User Manual

805U-E Wireless Ethernet

ELPRO Technologies Pty Ltd, 29 Lathe St, Virginia Q 4014, Australia.

Tel: +61 7 33524533 Fax: +61 7 33524577 Email: sales@elprotech.com

Web: www.elprotech.com

Thank you for your selection of the 805U-E Wireless Ethernet Modem. We trust it will give you many years of valuable service.

ATTENTION!

Incorrect termination of supply wires may

cause internal damage and will void warranty.

To ensure your 805U-E enjoys a long life,

double check ALL your connections with

the user's manual

before turning the power on.

Caution!

For continued protection against risk of fire, replace the internal module fuse only with the same type and rating.

CAUTION:

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 someone 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.

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 Technologies 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 805U-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 805U-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 805U-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 805U-E module is not suitable for use in explosive environments without additional protection.

© October 2007

Warranty, Disclaimer and Limitation of Remedies

ELPRO products are warranted to be free from manufacturing defects for the period outlined in the ELPRO Warranty Statement.

Please visit the following link for this document.

https://elprotech.com/resourcehub-category/company-policies/

"Serviceable lifetime is not an extension of the warranty period and does not constitute a lifetime warranty."

CONTENTS

CHAPTER ONE INTRODUCTION 7
1.1 NETWORK TOPOLOGY 7
1.2 GETTING STARTED QUICKLY 9
CHAPTER TWO INSTALLATION 10
2.1 GENERAL 10
2.2 ANTENNA INSTALLATION 10
2.2.1 Dipole and Collinear antennas. 11
2.2.2 Yagi antennas. 12
2.3 POWER SUPPLY 14
2.4 SERIAL CONNECTIONS 14
2.4.1 RS232 Serial Port 14
2.4.2 RS485 Serial Port 15
2.5 DISCRETE (DIGITAL) INPUT/OUTPUT 17
CHAPTER THREE OPERATION 18
3.1 START-UP 18
3.2 DEFAULT CONFIGURATION 20
3.3 CONFIGURING THE UNIT FOR THE FIRST TIME 21
3.3.1 Set PC to same network as 805U-E 21
3.3.2 Set 805U-E to same network as PC 24
3.4 QUICK CONFIGURATION 26
3.5 NETWORK CONFIGURATION 27
3.6 ETHERNET DATA 29
3.7 NORMAL OPERATION 29
3.8 FIXED FREQUENCY OPERATION 30
3.9 RADIO CONFIGURATION MENU 30
3.9.1 Duty Cycle Calculations 33
3.10 SPANNING TREE ALGORITHM / REDUNDANCY 33
3.11 ROUTING RULES 34
3.12 WIRELESS MESSAGE FILTERING 36
3.13 SERIAL PORT CONFIGURATION 39
3.12.1 RS-232 PPP Server 39
3.12.2 Serial Gateway 43
3.12.3 Modbus TCP to RTU Server 46
3.14 DIGITAL INPUT/OUTPUT AND I/O TRANSFER 47
3.15 MODULE INFORMATION CONFIGURATION 53
3.16 REMOTE CONFIGURATION 53
3.17 CONFIGURATION EXAMPLES 54

CHAPTER FOUR DIAGNOSTICS 59
4.1 DIAGNOSTICS CHART 59
4.2 DIAGNOSTIC INFORMATION AVAILABLE 60
4.2.1 Connectivity 60
4.2.2 Monitor Communications 61
4.2.3 Statistics 61
4.2.3 Statistics 62
4.2.4 Network Traffic Analysis 62
4.3 TESTING RADIO PATHS 62
4.4 UTILITIES 63
4.4.1 PING 63
4.4.2 IPCONFIG 65
4.4.4 ROUTE 66
CHAPTER FIVE SPECIFICATIONS 67
APPENDIX A FIRMWARE UPGRADE 69
APPENDIX B GLOSSARY 74

Chapter One INTRODUCTION

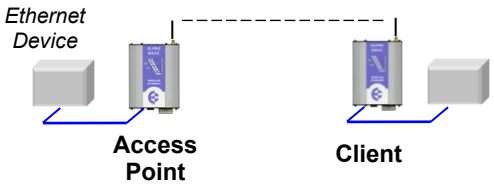
The 805U-E Wireless Ethernet module provides wireless connections between Ethernet devices or Ethernet wired networks (LAN's). It has an internal 869 MHz wireless transceiver, which can be used without a radio license in Europe and South Africa. The 805U-E transmits RF power of 500mW, requiring the transmit duty-factor be limited to 10%.

The 805U-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 up to 76 Kbit/sec.

1.1 Network Topology

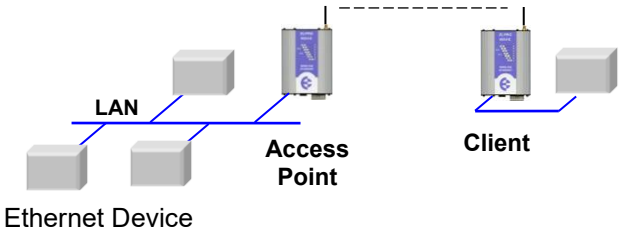
The 805U-E is an Ethernet device, and must be configured as part of an Ethernet network. Each 805U-E must be configured as:

- an "Access Point" or a "Client", and
- a "Bridge" or a "Router".



You can also connect to the 805U-E via a RS232 or RS485 serial port using PPP (point-to-point) protocol. PPP allows the 805U-E to connect serial communications into the Ethernet network.

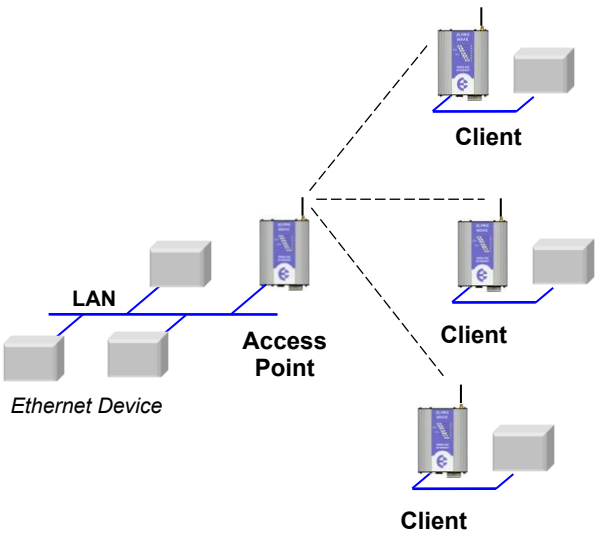
Access Point vs Client



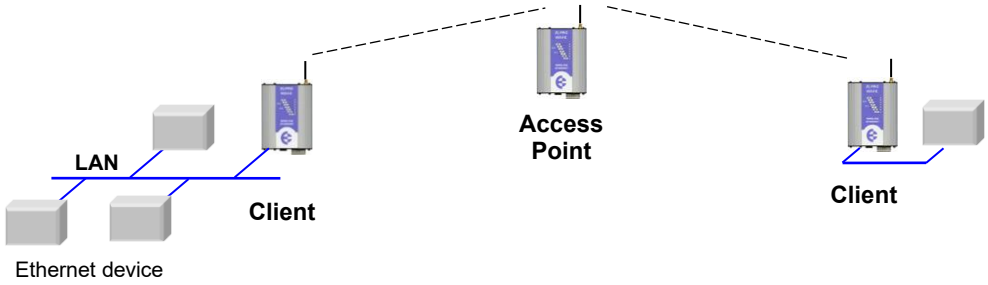
The Access Point unit acts as the "wireless master" unit. The Access Point sets up the wireless links to the Client units, and controls the wireless communications. The first diagram shows two Ethernet devices being linked. One 805U-E is configured as an Access Point and one as a Client - in this example it doesn't mater which unit is the Access Point.

The second diagram shows an existing LAN being extended using 805U-E's. In this example, the Access Point should be 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.



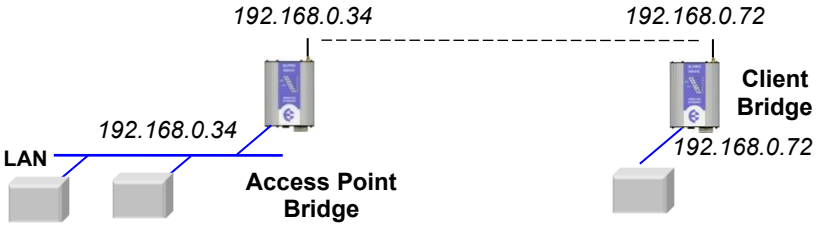
An Access Point could be used as a "Repeater" unit to connect two 805U-E Clients which do not have direct reliable radio paths.



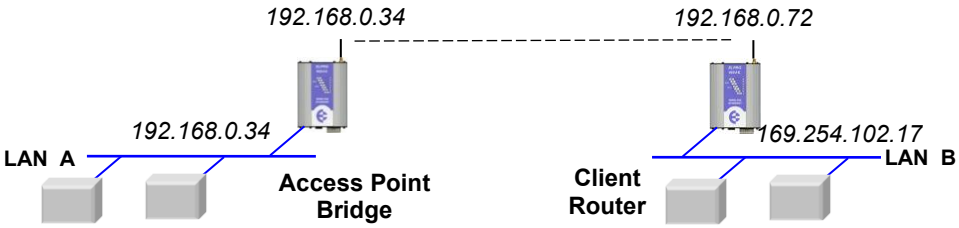
Bridge vs Router

Each 805U-E is configured with an IP address for the Ethernet side, and another for the wireless side.

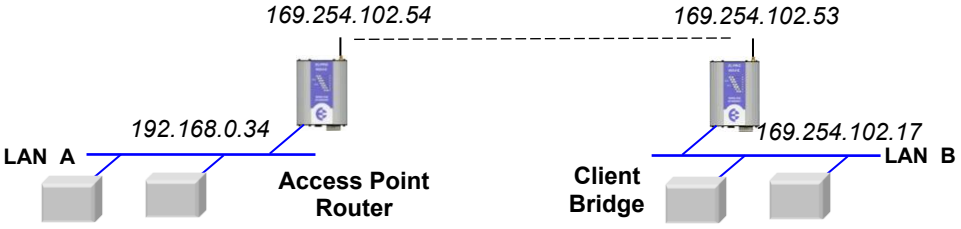
A **Bridge** connects devices within the same Ethernet network - for example, extending an existing Ethernet LAN. For a Bridge, the IP address for the wireless side is the same as the Ethernet side.



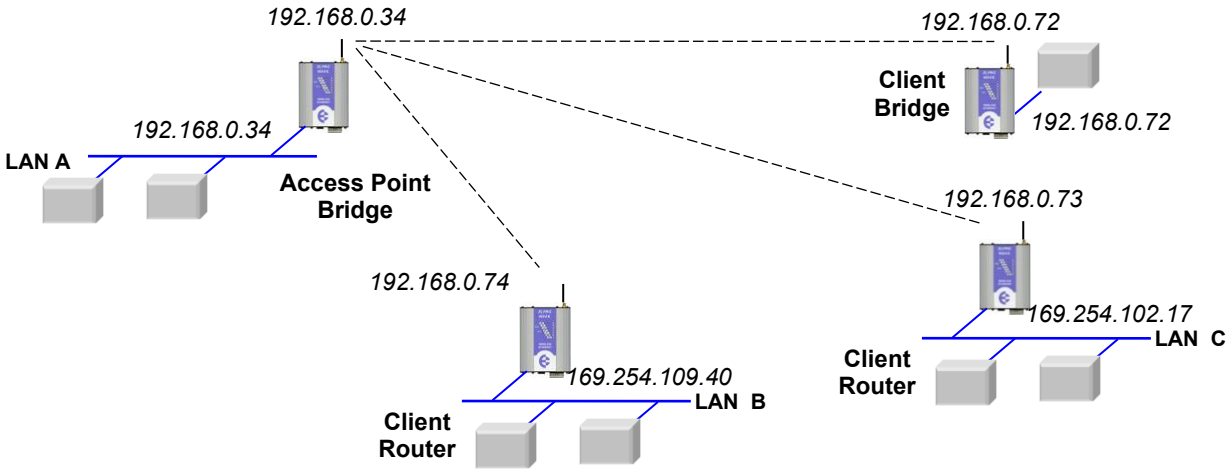
A **Router** connects devices on different LAN's. The IP addresses for the Ethernet and wireless sides are different.



In the above example, the wireless link is part of LAN A, with the Client unit acting as a Router between LAN A and LAN B. Alternately, the Access Point could be configured as a Router - the wireless link is then part of LAN B.



There is limit of two Routers within the same radio network. There is no limit to the number of Bridges in the same network - although there is a limit of 255 Client units linked to any one



Access Point.

1.2 Getting Started Quickly

Most applications for the 805U-E require little configuration. The 805U-E has many sophisticated features, however if you don't require these features, this section will allow you to configure the units quickly.

First, read Section 2, "Installation". The 805U-E requires an antenna and a power supply.

- Power the 805U-E and make an Ethernet connection to your PC (for further information on how to do this, refer to section 3.3)
- Set the 805U-E address settings as per section 3.4
- Save the configuration - the 805U-E is now ready to use.

Before installing the 805U-E, bench test the system. It is a lot easier to locate problems when the equipment is all together.

There are other configuration setting which may or may not improve the operation of the system. For detail on these settings, refer to section 3.

Chapter Two INSTALLATION

2.1 General

The 805U-E module is housed in an rugged aluminum case, suitable for DIN-rail mounting. Terminals will accept wires up to 2.5 sqmm in size.

All connections to the module must be SELV. Normal 110-240V mains supply should not be connected to any terminal of the 805U-E module. Refer to Section 2.3 **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 adjacent. Following installation, the most common problem is poor communications caused by incorrectly installed antennas, or radio interference on the same channel, or the radio path being inadequate. If the radio path is a problem (ie path too long, or obstructions in the way), then higher performance antennas or a higher mounting point for the antenna may rectify the problem. Alternately, use an intermediate 805U-E Module as a repeater.

The foldout sheet 805U-E ***Installation Guide*** provides an installation drawing appropriate to most applications. Further information is detailed below.

Each 805U-E module should be effectively earthed via the "GND" terminal on the 805U-E module - this is to ensure that the surge protection circuits inside the 805U-E module are effective.

2.2 Antenna Installation

The 805U-E module will operate reliably over large distances up to 5 km “line-of-sight”. The distance which may be reliably achieved will vary with each application - depending on the type and location of antennas, the degree of radio interference, and obstructions (such as hills or trees) to the radio path.

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. For example, a group of trees around the antenna is a larger obstruction than a group of trees further away from the antenna. The 805U-E modules provide a diagnostic feature which displays the radio signal strength of transmissions.

Line-of-sight paths are only necessary to obtain the maximum range. Obstructions will reduce the range, however may not prevent a reliable path. A larger amount of obstruction can be tolerated for shorter distances. For very short distances, it is possible to mount the antennas inside buildings. An obstructed path requires testing to determine if the path will be reliable - refer the section 6 of this manual.

Where it is not possible to achieve reliable communications between two 805U modules, then a third 805U 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.

An antenna should be connected to the module via 50 ohm coaxial cable (eg RG58, RG213 or Cellfoil) 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. For use on unlicensed frequency channels, there are several types of antennas suitable for use. It is important antenna are chosen carefully to avoid contravening the maximum power limit on the unlicensed channel - if in doubt refer to an authorized service provider.

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 maximum net gain of the antenna/cable configuration permitted is 0dB.

The gains and losses of typical antennas are

Antenna	*Gain (dB)*
3dB Collinear	3
6dB Collinear	6
6 element Yagi	10
Cable type	*Loss (dB per 10 m)*
RG58	-5
RG213	-2.5
Cellfoil	-3

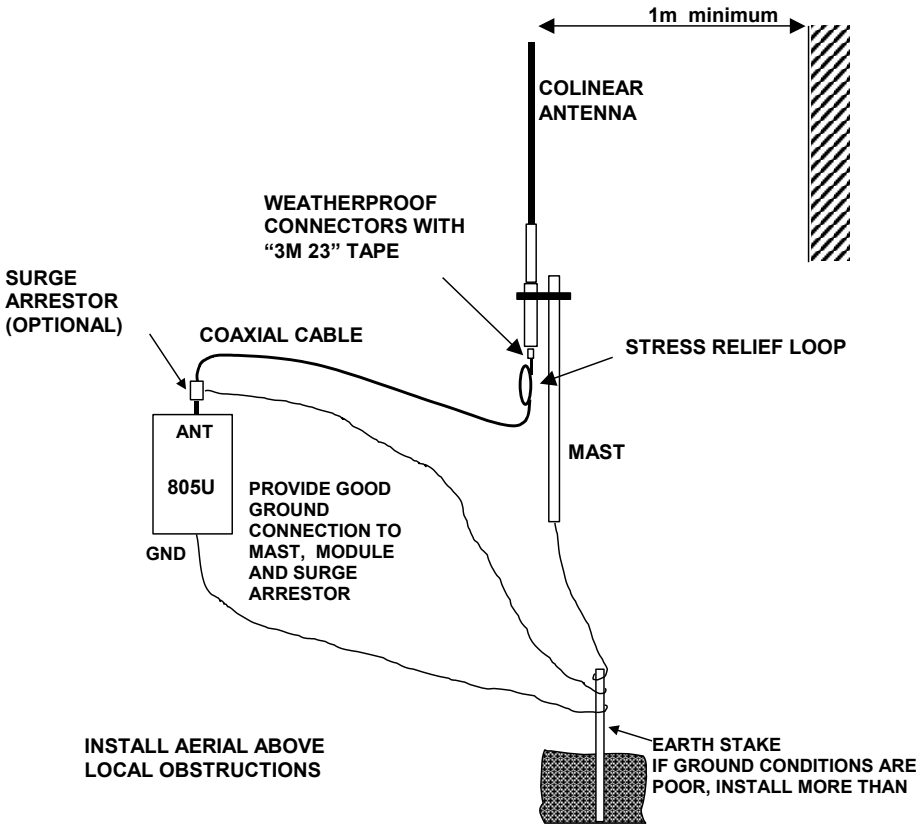
The net gain of the antenna/cable configuration is determined by adding the antenna gain and the cable loss. For example, a 6 element Yagi with 20 metres of RG58 has a net gain of 0 dB (10dB – 10dB).

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 a 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, surge suppression devices between the module and the antenna are recommended. 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.

2.2.1 Dipole and Collinear antennas.

A collinear antenna transmits the same amount of radio power in all directions - as such that are easy to install and use. The dipole antenna with integral 5m cable does not require any additional coaxial cable, however a cable must be used with the collinear antennas.



Collinear and dipole antennas should be mounted vertically, preferably 1 metre away from a wall or mast to obtain maximum range.

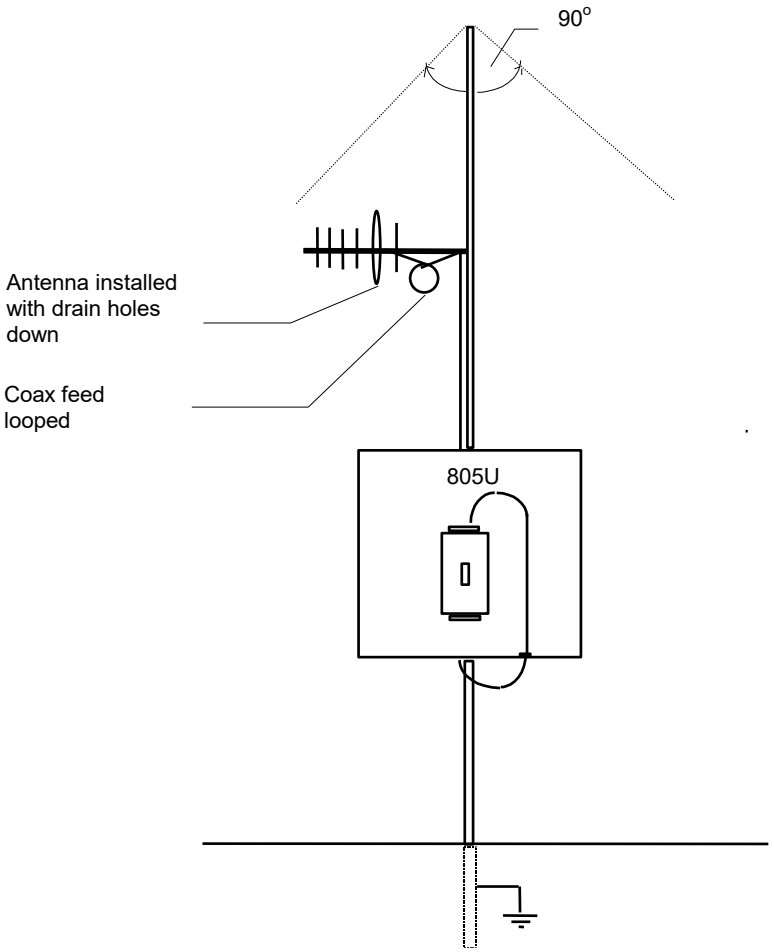
2.2.2 Yagi antennas.

A Yagi 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.

The Yagi gain also acts on the receiver, so adding Yagi antennas at both ends of a link provides a double improvement.

Yagi antennas are directional. That is, they have positive gain to the front of the antenna, but negative gain in other directions. Hence Yagi antennas 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. The Yagi antennas may be installed with the elements in a vertical plane (vertically polarized) or in a horizontal plane (horizontally polarized). For a two station installation, with both modules using Yagi antennas, horizontal polarization is recommended. If there are more than two stations transmitting to a common station, then the Yagi antennas should have vertical polarization, and the common (or "central" station should have a collinear (non-directional) antenna.

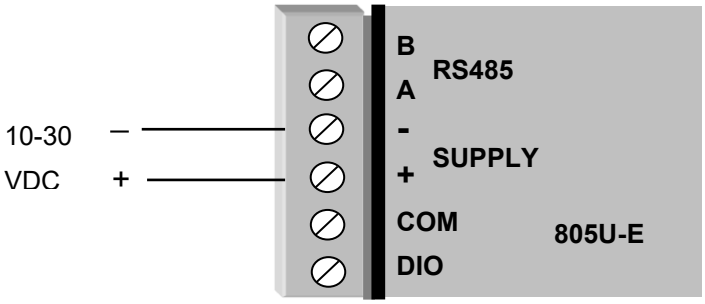
Also note that Yagi antennas normally have a drain hole on the folded element - the drain hole should be located on the bottom of the installed antenna.



