

Trio J-Series Ethernet Data Radio

User Manual

Date: 01/2024

www.se.com



Legal Information

The information provided in this documentation contains general descriptions and/or technical characteristics of the performance of the products contained herein. This documentation is not intended as a substitute for and is not to be used for determining suitability or reliability of these products for specific user applications. It is the duty of any such user or integrator to perform the appropriate and complete risk analysis, evaluation and testing of the products with respect to the relevant specific application or use thereof. Neither Schneider Electric nor any of its affiliates or subsidiaries shall be responsible or liable for misuse of the information contained herein. If you have any suggestions for improvements or amendments or have found errors in this publication, please notify us.

No part of this document may be reproduced in any form or by any means, electronic or mechanical, including photocopying, without express written permission of Schneider Electric.

All pertinent state, regional, and local safety regulations must be observed when installing and using this product. For reasons of safety and to help ensure compliance with documented system data, only the manufacturer should perform repairs to components.

This document contains standardized industry terms that some customers might find insensitive or offensive. These terms do not reflect the official policy or position of Schneider Electric.

Trademarks

Schneider Electric, ChannelShare, ClearSCADA, EcoStruxure, Modbus, Trio and TVIEW+ are trademarks and the property of Schneider Electric SE, its subsidiaries and affiliated companies. All other trademarks are the property of their respective owners.

Address

Schneider Electric

Schneider Electric
35 rue Joseph Monier
92500 Rueil-Malmaison, France

Email: RemoteOperations@se.com

www.se.com

© 2012 - 2024 Schneider Electric
All rights reserved.

Table of Contents

1	Part A - Preface.....	8
1.1	Technical Support.....	8
1.2	Safety Information.....	9
1.3	Cybersecurity.....	12
1.4	Revision History.....	14
1.5	Important Information.....	14
1.6	Compliance Information.....	15
1.7	Site Grounding.....	18
2	Part B - J-Series Overview.....	18
2.1	Product Range.....	18
2.2	Features and Benefits.....	19
2.3	Product Data Sheet Trio J-Series Model Code.....	22
3	Part C - Network Types.....	23
3.1	Point to Point Networks (PTP).....	24
3.2	Point to Multipoint Networks (PTMP).....	25
3.3	Point to Multipoint via KwikStream™ Repeater.....	26
3.4	Point to Point with LinkXtend™ Bridge (PTP/B).....	27
3.5	Point to Multipoint via LinkXtend™ Bridge (PTMP/B).....	28
4	Part D - Features.....	29
4.1	Over the Air Data.....	30
4.2	Modbus Gateway.....	31
4.2.1	Example: Traditional System Without J-Series Embedded Modbus Gateway.....	32
4.2.2	Example: System Using J-Series Embedded Modbus Gateway.....	32
4.3	Modbus Gateway Mode.....	33
4.3.1	Example: Using TCP With J-Series Modbus Gateway Functionality.....	33
4.4	Multi-Master Synchronization.....	34
4.5	Digital Collision Avoidance.....	35
4.6	Retries and Retransmissions.....	36
4.7	Ethernet Traffic Filtering.....	37

4.8	Static and DHCP IP Allocation.....	38
4.9	Compression.....	38
4.10	Security.....	39
4.11	Secure Shell (SSH).....	41
	4.11.1 SSH Example.....	41
4.12	HTTPS.....	42
	4.12.1 HTTPS Example.....	42
4.13	SmartPath™.....	42
	4.13.1 SmartPath™, Network Name, and Hopping Patterns.....	43
	4.13.2 SmartPath™ and Preferred/Alternative Access Points.....	44
	4.13.3 SmartPath™ PTMP Using LinkXtend™ Bridges.....	46
	4.13.4 Access Point Re-Acquisition Time.....	46
	4.13.5 SmartPath™ and Roaming Remotes.....	47
	4.13.6 RSSI Threshold and Roaming Remotes.....	47
	4.13.7 SmartPath™ and Hybrid Networks.....	48
	4.13.8 Configurationless Remotes.....	49
4.14	Diagnostics Tools.....	49
4.15	SNMP Diagnostics.....	50
4.16	SNMP Notifications.....	50
4.17	Text User Interface (TUI).....	51
4.18	Spectrum Analyzer and Channel Lockout Facility.....	51
4.19	Legacy Serial Support.....	52
	4.19.1 Differences between TCP and UDP.....	53
	4.19.2 Legacy Serial Modes Supported.....	54
5	Part E - RF Planning and Design.....	56
5.1	Understanding RF Path Requirements.....	56
5.2	Examples of Predictive Path Modelling.....	57
	5.2.1 Effect of Earth Curvature on Long Paths.....	59
5.3	Antennas.....	60
	5.3.1 Antenna Gain.....	61
	5.3.2 Antenna Placement.....	61
	5.3.3 Alignment of Directional Antennas.....	62
5.4	RF Feeders and Protection.....	62

5.5	Band Pass Filter (900 MHz Only).....	62
6	Part F - Quick Reference Guide.....	63
6.1	Mounting and Installation Instructions.....	63
6.2	DIN Mounting Kit.....	65
6.3	DIN Rail Mounting Bracket.....	65
6.4	DIN Rail Clip.....	66
6.4.1	Rear Mount DIN Rail Clip.....	67
6.4.2	Bottom Mount DIN Rail Clip.....	68
6.5	Connecting Antennas and RF Feeders.....	69
6.6	J-Series Connections Layout.....	70
6.7	Power Supply Requirements.....	70
6.8	Communication Ports.....	70
6.9	Cable Termination.....	71
6.10	Serial Port A & B Ports.....	72
6.11	LED Indicators.....	73
6.11.1	Firmware Updating and Factory Default Information LEDs.....	74
6.11.2	Event LED Indications.....	75
6.12	Web User Interface (WUI).....	75
6.13	Connection to WUI - Secure HTTPS Connection.....	77
6.14	Resolving Ethernet Configuration Problems.....	82
6.15	Multi Master Synchronization.....	84
6.16	Text User Interface (TUI).....	85
6.17	Spectrum Analyzer.....	89
6.18	Telnet Interface.....	93
6.19	Secure Shell (SSH).....	94
6.20	SNMP	97
6.20.1	Notifications.....	97
6.20.2	MIB Files.....	97
6.20.3	Status Levels for SNMP Parameters.....	98
6.20.4	Implementation of multiple use objects.....	98
6.20.5	Summary of SNMP Parameters Supported.....	98
6.20.6	Configurations of SNMP Parameters.....	102
6.20.7	Customizing SNMP notifications.....	104

6.21	e-Diags Example.....	106
6.22	e-Diags Parameters.....	107
6.23	Ethernet Filtering.....	109
7	Part G - Quick Start Guide.....	109
7.1	Device Hardening.....	110
7.2	Point to Point Ethernet Link Setup.....	110
7.3	Point to Point - TCP Serial Device Server Setup Guide.....	114
7.4	Point to Point - UDP (Unicast) Serial Device Server Setup Guide.....	116
7.5	Point to Multipoint - UDP (Multicast) Serial Device Server Setup Guide.....	118
7.6	Point to Multipoint with Peer to Peer - UDP (Multicast to Multicast) Serial Device Server Setup Guide.....	120
7.7	Point to Point - Modbus/TCP to Modbus RTU Setup Guide.....	122
7.8	Point to Multipoint - Modbus/TCP to Modbus RTU Setup Guide.....	123
8	Part H - Installation & Commissioning.....	124
8.1	Typical Installation Overview.....	125
8.2	Antenna Installation.....	126
8.3	LED Indicators.....	128
8.4	Optimizing the Antenna for Rx Signal.....	128
8.5	Commissioning.....	130
	8.5.1 HTML Diagnostics.....	131
	8.5.1.1 Access Point.....	132
	8.5.1.2 Review Remote Radio.....	132
	8.5.1.3 Packet Error Testing.....	133
	8.5.1.4 Commissioning Record.....	133
9	Part I - Firmware Updating and Maintenance.....	134
9.1	Firmware Update Overview (R2.x.x or later) Introduction.....	134
	9.1.1 Firmware Update Procedure.....	136
9.2	Replacing the Internal Fuse.....	138
10	Part J - FCC Approved Antennas.....	142
11	Part K - Support Options.....	144
12	Part L - Open Source License Acknowledgments.....	144
13	Part M - Specifications.....	148

1 Part A - Preface

- [Technical Support](#) ⁸
- [Safety Information](#) ⁹
- [Cybersecurity](#) ¹²
- [Revision History](#) ¹⁴
- [Important Information](#) ¹⁴
- [Compliance Information](#) ¹⁵
- [Site Grounding](#) ¹⁸

1.1 Technical Support

Questions and requests related to any part of this documentation can be directed to one of the following support centers.

Technical support: Americas, Europe, Middle East, Asia

Available Monday to Friday 8:00 am – 6:30 pm Eastern Time

	Check our FAQs	Explore our extensive knowledge database and FAQ videos to find answers quickly: https://se.com/faq
	Email us	Save time by emailing us your inquiry and an expert will contact you: supportRO@se.com Send us an email anytime.
	Call us	Need someone to provide some technical support? • Toll free within North America: 1-888-226-6876 • Direct Worldwide: +1-613-591-1943

Technical support: Australia/New Zealand (Pacific)

Available Monday to Friday 8:00 am - 5:00 pm Australian Eastern Standard Time

	Check our FAQs	Explore our extensive knowledge database and FAQ videos to find answers quickly: https://se.com/faq
	Email us	Save time by emailing us your inquiry and an expert will contact you: techsupport.pz@se.com Send us an email anytime.
	Call us	Need someone to provide some technical support? • Inside Australia: 13 73 28 (13 SEAU) • Inside New Zealand: 0800 652 999

1.2 Safety Information

Important information

Read these instructions carefully, and look at the equipment to become familiar with the device before trying to install, operate, or maintain it. The following special messages may appear throughout this documentation or on the equipment to warn of potential hazards or to call attention to information that clarifies or simplifies a procedure.



The addition of this symbol to a Danger or Warning safety label indicates that an electrical hazard exists, which will result in personal injury if the instructions are not followed.



This is the safety alert symbol. It is used to alert you to a potential personal injury hazards. Obey all safety messages that follow this symbol to avoid possible injury or death.

DANGER

DANGER indicates a hazardous situation which, if not avoided, **will result in** death or serious injury.

⚠ WARNING

WARNING indicates a hazardous situation which, if not avoided, **could result in** death or serious injury.

⚠ CAUTION

CAUTION indicates a hazardous situation which, if not avoided, **could result in** minor or moderate injury.

NOTICE

NOTICE is used to address practices not related to physical injury.

Please note

Electrical equipment should be installed, operated, serviced, and maintained only by qualified personnel. No responsibility is assumed by Schneider Electric for any consequences arising out of the use of this material.

A qualified person is one who has skills and knowledge related to the construction, installation, and operation of electrical equipment and has received safety training to recognize and avoid the hazards involved.

For the definition of a restricted access location, refer to the IEC 62368 standard.

⚠ WARNING**HAZARD OF THERMAL BURNS**

High operating temperature.

- Avoid direct contact with device while in operation.
- Install the JR900 or JR240 device in a restricted access location to avoid unintentional contact.

Failure to follow these instructions can result in death or serious injury.

⚠ WARNING**HAZARD OF RADIO FREQUENCY (RF) BURNS**

Ensure that a matching load or antenna is attached to the RF port prior to applying power to the device.

Failure to follow these instructions can result in death or serious injury.

⚠ WARNING**HAZARD OF EXPLOSION**

Ensure that all connected equipment is grounded to the power source ground termination.

Failure to follow these instructions can result in death or serious injury.

Before using this product, read the Safety Information, Compliance information and all recommendations related to the purchased wireless communications equipment found within the Installation and Commissioning section found within the product user manual.

⚠ WARNING**UNACCEPTABLE USE**

Do not use Trio Data Radios as an integral part of a safety system. These devices are not safety products.

Failure to follow these instructions can result in death or serious injury.

⚠ WARNING**LOSS OF CONTROL**

- The designer of any control scheme must consider the potential failure modes of control paths and, for certain critical control functions, provide a means to achieve a safe state during and after a path failure. Examples of critical control functions are emergency stop and over travel stop.
- Separate or redundant control paths must be provided for critical control functions.
- System control paths may include communication links. Consideration must be given to the implications of anticipated transmission delays or failures of the link¹
- Each implementation of equipment utilizing communication links must be individually and thoroughly tested for proper operation before being placed into service.

Failure to follow these instructions can result in death or serious injury.

¹For additional information about transmission delays or failures of the link, refer to NEMA ICS 1.1 (latest edition). Safety Guidelines for the Application, Installation, and Maintenance of Solid State Control or its equivalent in your specific country, language, and/or location.

Environment

This environment is 'enclosed'. It can be installed without any specific protection in areas with restricted access and low pollution levels (not exceeding 2), for example; stations or control rooms which have neither machines nor any activity generating metallic dust or other metallic particles. In other environments, it is recommended to follow rules as defined in the user manual. For the definition of a restricted access location, refer to the IEC 62368 standard.

⚠ WARNING**HAZARD OF DEATH OR SERIOUS INJURY**

- The JR900 and JR240 must be installed in a restricted access location
- Ensure that the operating temperature (air surrounding equipment) never exceeds 70 °C (158 °F)
- Ensure that all radio equipment is installed with a lightning arrestor
- Ensure that all connected equipment is grounded to the power source ground termination
- Where an internal fuse is to be replaced, the replacement fuse must be of the specified type and current rating. Refer to the fuse replacement instructions within the Product User Manual before servicing.
- Ensure that a matching load or antenna is attached to the RF port prior to applying power to the device

Failure to follow these instructions can result in death or serious injury.

Wiring

To improve the security of the installation, follow the rules below:

NOTICE**HAZARD OF EQUIPMENT DAMAGE**

The radio modem can be damaged if there is any potential difference between the chassis-ground, RS-232 signal ground, power (-) input, or antenna coaxial shield. Before connecting any wiring, ensure that all components are earthed to a common ground point.

Failure to follow these instructions can result in equipment damage.

1.3 Cybersecurity

Cybersecurity is a branch of network administration that addresses attacks on or by computer systems and through computer networks that can result in accidental or intentional disruptions. The objective of cybersecurity is to help provide increased levels of protection for information and physical assets from theft, corruption, misuse, or accidents while maintaining access for intended users.

No single cybersecurity approach is adequate. Schneider Electric recommends a defense-in-depth approach. This approach layers the network with security features, appliances, and processes. The basic components of this approach are:

- Risk assessment: A systematic security analysis of the environment and related systems.
- A security plan built on the results of the risk assessment.
- A multi-phase training campaign.
- Network separation and segmentation: Physical separation of the control network from other networks, and the division of the control network itself into segments and security zones.

- **System Access Control:** Controlling access to the system with firewalls, authentication, authorization, and other software means, and traditional physical security measures such as video surveillance, fences, locked doors and gates, and locked equipment cabinets.
- **Device hardening:** The process of configuring a device against communication-based threats. Device hardening measures include disabling unused network ports, password management, access control, and disabling unnecessary protocols and services.
- **Network monitoring and maintenance:** An effective defense-in-depth campaign requires continual monitoring and system maintenance to meet the challenge of new threats as they develop.

Data Privacy

This device is not designed or intended for the collection and storage of personal data. Data stored on the device can be deleted by performing a factory reset.

Contact us

For more information, refer to the Schneider Electric Cybersecurity Support Portal at:
<http://www.se.com/b2b/en/support/cybersecurity/overview.jsp>

Additional Resources

Schneider Electric Recommended Cybersecurity Best Practices
<https://www.se.com/ww/en/download/document/CS-Best-Practices-2019-340/>

Cybersecurity and Infrastructure Security Agency
<https://www.cisa.gov/>

ICS-CERT Recommended Practices
<https://ics-cert.us-cert.gov/Recommended-Practices>

Center for Internet Security (CIS) Top 20 Critical Security Controls
<https://www.cisecurity.org/cybersecurity-best-practices>

FBI Cyber Crime
<https://www.fbi.gov/investigate/cyber>

Guide to Industrial Control Systems (ICS) Security
<https://www.nist.gov/publications/guide-industrial-control-systems-ics-security>

WaterISAC Water Security Network
<https://www.waterisac.org>

1.4 Revision History

Release Version	Date	Updates
Issue: 10-12	October 2012	Added details for DIN mounting kit
Issue: 02-13	February 2013	Added specifications to the rear of manual
Issue: 12-13	December 2013	Modification to Serial port pin out specification
Issue: 12-22	December 2022	Updated the fuse replacement details Updated the firmware upgrade procedure
Issue: 01-24	January 2024	Updated compliance notice for Brazil

1.5 Important Information

This manual covers the operation of the J-Series of Digital Ethernet Data Radios. Specifications described are typical only and are subject to normal manufacturing and service tolerances.

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

This manual is copyright by Schneider Electric. All rights reserved. No part of the documentation or the information supplied may be divulged to any third party without the express written permission of Schneider Electric.

The manual is also proprietary to Schneider Electric and are supplied for the purposes referred to in the accompanying documentation and must not be used for any other purpose. All such information remains the property of Schneider Electric and may not be reproduced, copied, stored on or transferred to any other media or used or distributed in any way save for the express purposes for which it is supplied.

Products offered may contain software which is proprietary to Schneider Electric. However, the offer of supply of these products and services does not include or infer any transfer of ownership of such proprietary information and as such reproduction or reuse without the express permission in writing from Schneider Electric is forbidden. Permission may be applied for by contacting Schneider Electric in writing.

1.6 Compliance Information

Australian Compliance Notices

Maximum EIRP

ACMA Regulations allow up to 30 dBm (1 Watt) of effective isotropic radiated power (EIRP) in the 915 MHz license free band and 36 dBm (4 Watts) of EIRP in the 2.4 GHz band. Therefore, the sum of the transmitted power (in dBm), the cabling loss and the antenna gain cannot exceed the above stated EIRP limits.

Important Notices for Class I, Division 2, Groups A, B, C & D Hazardous Locations

Applies to models JR900-xxxx-xHx(CSA Marked)

This product is available for use in Class I, Division 2, Groups A, B, C & D Hazardous Locations. Such locations are defined in Article 500 of the US National Fire Protection Association (NFPA) publication NFPA 70, otherwise known as the National Electrical Code and in Section 18 of the Canadian Standards Association C22.1 (Canadian Electrical Code).

The transceiver has been recognized for use in these hazardous locations by the Canadian Standards Association (CSA) International. CSA certification is in accordance with CSA Standard C22.2 No. 213- M1987 and UL Standard 1604 subject to the following conditions of approval:

1. The radio modem must be mounted in a suitable enclosure so that a tool is required to gain access for disconnection of antenna, power and communication cables.
2. The antenna, DC power and interface cables must be routed through conduit in accordance with the National Electrical Codes.
3. Installation, operation and maintenance of the radio modem should be in accordance with the radio modem's user manual and the National Electrical Codes.
4. Tampering or replacement with non-factory components may adversely affect the safe use of the radio modem in hazardous locations and may void the approval.
5. A power connector with locking screws as supplied by Schneider Electric must be used.

Brazilian Compliance Notices

ANATEL - Resolução 680

Este equipamento não tem direito à proteção contra interferência prejudicial e não pode causar interferência em sistemas devidamente autorizados.

Para maiores informações, consulte o site da ANATEL - www.anatel.gov.br

EU (ETSI) Compliance Notices

RF Exposure

2.4 GHz Model: To satisfy EU (ETSI) requirements, a separation of 6 cm should be maintained between the antenna of this device and persons during operation.

Maximum EIRP

ETSI Maximum EIRP for the 2.4 GHz band is +20 dBm.

FCC Compliance Notices

FCC Part 15 Notice

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

This device must not be modified in any way or FCC compliance may be void.

FCC Approved Antennas

This device can only be used with Antennas listed in [Part J – FCC Approved Antennas](#)¹⁴². Contact Schneider Electric if you need more information or would like to order an antenna.

RF Exposure

To satisfy FCC RF exposure requirements for mobile transmitting devices, a separation distance of 26 cm or more should be maintained between the antenna of this device and persons during device operation. To ensure compliance, operations at closer than this distance is not recommended. The antenna used for this transmitter must not be co-located in conjunction with any other antenna or transmitter.

Maximum EIRP

FCC Regulations allow up to 36 dBm effective isotropic radiated power (EIRP). Therefore, the sum of the transmitted power (in dBm), the cabling loss and the antenna gain (in dBi) cannot exceed 36 dBm.

FCC Point to Point: More EIRP may be allowed for fixed point to point links. With the transmitter set to 27 dBm, an antenna gain (subtracting cable loss) of up to 15 dBi is allowed. For antenna gains of more than 15 dBi in a fixed point to point link, the power must be backed off from 27 dBm by 1 dB for every 3 dB the antenna gain exceeds 15 dBi.

Radio equipment directive

Applies to model JR240

⚠ WARNING

HAZARD TO HEALTH DUE TO ELECTRIC SHOCK

- To comply with the RED (Radio Equipment Directive) 2014/53/EU, all radio modem installations must include an external in-line lightning arrester or equivalent device that complies with the following specifications:
 - DC Blocking Capability - 1.5 kV impulse (Rise Time 10 mS, Fall Time 700 mS) (Repetition 10 Times) or 1.0 kV rms 50 Hz sine wave for 1 minute

Failure to follow these instructions can result in death or serious injury.

EU DECLARATION OF CONFORMITY

Hereby, Schneider Electric, declares that the radio equipment type JR240 is in compliance with Directive 2014/53/EU. The full text of the EU declaration of conformity is available at the following internet address: www.se.com/en/download

WEEE Regulation (Europe)

This symbol on the product or its packaging indicates that this product must not be disposed of with other waste.



Instead, it is your responsibility to dispose of your waste equipment by handing it over to a designated collection point for the recycling of waste electrical and electronic equipment. The separate collection and recycling of your waste equipment at the time of disposal will help conserve natural resources and help ensure that it is recycled in a manner that protects human health and the environment. For more information about where you can drop off your waste equipment for recycling, contact the dealer from whom you originally purchased the product.

Dieses Symbol auf dem Produkt oder seinem Verpacken zeigt an, daß dieses Produkt nicht mit anderer Vergeudung entledigt werden darf. Stattdessen ist es Ihre Verantwortlichkeit, sich Ihre überschüssige Ausrüstung zu entledigen, indem es rüber sie zu einem gekennzeichneten Ansammlungspunkt für die Abfallverwertung elektrische und elektronische Ausrüstung übergibt. Die unterschiedliche Ansammlung und die Wiederverwertung Ihrer überschüssigen Ausrüstung zu der Zeit der Beseitigung helfen, Naturressourcen zu konservieren und sicherzugehen, daß es in gewissem Sinne aufbereitet wird, daß menschliche Gesundheit und das Klima schützt. Zu mehr Information ungefähr, wo Sie weg von Ihrer überschüssigen Ausrüstung für die Wiederverwertung fallen können, treten Sie bitte mit dem Händler in Verbindung, von dem Sie ursprünglich das Produkt kauften.

1.7 Site Grounding

NOTICE

HAZARD OF EQUIPMENT DAMAGE

Ensure that the chassis mounting plate, power supply (-) Ground, RTU terminal device, and lightning arrester, are all securely connected to the ground in the building installation or a common ground point to which an earth/ground stake is attached.

Failure to follow these instructions can result in equipment damage.

2 Part B - J-Series Overview

- The advanced Schneider Electric Trio J-Series frequency hopping Ethernet Data Radio sets the standard for professional high speed serial data communications in the license free 900 MHz and 2.4G Hz bands.
- With maximum range and virtually unlimited system coverage due to its unique LinkXtend™ network bridging and KwikStream™ high speed repeater capabilities, the industrial strength J-Series is ideally suited for the most demanding point to multipoint and point to point wireless SCADA and Telemetry applications.
- The highly versatile J-Series also offers dual Ethernet ports with TVIEW+ network wide diagnostics compatibility.

See:

- [Product Range](#)^[18]
- [Features and Benefits](#)^[19]
- [Product Data Sheet Trio J-Series Model Code](#)^[22]

2.1 Product Range

The Schneider Electric Trio J-Series comprises of the following models:

- JR900: Operates within the 915 MHz license free frequency band (country specific models apply)
- JR240: Can be configured for use in the 2.4 GHz license free bands available throughout the world



J-Series Ethernet Data Radio

2.2 Features and Benefits

Outstanding and highly versatile operational capability

- Point to point and point to multipoint operation
- Configurable personality – access point-remote- bridge-repeater
- KwikStream™ high speed single radio repeater mode *
- Unlimited coverage networks
- No restriction on the number of radios in any system
- Unique dual antenna LinkXtend™ technology increases usable range
- Repeater and Bridge units support locally connected user devices
- ChannelShare™ collision avoidance for unsolicited remote transmissions allowing simultaneous polling and spontaneous reporting
- Up to 140 km (90 miles) single repeater system range with 6 dB antennas (900 MHz)

A Radio and Modem that extends performance boundaries

- License free operation in 900 MHz and 2.4 GHz ISM frequency bands
- 512 k high speed over-air data rate (can be reduced to 256 k, 128 K or 64 K for longer range)
- Robust, frequency hopping spread spectrum technology for superior interference immunity
- Ultra Long Range high performance receiver *
- 1 Watt maximum allowable transmitter power (900 MHz version only)
- Advanced accurate data delivery with CRC plus selectable FEC and ARQ
- Multi-Access Point synchronization mode for interference reduction with co-located Access Point radios
- High VSWR protection (900 MHz version only)

- Up to 70 km (45 miles) maximum single hop line-of-sight range with 6 dB antennas (900 MHz)

Total command of the radio system with embedded HTML web server

- Network Management and Remote Diagnostics with no software installation required!
- Supports SNMP V1 & V2c Traps and informs included)
- All configuration via a more secure embedded HTML interface (HTTP & HTTPS)
- Network wide access from any radio modem
- Over-the-air reconfiguration and diagnostics
- Powerful system commissioning and troubleshooting tools
- Compatible with TVIEW+ Diagnostics for stand alone network management.
- Local and Remote field upgradeable firmware
- Better securing of your network through Trusted Access Control
- 256-bit AES data encryption (export restrictions may apply)
- Proprietary multi-level scrambled over-the-air protocol
- Optional Trusted Access Point/Remote checklist
- A Ethernet Data Radio for the harshest environments and places:
- More reliable operation in environmental extremes (-40 °C to +70 °C)
- Hazardous Environment Certification – CSA Class I, Division II
- FCC & ETSI certification - accepted in multiple regions
- Compact, rugged alloy housing
- 10...30 Vdc power supply
- Dual industry standard TNC antenna connectors

Comprehensive and adaptable Ethernet interfacing, control, and transmission

- 2 x Independent Ethernet ports (Auto MDI/MIDX)
- 10/100 Mbps Interface (auto-detecting)
- Suitable for most Ethernet/IP protocols (including UDP, TCP, DHCP, ARP, ICMP, STP, IGMP, SNMP & TFPT)
- IEEE 802.3 including dual port Ethernet Bridging functionality
- Flexible Ethernet routing providing optimum radio channel efficiency
- Auto or Manual DHCP configuration
- NTP Client/Server Time Synchronization Support
- Legacy RS-232 serial support via embedded terminal servers (UDP/TCP/PPP)
- Embedded TCP Modbus gateway

- Configurable via Test user interface (Serial, Telnet, SSH)
- Configurable Ethernet Filtering helps to eliminate unnecessary bandwidth consumption

2.3 Product Data Sheet Trio J-Series Model Code

	TBURJRxxx-aabbbcode represents the part number matrix
Model	Model Type
TBURJ	J-Series
Code	Select: Unit Type
R	Base/Remote/Repeater Station with full enclosure
Code	Select: Generic Frequency Band
900	900 MHz
240	2.4 GHz
Code	Select: Frequency
	900 MHz Frequency Band
00	License-free band 902...928 MHz (FCC/IC - Requires Encryption for Canada and USA)
01	License-free band 915...928 MHz (Requires Encryption for Australia)
05	License-free band 921...928 MHz (New Zealand)
06	License-free band 902...907.5 MHz and 915...928 MHz (Brazil)
	2.4 GHz Frequency Band
00	License-free band 2.4 GHz, 500 mW (Requires Encryption for North America & Australia)
01	License-free band 2.4 GHz, ETSI/100 mW, ATEX (Europe)
Note: Other frequency bands available upon request.	
Code	Select: RF Channel Data Rate & Bandwidth (Internal Modem)
002	900 MHz: 64...512 kbps, 2.4 GHz: 64...256 kbps
Code	Select: Encryption
D	No Encryption
E	Encryption*

Code	Select: Approvals
H	Hazardous Environment CSA Class 1 Div 2
A	ATEX
Code	Future Option
0	None
Example: TBURJR900-00002EH0 specifies: Trio JR900 Remote Ethernet Station, 900 MHz band with a specific frequency range of 902...928 MHz, a 64...512 kbps modem, Encryption and Class1 Div2 rating. Communications Standards: FCC – Federal Communications Commission (USA) IC – Industry Canada ETSI – European Telecommunication Standards Institute ACMA – Australian Communications & Media Authority Contact your local sales office for accessories * Export restrictions may apply. Contact factory for details.	

3 Part C - Network Types

Fundamental to understanding the use of J-Series Ethernet Data Radios in your system is the need for a basic understanding of the different types of radio network topologies (known as NETWORK TYPES) and the function of each radio within them (known as RADIO TYPES).

Network Types

Point to Point (PTP): One Access Point radio is configured to communicate with a REMOTE radio in PTP mode.

Point to Point via Bridge (PTP/B): As per PTP mode but with additional network range extension using a LinkXtend™ Bridge.

Point to Multipoint (PTMP): One Access Point radio is configured to communicate with multiple REMOTE radio(s) a PTMP network.

Point to Multipoint with Bridges (PTMP/B): As per PTMP network but with additional network range extension using a LinkXtend™ Bridge.

Radio Types

Access Point: Defines the Access Point radio in a network. The function of the Access Point is to provide synchronization of the network and management of the radio protocol. There is always one Access Point per network.

Remote: A remote radio in the network. The function of a remote is to communication with the Access Point either directly or via one or more Bridges.

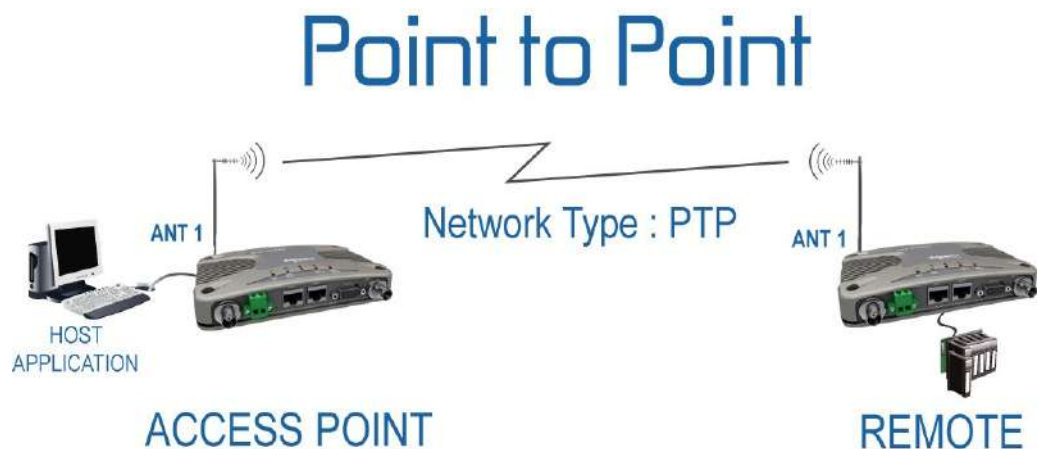
Bridge: A radio that provides network extension between an Access Point or another BRIDGE and additional REMOTES. A BRIDGE is a device with dual personalities, behaving as a REMOTE to its Access Point for 50% of the time, and then behaving as an Access Point for its REMOTES for the remaining time.

Each type of network is described in the following links:

- [Point to Point Networks \(PTP\)](#) ^[24]
- [Point to Multipoint Networks \(PTMP\)](#) ^[25]
- [Point to Multipoint via KwikStream™ Repeater](#) ^[26]
- [Point to Point with LinkXtend™ Bridge \(PTP/B\)](#) ^[27]
- [Point to Multipoint via LinkXtend™ Bridge \(PTMP/B\)](#) ^[28]

3.1 Point to Point Networks (PTP)

A Point to Point (PTP) network has one Access Point and one Remote radio. The available data bandwidth is shared between the two radios in each direction. Because a PTP network only has two radios, the over-the-air protocol can be optimized to provide best possible bandwidth, latency and security.



Each hop is divided into two halves. The Access Point can transmit in the first half and the Remote in the second half. This mode of operation is called Pseudo Full Duplex due to the shared division of available bandwidth. Due to the well defined nature of channel access in PTP mode, data collisions due to the Access Point and Remote trying to access the channel at the same time do not occur.

Pseudo Full Duplex has the advantage that it appears to the connected device to be a full duplex cable with a specific bandwidth (i.e. even if one device transmits continuously it will not block

the other device from sending data). This is useful for applications that expect full duplex communications or that are not designed to be radio modem friendly. The disadvantage of Pseudo Full Duplex is that the bandwidth is divided equally for each direction, even if one direction does not use its available bandwidth.

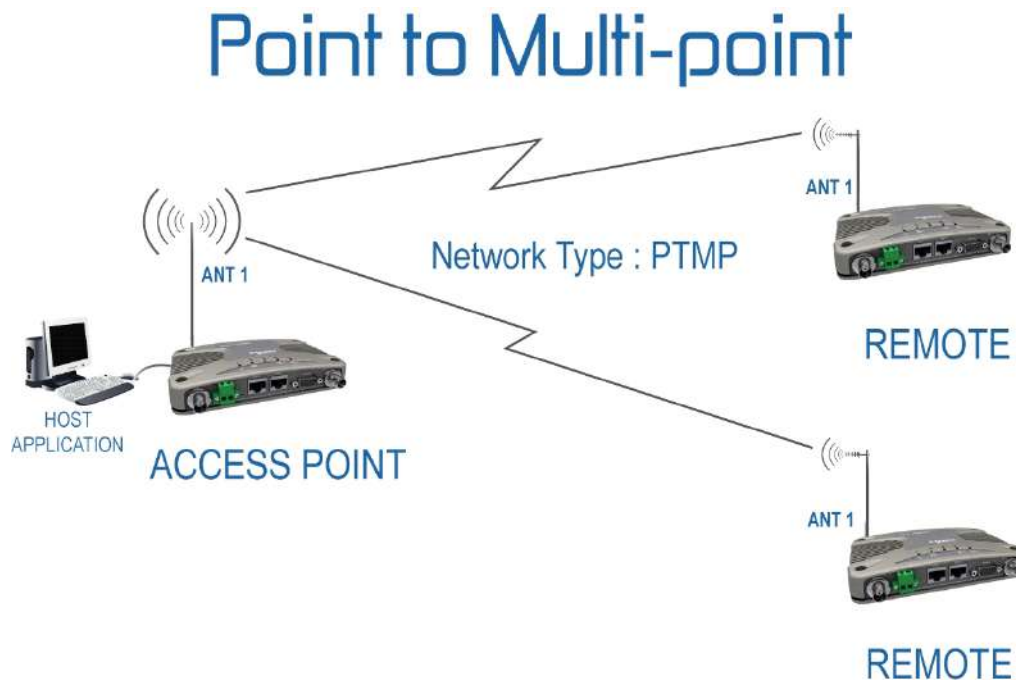
Receipt of data (in either Access Point to Remote OR Remote to Access Point directions) is acknowledged by the receiving radio. This provides the most efficient means of guaranteed data delivery as data does not need to be blindly “re-transmitted” which decreases the available bandwidth. For more information on data acknowledgments and retransmissions refer to [Part D – Features](#) ²⁹.

It is also possible to create a Point to Point (PTP) network using the Point to Multipoint (PTMP) Network Type and using only one Remote. In the PTMP mode, system bandwidth is not shared equally, but when additional REMOTE sites are added at a future date, the existing radios will not need to be re configured making additional Remote site deployment easier.

3.2 Point to Multipoint Networks (PTMP)

A Point to Multipoint (PTMP) network is normally chosen when one site (i.e. The HOST) needs to broadcast messages to multiple REMOTE sites.

Point to Multipoint (PTMP) operation requires the Access Point site to have adequate RF coverage of all Remote sites which need to synchronize to the Access Point. A PTMP offers the best available bandwidth and data latency when multiple remote sites are required.



If used in conjunction with an exception reporting protocol (i.e. DNP3) or when multiple applications are used on the network (i.e. A DNP3 RTU on Port A and a Modbus PLC on Port B) it is possible for more than one Remote radio to attempt to access the Access Point at the same time. This will cause data collisions, which requires the Remote radios to re-try their access to the Access Point. The result is a reduction in bandwidth and an increase in latency.

To optimize the access to the Access Point in this scenario, it is strongly recommended to enable the ChannelShare™ collision avoidance feature. The ChannelShare™ feature will minimize data collisions and increase effective throughput using a smart channel access strategy. More information on ChannelShare™ digital collision avoidance technology can be found in Part D - Features of this manual.

The Access Point radio needs to be located at a site which has adequate RF coverage of all Remote sites. If this is not possible, then Point to Multipoint via KwikStream™ Repeater is the preferred network topology.

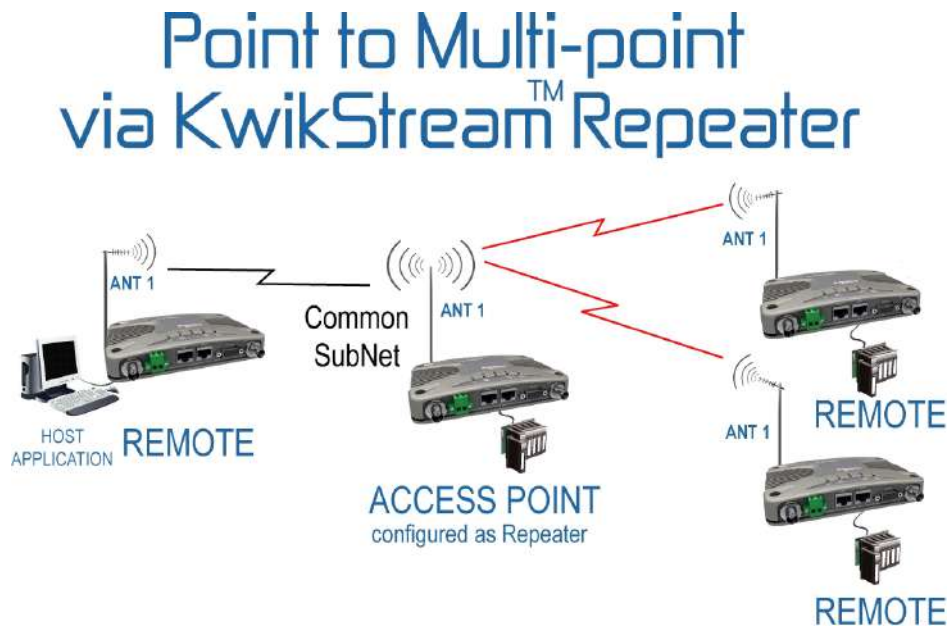
The bulk of network specific radio configuration parameters are configured in the Access Point radio. Remote radios in the network “learn” these configuration options from the Access Point. Remote radios can be added to the network without need to reconfigure the Access Point.

System wide diagnostics is available from any one remote to any other radio in the network.

It is recommended that omnidirectional antennas are used for the Access Point site and directional yagi antennas are used for REMOTE radio sites as this will provide maximum system gain legally allowed.

3.3 Point to Multipoint via KwikStream™ Repeater

A Point to Multipoint via KwikStream™ Repeater network is a variation of the Point To Multipoint network. It is normally chosen when the site where the SCADA (i.e. data) entry point does not have adequate RF coverage of other Remote sites in the network. The network diagram is shown below.



In this network topology, the Access Point radio is configured as a Repeater. The repeater should be located at a site with adequate RF coverage to each of the remotes. The Repeater still behaves as an Access Point to the Remotes as in a Point to Multipoint network, but the Repeater is configured to repeat data messages between remotes in the network. It therefore allows peer to peer communication to occur between remotes.

