Read and Retain for Future Reference

Cooper Bussmann

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

Version 1.0.12-Beta7

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, before turning the power on double-check ALL connections by referring to this User Manual.

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.
- 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.

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

FCC Notice:

- Part 15 – This device has been tested and found to comply with the limits for a Class B digital device, pursuant to Part15 of the FCC rules (Code of Federal Regulations 47CFR Part 15). Operation is subject to the condition that this device does not cause harmful interference.
- Part 90 – This device has been type accepted for operation by the FCC in accordance with Part90 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	1dB Gain
ELPRO	UDP400-5	Includes 5m Cellfoil	Unity Gain
ELPRO	BU-3/400	CC10/450	2.5dB Gain
ELPRO	BU-6/400	CC10/450	5.5dB Gain
ELPRO	YU3/400	CC10/450	3.5dB Loss
ELPRO	YU6/400	CC10/450	6.5dB Gain
ELPRO	YU9/400	CC20/450	5dB Gain
ELPRO	YU16/400	CC20/450	10dB Gain

- Part 15 – This device has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC rules (Code of Federal Regulations 47CFR Part 15). Operation is subject to the condition that this device does not cause harmful interference.
- Notice any changes or modifications not expressly approved by ELPRO could void the user’s authority to operate this equipment.

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

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:

1. The Wireless Ethernet module is to be installed by trained personnel / licensed electricians only and installation must be carried out in accordance with the instructions listed in the Installation Guide and applicable local regulatory codes.
2. The units are intended for Restricted Access Locations.
3. The Wireless Ethernet module is intended to be installed in a final enclosure, rated IP54, before use outdoors.
4. The Equipment shall be powered using an external Listed Power Supply with LPS outputs or a Class 2 Power Supply.
5. The Wireless Ethernet module must be properly grounded for surge protection before use.
6. 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 the program 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 F - GNU Free Doc License"

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.

1. 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.
2. 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.
3. 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 earth and the aerial, aerial cable, serial cables and the module should be installed as recommended in the Installation Guide.
4. 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. E.g. "This equipment is remotely controlled and may start without warning. Isolate at the switchboard before attempting adjustments."

5. The 450U-E module is not suitable for use in explosive environments without additional protection.
6. 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 July 2012 release of the 450U-E Ethernet Modem User Manual version 1.0.12-Beta7 which applies to version 1.2Beta 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 provide wireless connections between Ethernet devices and/or Ethernet wired networks (LAN's).

⚠ **450U-E, 5 Watt max power**

The 450U-E is a fixed frequency wireless transceiver that operates in the 380MHz to 520 MHz frequency communications band. There are various frequency bands available depending on the model purchased.

The 450U-E unit provides two serial connections as well as the 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 450U-E has a standard RJ45 Ethernet connection which will operate at up to 100Mbit/sec. The module will transmit the Ethernet messages on the wireless band at rates between 1 and 19.2Kbit/sec depending on model, band, encryption methods, and radio paths.

1.0 Network Topology

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

- "Access Point" or "Client (Station)"
- "Bridge" or "Router".

You can also connect to the 450U-E via a RS232 or RS485 serial port using serial server and allowing the 450U-E to connect the serial communications into the Ethernet network.

Access Point vs. Client

The Access Point unit acts as the "wireless master" unit. The Access Point accepts and authorises links initiated by the client units, and controls the wireless communications.

Clients (Stations) are slave units and when connected to the Access Point becomes transparent Ethernet links.

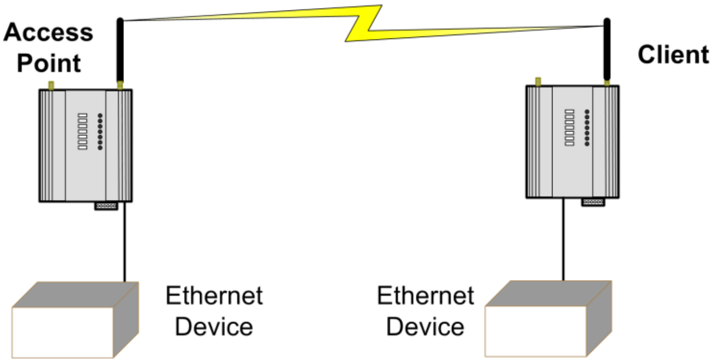


Figure 1 – AP-Client

The first diagram 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.

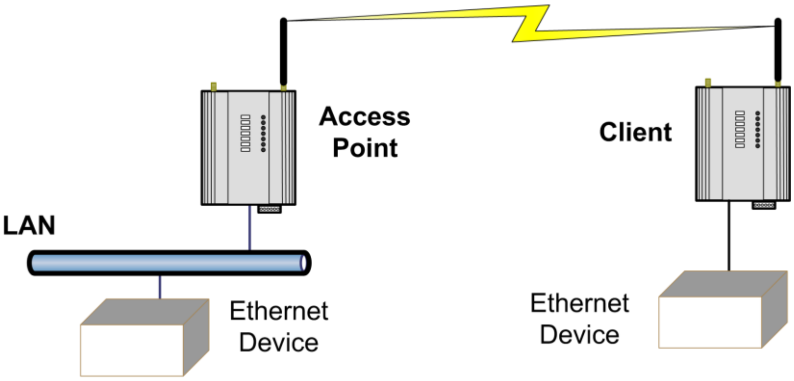


Figure 2 – AP-Client2

The second diagram shows an existing LAN being extended using 450U-E's. 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.

An Access Point can connect to multiple Clients. In this case, the Access Point should be the "central" unit.

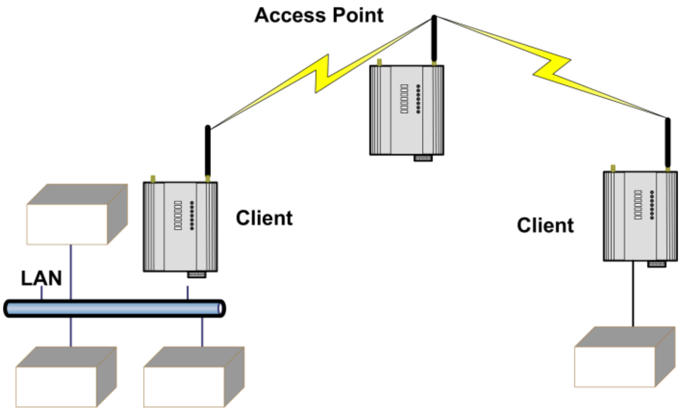


Figure 3 – Multi Client

An Access Point could be used as a "Repeater" unit to connect two 450U-E Clients, which do not have direct reliable radio paths. There is no "Special" repeater module, any 450U-E can be a repeater and at the same time, can be connected to an Ethernet devices or on a LAN

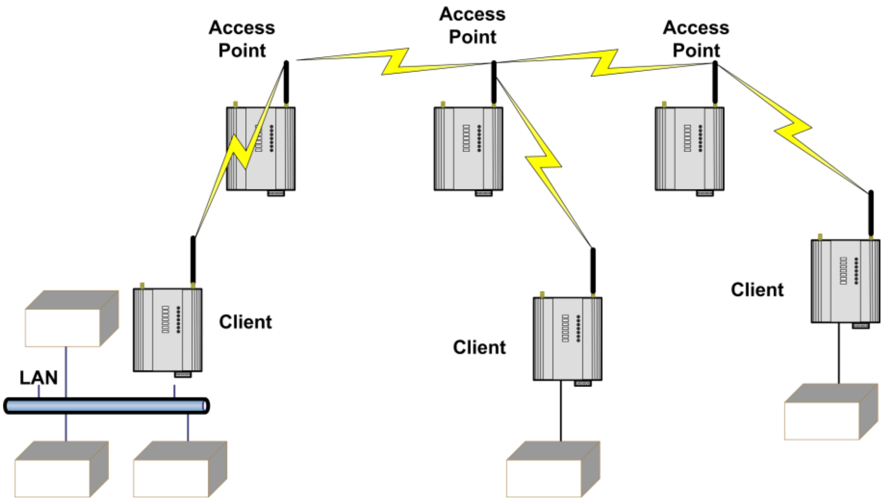


Figure 4 – Multi AP

Multiple Access Points can be set-up in a "mesh" network to provide multiple repeaters.

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.

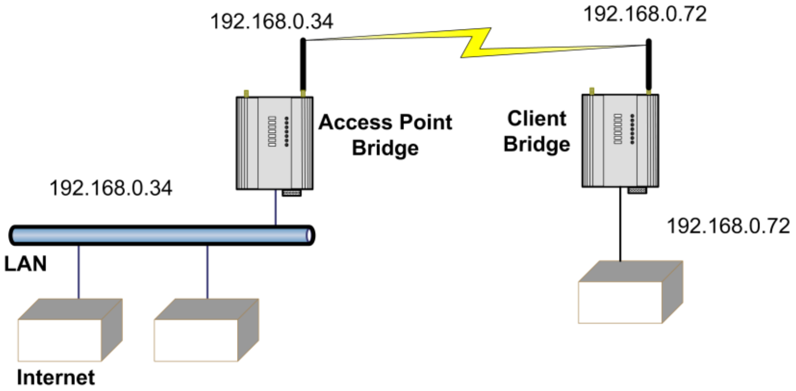


Figure 5 - Bridge

A Router connects devices on different LAN's. 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.

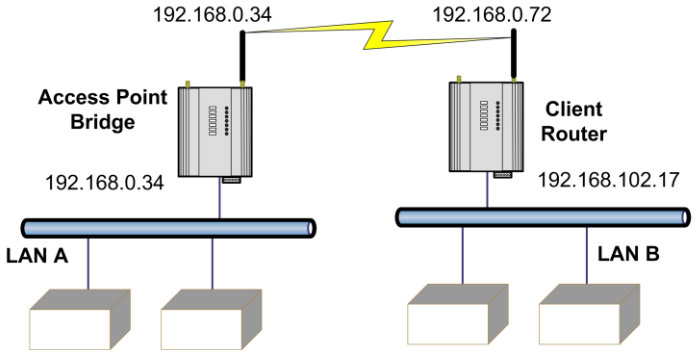


Figure 6 - Client Router

Alternately, the Access Point could be configured as a Router. The wireless link is then part of LAN B.

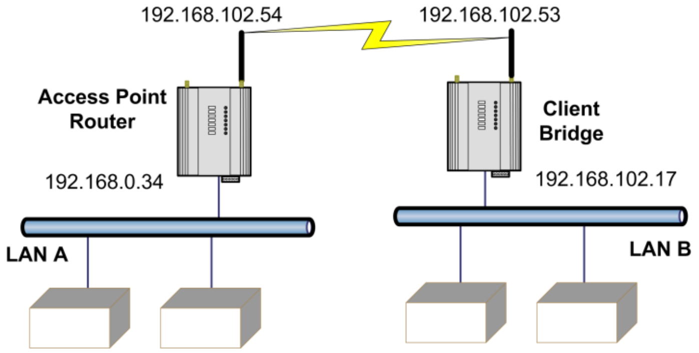


Figure 7 – AP Router

If more than two routers are required within the same radio network, then routing rules may need to be configured (refer to section 3.13 "IP Routing "for more details). There is no limit to the number of Bridges in the same network - although there is a limit of 128 Client units linked to any one Access Point.

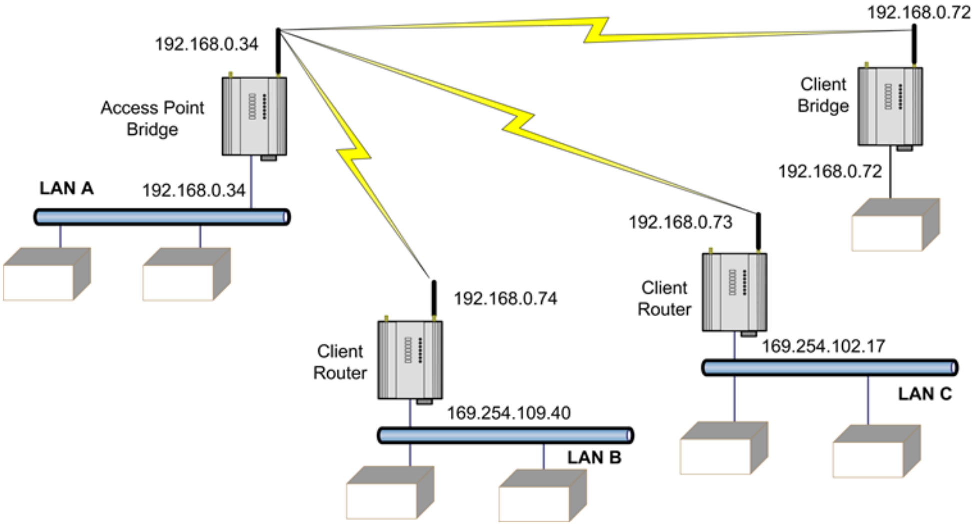


Figure 8 - Multi Router

1.1 Getting Started Quickly

This instruction will explain what sections of the manual should be read to get the modems configured quickly and easily. The out of the box basic configuration should cover most applications and require little configuration, however if more advanced applications are required the 450U-E's have many sophisticated features, which can be adjusted if need be.

- First, read Chapter 2, "Installation". This will explain the connections that are required for successful operation, i.e. Power, Antenna, Serial, Ethernet and I/O.
- Power the 450U-E and make an Ethernet connection to your PC (for further information on how to do this, refer to section 3.2 'Initial Connection'
- Set the 450U-E address, and other necessary configuration parameters by using the Quick Start as per section 3.4 'Quickstart'
- Save the configuration - the 450U-E is now ready to use.
- **If the modems are connected to an existing network read section 3.14 "Filtering" some form of filtering (MAC, IP and ARP) will reduce the amount of Ethernet network traffic being sent over the radio network.**

Before installing the 450U-E, bench test the system. It is a lot easier to locate problems with all the equipment located on the bench.

CHAPTER 2 - INSTALLATION

2.0 General

The 450U-E modules are housed in a rugged aluminium case, suitable for DIN-rail mounting. Terminals will accept wires up to 2.5 mm^2 (12 gauge) in size.

⚠ **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. Refer to Section 2.2 "Power Supply".**

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 the radio path being inadequate. If the radio path is a problem (i.e. path too long, or obstructed), a higher performance antenna or a higher mounting point for the antenna may rectify the problem. Alternately, use an intermediate 450U-E module as a repeater.

The 450U-E Installation Guide provides an installation drawing appropriate to most applications. Further information is detailed below.

Each 450U-E module should be effectively earthed via the "GND" screw on the back of the module - this is to ensure that the surge protection circuits inside are effective.

2.1 Antenna Installation

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

⚠ **A 450U-E can achieve 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 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 which are close to either antenna will have more of a blocking affect than obstructions in the middle of the radio path.

The 450U-E modules provide a diagnostic feature which displays the radio signal strength of transmissions (refer Chapter 4 "Diagnostics").

Line-of-sight paths are only necessary to obtain the maximum range. Obstructions will reduce the range, or degrade a reliable path. A larger amount of obstruction can be tolerated for shorter distances however an obstructed path requires testing to determine if the path will be reliable - refer to section CHAPTER 4 - of this manual for more information on determining a reliable path.

Where it is not possible to achieve reliable communications between two 450U-E modules, then a third 450U-E module may be used to receive the message and re-transmit it. This module is referred to as a repeater. This 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/demo or a 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' web page.
- If using Demo antennas on each end, fit 20dB 5W coax attenuator in-line with the coax 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 the level is not greater than -45dB

Antennas

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

The net gain of an antenna/cable configuration is the gain of the antenna (in dBi) less the loss in the coaxial cable (in dB). The 450U-E maximum net gain 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 30 m / 100 ft)**
RG58 Cellfoil Cable kits (3m,10m, 20m)	-1dB, -2.5dB, -4.8 dB
RG213 - per 10m (33ft)	-1.8 dB
LDF4-50 – per 10m (33ft)	-0.5 dB

The net gain of the antenna/cable configuration is determined by adding the antenna gain and the cable loss.

For example, an 8dBi antenna with 10 meters of Cellfoil (-2.5dB) has a net gain of 5.5dB (8dB – 2.5dB).

Installation tips

Connections between the antenna and 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, as it greatly increases the radio losses. We recommend that the connection be taped, firstly with a layer of PVC Tape, then 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 trouble shooting as the vulcanizing seal can be easily removed.

Where antennas are mounted on elevated masts, the masts should be effectively earthed 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 then 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 earthed structure, a lightning rod may be installed above the antenna to provide shielding.

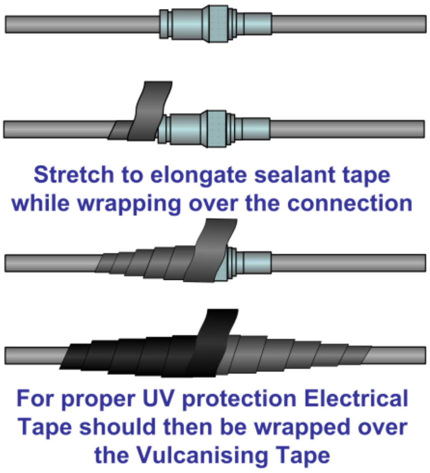

Stretch to elongate sealant tape while wrapping over the connection
For proper UV protection Electrical Tape should then be wrapped over the Vulcanising Tape

Figure 9 - Vulcanizing Tape

Dipole and Collinear antennas

A dipole or collinear antenna transmits the same amount of radio power in all directions - as such that are easy to install and use. 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.

Collinear and dipole antennas should be mounted vertically, preferably 1 wavelength away (see Figure 10 for distances) from a wall or mast and at least 3ft (1m) from the radio module to obtain maximum range.

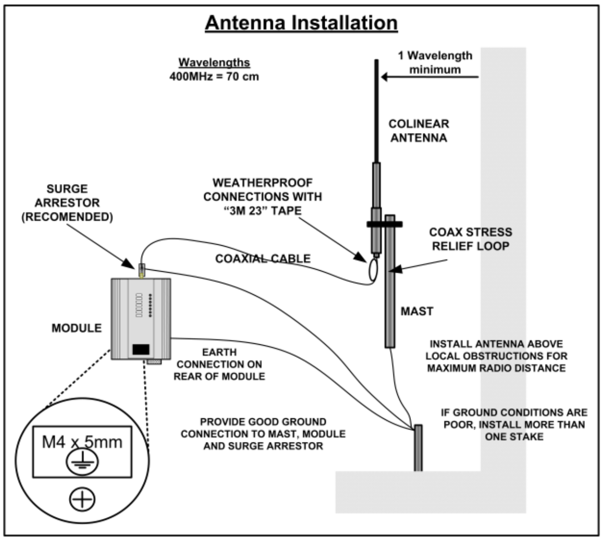

Antenna Installation
Wavelengths
400MHz = 70 cm
1 Wavelength minimum
COLINEAR ANTENNA
SURGE ARRESTOR (RECOMENDED)
WEATHERPROOF CONNECTIONS WITH "3M 23" TAPE
COAX STRESS RELIEF LOOP
COAXIAL CABLE
MODULE
MAST
EARTH CONNECTION ON REAR OF MODULE
INSTALL ANTENNA ABOVE LOCAL OBSTRUCTIONS FOR MAXIMUM RADIO 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 10 – Collinear/Dipole Antenna

Directional antennas.

Directional antennas can be

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

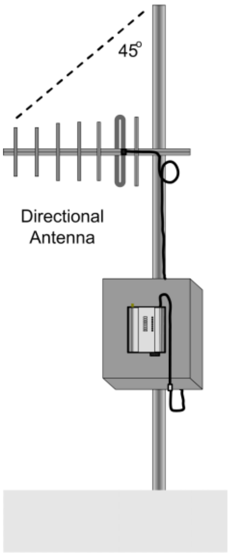


Figure 11 – Dipole Antenna

A directional antenna provides high gain in the forward direction, but lower gain in other directions. This may be used to compensate for coaxial cable loss for installations with marginal radio path.

Yagi antennas should be installed with the main beam horizontal, pointing in the forward direction. If the Yagi is transmitting to a vertically mounted omni-directional antenna, then the Yagi elements should be vertical. If the Yagi is transmitting to another Yagi, then the elements at each end of the wireless link need to 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 as per 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/earth".

2.2 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 earth. The supply negative is connected to the unit case internally. The DC supply may be a floating supply or negatively grounded.

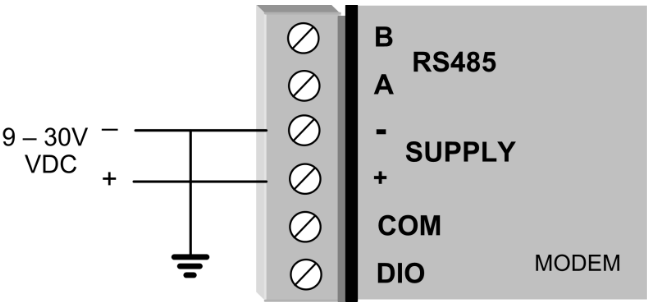


Figure 12 - Power Supply

	13.8VDC	24VDC
Quiescent	120mA	70mA
TX @500mW	400mA	220mA
TX @ 5W	1.2 - 1.5Amps	550mA - 650mA

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)

2.3 Serial Connections

RS232 Serial Port

The RS232 serial port on the 450U-E is a 9 pin DB9 female connector which provides connection for host devices as well as providing a connection point for diagnostics, field testing and factory testing. Communication is via standard RS232 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 local unit's input buffer. The

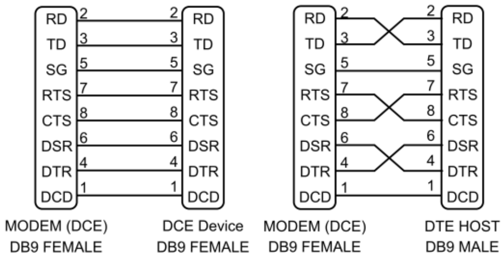


Figure 13 - Serial Cable

Example cable drawings for connecting to a DTE host (PC) or another DCE device (modem) are detailed in Figure 13 - Serial Cable. A General rule of thumb for determining if the device is DCE or DTE is to look at the DB9 Connector and if it's a Female the device is DCE and if its Male its DTE. Also if the device plugs into a computer with a standard straight through cable and works the device is a DCE.

DB9 Connector Pin outs

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

RS485 Serial Port

The RS485 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 in each multi-drop network.

As the RS485 communication medium is shared, only one of the units on the RS485 cable may send data at any one time. Thus, communication protocols based on the RS-485 standard require some type of arbitration.

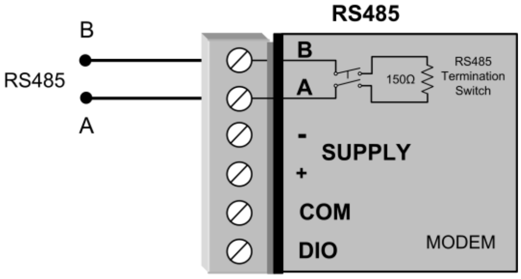


Figure 14 - RS485

RS485 is a multi-drop communication link or bus that can span relatively large distances (up to 1.2Km (4000ft)) using a balanced differential paired cable. It is recommended that the cable be shielded, twisted pair to reduce potential RF Interference.

An RS485 network should be wired as indicated in the diagram below and terminated at each end of the network with a 120-ohm resistor. An on-board 120-ohm resistor is provided in the modem which can be engaged by operating the single DIP switch on the end plate next to the RS485 terminals. The DIP switch should be in the "1" or "on" position to connect the resistor. If the RS485 device that the modem is being connected to does not have a termination switch a 120ohm resistor must be fitted manually across the RS485 terminals. Only devices at each end of the multi-drop RS485 cable will need to have a termination resistor enabled or fitted.

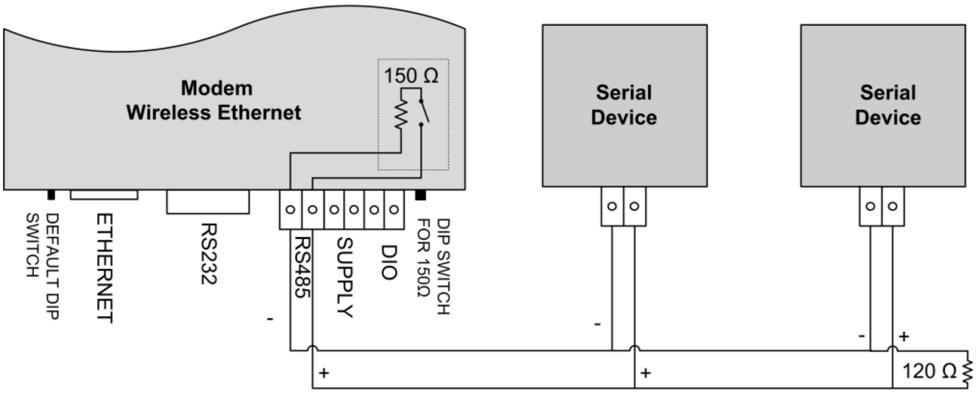


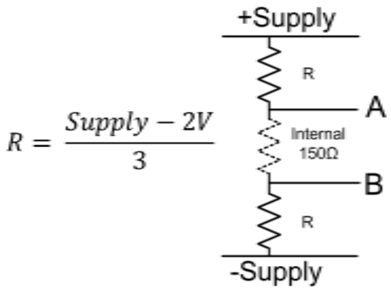
Figure 15 -Multidrop Serial

Failsafe Biasing

The 450U-E does not support Failsafe Biasing on the RS485 unless a 115S serial expansion module is also connected and has its termination switch enabled.

