Honeywell

XYR401-E Wireless Ethernet & Device Server

User Manual

34-XY-25-42

Version 1.8.1

April 2012

Honeywell Process Solutions

Notices and Trademarks

Version 1.8.1, April 2012

While this information is presented in good faith and believed to be accurate, Honeywell disclaims the implied warranties of merchantability and fitness for a particular purpose and makes no express warranties except as may be stated in its written agreement with and for its customers.

In no event is Honeywell liable to anyone for any indirect, special or consequential damages. The information and specifications in this document are subject to change without notice.

Honeywell Process Solutions

1860 West Rose Garden Lane

Phoenix, Arizona 85027

About This Document

This document describes preparation, operation and maintenance of the XYR 401 Wireless Ethernet device.

Revision Information

Document Name XYR401E Wireless Ethernet User Manual	**Document ID**	**Revision Number**	**Publication Date**
New	34-XY-25-42	Version 1.5	November 2010
Updates	34-XY-25-42	Version 1.6	April 2011
Updates	34-XY-25-42	Version 1.8.1	December 2011

References

The following list identifies all documents that may be sources of reference for material discussed in this publication.

Document Title
34-XY-25-42_XYR401E Wireless Ethernet User Manual

Support and contact info

United States and Canada

Contact: Honeywell Process Solution

- Global Technical Support - Phone: 001-800-423-9883
- Customer Service (HFS) - Phone: 001-800-343-0228
- Outside United States - Phone: 001-215-641-3610

Calls are answered by dispatcher between 6:00 am and 4:00 pm Mountain Standard Time. Emergency calls outside normal working hours are received by an answering service and returned within one hour.

Email support: ask-ssc@honeywell.com

Mail: Honeywell Process Solutions
1860 West Rose Garden Lane,
Phoenix, Arizona 85027

For Europe, Asia Pacific and North & South America contact details see pack page.

World Wide Web

Honeywell Solution Support Online:

www.honeywellprocess.com

Elsewhere

Call your nearest Honeywell office.

Training Classes

Honeywell Automation College:
http://www.automationcollege.com

Symbol Definitions

The following table lists those symbols used in this document to denote certain conditions.

Symbol	Definition
ℹ	**ATTENTION:** Identifies information that requires special consideration.
➡	**TIP:** Identifies advice or hints for the user, often in terms of performing a task.
CAUTION	Indicates a situation which, if not avoided, may result in equipment or work (data) on the system being damaged or lost, or may result in the inability to properly operate the process.
⚠	**CAUTION**: Indicates a potentially hazardous situation which, if not avoided, may result in minor or moderate injury. It may also be used to alert against unsafe practices. **CAUTION** symbol on the equipment refers the user to the product manual for additional information. The symbol appears next to required information in the manual.
⚠	**WARNING**: Indicates a potentially hazardous situation, which, if not avoided, could result in serious injury or death. **WARNING** symbol on the equipment refers the user to the product manual for additional information. The symbol appears next to required information in the manual.
⚡	**WARNING, Risk of electrical shock**: Potential shock hazard where HAZARDOUS LIVE voltages greater than 30 Vrms, 42.4 Vpeak, or 60 VDC may be accessible.
⚠	**ESD HAZARD:** Danger of an electro-static discharge to which equipment may be sensitive. Observe precautions for handling electrostatic sensitive devices.
⏚	**Protective Earth (PE) terminal**: Provided for connection of the protective earth (green or green/yellow) supply system conductor.
⏚	**Functional earth terminal**: Used for non-safety purposes such as noise immunity improvement. NOTE: This connection shall be bonded to Protective Earth at the source of supply in accordance with national local electrical code requirements.
⏚	**Earth Ground**: **Functional earth connection.** NOTE: This connection shall be bonded to Protective Earth at the source of supply in accordance with national and local electrical code requirements.
⊥	**Chassis Ground**: Identifies a connection to the chassis or frame of the equipment shall be bonded to Protective Earth at the source of supply in accordance with national and local electrical code requirements.

Thank you for your selection of the XYR401-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 XYR401-E enjoys a long life,

Double check ALL your connections with
the user's manual before turning the power on.

CAUTION:

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

DO NOT:

- operate the transmitter when 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.

FCC Notice:

This device complies with Part 15.247 of the FCC Rules.
Operation is subject to the following two conditions:

1) This device may not cause harmful interference and

2) This device must accept any interference received, including interference that may cause undesired operation.

This device must be operated as supplied by HONEYWELL. Any changes or modifications made to the device without the written consent of HONEYWELL may void the user’s authority to operate the device.
End user products that have this device embedded must be installed by experienced radio and antenna personnel, or supplied with non-standard antenna connectors, and antennas available from vendors specified by HONEYWELL. Please contact HONEYWELL for end user antenna and connector recommendations.

Part 15 – This device has been tested and found to comply with the limits for a Class B digital device, pursuant to Part15 of the FCC rules (Code of Federal Regulations 47CFR Part 15). Operation is subject to the condition that this device does not cause harmful interference.

Notice Any changes or modifications not expressly approved by HONEYWELL could void the user’s authority to operate this equipment.

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

Notices: Safety

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

UL NOTICE:

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

2. The units are intended for Restricted Access Locations.

3. The Wireless Ethernet module is intended to be installed in a final enclosure, rated IP54, before use outdoors.

4. The Equipment shall be powered using an external Listed Power Supply with LPS outputs or a Class 2 Power Supply.

5. The Wireless Ethernet module must be properly grounded for surge protection before use.

6. If installed in a hazardous environment coaxial cable shall be installed in a metallic conduit

Important Notice

HONEYWELL products are designed to be used in industrial environments, by experienced industrial engineering personnel with adequate knowledge of safety design considerations.
HONEYWELL 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, HONEYWELL 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 HONEYWELL 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 XYR401-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 XYR401-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 XYR401-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 XYR401-E module is not suitable for use in explosive environments without additional protection.

6. The XYR401-E Operates using the same Radio frequencies and communication protocols as commercially available off-the shelf equipment. If your system is not adequately secured, third parties may be able to gain access to your data or gain control of your equipment via the radio link. Before deploying a system make sure you have considered the security aspects of your installation carefully.

RELEASE NOTICE:

This is the December 2011 release of the XYR401-E Ethernet Modem User Manual version 1.8.1 which applies to version 2.0 Modem firmware.

Limited Lifetime Warranty, Disclaimer and Limitation of Remedies

Honeywell products are warranted to be free from manufacturing defects for the “serviceable lifetime” of the product. The “serviceable lifetime” is limited to the availability of electronic components. If the serviceable life is reached in less than 18 months following the original purchase from Honeywell, Honeywell will replace the product with an equivalent product if an equivalent product is available.
This warranty does not extend to:

- failures caused by the operation of the equipment outside the particular product's specification, or
- use of the module not in accordance with this User Manual, or
- abuse, misuse, neglect or damage by external causes, or
- repairs, alterations, or modifications undertaken other than by an authorized Service Agent.

Honeywell’s liability under this warranty is limited to the replacement or repair of the product. This warranty is in lieu of and exclusive of all other warranties. This warranty does not indemnify the purchaser of products for any consequential claim for damages or loss of operations or profits and Honeywell is not liable for any consequential damages or loss of operations or profits resulting from the use of these products. Honeywell is not liable for damages, losses, costs, injury or harm incurred as a consequence of any representations, warranties or conditions made by Honeywell or its representatives or by any other party, except as expressed solely in this document..
Full product specifications and maintenance instructions are available from your Service Agent, your source of purchase, or from the master distributor in your country upon request and should be noted if you are in any doubt about the operating environment for your equipment purchase
In the unlikely event of your purchase being faulty, your warranty extends to free repair or replacement of the faulty unit, after its receipt at the master distributor in your country. Our warranty does not include transport or insurance charges relating to a warranty claim.
Should you wish to make a warranty claim, or obtain service, please forward the module to the nearest authorised Service Agent along with proof of purchase. For details of authorised Service Agents, contact your sales distributor.

GNU Free Documentation Licence:

HONEYWELL is using a part of Free Software code under the GNU General Public License in operating the “*XYR401-E* ” product. This General Public License applies to most of the Free Software Foundation’s code and to any other program whose authors commit by using it. The Free Software is copyrighted by Free Software Foundation, Inc. and the program is licensed “As is” without warranty of any kind. Users are free to contact HONEYWELL at the following Email Address: ask-ssc@honeywell.com for instructions on how to obtain the source code used in the “*XYR401-E*”.

A copy of the license is included in the section entitled "GNU Free Documentation License".

CONTENTS

Chapter One INTRODUCTION

The XYR401-E Industrial 802.11 Wireless Ethernet module provide wireless connections between Ethernet devices and/or Ethernet wired networks (LAN's). They each comply with their relevant IEEE 802.11 standard.

The XYR401-E is available in a range of different models with different RF power and frequency options suitable for your country's local radio regulations.

XYR401-E-G	802.11 b/g 400mW max power

The above models have the same functionality but use a different radio to communicate. The different radios **do not** communicate with each other, e.g. an XYR401U-E-G will not communicate with an XYR401-E-A. Only modules of the same type are able to communicate wirelessly to each other.
Throughout this manual, any reference to "XYR401-E" refers to one of the above models.

The XYR401-E model uses a 2.4GHz Direct Sequence Spread Spectrum (DSSS) wireless transceiver. Users pick a 20 MHz channel with 5 MHz channel spacing from the available 13 starting with the first channel centred on 2.412 GHz. *Some limitations depending on country, see Appendix C for channel selections.*

Note that regulations in North America permit 11 x 2.4GHz channels and Europe permits 13 x 2.4GHz channels.

Please check with your HONEYWELL representative for the permitted channel usage in your country.
See Appendix C for channels selections.

The XYR401-E unit also provides two serial connections as well as the Ethernet connections. It is possible to use all three data connections concurrently, allowing the XYR401-E to act as a ***Device Server.*** Wireless connections can be made between serial devices and Ethernet devices. The XYR401-E provides connection functionality between serial "Modbus RTU" devices and Ethernet "Modbus TCP" devices. Appropriate driver applications will be required in the host devices to handle other protocols.

The XYR401-E has a standard RJ45 Ethernet connection which will operate at up to 100Mbit/sec. The module will transmit the Ethernet messages on the wireless band at rates between 1 and 54 Mbit/sec & 6 and 54 Mbit/sec depending on model, band, encryption methods and radio paths.

1.1 Network Topology

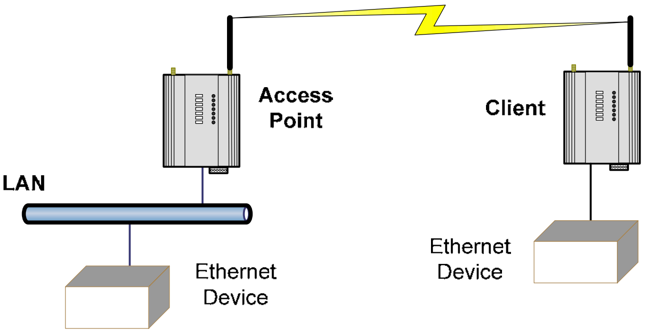
The XYR401-E is an Ethernet device, and must be configured as part of an Ethernet network. Each XYR401-E must be configured as an:

❑ "Access Point" or "Sta", "Station", Client"

Also needs to be configured as a:

❑ "Bridge" or "Router".

You can also connect to the XYR401-E via a RS232 or RS485 serial port using serial server or PPP (point-to-point) protocol. PPP allows the XYR401-E to connect serial communications into the Ethernet network.

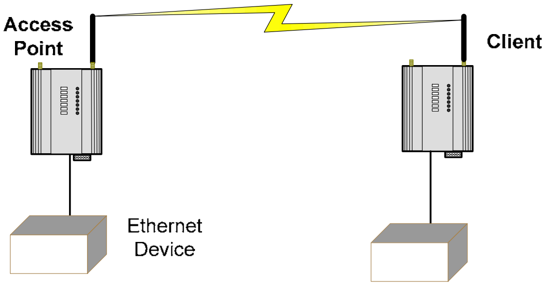


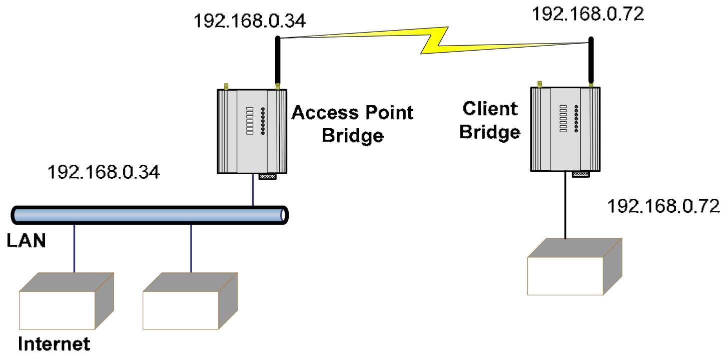
Access Point vs Client

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

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

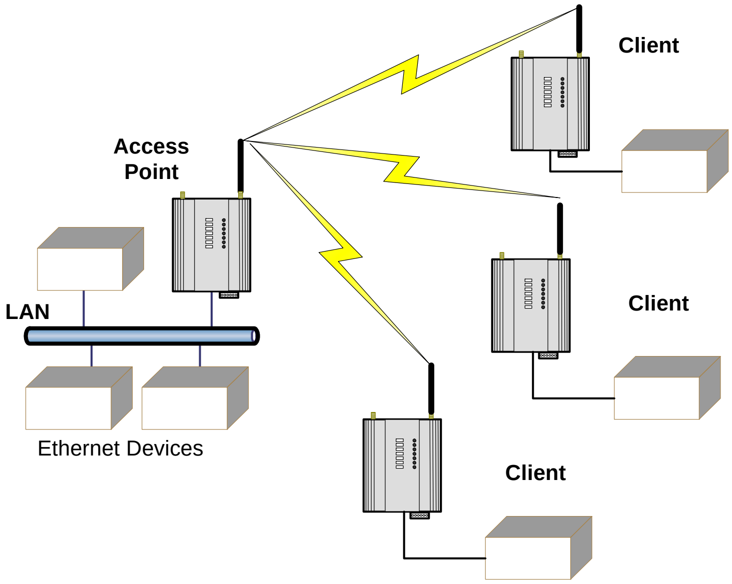
The first diagram shows a connection between two Ethernet devices using XYR401-E ethernet modems. In this example one XYR401-E is configured as an Access Point and the other as a Client - the Access Point can be connected.



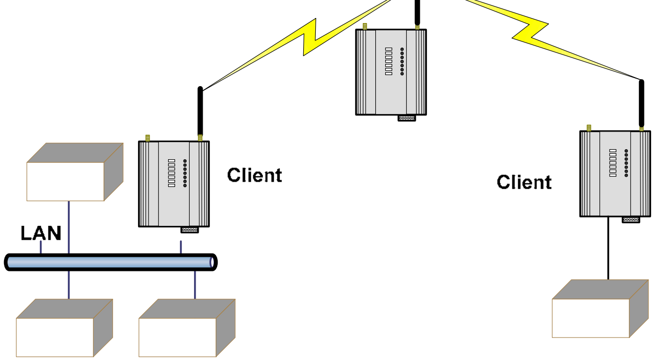


The second diagram shows an existing LAN being extended using XYR401-E’s. In this example, the Access Point should be configured at the LAN end - although the wireless link will still work if the Client is at the LAN end.

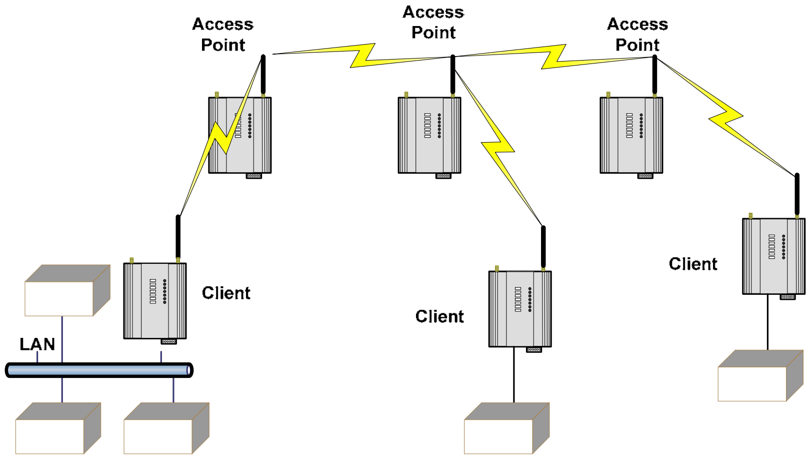
An Access Point can connect to multiple Clients. In this case, the Access Point should be the “central” unit.



An Access Point could be used as a “Repeater” unit to connect two XYR401-E Clients, which do not have direct reliable radio paths.
There is no “Special” repeater module, any XYR401-E can be a repeater and at the same time, can be connected to an Ethernet devices or on a LAN



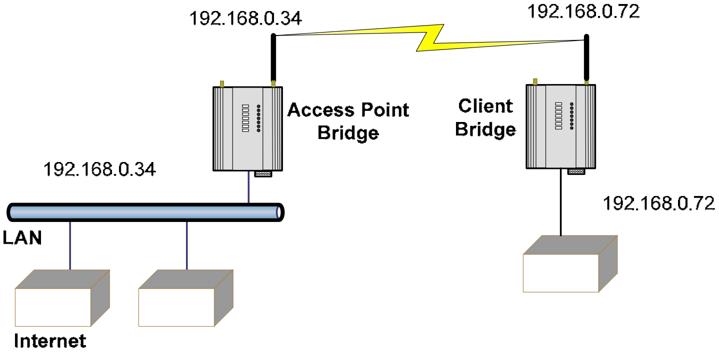
Multiple Access Points can be set-up in a “mesh” network to provide multiple repeaters.

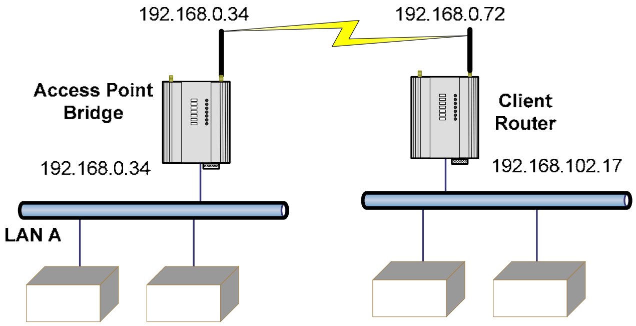


Bridge vs Router

Each XYR401-E is configured with an IP address for the Ethernet side, and another for the wireless side.

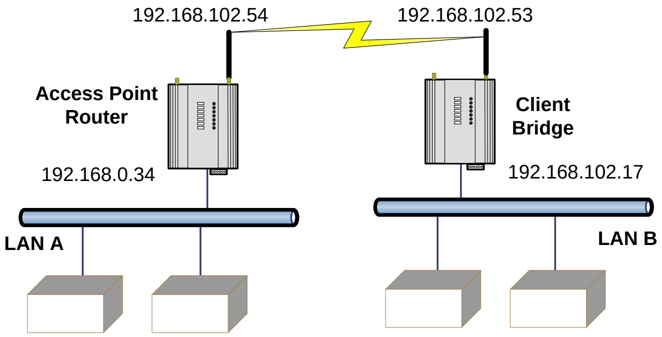
A **Bridge** connects devices within the same Ethernet network - for example, extending an existing Ethernet LAN. For a Bridge, the IP address for the wireless side is the same as the Ethernet side.



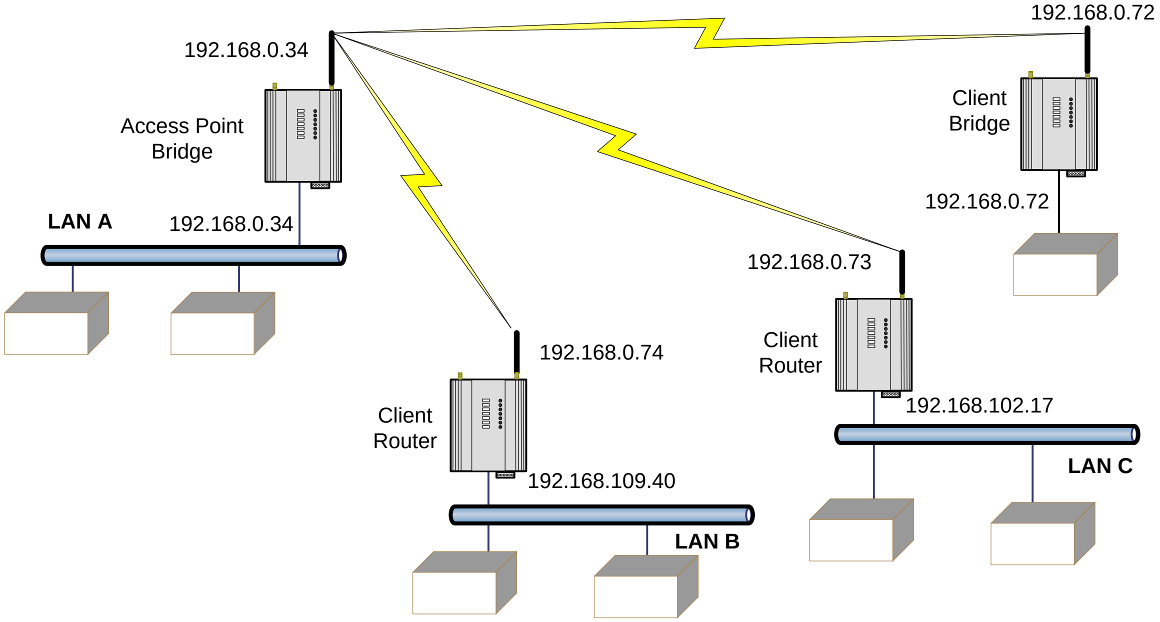


A **Router** connects devices on different LAN's. The IP addresses for the Ethernet and wireless sides are different. In this example, the wireless link is part of LAN A, with the Client unit acting as a Router between LAN A and LAN B.

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



If more than two routers are required within the same radio network, then routing rules may need to be configured (refer section “3.18 Routing Rules” for further details).
There is no limit to the number of Bridges in the same network - although there is a limit of 128 Client units linked to any one Access Point.



1.2 Getting Started Quickly

Most applications for the XYR401-E require little configuration. The XYR401-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 Chapter 2, “Installation”. The XYR401-E requires an antenna and a power supply.

- Power the XYR401-E and make an Ethernet connection to your PC (for further information on how to do this, refer to section 3.2 “Configuring the Unit for the first time”)
- Set the XYR401-E address settings as per section 3.2 “Configuring the Unit for the first time”
- Save the configuration - the XYR401-E is now ready to use.

Before installing the XYR401-E, bench test the system. It is a lot easier to locate problems when the equipment is all together.

There are other configuration settings, which may or may not improve the operation of the system. For details on these settings, refer to section 3.0 “Start-up”.

Chapter Two INSTALLATION

2.0 General

The XYR401-E modules are housed in a rugged aluminium case, suitable for DIN-rail mounting. Terminals will accept wires up to 2.5 mm^2 (12 gauge) in size.

⚠ **All connections to the module must be SELV (Safety Extra Low Voltage). Normal 110-250V mains supply must not be connected to any terminal of the XYR401-E module. Refer to Section 2.2 Power Supply**.

Before installing a new system, it is preferable to bench test the complete system. Configuration problems are easier to recognize when the system units are 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 (i.e. path too long, or obstructed), a higher performance antennas or a higher mounting point for the antenna may rectify the problem. Alternately, use an intermediate XYR401-E Module as a repeater.

The XYR401-E ***Installation Guide*** provides an installation drawing appropriate to most applications. Further information is detailed below.

Each XYR401-E module should be effectively earthed via the "GND" terminal on the back of the module - this is to ensure that the surge protection circuits inside are effective.

2.1 Antenna Installation

The XYR401-E module will operate reliably over large distances however the achievable distances will vary with the application, radio model, type and location of antennas, the degree of radio interference, and obstructions (such as buildings or trees) to the radio path.

The maximum range achievable depends on the radio model, the regulated RF power permitted in your country, and whether you use separate transmit and receive antennas.

- If using a XYR401-E-G (2.4GHz) with a single antenna, 10 km (6 miles) can be achieved in USA, Canada and Australia (4W EIRP) and 2km in Europe (100mW EIRP).

To achieve the maximum transmission distance, the antennas should be raised above intermediate obstructions so the radio path is true “line of sight”. The modules will operate reliably with some obstruction of the radio path, although the reliable distance will be reduced. Obstructions which are close to either antenna will have more of a blocking affect than obstructions in the middle of the radio path.

The XYR401-E modules provide a diagnostic feature which displays the radio signal strength of transmissions (refer 34.0 “Diagnostics”).

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 short distances, it is possible to mount the antennas inside buildings. An obstructed path requires testing to determine if the path will be reliable.

Where it is not possible to achieve reliable communications between two XYR401-E modules, then a third XYR401-E module may be used to receive the message and re-transmit it. This module is referred to as a repeater. This module may also have a host device connected to it.

The XYR401-E unit has two antenna connections at the top of the module, allowing for two antennas to be fitted to the module if need be. By default the right connector labeled TX/RX is the main connection used to transmitter and receiver. The left connector labeled ―RX" is not connected unless configured under the Advanced Radio Configuration in Section 3.10. Each antenna port can be configured for TX only, RX only or Diversity (TX and RX). Selection can be made by choosing one of the options from TX Antenna / RX Antenna on the Advanced Radio Configuration page.

Note: When only one antenna is used, it must be connected to the TX/RX connector.

Antenna Diversity

One reason to use multi antennas is because of local radio licensing regulations. All countries have a limit on the amount of transmitted power and radiated power from the antenna. In the US this is 400 millwatts transmit power and 4 watts EIRP (Effective Isotropic Radiated Power). In a normal system if a high gain antenna is used it improves the receive signal as well as boosting the transmit signal and possibly pushing it over the EIRP regulation limit. Using Antenna diversity we can use two antennas, one for receive and the other for transmit. The receive antenna has no regulatory limits as it does not radiate power so any gain antenna can be used. To calculate the transmit antenna limit see the examples below.

Example

If using the XYR401-E-G in the US the radio transmit power level will be 400mA which will allow up to 4 watts EIRP, what this means is that we can add a gain of approximately 10dB (including cable loss) without infringing the EIRP. This is calculated by using the general rule of thumb when working with dB and Power which is doubling the power is a 3dB gain.

If using 10m (33ft) of Cellfoil coax cable (approximately 6dB of loss) and an 8 dBi Antenna this would equate to approximately 2dB of gain, well below our 10dB limit.

If using 20m (66ft) of Cellfoil coax cable (approximately 12dB of loss) and an 18 dBi Antenna this would equate to approximately 6dB of gain, which is also below our 10dB limit.

Another application where antenna diversity may be needed is in industrial plants and factories installations which can suffer from ―multi-path fading‖ effects where multiple reflected radio signals adversely affect the signal strength. In a ―static‖ installation, where the radio path is not changing, moving an antenna to the position of maximum signal solves this problem. However where the radio path changes because the XYR401-E is mounted on moving equipment, or if there is moving equipment in the area, then the solution is to use two antennas. Because the two connectors are separated, the RF signal at each connector will be different in the presence of multi-path fading. The XYR401-E unit will automatically select the higher RF signal provided RX diversity has been enabled on radio Config page.

See Section 3.10 ―Advanced Radio Configuration" for details on configuring Antenna Diversity

Line-of-sight installations

In longer line-of-sight installations, the range may be increased by using a high gain antenna on the TX/RX connector. However, the gain should not cause the effective radiated power (ERP) to exceed the permitted value. A second higher gain antenna can be connected to the RX connector without affecting ERP - this will increase the operating range provided any interference in the direction of the link is low.

Antennas

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

The net gain of an antenna/cable configuration is the gain of the antenna (in dBi) less the loss in the coaxial cable (in dB). The maximum net gain of the antenna/cable configuration connected to the TX/RX connector is 0dB in Europe (100mW ERP). In USA, Canada and Australia (4W ERP), the maximum gain is 10dB for the XYR401-E-400 or 16dB for the XYR401-E-100. There is no gain restriction for antennas connected to the RX connector.

(*) 20dB attenuator must be fitted if radio distance is less than 33ft (10m).

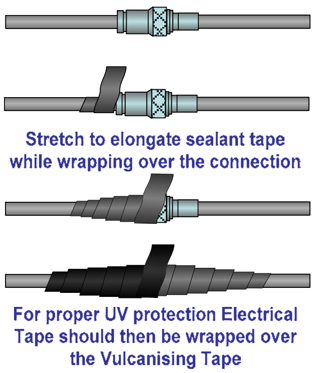
Antenna	***XYR401-E Gain (dBi)***
Dipole	2 dBi
Collinear	5 or 10 dBi
Directional	18 dBi
Cable Loss	***dB per 30 m / 100 ft***
RG58 Cellfoil	-17 dB
RG213	-16.2 dB
LDF4-50	-3.6 dB

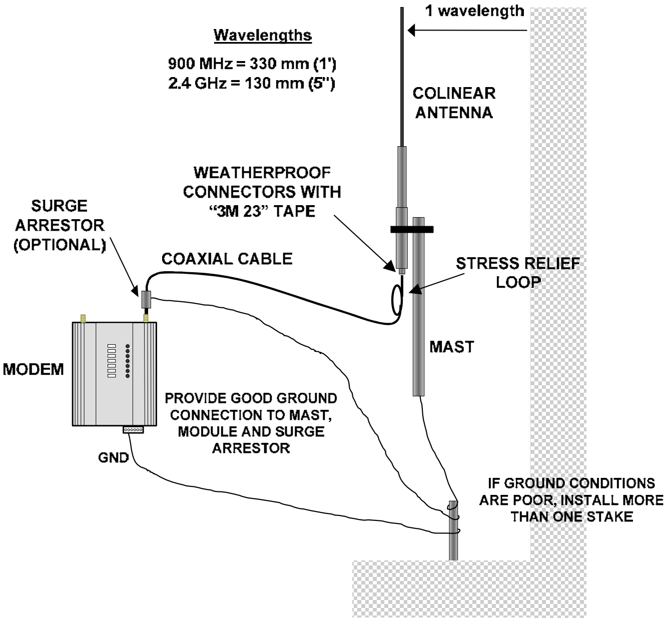
The net gain of the antenna/cable configuration is determined by adding the antenna gain and the cable loss.

For example, if using the XYR401-E a 10dBi antenna (7.8dBd) with 10 meters of Cellfoil (-5.6dB) has a net gain of 2.2dB (7.8dB – 5.6dB).

Installation tips

Connections between the antenna and coaxial cable should be carefully taped to prevent ingress of moisture. Moisture ingress in the coaxial cable is a common cause for problems with radio systems, as it greatly increases the radio losses. We recommend that the connection be taped, firstly with a layer of PVC Tape, then with 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.


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


Wavelengths
900 MHz = 330 mm (1')
2.4 GHz = 130 mm (5")
1 wavelength
COLINEAR ANTENNA
WEATHERPROOF CONNECTORS WITH “3M 23” TAPE
SURGE ARRESTOR (OPTIONAL)
COAXIAL CABLE
STRESS RELIEF LOOP
MAST
MODEM
PROVIDE GOOD GROUND CONNECTION TO MAST, MODULE AND SURGE ARRESTOR
GND
IF GROUND CONDITIONS ARE POOR, INSTALL MORE THAN ONE STAKE

Dipole and Collinear antennas

A dipole or collinear antenna transmits the same amount of radio power in all directions - as such that are easy to install and use. The dipole antenna with integral 15 ft (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 wavelength away (see drawing below for distances) from a wall or mast and at least 3ft (1m) from the radio module to obtain maximum range.

Directional antennas.

Directional antennas can be

- □ a Yagi antenna with a main beam and orthogonal elements, or
- □ a directional radome, which is cylindrical in shape, or
- □ a parabolic antenna.

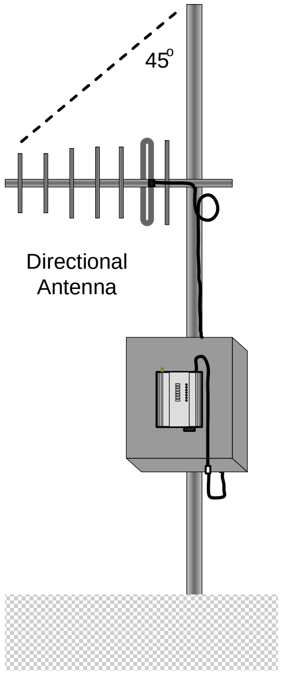
A directional antenna provides high gain in the forward direction, but lower gain in other directions. This may be used to compensate for coaxial cable loss for installations with marginal radio path.

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

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

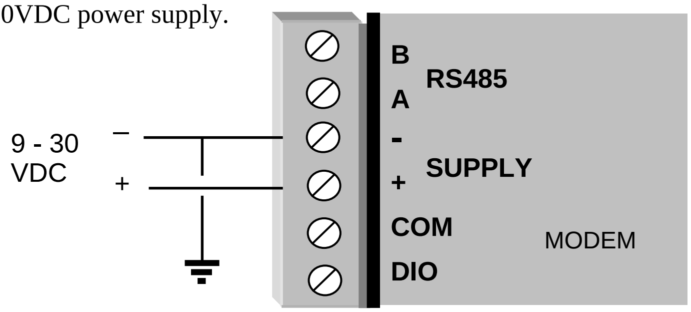
Parabolic antennas should be mounted as per the manufacturer’s instructions, with the parabolic grid at the “back” and the radiating element pointing in the direction of the transmission.

Ensure that the antenna mounting bracket is well connected to “ground/earth”.



2.2 Power Supply

The XYR401-E module can be powered from a 9 - 30VDC power supply. The power supply should be rated at 1 Amp. The positive side of the supply must not be connected to earth. The supply negative is connected to the unit case internally. The DC supply may be a floating supply or negatively grounded.



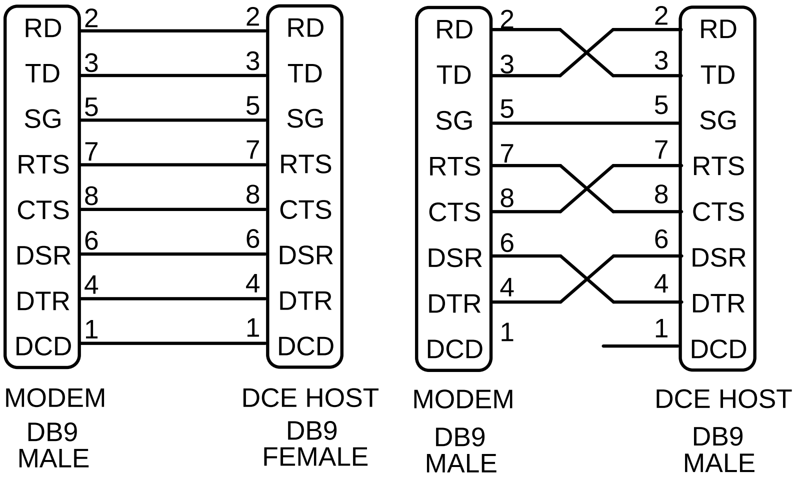
The power requirements of the XYR401-E unit are shown in the following table

	XYR401-E	
	12VDC	24VDC
Quiescent	290mA	150mA
TX @100mW	310mA	170mA
TX @ 400mW	340mA	180mA

A Ground Terminal is provided on the back of the module. This Terminal should be connected to the Main Ground point of the installation in order to provide efficient surge protection for the module (refer to the Installation Diagram)

2.3 Serial Connections

RS232 Serial Port
The 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 XYR401-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. The XYR401-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

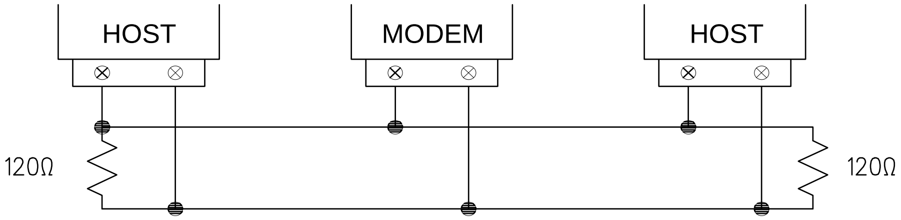
Pin	Name	Direction	Function
1	DCD	Out	**Data carrier detect**
2	RD	Out	**Transmit Data –** Serial Data Output (from DCE to DTE)
3	TD	In	**Receive Data –** Serial Data Input (from DTE to DCE)
4	DTR	In	**Data Terminal Ready**
5	SG		**Signal Ground**
6	DSR	Out	**Data Set Ready** - always high when unit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

RS485 Serial Port

The RS485 port provides for communication between the XYR401-E unit and its host device using a multi-drop cable. Up to 32 devices may be connected in each multi-drop network.

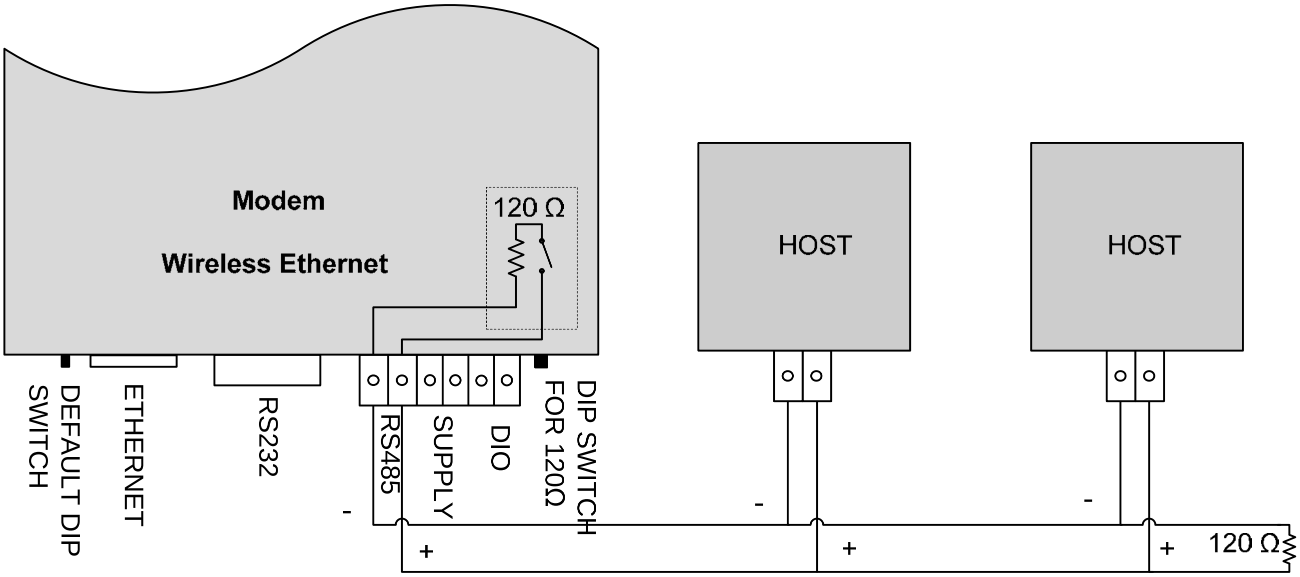
As the RS485 communication medium is shared, only one of the units on the RS485 cable may send data at any one time. Thus, communication protocols based on the RS-485 standard require some type of arbitration.

