.10.0/24

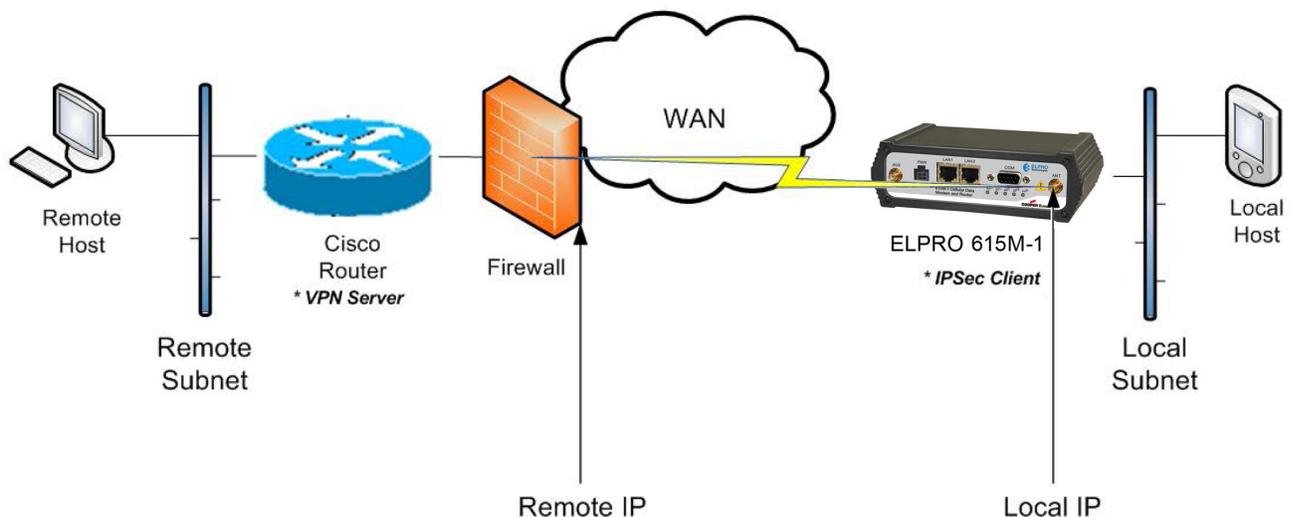


Figure 37 615M-1 Configured IPSEC Client

**Cisco Router-VPN Server Configuration**

```

!
crypto isakmp policy 2
  encr 3des
  authentication pre-share
  group 2
crypto isakmp key D3m0$K3y!2H3rk address W.X.Y.Z
!
crypto ipsec transform-set esp3dessha1 esp-3des esp-sha-hmac
crypto ipsec df-bit clear
!
crypto map ETH0 10010 ipsec-isakmp
  description ELPRO
  set peer W.X.Y.Z
  set transform-set esp3dessha1
  match address V1-ELPRO
  qos pre-classify
!
interface FastEthernet4
  ip address A.B.C.D 255.255.255.248
  ip access-group INET-ACL in
  load-interval 30
  duplex auto
  speed auto
  no cdp enable
  crypto map ETH0
!
!
ip access-list extended INET-ACL
  remark z-----
  permit esp any any
  permit udp any any eq isakmp
  permit icmp any any echo
  permit icmp any any echo-reply
  deny ip any any
  remark z-----
ip access-list extended V1-ELPRO
  remark z-----
  permit ip 10.100.0.0 0.0.7.255 10.100.10.0 0.0.0.255
  remark z-----

```

**615M-1-IPSEC Client Configuration**

When the IPsec tunnel is established between the 615M-1 and the Cisco, all the IP Packets coming from 10.100.0.0/21 to 10.100.10.0/24 and vice-versa will pass through the IPsec VPN tunnel.

