

WI-MOD-E Wireless Ethernet Modem User Manual

Preliminary Version



ATTENTION!

Incorrect termination of the supply wires may cause internal damage and will void the warranty. To ensure that your WI-MOD-E enjoys a long life, before turning the power on double-check ALL connections by referring to this User Manual.

CAUTION

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

DO NOT

- Operate the transmitter when anyone is within 20 cm of the antenna.
- Operate the transmitter unless all RF connectors are secure and any open connectors are properly terminated.
- Operate the equipment near electrical blasting caps or in an explosive atmosphere.

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

FCC Notice

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

- This device may not cause harmful interference, and
- This device must accept any interference received, including interference that may cause undesired operation.

This device must be operated as supplied by Weidmuller. Any changes or modifications made to the device without the written consent of ELPRO Technologies may void the user's authority to operate the device.

This device must be installed by professional installers in compliance with 47 CFR Part 15 Subpart C Section 15.204 and 15.205, who will be responsible for maintaining EIRP no greater than 36 dBm in accordance with 47 CFR Part 15 Subpart C Section 15.247 (b)(2)(4).

In accordance with 47 CFR Part 15 Subpart C Section 15.203, only the following antenna and coax cable combinations can be used with each radio.

Manufacturer	Model Number	Coax Cable	Net
Weidmuller	MD2400-EL	Includes 5 m Cellfoil	2 dBi Gain
Weidmuller	SG2400-EL	CC3-SMA (3 m)	2 dBi Gain
Weidmuller	Z2400-EL	CC10-SMA (10 m)	4 dBi Gain
Weidmuller	Y2400-EL	CC20-SMA (20 m)	6 dBi Gain

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



NOTE Any changes or modifications not expressly approved by Weidmuller could void the user's authority to operate this equipment.

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

Safety Notices

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

UL Notice

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

GNU Free Documentation License:

Copyright(C)2009 Weidmuller. Weidmuller is using a part of Free Software code under the GNU General Public License in operating the "WI-MOD-E-A/G" product. This General Public License applies to most of the Free Software Foundation's code and to any other program whose authors commit by using it. The Free Software is copyrighted by Free Software Foundation, Inc. and the program is licensed "As is" without warranty of any kind. Users are free to contact Weidmuller at the following Email Address: supportWeidmuller.com for instructions on how to obtain the source code used in the WI-MOD-E-A/G.

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

Important Notice

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

Weidmuller radio products are used on unprotected license-free radio bands with radio noise and interference. The products are designed to operate in the presence of noise and interference. However, in an extreme cases radio noise and interference could cause product operation delays or operation failure. As with all industrial electronic products, Weidmuller products can fail in a variety of modes due to misuse, age, or malfunction. We recommend that users and designers design systems using design techniques intended to prevent personal injury or damage during product operation, and provide failure tolerant systems to prevent personal injury or damage in the event of product failure. Designers must warn users of the

equipment or systems if adequate protection against failure has not been included in the system design. Designers must include this Important Notice in operating procedures and system manuals.

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

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

Follow Instructions

Read this entire manual and all other publications pertaining to the work to be performed before installing, operating, or servicing this equipment. Practice all plant and safety instructions and precautions. Failure to follow the instructions can cause personal injury and/or property damage.

Proper Use

Any unauthorized modifications to or use of this equipment outside its specified mechanical, electrical, or other operating limits may cause personal injury and/or property damage, including damage to the equipment. Any such unauthorized modifications: (1) constitute "misuse" and/or "negligence" within the meaning of the product warranty, thereby excluding warranty coverage for any resulting damage; and (2) invalidate product certifications or listings.

CONTENTS

Chapter 1 - INTRODUCTION	7	3.7 Security Menu	33
1.0 Network Topology	7	WEP (64-bit) and (128-bit)	33
Access Point vs. Client	8	Encryption Keys 1 to 4	33
Bridge vs. Router	9	Default WEP Key	34
1.1 Getting Started Quickly	11	Open or Shared Authentication Mode	34
Chapter 2 - INSTALLATION	12	WPA / WPA2	34
2.0 General	12	WPA Enterprise – Authenticator (AP)	
2.1 Antenna Installation	12	Configuration	35
Antenna Diversity	13	WPA Enterprise – Supplicant (Client)	
Line-of-sight Installations	13	Configuration	36
Antennas	13	3.8 Normal Operation	36
Installation Tips	13	Bridge Operation (Transparent Network)	36
Dipole and Collinear Antennas	14	Router Operation (Routed Network)	37
Directional Antennas	15	3.9 Radio Configuration	37
2.2 Power Supply	15	Channel Selection	39
2.3 Serial Connections	16	WI-MOD-E-G1 Modem (2.4 GHz 802.11b/g)	39
RS232 Serial Port	16	WI-MOD-E-A1 Modem (5 GHz 802.11a)	39
DB9 Connector Pinouts	17	3.10 Advanced Radio Configuration	40
RS485 Serial Port	17	Fixed Noise Floor	41
2.4 Discrete (Digital) Input/Output	18	3.11 Serial Port Configuration	41
Chapter 3 - OPERATION	19	RS-232 PPP Server	41
3.0 Startup	19	Serial Gateway (Server/Client/Multicast)	42
Access Point Startup (WI-MOD-E-G1)	19	Serial Gateway (Modbus RTU to TCP)	43
Access Point Startup (WI-MOD-E-A1)	19	Modbus TCP to RTU Gateway	43
Client Startup	19	3.12 Serial Menu	44
Link Establishment	19	RS-232 / RS485 Serial Port Configuration	44
How a Link Connection is Lost	19	RS232 PPP Server (Only RS232)	44
19 Roaming Clients	19	RS-232 / RS485 Serial Gateway Mode	45
3.1 Selecting a Channel	20	RS-232 / RS485 Modbus TCP/RTU Converter	46
802.11b/g (2.4 GHz)	20	3.13 Multicast Pipe Manager	46
802.11a (5 GHz)	21	3.15 Modbus I/O Transfer	47
Dynamic Frequency Selection	22	3.16 Roaming	51
3.2 Configuring the Unit for the First Time	23	3.17 Repeaters (WDS)	53
Default Configuration	23	3.18 Routing	60
Accessing Configuration for the First Time	23	3.19 Filtering	61
3.3 Quick Start Configuration	28	MAC Address Filter Configuration	63
3.5 Spanning Tree Algorithm	31	IP Address Filter Configuration	63
3.6 Compatibility	32	ARP Filter Configuration	64
3 Address Mode and 4 Address Mode	32	3.20 DHCP Client Configuration	64
Addresses in a Wireless Ethernet Data Frame	32	3.21 DHCP Server Configuration	65
Packets Between Access Point and Client	32	3.22 DNS Server Configuration	65
240U-E Compatibility	32	3.23 VLAN	65
		What is VLAN	65
		Operation	66

VLAN Group	67
Interface Membership	68
Example 1: Basic VLAN	68
Example 2: Multiple Wireless Interfaces	69
3.24 Module Information	72
3.25 Configuration Examples	73
Setting a WI-MOD-E to Factory Default Settings	73
Extending a Wired Network	73
Connecting Separate Networks	74
Extending Range Using Repeaters	76
Chapter 4 - DIAGNOSTICS	77
4.0 Diagnostics Chart	77
Boot Status LED Indication During Startup	77
4.1 Connectivity	77
Connected Devices	78
Site Survey	78
4.2 Channel Survey (Utilization)	79
Channel Utilization on a Live System	79
Channel Utilization for Channel Selection	
or RF Path Testing	79
Diagnosing Low Throughput	79
Solutions for High Channel Utilization	79
4.3 Custom Survey	81
4.4 Throughput Test	84
Internal Throughput Test	84
Throughput and Repeaters	86
4.5 Statistics	86
Wireless Statistics	87
Client	88
Network Traffic Analysis	88
4.6 System Tools	88
4.7 Testing Radio Paths	89
Connection and Signal Strength	89
Iperf Throughput Test	89
Internal Radio Test	89
RSSI	90
Throughput	90
4.8 Remote Configuration	91
4.9 Internal Diagnostics Modbus Registers	92
Connection Information	92
Statistic Registers	92
4.10 Utilities	93
ping	93
arp	95
route	96

Appendix A - FIRMWARE UPGRADE	99
Web-based Upgrade	99
Appendix B - GLOSSARY	100
Appendix C - CHANNELS	104

Chapter 5 - SPECIFICATIONS 97

Chapter 1 - INTRODUCTION

The WI-MOD-E Wireless Ethernet Modem and Device Server is an industrial 802.11-compliant module that provides wireless connections between Ethernet devices and/or Ethernet wired networks (LANs). The WI-MOD-E is available in two models with different RF power and frequency options suitable for your country's local radio regulations. The models comply with their relevant IEEE 802.11 standard.

WI-MOD-E-G1	802.11 b/g 600 mW max power
WI-MOD-E-A1	802.11 a 630 mW max power

The WI-MOD-E-G1 and WI-MOD-E-A1 have the same functionality, but use a different radio to communicate. The two types of radios do not communicate with each other, that is, a WI-MOD-E-G1 will not communicate with a WI-MOD-E-A1. Only modules of the same type are able to communicate wirelessly with each other. Throughout this manual, any reference to WI-MOD-E refers to one of the above models.

The WI-MOD-E-G1 model uses a 2.4-GHz direct sequence spread spectrum (DSSS) wireless transceiver. Users pick a 20-MHz channel with 5-MHz channel spacing from the available 13 channels, starting with the first channel centered on 2.412 GHz. There are some limitations depending on country. See "Appendix C - CHANNEL " for channel selections. Note that regulations in North America permit 11 x 2.4 GHz channels and Europe permits 13 x 2.4 GHz channels.

The WI-MOD-E-A1 uses a 5-GHz DSSS wireless transceiver, and users must select appropriate channel and transmit power allowable in their country. Check with your ELPRO representative for the permitted channel usage in your country. See "Appendix C- CHANNELS" for channels selections.

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

The modem is VLAN compliant and capable of passing VLAN tagged frames by default. VLAN bridging and Routing Modes are also available which will facilitate a number of different VLAN topologies.

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

1.0 Network Topology

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

- Access Point or Sta, Station, Client
- Bridge or Router

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

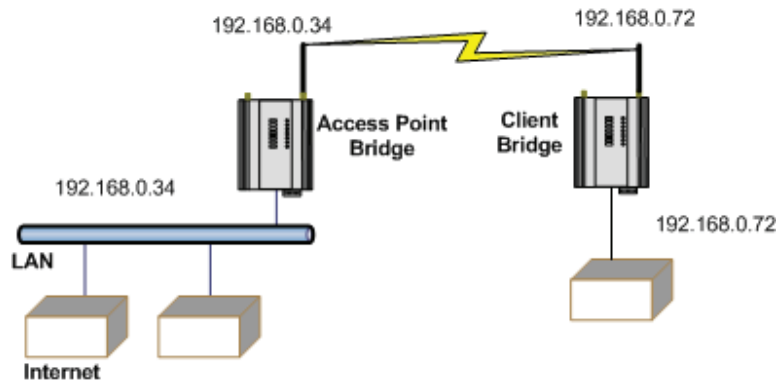


Figure 1 Network Topology

Access Point vs. Client

The access point unit acts as the wireless master unit. The access point accepts and authorizes links initiated by client units, and controls the wireless communications. Clients (Stations) are slave units and when connected to the access point becomes transparent Ethernet link. Figure 2 shows a connection between two Ethernet devices using WI-MOD-E Ethernet modems. In this example, one WI-MOD-E is configured as an access point and the other as a client.

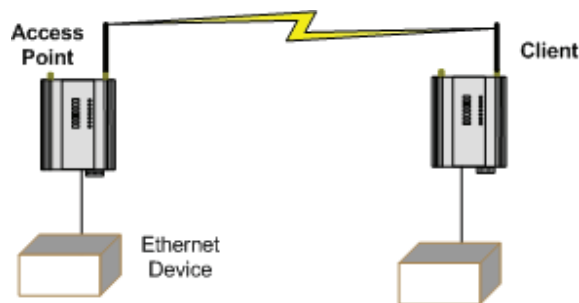


Figure 2 Access Point and Client (Example 1)

Figure 3 shows an existing LAN being extended using 245U-Es. In this example, the access point should be configured at the LAN end, although the wireless link will still work if the client is at the LAN end.

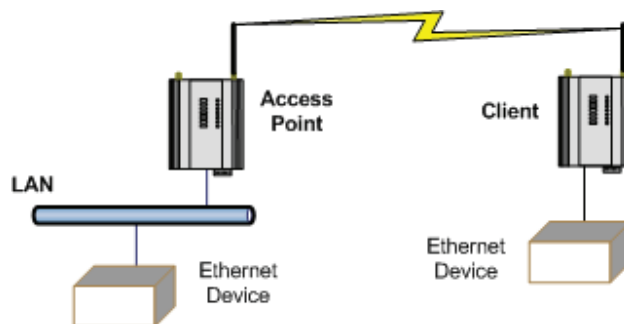


Figure 3 Access Point and Client (Example 2)

An access point can connect to multiple clients. In this case, the access point should be the central unit.

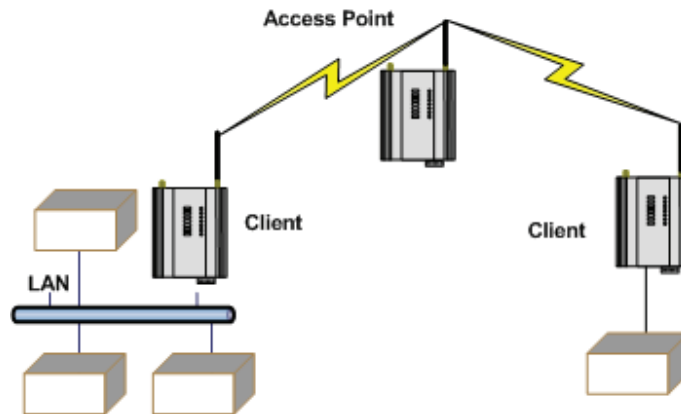


Figure 4 Repeater

An access point could be used as a repeater unit to connect two WI-MOD-E clients that do not have direct reliable radio paths. There is no special repeater module—any WI-MOD-E can be a repeater and at the same time, can be connected to an Ethernet devices or on a LAN.

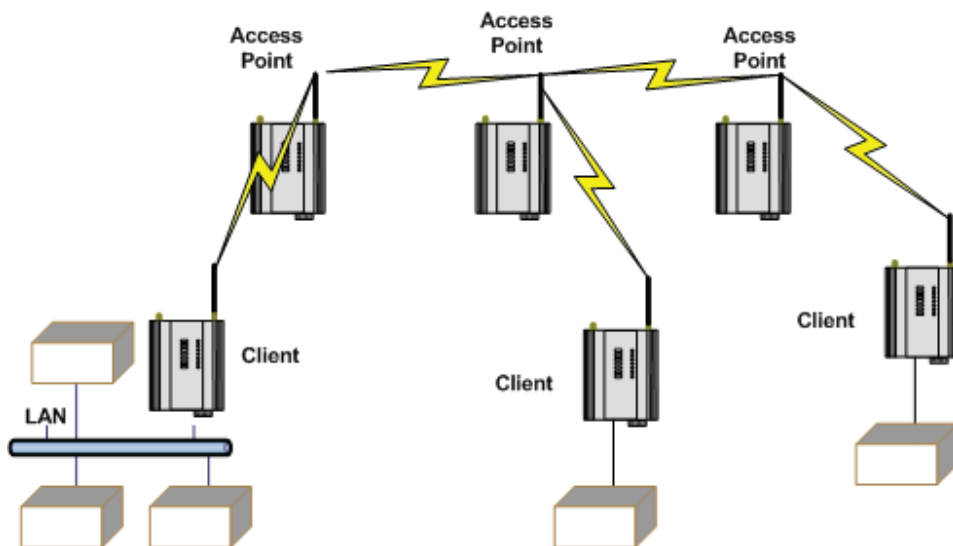


Figure 5 Multiple Repeaters

Multiple access points can be set up in a mesh network to provide multiple repeaters.

Bridge vs. Router

Each WI-MOD-E is configured with one IP address for the Ethernet side and another for the wireless side. A bridge connects devices within the same Ethernet network, for example, extending an existing Ethernet LAN. For a bridge, the IP address for the wireless side is the same as the Ethernet side.

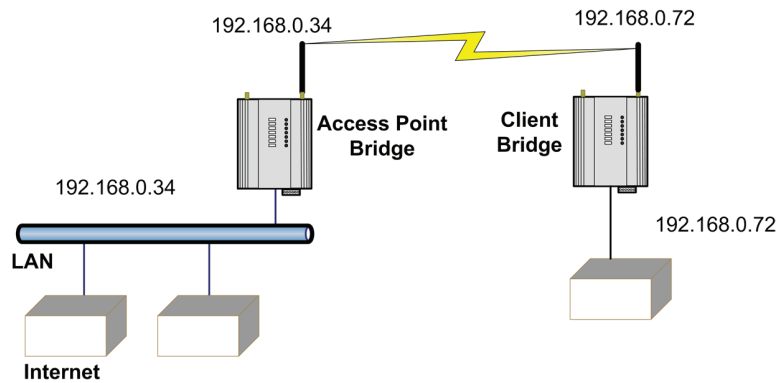


Figure 6 Bridge

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

Alternatively, the access point could be configured as a router. The wireless link is then part of LAN B. If more than two routers are required within the same radio network, routing rules may need to be configured

(see “3.18 Routing” for further details). There is no limit to the number of bridges in the same network, although there is a limit of 128 client units linked to any single access point.

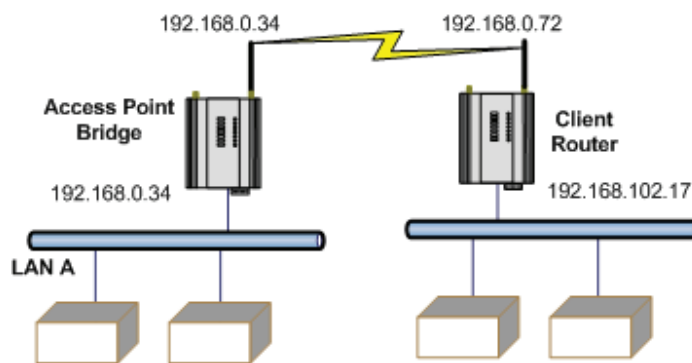


Figure 7 Client Router

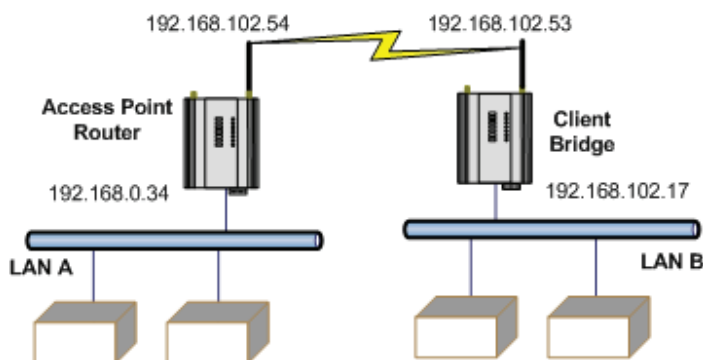


Figure 8 AP Router

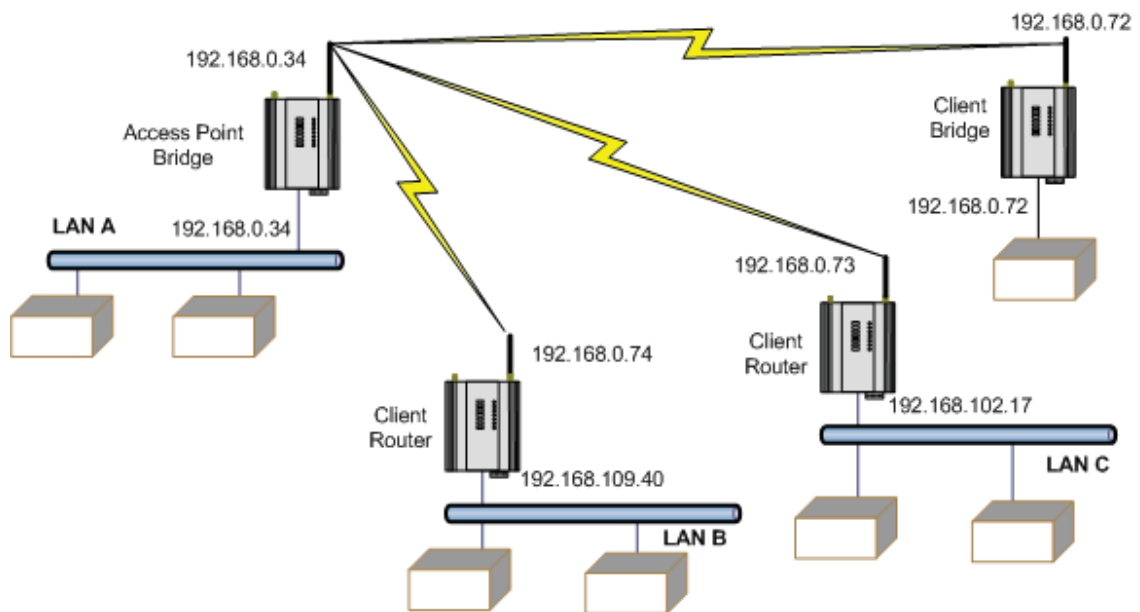


Figure 9 Router

1.1 Getting Started Quickly

Most applications for the WI-MOD-E require little configuration. The WI-MOD-E has many sophisticated features, but if you do not require these features this section will enable you to configure the units quickly.

To get started quickly:

1. First, read "Chapter 2 - INSTALLATION." The 245U-E requires an antenna and a power supply.
2. Power on the WI-MOD-E and make an Ethernet connection to your PC.
For detailed steps, refer to "3.2 Configuring the Unit for the First Time."
3. Set the WI-MOD-E address settings as described in "3.2 Configuring the Unit for the First Time."
4. Save the configuration.

The WI-MOD-E is now ready to use.

Before installing the WI-MOD-E, bench test the system. It is much easier to locate problems when the equipment is all together. There are other configuration settings, which may or may not improve the operation of the system. For more information, refer to "3.0 Startup."

Chapter 2 - INSTALLATION

2.0 General

The WI-MOD-E modules are housed in a rugged aluminum case suitable for DIN-rail mounting. Terminals will accept wires up to 2.5 mm² (12 gauge) in size. All connections to the module must be SELV (Safety Extra Low Voltage). Normal 110-250 V mains supply must not be connected to any terminal of the WI-MOD-E module. See “2.2 Power Supply.”

Before installing a new system, it is preferable to bench test the complete system. Configuration problems are easier to recognize when the system units are adjacent. Following installation, the most common problem is poor communications caused by incorrectly installed antennas, radio interference on the same channel, or the radio path being inadequate. If the radio path is a problem (for example, the path is too long or obstructed), a higher performance antenna or a higher mounting point for the antenna may rectify the problem. Alternatively, use an intermediate WI-MOD-E module as a repeater.

The *WI-MOD-E Installation Guide* provides an installation drawing appropriate to most applications. Further information is provided below. Each WI-MOD-E module should be effectively earthed via the “GND” terminal on the back of the module. This is to ensure that the surge protection circuits inside are effective.

2.1 Antenna Installation

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

The maximum range achievable depends on the radio model, the regulated RF power permitted in your country, and whether you use separate transmit and receive antennas. If using a WI-MOD-E-G1 (2.4 GHz) with a single antenna, 10 km (6 miles) can be achieved in USA, Canada, and Australia (4 W EIRP) and 2 km in Europe (100 mW EIRP). If using a WI-MOD-E-A1 (5 GHz) with a single antenna, 5 km (3 miles) can be achieved in USA, Canada, and Australia (1 W EIRP) and 3 km in Europe (500 mW EIRP), but more care is needed in selecting antennas and coax, and radio paths need to be complete line of site (no obstruction whatsoever).

To achieve the maximum transmission distance, the antennas should be raised above intermediate obstructions so that the radio path is true line-of-sight. The modules will operate reliably with some obstruction of the radio path, although the reliable distance will be reduced. Obstructions that are close to either antenna will have more of a blocking affect than obstructions in the middle of the radio path. The WI-MOD-E modules provide a diagnostic feature that displays the radio signal strength of transmissions (refer to “Chapter 4- DIAGNOSTICS”).

Line-of-sight paths are only necessary to obtain the maximum range. Obstructions will reduce the range, but may not prevent a reliable path. A greater amount of obstruction can be tolerated for shorter distances. For short distances, it is possible to mount the antennas inside buildings. An obstructed path requires testing to determine if the path will be reliable. Refer to “4.7 Testing Radio Paths.”

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

The WI-MOD-E unit has two antenna connections at the top of the module, allowing for two antennas to be fitted to the module if necessary. (Note: Antenna Diversity not available with the 245U-E-A1 model)

By default the right connector, labeled “TX/RX,” is the main connection used for transmitter and receiver. The left connector, labeled “RX,” is not connected unless configured as described in “3.10 Advanced Radio Configuration.” Each antenna port can be configured for TX only, RX only, or Diversity (TX and RX). Selection can be made by choosing one of the options from TX Antenna / RX Antenna on the Advanced Radio Configuration page.



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

Antenna Diversity (Note: not available with WI-MOD-E-A1 model)

One reason to use multi-antennas is to comply with local radio licensing regulations. All countries have a limit on the amount of transmitted power and radiated power from the antenna. In the US this is 400-milliwatts transmit power and 4-watts EIRP (effective isotropic radiated power). See “3.10 Advanced Radio Configuration” for details on configuring antenna diversity

In North America, the maximum allowable radiated power (EIRP) for a WI-MOD-E-G1 is 4 W, which is 10 dB higher than the modules transmit power of 400 mW. Therefore, you can increase the antenna gain as long as the overall system gain (antenna gain, coax loss) does not rise above 10 dB.

Example

- Using the WI-MOD-E with a 10 m (33 ft) Cellfoil coax cable (approximately 6 dB of loss) and an 8-dBi gain antenna would equate to approximately 2 dB of gain, which is well below the 10 dB limit.
- Using the WI-MOD-E with a 20 m (66 ft) Cellfoil coax cable (approximately 12 dB of loss) and an 18-dBi antenna would equate to approximately 6 dB of gain, which is also below the 10 dB limit.

Line-of-sight Installations

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

Antennas

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

The net gain of an antenna/cable configuration is the gain of the antenna (in dBi) less the loss in the coaxial cable (in dB). The maximum net gain of the antenna/cable configuration connected to the TX/RX connector is 0 dB in Europe (100 mW ERP). In USA, Canada and Australia (4 W ERP), the maximum gain is 10 dB for the WI-MOD-E-400 and 16 dB for the WI-MOD-E-100.

There is no gain restriction for antennas connected to the RX connector.

Antenna	WI-MOD-E-G1 Gain (dBi)	WI-MOD-E-A1 Gain (dBi)
Dipole	2 dBi	6 dBi
Collinear	5 or 10 dBi	10 dBi
Directional	18 dBi	10 – 20 dBi
Cable Loss	dB per 30 m / 100 ft	dB per 30 m / 100 ft
RG58 Cellfoil	-17 dB	-24.5 dB
RG213	-16.2 dB	-28.6 dB
LDF4-50	-3.6 dB	-5.5 dB
NOTE 20 dB attenuator must be fitted if radio distance is less than 33 ft (10 m).		

The net gain of the antenna/cable configuration is determined by adding the antenna gain and the cable loss. For example, using the WI-MOD-E-G1 a 10 dBi antenna (7.8 dBd) with 10 meters of Cellfoil (-5.6 dB) has a net gain of 2.2 dB (7.8 dB – 5.6 dB).

Installation Tips

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

Where antennas are mounted on elevated masts, the masts should be effectively earthed (grounded) to avoid lightning surges. For high lightning risk areas, surge suppression devices between the module and the antenna are recommended. If the antenna is not already shielded from lightning strike by an adjacent earthed/grounded structure, a lightning rod may be installed above the antenna to provide shielding.

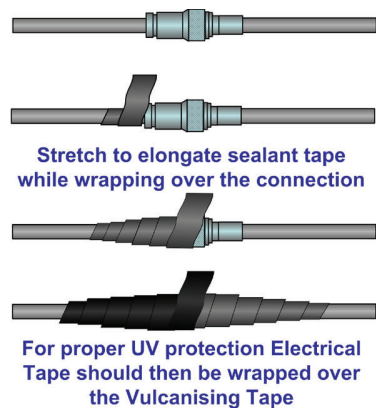


Figure 10 Vulcanizing Tape

Dipole and Collinear Antennas

A dipole or collinear antenna transmits the same amount of radio power in all directions—as such they are easy to install and use. The dipole antenna with integral 15 ft (5 m) cable does not require any additional coaxial cable. However, a cable must be used with the collinear antennas. To obtain maximum range, collinear and dipole antennas should be mounted vertically, preferably 1 wavelength away from a wall or mast (see Figure 11 for distances), and at least 3 ft (1 m) from the radio module.

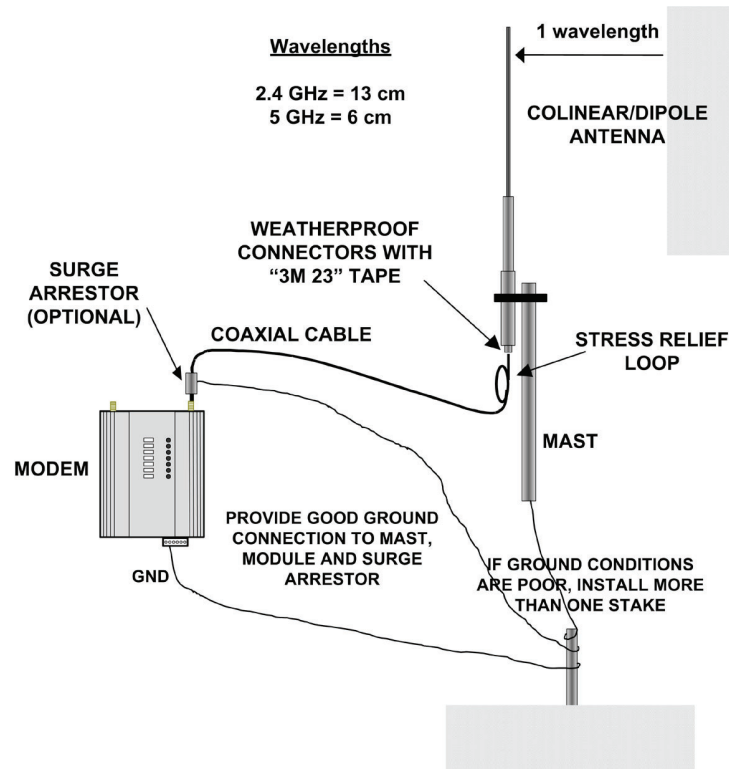


Figure 11 Colinear/Dipole Antenna

Directional Antennas

Directional antennas can be any of the following:

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

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

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

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

mounted as per the manufacturer’s instructions, with the parabolic grid at the back and the radiating element pointing in the direction of the transmission.

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

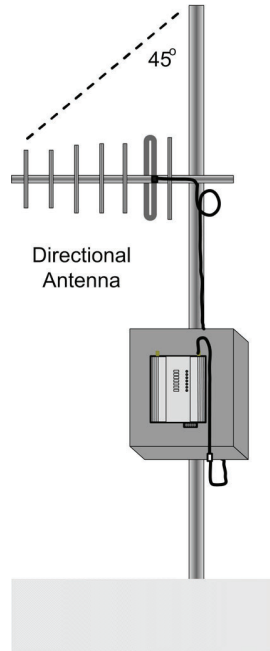


Figure 12 Collinear Antenna

2.2 Power Supply

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

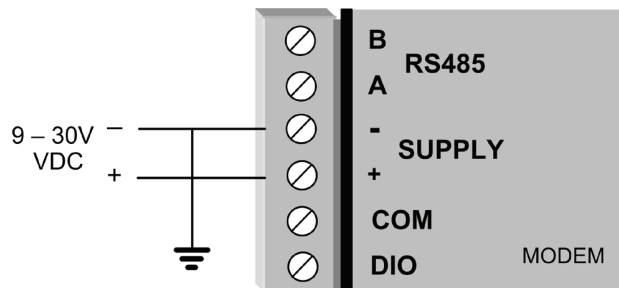


Figure 13 Power Supply

The power requirements of the WI-MOD-E unit are shown in the following table.

