Honeywell

# OneWireless
# Wireless LAN Controller Configuration Guide

OWDOC-X255-en-220A
October 2013

**Release 220**

Honeywell

| Document | Release | Issue | Date |
|---|---|---|---|
| OWDOC-X255-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

This guide provides information about planning, designing, setting up, and configuring a OneWireless Network using WDM, FDAPs, Cisco 1552S APs, and field devices. In addition, provides information about setting up WLC, switch, and Cisco 1552S AP.

### 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 |
|---|---|---|
| *OneWireless Field Device Access Point User's Guide* | OWDOC-X256-en-220A | This document describes the procedures to install, configure, and operate an FDAP. |
| *OneWireless Wireless Device Manager User's Guide* | 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). |
| *OneWireless Network Planning and Installation Guide* | OWDOC-X253-en-220A | This document 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. |

| Document | Document ID | Description |
|---|---|---|
| *OneWireless Migration User's Guide* | OWDOC-X258-en-220A | This document assists you in understanding, planning, and performing the migration of standalone OneWireless Network. |
| *OneWireless Parameter Reference Dictionary* | OWDOC-X260-en-220A | This document provides information about the parameters associated with OneWireless devices. |

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

# 2 Overview of OneWireless Network

**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 Plan and design a OneWireless Network

**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

# 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 | • IEEE 802.11a/n (mesh)<br>• IEEE 802.11 a/b/g/n (Wi-Fi access point)<br>• IEEE 802.3 wired Ethernet<br>• 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 | • IEEE 802.3 wired Ethernet<br>• 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.<br>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 | • Line powered<br>• Higher field device capacity<br>• 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 | • Battery powered<br>• Restricted range between field devices | • Consumes more battery power when functioning as routers.<br>• Supports routing for minimum number of downstream field devices.<br>• 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