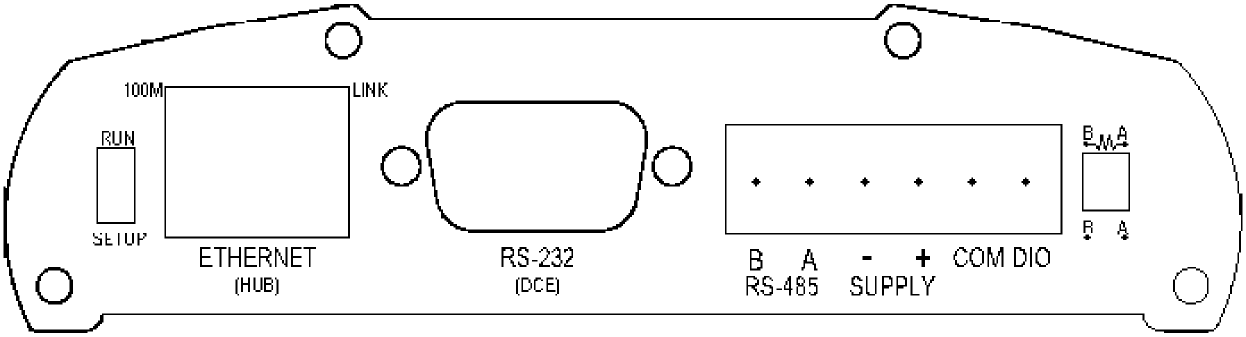
RS485 is a balanced, differential standard but it is recommended that shielded, twisted pair cable be used to interconnect modules to reduce potential RFI. It is important to maintain the polarity of the two RS485 wires. An RS485 network should be wired as indicated in the diagram below and terminated 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

Shorter runs of 485 cable may not require the termination resistors to be enabled.


Modem
Wireless Ethernet
120 Ω
HOST
HOST
DEFAULT DIP SWITCH
ETHERNET
RS232
RS485
SUPPLY
DIO
DIP SWITCH FOR 120Ω
-
+
-
+
-
+
120 Ω

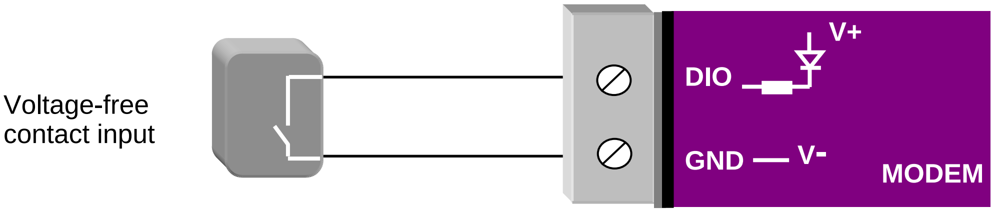

100M
LINK
RUN
SETUP
ETHERNET
(HUB)
RS-232
(DCE)
B
A
RS-485
-
+
SUPPLY
COM DIO
B A
B A

2.4 Discrete (Digital) Input/Output

The XYR401-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.

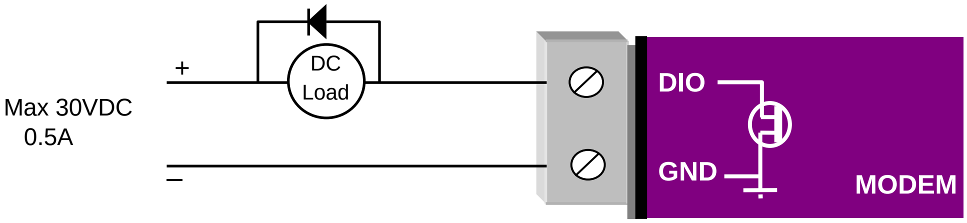
If used as an “input”, the I/O channel is suitable for voltage free contacts (such as mechanical switches) or NPN transistor devices (such as electronic proximity switches). PNP transistor devices are not suitable. Contact wetting current of approximately 5mA is provided to maintain reliable operation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



Chapter Three OPERATION

3.0 Start-up

“Access Point” Start-up (XYR401-E)

When an Access Point (AP) unit starts up it checks to see if the Channel selection is set to “Auto” and if so will scan all available channels, pick the quietest then begin transmitting periodic messages, called beacons, if it is configured with a fixed channel it will immediately begins sending beacons, on the configured channel.

Beacons include information that a Client may examine in order to identify if the Access Point is suitable for link establishment. Clients will only attempt to establish a link with an Access Point whose beacon indicates a matching SSID. Access Points do not initiate link establishment.

“Client” Start-up

When a Client powers up, it scans for beacons from Access Points. While a link is not established, the Client cyclically scans all available channels for a suitable Access Point. The Client will attempt to establish a link with an Access Point only if it has matching SSID, Encryption method, etc. and other compatible capabilities as indicated by the beacon. If more than one suitable Access Point is discovered, the client will attempt to establish a link with the Access Point that has the strongest radio signal.

Link Establishment

Once a Client identifies a suitable Access Point for link establishment it attempts to establish a link using a two step process – “Authentication” and “Association”. During Authentication the Client and Access Point check if their configurations permit them to establish a link. Once the Client has been authenticated, it will then request an Association to establish a link.

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

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

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

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

How a Link connection is lost

The Access Point refreshes the link status with a Client every time a message is received from that Client. If nothing is received from a Client for a period of 120 seconds, the Access Point sends a “link-check” message. If there is no response to the link-check a De-authenticate message is sent and the link is dropped.

A Client monitors beacon messages from an Access Point to determine whether the link is still present. If the Client can no longer receive beacons from the Access Point it assumes the AP is out-of-range and the link is dropped. Whenever a Client is not connected to an AP, it will cyclically scan all available channels for a suitable AP.

Roaming Clients

Clients can roam within a system however if the link to the Access Point fails or the radio signal level becomes too weak it will scan for beacons and connect to an Access Point (provided the SSID and any Encryption methods, keys, etc are compatible). If there are multiple Access Points it will select the connection with the best signal level. This functionality permits a client to have mobility whilst maintaining a link with the most suitable AP.

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	Flashing RED / GREEN	Module Boot Sequence
Radio RX	GREEN flash	Radio receiving data (Good Signal Strength)
Radio RX	RED flash	Radio receiving data (Low Signal strength)
TX/LINK	GREEN	Radio Connection Established
TX/LINK	RED Flash	Radio Transmitting
RS-232	GREEN flash	Data sent from RS-232 Serial Port
RS-232	RED flash	Data received to RS-232 Serial Port
LAN	ON	Link Established on Ethernet port
LAN	Flash	Activity on Ethernet port.
RS-485	GREEN flash	Data sent from RS-485 Serial Port
RS-485	RED flash	Data received to RS-485 Serial Port
DIO	GREEN	Digital Input is grounded.
DIO	RED	Digital Output is active
DIO	Off	Digital Output OFF ***and*** Input is open circuit.

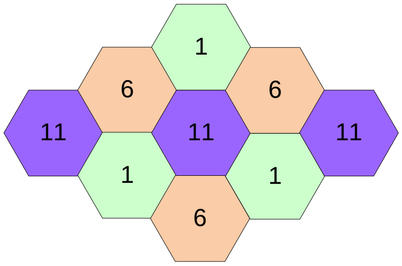
The Ethernet RJ45 port incorporates two indication LEDs. The LINK LED comes on when there is a connection on the Ethernet port, and will blink off briefly when activity is detected on the Ethernet Port. The 100MB LED indicates that the connection is at 100 MBit/Sec. The 100MB LED will be off for 10MB/Sec connection.
Other conditions indicating a fault are described in Chapter Four - DIAGNOSTICS.

3.1 Selecting a Channel

802.11b/g (2.4GHz)
The XYR401-E conforms to the IEEE 802.11b/g Wireless LAN specification. The XYR401-E supports 13 x 20MHz, 12 x 10MHz and 13 x 5MHz radio channels in the 2412MHz to 2482MHz frequency range. Channels are country or region specific. Please check your local regulatory body for compliance and channel selection.

You can see from the diagram below there are a limited number of channels available in the 2.4 GHz frequency range. Care must be taken when selecting an operating channel as some of the channels overlap.

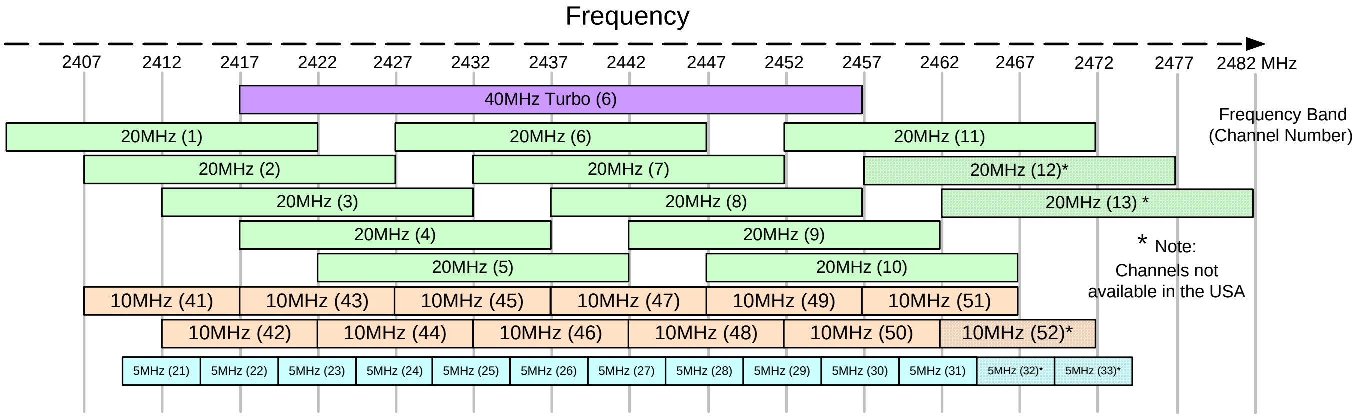
The 20M channels have a separation of 5MHz which means there is some overlap into the next channel, i.e. channel 1 will overlap into channel 2, 3 and 4; channel 6 will overlap into channels 3, 4, 5, 7, 8 and 9. If complete separation is required then you can use channels 1, 6 and 11 without any interference between the channels.



The 10M channels are also separated by 5MHz and overlap the adjacent channels by 5MHz forward and backward, i.e. Channel 41 will overlap with channel 42; channel 46 will overlap with channel 45 and 47.

Lastly the 5MHz channels are separated by 5MHz and do not overlap at all so you can operate all 13 channels at the same time with minimal interference with the adjacent channel.

Only one of these channels is used at a time and is configured at the Access Point, The Access Point then uses this channel to send out beacon transmissions and connections.
Clients scan all channels for a suitable Access Point and then adopt the same channel as the AP when a connection is established. 20MHz (7), 5MHz (23), 10MHz (41), 20MHz (2), 20MHz (1), 20MHz (6), 20MHz (11), 20MHz (8), 20MHz (3), 20MHz (9), 20MHz (4), 20MHz (10), 20MHz (5), 5MHz (22), 5MHz (21), 5MHz (24), 5MHz (33), *5MHz (27), 5MHz (26), 5MHz (25), 5MHz (28), 5MHz (31), 5MHz (30), 5MHz (29), 5MHz (32), *10MHz (43), 10MHz (45), 10MHz (47), 10MHz (49), 10MHz (51), 10MHz (42), 10MHz (44), 10MHz (46), 10MHz (48), 10MHz (52), *40MHz Turbo (6), 10MHz (50), 20MHz (12), *20MHz (13) * Frequency Band(Channel Number)24122417243224422452246224222427243724472457246724 07, Frequency2482 MHz24722477*
Note:Channels not available in the USA

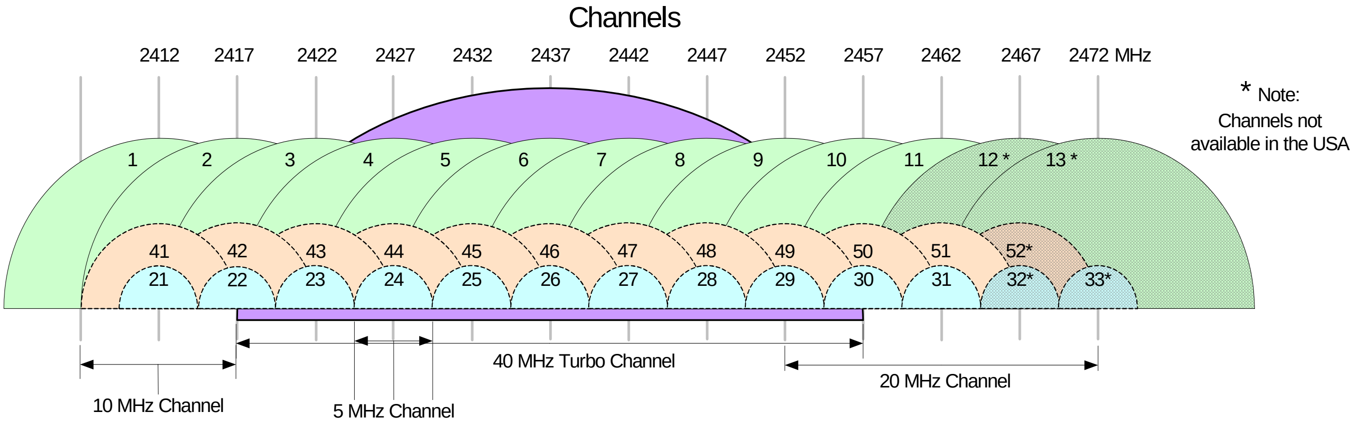


The following diagram shows the RF energy distribution for the 802.11b/g transmission:
On the 20MHz channel (Green) most of the energy is transmitted within the channel however some of the energy is transmitted on the channels either side therefore causing interference on the these channels. The 10MHz channels (Orange) are similar with half of the energy overlapping into the next channel however you can configure up to 6 x non interfering channel at the one time. Lastly the 5 MHz channels (Blue) do not overlap and so all 13 channels can be used at the same time.

There is also a single 40MHz Channel (Purple) which takes up over half of the full 2.4 GHz band and so it much more susceptible to interference from other channels.
If there is more than one 802.11 AP within the same wireless range, then it is important that the AP's are on channels as far apart as possible.
If there are two 20MHz channel AP's, then set them to channel 1 and 11. If there are three, set them to 1, 6, and 11.

If there is more than one 802.11 AP within the same wireless range, then it is important that the AP's are on channels as far apart as possible.

If there are only two AP's, then set them to 1 and 11. If there are three, set them to 1, 6, and 11.



Dynamic Frequency Selection (DFS)
Because of the push within the 802.11a market to open up new spectrum for unlicensed radio a mechanism called "Dynamic Frequency Selection" needed to be developed so that the 802.11 Wi-Fi could coexist with existing military and telecommunication radar systems.
Access points with 5GHz radios comply with regulations that require radio devices to use Dynamic Frequency Selection (DFS), which can detect radar signals and avoid interfering with them by automatically scanning and then selecting another channel or band.
When DFS is enabled, the Access Point (master device) goes through the following steps:

1. The master device that initiates communications selects a channel and monitors that channel for potential radar interference for a minimum listening time of 60sec (channel availability check time). No transmissions can occur during this period.

2. If interference is detected then the system has to go and select another channel and repeat the channel availability check on the new channel (the original channel is added to a list of channels with radar).

3. Once a channel has been selected and passes the channel availability check the network starts to use that channel.

4. While using the channel the network's master device continuously monitors for potential interference from a radar source (this is referred to as "in-service monitoring"). If interference is detected then the network master device issues commands to all other in-network devices to cease transmissions. The channel is added to the list of channels with radar.

5. The master device then selects a new channel (one that is not on the radar list).

6. A channel that has been flagged as containing a radar signal, either by a channel availability check or by in-service monitoring, is subject to a 30 min non-occupancy period where it cannot be used by the device in order to protect scanning radars. The channel on the radar list will be purged once the non-occupancy period has elapsed for that channel.

3.2 Configuring the Unit for the first time

The XYR401-E has a built-in web server, containing web pages for analyzing and modifying the module's configuration. The configuration can be accessed using Microsoft® Internet Explorer version 7 or greater. This program is shipped with Microsoft Windows or may be obtained freely via the Microsoft® website. If using other browsers they must be fully compliant with IE7 SSL security.

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

Default Configuration
The default factory configuration of the XYR401-E is

- Client/Bridge/
- IP address192.168.0.1XX, where XX is the last two digits of the serial number (the default IP address is shown on the printed label on the back of the module)
- netmask 255.255.255.0
- Username is "*user*" and the default password is "*user*"

The XYR401-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. **When in SETUP mode, wireless operation is disabled.** The previous configuration remains stored in non-volatile memory and will only change if a configuration parameter is modified and the change saved.

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

Accessing Configuration for the first time

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

Method 1 - Change your computer settings so that the configuring PC is on the same network as the XYR401-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 XYR401-E. The factory default Ethernet address for the XYR401-E is 192.168.0.1XX where XX are the last two digits of the serial number (check the label on the back of the module).

Method 2 - Requires temporarily changing the IP address in the XYR401-E via an RS232 connection such that it is accessible on your network without having to change your PC network settings. When connected you can change the modem network settings to match that of your network.

Method 1 - Set PC to same network as XYR401-E

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

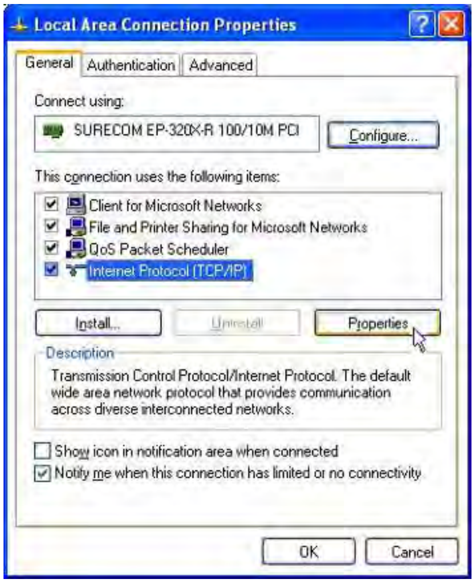
- Set the Factory Default Switch to the SETUP position. This will always start the XYR401-E with Ethernet IP address 192.168.0.1XX, subnet mask 255.255.255.0, gateway IP 192.168.0.1 and the radio disabled. **Do not forget** to set the switch back to the RUN position and restart the module at the conclusion of configuration for resumption of normal operation.

- Power up the XYR401-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.



Local Area Connection Properties

General | Authentication | Advanced

Connect using:

SURECOM EP-320X-R 100/10M PCI — Configure...

This connection uses the following items:

☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ QoS Packet Scheduler
☑ Internet Protocol (TCP/IP)

Install... | Uninstall | Properties

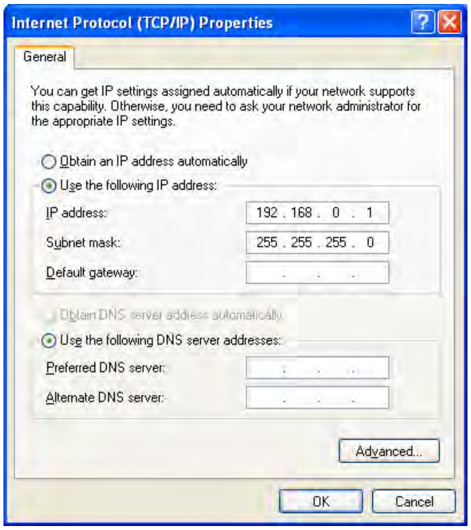
Description

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

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

OK | Cancel

- On the General tab enter IP address 192.168.0.1, Subnet mask 255.255.255.0 and press “OK”



Internet Protocol (TCP/IP) Properties

General

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

○ Obtain an IP address automatically
● Use the following IP address:

IP address: 192 . 168 . 0 . 1
Subnet mask: 255 . 255 . 255 . 0
Default gateway: . . .

○ Obtain DNS server address automatically
● Use the following DNS server addresses:

Preferred DNS server: . . .
Alternate DNS server: . . .

Advanced...

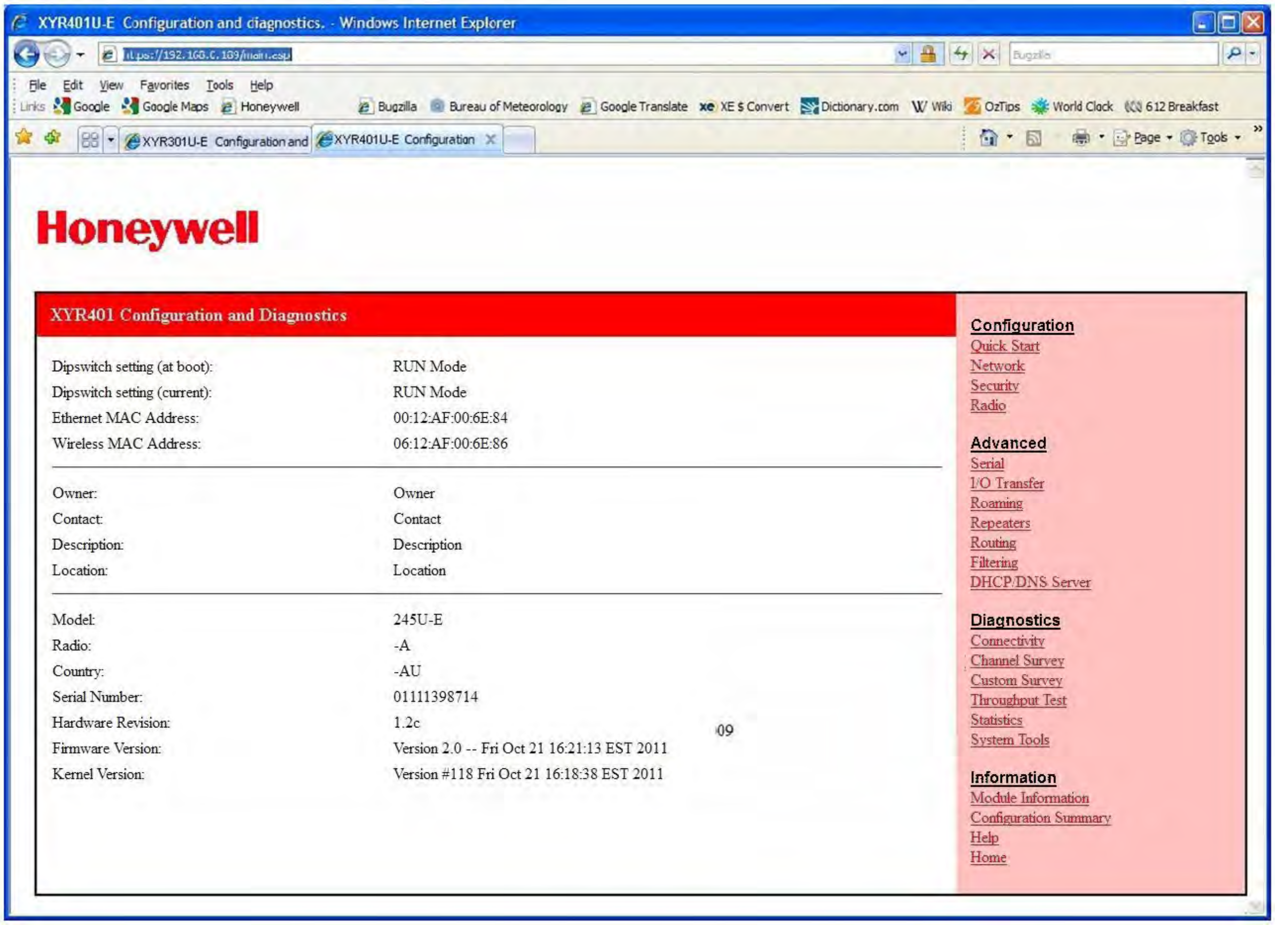
OK | Cancel

- 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 XYR401-E *https://192.168.0.1XX* where XX is the last two digits of the serial number.

- Enter the username “*user*” and default password “*user*”.


XYR401U-E Configuration and diagnostics. - Windows Internet Explorer
File Edit View Favorites Tools Help
Links Google Google Maps Honeywell Bugzilla Bureau of Meteorology Google Translate XE $ Convert Dictionary.com Wiki OzTips World Clock 612 Breakfast
XYR301U-E Configuration and
XYR401U-E Configuration
Page Tools
Honeywell
XYR401 Configuration and Diagnostics
Configuration
Quick Start
Network
Security
Radio
Advanced
Serial
I/O Transfer
Roaming
Repeaters
Routing
Filtering
DHCP/DNS Server
Diagnostics
Connectivity
Channel Survey
Custom Survey
Throughput Test
Statistics
System Tools
Information
Module Information
Configuration Summary
Help
Home
09

Dipswitch setting (at boot):	RUN Mode
Dipswitch setting (current):	RUN Mode
Ethernet MAC Address:	00:12:AF:00:6E:84
Wireless MAC Address:	06:12:AF:00:6E:86
Owner:	Owner
Contact:	Contact
Description:	Description
Location:	Location
Model:	245U-E
Radio:	-A
Country:	-AU
Serial Number:	01111398714
Hardware Revision:	1.2c
Firmware Version:	Version 2.0 -- Fri Oct 21 16:21:13 EST 2011
Kernel Version:	Version #118 Fri Oct 21 16:18:38 EST 2011

Figure 1 – Welcome Webpage

To resume normal configured operation when Configuration is complete, switch Factory Default dip-switch on the XYR401-E to RUN and cycle power.

Note: **Security Certificates**. Configuration of the XYR401-E uses an encrypted link (https). The security certificate used by the XYR401-E is issued by HONEYWELL and matches the IP address 192.168.0.100.

When you first connect to the XYR401-E, your web browser will issue a warning that HONEYWELL is not a trusted authority. Ignore this warning and proceed to the configuration web page. To avoid seeing this warning in future, you can install the certificate into your browser.

Internet Explorer 7 has an additional address check on security certificates. Unless the XYR401-E has the address 192.168.0.100, when you first connect to the XYR401-E, Internet Explorer 7 will issue a warning about mismatched security certificate address. You can turn off this behaviour in IE7 by selecting

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

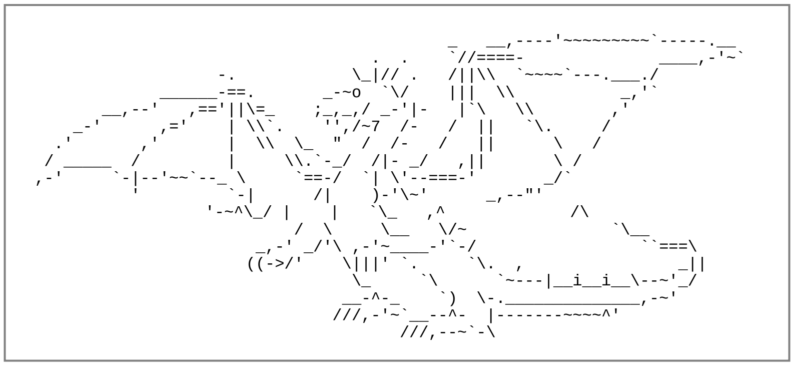
Method 2 - Set XYR401-E Network address to match the local network

For this method you will need to determine what IP address, Gateway address, and netmask to assign to the XYR401-E so that it appears on your network. Ask your system administrator if you don’t know the correct settings for your network. E.g.

The default IP address of the XYR401-E modem is 192.168.0.1 and the network you wish to connect to is on 10.10.0.X (PC is on 10.10.0.5)

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

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



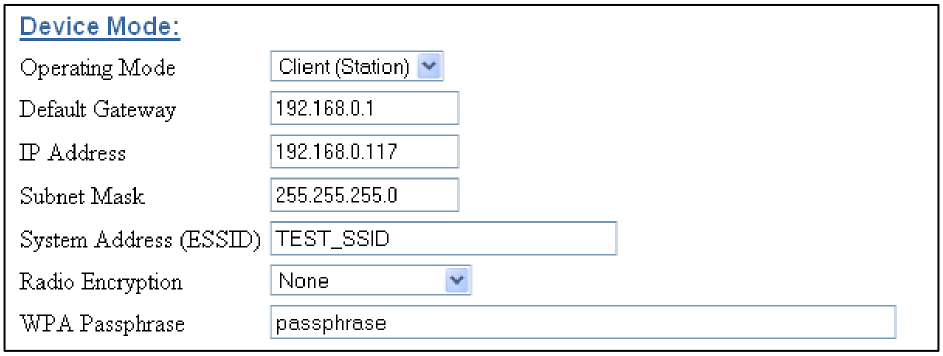
- Type the following "ifconfig" and it will show the configuration of the Ethernet port and from this you will be able to see what the IP address is, e.g.

```
eth0   Link encap:Ethernet  HWaddr 00:12:AF:FF:FF:FF
       inet addr:192.168.0.1  Bcast:192.168.0.255  Mask:255.255.255.0
       UP BROADCAST RUNNING MULTICAST MTU: 1500 Metric: 1
       RX packets:8 errors:0 dropped:0 overruns:0 frame:0
       TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
       collisions:0 txqueuelen:256
```

- Temporarily change the IP address to something that will enable connection to your local network. E.g type "ifconfig eth0 10.10.0.6 netmask 255.255.255.0" only add the netmask if the netmask is anything other than the standard 255.255.255.0
- IP address should now be changed and you can check by typing "ifconfig" again. Note these changes are only temporary and if the module is reset they will go back to the normal default (192.168.0.XXX).
- Open Internet Explorer and ensure that settings will allow you to connect to the IP address selected. If the PC uses a proxy server, ensure that Internet Explorer will bypass the Proxy Server for local addresses. This option may be modified by opening Tools -> Internet Options -> Connections Tab -> LAN Settings->Proxy Server -> bypass proxy for local addresses.
- Enter the IP address for the XYR401-E into the Internet Explorer Address bar e.g. http://10.10.0.6 which is the IP address you temporarily configured with the ifconfig command.
- Enter the username "*user*" and default password "*user*".
- You should now be connected to the main index page on the modem as per figure 1 above.
- From here connect to the Network page and change the Ethernet Interface and Wireless Interface IP addresses to 10.10.0.6. Switch the RUN/SETUP switch back to RUN and press "Save Changes and Reset" button.

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

3.3 Quick Start Configuration



Device Mode:

Operating Mode	Client (Station)
Default Gateway	192.168.0.1
IP Address	192.168.0.117
Subnet Mask	255.255.255.0
System Address (ESSID)	TEST_SSID
Radio Encryption	None
WPA Passphrase	passphrase

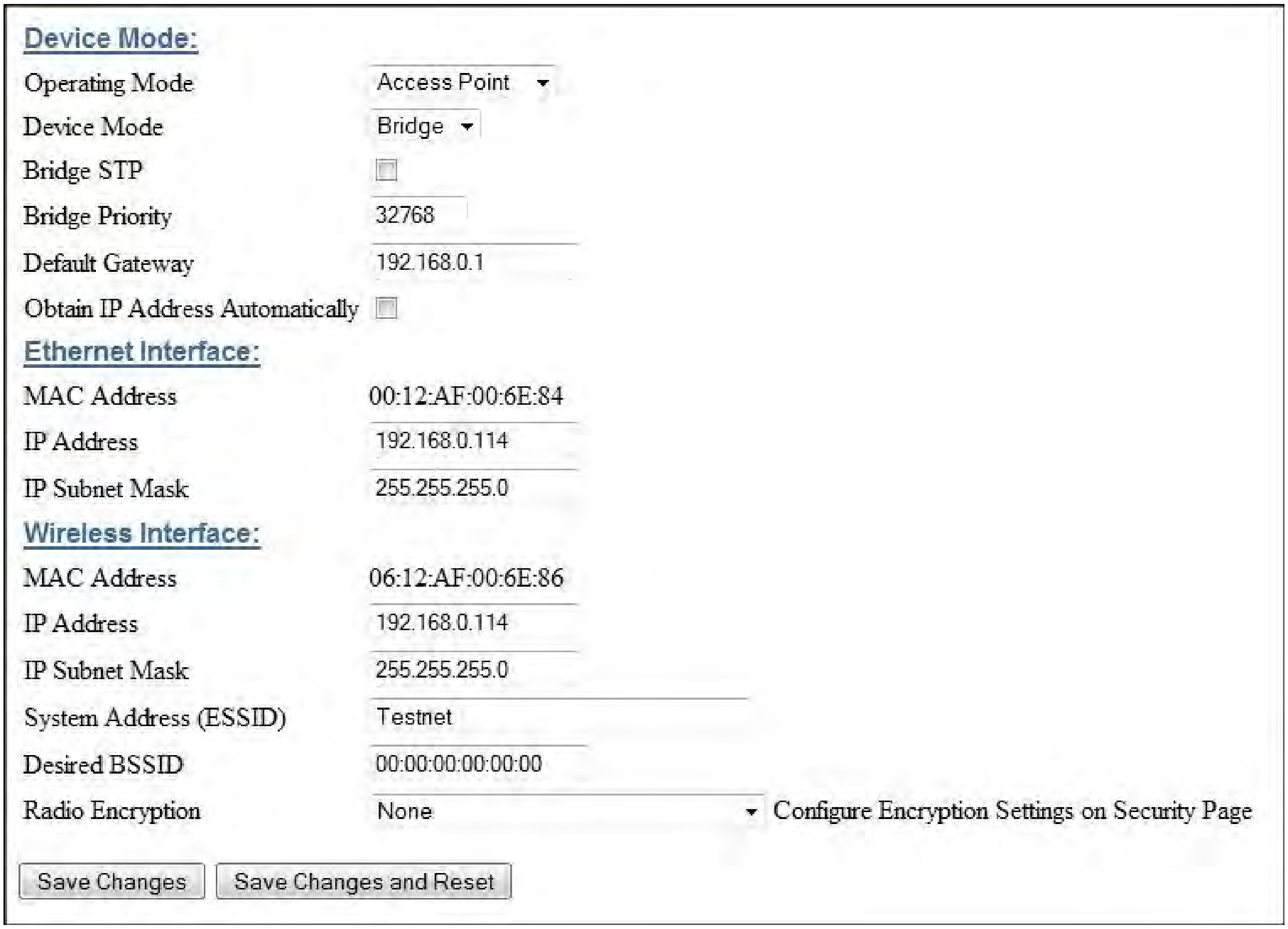
The XYR401 E has a Quick Start Configuration option, which will cover most important parameters that are needed to get an initial connection. This is the first stage of the module configuration. For most applications, no further configuration is required. For more advanced applications, the other parameters can be changed via the normal configuration pages after the Quick Start configuration has been saved.

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

Quick Start Configuration	
Operating Mode	Access Point or Client. Bridge operation is assumed - for Router selection, go to the Network page after Quick Start
Default Gateway	This is the address that the device will use to forward messages to remote hosts that are not connected to any of the local bridged network (Ethernet or Wireless)
IP Address / Subnet Mask	IP Address and Subnet Mask for your application.
System Address (ESSID)	The system address is a text string 1 to 31 characters in length used to identifies your system
Radio Encryption	Radio encryption selection - None, WPA-PSK (TKIP), WPA-PSK (AES) or WPA2 – refer to the Network Configuration section if WEP or Enterprise encryption is required.
WPA Passphrase	128bit Encryption keys are internally generated based on the Passphrase and System Address (ESSID). The Passphrase must be between 8 and 63 characters in length, and must be the same for all 245U-E units in the same system.

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.
After configuring, select “Save to Flash and Reset”.
Radio Data Rate and Channel will be set to Auto, Radio Transmit Power will be set to maximum and any previous configuration of unrelated parameters will not be modified, and will still apply.

3.4 Network Configuration



Device Mode:

Operating Mode	Access Point ▾
Device Mode	Bridge ▾
Bridge STP	□
Bridge Priority	32768
Default Gateway	192.168.0.1
Obtain IP Address Automatically	□

Ethernet Interface:

MAC Address	00:12:AF:00:6E:84
IP Address	192.168.0.114
IP Subnet Mask	255.255.255.0

Wireless Interface:

MAC Address	06:12:AF:00:6E:86
IP Address	192.168.0.114
IP Subnet Mask	255.255.255.0
System Address (ESSID)	Testnet
Desired BSSID	00:00:00:00:00:00
Radio Encryption	None ▾ Configure Encryption Settings on Security 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 "user" as the password in the password field (This is the factory default – See section 3.23 "Module Information Configuration" to change). If you have forgotten the IP address or password, the Factory Default switch may be used to access the existing configuration. Refer to previous section above for this procedure.

The Network Configuration page allows configuration of parameters related to the wired and wireless Ethernet interfaces. In general, IP address selection will be dependant upon the connected wired Ethernet device(s) – before connecting to an existing LAN consult the network administrator.

A system of XYR401-E's must have at least one Access Point configured as a master with one or more Clients. All XYR401-E's should be given the same System Address (ESSID) and Radio Encryption settings. For further information and examples on wireless network topologies refer section 1.1 "Network Topology" above.

The XYR401-E supports several different radio encryption schemes. If utilising any form of encryption, all modules in the system that communicate with each other will need the same encryption method and encryption keys.

WEP (*Wired Equivalent Privacy*) encryption is the weakest encryption method, defined by the original IEEE802.11 standard and uses a 40bit or 104bit key with a 24bit initialization vector to give a 64bit and 128bit WEP encryption level. WEP is not considered an effective security scheme, and should only be used if it is necessary to interoperate with other equipment which does not support more modern encryption methods.

WPA (*Wi-Fi Protected Access*) is a subset of the IEEE802.11i Security Enhancements specification.
The XYR401-E supports WPA-1 TKIP and WPA-2 AES using a *Pre-Shared Key* (PSK).

- TKIP (*Temporal Key Integrity Protocol*) enhances WEP by using 128-bit encryption plus separate 64bit Tx and Rx MIC (*Message Integrity Check*) keys.
- AES (*Advanced Encryption Standard*), the most secure encryption method, is also based on 128-bit encryption key and is the recommended encryption method in most applications.

WPA-Enterprise (802.1x) removes the need to manage the Pre-shared Key (PSK) by using an external server to provide client authentication. Clients that are not authorized will be prevented from accessing the network. Once a client has provided the correct authentication credentials, access is permitted and data encryption keys are established, similar to WPA-PSK. Fine-grain (user level) access control can be achieved using this method.
An 802.1x capable RADIUS server may already be deployed in a large scale network environment. The XYR401-E can make use of this server reducing replication of user authentication information.

In a typical WPA-enterprise setup, the XYR401-E Access point acts as Authenticator, controlling access to the network. Wireless clients (XYR401-E's, Laptops or other devices) act as Supplicants, requesting access to the network. The Authenticator communicates with an authentication (RADIUS) server on the Ethernet network to verify Supplicant identity. When a Supplicant requests access, it sends an access request to the Authenticator, which passes an authentication request to the external authentication server. When the user credentials of the Supplicant are verified, the Authenticator enables network access for the Supplicant, data encryption keys are established and network traffic can pass.
Configuration of WPA-Enterprise differs when the unit is configured as an Access point (Authenticator) or Client (Supplicant).
If WDS interfaces are used, it is possible for one XYR401-E to act as both an Authenticator and a Supplicant, however in this situation, only one set of user credentials can be entered for all Supplicants.
After changes are made to Network Configuration, it is important to save the configuration by selecting "Save Changes" or by selecting "Save Changes and Reset".

