ELPRO Technologies

Read and Retain for Future Reference

Cooper Bussmann 315-WH-Series WirelessHART User Manual

Version 2.07

COOPER Bussmann

ATTENTION!

Incorrect termination of supply wires may cause internal damage and will void warranty. To ensure that your 315-WH-Series module enjoys a long life, check this user manual to verify that all connections are terminated correctly before turning on power for the first time.

CAUTION

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

AVOID

- Operating the transmitter when anyone is within 20 cm of the antenna
- Operating the transmitter before ensuring that all RF connectors are secure and any open connectors are properly terminated
- Operating the equipment near electrical blasting caps or within an explosive atmosphere

NOTE 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 ELPRO. Any changes or modifications made to the device without the written consent of ELPRO 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/coax cable combinations can be used with each radio.

Wi-Fi Antenna

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

WirelessHART™ Antenna

Manufacturer	Model Number	Coax Cable	Net
ELPRO	MD2400-EL	Includes 5 m Cellfoil	2 dBi Gain
ELPRO	SG2400-EL	CC3-SMA (3 m)	2 dBi Gain
ELPRO	Z2400-EL	CC3-SMA (3 m)	6 dBi Gain

Ensure correct antennas are connected to the appropriate antenna port.

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 ELPRO could void the user's authority to operate this equipment.

To operate this equipment legally the user must obtain a radio operating license from the government agency. This allows the government to coordinate radio users in order to minimize interference.

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

NOTE WirelessHART antennas have a much lower transmit power level, and therefore do not receive the same FCC RF Exposure requirements.

Hazardous Location Notices

This equipment is suitable for use in Class I, Division 2, Groups A, B, C and D; Tamb -40˚C to +60˚C or non-hazardous locations only.

Equipment must be powered by a suitable certified Class II power supply.

When being installed in a Class I, Division 2 hazardous area, the equipment must be installed in a suitable enclosure such that a tool is required to gain access to the connectors external to the certified equipment.

This Device complies with 94/9/EC - ATEX Directive Ex nA IIC -40°C ≤ Ta ≤ +60°C T5 Gc.

WARNING: EXPLOSION HAZARD
Do not disconnect equipment unless power has been switched off or the area is known to be non-hazardous.

The equipment is designed to be installed as a component in an enclosure that meets IP54.

Safety

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

Industry Canada

This Class [A] digital apparatus complies with Canadian ICES-003.

Important Notice

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

ELPRO radio products are used on unprotected license-free radio bands with radio noise and interference. The products are designed to operate in the presence of noise and interference, however in an extreme case, radio noise and interference could cause product operation delays or operation failure. Like all industrial electronic products, ELPRO products can fail in a variety of modes due to misuse, age, or malfunction. We recommend that users and designers design systems using design techniques intended to prevent personal injury or damage during product operation, and provide failure tolerant systems to prevent personal injury or damage in the event of product failure. Designers must warn users of the equipment or systems if adequate protection against failure has not been included in the system design. Designers must include this Important Notice in operating procedures and system manuals.

To avoid the risk of electrocution, the aerial, aerial cable, serial cables and all terminals of the 315-WH-Series 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 *315-WH-GT WirelessHART Gateway Installation Guide*.

To avoid accidents during maintenance or adjustment of remotely controlled equipment, all equipment should be first disconnected from the 315-WH-Series module. 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."

The 315-WH-Series module is not suitable for use in explosive environments without additional protection.

The 315-WH-GT operates unlicensed Radio frequencies and proprietary protocols to communicate over the radio. Nevertheless, 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.

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

A radio license is not required in some countries, provided the module is installed using the aerial and equipment configuration described in the *315-WH-GT WirelessHART Gateway Installation Guide*. Check with your local distributor for further information on regulations.

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.

Release Notice

This is the April 2013 release of the *315-WH-Series WirelessHART User Manual* version 2.07, which relates to version 2.07 modem firmware.

Follow Instructions

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

Proper Use

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

CONTENTS

Chapter 1 - INTRODUCTION 6
1.1 Products. 6
1.2 Overview 6
Key Features. 7

Chapter 2 - INSTALLATION 8
2.1 General. 8
2.2 Power/Supply. 8
2.3 System Design/Antennas. 9
Wi-Fi Radio 9
WirelessHART Radio. 10
Plant and Factory Installations 10
Line-of-sight Installations 10
Basic WirelessHART System Design 11
Antennas – Wi-Fi. 11
Antennas – WirelessHART 12
Installation Tips. 12
Dipole and Collinear Antennas 12
Directional Antennas. 13
2.4 Connections. 14
Ethernet. 14
RS232 Serial Port 14
DB9 Connector Pinouts 15
RS485 Serial Port 15
WirelessHART Communications Fail Output . 16
2.5 LED Indications 17
Front panel LEDs 17
W-HART LED 17
WirelessHART RADIO LED 18

Chapter 3 - OPERATION 19
3.1 Different Modules Types 19
Models 19
315-WH-GT in Standalone Mode 19
315-WH-GT in Gateway Mode 19
Standalone Data Concentrator 20
3.2 Ethernet Modem Features 20
3.3 WirelessHART Network Manager Module 21

Chapter 4 - CONFIGURATION. 22
4.1 Initial Network Connection. 22
Default Configuration 22
Web Interface 22
4.2 315-WH-GT Configuration. 23
Standalone Mode 23
WirelessHART Network Configurations. . . 23
HART Server Parameters 26
WirelessHART Device Table 26
Device Blacklist Table 27
Modbus Register Mapping Table 28
Connections – HART 30
Connections – Modbus 30
Gateway Mode 31
4.3 315-WH-DC Configuration. 31
315-WH-DC Module 31
WirelessHART Network Configurations. . . 31
HART Server Parameters 32
WirelessHART Device Table 33
Device Blacklist Table 34
Modbus Register Mapping Table 35
Connections – HART 36
Connections – Modbus 37

Chapter 5 - DIAGNOSTICS 38
5.1 HART Diagnostics 38
Serial WirelessHART Debug Port 38
Serial HART Debug Port 39
Monitor HART Comms 39
WirelessHART Network Topology 40
WirelessHART Device Information 41
WirelessHART Statistics 41
Network Status 41
Network Statistics 42
5.2 Wi-Fi Network 43
Connectivity 44
Channel Survey. 44
Custom Survey 46
TCP Throughput Test 47
Statistics 49
Network Traffic Analysis 50
5.3 Ethernet Utilities. 50
ping 50
ipconfig 51
arp. 52
route 52

Chapter 6 - SPECIFICATIONS. 54

Appendix A - FIRST TIME CONNECTION. 57
Accessing Configuration for the First Time 57

Appendix B - HART COMMANDS 61
HART Universal Commands 61
HART Port (Multiplexor) Specific Commands 62

Appendix C - WirelessHART COMMANDS. 63

Appendix D - GLOSSARY 65

CHAPTER 1 - INTRODUCTION

The 315-WH-Series modules provide a way of gathering data from WirelessHART field devices (such as wireless sensors, and transducers) and transmitting this information back to a HART Management System (HMS). There are a number of ways the system can be setup, depending on the infrastructure and hardware. The following pages explain the various setup options.

1.1 Products

There are two different modules in the 315-WH-Series range:

- 315-WH-DC – The WirelessHART Data Concentrator
- 315-WH-GT – The WirelessHART Gateway

Each module is designed to perform a specific function. However, the 315-WH-GT can operate as a single standalone HART Gateway and Data Concentrator, or simply as a Wi-HART Gateway. Either of these models can be configured with a Modbus interface as well as a HART interface.

1.2 Overview

The standard setup for the 315-WH Series WirelessHART is to use a 315-WH-GT Gateway as the primary communicator with the WirelessHART network. This is then paired with the 315-WH-DC Data Concentrator to provide a remote connection into the HART Management System (HMS) via the 802.11a/b/g radio link, which means the HMS does not need to be placed within the WirelessHART radio mesh coverage.

The 315-WH-DC has a physical connection to the HMS, while maintaining a connection back to the WirelessHART Gateway.

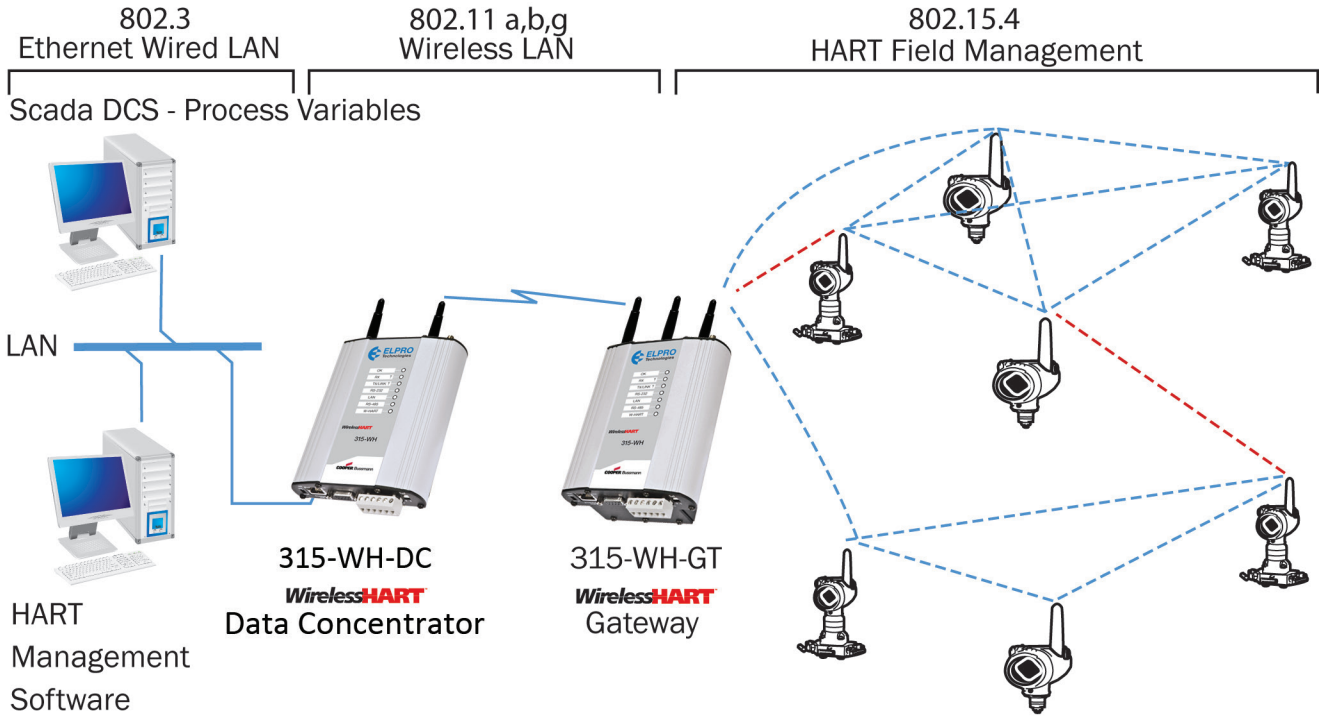


Figure 1

The 315-WH-DC Data Concentrator can have either an RS232 or an RS485 port that is commonly known as a HART Port (HPORT), which is then connected, to the HMS or Automation PC.

Either of the 315-WH-Series modules can be configured with a Modbus interface. This interface allows the process variables from the HART network to be mapped to an onboard database, which can then be accessed via the Ethernet network.

The 315-WH Series WirelessHART is a very flexible system and can operate in many different Ethernet topologies. For more information on standard Ethernet networking and configuration, this manual should be read in conjunction with the *ELPRO 245U-E Ethernet Modem User Manual*, which is available from the download section on our web site: www.cooperbussmann.com/wirelessresources

The 315-WH-GT can also be used in standalone fashion by combining the Data Concentrator and the Gateway into the same module. However, this does not allow the remote Wi-Fi link back to the HMS.

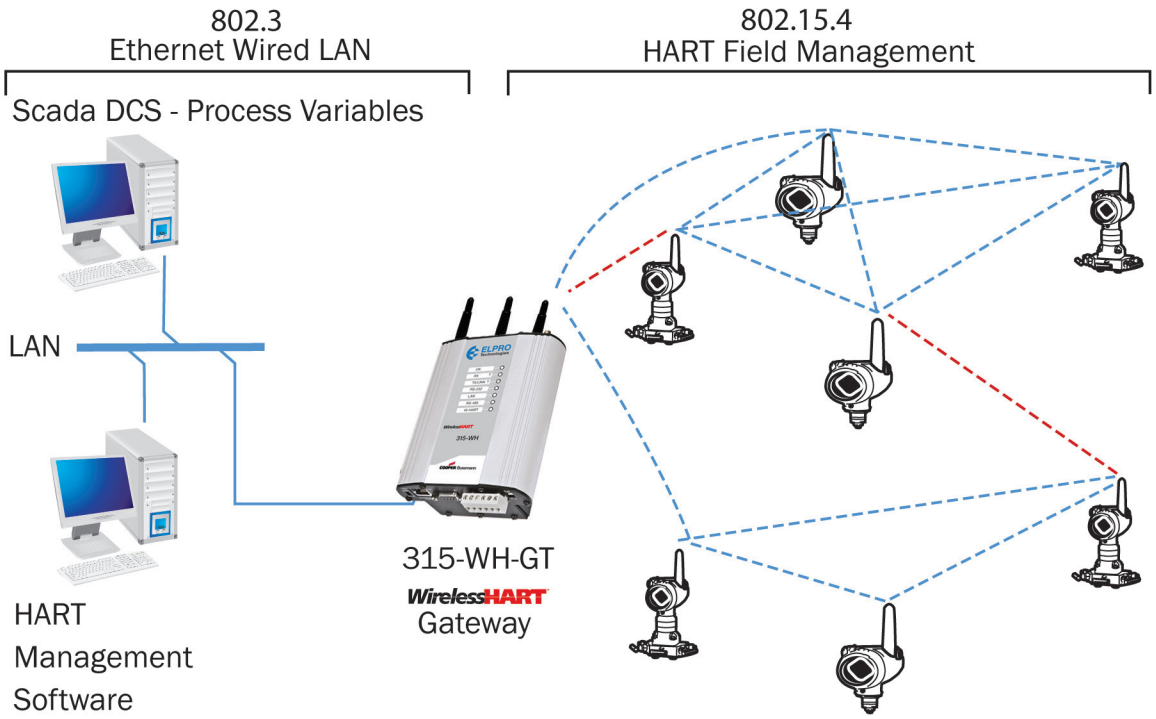


Figure 2

The 315-WH-Series modules are based on the ELPRO 245U-E Ethernet modem, and many of the standard Wi-Fi functions are available. However, the primary role of the modules is to provide an interface to a WirelessHART network.

This manual primarily covers the WirelessHART network connectivity and configuration. For more information on the Ethernet features available, see section “3.2 Ethernet Modem Features”

Key Features

- Compatible with HART 7.1.
- RS485, RS232 and Ethernet interfaces, with each interface supporting HART and Modbus Protocols.
- Web interface for remote configuration, monitoring and diagnostics.
- Using the 315-WH-DC (Data Concentrator), provides long-range WirelessHART communications.

CHAPTER 2 - INSTALLATION

2.1 General

The 315-WH Series WirelessHART modules are housed in a rugged aluminum case, suitable for DIN-rail mounting. Terminals will accept wires up to 12 gauge (2.5 sqmm) in size.

All connections to the module must be low voltage (SELV).

NOTE Do not connect 110-240V mains supply to any terminal on the 315-WH Series WirelessHART module. Refer to section "2.2 Power/Supply" for correct power supply terminations.

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 to one another. Following installation, the most common problem is poor communications caused by incorrectly installed aerials, radio interference on the same channel, or inadequate radio path. If the radio path is a problem (for example, the path is too long or there are obstructions), higher performance aerials or a higher mounting point for the aerial may rectify the problem. Alternately, use an intermediate 315-WH-Series module as a repeater.

The *315-WH Series WirelessHART Installation Guide* provides an installation drawing appropriate to most applications. Each 315-WH Series WirelessHART module should be effectively grounded (earthed) via the GND lug on the back of the 315-WH-Series module. This ensures that the surge protection circuits inside the module are effective.

2.2 Power/Supply

The 315-WH-Series modules can be powered from a 9–30 Vdc power supply. The power supply should be able to supply a minimum of 1 Amp and be CSA certified Class II approved for normal operation.

The positive side of the supply must not be connected to earth. The supply negative is connected to the unit case internally. The DC supply may be a floating supply or negatively grounded.

Power requirements of the modules, inclusive of radio and Ethernet ports being active and serial port plugged in:

- 315-WH-DC = 240 mA @ 12 Vdc or 150 mA @ 24 Vdc
- 315-WH-GT = 330 mA @ 12 Vdc or 210 mA @ 24 Vdc

Transmission current is nominally:

- 350 mA at 12 V (200 mA at 24 V) for the 100 mW RF unit
- 500 mA at 12 V (350 mA at 24 V) for the 400 mW RF unit

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 *315-WH Series WirelessHART Installation Guide*).

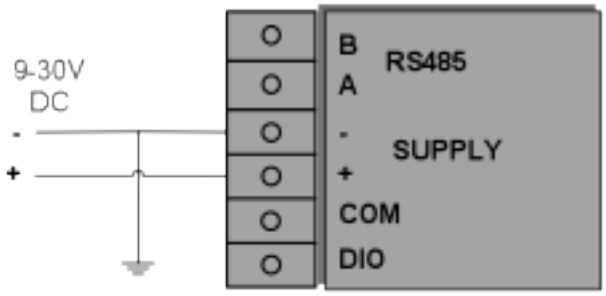


Figure 3

2.3 System Design/Antennas

The 315-WH-GT Gateway module uses two separate radio devices.

- **WirelessHART**—Operates in the 2.4GHz ISM radio band and complies with the 802.15.4 IEEE standard.
- **Standard Wi-Fi**—Operates in either the 2.4GHz band, which complies with the 802.11b/g standard, or the 5GHz band, which complies with the 802.11a.

Because the module has two radios in close proximity to each other, there will be some level of interference that will need to be addressed. The amount of interference between the two radios will depend on the frequency, transmit power level, and antenna type and location.

If using the 2.4GHz 802.11b/g radio, then both Wi-Fi and the WirelessHART radios use the 2.4GHz unlicensed frequency band but communicate using different IEEE standards. The Wi-Fi radio uses 802.11b/g Direct Sequence Spread Spectrum (DSSS) across a 20-megahertz band, while the WirelessHART radio communicates using 802.15.4 DSSS with a 2.75-megahertz bandwidth but uses frequency hopping technology to hop between channels within the frequency band.

Because each radio is communicating within the same frequency band, there will be some coexistence problems. However, by maintaining the recommended antenna separation and keeping the data rates in both systems low, these problems can be kept to a minimum. If using the 5GHz 802.11a model, there will be minimum interference because of the frequency difference. However, you will still need to maintain some level of separation.

The antenna separation needs to be >20dB to avoid exceeding the maximum input level of WirelessHART. Typically, this means at 2.4GHz the minimum required distance the antennas should be mounted is 0.5m (1.6 ft) vertical or 5m (16 ft) horizontal. At 5.8GHz, it will be 0.25m (10 ft) vertical or 2.5m (8 ft) horizontal.

The 315-WH-Series unit has three antenna connections. At the top of the module, two can be used for Wi-Fi communications. The connector labeled RX (see Figure 4) is connected to the internal Wi-Fi receiver. The connector labeled TX/RX is connected to both the Wi-Fi transmitter and receiver. The two Wi-Fi antenna connections are provided to allow a higher gain antenna to be connected to the RX-only connector without increasing the overall transmit gain on the TX/RX connector. The module will receive on both antenna ports, but transmit only on the TX/RX. Finally, the connector labeled Wi-HART is connected to the internal WirelessHART radio.

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

Figure 4

Wi-Fi Radio

The maximum achievable range 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 315-WH-GT (2.4GHz) with a single antenna, 5km (3 miles) can be achieved in USA, Canada and Australia (4W ERP) and 1km in Europe (100mW ERP). With separate transmit and receive antennas, more than 10km (6 miles) can be achieved in USA, Canada and Australia and more than 5km in Europe.

To achieve the maximum transmission distance, the antennas should be raised above intermediate obstructions such 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 block more than obstructions in the middle of the radio path.

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 larger amount of obstruction can be tolerated for shorter distances. For short distances, it is possible to mount the antennas inside buildings. An obstructed path may require testing to determine if the path will be reliable. Refer to section “TCP Throughput Test”

If using a 315-WH-GT (5GHz), similar distances can be achieved but more care is needed in selecting antennas, coax, and cables, and radio paths need to be complete line of site with no obstruction whatsoever. Environmental conditions will also have a larger effect on the higher 5GHz frequency, and this needs to be accounted for when performing initial path testing.

The 315-WH-Series modules provide a diagnostic feature that displays the Wi-Fi radio signal strength of transmissions (refer to “Chapter 5 - DIAGNOSTICS”).

Where it is not possible to achieve reliable communications between 315-WH-Series modules, an additional 315 or 245U-E series module may be used to receive the message and re-transmit it. This module is referred to as a repeater, which can also support additional WirelessHART networks.

WirelessHART Radio

The middle labeled SMA connector is used for the WirelessHART antenna connection. Typical achievable range for the WirelessHART radio is between 25 m and 100 m for indoor and 100 m to 300 m for outdoor. Actual RF range is subject to a number of installation-specific variables, including temperature, humidity, other radio interference, obstructions (such as trees, walls, signage) that may induce multipath fading.

Plant and Factory Installations

Most Wi-Fi installations in industrial plants and factories use single Omni-directional antennas rather than directional Yagi antennas.

Being in an area with many obstructions means the installations can suffer from multipath issues. This can be checked by moving the antenna a short distance (10 cm or 4 inches). If the signal increases significantly it means there are multipath effects.