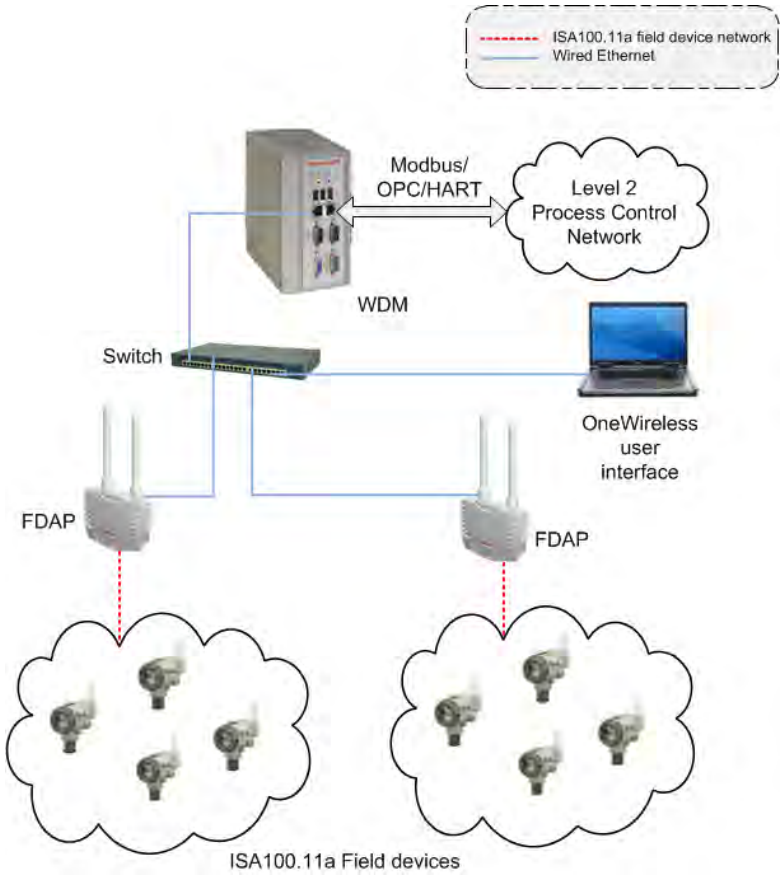



**Figure 1: ISA100 Wireless field device network**

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

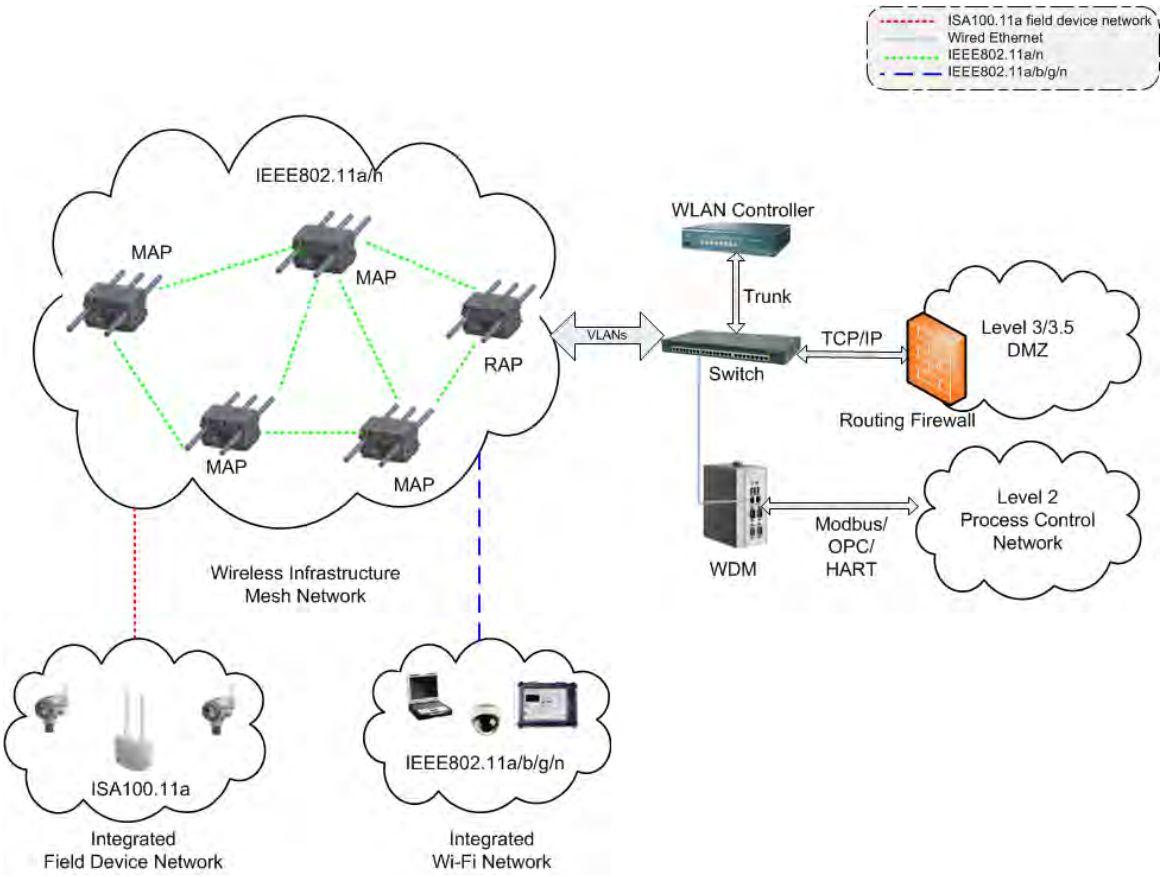



**Figure 2: ISA100 Wireless and IEEE 802.11a/b/g network**

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 | • IEEE 802.3 Fast Ethernet<br>• IEEE 802.3 Gigabit Ethernet<br>• IEEE 802.3af Power Over Ethernet | 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.<br>The web-based user interface hosted by Cisco Wireless LAN Controllers can be used to configure and monitor individual controllers and access points.<br>The supported WLCs are the 2500 series and 5500 controllers. Configuration files are available for the 2504 Controller and the 5508 Controller. |
| Cisco Prime NCS | • IEEE 802.3 Fast Ethernet<br>• IEEE 802.3 Gigabit Ethernet | 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. |
| Managed network switch | • IEEE 802.3 Fast Ethernet<br>• IEEE 802.3 Gigabit Ethernet | 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. |

# 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.

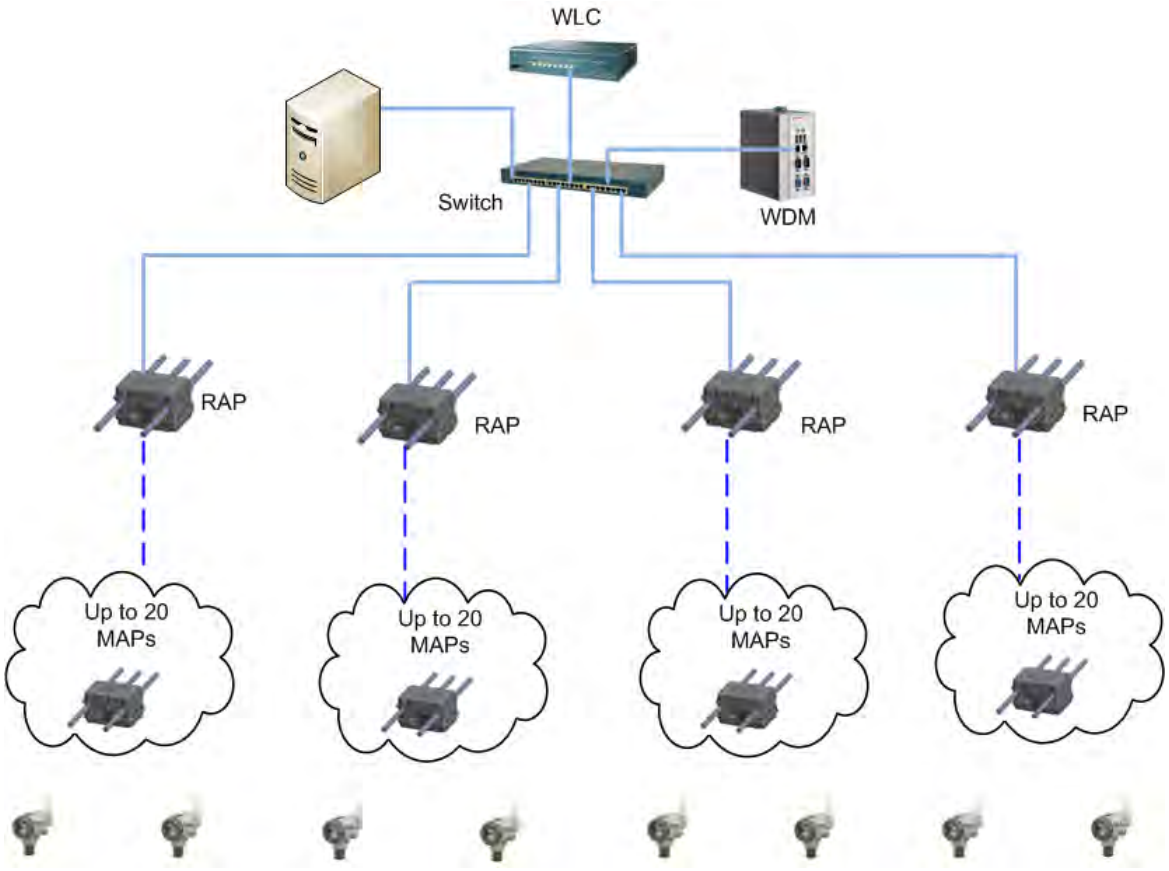



**Figure 3: Large network with multiple RAPs**

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.

