Development and Integration of Honeywell's One-Wireless Network

ENG470 - Engineering Honours Thesis – Report
Murdoch University Semester 2, 2018

Author:

Nicholas Lane

Academic Supervisor

Associate Professor Graeme Cole

Industrial Supervisor

Benjamin Dias

A thesis report submitted to the School of Engineering and Information Technology in partial fulfilment for the requirements of Bachelor of Engineering Honours in the discipline of:

Industrial Computer Systems Engineering

Instrumentation and Control Engineering

AUTHORS DECLARATION

I declare that I am the sole author of this Honours Thesis Report. To the best of my knowledge the work contained is my own except where acknowledgment has been made. This work contains no material that has been submitted as part of the requirements for any other academic or non-academic program, this document consists of 12297 words.

X

Nicholas Ross Lane

ABSTRACT

The purpose of this project has been to develop upon the Honeywell One-Wireless network in the Murdoch University Pilot Plant and integrate it into the Distributed Control System. This will give future students exposure to developing process control schemes around industrial wireless technology in a small plant setting. Industrial Wireless is still on the cutting edge of technology and it will challenge the status quo in Industry with its many advantages. A brief review of Industrial wireless technology has been included in this thesis report to provide the reader a background to the communications technology. Also included is Honeywell's One-Wireless Network solution which was used in this project. There, where significant challenges in getting the network operational, and as a result a systematic troubleshooting process was followed. Once the network was operational additional wireless instruments where added to expand the network and set up in the system. From here the One-Wireless network was integrated into the Distributive Control System which operates the pilot plant, this was done using Modbus TCP/IP. To determine the effectiveness of the network a post Radio Frequency assessment was carried out to determine the impact of the network and ensure that it was following best practices. Relevant documentation on the network was developed as a handover for future students to build upon the work carried out.

ACKNOWLEDGMENTS

I would like to thank the following people for providing me with their technical expertise and mentorship over the duration of this project, without their help this project would not have been possible.

Associate Professor Graeme Cole

Academic Supervisor, Murdoch University

Benjamin Dias

Industrial Supervisor, Honeywell

Will Stirling

Technical Officer, Murdoch University

Jarren Beveridge

Technical Officer, Murdoch University

Scott Spurway

Senior Systems Engineer, Motherwell Automation

TABLE OF CONTENTS

Authors Declaration 2

Abstract 3

Acknowledgments 4

Table of Figures 7

Table of Tables 9

List of Abbreviations 10

1 Introduction 13

2 Project Overview 15

2.1 Project Aim 15
2.2 Project Objectives 15
2.3 Project Background 16
3 Industrial Wireless Technology 18

3.1 Network Architecture 18
3.1.1 Application Layer 19
3.1.2 Transport Layer 20
3.1.3 Network Layer 21
3.1.4 Data Link Layer 22
3.1.5 Physical Layer 23
3.2 ISA100 27
3.3 WirelessHART 29
3.4 Industrial Wireless Applications 31
3.4.1 Environmental Monitoring 31
3.4.2 Condition Monitoring 32
3.4.3 Process Control 33
4 Honeywell’s One-Wireless Network 35

4.1 One-Wireless Network Security 35
4.2 Wireless Device Manager 36

4.3 Managed Network Switch 37
4.4 WLAN Controller 38
4.5 Access Point 38
5 Project Results 40
5.1 Current Network State 40
5.1.1 Network Layer 1/2 Troubleshooting 40
5.1.2 Network Layer 3 Troubleshooting 41
5.1.3 Troubleshooting Reflection 43
5.2 DCS Integration 45
5.2.1 Modbus TCP/IP 45
5.2.2 Modbus Server Configuration 47
5.3 RF Assessment 51
5.3.1 System Requirements 52
5.3.2 Bandwidth and Interference 53
6 Project Reflection 56
6.1 Future Works 58
6.1.1 Pilot Plant Expansion 58
7 Conclusion 59
8 Bibliography 60
9 Appendix 64
9.1 Network Troubleshooting Procedure 64
9.2 Layer 1/2 Diagram 67
9.3 Layer 3 Diagram 68
9.4 IP Address Table 69
9.5 Network Switch Configuration 70
9.6 Password Vault 72
9.7 Accessing the WLAN Controller GUI 73
9.8 Accessing the Wireless Device Manager GUI 75

TABLE OF FIGURES

Figure 1: Pilot Plant Network [5] 17

Figure 2: ARP Routing Table 21

Figure 3: CSMA/CA Diagram [18] 23

Figure 4: Honeywell R300 Instrument (Wireless Station) [20] 24

Figure 5: Cisco Aironet (Access Point) [21] 24

Figure 6: Cisco Network switch [22] 24

Figure 7: Honeywell Wireless Device Manager [23] 24

Figure 8: ODFM Spectrum 26

Figure 9: Inter-symbol Interference 26

Figure 10: Self-Healing ISA100 Mesh Network [21] 28

Figure 11: Wireless Gas Detector for Hazardous Areas 31

Figure 12: Wireless Vibration Sensor for Bearing Damage Detection [33] 33

Figure 13: Fisher 4320 Wireless Valve Positioner [34] 34

Figure 14: One-Wireless Network Components [21], [35] , [22], and [19] 35

Figure 15: WDM Graphical User Interface of Murdoch Pilot Plant 37

Figure 16: Cisco Aeronet 1552S Access Point [21] 39

Figure 17: Previous Network State 40

Figure 18: Layer 3 One-Wireless Network Diagram 42

Figure 19: Modbus Communication to DCS [41] [19] 45

Figure 20: CSTR Bank Wireless Network HMI 48

Figure 21: Wireless Network Diagnostics HMI 49

Figure 22: Modbus Communication to Computer [41] 50

Figure 23: RF Assessment of Pilot Plant 54

Figure 24: Access Point Performance Summary 55

Figure 25: Device Manager Ports in Use 64

Figure 26: PuTTY Terminal Configuration 64

TABLE OF TABLES

Table 1: Comparison between Wired and Wireless Networks [4]..14

Table 2: Open System Identification Model 19

Table 3: ISA100 Wireless OSI Model 27

Table 4: WirelessHART OSI Model 29

Table 5: Summary of WirelessHART Network Forming Procedure [32] 30

Table 6: Summary of Troubleshooting Procedure 44

Table 7: Modbus Function Codes [42] 46

Table 8: Modbus Data Tables [41] 47

Table 9: Modbus Packet Structure [42] 47

Table 10: Modbus TCP/IP Packet Structure [42]...47

Table 11: RF Assessment Requirements [43]...51

Table 12: Connecting Quality Assessment [37] 53

Table 13: Network Troubleshooting Procedure 66

LIST OF ABBREVIATIONS

Abbreviation	Acronym
ACI	Adjacent Carrier Interference
ACMA	Australian Communications and Media Authority
AP	Access Point
ARP	Address Resolution Protocol
CCTV	Closed-Circuit Television
CLI	Command Line Interface
CP	Cyclic Prefix
CSMA/CA	Carrier Sense Multiple Access Collision Avoidance
CSTR	Continually Stirred Tank Reactor
CYC	Cyclic Redundancy Check
DCS	Distributive Control System
DHCP	Dynamic Host Configuration Protocol
DIFS	Distributed Inter-Frame Spacing
EIRP	Equivalent Isotropic Radiated Power
FCS	Frame Check Sequence
FDN	Field Device Network
GUI	Graphic User Interface
HART	Highway Addressable Remote Transducer
HMI	Human Machine Interface
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol

ISA	International Society of Automation
ISI	Inter-symbol Interference
ISM	Industrial, Scientific, and Medical
ISO	International Standards Organisation
ITU	International Telecommunications Union
LAN	Local Area Network
LLC	Logical Link Layer
MAC	Media Access Control
NIC	Network Interface Card
OFDM	Orthogonal Frequency Division Modulation
OPC	OLE for Process Control
OSI	Open System Identification
PCN	Process Control Network
PDA	Personal Digital Assistant
PKS	Process Knowledge System
PLC	Programmable Logic Controller
RAM	Random Access Memory
RF	Radio Frequency
RSQI	Received Signal Quality Indication
RSSI	Received Signal Strength Indication
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network
VSD	Variable Speed Drive
WDM	Wireless Device Manager

WLAN	Wireless Local Area Network

1 INTRODUCTION

Industrial wireless technology allows for Industrial Computer Systems to collect data from processes wirelessly without the need for a physical wired connection to the network. A healthy scepticism has been applied to the adoption of wireless instrument technologies; this is due to factors concerning availability, and reliability [1]. These factors are influenced significantly when the wireless instrument is operating in a process plant where large metallic machinery and structures can obstruct the signal [2]. A direct consequence of adopting this new technology can negatively affect product quality, cause environmental damage, or put people in danger [3]. For these reasons, there has been a slow adoption of this new technology in industry. The idea of wireless sensor networks being unreliable has been reflected in industry trends where there has been a resistance to change with new communication technologies when what is currently implemented works [2]. Additionally, wireless sensor networks are deemed to be non-reliable when compared to wired networks [2]. However, wireless sensor networks are on the cutting edge of technology and moving forward we will begin to see the resource sector and manufacturing industry moving towards wireless sensor technology to reduce installation costs, reduce maintenance, and improve network scalability [3] as can be seen in Table 1 . This thesis outlines the aim, objectives and methodology of the developing a wireless sensor network within the Murdoch University Pilot Plant and the testing of its reliability.

Table 1: Comparison between Wired and Wireless Networks [4]

	Characteristic	Wired Networks	Wireless Networks
1	Installation	Difficult depending on network.	Easy to install due to no cables.
2	Cost	Less, cost of cables is low.	More, due to access points.
3	Reliability	High, because manufactures have been continuously improving.	Reasonably high, if network is designed correctly.
4	Mobility	Low, devices need to be linked to the wired network.	High, operators can connect wirelessly.
5	Security	High, the cables are localized to the plant equipment.	Low, because the data can be intercepted and compromised.
6	Interference	Low, using cable shielding and appropriate cable routing.	High, due to other wireless signals in the vicinity.
7	Speed	High, due to high speed ethernet connections.	Low, depending on what standard has been used.

2 PROJECT OVERVIEW

2.1 PROJECT AIM

This project aims to build upon the work of Hussaini (2018) by developing a wireless network for Honeywell's One-wireless R300 series instruments in the Murdoch Engineering Pilot Plant. First the current state of the one-wireless network needs to be established, if any network problems are identified they need to be rectified before the calibration, installation and commissioning of the sensors can take place. Once the sensors have been commissioned into the network the system will be integrated into the Honeywell Distributed Control System (DCS) which operates on Experion PKS software. In addition to this scope, a detailed handover document will be developed to allow expandability of the project in the future. The idea behind the project is to give future students the exposure to Industrial Wireless Networks and experience in developing control schemes around them as they offer their own unique advantages and limitations.

2.2 PROJECT OBJECTIVES

This project has been broken down into a total of five objectives which need to be completed over the duration of the project.

1. Conduct in-depth research into Wireless Instrumentation Technology, this includes different types of protocols and their associated standards. The purpose of this is to create a datum of the project as a reference point.
2. Develop the following documentation as a guide for this project:
    a. Commissioning Plan
    b. Wireless Device Manager Setup
    c. Ethernet Switch Setup

   d. Radio Background Assessment

3. Troubleshoot the current state of the Wireless Network and identify any potential problems.
4. Set up wireless Modbus communications from the instruments to the Experion1 Server and then proceed to configuration in the Pilot Plant Server.
5. Develop handover documentation and tutorials so that the work can be replicated by future students when added to the curriculum (found in appendix).

2.3 PROJECT BACKGROUND

This thesis project is an extension on the work completed by Hussani (2018), where the project aimed to design, commission and test the Honeywell One-Wireless system in the Murdoch University Pilot Plant [5]. The project involved designing a network architecture based on the requirements of the Pilot Plant system as shown in Figure 1, configuring key hardware components including the network switch, LAN controller, wireless device monitor and wireless access point [5]. The wireless instruments were then configured into the wireless device monitor as part of the commissioning procedure developed in conjunction with Honeywell. This project expands upon this work by reviewing the current state of the system, including the addition of four more sensors. The sensors will then need to be calibrated to their corresponding process variable being measured which is done through the Wireless Device Monitor. Once the instruments have been calibrated, they will be commissioned into the Pilot Plant server

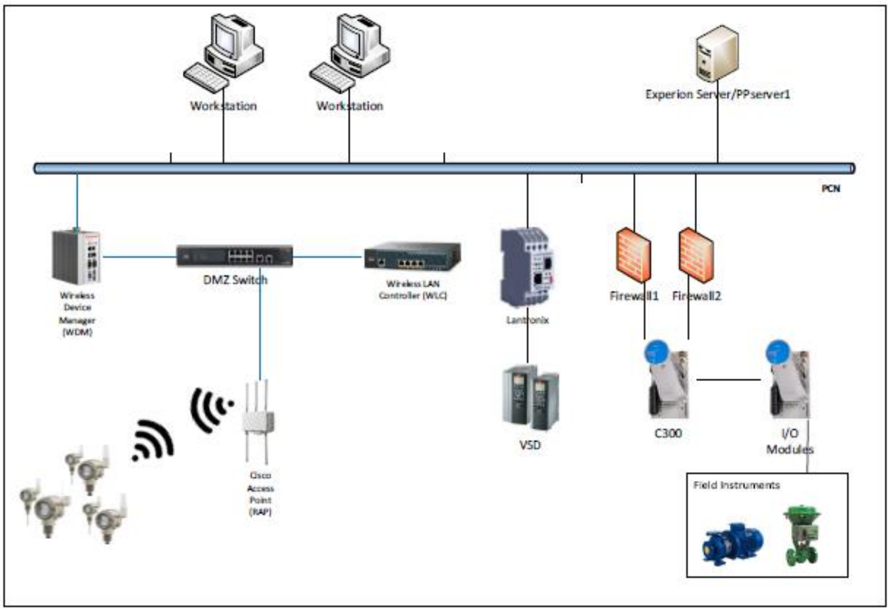


Figure 1: Pilot Plant Network [5]

To reflect the changes made in the Pilot Plant the DCS HMI screens have been modified giving the operator the option to use either the wired or wireless instruments to measure the process variable. It was determined that an RF assessment not be required due to the Pilot Plant not having any major interferences. However, as part of this project one will be completed to obtain a baseline for comparison when the project was completed.

3 INDUSTRIAL WIRELESS TECHNOLOGY

3.1 NETWORK ARCHITECTURE

Industrial wireless technology would not be possible without the logical and physical architecture of wireless communications. These architectures allow the wireless network to operate over a physical medium to interconnect devices with compatible logical architectures. The physical and logical architectures are dependent on each other and wouldn’t be possible without a framework defining their structure. The Open System Interconnection (OSI) Model is a networking framework for the interconnection of devices and is referred to as the logical architecture of networks. It was developed in 1983 by the International Standards Organization (ISO) [6]. The development of the OSI model was initiated when devices could not communicate effectively over a network because they were from different manufacturers [7]. With the OSI model being the framework of communications over a network, protocol standards have been developed at each layer to allow all devices to communicate effectively [7]. The OSI model consists of seven layers: Application, Presentation, Session, Transport, Network, Data-Link, and Physical (Table 2). Each of these layers perform a designated function in accordance with the ISO standard [8]. The key advantages of the OSI model are: industry standardisation, improved network troubleshooting, and it allows devices from differing manufacturers to communicate over a network [9].