Network Settings Webpage Fields

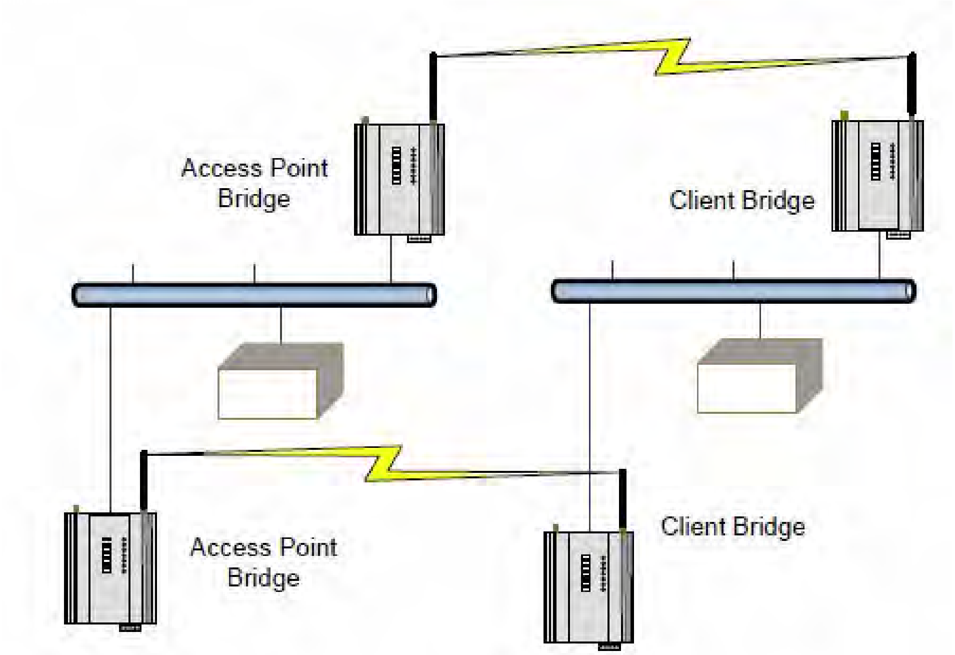
Operating Mode	Used to select Access Point (Infrastructure), Client (Infrastructure). By default this is set to Client.
Device Mode	Used to select Bridge or Router mode. By default this is set to Bridge.
Bridge STP	Checking this box enables Spanning Tree protocol in bridged networks. See to section **Error! Reference source not found.** "**Error! Reference source not found.**"" for more details
Bridge Priority	This is the priority associated with the Spanning tree protocol. Use lower numbers to move this station towards the root of the Spanning Tree, and use higher number here to move the station towards the leaves of the tree.
Default Gateway	This is the address that the device will use to forward messages to remote hosts that are not connected to any of the local bridged network (Ethernet or Wireless). This is only required if the wired LAN has a Gateway unit which connects to devices beyond the LAN - for example, Internet access. If there is no Gateway on the LAN, set to the same address as the Access Point - that is, the "Ethernet IP Address" below. Refer to section 3.19 "Routing" for more information.
Obtain IP Address Automatically	Checking this item enables DHCP client on the XYR401-E. A DHCP client requests its IP address from a DHCP server which assigns the IP Address automatically. For more information, refer to section 3.21 "DHCP Server Configuration", Default is unchecked.
MAC Address	This is the unique hardware address of the XYR401-E and is assigned in the Factory. The XYR401-E has two MAC addresses, one for each interface (Ethernet and Wireless) The Ethernet MAC is the primary MAC Address.
IP Address	The IP address of the XYR401-E on its wired (Ethernet Interface) port and wireless (Wireless Interface) port. This should be set to the IP address you require. If the device mode is set to bridge, then the wired and wireless ports will have the same IP address.

IP Subnet Mask	The IP network mask of the XYR401-E on its wired (Ethernet Interface) port and wireless (Wireless Interface) port. This should be set to appropriate subnet mask for your system (Typically 255.255.255.0).
System Address (ESSID)	A XYR401-E wireless network comprises modules with the same "system address”. Only modules with the same system address will communicate with each other. The system address is a text string 1 to 31 characters in length. Select a text string which identifies your system.
Desired BSSID	To force a client/station to always connect to the same Access Point enter the MAC address of that Access Point in the Desired BSSID field (Note that the ESSID of the Access Point must also match the configured ESSID of the client).
Radio Encryption	Select the desired radio Encryption level. Encryption key, passphrase, etc is entered on the “Security Menu” (See section 3.5 below for details)
Save Changes	Save changes to non-volatile memory. The module will need to be restarted before the changes take effect.
Save Changes and Reset.	Save settings to non-volatile memory, and reboot XYR401-E. Once the module has completed the reboot sequence, all changes are in effect.

3.5 Spanning Tree Algorithm

The bridge ―Spanning Tree Protocol" function was introduced to handle network loops and provide redundant paths in networks. To enable tick the STP box on any ―WDS Connections" you have configured on the ―Repeaters || configuration page.

For example, consider this network with a redundant wireless link. If the bridge Spanning Tree Protocol is enabled, one of the two wireless links will be disabled - that is, all wireless data will be transferred by one link only. If the active link fails, the other link will automatically start transferring the wireless data.



The Spanning Tree Protocol implemented is IEEE 802.1d compatible. The algorithm forms a loop-free network by blocking traffic between redundant links in the network. These blocked links are placed in a standby condition, and may be automatically enabled to repair the network if another link is lost. The Spanning Tree Algorithm maintains a single path between all nodes in a network, by forming a tree-like structure. The Bridge Priority determines where the node sits in the tree. A Bridge configured with the lowest priority (0) will become the root node in the network, and will direct traffic between each of its branches. The root node is typically the unit that handles the majority of traffic in the network. The XYR401-E is configured with a Bridge Priority of 32768 by default. The intention is to reduce traffic that the XYR401-E must handle, by placing it at the branch level in the network tree. As a branch, the XYR401-E needs only pass traffic to devices that are its ―leaves".

There is some overhead in maintaining a network utilizing the Spanning Tree Algorithm. Users wishing to increase their throughput, at the expense of redundancy should disable Spanning Tree. The Spanning Tree Protocol can be configured on the Repeaters configuration page.

3.6 Compatibility

3 Address (Layer 3 Bridge) & 4 Address Mode

What Addresses are in a wireless Ethernet data frame?

There are two different Wi-Fi communication ―modes" 3 Address and 4 Address Modes. Each mode has a slightly different way that it addresses the data frames to other devices on the network.

In 3 Address Mode the addressing is made up of a Destination Address (DA), a Source Address (SA), and a BSSID (MAC Address of the Access Point)

In 4 Address Mode the addressing is made of a Destination Address (DA), a Source Address (SA), a Radio Transmit Address (RTA), and a Radio Receive Address (RRA).

Packets between AP and Client

Communications between Access Points and Client is generally done using 3 Address Mode because there are only 3 addresses within the communication path as indicated in the path from the Laptop to Station #1 in the diagram below.

If the Laptop wishes to communicate to Station #1 the DA will be Station #1, the SA will be the Laptop and the BSSID will be the AP's MAC Address hence the 3 Address Mode.

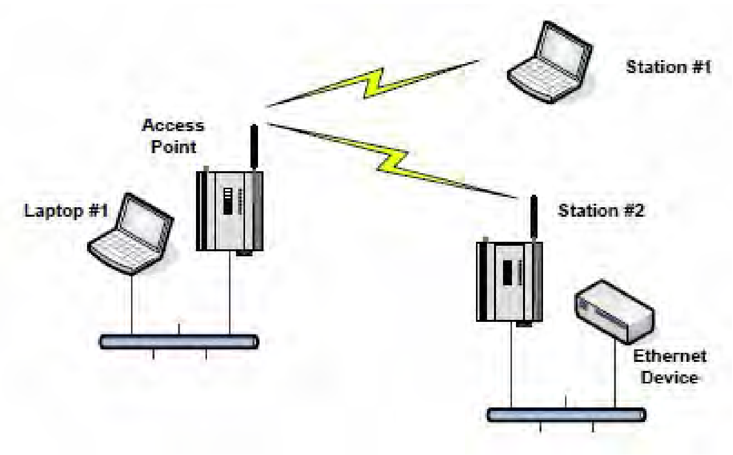
The example shows the Laptop may need to communicate to the Ethernet Device connected to Station #2.

You can see that there is now a fourth address that cannot be addressed using the 3 Address Mode of communications.

i.e. Laptop, AP, Station #2 and Ethernet Device.

The example shows the Access Point and the Station as both being XYR401-E modules which will happily communicate as both support 4 Address Mode.

However, there are some instances where a third Party Access Point may not be able to communicate using 4 Address Mode to a Client (Sta).



There are only a couple of ways around this sort of situation.

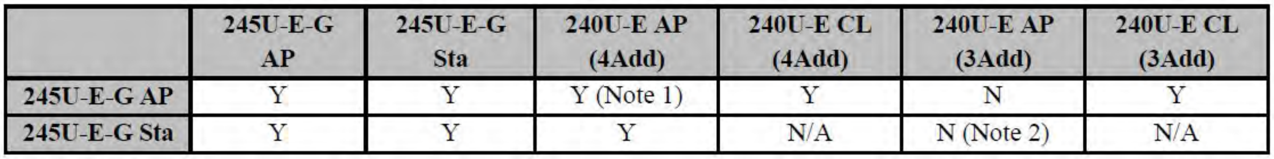
- Changing Station #2 to a Router, however this may mean that Station #2 and the Ethernet Device will use a different network address scheme which may be inconvenient and will require more setup.
- Configure the Access Point to communicate 4 Address Mode

If choosing the later this will only be possible if the Station and the AP support 4 Address Mode, some third Party AP's do not.

240U-E Compatibility

XYR401-E-G modules can communicate with ELPRO 240U-E Ethernet modems however only in certain modes. The following table shows compatible configurations.

If communicating with ELPRO 240U-E Ethernet modems the 240U-E's need to be configured with WDS (4 address mode), not the default —3-address mode || and the 240U-E AP's cannot be auto connect to any WDS AP.



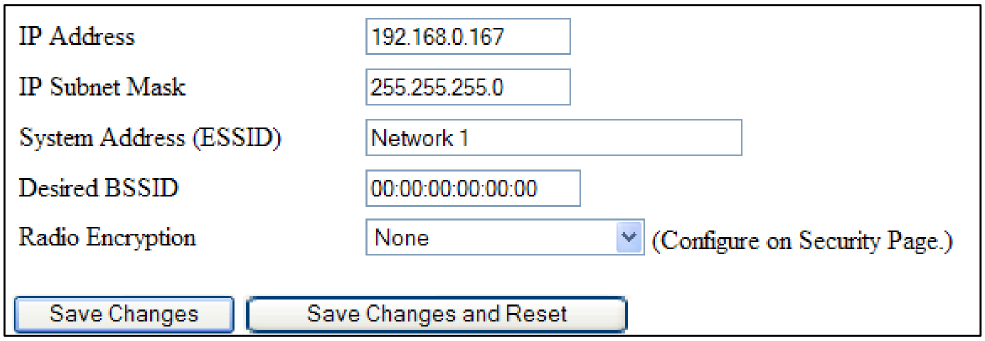
	245U-E-G AP	245U-E-G Sta	240U-E AP (4Add)	240U-E CL (4Add)	240U-E AP (3Add)	240U-E CL (3Add)
245U-E-G AP	Y	Y	Y (Note 1)	Y	N	Y
245U-E-G Sta	Y	Y	Y	N/A	N (Note 2)	N/A

Notes:
1. Connection only if the XYR401-E-G is configured with a virtual Station (Client) which in turn connects to the 240U-E Access Point.

2. Connection indication in the —connectivity || pages however it is not a true connection (see —3 Address & 4 Address Modes || above).

3.7 Security Menu

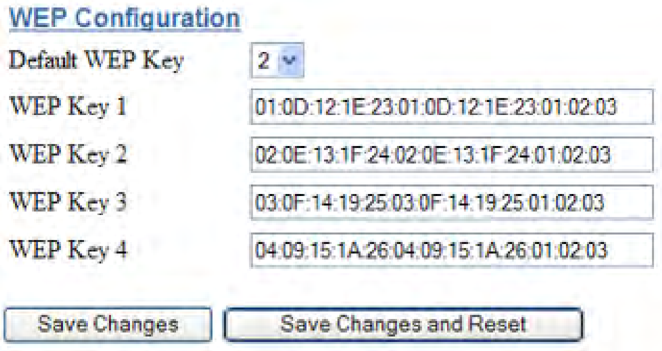
Select the Radio Encryption level from the drop down menu on the Main index page and then press the "Save Changes" button.
Available encryption levels are - "None", "WEP (64-bit)", "WEP (128-bit)", "WPA-PSK (TKIP)", "WPA-PSK (AES)", "WPA2-PSK (AES)", "WPA-PSK/ WPA2-PSK" & WPA-Enterprise. The default setting is "None".



IP Address	192.168.0.167
IP Subnet Mask	255.255.255.0
System Address (ESSID)	Network 1
Desired BSSID	00:00:00:00:00:00
Radio Encryption	None (Configure on Security Page.)

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

<u>Encryption Keys 1 to 4</u>
These are the keys used to encrypt radio data to protect data from unwanted eavesdroppers when WEP Encryption is selected. These keys should be the same for all XYR401-E units in the same system.
One of the four keys may be selected as the default key, and is used to encrypt transmitted messages from the configured unit. An XYR401-E can receive and decrypt a message from a module that has a different default key index as long as each module has the same key configured at the same index.
WEP keys must be entered as pairs of hexadecimal digits separated by colons. Hexadecimal digits are in the range 0...9 and A...F.



WEP Configuration

Default WEP Key	2
WEP Key 1	01:0D:12:1E:23:01:0D:12:1E:23:01:02:03
WEP Key 2	02:0E:13:1F:24:02:0E:13:1F:24:01:02:03
WEP Key 3	03:0F:14:19:25:03:0F:14:19:25:01:02:03
WEP Key 4	04:09:15:1A:26:04:09:15:1A:26:01:02:03

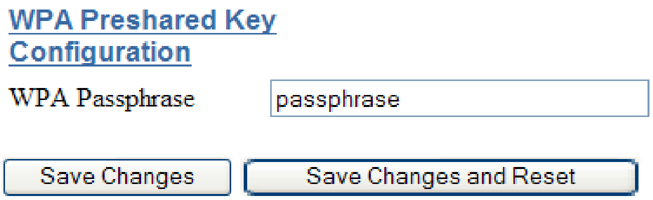
64bit WEP requires 10 Hexadecimal digits, and 128bit WEP requires 26 Hexadecimal digits. For example, 12:AB:EF:00:56. for 64bit encryption, and 12:AB:EF:00:56:15:6B:E4:30:C8:05:F0:8D for 128bit encryption
Encryption keys must not be all zeros, i.e. 00:00:00:00:00

WEP Open Authentication Mode
- Station sends an authentication request to the Access Point
- Access Point then authenticates the Station
- Station then associates with the Access Point and joins the network.

WEP Shares Authentication Mode
- Station sends an authentication request to the Access Point
- Access Point then sends a text based message to the Station
- Station uses its own WEP key to encrypt the text based message and sends it back to the Access Point.
- Access Point then decrypts the message using its on WEP key and if it matches authenticates the Station.
- Station then associates with the Access Point and joins the network.

When WPA Encryption is selected, 128bit Encryption keys are internally generated based on the Passphrase and System Address (ESSID). The Passphrase must be between 8 and 63 characters in length, and the Passphrase must be the same for all XYR401-E units in the same system.

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


WPA Preshared Key Configuration

WPA Passphrase: passphrase

WPA Enterprise - Supplicant Configuration

Username / Password:
user credentials that match a valid user on the RADIUS server.

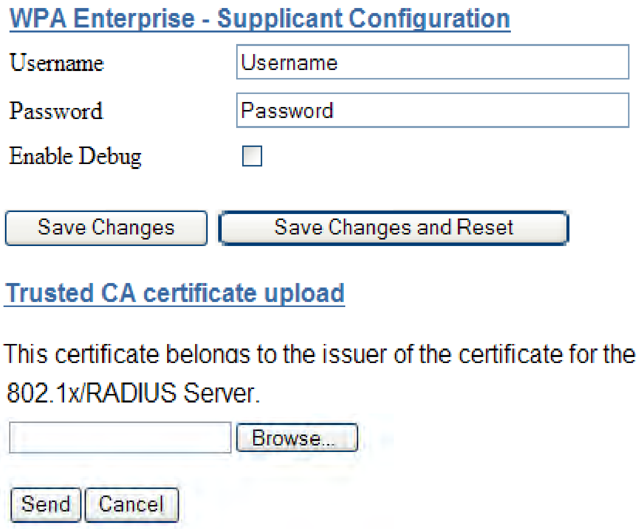
Enable Debug:
Must only be used during commissioning and only if requested by HONEYWELL Support. This must be disabled for normal operation.

Trusted CA certificate upload
Upload the certificate of the issuer of the RADIUS server’s certificate. This enables the Supplicant to verify the identity of the RADIUS server during the authentication process.
Supported EAP method - PEAP / MSCHAPv2

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

Trusted CA Certificate Contents:

Displays the contents of the loaded certificate.


WPA Enterprise - Supplicant Configuration

Username: Username

Password: Password

Enable Debug: □

Trusted CA certificate upload

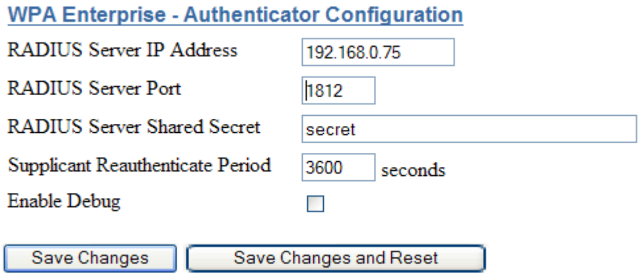
This certificate belongs to the issuer of the certificate for the 802.1x/RADIUS Server.

WPA Enterprise - Authenticator Configuration

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

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

Enable Debug:
Must only be used during commissioning and only if requested by HONEYWELL Support. This must be disabled for normal operation.


WPA Enterprise - Authenticator Configuration

RADIUS Server IP Address: 192.168.0.75

RADIUS Server Port: 1812

RADIUS Server Shared Secret: secret

Supplicant Reauthenticate Period: 3600 seconds

Enable Debug: □

3.8 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.

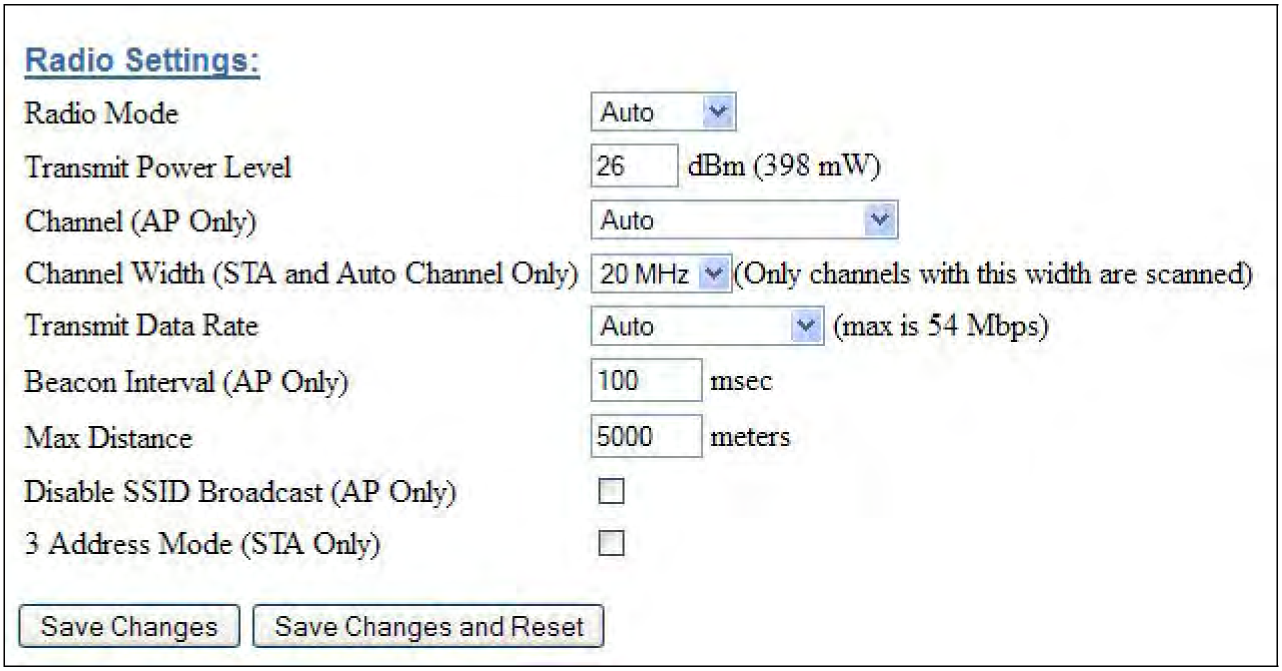
Transparent Bridge Operation
A bridge connects several Ethernet networks together, and makes them appear as a single Ethernet network to higher protocol layers.
By default, the XYR401-E is configured as a transparent bridge. When a transparent bridge is started, it learns the location of other devices 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 XYR401-E can be unnecessarily overburdened. Use filtering to reduce broadcast traffic sent over the radio. Refer Section 3.19 “Filtering” for how to configure a filter.

By default, a transparent bridge does not handle loops within the network. There must be a single path to each device on the network. Loops in the network will cause the same data to be continually passed around that loop. Redundant wireless links may be set up by enabling the bridge Spanning Tree Protocol (see section **Error! Reference source not found.** “**Error! Reference source not found.**” for more details).

Router Operation
A router joins separate IP sub-networks together. The router has different IP addresses on its wired and wireless ports, reflecting the different IP addresses of the separate Ethernet networks. All of the devices in these separate networks identify the router by IP address as their gateway to the other network. When devices on one network wish to communicate with devices on the other network, they direct their packets 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. For details on configuring routing rules, see section 3.18 “Routing”.

3.9 Radio Configuration



Radio Settings:

Radio Mode: Auto

Transmit Power Level: 26 dBm (398 mW)

Channel (AP Only): Auto

Channel Width (STA and Auto Channel Only): 20 MHz (Only channels with this width are scanned)

Transmit Data Rate: Auto (max is 54 Mbps)

Beacon Interval (AP Only): 100 msec

Max Distance: 5000 meters

Disable SSID Broadcast (AP Only) □

3 Address Mode (STA Only) □

The XYR401-E can be configured for different radio transmission rates. A reduction in rate increases the reliable range (transmission distance). The factory-default data rate settings are suitable for the majority of applications and should only be modified by experienced users.

Note: This rate is for Transmit messages only as radio can receive on all data rates.

The XYR401-E allows for a configurable *fixed* rate or an *Auto* radio transmission rate. When a fixed rate is configured the radio transmission rate is never altered, even under extremely poor conditions. The Auto rate will automatically change the radio data rate to give the best throughput. When a radio transmission is unsuccessful the XYR401-E will automatically drop to the next lowest data rate and if subsequent transmissions are successful at the lower rate, the XYR401-E will attempt to increase to the next highest rate. When a station connects to an access point the two devices negotiate a data rate based which is within configured range of radio data rates for both devices.

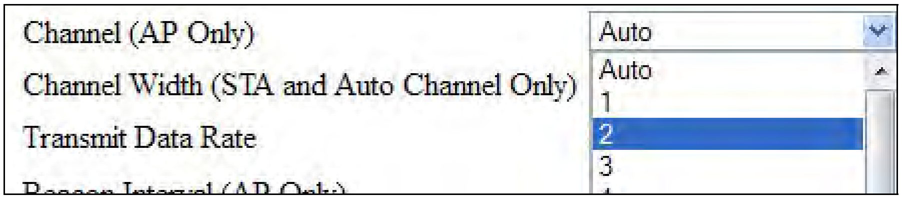
Select the “Radio” Menu to change the following configuration parameters. If a change is made, you need to select “Save Changes” to retain the changes. Changes will not take effect until the unit is reset.

Radio Mode	XYR401-E support 802.11b and 802.11g radio standards and to limit operation to one or the other, select the desired standard. Normally selecting “auto” allows the modem to make the best choice.
Transmit Power Level	This allows adjustment of the radio power. Do not set the radio power above the allowed setting for your country You can reduce the power for short range applications, or to allow the use of high gain transmitter antennas while still complying with the emission requirements of your country. See “Appendix D” for dBm to mW conversion
Channel (AP only)	XYR401-E Radio Channels 1 to 13 may be configured at the Access Point. Refer Section 3.1. XYR401-E Radio channels can be individually set (AP only – Client ignores the selection) or left in Auto (default) and then select the appropriate U-NII groups 1,2,3,4 each one having its own group of channels, Maximum Power and DFS selection. The default radio channel for both A & G modelsis Auto, meaning on startup it will scan all available and selected channel groups (Country dependent) and pick the quietest channel.

Channel Width (STA and Auto Channel Only)	XYR401-E Stations. When configured as a Station the module will periodically scan the channels looking for an Access Point. This option is used to speed up the Access Point scanning process of the Client radio by only scanning certain channel bands (5M, 10M, and 20M) or automatically scan all channels. Default is auto.
Turbo Mode **(Only for fixed Channels – No Auto)**	Selecting Turbo Mode doubles the transmit data rate offered on a Single channel. Maximum data rate up to 108Mbps. Only usable with other HONEYWELL XYR401-E module configured with the same Turbo Channel. If using the Turbo Mode feature all modem in the system will need to be configured with Turbo mode and the correct channel to communicate.
Transmit Data Rate	The radio baud rate in Mega (million) bits per second (Mbps) for point to point radio transmissions. The default value is Auto. Select a *fixed* rate to force the radio to use the selected rate. **Note: Increasing the Transmit Data rate will decrease the Transmit power level. E.g. selecting 54 Mbps fixed data rate will reduce the transmit power from 400mW down to 125mW. This is to comply with 802.11 regulations.**
Beacon Interval (AP only)	This interval is the period between beacon transmissions sent by an Access Point. The default value is 100 milliseconds, and it may be adjusted from 50 to 4095 milliseconds.
Disable SSID broadcast. (AP only)	This should be used to prevent unwanted eavesdroppers from detecting the radio network System Address (SSID) by passively listening to beacon transmissions from the Access Point. When disabled, Access Points will not transmit the System Address openly in Beacon messages. This is particularly useful in unencrypted radio networks.
3 Address Mode	Allows compatibility with Layer 3 Bridge devices. See section 3.6 ―Compatibility"
Max Distance	Configure the maximum distance the radio signal is expected to travel. This allows the modem to compensate for the flight time of messages as they pass from the transmitter to the receiver, and as the acknowledgement messages are returned. Setting this value larger will cause a small reduction in throughput. Setting this value too small will cause communications problems over longer distances. Default distance is 5km
Save Changes	Save changes to non-volatile memory. Changes will not take effect until module is reset.
Save Changes and Reset	Save changes to non-volatile memory and reset module

Channel Selection

XYR401-E modem (2.4 GHz 802.11b/g) selection is done by picking one of the channels from the drop down ―Channel" list. Normal 20MHz, 5 MHz, 10 MHz or Turbo channels are available depending on country or you can leave it in Auto and let the modem select the best channel.



Channel (AP Only) Auto

Channel Width (STA and Auto Channel Only)

Transmit Data Rate

Radio Throughput

Below is a table showing the maximum data throughput based on channel selection and receiver signal level. Throughput is based on TCP/IP and there are three channel Bandwidths 20M, 10M, & 5M. These throughput estimations are based on perfect radio conditions, i.e. little to no outside radio interference present while data is being passed.

XYR401-E Radio Data Throughput			
2400Mhz	Data Rate in Mbps		
Signal Strength	20MHz	10MHz	5MHz
-74dBm	22	11	5.5
-77dBm	20	10	5
-83dBm	17	8.5	4.3
-86dBm	11	5.5	2.8
-90dBm	9	4.5	2.3
-91dBm	6	3	1.5
-93dBm	4.5	2.3	1.1
-94dBm	3	1.5	0.75

Throughput and Repeaters

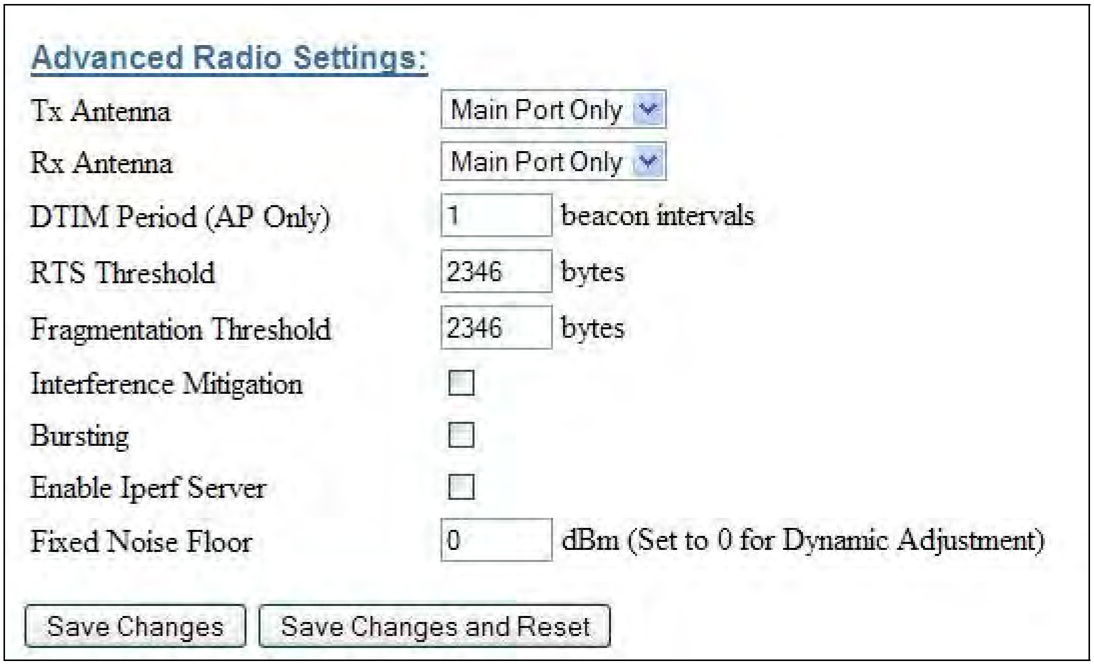
It should also be noted that if using repeaters to extend the range there will be a reduction in throughput for each repeater hop.

The following table shows the drop in throughput for each hop and for each of the channel widths.

Data Throughput based on Repeater Hops												
Rep Hops	1	2	3	4	1	2	3	4	1	2	3	4
Signal	20 MHz Channel				10 MHz Channel				5MHz Channel			
-74dBm	22	11.0	5.5	2.8	11.0	5.5	2.8	1.4	5.5	2.8	1.4	0.7
-77dBm	20	10.0	5.0	2.5	10.0	5.0	2.5	1.3	5.0	2.5	1.3	0.6
-83dBm	17	8.5	4.3	2.1	8.5	4.3	2.1	1.1	4.3	2.1	1.1	0.5
-86dBm	11	5.5	2.8	1.4	5.5	2.8	1.4	0.7	2.8	1.4	0.7	0.3
-90dBm	9	4.5	2.3	1.1	4.5	2.3	1.1	0.6	2.3	1.1	0.6	0.3
-91dBm	6	3.0	1.5	0.8	3.0	1.5	0.8	0.4	1.5	0.8	0.4	0.2
-93dBm	4.5	2.3	1.1	0.6	2.3	1.1	0.6	0.3	1.1	0.6	0.3	0.1
-94dBm	3	1.5	0.8	0.4	1.5	0.8	0.4	0.2	0.8	0.4	0.2	0.1

3.10 Advanced Radio Configuration

Some of the more advanced radio settings have been moved from the normal Radio configuration page so as to simplify the configuration process.
Care should be taken when making changes to parameters on this page.



Advanced Radio Settings:

Tx Antenna	Main Port Only
Rx Antenna	Main Port Only
DTIM Period (AP Only)	1 beacon intervals
RTS Threshold	2346 bytes
Fragmentation Threshold	2346 bytes
Interference Mitigation	□
Bursting	□
Enable Iperf Server	□
Fixed Noise Floor	0 dBm (Set to 0 for Dynamic Adjustment)

TX Antenna	Select which antenna port the module will transmit from. Selections available are Main Port Only – Messages are transmitted from the main ―TX/RX" port, The Auxiliary port ―RX" is disabled. Both (Diversity) – Both ports will be used to transmit however not at the same time; it calculates the best port based on previous transmissions and MAC addressing. Note: Broadcast / UDP transmission messages will initially toggle between the antenna ports, and could result in every second message not being heard until the module learns which device can be reached through which antenna port. Aux Port Only – Messages will be transmitted via the Auxiliary ―RX" port only
RX Antenna	Same as for TX Antenna above but for the Receiver port. Setting to ―Both (Diversity)" will allow a high gain antenna to be connected to the Auxiliary ―RX" port which will give better RX signal gain but not increase the TX gain and possibly pushing it over the regulatory EIRP threshold.
DTIM Period (AP only)	DTIM sets which beacon frames incorporate extra information for low power sleeping client devices. Normally set this to 1.
RTS Threshold **"Ready To Send"**	RTS frames can be used to help avoid radio collisions between two stations that cannot directly hear each other. Any frame larger than RTS Threshold bytes will be preceded by an RTS message. The default value of RTS Threshold is 2346, which effectively disables RTS signalling, as this value is larger than the maximum frame size (Fragmentation Threshold).
Fragmentation Threshold	(Client Stations only). The maximum transmission unit (MTU) of data over the radio. If more than this number of bytes is input into the module, it will be transmitted in more than one message (or fragmented).

Interference Mitigation (AP only)	Interference Mitigation should only be turn on (Default is Off) if using Demo Whip antenna's or if there is a high level of background interference. By enabling this option the radio will dynamically adjust radio parameters to help mitigate interference based on any background interference. It will reduce the receiver sensitivity and so should only be enabled on paths with a high fade Margin and good signal quality, etc.
Bursting	Selecting this option can increase the data throughput by reducing the overheads associated with wireless transmissions. If communicating with a device that does not support bursting the modem will drop back to non-bursting mode.
Passive Scanning (STA only)	Selecting this item stops a Client device from sending "probe request" messages when it is searching for an access point to connect to. Instead, the client waits for a beacon transmission from the access point.
Background Scanning (STA only)	Enabling this option will allow a modem to periodically rescan for Access Points so keep the connectivity page up to date with current system information. Default is off.
TX Antenna	Select which antenna port the module will transmit from. Selections are Main Port Only, Both (Diversity) or Auxiliary Port Only. Module does not transmit from both ports at the same time. If needed, i.e. broadcast messages the radio will toggle transmissions between the antenna ports.
RX Antenna	Same as for TX antenna above but for the Receiver
Enable Iperf Server	Enable Iperf Server function in the modem. Iperf is used for performing Radio surveys or radio path testing. See section **Error! Reference source not found.** "TCP Throughput Test"
Fixed Noise Floor	Allows the Radio Receiver sensitivity Noise Floor to be moved above any interference. What this will do is essentially stop the radio communicating with devices with lower signal strength. For use in areas where there is a greater amount of interference

Fixed Noise Floor

Due to the popularity of the 2.4 GHz band, there are many sources of interference. This interference can sometimes be a problem due to the way 802.11 devices communicate. Standard 802.11 communications uses a system called ―Clear Channel Assessment ‖ which means the radio will listen before transmission and if the channel is busy it will hold off regardless of the level of signal.

If the background interference is high due to other radio systems or noise you can raise the Fixed Noise floor to compensate. The Channel Utilisation page can be used to identify excess noise / interference.

Raising the Noise Floor will block out any receive signal levels below the value configured under ―Fixed Noise Floor ―on the Advanced Radio Configuration page. The value must be entered as a negative dBm number and should be at least 8dB greater than the weakest RSSI of any connected modems, otherwise communications may be lost.

E.g if the interfering noise levels are around -80 dB you can raise the Noise floor to -70dB to block out any signals below making sure the RSSI levels of any connected modules are not below this Noise Floor as they will not communicate.

The Connectivity page can be used to determine what other systems are around and what their RSSI levels are.

After configuring the fixed noise floor, confirm that the Channel Utilisation has dropped to a desirable level, and where possible perform an iperf Throughput Test to confirm acceptable performance.

3.11 Serial Port Configuration

The XYR401-E has an RS-232, and an RS-485 port for serial communications. These ports may be used for different purposes. The XYR401-E offers three different serial functions, which are PPP server; Serial Gateway; and Modbus TCP to RTU Gateway.

RS-232 PPP Server

The XYR401-E can be used as a PPP (Point-to-Point Protocol) Server to connect the wireless system to serial devices via the RS232 or RS485 serial ports.

PPP Server enables a network connection to the XYR401-E over a serial cable. This is much like dial up internet. The maximum serial data rate is 115,200bps. 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 XYR401-E, users must configure the local IP address for the XYR401-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 XYR401-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.

To configure Windows XP to establish a PPP connection to a XYR401-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 Connection Name
7. Select a COM port
8. Select availability
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 115200bps, 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 XYR401-E.
17. Ensure both the username and the password are entered exactly as configured in XYR401-E. (When booted in SETUP mode, the PPP server has username "user" and password "user".)

Serial Gateway (Server/Client/Multicast)

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.

The Serial Gateway can be configured as either as Server, Client, Multicast Group, or Modbus.

When configured as "Server", the module will wait for a TCP connection to be initiated by a remote client.

When configured as "Client", the module will automatically attempt to connect to a specified remote server using TCP.

When configured as "Multicast Group", the module will broadcast data to all members of the same Multicast Group using UDP. With the Serial Gateway Server, Client and Multicast functions it is possible for serial data from a XYR401-E to be transferred to any other XYR401-E serial ports including the corresponding port on the same XYR401-E.

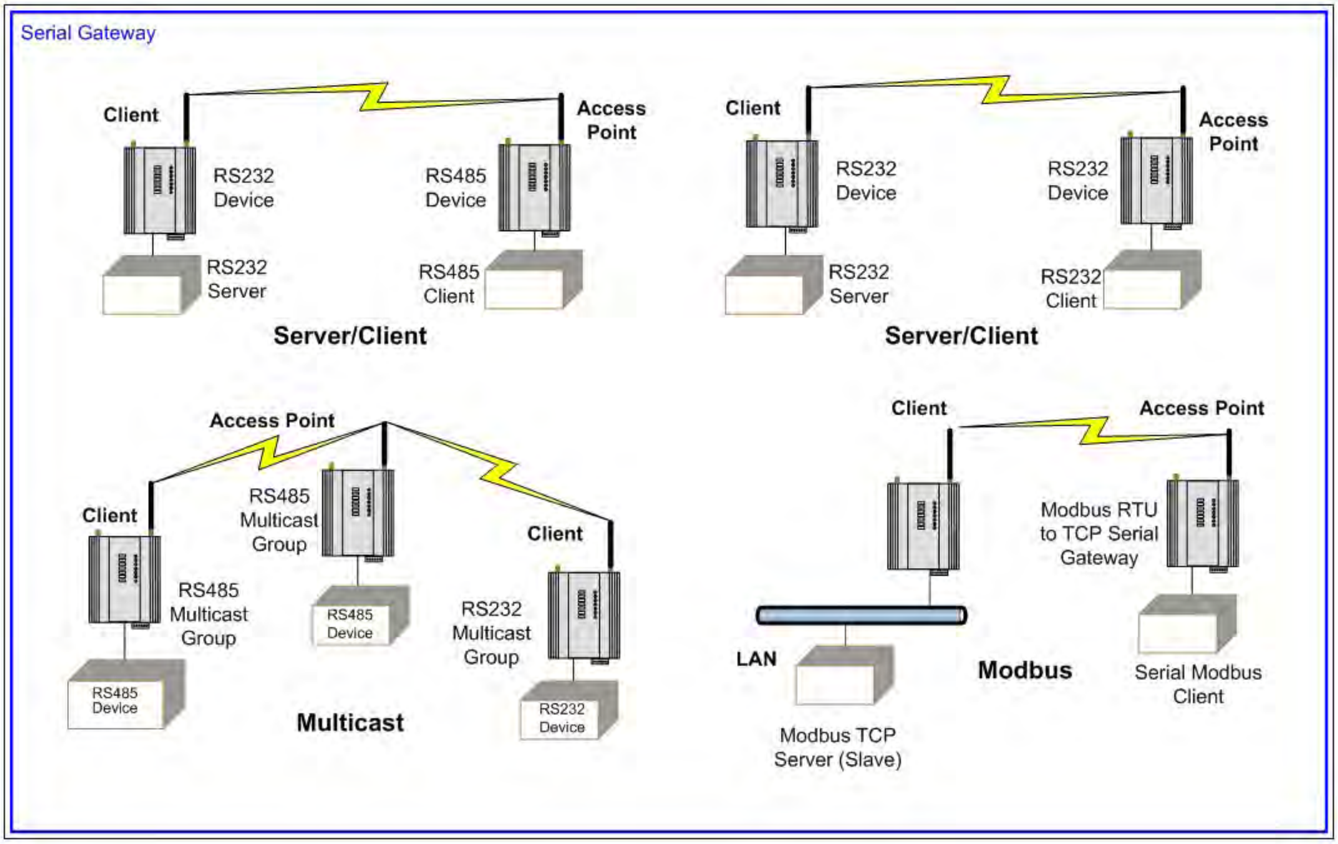
Serial Gateway (Modbus - Modbus RTU to TCP)

When configured as "Modbus", will allow a serial Modbus Client (Master) to connect with a single Ethernet Modbus TCP Server (Slave). With the Modbus Function the serial data is encapsulated within a TCP/IP data frame and made available on the Ethernet network.