Because the Access Point radio now needs to “Repeat” data, data latency for messages from the Host Application to/from the Remotes will be longer. However, the Repeater implements a smart repeating technology called KwikStream™ which allows the Repeater to perform multiple transactions within any one hop, ensuring available bandwidth remains high and data latency is kept low. KwikStream™ technology is achieved using a virtual “loop-back” plug ensuring data is repeated quickly and no user port with physical loop back plug is required. A key advantage is that a local RTU/PLC device can be located at the Repeater site and peer to peer communication is supported for this unit.

For more information on KwikStream™ technology, refer to the appropriate section in [Part D – Features](#)^[29].

All other aspects of the Point to Multipoint network apply to this network topology.

3.4 Point to Point with LinkXtend™ Bridge (PTP/B)

The typical range of the Point to Point (PTP) Network Type can be extended using the Schneider Electric unique dual antenna LinkXtend™ technology. This is achieved using a special radio mode called BRIDGING. A dual antenna LinkXtend™ bridge allows the maximum range possible from a single radio store and forward technology whilst remaining within legal antenna EIRP limits. A typical Point to Point with Bridge network is shown below.



The Point to Point with LinkXtend™ Bridge (PTP/B) type of network requires one Access Point, one or more Bridges and one Remote radio. The Bridge operates in two different modes which alternate depending on what hop (odd or even) the hopping pattern is currently on.

During even numbered hops, the Bridge functions as a Remote to the network Access Point. Using the location of the Bridge in the network as a reference point, any data sent from the Bridge to the Access Point is sent “Upstream”.

During odd numbered hops, the Bridge functions as an Access Point for the Remote radio. Using the location of the Bridge in the network as a reference point, any data sent from the Bridge to the Remote is sent “Downstream”.

Thus a Bridge is a radio which functions both as a REMOTE and an Access Point in a time division multiplexed network.

When implementing this network it is important that the NETWORK TYPE is selected as Point to Point via Bridge (PTMP/B). This ensures the network is divided up into multiple Sub-nets that supports the time division multiplexing of the system required by the Bridge. Each Sub-Net uses a completely different hopping pattern so that multiple Bridges in the network will not interfere with each other.

Access Point to Bridge communication occurs on one Sub-Net whilst Bridge to Remote communication occurs on another Sub-Net. The Access Point radio is responsible for network

timing so that the Bridge is always operating in the correct mode helping to help ensure that data is not lost due to collisions between Access Point and Remote.

Each additional bridge in the network requires the definition of a new Sub-net. For more information on Sub-Nets, refer to [Part D – Features](#)^[29]. Network latency is doubled when compared to the latency of a network without bridges but due to the high speed nature of the J-Series family, network latency is seldom an issue.

When Bridge mode is selected the radio can be configured for either a single antenna or dual antenna. Only on sites that require dual antenna LinkXtend™ technology does a bridge need to operate in dual antenna mode. There are no limits to the number of bridges allowed in any one network but additional Bridges will result in extra latency due to the time taken to transport data through the bridge.

It is recommended that omnidirectional and yagi antennas are used for BRIDGES (depending on network design) and directional yagi antennas are used for Access Point and REMOTE radio sites as this will provide maximum system gain legally allowed. However, some sites where Bridges may be located may not require the use of dual antennas and in these situations a single omnidirectional antenna can be used.

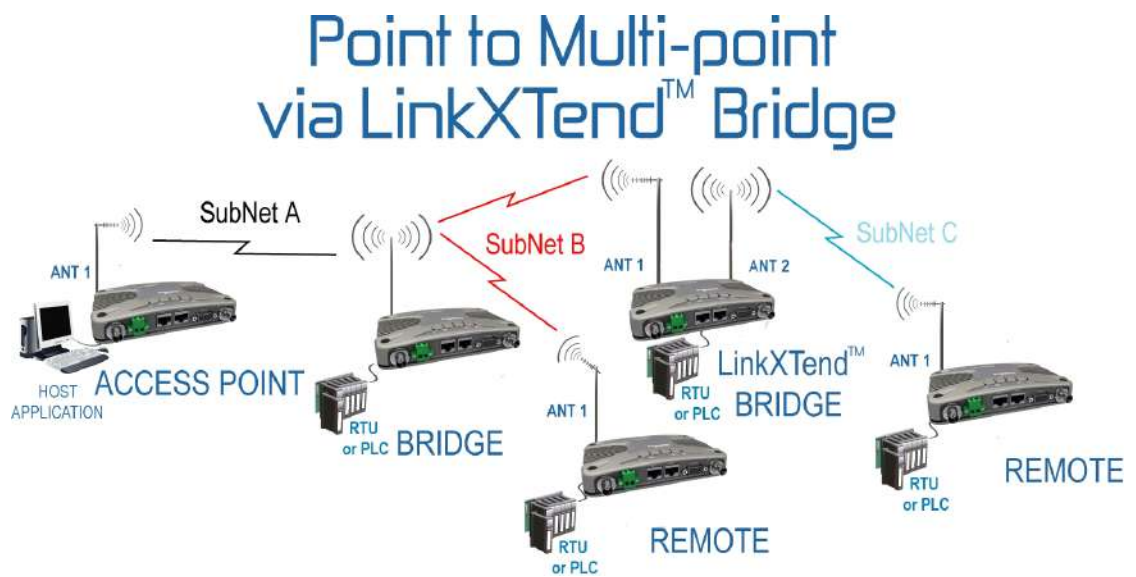
For more information the dual antenna port feature, refer to [Part D – Features](#)^[29].

All other aspects of the Point to Point (PTP) network previously mentioned apply to this type of network.

3.5 Point to Multipoint via LinkXtend™ Bridge (PTMP/B)

It is recommended that you first read Part C - Point to Multipoint (PTMP) Networks and Part C - Point to Point with LinkXtend™ Bridges before reading this section.

The typical range of the Point to Multipoint (PTMP) Network Type can also be extended using dual antenna LinkXtend™ technology. This is achieved using Bridges which operate in the same way as described in Point to Point with LinkXtend™ Bridges (PTMP/B) networks. A typical Point to Multipoint with Bridge network is shown below.



This type of network includes an Access Point, two or more multiple Bridges and multiple Remote radios.

If used in conjunction with an exception reporting protocol (i.e. DNP3) or when multiple applications are used on the network (i.e. A DNP3 RTU on Port A and a Modbus PLC on Port B) it is possible for more than one Remote radio to attempt to access the same Bridge at the same time. This will cause data collisions, and as such it is recommended to use the ChannelShare™ collision avoidance feature. More information on ChannelShare™ digital collision avoidance technology can be found in Part D of this manual.

The Point to Multipoint via Bridge network topology should only be chosen when two or more Bridges are required. If only one “Store and Forward” site is required then the Point to Multipoint with KwikStream™ Repeater network topology offers more bandwidth and lower latency. However, the LinkXtend™ dual antenna feature is only available when a Bridge network is selected.

Remote radios can synchronize to any Bridge or the Access Point in the network. The actual device the remote will synchronize to depends on the Sub-Net ID specified in the remote radio. For more information on Sub-Net refer to [Part D – Features](#)^[29].

The bulk of network specific radio configuration parameters are configured in the Access Point radio. Remotes and Bridges in the network “learn” these configuration options from the Access Point. Remotes and Bridges can be added to the network without need to reconfigure the Access Point.

System wide diagnostics is available from any one remote to any other radio in the network.

4 Part D - Features

In addition to the settings made to establish Radio Type, Network Type, and Subnet ID there are a number of parameters configured in the Access Point radio that can optimize the performance of the J-Series Ethernet radio network.

See:

- [Over the Air Data](#)^[30]
- [Modbus Gateway](#)^[31]
- [Modbus Gateway Mode](#)^[33]
- [Multi-Master Synchronization](#)^[34]
- [Digital Collision Avoidance](#)^[35]
- [Retries and Retransmissions](#)^[36]
- [Ethernet Traffic Filtering](#)^[37]
- [Static and DHCP IP Allocation](#)^[38]
- [Compression](#)^[38]
- [Security](#)^[39]
- [Secure Shell \(SSH\)](#)^[41]
- [HTTPS](#)^[42]
- [SmartPath™](#)^[42]
- [Diagnostics Tools](#)^[49]
- [SNMP Diagnostics](#)^[50]
- [SNMP Notifications](#)^[50]
- [Text User Interface \(TUI\)](#)^[51]
- [Spectrum Analyzer and Channel Lockout Facility](#)^[51]
- [Legacy Serial Support](#)^[52]

4.1 Over the Air Data

All Ethernet data sent over the air is packaged into data packets. These data packets are transported over the network together with a small amount of overhead (or management data).

The total amount of data sent in one single hop depends on the hop interval, RF data rate and the amount of data that is waiting to be sent. The larger the total amount of data, the smaller the ratio overhead compared to user data.

In almost all situations the default settings of the radio will provide the adequate performance. However, under some circumstances, it may be necessary to fine tune specific features so an understanding of how these features work is important.

Radio data rates

The radio data rate determines the over the air speed of the modem. Essentially it defines how much bandwidth is available. The J-Series offers four selectable data rates.

512 kbps with BER of 1E-6 @ -92 dBm
256 kbps with BER of 1E-6 @ -102 dBm
128 kbps with BER of 1E-6 @ -104 dBm
64 kbps with BER of 1E-6 @ -106 dBm

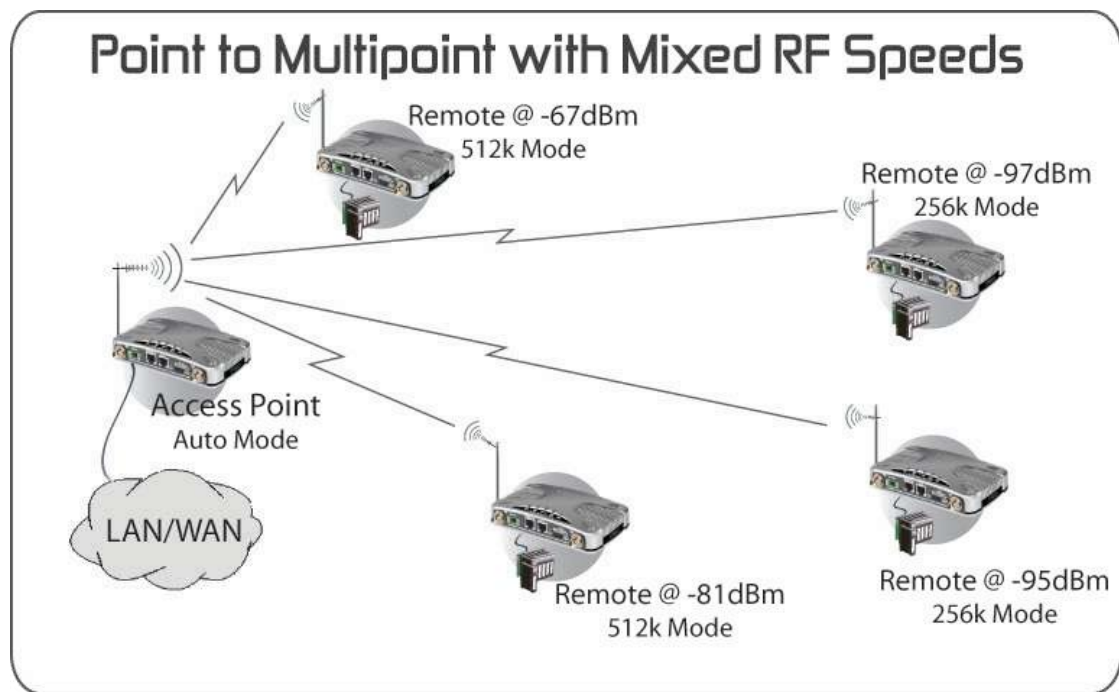
The choice of radio data rates will depend on the level of RF signal strength, but will also depend on other factors like RF noise. In general, higher RF signal levels are required when using the 512 kbps RF data rate, otherwise an unreliable link may result. It may be preferable to start at the lower speed of 256 kbps and change to 512 kbps once the network is configured correctly.

The J-Series also provides the ability to have mixed data rates in one system as shown in the diagram below. In this mode of operation, the J-Series Access Point and only the access point is configured for "Auto Radio Data Rate". Remote radios that have weak signal strength

are then configured for 256 kbps data rates while those remotes with stronger signal strength are configured for 512 kbps data rates.

The auto radio data rate only supports RF data rates of 512 K and 256 K. If RF data rates of 128 K or 64 K are being used, the entire J-Series system needs to be configured to operate at the same speed.

The configuration setting for radio Data Rates can be found in the "Unit Parameters" section of the Radio configuration area of the web programmer.



*The auto radio data rate feature is only compatible with 512 K and 256 K RF speeds.

4.2 Modbus Gateway

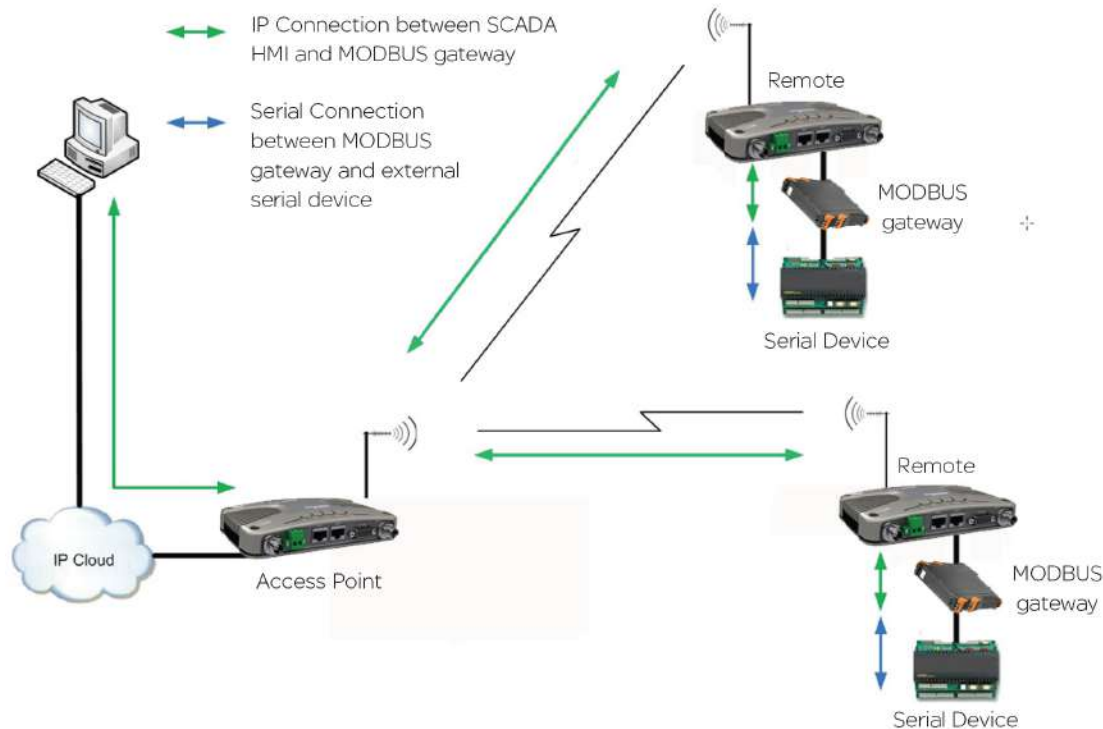
The J-Series has an embedded Modbus Gateway feature that can be enabled to function like an external Modbus gateway. The Modbus gateway is a protocol converter between Modbus/TCP and Modbus RTU protocols. The gateway is an addition to the Device Server feature on the legacy serial port.

When operating in Modbus gateway mode, the remote radio provides the same functionality as if there was an external Modbus gateway at each remote site of the system. In traditional systems, standalone Modbus gateways were required to convert the IP Modbus TCP protocol to Modbus RTU, the example below shows a traditional Modbus TCP system using stand alone Modbus gateways at each remote site.

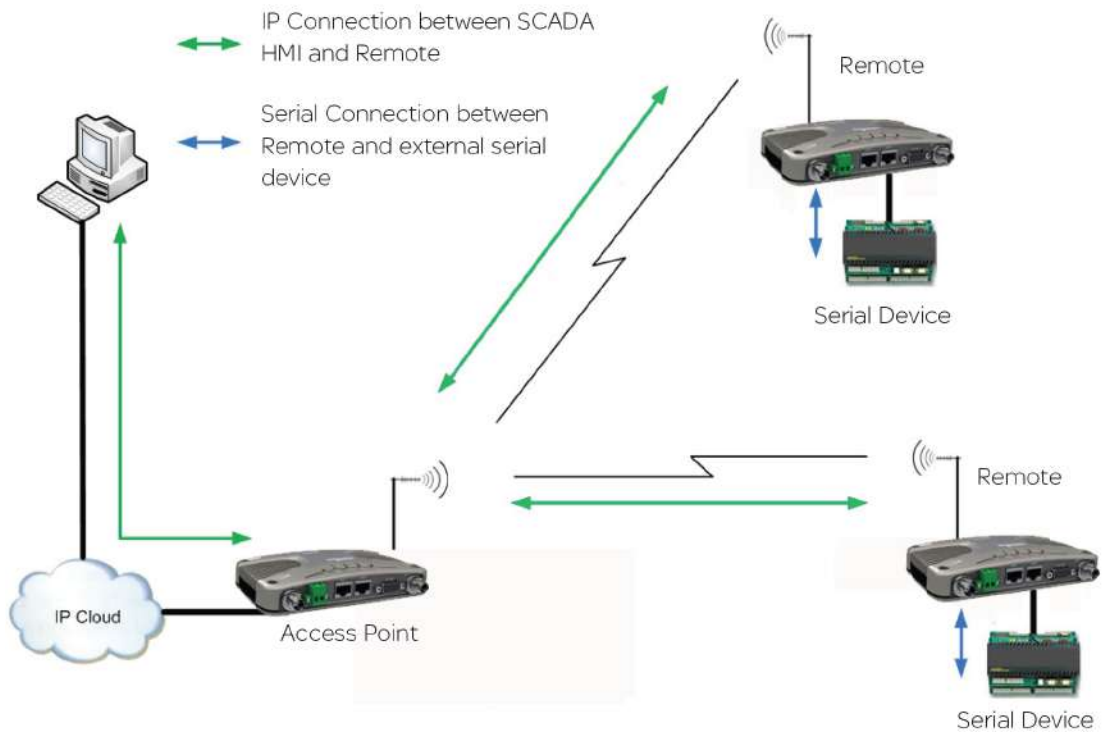
See:

- [Example: Traditional System Without J-Series Embedded Modbus Gateway](#) ^[32]
- [Example: System Using J-Series Embedded Modbus Gateway](#) ^[32]

4.2.1 Example: Traditional System Without J-Series Embedded Modbus Gateway



4.2.2 Example: System Using J-Series Embedded Modbus Gateway



4.3 Modbus Gateway Mode

When operating in Modbus gateway mode, the remote radio provides the same functionality as if there was an external Modbus gateway at each remote site.

Features of the embedded Modbus gateway include:

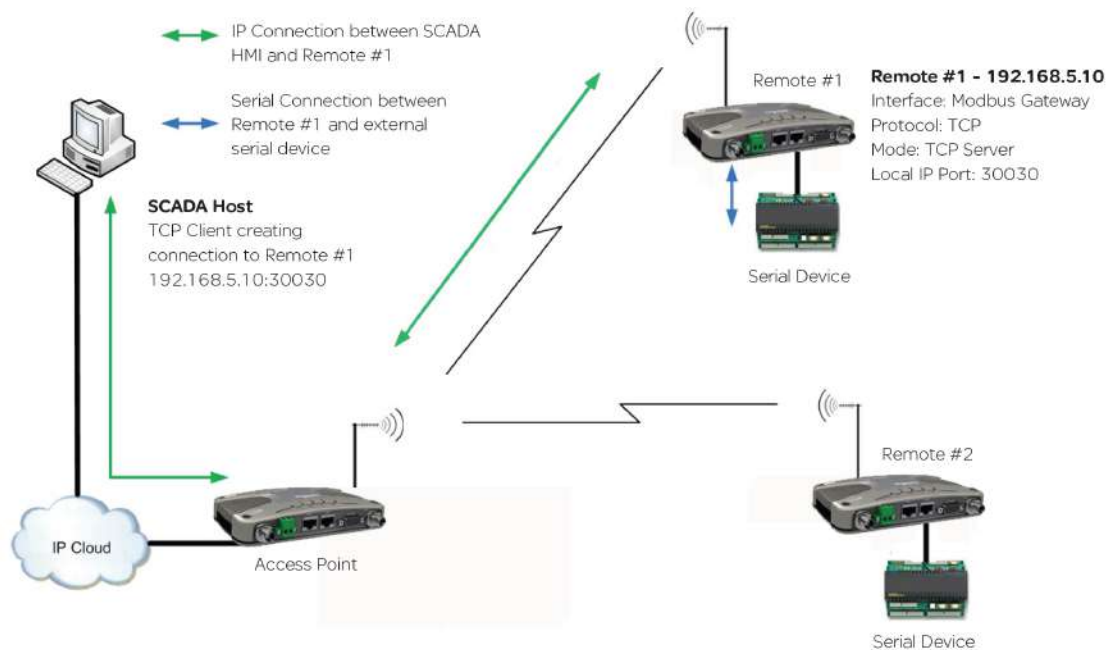
- Support two independent fully configurable Modbus gateways
- Supports two transport protocols; TCP and UDP
- Supports two modes of TCP operation; Client mode and Server mode
- User configurable port numbers
- Supports up to 16 simultaneous TCP connections when operating in server mode

Modbus gateway mode provides an easily configurable mechanism for transporting serial traffic over an IP network (LAN/ WAN). The result of the Modbus gateway feature is that the limitation of Modbus addressing (0...255) can be ignored as the IP address of the radio can be used giving unlimited addresses to external equipment such as RTUs or PLCs. Below is an example of a typical system using the Modbus gateway (remote) feature at each remote site to avoid the limitation of Modbus addressing.

See:

- [Example: Using TCP With J-Series Modbus Gateway Functionality](#) 

4.3.1 Example: Using TCP With J-Series Modbus Gateway Functionality



4.4 Multi-Master Synchronization

When more than one J-Series network shares the same physical site (i.e. antennas for each network are in close proximity) the Access Point (AP) radios can interfere with each other. This interference may occur when one AP is transmitting while the other AP is receiving. The problem is caused by receiver blocking and desensitization.

To avoid this problem, all collocated Access Point radios can be synchronized to transmit and receive at the same time using a special multiple "Access Point" synchronization feature. This feature is enabled by configuring one Access Point radio as the "multi-Access Point primary" Access Point and all other Access Point radios as the "multi-Access Point secondary" Access Point.

A cable is installed between all APs which connects all Pin 9s on the Port A/Port B data ports of all APs along with all pin 5s (GND). Configuration jumpers on the "primary" Access Point set it's Pin 9 as an output. This allows the "primary" AP to generate a synchronization pulse for all "secondary" Access Points, dictating to them when they can transmit and when they need to return to receive mode. In this mode of operation, the transmit/receive duty cycle is 50%.

When operating in this mode, all Access Point radios need to have the same hopping interval and have the appropriate configuration for the General Purpose Pin 9 on Port B (See Port B - Advanced).

Multi-Access Point synchronization divides each hop interval into half - the first half is a dedicated Access Point transmit time slot and the second half is a dedicated receive time slot. Because the Access

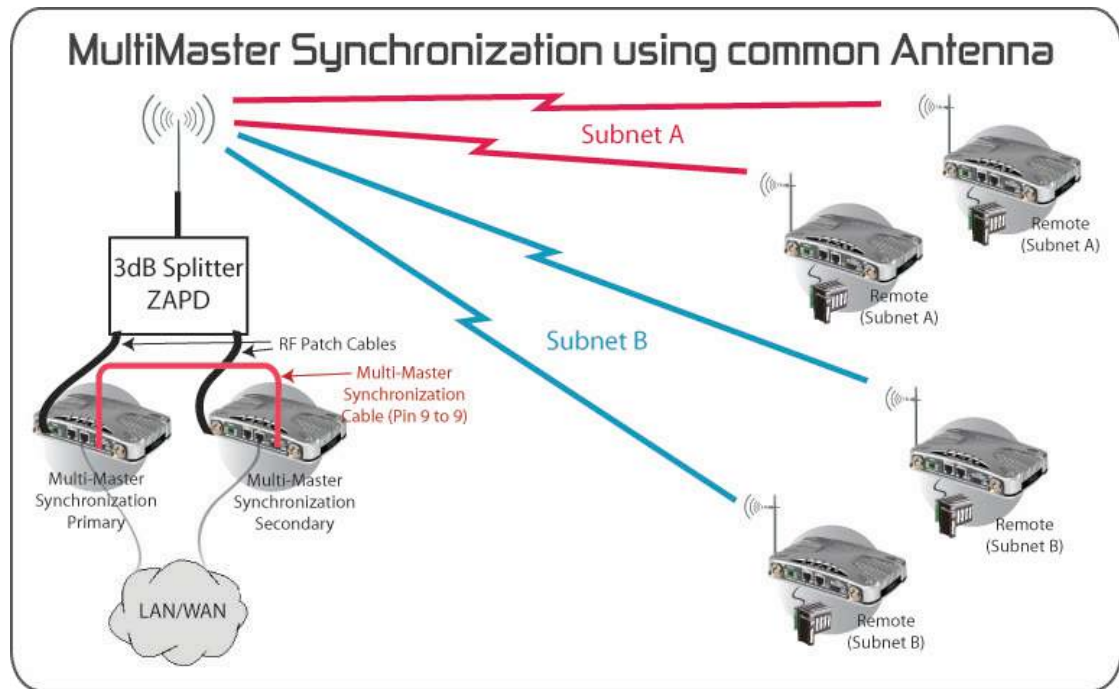
Points each have the same hop interval and each hop interval begins at the same time (as synchronized by the primary Access Point), no Access Point will transmit when the others are in receive mode.

As such, there is no opportunity for desensitization and interference is limited to a very low statistical probability of two radios transmitting on the same frequency at the same time

Multi-Access Point synchronization can also be used in a PTMP system by itself (i.e. even if there is only one Access Point) for the purpose equally sharing the bandwidth in each direction (Access Point to Remotes and Remotes to Access Point).

In some applications it is not possible to mount separate antennas for each Access Point. This may be due to physical (i.e. tower is already loaded to capacity) or economic reasons (i.e. too expensive to mount multiple omnidirectional antennas) or for antenna radiation pattern reasons (i.e. best location for omni antennas being at top of tower). In the above scenarios, it is desirable for multiple Access Points to share one common antenna.

This can also be achieved by using a 3 dB combiner/ splitter as shown in the diagram below. The 3 dB combiner/splitter (Mini-Circuits ZAPD-1 or similar) much provide >25 dB of isolation between ports and be capable of handling 1W (+30 dBm EIRP) RF input powers.



4.5 Digital Collision Avoidance

ChannelShare™

In some network applications there exists the potential for over the air data collisions between REMOTE radios. This can occur when an exception reporting type of protocol is used (such as DNP3) or when multiple applications are being transported over the radio network (such as Modbus and DNP3).

In both of these scenarios, the possibility exists for two or more REMOTE radios attempting to access the channel (i.e. talk to the Access Point) at exactly the same time.

If this occurs, both REMOTE radios are unaware of the other trying to access the Access Point and both will attempt to transmit their data. As such, the Access Point will receive a corrupted message from both radios and a re-try will be required.

ChannelShare™ digital collision avoidance is a type of Access Point controlled channel access scheme that decreases the possibility for over the air data collisions to occur. It achieves this by having any REMOTE (or BRIDGE) with data that needs to be transmitted request permission from the Access Point before transmitting the data. The mechanism which is used to achieve this is called a Token Grant.

Token Grants

When ChannelShare™ digital collision avoidance is enabled, the Access Point radio (or BRIDGE that is behaving as an Access Point for its DOWNSTREAM network) issues "Tokens" to each REMOTE (or BRIDGE) radio that needs to transmit data.

When a REMOTE (or BRIDGE) radio has data packets that need to be sent to an Access Point, it first requests a TOKEN from the Access Point (or BRIDGE) radio. When a TOKEN is requested, the requesting radio includes the amount of data that needs to be transmitted.

When the Access Point radio receives the TOKEN request, it determines a suitable time when the requesting radio can access the channel and transmit its data. The Access Point then grants a TOKEN to the radio wants to access the channel, and the TOKEN includes the serial number of the radio being granted, the starting time and length for which the TOKEN applies. All other radios not granted the TOKEN remain silent during the TOKEN period.

The function of the Access Point is to consider and manage all TOKEN requests and only grant TOKENS in such a way that no two devices accessing the channel will cause a collision.

TOKENs are granted to specific radios, based on their serial number. As such, there is no opportunity for multiple radios to become confused about what TOKEN has been granted.

The process of requesting “permission” to send data and receiving the “OK to Send” response does result in increased data latency and slightly slower data throughput. However, the practical reality of systems where large amounts of exception reporting data need to be handled mean the actual throughput perceived by the user is much higher because the number of over the air data collisions is significantly lower.

All radios in the network also employ a small amount of random channel access backoff timing so that when a TOKEN has expired, requests for TOKENs to be granted are not themselves the subject of a large number of over the air data collisions.

4.6 Retries and Retransmissions

No Ack retries

Data transmitted from a REMOTE to an Access Point is acknowledged by the Access Point. No Ack Retry Limit defines how many times the REMOTE attempts to transmit data to an Access Point if NO acknowledgment arrives from the Access Point for the previous attempt by the REMOTE.

Once the No Ack Retry Limit is reached, the data is discarded by the REMOTE. The important point to note is that the No Ack Retry mechanism does not have any bandwidth penalties as it is only required when interference prevents the successful delivery of data to the Access Point radio.

Retransmissions

Except in PTP modes, data transmitted from an Access Point (or BRIDGE) to a REMOTE is not acknowledged by the REMOTE. Data Retransmissions define how many times the Access Point (or BRIDGE) duplicates (or re-transmits) data to the REMOTES. The theory is that even if the REMOTE is subject to interference, at least one of the messages will be received. Duplicate messages are discarded by the REMOTE. Each data re-transmission results in less usable bandwidth in the Access Point to REMOTE direction. However, in a practical system it is a more efficient method of preventing lost data than waiting for the SCADA system to timeout and try again.

Force retransmissions across hops

For increased reliability and protection from other radios operating in the vicinity, it is possible to force the re-transmissions to occur in different hops. The data is first transmitted in one hop and then the second re- transmission takes place on the next hop. This method helps to ensure that each re-transmission will be sent on a different frequency within the hop pattern of the radio and so avoids fixed frequency interference. However, there is a larger decrease in usable bandwidth in the Access Point to REMOTE direction when re-transmissions are spread across multiple hops. To minimize the loss of bandwidth, it is recommended to choose a shorter hop interval.

4.7 Ethernet Traffic Filtering

As of firmware release V3.1, the J-Series radios implement several features to reduce the amount of redundant on air traffic so that higher actual bandwidths may be achieved. These features add no additional latency to the network, they require no configuration and improve bandwidth. As such they are always enabled.

Peer to peer repeat filtering

This feature greatly improves the available bandwidth in systems where peer to peer connectivity is required. The filtering is implemented in within the Access Point (or Bridge) of PTMP or PTMP/B systems. Essentially it helps to prevent the unnecessary repeating of Ethernet traffic which is inherently point to point in nature (i.e. a TCP session).

When two remote radios need to communicate with each other (often referred to as Peer to Peer), the Access Point (or Bridge) will repeat the traffic to provide peer to peer connectivity.

However, if the traffic is from a Remote to an AP (or Bridge), then peer to peer repeating is not required and the AP (or Bridge) does not repeat the traffic. The AP (or Bridge) learns what devices (MAC addresses) do not require repeating. Broadcast traffic is always repeated. By learning where devices are located on the network, the route table does not require any special configuration or setup.

Unicast transmissions and data acknowledgments

This feature provides an improvement in downstream bandwidth (i.e. From AP to Remote) as it prevents unnecessary retransmissions of data from AP to Remote (i.e. retransmission blindly transmit data multiple times). When the AP (or Bridge) detects that data is being unicast (i.e. sent to one remote device only), the AP (or Bridge) swaps from retransmission of data (i.e. blindly sending data multiple times) to data acknowledgment mode (No Ack Retires).

Essentially the AP (or Bridge) briefly swaps to a PTP mode of operation during the transmission of this unicast data. The remote radio acknowledges this unicast data from AP which in turn allows AP to send data to remote without the need for blind retransmissions. The acknowledge process is described earlier in this user manual. Refer to [Retries and Retransmissions](#)^[36].

When the AP (or Bridge) detects the traffic is of a broadcast or multicast type, the AP (or Bridge) returns to normal PTMP mode where traffic is retransmitted as per the normal process.

Upstream and downstream filtering for bridge radios

This feature helps to prevent unnecessary transmission of data either upstream or downstream of a bridge. It is useful for systems where Ethernet devices are connected to bridges. The bridge learns which direction (either upstream or downstream) the traffic needs to flow and filters out the traffic accordingly.

Configurable Ethernet filtering

Ethernet filtering provides an easy to configure filtering mechanism which can help to prevent unnecessary Ethernet traffic increasing channel loading. Although typical SCADA applications only require Unicast and ARP data, the filtering mechanism provides the option to allow:

- All Ethernet traffic
- Unicast & ARP only
- Unicast only
- or only allow data from a single MAC address

Although Spanning tree messages are multicast messages, they are also filtered out unless the user is allowing all Ethernet traffic to pass. This is also to help prevent unnecessary channel loading.

4.8 Static and DHCP IP Allocation

The J-Series radio give you the choice of IP allocation, via either Static or Dynamic (DHCP) IP address allocation. The choice of which to use will normally depend on the network you are integrating the radio into or the type of application you are trying to use the radio for.

Most large corporate environments utilize the DHCP method where a DHCP server dynamically assigns an IP address when requested to devices connected to its network. This allows for very large networks to be managed very easily without the need for complex IP address tables to be maintained.

Static IP address allocation is used in smaller environments or where the application being used requires a constant IP address for correct operation. The type of IP allocation should be discussed with your network administrator is connecting to an existing network or decided in the network design phase to help ensure correct operation.

4.9 Compression

In determining whether to use compression or not the type of application and the latency requirements are the most important considerations. A knowledge of your data transmission is needed to help ensure that no adverse effect on the data transmission occurs. Applications such as video or Audio are suitable to the use of compression as these data types are typically very noisy and the application of compression removes a lot of noise and causes no noticeable loss of quality. Straight data application are not suited to the use of compression as it will increase the latency and the possibility of data Loss would be increased.

Hopping intervals

Frequency Hopping Spread Spectrum (FHSS) radios like the J-Series operate in an unlicensed shared frequency band and collisions can be expected when multiple radios are operating in the same area.

Due to the hopping nature of the radio, the radio “hops” between a specific number of distinct frequencies in a specific pattern. The length of time that the radio remains on any one frequency is called the “Hopping Interval”. Data is transferred between radios during this time.

Once the hopping interval has expired, the transmitter (if active) is stopped, and all radios in the system “hop” to the next frequency in the hopping pattern. Whilst the radios are hopping, no data can be transferred between radios.

When two radios in the same area are transmitting on the same unique frequency, a data collisions may occur and this will help prevent successful data transfer until one or both radios “hop” onto another frequency.

Shorter hop intervals will reduce the amount of time that any such collisions may impact on the radio link and as such will make the radio link less susceptible to interference. However, the usable bandwidth of the radio will be reduced because the ratio of time spent hopping to a new frequency vs time spent transmitting data is higher.

Longer hop intervals will increase the amount of time that any such collisions may impact on the radio link and as such will make the radio link more susceptible to interference. However, the usable bandwidth of the radio will be increased because the ratio of time spent hopping to a new frequency vs time spent transmitting data is lower.

The radio will default to a Hopping Interval of 100 mS. For most systems, this setting provides a good balance between susceptibility to interference vs usable bandwidth.

4.10 Security

Frequency Hopping Spread Spectrum radios offer a high level of security because it is not possible to eaves drop on data transactions without knowing the hopping pattern being used and having proprietary knowledge about how the data is encoded.

Unlike 802.11 and WiFi equipment which can be purchased “off the shelf” the Schneider Electric Trio J-Series employs many levels of defense against potential security threats.

Security layers

The J-Series Radio employs several layers of security. Each layer is detailed below.

1. **Network Name:** The Network Name is used to derive the hopping pattern. The Network Name needs to be identical in all radios in the Network.
2. **Trusted Remotes/Access Points:** If enabled, only serial numbers in the Trusted Remotes/Access Points list can be communicated with. Serial numbers are unique and factory set. They can not be manipulated by the user.
3. **Encryption:** All data is encrypted with a 256-bit AES encryption key. If enabled, the same key needs to be used in all radios.

Password protected web site interface

When enabled the user will be required to enter a password to enter the web site interface to access the configuration of the radio.

Trusted access points and trusted remotes

Trusted Remotes

Access Point radios can be configured to communicate only with a list of trusted REMOTE radios. If any serial numbers of trusted remotes are entered into the "Trusted Remote List" then communications will only occur with radios entered on this list. If the list is empty, then communication can occur with any remote and this security feature is disabled. Up to 63 trusted remotes can be specified.

Trusted Access Points

REMOTE radios can be configured to communicate only with a list of trusted Access Point radios. If the Access Point radio serial number is in the "Trusted Access Point" list the communication can only occur to this Access Point. If the list is empty, then communication can occur with any Access Point that has the correct Network Name. Up to 4 trusted Access Points can be specified.

By entering any serial number into either the "Trusted Remote" or "Trusted Access Point" lists, this security feature is enabled and the radios will only communicate with radios defined on their trusted list, if these lists are empty the radios will communicate with any radio having the correct network name.

Encryption

When encryption is enabled in a network, all data sent over the air is more protected from eavesdropping and can only be read by radios sharing the same Encryption Key.

Encryption needs to be enabled in each radio in a network. The encryption key is 256 bits long and is entered as string or a hexadecimal number. For maximum security the key chosen should be one that is difficult for an intruder to guess.

Once written into the radio using the programmer, it is not possible to read the encryption key so record the key in a safe place.

Encryption key: string

For a string type of key, use up to a maximum of 32 printable characters. Note that the key is case sensitive.

Some examples are:

- TRIO2012
- Murray River Region

Encryption key: hexadecimal number

Hexadecimal numbers can have a value of 0...15 and are represented by 0...9 and A, B, C, D, E, or F

A hexadecimal key begins with 0x and has up to 64 digits following

Some examples are:

- 0x123
- 0x123456789ABCDEF
- 0x11111111222222223333333344444444 up to 64 digits

4.11 Secure Shell (SSH)

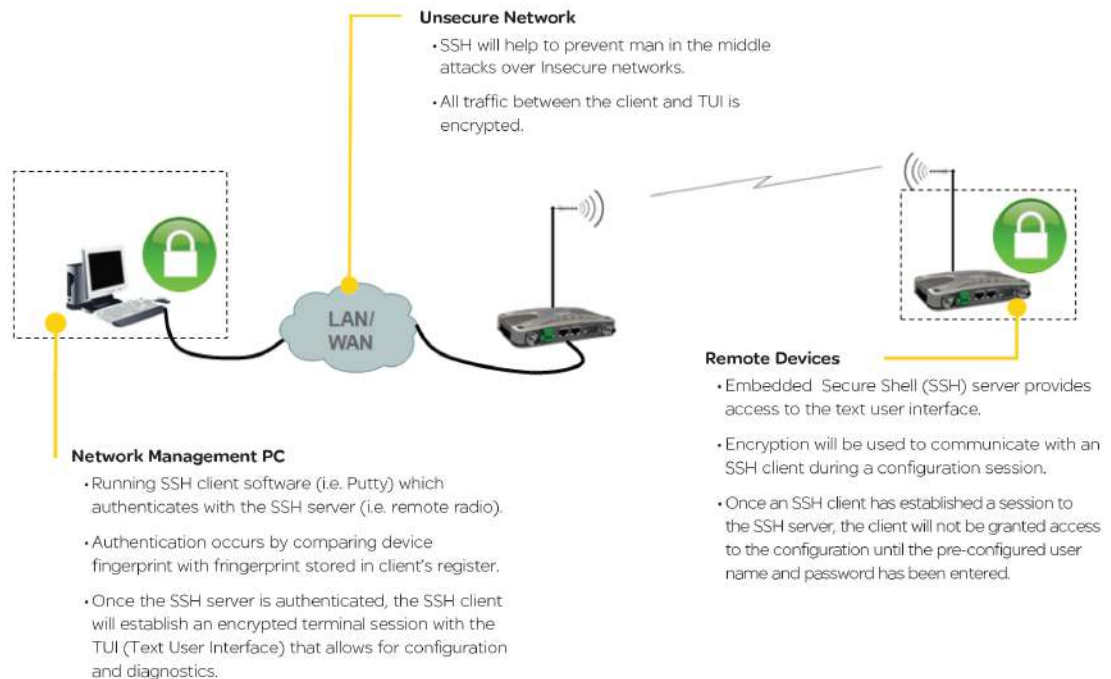
SSH provides a more secure and authenticated method for remotely accessing the J-Series text user interface (TUI) for configuration and diagnostics.