	WI-MOD-E-G1		WI-MOD-E-A1	
	12 Vdc	24 Vdc	12 Vdc	24 Vdc
Quiescent	290 mA	150 mA	300 mA	160 mA
TX @100 mW	310 mA	170 mA	370 mA	190 mA
TX @ 400 mW	340 mA	180 mA	410 mA	210 mA

A ground terminal is provided on the back of the module. This terminal should be connected to the main ground point of the installation in order to provide efficient surge protection for the module (refer to the installation diagram in the *WI-MOD-E Installation Guide*).

2.3 Serial Connections

RS232 Serial Port

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

Hardware handshaking using the CTS/RTS lines is provided. The CTS/RTS lines may be used to reflect the status of the local unit's input buffer. The WI-MOD-E does not support XON/XOFF. Example cable drawings for connection to a DTE host (a PC) or another DCE hosts (or modem) are detailed in Figure 14.

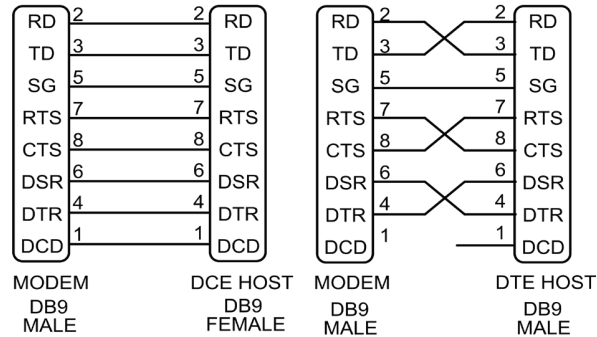


Figure 14 Serial Cable

DB9 Connector Pinouts

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

RS485 Serial Port

The RS485 port provides for communication between the WI-MOD-E unit and its host device using a multi-drop cable. Up to 32 devices may be connected in each multi-drop network. Because the RS485 communication medium is shared, only one of the units on the RS485 cable may send data at any time. Therefore, communication protocols based on the RS-485 standard require some type of arbitration.

RS485 is a balanced differential standard, but it is recommended that shielded twisted pair cable be used to interconnect modules to reduce potential RFI. It is important to maintain the polarity of the two RS485 wires. An RS485 network should be wired as indicated in the diagram below and terminated at each end of the network with a 120-ohm resistor. On-board 120-ohm resistors are provided and may be engaged by operating the single DIP switch in the end plate next to the RS485 terminals. The DIP switch should be in the “1” (on) position to connect the resistor. If the module is not at one end of the RS485 cable, the switch should be off.

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

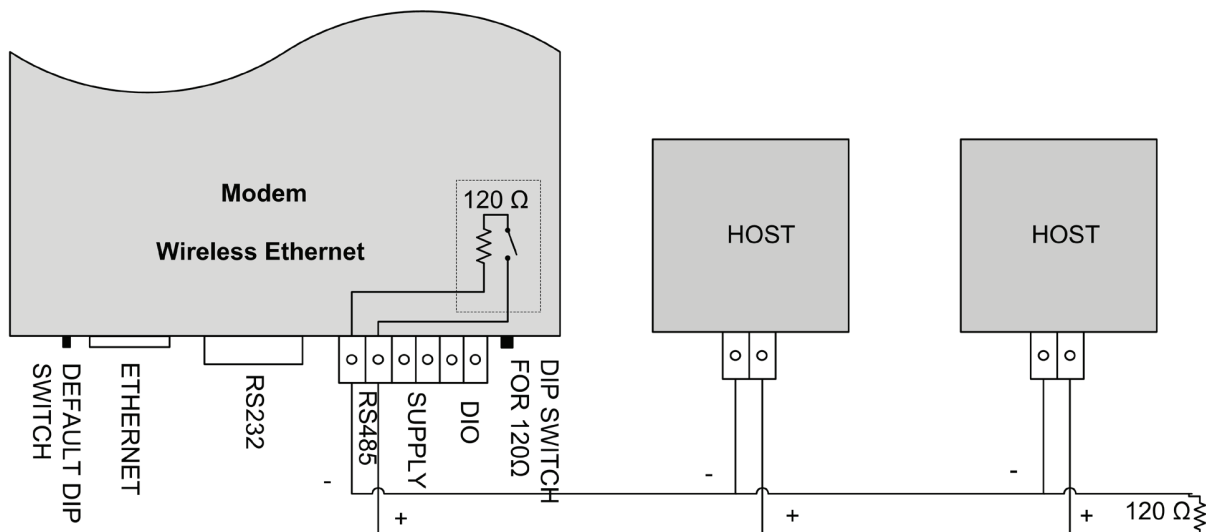


Figure 15 Multidrop Serial

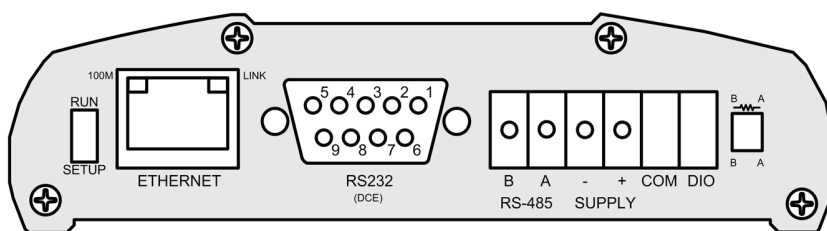


Figure 16 End Plate

2.4 Discrete (Digital) Input/Output

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

If used as an input, the I/O channel is suitable for voltage-free contacts (such as mechanical switches) or

NPN transistor devices (such as electronic proximity switches). PNP transistor devices are not suitable. Contact wetting current of approximately 5 mA is provided to maintain reliable operation of driving relays.

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

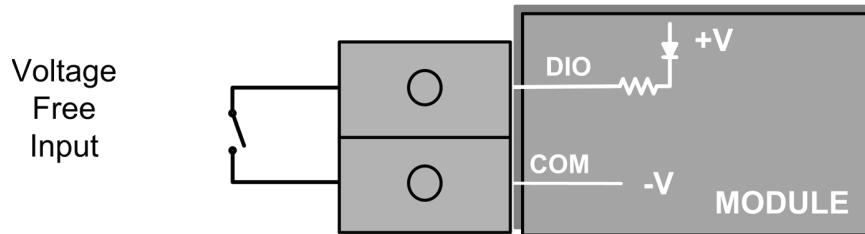


Figure 17 DIO Input

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

NOTE The output circuit is connected to the DIO terminal. The digital output circuit includes a LED indicator, which is red when the digital output is active.

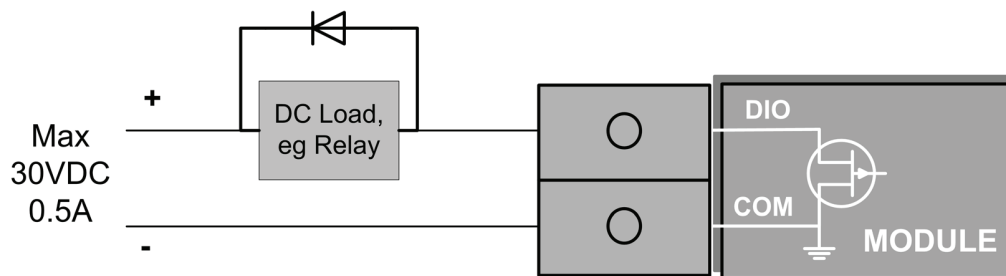


Figure 18 DIO Output

Chapter 3 - OPERATION

3.0 Startup

Access Point Startup (WI-MOD-E-G1)

When an access point unit starts up, it checks if the channel selection is set to “Auto.” If it is, the access point will scan all available channels, pick the quietest then begin transmitting periodic messages, called beacons. If the access point is configured with a fixed channel, it will immediately begin sending beacons on the configured channel. Beacons include information that a client may examine in order to identify if the access point is suitable for link establishment. Clients will only attempt to establish a link with an access point whose beacon indicates a matching SSID. Access points do not initiate link establishment.

Access Point Startup (WI-MOD-E-A1)

If the modem is configured to use Dynamic Frequency Selection (DFS), it will behave slightly differently than the WI-MOD-E-G1 because it needs to comply with DFS regulations. When an access point starts up, it will scan all available channels from the selected groups and then select the quietest, similar to the WI-MOD-E-G1. It will then go into a scan mode for 60 seconds where it listens for any radar signals. If a radar signal is detected, it will flag the channel as being unavailable (the channel will stay unavailable for 30 minutes) and then pick another random channel and repeat the same scanning process until a radar-free channel becomes available.

Client Startup


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

Link Establishment

Once a client identifies a suitable access point for link establishment it attempts to establish a link using a two-step process—authentication, and association. During authentication, the client and access point check if their configurations permit them to establish a link. Once the client has been authenticated, it will then request an association to establish a link.

Status of the wireless link is indicated via the TX/LINK LED. For an access point, the TX/LINK LED will be off while no links have been established. Once one or more links have been established, the TX/LINK LED is on green. For a client, the Link LED will reflect the connection status to an access point. Link status is also displayed on the Connectivity page of the Web interface.

After the link is established, data may be transferred in both directions. The access point will act as a master unit and will control the flow of data to the clients linked to it. Clients can only transmit data to the access point to which they are connected. When a client transfers data to another client, it first transmits the data to the access point, which then forwards the data to the destined client. A maximum of 127 clients may be linked to an access point.

 **NOTE** The presence of a link does not mean that the connected unit is authorized to communicate over radio. If the encryption keys are incorrect between units in the same system or a dissimilar

encryption scheme is configured, the LINK LED will turn on, but data cannot be passed over the wireless network.

How a Link Connection is Lost

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

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

Roaming Clients

Clients can roam within a system, but if the link to the access point fails or the radio signal level becomes too weak it will scan for beacons and connect to an access point (provided the SSID and any encryption methods, keys are compatible). If there are multiple access points, it will select the connection with the best signal level. This functionality permits a client to have mobility while maintaining a link with the most suitable access point.

LED Indication

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

LED Indicator	Condition	Meaning
OK	Green	Normal operation.
OK	Flashing Red / Green	Module boot sequence.
Radio RX	Green flash	Radio receiving data (good signal strength).
Radio RX	Red flash	Radio receiving data (low signal strength).
TX/LINK	Green	Radio connection established.
TX/LINK	Red flash	Radio transmitting.
RS-232	Green flash	Data sent from RS-232 serial port.
RS-232	Red flash	Data received to RS-232 serial port.
LAN	ON	Link established on Ethernet port
LAN	Flash	Activity on Ethernet port.
RS-485	Green flash	Data sent from RS-485 serial port.
RS-485	Red flash	Data received to RS-485 serial port.
DIO	Green	Digital input is grounded.
DIO	Red	Digital output is active.
DIO	Off	Digital output off and input is open circuit.

The Ethernet RJ45 port incorporates two indication LEDs. The Link LED comes on when there is a connection on the Ethernet port, and will blink off briefly when activity is detected on the Ethernet port. The 100-MB LED indicates that the connection is at 100 MBit/sec. The 100-MB LED will be off for 10 MB/sec connection. Other conditions indicating a fault are described in “Chapter 4- DIAGNOSTICS.”

3.1 Selecting a Channel

802.11b/g (2.4 GHz)

The WI-MOD-E-G1 conforms to the IEEE 802.11b/g Wireless LAN specification. The WI-MOD-E-G1 supports 13 x 20 MHz, 12 x 10 MHz and 13 x 5 MHz radio channels in the 2412 MHz to 2482 MHz frequency range. Channels are country or region specific. Please check your local regulatory body for compliance and channel selection.

Figure 20 shows that there are a limited number of channels available in the 2.4 GHz frequency range. Care must be taken when selecting an operating channel, as some of the channels overlap. The 20-MHz channels have a separation of 5 MHz, which means there is some overlap into the next channel. Channel 1 will overlap into channel 2, 3, and 4, channel 6 will overlap into channels 3, 4, 5, 7, 8 and 9. If complete separation is required, you can use channels 1, 6 and 11 without any interference between the channels.

The 10 MHz channels are also separated by 5 MHz and overlap the adjacent channels by 5 MHz forward and backward. Channel 41 will overlap with channel 42, channel 46 will overlap with channel 45 and 47. The 5 MHz channels are separated by 5 MHz and do not overlap at all, so you can operate all 13 channels at the same time with minimal interference from the adjacent channel.

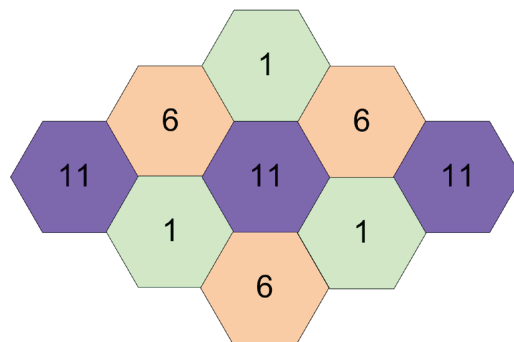


Figure 19 Channel Separation

Only one of these channels is used at a time and is configured at the access point, The access point then uses this channel to send out beacon transmissions and connections. Clients scan all channels for a suitable access point and then adopt the same channel as the access point when a connection is established. Figure 20 shows the RF energy distribution for the 802.11b/g transmission.

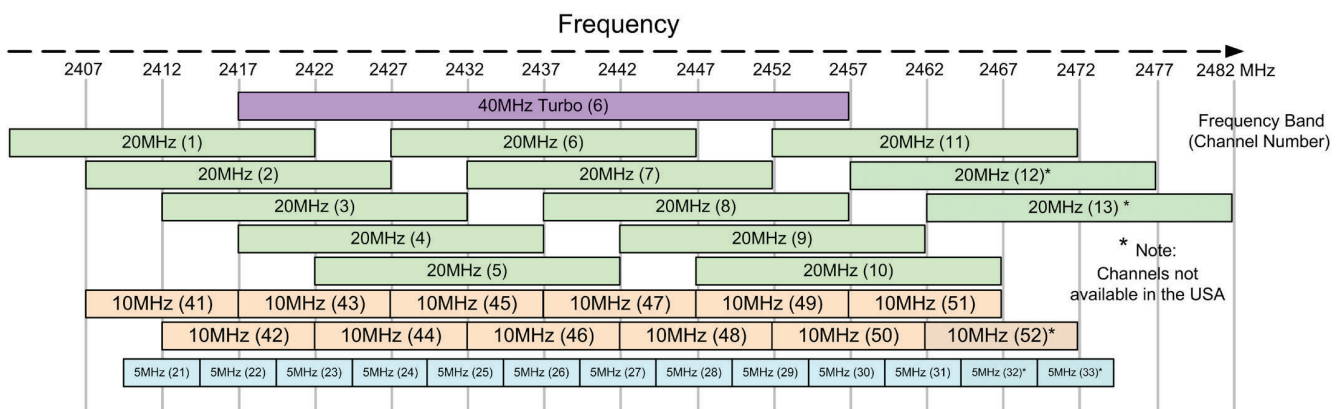


Figure 20 2.4-GHz Frequencies

On the 20-MHz channel (green), most of the energy is transmitted within the channel but some of the energy is transmitted on the channels on either side, therefore causing interference on these channels. The 10-MHz channels (orange) are similar, with half of the energy overlapping into the next channel, but you can configure up to 6 x non-interfering channels at the same time. The 5-MHz channels (blue) do not overlap, so all 13 channels can be used at the same time. There is also a single 40-MHz Channel (purple) that takes up over half of the full 2.4-GHz band, and is therefore much more susceptible to interference from other channels.

If there is more than one 802.11 access point within the same wireless range, it is important that the access points are on channels that are as far apart as possible. If there are two 20-MHz channel access points, set them to channel 1 and 11. If there are three, set them to 1, 6, and 11.

802.11a (5 GHz)

The WI-MOD-E-A1 utilizes frequency bands within the range of 5.15 GHz and 5.825 GHz. This is broken into 4 distinct U-NII bands, and each region (for example, EU, US, AUS, NZ) has their own power and operational constraints. See “Appendix C- CHANNELS” for details.

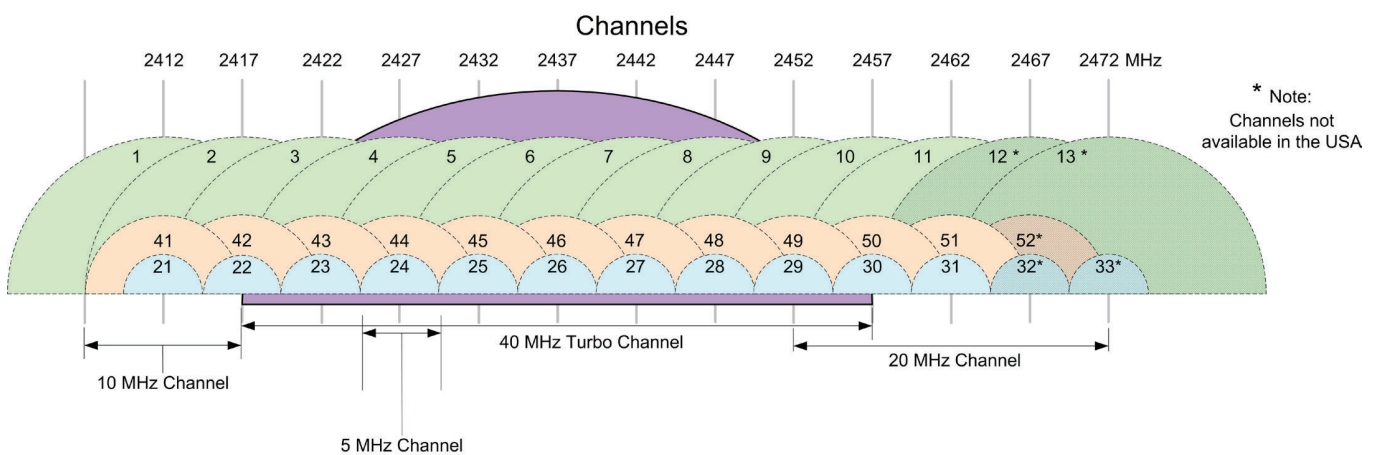


Figure 21 2.4-GHz Channels

The following table shows the US power and operational constraints.

Group 1	5.15–5.25 GHz	@ 50 mW
Group 2	5.25–5.35 GHz	@ 250 mW to 1 Watt
Group 3	5.47–5.725 GHz	@ 250 mW to 1 Watt
Group 4	5.725–5.825 GHz	@ 1 Watt

Each frequency band has certain limitations on the amount of radiated power that it can output, as well as whether the band uses Dynamic Frequency Selection (DFS), which is explained in the next section.

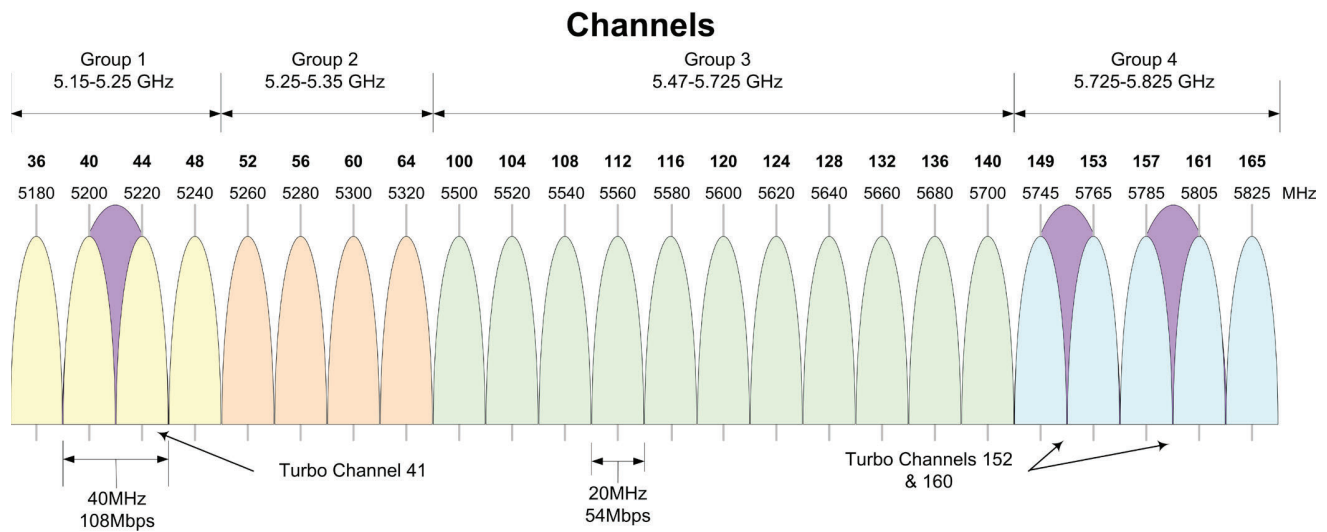


Figure 22 5-GHz Channels

Dynamic Frequency Selection

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

When DFS is enabled, the access point (master device) goes through the following steps:

1. The master device that initiates communications selects a channel and monitors that channel for potential radar interference for a minimum listening time of 60 seconds (channel availability check time). No transmissions can occur during this period.
2. If interference is detected, the system selects another channel and repeats the channel availability check on the new channel (the original channel is added to a list of channels with radar).
3. Once a channel has been selected and passes the channel availability check, the network starts to use that channel.
4. While using the channel, the network's master device continuously monitors for potential interference from a radar source (this is referred to as "in-service monitoring"). If interference is detected, the network master device issues commands to all other in-network devices to cease transmissions. The channel is added to the list of channels with radar.
5. The master device then selects a new channel (one that is not on the radar list).
6. A channel that has been flagged as containing a radar signal (either by a channel availability check or by in-service monitoring) is subject to a 30-minute non-occupancy period, during which time the channel cannot be used by the device in order to protect scanning radars. The channel on the radar list will be purged once the non-occupancy period has elapsed for that channel.

3.2 Configuring the Unit for the First Time

The WI-MOD-E has a built-in Web server containing webpages for analyzing and modifying the module's configuration. The configuration can be accessed using Microsoft® Internet Explorer® version 7 or greater. This program is shipped with Microsoft Windows® or may be obtained freely from the Microsoft website. If using other browsers, make sure that they are fully compliant with IE7 SSL security.



NOTE Microsoft Internet Explorer Version 6 will not load webpages due to a compatibility issue between IE6 and SSL-security websites.

Default Configuration

The default factory configuration of the WI-MOD-E is as follows:

- Client/Bridge/.
- IP address 192.168.0.1XX, where “XX” is the last two digits of the serial number (the default IP address is shown on the printed label on the back of the module).
- Netmask 255.255.255.0.
- Username is “user” and the default password is “user”.

The WI-MOD-E will temporarily load some factory default settings if powered up with the factory default switch (on the end-plate of the module) in SETUP position. The previous configuration remains stored in non-volatile memory and will only change if a configuration parameter is modified and the change saved.



NOTE Wireless operation is disabled when in SETUP mode. Remember set the switch back to the RUN position and cycle power at the conclusion of configuration for resumption of normal operation.

Accessing Configuration for the First Time

Because the default IP address is in the range 192.168.0.XXX, the unit may not connect to your network or PC. There are two methods for accessing the configuration for the first time.

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

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

Method 1 – Set PC to Same Network as WI-MOD-E

1. Connect the Ethernet cable between the module and the PC configuring the module.
2. Set the factory default switch to the SETUP position.

This will always start the WI-MOD-E with Ethernet IP address 192.168.0.1XX, subnet mask 255.255.255.0, gateway IP 192.168.0.1, and the radio disabled.



NOTE Remember to set the switch back to the RUN position and restart the module at the conclusion of configuration for resumption of normal operation.

3. Power up the WI-MOD-E module.
4. On the PC, open the Control Panel, and then open Network Settings.

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

5. Open Properties of Local Area Connection.
6. Select Internet Protocol (TCP/IP) and click Properties.

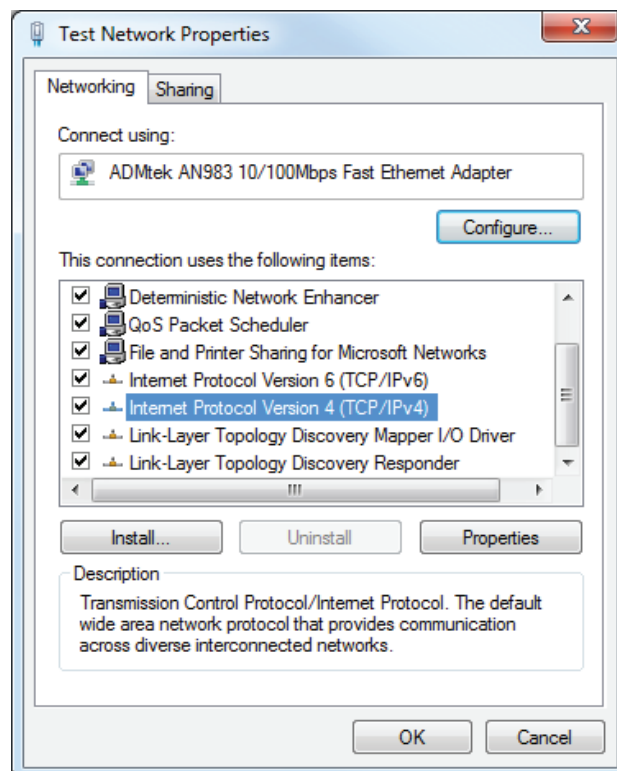


Figure 23 Local Area Connection

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

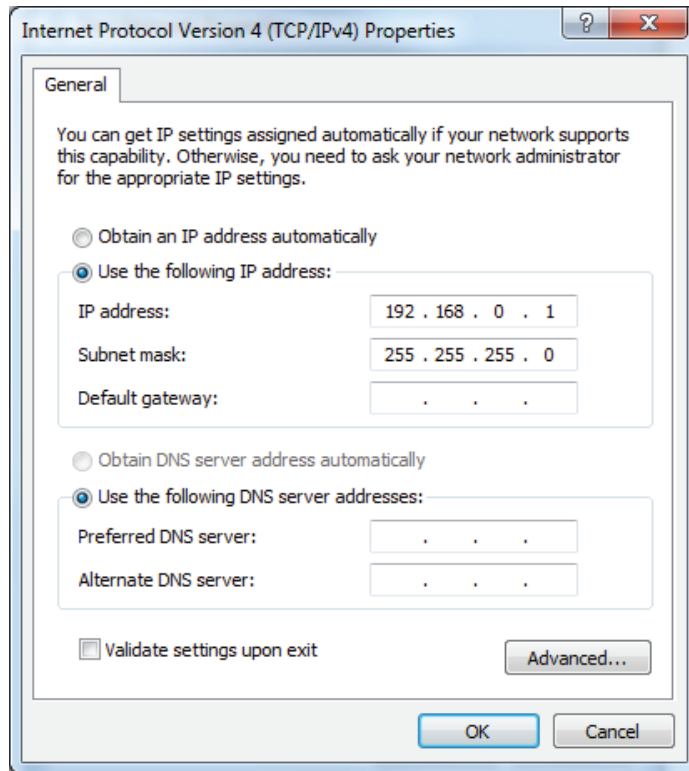


Figure 24 TCP/IP Properties

8. Open Internet Explorer and ensure that settings will allow you to connect to the IP address selected. If the PC uses a proxy server, ensure that Internet Explorer will bypass the proxy server for local addresses.
This option may be modified by opening Tools-> Internet Options-> Connections Tab-> LAN Settings->Proxy Server-> bypass proxy for local addresses.
9. Enter the default IP address for the WI-MOD-E:
https://192.168.0.1XX, where "XX" is the last two digits of the serial number.
10. Enter the username "user" and default password "user".

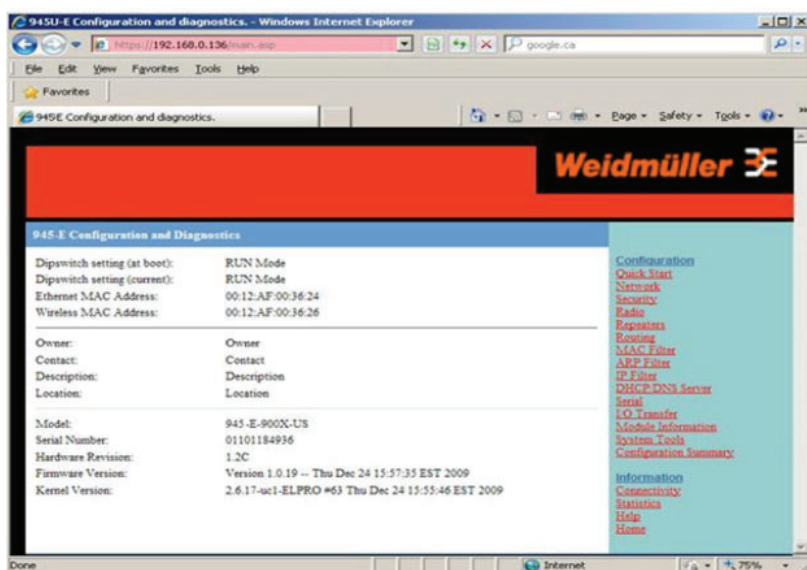


Figure 25 Main Screen

- To resume normal configured operation when configuration is complete, switch the factory default DIP switch on the WI-MOD-E to RUN and cycle power.



NOTE Security Certificates. Configuration of the WI-MOD-E uses an encrypted link (https). The security certificate used by the WI-MOD-E is issued by Weidmuller and matches the IP address 192.168.0.100.

When you first connect to the 245U-E, your Web browser will issue a warning that ELPRO is not a trusted authority. Ignore this warning and proceed to the Configuration webpage. To avoid seeing this warning in the future, you can install the certificate into your browser.

Internet Explorer 7 has an additional address check on security certificates. Unless the 245U-E has the address 192.168.0.100, when you first connect to the 245U-E Internet Explorer 7 will issue a warning about mismatched security certificate address. You can turn off this behavior in IE7 by selecting:

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

Method 2 – Set WI-MOD-E Network Address to Match the Local Network

For this method you will need to determine what IP address, gateway address, and netmask to assign to the WI-MOD-E so that it appears on your network. Ask your system administrator if you do not know the correct settings for your network. The default IP address of the WI-MOD-E modem is 192.168.0.1, and the network you wish to connect to is on 10.10.0.X (the PC is on 10.10.0.5).

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

- Open HyperTerminal and monitor communications.
- Set the SETUP/RUN switch to the SETUP position, and connect power to the modem.
- Observe HyperTerminal and when you see the Weidmuller Dragon screen (see below) press Enter to get the following prompt "#."
- Type the following "ifconfig" command to show the configuration of the Ethernet port. From this you will see what the IP address is.



Figure 26 Dragon

For example:

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

5. Temporarily change the IP address to one that will enable connection to your local network.
For example, type “ifconfig eth0 10.10.0.6 netmask 255.255.255.0.” Only add the netmask if the netmask is anything other than the standard 255.255.255.0
6. Verify that the IP address is changed by typing “ifconfig” again.
Note that these changes are only temporary, and if the module is reset the IP address will return to the normal default (192.168.0.XXX).
7. Open Internet Explorer and ensure that settings will allow you to connect to the IP address selected. If the PC uses a proxy server, ensure that Internet Explorer will bypass the proxy server for local addresses.
This option may be modified by opening Tools-> Internet Options-> Connections Tab-> LAN Settings->Proxy Server-> bypass proxy for local addresses.
8. Enter the IP address for the WI-MOD-E into the Internet Explorer address bar.
For example, if you changed the temporary address in step 5 to “10.10.0.6,” you would enter http://10.10.0.6.
Enter the username “user” and default password “user”.
You should now be connected to the main index page on the modem.
9. Connect to the Network page and change the Ethernet interface and Wireless interface IP addresses to

10.10.0.6.