Both XYR401-E serial ports and the hard wired Ethernet port can be configured to communicate completely separate data streams which can all be communicating at the same time.

Some of the possible Serial Gateway topologies are illustrated below.

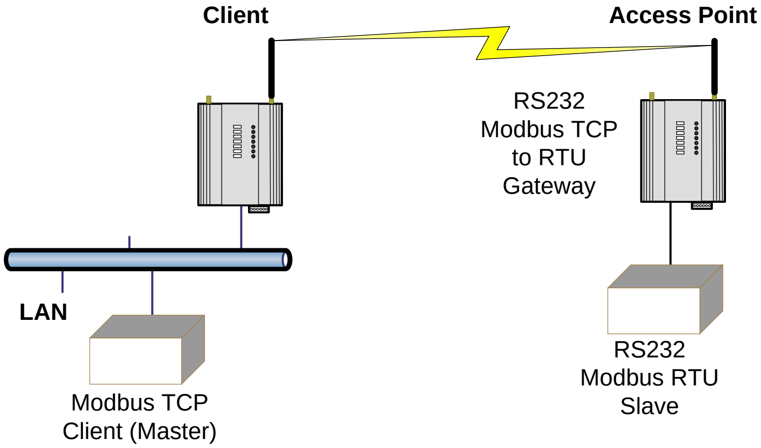
Care should be taken when making changes to parameters on this page.



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 XYR401-E serial port. Standard programs can then be used to access this serial port as if it were actually connected to the PC. Alternatively Hyperterminal may be used to connect to a serial port on the XYR401-E. When creating the Hyperterminal connection, select "Connect Using: TCP IP (Winsock)", enter the IP address of the XYR401-E, and the port selected in the "Network port" field.

Modbus TCP to RTU Gateway

The Modbus TCP to RTU Gateway allows an Ethernet Modbus/TCP Client (Master) to communicate with a serial Modbus RTU Slave. The XYR401-E makes this possible by internally performing the necessary protocol conversion. The conversion is always performed by the XYR401-E which is directly connected to the Modbus serial device (i.e. only this module needs to have Modbus TCP to RTU Gateway 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 XYR401-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 XYR401-E within the configured Response Timeout, the XYR401-E will initiate a number of retries specified by the configured Maximum Request Retries.
The Modbus TCP to RTU Gateway may be configured to operate on either the RS-232 or RS-485 port.

3.12 Serial Menu

RS232 / RS485 Serial Port Configuration

RS232 Port	Select the desired functionality. Select either PPP, Serial Gateway or Modbus TCP to RTU
Data Rate	The serial data rate desired. Serial data rates available range from 110bps to a maximum of 115,200bps.
Data Format	The data format desired. All the standard data formats are supported.
Flow Control	Selects CTS/RTS or None

RS232 PPP Server (Only RS232)

Username	User name to enter to access RS-232 PPP Server.
Password	Password to access RS-232 PPP Server.
Local IP Address	Select the IP address of the PPP server. The remote device may be made visible on the Ethernet or Wireless networks by either utilising proxy-arp or routing. The proxy-arp feature may be enabled by setting the Local IP address the same as the Ethernet IP Address or the Wireless IP Address. The module will respond on behalf of the remote device, making it seem like the device is present on the configured network. Alternatively, if the IP address selected is not the same as the Ethernet or Wireless IP address, routing is used to pass data to the Ethernet and Wireless ports.
Remote Device IP Address	Select the IP address of the remote device. Ensure this address is not the same as any other device on the Ethernet or Wireless networks.

RS232 / RS485 Serial Gateway

Serial Gateway Mode	**Server - Module will wait for a connection to be initiated by a remote Client.**
Character Timeout	Enter the maximum delay (in msec) between received serial characters before packet is sent via network.
Packet Size	The number of received bytes that will be buffered before a packet is sent via the network.
Listen Port (Server)	Server Only. Enter the TCP port number on which the server must listen for incoming connections. The standard TELNET port is 23.
Serial Gateway Mode	**Client** only. Module will automatically attempt to connect to the specified remote server.
Character Timeout	Enter the maximum delay (in msec) between received serial characters before packet is sent via network.
Packet Size	The number of received bytes that will be buffered before a packet is sent via the network.
Remote Device Port (Client)	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.
Serial Gateway Mode	Multicast - Allows point to multi-point serial transfer. All members of the group will receive serial transmissions made by any other member of the Multicast group.
Character Timeout	Enter the maximum delay (in msec) between received serial characters before packet is sent via network.
Packet Size	The number of received bytes that will be buffered before a packet is sent via the network.
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 Address	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.
Serial Gateway Mode	Modbus - Allows a serial Modbus Client (Master) to connect with a single Ethernet Modbus TCP Server (Slave)
Character Timeout	Enter the maximum delay (in msec) between received serial characters before packet is sent via network.
Packet Size	The number of received bytes that will be buffered before a packet is sent via the network.
Modbus Server Port	Enter the TCP port number of the remote server (i.e. the remote port to automatically connect to).
Modbus Server IP Address	Enter the IP Address of the remote server (i.e. the remote IP Address to automatically connect to).

RS232 / RS485 Modbus TCP / RTU Converter

Modbus Server TCP Port	Port number used for the Modbus TCP – Standard port is 502.
Pauses 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.

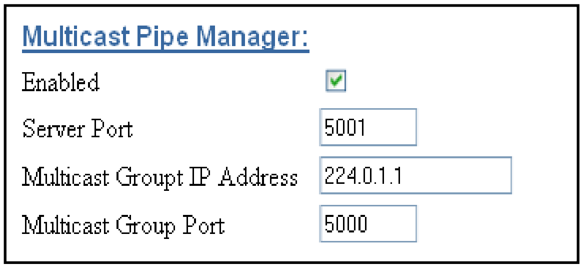
3.13 Multicast Pipe Manager

Previously it has been difficult to connect a single TCP device, i.e. a Scada / DCS system to multiple remote multicast serial devices.

Multicast Pipe allows this type of connection.

An example would be a Scada system that needs to communicate with multiple remote serial devices. A modem can be placed at each remote location and connected serially to each device. A multicast pipe is configured to communicate with all devices using a multicast address and port, i.e. 224.0.1.1:5000.

The Scada then communicates with the remotes via the IP address of the Multicast Manager and the port selected in the configuration, i.e. 5001.



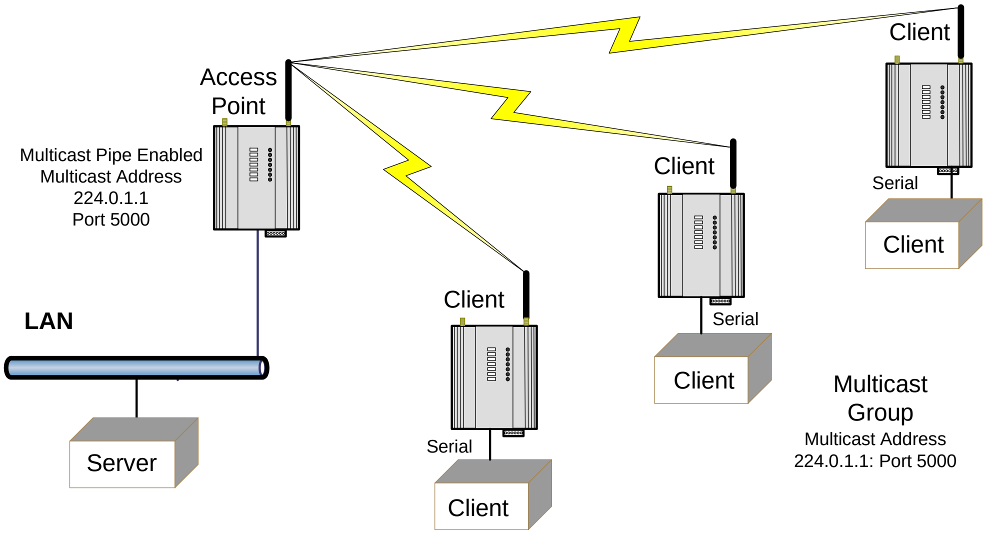
Multicast Pipe Manager:

Enabled ☑

Server Port 5001

Multicast Groupt IP Address 224.0.1.1

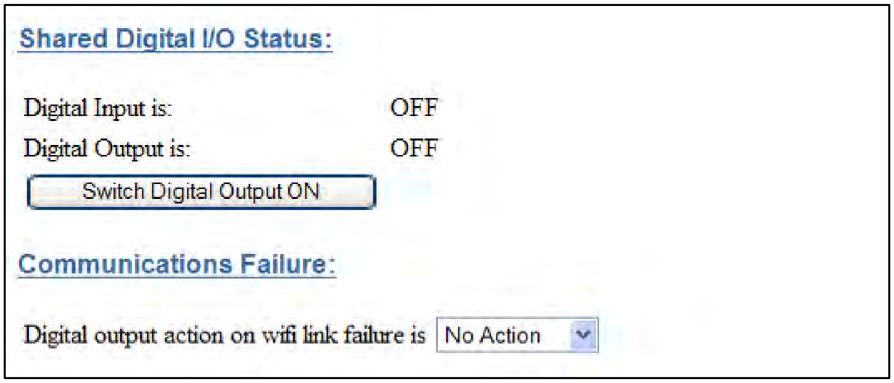
Multicast Group Port 5000



Multicast Pipe Manager	
Enabled	Enables or disables the Multicast Pipe manager.
Server Port	Server port used by the Multicast Pipe Manager. Will need to be configured the same as the Port on the Client, i.e. Scada, DCS, etc
Multicast Group IP Address	Broadcast Address used when communicating to all other Multicast devices. This address will need to be
Multicast Group Port	Multicast Port used when communicating to all other Multicast devices. Will need to be the same on all

3.14 Digital Input/Output

The functionality of the shared Digital Input/Output pin may be configured via the "I/O Transfer" webpage. As this pin is shared, the Digital Input status will be ON when the Digital Output is set ON.



Shared Digital I/O Status:

Digital Input is: OFF

Digital Output is: OFF

Communications Failure:

Digital output action on wifi link failure is No Action

The Digital I/O channel can be transferred to/from another device using Modbus (see section "**Error! Reference source not found.** Modbus I/O Transfer") or it can be configured to provide status of the module communications. If the XYR401-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).

3.15 Modbus I/O Transfer

The XYR401-E 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 XYR401-E can transfer I/O to/from almost any combination of Modbus TCP or RTU devices.

The layout of the XYR401-E I/O Registers is summarized in the table below. Each register is internally saved as a 16 bit unsigned integer value. A Modbus transaction may access the entire 16 bit value of any register, or alternatively the most significant bit of a register may be accessed as a discrete value. The main use for the general purpose I/O registers is for intermediate storage, i.e. when transferring I/O from one Modbus Slave device to another. Also provided is the status of the onboard digital I/O, as well as the status of the wireless link. The 16 bit status register contains 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.

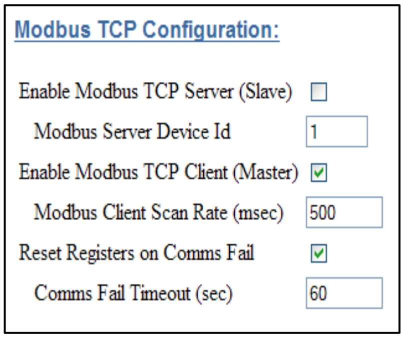
Registers	Purpose
1 – 4299	General purpose I/O registers (read/write)
4300	On-board Digital Input value (read only)
4301	Link Status (read only)
4320	On-board Digital Output value (read/write)
4370	On-board Digital Input inverted value (read only)
4371	Link Status inverted (read only)
4372-4999	Reserved for future use

Modbus TCP Client (Master) enables the XYR401-E to connect to one or more Modbus TCP Servers (Slaves).
All Modbus Master messages are directed 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 XYR401-E serial port by enabling the Modbus TCP to RTU gateway at the corresponding serial port (see section 3.11 “Serial Port Configuration”).

Modbus TCP Client functionality allows connections to a maximum of 100 mappings to be configured and a maximum of 25 different Modbus TCP Servers.

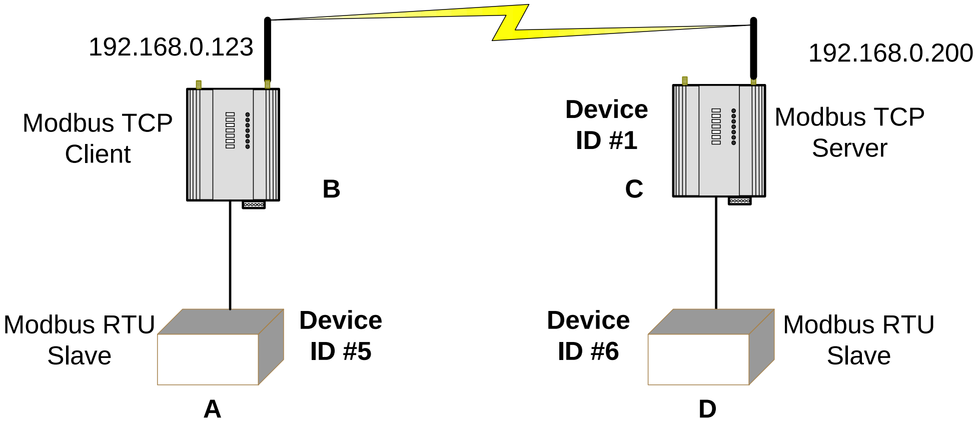
Modbus TCP Server (Slave) enables the XYR401-E to accept connections from one or more Modbus TCP Clients (Masters).

All Modbus transactions routed to the onboard Modbus TCP Server are directed to/from the onboard general purpose I/O registers. The Modbus TCP Server is shared with the Modbus TCP to RTU 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 TCP Configuration:

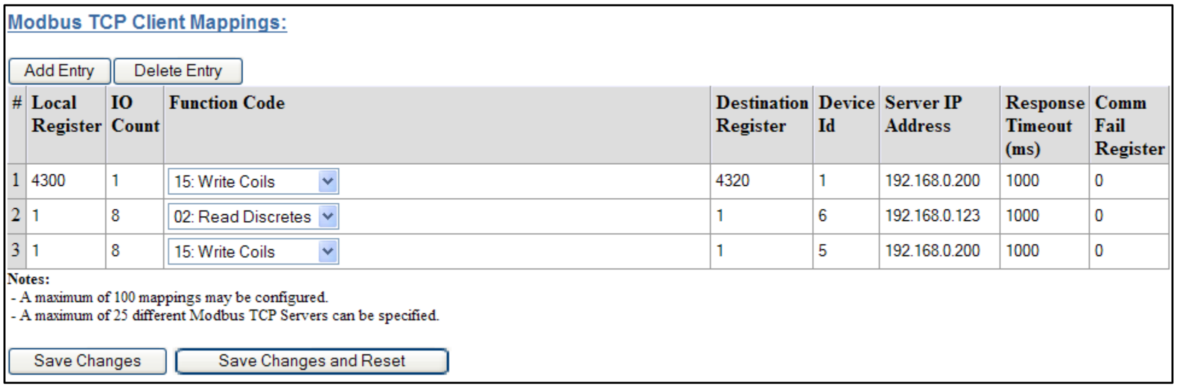
Enable Modbus TCP Server (Slave) □
Modbus Server Device Id 1
Enable Modbus TCP Client (Master) ☑
Modbus Client Scan Rate (msec) 500
Reset Registers on Comms Fail ☑
Comms Fail Timeout (sec) 60

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 XYR401-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 XYR401-E that the serial device is connected to.



The XYR401-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 XYR401-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 single bit registers from Modbus serial device D will be transferred to A.



Modbus TCP Client Mappings:

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

Notes:
- A maximum of 100 mappings may be configured.
- A maximum of 25 different Modbus TCP Servers can be specified.

Unit B is configured with Modbus TCP Server enabled and Device ID = 1, Unit C is configured as shown above.

- The first will write the register 4300 (Local Digital Input) to server IP address 192.168.0.200 (Unit B), Device ID #1, register 4320 (Local Digital output).
- The second mapping shows a Modbus read command of 8 Discretes starting at register 1 (Destination Reg) on Device ID #6 connected to IP address 192.168.0.123 (it self) and store the values at register #1 locally.
- The third mapping shows the Modbus write command (Write Coils) which is writing the local 8 I/O’s starting at register 1 across to Server IP address 192.168.0.200, Device ID #5, destination reg #1.

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 Modbus TCP to RTU Gateway” on page 50) 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 XYR401-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.

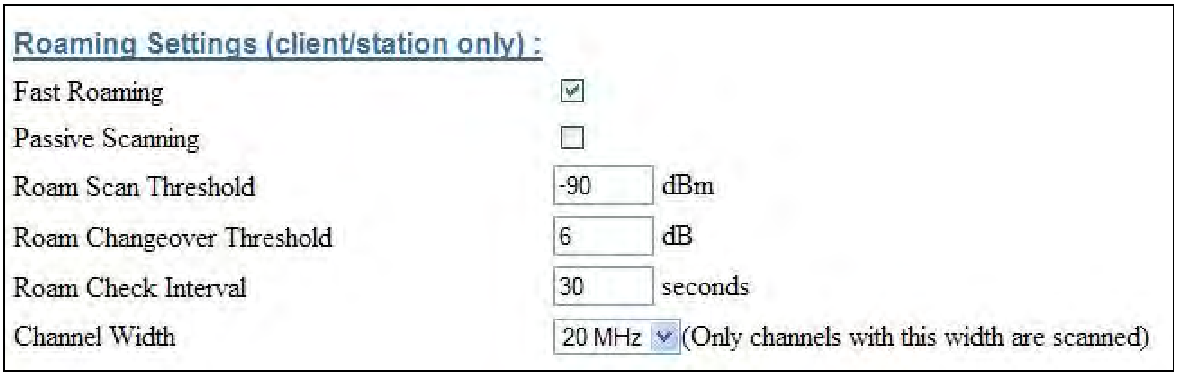
Modbus TCP Configuration on I/O Transfer Menu:

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.
Enable Modbus Statistics	Enables the Modbus Diagnostic registers as shown in Section 34.6 “Internal Diagnostic Modbus Registers” Disabling this option will free up the registers and also slightly increase processing resources.
Log background Noise	RSSI & BGND on Rx messages are made available in the diagnostic registers (See 4.4 “Internal Diagnostic Modbus Registers” for details. For a Hex value of 5F5D the 5D byte = RSSI and the 5F byte = BGND (Convert value from hex to dec and add a “-“e.g. 5F = -95dB). Enabling this option removes the RSSI byte from these registers and so only the Background Noise value is made available.

Modbus TCP Client Mappings on I/O Transfer Menu:

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

3.16 Roaming



Roaming Settings (client/station only) :

Fast Roaming ☑

Passive Scanning ☐

Roam Scan Threshold -90 dBm

Roam Changeover Threshold 6 dB

Roam Check Interval 30 seconds

Channel Width 20 MHz (Only channels with this width are scanned)

In certain cases a Client may be in a mobile situation and require a method of roaming to another Access Point.

Normal network communications provides only basic roaming behavior which means as the client moves further from the AP it will go through a period of poor communication followed by a complete disconnection of the radio link.

It is at this point that the Client will scan for Access Points and if one is in range it could take up to 10 seconds for the client to establish a connection.

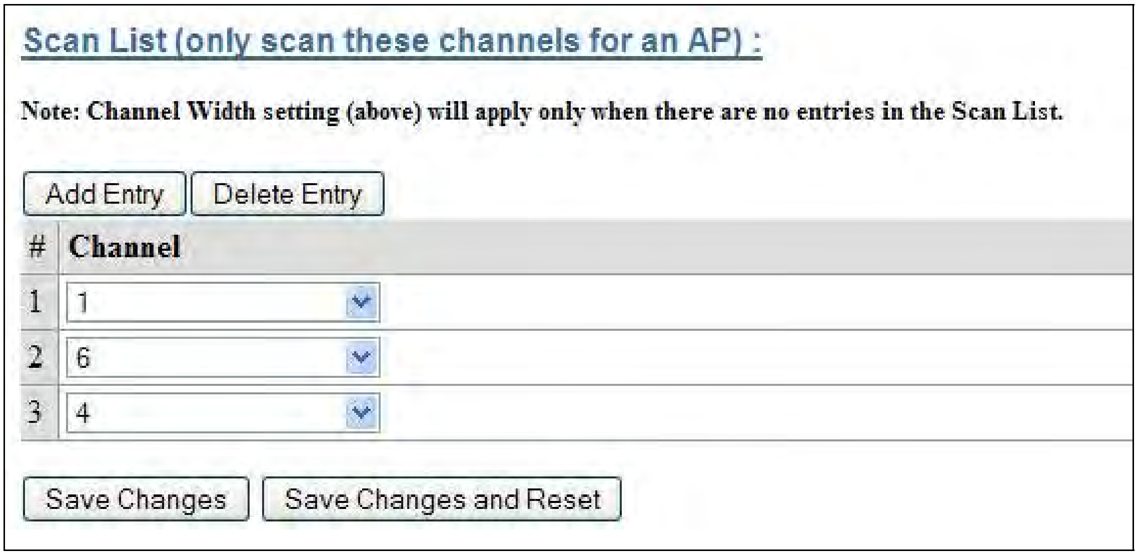
Fast Roaming will significantly reduce the time taken for a client to roam from Access Point to Access Point. Also the discovery of AP's is done before the existing radio link deteriorates therefore eliminating the periods of poor performance during transition to the next AP.

The following settings/thresholds can be configured to fine tune the fast roaming process.

Fast Roaming	Fast Roaming allows a client (station) to roam to an AP with a stronger signal strength without disrupting communications. Or roam seamlessly between multiple Access Points based on configuration parameters such as RSSI threshold.
Passive Scanning (STA only)	Selecting this item stops a Client device from sending ―probe request ‖ messages when it is searching for an access point to connect to. Instead, the client waits for a beacon transmission from the access point. Passive Scanning should be disabled when Fast Roaming is enabled.
Roam Scan Threshold	Background Scan will be initiated when the RSSI to the currently connected AP drops below this threshold and Fast Roaming (above) is enabled. Default is -90dBm
Roam changeover Threshold	This is the RSSI value above the Roam Scan Threshold that is required for the Client to change to the new Access Point. In the example shown above the Access Point RSSI would need to be above -84dB before it would changeover. In general, the Roam Changeover Threshold should be at least 6dB, otherwise changeovers could occur too frequently.
Roam check Interval	If a better AP is not found, the background scan is repeated every Roam Check Interval while the signal strength to the currently connected AP is below the Roam Scan Threshold. Default is 30seconds
Channel Width	Selects channel width bands for background scan. If 5MHz is selected then only 5MHz channels will be scanned during the background scan. Default is Auto, which means all channels will be scanned.
Save Changes	Save changes to non-volatile memory. Changes will not take effect until module is reset.
Save Changes and Reset	Save changes to non-volatile memory and reset module

When Fast Roaming is enabled the Client goes off-channel and periodically performs a background scan to identify available AP’s. When AP’s are identified the RSSI is recorded as a potential connection. It takes 50msec to scan each channel, with a 1 second delay between each scanned channel. So scanning 10 channels will take 10 second, during which time latency of up to 50msec will occur and any throughput traffic is essentially paused and buffered for retransmission when complete. It is therefore recommended the scan list is used to limit the number of channels the client needs to scan thus reducing the overall scan time.

During the background scan a client will scan all of the channels in the Scan List to identify better AP's. If no channels are configured it will scan all channels.



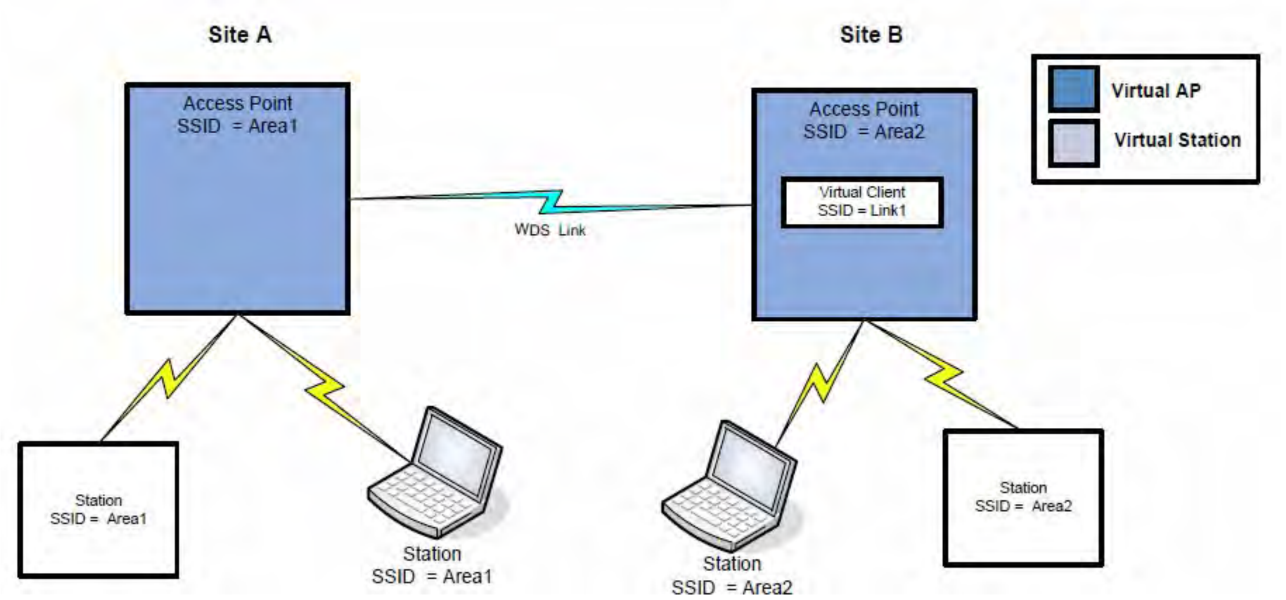
Scan List (only scan these channels for an AP) :

Note: Channel Width setting (above) will apply only when there are no entries in the Scan List.

#	Channel
1	1
2	6
3	4

The above configuration shows that the Client will start scanning when the RSSI of its current connection to the Access Point falls below -90dBm. When this happens it will scan the list of Access Points configured in the Roaming Scan List (in this case channels 1, 4 & 6, as shown below) and if any of the RSSI levels are greater than -84dBm it will change to this Access Point.

3.17 Repeaters (WDS)



The range of a wireless network can be extended by allowing Access Points to behave as repeaters and forward traffic to other Access Points. Access Point to Access Point communications is also known as Wireless Distribution System (WDS). The XYR401-E offers very powerful WDS configuration, allowing for a *mesh* network with self-healing functionality. Alternatively, fixed AP to AP links can be configured for optimized throughput.

Each XYR401-E Access Point supports up to 10 separate *interfaces* for WDS links to other devices.

Each WDS interface can be either a *bridge* or *router* interface (refer section 1.1 "Network Topology" for more information on bridge vs router). If you need a simple repeater network, use a bridge interface.

A WDS *bridge* interface allows traffic to be bridged to another Access Point on the same IP network. WDS bridge interfaces do not require additional IP Address configuration, as they are bridged with the standard *wireless interface* that is used for connections to associated clients. All of the WDS interfaces on the one Access Point may be bridged if required.

WDS bridge interfaces have the advantage that redundant paths are permitted when using the bridge Spanning Tree Protocol (see section **Error! Reference source not found.** "**Error! Reference source not found.**"), thus behaving as a self-healing mesh network. Bridged networks are also not as configuration intensive as routed networks. Since WDS bridge interfaces generally do not require IP address configuration (they inherit the IP address of the standard wireless interface).

A WDS *router* interface allows traffic to be routed to an Access Point on a different network, and therefore requires configuration of an IP address to reflect the network address of the destination network. WDS router interfaces cannot provide the redundancy of bridge interfaces, but can be used to reduce radio bandwidth requirements because the router can determine the destination based on IP address, whereas the bridge must go through a learning phase where all broadcast traffic must be retransmitted on each interface. Routed networks may also be used in some cases to avoid the overhead introduced by the bridge Spanning Tree Protocol when network loops exist.

Specify SSID for AP/STA modes or MAC Address for Point to point mode.

Encryption is not inherited from the main page.

Each WDS interface may also be configured with a different encryption algorithm; however each side of a single WDS link must specify the same encryption algorithm and keys.

Router IP and Subnet should be left blank unless that WDS interface is to be on a different subnet. Leaving these fields blank will mean that the WDS interface will be bridged with the default wireless interface.

When adding WDS router interfaces, you may also need to add a *Routing Rule* on the *Routing* configuration page.

Spanning Tree Protocol (STP) column only applies when two or more interfaces are bridged.

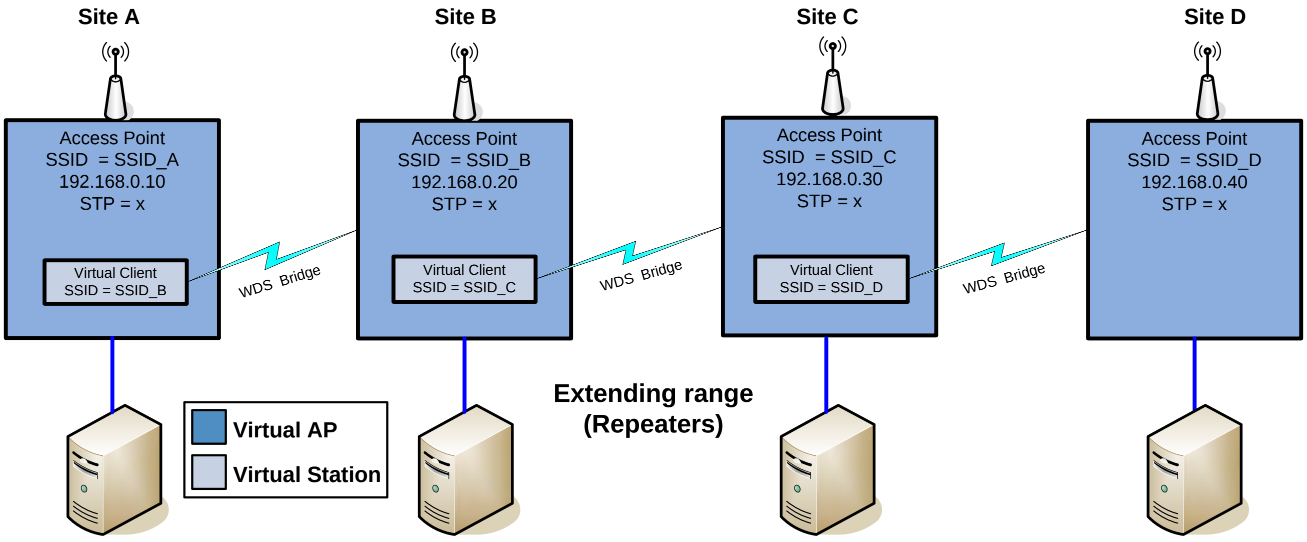
A maximum of 10 WDS Connections can be configured. (A combined maximum of 5 AP and STA virtual modules applies.)

WDS Connections are made by adding one or more "Virtual Modules" to an Access Point (as illustrated in the diagram at the start of the section). Each virtual module can be configured with one of the standard wifi operating modes (Access Point or Station) or a non-standard Point to Point mode.

- Access Point and Station virtual modules allow for the possibility of dynamically created connections (based on SSID) and support WPA Encryption. A combined maximum of 5 AP and STA virtual modules can be configured per unit.
- Point to point mode virtual modules provide static connections (based on MAC addresses), and cannot support WPA Encryption. Point to point virtual modules should only be used for establishing WDS connections with third party Access Points that do not support standard WDS operation.

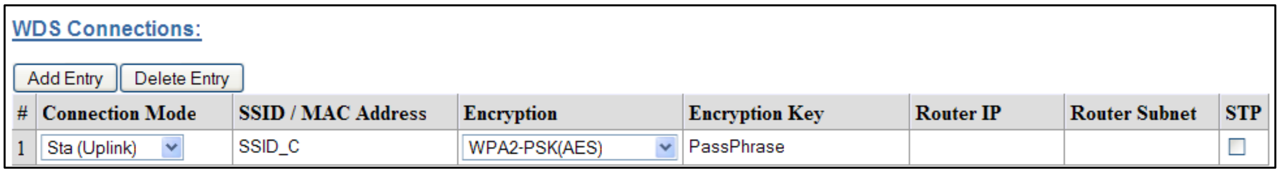
All Access Points must be configured on the same fixed radio channel. Auto Channel selection must not be selected (See "Radio" page for details on configuring the channel.)

There are many different ways to setup wireless networks; often it depends on the devices you wish to connect and the existing network topology.
The following pages show some examples of how to connect devices into different types of systems.



Example – Extending range using WDS

One of the most common uses for WDS is to extend the range of the wireless network using repeaters. The diagram above illustrates a simple example where the four Access Points are all at fixed locations (each of the Access Points could, of course, have one or more client/stations connected). Since the locations are fixed, we can avoid the overhead of using the Bridge Spanning Tree protocol here by configuring fixed WDS links to ensure that each Access Point will only connect to the next Access Point in the chain. Any number of additional intermediate repeaters could be added to the chain in a similar way.

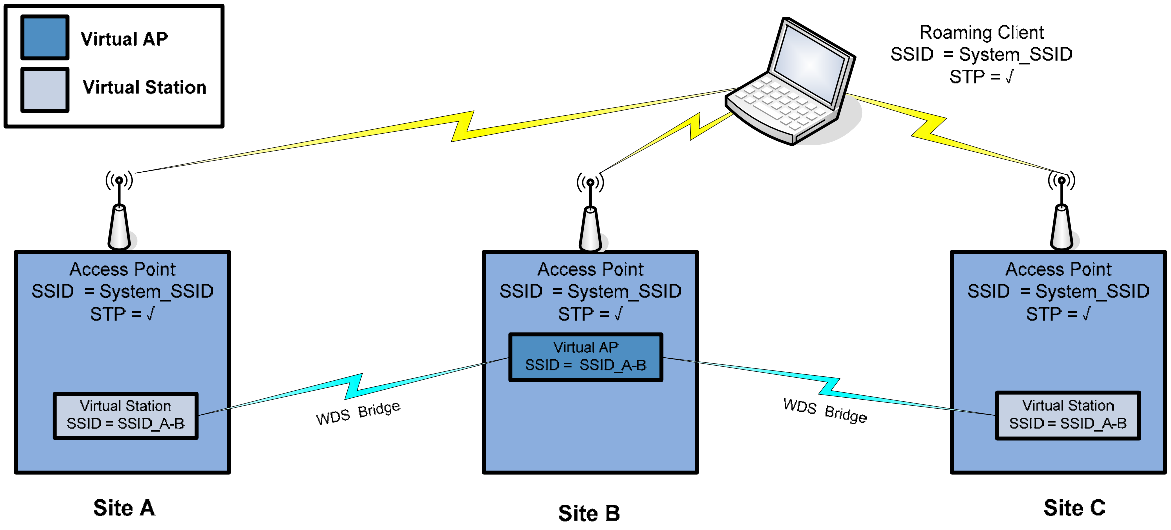


#	Connection Mode	SSID / MAC Address	Encryption	Encryption Key	Router IP	Router Subnet	STP
1	Sta (Uplink)	SSID_C	WPA2-PSK(AES)	PassPhrase			□

Site B WDS Configuration 1

The WDS configuration for unit B is shown above (this page is accessible via the *Repeaters* link from the configuration web pages). Site B is acting as an Access point for Site A, and is a client to Site C, likewise Site C is acting as an Access Point for Site B, and a Client for Site D. Since this example is a bridged network i.e. all devices on the same IP network and each link is using a different SSID, there is no possibility of loops (i.e. multiple paths to the same location) therefore we do not need to incur the overhead of enabling STP (bridge spanning tree protocol).
We specify the devices at the other end of the WDS links by SSID only –MAC addresses can be used to specify point-to-point links to third party devices which do not support meshing via SSID.
In this example each Virtual connection is using the same Encryption method (WPA-PSK (AES) with a key of “Pass Phrase”, however as in example #1 the Encryption method and key can be different for each virtual link or even disabled (no encryption). Also the Spanning Tree Protocol is disabled as there is no possibility of network loops.

Example - Roaming with WDS Access Points

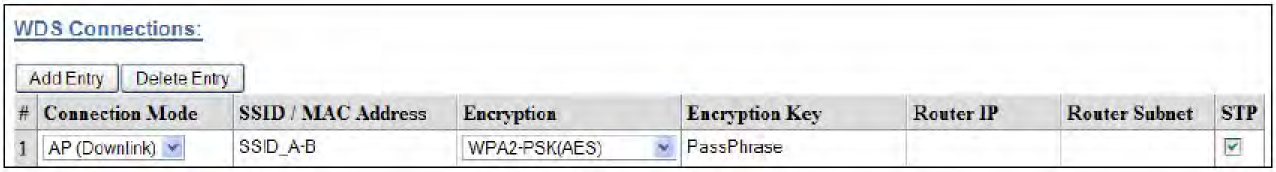


Another common use for WDS is extending the range across a large wireless network but allowing roaming connections between access points or being able to switch to the next Access Point when out of range of the previous Access Point.

The diagram above shows a bridging network with a number of Access Points all with the same SSID, network structure, etc (so as the Stations can freely roam between Access Points)

Each Access Point then needs a separate connection to the next Access Point, which is done using the WDS Virtual Access Points or Stations.

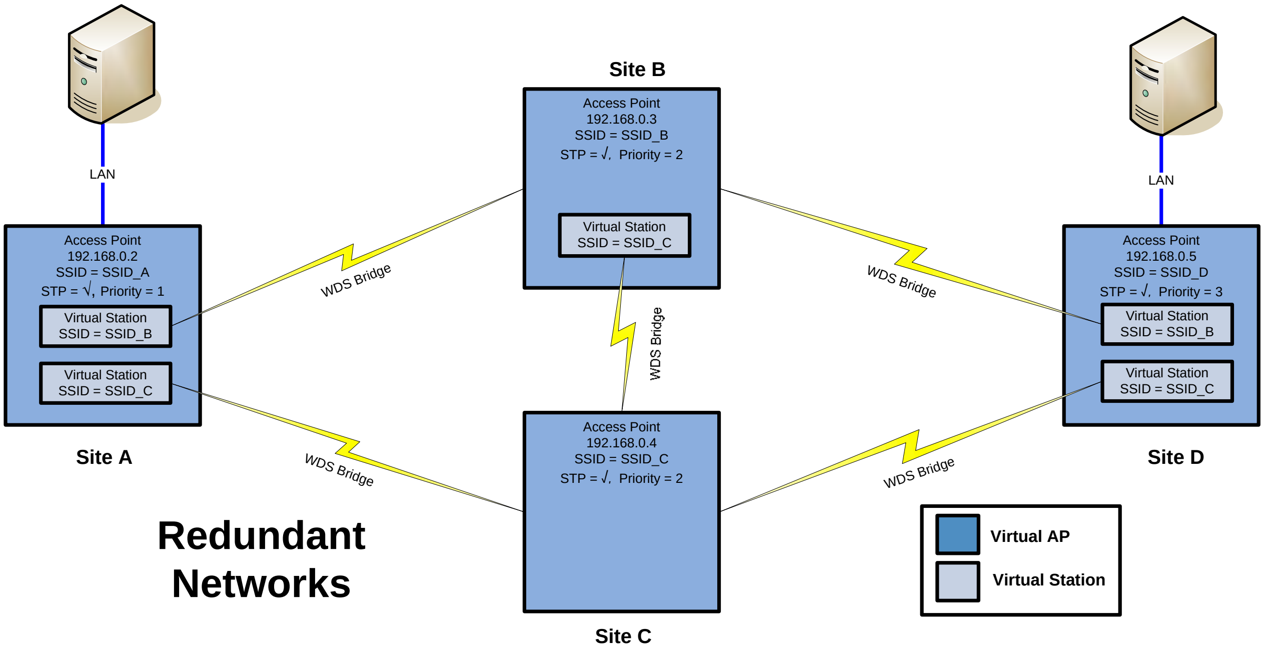
Site B is acting as a Virtual AP for Site A & C, which in turn are acting as Virtual Stations.
This setup can be replicated to extend the range and will allow any Roaming Stations full connectivity across a network
Site B WDS Configuration 2



#	Connection Mode	SSID / MAC Address	Encryption	Encryption Key	Router IP	Router Subnet	STP
1	AP (Downlink)	SSID_A-B	WPA2-PSK(AES)	PassPhrase			☑

Example – Adding Redundancy

In the example below, 4 x Access Points (A, B, C, & D) form a mesh network using only WDS bridge interfaces. Each of the Access Points may also have its own clients associated. Each Access Point is configured with a different SSID, meaning the clients associated with each Access Point are fixed.