Failsafe Biasing is a simple voltage divider that is connected to the RS485 bus and pulls the terminal voltages (high or low) when the communication state is idle rather than be left at a floating state which could cause data corruption.

If connecting a serial device that does not support Failsafe Biasing and an 115S expansion I/O module is also not fitted then Biasing resistors must be wired to each RS485 terminal to ensure correct operation. Resistor values will depend on the Supply voltage; see diagram for resistor value calculation and wiring.



USB Ports

Module has a two USB ports housed under the plastic bung on the top plate.

- USB A Host port is used for upgrading the module firmware and can only be used for full upgrades. Patches files are not loaded via the USB but through the web interface. The procedures for performing a full firmware upgrade and the patch file upgrade can be found in Section Appendix A - Firmware Upgrades

- USB B Device connector which is used as a secondary Ethernet connection point. Essentially this is a USB to Ethernet converter that will allow you to connect to the modules web interface without the need for disconnecting the existing Ethernet connection or the need to install a hub or switch to allow more ports.

2.4 Input/Output Connections

The 450U-E has a single physical on-board I/O channel that can be configured as either a Digital or an Analog via the web interface. The Digital channel can act as an input or an output. It can be monitored, set remotely, or alternatively used an output for a communications alarm status. If more I/O is required, you can add 115S serial expansion I/O modules via the RS232 or RS485 ports. See section 3.16 for more details on this.

Analog Input

The I/O channel can be configured to except a 0-20mA current sinking analog input.

Current source must be externally powered and the DIO must be configured for Analog Input rather than Digital Input/Output. This can be configured by going to the 'I/O Configuration' / 'External I/O Mode Configuration' screens see section 3.16 for details.

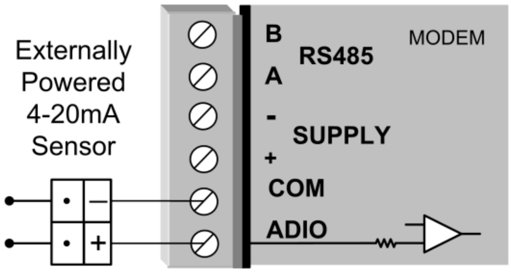


Figure 16 - Analog Input

Digital Output

The I/O channel can also be used as a discrete output. The digital output uses a FET transistor rated at 30VDC 500 mA, and can be used to switch a load, i.e. relay coil or contactor.

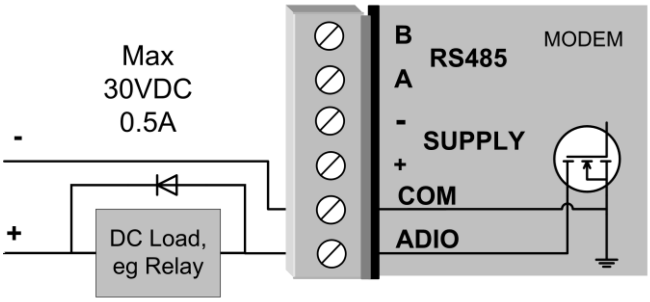


Figure 17 - DIO Output

⚠ **The output can be activated by manually writing a value of** ‘1’ to register location 1 using the ‘I/O Diagnostics’ menu or **by utilising the onboard Modbus TCP Server or Serial Modbus Master to turn on the output. It could also be accessed from an external Modbus Server, i.e. a PLC, DCS, Scada, etc. via the Ethernet network or Serial interface.**

⚠ **When activating the output the I/O indication on the front panel of the module will be lit RED when the output is on.**

⚠ **Note: The Digital Output will override the Digital Input operation, i.e. if the output is activated while the DIO is being read the indication will show the input as being on (1).**

Digital Input

When used as an “input”, the I/O channel supports voltage free contact connection such as a mechanical switch or a NPN transistor device such as an electronic proximity switches.

Contact wetting current of the input is approximately 5mA and is provided to maintain reliable operation for driving relays.

The digital input is activated by connecting between the "DIO" and “COM" terminals.

⚠ **When activating the input the I/O indication on the front panel of the module will be lit GREEN when the input is switched on (closed/shorted). Provided the resistance of the switching device is less than 200 ohms, the device will be able to activate the digital input.**

⚠ **PNP transistor devices are not suitable.**

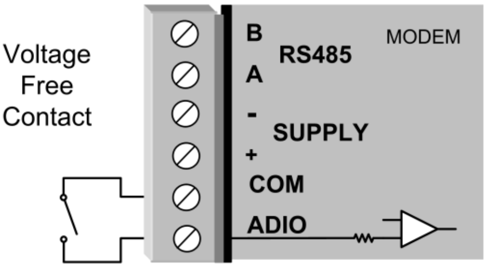


Figure 19- DIO Input (Switch)

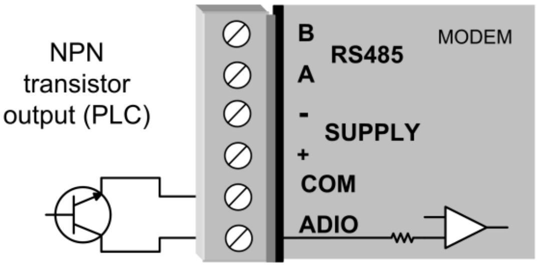


Figure 18 - Digital Input (Transistor)

CHAPTER 3 - OPERATION

3.0 Start-up

"Access Point" Start-up

Normal module startup time is approximately 1 minute and 20 Seconds from when first powered on to where you can connect to the IP address. When the Access Point (AP) has completed its startup process it will immediately begin broadcasting periodic messages, called 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 if 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 SSID. Access Points do not initiate link establishment.

"Client" Start-up

Normal module startup time is approximately 1 minute and 20 Seconds from when first powered on to where you can connect to the IP address. When a Client completes its startup process it will begin scanning its configured frequency for a suitable Access Point. The Client will attempt to establish a link with an Access Point only if it has matching SSID, Encryption method and the correct password. If more than one suitable Access Point is discovered, the client will attempt 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 if their configurations permit them to establish a link. Once the Client has been authenticated, it will then request an Association to establish a link.

Status of the wireless link is indicated via the TX/LINK LED. For an Access Point, the TX/LINK LED will be OFF while no links have been established. Once one or more links have been established, the TX/LINK LED is on GREEN. For a Client, the Link LED will reflect the connection status to an Access Point. Link status is also displayed on the "Connectivity" page of the web interface.

After the link is established, data may be transferred in both directions. The Access Point will act as a master-unit and will control the flow of data to the Clients linked to it. Clients can only transmit data to the AP to which they are connected. When a Client transfers data to another Client, it first transmits the data to the AP, which then forwards the data to the destined Client.

⚠ Presence of a "link" does not mean that the connected unit is authorized to communicate over radio. **If the encryption keys are incorrect between units in the same system, or a dissimilar encryption scheme is configured, the LINK led will light, however data cannot be passed over the wireless network.**

A maximum of 127 Clients may be linked to an Access Point.

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 will wait 7 beacon times (7 x 15 seconds) and then send a link check message and if it 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 5 minutes before dropping the link and clearing the connectivity list.

Roaming Clients

Clients can roam within a system however there are some limitations due to the link timeouts. If when connected to an Access Point the link fails because of a hardware problem or the signal level falls below the minimum threshold (-99dB, 25KHz channel @19200 baud or -100dBm @ 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, etc. The timeframe for the changeover will be approximately 105 seconds due to the link retires and timeouts.

LED Indication

The following table details the status of the indicating LEDs on the front panel for all operating conditions.

LED Indicator	Condition	Meaning
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.
IO	GREEN different intensity	Analog input current loop. dim = 4mA, bright= 20mA

The Ethernet RJ45 connector on the end of the module incorporates two indication LEDs. The LINK LED which comes on to indicate a connection on the Ethernet port, and it will blink OFF briefly when activity is detected, similar to the LAN Led on the front panel. The 100MB LED indicates that the LAN connection is at 100 MBit/Sec. The 100MB LED will be off for 10MB/Sec connection.

Other conditions indicating a fault are described in CHAPTER 4 - DIAGNOSTICS.

3.1 Radio Operating Parameters

Frequency Bands

The radios will operate within the range 360-512MHz; however the full range is broken into different frequency bands and the radios will be set to one of these frequency bands. Care must be taken when ordering to select the correct band as the frequency cannot be configured outside of its band.

The Frequency of the radio is configurable by the user within a Frequency band of the radio; the following bands are available.

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

The modems are capable of being configured in the frequency range of 380MHz – 512MHz however the modems are factory tuned for a particular 20MHz frequency band as shown above.

⚠ **Note: Modems must be ordered to operate in the chosen band; modems cannot be tuned to a frequency that is outside of this band.**

Transmit and Receive frequencies are configured by typing the frequency into the available TX and RX Frequency field. Frequency must be multiples of the step size and will automatically adjust itself to the correct format when you click out of the input box.

Receiver

The Radio Receive Sensitivity will vary depending on the radio channel width, whether it is a wide band radio using 25 KHz channels or if it a narrow band radio using 12.5 KHz channel. The transmit data rate will also vary the receiver sensitivity. Refer to the table below for Receiver Sensitivity

Receiver Sensitivity	Baud Rate		
Bandwidth	**4.8kbits**	**9.6kbits**	**19.2kbits**
25KHz Channel	N/A	-110 dBm	-99 dBm
12.5 KHz Channels	-111 dBm	-100 dBm	N/A

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, i.e. little to no outside radio interference present while data is being passed and they 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. The recommended method of measuring throughput is to use an external Modbus Client to poll the internal Modbus Server on the remote modem. It is recommended that the throughput test be performed on point to point links while the remainder of the wireless network is inactive (i.e. not sending any data).

Modbus TCP.

Below is a table showing the maximum number of polls per minute (ppm) based on the radio receiver signal level.

Results show two different test polls using two different data speeds and with and without Data Compression. For more details on what data compression is and how to implement it, read section 3.10 "Data Compression".

The test is designed to simulate a Modbus TCP Client polling a Modbus TCP server through the radio modems utilising the two different data rates (2 Level FSK and 4 Level FSK) and scanning a different number of I/O points.

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. TCP Client scan rate was 5msec, poll delay was 5msec and the Slave response time was 10seconds.

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 without compression	55 Ppm	90 Ppm
20 Words @ maximum Scan rate with Compression	58 Ppm	87 Ppm
120 Words @ maximum Scan rate without compression	39 Ppm	69 Ppm
120 Words @ maximum Scan rate with Compression	55 Ppm	87 Ppm

3.2 Initial Connection

The 450U-E has a built-in web server, for configuration and diagnostics. The preferred web browser is Microsoft® Internet Explorer version 7 or greater. This program is shipped with Microsoft Windows or may be obtained freely via the Microsoft® website or Google Chrome which is also downloadable from the web. Other browsers may not be fully compatible on all Beta web pages.

⚠ **Note: Microsoft Internet Explorer Version 6 will not load web pages due to a compatibility issue between IE6 and SSL-security web sites.**

Default Configuration

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

⚠ **Do not forget to set the switch back to the RUN position and cycle power at the conclusion of configuration for resumption of normal operation.**

The default factory configuration of the 450U-E is

- Client / Bridge
- IP address192.168.0.1XX, 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 is “user” and the default password is “user”

Accessing Configuration for the first time

Because the Default IP address is in the range 192.168.0.XXX it may not connect to you network or PC so there are two methods for accessing the configuration for the first time.

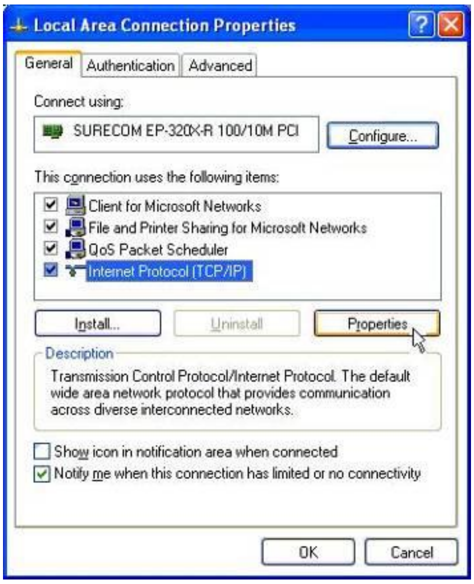
Method 1 - Change your computer settings so that the configuring PC is on the same network as the 450U-E with factory default settings. **This is the preferred method** and is much less complicated than the second method. You will need a “straight-through” Ethernet cable between the PC Ethernet port and the 450U-E. The factory default Ethernet address for the 450U-E is 192.168.0.1XX where XX are the last two digits of the serial number (check the label on the back of the module).

Method 2 - Requires temporarily changing the IP address in the 450U-E via an RS232 connection such that it is accessible on your network without having to change your PC network settings. When connected you be able to change the modem network settings to match that of your network.

Method 1 - Set PC to same network as 450U-E

Connect the Ethernet cable between unit and the PC configuring the module.

- Set the Factory Default Switch to the SETUP position. This will always start the 450U-E with Ethernet IP address 192.168.0.1XX, subnet mask 255.255.255.0, gateway IP 192.168.0.1 and the radio disabled. Do not forget to set the switch back to the RUN position and restart the module at the conclusion of configuration for resumption of normal operation.
- Power up the 450U-E module.
- Open "Network Settings" on your PC under Control Panel. The following description is for Windows XP - earlier Windows operating systems have similar settings.
- Open "Properties" of Local Area Connection.
- Select Internet Protocol (TCP/IP) and click on Properties.
- On the General tab enter IP address 192.168.0.1, Subnet mask 255.255.255.0 and press "OK"
- Open Internet Explorer and ensure that settings will allow you to connect to the IP address selected. 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.
- Enter the default IP address for the 450U-E 192.168.0.1XX where XX is the last two digits of the serial number.
- Enter the username "user" and default password "user".



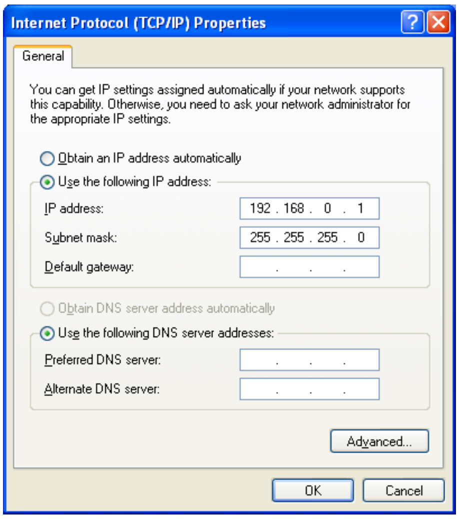
Connect using:
SURECOM EP-320X-R 100/10M PCI

This connection uses the following items:
☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ QoS Packet Scheduler
☑ Internet Protocol (TCP/IP)

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

☐ Show icon in notification area when connected
☑ Notify me when this connection has limited or no connectivity

Figure 20 - Local Area Connection

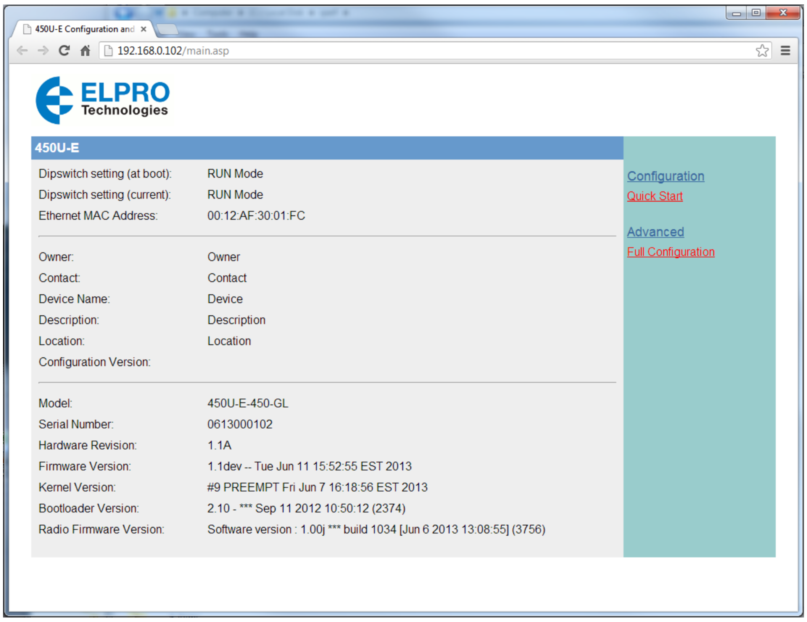


You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ 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: . . .

Figure 21 - TCP/IP Properties



450U-E

Dipswitch setting (at boot):	RUN Mode
Dipswitch setting (current):	RUN Mode
Ethernet MAC Address:	00:12:AF:30:01:FC
Owner:	Owner
Contact:	Contact
Device Name:	Device
Description:	Description
Location:	Location
Configuration Version:	
Model:	450U-E-450-GL
Serial Number:	0613000102
Hardware Revision:	1.1A
Firmware Version:	1.1dev -- Tue Jun 11 15:52:55 EST 2013
Kernel Version:	#9 PREEMPT Fri Jun 7 16:18:56 EST 2013
Bootloader Version:	2.10 - *** Sep 11 2012 10:50:12 (2374)
Radio Firmware Version:	Software version : 1.00j *** build 1034 [Jun 6 2013 13:08:55] (3756)

Figure 22 – Main Screen

To resume normal configured operation when Configuration is complete, switch Factory Default dip-switch on the 450U-E to RUN and cycle power.

Note: **Security Certificates**. Configuration of the 450U-E uses an encrypted link (https). The security certificate used by the 450U-E is issued by ELPRO and matches the IP address 192.168.0.100.

When you first connect to the 450U-E, your web browser will issue a warning that ELPRO is not a trusted authority. Ignore this warning and proceed to the configuration web page.

Internet Explorer 7 has an additional address check on security certificates. Unless the 450U-E has the address 192.168.0.100, when you first connect to the 450U-E, Internet Explorer 7 will issue a warning about mismatched security certificate address. You can turn off this behaviour in IE7 by selecting

"Tools > Internet Options > Advanced > Security > Warn about certificate address mismatch*"

Method 2 - Set 450U-E Network address to match the local network

For this method you will need to determine what IP address, Gateway address, and Netmask to assign to the 450U-E so that it appears on your network. Ask your system administrator if you don't know the correct settings for your network. E.g.

If the default IP address of the 450U-E modem is 192.168.0.1 and the network you wish to connect to is on 10.10.0.X (PC is on 10.10.0.5)

Once you have determined the correct settings for your network, you need to connect to the modem's RS-232 serial port using a straight through serial cable and a terminal package such as HyperTerminal set to 115,200 baud. 8 data bits, 1 stop bit, no Parity.

- Open HyperTerminal
- Set the SETUP/RUN switch to the SETUP position, and connect power to the modem.
- Observe HyperTerminal and when you see the Woody screen (see below) press <Enter> to get the following prompt "#"

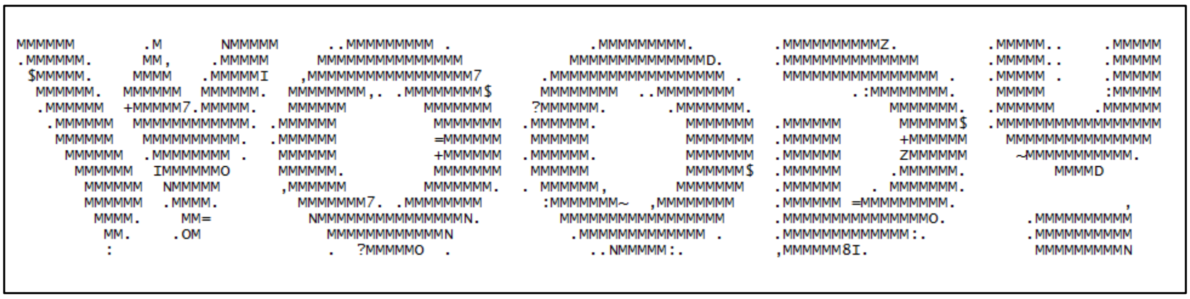
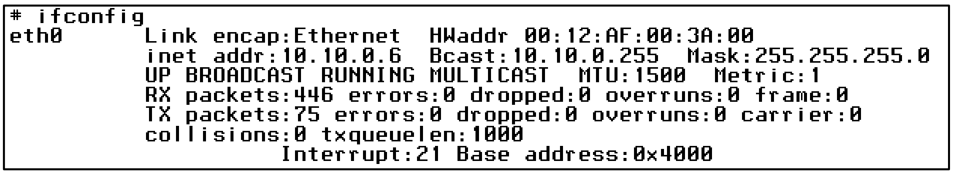


Figure 23 – Woody Screen

- Type the following "ifconfig" and it will show the configuration of the Ethernet port and from this you will be able to see what the IP address is, e.g.



```
# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:12:AF:00:3A:00
          inet addr:10.10.0.6  Bcast:10.10.0.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:446 errors:0 dropped:0 overruns:0 frame:0
          TX packets:75 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
                    Interrupt:21 Base address:0x4000
```

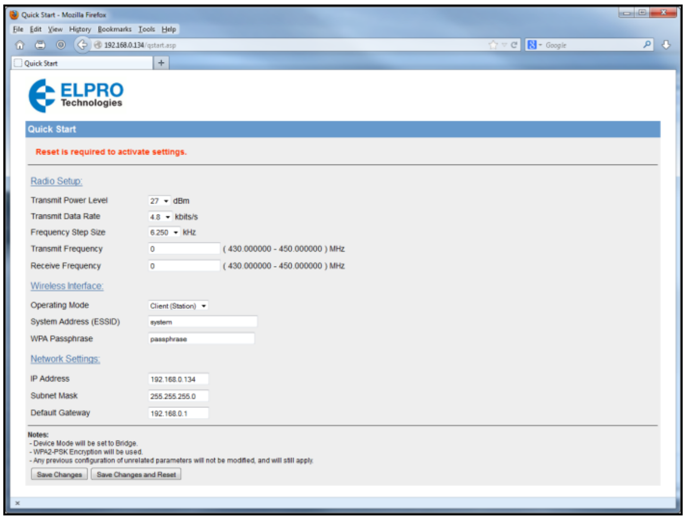
Figure 24 - Ifconfig

- Temporarily change the IP address to something that will enable connection to your local network. E.g type "ifconfig eth0 10.10.0.6 Netmask 255.255.255.0" only add the Netmask if the Netmask is anything other than the standard 255.255.255.0
- IP address should now be changed and you can check by typing "ifconfig" again. Note these changes are only temporary and if the module is reset they will go back to the normal default (192.168.0.XXX).

- Open Internet Explorer and ensure that settings will allow you to connect to the IP address selected. 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.
- Enter the IP address for the 450U-E into the Internet Explorer Address bar e.g. http://10.10.0.6 which is the IP address you temporarily configured with the ifconfig command.
- Enter the username "user" and default password "user".
- You should now be connected to the main index page on the modem as per figure 1 above.
- From here connect to the Network page and change the Ethernet Interface and Wireless Interface IP addresses to 10.10.0.6. Switch the RUN/SETUP switch back to RUN and press "Save Changes and Reset" button.

⚠ **Note: As the modem can be setup numerous ways, e.g. Bridge, Router, etc this setup will allow the modem to appear on the 10.10.0.X network. Any other configuration changes can be done after this initial connection (see the following sections on configuration)**

3.3 Startup



Quick Start

Reset is required to activate settings.

Radio Setup:

Transmit Power Level	27 dBm
Transmit Data Rate	4.8 kbits/s
Frequency Step Size	6.250 kHz
Transmit Frequency	0 (430.000000 - 450.000000) MHz
Receive Frequency	0 (430.000000 - 450.000000) MHz

Wireless Interface:

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

Network Settings:

IP Address	192.168.0.134
Subnet Mask	255.255.255.0
Default Gateway	192.168.0.1

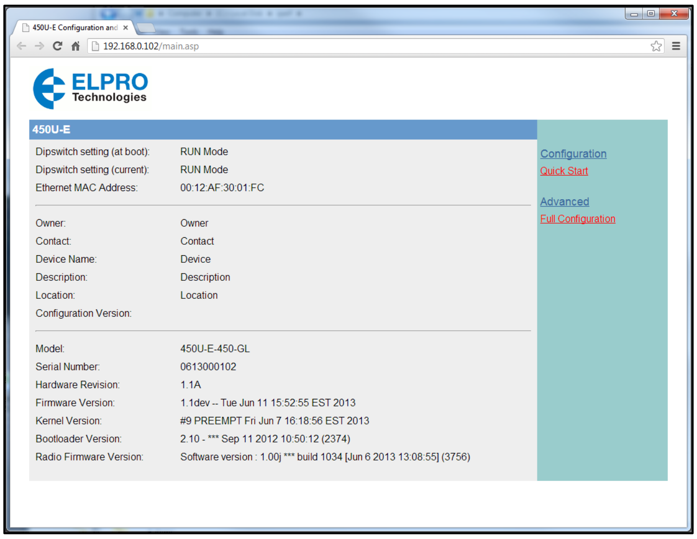
Notes:
- Device Mode will be set to Bridge.
- WPA2-PSK Encryption will be used.
- Any previous configuration of unrelated parameters will not be modified, and will still apply.