To access the J-Series via SSH, the network management PC requires an SSH capable program (i.e. Putty). All traffic over the SSH connection is encrypted.

During the first connection to the SSH terminal software, a “fingerprint” of the remote device is taken and stored on the Network Management PC. This allows for authentication in the future.

The SSH session also requires the user to enter a username and password for authorized access to the TUI.

4.11.1 SSH Example



4.12 HTTPS

HTTPS provides a more secure and authenticated method for remotely accessing the J-Series Web User Interface (WUI) for configuration and diagnostics.

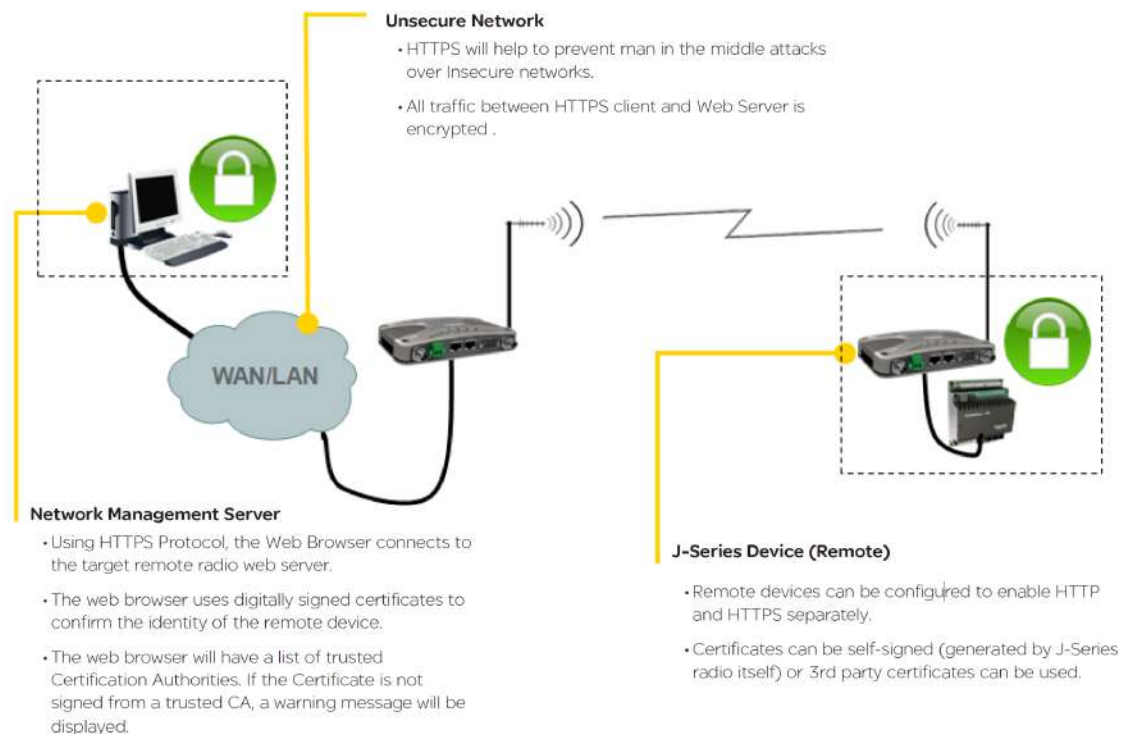
To access the J-Series via HTTPS, you need to use a browser which has HTTPS capabilities. Common Web browsers which will provide HTTPS capabilities include: Internet Explorer, Firefox, Chrome, etc.

The HTTPS client (web browser) will request a digitally signed certificate from the HTTPS server (J-Series) to help ensure that the target device is authentic.

All traffic over the HTTPS connection is encrypted.

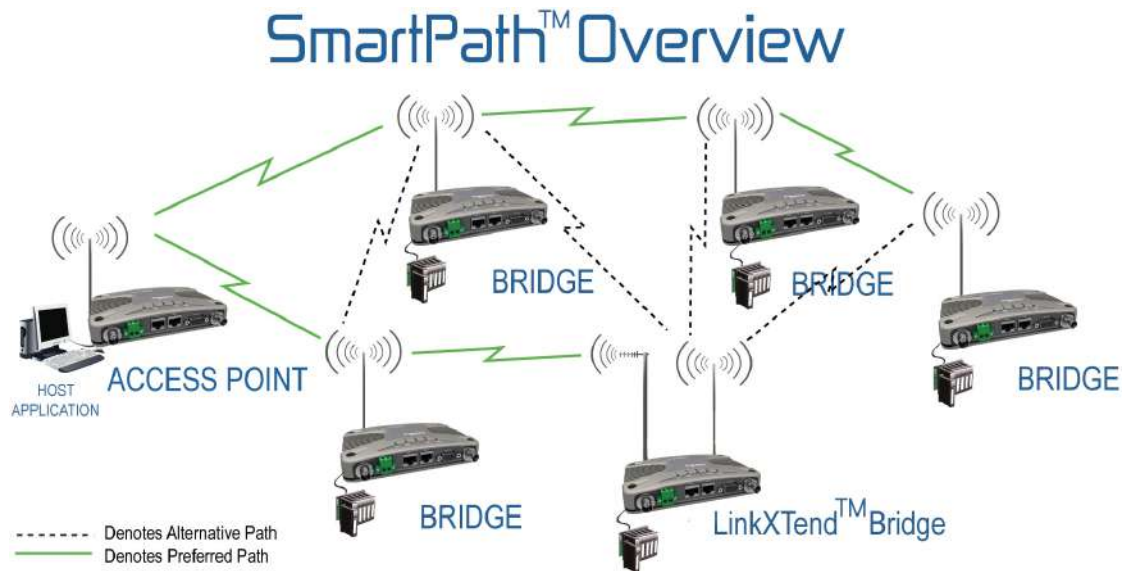
Two methods of certificate management are available: Self-signed certificates generated by the radio itself or the use of certificates generated by external certificate servers.

4.12.1 HTTPS Example



4.13 SmartPath™

The J-Series radio provides unique features to enhance connectivity and redundancy in both fixed and mobile applications. Typical SCADA and Telemetry systems require a high degree of radio link reliability. Using SmartPath™ features together with a small amount of system planning, the system designer can create a network topology that provides for multiple alternative radio link paths. This type of network is often referred to as a MESH network and a typical example is shown below. Note that the “Master” of the network for J-Series is referred to as the Access Point.



SmartPath™ has been optimized for SCADA and Telemetry systems, providing an ideal balance between connectivity (i.e. link reliability), latency, bandwidth and system design effort. Many peer to peer MESH networks are optimized for short range, high density networks. As a result, much of their over-the-air bandwidth can be consumed in radio protocol management overhead (i.e. keeping track of where peers are in the network, re-configuration of priority paths, etc).

SmartPath™ only re-configures the network topology when it is required. During normal operation, the system designer can utilize all of the over-the-air bandwidth and minimize message latency. Should one of the critical path radios fail, those radios dependent on that failed radio will search for alternative paths via other radios. The system designer can optimize radio path connectivity using a preferred/alternative arrangement. In applications where radios are mobile or roaming, SmartPath™ can provide an unlimited number of coverage areas including the ability to reliably hand-over coverage from one radio to another based on usable received signal strength.

4.13.1 SmartPath™, Network Name, and Hopping Patterns

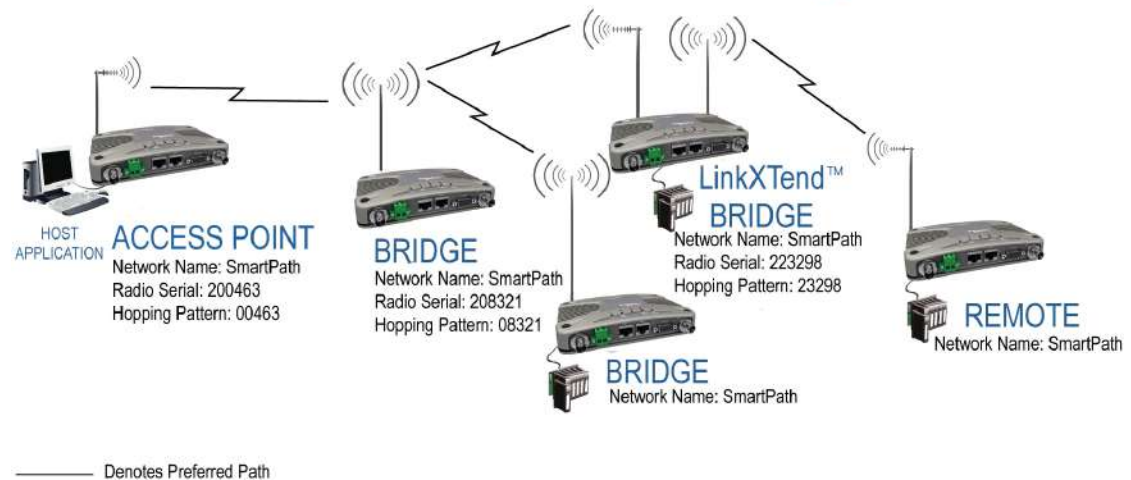
A fundamental rule of all J-Series radios (remotes or bridges) is that they will only synchronize to networks which have a matching Network Name. When implementing a network with Bridges, each section of the Network is broken up into smaller “Subnets” which is described in [Part C – Network Types](#) ^[23].

To help prevent interference between each Subnet, a unique hopping pattern is required for each Subnet. To make configuration management easier for the user, the J-Series (by default) derives the hopping pattern from the Network Name. Note: Only the Access Point (or a Bridge in Access Point mode) derives the hopping pattern from the Network Name. A remote (or Bridge in Remote mode) will find any Access Point on any hopping pattern, and then check to see if the Network Names match.

SmartPath™ allows the user to provide alternative paths for radios in any one network. To implement this, the Network Name needs to be identical in all radios which may need to provide an alternative path. In this scenario, the hopping pattern can no longer be derived from the Network Name since the Network Name needs to be the same in all radios. Failure to break the link between Network Name and Hopping Pattern would result in the hopping pattern being the

same in all radios in all Sub- Nets when the desired outcome is to have a unique hopping pattern for each Subnet.

Network Names and Hopping Patterns



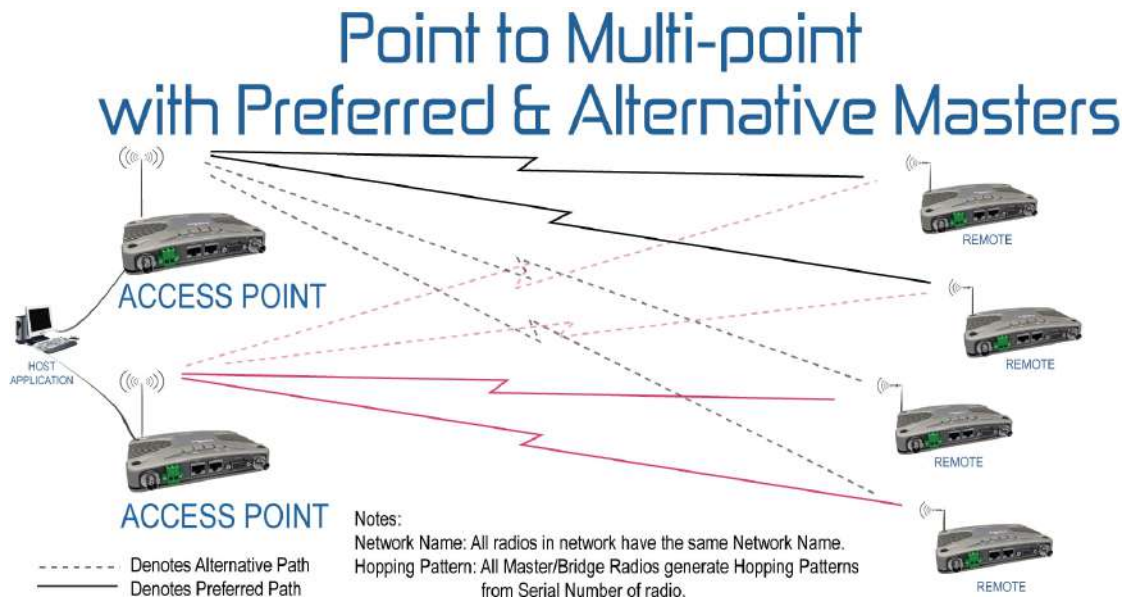
To overcome this problem, an option is provided to allow the generation of the hopping pattern from the serial number of the Access Point or Bridge radio.

Shown above is a diagram showing a typical SmartPath™ enabled system. The following points should be noted:

- The Network Name is common to every radio in the system
- The hopping pattern is generated from the Access Point (or Bridge) serial numbers
- Radios which normally function as remotes, but can provide an alternative path, are now configured as Bridges

4.13.2 SmartPath™ and Preferred/Alternative Access Points

SmartPath™ allows system designers to create redundant connection paths that help to negate single point failures. Consider the PTMP network shown below. In this network, the system designer requires that Remote radios quickly re-synchronize to an alternative Access Point should the preferred Access Point no longer be accessible. When the preferred Access Point has been restored and is accessible, the network needs to resolve itself to match the preferred topology with a balance in the number of remotes associated with each Access Point.



Typically, a PTMP system has one Access Point that communicates with several (many) remotes. If that Access Point fails, then the remotes configured to associate with that Access Point will lose connectivity. With SmartPath™ technology, the system designer can install multiple redundant Access Point sites and the remotes can be configured to associate with any of those Access Points.

The designer can also configure a preferred Access Point as well as up to three alternative Access Points should the preferred Access Point fail. The system designer only then needs to help ensure that the alternative Access Points have adequate overlapping signal strength at each remote site. If the Access Point radios are located at the same site, Multi-Access Point synchronization should be activated to help prevent unnecessary interference between each Access Point. Refer to [Part D – Features](#) ²⁹ for more information on Multi-Access Point synchronization.

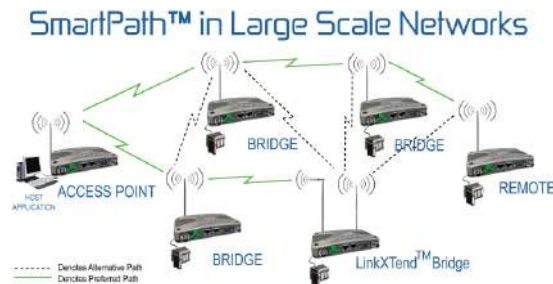
The use of SmartPath™ preferred/alternative mode helps to ensure that during normal operation, remotes are evenly distributed across available Access Points. This assists the network designer in balancing the load by limiting how many remotes are associated with each Access Point. Only during an interruption of one Access Point would those remotes reacquire an alternative Access Point. The channel loading on the remaining Access Point site would increase and the user may observe an increase in response time (i.e. increase latency due to the larger number of remote sites). In SCADA and Telemetry applications this is a much preferred outcome as opposed to total loss of remote site connectivity.

The time taken to acquire an alternative Access Point is proportional to the hopping interval and the number of channels the radio hops over. In general, the nominal synchronization time can be calculated by multiplying the number of channels the radio hops over by the hopping interval.

When the inoperative Access Point site has been restored to correct operation, the Remote radios will resolve themselves to match the preferred topology. This happens because when a Remote radio is associated with an alternative Access Point, it will break synchronization after a predefined time (normally 10 to 30 mins) and attempt to find the preferred Access Point. This time is known as the Access Point Reacquisition Time and is explained in the following example.

4.13.3 SmartPath™ PTMP Using LinkXtend™ Bridges

SmartPath™ allows the user to create multiple redundant connection paths in complex PTMP systems using LinkXtend™ bridges. Consider the PTMP with LinkXtend™ network shown below. The system designer requires that each unit synchronizes to the network as quickly as possible, even if the topology is not initially the preferred one. Over time the network needs to resolve itself to match the preferred topology.



Similar to the previous example, each Bridge or Remote in the network is configured to associate with multiple Access Points. Due to the split personality of the Bridge (Half-Access Point/Half-Remote) each Bridge site in the network is capable of providing an alternative path to the Access Point for any other radio in the network.

The system designer can configure a preferred Access Point, but may also specify up to three alternatives should the preferred Access Point become inoperable. The alternative Access Points for a specific site would be any other Access Point or Bridge radios that have adequate signal strength. All sites that need to provide alternative paths should be configured as Bridges. The Bridges can be single or dual antenna bridges depending on RF requirements.

The use of SmartPath™ preferred/alternative mode helps to ensure that during normal operation, the network remains in the optimum or preferred topology. This assists the network designer in balancing connectivity vs latency. Only during a breakdown of a site in the preferred topology will other sites that are dependent on that inoperable site need to reacquire alternative paths. When operating via alternative paths, the user may observe an increase in response time (i.e. increase latency due to the larger number of hops via bridges). In SCADA and Telemetry applications this is a much preferred outcome as opposed to total loss of remote site connectivity.

4.13.4 Access Point Re-Acquisition Time

SmartPath™ is optimized to provide remote synchronization (i.e. connectivity) as quickly as possible. This is important for SCADA systems where minimization of outage time is critical. To provide synchronization as quickly as possible, a Remote configured for SmartPath™ will synchronize to the first available Access Point (or Bridge) it can find, regardless of whether or not that Access Point (or Bridge) is the preferred unit. The time taken to find an available Access Point (or Bridge) will depend on the hopping interval. Smaller hopping intervals will result in faster synchronization times. A more detailed discussion on hopping intervals can be found in Part D of this User Manual.

On startup, if a Remote synchronizes to its preferred Access Point (or bridge) first, then it will remain synchronized unless a loss of signal from the Access Point (or Bridge) occurs.

However, if the Remote synchronizes to an alternative Access Point (or Bridge) first, it will remain synchronized to the alternative Access Point (or Bridge) for a limited length of time. This

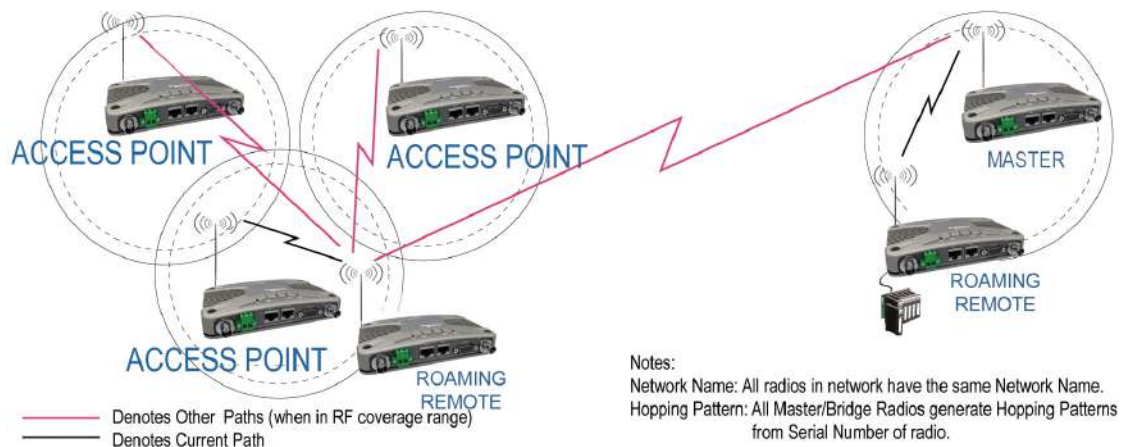
time is specified in the “Access Point Reacquisition Time” configuration parameter. This time is normally 10 to 30 minutes but can be configured from 1 to 255 minutes. When the time expires, the Remote will automatically de-synchronize and look for another Access Point.

The Remote is not guaranteed to find the preferred Access Point on first attempt, but statistical variation will help to ensure that eventually the Remote will find it's preferred Access Point if it's signal can be received. Once found, the Remote will no longer search for any other Access Point. This mechanism provides the best balance between connectivity and orientation of the network topology in preferred way. Over time, the network resolves itself to match the user defined preferred topology.

4.13.5 SmartPath™ and Roaming Remotes

SmartPath™ allows the user to design networks that permit Remote radios to roam. In a roaming network, a remote is typically installed on a moving vehicle or object, such as a truck or a train. Access Point radios are installed at key locations where good RF coverage can be provided. The desired outcome is for connectivity to any available Access Point. In this scenario, there is no requirement to configure a preferred or alternative list of Access Points. The trusted Access Point list remains empty, and the roaming remote radio will associated with any Access Point it can find that has the appropriate network name.

SmartPath™ Roaming Remote



4.13.6 RSSI Threshold and Roaming Remotes

SmartPath™ has a feature that allows the user to help prevent excessive Access Point hand-overs due to inadequate RF signal strength. Refer to the diagram shown above. In this scenario, several Access Points have been positioned or located together to provide over-lapping coverage. The outer circle represents the range of usable signal strength from that Access Point. To help prevent Remote radios from synchronizing to Access Points that do not currently provide adequate levels of received signal strength, RSSI Threshold filter facility can be enabled.

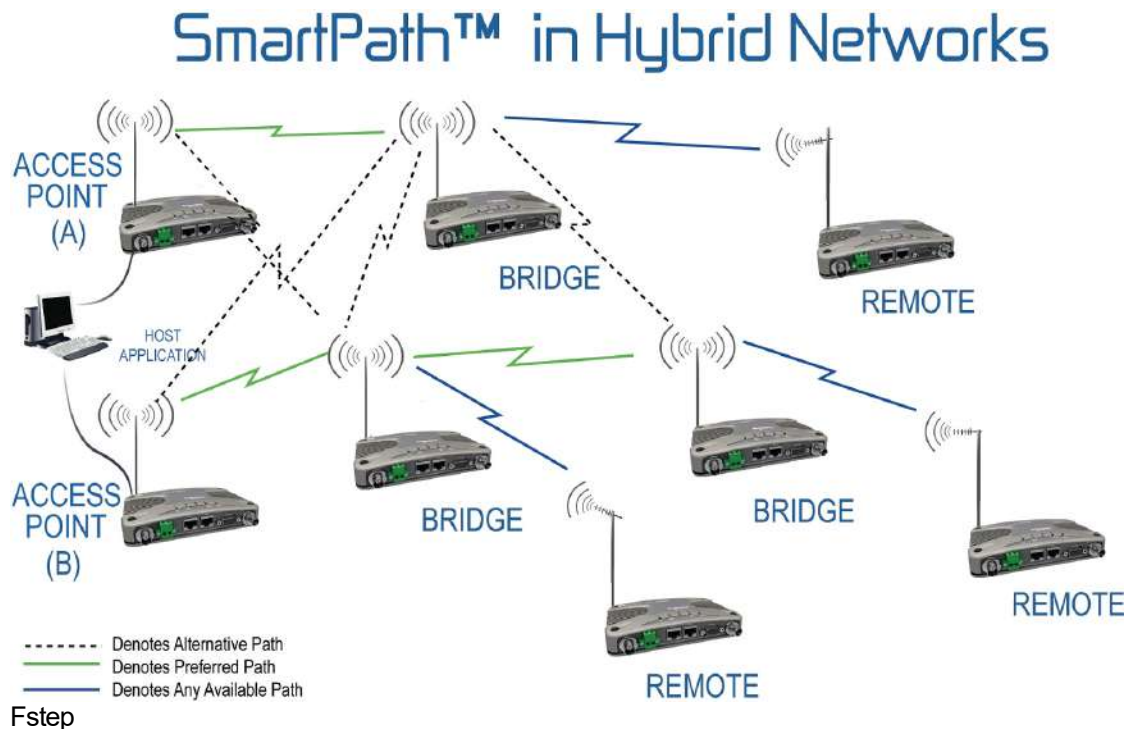
The RSSI Threshold defines the minimum acceptable received RSSI level before a radio will synchronize to an Access Point. When a Remote finds an acceptable Access Point in the network, it first checks to ensure that the received RSSI is above the RSSI Threshold. If the

received RSSI is below the threshold, the Remote radio will continue to search for other Access Points. Once synchronized to an Access Point, the Remote will remain synchronized until the RSSI level is 10dB below the threshold (i.e. a 10dB hysteresis is applied). When the RSSI drops below this value, the remote searches for new acceptable Access Points with a received signal strength above the RSSI Threshold.

For example, if the RSSI threshold is configured to be -80 dBm, then when a remote detects the current Access Point is being received at -90 dBm, the remote will drop synchronization with that Access Point and start searching for another Access Point with a signal strength of -80 dBm or better. This helps to ensure that Remotes which are in the range of other Access Points with more usable signal strength do not remain associated with their existing Access Point at very low or inadequate signal strengths.

4.13.7 SmartPath™ and Hybrid Networks

SmartPath™ allows the system designer additional flexibility to create a redundant backbone based on preferred and alternative paths while deploying remote radios where no configuration is required. This is shown in the network diagram below.



Two Access Points are installed to provide redundancy at the Access Point radio level. These Access Points may be located at different sites, or they may be co-located. If co-located, the user should implement Multi-Access Point synchronization to help prevent interference between Access Points.

Three key sites in the network (typically sites where good RF coverage can be provided) are configured as Bridge radios. These can be single antenna Bridge radios or dual antenna LinkXtend™ bridges depending on the path profile and link requirements. The system designer could then configure preferred and alternative paths between the Access Points and Bridges as required.

4.13.8 Configurationless Remotes

In some system designs, there will be occasions where radios located on the fringe of the network do not need to provide an alternative path. Since these radios will not be carrying additional network traffic, there is no need to configure a preferred or alternative path. Instead the Remote radio is configured to synchronize to any available Access Point radio that has the configured Network name. The system designer can deploy Bridge radios to provide overlapping RF coverage which would allow a remote to have two possible paths to an Access Point. It is recommend to use the RSSI Threshold feature to help prevent a Remote radio from associating with an Access Point that has poor signal strength. There is no limit to the number of possible Access Points (or Bridges) a Remote radio can associate with in this mode of operation.

The benefit of configuring Remotes in this mode of operation is that they are essentially Configurationless. Apart from the user configuring the required User Port, TX Power and Network Name, there is no other configuration required. The user does not need to enter preferred or alternative Access Points and this allows Remote radios to be pre-configured before deployment into the system.

4.14 Diagnostics Tools

As of firmware release V3.1, the J-Series radios implement SNMP access to radio diagnostics as well as providing embedded (web) diagnostics and commissioning features.

Radio Diagnostics

The J-Series radios include the ability for installers to review useful radio & Ethernet diagnostics parameters. The parameters include unit specific (date & time), network specific (Ethernet traffic) and radio specific parameters (Tx Power, DC volts, etc).

Diagnostics can be accessed via the HTML Interface or using the TVIEW+ Diagnostics suite (either via e-Diags Ethernet or directly via Port B using a serial port). Diagnostics can also be accessed via SNMP.

Diagnostics

Start Auto Refresh

5

s

Unit

Date

Thu Jan 1 02:32:26 1970

Up Time (sec)

9146.14

CPU Load

0.64

Network

Eth0 Rx Packets

0

Eth0 Rx Bytes

0

Eth0 Tx Packets

2

Eth0 Tx Bytes

168

Eth1 Rx Packets

0

Eth1 Rx Bytes

0

Eth1 Tx Packets

4

Eth1 Tx Bytes

316

Radio

Radio Rx Packets

22946

Radio Rx Bytes

2456778

Radio Tx Packets

110

Radio Tx Bytes

47223

Radio Reverse Power (dBm)

12.8

Radio Forward Power (dBm)

20.2

Radio RSSI (dBm)

-58.6

Supply Volts

11.9

Radio Temperature (C)

26.1

Radio Synchronized

Yes

Lost Sync Count

2

Failed Tokens

0

Retired Packets

0

Failed Packets

0

Diagnostics Logs

The J-Series radios include the ability measure radio diagnostics and performance statistics over a period of time. This facility is known as the diagnostics log. The diagnostics log can display data at a low, medium or high frequency depending on how often you want an update. The diagnostics log can also be saved to a CSV file for further analysis.

Packet Error Testing

When commissioning a radio link, it is useful to generate Ethernet traffic to test the link for functional performance. One method of generating traffic is using the “ping” utility provided on MS Windows based operating systems. Another method is to perform a packet error test. This can be done using the “Indicative Packet Error Test” facility provided in the J-Series radio.

To perform the test, the user specifies the destination radio serial number, number of packets to send and size of packets (in bytes). The test facility will then execute the test and provide the results, which can then form part of the commissioning process. For more information, refer to [Part H – Installation & Commissioning](#) ^[124].

4.15 SNMP Diagnostics

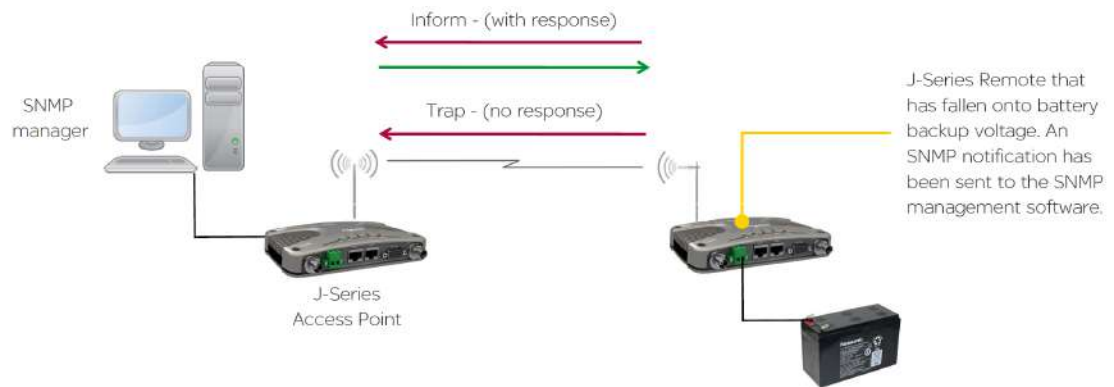
As of firmware version v3.5.0, the J-Series can provide SNMP diagnostic data via an internal SNMP agent. The radio supports SNMP v1 & v2c along with notifications which includes traps and informs. SNMP facilities include RFC1213, Ethernet diagnostics and radio diagnostics.

Schneider Electric supply .MIB files that can be imported into most major SNMP Management consoles. These .MIB files define the contents of the SNMP parameters including a description for each parameter. The parameters are sorted into six distinct groups. The general group, the radio group, the security group, the LAN group, the error group and the notification group. More information on SNMP can be found in Part F of this user manual.

4.16 SNMP Notifications

As of firmware version 3.5.0, the J-Series has the capability to send SNMP notifications. An SNMP notification is a message to inform a user that some sort of state of the radios has changed, these states include; input voltage, temperature, Tx power, etc. There are two types of SNMP notifications available which are traps and informs.

- A trap is a single UDP message that is sent from the J-Series to an SNMP manger.
- An inform is still a UDP message, however, an inform requests a response to the UDP message sent. This allows re-trys and time outs to be used within the radio.



4.17 Text User Interface (TUI)

As of firmware release V3.6, the J-Series radios provide a text user interface which can be accessed via Telnet, SSH and Serial connections. The text user interface (TUI) provides an alternative mechanism for managing the radio configuration and accessing radio diagnostics.

The TUI provides a very high speed interface even over radios links that are suffering from high error rates.

Online help is also provided by the TUI. The spectrum analyzer and channel lockout can only be accessed via the TUI. See [Spectrum Analyzer and Channel Lockout Facility](#) ⁵¹.

The TUI can be accessed via a Telnet "session" using any one of the common Telnet based terminal programs, including the native "Telnet" facility provided with Microsoft Windows based operating platforms.

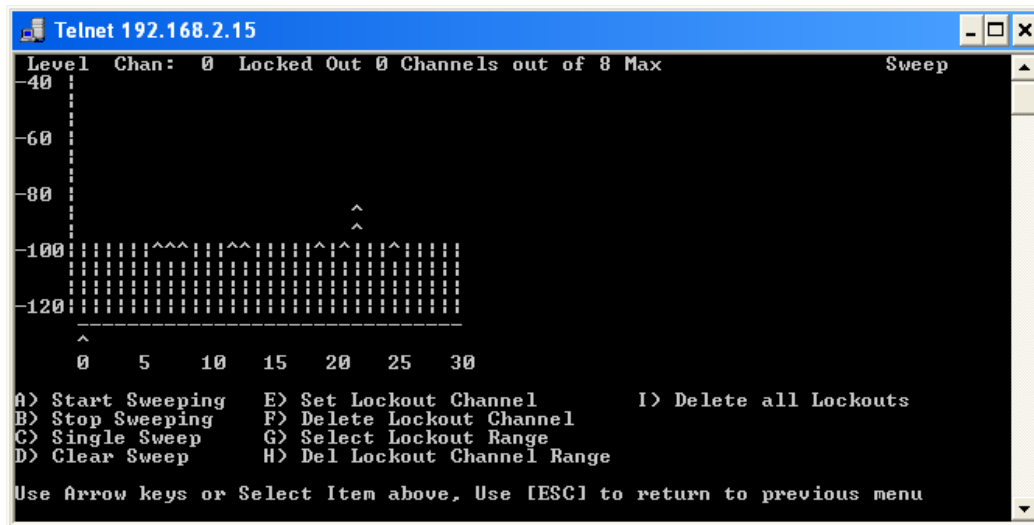
The J-Series can also enable an embedded SSH server

Alternatively, the TUI can be access via the serial data port using a standard RS-232 interface cable. This can be useful when the IP address of the radio is not known (or has been lost).

4.18 Spectrum Analyzer and Channel Lockout Facility

As of firmware release V3.1, the J-Series radios support a spectrum analysis and channel lockout facility*

This feature allows the user to perform a spectrum analysis and lockout channels that may be occupied.



The spectrum analysis facility is only available on any radio type. However, only on the Access Point and Bridge radios can you lock out channels. This is because the Access Point and/or Bridge radios are the only types of radios that specify what hopping pattern is in use, as well as what channels are excluded from that pattern.

*The spectrum Analyzer and channel lock out facility is not available on Brazilian compliant model types.

(JR900-06002-xH0).

4.19 Legacy Serial Support

The serial port device servers provide transparent encapsulation over IP (IP tunneling) of RS-232 serial data. It redirects raw serial data to remote hosts via the TCP or UDP IP protocol.

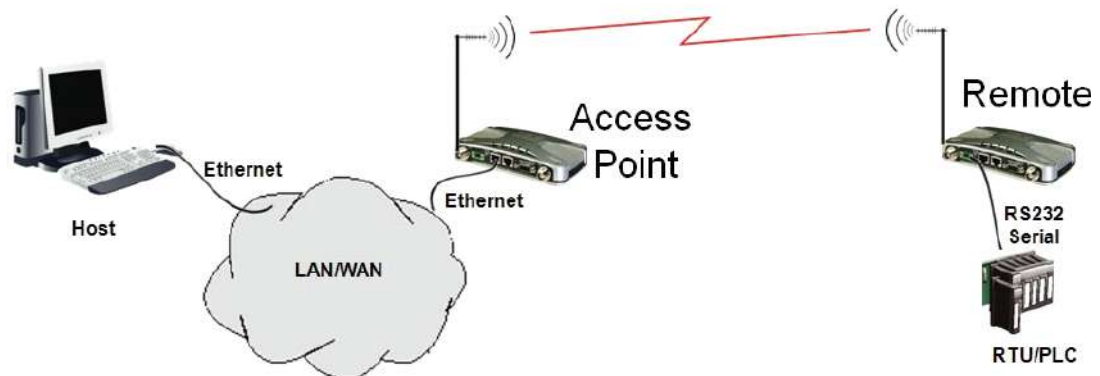
Note: The J-Series terminal servers support Internet Protocol version 4 (IPv4).

Data arriving at the J-Series serial port is packetized as defined by the configuration of the packet layer parameters. The raw data frame is then inserted into the data section of the TCP/UDP packet/datagram for transmission to the remote host. The remote host can be either another J-Series terminal server or some third party product.

The received serial data is extracted from the UDP/TCP datagram and sent out onto the serial port.

For example, PC applications can communicate with remote devices, with serial interfaces, by either sending/ receiving data via IP directly to the terminal server at the remote radio, or via the PC serial port to a local radio which transports the raw serial data via IP to the remote terminal server as shown in the diagram below.

Serial via Ethernet over J Series Network



Alternatively, the entry point to the J-Series network could also be an RS-232 serial connection as shown below.

Serial to Serial over J Series Network



4.19.1 Differences between TCP and UDP

TCP is a Point to Point (PTP) connection-oriented protocol, which means that upon communication it requires connection overhead to set up and maintain the end-to-end connection. The features of TCP are:

- **Reliable** - TCP manages message acknowledgment, retransmission and timeout. Many attempts to reliably deliver the message are made. If it gets lost along the way, the server will re-request the lost part. In TCP, there's either no missing data, or, in case of multiple timeouts, the connection is dropped.
- **Ordered** - if two messages are sent along a connection, one after the other, the first message will reach the receiving application first. When data packets arrive in the wrong order, the TCP layer holds the later data until the earlier data can be rearranged and delivered to the application.
- **Heavyweight** - TCP requires three packets just to set up a socket, before any actual data can be sent. It handles connections, reliability and congestion control. It is a large transport protocol designed on top of IP.
- **Streaming** - Data is read as a "stream," with nothing distinguishing where one packet ends and another begins. Packets may be split or merged into bigger or smaller data streams arbitrarily.

- Only supports uni-cast point-to-point (PTP) communication.

UDP is a simpler message-based connectionless protocol. In connectionless protocols, there is no effort made to setup a dedicated end-to-end connection.

Communication is achieved by transmitting information in one direction, from source to destination without checking to see if the destination is still there, or if it is prepared to receive the information. UDP datagrams cross the network in independent units.

- **Unreliable** - When a message is sent, it cannot be known if it will reach its destination; it could get lost along the way. There is no concept of acknowledgment, retransmission and timeout.
- **Not ordered** - If two messages are sent to the same recipient, the order in which they arrive cannot be predicted.
- **Lightweight** - There is no ordering of messages, no tracking connections, etc. It is a small transport layer designed on top of IP.
- **Datagrams** - Packets are sent individually and are expected to be whole if they arrive. Packets have definite bounds and no split or merge into data streams may exist.
- **Supports multicast protocols** – Point to multipoint and multipoint to multipoint.

Most SCADA type applications are well suited to the UDP protocol, where the application layer provides loss of packet and error recovery mechanisms.

4.19.2 Legacy Serial Modes Supported

Point to Point via TCP/IP

This mode of operation provides a more reliable point to point connection between two units (based on the IP address). When only two units need serial connectivity in a PTP arrangement and latency and bandwidth are not a major concern, the TCP IP mode should be selected.

For the purposes of clarity, a PTP radio network is shown in the diagram above. However, a PTP Serial Data link via TCP/IP can be established between any two radio units in the network, regardless of the type of radio network actually implemented (i.e. PTMP or PTMP with Bridges). Refer to [Part G – Quick Start Guide](#) ¹⁰⁹ for more information.

Point-to-Point Serial Data via TCP/IP



Point to Point via UDP/IP

This mode of operation provides a point to point connection between two units (based on the IP address). This mode of operation is best suited to high speed serial protocols which need low latency and high bandwidth. Refer to [Part G – Quick Start Guide](#)^[109] for more information.