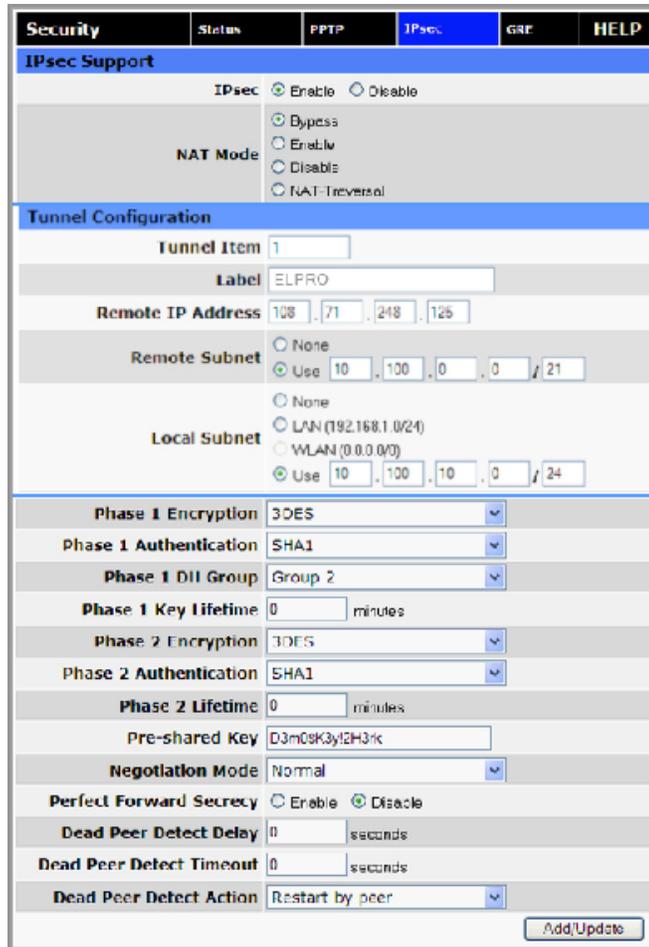


Figure 38 615M-1-IPSec Client Configuration Example

### 7.3 615M-1 Configured VPN Pass-through

The following configuration example uses the 615M-1 as an IPsec pass-through between two Cisco routers.

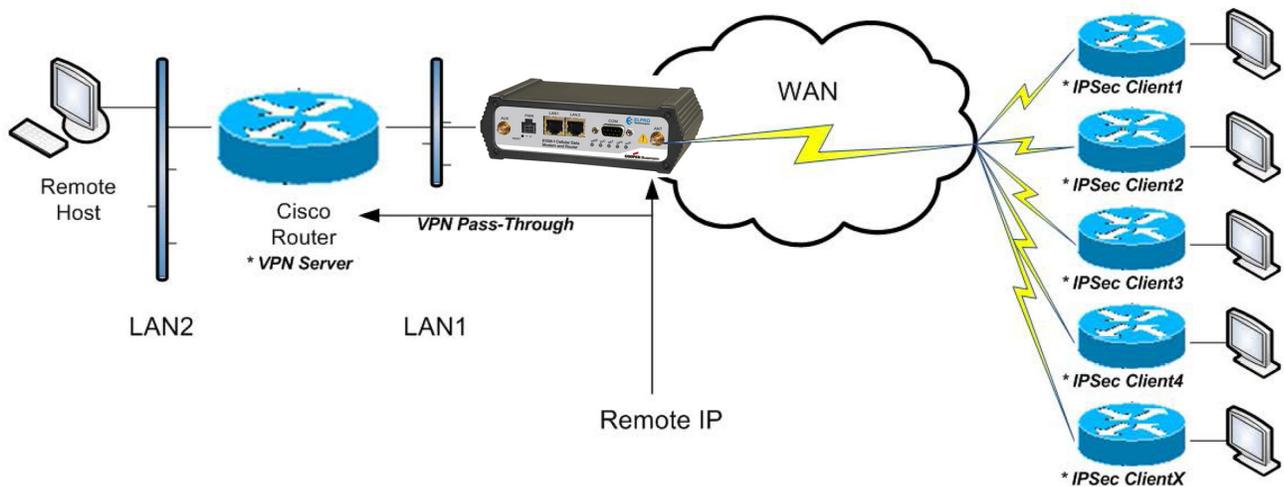


Figure 39 615M-1 Configured VPN Pass-through

### 615M-1-VPN Pass-Through Configuration

Using this scenario, the 615M-1 is acting a pass-through to the VPN connection. Apply these parameters changes into the 615M-1.

1. From the main navigation pane, click LAN.
2. On the LAN page, click the LAN Settings tab.
3. Disable the “LAN Masquerade” option and click Save.

LAN	LAN Settings	MAC Filtering	IP Filtering	HELP
<b>LAN Settings</b>				
Ethernet IP Address	192	168	1	50
Ethernet Subnet Mask	255	255	255	0
LAN Masquerade	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable		
Bind Services to Eth IP	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable		
				Cancel Save

Figure 40 LAN Settings

4. From the main navigation pane, click Router.
5. On the Router page, click the Port Forwarding tab.
6. Enable the “DMZ” option.
7. Enter the following for Friendly IP Address and Destination IP address:  
 Friendly IP Address = 0.0.0.0  
 Destination IP Address = Cisco Router (VPN server) LAN1 IP Address
8. Click Save.

 **NOTE** You can use port forwarding instead of DMZ to configure the VPN Pass-through.

Router	Port Forwarding	Static Routes	HELP
<b>DMZ Support</b>			
DMZ <input checked="" type="radio"/> Enable <input type="radio"/> Disable			
Friendly IP Address	0	0	0 / 0
Destination IP Address	192	168	1 . 100
Cancel Save			

Figure 41 Port Forwarding

## CHAPTER 8 - USER I/O PORT

The 615M-1 has a 10-pin connector on the back panel that can be used for general purpose analog inputs and digital input/outputs. The connector also provides access to two internal mechanical relays.

