Read and Retain for Future Reference

Cooper Bussmann

450U-E Wireless Ethernet Modem and Device Server User Manual

Version 1.4.0

ATTENTION!

Incorrect termination of the supply wires may cause internal damage and will void the warranty. To ensure that your 450U-E enjoys a long life, refer to this user manual to verify that all connections are terminated correctly before turning on power for the first time

CAUTION

To comply with FCC RF Exposure requirements in section 1.1310 of the FCC rules, antennas used with this device must be installed to provide a separation distance of at least 20 cm from all persons to satisfy RF exposure compliance.

Do not operate the transmitter when anyone is within 20 cm of the antenna. Ensure that the antenna is correctly installed in order to satisfy this safety requirement.

AVOID

- Operate the transmitter unless all RF connectors are secure and any open connectors are properly terminated
- Operate the equipment near electrical blasting caps or in an explosive atmosphere

⚠ **NOTE All equipment must be properly grounded for safe operations. All equipment should be serviced only by a qualified technician.**

FCC Notice

Part 15.19—This device complies with part 15 of the FCC rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Part 15.21—the grantee is not responsible for any changes or modifications not expressly approved by the party responsible for compliance. Such modifications could void the user's authority to operate the equipment.

Part 15.105(b)—This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

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

Part 90—This device has been type accepted for operation by the FCC in accordance with Part 90 of the FCC rules (47CFR Part 90). See the label on the unit for the specific FCC ID and any other certification designations.

⚠ **NOTE This device should only be connected to PCs that are covered by either a FCC DoC or are FCC certified.**

Manufacturer	Model Number	Coax Kit	Net
ELPRO	UDP400-3	Includes 3m Cellfoil	1 dB Gain
ELPRO	UDP400-5	Includes 5m Cellfoil	Unity Gain
ELPRO	BU-3/400	CC10/450	2.5 dB Gain
ELPRO	BU-6/400	CC10/450	5.5 dB Gain
ELPRO	YU3/400	CC10/450	3.5 dB Loss
ELPRO	YU6/400	CC10/450	6.5 dB Gain

Manufacturer	Model Number	Coax Kit	Net
ELPRO	YU9/400	CC20/450	5 dB Gain
ELPRO	YU16/400	CC20/450	10 dB Gain

Safety Notices

Exposure to RF energy is an important safety consideration. The FCC has adopted a safety standard for human exposure to radio frequency electromagnetic energy emitted by FCC regulated equipment as a result of its actions in Docket 93-62 and OET Bulletin 65 Edition 97-01.

UL Notice

The Wireless Ethernet module is to be installed by trained personnel or licensed electricians only, and installation must be carried out in accordance with the instructions listed in the Installation Guide and applicable local regulatory codes.

- The units are intended for Restricted Access Locations.
- The Wireless Ethernet module is intended to be installed in a final enclosure, rated IP54, before use outdoors.
- The Equipment shall be powered using an external listed power supply with LPS outputs or a Class 2 power supply.
- The Wireless Ethernet module must be properly grounded for surge protection before use.
- If installed in a hazardous environment, coaxial cable shall be installed in a metallic conduit

GNU Free Documentation License:

ELPRO Technologies is using a part of Free Software code under the GNU General Public License in operating the 450U-E product. This General Public License applies to most of the Free Software Foundation's code and to any other program whose authors commit by using it. The Free Software is copyrighted by Free Software Foundation, Inc., and is licensed "as is" without warranty of any kind. Users are free to contact ELPRO Technologies for instructions on how to obtain the source code used in the 450U-E.

A copy of the license is included in Appendix H.

Important Notice

ELPRO products are designed to be used in industrial environments, by experienced industrial engineering personnel with adequate knowledge of safety design considerations.

ELPRO radio products are used on unprotected license-free radio bands with radio noise and interference. The products are designed to operate in the presence of noise and interference. However, in an extreme case radio noise and interference could cause product operation delays or operation failure. Like all industrial electronic products, ELPRO products can fail in a variety of modes due to misuse, age, or malfunction. We recommend that users and designers design systems using design techniques intended to prevent personal injury or damage during product operation, and provide failure tolerant systems to prevent personal injury or damage in the event of product failure. Designers must warn users of the equipment or systems if adequate protection against failure has not been included in the system design.

Designers must include this Important Notice in operating procedures and system manuals.

These products should not be used in non-industrial applications, or life-support systems, without consulting ELPRO first.

- A radio license is not required in some countries, provided the module is installed using the aerial and equipment configuration described in the 450U-E Installation Guide. Check with your local distributor for further information on regulations.

- Operation is authorized by the radio frequency regulatory authority in your country on a non-protection basis. Although all care is taken in the design of these units, there is no responsibility taken for sources of external interference. Systems should be designed to be tolerant of these operational delays.
- To avoid the risk of electrocution, the aerial, aerial cable, serial cables and all terminals of the 450U-E module should be electrically protected. To provide maximum surge and lightning protection, the module should be connected to a suitable ground and the aerial, aerial cable, serial cables and the module should be installed as recommended in the Installation Guide.
- To avoid accidents during maintenance or adjustment of remotely controlled equipment, all equipment should be first disconnected from the 450U-E module during these adjustments. Equipment should carry clear markings to indicate remote or automatic operation. For example: “This equipment is remotely controlled and may start without warning. Isolate at the switchboard before attempting adjustments.”
- The 450U-E module is not suitable for use in explosive environments without additional protection.
- The 450U-E operates using the same radio frequencies and communication protocols as commercially available off-the-shelf equipment. If your system is not adequately secured, third parties may be able to gain access to your data or gain control of your equipment via the radio link. Before deploying a system, make sure you have considered the security aspects of your installation carefully.

Release Notice

This is the December 2013 release of the 450U-E Ethernet Modem User Manual version 1.4.0, which applies to version 1.4 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

Chapter 1 - INTRODUCTION

The 450U-E Industrial 802.11-based Wireless Ethernet module provides wireless connections between Ethernet devices and/or Ethernet wired networks (LANs). The 450U-E is a fixed frequency wireless transceiver that operates within the 360 MHz to 512 MHz frequency spectrum in one of eight 20-MHz frequency bands, depending on the model purchased.

The 450U-E module provides two serial connections and an Ethernet connection. It is possible to use all three data connections concurrently, allowing the 450U-E to act as a device server where wireless connections can be made between serial devices and Ethernet devices. The 450U-E also provides functionality between serial Modbus RTU devices and Ethernet Modbus TCP devices. Appropriate driver applications will be required in the host devices to handle other protocols. The modem is capable of passing VLAN tagged frames.

The Ethernet connection is a standard RJ-45 connection that will operate at up to 100 Mbps. The module will transmit the Ethernet messages on the wireless band at rates between 1 and 19.2 Kbps, depending on model, band, encryption methods, and radio paths.

1.1 Network Topology

The 450U-E is an Ethernet device, and must be configured as part of an Ethernet network. Each 450U-E module must be configured as one of the following:

- Access point or client (station)
- Bridge or router

Access Point vs. Client

The 450U-E module that is configured as an access point acts as the wireless master. The access point accepts and authorizes links initiated by the client modules, and controls the wireless communications. Clients (stations) are slave modules, and become transparent Ethernet links when connected to the access point.

Figure 1 shows a connection between two Ethernet devices using 450U-E Ethernet modems. In this example, one 450U-E is configured as an access point and the other as a client.

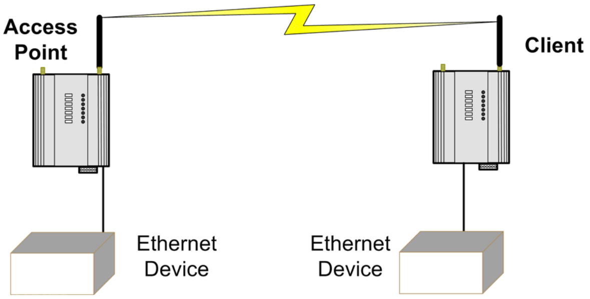


Figure 1 AP and Client

Figure 2 shows an existing LAN being extended using 450U-Es. In this example, the access point is configured at the LAN end—although the wireless link will still work if the client is at the LAN end.

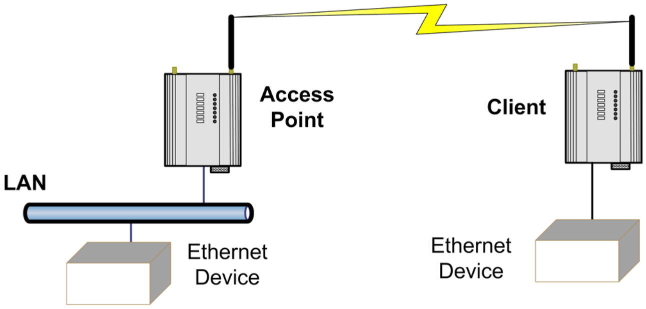


Figure 2 AP and Client

As the example in Figure 3 shows, an access point can connect to multiple clients. In this case, the access point should be the central unit.

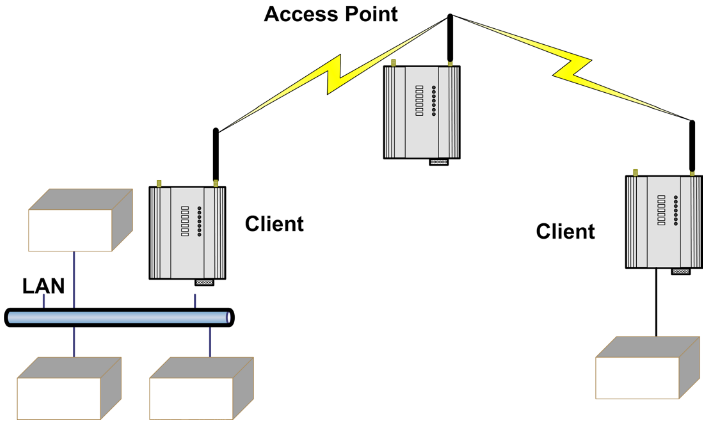


Figure 3 Multiple Clients

An access point could be used as a repeater unit to connect two 450U-E clients that do not have direct reliable radio paths. There is no special repeater module—any 450U-E module can function as a repeater and at the same time be connected to Ethernet devices or be on a LAN. Multiple access points can be set-up in a "mesh" network to provide multiple repeaters.

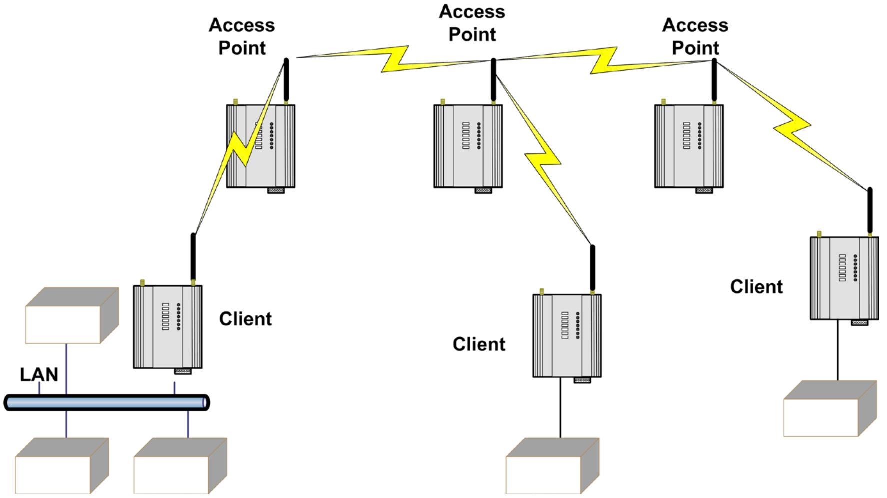


Figure 4 Multiple Access Points

Bridge vs. Router

Each 450U-E, when configured as a bridge, uses a single IP address for Ethernet and Wireless connections. A bridge connects devices within the same Ethernet network, for example, extending an existing Ethernet LAN.

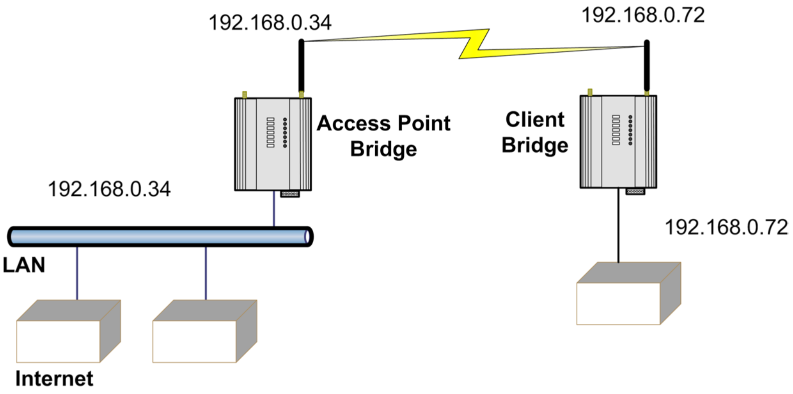


Figure 5 Bridge

A router connects devices on different LANs. The IP addresses for the Ethernet and the wireless sides must be different. In this example, the wireless link is part of LAN A, with the client (station) unit acting as the router between LAN A and LAN B.

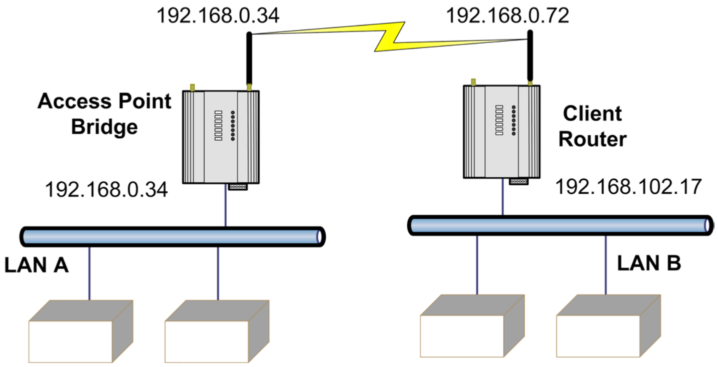


Figure 6 Client Router

Alternatively, the access point could be configured as a router. The wireless link is then part of LAN B.

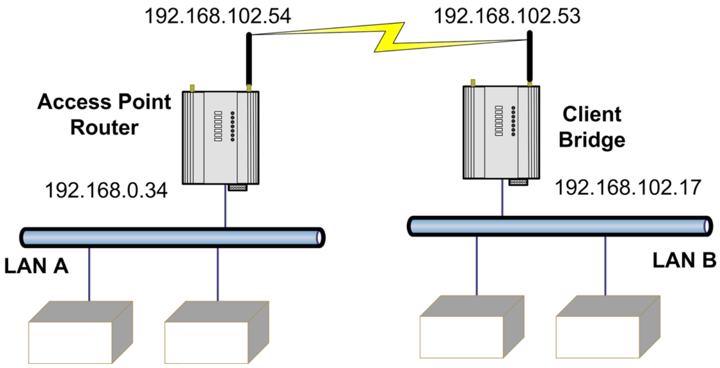


Figure 7 AP Router

If more than two routers are required within the same radio network, the routing rules may need to be configured (for details, see “4.9 IP Routing” on page 48). There is no limit to the number of bridges you can have in the same network, although a maximum of 128 client units can be linked to any one access point.

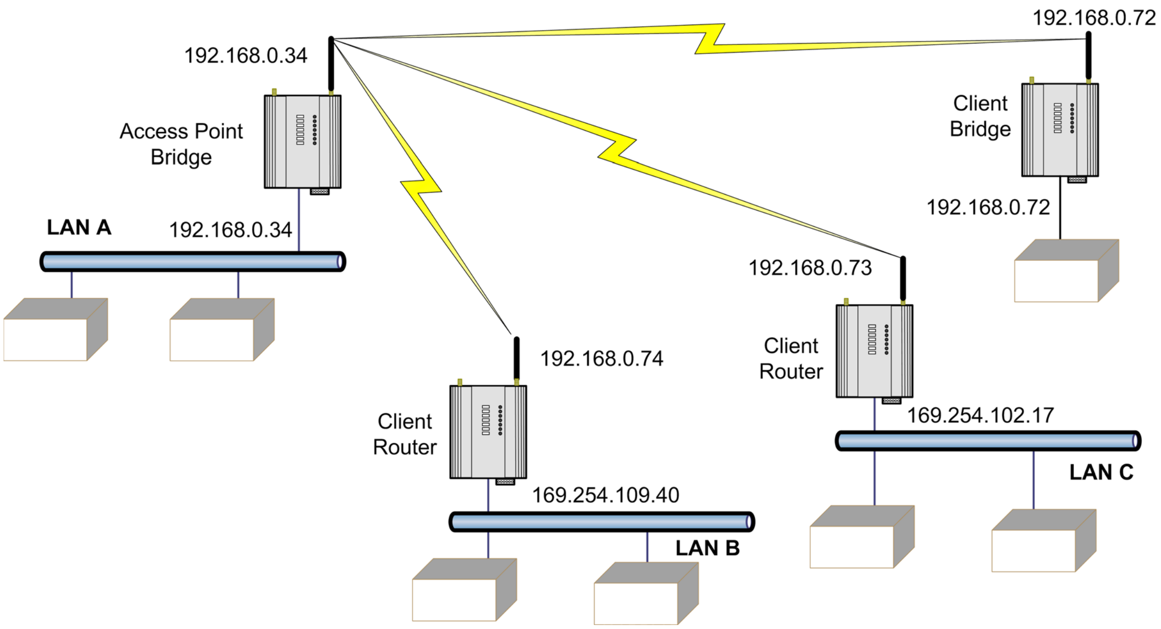


Figure 8 Multiple Routers

1.2 Getting Started

Most applications for the 450U-E require little configuration. The 450U-E has many sophisticated features, but if you do not require these features follow these steps to configure the modules quickly.

1. Read Chapter 2, which explains the power, antenna, serial, Ethernet, and I/O connections required for successful operation.
2. Power the 450U-E and set up an Ethernet connection to your PC.

   For detailed steps, see “4.1 Connecting and Logging On” on page 22.
3. Set the 450U-E address settings and other necessary configuration parameters as described in “4.2 Quick Start” on page 25.
4. Save the configuration.

   The 450U-E is now ready to use.

If the modems are connected to an existing network some form of filtering (MAC, IP, and ARP) will reduce the amount of Ethernet network traffic that is sent over the radio network. For more information, see “4.10 Filtering” on page 49. Before installing the 450U-E, bench test the system. It is much easier to locate problems when the equipment is all together.

Chapter 2 - INSTALLATION

2.1 General

The 450U-E modules are housed in a rugged aluminum case suitable for DIN rail mounting. The terminals will accept wires up to 2.5 mm^2 (12 gauge) in size. Before installing a new system, it is preferable to bench test the complete system. Configuration problems are easier to recognize when the system units are close to one another. Following installation, the most common problem is poor communications caused by incorrectly installed antennas, radio interference on the same channel, or an inadequate radio path. If the radio path is a problem (the path is too long, or obstructed), a higher performance antenna or a higher mounting point for the antenna may rectify the problem. Alternatively, use an intermediate 450U-E module as a repeater.

Each 450U-E module should be effectively grounded via the "GND" screw on the back of the module to ensure that the surge protection circuits inside are effective. The 450U-E Installation Guide provides details and an installation drawing appropriate to most applications.

⚠ **NOTE All connections to the module must be SELV (Safety Extra Low Voltage). Normal 110–250V mains supply must not be connected to any terminal of the 450U-E module. See "2.3 Power Supply" on page 14.**

2.2 Antenna Installation

The 450U-E module will operate reliably over large distances, but the achievable distances will vary with the application, radio configuration, location of antennas, degree of radio interference, and obstructions to the radio path (such as buildings or trees).

⚠ **NOTE A 450U-E module can successfully transmit up to 50 km (31 miles) with a directional antenna attached.**

To achieve the maximum transmission distance, the antennas should be raised above intermediate obstructions so that the radio path is true line-of-sight. The modules will operate reliably with some obstruction of the radio path, although the reliable distance will be reduced. Obstructions that are close to either antenna have a greater blocking affect than obstructions in the middle of the radio path. The 450U-E modules provide a diagnostic feature that displays the radio signal strength of transmissions (see Chapter 5).

Line-of-sight paths are only necessary if you need to achieve the maximum range. Obstructions will reduce the range, or degrade a reliable path. A larger amount of obstruction can be tolerated for shorter distances, but an obstructed path requires testing to determine if the path will be reliable. See Chapter 5 for more information on determining a reliable path.

Where it is not possible to achieve reliable communications between two 450U-E modules, a third 450U-E module may be used to receive the message and re-transmit it. This module is referred to as a repeater. A repeater module may also have a host device connected to it.

Bench Test and Demo System Setup

Care must be taken with placement of antenna in relation to the radios and the other antennas. Strong radio signals can saturate the receiver, hindering the overall radio communications. When setting up a bench test, demonstration, or short range system, the following considerations should be taken into account for optimum radio performance and reduced signal saturation.

- Reduce radio transmit power by adjusting the transmit power level on the Radio webpage (see "4.6 Radio Configuration" on page 33).
- If using demo antennas on each end, fit a 20 dB 5W coaxial attenuator in-line with the coaxial cable.
- Antennas must be kept a suitable distance from each other. Check the receive signal strength on the Connectivity page of the module and ensure that the level is not greater than –45 dB. For more information, see "5.2 Connectivity" on page 70.

Antennas

Antennas can be either connected directly to the module connectors or connected via 50-ohm coaxial cable (such as RG58 Cellfoil or RG213) terminated with a male SMA coaxial connector. The higher the antenna is mounted, the greater the transmission range, but as the length of coaxial cable increases so do cable losses.

The net gain of an antenna and cable configuration is the gain of the antenna (in dBi) less the loss in the coaxial cable (in dB). Maximum net gain for the 450U-E will depend on the licensing regulation for the country of operation and the operating frequency.

Typical antennas gains and losses are:

Antenna	Gain (dBi)
Dipole	2 dBi
Collinear	5 or 8 dBi
Directional (Yagi)	6–15 dBi
Cable Type	Loss (dB per 30m/100 ft)
RG58 Cellfoil Cable kits (3m,10m, 20m)	–1dB, –2.5dB, –4.8 dB
RG213 per 10m (33 ft)	–1.8 dB
LDF4-50 per 10m (33 ft)	–0.5 dB

The net gain of the antenna and cable configuration is determined by adding the antenna gain and the cable loss. For example, an 8 dBi antenna with 10 meters of Cellfoil (–2.5 dB) has a net gain of 5.5 dB (8 dB – 2.5 dB).

Dipole and Collinear antennas

Dipole and collinear antennas transmit the same amount of radio power in all directions, and are easy to install and use because they do not need to be aligned to the destination. The dipole antenna does not require any additional coaxial cable. However, a cable must be added if using any of the other collinear or directional antennas. In order to obtain the maximum range, collinear and dipole antennas should be mounted vertically, preferably one wavelength away (see Figure 9 for distances) from a wall or mast and at least 3 ft (1m) from the radio module.

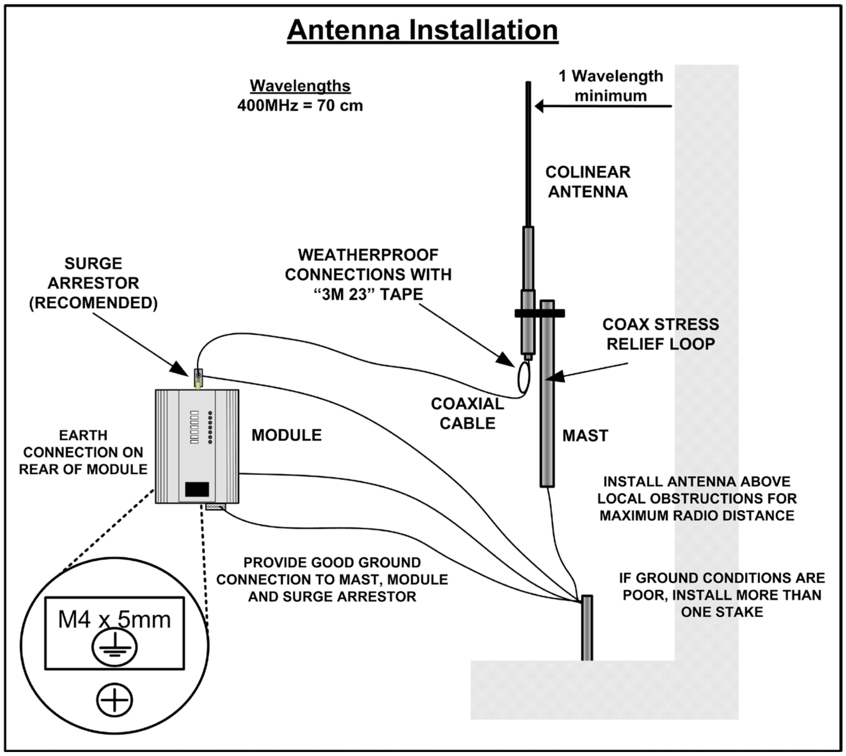

Antenna Installation
Wavelengths
400MHz = 70 cm
1 Wavelength minimum
COLINEAR ANTENNA
SURGE ARRESTOR (RECOMENDED)
WEATHERPROOF CONNECTIONS WITH “3M 23” TAPE
COAX STRESS RELIEF LOOP
COAXIAL CABLE
EARTH CONNECTION ON REAR OF MODULE
MODULE
MAST
INSTALL ANTENNA ABOVE LOCAL OBSTRUCTIONS FOR MAXIMUM RADIO DISTANCE
PROVIDE GOOD GROUND CONNECTION TO MAST, MODULE AND SURGE ARRESTOR
IF GROUND CONDITIONS ARE POOR, INSTALL MORE THAN ONE STAKE
M4 x 5mm

Figure 9 Collinear/Dipole

Directional Antennas

A directional antenna provides high gain in the forward direction, but lower gain in other directions. This type of antenna may be used to compensate for coaxial cable loss for installations with marginal radio path. Directional antennas can be any of the following:

- Yagi antenna with a main beam and orthogonal elements
- Directional radome, which is cylindrical in shape
- Parabolic antenna

Yagi antennas should be installed with the main beam horizontal, pointing in the forward direction. If the Yagi antenna is transmitting to a vertically mounted omni-directional antenna, the Yagi elements should be vertical. If the Yagi is transmitting to another Yagi, the elements at each end of the wireless link need to be in the same plane (horizontal or vertical).

Directional radomes should be installed with the central beam horizontal, and must be pointed exactly in the direction of transmission to benefit from the gain of the antenna.

Parabolic antennas should be mounted according to the manufacturer's instructions, with the parabolic grid at the back and the radiating element pointing in the direction of the transmission.

Ensure that the antenna mounting bracket is well connected to ground.

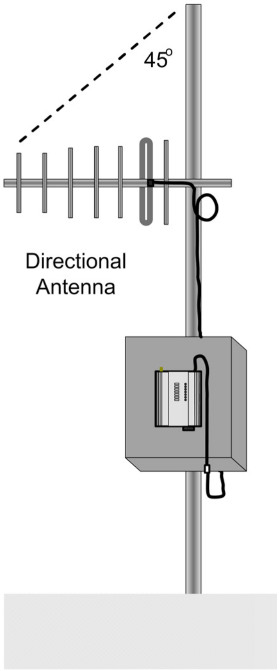


Figure 10 Directional Antenna

Installation Tips

Connections between the antenna and the coaxial cable should be carefully taped to prevent ingress of moisture. Moisture ingress in the coaxial cable is a common cause for problems with radio systems because it greatly increases the radio losses. We recommend that the connection be taped—first with a layer of PVC tape, next with vulcanizing tape (such as 3M™ 23 tape), and finally with another layer of PVC UV-stabilized insulating tape. The first layer of tape allows the joint to be easily inspected when troubleshooting because the vulcanizing seal can be easily removed (see Figure 11).

Where antennas are mounted on elevated masts, the masts should be effectively grounded to avoid lightning surges. For high lightning risk areas, approved ELPRO surge suppression devices, such as the CSD-SMA-2500 or CSD-N-6000, should be fitted between the module and the antenna. If using non-ELPRO surge suppression devices, the devices must have a “turn on” voltage of less than 90V. If the antenna is not already shielded from lightning strike by an adjacent grounded structure, a lightning rod may be installed above the antenna to provide shielding.

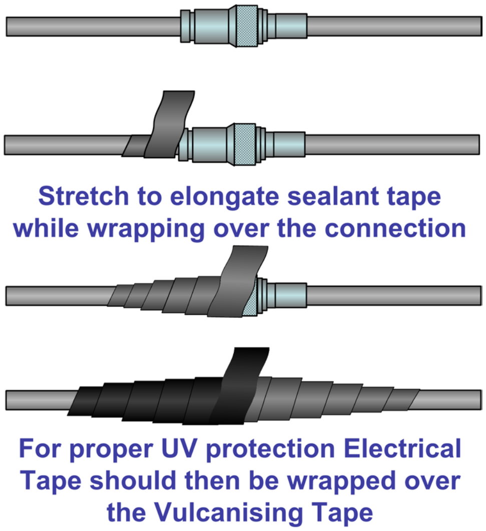

Stretch to elongate sealant tape while wrapping over the connection
For proper UV protection Electrical Tape should then be wrapped over the Vulcanising Tape

Figure 11 Vulcanizing Tape

2.3 Power Supply

The 450U-E module can be powered from a 9—30 Vdc supply. The supply should be rated in accordance with the supply voltage and radio power level. The power requirements for the 450U-E unit are shown in the table below. The positive side of the supply must not be connected to ground. The supply negative is connected to the unit case internally. The DC supply may be a floating supply or negatively grounded. A ground terminal is provided on the back of the module. This terminal should be connected to the main ground point of the installation in order to provide efficient surge protection for the module (refer to the installation diagram in the 450U-E Installation Guide).

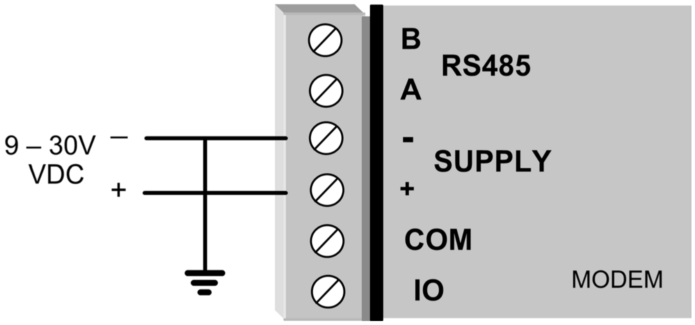


Figure 12 Power Supply

	13.8 Vdc	24 Vdc
Quiescent	120 mA	70 mA
TX @ 500 mW	400 mA	220 mA
TX @ 5W	1.2–1.5A	550–650 mA

2.4 Serial Connections

RS-232 Serial Port

The RS-232 serial port on the 450U-E is a nine pin DB-9 female connector that provides connection for host devices as well as providing a connection point for diagnostics, field testing, and factory testing. Communication is via standard RS-232 signals, and the 450U-E is configured as a DCE device. Hardware handshaking using the CTS/RTS lines is provided. The CTS/RTS lines may be used to reflect the status of the input buffer on the local unit.

Figure 13 shows example cable drawings for connecting to a DTE host (PC) or another DCE device (modem). A rule of thumb for determining if a device is DCE or DTE is to look at the DB-9 connector. If the connector is female the device is DCE, and if it is male the device is DTE. In addition, if the device functions when plugged into a computer using a standard straight-through cable, the device is a DCE.

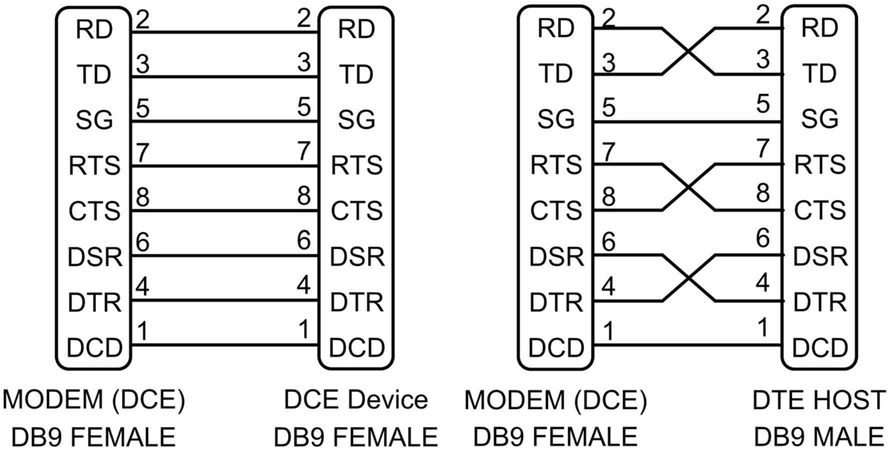


Figure 13 Serial Cable

DB-9 Connector Pinouts

Pin	Name	Direction	Function
1	DCD	Out	Data Carrier Detect
2	RXD	Out	Transmit Data (serial data output from DCE to DTE)
3	TXD	In	Receive Data (serial data input from DTE to DCE)
4	DTR	In	Data Terminal Ready
5	GND		Signal Ground
6	DSR	Out	Data Set Ready (always high when unit is powered on)
7	RTS	In	Request to Send
8	CTS	Out	Clear to Send
9	RI		Ring Indicator

RS-485 Serial Port

The RS-485 port provides a communication link from the 450U-E unit to a host device using a multi-drop cable. Up to 32 devices may be connected within each multi-drop network. Because the RS-485 communication medium is shared, only one unit at a time on the RS-485 cable may send data. Therefore, communication protocols based on the RS-485 standard require some type of arbitration. RS-485 is a multi-drop communication link or bus that can span relatively large distances (up to 1.2 km or 4000 ft) using a balanced differential paired cable. It is recommended that the cable be shielded or twisted pair to reduce potential RF interference.

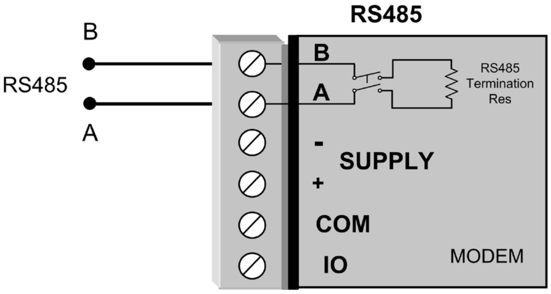


Figure 14 RS-485

An RS-485 network should be wired as indicated in Figure 15 and terminated at each end of the network with a 120-ohm resistor. An on-board terminating resistor is provided in the modem and can be engaged by operating the single DIP switch on the end plate next to the RS-485 terminals. The DIP switch should be in the “1” (on) position to connect the resistor. If the RS-485 device that the modem is being connected to does not have a termination switch, a 120-ohm resistor must be fitted manually across the RS-485 terminals. Only devices at each end of the multi-drop RS-485 cable need to have a termination resistor enabled or fitted.

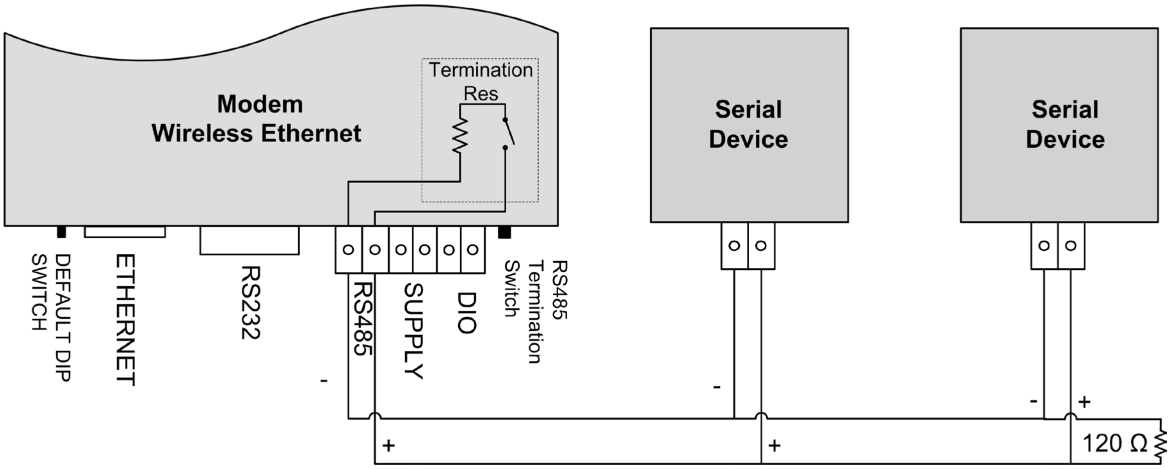


Figure 15 Multidrop Serial

Fail-safe Biasing

Fail-safe biasing is a simple voltage divider that is connected to the RS-485 bus and pulls the terminal voltages high or low when the communication state is idle, rather than leaving them in a floating state which could cause data corruption. If you are connecting a serial device that does not support fail-safe biasing and a 115S expansion I/O module is also not fitted, biasing resistors must be wired to each RS-485 terminal to ensure correct operation. Resistor values depend on the supply voltage. See Figure 16 for resistor value calculation and wiring.

NOTE The 450U-E does not support fail-safe biasing on the RS-485 unless a 115S Serial Expansion module is also connected and has its termination switch enabled.

$$R = \frac{Supply - 2V}{3}$$

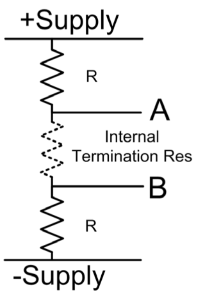


Figure 16 Resistor Value Calculation

USB Ports

Module has a two USB ports housed under the plastic cover on the front of the module.

- **USB A Host Port**—Used for performing a full upgrade of the module firmware. Patch files are not loaded via the USB, but rather through the module's Web Server. See Appendix A for instructions on performing a full firmware upgrade or patch file upgrade.
- **USB B Device Connector**—Used as a secondary Ethernet connection point. This is a USB-to-Ethernet converter that allows you to connect to the module's Web Server without having to disconnect the existing Ethernet connection or install a hub or switch to allow more ports. For more information about this connection, see Appendix B.

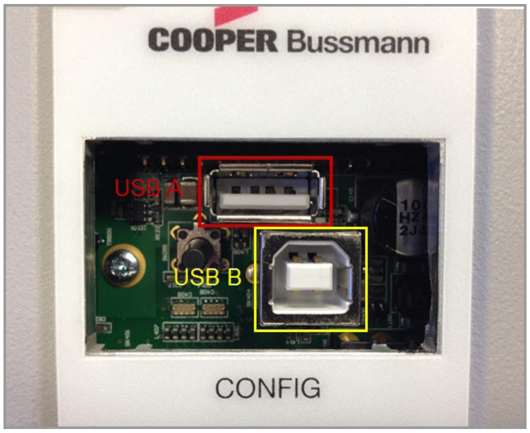


Figure 17 USB Connections

2.5 Input and Output Connections

The 450U-E has a single physical on-board I/O channel that can be configured as either digital or analog via the module's Web Server. The digital channel can act as an input or output. It can be monitored, set remotely, or used as an output for communications alarm status. If more I/O are required, you can add 115S Serial Expansion I/O modules via the RS-232 or RS-485 ports. For more information, see "4.12 Input/Output Configuration" on page 58.

Analog Input

The I/O channel can be configured to accept a 0–20 mA current sinking analog input. The current source must be externally powered, and the ADIO must be configured for analog input rather than digital input/output. This can be done using the I/O Configuration or the External I/O Mode Configuration webpage within the module's Web Server. For more information, "4.12 Input/Output Configuration" on page 58.

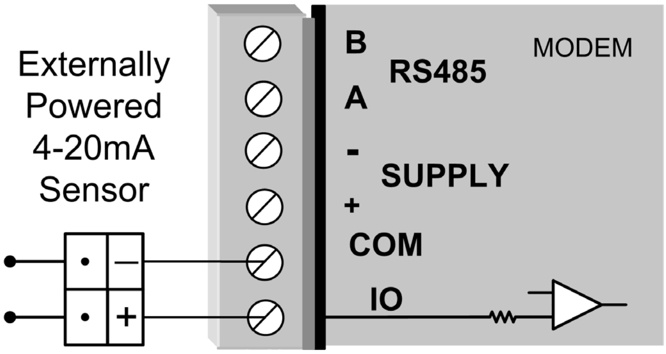


Figure 18 Analog Input

Digital Output

The I/O channel can also be used as a discrete output. The digital output uses an field-effect transistor (FET) rated at 30 Vdc 500 mA, and can be used to switch a load, such as a relay coil or contactor. The output can be activated by manually writing a value of “1” to register location 1 using the I/O Diagnostics page within the module’s Web Server or using the on-board Modbus TCP server or serial Modbus master to turn on the output. It can also be accessed from an external Modbus server (such as a PLC, DCS, or SCADA) via the Ethernet network or serial interface. When the output is activated, the I/O indicator appears red.

NOTE The digital output operation will override the digital input operation. For example, if the output is activated while the DIO is being read, the indication will show the input as being on (1).

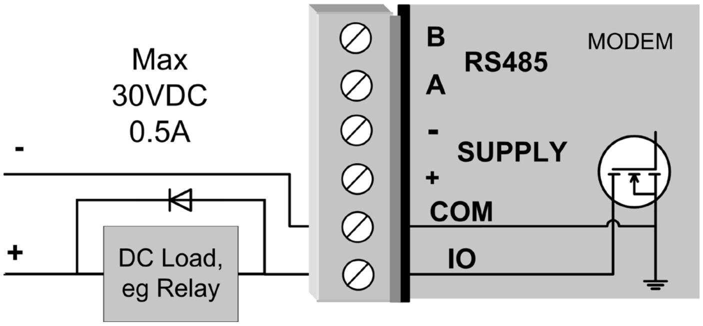


Figure 19 DIO Output

Digital Input

When used as an input, the I/O channel supports a voltage-free contact connection such as a mechanical switch or an NPN transistor device, such as an electronic proximity switch. Contact wetting current of the input is approximately 5 mA, and is provided to maintain reliable operation for driving relays. The digital input is activated by connecting between the “IO” and “COM” terminals.