Multipath issues are caused when radio waves reflect or pass through objects in the environment, which attenuates or weakens the radio signal depending on the material. Some materials (such as metal) are opaque to radio transmissions and therefore reflect more of the radio signal. Cluttered or obstructed environments can be very different from an open warehouse environment for radio transmissions and reception, which is why it is difficult to establish the range and data rate of a system.

Both 802.11a and 802.11g use OFDM modulation, which is good for multipath issues. In most obstructed environments, 802.11g (2.4 GHz) will perform better than 802.11a (5.8 GHz) due to better propagation of the lower frequency. In a static installation, where the radio path is not changing, moving an antenna to the position of maximum signal solves this problem. However, where the radio path changes because the 315-WH-Series is mounted on moving equipment, or if there is moving equipment in the area, the solution is to use two antennas. Because the two Wi-Fi connectors are separated, the RF signal at each connector will be different in the presence of multipath fading. The 315-WH-Series unit will automatically select the higher RF signal.

NOTE Directional antennas are not normally used in plant and factory installations.

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 the background noise in the direction of the link is low.

Basic WirelessHART System Design

Being a mesh network, every device can act as a repeater for messages from other devices. In other words, communications do not need to go directly to the Gateway, but can be forwarded through the next closest device. This extends the range of the network and provides redundant communication routes to increase reliability.

Because the WirelessHART radios have a low transmit power level, the maximum range is relatively short (300 m / 1000 ft) and therefore the placement of the WirelessHART nodes needs to be close to allow the WirelessHART mesh to communicate effectively. Remember that the WirelessHART devices and adapters do not need to communicate directly to the Gateway—only to another WirelessHART device.

When designing a WirelessHART network there are a few points that can ensure communications run as reliably and efficiently as possible. Each node within the mesh should have multiple communication paths with other nodes so that system reliability does not depend on a single link. A rule of thumb is to design the system such that each node has at least three neighbors. The WirelessHART network should have a minimum of five WirelessHART devices within range of the Gateway. In larger systems, 25% of the nodes should have a direct connection to the Gateway module.

Keep the Wi-Fi data transfer to a minimum; try not to use the Wi-Fi to transfer large amounts of data. It is also recommended to use the WirelessHART channel blacklist to avoid the four channels around the Wi-Fi channel. See “Chapter 4 - CONFIGURATION” for details.

The number of WirelessHART devices/adapters in the network will vary dependent on their configured update rates.

Recommended Network Size

- 12 Wireless Devices @ 1 second update
- 25 Wireless Devices @ 2 second update
- 50 Wireless Devices @ 4 second update
- 100 Wireless Devices @ 8 second update

Maximum Network Size

- 250 Wireless Devices @ >32 sec update

As the network size increases, the latency also increases. Typical latency for a network of 50 devices is 5 seconds and latency for a network of 100 is approximately 10 seconds.

Antennas – Wi-Fi

Antennas can be either connected directly to the module 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) minus the loss in the coaxial cable (in dB). The maximum net gain of the antenna/cable configuration connected to the TX/RX connector is 0dB in Europe (100mW ERP). In USA, Canada and Australia (4W ERP), the maximum gain is 10dB for the 315-WH-Series. There is no gain restriction for antennas connected to the RX connector.

The gains and losses of typical antennas/coax are shown in the following table.

Wi-Fi Antenna	2.4GHz Gain (dBi)	5GHz Gain (dBi)
Dipole	2 dBi	6 dBi
Collinear	5 or 10 dB	10 dBi
Directional	10 – 28 dB	10-20 dBi
Cable type	**Cable Loss (dB per 30m / 100 ft)**	**Cable Loss (dB per 30m / 100 ft)**
RG58 Cellfoil	-16.5 dB	-24.5 dB
RG213	-15.2 dB	-28.6 dB
LDF4-50	-3.9 dB	-5.5 dB

The net gain of the antenna/cable configuration is determined by adding the antenna gain and the cable loss. For example, a 5 dBi antenna with 10 meters of Cellfoil coax operating at 2.4 GHz has a net gain of -0.5 dB (5 dB – (10/30 m) x 16.5 dB) 6 dB).

Antennas – WirelessHART

The antenna should be mounted such that the radiating portion of the antenna protrudes from the module or enclosure, and connected to the middle SMA connector on the module using a suitable coaxial cable. For optimum performance, make sure the antenna is positioned vertically when installed, mounted at least one wavelength (130 mm for 2.4 GHz) from any vertical surface, and elevated as much as possible. Increasing the elevation of the antenna can significantly improve the signal path.

WirelessHART Antenna	315-WH-Series Gain (dBi)
Dipole	2 dB
Collinear	5 or 8 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 the most common cause for problems with radio systems because it greatly increases cable losses. It is recommended that the connection be taped first with a layer of PVC tape, and 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 troubleshooting, because the vulcanizing seal can easily be removed.

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

Dipole and Collinear Antennas

A dipole or collinear antenna transmits the same amount of radio power in all directions, and as such they are easy to install and use. The dipole antenna with integral 5 m (16 ft) cable does not require any additional coaxial cable. However, a cable must be used with the collinear antennas.

Collinear and dipole antennas should be mounted vertically, preferably one wavelength away from a wall or mast to obtain maximum range (see Figure 5 for distances).

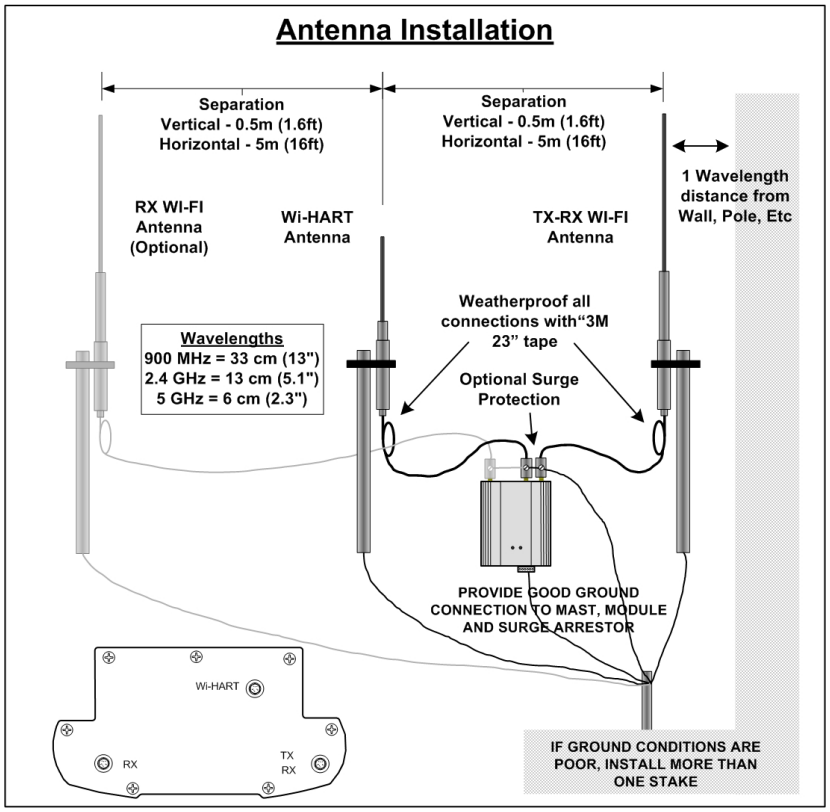


Figure 5

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 improve performance 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 according to 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.

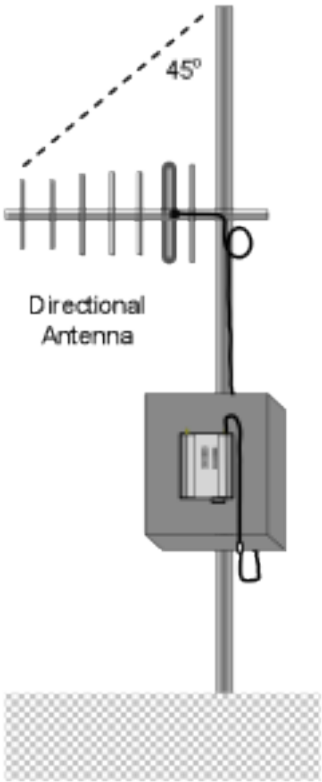


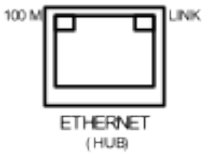
Figure 6

2.4 Connections

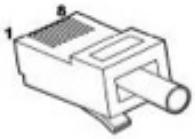
Ethernet

The Ethernet port is a standard 10/100 BaseT IEEE 802.3-compliant RJ45 connection.

- RJ45 connector has two LEDs in the connector.
- “100” – indicates 100 Mb/s Ethernet network speed.
- “LINK” – indicates a LAN connection.



- Connection is made with a standard RJ45 connector.



RS232 Serial Port

The serial port is a standard nine-pin DB9 female connector, which provides a connection for HART HMS Software or a Modbus Master. It can also be used to connect to a computer terminal for configuration, field testing, and factory testing. Communication is via standard RS232 signals. The 315-WH-Series is configured as DCE equipment with the cable details provided in Figure 7.

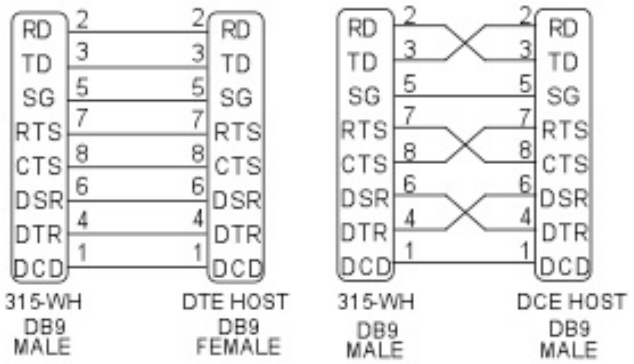


Figure 7

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 315-WH-Series does not support XON/XOFF.

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 communication between the 315-WH-Series unit and HART HMS Software or a Modbus Master using a multi-drop cable. 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 in Figure 8, and terminated at each end of the network with a 120-ohm resistor. On-board 120-ohm resistors are provided and may be engaged by operating the single dip switch in the end plate next to the RS485 terminals. The dip switch should be in the "1" or "on" position to connect the resistor. If the module is not at one end of the RS485 cable, the switch should be off.

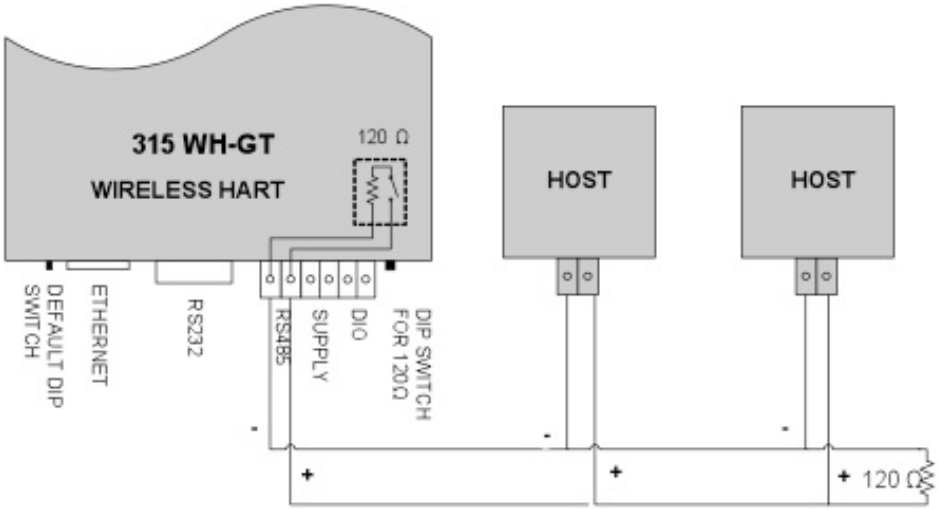


Figure 8

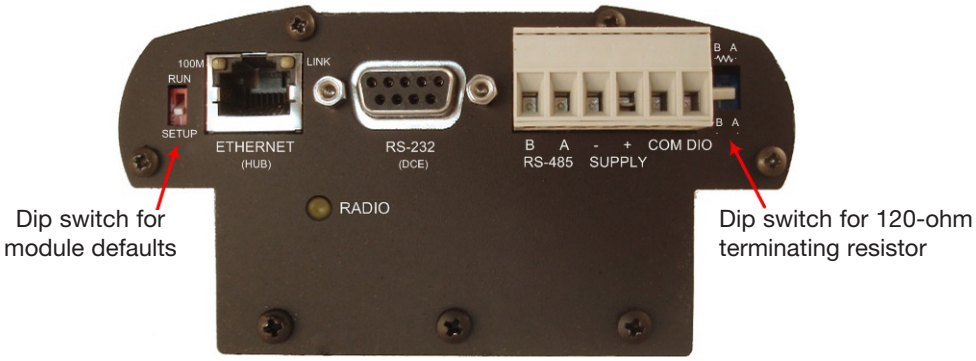


Figure 9

WirelessHART Communications Fail Output

The 315-WH-Series modules have a single discrete digital output. This output can be used to give an external indication or alarm for the WirelessHART communications status.

- 315-WH-GT will indicate communication with the WirelessHART manager module.
- 315-WH-DC will indicate communications with the WirelessHART 315-WH-GT Gateway.
- If the O/P is On (Closed contact), Communications is good (OK).
- If the O/P is Off (Open contact), Communications is bad (Failure).
- The Output is a FET transistor that switches to common and is rated at 30 Vdc 500 mA.
- It can be used to switch a load, as indicated by the relay in Figure 10.

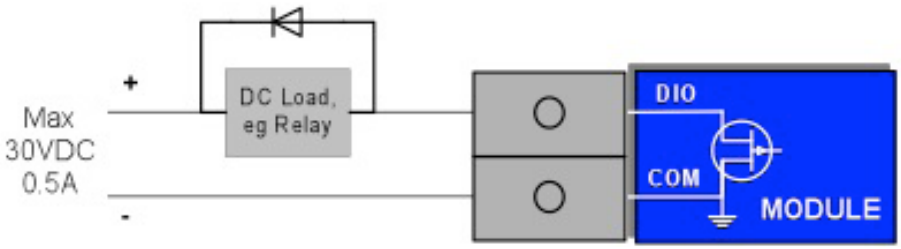


Figure 10

2.5 LED Indications

Front panel LEDs

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 during kernel (1/2 second red, 1/2 second green)
OK	Slow flash Red / Green	Module boot sequence during module initialization (1 second red, 1 second green)
RX	Green flash	Wi-Fi radio receiving data
RX	Red flash	Wi-Fi radio receiving data (low signal strength)
TX/LINK	Green	Connection established to remote device
TX/LINK	Red flash	Wi-Fi 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	Ethernet port activity
RS-485	Green flash	Data sent from RS-485 serial port
RS-485	Red flash	Data received to RS-485 serial port

A green OK LED on the front panel indicates correct operation of the unit. If this LED turns red (outside of the normal boot sequence at power up) it indicates a failure, such as Supply Low Volts or a Processor Fail.

W-HART LED

The WirelessHART LED on the front panel indicates the WirelessHART status. The indication will vary depending on the model and configuration, as shown in the following table. When the module first powers up it follows a boot-up sequence. During this time, you will see some of the LEDs flicker on and off.

W-HART LED	Condition	Meaning
When HARTPORT is Configured		
315-WH-GT	Green	During boot up, LED will be on for approximately 10 seconds, after which it will indicate a connection has been established with the WirelessHART Network Manager module. (Approximately 90 seconds). LED Off indicates no connection or a connection failure.
315-WH-DC	Green	Indicates a connection has been established with a WirelessHART 315-WH-GT Gateway. Will indicate only if the 315-WH-DC is configured with a HART MUX connection (HRTPORT). LED Off indicates no connection or a connection failure.
When HARTPORT is not Configured		
315-WH-DC	Green	Digital Output On or Input is Closed circuit.
315-WH-DC	Off	Digital Output Off or Input is Open circuit.

WirelessHART RADIO LED

There is a single yellow LED located on the connector end of the module that indicates any WirelessHART traffic, either received from or transmitted to the WirelessHART Network Manager.

Figure 11

CHAPTER 3 - OPERATION

3.1 Different Modules Types

Models

There are two models in the 315-WH-Series product list—the 315-WH-GT Gateway module and the 315-WH-DC Data Concentrator.

These two models provide a flexible solution for gathering data from remote WirelessHART devices and outputting the data to a HART Monitoring System (HMS) or DCS Software via a serial or Ethernet interface, either locally or at a remote location.

315-WH-GT in Standalone Mode

When configured in Standalone mode, the module performs as follows:

- Communicates with WirelessHART field devices and adapters and outputs the data to its local HARTPORT.
- Allows WirelessHART data to be outputted via Serial or Ethernet connection to a HART HMS.
- Has a Modbus interface option, which when enabled allows the HART data to be accessed via Ethernet or serial Modbus Host.

  This feature provides a means of mapping the four main process variables from WirelessHART field sensors and devices back to a standard Modbus interface, which is then made available to a distributed control system (DCS) or a supervisory control and data acquisition (SCADA) system. HMS/DCS and Modbus can be accessed simultaneously provided they are not using the same serial port.

Figure 12 illustrates the ELPRO 315-WH-GT when configured in a Standalone mode.

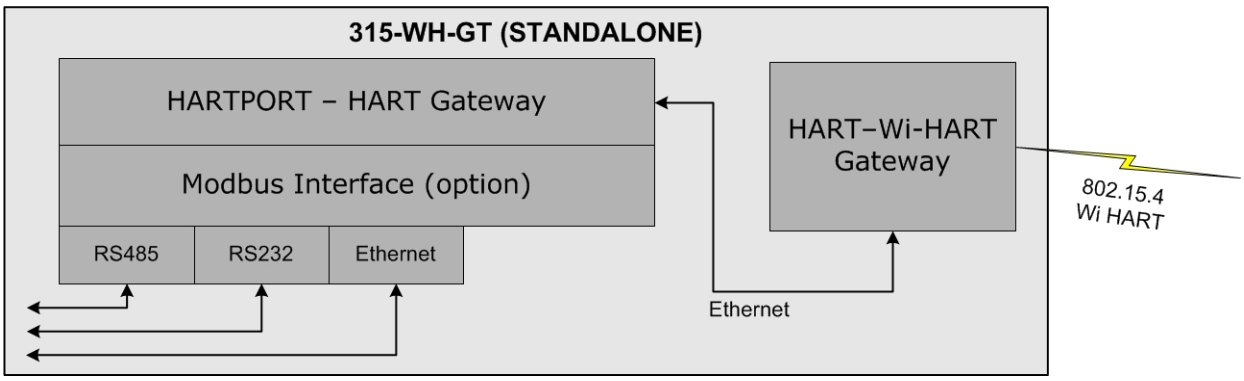


Figure 12

315-WH-GT in Gateway Mode

When using the Gateway mode option, the 315-WH-GT needs to be paired with the 315-WH-DC Data Concentrator module. The Data Concentrator can support connections for up to four Gateway devices.

When configured in Gateway mode, the 315-WH-GT performs as follows:

- Communicates with WirelessHART field devices and adapters and relays the data to the 315-WH-DC Data Concentrator using standard Wi-Fi.
- HART communication via Serial or Ethernet is disabled in the Gateway as data is relayed to the 315-WH-DC Data Concentrator.
- Modbus option is disabled as data is relayed to the Data Concentrator.

Figure 13 illustrates the ELPRO 315-WH-GT when configured in Gateway mode and used in conjunction with the 315-WH-DC Data Concentrator.

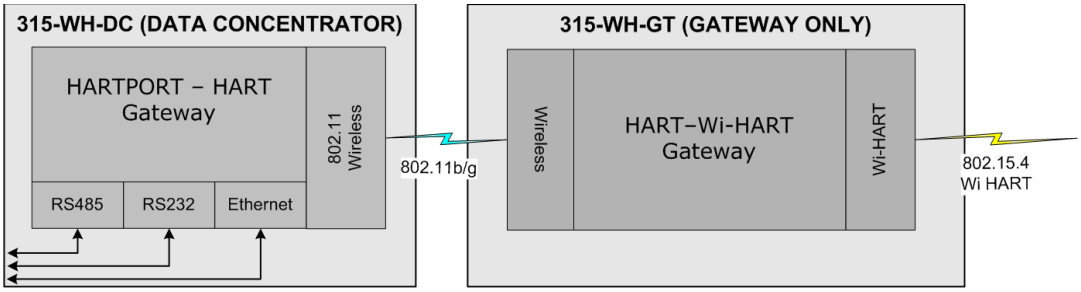


Figure 13

Standalone Data Concentrator

A standalone Data Concentrator performs as follows:

- DOES NOT communicate directly with WirelessHART field devices; must be used in conjunction with the 315-WH-GT Gateway.
- Accepts data from the 315-WH-GT Gateway and outputs the data to its local HARTPORT (RS232, RS485 or Ethernet).
- Allows WirelessHART data to be outputted via Serial or Ethernet to a HART HMS.
- Has a Modbus interface option, which when enabled allows the HART data to be accessed via Ethernet or serial Modbus Host. This feature provides a means of mapping the four main process variables from WirelessHART field sensors and devices back to a standard Modbus interface, which is then made available to a DCS or SCADA system.
- HMS/DCS (HART Data) and Modbus can be accessed simultaneously using separate ports (RS232/RS485/ Ethernet).

Having the HARTPORT at the 315-WH-DC instead of being at the 315-WH-GT means that communications with the HMS (HART Management System) is much faster because the connection is local over RS232, RS485 or hardwired Ethernet instead of via an 802.11 Wi-Fi Link.

3.2 Ethernet Modem Features

Because the 315-WH-Series modules are based on the ELPRO 245U-E Ethernet Modem, many of the features present in these modems are also available in the 315-WH-Series.