Figure 25 – Startup

When connecting to the module for the first time (new or factory defaulted module) you will see the above screen when accessing its default IP address. You are required to enter a number of configuration parameters before the modems can be used, these include Transmit and Receive Frequency as per the country regulation, Radio transmit power level, Operating mode, System Address, Encryption and Network Settings.

This opening screen is essentially the Quick Start configuration screen without the right hand menu. See “Quickstart” below for parameter descriptions.

When complete press the “Save Changes and Reset” button to apply the configuration. When the modem has reset you will be directed to the Main home screen as shown below.

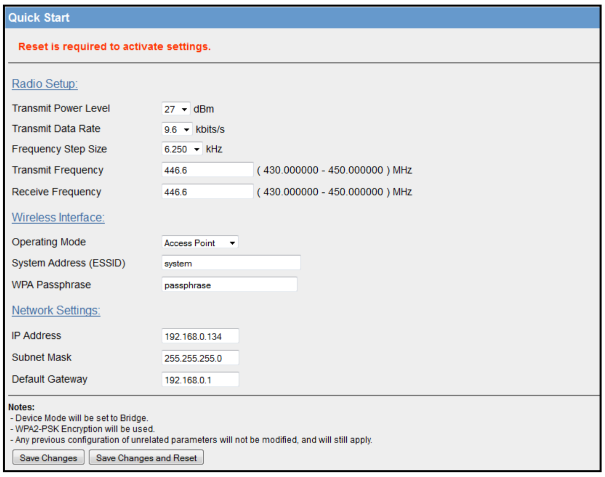


450U-E

Dipswitch setting (at boot):	RUN Mode
Dipswitch setting (current):	RUN Mode
Ethernet MAC Address:	00:12:AF:30:01:FC
Owner:	Owner
Contact:	Contact
Device Name:	Device
Description:	Description
Location:	Location
Configuration Version:	
Model:	450U-E-450-GL
Serial Number:	0613000102
Hardware Revision:	1.1A
Firmware Version:	1.1dev -- Tue Jun 11 15:52:55 EST 2013
Kernel Version:	#9 PREEMPT Fri Jun 7 16:18:56 EST 2013
Bootloader Version:	2.10 - *** Sep 11 2012 10:50:12 (2374)
Radio Firmware Version:	Software version : 1.00j *** build 1034 [Jun 6 2013 13:08:55] (3756)

Figure 26 – Main Screen

3.4 Quickstart



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 446.6 (430.000000 - 450.000000) MHz

Receive Frequency 446.6 (430.000000 - 450.000000) MHz

Wireless Interface:

Operating Mode Access Point

System Address (ESSID) system

WPA Passphrase passphrase

Network Settings:

IP Address 192.168.0.134

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 27 - Quick Start

The Quick Start Configuration option is designed to guide you through the configuration process with minimal effort. You can access it any time by selecting it from the right hand menu. This is a simple first stage configuration tool that will guide you through the configuration of the basic parameters that are needed to get a connection between two modules. For most applications, no further configuration should be needed however if more advanced options are required the normal configuration pages can be edited after the Quick Start configuration has been saved.

1. Select “Quick Start” from the Main Menu and then you need to select the following parameters:

    - **Transmit Power Level** - This allows adjustment of 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 C - ” for dBm to mW conversion

    - **Transmit Data Rate** - The 450U-E can be configured for different radio transmission rates. Note: reducing the configured data rate may increases the reliable range of the module (transmission distance).The radio baud rate 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 & 9600 kbps for narrow band. The Transmit Data Rate only applies to the Transmit messages as the radio can receive on either data rate.
    - **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 5Khz or 6.25KHz.
    - **Transmit Frequency** - The Frequency that you wish to configure for the radio Transmitter. Frequency selection will be in multiples of the frequency step configured in the previous parameter. E.g. 450.00500, 450.01000, 450.01500, 450.02000, etc. for 5Khz or 450.00625, 450.01250, 450.01875, 450.02500, etc. for 6.25KHz frequency step size.
    - **Receive Frequency** - The Frequency that you wish to configure for the radio Receiver. Frequency selection will be in multiples of the frequency step configured in the previous parameter. E.g. 450.00500, 450.01000, 450.01500, 450.02000, etc. for 5Khz or 450.00625, 450.01250, 450.01875, 450.02500, etc. for 6.25KHz frequency step size.
    - **Operating Mode** - Used to select Access Point or Client. The default is set to Client.
    - **System Address (ESSID)** - A 450U-E wireless network comprises 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 1 to 31 characters in length. Select a text string which identifies your system.
    - **WPA Passphrase** - It is assumed that WPA2-PSK (AES) Encryption will be used. Enter in the Encryption key passphrase that you wish to use. Select “Security” from the menu after the Quick Start has been saved if a different Encryption Method is required. (See section below for details)
    - **IP Address** - The IP address of the 450U-E module.
    - **Subnet Mask** - The IP address of the 450U-E module.

- **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). This is only required if the wired LAN has a Gateway unit which connects to devices beyond the LAN - for example, Internet access. If there is no Gateway on the LAN, set to the same address as the Access Point - that is, the "Ethernet IP Address" below. Refer to section 3.13 "IP Routing" for more information.

2. After configuring, select "**Save Changes and Reset**".

3.5 General Configuration

Connecting to Existing Networks.

When configured as a Bridge (default), the 450U-E will transmit all broadcast messages appearing at its wired Ethernet port over the radio. As the modem has a low data throughput any unnecessary traffic being sent over the radio could lower the available bandwidth which will compromise the reliability of the wireless link.

In many cases, the intended recipient of the broadcast traffic that is heard on the Ethernet port does not lie at the opposite end of a proposed radio link. Therefore it is recommended that the radios be configured with some basic filtering or be configured as a routing network to limit unnecessary broadcast traffic being sent over the radio. Refer to Section 3.14 "Filtering" for more details on how this can be implemented.

A system of 450U-E's must have at least one Access Point configured as a master with one or more Clients.

All 450U-E's should be given the same System Address (ESSID) and Radio Encryption settings. For further information and examples on wireless network topologies refer section 1.0 "Network Topology" above.

The 450U-E supports three different radio encryption methods, WEP128, WPA2-PSK and WPA Enterprise which can be configured on the Security Page. The default encryption method is WPA2 and is setup during the Quickstart process by simply entering a Password.

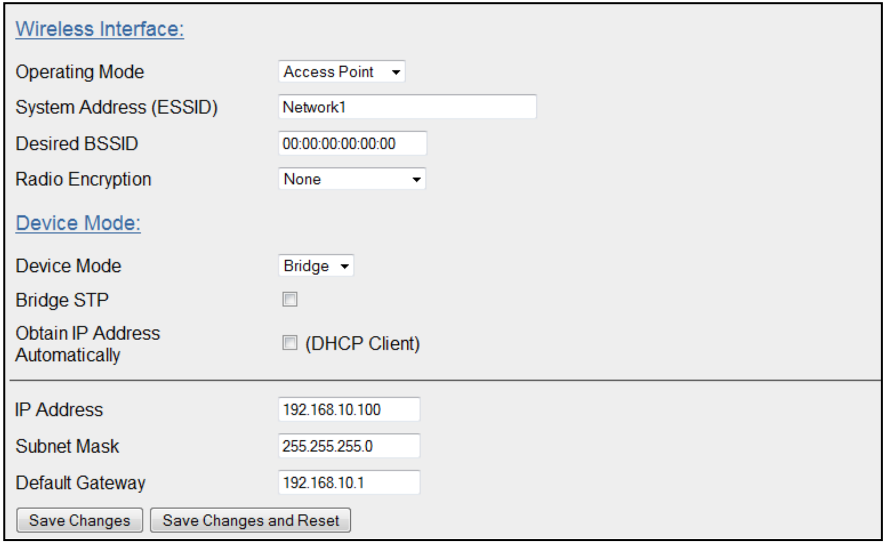
If utilising any form of encryption, all modules in the system will need the same encryption method and keys. It is advisable to enter a new password and to not use the default "passphrase". The available encryption methods are described in detail in Section 3.8 "Security Menu" below.

Note: If making changes to a remote module via the radio link make sure all changes are compliant and accurate before pressing the **"**Save **Changes and R**eset**"** button. Some field changes may stop the radio link from working **and will require a hard wire connection to change back.**

You can view or modify any of the webpage configuration parameters by selecting the appropriate link from the right hand menu. When prompted for username and password, enter "**user**" as the username, and "**user**" as the password (This is the factory default – See section 4.10 "Module Information Configuration" to change).

If you have forgotten the IP address or password, the Factory Default switch may be used to access the existing configuration. Refer to "Default Configuration" in Section 3.2 above for this procedure.

3.6 Network Configuration



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

You can view or modify Ethernet network parameters by selecting the “Network” menu. The Network Configuration page allows configuration of parameters related to the wired and wireless Ethernet interfaces. In general, IP address selection will be dependent upon the connected wired Ethernet device(s) – before connecting to an existing LAN consult the network administrator.

Default configuration of the module will be Client and Bridge. When in Bridged Mode the modules wired and wireless IP address will be the same, meaning only one IP Address is required. If the Device Mode is changed to Router the page will display two IP addresses, one for Ethernet and one for Wireless. For more information on Bridging Networks see section 3.13 “IP Routing“

Network Settings Webpage Fields

Operating Mode Used to select Access Point, Client. Default is set to Client.

System Address (ESSID) A 450U-E wireless network comprises 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 1 to 31 characters in length. Select a text string which identifies your system.

Desired BSSID To force a client/station to always connect to the same Access Point enter the MAC address of that Access Point in the Desired BSSID field

(Note that the ESSID of the Access Point must also match the configured ESSID of the client).

Radio Encryption Select the desired radio Encryption level.

Encryption key, passphrase, etc. is entered on the “Security Menu” (See section 3.8 below for details)

Device Mode Used to select Bridge or Router mode. 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 Checking this box enables Spanning Tree protocol in bridged networks. See to section 3.7 “Spanning Tree ” for more details

Obtain IP Address Automatically Checking this item 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, refer to section 4.10 “DHCP Client Configuration”, default is unchecked.

IP Address **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 The IP network mask of the 450U-E module. This should be set to 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). This is only required if the wired LAN has a Gateway unit which connects to devices beyond the LAN - for example, Internet access. If there is no Gateway on the LAN, set to the same address as the Access Point - that is, the "Ethernet IP Address" below. Refer to section 3.13 "IP Routing" for more information.

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 450U-E. Once the module has completed the reboot sequence, all changes are in effect.

3.7 Spanning Tree Protocol Algorithm

The bridge "Spanning Tree Protocol" function was introduced to handle network loops and provide redundant paths in networks. To enable tick the STP box on the "Network" configuration page.

For example, consider this network with a redundant wireless link. If the bridge Spanning Tree Protocol is enabled, one of the two wireless links will be disabled - that is, 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.

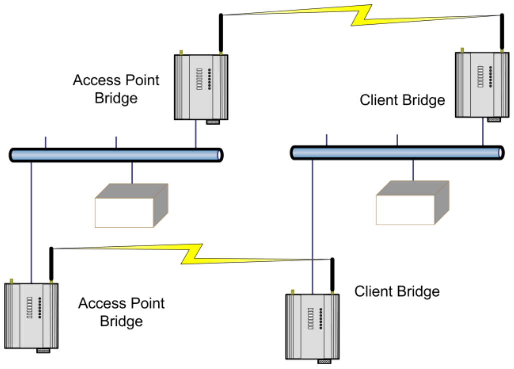


Figure 29 - Spanning Tree Protocol

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 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. "Bridge Priority" only becomes visible when STP is enabled. The root node is typically the unit that handles the majority of traffic in the network. The 450U-E is configured with a Bridge Priority of 32768 by default. The intention is to reduce traffic that the 450U-E must handle, by placing it at the branch level in the network tree. As a branch, the 450U-E needs only pass traffic to devices that are its "leaves".

There is some overhead in maintaining a network utilizing the Spanning Tree Algorithm. Users wishing 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.

3.8 Security Menu

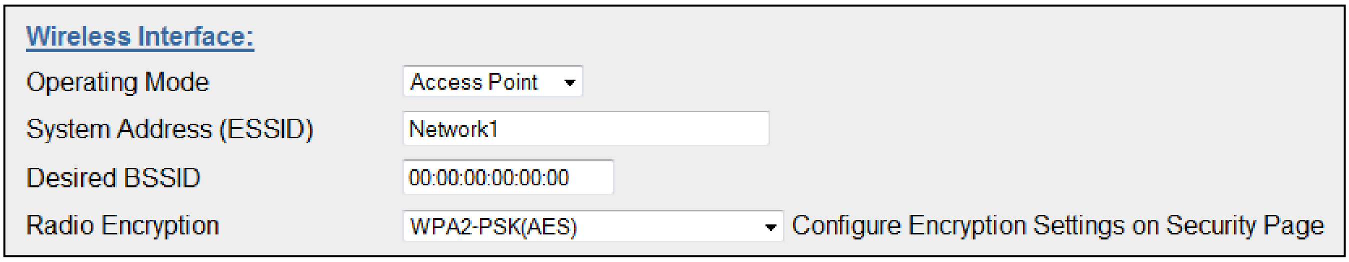
Select the Radio Encryption level from the drop down menu on the Network page and then press the "Save Changes" button. The default setting is "None".

Available encryption levels are:

- None
- WEP128 (Wired Equivalent Privacy)
- WPA2-PSK (AES) (Wi-Fi Protected Access 2)
- WPA-Enterprise (802.1x)

When selection has been made, it is important to save the configuration by selecting "Save Changes".

You will now need to go to the "Security Menu" and enter in the encryption keys (WEP), passphrase (WPA), etc.



Wireless Interface:

Operating Mode	Access Point
System Address (ESSID)	Network1
Desired BSSID	00:00:00:00:00:00
Radio Encryption	WPA2-PSK(AES) Configure Encryption Settings on Security Page

Figure 30 - Security Menu

When all selections have been made the configuration needs to be saved and the module restarted by selecting “Save Changes and Reset”.

WEP (128 bit)

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

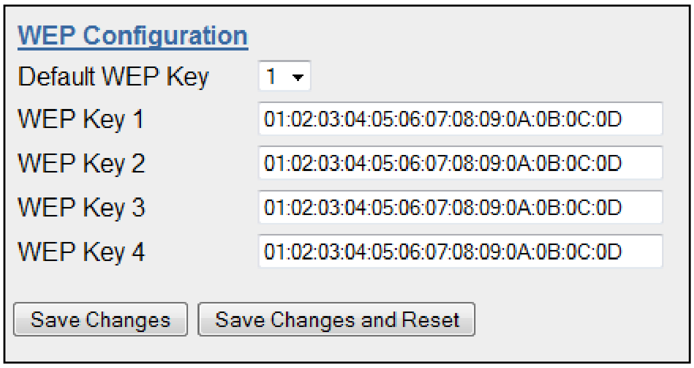
Encryption Keys 1 to 4

These are the keys used to encrypt radio data to protect data from unwanted eavesdroppers when WEP Encryption is selected. These keys should be the same for all 450U-E units in the same system.

WEP keys must be entered as pairs of hexadecimal digits separated by colons. Hexadecimal digits are in the range 0...9 and A...F.

128bit WEP requires 26 Hexadecimal digits. For example, 12:AB:EF:00:56:15:6B:E4:30:C8:05:F0:8D for 128bit encryption

Encryption keys must not be all zeros, i.e. 00:00:00:00:00



WEP Configuration

Default WEP Key	1
WEP Key 1	01:02:03:04:05:06:07:08:09:0A:0B:0C:0D
WEP Key 2	01:02:03:04:05:06:07:08:09:0A:0B:0C:0D
WEP Key 3	01:02:03:04:05:06:07:08:09:0A:0B:0C:0D
WEP Key 4	01:02:03:04:05:06:07:08:09:0A:0B:0C:0D

Figure 31 - WEP

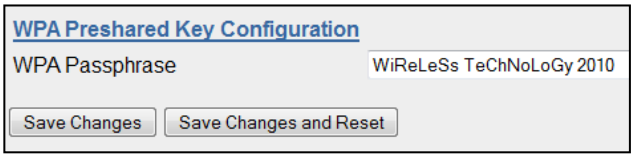
Default WEP Key

One of the four keys may be selected as the default key, and is used to encrypt transmitted messages from the configured unit. A 450U-E can receive and decrypt a message from a module that has a different default key index as long as each module has the same key configured at the same index.

WPA2

WPA2-PSK (AES) (Wi-Fi Protected Access 2) 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 (Advanced Encryption Standard) is the most secure encryption method, is also based on 128 bit encryption key.

When WPA Encryption is selected, 128bit Encryption keys are internally generated based on the Passphrase and System Address (ESSID). The Passphrase must be between 8 and 63 characters in length, and the Passphrase must be the same for all 450U-E units in the same system.



WPA Preshared Key Configuration

WPA Passphrase	WiReLeSs TeChNoLoGy 2010

Figure 32 – WPA2

For optimal security consider using a passphrase consisting of a combination of letters and numbers (i.e. not just a simple word or phrase) as well as upper and lower case. E.g. “WiReLeSs TeChNoLoGy 2010”

WPA Enterprise

WPA-Enterprise (802.1x) removes the need to manage the Pre-shared Key (PSK) by using an external server to provide client authentication. Clients that are not authorized will be prevented from accessing the network. Once a client has provided the correct authentication credentials, access is permitted and data encryption keys are established, similar to WPA-PSK. Fine-grain (user level) access control can be achieved using this method.

An 802.1x capable RADIUS server may already be deployed in a large scale network environment. The 450U-E can make use of this server reducing replication of user authentication information.

In a typical WPA-enterprise setup, the 450U-E Access point acts as Authenticator, controlling access to the network. The other wireless 450U-E clients act as Supplicants, requesting access to the network. The Authenticator communicates with an authentication (RADIUS) server on the Ethernet network to verify Supplicant identity. When a Supplicant requests access, it sends an access request to the Authenticator, which passes an authentication request to the external authentication server. When the user credentials of the Supplicant are verified, the Authenticator enables network access for the Supplicant, data encryption keys are established and network traffic can pass.

Configuration of WPA-Enterprise differs when the unit is configured as an Access point (Authenticator) or Client (Supplicant). If WDS interfaces are used, it is possible for one 450U-E to act as both an Authenticator and a Supplicant, however in this situation, only one set of user credentials can be entered for all Supplicants.

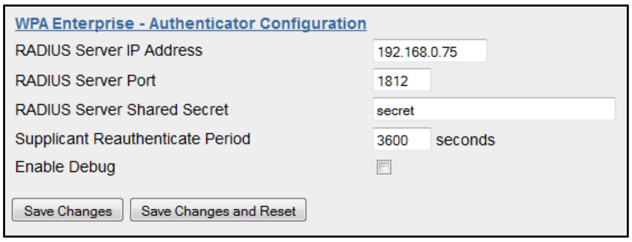
The 450U-E supports WPA-1 TKIP, WPA-1 AES and WPA-2 AES using a *Pre-Shared Key* (PSK).

Authenticator (AP) Configuration

RADIUS Server IP Address/Port/shared secret:
Connection information for the RADIUS Authentication Server.

Supplicant Re-authenticate Period:

Sets the maximum time at which the Supplicant must re-authenticate. This parameter determines maximum time a client will still have access to the network after its user credentials have been revoked.



WPA Enterprise - Authenticator Configuration

RADIUS Server IP Address	192.168.0.75
RADIUS Server Port	1812
RADIUS Server Shared Secret	secret
Supplicant Reauthenticate Period	3600 seconds
Enable Debug	□

Figure 33 - WPA Enterprise Authenticator

Enable Debug:

Must only be used during commissioning and only if requested by ELPRO Support. This must be disabled for normal operation.

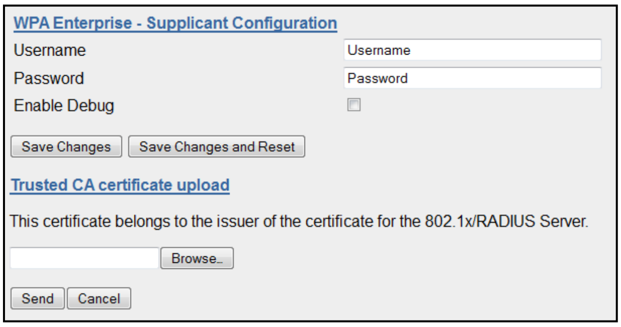
Supplicant (Client) Configuration

Username / Password:

User credentials that match a valid user on the RADIUS server.

Enable Debug:

Disabled for normal operation. Enables debug mode for use during commissioning. To be used only if requested by ELPRO Support.



WPA Enterprise - Supplicant Configuration

Username	Username
Password	Password
Enable Debug	□

Trusted CA certificate upload

This certificate belongs to the issuer of the certificate for the 802.1x/RADIUS Server.

Figure 34 - WPA Enterprise Supplicant

Trusted CA certificate upload

Upload the certificate of the issuer of the RADIUS server’s certificate. This enables the Supplicant to verify the identity of the RADIUS server during the authentication process.

Supported EAP method - PEAP / MSCHAPv2

Certificate Verification result:

Once a certificate has been loaded, this text box will contain validation information for the certificate. If this text is blank or contains errors, the certificate is invalid.

Trusted CA Certificate Contents:

.Displays the contents of the loaded certificate

3.9 Bridge / Router Operation

Bridge Operation (Transparent Network)

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 - 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. Refer Section 3.14 "Filtering" for how to configure a filter.

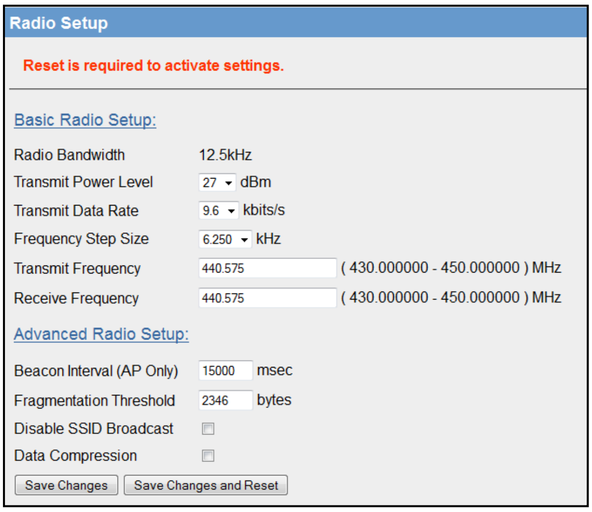
By default, a transparent bridge does not handle loops within the network. There must be a single path to each device on the network. Loops in the network will cause the same data to be continually passed around that loop. Redundant wireless links may be set up by enabling the bridge Spanning Tree Protocol (see section 3.7 "Spanning Tree Protocol Algorithm" for more 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 sub networks. 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 wish to communicate with devices on the other network, they direct their packets to the router for forwarding.

As the router has an IP address on each of the networks 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 to. For details on configuring routing rules, see section 3.13 "IP Routing".

3.10 Radio Configuration



Radio Setup

Reset is required to activate settings.

Basic Radio Setup:

Radio Bandwidth	12.5kHz
Transmit Power Level	27 dBm
Transmit Data Rate	9.6 kbits/s
Frequency Step Size	6.250 kHz
Transmit Frequency	440.575 (430.000000 - 450.000000) MHz
Receive Frequency	440.575 (430.000000 - 450.000000) MHz

Advanced Radio Setup:

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

Figure 35 - Radio Config

The Radio Configuration page is where configuration parameters associated with the radio can be adjusted or configured.

The first time out of the box configuration will run a configuration wizard that will step you through some radio questions that will allow you to select radio configuration for your country of operation and license.

The factory-default parameters of the radio will be set to values that will allow the radio to be powered up safely, without it interfering with radio equipment that may be available in the country of operation. I.e. transmit and receive frequencies will be set to zero.

After the initial out of the box configuration you will be able to configure available radio parameters by selecting the "Radio" page. When all changes are made, you will need to select "Save & Activate" to retain the changes.

Radio Menu

Radio Bandwidth This is the Bandwidth of the radio and it is factory set. It will be either 12.5KHz (narrow band) or 25Khz (wide band)

Transmit Power Level This allows adjustment of 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 E - " for dBm to mW conversion

Transmit Data Rate The 450U-E can be configured for different radio transmission rates. Note: reducing in the configured data rate may increases the reliable range of the module (transmission distance).

The radio baud rate 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 25KHz wide band or 4800 & 9600 kbps for 12.5KHz narrow band.

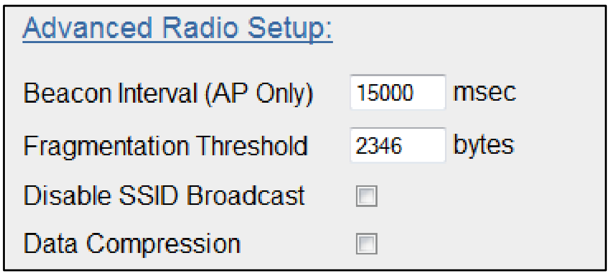
The Transmit Data Rate only applies to the Transmit messages as the radio can receive on either data rate.

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 5Khz or 6.25KHz.