The I/O indicator on the front panel of the module appears green when the input is switched on (closed/shorted). The device will be able to activate the digital input if the resistance of the switching device is less than 200 ohms.

NOTE PNP transistor devices are not compatible with this digital input.

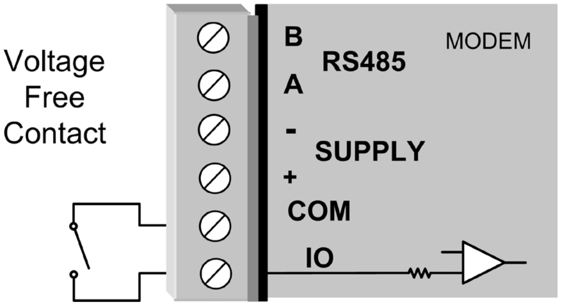


Figure 20 DIO Input (Switch)

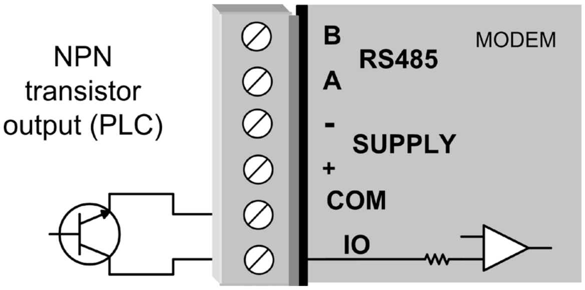


Figure 21 Digital Input (Transistor)

Chapter 3 - OPERATION

This chapter describes the normal operation of the 450U-E Ethernet modem. The modem allows transparent communications between different Ethernet devices, and also allows some connectivity with RS-232 and RS-485 serial devices. All configuration and diagnostics is performed by accessing the embedded Web Server, which is described in Chapter 4.

3.1 Startup

Access Point Startup

Normal module startup time is approximately 1 minute and 20 seconds from when the module is powered on to when you can connect to the IP address. After the access point (AP) completes its startup process, it immediately begins broadcasting periodic messages (beacons) on the configured channel using the default beacon interval time of 15 seconds.

Beacons include information that a client may examine in order to identify whether the access point is suitable for link establishment. Clients will only attempt to establish a link with an access point whose beacon indicates a matching service set identifier (SSID). Access points do not initiate link establishment.

Client Startup

Normal module startup time is approximately 1 minute and 20 seconds from when powered on to when you can connect to the IP address. After a client completes its startup process, it begins scanning its configured frequency for a suitable access point. The client will attempt to establish a link with an access point only if the access point has a matching SSID, encryption method, and the correct password. If more than one suitable access point is discovered, the client attempts to establish a link with the access point that has the strongest radio signal.

Link Establishment

Once a client identifies a suitable access point for link establishment it attempts to link using a two-step process— authentication, and association. During authentication, the client and access point check whether their configurations permit them to establish a link. Once the client is authenticated it requests an association to establish a link.

The status of the wireless link is indicated by the TX/LINK LED. For an access point, the TX/LINK LED is off as long as no links are established. Once one or more links are established the TX/LINK LED appears on and green. For a client, the Link LED reflects the connection status to an access point. Link status is also displayed on the Connectivity page of the Web interface (see “5.2 Connectivity” on page 70).

After the link is established, data may be transferred in both directions. The access point acts as a master unit and controls the flow of data to the clients linked to it. Clients can only transmit data to the access point to which they are connected. When a client transfers data to another client, it first transmits the data to the access point, which then forwards the data to the destined client.

A maximum of 127 clients may be linked to an access point.

⚠ **NOTE The presence of a link does not mean that the connected unit is authorized to communicate over the radio. If the encryption keys are incorrect between units in the same system, or a dissimilar encryption scheme is configured, the Link LED turns on, however data cannot be passed over the wireless network.**

How a Link Connection is Lost

A client monitors beacon messages from an access point to determine whether the link is still present. If the client can no longer hear the access point beacons it waits seven beacon times (7 x 15 seconds) and then sends a link check message. If the client still does not receive an acknowledgment, it will drop the link and clear its connectivity list. If an access point is connected to a single client and the client fails or is turned off, the access point will wait five minutes before dropping the link and clearing the connectivity list.

Roaming Clients

Clients can roam within a system, but there are some limitations due to link timeouts. If the client is connected to an access point and the link fails due to a hardware problem or the signal level falls below the minimum threshold (–99 dBm, 25 kHz channel @19200 baud, or –100 dBm @ 9600 baud), the client will scan for beacon signals and connect to the access point with the strongest RSSI level (if more than one access points can be heard and provided the SSID and any encryption methods/keys are the same). This functionality allows clients to roam to a stronger access point when the signal level gets too low or the link completely fails. The time frame for the changeover is approximately 105 seconds due to link retires and timeouts.

3.2 LED Indicators

The following table describes the front panel LEDs for all operating conditions.

LED	Condition	Description
OK	Green	Normal operation
OK	Flashing red/green	Module boot sequence
OK	Red	Default quick start mode (unconfigured)
Radio RX	Green flash	Radio receiving data (good signal strength)
Radio RX	Red flash	Radio receiving data (low signal strength)
TX/LINK	Green	Radio connection established
TX/LINK	Red	Radio transmitting
RS-232	Green flash	Data sent from RS-232 serial port
RS-232	Red flash	Data received to RS-232 serial port
LAN	On	Link established on Ethernet port
LAN	Orange flash	Activity on Ethernet port
RS-485	Green flash	Data sent from RS-485 serial port If expansion I/O is being used this will flash constantly
RS-485	Red flash	Data received to RS-485 serial port
IO	Green	Digital input is on
IO	Red	Digital output is active
IO	Off	Digital output off and input is open circuit Analog input current loop

IO	Green, different intensity	Dim = 4 mA
		Bright = 20 mA

The Ethernet RJ-45 connector on the end of the module incorporates two LEDs. The Link LED turns on to indicate a connection on the Ethernet port, and blinks off briefly when activity is detected, similar to the LAN LED on the front panel. The 100-MB LED appears on if the LAN connection supports 100 Mbps. The 100-MB LED appears off if only the 10-Mbps connection is supported. Other conditions indicating a fault are described in Chapter 5.

3.3 Default Configuration Switch

The 450U-E will temporarily load factory-default settings if it is powered on with the RUN/SETUP switch (on the end-plate of the module) in SETUP position. The previous configuration remains stored in non-volatile memory and will only change if a configuration parameter is modified and the change saved. When in SETUP mode, wireless operation will be disabled.

Because the default IP address of the modem will be within the IP range 192.168.0.XXX, it may not be compatible with the network or PC that you are using for configuration. You will temporarily need to change the computers IP address to allow connection to the module. For details, see “4.1 Connecting and Logging On” on page 22.

⚠ **IMPORTANT Remember to return the switch to the RUN position and cycle power at the conclusion of configuration to resume normal operation.**

The following is the default factory configuration of the 450U-E:

- **Operating mode:** Client
- **Device mode:** Bridge
- **IP address**: 192.168.0.1XX, where “XX” is the last two digits of the serial number (the default IP address is shown on the printed label on the back of the module)
- **Netmask:** 255.255.255.0
- **Username:** user
- **Password:** user

3.4 Radio Operating Parameters

Frequency Bands

The radios will operate within the range 360–512 MHz, but the radio must be factory-set to one of the 20 MHz frequency bands shown in the following table. Care must be taken when ordering to select the correct band for your locale because the frequency cannot be configured outside of its band.

The following frequency bands are available.

Band	Frequency Range	Band	Frequency Range
370	360–380 MHz	390	380–400 MHz
410	400–420 MHz	430	420–440 MHz
440	430–450 MHz	460	450–470 MHz
480	470–490 MHz	500	490–512 MHz

⚠ **NOTE Modems must be ordered to operate in the desired band. Modems cannot be tuned to a frequency outside of its factory-set band.**

Data Rate

The 450U-E can be configured with different radio transmission rates. Selections available are 9600 and 19200 bps for wide band radios or 4800 and 9600 bps for narrow band. The data rate only applies to transmit messages; the radio is able to receive on all available data rates. Reducing the data rate can increase the reliable communication range of the module. For example, if the received signal level is low, the data rate could be reduced to improve communications.

It is important that the data rates on the client radios be configured appropriately for the radio link. The default data rate will be set to the high level depending on the bandwidth. For example, it is set to 19.2 Kbps if the radio is wide band (25 kHz) and 9.6 Kbps if the radio is narrow band (12.5 kHz). If the signal strength (RSSI) for the radio is less than –100 dBm for narrow band and –110 dBm for wide band radios it is recommended that the radio data rate is reduced to the lower rate. The received signal strength indicator (RSSI) can be viewed on the Connectivity page of the module’s Web Server. For details, see “5.2 Connectivity” on page 70.

⚠ **NOTE When an access point first communicates with a client it remembers what data rate it is using and from then on will communicate at that rate. All UDP broadcast traffic and beacon messages will use the lowest date rate from all the modules in the system.**

Receiver

The RSSI varies depending on the radio channel width and whether the radio is a wide band radio using 25 kHz channels or a narrow band radio using 12.5 kHz channels. The transmit data rate also varies depending on the receiver sensitivity. Refer to the following table on receiver sensitivity.

Receiver Sensitivity	Baud Rate		
Bandwidth	4.8 Kb	9.6 Kb	19.2 Kb
25 kHz Channel	N/A	–110 dBm	–99 dBm
12.5 kHz Channels	–111 dBm	–100 dBm	N/A

Chapter 4 - CONFIGURATION

The 450U-E provides an embedded Web Server that resides in the module's memory. The Web Server allows you to perform configuration and diagnostics functions on the 450U-E using the Microsoft® Internet Explorer® or Google Chrome™ Web browser, which can be obtained from their websites. Using other browsers is not advised, since they may not be fully compatible with the 450U-E Web Server webpages.

⚠ **NOTE Microsoft Internet Explorer (IE) version 6 will not load webpages due to a compatibility issue between IE version 6 and SSL-security websites.**

4.1 Connecting and Logging On

Use the following procedure to directly connect a PC to the 450U-E in order to configure the module using the Web Server. Because the default IP address of the 450U-E is within the IP range 192.168.0.XXX, it may not be compatible with the network or computer that you are using for configuration. In the following steps, you will temporarily change the computer's IP address to allow connection to the module.

You will need a straight-through Ethernet cable for connecting to the module's Ethernet port. The module's default configuration settings are as follows:

- **Operating mode:** Client
- **Device mode:** Bridge
- **IP address**: 192.168.0.1XX, where "XX" is the last two digits of the serial number (the default IP address is shown on the printed label on the back of the module)
- **Netmask:** 255.255.255.0
- **Username:** user
- **Password:** user

1. Connect a straight-through Ethernet cable between the module's Ethernet port and the PC.
2. If you do not know the module's IP address, follow these steps to temporarily restore the module's default settings:

   a. Set the RUN/SETUP switch (located on the end plate of the 450U-E) to the SETUP position.

   b. Power on the 450U-E module.

   When the 450U-E is powered on with the switch in the SETUP position, the module temporarily loads its factory default settings and disables the radio. The previous configuration remains stored in non-volatile memory and will only change if a configuration parameter is modified via the Web Server and the change is saved.

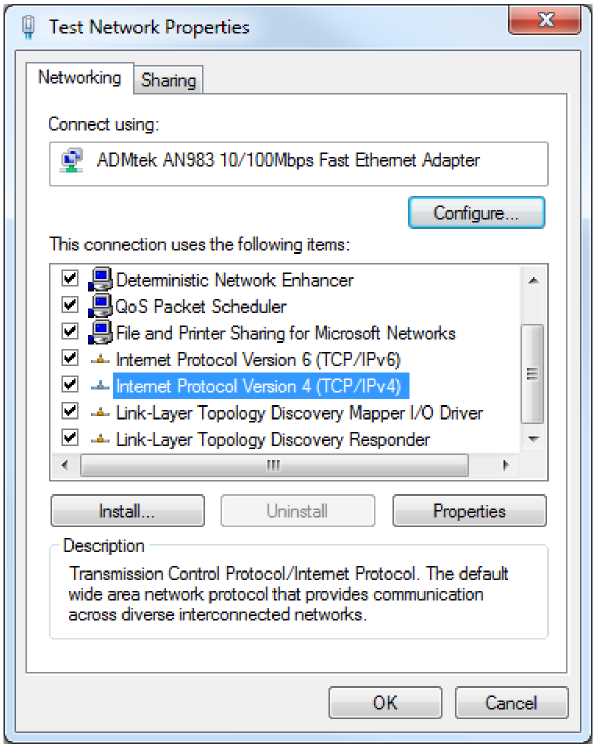
   ⚠ **NOTE Remember to set the RUN/SETUP switch back to the RUN position and restart the module at the conclusion of configuration.**

3. On the PC, open the **Control Panel**, and then click **Network Settings**.

   The following description is for Windows XP. Earlier Windows operating systems have similar settings.

4. Open **Properties** of **Local Area Connection**.

5. Select **Internet Protocol (TCP/IP)** and click **Properties**.



Connect using:

ADMtek AN983 10/100Mbps Fast Ethernet Adapter

This connection uses the following items:

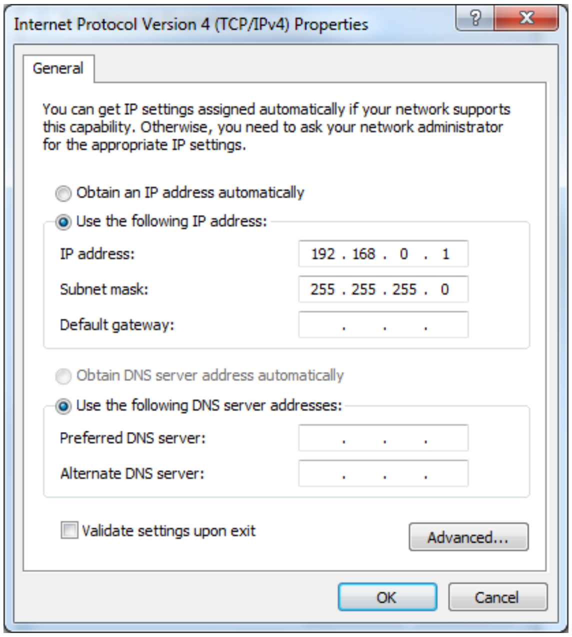
- ☑ Deterministic Network Enhancer
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

Figure 22 Local Area Connection

6. On the **General** tab, enter IP address 192.168.0.1 and subnet mask 255.255.255.0, and then click **OK**.



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 0 . 1

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

☐ Validate settings upon exit

Figure 23 TCP/IP Properties

7. Open Internet Explorer on the PC.

8. If the PC uses a proxy server, ensure that Internet Explorer will bypass the proxy server for local addresses.

   This option may be modified by opening Tools ->Internet Options ->Connections Tab -> LAN Settings-> Proxy Server -> bypass proxy for local addresses.

9. Type “http://” followed by the default IP address of the module, and then press **Enter**.

   The default IP address for the 450U-E 192.168.0.1XX where XX is the last two digits of the serial number.

10. Type the username and password.

11. Press **Enter** or click **OK**.

    If you are connecting to the module for the first time, the Local Configuration page appears (see Figure 24). See the next section, “First Time Configuration” for details.

    If you are not connecting for the first time, the home page appears (see “4.3 Full Configuration” on page 27).

First Time Configuration

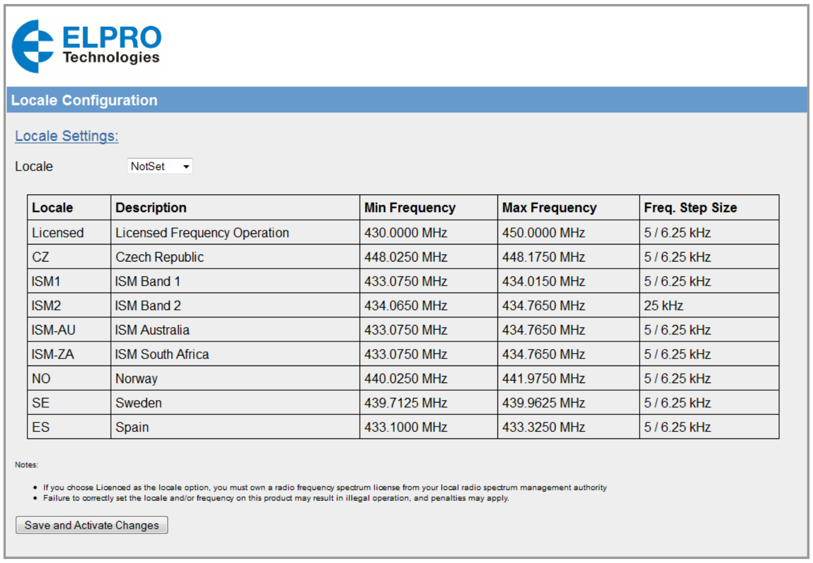
When you connect to a new module or one that is restored to its factory default settings, you need to configure the model locale and radio configuration parameters. These parameters must be specified before the modem can be used. Radio configuration parameters include transmit and receive frequency, channel step size, and the transmit power level as required by country regulation.

The Locale Configuration page (Figure 24) appears automatically when you connect to the module at the default IP address shown on the label on the underside of the module.

NOTE If the locale parameters are not configured on the modem, the OK LED appears red and the transmitter is unable to transmit.

1. On the **Local Configuration** page, click the **Locale** drop-down menu and select the appropriate locale designation for the country of operation.

   The table on the Local Configuration page shows the available locales and frequency ranges based on the radio hardware.



Locale	Description	Min Frequency	Max Frequency	Freq. Step Size
Licensed	Licensed Frequency Operation	430.0000 MHz	450.0000 MHz	5 / 6.25 kHz
CZ	Czech Republic	448.0250 MHz	448.1750 MHz	5 / 6.25 kHz
ISM1	ISM Band 1	433.0750 MHz	434.0150 MHz	5 / 6.25 kHz
ISM2	ISM Band 2	434.0650 MHz	434.7650 MHz	25 kHz
ISM-AU	ISM Australia	433.0750 MHz	434.7650 MHz	5 / 6.25 kHz
ISM-ZA	ISM South Africa	433.0750 MHz	434.7650 MHz	5 / 6.25 kHz
NO	Norway	440.0250 MHz	441.9750 MHz	5 / 6.25 kHz
SE	Sweden	439.7125 MHz	439.9625 MHz	5 / 6.25 kHz
ES	Spain	433.1000 MHz	433.3250 MHz	5 / 6.25 kHz

Notes:

- If you choose Licenced as the locale option, you must own a radio frequency spectrum license from your local radio spectrum management authority
- Failure to correctly set the locale and/or frequency on this product may result in illegal operation, and penalties may apply.

Figure 24 Locale Configuration

2. Click **Save and Activate Changes**.

   The Quick Start page appears (Figure 25) for you to specify the basic radio configuration parameters. See “4.2 Quick Start” on page 25.

   NOTE You cannot navigate away from the Quick Start page until the operating parameters have been set.

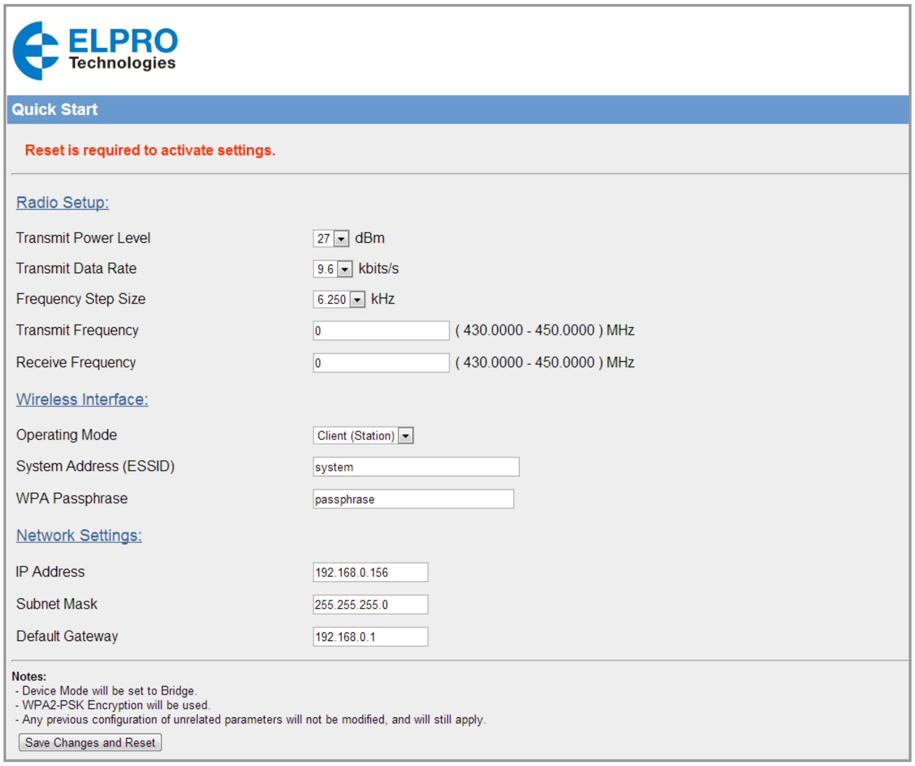
3. After specifying the parameters on the **Quick Start** page, set the **RUN/SETUP** switch on the module back to

RUN and click **Save Changes and Reset** to apply the settings.

The home page appears, as shown in Figure 26. From the home page you can click Full Configuration to adjust modem configuration settings.

4.2 Quick Start

The Quick Start page is a first-stage configuration tool that allows you to set the essential radio parameters needed to achieve a connection between two modules. For most applications, no further configuration should be needed. However, if more advanced options are required, you can use the Full Configuration menu to configure settings once the Quick Start configuration has been saved.



Quick Start

Reset is required to activate settings.

Radio Setup:

Transmit Power Level	27 dBm
Transmit Data Rate	9.6 kbits/s
Frequency Step Size	6.250 kHz
Transmit Frequency	0 (430.0000 - 450.0000) MHz
Receive Frequency	0 (430.0000 - 450.0000) MHz

Wireless Interface:

Operating Mode	Client (Station)
System Address (ESSID)	system
WPA Passphrase	passphrase

Network Settings:

IP Address	192.168.0.156
Subnet Mask	255.255.255.0
Default Gateway	192.168.0.1

Notes:
- Device Mode will be set to Bridge.
- WPA2-PSK Encryption will be used.
- Any previous configuration of unrelated parameters will not be modified, and will still apply.

Figure 25 Quick Start Page

Select **Quick Start** from the Main Menu, and configure the parameters described below (if necessary). When finished, click **Save Changes and Reset** to restart the modem. The Main Screen of the 450U-E webpage will now show the correctly configured model, locale and frequency, as shown in the example in Figure 26.

Transmit Power Level Allows you to adjust the radio power level. Depending on your locale the maximum radio power level may be limited to the maximum allowable for the locale. You can reduce the power for short range applications or for the use of high gain transmitter antennas while still complying with the emission requirements of your license. For dBm to mW conversion table see Appendix F.

Transmit Data Rate The 450U-E module can be configured with different radio transmission rates. The radio baud rate is displayed in kilobits per second (Kbps) for point-to-point radio transmissions. Select a fixed rate for the radio to use from the drop-down list. Selections available are 9600 and 19200 Kbps for wide band radios or 4800 and 9600 Kbps for narrow band radios. The transmit data rate only applies to the transmit messages; the radio can receive on all data rates.

⚠ **NOTE Reducing the configured data rate may increases the reliable range of the module (transmission distance).**

Frequency Step Size The frequency step size is the spacing between frequencies that you can select when configuring the TX and RX frequencies. The steps sizes available are 5 kHz or 6.25 kHz.

Transmit Frequency The frequency that you want to configure for the radio transmitter. Frequency selection is automatically adjusted to the frequency step size configured in the previous parameter. For example, 450.00500, 450.01000, 450.01500, 450.02000 (and so on) for 5 kHz frequency step size, or 450.00625, 450.01250, 450.01875, 450.02500 (and so on) for 6.25 kHz frequency step size.

Receive Frequency The frequency that you want to configure for the radio receiver. Frequency selection is automatically adjusted to the frequency step size configured. For example, 450.00500, 450.01000, 450.01500, 450.02000 (and so on) for 5 kHz frequency step size, or 450.00625, 450.01250, 450.01875, 450.02500 (and so on) for 6.25 kHz frequency step size.

Operating Mode Allows you to select the operating mode for the module:

- **Access Point**—Configures the module to function as an access point
- **Client**—Configures the module to function as a client. This is the default setting.

System Address (ESSID) A 450U-E wireless network is comprised of modules with the same system address. Only modules with the same system address will communicate with each other. The system address is a text string from 1 to 31 characters. Select a text string that identifies your system.

WPA Passphrase If you are using WPA2-PSK (AES) encryption, enter the encryption key passphrase that you want to use.

If a different encryption method is required, after completing the Quick Start configuration you can use the Security page to select the desired encryption method. For details, see “4.5 Security Configuration” on page 31.

IP Address Enter the IP address of the 450U-E module.

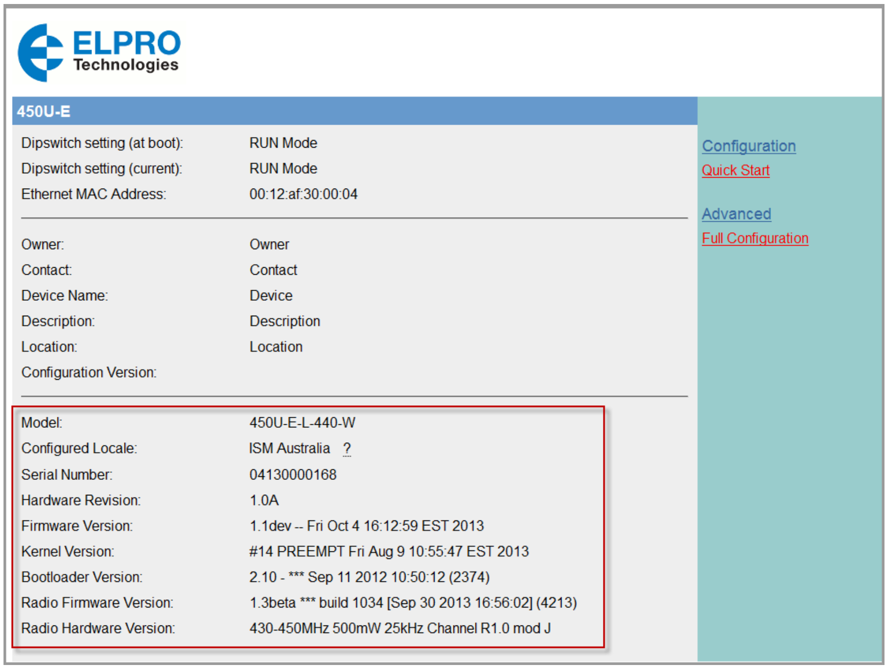
Subnet Mask Enter the subnet mask of the 450U-E module.

Default Gateway Enter the address that the device will use to forward messages to remote hosts that are not connected to any of the local bridged network (Ethernet or Wireless). This is only required if the wired LAN has a gateway unit that connects to devices beyond the LAN (such as Internet access). If there is no gateway on the LAN, set this parameter to the module’s IP address as configured above.

Save Changes Save changes to non-volatile memory. The module will need to be restarted before the changes take effect.

Save Changes and Reset Save settings to non-volatile memory, and reboot the 450U-E module. Once the module has completed the reboot sequence, all changes are in effect.

⚠ **IMPORTANT If the module is in SETUP mode, remember to set the RUN/SETUP switch back to RUN before clicking Save Changes and Reset to restore normal operation.**



450U-E

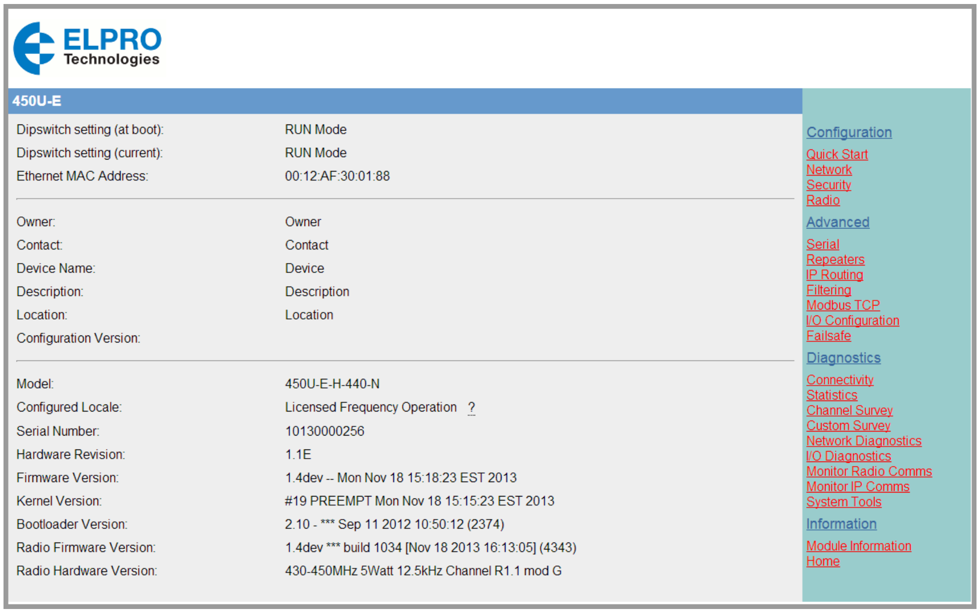
Dipswitch setting (at boot):	RUN Mode
Dipswitch setting (current):	RUN Mode
Ethernet MAC Address:	00:12:af:30:00:04
Owner:	Owner
Contact:	Contact
Device Name:	Device
Description:	Description
Location:	Location
Configuration Version:	
Model:	450U-E-L-440-W
Configured Locale:	ISM Australia ?
Serial Number:	04130000168
Hardware Revision:	1.0A
Firmware Version:	1.1dev -- Fri Oct 4 16:12:59 EST 2013
Kernel Version:	#14 PREEMPT Fri Aug 9 10:55:47 EST 2013
Bootloader Version:	2.10 - *** Sep 11 2012 10:50:12 (2374)
Radio Firmware Version:	1.3beta *** build 1034 [Sep 30 2013 16:56:02] (4213)
Radio Hardware Version:	430-450MHz 500mW 25kHz Channel R1.0 mod J

Figure 26 Home Page

4.3 Full Configuration

The full configuration and diagnostics menu (see Figure 27) is displayed by clicking **Full Configuration** on the home page that appears when you log onto the module. When prompted, enter the username and password (the default username is “user” and the default password is “user”).

To change configuration settings, click the appropriate menu item to display the associated configuration page. The pages are described in detail within this chapter.



450U-E

Dipswitch setting (at boot):	RUN Mode
Dipswitch setting (current):	RUN Mode
Ethernet MAC Address:	00:12:AF:30:01:88
Owner:	Owner
Contact:	Contact
Device Name:	Device
Description:	Description
Location:	Location
Configuration Version:	
Model:	450U-E-H-440-N
Configured Locale:	Licensed Frequency Operation ?
Serial Number:	10130000256
Hardware Revision:	1.1E
Firmware Version:	1.4dev -- Mon Nov 18 15:18:23 EST 2013
Kernel Version:	#19 PREEMPT Mon Nov 18 15:15:23 EST 2013
Bootloader Version:	2.10 - *** Sep 11 2012 10:50:12 (2374)
Radio Firmware Version:	1.4dev *** build 1034 [Nov 18 2013 16:13:05] (4343)
Radio Hardware Version:	430-450MHz 5Watt 12.5kHz Channel R1.1 mod G

Figure 27 Configuration and Diagnostics Menu

Configuration Tips

A system of 450U-E modules must have at least one access point configured as a master with one or more clients. All 450U-E modules should be given the same system address (ESSID) and radio encryption settings. For further information and examples on wireless network topologies, see “1.1 Network Topology” on page 7.

The 450U-E supports two radio encryption methods, WEP128 and WPA2-PSK. The default encryption method is WPA2 and is setup during the Quick Start process by simply entering a password. You can change the encryption method from the Security page (see “4.5 Security Configuration” on page 31). If you are using any form of encryption, all modules in the system will need the same encryption method and keys. We recommend that you enter a new password and not use the default “passphrase”.

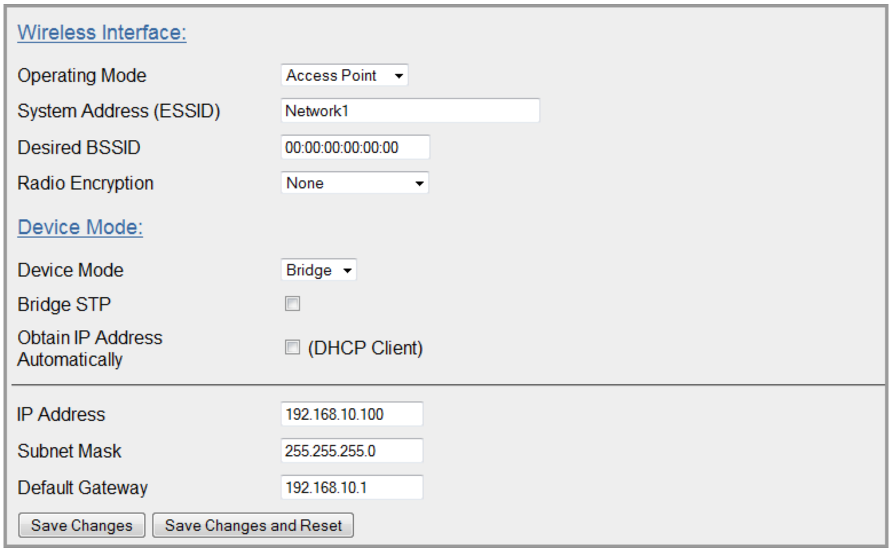
NOTE If you are making changes to a remote module via the radio link, make sure that all changes are compliant and accurate before clicking Save Changes and Reset. Some field changes may stop the radio link from working and will require a hardwire connection to restore the settings.

Care should be taken when connecting the modem to existing networks. When configured as a bridge (default), all broadcast messages appearing at the module’s wired Ethernet port will be transmitted over the radio. The modem has a low data throughput, and any unnecessary traffic being sent over the radio could compromise the reliability of the wireless link. In many cases, the intended recipient of the broadcast traffic heard on the Ethernet port does not lie at the opposite end of a radio link. Therefore, it is recommended that the radios be configured with basic filtering or configured as a routing network to limit sending unnecessary broadcast traffic over the radio. See “4.10 Filtering” on page 49 for more information.

4.4 Network Configuration

Click **Network** on the menu to view or modify parameters related to the wired and wireless Ethernet network interfaces. In general, IP address selection depends on the connected wired Ethernet device(s). Before connecting to an existing LAN, consult your network administrator.

By default, the Operating Mode is set to “Client” and the Device Mode is set to “Bridge.” When in Bridge mode, the module’s wired and wireless IP address is the same—only one IP address is required. If the Device mode is changed to “Router” the page displays two IP addresses, one for Ethernet and one for wireless. For more information on bridging networks see section “4.9 IP Routing” on page 48.



Wireless Interface:

Operating Mode	Access Point
System Address (ESSID)	Network1
Desired BSSID	00:00:00:00:00:00
Radio Encryption	None

Device Mode:

Device Mode	Bridge
Bridge STP	□
Obtain IP Address Automatically	□ (DHCP Client)
IP Address	192.168.10.100
Subnet Mask	255.255.255.0
Default Gateway	192.168.10.1

Figure 28 Network

Operating Mode

Allows you to select the operating mode for the module:

- **Access Point**—Configures the module to function as an access point
- **Client**—Configures the module to function as a client. This is the default setting.

System Address (ESSID)

A 450U-E wireless network is comprised of modules that have the same system address. Only modules with the same system address will communicate with each other. The system address is a text string from 1 to 31 characters. Select a text string that identifies your system.

Desired BSSID

To force a client or station to always connect to the same access point, enter the MAC address of that access point in the this field.

NOTE The ESSID of the access point must also match the configured ESSID of the client.

Radio Encryption

Select the desired radio encryption:

- None (default)
- WEP128 (Wired Equivalent Privacy)
- WPA2-PSK (AES) (Wi-Fi Protected Access 2)

If you select WEP encryption, you need to enter the encryption keys on the Security page (see “4.5 Security Configuration” on page 31).

If you select WPA2 encryption, you need to enter the encryption password in the next field.

WPA Passphrase

If you selected “WPA2-PSK (AES)” as the radio encryption you need to enter a passphrase to be used for WPA encryption. The passphrase must be between 8 and 63 characters, and the passphrase must be the same for all 450U-E modules in the same system. For optimal security, consider using a passphrase consisting of a combination of letters and numbers (not just a simple word or phrase), as well as upper and lower case. For example, “WiReLeSs TeChNoLoGy 2010”.

For more information on WPA2, see “WPA2 Encryption” on page 32.

Device Mode

Allows you to choose whether the module will function as a bridge or router. When “Router” is selected, separate IP addresses and netmasks are required for the Ethernet and wireless interfaces. By default this is set to “Bridge.”

Bridge STP

Selecting this checkbox enables Spanning Tree protocol in bridged networks. For more information, see “Bridge STP” on page 30.

Obtain IP Address Automatically

Selecting this checkbox enables DHCP client on the 450U-E. A DHCP client requests its IP address from a DHCP server, which assigns the IP address automatically. For more information, see “DHCP Client Configuration” on page 31. By default, this option is deselected.

IP Address

Enter the IP address required by the selected device mode:

- **Bridge Mode**—The IP address of the 450U-E module. Both wired (Ethernet Interface) port and wireless (Wireless Interface) ports will take on this address.
- **Router Mode**—Separate IP addresses are required for each interface. IP addresses must be different.

IP Subnet Mask

Enter the IP network mask of the 450U-E module. This should be set to the appropriate subnet mask for your system (typically, 255.255.255.0). In Router mode, each interface will have its own netmask.

Default Gateway	This is the address that the device will use to forward messages to remote hosts that are not connected to any of the local bridged network (Ethernet or Wireless). The default gateway address is only required if the wired LAN has a gateway unit that connects to devices beyond the LAN (for example, Internet access). If there is no gateway on the LAN, set the default gateway address to the same address as the modules IP Address as configured above.
Save Changes	Save changes to non-volatile memory. The module will need to be restarted before the changes take effect.
Save Changes and Reset	Save settings to non-volatile memory, and reboot the 450U-E module. Once the module has completed the reboot sequence, all changes are in effect.

Device Mode

The Device Mode field on the Network page allows you to configure the 450U-E as either a bridge and a router. When "Router" is selected, the screen displays a separate IP address for each interface (Ethernet and wireless). The default mode is "Bridge" which only requires one interface IP address.

- **Bridge Operation**—A bridge connects several Ethernet networks together, and makes them appear as a single Ethernet network to higher protocol layers. By default, the 450U-E is configured as a transparent bridge. When a transparent bridge is started, it learns the location of other devices by monitoring the MAC address of all incoming traffic. Initially it forwards all traffic between the wired Ethernet port and the wireless port. However, by keeping a list of devices heard on each port, the transparent bridge can decide which traffic must be forwarded between ports, and it will only transfer a message from the wired port to the wireless port if it is required.

  A bridge will forward all broadcast traffic between the wired and wireless ports. If the wired network is busy with broadcast traffic, the radio network on the 450U-E can be unnecessarily overburdened. Use filtering to reduce broadcast traffic sent over the radio. For information on creating filters, see "4.10 Filtering" on page 49.

  By default, a transparent bridge does not handle loops within the network. There must be a single path to each device on the network. Loops in the network will cause the same data to be continually passed around that loop. Redundant wireless links may be set up by enabling the bridge Spanning Tree Protocol (see "Bridge STP" on page 30 for details).

- **Router Operation**—(Routed network.) A router joins separate IP sub-networks together. The router has different IP addresses on its wired and wireless ports, reflecting the different IP addresses of the separate Ethernet subnetworks. All of the devices in these separate networks identify the router by IP address as their gateway to the other network. When devices on one network want to communicate with devices on the other network, they direct their packets to the router for forwarding.

  Because the router has an IP address on each of the networks that it joins, it inherently knows the packet identity. If the traffic directed at the router cannot be identified for any of the networks to which it is connected, the router must consult its routing rules as to where to direct the traffic. For details on configuring routing rules, see "4.9 IP Routing" on page 48.

Bridge STP

The bridge Spanning Tree Protocol function was introduced to handle network loops and provide redundant paths in networks. To enable this option, select the Bridge STP checkbox on the Network configuration page.

Consider the network in Figure 29, which has a redundant wireless link. If the bridge Spanning Tree Protocol is enabled, one of the two wireless links will be disabled, and all wireless data will be transferred by one link only. If the active link fails, the other link will automatically start transferring the wireless data.

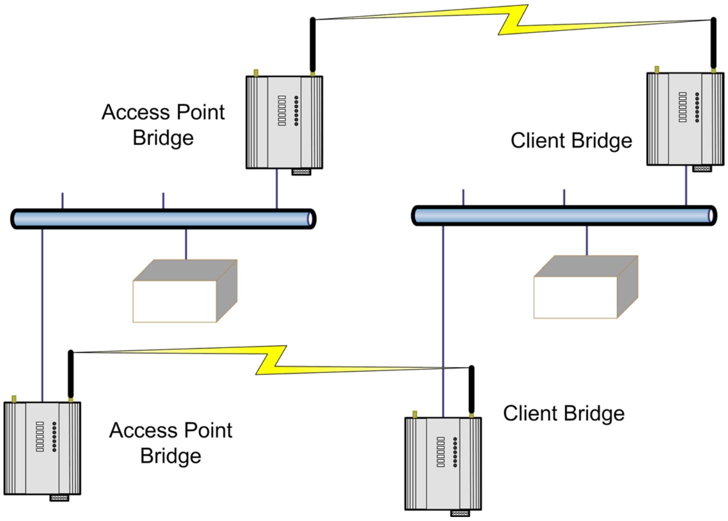


Figure 29 Spanning Tree Protocol

The Spanning Tree Protocol implemented is IEEE 802.1d compatible. The algorithm forms a loop-free network by blocking traffic between redundant links in the network. These blocked links are placed in a standby condition, and may be automatically enabled to repair the network if another link is lost. The Spanning Tree algorithm maintains a single path between all nodes in a network, by forming a tree-like structure.