The following is a list of standard features available on all 315-WH-Series modules:

- The 315-WH-Series Industrial 802.11 Wireless Ethernet module provides up to 54Mbps wireless connections between Ethernet devices or Ethernet wired networks (LANs). It complies with the IEEE 802.11a/b/g standards.
- Different models with various RF power and frequency options to suit local radio regulations are available.
- Supports bridging and routing networks.
- The 315-WH-Series supports several different radio encryption schemes, WEP, WPA (TKIP and AES) and WPA Enterprise.
- Supports WDS (Access Point to Access Point) communications, which allows for multi hop repeaters to extend radio coverage.
- Can be configured as a DHCP client to obtain an IP address automatically on startup. Can also be configured as a DHCP/DNS server, which can supply IP addresses to other DCHP clients.

- Spanning Tree functionality, enabling self-healing of networks.
- MAC Address, IP Address/Protocol/Port filtering and ARP filtering all available to help reduce traffic and provide a more secure wireless network.

For more information about these features and how they are configured, refer to the *245U-E Wireless Ethernet Modem User Manual*, available from the download section on our web site: www.cooperbussmann.com/wirelessresources.

3.3 WirelessHART Network Manager Module

The WirelessHART Network Manager is a separate radio module that is embedded within the 315-WH-GT Gateway and interfaces to the WirelessHART mesh network. The module then interfaces via an internal Ethernet connection with the main 315-WH-GT radio module.

The internal network connection is specifically for connecting the WirelessHART Network Manager to the Radio modem. The default address of the network manager is 192.168.99.100 and 192.168.99.1 for the second network interface on the main 315-WH-GT board.

Generally these IP addresses should not need to be changed, however it may be necessary if the address conflicts with the configured primary network address of the module. Contact ELPRO Technologies for details on how to change the IP addresses: www.cooperbussmann.com/wirelessresources.

CHAPTER 4 - CONFIGURATION

4.1 Initial Network Connection

This section explains how to connect to the module for the first time and how to setup the initial network connection.

Configuration of the modules is performed via the Ethernet interface by connecting to the default or configured IP address, as described in the following sections.

Default Configuration

The default factory configuration of the 315-WH-Series is setup with the following defaults:

- Client/Bridge/
- IP address192.168.0.1XX, where XX is the last two digits of the serial number (the default IP address is shown on the printed label on the back of the module). The module address can be found on the label on the rear of the module.
- Netmask 255.255.255.0
- Username is “user” and the default password is “user”

The 315-WH-Series will temporarily load factory-default settings if powered with the Factory Default “Run/Setup” switch (on the end plate of the module) in the SETUP position. The previous configuration remains stored in non-volatile memory and will only change if configuration parameters are modified and the changes are saved.

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

When in SETUP mode, wireless operation is disabled.

For step-by-step instructions on connecting to the modules for the first time, see “Appendix A - FIRST TIME CONNECTION” at the end of this manual.

Web Interface

The 315-WH-Series modules have a built-in web server that contains web pages for analyzing and modifying the module’s configuration. The configuration can be accessed using Microsoft® Internet Explorer® (IE7 or above). This program is shipped with Microsoft Windows® or can be obtained freely via the Microsoft website.

To access the Web pages, type the modules IP address into a web browser and press Enter to see the following main page. The right side of the page has a number of links to the different configuration or diagnostics options.

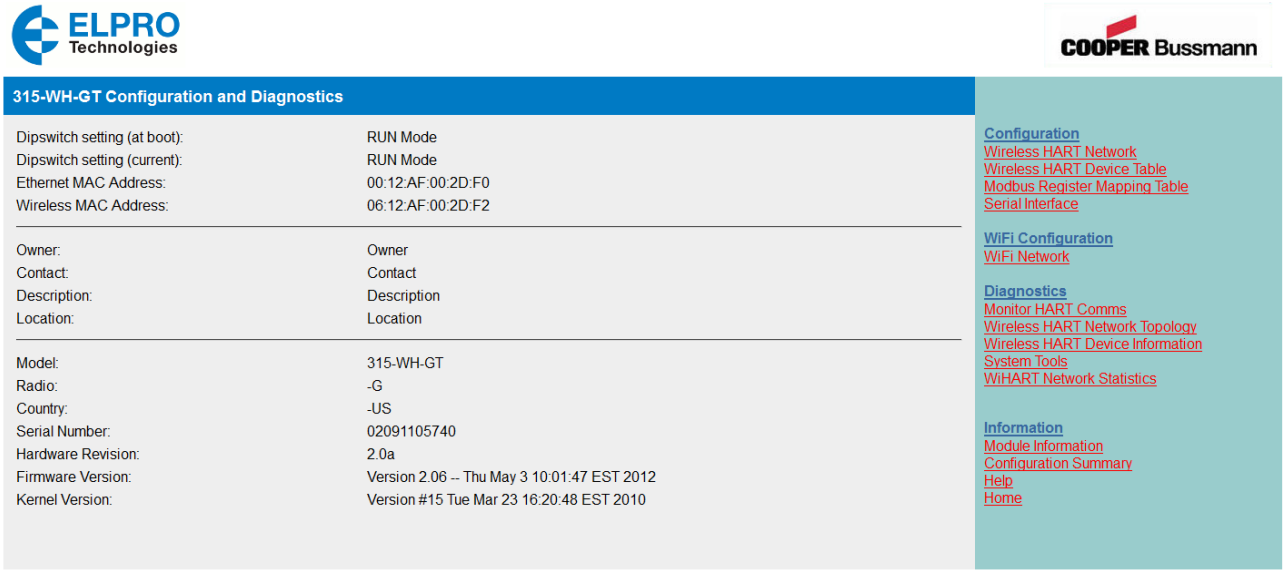


Figure 14

4.2 315-WH-GT Configuration

A 315-WH-GT can operate in two different modes:

- **Standalone mode**—WirelessHART Gateway (WirelessHART communications) and the Data Concentrator (HMS or DCS communications) are incorporated in the one module.
- **Gateway mode**—Only the WirelessHART Gateway is enabled and communications with the HMS or DCS is performed via a 315-WH-DC Data Concentrator. This allows the 315-WH-GT module to be located remotely from the HMS and close to the WirelessHART network.

Standalone Mode

In Standalone mode, the module communicates with the WirelessHART field devices and adapters and communicates directly to HART software or HMS via a serial or Ethernet connection. The 315-WH-GT also supports a standard 802.11a/b/g wireless Ethernet connection, which can be used for configuration, diagnostics and/or connectivity with other devices.

To configure the 315-WH-GT as a standalone unit, select WirelessHART Network from the links on the right side of the main page.

WirelessHART Network Configurations

The following page displays the WirelessHART network parameters.

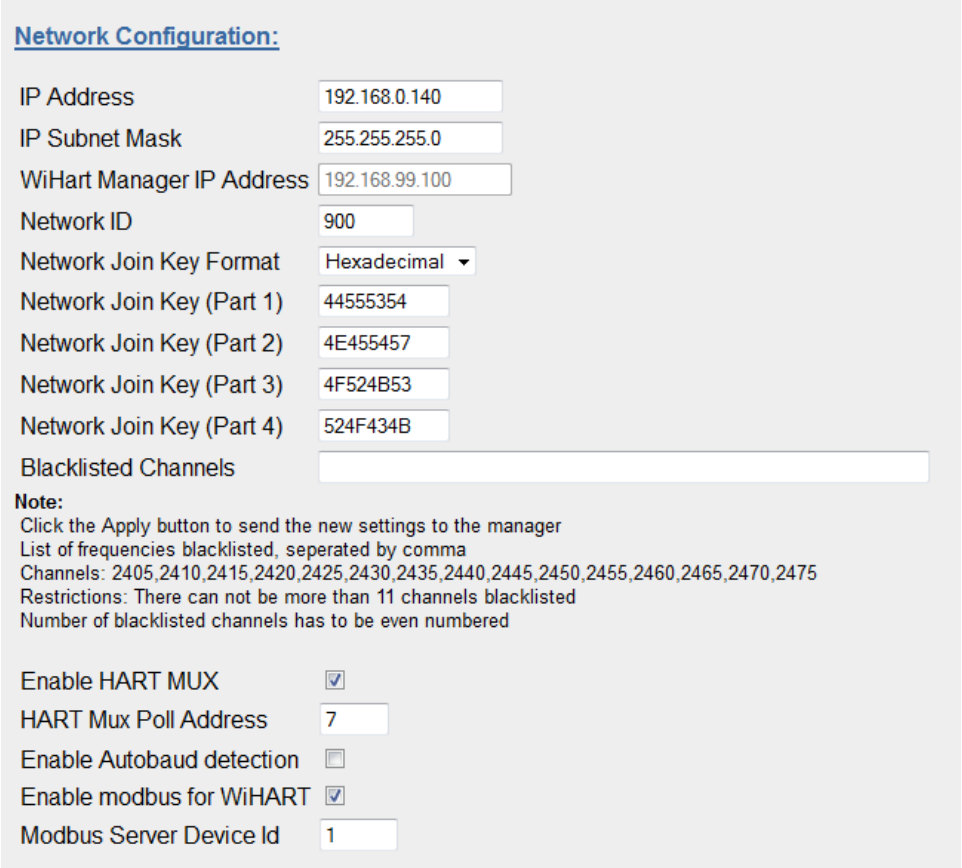


Figure 15

IP Address	The module's IP address; the address on the wired (CAT5 Ethernet) side of the module.
IP Subnet Mask	The IP network mask address on the wired (CAT5 Ethernet) side of the module.
WirelessHART Manager IP Address	The IP address of the WirelessHART Network Manager. This address is fixed at the default 192.168.99.100 and generally does not need to be changed unless the IP address conflicts with the configured network. Contact ELPRO Technologies if the IP address needs to be changed.
Network ID	A unique WirelessHART network ID. All WirelessHART devices need to have the same key configured to communicate successfully.
Network Join Key Format	Selection to display the network join key in either hexadecimal or integer format.
Network Join Key (Part 1-4)	All WirelessHART devices need to have the same join key configured to communicate successfully. All parts make up the complete join key. The default key is 445553545E4554574F524B53524F434B.
Blacklist Channels	Allows a number of radio channels to be "blacklisted" or banned from being used. No more than 11 of the 15 available channels can be blacklisted at any one time, and the number of blacklisted channels must be an even number. Enter the blacklist channel frequencies from the available list, separated by commas. It is recommended that the four WirelessHART channels that are within the configured Wi-Fi channel be blacklisted. For example, if Wi-Fi channel #1 is used then blacklist 2405, 2410, 2415 and 2420. Available channels are 2405, 2410, 2415, 2420, 2425, 2430, 2435, 2440, 2445, 2450, 2455, 2460, 2465, 2470, 2475.

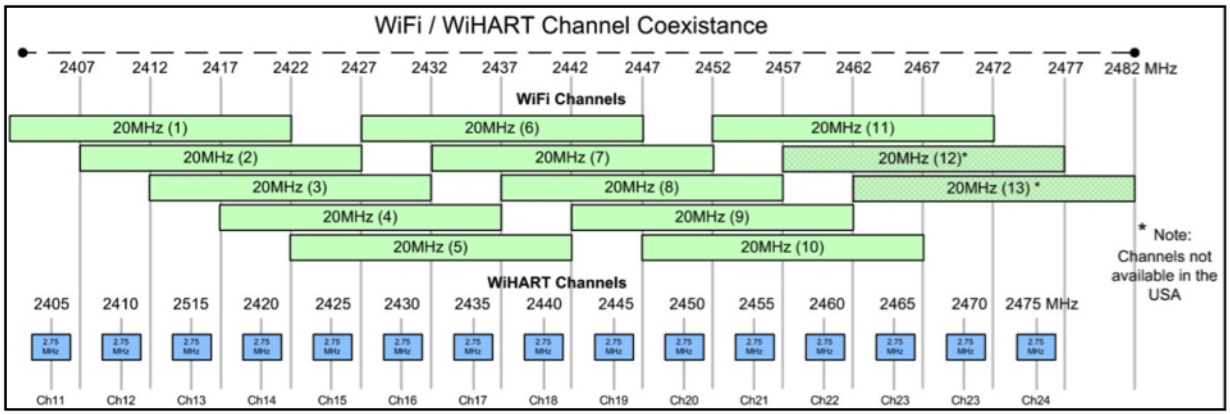


Figure 16

Enable HART MUX

Enables the HART MUX in the module. The HART MUX can be enabled on either the 315-WH-GT when configured as a standalone, or in the 315-WH-DC Data Concentrator.

NOTE If using serial interface, RS232 / RS485 communication parameters will need to be setup on the Serial Interface page.

HART MUX Poll Address

The polling address for the HART MUX interface. The address must be the same as what is configured in the HART Software or HMS. The default value for this address is seven.

Enable Auto baud Detection (HART MUX only)

Enables the automatic baud rate detection and will configure the serial parameters to match that of the connected device. This detection is only performed on startup of the module. Once the correct baud rate is detected, it will stay at that baud rate until the next power cycle.

Enable Modbus for WirelessHART

Enables the Modbus interface and allows process variables to be mapped to Modbus registers. If enabled, mappings will need to be setup on the Modbus Register Mapping Table screen to link the WirelessHART data to Modbus registers. See the section “Modbus Register Mapping Table” on page 35 for details.

Modbus Server Device ID

The Modbus Device ID for the onboard Modbus TCP Server. This is the address that the Modbus Client (Master) must poll to read data values.

HART Server Parameters

The HART Server Parameters only become available when the HART MUX is enabled in the network configuration described in the previous section.

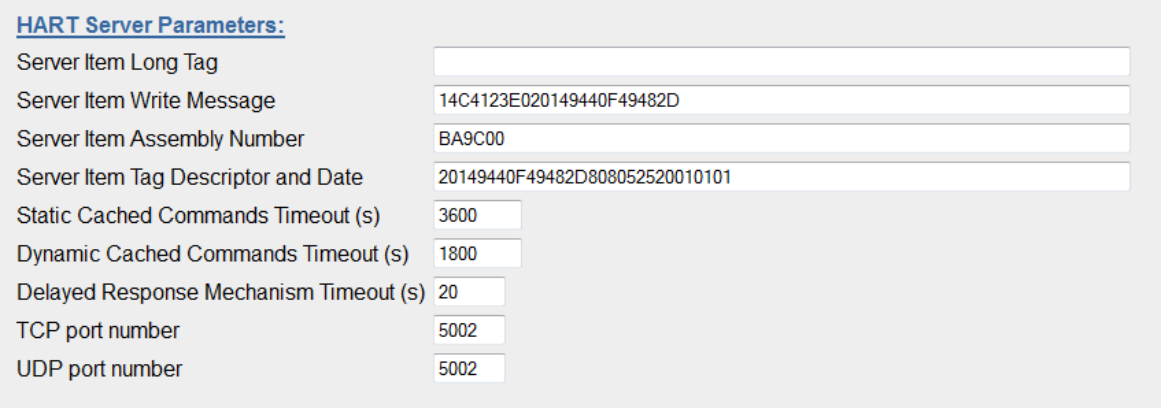


Figure 17

Server Item Long Tag	HART port MUX long tag, a 32-byte string read using HART command 20. The default value is HARTPORT – HART Gateway 06.
Server Item Write Message	HART Write Message string, a 24-byte hexadecimal string read using HART command 12. The default value is 14C4123E020149440F49482D.
Server Item Assembly Number	Assembly number of the HART port MUX, a 3-byte hex string read by HART command 16. The default is BA9C00.
Server Item Tag Descriptor and Date	HART port MUX descriptor and date tag, a 5-byte hex string read by HART command 13. The default value is 6A14A45AB4A482A8A8A5256AA1A1A1.
Static Cached Commands Timeout	Timeout to stale statically cached commands (Commands 000). All static data is cached for this period from when it was last received. The default is 3600 seconds.
Dynamic Cached Commands Timeout	Timeout to stale dynamic cached commands (Commands 001, 002, 003, 048). All dynamic data is cached for this period from when it was last received. The default is 1800 seconds.
Delayed Response Mechanism Timeout	Time the module waits before giving up waiting for responses from remote wireless devices. The default is 20 seconds.
TCP port number	Port number for HART TCP connection. The default port is 5002.
UDP port number	Port number for HART UDP connection. The default port is 5002.

WirelessHART Device Table

This device table is where WirelessHART sensors or devices are assigned to a particular location in the HART port MUX. It is organized into channels and shows the Address, Tag and State. See Figure 18.

It is recommended that the initial setup should be performed automatically by clicking the Refresh List button after the Gateway has been running for at least 10 minutes. This will allow time for the WirelessHART remotes to establish a connection with the WirelessHART Network Manager. Devices can be entered in manually, but it is much simpler and far more accurate to let the WirelessHART Network Manager refresh the table when the network has had time to establish its links. The order in which devices are entered in the table is generated by the order in which the devices join the WirelessHART network.

When all modules are entered or scanned, click the Save Changes and Reset button to write the changes to memory and reset the module.

NOTE Refreshing the list will cause the previous list to be overwritten.

Add Entry | Delete Entry

#	Channel	Address	Tag	State
1	1	00:00:18:C8:37	@@@@@@@@	Operational
2	2	26:58:7A:19:30	GENERIC	Operational
3	3	00:00:18:43:EF	SMART900	Operational
4	4	54:7A:52:01:30	TEMP354	Idle
5	5	36:A2:21:07:43	TEMP 333	Idle

Notes:
The address format has to be in a 5 byte format with each byte seperated by a ":"
Example: 01:02:03:34:A5

Refresh List

Figure 18

The device table in Figure 18 shows a number of WirelessHART devices. The maximum number of entries that can be entered into the table is 250.

Channel	The channel number allocated to the WirelessHART device. Each wireless device will have a separate channel, if the device is an adapter and able to support multiple wired HART sensors, each sensor will be allocated a different channel.
Address	A unique 5-byte address of the HART sensor. The format must be five hexadecimal bytes separated with colons. For example, 01:02:03:04:05.
Tag	Tag name assigned to the WirelessHART device. If the tag is unknown, the tag will show @@@@@@@@.
State	Indicates the status of the WirelessHART devices, for example Operational or Idle.

If you want to assign channels to a particular device, you can edit the refreshed list.

To add an entry manually:

1. Click **Add Entry**.
2. For each entry, fill in the Channel field and an address (5-byte hexadecimal HART address, with each byte separated by a colon). The Tag and the State will be updated by the WirelessHART Network Manager.

To remove an entry:

1. Select the entry and click **Delete Entry**.

When saved this table allocates field device values to fixed location (channels) within the MUX.

If the module is restarted or the Refresh List button is clicked, the module re-scans all devices. If it scans a device that is already in the table, it will be assigned to the same location as before. If the device is new and not defined in the table, it will be appended to the first available unallocated location in the MUX.

NOTE Care must be taken when deleting devices from the table because it can affect the order in the Modbus Table, when the Automatically Populate Table button on the Modbus Register Mapping Table is clicked.

Device Blacklist Table

The Device Blacklist Table is a list of WirelessHART devices that you want to “blacklist” or ban from making a connection with.

To add an entry:

1. Click **Add Entry** and add the unique 5-byte MAC Address in the device field.

   The MAC address must in the format of 5 hexadecimal bytes, with each byte separated by a colon. For example, 01:02:03:34:A5.

2. Click **Save Changes and Reset** for the changes to take effect.

To remove an entry:

1. Select the numbered table entry and then click **Delete Entry**.
2. Click **Save Changes and Reset** for the changes to take effect.

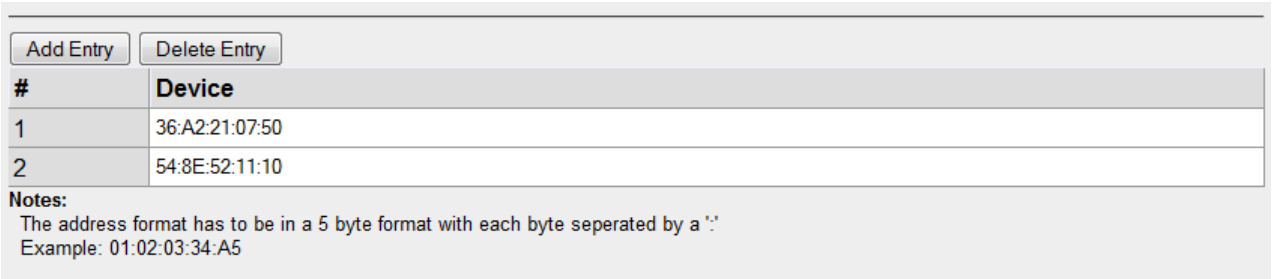


Figure 19

Modbus Register Mapping Table

The 315-WH-Series module has a Modbus interface, and when enabled can receive WirelessHART field data and store the values in a Modbus Database.

Configuration is performed by selecting “Modbus Register Mapping Table” from the menu on the right.

Figure 20 shows the Modbus Register Mapping Table screen, where you enter the appropriate Modbus mapping configurations.

