

OneWireless
Network Planning and Installation Guide

OWDOC-X253-en-220A
October 2013

Release 220

Document	Release	Issue	Date
OWDOC-X253-en-220A	220	0	October 2013

Disclaimer

This document contains Honeywell proprietary information. Information contained herein is to be used solely for the purpose submitted, and no part of this document or its contents shall be reproduced, published, or disclosed to a third party without the express permission of Honeywell International Sarl.

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

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

Copyright 2013 - Honeywell International Sarl

Contents

1 About this guide	5
2 OneWireless Network overview	7
2.1 About OneWireless Network	8
2.2 ISA100 Wireless compliance	9
2.3 Supported OneWireless Network protocols	10
2.4 OneWireless Network components	11
3 OneWireless Network planning	13
3.1 Supported network topologies	14
3.2 Planning an ISA100 Wireless field device network	15
3.3 Planning a network with IEEE 802.11a/b/g/n wireless infrastructure	16
3.4 Planning for large networks	18
3.5 Designing the OneWireless Network	21
3.6 Planning for OneWireless Network security	23
3.7 Integrating OneWireless Network with DCS	25
4 OneWireless components installation	27
4.1 OneWireless system requirements	28
4.2 Installing the OneWireless Network components	29
4.3 Setting up the field devices	30
5 Site survey and pre-installation	31
5.1 Regulatory Compliance	32
5.1.1 FCC, IC, and ETSI requirements	32
5.2 Tools and equipment	33
5.3 Antenna selection and RF output power	34
5.3.1 Antenna types	34
5.3.2 802.11a/n 5 GHz antennas	34
5.3.3 802.11b/g/n 2.4 GHz antennas	35
5.3.4 ISA 100.11a 2.4 GHz radio antennas	35
5.4 Range, coverage, and link budget analysis	36
5.4.1 Theoretical coverage and range prediction	36
5.4.2 Empirical coverage and range prediction	36
5.4.3 Wireless backhaul data rate	36
6 Hardware installation	39
6.1 Precautions	40
6.2 Antenna isolation	41
6.3 RF power output validation	42
6.4 Power supply options	43
6.5 Protecting and securing installation	44
6.5.1 Surge suppression	44
6.5.2 Weatherproofing	45
7 System configurations	47
7.1 Radio frequency considerations	48
7.1.1 Cisco AP frequency and operating mode	48
7.1.2 IEEE 802.11a and dynamic frequency selection	48

7.1.3	Unlikely sources of DFS-aware radar signals	48
7.1.4	Likely sources of DFS-aware radar signals	49
7.1.5	Field device radio frequency allocation	49
7.2	Network redundancy and availability	51
7.2.1	IEEE 802.11 network	51
7.2.2	ISA100 network	51
7.2.3	Cisco WLC redundancy	51
7.2.4	Root Access Point (RAP) redundancy	51
7.2.5	Mesh convergence time	51
7.2.6	Configuring the WDM redundancy	51
7.3	IP addressing and DHCP considerations	54
7.3.1	Cisco AP IP addressing	54
7.3.2	FDAP IP addressing	54
7.4	Time synchronization	55
7.4.1	Network time synchronization through NTP	55
7.4.2	ISA radio MAC layer time synchronization	55
8	Security and network isolation	57
8.1	ISA100 network security	58
8.2	IEEE 802.11 mesh and Wi-Fi client security	59
8.3	Virtual LAN considerations	60
9	Performance monitoring	61
9.1	Wireless link quality	62
9.1.1	Configuring Connection Quality Options	62
9.1.2	Verifying connectivity using maps	63
9.1.3	Generating reports	64
9.2	Network management tools	66
10	Notices	67
10.1	Documentation feedback	68
10.2	How to report a security vulnerability	69

1 About this guide

This guide provides information about planning, designing, and setting up the OneWireless Network using Cisco 1552S Light Weight Access Point and/or FDAP infrastructure nodes. It also provides security information and recommendations to assist you in deploying a secure environment for your network.

Intended audience

This guide is intended for people who are responsible for planning and designing the OneWireless Network. These people include Plant Managers, Process Engineers, and System Administrators.

Prerequisite skills

It is assumed that you are familiar with the operation of OneWireless Network, Microsoft Windows operating systems, and network administration tasks.

Required Honeywell documentation

The following documents and sources contain additional information required for deploying OneWireless Network. It is recommended to have these documents readily available for reference.

Document	Document ID	Description
<i>OneWireless Field Device Access Point User's Guide</i>	OWDOC-X256-en-220A	This document describes the procedures to install, configure, and operate an FDAP.
<i>OneWireless Wireless Device Manager User's Guide</i>	OWDOC-X254-en-220A	This document describes the procedures to provision, configure, operate, and monitor an ISA100 Wireless wireless field device network using Wireless Device Manager (WDM).
<i>OneWireless Wireless LAN Controller Configuration Guide</i>	OWDOC-X255-en-220A	This document provides information about planning, designing, setting up, and configuring a OneWireless Network using WDM, FDAPs, Cisco 1552S APs, and field devices.
<i>OneWireless Migration User's Guide</i>	OWDOC-X258-en-220A	This document assists you in understanding, planning, and performing the migration of standalone OneWireless Network.

Document	Document ID	Description
<i>OneWireless Parameter Reference Dictionary</i>	OWDOC-X260-en-220A	This document provides information about the parameters associated with OneWireless devices.
<i>OneWireless FDAP Regulatory Compliance Guide</i>	—	This document provides information about the FDAP regulatory compliance details.
<i>Cisco AP Professional Installation Guide</i>	—	This document provides information about Cisco AP installation details.

You can download Honeywell documentation from <http://www.honeywellprocess.com> web site.

2 OneWireless Network overview

Related topics

“About OneWireless Network” on page 8

“ISA100 Wireless compliance” on page 9

“Supported OneWireless Network protocols” on page 10

“OneWireless Network components” on page 11

2.1 About OneWireless Network

OneWireless Network is a multi-standard, multi-field protocol wireless network that can be tailored to offer coverage for industrial applications. This includes a simple wireless field device network to a completely integrated plant-wide, multi-application Wireless Local Area Network (WLAN). OneWireless Network extends the process control network into the field seamlessly.

OneWireless Network ensures support for Wi-Fi devices and ISA100 Wireless wireless field devices. Based on the type of coverage required, you can deploy a network with ISA100 Wireless wireless coverage or a network with ISA100 Wireless wireless coverage and Wi-Fi coverage throughout the plant.

The network also provides automatic prioritization of data, ensuring that critical information from wireless field devices is always received with priority. With high-speed and self-organizing mesh network, OneWireless delivers flexible channel allocation and a robust architecture with latency control and redundancy for safe wireless control.

The advantages of implementing the OneWireless Network are:

- Roll-out battery-powered wireless field devices to collect data to improve control strategies or meet regulations at lower costs.
- Empower mobile workforce by providing remote access to process data and other plant-related information.
- Enhance plant security cost effectively by implementing wireless CCTV cameras.
- Improve personnel safety using wireless personnel safety system.
- Connect remote controllers to the central control system.

2.2 ISA100 Wireless compliance

OneWireless Network is compliant with the ISA100 Wireless standard. This standard mandates reliable and secure wireless operation for monitoring, alerting, supervisory control, open loop control, and closed loop control applications. The following table describes the ISA100 Wireless functional roles and the OneWireless components that implement these roles.

Table 1: ISA100 Wireless roles of OneWireless components

Role	OneWireless components	Functional description
IO	XYR 6000 field devices	Entity capable of either providing a measurement value (I) or consuming an actuator command (O).
Router	XYR 6000 field devices and FDAPs	Entity that implements field device routing. An ISA100 Wireless wireless router can self-discover neighboring field devices and form an ISA100 Wireless wireless field device network. An ISA100 Wireless field device can send its own data as well as route data received from the neighboring field devices.
Access Point (Infrastructure)	Cisco Aironet 1552S Access Point	Entity responsible for implementing high bandwidth backhaul using IEEE 802.11a/n WLAN technology. It also functions as infrastructure access point for IEEE 802.11a/b/g/n Wi-Fi clients.
Access Point (Field Device)	FDAP	Entity responsible for the receipt of data packets from the ISA100 Wireless wireless field device network which is routed to the WDM through the IEEE 802.3 LAN and possibly the IEEE 802.11a/b/g WLAN.
System Manager	WDM	Entity responsible for managing all aspects of the ISA100 Wireless wireless field device network including slot allocation, routing algorithms, and address assignment.
Security Manager	WDM	Entity responsible for managing the security of the ISA100 Wireless wireless field device network communication by generating, issuing, and managing security keys, which is essential for all the field devices that are added to the secured network.
Gateway	WDM	Entity responsible for bridging the communication gap between the wired control system protocols and the ISA100 Wireless wireless communication protocol.

ISA100 Wireless ensures interoperability between wireless field devices from different vendors. Existing OneWireless users can migrate from their current infrastructure to an ISA100 Wireless compatible infrastructure.

2.3 Supported OneWireless Network protocols

IEEE 802.11a/b/g/n Wireless Local Area Network

OneWireless Network can be used to provide an industry standard IEEE 802.11 a/b/g/n WLAN. The WLAN is scalable from localized to plant-wide coverage. This enables Wi-Fi coverage in 2.4 GHz ISM band or 5 GHz UNII band.

IEEE 802.11a/ n Wireless Infrastructure Backhaul

OneWireless Network can be used to provide a plant-wide high bandwidth wireless backbone using IEEE 802.11s mesh networking. The backhaul mesh operates in the 5 GHz band.

ISA100 Wireless Wireless Field Device Network

OneWireless Network can be used to provide a standard ISA100 Wireless field device network. The field device network can be used to communicate with ISA100 Wireless compliant field devices, including Honeywell XYR 6000, and other third-party field devices.

IEEE 802.3 Fast and Gigabit Ethernet

OneWireless Network supports 100/10BASE-TX Fast Ethernet and 1000/100/10BASE-T Gigabit Ethernet over CAT5E twisted pair cables and 1000BASE-X Ethernet over fiber optic cable.

2.4 OneWireless Network components

The OneWireless Network consists of the following components.

- Wireless Device Manager
- Field Device Access Point
- Access Point (Cisco 1552S Light Weight Access Point)
- Wireless LAN Controller (Cisco WLC)
- XYR 6000 and other ISA100 Wireless field devices
- Provisioning Device handheld

Wireless Device Manager

The Wireless Device Manager (WDM) is the central management component of a single ISA100 Wireless wireless field device network. The WDM is responsible for the configuration, scheduling, and security of the wireless field device network. OneWireless Network supports integration of ISA100 Wireless data with existing control systems using industry standard protocols such as HART, Modbus TCP, Modbus RTU, and OPC. The WDM hosts the interfaces required to connect the field device data to the control application.

The WDM provides an HTTP-based user interface for configuring and monitoring the devices connected to the ISA100 Wireless network. You do not have to install any software to start using the user interface.

The following are some of the tasks that you can perform using the WDM user interface.

- Generating security keys for device provisioning
- Device configuration
- Network/device monitoring
- Network topology display
- Troubleshooting and routine maintenance

For more information about the tasks that can be performed using the OneWireless user interface, refer to the *Wireless Device Manager User's Guide*.

Field Device Access Point

The Field Device Access Point (FDAP) is an ISA100 Wireless network device that can operate in two modes. As an infrastructure node, it provides connectivity between the WDM and the wireless field device network when connected to the WDM through Ethernet. It can also act as an ISA100 Wireless wireless field router by routing wireless data from ISA100 Wireless field devices and other FDAPs to the WDM. For more information about FDAP, refer to the *Field Device Access Point User's Guide*.

Cisco 1552S Lightweight Access Point

The Cisco 1552S Access Point is an infrastructure node that provides IEEE802.11a/b/g/n WLAN and ISA100 Wireless wireless field device network. For more information about Cisco 1552S AP, refer to the *Cisco 1552S AP User's Guide*.

XYR 6000 and other ISA100 Wireless field devices

The ISA100 Wireless field devices are industrial wireless devices, such as temperature or pressure transmitters. Compatible ISA100 Wireless field devices function as wireless routers to provide connectivity between the wireless field devices. Honeywell offers the XYR 6000 family of ISA100 Wireless field devices. XYR 6000 field devices support wireless field routing.

Provisioning Device handheld

The Provisioning Device handheld is a Personal Digital Assistant (PDA) used to provision FDAPs, Cisco 1552S APs, and field devices on the ISA100 Wireless wireless field device network. The Provisioning Device handheld must have an Infrared (IR) port and run Windows Mobile 5.0 or Windows Mobile 6.5.

3 OneWireless Network planning

Related topics

“Supported network topologies” on page 14

“Planning an ISA100 Wireless field device network” on page 15

“Planning a network with IEEE 802.11a/b/g/n wireless infrastructure” on page 16

“Planning for large networks” on page 18

“Designing the OneWireless Network” on page 21

“Planning for OneWireless Network security” on page 23

“Integrating OneWireless Network with DCS” on page 25

3.1 Supported network topologies

There are different types of network topologies available for the OneWireless Network. The topology diagrams used in this document represents only some of the possible topology variations. You can scale the OneWireless Network topology to accommodate small networks or large networks, according to the requirement.

The following are the different types of network topologies supported by the OneWireless Network.

- Small ISA100 Wireless field device network with field devices as routers.
- Medium ISA100 Wireless field device network with field devices and FDAPs as routers.
- ISA100 Wireless and IEEE 802 a/b/g/n network for multi-applications (wireless field devices, Wi-Fi, and Ethernet devices).