2.3 Power Supply

The 805U-E module can be powered from a 10 - 30VDC power supply. The power supply should be rated at 1 Amp. The negative side of the supply should be connected to a good "ground" point for surge protection. The supply negative is connected to the unit case internally.

The positive side of the supply must not be connected to earth. The DC supply may be a floating supply or negatively grounded. The power requirements of the 805U-E unit is 280mA @ 12V or 150mA @ 24VDC. This is inclusive of radio and Ethernet ports active, & serial port plugged in.



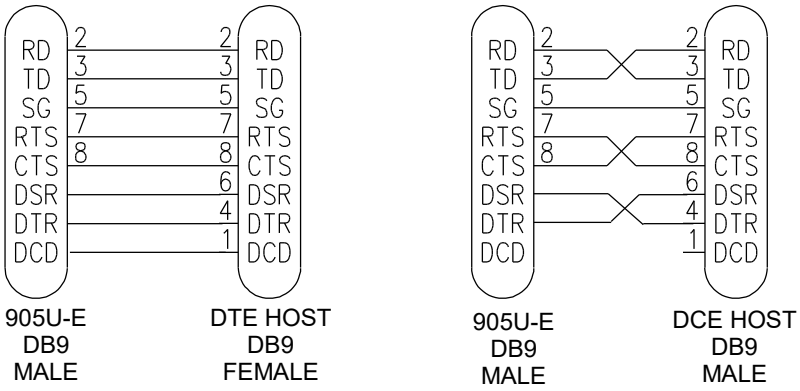
Transmission current (500mW RF) is nominally 500mA at 12V, 250mA at 24VDC.

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)

2.4 Serial Connections

2.4.1 RS232 Serial Port

The serial port is a 9 pin DB9 female and provides for connection to a host device as well as a PC terminal for configuration, field testing and for factory testing. Communication is via standard RS232 signals. The 805U-E is configured as DCE equipment with the pinouts detailed below.



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, or may be configured to reflect the status of CTS/RTS lines at the remote site. The 805U-E does not support XON/XOFF.

Example cable drawings for connection to a DTE host (a PC) or another DCE hosts (or modem) are detailed above.

DB9 Connector Pinouts

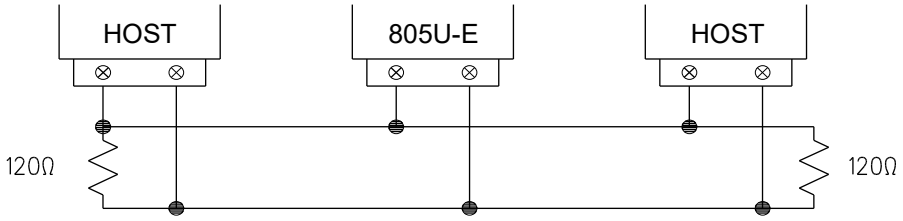
Pin	Name	Direction	Function
1	DCD	Out	**Data carrier detect** –
2	RD	Out	**Transmit Data** – Serial Data Output
3	TD	In	**Receive Data** – Serial Data Input
4	DTR	In	**Data Terminal Ready** -
5	SG		**Signal Ground**
6	DSR	Out	**Data Set Ready** - always high when unit is powered on.
7	RTS	In	**Request to Send -**
8	CTS	Out	**Clear to send -**
9	RI		**Ring indicator** -

2.4.2 RS485 Serial Port

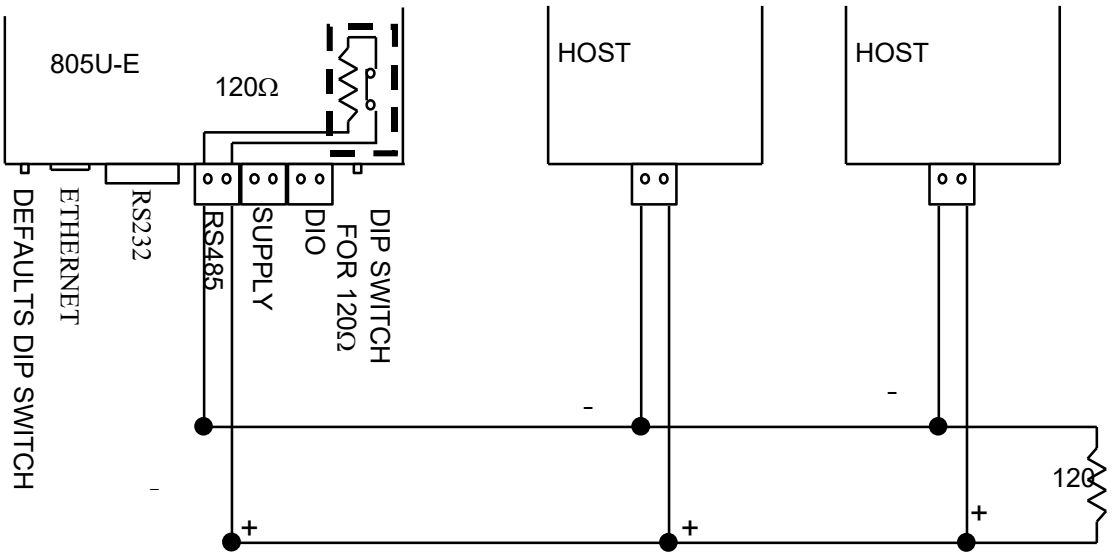
The RS485 port provides for communication between the 805U-E unit and its host device using a multi-drop cable. Up to 32 devices may be connected in each multi-drop network.

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.

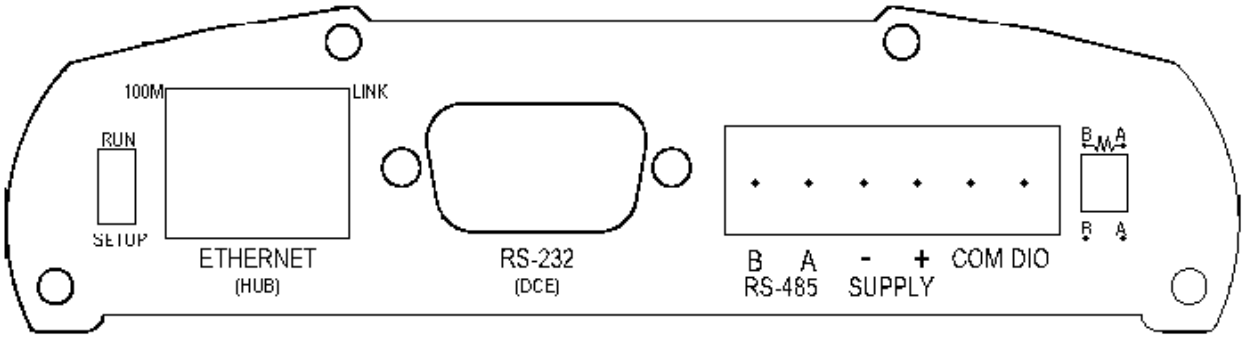
RS485 is a balanced, differential standard but it is recommended that shielded, twisted pair cable be used to interconnect modules to reduce potential RFI. It is important to maintain the polarity of the two RS485 wires. An RS485 network should be wired as indicated in the diagram below and terminated at each end of the network with a 120 ohm resistor. On-board 120 ohm resistors are provided and may be engaged by operating the single DIP switch in 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 module is not at one end of the RS485 cable, the switch should be off.



RS485 CONNECTIONS



RS485 CONNECTION USING TERMINATING RESISTOR

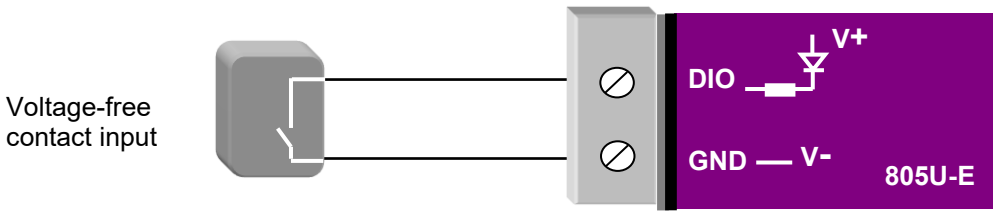


2.5 Discrete (Digital) Input/Output

The 805U-E has one on-board discrete/digital I/O channel. This channel can act as either a discrete input or discrete output. It can be monitored, or set remotely, or alternatively used to output a communications alarm status.

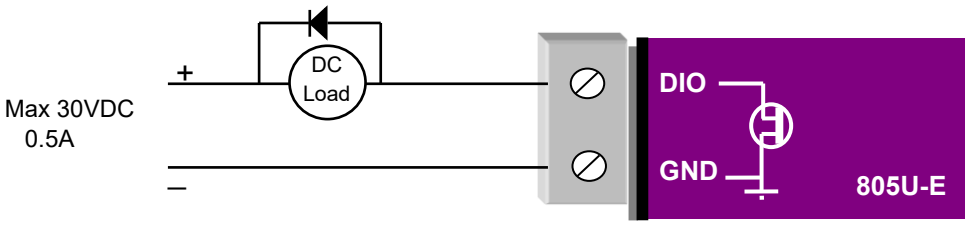
If used as an “input”, the I/O channel is suitable for voltage free contacts (such as mechanical switches) or NPN transistor devices (such as electronic proximity switches). PNP transistor devices are not suitable. Contact wetting current of approximately 5mA is provided to maintain reliable operation of driving relays.

The digital input is connected between the "DIO" terminal and common "COM". The I/O circuit includes a LED indicator which is lit when the digital input is active, that is, when the input circuit is closed. Provided the resistance of the switching device is less than 200 ohms, the device will be able to activate the digital input.



The I/O channel may also be used as a discrete output. The digital outputs are transistor switched DC signals, FET output to common rated at 30VDC 500 mA.

The output circuit is connected to the "DIO" terminal. The digital output circuit includes a LED indicator which is lit when the digital output is active.



Chapter Three OPERATION

3.1 Start-up

"Access Point" Start-up

An Access Point unit starts and immediately begins transmitting periodic messages called beacons. These beacon messages are messages contain information for Clients on how to establish a link with the Access Point.

Any Client that hears the messages, which are not already linked to another Access Point unit, will respond and links will be established between the new Access Point and these Clients.

"Client" Start-up

When a Client powers up, it immediately scans for messages from Access Point units. The Client will continue to scan for twice the configured beacon interval in the Client. During the scan, the RX led will flicker now and again indicating messages received, perhaps from an Access Point. If the Client finds suitable Access Points during the scan, it will then attempt to establish a link with the Access Point with the strongest radio signal.

Link Establishment

When the Client wishes to establish a link with an Access Point it follows a two step process. The first step is "authentication". During this step the Client and Access Point check if they can establish a secure link, based upon the configured security encryption.

Once the Client has been authenticated, it will then request a link. This step is called "association".

While no links have been established, the LINK led will be OFF. Once a single link has been established, the LINK led is ON.

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 information to the Clients linked to it.

The maximum number of 255 Clients may be linked to an Access Point.

How a Link connection is lost

The 805U-E will reset the Link if:

- Excessive retries: When a 805U-E unit transmit a wireless message to another unit, the destination unit will transmit back an acknowledgment. If the source unit does not receive an acknowledgment, it will re-send the message - this is known as a "re-try". Both Access Point and Client will drop the link if the number of retries for a single packet exceeds (7) times. Packets are retransmitted according to an increasing time delay between retries, with each attempt on a different frequency.
- Inactivity: During periods of inactivity, Clients will periodically check that the link to the Access Point remains intact. This process is called "reassociation", and will occur approximately (6) beacon intervals after the last packet was sent to the Access Point. If a Client unit does not get a response from its Access Point, it will retry the reassociating request (7) times before resetting the link. If an Access Point does not receive any traffic from a Client, including reassociating requests, within (12) beacon intervals, the Access Point will reset the link.

After a Client has reset it's Link status, it will start scanning for an Access Point, as if it has just started up.

LED Indication

The following table details the status of the indicating LEDs on the front panel under **normal** operating conditions.

LED Indicator	Condition	Meaning
OK	GREEN	Normal Operation
OK	RED	Supply voltage too low.
Radio RX	GREEN flash	Radio receiving data
Radio RX	RED flash	Weak radio signal
Radio TX	Flash	Radio Transmitting
Radio LINK	On	On when a radio communications link is established
Radio LINK	Off	Communications failure or radio link not established
Radio LINK	GREEN flash RED flash	Serial Port Receiving CTS low
LAN	ON	Link Established on Ethernet port
LAN	Flash	Activity on Ethernet port.
Serial	GREEN flash	RS232 Serial Port Activity
Serial	RED flash	Rs485 Serial Port Activity
DIO	On	Digital Output ON ***or*** Input is grounded.
DIO	Off	Digital Output OFF ***and*** Input is open circuit.

The Ethernet RJ45 port incorporates two indication LEDs. The LINK LED comes on when there is a connection on the Ethernet port, and will blink off briefly when activity is detected on the Ethernet Port. The 100MB LED indicates that the 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 Six **Troubleshooting**.

3.2 Default Configuration

The default factory configuration of the 805U-E is

- Bridge/Client
- 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*"

The 805U-E will temporarily load some factory-default settings if powered up with the Factory Default switch (on the end-plate of the module) in SETUP position. In the position, wireless operation is disabled. The previous configuration remains stored in 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.

3.3 Configuring the Unit for the First Time

The 805U-E has a built-in webserver, containing webpages for analysis and modification of configuration. The configuration can be accessed using Microsoft® Internet Explorer. This program is shipped with Microsoft Windows or may be obtained freely via the Microsoft® website.

Configuration of IP address, gateway address and subnet mask may also be accessed via the RS-232 serial port.

Accessing Configuration for the first time

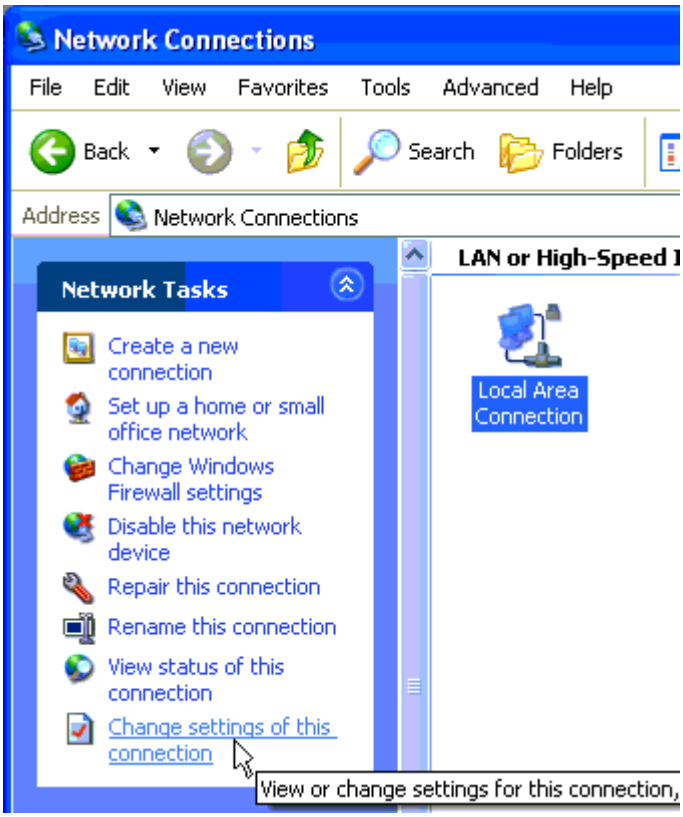
There are two methods for accessing the configuration inside a 805U-E. The first method requires changing your computer settings so that the configuring PC is on the same network as the 805U-E with factory default settings. **This is the preferred method** and is much less complicated than the second method. You will need a "straight-through" Ethernet cable between the PC Ethernet port and the 805U-E. The factory default Ethernet address for the 805U-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).

The second method requires setting an IP address in the 805U-E such that it is accessible on your network without having to change your network settings.

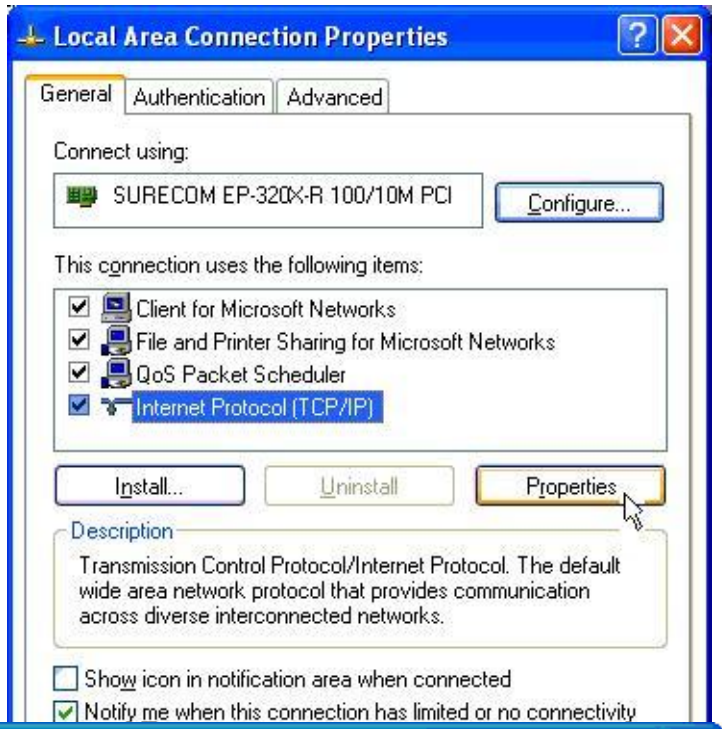
3.3.1 Set PC to same network as 805U-E

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 805U-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 cycle power at the conclusion of configuration for resumption of normal operation.
- Power up the 805U-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.

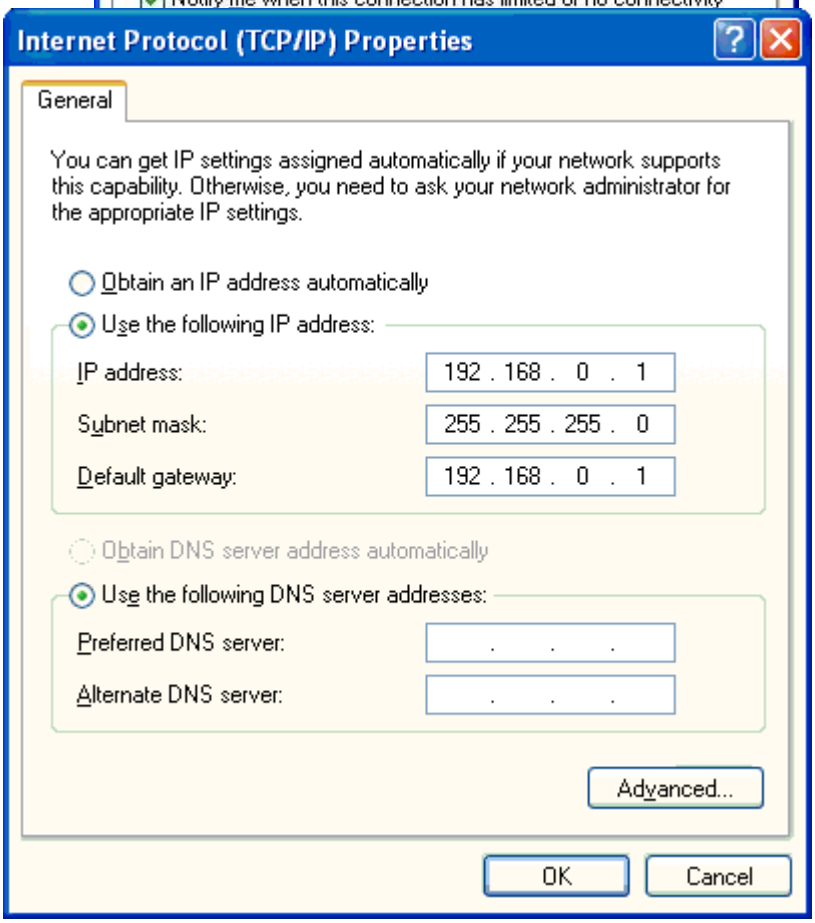


- Open “Properties” of Local Area Connection.



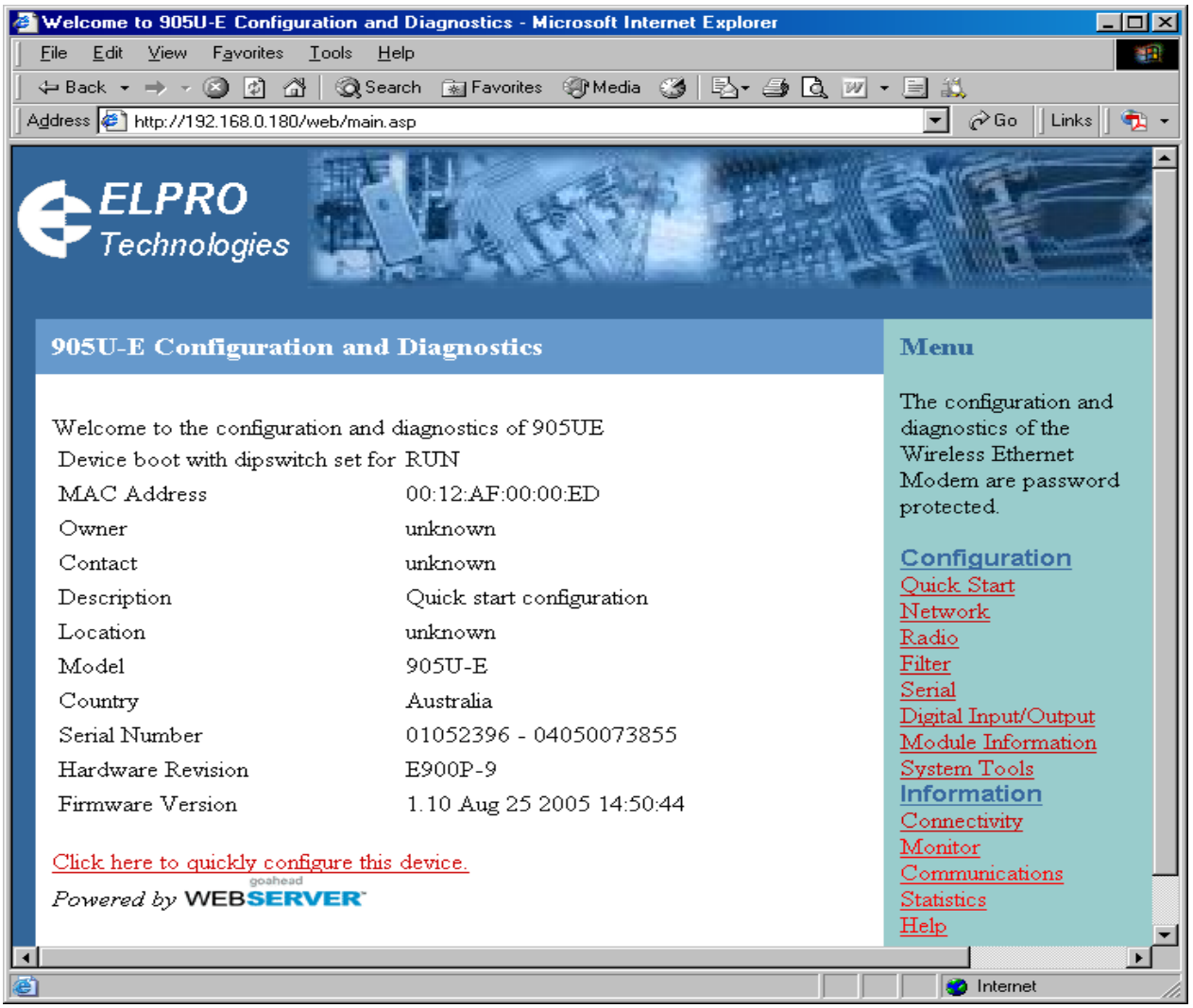
- Select Internet Protocol (TCP/IP) and click on Properties.