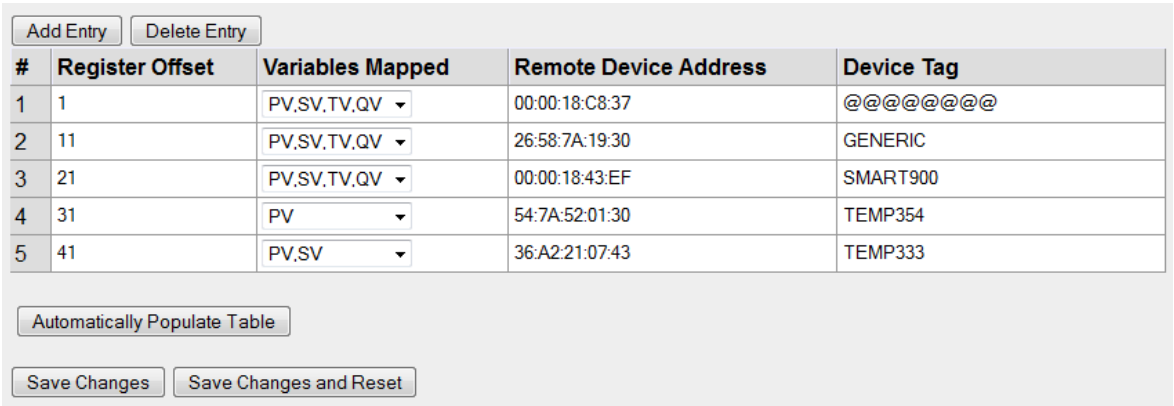


Figure 20

On first configuration of the module, it is recommended that you let the Gateway allocate the registers automatically by clicking the Automatically Populate Table button.

Registers can be mapped manually by clicking the Add Entry button and filling in the appropriate fields or automatically.

Automatically Populate Table

Clicking the Automatically Populate Table button scans all configured devices in the WirelessHART device table and populates the Modbus Table accordingly. The default 10 registers (5 x 32 bit values) will be allocated per device and assigned a register offset (Modbus address).

NOTE Auto Populate Table can take some time to refresh especially on larger systems. If the WirelessHART device table has been changed (for example, devices have been removed) the Modbus register order can change.

The Modbus Register Mapping Table can be manually edited, but care must be taken to ensure that all values are entered correctly.

Register Offset

Register Offset is an offset from the base Modbus Holding Register address. For example, register 1 can be read at 30001, register 31 can be read from 30031, and so on. The register offset must start at one and check that the values do not overlap with the previous offset.

Each variable mapped takes up two registers. For example, if the primary, secondary, tertiary and quaternary variables are mapped, the total number of registers required will be 10 (two registers x PV, SV, TV and QV) + two x Comms Fail register. Comms Fail registers are always available regardless of selection.

Select the required variables from the drop down list. If you edit a table that has been automatically populated, the register offsets will need to be amended because they are not adjusted automatically.

Variables Mapped

Variables Mapped is where you select the process variables that you want to read from the device. Each variable is a 32-bit IEEE754 floating-point value and is stored as two 16-bit words in consecutive registers. The most significant word is at the lower address (Default Odd). The least significant word is at the higher address (Default Even). For example, a Primary Variable with a hexadecimal value of 3F800000 would be stored in registers 2 and 3 as hexadecimal 3F80 in Register 2 and hexadecimal 0000 in register 3.

In addition to the HART variables, a communication status is also reported in the Modbus registers. The Communication Fail register has the value 1.0 when in communications failure, and 0.0 when communications are okay.

The following variables are available for each device.

- Offset Register = Comms Fail (Always available regardless of selection)
- Offset Register + 2 = PV (Primary Variable)
- Offset Register + 4 = SV (Secondary Variable)
- Offset Register + 6 = TV (Tertiary Variable)
- Offset Register + 8 = QV (Quaternary Variables)

NOTE Modbus Register Mapping Table must be saved and the unit reset for changes to take effect.

Remote Device Address

A unique 5-byte address of the remote WirelessHART devices (the format must be five hexadecimal bytes separated by a colon). If the table is automatically populated this address will be read from the device table.

Device Tag

The name of the device acquired from the WirelessHART device table. If read while the device is active, it will show the device name otherwise it will be blank or have the tag @@@@@@@@.

Connections – HART

NOTE HART Data and Modbus Data can be accessed simultaneously using separate ports (RS232/RS485/ Ethernet).

Ethernet

1. On the **WirelessHART Network** page for Ethernet HART communications, select “Enable HART MUX.”
2. Configure the HART MUX poll address and take note of the address for Configuration of HMS.
3. When finished, click **Save Changes and Reset** to save all parameters and reset the module.

Serial

1. On the **WirelessHART Network** page, select “Enable HART MUX.
2. Configure the HART MUX poll address and take note of the address for Configuration of HMS.
3. Click **Save Changes** to save all parameters.
4. Click **Serial Interface** from the menu on the right, and select a serial port that will be used for HART communications (either RS232 or 485). Choose **HART MUX** from the Port Type drop-down menu.
5. Setup the appropriate serial parameters as per your HART connection (baud rate, parity, format and flow control).
6. When finished, click **Save Changes and Reset** to save all parameters and reset the module.

Connections – Modbus

NOTE HART Data and Modbus Data can be accessed simultaneously using separate ports (RS232/RS485/ Ethernet).

Ethernet

1. On the **WirelessHART Network** page for all Modbus communications, select “Enable Modbus for WirelessHART.”
2. Configure a Modbus Server Device ID and take note of the address for Configuration of SCADA or DCS.
3. When finished, click **Save Changes and Reset** to save all parameters and reset the module.

   Modbus values can be accessed using a Modbus TCP connection by connecting to the IP address of the module, TCP Port 502, Modbus Server Device ID and then the appropriate Modbus address. For example, register 1 can be read as a 16-bit word at Modbus register 30001 or as a single bit at register 10001, register 50 can be read a 16-bit word at 30050 or as a single bit at Register 10050.

Serial

1. On the **WirelessHART Network** page for all Modbus communications, select “Enable Modbus for WirelessHART.”
2. Configure a Modbus Server Device ID and take note of the address for Configuration of SCADA or DCS.
3. Click **Save Changes** to save all parameters.
4. Click the **Serial Interface** page from the menu on the right, and choose a serial port that will be used for the Modbus connection (either RS232 or 485).
5. Select “Serial Gateway” from the Port Type selection and then choose Modbus from the Serial Gateway Mode drop-down list.
6. Setup the appropriate serial port parameters as per your Modbus connection (baud rate, parity, format and flow control).
7. When finished, click **Save Changes and Reset** to save all parameters and reset the module.

Gateway Mode

Gateway mode is used to extend the range of the WirelessHART network. The 315-WH-GT module will communicate with the WirelessHART field devices, and then pass the data to the 315-WH-DC via a standard 802.11a/b/g Wi-Fi connection. In addition to extending the WirelessHART communications, this Wi-Fi link can be used for configuration and diagnostics, as well as providing a wireless Ethernet connection for other devices.

Configuration of the WirelessHART network parameters on the 315-WH-DC in Gateway mode is very similar to the configuration in Standalone mode, except that the HART MUX is not enabled.

Because the HART MUX is disabled, configuration of the WirelessHART device table, Modbus Register Mapping table and the Serial Interface are not required.

When configured in Gateway mode, the Gateway must be paired with a 315-WH-DC Data Concentrator module.

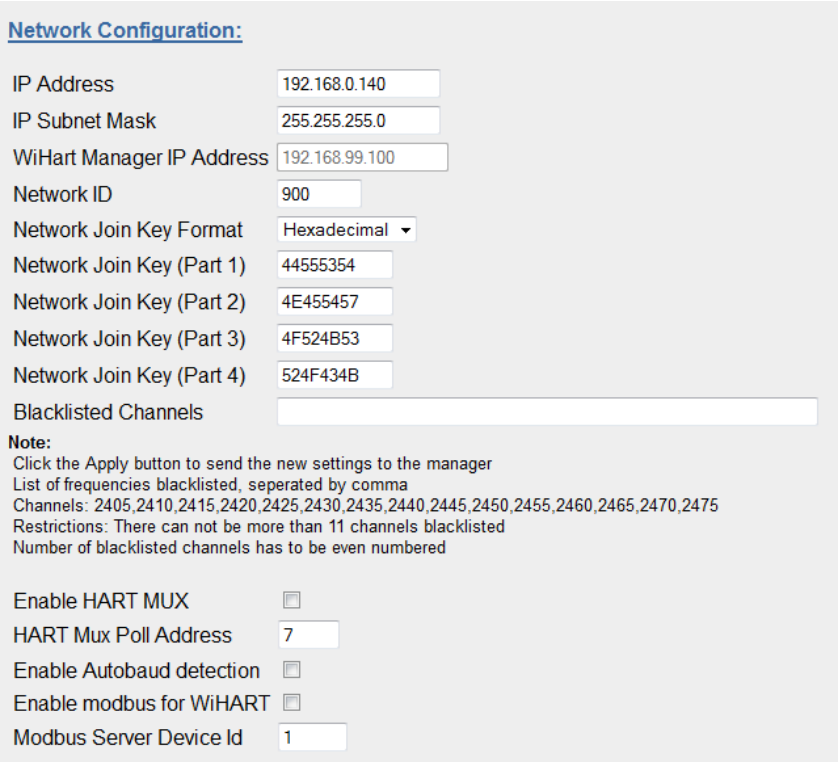


Figure 21

4.3 315-WH-DC Configuration

315-WH-DC Module

WirelessHART Network Configurations

Configuration of the 315-WH-DC Data Concentrator is very similar to configuration of the 315-WH-GT in Standalone mode, with the exception of the Network Configuration and some of the WirelessHART Network Manager diagnostic features, such as network topology and device Information.

A 315-WH-DC cannot be configured as a WirelessHART Gateway because it does not have a WirelessHART network module. However, it does have a HARTPORT which requires further configuration along with any Modbus connectivity (if used).

The Data Concentrator needs to know what Gateway (315-WH-GT) modules are configured in the system, and therefore requires the IP addresses to be entered into the Network Configuration.

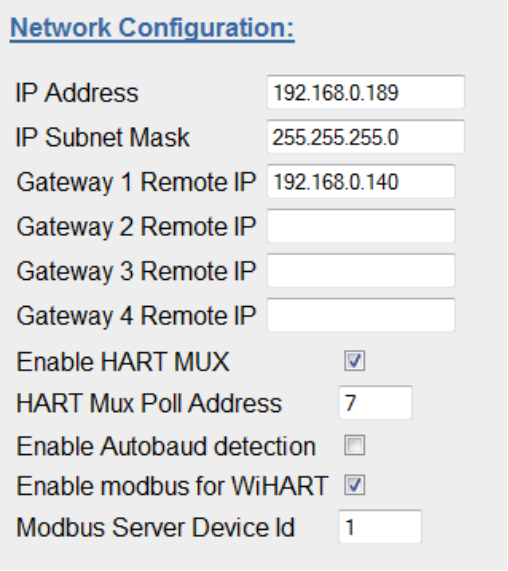


Figure 22

IP Address	The module's IP address; the address on its wired (CAT5 Ethernet) side of the module.
IP Subnet Mask	The IP network mask of the module on its wired (CAT5 Ethernet) side of the module.
Gateway Remote IP (1-4) IP	Address of any 315-WH-DC WirelessHART Gateway modules in the system. There is provision for up to four remote WirelessHART Gateway addresses. Leave the remaining IP addresses blank if only one Gateway is used.
Enable HART MUX	Enables the HART MUX in the module. This will need to be enabled to communicate with an HMS or DCS.
HART MUX Poll Address	Polling address for the HART MUX interface. Address must be the same as is configured in the HART Software or HMS. The default value is seven.
Enable Auto baud Detection (HART MUX only)	Enables the automatic baud rate detection and will configure the serial parameters to match that of the connected device. This detection is only performed on startup of the module. Once the correct baud rate is detected, it will stay at that baud rate until the next power cycle.
Enable Modbus for WirelessHART	Enables the Modbus interface and will allow process variables to be mapped to Modbus registers. If enabled, Modbus Mappings will need to be setup on the Modbus Register Mapping Table screen. See "Modbus Register Mapping Table" for details.
Modbus Server Device ID	This is the Modbus Device ID for the onboard Modbus TCP Server. This is the address that the Modbus Client (Master) must poll to read data values.

HART Server Parameters

The HART Server Parameters only become available when the HART MUX has been enabled in the Network Configuration.

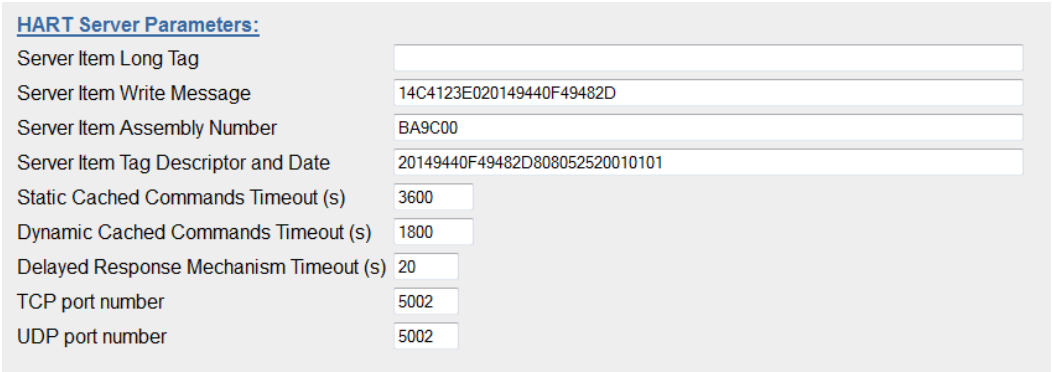


Figure 23

Server Item Long Tag	Hart port MUX long tag, a 32-byte string read using HART command 20. The default value is HARTPORT – HART Gateway 06.
Server Item Write Message	HART Write Message string, a 24-byte hexadecimal string read using HART command 12. The default value is 14C4123E020149440F49482D.
Server Item Assembly Number	Assembly number of the HART port MUX, a 3-byte hexadecimal string read by HART command 16. The default is BA9C00.
Server Item Tag Descriptor and Date	HART port MUX descriptor and date tag, a 15-byte hexadecimal string read by HART command 13. The default value is 6A14A45AB4A482A8A8A5256AA1A1A1.
Static Cached Commands Timeout	Timeout to stale statically cached commands (Commands 000). All static data is cached for this period from when it was last received. The default is 3600 seconds.
Dynamic Cached Commands Timeout	Timeout to stale dynamic cached commands (Commands 001, 002, 003, 048). All dynamic data is cached for this period from when it was last received. The default is 1800 seconds.
Delayed Response Mechanism Timeout	Amount of time the Module waits before giving up waiting for responses from remote wireless devices. The default is 20 seconds.
TCP port number	Port number for HART TCP connection. The default port is 5002.
UDP port number	Port number for HART UDP connection. The default port is 5002.

WirelessHART Device Table

This device table is where WirelessHART sensors or devices are assigned to a particular location in the HART port MUX. It is organized into channels and shows the Address, Tag and State (see Figure 24).

It is recommended that the initial setup be performed automatically by clicking the Refresh List button after the Gateway has been running for at least 10 minutes. This will allow time for the WirelessHART remotes to establish a connection with the WirelessHART manager. Devices can be entered in manually, but it is much simpler and far more accurate to let the WirelessHART manager refresh the table when the network has had time to establish its links. The order in which devices are entered into the table is generated by the order in which they join the WirelessHART network.

When all modules are entered or scanned, click the Save changes and Reset button to write the changes to memory and reset the module.

NOTE Refreshing the list will cause the previous list to be overwritten.

Add Entry | Delete Entry

#	Channel	Address	Tag	State
1	1	00:00:18:C8:37	@@@@@@@@	Operational
2	2	26:58:7A:19:30	GENERIC	Operational
3	3	00:00:18:43:EF	SMART900	Operational
4	4	54:7A:52:01:30	TEMP354	Idle
5	5	36:A2:21:07:43	TEMP 333	Idle

Notes:
The address format has to be in a 5 byte format with each byte seperated by a ":"
Example: 01:02:03:34:A5

Refresh List

Figure 24

The device table in Figure 24 shows a number of WirelessHART devices. The maximum number of entries that can be entered into the table is 250.

Channel	The channel number that is allocated to the WirelessHART device. Each wireless device will have a separate channel. If the device is an adapter and able to support multiple wired HART sensors, each sensor will be allocated a different channel.
Address	A unique 5-byte address of the HART sensor. The format must be five hexadecimal bytes, separated by colons. For example, 01:02:03:04:05.
Tag	Tag name assigned to the WirelessHART device. If the tag is unknown, the tag will show @@@@@@@@.
State	Indicates the status of the WirelessHART devices (for example, Operational or Idle).

If you want to assign channels to a particular device, you can edit the refreshed list.

To add entries manually:

1. Click **Add Entry**.
2. For each entry, fill in the Channel field and an address (5-byte hexadecimal HART address with each byte separated by a colon). The Tag and the State will be updated by the WirelessHART manager.

To delete an entry:

1. Select the entry and click **Delete Entry**.

When saved, this table allocates field device values to fixed location (channels) within the MUX.

If the module is restarted or the Refresh List button is clicked, the module re-scans all devices. If it scans a device that is already in the table, the device will be assigned to the same location as it was previously. If the device is new and not defined in the table, it will be appended to the first available unallocated location in the MUX.

NOTE Care must be taken when deleting devices from this table as it can affect the order in the Modbus Table, when the Automatically Populate Table button on the Modbus Register Mapping Table is clicked.

Device Blacklist Table

The device blacklist table is a list of WirelessHART devices that you want to “blacklist” or ban from making a connection with.

To add a device to the blacklist table:

1. Click **Add Entry**.
2. Add the unique 5-byte MAC address of the device in the device field.

   The MAC address must in the format of 5 hexadecimal bytes with each byte separated by a colon. For example, 01:02:03:34:A5.
3. Click **Save Changes and Reset** for the change to take effect.

To remove a device from the blacklist table:

1. Select the numbered table entry and click **Delete Entry**.
2. Click **Save Changes and Reset** for the change to take effect.

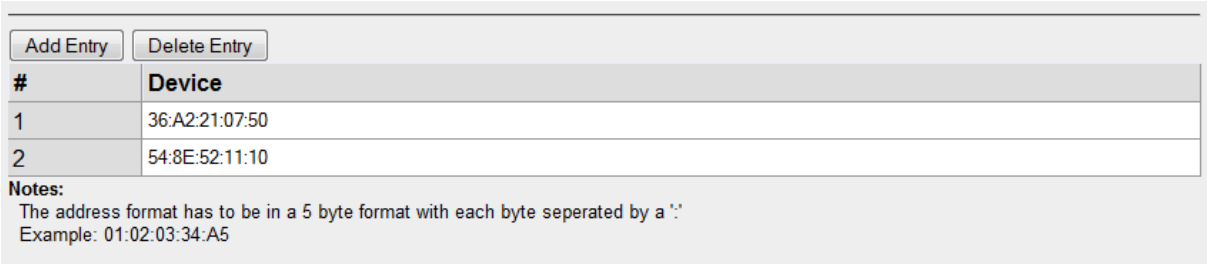


Figure 25

Modbus Register Mapping Table

The 315-WH-Series module has a Modbus interface and when enabled can receive WirelessHART field data and store the values in a Modbus Database.

Configuration is performed by selecting “Modbus Register Mapping Table” from the menu on the right.

Figure 26 shows the Modbus Register Mapping Table screen, where you will enter in the appropriate Modbus mapping configurations.

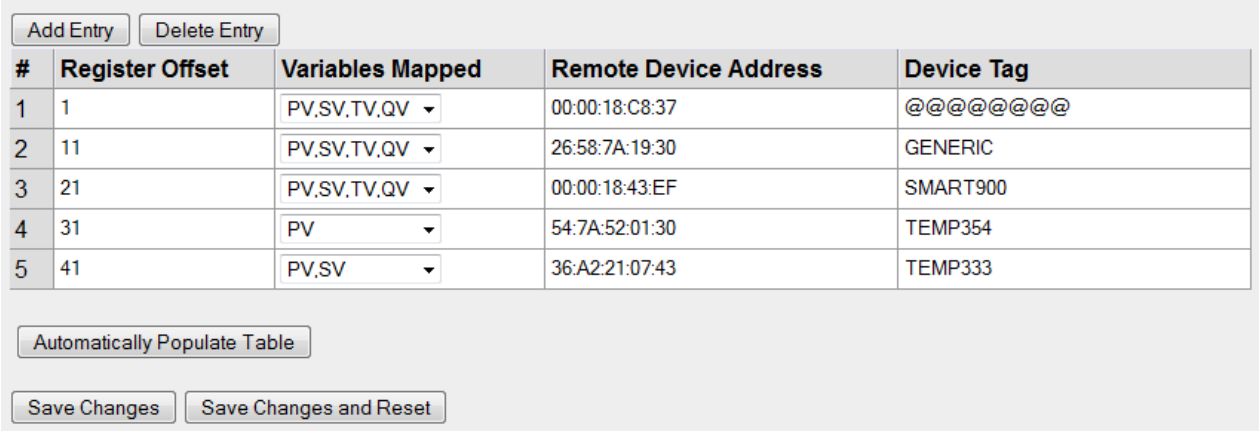


Figure 26

When configuring the module for the first time, it is recommended that you let the Gateway allocate the registers automatically by clicking the Automatically Populate Table button. Registers can be mapped manually by clicking the Add Entry button and filling in the appropriate fields.

Automatically Populate Table

Clicking the Automatically Populate Table button scans all configured devices in the WirelessHART device table and populates the Modbus Table accordingly. The default 10 registers (5 x 32 bit values) will be allocated per device and assigned a register offset (Modbus address).

NOTE Auto Populate Table can take some time to refresh especially on larger systems. If the WirelessHART device table has been changed (devices removed), the Modbus register order can change.

The Modbus Register Mapping Table can be manually edited, but care must be taken to ensure that all values are entered correctly.

Register Offset

The register offset is an offset from the base Modbus Holding Register address. For example, register 1 can be read at 30001, register 31 can be read from 30031, and so on. The register offset must start at one and check that the values do not overlap with the previous offset.

Each variable mapped will take up two registers. For example, if the primary, secondary, tertiary and quaternary variables and mapped the total number of registers required will be 10 (two registers x PV, SV, TV and QV) + a two x Comms Fail register. Comms Fail registers are always available regardless of selection.

Select the required variables from the drop-down list. If editing a table that has been automatically populated, the register offsets will need to be amended because they are not adjusted automatically.