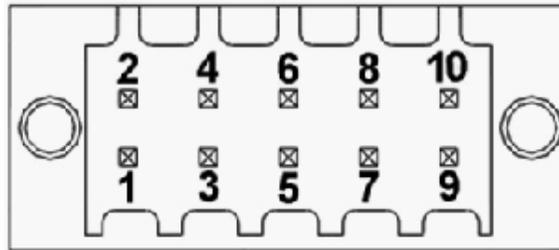


Figure 42 10-pin Connector

Table 10 Connector Pin Out

Pin Number	Name	Notes
1	NO 1	Normally Open Terminal of Relay #1
2	COM 1	Common Terminal of Relay #1
3	NO 2	Normally Open Terminal of Relay #2
4	COM 2	Common Terminal of Relay #2
5	Digital I/O 1	
6	Digital I/O 2	
7	Analog Ground	Analog and Digital Ground have different ground planes internally. They are connected internally at one point only.
8	Digital Ground	
9	Analog Input 1	
10	Analog Input 2	

Table 11

Symbol	Parameter	Min	Typ	Max	Units
<b>Digital Inputs</b>					
VIN	Digital Voltage Recommended Input Range	0		5.5	V
VP	Positive Threshold Voltage for Digital Inputs		1.8	2.3	V
VN	Negative Threshold Voltage for Digital Inputs	0.7	1.1		V
VH	Hysteresis Voltage for Digital Inputs		0.7		V
<b>Digital Outputs</b>					
VOH	High Level Output Voltage IOH = -10uA IOH = -100uA		3.1 1.4		V V
VOL	Low Level Output Voltage IOL = 100uA IOL = 1mA IOL = 10mA		0.2 0.3 1.2		V V V

Symbol	Parameter	Min	Typ	Max	Units
RPU	Pull Up Resistance		18.2		kΩ
RPD	Pull Down Resistance		100		Ω
Analog Inputs					
VIN	Analog Voltage Recommended Input Range	0		30	V
Accuracy			+/- 0.2		V
Relays					
VDiff	Recommended Differential Voltage Range Between NO and COM Terminals	-30		30	V
ISwitch	Switching Current			1	A
RInitial	Initial Contact Resistance			100	mΩ
ROpen	Pass Through Resistance when Contacts are Open.		1000		kΩ
Expected Life	1A, 30VDC, 20 Cycles per Minute	105			Cycles