The Bridge Priority field only becomes visible when the Bridge STP option is enabled. The bridge priority determines where the node sits in the tree. A bridge configured with the lowest priority (0) will become the root node in the network, and will direct traffic between each of its branches. The root node is typically the unit that handles the majority of traffic in the network. By default, the 450U-E is configured with a bridge priority of 32768. The intention is to reduce the amount of traffic that the 450U-E must handle by placing it at the “branch” level in the network tree. As a branch, the 450U-E need only pass traffic to devices that are its “leaves.”

There is some overhead in maintaining a network using the Spanning Tree algorithm. Users wanting to increase their throughput at the expense of redundancy should disable Spanning Tree. The Spanning Tree Protocol can be configured on the Repeaters configuration page (see “4.8 Repeaters” on page 44).

DHCP Client Configuration

DHCP (Dynamic Host Configuration Protocol) allows DHCP clients to automatically obtain their IP address at start-up. This simplifies network administration because there is no need to manually configure each device with a separate IP address. The 450U-E is able to act as a DHCP client. To set the 450U-E to acquire its IP address from a DHCP server, select the Obtain IP Address Automatically checkbox on the Network Configuration page. When configured as a DHCP client, the device name on the Module Information page will be the module identifier (since the IP address will be unknown), and therefore should be given a unique name.

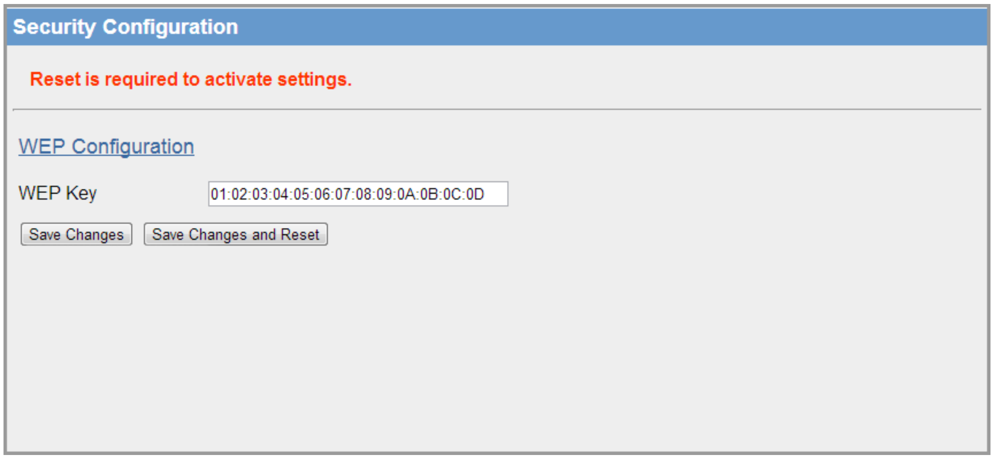
4.5 Security Configuration

To configure security, select the desired radio encryption method on the **Network** page (see “4.4 Network Configuration” on page 28), and then click **Save Changes**. Next, use the **Security** page to enter the encryption key (WEP) or passphrase (WPA2) and click **Save Changes and Reset** to save the settings and restart the module.

The following sections describe the Security pages for WEP configuration (Figure 30) and WPA2 configuration (Figure 31).

WEP - 128-bit Encryption

WEP128 (Wired Equivalent Privacy) encryption is the weakest encryption method, defined by the original IEEE802.11 standard, and uses a 104-bit key with a 24-bit initialization vector to give a 128-bit WEP encryption level. WEP is not considered an effective security scheme, and should only be used if it is necessary to inter-operate with other equipment that does not support more modern encryption methods.



Security Configuration

Reset is required to activate settings.

WEP Configuration

WEP Key 01:02:03:04:05:06:07:08:09:0A:0B:0C:0D

Figure 30 WEP Configuration

WEP Key Enter the WEP encryption keys that will be used to encrypt radio data to protect data from unwanted eavesdroppers when WEP encryption is selected. This key should be the same for all 450U-E modules in the same system.

The WEP key must be entered as pairs of hexadecimal digits, separated by colons. Hexadecimal digits are in the range 0–9 and A–F. 128-bit WEP encryption requires 26 hexadecimal digits. For example, 12:AB:EF:00:56:15:6B:E4:30:C8:05:F0:8D. Encryption keys must not be all zeros (00:00:00:00:00).

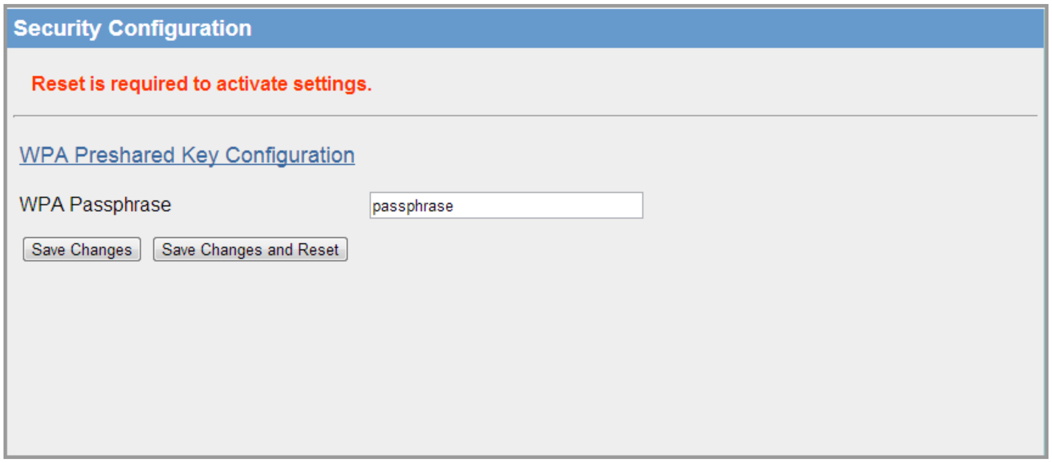
Save Changes Save changes to non-volatile memory. The module will need to be restarted before the changes take effect.

Save Changes and Reset Save settings to non-volatile memory, and reboot the 450U-E module. Once the module has completed the reboot sequence, all changes are in effect.

WPA2 Encryption

WPA2-PSK, AES, (Wi-Fi Protected Access 2) encryption has replaced WPA and provides significant security improvements over this method. In particular, it introduces CCMP, a new Advanced Encryption Standard (AES) based encryption mode with strong security. WPA2 AES is the most secure encryption method, and is also based on 128-bit encryption key.

When WPA encryption is selected on the Network page, the 128-bit encryption keys are internally generated based on the passphrase and system address (ESSID) you enter. The passphrase can be entered on the Network page or the on the Security configuration page (Figure 31).



Security Configuration

Reset is required to activate settings.

WPA Preshared Key Configuration

WPA Passphrase	passphrase

Figure 31 WPA2 Configuration

WPA Passphrase Enter a passphrase to be used for WPA encryption. The passphrase must be between 8 and 63 characters, and the passphrase must be the same for all 450U-E modules in the same system. For optimal security, consider using a passphrase consisting of a combination of letters and numbers (not just a simple word or phrase), as well as upper and lower case. For example, "WiReLeSs TeChNoLoGy 2010".

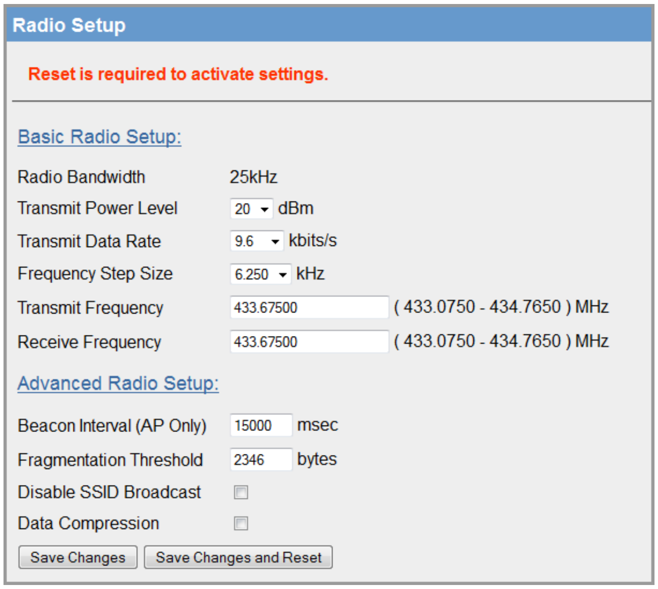
Save Changes Save changes to non-volatile memory. The module will need to be restarted before the changes take effect.

Save Changes and Reset Save settings to non-volatile memory, and reboot the 450U-E module. Once the module has completed the reboot sequence, all changes are in effect.

4.6 Radio Configuration

When you initially configure a new 450U-E, you must specify the radio configuration settings for your country of operation and license. The factory default parameters of the radio are set to values that allow the radio to be powered up safely without interfering with radio equipment that may be available in the country of operation (transmit and receive frequencies will be set to zero).

After initial configuration, you can adjust available radio parameters by clicking **Radio** on the menu to display the page in Figure 32.



Radio Setup

Reset is required to activate settings.

Basic Radio Setup:

Radio Bandwidth	25kHz
Transmit Power Level	20 dBm
Transmit Data Rate	9.6 kbits/s
Frequency Step Size	6.250 kHz
Transmit Frequency	433.67500 (433.0750 - 434.7650) MHz
Receive Frequency	433.67500 (433.0750 - 434.7650) MHz

Advanced Radio Setup:

Beacon Interval (AP Only)	15000 msec
Fragmentation Threshold	2346 bytes
Disable SSID Broadcast	□
Data Compression	□

Figure 32 Radio Configuration

Radio Bandwidth The bandwidth of the radio is set at the factory, and is either 12.5 kHz (narrow band) or 25 kHz (wide band).

Transmit Power Level Allows you to adjust the radio power. Do not set the radio power above the allowed setting for your country or radio license. You can reduce the power for short range applications, or to allow the use of high gain transmitter antennas while still complying with the emission requirements of your license. See Appendix F for dBm-to-mW conversion.

Transmit Data Rate You can configure the 450U-E module for different radio transmission rates. The radio baud rate is displayed in kilobits per second (Kbps) for point-to-point radio transmissions. Select a fixed rate for the radio to use from the drop-down list.

The selections available are 9600 and 19200 Kbps for 25-kHz wide band or 4800 and 9600 Kbps for 12.5-kHz narrow band. The transmit data rate only applies to transmit messages—the radio can receive on either data rate.

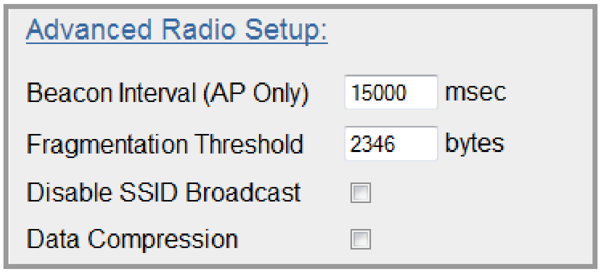
⚠ **NOTE Reducing in the configured data rate may increases the reliable range of the module (transmission distance).**

Frequency Step Size The frequency step size is the spacing between frequencies that you can select when configuring the TX and RX frequencies. The steps sizes available are 5 kHz or 6.25 kHz.

Transmit Frequency Sets the frequency for the radio transmitter. Frequency options will be in multiples of the frequency step configured in the Frequency Step Size field. For example, 450.00500, 450.01000, 450.01500, 450.02000 (and so on) for a frequency step size of 5 kHz, or 450.00625, 450.01250, 450.01875, 450.02500 (and so on) for a frequency step size of 6.25 kHz.

Receive Frequency Sets the frequency for the radio receiver. Frequency options will be in multiples of the frequency step size configured in the Frequency Step Size field. For example, 450.00500, 450.01000, 450.01500, 450.02000 (and so on) for a frequency step size of 5 kHz, or 450.00625, 450.01250, 450.01875, 450.02500 (and so on) for a frequency step size of 6.25 kHz.

The following are advanced radio parameters, and care should be taken when making changes to these settings.



Advanced Radio Setup:

Beacon Interval (AP Only) 15000 msec

Fragmentation Threshold 2346 bytes

Disable SSID Broadcast □

Data Compression □

Figure 33 Advanced Radio Parameters

Beacon Interval (AP only.) This interval is the period between beacon transmissions sent by an access point. The default value is 15 seconds, and may be adjusted from 1 to 60 seconds. Reducing the beacon interval will increase the amount of radio messages in the system, which could compromise normal communications. Do not change this setting unless advised by an ELPRO Systems Engineer.

Fragmentation Threshold (Client Stations only.) The maximum transmission unit (MTU) of data over the radio. If more than this number of bytes is input into the module, it will be transmitted in more than one message (or fragmented).

Disable SSID Broadcast (AP only.) This option is used to reduce bandwidth eavesdroppers from detecting the radio network system address (SSID) by passively listening to beacon transmissions from the access point. When disabled, access points will not transmit the system address openly in beacon messages. This is particularly useful in unencrypted radio networks and where all stations know the SSID of the access point.

Data Compression Allows you to enable or disable data compression. For details, see the following section, “Data Compression.”

Save Changes Save changes to non-volatile memory. The module will need to be restarted before the changes take effect.

Save Changes and Reset Save settings to non-volatile memory, and reboot the 450U-E module. Once the module has completed the reboot sequence, all changes are in effect.

Data Compression

The radios incorporate a data compression algorithm based on RFC1951 specifications. This algorithm is similar to the one used in file compression utilities, such as PKZip, which simply matches duplicate strings within the data frame with pointers to previous data patterns. The algorithm keeps a running image of previous received data frames which it uses to compare with the current data frame. When it finds a data string that is the same as a previous data string, a pointer to this location is sent instead of the data. Depending on the data, this could considerably reduce the amount of data that needs to be sent.

Performance is dependent on the type of data frames that are being sent. Typical improvements in throughputs that can be expected when compression is enabled are:

- 15–40% improvement if using Modbus, depending on the radio baud rate
- 70% improvement for webpage download
- 40% improvement if using FTP download

4.7 Serial Configuration

Click **Serial** on the menu to configure the onboard serial ports. The 450U-E has one RS-232 port and one RS-485 port available for serial communications with other devices. These ports are completely independent of each other and can be configured for different functions and can even be used at the same time.

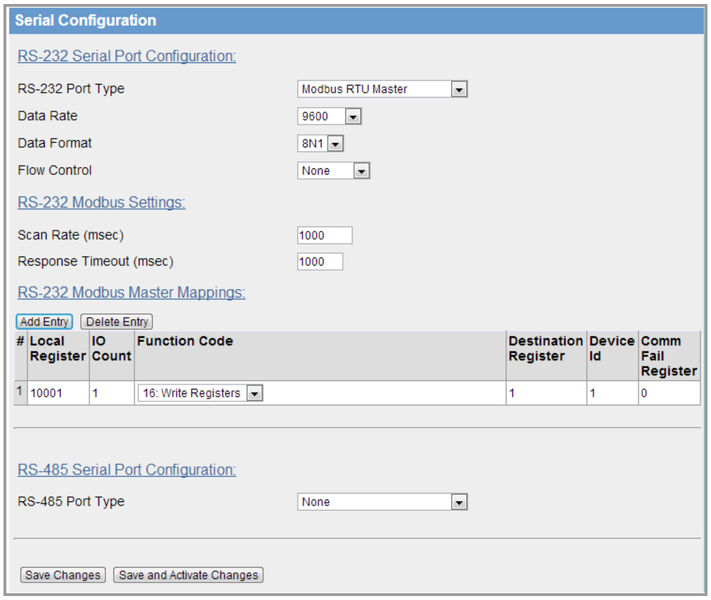
The 450U-E offers five port types. Each port is configured separately by selecting the port type from the drop down list on the Serial Configuration page and then configuring the appropriate parameters.

The the five port types are:

- **Modbus RTU Master—**This type should be selected when the port is operating as a Modbus Master, that is, when Modbus RTU slave devices are connected directly to the serial port. Modbus mappings will need to be configured in the table provided. For details, see “Modbus RTU Master.”
- **Expansion I/O—**This type should be selected when ELPRO Serial Expansion modules (115S-XX) are connected to the modem. For details, see “Expansion I/O.”
- **Modbus RTU Slave—**This type should be selected if the port is being used as a Modbus RTU slave, that is, the module it is being connected to/from a Modbus Master (such as DCS, or SCADA) via the serial port. For details, see “Modbus RTU Slave.”
- **Serial Gateway—**This type should be selected if you want to allow point-to-point or point-to-multipoint transparent serial data transfers. For details, see “Serial Gateway.”
- **Modbus TCP/RTU Converter—**This port type allows Modbus TCP to Modbus RTU conversion. For details, see “Modbus TCP/RTU Converter.”

Modbus RTU Master

To configure a serial port as a Modbus RTU Master, click **Serial** on the menu and select **Modbus RTU Master** from the Port Type drop-down list (see Figure 34). Configure the parameters described below.



Serial Configuration

RS-232 Serial Port Configuration:

RS-232 Port Type: Modbus RTU Master

Data Rate: 9600

Data Format: 8N1

Flow Control: None

RS-232 Modbus Settings:

Scan Rate (msec): 1000

Response Timeout (msec): 1000

RS-232 Modbus Master Mappings:

#	Local Register	IO Count	Function Code	Destination Register	Device Id	Comm Fail Register
1	10001	1	16: Write Registers	1	1	0

RS-485 Serial Port Configuration:

RS-485 Port Type: None

Figure 34 Serial Configuration - Modbus RTU Master

Port Type Select **Modbus RTU Master** from the drop down list.

Data Rate Select the serial data rate that matches the data rate of the serial device that is connected and communicating via the port. Baud rates range from 110 to 230400 baud.

Data Format Defines the data bits, parity and start/stop bits used to communicate with the serial device.

Flow Control Flow control is used by some serial devices to regulate the flow of data by turning on or off flags that are used to tell the connected serial devices to start or stop transmitting data. The RS-232 supports CTC/RTS hardware flow control.

Scan Rate How frequently the slave device will be polled. Default is 100 msec.

Response Timeout Number of milliseconds that the RTU Master/TCP client will wait for a slave to respond to a poll.

Modbus Master Mapping Table

Click **Add Entry** and specify the following mapping parameters:

- **Local Register**—Enter the starting onboard I/O register number that the specified Modbus Master transaction will transfer I/O to/from, depending on whether it is a read or a write mapping.
- **I/O count**—Specify the number of consecutive I/O register that will be transferred in the mapping.
- **Function Code**—Modbus function code used for the transaction. Standard function codes are:
    - **01: Read Coil**—Read from a Coil (Output) register.
    - **02: Read Discretes**—Read from a Discrete Input register.
    - **03: Read Registers**—Read from an Analog Output register.
    - **04: Read Inputs**—Read from an Analog Input register.
    - **15: Write Coils**—Write to a Coil (output) register.
    - **16: Write Registers**—Write to an Analog Output register.
- **Destination Register**—Enter the starting I/O register number in the destination device that the Modbus mapping will transfer I/O to/from.
- **Device ID**—Enter the Modbus device ID of the destination device
- **Comms Fail Register**—Enter the onboard local I/O register number to store the communication status for the specified mapping. The register will be set to one of the following:
    - 0 if communications is successful
    - 0xFFFF if there is no connection to the specified server
    - 0xFFxx where “xx” is the Modbus Exception Code (see Appendix E for information on the codes).

Add Entry Adds an entry to the Modbus Master Mappings table.

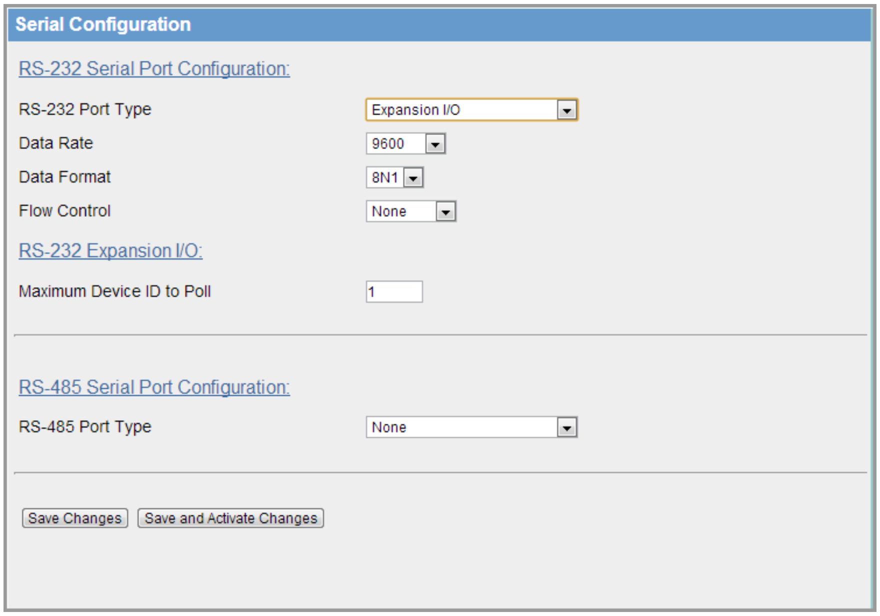
Delete Entry Deletes an selected entry from the Modbus Master Mappings table.

Save Changes Save changes to non-volatile memory.

Save and Activate Changes Save changes to non-volatile memory and activate the process.

Expansion I/O

To configure a serial port for an expansion I/O device, click **Serial** on the menu and select **Expansion I/O** from the Port Type drop-down list (see Figure 35). Configure the parameters described below.



Serial Configuration

RS-232 Serial Port Configuration:

RS-232 Port Type: Expansion I/O

Data Rate: 9600

Data Format: 8N1

Flow Control: None

RS-232 Expansion I/O:

Maximum Device ID to Poll: 1

RS-485 Serial Port Configuration:

RS-485 Port Type: None

Figure 35 Serial Configuration - Expansion I/O

Port Type Select **Expansion I/O** from the drop down list.

Data Rate Select the data rate to match that of the serial device that is connected and communicating via the port. Baud rates available from 110 to 230400 baud.

Data Format Defines the number of data bits, parity and start/stop bits used to communicate with the serial device.

Flow Control Flow control is used by some serial devices to regulate the flow of data by turning on/off flags that are used to tell the connected serial devices to start or stop transmitting data. The RS-232 supports CTC/RTS hardware flow control.

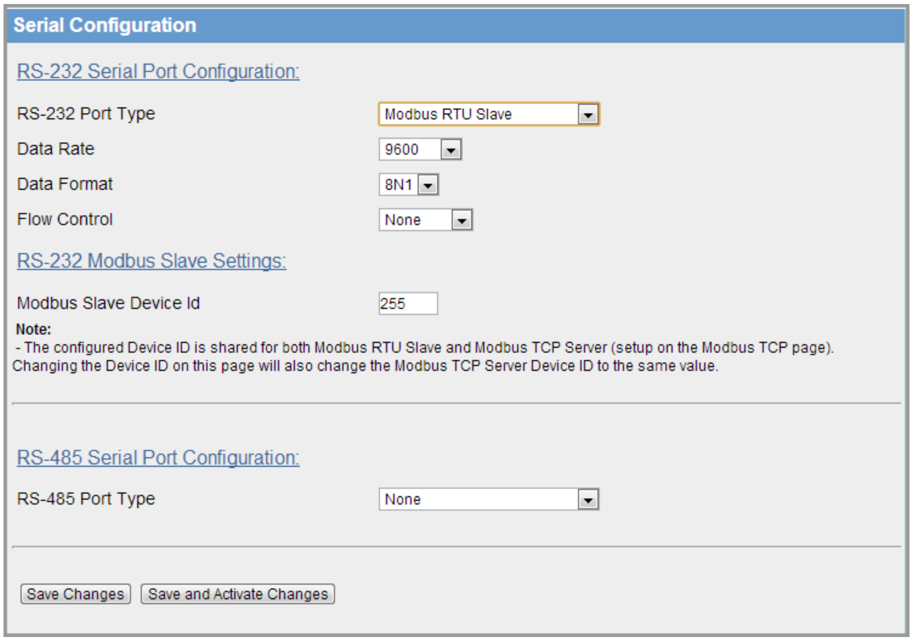
Maximum Device ID to Poll The maximum number of Modbus addresses that will be polled on the serial interface. The default for RS-232 is one. Three addresses will be polled on the RS-485.

Save Changes Save changes to non-volatile memory.

Save and Activate Changes Save changes to non-volatile memory and activate the process.

Modbus RTU Slave

To configure a serial port as a Modbus RTU slave, click **Serial** on the menu, and then select **Modbus RTU Slave** from the Port Type drop-down list (see Figure 36). Configure the parameters described below.



Serial Configuration

RS-232 Serial Port Configuration:

RS-232 Port Type: Modbus RTU Slave

Data Rate: 9600

Data Format: 8N1

Flow Control: None

RS-232 Modbus Slave Settings:

Modbus Slave Device Id: 255

Note:
- The configured Device ID is shared for both Modbus RTU Slave and Modbus TCP Server (setup on the Modbus TCP page). Changing the Device ID on this page will also change the Modbus TCP Server Device ID to the same value.

RS-485 Serial Port Configuration:

RS-485 Port Type: None

Figure 36 Serial Configuration - Modbus RTU Slave

Port Type Select **Modbus RTU Slave** from the drop down list.

Data Rate Select the serial data rate to match that of the serial device that is connected and communicating via the port. Baud rates available from 110 to 230400 baud.

Data Format Defines the number of data bits, parity and start/stop bits used to communicate with the serial device.

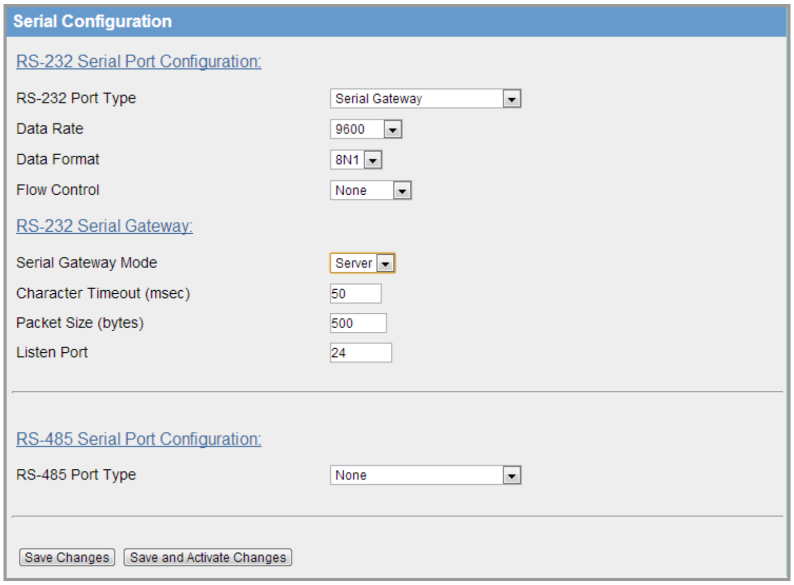
Flow Control Flow control is used by some serial devices to regulate the flow of data by turning on/off flags that are used to tell the connected serial devices to start or stop transmitting data. The RS-232 supports CTC/RTS hardware flow control.

Modbus Slave Device ID Address of the onboard Modbus RTU slave/TCP server. This is the address that will be polled by an external Modbus master/TCP client. Default address is 255 and can be set here or on the Modbus TCP page.

Save Changes and Activate Save changes to non-volatile memory and activate the process.

Serial Gateway

To configure the port to allow point-to-point or point-to-multipoint transparent serial data transfers, click **Serial** on the menu, and then select **Serial Gateway** from the Port Type drop-down list on the Serial Configuration page. Configure the parameters described below. Note that different fields are presented depending on whether you select the gateway mode as "Server" (Figure 36), or "Client" (Figure 38).



Serial Configuration

RS-232 Serial Port Configuration:

RS-232 Port Type	Serial Gateway
Data Rate	9600
Data Format	8N1
Flow Control	None

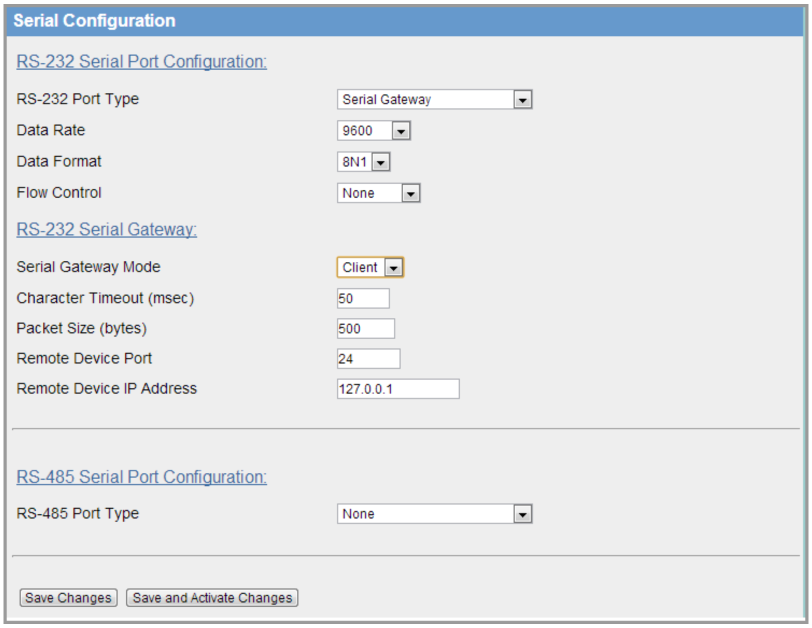
RS-232 Serial Gateway:

Serial Gateway Mode	Server
Character Timeout (msec)	50
Packet Size (bytes)	500
Listen Port	24

RS-485 Serial Port Configuration:

RS-485 Port Type	None

Figure 37 Serial Configuration - Serial Gateway - Server Mode



Serial Configuration

RS-232 Serial Port Configuration:

RS-232 Port Type	Serial Gateway
Data Rate	9600
Data Format	8N1
Flow Control	None

RS-232 Serial Gateway:

Serial Gateway Mode	Client
Character Timeout (msec)	50
Packet Size (bytes)	500
Remote Device Port	24
Remote Device IP Address	127.0.0.1

RS-485 Serial Port Configuration:

RS-485 Port Type	None

Figure 38 Serial Configuration - Serial Gateway - Client Mode

Port Type Select **Serial Gateway** from the drop down list.

Data Rate Select the data rate to match that of the serial device that is connected and communicating via the port. Baud rates available from 110 to 230400 baud.

Data Format Defines the number of data bits, parity and start/stop bits used to communicate with the serial device.

Flow Control Flow control is used by some serial devices to regulate the flow of data by turning on/off flags that are used to tell the connected serial devices to start or stop transmitting data. The RS-232 supports CTC/RTS hardware flow control.

Serial Gateway Mode

- **Server**—When configured as a server, the modem will wait for a TCP connection to be initiated by a remote client.
- **Client**—When configured as a client, the modem will automatically attempt to connect to a specific remote server that matches the configured device IP address and port

Character Timeout Enter the maximum delay (in msec) between receiving the last serial character on the serial port and the radio transmitting the whole packet. Data will be sent when this time is exceeded.

Packet Size The Maximum number of received bytes that will be buffered before the packet is sent. Data will be sent when packet size is exceeded.

Listen Port Only available when "Server" is selected as the Serial Gateway Mode. Enter a TCP port number on which the server must listen for incoming connections. Default is 24.

Remote Device Port Only available when "Client" is selected as the Serial Gateway Mode. Enter the TCP port number configured on the Listen Port of the remote Server. Default will be 24

Remote Device IP Address Only available when "Client" is selected in the Serial Gateway Mode. Enter the IP address of the remote server you want to communicate with.

Save Changes Save changes to non-volatile memory.

Save Changes and Activate Save changes to non-volatile memory and activate the process.

Modbus TCP/RTU Converter

The Modbus TCP/RTU converter function of the 450U-E allows an Ethernet Modbus TCP client (master) to communicate with a serial Modbus RTU slave. The 450U-E makes this possible by internally performing the necessary protocol conversion. The conversion is always performed by the 450U-E that is directly connected to the Modbus serial device. Only this module needs to have Modbus TCP/RTU Conversion enabled.

Figure 39 demonstrates how a Modbus/TCP client (master) can connect to one or more Modbus RTU slave devices. In this example the 450U-E access point is configured with the RS-232 serial port set for "Modbus TCP/RTU Converter." When configured with this Port Type, the module converts the Modbus/TCP query from the client into a Modbus RTU frame and forwards it out the appropriate serial port to the slave device. When the serial device responds the query is received on the serial port, it is then converted into a Modbus/TCP response and forwarded via the network to the Modbus/TCP client.

The Modbus TCP/RTU Converter may be configured to operate on either the RS-232 or RS-485 port.

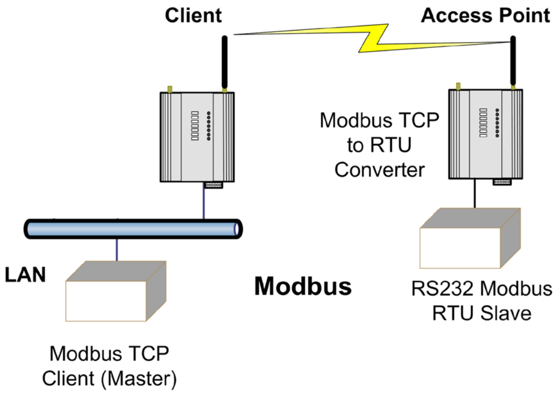
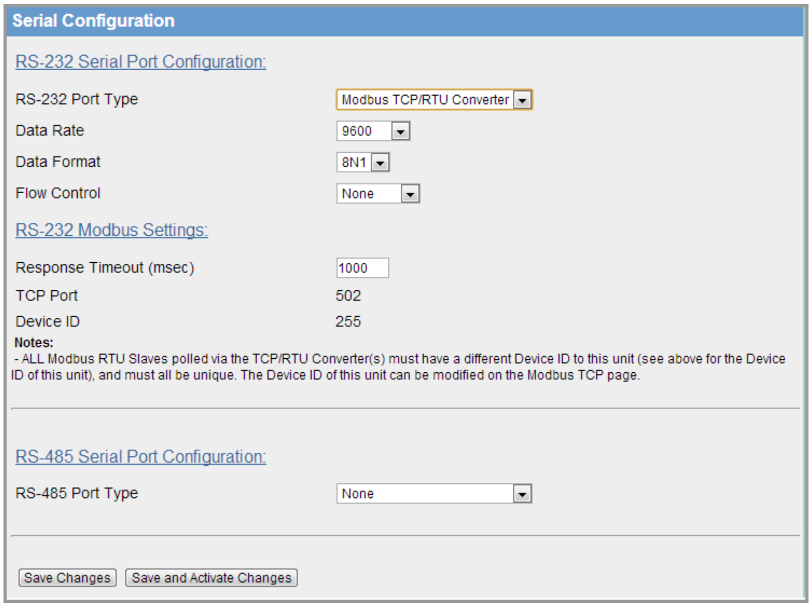


Figure 39 Modbus TCP/RTU Converter

To configure a serial port to allow Modbus TCP to Modbus RTU conversion, click **Serial** on the menu and select **Modbus TCP/RTU Converter** from the Port Type drop-down list (see Figure 40). Configure the parameters described below.



Serial Configuration

RS-232 Serial Port Configuration:

RS-232 Port Type: Modbus TCP/RTU Converter

Data Rate: 9600

Data Format: 8N1

Flow Control: None

RS-232 Modbus Settings:

Response Timeout (msec): 1000

TCP Port: 502

Device ID: 255

Notes:
- ALL Modbus RTU Slaves polled via the TCP/RTU Converter(s) must have a different Device ID to this unit (see above for the Device ID of this unit), and must all be unique. The Device ID of this unit can be modified on the Modbus TCP page.

RS-485 Serial Port Configuration:

RS-485 Port Type: None

Figure 40 Serial Configuration - Modbus TCP/RTU Converter

Port Type Select Modbus TCP/RTU Converter from the drop down list.

Data Rate Select the data rate to match that of the serial device that is connected and communicating via the port. Baud rates available from 110 to 230400 baud.

Data Format Defines the number of data bits, parity and start/stop bits used to communicate with the serial device.

Flow Control Flow Control is used by some serial devices to regulate the flow of data by turning on/off flags that are used to tell the connected serial devices to start or stop transmitting data. The RS-232 supports CTC/RTS hardware flow control.

Response Timeout The amount of time the TCP/RTU Converter waits for a response from the slave before sending the next poll.

TCP Port Fixed to 502.

Device ID Address of the onboard Modbus RTU slave/TCP server. This is the address that will be polled by the Modbus master/TCP client. Default address is 255, and cannot be changed on this page. To modify this address, use the Modbus I/O page (see “4.11 Modbus TCP” on page 54).

Save Changes Save changes to non-volatile memory.

Save Changes and Activate Save changes to non-volatile memory and activate the process.

Modbus RTU Mappings Example

The system in Figure 41 shows that Unit B is a Modbus RTU master that is configured to poll the RTU slave device at Unit A via the serial interface and read the status of eight onboard I/O registers, which will then be reflected to eight local I/O registers at Unit B.

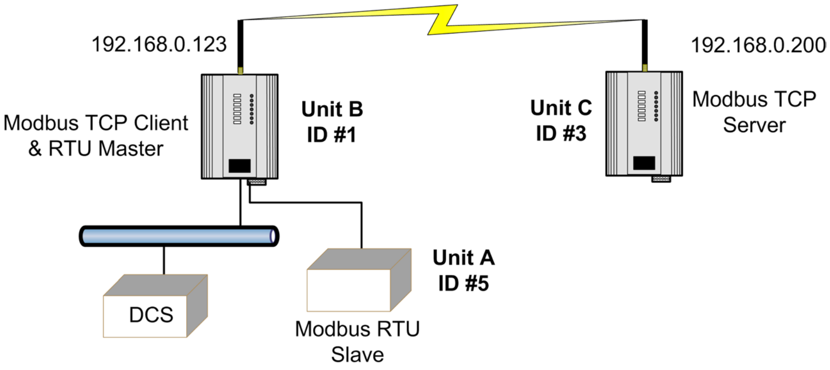
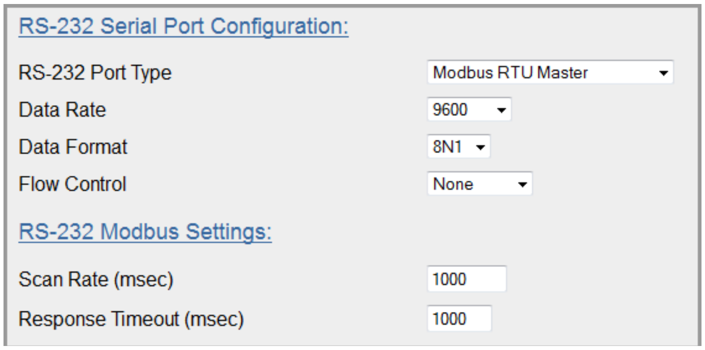


Figure 41 Modbus Example

Figure 42 shows the serial configuration for Unit B:

- Modbus RTU Master needs to be selected as the Port Type of the serial port that will be used to communicate with the slave device.
- The serial data rate, data format and flow control need to match that of the device and then the scan rate and response time need to be appropriate for the application.
- The scan rate in this example is set for 1 second and it will also wait 1 second for a response from the slave before flagging a Comms Failure.



RS-232 Serial Port Configuration:

RS-232 Port Type	Modbus RTU Master
Data Rate	9600
Data Format	8N1
Flow Control	None

RS-232 Modbus Settings:

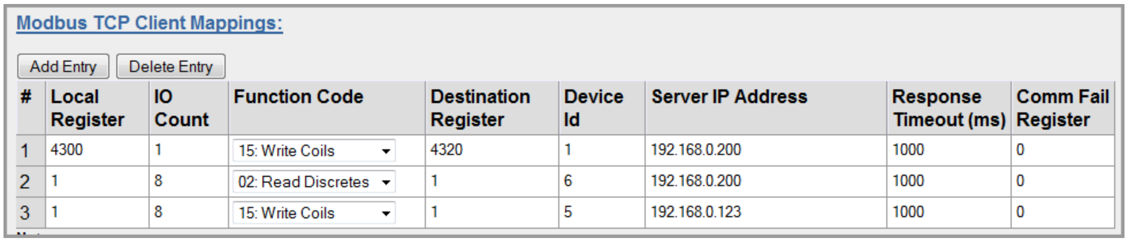
Scan Rate (msec)	1000
Response Timeout (msec)	1000

Figure 42 Modbus RTU Serial Port Configuration

Because the Unite B module is also communicating with a Modbus RTU slave device (Device #5) it will need to have an RTU Master Mapping configured. In the RTU mapping example in Figure 43, Unit B Modbus RTU mapping is configured to read 8 x discrete values starting at register 501 from a Modbus slave device ID #5 connected to the RS-232 port and store the values at its own local internal register 501.

- Local Register (501) specifies a general purpose Bit Storage area in the local module (Unit B).
- I/O Count (8) specifies that it is passing 8 I/O points.
- Function Code “02: Read Discretes” specifies the standard Modbus function code to read a digital input.
- Destination Register (501) specifies the register location on the remote Modbus RTU Slave (Unit A).
- Device ID (5) is the Device ID of the Modbus RTU Slave at Unit A.
- Comms Fail Register (509) is the local Register location that will indicate a communication failure for this mapping.