- On the General tab enter IP address 192.168.0.1, Subnet mask 255.255.255.0, and default gateway 192.168.0.1.



- 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 805U-E *http://192.168.0.1XX* where XX is the last two digits of the serial number
- A welcome webpage should be displayed as illustrated below.
- Configuration and Diagnostics may be opened by clicking on any of the menu items, and entering the username "*user*" and default password "*user*". Configure the unit to your requirements (refer later sections of this manual).



When Configuration is complete, switch Factory Default dip-switch on 805U-E to RUN position, and cycle power to resume normal configured operation.

3.3.2 Set 805U-E to same network as PC

This is the alternate procedure to setting an IP address in the 805U-E. Consult your network administrator for an IP address on your network, the gateway IP address, and network mask.

a) Switch Factory Default dip-switch on 805U-E to SETUP position.

b) Connect the RS232 port on the 805U-E to the RS232 port on the PC using a "straight-through" serial cable.

c) Open a terminal package (such as Hyperterminal) with 19200bps data rate, 8 data bit, 1 stop, no parity and no flow control. Make sure that no other programs have control of the serial port.

d) Power up 805U-E. Basic network settings will be displayed on the terminal as illustrated below. When prompted, hit enter key to stop automatic boot process. You have 5 seconds to abort the boot process.

```
My Right Boot 2.1
 Copyright 1999-2004 Cybertec Pty Ltd, All rights reserved.
 This software is provided by Cybertec ``as is'' and with NO WARRANTY.
   http://www.cybertec.com.au/

ROM :   256KB @ 0xffe00000
RAM :  8192KB @ 0x00000000 (141KB / 0x0002366c)

ROM Configuration table ... PASSED.
RAM address pattern check . PASSED.
RAM address bus check ..... PASSED.

Product       : E900P R2.3F
Variant       : default-variant
Serial No.    : 09040569 - 012345678910
Release       : epm_mrb_elpro_E900P_1.5
Released date : 11 August 2005
Released host : Anxosity
Build date    : Thu Aug 11 12:01:05 2005
Build host    : Anxosity
Boot Flags    : no RAM test, no ROM test, bus timer on, wdog on
                static IP, auto-boot, net-boot, reset on
                local file, no binary load
Boot delay    : 0
Boot Filename : /memory/0xffe40000,0x60000
Boot Address  : 192.168.123.113
Boot Netmask  : 255.255.255.0
Boot Gateway  : 192.168.123.113
Boot Host     : 192.168.123.1
Boot Mac 0    : 00:12:af:00:00:10
Boot Mac 1    : 00:12:af:00:00:10

RTE data store .... no error
Setting bus timer (on) and watchdog (on) ... PASSED

Recovery Configuration :
ip address : 192.168.0.110
net mask   : 255.255.255.0
gateway    : 192.168.0.1
host       : 192.168.0.1

eip: mount point /memory
fec0: connected at 100M Full Duplex.
fec0: local ip = 192.168.0.110, server ip = 192.168.0.1

Press ENTER to abort automatic booting ... 5
```

e) Check values for Boot Address, Boot Netmask, and Boot Gateway. These values should be set to reflect those of the PC you are using to configure the unit. If these are correct skip to step (h). You may check settings again with the *rct* command. For further help, type the *help* command.

f) Set Boot Netmask to the same settings as the computer you have the Ethernet cable connected to. This may be performed with the command: *bnm <Type the netmask>*

g) Set Boot Gateway to the same settings as the computer you have the Ethernet cable connected to. This may be performed with the command: *bgw <Type the gateway IP address>*

h) Choose an IP address for the 805U-E being upgraded. This IP address must be on the same network as the computer you have connected the Ethernet cable to. This may be performed with the command: *bip <Type the IP address>*

i) Switch dip-switch on 805U-E to RUN position.

j) Type the command *reset*, or cycle power to the unit. The 805UE will reset and start with the network settings you have entered.

k) 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.

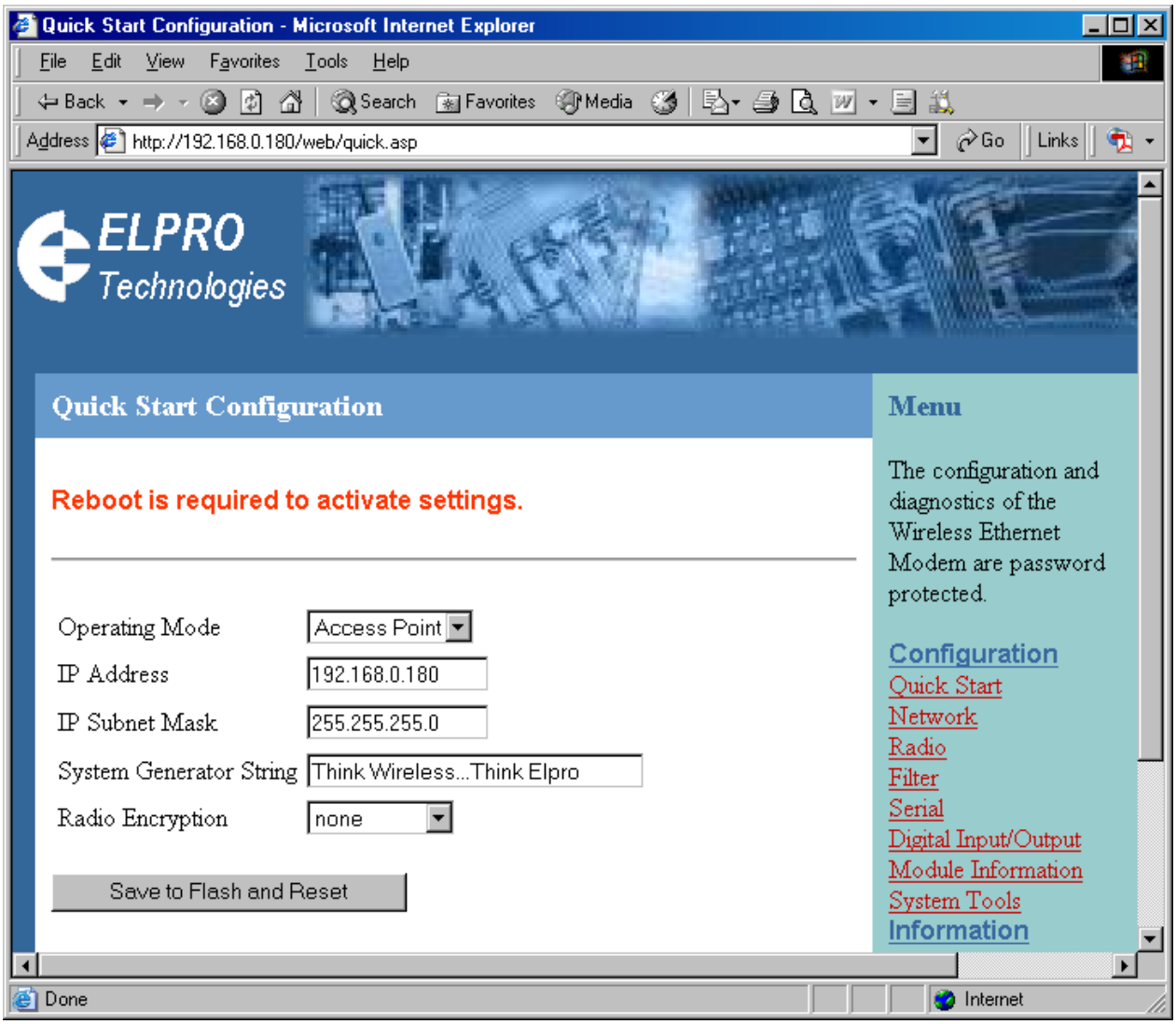
l) Enter the webpage *http://xxx.xxx.xxx.xxx/* where *xxx.xxx.xxx.xxx* is the IP address selected for the module. A welcome webpage should be displayed as illustrated.

m) Clicking on any of the menu items, and entering the username “user” and password “user” may open Configuration and Diagnostics. If the password has previously been configured other than the default password, then enter this instead.

3.4 Quick Configuration

The 805U-E has default configurations which will cover most applications. These parameters can be manually changed however this is not necessary for the majority of applications.

A "Quick Start" configuration is provided for simple networks. This is the first stage of the module configuration. For most applications, no further configuration is required. For more advanced applications, the other parameters can be changed via the other configuration pages after the Quick Start page.



Enter the Configuration web-page as per section 3.3 and select "Quick Start".

You need to select:

- Access Point or Client. Bridge operation is assumed - for Router selection, go to the Network page after Quick Start
- IP Address and Subnet Mask for your application. The default settings will be shown. If your system is connecting individual devices which are not connected to an existing Ethernet LAN, then you can use the factory default IP values. If you are connecting to

an existing LAN, then you need to change the IP addresses to match your LAN addresses.

- A "System Generator String" - refer to section 3.4.1 below
- Radio encryption selection - None, 64-bit Proprietary or 128-bit AES - refer section 3.4.2 for more information on this.

After configuring, select "Save to Flash and Reset".

3.4.1 System Generator String

The System Generator String is an alpha-numeric string of between 1 and 31 characters. Characters can be any ASCII alpha-numeric character (except the "null" character). The 805U-E uses this string as an input to pseudo-random algorithms to create the following parameters:

- A system address, which is transmitted as part of each wireless data message to differentiate one wireless system from another,
- Encryption keys for the data encryption method selected
- Select a hop-set. The spread spectrum radio in the 805U-E continually changes frequency, or hops to different frequencies, according to a "hop-set" pattern. There are 8 different hop-set patterns available. Different hop-sets are automatically selected to minimize any radio interference from other 805U-E systems.

The System Generator String should be a unique data string - for example, *BLUEpencil93*

The same System Generator String should be entered in each module operating in the same system.

3.4.2 Radio Encryption

Wireless data can be encrypted to provide security. If you do not require this feature, do nothing - the default configuration is "no encryption". The 805U-E operation is faster without data encryption.

If you do require this security feature, you have a choice of 64-bit proprietary encryption or 128-bit AES encryption. AES is a superior encryption scheme accepted by most users as one of the most secure encryption schemes available. For users who prefer not to use a "public-domain" encryption scheme, a proprietary scheme is available. Both encryption methods provide an extremely high level of security of the wireless data.

3.5 Network Configuration

After configuring the Quick Start page, you can view or modify Ethernet network parameters by selecting the "Network" menu. When prompted for username and password, enter "user" as the username, and the previously configured password in the password field.

If IP address or password has been forgotten, the Factory Default switch may be used to access the existing configuration. Refer to section 3.3 above.

After the addresses are configured, it is important to save the configuration by selecting "Save and Reboot".

Network Settings Webpage Fields

Device Mode	Used to select Bridge or Router mode. By default this is set to Bridge.
Operating Mode	Used to select Access Point or Client mode. By default this is set to Client.
Bridge Priority	The priority of the 805U-E, if configured as a bridge, in the Bridge Spanning Tree algorithm. By default this is set to the lowest priority at 255. This setting will have no effect and should not be used unless the redundant wireless links are being used. This is explained in Section 3.9
MAC Address	This is the unique hardware address of the 805U-E, assigned in the Factory. For the majority of systems, this item should not be changed. If the device is to be connected to equipment that will only communicate with a set MAC Address, the 805U-E may clone that MAC address.
Gateway IP Address	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.
Ethernet IP Address	The IP address of the 805U-E on its Ethernet port. This should be set to the IP address you require.
Ethernet IP Subnet Mask	The IP network mask of the 805U-E on its Ethernet port. This should be set to the IP address you require.
Wireless IP Address	The IP address of the 805U-E on the wireless port. If the unit is configured as a bridge this address will be the same as the Ethernet IP address. If configured as a router, the IP address must be different from the Ethernet IP Address - it must be consistent with the LAN it is connecting to on the wired side.
Wireless IP Subnet Mask	The network mask of the 805U-E on the radio port. If configured as a Bridge, this must be the same as the Ethernet IP Subnet Mask.
System Address	A 805U-E 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 and is normally automatically generated by the System Generator String.
Radio Encryption	Select "None", "64-bit" or "128 AES" security encryption of the wireless data. The default setting is "None".
Encryption Keys 1 to 4	These are the keys used to encrypt radio data to protect data from unwanted eavesdroppers. These keys must be set the same for all 805U-E units in the same system. If encryption is not selected, the Key values can be ignored.

	These keys will be automatically generated by the System Generator String - however the encryption keys can be manually changed. If they are manually changed, you need to make the same change to all modules in the system. Each of the fields are 5 bytes in length for 64-bit encryption and 4 bytes for 128-bit AES encryption. These keys must be entered as hexadecimal numbers separated by colons. For example, 12:AB:EF:00:56. for 64bit encryption, and 12:AB:EF:00 for 128bit AES encryption Encryption keys must not be all zeros, ie 00:00:00:00:00 64bit encryption uses each keys alternatively for each radio packet. 128bit AES encryption combines these keys to form a single 128bit key, used on all radio packets.
Save and Reboot.	Save settings to non-volatile memory, and reboot 805U-E.

3.6 Ethernet Data

All Ethernet devices are uniquely identified by a MAC Address that identifies the hardware device. These addresses are factory-set and are six bytes in size and are expressed in hexadecimal in the form *xx:xx:xx:xx:xx:xx*

Ethernet messages can be addressed to a single device (a point-to-point message) or can be directed towards multiple destinations by using Multicast addresses and Broadcast addresses. The broadcast address is used to send data to all devices. The broadcast address is FF:FF:FF:FF:FF:FF.

Multicast addresses are used to direct data at a set of devices. Multicast addresses may be recognized as they are always have the least significant bit of the first byte of the MAC Address set. For example, 0**1**:00:5E:00:00:00 is a multicast address, 0**1**:80:C2:00:00:00 is also a multicast address.

3.7 Normal Operation

After addresses are configured, the units are ready for operation.

Refer to section 1 for an explanation on the operation of a Bridge and Router.

Transparent Bridge Operation

Bridges are typically used to connect sections of the same IP network together.

By default, the 805U-E is configured as a transparent bridge. When a transparent bridge is started, it learns the location of other devices by monitoring the source 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 805U-E can be unnecessarily overburdened. Filtering may be used to reduce broadcast traffic sent over the radio. Refer Section 3.10 for how to configure a filter.

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 using the Spanning Tree Algorithm function - refer to section 3.9.

Router Operation

A router joins separate Ethernet networks together. The router has different IP addresses on its wired and wireless ports, reflecting the different IP addresses of the separate Ethernet networks. All the devices in the 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 at 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 can not 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.

The 805U-E has one routing rule which may be configured. This routing rule is the gateway address. The 805U-E will direct all unknown IP network traffic to this gateway IP address.

3.8 Fixed Frequency Operation

The 805U-E operates on the 869MHz band. The modules are designed to be fixed frequency in accordance with European regulations. The 869MHz Band is split into different bands with varying duty cycle and power limits. Generally the 2 bands used by Elpro are

500mW	869.525MHz	0.dB gain	10% Duty Cycle
5mW	869.275MHz	0dB gain	100% Duty Cycle

EC regulations are designed to either limit

a) the time a radio can transmit, giving other systems a chance to operate, and

b) the range of a radio, allowing more systems in a given area.

3.9 Radio Configuration Menu

The 805U-E can be configured to different radio transmission rates. A reduction in rate increases the reliable range (transmission distance). An “automatic rate” function is provided which automatically selects the highest data rate for reliable operation. This feature starts at the highest rate and reduces rate if the received radio signal strength is below a user-configurable limit.

The factory-default settings for the radio port will be correct for the majority of applications. Only make changes if you experience operating problems.

Select the "Radio" Menu to change the following configuration parameters. If a change is made, you need to select "Apply Changes and Save" to retain the changes.

Power Level	The RF power level is selectable between 500mW (27dBm) and 50mW (17dBm). The default value is 500mW.
Data Rate	The radio baud rate in bits per second (bps). The data rate can be configured to a fixed rate up to 76.8 Kbps, or set to "Auto". The default value is Auto. In Auto mode, the 805U-E will automatically adjust the data rate to the fastest rate for reliable operation in each radio path.
Fade Margin This is the difference (in dB) between the received radio signal and the receiver sensitivity (minimum radio signal).	When automatic rate is selected, the 805U-E initially chooses a rate based on the received signal strength of transmissions. Firmware version 1.32 and later will then adjust rate on each channel to according to packet errors. Earlier versions will adjust rate based upon the received signal strength. The Fade Margin value is used by the 805U-E to determine what initial data rate should be selected. In firmware versions before v1.32, it is also used to select the current radio rate. A larger Fade Margin means that the 805U-E will select a lower initial rate. The default value is 10 dB.
Beacon Period This interval is the period between beacon transmissions sent by an Access Point.	The Beacon Interval is also related to the scan period on a Client. Re-association interval is (6) times the Beacon Interval when the link has been inactive. Access Points will timeout after 12 times the Beacon Interval if no response is heard. Refer to Section 3.1 for more information. The default value is 10 seconds. This should be adjusted to larger values as the system is increased in size. This will reduce the overhead of checking each link, at the expense of response time when a link is dropped.
Fragmentation Threshold The maximum transmission unit (MTU) of data over the radio.	This selects the maximum number of bytes that will be transmitted in one message. If more than this number of bytes is input into the 805U-E, the module will transmit more than one message. The default value is 500 bytes. If fixed radio rates are configured, this value can be increased and will reduce radio transmission overhead. For 76.8 Kbps , the fragmentation threshold can be increased to 2000, and at 38.4Kbps, to 1000. However if the radio path is poor, or there is high radio interference, increasing this value will decrease system performance as the number of re-try messages will increase. If Ethernet traffic is only small packets sizes (ie <300 bytes), an improvement in overall throughput rate can be achieved by reducing MTU size. This improvement is achieved through a reduction in the retry holdoff time required for units in the system. As packets in the

	system are smaller, units will holdoff for shorter periods of time and be confident that their retry transmission will not cause interference with other units.
RSSI Threshold The received signal strength level at which beacons from Access Points are to be ignored.	This should be used to prevent Clients and Access Points establishing links beyond a sustainable range. The default value is set below the noise floor at -150 dBm. This allows all messages received to be processed. If a value of –90 is entered, any beacons weaker than –90dBm will be ignored, resulting in the link eventually resetting if the radio path continues at less than –90.
Contention Window Size The number of time slots allocated by the Access Point.	The Access Point allocates a "time slot" to each Client, to minimise transmission contention between Clients. Each Client can only transmit during its allocated time slot. The width of each time slot varies from 7msec to 12 msec depending on the Beacon time – the time slot is 5msec at the shortest Beacon and 12 msec at the longest beacon. The number of time slots can be manually set (1 to 8) or a value of zero (default) allows the Access Point to automatically determine the number of time slots, which it does based on the number of Clients connected. If there are more than 8 Clients, then more than one Client is allocated to some time slots. In a large system where there is inherently little transmission overlap (such as in a polling system), then manually setting the Contention Window size to a smaller number than 8 will increase the overall data rate.
Duty Cycle Alarm Threshold Duty cycle alarm activation point	In CE countries, the 869.4 MHz 500mW band has a regulated transmit duty factor of 10%. The Access Point calculates the system duty cycle and will set an internal alarm flag if the actual duty cycle exceeds this parameter. Refer to more information on Duty Cycle calculations at the end of this section. The internal alarm flag can be configured to drop to wireless link or to set the digital output channel (refer Digital I/O configuration). Default value is 10%.
Duty Cycle Alarm Minimum	The internal alarm flag will reset when the actual duty cycle drops below this value - default value is 9%.
Duty Interval	The time period over which the duty cycle is calculated - default is 60 minutes
Current Duty Cycle Achieved	A display of the current duty cycle value.
Drop Radio Link on Duty Cycle Alarm	Allows the internal duty cycle alarm to force the Access Point to reduce radio activity. The Access Point will disassociate from all Client units and will not allow re-association until the duty cycle alarm resets. Default value is "not selected".
Fallback Probation Counter	When data rate is reduced automatically due to poor signal, the module may attempt to increase back to the higher rate after the specified number of successful transmissions have been made.

Drop Link On Retry Threshold	When enabled, the module will drop radio link if all retries for sending a packet fails. When disabled, the module will only drop link on failure of regular link check transmissions, sent regularly on inactivity of 6 times the beacon interval. Disabling this item can improve usability of poor radio paths.
Coexist Mode	When enabled, the module will holdoff retries longer to avoid interfering with module outside radio range. When disabled on an AP, the AP will shuffle retries with packets destined for other modules. When disabled on a Client, the module will reduce delay between retries.
Apply Changes	Update settings.
Apply Changes and Save	Update settings and save to non-volatile memory.

3.9.1 Duty Cycle Calculations

CE radio regulations limit the transmit duty cycle of the 869.525MHz 500mW channel to 10%. That is, the total transmission time of the radio system should be less than 10% of the total time.