Variables Mapped

The Variables Mapped column is where you select the process variables that you want to read from the device.

Each variable is a 32-bit IEEE754 floating-point value and is stored as two 16-bit words in consecutive registers. The most significant word is at the lower address (Default Odd). The least significant word is at the higher address (Default Even). For example, a Primary Variable with a hexadecimal value of 3F800000 would be stored in registers 2 and 3 as hexadecimal 3F80 in register 2 and hexadecimal 0000 in register 3.

In addition to the HART variables, the communication status is also reported in the Modbus registers. The Communication Fail register has the value 1.0 when in communications failure and 0.0 when communications are okay.

The following variables are available for each device:

- Offset Register = Comms Fail (always available regardless of selection)
- Offset Register + 2 = PV (Primary Variable)
- Offset Register + 4 = SV (Secondary Variable)
- Offset Register + 6 = TV (Tertiary Variable)
- Offset Register + 8 = QV (Quaternary Variables)

NOTE Modbus Register Mapping Table must be saved and the unit reset for changes to take effect.

Remote Device Address

A unique 5-byte address of the remote WirelessHART devices (the format must be five hexadecimal bytes separated by a colon). If the table is automatically populated, this address will be read from the device table.

Device Tag

The device tag is the name of the device acquired from the WirelessHART device table. If read while the device is active, it shows the device name. Otherwise, it is left blank or has the tag @@@@@@@@.

Connections – HART

NOTE HART Data and Modbus Data can be accessed simultaneously using separate ports (RS232/RS485/Ethernet).

Ethernet

1. On the **WirelessHART Network** page for Ethernet HART communications, select “Enable HART MUX.”
2. Configure the HART MUX poll address and take note of the address for Configuration of HMS.
3. When finished, click **Save Changes and Reset** to save all parameters and reset the module.

Serial

1. On the **WirelessHART Network** page, select “Enable HART MUX.”
2. Configure the HART MUX poll address and take note of the address for Configuration of HMS.
3. Click **Save Changes** to save the parameters.
4. Click the **Serial Interface** page link from the menu on the right, and choose a serial port that will be used for HART communications (either RS232 or 485).
5. Choose **HART MUX** from the Port Type menu.
6. Setup the appropriate serial parameters for your HART connection (baud rate, parity, format and flow control).
7. When finished, click **Save Changes and Reset** to save all parameters and reset the module.

Connections – Modbus

HART Data and Modbus Data can be accessed simultaneously using separate ports (RS232/RS485/Ethernet).

Ethernet

1. On the **WirelessHART Network** page for all Modbus communications, select “Enable Modbus for WirelessHART.”
2. Configure a Modbus Server Device ID and take note of the address for Configuration of SCADA or DCS.
3. When finished, click **Save Changes and Reset** to save all parameters and reset the module.

Modbus values can be accessed using a Modbus TCP connection by connecting to the IP address of the module, TCP Port 502, Modbus Server Device ID and then the appropriate Modbus address. For example, register 1 can be read as a 16-bit word at Modbus Register 30001 or as a single bit at register 10001; register 50 can be read a 16-bit word at 30050, or as a single bit at register 10050.

Serial

1. On the **WirelessHART Network** page for all Modbus communications, select “Enable Modbus for WirelessHART.”
2. Configure a Modbus Server Device ID and take note of the address for Configuration of SCADA or DCS.
3. Click **Save Changes** to save all parameters.
4. Click the **Serial Interface** page link from the menu on the right, and choose a serial port that will be used for the Modbus connection (either RS232 or 485).
5. Choose **Serial Gateway** from the Port Type menu.
6. Choose **Modbus** from the Serial Gateway Mode menu.
7. Setup the appropriate serial port parameters as per your Modbus connection (baud rate, parity, format, and flow control).
8. When finished, click **Save Changes and Reset** to save all parameters and reset the module.

CHAPTER 5 - DIAGNOSTICS

5.1 HART Diagnostics

Both 315-WH-Series modules have built in HART and WirelessHART diagnostics. On the Serial web page, you can select the RS232 or RS485 serial port to monitor either the WirelessHART Debug Port or the HART Debug Port. The diagnostic features allow you to output any Raw WirelessHART or HART data frames to the configured serial port.

Serial WirelessHART Debug Port

The WirelessHART debug option monitors and displays communication frames between the WirelessHART Gateway (WirelessHART module) and the HARTPORT. This allows you to diagnose WirelessHART data frames as they are received on the WirelessHART and sent to the HARTPORT.

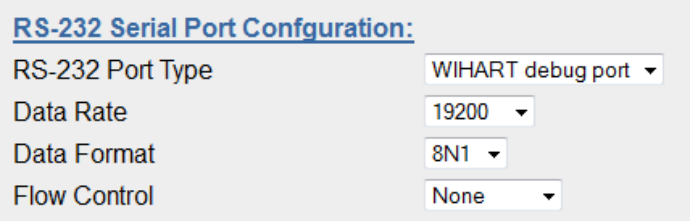


Figure 27

You will see two different frames. “WIRELESS,” refers to the wireless data frames that have been received and transmitted on the 802.15.4 WirelessHART radio, and “WIRED” refers to the data frames that are received and transmitted between the WirelessHART Gateway and the HARTPORT.

By connecting a terminal (Windows HyperTerminal) to the serial port at the configured baud rate, parity, and flow control, you will see the following.

```
 A0 00 00 94
GT [WIRELESS] R <-- : 717192.84227      00 00 00 03 19 00 00 00 00 00 fb 00 00 00 00 fb 3f 80 00 00 fa 7f a0 00 00 fa 7f a0 00 00
GT [WIRED] S --> : 717192.85938         86 00 00 18 43 EF 03 1A 00 00 00 00 00 00 FB 00 00 00 00 FB 3F 80 00 00 FA 7F A0 00 00 FA 7F
 A0 00 00 94
GT [WIRELESS] R <-- : 717222.519069     00 00 00 03 19 00 00 00 00 00 fb 00 00 00 00 fb 3f 80 00 00 fa 7f a0 00 00 fa 7f a0 00 00
GT [WIRED] S --> : 717222.520800        86 00 00 18 43 EF 03 1A 00 00 00 00 00 00 FB 00 00 00 00 FB 3F 80 00 00 FA 7F A0 00 00 FA 7F
 A0 00 00 94
GT [WIRELESS] R <-- : 717250.417212     00 00 00 03 19 00 00 00 00 00 fb 00 00 00 00 fb 3f 80 00 00 fa 7f a0 00 00 fa 7f a0 00 00
GT [WIRED] S --> : 717250.419076        86 00 00 18 43 EF 03 1A 00 00 00 00 00 00 FB 00 00 00 00 FB 3F 80 00 00 FA 7F A0 00 00 FA 7F
 A0 00 00 94
GT [WIRELESS] R <-- : 717280.851699     00 00 00 03 19 00 00 00 00 00 fb 00 00 00 00 fb 3f 80 00 00 fa 7f a0 00 00 fa 7f a0 00 00
GT [WIRED] S --> : 717280.853412        86 00 00 18 43 EF 03 1A 00 00 00 00 00 00 FB 00 00 00 00 FB 3F 80 00 00 FA 7F A0 00 00 FA 7F
 A0 00 00 94
GT [WIRELESS] R <-- : 717311.286385     00 00 00 03 19 00 00 00 00 00 fb 00 00 00 00 fb 3f 80 00 00 fa 7f a0 00 00 fa 7f a0 00 00
GT [WIRED] S --> : 717311.288260        86 00 00 18 43 EF 03 1A 00 00 00 00 00 00 FB 00 00 00 00 FB 3F 80 00 00 FA 7F A0 00 00 FA 7F
 A0 00 00 2B
GT [WIRELESS] R <-- : 717339.184690     00 00 00 03 19 00 00 00 00 00 fb 00 00 00 00 fb 3f 80 00 00 fa 7f a0 00 00 fa 7f a0 00 00
GT [WIRED] S --> : 717339.186415        86 00 00 18 43 EF 03 1A 00 00 00 00 00 00 FB 00 00 00 00 FB 3F 80 00 00 FA 7F A0 00 00 FA 7F
 A0 00 00 94
GT [WIRELESS] R <-- : 717369.619330     00 00 00 03 19 00 00 00 00 00 fb 00 00 00 00 fb 3f 80 00 00 fa 7f a0 00 00 fa 7f a0 00 00
GT [WIRED] S --> : 717369.621035        86 00 00 18 43 EF 03 1A 00 00 00 00 00 00 FB 00 00 00 00 FB 3F 80 00 00 FA 7F A0 00 00 FA 7F
 A0 00 00 94
GT [WIRELESS] R <-- : 717400.78190      00 00 00 03 19 00 00 00 00 00 fb 00 00 00 00 fb 3f 80 00 00 fa 7f a0 00 00 fa 7f a0 00 00
GT [WIRED] S --> : 717400.78455         86 00 00 18 43 EF 03 1A 00 00 00 00 00 00 FB 00 00 00 00 FB 3F 80 00 00 FA 7F A0 00 00 FA 7F
 A0 00 00 94
GT [WIRELESS] R <-- : 717430.510683     00 00 00 03 19 00 00 00 00 00 fb 00 00 00 00 fb 3f 80 00 00 fa 7f a0 00 00 fa 7f a0 00 00
GT [WIRED] S --> : 717430.512403        86 00 00 18 43 EF 03 1A 00 00 00 00 00 00 FB 00 00 00 00 FB 3F 80 00 00 FA 7F A0 00 00 FA 7F
 A0 00 00 94
GT [WIRELESS] R <-- : 717458.386661     00 00 00 03 19 00 00 00 00 00 fb 00 00 00 00 fb 3f 80 00 00 fa 7f a0 00 00 fa 7f a0 00 00
GT [WIRED] S --> : 717458.388533        86 00 00 18 43 EF 03 1A 00 00 00 00 00 00 FB 00 00 00 00 FB 3F 80 00 00 FA 7F A0 00 00 FA 7F
 A0 00 00 94
GT [WIRELESS] R <-- : 717488.821292     00 00 00 03 19 00 00 00 00 00 fb 00 00 00 00 fb 3f 80 00 00 fa 7f a0 00 00 fa 7f a0 00 00
GT [WIRED] S --> : 717488.823016        86 00 00 18 43 EF 03 1A 00 00 00 00 00 00 FB 00 00 00 00 FB 3F 80 00 00 FA 7F A0 00 00 FA 7F
 A0 00 00 94
GT [WIRELESS] R <-- : 717519.431427     00 00 00 03 19 00 00 00 00 00 fb 00 00 00 00 fb 3f 80 00 00 fa 7f a0 00 00 fa 7f a0 00 00
GT [WIRED] S --> : 717519.433143        86 00 00 18 43 EF 03 1A 00 00 00 00 00 00 FB 00 00 00 00 FB 3F 80 00 00 FA 7F A0 00 00 FA 7F
 A0 00 00 94
GT [WIRELESS] R <-- : 717549.690488     00 00 00 03 19 00 00 00 00 00 fb 00 00 00 00 fb 3f 80 00 00 fa 7f a0 00 00 fa 7f a0 00 00
GT [WIRED] S --> : 717549.692201        86 00 00 18 43 EF 03 1A 00 00 00 00 00 00 FB 00 00 00 00 FB 3F 80 00 00 FA 7F A0 00 00 FA 7F
 A0 00 00 94
GT [WIRELESS] R <-- : 717577.588904     00 00 00 03 19 00 00 00 00 00 fb 00 00 00 00 fb 3f 80 00 00 fa 7f a0 00 00 fa 7f a0 00 00
GT [WIRED] S --> : 717577.590635        86 00 00 18 43 EF 03 1A 00 00 00 00 00 00 FB 00 00 00 00 FB 3F 80 00 00 FA 7F A0 00 00 FA 7F
 A0 00 00 2B
GT [WIRELESS] R <-- : 717608.160753     00 00 00 03 19 00 00 00 00 00 fb 00 00 00 00 fb 3f 80 00 00 fa 7f a0 00 00 fa 7f a0 00 00
GT [WIRED] S --> : 717608.162482        86 00 00 18 43 EF 03 1A 00 00 00 00 00 00 FB 00 00 00 00 FB 3F 80 00 00 FA 7F A0 00 00 FA 7F
 A0 00 00 94
GT [WIRELESS] R <-- : 717638.457728     00 00 00 03 19 00 00 00 00 00 fb 00 00 00 00 fb 3f 80 00 00 fa 7f a0 00 00 fa 7f a0 00 00
GT [WIRED] S --> : 717638.460127        86 00 00 18 43 EF 03 1A 00 00 00 00 00 00 FB 00 00 00 00 FB 3F 80 00 00 FA 7F A0 00 00 FA 7F
 A0 00 00 94
```

Figure 28

Serial HART Debug Port

By selecting the “Serial HART Debug Port” option, you can see communications between the HMS and the HARTPORT on the module, provided that the debug port is not the same port that would normally be connected to the HMS.

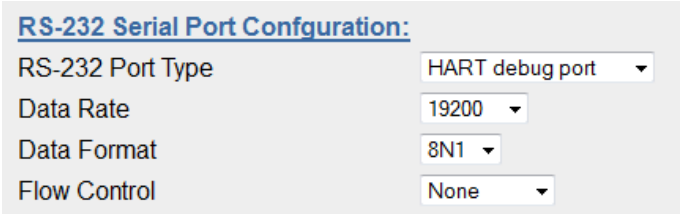


Figure 29

You will see similar data frames by connecting a terminal package or Windows HyperTerminal to the serial port at the configured baud rate, parity, and flow control. These data frames are the raw transmit and received data frames between the HARTPORT and the HMS.

Again, you will see two different frames. “WIRELESS” refers to data frames that have been received from the WirelessHART Gateway, and “WIRED” refers to data frames received and transmitted between the MUX and the HMS.

```
AP [WIRELESS] R <-- : 1055278.234695    86 00 00 18 55 65 A0 0A 00 00 00 17 0D 00 00 18 55 65 36
AP [WIRELESS] T --> : 1055278.236247    82 00 00 18 55 65 00 00 AA
AP [WIRELESS] R <-- : 1055567.966761    86 00 00 18 43 EF 1F 04 00 00 03 14 3E
AP [WIRELESS] T --> : 1055567.969709    82 00 00 18 43 EF 00 00 36
AP [WIRELESS] R <-- : 1055604.188136    86 00 00 18 43 EF 00 18 00 00 FE 40 ED 05 07 01 01 0C 01 12 34 57 05 04 00 00 00 00 40 00 40
 82 84
AP [WIRELESS] T --> : 1055604.771702    82 00 00 18 43 EF 0D 00 3B
AP [WIRELESS] R <-- : 1055609.259992    86 00 00 18 43 EF 0D 17 00 00 4C D0 52 53 1C B3 FF FF FF FF FF FF FF FF FF FF FF FF 00 00 00
 1A
AP [WIRELESS] T --> : 1055630.816656    82 00 00 18 43 EF 03 00 35
AP [WIRELESS] R <-- : 1055639.695629    86 00 00 18 43 EF 03 1A 00 00 00 00 00 00 FB 00 00 00 00 FB 00 00 00 00 FA 7F A0 00 00 FA 7F
 A0 00 00 2B
AP [WIRELESS] R <-- : 1055677.974935    81 40 00 18 43 EF 03 1A 00 00 00 00 00 00 FB 00 00 00 00 FB 3F 80 00 00 FA 7F A0 00 00 FA 7F
 A0 00 00 D3
AP [WIRELESS] R <-- : 1055705.639343    81 40 00 18 43 EF 03 1A 00 00 00 00 00 00 FB 00 00 00 00 FB 3F 80 00 00 FA 7F A0 00 00 FA 7F
 A0 00 00 D3
AP [WIRELESS] R <-- : 1055736.74339     81 40 00 18 43 EF 03 1A 00 00 00 00 00 00 FB 00 00 00 00 FB 3F 80 00 00 FA 7F A0 00 00 FA 7F
 A0 00 00 D3
AP [WIRELESS] R <-- : 1055766.510077    81 40 00 18 43 EF 03 1A 00 00 00 00 00 00 FB 00 00 00 00 FB 3F 80 00 00 FA 7F A0 00 00 FA 7F
 A0 00 00 D3
AP [WIRELESS] R <-- : 1055796.944660    81 40 00 18 43 EF 03 1A 00 00 00 00 00 00 FB 00 00 00 00 FB 3F 80 00 00 FA 7F A0 00 00 FA 7F
 A0 00 00 D3
AP [WIRELESS] R <-- : 1055824.843641    81 40 00 18 43 EF 03 1A 00 00 00 00 00 00 FB 00 00 00 00 FB 3F 80 00 00 FA 7F A0 00 00 FA 7F
 A0 00 00 D3
AP [WIRELESS] R <-- : 1055855.278797    81 40 00 18 43 EF 03 1A 00 00 00 00 00 00 FB 00 00 00 00 FB 3F 80 00 00 FA 7F A0 00 00 FA 7F
 A0 00 00 D3
AP [WIRELESS] R <-- : 1055885.713956    81 40 00 18 43 EF 03 1A 00 00 00 00 00 00 FB 00 00 00 00 FB 3F 80 00 00 FA 7F A0 00 00 FA 7F
 A0 00 00 D3
AP [WIRELESS] R <-- : 1055916.170810    81 40 00 18 43 EF 03 1A 00 00 00 00 00 00 FB 00 00 00 00 FB 3F 80 00 00 FA 7F A0 00 00 FA 7F
 A0 00 00 D3
AP [WIRELESS] R <-- : 1055944.231698    81 40 00 18 43 EF 03 1A 00 00 00 00 00 00 FB 00 00 00 00 FB 3F 80 00 00 FA 7F A0 00 00 FA 7F
 A0 00 00 D3
AP [WIRELESS] R <-- : 1055974.483981    81 40 00 18 43 EF 03 1A 00 00 00 00 00 00 FB 00 00 00 00 FB 3F 80 00 00 FA 7F A0 00 00 FA 7F
 A0 00 00 D3
AP [WIRELESS] R <-- : 1056004.935874    81 40 00 18 43 EF 03 1A 00 00 00 00 00 00 FB 00 00 00 00 FB 3F 80 00 00 FA 7F A0 00 00 FA 7F
 A0 00 00 D3
AP [WIRELESS] R <-- : 1056033.172019    81 40 00 18 43 EF 03 1A 00 00 00 00 00 00 FB 00 00 00 00 FB 3F 80 00 00 FA 7F A0 00 00 FA 7F
 A0 00 00 D3
AP [WIRELESS] R <-- : 1056063.396435    81 40 00 18 43 EF 03 1A 00 00 00 00 00 00 FB 00 00 00 00 FB 3F 80 00 00 FA 7F A0 00 00 FA 7F
 A0 00 00 D3
AP [WIRELESS] R <-- : 1056093.778392    81 40 00 18 43 EF 03 1A 00 00 00 00 00 00 FB 00 00 00 00 FB 3F 80 00 00 FA 7F A0 00 00 FA 7F
 A0 00 00 D3
AP [WIRELESS] R <-- : 1056124.127023    81 40 00 18 43 EF 03 1A 00 00 00 00 00 00 FB 00 00 00 00 FB 3F 80 00 00 FA 7F A0 00 00 FA 7F
 A0 00 00 D3
AP [WIRELESS] R <-- : 1056152.23715     81 40 00 18 43 EF 03 1A 00 00 00 00 00 00 FB 00 00 00 00 FB 3F 80 00 00 FA 7F A0 00 00 FA 7F
 A0 00 00 D3
```

Figure 30

Monitor HART Comms

Clicking the Monitor HART Comms link in the Diagnostics section on the main web page shows the same communication data frames as the WirelessHART Debug and Monitor HART Comms explained in the previous sections. The difference is that the communications are only monitored via the web page, and are not ported out either serial port.

Monitor HART Communications

```
GT [WIRELESS] R <-- : 175412.650451     40 00 00 03 19 00 00 00 00 00 fb 00 00 00 00 27 3e 17
31 d2 fa 7f a0 00 00 fa 7f a0 00 00
GT [WIRED] S --> : 175412.652045        81 40 00 18 C8 37 03 1A 00 40 00 00 00 00 FB 00 00 00
00 27 3E 17 31 D2 FA 7F A0 00 00 FA 7F A0 00 00 69

GT [WIRELESS] R <-- : 175415.887281     40 00 00 03 19 00 00 00 00 00 fb 00 00 00 00 fb 3f 80
00 00 fa 7f a0 00 00 fa 7f a0 00 00
GT [WIRED] S --> : 175415.888807        81 40 00 18 43 EF 03 1A 00 40 00 00 00 00 FB 00 00 00
00 FB 3F 80 00 00 FA 7F A0 00 00 FA 7F A0 00 00 93

GT [WIRELESS] R <-- : 175423.370827     d0 00 00 01 06 00 20 7f a0 00 00
GT [WIRED] S --> : 175423.371714        81 66 58 7A 19 30 01 07 00 D0 20 7F A0 00 00 C5

GT [WIRELESS] R <-- : 175438.365051     d0 00 00 01 06 00 20 7f a0 00 00
GT [WIRED] S --> : 175438.365995        81 66 58 7A 19 30 01 07 00 D0 20 7F A0 00 00 C5

GT [WIRELESS] R <-- : 175443.84798      40 00 00 03 19 00 00 00 00 00 fb 00 00 00 00 27 3e 01
33 e2 fa 7f a0 00 00 fa 7f a0 00 00
GT [WIRED] S --> : 175443.86361         81 40 00 18 C8 37 03 1A 00 40 00 00 00 00 FB 00 00 00
00 27 3E 01 33 E2 FA 7F A0 00 00 FA 7F A0 00 00 4D

GT [WIRELESS] R <-- : 175447.122669     40 00 00 03 19 00 00 00 00 00 fb 00 00 00 00 fb 3f 80
00 00 fa 7f a0 00 00 fa 7f a0 00 00
GT [WIRED] S --> : 175447.124204        81 40 00 18 43 EF 03 1A 00 40 00 00 00 00 FB 00 00 00
00 FB 3F 80 00 00 FA 7F A0 00 00 FA 7F A0 00 00 93

GT [WIRELESS] R <-- : 175456.119901     d0 00 00 01 06 00 20 7f a0 00 00
GT [WIRED] S --> : 175456.120978        81 66 58 7A 19 30 01 07 00 D0 20 7F A0 00 00 C5
```

Start Stop Clear Buffer Size: 3000

Figure 31

WirelessHART Network Topology

Clicking the WirelessHART Network Topology link in the Diagnostics section on the main web page opens a window displaying a graphical representation of the WirelessHART network (see Figure 32). This view shows the communication path between the field devices and the Gateway. You can see what paths the modules have taken for upstream communications (to the Gateway) and downstream communications (from the Gateway).