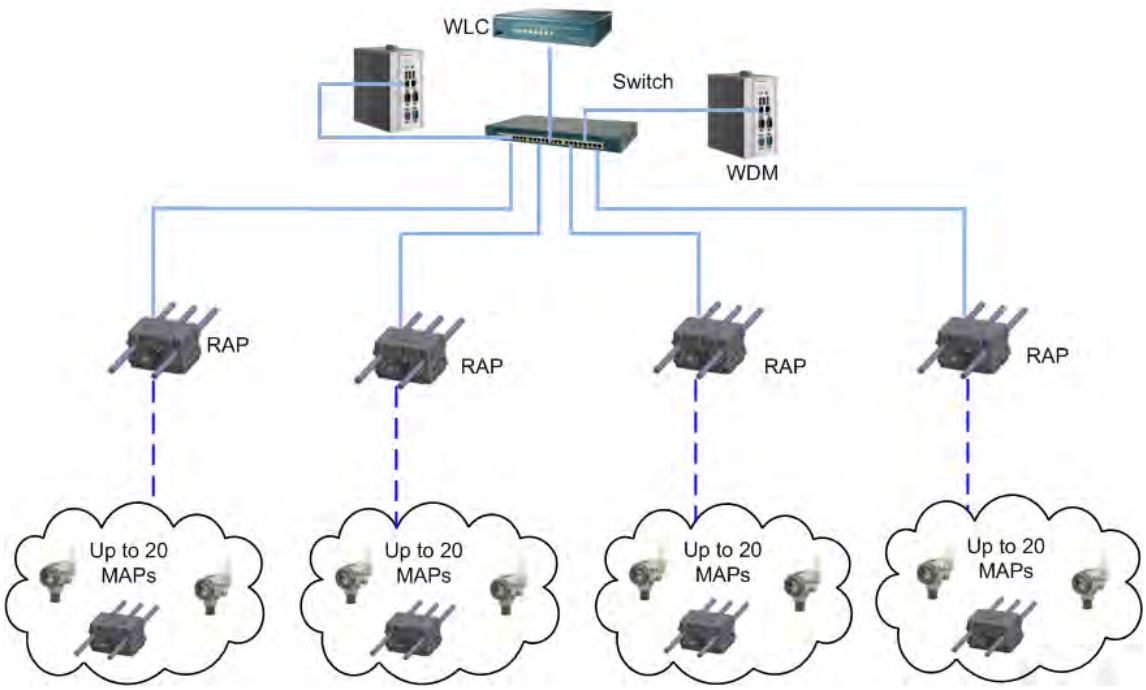



**Figure 4: Multiple ISA100 Wireless networks using multiple WDMs and single wireless infrastructure mesh network**

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 is128-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.

# 4 Deploy OneWireless Network

**Related topics**

“OneWireless system requirements” on page 26
“Installing the OneWireless Network components” on page 27
“Setting up the field devices” on page 28
“Configuring OneWireless Network” on page 29
“Setting up WLC, switch, and Cisco 1552S AP” on page 33

# 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 Ethernet interfaces that are used to connect to the Field Device Network (FDN) and Process Control Network (PCN). RS232 and RS485 serial interfaces are also available to support communication of serial protocol such as serial Modbus.

For detailed information about the technical specifications of the WDM, refer to the *Wireless Device Manager Specification* document available at Honeywell Online Support website.

### Specifications of FDAP

For detailed information about the technical specifications of the FDAP, refer to the *FDAP Specifications* document available at Honeywell Online Support 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 latest *OneWireless Release Notes*.
- Available Ethernet port on the desktop or laptop computer.
- Ethernet cable required for wired network access to the WDM.

# 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.

# 4.4 Configuring OneWireless Network

**Related topics**

“Configuring network switch and VLAN” on page 29
“Understanding the DHCP configuration requirements” on page 30
“Configuring the Wireless LAN Controller ” on page 31
“Configuring Cisco 1552S AP” on page 31
“High level guidelines for changing the configuration files” on page 31
“Provisioning the OneWireless devices” on page 32