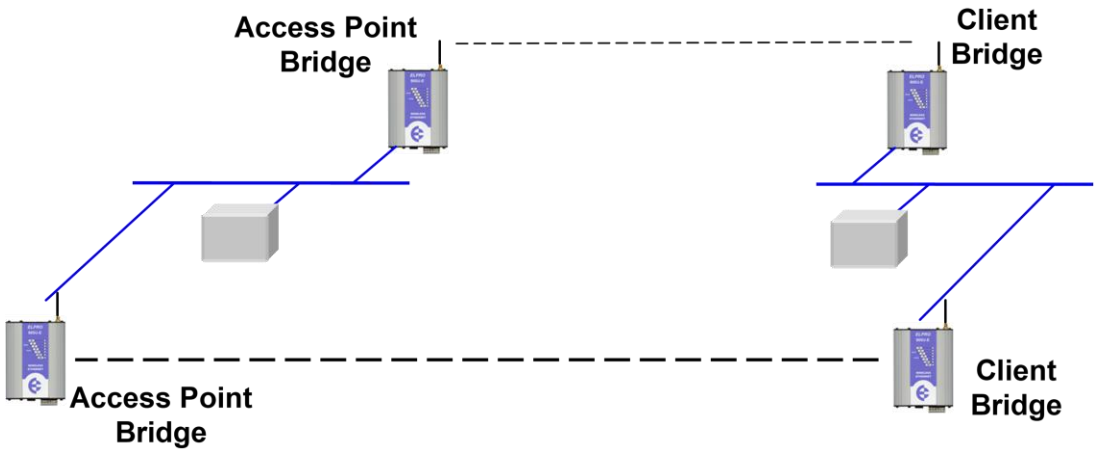
The Access Point calculates the duty cycle, and provides an internal alarm flag if the calculated duty cycle exceeds the user-configured setpoint value (default value is 10%). The alarm flag will reset when the duty cycle drops below a user-configurable "minimum value" (default 9%). The internal flag can be used to automatically reset the wireless links between the Access Points and Clients to avoid duty cycle exceeded the configured limit - this feature needs to be configured by the user; the default setting is "no automatic reset". The calculated duty cycle can also be viewed.

The duty cycle is calculated over a duty interval period which is also user-configurable (default is 60 minutes). The transmission time for each 5 second block is stored. The duty cycle is calculated every 5 seconds by summing the transmission times over the interval period and expressing this as a percent of the interval period. For example, if the interval period is 60 minutes, then the duty cycle is the sum of the transmit times in the most recent 720 x 5-sec blocks, divided by the interval period.

A calculated duty cycle of 10% indicates that the total transmission time has reached 360 seconds in the previous 60 minutes.

3.10 Spanning Tree Algorithm / Redundancy

The "Spanning Tree Algorithm" function was introduced to handle network loops and provide redundant paths in networks. The Spanning Tree Algorithm can be configured, however the factory default setting is "disabled".



For example, consider this network with a redundant wireless link. If the Spanning Tree Algorithm function 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.

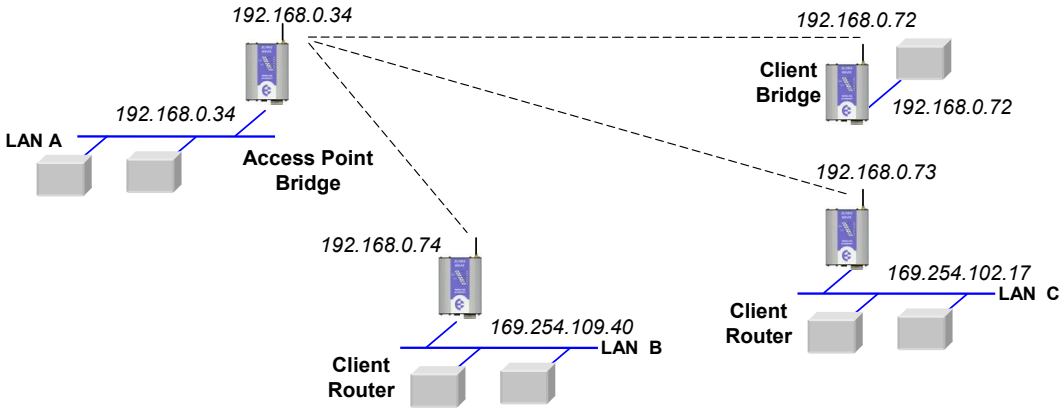
The Spanning Tree Algorithm implemented is IEEE 802.1d compatible. The algorithm forms a loop-free network by blocking traffic between redundant links in the network. These blocked links are placed in a standby condition, and may be automatically enabled to repair the network if another link is lost. 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 with the lowest priority configured (0) will become the root node in the network, and will direct traffic between each of its branches. The root node is typically the unit that handles the majority of traffic in the network. As a low bandwidth radio device, the 805U-E is configured with a Bridge Priority of (255) by default. The intention is reduce traffic that the 805U-E must handle, by placing it at the branch level in the network tree. As a branch, the 805U-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.

3.11 Routing Rules

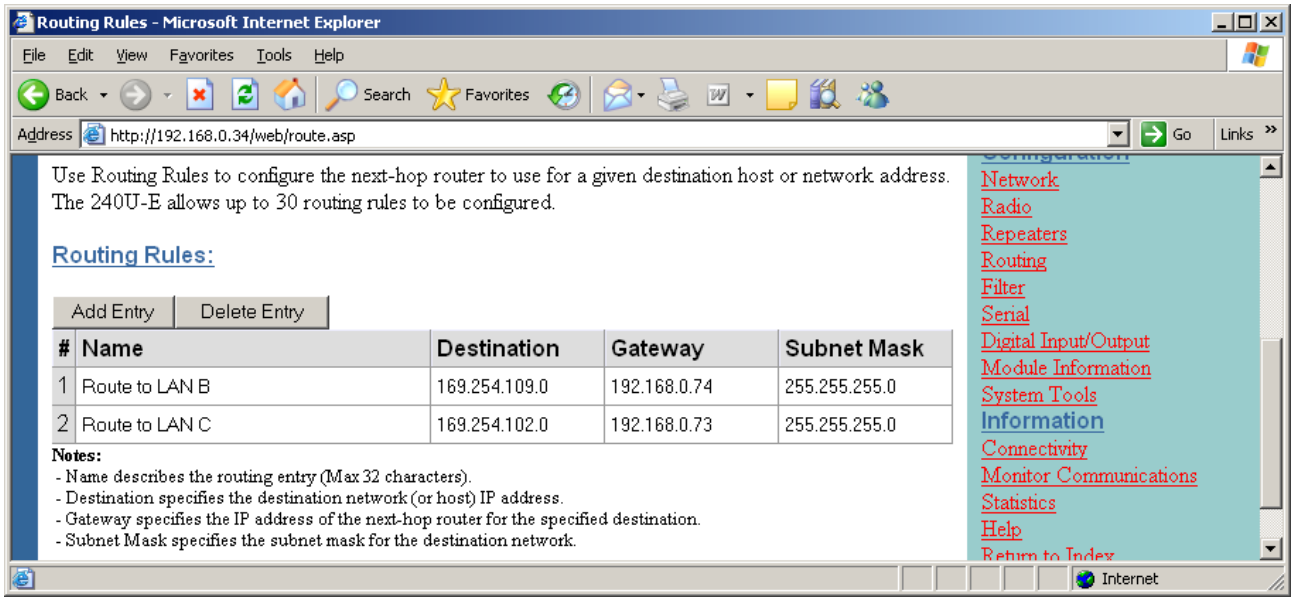
When a 805U-E receives an IP frame that is destined for an IP address on a different network, it checks if the network address matches the network address of one of its own interfaces (i.e. hard wired Ethernet, or wireless Ethernet, or PPP) and forwards the frame appropriately. However, if the IP network address does not match any of its interfaces, the 805U-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 805U-E routers). If more than one “next-hop router” is required, the 805U-E allows for up to 30 *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).



The above network diagram illustrates a situation where routing rules may need to be configured. In this example, the 805U-E clients need only specify the Access Point as their default gateway (i.e. they require no routing rules 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 805U-E client/routers as next-hop routers (i.e. gateways) to networks B and C. Note that devices on LAN A should specify the 805U-E Access Point as their default gateway. An alternative to adding routing rules to the 805U-E in this example would be for each device on LAN A that needs to communicate with LANs B and C to independently have routing rules specifying the 805U-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. 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 805U-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 805U-E at LAN B.



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 805U-E. The table below summarises the configurable parameters a routing rule.

Name	A name to describe 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 a class C IP address 192.168.0.0 would specify a destination network, while 192.168.0.16 specifies a destination host).
Gateway	The IP address of the next-hop router for the specified destination.
Subnet Mask	The subnet mask for the destination network.

3.12 Wireless Message Filtering

When configured as a Bridge, the 805U-E will transmit all broadcast messages appearing at its wired Ethernet port. When the 805U-E is configured as a Router, this does not occur.

In many cases, the intended recipient of the broadcast traffic does not lie at the opposite end of a proposed radio link. Reducing unnecessary broadcast traffic sent over the radio link, will increase available bandwidth for data. The 805U-E has a filtering feature to help reduce unnecessary wireless transmissions and enhance security.

The 805U-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 805U-E.

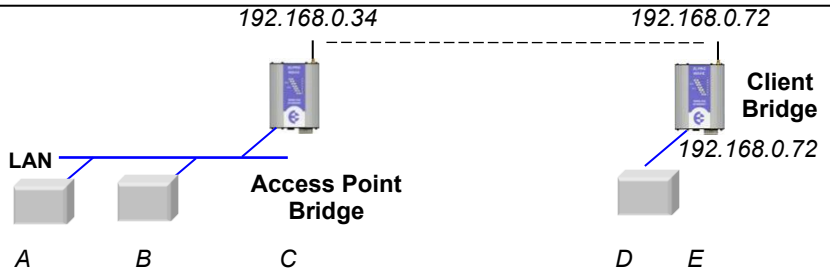
The Filter comprises of two lists: one of MAC Addresses and another listing IP protocol details. Each list may be set as either a blacklist (to block traffic for listed devices and protocols), or as a whitelist (to allow traffic for listed devices and protocols). The Filter operates on two rules listed below.

1. A Blacklist has priority over a whitelist. Traffic matching detail in a blacklist will be discarded if it also appears in a whitelist.

2. When one or both lists are whitelists, traffic must have matching detail in at least one of the whitelists for it to be passed. Note that, as this must agree with rule 1 above, the traffic detail must not match anything in a blacklist, if present, for it to be passed.

When configuring a Whitelist it is important to add the Addresses of all devices connected to the 805U-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 Ethereal program, will list broadcast traffic sent on the network.

In the example below, Computer B sees the computer D via Ethernet Modems C & E. The White Filtering requires that at Modem C has computer B in its white list, Modem E has



computer D in its Whitelist. Computer A will be not be able to access Computer D, as Computer A is not present in the Whitelist in Modem C.

It is advisable to use the Apply Changes button to test the configuration entered. Once the configuration is determined to be correct, the Apply Changes and Save button should be used. In the event that the configuration is incorrect, a power reset will revert the unit to previously saved configuration.

If an erroneous configuration has prevented all access to the module, SETUP mode may be used analyze what is wrong with the configuration. Simply switch the dipswitch to SETUP and cycle power. The 805U-E will retain its configuration, however will load up at IP address 192.168.0.1XX, netmask 255.255.255.0 with the radio and filter disabled. The *XX in the IP address* is the last two digits of the serial number. Configuration webpages will still show the original configuration. No changes are made to configuration until the user saves changes. To resume normal operation, set the dipswitch to RUN and cycle power.

MAC Address Filter Configuration:

Add Entries	Enter the MAC addresses of devices to be added to the list. Multiple entries must be separated by a semi-colon (;).
Delete Entries	Check the box alongside entries selected for removal from the list.
Whitelist or Blacklist	Check the box to make the list a whitelist. This will allow devices with the MAC addresses listed to communicate with the module and utilise the radio link. All other devices are blocked unless they exist in an IP whitelist. Uncheck the box to make the list a blacklist. This will prevent all listed devices from using accessing the module and using the radio link.
Apply Changes	Update settings.
Apply Changes and Save	Update settings and save to non-volatile memory.

IP Address Filter Configuration:

Add Entries	Enter the details of IP traffic to be added to the list. Protocols ARP, ICMP, TCP and UDP may be selected. Other IP protocols may be selected provided the IP protocol number within packets is known. TCP and UDP traffic may be also limited to specific port numbers.
Delete Entries	Check the delete box alongside entries selected for removal from the list. Alternatively, check the enable box alongside entries if you want to make the rule active.
Whitelist or Blacklist	Check the box to make the list a whitelist. This will only allow traffic described in the list to be sent over the radio link. All other traffic is blocked unless it is present in a MAC whitelist. Uncheck the box to make the list a blacklist. This will ban all traffic described in the list from being sent to the module or over the radio link.
Apply Changes	Update settings.
Apply Changes and Save	Update settings and save to non-volatile memory.

NOTE: When configuring a TCP filter it is often desirable to also configure both an ARP and an ICMP filter for the same IP Address range. The ARP filter is required whenever the sending device does not have a fixed IP to MAC Address translation table entry (i.e. whenever the device may need to send an ARP request to determine the MAC address of a device with a known IP Address). An ICMP filter is needed to allow/disallow “pings”.

3.13 Serial Port Configuration

The 805U-E has an RS-232, and RS-485 port for serial communications. These ports may be used for different purposes. The 805U-E offers three different serial functions which are PPP server, Serial Gateway, and Modbus TCP to RTU server.

3.12.1 RS-232 PPP Server

The 805U-E can be used as a PPP Server to connect the wireless Ethernet system to serial devices via the RS232 or RS485 serial ports.

PPP Server enables a network connection to the 805U-E over a serial cable. This is much like dial up internet. The maximum serial data rate is 38.4Kb/s. Hardware or Software flow control may be selected.

With minimal configuration on the PC, you may use Dial up networking in Windows XP to connect to the network via the serial port.

For the 805U-E, users must configure the local IP address for the 805U-E and the remote device IP address. Some care must be taken in selecting these IP addresses.

If you wish to use routing over this serial network connection, then the IP addresses selected must not lie on Wireless or Wired Ethernet networks already configured into the device. You must ensure they set routing rules appropriately for devices either side of the network.

If you want the serial device visible as present on the Wireless or Wired network, then the local IP address must be the same as the IP address set for the desired port. A process called "Proxy ARP" is used to make the device visible on the network. In this process, the 805U-E pretends that it holds the IP address on the network, and responds on behalf of the remote device.

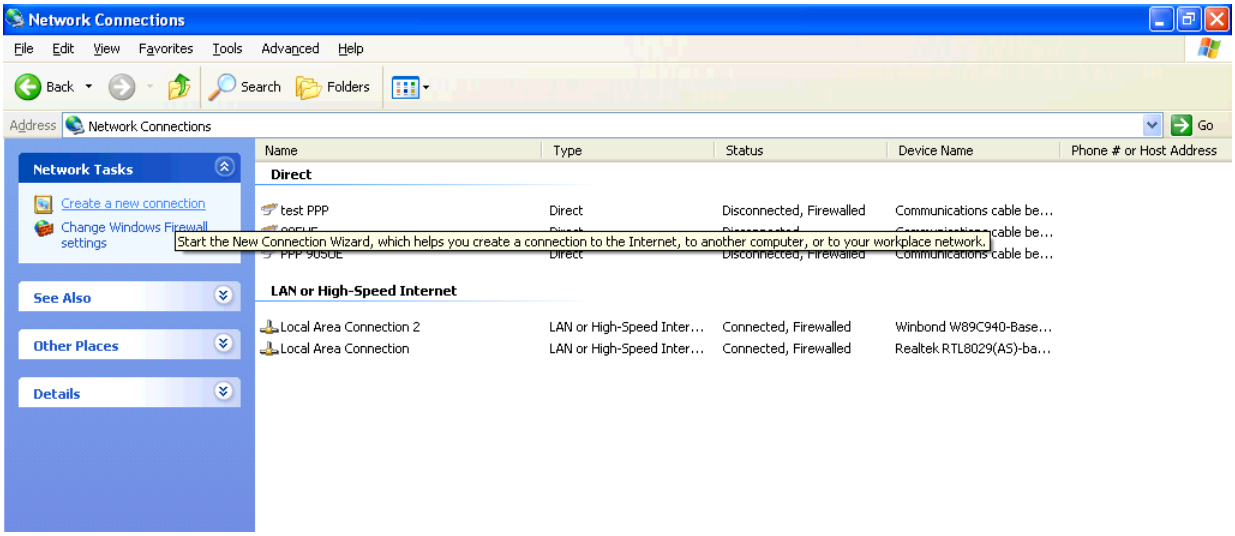
The result of this is similar to bridging for a single device, with some exceptions. One of these exceptions is the inability to handle name server searches of the network via this serial link. For example, you would encounter difficulty if you were to use Windows Explorer over the serial link to find a PC on the wired network. For this to operate correctly you must explicitly map computer names to IP addresses in the "LMHOSTS" file on your PC.

When in SETUP mode, the 805U-E PPP server is enabled. This may also be used to configure the module. Settings whilst in SETUP mode are as follows:

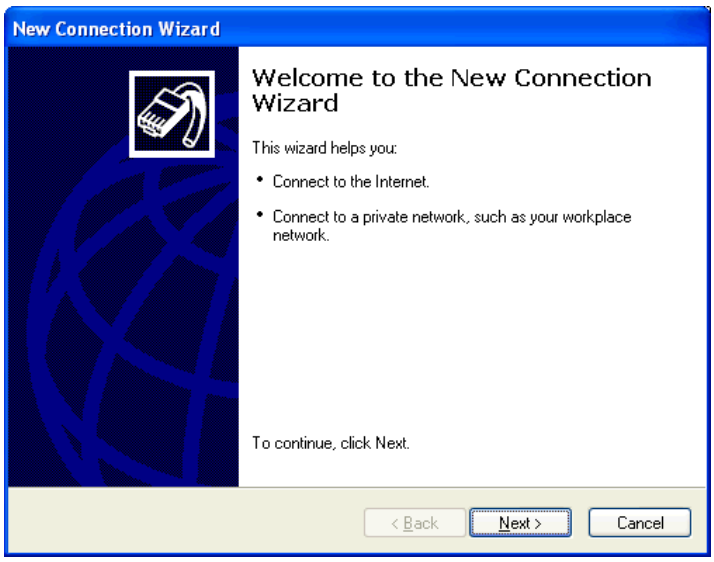
- username *user*, password is *user*.
- Serial baud rate 38400bps
- Hardware flow control
- Local address 192.168.123.123
- Remote address 192.168.123.124

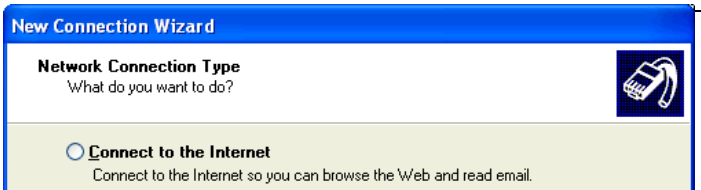
To configure Windows XP to establish a PPP connection to a 805U-E in SETUP mode, follow these steps:

1. On Network Connections in Windows XP, select Create a new connection



2. On the New Connection Wizard, click Next





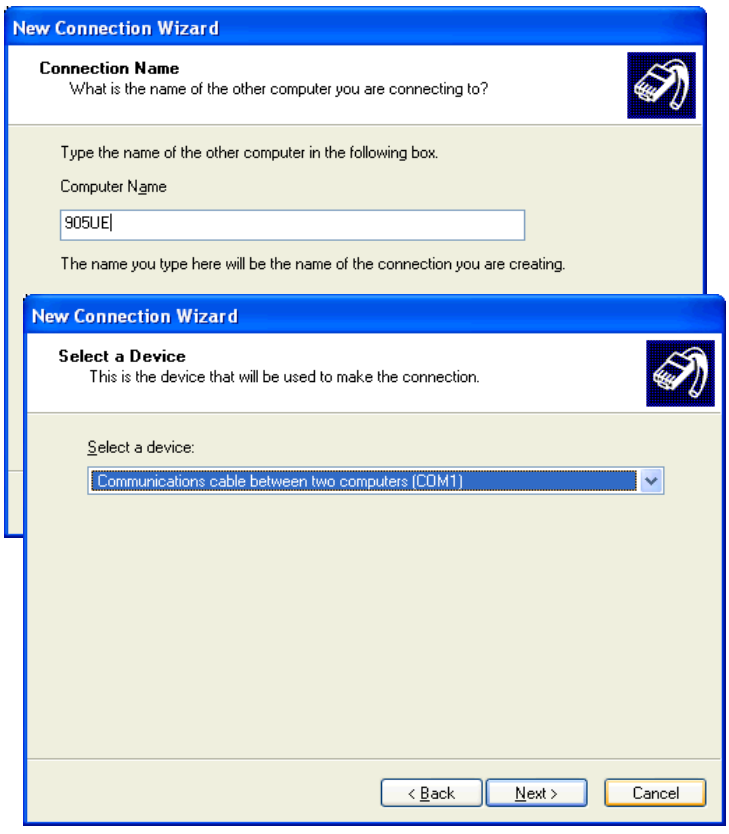
3. Set up an advanced connection

4. Connect directly to another computer

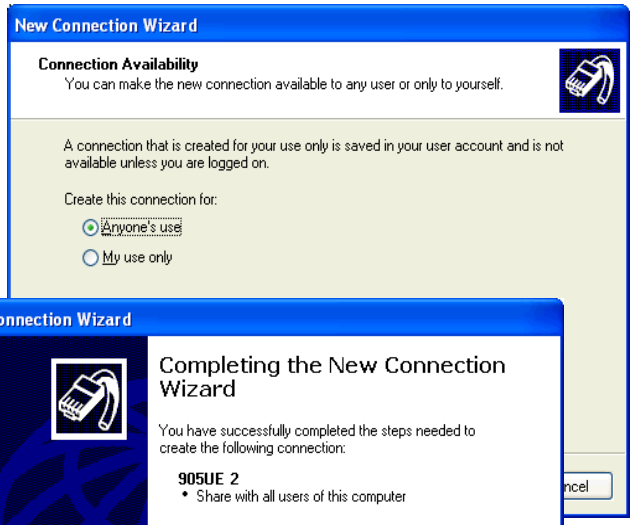
5. Set PC as guest

6. Set Computer name as something…

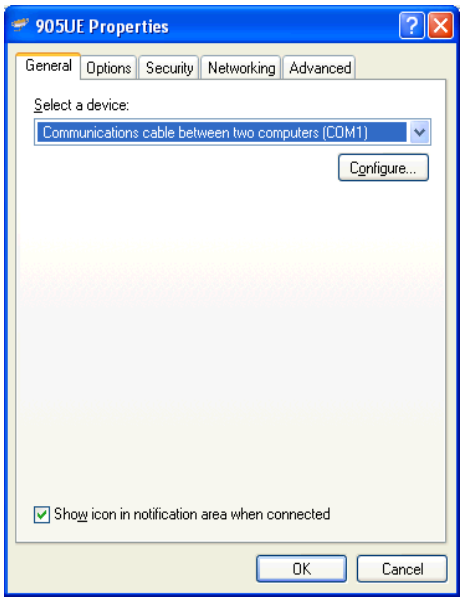
7. Select a COM port



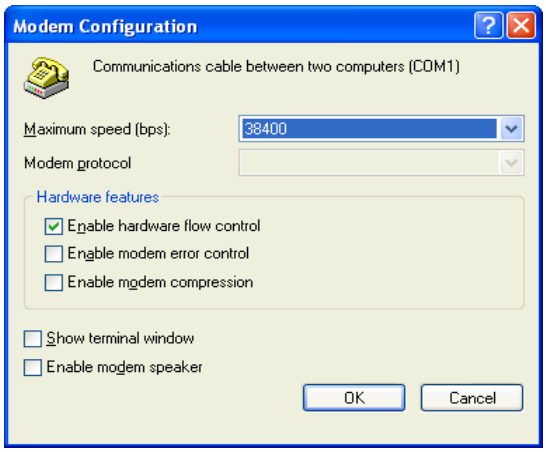
8. Select who can access this connection