10. Switch the RUN/SETUP switch back to RUN and click Save Changes and Reset.



NOTE Because the modem can be setup in various ways (such as a bridge or router) this setup will allow the modem to appear on the 10.10.0.X network. Any other configuration changes can be made after this initial connection (see the following sections on configuration).

3.3 Quick Start Configuration

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

Device Mode:	
Operating Mode	Access Point
Default Gateway	192.168.0.1
IP Address	192.168.0.100
Subnet Mask	255.255.255.0
System Address (ESSID)	VLANTest
Radio Encryption	None
WPA Passphrase	WiReLeSs TeChNoLoGy 2010

Figure 27 Quick Start

Quick Start Configuration:

1. Select Quick Start from the Main Menu and select the following parameters:
 - **Operating Mode**—Access Point or Client. Bridge operation is assumed. For router selection, go to the Network page after Quick Start
 - **Default Gateway**—This is the address that the device will use to forward messages to remote hosts that are not connected to any of the local bridged networks (Ethernet or Wireless).
 - **IP Address / Subnet Mask**—IP address and subnet mask for your application.
 - **System Address (ESSID)**—The system address is a text string 1 to 31 characters long used to identify your system.
 - **Radio Encryption**—Radio encryption selection (None, WPA-PSK (TKIP), WPA-PSK (AES) or WPA2). Refer to “3.7 Security Menu” if WEP or enterprise encryption is required.
 - **WPA Passphrase**—128-bit encryption keys are internally generated based on the passphrase and system address (ESSID). The passphrase must be between 8 and 63 characters long, and must be the same for all WI-MOD-E units in the same system.

The default settings will be shown. If your system is connecting individual devices that are not connected to an existing Ethernet LAN, you can use the factory default IP values. If you are connecting to an existing LAN, you need to change the IP addresses to match your LAN addresses.

2. After configuring, click Save to Flash and Reset.

Radio Data Rate and Channel will be set to Auto, Radio Transmit Power will be set to maximum and any previous configuration of unrelated parameters will not be modified and will still apply.

3.4 Network Configuration

You can view or modify Ethernet network parameters by selecting the Network menu. When prompted for the username and password, enter “user” as the username, and “user” as the password. This is the factory default setting. To change the default username and password, see “3.24 Module Information.” If you have forgotten the IP address or password, the factory default switch may be used to access the existing configuration. Refer to previous section for more information.

The screenshot displays a web-based configuration interface for a network device. It is organized into three main sections: **Wireless Interface:**, **Radio Settings:**, and **Network Settings:**. Each section contains various configuration fields, many of which are dropdown menus or checkboxes. At the bottom of the form, there are two buttons: "Save Changes" and "Save Changes and Reset".

Section	Parameter	Value
Wireless Interface:	Operating Mode	Access Point
	System Address (ESSID)	Network1
	Desired BSSID	00:00:00:00:00:00
	Radio Encryption	None
Radio Settings:	Region	US
	Transmit Power Level	26 dBm (398 mW)
	Channel (AP Only)	Auto
Network Settings:	Device Mode	Bridge
	Bridge STP	<input type="checkbox"/>
	Obtain IP Address Automatically	<input type="checkbox"/>
	IP Address	192.168.17.10
	Subnet Mask	255.255.255.0
	Default Gateway	192.168.17.10
	Buttons	Save Changes Save Changes and Reset

Figure 28 Network

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

Default configuration of the module will be “Client” and “Bridge.” When in Bridged mode, the module’s wired and wireless IP address will be the same, meaning only one IP address is required. If the device mode is changed to “Router,” the page will display two IP addresses, one for Ethernet and one for wireless. For more information on bridging networks see “3.18 Routing.”

If the module has been configured for VLAN, the page will show the device mode as “VLAN Bridge” and the Ethernet IP and netmask will no longer be editable. See “3.23 VLAN” for details on VLAN configuration.

A system of WI-MOD-ES must have at least one access point (configured as a master) and have one or more clients. All WI-MOD-ES must have the same system address (ESSID). For further information and examples on wireless network topologies refer to “1.0 Network Topology.”

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

encryption keys.

The available encryption methods are as follows:

- WEP (Wired Equivalent Privacy) encryption is the weakest encryption method, defined by the original IEEE802.11 standard and uses a 40-bit or 104-bit key with a 24-bit initialization vector to give a 64-bit and 128-bit WEP encryption level. WEP is not considered an effective security scheme, and should only be used if it is necessary to inter-operate with other equipment which does not support more modern encryption methods.
- WPA (Wi-Fi Protected Access) is a subset of the IEEE802.11i Security Enhancements specification.
- WPA2 (Wi-Fi Protected Access 2) replaced WPA and provides significant security improvements over this method. In particular, it introduces CCMP, a new AES-based encryption mode with strong security.
- WPA/WPA2-PSK (Legacy Support) enables the modem to communicate to all WPA methods including TKIP, AES and WPA2 AES. Generally only used if the network has older devices that does not support the higher level encryption methods. Enabling this option will lower the security level of the network down to the weakest configured encryption level (WPA TKIP).
- WPA-Enterprise (802.1x) removes the need to manage the pre-shared key (PSK) by using an external server to provide client authentication. Clients that are not authorized will be prevented from accessing the network. Once a client has provided the correct authentication credentials, access is permitted and data encryption keys are established, similar to WPA-PSK. Fine-grain (user level) access control can be achieved using this method.

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

In a typical WPA-enterprise setup, the WI-MOD-E access point acts as Authenticator, controlling access to the network. Wireless clients (245U-Es, laptops or other devices) act as Supplicants, requesting access to the network. The Authenticator communicates with an authentication (RADIUS) server on the Ethernet network to verify Supplicant identity. When a Supplicant requests access, it sends an access request to the Authenticator, which passes an authentication request to the external authentication server. When the user credentials of the Supplicant are verified, the Authenticator enables network access for the Supplicant, data encryption keys are established and network traffic can pass.

Configuration of WPA-enterprise differs when the unit is configured as an access point (Authenticator) or client (Supplicant). If WDS interfaces are used, it is possible for one WI-MOD-E to act as both an Authenticator and a Supplicant, but in this situation only one set of user credentials can be entered for all Supplicants.

The WI-MOD-E supports WPA-1 TKIP, WPA-1 AES and WPA-2 AES using a pre-shared key (PSK).

- WPA PSK (TKIP) (Temporal Key Integrity Protocol) enhances WEP by using 128-bit encryption plus separate 64-bit TX and RX MIC (message integrity check) keys.
- WPA PSK (AES) (Advanced Encryption Standard) uses the more advanced CCMP encryption protocol and is essentially a draft of the IEEE 802.11i wireless network standard. This is the recommended encryption method in most applications.
- WPA2 AES (Advanced Encryption Standard) is the most secure encryption method and is also based on 128-bit encryption key.

After changes are made to Network Configuration, it is important to save the configuration by clicking Save Changes or by selecting Save Changes and Reset.

Network Settings Webpage Fields

Operating Mode	Used to select Access Point (Infrastructure), Client (Infrastructure). By default this is set to Client.
System Address (ESSID)	A WI-MOD-E network comprises modules with the same system address. Only modules with the same system address will communicate with each other. The system address is a text string 1 to 31 characters long. Select a text string which identifies your system.
Desired BSSID	To force a client/station to always connect to the same access point, enter the MAC address of that access point in the Desired BSSID field. Note that the ESSID of the access point must also match the configured ESSID of the client.
Radio Encryption	Select the desired radio encryption level. The encryption key, passphrase and other security information is entered on the Security menu. See “3.7 Security Menu” for details.
Region	Select from the list of regions, Global, AU, EU, NZ & US. Changing the Region will reload the allowable Transmit Power and Channel settings for this radio. Failure to correctly set the region on this product may breach local regulations, if unsure set the region to Global.
Transmit Power Level	This allows adjustment of the radio power. Do not set the radio power above the allowed setting for your country. You can reduce the power for short range applications or to allow the use of high gain transmitter antennas while still complying with the emission requirements of your country
Channel (AP Only)	The WI-MOD-E-G1 radio channels 1 to 13 (depending on country) may be configured at the access point. See “3.1 Selecting a Channel.” The WI-MOD-E-A1 radio channels can be individually set (access point only; client ignores the selection), or left on Auto (default). Select the appropriate U-NII groups (1, 2, 3, or 4), each having its own group of channels, maximum power, and DFS selection. The default radio channel for both A and G models is Auto. When set to Auto, on startup the module will scan all available and selected channel groups (country dependent) and pick the quietest channel.
Device Mode	Used to select Bridge or Router mode. By default this is set to Bridge. If VLAN is enabled, the Device Mode will indicate “VLAN” and the IP address and netmask will only be editable from the VLAN page.
Bridge STP	Checking this box enables Spanning Tree Protocol in bridged networks. See “3.5 Spanning Tree Algorithm” for details.
Obtain IP Address Automatically	Selecting this option enables DHCP client on the WI-MOD-E. A DHCP client requests its IP address from a DHCP server which assigns the IP address automatically. For more information, see “3.21 DHCP Server Configuration.” By default this option is not selected.

IP Address	Bridge Mode—The IP address of the WI-MOD-E module. Both wired (Ethernet Interface) port and wireless (Wireless Interface) ports will take on this address.
	Router Mode—Separate IP addresses are required for each interface. IP addresses must be different.
IP Subnet Mask	The IP network mask of the WI-MOD-E module. This should be set to the appropriate subnet mask for your system (typically, 255.255.255.0). In Router mode, each interface will have its own netmask.
Default Gateway	This is the address that the device will use to forward messages to remote hosts that are not connected to any of the local bridged networks (Ethernet or Wireless). This is only required if the wired LAN has a gateway unit that connects to devices beyond the LAN (for example, Internet access). If there is no gateway on the LAN, set this to the same address as the access point (the Ethernet IP address below).
Save Changes	Refer to “3.18 Routing” for more information. Save changes to non-volatile memory. The module will need to be restarted before the changes take effect.
Save Changes and Reset	Save settings to non-volatile memory and reboot the WI-MOD-E. Once the module has completed the reboot sequence, all changes are in effect.

3.5 Spanning Tree Algorithm

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

For example, consider the network below (Figure 29) with a redundant wireless link. If the bridge Spanning Tree Protocol is enabled, one of the two wireless links will be disabled and all wireless data will be transferred by one link only. If the active link fails, the other link will automatically start transferring the wireless data. The Spanning Tree Protocol implemented is IEEE 802.1d compatible. The algorithm forms a loop-free network by blocking traffic between redundant links in the network. These blocked links are placed in a standby condition and may be automatically enabled to repair the network if another link is lost.

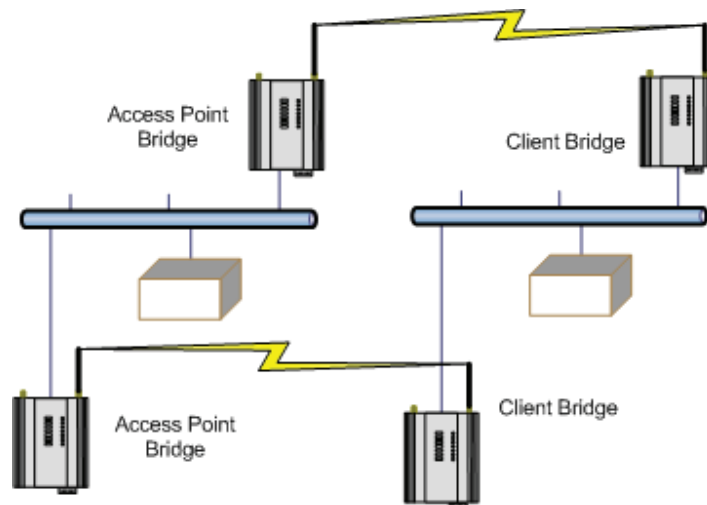


Figure 29 Spanning Tree Protocol

The Spanning Tree Algorithm maintains a single path between all nodes in a network by forming a tree-like structure. The bridge priority determines where the node sits in the tree. A bridge configured with the lowest priority (0) will become the root node in the network, and will direct traffic between each of its branches. The root node is typically the unit that handles the majority of traffic in the network. By default, the WI-MOD-E is configured with a bridge priority of 32768. The intention is to reduce traffic that the WI-MOD-E must handle by placing it at the branch level in the network tree. As a branch, the WI-MOD-E need only pass traffic to devices that are its leaf nodes.

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

3.6 Compatibility

3 Address Mode and 4 Address Mode

Addresses in a Wireless Ethernet Data Frame

There are two Wi-Fi communication modes—3 Address mode (Layer 3 Bridge) and 4 Address mode. The modes have a slightly different way of addressing the data frames to other devices on the network. In 3 Address mode, the addressing is made up of a destination address (DA), a source address (SA), and a BSSID (MAC address of the access point). In 4 Address mode, the addressing is made of a destination address (DA), a source address (SA), a radio transmit address (RTA), and a radio receive address (RRA).

Packets Between Access Point and Client

Communications between access points and client generally uses 3 Address mode because there are only three addresses within the communication path, as indicated in the path from the laptop to Station #1 in Figure 30. If the laptop wishes to communicate to Station #1, the DA will be Station #1, the SA will be the laptop, and the BSSID will be the access point's MAC address—therefore, 3 Address mode is used.

The example in Figure 30 shows that the laptop may need to communicate to the Ethernet device connected to Station #2. You can see that there is now a fourth address (laptop, access point, Station #2, and Ethernet device) that cannot be addressed using the 3 Address mode of communications. The example

shows the access point and the station as both being WI-MOD-E modules that will communicate, since both support 4 Address mode. However, there are some instances where a third party access point may not be able to communicate using 4 Address mode to a client (Sta).

There are only a couple of ways around this situation. You could change Station #2 to a router, but this may mean that Station #2 and the Ethernet device will use a different network address scheme, which may be inconvenient and will require more setup. You could configure the access point to communicate using 4 Address Mode, but this is only possible if the station and the access point support 4 Address Mode (some third party access points do not support this mode).

WI-MOD-E-300 / 100 Compatibility

The WI-MOD-E-G1 modules can communicate with Weidmuller WI-MOD-E-300 or 100 Ethernet modems, but only in certain modes. The following table shows compatible configurations. If communicating with Weidmuller WI-MOD-E-300 or 100 Ethernet modems, the WI-MOD-E-300 or 100's need to be configured with WDS (4 Address mode), not the default 3 Address mode, and the WI-MOD-E-300 or 100 access points cannot be auto-connect to any WDS access points.

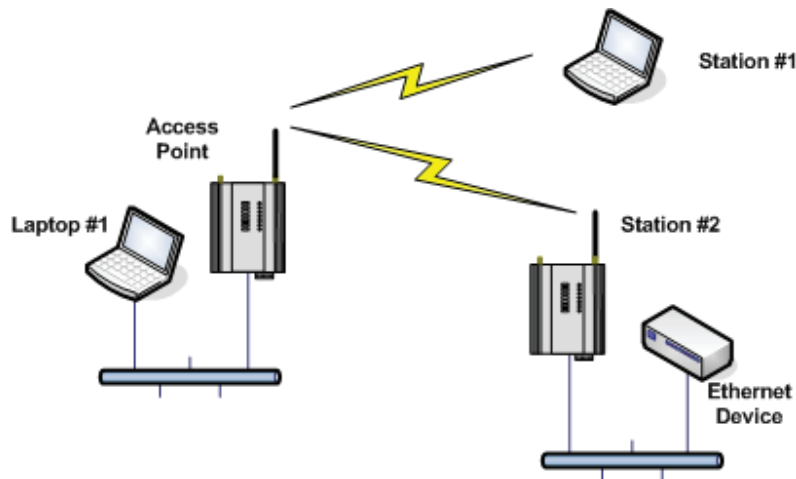


Figure 30 Compatibility

	WI-MOD-E-G1 AP	WI-MOD-E-G1 Sta	WI-MOD-E-300/ 100 AP (4Add)	WI-MOD-E-300/ 100 CL(4Add)	WI-MOD-E-300/ 100 AP(3Add)	WI-MOD-E-300/ 100 CL (3Add)
WI-MOD-E-G1 AP	Y	Y	Y ⁽¹⁾	Y	N	Y
WI-MOD-E-G1 Sta	Y	Y	Y	N/A	N ⁽²⁾	N/A

NOTES

- 1 Connection only if the WI-MOD-E-G1 is configured with a virtual station (client) which in turn connects to the WI-MOD-E-300/100 access point.
- 2 Connection indication in the Connectivity pages, but it is not a true connection (see “3 Address Mode and 4 Mode above).

3.7 Security Menu

Select the Radio encryption level from the drop down menu on the main index page, and then click Save Changes. Available encryption levels are None, WEP (64-bit), WEP (128-bit), WPA PSK (TKIP), WPA PSK (AES), WPA2 PSK (AES), WPA PSK/WPA2 PSK (Legacy), and WPA-Enterprise. The default setting is “None.”

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

(WPA).

The screenshot shows the 'Wireless Interface' configuration section. It includes the following fields and options:

- Operating Mode:** Access Point (dropdown menu)
- System Address (ESSID):** Network1 (text input)
- Desired BSSID:** 00:00:00:00:00:00 (text input)
- Radio Encryption:** WPA2-PSK(AES) (dropdown menu) with a link to 'Configure Encryption Settings on Security Page'

Figure 31 Security Menu

WEP (64-bit and 128-bit

Encryption Keys 1 to 4

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

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

The screenshot shows the 'WEP Configuration' section with the following settings:

- Authentication Mode:** Open (dropdown menu)
- Default WEP Key:** 2 (dropdown menu)
- WEP Key 1:** 01:0D:12:1E:23:01:0D:12:1E:23:01:02:03
- WEP Key 2:** 02:0E:13:1F:24:02:0E:13:1F:24:01:02:03
- WEP Key 3:** 03:0F:14:19:25:03:0F:14:19:25:01:02:03
- WEP Key 4:** 04:09:15:1A:26:04:09:15:1A:26:01:02:03

Buttons at the bottom: Save Changes, Save Changes and Reset

Figure 32 WEP

Default WEP Key

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

Open or Shared Authentication Mode

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

WEP Open Authentication Mode

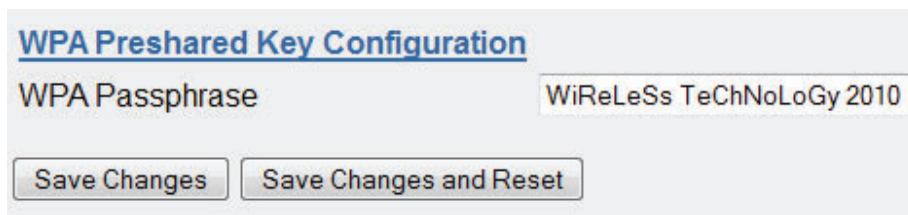
- Station sends an authentication request to the access point.
- Access point then authenticates the station.
- Station then associates with the access point and joins the network.

WEP Shares Authentication Mode

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

WPA / WPA2

When WPA encryption is selected, 128-bit encryption keys are internally generated based on the passphrase and system address (ESSID). The passphrase must be between 8 and 63 characters long, and the passphrase must be the same for all WI-MOD-E units in the same system. For optimal security, consider using a passphrase consisting of a combination of letters and numbers (not a simple word or phrase), as well as upper and lowercase. For example, “WiReLeSs TeChNoLoGy 2010.”



The image shows a web-based configuration interface for WPA Preshared Key Configuration. At the top, the title "WPA Preshared Key Configuration" is displayed in blue text. Below the title, there is a label "WPA Passphrase" followed by a text input field containing the passphrase "WiReLeSs TeChNoLoGy 2010". At the bottom of the configuration area, there are two buttons: "Save Changes" and "Save Changes and Reset".

Figure 33 WPA

WPA Enterprise – Authenticator (AP) Configuration

WPA Enterprise - Authenticator Configuration

RADIUS Server IP Address: 192.168.0.75

RADIUS Server Port: 1812

RADIUS Server Shared Secret: secret

Supplicant Reauthenticate Period: 3600 seconds

Enable Debug:

Save Changes Save Changes and Reset

Figure 34 WPA Enterprise Authenticator

- RADIUS Server IP Address/Port/Shared secret** Connection information for the RADIUS authentication server.
- Supplicant Re-authenticate Period** Sets the maximum time at which the Supplicant must re-authenticate. This parameter determines maximum time a client will still have access to the network after its user credentials have been revoked.
- Enable Debug** Must only be used during commissioning and only if requested by Weidmuller technical support. This must be disabled for normal operation.

WPA Enterprise – Supplicant (Client) Configuration

WPA Enterprise - Supplicant Configuration

Username: Username

Password: Password

Enable Debug:

Save Changes Save Changes and Reset

Trusted CA certificate upload

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

Browse...

Send Cancel

Figure 35 WPA Enterprise Supplicant

- Username / Password** User credentials that match a valid user on the RADIUS server.
- Enable Debug** Must only be used during commissioning and only if requested by Weidmuller technical support. This must be disabled for normal operation.

Trusted CA certificate upload	Upload the certificate of the issuer of the RADIUS server's certificate. This enables the Supplicant to verify the identity of the RADIUS server during the authentication process. Supported EAP method is PEAP / MSCHAPv2.
Certificate Verification result	Once a certificate has been loaded, this field will contain validation information for the certificate. If this field is blank or contains errors, the certificate is invalid.
Trusted CA Certificate Contents	Displays the contents of the CA certificate.

3.8 Normal Operation

After addresses are configured the units are ready for operation. Refer to "1.0 Network Topology" for an explanation on the operation of a bridge and router.

Bridge Operation (Transparent Network)

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

A bridge will forward all broadcast traffic between the wired and wireless ports. If the wired network is busy with broadcast traffic, the radio network on the WI-MOD-E can be unnecessarily overburdened. Use filtering to reduce broadcast traffic sent over the radio. Refer to "3.19 Filtering" for information on how to configure a filter.

By default, a transparent bridge does not handle loops within the network. There must be a single path to each device on the network. Loops in the network will cause the same data to be continually passed around that loop. Redundant wireless links may be set up by enabling the bridge Spanning Tree Protocol (see "3.5 Spanning Tree Algorithm" for details).

Router Operation (Routed Network)

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

Because the router has an IP address on each of the networks it joins, it inherently knows the packet identity. If the traffic directed at the router cannot be identified for any of the networks to which it is connected, the router must consult its routing rules as to where to direct the traffic. For details on configuring routing rules, see "3.18 Routing."

3.9 Radio Configuration

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



NOTE This rate is for transmit messages only. The radio can receive on all data rates.

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

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

Radio Settings:

Radio Mode	auto
Transmit Power Level	26 dBm (398 mW)
Channel (AP Only)	Auto
Channel Width (STA and Auto Channel Only)	20 MHz (Only channels with this width are scanned)
Transmit Data Rate	Auto (max is 54 Mbps)
Beacon Interval (AP Only)	100 msec
Max Distance	5000 meters
Disable SSID Broadcast (AP Only)	<input type="checkbox"/>
3 Address Mode (STA Only)	<input type="checkbox"/>

Go to [Advanced Radio Configuration](#)

Figure 36 Radio Configuration


Radio Mode

The WI-MOD-E-G1 supports 802.11b and 802.11g radio standards. To limit operation to one or the other, select the desired standard. Normally, selecting “Auto” allows the modem to make the best choice.

The WI-MOD-E-A1 only supports the 802.11a radio standard.

Transmit Power Level

This allows adjustment of the radio power. Do not set the radio power above the allowed setting for your country. You can reduce the power for short range applications or to allow the use of high gain transmitter antennas while still complying with the emission requirements of your country. See “Appendix C- CHANNELS” for dB to mW conversion.

Channel (AP Only)	<p>The WI-MOD-E-G1 radio channels 1 to 13 (depending on country) may be configured at the access point. See “3.1 Selecting a Channel.”</p> <p>The WI-MOD-E-A1 radio channels can be individually set (access point only; client ignores the selection), or left on Auto (default). Select the appropriate U-NII groups (1, 2, 3, or 4), each having its own group of channels, maximum power, and DFS selection.</p> <p>The default radio channel for both A and G models is Auto. When set to Auto, on startup the module will scan all available and selected channel groups (country dependent) and pick the quietest channel.</p>
Channel Width (STA and Auto Channel Only)	<p>WI-MOD-E-G1 stations only. When configured as a station, the module will periodically scan the channels looking for an access point. This option is used to speed up the access point scanning process of the client radio by only scanning certain channel bands (5 MHz, 10 MHz, and 20 MHz) or automatically scanning all channels. Default is 20 MHz.</p>
Turbo Mode	<p>(Only for fixed channels, No Auto). Selecting Turbo Mode doubles the transmit data rate offered on a single channel. Maximum data rate up to 108 Mbps.</p> <p>Only usable with other Weidmuller WI-MOD-E-A1 and WI-MOD-E-G1 modules configured with the same turbo channel. If using the Turbo mode feature, all modems in the system will need to be configured with Turbo mode and the correct channel in order to communicate.</p>
Transmit Data Rate	<p>The radio baud rate in Mega (million) bits per second (Mbps) for point-to-point radio transmissions. The default value is Auto. Select a fixed rate to force the radio to use the selected rate.</p> <p>Fixing the TX Rate is not recommended except for advanced users.</p> <p> NOTE Increasing the transmit data rate will decrease the transmit power level. For example, selecting a 54-Mbps fixed data rate will reduce the transmit power from 400 mW down to 125 mW. This is to comply with 802.11 regulations.</p>
Beacon Interval (AP only)	<p>This interval is the period between beacon transmissions sent by an access point. The default value is 100 milliseconds, and it may be adjusted from 50 to 4095 milliseconds.</p>
Max Distance	<p>Configure the maximum distance the radio signal is expected to travel. This allows the modem to compensate for the flight time of messages as they pass from the transmitter to the receiver, and as the acknowledgment messages are returned. Setting this value larger will cause a small reduction in throughput. Setting this value too small will cause communications problems over longer distances. Default distance is 5 km.</p>

- Disable SSID broadcast (AP only)** This should be used to prevent unwanted eavesdroppers from detecting the radio network system address (SSID) by passively listening to beacon transmissions from the access point. When disabled, access points will not transmit the system address openly in beacon messages. This is particularly useful in unencrypted radio networks.
- 3 Address Mode** Allows compatibility with Layer 3 Bridge devices. See “3.6 Compatibility.”
- Save Changes** Save changes to non-volatile memory. Changes will not take effect until module is reset.
- Save Changes and Reset** Save changes to non-volatile memory and reset module.

Channel Selection

WI-MOD-E-G1 Modem (2.4 GHz 802.11b/g)

Selection is made by picking one of the channels from the drop-down channel list. If Auto is selected the modem will select the best channel based on signal level and channel density. Channel can also be manually selected by picking the channel number from the list. Available channels 1-11 are 20 MHz, channels 41-51 are 10 MHz and channels 21-31 are 5 MHz. Turbo channels can also be selected depending on the country.

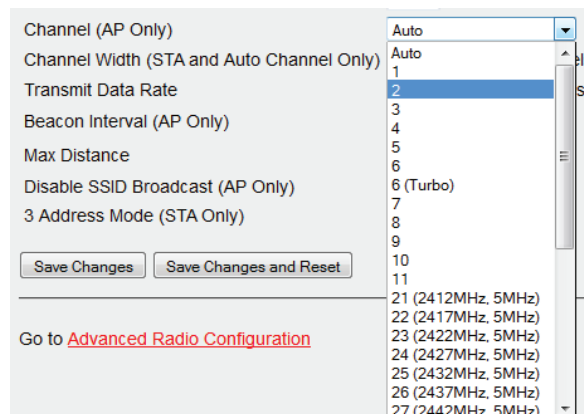



Figure 37 2.4GHz Channel Selection

WI-MOD-E-A1 Modem (5 GHz 802.11a)

You can select an individual channel from the list, keeping in mind that the channel will have some transmit and/or DFS constraints, as indicated in “3.1 Selecting a Channel” and “Appendix C- CHANNELS.” If using the Auto mode, you will need to select the appropriate groups that you wish to use and the modem will automatically select an available channel from within the selected groups.

Channel (AP Only)	Auto	Select the channel group(s) to use for Auto selection below:
Channel Group 1: 5.150-5.250GHz	<input checked="" type="checkbox"/>	(Channels 36,40,44,48)
Channel Group 2: 5.250-5.350GHz	<input type="checkbox"/>	(Channels 52,56,60,64) [DFS]
Channel Group 3: 5.470-5.725GHz	<input type="checkbox"/>	(Channels 100,104,108,112,116,120,124,128,132,136,140) [DFS]
Channel Group 4: 5.725-5.825GHz	<input type="checkbox"/>	(Channels 149,153,157,161,165)

Figure 38 5 GHz Channel Selection

 **NOTE** Some of the groups use Dynamic Frequency Selections (DFS). If using these DFS channels you need to be aware that there will be a minimum 60-second scan or monitoring that the radio must perform to check that there are no military or commercial radars using the same frequency. If a radar is detected, the radio must select another random channel and repeat the 60-second scan or monitoring.

3.10 Advanced Radio Configuration

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

Advanced Radio Settings:

Tx Antenna	Main Port Only
Rx Antenna	Main Port Only
DTIM Period (AP Only)	1 beacon intervals
RTS Threshold	2346 bytes
Fragmentation Threshold	2346 bytes
Interference Mitigation	<input type="checkbox"/>
Bursting	<input type="checkbox"/>
Enable Iperf Server	<input type="checkbox"/>
Fixed Noise Floor	0 dBm (Set to 0 for Dynamic Adjustment)

Figure 39 Advanced Radio

**TX Antenna (Note:
Not used on WI-MOD-
E-A1 or WI-MOD-E-G1)**

Select the antenna port that the module will use for transmissions:

Main Port Only—Messages are transmitted from the main TX/RX port. The auxiliary port RX is disabled.

Both (Diversity)—Both ports will be used to transmit, but not at the same time. The module calculates the best port based on previous transmissions and MAC addressing.



NOTE Broadcast / UDP transmission messages will initially toggle between the antenna ports, and could result in every second message not being heard until the module learns which device can be reached through which antenna port.

Aux Port Only—Messages will be transmitted via the auxiliary RX port only.

**RX Antenna (Note:
Not used on WI-MOD-
E-A1)**

Same as for TX antenna above, but for the receiver port. Setting to “Both (Diversity)” will allow a high gain antenna to be connected to the auxiliary RX port, which will give better RX signal gain without increasing the TX gain and possibly pushing it over the regulatory EIRP threshold.

DTIM Period)

(Access point only.) DTIM sets which beacon frames incorporate extra information for low power sleeping client devices. Normally set this to 1.

RTS Threshold

Ready To Send threshold. RTS frames can be used to help avoid radio collisions between two stations that cannot directly hear each other. Any frame larger than the RTS threshold bytes will be preceded by an RTS message. The default value of RTS threshold is 2346, which effectively disables RTS signaling, since this value is larger than the maximum frame size (fragmentation threshold).

**Fragmentation
Threshold**

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

Interference Mitigation

(Access point only.) Interference Mitigation should only be turn on (default is off) if using demo whip antennas or if there is a high level of background interference.

By enabling this option, the radio will dynamically adjust the radio parameters to help mitigate interference based on any background interference. It will reduce the receiver sensitivity and therefore should only be enabled on paths with a high fade margin and good signal quality.

Bursting	Selecting this option can increase the data throughput by reducing the overheads associated with wireless transmissions. If communicating with a device that does not support bursting, the modem will drop back to non-bursting mode.
Enable Iperf Server	Enable Iperf server function in the modem. Iperf is used for performing radio surveys or radio path testing. See “4.4 Throughput Test.”
Fixed Noise Floor	Allows the radio receiver noise floor (and therefore sensitivity) to be moved above any interference. This essentially stops the radio from communicating with devices that have lower signal strength. For use in areas where there is a greater amount of interference.

Fixed Noise Floor

Due to the popularity of the 2.4 GHz band, there are many sources of interference. This interference can sometimes be a problem due to the way 802.11 devices communicate. Standard 802.11 communications uses a system called “clear channel assessment” which means the radio will listen before transmission and if the channel is busy it will hold off regardless of the level of signal. If the background interference is high due to other radio systems or noise, you can raise the fixed noise floor to compensate. The Channel Utilization page can be used to identify excess noise or interference.