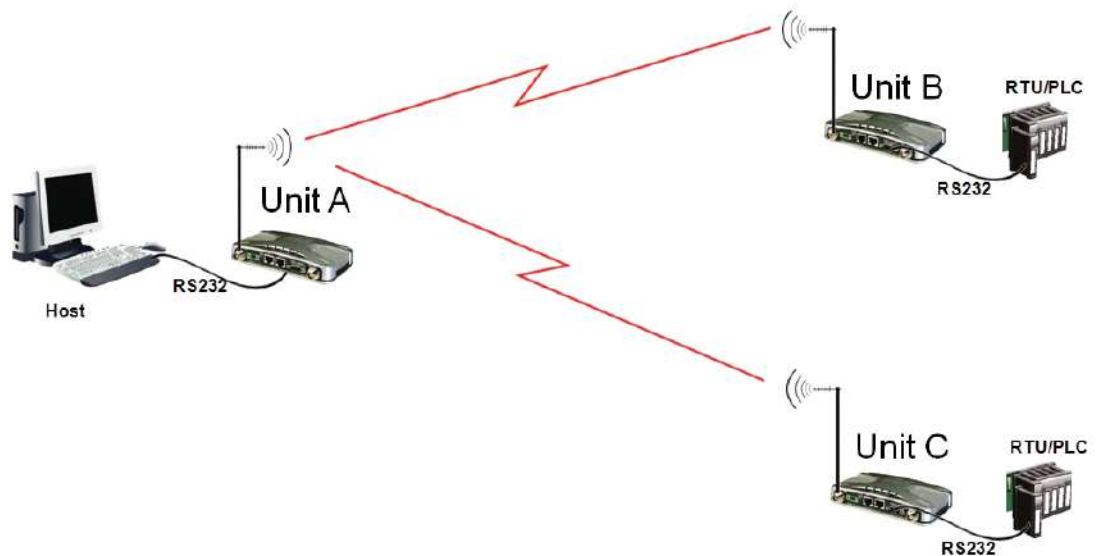
Point-to-Point Serial Data via UDP/IP (Unicast)



Point to Multipoint via UDP/IP

This mode of operation provides a point to multipoint connection between multiple units (based on the IP address). This mode of operation uses UDP/IP Multicasting and suitable Multicasting IP address ranges should be used. Refer to [Part G – Quick Start Guide](#)^[109] for more information.

Point-to-MultiPoint Serial Data via UDP/IP (Multicast)

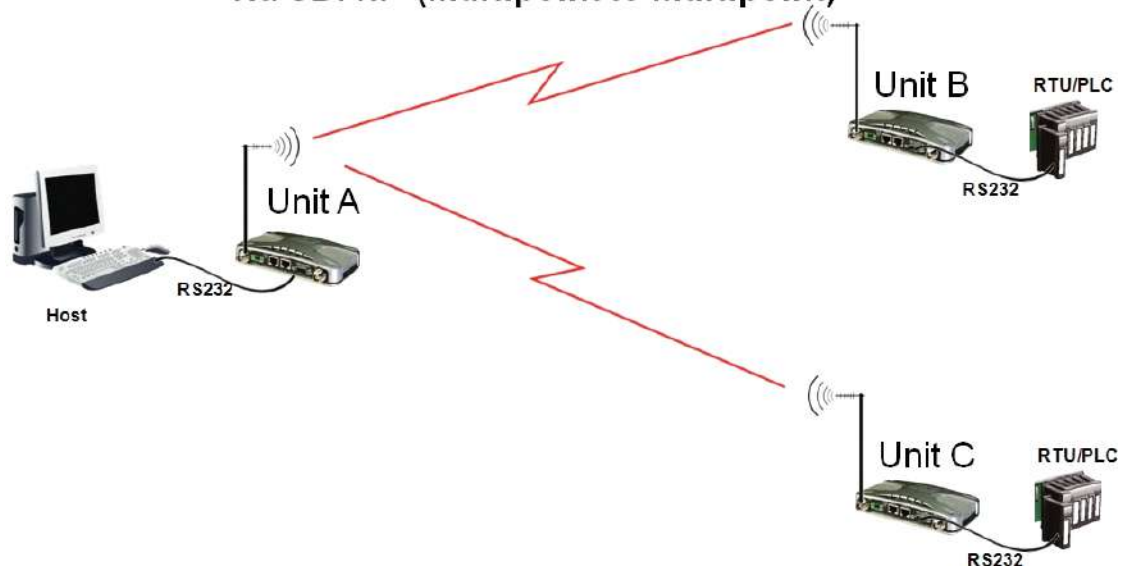


Point to Multipoint with Peer to Peer via UDP/IP

This mode of operation provides a point to multipoint connection between multiple units (based on the IP address) with peer to peer connectivity.

This mode of operation uses UDP/IP Multicasting and suitable Multicasting IP address ranges should be used. In this mode, each serial data message is “echoed” back to the sending device. Refer to [Part G – Quick Start Guide](#)^[108] for more information.

Point to Multipoint Serial Data (with Peer to Peer) via UDP/IP (Multipoint to Multipoint)



5 Part E - RF Planning and Design

See:

- [Understanding RF Path Requirements](#)^[56]
- [Examples of Predictive Path Modelling](#)^[57]
- [Antennas](#)^[60]
- [RF Feeders and Protection](#)^[62]
- [Band Pass Filter \(900 MHz Only\)](#)^[62]

5.1 Understanding RF Path Requirements

A radio modem needs a minimum amount of received RF signal to operate reliably and provide adequate data throughput.

In most cases, spectrum regulatory authorities will also define or limit the amount of signal that can be transmitted, and the transmitted power will decay with distance and other factors, as it moves away from the transmitting antenna.

It follows, therefore, that for a given transmission level, there will be a finite distance at which a receiver can operate reliably with respect to the transmitter.

Apart from signal loss due to distance, other factors that will decay a signal include obstructions (hills, buildings, foliage), horizon (effectively the bulge between two points on the earth), and factors such as fog, heavy rain- bursts, dust storms, etc.

To ascertain the available RF coverage from a transmitting station, it will be necessary to consider these factors. This can be done in a number of ways, including:

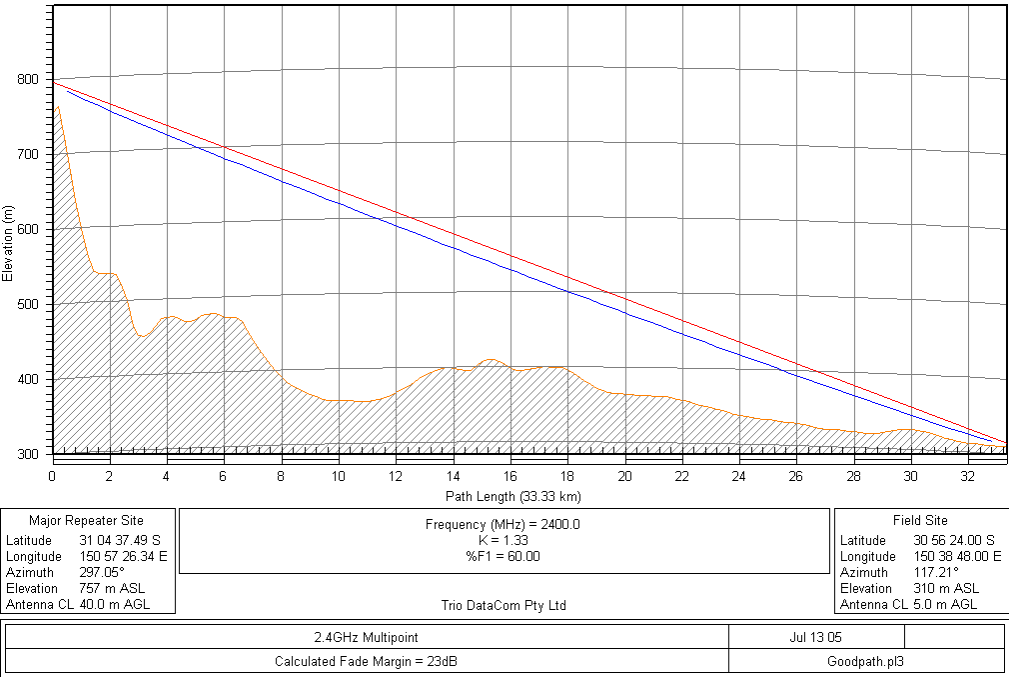
- using basic formulas to calculate the theoretically available signal - allowing only for free space loss due to distance,
- using sophisticated software to build earth terrain models and apply other correction factors such as earth curvature and the effects of obstructions, and
- by actual field strength testing.

It is good design practice to consider the results of at least two of these models to design a radio path.

5.2 Examples of Predictive Path Modelling

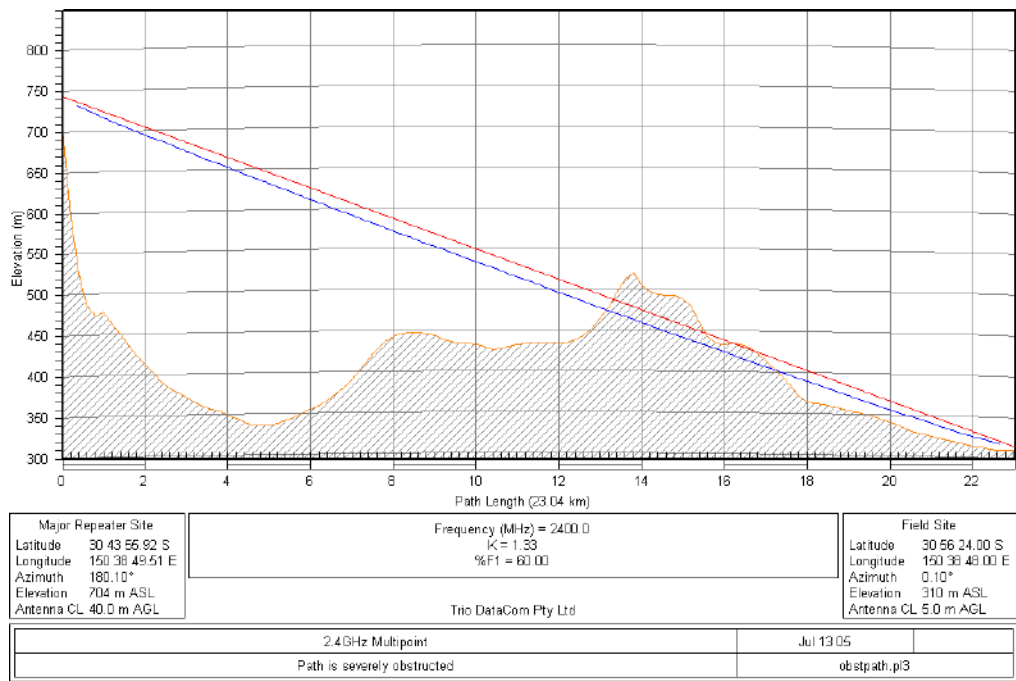
Clear line of site

Radio path with good signal levels, attenuated only by free space loss.



Obstructed radio path

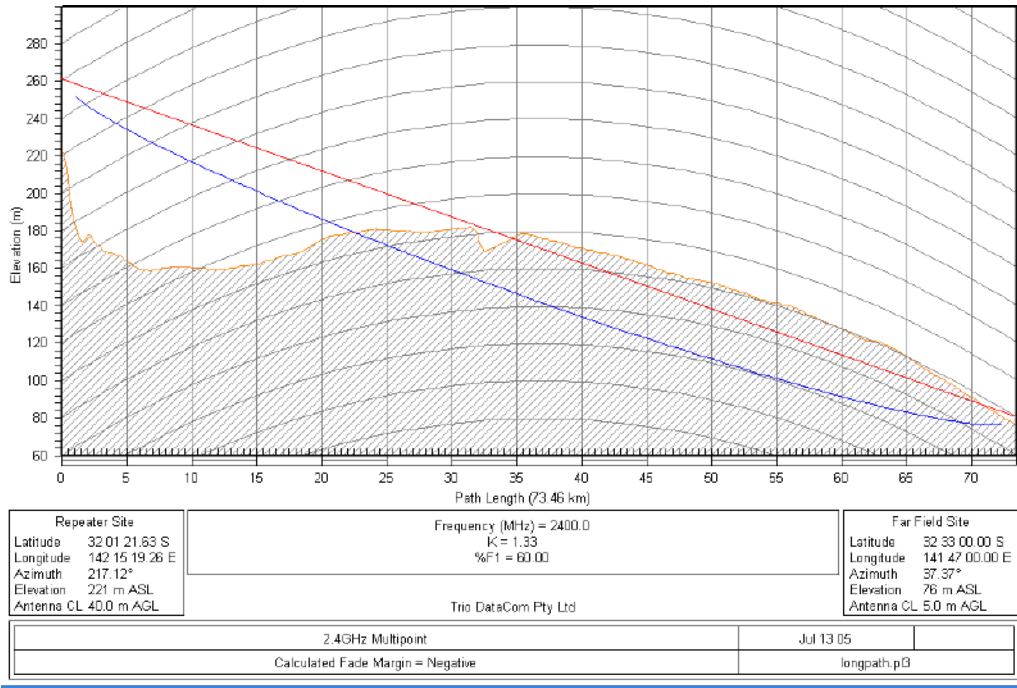
This path has an obstruction that will seriously degrade the signal arriving at the field site.



GOODPATH2400.pl4	Major Repeater Site	Field Site
Elevation (m)	756.69	309.67
Latitude	31 04 37.49 S	30 56 24.00 S
Longitude	150 57 26.34 E	150 38 48.00 E
True azimuth (°)	297.05	117.21
Vertical Angle (°)	-0.94	0.72
Antenna Model	6dB Omni	16dB Grid Reflector
Antenna Height (m)	40.00	5.00
Antenna Gain (dBi)	8.15	18.15
(dBd)	6.00	16.00
TX Line Type	LDF4-50	LDF4-50
TX Line Length (m)	40.00	5.00
TX Line Unit loss (dB /100 m)	6.79	6.79
TX Line loss (dB)	2.72	0.34
Connector loss (dB)	2.00	2.00
Frequency (MHz)	2400.00	
Polarization	Vertical	
Path Length (km)	33.33	
Free Space loss (dB)	130.53	
Diffraction loss (dB)	0.00	
Net Path loss (dB)	111.29	111.29
Radio Model	HR240	HR240
TX power (watts)	1.00	1.00
(dBm)	30.00	30.00
Effective Radiated Power (Watts)	1.34	23.23
(dBm)	31.28	43.66
RX Sensitivity (µv)	1.26	1.26
(dBm)	-105.00	-105.00
RX Signal (µv)	19.28	19.28
(dBm)	-81.29	-81.29
RX Field Strength (µv/m)	1014.39	243.90
Fade Margin (dB)	23.71	23.71
Rayleigh Fade Probability (%)	0.42	0.42
Log Normal Fade Probability (%)	3.88E-03	3.88E-03

5.2.1 Effect of Earth Curvature on Long Paths

This path requires greater mast height to offset the earth curvature experienced at such a distance (73km).



LONGPATH.PL3	Repeater Site	Far Field Site
Elevation (m)	221.26	75.58
Latitude	32 01 21.63 S	32 33 00.00 S
Longitude	142 15 19.26 E	141 47 00.00 E
True azimuth (°)	217.12	37.37
Vertical Angle (°)	-0.37	-0.03
Antenna Model	6dB Omni	15dB Grid Reflector
Antenna Height (m)	40.00	5.00
Antenna Gain (dBi)	8.15	17.15
(dBd)	6.00	15.00
TX Line Type	LDF4-50	LDF4-50
TX Line Length (m)	40.00	5.00
TX Line Unit loss (dB /100 m)	6.79	6.79
TX Line loss (dB)	2.72	0.34
Connector loss (dB)	2.00	2.00
Frequency (MHz)	2400.00	
Polarization	Vertical	
Path Length (km)	73.46	
Free Space loss (dB)	137.39	
Diffraction loss (dB)	34.02	
Net Path loss (dB)	153.18	153.18
Radio Model	HR240	HR240
TX power (watts)	1.00	1.00
(dBm)	30.00	30.00
Effective Radiated Power (Watts)	1.34	18.45
(dBm)	31.28	42.66
RX Sensitivity (µv)	1.26	1.26
(dBm)	-105.00	-105.00
RX Signal (µv)	0.16	0.16
(dBm)	-123.18	-123.18
RX Field Strength (µv/m)	8.16	2.20
Fade Margin (dB)	-18.18	-18.18

Location - Woodland (sigma = 6 dB)

1

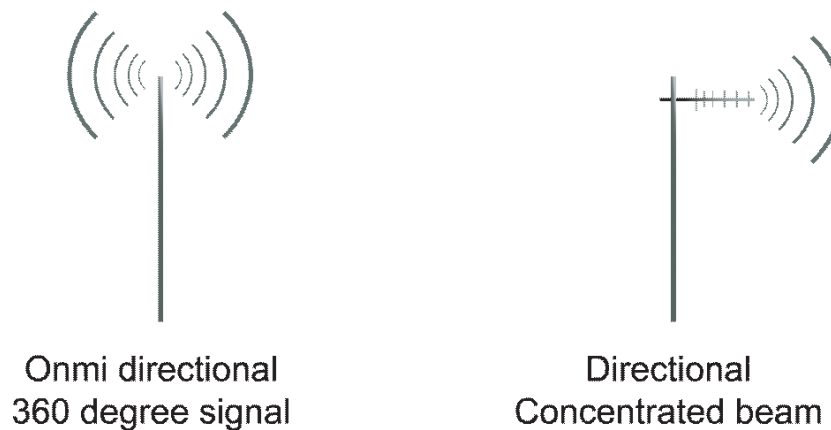
5.3 Antennas

There are basically two types of antennas – omni- directional and directional.

Omnidirectional antennas are designed to radiate signal in a 360 degrees segment around the antenna. Basic short range antennas such as folded dipoles and ground independent whips are used to radiate the signal in a “ball” shaped pattern. High gain omni antennas such as the “co-linear” compress the sphere of energy into the horizontal plane, providing a relatively flat “disc” shaped pattern which goes further because all of the energy is radiated in the horizontal plane.

Directional antennas are designed to concentrate the signal into a “beam” of energy for transmission in a single direction (i.e. for point-to-point or remote to base applications).

Beamwidths vary according to the antenna type, and so can be selected to suit design requirements. The most common directional antenna is the yagi, which offers useable beam widths of 15-40 degrees. Even higher “gain” is available using parabolic “dish” type antennas such as gridpacks.



5.3.1 Antenna Gain

By compressing the transmission energy into a disc or beam, the antenna provides more energy (a stronger signal) in that direction, and thus is said to have a performance “gain” over a basic omni antenna. Gain

is usually expressed in dBd, which is referenced to a standard folded dipole. Gain can also be expressed in dBi, which is referenced to a theoretical “isotropic” radiator. Either way, if you intend to send and receive signals from a single direction, there is advantage in

using a directional antenna - both due to the increased signal in the wanted direction, and the relatively decreased signal in the unwanted direction (i.e. “interference rejection” properties).

5.3.2 Antenna Placement

When mounting the antenna, it is necessary to consider the following criteria:

- The mounting structure will need to be solid enough to withstand additional loading on the antenna mount due to extreme wind, ice or snow (and in some cases, large birds).
- For omni directional antennas, it is necessary to consider the effect of the mounting structure (tower mast or building) on the radiation pattern. Close in structures, particularly steel structures, can alter the radiation pattern of the antenna. Where possible, omni antennas should always be mounted on the top of the mast or pole to minimize this effect. If this is not possible, mount the antenna on a horizontal outrigger to get it at least
- 1...2m away from the structure. When mounting on buildings, a small mast or pole (2...4m) can significantly improve the radiation pattern by providing clearance from the building structure.
- For directional antennas, it is generally only necessary to consider the structure in relation to the forward radiation pattern of the antenna, unless the structure is metallic, and of a solid nature. In this case it is also prudent to position the antenna as far away from the structure as is practical. With directional antennas, it is also necessary to help ensure that the antenna cannot move in such a way that the directional beamwidth will be affected. For long yagi antennas, it is often necessary to install a fiberglass strut to stabilize the antenna under windy conditions.

5.3.3 Alignment of Directional Antennas

This is generally performed by altering the alignment of the antenna whilst measuring the received signal strength. If the signal is weak, it may be necessary to pre-align the antenna using a compass, GPS, visual or map guidance to “find” the wanted signal. Yagi antennas have a number of lower gain “lobes” centered around the primary lobe. When aligning for best signal strength, it is important to scan the antenna through at least 90 degrees, to help ensure that the center (strongest) lobe is identified.

When aligning a directional antenna, avoid placing your hands or body in the vicinity of the radiating element or the forward beam pattern, as this will affect the performance of the antenna.

5.4 RF Feeders and Protection

The antenna is connected to the radio modem by way of an RF feeder. In choosing the feeder type, there is a compromise between the loss caused by the feeder, and the cost, flexibility, and bulk of lower loss feeders. To do this, it is often prudent to perform path analysis first, to determine how much “spare” signal can be allowed to be lost in the feeder. The feeder is also a critical part of the lightning protection system.

All elevated antennas may be exposed to induced or direct lightning strikes, and correct grounding of the feeder and mast are an essential part of this process. Gas discharge lightning arresters should also be fitted to all sites.

Note: All ETSI installations require the use of a lightning surge arrester.

Common Cable Types	Loss per 30.5 m	Loss per 30.5 m
	@ 915 MHz	@ 2.4 GHz
RG213/U	7.4 dB	14 dB
FSJ1-50 (1/4" superflex)	5.6 dB	9.9 dB
LDF4-50 (1/2" heliax)	2.2 dB	3.5 dB
LDF5-50 (7/8" heliax)	1.2 dB	2 dB

5.5 Band Pass Filter (900 MHz Only)

The J-Series radio is a robust, industrial strength radio designed for harsh RF environments, and in the majority of applications there is no requirement for additional protection from interference. In some circumstances, particularly when the radio is operated in very close proximity (i.e. less than 25 m of separation) to 900 MHz GSM/CDMA mobile phone base stations or other radios operating close to the 900 MHz ISM band, the J-Series radio may be subject to exceptionally high levels of RF interference.

These high levels of RF interference can result in a degradation of radio performance, and it is strongly recommended that an external RF band pass filter be installed to reduce the interference to an acceptable RF level. Contact the factory for recommendation of a suitable RF band pass filter for your country or region.

6 Part F - Quick Reference Guide

Welcome to the Quick Start Guide for the J-Series Ethernet Radio. This guide provides step-by-step instructions, with simple explanations to get you up-and-running. For a summary of this information, refer to the J-Series Quick Start Guide.



See:

- [Mounting and Installation Instructions](#) ^[63]
- [DIN Mounting Kit](#) ^[65]
- [DIN Rail Mounting Bracket](#) ^[65]
- [DIN Rail Clip](#) ^[66]
- [Connecting Antennas and RF Feeders](#) ^[69]
- [J-Series Connections Layout](#) ^[70]
- [Power Supply Requirements](#) ^[70]
- [Communication Ports](#) ^[70]
- [Cable Termination](#) ^[71]
- [Serial Port A & B Ports](#) ^[72]
- [LED Indicators](#) ^[73]
- [Web User Interface \(WUI\)](#) ^[75]
- [Connection to WUI - Secure HTTPS Connection](#) ^[77]
- [Resolving Ethernet Configuration Problems](#) ^[82]
- [Multi Master Synchronization](#) ^[84]
- [Text User Interface \(TUI\)](#) ^[85]
- [Spectrum Analyzer](#) ^[89]
- [Telnet Interface](#) ^[93]
- [Secure Shell \(SSH\)](#) ^[94]
- [SNMP](#) ^[97]
- [e-Diags Example](#) ^[106]
- [e-Diags Parameters](#) ^[107]
- [Ethernet Filtering](#) ^[109]

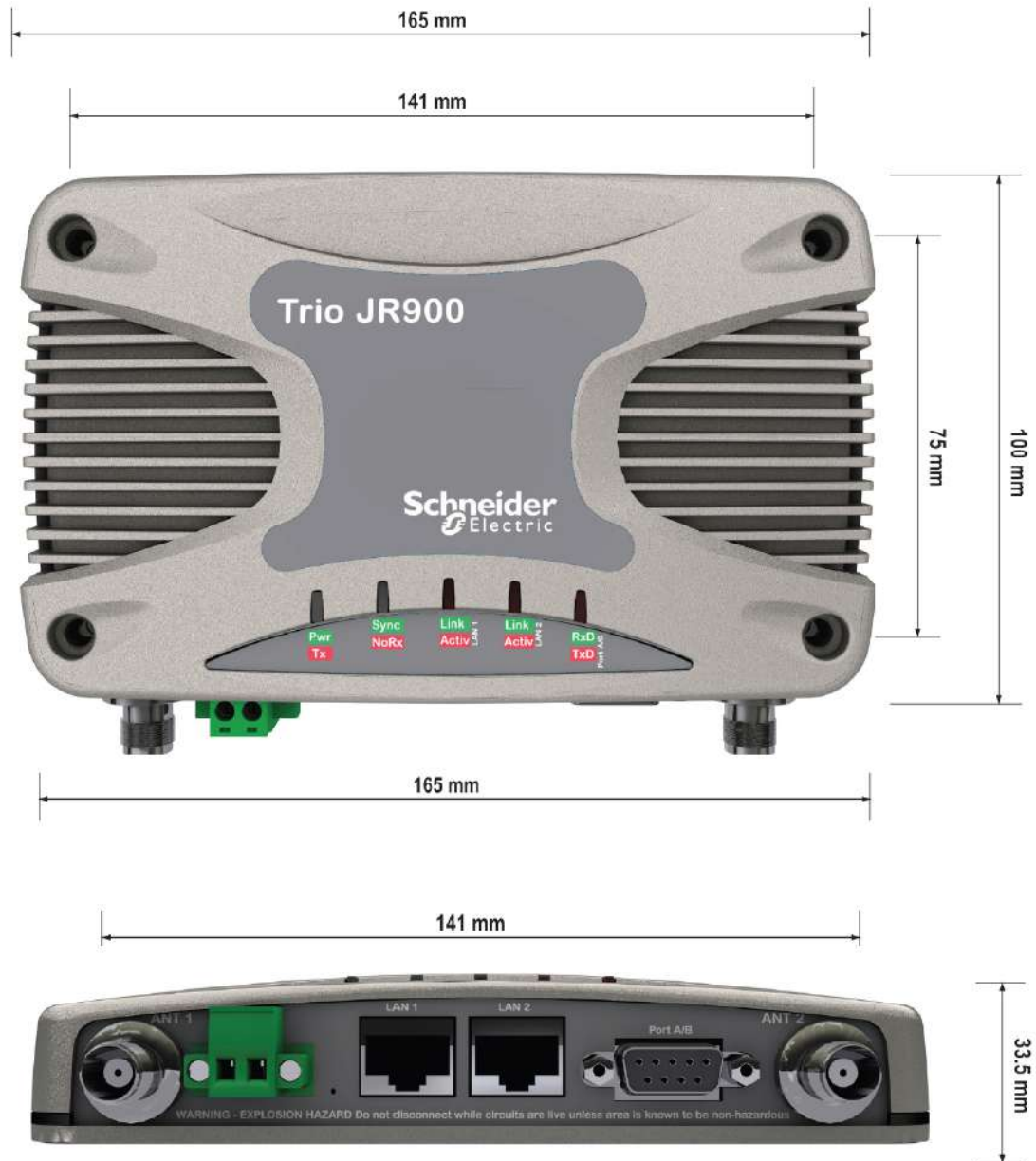
6.1 Mounting and Installation Instructions

The radio should be mounted in a clean and dry location, protected from water, excessive dust, corrosive fumes, extremes of temperature and direct sunlight. In high power or high

temperature applications, allow sufficient passive or active ventilation. To avoid moisture ingress mount the radio with the connectors facing downwards.

Choose an enclosure that is suitable for the size of the radio: Dimensions are 100 x 34 x 165 mm (4.0 x 1.4 x 6.5 inches). The radio is rated for use in ambient (operating) environments from -40 °C...70 °C.

Physical dimensions - remote Ethernet data radio



Note : Drawings not to scale.

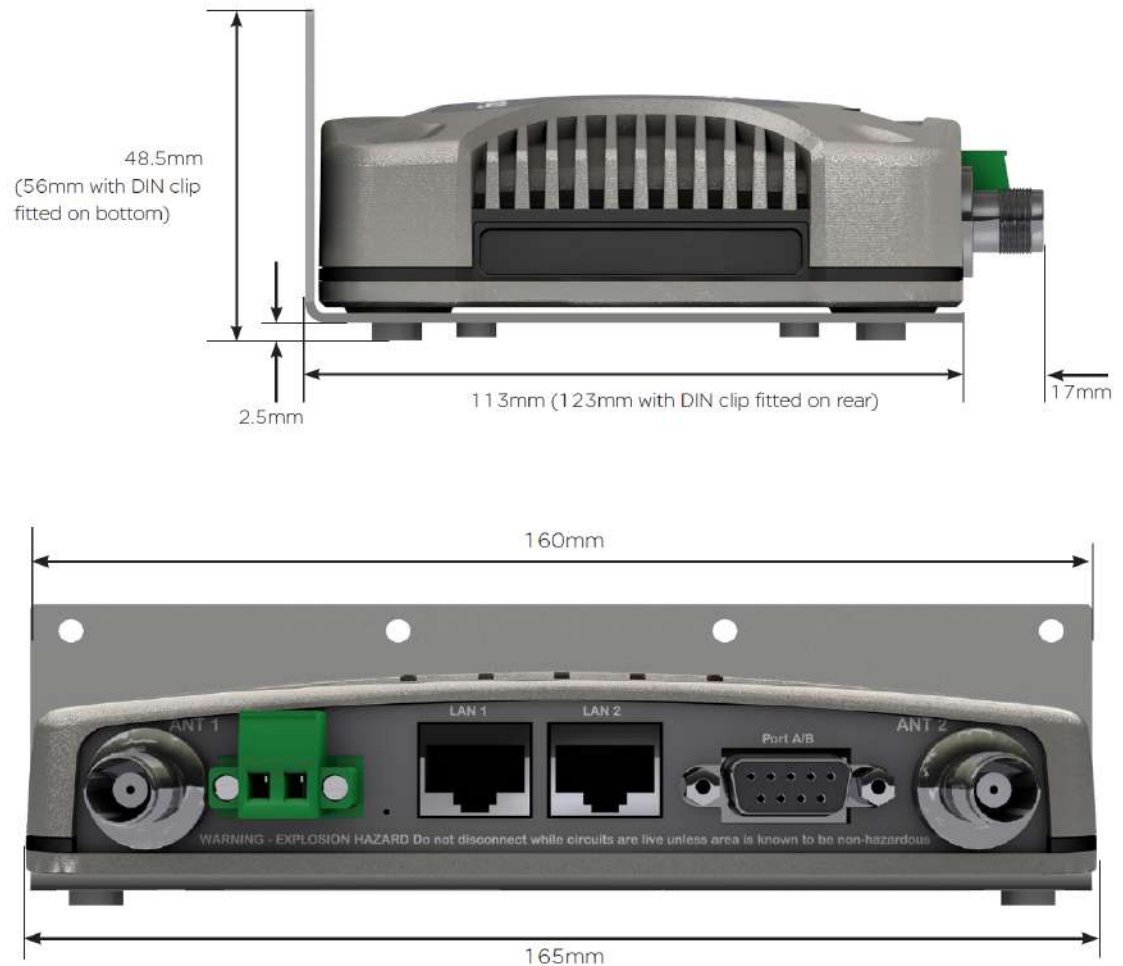
6.2 DIN Mounting Kit

An optional DIN mounting kit is available for the J-Series. The Mount is screwed onto the bottom of J-Series giving the unit the ability to be 'clipped' and Locked onto 3.5 mm Din Rail.

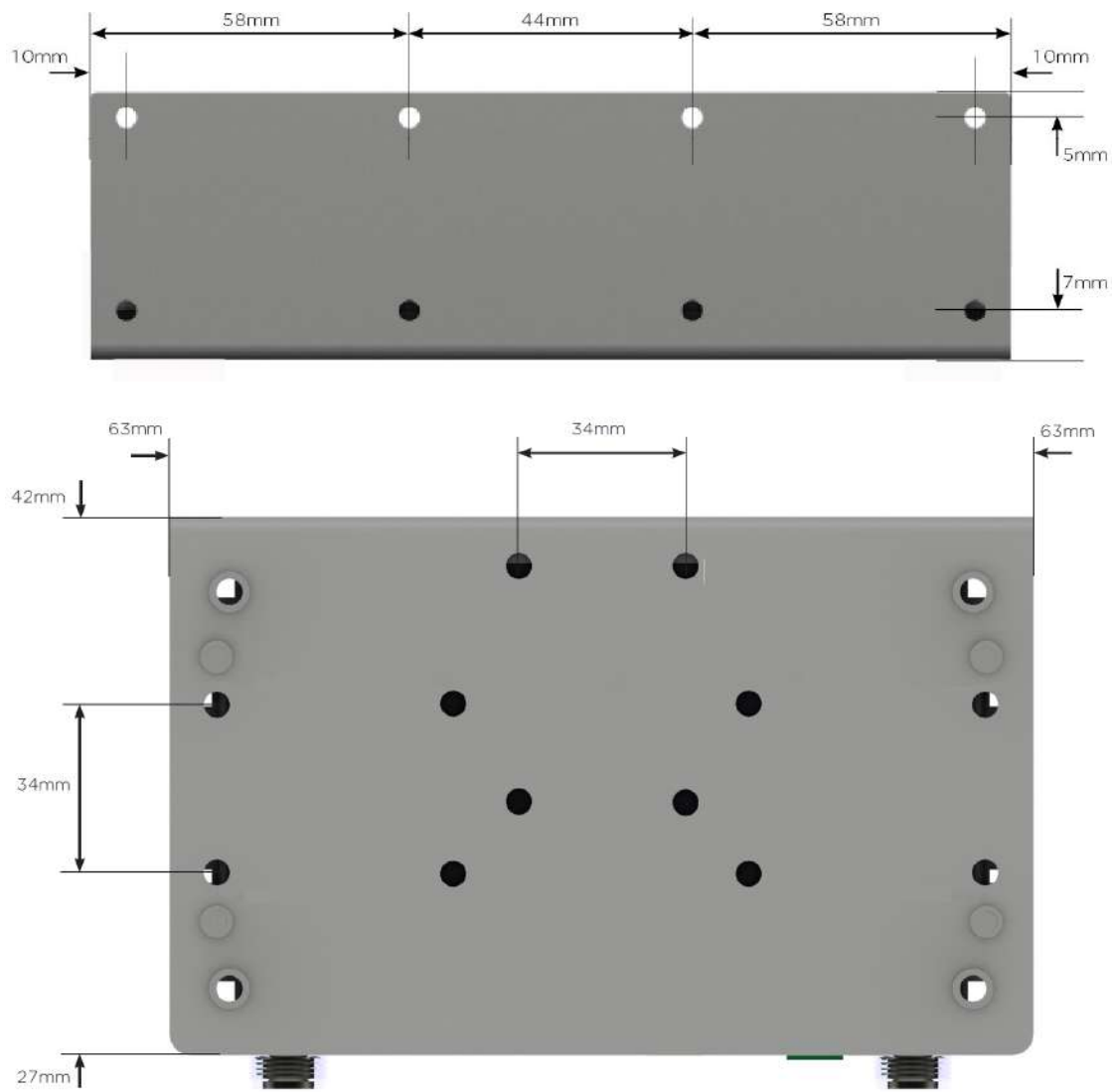
Each Din kit supplies:

- A DIN rail mounting bracket
- A Phoenix DIN rail clip
- x4 Countersunk M4X8 screws (to mount DIN rail clip to bracket)
- x4 M4 nuts (to mount DIN rail clip to bracket)
- x4 Pan head M3X6 screws (to mount Spread spectrum radio to bracket)
- x4 Pan head M4X2.5 screws (to mount M-Series to bracket)

6.3 DIN Rail Mounting Bracket



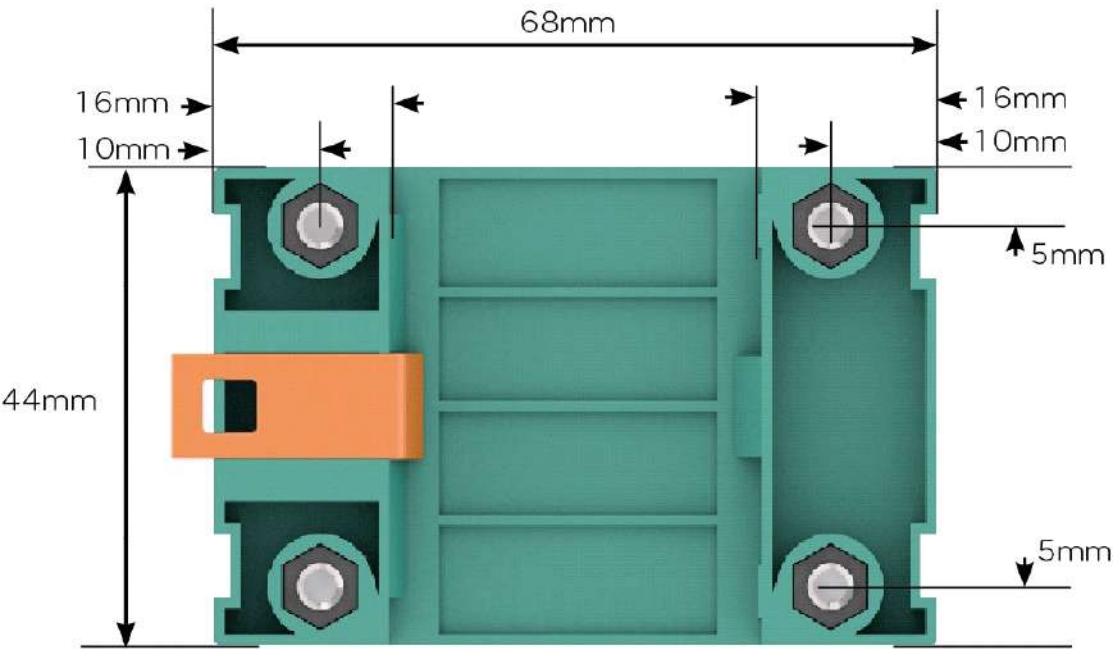
Note : Drawings not to scale.



6.4 DIN Rail Clip

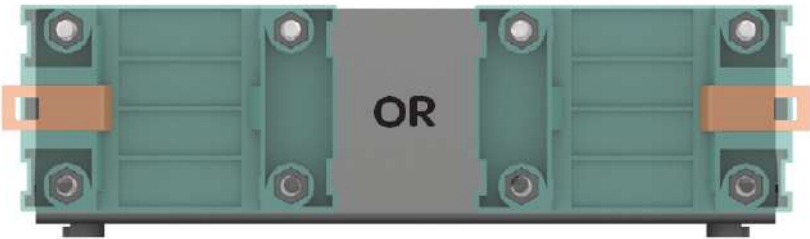
The DIN rail clip has a spring loaded latch to allow easy installation/removal of the radio device being installed.

The DIN rail clip can be fitted to the DIN rail mounting bracket x5 different ways to allow as much installation flexibility as possible.



6.4.1 Rear Mount DIN Rail Clip

The DIN rail clip can be fitted on the rear of the DIN rail mounting bracket two ways shown below.

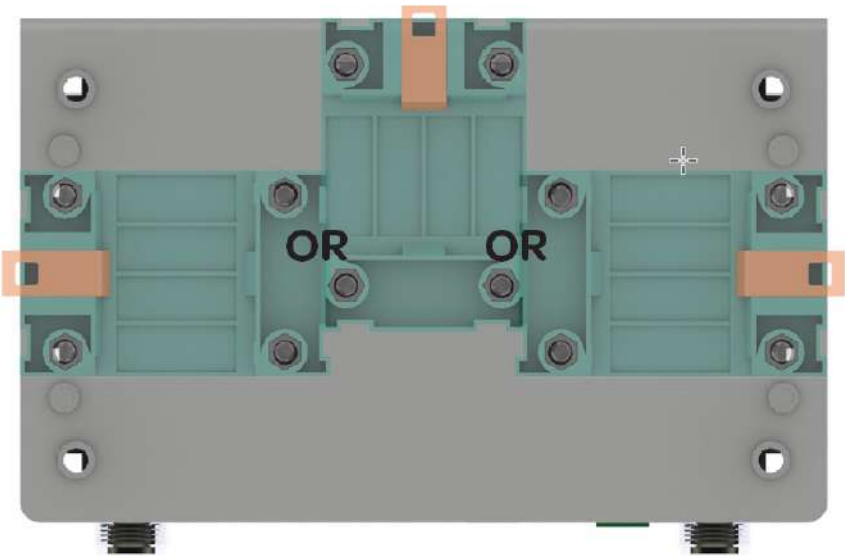


Examples of rear fitted DIN clips



6.4.2 Bottom Mount DIN Rail Clip

The DIN rail clip can be fitted on the bottom of the DIN rail mounting bracket three different ways shown below.