Table 2: Open System Identification Model

Layer	Data	Description
Application	Data	Network Process to application
Presentation	Data	Data encryption
Session	Data	Interhost communication
Transport	Segments	End to end connection and reliability
Network	Packets	Logical addressing and route determinisation
Data Link	Frames	Physical addressing
Physical	Bits	Signal propagation

When communication is first initiated the message is constructed into a packet at the application layer, which will then pass through each layer of the OSI model where each layer performs its specified function. Once the packet reaches the physical layer, it is transmitted across the physical medium to the receiving device, which decodes the signal into a bit stream and reads the address attached to the packet. If the address matches the receiving device the packet travels up its OSI model where the packet is reconstructed at each level. The OSI model is a powerful tool allowing the interconnection of devices across a network because of its framework. The following sections discuss the layers of the OSI model and associated protocols that are specific to Industrial Wireless Technology and the Honeywell One-Wireless Network.

3.1.1 Application Layer

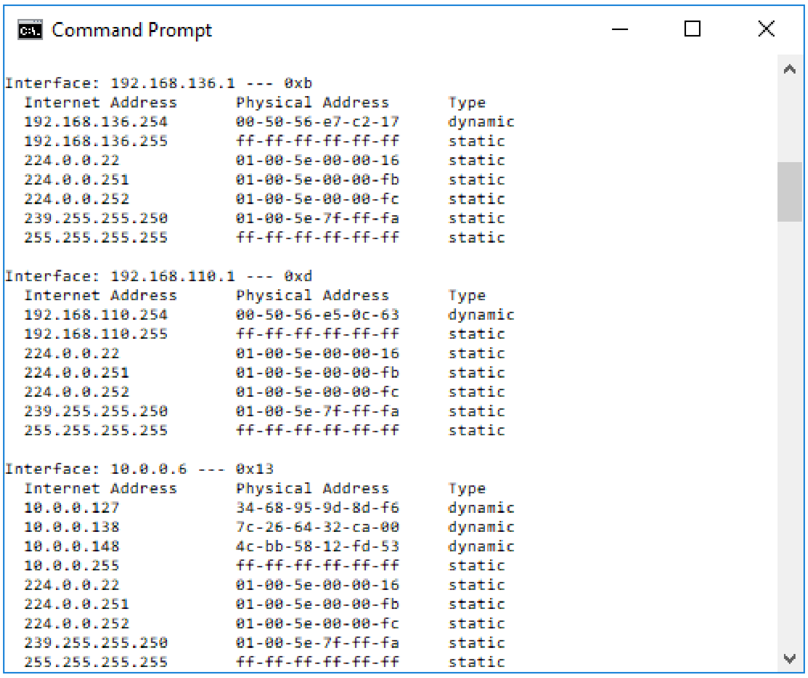
The application layer is the topmost layer of the OSI model. Its role is to provide applications access through authentication and control of the network on the TCP/IP stack [10]. An example of these applications includes email (Simple Mail Transfer Protocol, file transfer (File Transfer Protocol), and communication between devices (Modbus) [7]. Each application layer protocol is governed by a set of standards which specify how the data is prepared, methods of data exchange, addressing and packet sizes [10]. When communication on a network is instigated, the message is constructed at the application layer which will check the network for availability and device authentication before transferring the data to the following layer [8]. At the application layer, the most common protocols for industrial wireless networks are ISA100, WirelessHART, and Zigbee.

3.1.2 Transport Layer

The transport layer has been developed to allow multiple application layer protocols to access the network simultaneously using ports on the transport layer stack; this is referred to as multiplexing [11]. A computer port is an interface that provides an application access to the computer network [10]. There are two types of transport layer protocols: connection orientated and connectionless [10]. Connection-orientated protocols function by creating a connection between two devices on a network; this is established using a three-way handshake before data is transmitted [11]. Connection-orientated protocols are considered more reliable because they include error checking mechanisms that ensure that data arrives in the correct order and all the packets are received [11]. If an acknowledge isn't received for a sent packet within a timeframe the packet is sent again. Connectionless protocols send single messages in any order which is not considered reliable. One of the reasons that connectionless protocols are not considered reliable is because they do not utilise an acknowledgement packet when a packet is received, this means corrupted data is not retransmitted [12]. The Transport layer is also responsible for congestion control where the transmitting device will wait until there is an opening in the network before transmitting. The two most common Transport Layer protocols are: Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) [10].