Raising the noise floor will block out any receive signal levels below the value configured under “Fixed Noise Floor” on the Advanced Radio configuration page. The value must be entered as a negative dBm number and should be at least 8 dB greater than the weakest RSSI of any connected modems, otherwise communications may be lost. For example, if the interfering noise levels are around -80 dB, you can raise the noise floor to -70 dB to block out any signals below, making sure the RSSI levels of any connected modules are not below this noise floor as they will not communicate. The Connectivity page can be used to determine if other systems are in the area and their RSSI levels.

After configuring the fixed noise floor, confirm that the channel utilization has dropped to a desirable level and where possible perform an Iperf throughput test to confirm acceptable performance.

3.11 Serial Port Configuration

The WI-MOD-E has an RS-232 and an RS-485 port for serial communications. These ports may be used for different purposes. The WI-MOD-E offers three serial functions—PPP server, serial gateway, and Modbus TCP to RTU gateway.

RS-232 PPP Server

The WI-MOD-E can be used as a PPP (Point-to-Point Protocol) server to connect the wireless system to serial devices via the RS232 or RS485 serial ports. PPP server enables a network connection to the WI-MOD-E over a serial cable. This is much like dial-up Internet. The maximum serial data rate is 115,200 bps. Hardware or software flow control may be selected. With minimal configuration on the PC, you may use dial-up networking in Windows XP to connect to the network via the serial port.

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

- If you want to use routing over this serial network connection, the IP addresses selected must not lie on wireless or wired Ethernet networks already configured into the device. You must ensure they set

routing rules appropriately for devices either side of the network.

- If you want the serial device visible as present on the wireless or wired network, the local IP address must be the same as the IP address set for the desired port. A process called “proxy ARP” is used to make the device visible on the network. In this process, the WI-MOD-E pretends that it holds the IP address on the network, and responds on behalf of the remote device.

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

To configure Windows XP to establish a PPP connection to a WI-MOD-E in SETUP mode:

1. On Network Connections in Windows XP, select “Create a new connection.”
2. In the New Connection Wizard, click Next.
3. Set up an advanced connection.
4. Connect directly to another computer.
5. Set PC as guest.
6. Set the Connection Name.
7. Select a COM port.
8. Select availability.
9. Click Finish.
10. Select properties of this new connection by right-clicking the connection.
11. On the General tab click Configure.
12. Ensure that the maximum speed is 115200 bps, and click OK.
13. Select the Networking tab, and then click Internet Protocol (TCP/IP) in the list box and click Properties.
14. On Properties, click Advanced.
15. On the Advanced TCP/IP Settings, General tab, clear the field in the PPP link “Use IP header compression.”
Configuration is now complete.
16. Click the newly created link to establish a connection to WI-MOD-E.
17. Ensure that the username and the password are entered exactly as configured in WI-MOD-E.

When booted in SETUP mode, the PPP server has username “user” and the password “user.”

Serial Gateway (Server/Client/Multicast)

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

The serial gateway can be configured as either as server, client, multicast group, or Modbus.

- Server—When configured as server, the module will wait for a TCP connection to be initiated by a remote client.
- Client—When configured as client, the module will automatically attempt to connect to a specified remote server using TCP.
- Multicast Group—When configured as multicast group, the module will broadcast data to all members of the same multicast group using UDP.

With the serial gateway server, client, and multicast functions it is possible for serial data from a WI-MOD-E to be transferred to any other WI-MOD-E serial ports including the corresponding port on the same WI-MOD-E.

Serial Gateway (Modbus RTU to TCP)

When configured as Modbus, the module will allow a serial Modbus client (master) to connect with a single Ethernet Modbus TCP server (slave). With the Modbus function, the serial data is encapsulated within a TCP/IP data frame and made available on the Ethernet network. Both WI-MOD-E serial ports and the hard wired Ethernet port can be configured to communicate completely separate data streams that can all be communicating at the same time.

Some of the possible serial gateway topologies are shown in Figure 40.

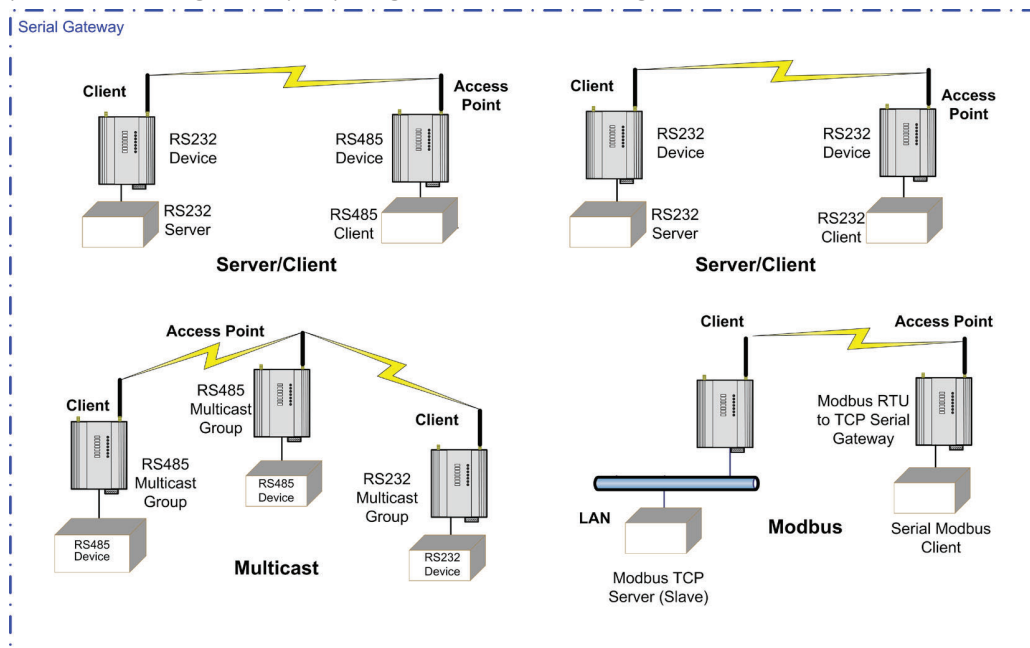


Figure 40 Serial Gateway

There are software packages available (such as SerialIP Redirector by Tactical Software) that can create a virtual serial port on a PC. This virtual serial port can be configured to connect to a WI-MOD-E serial port. Standard programs can then be used to access this serial port as if it were actually connected to the PC. Alternatively, HyperTerminal may be used to connect to a serial port on the WI-MOD-E. When creating the HyperTerminal connection, select “Connect Using: TCP IP (Winsock),” enter the IP address of the WI-MOD-E and the port selected in the “Network port” field.

Modbus TCP to RTU Gateway

The Modbus TCP to RTU gateway allows an Ethernet Modbus/TCP client (master) to communicate with a serial Modbus RTU slave. The WI-MOD-E makes this possible by internally performing the necessary protocol conversion. The conversion is always performed by the WI-MOD-E which is directly connected to the Modbus serial device, only this module needs to have Modbus TCP to RTU gateway enabled.

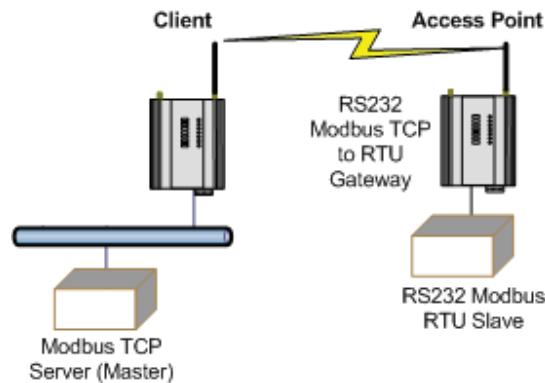


Figure 41 Modbus/TCP Client to Modbus RTU Slaves

The above example demonstrates how a Modbus/TCP client (master) can connect to one or more Modbus RTU (serial) slaves. In this example, the WI-MOD-E access point is configured with the “RS232 Modbus/TCP to RTU Gateway” enabled. Once enabled, the gateway converts the Modbus/TCP queries received from the master into Modbus RTU queries and forwards these over the RS232 port to the slave. When the serial response to the query arrives from the slave, it is converted to a Modbus/TCP response and forwarded via the network to the Modbus/TCP master. If no response was received serially by the WI-MOD-E within the configured Response Timeout, the WI-MOD-E will initiate a number of retries specified by the configured Maximum Request Retries.

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

3.12 Serial Menu

RS-232 / RS485 Serial Port Configuration

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

RS232 PPP Server (Only RS232)

Username	User name to enter to access RS-232 PPP server.
Password	Password to access RS-232 PPP server.

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

RS-232 / RS485 Serial Gateway Mode

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

Multicast Group IP Address	Enter a valid Multicast IP Address identifying the group. All group members should use the same Multicast Group IP Address. Valid multicast IP addresses are in the range 224.0.1.0 to 238.255.255.255.
Serial Gateway Mode	Modbus—Allows a serial Modbus client (master) to connect with a single Ethernet Modbus TCP server (slave).
Character Timeout	Enter the maximum delay (in msec) between received serial characters before packet is sent via network.
Packet Size	The number of received bytes that will be buffered before a packet is sent via the network.
Modbus Server Port	Enter the TCP port number of the remote server (the remote port to automatically connect to).
Modbus Server IP Address	Enter the IP Address of the remote server (the remote IP Address to automatically connect to).

RS-232 / RS485 Modbus TCP/RTU Converter

Modbus Server TCP Port	Port number used for the Modbus TCP. Standard port is 502.
Pauses Between Requests	Enter the delay between serial request retries, in milliseconds.
Response Timeout	Enter the serial response timeout, in milliseconds. A serial retry will be sent if a response is not received within this timeout period.
Connection Timeout	Enter the TCP connection timeout in seconds. If no Modbus/TCP data is received within this timeout period, the TCP connection will be dropped. Set this field to zero for no timeout.
Maximum Request Retries	Enter the maximum number of request retries performed serially.
Maximum Connections	Enter the maximum number of simultaneous TCP connections to the server allowed.

3.13 Multicast Pipe Manager

Previously, it has been difficult to connect a single TCP device (such as a SCADA or DCS system) to multiple remote multicast serial devices. Multicast pipe allows this type of connection. An example would be a SCADA system that needs to communicate with multiple remote serial devices. A modem can be placed at each remote location and connected serially to each device. A multicast pipe is configured to communicate with all devices using a multicast address and port, for example, 224.0.1.1:5000. The SCADA then communicates with the remotes using TCP via the IP address of the multicast manager and the port selected in the configuration, for example, 5001.

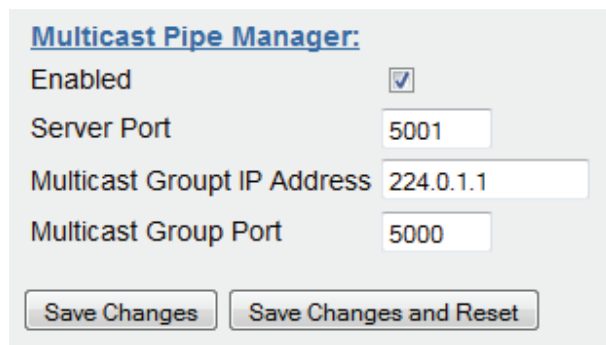


Figure 42 Multicast Pipe

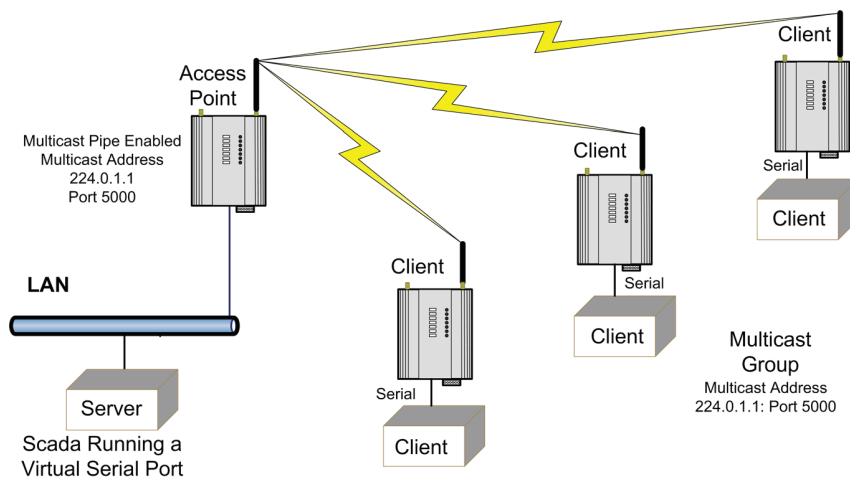


Figure 43 Multicast Group

- Enabled** Enables or disables the multicast pipe manager.
- Server Port** Server port used by the multicast pipe manager. Will need to be configured the same as the port on the client (for example, SCADA or DCS).
- Multicast Group IP Address** Broadcast address used when communicating to all other multicast devices. This address will need to be the same on all communicating multicast devices.
- Multicast Group Port** Multicast port used when communicating to all other multicast devices. This will need to be the same on all communicating multicast devices.

3.14 Digital Input/Output

The functionality of the shared Digital Input/Output pin may be configured via the Transfer webpage. As this pin is shared, the digital input status will be On when the digital output is set to On.

The Digital I/O channel can be transferred to/from another device using Modbus (see “3.15 Modbus I/O Transfer” below) or it can be configured to provide status of the module communications. If the WI-MOD-E disassociates from another unit (that is, there is no wireless link), you can configure the digital output to turn On (set) or Off (drop).

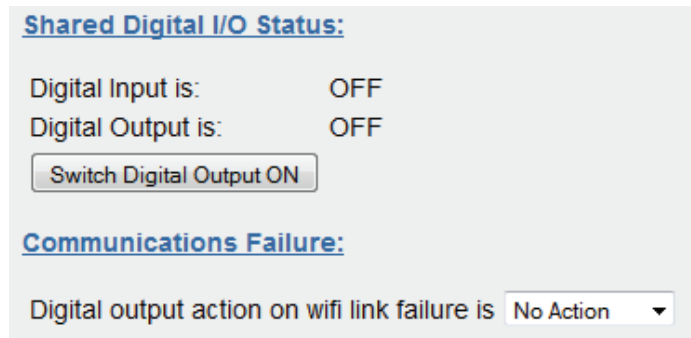


Figure 44 Digital I/O

3.15 Modbus I/O Transfer

The WI-MOD-E provides Modbus TCP client and Modbus TCP server functionality for I/O transfer. The 5000 x 16-bit general purpose registers are provided for Modbus (including the onboard digital input/output) and are shared for both client and server. Modbus TCP client (master) and Modbus TCP server (slave) are both supported simultaneously, and when combined with the built-in Modbus TCP to RTU gateway, the WI-MOD-E can transfer I/O to and from almost any combination of Modbus TCP or RTU devices.

The layout of the WI-MOD-E I/O registers is summarized in the table below. Each register is internally saved as a 16-bit unsigned integer value. A Modbus transaction may access the entire 16-bit value of any register. Alternatively, the most significant bit of a register may be accessed as a discrete value. The main use for the general purpose I/O registers is for intermediate storage, as when transferring I/O from one Modbus slave device to another. Also provided is the status of the onboard digital I/O, as well as the status of the wireless link. The 16-bit status register contains the value FFFF (hexadecimal) for On and 0000 (hexadecimal) for Off. Inverted status registers are also provided where the registers contain 0000 (hexadecimal) for On and FFFF (hexadecimal) for Off.

Registers	Purpose
1–4299	General purpose I/O registers (read/write).
4300	On-board digital input value (read only).
4301	Link status (read only).
4302	Serial gateway connection status (RS232).
4303	Serial gateway connection status (RS485).
4304	TCP-RTU connection status (RS232).
4305	TCP-RTU connection status (RS485).
4306	TCP-RTU Modbus server connection status.
4307	Multicast pipe connection status.
4310	TCP-RTU number of connections (RS232).

4311	TCP-RTU number of connections (RS485).
4312	TCP-RTU number of connections (Modbus server).
4320	On-board digital output value (read/write).
4370	On-board digital input inverted value (read only).
4371	Link status (read only) inverted.
4372	Serial gateway connection status (RS232) inverted.
4373	Serial gateway connection status (RS485) inverted.
4374	TCP-RTU connection status (RS232) inverted.
4375	TCP-RTU connection status (RS485) inverted.
4376	TCP-RTU Modbus server connection status inverted.
4377	Multicast pipe connection status inverted.
4378–4999	Reserved for future use.

Modbus TCP client (master) enables the WI-MOD-E to connect to one or more Modbus TCP servers (slaves). All Modbus master messages are directed to/from the onboard I/O registers depending on configuration (described below). The Modbus TCP client may also poll Modbus RTU (serial) devices connected to either the local serial port or a remote WI-MOD-E serial port by enabling the Modbus TCP to RTU gateway at the corresponding serial port (see “3.11 Serial Port Configuration”).

Modbus TCP client functionality allows a maximum of 100 mappings to be configured and a maximum of 25 different Modbus TCP servers. Modbus TCP server (slave) enables the WI-MOD-E to accept connections from one or more Modbus TCP clients (masters).

Figure 45 Modbus TCP

All Modbus transactions routed to the onboard Modbus TCP server are directed to and from the onboard general purpose I/O registers. The Modbus TCP server is shared with the Modbus TCP to RTU gateway, so that the Modbus device ID is used to determine if a Modbus transaction is to be routed to the onboard Modbus TCP server or to a Modbus RTU device connected to the serial port. Care should be taken to ensure that all serially connected Modbus devices use a different Modbus device ID (Modbus slave address) to the onboard Modbus TCP server. Up to 32 separate connections to the Modbus TCP server are supported.

Modbus RTU (serial) master functionality is achieved by combining the Modbus TCP client (master) and Modbus TCP to RTU gateway. Simply specify a Modbus TCP client (master) connection to a Modbus TCP server, where the server is the address of any WI-MOD-E with Modbus TCP to RTU gateway enabled. Care

should be taken to ensure that the device ID (Modbus address) of the serial device is different than the device ID of the onboard Modbus TCP server of the WI-MOD-E to which the serial device is connected.

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

The example shown in Figure 46 shows a typical Modbus setup. In this example the status of the onboard digital input at B will be reflected at the onboard digital output at C. Also, eight single-bit registers from Modbus serial device D will be transferred to A.

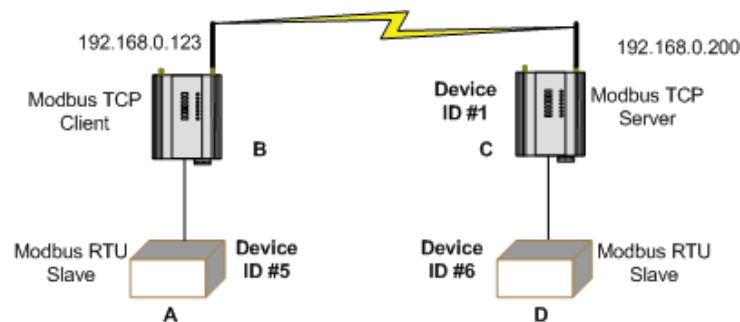


Figure 46 Modbus Setup

Modbus TCP Client Mappings:

Add Entry Delete Entry

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

Figure 47 Modbus Mappings for Unit B

Unit C is configured with Modbus TCP server enabled and device ID set to 1, so that the Modbus TCP client at unit B can connect and read the status of the onboard digital input. Unit C also has the Modbus TCP to RTU gateway enabled (see “RS-232 / RS485 Modbus TCP/RTU Converter”) so that the Modbus TCP client at unit B can communicate with the serial Modbus RTU device D.

Unit B is configured as shown above in Figure 47.

- The first mapping will write the register 4300 (local digital input) to server IP address 192.168.0.200 (Unit C), device ID #1 and register 4320 (digital output).
- The second mapping shows a Modbus read command of 8 discretes, starting at register 1 (Destination Reg) on device ID #6 connected to IP address 192.168.0.200, and storing the values locally at register #1(itself) .
- The third mapping shows the Modbus write command (write coils), which is writing the local 8 I/Os starting at register 1 across to server IP address 192.168.0.123, device ID #5, destination reg #1.

Additional configuration parameters for unit B are shown in Figure 48. The Modbus TCP client has been enabled with a 500 msec scan rate, indicating that there will be a 500-msec delay between each of the

mappings directed at any server. The “Reset Registers on Comms Fail” option is enabled with a timeout of 60 seconds, indicating that any of the registers at unit B will be reset if a successful Modbus transaction involving that register has not been executed in the last 60 seconds.

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

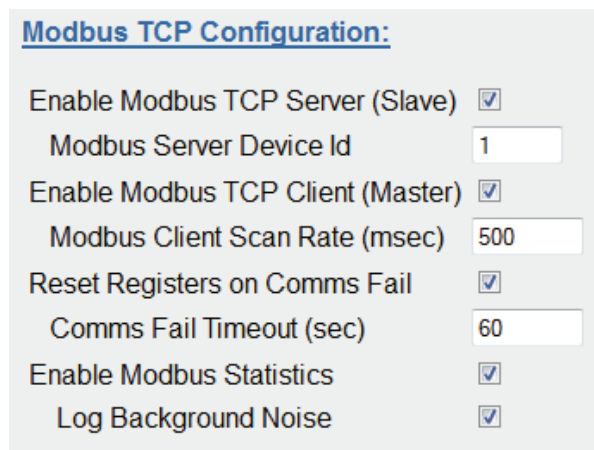


Figure 48 TCP Client Configuration

Modbus TCP Configuration on I/O Transfer Menu

The following table describes the settings shown in Figure 48.

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

Enable Modbus Statistics	Enables the Modbus diagnostic registers, as shown in “4.9 Internal Diagnostics Modbus Registers.” Disabling this option will free up the registers and also slightly increase processing resources.
Log background Noise	RSSI and BGND on RX messages are made available in the diagnostic registers See “4.9 Internal Diagnostics Modbus Registers” for details. For a hexadecimal value of 5F5D, the 5D byte = RSSI and the 5F byte = BGND. Convert the value from hexadecimal to decimal and add a “-” (for example, 5F = -95dB). Disabling this option removes the background noise byte from these registers so that only the RSSI value is made available.

Modbus TCP Client Mappings on I/O Transfer Menu

Local Register	Enter the starting onboard I/O register number that the specified Modbus master transaction will transfer I/O to/from.
I/O Count	Specify the number of consecutive I/O register to be transferred for the specified transaction.
Function Code	Specify the Modbus function code for the transaction.
Destination Register	Enter the starting I/O register number in the destination device that the specified Modbus master transaction will transfer I/O to/from.
Device ID	Enter the Modbus device ID of the destination Modbus device
Server IP Address	Specify the IP address of the destination Modbus TCP server for the specified transaction.
Response Timeout	Enter the timeout (in milliseconds) to wait for a response to the specified transaction.
Comm Fail Register	Enter the onboard I/O register number to store the communication status of the specified transaction. The specified register will be set to 0 if communications is successful, 0xFFFF if there is no connection to the specified server, or 0xFFxx where “xx” is the Modbus exception code

3.16 Roaming

In certain cases a client may be in a mobile situation and require a method of roaming to another access point. Normal network communications provide only basic roaming behavior, which means as the client moves further from the access point it will go through a period of poor communication followed by a complete disconnection of the radio link. It is at this point that the client will scan for access points, and if one is in range it could take up to 10 seconds for the client to establish a connection.

Fast roaming will significantly reduce the time taken for a client to roam from access point to access point. In addition, the discovery of access points is completed before the existing radio link deteriorates, therefore eliminating the periods of poor performance during transition to the next access point.

Roaming Settings (client/station only) :

Fast Roaming

Passive Scanning

Roam Scan Threshold dBm

Roam Changeover Threshold dB

Roam Check Interval seconds

Channel Width (Only channels with this width are scanned)

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

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

Figure 49 Roaming

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

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

When fast roaming is enabled, the client goes off-channel and periodically performs a background scan to identify available access points. When access points are identified, the RSSI is recorded as a potential connection. It takes 50-msec to scan each channel, with a 1-second delay between each scanned channel. Scanning 10 channels will take 10 seconds, during which time latency of up to 50 msec will occur and any throughput traffic is essentially paused and buffered for retransmission when complete. It is therefore

recommended that the scan list be used to limit the number of channels the client needs to scan, thus reducing the overall scan time.

During the background scan, a client will scan all of the channels in the scan list to identify better access points. If no channels are configured it will scan all channels.

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

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

Add Entry Delete Entry

#	Channel
1	1
2	6
3	4

Save Changes Save Changes and Reset

Figure 50 Scan List

The configuration in Figure 50 shows that the client will start scanning when the RSSI of its current connection to the access point falls below -90 dBm. When this happens it will scan the list of access points configured in the roaming scan list (in this case, channels 1, 4 and 6), and if any of the RSSI levels are greater than -84 dBm it will change to this access point.

3.17 Repeaters (WDS)

The range of a wireless network can be extended by allowing access points to behave as repeaters and forward traffic to other access points. Access point to access point communications is also known as wireless distribution system (WDS). The WI-MOD-E offers very powerful WDS configuration, allowing for a mesh network with self-healing functionality. Alternatively, fixed access point to access point links can be configured for optimized throughput.

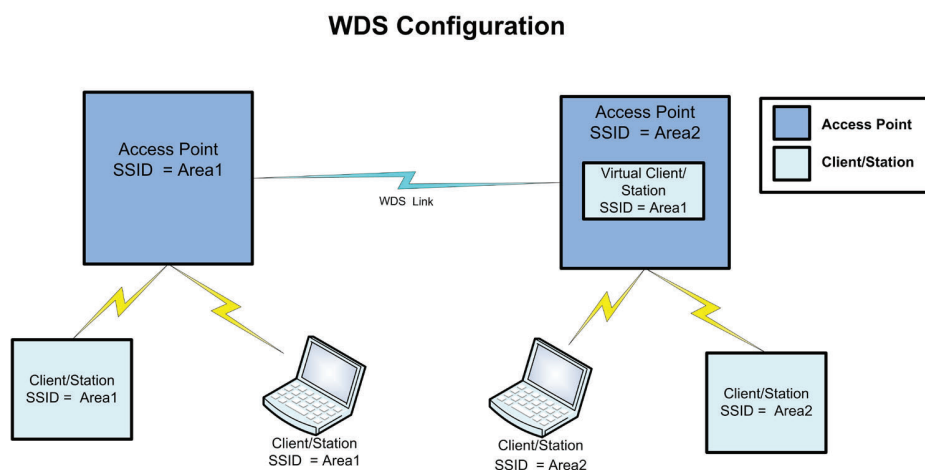


Figure 51 WDS Repeaters

Each WDS interface can be either a bridge or router interface (see “1.0 Network Topology” for more information on bridge versus router). If you need a simple repeater network, use a bridge interface.

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

WDS bridge interfaces have the advantage that redundant paths are permitted when using the bridge Spanning Tree Protocol (see “3.5 Spanning Tree Algorithm”), thus behaving as a self-healing mesh network. Bridged networks are also not as difficult to configure as routed networks because WDS bridge interfaces generally do not require IP address configuration (they inherit the IP address of the standard wireless interface).

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

Important Notes

- All access points must be configured on the same fixed radio channel. Auto Channel Selection must not be selected (see the Radio Configuration page for details on configuring the channel).
- Specify SSID for AP/STA modes or MAC Address for point-to-point mode.
- Router IP and Subnet should be left blank unless that WDS interface is to be on a different subnet. Leaving these fields blank will mean that the WDS interface will be bridged with the default wireless interface.
- Encryption is not inherited from the main page.
- Each WDS interface can also be configured with a different encryption algorithm. However, each side of a single WDS link must specify the same encryption algorithm and keys.
- When adding WDS router interfaces, you may need to add a routing rule on the Routing configuration page.
- When VLANs are enabled, router IP and subnet are ignored and the WDS interface is bridged, depending on membership to a VLAN group.
- Spanning Tree Protocol (STP) column only applies when two or more interfaces are bridged.
- A maximum of 10 WDS connections can be configured. A combined maximum of 5 virtual access points and 5 virtual client/STA applies.
- WPA-Enterprise configuration is shared with the base access point (Authenticator) or station (Supplicant).

WDS connections are made by adding one or more virtual modules to an access point (see Figure 51). Each virtual module can be configured with one of the standard Wi-Fi operating modes (Access Point or Station) or a non-standard point-to-point mode.

- Access point and station virtual modules allow for the possibility of dynamically created connections (based on SSID) and support WPA encryption.

- Point-to-Point mode virtual modules provide static connections (based on MAC addresses), and cannot support WPA encryption. Point-to-point virtual modules should only be used for establishing WDS connections with third party access points that do not support standard WDS operation.

WDS Connections

The WDS Configuration page is accessible from the Repeaters link on any of the configuration webpages. The configurable WDS parameters are summarized below.

Add Entry Button	Add an entry to the WDS connections table. This adds a virtual station to the device.
Delete Entry Button	Delete the currently selected entry in the WDS connections table. To select (highlight) a row, click anywhere in the row.
Connection Mode	Specify the connection mode for this link. AP (downlink) configures the connection as a virtual access point. Sta (uplink) configures the connection as a virtual client. Point-to-point configures the connection as a fixed link.
SSID / MAC Address	AP Mode—Specify the SSID that this virtual access point will use. Stations connecting to this virtual access point use this SSID. Sta Mode—Specify the SSID that this virtual station will use when connecting to other access points. Point-to-Point Mode—Specify the MAC address of an access point with which a fixed link will be established. Usually only required for third-party devices.
Encryption	Select the required encryption (if any) for this WDS link.
Encryption Key	Enter the encryption key (for WEP encryption) or the passphrase (for WPA encryption). For WEP encryption, the encryption key is set as WEP Key 1. For Sta Mode, this must match WEP Key 1 on the access point to which this virtual client is connected. For AP mode, clients must configure their WEP Key 1 to the same value as this key and select the default WEP Key to be WEP Key 1.
Router IP	Leave this field blank if this WDS interface is to be bridged with the default wireless interface. Otherwise, enter the IP address for this connection that specifies the IP network to which messages are routed.
Router Subnet	Leave this field blank if this WDS interface is to be bridged with the default wireless interface. Otherwise enter the subnet mask of the network to which messages are routed.
STP	Applicable to WDS bridged connections only. Select the STP option if you wish to enable the bridge Spanning Tree Protocol on this connection.

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

Example 1: Extending Range Using WDS

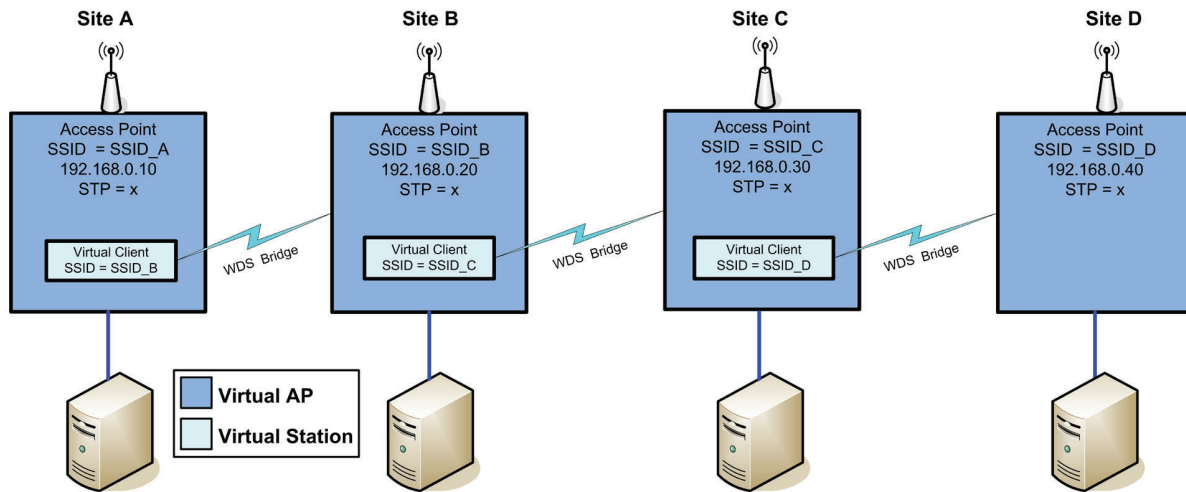


Figure 52 Extending Range

One of the most common uses for WDS is to extend the range of the wireless network using repeaters. Figure 52 illustrates a simple example where the four access points are all at fixed locations (each of the access points could, have one or more client/stations connected). Since the locations are fixed, you can avoid the overhead of using the bridge Spanning Tree protocol by configuring fixed WDS links to ensure that each access point will only connect to the next access point in the chain. Any number of additional intermediate repeaters could be added to the chain in a similar way.