Examples of bottom fitted DIN clips

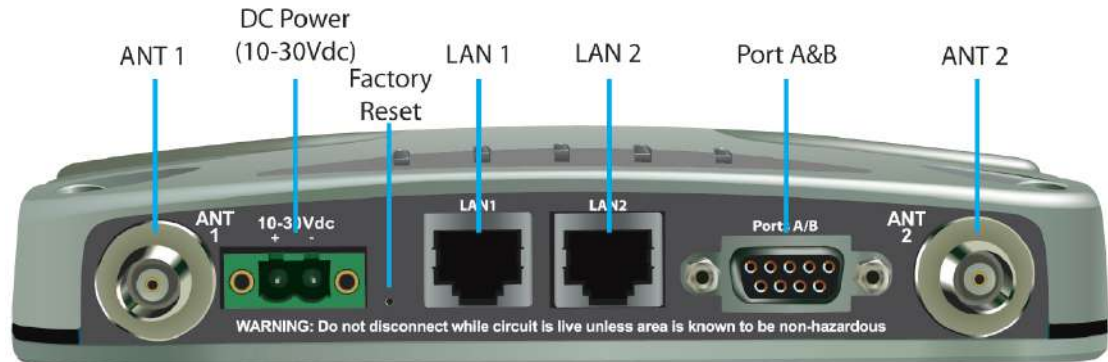


6.5 Connecting Antennas and RF Feeders

The RF antenna system should be installed in accordance with the manufacturers notes. Antenna gain needs to be considered when setting Transmit Power. Refer to Compliance notices at the end of this document and in the use manual for more information.

The RF connectors on this product are TNC Type female connectors. Always use good quality low loss feeder cable, selected according to the length of the cable run. Ensure all external connections are waterproofed.

6.6 J-Series Connections Layout



6.7 Power Supply Requirements

Tx: Nominal 13.8 Vdc @ 800 mA (Max 1 A)

Rx: Nominal 13.8 Vdc @ 150 mA

Rated Operating Voltage 10...30 Vdc

The J-Series Radio is supplied with the a mating DC power connector:

Phoenix Contact Part Number 1777989. The DC Power connector should be installed with the locking screws done up tightly. Cable needs to be #22 AWG or larger, 70 °C min. temperature rating. CSA maximum current rating: 2.5 A.

The J-Series Ethernet radio modem will operate from a 10...30 volt (filtered) DC supply. The radio is designed to help protect itself from permanent damage if the voltage exceeds 30 Vdc or if reverse polarity is applied. The replaceable internal fuse has a rating 3 Amp.

The current requirement is typically 180 mA @ 13.8 Vdc in receive mode, and will vary in transmit mode according to RF output power level & duty cycle. The radio modem can be damaged if there is any potential difference between the chassis- ground, RS-232 signal ground, power (-) input, or antenna coaxial shield.

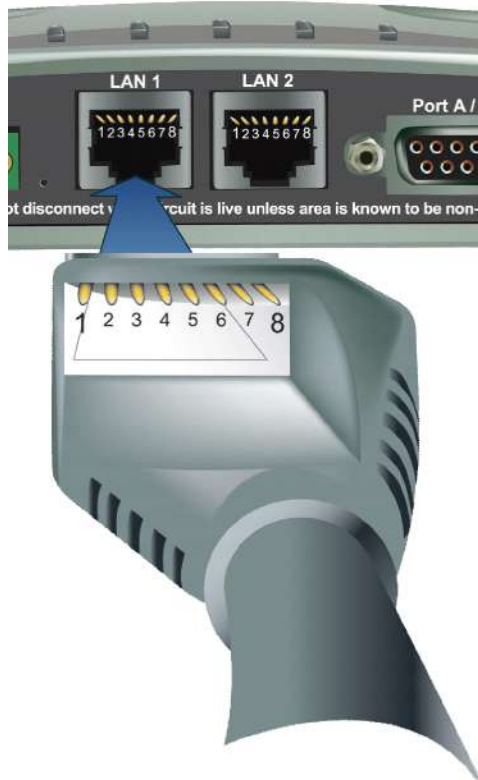
Before connecting any wiring, ensure all components are earthed to a common ground point (pay particular attention to 24 V PLC power systems where DC-DC converters are used).

Connect the antenna, Ethernet and RS-232 plugs BEFORE applying power to the unit. Lastly, before inserting the power plug, re-check that the polarity and voltage on the DC power plug is correct using a multimeter.

6.8 Communication Ports

LAN 1 and LAN 2 Ethernet Ports

The LAN 1 and LAN 2 ports are 10/100 Base-T compliant ports using an RJ-45 connector. These ports support both TIA/EIA-568-A & B wiring as they have Auto MDI/MIDX Auto Sensing. This means you can use both straight-through and cross-over type CAT-5 or better patch cables.



6.9 Cable Termination

If termination of a cable is required, then the following wiring arrangement should be followed (Compliant with TIA/EIA-568-A).

Note: Maximum differential voltage: 5 V, 50 mA max through each differential pair.

Note: If 100-BaseT connection speed is required, CAT-6 Shielded cable should be used for installation to comply with ETSI EMC directives.

Pin	Pair	Wire	Color
1	3	tip	 white/green
2	3	ring	 green
3	2	tip	 white/orange
4	1	ring	 blue
5	1	tip	 white/blue
6	2	ring	 orange
7	4	tip	 white/brown
8	4	ring	 brown

6.10 Serial Port A & B Ports

The J-Series Radio features a 9 pin miniature D-Shell (DE-9) Female connector that supports two individual serial port connections. Each serial port is associated with an embedded serial terminal server that provides the RS-232 to TCP/IP or UDP/ IP connectivity. Refer to [Legacy Serial Modes Supported](#)^[54] for more information on the serial terminal servers.

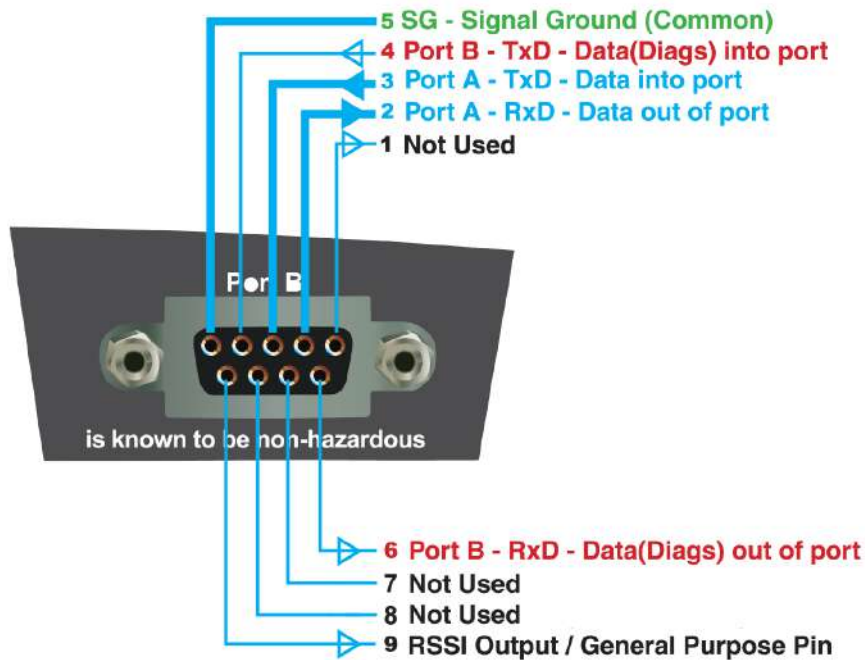
Data Port A uses pins 2 & 3 with pin 5 as the common ground.

Data Port B uses pins 4 & 6 with pin 5 as the common ground.

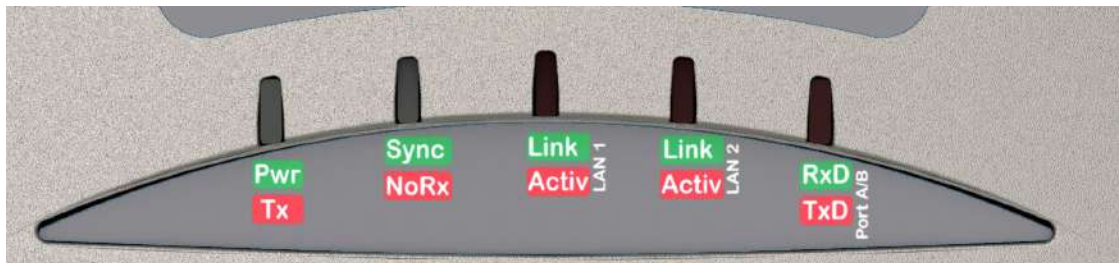
An RSSI output is available on pin 9 which is useful for antenna alignment. See below for details.

Notes:

- (1) Pins 2 & 6 are outputs rated at +/- 6 V, 65 mA max.
- (2) Pins 3 & 4 are inputs rated at +/- 15 V, 5 mA max.
- (3) Pin 9 is a multipurpose IO pin with 120 mA max input / 5 mA max output.
- (4) Connecting wires should be #26 AWG or larger.



6.11 LED Indicators



Pwr/TX - DC Power & TX LEDs

If all the LEDs are off, no DC power is reaching the radio modem or the internal fuse is open. Successful power-up is indicated by the Pwr/Tx LED showing a continuous GREEN state for Remotes or an alternating Red/Green for Access Points.

Tx Indicator (Tx): When the transmitter is active the Pwr/Tx LED is in a RED state.

Note: The J-Series radio will take approximately 45 seconds to boot up - during this time, the DC power LED will remain solid green and various LED activity may occur. Wait at least 45 seconds before attempting to use radio.

Sync/No RX - Synchronization and No Received Signal LEDs

A regular flashing GREEN Sync/No RX LED indicates that the modem is synchronized to its Access Point. The Sync/No RX LED will also flash GREEN when the modem is receiving data.

A regular flashing RED Sync/No RX LED indicates the REMOTE is not synchronized to an Access Point or BRIDGE. Check the antenna, all RF connections and the radio configuration. Some common causes of this event is that the Subnet ID may not match the Access Point or there may be insufficient RX signal or too much interference.

LAN 1 & LAN 2 - LAN Link and Activity LEDs

The Green Link and Amber Activity LEDs indicate Ethernet status on the two LAN ports. These LEDs will show solid Green when an Ethernet Link is established and will flash Amber to indicate Ethernet data transmission is occurring.

TxD/RxD - Serial TxD/RxD LEDs

The TxD/RxD LEDs indicate data flow into/out of the user port. Data being sent to the port for transmission is indicated by a RED flash, and data being received over the air and then forwarded to the serial port is shown as a GREEN flash.

6.11.1 Firmware Updating and Factory Default Information LEDs

In some circumstances a firmware update or factory default might be required. A special LED sequence is shown during this phase.

	Pwr / Tx	Sync / NoRx	Link 1 / Activ 1	Link 2 / Activ 2	RxD / TxD
Firmware upgrade	Amber	Amber	Amber	Amber	Amber
Factory Defaults	Green	Green	Green	Green	Green

Firmware Upgrade: All LEDs flash AMBER (as shown in table above) - 1 second ON and 1 second OFF

Factory Default: Factory Default LEDs (as shown in table above) are permanently GREEN during factory default reset.

6.11.2 Event LED Indications

In some circumstances the radio will indicate an event state. This is shown as all LEDs flashing RED for 1 sec and then a pattern of green LEDs for 1 sec. The pattern of green LEDs indicate the type of event. Consult the table for more information.

	Pwr / Tx	Sync / NoRx	Link 1 / Activ 1	Link 2 / Activ 2	RxD / Tx	Problem
High VSWR	Green			Green		Ant 1 or 2 has high VSWR
High Temperature	Green	Green		Green		Internal Temperature too high
DC Voltage out of Spec	Green	Green		Green	Green	DC Voltage Out of Spec

For all other patterns of event LEDs the radio needs to be returned to the factory for repair.

6.12 Web User Interface (WUI)

Read the following notes carefully. Configuration errors with Ethernet connections can be difficult to find and resolve. It is strongly recommended that you follow these guidelines.

Factory Default Reset

The factory default IP address of the J-Series is **192.168.2.15**. If you do not know the IP address of the J-Series you will need to activate a factory reset.

A factory reset will cause all previous configuration settings to be erased and returned to the factory default values. A factory default can be initiated by applying DC power to the radio (wait 45 seconds), depress the factory default switch using a paper clip or similar object and keep the switch depressed for 5 seconds until all five LEDs illuminate solid GREEN indicating the radio will return to the factory default settings. Wait 30 seconds for the factory default reset process to complete.

The radio is vulnerable while it is in factory default state. Do not connect the radio to an untrusted network while it remains in this state. See [Device Hardening](#) [11b].

Connection to HTML Web Server - HTTP connection

The J-Series radio contains an embedded Web Server. To change a configuration parameter in the J-Series you will need to connect your PC to one of the Ethernet Ports (LAN1 or LAN2) and direct your browser to the IP address of the J-Series. It is strongly recommended that you follow these guidelines for successful connection to the radio:

1. Ensure the J-Series is powered up and has fully booted. This is indicated by a solid green power LED and a flashing Synch/ NoRx LED. It takes approximately 45 seconds from applying DC power for the J-Series to fully power up.

2. Disconnect your PC from any other Internet/LAN networks. Failure to do so may create a conflict in IP addresses or the J-Series IP might not meet the subnet mask specified by your network.
3. Connect your PC Ethernet Port to one of the Ethernet Ports (LAN 1 or LAN2) using an RJ-45 patch cable. Cross over cables will also work. Successful cable connection is indicated by a solid Green "Link" LED on the Ethernet Port.

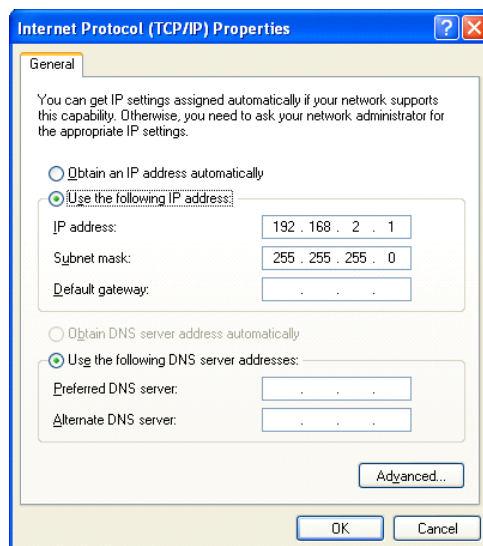
Note: The LAN1/2 LEDs will also flash orange when data is being transferred.

4. Ensure your PC LAN Port is configured for a suitable IP address. You can do this by configuring the LAN settings via the Control Panel. Navigate to your Windows "Start" button and open Control Panel > Network Connections > Local Area Connection > Properties. You should see the window as shown.

Scroll Down and Select "Internet Protocol (TCP/IP) and then click on Properties. You will now see the window as shown.

Ensure "Obtain IP Address Automatically" is not selected. It is recommended that you manually specify a compatible IP Address. In this example, a factory default radio is being configured. The IP address of that radio is 192.168.2.15 and a compatible IP address for the PC would be 192.168.2.1. Click OK to accept the changes.

Note: Check with your Network Administrator before allocating IP addresses as each LAN/WAN network is different.



5. You should start your web browser and insert the IP address of the J-Series into the URL. In this case, we type "192.168.2.15" and the configuration page is now displayed in the browser.

Note: You may need to disable a web proxy (if in use) or disable or modify your local firewall to help ensure the security rules allow access to the J-Series IP address. Secure HTTPS



6.13 Connection to WUI - Secure HTTPS Connection

The J-Series HTML Web user interface can be accessed through a secure HTTP (HTTPS) connection.

There are multiple steps required to establish a successful HTTPS connection to the J-Series, which include:

- Enabling HTTPS within the J-Series
- Loading a signed, digital certificate into the J-Series (This may be generated by a certificate server (i.e. Active directory) or can be self-generated by the J-Series).
- Resolving web browser issues

Once the above steps have been completed, enter “HTTPS://xxx.xxx.xxx.xxx” where ‘x’ is your units IP address, into your web browsers URL bar and press enter.

Enabling HTTPS within the J-Series

Browse to the unit’s Security page (Setup > Security) and under the Administration heading, you are able to enable/disable HTTPS. You also have the option to disable HTTP access once HTTPS is enabled.

Administration		
Security	☐ Enable ☒ Disable	Security: Enable administration security.
Telnet Terminal	☒ Enable ☐ Disable	Telnet Terminal: Set to enable Telnet Sessions.
Https Access	☒ Enable ☐ Disable	Https Access: Enable secure http (https) access.
Http Access	☒ Enable ☐ Disable	Http Access: Enable insecure http access.

Loading a digitally signed certificate into the J-Series

Certificate Management Server

A certificate can be generated and signed from a certificate management server. Once a certificate is signed, it needs to be loaded into the J-Series. An example of commonly used certificate management server is Active directory. Note that a unique certificate is required for

each individual unit. Certificates are bound to each unit by its IP address and serial number. If the IP address of a unit is changed, the certificate needs to be re-generated and re-loaded back into the J-Series.

HTTP SSL Certificate

Upload Certificate:

To load a signed certificate into a J-Series via the WUI, browse to the Security Management page (Maintenance > Security management) and select the 'Browse' button.

Verify the correct file has been selected, then press the 'Upload' button.

Once the certificate has been successfully uploaded, a message will appear and information about the certificate will be visible within the current certificate section.

Unless the certificate management server has been linked to your web browser as a trusted certificate server, the browser may display security warnings upon entry to the J-Series WUI via HTTPS. To add exceptions into your browser for these security warnings, see the instructions below.

Self signed certificate

A self signed certificate can easily be generated from within the J-Series. To generate a self signed certificate, browse to the security update page (Maintenance > Security maintenance) and select the 'Generate' button.

HTTP SSL Certificate

Upload Certificate:

Generate Certificate:

Self-signed certificate generated successfully.

Once the self signed certificate has been created, a message will appear and information about the certificate will be visible within the current certification section.

Resolving web browser issues

Every web browser has a list of trusted Certification Authorities (CAs). When either a CA that is not included within the web browsers trusted list is used to sign a certificate, or a self signed certificate is used, a security warning will appear within the web browser when an attempt to access the J-Series via HTTPS is made. See the example below (Example uses internet explorer 8).

This warning is identifying the fact that the signature of the certificate being read is not within the browser's trusted list.



There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.
The security certificate presented by this website has expired or is not yet valid.

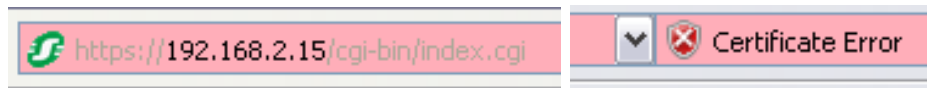
Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage and do not continue to this website.

 [Click here to close this webpage.](#)

 [Continue to this website \(not recommended\).](#)

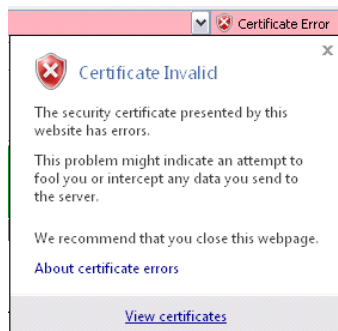
Pressing the 'Continue to this website (not recommended)' button will allow a HTTPS connection through to the J-Series. You will notice that the URL bar of the browser is still indicating that the certificate is still not trusted.



Although the Browser is identifying this error, a secure connection is still being established to the J-Series.

To add the signer to the browser's trusted list:

Click on the 'Certificate Error' warning within the URL bar as shown. This will open a Certificate invalid window, click on the 'View certificates' button.



Once the 'View certificates' button is selected, a certificate information window will open. Once this window has opened, select the 'Install Certificate..' button.

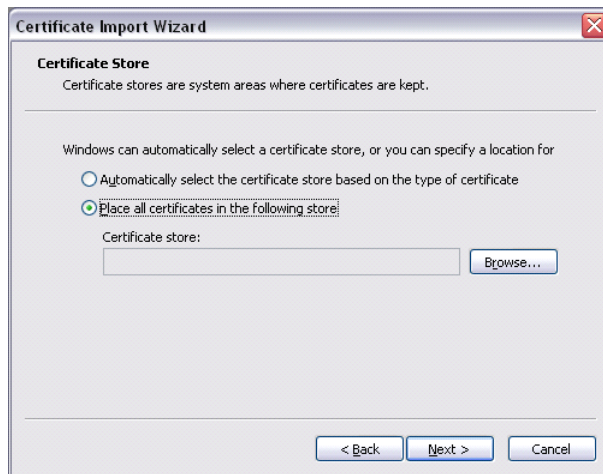
If you cannot see the 'Install Certificate..' button, you need to restart Internet Explorer in administration mode. Do this by right clicking the Internet Explorer icon on the desktop and selecting 'open in administrator mode'. If this selection is not available, contact your system administrator.



This will start the certificate import wizard. Select the Next button.



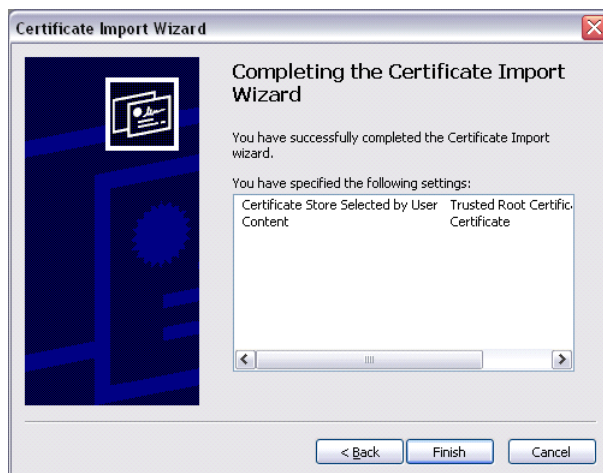
Select the 'Place all certificates in the following store' option and press the 'Browse...' button.



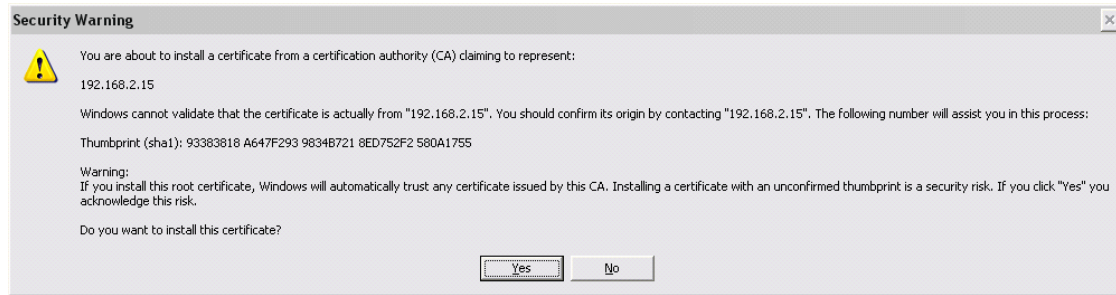
Select the 'Trusted Root Certification Authorities' folder and press the 'OK' button.



Once the import directory has been selected, press the 'Finish' button.



A security warning will appear providing information about the added certificate exception. Press the 'Yes' button to complete the installation process.



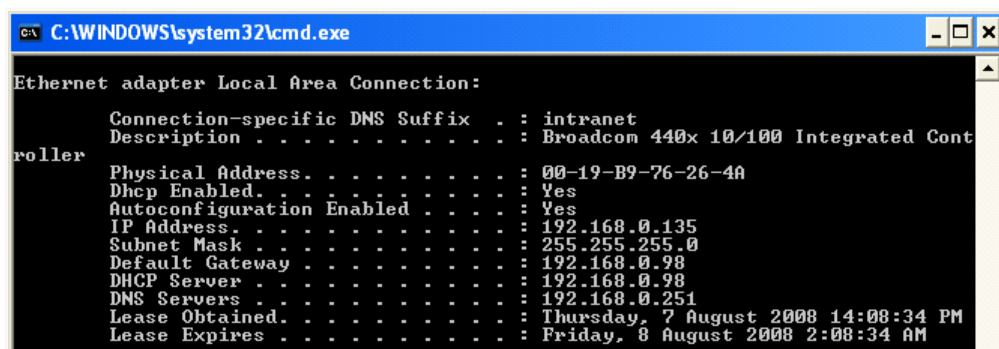
6.14 Resolving Ethernet Configuration Problems

Here are some basic tips to help you along the way with Ethernet configuration problems. The Windows operating system (and others) comes complete with many useful tools. First, you need to open a command window. This can be done by clicking on "Start" then "Run" and entering "CMD" and clicking OK.

Obtaining IP information about your PC

If you need to find out more information about your computer's Ethernet IP configuration, network gateways, and DNS servers, you can use a tool called "IPConfig".

Type "IPconfig /all" into your command window. The results are shown in window below.



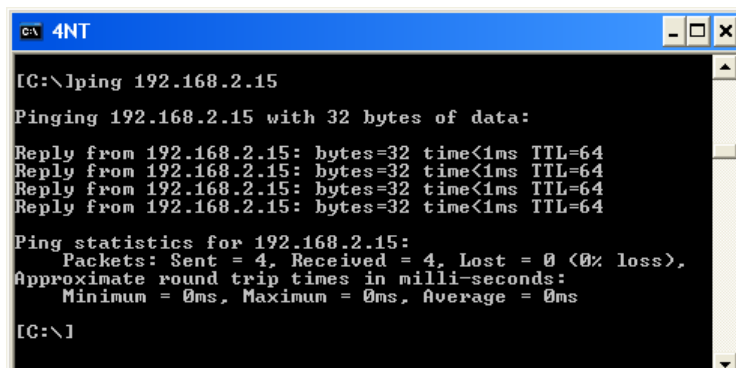
Checking IP connectivity

The most reliable way to check IP connectivity to a device is using the "Ping" utility. Type "ping xxx" where xxx is the complete IP address of the destination device you want to check. Ping will either respond with latency results (as shown) or say "timed out" if no connection was possible.

Here are some basic tips to help you along the way with Ethernet configuration problems. The Windows operating system (and others) comes complete with many useful tools. First, you need to open a command window. This can be done by clicking on "Start" then "Run" and entering "CMD" and clicking OK.

Obtaining IP information about your PC

If you need to find out more information about your computer's Ethernet IP configuration, network gateways and DNS servers, you can use a tool called "IPConfig". Type "IPconfig /all" into your command window. The results are shown in window below.



```
C:\ 4NT
[ C:\>ping 192.168.2.15

Pinging 192.168.2.15 with 32 bytes of data:

Reply from 192.168.2.15: bytes=32 time<1ms TTL=64
Reply from 192.168.2.15: bytes=32 time<1ms TTL=64
Reply from 192.168.2.15: bytes=32 time<1ms TTL=64
Reply from 192.168.2.15: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.2.15:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

[ C:\>]
```

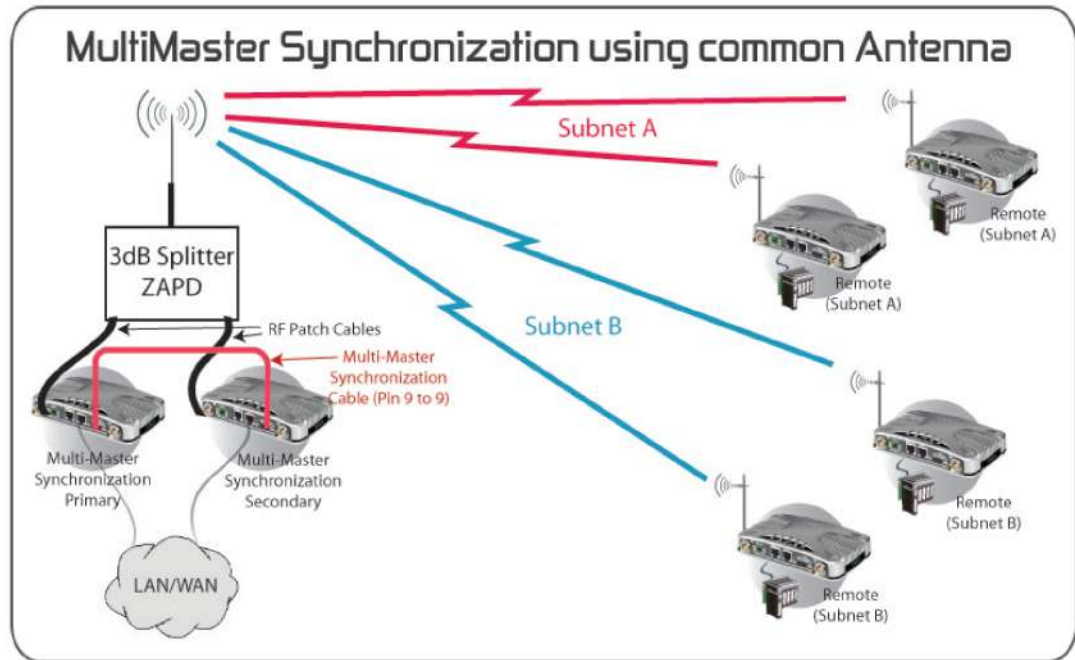
Checking IP connectivity

The most reliable way to check IP connectivity to a device is using the "Ping" utility. Type "ping xxx" where xxx is the complete IP address of the destination device you want to check. Ping will either respond with latency results (as shown) or say "timed out" if no connection was possible.

Repeated connections to multiple devices with same IP address

A common problem experienced when attempting to configure multiple radios with the same IP address (such as factory default radios). The problem is due to invalid MAC table entries. If you change your Ethernet connection between two devices with the same IP address quickly, you may need to reset the MAC look up table in your PC. You can do this by typing "arp -d*" in the command window.

6.15 Multi Master Synchronization



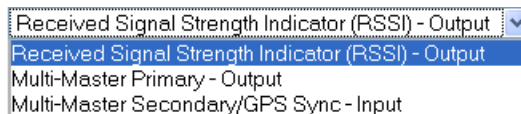
When operating two Access Points in Multi-master synchronization mode (Refer to [Part D – Features](#)^[29] for more information on this feature), the Access Point radios need to have the correct configuration options enabled.

The configuration required can be divided into two steps.

Software Configuration of the General Purpose IO

Configuration of this option can be found in “Configuration > Radio > Advanced Parameters” as shown below.

GeneralPurpose I/O



Access Point radios that are to be configured as the “Multi-Master Primary” need to have the General Purpose I/O pin configured as “Multi-Master Primary-Output”

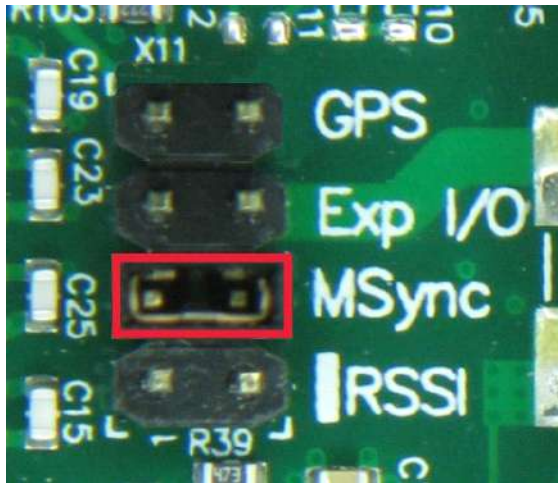
Access Point radios that are to be configured as the “Multi-Master Secondary” need to have the General Purpose I/O pin configured as “Multi-Master Secondary/GPS Sync - Input”

Hardware (Jumper) Configuration of the General Purpose IO

Access Point radios that are to be configured as the “Multi-Master Primary” need to have the General Purpose I/O pin jumper configuration set to MSync.

Access Point radios that are to be configured as the “Multi-Master Secondary” need to have the General Purpose I/O pin jumper configuration set to MSync.

All that is now required is to inter-connect Pin 9 on the Data Port between all Access Points.

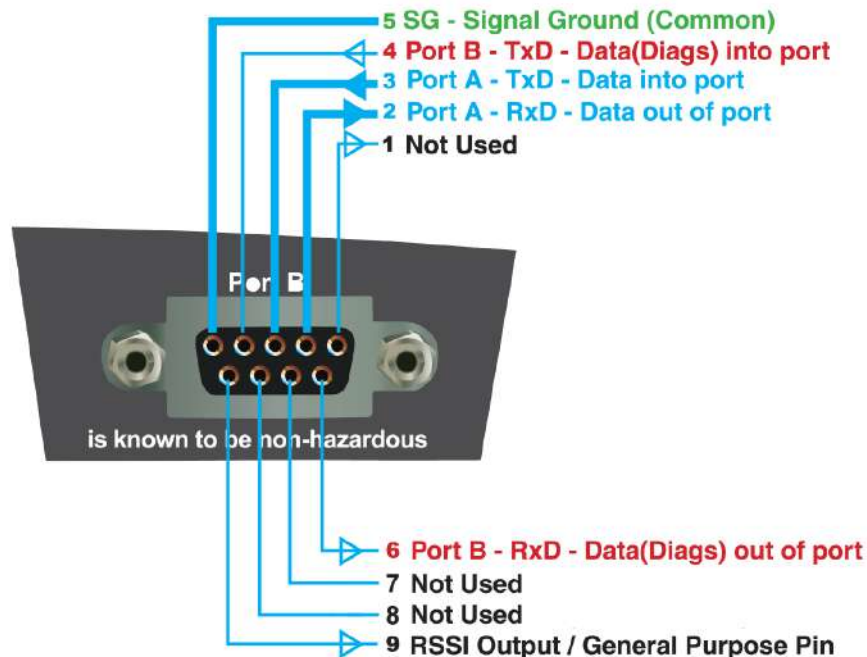


6.16 Text User Interface (TUI)

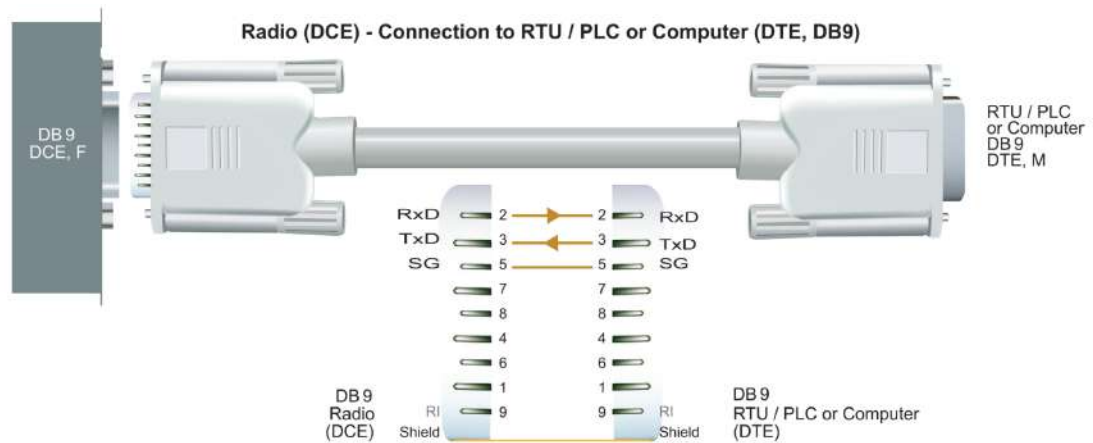
The text user interface (TUI) provides an alternative to the HTML web interface for configuration and diagnostics. The TUI can be accessed directly from the serial port of the J-Series or via a Telnet session. The TUI is enabled on Port A by default as well as Telnet. Access to the TUI via the serial port is useful if you have forgotten the IP address of the radio you are trying to configure or diagnose.

Serial TUI Interface

The serial TUI interface is accessed via the Port A/Port B interface as shown in the diagram below. By default, the TUI is accessed on Port A (Pins 2,3 & 5).

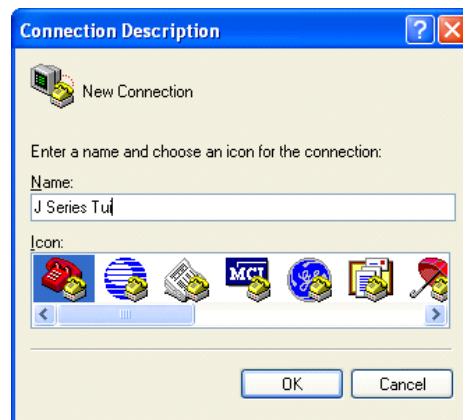


Connection to the PC requires a straight-through serial cable with Pins 2,3 & 5 connected. The J-Series does NOT have hardware handshaking therefore no other connections are required.



Once the J-Series is connected to your PC via a straight-through serial cable, Hyper Terminal can then be started to create a serial communications connection to the TUI. To do this, start the Hyper Terminal software: "Start Menu" > All Programs > Accessories > Communications > Hyper terminal. Once started, a new connection needs to be created.

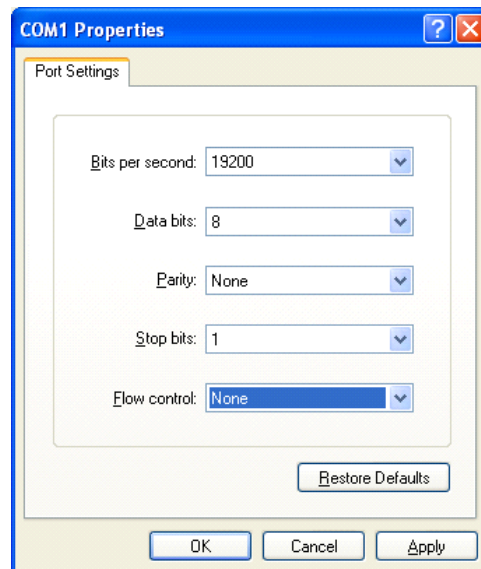
1. Enter a name for the new connection (i.e. J-Series TUI).



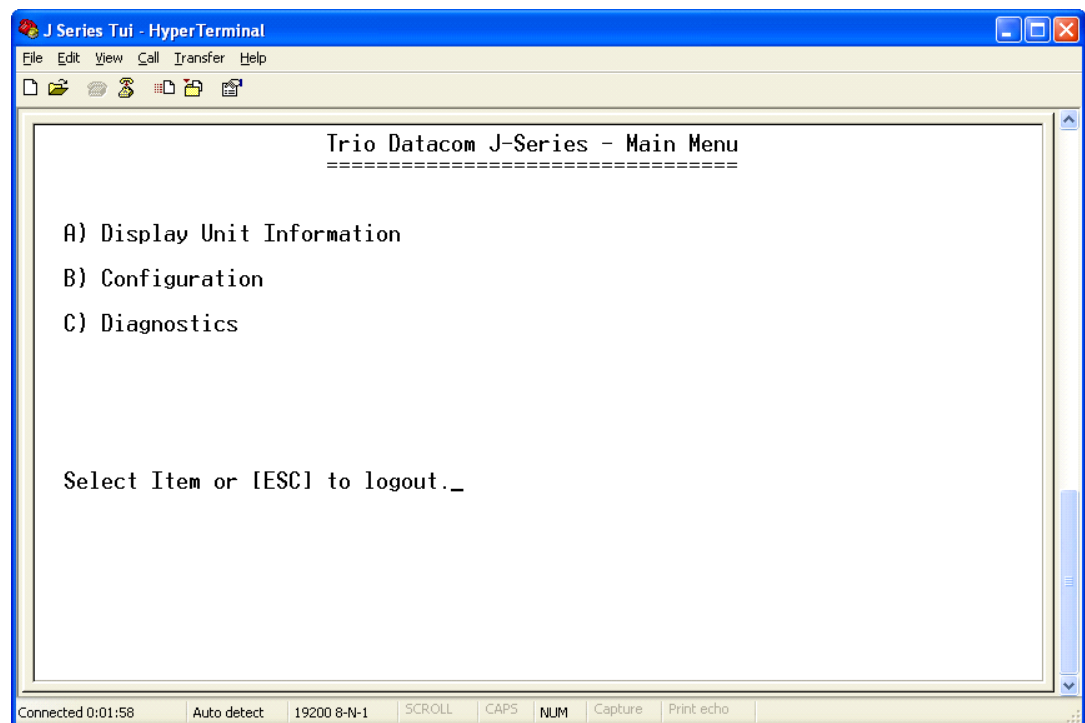
2. Select the appropriate communications port.