3.1.3 Network Layer

The network layer is the third layer of the OSI model. Its role is to break down the application layer message into a series of packets which are assigned a destination address, and a route through the network [13]. Because there are limitations on the maximum packet size, data is broken down into multiple packets which are reassembled when they are received at the destination address [14]. Each device must have an address seen from the perspective from the application layer, this is referred to as a logical address. The logical address that is assigned to a device may change (dynamic address) or stay the same (static). These addresses are assigned using the Internet Protocol (IP) addressing system which consists of two addressing types IPV4 and IPV6 [8]. The routing of packets through a network is done by the Internet Protocol using the Address Resolution Protocol (ARP) which compares the packet IP address to a routing table stored in the device [8]. The routing table (Figure 2) contains the IP address, and the corresponding Media Access Control (MAC) address for each device it has communicated with. When a match is found in the table the packet route is determined, otherwise, the packet is sent to a default forwarding address [7].



```
Interface: 192.168.136.1 --- 0xb
  Internet Address      Physical Address      Type
  192.168.136.254       00-50-56-e7-c2-17     dynamic
  192.168.136.255       ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 192.168.110.1 --- 0xd
  Internet Address      Physical Address      Type
  192.168.110.254       00-50-56-e5-0c-63     dynamic
  192.168.110.255       ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 10.0.0.6 --- 0x13
  Internet Address      Physical Address      Type
  10.0.0.127            34-68-95-9d-8d-f6     dynamic
  10.0.0.138            7c-26-64-32-ca-00     dynamic
  10.0.0.148            4c-bb-58-12-fd-53     dynamic
  10.0.0.255            ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

Figure 2: ARP Routing Table

3.1.4 Data Link Layer

The Data-link layer is found between the network and physical layer. It consists of two sub-layers: Logical Link Control (LLC) and Media Access Control (MAC). The main purpose of the data-link layer is to prepare data for transmission when it reaches the physical layer and to format incoming packets for the network layer.

3.1.4.1 Logical Link Control Sub-Layer

The logical link control layer (LLC) prepares the data for transmission by acting as an interface between the physical and network layers. The main functions of the LLC sub-layer is Error Checking, Frame Synchronization, and Flow control [15]. Error checking is done at the data-link layer to ensure the integrity of the packet by computing a cyclic redundancy check (CYC) which works by performing a binary division of the packet; the remainder is added to the packet in the CYC field [16]. When the receiving device receives the data, it performs the same binary division, and if the remainder is zero the packet is accepted and passed to the network layer, otherwise it is deemed corrupted and dropped [8]. In addition to this, the acknowledgments received are tracked to determine if there was an error in transmission, if this is the case the LLC will specify for the packet to be retransmitted. Frame synchronisation is used to ensure that the receiving device can properly decode incoming signals [16]. Flow control at the LLC sub-layer ensures that devices do not overwhelm each other by transmitting at a faster rate than the receiving device, this is managed by using two techniques: stop - wait, and sliding window [17].

3.1.4.2 Media Access Control Sub-Layer

The MAC sub-layer is responsible for the packet encapsulation, physical addressing, and device access to the physical layer [7]. The packet encapsulation feature addresses the packet with a header and a trailer. The header consists of the physical address of the receiving device; this is referred to as the MAC address which is assigned by the manufacturer during the manufacturing process (48 bits long) [8]. The trailer consists of a Frame Check Sequence (FCS) (8 bytes) and a stop frame to notify the network that the transmission has ended. The MAC sub-layer is also used to control a device's access to the physical layer; this is used to ensure that two devices don't transmit across and cause a packet collision which result in loss of bandwidth [8]. In wireless networks, collision detection and avoidance is more difficult because the radio transmitter is unable to both transmit outgoing packets and listen for other devices transmitting simultaneously. To overcome this, a mechanism called Carrier Sense Multiple Access Collision Avoidance (CSMA/CA) is utilised. The CSMA/CA protocol works by waiting for the network medium to be free of transmissions and then it waits a predetermined amount of time called the Distributed Inter-Frame Spacing (DIFS) and then a random amount of time which is referred to as back-off time, and if the network is still free, it will transmit its data [8].

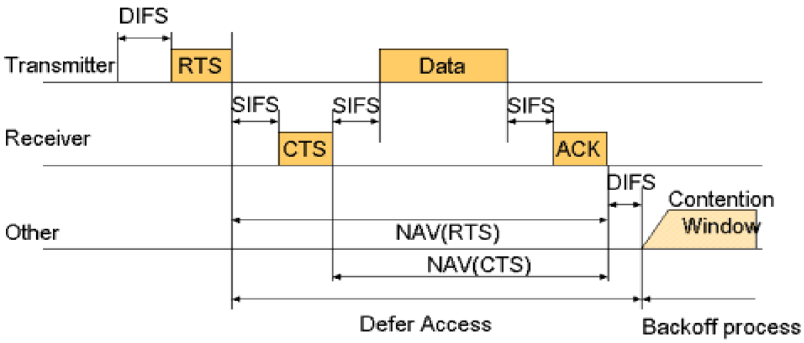


Figure 3: CSMA/CA Diagram [18]

3.1.5 Physical Layer

The physical layer is at the bottom layer of the OSI model where all the other layers are built on; it is responsible for converting a digital packet into a physical signal which is transmitted across the network [10]. For Wireless Local Area Networks (WLAN) this consists of three hardware components: stations, access point and a distribution system, the Honeywell One-Wireless system also uses a Wireless Device Monitor (WDM) [19]. A Station is any wireless device that has access to a network; this is achieved through the use of a wireless Network Interface Card (NIC). Stations can communicate to each other through peer to peer networks or access points in the network (Figure 4) [8]. The Access Point (AP) provides configurable authentication, security and access control features in addition to supporting wireless local area network (WLAN) communications. The AP is usually connected to another network which provides access to and from the wireless devices (Figure 5) [8]. A network switch acts as a distribution system between networks and provides network management features. Its main role is to facilitate centralised control and configuration of the network distribution system from a single location (Figure 6) [10]. The WDM is used to manage wireless sensors that are communicating to the AP; it can be used to integrate wireless devices in the field into a Distributed Control System (DCS) such as Honeywell's Experion PKS DCS system (Figure 7) [19].

Figure 4: Honeywell R300 Instrument (Wireless Station) [20]

Figure 5: Cisco Aironet (Access Point) [21]

Figure 6: Cisco Network switch [22]

Figure 7: Honeywell Wireless Device Manager [23]

3.1.5.1 Signal Propagation

Radio forms part of the electromagnetic spectrum where oscillations occur between 9kHz and 300GHz [8]. Each section of the radio spectrum is allocated to a specific purpose by the Australian

Radiofrequency Spectrum Plan (ARSP) by the Australian Communications and Media Authority (ACMA) to manage the spectrum usage in Australia and meet international obligations as per the International Telecommunications Union (ITU). Wireless communications for Wi-Fi occur in the 2.4GHz and 5.8GHz range as per the IEEE 802.11 standard and is classified as secondary service under the ARSP [24]. The AMCA also specifies the maximum radiated power for antennas in a specific direction for each frequency band; this is measured in Equivalent Isotropic Radiated Power (EIRP) [24]. EIRP uses the antenna as a reference point where a signal is transmitted in all directions, in addition to this the signal will be concentrated into a direction if the antenna has an antenna gain [25]. The EIRP is calculated by the sum of power output from the transmitter and antenna gain and subtracting any losses. ACMA specifies that for Wi-Fi communications the maximum EIRP can't exceed 200mW for 2.4GHz networks or 4000mW in 5.8GHz networks, this is to ensure minimal interference on the other bands and community safety [24].

3.1.5.2 Signal Modulation

One of the main issues with transmission of radio signals is the interference between networks operating on the same frequency and area, this can result in transmission errors and as a result, can reduce the networks reliability [8]. This problem is overcome in IEEE 802.11 by using a signal modulation technique called Orthogonal Division Frequency Modulation (ODFM) [8]. ODFM operates by dividing a frequency band into several sub-carrier frequencies. These sub-carriers operate orthogonal to each other where the minima of the signals overlap with adjacent sub-carriers in the time domain (Figure 8) [8]. This spacing has been selected to minimise the Adjacent Carrier Interference (ACI) between broadcasts and as a result, makes more efficient use of the frequency band. Inter-symbol Interference (ISI) occurs at the minima of the sub-carrier where it overlaps with the adjacent sub-carrier (Figure 9) [26], this is reduced in ODFM systems by inserting a Cyclic Prefix

(CP) before the transmission of the adjacent subcarrier can begin [27]. Once the sub-carriers have been set up the data packet is encoded into parallel bit streams to be encoded across the network.

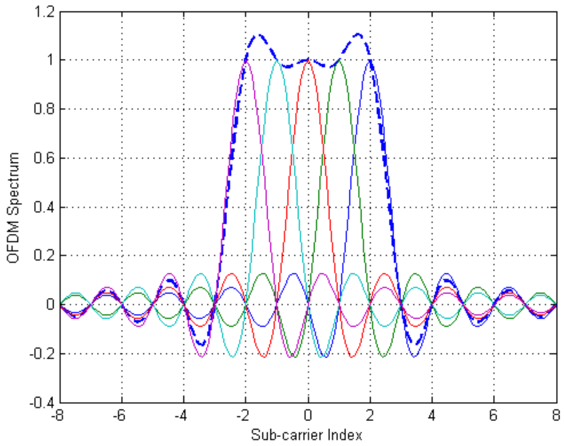


Figure 8: ODFM Spectrum

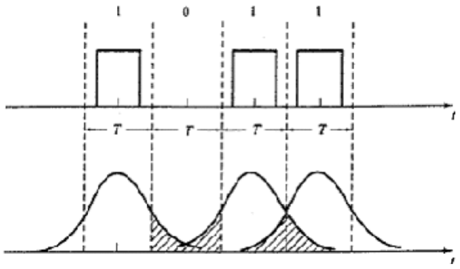


Figure 9: Inter-symbol Interference

3.2 ISA100

The ISA100 Wireless standard was developed to meet the need for an Industrial Wireless Protocol it needed to be reliable, be secure from cyber threats and accommodate other application layer protocols [28]. ISA100 was built on the Internet Protocol Suite using IPV6 addressing and Internet Protocol Security (IPSec). The IPV6 addressing removes any addressing constraints and allows networks to be segmented into different management groups [29]. The IPSec functionality is used to encrypt traffic at the network layer to prevent application layer data becoming available to unauthenticated devices on the network [29]. Because ISA100 was built on the Internet Protocol Suite it is compatible with most network infrastructures and allows other proprietary protocols to run at its application layer and as a result supports legacy applications (Table 3) [28]. An example of this is a company called Gas Secure that has developed a protocol that operates on the ISA100 application layer called PROFIsafe, for Safety Integrity Level (SIL) related functions [30].

Table 3: ISA100 Wireless OSI Model

Layer	Description
Application	ISA100 Wireless Native Protocol
Presentation	
Session	AES 128 Bit encryption Device Provisioning
Transport	User Datagram Protocol
Network	IPv6 Addressing IPv6 Routing
Data Link	Mesh / Star / Hybrid Network Configuration
Physical	IEEE 802.15.4 (2.4GHz ISM band)