## 4.4.1 Configuring network switch and VLAN

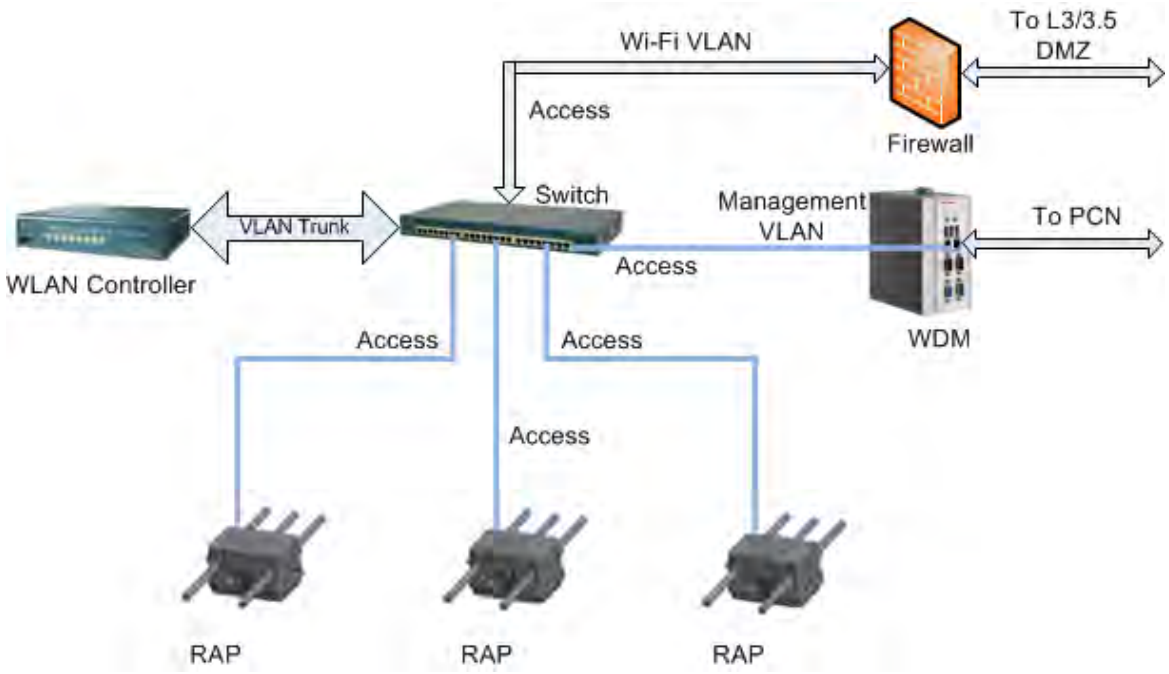



**Figure 5: Switch configuration for ISA100 Wireless/Cisco WLAN integrated network**

The network switch that interconnects the WLAN Controller, WDM, and the Cisco 1552 RAP must be a managed switch that supports IEEE 802.1Q VLAN tagging such as the Cisco Catalyst 2900 series. The Figure 6 and the Table 8 illustrates how the devices interconnect. VLAN trunking must be enabled between the switch and the WLAN Controller. The RAP and the WDM ports on the switch must be configured as standard VLAN access ports for the respective VLAN IDs. Wi-Fi clients and other services using the WLAN mesh infrastructure must be assigned to separate VLANs. This logically separates the ISA100 Wireless traffic routed to the WDM from the Wi-Fi traffic. All the other ports on the switch can be configured as VLAN access ports for other Wi-Fi enabled services or can be left untagged.

**Attention**

The VLANs that are used to separate the traffic cannot be used as security barriers, hence the guests or other untrusted user traffic should not be permitted on the network. Separate APs should be set up in the areas where this traffic is required and should be routed through the appropriate security level network.

**Table 8: Switch port configuration**

| Port<br>According to the configuration file provided the port numbers are as suggested below | Switch interface | Configuration |
|---|---|---|
| Gigabit port (according to the configuration file provided) or any other port of your choice. Depending on the switch version the configuration file changes. | From port 1 of WLC | VLAN Trunk |
| 1<br>Port for connection to Level 3 and 3.5 DMZ | Firewall for level 3/3.5 DMZ | VLAN Access Port<br>Different VLAN other than 2, according to the examples provided in the configuration file. |
| 2<br>According to the configuration file provided | WDM | VLAN Access (must be the same VLAN ID identified for the ISA100 traffic.)<br>You must configure the WDM port as spanning-tree port fast. For redundant WDM, you must configure two ports of the switch as spanning-tree port fast.<br>According to the configuration file example, VLAN = 2. |
| 3<br>3 and onwards depending upon ports available | RAPs | VLAN Access Port<br>According to the configuration file example, VLAN = 2. |
| Others | Others | VLAN or untagged, depending on the requirement |

A reference configuration file for the 8- or 24-port Cisco Catalyst 2960 switch is available. The configuration can be applied directly or modified to meet specific requirements for the network.

## 4.4.2 Understanding the DHCP configuration requirements

On startup, the ISA100 Wireless Backbone Router (BBR) in the Cisco 1552S AP must obtain the IP address from the WDM through the Dynamic Host Configuration Protocol (DHCP). The WDM has an internal DHCP server that is used for this purpose and must be enabled. To prevent network problems in the OneWireless Network, the DHCP server in the Cisco WLAN Controller must be disabled and there must be no other DHCP server available on the same broadcast domain. The WDM is the endpoint of TCP/IP traffic from the BBR and is completely isolated from all the other IP networks. This means a non-routable IP address range can be used for WDM and BBRs without expending the corporate assigned IP address range. A list of available private network addresses is available in the following table. WLAN devices including the Cisco WLAN Controller, Cisco 1552S AP, and all Wi-Fi clients must be assigned static IP addresses that are in different subnets than the DHCP server in the WDM.

**Table 9: Available private network IP addresses**

| IP address range | CIDR Subnet Mask | Number of addresses | Remarks |
|---|---|---|---|
| 10.0.0.0 – 10.255.255.255 | 255.0.0.0 | 16,777,216 | Single Class A |
| 172.16.0.0 – 172.31.255.255 | 255.240.0.0 | 1,048,576 | 16 Contiguous Class Bs |
| 192.168.0.0 – 192.168.255.255 | 255.255.255.0 | 65,536 | 256 Contiguous Class C |

### 4.4.3 Configuring the Wireless LAN Controller

The WLAN Controller requires an initial configuration to setup and configure additional settings for both primary and secondary controllers. For more information about the tasks that are required for the basic configuration of the WLAN Controller, refer to the section “Configuring Hyperterminal” on page 33. After the basic configuration is complete, additional configurations can be applied based on the application need. Refer to “Table 10: OneWireless configuration files” on page 31 for a list of configuration files available. These configuration files can be edited to meet application and network requirements and then can be applied to the controller.

### 4.4.4 Configuring Cisco 1552S AP

The Cisco 1552S AP is a lightweight access point and it obtains the configurations and firmware updates from the WLAN Controller. However, a basic configuration directly on the Cisco 1552S AP is necessary for the initial configuration. This requires connecting to the console port on the Cisco 1552S AP and setting up some initial configuration parameters. Typical configuration information needed for the initial setup is provided in the files listed in “Table 10: OneWireless configuration files” on page 31.

### 4.4.5 High level guidelines for changing the configuration files

The Cisco WLC, 1552S AP, and Switch can be configured by using the sample configuration files. The table below provides some high level guidelines for changing the configuration files according to your site configuration. The exact steps with commands and the sequence of performing the configuration is provided in the section “Configuring WLC, switch, and Cisco 1552S AP” on page 34.

**Attention**

You can download the configuration files from http://www.honeywellprocess.com web site. The current released version of the configuration files is Version 7.

Log on to the http://www.honeywellprocess.com, and then copy paste the below links in the Address bar of the browser window.

www.honeywellprocess.com/library/support/software-downloads/Experion/Configuration_files_Version7_5500_Controller.zip .

www.honeywellprocess.com/library/support/software-downloads/Experion/Configuration_files_Version7_2504_Controller.zip .