The following tables provide guidance for selecting the network components to deploy a topology of required size and performance.

Table 2: Selecting the Access Point type

Access Point type	Interfaces	Remarks
Cisco 1552S AP	<ul style="list-style-type: none"> • IEEE 802.11a/n (mesh) • IEEE 802.11 a/b/g/n (Wi-Fi access point) • IEEE 802.3 wired Ethernet • ISA100 Wireless field device network 	Use Cisco 1552S AP when deploying a network to provide wireless coverage for IEEE 802.11a/b/g/n Wi-Fi clients, ISA100 Wireless field devices, and Ethernet devices. The Cisco 1552S APs interconnect to form a high bandwidth, IEEE 802.11a/n wireless mesh backhaul.
FDAP as access point	<ul style="list-style-type: none"> • IEEE 802.3 wired Ethernet • ISA100 Wireless field device network 	Use an FDAP when deploying a network to provide wireless coverage for ISA100 Wireless field devices. The FDAP can also be integrated into existing wired Ethernet backhaul. Note that this standalone routing mode is not supported by the Cisco 1552S AP.

FDAP and XYR 6000 field devices can be configured as ISA100 Wireless network routers to route traffic from other field devices. The following table explains the difference in characteristics of the devices, when deployed as a field router.

Table 3: Selecting the router type

Router Type	Characteristics	Remarks
FDAP as router	<ul style="list-style-type: none"> • Line powered • Higher field device capacity • Higher range between field devices and access points 	Preferred in networks with higher performance requirement in terms of faster update rates.
Field device as router	<ul style="list-style-type: none"> • Battery powered • Restricted range between field devices 	<ul style="list-style-type: none"> • Consumes more battery power when functioning as routers. • Supports routing for minimum number of downstream field devices. • Preferred in small and medium size networks with lower performance requirement in terms of slower update rates.

3.2 Planning an ISA100 Wireless field device network

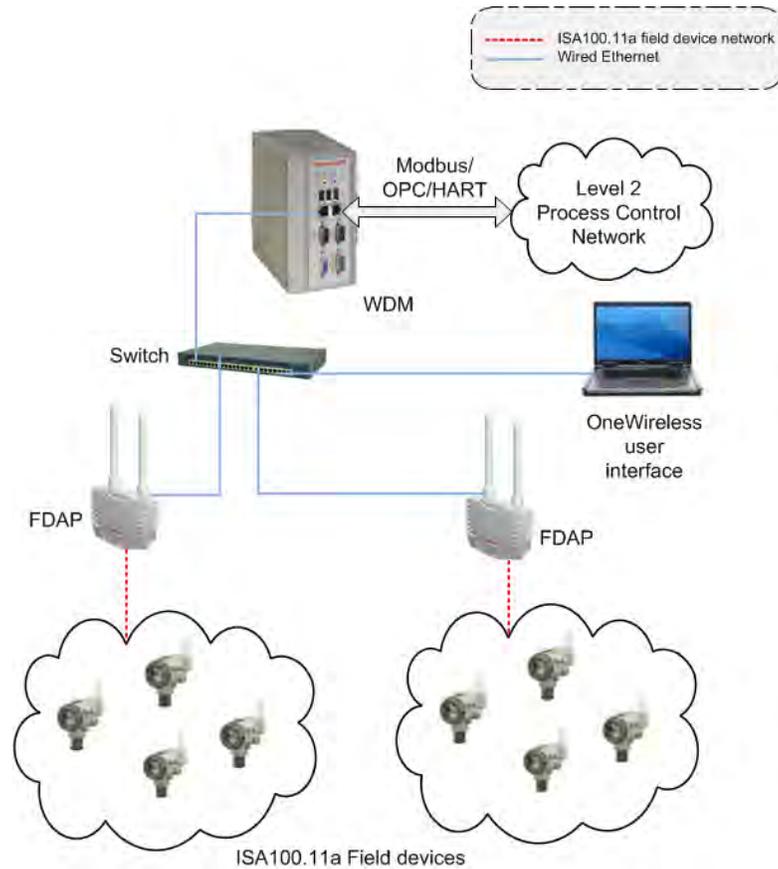


Figure 1: ISA100 Wireless field device network

The above ISA100 Wireless field device network is recommended to be used in small sites that require only few field devices and that do not require an elaborate backbone infrastructure. These small networks are typically used for noncritical monitoring purposes and for systems that do not require fast update rates. The network can be extended to include as many FDAPs as necessary to achieve the desired coverage in the ISA100 Wireless network.

The mandatory components required for implementing a small ISA100 Wireless field device network are the WDM, FDAP, field devices, Provisioning Device handheld, and a desktop or laptop computer with a browser for accessing the OneWireless user interface. An Ethernet switch if required, can be used to connect the WDM to the FDAP. Each field device in the network communicates with other field devices to form an ISA100 Wireless mesh network. They can send data as well as route data received from the neighboring field devices. Data passes through various field devices before reaching the host WDM.

The WDM is connected to the Plant Control Network (PCN) using the PCN port of the WDM and to the ISA100 Wireless wireless field device network using the FDN port. The third-party TCP/IP interface clients (HART, OPC, or Modbus) can be connected to the WDM through the PCN.

3.3 Planning a network with IEEE 802.11a/b/g/n wireless infrastructure

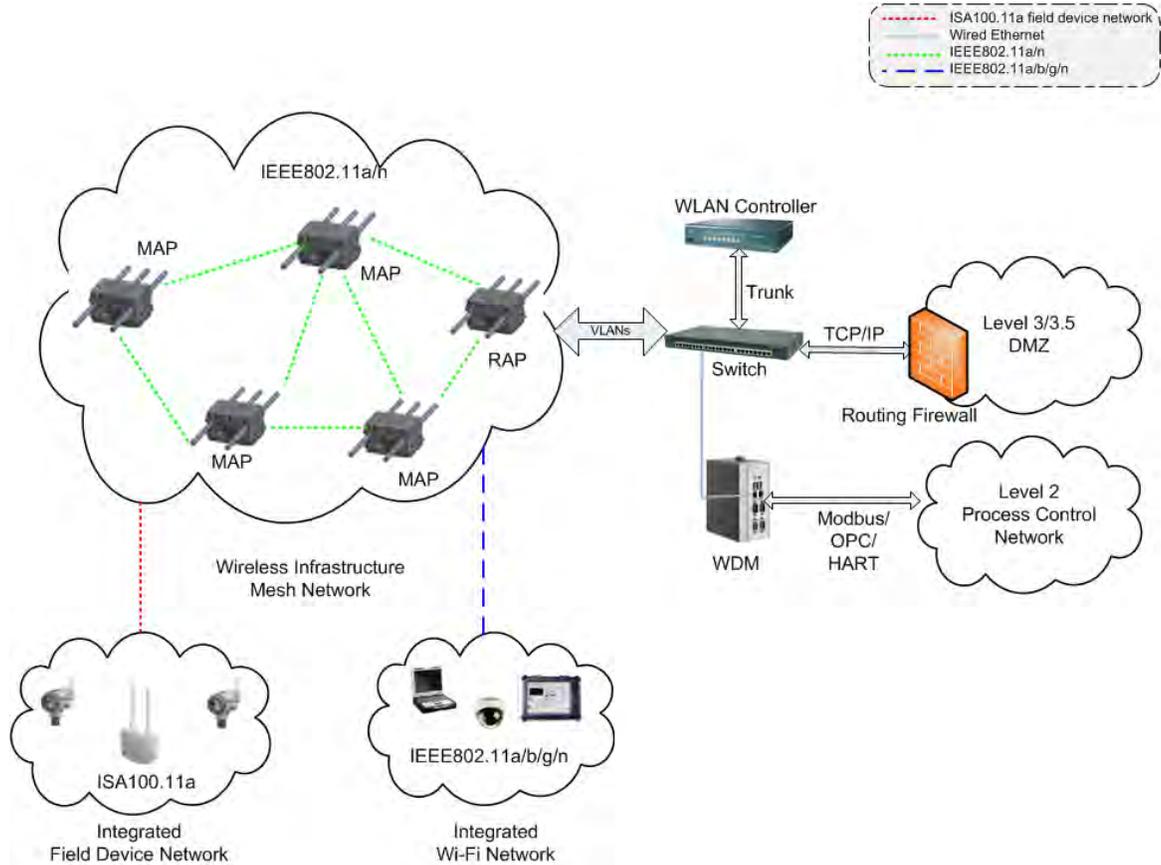


Figure 2: ISA100 Wireless and IEEE 802.11a/b/g network

A combination of ISA100 Wireless and IEEE 802.11a/b/g/n network can be implemented using Cisco 1552 APs, WDM, XYR 6000 transmitters, Wireless LAN Controller, and managed network switch. Optional devices include FDAPs to connect to a cluster of instruments in locations that do not need Wi-Fi coverage and use of Cisco Prime Network Control System (NCS) to manage the Cisco 1552S APs and Cisco wired network devices. This type of network is typically implemented in networks that use handhelds for the mobile workforce, personnel safety, and plant security systems. This topology is also implemented in plants that have hundreds of field devices for monitoring and control purposes.

The following table describes the features and roles of the Wireless LAN Controller, Switches, and Cisco Prime NCS. For more information about WDM, FDAP and XYR 6000, refer to the section “ISA100 Wireless compliance” on page 9.

Table 4: Additional components required for large multifunctional network

Access Point type	Interfaces	Remarks
Cisco Wireless LAN Controller	<ul style="list-style-type: none"> • IEEE 802.3 Fast Ethernet • IEEE 802.3 Gigabit Ethernet • IEEE 802.3af Power Over Ethernet 	<p>Cisco Wireless LAN Controllers are responsible for system wide wireless LAN functions, such as security policies, intrusion prevention, RF management, quality of service (QoS), and mobility.</p> <p>The web-based user interface hosted by Cisco Wireless LAN Controllers can be used to configure and monitor individual controllers and access points.</p> <p>The supported WLCs are the 2500 series and 5500 controllers. Configuration files are available for the 2504 Controller and the 5508 Controller.</p>
Cisco Prime NCS	<ul style="list-style-type: none"> • IEEE 802.3 Fast Ethernet • IEEE 802.3 Gigabit Ethernet 	<p>Cisco Prime NCS is a network appliance for managing, monitoring, and troubleshooting wired and wireless LAN. NCS enables you to configure and monitor one or more controllers, switches, and associated access points. The configuration, performance monitoring, security, fault management, and accounting options of NCS is similar to the options used at the controller level. It also provides a graphical view of multiple controllers and managed access points. It runs on predefined physical appliance and on specific virtual deployments.</p>
Managed network switch	<ul style="list-style-type: none"> • IEEE 802.3 Fast Ethernet • IEEE 802.3 Gigabit Ethernet 	<p>A managed network switch is necessary to support VLAN and trunking between the WLC and the wired network. Configuration files are supported and are available for the Cisco Catalyst 2960 series switches.</p>

3.4 Planning for large networks

The OneWireless Network uses Cisco’s Unified Wireless Network technology and supports standard Cisco configurations and topologies for high availability. This includes using redundant switches, redundant Wireless LAN Controllers, and multiple Root Access Points (RAP) and Mesh Access Points (MAP) to achieve a robust and highly available network. For more information about the topologies and the configurations, refer to Cisco documentation and *Best Practices*. This section provides details about specific topologies and considerations for large networks that require multiple RAPs and WDMs.

The OneWireless Network can be scaled from small networks as described in “Figure 1: ISA100 Wireless field device network” and “Figure 2: ISA100 Wireless and IEEE 802.11a/b/g network” to large networks that comprise hundreds of nodes. To maintain performance and availability, the following practical limits must be observed when deploying such a large system.

Table 5: Planning considerations for deploying large networks

Parameter	Description
RAP to MAP ratio	The recommended RAP to MAP ratio is twenty (20).
802.11 hop count	Each MAP must be within four hops of its RAP for reasonable throughput and latency. The maximum hop count is eight (8).
Multiple WDMs	Multiple WDMs are required when the total number of ISA100 Wireless devices exceed the published WDM capacity.

Multiple RAPs

The RAPs provide high throughput aggregate connection from the wireless network to the plant network. This connection is typically through Gigabit Ethernet or optical fiber connection. As the network size increases and the number of MAPs increase, it is necessary to use multiple RAPs to maintain the required performance and throughput for the wireless network. The recommended RAP to MAP ratio is 20. This means that up to 20 MAPs can share the same primary and secondary RAP.