NOTE Care should be taken to ensure that the device ID (Modbus address) of the remote serial device is different from the device ID of the onboard Modbus TCP server (if its enabled, the TCP server only needs to be enabled if the I/O registers are to be read from another external TCP client).



Modbus TCP Client Mappings:

#	Local Register	IO Count	Function Code	Destination Register	Device Id	Server IP Address	Response Timeout (ms)	Comm Fail Register
1	4300	1	15: Write Coils	4320	1	192.168.0.200	1000	0
2	1	8	02: Read Discretes	1	6	192.168.0.200	1000	0
3	1	8	15: Write Coils	1	5	192.168.0.123	1000	0

Figure 43 RS-232 Modbus Master Mappings

4.8 Repeaters

Wireless networks can be extended by allowing access points to behave as repeaters and forward traffic to other access points. Access point to access point communications is also known as WDS (Wireless Distribution System). The 450U-E offers very powerful WDS configuration, allowing mesh network technology with self-healing functionality. Alternatively, fixed access point to access point links can be configured for optimized throughput. Each 450U-E access point supports up to three virtual access point or five virtual station/client connections to other devices.

The WDS virtual interfaces will always be bridged with the main wireless interface. A WDS bridge interface allows traffic to be bridged to another access point on the same IP network. WDS bridge interfaces do not require additional IP address configuration because they are bridged with the standard wireless interface that is used for connections to associated clients. All WDS interfaces on the one access point may be bridged, if required.

WDS bridge interfaces have the advantage that redundant paths are permitted when using the bridge Spanning Tree Protocol, thus behaving as a self-healing mesh network (see section “Bridge STP” on page 30). Bridged networks are also not as configuration-intensive as routed networks, since WDS bridge interfaces generally do not require IP address configuration (they inherit the IP address of the standard wireless interface).

Important notes:

- All access points must be configured on the same radio frequency
- Specify SSID for AP/STA modes
- SSID and encryption is not inherited from the main network page
- Each WDS interface can be configured with a different encryption algorithm, but each side of a single WDS link must specify the same encryption algorithm and keys
- A maximum of three virtual APs or five virtual client/STA applies per unit

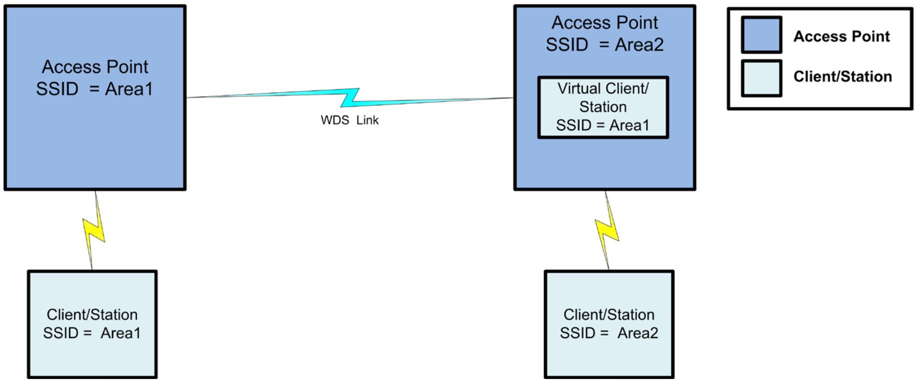
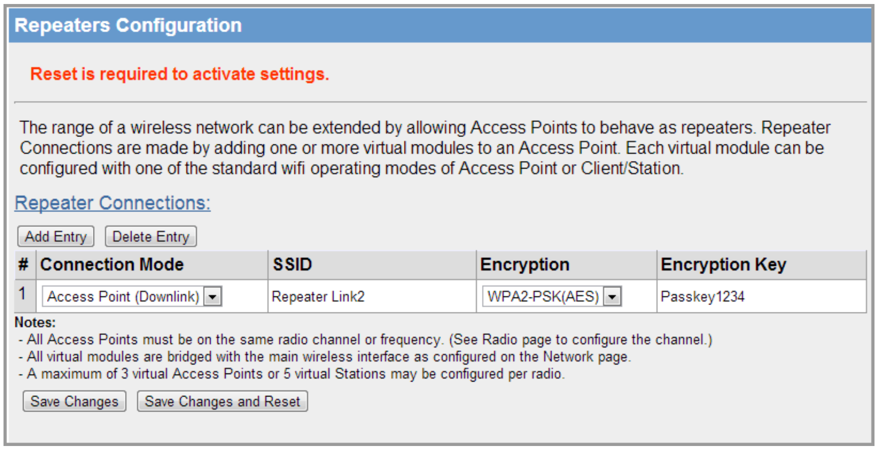


Figure 44 Repeaters

To configure an access point as a repeater, click Repeaters on the menu to display the WDS Configuration page (Figure 45).



Repeaters Configuration

Reset is required to activate settings.

The range of a wireless network can be extended by allowing Access Points to behave as repeaters. Repeater Connections are made by adding one or more virtual modules to an Access Point. Each virtual module can be configured with one of the standard wifi operating modes of Access Point or Client/Station.

Repeater Connections:

#	Connection Mode	SSID	Encryption	Encryption Key
1	Access Point (Downlink)	Repeater Link2	WPA2-PSK(AES)	Passkey1234

Notes:
- All Access Points must be on the same radio channel or frequency. (See Radio page to configure the channel.)
- All virtual modules are bridged with the main wireless interface as configured on the Network page.
- A maximum of 3 virtual Access Points or 5 virtual Stations may be configured per radio.

Figure 45 Repeaters Configuration

Add Entry	Add an entry to the WDS Connections table. This adds a virtual station to the device.

Delete Entry	Delete the currently selected entry in the WDS Connections table. To select a row, click anywhere in the row with the mouse, to highlight the entire row.

Connection Mode	Specify the connection mode for this link:

- **Access Point (Downlink)**—Configures the connection as a virtual access point.
- **Sta (Uplink)**—Configures the connection as a virtual station/client.

SSID

- **AP Mode**—Specify the SSID that this virtual access point will use. Stations connecting to this virtual access point use this SSID.
- **Sta Mode**—Specify the SSID that this virtual station will use when connecting to other access points.

Encryption	Select the required Encryption (if any) for this WDS link.

Encryption Key	Enter the Encryption key (for WEP encryption) or the passphrase (for WPA encryption). For WEP encryption, the encryption key is set as WEP Key 1. For Sta Mode, this must match WEP Key 1 on the access point this virtual client will connect to. For AP mode, clients must configure their WEP Key 1 to the same value as this key and select the Default WEP Key to be WEP Key 1.

Save Changes	Save changes to non-volatile memory. The module will need to be restarted before the changes take effect.

Save Changes and Reset	Save settings to non-volatile memory, and reboot the 450U-E module. Once the module has completed the reboot sequence, all changes are in effect.

There are many ways to setup wireless networks. Often it depends on the devices you want to connect and the existing network topology. The following sections show examples of how to connect devices into different types of systems.

Extending Range Using WDS

One of the most common uses for WDS is to extend the range of the wireless network using repeaters. The diagram in Figure 46 illustrates a simple example where the four access points are all at fixed locations. Each of the access points could, of course, have one or more client/stations connected. Since the locations are fixed, there is no chance of network loops and therefore we can avoid the overhead of using the Bridge Spanning Tree protocol by configuring fixed WDS links to ensure that each access point will only connect to the next access point in the chain. Any number of additional intermediate repeaters could be added to the chain in a similar way.

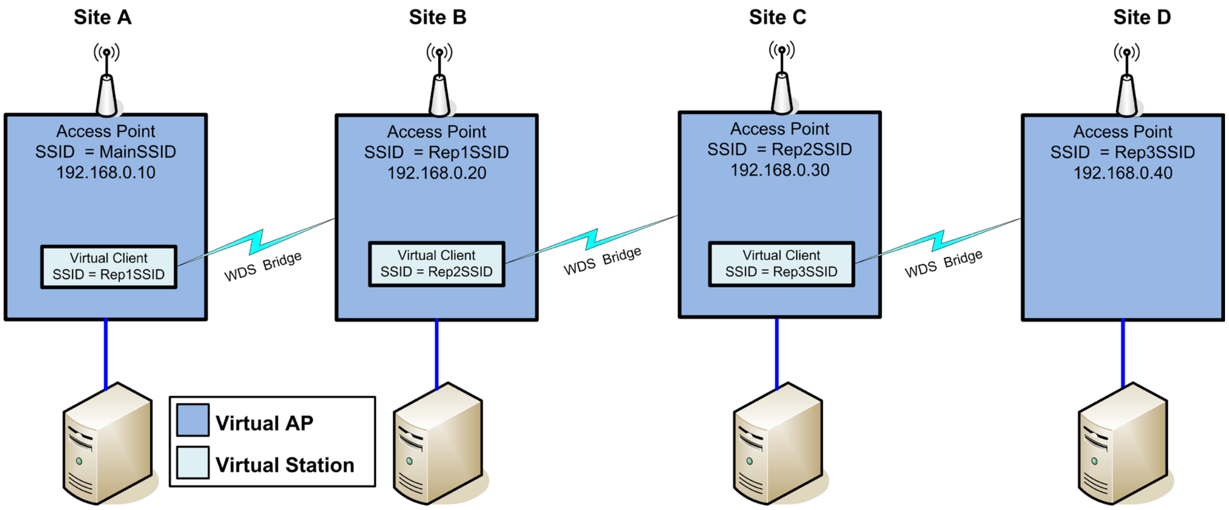
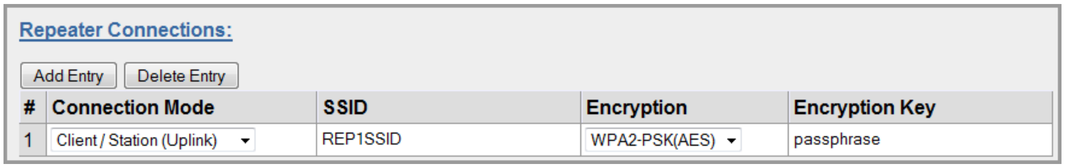


Figure 46 Extending Range

The WDS configuration is accessed by clicking **Repeaters** from the menu. Configuration for Site A is shown in Figure 47. Site A is configured with a virtual client that will connect to the access point at Site B using the SSID “REP1SSID” and WPA2 encryption with the key “passphrase”. Likewise, Site B also has a virtual client configured that connects with the access point at Site C, which also has a virtual client that connects to the access point at Site D.

In this example each virtual connection is using the same encryption method (WPA2-PSK (AES) with a key of “passphrase”. The encryption method and key can be different for each virtual link, or even disabled (no encryption). However, it is recommended that the encryption method be equal to or greater than the main system in order to maintain system security. In addition, since it is a bridged network the Spanning Tree Protocol is disabled on the Network configuration page since there is no possibility of network loops.



#	Connection Mode	SSID	Encryption	Encryption Key
1	Client / Station (Uplink)	REP1SSID	WPA2-PSK(AES)	passphrase

Figure 47 Site A Repeater Configuration

Roaming with WDS Access Points

Another common use for WDS is extending the range across a large wireless network but allowing roaming connections between access points or permitting switching to the next access point when out of range of the previous access point.

The diagram in Figure 48 shows a bridging network with a number of access points, all with the same SSID, network structure (and so on) so that the roaming client/stations can freely roam between access points. Each access point then needs a separate connection to the next access point, which is done using the WDS virtual access points and client/stations

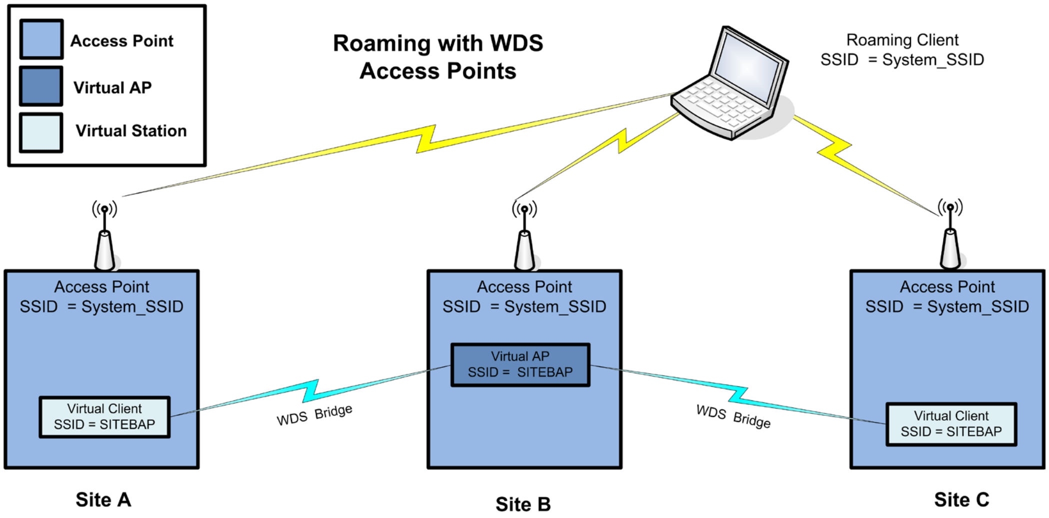
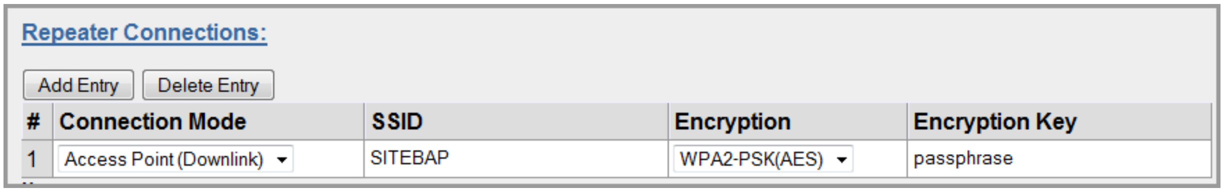


Figure 48 Roaming

The configuration for Site B is shown below in Figure 49. The WDS is configured with a virtual access point for the virtual clients configured at Sites A and C. For simplicity, the encryption method and key are configured the same as the main network.

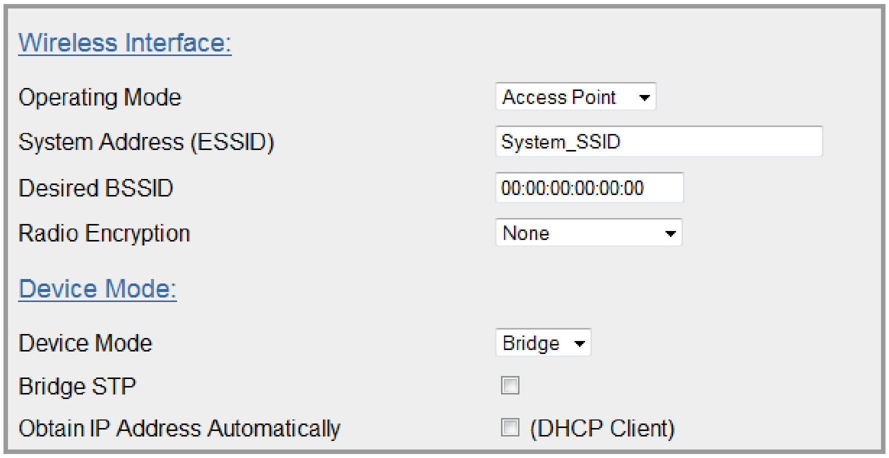


Repeater Connections:

#	Connection Mode	SSID	Encryption	Encryption Key
1	Access Point (Downlink)	SITEBAP	WPA2-PSK(AES)	passphrase

Figure 49 Site B Repeater Configuration 2

The WDS configuration for Site A and Site C will be exactly the same as Site B except the Connection Mode will need to be set to “Client/Station (Uplink)” instead of “Access Point (Downlink).” The main network configuration settings for all sites will all be the same for each site (as shown in Figure 50). This setup can be replicated many times which will allow roaming stations full connectivity across the network.



Wireless Interface:

Operating Mode	Access Point
System Address (ESSID)	System_SSID
Desired BSSID	00:00:00:00:00:00
Radio Encryption	None

Device Mode:

Device Mode	Bridge
Bridge STP	□
Obtain IP Address Automatically	□ (DHCP Client)

Figure 50 System Network Settings

4.9 IP Routing

When a 450U-E module receives an IP frame that is destined for an IP address on a different network, it checks whether the network address matches the network address of one of its own interfaces (hard-wired Ethernet, wireless Ethernet, or WDS) and forwards the frame appropriately. However, if the IP network address does not match the network address of any of its interfaces, the 450U-E will forward the frame to its default gateway. In this case, it is assumed that the default gateway has a valid route to the destination.

In some cases, it is not practical to have just one default gateway. For example, this is true in routed wireless networks with more than two 450U-E routers, and in some cases when WDS router interfaces are used. If more than one “next-hop router” is required, the 450U-E allows for up to 100 routing rules to be configured. A routing rule specifies a destination network (or host) IP address and the corresponding next-hop router that messages for the specified destination will be forwarded to. It is assumed that the next-hop router (or gateway) will then deliver the data to the required destination (or forward it on to another router that will).

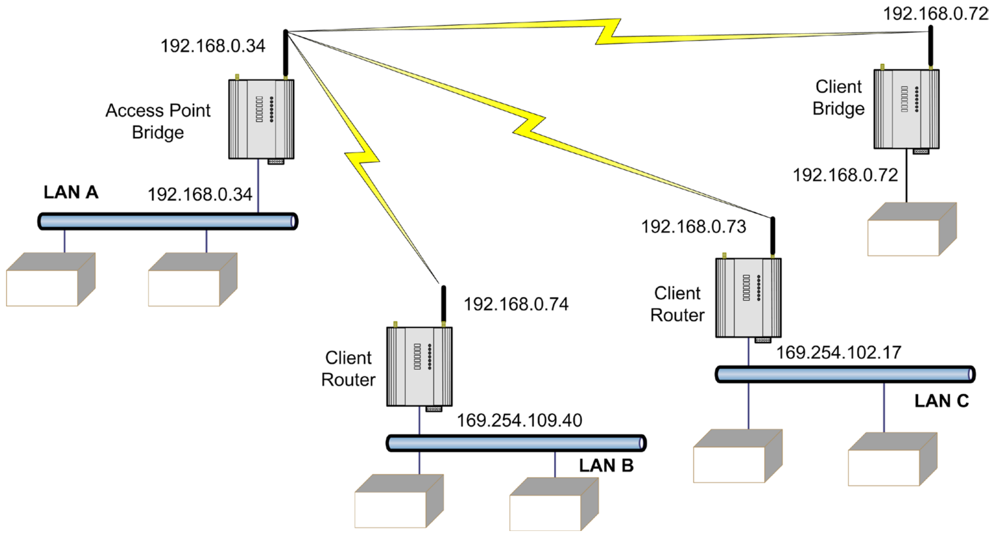
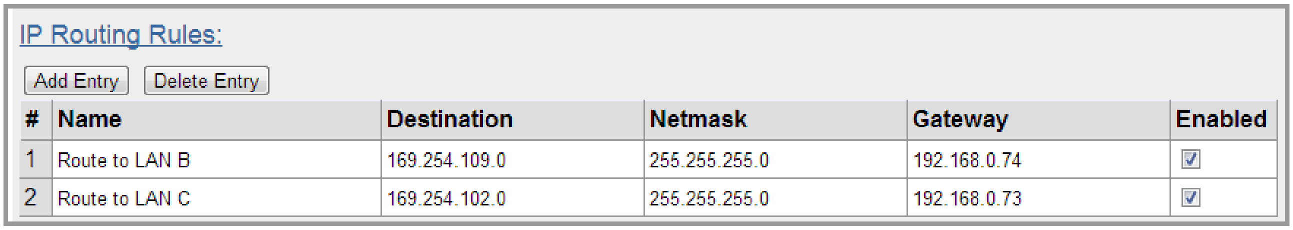


Figure 51 Routing

Figure 51 illustrates a situation where routing rules may need to be configured. In this example, the 450U-E clients need only specify the access point as their default gateway (they require no routing rules to be configured). However, for the access point to be able to deliver traffic to LAN B and LAN C it needs to have routing rules configured that specify the respective 450U-E client/routers as next-hop routers (gateways) to networks B and C.

Note that devices on LAN A should specify the 450U-E access point as their default gateway. An alternative to adding routing rules to the 450U-E in this example would be for each device on LAN A that needs to communicate with LAN B and C to have independent routing rules specifying the 450U-E clients at B and C as gateways to those networks.

The routing rules for the access point in the above example are shown in Figure 52. The first entry shows the route to LAN B. The gateway for the route to LAN B is configured as the wireless IP address of the 450U-E client connected to LAN B. The destination for the route is configured as the network address of LAN B. Because the host ID of the destination IP address is 0, it specifies a network address. Consequently, any traffic received at the access point with destination IP address 169.254.109.x (where x is any host ID) will be forwarded to the 450U-E at LAN B.

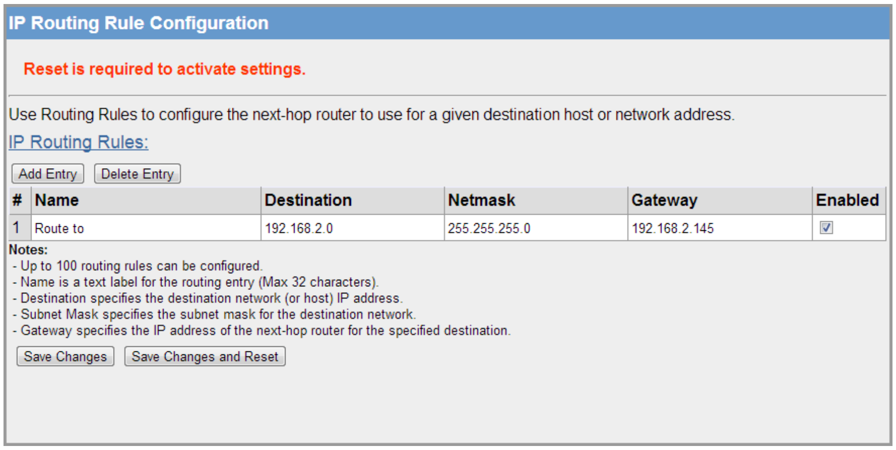

IP Routing Rules:

#	Name	Destination	Netmask	Gateway	Enabled
1	Route to LAN B	169.254.109.0	255.255.255.0	192.168.0.74	☑
2	Route to LAN C	169.254.102.0	255.255.255.0	192.168.0.73	☑

Figure 52 Routing Rules at Access Point

Devices on LAN B and LAN C that needs to send messages back to LAN A will need to have their gateway addresses directed to the 450U-E on their respected networks. For example, a LAN B device needs to send data back to LAN A. The gateway address will need to be configured as 169.254.109.40 as this is the IP address of the wired side of the LAN B 450U-E. Any message coming in with a 192.168.0.X IP address will be directed across the wireless interface to LAN A.

To access the **IP Routing Rules** configuration page, click **IP Routing** from the menu. Up to 30 routing rules may be added to each 450U-E. The table below summarizes the configurable parameters of a routing rule.



IP Routing Rule Configuration

Reset is required to activate settings.

Use Routing Rules to configure the next-hop router to use for a given destination host or network address.

IP Routing Rules:

#	Name	Destination	Netmask	Gateway	Enabled
1	Route to	192.168.2.0	255.255.255.0	192.168.2.145	☑

Notes:
- Up to 100 routing rules can be configured.
- Name is a text label for the routing entry (Max 32 characters).
- Destination specifies the destination network (or host) IP address.
- Subnet Mask specifies the subnet mask for the destination network.
- Gateway specifies the IP address of the next-hop router for the specified destination.

Figure 53 IP Routing

Name A name that describes the routing rule (max 32 characters).

Destination The destination network (or host) IP address. To specify a network address, set the host address to 0. For example, an IP address 192.168.0.0 with netmask 255.255.255.0 specifies a destination network, while 192.168.0.16 specifies a destination host.

Netmask The subnet mask for the destination network.

Gateway The IP address of the next-hop router for the specified destination.

Enabled Select this checkbox to enable the rule. You can deselect the checkbox to disable a routing rule without needing to re-enter the information at a later time.

Save Changes Save changes to non-volatile memory. The module will need to be restarted before the changes take effect.

Save Changes and Reset Save settings to non-volatile memory, and reboot the 450U-E module. Once the module has completed the reboot sequence, all changes are in effect.

⚠ **NOTE Dedicated Ethernet routes can also be added to the wired Ethernet LAN in place of generating or adding routing rules in the modems.**

4.10 Filtering

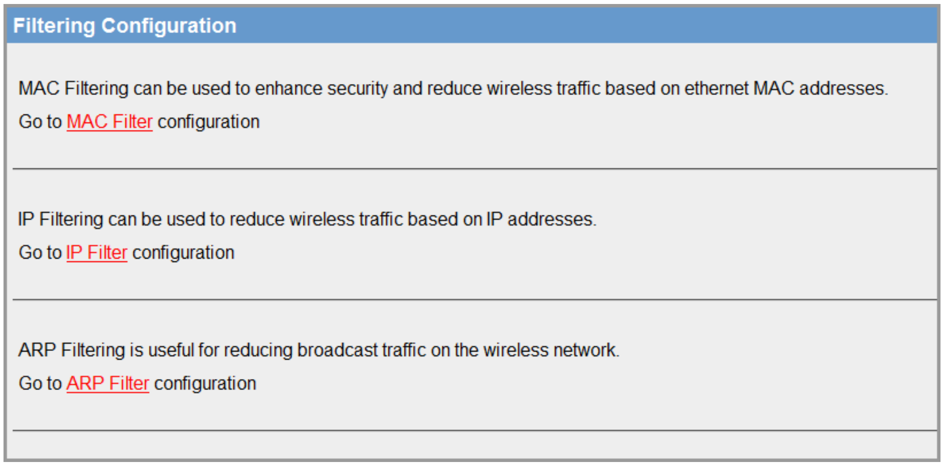
The 450U-E has a filtering feature to reduce unnecessary wireless transmissions and enhance security. To configure filters, click **Filtering** on the menu to display the page shown in Figure 54. Filtering applies only to messages appearing at the wired Ethernet port of the configured 450U-E module. You can configure three types of filters—MAC Addresses, IP Address/Protocol/Port, and ARP. Each filter list may be set as either a blacklist (to block traffic for listed devices and protocols), or as a whitelist (to allow traffic for listed devices and protocols).

The filters operate on the following rules:

- The MAC Address filter is always checked before the IP Address filter.
- If a message matches a MAC Address filter entry, it is not subsequently processed by the IP Address filter.

If the MAC Address filter list is a whitelist, the message is accepted. If the MAC Address filter list is a blacklist, the message is dropped.

- The MAC Address filter checks the source address of the message only.
- The IP Address filter checks both the source address and the destination address of the message. If either address match, then the rule is activated.
- ARP filtering applies only to ARP request packets (typically these are broadcast packets) that are sourced from the Ethernet interface and destined for the wireless interface. ARP requests from devices on the wireless network will always be passed to the Ethernet interface. ARP response packets will always be passed.



Filtering Configuration

MAC Filtering can be used to enhance security and reduce wireless traffic based on ethernet MAC addresses.

Go to MAC Filter configuration

IP Filtering can be used to reduce wireless traffic based on IP addresses.

Go to IP Filter configuration

ARP Filtering is useful for reducing broadcast traffic on the wireless network.

Go to ARP Filter configuration

Figure 54 Filtering

When configuring a whitelist, it is important to add the addresses of all devices connected to the 450U-E wired Ethernet port, that communicate over the wireless link. It is particularly important to add the address of the configuration PC to the whitelist. Failure to add this address will prevent the configuration PC from making any further changes to configuration. Design of the filter may be simplified by monitoring network traffic and forming a profile of traffic on the wired network. Network analysis software, such as the freely available “Wireshark” program, will list broadcast traffic sent on the network.

Filter Example

In the example shown in Figure 55, device B needs to communicate with device E via modems C and D. The filtering requires that modem C has device B in its whitelist. IP filtering checks both source and destination IPs, therefore, any traffic from device E will be passed back into the LAN via modem C because the destination matches the IP for device B. This works because device B is a Modbus master and it initiates all communications. If the communications were being initiated from each end (a non-polling system) you would need to configure a filter list for each modem to allow the communications to be passed from each end.

With this filter configuration device A will not be able to access device E because device A is not present in the whitelist in modem C.

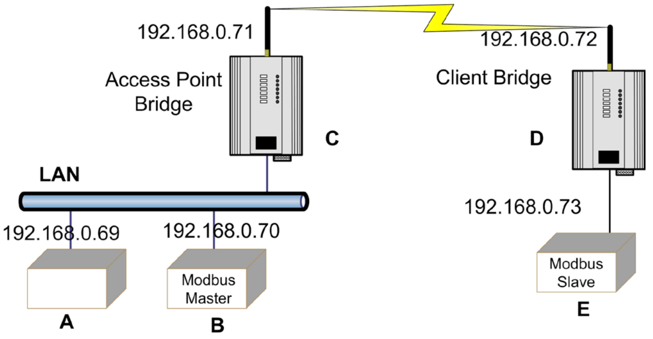


Figure 55 Filter Example

An ARP (Address Resolution Protocol) filters is also recommended because it would filter out broadcast ARP requests from other devices on the LAN that would normally be sent over the radio. ARP is a communication protocol used by Ethernet devices for associating MAC addresses and IP addresses, and is a crucial part of normal network communications. When a device on a LAN wants to communicate with another device it needs to know the MAC address. If the MAC address is not already known or is in its look-up table, it will broadcast an ARP request which subsequently would be passed over the radio if the modems were setup in bridging mode. For small networks it may not matter, but in larger systems there can be a considerable amount of broadcast ARP traffic, which if sent over the radio would compromise the reliability of the wireless link.

NOTE ARP filters will only filter out ARP traffic, and IP filters will only filter out IP traffic. If using an IP filter, any Ethernet traffic that is not IP is passed (this could include NetBIOS, IPX, PPP, and so on). These protocols could be more effectively filtered using MAC filtering or by configuring the modems in a router configuration instead of a bridge.

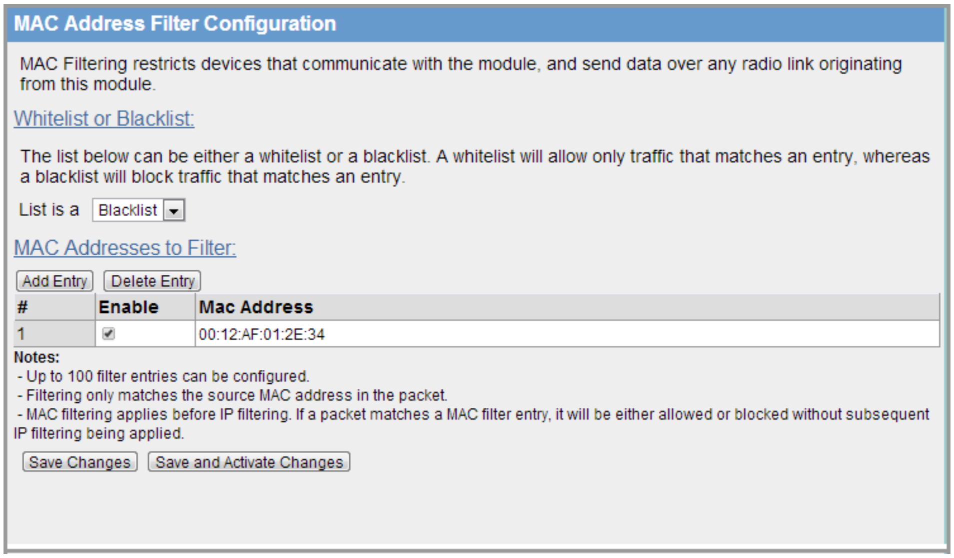
If after configuring the modem with filtering, you no longer have access to the modem, it probably means the computer IP or MAC address was not added to the filter list. To restore operation, you will need to restart the 450U-E with the RUN/SETUP switch in the SETUP position which will temporarily load the factory defaults allowing you access to its IP address.

MAC Address Filter

MAC addresses are uniquely assigned to each device and therefore can be used to permit or deny network access to specific devices through the use of blacklists and whitelists. In theory, MAC filtering allows administrators to permit or deny network access to hosts associated with the MAC address, though in practice there are methods to circumvent this form of access control through address modification. The MAC filter entry will match only the source MAC address in the packet.

To configure MAC address filters, click **Filtering** from the menu, and then click **MAC Filter** on the **Filtering Configuration** page to display the page in Figure 56.

NOTE It is important to add the MAC address of the configuration PC when creating a whitelist. If the configuration PC is not on the whitelist, it will be unable to communicate with the module for further configuration.



MAC Address Filter Configuration

MAC Filtering restricts devices that communicate with the module, and send data over any radio link originating from this module.

Whitelist or Blacklist:

The list below can be either a whitelist or a blacklist. A whitelist will allow only traffic that matches an entry, whereas a blacklist will block traffic that matches an entry.

List is a Blacklist

MAC Addresses to Filter:

#	Enable	Mac Address
1	☑	00:12:AF:01:2E:34

Notes:
- Up to 100 filter entries can be configured.
- Filtering only matches the source MAC address in the packet.
- MAC filtering applies before IP filtering. If a packet matches a MAC filter entry, it will be either allowed or blocked without subsequent IP filtering being applied.

Figure 56 Filtering - MAC Address Filter

Blacklist
Whitelist Select whether the filter list is a blacklist or a whitelist. A blacklist will prevent all listed devices from accessing the module and using the radio link. A whitelist will allow devices with the MAC addresses listed to communicate with the module and utilize the radio link—all other devices are blocked.

Add Entry Adds a new row to the table for you to enter a new address filter rule.

Delete Entry Removes the currently selected MAC address filter rule.

Enable Select this checkbox to enable the rule.

Mac Address Enter the desired source MAC address.

Save Changes Save changes to non-volatile memory (reset is required to activate).

Save and Activate Changes Save changes to non-volatile memory and activate the process.

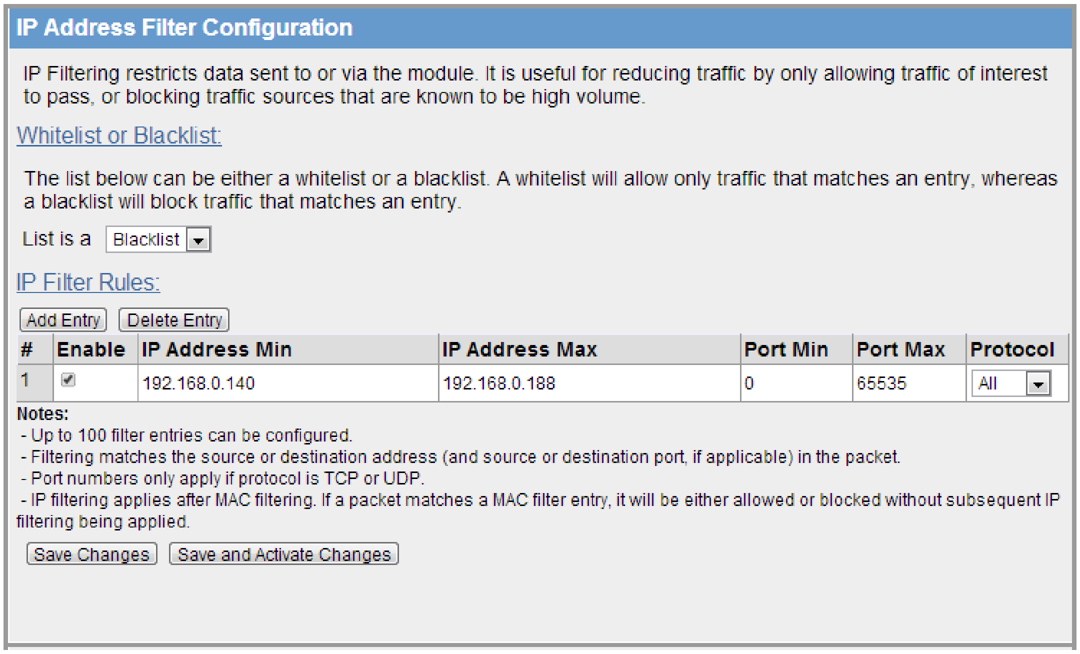
IP Address Filter

The IP address filter can be used to permit or deny network access to specific devices through the use of blacklists (blocking of traffic that matches a rule) and whitelists (allow traffic that matches a rule). To configure IP address filters, click **Filtering** from the menu, and then click **IP Filter** on the **Filtering Configuration** page to display the page in Figure 57.

The IP filter entry will match either source or destination address in the packet. That is, if either the source or destination IP address falls within the address range specified in the rule, the packet is matched and will be discarded (blacklist) or allowed (whitelist).

If the protocol is specified, the protocol of the packet must also match. If the protocol is TCP or UDP the source or destination TCP/UDP can also be inspected. If the IP address and protocol matches and the source or destination port number falls within the range specified, the packet is matched.

NOTE Configuration pages use TCP protocol on ports 80 and 443. Create whitelist rules specifying the configuration PC's IP address, with TCP protocol, ports 80 and 443.



IP Address Filter Configuration

IP Filtering restricts data sent to or via the module. It is useful for reducing traffic by only allowing traffic of interest to pass, or blocking traffic sources that are known to be high volume.

Whitelist or Blacklist:

The list below can be either a whitelist or a blacklist. A whitelist will allow only traffic that matches an entry, whereas a blacklist will block traffic that matches an entry.

List is a Blacklist

IP Filter Rules:

#	Enable	IP Address Min	IP Address Max	Port Min	Port Max	Protocol
1	☑	192.168.0.140	192.168.0.188	0	65535	All

Notes:
- Up to 100 filter entries can be configured.
- Filtering matches the source or destination address (and source or destination port, if applicable) in the packet.
- Port numbers only apply if protocol is TCP or UDP.
- IP filtering applies after MAC filtering. If a packet matches a MAC filter entry, it will be either allowed or blocked without subsequent IP filtering being applied.

Figure 57 Filtering - IP Address Filter

Blacklist
Whitelist
Select whether the filter list is a blacklist or a whitelist. A blacklist will prevent all listed devices from accessing the module and using the radio link. A whitelist will allow devices with the IP addresses listed to communicate with the module and utilize the radio link—all other devices are blocked.

Add Entry
Adds a new row to the table for you to enter a new filter rule.

Delete Entry
Removes the currently selected address filter rule.

Enable
Select this checkbox to enable the rule.

IP Address Min,
IP Address Max
Sets the range of IP addresses that are affected by the rule.

Port Min,
Port Max
When the protocol is set to “TCP” or “UDP,” this is the range of port addresses to which the rule applies. When the protocol is set to “All” or “ICMP,” these settings have no effect.

Protocol
Select the protocol to which the rule applies. The rule can apply to any protocol (All), or to only one of TCP, UDP, or ICMP (Ping).

Save Changes
Save changes to non-volatile memory (reset is required to activate).

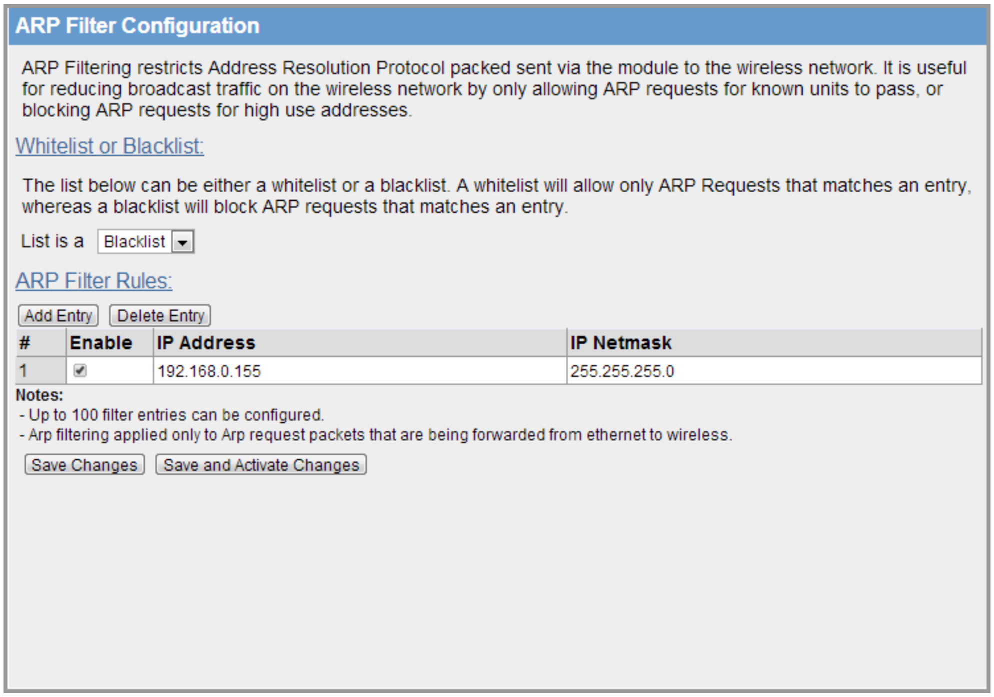
Save and Activate Changes
Save to non-volatile memory and restart to activate changes.

ARP Filter

ARP (Address Resolution Protocol) is a broadcast message and is primarily used for identifying MAC addresses when only the IP address or some other Network layer address is known. Large networks tend to get a high proportion of broadcast messages. ARP filters are useful for reducing broadcast traffic that is generated on the wired side of the network from being passed on to the wireless network. This is done by only allowing ARP requests for the devices that are on the wireless network, or by blocking ARP requests for high-use addresses. This means that all other ARP requests for devices on the wired network will not be passed over the radio. The 450U-E has a reduced throughput compared with other Ethernet modems, and it is very important that unnecessary traffic is not broadcast over the radio. Therefore, we highly recommend that you enable and configure ARP filters.