**Table 10: OneWireless configuration files**

| File name | Purpose | Remarks |
|---|---|---|
| overallWLCConfig.txt | Base configuration for WLC. | Bootstrap configuration<br>Ensure that names used are unique and the same name is used in all other files. Add the name and MAC address of RAPs and MAPs. If required, advanced users can change interface and WLAN configuration and assignments. |
| overallWLCSecConfig.txt | Base configuration for secondary WLC, if used. | This file is optional if redundant WLCs are used. The secondary name must be unique and the IP address must be edited in the RAPConfig and MAPConfig files, if redundant WLC is used. Secondary configuration lines must be deleted from these files if there is no redundancy requirement. |
| RAPConfig.txt | Base RAP configuration. | Use multiple RAP configurations if multiple bridging groups are available. Change new name of RAPs, modify the old name (with MAC address), specify correct name and IP address of primary and secondary WLC. If secondary WLC is not present, remove the corresponding line. |

| File name | Purpose | Remarks |
|---|---|---|
| RAPBridgingConfig.txt | Sets up bridging in RAPs. | Add/edit individual sections for each bridge group/RAP. If there is more than one RAP device, add all the RAP devices to the same configuration file. |
| MAPConfig.txt | Base MAP configuration. | Include all MAP MAC addresses by replicating configuration. Ensure that there are no duplicates available after editing. Change new name of MAPs, modify the old name (with MAC address), specify correct name and IP address of primary and secondary WLC. If secondary WLC is not present, remove the corresponding line. If there is more than one MAP device, add all the MAP devices to the same configuration file. |
| MAPBridgingConfig.txt | Sets up bridging in MAPs | Add/edit individual sections for each bridge group/MAP. Set correct bridge group name that you have configured earlier. Also, change the name of MAPs according to the new name. |

**Attention**

- Ensure that the configuration files contain correct information and does not contain any blank lines, typos, or other extraneous characters.
- Ensure that all the devices are in the factory default state. Any equipment that is not in this state must be returned to this state. For more information about restoring the device to the factory default state, refer to the Cisco documentation.
- Ensure that you add all the MAP device data to the same configuration file, in a similar manner.

### 4.4.6 Provisioning the OneWireless devices

Firstly, the Cisco Mesh network must be up and running, the WDM must be connected and initial configuration must be completed and then you can start provisioning the devices. Firstly, the RAPs must be provisioned, then the MAPs. Best practice is to provision XYR 6000 or field devices after the APs and FDAPs are provisioned.

FDAPs/Wireless Infrastructure Node/field devices must be securely provisioned before adding them to the OneWireless Network. Provisioning involves the process of downloading the security keys from the WDM to the Provisioning Device handheld and then transferring them to the FDAPs, Wireless Infrastructure Node, or field devices through their Infrared (IR) ports. In addition, from OneWireless R210 release onwards, over the air provisioning is supported. This allows the devices to join the secure OneWireless Network and establish communication with other devices and the WDM.

For more information about provisioning OneWireless Network components, refer to the *WDM User's Guide*.

# 4.5 Setting up WLC, switch, and Cisco 1552S AP

The following are the initial configuration commands issued to the Cisco wireless controller through the serial port using Windows HyperTerminal. The instructions are based on the user interface and the capabilities of Windows HyperTerminal.

Windows HyperTerminal is available from Honeywell for configuring network equipment. Other terminal emulators with similar capabilities can also be used.

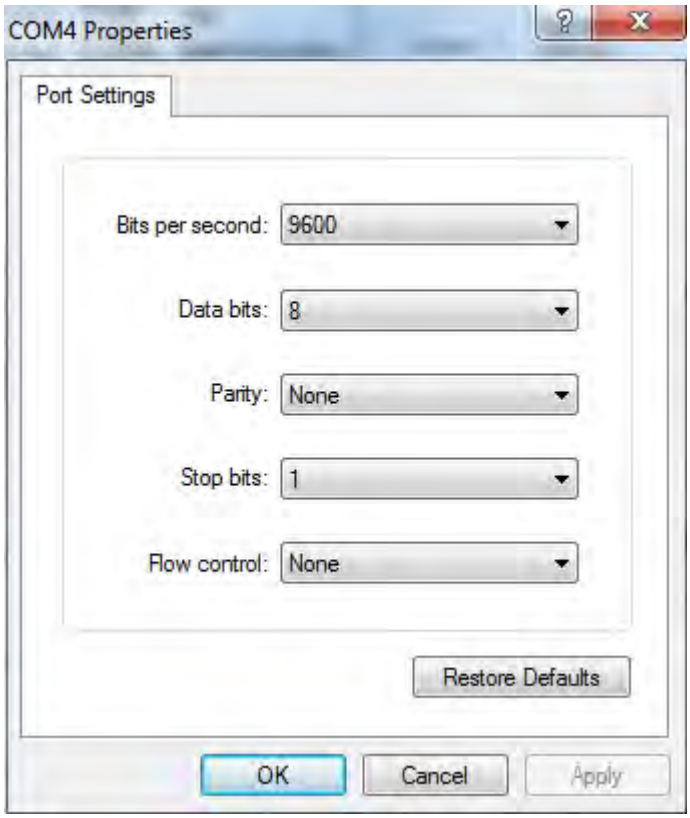
**Prerequisites**

- Ensure that the configuration files contain correct information and do not contain any blank lines, typos, or other extraneous characters.
- Ensure that all the devices are in the factory default state. Any equipment that is not in this state must be returned to this state. For more information about restoring the device to the factory default state, refer to the Cisco documentation.