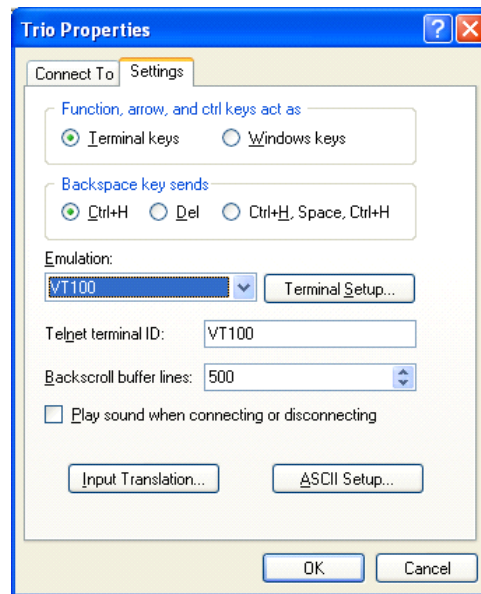
3. Ensure the COM port properties are set to: - > 19200, 8, N, 1 with NO flow control.



4. Press the "Enter" key and the TUI interface should display.

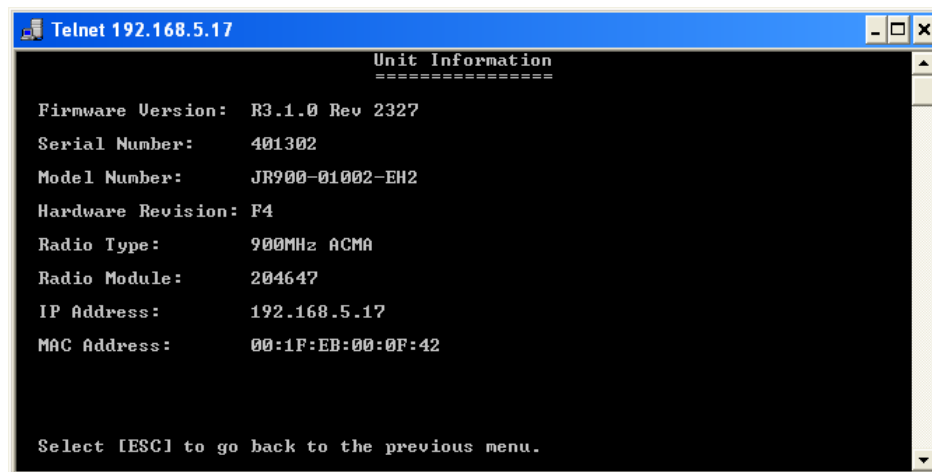


5. For complete functionality of the text interface, you need to change your terminal emulation to VT-100. To do this, go to "File > Properties" and in the Settings window pane ensure that the emulation is set to VT-100.



The TUI is divided into three distinct areas:

- **Unit Information** - Displays important information about the radio such as serial number, currently configured IP address and firmware pack version identification.



- **Configuration** - Provides access to the configuration of Network Parameters, Radio configuration, Security, SNMP and the Spectrum Analyzer.

```

Telnet 192.168.5.17
Configuration Menu
=====
A> Network
B> Radio
C> Serial Port A
D> Serial Port B
E> eDiags
F> Security
G> SNMP
H> Spectrum Analyzer
I> Activate Configuration
Select Item or [ESC] to go back

```

- **Diagnostics** - Provides access to the Diagnostics facilities in the radio.

```

Telnet 192.168.5.17
Diagnostics
=====

Unit                                Radio
====                                =====
Date:      Thu Jan  1 01:29:55 1970  Radio Rx Packets:      5636
Uptime(s): 5394.79                  Radio Rx Bytes:       405648
CPU Load:  1.22                     Radio Tx Packets:      537
                                      Radio Tx Bytes:       50055
Network                               Radio Forward Power <dBm>: 30.2
=====                             Radio Reverse Power <dBm>: 10.2
LAN 1 Rx Packets: 688                Radio USWR:            < 1.5:1
LAN 1 Rx Bytes: 59826                Radio RSSI <dBm>:      -53.9
LAN 1 Tx Packets: 5839                Supply Volts <V>:       12.1
LAN 1 Tx Bytes: 568550                Radio Temperature <C>: 30.5
LAN 2 Rx Packets: 0                  Radio Synched:          Yes
LAN 2 Rx Bytes: 0                    Acquired Access Point: 400213
LAN 2 Tx Packets: 3                  Lost Sync Count:        0
LAN 2 Tx Bytes: 238                  Failed Tokens:          1
                                      Retired Packets:        0
                                      Failed Packets:         16

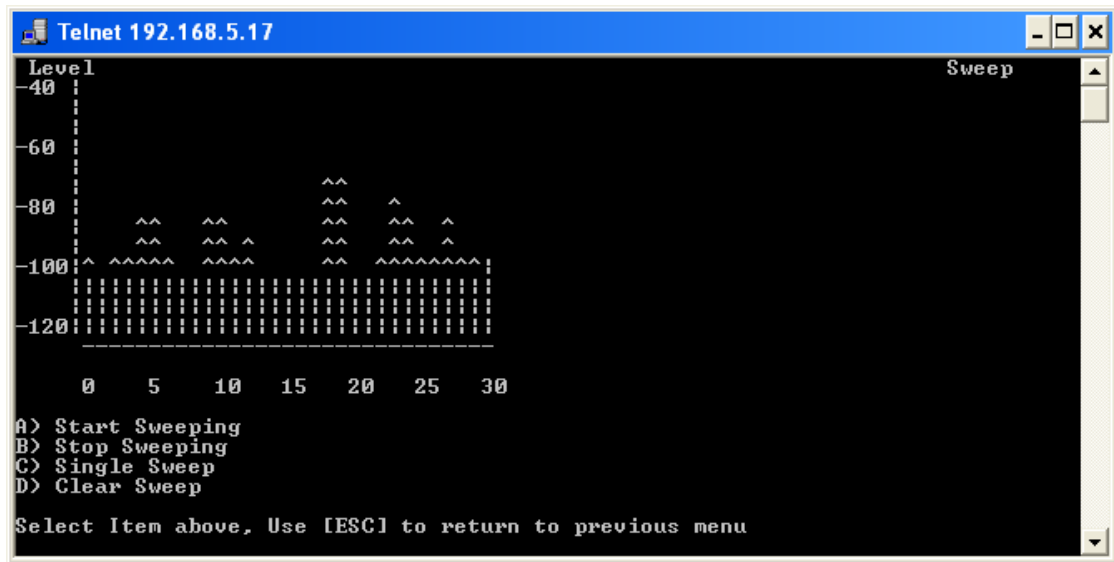
Select [ESC] to go back.

```

6.17 Spectrum Analyzer

The Spectrum Analyzer is a facility that allows user to observe interfering signals in the ISM band. In Access Point radios, channels that suffer from high levels of interference can be blocked out of the hopping pattern. The spectrum analyzer can only be accessed via the Text User Interface (TUI). An example of a spectrum analysis sweep is shown below.

The Spectrum Analyzer and channel lock out facility is not available on Brazilian compliant model types. (JR900-06002-xH0).



When configured for “Spectrum Analysis” mode:

- Only in Access Point radios can the user exclude channels using the channel lockout facility.
- The Spectrum Analysis mode is a special mode of operation where the radio scans each channel and measures the level of signals (interference) received. For this reason, the Spectrum Analysis mode can only be initiated from a local connection (not remotely via the radio channel).

Channel Lockout Facility

The channel lockout facility provides a mechanism for users to lockout channels. This allows the user to select of a number of channels which will be excluded from the Frequency Hopping Pattern.

The number of channels which can be excluded depends on country specific models of the J-Series radio. Even if only one channel needs to be excluded, you need to exclude a bank of channels as noted below. This is because the J-Series uses a highly advanced hopping algorithm that requires a prime number of hopping channels to be in the pattern (after channel exclusion).

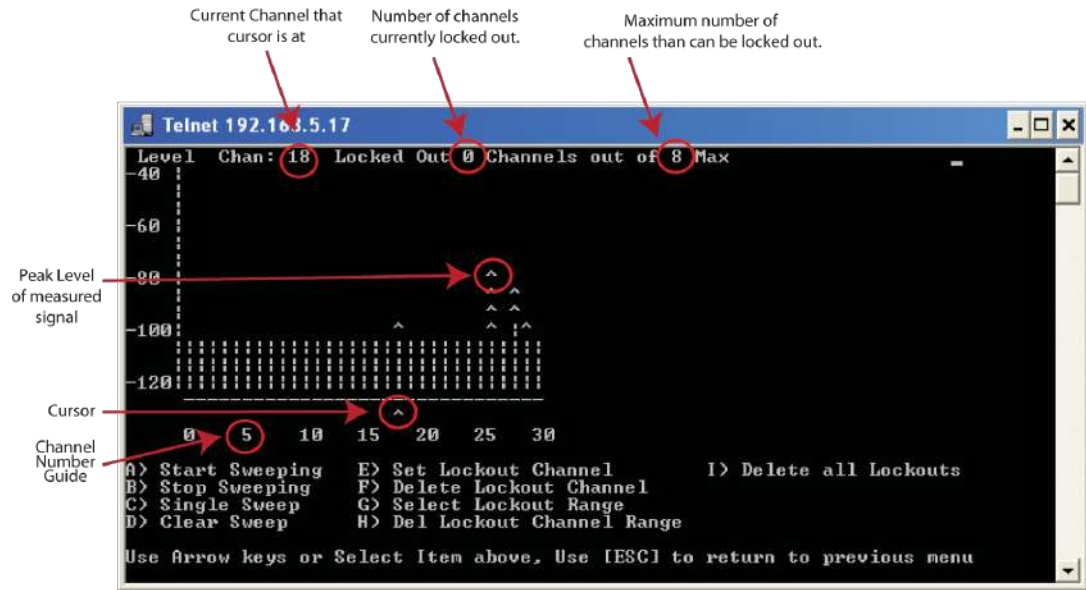
Country	Total	Excluded Channels
Australia (915...928 MHz)	31	2, 8
New Zealand (924...928 MHz)	17	4, 6, 10 or 12
Brazil (902-907.5 MHz and 915 MHz to 928 MHz)	43	None allowed
United States/Canada FCC (902-928 MHz)	67	6, 8 or 14
2.4 GHz (Europe)	73	2,6,12,14,20,26,30,32,36, 42,44,50,54,or 56
2.4 GHz (International)	197	6,16,24,30,40,48,58,66, 70,84,90,96,100,108 or 118

Using the Channel Lockout facility

To lockout channels using the facility in the text user interface, perform the following steps.

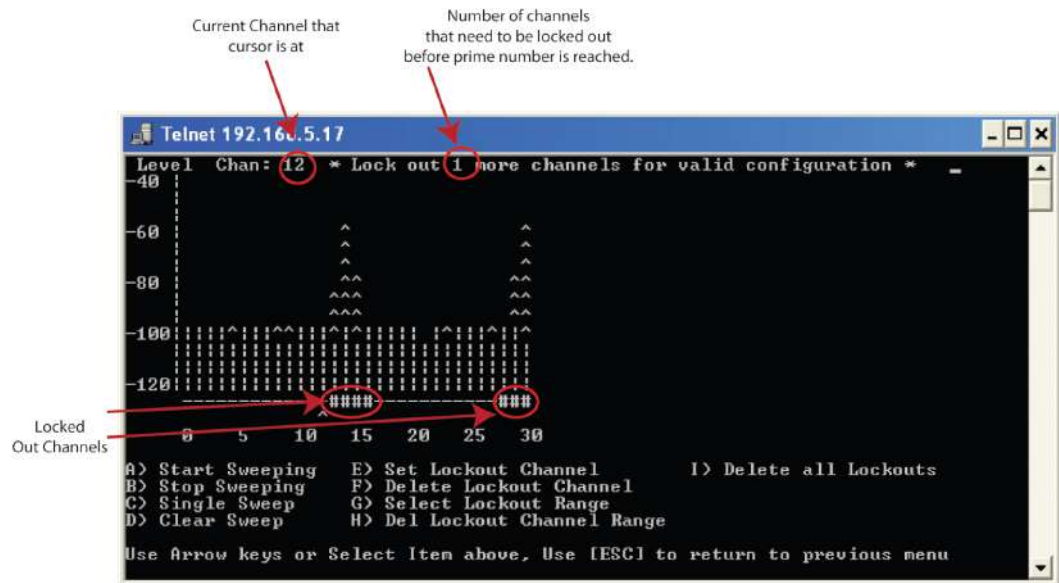
1. Connect to the text user interface of the Access Point. Note: You need to be locally connected, either via Telnet or the Serial interface.
2. Browse to the Spectrum Analyzer facility. This is found under "Configuration > Spectrum Analyzer"
3. Perform a repetitive sweep of the spectrum (by selection option "A") and leave this sweep running for several minutes. Once you are satisfied that the sweep has been completed over an adequate length of time, stop the sweep using option "B"

You should now be presented with a screen that looks similar to the one shown below.



Note that at the top of the screen, the text user interface (TUI) displays the current channel number that the cursor is located at, the number of channels that are currently locked out and the maximum number of channels that can be locked out.

- Using your left and right arrow keys, move the cursor over the channel number you wish to exclude and set the channel for exclusion using option "E" as shown below.



Note that locked out channels are noted with a "#" character. The TUI also advises how many more channels need to be locked out to have a prime number of channels (not locked out) remaining. When finished, press the "ESC" key which will return you to the programming interface.

6.18 Telnet Interface

The text user interface can be accessed via Telnet. This is convenient if you are remotely connected to a J-Series via an Ethernet network. The Telnet interface provides high speed access to the text user interface via a “Telnet” session. Most computer operating systems come with integrated Telnet software. For Windows based operating system, you can initiate a Telnet session using the command line interface.

Before you can connect to the text user interface (TUI) via Telnet, ensure that the Telnet interface is enabled. For security reasons, the Telnet interface is disabled by default. It can be enabled using the Web based configuration programmer. Enable the interface via the “Configuration > Security” menu item as shown below.

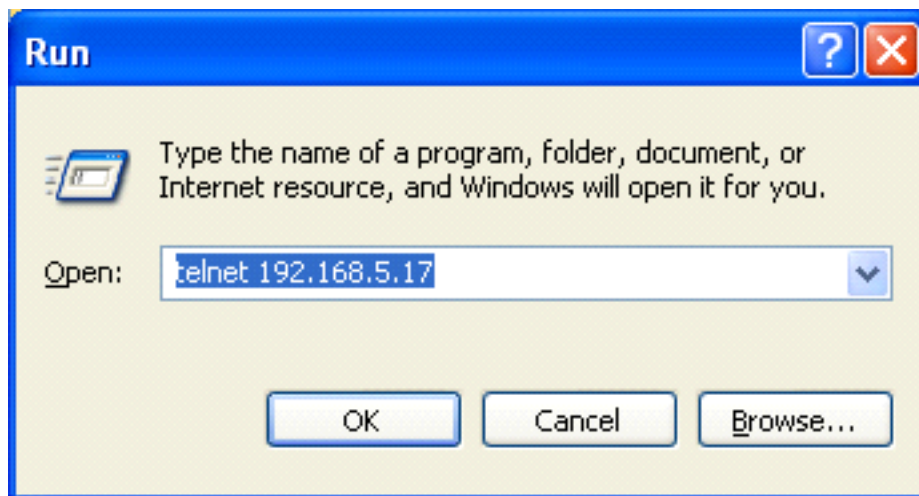
Telnet Terminal

☒ Enable ☐ Disable

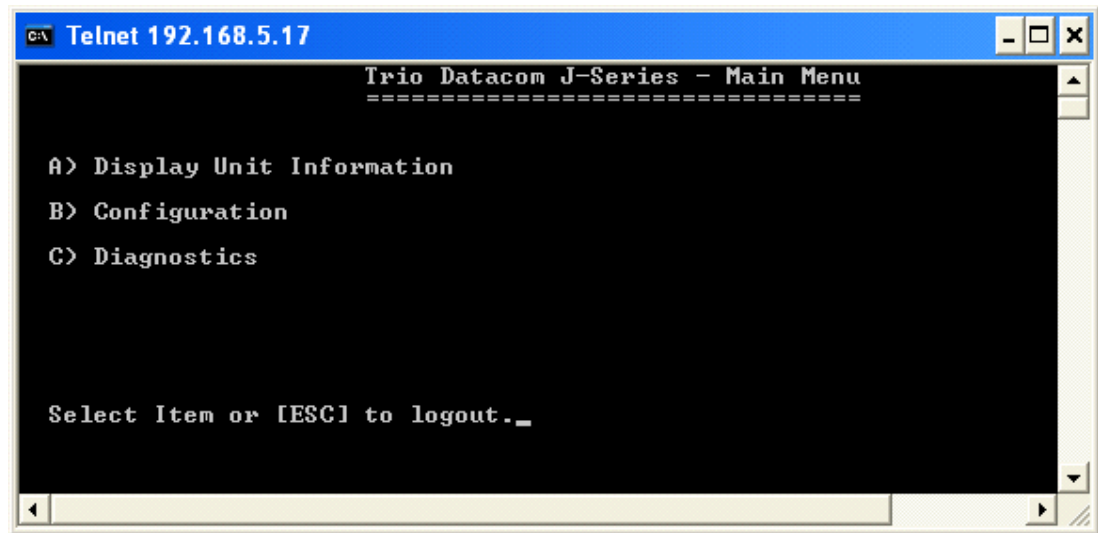
Telnet Terminal:

Set to enable Telnet Sessions.

To start a Telnet session, open a command window via “Start > Run” and type “Telnet xxx.xxx.xxx.xxx” where xxx is the IP address of the target radio. See example below.



If the Telnet connection was successful, the following screen will be displayed.



Note: If security password protection has been enabled, you will first need to enter the appropriate username and password.

6.19 Secure Shell (SSH)

SSH provides a secure alternative to standard Telnet. To access the J-Series TUI via the embedded SSH server, an SSH client needs to be used. The following example shows how to access the J-Series TUI using a commonly used Windows SSH client called Putty.

Before you can connect to the text user interface (TUI) via SSH, ensure that the SSH server within the J-Series is enabled (Set to configuration). For security reasons, the SSH interface is disabled by default. It can be enabled using the Web based configuration programmer. Enable the interface via the "Configuration > Security" menu item as shown.

Upon enabling SSH, you will also be required to fill out a user name and password. Ensure you record this user name and password for future use.

For the SSH client to know it is communicating with the device it is addressing (not a man in the middle), the client needs to first authenticate the server.

Administration

Security ☒ Enable ☐ Disable

Login name

Password

Confirm Password

Ssh Terminal

The process the client will take to authenticate the server is as follows:

- The client requests the device finger print from the server it is trying to connect to.
- Once the client has received the server's finger print, it will check it's own records to see whether it already has this finger print in memory.
- If it does have the finger print on record, the connection between the client and the server should automatically begin.
- If the client does not have the finger print in memory, a security alert will appear, warning the user that either an attacker could be intercepting the device as it does not have the finger print on record, or it is a new device that it has not connected to before.

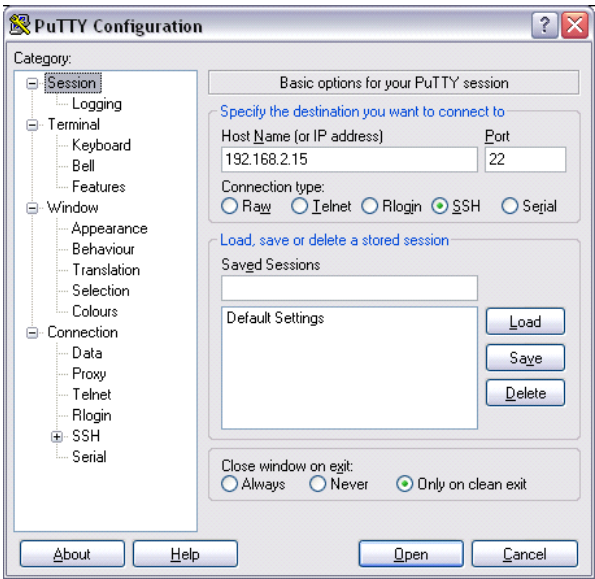


As there is no way of differentiating between a man in the middle attack or a first time connection due to the finger print not on the client's records, it is advised that the SSH server (J-Series) is always connected locally to the client and read before they are deployed in the field. This will allow the client to store the server's finger print on record and will help prevent any chances of undetected man-in-the-middle attacks.

Once a finger print has been stored into memory, they can be extracted from the registry (Putty example only) at: HKEY_CURRENT_USER\Software\SimonTatham\Putty\SSHHostKeys. This can then be deployed into another client PC if required.

Configure the SSH client (in this case Putty) to interface correctly with the embedded J-Series SSH server.

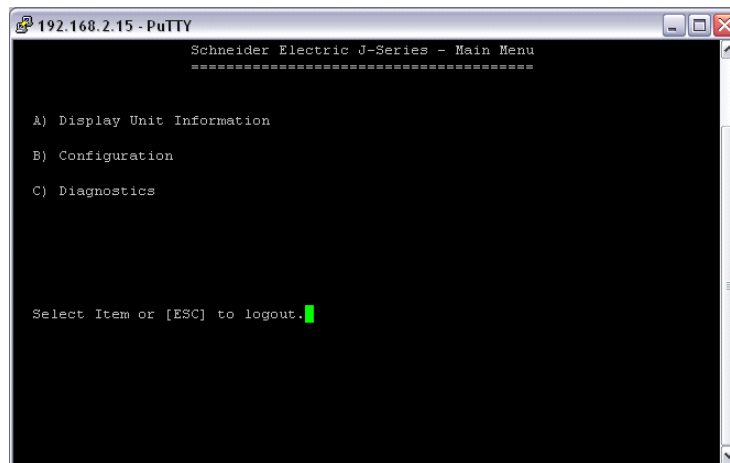
The Port number for the embedded J-Series SSH terminal is 22. This is a standard and is not user definable.



The SSH terminal also requires a user name and password to be configured. Upon logging into the J-Series via SSH, the user will be prompted for the user name and password.



Once the correct username and password have been entered, the J-Series will grant access to the TUI main menu.



6.20 SNMP

As of J-Series Firmware V3.5.0, SNMP with notifications is supported. The J-Series SNMP Interface supports:

- Supports RFC1213 (Unit name, Unit Location, Firmware, Uptime, etc) Note: Details about RFC1213 and the SNMP parameters included in this standard can be found in this link: <http://www.ietf.org/rfc/rfc1213.txt>
- Supports Radio and Ethernet Diagnostics (as seen in the HTML Diagnostics overview)
- SNMP V1 & V2c
- SNMP notifications which include traps and informs

6.20.1 Notifications

J-Series notifications are unsolicited SNMP messages designed to inform a user of a change in state within the J-Series that may cause an issue on the radio system. The J-series supports two types of notifications:

- **Traps:** Traps are low bandwidth consuming UDP notifications that have no requirement for a response. If the message is lost along the way to the destination IP address, the message will be lost.
- **Informs:** Informs are essentially a trap that requires a response from the destination IP address once a notification has been sent. This gives informs more reliability getting to a destination as the J-Series will support retries and timeout periods.

6.20.2 MIB Files

Distributed with the J-Series firmware are three MIB files which provide structure definitions for the SNMP objects. The MIBs are suitable for importing into most common SNMP browsers including Castle Rock. Definitions for each SNMP object are noted as comments in the MIB files. Only a summary of these objects are noted in this user manual.

6.20.3 Status Levels for SNMP Parameters

There are a maximum of three status levels for the J-Series SNMP parameters. Each one is also represented with a status number. The status levels and corresponding numbers are as follows:

- **Normal - 1:** The 'Normal' status level will be displayed within a notification when a parameter has recovered from an alarm state. For example: the input voltage to the J-Series drops below 9VDC, this will cause a 'critical alarm' notification to be sent. Once the input voltage has recovered back to normal operating voltage, a 'Normal' status notification will be sent to inform a user that the critical error has recovered.
- **User alarm - 2:** A 'User alarm' notification will be sent when a parameter within the J-Series falls out-side of the user defined alarm limits.
- **Critical alarm - 3:** A 'Critical alarm' notification will be sent when a parameter within the J-Series falls out-side of the unit's hardware specification.

6.20.4 Implementation of multiple use objects

Some SNMP objects such as Tx Power need to be separately reported in dual antenna bridge mode. To achieve this but to keep the .MIB files common for all modes of operation (access point, single and dual antenna bridges, and remotes) the object is provided as a table. The first cell in the table represents the value associated with Antenna 1. The second cell in the table represents Antenna 2. This should be noted when importing the .MIB files into your SNMP management package.

6.20.5 Summary of SNMP Parameters Supported

Object name	Object description
General Group:	
serialNumber	Serial number of the J-Series
modelName	Model number of the J-Series
hardwareRevision	Hardware revision of the J-Series
radioType	The type of radio module in the J-Series
firmwareRevision	The firmware revision the J-Series
date	The date as reported by the J-Series
time	The time as reported by the J-Series
utcTimeOffset	Time offset from UTC for the J-Series local time zone
upTime	The uptime of the J-Series
primaryNtpServer	Primary Network Time Protocol (NTP) domain name

cpuLoad	Average CPU utilization (%) for the past 15 minutes
supplyVoltage	Supply Voltage of the J-Series in mV
temperatureC	The internal temperature of the J-Series (degrees C)
temperatureF	The internal temperature of the J-Series (degrees F)
ipAddress	The IP address of the J-Series.
Radio Group:	
radioMode	The operating mode of the radio
subnetIdTable	Table of subnet ID's. If there are two rows in this table then the first row represents the upstream subnet ID and the second row represents downstream subnet ID. If there is only one row in the table then that represents the subnet ID.
radioReceivedPackets	Number of packets received from the radio link
radioTrasnmittedPackets	Number of packets transmitted over the radio link
radioForwardPowerTable	Table of radio forward powers. If there are two rows in this table then the first row represents the forward power for ANT1 and the second row represents the forward power for ANT2. If there is only one row in the table then that represents the forward power.
radioReversePowerTable	Table of radio Reverse powers. If there are two rows in this table then the first row represents the Reverse power for ANT2. If there is only one row in the table then that represents the Reverse power.
radioVswrTable	Table of radio VSWR's. If there are two rows in this table then the first row represents the VSWR for ANT1 and the
radioRssiTable	Table of RSSI values. If there are two rows in this table then the first row represents the RSSI value for ANT1 and
syncStatus	The synchronization status of the J-Series.
failedTokens	Number of failed tokens (for Remotes or up-stream side of a Bridge).
retriedPackets	Number of packets that have exceeded the retry limit (for Remotes or up-stream side of a Bridge).
failedPackets	Number of incoming packets that have been discarded due to an incorrect CRC.

hopInterval	The hop interval (ms) of the J-Series.
radioDataRate	The over-the-air data rate of the J-Series.
accessPoint	The serial number of the current Access Point.

Security Group:	
snmpVersion	Default SNMP version.
consoleLoginStatusA	Console login status for Port A.
consoleLoginStatusB	Console login status for Port B.
numberOfActiveTelnetSessions	Number of active Telnet sessions.
telnet1SessionStatus	Status of the first of three possible Telnet sessions.
telnet1IpAddress	IP address of the remote device using the first of three possible Telnet sessions.
telnet2SessionStatus	Status of the second of three possible Telnet sessions.
telnet2IpAddress	IP address of the remote device using the second of three possible Telnet sessions.
telnet3SessionStatus	Status of the third of three possible Telnet sessions.
telnet3IpAddress	IP address of the remote device using the third of three possible Telnet sessions.
encryptionStatus	Encryption status.
LAN Group:	
lan1LinkStatus	The link status of LAN port 1
lan1LinkSpeed	The link speed of LAN port 1
lan1LinkMode	The link mode of LAN port 1 (half duplex/Full duplex)
lan2LinkStatus	The link status of LAN port 2
lan2LinkSpeed	The link speed of LAN port 2
lan2LinkMode	The link mode of LAN port 2 (half duplex/Full duplex)

Error Group:	
fatalError	J-Series fatal alarm.
pllLocked	J-Series PLL out of lock alarm.
oldProtocol	J-Series detects an old protocol
configurationRecordPresent	J-Series configuration record present
radioVswrErrorTable	J-Series High VSWR detected
externalSupplyVoltageErrorState	J-Series external voltage alarm
temperatureErrorState	J-Series temperature alarm
radioRssiErrorTable	J-Series RSSI alarm
radioTxPowerErrorTable	J-Series Tx power alarm
globalErrorState	J-Series global alarm
syncErrorState	J-Series synch alarm
Notification Group:	
notificationFatalError	J-Series Fatal alarm notification.
notificationPllLock	J-Series PLL out of lock alarm notification.
notificationOldProtocol	J-Series detects and old protocol notification
notificationConfigurationRecord	J-Series configuration record present notification
notificationVswr	J-Series High VSWR detected notification
notificationSupplyVoltage	J-Series external voltage alarm notification
notificationTemperature	J-Series temperature alarm notification
notificationRssi	J-Series RSSI alarm notification
notificationTxPower	J-Series Tx power alarm notification
notificationSync	J-Series synch alarm notification
notificationApChanged	J-Series Access Point change alarm notification

notificationIpAddressChanged	J-Series IP address has changed.
notificationGlobalErrorChanged	J-Series global alarm notification
notificationDiagnostic	J-Series Diagnostics notification

6.20.6 Configurations of SNMP Parameters

To configure the SNMP Parameters within the J-Series web user interface, log into the J-Series and go to: Setup > SNMP. The following configuration parameters will be displayed.

SNMP

SNMP Enabled

Enabled

SNMP Version

2c

- **SNMP Enabled:** Toggles the operation of the internal J-Series SNMP agent.
- **SNMP Version:** Allows the user to configure the J-Series to operate using SNMP protocols 1 or 2c.

Community Strings

SNMP Read Community String

SNMP Read/Write Community String

- **SNMP Read Community String:** The community string for reading (getting) SNMP objects from the J-Series.
- **SNMP Read/Write Community String:** The community string for reading and writing (setting) SNMP objects within the J-Series.

SNMP Notifications

SNMP Notifications	Enabled ▼
SNMP Notification Version	2c ▼
Use informs	Yes ▼
Inform timeout	1
Inform retries	0
Notification Community String	*****
Manager 1 IP Address	
Manager 2 IP Address	
Manager 3 IP Address	
Manager 4 IP Address	

- **SNMP Notifications:** Toggles the operation of SNMP notifications sent from the J-Series.
- **SNMP Notification Version:** Allows the user to configure the J-Series to send notifications using SNMP protocols 1 or 2c.
- **Use informs:** Toggles between notification types. When enabled, informs will be sent, if disabled, traps will be sent.
- **Inform timeout:** Only available when informs are enabled. The amount of time in seconds the J-Series will wait for a response after it has sent an inform. Once the timeout reaches 0, a retry will be sent.
- **Inform retries:** Only available when informs are enabled. The amount of retries the J-Series will attempt to perform before the inform is discarded.
- **Notification Community String:** The community string for Notifications.
- **Manager 1 IP Address:** The IP address the J-Series will send notifications to.
- **Manager 2 IP Address:** The IP address the J-Series will send notifications to if enabled in addition to other manager IP addresses set. This is used in redundant systems.
- **Manager 3 IP Address:** The IP address the J-Series will send notifications to if enabled in addition to other manager IP addresses set. This is used in redundant systems.
- **Manager 4 IP Address:** The IP address the J-Series will send notifications to if enabled in addition to other manager IP addresses set. This is used in redundant systems.

6.20.7 Customizing SNMP notifications

Customizations can be made on which SNMP notifications will be active along with the limits that will trigger a notification.

To configure which notifications are enabled, see the alarms section found within the J-Series web user interface, to configure the limits of an alarm see the alarm limits section found within the J-Series web user interface. The configurable notifications available are as follows:

Voltage

- **Status level states:** Normal (1), User alarm (2) and Critical alarm (3)
- **User alarm limits:** Configurable upper and lower limit, 10000 to 30000 (mVDC)
- **Critical alarm limits:** Lower hardware limit: 9500 (mVDC), Upper hardware limit: 30500 (mVDC)
- **Hysteresis:** +/- 500 (mVDC)
- **OID:** .1.3.6.1.4.1.33302.10.10.7

Temperature

- **Status level states:** Normal (1), User alarm (2) and Critical alarm (3)
- **User alarm limits:** Configurable upper and lower limit, -40 to +70 (Deg C)
- **Critical alarm limits:** Upper hardware limit: +75 (Deg C). (No lower limit)
- **Hysteresis:** +/- 5 (Deg C)
- **OID:** .1.3.6.1.4.1.33302.10.10.6

Access point changed

The Access point changed notification is not a part of the J-Series MIB event group, which means it only sends a status change notification, not necessarily indicating an event. This notification is useful when used in SmartPath™ applications where remotes and bridges can acquire different upstream paths at different times. The notification will include the serial number of the upstream device the device is synchronized to.

- **OID:** .1.3.6.1.4.1.33302.10.10.11

Global error

The Global error notification is used to indicate changes of state within a group of alarm parameters. These alarm parameters include: Voltage, temperature, Tx Power, VSWR, PLL Lock alarm, sync alarm, fatal alarm and old protocol alarm.

- **Status level states:** Normal (1), User alarm (2) and Critical alarm (3).
- **User alarm limits:** defined by each user defined parameter limit.
- **Critical alarm limits:** Varies for each parameter.
- **Hysteresis:** Varies for each parameter.

- **OID:** .1.3.6.1.4.1.33302.10.10.13

Heartbeat

The heartbeat notification used to provide diagnostic information on a J-Series. A notification is sent periodically, where the time between heartbeat notifications is defined by the user. The group of diagnostic parameters included within each heartbeat notification include: system name, system location, serial number, model number, temperature (Deg C), temperature (Deg F), supply voltage, system up time, global error state, Tx Power, VSWR and RSSI.

- **OID:** .1.3.6.1.4.1.33302.10.10.14

Fatal error

- **Status level states:** Normal (1) and Critical alarm (3).
- **Critical alarm limits:** No limits, if the radio detects a fatal alarm it will send a Critical alarm notification.
- **OID:** .1.3.6.1.4.1.33302.10.10.1

PLL lock error

- **Status level states:** Normal (1) and Critical alarm (3).
- **Critical alarm limits:** No limits, if the radio detects a PLL lock alarm it will send a Critical alarm notification.
- **OID:** .1.3.6.1.4.1.33302.10.10.2

Old protocol

- **Status level states:** Normal (1) and Critical alarm (3).
- **Critical alarm limits:** No limits, if the radio detects an old non-supported protocol it will send a Critical alarm notification.
- **OID:** .1.3.6.1.4.1.33302.10.10.3

Sync status

- **Status level states:** Normal (1) and Critical alarm (3).
- **Critical alarm limits:** No limits, if the radio loses synchronization with an upstream device, it will send a Critical alarm notification.
- **OID:** .1.3.6.1.4.1.33302.10.10.10

RSSI

- **Status level states:** Normal (1) and User alarm (2).
- **User alarm limits:** Configurable upper and lower limit, -140 to 0 (dBm).

- **Hysteresis:** +/- 10 (dBm).
- **OID:** .1.3.6.1.4.1.33302.10.10.8

Transmit power

- **Status level states:** Normal (1) and User alarm (2).
- **User alarm limits:** Configurable upper and lower limit, 0 to +40 (dBm).
- **Hysteresis:** +/- 10 (dBm).
- **OID:** .1.3.6.1.4.1.33302.10.10.9

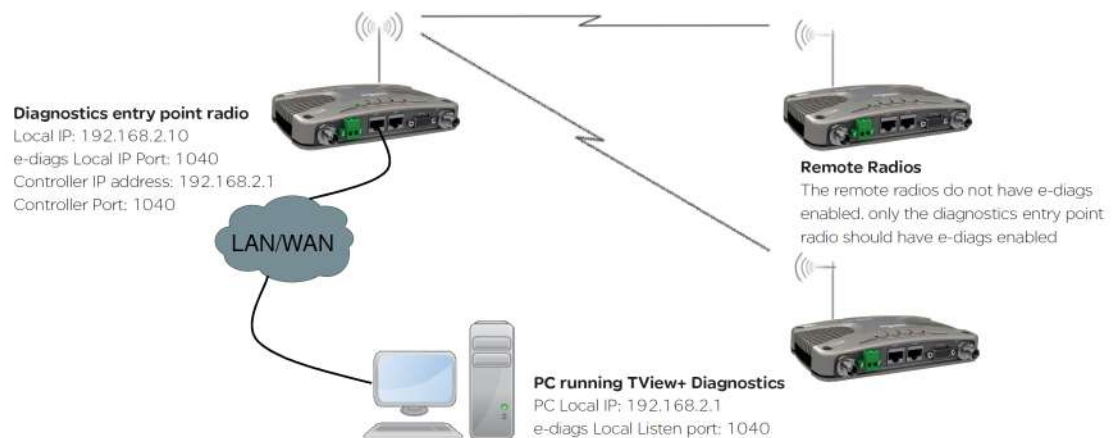
VSWR

- **Status level states:** Normal (1), User alarm (2) and Critical alarm (3).
- **User alarm limits:** Optional limit, 1.5:1, 2:1 or 3:1
- **Critical alarm limits:** hardware limit: >10:1.
- **Hysteresis:** None.
- **OID:** .1.3.6.1.4.1.33302.10.10.5

6.21 e-Diags Example

e-Diagnostics (also known as e-Diags) is a feature of the TVIEW+ Diagnostics software that encapsulates the TVIEW+ Diagnostics protocol in an Ethernet UDP/IP packet. Together with the e-Diags server embedded into each J-Series radio, the user can monitor the J-Series Ethernet radios network using the TVIEW+ Diagnostics software over an Ethernet LAN/WAN. A typical use diagram is shown below.

For more information on the features and benefits of the TVIEW+ Diagnostics software, refer to the TVIEW+ Management Suite Brochure and for additional technical details, the TVIEW+ Diagnostics User Manual.



The following instructions will explain how to poll J-Series radios using e-Diags on a synchronized network.

1. Enable e-Diags within the 'diagnostics entry point' radio and configure the following parameters (The example above shows where the entry point radio is located):
 - Local Port number - The port number the e-Diags session (within the PC) will address all e-Diags data to (example uses: 1040)
 - Controller IP address - The IP address of the PC running the e-Diags session
 - Controller Port number - The port number the PC has been configured to use for e-Diags.
2. Ensure the TVIEW+ Diagnostics software has been installed on your PC.
3. Open the TVIEW+ Diagnostics software on the PC and configure the following items (for detailed instructions on the TVIEW+ Diagnostics software, refer to the TVIEW+ Diagnostics user manual):
 - Create a list (database) of J-Series radios that need to be polled for diagnostics. Each data base entry needs to have the communications port set to e-Diags (Ethernet) and configured to use the IP address and e-Diags port number of the diagnostics entry point radio. Each serial number entered needs also to be correct. Other information can also be specified.
 - Define the IP address and local listening port number for the e-Diags session (controller address and port number). This can be configured in Settings > e-Diags Port settings. The IP address and port number configured need to match the controller IP address and controller port number specified within the e-Diags setting of the diagnostics entry point radio.

This now completes the requirements for configuring e-Diags. The operation of e-Diags for a typical poll/response diagnostics transaction is as follows:

1. The TVIEW+ Diagnostics software constructs a UDP/IP data gram which targets the embedded e-Diags server within the entry point radio as configured in each entry within the diagnostics database.
2. The UDP Datagram is placed onto the LAN/WAN which routes the datagram onto the radio network.
3. When the datagram arrives at the entry point radio & port, the UDP encapsulation is removed and the datagram contents is transmitted over the air to the target radio.
4. The target radios diagnostics response is constructed as a datagram and the entry point radio will reconstruct a UDP/IP datagram out of the diagnostics message and send it to the PC operating e-Diags.