To configure ARP filters, click **Filtering** from the menu, and then click **ARP Filter** on the **Filtering Configuration** page to display the page in Figure 58.

By far the easiest ARP filter to apply is the whitelist. To create a whitelist, add the IP address for all remote modems and any device that is connected to these remote radios in the ARP filter table. When complete, make sure the entries are enabled (select the enable checkbox) and click Save and Activate Changes. After the modem reboots, it will only pass ARP traffic for the IP addresses configured.



ARP Filter Configuration

ARP Filtering restricts Address Resolution Protocol packed sent via the module to the wireless network. It is useful for reducing broadcast traffic on the wireless network by only allowing ARP requests for known units to pass, or blocking ARP requests for high use addresses.

Whitelist or Blacklist:

The list below can be either a whitelist or a blacklist. A whitelist will allow only ARP Requests that matches an entry, whereas a blacklist will block ARP requests that matches an entry.

List is a Blacklist

ARP Filter Rules:

#	Enable	IP Address	IP Netmask
1	☑	192.168.0.155	255.255.255.0

Notes:
- Up to 100 filter entries can be configured.
- Arp filtering applied only to Arp request packets that are being forwarded from ethernet to wireless.

Figure 58 Filtering - ARP Filter

Blacklist Whitelist Select whether the filter is a blacklist or whitelist. A blacklist will block ARP requests that match the entry. A whitelist will allow only ARP requests that match the entry—all other devices are blocked.

Add Entry Adds a new row to the table for you to enter a new address filter rule.

Delete Entry Removes the currently selected address filter rule.

Enable Select this checkbox to enable the rule.

IP Address Sets the IP address that you want to filter.

IP Netmask Sets the IP netmask.

Save Changes Save changes to non-volatile memory (reset is required to activate).

Save and Activate Changes Save to non-volatile memory and restart to activate changes.

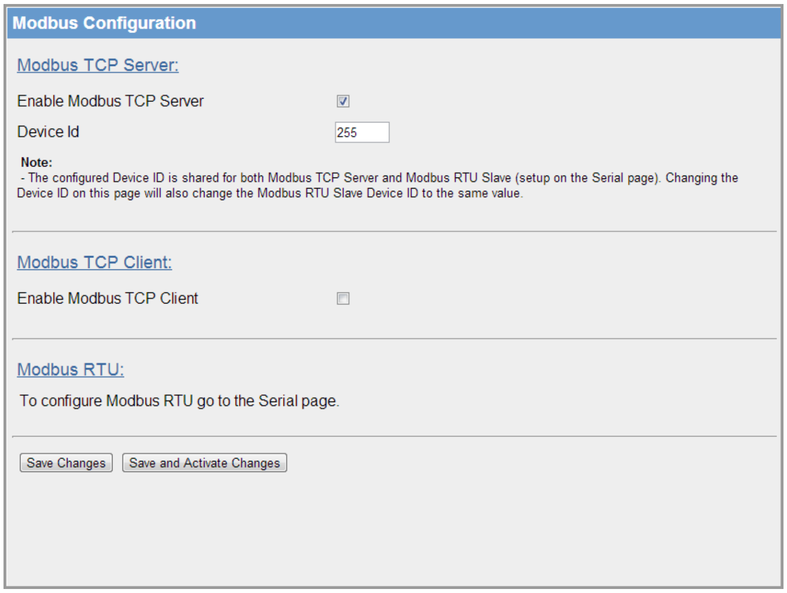
4.11 Modbus TCP

The 450U-E also has an on-board Modbus TCP server and Modbus TCP client that provide connectivity for a range of Modbus applications. The Modbus TCP client and the Modbus TCP server can be enabled simultaneously, and when combined with the built in Modbus TCP/RTU converter (enabled on the Serial page) the 450U-E can transfer I/O to and from almost any combination of Modbus TCP or RTU devices.

Modbus TCP Server

The Modbus TCP server enables the 450U-E to accept connections from Modbus TCP clients. To configure the Modbus TCP server, click **Modbus TCP** on the menu, and then click **Modbus TCP Server** to display the page in Figure 59.

All Modbus transactions routed to the onboard Modbus TCP server are directed to/from the onboard general purpose I/O registers. Because the Modbus TCP server can also be shared with the Modbus TCP/RTU converter (if enabled), the “Device ID” must be a unique address—which is why the default is set to 255. Care should be taken to ensure that all serially connected Modbus devices use a different Modbus device ID (Modbus slave address) from that of the onboard Modbus TCP server. Up to 32 separate connections to the Modbus TCP server are supported.



Modbus Configuration

Modbus TCP Server:

Enable Modbus TCP Server ☑

Device Id 255

Note:
- The configured Device ID is shared for both Modbus TCP Server and Modbus RTU Slave (setup on the Serial page). Changing the Device ID on this page will also change the Modbus RTU Slave Device ID to the same value.

Modbus TCP Client:

Enable Modbus TCP Client □

Modbus RTU:

To configure Modbus RTU go to the Serial page.

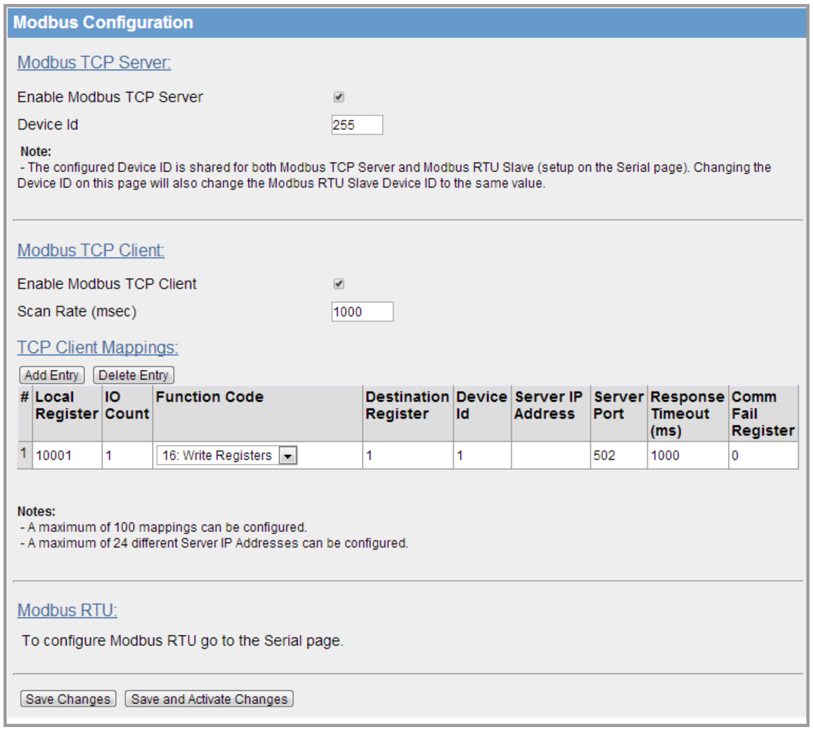
Figure 59 Modbus TCP Server

Enable Modbus TCP Server	Select this checkbox to enable the Modbus TCP server and allow the 450U-E to accept connections from Modbus TCP clients.
Device ID	Device ID assigned to the Modbus TCP server.
Save Changes	Save changes to non-volatile memory (reset is required to activate).
Save and Activate Changes	Save to non-volatile memory and restart to activate changes.

Modbus TCP Client

The Modbus TCP client enables the 450U-E to connect to one or more Modbus TCP servers. To configure the Modbus TCP client, click **Modbus TCP** on the menu, and then select the **Enable Modbus TCP Client** checkbox to display the client parameters (see Figure 60).

Communications with the remote TCP servers is achieved using mappings. All Modbus mappings are directed to/from the onboard I/O registers and are setup using the table in the Modbus Configuration page. To add a mapping, select the “Add Entry” button. A new default mapping is added to the table. You will need to edit this entry to configure the parameters to match the application.



Modbus Configuration

Modbus TCP Server:

Enable Modbus TCP Server ☑

Device Id 255

Note:
- The configured Device ID is shared for both Modbus TCP Server and Modbus RTU Slave (setup on the Serial page). Changing the Device ID on this page will also change the Modbus RTU Slave Device ID to the same value.

Modbus TCP Client:

Enable Modbus TCP Client ☑

Scan Rate (msec) 1000

TCP Client Mappings:

#	Local Register	IO Count	Function Code	Destination Register	Device Id	Server IP Address	Server Port	Response Timeout (ms)	Comm Fail Register
1	10001	1	16: Write Registers	1	1		502	1000	0

Notes:
- A maximum of 100 mappings can be configured.
- A maximum of 24 different Server IP Addresses can be configured.

Modbus RTU:

To configure Modbus RTU go to the Serial page.

Figure 60 Modbus TCP Client Mapping

Enable Modbus TCP Client Select this checkbox to enable the Modbus TCP client and display the client parameters.

Scan Rate Sets how frequently the device will be polled.

Add Entry Adds a default mapping to the table. Edit the entry to configure the parameters to match the application.

Delete Entry Removes the selected mapping.

Local Register Enter the starting on-board I/O register number that the specified Modbus master transaction will transfer I/O to/from.

I/O Count Specify the number of consecutive I/O registers to be transferred for the specified transaction.

Function Code Specify the Modbus Function Code for the transaction:

- **01 Read Coil**—Reads the on/off status of a digital output in the slave device (for example, DO status, 0X register).
- **02 Read Discrete**—Reads the on/off status of a digital input in the slave device (for example, DI status, 1X register).
- **03 Read Registers**—Reads the analog value of a holding register in the slave device (for example, AO status, 4X registers).
- **04 Read Inputs**—Reads the analog content of input registers in the slave device (for example, AI status, 3X registers).
- **15 Write Coils**—Writes an on or off value to a digital output in the slave device (for example, DO or 0X register).
- **16 Write Registers**—Writes an analog value into a holding register in the slave device (for example, AO, 4X register).

Destination Register Enter the starting I/O register number in the destination device that the specified Modbus master transaction will transfer I/O to/from.

Device ID Enter the Modbus device ID of the destination Modbus device.

Server IP Address Specify the IP address of the destination Modbus TCP server for the specified transaction.

Sever Port Specify the server port number used for Modbus TCP. The default/standard port number is 502.

Response Timeout Enter the timeout (in milliseconds) to wait for a response to the specified transaction. Response time should be configured in conjunction with the response time for the serial ports if using TCP to RTU communications.

Comm Fail Register Enter the on-board I/O register number to store the communication status of the specified transaction. The specified register will be set to 0 if communications is successful, 0xFFFF if there is no connection to the specified server, or 0xFFxx where “xx” is the Modbus exception code (see Appendix E).

Save Changes Save changes to non-volatile memory (reset is required to activate).

Save and Activate Changes Save to non-volatile memory and restart to activate changes.

NOTE When entering the local or destination registers, you do not need to enter in the full Modbus address (for example, 30001 or 10001). Only the I/O address is needed because the function code determines what type of command is being used.

For example, if you want to read from Destination register 30001 you need to select function code 04: Read Inputs and then enter the destination register of 1. Or, if you want to read register 10501 you need to select function code 02: Read Discretes and then enter the destination register of 501.

TCP Mapping Example

The system in Figure 61 shows that Unit B is a Modbus TCP client that will poll the TCP server at Unit C via the Wireless Ethernet interface to gather the status of the on board DIO (digital input), which will then be reflected on its own DIO (digital output).

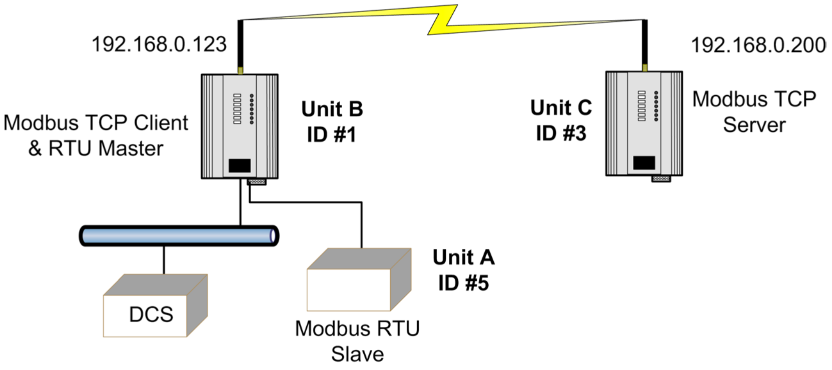
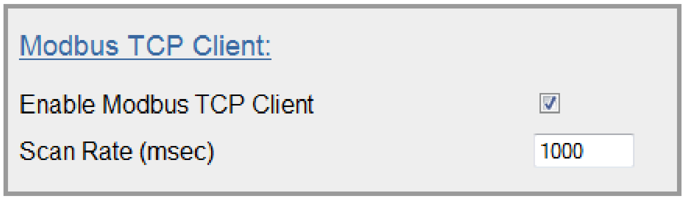


Figure 61 Modbus Example

Enabling the Modbus TCP server within Unit B provides a register location for the polled values from Unit C to be stored. It will also allow an external Modbus TCP client (DCS or SCADA) to monitor the stored I/O values from units A and C. First, the Modbus TCP client must be enabled and a suitable scan rate be selected (Figure 62). The default times will be 1000 msec, meaning that there will be a 1-second delay between the client mappings directed at any Modbus server.



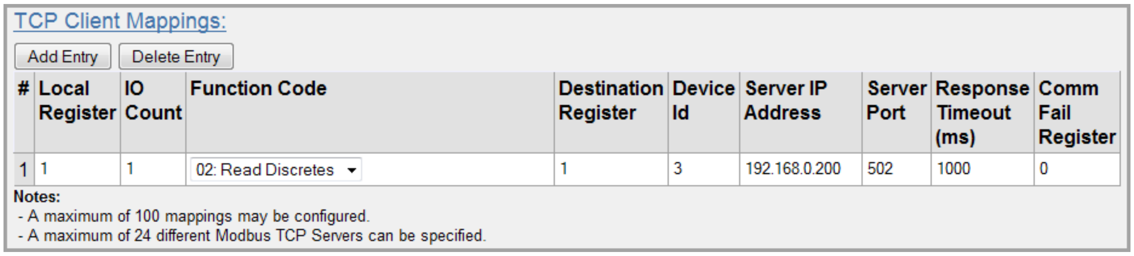
Modbus TCP Client:

Enable Modbus TCP Client ☑

Scan Rate (msec) 1000

Figure 62 TCP Client

Next, the mappings need to configured. The example TCP mapping in Figure 63 is configured to transfers the status of the onboard digital input at Unit C (Device ID #3) to the on-board digital output at Unit B.



TCP Client Mappings:

#	Local Register	IO Count	Function Code	Destination Register	Device Id	Server IP Address	Server Port	Response Timeout (ms)	Comm Fail Register
1	1	1	02: Read Discretes	1	3	192.168.0.200	502	1000	0

Notes:
- A maximum of 100 mappings may be configured.
- A maximum of 24 different Modbus TCP Servers can be specified.

Figure 63 Unit B Modbus TCP Mappings

- Local Register (1) specifies the register for the onboard digital output at Unit B. This register is configured with 1, which is the register used to turn on the digital output.
- I/O Count (1) specifies that only one I/O point is being transferred (the single digital I/O).
- Function Code (02: Read Discretes) specifies the standard Modbus function code to read discrete (digital) inputs.
- Destination Register (1) specifies the register for the onboard digital input (1). Because the function code is a read discrete, it indicates that the destination register will be in the range 10XXX range and you only need to enter the register location, and not the function designator (10XXX).
- Device ID (3) is the ID of the onboard Modbus TCP server at Unit C.
- Server IP address (192.168.0.200) is the IP address of Unit C – which is the Modbus TCP server we are reading from.
- Server Port is the TCP port used.
- Response Timeout (1000 ms) specifies that Unit C must respond to this message within 1000 ms.
- Comm Fail Register (0) specifies the local register where the communications status for this mapping will be stored.

Modbus TCP client functionality allows a maximum of 100 mappings to be configured and a maximum of 24 different Modbus TCP servers.

4.12 Input/Output Configuration

The 450U-E has a single physical on-board I/O channel that can be configured as either digital or analog via the Web Server. The digital channel can also act as an input or an output. The 450U-E also has a number of internal register locations that are used for monitoring internal I/O, general purpose I/O, and module information, as well as an area of memory that will hold the values from any expansion I/O modules that may be connected to the serial ports.

To configure the physical I/O (analog input or digital input/output) click **I/O Configuration** on the menu, and then click **Onboard I/O Mode Configuration** to display the page in Figure 65.

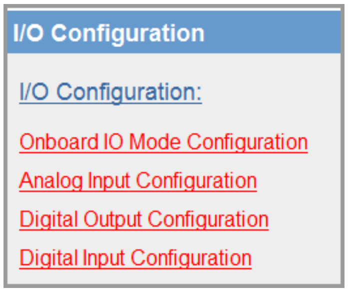
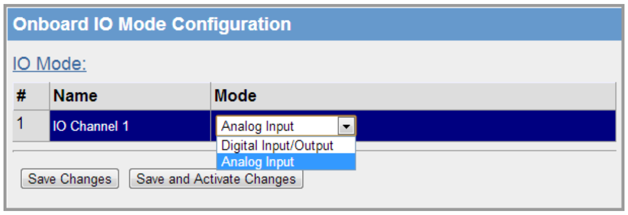

I/O Configuration
I/O Configuration:
Onboard IO Mode Configuration
Analog Input Configuration
Digital Output Configuration
Digital Input Configuration

Figure 64 I/O Configuration


Onboard IO Mode Configuration

IO Mode:

#	Name	Mode
1	IO Channel 1	Analog Input

Figure 65 Input Mode

Name Name associated with the channel. You can change the default channel name to something more descriptive, such as “Tank Level”.

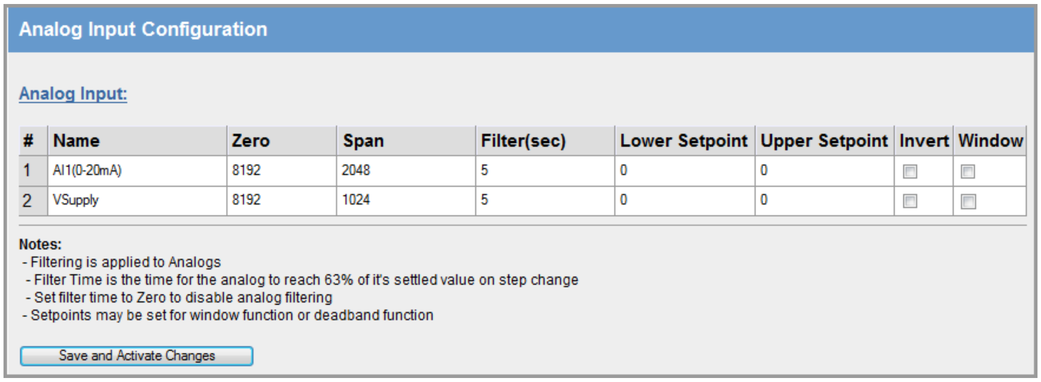
Mode Select the input mode (digital input/output, or analog input). The default mode is digital input/output.

Save and Activate Changes Save to non-volatile memory and restart to activate changes.

Analog Input Configuration

To configure the I/O channel as an analog, make sure that “Analog Input” is selected in the Mode field on the External I/O Mode Configuration page (see the previous section). After saving the changes, click **Analog Input Configuration.**

The I/O channel can be configured to accept a 0–20 mA current sinking analog input. The default settings should suffice for most applications. The following parameters can be adjusted to suit the application.


Analog Input Configuration

Analog Input:

#	Name	Zero	Span	Filter(sec)	Lower Setpoint	Upper Setpoint	Invert	Window
1	AI1(0-20mA)	8192	2048	5	0	0	□	□
2	VSupply	8192	1024	5	0	0	□	□

Notes:
- Filtering is applied to Analogs
- Filter Time is the time for the analog to reach 63% of it's settled value on step change
- Set filter time to Zero to disable analog filtering
- Setpoints may be set for window function or deadband function

Figure 66 Analog Input

Name You can enter a descriptive name for the analog input, or use the default. The name can be up to 30 characters, including spaces.

Zero Configures the scale of the analog input. This is the starting variable (in counts) when the analog input is at the bottom or zero scale. The default is 8192, which equates to the number of raw counts in the register when the input is at the zero or minimum value (0 mA on the analog input).

Span Configures the scale of the analog input. This is the number of counts per measured value (for example, 1 mA, 1 V, or 1 Hz,). Default is 2048 which equates to 20 mA on the analog input.

For example, the register range has a total range of 32768 counts with a total mA range of 16 mA. Therefore, the Span is calculated by dividing the total range in counts by the total range in mA, V, Hz, and so on (32768 / 16 = 2048).

Filter (sec) The filter time constant is the time the analog takes to settle on a step change of an analog value. By default, inputs have a time constant of 5 seconds.

Lower Setpoint This parameter is the lower control point value that is used in conjunction with the upper setpoint to turn on and off the analog setpoint register. The AI1 setpoint location is at register 10002 and VSupply setpoint is located at register 10003.

Upper Setpoint This parameter is the upper control point value that is used in conjunction with the lower setpoint to turn on and off the analog setpoint register.

Invert Select this checkbox to allow the setpoint control logic to be inverted. The function does not change, only the operation is inverted. For example, if the setpoint is "on" in its normal state, inverting the signal will mean the setpoint will be "off "in the normal state. Default state is not inverted (checkbox unselected).

Window Selecting this option sets the set point operation to Window mode. Deselecting this option sets the set point operation to Default mode.

- **Window Mode**—In this mode, if the analog value is inside the upper and lower set points, the set point will be active (on, "1"), and if the analog value is outside of these set points the set point will be reset (off, "0").
- **Default Mode**—In this mode, the set point operates in default mode. If the analog input is greater than the Upper Setpoint, the set point status will be active (on, or "1"). When the analog input is less than the Lower Setpoint the set point will reset (off, or "0").

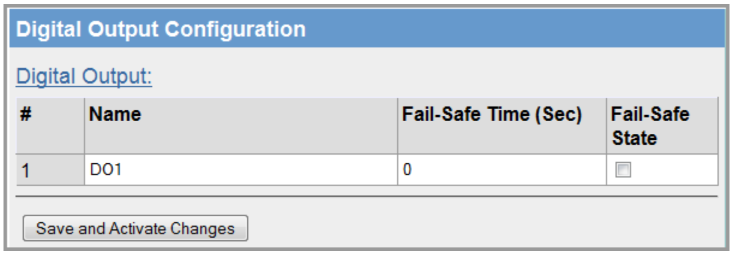
⚠ **NOTE The upper set point must always be higher than the lower set point.**

Save and Activate Changes Save to non-volatile memory and restart to activate changes.

Digital Output Configuration

To configure the I/O channel as digital output, make sure that "Digital Input/Output" is selected in the Mode field on the External I/O Mode Configuration page (Figure 65). After saving the changes, click **Digital Output Configuration**.

The default parameters for the digital output should suffice for normal operation, but if you want to configure the output to have a fail-safe indication you need to configure the following parameters.



Digital Output Configuration

Digital Output:

#	Name	Fail-Safe Time (Sec)	Fail-Safe State
1	DO1	0	□

Figure 67 Digital Output Configuration

Name You can enter a descriptive name for the digital output, or use the default. The name can be up to 30 characters, including spaces.

Fail-safe Time (sec) The time before the output actives its fail-safe state if it does not receive an update or a COS message from the sender. If the fail-safe timer counts down to zero, the output will be set to the Fail-safe State depending on how it is configured. If Fail-safe State option is selected, the output will be on; if the Fail-safe State option is deselected, the output will be off. When an update or a COS message is received, the fail-safe timer is restarted.

We recommend that the Fail-safe Time be configured for a little more than twice the update time of the input that is turning it on. That way the output will reset if it fails to receive two update messages.

Fail-safe State The state to which the output will be set if the Fail-safe Time countdown elapses.

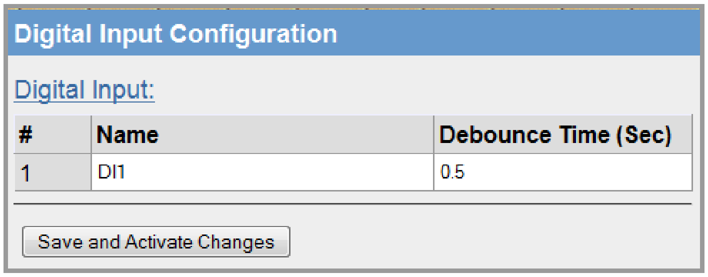
If the Fail-safe State checkbox is selected (enabled), the LED and the digital output will be turned on.

If the Fail-safe State checkbox is deselected (disabled), the LED and the digital output will be turned off.

Save and Activate Changes Save to non-volatile memory and restart to activate changes.

Digital Input Configuration

To configure the I/O channel as digital input, make sure that "Digital Input/Output" is selected in the Mode field on the External I/O Mode Configuration page (Figure 65). After saving the changes, click **Digital Input Configuration**.



Digital Input Configuration

Digital Input:

#	Name	Debounce Time (Sec)
1	DI1	0.5

Figure 68 Digital Input Configuration

Name You can enter a descriptive name for the input to help with configuration, or use the default. The name can be up to 30 characters, including spaces.

Debounce Time (Sec) Debounce is the time which an input must stay stable before the module decides that a change of state has occurred. If a digital input changes (on - off) and changes again (off - on) in less than the debounce time, then the module will ignore both changes. Default debounce time is 0.5 seconds.

Save and Activate Changes Save to non-volatile memory and restart to activate changes.

I/O Register Locations

There are over 5000 x 16-bit general purpose registers that are available for Modbus and are shared with both Modbus client and server. This includes the onboard analog/digital input/output registers.

Along with the physical DIO status, the internal I/O can be accessed by reading from or writing to the following register locations. The register locations are structured into standard Modbus I/O types, and can be accessed using the local onboard Modbus TCP server, Modbus serial master or an external Modbus master device.

The layout of the 450U-E I/O registers are summarized in the following table. Each register is internally saved as a 16-bit unsigned integer value. A Modbus transaction may access the entire 16-bit value of any register, or alternatively, the most significant bit of a register may be accessed as a discrete value. The main use for the general purpose I/O registers is for intermediate storage—for example, when transferring I/O from one Modbus slave device to another. Also provided is the status of the on-board digital I/O, the status of the wireless link, and any serial or TCP connections.

Digital Outputs Coils

Registers	Purpose
0001	Local digital output register
0021–0500	I/O space for locally attached 115S Expansion I/O modules. Twenty registers per module address. Maximum 24.
0501–3000	General purpose bit storage—area assigned in memory for Modbus mapping storage

Digital Input Bits

Registers	Purpose
10001	Local digital input register
10002	Setpoint status register for analog input 1
10003	Setpoint status register for VSupply
10021–10500	I/O space for locally attached 115S expansion I/O modules. Twenty registers per module address. Maximum 24.
10501–12500	General purpose bit storage—area assigned in memory for Modbus mapping storage

Analog Input Registers

Registers	Purpose
30001	Local analog input register
30002	Local supply voltage (8–40 Vdc)
30021 30493	I/O Space for locally attached 115S expansion I/O modules. Twenty registers per module address. Maximum 24.
30494–30500	Internal information registers—serial number, firmware version and patch level.
30501–32500	General purpose bit storage—area assigned in memory for Modbus mapping storage.
38001	Local DIO register (as a floating point value)
38003	Local supply voltage (8–40 Vdc) as a floating point

Expansion I/O

115S Serial Expansion I/O modules can be added to provide additional I/O. When adding expansion I/O modules to the 450U-E, the appropriate serial port must be configured as “Expansion I/O.” The default serial parameters of the port should be 9600, N, 8, 1, which matches the defaults of the 115S Serial Expansion modules. These parameters can be changed to increase poll speeds in larger systems. However, the 115S serial port and the 450U-E serial port need to match. If more than three serial expansion modules are added, the Maximum Units to Poll field on the Serial page will also need to be adjusted (see “4.7 Serial Configuration” on page 35).

Connect the serial expansion module and make a note of the address (rotary switches on the bottom) because this address will be used as an offset to locate the I/O within the 450U-E. Make sure that the devices at either end of the RS-485 cable have the termination switch enabled (on)—this includes the 450U-E. Failure to terminate the RS-485 correctly could result in the modules not operating correctly.

115S Expansion I/O Memory Map

Input/output data on the 115S module is read into memory locations according to their Modbus address. The maximum number of Modbus addresses is 24. Each 115S module has an offset that applies to the location of its registers. This offset is equal to the units Modbus address (selected on the rotary switch on the end of the 115S expansion I/O module), multiplied by 20.

For example, if connecting a 115S-11 (16 x DIO) with address #15:

- Digital input 1 will be at register location 10301 ((15*20) +10001)
- Digital Output 1 will be at register location 301 ((15*20) +1)

If using a 115S-12 (8 x DIO & 8 AIN) with address 16:

- Digital input 1 will be at register location 10321 ((16*20) +10001)
- Analog input 1 will be at register location 30321 ((16*20) +30001)

See Appendix D for a more detailed address map of the serial expansion I/O modules.

When adding expansion I/O modules to the 450U-E, there are two built-in registers used to indicating the communication status of the module.

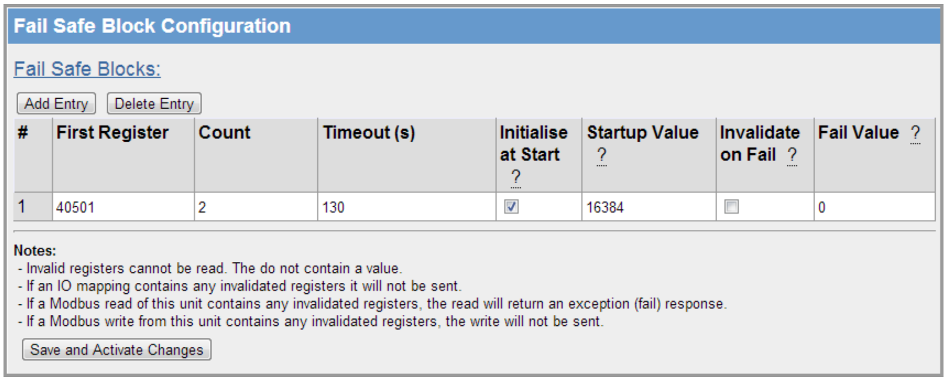
- **Communication Fail—**This register is located at register location 10019 + offset value. It will indicate “1”when the module is in failure.
- **Communication OK—**This register is located at register location 10020 + offset value. It will indicate “1”when the module is communicating OK.

Fail-safe Blocks

Fail-safe block configuration allows the internal registers to be set to a pre-configured value on startup, as well as configuring the DIO to reset to a predefined value after a timeout period has elapsed. In addition, if a remote device is sending I/O to the local DIO and it is in “communications fail,” the output can set to the configured fail value after a pre-configured time.

In Figure 69, register 40501 holds an analog value that is being updated from another module every 60 seconds. The module is configured so that on startup the value 16384 will be written into register 40501, and then it will start counting down the timeout period (in this case, 130 seconds), which is a little over two times the one-minute update period from the sending module. After 130 seconds, if the module still has not received an update from the other module, register 40501 will be set to the fail value (in this case, 0).

If the “Invalidate on Fail” option is selected, the value is set to a null or invalidated value (~). See “Invalid Register State” on page 64. If this register is mapped to another module and the state is “Invalidated” the mapping will be inhibited from sending until the invalid value is updated with a real value. In addition, if the register is being read by a Modbus master or client, an exception response will be returned because the register is invalid. If a Modbus master or client is writing from a register with an invalid state to another device, the message will not be sent. The maximum number of fail-safe blocks is 50.



Fail Safe Block Configuration

Fail Safe Blocks:

#	First Register	Count	Timeout (s)	Initialise at Start ?	Startup Value ?	Invalidate on Fail ?	Fail Value ?
1	40501	2	130	☑	16384	□	0

Notes:
- Invalid registers cannot be read. The do not contain a value.
- If an IO mapping contains any invalidated registers it will not be sent.
- If a Modbus read of this unit contains any invalidated registers, the read will return an exception (fail) response.
- If a Modbus write from this unit contains any invalidated registers, the write will not be sent.

Figure 69 Fail-safe Block Configuration - Analog

First Register First local register in the fail-safe block.

Count Number of registers to incorporate in the fail-safe block

Timeout Time allocated to the fail-safe block before triggering a fail-safe state.

Initialize at Startup Select this checkbox if you want to initialize the value on startup. If this option is deselected, the register will be uninitialized (~).

Startup Value Sets the value that the register will be set to on module startup.

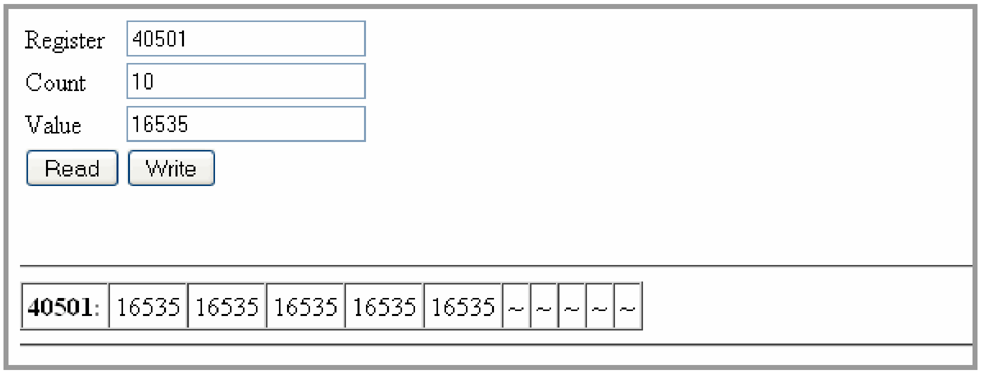
Invalidate on Fail Select this checkbox if you want the register to be invalidated on failure.

Fail Value Sets the value that the register is set to when a fail occurs.

Invalid Register State

All registers within the module can have various states depending on the type of register and the type of value it holds. A typical analog range is between 0 and 65535, and a digital value can be 0 or 1. Registers can also be in an "invalid" state, which means that the register has not been written to and therefore holds non or null value. If you were to read the registers using I/O Diagnostics, an invalid register would read as "~" (see Figure 70.

NOTE Any mapping with an invalid register will be inhibited from sending. This is to ensure that the data that arrives at the destination is valid and not the default values that the module has on startup.



Register: 40501
Count: 10
Value: 16535

40501:	16535	16535	16535	16535	16535	~	~	~	~	~

Figure 70 Invalid Register State

4.13 Configuration Examples

Extending a Wired Network

This example describes how to configure a bridged network.

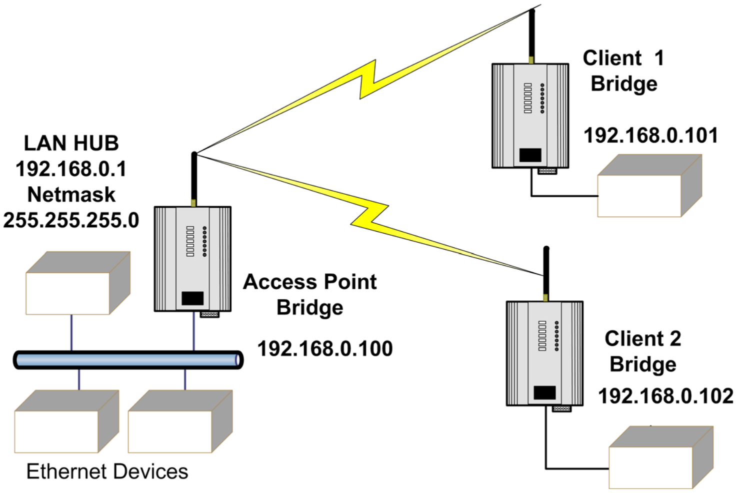


Figure 71 Example of Bridged Network

Access Point Configuration

1. Connect a straight-through Ethernet cable between the PC and the 450U-E module.
2. Ensure that the PC and 450U-E are set up to communicate on the same network.
3. Set the DIP switch on the 450U-E to SETUP.
4. Power on the module and wait for the OK LED to stop flashing.
5. Configure the network setting on the PC with an IP address of 192.168.0.1 and a netmask of 255.255.255.0.
6. Using Internet Explorer, open the module's Web Server at the address 192.168.0.1XX/ where "XX" is the last two digits of the module's serial number.
7. When prompted, enter default username "user" and password "user".
8. On the home page menu, click **Quick Start**.
9. On the Quick Start page, configure the following:
   a. Configure the Transmit Power Level, Transmit Data Rate, Frequency Step Size, and Transmit and Receive Frequency settings. Record these settings, as they will need to be the same for all radios in the example.
   b. Select the Operating Mode as "Access Point."
   c. Enter a System Address (ESSID) string. Record this string, as it will need to be exactly the same for all radios in the example.
   d. The encryption is automatically set to WPA2 on the Quick Start page. You need to configure an encryption key (passphrase). Record the key, as it also needs to be the same on all radios in the example.
   e. Change the IP addresses to 192.168.0.100.
   f. Leave the Subnet masks at the default of 255.255.255.0.
   g. Leave the Gateway IP Address at the default 192.168.0.1, as it is not used in this example.
10. Set the DIP switch on the module to RUN.

11. Click **Save Changes and Reset**.

    The module restarts with the new settings.

Client 1 Configuration

1. Perform the same configuration steps as the access point configuration with the following differences:
    - Ensure that the Radio, System Address (ESSID) and Encryption key are the same as the access point.
    - Set the Operating Mode to "Client."
    - Change the IP addresses to 192.168.0.101.
2. When complete, set the DIP switch back to RUN and click **Save Changes and Reset**.

Client 2 Configuration

1. As for Client 1 above, but set the IP address as 192.168.0.102.
2. When complete, set the DIP switch back to RUN and click **Save Changes and Reset**.

Connecting Two Networks Together

This example describes how to configure a routed network.

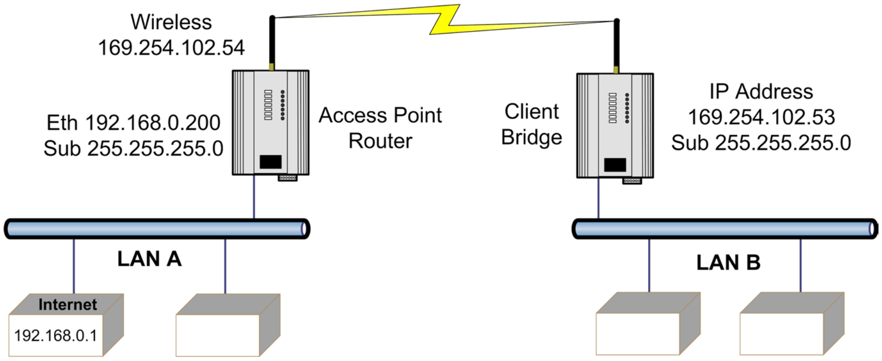


Figure 72 Example of Routed Network

LAN A Configuration

In this example, network A is connected to the Internet via a router at IP address 192.168.0.1. Devices on LAN A that require a connection to devices on LAN B, should set their gateway IP addresses to the Ethernet address of the 450U-E access point/router (192.168.0.200).

Devices on LAN A, that interact with devices on the Internet and LAN B should set their gateway IP address to the Internet router (192.168.0.1), and then apply a routing rule for devices on Network B. On Windows-based PCs, this may be achieved using the MS-DOS command ROUTE. For this example, the command would be: ROUTE ADD 169.254.102.0 MASK 255.255.255.0 192.168.0.200. For more information on the DOS ROUTE command, see section "5.13 Utilities" on page 85.

LAN B Configuration

All devices on LAN B should be configured so that their gateway IP addresses are configured with the IP address of 169.254.102.54, which is the 450U-E access point/router.

Access Point Configuration

1. Connect a straight-through Ethernet cable between the PC and the 450U-E.
2. Ensure that the PC and 450U-E are set up to communicate on the same network.
3. Set the DIP switch on the 450U-E to SETUP.
4. Power up the module, and wait for the OK LED to stop flashing.
5. Configure the network setting on the PC with an IP address of 192.168.0.1 and a netmask of 255.255.255.0.
6. Using Internet Explorer, open the module’s Web Server at address 192.168.0.1XX, where “XX” is the last two digits of the module’s serial number.
7. When prompted, enter the default username “user” and password “user”.
8. On the home page menu, click **Quick Start**.
9. On the Quick Start page, configure the following:
    a. Configure the Transmit Power level, Transmit Data Rate, Frequency Step size and Transmit and Receive Frequency settings. Record these settings, as they will need to be the same for all radios in the example.

    b. Select Operating Mode as “Access Point.”

    c. Enter a System Address (ESSID) string. Record this setting, as it will need to be exactly the same for all radios in the example.

    d. The encryption is automatically set to WPA2 on the Quick Start page. You need to configure an encryption key (passphrase). Record the key, as it also needs to be the same on all radios in the example.

    e. Change the IP addresses to 192.168.0.200.

    f. Leave the Subnet masks at the default 255.255.255.0.

    g. Leave the Gateway IP Address at the default 192.168.0.1, as it is not used in this example.

    h. Click **Save Changes** (not Save Changes and Reset) since we need to make some other changes to the configuration before resetting the module.
10. Click **Network** on the menu, and change the Device Mode to “Router.”

    This will display separate IP address fields for Ethernet and wireless. Because the access point is now configured as a router, it will route the IP traffic from one network to another.
11. Change the Wireless IP address to 169.254.102.54, which is the IP address on the wireless network.
12. Set the DIP switch back to RUN, and click **Save Changes and Reset**.

Client Configuration

1. Perform the same configuration steps as the access point configuration with the following differences:
    - Ensure that the Radio, System Address (ESSID), and Encryption key are the same as the access point.
    - Set the Operating Mode to “Client.”
    - Because the radio network is on a different IP range, change the IP addresses to 168.254.102.53.
2. When complete, set the DIP switch back to RUN and click **Save Changes and Reset**.