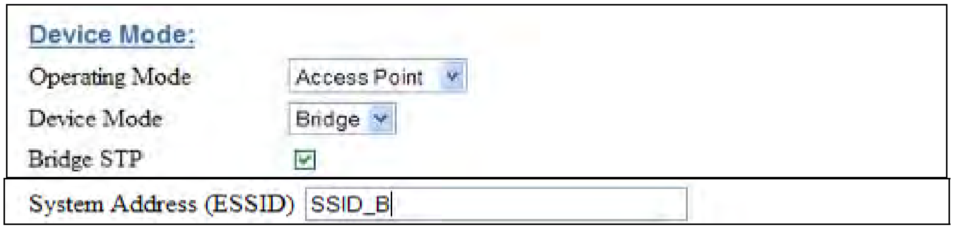


Sites A, B, C, and D can all exchange data with each other (as can all of their Stations) as if they were all on the same wired segment. It can be seen that there are redundant paths and therefore the possibility for loops to occur, so the bridge Spanning Tree Protocol should be enabled and depending on the size of the mesh possibly configuring a Bridge Priority.

Bridge Priority is used to determine the connection priority when selecting an interface to put into the forwarding state. You can assign higher priority values to interfaces that you want spanning tree to select first and lower priority values to interfaces that you want spanning tree to select last. If all interfaces have the same priority value, the MAC address is used to work out the priority.

To illustrate the redundancy, consider that if Site A needs to send data to Site D it has redundant paths through both B and C. However, due to the spanning tree protocol only one of B or C will relay the data, with the other taking over in the event of a failure.

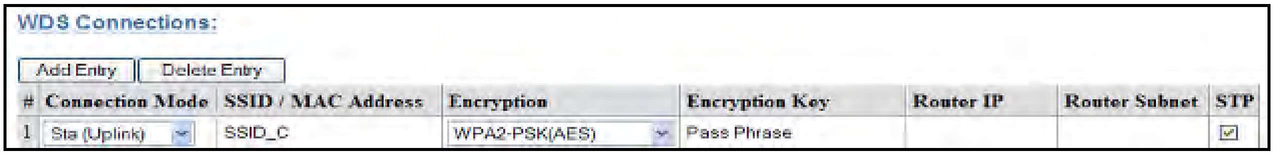
The configuration for Site A and B are shown below. In this example, Site B uses its primary access point to act as an access point for Virtual Stations on Site A and D, and uses a Virtual Station to act as a client to Site C. Site A uses two Virtual Stations to act as clients to Site B and to Site C.



Device Mode:

Operating Mode	Access Point
Device Mode	Bridge
Bridge STP	☑
System Address (ESSID)	SSID_B

Site B configuration – Network Page configured as Primary Access Point

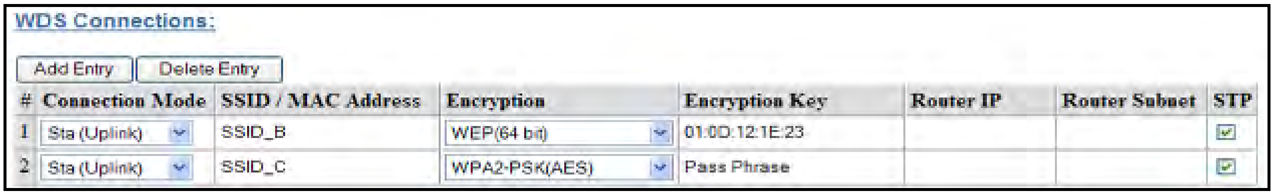


WDS Connections:

Add Entry | Delete Entry

#	Connection Mode	SSID / MAC Address	Encryption	Encryption Key	Router IP	Router Subnet	STP
1	Sta (Uplink)	SSID_C	WPA2-PSK(AES)	Pass Phrase			☑

Site B WDS configuration - Repeaters Page configured with Virtual Station to Site C



WDS Connections:

Add Entry | Delete Entry

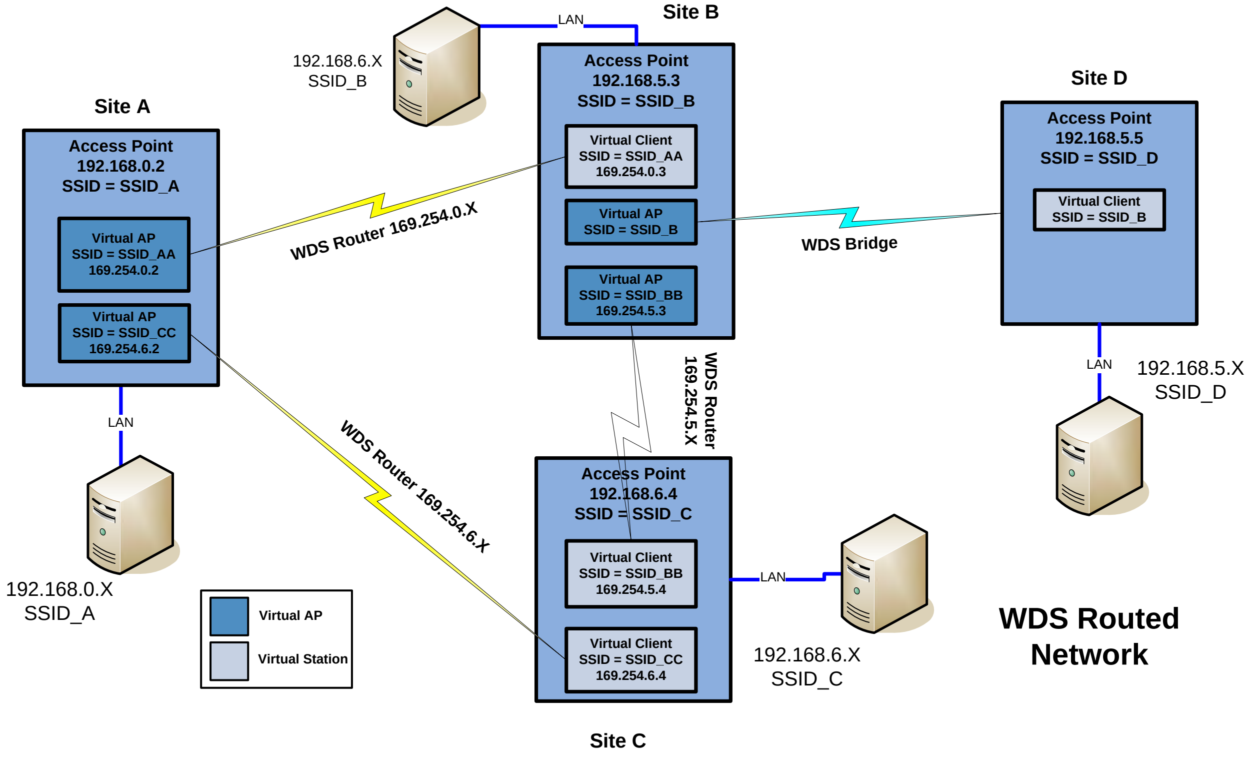
#	Connection Mode	SSID / MAC Address	Encryption	Encryption Key	Router IP	Router Subnet	STP
1	Sta (Uplink)	SSID_B	WEP(64 bit)	01:0D:12:1E:23			☑
2	Sta (Uplink)	SSID_C	WPA2-PSK(AES)	Pass Phrase			☑

Site A WDS configuration - Repeaters Page configured with two Virtual Clients to Sites B & C.

Encryption levels and key above are shows as being different however they can be the same as in some of the earlier examples. One reason why the Encryption level and key would be different is because the Access Point may have clients that communicate using a different Encryption method e.g. 128 bit WEP and may not support the same Encryption method.

Example – WDS Routed Network

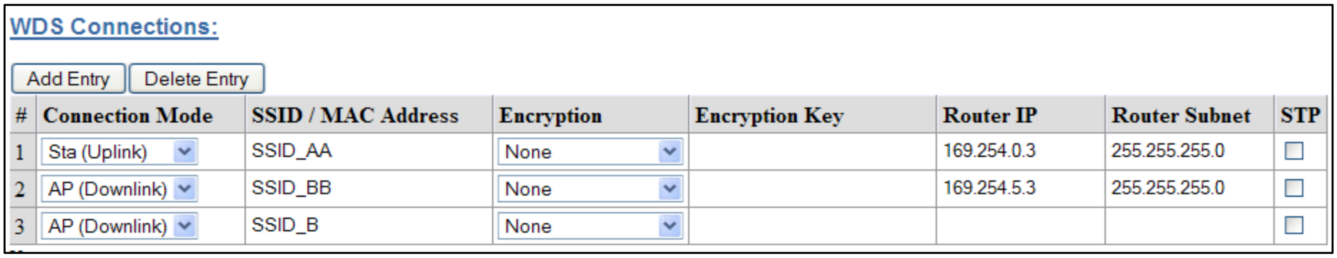
An example of using WDS router interfaces to achieve a similar physical topology to the WDS bridge example discussed earlier is illustrated below.



In both examples, there are four WDS Access points each with the possibility of having their own client/stations associated. In both examples A, B, C, and D can all exchange data with each other. The bridged example has the advantage of redundancy but at the expense of extra overhead. The routed example below cannot provide the redundancy of the bridged example, and requires more configuration effort, but does not have the overhead of using the bridge Spanning Tree Protocol, so is suited to fixed installations that do not require redundancy.

As mentioned previously, configuration of the WDS router example is more complex than the bridged example given earlier. Each Modem and each link have a different SSID. This is done to limit broadcast traffic and to route data only were it needs to go.

Site B in the WDS router example above has three WDS links – to Site A, C, and D; we show Site B's configuration below. It can be seen that there are 3 entries in the WDS Connections list.



WDS Connections:

#	Connection Mode	SSID / MAC Address	Encryption	Encryption Key	Router IP	Router Subnet	STP
1	Sta (Uplink)	SSID_AA	None		169.254.0.3	255.255.255.0	□
2	AP (Downlink)	SSID_BB	None		169.254.5.3	255.255.255.0	□
3	AP (Downlink)	SSID_B	None				□

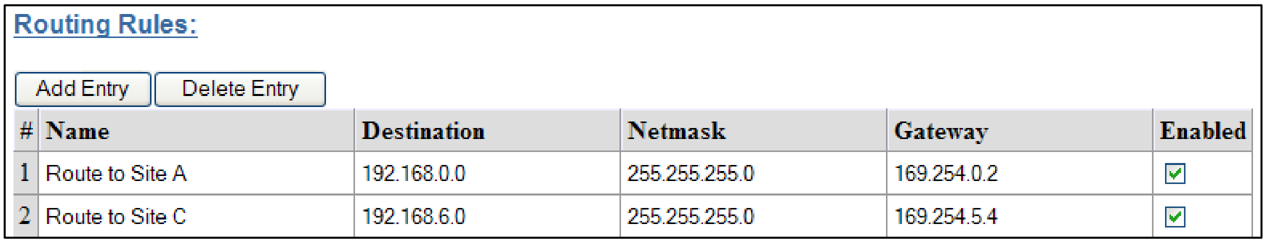
- The first entry specifies a connection from Site B to the virtual AP at Site A whose SSID is "SSID_AA", and has a separate Router IP address of 169.254.0.3 (this is the address that Site B adopts for the link to Site A). Note that this IP Address specifies a different network than that of the default interface for Site A or B (i.e. default interfaces 192.168.0.X and 192.168.X respectively). It is a requirement that the virtual interfaces at each end-point of a WDS link have the same network structure; this ensures that the WDS links at either end point are not bridged with their default interface.

- The second WDS entry above specifies a WDS link from Site B to the virtual Client at Site C whose SSID is "SSID_BB" and like the WDS link to Site A uses a different Router IP address (169.254.5.X) than the default interface. Note that this network address is also different to that used for the WDS link to Site A, so that these separate WDS interfaces are not internally bridged. In addition to adding these WDS link to Site A & C routing rules are required to direct traffic destined for the network address of these units, i.e. 192.168.0.X & 169.254.6.X. See below for examples routing rules.

- The third WDS entry specifies the WDS link to Site D. In the example, Site D is part of the same network structure as Site B; therefore does not require any entries in the Router IP and Subnet fields as the XYR401-E automatically bridges this interface with the default wireless interface. A consequence of using a different network address for the WDS link between Sites B & A and Site B & C, is that we now need to configure routing rules at Sites A, B and C so that the XYR401-E's can determine where to send traffic destined for the other networks.

A consequence of using a different network address for the WDS link between Sites B & A and Site B & C, is that we now need to configure routing rules at Sites A, B and C so that the XYR401-E's can determine where to send traffic destined for the other networks.

For example, if Site B receives traffic destined for network 192.168.0.x (i.e. somewhere on Site A's network), the routing rule specifies that the traffic must be forwarded to the end point of the WDS link to Site A. The routing rules for Site B are shown below (for more information on routing rules, refer to the section 3.14 "Routing Rules").



Routing Rules:

#	Name	Destination	Netmask	Gateway	Enabled
1	Route to Site A	192.168.0.0	255.255.255.0	169.254.0.2	☑
2	Route to Site C	192.168.6.0	255.255.255.0	169.254.5.4	☑

So, in this example, Site B has a total of three IP addresses: 192.168.5.3 for the default interface; 169.254.0.3 for the WDS link to Site A; and 169.254.5.3 for the WDS link to Site C. Note: We choose to always use the same *host* address of 3 for unit B on all of its interfaces regardless of the network address.

- The first routing rule specifies 192.168.0.0 as the destination address (the network address of Site A) – because the last byte is zero, this refers to a route to the network (192.168.0.1 – 192.168.0.254 as opposed to a route to an individual host IP). The same rule specifies the address 169.254.0.2 as the gateway address (this is the WDS Router IP address that Site A has been configured with for its WDS link to Site B). So, this routing rule effectively tells the XYR401-E that any traffic destined for the network 192.168.0.X should be forwarded to Site A via WDS link address 169.254.0.2.
- The second routing rule will be similar except the Destinations IP address will be 192.168.6.0 with a Netmask of 255.255.255.0, indicating all traffic for the 192.168.6.X network will be routed through the WDS link address 169.254.5.4. This is the WDS Router IP address that Site C has been configured with for its WDS link to Site B).

Units A and C would also require similar pairs of routing rules to direct traffic to the network addresses at the end points of their respective WDS links. Refer to section 3.18 "Routing" for further information on routing rules.

The WDS Configuration page (as seen above) is accessible from the "Repeaters" link on any of the configuration web pages. The configurable WDS parameters are summarized below.

Add Entry Button	Add an entry to the WDS Connections table. This adds a virtual station to the device.
Delete Entry Button	Delete the currently selected entry in the WDS Connections table. To select a row, click anywhere in the row with the mouse, to highlight the entire row.

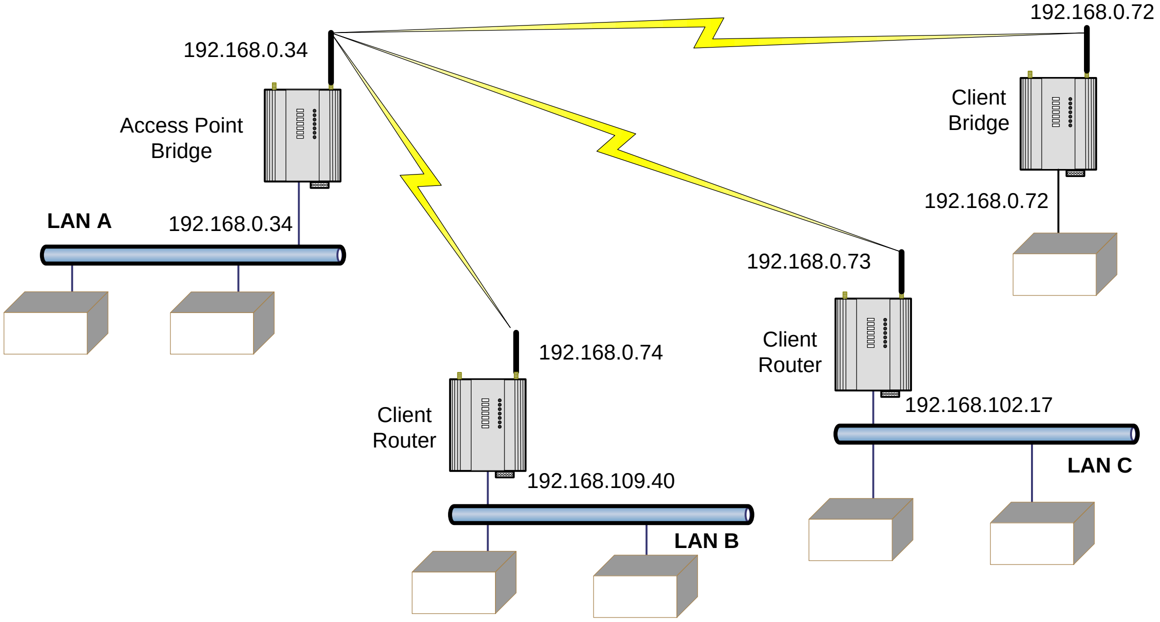
WDS Connections:

Connection Mode	Specify the connection mode for this link. **AP (Downlink)** configures the connection as a virtual access point. **Sta (Uplink)** configures the connection as a virtual client. **Point-to-point** configures the connection as a fixed link.
SSID / MAC Address	**AP Mode:** Specify the SSID that this virtual access point will use. Stations connecting to this virtual access point use this SSID. **Sta Mode:** Specify the SSID that this virtual station will use when connecting to other access points. **Point-to-Point Mode:** Specify the MAC address of an Access Point to establish a Fixed link with. Usually only required for third-party devices.
Encryption	Select the required Encryption (if any) for this WDS link.
Encryption Key	Enter the Encryption key (for WEP encryption) or the passphrase (for WPA encryption). For WEP encryption, the encryption key is set as WEP Key 1. For Sta Mode, this must match WEP Key 1 on the Access point this virtual client will connect to. For AP mode, clients must configure their WEP Key 1 to the same value as this key and select the Default WEP Key to be WEP Key 1.
Router IP	Leave this field blank if this WDS interface is to be bridged with the default wireless interface. Otherwise enter the IP address for *this* connection that specifies the IP network to which messages are routed.
Router Subnet	Leave this field blank if this WDS interface is to be bridged with the default wireless interface. Otherwise enter the subnet mask of the network to which messages are routed.
STP	Applicable to WDS bridged connections only. Select the STP option if you wish to enable the bridge Spanning Tree Protocol on this connection.

3.18 Routing

When a XYR401-E receives an IP frame that is destined for an IP address on a different network, it checks if the *network address* matches the network address of one of its own interfaces (i.e. hard-wired Ethernet, or wireless Ethernet, or WDS) and forwards the frame appropriately. However, if the IP network address does not match the network address of any of its interfaces, the XYR401-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 XYR401-E routers; and in some cases when WDS router interfaces are used). If more than one "next-hop router" is required, the XYR401-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).

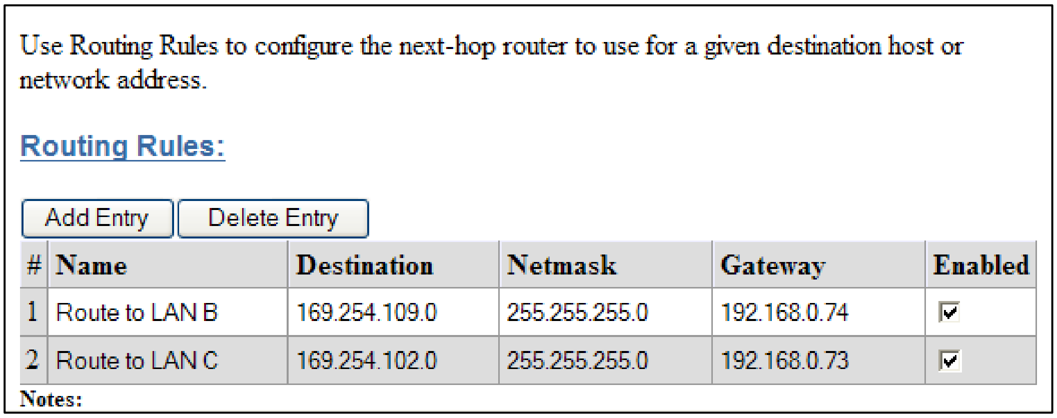


The above network diagram illustrates a situation where routing rules may need to be configured. In this example, the XYR401-E clients need only specify the Access Point as their default gateway (i.e. they require no routing rules be configured). However, for the Access Point to be able to deliver traffic to LAN B and LAN C it needs to have routing rules configured that specify the respective XYR401-E client/routers as next-hop routers (i.e. gateways) to networks B and C. Note that devices on LAN A should specify the XYR401-E Access Point as their default gateway. An alternative to adding routing rules to the XYR401-E in this example would be for each device on LAN A that needs to communicate with LANs B and C to have independent routing rules specifying the XYR401-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 XYR401-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 XYR401-E at LAN B.

Devices on LAN B & LAN C that needs to send messages back to LAN A will need to have their Gateway addresses directed to the XYR401-E on their respected networks. I.e. a LAN B device needs to send data back to LAN A. The Gateway address will need to be configured as 169.254.109.40 as this is the IP address of the wired side of the LAN B XYR401-E. Any message coming in with a 192.168.0.X IP address will be directed across the wireless interface to LAN A.

The Routing Rules configuration page can be accessed by selecting the "Routing" link on any of the configuration web pages. Up to 30 routing rules may be added to each XYR401-E. The table below summarizes the configurable parameters of a routing rule.



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

Routing Rules:

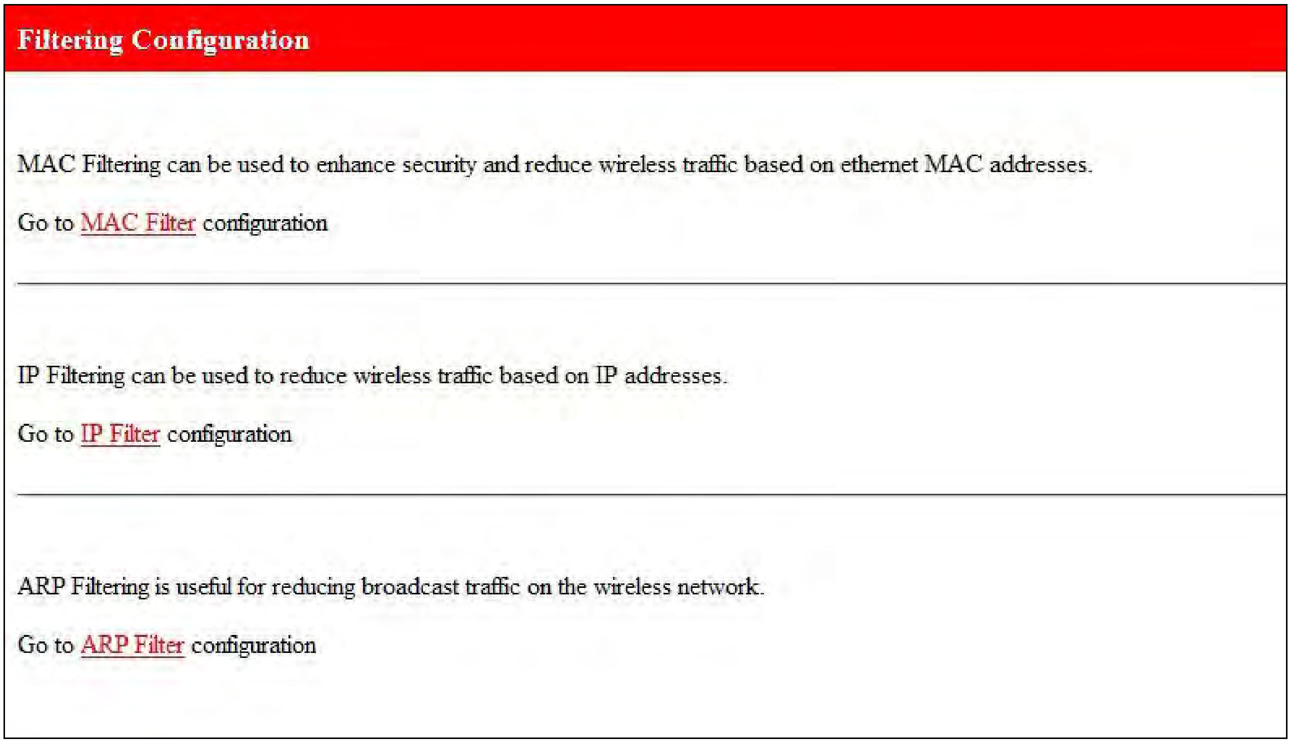
#	Name	Destination	Netmask	Gateway	Enabled
1	Route to LAN B	169.254.109.0	255.255.255.0	192.168.0.74	☑
2	Route to LAN C	169.254.102.0	255.255.255.0	192.168.0.73	☑

Notes:

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 an IP address 192.168.0.0 with Netmask 255.255.255.0 would specify a destination network, while 192.168.0.16 specifies a destination host).
Subnet Mask	The subnet mask for the destination network.
Gateway	The IP address of the next-hop router for the specified destination.
Enabled	Check this box to enable the rule. You can Uncheck the box to disable a routing rule without needing to re-enter the information at a later time.

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

3.19 Filtering



Filtering Configuration

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

Go to MAC Filter configuration

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

Go to IP Filter configuration

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

Go to ARP Filter configuration

When configured as a Bridge, the XYR401-E will transmit all broadcast messages appearing at its wired Ethernet port. When the XYR401-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 XYR401-E has a filtering feature to help reduce unnecessary wireless transmissions and enhance security.

The XYR401-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 XYR401-E.

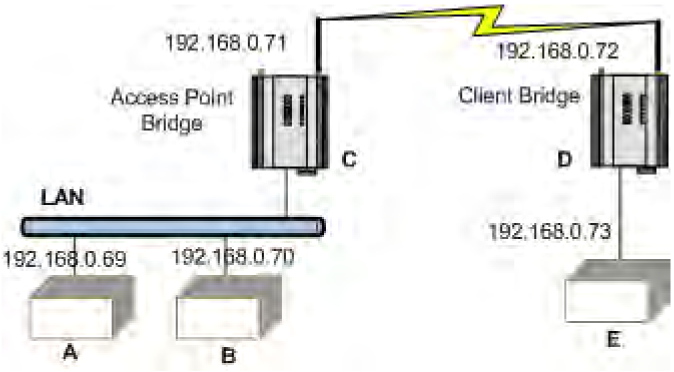
The Filter comprises of three lists: MAC Addresses, IP Address/Protocol/Port and ARP Filters. Each list may be set as either a Blacklist (to block traffic for listed devices and protocols), or as a Whitelist (to allow traffic for listed devices and protocols). The Filter operates on four rules listed below.

- The MAC Address filter is always checked before the IP Address filter.
- If a message matches a MAC filter entry, it will not be subsequently processed by the IP filter. If the MAC filter list is a Whitelist, the message will be accepted. If the MAC filter list is a Blacklist, the message will be dropped.
- The MAC address list checks the Source address of the message only.
- The IP Address filter checks both the source address and the destination address of the message. If either address match, then the rule is activated.
- ARP filtering applies only to ARP request packets (typically these are broadcast packets) which are sourced from the Ethernet interface and destined for the wireless interface. (ARP requests from devices on the wireless network will always be passed to the Ethernet interface. ARP response packets will always be passed).

When configuring a Whitelist it is important to add the Addresses of all devices connected to the XYR401-E wired Ethernet port, that communicate over the wireless link. It is particularly important to add the Address of the configuration PC to the Whitelist. Failure to add this address will prevent the configuration PC from making any further changes to configuration. Design of the filter may be simplified by monitoring network traffic and forming a profile of traffic on the wired network. Network Analysis software, such as the freely available "Wireshark" program, will list broadcast traffic sent on the network.

For example, in the figure below, Device B needs to communicate with Device E via modems C & D. The Filtering requires that at Modem C has Device B in its Whitelist and Modem E has Device E in its Whitelist. With this filtering Device A will be not be able to access Device E, as Device A is not present in the Whitelist in Modem C.

If radio links are chained together to form a radio backbone, it is also important to consider the operation of the Layer 3 Transparent Bridge (Refer Section 3.8). A XYR401-E Client will act as a MAC Address translator, as it acts as a MAC address proxy on behalf of devices connected to its wired Ethernet port. Addition of XYR401-E Client MAC addresses into intermediate XYR401-E units' Whitelist filters may be required for correct operation.



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

MAC Address Filter Configuration:

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

In theory, MAC filtering allows a administrators to permit or deny network access to hosts associated with the MAC address, though in practice there are methods to circumvent this form of access control through address modification

The MAC filter entry will match only the source MAC address in the packet.

Note: It is important to add the MAC Address of the configuration PC when creating a Whitelist. If the configuration PC is not on the Whitelist, it will be unable to communicate with the module for further configuration.

Select "Blacklist" or "Whitelist".	Blacklist will prevent all listed devices from accessing the module and using the radio link. Whitelist will allow devices with the MAC addresses listed to communicate with the module and utilize the radio link. All other devices are blocked.
Add Entry	Add a row to the table of Mac Address filter rules
Delete Entry	Delete the currently selected MAC address filter rule.
Enable	Check to enable the rule.
Mac Address	Enter the desired source MAC Address
Save Changes	Save changes to non-volatile memory (Reset is required to activate)
Save Changes and Reset	Save to non-volatile memory And restart to activate changes

IP Address Filter Configuration:

The IP filter allows can be used to permit or deny network access to specific devices through the use of Blacklists (blocking of traffic that matches a rule) and Whitelists (allow traffic that matches a rule).
The IP filter entry will match either source or destination address in the packet. That is, if either the source or destination IP address falls within the address range specified in the rule, the packet is matched and will be discarded (Blacklist) or allowed (Whitelist).

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

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

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

ARP Filter Configuration

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

On large networks, you generally tend to get a high proportion of broadcast messages. Using ARP filters is useful for reducing broadcast traffic on the wireless network by only allowing ARP requests for known units to pass, or blocking ARP requests for high use addresses.

Select “Blacklist” or “Whitelist”.	A Blacklist will block ARP requests that match the entry. A Whitelist will allow only ARP Requests that match the entry. All other devices are blocked.
Add Entry	Add a row to the table of ARP Address filter rules
Delete Entry	Delete the currently selected ARP address filter rule.
Enable	Check this box to enable the rule
IP Address	This sets the IP address that you wish to filter.
IP Netmask	Sets the IP Netmask
Save Changes	Save changes to non-volatile memory (Reset is required to activate)
Save Changes and Reset	Save to non-volatile memory and restart to activate changes

3.20 DHCP Client Configuration

DHCP (Dynamic Host Configuration Protocol) allows DHCP Clients to automatically obtain their IP Address at start-up. This simplifies network administration, as there is no need to manually configure each device with a separate IP Address. The XYR401-E is able to act as a DHCP client. To set the XYR401-E to acquire its IP address from a DHCP Server, check the box "Obtain IP Address Automatically" on the Network Configuration page.
When configured as a DHCP Client the "Device Name" on the Module Information page will be the module identifier (as the IP address will be unknown) and so should be given a unique name.

3.21 DHCP Server Configuration

The XYR401-E is able to act as a DHCP server, supplying IP addresses automatically to other DHCP Client devices. Note that the XYR401-E units need to act in conjunction with their connected devices. If a connected device is a DHCP server, the local and remote XYR401-E units can be configured as DHCP Clients and receive IP addresses from the server device. Similarly, if a XYR401-E is configured as a DHCP server, it can provide IP addresses to DHCP Clients, both XYR401-E units as well as other connected devices. Configuration items for the DHCP Server are listed below.

Enabled	Tick this box to enable the DHCP Server
IP Range Minimum / Maximum	The DHCP Server will assign IP addresses to DHCP Clients from within this range of addresses.
Gateway / Primary DNS / Secondary DNS	These Settings are common to all of the DHCP Clients, and refer to the gateway address, and Domain Name Service (DNS) Configuration
Lease Time	This is the number of seconds the client is granted the assigned IP address. The client should renew its lease within this time.

3.22 DNS Server Configuration

DNS (Domain Name Service) allows devices to be given human-readable names in additions to their IP address. This makes identification of devices (hosts) simpler, and makes it possible to identify devices which have been automatically assigned their IP address by a DHCP server (See section 3.21 "DHCP Server Configuration"). DNS is the system which translates internet names (such as www.honeywell.com/ps) to IP Addresses. The HONEYWELL XYR401-E can act as a DNS Server for a local network. Name to IP address mapping are automatically updated by the built in DHCP server when it issues an IP address to a client unit.
For the DNS Server configuration to be effective, Each DNS Client must be configured with the address of this DNS server, as either the primary or secondary DNS (secondary DNS is only used if there is no response from the primary DNS). Normally, this is done by setting the primary DNS field of the DHCP server configuration to the wireless IP address. This address is then provided to client units to use as their primary DNS server address when the DHCP server issues an IP address. The DNS Server is configured using the following settings.

Enabled	Tick this box to enable the DNS Server
Domain Name	This is a common suffix applied to the name of each device in the network. If your network is part of a larger network, this would be assigned to you by the relevant naming authority. If your network is stand-alone, this field is set to an arbitrary name of your choice.
Device Name (Host Name)	This is the DNS name of the local device. (Commonly referred to as the host name or computer name). This setting is duplicated on the main Module Information configuration page. This is the name which is used to refer to this device. (Refer Section 3.23 "Module Information Configuration")

3.23 Module Information Configuration

Module Information Webpage Fields

This configuration page is primarily for information purposes. With the exception of the password, the information entered here is displayed on the home configuration webpage of the XYR401-E.

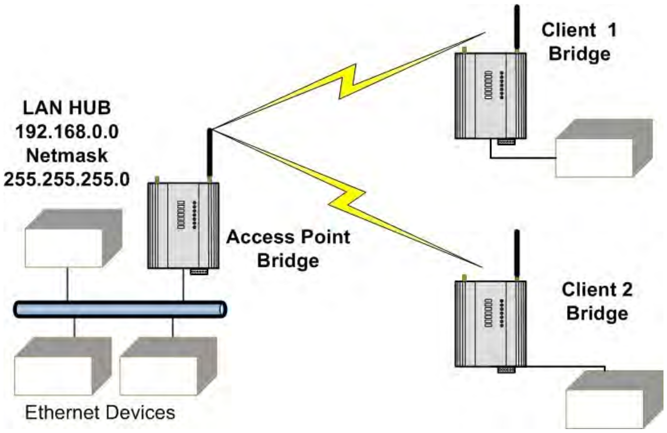
Username	Configuration of Username. This is the username used to access the configuration on the XYR401-E. Take care to remember this username if you change it as it will be needed to access the XYR401-E in future.
Password	Configuration of Password. This is the password used to access the configuration on the XYR401-E. Take care to remember this password if you change it as it will be needed to access the module in future.
Device Name	A text field if you wish to label the particular XYR401-E. This is also the DNS name (hostname) of the device if you are using DNS.
Owner	A text field for owner name.
Contact	A text field for owner phone number, email address etc.
Description	A text field used for a description of the purpose of the unit.
Location	A text field used to describe the location of the XYR401-E.

3.24 Configuration Examples

Setting an XYR401-E to Factory Default Settings

Access configuration webpage on the XYR401-E.
Refer section”3.2”.

- Click on “System Tools” Menu Item
- Click on Factory Default Configuration Reset, and wait for unit to reset. While the module executes the reset sequence the OK LED will flash. The OK LED will turn green when the reset sequence is complete.



Extending a wired network

Access Point Configuration

Connect straight through Ethernet cable between PC and XYR401-E.

Ensure configuration PC and XYR401-E are setup to communicate on the same network

Set dipswitch to SETUP mode.

Power up unit, and wait for the OK LED to cease flashing. Adjust PC network settings

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

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

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

Click “Network”, and select Operating Mode as Access Point.

Select Device Mode as Bridge.

Change the Gateway IP Address to 192.168.0.1

Change the Ethernet and Wireless IP addresses to 192.168.0.200

Change Ethernet and Wireless Subnet masks to 255.255.255.0

Enter a System Address (ESSID) string

Select the Radio Encryption required.

Set dipswitch to RUN

Save the changes and unit will restart with new settings.

Client 1 Configuration

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

Set the Ethernet and Wireless IP addresses of XYR401-E to 192.168.0.201

Set the Operating Mode to Client.

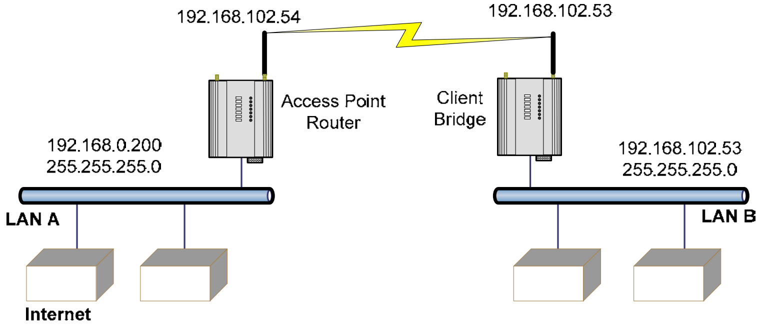
Ensure the ESSID and Radio Encryption method match the Access Point.

If encryption is used, ensure the encryption keys or passphrase match the Access Point.

Client 2 Configuration

As above, however set the Ethernet and Wireless IP addresses as 192.168.0.202

Connecting two separate networks together



LAN A Configuration

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

Devices on LAN A that only require access to devices on LAN A and B, should have their gateway IP address set to the XYR401-E Access Point as 192.168.0.200.

Devices on LAN A, that must interact with devices on LAN 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 LAN B. On PCs, this may be achieved with the MS-DOS command ROUTE. For this example use: ROUTE ADD 169.254.102.0 MASK 255.255.255.0 192.168.0.200

LAN B Configuration

All devices on LAN B should be configured so their gateway IP address is that of the XYR401-E Access Point as 169.254.102.54

Access Point Configuration

- Connect straight through Ethernet cable between PC and XYR401-E.
- Ensure configuration PC and XYR401-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 https://192.168.0.1XX/

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

  Enter “Network”, and select Operating Mode as Access Point.

  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

  Select the Radio Encryption required, and enter encryption keys or passphrase if necessary.

  Set dipswitch to RUN.

  Click on button Save to Flash and Reset. Webpage will display that message indicating details are being written to flash. Wait for XYR401-E to reboot before removing power. Enter a System Generator String

Client Configuration

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

Enter “Network”, and select Operating Mode as Client.

Device Mode should be set to Bridge.

Set the Gateway IP address to 169.254.102.54

Set the Ethernet IP address to 169.254.102.53, 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 XYR401-E to reboot before removing power.

Extending range of a network with a Repeater hop

3.25 Configure units as described in “Error! Reference source not found.”. Place the Access Point at the remote intermediate repeater location. Additional repeaters can be added using Wireless Distribution System (WDS) – refer 3.12 ”Serial Menu

RS232 / RS485 Serial Port Configuration

RS232 Port	Select the desired functionality. Select either PPP, Serial Gateway or Modbus TCP to RTU
Data Rate	The serial data rate desired. Serial data rates available range from 110bps to a maximum of 115,200bps.
Data Format	The data format desired. All the standard data formats are supported.
Flow Control	Selects CTS/RTS or None

RS232 PPP Server (Only RS232)

Username	User name to enter to access RS-232 PPP Server.
Password	Password to access RS-232 PPP Server.
Local IP Address	Select the IP address of the PPP server. The remote device may be made visible on the Ethernet or Wireless networks by either utilising proxy-arp or routing. The proxy-arp feature may be enabled by setting the Local IP address the same as the Ethernet IP Address or the Wireless IP Address. The module will respond on behalf of the remote device, making it seem like the device is present on the configured network. Alternatively, if the IP address selected is not the same as the Ethernet or Wireless IP address, routing is used to pass data to the Ethernet and Wireless ports.
Remote Device IP Address	Select the IP address of the remote device. Ensure this address is not the same as any other device on the Ethernet or Wireless networks.