Radio path quality is also indicated by the different colored path lines. Green indicates a good path, orange a marginal path, and red a bad path.

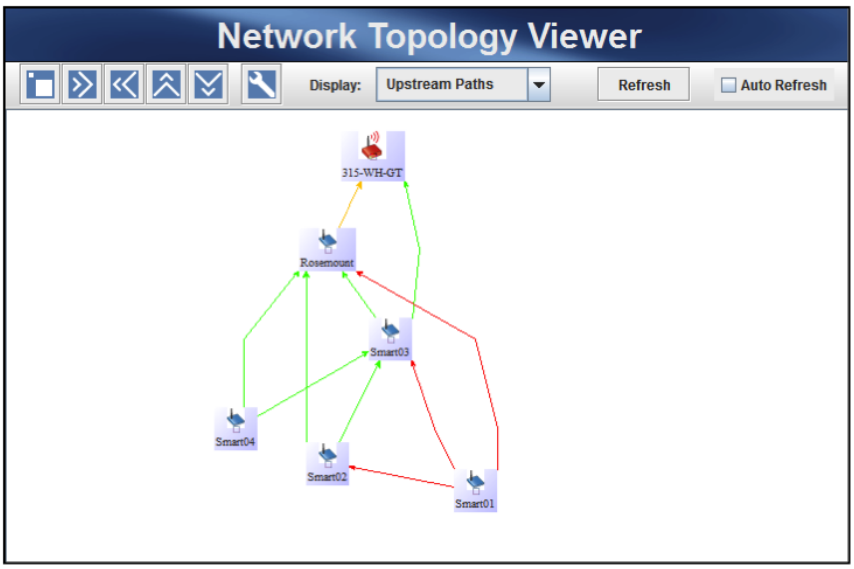


Figure 32

WirelessHART Device Information

The WirelessHART Device Information option shows the WirelessHART device IDs that can be heard by the Gateway. The list shows the HART MAC address, Device Short Tag (if the tag is unknown, it shows @@@@@@@@), the communication status (Operational or Idle), and the values of the four process variable (PV, SV, TV and QV).

The four process variables display the raw Floating Point value. If no value is present in the device, the value is undefined, or unpresentable it displays “nan,” as shown in the following figure.

Remote Devices Address List

Mac Address	Short Tag	State	PV	SV	TV	QV
00:00:18:C8:37	@@@@@@@@	Operational	0.000000	0.179866 mA	nan	nan
26:58:7A:19:30	GENERIC	Operational	nan °C	nan °C	25.250000 °C	7.134691 V
00:00:18:43:EF	SMART900	Operational	0.000000	1.000000	nan	nan

Figure 33

Clicking the Remote Device Mac Address link displays more information about the remote device, including the primary, secondary, tertiary and quaternary variables, receive signal level, and number of neighbors.

Device Details:

Address	26:58:7A:19:30
Nickname	8
Receive Signal Level	-42 dBm
Number of Neighbours	2
Parent (nickname)	1
Primary Variable	nan
Secondary Variable	nan
Tertiary Variable	25.000000
Quaternary Variable	7.134976

Figure 34

WirelessHART Statistics

Network Status

The Statistics page shows the status of the WirelessHART network and a number of other network parameters.

Manager Uptime	Amount of time since the manager software was last started.
Manager Hardware Model	The manager hardware model number.
Manager Software Version	Software version running on the manager.
Number of Live Motes (Remote devices)	Number of devices that are connected and reporting to the network.
Number of Unreachable Remotes	Number of devices/adapters that are not currently reporting to the network, but were in the network at some time in the past.

Network Statistics

The Network Statistics show the overall WirelessHART network condition. There are three main parameters, Reliability, Stability and Latency, and each is measured over three different times, Lifetime (the amount of time the module has been running), Last day, and Last 15 minutes.

Reliability—The percentage of expected data packets that the manager actually received. One-hundred percent reliability means that every expected packet was received. The reported values are network averages. The manager calculates data reliability by dividing the number of packets it received by the sum of packets received and packets lost. If the Reliability is below 99%, it is recommended that more devices be added to the network to act as repeaters.

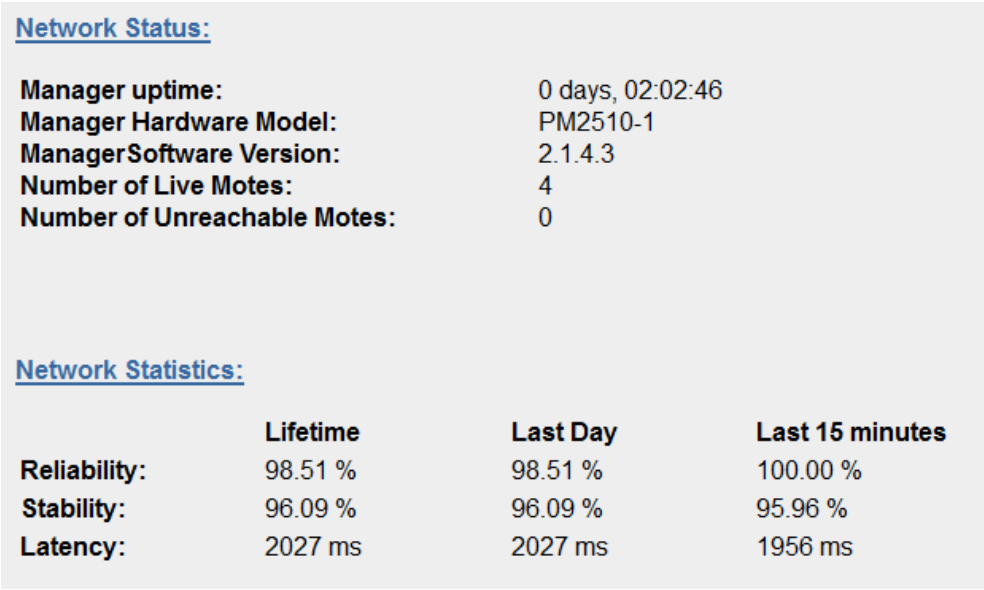
% Reliability = Packets Received / Total Packets x 100

Stability—Path stability measures transmissions between devices. It is the average percentage of data packets in the network that have successfully reached their destination. The manager calculates path stability by dividing the number of successfully transmitted packets by the total number of packets (successfully and unsuccessfully transmitted). If the Stability is below 60%, it is recommended that more devices be added to help with communications.

% Path Stability = Packets Successfully Transmitted / Total Packets x 100

Latency—The average time (in milliseconds) required for a data packet to travel from the originating device to the manager. Latency varies across the network, and is dependent on the number of devices in the network and their configured update rates. The value represents the average network latency. The manager calculates data latency for each packet by subtracting the time the packet was received at the manager from the packet timestamp, which indicates when the packet was sent by the device.

Data Latency = Received Packet Timestamp - Transmitted Packet Timestamp



Network Status:

Manager uptime:	0 days, 02:02:46
Manager Hardware Model:	PM2510-1
ManagerSoftware Version:	2.1.4.3
Number of Live Motes:	4
Number of Unreachable Motes:	0

Network Statistics:

	Lifetime	Last Day	Last 15 minutes
Reliability:	98.51 %	98.51 %	100.00 %
Stability:	96.09 %	96.09 %	95.96 %
Latency:	2027 ms	2027 ms	1956 ms

Figure 35

5.2 Wi-Fi Network

The Wi-Fi Network link displays the Wi-Fi Ethernet Modem menu structure, which allows you use any of the standard Ethernet modem features.

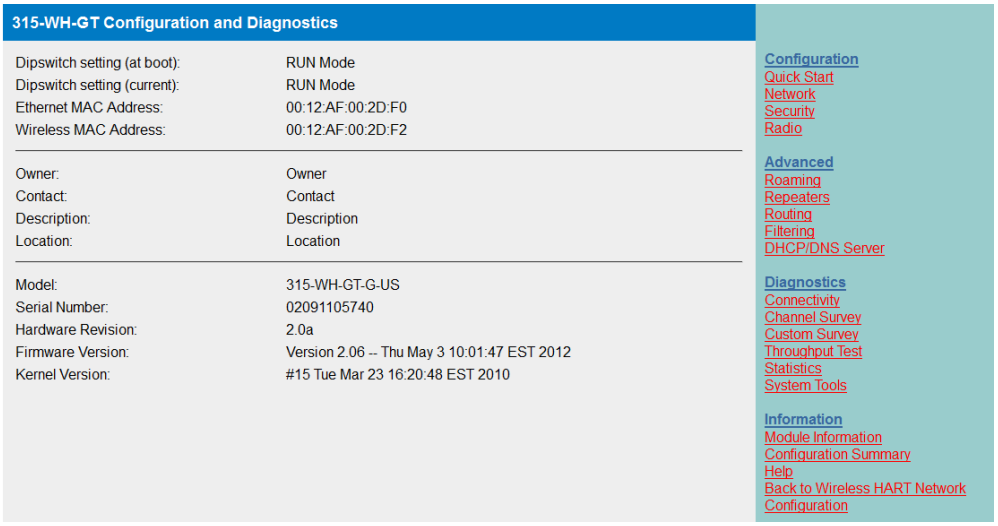


Figure 36

Normal setup for the modules is with the Gateway configured as a client and the Data Concentrator configured as an access point.

The easiest way to configure this on 315-WH-Series modules is to use the Quick Start Configuration option from the menu on the right. For most applications, no further configuration is required. However, for more advanced applications, the other parameters can be changed using the normal configuration pages after the Quick Start configuration has been saved.

The following steps should be performed on both the Gateway and Data Concentrator modules to ensure that they are setup correctly.

To use Quick Start Configuration:

1. Click **Quick Start** from the menu on the right, and then configure the following parameters.

Parameter	Quick Start Configuration
Operating Mode	Access Point or Client. Bridge operation is assumed - for Router selection; go to the Network page after *Quick Start* has been completed. The Gateway should be configured as a client and the Data Concentrator should be an access point.
Default Gateway	This is the address that the device will use to forward messages to remote hosts that are not connected to any of the local bridged network (Ethernet or Wireless).
IP Address / Subnet Mask	IP Address and Subnet Mask for your application.
System Address (ESSID)	The system address is a text string, 1 to 31 characters in length, used to identify your system.
Radio Encryption	Radio encryption selection - None, WPA-PSK (TKIP), WPA-PSK (AES) or WPA2. Refer to the *245U-E Ethernet Modem Configuration Manual* for other encryption options, such as WEP or Enterprise encryption.
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 in length, and must be the same for all 315-WH-Series units in the system.

2. When finished, click **Save to Flash and Reset** to complete the Wi-Fi setup.

The following sections outline some of the diagnostic features available in the module that may be of help when setting up a Wi-Fi Network between the Gateway and Data Concentrator modules. For a description of all the diagnostic and operational characteristics of the modem, review the 245/945U-E Ethernet Modem documentation available on our web site.

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 its 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 To update the Connectivity webpage, hold down the CTRL key and click the Refresh button.

Channel Survey

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

The modems allow you to see how much RF activity is on a given channel as a percentage of the total channel 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. They are also valuable diagnostics tools for identifying the spare capacity on a given channel, as well as possible sources of interference.

The Channel Survey screen displays a graph showing the percentage of time that a channel is unavailable, or busy, due to three possible 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

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

The first screen (Figure 37) shows the percentage of the overall radio traffic on the channel that is currently being used.

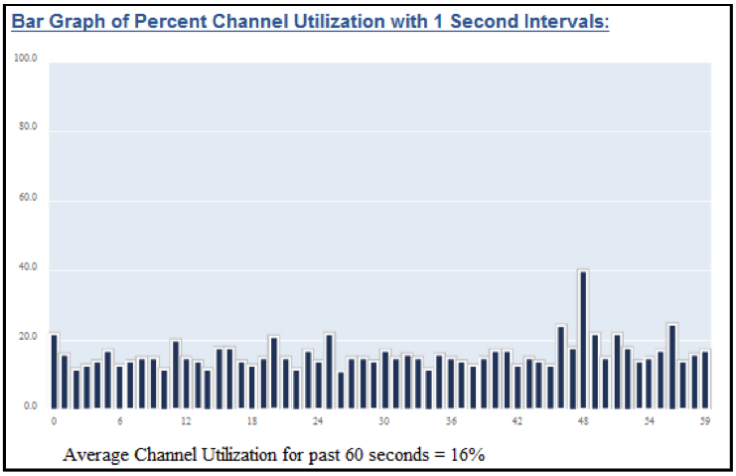


Figure 37

The next screen (Figure 38) shows the radio receive noise floor for the last 60 seconds.

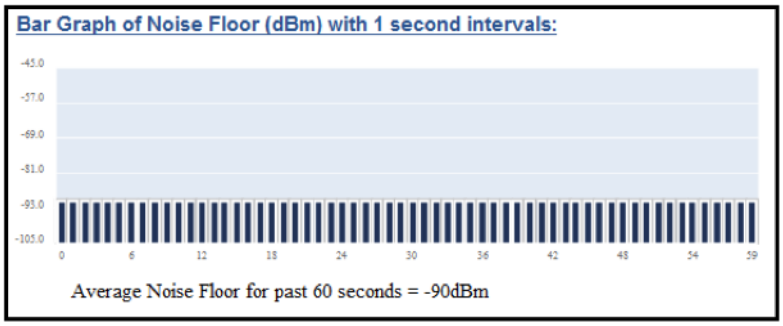


Figure 38

The next screen (Figure 39) shows the average channel utilization for each minute up to one hour. It also provides a running average for the total number of minutes, up to 59 minutes.

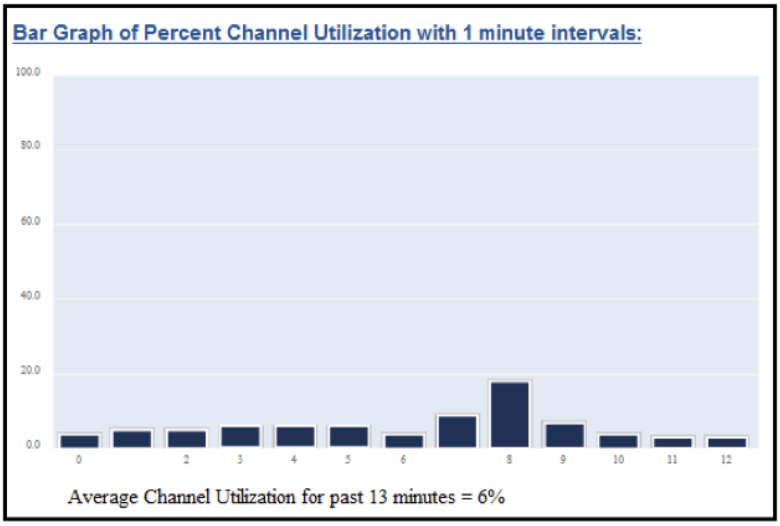


Figure 39

The next screen (Figure 40) shows the running radios receive noise floor average for each minute, up to 59 minutes.

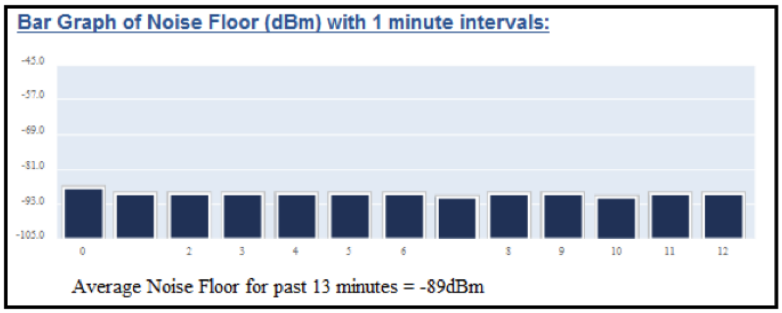


Figure 40

The Channel Survey page also shows two additional screens (not shown) that indicate the Percent Channel Utilization and Noise Floor in one hour intervals. The screens only show the last 24-hour period.

Custom Survey

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

Percent Radio TX	All transmitted messages from the radio to other devices.
Percent Radio RX	All DSSS or OFDM messages received by the radio (any Standard Wi-Fi data packets from either ELPRO or competitor radios).
Percent Busy (CCA or Noise)	Clear Channel Assessment is the detection of any ongoing transmissions or noise, such as Microwaves, 2.4 Mhz 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 and received, and the amount of other noise that can be heard at the radio. Configure what you want logged on each chart, select a time interval, and save changes. The charts are 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

In Figure 41, 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). You can see from these charts that there is very little outgoing data, but a constant stream of data is being received.

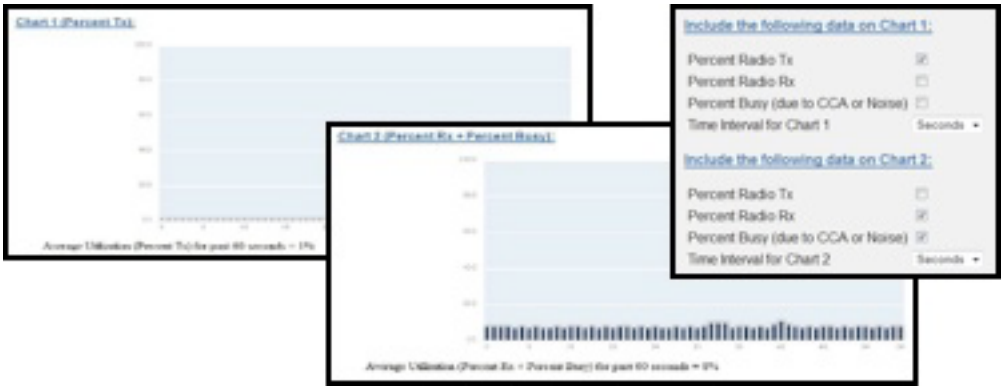


Figure 41

Example 2

In Figure 42, you can see that chart one shows the amount of Data being received from Wi-Fi devices and chart two shows the amount of other noise that is being received. From this, you can see that in the last 60-second period there was a 20-second interval with around 60-80 % channel Utilization in this case from a 2.4 MHz FHSS telemetry device.

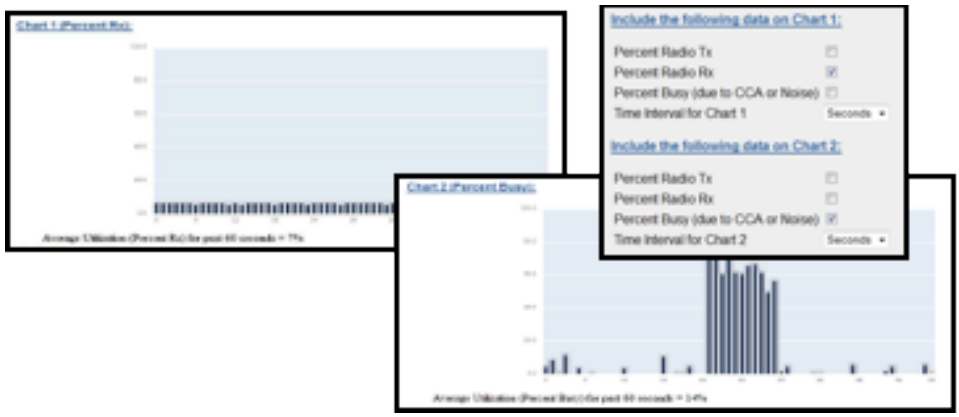


Figure 42

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

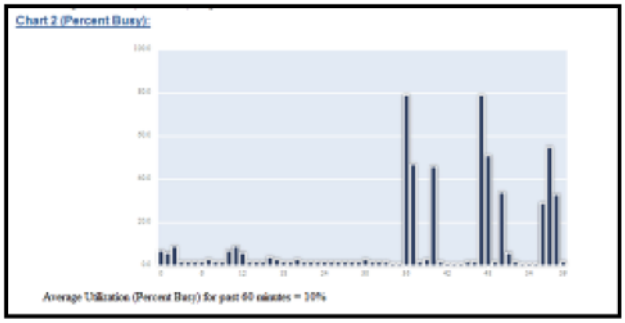


Figure 43

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. The 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).

The Iperf utility is built into the modems for convenience, and allows measurement of TCP throughput with default Iperf parameters. For access to all Iperf features and a slightly more accurate result due to module processor overheads, it is recommended that Iperf be run externally on a PC or laptop. For details, refer to the section “External Iperf Test” in the *245U/945U-E User Manual*.

Before testing, ensure that the end node of the Wi-Fi Link you want to test has the Iperf Server option enabled on the Advanced Radio Settings page, and that this setting is Saved to Flash and the module has been reset (see Figure 44).