6.22 e-Diags Parameters

Information on the various e-Diags parameters can be found below. Multiple controller IP addresses are set when there is more than one e-Diags server polling the radio system at a time. This is typical in redundant systems.

eDiags

eDiags ☒ Enable ☐ Disable

- **eDiags:** Enables/disables the internal e-Diags server within the radio

Local IP Port

- **Local IP Port:** The port number the J-Series will receive e-Diags messages on

Controller 1 IP Address

Controller 1 IP Port

Controller 2 IP Address

Controller 2 IP Port

Controller 3 IP Address

Controller 3 IP Port

Controller 4 IP Address

Controller 4 IP Port

- **Controller 1 IP Address:** The IP address the J-Series will send e-Diags messages to.
- **Controller 1 IP Port:** The IP port the J-Series will address e-Diags messages to for Controller 1.
- **Controller 2 IP Address:** The IP address the J-Series will send e-Diags messages to, in addition to other Controller IP addresses set. This is used in redundant systems.
- **Controller 2 IP Port:** The IP port the J-Series will address e-Diags messages to for Controller 2.
- **Controller 3 IP Address:** The IP address the J-Series will send e-Diags messages to, in addition to other Controller IP addresses set. This is used in redundant systems.

- **Controller 3 IP Port:** The IP port the J-Series will address e-Diags messages to for Controller 3.
- **Controller 4 IP Address:** The IP address the J-Series will send e-Diags messages to, in addition to other Controller IP addresses set. This is used in redundant systems.
- **Controller 4 IP Port:** The IP port the J-Series will address e-Diags messages to for Controller 4.

6.23 Ethernet Filtering

This section provides the configurable parameters for MAC layer filtering. The various options of MAC filtering include:

Filtering

Traffic type	All All Arp and unicast Unicast
Single source	☒ Enabled ☐ Disabled
Source MAC address	FF:FF:FF:FF:FF:FF

Allow all Ethernet traffic

Allowing all Ethernet traffic to be sent over the air will effectively turn the MAC layer filtering OFF.

Allow ARP and Unicast

Allowing ARP and Unicast traffic to only be sent over the air will filter out all other protocols such as spanning tree and broadcast messages which can be produced by a typical LAN/WAN and overwhelm a narrow band radio link.

Allow Unicast only

Allowing Unicast traffic to only be sent over the air will filter out all other protocols such as spanning tree, broadcast and ARP messages which can be produced by a typical LAN/WAN and overwhelm a narrow band radio link.

Allow traffic from single MAC only

Allowing traffic from a single MAC address will allow all protocols from the specified MAC address and filter out all other traffic from any other MAC address.

7 Part G - Quick Start Guide

See:

- [Device Hardening](#) ¹¹⁰
- [Point to Point Ethernet Link Setup](#) ¹¹⁰

- [Point to Point - TCP Serial Device Server Setup Guide](#) ^[114]
- [Point to Point - UDP \(Unicast\) Serial Device Server Setup Guide](#) ^[116]
- [Point to Multipoint - UDP \(Multicast\) Serial Device Server Setup Guide](#) ^[118]
- [Point to Multipoint with Peer to Peer - UDP \(Multicast to Multicast\) Serial Device Server Setup Guide](#) ^[120]
- [Point to Point - Modbus/TCP to Modbus RTU Setup Guide](#) ^[122]
- [Point to Multipoint - Modbus/TCP to Modbus RTU Setup Guide](#) ^[123]

7.1 Device Hardening

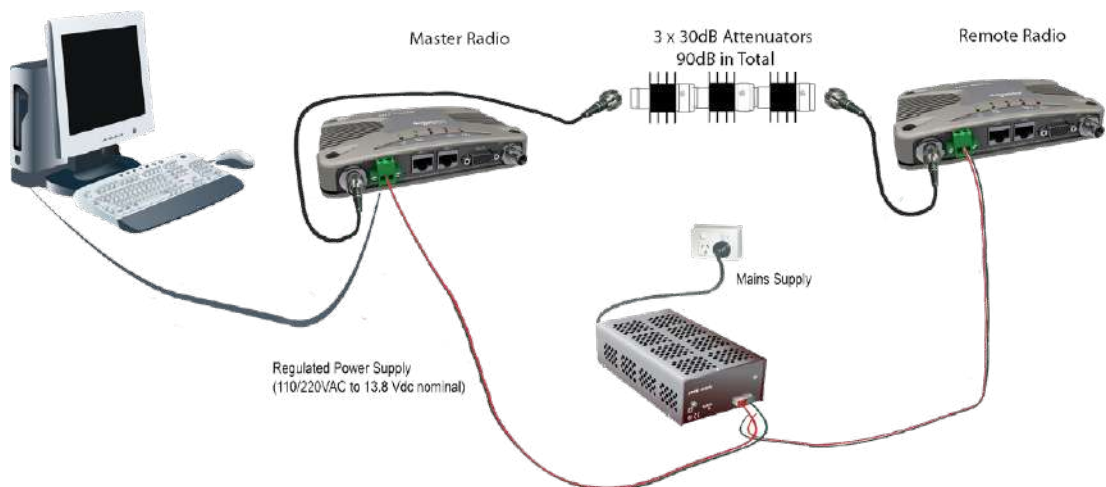
When the radio is in a factory default state, or when a user password has not yet been configured, the radio is vulnerable to unauthorized access which may compromise the integrity and authenticity of the radio. While the radio is in this state, do not connect it to an untrusted network.

To implement device hardening, a login name and password should be configured under Setup > Administration.

It is also recommended to use SSH instead of Telnet (see [Secure Shell \(SSH\)](#) ^[94]) to access the text user interface, and HTTPS (see [Connection to WUI - Secure HTTPS Connection](#) ^[77]) instead of HTTP to access the web interface.

7.2 Point to Point Ethernet Link Setup

This is the sequence of steps required for configuring two J-Series in a point-to-point network. One will be configured as an Access Point and the other as a Remote.



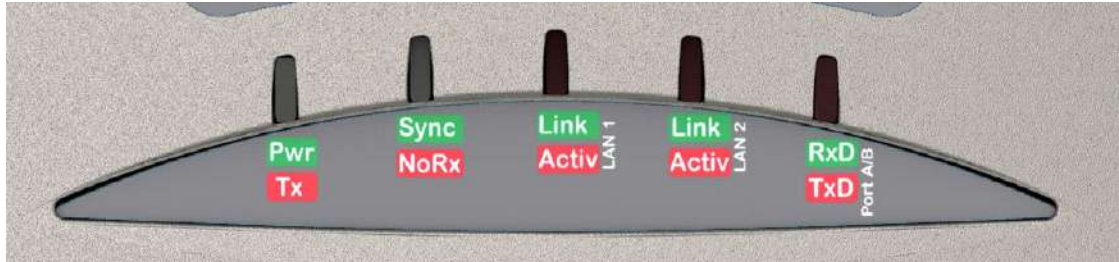
Step 1 - RF and DC power connection

Connect a whip antenna to the ANT1 TNC connector of both radios.

NOTICE**HAZARD OF EQUIPMENT DAMAGE**

Ensure the whip antennas you are using are for the correct frequency otherwise a high VSWR error may occur.

Failure to follow these instructions can result in equipment damage.

**⚠ CAUTION****RISK DUE TO OVERVOLTAGE**

Check the DC polarity and ensure the DC voltage is between 10 V and 30 V with a maximum current capacity of 1 Amp (nom 500 mA).

Incorrect polarity or excessive voltage may result in a blown fuse.

Failure to follow these instructions can result in injury or equipment damage.

Apply DC power to the radios. The “Pwr” LED should now be solid GREEN.

Wait 45 seconds for the boot up sequence to be complete. This will be indicated when the Sync/NoRx LED flashes at a rate of once a second.

Step 2 - Preliminary configuration**IP Address and Factory Default**

The default IP address of the J-Series radio is 192.168.2.15. To configure the J-Series radio you need to know the IP address of the radio. If you are uncertain of the current IP programmed into the radio you will need to reset the radio configuration to factory default.

This can be done by powering up the radio (wait 45 seconds), depress the factory default switch using a paper clip or similar thin blunt wire and keep the switch depressed for 5 seconds. All 5 LEDs will illuminate solid GREEN indicating the radio will return to factory default settings. Wait 30 seconds with the factory default reset process to occur.

Ethernet Configuration Ping Test

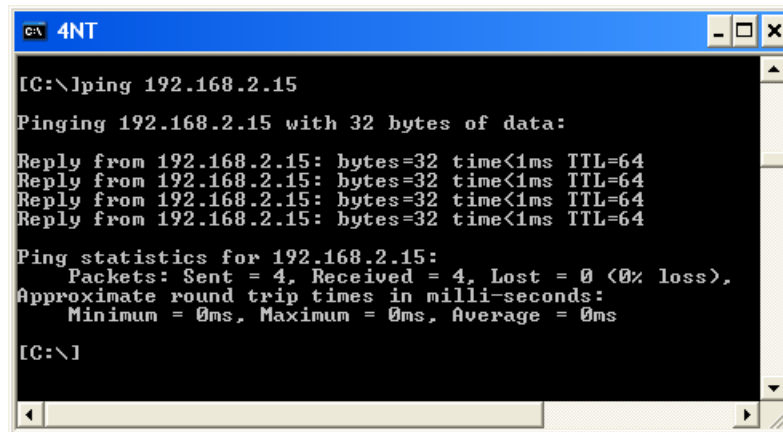
Connect your PC LAN Port to one of the Ethernet Ports (LAN1 or LAN2).

The corresponding Link/Activ LAN LED will illuminate continuously Green. If data is being transferred, the Link/ Activ LAN LED may also flash Amber.

To verify your PC can communicate with the J-Series you should first use the “ping” utility to test the connection to the Ethernet Port.

Open up a command window on your PC by going to the “Start” > Run and typing “CMD” then OK. Then type “ping 192.168.2.15” which is the default address of the radio.

If both the radio and PC have their LAN port connection and configuration correct, the radio should respond to the ping as shown below.



```
C:\ 4NT

[ C:\>ping 192.168.2.15

Pinging 192.168.2.15 with 32 bytes of data:

Reply from 192.168.2.15: bytes=32 time<1ms TTL=64
Reply from 192.168.2.15: bytes=32 time<1ms TTL=64
Reply from 192.168.2.15: bytes=32 time<1ms TTL=64
Reply from 192.168.2.15: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.2.15:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

[ C:\>
```

Step 3 - Web browser connection

Open a web browser and type in the IP address of the J-Series radio (In this case, we type “192.168.2.15”).

If successful, your browser should connect to the internal web server of the J-Series and display the home page of the configuration interface as shown below.



If the “ping” test worked in Step 3 but you are unable to connect to the internal web server of the J-Series you may have a problem with a proxy setting in your web browser. Make sure you disable any proxy settings before attempting to connect again.

Step 4 - PTP Wizard activation

The easiest way to get the a PTP J-Series Ethernet link up and running is to use the Wizards. Using the Wizards is a two part process - First the Access Point needs to be configured, and then the Remote.

Locate the “Point to Point - Access Point” button and click on the “Start The Wizard” button. The Access Point Wizard screen is now shown.

The Wizard now prompts the user to configure some critical items for point to point operation. For each configuration item, help text is provided on the HTML programmer interface. For the purposes of this demonstration, the following configuration options should be configured.

Wizards [Activate Configuration]

Point to Point - Access Point

Connection Type	Static IP	Connection Type: Select DHCP (Dynamic Host Configuration Protocol) to automatically obtain network configuration from a DHCP server on the local network. Select Static IP to manually configure network settings.
IP Address	192.168.0.191	IP Address: The network address of the radio on the local area network. The IP address that is configured here is used to access this Web-based management interface. If the IP address is changed, the PC's network settings may have to be adjusted in order to access the Web interface again. Every radio on the network must be configured with a unique IP address.
Subnet Mask	255.255.255.0	Subnet Mask: The subnet mask determines which IP addresses are local to the device, and which must be reached through a gateway or router.
Subnet ID	QuickBrownFox	Subnet ID: The Subnet ID is a text string that is used by the radio to generate a hopping pattern for the system. The Subnet ID must be identical for all radios in the network.
Remote Serial Number	400043	Remote Serial Number: Enter the serial number of the remote unit.

Ensure that the connection type is set as “Static IP”.

The IP Address for the Access Point should be left at the factory default value of 192.168.2.15

The IP Address for the Remote should be configured as 192.168.2.16

Change the Subnet ID from “default” to a descriptive name like “TestPTPLink”

The Subnet ID needs to be identical in both Access Point and Remote radios for correct operation to occur.

You can not use the factory default Subnet ID name of “default”.

Under trusted Remote serial number add the serial number of the other J-Series that will become the Remote in this point-to-point network.

After configuration of all items are complete, activate the configuration by clicking on the “Activate Configuration” button in the top right corner.

Step 5 - PTP Wizard activation (remote)

Repeat steps (3) to (6) for the Remote radio.

Step 6 - Verify modem operation

The J-Series Ethernet radio modems are now ready for operation. Allow 15 seconds for the Remote radio to synchronize with the Access Point radio.

Access Point LEDs

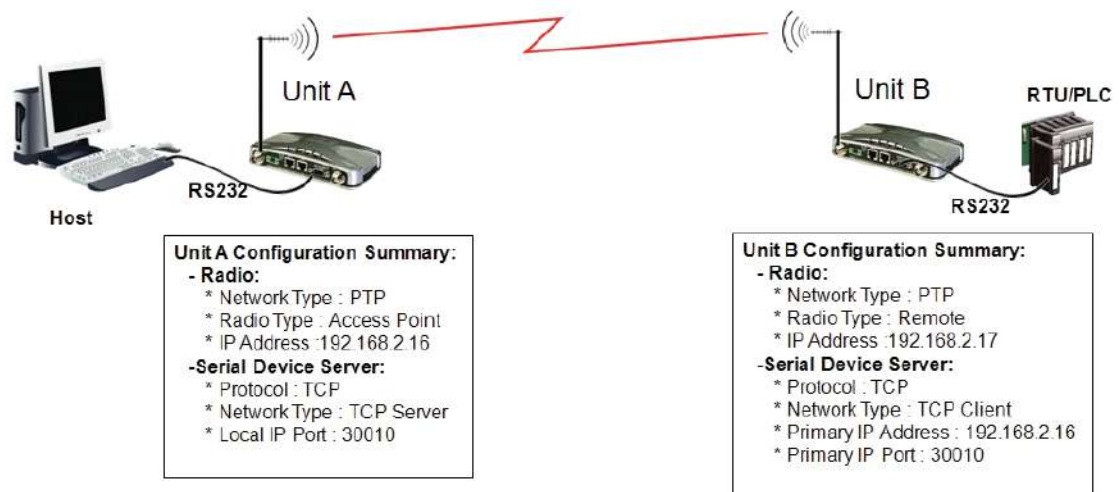
Pwr/Tx LED will be solid Green but flash Red once per second on Tx.

Remote Rx LEDs

Pwr/Tx LED will be Green and Sync/NoRX LED will flash Green once per second indicating the Remote has synchronized with the Access Point.

7.3 Point to Point - TCP Serial Device Server Setup Guide

Point-to-Point Serial Data via TCP/IP



Point to Point connectivity using the TCP/IP mode of the embedded J-Series terminal servers is useful for PTP (Point to Point) serial link requiring high reliability data delivery.

In PTP Serial via TCP/IP two unique types of J-Series configuration are required. One J-Series needs to be configured as the TCP Server. The other J-Series needs to be configured as a TCP Client. Any J-Series device (Access Point, Bridge or Remote) can function as either a TCP server or client.

More information on PTP Serial via TCP/IP can be found in [Part D – Features](#) ^[29].

The following information will guide you through the minimum steps required to configure this feature in the J-Series. Refer to the HTML programmer for more information about each item.

Ensure you have already configured the J-Series radios for PTP mode as described in the Point to Point Quick Start Guide using the IP addresses as defined in the image above. The following procedure assumes this has already been done.

Step 1 - TCP server configuration (Unit A)

Connect your browser to the J-Series configuration web page of Unit A (192.168.2.16) and select to the "Configuration" page and then select the "Serial Port A" option.

- a. Ensure the Mode is configured to be "Serial Device Server"
- b. Ensure the Character Layer matches the configuration of the external serial device you are connecting to the J-Series Serial Port. The default is 9600,8,N,1.
- c. Ensure the Packet Layer is set to "Standard"
- d. Ensure the Protocol is configured to be "TCP"
- e. Ensure the Network Type is configured to be "TCP Server"
- f. Ensure the Local IP Port is configured to be "30010"
- g. Ensure the Inactivity Timeout is set to "5" seconds.

Click on Activate Configuration.

Once the web browser has activated the new configuration and then returned to the Configuration page, the configuration of the TCP Server is now complete. The next step is to configure the TCP Client.

Step 2 - TCP client configuration (Unit B)

Connect your browser to the J-Series configuration web page of Unit B (192.168.2.17) and select to the "Configuration" page and then select the "Serial Port A" option.

Repeat the steps as shown above in "1 - TCP Server Configuration" with the exception of the following steps.

Ensure the Network Type is configured to be "TCP Client"

Ensure the Primary IP Address is configured to be the IP address of Unit A which is "192.168.2.16"

Ensure the Primary IP Port is configured to be "30010" Ensure the Secondary IP Address & Port is blank.

Click on Activate Configuration.

Once the web browser has activated the new configuration and then returned to the Configuration page, the configuration of the TCP Client is now complete.

Step 3 - RS-232 final testing

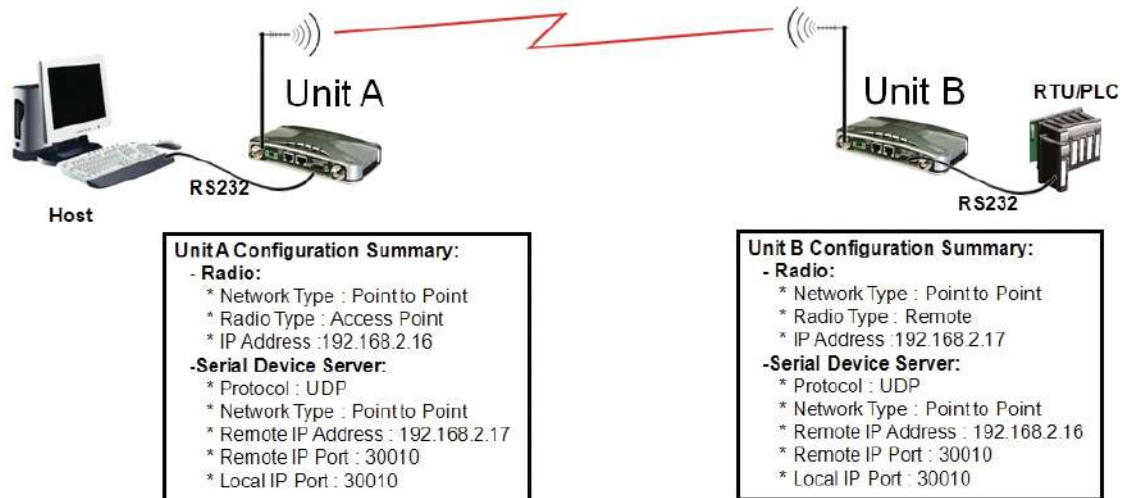
The Point to Point via TCP Serial connectivity is now complete.

The RS-232 link can be tested using an RS-232 Serial Packet Test Program such as LinkTest or by connecting your RS-232 application.

The Port A/B LED status can also be used to diagnose the PTP via TCP Serial Link. A flashing RED LED means that RS-232 data is being sent into the radio for transmission. A flashing GREEN LED means that RS-232 data is being received from the link and presented to the port.

7.4 Point to Point - UDP (Unicast) Serial Device Server Setup Guide

Point-to-Point Serial Data via UDP/IP (Unicast)



Point to Point (PTP) connectivity using the UDP mode of the embedded J-Series terminal servers is useful for PTP serial links requiring low latency and high throughput.

Unlike the TCP mode of operation, there are no Client or Server modes. Both ends of a PTP Serial via UDP are

configured in a similar way (with the exception of destination IP address and port numbers).

More information on PTP Serial via UDP/IP(Unicast) can be found in Part D of this user manual.

The following information will guide you through the minimum steps required to configure this feature in the J-Series. Refer to the HTML programmer for more information about each item.

Ensure you have already configured the J-Series radios for PTP mode as described in the Point to Point Quick Start Guide using the IP addresses as defined in the image above. The following procedure assumes this has already been done.

Step 1 - UDP configuration (Unit A)

Connect your browser to the configuration web page for Unit A using the IP address of Unit A and navigate to the

“Configuration” page and then select the “Serial Port A” option.

a. Ensure the Mode is configured to be “Serial Device Server”

- b. Ensure the Character Layer matches the configuration of the external serial device you are connecting to the J-Series Serial Port. The default is 9600,8,N,1.
- c. Ensure the Packet Layer is set to "Standard"
- d. Ensure the Protocol is configured to be "UDP"
- e. Ensure the Network Type is configured to be "Point to Point"
- f. Ensure the Remote IP Address is configured to be the IP address of Unit B. (in the above example this would be 192.168.2.17)
- g. Ensure the Remote IP Port is configured to be 30010
- h. Ensure the Local IP Port is configured to be 30010

Click on Activate Configuration.

Once the web browser has activated the new configuration and then returned to the configuration page, the configuration of Unit A is now complete. The next step is to configure Unit B.

Step 2 - UDP configuration (Unit B)

Repeat the steps as shown above in "1 - UDP Configuration (Unit A)" with the exception of step (e).

Ensure the Remote IP Address is configured to be the IP address of Unit A. (in the above example this would be 192.168.2.16)

Click on Activate Configuration.

Once the web browser has activated the new configuration and then returned to the configuration page, the configuration of Unit B is now complete.

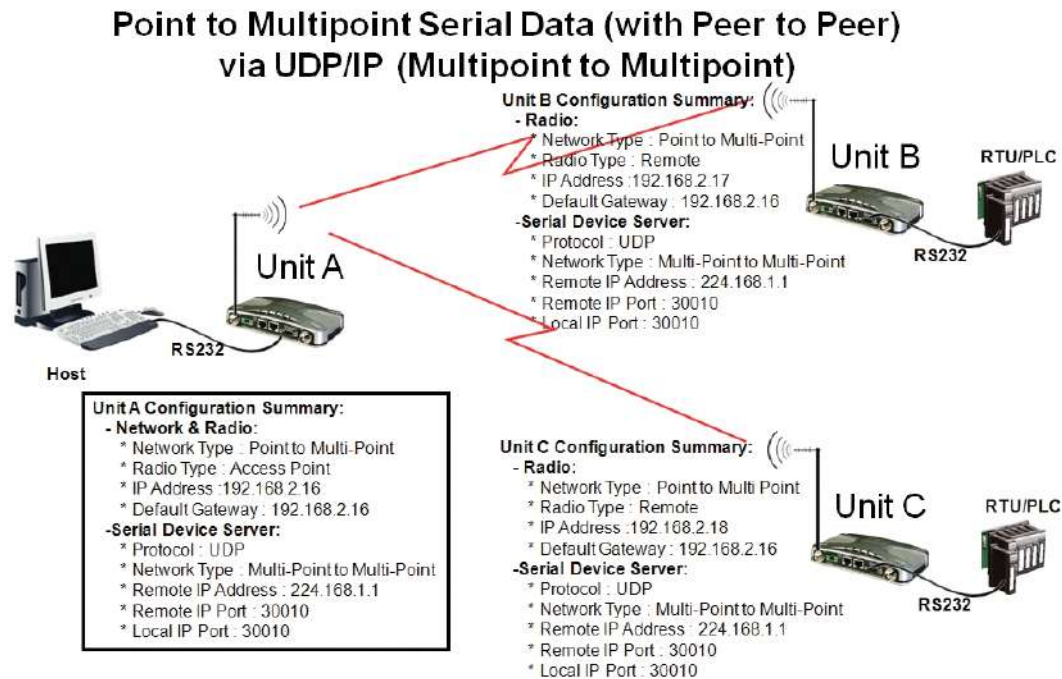
Step 3 - RS-232 final testing

The Point to Point via UDP Serial connectivity is now complete.

The RS-232 link can be tested using an RS-232 Serial Packet Test Program such as LinkTest or by connecting your RS-232 application.

The Port A/B LED status can also be used to diagnose the PTP via TCP Serial Link. A flashing RED LED means that RS-232 data is being sent into the radio for transmission. A flashing GREEN LED means that RS-232 data is being received from the link and presented to the port.

7.5 Point to Multipoint - UDP (Multicast) Serial Device Server Setup Guide



Point to Multipoint (PTMP) connectivity using the UDP mode of the embedded J-Series terminal servers is useful for PTMP serial links requiring low latency and high throughput.

In PTMP via UDP there are no Client or Server modes. All units in a PTMP Serial via UDP are configured in a similar way (with the exception of destination IP address and port numbers).

More information on PTMP Serial via UDP (multicast) can be found in Part D of this user manual.

The following information will guide you through the minimum steps required to configure this feature in the J-Series. Refer to the HTML programmer for more information about each item.

Ensure you have already configured the J-Series radios for PTMP mode as described in this manual (Alternatively you can use the PTMP wizards). Ensure you have configured the units with the IP addresses as specified in the diagram above.

Ensure the Default Gateway in the Network Parameters configuration of the Access Point is configured as shown.

Step 1 - UDP point configuration (Unit A)

Connect your browser to the J-Series configuration web page of Unit A (192.168.2.16) and select to the "Configuration" page and then select the "Serial Port A" option.

- Ensure the Mode is configured to be "Serial Device Server"
- Ensure the Character Layer matches the configuration of the external serial device you are connecting to the J-Series Serial Port. The default is 9600,8,N,1.

- c. Ensure the Packet Layer is set to "Standard"
- d. Ensure the Protocol is configured to be "UDP"
- e. Ensure the Network Type is configured to be "Point to Multipoint"
- f. Ensure the Node Type is configured to be "Point"
- g. Ensure the Remote IP Address is an address from the designated multicast range of IP Addresses, in this example we are using 224.168.1.1 (this is the multicast address as configured in the multipoint units B & C).
- h. Ensure the Remote IP Port is configured to be 30010
- i. Ensure the Local IP Port is configured to be 30010
- j. Ensure the Time to Live is configured as "Restrict to same Subnet"

Click on Activate Configuration.

Once the web browser has activated the new configuration and then returned to the configuration page, the configuration of Unit A is now complete. The next step is to configure the multipoint Units B & C.

Step 2 - UDP Multipoint Configuration (Units B and C)

Repeat the steps as shown above in "1 - UDP Point Configuration (Unit A)" with the exception of steps (e) & (f) and a new step for the Local IP Address.

- a. Ensure the Node Type is configured to be "Multipoint"
- b. Ensure the Remote IP Address is configured to be the IP address of Unit A. (in the above example this would be 192.168.2.16)
- c. Ensure the Local IP Address is an address from the designated multicast range of IP Addresses, in this example we are using 224.168.1.1 (this is the multicast address as configured in the multipoint units B & C).

Click on Activate Configuration.

Once the web browser has activated the new configuration and then returned to the Configuration page, the configuration of Unit B is now complete and the process can be repeated for Unit C (which is identical to Unit B)

Step 3 - RS-232 final testing

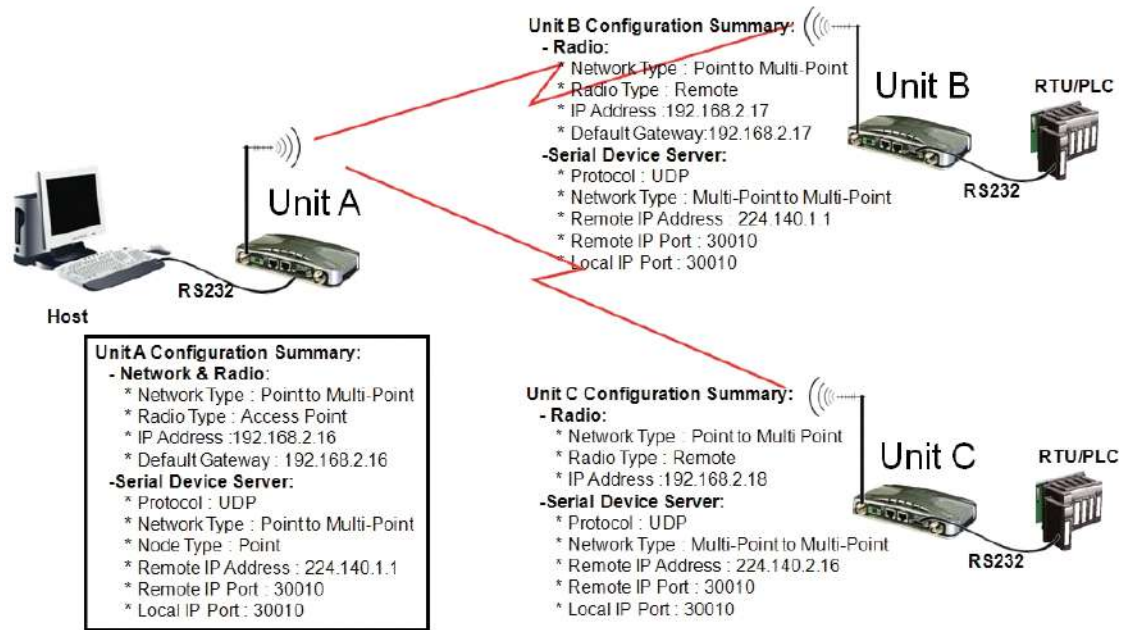
The Point to Multipoint via UDP Serial connectivity is now complete.

The RS-232 link can be tested using an RS-232 Serial Packet Test Program such as LinkTest or by connecting your RS-232 application.

The Port A/B LED status can also be used to diagnose the PTP via TCP Serial Link. A flashing RED LED means that RS-232 data is being sent into the radio for transmission. A flashing GREEN LED means that RS-232 data is being received from the link and presented to the port.

7.6 Point to Multipoint with Peer to Peer - UDP (Multicast to Multicast) Serial Device Server Setup Guide

Peer-to-Peer Serial Data via UDP/IP (Multicast to Multicast)



Point to Multipoint (PTMP) with Peer to Peer connectivity using the UDP mode of the embedded J-Series terminal servers is useful for PTMP serial links requiring peer to peer connectivity.

More information on PTMP Serial with Peer to Peer via UDP (Multicast to Multicast) can be found in Part D of this user manual.

The following information will guide you through the minimum steps required to configure this feature in the J-Series. Refer to the HTML programmer for more information about each item.

Ensure you have already configured the J-Series radios for PTMP mode as described in this manual (Alternatively you can use the PTMP wizards). Ensure you have configured the units with the IP addresses as specified in the diagram above.

Ensure the Default Gateway in the Network Parameters configuration of all radios is configured as shown.

Step 1 - Configuration (Unit A)

Connect your browser to the J-Series configuration web page of Unit A (192.168.2.16) and select to the "Configuration" page and then select the "Serial Port A" option.

- Ensure the Mode is configured to be "Serial Device Server"
- Ensure the Character Layer matches the configuration of the external serial device you are connecting to the J-Series Serial Port. The default is 9600,8,N,1.

- c. Ensure the Packet Layer is set to "Standard"
- d. Ensure the Protocol is configured to be "UDP"
- e. Ensure the Network Type is configured to be "Multipoint to Multipoint"
- f. Ensure the Local IP Address is an address from the designated multicast range of IP Addresses, in this example we are using 224.140.1.1 (this is the multicast address as configured in the multipoint units B & C. In this mode, all the multicast IP addresses are the same).
- g. Ensure the Local IP Port is configured to be 30010
- h. Ensure the Remote IP Address is an address from the designated multicast range of IP Addresses, in this example we are using 224.140.1.1 (this is the multicast address as configured in the multipoint units B & C. In this mode, all the multicast IP addresses are the same).
- i. Ensure the Remote IP Port is configured to be 30010
- j. Ensure the Time to Live is configured as "Restrict to same Subnet"

Click on Activate Configuration.

Once the web browser has activated the new configuration and then returned to the Configuration page, the configuration of Unit A is now complete. The next step is to configure the Multipoint Units B & C.

Step 2 - Configuration (Units B and C)

Repeat the steps as shown above in "1 - Configuration (Unit A)" with the exception of default Gateway Address as found in the "Configuration > Network Parameters"

The Default Gateway IP address should be the IP address of your Gateway in the network. In this example, the Access Point IP address is defined as the Gateway (192.168.2.16).

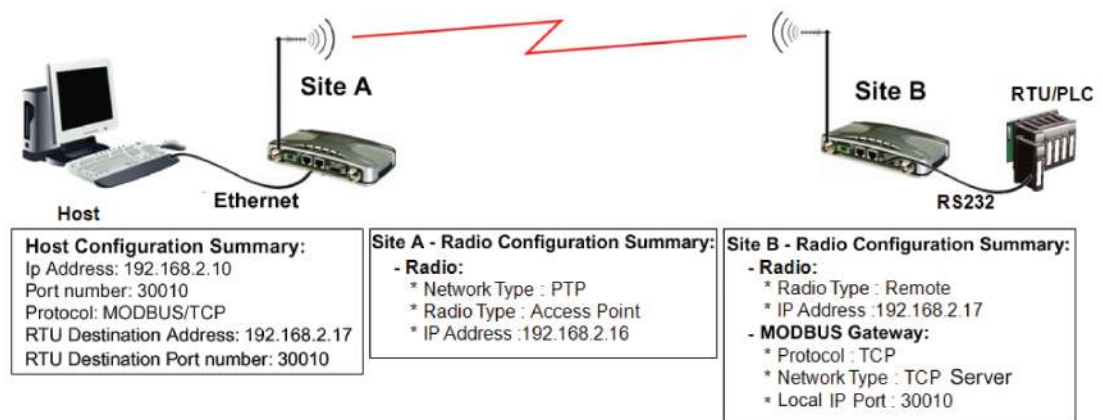
Step 3 - RS-232 final testing

The Point to Multipoint via UDP Serial connectivity is now complete.

The RS-232 link can be tested using an RS-232 Serial Packet Test Program such as LinkTest or by connecting your RS-232 application.

The Port A/B LED status can also be used to diagnose the PTP via TCP Serial Link. A flashing RED LED means that RS-232 data is being sent into the radio for transmission. A flashing GREEN LED means that RS-232 data is being received from the link and presented to the port.

7.7 Point to Point - Modbus/TCP to Modbus RTU Setup Guide



Point to Point (PTP) with Modbus TCP to Modbus RTU can be performed by using the Modbus gateway feature embedded within the J-Series.

The following information will guide you through the minimum steps required to configure the Modbus gateway feature in the J-Series. Refer to the HTML programmer for more information about each configuration item.

Ensure you have already configured the J-Series radios for PTP mode as described in this manual (Alternatively you can use the PTP wizards). Ensure you have configured the units with the IP addresses as specified in the diagram above.

Step 1 - Radio configuration (Site A)

In this scenario, the entry point radio (Unit A) is essentially transparent between the Host application and the Remote Radio (Unit B) in terms of Modbus TCP

data addressed to the RTU/PLC. This means there are no configuration requirements for Unit A other than setting up the unit to operate in PTP mode with Unit B (For instruction on how to set up a PTP link, follow the PTP link wizard located within the web user interface).

Step 2 - Radio configuration (Site B)

To use the Modbus gateway feature in a PTP scenario, Connect your browser to the J-Series configuration web page of Unit B (192.168.2.17) and select to the "Setup" page and then select the "Serial Port A" option.

- Ensure the Mode is configured to be "Modbus TCP Gateway"
- Ensure the Character Layer matches the configuration of the external serial device you are connecting to the J-Series Serial Port. The default is 9600,8,N,1.
- Ensure the Packet Layer is set to "Modbus"
- Ensure the Protocol is configured to be "TCP"
- Ensure the Protocol Mode is configured to be "TCP Server"

f. Ensure the Local IP Port is configured to be 30010

Click on Activate Configuration.

Once the web browser has activated the new configuration and then returned to the Configuration page, the configuration of Unit B is now complete.

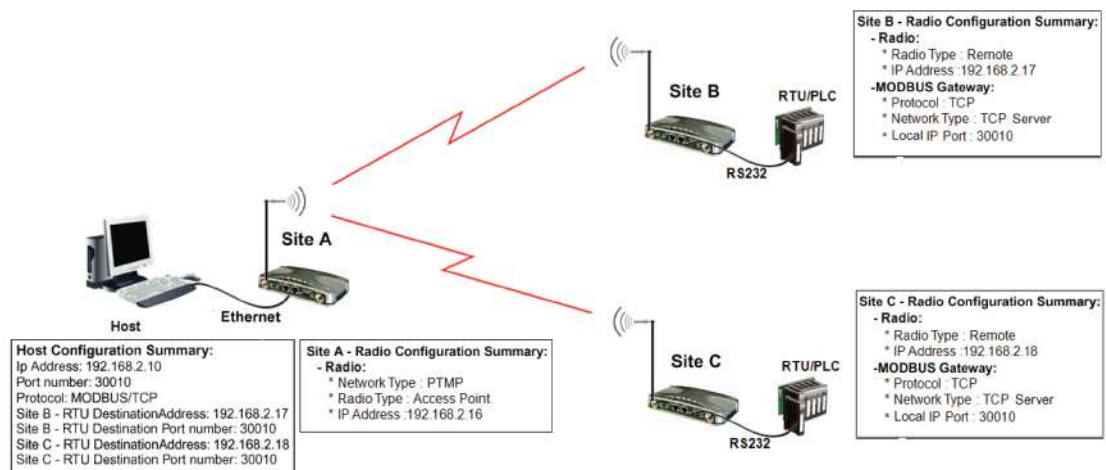
Step 3 - Final testing

The Point to Point Modbus TCP to Modbus RTU is now complete.

Final testing can now be performed by polling the RTU at the Remote end. The RTU should now successfully respond to polls from the host application.

The Port A/B LED status can also be used to diagnose the PTP via TCP Serial Link. A flashing RED LED means that RS-232 data is being sent into the radio for transmission. A flashing GREEN LED means that RS-232 data is being received from the link and presented to the port.

7.8 Point to Multipoint - Modbus/TCP to Modbus RTU Setup Guide



Point to Multipoint (PTMP) with Modbus TCP to Modbus RTU can be performed by using the Modbus gateway feature embedded within the J-Series at each remote site.

The following information will guide you through the minimum steps required to configure the Modbus gateway feature in the J-Series radios. Refer to the HTML programmer for more information about each configuration item.

Ensure you have already configured the J-Series radios for PTMP mode as described in this manual (Alternatively you can use the PTMP wizards). Ensure you have configured the units with the IP addresses as specified in the diagram above.

Step 1 - Radio configuration (Site A)

In this scenario, the entry point radio (Unit A) is essentially transparent between the Host application and the Remote Radios (Units B & C) in terms of Modbus TCP data addressed to the RTUs/PLCs. This means there are no configuration requirements for Unit A other than

setting up the unit to operate in PTMP mode with Units B & C (For instruction on how to set up a PTMP link, follow the PTMP link wizard located within the web user interface).

Step 2 - Radio configuration (Sites B and C)

To use the Modbus gateway feature in a PTMP scenario, Connect your browser to the J-Series configuration web page of the Site B Radio (192.168.2.17) and select to the "Setup" page and then select the "Serial Port A" option.

- a. Ensure the Mode is configured to be "Modbus TCP Gateway"
- b. Ensure the Character Layer matches the configuration of the external serial device you are connecting to the
- c. J-Series Serial Port. The default is 9600,8,N,1.
- d. Ensure the Packet Layer is set to "Modbus"
- e. Ensure the Protocol is configured to be "TCP"
- f. Ensure the Protocol Mode is configured to be "TCP Server"
- g. Ensure the Local IP Port is configured to be 30010 Click on Activate Configuration.

Once the web browser has activated the new configuration and then returned to the Configuration page, the configuration of Unit B is now complete.

For configuration of Unit C, follow steps (a) through to (f) for Unit C.

Step 3 - Final testing

The Point to Multipoint Modbus TCP to Modbus RTU is now complete.

Final testing can now be performed by polling the RTUs at the Remote sites. The RTUs should now successfully respond to polls from the host application.

The Port A/B LED status can also be used to diagnose the PTMP via TCP Serial Link. A flashing RED LED means that RS-232 data is being sent into the radio for transmission. A flashing GREEN LED means that RS-232 data is being received from the link and presented to the port.