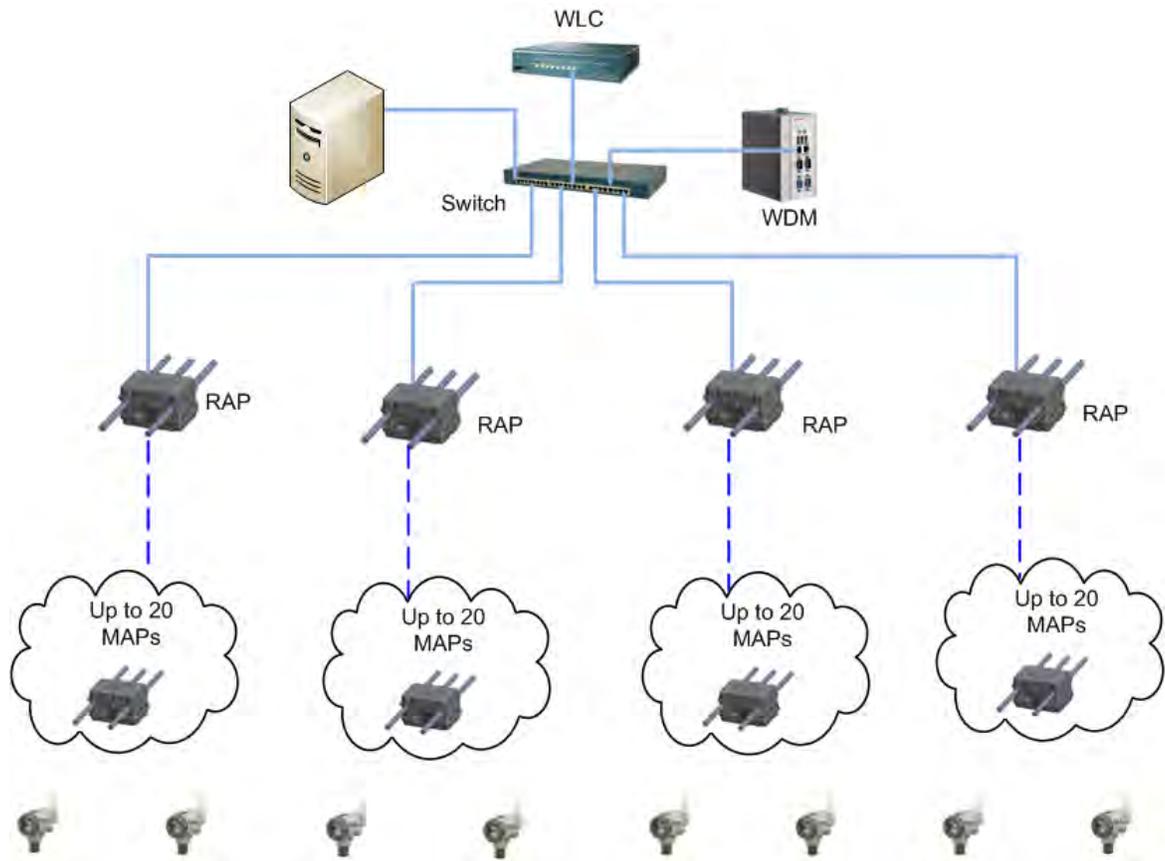


Figure 3: Large network with multiple RAPs

However, the maximum number of hops from the RAP should not exceed four. Although the network can support up to eight hops, exceeding four hops can significantly reduce the available throughput for those links. Devices such as cameras that require high bandwidth must be located within the minimum number of hops possible from the RAP.

Multiple Wireless Device Managers

Each WDM can support a fixed number of ISA100 Wireless devices which include FDAPs, Cisco 1552 APs with integrated ISA100 Wireless backbone, and ISA100 Wireless field devices. Additional WDMs are required if the number of ISA100 Wireless devices exceed the published capacity specification.

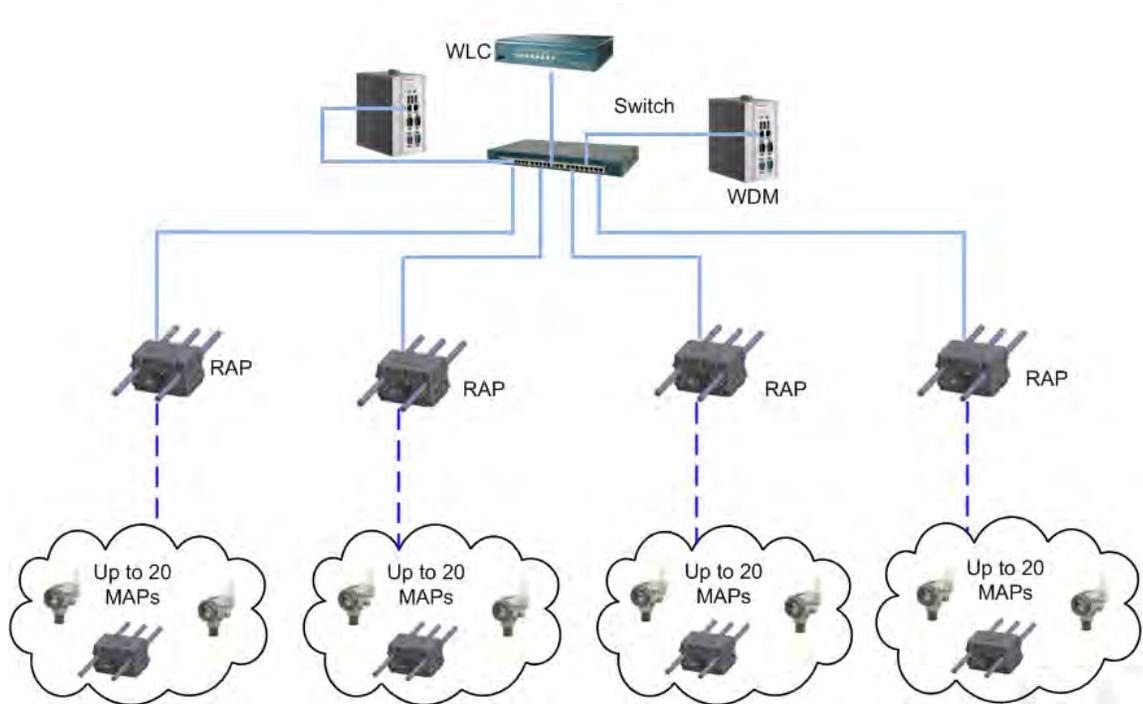


Figure 4: Multiple ISA100 Wireless networks using multiple WDMs and single wireless infrastructure mesh network

As illustrated in “Figure 2: ISA100 Wireless and IEEE 802.11a/b/g network”, multiple ISA100 Wireless networks can share a common IEEE 802.11 wireless infrastructure backbone. The multiple ISA100 Wireless networks are logically separated by provisioning them to use their respective WDMs. Since all the ISA100 Wireless devices are located in a common Layer 2 broadcast domain, any DHCP server on the network is accessible to all the devices. It is recommended to enable DHCP service in only one of the WDMs with address scope wide enough to service all the FDAPs and the ISA100 Wireless backbone devices in the Cisco 1552S AP.



Attention

- Recommend two RAP's per system for better network redundancy.

3.5 Designing the OneWireless Network

Network site planning must be completed to understand how a wireless network can be deployed for your application using the OneWireless Network components. Installing any type of network requires planning to ensure acceptable levels of performance, reliability, and security. Additionally, prior to deploying the OneWireless Network, it is recommended to conduct Radio Frequency (RF) assessment to determine the number and placement of access points that provide adequate network coverage throughout the network.

Planning considerations

The following table highlights some of the planning considerations for the OneWireless Network.

Table 6: Site planning considerations

Network planning
Decide the best system topology, including time synchronization.
Determine the optimal number of Cisco 1552S APs, WDMs, and FDAPs in the network.
Determine the number and distribution of Cisco 1552S APs and their role (MAP/RAP) and WLAN Controller sized to support the infrastructure mesh and Wi-Fi coverage required.
Determine the number and location of network switches, firewalls, and routers and how they can be integrated into the plant network to support the wireless network.
Assess the requirement for network management tools such as the Cisco Prime NCS.
Determine RF power level settings according to the location of deployment.
Physical layout
Position the wireless devices to minimize obstructions between interconnected devices. Maintaining line of sight or near line of sight improves the wireless link performance.
Consider hazardous location requirements.
Security
Restrict access to the Provisioning Device handheld and the WDM.
Use WPA2 and RADIUS authentication for Cisco 1552S APs.
Performance
Limit the number of devices connected between the process network and the WDM to prevent time delays.
Place the wireless devices less than 300 meters from one another. The range varies depending on the environment, line of sight, transmit power settings, antenna type, and antenna gain.
Balance the transmission rate of wireless field devices with the battery life.

Site planning checklist

Use the following checklist for site planning to determine the optimal placement and operating conditions for all the OneWireless devices.

Table 7: Site planning checklist

Consideration
Physical obstacles that can be barriers to proper signal path.
External or internal sources of radio interference.
Hazardous location certifications for each of the wireless field devices (Refer to the field device specific documentation).
Coverage area required for each Cisco 1552S AP/FDAP.

Consideration
Locations of wired network access.
Power access requirements for the Cisco 1552S AP/FDAPs.
Frequency requirements and channel allocation.
Transmit power settings.
Antenna selection.
Antenna mounting and placement requirements.

For more information about Site survey and pre-installation, refer to the *OneWireless Network Planning and Installation Guide*.

RF assessment

The need for an RF assessment depends on the type of network. ISA100 Wireless devices coexist with other wireless devices operating in the 2.4 GHz ISM band. However, it is a good practice to be aware of the site RF spectrum utilization. Honeywell OneWireless Services can perform a comprehensive site assessment to provide a proper representation of your site RF spectrum utilization and minimize interference.

Consider the following while conducting a site assessment.

- Conduct the site assessment when the plant is operating, so that the maximum possible interference is measured and addressed.
- Conduct an RF spectrum analysis on the 2.40-2.483GHz band and 5 GHz band (if available to be used) to detect any potential RF interference. Strong interference sources must be addressed (removed, avoided, or minimized) before the installation. Note that some frequencies may not be available for use in some locations and countries.
- Arrange point-to-point mesh in various locations to measure the RF propagation ability in the site. Received Signal Strength Indicator (RSSI) can serve as an indicator of the RF environment. For Wi-Fi and IEEE 802.11 mesh networks, TCP/IP throughput testing and UDP/IP throughput and packet drop rate testing must be conducted in all the selected locations to measure the quality of the signal strength in the site.
- The ISA100 Wireless radio shares the 2.4 GHz ISM band with the IEEE 802.11b/g radio. The WDM has the capability to exclude certain frequencies from use by the radio. To minimize interference, exclude ISA100 Wireless frequencies that corresponds to the IEEE 802.11b/g channel used by the Wi-Fi network. For more information about how to exclude frequencies, refer to the *WDM User's Guide*.

3.6 Planning for OneWireless Network security

About OneWireless Network security

Wireless networks lack physical security afforded by a set of wires and this is compensated by state of the art cryptographic security that enables node authentication and ensures data privacy and integrity. The following sections explain the security features that are supported by the OneWireless Network.

Embedded WDM firewall

The WDM supports an embedded firewall that inspects the incoming and outgoing data packets and limits access to and from the WDM. The firewall ensures that no routing occurs between the WDM network ports that connect the ISA100 Wireless field device network and the plant control network.

Robust embedded ISA100 Wireless security

To reduce security threats, ISA100 Wireless ensures that all process data is 128-bit encrypted. The data is encrypted at the source and decrypted at the destination to provide end-to-end security for the process data. The FDAPs self-discover other neighboring ISA100 Wireless routing devices, such as Cisco 1552S APs and routing ISA100 Wireless field devices, to form a reliable and secure ISA100 Wireless wireless field device network. ISA100 Wireless security enables the field device network to dynamically re-optimize itself when an FDAP is added to or removed from the network.

Infrared-based security

In addition to data encryption, ISA100 Wireless standard requires all the devices to be authenticated before joining the network. OneWireless Network supports infrared authentication key distribution mechanism. This mechanism is secured since it requires the user to be physically located near the device to authenticate it. The keys are encrypted when distributed over the network.

Key rotation policy

OneWireless Network also supports a key rotation policy to enable a secure network. After transferring the security keys to the devices, the WDM validates the keys and allows the devices to join the network. Once a device joins the network, a master key and a session key are assigned to the device. Following the initial deployment, the session key can be rotated on a periodic basis (key rotation). The key rotation period for the devices can be configured from the OneWireless user interface.

The OneWireless Network follows different security mechanisms for each of the supported network types. Following the security best practices outlined here makes the network as secure as possible, given the state of the art security technology.

ISA100 Wireless field device network security

Wireless field devices operate in a secure mode by default and all the data is cryptographically encoded and authenticated. Perform the following guidelines to maintain a secure sensor network.

- Place the Provisioning Device handheld in a physically secure location and limit the access to authorized installers.
- Erase all the security keys from the Provisioning Device handheld, before storing it to prevent unauthorized use.
- Load the Provisioning Device handheld with adequate number of keys to provision all the devices and set the expiration to a reasonable limit.

IEEE 802.11a/b/g/n WLAN network security

The IEEE 802.11a/b/g/n WLAN utilizes a combination of access control, VLAN, and encryption over Control and Provisioning of Wireless Access Points (CAPWAP) to protect the WLAN network. Cisco 1552S is a lightweight access point for which the configuration and security scheme is controlled by the WLAN controller.

All data from Wi-Fi clients devices using the WLAN mesh are encapsulated with the CAPWAP protocol and transmitted to the WLAN Controller. The WLAN Controller removes the encapsulation and forwards the data to the appropriate consumer over the wired network. Perform the following methods of security to secure the WLAN network.

- Enable MAC address white list on the WLAN Controller to ensure that only authorized Cisco 1552S APs join the IEEE 802.11 mesh network.
- Use VLAN tagging to separate traffic between different Wi-Fi services utilizing the WLAN mesh network. Such traffic from the management VLAN must be separated.
- Enable IEEE 802.1x security for Authentication, Authorization, and Accounting (AAA) in combination with IEEE 802.11i (WPA2) to secure the Wi-Fi client network. The Microsoft version of a RADIUS server is the Internet Authentication Service or IAS, which is available free with Windows Server and is easily added to an active directory domain controller. FreeRADIUS and open source AAA server is also supported by the Cisco WLAN Controller. For more information about network security, refer to the online Cisco documentation for Wireless LAN Controller.