### 8.1 Circuit for Analog Inputs

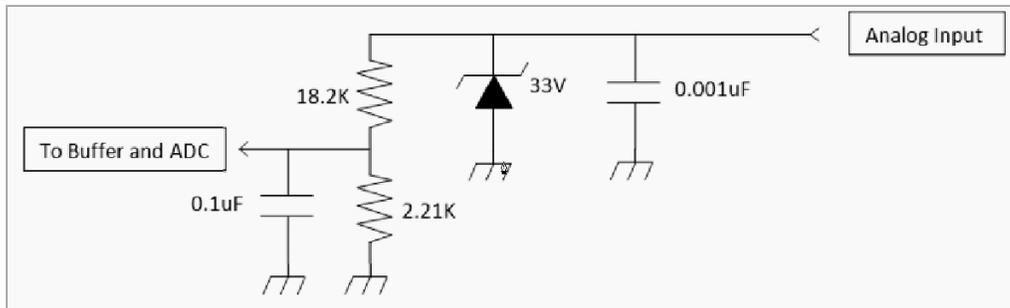


Figure 43 Circuit for Analog Inputs

### 8.2 Simplified Circuit for Digital Input/Outputs

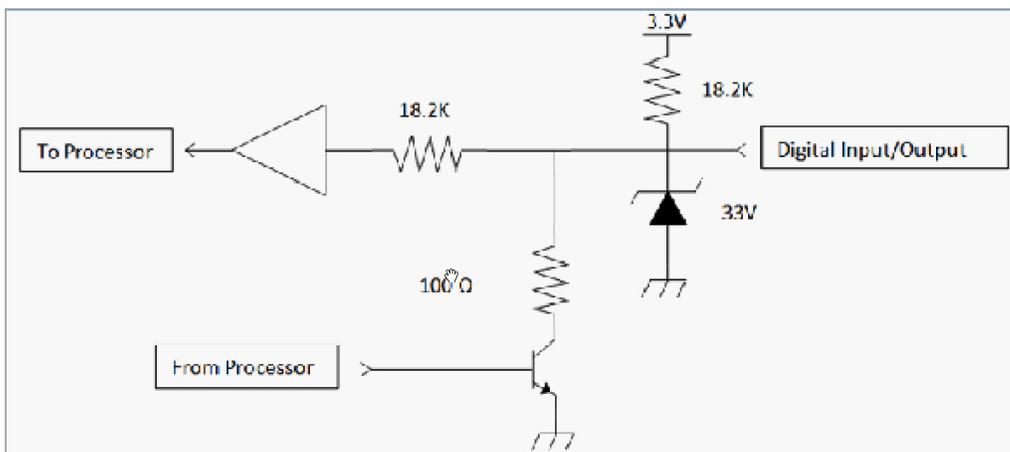


Figure 44 Circuit for Digital Inputs/Outputs

### 8.3 Simplified Circuit for Mechanical Relays

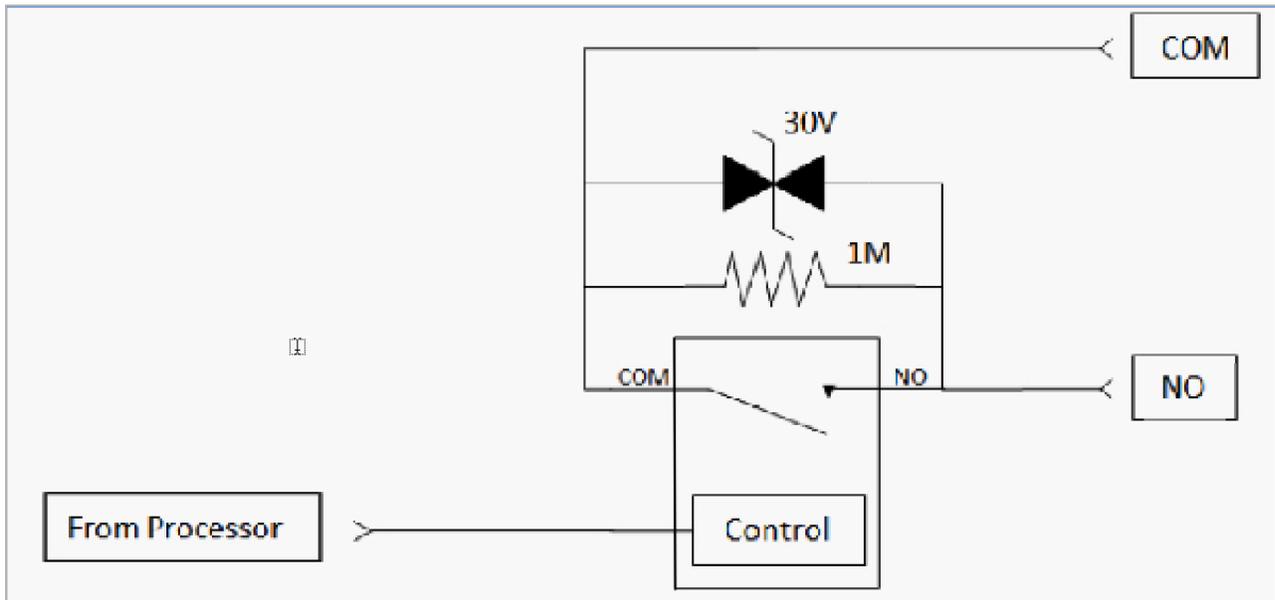


Figure 45 Circuit for Mechanical Relays

### 8.4 Inserting Wires into User Port Connector

Insert a small flathead screwdriver into the insertion slot to open the terminal. Insert wire and remove screwdriver (Figure 46).