Extending Network Range with Repeater Hop

Configure units as described in the “Extending a Wired Network” on page 65. Place the access point at the remote intermediate repeater location. Additional repeaters can be added using Wireless Distribution System (WDS). For details, see “4.8 Repeaters” on page 44.

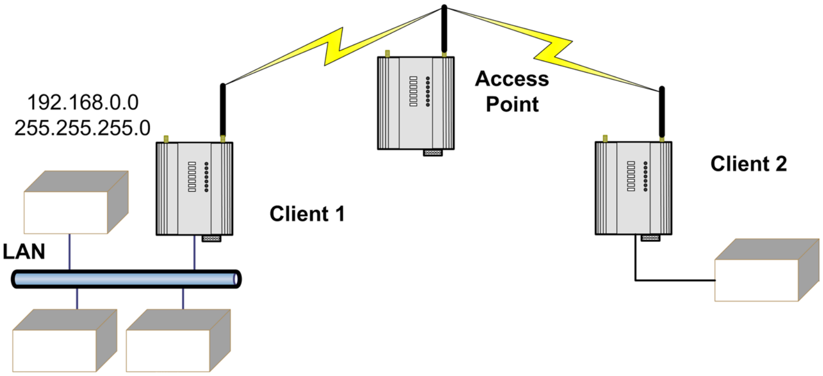


Figure 73 Example of Repeaters

Chapter 5 - DIAGNOSTICS

5.1 Diagnostics Chart

LED Indicator	Condition	Meaning
OK	Green	Normal operation
OK	Red solid	Factory default mode, locale not set, supply voltage low, or internal module fault
OK	Red at power on	Boot loader delay at startup
OK	Fast flash red/green	Module boot sequence
OK	Slow flash red / green	Module boot sequence
Radio RX	Green flash	Radio is receiving a valid ELPRO 450U-E data frame
Radio RX	Red flash	Radio is receiving a data frame with a low signal level. Threshold is –100 dBm for 2-level FSK and –90 dBm for 4-level FSK.
TX/LINK	Green	Connection established to remote device
TX/LINK	Red flash	Radio transmitting
RS-232	Green flash	Data sent from RS-232 serial port
RS-232	Red flash	Data received to RS-232 serial port
LAN	On	Link established on Ethernet port
LAN	Flash	Activity on Ethernet port
RS-485	Green flash	Data sent from RS-485 serial port
RS-485	Red flash	Data received to RS-485 serial port
I/O	Green	Digital input is turned on (shorted to GND)
I/O	Red	Digital output is active
I/O	Off	Digital output is off and input is open circuit
I/O	Green varying intensity	Analog input current in circuit (dim = 4 mA, bright = 20 mA)

The green OK LED on the front panel indicates that the 450U-E is operating correctly. A red OK LED can indicate a number of conditions. When the module is reset to its factory default settings and requires the locale to be configured, the LED will remain red until the module has been configured and reset. The OK LED also turns red when the module has a processor fault or the supply voltage is low. It may also indicate a shutdown state. For example, if there is a processor failure or failure during start-up diagnostics, the unit shuts down and remains in shutdown until the fault is rectified. During Module, boot-up the OK LED flashes red-green until the boot sequence is complete.

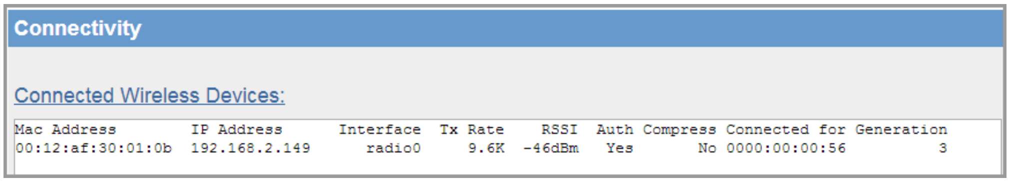
Boot Status LED Indication During Startup

The OK LED indicates the status of the module during the bootup process. At power on, the OK LED comes on red. During kernel boot the OK LED flashes red-green at a 1-Hz rate (½ second red, ½ second green). During module initialization, the OK LED flashes red-green at 0.5-Hz rate (1-second red, 1-second green). When initialization is complete, the OK LED becomes steady green.

If the OK LED remains red at power on, it could indicate either low supply voltage, module fault, or that the module is in factory default mode. The module will not attempt to boot until supply voltage is within range.

5.2 Connectivity

Click **Connectivity** on the menu to display information on the current connection with either the client or the access point, depending on how the module is configured. The Connected Wireless Devices area on the Connectivity page shows the MAC address, IP address, interface being used, radio data rate, received signal strength (RSSI), authentication status, compression status, connection time, and the number of access point connections. The readings displayed are based upon the last received data message from the client.



Connectivity

Connected Wireless Devices:

```
Mac Address        IP Address      Interface  Tx Rate    RSSI  Auth Compress Connected for Generation
00:12:af:30:01:0b  192.168.2.149      radio0     9.6K  -46dBm   Yes       No 0000:00:00:56          3
```

Figure 74 Connected Wireless Devices

NOTE When updating the Connectivity webpage, you need to hold down the <CTRL> key while pressing the refresh button to ensure that the most up to date information is displayed.

Mac Address Mac address of the connected device.

IP Address IP Address of the connected device.

Interface Interface being used for the connection. Will indicate Radio0 – Radio5 depending on the interface. Radio0 is the main Network interface and Radio 1-5 indicates the virtual WDS interfaces.

RATE Radio data rate.

RSSI The last radio receive signal strength from that site.

Auth Indicates whether the modem is authenticated, i.e. modem has the correct SSID and encryption keys. ‘No’ indicates the modem has the correct SSID but the wrong Encryption method/key, etc.

Compress Indicates whether the connected devices have compression turned on or off. Compression is described in “4.6 Radio Configuration” on page 33.

Connected For Shows the current link time that the client has been connected to the access point. If either modem is restarted, the time restarts from zero.

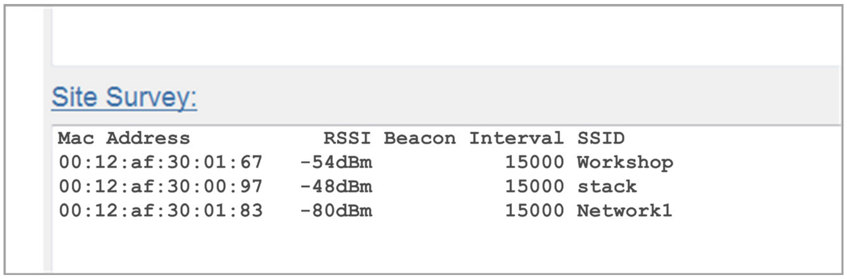
Generation Number of times the client has connected to the access point. Each device keeps a running total, which is shared with the other devices if possible. If the access point tries to communicate with a client that is no longer available, the access point will reset its count for that device after five minutes. A client will reset its count if it does not hear from an access point for seven beacon intervals (approximately 105 seconds).

NOTE If the default RUN/SETUP switch is enabled the radio is disabled and you will not see anything in the connectivity list.

The Site Survey area on the Connectivity page displays information on access points that the module can hear. If more than one access point can be heard, multiple entries are displayed, as shown in Figure 75. The table will display the Mac address, RSSI, SSID, and so on, for each access point.

To scan for a list of available access points, configure the client with an SSID that is not available for connection (there are no access points it can connect to). Save the configuration, and when the module is restarted the Site Survey will display a list of access points and their RSSI values. This information is useful for determining the best connection if multiple access points are available.

NOTE The site survey list is only refreshed when the module starts up, and only if the client is not connected to an existing access point. When the client does connect to an access point, the list will refresh and only indicate the access point to which the module is connected.


Site Survey:

```
Mac Address           RSSI Beacon Interval SSID
00:12:af:30:01:67   -54dBm           15000 Workshop
00:12:af:30:00:97   -48dBm           15000 stack
00:12:af:30:01:83   -80dBm           15000 Network1
```

Figure 75 Site Survey

Mac Address	Mac address of the access point.
RSSI	Last radio receive signal strength from the access point (only scanned on startup).
Beacon Interval	Beacon Interval configured on the access point.
SSID	SSID of the access point.

5.3 Throughput Testing

Radio Throughput

There are a number of throughput estimations that may help to determine the amount of data that can be successfully transmitted through the modems. These throughput estimations are based on perfect radio conditions in which there is little to no outside radio interference present while data is being passed, and are calculated using real-life conditions and communication constraints.

The performance of a wireless link is best measured in terms of the maximum throughput that can be achieved. Two methods are recommended for measuring modem throughput:

- **Modbus TCP Client Polling**—Use an external Modbus client to poll the internal Modbus server on the remote modem.
- **FTP File Transfer**—Use an FTP server/client arrangement and transfer a file, measuring the time it takes to send.
- **Iperf Throughput Test**—Uses a MS-DOS-based application that is run on a PC or laptop at each end of the radio link and measures the data throughput. When used in conjunction with Jperf, it can display the throughput data graphically.

It is recommended that the throughput tests be performed on point-to-point link with minimal radio interference (no communications from other wireless network traffic). All of the following procedures measure the raw data throughput, and from these throughput measurements you can determine if interference is a contributing factor in the overall performance of the modems.

Modbus TCP Client Polling Test

The following table shows the maximum number of polls per minute (ppm) based on the radio receiver signal level. The results show two test polls using different data speeds, with and without data compression. For more information about data compression and how to implement it, see “Data Compression” on page 35.

The test is designed to simulate a Modbus TCP client polling a Modbus TCP server through the radio modems using two different data rates (2 Level FSK and 4 Level FSK) and scanning a different number of I/O points. The setup for the Modbus client was made to simulate the fastest polling rate possible and then determine the number of messages that were successfully polled in a one minute period. The TCP client scan rate was 5 msec, poll delay was 5 msec, and the slave response time was 10 seconds.

Typical results for this setup are shown below.

Data Throughput – Modbus (Polls per Minute)	4800 Baud (2 level FSK)	9600 Baud (4 Level FSK)
20 Words @ maximum Scan rate – No Compression	72 Ppm	91 Ppm
20 Words @ maximum Scan rate – With Compression	89 Ppm	113 Ppm
120 Words @ maximum Scan rate – No Compression	50 Ppm	58 Ppm
120 Words @ maximum Scan rate – With Compression	89 Ppm	113 Ppm

FTP Fill Transfer Test

Another means for gaging the data throughput performance of the modem is to transfer a known data file using FTP (File Transfer Protocol) and time how long it takes for the file to download. To perform this test you will need a computer at each end of the radio link. One of the PCs will need to run an FTP server application, such as Fillzilla or Cerberus Server, and the other PC needs to run as an FTP client. Because the 450U-E has a reduced throughput compared to other Ethernet modems, you will need to adjust the connection timeout under the settings within the application. Below are some estimated throughputs for FTP transfer using different radio baud rates.

⚠ **NOTE The results will vary depending on the type of file being sent and whether compression is enabled.**

Data Throughput – FTP (file transfer)	4800 baud (2 level FSK)	9600 baud (4 Level FSK)
100 KB text file – No Compression	294 sec @ 0.34 Kbps	185 sec @ 0.72 Kbps
100 KB text file – With Compression	65 sec @ 1.54 Kbps	46 sec @ 2.17 Kbps
134 KB jpg file – No Compression	404 sec @ 0.33 Kbps	185 sec @ 0.72 Kbps
134 KB jpg file – With Compression	215 sec @ 0.62 Kbps	183 sec @ 0.73 Kbps

Iperf Throughput Test

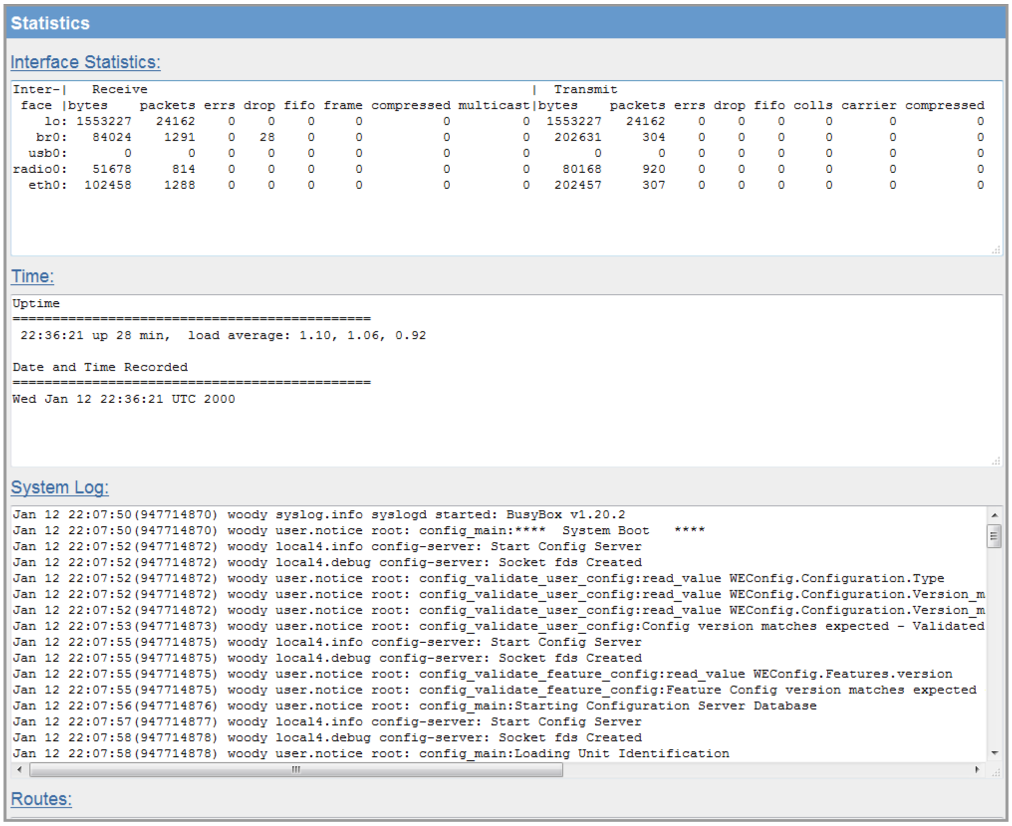
A more thorough test is to perform a throughput test that will check the amount of data that can be reliably achieved via the wireless link. Software tools that can be used to check the data throughput include FTP (File Transfer Protocol), Iperf, and Qcheck. The preferred application is “Iperf,” which is an MS-DOS-based bandwidth measurement application that is run on a laptop or PC at each end of the radio link. The Iperf/Jperf application can be downloaded from http://sourceforge.net/projects/iperf/.

Configure one Iperf session on one of the computers as a server, and another session on the other end of the link as a client. The Iperf client will then pass data over the link, calculate the results, and display the throughput accordingly. See Appendix G for a detailed procedure on using Iperf to externally check radio data throughput.

5.4 Statistics

The Statistics page is used for advanced debugging purposes, and is accessed by clicking **Statistics** on the menu. The page provides detailed information about the state and performance of the 450U-E, and allows you to gather information about how the module is connected and communicating. Dynamic list boxes display statistics about various functions (see Figure 76). This information is useful to ELPRO technical support personnel in diagnosing problems with the module.

⚠ **NOTE When updating the Statistics page, you need to hold down the <CTRL> key while clicking Refresh to ensure that the most up-to-date information is displayed.**



Interface Statistics:

```
Inter-|   Receive                                                |  Transmit
 face |bytes    packets errs drop fifo frame compressed multicast|bytes    packets errs drop fifo colls carrier compressed
    lo: 1553227   24162    0    0    0     0          0         0 1553227   24162    0    0    0     0       0          0
   br0:   84024    1291    0   28    0     0          0         0  202631     304    0    0    0     0       0          0
  usb0:       0       0    0    0    0     0          0         0       0       0    0    0    0     0       0          0
radio0:   51678     814    0    0    0     0          0         0   80168     920    0    0    0     0       0          0
  eth0:  102458    1288    0    0    0     0          0         0  202457     307    0    0    0     0       0          0
```

Time:

```
Uptime
=============================================
 22:36:21 up 28 min,  load average: 1.10, 1.06, 0.92

Date and Time Recorded
=============================================
Wed Jan 12 22:36:21 UTC 2000
```

System Log:

```
Jan 12 22:07:50(947714870) woody syslog.info syslogd started: BusyBox v1.20.2
Jan 12 22:07:50(947714870) woody user.notice root: config_main:****  System Boot   ****
Jan 12 22:07:52(947714872) woody local4.info config-server: Start Config Server
Jan 12 22:07:52(947714872) woody local4.debug config-server: Socket fds Created
Jan 12 22:07:52(947714872) woody user.notice root: config_validate_user_config:read_value WEConfig.Configuration.Type
Jan 12 22:07:52(947714872) woody user.notice root: config_validate_user_config:read_value WEConfig.Configuration.Version_m
Jan 12 22:07:52(947714872) woody user.notice root: config_validate_user_config:read_value WEConfig.Configuration.Version_m
Jan 12 22:07:53(947714873) woody user.notice root: config_validate_user_config:Config version matches expected - Validated
Jan 12 22:07:55(947714875) woody local4.info config-server: Start Config Server
Jan 12 22:07:55(947714875) woody local4.debug config-server: Socket fds Created
Jan 12 22:07:55(947714875) woody user.notice root: config_validate_feature_config:read_value WEConfig.Features.version
Jan 12 22:07:55(947714875) woody user.notice root: config_validate_feature_config:Feature Config version matches expected
Jan 12 22:07:56(947714876) woody user.notice root: config_main:Starting Configuration Server Database
Jan 12 22:07:57(947714877) woody local4.info config-server: Start Config Server
Jan 12 22:07:58(947714878) woody local4.debug config-server: Socket fds Created
Jan 12 22:07:58(947714878) woody user.notice root: config_main:Loading Unit Identification
```

Routes:

Figure 76 Statistics

Interface Statistics Displays the number of bytes transmitted and received and the number of CRC errors, dropped packets, FIFO alarms, and types of frames (fragmented, compressed or multicast). This is the main area for gathering diagnostics information, because it indicates how the radios are communicating.

Time Shows how long the module has been running since its last reset.

System Log Displays a running log of information about how the module's operating system is running. The log also shows any errors and resets.

Routes Displays the current IP routes configured in the module.

IP statistics Displays various of statistics for each interface.

TCP/UDP Statistics Shows the number of TCP and UDP connections currently established.

Memory Statistics Shows the amount of memory available for each function.

Serial Statistics Shows the current status of each of the serial ports.

Network Traffic Analysis

There are many devices and PC programs that can analyze the performance of an Ethernet network. A freely available program, such as "Ethereal," provides a simple cost effective means for more advanced analysis. By monitoring traffic on the wired Ethernet, you can gain a better idea of regular traffic. Network analysis programs make configuring a filter for the 450U-E a simple task.

5.5 Channel Survey

The Channel Survey page provides a visual display of how busy the current radio channel is over a given period of time. Channel utilization is logged by the radio over three separate time intervals:

- 1 second intervals, which covers the previous 60 seconds
- 1 minute intervals, which covers the last 60 minutes
- 1 hour intervals, which covers the last 60 hours

At any given time, an access point and its associated clients occupy a radio channel. This radio channel, or frequency, may contain interference from other radio transmitters. When installing or diagnosing the 450U-E modem, the potential capacity of a given radio channel will be reduced by the existence of these other interfering RF signals.

Channel utilization allows us to see how much RF activity is on a given channel as a percentage of the total utilization. When reviewing the utilization graph, you need to look at the average percentage level (rather than peak bursts), and also look at the average percentage over a longer time period. It is normal for the graph to show bursts of 60–80% utilization, because the 450U-E uses the majority of the channel when transmitting due to the lower bandwidth. If most of the graph is filled to 60–80%, it indicates there is excessive traffic. A channel that is very busy will have high channel utilization. Conversely, a channel that is quiet will have low channel utilization.

The Channel Survey and Custom Survey can be valuable tools when performing site surveys because they allow you to determine how much of the frequency is being used. They are also valuable diagnostics tools for identifying possible sources of interference.

Channel Utilization on a Live System

Channel utilization can be used on a live system, and is the simplest method for determining how busy the channel is and how much spare capacity the channel has for additional data transfers. Performing a standard channel survey scan on a live system will show all transmit and receive packet from the system. It may also show transmit and receive packets for other systems if they happen to be on the same frequency.

To identify possible interference on the current channel, you can use the Custom Survey page and select “All RX Frames.” If possible, temporarily disable all data transfer on the system. If the channel utilization remains high, it will confirm the presence of outside interference.

Diagnosing Low Throughput

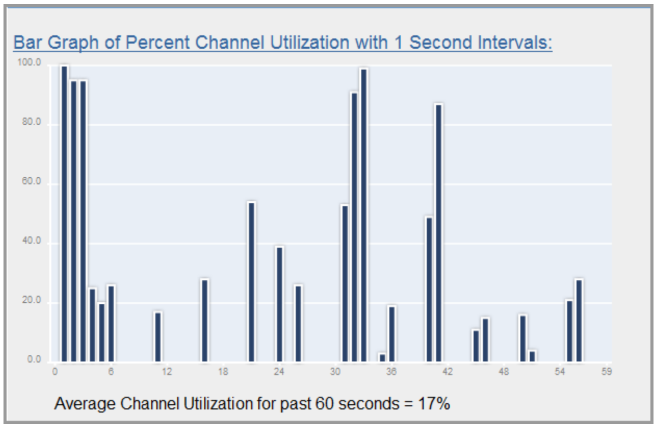
If normal communications between modems is poor, as determined by data throughput measurements are lower than estimated it could be attributed to interference (see “5.3 Throughput Testing” on page 71). The channel utilization graphs can be used to confirm how much other radio traffic or interference is present. If the channel utilization is high, this could be the contributing factor in poor throughput performance. If the channel utilization was low (indicating little interference), poor throughput performance could be attributed to a low RSSI, which can be checked on the Connectivity page (see “5.2 Connectivity” on page 70).

Channel Utilization Graphs

The Channel Survey page displays a graph showing the percentage of time that a channel is being used for any of the following activities:

- The connected modem is transmitting.
- The connected modem is receiving valid data from other ELPRO 450U-E modems in the system.
- The connected modem is receiving valid data from other 450U-E modems that are not in the system but are on the same frequency, or from modems in the same system that are not communicating directly but through repeaters.

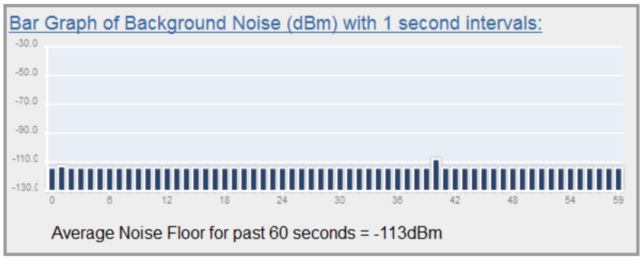
There are three time periods displayed on the page—one second, one minute, and one hour. Each graph shows the channel utilization and background noise level over that time period. Figure 77 shows the radio traffic on the channel over the last 60 seconds and a calculated average percentage of utilization for the one minute period.


Bar Graph of Percent Channel Utilization with 1 Second Intervals:

Average Channel Utilization for past 60 seconds = 17%

Figure 77 Channel Utilization (Seconds)

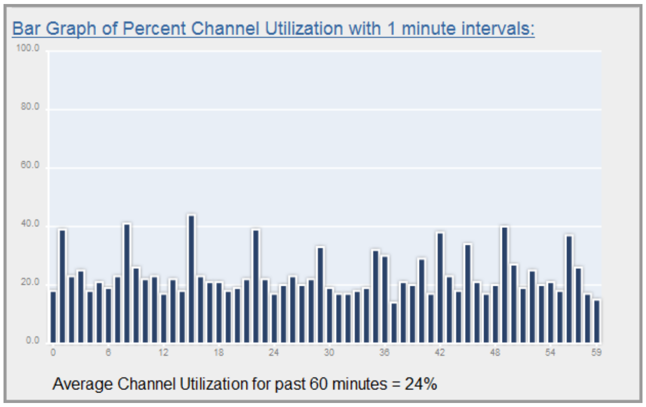
Figure 78 shows the radio background noise level for the last 60 seconds.


Bar Graph of Background Noise (dBm) with 1 second intervals:

Average Noise Floor for past 60 seconds = -113dBm

Figure 78 Background Noise (Seconds)

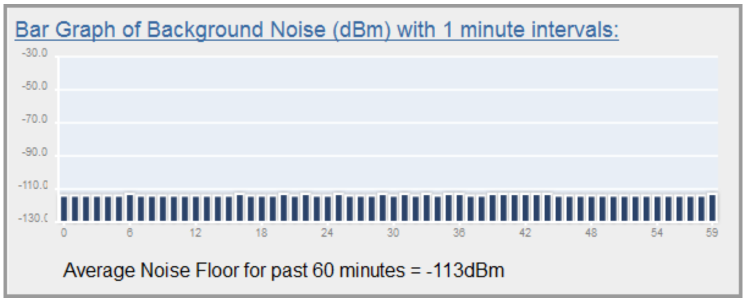
Figure 79 shows the Channel utilization for each minute over a one-hour period. Each minute is calculated from the running average of the 60-second scan.


Bar Graph of Percent Channel Utilization with 1 minute intervals:

Average Channel Utilization for past 60 minutes = 24%

Figure 79 Channel Utilization Minutes

Figure 80 shows the running radio background average noise level for each minute over the last one hour period. The Channel Survey page also shows two graphs (not shown here) which indicate the Percent Channel Utilization (average readings from each minute) and the Noise Floor in one hour intervals (the graphs will only show the last 60-hour period.


Bar Graph of Background Noise (dBm) with 1 minute intervals:

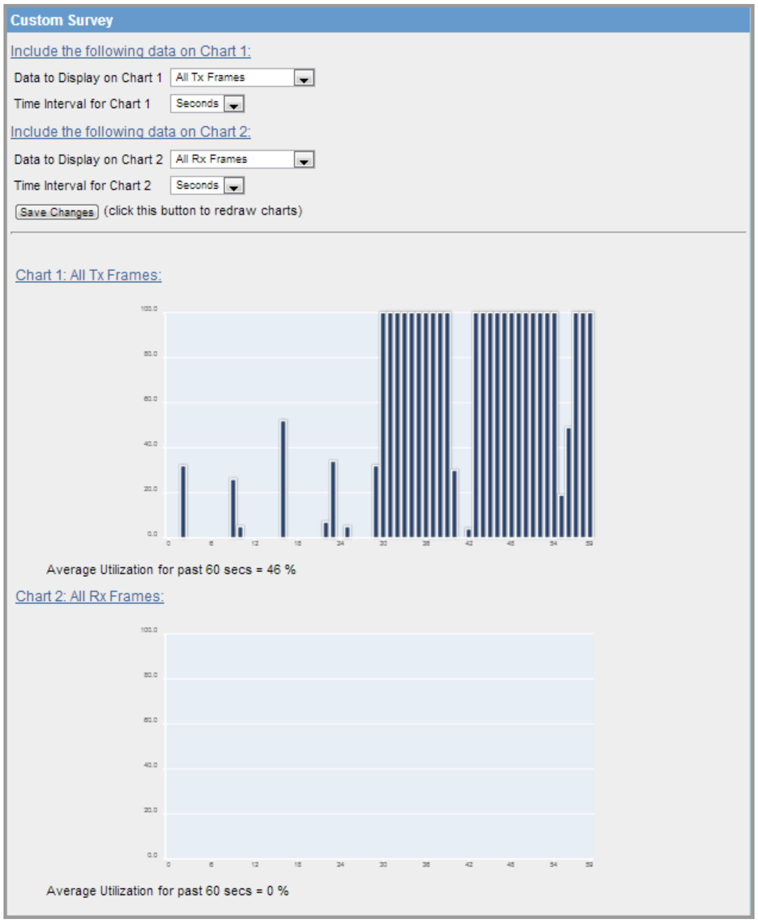
Average Noise Floor for past 60 minutes = -113dBm

Figure 80 Background Noise Minutes

5.6 Custom Survey

The **Custom Survey** page (Figure 81) displays two separate charts that can be configured to show different radio channel characteristics over three time scales (seconds, minutes, or hours). The custom survey is similar to the channel survey (see the previous section) except that it allows two sets of channel-related data to be displayed—which is useful for diagnosing channel utilization problems.

The default selection on the Custom Survey page shows the total percentage of transmitted frames over a 60-second period in chart one, and the total percentage of received frames over a 60-second period in chart two. From this default view you can determine if there are too many transmissions being sent from this radio and if there are too many radio messages being received from other sites in the radio network. To display different data, select the data components from the drop-down list, select a time interval, and click **Save Changes** to refresh the graphs. Each graph displays a percent channel utilization using the selected criteria and time interval (seconds, minutes or hours).


Custom Survey

Include the following data on Chart 1:

Data to Display on Chart 1: All Tx Frames

Time Interval for Chart 1: Seconds

Include the following data on Chart 2:

Data to Display on Chart 2: All Rx Frames

Time Interval for Chart 2: Seconds

(click this button to redraw charts)

Chart 1: All Tx Frames:

Average Utilization for past 60 secs = 46 %

Chart 2: All Rx Frames:

Average Utilization for past 60 secs = 0 %

Figure 81 Custom Survey

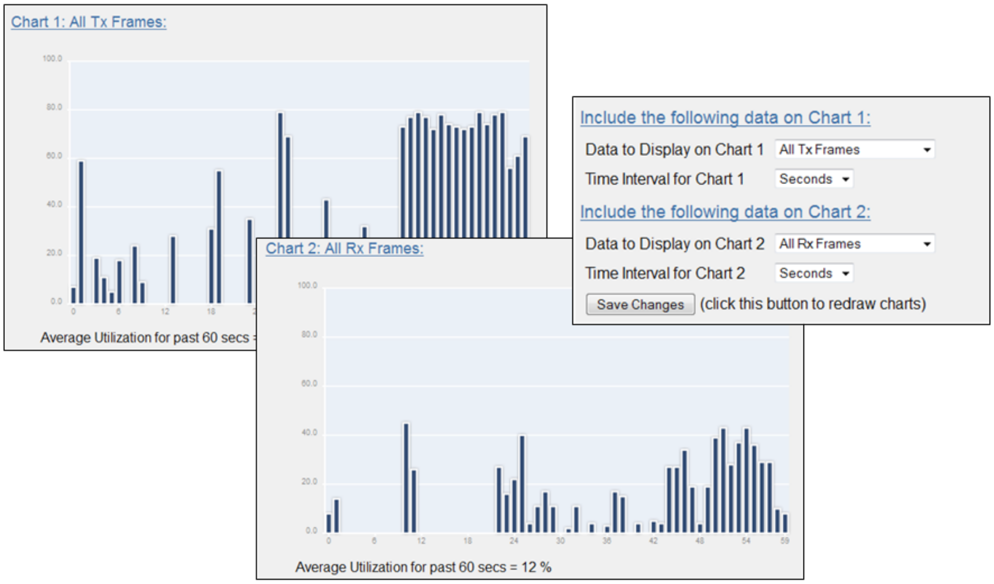
The following table describes the data components that can be selected for graphing.

Custom Selections	Description
All TX & RX Frames	All ELPRO transmissions sent and received by the radio being monitored. This option is the same as the normal Channel Survey explained in “5.5 Channel Survey” on page 74.
All TX Frames	All data frames transmitted by the radio being monitored. This is the default for chart one and will help to segregate the overall channel utilization into transmissions from the radio being monitored or transmissions from other radios. This option encompasses TX first attempt, TX retries and TX ACK messages described in this table.
All RX Frames	All data frames received by the radio being monitored. This is the default for chart two and will display only received ELPRO data frames.
TX First Attempt Messages	Amount of time spent transmitting first-attempt messages from the modem (all messages will be retried if the first do not succeed). This option allows you to log the number of times messages fail to get through on the first attempt, which can indicate some level of interference because the message may have clashed with other radio messages. This option (along with TX Retries and TX Acknowledge) is useful for breaking down the amount of time spent transmitting messages into “normal transmissions,” “retries,” and “acknowledgments.”
TX Retries	Percentage of time spent transmitting retry messages from the modem. This is useful for determining if the communications get through after the first retry or they continue to fail.
TX Acknowledge Messages	Percentage of time spent transmitting acknowledgment messages from the modem and Broadcast messages.
Radio Hold Off	Percentage of time that the radio has spent holding off from transmitting data, possibly because the channel is busy.
RX to This Radio	Percentage of time receiving messages specifically for the radio being monitored. For example, ELPRO radio communication frames from other modems in the system that are specifically addressed to this modem.
RX to Other Radios	Percentage of time receiving valid ELPRO messages addressed to other radios within the system. For example, radios may be communicating through a repeater and the host can hear the message directly. This is useful for determining how much radio traffic the modem can hear that it may not need to hear.
RX Acknowledgments	Percentage of time receiving acknowledge messages.
RX Errors	Percentage of time handling radio receive error messages, such as corrupted data, and data collisions.

Example 1

A good test would be to configure chart one to show “All Tx Frames,” which are all valid data frames transmitted over the radio link, and configure chart two to show “All Rx Frames,” which are all valid data frames received from any source (ELPRO 450U-E data frames). From the results shown Figure 82, you can see that Chart 1 shows a large amount of data is being transmitted in the last part of the 60-second scan (the end of the chart), and the receive data in Chart 2 also shows a slight increase in traffic. From this you can deduce that the radio itself or a device on the Ethernet network of the radio is transmitting a large amount of data.

If the charts showed an increased number of RX Frames instead of TX frames, it would indicate one or all of the remote radios are transmitting excessive data, and it would be advisable to perform the same TX/RX Custom Survey on these remote site/sites to determine the cause for the excessive data.



Average Utilization for past 60 secs =

Average Utilization for past 60 secs = 12 %

Include the following data on Chart 1:

Data to Display on Chart 1: All Tx Frames

Time Interval for Chart 1: Seconds

Include the following data on Chart 2:

Data to Display on Chart 2: All Rx Frames

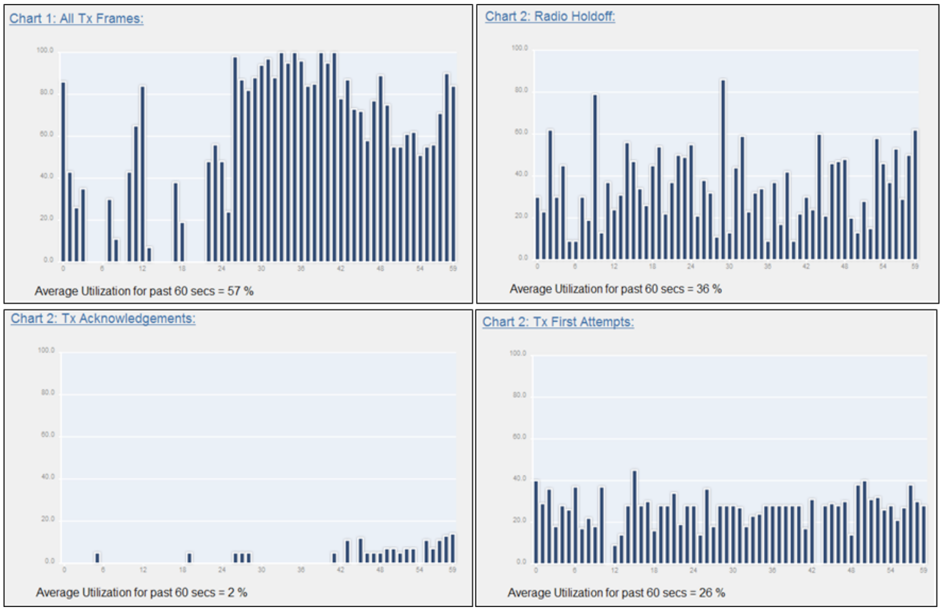
Time Interval for Chart 2: Seconds

(click this button to redraw charts)

Figure 82 Custom Survey 1

Example 2

In the second example, we can see that Chart 1 shows the radio is transmitting a large amount of data in the last half of the sixty second scan. Configuring the second chart to read specific information about the radio link can help us determine what is causing the increase in traffic. The “Chart 2: Radio Holdoff” shows that the radio is holding off from transmitting around 36% of the time, which is a clear indication that the radio frequency is busy. The other two charts show that it is not transmitting many acknowledgments, but is send a number of first attempts indicating that it is initiating the increase in communications.



Average Utilization for past 60 secs = 57 %

Average Utilization for past 60 secs = 36 %

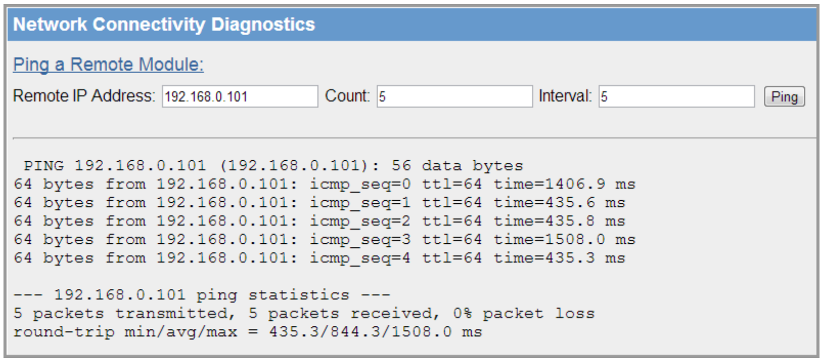
Average Utilization for past 60 secs = 2 %

Average Utilization for past 60 secs = 26 %

Figure 83 Custom Survey 2

5.7 Network Diagnostics

The **Network Diagnostics** page allows you to check the communications path to other modules within the system.



Network Connectivity Diagnostics

Ping a Remote Module:

Remote IP Address: 192.168.0.101 Count: 5 Interval: 5 Ping

```
 PING 192.168.0.101 (192.168.0.101): 56 data bytes
64 bytes from 192.168.0.101: icmp_seq=0 ttl=64 time=1406.9 ms
64 bytes from 192.168.0.101: icmp_seq=1 ttl=64 time=435.6 ms
64 bytes from 192.168.0.101: icmp_seq=2 ttl=64 time=435.8 ms
64 bytes from 192.168.0.101: icmp_seq=3 ttl=64 time=1508.0 ms
64 bytes from 192.168.0.101: icmp_seq=4 ttl=64 time=435.3 ms

--- 192.168.0.101 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 435.3/844.3/1508.0 ms
```

Figure 84 Network Diagnostics

Ping a Remote Module

Ping is a standard network instruction that sends a small data probe to the IP address configured, letting you know whether you have a communication path. You will receive a response for each Ping, that will show packet size, IP address, sequence number, and time, in milliseconds. This is followed by a summary showing the number of packets transmitted, the number of packets received, the number of packets lost, and the minimum, average and maximum Ping times, in milliseconds.

A Ping can be executed on either the radio network or Ethernet network. The Ping command will automatically select the correct network interface according to the address selected.

Remote IP Address

The IP address that you want to Ping.

Count / Max Hops

Number of Ping probes that are send out. You should see this many responses come back.

Interval

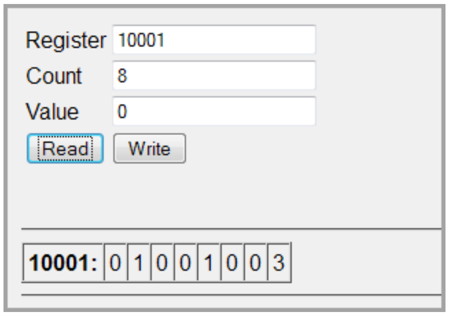
Wait time between Ping requests. Default is 5 seconds, and typically will not need to be changed unless using repeaters.

5.8 IO Diagnostics

Click **I/O Diagnostics** on the menu read and write the I/O store registers within the module (Figure 85).

- To read a register location, enter an address location (for example, 10001–12500 for digital inputs), enter a count (number of consecutive registers) and then click **Read**. You will see the returned address location and the returned values. When reading the status of the DIO on the module, if you see the value “3” it indicates that the DIO is being used as an output in the “on” state.
- To write to an output register location (for example, 1–2500), enter the address location, count, and value, and then click **Write**. For example, a write to register 1 with a count of 1 and a value of 1 will turn the local digital output on.
- To read an analog register location, enter an address location (for example, 30001–32500) enter a count (number of consecutive registers), and then click **Read**.

⚠ **NOTE If you read a register and get the symbol “~“, it indicates that the register is in an invalid state and has no value (not even zero). See “Invalid Register State” on page 64 for details.**


Register 10001
Count 8
Value 0

10001: 0 1 0 0 1 0 0 3

Figure 85 I/O Diagnostics

Modem Module Information Registers

There are registers available in the module that show modules characteristics, such as serial number and firmware version. This information is available on the home webpage of the module’s Web Server. Having the information available in registers allows a host system to read the values via Modbus (provided the Modbus has been activated).

- Register 30494, 30495, and 30496 = Module serial number
- Register 30497, 30498, and 30499 = Module firmware version
- Register 30500 = Firmware patch level.

Expansion I/O Diagnostic/Error Registers

The 450U-E has a number of diagnostics registers are allocated for expansion I/O diagnostic information. Every connected module has its own diagnostic information that indicates the module type, error counts, error codes, and so on. The register locations are dynamic with regard to the module address, and require an offset to read the correct location. The offset can be calculated by reading the module’s Modbus address, which can be read on the rotary switches on the end on the expansion module, and multiplying this by 20. For example, if a module has an address of 2, the offset is (2 x 20) = 40. If it has an address of 18, the offset is (18 x 20) = 360.

Each expansion I/O module has the following diagnostic registers. Add the offset to the fixed register number to get the actual register location.