Transmit Frequency The Frequency that you wish to configure for the radio Transmitter. Frequency selection will be in multiples of the frequency step configured in the previous parameter. E.g. 450.00500, 450.01000, 450.01500, 450.02000, etc. for 5Khz or 450.00625, 450.01250, 450.01875, 450.02500, etc. for 6.25KHz frequency step size.

Receive Frequency The Frequency that you wish to configure for the radio Receiver. Frequency selection will be in multiples of the frequency step configured in the previous parameter. E.g. 450.00500, 450.01000, 450.01500, 450.02000, etc. for 5Khz or 450.00625, 450.01250, 450.01875, 450.02500, etc. for 6.25KHz frequency step size.

The following are advanced settings and care should be taken when making changes to the parameters on this page.



Advanced Radio Setup:

Beacon Interval (AP Only) 15000 msec

Fragmentation Threshold 2346 bytes

Disable SSID Broadcast □

Data Compression □

Figure 36 - Advanced Radio

Beacon Interval (AP only) This interval is the period between beacon transmissions sent by an Access Point. The default value is 15 seconds, and it 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 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 should be 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 Enable/Disable Data compression. See below for details

Save Changes Save changes to non-volatile memory

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

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, etc. which simply matches duplicate strings within the data frame with pointers to previous data patterns. It 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 web page download
- 40% improvement if using FTP download

3.11 Serial Port Configuration

The 450U-E has an RS-232, and an RS-485 port which is used for serial communications. These ports may be used for different purposes. The 450U-E offers three different serial functions, Modbus RTU Master, Expansion I/O and Modbus RTU Slave which are configured on the “Serial Configuration” page along with any other serial communication parameters.

Operating Mode

- **Modbus RTU Master** – This mode should be configured when the port is operating as a Modbus Master, i.e. Modbus RTU slave devices are connected directly to the serial port.
- **Modbus RTU Slave** – This operating mode should be used if the port is being used as a Modbus RTU slave, i.e. if a Modbus Master (DCS, Scada, etc.) is connected to the serial port.
- **Expansion I/O** – This operating Mode should be selected when Elpro Serial Expansion modules (115S-XX) are connected to the modem.

Date Rate Serial date Rate. The data rate will need to be configured 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 The Serial Data format defines the number of data bits, parity and start/stop bits that is used to communicate with the serial device.

Flow Control The 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 RS232 supports CTC/RTS hardware flow control.

Max Num Units to Poll This is the maximum number of Modbus address that will be polled on the serial interface when the port is configured for Expansion I/O. The default for RS232 is one and three addresses will be polled on the RS485

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

3.12 Repeaters (WDS)

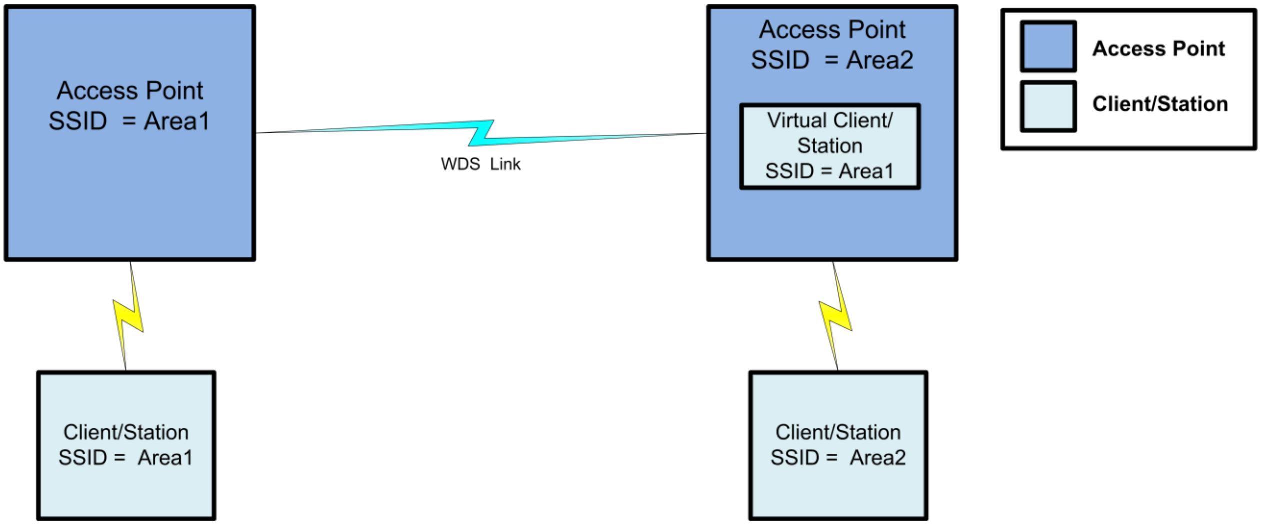


Figure 37 - WDS Repeaters

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 AP to AP links can be configured for optimized throughput.

Each 450U-E Access Point supports up to 3 Virtual Access Point or 5 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, as they are bridged with the standard *wireless interface* that is used for connections to associated clients. All of the 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 (see section 3.7 "Spanning Tree Protocol Algorithm"), thus behaving as a self-healing mesh network. 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; however each side of a single WDS link must specify the same encryption algorithm and keys.
- A maximum of 3 virtual AP's or 5 virtual Client/STA applies per unit.
- WPA-Enterprise configuration is shared with the base AP (Authenticator) or Station (Supplicant).

WDS Connections:

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

Delete Entry Button 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.

- AP (Downlink) configures the connection as a virtual Access Point.
- Sta (Uplink) configures the connection as a virtual Station/Cient.

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.*

There are many different ways to setup wireless networks; often it depends on the devices you wish to connect and the existing network topology.

The following pages show some examples of how to connect devices into different types of systems.

Example 1 – Extending range using WDS

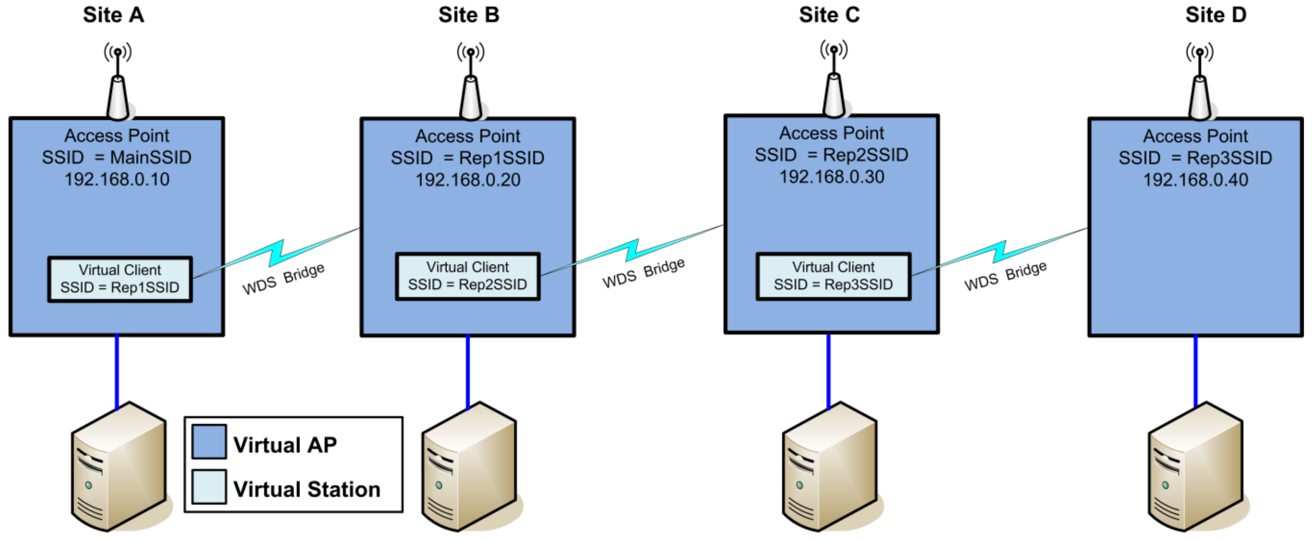
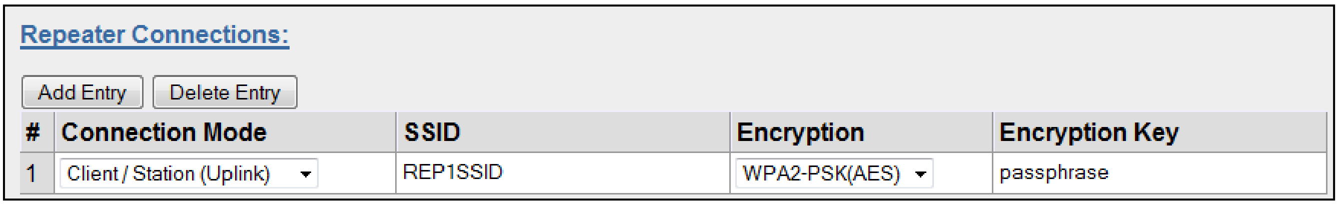


Figure 38 - Extending Range

One of the most common uses for WDS is to extend the range of the wireless network using repeaters. The diagram in Figure 38 above 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 so 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.

The WDS configuration is accessed by selecting the *Repeaters* link on the configuration web page. Configuration for Site A is shown above in Figure 39. 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 who also has a Virtual Client that connects to the Access Point at Site D.



Repeater Connections:

Add Entry | Delete Entry

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

Figure 39 - Site A WDS Configuration

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 the encryption method be equal to or greater than the main system so as to maintain system security. Also since it is a bridged network the Spanning Tree Protocol is disabled on the network configuration page as there is no possibility of network loops.

Example 2 - Roaming with WDS Access Points

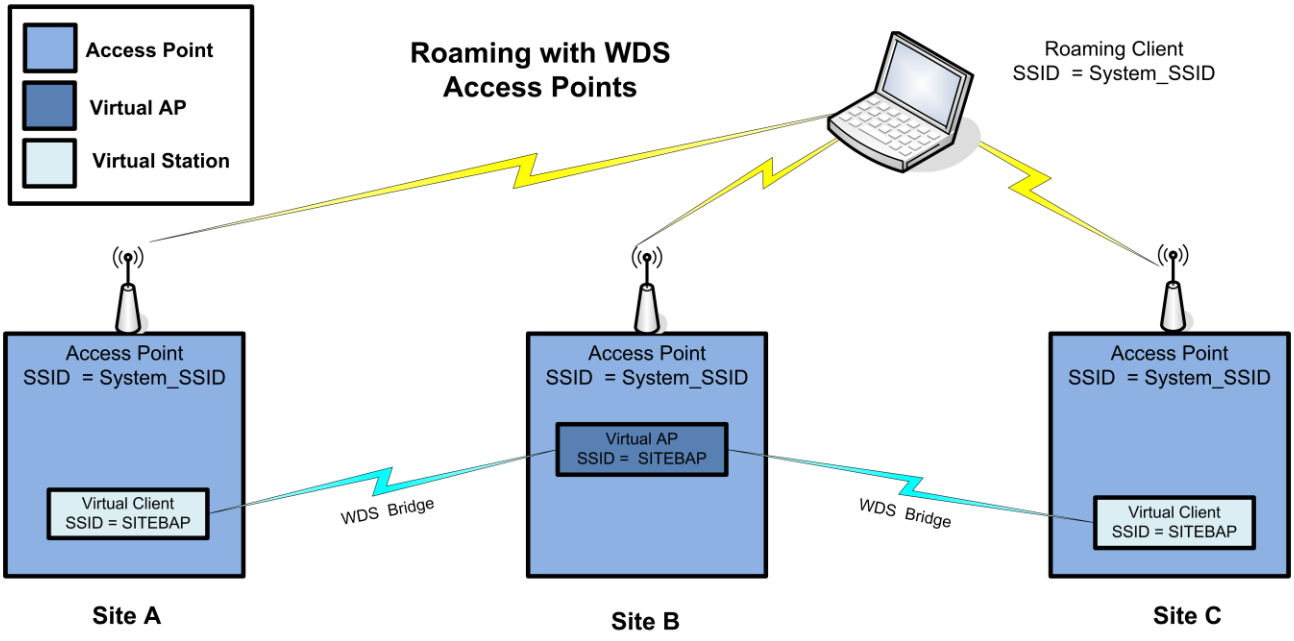


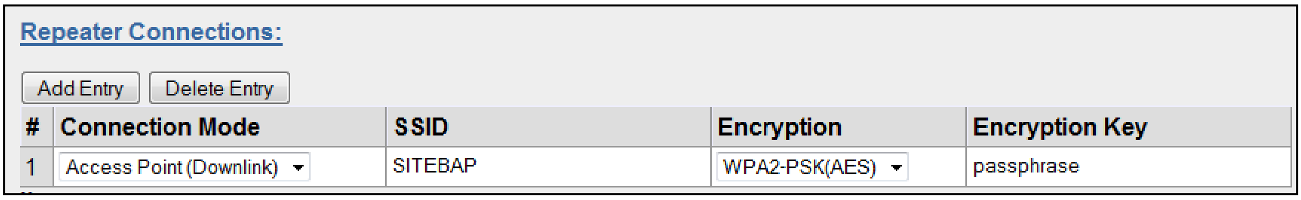
Figure 40 - WDS Roaming

Another common use for WDS is extending the range across a large wireless network but allowing roaming connections between access points or being able to switch to the next Access Point when out of range of the previous Access Point.

The diagram in Figure 40 above shows a bridging network with a number of Access Points all with the same SSID, network structure, etc. (so as 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

The configuration for Site B is shown below in Figure 41. The WDS is configured with a Virtual Access Point for the virtual clients configured at Sites A & C. The Encryption Method and key are configured the same as the main network for simplicity.



Repeater Connections:

Add Entry | Delete Entry

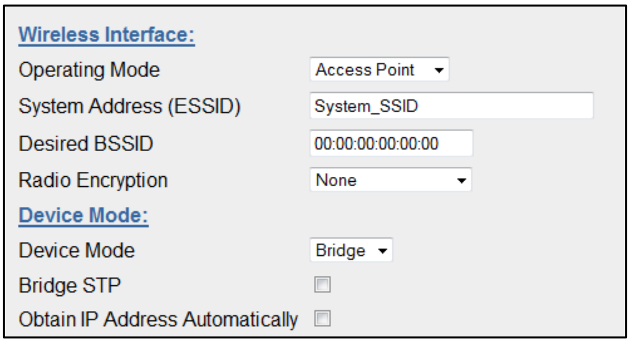
#	Connection Mode	SSID	Encryption	Encryption Key
1	Access Point (Downlink)	SITEBAP	WPA2-PSK(AES)	passphrase

Figure 41 - Site B WDS Configuration 2

The WDS configuration for Site A & Site C will be exactly the same as Site B except the ‘Connection Mode’ will need to be ‘Client / Station (Uplink)’ instead of ‘Access Pint (Downlink)’.

The main network configuration settings for all sites will all be the same for each site (as shown).

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	□

Figure 42 - System Network Settings

3.13 IP Routing

When a 450U-E receives an IP frame that is destined for an IP address on a different network, it checks if the *network address* matches the network address of one of its own interfaces (i.e. hard-wired Ethernet, or 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 (i.e. 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).

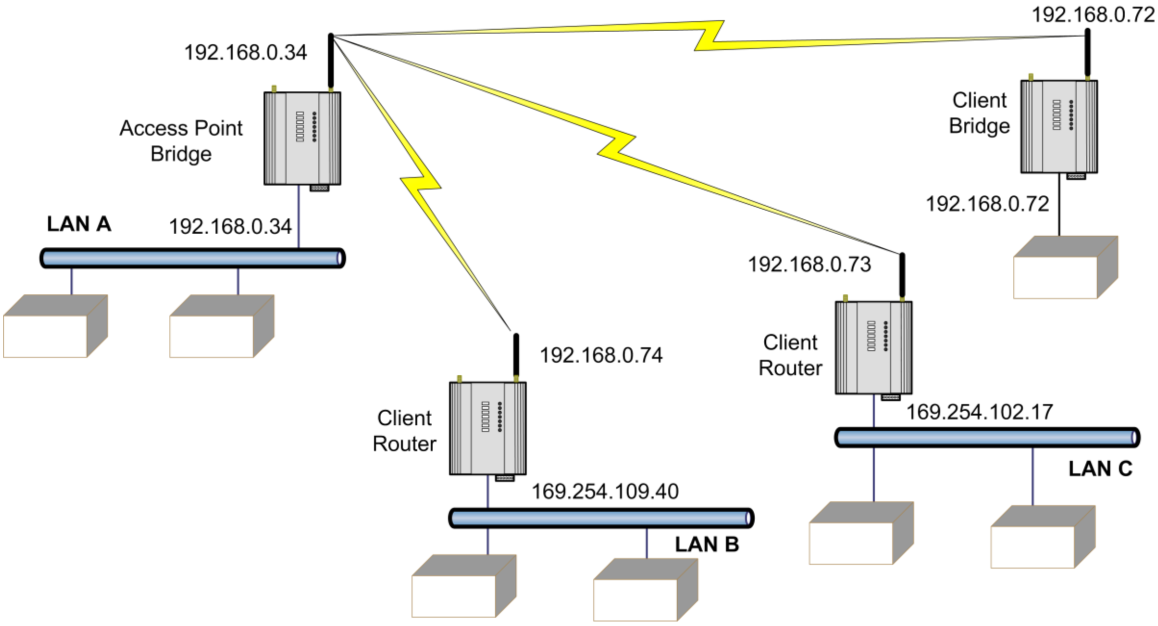
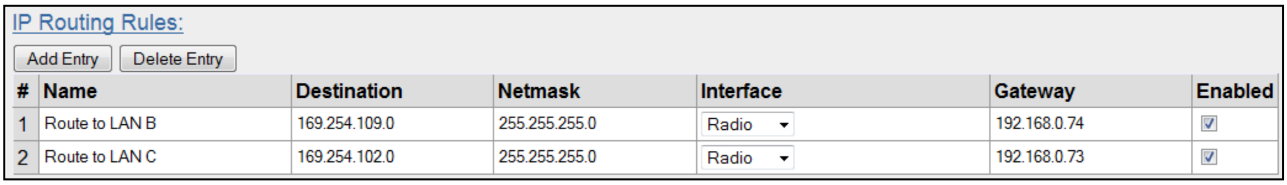


Figure 43 - Routing

The above network diagram 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 (i.e. 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 (i.e. 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 LANs 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 below in Figure 44. 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	Interface	Gateway	Enabled
1	Route to LAN B	169.254.109.0	255.255.255.0	Radio	192.168.0.74	☑
2	Route to LAN C	169.254.102.0	255.255.255.0	Radio	192.168.0.73	☑

Figure 44 - Routing Rules @ AP

Devices on LAN B & 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. I.e. 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.

The Routing Rules configuration page can be accessed by selecting the “Routing” link on any of the configuration web pages. Up to 30 routing rules may be added to each 450U-E. The table below summarizes the configurable parameters of a routing rule.

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. i.e. for an IP address 192.168.0.0 with Netmask 255.255.255.0 would specify a destination network, while 192.168.0.16 specifies a destination host).

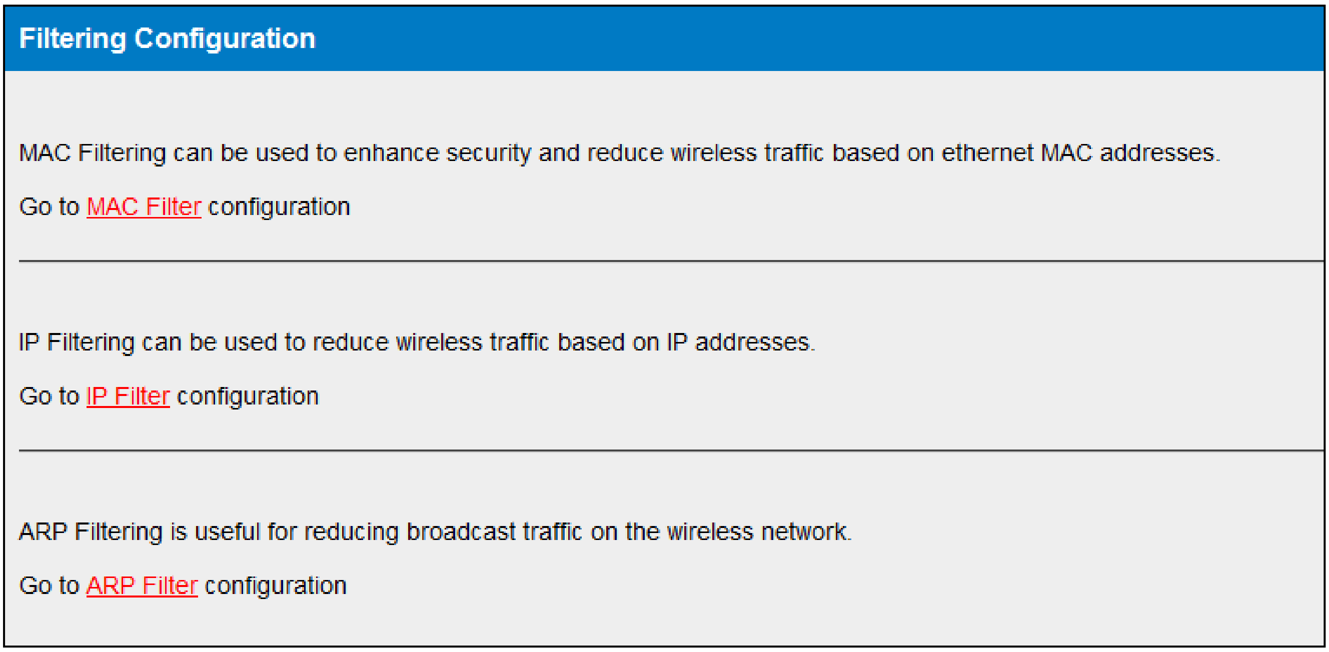
Subnet Mask The subnet mask for the destination network.

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

Enabled Check this box to enable the rule. You can uncheck the box to disable a routing rule without needing to re-enter the information at a later time.

⚠ **Note: Entering dedicated Ethernet Routes can also be added to the wired Ethernet LAN in place of generating / adding routing rules into the modems.**

3.14 Filtering



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 45 - Filtering

The 450U-E has a filtering feature to help reduce unnecessary wireless transmissions and enhance security.

The 450U-E may be configured to reject or accept messages to and from certain Addresses. To accept wireless messages from particular devices a “Whitelist” of Addresses must be made. Alternatively to reject messages from particular devices, a “Blacklist” of Addresses must be made. Filtering applies only to messages appearing at the wired Ethernet port of the configured 450U-E.

The Filter comprises of three lists: MAC Addresses, IP Address/Protocol/Port and ARP Filters. Each 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 Filter operates on four rules listed below.

- The MAC Address filter is always checked before the IP Address filter.
- If a message matches a MAC filter entry, it will not be subsequently processed by the IP filter. If the MAC filter list is a Whitelist, the message will be accepted. If the MAC filter list is a Blacklist, the message will be dropped.
- The MAC address list 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) which 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).

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.

An example of IP filtering is shown below;

Device B needs to communicate with Device E via modems C & D. The Filtering requires that Modem C has Device B in its Whitelist. As IP filtering checks both source and destination IP’s 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 was being initiated from each end, i.e. a non-polling system you would need to put a filter list in 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, as Device A is not present in the Whitelist in Modem C.

It is also recommended to add an ARP filter as this would filter out broadcast ARP requests from other devices on the LAN which would normally be sent over the radio. ARP (Address Resolution Protocol) 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 wishes to communicate with another device it needs to know the MAC Address. If the MAC address is not already known or is in its lookup table it will broadcast an ARP request which subsequently would be passed over the radio if the modems were setup in bridging mode. If this is a small network it may not matter however 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.

It should be noted that adding ARP and IP filters will only filter out ARP traffic and IP traffic, any Ethernet traffic that is not IP will be passed, and this could include Netbios, IPX, PPP, etc. These protocols could be more effectively filtered by using MAC filtering or configuring the modems in a Router configuration instead of a Bridge.

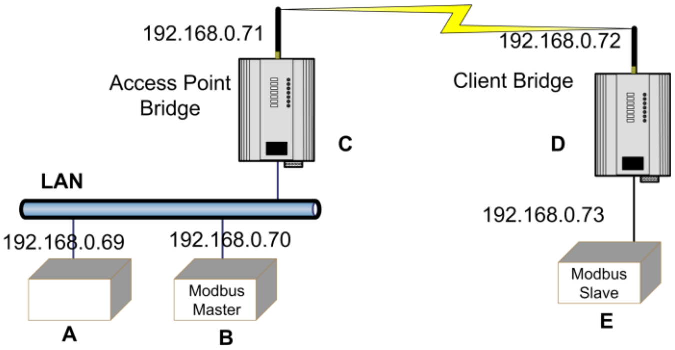


Figure 46 - Filtering Example

⚠ **If an erroneous configuration has prevented all access to the module, SETUP mode may be used to restore operation.**

MAC Address Filter Configuration:

MAC addresses are uniquely assigned to each device and so can be used to permit or deny network access to specific devices through the use of Blacklists and Whitelists.

In theory, MAC filtering allows a 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.