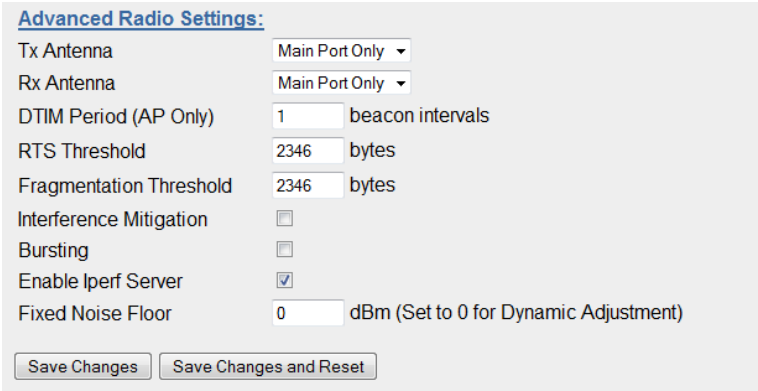


Figure 44

To conduct a TCP throughput test:

1. Connect to the web page of the module that will be performing the Iperf test.
2. Click the **System Tools** link on the menu on the right, and then select "TCP Throughput Test."

   The screen in Figure 45 appears.

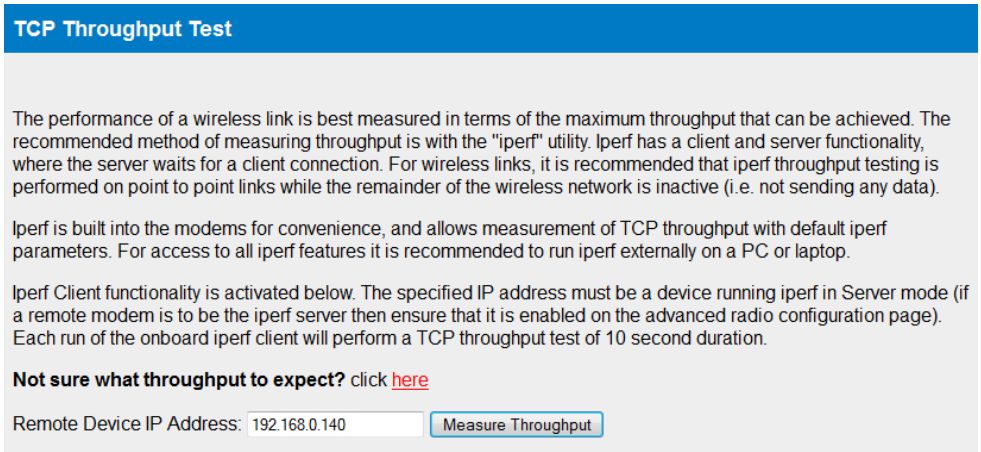


Figure 45

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

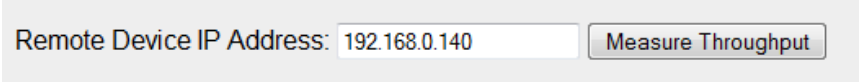


Figure 46

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

   Each click of the Measure Throughput button performs a 10-second TCP throughput test. The message "Performing Iperf Test" appears, and the TX/Link & RX LEDs on the module flash very fast as it performs the test. Approximately 10 seconds later, a graph showing the actual throughput over the 10-second period and a calculated average is displayed.

   NOTE The specified IP address must be running Iperf in Server mode. If the remote modem does not have the Iperf server running, you will see the Error message "Iperf error, check connectivity to server." Ensure that Enable Iperf Server is selected and the module is reset before re-testing.

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

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

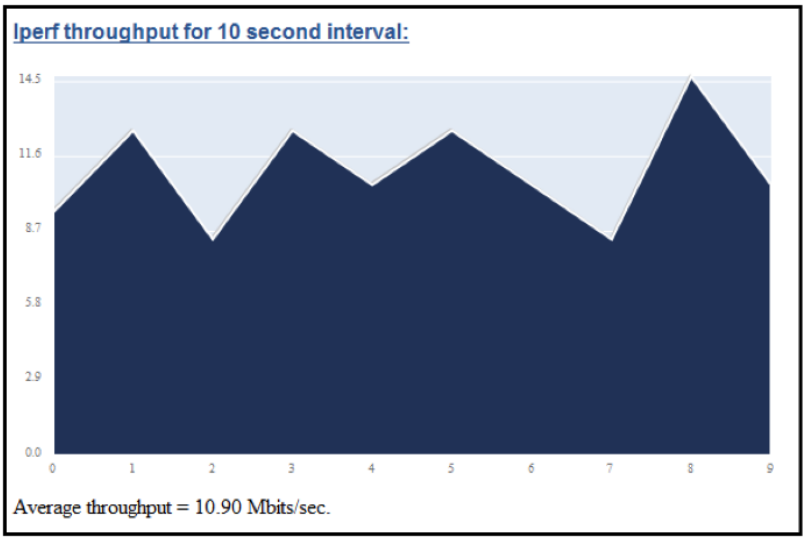


Figure 47

Statistics

The Statistics webpage (Figure 48) is used for advanced debugging of 315-WH-Series. This webpage details the state of the 315-WH-Series and performance information. It is typically useful to ELPRO technical support personnel in diagnosing problems with the module.

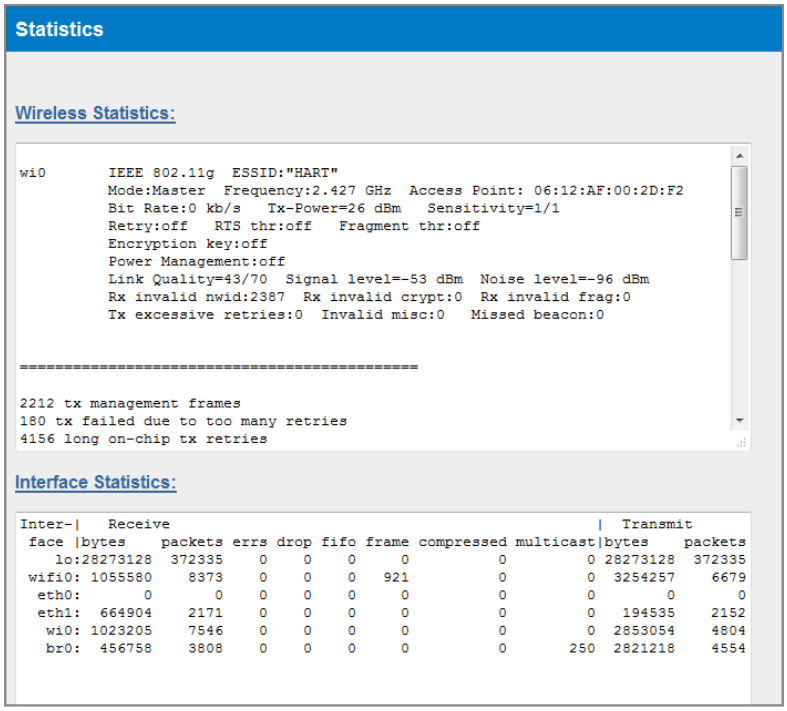


Figure 48

NOTE When updating the Statistics webpage, you need to hold down the CTRL key while clicking the Refresh. Otherwise, the information will not be updated.

Network Traffic Analysis

Many freely available devices and PC programs (such as Ethereal) will analyze the performance of an Ethernet network and can provide a simple cost effective means for more advanced analysis. By monitoring traffic on the wired Ethernet, a better idea of regular traffic can be discovered. Network analysis programs make configuration of a filter for the 315-WH-Series a simple task.

5.3 Ethernet 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 you are trying to reach is actually operating. For example, if a user cannot ping a host then 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.

To ping a device:

1. Click the **Start Menu** and click **Run**.
2. Type “came” and press **Enter**.

   The command screen appears. A directory is specified (unique to your own PC) with a flashing cursor.
3. At the cursor, type the word “ping” leaving a space and type the default IP address for the 315-WH-Series at first startup.

   For example: ping 192.168.0.118
4. Press **Enter**.

   The PC replies with an acknowledgment of the command. If the 315-WH-Series is correctly configured the reply looks something like Figure 49.

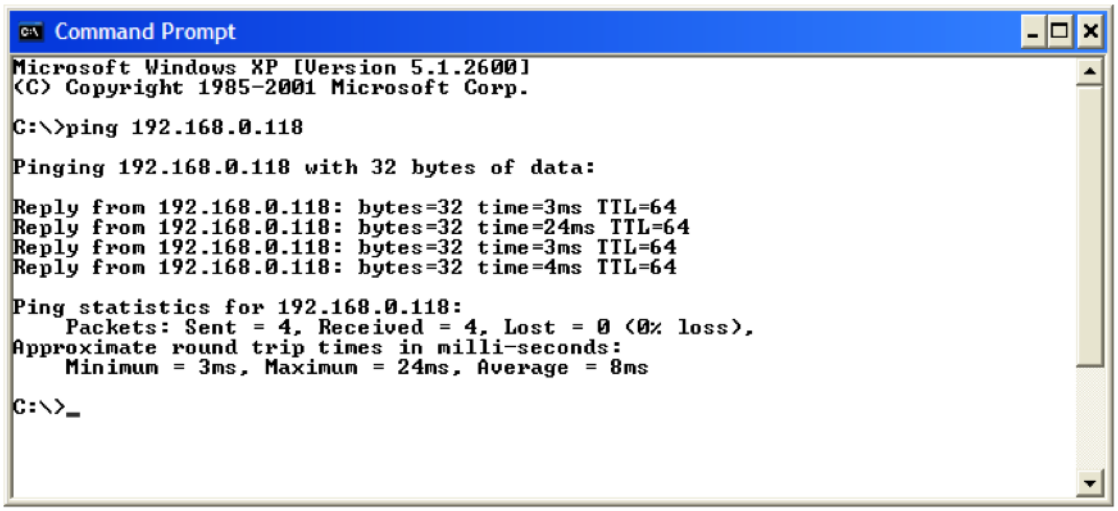


Figure 49

You can use the “ping –t” command to repeatedly ping the specified node in the network. To cancel the ping, use CTRL+C. When you enter CTRL+C the program reports a packet sent-received-lost percentage. Figure 50 shows the response of the “ping –t 192.168.0.118” command.

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.

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

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

Figure 50

ipconfig

The “ipconfig” command can be used to show current TCP/IP information, such as your address, DNS server addresses, and adapter type. In the following example, “ipconfig” was entered at the command prompt. The reply shows the PC’s IP address, subnet mask and the default Gateway.

Other ipconfig commands return more information:

- ipconfig /all shows the hardware or MAC address of the computer
- Ipconfig /? lists all available options and their usage

```
Command Prompt
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 . . . . . . . . . : 192.168.0.1

C:\>
```

Figure 51

arp

The “arp” command displays and modifies the IP-to-Physical address translation tables used by Address Resolution Protocol (ARP). Once a remote computer has been pinged, the “arp” command can be used to see the IP address & MAC address of the remote computer. It will also show any other devices on the network that it may be connected to.

The command “arp –a” produced the results shown in Figure 52. It shows the PC’s direct IP address of 192.168.0.17 as also shown before with “ipconfig” command. The other IP address shown with its associated MAC address is another device with a connection to the PC. In this example, it is the IP address of a PLC also connected to the PC. The command “arp –n” lists all the commands available for this function.

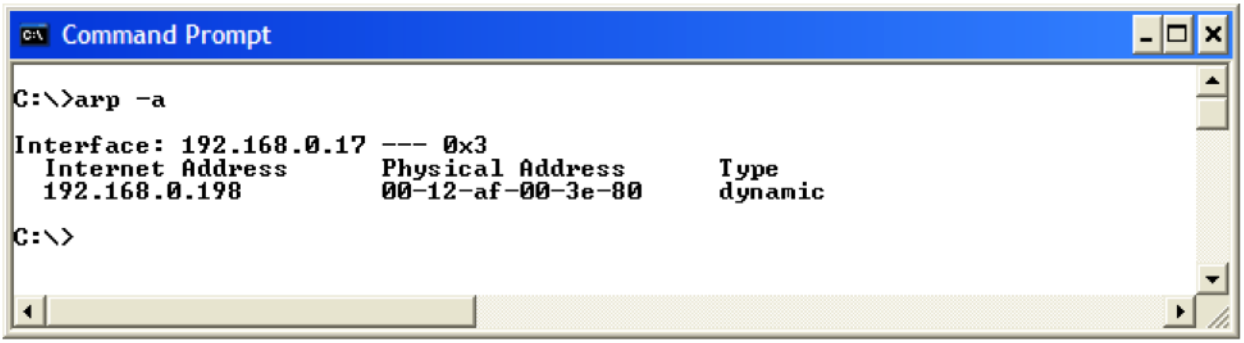


Figure 52

route

The “route” command is used for the Router function, when you are joining two different networks together using the 315-WH-Series (refer to “Chapter 1 - INTRODUCTION”).

The 315-WH-Series can only accept one Routing table. That is it can only accept one router per network of radios. On the Router radio network PC a routing rule needs to entered to allow access between Network A and Network B. This is entered in the command prompt, as per all other instruction above.

- Route PRINT shows all active routes on PC.
- Route ADD adds a routing table to network.
- Route DELETE <destination netmask gateway interface> deletes the unwanted routing table.
- Route CHANGE modifies an existing route.

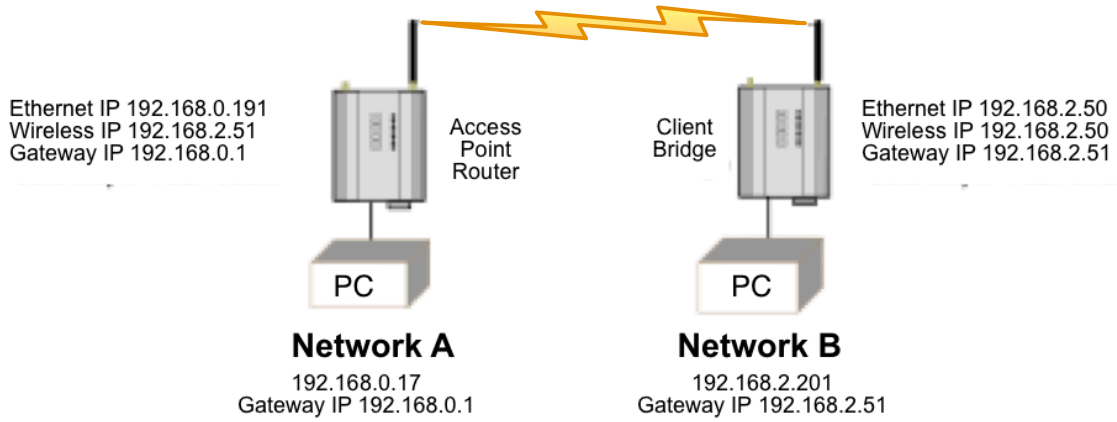


Figure 53

The following is an example of a routing table for the configuration.

Network A Settings	Client Bridge Settings
IP Address 192.168.0.17	Gateway IP 192.168.2.51
Subnet Mask 255.255.255.0	Ethernet IP 192.168.2.50
Gateway IP 192.168.0.1	Subnet Mask 255.255.255.0
	Wireless IP 192.168.2.50
	Subnet Mask 255.255.255.0

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

The PC on Network A requires a routing rule is to be set. To enter the routing rule, open a command prompt and type the following:

Route ADD 192.168.2.0 MASK 255.255.255.0 192.168.0.191

This will allow the PC on Network A to communicate with any device on the Network. It is indicating that if communicating to a device with an IP Address of 192.168.2.0 and a subnet mask of 255.255.255.0 (any device on the 192.168.2.0 network), all communications need to be routed through 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 into the table. Once entered, the router will determine whether to pass information over the router if it is addressed to do so. For added security, MAC address filtering could be added as mentioned earlier.

CHAPTER 6 - SPECIFICATIONS

General	
EMC specification	EN 300 683, FCC Part 90
Radio specification	EN 300 328, FCC Part 15.247, RSS 210
Emission designator	As per 802.11 standard
Hazardous Spec	Class 1 Division 2 groups A, B and C
IP Rating	IP20
Module Housing	Powder-coated, extruded aluminum 315-WH-GT = 115 x 138 x 66 mm, 4.5” x 5.4” x 2.6” 315-WH-DC = 115 x 138 x 36 mm, 4.5” x 5.4” x 1.4”
Mounting	DIN rail mount
Terminal blocks	Removable, Suitable for 12 gauge (2.5 sqmm) conductors
LED indication	Module Status, Serial RX and TX, Radio RX and TX, Radio Link, Ethernet Activity / Link and WirelessHART
Operating Temp	-40 to +60°C, -40 to +140°F
Humidity	0 – 99% RH non-condensing
Pollution Degree	2
Installation Category	2
Altitude	2000m

Power Supply	
Battery supply	N/A
AC Supply	N/A
DC Supply	9 to 30 Vdc, Overvoltage and reverse voltage protected
Solar Supply	N/A
Analog Loop Supply	N/A
Static Current Drain	
315-WH-DC	240 mA @ 12 Vdc or 150 mA @ 24 Vdc
315-WH-GT	330 mA @ 12 Vdc or 210 mA @ 24 Vdc
TX Current drain	**490 mA @ 12 Vdc or 310 mA @ 24 Vdc**
Battery charging current	**N/A**

Radio Transceiver 802.11b/g Wi-Fi	
Operating Frequency	First channel center at 2.412 GHz
Channels / Hop sets	11 x 5 MHz Spacing
Line of Site Range	1 km @100 mW (EU), 3 miles/5km @ 400 mW (Americas/Australia)
Antenna Connector	SMA
Radio data rate	1 to 54 Mb/s (-G model), Turbo – 108 Mb/s

Transmitter 802.11b/g Wi-Fi	
Transmit power (Power may be limited by country-specific configuration)	1-24 Mb/s: 400 mW (+26 dBm) 1-24 Mb/s: 400 mW (+26 dBm) 36 Mb/s: 250 mW (+24 dBm) 48 Mb/s: 160 mW (+22 dBm) 54 Mb/s: 125 mW (+21 dBm)
Modulation	IEEE 802.11 DSSS

Receiver 802.11b/g Wi-Fi	
RX Sensitivity	-97 dBm @ 1 Mb/s, -94 dBm @ 6 Mb/s -90 dBm @ 18 Mb/s, -74 dBm @ 54 Mb/s
Frame Error Rate (FER)	8% FER

Radio Transceiver 802.11a Wi-Fi	
Operating Frequency	5.180 GHz – 5.825 GHz
Channels / Hop sets	12 fixed channels, (3 Turbo Mode) or Auto Channel/Group selection
Line of Site Range	1 km @100 mW (EU), 3 miles/5 km @ 400 mW (Americas/Australia)
Antenna Connector	SMA
Radio data rate	6 to 54 Mb/s (-A model), Turbo – 108 Mb/s

Transmitter 802.11a Wi-Fi	
Transmit power (Power may be limited by country-specific configuration)	6-24 Mb/s: 400 mW (+26 dBm) 36 Mb/s: 250 mW (+24 dBm) 48 Mb/s: 160 mW (+22 dBm) 54 Mb/s: 125 mW (+21 dBm)
Modulation	IEEE 802.11 DSSS

Receiver 802.11a Wi-Fi	
RX Sensitivity	-94 dBm @ 6 Mb/s, -90 dBm @ 18 Mb/s, -74 dBm @ 54 Mb/s
Frame Error Rate (FER)	8% FER

Radio Transceiver 802.15.4 WirelessHART	
Operating Frequency	2.400 GHz – 2.4835 GHz
Channels / Hop sets	15
Line of Site Range	100 – 300 m – Outdoor, PA enabled (default) 25 – 100 m – Indoor, PA disabled
Antenna Connector	SMA
Radio data rate	250 Kbps

Transmitter 802.15.4 WirelessHART	
Transmit power	6.3 mW (+8 dBm) with PA enabled (default) 630 uW (-2 dBm) with PA disabled
Modulation	IEEE 802.15.4 DSSS

Receiver 802.15.4 WirelessHART	
RX Sensitivity	-92.5 dBm @ 50% PER, -90 dBm @ 1% PER

Serial Ports	
RS232 Port	DB9 female DCE, RTS/CTS/DTR/DCD hardware signals provided
RS485 Port	2 pin terminal block, Max distance 4000’ / 1.2 km
Transmission Modes	7 or 8 data bits
Data rates	1200, 2400, 4800, 9600, 14400, 19200, 38400, 57600, 76800, 115200
Parity	Configurable, Odd, Even, None
Stop Bits	Stop/start

Comms Fail Output	
D/O Max voltage	FET output to common rated at 30 Vdc
D/O Max current	500 mA

System Parameters	
Encryption	WEP (64 bit and 128 bit), WPAPSK (TKIP), WPAPSK (AES), WPA2-PSK(AES), WPAPSK/WPA2-PSK, WPA Enterprise
User Configuration	Via embedded web page, Via RS232 commands, or RS232 PPP connection
Diagnostics LEDs	Power / OK, Ethernet Link, Activity, 100 mb/s, Radio Link, RX, Rx Weak Signal, TX, Serial RX/TX, WirelessHART Communications status
Other	RSSI measurement in dBm Connectivity information System log file

APPENDIX A - FIRST TIME CONNECTION

Accessing Configuration for the First Time

Because the default IP address is within the range 192.168.0.XXX, the 315-WH-Series 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 315-WH-Series with factory default settings. This is the preferred method and is much less complicated than the second method. You will need a straight-through Ethernet cable between the PC Ethernet port and the 315-WH-Series. The factory default Ethernet address for the 315-WH-Series 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 315-WH-Series 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 your network settings.

Method 1 – Set PC to the Same Network as the 315-WH-Series

1. Connect the Ethernet cable between the 315-WH-Series and the PC configuring the module.
2. Set the Factory Default Switch to the SETUP position.