8 Part H - Installation & Commissioning

All Ethernet radio modems need to be properly installed and commissioned to function reliably. It is important that installers are familiar with RF products / installations and are equipped with appropriate tools necessary to help ensure the ongoing reliability of a communications system.

This informed is provided as a short form guide to assist with the correct installation and commissioning of the J-Series Ethernet and that important tests are made and recorded at each site for future reference should a problem eventuate.

Installers should check that each J-Series Ethernet radio has been programmed to suit their specific requirements before installation.

Installations play a critical role in network performance. It is essential that the installation be performed in a professional manner with careful attention and consideration to the following items:

- Adequate primary power cable - relative to the length of cable to minimize voltage drop
- Shielded CAT-5 or CAT-6 Ethernet patch cable between the J-Series radio and any external Ethernet equipment
- Shielded RS-232 data cable between the J-Series radio and any external RS-232 equipment
- Low loss coax used for antenna feed line
- Careful termination of RF connectors
- A suitable antenna for the requirement
- Suitable placement of the antenna
- Adequate signal strength from the Access Point or Bridge radio

See:

- [Typical Installation Overview](#) ¹²⁵
- [Antenna Installation](#) ¹²⁶
- [LED Indicators](#) ¹²⁸
- [Optimizing the Antenna for Rx Signal](#) ¹²⁸
- [Commissioning](#) ¹³⁰

8.1 Typical Installation Overview

The following information should assist when installing and commissioning a J-Series Ethernet system.

Data connection

In industrial environments connection to any external device should be by shielded CAT-5 or CAT-6 patch cable. A cables should be routed with strain relief essential.

Mounting

The radio modem should be mounted in a cool, dry, and vibration free environment. Mounting of the unit should be in a location providing easy access to mounting screws and all connections.

Power connections

The power required is:

Tx: Nominal 13.8 Vdc @ 800 mA (Max 1A) Rx: Nominal 13.8 Vdc @ 150 mA

Rated Operating Voltage 10...30 Vdc

The J-Series Radio is supplied with the a mating DC power connector:

Phoenix Contact Part Number 1777989. The DC Power connector should be installed with the locking screws done up tightly. Cable needs to be #22 AWG or larger, 70 °C min. temperature rating. CSA maximum current rating: 2.5 A.

The J-Series Ethernet radio modem will operate from a 10 to 30 volt (filtered) DC supply. The radio is designed to self protect from permanent damage if the voltage exceeds 30 Vdc or if reverse polarity is applied. The replaceable internal fuse has a rating 3 Amp.

The radio modem can be damaged if there is any potential difference between the chassis-ground, RS-232 signal ground, power (-) input, or antenna coaxial shield.

Before connecting any wiring, ensure all components are earthed to a common ground point (pay particular attention to 24 V PLC power systems where DC-DC converters are used).

Connect the antenna, Ethernet and RS-232 plugs BEFORE applying power to the unit. Lastly, before inserting the power plug, re-check that the polarity and voltage on the DC power plug is correct using a multimeter.

Coax cable connection

It is important to select the correct cable and connectors for each application as a poor selection can seriously degrade the performance of the system.

As an example, for each 3 dB of cable and connector loss, half the transmitter power is lost and twice the receiver signal power is required to produce the same bit error rate.

In some installations where strong signals are present, a compromise of cable and connector cost may be acceptable.

It is essential that all connector termination's are performed as per the manufacturers specifications (especially at 900MHz and above) and if connectors are to be used outside, it is essential that a sealant such as amalgamating tape be used to seal connectors. DO NOT use acetic cure silicon to seal the connectors.

It is also important that coax cables are not stressed by tight bends, kinking or excessive flexing. Ensure that coax cables have sufficient strain relief and are secure. If large diameter rigid or semi rigid cable is used, it is recommended to use a short length of high quality RG223 cable between the unit and main cable feed.

8.2 Antenna Installation

The selection of antennas and their placement is one of the most important factors when installing a radio based network.

Antennas are generally mounted to a vertical pole with either vertical or horizontal polarization as per the license requirement.

Antennas should be mounted as high as practical and away from metal surfaces which can cause reflections.

Determining the type of antenna is very important and as a typical generic example, Point to Multipoint (PTMP) systems generally employ high gain (3, 6, or 9 dB gain) omni directional

antennas at the Access Point sites and either omni directional whips (unity gain) or preferably high gain directional yagi antennas (9 or 14 dB gain) at the remote sites.

Yagi antennas

Yagi antennas not only provide signal gain and directivity, but also provides protection from interfering signals which are outside the beam width of the antenna. Yagi antennas are essential when communicating over very long distances.

Yagi antennas are polarized and need to be mounted either vertically (elements pointing from the ground to the sky) or horizontally (elements in parallel with the horizon).

When mounting yagi antennas with vertical polarization, it should be noted that some antennas have a drain hole in the dipole (loop section of antenna). The small drain hole on one end of the dipole needs to be pointed towards the ground so that water will drain out of the antenna.

Omni directional antennas

Omni directional antennas provide a radiation pattern of equal strength through 360° in the horizontal plane.

This makes them ideal for Access Point antennas in point to multipoint systems because they can reach a large populous of remote sites.

Omni directional antennas are also used at remote sites (although yagi antennas are preferred) and are typically ground independent whip type antennas. The main reason for using whips at remote sites is for aesthetics as they are far less obtrusive than a yagi.

Regardless of the type, antennas need to be mounted properly and in a suitable location as covered below.

Antenna placement

Antenna placement is of paramount importance and plays a big part of the antennas and in turn systems performance.

When choosing antenna locations the aim is to find the largest path of unobstructed space and locate the antennas within that space. It is important to locate antennas as high as possible and definitely clear of any moving obstructions.

Where possible it is important to avoid mounting antennas:

- Against or adjacent to steel structures.
- In an area which will have constant intermittent obstructions - people walking past, vehicles driving past etc. That is, mount antennas well above such moving obstructions.
- Near any electrical equipment.
- Near metal beams, structures etc.
- Inside any metal enclosures, tin sheds / warehouses etc. - Note meshed wire fences act like a "brick wall" to RF transmissions.
- Away from guard rails or support beams.

- Above any pipe work or corrugated iron roofs.

Note: Sometimes installations in such environments are unavoidable and where this is the case, certain care can be taken to still ensure a reliable installation.

If tests indicate poor signal strength then the antennas at one or both ends of the link should be raised, and/ or moved clear of obstructing objects, or if directional antennas are employed they should be checked for correct directional orientation and polarization (horizontal or vertical signal orientation).

8.3 LED Indicators

LED indicators are documented in Part F - Quick Reference Guide of this User Manual. However, during the installation process it is important to check that the LED indicators are operating correctly.

DC power

If all the LEDs are off, no DC power is reaching the radio modem or the fuse is open. Successful power-up is indicated by the “Pwr/Tx” LED showing a continuous GREEN state for REMOTES or an alternating Red/Green for Access Points.

When the transmitter is active the “Pwr/Tx” LED turns RED.

Sync/No RX LED indicator

The “Sync/NoRx” LED is used to indicate the state of the receiver.

A regular flashing GREEN LED shows that the modem is synchronized to its Access Point. The GREEN LED also flashes when the modem is receiving data.

A regular flashing RED indicates the REMOTE not synchronized to an Access Point or BRIDGE. Check the antenna, RF signal levels and ensure the Subnet names are correct.

LAN LED indicator

The Green Link and Amber Activity LEDs indicate Ethernet status on the two LAN ports. These LEDs will show solid Green when an Ethernet Link is established and will flash Amber to indicate Ethernet data transmission is occurring.

8.4 Optimizing the Antenna for Rx Signal

When using a directional antenna, it will be necessary to align the antenna for the best received signal. This can be done using TVIEW+ Diagnostics (measured RSSI) or by measuring the RSSI output on Pin 9 of the serial data port.

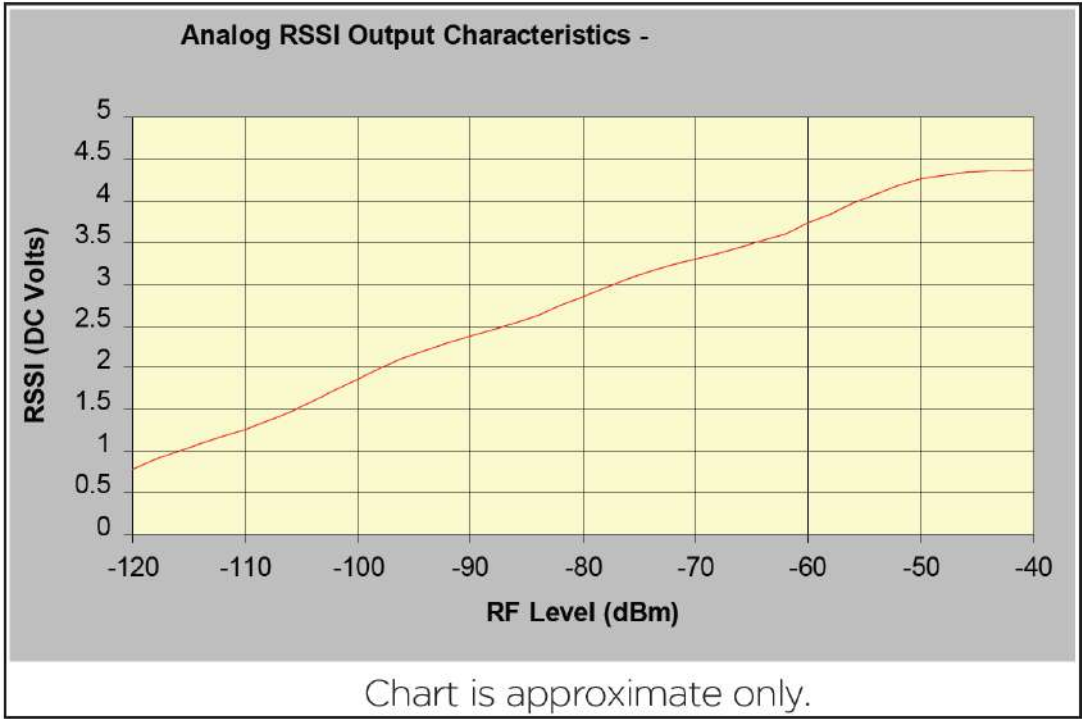
This can be done by using the (0...5 Vdc) output on Pin 9 of the Data Port to indicate signal strength (RSSI). This voltage can be converted to dBm using the chart below.

The RSSI output is a latched value of the received signal which is updated every 100 mS but will peak-hold for about 4 seconds if the Remote has lost synchronization with the Access Point.

Access Point: RSSI voltage is only present if it is receiving valid data from down stream.

Bridge: Only looks at the upstream received signal. If you need to measure downstream RSSI you would need to temporarily convert it to an access point talking to the remote with the remote sending data back.

Remotes: RSSI voltage is only present if unit is in sync with the Access Point or Bridge.





8.5 Commissioning

When commissioning an Ethernet radio network, it is important to ensure that the incoming received signal strength (RSSI) is adequate to provide reliable communications.

For a system to operate reliably, an “adequate” signal level needs to be present which allows for fading and interference.

An adequate level is typically 25 to 30 dB above the minimum threshold of the receiving device.

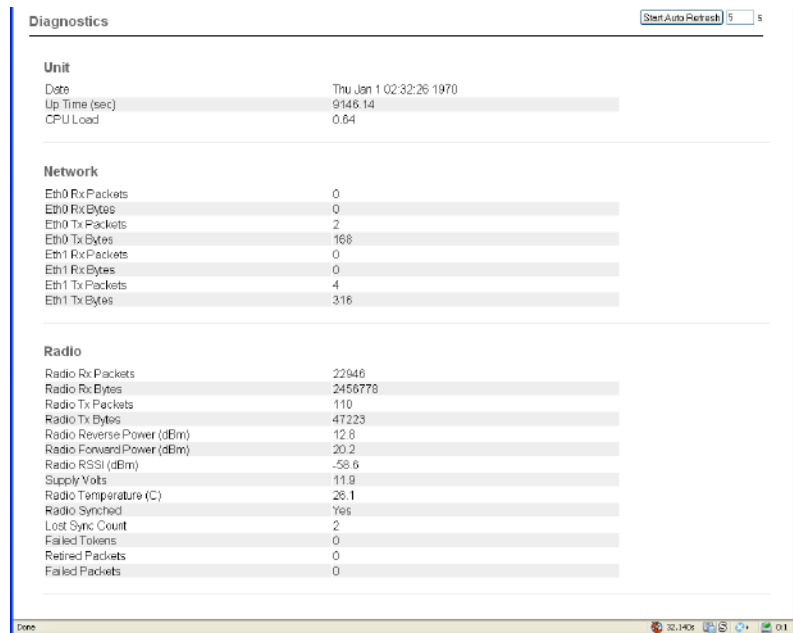
Should this level not be achieved, then either;

1. Find a more suitable location to mount the antenna.
2. Mount the antenna higher in a more prominent location to achieve as close as possible to clear line of site.
3. Use an alternate Access Point site to achieve communications or as a last resort.
4. Lower the RF Data Speed to 256 k to increase the sensitivity of the radio.
5. Increase the Data Re-transmissions and No Ack Re-Try limit to improve the reliability of the Ethernet radio link.

8.5.1 HTML Diagnostics

After the J-Series radios have been configured and installed, the next most important step in the commissioning process is to review the HTML diagnostics which is available in every radio. The diagnostics that is available is shown in the image below and is as follows:

After the J-Series radios have been configured and installed, the next most important step in the commissioning process is to review the HTML diagnostics which are available in every radio. The available diagnostics are shown in the image below:



Diagnostics	
Start Auto Refresh 5 s	
Unit	
Date	Thu Jan 1 02:32:26 1970
Up Time (sec)	9146.14
CPU Load	0.64
Network	
Eth0 Rx Packets	0
Eth0 Rx Bytes	0
Eth0 Tx Packets	2
Eth0 Tx Bytes	168
Eth1 Rx Packets	0
Eth1 Rx Bytes	0
Eth1 Tx Packets	4
Eth1 Tx Bytes	316
Radio	
Radio Rx Packets	22946
Radio Rx Bytes	2456778
Radio Tx Packets	110
Radio Tx Bytes	47223
Radio Reverse Power (dBm)	12.8
Radio Forward Power (dBm)	20.2
Radio RSSI (dBm)	-58.6
Supply Volts	11.9
Radio Temperature (C)	26.1
Radio Synched	Yes
Lost Sync Count	2
Failed Tokens	0
Retired Packets	0
Failed Packets	0

Unit Specific

- **Date:** Specifies the current date and time. For the date and time to be correct the radio needs to be configured to synchronize with a NTP Time Server.
- **CPU Load:** Specifies the amount of CPU load the Linux based kernel is experiencing.

Network Specific

- **LAN 1 Rx Packets:** The number of Ethernet packets received on LAN1.
- **LAN 1 Rx Bytes:** The number of bytes received on LAN1.
- **LAN 1 Tx Packets:** The number of Ethernet packets transmitted on LAN1.
- **LAN 1 Tx Bytes:** The number of Ethernet packets received on LAN1.
(the same applies for LAN2)

Radio Specific

- **Radio Rx Packets:** The number of packets received by the radio.
- **Radio Rx Bytes:** The number of bytes received by the radio.

- **Radio Tx Packets:** The number of packets transmitted by the radio.
- **Radio Tx Bytes:** The number of bytes transmitted by the radio.
- **Radio Reverse Power (dBm):** TX Reverse power measured in dBm.
- **Radio Forward Power (dBm):** TX Forward power measured in dBm.
- **Radio RSSI (dBm):** The RSSI (Received Signal Strength Indicator) measured in dBm.
- **Supply Volts:** The DC supply voltage measured in dBm.
- **Radio Temperature (C):** The internal radio temperature measured in degrees Celsius.
- **Radio Synched:** Displays the status of the radio modem being in synchronization with an Access Point (Yes or No)
- **Lost Sync Count:** The number of times a radio has lost synchronization with an Access Point.
- **Failed Tokens:** The number of failed token attempts (see [Digital Collision Avoidance](#)^[35])
- **Retired Packets:** The number of packets that were sent but for which an acknowledgment from the Access Point was never received.
- **Failed Packets:** The number of incoming packets that have failed CRC check and have been discarded.

8.5.1.1 Access Point

Start your web browser and insert the IP address of the J-Series Access Point into the URL. Once loaded, click on the Diagnostics option. This will display the Diagnostics summary page. Review the diagnostics parameters checking for abnormal items such as high VSWR (high TX reverse power) and lower than expected radio RSSI (Received Signal Strength).

8.5.1.2 Review Remote Radio

Click on the sub-menu "Browse Network". The remote radio will appear in the list (serial number and unit type is listed). Click on the Serial Number of the Remote Radio. The browser will now re-direct to the Remote radio.

Click on the "Summary" TAB and the remote radios diagnostics can now be reviewed.

The screenshot shows a web browser window with the title "Indicative Packet Error Test". The page content includes a description: "This test will determine the ability of the system to pass data". Below this are three buttons: "Start Packet Test", "Cancel Packet Test", and "Commissioning Record". The "Test Setup" section contains several input fields: "Destination Serial Number" (empty), "Packet Length" (160), "Number of Packets" (100), "Time Out (ms)" (5000), "Time Between Packets (ms)" (0), and "Page Refresh Rate (s)" (5). The "Test Results" section has five labels with corresponding empty input fields: "Tx Packets", "Rx Packets", "Lost Packets", "Percentage Error", and "Normalised BER". The browser's status bar at the bottom shows "Done" and the address "0.7902".

8.5.1.3 Packet Error Testing

This tool provides a useful way to test a radio communications link by transmitting data packets between two units in a loop-backed mode.

To start the test, direct the browser to Access Point by typing the IP address of this unit into your URL. Select the "Diagnostics" menu and click on the "Packet Error Testing" sub-menu.

Enter the "Destination Serial Number" of the Remote radio and ensure the "Number of Packets" is set to 1000.

Click on the "Start Packet Test" button. The radio will indicate the packet test has started and is currently running.

When the test is complete, a note stating "Packet error test completed" will be shown and the test results summarized in the "Test Results" section.

The test results show TX & RX Packets, Lost Packets and the Packet Error Rate.

8.5.1.4 Commissioning Record

After an Indicative Packet Error test has been performed, a Commissioning Record can be prepared. This facility is activated by clicking on the "Commissioning Record" button.

Commissioning Record
Tuesday, 5 August 2008
12:03:41 Local Time

Identity Unit Name: Access Point Location: Mt Burch Serial Number: 400038		Firmware Information Rev: R2.0.0 build 1 rev 621 MCU Rev: R1.3.6 build 6044 FPGA Rev: R1.3.1 build 322	
Last Poll Results Supply Volts: 12.0 Temperature: 26.1 Rx Signal: -59.7 Tx Forward Power: 20.1 Tx Reverse Power: 7.3 Tue Aug 5 12:03:41 2008		Packet Error Test Results Tx Packets: 1000 Rx Packets: 1000 Lost Packets: 0 Percentage Error: 0.0 Normalised BER: less than 10 ⁻⁶ Tue Aug 5 12:01:30 2008	
Comment Access Point communicating with remote radio.			
Finished			

It is recommended that the radio is configured to obtain the current date / time from an NTP server, otherwise the date / time shown may not be correct.

The user can enter an appropriate Unit Name and Location for reference purposes. Additionally, a comment may be added noting the type of antenna in use. Once this information has been added, the web page can be printed (using the print facility in your web browser). It may be useful to print the commissioning record to PDF for future reference.

This now completes the requirements for setting up a Point to Point J-Series Link. The radios are now ready for application testing. The application can be connected to either LAN1 or LAN2 or both (as required). For more information on testing, consult the J-Series User Manual.

9 Part I - Firmware Updating and Maintenance

See:

- [Firmware Update Overview \(R2.x.x or later\) Introduction](#) ¹³⁴
- [Replacing the Internal Fuse](#) ¹³⁸

9.1 Firmware Update Overview (R2.x.x or later) Introduction

Note: These instructions apply only to J-Series running firmware packs R2.x.x or later.

From time to time there will be enhancements and improvements made in the firmware of the J-Series. It is recommended that you keep your J-Series radio up to date with the latest firmware releases.

Using a standard web browser you can connect to the J-Series and inspect the current firmware version which is located in the Unit Information section of the web page.

Check the release notes on the web site <https://www.se.com/ww/en/product-range/61420-trio-licensefree-radios/#software-and-firmware> for newer firmware that may be beneficial to your system.

Download the firmware from the website and store it on your PC or in a location on your computer network which can be accessed during the firmware update process.

The firmware hash is included in the release notes from release 3.8.2 and later. It is recommended to compare this hash against the hash generated from the downloaded firmware to verify its authenticity. The hash is generated using SHA256 algorithm and can be obtained using third party tools such as 7-Zip, or internally within Windows 10's PowerShell.

To generate the hash from Windows 10's PowerShell

1. Navigate to the Start button, enter **Windows PowerShell** and click on **Windows PowerShell**.
2. Generate the SHA256 hash for the downloaded file.

E.g. `Get-FileHash "C:\temp\JSeriesFirmware-3.8.2-4085.tpk"`

To generate the hash using 7-Zip

1. Install 7-Zip
2. Right click the downloaded file, and select 7-Zip > CRC SHA > SHA-256.

NOTICE

HAZARD OF EQUIPMENT DAMAGE

If the generated hash does not match the supplied hash in the release notes, do not install the downloaded firmware. Installing the mismatched firmware may compromise the radio's security and operational integrity.

Failure to follow these instructions can result in equipment damage.

Firmware updates can be performed on a unit connected locally to the PC or remotely via an operational radio link. For a local upgrade, it is recommended that all other cabling to the unit be disconnected prior to commencing the firmware update to minimize any interruption to the process or disturbances of signals on cables still connected.

For a remote upgrade, ensure that the radio link is operating correctly and that other traffic using the link is minimized.

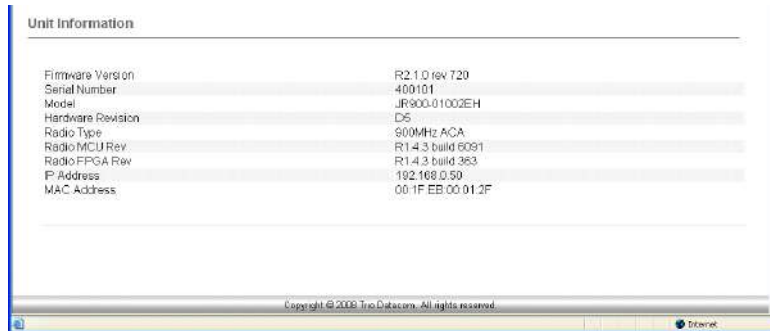
The firmware update process is a two part process. First, the firmware is transferred from the PC to the J-Series via the HTML browser. This is called "uploading" the firmware. This typically takes 30 to 40 seconds.

The second process involves the radio writing the new firmware into non-volatile memory and re-booting. This typically takes between 1 and 12 minutes, depending on how much firmware needs to be updated.

9.1.1 Firmware Update Procedure

Ensure that an Ethernet patch cable is connected from your LAN port to either LAN1 or LAN2 of the J-Series, and the correct IP address is entered into your web browser. Check the serial number displayed in the HTML page against the J-Series that you intend to update. This serial number can be found in the top right hand corner for the web page as shown below.

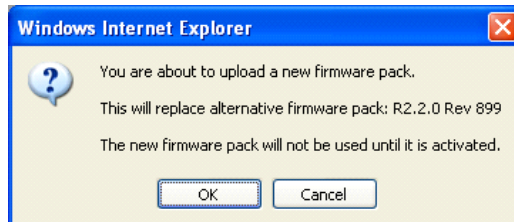
Click on the upload Firmware option. The firmware upload web page will now be displayed as shown below.



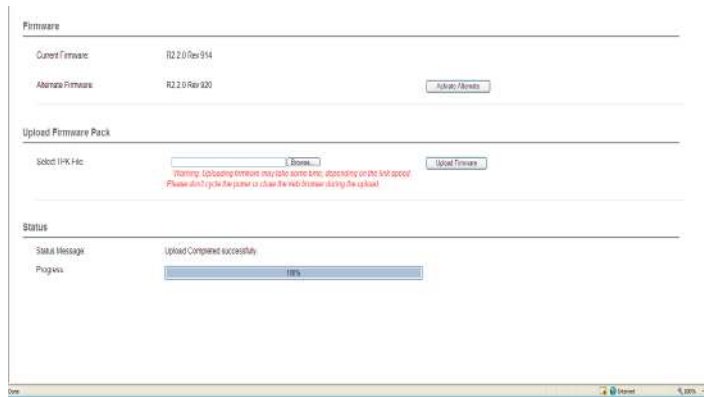
Click on the Browse button and locate the .TPK file which contains the new firmware. Select the file and click on “Open”.



Select Upload and once the warning below pops up Click on OK to confirm you are happy to delete old firmware. Noting that current operating firmware will be placed into Alternate Firmware position once Firmware Update is completed.



The upload of the firmware update file will begin and the “Upload Progress” section will display the progress through Uploading, Storing, deleting old firmware and verifying the new firmware. Once complete you will see Upload complete displayed in the status bar.



The second stage of the firmware update can be initiated, by selecting “Activate Alternative”. Again click OK to warning that you are happy to swap Firmware versions.



During this phase, all 5 LED indicators will flash amber simultaneously. After 1 to 10 minutes the J-Series will re-boot and the new firmware will be activated.



The J-Series rebooting sequence will take about 30 to 45 seconds. Once complete the LED indicators will flash in the normal sequence.

For and Access Point the Pwr/Tx will be continuously Green and will flash Red at a rate of once per second.

For a Remote the Pwr/Tx will be continuously Green whilst the Sync/NoRx will flash at a rate of once per second.

Note: With two or more J-Series within range of each other the Sync LED will flash on both the Access Point and the Remote indicating they are receiving Sync pulses from each other. (i.e. Access Point and Trusted Remotes are communicating).

If at any time a failure occurs during the firmware upload this will not affect the operation of the radio. as the new firmware is only stored until the user activates it. If at any time the upload fails you are able to restart the upload without any adverse effects. Care should still be taken to ensure the power is not turned off to the radio.

9.2 Replacing the Internal Fuse

WARNING

HAZARD OF FIRE

Where an internal fuse is to be replaced, the replacement fuse must be of the specified type and current rating. Refer to fuse replacement instructions within the product user manual before servicing.

Failure to follow these instructions can result in death or serious injury.

NOTICE

HAZARD OF EQUIPMENT DAMAGE

Remove power before replacing the fuse.

Failure to follow these instructions can result in equipment damage.

To access the internal fuse of the J-Series, the lid needs to be removed. To remove the lid, remove a single 2.5mm hex head screw from underneath the unit. When the fuse is replaced, re-fasten the lid with the single hex screw.

The procedure for changing the internal fuse depends on the serial number of the unit.

Serial numbers 421207 and greater

CAUTION

UNEXPECTED HARDWARE BEHAVIOR

The replaceable internal fuse has a rating of 3 Amps. Only Lead Free solder and soldering equipment should be used to replace the fuse.

These units have the fuse soldered directly to the PCB. Fuse replacement needs to be done in a qualified facility.

Failure to follow these instructions can result in injury or equipment damage.

DigiKey Part number: **486-2998-ND**

DigiKey description: **FUSE BRD MNT 3A 125VAC/VDC 2SMD**

Manufacturer: **SCHURTER Inc**

Manufacturer's part number: **3404.0014.11**

Manufacturer's description: **Surface Mount Fuse, 7.4 x 3.1 mm, Quick-Acting F, 125 VAC, 125 VDC**

Serial numbers less than 421207

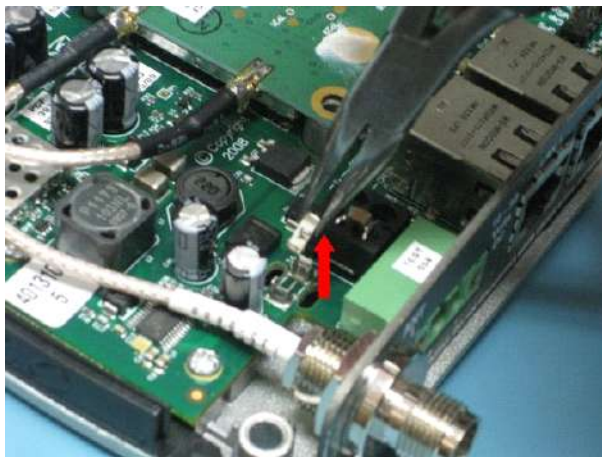
The fuse is not soldered into place. Instead it is mounted between 2 surface mount fuse holders and held down into place by a plastic fuse retainer. The plastic fuse retainer is required for hazardous compliance and needs to be fitted back into place each time a fuse is replaced.

To replace the fuse:

1. Remove the plastic fuse retainer. This may be done by levering it upwards with a small screwdriver.



2. Remove the blown fuse by using a pair of pliers and lifting upwards, as per below diagram.



3. Use a pair of pliers to sit the fuse straight across the top of the fuse clamps, as per below diagram.



4. Then with your finger, push down firmly on to the center of the fuse until it clicks down into place between the fuse clamps.
5. Fit the plastic fuse retainer by pinching the top 2 finger tabs gently together, then slipping the retainer arms over the fuse and through the two holes either side of the fuse until it has clipped onto the underneath of the J-Series PCB, as shown below.



6. Once the fuse is replaced, refasten the lid the single hex screw.

Schneider Part number: **TBUM297393**

Schneider Description: **Trio Series J and K Fuse Kit, 10 fuses**

DigiKey Part number: **SSQC 3-ND**

DigiKey description: **FUSE 3A 125VAC 2410 FAST**

Manufacturer: **Bel**

Manufacturer's part number: **SSQC 3**

Manufacturer's description: **QUICK ACT SMD, 3A, SQUARE CERAMIC 2410 SIZE, in SMT Clips**

10 **Part J - FCC Approved Antennas**

Yagi antennas

Part Number	Description
BMX890K	10 dBd, 900 MHz Yagi Directional Antenna Bluewave, Marathon Series
BMX890G	6.5 dBd, 900 MHz Yagi Directional Antenna Bluewave, Marathon Series
BGY890K	10 dBd, 900 MHz Yagi Directional Antenna Bluewave, Guardian Series
BGY890G	6.5 dBd, 900 MHz Yagi Directional Antenna Bluewave, Guardian Series
BXY24XI	6 dBd, 2.4 GHz Yagi Directional Antenna Bluewave, Sentinel Series
BXY24XK	8 dBd, 2.4 GHz Yagi Directional Antenna Bluewave, Sentinel Series
BXY24XM	10 dBd, 2.4 GHz Yagi Directional Antenna Bluewave, Sentinel Series

Omni antennas

Part Number	Description
BMO902J	9 dBd, 900 MHz Omni Directional Antenna Bluewave, Marathon Series
BMO902H	7 dBd, 900 MHz Omni Directional Antenna Bluewave, Marathon Series
BMO902G	6 dBd, 900 MHz Omni Directional Antenna Bluewave, Marathon Series
BGO902G	6 dBd, 900 MHz Omni Directional Antenna Bluewave, Guardian Series
BXO24XD	1 dBd, 2.4 GHz Omni Directional Antenna Bluewave, Sentinel Series
BXO24XG	4 dBd, 2.4 GHz Omni Directional Antenna Bluewave, Sentinel Series
BXO24XJ	7 dBd, 2.4 GHz Omni Directional Antenna Bluewave, Sentinel Series
BXO24XM	10 dBd, 2.4 GHz Omni Directional Antenna Bluewave, Sentinel Series
ANT2G4WHIP	0 dBd, 2.4 GHz Omni Directional Antenna Schneider Electric, Whip Series

Panel antennas

Part Number	Description
BXL24XM	10 dBd, 2.4 GHz Panel Directional Antenna Bluewave, Sentinel Series

Attention

Changes or modifications not expressly approved by Trio Schneider Electric could void the user's authority to operate the equipment. Fixed antennas require installation preventing end-users from replacing them with non-approved antennas. Antennas not listed in the above table need to be tested to comply with FCC Section 15.203 (unique antenna connectors) and Section 15.247 (emissions). Contact Schneider Electric if you need more information.

11 Part K - Support Options

When e-mailing questions to our support staff, make sure you tell us the exact model number (and serial number if possible) of the Trio equipment you are working with. Include as much detail as possible about the situation, and any tests that you have done which may help us to better understand the issue. If possible, include your telephone contact information should we wish to further clarify any issues.

See [Technical Support](#) 

12 Part L - Open Source License Acknowledgments

Schedule 1

If this product contains open source software licensed under Version 2 of the "GNU General Public License" then the license terms below in this Schedule 2 will apply to that open source software. If You would like a copy of the GPL source code in this product on a CD, Trio Datacom will mail to You a CD with such code for \$9.99 plus the cost of shipping, upon request.

The license terms below in this Schedule 2 are from the public web site at [http:// www.gnu.org/copyleft/gpl.html](http://www.gnu.org/copyleft/gpl.html)

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright © 1989, 1991 Free Software Foundation, Inc. 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

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. If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.) These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it. Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program. In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.
3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:
 - a. Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
 - b. Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
 - c. Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for non-commercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.) The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable. If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.
4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.
5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.
6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.
7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would 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.

END OF TERMS AND CONDITIONS END OF SCHEDULE 1

Schedule 2

If this product contains open source software licensed under the OpenSSL license:

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>). This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com). In addition, if this Linksys product contains open source software licensed under the OpenSSL license then the license terms below in this Schedule 3 will apply to that open source software. The license terms below in this Schedule 3 are from the public web site at <http://www.openssl.org/source/license.html>. The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org. OpenSSL License Copyright c 1998-2012 The OpenSSL Project. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)"
4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit <http://www.openssl.org/>"

THIS SOFTWARE IS PROVIDED BY THE OPENSSL PROJECT "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OPENSSL PROJECT OR ITS CONTRIBUTORS BE

LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License Copyright c 1995-1998 Eric Young (eay@cryptsoft.com) All rights reserved. This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with Netscape's SSL. This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)" The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related.
4. If 4. You include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR

A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License.]

END OF SCHEDULE 2

Schedule 3

If this product contains open source software from the NTP project, refer to the following license:

* Copyright (c) David L. Mills 1992-2012

* Permission to use, copy, modify, and distribute this software and its documentation for any purpose with or without fee is hereby granted, provided that the above copyright notice appears in all copies and that both the copyright notice and this permission notice appear in supporting documentation, and

that the name University of Delaware not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission. The University of Delaware makes no representations about the suitability this software for any purpose. It is provided "as is" without express or implied warranty.

***** END OF SCHEDULE 3

Schedule 4

If this product contains open source software from the NetSNMP project

Part 1:

Copyright 1989, 1991, 1992 by Carnegie Mellon University Derivative Work - 1996, 1998-2012 Copyright 1996, 1998-2012 The Regents of the University of California All Rights Reserved Permission to use, copy, modify and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appears in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of CMU and The Regents of the University of California not be used in advertising or publicity pertaining to distribution of the software without specific written permission.

Part 2:

Copyright (c) 2001-2012, Networks Associates Technology, Inc Portions of this code are copyright (c) 2001-2003, Cambridge Broadband Ltd. Copyright© 2003 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054,

U.S.A Copyright (c) 2003-2004, Sparta, Inc All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of the Networks Associates Technology, Inc nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS

OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

END OF SCHEDULE 4

13 Part M - Specifications

	> Trio JR900 JR240
Modem	
RF Channel Data Rate	900 MHz version - 512 kbps / 256 k / 128 k and 64 k, 2.4GHz version - 256 kbps / 128 k and 64 k
Auto Data Rate	900 MHz version only - Mixed 512 kbps and 256 kbps in same network
Bit Error Rate	BER <1x10-6 for 512 k @ -92 dBm, 256 k @ -102 dBm, 128 k @ -104 dBm and 64 k @ -106 dBm
Operating Modes	Access Point, remote, repeater or network-bridge
Network Types	Point-to-Point, Point-to-Multipoint, Point-to-Multipoint with Repeaters / Store and Forward, Mesh
Channelshare™	Trio's unique supervisory collision avoidance system
SmartPath™	Technology for enhanced redundancy in network configuration (Mesh)
Firmware	Local and over-the-air flash-based firmware
Security	
Encryption*	256-bit AES

HTML Interface	Password Protected HTTP and HTTPS configuration and management interface
Console Interface	Password Protected Telnet, SSH & serial console interface
Trusted Unit	Optional Trusted Access point-Trusted Remote operation
Diagnostics	
Diagnostics Overview	• Network Management & Remote Diagnostics with no software installation required • Network-wide operation from any remote terminal • Non intrusive protocol – runs simultaneously with the application • SNMP Access to Radio Diagnostics • Spectrum Analyzer and Channel Lockout facilities (Telnet/Text Interface) • Fully compatible with TVIEW+ Network Management Software • Diagnostics parameters available ○ Transmitter Power ○ Received Signal Strength ○ DC Supply Voltage ○ Received Frequency Error ○ Radio Temperature ○ VSWR (900 MHz version only)
General	
Operating Temperature Range	-40... 70 °C (-40... 158 °F)
Power Supply	13.8 Vdc nominal (10...30 Vdc)
Transmit Current	• 900 MHz: 800 mA nominal @ 1 W • 2.4 GHz: 620 mA nominal @ 0.5 W
Receive Current	<150 mA nominal @ 13.8 Vdc
Housing & Dimensions	Rugged die-cast, 100 x 34 x 165 mm, (4.0 x 1.4 x 6.5 in.)
Mounting	Integrated Mounting Holes or DIN Rail mounting (optional)
Weight	0.5 kg (1.1lbs.)

Approvals and Certifications	
Europe (ETSI)	ETSI EN 62368-1, EN50392 EN300328 EN301489 (2.4 GHz only)
FCC	FCC PART 15
Industry Canada	IC RSS210
Australia	ACMA AS/NZS 4268
Hazardous Locations	900 MHz: CSA Class I, Division II, Groups (A,B,C,D) for Hazardous Locations ANSI/UL equivalent) 2.4 GHz: ATEX II 3G Ex nA IIC T4
* Export restrictions may apply. Contact your local representative for more details. Note: Not all product features are available in every mode of operation. Disclaimer: Schneider Electric reserves the right to change product specifications. For more information visit www.schneider-electric.com.	

	TBURJRxxx-aabbbcd represents the part number matrix
Model	Model Type
TBURJ	J-Series
Code	Select: Unit Type
R	Base/Remote/Repeater Station with full enclosure
Code	Select: Generic Frequency Band
900	900 MHz
240	2.4 GHz
Code	Select: Frequency
	900 MHz Frequency Band
00	License-free band 902...928 MHz (FCC/IC - Requires Encryption for Canada and USA)
01	License-free band 915...928 MHz (Requires Encryption for Australia)
05	License-free band 921...928 MHz (New Zealand)
06	License-free band 902...907.5 MHz and 915...928 MHz (Brazil)

	2.4 GHz Frequency Band
00	License-free band 2.4 GHz, 500 mW (Requires Encryption for North America & Australia)
01	License-free band 2.4 GHz, ETSI/100 mW, ATEX (Europe)
Note: Other frequency bands available upon request.	
Code	Select: RF Channel Data Rate & Bandwidth (Internal Modem)
002	900 MHz: 64...512 kbps , 2.4 GHz: 64...256 kbps
Code	Select: Encryption
D	No Encryption
E	Encryption*
Code	Select: Approvals
H	Hazardous Environment CSA Class 1 Div 2
A	ATEX
Code	Future Option
0	None
Example: TBURJR900-00002EH0 specifies: Trio JR900 Remote Ethernet Station, 900 MHz band with a specific frequency range of 902...928 MHz, a 64...512 kbps modem, Encryption and Class1 Div2 rating. Communications Standards: FCC – Federal Communications Commission (USA) IC – Industry Canada ETSI – European Telecommunication Standards Institute ACMA – Australian Communications & Media Authority Contact your local sales office for accessories * Export restrictions may apply. Contact factory for details.	

Schneider Electric

Schneider Electric
35 rue Joseph Monier
92500 Rueil-Malmaison, France

Email: RemoteOperations@se.com

www.se.com

© 2012 - 2024 Schneider Electric
All Rights Reserved.