WDS Connections:

Add Entry Delete Entry

#	Connection Mode	SSID / MAC Address	Encryption	Encryption Key	Router IP	Router Subnet	STP
1	Client / Station (Uplink)	SSID_C	WPA2-PSK(AES)	PassPhrase			<input type="checkbox"/>

Figure 53 Site B WDS Configuration 1

The WDS configuration for unit B is shown above (this page is accessible via the repeaters link from the configuration webpages). Site B is acting as an access point for Site A, and is a client to Site C. Likewise, Site C is acting as an access point for Site B, and a client for Site D. Since this example is a bridged network (all devices are on the same IP network and each link is using a different SSID), there is no possibility of loops (multiple paths to the same location) and you do not need to incur the overhead of enabling STP (bridge Spanning Tree Protocol).

You specify the devices at the other end of the WDS links by SSID only. MAC addresses can be used to specify point-to-point links to third party devices that do not support meshing via SSID.

In this example, each virtual connection is using the same encryption method (WPA-PSK (AES) with a key of "Pass Phrase." However, as in example #1, the encryption method and key can be different for each virtual link or even disabled (no encryption). Also the Spanning Tree Protocol is disabled because there is no possibility of network loops.

Example 2: Roaming with WDS Access Points

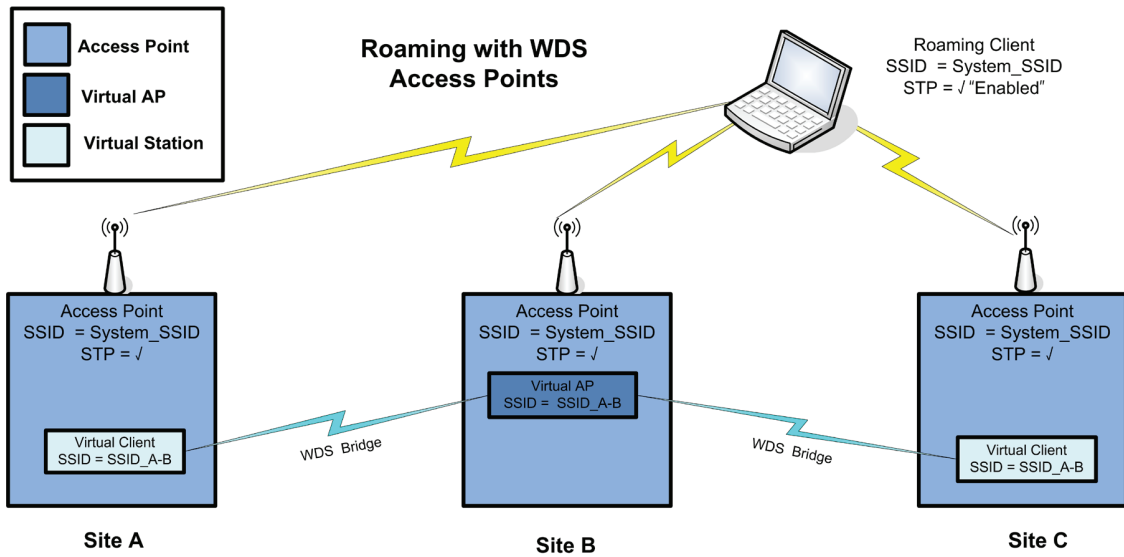


Figure 54 WDS Roaming

Another common use for WDS is extending the range across a large wireless network but allowing roaming connections between access points or being able to switch to the next access point when out of range of the previous access point. Figure 54 shows a bridging network with a number of access points all with the same SSID, and network structure, so the Stations can freely roam between access points.

Each access point then needs a separate connection to the next access point, which is provided using the WDS virtual access points or stations. Site B is acting as a virtual access point for Site A and C, which in turn are acting as virtual Stations. This setup can be replicated to extend the range and will allow any roaming stations full connectivity across a network

WDS Connections:

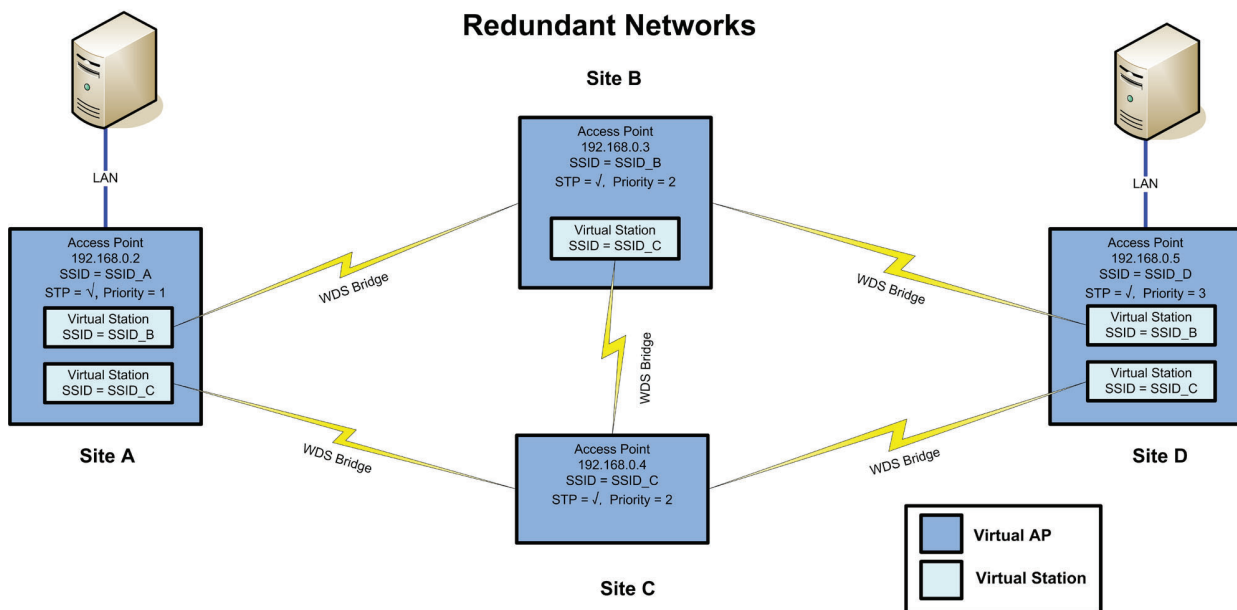
Add Entry Delete Entry

#	Connection Mode	SSID / MAC Address	Encryption	Encryption Key	Router IP	Router Subnet	STP
1	Access Point (Downlink)	SSID_A-B	WPA2-PSK(AES)	PassPhrase			<input checked="" type="checkbox"/>

Figure 55 Site B WDS Configuration 2

Example 3: Adding Redundancy

In the example below, 4 x access points (A, B, C, and D) form a mesh network using only WDS bridge interfaces. Each of the access points may also have its own associated clients. Each access point is configured with a different SSID, which means that the clients associated with each access point are fixed.



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

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

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

In this example, Site B uses its primary access point to act as an access point for virtual stations on Site A and D, and uses a virtual station to act as a client to Site C. Sites A and D use two virtual stations to act as clients to Site B and to Site C. The configuration for Site B and A and D are shown below.

WDS Connections:

#	Connection Mode	SSID / MAC Address	Encryption	Encryption Key	Router IP	Router Subnet	STP
1	Client / Station (Uplink)	SSID_C	WPA2-PSK(AES)	PassPhrase			<input checked="" type="checkbox"/>

Figure 57 Site B WDS Configuration

WDS Connections:

Add Entry Delete Entry

#	Connection Mode	SSID / MAC Address	Encryption	Encryption Key	Router IP	Router Subnet	STP
1	Client / Station (Uplink)	SSID_B	WEP(64 bit)	01:0D:12:1E:23			<input checked="" type="checkbox"/>
2	Client / Station (Uplink)	SSID_C	WPA2-PSK(AES)	PassPhrase			<input checked="" type="checkbox"/>

Figure 58 Site A and D WDS Configuration

Encryption levels and key above are shown as being different, but they can be the same as in some of the earlier examples. One reason why the encryption level and key would be different is that the access point may have clients that communicate using a different encryption method (such as 128-bit WEP) and may not support the same encryption method.

Example 4: WDS Routed Network

Figure 59 is an example of using WDS router interfaces to achieve a similar physical topology to the WDS bridge example provided earlier. In both examples, there are four WDS access points each with the possibility of having their own associated client and stations. In both examples, Sites A, B, C, and D can all exchange data with each other. The bridged example has the advantage of redundancy, but at the expense of extra overhead. The routed example below cannot provide the redundancy of the bridged example, and requires more configuration effort, but does not have the overhead of using the bridge Spanning Tree Protocol, and therefore is suited to fixed installations that do not require redundancy.

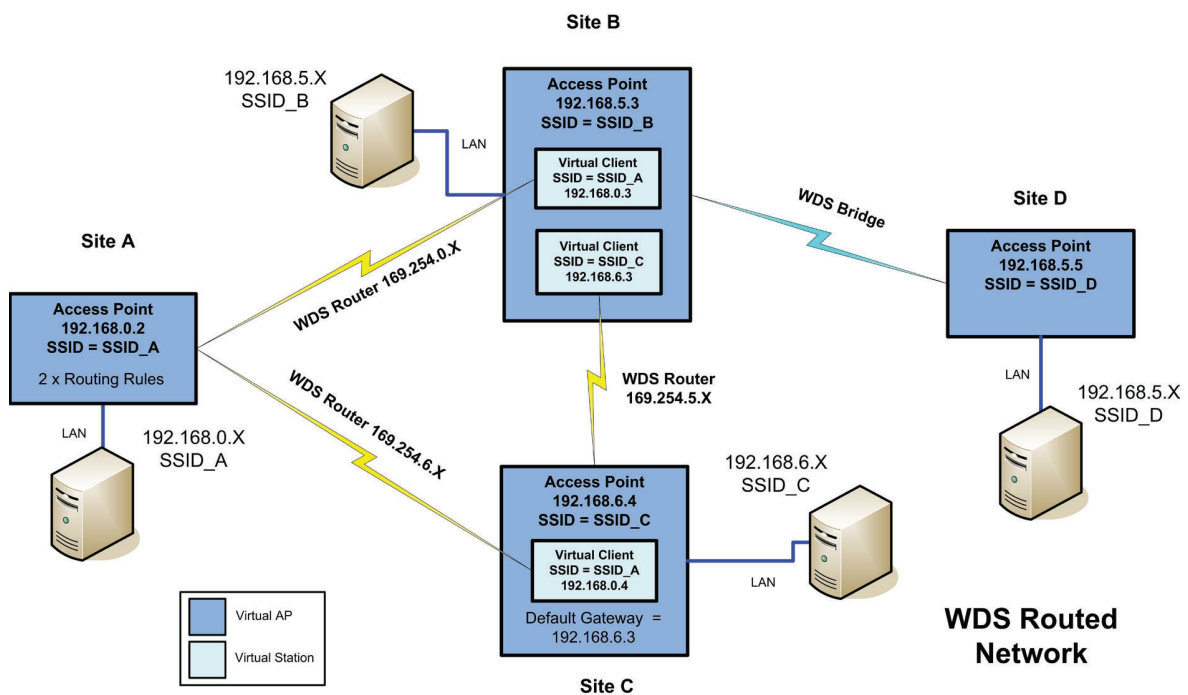


Figure 59 WDS Routed

Each modem has a different SSID. This is done to limit broadcast traffic and to route data only where it needs to go. Site B has two virtual client WDS links configured—one to Site A’s access point, and one to Site C’s access point. Figure 60 shows the WDS connections at Site B.

WDS Connections:

Add Entry Delete Entry

#	Connection Mode	SSID / MAC Address	Encryption	Encryption Key	Router IP	Router Subnet	STP
1	Client / Station (Uplink)	SSID_A	WPA2-PSK(AES)	PassPhrase1	192.168.0.3	255.255.255.0	<input type="checkbox"/>
2	Client / Station (Uplink)	SSID_C	WPA2-PSK(AES)	PassPhrase2	192.168.6.3	255.255.255.0	<input type="checkbox"/>

Figure 60 Site B WDS Connections

- The first entry configures a virtual WDS client connection from Site B to the access point at Site A. The SSID is the same as Site A and the router IP address is 192.168.0.3, which is on the same subnet. Encryption is not inherited from the main page. Therefore, if the encryption method and keys are left blank the WDS link will be open. This example shows the encryption method and keys as being different, but they can be the same or take on the same method and key as the main wireless interface.
- The second entry configures another virtual WDS client connection, but this time to the access point of Site C. Again, the SSID is the same as the access point and the router IP is on the same subnet as the access point.

In addition to adding these WDS connections, Sites C and D will need a default gateway address configured so that the module can determine where to send traffic destined for the other networks. In addition, because Site A does not know how to get to networks 192.168.5.0 and 192.168.6.0, it requires rules to confirm the routing paths. A default gateway and one routing rule could be configured, but it is easier to configure two routing rules as shown in the example in Figure 61.

Routing Rules:

Add Entry Delete Entry

#	Name	Destination	Netmask	Gateway	Enabled
1	Route to Site B	192.168.5.0	255.255.255.0	192.168.0.3	<input checked="" type="checkbox"/>
2	Route to Site C	192.168.6.0	255.255.255.0	192.168.0.4	<input checked="" type="checkbox"/>

Figure 61 Site A Routing Rules

- The first routing rule specifies 192.168.5.0 as the destination with a netmask of 255.255.255.0, (network address range of Site B). Because the last byte of the destination IP is zero, this refers to the network (192.168.5.1 – 192.168.5.254), as opposed to an individual host IP. The same rule specifies the address 192.168.0.3 as the gateway address. The routing rule effectively tells the WI-MOD-E that any traffic destined for the network 192.168.5.X should be forwarded to Site B via WDS link address 192.168.0.3.
- The second routing rule is similar except the destinations IP address range is 192.168.6.0 with a Netmask of 255.255.255.0, indicating all traffic for the 192.168.6.X network will be routed through the WDS link address 192.168.0.4. This is the WDS router IP address that Site C has been configured with for its WDS link to Site A.

For more information on routing rules, refer to the “3.18 Routing.”

Unit C and D require some sort of routing rule that will determine how they communicate to networks outside of their configuration. Similar routing rules as shown above could be configured to direct traffic to these other networks. However, if only one routing path is required a default gateway address can be configured on the Network page.

IP Address	192.168.6.4
Subnet Mask	255.255.255.0
Default Gateway	192.168.6.3

Figure 62 Gateway Address

3.18 Routing

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

In some cases, it is not practical to have just one default gateway. For example, this is true for routed wireless networks with more than two WI-MOD-E routers, and in some cases when WDS router interfaces are used. If more than one next-hop router is required, the WI-MOD-E allows for up to 30 routing rules to be configured. A routing rule specifies a destination network (or host) IP address and the corresponding next-hop router to which messages for the specified destination will be forwarded. It is assumed that the next-hop router (or gateway) will then deliver the data to the required destination (or forward it on to another router that will).

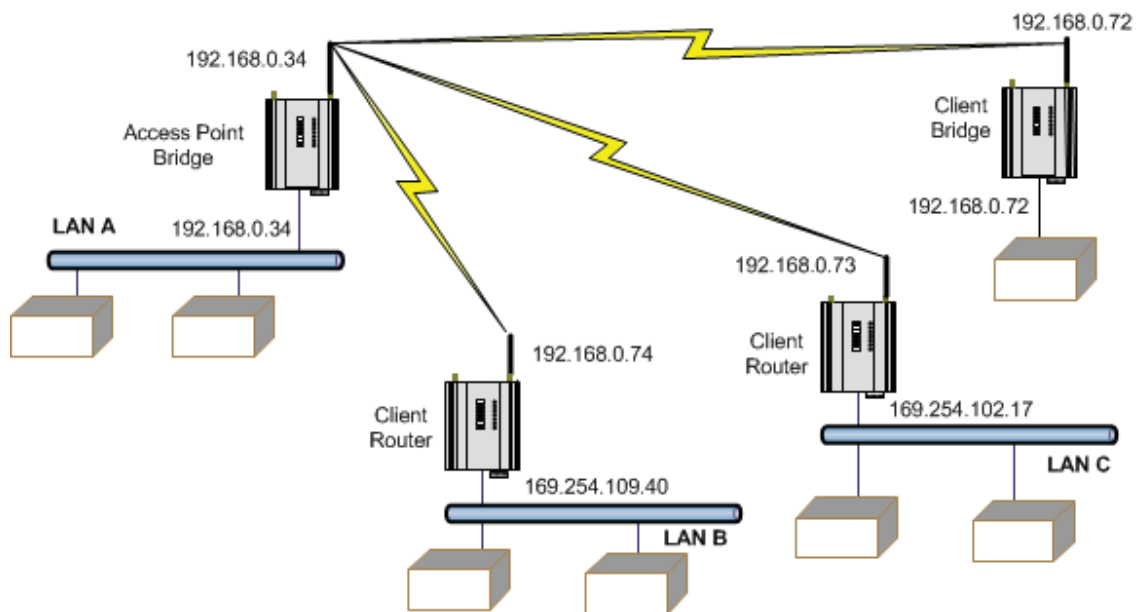


Figure 63 Routing

Figure 63 illustrates a situation where routing rules may need to be configured. In this example, the WI-MOD-E clients need only specify the access point as their default gateway (they require no routing rules to be configured). However, for the access point to be able to deliver traffic to LAN B and LAN C it needs to have routing rules configured that specify the respective WI-MOD-E client and routers as next-hop routers (gateways) to networks B and C. Note that devices on LAN A should specify the WI-MOD-E access point as their default gateway. An alternative to adding routing rules to the WI-MOD-E in this example would be for

each device on LAN A that needs to communicate with LANs B and C to have independent routing rules specifying the WI-MOD-E clients at B and C as gateways to those networks.

The routing rules for the access point in the Figure 63 are shown in Figure 64. The first entry shows the route to LAN B. The gateway for the route to LAN B is configured as the wireless IP address of the WI-MOD-E client connected to LAN B. The destination for the route is configured as the network address of LAN B. Because the host ID of the destination IP address is 0, it specifies a network address. Consequently, any traffic received at the access point with destination IP address 169.254.109.x (where x is any host ID) will be forwarded to the WI-MOD-E at LAN B.

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

The Routing Rules configuration page can be accessed by selecting the “Routing” link on any of the configuration webpages. Up to 30 routing rules may be added to each WI-MOD-E.

Routing Rules:

#	Name	Destination	Netmask	Gateway	Enabled
1	Route to LAN B	169.254.109.0	255.255.255.0	192.168.0.74	<input checked="" type="checkbox"/>
2	Route to LAN C	169.254.102.0	255.255.255.0	192.168.0.73	<input checked="" type="checkbox"/>

Figure 64 Routing Rules

The table below summarizes the configurable parameters of a routing rule.

Name	A name that describes the routing rule (maximum 32 characters).
Destination	The destination network (or host) IP address. To specify a network address, set the host address to 0. For example, an IP address 192.168.0.0 with netmask 255.255.255.0 would specify a destination network, while 192.168.0.16 specifies a destination host.
Subnet Mask	The subnet mask for the destination network.
Gateway	The IP address of the next-hop router for the specified destination.
Enabled	Select this checkbox to enable the rule. You can clear the box to disable a routing rule without needing to re-enter the information at a later time.

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

3.19 Filtering

When configured as a bridge, the WI-MOD-E will transmit all broadcast messages appearing at its wired Ethernet port. When the WI-MOD-E is configured as a router, this does not occur. In many cases, the intended recipient of the broadcast traffic does not lie at the opposite end of a proposed radio link. Reducing unnecessary broadcast traffic sent over the radio link will increase available bandwidth for data. The WI-MOD-E has a filtering feature to help reduce unnecessary wireless transmissions and enhance security.

The WI-MOD-E may be configured to reject or accept messages to and from certain addresses. To accept wireless messages from particular devices a “whitelist” of addresses must be made. Alternatively, to reject messages from particular devices, a “blacklist” of addresses must be made. Filtering applies only to messages appearing at the wired Ethernet port of the configured WI-MOD-E.

The Filter comprises of three lists—MAC Addresses, IP address/protocol/port, and ARP Filters. Each list may be set as either a blacklist (to block traffic for listed devices and protocols), or as a whitelist (to allow traffic for listed devices and protocols).

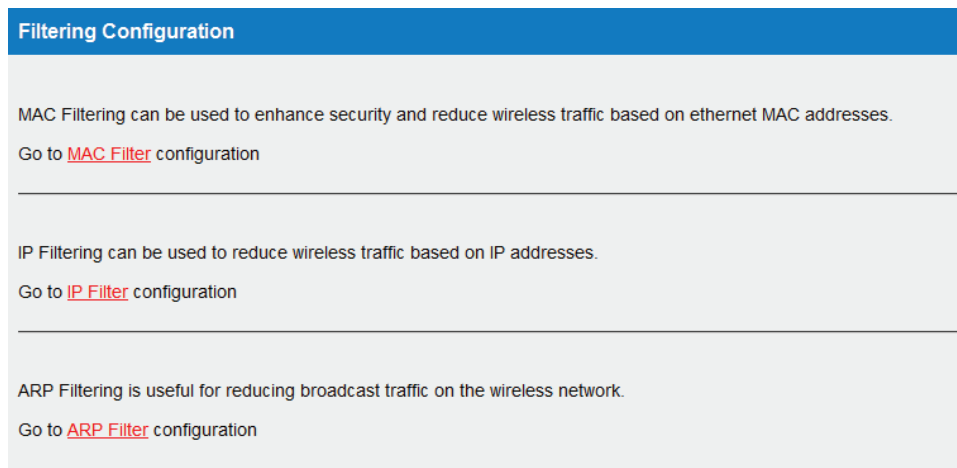


Figure 65 Filtering

The filter operates on the following rules:

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

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

In the example in Figure 66, device B needs to communicate with device E via modems C and D. The filtering requires that at modem C has device B in its whitelist and modem D has device E in its whitelist.

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

If radio links are chained together to form a radio backbone, it is also important to consider the operation of the Layer 3 Transparent Bridge (refer “3.8 Normal Operation”). A WI-MOD-E client will act as a MAC address translator, as it acts as a MAC address proxy on behalf of devices connected to its wired Ethernet port. The addition of WI-MOD-E client MAC addresses into intermediate WI-MOD-E units’ whitelist filters may be required for correct operation.

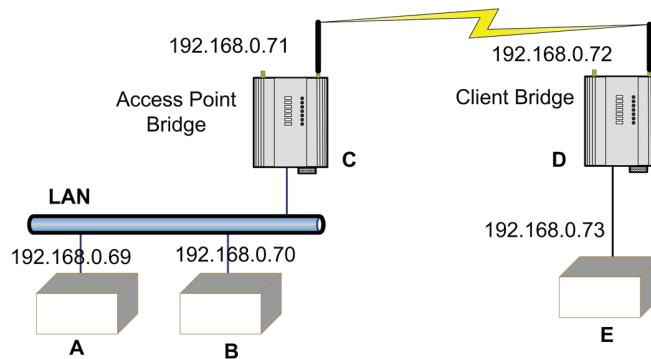


Figure 66 Filtering Example

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

MAC Address Filter Configuration

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

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

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

IP Address Filter Configuration

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

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



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

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

ARP Filter Configuration

Address Resolution Protocol (ARP) is a broadcast message and is primarily used for finding a MAC address when only the IP or some other Network Layer address is known. On large networks, you tend to get a high proportion of broadcast messages. Using ARP filters is useful for reducing broadcast traffic on the wireless network by only allowing ARP requests for known units to pass, or by blocking ARP requests for high use addresses.

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

3.20 DHCP Client Configuration

Dynamic Host Configuration Protocol (DHCP) allows DHCP clients to automatically obtain their IP address at startup. This simplifies network administration because there is no need to manually configure each device with a separate IP address. The WI-MOD-E is able to act as a DHCP client. To set the WI-MOD-E to acquire its IP address from a DHCP server, select the option “Obtain IP Address Automatically” on the Network Configuration page.

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

3.21 DHCP Server Configuration

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

Enabled	Select this checkbox to enable the DHCP server.
IP Range Minimum Maximum	The DHCP server will assign IP addresses to DHCP clients from within this range of addresses.
Gateway Primary DNS Secondary DNS	These settings are common to all of the DHCP clients, and refer to the gateway address, and Domain Name Service (DNS) configuration.
Lease Time	This is the number of seconds the client is granted the assigned IP address. The client should renew its lease within this time.

3.22 DNS Server Configuration

Domain Name Service (DNS) allows devices to be given human-readable names in additions to their IP address. This makes identification of devices (hosts) simpler, and makes it possible to identify devices that have been automatically assigned their IP address by a DHCP server (see section “3.21 DHCP Server

Configuration.” DNS is the system that translates Internet names (such as www.weidmuller.com) to IP addresses. The Weidmuller WI-MOD-E can act as a DNS server for a local network. Name to IP address mapping is automatically updated by the built-in DHCP server when it issues an IP address to a client unit.

For the DNS server configuration to be effective, each DNS client must be configured with the address of this DNS server, as either the primary or secondary DNS (secondary DNS is only used if there is no response from the primary DNS). Normally, this is done by setting the primary DNS field of the DHCP server configuration to the wireless IP address. This address is then provided to client units to use as their primary DNS server address when the DHCP server issues an IP address. The DNS server is configured using the following settings.

Enabled	Select this checkbox to enable the DNS server.
Domain Name	This is a common suffix applied to the name of each device in the network. If your network is part of a larger network, this would be assigned to you by the relevant naming authority. If your network is stand-alone, this field is set to an arbitrary name of your choice.
Device Name (Host Name)	This is the DNS name of the local device (commonly referred to as the host name or computer name). This setting is duplicated on the main Module Information configuration page. This is the name which is used to refer to this device (see “3.24 Module Information”).

3.23 VLAN

What is VLAN

Virtual Local Area Network (VLAN) is a way of splitting a network into groups that could extend beyond a single traditional LAN to groups of LANs, each identified with a different VLAN ID (VID). Using a VLAN, you can group users by logical connections instead of physical location. This can increase security and help improve the efficiency of traffic flow by limiting multicast and broadcast messages. Traffic between VLANs is blocked unless the VLAN is identified with the correct VLAN ID.

There are three main VLAN modes that the WI-MOD-E supports:

- VLAN (Pass-through Mode)—A transparent bridge in which frames are forwarded unmodified. This is the default mode of the modem in which all frames pass transparently through the bridge regardless of whether they are VLAN tagged or untagged. This is the most common VLAN mode and requires no VLAN configuration at all. In VLAN Pass-through mode, access to the internal management functions is via untagged frames only, using the IP address and subnet mask configured on the Network page.
- VLAN Aware (Bridging Mode)—A VLAN bridge that allows only explicitly configured VLANs that correspond to the configured VLAN groups to pass data. VLAN Bridging mode is used when the tagging method is changed in a bridged network, for example, if a frame traverses from a VLAN group to an interface that is not configured in a VLAN. When a VLAN packet is passed to an untagged VLAN interface, the tag is removed so that the packet can properly enter the network. Likewise, if an untagged VLAN packet is passed to a VLAN group a VLAN tag is added. When one or more VLAN groups have been configured, VLAN Pass-through is disabled and VLAN Aware mode is enabled.
- VLAN Aware (Routing Mode)—Same as VLAN Aware (Bridging Mode) described above, except that VLANs are routed not bridged. When a packet is routed from one VLAN to another on a different interface. The interfaces can be tagged or untagged and are generally on different subnets.

Enabling VLANs will allow the module to facilitate a number of possible VLAN topologies, such as:

- Segregating a wireless network into multiple virtual networks.
- Functioning as the wireless backbone on a VLAN trunk.
- Enabling a wireless network or part of the wireless network to form a VLAN trunk.
- Defining multiple virtual networks, each with a different priority to define traffic class based forwarding behavior over the radio channel.

Each module can be set up to accept different networks by configuring VLAN groups and having the interfaces (such as Ethernet, Wireless, or WDS repeater) configured to accept or reject tagged or untagged communications frames.

Operation

VLAN Pass-through is enabled by default in the modem. No VLAN configuration is needed and modem will pass any VLAN tagged frames. To initiate VLAN bridge or router operation, VLAN Aware mode must be enabled on the VLAN page.

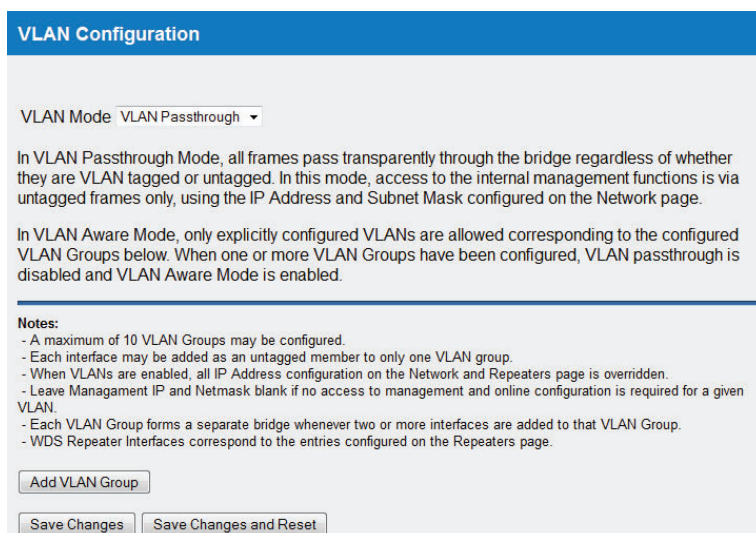


Figure 67 VLAN Pass-through

When VLAN Aware is enabled a default “Management VLAN Group” is created bridging the Ethernet and wireless interfaces and configuring both with untagged frames. The “Management IP” and “Management Netmask” addresses will override the modules “IP Address” and “Subnet Mask” and the Device Mode will be changed to “VLAN Bridge.” These changes will be indicated on the Network page of the module. A Management VLAN is created to ensure that the module will be accessible for configuration and diagnostics after setup.

If more than one interface is added to a VLAN group, a separate bridge will be created for the VLAN group. The configured interfaces for the VLAN group will then be configured as ports on the bridge.

In Figure 68, the Management VLAN has two interfaces configured, Ethernet and Wireless, and both are set to “Untagged.” This means the module can be accessed by either Ethernet or Wireless networks using untagged frames.

VLAN Configuration

VLAN Mode VLAN Aware

In VLAN Passthrough Mode, all frames pass transparently through the bridge regardless of whether they are VLAN tagged or untagged. In this mode, access to the internal management functions is via untagged frames only, using the IP Address and Subnet Mask configured on the Network page.

In VLAN Aware Mode, only explicitly configured VLANs are allowed corresponding to the configured VLAN Groups below. When one or more VLAN Groups have been configured, VLAN passthrough is disabled and VLAN Aware Mode is enabled.

Modify the Management VLAN as required to provide access to the internal management functions and online configuration interface. The Management VLAN will override the Network page settings.

Management VLAN: Delete Management VLAN

#	Name	VLAN ID	VLAN Priority	Management IP	Management Netmask	Bridge STP	Bridge Priority
1	Management VLAN	1	0	192.168.0.100	255.255.255.0	<input type="checkbox"/>	32768

Interface Membership for Management VLAN:

Add Entry Delete Entry

#	Interface	Type
1	Ethernet Interface	Untagged
2	Wireless Interface	Untagged

Figure 68 VLAN Aware




NOTE Leaving the default Management VLAN is advised, as it will ensure that the module is accessible through any interface.