## 4.5.1 Configuring Hyperterminal

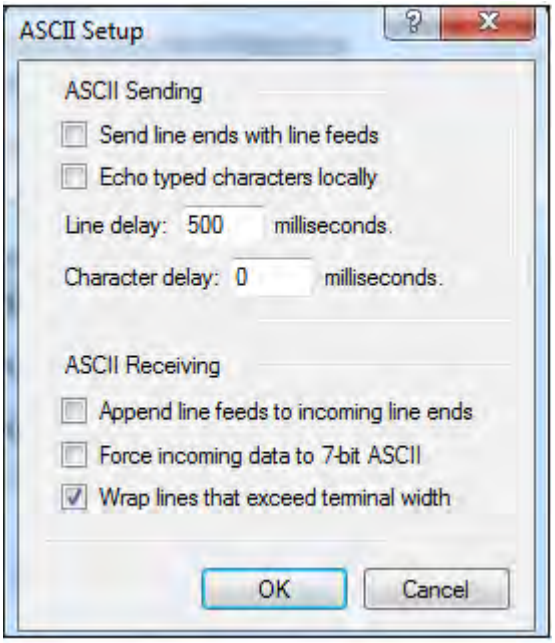
**Hyperterminal configuration to connect WLC, switch, and Cisco 1552S AP**

- Ensure that Windows HyperTerminal is configured with the following settings.
  a Set the COM port properties as follows:
    - Bits per second – 9600
    - Data bits – 8
    - Parity – None
    - Stop bits – 1
    - Flow control – None



b Set the **ASCII Setup** properties as follows:

1. Choose **File** > **Properties** and then click the **Settings** tab.
2. Click **ASCII Setup** and set the **Line delay** as 500 milliseconds.




3. Click **OK** to close the **ASCII Setup** dialog box.

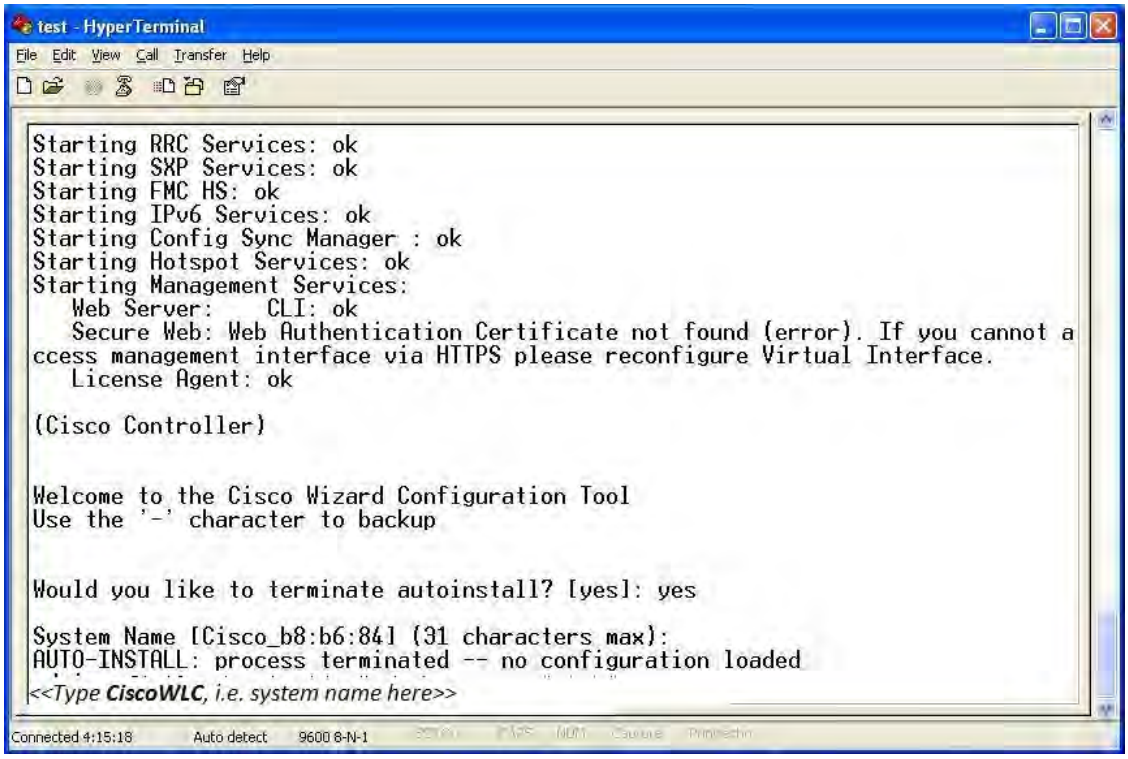
## 4.5.2 Configuring WLC, switch, and Cisco 1552S AP

### To configure WLC

1 Power on the primary Cisco Wireless LAN Controller and perform the following steps to configure the controllers and the access points.

> **Attention**
> The example configuration provided here is applicable only for 2504 model of the WLC.

The bold text indicates a user variable that you need to configure. Lines without bold phase at the end indicate a place where the user presses the **Enter** key. For an incorrect entry, the cursor (-) moves one line backwards.




Would you like to terminate auto install? [YES][no]: **YES.**

A message appears as *AUTO-INSTALL: process terminated -- no configuration loaded*

System Name [Cisco_f4:f0:40] (31 characters max): **CiscoWLC (CiscoSecondaryWLC** if configuring a redundant WLC )

Enter Administrative User Name (24 characters max): **admin**

Enter Administrative Password (3 to 24 characters): **Honeywell@**

Re-enter Administrative Password : **Honeywell@**

Management Interface IP Address: **10.0.1.105** (**10.0.1.107** for secondary)

Provide an IP, which is of different network address series as that of FDN. For example, if FDN is 192.168.0.1 then management IP can be 10.0.1.X (X = host address, for example, 105). If you want to use the same network address series as that of FDN, then care must be taken to avoid IP address conflict.

Management Interface Netmask: **255.255.255.0**

Management Interface Default Router: **10.0.1.1**

Management Interface VLAN Identifier (0 = untagged): **2**

Management Interface Port Num [1 to 8]: **1**

Management Interface DHCP Server IP Address: **10.0.1.105**

This IP address can be same as Management interface IP address. Some of the new WLC firmware, you might have to enter the Multicast IP address: **225.0.0.0** or any other address according to your network configuration.