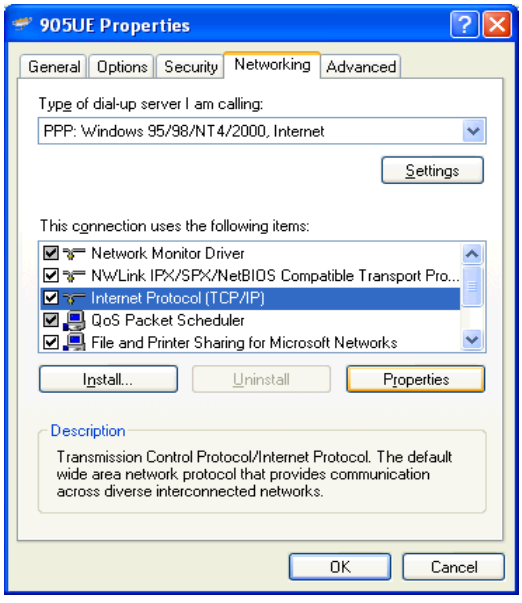
9. Click Finish



10. Select properties of this new connection by right clicking on connection.
11. General Tab click on Configure button

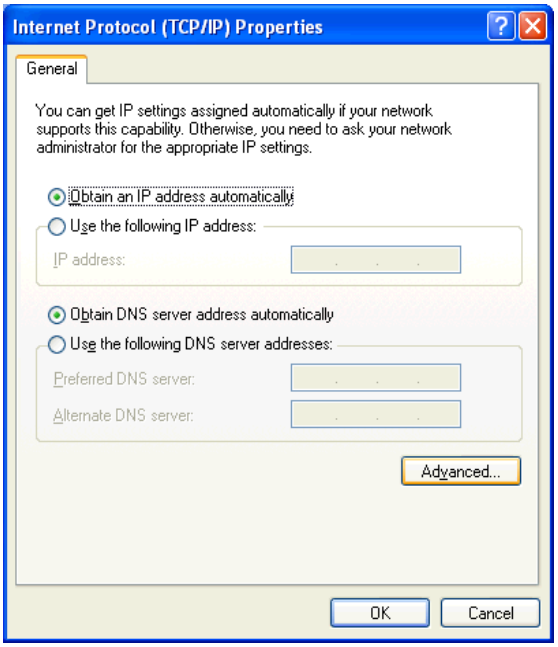


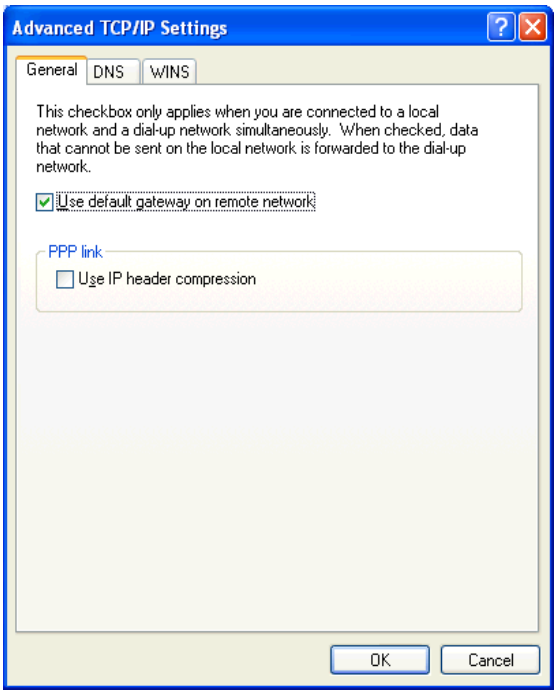
12. Ensure maximum speed is 38400bps, click OK



13. Select Networking Tab -> click on Internet Protocol (TCP/IP) in list box and then click Properties button.

14. On Properties form click Advanced button





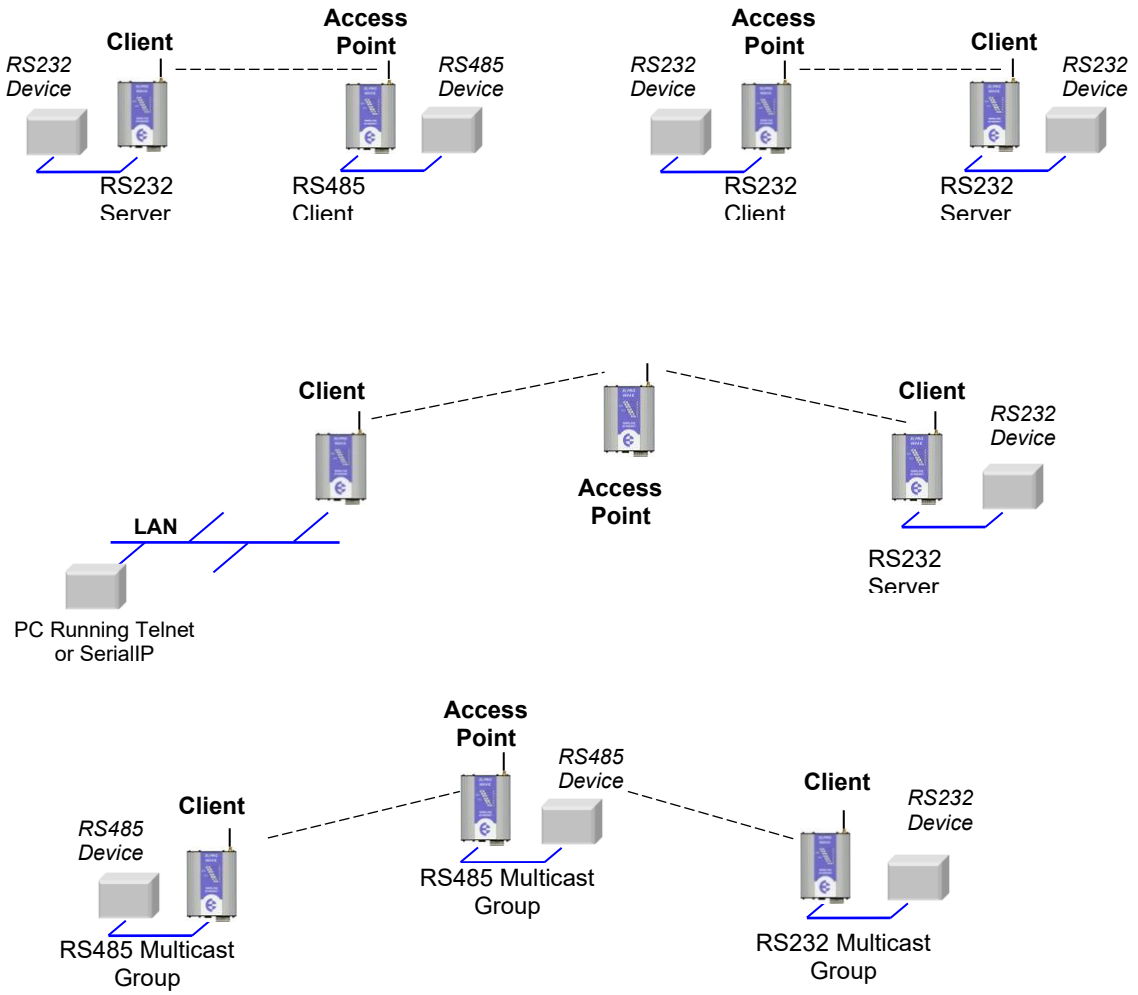
15. On Advanced TCP/IP Settings form->General Tab, uncheck field in PPP link stating "Use IP header compression".
16. Configuration is now complete. Click on this newly created link to establish a connection to 805U-E.
17. Ensure both the username and the password are entered exactly as configured in 805U-E. (When booted in SETUP mode, the PPP server has username “user” and password “user”.)

3.12.2 Serial Gateway

Serial Gateway functionality is available for both RS-232 and RS-485 ports independently, and enables serial data to be routed via the wired or wireless network connection. Serial Gateway functionality is similar to radio modem functionality, allowing point-to-point and multipoint serial data transfer.

Each 805U-E serial port may be configured as Server, Client, or Multicast Group. When configured as Server, the module will wait for a connection to be initiated by a remote client. When configured as Client, the module will automatically attempt to connect to the specified remote server. When configured as Multicast Group, the module will broadcast data to all members of the same Multicast Group.

Some of the possible Serial Gateway topologies are illustrated below. As can be seen, it is possible for serial data from a 805U-E to be transferred to one or more 805U-E serial ports, or to be encapsulated within a TCP/IP socket for availability on an Ethernet network. Conversely, data encapsulated in a TCP/IP socket can be reproduced at a 805U-E serial port. Both 805U-E serial ports and the hard wired Ethernet port can be in use at the same time.



There are software packages available (i.e. SerialIP Redirector by Tactical Software) that can create a virtual serial port on a PC. This virtual serial port can be configured to connect to a 805U-E serial port. Standard programs can then be used to access this serial port as if it were actually connected to the PC. Alternatively the program telnet may be used to connect to a serial port on the 805U-E. The telnet command used should be:

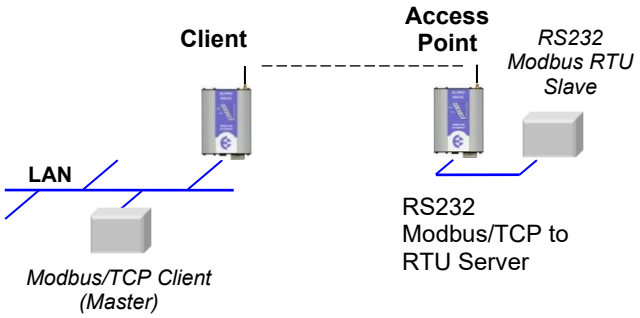
TELNET *[IP address] [Listen Port]*

eg. TELNET 192.168.0.155 23 where the *IP address* is 192.168.0.155 and *Listen Port* is 23.

Enable RS-232 PPP Server	Check this box to enable the PPP network server on the RS-232 port.
Enable RS-485 Serial Gateway	Check this box to enable the Serial Gateway Server on the RS-485 port.
Data Rate	The serial data rate desired. Serial data rates available range from 110bps to a maximum of 230,400bps.
Data Bits Parity Stop Bits	The data format desired. Data formats of 8N1, 7E1, 7O1, 7E2, 7O2 are supported.
Character Timeout	Enter the maximum delay (in msec) between received serial characters before packet is sent via network.
Server	When configured as Server, the module will wait for a connection to be initiated by a remote client
Listen Port	Server Only. Enter the TCP port number on which the server must listen for incoming connections. The standard TELNET port is 23.
Client	When configured as Client, the module will automatically attempt to connect to the specified remote server
Remote Device Port	Client only. Enter the TCP port number of the remote server (i.e. the remote port to automatically connect to).
Remote Device IP Address	Client only. Enter the IP Address of the remote server (i.e. the remote IP Address to automatically connect to).
Multicast Group Port	Enter the UDP port number that all members of the group will use (i.e. all group members should use the same port number).
Multicast Group IP	Enter a valid Multicast IP Address identifying the group (i.e. all group members should use the same Multicast Group IP Address). Valid Multicast IP Addresses are in the range 224.0.1.0 to 238.255.255.255.

3.12.3 Modbus TCP to RTU Server

The Modbus TCP to RTU Server allows an Ethernet Modbus/TCP Client (Master) to communicate with a serial Modbus RTU Slave. The 805U-E makes this possible by internally performing the necessary protocol conversion. The conversion is always performed by the 805U-E which is directly connected to the Modbus serial device (i.e. only this module needs to have Modbus TCP to RTU Server enabled).



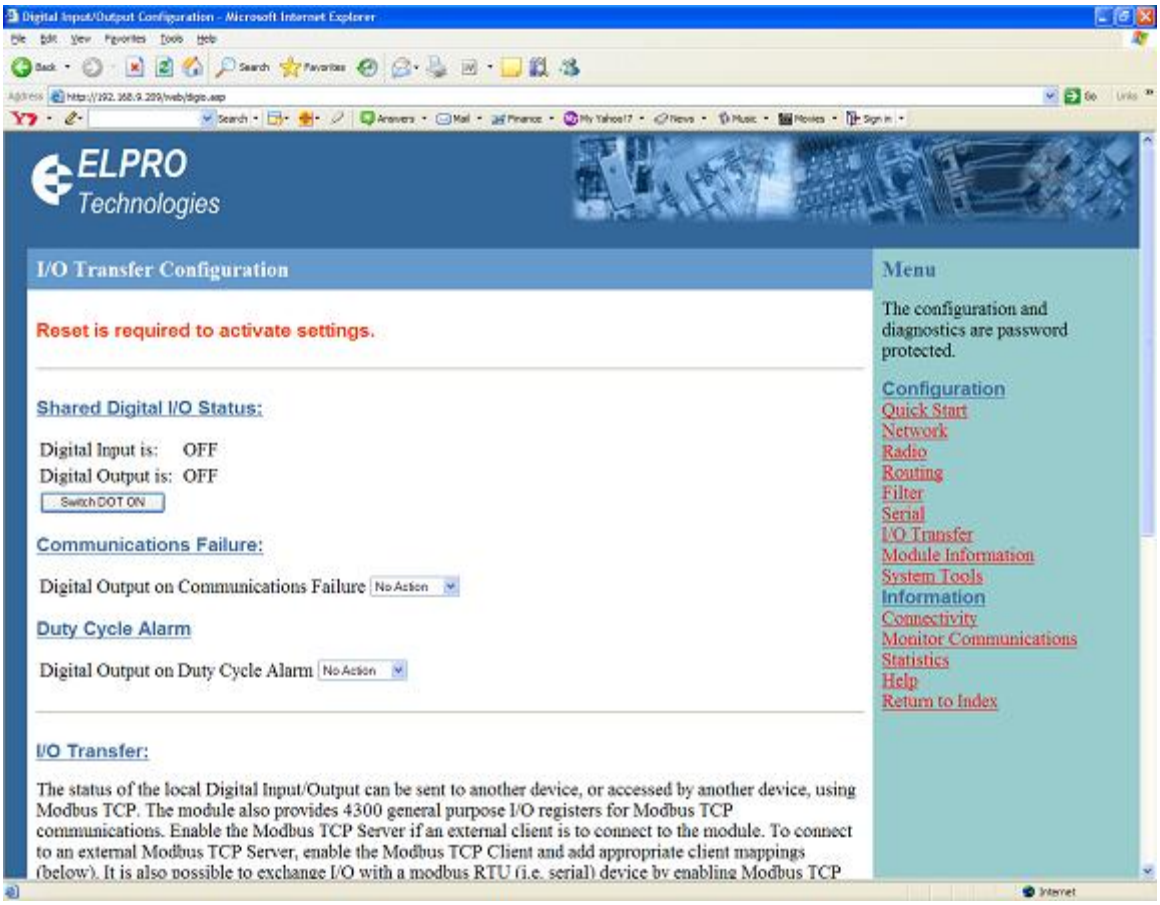
The above example demonstrates how a Modbus/TCP Client (Master) can connect to one or more Modbus RTU (i.e serial) Slaves. In this example the 805U-E Access Point is configured with the "RS232 Modbus/TCP to RTU Gateway" enabled. Once enabled, the gateway converts the Modbus/TCP queries received from the Master into Modbus RTU queries and forwards these over the RS232 port to the Slave. When the serial response to the query arrives from the Slave, it is converted to a Modbus/TCP response and forwarded via the network to the Modbus/TCP Master. If no response was received serially by the 805U-E within the configured Response Timeout, the 805U-E will initiate a number of retries specified by the configured Maximum Request Retries.

The Modbus TCP to RTU Server may be configured to operate on either the RS-232 or RS-485 port. It does not support operation on both ports at the same time.

Enable RS-232 Modbus TCP to RTU Gateway	Check this box to enable the Modbus TCP to RTU Server on the RS-232 port. Only a single serial port is allowed at a time.
Enable RS-485 Modbus TCP to RTU Gateway	Check this box to enable the Modbus TCP to RTU Server on the RS-485 port. Only a single serial port is allowed at a time.
Data Rate	The serial data rate desired. Serial data rates available range from 110bps to a maximum of 38,400bps.
Data Bits Parity Stop Bits	The data format desired. Data formats of 8N1, 7E1, 7O1, 7E2, 7O2 are supported.
Pause Between Requests	Enter the delay between serial request retries in milliseconds
Response Timeout	Enter the serial response timeout in milliseconds – a serial retry will be sent if a response is not received within this timeout.
Connection Timeout	Enter 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	Enter the maximum number of request retries performed serially.
Maximum Connections	Enter the maximum number of simultaneous TCP connections to the server allowed.

3.14 Digital Input/Output and I/O Transfer

In firmware versions v1.28 and earlier, the menu item was named Digital Input/Output. In later versions it was renamed I/O Transfer, due to enhanced functionality where units can send the status of the Digital Input to another module or Modbus device.



The shared Digital Input/Output pin may be monitored and set via the internal webpage. As this pin is shared, the Digital Input status will be ON when the Digital Output is set ON.

The Digital I/O channel can also be configured to provide a status output of the module communications. If the 805U-E disassociates from another unit (that is, there is no wireless link), you can configure the digital output to turn ON (set) or OFF (drop).

The configurable Digital I/O status and alarm options are summarized below.

Shared Digital I/O Status	The Digital I/O is a shared pin on the unit. As an output, it is similar to an open collector transistor. As an input, a short to ground is detected as ON. When the Digital Output is driven low, the Digital Input will detect an ON condition. By clicking on the button provided, the Digital Output may be switched ON and OFF, provided Communications Failure has previously been set to no action.
Digital Output on Communications Failure	The digital output can be configured here to perform various actions when a link is present. Select Set Output to drive the open collector output when there is no radio link. Select Drop Output to drive the open collector output when a radio link is present.
Duty Cycle Alarm	This field is visible only on Access Points. Select Set Output to drive the open collector output when Duty Cycle Alarm Threshold has been exceeded. Select Drop Output to drive the open collector output when Duty Cycle Alarm Threshold has NOT been exceeded.

The 805U-E also provides Modbus TCP Client and Modbus TCP Server functionality for I/O transfer. 5000 x 16bit general purpose registers are provided for Modbus (including the onboard Digital Input/Output) and are shared for both Client and Server. Modbus TCP Client (Master) and Modbus TCP Server (Slave) are both supported simultaneously, and when combined with the built in Modbus TCP to RTU Gateway the 805U-E can transfer I/O to/from almost any combination of Modbus TCP or RTU devices.

The layout of the I/O registers is summarized in the table below. Each register is internally saved as a 16 bit 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. The 16 bit status register contain the value FFFF(hex) for ON and 0000(hex) for OFF. Inverted status registers are also provided where the registers contain 0000(hex) for ON and FFFF(hex) for OFF.

Registers	Purpose
1 – 4299	General purpose I/O registers (read/write)
4300	On-board Digital Input value (read only)
4301	Reserved
4320	On-board Digital Output value (read/write)
4370	On-board Digital Input inverted value (read only)
4371-4999	Reserved for future use

Modbus TCP Client (Master) enables the 805U-E to connect to one or more Modbus TCP Servers (Slaves). All Modbus Master messages are directed either to/from the onboard I/O registers depending on configuration (described below). The Modbus TCP Client may also poll Modbus RTU (i.e. serial) devices connected to either the local serial port or a remote 805U-E serial port by enabling the Modbus TCP to RTU gateway at the corresponding serial

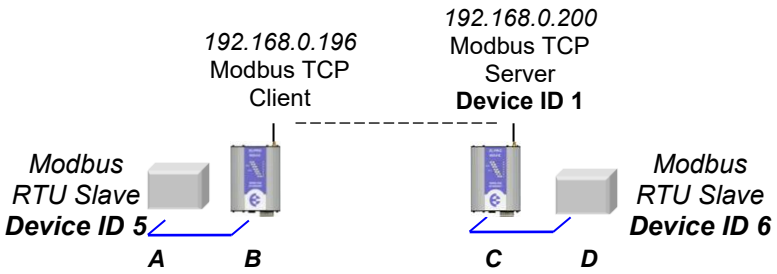
port (see section "3.13.3 Modbus TCP to RTU Gateway"). Modbus TCP Client functionality allows connections to a maximum of 5 different Modbus TCP Servers.

Modbus TCP Server (Client) enables the 805U-E to accept connections from one or more Modbus TCP Clients (Masters). All Modbus transactions routed to the onboard Modbus TCP Server are directed either to/from the onboard general purpose I/O registers. The Modbus TCP Server is shared with the Modbus TCP to RTU Gateway, 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.