Fixed Register	Description	Example
30017	Modbus Error Counter Number of Modbus errors the modules has had since it was powered on.	If the module address is #2, the register location will be 30017+ (2*20) = 30057.
30018	Last 115S Status Code Modbus Error Code that the module has had.	If the module address is #2, the register location will be 30018 + (2*20) = 30058.
30019	Modbus Lost Link Counter Number of communication errors.	If the module address is #2, the register location will be 30019 + (2*20) = 30059.
30020	Expansion I/O Module Type • dec 257 (101hex) indicates a 115S-11 module • dec 513 (201hex) indicates a 115S-12 module • dec 769 (301hex) indicates a 115S-13 module	If the module address is #2, the register location will be 30020 + (2*20) = 30060.

115S Expansion I/O Error Codes

These error codes are initiated by the 450U-E when trying to communicate with 115S expansion I/O modules, and will only be available if “Expansion I/O” has been selected as the port type on the Serial configuration page (see “4.7 Serial Configuration” on page 35).

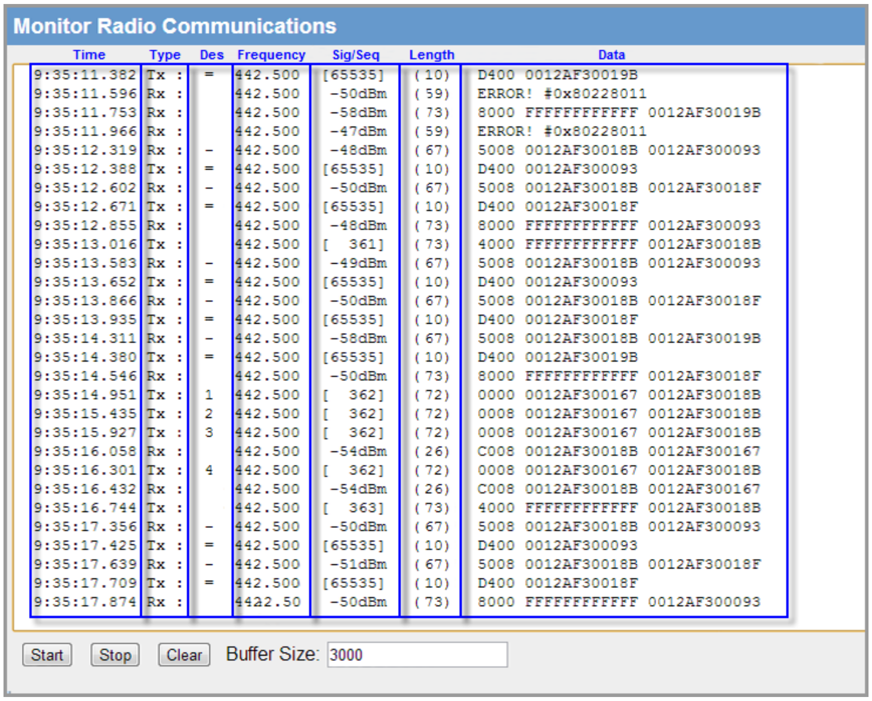
Appendix D describes Modbus Error Response Codes that are responses from the slave device showing any errors it has with the communications.

Dec Code	Hex Code	Name	Meaning
1	0x0001	No Response	No response from a poll.
2	0x0002	Corrupt/Invalid	Corrupt or invalid data.
3	0x0003	CRC Fail	CRC error check does not match the message, Different message or possible data corruption.
4	0x0004	Response did not match request.	The response heard was not the correct ID, possibly heard other RS-485 traffic.
5	0x0005	Message type did not match request.	The response heard did not match the requested poll (different command response). Possibly heard other RS-485 traffic.
81	0x0129	Problem accessing local memory.	Could not access register location, possibly because the register is not initialized.

5.9 Monitor Radio Comms

The **Monitor Radio Comms** page shows radio communication frames received or transmitted by the radio. The example in Figure 86 shows typical data frames from the communication log screen. Corrupted data frames are shown with an “ERROR!” within the frame.

NOTE The Comms Log displays ELPRO 450U-E data frames only.



```
    Time        Type  Des  Frequency  Sig/Seq   Length            Data
9:35:11.382 Tx :   =   442.500   [65535]   ( 10)   D400 0012AF30019B
9:35:11.596 Rx :       442.500    -50dBm   ( 59)   ERROR! #0x80228011
9:35:11.753 Rx :       442.500    -58dBm   ( 73)   8000 FFFFFFFFFFFF 0012AF30019B
9:35:11.966 Rx :       442.500    -47dBm   ( 59)   ERROR! #0x80228011
9:35:12.319 Rx :   -   442.500    -48dBm   ( 67)   5008 0012AF30018B 0012AF300093
9:35:12.388 Tx :   =   442.500   [65535]   ( 10)   D400 0012AF300093
9:35:12.602 Rx :   -   442.500    -50dBm   ( 67)   5008 0012AF30018B 0012AF30018F
9:35:12.671 Tx :   =   442.500   [65535]   ( 10)   D400 0012AF30018F
9:35:12.855 Rx :       442.500    -48dBm   ( 73)   8000 FFFFFFFFFFFF 0012AF300093
9:35:13.016 Tx :       442.500   [   361]  ( 73)   4000 FFFFFFFFFFFF 0012AF30018B
9:35:13.583 Rx :   -   442.500    -49dBm   ( 67)   5008 0012AF30018B 0012AF300093
9:35:13.652 Tx :   =   442.500   [65535]   ( 10)   D400 0012AF300093
9:35:13.866 Rx :   -   442.500    -50dBm   ( 67)   5008 0012AF30018B 0012AF30018F
9:35:13.935 Tx :   =   442.500   [65535]   ( 10)   D400 0012AF30018F
9:35:14.311 Rx :   -   442.500    -58dBm   ( 67)   5008 0012AF30018B 0012AF30019B
9:35:14.380 Tx :   =   442.500   [65535]   ( 10)   D400 0012AF30019B
9:35:14.546 Rx :       442.500    -50dBm   ( 73)   8000 FFFFFFFFFFFF 0012AF30018F
9:35:14.951 Tx :   1   442.500   [   362]  ( 72)   0000 0012AF300167 0012AF30018B
9:35:15.435 Tx :   2   442.500   [   362]  ( 72)   0008 0012AF300167 0012AF30018B
9:35:15.927 Tx :   3   442.500   [   362]  ( 72)   0008 0012AF300167 0012AF30018B
9:35:16.058 Rx :       442.500    -54dBm   ( 26)   C008 0012AF30018B 0012AF300167
9:35:16.301 Tx :   4   442.500   [   362]  ( 72)   0008 0012AF300167 0012AF30018B
9:35:16.432 Rx :       442.500    -54dBm   ( 26)   C008 0012AF30018B 0012AF300167
9:35:16.744 Tx :       442.500   [   363]  ( 73)   4000 FFFFFFFFFFFF 0012AF30018B
9:35:17.356 Rx :   -   442.500    -50dBm   ( 67)   5008 0012AF30018B 0012AF300093
9:35:17.425 Tx :   =   442.500   [65535]   ( 10)   D400 0012AF300093
9:35:17.639 Rx :   -   442.500    -51dBm   ( 67)   5008 0012AF30018B 0012AF30018F
9:35:17.709 Tx :   =   442.500   [65535]   ( 10)   D400 0012AF30018F
9:35:17.874 Rx :       4422.50    -50dBm   ( 73)   8000 FFFFFFFFFFFF 0012AF300093
```

Buffer Size: 3000

Figure 86 Monitor Radio Comms

Time Message time stamp—the time from when module was last started.

Message Type Indicates whether the message is a transmit (Tx) or a receive (Rx) Ethernet frame.

Des

The frame designator (labeled “Des”) can be blank or any of the following characters: -, *, =, 1, 2, 3 or 4.

- **RX “blank”** indicates a received packet is a broadcast packet; no acknowledgment is required.
- **RX “-”** indicates a received packet requires a message acknowledgment.
- **RX “*”** indicates acknowledgment of a previously transmitted packet from this radio.
- **TX “1,2,3,4”** indicates the number of times the packet has been transmitted (reties).
- **TX “=”** indicates the transmitted packet is an acknowledgment of a previously received frame.
- **TX “blank”** indicates the transmitted packet is a broadcast packet; no acknowledgment required.

Frequency

Shows the frequency of the RX/TX frame.

Sig/Seq

Signal/Seq Number. Shows the receive signal level on any received message, or an internal handle number used for transmitted messages. If the number is 65535, it indicates its an ACK transmission.

Data Length

Total length of the transmitted or received message.

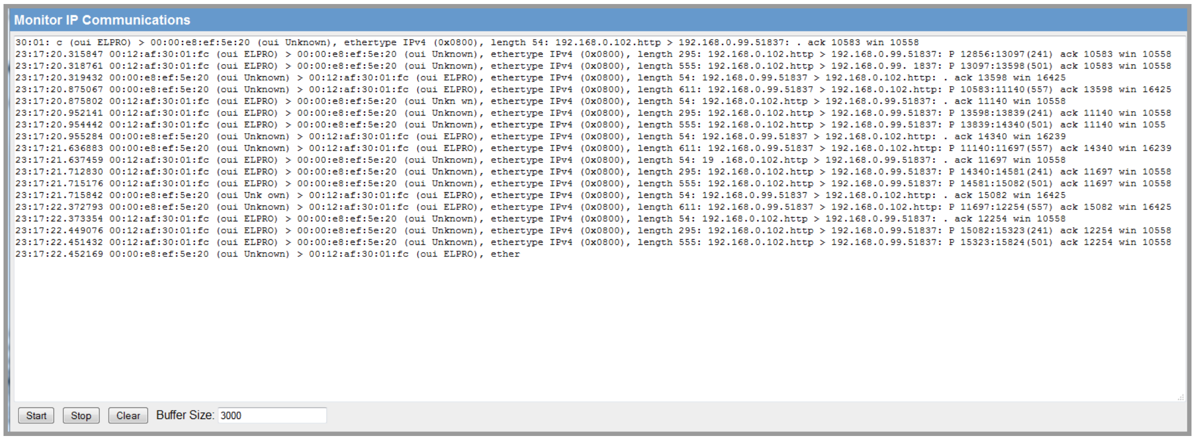
Data

Data packet. The first 16-bit number is the frame control field, of which the first two digits indicate the standard 802.11 frame type. The table below shows some of the more common codes associated with the frame type. For more information, consult the 802.11 specifications. The last two numbers indicate the destination MAC address and the source MAC address. If the message is a TX ACK, as indicated by the message type and the D4 Frame Code, there will only be one MAC address shown.

Frame Code	Description
Management	
0	Association request
10	Association response
20	Re-association request
30	Re-association response
40	Probe request
50	Probe response
80	Beacon
A0	Disassociation
B0	Authentication
C0	De-authentication
D0	Action
Control	
D4	ACK
Data	
8	Data
48	Null (no data)

5.10 Monitor IP Comms

This option shows the standard IP communication data frames and allows you to see the source and destination MAC addresses, along with other IP communications data. More information on standard IP communications can be found on the Internet.



```
30:01: c (oui ELPRO) > 00:00:e8:ef:5e:20 (oui Unknown), ethertype IPv4 (0x0800), length 54: 192.168.0.102.http > 192.168.0.99.51837: . ack 10583 win 10558
23:17:20.315847 00:12:af:30:01:fc (oui ELPRO) > 00:00:e8:ef:5e:20 (oui Unknown), ethertype IPv4 (0x0800), length 295: 192.168.0.102.http > 192.168.0.99.51837: P 12856:13097(241) ack 10583 win 10558
23:17:20.318761 00:12:af:30:01:fc (oui ELPRO) > 00:00:e8:ef:5e:20 (oui Unknown), ethertype IPv4 (0x0800), length 555: 192.168.0.102.http > 192.168.0.99. 1837: P 13097:13598(501) ack 10583 win 10558
23:17:20.319432 00:00:e8:ef:5e:20 (oui Unknown) > 00:12:af:30:01:fc (oui ELPRO), ethertype IPv4 (0x0800), length 54: 192.168.0.99.51837 > 192.168.0.102.http: . ack 13598 win 16425
23:17:20.875067 00:00:e8:ef:5e:20 (oui Unknown) > 00:12:af:30:01:fc (oui ELPRO), ethertype IPv4 (0x0800), length 611: 192.168.0.99.51837 > 192.168.0.102.http: P 10583:11140(557) ack 13598 win 16425
23:17:20.875802 00:12:af:30:01:fc (oui ELPRO) > 00:00:e8:ef:5e:20 (oui Unkn wn), ethertype IPv4 (0x0800), length 54: 192.168.0.102.http > 192.168.0.99.51837: . ack 11140 win 10558
23:17:20.952141 00:12:af:30:01:fc (oui ELPRO) > 00:00:e8:ef:5e:20 (oui Unknown), ethertype IPv4 (0x0800), length 295: 192.168.0.102.http > 192.168.0.99.51837: P 13598:13839(241) ack 11140 win 10558
23:17:20.954442 00:12:af:30:01:fc (oui ELPRO) > 00:00:e8:ef:5e:20 (oui Unknown), ethertype IPv4 (0x0800), length 555: 192.168.0.102.http > 192.168.0.99.51837: P 13839:14340(501) ack 11140 win 1055
23:17:20.955284 00:00:e8:ef:5e:20 (oui Unknown) > 00:12:af:30:01:fc (oui ELPRO), ethertype IPv4 (0x0800), length 54: 192.168.0.99.51837 > 192.168.0.102.http: . ack 14340 win 16239
23:17:21.636883 00:00:e8:ef:5e:20 (oui Unknown) > 00:12:af:30:01:fc (oui ELPRO), ethertype IPv4 (0x0800), length 611: 192.168.0.99.51837 > 192.168.0.102.http: P 11140:11697(557) ack 14340 win 16239
23:17:21.637459 00:12:af:30:01:fc (oui ELPRO) > 00:00:e8:ef:5e:20 (oui Unknown), ethertype IPv4 (0x0800), length 54: 19 .168.0.102.http > 192.168.0.99.51837: . ack 11697 win 10558
23:17:21.712830 00:12:af:30:01:fc (oui ELPRO) > 00:00:e8:ef:5e:20 (oui Unknown), ethertype IPv4 (0x0800), length 295: 192.168.0.102.http > 192.168.0.99.51837: P 14340:14581(241) ack 11697 win 10558
23:17:21.715176 00:12:af:30:01:fc (oui ELPRO) > 00:00:e8:ef:5e:20 (oui Unknown), ethertype IPv4 (0x0800), length 555: 192.168.0.102.http > 192.168.0.99.51837: P 14581:15082(501) ack 11697 win 10558
23:17:21.715842 00:00:e8:ef:5e:20 (oui Unk own) > 00:12:af:30:01:fc (oui ELPRO), ethertype IPv4 (0x0800), length 54: 192.168.0.99.51837 > 192.168.0.102.http: . ack 15082 win 16425
23:17:22.372793 00:00:e8:ef:5e:20 (oui Unknown) > 00:12:af:30:01:fc (oui ELPRO), ethertype IPv4 (0x0800), length 611: 192.168.0.99.51837 > 192.168.0.102.http: P 11697:12254(557) ack 15082 win 16425
23:17:22.373354 00:12:af:30:01:fc (oui ELPRO) > 00:00:e8:ef:5e:20 (oui Unknown), ethertype IPv4 (0x0800), length 54: 192.168.0.102.http > 192.168.0.99.51837: . ack 12254 win 10558
23:17:22.449076 00:12:af:30:01:fc (oui ELPRO) > 00:00:e8:ef:5e:20 (oui Unknown), ethertype IPv4 (0x0800), length 295: 192.168.0.102.http > 192.168.0.99.51837: P 15082:15323(241) ack 12254 win 10558
23:17:22.451432 00:12:af:30:01:fc (oui ELPRO) > 00:00:e8:ef:5e:20 (oui Unknown), ethertype IPv4 (0x0800), length 555: 192.168.0.102.http > 192.168.0.99.51837: P 15323:15824(501) ack 12254 win 10558
23:17:22.452169 00:00:e8:ef:5e:20 (oui Unknown) > 00:12:af:30:01:fc (oui ELPRO), ether
```

Buffer Size: 3000

Figure 87 Monitor IP Comms

4.11 System Tools

The **System Tools** page has various tools that help maintain the module firmware and configuration.

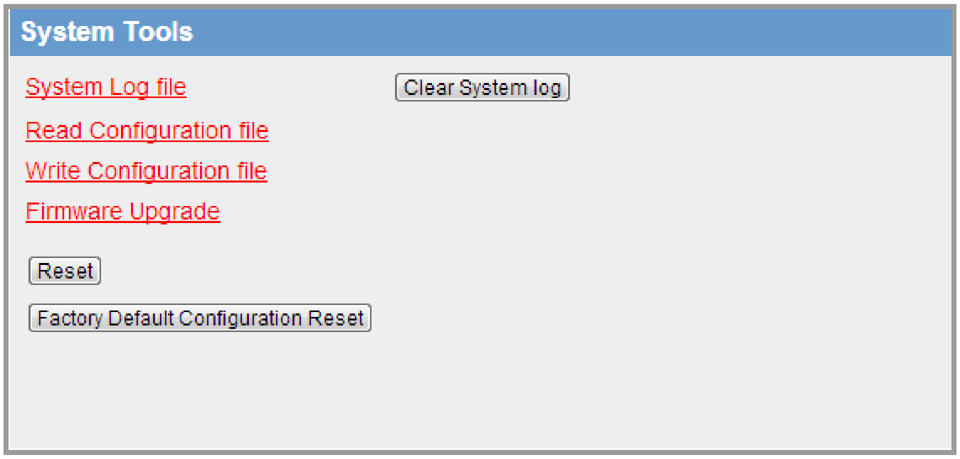


Figure 88 System Tools

System Log File Shows an event log of the modules operation, used for diagnosing problems. The page can be saved and emailed to ELPRO, if requested. Click Clear System Log to erase the log file and start fresh.

Read Configuration File This option shows the module configuration in XML format. This file can be saved for future reference or backup.

Write Configuration File Configuration XML files saved using the Read Configuration File option can be loaded back into the module using this option.

Firmware Upgrade This option is used for patch firmware upgrades only. Click Browse to locate the file, and then click Send to load the file into the module. When the update is complete, click Reset. A firmware upgrade can be performed locally, or remotely via the radio.

For instructions on executing a full upgrade, see Appendix A.

Reset Resets the module.

Factory Default Configuration Loads the factory default configuration and resets.

⚠ **CAUTION Loading the factory default configuration will overwrite any current configuration.**

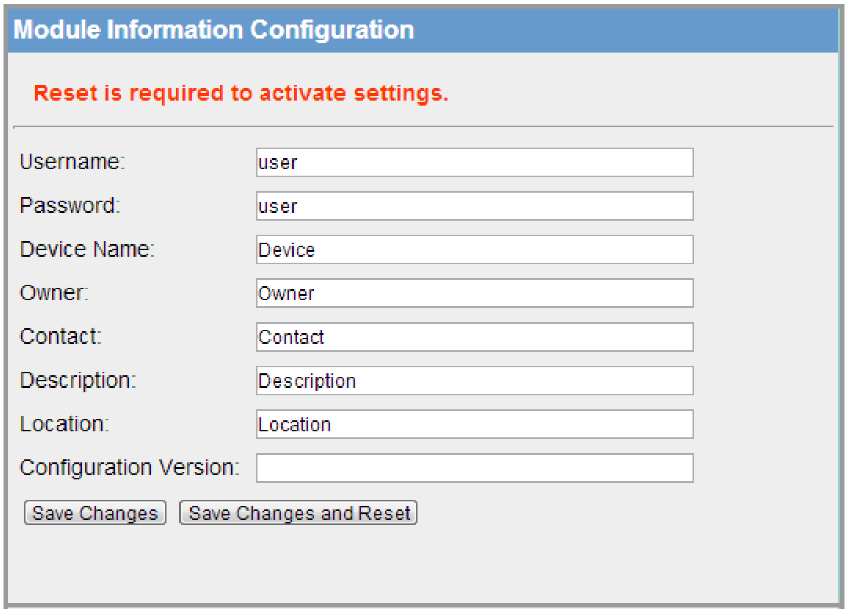
Setting a 450U-E to Factory Default Settings

1. Access the Web Server on the 450U-E (for details, see “4.1 Connecting and Logging On” on page 22).
2. Click **System Tools** on the menu.
3. Click **Factory Default Configuration Reset**, and wait for unit to reset.

   While the module executes the reset sequence, the OK LED flashes. The OK LED turns green when the reset sequence is completed. After the module resets, you should be able connect to the module’s default IP address, which is displayed on the label on the bottom of the module.

5.12 Module Information

Use the **Module Information** page to change the username and password, and the module information that appears on the home page of the 450U-E Web Server.



Module Information Configuration

Reset is required to activate settings.

Username: user
Password: user
Device Name: Device
Owner: Owner
Contact: Contact
Description: Description
Location: Location
Configuration Version:

Figure 89 Module Information

Username Current username for accessing the 450U-E Web Server. You can change the username by entering a new username and clicking **Save Changes and Reset**. Be sure to record the new username for future reference.

Password Current password for accessing the 450U-E Web Server. You can change the password by entering a new password and clicking **Save Changes and Reset**. Be sure to record the new password for future reference.

Device Name Allows you to label the 450U-E. This will also become the DNS name (hostname) of the device if you are using DNS.

Owner Allows you to specify an owner name.

Contact Owner phone number, email address, and other contact information.

Description Description of the purpose of the 450U-E module.

Location Location description for the 450U-E.

Configuration Version Allows you to enter in a version for the configuration

5.13 Utilities

Ping Command

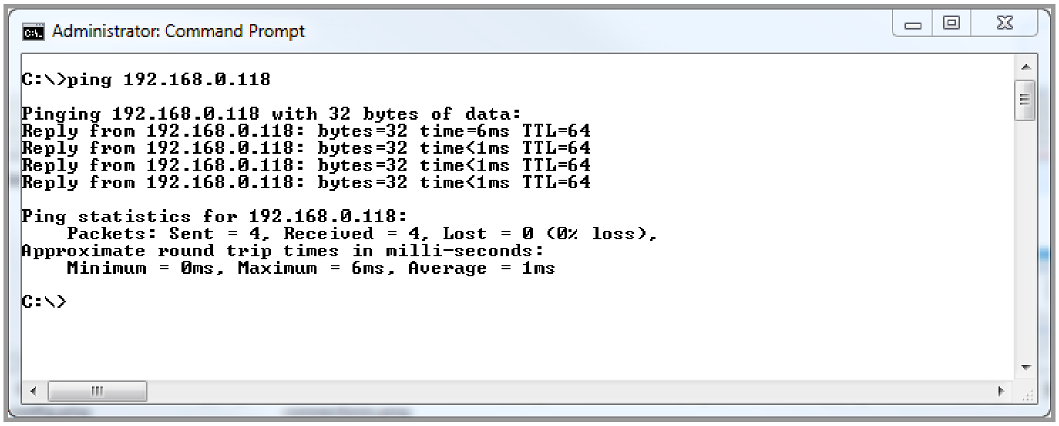
The “ping” command is a basic Internet program that lets you verify that a particular IP address exists and can accept requests. Ping is used diagnostically to ensure that a host computer that you are trying to reach is actually operating. For example, if a user cannot ping a host, the user will be unable to send files to that host. Ping operates by sending a packet to a designated address and waiting for a response. The basic operation of Ping can be performed by following these steps in any Windows operating system.

1. Click the **Start** button, and then click **Run**.
2. Type “cmd” and press **Enter**.

   The command screen appears. The screen shows a directory (unique to your own PC), and a flashing cursor.
3. At the cursor type the word “ping” followed by a space and the default IP address for the 450U-E at first startup.

   For example if the default IP address is 192.168.0.118, you would type “ping 192.168.0.118”.
4. Press **Enter** to send the ping command.

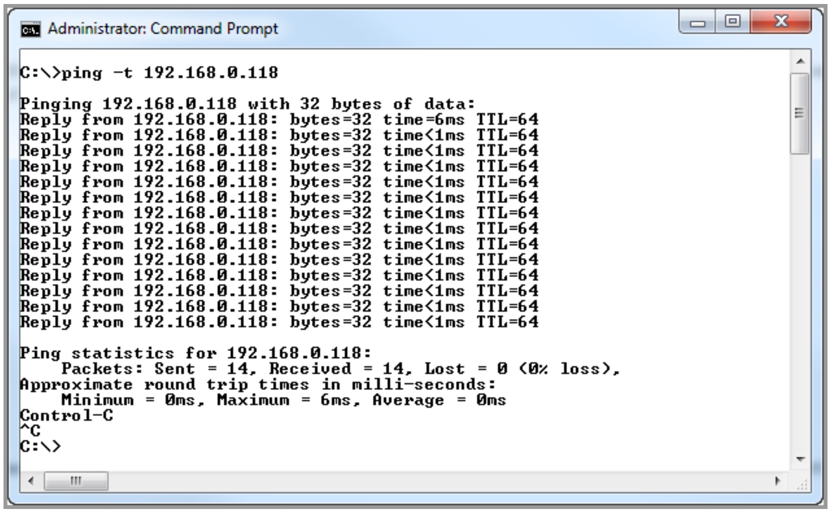
   The PC will reply with an acknowledgment of your command. If the 450U-E is correctly configured, the reply will look something like Figure 90.



```
C:\>ping 192.168.0.118

Pinging 192.168.0.118 with 32 bytes of data:
Reply from 192.168.0.118: bytes=32 time=6ms TTL=64
Reply from 192.168.0.118: bytes=32 time<1ms TTL=64
Reply from 192.168.0.118: bytes=32 time<1ms TTL=64
Reply from 192.168.0.118: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.0.118:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 6ms, Average = 1ms

C:\>
```

Figure 90 Ping

Figure 91 shows the response of the “ping –t 192.168.0.118” command.



```
C:\>ping -t 192.168.0.118

Pinging 192.168.0.118 with 32 bytes of data:
Reply from 192.168.0.118: bytes=32 time=6ms TTL=64
Reply from 192.168.0.118: bytes=32 time<1ms TTL=64
Reply from 192.168.0.118: bytes=32 time<1ms TTL=64
Reply from 192.168.0.118: bytes=32 time<1ms TTL=64
Reply from 192.168.0.118: bytes=32 time<1ms TTL=64
Reply from 192.168.0.118: bytes=32 time<1ms TTL=64
Reply from 192.168.0.118: bytes=32 time<1ms TTL=64
Reply from 192.168.0.118: bytes=32 time<1ms TTL=64
Reply from 192.168.0.118: bytes=32 time<1ms TTL=64
Reply from 192.168.0.118: bytes=32 time<1ms TTL=64
Reply from 192.168.0.118: bytes=32 time<1ms TTL=64
Reply from 192.168.0.118: bytes=32 time<1ms TTL=64
Reply from 192.168.0.118: bytes=32 time<1ms TTL=64
Reply from 192.168.0.118: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.0.118:
    Packets: Sent = 14, Received = 14, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 6ms, Average = 0ms
Control-C
^C
C:\>
```

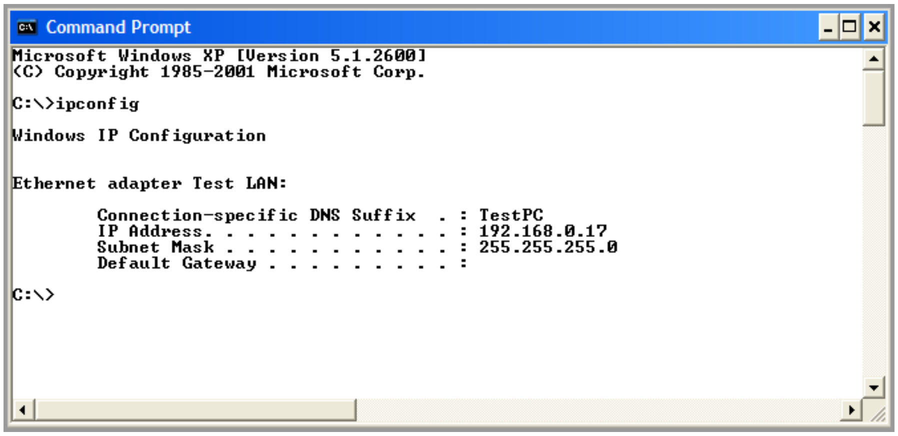
Figure 91 Ping-t

This –t command is used to repeatedly ping the specified node in the network. To cancel, press CTRL+C.

A good test for the network once it is first set up is to use ping repeatedly from one PC’s IP address to the other PC’s IP address. This gives a good indication of the network’s reliability and how responsive it is from point to point. When you enter CTRL+C, the program reports a packet sent-received-lost percentage.

Ipconfig Command

The “ipconfig” command can be used to show your current TCP/IP information, including your address, DNS server addresses, adapter type, and so on.



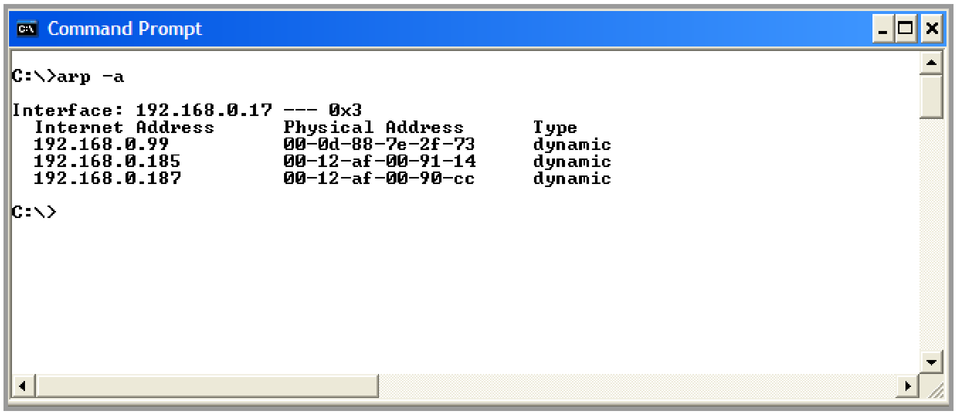
```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\>ipconfig

Windows IP Configuration


Ethernet adapter Test LAN:

        Connection-specific DNS Suffix  . : TestPC
        IP Address. . . . . . . . . . . . : 192.168.0.17
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . :

C:\>
```

Figure 92 Ipconfig

In the example in Figure 92, the ipconfig command was entered at the command prompt. The reply shows the PC’s IP address, subnet mask, and the gateway to which it is connected. Other ipconfig commands will return more information. The hardware or MAC address of the computer may be discovered using the “ipconfig /all” command. The command “Ipconfig /?” lists all of the commands available and their usages.

Arp Command

Displays and modifies the IP-to-physical address translation tables used by Address Resolution Protocol (ARP). Once a remote computer has been pinged, this command can be used to see the IP address and MAC address of the remote computer. It will also show any other devices on the network to which it may be connected.



```
C:\>arp -a

Interface: 192.168.0.17 --- 0x3
  Internet Address      Physical Address      Type
  192.168.0.99          00-0d-88-7e-2f-73     dynamic
  192.168.0.185         00-12-af-00-91-14     dynamic
  192.168.0.187         00-12-af-00-90-cc     dynamic

C:\>
```

Figure 93 Arp Command

The command used in the screen shot above is “arp –a”. It shows the PC’s IP address (like the previous ipconfig command). In this case, the IP address is still 192.168.0.17. It also shows the IP address and associated MAC address of any another device that has a connection to it. The command “arp –?” lists the commands available for this function.

Route Command

The “route” command is used when joining two or more networks together via the 450U-E. For more information about network configurations, see “1.1 Network Topology” on page 7. When routing from one subnet to another, the devices on the first subnet need to know where to pass the message so that it will get to the second subnet. This can be accomplished in two ways:

- Setting up a route within the device, which is a lookup table that lists the subnets and the IP address to use as the gateway.
- Setting up a default gateway address on the modem. This is a link to an IP address that knows how to get to the required subnet. This is a fallback address. If the modem does not know where to send the message, it will sent it to the default gateway.

If there are multiple networks, each with a different IP range, routing rules must be used because the default gateway only allows one address to be configured. In the example in Figure 94, a routing rule needs to be entered into Network A’s PC which will allow access from Network A to Network B.

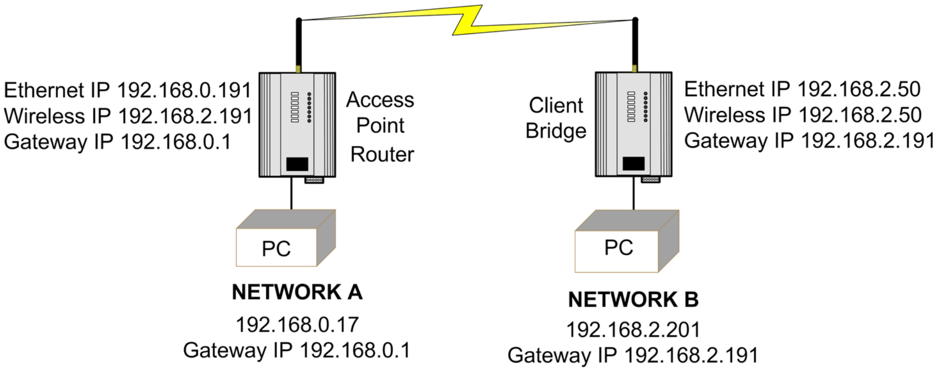


Figure 94 Route

To enter a Routing rule, open a MS-DOS command window and enter the following command at the prompt.

```
Route ADD 192.168.2.0 MASK 255.255.255.0 192.168.0.191
```

This routing rule states that if you want to access any IP address on network B (192.168.2.0) with the netmask of 255.255.255.0, the message needs to be sent to 192.168.0.191. Devices on Network B should also have their default gateway address set to the routers Wireless address (192.168.2.191). This will ensure that any traffic destined for the 192.168.0.0 network can be returned successfully.

There are a number of route commands that can be used to edit, manipulate, and delete routing rules:

- **Route PRINT—**Shows all active routes on PC
- **Route ADD—**Adds a routing table to network, format: Route<IP Address> Mask<Subnet Mask> <Route IP Address>
- **Route DELETE—**Deletes the unwanted routing table, format: Delete <Destination IP >
- **Route CHANGE—**Modifies an existing route, format: Change<IP Address> Mask<Subnet Mask> <Route IP Address>

Chapter 6 - SPECIFICATIONS

Specifications	
Transmitter/Receiver	
Frequency	360–512 MHz (8 x 20 MHz bands)
Transmit Power	Licensed: 5W (+37 dBm) Unlicensed: 0.5W (+27 dBm)
Data Encoding	2-FSK, 4-FSK
Receiver Sensitivity	25 kHz channel: –99 dBm @19,200 baud, –110 dBm @ 9600 baud 12.5 kHz channel: –100 dBm @9600 baud, –111 dBm @ 4800 baud
Channel Bandwidths	25 kHz channel 12.5 kHz channel
Data Rate	25 kHz channel: 4800 baud, 9600 baud 12.5 kHz channel: 9600 baud, 19,200 baud
Range, Line of Site (LoS)	50 km (31 mi) @ 5W 10 km (6 mi) @ 0.5W
Antenna Connector	Female SMA standard polarity
Input/Output	
Discrete Input	Voltage-free contact: Max 30 Vdc Wetting current: 5 mA
Discrete Output [1]	FET: 30 Vdc 500 mA
Analog Input	Current sinking: 4–24 mA +/- 0.2% accuracy, 150-ohm impedance
Ethernet Port	
Ethernet Port	10/100baseT; RJ-45 connector – IEEE 802.3, Auto MDIX
Link Activity	Link, 100baseT via LED
Serial Port	
RS-232	DB-9 female DCE; RTS/CTS/DTR/DCD
RS-485 [2]	2-pin terminal block, non-isolated
Data Rate (Bps)	1200, 2400, 4800, 9600, 14400, 19200, 38400, 57600, 76800, 115200, 230400 Bps
Serial Settings	7/8 data bits; stop/start/parity (configurable)
Protocols/Configuration	
System Address	ESSID; 1–31 character text string
Protocols Supported	TCP/IP, UDP, ARP, SNMP, RADIUS/802.1x, DHCP, DNS, PPP, ICMP, HTTP, FTP, TFTP, TELNET, MODBUS AND MODBUS-TCP
User Configuration	User configurable parameters via HTTPS embedded Web server
Configurable Parameters	Access point/client/bridge/router Point-to-point, point-to-multi-point Wireless distribution system (AP–AP repeater) Modbus TCP/RTU gateway Serial client/server/multicast Simultaneous RS-232/485 connection Embedded Modbus master/slave for I/O transfer
Security	Data encryption: 802.11i with CCMP 128-bit AES Support for 802.1x Radius server Secure HTTP protocol
Bandwidth Protection	MAC address: whitelist/blacklist IP filtering: whitelist/blacklist ARP/GARP filtering: whitelist/blacklist
LED Indicators/Diagnostics	

Specifications	
LED Indicators	Power/OK; RX; TX/Link; RS-232; LAN; RS-485; Analog/Digital I/O status
Reported Diagnostics	RSSI measurements (dBm) Connectivity information/statistics System log file
Network Management	Compatible with Cooper Network Management System
Compliance	
EMC	USA - FCC CFR47 P 90,15; CAN - IC RSS 119; EU - EN301 489-3; AS/NZS - CISPR22
RF (Radio)	USA- FCC CFR47 P 90,15, CAN - IC RSS 119, EU - EN300113-2/ EN300220-2, AS/NZS - AS/NZS4295
Hazardous Area	CSA Class I, Div 2; ATEX IEC Ex zone2
Safety	UL Listed, IEC 60950 (RoHS compliant)
General	
Size	186 x 115 x 36 mm (7.3” x 4.5” x 1.4”)
Housing	IP20 powder-coated aluminum
Mounting	DIN rail
Terminal Blocks	Removable; max conductor 12 AWG (2.5 mm^2)
Temperature Rating	–40 to +70°C –40 to +120°F
Humidity Rating	0–99% RH noncondensing
Weight	0.55 kg (1.2 lb)
Pollution Degree	2—Not sealed, not subject to dust, dirt, condensation
Installation Category	2—Transient voltages are not higher than 2.5 kV at 250 Vac supply
Altitude	0–2000m (6500 ft)
Power Supply	
Nominal Supply	9 to 30 Vdc Under/over voltage protection
Average Current Draw	120 mA @ 13.8V (idle) 70 mA @ 24V (idle)
Transmit Current Draw	1.2–1.5A @ 13.8V (5W) 550–650 mA @ 24V (5W)

NOTE Specifications subject to change.

1) Can be used to transfer I/O status or Communications Failure output

2) Maximum Distance 1200 meters

Appendix A - FIRMWARE UPGRADES

You can check the firmware version that is loaded in the module by viewing the home page of the module’s Web Server. Firmware upgrades should be performed locally with a PC connected directly to the module. Remote firmware upgrades are not recommended over the radio link due to bandwidth limitations.

Full Firmware Upgrade

The 450U-E firmware can be upgraded using a USB flash drive with the firmware files installed. A full USB upgrade is necessary if a patch file is not available or the existing firmware is a much older version and would require multiple patch files to upgrade to the latest version.

The following procedures provides instructions for performing a full USB firmware upgrade on a 450U-E.

Requirements

- USB memory stick
- Firmware files (contact ELPRO Technical Support to obtain these files)
- Ethernet cable
- PC for transferring files

To prepare the USB flash drive

Not all USB flash drives are configured correctly for use as a firmware upgrade drive. Use the following procedure to check the configuration of the USB drive and re-configure the drive if necessary.

1. Plug USB drive into the USB port on the PC and wait until Windows recognizes the drive and completes the driver installation.
2. Open the **Windows Start** menu, choose **Run**, and then enter “CMD” to open a command prompt. Type “diskpart” at the command prompt. This opens the Diskpart utility.

   ```
   C:\>diskpart
   Microsoft DiskPart version 6.1.7601
   Copyright (C) 1999-2008 Microsoft Corporation.
   On computer: TEST_COMPUTER
   ```

3. Type command “list disk” to list available disks, and identify the USB drive based on the size.

   In the following example, the USB drive is a 1911 MB (2 GB) drive, which corresponds to Disk 1.

   ```
   DISKPART> list disk
   Disk ###  Status          Size      Free      Dyn  Gpt
   --------  -------------  -------  -------   ---  ---
   Disk 0     Online          232 GB     0 B
   Disk 1     Online         1911 MB     0 B
   ```

4. When you have identified the USB disk, enter the “select Disk X” command to select this disk.

   Warning: The commands that follow this step can destroy the contents of the selected disk, make sure that you have selected the correct drive before continuing. Selecting the wrong drive could format your PC’s hard drive.

   ```
   DISKPART> select Disk 1
   Disk 1 is now the selected disk.
   ```

5. Enter the command “list partition” to check how the USB drive is partitioned.

   This command indicates whether the drive is correctly configured for use as a firmware upgrade drive on the 450U-E.

- If the drive contains only one partition and the “Offset” value is non-zero, as shown in the example below, you can proceed to format the drive and use it “as is” for firmware upgrade. Skip to step 7 for instructions on how to format the drive using the Diskpart utility.

```
DISKPART> list partition
  Partition ###  Type              Size     Offset
  -------------  ----------------  -------  -------
  Partition 1     Primary           1910 MB    64 KB
```

- If the “Offset” is zero or if there is more than one partition, as shown in the examples below, go to steps 6 and 7 below to re-configure the drive.

```
Partition ###  Type              Size     Offset
  -------------  ----------------  -------  -------
Partition 1     Primary           1911 MB      0 B

Partition ###  Type              Size     Offset
-------------  ----------------  -------  -------
Partition 1     Primary            100 MB    64 KB
Partition 2     Primary           1810 MB   101 MB
```

6. Enter the command “clean” to delete all partitions on the disk, and then enter “list disk” to check that all memory is now free.