VLAN Group

Enabling VLAN Aware on the module will require one or more configurable VLAN groups. A maximum of up to 10 VLAN groups can be supported. Each VLAN group will contain the following configurable parameters and associated functionality.

- Name** A textual description of the VLAN group, consisting of a maximum of 32 ASCII characters. This parameter is descriptive only and serves no functional purpose.
- VLAN ID** A valid 12-bit IEEE802.1Q VID, with a range of 1–4095. The VLAN ID will be added to all outgoing VLAN tagged frames for this VLAN group. All incoming VLAN tagged frames for the VLAN group must have this VLAN ID.
- VLAN Priority** An IEEE802.1Q compatible, 3-bit Priority Code Point, with a range of 0–7, where seven is the highest priority, one is the lowest, and zero is the default, which is a mid-range “best effort” value. The VLAN priority will be added to all outgoing VLAN tagged frames for this VLAN group. Furthermore, the VLAN priority will be used to determine which of four priority radio queues VLAN tagged frames will be queued on when transmitted via the radio.

Management IP The management IP is the address of the module if only one VLAN group is configured. Access to the module’s internal Web-based configuration and IP-based functions (such as serial gateway, or Modbus server) is provided via this management IP address and subnet mask.

 **NOTE** If only one VLAN group is configured, it must have a management IP and netmask. If further VLAN groups are configured (groups 2-9) they only need a management IP and subnet if access to the modules IP-based functions (such as Modbus or webpages) is required.

Management Netmask The IP network mask of the management IP (see above).

Bridge STP Turns on Spanning Tree Protocol (STP) for the bridge. STP prevents network loops that can cause broadcast storms.

Bridge Priority The STP priority number for the bridge. This value should be set in context with other devices that are connected on the same network.

Interface Membership

Each VLAN group has a configurable interface membership list. The membership list will allow up to 12 possible interfaces to be added. The following configurable parameters will apply to each entry:

Interface	Select interface from the drop-down list to be used for the VLAN group. Available interfaces are, Ethernet, Wireless or one of the 10 WDS Repeater connections that correspond to configured entries on the Repeaters page.
Type	Specifies whether the interface is to support VLAN tagged or untagged frames. When untagged is specified, all incoming frames on the interface must be untagged, and all outgoing frames will be sent untagged. When tagged is specified, all incoming frames must have a VLAN tag with VLAN ID matching the configured VLAN ID for the VLAN group; all outgoing frames on this interface will have a VLAN tag added with the configured VLAN ID and priority for that VLAN group.

Example 1: Basic VLAN

A common use for VLAN functionality in a module is to tag data from a VLAN unaware device and send this to a VLAN trunk. A simple example of this involves bridging between Ethernet and wireless ports for just one VLAN. In Figure 69, the Ethernet interface is tagged and the wireless interface is untagged. Any data arriving at the Ethernet port is expected to have VLAN tagged data with “VLAN ID 10,” and any data sent from the Ethernet port will have the VLAN tag added. This example allows wireless data from VLAN-unaware devices to be bridged with the Ethernet interface and have VLAN tags added (the Ethernet connection is now part of a VLAN trunk that will send/receive data to/from other VLAN-aware devices).

Example 1

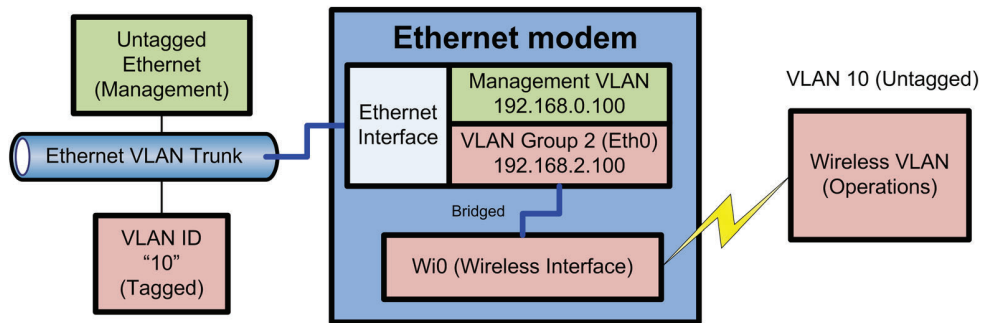


Figure 69 VLAN Example 1

The module configuration below shows there are two VLAN groups configured. The first group is used for management of the module and ensures a connection is maintained for configuration and diagnostics from untagged devices on the VLAN trunk.

Modify the Management VLAN as required to provide access to the internal management functions and online configuration interface. The Management VLAN will override the Network page settings.

Management VLAN: [Delete Management VLAN](#)

#	Name	VLAN ID	VLAN Priority	Management IP	Management Netmask	Bridge STP	Bridge Priority
1	Management VLAN	1	0	192.168.0.100	255.255.255.0	<input type="checkbox"/>	32768

Interface Membership for Management VLAN:
[Add Entry](#) [Delete Entry](#)

#	Interface	Type
1	Ethernet Interface	Untagged

VLAN Group 2: [Delete VLAN Group 2](#)

#	Name	VLAN ID	VLAN Priority	Management IP	Management Netmask	Bridge STP	Bridge Priority
1	Operations	10	0	192.168.2.100	255.255.255.0	<input type="checkbox"/>	32768

Interface Membership for VLAN Group 2:
[Add Entry](#) [Delete Entry](#)

#	Interface	Type
1	Ethernet Interface	Tagged
2	Wireless Interface	Untagged

Figure 70 Example 1 Configuration

Example 2: Multiple Wireless Interfaces

Another very desirable VLAN configuration for a wireless device is to support multiple virtual wireless networks. For example, consider a corporate facility where separate networks may be provided for a) permanent staff, b) guests, and c) production network. Each of the three different virtual networks can be set up using different encryption keys to enhance security. The setup is illustrated in Figure 71.

Example 2

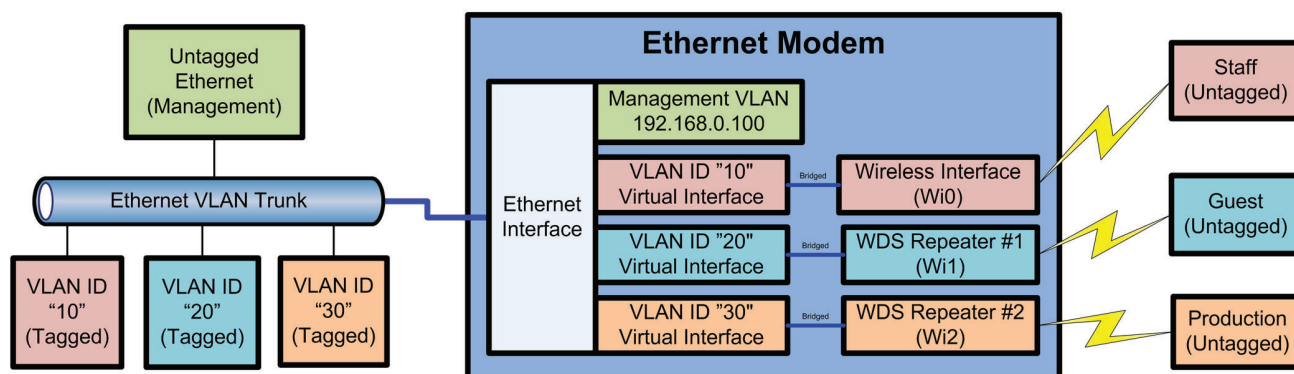


Figure 71 VLAN Example 2

The module is configured with three wireless interfaces. The first one is the normal wireless interface found on the Network page (wi0), the second (wi1) and third (wi2) are virtual interfaces created on the Repeaters page. Each interface is configured as an access point and can be setup with unique SSIDs and encryption settings. In this example, all three wireless interfaces are untagged so that devices joining each of the networks need not be VLAN-aware.

Untagged data from each of the wireless interfaces are individually bridged with one of the three VLAN-aware virtual interfaces "VLAN ID 10," "VLAN ID 20," and "VLAN ID 30" on the physical Ethernet Interface that forms a VLAN trunk. Untagged data transferred via the first Wireless interface (wi0) is internally bridged with the virtual interface VLAN ID 10. Likewise, untagged data transferred via the other two WDS repeater interfaces (wi1 and wi2) are bridged respectively with VLAN ID 20 and VLAN ID 30. The unique VLAN tags are used for corresponding Ethernet data, so that the Ethernet port becomes a VLAN trunk.

Because the WI-MOD-E supports flexible VLAN functionality such that any of the available interfaces can have membership to particular VLAN(s) by assigning membership to one or more VLANs groups—virtually any possible topology can be achieved.

Figure 72 shows the configuration for the multi-VLAN example described above. Notice that there are four groups configured, one for management and one for each of the VLAN IDs. The management group only has the untagged Ethernet interface configured, which means only untagged device on the same IP subnet can access the modules configuration.

Modify the Management VLAN as required to provide access to the internal management functions and online configuration interface. The Management VLAN will override the Network page settings.

Management VLAN: Delete Management VLAN

#	Name	VLAN ID	VLAN Priority	Management IP	Management Netmask	Bridge STP	Bridge Priority
1	Management VLAN	1	0	192.168.0.100	255.255.255.0	<input type="checkbox"/>	32768

Interface Membership for Management VLAN: Add Entry Delete Entry

#	Interface	Type
1	Ethernet Interface	Untagged

VLAN Group 2: Delete VLAN Group 2

#	Name	VLAN ID	VLAN Priority	Management IP	Management Netmask	Bridge STP	Bridge Priority
1	Staff	10	3	192.168.2.100	255.255.255.0	<input type="checkbox"/>	32768

Interface Membership for VLAN Group 2: Add Entry Delete Entry

#	Interface	Type
1	Ethernet Interface	Tagged
2	Wireless Interface	Untagged

VLAN Group 3: Delete VLAN Group 3

#	Name	VLAN ID	VLAN Priority	Management IP	Management Netmask	Bridge STP	Bridge Priority
1	Guest	20	5	192.168.5.100	255.255.255.0	<input type="checkbox"/>	32768

Interface Membership for VLAN Group 3: Add Entry Delete Entry

#	Interface	Type
1	Ethernet Interface	Tagged
2	WDS Repeater #1	Untagged

VLAN Group 4: Delete VLAN Group 4

#	Name	VLAN ID	VLAN Priority	Management IP	Management Netmask	Bridge STP	Bridge Priority
1	Production	30	7	10.94.74.100	255.255.255.0	<input type="checkbox"/>	32768

Interface Membership for VLAN Group 4: Add Entry Delete Entry

#	Interface	Type
1	Ethernet Interface	Tagged
2	WDS Repeater #2	Untagged

Figure 72 Example 2 Configuration

The other VLAN groups each have an Ethernet and a wireless interface configured. All Ethernet interfaces are tagged because they are all connected to a VLAN network. Each wireless interface is configured as untagged to allow connection from untagged devices. VLAN Group 2 is using the standard wireless interface which is configured from the main Network page, while the other two are each using one of the WDS Repeater virtual interfaces.

VLAN Group 2 is bridging the default wireless interface with the VLAN ID 10 virtual Ethernet interface. Configuration of the wireless bridge (operating mode, SSID and radio encryption methods/keys) is performed from the main Network page, as shown in Figure 73.

Wireless Interface:

Operating Mode: Access Point

System Address (ESSID): Staff

Desired BSSID: 00:00:00:00:00:00

Radio Encryption: WPA2-PSK(AES) Configure Encryption Settings on Security Page

Device Mode:

Device Mode: VLAN Bridge

Figure 73 VLAN Encryption.

VLAN groups 3 and 4 are similarly bridging their wireless interfaces, but they are using virtual modules that are configured on the Repeaters page. WDS repeater #1 and WDS repeater #2 are being bridged to VLAN ID 20 and VLAN ID 30 respectively. Configuration for these wireless bridges is set from the Repeaters page (see the example in Figure 74).

WDS Connections:

#	Connection Mode	SSID / MAC Address	Encryption	Encryption Key	Router IP	Router Subnet	STP
1	Access Point (Downlink)	Guest	WEP(128 bit)	dDS@34aZx	169.254.5.100	255.255.255.0	<input type="checkbox"/>
2	Access Point (Downlink)	Production	WPA2-PSK(AES)	WiReLeSs_TeChNoLoGy	10.94.74.100	255.255.255.0	<input type="checkbox"/>

Figure 74 WDS Encryption

Notice that all three wireless interfaces are setup as access points, but are configured with different SSIDs and encryption methods/keys. If encryption fields are left blank, the connection will use the default wireless interface parameters as configured on the Network page. Likewise, if the router IP and subnet are left blank the connection will use the same default settings.

NOTE Router IP and subnet do not need to be configured in WDS Connections because it will use the IP address assigned in the VLAN group.

The VLAN Multiple Wireless Interfaces example above shows that each group is using a different VLAN priority. Priorities can be given to each interface by configuring a value between zero and seven, seven being the highest priority and one being the lowest. These values can be used to prioritize the configured VLAN networks. In our example, the “Production” VLAN has the highest priority which means it will have more time slots available to send data, followed by the “Guest” network, and then “Staff.” The default value is zero which will configure the group to have a mid-range “best effort” value.

3.24 Module Information

Module Information Webpage Fields

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

Username	The username used to access the configuration on the WI-MOD-E. Take care to remember this username if you change it, as it will be needed to access the WI-MOD-E in future.
Password	The password used to access the configuration on the WI-MOD-E. Take care to remember this password if you change it, as it will be needed to access the module in future.
Device Name	A label for the particular WI-MOD-E. This is also the DNS name (hostname) of the device if you are using DNS.
Owner	Owner name.
Contact	Owner contact information (such as phone number and email address).
Description	Description of the purpose of the unit.
Location	Location of the WI-MOD-E.

3.25 Configuration Examples

Setting a WI-MOD-E to Factory Default Settings

1. Access the Configuration webpage on the 245U-E.
For details, see “3.2 Configuring the Unit for the First Time.”
2. Click the System Tools menu item.
3. Click Factory Default Configuration Reset and wait for the unit to reset.
While the module executes the reset sequence the OK LED will flash. The OK LED will turn green when the reset sequence is complete.

Extending a Wired Network

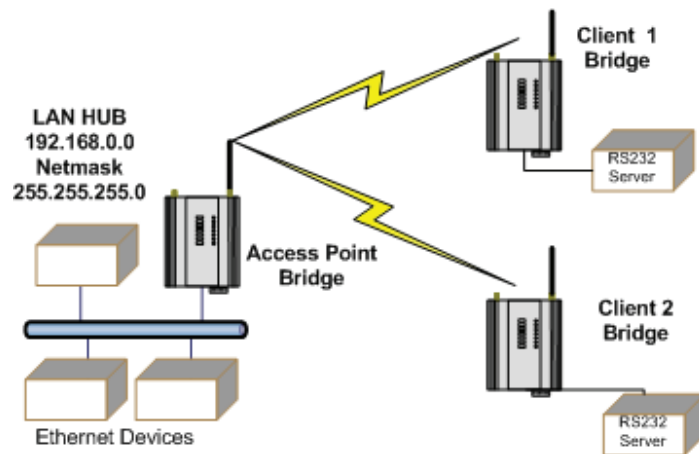


Figure 75 Example Configuration 1

Access Point Configuration

1. Connect a straight-through Ethernet cable between the PC and the WI-MOD-E.
2. Ensure that the configuration of the PC and WI-MOD-E are setup to communicate on the same network.
3. Set DIP switch to SETUP mode.
4. Power up the unit and wait for the OK LED to stop flashing.
5. Adjust the PC network settings.
6. Set Configuration PC network card with the network setting of IP address 192.168.0.1, netmask 255.255.255.0.
7. Open the Configuration webpage within Internet Explorer at <https://192.168.0.1XX/>, where "XX" is the last two digits of the module's serial number.
8. When prompted for the password, enter default username "user" and password "user."
9. Click Network and set the Operating Mode to "Access Point."
10. Set the Device Mode as "Bridge."
11. Change the Gateway IP Address to 192.168.0.1.
12. Change the Ethernet and Wireless IP addresses to 192.168.0.200.
13. Change the Ethernet and Wireless Subnet masks to 255.255.255.0.
14. Enter a System Address (ESSID) string.
15. Select the radio encryption required.
16. Set DIP switch to RUN.
17. Save the changes and unit will restart with new settings.

Client 1 Configuration

Perform the same configuration steps as the access point configuration with the following differences:

1. Set the Ethernet and Wireless IP addresses of WI-MOD-E to 192.168.0.201.
2. Set the Operating Mode to "Client."
3. Ensure that the ESSID and radio encryption method match the access point.
4. If encryption is used, ensure the encryption keys or passphrase match the access point.

Client 2 Configuration

Perform the same configuration steps as for client 1 above, except set the Ethernet and Wireless IP addresses as 192.168.0.202.

Connecting Separate Networks

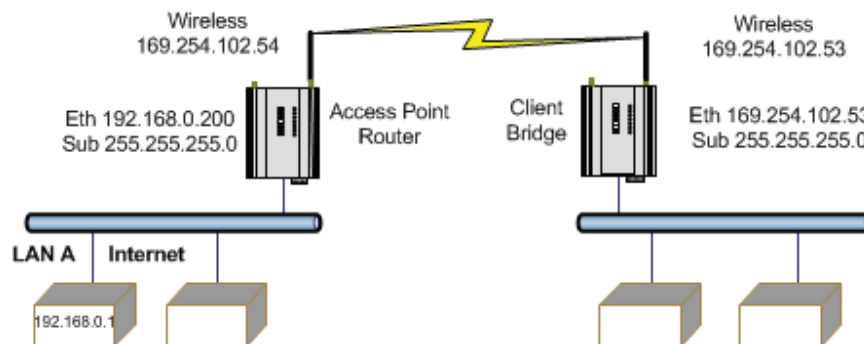


Figure 76 Routing

LAN A Configuration

In this example, LAN A is connected to the Internet via a router at IP address 192.168.0.1. Devices on LAN A that only require access to devices on LAN A and B, should have their gateway IP address set to the WI-MOD-E access point as 192.168.0.200.

Devices on LAN A, that must interact with devices on LAN A and B and the Internet should set the Internet router 192.168.0.1 as their gateway, and must have a routing rule established for devices on LAN B. On PCs, this may be achieved with the MS-DOS command ROUTE. For this example use: ROUTE ADD 169.254.102.0 MASK 255.255.255.0 192.168.0.200.

LAN B Configuration

All devices on LAN B should be configured so that their gateway IP address is that of the WI-MOD-E access point as 169.254.102.54.

Access Point Configuration

1. Connect a straight-through Ethernet cable between the PC and the WI-MOD-E.
2. Ensure that the configuration of the PC and WI-MOD-E are setup to communicate on the same network.
3. Set the DIP switch to SETUP.
4. Power up the unit, and wait for the LINK LED to stop flashing.

5. Adjust the PC network settings.
6. Set the Configuration PC network card with the network setting of IP address 192.168.0.1, and netmask 255.255.255.0.
7. Open the Configuration webpage within Internet Explorer at address <https://192.168.0.1XX/>.
8. When prompted for your password, enter default username “user” and password “user.”
9. Enter “Network” and set the Operating Mode to “Access Point.”
10. Set the Device Mode to “Router.”
11. Set the Gateway IP address to 192.168.0.1.
12. Set the Ethernet IP address to 192.168.0.200, and the network mask to 255.255.255.0.
13. Set the Wireless IP address to 169.254.102.54, and the network mask to 255.255.255.0.
14. Select the radio encryption required, and enter the encryption keys or passphrase, if necessary.
15. Set the DIP switch to RUN.
16. Click Save to Flash and Reset.
The webpage displays a message indicating that details are being written to flash. Wait for the WI-MOD-E to reboot before removing power.
17. Enter a System Generator String.

Client Configuration

Perform the same configuration steps as the access point configuration, with the following differences:

1. Enter “Network” and set the Operating Mode as “Client.”
2. Set the Device Mode to “Bridge.”
3. Set the Gateway IP address to 169.254.102.54.
4. Set the Ethernet IP address to 169.254.102.53, and network mask to 255.255.255.0.
5. Set the Wireless IP address to 169.254.102.53, and network mask to 255.255.255.0.
6. Click Save to Flash and Reset.

The webpage displays a message indicating that details are being written to flash. Wait for the WI-MOD-E to reboot before removing power.

Extending Range Using Repeaters

Configure units as described in “Extending a Wired Network.” Place the access point at the remote intermediate repeater location. Additional repeaters can be added using Repeaters. See “3.17 Repeaters (WDS).”

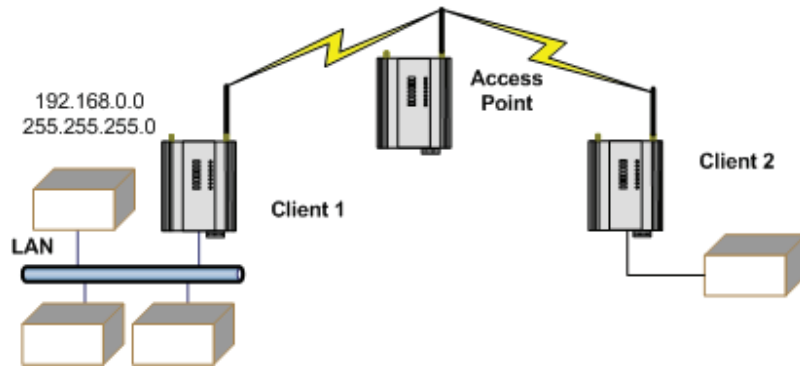


Figure 77 Example Repeaters

Chapter 4 - DIAGNOSTICS

4.0 Diagnostics Chart

LED Indicator	Condition	Meaning
OK	Green	Normal operation.
OK	Red Continuously	Supply voltage too low or internal module fault.
OK	Red At Power On	Boot loader delay at startup.
OK	Fast Flash Red / Green	Module boot sequence.
OK	Slow Flash Red / Green	Module boot sequence.
Radio RX	Green flash	Radio receiving data.
Radio RX	Red flash	Radio receiving data (low signal strength).
TX/LINK	Green	Connection established to remote device.
TX/LINK	Red Flash	Radio transmitting.
RS-232	Green flash	Data sent from RS-232 serial port.
RS-232	Red flash	Data received to RS-232 serial port
LAN	On	Link established on Ethernet port.
LAN	Flash	Activity on Ethernet port.
RS-485	Green flash	Data sent from RS-485 serial port.
RS-485	Red flash	Data received to RS-485 serial port.
DIO	Green	Digital input is grounded.
DIO	Red	Digital output is active.
DIO	Off	Digital output Off and input is open circuit.

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

Boot Status LED Indication During Startup

The OK LED indicates the status of the module during the boot up process. At power on, the OK LED turns red. During kernel boot the OK LED flashes red-green at a 1-Hz rate (1/2 second red, 1/2 second green). During module initialization, the OK LED flashes red-green at 0.5-Hz rate (1-second red, 1-second green). When initialization is complete, the OK LED switches to green continuously.

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

4.1 Connectivity

The Connectivity webpage displays connections and available networks. The “Connected Devices” section displays the radio channel, received signal strength, and radio data rate for each client or access point by their MAC address. The readings shown are based upon the last received data message from the access point or client. Client stations also display a list of detected access points (site survey), including network name (SSID), channel and maximum data rate.



NOTE When updating the Connectivity webpage, it is necessary to hold down the CTR key while pressing the Refresh button, otherwise the information will not be updated.

Connected Devices

Connected Devices:							
wi0:							
=====							
MAC ADDRESS	IP ADDRESS	AID	CHAN	RATE	RSSI	BGND	CAPS
06:12:af:00:91:16	192.168.0.185	1	7	54.00M	-52	-99	EPS

Figure 78 Connected Devices

MAC Address	Media Access Control address, which is a unique factory-configured address assigned to the hardware.
IP Address	IP address assigned to the hardware.
AID	Association ID. Every client gets a unique temporary ID from the access point.
CHAN	The radio channel being used.
RATE	Radio data rate.
RSSI	Radio signal strength index (the amount of received signal strength).
BGND	Background interference level, in dBms. The amount of internal noise the radio is able to hear. This level does not indicate external radio interference noise level.
CAPS	Capabilities (Ref 802.11 Standard).

Site Survey

Site Survey is a one-off snapshot showing the access points that are available for connection. This list is only available on clients, and only available at startup of the module or by selecting “Background Scanning” on the Radio page.

Site Survey:							
SSID	BSSID	CHAN	RATE	S:N	INT	CAPS	
TEST_SSID	06:12:af:00:56:fe	24	54.00M	-52:-96	100	ESS	WME ATH

Figure 79 Connectivity / Site Survey

SSID	The service set identifier or network name used to identify a particular network.
BSSID	The MAC (media access control) address of the access point.
CHAN	The radio channel being used.
RATE	Maximum radio data rate.
S:N	Signal strength and noise level. In the case above, the signal is -44 dB and the background noise level is -88 dB.
INT	Beacon interval.
CAPS	Capabilities (Ref 802.11 Standard).

4.2 Channel Survey (Utilization)

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

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

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

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

Channel Utilization on a Live System

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

Channel Utilization for Channel Selection or RF Path Testing

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

Diagnosing Low Throughput

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

Solutions for High Channel Utilization

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

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

- The connected modem is transmitting.
- The connected modem is receiving valid data from another modem.
- The connected modem has detected RF noise or interference.

The Channel Survey shows the channel utilization and noise floor graph with 1-second, 1-minute and 1-hour periods.

Figure 80 shows a percent of the overall radio traffic on the channel that is currently being used.

Bar Graph of Percent Channel Utilization with 1 Second Intervals:

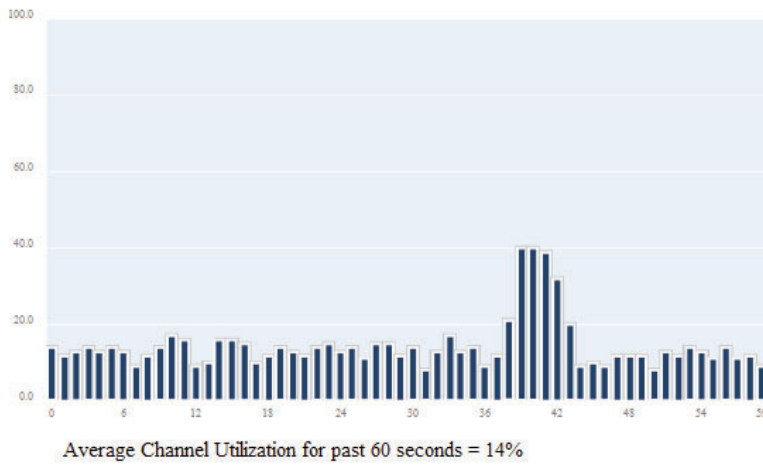


Figure 80 Channel Utilization

Figure 81 shows the radio receive noise floor for the last 60 seconds.

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

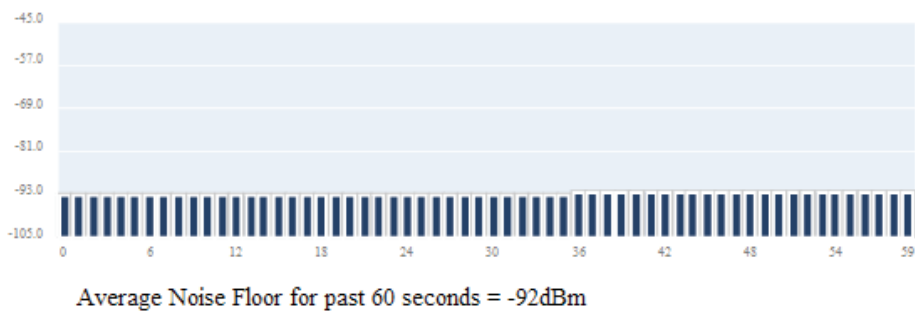


Figure 81 RX Noise Floor

Figure 82 shows the average Channel Utilization for each minute up to one hour. It will also give a running average for the total number of minutes up to 59 minutes.

Bar Graph of Percent Channel Utilization with 1 minute intervals:

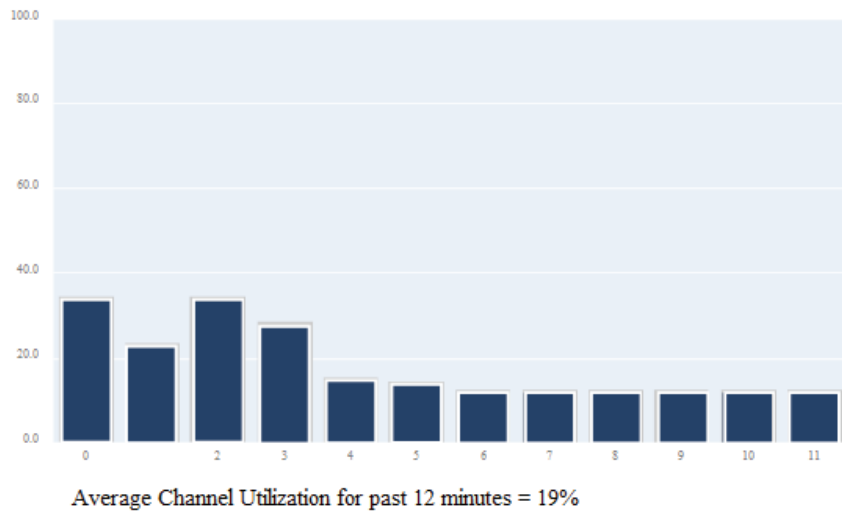


Figure 82 Channel Utilization Minutes

Figure 83 shows the running radio receive noise floor average for each minute up to 59 minutes.

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

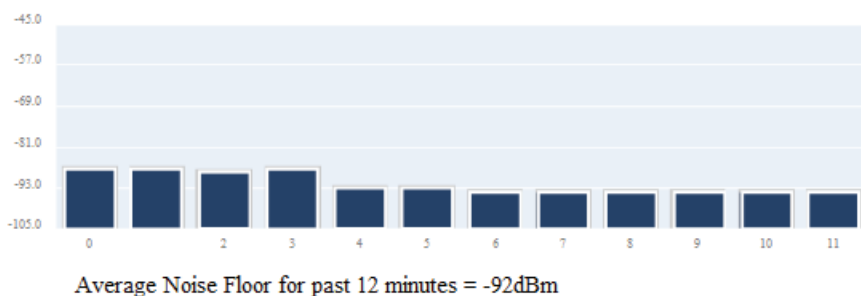


Figure 83 Noise Floor Minutes

The Channel Survey page also shows two other screens not shown here that indicate the percent channel utilization and noise floor in one hour intervals. The screens will only show the last 24-hour period.

4.3 Custom Survey

Custom Survey is essentially the same as the Channel Survey (see the previous section), except that the three channel utilizations can be turned on or off to show the different amount of traffic-related data.

- Percent Radio TX** Any transmitted messages from the radio to other devices.
- Percent Radio RX** Any DSSS or OFDM messages received by the radio (basically any standard Wi-Fi data packets from either Weidmuller or competitor radios).
- Percent Busy (CCA or Noise)** Clear Channel Assessment (CCA) is the detection of any ongoing transmissions or noise, for example, from devices such as microwaves, 2.4Ghz FHSS, cordless phones, or RC devices.

By configuring the different chart options, you can get a clear idea of the amount of data being transmitted, received and the amount of other noise that can be heard at the radio. Configure what is to be logged on each chart, select a time interval and save changes and the charts will then be displayed below the settings. Click the button again to manually redraw the graphs. Each graph will display a percent channel utilization using the selected criteria and time interval (seconds, minutes or hours).

Example 1

Chart one shows the amount of data that is being transmitted over a Wi-Fi link. Chart two shows the amount of data being received from all sources (Wi-Fi and other noise). Notice that there is very little outgoing data, but a constant stream of data is being received.