An ISA100 network will consist of: field instruments (i) which act as inputs/outputs, router (ii) used as part of the mesh network topology system manager (iii) to establish mesh pathways (Figure 10), security manager (iv) which creates secure lines of communication, and a gateway device (v) used to interconnect the ISA100 devices to another network [31]. Some hardware can fulfil multiple functions such as the field instruments which are capable of routing and forming the mesh network topology. The ISA100 standard explicitly states that there is a maximum delay between data transmission of 100ms this is referred as latency, and literature goes on to suggest that we can expect to see four transmissions per second [28]. This means that ISA100 Wireless is well suited to control applications where a faster sample rate is desired [29]. ISA100 supports self-healing mesh network topologies which allow devices to be configured as routers, this allows for information to pass through an alternative path by relaying their information between devices configured for routing, this provides the network with greater redundancy. Because the network uses the Internet Protocol and the security mechanisms associated with it in conjunction with self-healing mesh network topologies ISA100 can be considered a future proof technology moving forward.

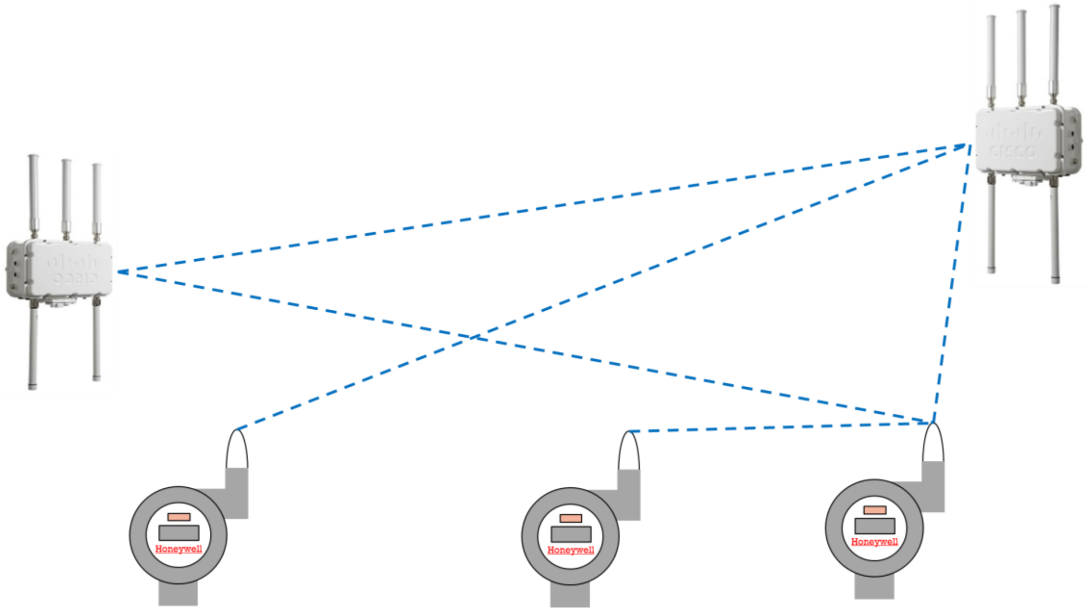


Figure 10: Self-Healing ISA100 Mesh Network [21]

3.3 WirelessHART

The most common type of instrumentation communication standard implemented is the 4 to 20mA current loop for its ease of troubleshooting and long cable runs. As instrumentation technology advanced, smart instruments have become available which allow for calibration, diagnostics and additional measurements. Smart instruments have been integrated with the pre-existing current loop technology by modulating a digital signal over the 4 to 20 current loops using Frequency Key Shifting as the modulation technique which did not affect the mean value of the current [29]. By using the current loop as the physical layer Highway Addressable Remote Transducer (HART) communication became the standard for smart transmitters [29],. WirelessHARTs' OSI Model can be seen in Table 4.

Table 4: WirelessHART OSI Model

Layer	Description
Application	WirelessHART Native Protocol
Presentation	
Session	Command orientated communication
Transport	Segmented transmission of data
Network	Redundant Pathway Mesh Topology
Data Link	TDMA, and Channel Hopping
Physical	IEEE 802.11 (2.4GHz ISM band)

WirelessHART technology was developed from HART because of the need for wireless instruments in the Process Automation Industry [29]. The requirements of wireless technology in industry has different requirements from wireless technology in consumer applications. These requirements are focused around reliability, ease of installation, and minimal interference. WirelessHART uses the same Frequency Key Shifting modulation technique as HART; however, instead of the physical layer being a current loop WirelessHART was built on Bluetooth technology [29]. Bluetooth was selected due to the requirements of wireless instruments in the process automation industry which needs sensors to be reliable and have a low power consumption. A disadvantage of using Bluetooth is that there is a lower signal throughput [29].

Sensors Using a Wireless HART network consist of three components: the WirelessHART Field Device, WirelessHART Gateway, and a Network Manager. When a network is formed, it will have a Network ID which is unique and is managed by the network manager (Table 5). The network manager also manages the wireless keys used on the network that encrypt the traffic. Only when a device has the correct network ID and key will it be able to connect to the network manager through the WirelessHART gateway [19]. The WirelessHART Gateway is located in the proximity of the field devices so that it can both transmit and receive data reliability.

Table 5: Summary of WirelessHART Network Forming Procedure [32]

Step	Description
1	The Network ID and Network Key are transferred to the field device.
2	The field device looks for advertisement message from the network.
3	The field device receives the advertisement message and synchronizes.
4	The field device transmits a join request to the network manager.
5	The network manager will authorize the device to join the network.
6	The network manager will optimize the network pathways with the new sensor.

3.4 INDUSTRIAL WIRELESS APPLICATIONS

The best application of Industrial Wireless technology is in situations where a fast sample rate and high availability are not essential, such as in environmental monitoring, condition monitoring, and asset management. The advantages of using wireless over wired technology in these applications are: reduced installation costs and improved network scalability. Once Industrial Infrastructure is in place the costs associated with adding additional wireless instruments is small compared to running cables for a wired instrument. This is particularly true in Hazardous Areas where personnel could be put in potential risk for prolonged amounts of time whilst installing cabling, whereas with wireless the technicians will be turning the instrument on and connecting it to the process (Figure 11).

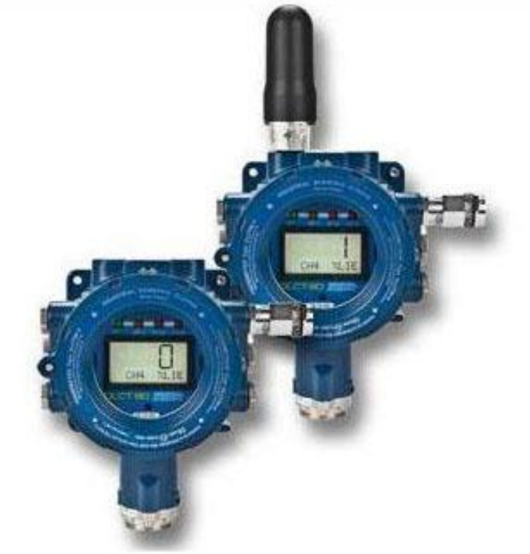


Figure 11: Wireless Gas Detector for Hazardous Areas

3.4.1 Environmental Monitoring

Environmental monitoring is used to assess the impact of industrial activity on the neighbouring environment. This can include the monitoring of: air quality, water quality, and soil quality. These measurements can be undertaken by technicians or alternatively measured using smart instruments using ISA100 or WirelessHART to relay the data to a network for analysis. The environmental monitoring network can poll the instruments with a large sample rate because changes in the environment occur over a large time span. Using the WirelessHART mesh network topology the instruments won't need to have direct access the WirelessHART access point, the instruments only need to be in range of a neighbouring instrument to forward the data back to the network. Once the network receives the data from the field devices it will be able to alert the plant operators to any environmental concerns.

3.4.2 Condition Monitoring

Condition monitoring is the process of monitoring equipment to identify a developing fault, it is typically used on critical equipment to prevent unscheduled downtime in manufacturing. When a developing fault is detected, preventative maintenance can be scheduled before the equipment sustains catastrophic damage. Condition monitoring measurements are performed by a service technician whom schedules condition monitoring measurements when the equipment is running, on large processing facilities and mine sites this can be a challenge. Using industrial wireless technology it is possible to take these measurements remotely across an industrial facility and transmit an alarm to the service technician when a fault is developing. Some examples of condition monitoring that this would be suitable for is abrasion detection in valves, corrosion detection in piping, bearing damage detection in pumps and motors (Figure 12). This application plays to the strength of wireless technology because as the network is scaled, the benefits of using a wireless network improve.

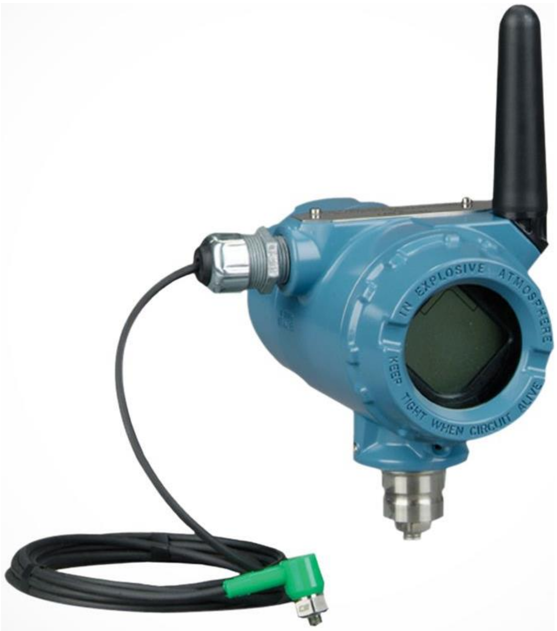


Figure 12: Wireless Vibration Sensor for Bearing Damage Detection [33]

3.4.3 Process Control

In process applications that do not require a fast sampling time wireless instruments can be installed to monitor process variables which may not have been possible previously due to their location, or availability of network coverage. Industrial wireless technology can be applied to both the measurement and control parts of a control loop by using wireless valve positioners (Figure 13) or pressure sensors, the advantage of using both would mean that the additional wireless instruments could be used to form part of the wireless mesh network topology further increasing their reliability. However, if the equipment management are not comfortable with a completely wireless solution then they can adopt a hybrid system consisting of both wired and wireless instruments in the control loop.

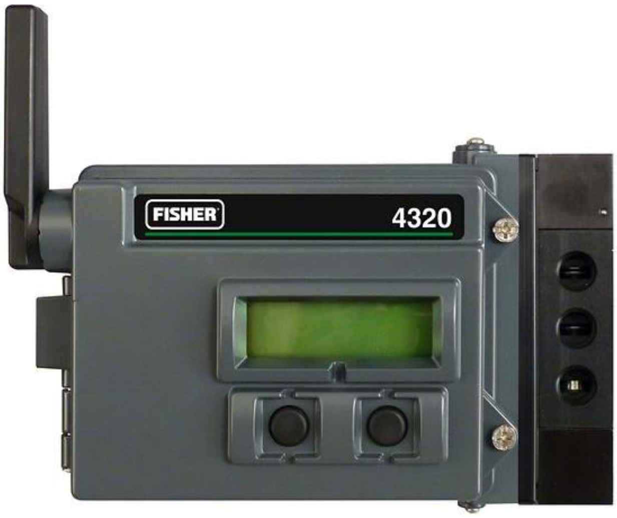


Figure 13: Fisher 4320 Wireless Valve Positioner [34]

4 HONEYWELL'S ONE-WIRELESS NETWORK

Honeywell's One-Wireless Network has been developed to meet the needs of their customers seeking a solution to industrial wireless networks using ISA100 or WirelessHART field instruments [35]. One of the key forces driving the adoption of wireless technology is accessibility of plant data that was not available with a wired topology. Some examples include equipment in remote locations, behind mechanical guards, and hazardous areas. By reducing the installation costs and by improving the scalability of a network Honeywell's Industrial Wireless exceeds the capabilities of legacy wired networks in some applications. The One-Wireless network consists of four main components: Cisco Aironet Access Point, Cisco WLAN Controller, Cisco Managed Network Switch, and the Honeywell Wireless Device Manager [35]. This hardware configuration can be scaled to support a larger network if required by adding in additional Aironet Access Points around a facility.

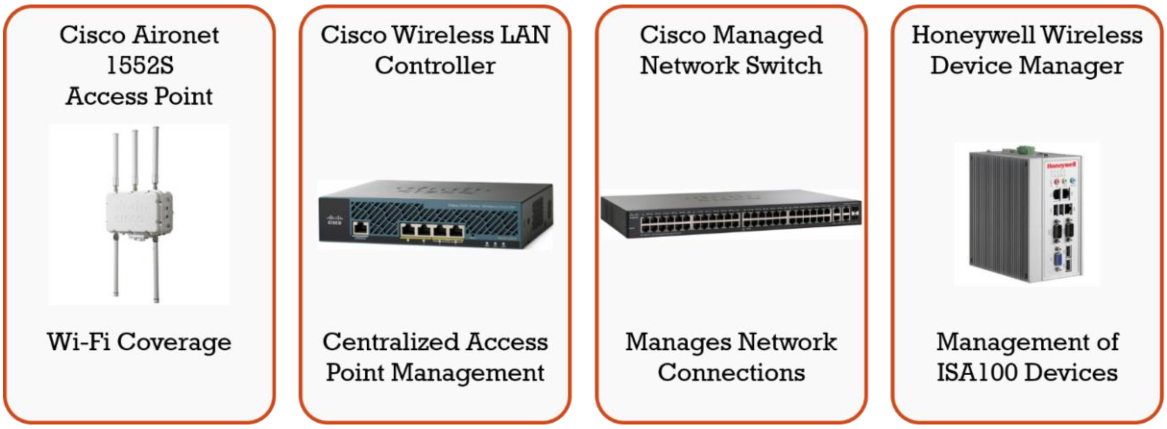

Cisco Aironet 1552S Access Point
Wi-Fi Coverage
Cisco Wireless LAN Controller
Centralized Access Point Management
Cisco Managed Network Switch
Manages Network Connections
Honeywell Wireless Device Manager
Management of ISA100 Devices

Figure 14: One-Wireless Network Components [21], [36] , [22], and [19]

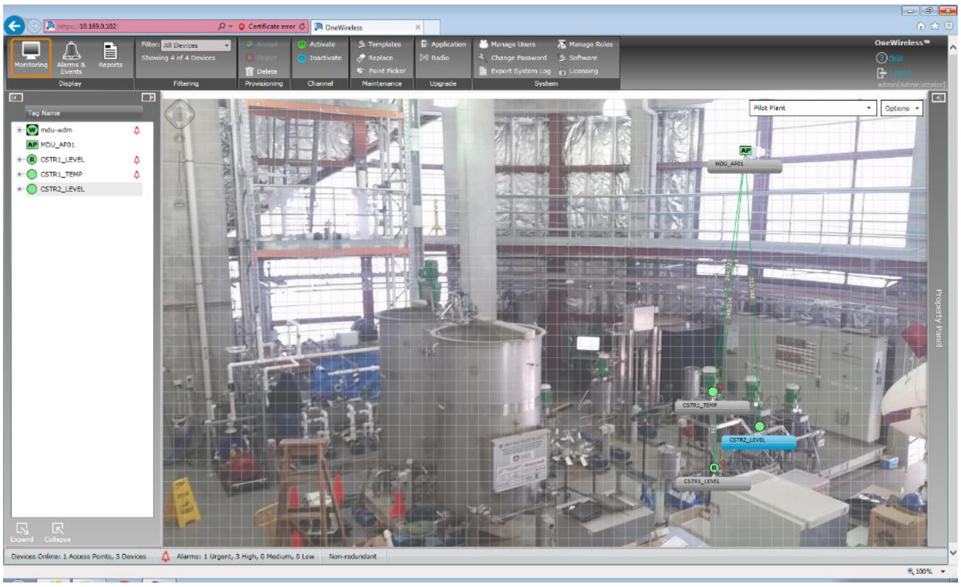
4.1 ONE-WIRELESS NETWORK SECURITY

Legacy wired networks have a strong physical security protecting the network through physical barriers such as fences, locked cabinets and structures. Wireless devices have a low physical security because wireless signals can be intercepted outside the facility, for this reason Industrial Wireless Networks use a high level of Logical Security. This is done in by the Honeywell One Wireless network using the following mechanisms:

- Embedded firewall: located in the WDM which monitors incoming and outgoing traffic between the Field Device Network (FDN) and the Process Control Network (PCN) [35].
- End-to-end encryption: used to protect data transmissions between the wireless instruments in the field and the Access Point [35].
- Device authentication: each device can be authenticated though a short-range infrared authentication method which prevents unauthorised access to the network [35].
- Key rotation policy: the wireless instruments are given a key to communicate on the encrypted network which is set up to periodically change [35].

4.2 Wireless Device Manager

The Wireless Device Manager (WDM) is the centralised part of the One-Wireless network, it is responsible for the management of ISA100 devices and WirelessHART devices [35]. The WDM can be managed by accessing its Graphical User Interface (GUI) through internet explorer by entering its IP address into the address bar [19]. The GUI provides the operator a graphical layout of the network and the communication paths between the wireless instruments and Access Point which can be overlayed over an image of the facility (Figure 15). In this interface devices can be set up to form a self-healing mesh network topology by selecting a device and changing its configuration to routing [19]. When a device is routing it will forward any messages from nearby devices to the Access Point in the event that a pathway is interrupted. It is worth noting that by configuring a device to form part of a mesh the battery will not last as long [19].



https://10.169.0.102/

Filter: All Devices

Showing 4 of 4 Devices

Devices Online: 1 Access Points, 3 Devices

Alarms: 1 Urgent, 3 High, 0 Medium, 0 Low

Non-redundant

Figure 15: WDM Graphical User Interface of Murdoch Pilot Plant