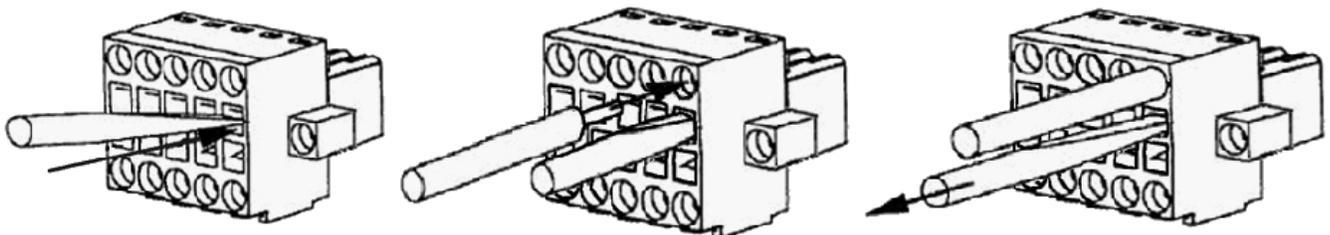


Figure 46 Inserting Wires into User Port Connector

## APPENDIX A - GLOSSARY

Term	Definition
<b>APN, Access Point</b>	Access Point Name (APN). An access point connects wireless network stations (or clients) to other stations within the wireless network and also can serve as the point of interconnection between the wireless network and a wired network. Each access point can serve multiple users within a defined network area. Also known as a base station.
<b>AWG</b>	American wire gauge (AWG), also known as the Brown & Sharpe wire gauge, is a standardized wire gauge system used predominantly in the United States and Canada for the diameters of round, solid, nonferrous, electrically conducting wire.
<b>Bandwidth</b>	The maximum data transfer speed available to a user through a network.
<b>CDMA</b>	Code division multiple access (CDMA) is a channel access method used by various radio communication technologies in which the transmitter encodes the signal using a pseudo-random sequence that the receiver also knows and can use to decode the received signal. Each different random sequence corresponds to a different communications channel.
<b>CTS</b>	Clear To Send. In serial communications, a signal sent, as from a modem to its computer, to indicate that transmissions can proceed.
<b>DCD</b>	Data Carrier Detected. A control signal in serial communications that is sent between a computer and another device, such as a modem, to indicate that the device is ready for transmitting.
<b>DCE</b>	Data communications equipment (DCE) is a device that sits between the data terminal equipment (DTE) and a data transmission circuit. Usually, the DTE device is the terminal (or computer), and the DCE is a modem.
<b>DTE</b>	Data terminal equipment (DTE) is an end instrument that converts user information into signals or reconverts received signals. These can also be called tail circuits. A DTE device communicates with the data circuit-terminating equipment (DCE).
<b>DHCP</b>	Dynamic Host Configuration Protocol is a utility that enables a server to dynamically assign IP addresses from a predefined list and limit their time of use so that they can be reassigned. Without DHCP, an IT manager would need to manually enter in all the IP addresses of all the computers on the network. If DHCP is used, whenever a computer logs onto the network, it automatically gets an IP address assigned to it.
<b>DNS</b>	Domain Name Service is a program that translates URLs to IP addresses by accessing a database maintained on a collection of Internet servers. The program works behind the scenes to facilitate surfing the Web with alpha versus numeric addresses. A DNS server converts a name like mywebsite.com to a series of numbers like 107.22.55.26. Every website has its own specific IP address on the Internet.
<b>EDGE</b>	Enhanced Data rates for GSM Evolution (EDGE), also known as Enhanced GPRS (EGPRS), or IMT Single Carrier (IMT-SC), or Enhanced Data rates for Global Evolution) is a digital mobile phone technology that allows improved data transmission rates as a backward-compatible extension of GSM.
<b>EVDO</b>	Enhanced Voice-Data Optimized (EVDO) is a telecommunications standard for the wireless transmission of data through radio signals, typically for broadband Internet access. It uses multiplexing techniques including code division multiple access (CDMA) as well as time division multiplexing (TDM) to maximize both individual users' throughput and the overall system throughput.
<b>Firewall</b>	A device or computer program that keeps unauthorized users out of a private network. Everything entering or leaving a system's internal network passes through the firewall and must meet the system's security standards in order to be transmitted. Often used to keep unauthorized people from using systems connected to the Internet.
<b>FTP</b>	File Transfer Protocol (FTP) is a standard network protocol used to transfer files from one host to another host over a TCP-based network, such as the Internet.