3.7 Integrating OneWireless Network with DCS

The WDM acts as the protocol Server when integrating OneWireless Network with DCS. The following protocols are supported by OneWireless Network for DCS integration – OPC, Modbus TCP and Modbus RTU, and HART. WDM translates ISA100 Wireless protocol to other field protocols. Open system communications supported by the wireless network infrastructure falls into the following categories.

- Data access applications that use OPC clients for data access.
- Controllers that use Modbus for wireless data.
- Asset management applications that use HART interface.

About integrating OneWireless devices using OPC clients

OneWireless Network supports OPC clients such as OPC UA and Classic OPC to provide open system communication to the wireless field device data. OPC server allows an OPC data access client to receive current data from the WDM. An OPC server is an integral part of the data access solution. Configuration, diagnostics, and run-time data provided by wireless devices are available through OPC client.

For more information about configuring OPC, refer to the *Wireless Device Manager User's Guide*.

About integrating OneWireless devices using Modbus TCP and Modbus RTU

When wireless data is used for control, the open system access protocol of choice is Modbus TCP and Modbus RTU. Only process variables and device status are available through Modbus.

The MODBUS TCP is the Transmission Control Protocol/Internet Protocol (TCP/IP) version of the MODBUS protocol. It facilitates communication between devices connected on an Ethernet TCP/IP network based on a client/server model that uses the following two types of messages with standard TCP acknowledge in response to a message.

- MODBUS Request: A message sent on the network by the client to initiate a transaction.
- MODBUS Response : A message sent by the server in response to a client.

For more information about configuring Modbus, refer to the *Wireless Device Manager User's Guide*.

About integrating OneWireless devices using HART

Using HART, OneWireless devices are integrated with asset management systems like Honeywell's Field Device Manager (FDM) and Emerson's AMS Device Manager. OneWireless Network allows asset management systems to interface with OneWireless devices to access the data from the field devices connected to the network. For data transmission between the WDM and the asset management system, OneWireless Network supports Serial communication interface and Ethernet/User Datagram Protocol (UDP) interface.

The serial communication interface establishes RS-232 connection between the WDM and the HART client. This can be achieved by connecting the WDM to the HART client using a serial cable.

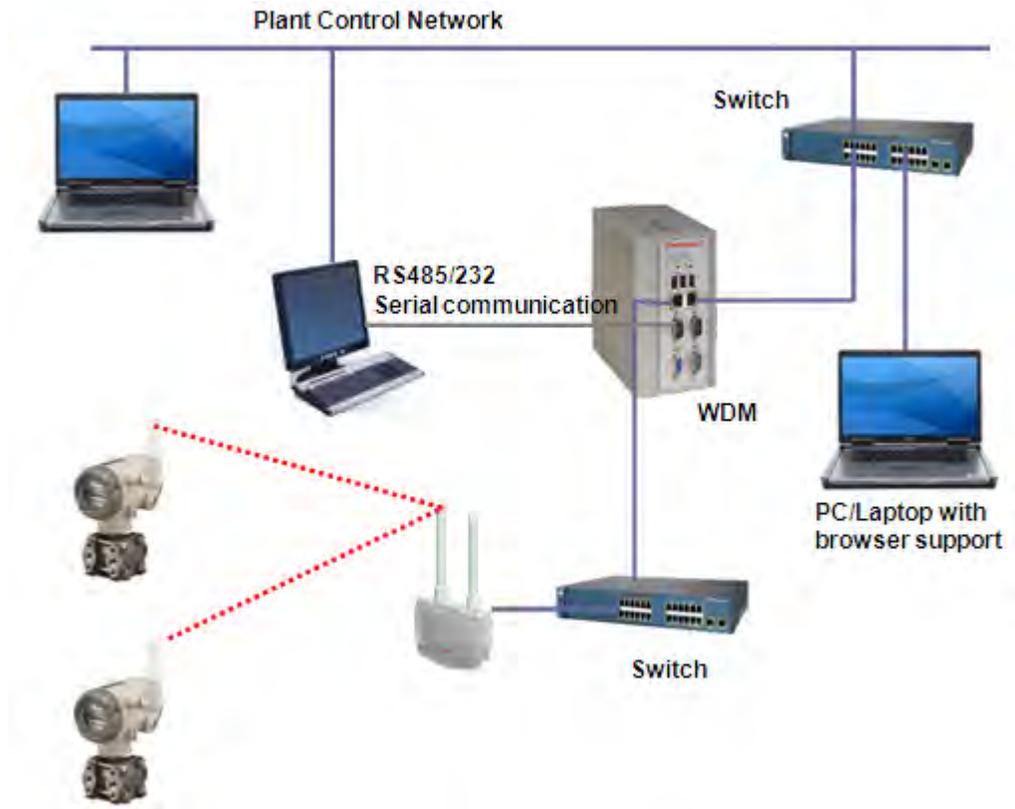


Figure 5: HART Serial communication

Ethernet/UDP interface tunnels the serial communication to UDP packets. Serial communication can be tunneled by using a Lantronix device or serial-to-Ethernet/UDP driver on the asset management system. For more information about configuring HART interfaces, refer to the *Wireless Device Manager User's Guide*.

4 OneWireless components installation

Related topics

“OneWireless system requirements” on page 28

“Installing the OneWireless Network components” on page 29

“Setting up the field devices” on page 30

4.1 OneWireless system requirements

Specifications of WDM

The WDM is an embedded device that is a part of the process control network. It provides two 10/100 Mbps Ethernet ports and three serial ports, of which COM1 and COM2 are used as standard RS232 and RS485 ports. The third port, COM3 is currently not supported.

For detailed information about the technical specifications of the WDM, refer to the *Wireless Device Manager Specifications* document available at Honeywell Process Solutions website.

Specifications of FDAP

For detailed information regarding specifications of FDAP , refer to the respective Specifications documents available at Honeywell Process Solutions website.

Specifications of Cisco 1552S AP

For detailed information about specifications of Cisco 1552S AP, refer to latest specification document available at Cisco website.

Specifications for using the OneWireless user interface

- Desktop or laptop computer installed with any operating system with supported Web browser installed. For more information on supported Web browsers, refer to the *OneWireless Release Notes*.
- Ethernet cable required for wired network access to the WDM
- Ethernet card

4.2 Installing the OneWireless Network components

Install the WDM

For detailed and complete information about installing the WDM, refer to the *Wireless Device Manager User's Guide*.

Install the FDAP

For detailed and complete information about installing the FDAP, refer to the *Field Device Access Point User's Guide*.

Install the Cisco 1552S AP

For detailed and complete information about installing the Cisco 1552 AP, refer to the installation document that is shipped with the Cisco 1552S AP or online specification at Cisco website. For more information about configuring the Cisco 1552S AP for functioning in the OneWireless network, refer to the *OneWireless Wireless LAN Controller Configuration Guide*.

Install the Cisco Wireless LAN Controller

For detailed and complete information about installing the Cisco WLC, refer to the installation document that shipped is with the WLC or refer to the online specification at Cisco website. For more information about configuring the Cisco WLC for functioning along with OneWireless Network, refer to the *OneWireless Wireless LAN Controller Configuration Guide*.

4.3 Setting up the field devices

Connect the batteries

Batteries are installed in the field devices by Honeywell. However, the battery connector power is disconnected before shipping. Hence, you need to reconnect the batteries before installing the field devices. For more information about reconnecting the batteries, refer to the documentation for the respective field devices.

Install the field devices

Installation of field devices involves the following tasks:

- Installing the antenna
- Mounting the device
- Calibrating the device

For detailed information about installing, configuring, and operating the field devices, refer to the user documentation for the specific transmitter.

Detailed instructions for installing, configuring, and operating Honeywell's wireless transmitters are available in the following documents.

- *Quick Start guide* for all the wireless transmitters.
- Specifications for the differential pressure transmitter, absolute pressure transmitter, gauge pressure transmitter, temperature transmitter, HLAI transmitter, and corrosion transmitter.
- User manuals for pressure transmitters, temperature transmitters, HLAI transmitters, and corrosion transmitters.

5 Site survey and pre-installation

Related topics

“Regulatory Compliance” on page 32

“Tools and equipment” on page 33

“Antenna selection and RF output power” on page 34

“Range, coverage, and link budget analysis” on page 36

5.1 Regulatory Compliance

The OneWireless FDAP operates in the 2.4 GHz unlicensed frequency band known as the Industrial Scientific Medical (ISM) band. The Cisco AP operates in both the 2.4 GHz ISM band and the 5 GHz Unlicensed National Information Infrastructure (U-NII) band. Although these bands are unlicensed and available for all to use, you must abide by strict regulatory guidelines published by the Federal Communications Committee (FCC), European Telecommunication Standards Institute, Industry Canada (IC) and other regulatory bodies. The OneWireless Cisco AP and FDAP have published regulatory compliance guidelines (*FDAP Regulatory Compliance Guide and Cisco AP Professional Installation Guide*) that must be followed to ensure compliance in the various regulatory domains.

5.1.1 FCC, IC, and ETSI requirements

To install the FDAP or Cisco AP, you must be familiar with key radio characteristics such as frequency, power, antenna gain, and antenna type to understand the OneWireless Regulatory Compliance Guides. In addition, you must be familiar with regulatory requirements for the operating radios in that region. Most regulatory domains limit the Effective Isotropic Radiated Power (EIRP) for radios operating in the ISM and U-NII bands.

The EIRP is determined by: **EIRP = Conducted RF output + Antenna Gain – Cable and connector losses**

For instance a 16 dBm power setting for an FDAP using a 6 dBi standard integral antenna has an EIRP of 22 dBm (16 dBm + 6 dBi). For more information about maximum EIRP for the approved antenna types and gain, refer to the *OneWireless Regulator Compliance Guides (FDAP Regulatory Compliance Guide and Cisco AP Professional Installation Guide)*.

5.2 Tools and equipment

The following tools are recommended for installation and troubleshooting of OneWireless network:

- Portable RF Power Meter (0 – 6 GHz) for verifying conducted power output
- Portable Vector Signal Analyzer for measuring cable and connector characteristics
- Portable Spectrum Analyzer such as Air Magnet Spectrum XT
- A pair of Binoculars
- Range Finder or scaled map of the site to measure distances
- Portable GPS equipment

5.3 Antenna selection and RF output power

The Cisco AP and FDAP have very flexible selection of antennas and power levels to meet different application and environmental conditions. The antennas include directional and omnidirectional antennas. A careful selection of antenna types, gain, and power settings is required for any successful OneWireless installation and operation. In addition choosing antenna with higher gain than necessary or setting power levels higher than necessary can degrade the network performance by exacerbating multipath fading.

5.3.1 Antenna types

In general directional antennas should be used in applications where covering great distances are more important than broad localized coverage. Omnidirectional antennas should be used where broad localized coverage is desired.

Omnidirectional antennas

Low gain omnidirectional antenna (typically 5 or 6 dBi) are recommend for applications where 360° coverage is necessary such as Wi-Fi access point or field I/O radio that needs connectivity to multiple field devices around it. Higher gain omnidirectional antennas (greater than 8 dBi) offer good compromise between range and coverage. Note that due to the narrow vertical beam width of these antennas the link partners have to be farther away for good connectivity.

Sectorized antennas

Sector antennas come in a variety of gains and beam widths (typically 45° to 180° horizontal beam width). These are recommended for applications where it is necessary to limit coverage to a small region of space. Examples are FDAPs installed at the periphery of a tank farm or a plant. The Cisco 1552 APs do not support remote antennas at this time. Sector antennas, like other directional antennas, are recommended for environments where multipath propagation is prevalent. The high directivity of the antennas serves as a natural rejection of reflected signals that would otherwise reach the receiver and impair communication.

Circularly polarized antennas

These antennas are generally directional and are recommended for severe multipath environments such as enclosed warehouse or other enclosed buildings with multiple reflecting surfaces. The reflecting surfaces may include corrugated metal sheet walls, grated steel floors and ceilings, boilers, pipes, and other metallic process equipment. A circularly polarized antenna naturally rejects multipath signals that arrive out of phase with the direction of circular polarization (right-hand polarized versus left-hand polarized). The downside of these antennas is the theoretical 3 dB reduction of received signal, but this is normally outweighed by its resilience to multipath fading. For more information about circularly polarized antennas that may be used with the FDAP, refer to the *FDAP Regulatory Compliance Guide*.

Antenna diversity

The FDAP supports spatial diversity antennas. These antennas mitigate the effect of fading due to multipath propagation and improve link quality. The integral antennas are spaced for optimum diversity performance. Remote antennas connected to the FDAP must be spaced at least 6 cm apart for improved diversity gain. Spacing the antennas any further does not degrade performance, but it does no add much value to the diversity performance. Directional antennas used in diversity arrangement must point in the same general direction for optimum performance. There is no restriction on the combination of antennas in the spatial diversity arrangement, but performance is limited to the lowest gain antenna.

5.3.2 802.11a/n 5 GHz antennas

The Cisco AP and mesh radios may be configured to use IEEE 802.11a/n in the 5 GHz U-NII and HiperLAN bands. Note that unlike the 2.4 GHz ISM band the U-NII band is much wider (300 MHz) and so it is difficult to optimize a single antenna element for that band. With exception of the dual-band 5 dBi integral antennas that

comes standard with the Cisco AP, most high gain antennas are tuned for operation in a particular U-NII sub-band. When using high gain 802.11a antennas ensure that the antenna selected is rated for the operational sub-band the radio is configured for. The table below displays the available sub-bands within the U-NII/HiperLAN band.