⚠ **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.**

Select “Blacklist” or “Whitelist”.	Blacklist will prevent all listed devices from accessing the module and using the radio link. 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	Add a row to the table of Mac Address filter rules
Delete Entry	Delete the currently selected MAC address filter rule.
Enable	Check 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 Changes and Reset	Save to non-volatile memory And restart to activate changes

IP Address Filter Configuration:

The IP filter allows 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).
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.**

Select “Blacklist” or “Whitelist”.	Blacklist will prevent all listed devices from accessing the module and using the radio link. 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	Add a row to the table of IP Address filter rules
Delete Entry	Delete the currently selected IP address filter rule.
Enable	Check this box to enable the rule
IP Address Min, **IP Address Max**	These set the range of IP addresses. All addresses within the specified range are affected by the rule.
Port Min, **Port Max**	When the protocol is set to TCP or to UDP, this is the range of port addresses to which the rule applies. When protocol is set to All or to ICMP, these settings have no effect.
Protocol	This chooses 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 Changes and Reset	Save to non-volatile memory and restart to activate changes

ARP Filter Configuration

ARP (Address Resolution Protocol) is a broadcast message and is primarily used for finding a MAC address when only its IP or some other Network Layer address is known.

On large networks, you generally tend to get a high proportion of broadcast messages. Using ARP filters 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.

Select “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	Add a row to the table of ARP Address filter rules
Delete Entry	Delete the currently selected ARP address filter rule.
Enable	Check this box to enable the rule
IP Address	This sets the IP address that you wish to filter.
IP Netmask	Sets the IP Netmask
Save Changes	Save changes to non-volatile memory (Reset is required to activate)
Save Changes and Reset	Save to non-volatile memory and restart to activate changes

3.15 Modbus

The 450U-E has an on-board Modbus TCP Server/RTU Slave and a Modbus TCP Client/RTU Master which provide connectivity for a range of Modbus applications. The modem can be configured with any combination of the following modes.

- **Modbus TCP Server** – This mode will allow an external Modbus TCP Client to access the internal I/O and status registers of the module.
- **Modbus TCP Client** – This mode will allow the module to act as a TCP Client (Master) and poll external TCP server devices, transferring any polled data values to either the internal registers or an external TCP server device.
- **Modbus RTU Slave** – In this mode the module will act as a Modbus RTU slave and allow the internal registers to be accessed by a Modbus RTU Master via the RS 232 or RS485 serial ports.
- **Modbus RTU Master** – This mode will allow the module to act as a Modbus RTU Master and poll any Modbus RTU slave devices via the serial ports, transferring any data to or from the units internal I/O registers.
- **Modbus TCP to RTU Converter** – This mode will convert any Modbus TCP Client data coming in via the Radio or Ethernet connections and pass it to any Modbus RTU devices connected to the serial ports and visa versa.

The Modbus TCP Client and the Modbus TCP Server/RTU Slave can be supported simultaneously, and when combined with the built in Modbus TCP to RTU Gateway the 450U-E can transfer I/O to/from almost any combination of Modbus TCP or RTU devices.

Modbus RTU Master ports

Each serial port has a number of parameters that can be adjusted for different applications.

TCP Port Port numbers used for the Modbus TCP to RTU conversion – Standard ports are 503 for RS232 and 504 for RS485.

Pauses Between Requests This is the delay between serial request retries in milliseconds

Response Timeout The serial response timeout in milliseconds – a serial retry will be sent if a response is not received within this timeout. If using TCP to RTU communication this Response time should be configured in conjunction with the Response time for the TCP Client.

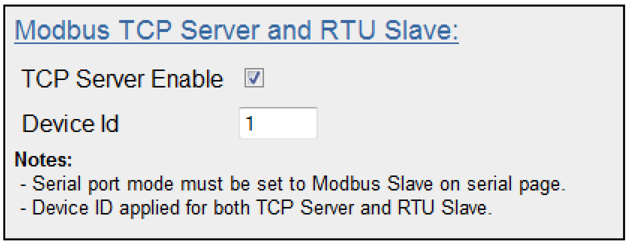
Connection Timeout The TCP connection timeout in seconds – if no Modbus/TCP data is received within this timeout then the TCP connection will be dropped. Set this field to zero for no timeout.

Maximum Request Retries The maximum number of request retries performed serially.

Modbus TCP Server / RTU Slave

Modbus TCP Server / RTU Slave enable the 450U-E to accept connections from Modbus TCP Clients (Masters).

All Modbus transactions routed to the onboard Modbus TCP Server are directed to/from the onboard general purpose I/O registers. The Modbus TCP Server is shared with the Modbus TCP to RTU Converter, so that the Modbus “Device ID” is used to determine if a Modbus transaction is to be routed to the onboard Modbus TCP Server or to a Modbus RTU device connected to the serial port. Care should therefore be taken that all serially connected Modbus devices use a different Modbus Device ID (i.e. Modbus Slave Address) to the onboard Modbus TCP Server. Up to 32 separate connections to the Modbus TCP Server are supported.



Modbus TCP Server and RTU Slave:

TCP Server Enable ☑

Device Id 1

Notes:
- Serial port mode must be set to Modbus Slave on serial page.
- Device ID applied for both TCP Server and RTU Slave.

Figure 47 -Modbus TCP Server

Modbus TCP Client

The Modbus TCP Client/RTU Master enables the 450U-E to connect to one or more Modbus TCP Servers/RTU Slaves.

All Modbus Mappings are directed to/from the onboard I/O registers depending on configuration which is described below.

There are two separate mapping tables, one for TCP Clients mappings and one for RTU Master Mappings. The RTU Master Mappings table is used for communications to Modbus Slave devices connected on the RS232 or RS485 ports and the TCP Client Mappings table is used for communications with TCP Servers via the Ethernet port. Each of the mapping scenarios will be explained below based on the system in Figure 48 – Modbus Example

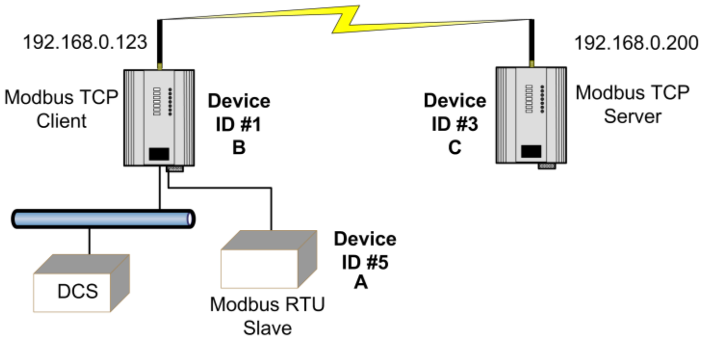


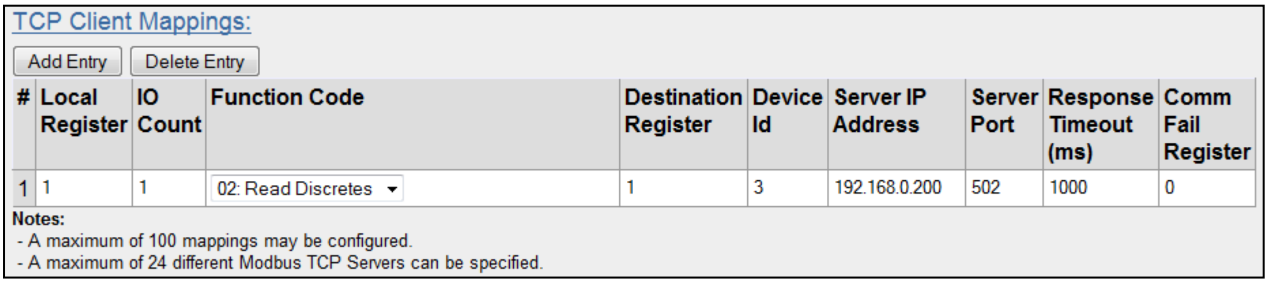
Figure 48 – Modbus Example

The system in Figure 48 above shows that site B is a Modbus TCP Client and will poll the TCP server at Unit C via the Wireless Ethernet interface to get the status of the on board DIO which will then be reflected on its own DIO.

Site B is also setup as a Modbus RTU Master which will poll 8 x single bit registers from Modbus serial device A and then transfers the values to internal registers.

Enabling the Modbus TCP Server within unit B will provide a register location for the previously polled values 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 & C via the extended wired or wireless networks.

TCP Client Mappings

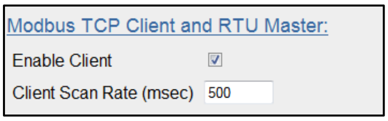


#	Local Register	IO Count	Function Code	Destination Register	Device Id	Server IP Address	Server Port	Response Timeout (ms)	Comm Fail Register
1	1	1	02: Read Discretes ▾	1	3	192.168.0.200	502	1000	0

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

Figure 49 - Site B Modbus TCP Mappings

The Modbus TCP Client / RTU Master is enabled and is using a 500msec scan rate, meaning that there will be a 500msec delay between each of the *mappings* directed at any Modbus server.



Enable Client ☑

Client Scan Rate (msec) 500

- This TCP mapping transfers the status of the onboard digital input at C to the onboard digital output at B. ***Local Register*** (1) specifies the register for the onboard digital output at 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 (i.e. the single digital I/O). ***Function Code*** 02: Read Discretes specifies the standard Modbus function code to read discrete (i.e. digital) inputs. ***Destination Register*** (1) specifies the register for the onboard digital input at the Server IP address (unit C). ***Device ID*** *(*3) is the ID of the onboard Modbus TCP Server at 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*** (1000ms) specifies that unit C must respond to this message within 1000ms. ***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.

Modbus TCP Client Mappings:

Local Register — Enter the starting onboard 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 register to be transferred for the specified transaction.

Function Code — Specify the Modbus Function Code for the transaction.

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.

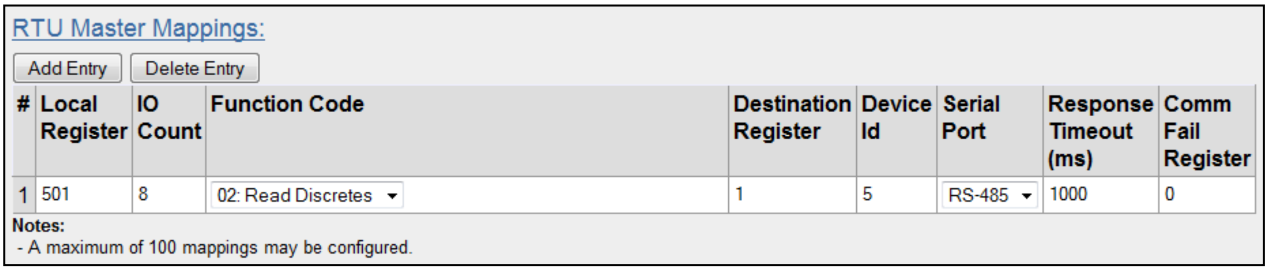
Sever Port — Server Port number used for Modbus TCP. Default/standard port number is 502

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 utilising TCP to RTU communications.

Comm Fail Register — Enter the onboard 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

RTU Master Mappings

As the module is also communicating with a Modbus RTU slave device (Device #5) it will need to have an RTU Master Mapping configured.



#	Local Register	IO Count	Function Code	Destination Register	Device Id	Serial Port	Response Timeout (ms)	Comm Fail Register
1	501	8	02: Read Discretes	1	5	RS-485	1000	0

Notes:
- A maximum of 100 mappings may be configured.

Figure 50 - Site B RTU Mapping

- The RTU Mapping is configured to read 8 x Discrete values starting at register 1 from a Modbus Slave Device ID #5 connected to the RS485 port and store the values at its own local internal register. ***Local Register*** (501) specifies a general purpose Bit Storage area in the module. ***I/O Count*** (8) specifies that it is passing 8 discrete I/O points. ***Function Code*** "02: Read Discretes" specifies the standard Modbus function code to read discrete (i.e. digital) inputs. ***Destination Register*** (1) specifies the register that will be read at the Modbus RTU Slave (unit C). ***Device ID*** (3) is the ID of the onboard Modbus RTU Slave at C.

Care should be taken to ensure that the Device ID (i.e. Modbus Address) of the serial device is different to the Device ID of the onboard Modbus TCP Server of the 450U-E that the serial device is connected to.

⚠ **When configuring RTU Master Mappings you will need to ensure the appropriate serial port is configured for the right mode, in this case the port will need to be configured as a Modbus Master. For more details on how this is done see section 3.11 "Serial Port Configuration").**

Modbus RTU Master Mappings:

Local Register
Enter the starting onboard 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 register to be transferred for the specified transaction.

Function Code
Specify the Modbus Function Code for the transaction.

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
Server Port number used for Modbus TCP. Default/standard port number is 502

Response Timeout
Enter the timeout (in milliseconds) to wait for a response to the specified transaction.

Comms Fail Register
Enter the onboard I/O Register number to store the communication status for the specified transaction. If the register selection is a digital input register (10501), the register will be set to 0 (off) if communications is successful and 1 (on) if there is no connection to the server. If a general Input register is used (30501-32500) for the Comms Fail is it will write the status and the error code which is useful for diagnosing communication problems. I.e. 0xFFxx where xx is the Modbus Exception Code. See Appendix D - “Modbus Error Codes” for more details on the Modbus Error Codes.

⚠ **Note: When entering the Local or Destination registers you do not need to enter in the full Modbus Address, i.e. 30001 or 10001 only the I/O address is needed as the Function Code determines what type of command is being used.**

E.g. if you wish 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 wish to read register 10501 you need to select Function Code 02: Read Discretes and then enter the Destination Register of 501.

Modbus TCP to RTU Conversion

The Modbus TCP to RTU Gateway 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 which is directly connected to the Modbus serial device (i.e. only this module needs to have Modbus TCP to RTU Gateway enabled).

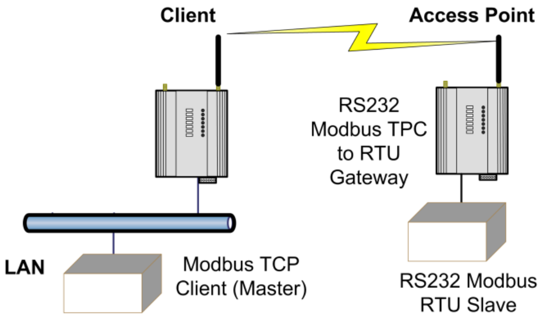


Figure 51 - Modbus TCP-RTU

The above example demonstrates how a Modbus/TCP Client (Master) can connect to one or more Modbus RTU (i.e. serial) Slaves. In this example the 450U-E Access Point is configured with the connected serial port configured for “Modbus RTU Master”. When enabled, the gateway converts the Modbus/TCP query into Modbus RTU and forwards theme out the serial port to the Slave. When the serial device response the query arrives from the Slave, it is converted back into a Modbus/TCP response and forwarded via the network to the Modbus/TCP Master. If no response was received serially by the 450U-E within the configured Response Timeout, the 450U-E will initiate a number of retries specified by the configured Maximum Request Retries.

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

3.16 Input/Output Configuration

The 450U-E has a single physical on-board I/O channel that can be configured as either a Digital or an Analog via the web interface. The Digital channel can 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 registers and module information as well as an area of memory that will hold the values from any expansion modules I/O that maybe connected to the modem.

I/O Configuration

Configuration of the physical I/O (Analog Input or the Digital Input/output) is done by select 'Onboard I/O Mode Configuration' on the 'I/O Configuration' menu, which can be accessed from the main right hand web links.

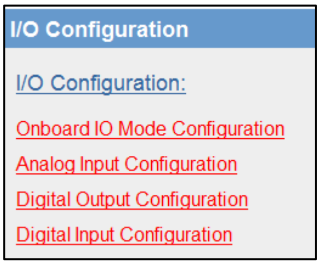
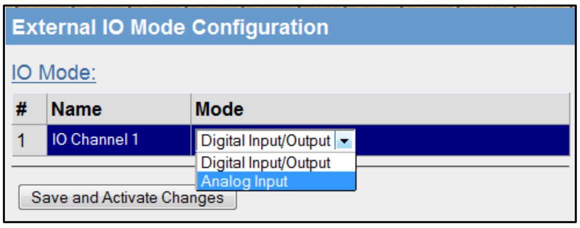

I/O Configuration
I/O Configuration:
Onboard IO Mode Configuration
Analog Input Configuration
Digital Output Configuration
Digital Input Configuration

Figure 52 - I/O Configuration

Selecting the 'Onboard I/O Mode Configuration' screen allows you to change the name of the channel to something more descriptive, i.e. Tank Level, etc and it also allows you to change the input mode from Digital Input /Output to Analog.

When the I/O mode and name have been changed you must press the 'Save Changes and Activate' button for the changes to take effect.

The default I/O Mode is Digital Input/Output


External IO Mode Configuration

IO Mode:

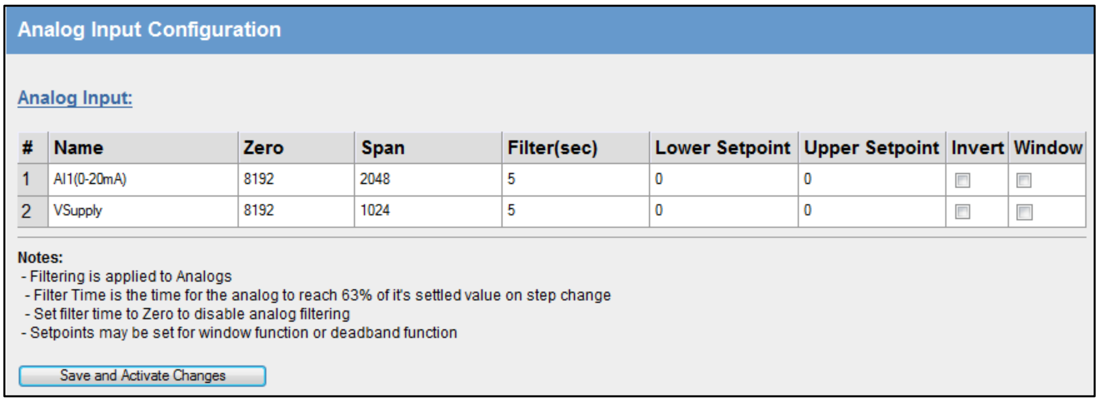
#	Name	Mode
1	IO Channel 1	Digital Input/Output

Figure 53- Input Mode

Analog Input Configuration

Configuration of the I/O channel as an Analog is done by firstly ensuring 'Analog Input' is selected on the 'Onboard I/O Mode Configuration' Screen as shown in "Figure 53 - Input Mode" and then activating the changes by pressing the 'Save and Activate Changes' button

Configuration of the Analog Input channel is performed by selecting 'Analog Input configuration' from the 'I/O Configuration' link.


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 54 - Analog Input

The I/O channel can be configured to accept a 0-20mA current sinking analog input.

The default settings should suffice for most applications however the following parameters can be adjusted to suit the application if needed.

Analog Input configuration parameters

Name – Configure a descriptive name for the Analog input.

Zero – This parameter is used to configure the scale of the analog input. This is the starting variable (in counts) when the analog input is at the bottom or zero scale. Default is 8192 which equates to the number of raw counts in the register when the input is at the zero or minimum value, i.e. 0mA on the analog input.

Span – This parameters is used to configure the scale of the analog input. This is the number of counts per measured value, i.e. 1 mA, 1 V, 1 HZ, etc.). Default is 2048 which equates to 20mA on the analog input. E.g. the register range has a total range of 32768 counts with a total mA range of 16mA; therefore the Span is calculated by dividing the total range in counts by the total range in mA, V, Hz, etc. (32768 / 16 = 2048)

Filter (sec) – The Filter time Constant is the time the analog takes to settle on a step changed 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. 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 – This option toggles the Setpoint control logic between the default normal and inverted state. The function does not change, only the operation is inverted, e.g. if 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 (not ticked)

Window – This parameter toggles the Set point operation between the Default and the Windowed modes.

- Default (un-ticked) - If the Analog Input is greater than the Upper Set point, the set-point status will be active (on, “1”). When the Analog Input is less than the Lower Set Point the setpoint will reset (off, “0”).

  Note: The Upper Set Point must always be higher than the Lower Set Point.”

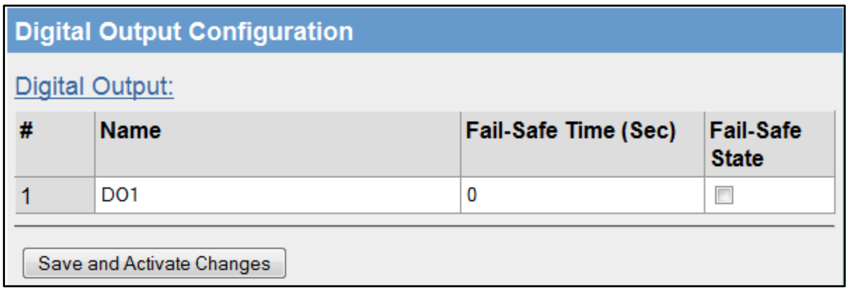
- Windowed – If the analog value is inside the upper and lower setpoints, the setpoint will be active (on, “1”), and if the analog value is outside of these setpoints the setpoint will be reset (off, “0”)

Digital Output

Configuration of the I/O channel as a Digital Output is done by firstly ensuring ‘Digital Input/Output’ is selected in the ‘Onboard I/O Mode Configuration’ Screen as shown in “**Figure 53- Input Mode**” and then activating the changes by pressing the ‘Save and Activate Changes’ button

The default parameters for the digital output should suffice for normal operation however if you wish to configure the output to have a failsafe indication you will need to configure the parameters below.

Digital Output Configuration Parameters



Digital Output Configuration

Digital Output:

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

Figure 55 – Digital Output

Name – A descriptive name can be configured for the Digital Output, up to 30 characters including spaces.

Fail-Safe Time (sec) –The time before the output actives its Failsafe state if it does not receive an update or a COS message from the sending input. If the Fail Safe Timer counts down to zero the output will be set to the ON /OFF Fail Safe state depending on how it is configured. When an update or a COS message is received the Failsafe timer is then restarted.

It is recommend this 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 that the output will be set to if the 'Failsafe Time' countdown has elapsed.

If the Failsafe state is enabled (ticked) the LED and the digital output will be turned ON.

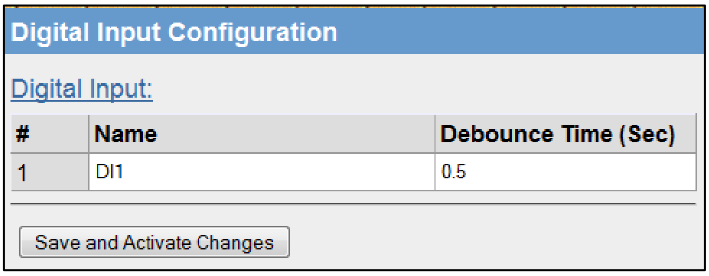
If the Failsafe state is disabled (unticked) the LED and the digital output will be turned OFF.

Digital Input

Configuration of the I/O channel as a Digital Input is done by firstly ensuring 'Digital Input/Output' is selected in the 'Onboard I/O Mode Configuration' Screen as shown in "**Figure 53- Input Mode**" and then activating the changes by pressing the 'Save and Activate Changes' button

If you wish to adjust the digital input parameters see below for details.

Digital Input Configuration Parameters



Digital Input Configuration

Digital Input:

#	Name	Debounce Time (Sec)
1	DI1	0.5

Figure 56 – Digital Input

Name – A descriptive name that can be given to the input to help with configuration, up to 30 characters including spaces or use the default,

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.

I/O Register locations

There are over 5000 x 16bit general purpose registers that are available for Modbus (including the onboard Analog/Digital Input/Output) and are shared with both Modbus Client and Server.

Along with the physical DIO status the internal I/O can be accessed by reading 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 table below. Each register is internally saved as a 16bit 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, i.e. when transferring I/O from one Modbus Slave device to another. Also provided is the status of the onboard digital I/O, as well as the status of the wireless link and any serial or TCP connections.

The different I/O Types and Registers are shown below.

Digital Outputs Coils

Registers	Purpose
0001	Local Digital Output Register
0021 - 0500	I/O Space for locally attached 115S expansion I/O modules. 20 registers per module address. Max 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. 20 registers per module address. Max 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 (8-40VDC)
30021 30493	I/O Space for locally attached 115S expansion I/O modules. 20 registers per module address. Max 24.
30494 - 30500	Internal information registers – Serial Number, Firmware Version and Patch Level.
30501 - 32500	General Purpose Bit Storage – Area assigned in memory Modbus Mapping storage.
38001	Local DIO register (as a Floating Point value)
38003	Local Supply Voltage (8-40VDC) 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 match 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 will need to match.

If more than 3 serial expansion modules are added the “Maximum Units to Poll” on the “Serial” page will also need to be adjusted.

Connect the serial expansion module and take note of the address (Rotary switches on the bottom) as this address will be used as an offset to locate the I/O within the 450U-E.

Make sure the devices at either end of the RS485 cable have the termination switch enabled (on), this includes the 450U-E. Failure to terminate the RS485 correctly could result in the modules not operating correctly.

115S Expansion I/O Memory Map

I/O 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” which applies to the location of all 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.