## Cooper Bussmann 615M-1 Cellular Data Modem and IP Router Series Manual

Term	Definition
<b>GPRS</b>	General packet radio service (GPRS) is a packet oriented mobile data service on the 2G and 3G cellular communication system's global system for mobile communications (GSM).
<b>GPS</b>	The Global Positioning System (GPS) is a space-based satellite navigation system that provides location and time information in all weather conditions, anywhere on or near the Earth where there is an unobstructed line of sight to four or more GPS satellites.
<b>GSM</b>	Global System for Mobile Communications (GSM) is a standard set developed by the European Telecommunications Standards Institute (ETSI) to describe protocols for second generation (2G) digital cellular networks used by mobile phones.
<b>Hz</b>	Hertz. The international unit for measuring frequency, equivalent to the older unit of cycles per second. One megahertz (MHz) is one million hertz. One gigahertz (GHz) is one billion hertz. The standard US electrical power frequency is 60 Hz, the AM broadcast radio frequency band is 535–1605 kHz, the FM broadcast radio frequency band is 88–108 MHz, and wireless 802.11b/g LANs operate at 2.4 GHz.
<b>HSDPA</b>	High-Speed Downlink Packet Access (HSDPA) is an enhanced 3G (third generation) mobile telephony communications protocol in the High-Speed Packet Access (HSPA) family, also dubbed 3.5G, 3G+ or turbo 3G, which allows networks based on Universal Mobile Telecommunications System (UMTS) to have higher data transfer speeds and capacity. Current HSDPA deployments support down-link speeds of up to 42 Mbit/s.
<b>HSPA</b>	High Speed Packet Access (HSPA) is an amalgamation of two mobile telephony protocols, High Speed Downlink Packet Access (HSDPA) and High Speed Uplink Packet Access (HSUPA), that extends and improves the performance of existing 3rd generation mobile telecommunication networks utilizing the WCDMA protocols.
<b>HSUPA</b>	High-Speed Uplink Packet Access (HSUPA) is a 3G mobile telephony protocol in the HSPA family with up-link speeds up to 5.76 Mbit/s.
<b>HTTP</b>	The Hypertext Transfer Protocol (HTTP) is an application protocol for distributed, collaborative, hypermedia information systems, and is the foundation of data communication for the World Wide Web. Hypertext is a multi-linear set of objects, building a network by using logical links (the so-called hyperlinks) between the nodes (text or words). HTTP is the protocol to exchange or transfer hypertext.
<b>IANA</b>	The Internet Assigned Numbers Authority (IANA) is the entity that oversees global IP address allocation, autonomous system number allocation, root zone management in the Domain Name System (DNS), media types, and other Internet Protocol-related symbols and numbers.
<b>ICMP</b>	The Internet Control Message Protocol (ICMP) is one of the core protocols of the Internet Protocol Suite. It is used by the operating systems of networked computers to send error messages indicating, for example, that a requested service is not available or that a host or router could not be reached. ICMP can also be used to relay query messages. It is assigned protocol number 1.
<b>IEEE</b>	Institute of Electrical and Electronics Engineers, New York, <a href="http://www.ieee.org">www.ieee.org</a> . A membership organization that includes engineers, scientists and students in electronics and allied fields. It has more than 300,000 members and is involved with setting standards for computers and communications.
<b>IMEI</b>	The International Mobile Station Equipment Identity (IMEI) is a number, usually unique, to identify 3GPP and iDEN mobile phones, as well as some satellite phones. It is usually found printed inside the battery compartment of the phone, but can also be displayed on-screen.
<b>IMSI</b>	The International Mobile Subscriber Identity (IMSI) is a unique identification associated with all cellular networks. It is stored as a 64 bit field and is sent by the phone to the network. It is also used for acquiring other details of the mobile in the home location register (HLR) or as locally copied in the visitor location register. To prevent eavesdroppers identifying and tracking the subscriber on the radio interface, the IMSI is sent as rarely as possible and a randomly generated TMSI is sent instead.
<b>I/O</b>	Input / Output. The term used to describe any operation, program or device that transfers data to or from a computer.

Term	Definition
<b>IP</b>	Internet protocol. A set of rules used to send and receive messages across local networks and the Internet.
<b>IP Address</b>	A 32-bit number that identifies each sender or receiver of information that is sent across the Internet. An IP address has two parts: an identifier of a particular network on the Internet and an identifier of the particular device (which can be a server or a workstation) within that network.
<b>IPsec</b>	Internet Protocol Security (IPsec) is a 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.
<b>LAN</b>	Local Area Network. A system of connecting PCs and other devices within the same physical proximity for sharing resources such as an Internet connections, printers, files and drives.
<b>LED</b>	A light-emitting diode (LED) is a semiconductor light source. LEDs are used as indicator lamps in many devices.
<b>Receive Sensitivity</b>	The minimum signal strength required to pick up a signal. Higher bandwidth connections usually have less receive sensitivity than lower bandwidth connections.
<b>Router</b>	A device that forwards data from one WLAN or wired local area network to another.
<b>Transmit Power</b>	The power (usually expressed in mW or dBm) at which the wireless device transmits.
<b>MAC Address</b>	Media Access Control address. A unique code assigned to most forms of networking hardware. The address is permanently assigned to the hardware. Limiting a wireless network's access to hardware, such as wireless cards, is a security feature employed by closed wireless networks. However, an experienced hacker armed with the proper tools can still figure out an authorized MAC address, masquerade as a legitimate address, and access a closed network.  Every wireless 802.11 device has its own specific MAC address hard-coded into it. This unique identifier can be used to provide security for wireless networks. When a network uses a MAC table, only 802.11 radios that have had their MAC addresses added to that network's MAC table will be able to get onto the network.
<b>MDIX</b>	A Medium Dependent Interface (MDI) describes the interface (both physical and electrical) in a computer network from a physical layer implementation to the physical medium used to carry the transmission. Ethernet over twisted pair also defines a medium dependent interface crossover (MDIX) interface. Auto-MDIX ports on newer network interfaces detect if the connection would require a crossover, and automatically chooses the MDI or MDIX configuration to properly match the other end of the link.
<b>MEID</b>	A mobile equipment identifier (MEID) is a globally unique number identifying a physical piece of CDMA mobile station equipment. An MEID is 56 bits long (14 hex digits). It consists of three fields, including an 8-bit regional code (RR), a 24-bit manufacturer code, and a 24-bit manufacturer-assigned serial number. The check digit (CD) is not considered part of the MEID.
<b>MS</b>	A mobile station (MS)[ comprises all user equipment and software needed for communication with a mobile network.
<b>NAT</b>	Network Address Translation. A network capability that enables a number of computers to dynamically share a single incoming IP address from a dial-up, cable or xDSL connection. NAT takes the single incoming IP address and creates new IP address for each client computer on the network.
<b>NID</b>	A Network Interface Device (NID) is a device that serves as the demarcation point between the carrier's local loop and the customer's premises wiring.
<b>NIMEA</b>	National Marine Electronics Association (NMEA) is a combined electrical and data specification for communication between marine electronic devices such as echo sounder, sonars, anemometer, gyrocompass, autopilot, GPS receivers and many other types of instruments. It has been defined by, and is controlled by, the U.S.-based National Marine Electronics Association.
<b>NTP</b>	Network Time Protocol (NTP) is a networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks.