The WDM is capable of managing devices from different vendors provided that they are either ISA100 or WirelessHART compliant, this is done by downloading a Device Description (DD) file to the WDM [19]. A device DD file is supplied by the equipment manufacturer to integrate their hardware into other manufacturer's software [35]. The WDM has two ethernet port interfaces, one is for the Field Device Network (FDN) and the other is for the Process Control Network (PCN). The FDN interface connects to the managed network switch where incoming traffic from wireless instruments on the network is accessed [37]. The PCN interface connects to the DCS system. It has been designed for ease of use when incorporating it into a Programmable Logic Controller or Distributed Control System by supporting multiple communication protocols.

4.3 Managed Network Switch

Network switches are used to interconnect ethernet devices and allows them to communicate across multiple networks [22]. In an industrial environment some of these devices could be HMI displays, Variable Speed Drives (VSD), instruments and final control elements which are connected to a centralised controller such as a DCS or PLC. A managed network switch allows the user to configure each network interface to meet the needs of the application, provide diagnostics, data prioritisation, segregation, and security [22]. For this project a Cisco DMZ switch was used which is configured through a console port using RS232, this port can be connected to a computer using a serial to USB adapter. This allows you to make changes to the switches configured settings through a Command Line Interface (CLI) program such as PuTTY. In this application the network switch is used to segment the network into a total of 3 VLAN's, this is done for security purposes and to organise the network [37]. A summary of the network switches configuration can be found in the Appendix.

4.4 WLAN Controller

A Wireless LAN (WLAN) controller is used in wireless networks to manage RF utilisation, access policy, quality of service, general configuration and security monitoring in access points [37]. A network can be scaled by deploying additional access points and will be auto configured by the WLAN controller when it is connected to the network. The WLAN controller can be managed through either a Command Line Interface (CLI) by connecting to the console port or by using the web interface, this is done by entering the IP address of the WLAN controller into a web browser [37].

4.5 Access Point

The Access Point is used to provide wireless coverage through a facility, it will poll each device on the network requesting for their process values [35]. Once a packet from a wireless field device has been received it is then routed to the Wireless Device Manager through the ethernet network [35]. The Cisco Aeronet 1552S was selected by Honeywell due to its high bandwidth backhaul, supports ISA100, supports WirelessHART, and it is capable of operating in the tough environments that industry demands. It can be used in conjunction with a wireless Closed Circuit Television (CCTV) network for monitoring of production lines and process plants. This gives Plant Operators the ability to monitor both the process values from the One-Wireless Network as well as have a visual of the equipment in operation.

Figure 16: Cisco Aeronet 1552S Access Point [21]

5 Project Results

5.1 Current Network State

5.1.1 Network Layer 1/2 Troubleshooting

Upon investigation of the current state of the network, it was found that the network was not operational and documentation of the current set-up was limited (Figure 17). To troubleshoot a network, a concise understanding of how the network operates is required. This was done by reviewing the Honeywell document “One-Wireless Wireless LAN Controller Configuration Guide” [37]. This Honeywell document outlines the set-up procedure for configuring the Managed Network Switch, Wireless LAN Controller, and Access Point. The current device configuration of these devices was uploaded to a computer by connecting a serial cable to the console port with the other end connected to a laptop using terminal emulator software such as PuTTY. To access the configuration on Cisco equipment the operator needs to enter Privileged Executive Mode by using the command “enable”, from here the operator can view the configuration by using the command “show running-configuration”. This configuration can be then exported into a text document as a back-up and reference.

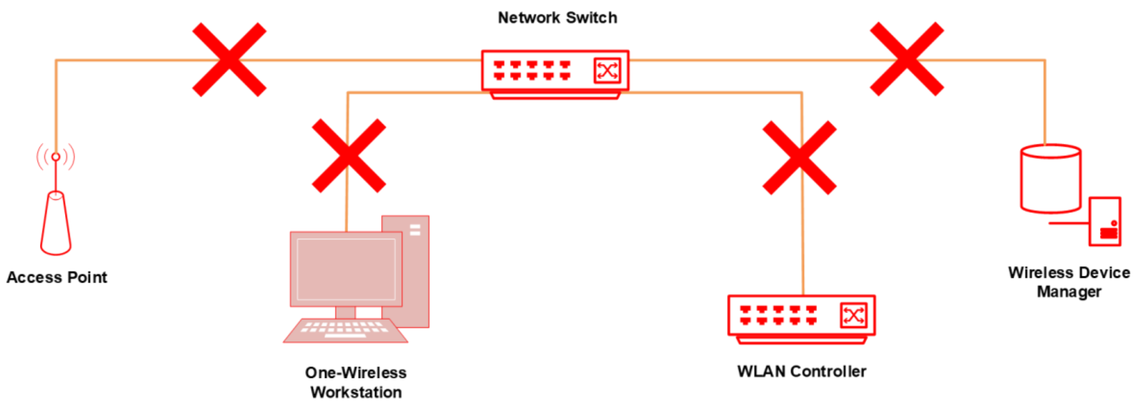


Figure 17: Previous Network State

Once the device configurations were obtained, the network components were connected to their corresponding ports on the managed network switch. The device configuration is important because a managed network switch can be configured to operate differently depending on the port interface is used. Using the network switch configuration file, a Layer 1/2 Network Diagram was developed of the One-Wireless network which shows the physical connections of each device on the network. Developing upon this diagram, a Layer 3 Network Diagram was created (Figure 18). This was done to illustrate the IP address of each device, their corresponding protocol configuration and the Virtual Local Area Network (VLAN). A VLAN is used to segment a network into different logical parts unless a device is given switch port access to a non-native VLAN it won't have access to it. These documents were then compared to the Honeywell document to verify that Network Switch, WLAN Controller and Access Point matched the configuration which was outlined by Honeywell.

5.1.2 Network Layer 3 Troubleshooting

The configuration of each network device strongly matched Honeywell's recommended setup as outlined in their documentation (Figure 18), so further troubleshooting was required. The Network Switch is the central component in the network which interconnects each device, by connecting to the console port over serial connection. The connection of each component could be verified by pinging each device through the CLI. The ping utility is used on networks to determine the reachability of a specified IP address, and the time taken for the device to respond. When the network components where pinged, every device responded except the WLAN Controller. To eliminate the possibility that there was not a Layer 1 fault, the ethernet cable interconnecting the two devices was replaced. The device was pinged again. However, the WLAN Controller did not respond to the Network Switch; this means that the fault is located on Layer 3 of the network between the network switch port interface and the WLAN Controller.

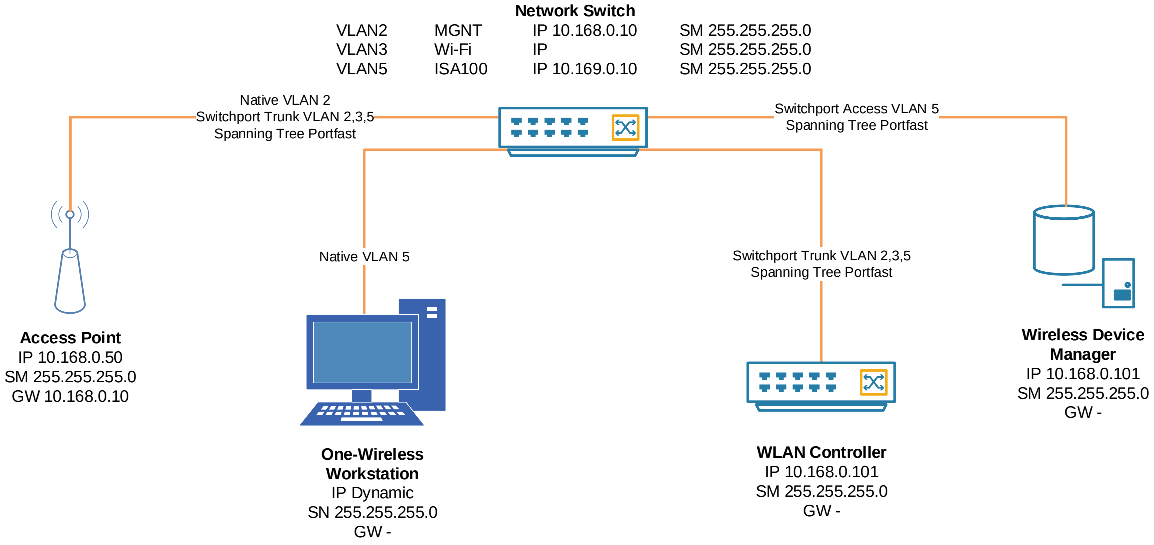


Figure 18: Layer 3 One-Wireless Network Diagram

As a result of this fault, the Access Point was not able to join the LAN even though it was able to be pinged from the network. To further verify this problem a serial connection was established to the Access Point console port, using the CLI to access the error logs. When an Access Point first joins a network it uses a protocol called Control And Provisioning of Wireless Access Points (CAPWAP) [38]. This protocol is used between Access Points and WLAN Controllers to manage device configuration, security policy's and WLAN management [38]. The error logs revealed that the Access Point was sending a CAPWAP discovery request to any WLAN Controllers on the network, but there was no response. At this point, the specialist communications team at Murdoch University got involved in fault finding on the network. It was identified that the Network Switch port that connected to the WLAN Controller was configured for two conflicting protocols which were Switch Port and Trunk.

Due to the conflicting protocols, the WLAN Controller did not respond to any packets, This was resolved by removing the switch port protocol and leaving the trunk port protocol on the network.

The trunk port protocol allows a device to communicate to and only to other trunk ports over multiple VLAN's whereas the switch port protocol only allows for the device to communicate over a single VLAN. Once this correction was made the Access Point and WLAN controller could communicate over a trunk connection to each other and the Access Point was added to the network. It was then found that wireless devices connected to the network where not being assigned a dynamic IP address from the Dynamic Host Configuration Protocol (DHCP), this is a server/client protocol which dynamically allocates IP addresses to client devices [39]. This problem was resolved by accessing the WLAN Controllers Graphic User Interface (GUI) and pointing it to the Wireless Device Manager which operates the DHCP server on the network.

5.1.3 Troubleshooting Reflection

The reason for the network faulting was investigated once it was fully operational again. This is important to ensure that these mistakes are not repeated. Upon investigation, it was suspected that if the network was operational before the commencement of this project that the configuration of the Network Switch and WLAN Controller had not been saved to the flash memory. Because of the configuration not being saved to flash memory the equipment lost its configuration when the power was cycled because it was stored in RAM. For each device, on the network, the current configuration was saved to the devices flash memory, and a configuration backup was saved as a back-up. These problems go to show the importance of developing documentation for an industrial network; it is suggested that the minimum amount of documentation for a network is: Layer 1/2 Network Diagram, Layer 3 Network Diagram, IP Address Table, Password Tables and a backup of each devices configuration. Using this documentation, it is possible to quickly and effectively troubbleshoot and expand upon a network. A brief summary of the troubleshooting process followed can be seen in Table 6.

Table 6: Summary of Troubleshooting Procedure

Step	Task
1	Obtain the device configuration
2	Develop Level 1/2 Network Diagram
3	Check Layer 1/2 Device Configuration
4	Develop Level 3 Network Diagram
5	Develop IP Address Table
6	Check each network device configuration
7	Perform layer 3 troubleshooting tools (Ping, and system logs)
8	Document Results

5.2 DCS Integration

The Wireless Device Manager has two network connections. The first is for the Field Device Network (FDN) and the second is for the Process Control Network (PCN) [19]. The FDN ethernet connection is connected to the managed network switch which receives the process data from the field instruments and the PCN connection is used to connect the network to the DCS network [40]. When the WDM is connected to the DCS network it behaves like a server where the DCS (client) will poll the WDM (server) for the field instrument data [41]. The protocol used for communication between the WDM and DCS depends on the hardware currently being used and the software licenses available. Honeywell's' WDM can use either OPC, CDI, GCI, Modbus TCP/IP and HART [40]. Honeywell suggest that if the wireless data is being used for measurement and control then the best protocol to use is Modbus TCP/IP which has been implemented in this project (Figure 19) [40].

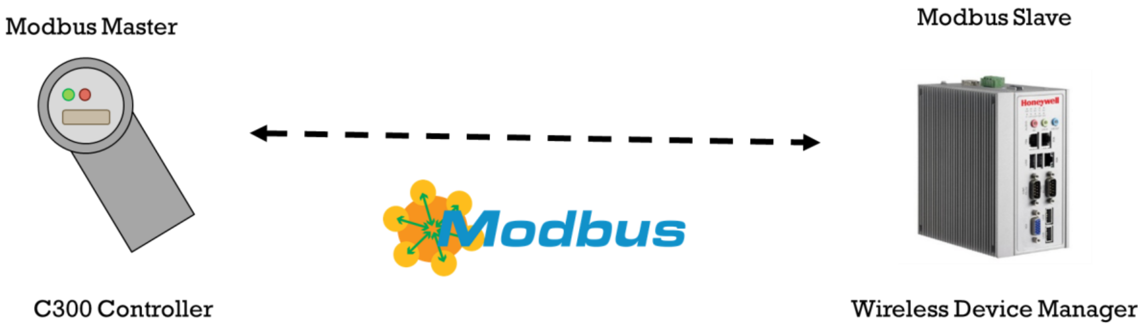


Figure 19: Modbus Communication to DCS [41] [19]

5.2.1 Modbus TCP/IP