Table 8: 5GHz U-NII / HiperLAN sub-bands

U-NII Sub-Band	Frequency range
U-NII Low (U-NII-1)	5.15 – 5.25 GHz
U-NII Mid (U-NII-2)	5.25 – 5.35 GHz
U-NII Worldwide	5.47 – 5.725 GHz
U-NII Upper (U-NII-3)	5.47 – 5.725 GHz

5.3.3 802.11b/g/n 2.4 GHz antennas

The Cisco AP radio may be configured to use IEEE 802.11b/g/n radio in the 2.4 GHz ISM band and there is generally a single antenna optimized for the entire 83.5 MHz band. Note that the Cisco AP does not support mesh network over 802.11 b/g radio.

5.3.4 ISA 100.11a 2.4 GHz radio antennas

The ISA 100 compliant field I/O radio in the Cisco AP and FDAP operate within the 2.4 GHz ISM band. These radios may be casually referred to as IEEE 802.15.4 radio, DSSS radio, or sensor radio. There is typically a single antenna optimized for the entire band.

5.4 Range, coverage, and link budget analysis

The range for most radio equipment is specified for clear Line Of Site (LOS) conditions. The practical range, however, is dependent on the environment in which the radio is operated. For optimum performance a clear LOS is necessary to reduce the effect of reflection, diffraction, and scattering of the radio waves. During site survey and installation it is necessary to determine the practical range of the radio in the given environment. Various techniques may be employed to determine the useful range of the radio.

5.4.1 Theoretical coverage and range prediction

The theoretical range for FDAPs and Cisco APs are shown in the table below, for some typical antenna and power combinations. This range can be reduced significantly in NLOS conditions. The reduction can be as much as 60% depending on the density and type of obstructions. Multipath fading may contribute additional signal degradation, which reduces the effective range. Due to site variations, any theoretical predictions must always be followed up with empirical prediction.

Table 9: Theoretical range for typical antennas and power combination

ISA100 antenna	Power (dBm)	XYR6000 antenna	LOS range
5 dBi Omni	16	4 dBi Omni	1000 m
6 dBi Omni	16	4 dBi Omni	1200 m
8 dBi Omni	10	4 dBi Omni	> 1500 m

5.4.2 Empirical coverage and range prediction

Empirical range and coverage must be determined as part of the site survey and evaluation. This requires measuring key performance metrics to determine the health and throughput of the wireless links for the intended locations. Some key metrics and their acceptable range are shown in the tables below.

Table 10: Coverage and range prediction metrics for ISA100 Wireless radio

Metric	Acceptable range	Comments
RSSI	-70 dBm to -25 dBm	Including 10 – 15 dB fade margin
RSQI	180 to 255	
TX Fail Ratio	0 to 20	
Communication Redundancy Ratio	90 to 100	

5.4.3 Wireless backhaul data rate

Backhaul is used to create only the wireless connection between the access points. By default, the backhaul interface is 802.11a or 802.11a/n depending upon the access point. The rate selection is important for effective use of the available RF spectrum. The rate can also affect the throughput of client devices, and throughput is an important metric used by industry publications to evaluate vendor devices. Dynamic Rate Adaptation (DRA) introduces a process to estimate optimal transmission rate for packet transmissions. It is important to select rates correctly. If the rate is too high, packet transmissions fail resulting in communication failure. If the rate is too low, the available channel bandwidth is not used, resulting in inferior products, and the potential for catastrophic network congestion and collapse. Data rates also affect the RF coverage and network performance. Lower data rates, for example 6 Mbps, can extend farther from the access point than can higher data rates, for example 300 Mbps. As a result, the data rate affects cell coverage and consequently the number of access points required. Different data rates are achieved by sending a more redundant signal on the wireless link, allowing data to be

easily recovered from noise. The number of symbols sent out for a packet at the 1 Mbps data rate is higher than the number of symbols used for the same packet at 11 Mbps. Therefore, sending data at the lower bit rates takes more time than sending the equivalent data at a higher bit rate, resulting in reduced throughput.

A lower bit rate might allow a greater distance between MAPs, but there are likely to be gaps in the WLAN client coverage, and the capacity of the backhaul network is reduced. An increased bit rate for the backhaul network either requires more MAPs or results in a reduced SNR between MAPs, limiting mesh reliability and interconnection.

! Attention

- The data rate can be set on the backhaul on a per AP basis. It is not a global command.

The required minimum LinkSNR for backhaul links per data rate is shown in the table below.

Table 11: Backhaul data rates and minimum LinkSNR requirements

802.11a data rate (Mbps)	Minimum required linkSNR (dB)
54	31
48	29
36	26
24	22
18	18
12	16
9	15
6	14

6 Hardware installation

Related topics

“Precautions” on page 40

“Antenna isolation” on page 41

“RF power output validation” on page 42

“Power supply options” on page 43

“Protecting and securing installation” on page 44

6.1 Precautions

The following precautions must be observed when handling and installing the OneWireless hardware.

1. Observe electrostatic discharge precautions when handling the antennas or antenna ports on the FDAP and Cisco AP radios. Like most electronic circuits, the sensitive radio receiver circuit could be damaged by ESD induced on the antenna.
2. Handle the FDAP or Cisco AP carefully to prevent dropping of the unit. Dropping could damage the antennas or antenna ports on the units.
3. Do not use the power, data, and RF cable or the antennas as a handle for the FDAP and Cisco AP.

6.2 Antenna isolation

The FDAP and Cisco AP can be installed on a pole or a flat surface such as a wall. When installed on a metal wall ensure that the wall is not within the near field of the antennas. For pole mounting ensure that the pole is not in the near field of the antennas. The device must be mounted such that the antenna is isolated from the mounting pole or other nearby conductive structures. Observe the following precautions with the antennas:

1. With exception of diversity antennas, all antennas must have a minimum of 30 dB of isolation. Antenna isolation can be determined using the path loss equation below. For example, a spacing of 3 ft between the ISA100 radio antennas (2.4 GHz) and other antennas or conductive material is given an isolation of 39 dB.

$$\text{Isolation} = 32.4 + 20 \text{ Log } (D/1000) + 20 \text{ Log}(f),$$

where D is the separation in meters between the antennas, and f is the operating frequency in MHz.

2. There should not be any conductive object in the near field of the antenna. Having such objects in the near field severely distorts the radiation pattern of the antenna and affect its performance. The near field is the radial distance R_{ff} from the antenna.

$$R_{ff} = 2D^2/\lambda,$$

where D is largest dimension of the antenna, λ is the wavelength of the operating frequency.

6.3 RF power output validation

It is recommended to verify RF power output with a power meter during installation. This should be verified after all lightning suppressors and remote cables are in place to ensure the integrity of the RF transmitter. In addition all connectors and center pins must be inspected before installation. For gas discharge tube (GDT) base lightning suppressors, also inspect any screw cap for the GDT capsule to make it is secure to prevent water ingress. These caps are often times loose out of the box.

6.4 Power supply options

FDAP power considerations

The FDAP supports both DC input and AC input without the need for an external junction box. When the AC input is used separate the AC wiring from any low voltage signals such as data cables. Follow the hazardous location wiring method as well as any national and local electrical wiring codes when installing the FDAP. Note that the AC option may not be used in Class I, Division 1 or Zone 0/1 hazardous locations. Refer to the *Cisco Wireless Mesh Access Points, Design and Deployment Guide, Release 7.0, Table 2 for AP power requirements*.

Cisco AP power considerations

The Cisco AP supports both DC input and AC input without the need for an external junction box. Data cable can be terminated using the external Ethernet and console ports. Power termination requires opening enclosure to terminate the field wiring. Follow the hazardous location wiring method as well as any national and local electrical wiring codes when installing the FDAP.

6.5 Protecting and securing installation

A properly installed OneWireless device must be secured and protected from the elements. This is necessary because the FDAP and Cisco AP are typically installed outdoors or in harsh environment. The following sections outline some techniques for protecting the installation.

6.5.1 Surge suppression

It is highly recommended that lightning suppressors are used when the FDAP or Cisco AP is installed outdoors. The antennas, network and power cables are susceptible for electromagnetic energy surge from nearby lightning strokes.

Antenna lightning protection

In general surge protection devices must be as close as possible to the equipment under protection. When only one suppressor is used, it is recommended that the suppressor be an integral type directly connected to the antenna ports on the FDAP or Cisco AP enclosure. Any remote cables can then be connected from the integral lightning suppressor to the remote antenna.



Attention

The FDAP comes with integrated lightning protection that uses a quarter-wave stub to suppress lightning-induced transients. This type of device is recommended over a traditional gas discharge tube (GDT) based suppressor because it is maintenance free and capable of withstanding multiple high energy strikes. When a GDT type suppressor is used, follow recommended maintenance practice to inspect and replace the GDT capsule. The maintenance interval depends on the ratings for the GDT lightning suppressor and the amount of lightning activity expected in the region. Lightning activity map can be obtained from regional weather and climate authorities such as the National Oceanographic and Atmospheric Administration (NOAA) website for the USA.

Power and data cable surge suppression

Power and data runs that go from an FDAP or Cisco AP in the field to lightning-safe areas such as control rooms must have lightning protection at the building entrance as shown in the figure below. This is necessary to prevent lightning transients that are coupled onto the field cables from entering the building and damaging sensitive equipment. Such protection device offers protection to the FDAP or Cisco AP upstream.

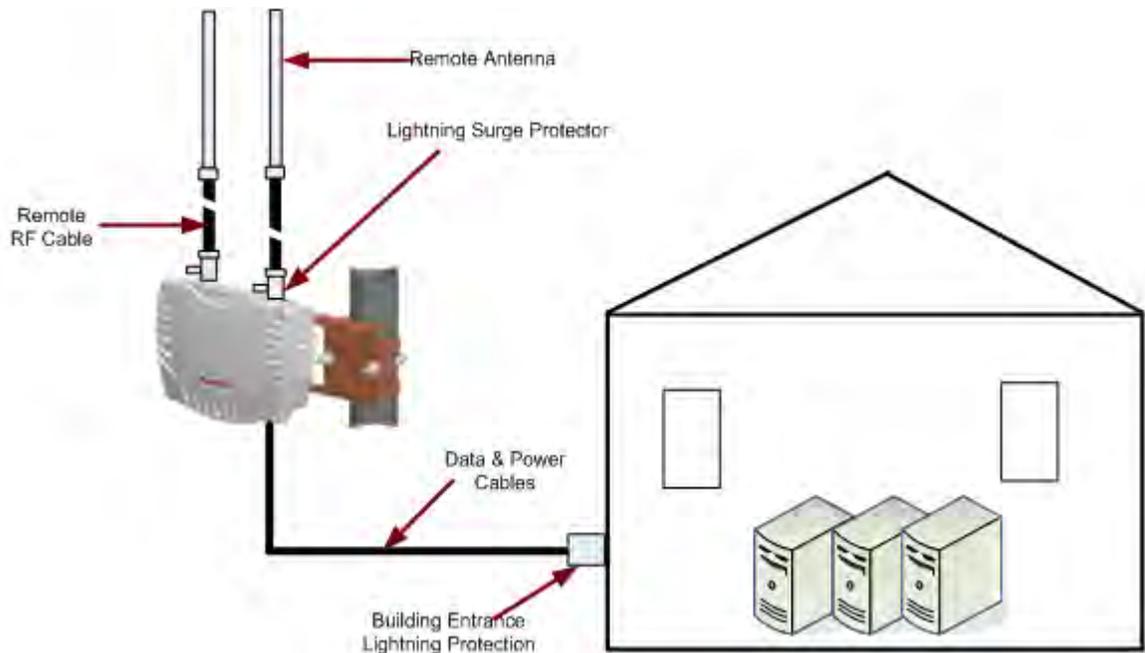


Figure 6: Recommended lightning protection for FDAP

Conduit considerations

The Cisco Aironet 1552S Access Point (1552S AP) typically requires two conduit entrances at the bottom for power and network cables. These conduit entrances are close to the ISA100 radio antennas. The use of metallic rigid conduit running parallel to the antennas can reduce the performance of the ISA100 radio, hence the following precautions must be taken:

- To avoid reducing the ISA100 radio performance, it is recommended that all installations of the 1552S AP use flexible conduit near the ISA100 antennas.
- Ensure that the conduits do not run parallel to the ISA100 radio antennas.

6.5.2 Weatherproofing

The OneWireless Cisco AP and FDAP are housed in rugged die-cast aluminum enclosures that protect the electronics from water and dust ingress. Additional measures must be taken during installation to maintain this ingress protection. The Cisco AP has multiple ports on it used for Ethernet, PoE out, and console. Ensure that all these ports are sealed as well.

Protection from dust, water, and ice

The equipment is dust protected to IP66 and NEMA Type 4X. During installation all entry points must be properly sealed to maintain protection from dust¹, water, and ice.

Table 12: Weatherization of Cisco AP and FDAP connections

Entrance	Recommended action	Typical picture
Conduit Entrance	Apply water tight Teflon tape or other sealing compound to the treaded nipple before screwing to the conduit hub.	Soliciting representative field pictures from OW community.

¹ Dust protection does not include explosive dust-proof protection. The FDAP and Cisco AP must not be installed in environments where such conditions exist.