   This setting causes the 315-WH-Series to always start 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 315-WH-Series module.
4. From the **Start** menu, click **Control Panel** and **Network and Internet**. Then, click **Network and Sharing Center** and click **Change Adapter Settings.**

   The following description is for Windows7. Earlier Windows operating systems have similar settings.
5. Right-click **Local Area Network** and click **Properties**.
6. Select **Internet Protocol Version 4 (TCP/IPv4)**, and click **Properties**

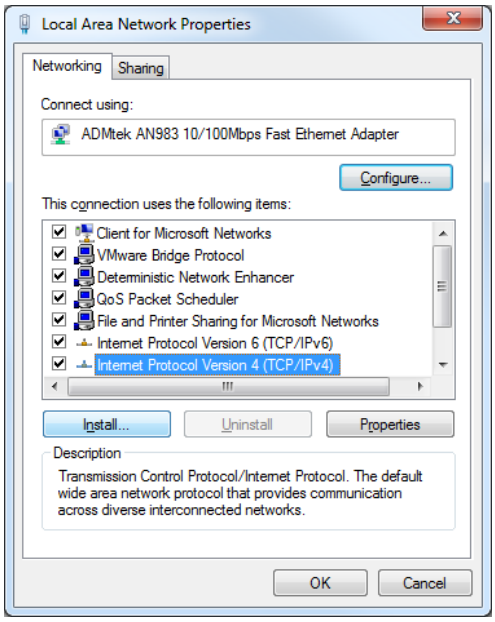


Figure 54

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

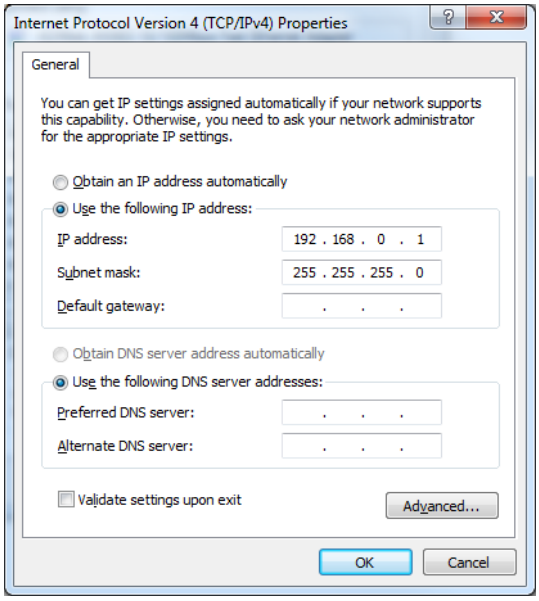


Figure 55

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 315-WH-Series:

   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.”

    The main Welcome screen displays.

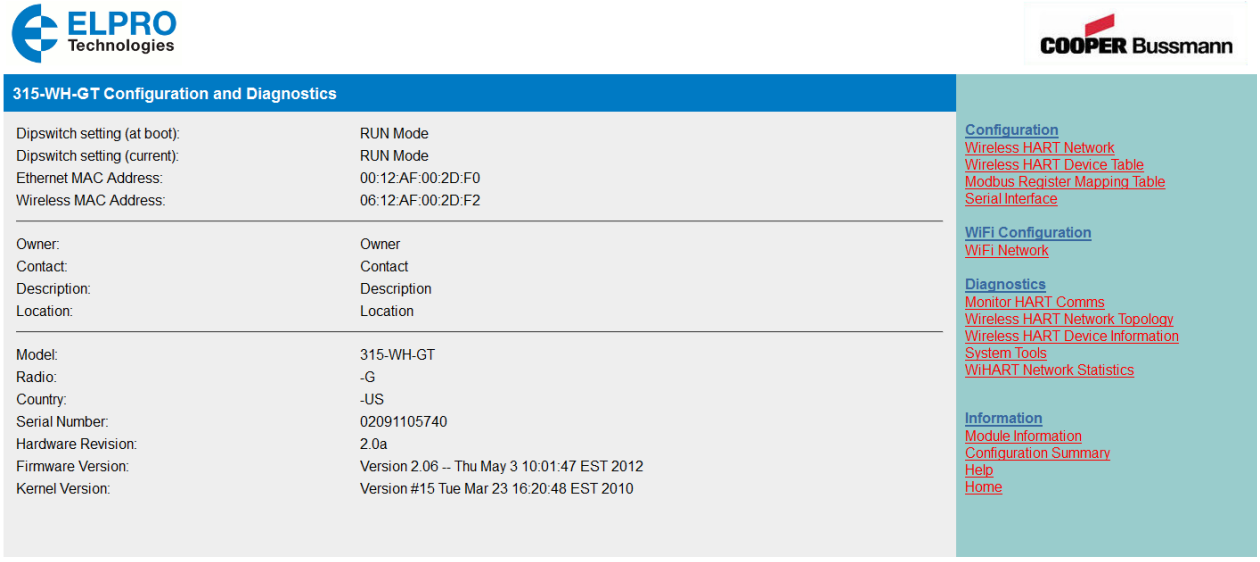


Figure 56

11. To resume normal configured operation when Configuration is complete, switch the Factory Default DIP switch on the 315-WH-Series to RUN, and then cycle power.

NOTE Security Certificates. Configuration of the 315-WH-Series uses an encrypted link (https). The security certificate used by the 315-WH-Series is issued by ELPRO and matches the IP address 192.168.0.100.

When you first connect to the 315-WH-Series, your web browser issues a warning that ELPRO is not a trusted authority. Ignore this warning and proceed to the configuration web page. To avoid seeing this warning in future, you can install the certificate on your browser.

Internet Explorer 7 has an additional address check on security certificates. Unless the 315-WH-Series has the address 192.168.0.100, when you first connect to the 315-WH-Series, Internet Explorer 7 issues a warning about mismatched security certificate address. You can turn off this behavior in IE7 by selecting the following:

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

Method 2 – Set 315-WH-Series 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 315-WH-Series for it to appear on your network. Ask your system administrator if you do not know the correct settings for your network. The default IP address of the 315-WH-Series is 192.168.0.1, and the network you want to connect to is on 10.10.0.X (PC is on 10.10.0.5).

Once you have determined the correct settings for your network, you need to connect to the modem’s RS-232 serial port. Use a terminal package such as HyperTerminal to connect at 115,200 baud, eight data bits, 1 stop bit, no parity.

1. Open **HyperTerminal** and monitor.
2. Set the **SETUP/RUN** switch to the **SETUP** position, and connect power to the modem.
3. Wait for the ELPRO Dragon screen (Figure 57) to appear in HyperTerminal.

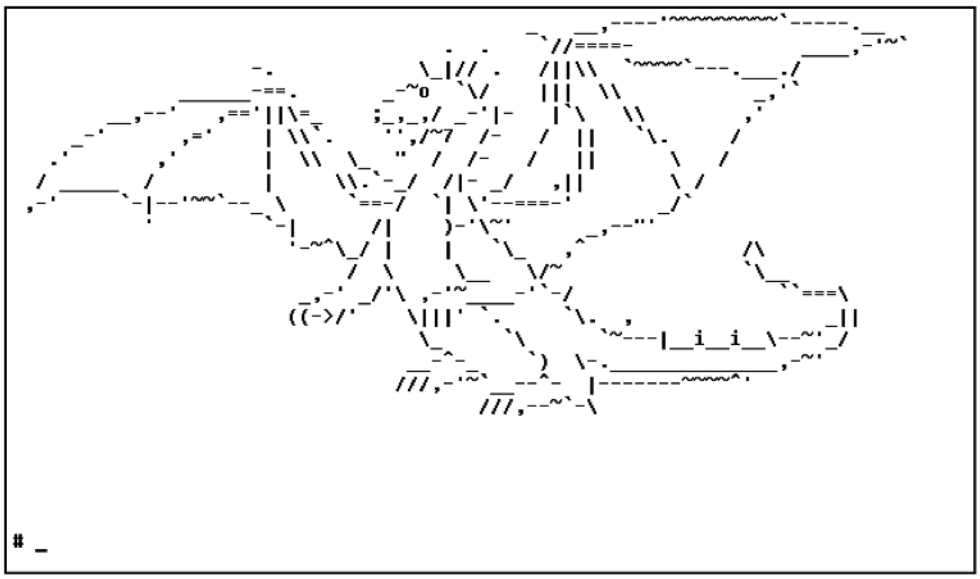


Figure 57

4. At the # prompt, type “ifconfig” to show the configuration of the Ethernet port and its current IP address.

   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 something that will enable connection to your local network.

   For example, type “ifconfig eth0 10.10.0.5 netmask 255.255.255.0”. Only add the netmask if the netmask is anything other than the standard 255.255.255.0.

   The IP address should now be changed. You can check by typing “ifconfig” again. Note these changes are only temporary, and if the module is reset, they will return to the normal default (192.168.0.XXX).

6. 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.

7. Enter the IP address for the 315-WH-Series into the Internet Explorer Address bar, e.g., http://10.10.0.5, which is the IP address you temporarily configured with the ifconfig command.

8. Enter the username “user” and default password “user.”

   You should now be connected to the main index page on the modem, as shown in Figure 56.

9. Connect to the Network page and change the Ethernet Interface and Wireless Interface IP addresses to 10.10.0.5.

10. On the 315-WH-Series, set the RUN/SETUP switch back to RUN.

11. Click **Save Changes and Reset**.

APPENDIX B - HART COMMANDS

HART Universal Commands

Command Number	Description
0	Read Unique Identifier
1	Read Primary Variable
2	Read Loop Current and Percent Of Range
3	Read Dynamic Variables and Loop Current
6	Write Polling Address
7	Read Loop Configuration
11	Read Unique Identifier Associated with Tag
12	Read Message
13	Read Tag, Descriptor, Date
15	Read Device Information
16	Read Final Assembly Number
17	Write Message
18	Write Tag, Descriptor, Date
19	Write Final Assembly Number
20	Read Long Tag
21	Read Unique ID associated with Long Tags
22	Write Long Tag
38	Reset Configuration Changed Flag
42	Perform Device Reset
48	Read Additional Device Status
74	Read I/O System Capabilities
75	Poll Sub-Device
77	Send Command to Sub-Device
84	Read Sub Device Identity Command
106	Flush Delayed Responses of Host

HART Port (Multiplexor) Specific Commands

Command Number	Description
128	Read HARTPORT Parameters
129	Read Loop Status
130	Read Instrument List From Index
131	Read Instrument Static Data
133	Remove Instrument From Instrument List
134	Read Scan List From Index
135	Read Instrument Dynamic Data
136	Read Instrument Scan Status
137	Write Instrument Scan Status
138	Read Instrument Cumulative Responses
139	Reset Instrument Cumulative Responses
140	Read Instrument Counts of Tries and Failures
141	Reset Instrument Counts of Tries and Failures
142	Read Counts of Host Communications
143	Reset Counts of Host Communications
144	Read Retry Limits
145	Write Retry Limits
146	Read Scan Command
147	Write Scan Command
148	Read Scan Status
149	Write Scan Status
150	Read Gender
151	Write Gender
152	Read Loop Search Type
153	Write Loop Search Type
154	Rebuild Loops
155	Copy Command and Reply
156 *	Write Device Table
157 *	Read Device Table List From Index
158 *	Commit Device Table
159 *	Rebuild All Loops
160 *	Get Gateway List
161 *	Write Modbus Table List
162 *	Read Modbus Table List
163 *	Commit Modbus table list
164 *	Activate Modbus Table
247	Command Write MTL 4841 Mode
* Custom ELPRO commands.	

APPENDIX C - WIRELESSHART COMMANDS

This appendix lists describes the WirelessHART commands that are supported in the 315-WH product.

HART CMD	Description
Physical Commands	
797	Write Radio Power
798	Read Radio Power
804	Read Radio CCA Mode
805	Write Radio CCA Mode
Data Link Layer Commands	
795	Write Timer Interval
796	Read Timer Interval
773	Write Network Id
774	Read Network Id
781	Read Device Address
783	Read Super Frame Entries
784	Read Link Entries
785	Read Graph Connections
786	Read Neighbor Properties
787	Read Neighbor Table
788	Alarm Path Down
806	Read Maintenance Frame Status
807	Enable Maintenance Frame
810	Read Join Priority
811	Write Join Priority
812	Read Packet Priority
813	Write Packet Priority
Network Layer Commands	
768	Write Join Key
769	Read Join Status
770	Request Active Advertise
771	Force Join
772	Read Join Shed Time
808	Read Time-to-Live
809	Write Time-to-Live
814	Read Black-list Entry
815	Write Black-list Entry
816	Delete Black-list Entry
Gateway Commands	
775	Write Network Tag
776	Read Network Tag
832	Read Network Information
836	Flush Cached Responses for a Device
837	Write Update Notification Bit Mask for a Device

HART CMD	Description
838	Read Update Notification Bit Mask for a Device
839	Cancel Update Notification
840	Change Notification

APPENDIX D - GLOSSARY

Term	Definition
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.
Antenna Gain	Antennae do not increase the transmission power, but instead focus the signal. Instead of transmitting in every direction (including the sky and ground) the signal is usually focused more horizontally or in a particular direction. This gain is measured in decibels.
Bandwidth	The maximum data transfer speed available to a user through a network.
Bridge	A bridge is used to connect two local area networks. Bridges are typically used to connect wireless networks to wired networks. Typically, bridges transfer messages between networks only when the message destination is on the other network. Messages destined for the same network as they originated on are not passed to the other network, which reduces traffic on the entire network.
Collision Avoidance	A network node procedure for proactively detecting that the node can transmit a signal without risking a collision with transmissions from other network nodes.
Client / Sta / Station	A device on a network that gains access to data, information, and other devices through a Server (access point).
Crossover Cable	A special cable used for networking two computers without the use of a hub. Crossover cables may also be required for connecting a cable or DSL modem to a wireless gateway or access point. The cable is wired so that the signals “crossover,” connecting transmit signal on one side to receiver signals on the other.
CSMA/CA	Carrier Sense Multiple Access/Collision Avoidance is a “listen before talk” method of minimizing (but not eliminating) collisions caused by simultaneous transmission by multiple radios. IEEE 802.11 states that a collision avoidance method rather than a collision detection must be used, because the standard employs half duplex radios (radios capable of transmission or reception, but not both simultaneously). Unlike conventional wired Ethernet nodes, a WLAN station cannot detect a collision while transmitting. If a collision occurs, the transmitting station will not receive an ACKnowledge packet from the intended receive station. For this reason, ACK packets have a higher priority than all other network traffic. After completion of a data transmission, the receive station will begin transmission of the ACK packet before any other node can begin transmitting a new data packet. All other stations must wait a longer pseudo-randomized period of time before transmitting. If an ACK packet is not received, the transmitting station will wait for a subsequent opportunity to retry transmission.
CSMA/CD	Carrier Sense Multiple Access/Collision Detection is the access method used on an Ethernet network. A network device transmits data after detecting that a channel is available. However, if two devices transmit data simultaneously, the sending devices detect a collision and retransmit after a random time delay.
DHCP	Dynamic Host Configuration Protocol 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 in all the IP addresses of all the computers on the network. If DHCP is used, whenever a computer logs onto the network, it automatically gets an IP address assigned to it.
Dial-up	A communication connection via the standard telephone network, or POTS.
DNS	Domain Name Service 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. Various technology protocols for high-speed data, voice and video transmission over ordinary twisted-pair copper POTS telephone wires.

Term	Definition
Encryption Key	An alphanumeric (letters and/or numbers) series that enables data to be encrypted and then decrypted so that 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.
HPORT	Physical port/interface to the WirelessHART MUX.
HMS	Management software that interfaces to the WirelessHART MUX.
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 four computers; a large hub can connect 48 or more computers.
Hz	Hertz. The international unit for measuring frequency, equivalent to the older unit of cycles per second. One megahertz (MHz) is one million hertz. One gigahertz (GHz) is one billion hertz. The standard US electrical power frequency is 60 Hz, the AM broadcast radio frequency band is 535—1605 kHz, the FM broadcast radio frequency band is 88—108 MHz, and wireless 802.11b/g LANs operate at 2.4 GHz.
IEEE	Institute of Electrical and Electronics Engineers, New York, www.ieee.org. A membership organization that includes engineers, scientists and students in electronics and allied fields. It has more than 300,000 members and is involved with setting standards for computers and communications.
Infrastructure Mode	An 802.11 setting providing connectivity to an access point (AP). In contrast to Ad-Hoc mode, where 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 intended primarily for Internet access which is simple to set up and usually does not support installation of third-party software. These computers generally offer customized web browsing, touch-screen navigation, e-mail services, entertainment and personal information management applications.
IP	Internet protocol. A set of rules used to send and receive messages across local networks and the Internet.
IP Telephony	Technology that supports voice, data and video transmission via IP-based LANs, WANs, and the Internet. This includes VoIP (Voice over IP).
IP Address	A 32-bit number that identifies each sender or receiver of information that is sent across the Internet. An IP address has two parts: an identifier of a particular network on the Internet and an identifier of the particular device (which can be a server or a workstation) within that network.
IPX-SPX	Internetwork Packet Exchange, a networking protocol used by the Novell® NetWare® operating systems. Like UDP/IP, IPX is a datagram protocol used for connectionless communications. Higher-level protocols, such as SPX and NCP, are used for additional error recovery services. Sequenced Packet Exchange, SPX, a transport layer protocol (layer 4 of the OSI Model) used in Novell Netware networks. The SPX layer sits on top of the IPX layer (layer 3) and provides connection-oriented services between two nodes on the network. SPX is used primarily by client/server applications.
ISDN	A type of broadband Internet connection that provides digital service from the customer's premises to the dial-up telephone network. ISDN uses standard POTS copper wiring to deliver voice, data or video.

Term	Definition
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, and Application.
LAN	Local Area Network. A system of connecting PCs and other devices within the same physical proximity for sharing resources such as an Internet connections, printers, files and drives.
Receive Sensitivity	The minimum signal strength required to pick up a signal. Higher bandwidth connections usually have less receive sensitivity than lower bandwidth connections.
Router	A device that forwards data from one WLAN or wired local area network to another.
SNR	Signal to Noise Ratio. The number of decibels difference between the signal strength and background noise.
Transmit Power	The power (usually expressed in mW or dBm) at which the wireless device transmits.
MAC Address	Media Access Control address. A unique code assigned to most forms of networking hardware. The address is permanently assigned to the hardware. Limiting a wireless network's access to hardware, such as wireless cards, is a security feature employed by closed wireless networks. However, an experienced hacker armed with the proper tools can still figure out an authorized MAC address, masquerade as a legitimate address, and access a closed network. Every wireless 802.11 device has its own specific MAC address hard-coded into it. This unique identifier can be used to provide security for wireless networks. When a network uses a MAC table, only 802.11 radios that have had their MAC addresses added to that network's MAC table will be able to get onto the network.
NAT	Network Address Translation. A network capability that enables a number of computers to dynamically share a single incoming IP address from a dial-up, cable or xDSL connection. NAT takes the single incoming IP address and creates new IP address for each client computer on the network.
NAN	Not a Number is a numerical data type value that represents an undefined or unpresentable floating-point number.
NIC	Network Interface Card 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 10Mbps (Ethernet), 100 Mbps (Fast Ethernet) or 10/100 Mbps dual speed. High-speed Gigabit and 10 Gigabit NIC cards are also available.
Proxy Server	Used in larger companies and organizations to improve network operations and security, a proxy server is able to prevent direct communication between two or more networks. The proxy server forwards allowable data requests to remote servers and/or responds to data requests directly from stored remote server data.
RJ-45	Standard connectors used in Ethernet networks. RJ-45 connectors are similar to standard RJ-11 telephone connectors, except that RJ-45 connectors can have up to eight wires, whereas telephone connectors have four wires.
Server	A computer that provides its resources to other computers and devices on a network. These include print servers, Internet servers and data servers. A server can also be combined with a hub or router.
Site Survey	The process whereby a wireless network installer inspects a location prior to installing a wireless network. Site surveys are used to identify the radio- and client-use properties of a facility so that access points can be optimally placed.
SSL	Secure Sockets Layer. A commonly used encryption scheme used by many online retail and banking sites to protect the financial integrity of transactions. When an SSL session begins, the server sends its public key to the browser. The browser then sends a randomly generated secret key back to the server in order to have a secret key exchange for that session.
Sub Network or Subnet	Found in larger networks, these smaller networks are used to simplify addressing between numerous computers. Subnets connect together through a router.

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

Notes:

Customer Assistance

Technical Support:

United States:+1 866 713 4409
Australasia.: +61 7 3352 8624
Other: +1 604 944 9247

Email: ELPRO-Support@cooperindustries.com
Website: www.cooperbussmann.com/wireless
Australasia Fax: +61 7 33528677
US Fax: +1 925 924 8502

Online Resources

Visit www.cooperbussmann.com/wirelessresources for the following resources and more:

- User Manuals
- Installation Guides
- Configuration Software
- Datasheets
- Dimensional Drawings

North America & Latin America

5735 W. Las Positas Suite 100
Pleasanton, California 94588 USA
Telephone: +1 925 924 8500
elpro-sales@cooperindustries.com

Australia, New Zealand

Cooper Technology Centre
Suite 2.01, Quad 2, 8 Parkview Drive
Sydney Olympic Park, NSW, 2127, AUSTRALIA
Telephone: +61 2 8787 2777
elpro-sales@cooperindustries.com

China

955 Shengli Road
East Area of Zhangjiang High-Tech Park
Shanghai, 201201, CHINA
Telephone: +86 21 2899 3600
elpro-sales@cooperindustries.com

Southeast Asia

2 Serangoon North Avenue 5
06-01 Fu Yu Building, 554911, SINGAPORE
Telephone: +65 6645 9888
elpro-sales@cooperindustries.com

©2013 Cooper Bussmann
www.cooperbussmann.com/wireless

Your Authorized Cooper Bussmann Distributor is:

ELPRO Technologies

The trade names and brand names contained herein are valuable trademarks of Cooper Industries in the U.S. and other countries. You are not permitted to use the Cooper Trademarks without the prior written consent of Cooper Industries.

COOPER Bussmann