RS232 / RS485 Serial Gateway

Serial Gateway Mode	**Server - Module will wait for a connection to be initiated by a remote Client.**
Character Timeout	Enter the maximum delay (in msec) between received serial characters before packet is sent via network.
Packet Size	The number of received bytes that will be buffered before a packet is sent via the network.
Listen Port (Server)	Server Only. Enter the TCP port number on which the server must listen for incoming connections. The standard TELNET port is 23.
Serial Gateway Mode	**Client** only. Module will automatically attempt to connect to the specified remote server.
Character Timeout	Enter the maximum delay (in msec) between received serial characters before packet is sent via network.
Packet Size	The number of received bytes that will be buffered before a packet is sent via the network.
Remote Device Port (Client)	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.
Serial Gateway Mode	Multicast - Allows point to multi-point serial transfer. All members of the group will receive serial transmissions made by any other member of the Multicast group.
Character Timeout	Enter the maximum delay (in msec) between received serial characters before packet is sent via network.
Packet Size	The number of received bytes that will be buffered before a packet is sent via the network.
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 Address	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.
Serial Gateway Mode	Modbus - Allows a serial Modbus Client (Master) to connect with a single Ethernet Modbus TCP Server (Slave)
Character Timeout	Enter the maximum delay (in msec) between received serial characters before packet is sent via network.
Packet Size	The number of received bytes that will be buffered before a packet is sent via the network.
Modbus Server Port	Enter the TCP port number of the remote server (i.e. the remote port to automatically connect to).
Modbus Server IP Address	Enter the IP Address of the remote server (i.e. the remote IP Address to automatically connect to).

RS232 / RS485 Modbus TCP / RTU Converter

Modbus Server TCP Port	Port number used for the Modbus TCP – Standard port is 502.
Pauses 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.

3.26 Multicast Pipe Manager

Previously it has been difficult to connect a single TCP device, i.e. a Scada / DCS system to multiple remote multicast serial devices.

Multicast Pipe allows this type of connection.

An example would be a Scada system that needs to communicate with multiple remote serial devices. A modem can be placed at each remote location and connected serially to each device. A multicast pipe is configured to communicate with all devices using a multicast address and port, i.e. 224.0.1.1:5000.

The Scada then communicates with the remotes via the IP address of the Multicast Manager and the port selected in the configuration, i.e. 5001.

3.27 Digital Input/Output

The functionality of the shared Digital Input/Output pin may be configured via the “I/O Transfer” 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 be transferred to/from another device using Modbus (see section “**Error! Reference source not found.** Modbus I/O Transfer”) or it can be configured to provide status of the module communications. If the XYR401-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).

3.28 Modbus I/O Transfer

The XYR401-E 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 XYR401-E can transfer I/O to/from almost any combination of Modbus TCP or RTU devices.

The layout of the XYR401-E I/O Registers is summarized in the table below. Each register is internally saved as a 16 bit unsigned integer value. A Modbus transaction may access the entire 16 bit value of any register, or alternatively the most significant bit of a register may be accessed as a discrete value. The main use for the general purpose I/O registers is for intermediate storage, i.e. when transferring I/O from one Modbus Slave device to another. Also provided is the status of the onboard digital I/O, as well as the status of the wireless link. The 16 bit status register contains 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	Link Status (read only)
4320	On-board Digital Output value (read/write)
4370	On-board Digital Input inverted value (read only)
4371	Link Status inverted (read only)
4372-4999	Reserved for future use

Modbus TCP Client (Master) enables the XYR401-E to connect to one or more Modbus TCP Servers (Slaves).
All Modbus Master messages are directed 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 XYR401-E serial port by enabling the Modbus TCP to RTU gateway at the corresponding serial port (see section 3.11 “Serial Port Configuration”).

Modbus TCP Client functionality allows connections to a maximum of 100 mappings to be configured and a maximum of 25 different Modbus TCP Servers.

Modbus TCP Server (Slave) enables the XYR401-E to accept connections from one or more Modbus TCP Clients (Masters).

All Modbus transactions routed to the onboard Modbus TCP Server are directed to/from the onboard general purpose I/O registers. The Modbus TCP Server is shared with the Modbus TCP to RTU 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 XYR401-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 XYR401-E that the serial device is connected to.

The XYR401-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 XYR401-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 single bit registers from Modbus serial device D will be transferred to A.

Unit B is configured with Modbus TCP Server enabled and Device ID = 1, Unit C is configured as shown above.

- The first will write the register 4300 (Local Digital Input) to server IP address 192.168.0.200 (Unit B), Device ID #1, register 4320 (Local Digital output).
- The second mapping shows a Modbus read command of 8 Discretes starting at register 1 (Destination Reg) on Device ID #6 connected to IP address 192.168.0.123 (it self) and store the values at register #1 locally.
- The third mapping shows the Modbus write command (Write Coils) which is writing the local 8 I/O's starting at register 1 across to Server IP address 192.168.0.200, Device ID #5, destination reg #1.

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 Modbus TCP to RTU Gateway" on page 50) 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 XYR401-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.

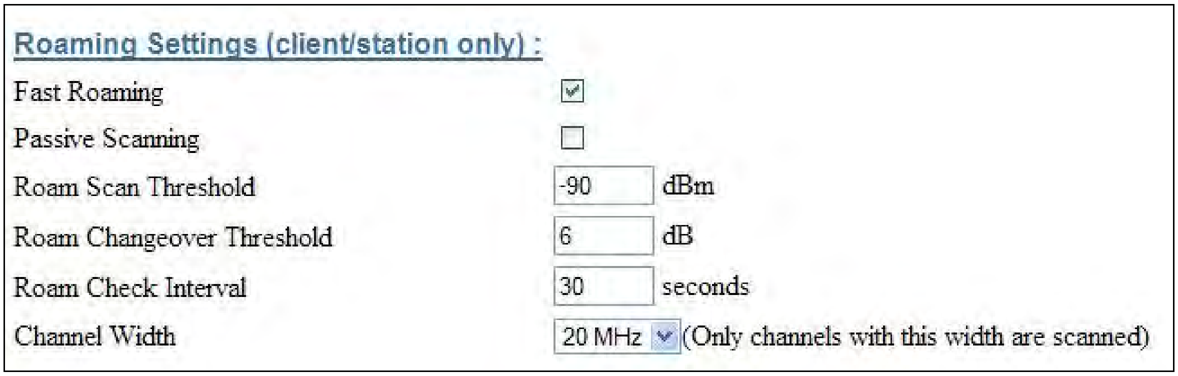
Modbus TCP Configuration on I/O Transfer Menu:

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.
Enable Modbus Statistics	Enables the Modbus Diagnostic registers as shown in Section 34.6 "Internal Diagnostic Modbus Registers" Disabling this option will free up the registers and also slightly increase processing resources.
Log background Noise	RSSI & BGND on Rx messages are made available in the diagnostic registers (See 4.4 "Internal Diagnostic Modbus Registers" for details. For a Hex value of 5F5D the 5D byte = RSSI and the 5F byte = BGND (Convert value from hex to dec and add a "-"e.g. 5F = -95dB). Enabling this option removes the RSSI byte from these registers and so only the Background Noise value is made available.

Modbus TCP Client Mappings on I/O Transfer Menu:

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

3.29 Roaming



Roaming Settings (client/station only) :

Fast Roaming	☑
Passive Scanning	□
Roam Scan Threshold	-90 dBm
Roam Changeover Threshold	6 dB
Roam Check Interval	30 seconds
Channel Width	20 MHz (Only channels with this width are scanned)

In certain cases a Client may be in a mobile situation and require a method of roaming to another Access Point.

Normal network communications provides only basic roaming behavior which means as the client moves further from the AP it will go through a period of poor communication followed by a complete disconnection of the radio link.

It is at this point that the Client will scan for Access Points and if one is in range it could take up to 10 seconds for the client to establish a connection.

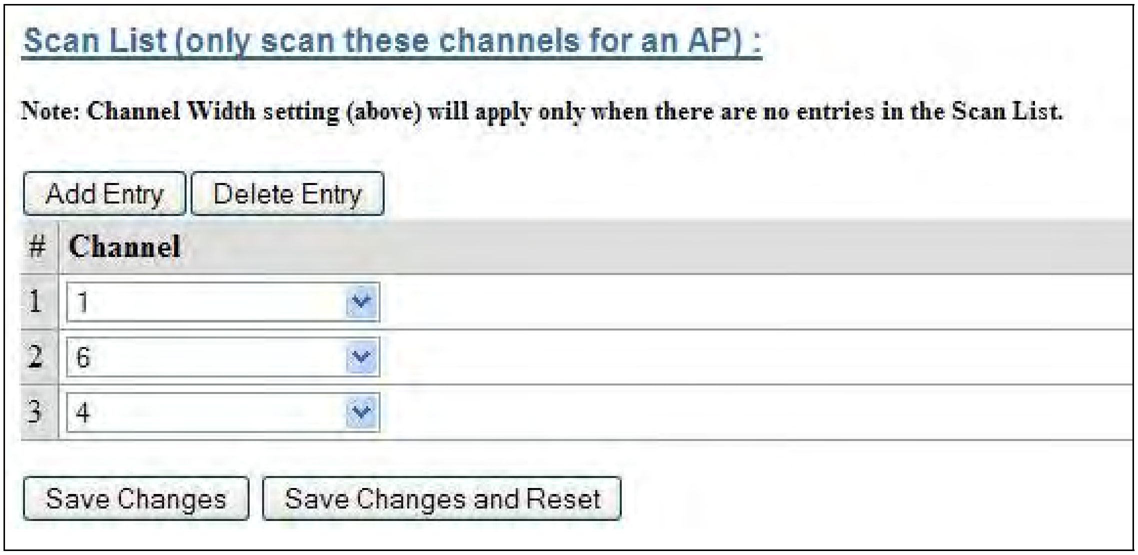
Fast Roaming will significantly reduce the time taken for a client to roam from Access Point to Access Point. Also the discovery of AP's is done before the existing radio link deteriorates therefore eliminating the periods of poor performance during transition to the next AP.

The following settings/thresholds can be configured to fine tune the fast roaming process.

Fast Roaming	Fast Roaming allows a client (station) to roam to an AP with a stronger signal strength without disrupting communications. Or roam seamlessly between multiple Access Points based on configuration parameters such as RSSI threshold.
Passive Scanning (STA only)	Selecting this item stops a Client device from sending ―probe request ‖ messages when it is searching for an access point to connect to. Instead, the client waits for a beacon transmission from the access point. Passive Scanning should be disabled when Fast Roaming is enabled.
Roam Scan Threshold	Background Scan will be initiated when the RSSI to the currently connected AP drops below this threshold and Fast Roaming (above) is enabled. Default is -90dBm
Roam changeover Threshold	This is the RSSI value above the Roam Scan Threshold that is required for the Client to change to the new Access Point. In the example shown above the Access Point RSSI would need to be above -84dB before it would changeover. In general, the Roam Changeover Threshold should be at least 6dB, otherwise changeovers could occur too frequently.
Roam check Interval	If a better AP is not found, the background scan is repeated every Roam Check Interval while the signal strength to the currently connected AP is below the Roam Scan Threshold. Default is 30seconds
Channel Width	Selects channel width bands for background scan. If 5MHz is selected then only 5MHz channels will be scanned during the background scan. Default is Auto, which means all channels will be scanned.
Save Changes	Save changes to non-volatile memory. Changes will not take effect until module is reset.
Save Changes and Reset	Save changes to non-volatile memory and reset module

When Fast Roaming is enabled the Client goes off-channel and periodically performs a background scan to identify available AP’s. When AP’s are identified the RSSI is recorded as a potential connection. It takes 50msec to scan each channel, with a 1 second delay between each scanned channel. So scanning 10 channels will take 10 second, during which time latency of up to 50msec will occur and any throughput traffic is essentially paused and buffered for retransmission when complete. It is therefore recommended the scan list is used to limit the number of channels the client needs to scan thus reducing the overall scan time.

During the background scan a client will scan all of the channels in the Scan List to identify better AP's. If no channels are configured it will scan all channels.



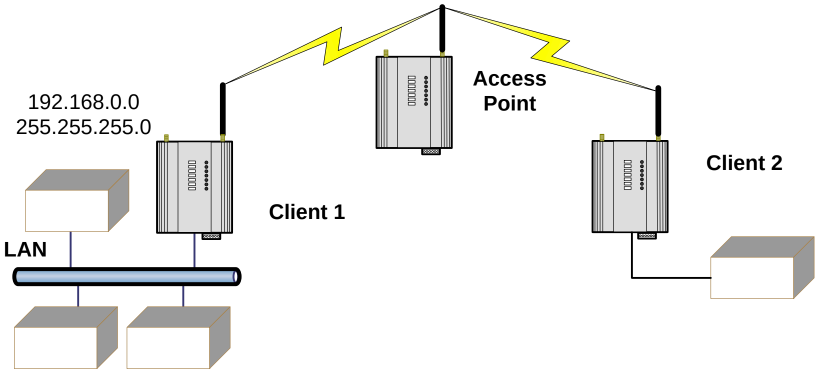
Scan List (only scan these channels for an AP) :

Note: Channel Width setting (above) will apply only when there are no entries in the Scan List.

#	Channel
1	1
2	6
3	4

The above configuration shows that the Client will start scanning when the RSSI of its current connection to the Access Point falls below -90dBm. When this happens it will scan the list of Access Points configured in the Roaming Scan List (in this case channels 1, 4 & 6, as shown below) and if any of the RSSI levels are greater than -84dBm it will change to this Access Point.

for further details.



Chapter Four DIAGNOSTICS

4.0 Diagnostics Chart

LED Indicator	Condition	Meaning
OK	GREEN	Normal Operation
OK	RED Continuously	Supply voltage too low. OR Internal Module Fault
OK	RED At Power On	Boot Loader delay at start-up
OK	Fast Flash RED / GREEN	Module Boot Sequence
OK	Slow Flash RED / GREEN	Module Boot Sequence
Radio RX	GREEN flash	Radio receiving data
Radio RX	RED flash	Radio receiving data (Low Signal strength)
TX/LINK	GREEN	Connection Established to remote device
TX/LINK	RED Flash	Radio Transmitting
RS-232	GREEN flash	Data sent from RS-232 Serial Port
RS-232	RED flash	Data received to RS-232 Serial Port
LAN	ON	Link Established on Ethernet port
LAN	Flash	Activity on Ethernet port.
RS-485	GREEN flash	Data sent from RS-485 Serial Port
RS-485	RED flash	Data received to RS-485 Serial Port
DIO	GREEN	Digital Input is grounded.
DIO	RED	Digital Output is active
DIO	Off	Digital Output OFF ***and*** Input is open circuit.

The green OK LED on the front panel indicates correct operation of the unit. This LED turns red on failure as described above. When the OK LED turns red shutdown state is indicated. On processor failure, or on failure during start-up diagnostics, the unit shuts down, and remains in shutdown until the fault is rectified. During Module, boot-up the OK LED flashes RED-GREEN until the boot sequence is complete.

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

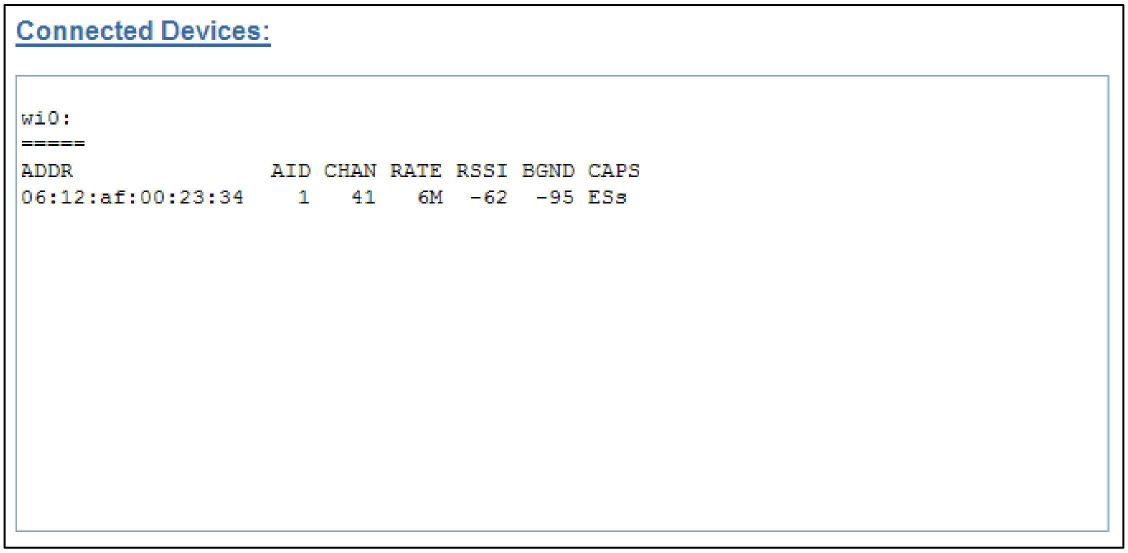
If the OK LED remains red at power on, this could indicate either low supply voltage (The module will not attempt to boot until supply voltage is within range); Module fault; or a long boot delay. To check if the boot delay is the problem, plug a terminal into the RS-232 serial port and configure for 115,200 baud, 8 data, no parity.

4.1 Connectivity

Connectivity

The Connectivity webpage displays connections and available networks. The "Connected Devices" section displays the radio channel, received signal strength, and radio data rate for each Client or Access Point by their MAC Address. The readings shown are based upon the last received data message from the Access Point or Client. Client stations also display a list of detected Access points (Site Survey), including network name (SSID), channel and maximum data rate.

Note that when updating the Connectivity webpage, it is necessary to hold down the <ctrl> key while pressing the refresh button. Otherwise, the information will not be updated.



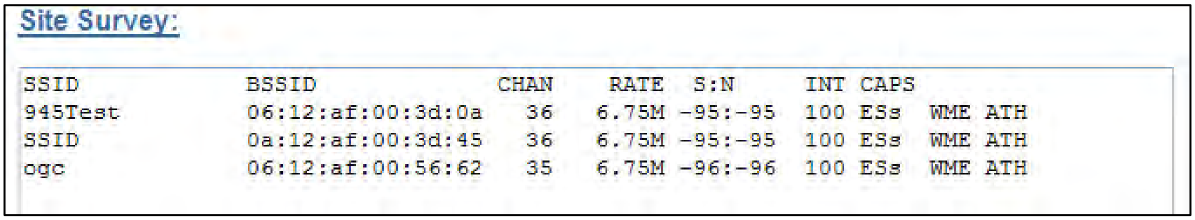
Connected Devices:

```
wi0:
=====
ADDR                 AID CHAN RATE RSSI BGND CAPS
06:12:af:00:23:34     1   41   6M  -62  -95 ESs
```

Connectivity Parameters	
AID	Association ID: Every Client gets a unique temporary ID from the AP
CHAN	Channel: What radio channel is being used.
RATE	Radio Data Rate:
RSSI	Radio Signal Strength Index (Amount of received signal strength).
BGND	Background interference level in dBms: The amount of internal noise the radio is able to hear. This level does not indicate external radio interference noise level
CAPS	Capabilities (Ref 802.11 Standard)

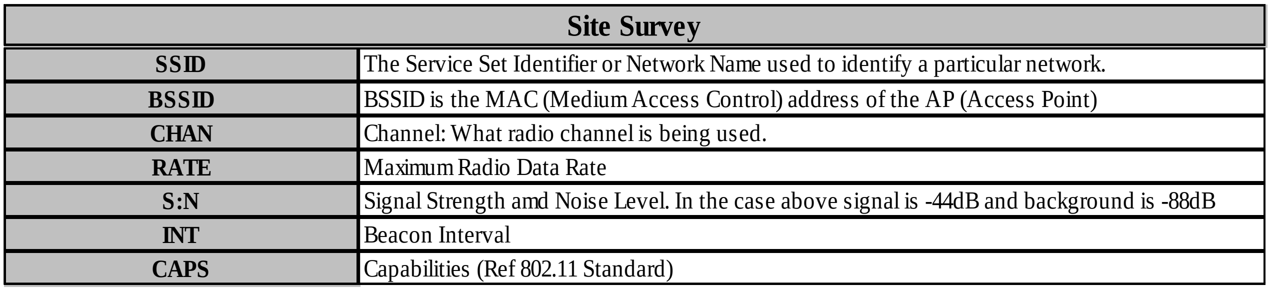
Site Survey

Site Survey is a one off snapshot showing what Access Points are available for connection.
This list is only available on Clients and only available at start-up of the module or by selecting Background Scanning on the radio page.



Site Survey:

```
SSID            BSSID              CHAN   RATE  S:N     INT CAPS
945Test         06:12:af:00:3d:0a   36   6.75M -95:-95  100 ESs  WME ATH
SSID            0a:12:af:00:3d:45   36   6.75M -95:-95  100 ESs  WME ATH
ogc             06:12:af:00:56:62   35   6.75M -96:-96  100 ESs  WME ATH
```



Site Survey	
SSID	The Service Set Identifier or Network Name used to identify a particular network.
BSSID	BSSID is the MAC (Medium Access Control) address of the AP (Access Point)
CHAN	Channel: What radio channel is being used.
RATE	Maximum Radio Data Rate
S:N	Signal Strength amd Noise Level. In the case above signal is -44dB and background is -88dB
INT	Beacon Interval
CAPS	Capabilities (Ref 802.11 Standard)

4.2 Channel Survey (Utilisation)

Channel Utilisation gives a visual display of how busy the current channel is over a given time period. Channel Utilisation is made up of 3 components: transmissions made by this radio; data received by this radio; and noise or interference that this radio can hear. These 3 components may also be viewed individually on the ―Custom Survey” page. Channel Utilisation is logged by the radio for 3 separate time intervals: every second for the last 60 seconds; every minute for the last 60 minutes; and every hour for the last 60 hours.

The Elpro 802.11 Ethernet modem utilizes a half duplex radio channel for communications. At any given time, an Access Point and its associated clients occupy a radio channel. These radio channels, or frequencies, are license free and may contain interference from any number of other radio transmitters. When installing or diagnosing a 245 modem, the potential capacity of a given radio channel will be reduced by the existence of these other RF signals on the same channel.

Channel Utilisation allows us to see how much RF activity is on a given channel as a percentage of the total utilisation. A channel that is very busy will have high channel Utilisation (usually 50% or greater). Conversely a channel that is quiet will have low channel utilisation.

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

Channel Utilisation on a Live System:

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

Using Channel Utilisation for Channel Selection or RF Path Testing:

When used on an inactive system, the Channel Utilisation will indicate how quiet the current channel is, and therefore indicate how much interference is present. To select the quietest channel, configure the radio as an Access Point with no data transfer, and on each channel of interest record the Channel Utilisation over a period of time. The channel with the lowest Channel Utilisation will be the quietest channel, and therefore is likely to provide the best performance. This procedure, in addition to a Throughput Test, is recommended for complete radio path testing.

Diagnosing Low Throughput:

When iperf throughput testing has given poor results, Channel Utilisation can be used to confirm whether or not the poor results were due to interference. If the Channel Utilisation (excluding the time period while iperf was running) is seen to be high, then this will confirm that the poor throughput was due to other RF interference. Alternatively if the Channel Utilisation is seen to be low (indicating little interference), then the poor throughput would more likely be attributed to poor RSSI - which could be confirmed on the Connectivity page.

Solutions for High Channel Utilisation:

When substantial interference has been identified using Channel Survey or Custom Survey, the simplest solution is to change to another channel that is seen to have lower Channel Utilisation. If a better channel is not available, configuring a fixed noise floor can often greatly improve performance. Configuring a fixed noise floor can be performed on the Advanced Radio Configuration page. The fixed noise floor should be at least 8dB greater than the weakest RSSI of any connected modem, otherwise communications could be lost. After configuring the fixed noise floor, confirm that the Channel Utilisation has dropped to a desirable level, and where possible perform a Throughput Test to confirm acceptable performance.

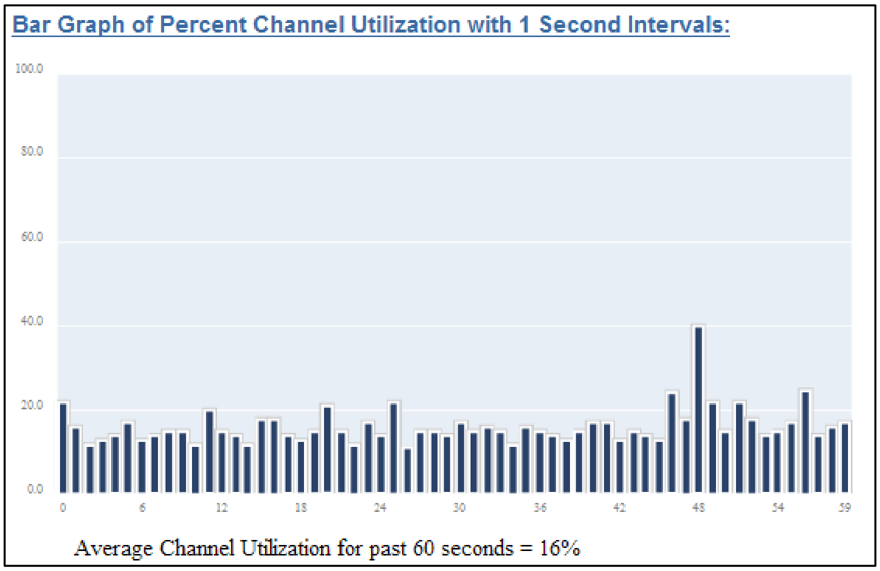
Channel Survey screen displays a graph showing the percentage of time that a channel is being utilised by any of the following causes:

1) The connected modem is transmitting.

2) The connected modem is receiving valid data from another modem.

3) The connected modem has detected RF noise or interference.

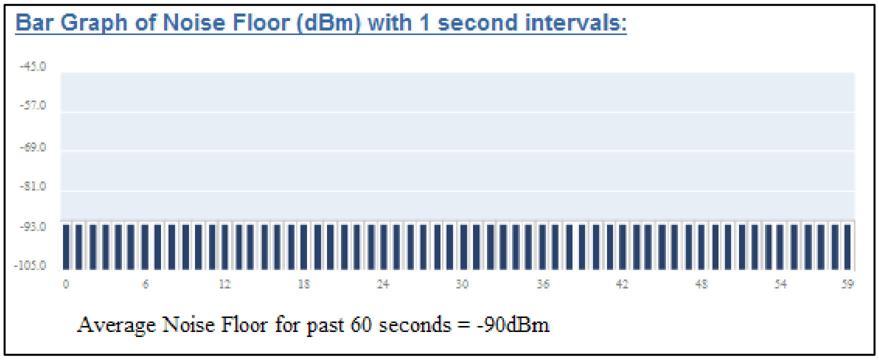
Channel Survey shows the Channel Utilisation and Noise Floor Graph with 1 second, 1 minute and 1 hour periods.



Bar Graph of Percent Channel Utilization with 1 Second Intervals:

Average Channel Utilization for past 60 seconds = 16%

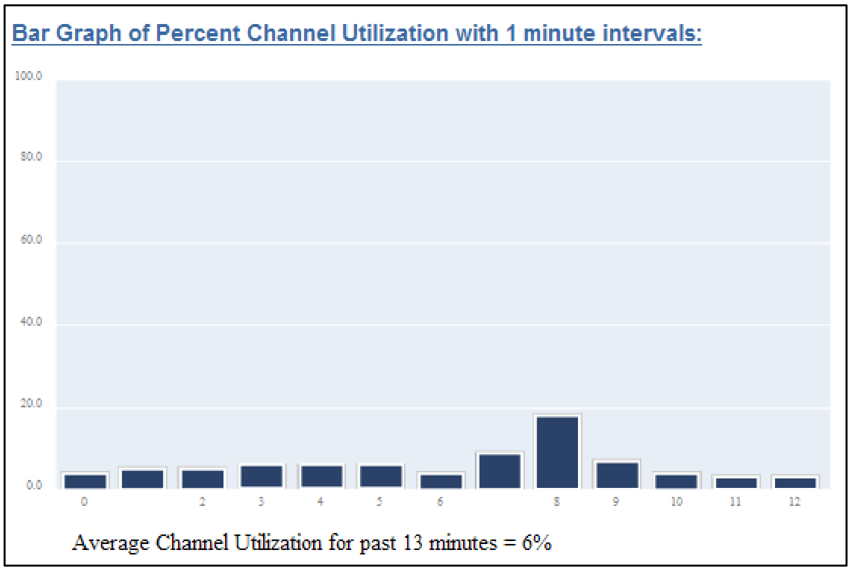
The first screen shows a percent of the overall radio traffic on the channel that is currently being used.



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

Average Noise Floor for past 60 seconds = -90dBm

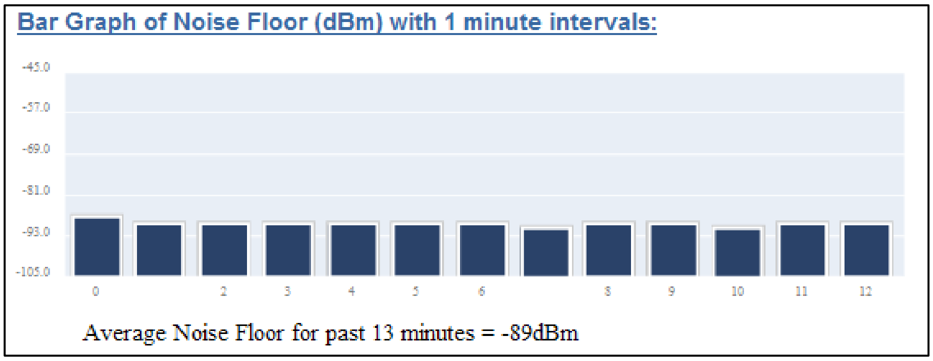
The next screen shot shows the radio receive noise floor for the last 60 seconds.



Bar Graph of Percent Channel Utilization with 1 minute intervals:

Average Channel Utilization for past 13 minutes = 6%

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



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

Average Noise Floor for past 13 minutes = -89dBm

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

The Channel Survey page also shows two other screen shots (not shown here) which indicate the Percent Channel Utilisation and Noise Floor in one hour intervals. The screens will only show the last 24 hour period.

4.3 Custom Survey

Custom Survey is essentially the same as the Channel Survey (explained in the previous section) except the three channel utilizations can be turned on or off thus showing the different amount of traffic related data.

Percent Radio TX – Any transmitted messages from the radio to other devices.

Percent Radio RX – Any DSSS or OFDM messages received by the radio (basically any Standard Wi-Fi data packets from either other equivalent radios or competitor radios).

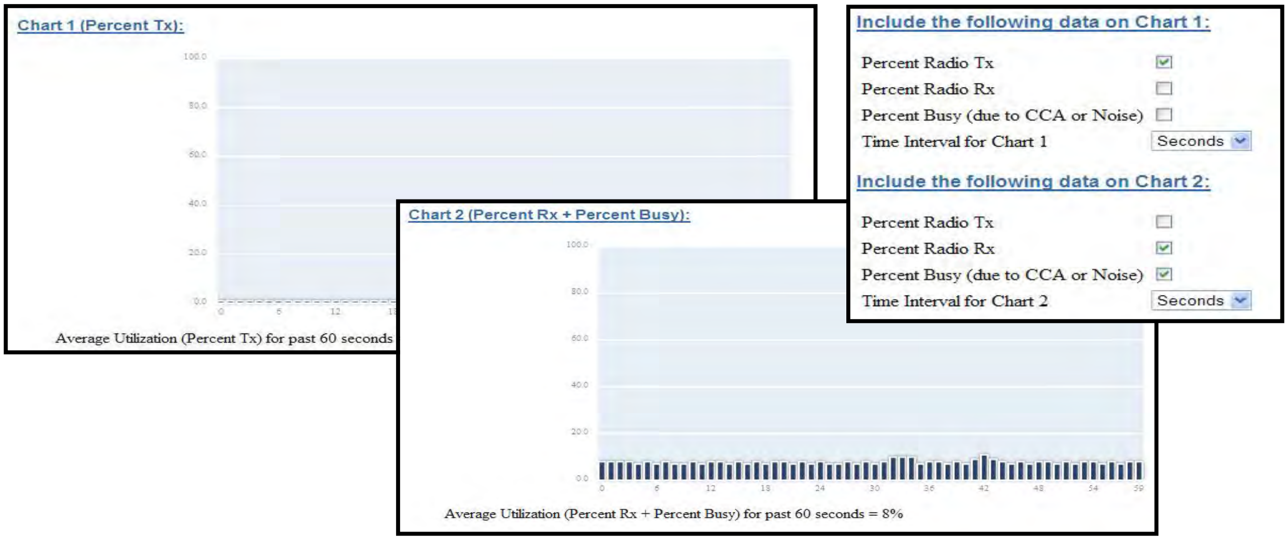
Percent Busy (CCA or Noise) – Clear Channel Assessment is the detection of any ongoing transmissions or noise, i.e. Microwaves, 2.4Ghz FHSS, Cordless Phones, RC devices, etc.

By configuring the different chart options we can get a clear idea of the amount of data being transmitted, received and the amount of other noise that can be heard at the radio.

Configure what is to be logged on each chart, select a time interval and save changes and the charts will then be displayed below the settings. Click the button again to manually redraw the graphs.

Each graph will display a Percent Channel Utilisation using the selected criteria and time interval (Seconds, Minutes or Hours).

Example One.
Chart one shows the amount of data that is being transmitted over a Wi-Fi link and chart two shows the amount of data being received from all sources (Wi-Fi and other noise). We can see from this that there is very little outgoing data but you can see a constant stream of data being received.



Include the following data on Chart 1:

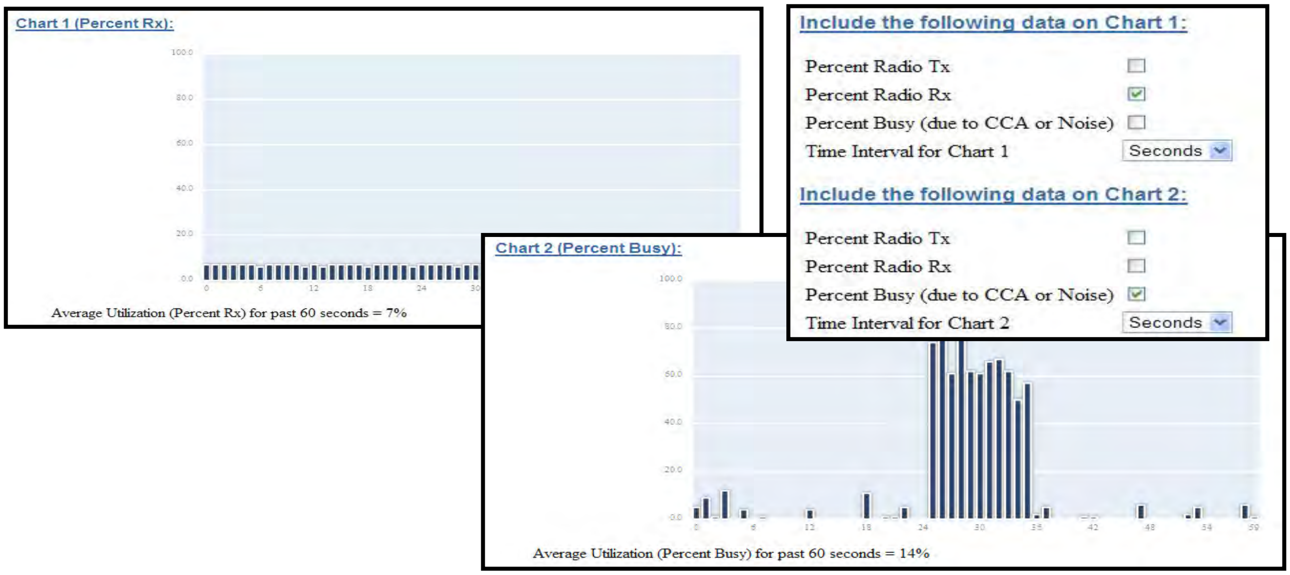
Percent Radio Tx ☑
Percent Radio Rx □
Percent Busy (due to CCA or Noise) □
Time Interval for Chart 1: Seconds

Include the following data on Chart 2:

Percent Radio Tx □
Percent Radio Rx ☑
Percent Busy (due to CCA or Noise) ☑
Time Interval for Chart 2: Seconds

Chart 1 (Percent Tx):
100.0
80.0
60.0
40.0
20.0
0.0
0
6
12
Average Utilization (Percent Tx) for past 60 seconds
Chart 2 (Percent Rx + Percent Busy):
100.0
80.0
60.0
40.0
20.0
0.0
0
6
12
18
24
30
36
42
48
54
59
Average Utilization (Percent Rx + Percent Busy) for past 60 seconds = 8%

Example Two.
In the second example we can see that chart one shows the amount of Data being received from Wi-Fi devices and chart two shows the amount of other noise that is being received. From this you can see that in the last 60 second period there was a 20 second interval with around 60-80 % channel Utilization in this case from a 2.4GHz FHSS telemetry device.



Average Utilization (Percent Rx) for past 60 seconds = 7%

Include the following data on Chart 1:

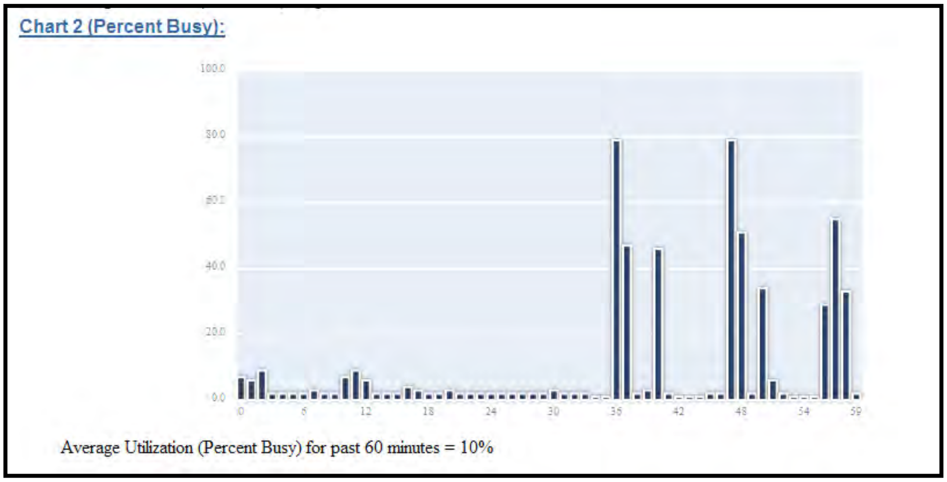
Percent Radio Tx □
Percent Radio Rx ☑
Percent Busy (due to CCA or Noise) □
Time Interval for Chart 1 Seconds

Include the following data on Chart 2:

Percent Radio Tx □
Percent Radio Rx □
Percent Busy (due to CCA or Noise) ☑
Time Interval for Chart 2 Seconds

Average Utilization (Percent Busy) for past 60 seconds = 14%

With this sort of outside interference it is recommended to perform the same test but over a longer period so as to get a clearer indication of channel utilization.