Modbus is an application layer protocol developed by Schneider Electric in 1979 for industrial computer system networks [41]. The Modbus protocol is considered open allowing different vendors to develop it into their products without paying royalties or licensing [41]. As a result of being an open protocol, the technology is supported by multiple vendors and is considered the industry standard having proven its functionality [42]. Modbus supports a single master device on a network with a maximum of 247 slave devices. Communication is initiated when the master device sends a request with a packet containing the Slave ID, Function code, Starting address, and the Data [42]. The slave device with the same slave address then sends an acknowledge packet back to the master to confirm the packet was received. The function codes sent by the master device are issued to tell the slave device what data table range it is reading or writing to as seen in Table 7 [42].

Table 7: Modbus Function Codes [42]

Function Code	Description
1	Read Slave Coil Status
2	Read Slave Input Status
3	Read Slave Holding Registers
4	Read Slave Input Registers
5	Write Slave Single Coil Status
6	Write Slave Single Register

Modbus uses a data table system which contains information about a slave device inputs and outputs, the slave devices data table consists of four sections which are have designated read and write permissions (Table 8) [41]. The Modbus data table resides in the slave devices application memory and has a maximum of 9999 addressable data points per section. The first section is used for reading the slave's discrete inputs; the second section can be both read from and written to is the slave devices discrete outputs. The last two sections are the input and holding registers which contain integer data with both read and read-write access.

Table 8: Modbus Data Tables [41]

Table / PDU	Object Size	Type	Description
Discrete Inputs	1 bit	Read-only	Slave device discrete input status
Discrete Outputs	1 bit	Read / Write	Slaves outputs which can be altered
Input register	16 bits	Read-only	Slaves data representing analog inputs
Output register	16 bits	Read / Write	Slave data that can be written to

There are three types of Modbus versions: ASCII, RTU and TCP/IP. Modbus TCP/IP is as version of Modbus that is used for communications over TCP/IP networks on TCP port 502 [41]. The defining features of Modbus TCP/IP is that the Modbus application header (MBAP) replaces the slave ID section of the packet at the beginning of each Modbus packet, in addition to this the Cyclic Redundancy Check (CRC) is also removed because it is already contained within the TCP packet structure these key differences are outlined in Table 9 and Table 10 [42].

Table 9: Modbus Packet Structure [42]

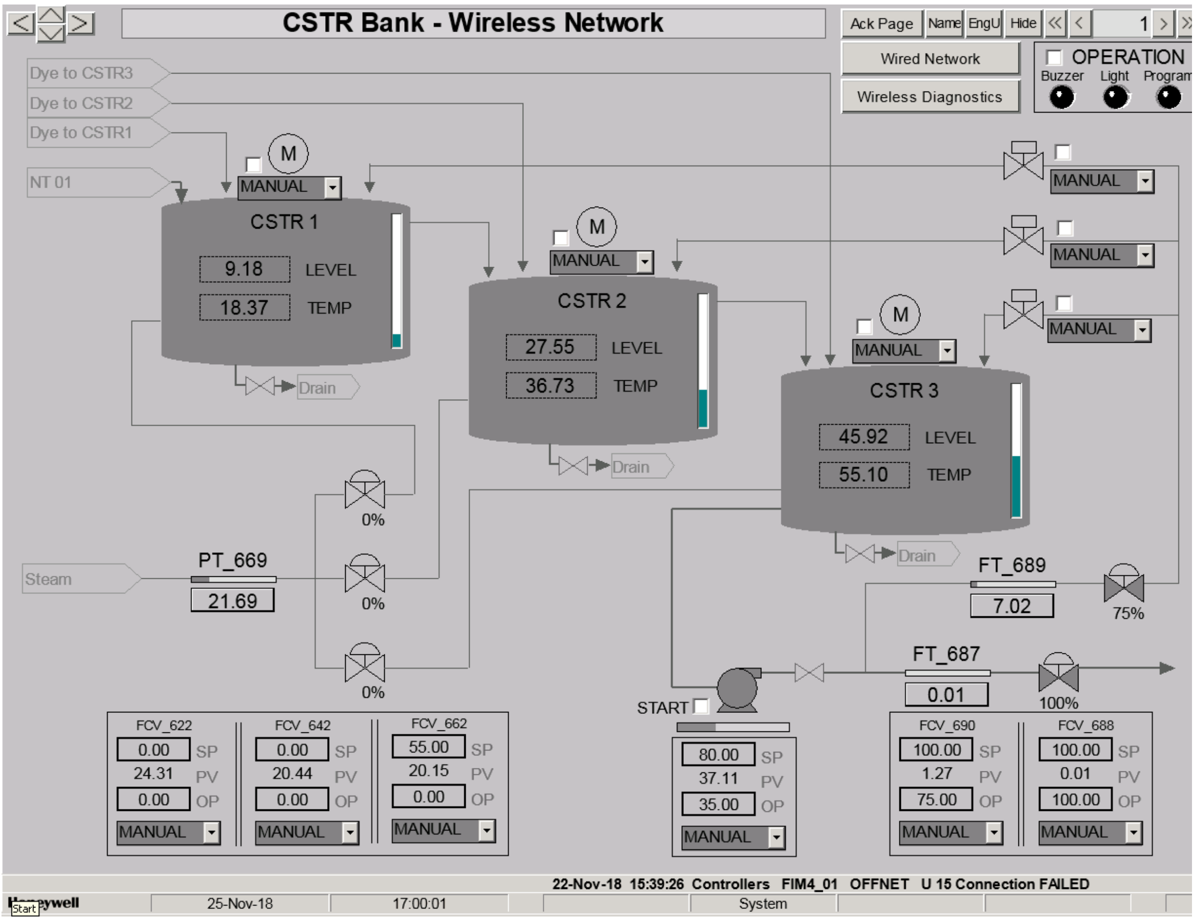
Slave ID	Function Field	Data Field	Error Check Field
1 Byte	1 Byte	1 Word	2 Bytes

Table 10: Modbus TCP/IP Packet Structure [42]

Modbus Header	Function Field	Data Field
1 Byte	1 Byte	1 Word

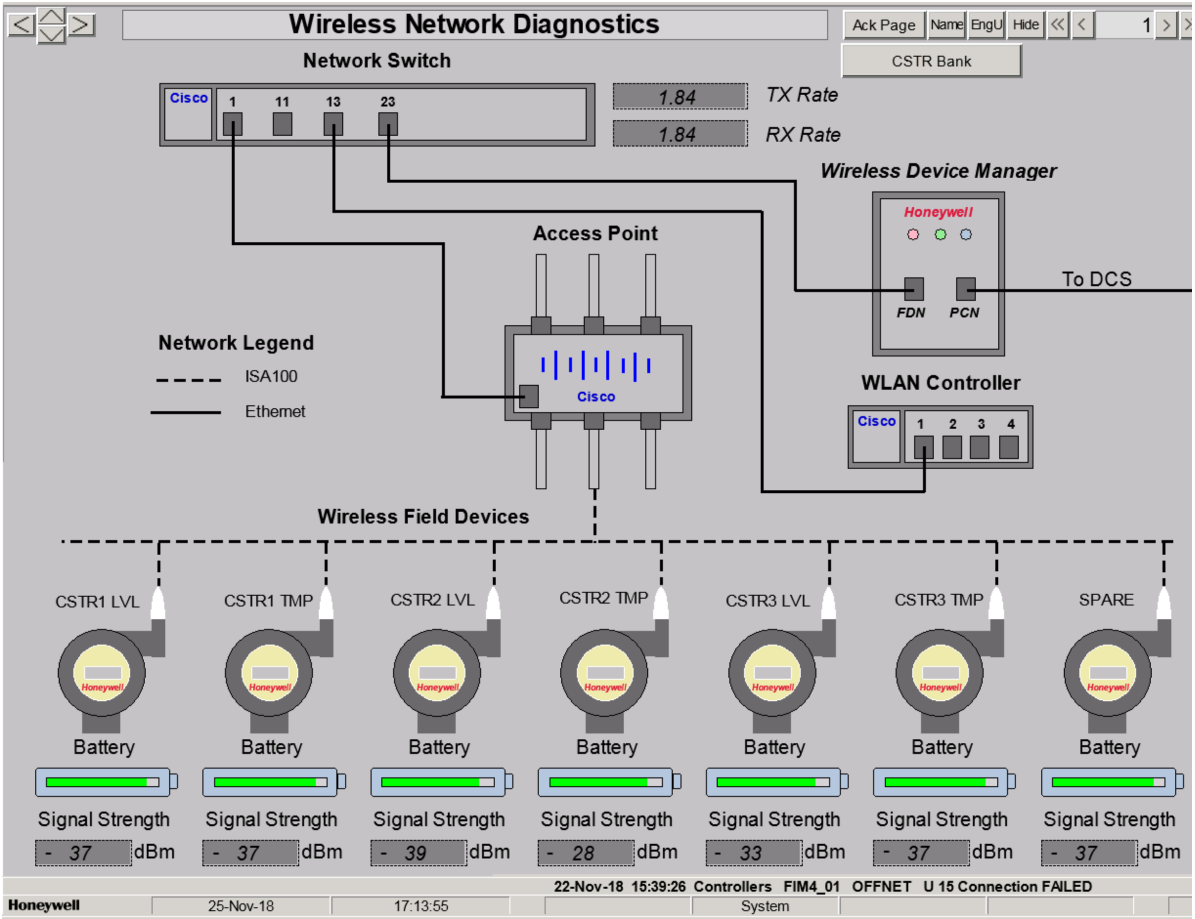
5.2.2 Modbus Server Configuration

The Modbus server is configured in the WDM GUI accessible through the PC workstation which lists the Modbus Discrete Inputs, Discrete Outputs, Input Register, and Output Register [19]. Parameters are added to the tables by using the point picker tool, which allows you to view the available parameters for each device on the network [19]. The Modbus input register was set up to display the process value coming from each device, signal strength and battery level percentage. These parameters where chosen to allow students to troubleshoot the network performance from the Station HMI in the control room. A Station HMI was developed to represent the physical plant which allows students to select between either a wired or wireless network to display the process values (Figure 20), this is done by toggling the button at the top left of the HMI “Wired Network”. On this same HMI page there is an option to open a “Wireless Diagnostics” page which provides key information to for troubleshooting network performance and fault finding (Figure 21).



22-Nov-18 15:39:26 Controllers FIM4_01 OFFNET U 15 Connection FAILED

Figure 20: CSTR Bank Wireless Network HMI



1.84 TX Rate

1.84 RX Rate

CSTR1 LVL	CSTR1 TMP	CSTR2 LVL	CSTR2 TMP	CSTR3 LVL	CSTR3 TMP	SPARE
Battery	Battery	Battery	Battery	Battery	Battery	Battery
Signal Strength	Signal Strength	Signal Strength	Signal Strength	Signal Strength	Signal Strength	Signal Strength
- 37 dBm	- 37 dBm	- 39 dBm	- 28 dBm	- 33 dBm	- 37 dBm	- 37 dBm

22-Nov-18 15:39:26 Controllers FIM4_01 OFFNET U 15 Connection FAILED

Honeywell 25-Nov-18 17:13:55 System

Figure 21: Wireless Network Diagnostics HMI

As part of the process integrating the One-Wireless network into the DCS, simulation software on a laptop was used to simulate the WDM by acting as the Modbus Slave, the computer was then connected to the Process Control Network (PCN) over ethernet cable (Figure 22). The reason this was done is because the instruments set up in the network have not been physically installed on the network and as a result would not show a process value. The Computer was given the same IP address, subnet mask and port as the Wireless Device Manager and values where entered into the corresponding Input Register and checked against the HMI screens in Figure 20 and Figure 21.

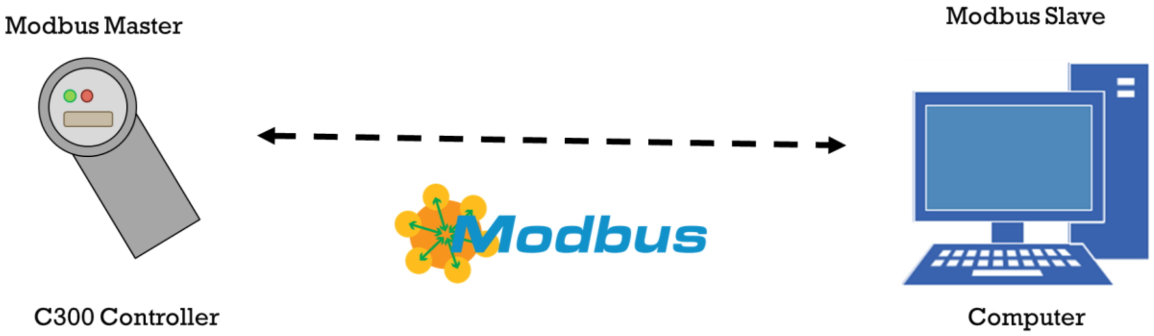


Figure 22: Modbus Communication to Computer [41]

5.3 RF ASSESSMENT

The requirement for a Radio Frequency assessment before deployment or upgrading of an existing wireless network is essential in industrial wireless networks, this is because ISA100 and WirelessHART operate alongside devices using the 2.4GHz Industrial, Scientific, and Medical (ISM) band [24]. In industrial wireless this is particularly important because of the damage that can be done if a network experiences co-channel interference or excessive retransmissions [35]. At the commencement of the project the Honeywell One-Wireless system had already been deployed so a post site RF assessment was performed. When completing a RF assessment, a systematic approach must be followed to ensure that problems don’t arise during normal operation or if the system is scaled. A summary of these steps can be seen in Table 11 adapted from Cisco’s recommended procedure [43].

Table 11: RF Assessment Requirements [43]

Step	Task
1	Review Requirements of the system
2	Inspect the environments wireless bandwidth
3	Evaluate LAN setup
4	Identify RF interference in the area
5	Validate AP location, placement and settings
6	Document the results of the RF Assessment

5.3.1 System Requirements

The One-Wireless system located in the Murdoch University Pilot Plant consists of seven instruments in total. The wireless instruments are to be installed alongside their corresponding wired transmitters in the CSTR tanks to measure tank height and temperature. The intent of the system is to not replace the existing instruments but allow students to select wired or wireless in the station HMI, from there they will be able to develop control schemes around them. Because the system is small and located in a small area only a single access point is required for the system, which is currently located above a walkway. The permanent location for the access point is not yet determined due to the Pilot Plant upgrades taking place in 2019 [44]. These upgrades could result in a walkway being installed above the plant which could affect signal quality and as a result reduce the reliability of the system.

With regards to connection quality it is recommended by Honeywell that the lowest RSQI for each device connection is more than 180 and the RSSI should be more than -80dBm (Table 12), the reason for this is that values outside these constrains will result in signal degradation due to transients in the environment [35]. If the wireless instruments can’t be in an area where it can reach the Access Point a neighbouring instrument can be configured to forward messages to ensure plant wide coverage [19]. The routing policies for each device can be configured in the Wireless Device Manger GUI however, it is worth noting that when a device has been configured to forward packets its battery life won’t last as long which will need to be taken into consideration [19].

Table 12: Connecting Quality Assessment [37]

	Good	Fair	Poor
RSQI Range	255 to 128	127 to 64	63 to 1
RSSI Range	-25 to -75	-76 to -85	-86 to -100
Tx Fail Ratio	0 to 25	24 to 50	49 to 100

5.3.2 Bandwidth and Interference

The neighbouring networks will affect the system depending on their bandwidth utilization, if another network is creating noise on the Industrial Network the transmit fail ratio can be effected and as a result of additional noise on the channel in addition to this it may affect the sample rate of the sensors when waiting to transmit [35]. Because of this it is important to measure the bandwidth usage in the RF assessment. The RF assessment is typically done when the plant is in operation to measure as much interference as possible which can come from neighbouring networks or devices. The bandwidth usage test was conducted by using a Wi-Fi adapter (IEEE802.11ac) which can go into monitor mode. By placing the Wi-Fi adapter in the location of where the wireless instruments are going to be installed the neighbouring networks operating in the 2.4GHz band can be measured.

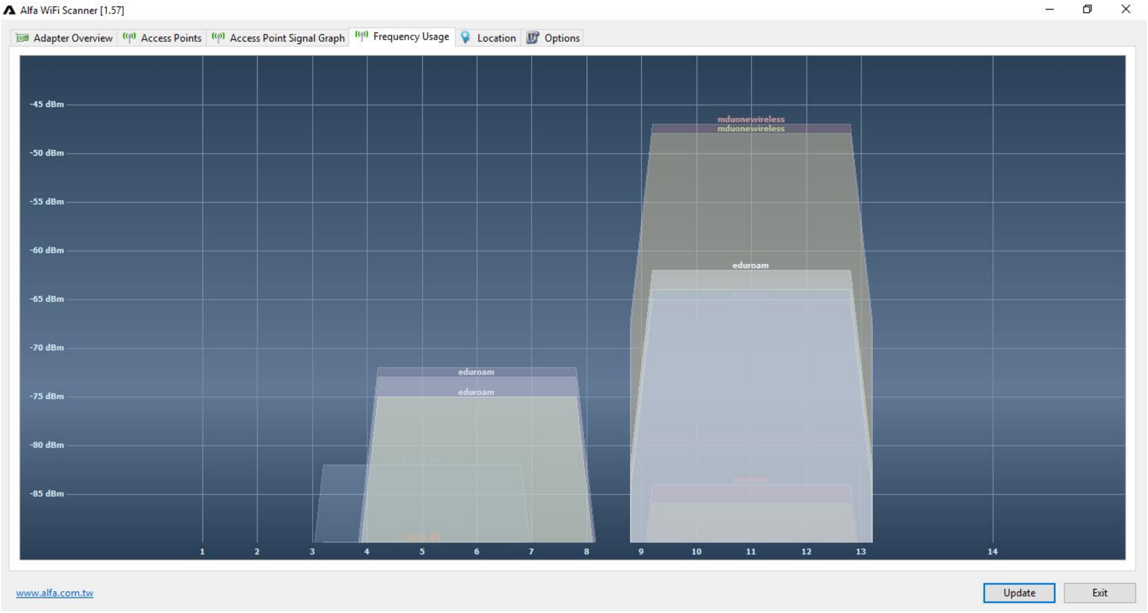
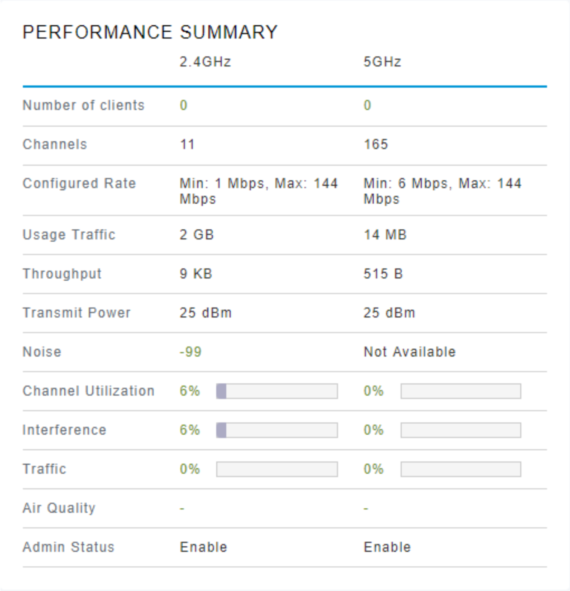


Figure 23: RF Assessment of Pilot Plant

For this assessment a spectrum capture was done with the One-Wireless enabled, from this data the effect of the One-Wireless system can be analysed. It was found that the One-Wireless network operates on the same channel (Channel 12) as the Murdoch student wireless network. Although the access point operates on the same channel as the Murdoch wireless network it is only using a small bandwidth, this was confirmed by accessing the WLAN Controller GUI which manages the access point and provides an access point summary. The access point summary includes all the important information about the access point including its name, location and other information relating to its radio capability's. Contained within the access point summary is the performance summary which details the throughput, and key performance indicators (noise, channel utilisation and interference). With the Pilot Plant running it was found that there is a measured 6% interference and only 6% channel utilisation on channel 12.



PERFORMANCE SUMMARY

	2.4GHz	5GHz
Number of clients	0	0
Channels	11	165
Configured Rate	Min: 1 Mbps, Max: 144 Mbps	Min: 6 Mbps, Max: 144 Mbps
Usage Traffic	2 GB	14 MB
Throughput	9 KB	515 B
Transmit Power	25 dBm	25 dBm
Noise	-99	Not Available
Channel Utilization	6%	0%
Interference	6%	0%
Traffic	0%	0%
Air Quality	-	-
Admin Status	Enable	Enable

Figure 24: Access Point Performance Summary

The recommended channel utilisation for wireless networks is 50%, because the interference and channel utilisation are bellow this threshold the access point settings where not modified [21]. A visual inspection of the Pilot Plant was also conducted to identify what contributed to the measured 6% of interference. In the immediate vicinity there was Bluetooth controlled drones, Microwaves, potentially unshielded cables, and Bluetooth accessories. Because the test was conducted when the plant was running a majority of these factors where captured in the performance summary results in the WLC Controller. If additional instruments are added to the Honeywell One-Wireless network another RF assessment will needed to be completed to ensure that the system is operating within its specifications [35].