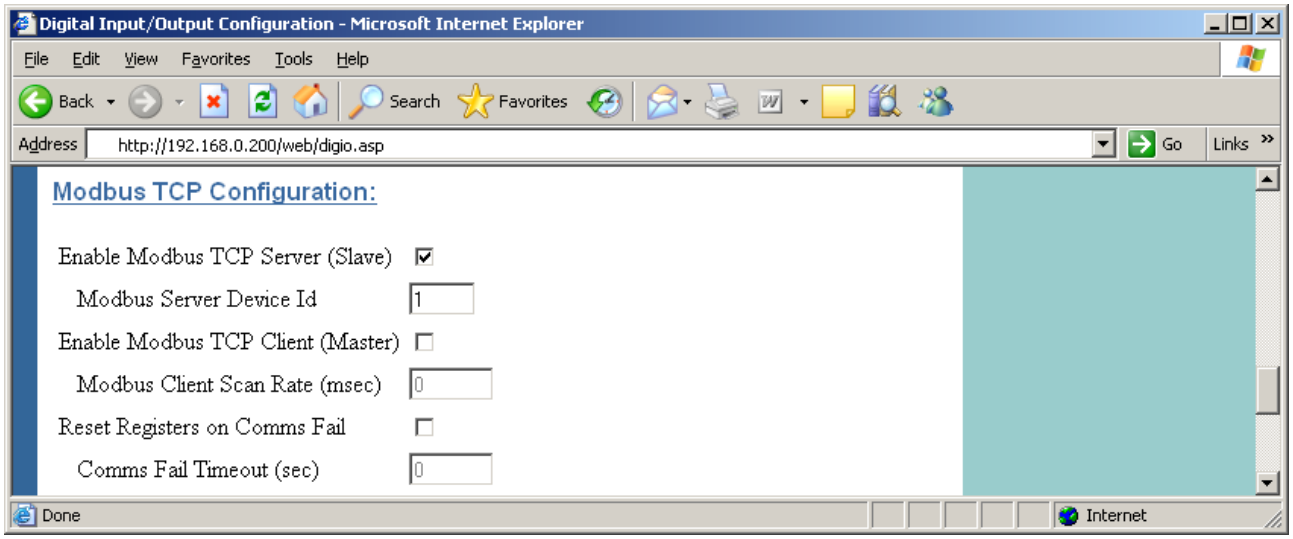
Modbus RTU (serial) Master functionality is achieved by combining the Modbus TCP Client (Master) and Modbus TCP to RTU Gateway. Simply specify a Modbus TCP Client (Master) connection to a Modbus TCP Server where the server is the address of any 805U-E with Modbus TCP to RTU Gateway enabled. Care should 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 805U-E that the serial device is connected to.

The 805U-E provides a configurable option to automatically reset the value of the onboard I/O registers to zero in the event of a communications failure. If a valid Modbus transaction directed to/from a given register has not been completed for longer than a configurable timeout, then the value of that register will be reset to zero.

An example of the Modbus functionality of the 805U-E is illustrated below. In this example the status of the onboard digital input at C will be reflected at the onboard digital output at B. Also, 8 I/O registers from Modbus serial device D will be transferred to A.

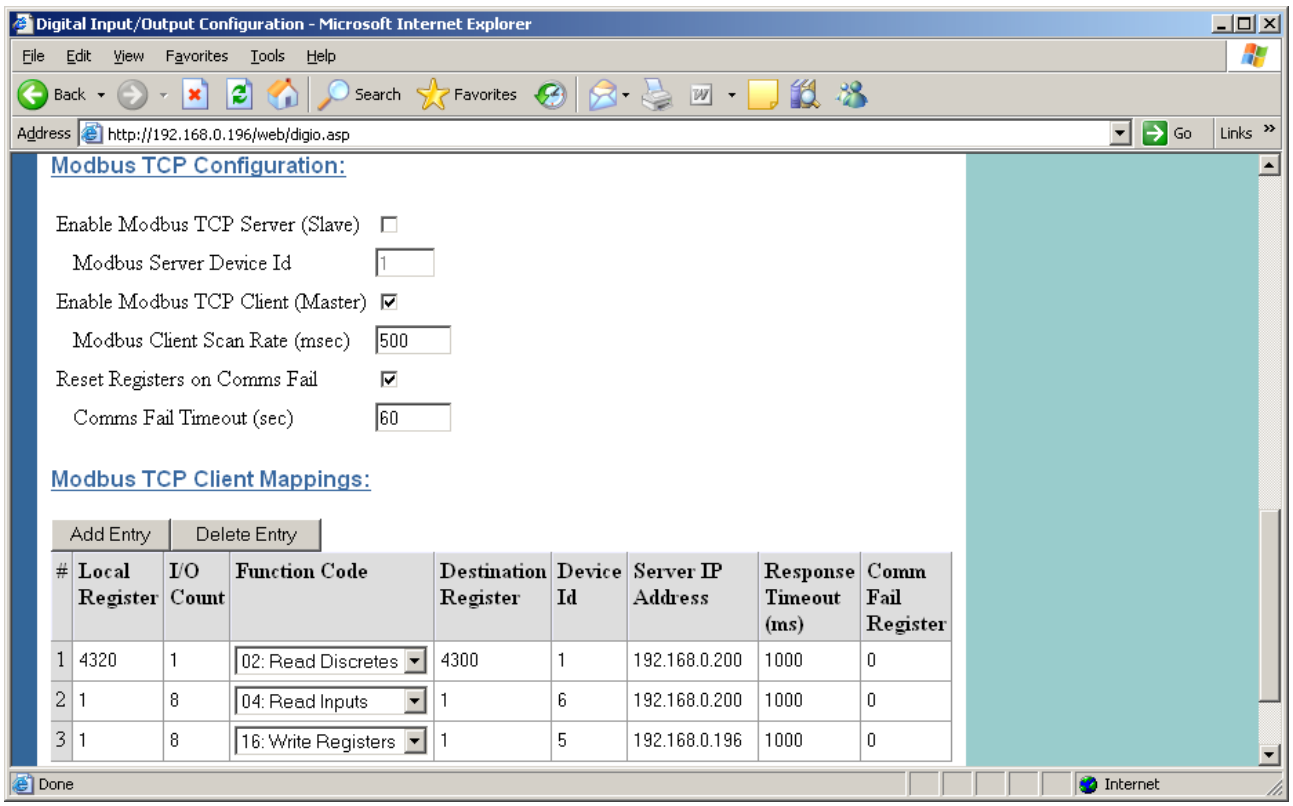


The Modbus configuration for unit C is shown below.



Unit C is configured with Modbus TCP Server enabled and Device ID = 1, so that the Modbus TCP Client at B can connect and read the status of the onboard digital input. Unit C also has Modbus TCP to RTU Gateway enabled (see section "3.13.3 Modbus TCP to RTU Gateway") so that the Modbus TCP Client at B can communicate with the serial Modbus RTU device D.

The configuration of unit B is shown below (accessible via the "I/O Transfer" configuration page).



It can be seen that Modbus TCP Client has been enabled with a 500msec scan rate, meaning that there will be a 500msec delay between each of the *mappings* directed at any server. The "Reset Registers on Comms Fail" option is enabled with a timeout of 60 seconds, indicating

that any of the registers at unit B will be reset if a successful Modbus transaction involving that register has not been executed in the last 60 seconds. The Modbus TCP to RTU Gateway at B must also be enabled (see section "3.13.3 Modbus TCP to RTU Gateway") to allow Modbus communications with the serial device A.

Three "Modbus TCP Client Mappings" are also configured at B in order to perform the required I/O transfer. The first mapping transfers the status of the onboard digital input at C to the onboard digital output at B. *Local Register* 4320 specifies the register for the onboard digital output at B (since B is the *local* unit at which the mapping is configured). *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* 4300 specifies the register for the onboard digital input at unit C (since C is the *destination* unit for this mapping). *Device ID* 1is 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. *Response Timeout* 1000 ms 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.

The second mapping reads 8 registers from serial unit D into onboard registers in unit B. Note that in this case the specified Device ID 6 is the Modbus Address of the serial device D, while the Server IP Address 192.168.0.200 is the IP Address of unit C since the Modbus TCP to RTU Gateway at unit C converts the Modbus TCP message to Modbus RTU and routes it out the serial port to unit D.

The third mapping takes the 8 registers read by the second mapping and writes them to the serial unit A. The specified Device ID 5 is the Modbus Address of the serial device A, and the Server IP Address 192.168.0.196 is the IP Address of the local unit B since the local Modbus TCP to RTU Gateway is to route the message out the serial port to unit A.

Since the 805U-E supports Modbus TCP Client and Server simultaneously, the Modbus TCP Server for unit B above could also be enabled. This would allow one (or more) external Modbus TCP Clients anywhere on the extended wired or wireless network to connect to unit B and monitor the status of the I/O registers – including the I/O at units A, C, and D. This is a very powerful and flexible feature which could, for example, be exploited by a central monitoring facility or SCADA.

The configurable Modbus I/O transfer options are summarized in the tables below.

Modbus TCP Configuration:

Enable Modbus TCP Server (Slave)	Check this box to enable the onboard Modbus TCP Server. All Modbus TCP connections to the module IP Address and specified Modbus Server Device ID will be routed to the onboard I/O registers.
Modbus Server Device ID	Specify the Modbus Device ID for the onboard Modbus TCP Server. Allowed values are 0 to 255.
Enable Modbus TCP Client (Master)	Check this box to enable the onboard Modbus TCP Client. I/O to be transferred via the Modbus TCP client is specified with Modbus TCP Client Mappings.
Modbus Client Scan Rate	Enter the delay (in milliseconds) between execution of consecutive Modbus TCP Client Mappings to the same Server.
Reset Registers on Comm's Fail	When Enabled the value in any onboard I/O register will be reset to zero if a valid Modbus transaction directed to/from the given register has not been completed for longer than the Comms Fail Timeout.
Comms Fail Timeout	The period of time after which onboard I/O registers will be reset if a valid Modbus transaction directed at that register has not completed.

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

3.15 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 root webpage of the 805U-E.

Password Configuration password.	When changing the password on this screen, it will be sent unencrypted over any wired network. If encryption is enabled on the 805U-E, any radio communications are encrypted, and therefore hidden from radio eavesdroppers. Caution must only be taken if there are potential eavesdroppers on the wired network.
Device Name	A text field if you wish to label the particular 805U-E.
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 805U-E.

3.16 Remote Configuration

Because a module configuration is viewed and changed in a web format (which is an Ethernet application), you can view or change the configuration of a remote module via the wireless link, provided the remote module is already "linked" to the local 805U-E.

To perform remote configuration, connect a PC to the local module, run Internet Explorer and enter the IP address of the remote unit - the configuration page of the remote module will be shown and changes can be made. If the remote module is configured as a Router, enter the wireless IP address of the router, not the Ethernet address.

Care must be taken if modifying the configuration of a module remotely. If the Radio Configuration is changed, some changes made may cause loss of the radio link, and therefore the network connection.

It is advisable to determine path of the links to the modules you wish to modify, and draw a tree diagram if necessary. Modify the modules at the "leaves" of your tree diagram. These will be the furthest away from your connection point in terms of the number of radio or Ethernet links.

In a simple system, this usually means modifying the Client modules first and the Access Point last.

3.17 Configuration Examples

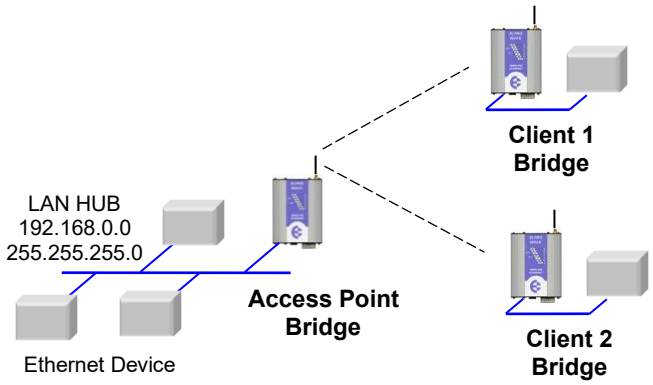
Setting a 805U-E to Factory Default Settings

Access configuration webpages of 805U-E. Refer section *Accessing Configuration inside a module for the first time*, or *Modifying an existing configuration*.

1. Click on System Tools Menu Item
2. Enter username “user” and password “user”, when prompted for password.

Click on Factory Default Configuration Reset, and wait for unit to reset. When reset, the LINK LED will flash.

Extending a wired network



Access Point Configuration

Connect straight through Ethernet cable between PC and 805U-E.

- Ensure configuration PC and 805U-E are setup to communicate on the same network
- Set dipswitch to SETUP mode.
- Power up unit, and wait for LINK 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 http://192.168.0.1XX/ where XX is the last two digits of the serial number

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

  Enter “Quick Start”, and select Access Point.

  Change the IP address to 192.168.0.200

  Enter a System Generator String

  Select the Radio Encryption required.

  Set dipswitch to RUN

  Save the changes and unit will restart with new settings.

Alternate procedure – Adjust 805U-E network settings using serial port(assuming configuration PC is on existing network)

a) Open terminal program with settings with data rate 19200bps, 8 data bits, 1 stop bit and no parity.

b) Set dipswitch to SETUP

c) Connect straight through serial cable to 805U-E and power up unit.

d) When prompted, strike the Enter key to abort automatic boot

e) Set IP address of 805U-E to 192.168.0.200 with command bip 192.168.0.200

f) Set netmask of 805U-E to 192.168.0.200 with command bnm 255.255.255.0

g) Set gateway address of 805U-E to 192.168.0.1 with command bgw 192.168.0.1

h) Set dipswitch to RUN

i) Reset 805U-E with reset command.

j) Open configuration webpage with Internet Explorer at address http://192.168.0.200/

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

Enter “Quick Start”, and select Access Point.

IP address should be 192.168.0.200

Enter a System Generator String

Select the Radio Encryption required.

Save the changes.

Client 1 Configuration

Perform the same configuration steps as the Access Point configuration with the following differences:

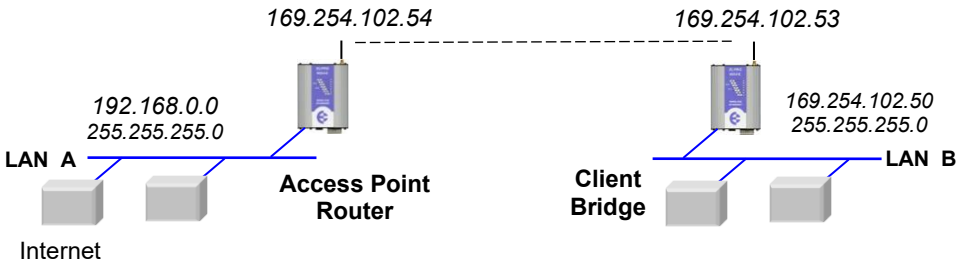
- set IP address of 805U-E to 192.168.0.201
- set the Operating Mode to Client.

Ensure the same System Generator String is used and the same Radio Encryption method is selected.

Client 2 Configuration

- As above, but use IP address 192.168.0.202

Connecting two separate networks together



Network A Configuration

In this example, network A is connected to the internet via a router at IP address 192.168.0.1.

Devices on Network A that only require access to devices on Networks A and B, should have their gateway IP address set to the 805U-E Access Point as 192.168.0.200.

Devices on Network A, that must interact with devices on Networks A and B and the internet should set the internet router 192.168.0.1 as their gateway, and must have a routing rule established for devices on Network B. On PCs, this may be achieved with the MS-DOS command ROUTE. For this example use: ROUTE ADD 192.168.102.0 MASK 255.255.255.0 192.168.0.200

Network B Configuration

All devices on Network B should be configured so their gateway IP address is that of the 805U-E Access Point as 192.168.102.54

Access Point Configuration

- Connect straight through Ethernet cable between PC and 805U-E.
- Ensure configuration PC and 805U-E are setup to communicate on the same network
- Set dipswitch to SETUP
- Power up unit, and wait for LINK 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 http://192.168.0.1XX/

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

  Enter “Quick Start”, and select Access Point.

  Change the IP address to 192.168.0.200

  Enter a System Generator String

  Select the Radio Encryption required.

  Set dipswitch to RUN.

  Save the changes, and unit will reset. Wait for unit to complete reset.
- Open configuration webpage with Internet Explorer at address http://192.168.0.200/

  Select Network settings menu option

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

Device Mode should be set to Router.

Set the Gateway IP address to 192.168.0.1

Set the Ethernet IP address to 192.168.0.200, network mask 255.255.255.0

Set the Wireless IP address to 169.254.102.54, network mask 255.255.255.0

Click on button Save to Flash and Reset. Webpage will display that message indicating details are being written to flash. Wait for 805U-E to reboot before removing power.

Client Configuration

Perform the same configuration steps as the Access Point configuration with the following differences:

- Connect straight through Ethernet cable between PC and 805U-E.
- Ensure configuration PC and 805U-E are setup to communicate on the same network
- Set dipswitch to SETUP
- Power up unit, and wait for LINK 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 http://192.168.0.1XX/

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

  Enter “Quick Start”, and select Client.

  Change the IP address to 192.168.0.53

  Enter a System Generator String

  Select the Radio Encryption required.

  Set dipswitch to RUN.

  Save the changes, and unit will reset. Wait for unit to complete reset.
- Open configuration webpage with Internet Explorer at address http://192.168.0.53/

  Select Network settings menu option

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

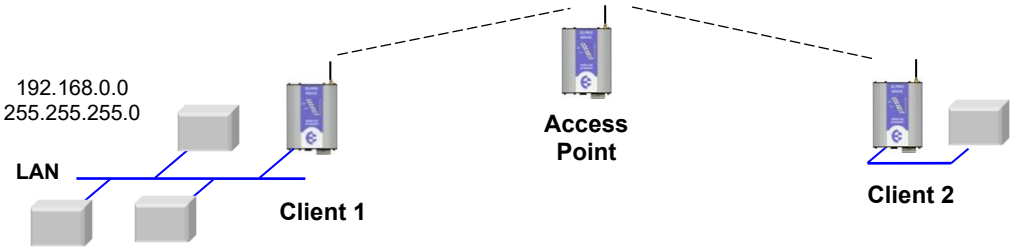
  Set the Gateway IP address to 192.168.102.54

  Set the Ethernet IP address to 192.168.102.53, network mask 255.255.255.0

  Set the Wireless IP address to 169.254.102.53, network mask 255.255.255.0

Click on button Save to Flash and Reset. Webpage will display that message indicating details are being written to flash. Wait for 805U-E to reboot before removing power.

Extending range of a network with a Repeater hop



Configure units as described in Section *Extending a wired network*. Place the Access Point at the remote intermediate repeater location.

Chapter Four DIAGNOSTICS

4.1 Diagnostics Chart

LED Indicator	Condition	Meaning
OK	GREEN	Normal Operation
OK	RED	Supply voltage too low.
Radio RX	GREEN flash	Radio receiving data
Radio RX	RED flash	Weak radio signal
Radio TX	Flash	Radio Transmitting
Radio LINK	On	On when a radio communications link is established
Radio LINK	Off	Communications failure or radio link not established
Radio LINK	GREEN flash RED flash	Serial Port Receiving CTS low
LAN	ON	Link Established on Ethernet port
LAN	Flash	Activity on Ethernet port.
Serial	GREEN flash	RS232 Serial Port Activity
Serial	RED flash	Rs485 Serial Port Activity
DIO	On	Digital Output ON ***or*** Input is grounded.
DIO	Off	Digital Output OFF ***and*** Input is open circuit.

The green Active LED on the front panel indicates correct operation of the unit. This LED turns red on failure as described above. When the Active LED turns red shutdown state is indicated. On processor failure, or on failure during startup diagnostics, the unit shuts down, and remains in shutdown until the fault is rectified.

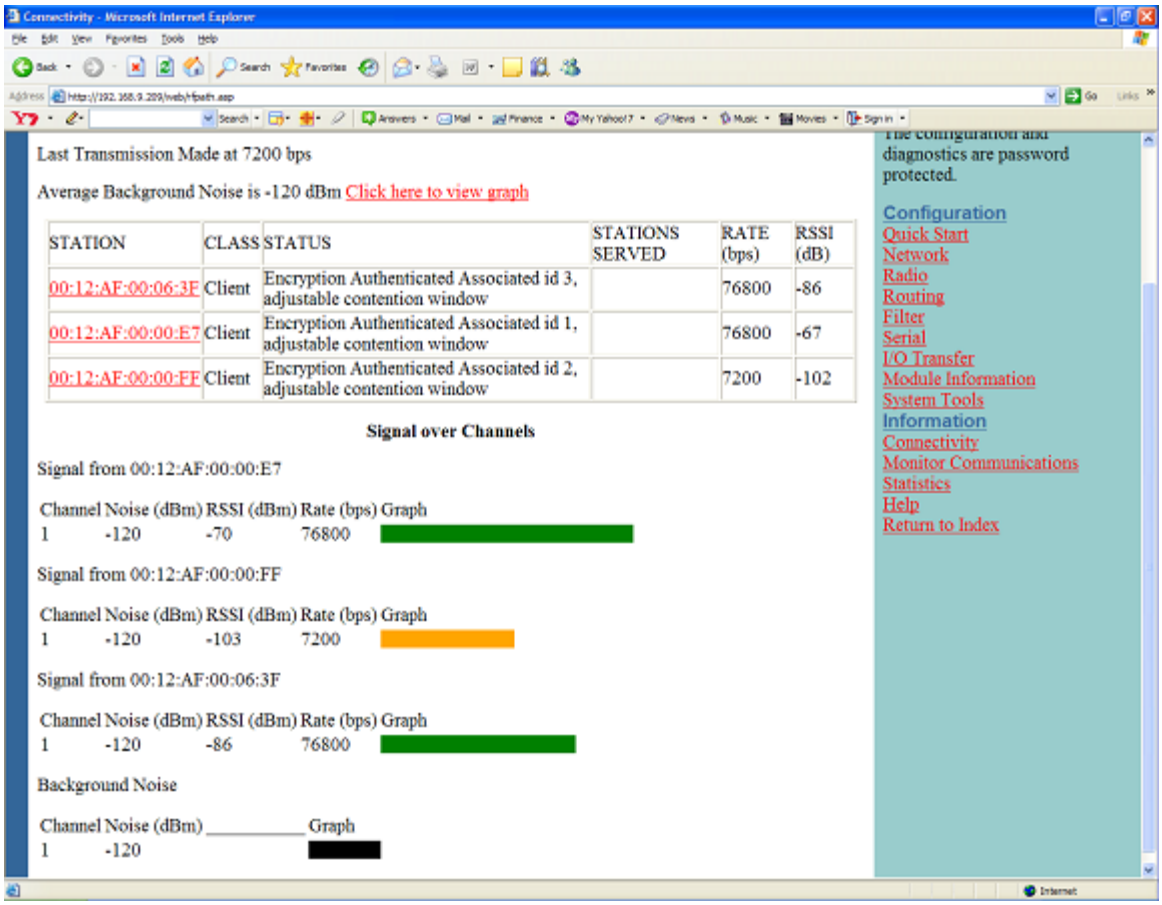
Boot Loader LED Indication during Startup

Serial	LAN	LINK	ACTIVE	Comment
Orange	Orange	Orange	RED	Initial Power Up & bootload Initialisation
RED	Orange	Orange	RED	Check Config & Print Sign-on message (If boot delay not zero)
Orange	Orange	Orange	RED	Print Configuration Table to terminal (If boot delay not zero)
Green	LAN	Off	RED	Initialise Networking and Start Auto Boot sequence
Orange	LAN	Off	GREEN	Wait for <ENTER> to abort Auto boot (If boot delay not zero)
Sequence	LAN	Sequence	GREEN	Boot – loader active (auto boot aborted or no application)
SERIAL	LAN	LINK	GREEN	Normal Operation. Application Running.