E.g. 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)

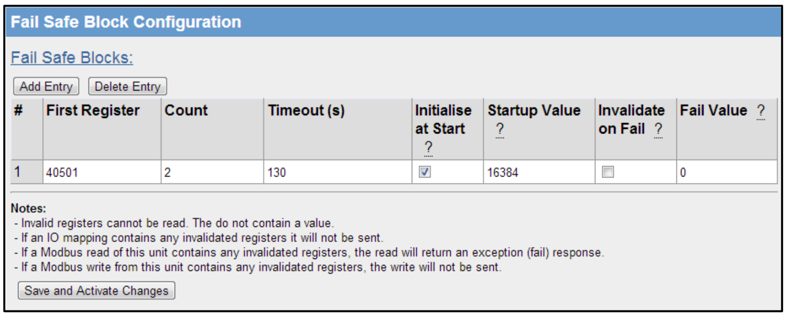
See Appendix C - “Expansion I/O Registers” for a more detailed address map of the serial expansion I/O modules.

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

- The first is a ‘Communication Fail’ which is located at register location 10019 + offset value. This register will indicate “1”when the module is in failure.
- The second is a ‘Communication OK’ which is located at register location 10020 + offset value. This register will indicate “1”when the module is communicating OK.

Failsafe Blocks

Fail Safe Block configuration allows the internal registers to be set to a pre-configured value on start-up as well as configuring the DIO to reset to a predefined value after a timeout period has elapsed. Also 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.



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 57 - Failsafe Block Analog

In the screenshot above, register 40501 holds an analog value that is being updated from another module every 60 seconds.

The module is configured so that on start-up a value 16384 will be written into register 40501 and then start counting down the “Timeout” period , in this case it is 130 seconds which is a little over two times the 1 minute update period from the sending module. If after 130 seconds, 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).

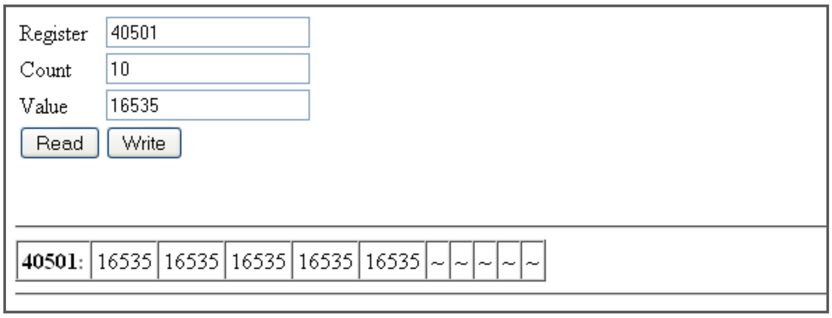
If the “Invalidate on Fail” were ticked, the value would be set to a null or invalidated value (~). See “Invalid Register State” below.

If this register happens to be mapped to another module and the state is ‘Invalidated’ the mapping will be inhibited from sending until the” Invalid” value has been updated with a real value.

Also if the register is being read by a Modbus Master or Client an exception response will be returned as 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 you can have is 50.

Registers	Purpose
First Register	First local register were the Failsafe block will start from.
Count	Number of registers to incorporate in the Failsafe block
Timeout	Time allocated to the failsafe block before triggering a failsafe state.
Initialise at Startup	Initialise the value on startup (if un ticked the register will be uninitialized (~))
Startup Value	Value to Initialise the register to on startup of the module.
Invalidate on Fail	Register will be invalidated on failure
Fail Value	Value to set the Register when a fail occurs

“Invalid” register state



Register 40501

Count 10

Value 16535

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

Figure 58 - Invalid Register State

All registers within the module can have various states depending on what type of register it is and what sort of value it holds, a typical analog range is between 0 and 65535 and a digital can be 0 or 1.

Registers can also have another state which we call “invalid”, this state means that the value has not been written to and so does not hold a value but more a non-value or null.

If you were to read the registers using the “I/O Diagnostics” an invalid register would read as a “~“shown above.

⚠ **Any mapping with an invalid register will be inhibited from sending. This is to ensure the data that gets to the destination is valid and not just default values that the module starts up with.**

3.17 Configuration Examples

Extending a wired network (Bridged Network)

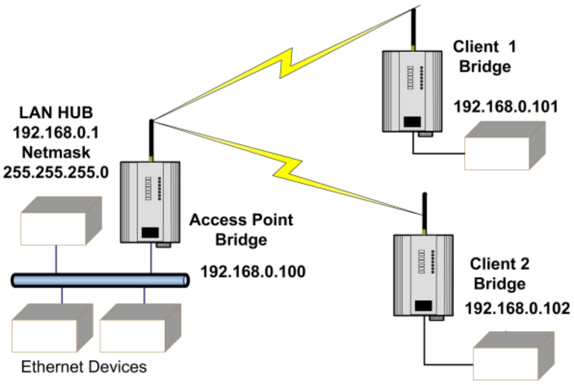


Figure 59 - Example Config 1

Access Point Configuration

Connect straight through Ethernet cable between PC and 450U-E.

Ensure configuration PC and 450U-E are setup to communicate on the same network

Set dipswitch to SETUP mode.

Power up unit, and wait for the OK LED to cease flashing.

Adjust PC network settings

Set Configuration PC network card with network setting of IP address 192.168.0.1, Netmask 255.255.255.0

Open configuration webpage with Internet Explorer at address 192.168.0.1XX/ where XX is the last two digits of the module’s serial number

When prompted for password, enter default username “user” and password “user”

From the main home screen you will need to select the “Quickstart” Configuration option on the right hand side of the screen.

On this screen select the Transmit Power level, Transmit Data Rate, Frequency Step size and Transmit & Receive Frequencies under “Radio “heading. Record these settings as they will need to be the same for all radios in the example.

Select Operating Mode as Access Point.

Enter a System Address (ESSID) string. And record as this will need to be exactly the same for all radios in the example.

The Radio Encryption is configured for WPA2 AES and will require an encryption key which will also need to be the same on all radios in the example.

Change the IP addresses to 192.168.0.100

Leave the Subnet masks at the default 255.255.255.0

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

Set dipswitch to RUN

Save the changes and unit will restart with new settings.

Client 1 Configuration

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

When complete, set the dipswitch back to RUN and press “Save Changes and Reset”.

Client 2 Configuration

As for Client1 above, however set the IP address as 192.168.0.102

When complete, set the dipswitch back to RUN and press “Save Changes and Reset”.

Connecting two different networks together (Routed Network)

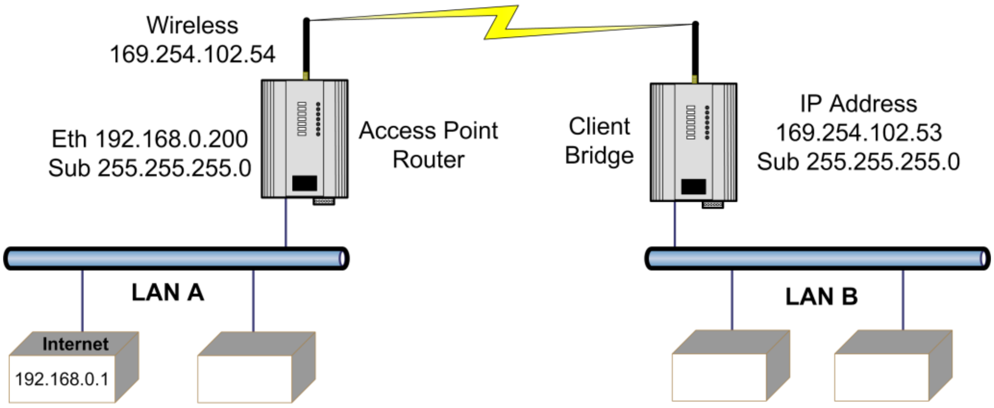


Figure 60 - Example Config 2

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, i.e.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 PCs, this may be achieved with the MS-DOS command ROUTE. For example2 this 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 4.11 “Utilities”

LAN B Configuration

All devices on LAN B should be configured so their Gateway IP addresses are configured with the IP address 169.254.102.54 which is the 450U-E Access Point/Router.

Access Point Configuration

Connect straight through Ethernet cable between the PC and the 450U-E.

Ensure configuration PC and 450U-E are setup to communicate on the same network

Set dipswitch to SETUP

Power up unit, and wait for OK led to cease flashing.

Adjust PC network settings

Set Configuration PC network card with network setting of IP address 192.168.0.2, Netmask 255.255.255.0

Open configuration webpage with Internet Explorer at address 192.168.0.1XX where XX is the last two digits of the module's serial number

When prompted for password, enter default username "user" and password "user"

From the main home screen you will need to select the "Quickstart" Configuration option on the right hand side of the screen.

On this screen select the Transmit Power level, Transmit Data Rate, Frequency Step size and Transmit & Receive Frequencies under "Radio "heading. Record these settings as they will need to be the same for all radios in the example.

Select Operating Mode as Access Point.

Enter a System Address (ESSID) string. And record as this will need to be exactly the same for all radios in the example.

The Radio Encryption is configured for WPA2 AES and will require an encryption key which will also need to be the same on all radios in the example.

Change the IP addresses to 192.168.0.200

Leave the Subnet masks at the default 255.255.255.0

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

Press the "Save changes" button instead of the "Save Changes and Reset" as we need to make some other changes to the configuration before resetting the module.

Select the "Network menu" and change the "Device Mode" from Bridge to Router.

This will then display separate IP address fields for Ethernet and Wireless.

As the Access Point is now configured as a Router it will route the IP traffic from one network to another.

Change the Wireless IP address to the 169.254.102.54 which is the IP address on the Wireless network.

Set dipswitch back to RUN and press "Save Changes and Reset".

Client Configuration

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

When complete, set the dipswitch back to RUN and press "Save Changes and Reset".

Extending range of a network with a Repeater hop

Configure units as described in the "Extending a wired network" example above. Place the Access Point at the remote intermediate repeater location. Additional repeaters can be added using Wireless Distribution System (WDS) – refer section 3.12 "Repeaters (WDS)"Repeaters (WDS)" for further details.

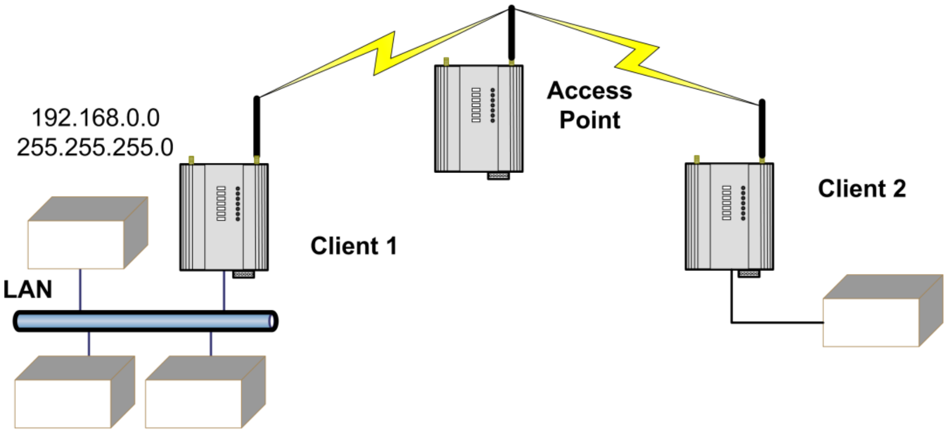


Figure 61 - Example Repeaters

CHAPTER 4 - DIAGNOSTICS

4.0 Diagnostics Chart

LED Indicator	Condition	Meaning
OK	GREEN	Normal Operation
OK	RED Solid	Factory Default Mode, Supply voltage low or Internal Module Fault
OK	RED At Power On	Boot Loader delay at start-up
OK	Fast Flash RED / GREEN	Module Boot Sequence
OK	Slow Flash RED / GREEN	Module Boot Sequence
Radio RX	GREEN flash	Radio receiving data
Radio RX	RED flash	Radio receiving data (-XXdB indicates a low signal strength)
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 OFF and Input is open circuit.
I/O	GREEN varying intensity	Analog input current in circuit (Dim =4mA, bright=20mA)

The green OK LED on the front panel indicates correct operation of the unit. This LED turns red for a number of reasons, i.e. module has been reset to Factory default and will remain on until the module has been configured and reset. Also if the module has a processor fault or the supply voltage is low.
When the OK LED turns red shutdown state is indicated. On processor failure, or on 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 Start-up

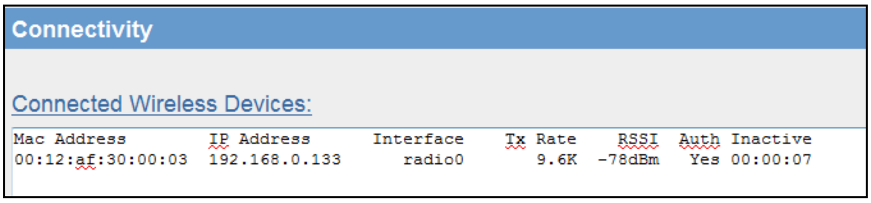
The OK LED indicates the status of the module during the boot up process. At power on, the OK LED comes on RED. During kernel boot the OK LED flashes Red-Green at a 1Hz rate (½ second red, ½ second green). During module initialisation, the OK LED flashes Red-Green at 0.5Hz rate (1-second red, 1-second green). When initialisation is complete, the OK LED switches to green continuously.

If the OK LED remains red at power on, this could indicate either low supply voltage (The module will not attempt to boot until supply voltage is within range); Module fault; or module is in Factory Default mode.

4.1 Connectivity

The Connectivity webpage displays connection information and available devices on the network. The "Connected Devices" will display the MAC address, data rate, received signal strength (RSSI), authentication status and the inactive time for each Client connected to the Access Point. The readings shown are based upon the last received data message from the Access Point or Client. Client stations also display a list of detected Access points (Site Survey), including network name (SSID), channel and maximum data rate.

⚠ **Note: When updating the Connectivity webpage, it is necessary to hold down the <ctrl> key while pressing the refresh button to ensure the most up to date information is displayed.**



```
Mac Address          IP Address        Interface     Tx Rate     RSSI  Auth Inactive
00:12:af:30:00:03    192.168.0.133        radio0        9.6K   -78dBm   Yes 00:00:07
```

Figure 62 - Connected Devices

Connectivity Parameters

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.

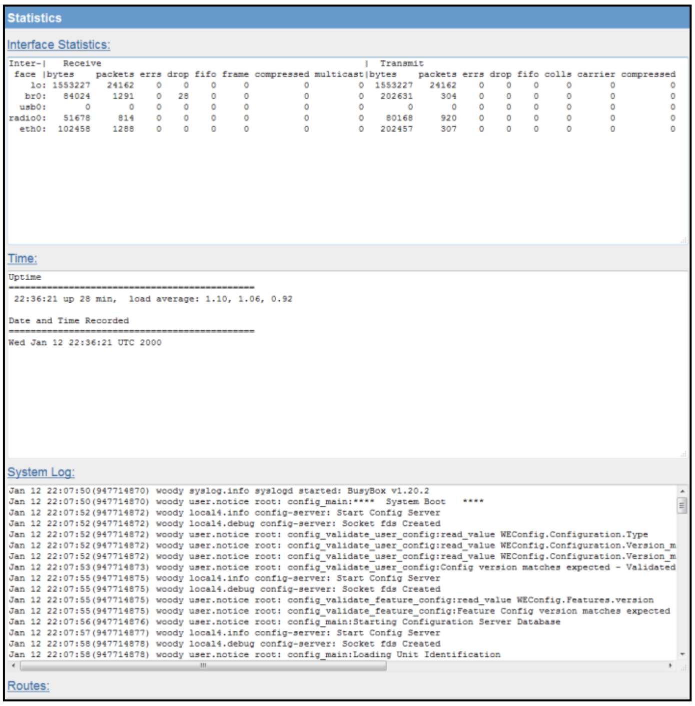
RATE Radio Data Rate:

RSSI The radio receive signal strength

Auth Shows if 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.

Inactive Shows the last time data is received from the device.

4.2 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
```

```
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
```

```
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
```

Figure 63 - Statistics

The Statistics webpage is used for advanced debugging of 450U-E. This webpage details the state of the 450U-E and performance information. This page is typically useful to ELPRO technical support personnel in diagnosing problems with the module.

⚠ **Note: When updating the Connectivity webpage, it is necessary to hold down the <ctrl> key while pressing the refresh button to ensure the most up to date information is displayed.**

The Statistics Page is used for gathering information about how the module is connected and communicating. It is comprised of a number of dynamic list boxes with each showing particular statistics about its function.

Interface Statistics: will show the number of bytes transmitted and received as well as the number of CRC errors, dropped packets, fifo alarms and the different types of frames (fragmented, compressed or multicast).

The "Interface Statistics" is the main area for gathering diagnostics information as this will indicate how the Radios are communicating.

Time: shows the amount of time the module has been running since its last reset.

System Log: shows a running log of information about how the modules operating system is running. This log will also log any errors and resets.

Routes: will display the current IP routes configured in the module.

IP statistics: show a number 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 will analyse 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, a better idea of regular traffic can be discovered.

Network Analysis programs make configuration of a filter for the 450U-E a simple task.

4.3 Channel Survey (Utilisation)

Channel Utilisation gives a visual display of how busy the current radio channel is over a given time period.

Channel Utilisation is logged by the radio over three separate time intervals: 1 Second which will cover the last 60 seconds; 1 Minute which covers the last 60 minutes; and 1 Hour 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 Utilisation allows us to see how much RF activity is on a given channel as a percentage of the total utilisation. A channel that is very busy will have high channel utilisation (usually 50% or greater). Conversely a channel that is quiet will have low channel utilisation.

Channel Survey and Custom Survey can therefore be valuable tools to use when performing site surveys in order to determine the best RF channel to use. It is also a valuable diagnostics tool for identifying the spare capacity on a given channel, as well as possible sources of interference.

Channel Utilisation on a Live System:

Channel Utilisation can be used on a live system to get an indication of how much spare capacity the channel has for additional data transfer. To identify possible interference on the current channel, observe the "All RX Frames" on the Custom Survey page. If possible, temporarily disable all data transfer on the system, and if the Channel Utilisation remains high this will confirm the presence of outside interference.

Diagnosing Low Throughput:

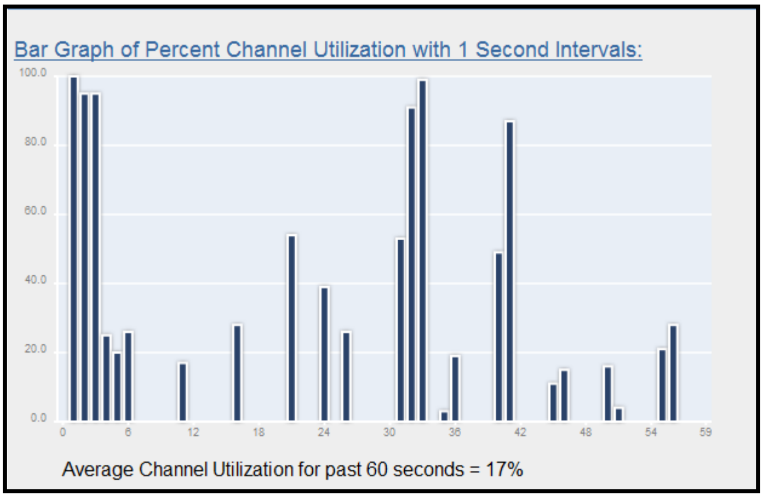
If normal communications between modems is poor, Channel Utilisation can be used to confirm whether or not the poor results were due to interference. If the Channel Utilisation is seen to be high, then this will confirm that poor throughput was due to other RF interference. Alternatively if the Channel Utilisation is seen to be low (indicating little interference), then the poor throughput would more likely be attributed to poor RSSI - which could be confirmed on the "Connectivity" page.

Channel Utilisation Graphs:

Channel Survey screen displays a graph showing the percentage of time that a channel is being utilised by any of the following causes:

1. The connected modem is transmitting.
2. The connected modem is receiving valid data from other modems.
3. The connected modem has detected RF noise or interference from some other source.

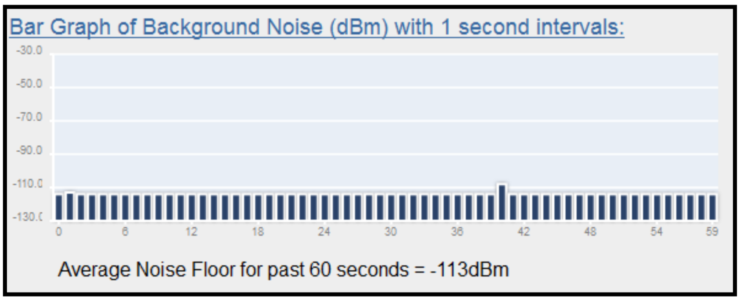
Channel Survey shows the Channel Utilisation and Noise Floor Graph with 1 second, 1 minute and 1 hour periods.


Bar Graph of Percent Channel Utilization with 1 Second Intervals:

Average Channel Utilization for past 60 seconds = 17%

Figure 64 - Channel Utilization Seconds

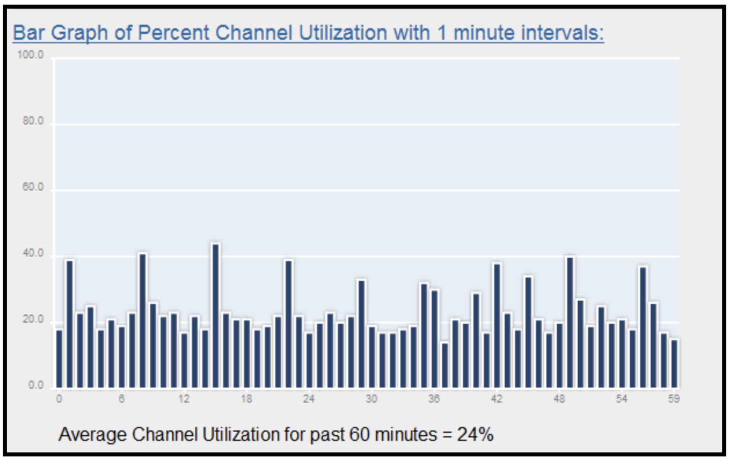
The first screen shows a percent of the overall radio traffic on the channel that is currently being used.


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

Average Noise Floor for past 60 seconds = -113dBm

Figure 65 – Background Noise (Sec)

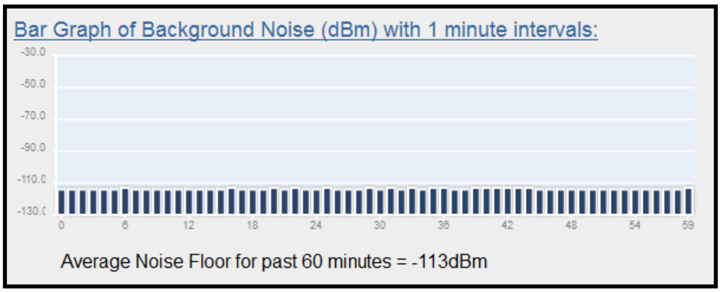
The next screen shot shows the radio background noise level for the last 60 seconds.



Average Channel Utilization for past 60 minutes = 24%

Figure 66 - Channel Utilisation Minutes

The third screen shot shows the average Channel utilisation for each minute up to one hour. It will also give a running average for the total number of minutes up to 59 minutes.



Average Noise Floor for past 60 minutes = -113dBm

Figure 67 - Background Noise Minutes

The next screen shot shows the running radio background average noise level for each minute up to 59 minutes.

The Channel Survey page also shows two other screen shots (not shown here) which indicate the Percent Channel Utilisation and Noise Floor in one hour intervals. The screens will only show the last 60 hour period.

4.4 Custom Survey

Custom Survey is made up of two separate charts that can be configured to display different radio channel characteristics over three different time scales (Seconds, Minutes or Hours).

The custom survey is essentially the same as the channel survey (explained in the previous section) except it allows different channel related data to be displayed which is useful for diagnosing channel utilisations problems.

The default selection on the custom page will display 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 we can determine if there are too many transmissions being sent from this radio or if there is too much radio messages being received from other sites in the radio network.

To display different data select the appropriate parameter from the drop down list and press “Save Changes” button to refresh the chart.

As there are two separate charts different data values can be displayed and compared at the same time.

The data components available for graphing are displayed in the following table:

Custom data	**Percentage of channel utilisation over the configured time period**
All TX & RX Frames	All transmissions sent and received by the radio being monitored. This option is the same as the normal channel survey which is explained in the previous section.
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 utilisation into transmissions from the radio in question or transmissions from other radios. This option encompasses TX first

attempt, TX retries and TX Ack messages from below.

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
The amount of time spent transmitting first attempt messages from the modem. This option and the following two are useful for breaking down the amount of time that is spent transmitting messages into normal transmissions, retries and acknowledgements.

TX Retries
The percentage of time spent transmitting retry messages from the modem.

TX Acknowledge messages
The percentage of time spent transmitting acknowledgment messages from the modem and Broadcast messages.

Radio Hold off
The percentage of time that the radio has spent holding off from transmitting data, possibly because the channel is busy.

RX to this radio
The percentage of time receiving messages specifically for the radio being monitored, i.e. valid Elpro radio communication frames from other modems in the system that are specifically addressed to this modem.

RX to other radios
The percentage of time receiving valid Elpro messages addressed to other radios within the system.

RX acknowledgements
The percentage of time receiving acknowledge messages

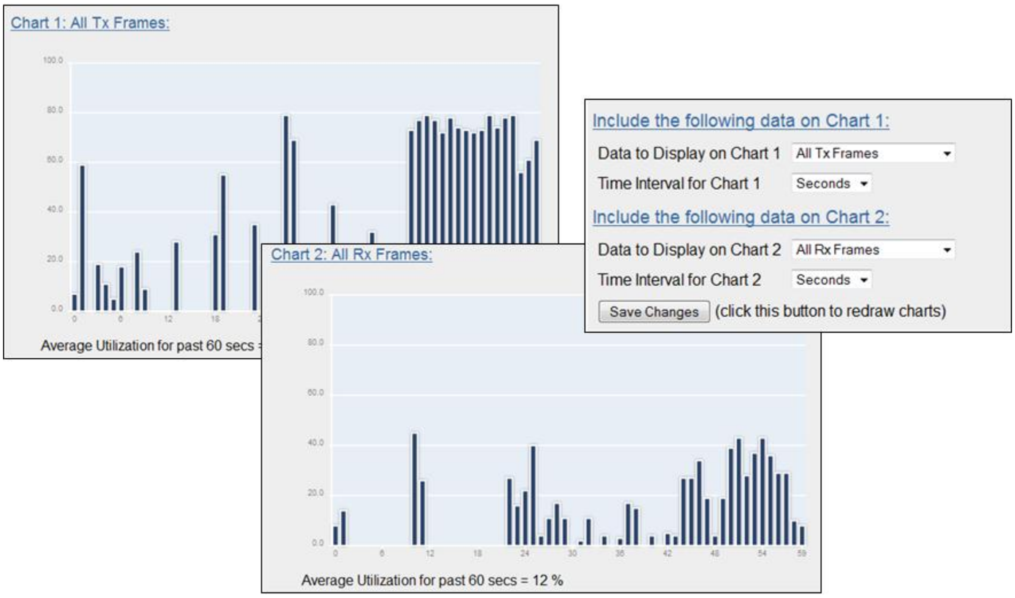
RX Errors
The percentage of time dealing with Elpro radio receive error messages, i.e. corrupted data, Data Collisions, etc.

By configuring the different chart options from above we can get a clear idea of the percentage of time spent handling transmit and receive messages and/or the amount of other receive data that can be heard at the radio.

Configure what is to be logged from the drop down list, select a time interval, press "Save Changes" and the charts will then redraw the graphs and display below the settings. Each graph will display a percent channel utilisation using the selected criteria and time interval (Seconds, Minutes or Hours).

Example One.

Chart one show all transmit data frames over the radio link and chart two shows Rx valid Elpro data frames being received from any sources (Any Elpro 450U-E data frames). We can see from this that there is a large amount of Transmit data being sent toward the end of the chart and the receive data in chart two also shows an increase in traffic. From this we can deduce that the radio itself or a device on the Ethernet network it transmitting large amounts of data.



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 68 - Custom Survey 1

Example Two.

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

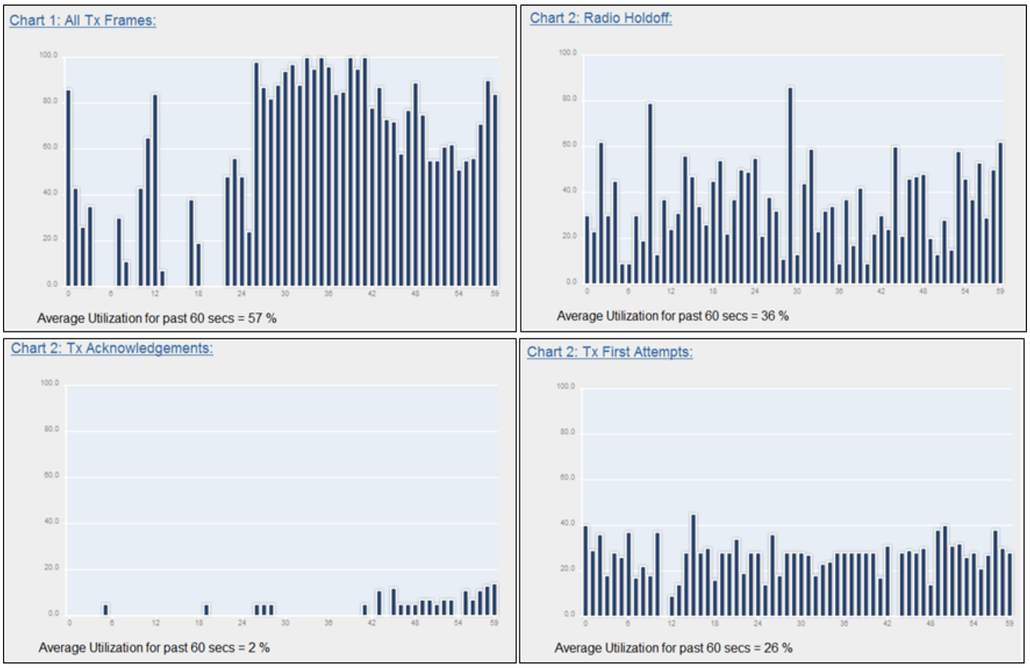
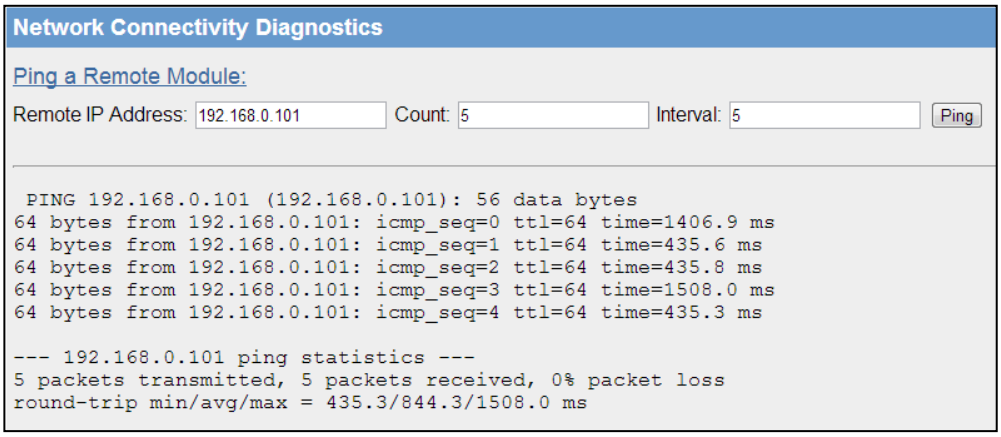


Figure 69 - Custom Survey 2

4.5 Network Diagnostics



Remote IP Address: 192.168.0.101 Count: 5 Interval: 5