   In the example below, the asterisk (*) indicates that Disk 1 is the selected disk.

```
DISKPART> clean
DiskPart succeeded in cleaning the disk.
DISKPART> list disk

  Disk ###  Status         Size     Free     Dyn  Gpt
  --------  -------------  -------  -------  ---  ---
  Disk 0    Online          232 GB      0 B
* Disk 1    Online         1911 MB  1910 MB
```

7. Enter the command “create partition primary” to create a partition on the USB drive. Then, enter the “list partition” command and note that there is only one partition, and that the offset is non-zero.

```
DISKPART> create partition primary
DiskPart succeeded in creating the specified partiti Type    Size     Offset
  -------------  ----------------  -------  -------
* Partition 1    Primary           1910 MB    64 KB
```

8. Finally, the drive can be formatted using the Diskpart command line. The file system format should be selected as FAT32 using the option “fs=fat32”. You can select any convenient label. In the example below the label “FW_UPGRADE” was used.

```
DISKPART> format fs=fat32 label=FW_UPGRADE
100 percent completed
DiskPart successfully formatted the volume.
```

   Alternatively the drive can be formatted from within the Windows GUI environment using the following procedure.

To format the USB flash drive

1. Plug the USB drive into the USB port on the PC.
2. Right-click the USB drive within Windows Explorer, and select **Format** from the menu.

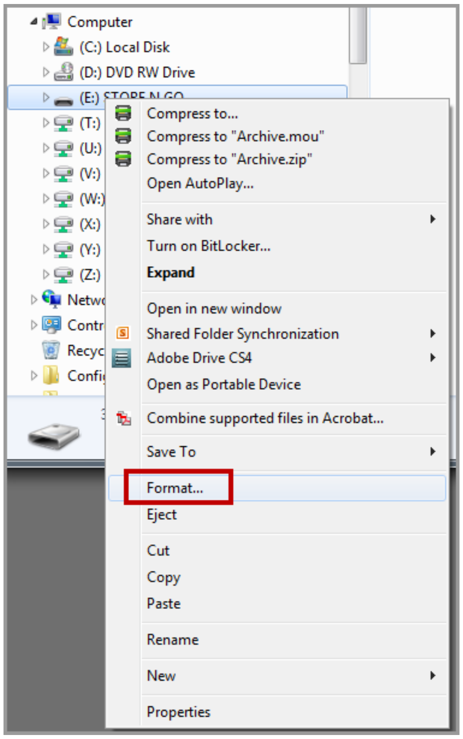
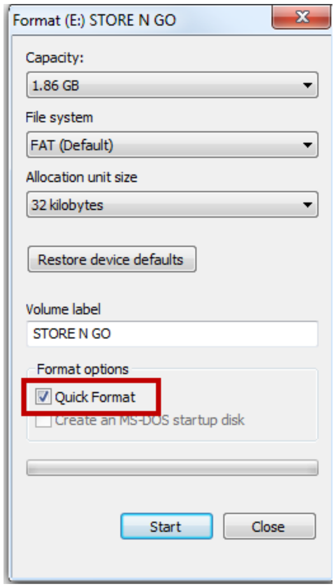


Figure 95 Format USB Drive

3. Make sure that “Quick Format” is not selected, and then click **Start**.


Format (E:) STORE N GO

Capacity: 1.86 GB

File system: FAT (Default)

Allocation unit size: 32 kilobytes

Volume label: STORE N GO

Format options

☑ Quick Format

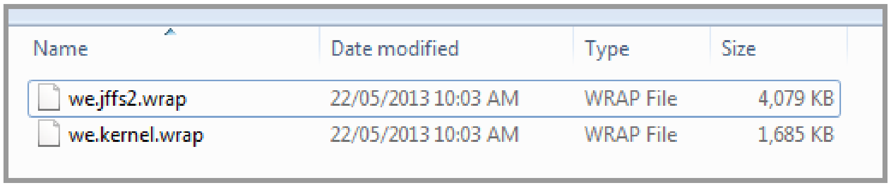
□ Create an MS-DOS startup disk

Figure 96 Quick Format

To perform a full firmware upgrade

1. Copy the supplied firmware files to the root directory on the USB flash drive.

   The files should look similar to Figure 97.



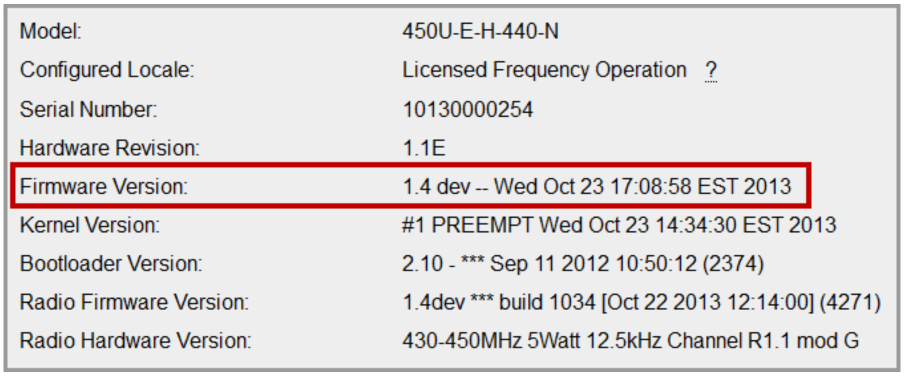
Name	Date modified	Type	Size
we.jffs2.wrap	22/05/2013 10:03 AM	WRAP File	4,079 KB
we.kernel.wrap	22/05/2013 10:03 AM	WRAP File	1,685 KB

Figure 97 Firmware Files

2. Remove the USB drive from the PC.

3. Connect to the module's Web Server and make a note of the current firmware version, which appears on the home webpage.

   This will enable you to compare versions to confirm that the upgrade procedure has been performed successfully.



Model:	450U-E-H-440-N
Configured Locale:	Licensed Frequency Operation ?
Serial Number:	10130000254
Hardware Revision:	1.1E
Firmware Version:	1.4 dev -- Wed Oct 23 17:08:58 EST 2013
Kernel Version:	#1 PREEMPT Wed Oct 23 14:34:30 EST 2013
Bootloader Version:	2.10 - *** Sep 11 2012 10:50:12 (2374)
Radio Firmware Version:	1.4dev *** build 1034 [Oct 22 2013 12:14:00] (4271)
Radio Hardware Version:	430-450MHz 5Watt 12.5kHz Channel R1.1 mod G

Figure 98 Firmware Version

4. Remove the black plastic cover on the front of the Module to reveal a USB port and push button Reset switch.

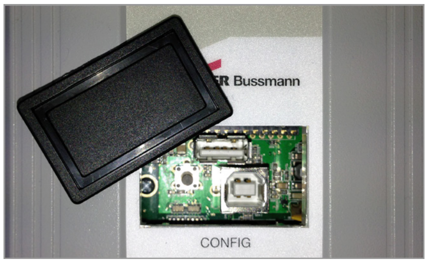


Figure 99 Front Access Panel

5. Plug the USB drive into the USB A port and press the **Reset** button.

   During the upgrade process, the OK LED will flash, as shown in Figure 100. When the OK LED appears solid green, the upgrade is complete.

⚠ **Do not remove the USB drive or interrupt the power to the module while the upgrade is in process. If the upgrade process is interrupted, the module may become unserviceable and need to be returned to ELPRO for repair.**

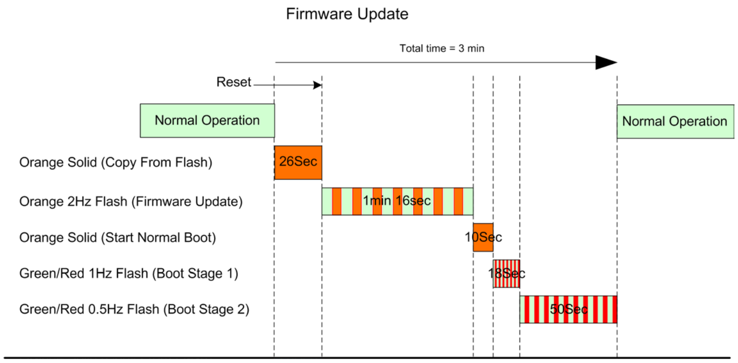

Firmware Update
Total time = 3 min
Reset
Normal Operation
Normal Operation
Orange Solid (Copy From Flash)
26Sec
Orange 2Hz Flash (Firmware Update)
1min 16sec
Orange Solid (Start Normal Boot)
10Sec
Green/Red 1Hz Flash (Boot Stage 1)
18Sec
Green/Red 0.5Hz Flash (Boot Stage 2)
50Sec

Figure 100 Firmware Update LEDs

6. When the upgrade is complete, remove the USB drive from the 450U-E and replace the plastic cover.

   The upgrade process does not change or erase the configuration settings.

7. To verify that the firmware version has been updated and that all other configuration settings are unchanged, navigate to the home page of the Web Server on the 450U-E.

Patch File Firmware Upgrade

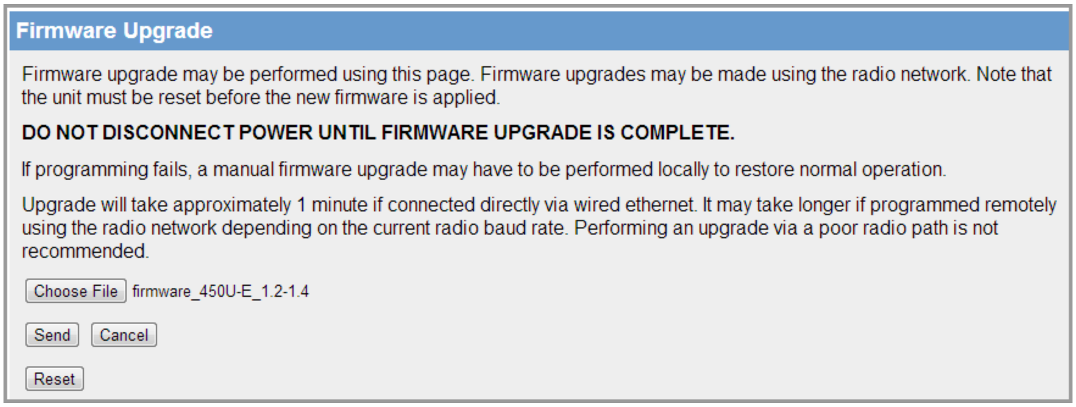
Follow these steps to upgrade the module firmware locally using a firmware patch file. If the device firmware version has fallen multiple versions behind the desired version, it may be necessary to upload multiple patch files.

1. Access the module’s Web Server.

   For instructions, see “4.1 Connecting and Logging On” on page 22.

2. Click **Full Configuration** to display the full configuration menu.

3. Click **System Tools**, and then click **Firmware Upgrade**.



Firmware Upgrade

Firmware upgrade may be performed using this page. Firmware upgrades may be made using the radio network. Note that the unit must be reset before the new firmware is applied.

DO NOT DISCONNECT POWER UNTIL FIRMWARE UPGRADE IS COMPLETE.

If programming fails, a manual firmware upgrade may have to be performed locally to restore normal operation.

Upgrade will take approximately 1 minute if connected directly via wired ethernet. It may take longer if programmed remotely using the radio network depending on the current radio baud rate. Performing an upgrade via a poor radio path is not recommended.

firmware_450U-E_1.2-1.4

Figure 101 Firmware Upgrades

4. Click **Browse** and locate the saved firmware patch file, and then click **Send.**

   File is typically labeled “firmware_450U-E_X.X-X.X” where the Xs indicate the current firmware version and the upgrade version. When you click Send, the file is uploaded to the module and a status message appears.

5. If the upgrade was successful, click **Reset**. If it was not successful, repeat steps 1 through 4.

   The module will verify that the file is valid before a reset can be initiated.

APPENDIX B - USB ETHERNET CONNECTION

Connecting to the Secondary Ethernet Port

To connect to the USB port on the module you will need a standard USB printer cable (USB-A to USB-B), which can be purchased from any electrical store.

1. Download the USB driver file from our Technical Resource Library at www.cooperbussmann.com/wirelessresources.
2. Right-click the USB driver file and select **Install**, and then save the file to the C:\Windows\inf directory.
3. Connect a suitable power source to the modem and wait for it to power up.
4. Open the plastic cover on the front of the module and connect the USB cable to the USB-B socket. Connect the other end of the cable to a free USB socket on the PC.

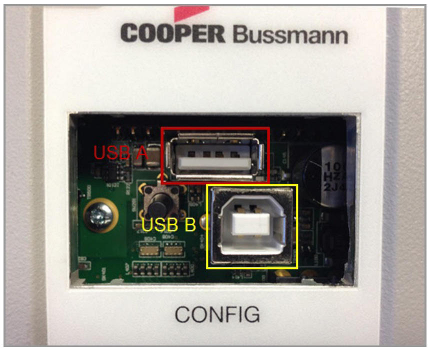
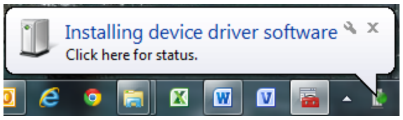


Figure 102 USB Ports

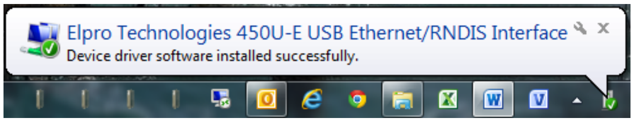
When the cable is connected, Windows detects the new device indicates that it is installing the device driver.


Installing device driver software

Click here for status.

Figure 103 Installing Driver

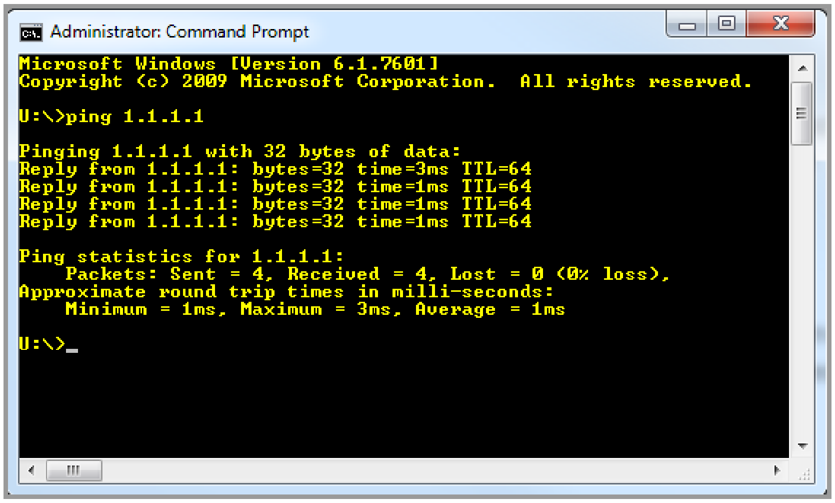
After a short time, a message indicate that the driver is successfully installed.


Elpro Technologies 450U-E USB Ethernet/RNDIS Interface

Device driver software installed successfully.

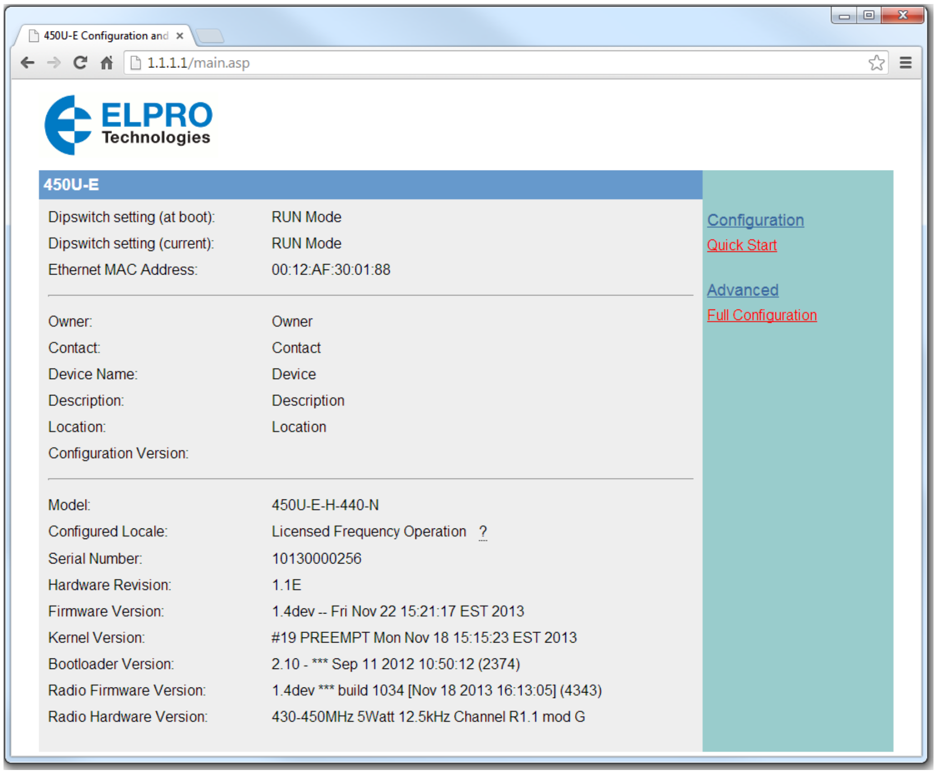
Figure 104 Driver Installed

You should now be able to connect to the 450U-E Ethernet modem via the USB-to-Ethernet connection by opening a command window and pinging the device IP address 1.1.1.1 (Figure 105), or by opening a browser window and connecting to the same IP address (Figure 106).



```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

U:\>ping 1.1.1.1

Pinging 1.1.1.1 with 32 bytes of data:
Reply from 1.1.1.1: bytes=32 time=3ms TTL=64
Reply from 1.1.1.1: bytes=32 time=1ms TTL=64
Reply from 1.1.1.1: bytes=32 time=1ms TTL=64
Reply from 1.1.1.1: bytes=32 time=1ms TTL=64

Ping statistics for 1.1.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 3ms, Average = 1ms

U:\>_
```

Figure 105 Using Ping Command to Connect



450U-E

Dipswitch setting (at boot):	RUN Mode
Dipswitch setting (current):	RUN Mode
Ethernet MAC Address:	00:12:AF:30:01:88
Owner:	Owner
Contact:	Contact
Device Name:	Device
Description:	Description
Location:	Location
Configuration Version:	
Model:	450U-E-H-440-N
Configured Locale:	Licensed Frequency Operation ?
Serial Number:	10130000256
Hardware Revision:	1.1E
Firmware Version:	1.4dev -- Fri Nov 22 15:21:17 EST 2013
Kernel Version:	#19 PREEMPT Mon Nov 18 15:15:23 EST 2013
Bootloader Version:	2.10 - *** Sep 11 2012 10:50:12 (2374)
Radio Firmware Version:	1.4dev *** build 1034 [Nov 18 2013 16:13:05] (4343)
Radio Hardware Version:	430-450MHz 5Watt 12.5kHz Channel R1.1 mod G

Figure 106 Using Web Browser to Connect

Appendix C - GLOSSARY

ACK	Acknowledgment.
Access Point	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.
Antenna Gain	Antennae do not increase the transmission power, but instead focus the signal. Rather than transmitting in every direction (including the sky and ground), antenna focus the signal either more horizontally or in one particular direction. This gain is measured in decibels
Bandwidth	The maximum data transfer speed available to a user through a network.
Bridge	A bridge connects two local area networks, and is typically used to connect wireless networks to wired networks. Bridges usually transfer messages between networks only when the message destination is on the other network. Messages destined for the network on which they originated are not passed on to the other network. This reduces traffic on the entire network.
Collision avoidance	A network node procedure for proactively detecting that it can transmit a signal without risking a collision with transmissions from other network nodes.
Client / Sta / Station	A device on a network that gains access to data, information, and other devices through a server (access point).
Crossover cable	A cable used for networking two computers without the use of a hub. Crossover cables may also be required for connecting a cable or DSL modem to a wireless gateway or access point. The cable is wired so that the signals “crossover,” connecting transmit signal on one side to receiver signals on the other.
DHCP	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. When DHCP is used, whenever a computer logs onto the network an IP address is automatically assigned to it.
DNS	Domain name service (DNS) 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.
Encryption key	An alphanumeric (letters and/or numbers) series that enables data to be encrypted and then decrypted so it can be safely shared among members of a network. WEP uses an encryption key that automatically encrypts outgoing wireless data. On the receiving side, the same encryption key enables the computer to automatically decrypt the information so it can be read. Encryption keys should be kept secret.
Hub	A multiport device used to connect PCs to a network via Ethernet cabling or via 802.11. Wired hubs can have numerous ports and can transmit data at speeds ranging from 10 Mbps to multi-Gigabyte speeds per second. A hub transmits packets it receives to all the connected ports. A small wired hub may only connect four computers; a large hub can connect 48 or more.
Hz	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.
IEEE	Institute of Electrical and Electronics Engineers, New York, www.ieee.org. 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.

I/O	Input/output. The term used to describe any operation, program, or device that transfers data to or from a computer.
IP	Internet Protocol. A set of rules used to send and receive messages across local networks and the Internet.
IP address	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.
IPX-SPX	Internetwork Packet Exchange, is a networking protocol used by the Novell NetWare® operating systems. Like UDP/IP, IPX is a datagram protocol used for connectionless communications. Higher-level protocols, such as Sequenced Packet Exchange (SPX) and NCP, are used for additional error recovery services. SPX is a transport layer protocol (layer 4 of the OSI Model) used in Novell Netware networks. The SPX layer sits on top of the IPX layer (layer 3) and provides connection-oriented services between two nodes on the network. SPX is used primarily by client/server applications.
ISDN	A type of broadband Internet connection that provides digital service from the customer's premises to the dial-up telephone network. ISDN uses standard POTS copper wiring to deliver voice, data, or video.
LAN	Local Area Network (LAN) is 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.
Receive Sensitivity	The minimum signal strength required to pick up a signal. Higher bandwidth connections usually have less receive sensitivity than lower bandwidth connections.
Router	A device that forwards data from one WLAN or wired local area network to another.
Transmit Power	The power at which the wireless devices transmits, usually expressed in mW or dBm.
MAC Address	Media Access Control (MAC) address is a unique code assigned to most forms of networking hardware. The address is permanently assigned to the hardware, so limiting a wireless network's access to hardware (such as wireless cards) is a security feature employed by closed wireless networks. But 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 the 802.11 radios that have had their MAC addresses added to that network's MAC table will be able to get onto the network.
Proxy Server	Used in larger companies and organizations to improve network operations and security, a proxy server is able to prevent direct communication between two or more networks. The proxy server forwards allowable data requests to remote servers and/or responds to data requests directly from stored remote server data.
RJ-45	Standard connectors used in Ethernet networks. RJ-45 connectors are similar to standard RJ-11 telephone connectors, but RJ-45 connectors can have up to eight wires, whereas telephone connectors have four.
Server	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.

Site survey	The process whereby a wireless network installer inspects a location prior to installing a wireless network. Site surveys are used to identify the radio- and client-use properties of a facility so that access points can be optimally placed.
Sub network or Subnet	Found in larger networks, these smaller networks are used to simplify addressing between numerous computers. Subnets connect together through a router.
Switch	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.
TCP	Transmission Control Protocol (TCP) is 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 webpage 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.
TCP/IP	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.
WEP	Wired Equivalent Privacy (WEP) is a basic wireless security provided by Wi-Fi. In some instances, WEP may be all a home or small-business user needs to protect wireless data. WEP is available in 40-bit (also called 64-bit), or in 108-bit (also called 128-bit) encryption modes. As 108-bit encryption provides a longer algorithm that takes longer to decode, it can provide better security than basic 40-bit (64-bit) encryption.
WPA2	Wi-Fi Protected Access II (WPA2) is a security protocol and security certification program developed by the Wi-Fi Alliance to secure wireless computer networks. WPA2-PSK, AES (Advanced Encryption Standard) has replaced WPA and provides significant security improvements over this method. In particular, it introduces CCMP, a new AES-based encryption mode with strong security. WPA2 AES is the most secure encryption method, and is also based on 128-bit encryption key.
Wi-Fi	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.

Appendix D - EXPANSION I/O REGISTERS

Adding 115S Expansion I/O modules to the 450U-E will automatically add the I/O to the internal 450U-E I/O store. To calculate the register location in the I/O store, find the address of the I/O point in the tables in this appendix, and then add the offset. The offset is the Modbus slave address, multiplied by 20.

Examples:

- Digital input #1 on an 115S-11 with address 5 would be: (5x20) +10001 = 10101
- Digital output #2 on an 115S-11 with address 6 would be: (6x20) +2 = 122
- Analog input #3 on an 115S-12 with address 3 would be: (3x20) +30003 = 30063.
- Analog Output #8 on an 115S-13 with address # 7 would be: (7x20) + 40007 = 40147

I/O Store for 115S-11 Expansion I/O Modules

I/O Store	Description
0001–0016 + Offset	DIO outputs 1–16
10001–10016 + Offset	DIO inputs 1–16
10019 + Offset	Modbus Comms Fail indication for this 115S module
10020 + Offset	Modbus Comms Fail indication (inverse) for this 115S module
30001–30004 + Offset	115S-11 pulsed input rate 1– 4
30005–30012 + Offset	115S-11 pulsed input count
30017 + Offset	Modbus Error counter for this 115S module
30018 + Offset	Modbus Last Error code for this 115S module. (See Appendix E for Modbus error codes.)
30019 + Offset	Modbus Lost Link counter for this 115S module
30020 + Offset	Module type (0x0101) = 257 / error status
40009–40016 + Offset	Pulsed output target 1–8 (1 register per pulsed output)

I/O Store for 115S-12 Expansion I/O Modules

I/O Store	Description
0001–0008 + Offset	DIO Outputs 1–8
10001–10008 + Offset	DIO Inputs 1–8
10019 + Offset	Modbus Error indication for 115S module
10020 + Offset	Detected indication for this 115S module
30001–30008 + Offset	Inputs AIN 1–AIN8
30017 + Offset	Modbus Error Counter for this 115S module
30018 + Offset	Modbus Last Error Code for this 115S module. (See Appendix E for Modbus error codes.)
30019 + Offset	Modbus Lost Link Counter for this 115S module
30020 + Offset	Module type (0x0201) = 513 / error status
40009–40016 + Offset	Pulsed Output target 1–8 (1 register per output)

I/O Store for 115S-13 Expansion I/O Modules

I/O Store	Description
0001–0008 + Offset	DIO Outputs 1–8
10001–10008 + Offset	DIO Inputs 1–8
10019 + Offset	Modbus Error indication for 115S module
10020 + Offset	Detected indication for this 115S module

I/O Store	Description
30017 + Offset	Modbus Error counter for this 115S module
30018 + Offset	Modbus Last Error code for this 115S module. (See Appendix E for Modbus error codes.)
30019 + Offset	Modbus Lost Link counter for this 115S module
30020 + Offset	Module type (0x0301) = 769 / error status
40001–40008 + Offset	Analog output 1–8
40009–40016 + Offset	Pulsed output target 1–8 (1 register per pulsed output)

Appendix E - MODBUS EXCEPTION CODES

The following are Modbus exception codes that the Master will generate and write to a general purpose analog register (30501, 40501, and so on) in the event of a poll fail.

Dec Code	Hex Code	Name	Meaning
65281	FF01	Illegal Function	The function code received in the query is not an allowable action for the server (or slave). This may be because the function code is only applicable to newer devices, and was not implemented in the unit selected. It could also indicate that the server (or slave) is in the wrong state to process a request of this type.
65282	FF02	Illegal Data Address	The data address received in the query is not an allowable address for the server (or slave). More specifically, the combination of reference number and transfer length is invalid. For a controller with 100 registers, the PDU addresses the first register as 0, and the last one as 99. If a request is submitted with a starting register address of 96 with a quantity of 4 registers, then this request will successfully operate on registers 96, 97, 98, 99. If a request is submitted with a starting register address of 96 and a quantity of registers of 5, this request will fail with Exception Code 0x02 “Illegal Data Address.”
65283	FF03	Illegal Data Value	A value contained in the query data field is not an allowable value for server (or slave). This indicates a fault in the structure of the remainder of a complex request, such as that the implied length is incorrect. It specifically does not mean that a data item submitted for storage in a register has a value outside the expectation of the application program, since the Modbus protocol is unaware of the significance of any particular value of any particular register.
65384	FF04	Slave Device Failure	An unrecoverable error occurred while the server (or slave) was attempting to perform the requested action.
65285	FF05	Acknowledge	Specialized, use in conjunction with programming commands. The server (or slave) has accepted the request and is processing it, but a significant amount of time will be required to complete this task. This response is returned to prevent a timeout error from occurring in the client (or master).
65286	FF06	Slave Device Busy	Specialized, use in conjunction with programming commands. The server (or slave) is engaged in processing a long–duration program command. The client (or master) should retransmit the message later when the server (or slave) is free.
65288	FF08	Memory Parity Error	Specialized, use in conjunction with function codes 20 and 21 and reference type 6, to indicate that the extended file area failed to pass a consistency check.
65290	FF0A	Gateway Path Unavailable	Specialized, use in conjunction with gateways. Indicates that the gateway was unable to allocate an internal communication path from the input port to the output port for processing the request. Usually means that the gateway is misconfigured or overloaded.
65291	FF0B	Gateway Device Failed to Respond	Specialized, use in conjunction with gateways. Indicates that no response was obtained from the target device. Usually means that the device is not present on the network
65024	FE00	Invalid Response from Slave	Command type or slave address did not match request (the address may belong to another unit).
64512	FC00	Server Offline	Could not connect to Modbus TCP server.
63488	F800	Invalid Local Memory Address	Local address invalid in command. Memory location does not exist or is not initialized.
65535	FFFF	No Response to the Poll	No response to poll message.

Appendix F - POWER CONVERSION

dBm to mW Conversion

Watts	dBm	Watts	dBm
10 mW	10 dB	200 mW	23 dB
13 mW	11 dB	316 mW	25 dB
16 mW	12 dB	398 mW	26 dB
20 mW	13 dB	500 mW	27 dB
25 mW	14 dB	630 mW	28 dB
32 mW	15 dB	800 mW	29 dB
40 mW	16 dB	1.0 W	30 dB
50 mW	17 dB	1.3 W	31 dB
63 mW	18 dB	1.6 W	32 dB
79 mW	19 dB	2.0 W	33 dB
100 mW	20 dB	2.5 W	34 dB
126 mW	21 dB	3.2 W	35 dB
158 mW	22 dB	4.0 W	36 dB

Appendix G - EXTERNAL IPERF TEST

This appendix provides instructions on how to set up and use the Iperf application to test the throughput of Ethernet modems. Iperf is a tool used to measure the throughput and quality of a network link. Jperf is an application that can be used in conjunction with Iperf to graphically display the Iperf data results. The following instructions cover both Iperf and Jperf, but do not cover the setup and configuration of the modems. Modem setup instructions are provided earlier in this manual.

Materials

- 2 x Ethernet modems configured as a bridge
- 2 x PC computers with Ethernet ports and cables
- Suitable power supplies for the Ethernet modems
- Iperf/Jperf application

Installation

1. Downloaded the application from the link http://sourceforge.net/projects/iperf/, and save the application to a location on your PC.
2. Extract the zip file to the root directory on your PC (C:\ directory).

   The extracted folder contains the main Iperf application and the Jperf graphical interface.
3. Copy this folder to the second PC, or download to the second PC and extract, as described in steps 1 and 2.

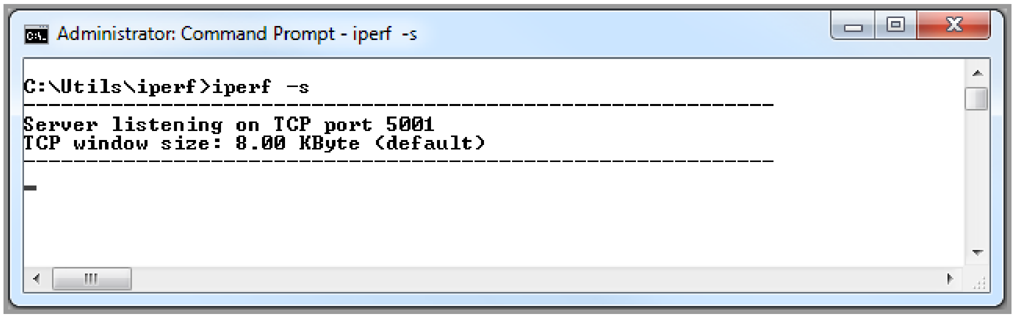
Iperf Applications

The Iperf/Jperf application needs to be run on the PC or laptop at each end of the wireless link that is to be tested.

1. On the server PC, open the **Windows Start** menu, choose **Run**, and then enter “CMD” to open a command prompt.
2. When command prompt appears, set the directory to where the Iperf application is located (where it was saved in the previous procedure).
3. Enter “iperf – s” to run the Iperf server command (Figure 107).

   This will run the Iperf application in server mode, which is configured to respond to any communication frames sent to it from the client.

   NOTE If a security messages appears on the PC, select “Unblock” to allow the application to run.

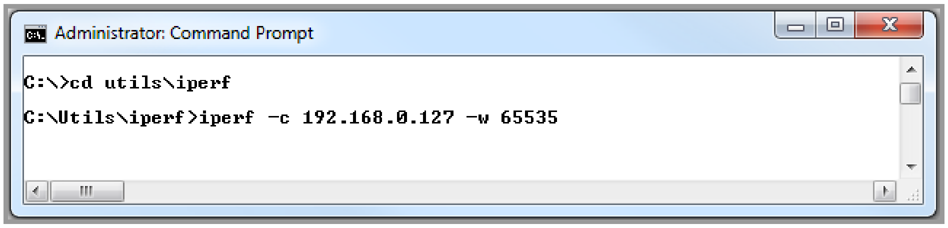


```
C:\Utils\iperf>iperf -s
------------------------------------------------------------
Server listening on TCP port 5001
TCP window size: 8.00 KByte (default)
------------------------------------------------------------
_
```

Figure 107 Iperf Server

4. On the client PC, open up a command prompt window and change to the directory where the Iperf application is located.

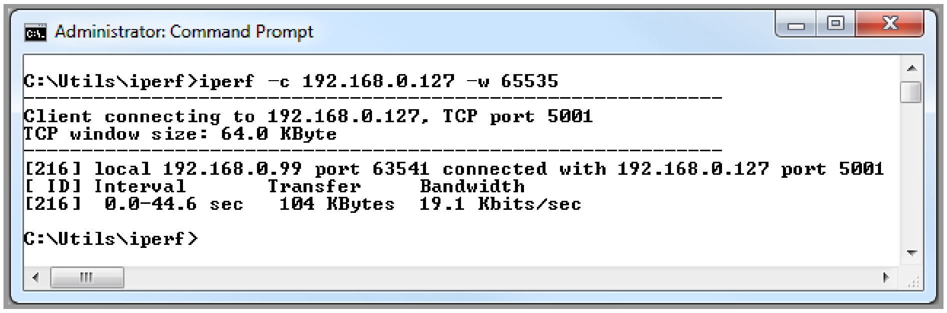
5. Enter the Iperf command “Iperf –c <IP address of Server PC> -w 65535” to start the client communication to the server.



```
C:\>cd utils\iperf

C:\Utils\iperf>iperf -c 192.168.0.127 -w 65535
```

Figure 108 Iperf Client

This command runs a test over the radio link to the server PC and reports back the results, as shown in Figure 109. These results show the bandwidth (throughput) of the test as 19.2 Kbps. We recommend that you run the test several times to get an average.



```
C:\Utils\iperf>iperf -c 192.168.0.127 -w 65535
------------------------------------------------------------
Client connecting to 192.168.0.127, TCP port 5001
TCP window size: 64.0 KByte
------------------------------------------------------------
[216] local 192.168.0.99 port 63541 connected with 192.168.0.127 port 5001
[ ID] Interval       Transfer     Bandwidth
[216]  0.0-44.6 sec   104 KBytes  19.1 Kbits/sec

C:\Utils\iperf>
```

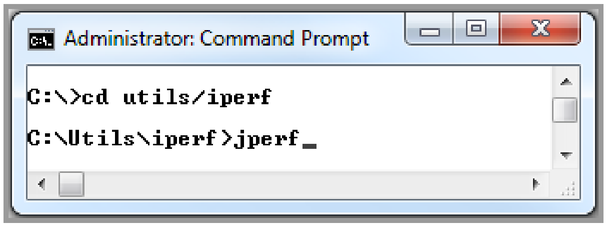
Figure 109 Iperf Results

JPerf Application

Jperf is a graphical interface that runs over the top of Iperf and displays a graph result from the Iperf test.

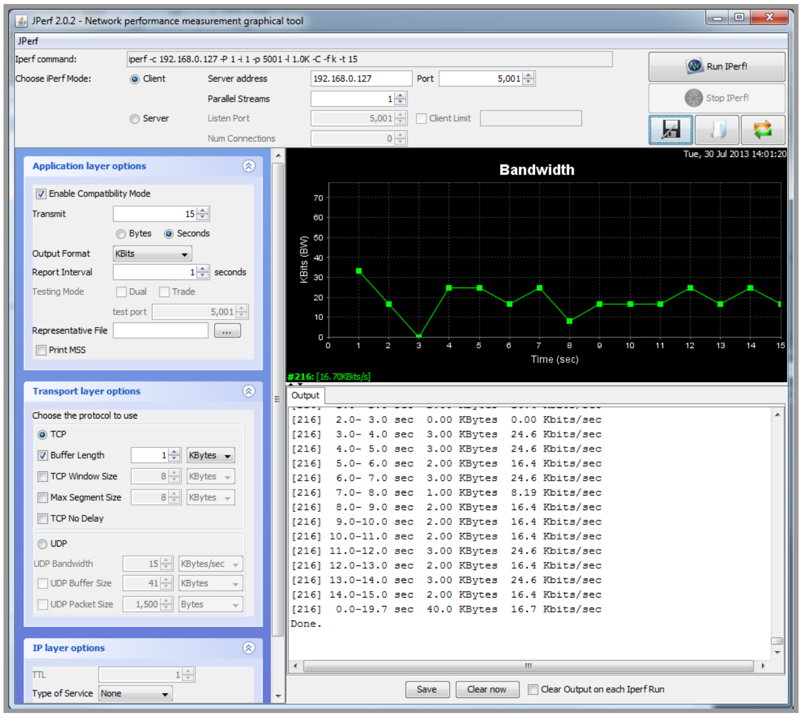
1. Open a command prompt and change to the jperf-2.0.2: directory
2. Run the Jperf application, as shown in Figure 110.

   The command prompt screen is replaced by the Jperf screen shown in Figure 111.



```
C:\>cd utils/iperf

C:\Utils\iperf>jperf_
```

Figure 110 Command Line



JPerf 2.0.2 - Network performance measurement graphical tool

Iperf command: iperf -c 192.168.0.127 -P 1 -i 1 -p 5001 -l 1.0K -C -f k -t 15

Choose iPerf Mode: ● Client ○ Server

Server address: 192.168.0.127
Port: 5,001
Parallel Streams: 1
Listen Port: 5,001
□ Client Limit
Num Connections: 0

Application layer options

☑ Enable Compatibility Mode
Transmit: 15 ○ Bytes ● Seconds
Output Format: KBits
Report Interval: 1 seconds
Testing Mode: □ Dual □ Trade
test port: 5,001
Representative File:
□ Print MSS

Transport layer options

Choose the protocol to use
● TCP
☑ Buffer Length: 1 KBytes
□ TCP Window Size: 8 KBytes
□ Max Segment Size: 8 KBytes
□ TCP No Delay
○ UDP
UDP Bandwidth: 15 KBytes/sec
□ UDP Buffer Size: 41 KBytes
□ UDP Packet Size: 1,500 Bytes

IP layer options

TTL: 1
Type of Service: None

```
[216]  2.0- 3.0 sec  0.00 KBytes  0.00 Kbits/sec
[216]  3.0- 4.0 sec  3.00 KBytes  24.6 Kbits/sec
[216]  4.0- 5.0 sec  3.00 KBytes  24.6 Kbits/sec
[216]  5.0- 6.0 sec  2.00 KBytes  16.4 Kbits/sec
[216]  6.0- 7.0 sec  3.00 KBytes  24.6 Kbits/sec
[216]  7.0- 8.0 sec  1.00 KBytes  8.19 Kbits/sec
[216]  8.0- 9.0 sec  2.00 KBytes  16.4 Kbits/sec
[216]  9.0-10.0 sec  2.00 KBytes  16.4 Kbits/sec
[216] 10.0-11.0 sec  2.00 KBytes  16.4 Kbits/sec
[216] 11.0-12.0 sec  3.00 KBytes  24.6 Kbits/sec
[216] 12.0-13.0 sec  2.00 KBytes  16.4 Kbits/sec
[216] 13.0-14.0 sec  3.00 KBytes  24.6 Kbits/sec
[216] 14.0-15.0 sec  2.00 KBytes  16.4 Kbits/sec
[216]  0.0-19.7 sec  40.0 KBytes  16.7 Kbits/sec
Done.
```

□ Clear Output on each Iperf Run

Figure 111 Jperf Screen

3. When the Jperf screen appears, select “Client” as the Iperf Mode, and enter the IP address of the server PC. Leave the Port field at the default, and click **Run Iperf**.

   The test will run and then display the measured bandwidth (throughput) over time. You can run this test as often as needed to gather a more accurate average.

NOTE Jperf runs using Java technology. Depending on your PC setup, further installation of Java software may be required.

Appendix H - GNU FREE DOCUMENT LICENSE

Version 2, June 1991

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software—to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

Terms and Conditions

This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

   You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

   a. You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

   b. You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

   c. If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

      These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

      Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

      In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

   a. Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

   b. Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

   c. Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for non-commercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

      The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

   If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

   It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

   This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

   Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

NOTES

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
Website: www.cooperbussmann.com/wireless
Australasia Fax: +61 7 33528677
US Fax: +1 925 924 8502

Online Resources

Visit 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

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

China

955 Shengli Road
East Area of Zhangjiang High-Tech Park
Shanghai, 201201, CHINA
Telephone: +86 21 2899 3600
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

www.cooperbussmann.com/wireless

Your Authorized Cooper Bussmann Distributor is:

ELPRO
Technologies

COOPER Bussmann