4.2 Diagnostic Information Available

4.2.1 Connectivity

The Connectivity webpage at an Access Point lists all units for which a transmission was received.



The table shows the averaged receive signal strength and last received radio data rate for each Client or Access Point by their MAC Address. The unit listed at an Access Point may not even be in the same system. This can provide an idea of how busy the radio band is.

The connectivity page above shows the stations it is receiving valid status from. These sending units identity is shown as their corresponding MAC addresses. The graph is a representation of the RSSI and indicates the value of this RSSI on each channel once they are received. The background noise and last transmission rate to the unit is also listed in the graph beside each bar in the graph.

The bargraph is colored. Red for too weak or too strong signal (>-50dBm), orange when the signal is within fade margin, and green when signal is above fade margin.

Background noise level is also graphed.

Note that in the above Connectivity screen for an Access Point, the STATUS section for the Client is "adjustable contention window". If the Access Point is V1.18 or later, you can check if there are pre-V1.18 units in the system - these units will not have "adjustable contention window". If this is the case, a compatible contention window size is set, and performance will not be optimal. Upgrade the firmware on pre-V1.18 units to improve overall performance.

4.2.2 Monitor Communications

The "Monitor Communications" function buffers the last 30 transmissions since the last enquiry was made. If there have not been 30 transmissions since the last enquiry, the 805U-E will wait 4 seconds for further transmissions to occur before completing the webpage. Use of this feature together with the Connectivity webpage will reveal the variability of communications over a link.

Monitor Communications

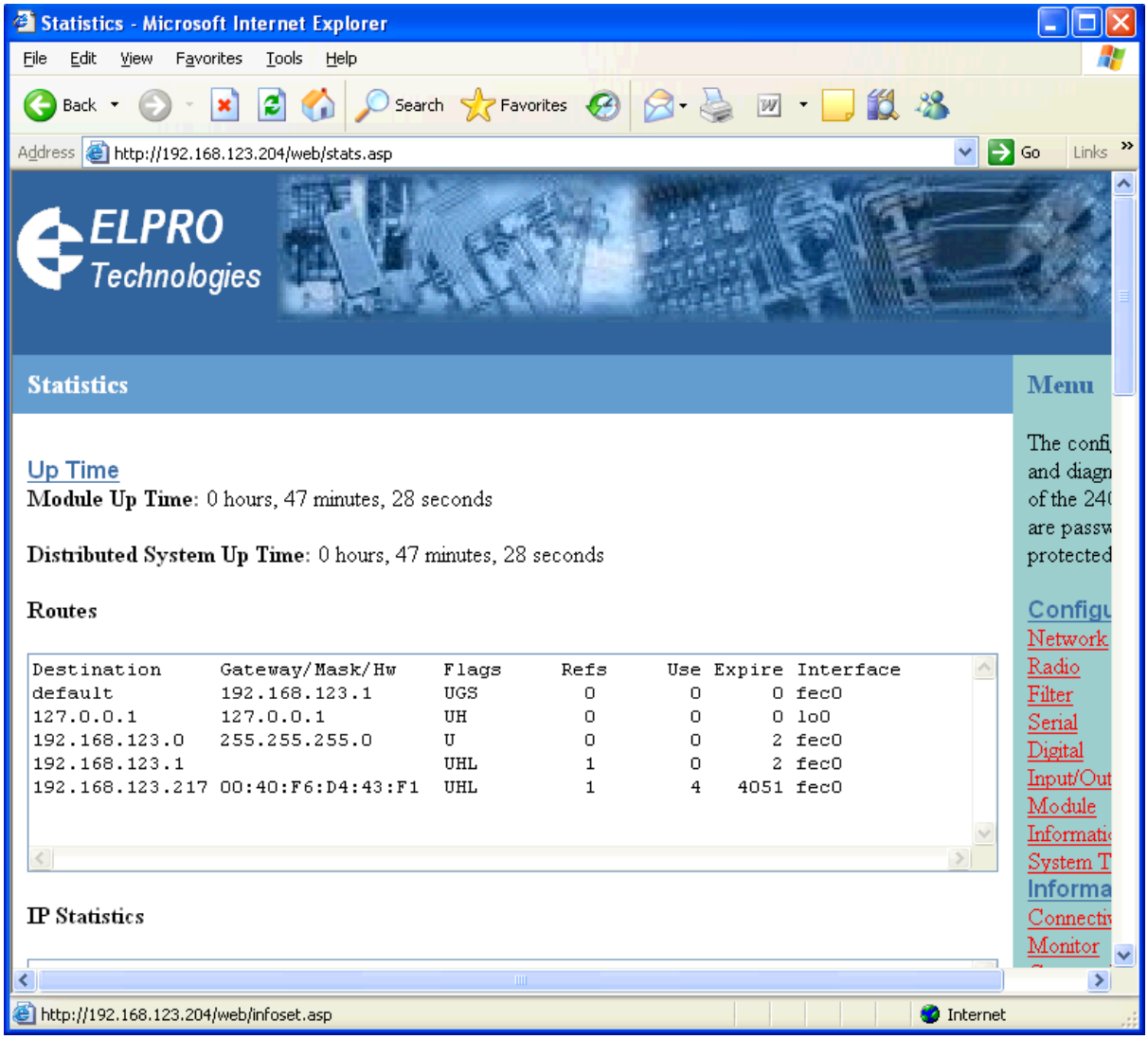
MAC Address of this 905U-E: 00:12:AF:00:00:ED

BSSID/AP associated: 00:12:AF:00:00:ED

TSF (usec)	TX/RX	MESSAGE	RATE (bps)	RSSI (dB)
6245457000	TX	08070D000012AF00008A0012AF0000ED00112FB16E32C0320012AF0000ED	200000	
6245509000	TX	08070D000012AF00008A0012AF0000ED00112FB16E32C1320012AF0000ED	200000	
6245561000	TX	08070D000012AF00008A0012AF0000ED00112FB16E32C2320012AF0000ED	200000	
6245654000	RX	08030D000012AF0000ED0012AF00008A0012AF0000ED004900112FB16E32	200000	-47
6245664000	TX	D40001000012AF00008A0012AF00	200000	
6245695000	TX	08030D000012AF00008A0012AF0000ED00112FB16E32C3320012AF0000ED	200000	
6245756000	TX	08070D000012AF00008A0012AF0000ED00112FB16E32D0320012AF0000ED	200000	
6245808000	TX	08070D000012AF00008A0012AF0000ED00112FB16E32D1320012AF0000ED	200000	

4.2.3 Statistics

The Statistics webpage is used for advanced debugging of 805U-E. This webpage details the state of the 805U-E and its performance in the system.



4.2.4 Network Traffic Analysis

There are many devices and PC programs that will analyse performance of an Ethernet network. Freely available programs such as Ethereal provide 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 805U-E a simple task.

4.3 Testing Radio Paths

The general procedure for radio range testing a link is fairly simple. Configure two units to form a link using automatic radio rates. Install the Access Point at a fixed location. Take a laptop computer and the Client to each of the remote locations, and analyse the link using the

Connectivity webpage. If a beacon is heard from the Access Point, the Client will update its Connectivity webpage with the received signal strength of beacon messages from the Access Point.

The RX led on the Client should also be observed. If the RX led flickers red, then the signal strength is weak. If the RX led is always green when a message is received, then the signal is strong.

If the signal is strong enough, a link may be established, and the Connectivity webpage of the Access Point may be opened. If the link is weak, the LINK led will go out, and the remote Connectivity webpage of the Access Point will fail to load. Using this procedure, the signal strengths of units at both locations may be analyzed, and traffic is sent between the units whilst remote webpages are opened.

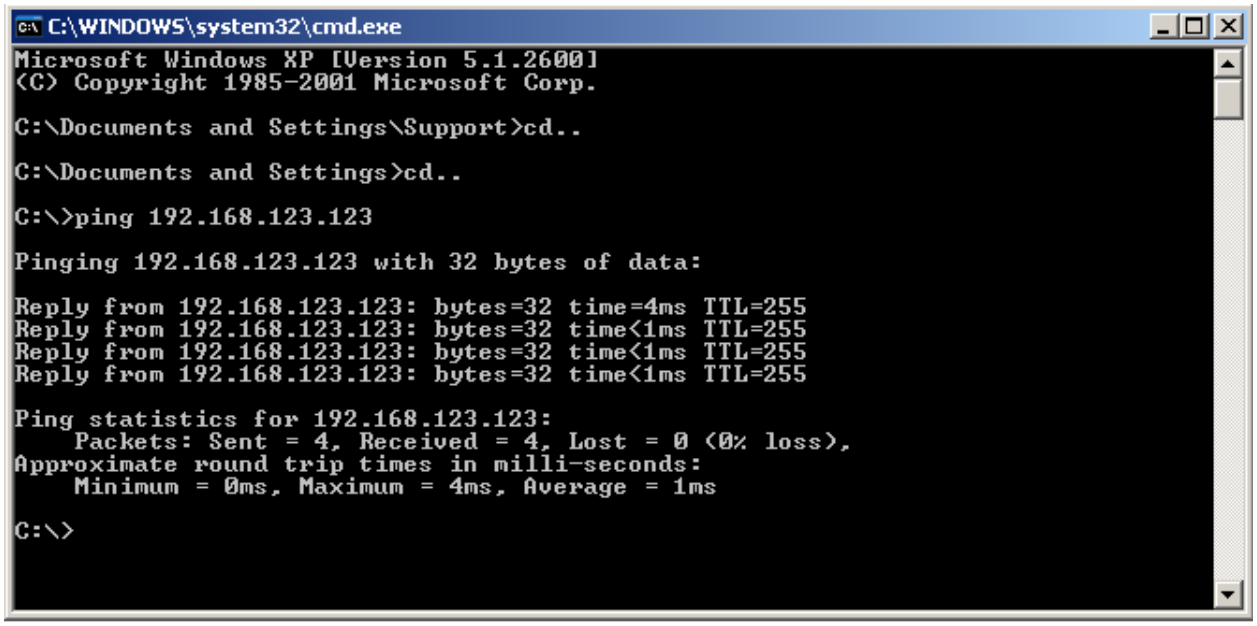
4.4 Utilities

4.4.1 PING

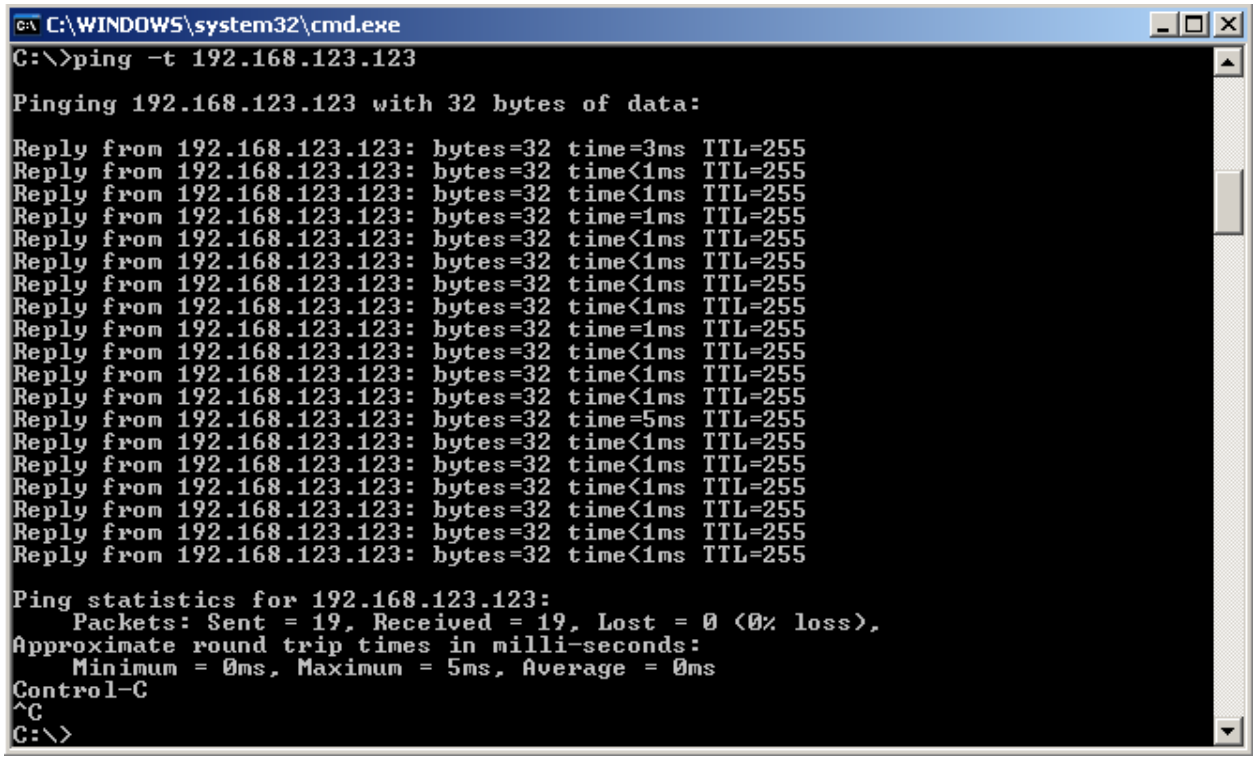
Ping is a basic Internet program that lets you verify that a particular IP address exists and can accept requests. Ping is used diagnostically to ensure that a host computer you are trying to reach is actually operating. If, for example, a user can't ping a host, then the user will be unable to send 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 805U-E at first startup.

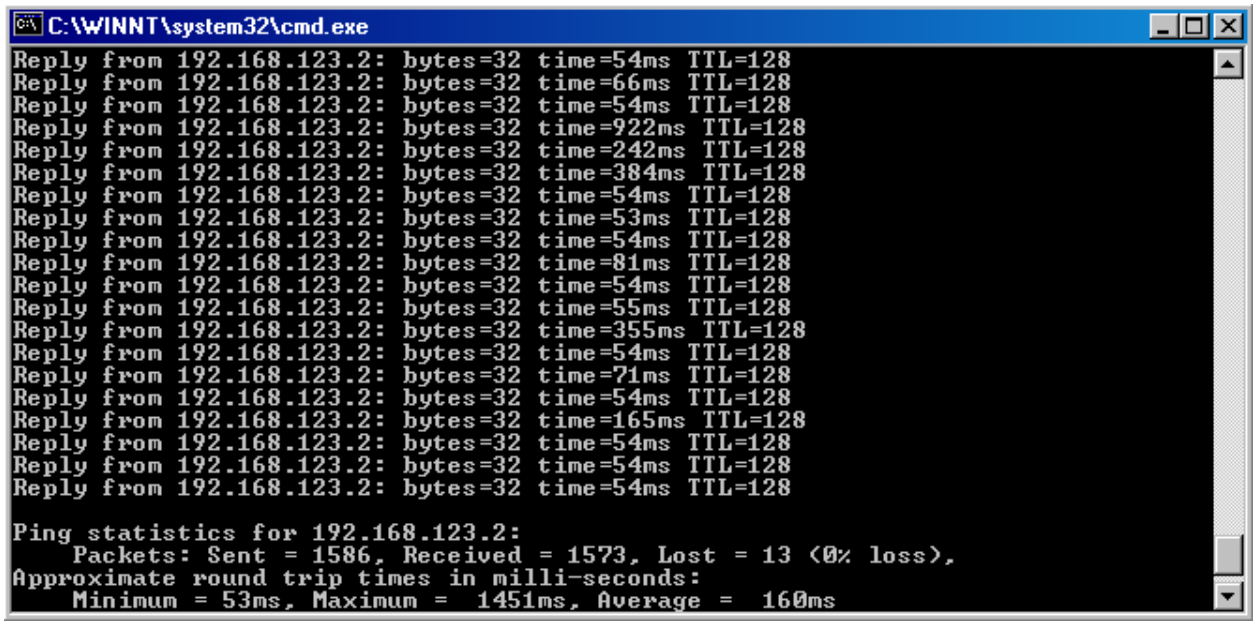
This command would be written as Ping 192.168.123.123 then Enter to send the ping command. The pc will reply with an acknowledgement of your command and if your 805U-E is correctly configured your reply will look something like this.



The screen shot below shows the response of the "ping 192.168.123.123 –t" command.

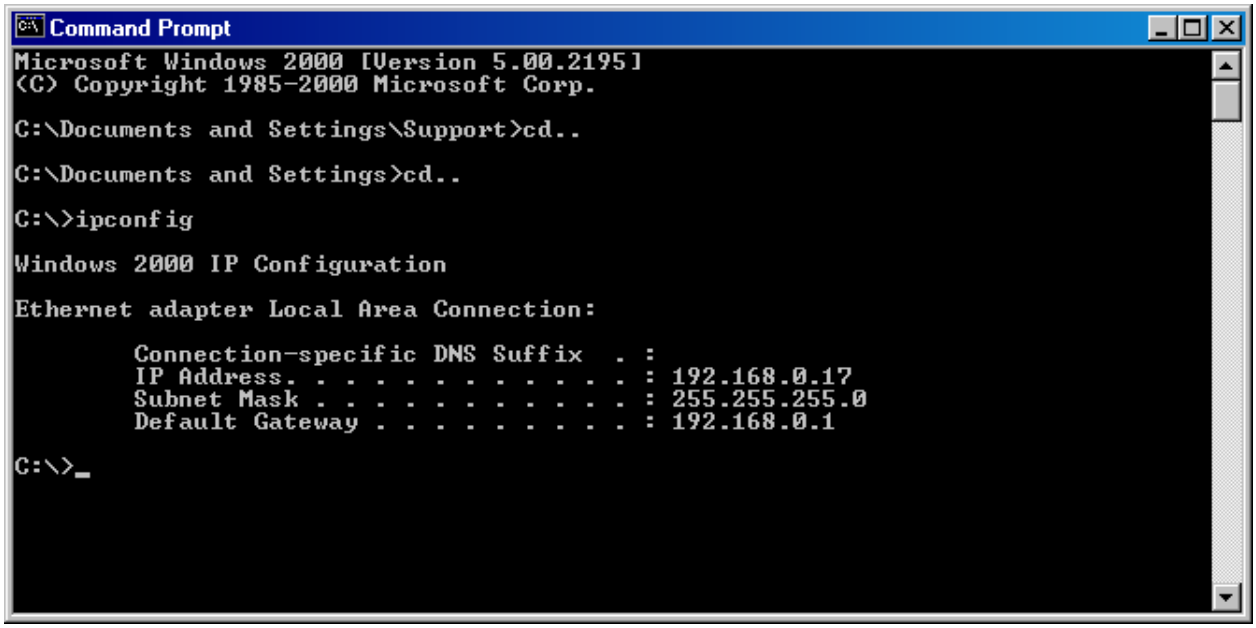


This -t command is used to repeatedly ping the specified node in the network, to cancel use "Ctrl – C"
A good test for the network once it is first set up is to use PING repeatedly from one PC's IP address to the other PC's IP address. This gives a good example of the networks reliability and how responsive it is from point to point. When you enter "Ctrl C" the program reports a packet sent-received-lost percentage.



4.4.2 IPCONFIG

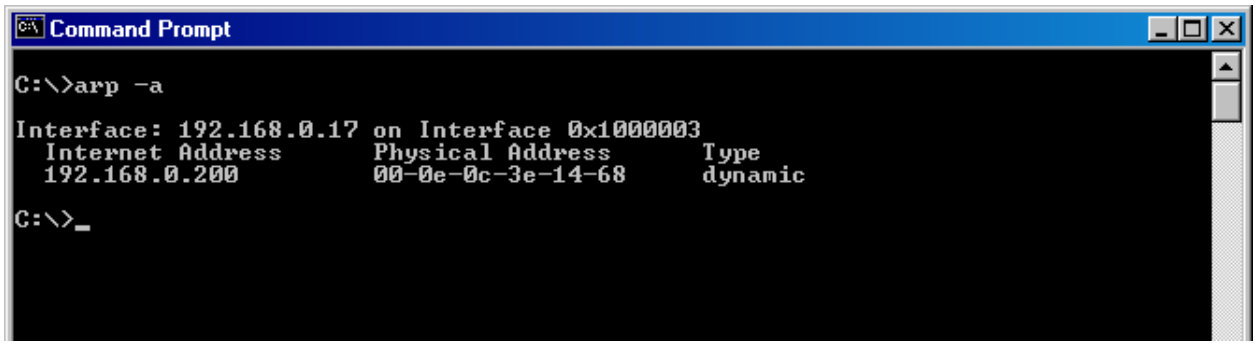
IPCONFIG can be used to show your current TCP/IP information, including your address, DNS server addresses, adapter type and so on.



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 /? will list all of the commands and their usages available for use.

4.4.3 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.



Command used for above screen shot is Arp –a. It shows the PC's direct IP address of 192.168.0.17 as also shown before with IPCONFIG command. The other IP address shown with its associated MAC address is another device with a connection to the PC. In this example it is the IP address of a PLC connected to the PC also.

Arp –n lists all the commands available for this function.