```
 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 70– Network Diagnostics

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

Ping

Ping is a standard Network instruction that sends out a small data probe to the IP address configured letting you know if you have a communication path or not.

You will receive a response for each Ping, which will show a packet size, IP Address, Sequence number and a time in milliseconds.

Followed by a summary showing the number of packets transmitted, the number of packets received, any lost packets and the Minimum, Average and Maximum Ping times in milliseconds.

A Ping can be done on either the Radio Network or Ethernet Network. The ping command will automatically select the correct network interface according to the address selected.

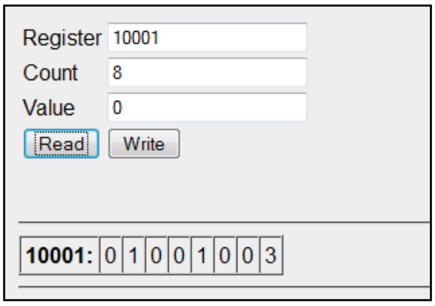
Remote IP Address – This is the IP address that you want to Ping

Count / Max Hops – This is the 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 generally will not need to be changed unless using repeaters.

When pinging on the radio network, the response time for the first ping will be longer if the device needs to establish a network route to the destination.

4.6 IO Diagnostics



Register 10001

Count 8

Value 0

10001: 0 1 0 0 1 0 0 3

Figure 71 - I/O Diagnostics

Selecting this option from the main screen will allow some basic reading and writing of the I/O store registers within the module.

To read a register location, enter an address location, e.g. 10001-12500 (for digital Inputs), enter a count (number of consecutive registers) and then press the "Read" button

Below the buttons, you will see the returned address location and the returned values

To "Write" to an Output register location, E.g. 1-2500, enter the address location, count, and value and then press the "Write" button.

E.g. 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, e.g. 30001-32500 enter a count (number of consecutive registers) and then press the "Read" button

⚠ Note: If when reading a register and getting the symbol **"**~**"**this indicates that the register **is in an invalid state and has no value (not even zero). see 3.16** "Invalid Register State**" for more details on Invalid register states**.

Using the I/O Diagnostics enables you to check the register locations for invalid states "~", read Digital or Analog input states and even write values to internal register or the DIO if required. If when reading the Status of the DIO on the module you see the value "3", this indicates that the DIO is being used as an output in the "ON" state.

Modem Module Information Registers

There are registers available in the module that show a number of the modules characteristics, i.e. Serial Number, Firmware version, etc.

This information is available on the main Web page of the module however 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 & 30496 = Module Serial number

Register 30497, 30498 & 30499 = Module Firmware version

Register 30500 = Firmware patch level.

Expansion I/O Error Registers

The 450U-E has a number of diagnostics registers that are allocated for each Expansion I/O module that will indicate the module type, error counts, error codes, etc.

Each Expansion I/O module has the following registers.

- 30017 + Offset = Modbus Error Counter (number of errors the modules has had)
- 30018 + Offset = Last 115S Status Code / Modbus Error Code that the module has had.
- 30019 + Offset = Modbus Lost Link Counter (number of Communication Errors)
- 30020 + Offset = Modbus 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

The "Offset" can be calculated by reading the Modbus address of the 115S and multiply this by the 20

E.g. If connecting a 115S-11 (16 x DIO) with address #2

Modbus Error Counter will be at register location 30017 + (2*20) = 30057

Last 115S Status Code will be at register location 30018 + (2*20) = 30058

Modbus Lost Link Counter will be at register location 30019 + (2*20) = 30059

Modbus Module Type will be at register location 30020 + (2*20) = 30060

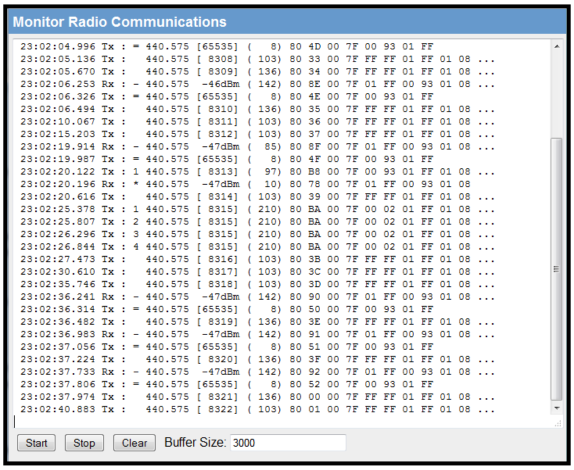
These Expansion I/O Error registers display the following 115S Status Codes (Hex code 0001-0005 & 0129), as well as displaying the standard Modbus Response Codes shown in Appendix D - "Modbus Error Codes" with a slight variance in the code. The Most significant Byte (MSB) of the Word will be one of the following bytes, 82, 84, 8F or 90 followed by the standard Modbus Response codes (01 -0B).

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 RS485 traffic.
5	0x0005	Message type did not match request.	The response heard did not match the requested poll, i.e. different command response, possibly heard other RS485 traffic.
81	0x0129	Problem accessing local memory	Could not access register location, possibly because the register is not initialised.
	0x??01-0x??0B	Standard Modbus Error Codes	As per Appendix D - "Modbus Error Codes"

4.7 Monitor Radio Comms

The Monitor Radio Comms page shows radio communication frames that are received or transmitted by the radio.

⚠ **Note: Comms log will display Elpro 450U-E data frames only.**



Monitor Radio Communications

```
23:02:04.996 Tx : = 440.575 [65535] (   8) 80 4D 00 7F 00 93 01 FF
23:02:05.136 Tx :   440.575 [ 8308] ( 103) 80 33 00 7F FF FF 01 FF 01 08 ...
23:02:05.670 Tx :   440.575 [ 8309] ( 136) 80 34 00 7F FF FF 01 FF 01 08 ...
23:02:06.253 Rx : - 440.575  -46dBm ( 142) 80 8E 00 7F 01 FF 00 93 01 08 ...
23:02:06.326 Tx : = 440.575 [65535] (   8) 80 4E 00 7F 00 93 01 FF
23:02:06.494 Tx :   440.575 [ 8310] ( 136) 80 35 00 7F FF FF 01 FF 01 08 ...
23:02:10.067 Tx :   440.575 [ 8311] ( 103) 80 36 00 7F FF FF 01 FF 01 08 ...
23:02:15.203 Tx :   440.575 [ 8312] ( 103) 80 37 00 7F FF FF 01 FF 01 08 ...
23:02:19.914 Rx : - 440.575  -47dBm (  85) 80 8F 00 7F 01 FF 00 93 01 08 ...
23:02:19.987 Tx : = 440.575 [65535] (   8) 80 4F 00 7F 00 93 01 FF
23:02:20.122 Tx : 1 440.575 [ 8313] (  97) 80 B8 00 7F 00 93 01 FF 01 08 ...
23:02:20.196 Rx : * 440.575  -47dBm (  10) 80 78 00 7F 01 FF 00 93 01 08
23:02:20.616 Tx :   440.575 [ 8314] ( 103) 80 39 00 7F FF FF 01 FF 01 08 ...
23:02:25.378 Tx : 1 440.575 [ 8315] ( 210) 80 BA 00 7F 00 02 01 FF 01 08 ...
23:02:25.807 Tx : 2 440.575 [ 8315] ( 210) 80 BA 00 7F 00 02 01 FF 01 08 ...
23:02:26.296 Tx : 3 440.575 [ 8315] ( 210) 80 BA 00 7F 00 02 01 FF 01 08 ...
23:02:26.844 Tx : 4 440.575 [ 8315] ( 210) 80 BA 00 7F 00 02 01 FF 01 08 ...
23:02:27.473 Tx :   440.575 [ 8316] ( 103) 80 3B 00 7F FF FF 01 FF 01 08 ...
23:02:30.610 Tx :   440.575 [ 8317] ( 103) 80 3C 00 7F FF FF 01 FF 01 08 ...
23:02:35.746 Tx :   440.575 [ 8318] ( 103) 80 3D 00 7F FF FF 01 FF 01 08 ...
23:02:36.241 Rx : - 440.575  -47dBm ( 142) 80 90 00 7F 01 FF 00 93 01 08 ...
23:02:36.314 Tx : = 440.575 [65535] (   8) 80 50 00 7F 00 93 01 FF
23:02:36.482 Tx :   440.575 [ 8319] ( 136) 80 3E 00 7F FF FF 01 FF 01 08 ...
23:02:36.983 Rx : - 440.575  -47dBm ( 142) 80 91 00 7F 01 FF 00 93 01 08 ...
23:02:37.056 Tx : = 440.575 [65535] (   8) 80 51 00 7F 00 93 01 FF
23:02:37.224 Tx :   440.575 [ 8320] ( 136) 80 3F 00 7F FF FF 01 FF 01 08 ...
23:02:37.733 Rx : - 440.575  -47dBm ( 142) 80 92 00 7F 01 FF 00 93 01 08 ...
23:02:37.806 Tx : = 440.575 [65535] (   8) 80 52 00 7F 00 93 01 FF
23:02:37.974 Tx :   440.575 [ 8321] ( 136) 80 00 00 7F FF FF 01 FF 01 08 ...
23:02:40.883 Tx :   440.575 [ 8322] ( 103) 80 01 00 7F FF FF 01 FF 01 08 ...
```

Buffer Size: 3000

Figure 72 - Monitor Comms

Figure 72 - Monitor Comms above shows typical data frames from the communication log screen.

Below is a table explaining each of the fields within the data frame.

Corrupted data frames are shown with an "ERROR!" in the frame.

Time Message Time Stamp – Time from when module was last started

Message Type Displays if message is a Transmit (Tx) or a Receive (Rx) Ethernet frame

Frame designator RX "**blank**" Indicates a Received packet is a broadcast packet, no acknowledgement is required.

RX "-" Indicates Received packet requires a message acknowledgement

RX "*****" Indicates Acknowledgement of a previous transmitted packet from this radio.

TX "**1,2,3,4**" Indicates the number of times the packet has been transmitted, i.e. reties

TX "**=**" Indicates the Transmitted packet is the acknowledgement of a previous received frame.

TX "**blank**" Indicates the transmitted packet is a broadcast packet, no acknowledgement required.

Frequency Shows the Frequency of the RX/TX frame

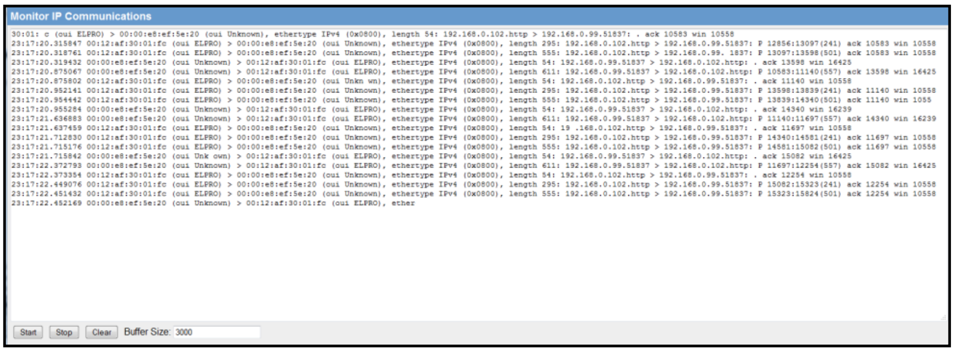
Signal /Seq Number Shows the Receive Signal Level on any received message or an internal sequence number for the transmitted message.

Data Length Total length of the transmitted or received message

Data Data packet

4.8 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 some other IP Comms data. More information on standard IP Comms can be found on the internet.



Monitor IP Communications

```
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 73 – Monitor IP Comms

4.9 System Tools

The System Tools Page has a number of tools that help maintain the module firmware and configuration.

System Log File Shows an event log of the modules operation, used for diagnosing problems. Page can be saved and emailed to ELPRO if requested. “Clear System Log” will clear out the log file and start fresh.

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

Write Configuration File Any configuration XML files saved using the “Read Configuration” above can be loaded back into the module

Firmware Upgrade This option is used for Patch firmware upgrades only. See Appendix A - for full upgrade procedure. Load the file using the “Browse” button and when found press “Send” which will load the file into the module. When completed press “Reset” Firmware upgrade can be done locally or remotely via the radio.

Reset Resets the module

Factory Default Configuration Loads the Factory default configuration and resets. CAUTION – Doing this will overwrite any current configuration

Setting a 450U-E to Factory Default Settings

- Access the configuration webpages on the 450U-E. Refer section”3.2 ”Initial Connection”.
- Click on the menu item “System Tools” from the main menu.
- Click on “Factory Default Configuration Reset” button, and wait for unit to reset. While the module executes the reset sequence the OK LED will flash. The OK LED will turn green when the reset sequence is complete.
- When complete you should be able connect to the modules default IP address which will be displayed on the label on the bottom of the module.

4.10 Module Information Configuration

Module Information Webpage Fields

This configuration page is primarily for information purposes. With the exception of the password, the information entered here is displayed on the home configuration webpage of the 450U-E.

Username Configuration of Username. This is the username used to access the configuration on the 450U-E. Take care to remember this username if you change it as it will be needed to access the 450U-E in future.

Password Configuration of Password. This is the password used to access the configuration on the 450U-E. Take care to remember this password if you change it as it will be needed to access the module in future.

Device Name A text field if you wish to label the particular 450U-E. This is also the DNS name (hostname) of the device if you are using DNS.

Owner A text field for owner name.

Contact A text field for owner phone number, email address etc.

Description A text field used for a description of the purpose of the unit.

Location A text field used to describe the location of the 450U-E.

Configuration Version A text field used to enter in a version for the configuration

DHCP Client Configuration

DHCP (Dynamic Host Configuration Protocol) allows DHCP Clients to automatically obtain their IP Address at start-up. This simplifies network administration, as 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, check the box “Obtain IP Address Automatically” on the Network Configuration page.

When configured as a DHCP Client the “Device Name” on the Module Information page will be the module identifier (as the IP address will be unknown) and so should be given a unique name.

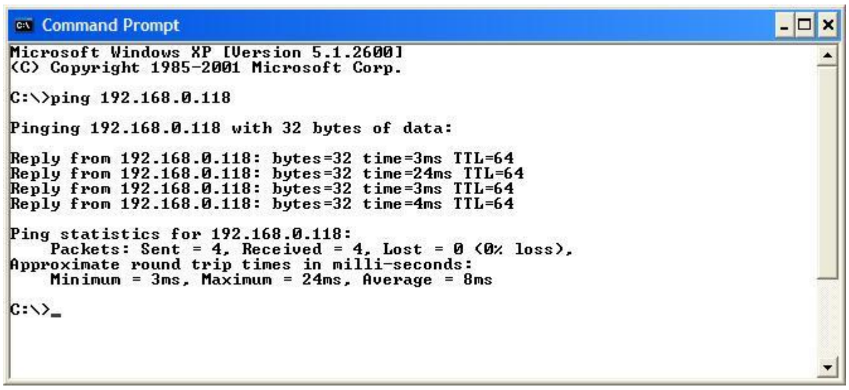
4.11 Utilities

"Ping"

Ping 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 you are trying to reach is actually operating. If, for example, a user can't ping a host, then 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.

Click on the Start Menu and select Run. Type in "cmd" and enter, you should then see the command screen come up. There will be a certain directory specified (unique to your own PC) with a flashing cursor at the end. At the cursor type the word "ping" leaving a space and the default IP address for the 450U-E at first start-up.

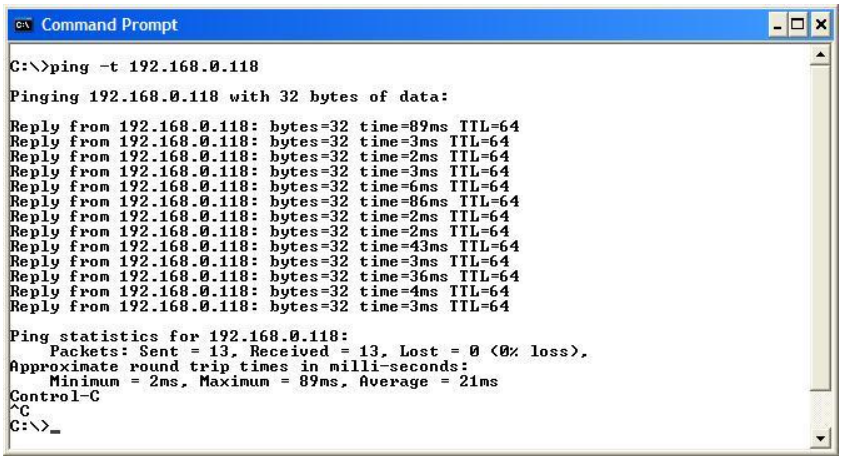
This command would be written as "ping 192.168.0.118" then <enter> to send the ping command. The PC will reply with an acknowledgement of your command and if your 450U-E is correctly configured the reply will look something like this.



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

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=3ms TTL=64
Reply from 192.168.0.118: bytes=32 time=24ms TTL=64
Reply from 192.168.0.118: bytes=32 time=3ms TTL=64
Reply from 192.168.0.118: bytes=32 time=4ms 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 = 3ms, Maximum = 24ms, Average = 8ms

C:\>_
```

Figure 74 - Ping

The screen shot below 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=89ms TTL=64
Reply from 192.168.0.118: bytes=32 time=3ms TTL=64
Reply from 192.168.0.118: bytes=32 time=2ms TTL=64
Reply from 192.168.0.118: bytes=32 time=3ms TTL=64
Reply from 192.168.0.118: bytes=32 time=6ms TTL=64
Reply from 192.168.0.118: bytes=32 time=86ms TTL=64
Reply from 192.168.0.118: bytes=32 time=2ms TTL=64
Reply from 192.168.0.118: bytes=32 time=2ms TTL=64
Reply from 192.168.0.118: bytes=32 time=43ms TTL=64
Reply from 192.168.0.118: bytes=32 time=3ms TTL=64
Reply from 192.168.0.118: bytes=32 time=36ms TTL=64
Reply from 192.168.0.118: bytes=32 time=4ms TTL=64
Reply from 192.168.0.118: bytes=32 time=3ms TTL=64

Ping statistics for 192.168.0.118:
    Packets: Sent = 13, Received = 13, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 89ms, Average = 21ms
Control-C
^C
C:\>_
```

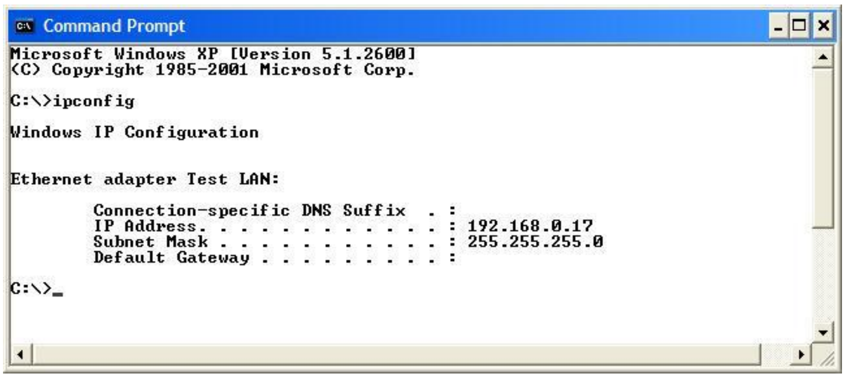
Figure 75 - Ping-t

This –t command is used to repeatedly ping the specified node in the network, to cancel use "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”

“ipconfig” 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  . :
        IP Address. . . . . . . . . . . . : 192.168.0.17
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . :

C:\>_
```

Figure 76 - Ipconfig

In the above example ipconfig was entered in the command prompt. The reply back shows the PC’s IP address, Subnet mask and the gateway it is connected to.