## Cooper Bussmann 615M-1 Cellular Data Modem and IP Router Series Manual

Term	Definition
<b>OMA-DM</b>	OMA Device Management is a device management protocol designed for management of small mobile devices such as mobile phones, PDAs and palm top computers.
<b>OTA, OTASP</b>	Over-the-air programming (OTA) refers to various methods of distributing new software updates or configuration settings to devices like cellphones and set-top boxes. In the mobile content world these include over-the-air service provisioning (OTASP), over-the-air provisioning (OTAP) or over-the-air parameter administration (OTAPA), or provisioning handsets with the necessary settings with which to access services.
<b>PDP</b>	The packet data protocol (PDP) context is a data structure present on both the serving GPRS support node and the gateway GPRS support node which contains the subscriber's session information when the subscriber has an active session.
<b>PLC</b>	A Programmable Logic Controller (PLC) is a digital computer used for automation of electro-mechanical processes, such as control of machinery on factory assembly lines, amusement rides, or light fixtures.
<b>PPP</b>	The Point-to-Point Protocol (PPP) is a data link protocol commonly used in establishing a direct connection between two networking nodes. It can provide connection authentication, transmission encryption (using ECP, RFC 1968), and compression.
<b>PPTP</b>	The Point-to-Point Tunneling Protocol (PPTP) is a method for implementing virtual private networks. PPTP uses a control channel over TCP and a GRE tunnel operating to encapsulate PPP packets. The PPTP specification does not describe encryption or authentication features and relies on the Point-to-Point Protocol being tunneled to implement security functionality.
<b>PRL</b>	The Preferred Roaming List (PRL) is a database residing in a wireless (primarily CDMA) device, such as a cellphone, that contains information used during the system selection and acquisition process. Without a PRL, the device may not be able to roam (obtain service outside of the home area).
<b>RJ-45</b>	Standard connectors used in Ethernet networks. RJ-45 connectors are similar to standard RJ-11 telephone connectors, except that RJ-45 connectors can have up to eight wires, whereas telephone connectors have four wires.
<b>RSSI</b>	Received signal strength indicator (RSSI) is a measurement of the power present in a received radio signal. In an IEEE 802.11 system, RSSI is the relative received signal strength in a wireless environment, in arbitrary units. RSSI is an indication of the power level being received by the antenna. Therefore, the higher the RSSI number (or less negative in some devices), the stronger the signal.
<b>RTT</b>	The round-trip time (RTT) is the length of time it takes for a signal to be sent plus the length of time it takes for an acknowledgment of that signal to be received. This time delay therefore consists of the transmission times between the two points of a signal. In the context of computer networks, the signal is generally a data packet, and the RTT is also known as the ping time. An Internet user can determine the RTT by using the ping command.
<b>RTU</b>	A remote terminal unit (RTU) is a microprocessor-controlled electronic device that interfaces objects in the physical world to a distributed control system or SCADA (supervisory control and data acquisition) system by transmitting telemetry data to a master system, and by using messages from the master supervisory system to control connected objects.
<b>Rx</b>	Receive.
<b>Server</b>	A computer that provides its resources to other computers and devices on a network. These include print servers, Internet servers and data servers. A server can also be combined with a hub or router.
<b>SID</b>	System identity codes (SID) are assigned to every carrier (for example, Verizon, Sprint, Alltel) by national regulators. SIDs are programmed into the phone when you purchase them. A phone will maintain a list of "preferred" systems identified by their SID code.
<b>SIM</b>	A subscriber identity module (SIM) is an integrated circuit that securely stores the international mobile subscriber identity (IMSI) and the related key used to identify and authenticate subscribers on mobile telephony devices, such as mobile phones and computers. A SIM is embedded into a removable SIM card that can be transferred between different mobile devices.
<b>Sub Network or Subnet</b>	Found in larger networks, these smaller networks are used to simplify addressing between numerous computers. Subnets connect together through a router.