4.4.4 ROUTE

Route is used for the Router function. This is where you are joining 2 different networks together via the 805U-E *refer to Section 1.1*
The 805U-E can only accept 1 Routing table. That is it can only accept one router per network of radios. On the Router radio network PC a routing rule needs to entered to allow access between Network A and Network B. This is entered in the command prompt as per all other instruction above.

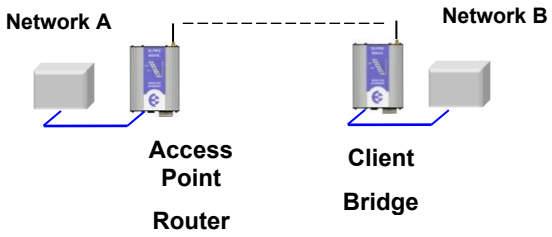
Route PRINT will show all active routes on PC,

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.

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



Network A Settings

IP Address 192.168.0.17

Subnet Mask 255.255.255.0

Gateway IP 192.168.0.1

Client Bridge Settings

Gateway IP 192.168.2.51

Ethernet IP 192.168.2.50

Subnet Mask 255.255.255.0

Wireless IP 192.168.2.50

Subnet Mask 255.255.255.0

Access Point Router Settings

Gateway IP 192.168.0.1

Ethernet IP 192.168.0.191

Subnet Mask 255.255.255.0

Wireless IP 192.168.2.051

Subnet Mask 255.255.255.0

Network B Settings

IP Address 192.168.2.201

Subnet Mask 255.255.255.0

Gateway IP 192.168.2.51

In the Network A PC a routing rule is to be set.

This will allow Network A & B to have access to each other. This is entered under cmd prompt.

Route ADD 192.168.2.0 MASK 255.255.255.0 192.168.0.191

This says access everything on network B (192.168.2.0) with the Mask of 255.255.255.0 on Network A via the Ethernet IP Interface 192.168.0.191

IP Address 192.168.2.0 will allow everything on this network to be shared by the router. When adding a routing table you will need to enter this in. Once entered in the Router will determine whether to pass information over the router if it is addressed to do so or not. For added security MAC address filtering could be added as mentioned earlier in Section 3.

Chapter Five SPECIFICATIONS

General		
EMC specification	EN 300 683	89/336/EEC
Radio specification	EN 300-220, pt1	869.525MHz, 0.5W 869.275MHz, 5mW
Housing	110 x 185 x 30mm	Powder-coated, extruded aluminum DIN rail mount
Terminal blocks	Removable	Suitable for 12 gauge (2.5sqmm) conductors
LED indication	Active, Serial RX and TX, Radio RX and TX, Link	
Operating Temperature	-40 to +60 degrees C	0 – 99% RH non-condensing
Power Supply		
Nominal supply	10 to 30VDC	Overvoltage and reverse voltage protected
Current Drain @ 12VDC	280 mA	During transmission 500mA (1W)
Current Drain @ 24VDC	150 mA	During transmission 300mA (1W)
Ethernet Port	10/100 BaseT	RJ45
Standard	IEEE 802.3 compliant	Bridge/router, Access point/ client functionality
Radio Transceiver		
Transmit power	50 - 500mW	configurable
Signal detect / RSSI	-120 to -50 dBm	
Expected line-of-sight range	Principal EU Range based on lowest data rate Range may be extended using intermediate modules as repeaters.	5+ km @ 500mW ERP depending on local conditions
Antenna Connector	Female SMA coaxial	
Wireless data rate (bit/sec) - configurable	up to 76.8Kbps	"Auto" function determines fastest rate within user-configured fade-margin

Serial Ports		
RS232 Port	DB9 female DCE	RTS/CTS/DTR/DCD hardware signals provided
RS485 Port	2 pin terminal block	Max distance 4000’ / 1.2 km
Data rate (bit/sec) - configurable	1200, 2400, 4800, 9600, 14400, 19200, 38400, 57600, 76800, 115200	
Byte format	7 or 8 data bits	Stop/start/parity bits configurable
System Parameters		
System address	255 word string	
Wireless data encryption	None, 64-bit proprietary or 128-bit AES	
User Configuration	Via embedded web page	Via RS232 commands
Diagnostics	LED’s	OK, DCD, Radio and Serial RX/TX
		Low signal receive led
	RSSI measurement in dBm	BER test

Appendix A FIRMWARE UPGRADE

Determine which firmware version is present in the module to be upgraded by viewing the root webpage of the module

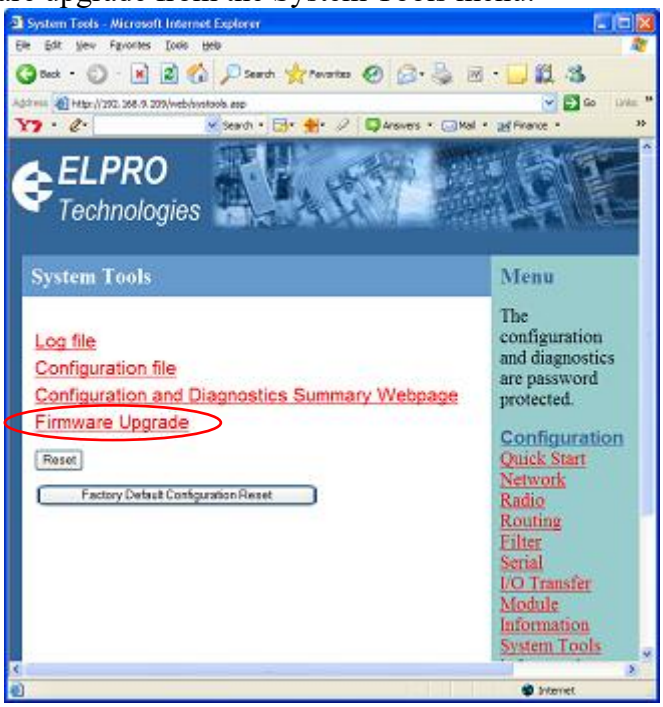
Firmware versions 805U-E v1.26 and later may be upgraded to later versions using webpages inside the module. This upgrade can be done locally with a PC connected directly to the module, or remotely over a working radio link. For remote upgrades, it is advisable to reduce radio traffic over the link from other devices, as much as possible. If necessary, create a temporary separate radio network to perform the upgrade to remote modules. Please refer to the "Web based Upgrade" section for the upgrade procedure.

Previous versions require an upgrade package using the program FlashUpdate, and can only be performed local to the module. Also refer to this procedure if firmware version of modules is unknown. The section "Manual Upgrade using Flash Update" outlines the upgrade procedure.

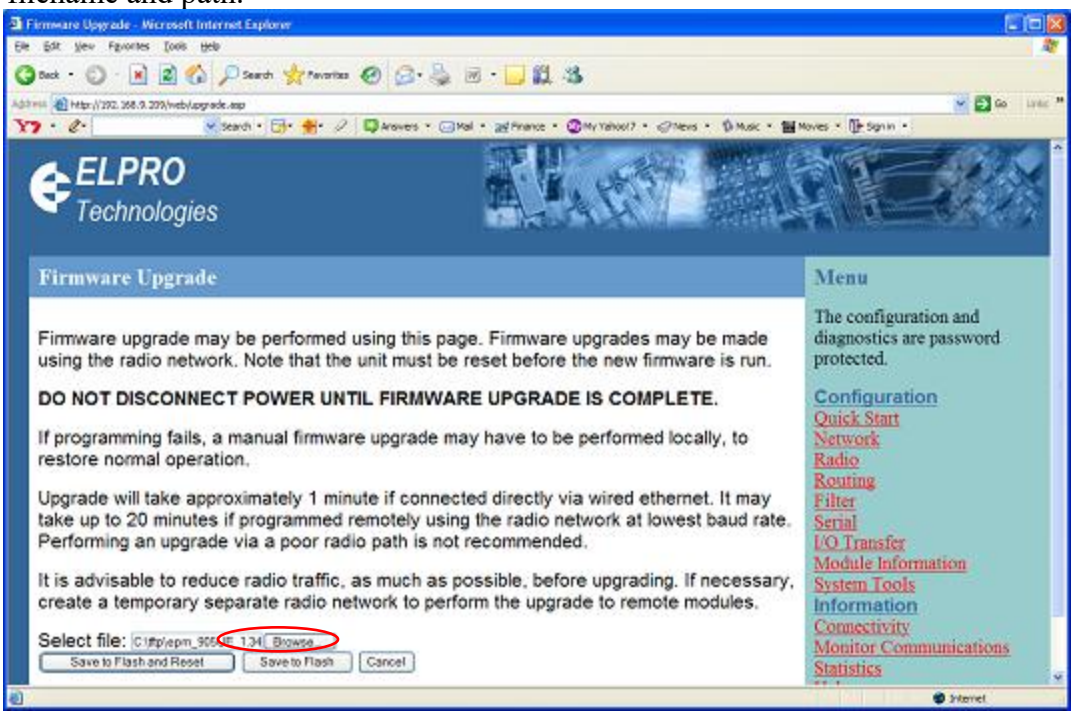
Web based Upgrade

If the modules have application firmware version 805U-E v1.26and later currently installed, please follow these steps to upgrade the unit.

1. Place the new application firmware file epm_805UE_*x.x*.bin.gz on the computers hard drive. Ensure that the file is not placed in a deeply nested folder.
2. Open internal webpage of unit to be upgraded, and Select System Tools from Menu
3. Select Firmware upgrade from the System Tools menu.



4. Click Browse button and find the application firmware file on your computer. Ensure that the file is not in a deeply nested folder, as there is a character limitation of the filename and path.

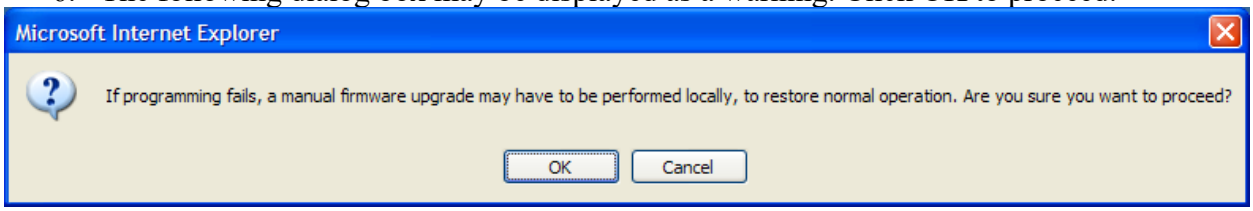


5. There are two options:

   a. The “Save to Flash and Reset” button may be clicked, to initiate a reset immediately after a successful firmware upgrade so that the new firmware is run.

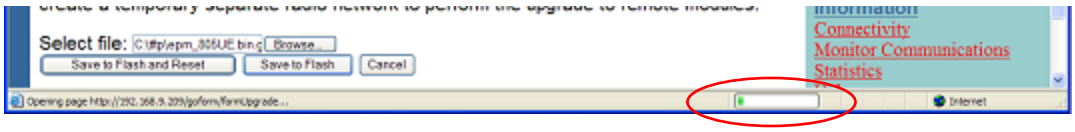
   b. Alternatively, Click “Save to Flash” button to just program the new firmware to the unit. A reset is necessary to run the new firmware. This is useful for maintaining radio link whilst performing upgrades to remote units.

6. The following dialog box may be displayed as a warning. Click OK to proceed.



7. Firmware upgrade will proceed, and should take about 1 minute if performed locally. If performed over a radio link, the upgrade may take between 4 to 20 minutes, depending upon the quality of the radio link, and the amount of traffic on the network.

   During the upgrade, the webpage shows a progress bar at the bottom right side of the browser window.



   When upgrade is completed, the System Tools webpage will be shown if "Save to Flash" was clicked. If "Save to Flash and Reset" was clicked, the unit will display a message that the module is resetting.

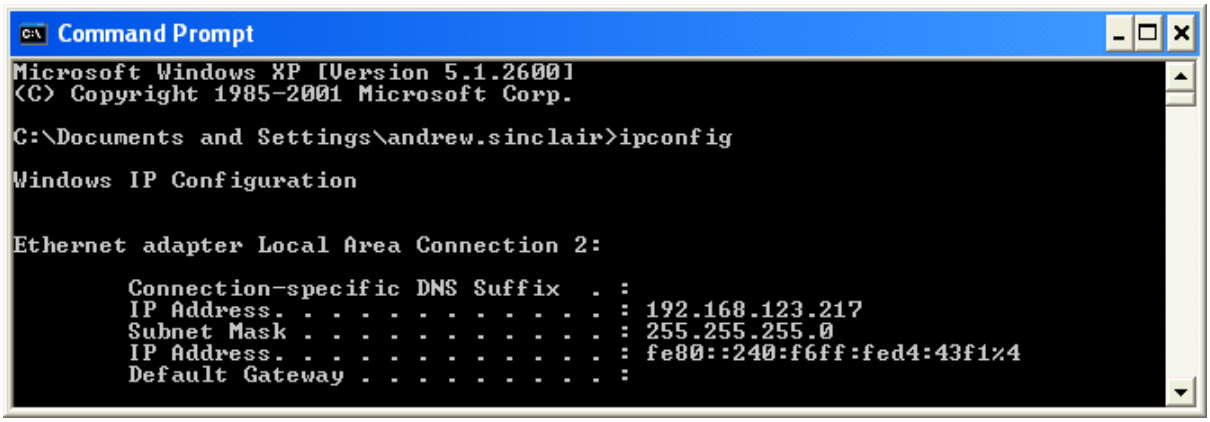
   Firmware upgrade is now complete.

Manual Upgrade using Flash Update

1. Connect the module's ethernet port to PC ethernet port via a "straight through" ethernet cable. "Straight through" ethernet cable is typically a blue colour.

   Alternatively, connect the module to PC via a network switch or hub, as some configurations of Windows can encounter difficulty upgrading without a hub connected. On some PCs, Windows can take much longer than expected to initialise its network interface when the device is reset - connecting via a hub/switch removes this issue during the upgrade procedure.

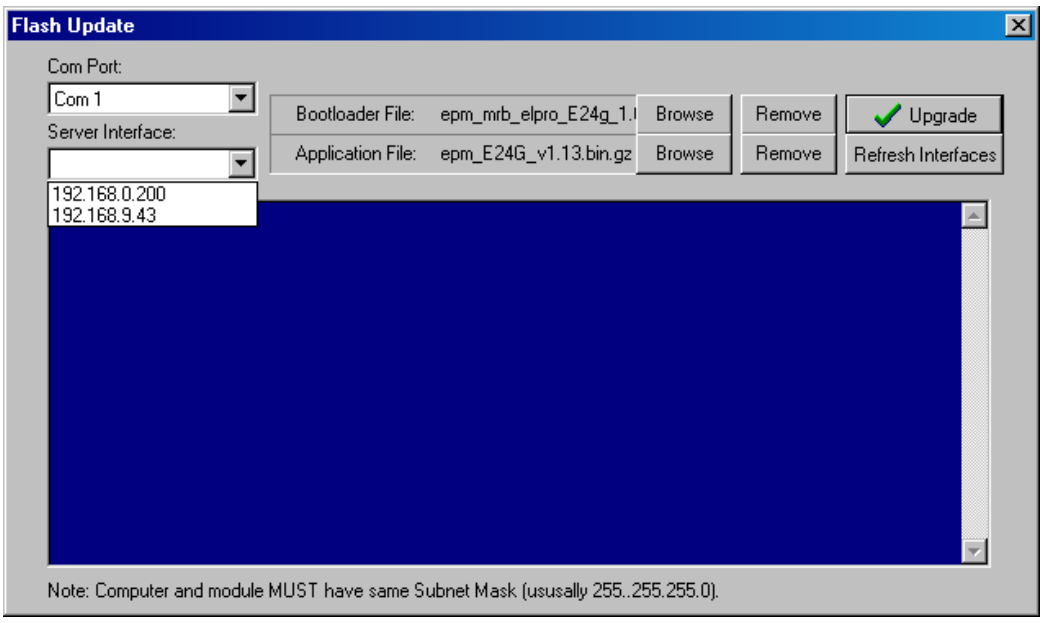
2. Switch dip-switch on module to **SETUP** mode.
3. **Power up** the module and wait a couple seconds. This will ensure that Windows networking can correctly detect an operating ethernet port.
4. Ensure your PC network settings have a Subnet Mask of 255.255.255.0. This can be easily checked using DOS command IPCONFIG.



5. Extract FlashUpdate program, and start the program.

6. If you are running Windows firewall you may be prompted with the following message. Select Unblock so that FlashUpdate program may operate. If any other firewall software is operating, disable it.

7. Copy new firmware files to a known location on the hard drive of your PC. Do not unzip these files.
8. Specify location of firmware bootloader file (epm_mrb_elpro_E900_*x.x*.bin.gz) and firmware application file (epm_805UE_*x.x*.bin.gz) using the Browse buttons in the FlashUpdate program.
9. Connect PC to module RS-232 serial port with "straight-though" serial cable.
10. Select COM port connected to module in the *FlashUpdate* program.
11. Select Server Interface in the *FlashUpdate program. (IP address of PC connected to which can be found from step 4 above)*

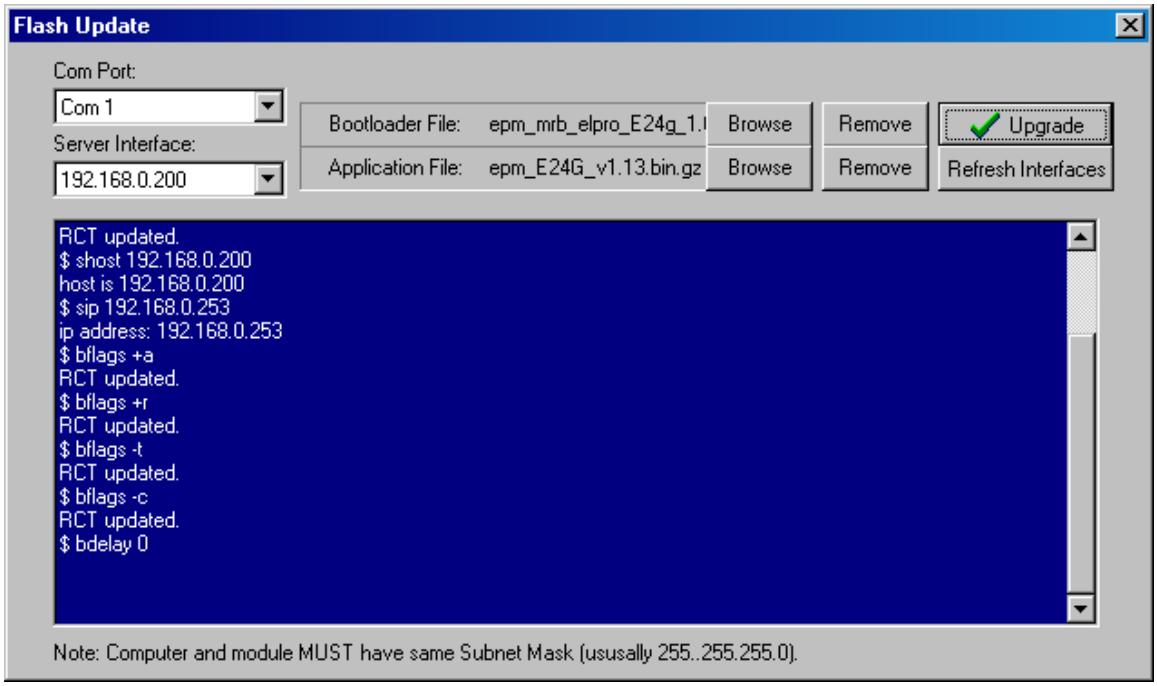


12. Click on *Upgrade* button in *FlashUpdate* program.

13. Follow instructions from confirmation window.

14. Click *OK,* **Power down** module, wait approximately 1 second, and power up module. This entire step must be accomplished within 30 seconds of completing the previous step.

15. Programming will commence…



16. If programming was successful, a dialog box is displayed showing this.

17. Switch dipswitch to RUN position and cycle power for normal operation.

Appendix B GLOSSARY

ACK	Acknowledgment.
Access point	An access point is the connection that ties wireless communication devices into a network. Also known as a base station, the access point is usually connected to a wired network.
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 amount of "transportation" space an Internet user has at any given time.
Bridge	
Collision avoidance	A network node characteristic for proactively detecting that it can transmit a signal without risking a collision.
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. Instead of the signals transferring in parallel paths from one set of plugs to another, the signals "crossover." If an eight-wire cable was being used, for instance, the signal would start on pin one at one end of the cable and end up on pin eight at the other end. They "cross-over" from one side to the other.
	CSMA/CA 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	A method of managing traffic and reducing noise 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	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	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	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.
Firewall	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 WiFi. Wired hubs can have numerous ports and can transmit data at speeds ranging from 10 Mbps to multigigabyte 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	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 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	A client setting providing connectivity to an AP. As compared to Ad-Hoc mode, whereby PCs 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 neighborhood, but also provides communication with the wired network. See Ad-Hoc and AP.
I/O	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	A set of rules used to send and receive messages at the Internet address level.
IP (Internet Protocol) 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	IPX, short for 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. Whereas the IPX protocol is similar to IP, SPX is similar to TCP. Together, therefore, IPX-SPX provides connection services similar to TCP/IP.
ISA	A type of internal computer bus that allows the addition of card-based components like modems and network adapters. ISA has been replaced by PCI and is not very common anymore.
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	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 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 db that the wireless device transmits at.
MAC Address	A MAC address, short for Media Access Control address, is a unique code assigned to most forms of networking hardware. The address is permanently assigned to the hardware, so limiting a wireless network's access to hardware -- such as wireless cards -- is a security feature employed by closed wireless networks. But an experienced hacker -- armed with the proper tools -- can still figure out an authorized MAC address, masquerade as a legitimate address and access a closed network. Every wireless 802.11 device has its own specific MAC address hard-coded into it. This unique identifier can be used to provide security for wireless networks. When a network uses a MAC table, only the 802.11 radios that have had their MAC addresses added to that network's MAC table will be able to get onto the network.
NAT	Network Address Translation: A network capability that enables a houseful 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	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. Even though they look very similar to standard RJ-11 telephone connectors, RJ-45 connectors can have up to eight wires, whereas telephone connectors have only 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 putting in 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	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
Subnetwork or Subnet	Found in larger networks, these smaller networks are used to simplify addressing between numerous computers. Subnets connect to the central network through a router, hub or gateway. Each individual wireless LAN will probably use the same subnet for all the local computers it talks to.
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	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 a single file.
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 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	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	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	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.