Entrance	Recommended action	Typical picture
Antenna Port	In addition to the protection offered by the N connector gasket, it is recommended to apply self-amalgamating tape over the antenna connection. Once annealed, this tape provides a protective barrier and prevent water from entering the antenna connection.	Soliciting representative field pictures from OW community.
Unused Antenna Port	Ensure that the protective dust cap is attached to any unused antenna ports. Apply self-amalgamating tape over the seal.	Soliciting representative field pictures from OW community.
Cable Connectors	All cable connectors must be handled similar to antenna port connection by applying self amalgamating tape over the connections.	Soliciting representative field pictures from OW community.

Protection from sun and wind

Use the recommended mounting hardware and secure all cables to protect the device from wind damage after installation. In areas with high temperatures and prolonged sun exposure, install the FDAP or Cisco AP in the shade or use nonmetallic visor to block direct sun rays from reaching the unit to reduce solar loading.

Antennas and cables restraints

Remote mount antennas must be mounted using the recommended mounting hardware to ensure the antenna meets wind survivability ratings. All cables, especially the coaxial RF cables, must be secured with straps so that they do not flap in the wind. Any wind stress on the cable can contribute to premature failure of the connections.

7 System configurations

This section describes frequency planning and allocation for the OneWireless network as well as system configurations such as time synchronization and IP addressing.

Related topics

“Radio frequency considerations” on page 48

“Network redundancy and availability” on page 51

“IP addressing and DHCP considerations” on page 54

“Time synchronization” on page 55

7.1 Radio frequency considerations

As previously noted, the FDAP and Cisco AP operate in the ISM and U-NII bands. Special considerations must be taken to ensure compliance with regulatory requirements and optimum operation within these unlicensed bands.

7.1.1 Cisco AP frequency and operating mode

The Cisco AP mesh radio can be configured as IEEE 802.11a or IEEE 802.11n for operation in the 5 GHz U-NII band. The mesh radio does not support IEEE 802.11b/g or operation in the 2.4 GHz ISM band.

The Wi-Fi radio can be configured for operation in 5 GHz or 2.4 GHz band. However, it is recommended to operate the Wi-Fi in the 2.4GHz band (802.11b/g/n). This separates the high bandwidth mesh backhaul traffic from the 2.4 GHz ISM spectrum used by Wi-Fi client network and the ISA100 field device network. Note that the channels available in 2.4 GHz ISM band and the 5 GHz U-NII depends on the regulatory domain. For instance U-NII-3 channels are not used in ETSI regulatory domains. When the Cisco AP set to a particular country or regulatory domain only channels permitted in that domain are available for selection.

7.1.2 IEEE 802.11a and dynamic frequency selection

The 5 GHz U-NII band is used by civilian and maritime radars, military radars, and weather radars in North America, Europe, Japan and other places around the world. To prevent interference with these radars FCC and ETSI require WLAN radios to monitor the channel for active radar operation. When an active radar signal is detected the WLAN radio must stop using that channel to prevent interference with the radar. This ability to sense and detect radar pattern in conformance with FCC and ETSI regulation is known as Dynamic Frequency Selection (DFS). Transmit Power Control (TPC) is the ability of the WLAN radios in the U-NII band to reduce their power levels to comply with maximum EIRP for individual channels.

The table below displays the 5 GHz U-NII band and the requirement for DFS and TPC in North America and Europe.

Table 13: DFS and TPC requirement for FCC and ETSI regulatory domains

U-NII Sub-band	Frequency range	FCC/IC (NA) DFS and TPC required	ETSI (EU) DFS and TPC required
U-NII Low (U-NII-1)	5.15 - 5.25 GHz	Not available	Not available
U-NII Mid (U-NII-2)	5.25 - 5.35 GHz	DFS comply	DFS comply
U-NII Worldwide	5.47 - 5.725 GHz	DFS comply	DFS comply
U-NII Upper (U-NII-3)	5.725 - 5.825 GHz	DFS not required	DFS not required

All WLAN radios operating in the 5 GHz U-NII band must comply with the DFS and TPC requirements for FCC and ETSI regulatory domains. Japan and a number of other countries have similar regulations. The Cisco AP radio supports DFS and so if it detects radar pattern in the 5 GHz channel it is using, it ceases using that channel for the lockout period mandated by the regulation (currently 30 minutes for FCC/ETSI). This may lead to temporary outage of the mesh network until the channel is clear again or mesh communication is established on an available free channel.

7.1.3 Unlikely sources of DFS-aware radar signals

The ubiquity of radar usage for weather tracking, traffic control, and maritime navigation suggest that the DFS enable channels in the U-NII band may not be suitable or available for use most of the time. However, practical data suggests otherwise as outlined in the following sections.

Weather radars

Weather radars are used around the world to track storms and locate precipitations. The most common type used is Doppler Radar. In the USA the FAA operates the Terminal Doppler Weather Radar (TDWR). These types of radars operate in the C-band and have very narrow beamwidth (1 σ). These radars should not trigger DFS event, because according to the FAA all of these radars, located near major airports, are confined to the 5.6 – 5.65 GHz² range. In addition to the narrow beamwidth, the sweep path and the earth's curvature limit effective range to about 10 miles. This means sites located 20 miles or farther from major airports should have very low probability of encountering DFS events triggered by such radar. Some television stations deploy fixed and mobile weather Doppler radars but these are likely to operate in the same 5.6 – 5.65 GHz range due to suitability of that frequency for weather tracking.

Air traffic control radars

In the USA, the FAA operates hundreds of radar sites for air traffic control. These radars (ASR-9, ASR-11, ARSR-1/2, ARSR-3, ARSR-4, NEXRAD) operate in the S-band (2 – 4 GHz) and does not trigger DFS events.

7.1.4 Likely sources of DFS-aware radar signals

The most likely sources of radar signals that would be encountered during operation in the 5 GHz U-NII band are maritime and military radars. With proper planning the effect of these encounters can be minimized.

Civilian and maritime radars

Civilian and maritime navigation radars are primarily used by sea vessels and so would be encountered near waterways. It is common practice for vessels to turn off their radars or put them in non-transmitting standby mode while docked at port. However, some vessels still leave their radars on turn them on for maintenance or other operational purposes. These radars can trigger DFS events in the Cisco AP.

Military radars

Civilian and maritime navigation radars are primarily used by sea vessels and so would be encountered near waterways. It is common practice for vessels to turn off their radars or put them in non-transmitting standby mode while docked at port. However, some vessels still leave their radars on or turn them on for maintenance or other operational purposes. These radars can trigger DFS events in the Cisco AP.

7.1.5 Field device radio frequency allocation

The OneWireless field devices radios operate in the 2.4GHz ISM band (2.400 – 2.483 GHz). This band is commonly used by many unlicensed radios³ including Wi-Fi (802.11b/g), Bluetooth, Cordless phones, WirelessUSB, and IEEE 802.15.4 based radios such as ZigBee, 6LoWPAN, and ISA100 Wireless. The IEEE 802.15.4 specification divides the ISM band into 16 channels of 5MHz each as shown in the below table.

Table 14: IEEE 802.15.4 channels used by ISA100 radios

2.4 GHz ISM Band	IEEE 802.15.4	
	Channel	Frequency (GHz)
	11	2.405
	12	2.410
	13	2.415
	14	2.420

² The channels in this range are generally excluded from US channels for WLAN radios.

³ The magnetron in a microwave oven operates in this band and can leak about 1 W (30 dBm) of power outside the oven.

15	2.425
16	2.430
17	2.435
18	2.440
19	2.445
20	2.450
21	2.455
22	2.460
23	2.465
24	2.470
25	2.475
26	2.480 – not used

Unlike the IEEE 802.11 radios there are no user selectable channels for the ISA100 field radios. Also, there are no DFS or TPC concerns for this band. However, because of the myriad devices that may use this frequency band, a frequency sweep is necessary during site survey and deployment to determine the level of activity within that band. The field radio uses 13⁴ of the 15 channels in the table above for frequency hopping and retransmission on different channels at different times when there is interference on any particular channel. The bursty nature of radio communication and the use of temporal, frequency, and spatial diversity as well as spread spectrum techniques allow the ISA100 field radio to coexist with other ISM band radios. However, the following precautions are recommended to minimize interference:

1. Identify and disable any unused radio equipment that shares the 2.4 GHz ISM band
2. Use the 5 GHz band (IEEE 802.11a mode) for backhaul mesh network if possible. IEEE 802.11 backhaul network tend to have high bandwidth and duty cycles so operation in the ISM band causes more interference with the ISA100 radio.

⁴ An odd number of frequencies are used to ensure the frequency and time domains are orthogonal. Otherwise frequencies could synchronize with time slots and cause transmission in a given time slot to use the same frequency every time and defeat the diversity gain from frequency hopping.

7.2 Network redundancy and availability

By design mesh networks like the IEEE802.11 mesh and ISA100 mesh used in OneWireless have high availability because of their resilience to node failures. Traffic is automatically re-routed around failed nodes using other available redundant paths. This allows the network to heal itself in the event of a node failure, path obstruction, or interference. To realize this high availability and self-healing, the network must be designed such that each node has redundant path to the upstream network.

7.2.1 IEEE 802.11 network

Each mesh radio unit must have good RF communication link to two or more other Cisco APs. Data is typically routed over one link at a time, but in the event of a link failure the Cisco AP must be able to find an alternative path to the upstream network.

7.2.2 ISA100 network

Each device must have good RF link to more than one FDAP or routing field devices. The network links will resolve to a cut set without forming a close path, but in the event of a link or node failure the device can route data using the available alternative paths or activate new paths.

7.2.3 Cisco WLC redundancy

For high availability network it is recommended to use redundant Cisco WLCs. In a redundant configuration one Cisco WLC is in hot standby and takes control of the network if the primary controller is not available. The switchover causes a relatively short outage of the mesh network (up to several minutes) compared to the time it would typically take to replace a failed Cisco WLC. For details about redundant WLC configuration, refer to the *Table 2 in Wireless LAN Controller (WLC) Configuration Best Practices*.

7.2.4 Root Access Point (RAP) redundancy

For high availability network it is recommended to use redundant RAPs. Using redundant RAPs, eliminates a single point of failure and allows the network to function when one of the RAPs fail. For information about RAP redundancy configuration, refer to the *Cisco Wireless Mesh Access Points, Design and Deployment Guide, Release 7.0, Table 2*.

7.2.5 Mesh convergence time

The Cisco Unified Wireless Mesh Network is a centralized network with the WLAN controller managing the lightweight APs and the mesh network. In the event of a node failure or system restart it can take several minutes for the network to converge and become stable. Some of the factors that affect the mesh convergence time include firmware version, number of neighbors, number of hops to the RAP, signal quality, and available RF channels. To minimize convergence time the recommended ratio of one RAP to 20 MAPs and the 4 hops limit should not be exceeded. When multiple RAPs are deployed for redundancy it is recommended that the RAPs are deployed on the same channel as the primary RAP to minimize convergence time in the event of a RAP failure. In addition, the RAPs should be on the same subnet to minimize convergence time. For more information about mesh convergence time, refer to the *Cisco Wireless Mesh Access Points, Design and Deployment Guide, Table 2*.

7.2.6 Configuring the WDM redundancy

A OneWireless redundant system consists of two identical WDMs, one acts as a primary and the other acts as a secondary (redundant backup). In a redundant system, the secondary is actively linked to the primary (running),

so that it can take control whenever the primary fails or is shut down. The primary and the secondary WDMs are connected to each other through the RDN Ethernet port.

! Attention

- Redundancy is supported only on the WDMX hardware (with three Ethernet ports).

The following are the redundancy features:

- Provides an uninterrupted view to the ISA100 wireless network in the event of a hardware or a software failure.
- Synchronize process data, alarms and events, ISA100 network databases, and WDM configuration in real time.
- Enables transparent switchover with no loss of view to the ISA100 network across all external interfaces.
- Enables you to implement the network topology with no single point of failure, including the network switches. The following figure describes a dual switch network topology without a single point of failure.