Term	Definition
<b>Switch</b>	A type of hub that efficiently controls the way multiple devices use the same network so that each can operate at optimal performance. A switch acts as a networks traffic cop. Rather than transmitting all the packets it receives to all ports as a hub does, a switch transmits packets to only the receiving port.
<b>TCP</b>	Transmission Control Protocol. A protocol used along with the Internet Protocol (IP) to send data in the form of individual units (called packets) between computers over the Internet. While IP takes care of handling the actual delivery of the data, TCP takes care of keeping track of the packets that a message is divided into for efficient routing through the Internet. For example, when a web page is downloaded from a web server, the TCP program layer in that server divides the file into packets, numbers the packets, and then forwards them individually to the IP program layer. Although each packet has the same destination IP address, it may get routed differently through the network. At the other end, TCP reassembles the individual packets and waits until they have all arrived to forward them as single message.
<b>TCP/IP</b>	The underlying technology behind the Internet and communications between computers in a network. The first part, TCP, is the transport part, which matches the size of the messages on either end and guarantees that the correct message has been received. The IP part is the user's computer address on a network. Every computer in a TCP/IP network has its own IP address that is either dynamically assigned at startup or permanently assigned. All TCP/IP messages contain the address of the destination network as well as the address of the destination station. This enables TCP/IP messages to be transmitted to multiple networks (subnets) within an organization or worldwide.
<b>TFTP</b>	Trivial File Transfer Protocol (TFTP) is a file transfer protocol notable for its simplicity. It is generally used for automated transfer of configuration or boot files between machines in a local environment.
<b>UDP</b>	The User Datagram Protocol (UDP) is one of the core members of the Internet protocol suite, the set of network protocols used for the Internet. With UDP, computer applications can send messages, in this case referred to as datagrams, to other hosts on an Internet Protocol (IP) network without prior communications to set up special transmission channels or data paths.
<b>UMTS</b>	The Universal Mobile Telecommunications System (UMTS) is a third generation mobile cellular system for networks based on the GSM standard.
<b>UTC</b>	Coordinated Universal Time (UTC) is the primary time standard by which the world regulates clocks and time. It is one of several closely related successors to Greenwich Mean Time (GMT). For most purposes, UTC is synonymous with GMT.
<b>VPN</b>	Virtual Private Network (VPN) is a type of technology designed to increase the security of information transferred over the Internet. VPN can work with either wired or wireless networks, as well as with dial-up connections over POTS. VPN creates a private encrypted tunnel from the end user's computer, through the local wireless network, through the Internet, all the way to the corporate servers and database.
<b>WAN</b>	Wide Area Network. A communication system of connecting PCs and other computing devices across a large local, regional, national or international geographic area. Also used to distinguish between phone-based data networks and Wi-Fi. Phone networks are considered WANs and Wi-Fi networks are considered Wireless Local Area Networks (WLANs).
<b>Wi-Fi</b>	Wireless Fidelity. An interoperability certification for wireless local area network (LAN) products based on the Institute of Electrical and Electronics Engineers (IEEE) 802.11 standard.



## Customer Assistance

### Technical Support:

United States: +1 866 713 4409

Australasia.: +61 7 3352 8624

Other: +1 604 944 9247

Email: [ELPRO-Support@cooperindustries.com](mailto:ELPRO-Support@cooperindustries.com)

Website: [www.cooperbussmann.com/wireless](http://www.cooperbussmann.com/wireless)

Australasia Fax: +61 7 33528677

US Fax: +1 925 924 8502

### Online Resources

Visit [www.cooperbussmann.com/wirelessresources](http://www.cooperbussmann.com/wirelessresources) for the following resources and more:

- User Manuals
- Installation Guides
- Configuration Software
- Datasheets
- Dimensional Drawings



## North America & Latin America

5735 W. Las Positas Suite 100

Pleasanton, California 94588 USA

Telephone: +1 925 924 8500

[elpro-sales@cooperindustries.com](mailto:elpro-sales@cooperindustries.com)

## Australia, New Zealand

Cooper Technology Centre

Suite 2.01, Quad 2, 8 Parkview Drive

Sydney Olympic Park, NSW, 2127, AUSTRALIA

Telephone: +61 2 8787 2777

[elpro-sales@cooperindustries.com](mailto:elpro-sales@cooperindustries.com)

## China

955 Shengli Road

East Area of Zhangjiang High-Tech Park

Shanghai, 201201, CHINA

Telephone: +86 21 2899 3600

[elpro-sales@cooperindustries.com](mailto:elpro-sales@cooperindustries.com)

## Southeast Asia

2 Serangoon North Avenue 5

# 06-01 Fu Yu Building, 554911, SINGAPORE

Telephone: +65 6645 9888

[elpro-sales@cooperindustries.com](mailto:elpro-sales@cooperindustries.com)

©2013 Cooper Bussmann  
[www.cooperbussmann.com/wireless](http://www.cooperbussmann.com/wireless)

Your Authorized Cooper Bussmann Distributor is:



The trade names and brand names contained herein are valuable trademarks of Cooper Industries in the U.S. and other countries. You are not permitted to use the Cooper Trademarks without the prior written consent of Cooper Industries.