6 PROJECT REFLECTION

This thesis has investigated the types of industrial wireless protocols in use today and their applications in a process plant. From this information a brief datum on industrial wireless technology was created which the project was based off detailing the applications of wireless technology, WirelessHART, and ISA100. From here the current state of the network was investigated and identified several problems with the Network Switch and WLAN controller configuration, these configuration issues where resolved with the support of Murdoch University's network engineers. The cause for the problem is suspected to be that the running configuration was not saved to the devices flash memory and as a result was lost when power was cycled. A backup of the correct device configuration for each network device was created as part of best practice and in case there was a different problem which removed the correct configuration from the network devices.

Once the network was operational the remaining four instruments where added to the network by transferring a key to them through the PDA device. Each device was given a description corresponding to their placement within the Pilot Plant and their parameters where added to the Modbus TCP/IP server table. The Wireless Device Manager interface was added into the Pilot Plant server through the DCS software and the corresponding station HMI screens were built to reflect the changes to be made in the plant. On one screen a graphical representation of the network could be used to assist in network troubleshooting, the secondary screen is a graphical representation of the fixed equipment layout where the instruments are planned to be installed. As an extension of this work a short reliability test of the network was completed to ensure it will operate as intended.

This project has been a rewarding experience where through unforeseen circumstances the initial project changed when I found that the network was not operational and It took a lot of work getting it up and running. I gained a lot of value in knowledge through the troubleshooting process however, these problems would not have been resolved without the assistance of Murdoch University staff members Will Stirling, and Jarren Beveridge and Motherwell Automation Senior Engineer Scott Spurway. I found that the technical expertise in this area was limited due to a lack in confidence in troubleshooting industrial wireless networks. Having experienced so many problems firsthand the importance of documentation in the engineering process was further reinforced. This project has given me guidance in what I want to do with my career in engineering which has pushed me to further develop my understanding in Industrial Wireless Networks and Distributive Control Systems. I plan on gaining this experience at my Graduate Engineering role at Motherwell Automation and by becoming a Cisco Certified Network Engineer.

For me the Murdoch engineering pilot plant has been a key success in the understanding industrial computer systems and process control throughout my studies. I hope that the Murdoch University Staff with the assistance of students continue to develop the facility so that other students get to reap the benefits and skills of working on an operating processing facility. With the integration of the Honeywell One-Wireless Network into the facility students will be able to gain experience in an area that is likely to disrupt traditional network architectures in industry giving them exposure in this rewarding and unique field. With the addition the works completed in this thesis a mix of old and new technology has been set up in the facility to keep the Murdoch Engineering Pilot Plant inline with industry requirements.

6.1 FUTURE WORKS

6.1.1 Pilot Plant Expansion

In 2019 to 2020 the Murdoch university pilot plant will undergo an expansion where several plant issues will be resolved, in conjunction with this there will be an expansion on the CSTR tank setup which will be relocated and have additional fixed plant equipment added. This upgrade will include the installation of eight tanks, associated instrumentation, and final control elements for use with the dilution and recycling of salt. The objective of this upgrade is to give students exposure to concentration control systems, reduce water wastage, and to extend the life of the Plant. It is suggested that the Honeywell One-Wireless Instrumentation be used in this setup in conjunction to the wired instrumentation being used for this project. This will mean that the current planned location for the sensors will change in the near future and as a result won't be physically installed until these upgrades are finalized.

Once the location of the wireless field devices is confirmed the Access Point will need be relocated to a more suitable location. The Access Point is currently located on the second level walkway which could pose as a hazard in the event of prolonged exposure. As a precaution a flashing beacon has been installed so that students and staff know when the access point is operating until it is eventually relocated. In the event that some of the instruments not having a line of sight connection to the Access Point some of the instruments can be assigned a routing assignment to forward messages. If routing assignments are not suitable a secondary Access Point can be installed and configured to form mesh continuity with the pre-existing Access Point to provide plant-wide coverage in the Engineering Pilot Plant. This can be set up in the WLAN controller and the Honeywell Wireless Device Manager.

7 CONCLUSION

The outcome of this thesis project was to further develop the Honeywell One-Wireless Network into Murdoch University's Pilot Plant, a secondary objective was to demonstrate that wireless sensor networks are reliable in a small scale process plant. Given the right circumstances over the coming years, we can expect industry to adopt this cutting-edge technology to reduce installation costs, reduce equipment maintenance and most importantly improve network scalability across the manufacturing and resource sectors [1]. The project will also provide students in successive years exposure to wireless sensor networks and give them experience in developing process control strategies in the Pilot Plant with these systems. This project has included the development of handover documentation and procedures with regards to network architecture, device configuration, and network management so that the network can be developed upon in forthcomming years by Murdoch University Staff and studnets.

8 BIBLIOGRAPHY

[1] R. Marshall, “Practically wireless: these systems can be as reliable and secure as hard-wired systems--in some cases, even more so. Yet, the proof isn't in how they have replaced, but rather how they have extended, wired-in networks,” *Chemical Engineering,* 2018.

[2] X. Vilajosana, C. Cano, B. Martinez, P. Tuset, J. Melià and F. Adelantado, “The Wireless Technology Landscape in the Manufacturing Industry: A Reality Check,” Universitat Oberta de Catalunya, Catalonia, Spain, 2018.

[3] I. Silva, L. A. Guedes, P. Portugal and F. Vasques, “Reliability and Availability Evaluation of Wireless Sensor Networks for Industrial Applications,” *sensors,* vol. 12, pp. 806-838, 2012.

[4] N. Kaur and S. Monga, “Comparisons of Wired and Wireless Networks: a Review,” *International Journal of Advanced Engineering Technology,* vol. 5, no. 2, pp. 34-35, 2014.

[5] H. Hussaini, “Design, Commissioning and Testing of Honeywell OneWireless System for Murdoch University Pilot Plant,” Murdoch University, Perth, 2017.

[6] T. Zhou, “Management and Mobility: ISO/OSI, IEEE 802.2, and TCP/IP,” ITPro Today, 30 4 1997. [Online]. Available: https://www.itprotoday.com/management-mobility/isoosi-ieee-8022-and-tcpip. [Accessed 19 08 2018].

[7] A. Leon-Garcia and I. Widjaja, Communication Networks: Fundamental Conepts and Key Architecctures, USA: McGraw-Hill, 2000.

[8] S. Rackley, Wireless Networking Technology: From Principles to Successful Implementation, Burlington: Newnes, 2007.

[9] Computer Networking Notes, “OSI Model Advantages and Basic Purpose Explained,” Computer Networking Notes, 22 01 2018. [Online]. Available: https://www.computernetworkingnotes.com/ccna-study-guide/osi-model-advantages-and-basic-purpose-explained.html. [Accessed 19 08 2018].

[10] D. Reynders and E. Wright, Practical TCP/IP and Ethernet Networking, Burlington: Oxford, 2003.

[11] Information Sciences Institute University of Southern California, Transmission Control Protocol, Virginia: DARPA Internet Program Protocol Specifcation, 1981.

[12] J. Postel, User Datagram Protocol, 08: Information Sciences Institute University of Southern California, 1980.

[13] Texolbd, “Features of TCP and UDP,” Texolbd, 13 05 2017. [Online]. Available: http://texolbd.com/2017/06/13/tcp-udp-features/. [Accessed 06 09 2018].

[14] M. Rouse, “Network layer,” 04 2018. [Online]. Available: https://searchnetworking.techtarget.com/definition/Network-layer. [Accessed 06 09 2018].

[15] M. Rouse and S. Curtis, “Logical Link Control layer (LCL layer),” Search Networking, 2014. [Online]. Available: https://searchnetworking.techtarget.com/definition/Logical-Link-Control-layer. [Accessed 17 09 2018].

[16] A. Shekhar, “LLC Layer (Logical Link Control): Data Link Layer Of OSI Model,” FossBytes, 18 04 2016. [Online]. Available: https://fossbytes.com/llc-logical-link-control-layer-osi-model/. [Accessed 17 09 2018].

[17] M. Probst and L. Trieloff, “Bit and Frame Synchronization Techniques,” Hasso-Plattner-Institute for Software System Engineering.

[18] Stanford, “Inter-LAN Interference,” Wireless Computing, 2018. [Online]. Available: https://cs.stanford.edu/people/eroberts/courses/soco/projects/2003-04/wireless-computing/int_interlan.shtml. [Accessed 22 09 2018].

[19] Honeywell, “OneWireless Wireless Device Manager User's Guide,” Honeywell, New Jersey, 2011.

[20] Fluidic, “Honeywell XYR6000 ISA100 Temperature Transmitte,” Fluidic, 2018. [Online]. Available: https://fluidic-ltd.co.uk/product/xyr6000-temperature/. [Accessed 22 09 2018].

[21] Cisco, “Cisco Aironet 1552S Outdoor Access Point,” Cisco, 2018. [Online]. Available: https://www.cisco.com/c/en/us/support/wireless/aironet-1552s-outdoor-access-point/model.html. [Accessed 22 09 2018].

[22] Cisco, “Cisco Gigabit Managed Switch,” Cisco, 2018. [Online]. Available: https://www.cisco.com/c/en/us/support/switches/sg300-28-28-port-gigabit-managed-switch/model.html. [Accessed 22 09 2018].

[23] Fluidic, “Honeywell ISA100 WDM Wireless Device Manager,” Fluidic, 2018. [Online]. Available: https://fluidic-ltd.co.uk/product/isa100-wdm/. [Accessed 22 09 2018].

[24] Australian Communications and Media Authority, 2018. [Online]. Available: https://www.acma.gov.au/-/media/Spectrum-Transformation-and-Government/Publication/pdf/spectrum_chart2013-pdf.pdf. [Accessed 23 09 2018].

[25] Everything RF, “EIRP Calculator,” Everything RF, 2015. [Online]. Available: https://www.everythingrf.com/rf-calculators/eirp-effective-isotropic-radiated-power. [Accessed 23 09 2018].

[26] D. M. Z. Kurian, R. B. N and C. B, “The effects of Inter Symbol Interference (ISI) and FIR Pulse Shaping Filters,” *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering,* vol. 3, no. 5, pp. 9411-9416, 2014.

[27] Nutaq, “An Introduction To Orthogonal Frequency Division Multiplex (OFDM),” Nutaq, 2018. [Online]. Available: https://www.nutaq.com/blog/introduction-orthogonal-frequency-division-multiplex-ofdm. [Accessed 23 09 2018].