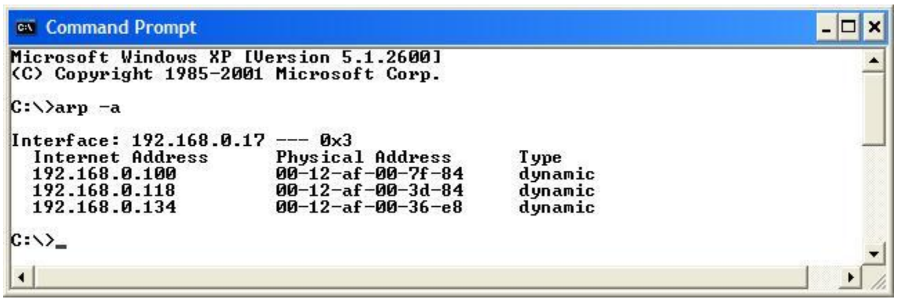
Other ipconfig commands will return back more information. The hardware or MAC address of the computer may be discovered using the command ipconfig /all.

Ipconfig /? Lists all of the commands and their usages available for use.

“Arp”

Displays and modifies the IP-to-Physical address translation tables used by Address Resolution Protocol (ARP).

Once a remote computer has been pinged, this can be used to see the IP address & MAC address of the remote computer. It will also show any other devices on the network that it may be connected to.



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

C:\>arp -a

Interface: 192.168.0.17 --- 0x3
  Internet Address      Physical Address      Type
  192.168.0.100         00-12-af-00-7f-84     dynamic
  192.168.0.118         00-12-af-00-3d-84     dynamic
  192.168.0.134         00-12-af-00-36-e8     dynamic

C:\>_
```

Figure 77 - Arp

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 its associated MAC address of any another device that has a connection to it.

“Arp –?” Lists the commands available for this function.

”Route”

Route is used when joining two or more different networks together via the 450U-E. Refer to Section 1.1 for more details.

When routing from one subnet to another devices on one subnet need to know where to pass the message to get it to the other subnet. This is done one of two ways;

- Setting up a route within the device which is a lookup table showing a list of subnets and which 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; essentially it’s a fallback address where if it 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 as you can only have one Gateway Address.

In the example below a routing rule needs to be entered into Network A’s PC to will allow access between Network A and Network B. The default Gateway address is not used as the Pc has other network adaptors This is can be entered at the command prompt as instructed.

Route PRINT will show all active routes on PC,

Route ADD will add a routing table to network,

Route DELETE <***Destination Netmask Gateway Interface>*** will delete the unwanted routing table

Route CHANGE modifies an existing route.

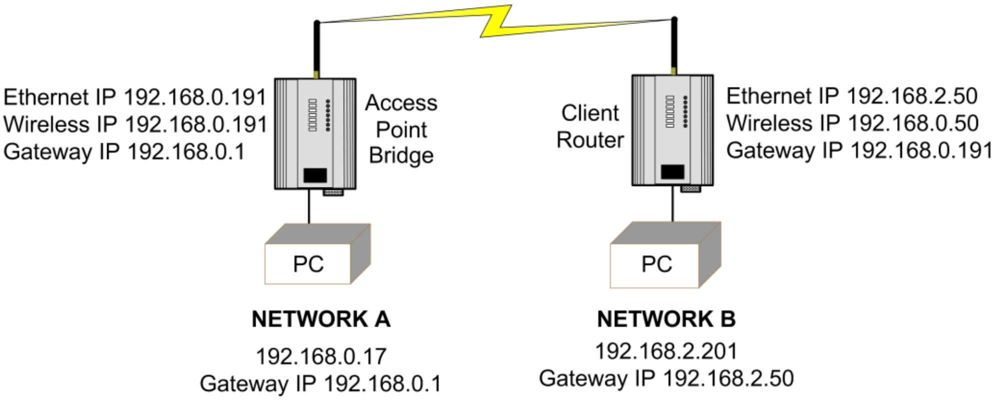


Figure 78 - Route

An example of a routing table is shown for the configuration below,

Network A	Access Point Bridge	Client Router	Network B
IP Address 192.168.0.17	IP Address 192.168.0.191	Ethernet IP 192.168.2.50	Ethernet IP 192.168.2.201
Netmask 255.255.255.0	Netmask 255.255.255.0	Netmask 255.255.255.0	Netmask 255.255.255.0
Gateway IP 192.168.0.50	Gateway IP 192.168.0.50	Wireless IP 192.168.0.50	Gateway IP 192.168.2.50
		Netmask 255.255.255.0	
		Gateway IP 192.168.0.50	

A routing rule must be set in the PC on Network A

This will allow communications from Network A to Network B.

To enter a Routing rule:

Open a DOS command window and enter the following.

Route ADD 192.168.2.0 MASK 255.255.255.0 192.168.0.50

This routing rule says that if you wish 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 192.168.0.50.

Devices on Network B should also have their Default Gateway Address set to the Client Router Ethernet address (192.168.2.50). This will ensure that any traffic for the 192.168.0.0 network can be returned.

CHAPTER 5 - SPECIFICATIONS

Transmitter/Receiver

Frequency	360-512MHz (8 x 20MHz bands)
Transmit Power	Licensed - 5 Watt (+37dBm), Unlicensed – 0.5Watt (+27dBm)
Data Encoding	2-FSK, 4-FSK
Receiver Sensitivity	25 KHz channel : -99dBm @19,200 baud, -110dBm @ 9600 baud 12.5 KHz channel : -100dBm @9600 baud, -111dBm @ 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)	50Km (31mi.) @ 5Watts 10Km (6mi.) @ 0.5Watts
Antenna Connector	Female SMA Standard Polarity

Input/Output

Discrete I/O [1]	Discrete Input - Voltage-Free Contact – Max 30VDC, 5mA Wetting Current Discrete Output - FET 30Vdc 500mA Analog Input - Current sinking, 4-24mA +/- 0.2% Accuracy, 150 Ohm Impedance

Ethernet Port

Ethernet Port	10/100baseT; RJ45 Connector – IEEE 802.3, Auto MDIX
Link Activity	Link, 100baseT via LED

Serial Port

RS232	DB9 Female DCE; RTS/CTS/DTR/DCD
RS485 [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 RS232/485 connection Embedded Modbus Master/Slave for I/O transfer
Security	Data Encryption – 802.11i With CCMP 128bit 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 Indication/Diagnostics

LED Indication	Power/OK; RX; TX/Link; RS232; LAN; RS485; Analog/Digital I/O status Please refer to product manual for further information
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 115x 36mm (7.3” x 4.5” x 1.4”)
Housing	IP20 Powder-Coated Aluminum
Mounting	DIN Rail
Terminal Blocks	Removable; Max conductor 12AWG (2. 5mm2)
Temperature Rating	-40 to +70°C ; -40 to +120°F
Humidity Rating	0 – 99% RH Non-condensing
Weight	0.55kg (1.2lb).
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 V ac supply
Altitude	0 - 2000m (6500ft)

Power Supply

Nominal Supply	9 to 30Vdc; Under/Over Voltage Protection
Average Current Draw	120mA @ 13.8V (Idle);70mA @ 24V (Idle)
Transmit Current Draw	1.2-1.5A @ 13.8V (5Watts); 550-650mA @ 24V (5Watts)

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 present in the module by viewing the Home webpage of the module.

Firmware upgrades should be done locally with a PC connected directly to the module, remote firmware upgrades are not recommended over the radio link due to bandwidth limitations.

Firmware Upgrade – USB (Full Firmware Upgrade)

Firmware can be upgraded using a USB flash drive with the firmware files installed. Typically a full USB upgrade is required if the existing firmware is a much older version and requires multiple patch files to upgrade to the latest version or a patch file may not be available for the particular version to version.

The following procedure will guide you through performing a full USB firmware upgrade on a 450U-E

Requirements

- USB memory stick
- Firmware files – contact ELPRO Technical Support for these files.
- Ethernet Cable
- PC for transferring files

Preparing the USB memory stick for firmware upgrade.

Not all USB flash drives are configured correctly and can be used for firmware upgrade on the 450U-E. The following procedure describes how to check and if necessary re-configure the USB drive for use as a Firmware upgrade drive.

1. Plug in the USB drive, and wait until windows has recognised the drive and completed software installation.

2. Start a command prompt (Run cmd.exe), and type “diskpart” at the command prompt. This should bring up 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 example below the USB drive is a 1911 MB (2GB) 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 the USB disk is identified, issue the command “select Disk X” 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. Type the command “list partition” to check how the USB drive is partitioned. This will indicate whether the drive is correctly configured for use as a firmware upgrade drive on the 450U-E.

The drive should contain only one partition, and the Offset value should be non-zero as shown below.

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

You can now 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.

If the "Offset" is zero or if there is more than one Partition, as indicated in the examples below, follow 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. Issue the command "clean" to delete all partitions on the disk, then "list disk" to check that all memory is now free. (note in the example below, the "*" indicates that Disk 1 is the selected disk)

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

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. Now, issue the command "create partition primary" to create a partition on the USB drive. Issue 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 by performing the procedure below.

Formatting USB Memory Stick

Plug the USB stick in to the PC, select and right click the stick from within Windows Explorer. Select 'Format' from the right clicked menu.

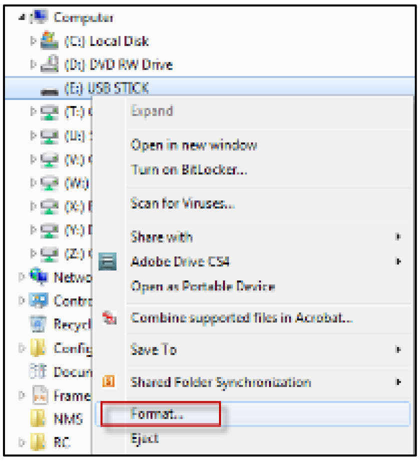
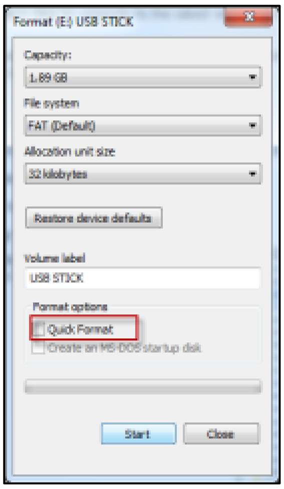


Figure 79 - Format USB

From the Format screen, ensure that 'Quick Format' is de-selected before pressing the Start button.


Format (E:) USB STICK

Capacity: 1.89 GB

File system: FAT (Default)

Allocation unit size: 32 kilobytes

Volume label: USB STICK

Format options

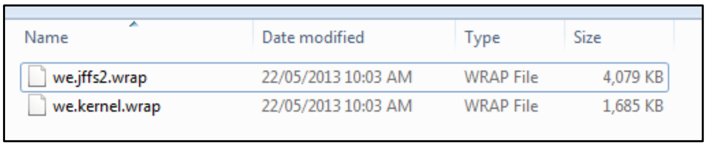
□ Quick Format

□ Create an MS-DOS startup disk

Figure 80 - Quick Format

Upgrade Procedure

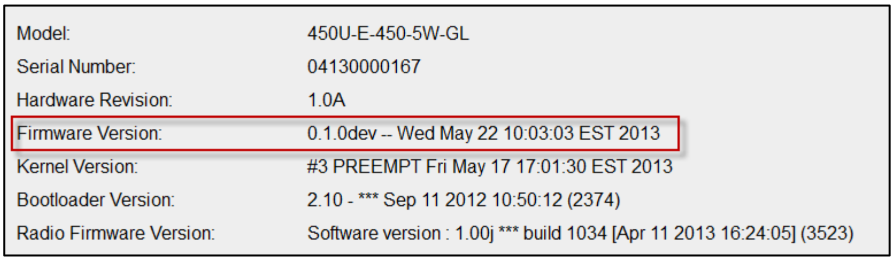
1. Prior to performing the upgrade you will need to copy the supplied firmware files to the USB Stick root directory. They should look something like the screenshot shown in Figure 81.



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 81 - Firmware Files

2. When the files have been copied, remove the USB stick from the PC. Note the current firmware version of the 450U-E by connecting to the modules home webpage. This will allow you to compare this version with the final version to confirm the upgrade procedure has been performed successfully.



Model:	450U-E-450-5W-GL
Serial Number:	04130000167
Hardware Revision:	1.0A
Firmware Version:	0.1.0dev -- Wed May 22 10:03:03 EST 2013
Kernel Version:	#3 PREEMPT Fri May 17 17:01:30 EST 2013
Bootloader Version:	2.10 - *** Sep 11 2012 10:50:12 (2374)
Radio Firmware Version:	Software version : 1.00j *** build 1034 [Apr 11 2013 16:24:05] (3523)

Figure 82- firmware version

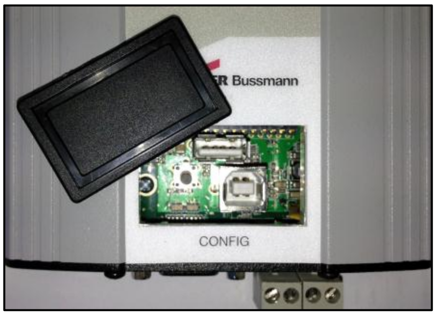


Figure 83 - Side access panel

3. Remove power from 450U-E if it is currently powered on.
4. Remove the black plastic cover on the front of the Module which will reveal a USB port and a reset push button switch.
5. Plug USB stick into USB port and apply power to the 450U-E Module.
6. The 'OK' LED will flash as per diagram below.
7. When complete, remove USB stick from 450U-E and refit the hatch cover.
8. Upgrade is now complete; Navigate to the Home page and check firmware version has been updated and that all other configuration settings are ok, configuration should not have been changed or erased during this process.

DO NOT remove the Flash drive or interrupt the power to the module while this is happening. If the upgrade process is interrupted module could become unserviceable and will need to be returned to ELPRO for repair.

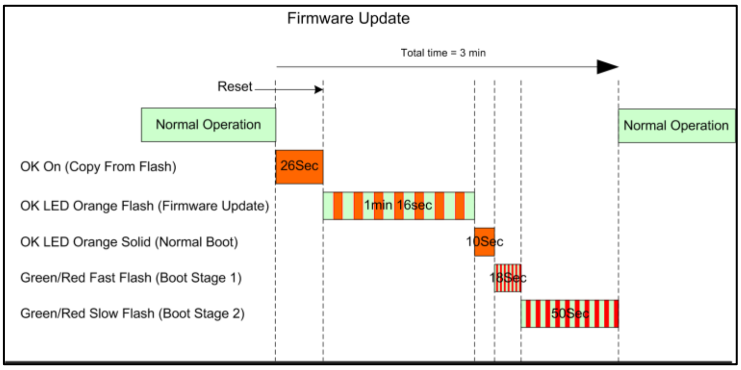

Firmware Update
Total time = 3 min
Reset
Normal Operation
Normal Operation
OK On (Copy From Flash)
26Sec
OK LED Orange Flash (Firmware Update)
1min 16sec
OK LED Orange Solid (Normal Boot)
10Sec
Green/Red Fast Flash (Boot Stage 1)
18Sec
Green/Red Slow Flash (Boot Stage 2)
50Sec

Figure 84 - Firmware Update LEDs

Web based Upgrade

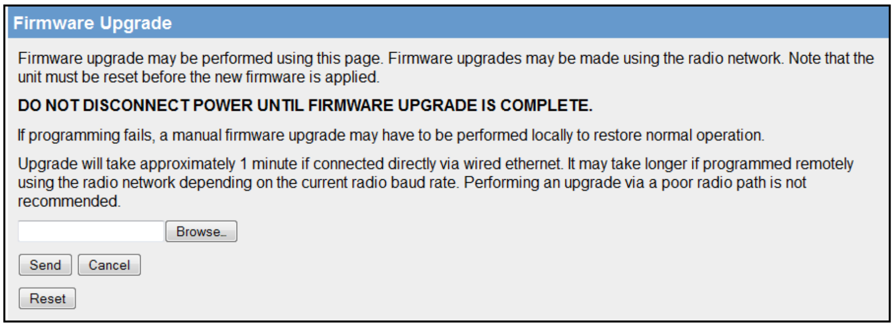
Web based firmware upgrade is available from the System tools page by selecting "firmware upgrade" from the "System Tools" web page.

Firmware upgrade is performed by uploading a "patch" file which is specific to the currently installed firmware version.

File will typically be named as "firmware_woody_X.X-X.X" where the X's indicate the current firmware version and the version it will be upgraded to.

If the device firmware version has fallen multiple versions behind the desired version, it may be necessary to upload multiple "patch" files.

Select 'Browse' and locate the patch file. When the patch file has been load press 'Send' to upload to the module. When the patch files have been uploaded, press 'Reset' for the module to perform the firmware upgrade. You will receive more detailed instructions if it is necessary to upgrade the module firmware.



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.

Figure 85 – Webpage Firmware Upgrades

Appendix B - 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 don't increase the transmission power, but focus the signal more. So instead of transmitting in every direction (including the sky and ground) antenna focus the signal usually 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 is used to connect two local area networks together. Bridges are typically used to connect wireless networks to wired networks. Typically, bridges will transfer messages between networks only when the message destination is on the other network. Messages that are destined for the same network as they originated on are not passed to the other network, therefore reducing 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 special 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.

CSMA/CA Carrier Sense Multiple Access/Collision Avoidance is a “listen before talk” method of minimizing (but not eliminating) collisions caused by simultaneous transmission by multiple radios. IEEE 802.11 states collision avoidance method rather than collision detection must be used, because the standard employs half duplex radios—radios capable of transmission or reception—but not both simultaneously. Unlike conventional wired Ethernet nodes, a WLAN station cannot detect a collision while transmitting. If a collision occurs, the transmitting station will not receive an ACKnowledge packet from the intended receive station. For this reason, ACK packets have a higher priority than all other network traffic. After completion of a data transmission, the receive station will begin transmission of the ACK packet before any other node can begin transmitting a new data packet. All other stations must wait a longer pseudo randomized period of time before transmitting. If an ACK packet is not received, the transmitting station will wait for a subsequent opportunity to retry transmission.

CSMA/CD Carrier Sense Multiple Access/Collision Detection is the access method used on an Ethernet network. A network device transmits data after detecting that a channel is available. However, if two devices transmit data simultaneously, the sending devices detect a collision and retransmit after a random time delay.

DHCP Dynamic Host Configuration Protocol 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 have 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, it automatically gets an IP address assigned to it.

Dial-up A communication connection via the standard telephone network, or Plain Old Telephone Service (POTS).

DNS Domain Name Service 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.

DSL
Digital Subscriber Line Various technology protocols for high-speed data, voice and video transmission over ordinary twisted-pair copper POTS (Plain Old Telephone Service) telephone wires.

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

Firewall
A device or computer program that keeps unauthorized users out of a private network. Everything entering or leaving a system's internal network passes through the firewall and must meet the system's security standards in order to be transmitted. Often used to keep unauthorized people from using systems connected to the Internet.

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 4 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.

Infrastructure mode
An 802.11 setting providing connectivity to an AP. As compared to Ad-Hoc mode, whereby 802.11 devices communicate directly with each other, clients set in Infrastructure Mode all pass data through a central AP. The AP not only mediates wireless network traffic in the immediate neighbourhood, but also provides communication with the wired network. See Ad-Hoc and AP.

I/O
Input / Output. The term used to describe any operation, program or device that transfers data to or from a computer.

Internet appliance
A computer that is intended primarily for Internet access is simple to set up and usually does not support installation of third-party software. These computers generally offer customized web browsing, touch-screen navigation, e-mail services, entertainment and personal information management applications.

IP
Internet Protocol. A set of rules used to send and receive messages across local networks and the Internet.

IP telephony
Technology that supports voice, data and video transmission via IP-based LANs, WANs, and the Internet. This includes VoIP (Voice over IP).

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, 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 SPX and NCP, are used for additional error recovery services. Sequenced Packet Exchange, SPX, 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.

ISO Network Model
A network model developed by the International Standards Organization (ISO) that consists of seven different levels, or layers. By standardizing these layers, and the interfaces in between, different portions of a given protocol can be modified or changed as technologies advance or systems requirements are altered. The seven layers are: Physical , Data Link, Network, Transport, Session, Presentation, Application.

LAN
Local Area Network. A system of connecting PCs and other devices within the same physical proximity for sharing resources such as an Internet connections, printers, files and drives.

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.

SNR
Signal to Noise Ratio. The number of decibels difference between the signal strength and background noise.

Transmit Power
The power usually expressed in mW or dBm that the wireless device transmits at.

MAC Address
Media Access Control address. 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.

NAT
Network Address Translation: A network capability that enables a number of computers to dynamically share a single incoming IP address from a dial-up, cable or xDSL connection. NAT takes the single incoming IP address and creates new IP address for each client computer on the network.

NIC
Network Interface Card. A type of PC adapter card that either works without wires (Wi-Fi) or attaches to a network cable to provide two-way communication between the computer and network devices such as a hub or switch. Most office wired NICs operate at 10 Mbps (Ethernet), 100 Mbps (Fast Ethernet) or 10/100 Mbps dual speed. High-speed Gigabit and 10 Gigabit NIC cards are also available. See PC Card.

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.

SSL

Secure Sockets Layer. A commonly used encryption scheme used by many online retail and banking sites to protect the financial integrity of transactions. When an SSL session begins, the server sends its public key to the browser. The browser then sends a randomly generated secret key back to the server in order to have a secret key exchange for that session

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. A protocol used along with the Internet Protocol (IP) to send data in the form of individual units (called packets) between computers over the Internet. While IP takes care of handling the actual delivery of the data, TCP takes care of keeping track of the packets that a message is divided into for efficient routing through the Internet. For example, when a web page is downloaded from a web server, the TCP program layer in that server divides the file into packets, numbers the packets, and then forwards them individually to the IP program layer. Although each packet has the same destination IP address, it may get routed differently through the network. At the other end, TCP reassembles the individual packets and waits until they have all arrived to forward them as single message.

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.

VoIP

Voice Over Internet Protocol. Voice transmission using Internet Protocol to create digital packets distributed over the Internet. VoIP can be less expensive than voice transmission using standard analog packets over POTS (Plain Old Telephone Service).

VPN

Virtual Private Network. A type of technology designed to increase the security of information transferred over the Internet. VPN can work with either wired or wireless networks, as well as with dial-up connections over POTS. VPN creates a private encrypted tunnel from the end user's computer, through the local wireless network, through the Internet, all the way to the corporate servers and database.

WAN

Wide Area Network. A communication system of connecting PCs and other computing devices across a large local, regional, national or international geographic area. Also used to distinguish between phone-based data networks and Wi-Fi. Phone networks are considered WANs and Wi-Fi networks are considered Wireless Local Area Networks (WLANs).

WEP

Wired Equivalent Privacy. 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.

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 C - Expansion I/O Registers

Adding 115S Expansion I/O modules to the 450U-E the I/O will automatically be added to the 450U-E modules I/O store. To calculate the register location, add the address of the I/O point from the tables below to the offset.

The offset ids calculated by finding the address of the Modbus Slave X 20.

E.g1. Digital input #1 on an 115S-11 with address 5 would be: (5x20) +10001 = 10101

E.g2. Digital output #2 on an 115S-11 with address 6 would be: (6x20) +2 = 122

E.g3. Analog input #3 on an 115S-12 with address 3 would be: (3x20) +30003 = 30063.

E.g4. Analog Output #8 on an 115S-13 with address # 7 would be: (7x20) + 40007 = 40147

I/O store for a 115S-11 Expansion I/O module

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. (Appendix D - 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 a 115S-12 Expansion I/O module

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. (Appendix D - 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 a 115S-13 Expansion I/O module

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
30017 + Offset	Modbus Error Counter for this 115S module
30018 + Offset	Modbus Last Error Code for this 115S module. (Appendix D - 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 D - Modbus Error Codes

The following are Modbus Error Response codes that can be read if utilising the Modus mapping fail register and selecting a General Purpose Analog Register (30501, 40501, etc.) instead of a General Purpose Digital register (10501, 501, etc.)

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, then 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 long duration of time will be required to do so. 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 (probably another unit)
64512	**FC00**	Server Offline	Couldn't connect to Modbus TCP server
63488	**F800**	Invalid Local Memory Address	Local address invalid in command - Memory location does not exist or is not initialised.
65535	**FFFF**	No Response to the Poll	No response to poll message

Appendix E - Power Conversion

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 F - GNU Free Doc License

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.