Virtual Gateway IP Address: **1.1.1.1**

Mobility/RF Group Name: **Wrigley**

Network Name (SSID): **CiscoMesh**

Configure DHCP Bridging Mode [yes][NO]:

```
Allow Static IP Addresses [YES][no]:

Configure a RADIUS Server now? [YES][no]: no
Warning! The default WLAN security policy requires a RADIUS server. See documentation for more
details.

Enter Country Code list (enter 'help' for a list of countries) [US]:
```

Please enter your country code. This country code is used by 802.11a/n radio. If you have ordered the APs for US, then just press enter, default is US. Otherwise, type help and enter proper country code.

```
Enable 802.11b Network [YES][no]:

Enable 802.11a Network [YES][no]:

Enable 802.11g Network [YES][no]:

Enable Auto-RF [YES][no]:

Configure a NTP server now? [YES][no]: no

Configure the system time now? [YES][no]:

Enter the date in MM/DD/YY format: 08/30/11Enter the time in HH:MM:SS format: 10:47:30
```

After completing the configuration data entry the following message displays.

```
Configuration correct? If yes, system will save it and reset. [yes][NO]:
```

2 Type **Yes** and press **Enter**.
The following message displays.

```
Configuration saved! Resetting system with new configuration... Configuration saved! Resetting
system with new configuration...
```

Initial configuration of WLC is complete.

**To configure switch**

3 Configure the switch. For more information, refer to “Configuring network switch and VLAN” on page 29. You can modify and use either *Wrigley_mst_2960_8 or Wrigley_mst_2960_24*; that is 8 or 24 port switch, respectively provided along with the configuration files. The WLC, Switch, and RAP must be interconnected. WLC must be connected to Trunk port of the Switch.
Cisco WLC can be accessed through https://10.0.1.105 for primary WLC or https://10.0.1.107 for secondary WLC. If you have changed the primary and secondary WLC IP address then use the same. You need to provide the same username - admin and password - Honeywell@.


If you are able to access the above login page of Cisco WLC, then the basic configuration of Cisco WLC and Cisco Switch along with VLAN is correctly completed.

**To configure 1552S Root Access Point (RAP) and Mesh Access Point (MAP)**

4 Open Console port blind and connect the console cable to the 1552S Access Point. Configure the static IP address using a Cisco serial configuration cable (the blue cable) using the following steps.

a Type **RETURN** and press **Enter**.

If an error message `%CAPWAP-3-ERRORLOG: Not sending discovery request AP does not have an Ip !!` or similar appears, ignore it and continue typing.

b User access verification:

`Username: cisco`

Note this is similar for all the factory default configurations.

`Password: Cisco`

Note this is similar for all the factory default configurations.

`AP1234.5678.9abc> ena` .

`Password: Cisco`

Note that this is similar for all the factory default configurations.

`AP1234.5678.9abc# capwap ap ip address 10.0.1.112 255.255.255.0`

Provide the IP address in the same network series as that of WLC management IP address - 10.0.1.X. (where X = a different host address) The warning messages might come, but ignore them and continue typing.

`AP1234.5678.9abc# capwap ap ip default-gateway 10.0.1.105`

Provide the WLC IP address or default gateway address.

`AP1234.5678.9abc# capwap ap controller ip address 10.0.1.105`

If you have single non-redundant controller then follow the above step. If you have redundant controller then, type **`capwap ap primary-base 10.0.1.105`** for the primary WLC IP address and then type **`capwap ap secondary-base 10.0.1.107`** for the secondary WLC IP address.

The AP configuration is complete. If you have multiple APs, then configure them in similar way.

5 Repeat step 4 for additional APs. Unique static IP address must be provided for each APs.

**WLC configuration continued**

6 Startup the Cisco Wireless LAN Controller and ensure that the startup operation is complete.

7 Using hyper terminal or similar tool, log on to WLC.

8 Enter the admin username and password.

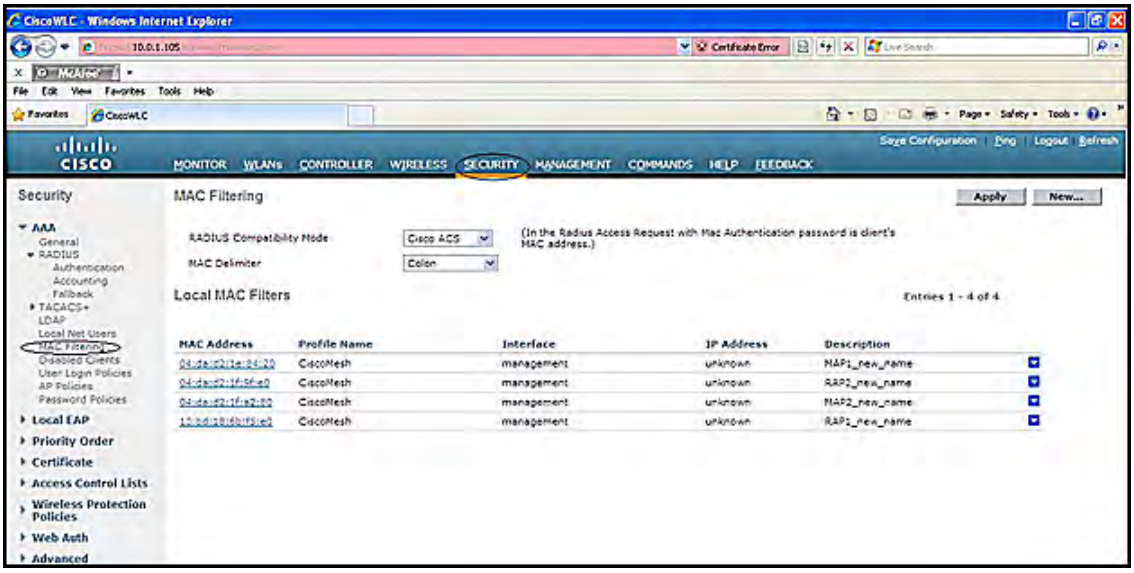
9 Edit the *`overallWLCConfig.txt`* text file to add the MAC addresses of the RAPs and MAPs, under the MAC address filtering. This enables only the mentioned MAC addresses to join the WLC network.

10 To configure MAC address filtering and name of the access point, modify the command **`config macfilter add a8:b1:d4:d4:b5:00 1 management RAP1_new_name`**.

11 In the Windows HyperTerminal, choose **Transfer > Send Text File**. Then browse and open the file that you have modified based on *`overallWLCConfig.txt`*.