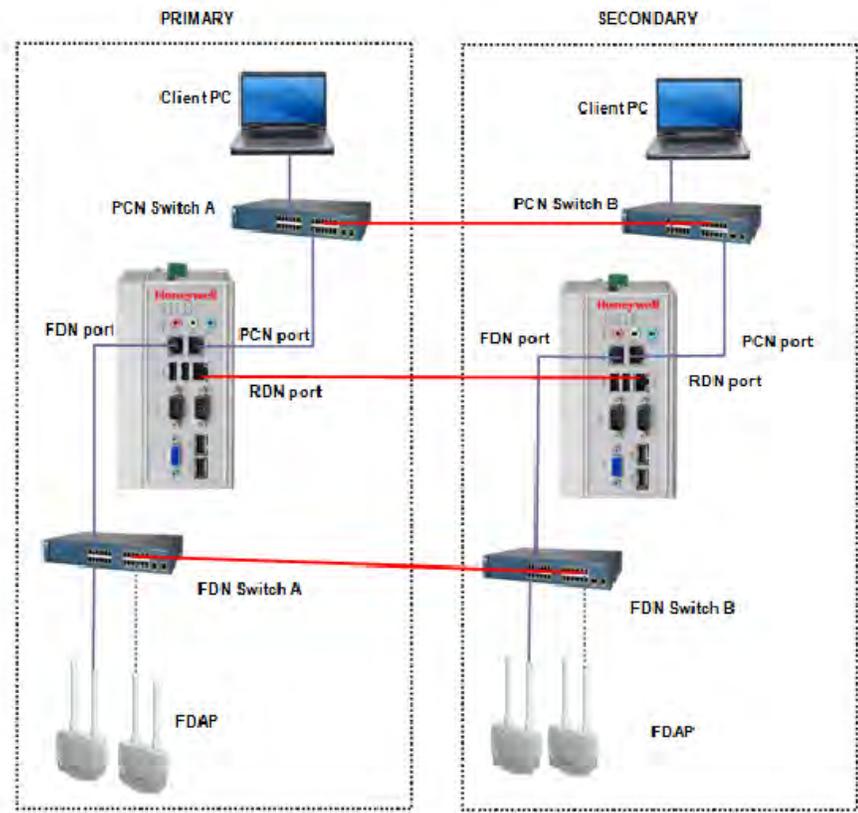


Figure 7: Redundant Network Topology with FDAP

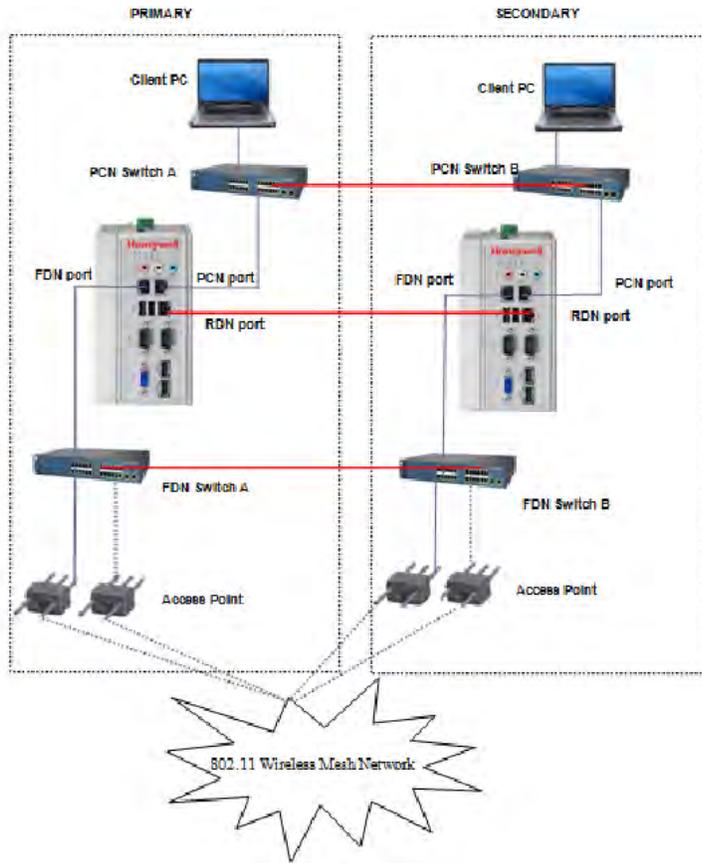


Figure 8: Redundant Network Topology with Access Point

Attention

- Cisco Catalyst 2960 Series 8 port switches and Cisco Catalyst 2960G Series 24 port switches are the supported FDN switches. For more information, refer to the Cisco Catalyst 2960 Series documents.
- For information about the Cisco Access Point configuration, refer to the OneWireless Wireless LAN Controller Configuration Guide.
- You can use a single PCN/single FDN switch or a dual PCN/dual FDN switches. Single switches are used for simple networks, less expensive, possible single point of failure. Dual switches are used for more robust networks, which are more expensive, but do not contain single point of failure.

In case you plan to set up a redundant WDM, ensure the following:

1. CISCO switch port, where the WDM is connected, is configured to operate in access mode.
2. Spanning-tree portfast feature is enabled.
3. Speed is set to auto.
4. Port is in full duplex mode.

For an example of the CISCO switch configuration for WDM port, refer to the OneWireless Migration User's Guide.

7.3 IP addressing and DHCP considerations

The Cisco AP and FDAP are IPv4 devices and so must be assigned valid IP addresses for configuration and normal operation. Because IP address is scarce resource most institutions reserve public addresses for use by endpoints such as PCs and servers that require globally routable IP addresses. The FDAP and Cisco AP can use private IP addresses. This address space, as shown in the table below, is reserved by the Internet Engineering Task Force (IETF) for use in private LANs and frees the user from using assigned public addresses.

Table 15: Private IPv4 address space

Private IP address space	Largest subnet	Number of addresses
10.0.0.0 – 10.255.255.255	10.0.0.0/8 (255.0.0.0)	16,777,216
172.16.0.0 – 172.31.255.255	172.16.0.0/12 (255.240.0.0)	1,048,576
192.168.0.0 – 192.168.255.255	192.168.0.0/16 (255.255.0.0)	65,536

7.3.1 Cisco AP IP addressing

Management of the Cisco AP is performed through the Cisco WLC management interface (web or console). In addition to assigning IP address to the Cisco WLC, the Cisco AP must have IP addresses for proper operation. It is recommended to assign static IP addresses to the Cisco WLC and Cisco AP during initial configuration. Wi-Fi clients must be assigned static IP address. The DHCP server in the Cisco WLC must be disabled to avoid problems and conflict on the network.

7.3.2 FDAP IP addressing

The FDAP needs IP address for normal operation. The FDAP IP address must be assigned dynamically by a DHCP server. Any available DHCP server may be used, but it is recommended to use the DHCP server in the WDM. Ensure that only one DHCP server is available on the FDAP network. If more than one DHCP server has to be used for any reason the address range offered by the DHCP servers must not overlap.

7.4 Time synchronization

Most large networks maintain a coordinated sense of time by using the network time protocol (NTP). Cisco APs can synchronize their internal clocks to be in sync with a user defined NTP server. The configuration of the NTP time sync depends upon the particular customer installation. This section outlines how to configure NTP for OneWireless installation for the IEEE 802.11 mesh network and the ISA 100 network.

7.4.1 Network time synchronization through NTP

Cisco AP NTP setup

The easiest way to use NTP time synchronization is to have the Cisco WLC synchronize directly with the site's time server. One can configure the controller's time server source through the controller's web interface.

Wireless Device Manager NTP setup

NTP settings for ISA 100 network is configured in WDM using the web management interface. The WDM can use its local system time as the time source or point to an external NTP server. To use an external NTP server the necessary ports must be open in any firewall.

7.4.2 ISA radio MAC layer time synchronization

The low level protocol used in the ISA 100 radio communication requires precise time synchronization among all the radio devices. The devices form a hierarchical time synchronization cluster where one device becomes the time sync root. The time distribution tree is built automatically based on the wireless connectivity between the devices. It is therefore possible to end up with separate time sync clusters within the same ISA 100 network as shown in the figure below. This can happen if there is no good RF communication path between the devices in cluster 1 and cluster 2. If the plant layout and device location leads to such separation it is important to augment the separation by lowering RF power output and using directional and lower gain antennas to localize the clusters and prevent devices from bouncing between time sync cluster. In general device can join any time sync cluster and communicate without a problem if there is sufficient signal strength. However, practical observation suggests that it is better to keep devices in a single time sync cluster without bouncing around.

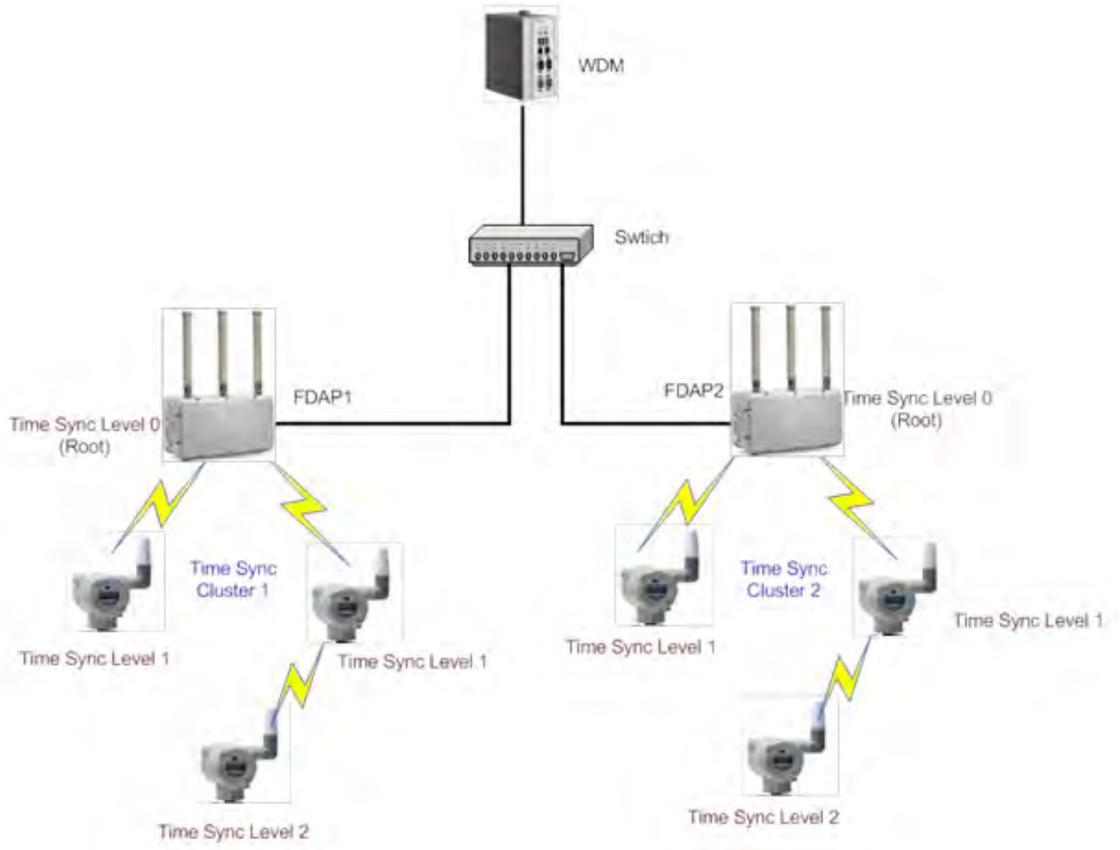


Figure 9: ISA 100 time synchronization clusters

8 Security and network isolation

Wireless networks lack physical security afforded by a set of wires and have to compensate for that by state of the art cryptographic security that enables node authentication, ensures data privacy and integrity. OneWireless network consists of three independent wireless networks with different security mechanisms. Following security best practices outlined here makes the OneWireless network as secure as possible given the state of the art security technology.

Related topics

“ISA100 network security” on page 58

“IEEE 802.11 mesh and Wi-Fi client security” on page 59

“Virtual LAN considerations” on page 60

8.1 ISA100 network security

By default, Wireless field devices operate in a secure mode and all the data is cryptographically encrypted and authenticated. Follow the below mentioned rules to keep the sensor network secure.

1. Keep the provisioning device handheld in a physically secure location and limit the access to authorized installers.
2. Erase all the security keys from the provisioning device handheld, before storing it to prevent unauthorized use.
3. Load the provisioning device handheld with adequate number of keys to provision all the devices and set the expiration to a reasonable limit.

8.2 IEEE 802.11 mesh and Wi-Fi client security

The IEEE 802.11a/b/g/n WLAN uses a combination of access control, VLAN, and encryption over Control and Provisioning of Wireless Access Points (CAPWAP) to protect the WLAN network. Each Cisco 1552S is a lightweight access point, this means that its configuration and security scheme is controlled by the Cisco WLC. All data from Wi-Fi clients and ISA 100 devices using the WLAN mesh are encapsulated with the CAPWAP protocol and sent to the Cisco WLC. The Cisco WLC removes the encapsulation and forwards the data to the appropriate user over the wired network.

Following are available methods of security that must be used to secure the WLAN network.

1. Enable MAC address white list on the Cisco WLC so that only known Cisco 1552S APs can join the IEEE 802.11 mesh network.
2. Use VLAN tagging to separate traffic among different Wi-Fi services utilizing the WLAN mesh network. Separate such traffic from the management VLAN.
3. Enable IEEE 802.1x security for Authentication, Authorization, and Accounting (AAA) in combination with IEEE 802.11i (WPA2) to secure the Wi-Fi client networks. The Microsoft version of a RADIUS server is the Internet Authentication Service (IAS), which is available free with Windows Server and is easily added to an active directory domain controller.

FreeRADIUS, an open source AAA server, is also supported by the Cisco WLC. For additional details about security, refer to the online *Cisco documentation for Wireless LAN Controller*.

8.3 Virtual LAN considerations

It is recommended to enable and use VLANs in the OneWireless network. VLANs allow logical separation of services that use the OneWireless network. In addition to traffic isolation backend, different quality of service levels can be provisioned based on VLANs. The figure below shows an example of how such multiple VLANs may be implemented on the OneWireless network.