[28] D. Carlo, “Wireless Field Instrumentation,” CMC, Massachusetts, 2013.

[29] G. Lohmann, “Technical White Paper Wireless Technology WirelessHART,” Pepperl+Fuchs, Berlin, 2011.

[30] Gas Secure, “Wireless Communication in Safety Systems,” Safe Wireless, Norway, 2018.

[31] J. Werb and S. Amidi, “Control Over Wireless Current Applications and Future Opportuinities,” ISA, North Carolina, 2012.

[32] A. Feng, “An Overview Of WirelessHART’s OSI Layers,” AWAITech, 24 11 11. [Online]. Available: https://www.awiatech.com/an-overview-of-wirelesshart%E2%80%99s-osi-layers/. [Accessed 29 11 2018].

[33] Emerson, “AMS 9420 Wireless Vibration Transmitter,” Emerson, 2018. [Online]. Available: https://www.emerson.com/en-us/catalog/ams-a9420. [Accessed 30 11 2018].

[34] Emerson, “Fisher™ 4320 Wireless Position Monitor,” Emerson, 2018. [Online]. Available: https://www.emerson.com/en-us/catalog/fisher-4320. [Accessed 30 11 2018].

[35] Honeywell, “OneWireless Network Planning and Installation Guide,” Honeywell, New Jersey, 2016.

[36] Cisco, “Cisco 2500 Series Wireless Controllers,” Cisco, 2018. [Online]. Available: https://www.cisco.com/c/en/us/support/wireless/2500-series-wireless-controllers/tsd-products-support-series-home.html. [Accessed 29 11 2018].

[37] Honeywell, “OneWireless Wireless LAN Controller Configuration Guide,” Honeywell, New Jersey, 2016.

[38] J. Scarpati, “CAPWAP (Control and Provisioning of Wireless Access Points),” Search Networking, October 2014. [Online]. [Accessed 05 11 2018].

[39] Microsoft, “Dynamic Host Configuration Protocol (DHCP),” Microsoft, 09 01 2018. [Online]. Available: https://docs.microsoft.com/en-us/windows-server/networking/technologies/dhcp/dhcp-top. [Accessed 05 11 2018].

[40] Honeywell, “OneWireless OneWireless Experion PKS Integration Guide,” Honeywell, New Jersey, 2016.

[41] Modbus Organization, “Modbus Application Protocol Specification,” Modbus, Massachusetts.

[42] S. Mackay, E. Wright, D. Reynders and J. Park, Practical Industrial Data Networks: Design, Installation and Troubleshooting, USA: Oxford, 2004.

[43] Cisco, “Site Survey and RF Design Validation,” Cisco, California, 2018.

[44] R. Sebesta, “Design, Planning and Implementation of the Dilution and Recycle Section of the Engineering Pilot Plant,” Murdoch University, Perth, 2018.

[45] Lifewire, “OSI Model Reference Guide,” Lifewire, 10 2016. [Online]. Available: https://www.lifewire.com/osi-model-reference-guide-816289. [Accessed 06 09 2018].

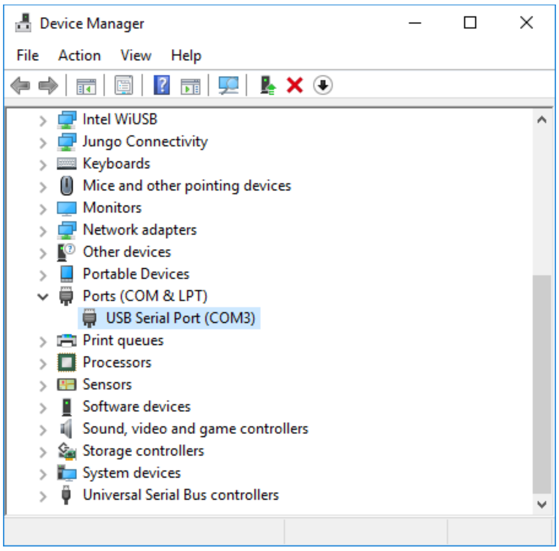
9 APPENDIX

9.1 NETWORK TROUBLESHOOTING PROCEDURE

If the network isn't operating the procedure documentation at a minimum is required:

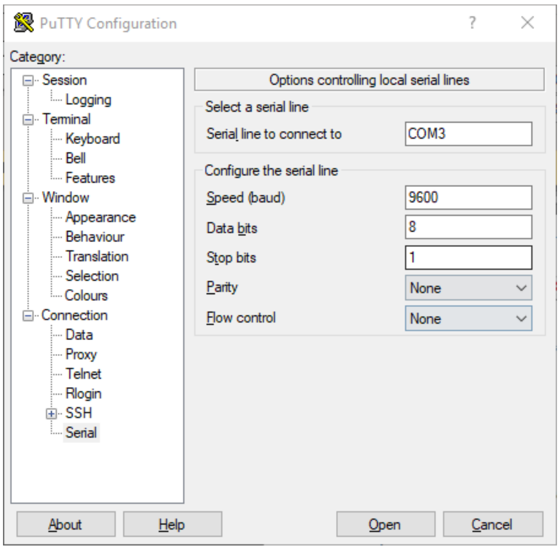
1. Layer 1/2 Network Diagram
2. Layer 3 Network Diagram
3. IP address table
4. Network Switch Configuration
5. Password vault

This documentation can be found in the following sections, in addition to this a Cisco console cable is needed to connect to the Cisco hardware and PuTTY needs to be installed on a computer to access the devices configuration. The settings for the CLI program can be seen in Figure 26. The serial line is dependant on the computer being used and can be found under device manager and ports (Figure 25).



- Intel WiUSB
- Jungo Connectivity
- Keyboards
- Mice and other pointing devices
- Monitors
- Network adapters
- Other devices
- Portable Devices
- Ports (COM & LPT)
  - USB Serial Port (COM3)
- Print queues
- Processors
- Sensors
- Software devices
- Sound, video and game controllers
- Storage controllers
- System devices
- Universal Serial Bus controllers

Figure 25: Device Manager Ports in Use



Options controlling local serial lines

Select a serial line

Serial line to connect to: COM3

Configure the serial line

Speed (baud): 9600

Data bits: 8

Stop bits: 1

Parity: None

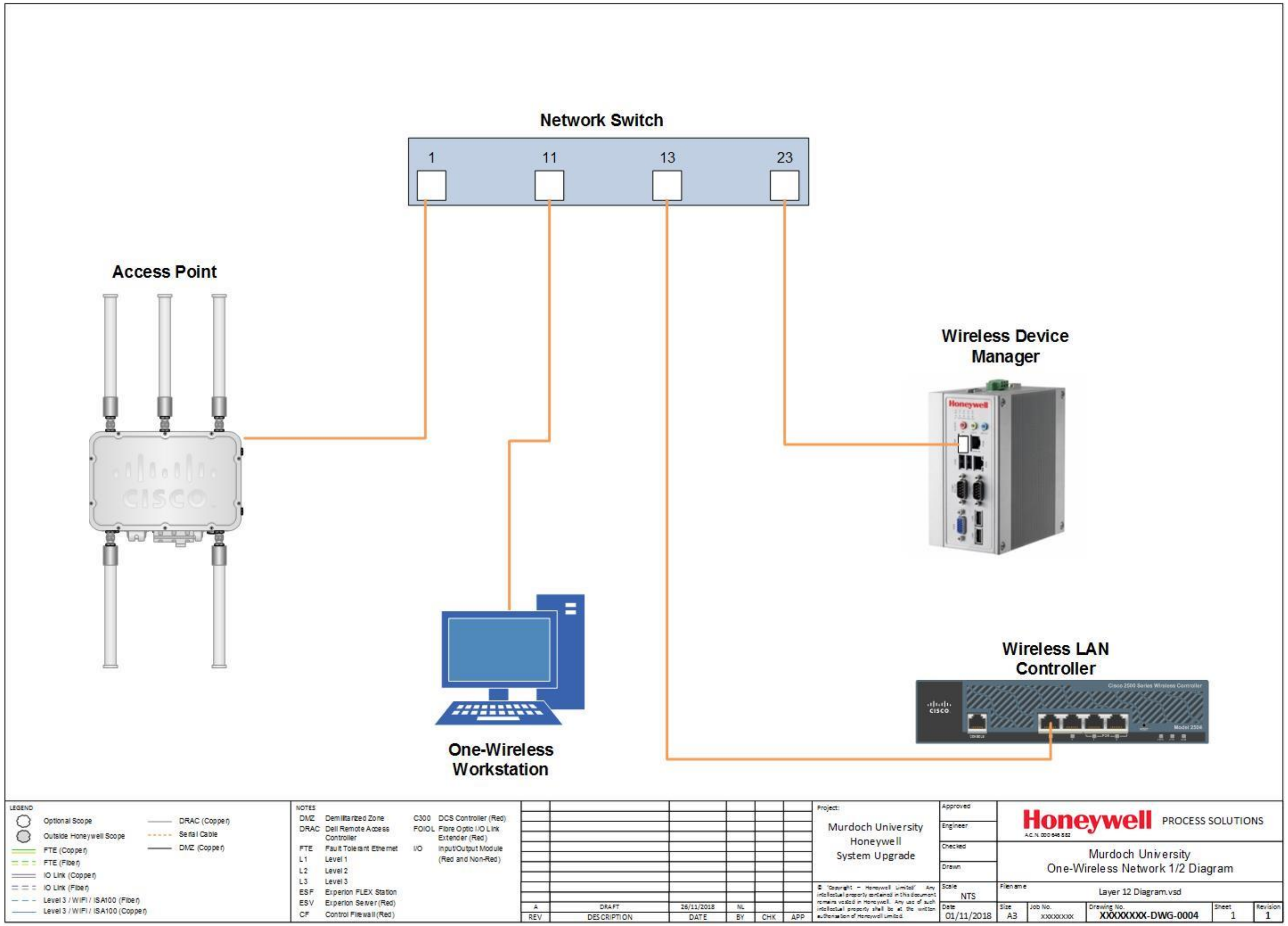
Flow control: None

Figure 26: PuTTY Terminal Configuration

Table 13: Network Troubleshooting Procedure

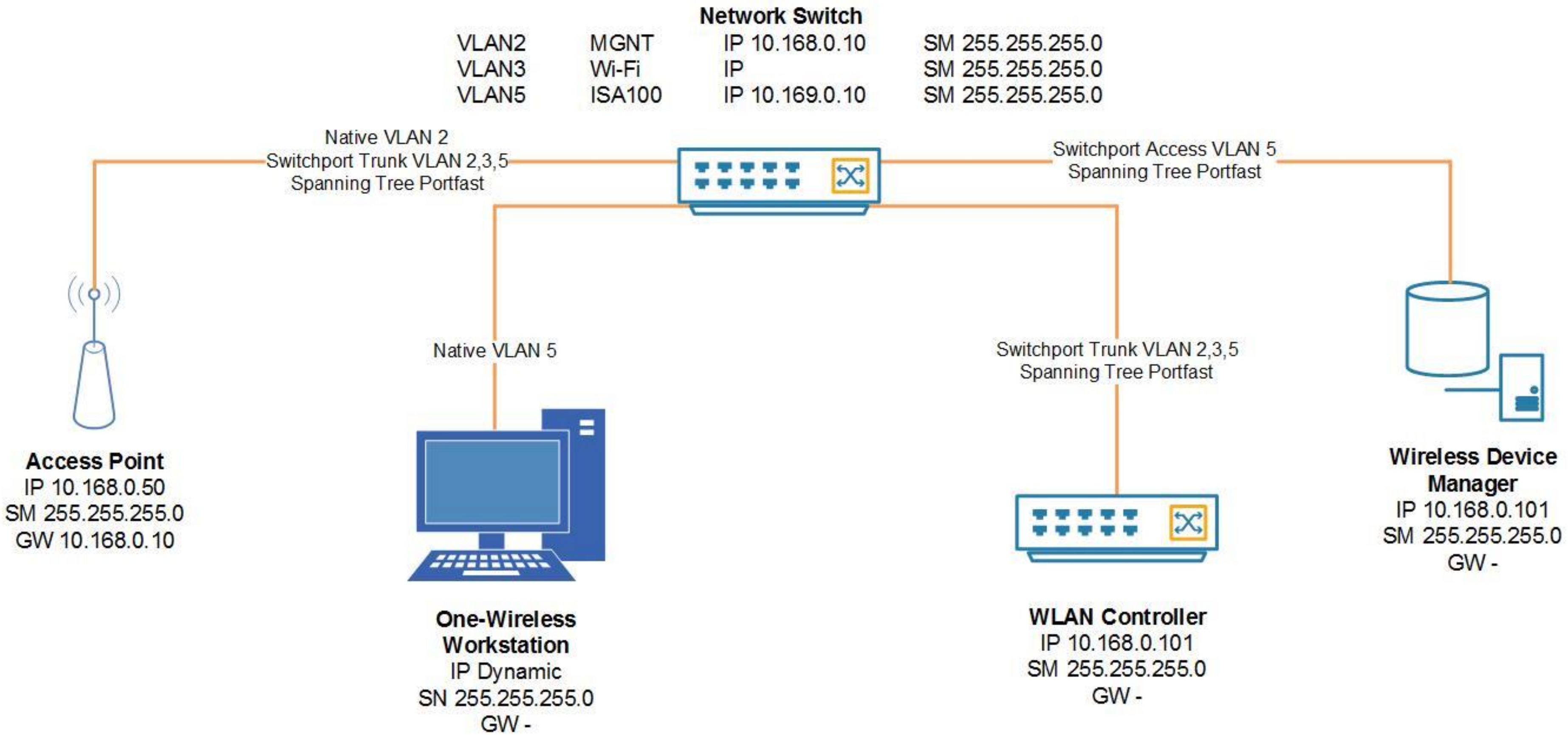
Step	Task
1	Ensure that each device is turned on: Network Switch, WLAN Controller, Access Point, Wireless Device Manager, PC and Instruments.
2	Using the Layer 1/2 Network Diagram check the physical connection for each device.
3	Reset power to each device.
4	On the Network Switch ensure that each connected port is green for operational.
5	Using the Cisco console cable connect to the console port of the network switch.
6	On a PC open a CLI program such as PuTTY and set the following settings: Serial, Speed (9600), Data bits (8), Stop bits (1), Parity (none), and Flow control (none).
7	Once connection is established enter privileged executive mode by typing "enable"
8	In the command line ping each device in the IP Address table (ping xxxx.xxx.xxx.xxx).
9	If an address is unreachable from the network switch check the network switch configuration for that port by typing "show running-config".
10	Compare the running configuration of the network switch to the configuration file.
11	Check the network switch system log "show logging".
12	Repeat this process with the faulty Cisco device, any password requirements can be found in the Password Vault
13	Document what the issue is and how it was resolved for others.

9.2 LAYER 1/2 DIAGRAM



Network Switch
1
11
13
23
Access Point
Wireless Device Manager
One-Wireless Workstation
Wireless LAN Controller
LEGEND
Optional Scope
Outside Honeywell Scope
FTE (Copper)
FTE (Fiber)
IO Link (Copper)
IO Link (Fiber)
Level 3 / WIFI / ISA100 (Fiber)
Level 3 / WIFI / ISA100 (Copper)
DRAC (Copper)
Serial Cable
DMZ (Copper)
NOTES
DMZ Demilitarized Zone
DRAC Dell Remote Access Controller
FTE Fault Tolerant Ethernet
L1 Level 1
L2 Level 2
L3 Level 3
ESF Experion FLEX Station
ESV Experion Server (Red)
CF Control Firewall (Red)
C300 DCS Controller (Red)
FOIOL Fibre Optic I/O Link Extender (Red)
I/O Input/Output Module (Red and Non-Red)
A DRAFT 26/11/2018 NL
REV DESCRIPTION DATE BY CHK APP
Project:
Murdoch University
Honeywell
System Upgrade
© 'Copyright – Honeywell Limited' Any intellectual property contained in this document remains vested in Honeywell. Any use of such intellectual property shall be at the written authorisation of Honeywell Limited.
Approved
Engineer
Checked
Drawn
Honeywell PROCESS SOLUTIONS
A.C.N. 000 646 882
Murdoch University
One-Wireless Network 1/2 Diagram
Scale NTS
Filename Layer 12 Diagram.vsd
Date 01/11/2018
Size A3
Job No. XXXXXXXX
Drawing No. XXXXXXXX-DWG-0004
Sheet 1
Revision 1

9.3 Layer 3 Diagram



9.4 IP Address Table

Device	Static	Dynamic	IP Address	Subnet Mask	VLAN
Access Point	✓	✗	10.168.0.50	255.255.255.0	2,3,5
Network Switch (VLAN1)	✓	✗	10.168.0.10	255.255.255.0	2
Network Switch (VLAN2)	✓	✗	N/A	255.255.255.0	3
Network Switch (VLAN3)	✓	✗	10.169.0.10	255.255.255.0	5
Wireless Device Manager (FDN)	✓	✗	10.169.0.102	255.255.255.0	5
Wireless Device Manager (PCN)	✓	✗	192.168.133.190	255.255.255.0	N/A
WLAN Controller	✓	✗	10.168.0.101	255.255.255.0	2,3,5
Workstation	✗	✓	N/A	255.255.255.0	5

9.5 Network Switch Configuration

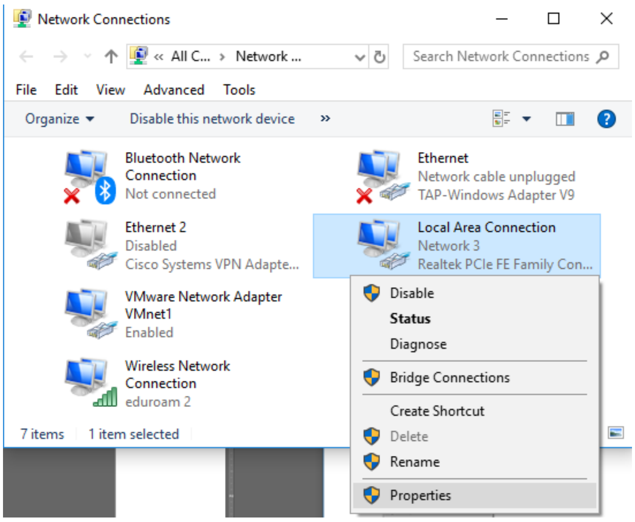
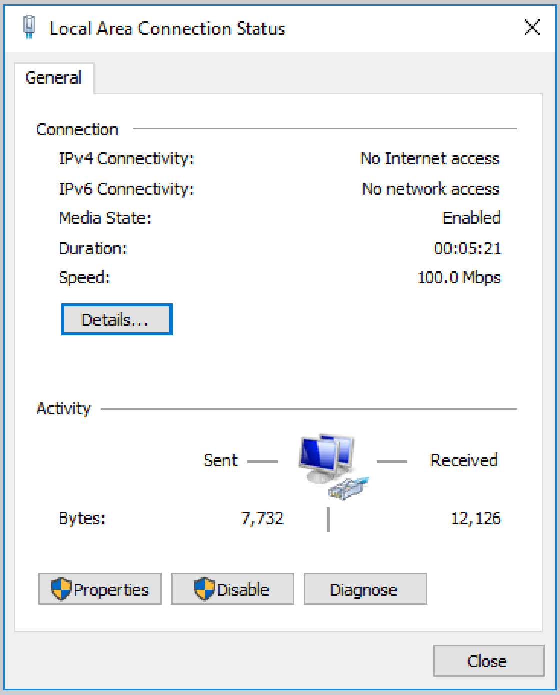
Ethernet Port	Description	Configuration
1	Root Access Point	switchport trunk encapsulation dot1q switchport trunk native vlan 2 switchport trunk allowed vlan 2,3,5 switchport mode trunk spanning-tree portfast trunk
2	Field Access Point	switchport access vlan 2 switchport trunk encapsulation dot1q switchport trunk native vlan 2 switchport trunk allowed vlan 2,3,5 switchport mode access spanning-tree portfast trunk

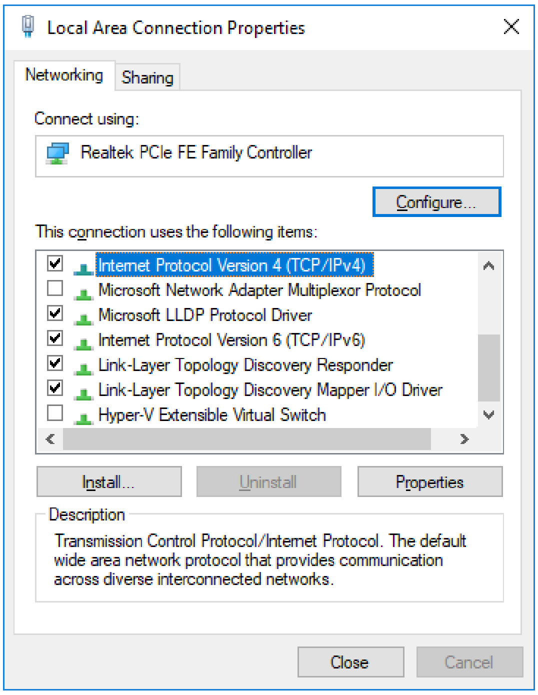
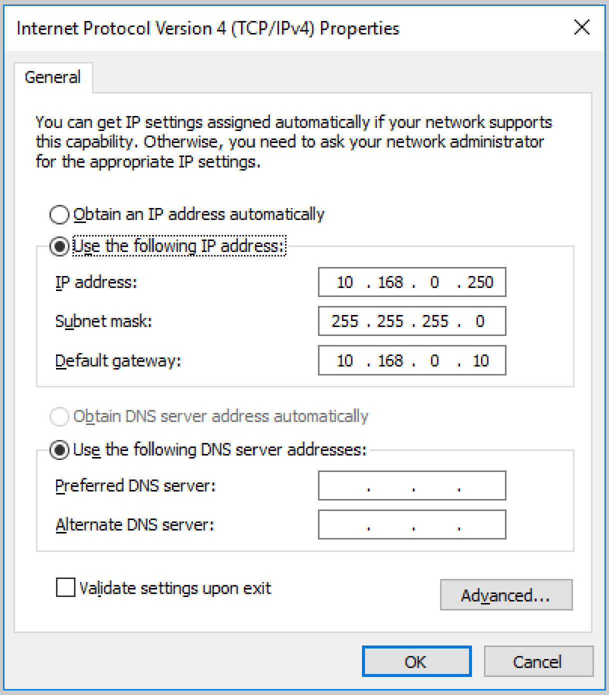
11	Workstation	switchport access vlan 5 switchport mode dynamic desirable
13	WLAN Controller	switchport trunk encapsulation dot1q switchport trunk allowed vlan 2,3,5 switchport mode trunk spanning-tree portfast trunk
23	WDM	description WDM-001 switchport access vlan 5 switchport mode dynamic desirable duplex full spanning-tree portfast

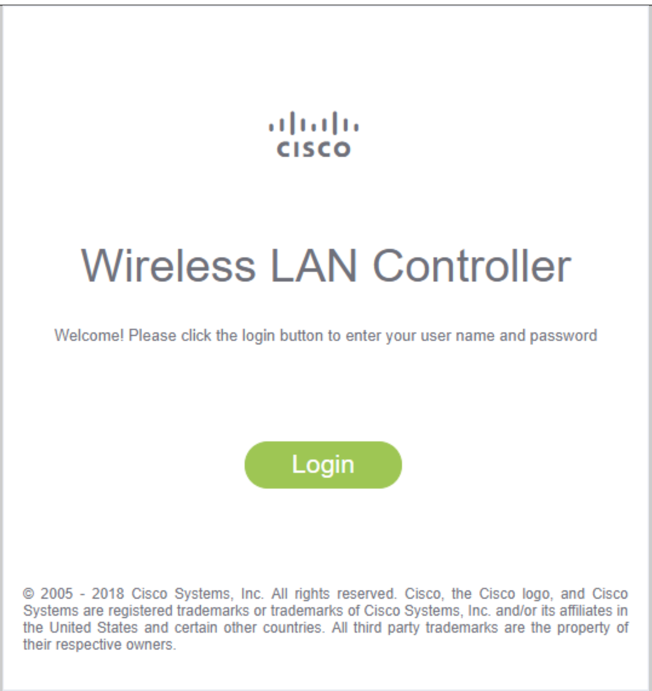
9.6 PASSWORD VAULT

Device	Username	Password	Role
WDM	admin	standoff atomizer faraway	Administration
WDM	Technician	nonskid calmly rabble	Restricted Privileges
WDM	Student	encircle cutlass payoff	View-Only
WLAN Controller	Admin	Honeywell@	Administration
AP	Admin	Honeywell@	Administration
PDA	onewireless	1682	Administration
PC	EEPROJ-28\onewireless	Onew!rel3ss	Administration

9.7 Accessing the WLAN Controller GUI

Item	Task
1	Connect an ethernet cable from your PC to the second port of the Network Switch.
2	On the PC open network connections and select the properties for the NIC that is connected to the Network Switch.  Network Connections Bluetooth Network Connection – Not connected Ethernet – Network cable unplugged – TAP-Windows Adapter V9 Ethernet 2 – Disabled – Cisco Systems VPN Adapte... Local Area Connection – Network 3 – Realtek PCIe FE Family Con... VMware Network Adapter VMnet1 – Enabled Wireless Network Connection – eduroam 2 7 items 1 item selected « All C... › Network ... Search Network Connections File Edit View Advanced Tools Organize ▾ Disable this network device » Disable Status Diagnose Bridge Connections Create Shortcut Delete Rename Properties
3	Open Properties under Local Area Connection Status.  Local Area Connection Status General Connection IPv4 Connectivity: No Internet access IPv6 Connectivity: No network access Media State: Enabled Duration: 00:05:21 Speed: 100.0 Mbps Activity Sent — Received Bytes: 7,732 | 12,126

4	Open the Properties for Internet Protocol Version 4 (TCP/IPv4)  Local Area Connection Properties Networking Sharing Connect using: Realtek PCIe FE Family Controller Configure... This connection uses the following items: ☑ Internet Protocol Version 4 (TCP/IPv4) □ Microsoft Network Adapter Multiplexor Protocol ☑ Microsoft LLDP Protocol Driver ☑ Internet Protocol Version 6 (TCP/IPv6) ☑ Link-Layer Topology Discovery Responder ☑ Link-Layer Topology Discovery Mapper I/O Driver □ Hyper-V Extensible Virtual Switch Install... Uninstall Properties Description Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks. Close Cancel
5	Enter the following settings into the Properties window.  Internet Protocol Version 4 (TCP/IPv4) Properties General You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings. ○ Obtain an IP address automatically ● Use the following IP address: IP address: 10 . 168 . 0 . 250 Subnet mask: 255 . 255 . 255 . 0 Default gateway: 10 . 168 . 0 . 10 ○ Obtain DNS server address automatically ● Use the following DNS server addresses: Preferred DNS server: . . . Alternate DNS server: . . . □ Validate settings upon exit Advanced... OK Cancel
6	Open a web browser and type the following into the address bar http://10.168.0.101
7	You'll be able to log into the WLC Controller using the username and password listed in the Password Vault.

	 Wireless LAN Controller Welcome! Please click the login button to enter your user name and password © 2005 - 2018 Cisco Systems, Inc. All rights reserved. Cisco, the Cisco logo, and Cisco Systems are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. All third party trademarks are the property of their respective owners.

9.8 Accessing the Wireless Device Manager GUI

Item	Task
1	Ensure that the network is physically connected as per the Layer 1/2 network diagram.
2	Open internet explorer and type the following into the address bar http://10.169.0.102
3	Using the username and password in the Password Vault you’ll be able to log in.