Average Utilization (Percent Busy) for past 60 minutes = 10%

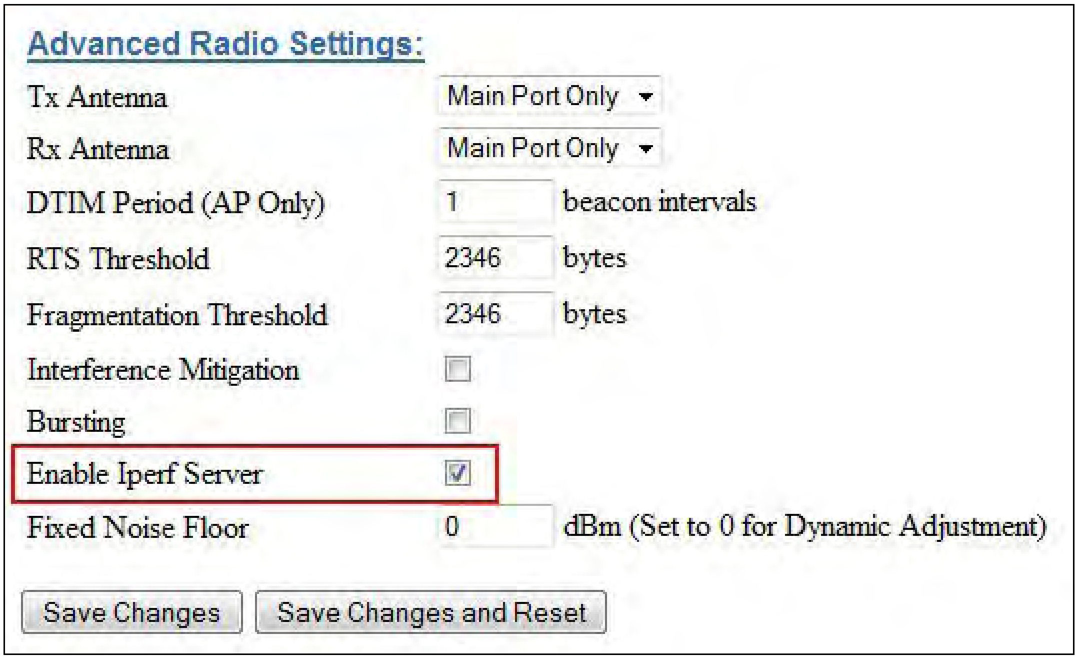
4.4 Throughput Test

The performance of a wireless link is best measured in terms of the maximum throughput that can be achieved. The recommended method of measuring throughput is with the "iperf" utility. Iperf has client and server functionality, where the server waits for a client connection. For wireless links, it is recommended that iperf throughput testing is performed on point to point links while the remainder of the wireless network is inactive (i.e. not sending any data). Iperf is built into the modems for convenience, and allows measurement of TCP throughput with default iperf parameters. For access to all iperf features and a slightly more accurate result due to module processor overheads etc, it is recommended that iperf be run externally on a PC or laptop, see Appendix E "External Iperf Test".

Iperf is built into the modems for convenience, and allows measurement of TCP throughput with default Iperf parameters. The internal Iperf utility always gives a lower result than running Iperf externally because of the additional load placed on the internal microprocessor. Even so, the throughput results still gives an excellent indication of link performance as long as you compare the measured result against the expected result in the table. See Appendix E ―External Iperf Test‖ for details on running this application externally.

Internal Throughput Test

Before testing ensure that the end node of the Wi-Fi Link that you wish to test has the Iperf Server enabled under the Advanced Radio Settings page and Saved to Flash and the module has been reset. See 3.10 ―Advanced Radio Configuration"

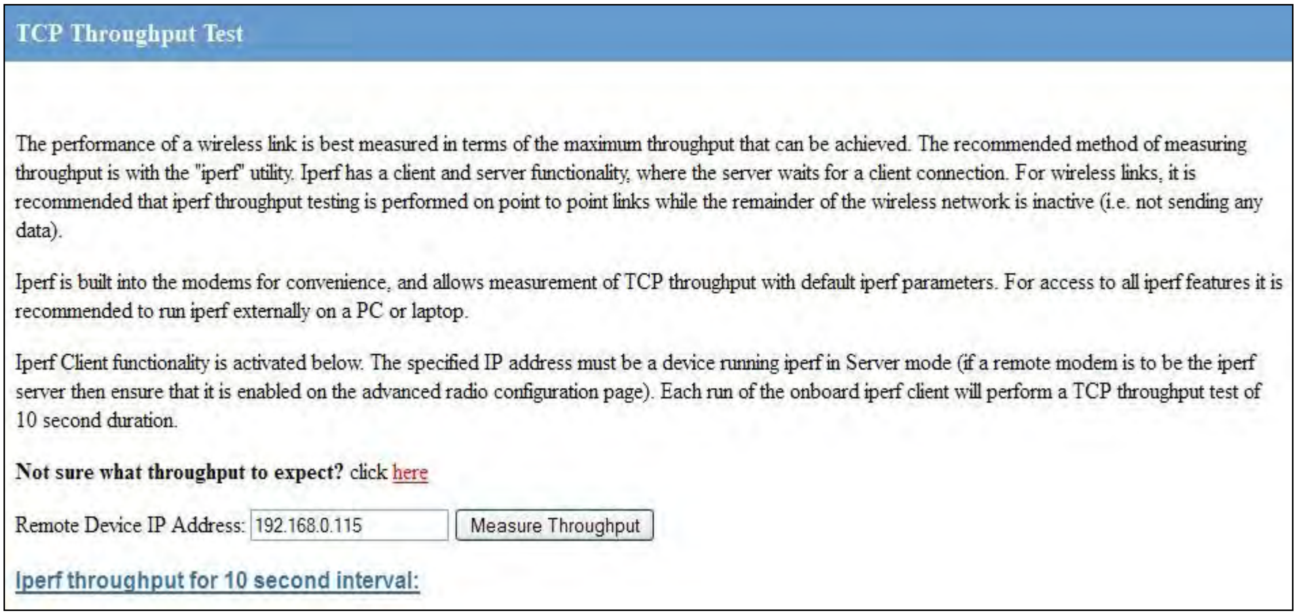


Advanced Radio Settings:

Tx Antenna	Main Port Only	
Rx Antenna	Main Port Only	
DTIM Period (AP Only)	1	beacon intervals
RTS Threshold	2346	bytes
Fragmentation Threshold	2346	bytes
Interference Mitigation	□	
Bursting	□	
Enable Iperf Server	☑	
Fixed Noise Floor	0	dBm (Set to 0 for Dynamic Adjustment)

Figure 2 Advanced Radio Settings

Connect to the web page of the module that will be performing the Iperf test, select "System Tools" link on the right hand side of the webpage and then select "TCP Throughput Test" and you will see the Screen as shown below.



TCP Throughput Test

The performance of a wireless link is best measured in terms of the maximum throughput that can be achieved. The recommended method of measuring throughput is with the "iperf" utility. Iperf has a client and server functionality, where the server waits for a client connection. For wireless links, it is recommended that iperf throughput testing is performed on point to point links while the remainder of the wireless network is inactive (i.e. not sending any data).

Iperf is built into the modems for convenience, and allows measurement of TCP throughput with default iperf parameters. For access to all iperf features it is recommended to run iperf externally on a PC or laptop.

Iperf Client functionality is activated below. The specified IP address must be a device running iperf in Server mode (if a remote modem is to be the iperf server then ensure that it is enabled on the advanced radio configuration page). Each run of the onboard iperf client will perform a TCP throughput test of 10 second duration.

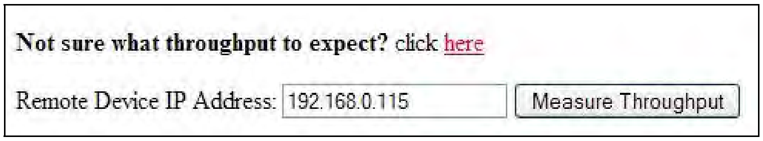
Not sure what throughput to expect? click here

Remote Device IP Address: 192.168.0.115

Iperf throughput for 10 second interval:

Note: TCP Throughput test must be run using Microsoft Internet Explorer 8 or later

Enter the IP address of the remote device that you wish to test and press the “Measure Throughput” button.



Not sure what throughput to expect? click here

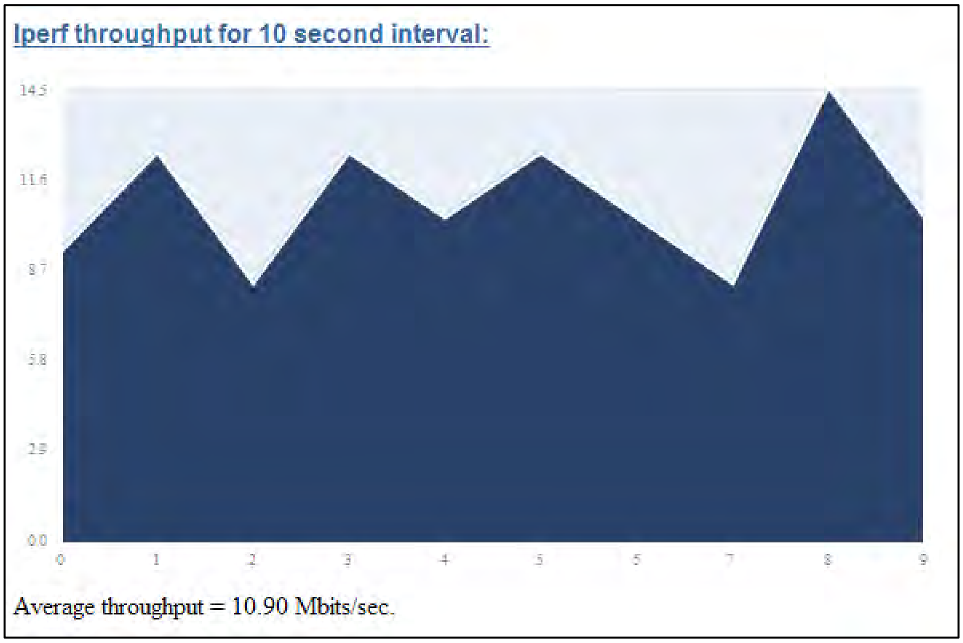
Remote Device IP Address: 192.168.0.115

The specified IP address must be running Iperf in Server mode (if the remote modem does not have the Iperf server running then you will get the following Error message on the web page, “Iperf error, check connectivity to server.” Ensure that it has been enabled and the module has been reset. Each press of the “Measure Throughput” button will perform a TCP throughput test of 10 second duration.

You will see the message “Performing Iperf Test” text and if you look at the modules you will see the TX/Link & RX Led’s flashing very fast as it performs the test. Approximately 10 seconds later a graph showing the actual throughput over the 10 second period and a calculated average will be displayed.

The graph below shows the data throughput range between 8 and 14.5Mbits per second with an overall average of 10.9Mbits per second.

It is recommended to perform this throughput test a number of times to get better sample of the overall throughput.



Iperf throughput for 10 second interval:

Average throughput = 10.90 Mbits/sec.

The expected throughput will depend on a number of things, the distance setting, selected channel width, and whether using the internal Iperf utility or running Iperf externally on a laptop or PC (at both ends of the link).

The following table shows real world throughput estimates based on channel selection and receiver signal levels. Throughput is calculated using the inbuilt ―Iperf ‖ utility and communicating TCP/IP over the three different bandwidth channels (20M, 10M, & 5M). These estimates are not necessarily the maximum that are achievable in the modems but are used more as a guideline to determine the performance of the radio link.

See Appendix E for details on using the external Iperf throughput test.

The Iperf throughput result provides an excellent measure of the performance of a radio link. In general, if the results you get are a lot worse than the best case values listed below, this is a certain indication that the radio link has either poor RSSI, or high noise or interference, or both.

XYR401-E Radio Data Throughput				
Distance	**Iperf**	**20MHz**	**10MHz**	**5MHz**
1000m	Internal	10.5 Mbps	7.5 Mbps	5. Mbps
1000m	External	16. Mbps	10.5 Mbps	6. Mbps
3000m	Internal	10. Mbps	7. Mbps	4.7 Mbps
3000m	External	15. Mbps	9. Mbps	6. Mbps
5000m	Internal	9. Mbps	6. Mbps	4.5 Mbps
5000m	External	13. Mbps	8. Mbps	6. Mbps
10000m	Internal	7. Mbps	5. Mbps	4. Mbps
10000m	External	10. Mbps	7. Mbps	5. Mbps

Throughput and Repeaters

It should also be noted that if using repeaters to extend the range there will be a reduction in throughput for each repeater hop.

The following table shows the drop in throughput for each hop and for each of the channel widths.

Rep Hops	**Rep Hops**	**1**	**2**	**3**	**4**	**1**	**2**	**3**	**4**	**1**	**2**	**3**	**4**
Signal	**Signal**	**20 MHz Channel**				**10 MHz Channel**				**5 MHz Channel**			
1000m	Internal	10.5	5.3	2.6	1.3	7.5	3.8	1.9	0.9	5.0	2.5	1.3	0.6
1000m	External	16	8.0	4.0	2.0	10.5	5.3	2.6	1.3	6.0	3.0	1.5	0.8
3000m	Internal	10	5.0	2.5	1.3	7	3.5	1.8	0.9	4.7	2.4	1.2	0.6
3000m	External	15	7.5	3.8	1.9	9	4.5	2.3	1.1	6.0	3.0	1.5	0.8
5000m	Internal	9.0	4.5	2.3	1.1	6	3.0	1.5	0.8	4.5	2.3	1.1	0.6
5000m	External	13	6.5	3.3	1.6	8	4.0	2.0	1.0	6.0	3.0	1.5	0.8
10000m	Internal	7.0	3.5	1.8	0.9	5	2.5	1.3	0.6	4.0	2.0	1.0	0.5
10000m	External	10	5.0	2.5	1.3	7	3.5	1.8	0.9	5.0	2.5	1.3	0.6

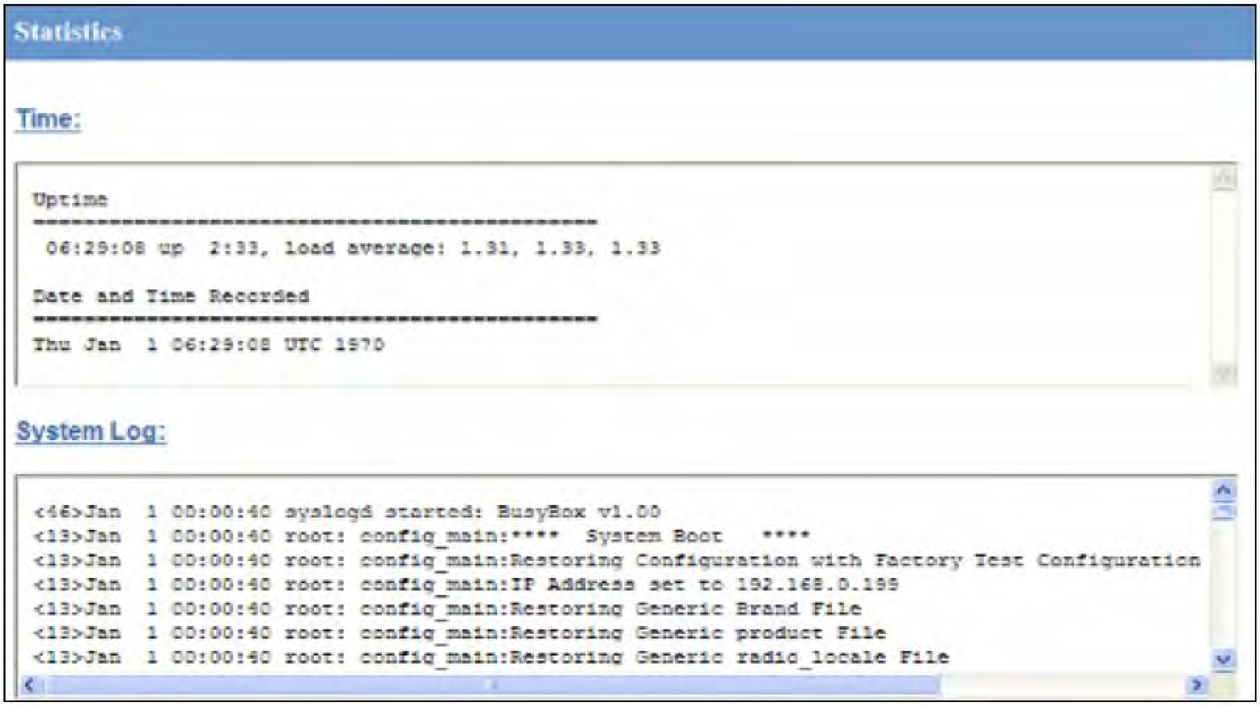
The 40MHz Turbo channels rarely give a better throughput than the 20MHz in real world because it occupies a larger portion of the 2.4GHz band and is more prone to interference.

For RSSI or Received Signal Strength Indication see section 4.1 “Connectivity”

For information on checking interference or noise see section 4.2 —Channel Survey”

4.5 Statistics

The Statistics webpage is used for advanced debugging of XYR401-E. This webpage details the state of the XYR301-E and performance information. This page is typically useful to HONEYWELL technical support personnel in diagnosing problems with the module.
Note that when updating the Statistics webpage, it is necessary to hold down the <ctrl> key while pressing the refresh button. Otherwise, the information will not be updated.



Statistics

Time:

```
Uptime
----------------------------------------------
 06:29:08 up  2:33, load average: 1.31, 1.33, 1.33

Date and Time Recorded
----------------------------------------------
Thu Jan  1 06:29:08 UTC 1970
```

System Log:

```
<46>Jan  1 00:00:40 syslogd started: BusyBox v1.00
<13>Jan  1 00:00:40 root: config_main:****  System Boot   ****
<13>Jan  1 00:00:40 root: config_main:Restoring Configuration with Factory Test Configuration
<13>Jan  1 00:00:40 root: config_main:IP Address set to 192.168.0.195
<13>Jan  1 00:00:40 root: config_main:Restoring Generic Brand File
<13>Jan  1 00:00:40 root: config_main:Restoring Generic product File
<13>Jan  1 00:00:40 root: config_main:Restoring Generic radio_locale File
```

Wireless Statistics

The —Wireless Statistics” is the main area for further diagnostics statistics.

The list of statistics produced is dynamic and may vary depending on the model and configuration, i.e. 2.4.GHz, 5GHz or 900MHz & Client or Access Point.

Access Point:

Beacon Miss Count: Number of Beacons unable to be sent (100msec intervals) due to Interference or CCA

Beacon Missed Reset Count: After 15 Consecutive Beacon misses (1.5seconds) will increment by 1. This will indicate high interference as AP is holding off sending Beacon and Utilisation will increase.

TX Queue stopped because full: Message buffer (Ethernet Frames) in radio queue. If Radio cannot transmit due to high noise, this will increment. When the buffer is full all new messages are dropped. Buffer size 150 messages.

Client:

Beacon Missed Interrupts: How many beacons (100msec) the Client has missed from the Access Point

X Failed due to too many retries: This is how many frames that have been lost. Original Message + 7 Retries = 1 TX Failed due to too many retires. Each retry is sent within a few msec.

TX Failed / TX Antenna Profile = Frame Packet Loss Rate (How many undelivered as a %)

RX Failed due to bad CRC: This can be from any AP not only your own. If other Wi-Fi is around then this number could be high due to other Encryption keys, weak signal etc.

RX Failed / RX Antenna Profile = RX Frame Error Rate (Note this can be high due to other wireless devices around.)

Broadcast Notes: When Broadcast message is sent from CL – AP the AP will always ACK the Client. When Broadcast Message is sent from AP – CL no ACK will be sent back.

Management Frames: Can be probes, Authenticate/ Associate messages, RTS Messages, Beacons, etc

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 XYR401-E a simple task.

4.6 System Tools

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

Configuration Summary	This option is used to save all the different configuration pages onto one page, for easy viewing. Page can also be saved (using the File/Save As function on the drop File Menu) for future reference and emailing module configuration details to Technical Support in the event of any configuration problems.
TCP Throughput Test	Performs a Throughput Test. See section 4.4"Throughput Test" above for details
Radio Path Test	Perform a Radio Path test without the use of a Laptop and get a visual indication of RSSI and Throughput on the front panel LEDs.
Read Configuration File	This option will show the module configuration in XML format. This file can be saved for future reference.
Write Configuration File	Any configuration XML files saved using the —Read Configuration" above can be loaded back into the module
Firmware Upgrade	This option is used for firmware upgrades. Load the file using the —Browse" button and when found press —Send" which will load the file into the module. When completed press —Reset" Firmware upgrade can be done locally or remotely via the radio.
System Log File	Shows an event log of the modules operation, used for diagnosing problems. Page can be saved and emailed to ELPRO if requested. —Clear System Log" will clear out the log file and start fresh.
Reset	Resets the module
Factory Default Configuration	Loads the Factory default configuration and resets. CAUTION – Doing this will overwrite any current configuration

System Tools

4.7 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.
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 analysed, and traffic is sent between the units whilst remote WebPages are opened.

Iperf Throughput Test

A more thorough test is to perform a throughput test which will check the amount of data that can be reliably achieved via the Wireless link. There are a number of software tools that we can use to check the data throughput, i.e. FTP - file transfer protocol, Iperf, Qcheck, etc.

The preferred application is —Iperf” which has been configured in each modem and can be enabled to perform this test. It can also be run externally using Laptops at either end of the radio link. The preferred application is “Iperf” which can be downloaded from http://sourceforge.net/projects/iperf/

All of the above applications measure the raw data throughput and from this we can determine the amount of interference from the measured and calculated data throughput levels.

The way —iPerf” works is a Server is enabled at one end of the link and a Client at the other. The —iPerf” Client will then pass data over the link and calculate and display the throughput accordingly.

—iPerf” server can be run internally on the modem by enabling this feature on the Advanced Radio page of one of the modems, see section 4.4 —Throughput Test”. It can also be run externally on a PC or laptop connected at each end of the radio link. See Appendix E —External Iperf Test” for a detailed procedure on how to use Iperf to externally check radio data throughput.

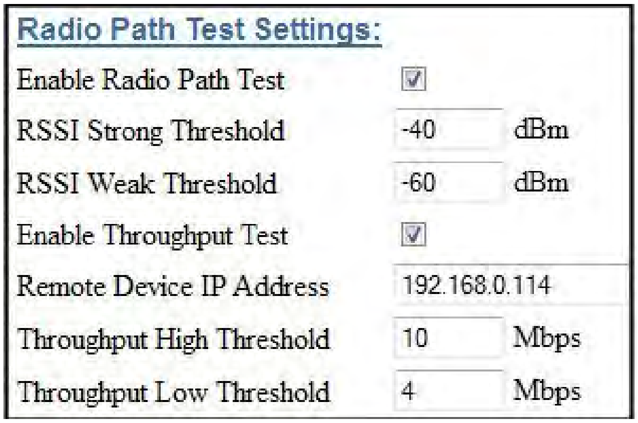
The internal —iPerf” is a basic cut down version of the standard —iPerf” and should be used as a guide only. For a more comprehensive test —iPerf” should be run externally using Laptops or PCs at each end of the Wi-Fi link.

Internal Radio Test

The module also has an internal Radio Path test that will allow you to perform a basic radio path test without the need for a laptop or PC.

There are two tests that can be run, RSSI and Throughput; Throughput can be disabled independently from RSSI however disabling RSSI test will turn off both tests.

Typically, the Radio Path Test should be enabled at a modem configured as a Client/Station.



Radio Path Test Settings:

Enable Radio Path Test	☑	
RSSI Strong Threshold	-40	dBm
RSSI Weak Threshold	-60	dBm
Enable Throughput Test	☑	
Remote Device IP Address	192.168.0.114	
Throughput High Threshold	10	Mbps
Throughput Low Threshold	4	Mbps

The Radio Path Test feature should not be enabled on a live system; it is intended for testing only.

Radio Path Test Settings	
Enable Radio Path Test	Enables or disables the Radio Path Test.
RSSI Strong Threshold	Strong RSSI indication threshold
RSSI Weak Threshold	Weak RSSI indication threshold
Enable Throughput Test	Enables or disables the Throughput test (independent of Radio Path Test (RSSI)
Remote Device IP Address	IP Address of the Remote device that you wish to path test
Throughput High Threshold	High Throughput indication value. Generally configured with the desired throughput level
Throughput Low Threshold	Low Throughput indication value.

RSSI

The first test uses the RS232, LED to indicate the RSSI level from the Access Point. The LED will be green when the RSSI to the Access Point is greater than the configured RSSI Strong Threshold or red when the RSSI to the AP is greater than the configured RSSI Weak Threshold. If the RSSI to the AP is less than the RSSI Weak Threshold then the RS232 LED will be off.
When the Radio Path Test is enabled, the OK LED will flash alternately between green and red indicating that it is in a diagnostic mode.

Throughput

The second test is the Throughput Test which when enabled performs a basic throughput test between the AP and Client. The configurable Remote Device IP Address should specify the IP Address of the AP

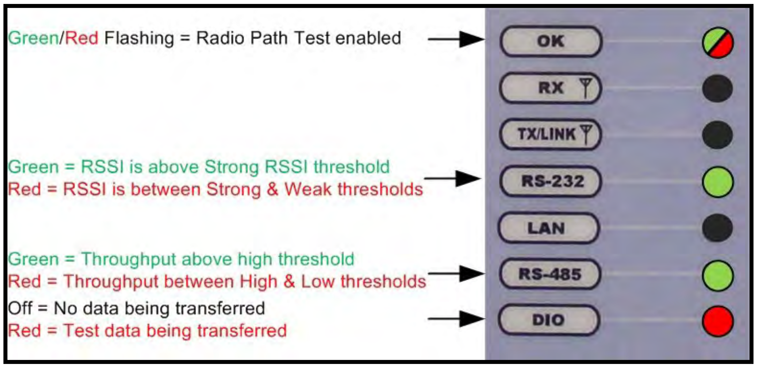
(Note that the on-board iperf server must be enabled at the AP prior to running this test).

The Throughput Test will run through a continuous cycle where data is transferred for 10 seconds, followed by 10 seconds of silence. The RS485 LED and the DIO LED are used as indicators of the throughput test. While data is being transferred the DIO LED will be red, and while no data is being transferred the DIO LED will be off.

If the average throughput over the 10 second duration of the throughput test is greater than the configurable Throughput High Threshold, then the RS485 LED will be green; otherwise if the throughput is greater than the configurable Throughput Low Threshold then the RS485 LED will be red; if the measured throughput is less than the Throughput Low Threshold then the RS485 LED will be off.

Radio Path Test can be accesses by selecting the link from the —System Tools‖ page and then ticking the —Enable Radio Path Test‖ and entering in appropriate thresholds levels to indicate RSSI and Throughput and the IP address of the Iperf Server (normally the Access Point).

The following screen shot shows the indications you will see using the Configuration above.


Green/Red Flashing = Radio Path Test enabled
Green = RSSI is above Strong RSSI threshold
Red = RSSI is between Strong & Weak thresholds
Green = Throughput above high threshold
Red = Throughput between High & Low thresholds
Off = No data being transferred
Red = Test data being transferred
OK
RX
TX/LINK
RS-232
LAN
RS-485
DIO

The OK Led will flash between Red and Green which indicates the module is in a diagnostic Radio Test Mode.

RS-232 Led is showing a green indication which means the RSSI to the Access Point is greater than -40dB. If the RS232 Led showed Red it would indicate the RSSI level was greater than -60dB.

RS-485 Led is showing a green indication which means the Throughput to the Access Point is greater than 10 Mbps. If the Led showed a Red indication this would mean the throughput is between 10Mbps & 4 Mbps.

Radio Path Test can be accesses by selecting the link from the —System Tools‖ page and then ticking the —Enable

Radio Path Test ‖ and entering in appropriate thresholds levels to indicate RSSI and Throughput.
Note: Advanced configuration settings such as Serial or I/O Transfer should be disabled and if using the Throughput Test, Iperf Server in the Advanced Radio Settings page on the Access Point must be enabled.

4.8 Remote Configuration

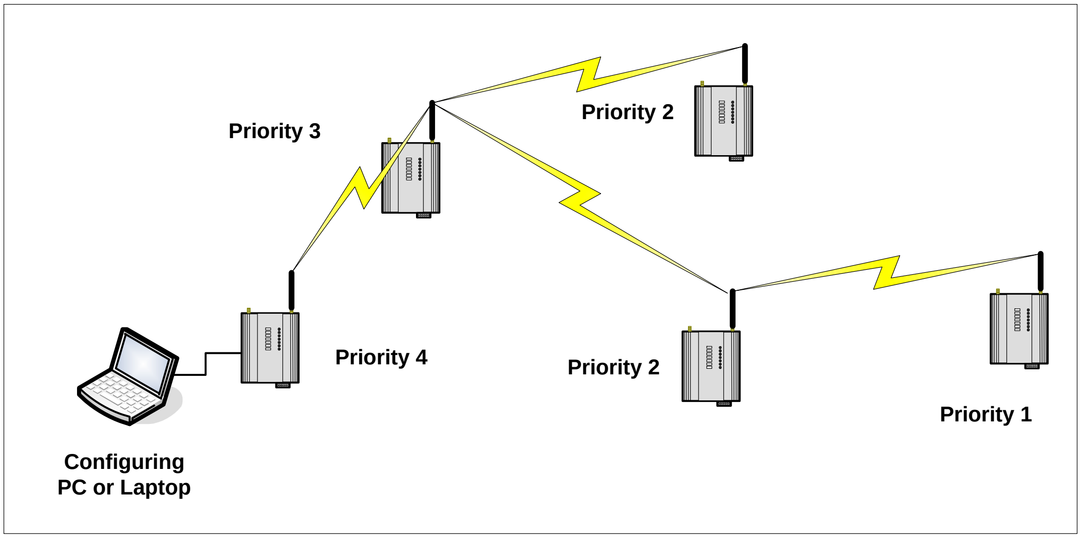
Because a module configuration is viewed and changed in a web format (which uses TCP/IP protocol), you can view or change the configuration of a remote module via the wireless link, provided the remote module already have a wireless link established to the local XYR401-E.

To perform remote configuration, connect a PC to the local module, run Internet Explorer and enter the IP address of the remote unit (or device name if using DNS) - the configuration page of the remote module will be shown and changes can be made.

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 the 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.



Remote Configuration Priority

4.9 Internal Diagnostics Modbus Registers

There are a number of internal diagnostic registers that can be accessed via Modbus TCP/RTU that will help with analysing and diagnosing the radio network. To access these register the Modbus Server will need to be enabled and a Modbus Server address will need to be configured (See **Error! Reference source not found.** "Modbus I/O Transfer" for details on how this is done).

After enabling the Modbus Client you can then access the following information by reading the corresponding Modbus Address at the Server ID address.

Note: „wi0" is the normal default interface. If more interfaces are added by entering in virtual WDS connections (either Client or AP) in section 3.17"Repeaters (WDS)" then they will take on the next available interface number i.e. wi1, wi2, etc

Register	Module	Description
5000	Both	Total number Associated Stations
5001	Both	Current Radio Channel. See section 3.6 "Radio Configuration" for channel details
5002	Both	Number Wireless Interfaces configured, includes Virtual Interfaces – wi1-wi10
5010	Both	Wireless Adaptor (wi0) - Link Status
5011	Both	Wireless Adaptor (wi0) - Link Status Inverted
5012	Both	Wireless Adaptor (wi0) - Number Associated Stations for this interface
5013	AP Only	Wireless Adaptor (wi0) - Points to the starting register of the AP's Station List. First interface (wi0) will always start at 5200 and dynamically enter data depending on the number of STA's. Remaining interfaces (wi1-wi10) will be entered after wi0 data.
5014	STA Only	Wireless Adaptor (wi0) – RSSI & BGND of Rx message from AP e.g. Hex 5F5D = 5F for RSSI and 5D for BGND (Convert value from hex to dec and add a "-" e.g. 5F = -95dB)
5015	STA Only	Wireless Adaptor (wi0) - Transmit Data Rate from the Access Point
5016	STA Only	Wireless Adaptor (wi0) - MAC Address of the Access Point
5020-5026	As per 5010-5016	As per registers 5010-5016 but for the next Wireless Adaptor (wi1)
5030-5036	As per 5010-5016	As per registers 5010-5016 but for the next Wireless Adaptor (wi2)
5040-5046	As per 5010-5016	As per registers 5010-5016 but for the next Wireless Adaptor (wi3)
……etc	As per 5010-5016	As per registers 5010-5016 but for the next Wireless Adaptor (wi10)
5200	AP Only	RSSI of the Client (STA)
5201	AP Only	Transmit Data Rate to Client (STA)
5202	AP Only	MAC address of Client (STA)
…..etc	AP Only	Dynamic list of STA's Refer to register 5023, 5033, etc for starting register of each wi interface
9999	Both	Reset module (enter FFFF to reset module)

Table Continued

Statistic Registers	Module	Description
4500	Both	Total data packets received on the interface
4502	Both	Received frames with antenna 1 (TX/RX)
4504	Both	Received frames with antenna 2 (RX)
4506	Both	Receiver / default antenna switches
4508	Both	Receive message failed due to bad CRC
4510	Both	Receive message failed due to decryption
4512	Both	Receive message failed due to MIC failure
4514	Both	Receive message failed due to FIFO overrun
4516	Both	Beacon missed interrupts
4518	Both	Total data packet sent on the interface
4520	Both	Transmit frames with antenna 1 (TX/RX)
4522	Both	Transmit frames with antenna 2 (RX)
4524	Both	Transmitter antenna switches
4526	Both	Transmitter on-chip retries
4528	Both	Transmit message failed due to too many retries
4530	Both	Transmit frames with alternate rate
4532	Both	Transmit frames with no ack marked (i.e. broadcast, multicast)
4534	Both	Management frames transmitted
4536	Both	Transmit frames with rts enabled
4538	Both	Transmit frames with cts enabled
4540	Both	Beacons transmitted
4542	Both	Beacon missed count
4544	Both	Beacon miss reset count
4546	Both	Transmit message failed due to no tx buffer (data)
4548	Both	Fatal hardware error interrupts
4550	Both	Receiver PHY error summary count
4552	Both	Transmitter queue stopped because it's full

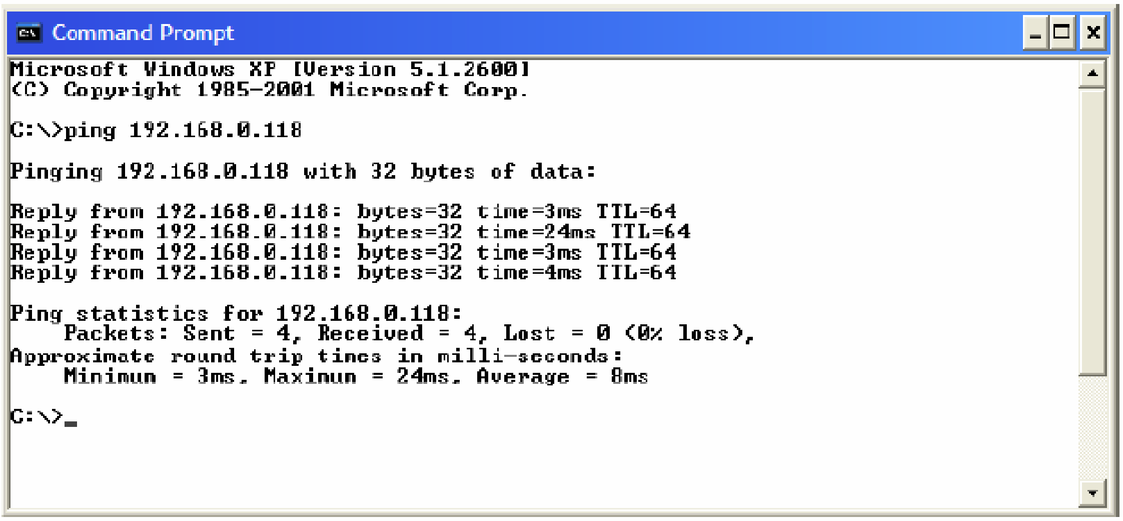
4.10 Utilities

"Ping"

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

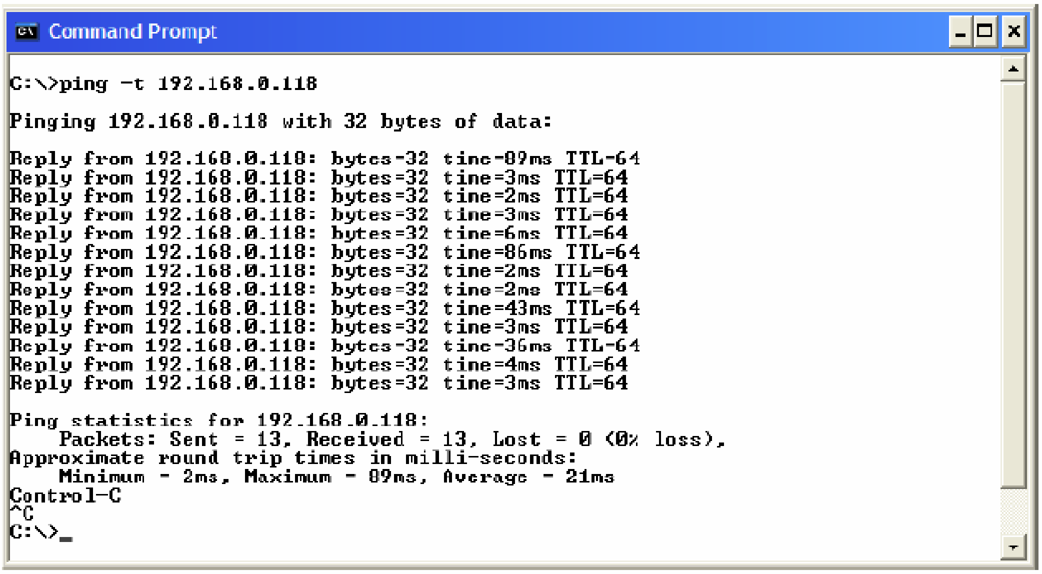
Click on the Start Menu and select Run. Type in "cmd" and enter, you should then see the command screen come up. There will be a certain directory specified (unique to your own PC) with a flashing cursor at the end. At the cursor type the word "ping" leaving a space and the default IP address for the XYR401-E at first start-up.

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 XYR401-E is correctly configured your reply will look something like this.