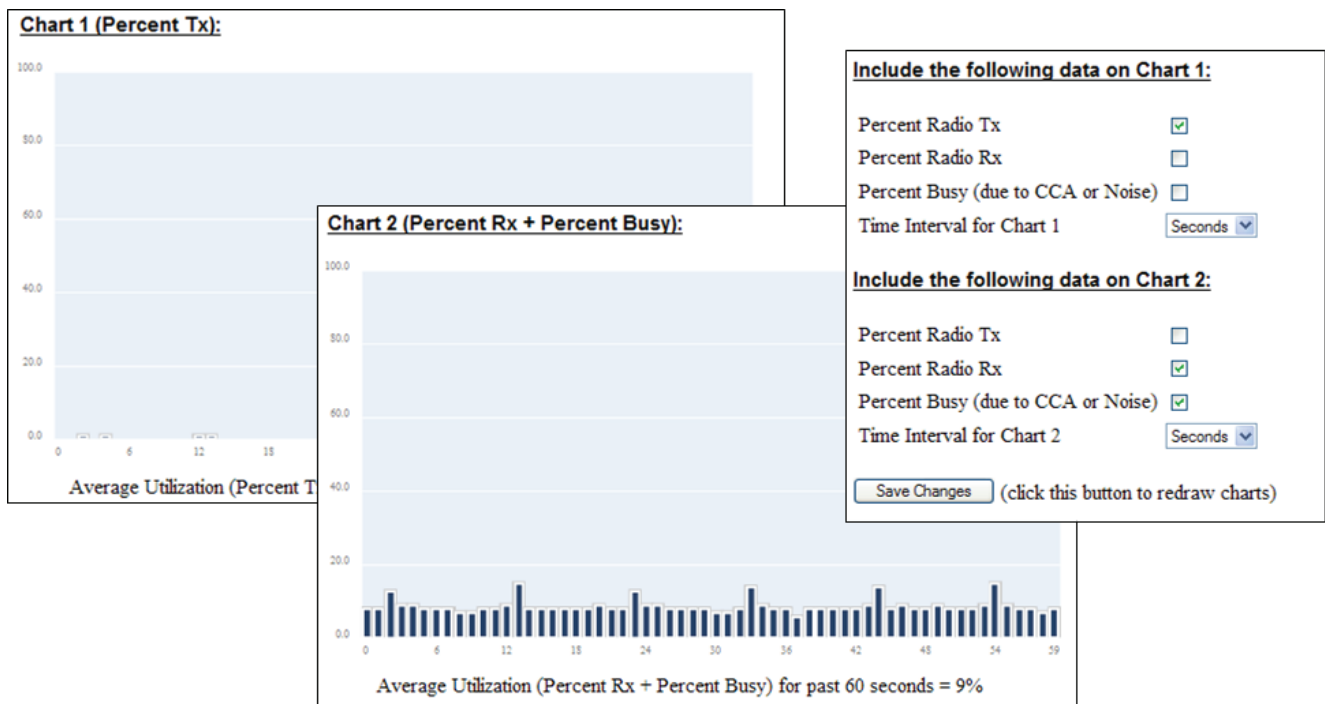


Figure 84 Custom Survey 1

Example 2

In the second example (Figure 85), chart one shows the amount of data being received from Wi-Fi devices. Chart two shows the amount of other noise that is being received. Notice that in the last 60-second period there was a 20-second interval with around 60–80% channel utilization, in this case from a 2.4-GHz FHSS telemetry device.

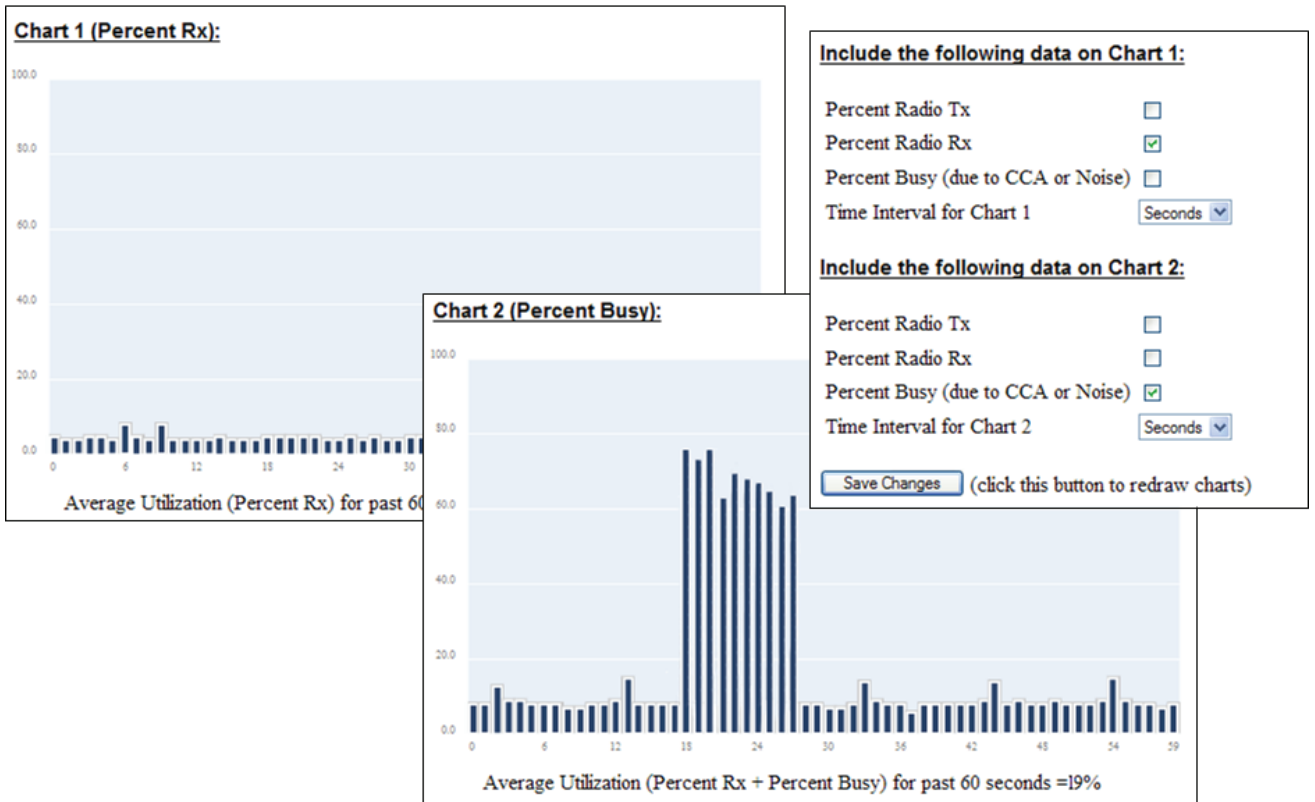


Figure 85 Custom Survey 2

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

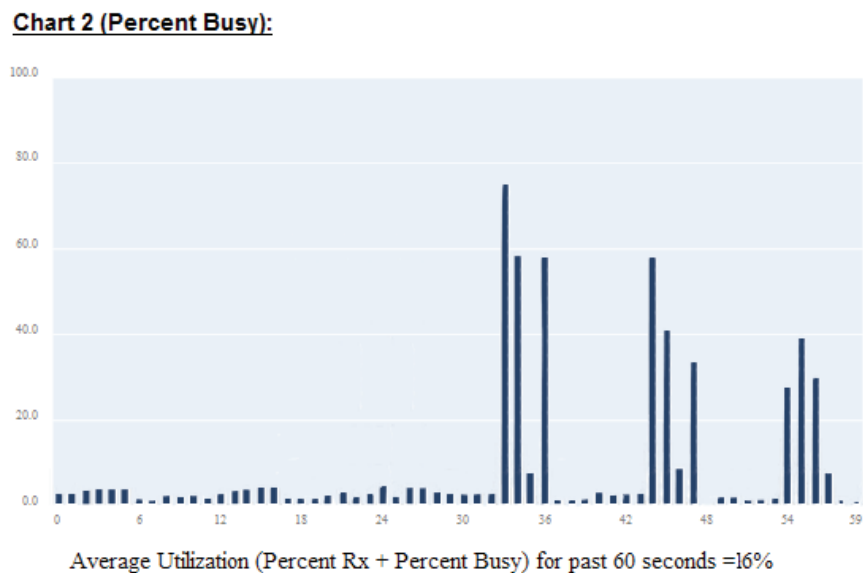


Figure 86 Channel Utilization

4.4 Throughput Test

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

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

Internal Throughput Test

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



NOTE TCP throughput test must be run using Microsoft Internet Explorer 8 or later.

Advanced Radio Settings:	
Tx Antenna	Main Port Only ▾
Rx Antenna	Main Port Only ▾
DTIM Period (AP Only)	1 beacon intervals
RTS Threshold	2346 bytes
Fragmentation Threshold	2346 bytes
Interference Mitigation	<input type="checkbox"/>
Bursting	<input type="checkbox"/>
Enable Iperf Server	<input checked="" type="checkbox"/>
Fixed Noise Floor	0 dBm (Set to 0 for Dynamic Adjustment)

Figure 87 Throughput Test Configuration

To run an internal throughput test:

1. Connect to the webpage of the module that will be performing the Iperf test.
2. Select “System Tools” on the right pane of the webpage, and then select “TCP Throughput Test.”

The screen shown in Figure 88 appears.

TCP Throughput Test

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

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

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

Not sure what throughput to expect? click [here](#)

Remote Device IP Address:

[Iperf throughput for 10 second interval:](#)

Figure 88 Throughput Test

3. Enter the IP address of the remote device that you want to test, and then click Measure Throughput.

Not sure what throughput to expect? click [here](#)

Remote Device IP Address:

[Iperf throughput for 10 second interval:](#)

Figure 89 Iperf

The specified IP address must be running Iperf in Server mode. If the remote modem does not have the Iperf server running, you will get the error message "perf error, check connectivity to server." Ensure that it has been enabled and reset the module. Each time you click Measure Throughput, a 10-second TCP throughput test is performed.

You will see the message "Performing Iperf Test," and if you look at the modules you will see the TX/Link and RX LEDs flashing quickly as it performs the test. After about 10 seconds, a graph appears showing the actual throughput over the 10-second period and a calculated average.

The graph below shows the data throughput range between 8 and 14.5 Mbits per second with an overall average of 10.9 Mbits per second. It is recommended to perform this throughput test a number of times to get a better sample of the overall throughput.

Iperf throughput for 10 second interval:

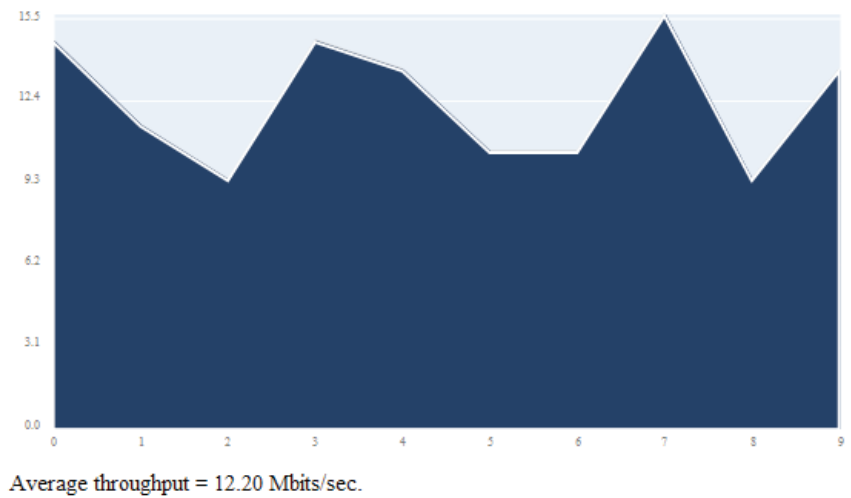


Figure 90 Iperf Throughput

The expected throughput will depend on a number of things, including the distance setting, selected channel width, and whether using the internal Iperf utility or running Iperf externally on a laptop or PC (at both ends of the link). The following table shows real-world throughput estimates based on channel selection and receiver signal levels. Throughput is calculated using the built-in Iperf utility and communicating TCP/IP over the three bandwidth channels (20 MHz, 10 MHz, and 5 MHz). These estimates are not necessarily the maximum achievable for the modems, but are used as a guideline to determine the performance of the radio link. See “Appendix D- EXTERNAL IPERF TEST” for details on using the external Iperf throughput test.

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

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

Throughput and Repeaters

It should be noted that if you are using repeaters to extend the range, there will be a reduction in throughput for each repeater hop. The 40-MHz Turbo channels rarely provide better throughput than the 20-MHz in the real world because they occupy a larger portion of the 2.4-GHz band and are more prone to interference. For RSSI, see

“4.1 Connectivity.” For information on checking interference or noise, see “4.2 Channel Survey (Utilization).”

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

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

4.5 Statistics

The Statistics webpage is used for advanced debugging of WI-MOD-E. This webpage details the state of the WI-MOD-E and performance information. This page is useful to Weidmuller technical support in diagnosing problems with the module.



NOTE When updating the Statistics webpage, it is necessary to hold down the CTRL key while clicking Refresh, otherwise the information will not be updated.

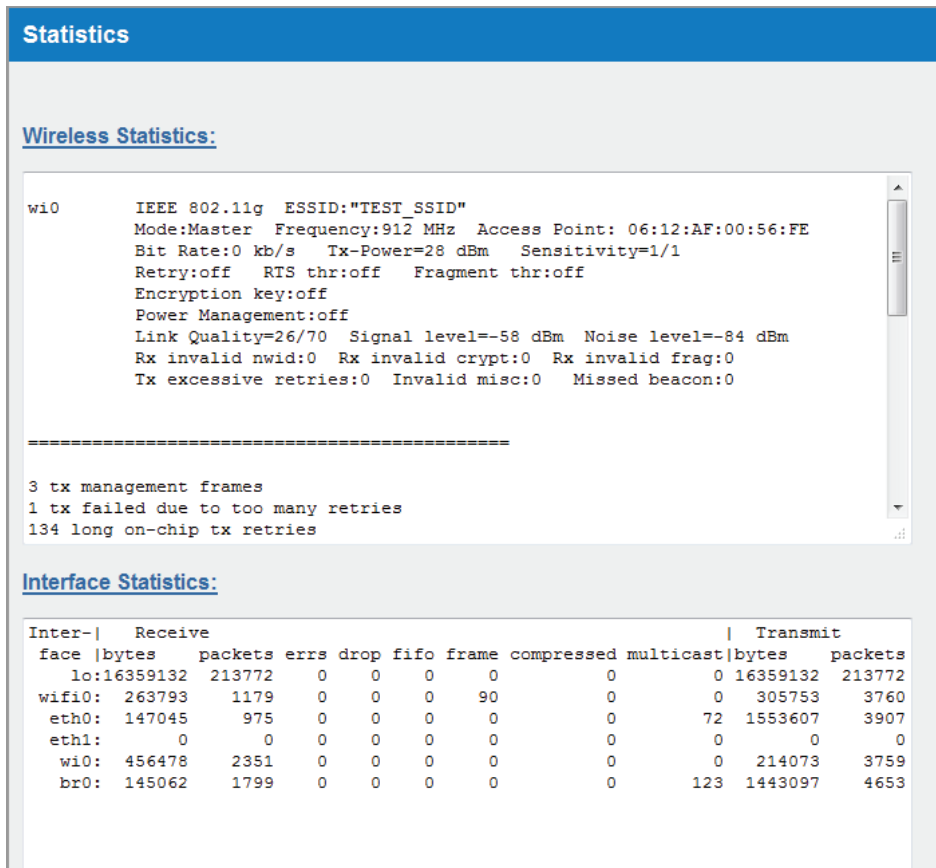


Figure 91 Statistics

Wireless Statistics

On the Statistics webpage, Wireless Statistics is the main area for additional diagnostics statistics. The list of statistics produced is dynamic and may vary depending on the model and configuration (2.4 GHz, 5 GHz or 900 MHz, and client or access point).

Access Point

- Beacon Miss Count** Number of beacons unable to be sent (100-msec intervals) due to interference or CCA.
- Beacon Missed Reset Count** After 15 consecutive beacon misses (1.5 seconds), this count will increment by 1. This will indicate high interference because the AP is holding off sending beacons, and utilization will increase.
- TX Queue stopped because full** Message buffer (Ethernet frames) in radio queue. If the radio cannot transmit due to high noise, this queue increments. When the buffer is full, all new messages are dropped. Buffer size is 150 messages.

Client

- Beacon Missed Interrupts** The number of beacons (100 msec) the client has missed from the access point.

TX Failed due to too many retries	This is the number of frames that have been lost. Original Message + 7 Retries = 1 TX failed due to too many retries. Each retry is sent within a few msec. TX Failed / TX Antenna Profile = Frame Packet Loss Rate (number undelivered as a %).
RX Failed due to bad CRC	This can be from any access point, not only your own. If there are other Wi-Fi networks in the area, this number could be high due to other encryption keys and weak signals. RX Failed / RX Antenna Profile = RX Frame Error Rate (this can be high due to other wireless devices in the area).
Broadcast Notes	When a broadcast message is sent from client to the access point, the access point will always ACK the client. When a broadcast message is sent from the access point to the client, no ACK is returned.
Management Frames	Management frames can be probes, authenticate/associate messages, RTS messages, and beacons.

Network Traffic Analysis

There are many devices and PC programs that will analyze performance of an Ethernet network. Freely available programs, such as Ethereal, provide a simple cost-effective means for more advanced analysis. By monitoring traffic on the wired Ethernet, a better idea of regular traffic can be gained. Network analysis programs make configuration of a filter for the WI-MOD-E a simple task.

4.6 System Tools

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

Configuration Summary	This option is used to save all the different configuration pages onto one page for easy viewing. The page can also be saved (using the File/Save As function on the drop File Menu) for future reference and for emailing module configuration details to Weidmuller technical support in the event of a configuration problem.
TCP Throughput Test	Performs a throughput test. For more information, see “4.4 Throughput Test.”
Radio Path Test	Performs a radio path test without the use of a laptop, and provides a visual indication of RSSI and throughput on the front panel LEDs.
Read Configuration File	This option shows the module configuration in XML format. This file can be saved for future reference.
Write Configuration File	Any configuration XML files saved using Read Configuration File above can be loaded back into the module using this option.
Firmware Upgrade	This option is used for firmware upgrades. Load the file using the Browse button. When the file is found, click Send to load the file into the module. When completed, click Reset. Firmware upgrades can be performed locally or remotely via the radio.

System Log File	Shows an event log of the modules operation, used for diagnosing problems. The page can be saved and emailed to Weidmuller if requested. "Clear System Log" will clear the log file and start fresh.
Reset	Resets the module.
Factory Default Configuration	Loads the factory default configuration and resets the module.



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

4.7 Testing Radio Paths

Connection and Signal Strength

The general procedure for radio range testing a link is fairly simple. Configure two units to form a link using automatic radio rates. Install the access point at a fixed location. Take a laptop computer and the client to each of the remote locations, and analyze the link using the Connectivity webpage. If a beacon is heard from the access point, the client will update its Connectivity webpage with the received signal strength of beacon messages from the access point.

If the signal is strong enough, a link may be established and the Connectivity webpage of the access point may be opened. If the link is weak, the LINK LED will turn off and the remote Connectivity webpage of the access point will fail to load. Using this procedure, the signal strengths of units at both locations may be analyzed, and traffic is sent between the units while remote webpages are opened.

Iperf Throughput Test

A more thorough test of radio paths is a throughput test, which will check the amount of data that can be reliably achieved via the wireless link. There are a number of software tools that you can use to check the data throughput, such as FTP (File Transfer Protocol), Iperf, and Qcheck. The preferred application is "Iperf," which has been configured in each modem and can be enabled to perform this test. It can also be run externally using laptops at either end of the radio link. The Iperf/Jperf application can be downloaded from <http://sourceforge.net/projects/iperf/>.

All of the above applications measure the raw data throughput. From this you can determine the amount of interference from the measured and calculated data throughput levels. The way Iperf works is that a server is enabled at one end of the link and a client at the other. The Iperf client then passes data over the link and calculates and displays the throughput accordingly.

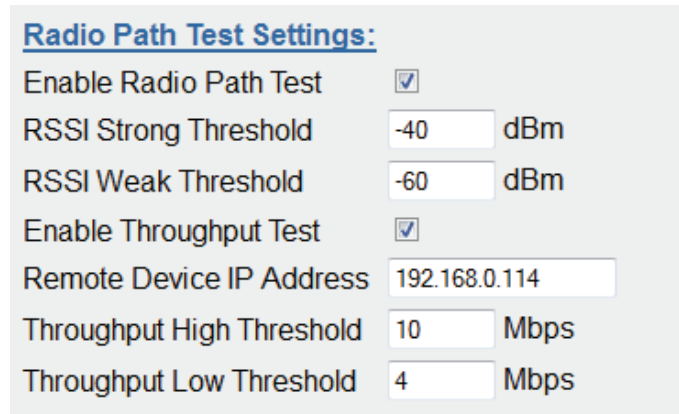
The Iperf server can be run internally on the modem by enabling this feature on the Advanced Radio page of one of the modems (see "4.4 Throughput Test"). It can also be run externally on a PC or laptop connected at each end of the radio link. For a detailed procedure on using Iperf to externally check radio data throughput, see "Appendix D- EXTERNAL IPERF TEST."

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

Internal Radio Test

The module also has an internal Radio Path test that will allow you to perform a basic radio path test without the need for a laptop or PC. Two tests that can be run—RSSI, and Throughput. The throughput test can be disabled independently from the RSSI test, but disabling the RSSI test will turn off both tests. Typically, the radio path test should be enabled at a modem configured as a client or station

⚠ NOTE The Radio Path Test feature should not be enabled on a live system. It is intended for testing only.



The screenshot shows a configuration page titled "Radio Path Test Settings:". It contains several settings:

- Enable Radio Path Test:** A checked checkbox.
- RSSI Strong Threshold:** A text input field containing "-40" followed by "dBm".
- RSSI Weak Threshold:** A text input field containing "-60" followed by "dBm".
- Enable Throughput Test:** A checked checkbox.
- Remote Device IP Address:** A text input field containing "192.168.0.114".
- Throughput High Threshold:** A text input field containing "10" followed by "Mbps".
- Throughput Low Threshold:** A text input field containing "4" followed by "Mbps".

Figure 92 Radio Path Tests

Radio Path Test Settings

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

RSSI

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

Throughput

The second test is the throughput test, which when enabled performs a basic throughput test between the access point and the client. The configurable remote device IP address should specify the IP address of the access point.

NOTE The on-board Iperf server must be enabled at the access point prior to running this test.

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

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

The radio path test can be accessed by selecting the link from the System Tools page and then selecting the “Enable Radio Path Test” option and entering the appropriate thresholds levels to indicate RSSI and throughput and the IP address of the Iperf server (normally the access point).

Figure 93 shows the indications you will see using the configuration above.

- The OK LED will flash between red and green, which indicates that the module is in a diagnostic Radio Test mode.
- RS-232 LED is green, indicating the RSSI to the access point is greater than -40 dB. If the RS232 LED were red, it would indicate the RSSI level was greater than -60 dB.
- RS-485 LED is green, indicating the throughput to the access point is greater than 10 Mbps. If the LED were red, it would mean the throughput is between 10 Mbps and 4 Mbps.

NOTE Advanced configuration settings such as Serial or I/O Transfer should be disabled, and if using the throughput test, the Iperf server option on the Advanced Radio Settings page for the access point must be enabled.

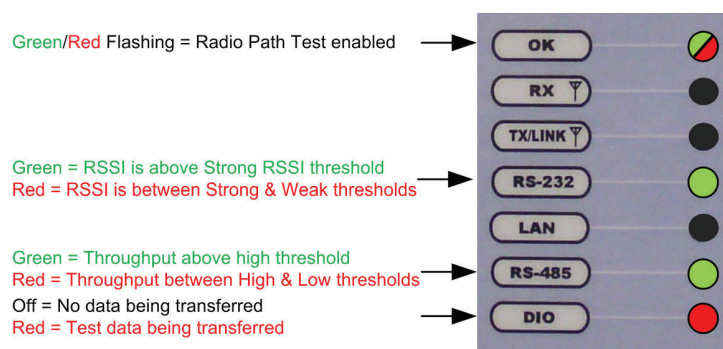


Figure 93 Throughput Test LEDs

4.8 Remote Configuration

Because a module configuration is viewed and changed in a Web format (which uses TCP/IP protocol), you can view or change the configuration of a remote module via the wireless link, provided the remote module already has a wireless link established to the local WI-MOD-E. To perform a remote configuration, connect a PC to the local module, run Internet Explorer and enter the IP address of the remote unit (or device name if using DNS). The Configuration page of the remote module will appear and changes can be made.

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

It is advisable to determine the path of the links to the modules you wish to modify and draw a tree diagram, if necessary. Modify the modules at the “leaf nodes” of your tree diagram. These will be the furthest away from your connection point in terms of the number of radio or Ethernet links. In a simple system, this usually means modifying the client modules first and the access point last.

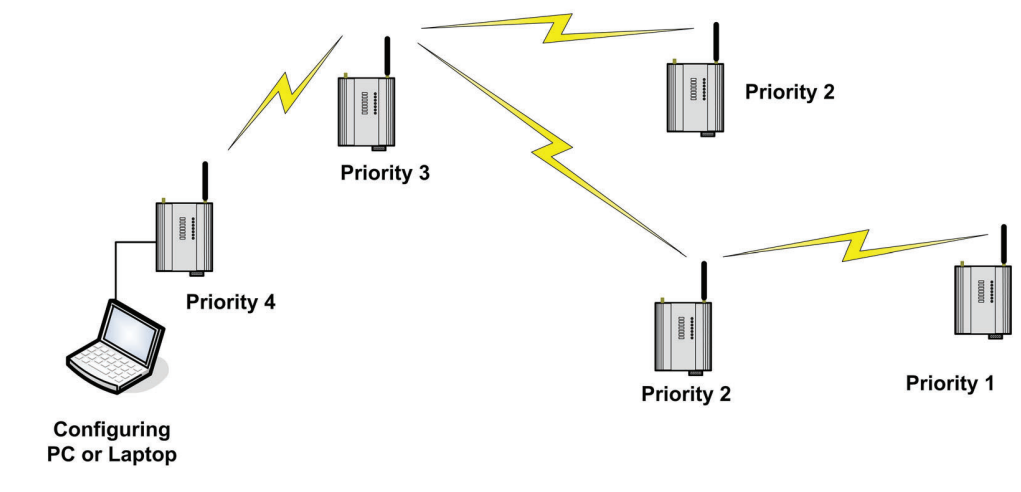


Figure 94 Remote Configuration

4.9 Internal Diagnostics Modbus Registers

There are a number of internal diagnostic registers that can be accessed via Modbus TCP/RTU that will help with analyzing and diagnosing the radio network. To access these registers, the Modbus server needs to be enabled and a Modbus server address needs to be configured. For details, see “3.15 Modbus I/O Transfer.” After enabling the Modbus client, you can access the following information by reading the corresponding Modbus address at the server ID address.

NOTE The normal default interface is “wi0.” If additional interfaces are added by entering virtual WDS connections (either client or access point) as described in “3.17 Repeaters (WDS),” they will take on the next available interface number (wi1, wi2, and so on).

Connection Information

Register	Module	Description
5000	Both	Total number of associated stations.
5001	Both	Current radio channel. See “3.9 Radio Configuration” for channel details.
5002	Both	Number of wireless interfaces configured, including virtual interfaces wi1–wi10.
5010	Both	Wireless adapter (wi0) – link status.
5011	Both	Wireless adapter (wi0) – link status inverted.
5012	Both	Wireless adapter (wi0) – number of associated stations for this interface.
5013	AP Only	Wireless adapter (wi0) – points to the starting register of the access point’s station list. First interface (wi0) will always start at 5200 and dynamically enter data depending on the number of STAs. The remaining interfaces (wi1-wi10) will be entered after wi0 data. Register 5023, 5033 (and so on) will indicate the starting location for each interface.
5014	STA Only	Wireless adapter (wi0) – RSSI and BGND of RX message from the access point, for example, hexadecimal 5F5D = 5D for RSSI, and 5F for BGND. (Convert the value from hexadecimal to decimal and add a “-”. For example, 5F = -95dB.)
5015	STA Only	Wireless adapter (wi0) – Transmit data rate from the access point.
5016	STA Only	Wireless adapter (wi0) – MAC address of the access point.
5020-5026	As per 5010-5016	As per registers 5010–5016, but for the next wireless adapter (wi1).
5030-5036	As per 5010-5016	As per registers 5010–5016, but for the next wireless adapter (wi2).
5040-5046	As per 5010-5016	As per registers 5010–5016, but for the next wireless adapter (wi3).
...etc	As per 5010-5016	As per registers 5010–5016, but for the next wireless adapter (wi10).
5200	AP Only	RSSI of the client (STA).
5201	AP Only	Transmit data rate to client (STA).
5202	AP Only	MAC address of client (STA).
...etc	AP Only	Dynamic list of STAs. Refer to register 5023, 5033 (and so on) for the starting register of each wi interface.
9999	Both	Reset the module (enter FFFF to reset module).

Statistic Registers

Register	Module	Description
4500	Both	Total data packets received on the interface.
4502	Both	Received frames with antenna 1 (TX/RX).
4504	Both	Received frames with antenna 2 (RX).
4506	Both	Receiver / default antenna switches.
4508	Both	Receive message failed due to bad CRC.
4510	Both	Receive message failed due to decryption.
4512	Both	Receive message failed due to MIC failure.
4514	Both	Receive message failed due to FIFO overrun.
4516	Both	Beacon missed interrupts.
4518	Both	Total data packet sent on the interface.
4520	Both	Transmit frames with antenna 1 (TX/RX).
4522	Both	Transmit frames with antenna 2 (RX).

Register	Module	Description
4524	Both	Transmitter antenna switches.
4526	Both	Transmitter on-chip retries.
4528	Both	Transmit message failed due to too many retries.
4530	Both	Transmit frames with alternate rate.
4532	Both	Transmit frames with no ACK marked (such as broadcast, multicast).
4534	Both	Management frames transmitted.
4536	Both	Transmit frames with RTS enabled.
4538	Both	Transmit frames with CTS enabled.
4540	Both	Beacons transmitted.
4542	Both	Beacon missed count.
4544	Both	Beacon miss reset count.
4546	Both	Transmit message failed due to no TX buffer (data).
4548	Both	Fatal hardware error interrupts.
4550	Both	Receiver PHY error summary count.
4552	Both	Transmitter queue stopped because it is full.

4.10 Utilities

ping

Ping is a basic Internet program that lets you verify that a particular IP address exists and can accept requests. Ping is used diagnostically to ensure that a host computer or device that you are trying to reach is actually operating. For example, if a user cannot ping a host, the user will be unable to send files to that host. Ping operates by sending a packet of data to a designated address and waiting for a response.

The basic operation of ping can be performed by following these steps in any Windows operating system.