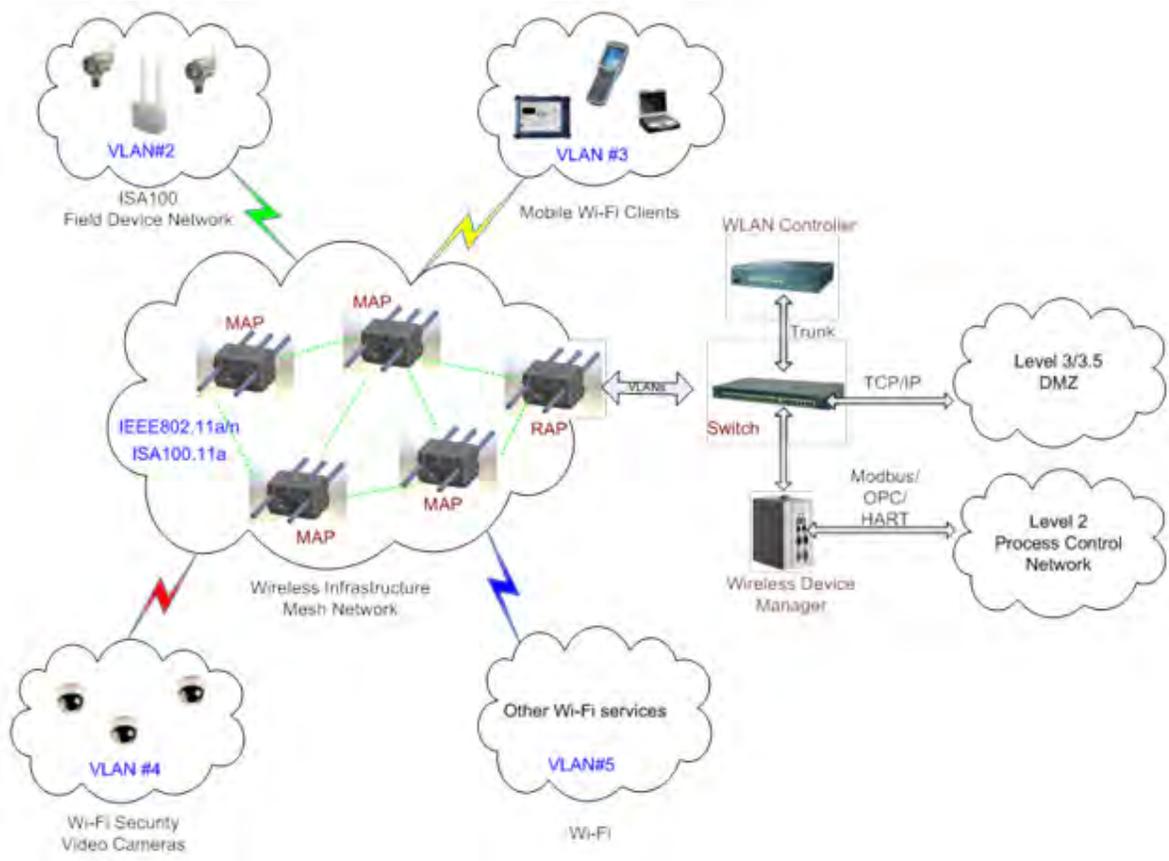


Figure 10: Multiple VLANs on OneWireless Network

9 Performance monitoring

Continuous monitoring and maintenance of the OneWireless network is necessary to ensure the health of the network. OneWireless provides monitoring and management tools for this purpose.

Related topics

“Wireless link quality ” on page 62

“Network management tools” on page 66

9.1 Wireless link quality

Unlike wired communication links, radio communication links are dynamic because they are affected by environmental changes. Changes such as addition of new radios, construction, weather events, and tree foliage are among the many environmental changes that can affect radio communication performance. Continuous monitoring is necessary to ensure optimum operation of the network. Some of the performance metrics to monitor over time are RSSI and RSQI. The OneWireless user interface is the primary monitoring tool for the ISA 100 network.

9.1.1 Configuring Connection Quality Options

Connection quality is based on the Receive Signal Strength Index (RSSI), Receive Signal Quality Index (RSQI), and Transmit Fail Ratio (TxFailRatio). Using the **Connection Status Options**, you can configure thresholds for RSQI, RSSI, and TxFailRatio. The overall quality of an active connection is based on RSQI, RSSI, or TxFailRatio. If RSQI, RSSI, or TxFailRatio is poor, connection quality is poor. Connection quality is displayed as good (green), fair (orange), or poor (red).

To configure connection quality options

- 1 On the top-right of Map view, click **Options > Overlay > Connection Status Options**. The **Connection Status Options** dialog box appears.

Connection Status Options

Ranges can be changed by direct input of new values or dragging the separator bars up and down.

Range	Good (Green)	Fair (Orange)	Poor (Red)
RSQI Range	180 - 255	150 - 180	1 - 150
RSSI Range	-25 - -75	-75 - -85	-85 - -100
Tx Fail Range	0 - 20	20 - 50	50 - 100

Notes:

- The overall quality of a connection reflects the worst-case quality across RSQI, RSSI, and Tx Fail Ratio (as applicable).
- The overall quality of an active connection is based on RSQI, RSSI, and Tx Fail Ratio measurements.
- The overall quality of an inactive connection is based solely on the RSQI measurement.

Buttons: Restore Defaults, Apply, OK, Cancel

- 2 In the boxes near the separator bars, type the RSSI, RSQI, and TxFailRatio values or drag the separator bars up and down.
- 3 Click **Apply**, and then click **OK**.

**Attention**

Click **Restore Defaults** to restore the Honeywell recommended default values.

9.1.2 Verifying connectivity using maps

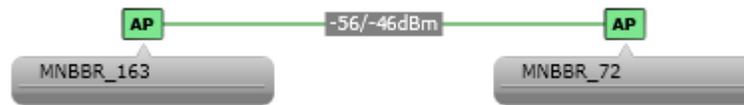
Perform the following steps, to verify mesh connectivity and device connectivity.

To verify mesh connectivity and device connectivity

- 1 Click the **Monitoring** tab to view the map view.
- 2 Visually inspect network topology map and connectivity.
- 3 Navigate to the device in the topology map and check the link signal quality and connectivity.
The RSSI range is displayed in the format -xx/-yy dBm, where -xx and -yy represent the link strength of the devices connected to each other. When the difference between -xx and -yy is less than 5, the lowest of the two values is displayed.

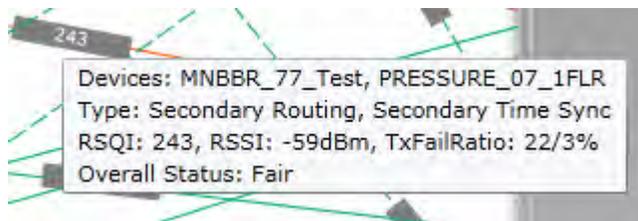
The RSSI range is displayed in the format xx/yy, where xx and yy represent the link quality index of the devices connected to each other. When the difference between xx and yy is less than 10, the highest of the two values is displayed.

For example, in the following illustration, the value -56 represents RSSI of the device (MNBBR_163) and the value -46 represents the RSSI of the device (MNBBR_72).



- 4 Verify device communication statistics information such as RSQI, RSSI, and TxFailRatio.
A green line between the devices in the map view indicates strong signal quality, whereas a red line indicates weak signal quality. A solid line between the devices represents an active connection between the devices and a dotted line represents an inactive connection.

The connection quality details are displayed as tool tip when you hover the mouse over the connection.



Option	Description
RSQI range	235 to 255: Excellent
	180 to 235: Good
	150 to 180: Fair
	0 to 150: Poor
RSSI range	-75 to -25: Good
	-85 to -75: Fair
	-100 to -85: Poor
TxFailRatio	0 to 20: Good
	20 to 50: Fair

Option	Description
You can modify connection quality ranges.	50 to 100: Poor
<p>Attention</p> <ul style="list-style-type: none"> While configuring the network, ensure that the lowest RSQI on each active link is greater than 180 and the lowest RSSI on each active link is greater than -80 dbm. An active link with RSQI/RSSI values higher than the specified values protects the signals when the signal strength/quality degrades due to transient environmental conditions. 	

9.1.3 Generating reports

The OneWireless user interface enables you to generate and view various reports about connectivity, device health, and battery life of the devices in a network.

You can generate and view the following reports:

- **Battery Life:** This report lists all devices that require battery replacement and lists the devices with battery level less than 50%.
- **Device Health Overview:** This report lists all the devices with wireless network disconnection and alarms.
- **Device Summary:** This report provides a summary of each of the device that is configured in the network. The report does not display the details of the devices that are filtered out using the **Filter** option in the ribbon bar.
- **Device History:** This report lists all the device status changes. For example, status change from online to offline device, routing to time synchronization, non-redundant connection to redundant connection.
- **Connection Summary:** This report provides a summary of current status of device connections in the network, redundancy state, and lists all connections with a poor or unacceptable signal strength and quality. The RSQI value when less than 128 results in poor or unacceptable signal quality.
- **Connection History:** This report lists all the history of connection changes. For example, change of RSQI, RSSI, transmit fail ratio.

To view, print, and save the report

- 1 Click the **Reports** tab to view a list of reports.
- 2 In the left pane, click **Reports** and then click the required report.
- 3 Click **Run Report**.

The **Data Preview** pane displays the report.

The following is a sample illustration of the **ConnectivityConnection Summary** report.

Connection Summary
Report Generated By Administrator
9/17/2013 2:25:54 PM

The Connection Summary Report provides information about communications redundancy, and signal strength and quality.

Device Information	Primary Parent	Secondary Parent
Tag Name: MNBRR_81 Type: Access Point Network Address: 3 Redundancy State: Not Applicable Redundancy Ratio: 0	Tag Name: MNBRR_81 Network Address: 3 RSSI: 34 Tx/FallRatio: 0 Overall Status: Good	Tag Name: MNBRR_81 Network Address: 3 RSSI: 34 Tx/FallRatio: 0 Overall Status: Good
Tag Name: MNBRR_S2 Type: Access Point Network Address: 4 Redundancy State: Not Applicable Redundancy Ratio: 0	Tag Name: MNBRR_81 Network Address: 3 RSSI: 255 RSSI: 34 Tx/FallRatio: 0 Overall Status: Good	Tag Name: MNBRR_81 Network Address: 3 RSSI: 255 RSSI: 34 Tx/FallRatio: 0 Overall Status: Good
Tag Name: FDAPS Type: Roaming Network Address: 10 Redundancy State: Redundant Redundancy Ratio: 59	Tag Name: MNBRR_S2 Network Address: 4 RSSI: 154 RSSI: 09 Tx/FallRatio: 60 Overall Status: Poor	Tag Name: MNBRR_81 Network Address: 3 RSSI: 194 RSSI: -00 Tx/FallRatio: -12 Overall Status: Fair
Tag Name: TD_1044 Type: Device, Roaming Network Address: 7 Redundancy State: Redundant Redundancy Ratio: 07	Tag Name: MNBRR_S2 Network Address: 4 RSSI: 231 RSSI: -48 Tx/FallRatio: 12 Overall Status: Good	Tag Name: FDAPS Network Address: 10 RSSI: 202 RSSI: -09 Tx/FallRatio: 08 Overall Status: Fair
Tag Name: MNBRR_81 Network Address: 3 RSSI: 34 Tx/FallRatio: 0 Overall Status: Good	Tag Name: MNBRR_81 Network Address: 3 RSSI: 34 Tx/FallRatio: 0 Overall Status: Good	Tag Name: MNBRR_81 Network Address: 3 RSSI: 34 Tx/FallRatio: 0 Overall Status: Good

- 4 To print the report, click **Print Report**.
- 5 To save the report in .csv format, click **Export As** and save the report to your system.
 - Select the **Include column headers in exported file** check box to include the column headers in the exported file format.

9.2 Network management tools

ISA 100 Network Management Tool

The OneWireless user interface is the primary monitoring tool for the ISA 100 network. The OneWireless user interface displays color coded link state and provides key metrics such as RSSI and RSQI. The OneWireless user interface provides detail channel error statistics that can help to identify any persistent interference or communication problems. The OneWireless user interface can generate connection summary and connection history reports with RSSI, RSQI, and TX Fail Ratio key metrics.

For more information about link quality metrics and reports, refer to the *Wireless Device Manager User's Guide*.

Cisco 1552 Network Management Tool

The Cisco WLC can provide key performance information about the mesh network and allows central management of Cisco APs and connected Wi-Fi clients. For large networks the preferred management tool is the Cisco® Prime Network Control System (NCS). The NCS is a comprehensive management platform for user access and identity management, real-time monitoring of devices, and uses across the entire wireless network. For more information about NCS specification, refer to the NCS data sheet, Table 2.

10 Notices

Other trademarks

Microsoft and SQL Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Trademarks that appear in this document are used only to the benefit of the trademark owner, with no intention of trademark infringement.

Third-party licenses

This product may contain or be derived from materials, including software, of third parties. The third party materials may be subject to licenses, notices, restrictions and obligations imposed by the licensor. The licenses, notices, restrictions and obligations, if any, may be found in the materials accompanying the product, in the documents or files accompanying such third party materials, in a file named `third_party_licenses` on the media containing the product, or at <http://www.honeywell.com/ps/thirdpartylicenses>.

10.1 Documentation feedback

You can find the most up-to-date documents on the Honeywell Process Solutions website at:

<http://www.honeywellprocess.com/>

If you have comments about Honeywell Process Solutions documentation, send your feedback to:

hpsdocs@honeywell.com

Use this email address to provide feedback, or to report errors and omissions in the documentation. For immediate help with a technical problem, contact your local support center.

10.2 How to report a security vulnerability

For the purpose of submission, a security vulnerability is defined as a software defect or weakness that can be exploited to reduce the operational or security capabilities of the software.

Honeywell investigates all reports of security vulnerabilities affecting Honeywell products and services.

To report a potential security vulnerability against any Honeywell product, please follow the instructions at:

<https://honeywell.com/pages/vulnerabilityreporting.aspx>

Submit the requested information to Honeywell using one of the following methods:

- Send an email to security@honeywell.com.
- or
- Contact your local Honeywell Technical Assistance Center (TAC) or support center listed in the “Support and other contacts” section of this document.