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

C:\>ping 192.168.0.118

Pinging 192.168.0.118 with 32 bytes of data:

Reply from 192.168.0.118: bytes=32 time=3ms TTL=64
Reply from 192.168.0.118: bytes=32 time=24ms TTL=64
Reply from 192.168.0.118: bytes=32 time=3ms TTL=64
Reply from 192.168.0.118: bytes=32 time=4ms TTL=64

Ping statistics for 192.168.0.118:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 24ms, Average = 8ms

C:\>_
```

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



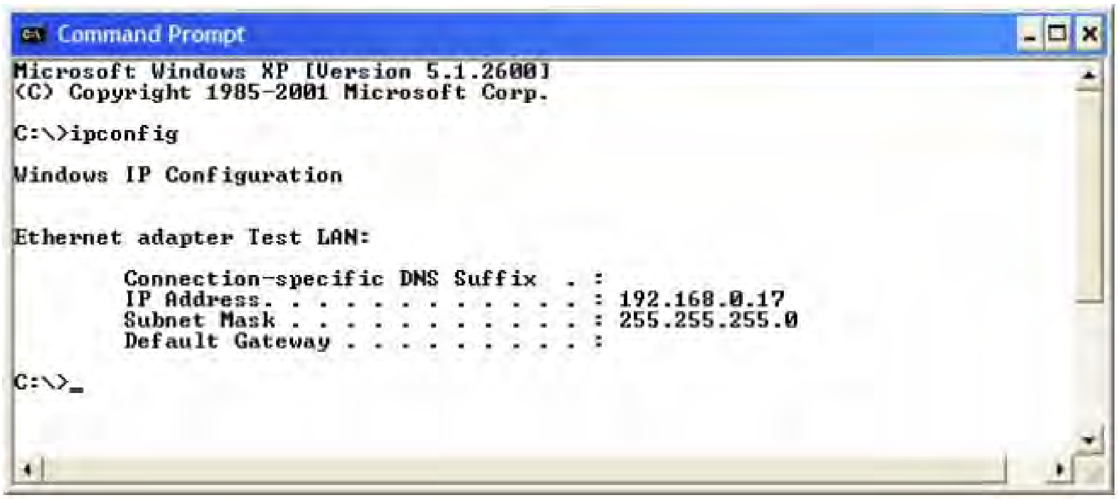
```
C:\>ping -t 192.168.0.118

Pinging 192.168.0.118 with 32 bytes of data:

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

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

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

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

”Ipconfig”

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



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

C:\>ipconfig

Windows IP Configuration


Ethernet adapter Test LAN:

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

C:\>_
```

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

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

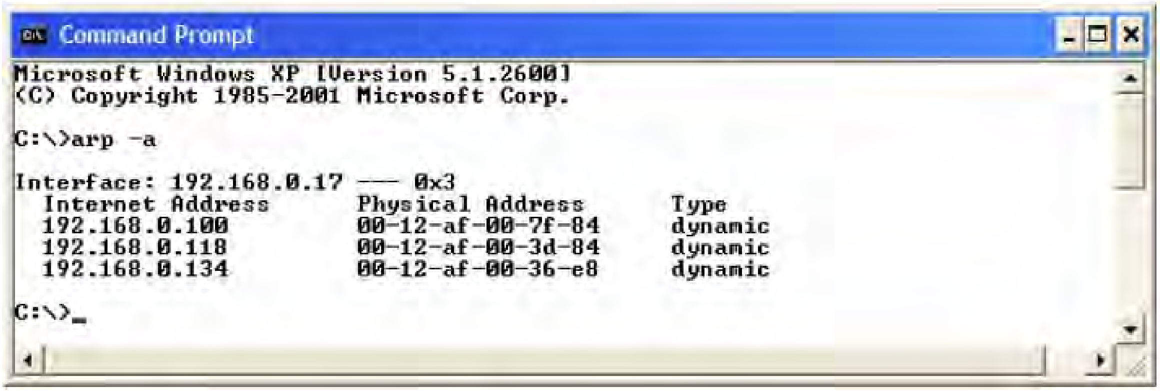
Ipconfig /? lists all of the commands and their usages available for use.

“Arp”

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

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

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.

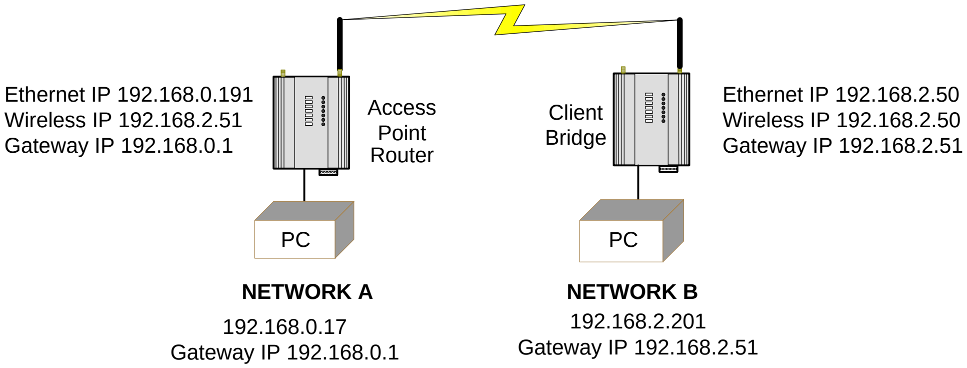


```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\>arp -a

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

C:\>_
```

”Route”

Route is used for the Router function. This is where you are joining 2 different networks together via the XYR401-E *refer to Section 1)*
The XYR401-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	Client Bridge Settings
IP Address 192.168.0.17	Gateway IP 192.168.2.51
Subnet Mask 255.255.255.0	Ethernet IP 192.168.2.50
Gateway IP 192.168.0.1	Subnet Mask 255.255.255.0
	Wireless IP 192.168.2.50
	Subnet Mask 255.255.255.0

Access Point Router Settings	Network B Settings
Gateway IP 192.168.0.1	IP Address 192.168.2.201
Ethernet IP 192.168.0.191	Subnet Mask 255.255.255.0
Subnet Mask 255.255.255.0	Gateway IP 192.168.2.51
Wireless IP 192.168.2.051	
Subnet Mask 255.255.255.0	

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 3.0.

Chapter Five SPECIFICATIONS

General		
EMC specification	EN 300 683	FCC Part 90
Radio specification	EN 300 328	FCC Part 15.247, RSS 210
Housing	114 x 140 x 30mm, 4.5 x 5.5 x 1.2 inch	Powder-coated, extruded aluminium DIN rail mount
Terminal blocks	Removable	Suitable for 12 gauge (2.5mm^2) conductors
LED indication	Module Status, Serial RX and TX, Radio RX and TX, Radio Link, Ethernet Activity / Link	
Operating Temperature	-40 to +60°C, -40 to +140 F	0 – 99% RH non-condensing
Power Supply		
Nominal supply	9 to 30VDC	Overvoltage and reverse voltage protected
Average current drain	XYR401-E = 290 mA @ 12V	XYR401-E = 150mA @ 24VDC
Current drain when transmitting (400mW)	XYR401-E = 340 mA @ 12V	XYR401-E = 180mA @ 24VDC
Ethernet Port	10/100 BaseT	RJ45
Standard	IEEE 802.3 compliant	Bridge/router, Access point/ client functionality
Radio Transceiver		
Transmit power	Model	Maximum Power
(Power may be limited by country specific configuration)	XYR401-E	1-24 Mb/s: 400mW (+26 dBm) 36 Mb/s: 250mW(+24 dBm) 48 Mb/s: 160mW(+22 dBm) 54 Mb/s: 125mW(+21 dBm)
Channels 2.4 GHz	13 x 5MHz Spacing	First channel centre at 2.412 GHz
Channels 5 GHz	12 fixed channels (3 Turbo Mode) or Auto Channel/Group selection	Auto Channel/Group selection utilises DFS depending on Group selection
Receiver sensitivity	Model	Receiver Sensitivity
(8% FER)	XYR401-E	-97dBm @ 1Mb/s, -94dBm @ 6Mb/s, -90dBm @ 18Mb/s, -74dBm @ 54Mb/s
Antenna Connector	x Female SMA coaxial	Two connectors for signal diversity or High gain receive antenna.
Wireless data rate – configurable	1 to 54Mb/s (XYR401-E), Turbo – 108Mb/s	“Auto” function determines fastest rate possible
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	7 or 8 data bits, Stop/start/parity bits configurable
System Parameters		
System address (ESSID)	1 to 31 character text string	
Maximum # Clients per AP	127 clients per Access Point	
Wireless data encryption	WEP (64bit and 128bit), WPA-PSK (TKIP), WPA-PSK (AES), WPA2-PSK(AES), WPA-PSK/WPA2-PSK, WPA Enterprise (EAP method - PEAP / MSCHAPv2)	
User Configuration	Via embedded web page via RS232 commands	
Diagnostics LED’s	Power / OK, Ethernet Link, Activity, 100mb/s, Radio Link, RX, Rx Weak Signal, TX, Serial RX/TX, Digital I/O Input / Output status	

Other	RSSI measurement in dBm Connectivity Information System Log file

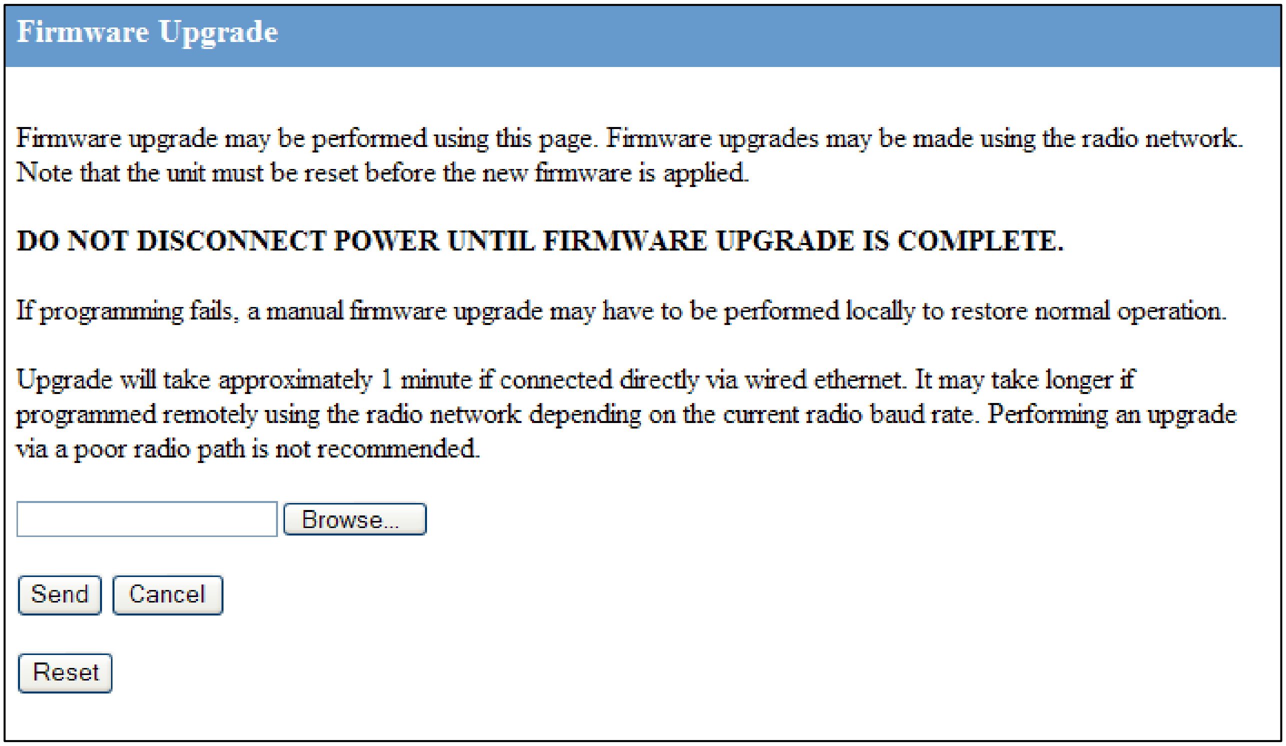
Appendix A FIRMWARE UPGRADE

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

Firmware versions 1.0.3 and later may be upgraded via the configuration web pages. This upgrade can be done locally with a PC connected directly to the module, or remotely over a working radio link. For remote upgrade, 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.

Web based Upgrade

Web based firmware upgrade is available from the System tools page by selecting "firmware upgrade". Firmware upgrade is performed by uploading a "patch" file which is specific to the currently installed firmware version. If the device firmware version has fallen multiple versions behind the desired version, it may be necessary to upload multiple "patch" files. Once the patch files are uploaded, reset the module to perform the firmware upgrade. You will receive more detailed instructions if it is necessary to upgrade the module firmware.



Firmware Upgrade

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

DO NOT DISCONNECT POWER UNTIL FIRMWARE UPGRADE IS COMPLETE.

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

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

Appendix B GLOSSARY

ACK	Acknowledgment.
Access Point	An access point connects wireless network stations (or clients) to other stations within the wireless network and also can serve as the point of interconnection between the wireless network and a wired network. Each access point can serve multiple users within a defined network area. Also known as a base station.
Antenna Gain	Antennae don't increase the transmission power, but focus the signal more. So instead of transmitting in every direction (including the sky and ground) antenna focus the signal usually either more horizontally or in one particular direction. This gain is measured in decibels
Bandwidth	The maximum data transfer speed available to a user through a network"".
Bridge	A bridge is used to connect two local area networks together. Bridges are typically used to connect wireless networks to wired networks. Typically, bridges will transfer messages between networks only when the message destination is on the other network. Messages that are destined for the same network as they originated on are not passed to the other network, therefore reducing traffic on the entire network.
Collision avoidance	A network node procedure for proactively detecting that it can transmit a signal without risking a collision with transmissions from other network nodes.
Client / Sta / Station	A device on a network that gains access to data, information, and other devices through a Server (Access Point).
Crossover cable	A special cable used for networking two computers without the use of a hub. Crossover cables may also be required for connecting a cable or DSL modem to a wireless gateway or access point. The cable is wired so that the signals "crossover", connecting transmit signal on one side to receiver signals on the other.
CSMA/CA	Carrier Sense Multiple Access/Collision Avoidance is a "listen before talk" method of minimizing (but not eliminating) collisions caused by simultaneous transmission by multiple radios. IEEE 802.11 states collision avoidance method rather than collision detection must be used, because the standard employs half duplex radios—radios capable of transmission or reception—but not both simultaneously. Unlike conventional wired Ethernet nodes, a WLAN station cannot detect a collision while transmitting. If a collision occurs, the transmitting station will not receive an ACKnowledge packet from the intended receive station. For this reason, ACK packets have a higher priority than all other network traffic. After completion of a data transmission, the receive station will begin transmission of the ACK packet before any other node can begin transmitting a new data packet. All other stations must wait a longer pseudo randomized period of time before transmitting. If an ACK packet is not received, the transmitting station will wait for a subsequent opportunity to retry transmission.
CSMA/CD	Carrier Sense Multiple Access/Collision Detection is the access method used on an Ethernet network. A network device transmits data after detecting that a channel is available. However, if two devices transmit data simultaneously, the sending devices detect a collision and retransmit after a random time delay.
DHCP	Dynamic Host Configuration Protocol A utility that enables a server to dynamically assign IP addresses from a predefined list and limit their time of use so that they can be reassigned. Without DHCP, an IT Manager would have to manually enter in all the IP addresses of all the computers on the network. When DHCP is used, whenever a computer logs onto the network, it automatically gets an IP address assigned to it.
Dial-up	A communication connection via the standard telephone network, or Plain Old Telephone Service (POTS).
DNS	Domain Name Service A program that translates URLs to IP addresses by accessing a database maintained on a collection of Internet servers. The program works behind the scenes to facilitate surfing the Web with alpha versus numeric addresses. A DNS server converts a name like mywebsite.com to a series of numbers like 107.22.55.26. Every website has its own specific IP address on the Internet.
DSL	Digital Subscriber Line Various technology protocols for high-speed data, voice and video transmission over ordinary twisted-pair copper POTS (Plain Old Telephone Service) telephone wires.

Encryption key	An alphanumeric (letters and/or numbers) series that enables data to be encrypted and then decrypted so it can be safely shared among members of a network. WEP uses an encryption key that automatically encrypts outgoing wireless data. On the receiving side, the same encryption key enables the computer to automatically decrypt the information so it can be read. Encryption keys should be kept secret
Firewall	A device or computer program that keeps unauthorized users out of a private network. Everything entering or leaving a system's internal network passes through the firewall and must meet the system's security standards in order to be transmitted. Often used to keep unauthorized people from using systems connected to the Internet.
Hub	A multiport device used to connect PCs to a network via Ethernet cabling or via 802.11. Wired hubs can have numerous ports and can transmit data at speeds ranging from 10 Mbps to multi-Gigabyte speeds per second. A hub transmits packets it receives to all the connected ports. A small wired hub may only connect 4 computers; a large hub can connect 48 or more.
Hz	Hertz. The international unit for measuring frequency, equivalent to the older unit of cycles per second. One megahertz (MHz) is one million hertz. One gigahertz (GHz) is one billion hertz. The standard US electrical power frequency is 60 Hz, the AM broadcast radio frequency band is 535—1605 kHz, the FM broadcast radio frequency band is 88—108 MHz, and wireless 802.11b/g LANs operate at 2.4 GHz.
IEEE	Institute of Electrical and Electronics Engineers, New York, www.ieee.org. A membership organization that includes engineers, scientists and students in electronics and allied fields. It has more than 300,000 members and is involved with setting standards for computers and communications.
Infrastructure mode	An 802.11 setting providing connectivity to an AP. As compared to Ad-Hoc mode, whereby 802.11 devices communicate directly with each other, clients set in Infrastructure Mode all pass data through a central AP. The AP not only mediates wireless network traffic in the immediate neighbourhood, but also provides communication with the wired network. See Ad-Hoc and AP.
I/O	Input / Output. The term used to describe any operation, program or device that transfers data to or from a computer.
Internet appliance	A computer that is intended primarily for Internet access is simple to set up and usually does not support installation of third-party software. These computers generally offer customized web browsing, touch-screen navigation, e-mail services, entertainment and personal information management applications.
IP	Internet Protocol. A set of rules used to send and receive messages across local networks and the Internet.
IP telephony	Technology that supports voice, data and video transmission via IP-based LANs, WANs, and the Internet. This includes VoIP (Voice over IP).
IP address	A 32-bit number that identifies each sender or receiver of information that is sent across the Internet. An IP address has two parts: an identifier of a particular network on the Internet and an identifier of the particular device (which can be a server or a workstation) within that network.
IPX-SPX	Internetwork Packet Exchange, a networking protocol used by the Novell NetWare operating systems. Like UDP/IP, IPX is a datagram protocol used for connectionless communications. Higher-level protocols, such as SPX and NCP, are used for additional error recovery services. Sequenced Packet Exchange, SPX, a transport layer protocol (layer 4 of the OSI Model) used in Novell Netware networks. The SPX layer sits on top of the IPX layer (layer 3) and provides connection-oriented services between two nodes on the network. SPX is used primarily by client/server applications.
ISDN	A type of broadband Internet connection that provides digital service from the customer's premises to the dial-up telephone network. ISDN uses standard POTS copper wiring to deliver voice, data or video.
ISO Network Model	A network model developed by the International Standards Organization (ISO) that consists of seven different levels, or layers. By standardizing these layers, and the interfaces in between, different portions of a given protocol can be modified or changed as technologies advance or systems requirements are altered. The seven layers are: Physical , Data Link, Network, Transport, Session, Presentation, Application.
LAN	Local Area Network. A system of connecting PCs and other devices within the same physical proximity for sharing resources such as an Internet connections, printers, files and drives.
Receive Sensitivity	The minimum signal strength required to pick up a signal. Higher bandwidth connections usually have less receive sensitivity than lower bandwidth connections.

Router	A device that forwards data from one WLAN or wired local area network to another.
SNR	Signal to Noise Ratio. The number of decibels difference between the signal strength and background noise.
Transmit Power	The power usually expressed in mW or dBm that the wireless device transmits at.
MAC Address	Media Access Control address. A unique code assigned to most forms of networking hardware. The address is permanently assigned to the hardware, so limiting a wireless network's access to hardware -- such as wireless cards -- is a security feature employed by closed wireless networks. But an experienced hacker -- armed with the proper tools -- can still figure out an authorized MAC address, masquerade as a legitimate address and access a closed network. Every wireless 802.11 device has its own specific MAC address hard-coded into it. This unique identifier can be used to provide security for wireless networks. When a network uses a MAC table, only the 802.11 radios that have had their MAC addresses added to that network's MAC table will be able to get onto the network.
NAT	Network Address Translation: A network capability that enables a number of computers to dynamically share a single incoming IP address from a dial-up, cable or xDSL connection. NAT takes the single incoming IP address and creates new IP address for each client computer on the network.
NIC	Network Interface Card. A type of PC adapter card that either works without wires (Wi-Fi) or attaches to a network cable to provide two-way communication between the computer and network devices such as a hub or switch. Most office wired NICs operate at 10 Mbps (Ethernet), 100 Mbps (Fast Ethernet) or 10/100 Mbps dual speed. High-speed Gigabit and 10 Gigabit NIC cards are also available. See PC Card.
Proxy Server	Used in larger companies and organizations to improve network operations and security, a proxy server is able to prevent direct communication between two or more networks. The proxy server forwards allowable data requests to remote servers and/or responds to data requests directly from stored remote server data.
RJ-45	Standard connectors used in Ethernet networks. RJ-45 connectors are similar to standard RJ-11 telephone connectors, but RJ-45 connectors can have up to eight wires, whereas telephone connectors have four.
Server	A computer that provides its resources to other computers and devices on a network. These include print servers, Internet servers and data servers. A server can also be combined with a hub or router.
Site survey	The process whereby a wireless network installer inspects a location prior to installing a wireless network. Site surveys are used to identify the radio- and client-use properties of a facility so that access points can be optimally placed.
SSL	Secure Sockets Layer. A commonly used encryption scheme used by many online retail and banking sites to protect the financial integrity of transactions. When an SSL session begins, the server sends its public key to the browser. The browser then sends a randomly generated secret key back to the server in order to have a secret key exchange for that session
Sub network or Subnet	Found in larger networks, these smaller networks are used to simplify addressing between numerous computers. Subnets connect together through a router.
Switch	A type of hub that efficiently controls the way multiple devices use the same network so that each can operate at optimal performance. A switch acts as a networks traffic cop: rather than transmitting all the packets it receives to all ports as a hub does, a switch transmits packets to only the receiving port.
TCP	Transmission Control Protocol. A protocol used along with the Internet Protocol (IP) to send data in the form of individual units (called packets) between computers over the Internet. While IP takes care of handling the actual delivery of the data, TCP takes care of keeping track of the packets that a message is divided into for efficient routing through the Internet. For example, when a web page is downloaded from a web server, the TCP program layer in that server divides the file into packets, numbers the packets, and then forwards them individually to the IP program layer. Although each packet has the same destination IP address, it may get routed differently through the network. At the other end, TCP reassembles the individual packets and waits until they have all arrived to forward them as single message.

TCP/IP	The underlying technology behind the Internet and communications between computers in a network. The first part, TCP, is the transport part, which matches the size of the messages on either end and guarantees that the correct message has been received. The IP part is the user's computer address on a network. Every computer in a TCP/IP network has its own IP address that is either dynamically assigned at startup or permanently assigned. All TCP/IP messages contain the address of the destination network as well as the address of the destination station. This enables TCP/IP messages to be transmitted to multiple networks (subnets) within an organization or worldwide.
VoIP	Voice Over Internet Protocol. Voice transmission using Internet Protocol to create digital packets distributed over the Internet. VoIP can be less expensive than voice transmission using standard analog packets over POTS (Plain Old Telephone Service).
VPN	Virtual Private Network. A type of technology designed to increase the security of information transferred over the Internet. VPN can work with either wired or wireless networks, as well as with dial-up connections over POTS. VPN creates a private encrypted tunnel from the end user's computer, through the local wireless network, through the Internet, all the way to the corporate servers and database.
WAN	Wide Area Network. A communication system of connecting PCs and other computing devices across a large local, regional, national or international geographic area. Also used to distinguish between phone-based data networks and Wi-Fi. Phone networks are considered WANs and Wi-Fi networks are considered Wireless Local Area Networks (WLANs).
WEP	Wired Equivalent Privacy. Basic wireless security provided by Wi-Fi. In some instances, WEP may be all a home or small-business user needs to protect wireless data. WEP is available in 40-bit (also called 64-bit), or in 108-bit (also called 128-bit) encryption modes. As 108-bit encryption provides a longer algorithm that takes longer to decode, it can provide better security than basic 40-bit (64-bit) encryption.
Wi-Fi	Wireless Fidelity: An interoperability certification for wireless local area network (LAN) products based on the Institute of Electrical and Electronics Engineers (IEEE) 802.11 standard.

Appendix C CHANNELS

802.11b/g

Channel	Frequency (MHz)	North America	Europe	Australia	Japan	Most of world
1	2412	Yes	Yes	Yes	Yes	Yes
2	2417	Yes	Yes	Yes	Yes	Yes
3	2422	Yes	Yes	Yes	Yes	Yes
4	2427	Yes	Yes	Yes	Yes	Yes
5	2432	Yes	Yes	Yes	Yes	Yes
6	2437	Yes	Yes	Yes	Yes	Yes
7	2442	Yes	Yes	Yes	Yes	Yes
8	2447	Yes	Yes	Yes	Yes	Yes
9	2452	Yes	Yes	Yes	Yes	Yes
10	2457	Yes	Yes	Yes	Yes	Yes
11	2462	Yes	Yes	Yes	Yes	Yes
12	2467	No	Yes	Yes	Yes	Yes
13	2472	No	Yes	Yes	Yes	Yes
14	2484	No	No	No	.11b only	No

802.11b/g Turbo

6	**2437**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**

Appendix D 802.11a TX Power regulations

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

Appendix E External Iperf Test

This Appendix shows how to set up and use the Iperf application to test the throughput of Ethernet Modems.

Iperf is a tool used to measure the throughput and quality of a network link. Another Application called Jperf can also be used which gives a graphical interface for all results. This instruction covers both Iperf and Jperf, it does not cover the setup and configuration of the modems. Details can be found in previous sections.

Materials

- x Ethernet Modems configured as a bridge
- 2 x PC Computers with Ethernet Ports
- Suitable Power Supplies for the Ethernet Modems
- Straight through Ethernet cables
- Iperf / Jperf Application

Installation

The Application can be downloaded from the following link http://www.honeywell.com/ps/hfs download and save to a location on your PC.

Extract to zip file to the ROOT directory on your PC, i.e. C:\ This folder contains the main Iperf application as well as the Jperf graphical interface.

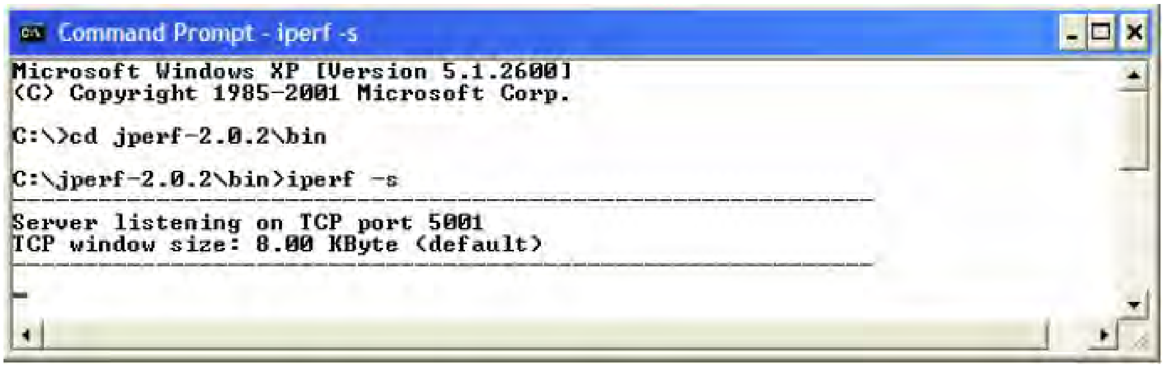
Copy this folder to the 2nd PC or download to the second PC and extract as per above instructions.

Iperf Applications

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

At the Server PC open a Command prompt by selecting Windows Start/run and enter “CMD”.

When command prompt appears we need to set the directory to where the Iperf application resides, i.e. where it was saved above, and from here run the Iperf server command “iperf – s”. See figure below.



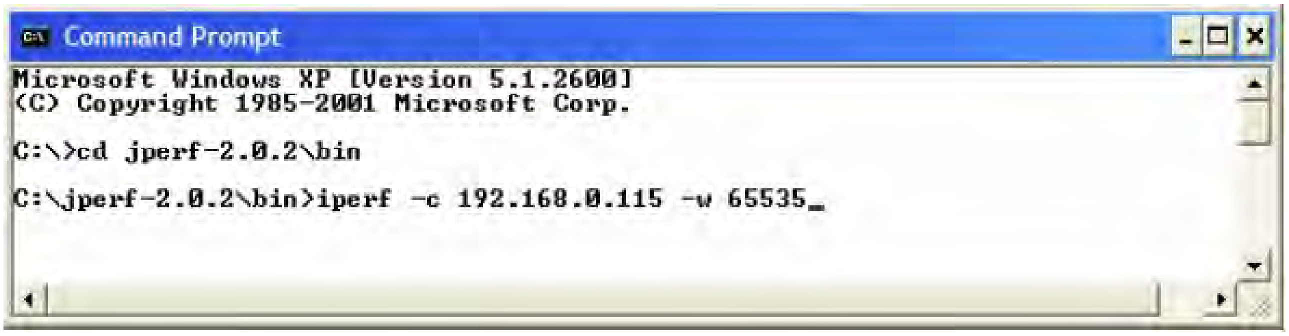
```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\>cd jperf-2.0.2\bin

C:\jperf-2.0.2\bin>iperf -s
------------------------------------------------------------
Server listening on TCP port 5001
TCP window size: 8.00 KByte (default)
------------------------------------------------------------
_
```

Note: If you get a security pop up on PC select Unblock for the application to run.

Iperf server application is now running and waiting for a Client connection.

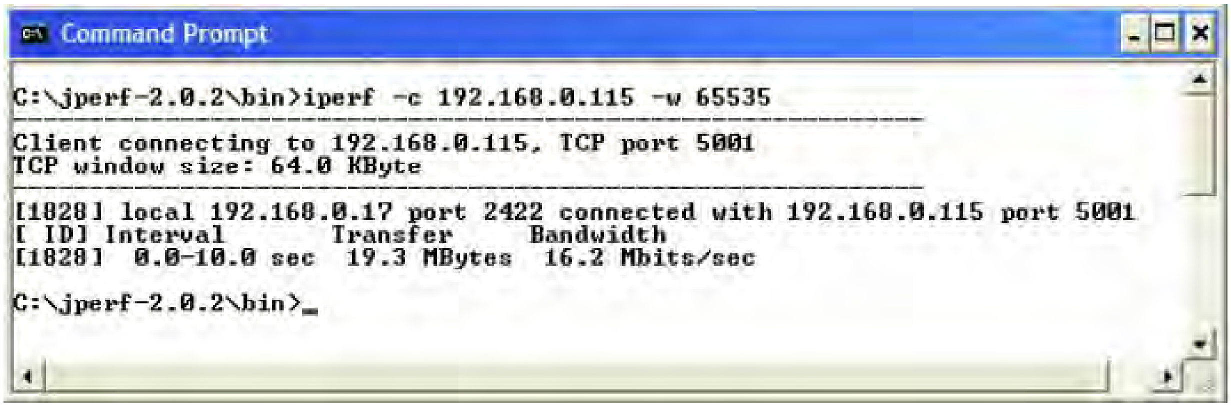
On the Client PC open up a CMD prompt and change the directory to jperf-2.0.2\bin as performed above for the server.

This time enter the Iperf command to start the client communication to the server. “Iperf –c <IP address of Server PC> -w 65535. See figure below.



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

C:\>cd jperf-2.0.2\bin

C:\jperf-2.0.2\bin>iperf -c 192.168.0.115 -w 65535_
```

This will run a test over the Wi-Fi Link to the Server PC and report back results as seen in figure below.
These results show the Bandwidth (Throughput) of the test as 16.2Mbits/sec.



```
C:\jperf-2.0.2\bin>iperf -c 192.168.0.115 -w 65535
------------------------------------------------------------
Client connecting to 192.168.0.115, TCP port 5001
TCP window size: 64.0 KByte
------------------------------------------------------------
[1828] local 192.168.0.17 port 2422 connected with 192.168.0.115 port 5001
[ ID] Interval       Transfer     Bandwidth
[1828]  0.0-10.0 sec  19.3 MBytes  16.2 Mbits/sec

C:\jperf-2.0.2\bin>_
```

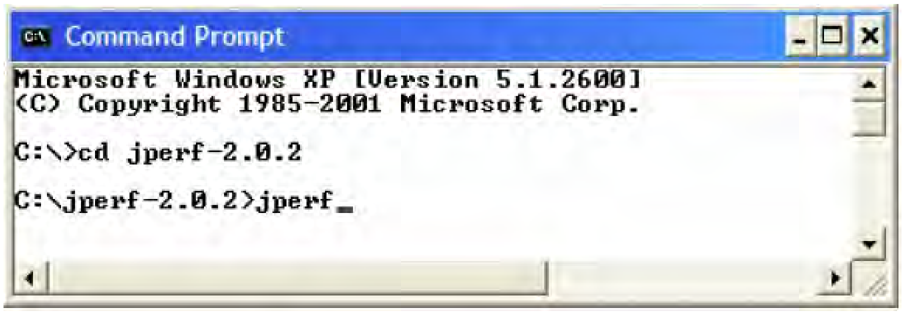
Using the Theoretical throughput calculations in Table below you can compare the results with the measured to give an indication of the difference between expected and measured. Remembering that the theoretical calculations are best case possible results

	XYR400-E	XYR401-E	XYR301-E (20Mhz)	XYR300-E
54Mbps		27Mbps	27Mbps	
11Mbps	5Mbps	5Mbps	5Mbps	
1Mbps	500Mbps	500Mbps	500Mbps	
200Kbps				80Kbps
100Kbps				40Kbps
78Kbps				
19.2Kbps				7.8Kbps

In the command line for the Client mapping we established the Server IP address followed by the –w 65535, -w is the window size and the maximum TCPIP window size is 65535bytes.
Another entry that can be added is –t <seconds> to run the test for a specific time period. Example of this is in where the same test is run for 30 seconds.

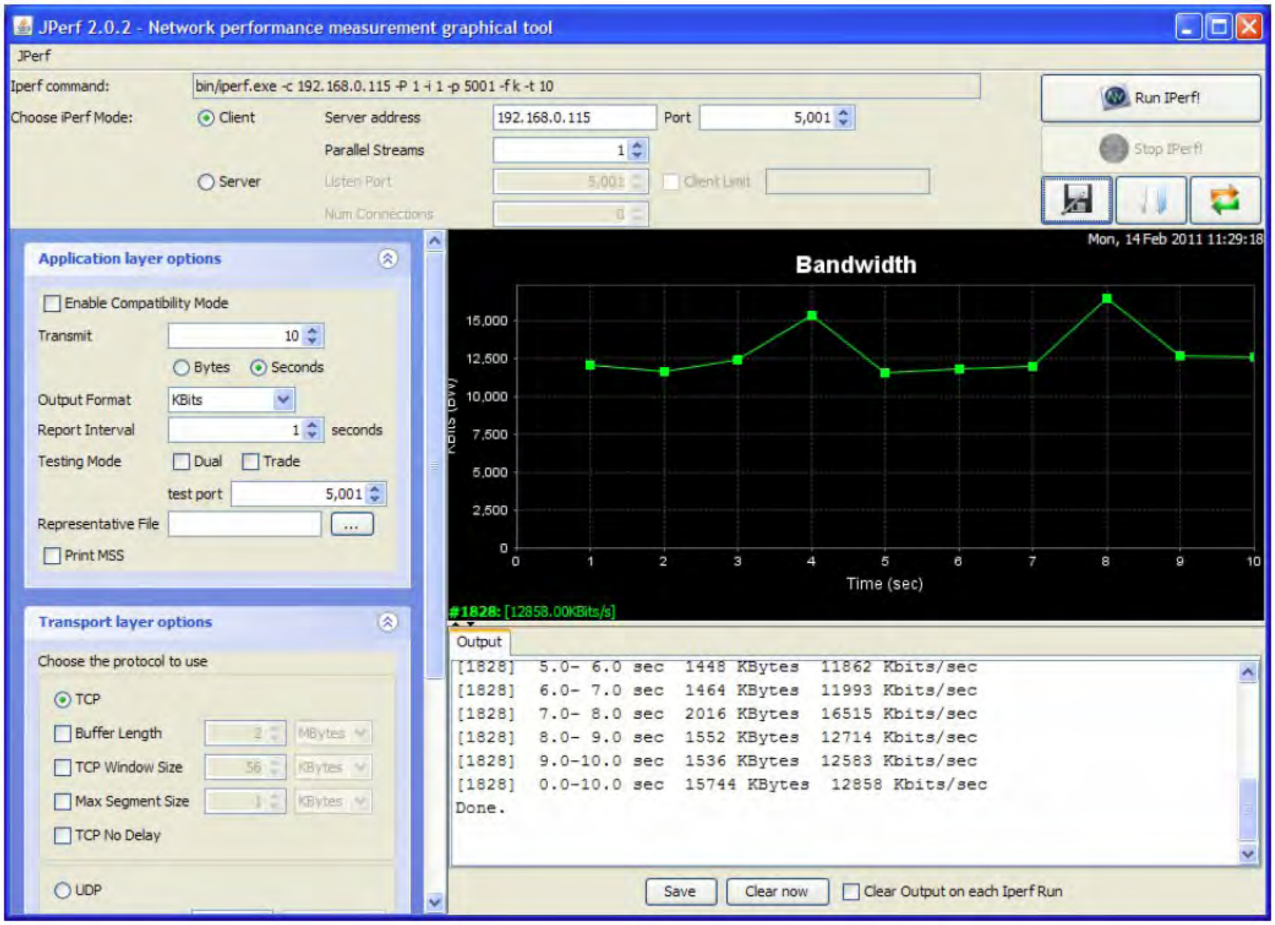
JPerf Application

Jperf is a graphical interface that runs over the top of Iperf. It will display a graph result from the Iperf test.
To run Jperf open a CMD prompt and change to the “jperf-2.0.2: directory and run the “Jperf” application as shown in the figure below.



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

C:\>cd jperf-2.0.2

C:\jperf-2.0.2>jperf_
```

The CMD screen will disappear and the Jperf Screen will appear as seen in the figure below.



Iperf command: bin/iperf.exe -c 192.168.0.115 -P 1 -i 1 -p 5001 -f k -t 10

Choose iPerf Mode: ● Client Server address 192.168.0.115 Port 5,001
Parallel Streams 1
○ Server Listen Port 5,001 □ Client Limit
Num Connections 0

□ Enable Compatibility Mode
Transmit 10 ○ Bytes ● Seconds
Output Format KBits
Report Interval 1 seconds
Testing Mode □ Dual □ Trade
test port 5,001
Representative File ...
□ Print MSS

Choose the protocol to use
● TCP
□ Buffer Length 2 MBytes
□ TCP Window Size 56 KBytes
□ Max Segment Size 1 KBytes
□ TCP No Delay
○ UDP

```
[1828]  5.0- 6.0 sec  1448 KBytes  11862 Kbits/sec
[1828]  6.0- 7.0 sec  1464 KBytes  11993 Kbits/sec
[1828]  7.0- 8.0 sec  2016 KBytes  16515 Kbits/sec
[1828]  8.0- 9.0 sec  1552 KBytes  12714 Kbits/sec
[1828]  9.0-10.0 sec  1536 KBytes  12583 Kbits/sec
[1828]  0.0-10.0 sec  15744 KBytes  12858 Kbits/sec
Done.
```

□ Clear Output on each Iperf Run

When Jperf screen appears select Client Mode, enter in IP address of the Server PC; leave Port as default and press Run Iperf button. The test will run again and the Bandwidth (Throughput) display will show results of the test.

Note: Jperf runs using Java technology and depending on PC setup further installation of Java software may be required.

Appendix F GNU Free Documentation Licence

Version 2, June 1991

Preamble

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

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

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

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

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

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

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

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

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Sales and Service

For application assistance, current specifications, pricing, or name of the nearest Authorized Distributor, contact one of the offices below.

ASIA PACIFIC

(TAC) **hfs-tac-support@honeywell.com**

Australia
Honeywell Limited
Phone: +(61) 7-3846 1255
FAX: +(61) 7-3840 6481
Toll Free 1300-36-39-36
Toll Free Fax:
1300-36-04-70

China – PRC - Shanghai
Honeywell China Inc.
Phone: (86-21) 5257-4568
Fax: (86-21) 6237-2826

Singapore
Honeywell Pte Ltd.
Phone: +(65) 6580 3278
Fax: +(65) 6445-3033

South Korea
Honeywell Korea Co Ltd
Phone: +(822) 799 6114
Fax: +(822) 792 9015

EMEA

Phone: + 80012026455 or +44 (0)1202645583

FAX: +44 (0) 1344 655554

Email: (Sales) **sc-cp-apps-salespa62@honeywell.com** or

(TAC) **hfs-tac-support@honeywell.com**

NORTH AMERICA

Honeywell Process Solutions,

Phone: 1-800-423-9883

Or 1-800-343-0228

Email: (Sales) **ask-ssc@honeywell.com** or

(TAC) **hfs-tac-support@honeywell.com**

SOUTH AMERICA

Honeywell do Brazil & Cia

Phone: +(55-11) 7266-1900

FAX: +(55-11) 7266-1905

Email: (Sales) **ask-ssc@honeywell.com** or
(TAC) **hfs-tac-support@honeywell.com**

Honeywell

Honeywell Process Solutions
1860 West Rose Garden Lane
Phoenix, Arizona 85027
www.honeywellprocess.com

34-XY-25-42 Version 1.8.1
April 2012