1. Click the Start menu and choose Run.
2. Type "cmd" and press Enter.
You should see the command screen come up. There will be a certain directory specified (unique to your own PC) with a flashing cursor.
3. At the cursor, type the word "ping" followed by a space and the default IP address for the WI-MOD-E at first startup.
This command would be written as "ping 192.168.0.118". Press Enter to send the ping command. The PC will reply with an acknowledgment of the command, and if the WI-MOD-E is correctly configured your reply will look similar to Figure 95.

```
Administrator: Command Prompt

C:\>ping 192.168.0.118

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

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

C:\>
```

Figure 95 ping Command

Figure 96 shows the response of the “ping-t 192.168.0.118” command.

```
Administrator: Command Prompt

C:\>ping -t 192.168.0.118

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

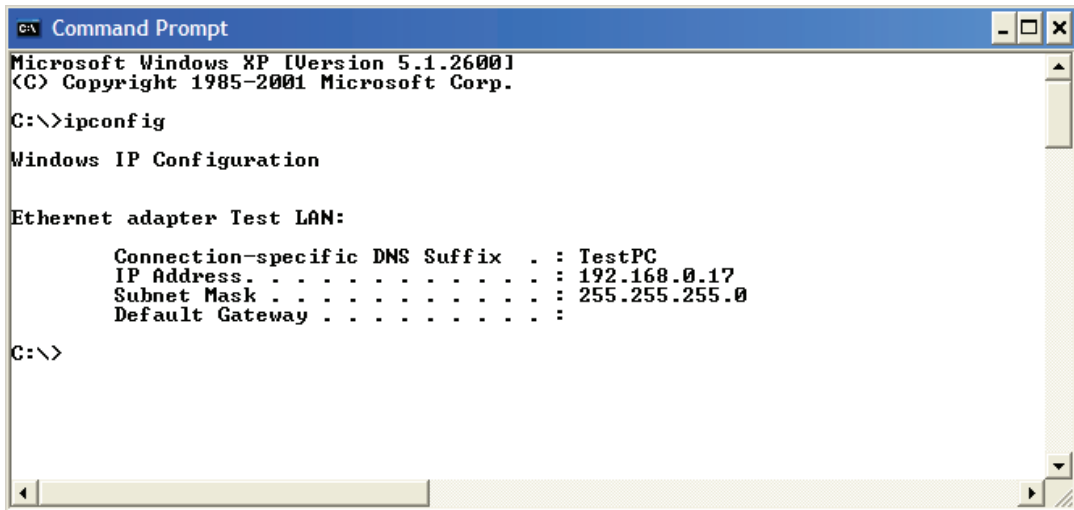
Ping statistics for 192.168.0.118:
    Packets: Sent = 14, Received = 14, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 6ms, Average = 0ms
Control-C
^C
C:\>
```

Figure 96 ping -t Command

This -t command is used to repeatedly ping the specified node in the network. To cancel, press CTRL+C. A good test for the network once it is first set up is to use “ping” repeatedly from one PC’s IP address to the other PC’s IP address. This gives a good indication of the network’s reliability and how responsive it is from point to point. When you enter CTRL+C, the program reports a packet sent-received-lost percentage.

ipconfig

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



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

C:\>ipconfig

Windows IP Configuration

Ethernet adapter Test LAN:

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

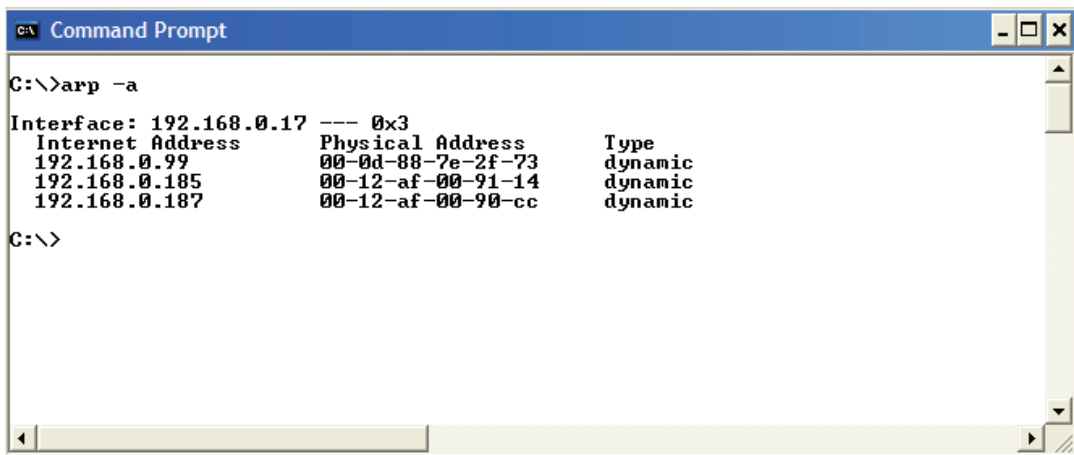
C:\>
```

Figure 97 Ipconfig Command

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

arp

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



```
C:\>arp -a

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

C:\>
```

Figure 98 arp Command

The command used in Figure 98 is “arp-a”. It shows the PC’s IP address (like the previous ipconfig command). In this case the IP address is still 192.168.0.17. It also shows the IP address and associated MAC address of any another device that has a connection to it.

The command “arp-?” lists the commands available for this function.

route

The “route” command is used for the router function. This is where you are joining two different networks together via the WI-MOD-E. Refer to “1.1 Getting Started Quickly” for details.

Normally the WI-MOD-E will only accept one routing rule, by using the default gateway IP address on the Main Network page. If more than one routing rule is needed (for example, for multiple networks each with a different IP range), a routing table is required. In the example in Figure 99, a routing rule needs to be entered into the Network A’s PC which will allow access between Network A and Network B. This can be entered at the command prompt using the following instructions.

- route PRINT will show all active routes on PC.
- route ADD will add a routing table to network.
- route DELETE <destination netmask gateway interface> will delete the unwanted routing table.
- route CHANGE modifies an existing route.

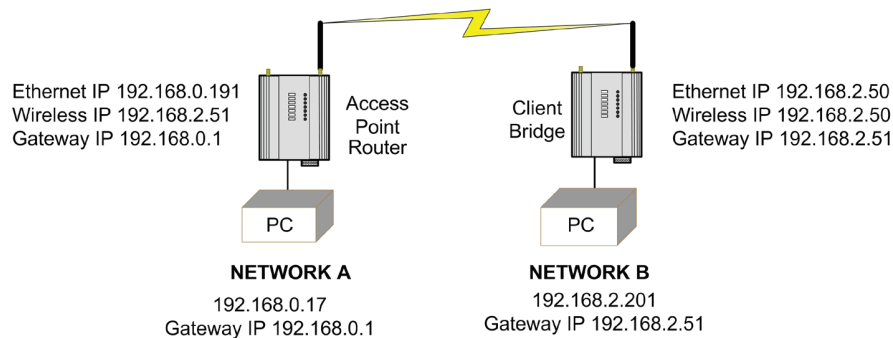


Figure 99 Route

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

Access Point Router Settings

Gateway IP 192.168.0.1
 Ethernet IP 192.168.0.191
 Subnet Mask 255.255.255.0
 Wireless IP 192.168.2.051
 Subnet Mask 255.255.255.0

Client Bridge Settings

Gateway IP 192.168.2.51
 Ethernet IP 192.168.2.50
 Subnet Mask 255.255.255.0
 Wireless IP 192.168.2.50
 Subnet Mask 255.255.255.0

Network A Settings

IP Address 192.168.0.17
 Subnet Mask 255.255.255.0
 Gateway IP 192.168.0.1

Network B Settings

IP Address 192.168.2.201
 Subnet Mask 255.255.255.0
 Gateway IP 192.168.2.51

In the Network A PC, a routing rule needs to be set. This will allow Network A and B to have access to each other. This is entered under the cmd prompt, as follows:

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

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

IP address 192.168.2.0 will allow everything on this network to be shared by the router. When adding a routing table you will need to enter this address. Once entered, the router will determine whether to pass information over the router if it is addressed to do so or not. For added security, MAC address filtering could be added, as discussed earlier in “3.19 Filtering.”

Chapter 5 - SPECIFICATIONS

Transmitter/Receiver	
Frequency	2.412–2.472GHz ⁽¹⁾ 5.150–5.825GHz ⁽²⁾
Transmit Power	15–630 mW (Data rate, model type and country specific)
Transmission	Direct Sequence Spread Spectrum (DSSS) ^(1, 2)
Modulation	Orthogonal Frequency Data Modulation (OFDM) ^(1, 2)
Receiver Sensitivity	–100 dBm @ 250 kbps, 74 dBm @ 108 Mbps (8% FER) ⁽¹⁾ –95 dBm @ 6 Mbps, 74 dBm @ 108 Mbps (8% FER) ⁽²⁾
Channel Spacing	5 MHz spacing (13 channels, 2.412 – 2.472GHz) ⁽¹⁾ 20 MHz spacing (27 channels, 5.150 – 5.8GHz) ⁽²⁾
Data Rate	1–108 Mbps ⁽¹⁾ 6–108 Mbps ⁽²⁾
Range (LoS)	6 mi (10 Km) @ 400 mW ^(1, 3) 3 mi (5Km) @ 400 mW ^(2, 3) 9 mi (15Km) @ 630 mW ^(2, 3)
Antenna Connector	2 x Female SMA Standard Polarity ⁽⁴⁾ 1 x Female SMA Standard Polarity on WI-MOD-E-A1 and WI-MOD-E-G1
Input/Output	
Discrete I/O	Input Voltage-Free Contact ⁽⁵⁾ Output FET 30 Vdc 500mA ⁽⁵⁾
Ethernet Port	
Ethernet Port	10/100baseT; RJ45 Connector – IEEE 802.3
Link Activity Linkc	100baseT via LED
Serial Port	
RS232	DB9 Female DCE; RTS/CTS/DTR/DCD
RS485	2-Pin Terminal Block – Non-isolated ⁽⁶⁾
Data Rate (Bps)	1200, 2400, 4800, 9600, 14400, 19200, 38400, 57600, 76800, 115200, 230400 Bps
Serial Settings	7/8 Data Bits; Stop/Start/Parity (Configurable)
Protocols/Configuration	
System Address	ESSID; 1–31 Character Text String
Protocols Supported	TCP/IP, UDP, ARP, SNMP, RADIUS/802.1x, DHCP, DNS, PPP, ICMP, HTTP, FTP, TFTP, TELNET, MODBUS and MODBUS-TCP
User Configuration	User Configurable Parameters via HTTPS Embedded Web Server
Configurable Parameters	Access Point/Client/Bridge/Router Point-to-Point, Point-to-Multi-Point Wireless Distribution System (AP- AP Repeater) Modbus TCP/RTU Gateway Serial Client/Server/Multicast Simultaneous RS232/485 Connection Embedded Modbus Master/Slave for I/O Transfer

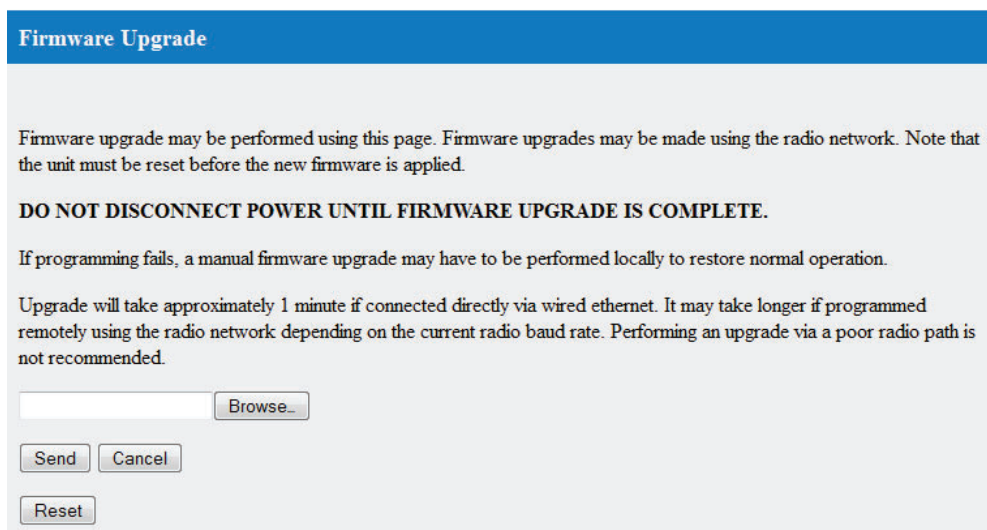
Security	Data Encryption – 802.11i With CCMP 128bit AES Support for 802.1x Radius Server Secure HTTP Protocol
Bandwidth Protection	MAC Address – Whitelist/Blacklist IP Filtering – Whitelist/Blacklist ARP/GARP Filtering – Whitelist/Blacklist
LED Indication/Diagnostics	
LED Indication	Power/OK; RX; TX/Link; RS232; LAN; RS485; Digital I/O status. Please refer to the product manual for further information.
Reported Diagnostics	RSSI Measurements (dBm); Connectivity Information/Statistics; System Log file
Network Management	Optional Network Management System
Compliance	
EMC	FCC Part 15; EN 301 489 – 17; AS/NZS CISPR22
RF (Radio)	EN 300 328 ⁽¹⁾ ; EN 301 893 ⁽²⁾ ; FCC Part 15; RSS 210
Hazardous Area	CSA Class I, Division 2; ATEX; IECEx nA IIC (WI-MOD-E-G1 & WI-MOD-E-A1 Only)
Safety	IEC 60950 (RoHS Compliant)
UL	UL Listed
General	
Size	4.5" x 5.5" x 1.2" (114 mm x 140 mm x 30 mm)
Housing	Powder-Coated Aluminum
Mounting	DIN Rail
Terminal Blocks	Removable; Max conductor 12 AWG (2.5 mm ²)
Temperature Rating	–40 to +140°F (–40 to +60°C)
Humidity Rating	0–99% RH noncondensing
Weight	1.0 lb (0.45 kg)
Pollution Degree	2- Not sealed, not subject to dust, dirt, condensation.
Installation Category	2- Transient voltages are not higher than 2.5 kV at 250 Vac supply.
Ingress Protection	IP 20
Altitude	2000 m
Power Supply	
Nominal Supply	9 to 30 Vdc; Under/Over Voltage Protection
Average Current Draw	270 mA @ 12 V (Idle); 140 mA @ 24 V (Idle)
Transmit Current Draw	470 mA @ 12 V (400 mW); 250 mA @ 24 V (400 mW)
<p>NOTE Specifications subject to change.</p> <p>1 Order option for 802.11b/g.</p> <p>2 Order option for 802.11a.</p> <p>3 Typical maximum line-of-sight range.</p> <p>4 Supports signal diversity or high gain antenna.</p> <p>5 Can be used to transfer I/O status or communications failure output.</p> <p>6 Maximum distance 1200 meters.</p>	

Appendix A - FIRMWARE UPGRADE

Determine the firmware version present in the module to be upgraded by viewing the index webpage of the module. Firmware versions 1.0.3 and later may be upgraded via the Configuration webpages. This upgrade can be executed locally with a PC connected directly to the module, or remotely over a working radio link. For remote upgrades, it is advisable to reduce radio traffic over the link from other devices as much as possible. If necessary, create a temporary separate radio network to perform the upgrade to remote modules.

Web-based Upgrade

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



The screenshot shows a web interface titled "Firmware Upgrade" with a blue header. The main content area is light gray and contains the following text:

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

DO NOT DISCONNECT POWER UNTIL FIRMWARE UPGRADE IS COMPLETE.

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

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

Below the text, there is a file upload section with an empty text input field and a "Browse..." button. At the bottom of the form, there are three buttons: "Send", "Cancel", and "Reset".

Figure 100 Firmware Upgrade

Appendix B - GLOSSARY

ACK	Message acknowledgment.
Access Point	An access point connects wireless network stations (or clients) to other stations within the wireless network and also can serve as the point of interconnection between the wireless network and a wired network. Each access point can serve multiple users within a defined network area. Also known as a base station.
Ad-Hoc Network	Ad hoc network often refers to a mode of operation of IEEE 802.11 wireless networks. An ad hoc network is any set of networks where all devices have equal status on a network and are free to associate with any other ad hoc network device in link range. Each node participates in routing by forwarding data for other nodes, so the determination of which nodes forward data is made dynamically on the basis of network connectivity.
Antenna Gain	Antennae do not increase the transmission power, but instead focus the signal. Rather than transmitting in every direction (including the sky and ground), antenna focus the signal more horizontally or in one particular direction. This gain is measured in decibels.
Bandwidth	The maximum data transfer speed available to a user through a network.
Bridge	A bridge connects two local area networks, and is typically used to connect wireless networks to wired networks. Bridges usually transfer messages between networks only when the message destination is on the other network. Messages destined for the network on which they originated are not passed on to the other network. This reduces traffic on the entire network.
Collision Avoidance	A network node procedure for proactively detecting that it can transmit a signal without risking a collision with transmissions from other network nodes.
Client / Sta / Station	A device on a network that gains access to data, information, and other devices through a server (access point).
Crossover Cable	A cable used for networking two computers without the use of a hub. Crossover cables may also be required for connecting a cable or DSL modem to a wireless gateway or access point. The cable is wired so that the signals “crossover,” connecting transmit signal on one side to receiver signals on the other.
CSMA/CA	<p>Carrier sense multiple access/collision avoidance (CSMA/CA) is a “listen before talk” method of minimizing (but not eliminating) collisions caused by simultaneous transmission by multiple radios. IEEE 802.11 states that a collision avoidance method rather than collision detection must be used because the standard employs half-duplex radios, which are capable of transmission or reception but not both simultaneously.</p> <p>Unlike conventional wired Ethernet nodes, a WLAN station cannot detect a collision while transmitting. If a collision occurs, the transmitting station will not receive an ACKnowledge packet from the intended receive station. For this reason, ACK packets have a higher priority than all other network traffic. After completion of a data transmission, the receive station will begin transmission of the ACK packet before any other node can begin transmitting a new data packet. All other stations must wait a longer pseudo-randomized period of time before transmitting. If an ACK packet is not received, the transmitting station will wait for a subsequent opportunity to retry the transmission.</p>

CSMA/CD	Carrier sense multiple access/collision detection (CSMA/CD) is the access method used on an Ethernet network. A network device transmits data after detecting that a channel is available. However, if two devices transmit data simultaneously, the sending devices detect a collision and retransmit after a random time delay.
DHCP	Dynamic Host Configuration Protocol (DHCP) is a utility that enables a server to dynamically assign IP addresses from a predefined list and limit their time of use so that they can be reassigned. Without DHCP, an IT manager would need to manually enter all the IP addresses of all the computers on the network. When DHCP is used, whenever a computer logs onto the network, an IP address is automatically assigned to it.
Dial-up	A communication connection via the standard telephone network, or plain old telephone service (POTS).
DNS	Domain name service (DNS) is a program that translates URLs to IP addresses by accessing a database maintained on a collection of Internet servers. The program works behind the scenes to facilitate surfing the Web with alpha versus numeric addresses. A DNS server converts a name like mywebsite.com to a series of numbers like 107.22.55.26. Every website has its own specific IP address on the Internet.
DSL	Digital subscriber line (DSL) is a family of technology protocols for high-speed data, voice and video transmission over ordinary twisted-pair copper plain old telephone service (POTS) telephone wires.
Encryption Key	An alphanumeric (letters and/or numbers) series that enables data to be encrypted and then decrypted so it can be safely shared among members of a network. WEP uses an encryption key that automatically encrypts outgoing wireless data. On the receiving side, the same encryption key enables the computer to automatically decrypt the information so that it can be read. Encryption keys should be kept secret.
Firewall	A device or computer program that keeps unauthorized users out of a private network. Everything entering or leaving a system's internal network passes through the firewall and must meet the system's security standards in order to be transmitted. Often used to keep unauthorized people from using systems connected to the Internet.
Hub	A multiport device used to connect PCs to a network via Ethernet cabling or via 802.11. Wired hubs can have numerous ports and can transmit data at speeds ranging from 10 Mbps to multi-Gigabyte speeds per second. A hub transmits packets it receives to all the connected ports. A small wired hub may only connect 4 computers; a large hub can connect 48 or more.
Hz	Hertz. The international unit for measuring frequency, equivalent to the older unit of cycles-per-second. One megahertz (MHz) is one million hertz. One gigahertz (GHz) is one billion hertz. The standard US electrical power frequency is 60 Hz, the AM broadcast radio frequency band is 535–605 kHz, the FM broadcast radio frequency band is 88–108 MHz, and wireless 802.11b/g LANs operate at 2.4 GHz.
IEEE	Institute of Electrical and Electronics Engineers, New York, www.ieee.org . A membership organization that includes engineers, scientists and students in electronics and allied fields. IEEE has more than 300,000 members and is involved with setting standards for computers and communications.

Infrastructure Mode	An 802.11 setting providing connectivity to an access point. As compared to ad-hoc mode, whereby 802.11 devices communicate directly with each other, clients set in Infrastructure mode all pass data through a central AP. The AP not only mediates wireless network traffic in the immediate neighborhood, but also provides communication with the wired network.
I/O	Input/Output. The term used to describe any operation, program, or device that transfers data to or from a computer.
Internet Appliance	A computer that is intended primarily for Internet access, is simple to set up, and usually does not support installation of third-party software. These computers generally offer customized Web browsing, touch-screen navigation, e-mail services, entertainment, and personal information management applications.
IP	Internet Protocol. A set of rules used to send and receive messages across local networks and the Internet.
IP Telephony	Technology that supports voice, data, and video transmission via IP-based LANs, WANs, and the Internet. This includes VoIP (Voice over IP).
IP Address	A 32-bit number that identifies each sender or receiver of information that is sent across the Internet. An IP address has two parts—an identifier of a particular network on the Internet and an identifier of the particular device (a server or a workstation) within that network.
IPX-SPX	Internetwork Packet Exchange (IPX) is a networking protocol used by the Novell NetWare® operating systems. Like UDP/IP, IPX is a datagram protocol used for connectionless communications. Higher-level protocols, such as Sequenced Packet Exchange (SPX) and NCP, are used for additional error recovery services. SPX is a transport layer protocol (layer 4 of the OSI Model) used in Novell Netware networks. The SPX layer sits on top of the IPX layer (layer 3) and provides connection-oriented services between two nodes on the network. SPX is used primarily by client/server applications.
ISDN	A type of broadband Internet connection that provides digital service from the customer's premises to the dial-up telephone network. ISDN uses standard POTS copper wiring to deliver voice, data, or video.
ISO Network Model	A network model developed by the International Standards Organization (ISO) that consists of seven different levels, or layers. By standardizing these layers, and the interfaces in between, different portions of a given protocol can be modified or changed as technologies advance or systems requirements are altered. The seven layers are Physical, Data Link, Network, Transport, Session, Presentation, Application.
LAN	Local Area Network. A system of connecting PCs and other devices within the same physical proximity for sharing resources such as an Internet connections, printers, files, and drives.
Receive Sensitivity	The minimum signal strength required to pick up a signal. Higher bandwidth connections usually have less receive sensitivity than lower bandwidth connections.
Router	A device that forwards data from one WLAN or wired local area network to another.
SNR	Signal to noise ratio (SNR) is the number of decibels difference between the signal strength and background noise.
Transmit Power	The power at which the wireless devices transmits (usually expressed in mW or dBm).

MAC Address	<p>Media Access Control (MAC) address is a unique code that is permanently assigned to most forms of networking hardware. Limiting a wireless network's access to hardware, such as wireless cards, is a security feature employed by closed wireless networks. But an experienced hacker armed with the proper tools can still figure out an authorized MAC address, masquerade as a legitimate address, and access a closed network.</p> <p>Every wireless 802.11 device has its own specific MAC address hard-coded into it. This unique identifier can be used to provide security for wireless networks. When a network uses a MAC table, only the 802.11 radios that have had their MAC addresses added to that network's MAC table will be able to get onto the network.</p>
NAT	<p>Network address translation (NAT) is a network capability that enables a number of computers to dynamically share a single incoming IP address from a dial-up, cable, or xDSL connection. NAT takes the single incoming IP address and creates new IP address for each client computer on the network.</p>
NIC	<p>Network interface card (NIC) is a type of PC adapter card that either works without wires (Wi-Fi) or attaches to a network cable to provide two-way communication between the computer and network devices, such as a hub or switch. Most office wired NICs operate at 10 Mbps (Ethernet), 100 Mbps (Fast Ethernet) or 10/100 Mbps dual speed. High-speed Gigabit and 10 Gigabit NIC cards are also available.</p>
Proxy Server	<p>Used in larger companies and organizations to improve network operations and security, a proxy server is able to prevent direct communication between two or more networks. The proxy server forwards allowable data requests to remote servers and/or responds to data requests directly from stored remote server data.</p>
RJ-45	<p>Standard connectors used in Ethernet networks. RJ-45 connectors are similar to standard RJ-11 telephone connectors, but RJ-45 connectors can have up to eight wires, whereas telephone connectors have four.</p>
Server	<p>A computer that provides its resources to other computers and devices on a network. These include print servers, Internet servers, and data servers. A server can also be combined with a hub or router.</p>
Site Survey	<p>The process whereby a wireless network installer inspects a location prior to installing a wireless network. Site surveys are used to identify the radio- and client-use properties of a facility so that access points can be optimally placed.</p>
SSL	<p>Secure Sockets Layer (SSL) is an encryption scheme commonly used by many online retail and banking sites to protect the financial integrity of transactions. When an SSL session begins, the server sends its public key to the browser. The browser then sends a randomly generated secret key back to the server in order to have a secret key exchange for that session</p>
Sub Network or Subnet	<p>Found in larger networks, these smaller networks are used to simplify addressing between numerous computers. Subnets connect together through a router.</p>
Switch	<p>A type of hub that efficiently controls the way multiple devices use the same network so that each can operate at optimal performance. A switch acts as a networks traffic cop. Rather than transmitting all the packets it receives to all ports as a hub does, a switch transmits packets to only the receiving port.</p>

TCP	Transmission Control Protocol (TCP) is a protocol used along with the Internet Protocol (IP) to send data in the form of individual units (called packets) between computers over the Internet. While IP takes care of handling the actual delivery of the data, TCP takes care of keeping track of the packets that a message is divided into for efficient routing through the Internet. For example, when a webpage is downloaded from a web server, the TCP program layer in that server divides the file into packets, numbers the packets, and then forwards them individually to the IP program layer. Although each packet has the same destination IP address, it may get routed differently through the network. At the other end, TCP reassembles the individual packets and waits until they have all arrived to forward them as single message.
TCP/IP	The underlying technology behind the Internet and communications between computers in a network. The first part, TCP, is the transport part, which matches the size of the messages on either end and guarantees that the correct message has been received. The IP part is the user's computer address on a network. Every computer in a TCP/IP network has its own IP address that is either dynamically assigned at startup or permanently assigned. All TCP/IP messages contain the address of the destination network as well as the address of the destination station. This enables TCP/IP messages to be transmitted to multiple networks (subnets) within an organization or worldwide.
VoIP	Voice over Internet Protocol (VoIP). Voice transmission using Internet Protocol to create digital packets distributed over the Internet. VoIP can be less expensive than voice transmission using standard analog packets over POTS (plain old telephone service).
VPN	Virtual private network (VPN) is a type of technology designed to increase the security of information transferred over the Internet. VPN can work with either wired or wireless networks, as well as with dial-up connections over POTS. VPN creates a private encrypted tunnel from the end user's computer, through the local wireless network, through the Internet, all the way to the corporate servers and database.
WAN	Wide area network (WAN) is a communication system of connecting PCs and other computing devices across a large local, regional, national or international geographic area. Also used to distinguish between phone-based data networks and Wi-Fi. Phone networks are considered WANs and Wi-Fi networks are considered wireless local area networks (WLANS).
WEP	Wired Equivalent Privacy (WEP) is basic wireless security provided by Wi-Fi. In some instances, WEP may be all a home or small-business user needs to protect wireless data. WEP is available in 40-bit (also called 64-bit), or in 108-bit (also called 128-bit) encryption modes. As 108-bit encryption provides a longer algorithm that takes longer to decode, it can provide better security than basic 40-bit (64-bit) encryption.
Wi-Fi	Wireless fidelity (Wi-Fi) is an interoperability certification for wireless local area network (LAN) products based on the Institute of Electrical and Electronics Engineers (IEEE) 802.11 standard.

Appendix C - CHANNELS

802.11b/g

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

802.11b/g Turbo

Channel	Frequency (MHz)	North America	Europe	Australia	Japan	Most of world
6	2437	Yes	Yes	Yes	Yes	Yes

802.11a – Maximum Radio Transmitter Power

Channel	Freq (MHz)	Europe Max TX Power (Master)	Europe Max TX Power (Slave)	Australia Max TX Power	NZ Max TX Power	USA Max TX Power
36	5180	23 dBm	23 dBm	23 dBm	23 dBm	17 dBm
40	5200	23 dBm	23 dBm	23 dBm	23 dBm	17 dBm
44	5220	23 dBm	23 dBm	23 dBm	23 dBm	17 dBm
48	5240	23 dBm	23 dBm	23 dBm	23 dBm	17 dBm
52	5260	20 dBm	20 dBm	20 dBm	20 dBm	24 dBm
56	5280	20 dBm	20 dBm	20 dBm	20 dBm	24 dBm
60	5300	20 dBm	20 dBm	20 dBm	20 dBm	24 dBm
64	5320	20 dBm	20 dBm	20 dBm	20 dBm	24 dBm
100	5500	26 dBm	20 dBm	20 dBm	20 dBm	24 dBm
104	5520	26 dBm	20 dBm	24 dBm	20 dBm	24 dBm
108	5540	26 dBm	20 dBm	24 dBm	20 dBm	24 dBm
112	5560	26 dBm	20 dBm	24 dBm	20 dBm	24 dBm
116	5580	26 dBm	20 dBm	24 dBm	20 dBm	24 dBm
120	5600	26 dBm	20 dBm	n/a	20 dBm	24 dBm
124	5620	26 dBm	20 dBm	n/a	20 dBm	24 dBm

Channel	Freq (MHz)	Europe Max TX Power (Master)	Europe Max TX Power (Slave)	Australia Max TX Power	NZ Max TX Power	USA Max TX Power
128	5640	26 dBm	20 dBm	n/a	20 dBm	24 dBm
132	5660	26 dBm	20 dBm	24 dBm	20 dBm	24 dBm
136	5680	26 dBm	20 dBm	24 dBm	20 dBm	24 dBm
140	5700	26 dBm	20 dBm	24 dBm	20 dBm	24 dBm
149	5745	n/a	n/a	26 dBm	26 dBm	26 dBm
153	5765	n/a	n/a	26 dBm	26 dBm	26 dBm
157	5785	n/a	n/a	26 dBm	26 dBm	26 dBm
161	5805	n/a	n/a	26 dBm	26 dBm	26 dBm
165	5825	n/a	n/a	26 dBm	26 dBm	26 dBm

802.11a Turbo - Maximum Radio Transmitter Power

Channel	Freq (MHz)	Europe max (Master)	Europe max (Slave)	Australia max	NZ max	USA max
42	5210	23 dBm	23 dBm	23 dBm	23 dBm	17 dBm
152	5755	n/a	n/a	26 dBm	26 dBm	26 dBm
160	5795	n/a	n/a	26 dBm	26 dBm	26 dBm

802.11a and TX Power

Band & Frequency		EU & South Africa		USA		Australia		New Zealand	
U-NII Band	Frequency (MHz)	No DFS	DFS	No DFS	DFS	No DFS	DFS	No DFS	DFS
1	5150-5250	200 mW	—	50 mW	—	200 mW	—	200 mW	—
2	5250-5350	—	100 mW	—	500 mW	—	100 mW	—	100 mW
3	5470-5725	—	500 mW	—	500 mW	—	500 mW	—	500 mW
4	5725-5825	—	—	4 W	—	4 W	—	4 W	—

All power levels are shown as EIRP (Effective Isotropic Radiated Power).

dB to mWatt Conversion

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

Weidmüller – Your Solution Partner in Industrial Connectivity

Be it automotive manufacturing, electricity generation or water management – there's hardly any industry that can do without electronics and electrical connectivity today. As experienced experts we support our customers and partners around the world with products, solutions and services in the industrial environment of power, signal and data. We are continuously developing innovative, sustainable and useful products and solutions for our customer's individual needs. We are a true partner with extensive knowledge and understanding of its customer and their application. Together we set standards in Industrial Connectivity.

Weidmuller Inc

821 Southlake Blvd.
Richmond, Virginia
USA 23236
Toll-Free: (800) 849-9343
info@weidmueller.com
www.weidmuller.com

Weidmuller Ltd

10 Spy Court
Markham, Ontario
Canada L3R 5H6
Toll-Free: (800) 268-4080
orders_can@weidmueller.com
www.weidmuller.ca

Weidmuller SA de C.V.

Bld. Hermanos Serdán 698,
Col. San Rafael Oriente
Puebla, Puebla, Mexico
C.P. 72029
Telephone: 01 222 2686267
clientes@weidmuller.com.mx
www.weidmuller.com.mx