12 When complete, verify for any error messages and debug. Verify for typos, if errors are encountered. Ignore any warnings for the default configuration items that are already configured. In case of any errors, correct the errors, and then resend the file.

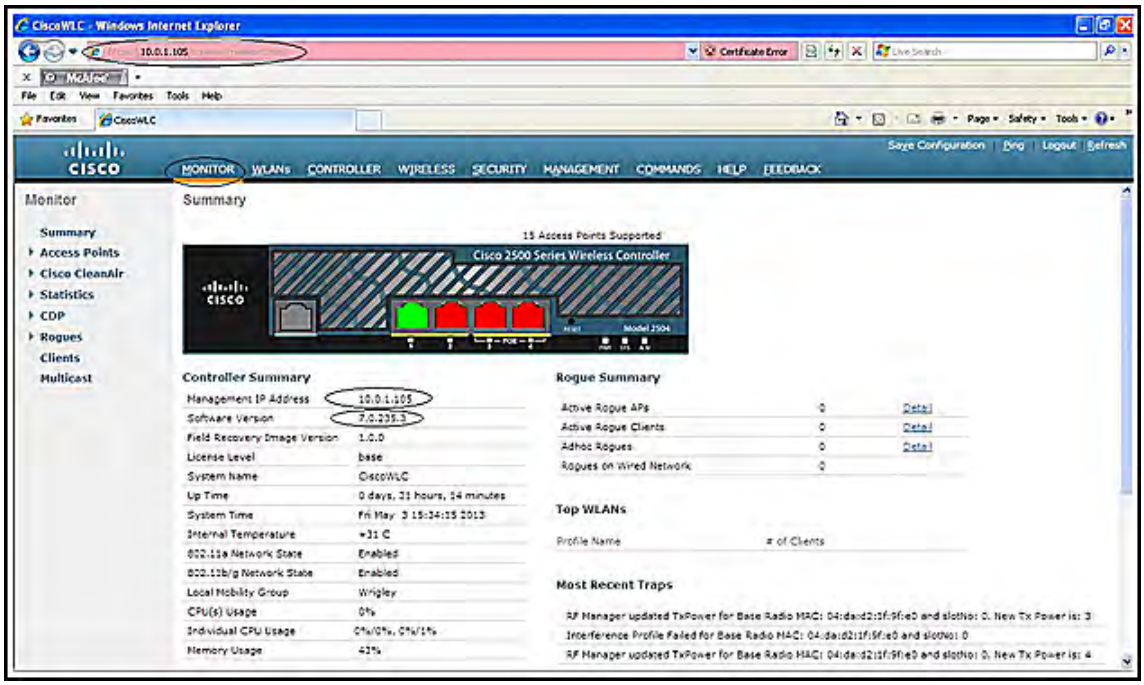
From the Cisco web GUI, MAC address filtering can be also added.




**Attention**

In case you want to change the Cisco WLC software then you have to use either ftp or tftp application to download Honeywell compatible WLC software. For more information about WLC software upgrade, refer to Cisco documentation available in the link http://www.cisco.com/en/US/tech/tk722/tk809/technologies_configuration_example09186a00805f381f.shtml.

From the Cisco web GUI, you can verify the current WLC software.




If WLC software and 1552S software are not similar then Cisco 1552S AP might not join over mesh, but will join if connected to switch. If the 1552S AP is connected to the switch where the WLC is connected and the AP ID is already configured then AP will be automatically updated to the same software that of WLC.

13 If you perform the changes directly in the WLC CLI, then to save the configuration, type **`save config`** in the WLC CLI and press **`Enter`**.

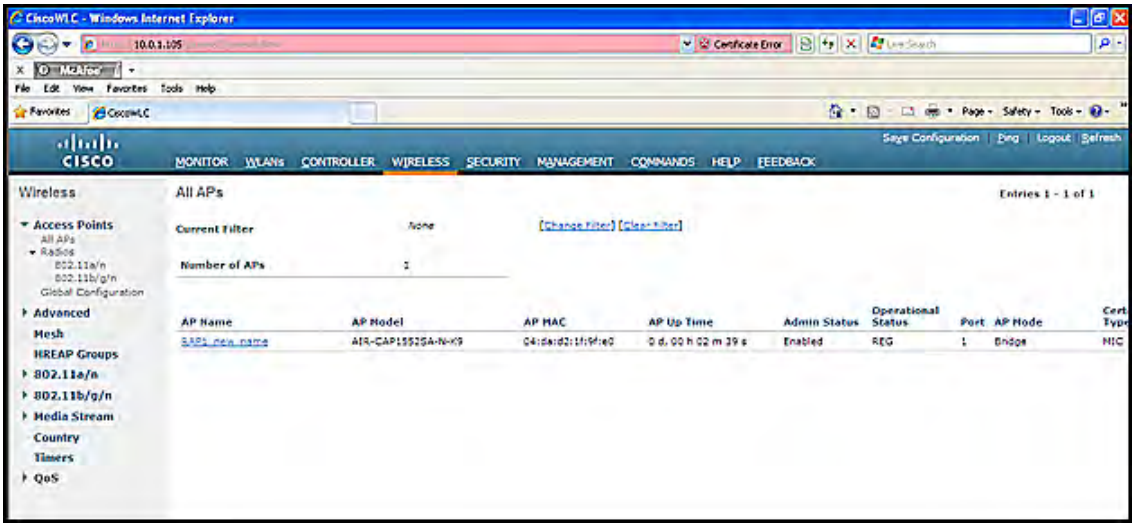
14 Connect RAP to the non-trunk port of the switch. For more information, refer to “Table 8: Switch port configuration”.

15 Power on the RAPs.

After 5 to 15 minutes, the RAPs join the controller. The time is a function of whether the AP and the controller contain the matching firmware version. The controller loads the APs if the firmware does not match.

16 In WLC CLI command prompt, type the command **`show ap join stats summary all`** to verify if the RAP has joined WLC system.

From the Cisco web GUI, you can monitor the joined status.

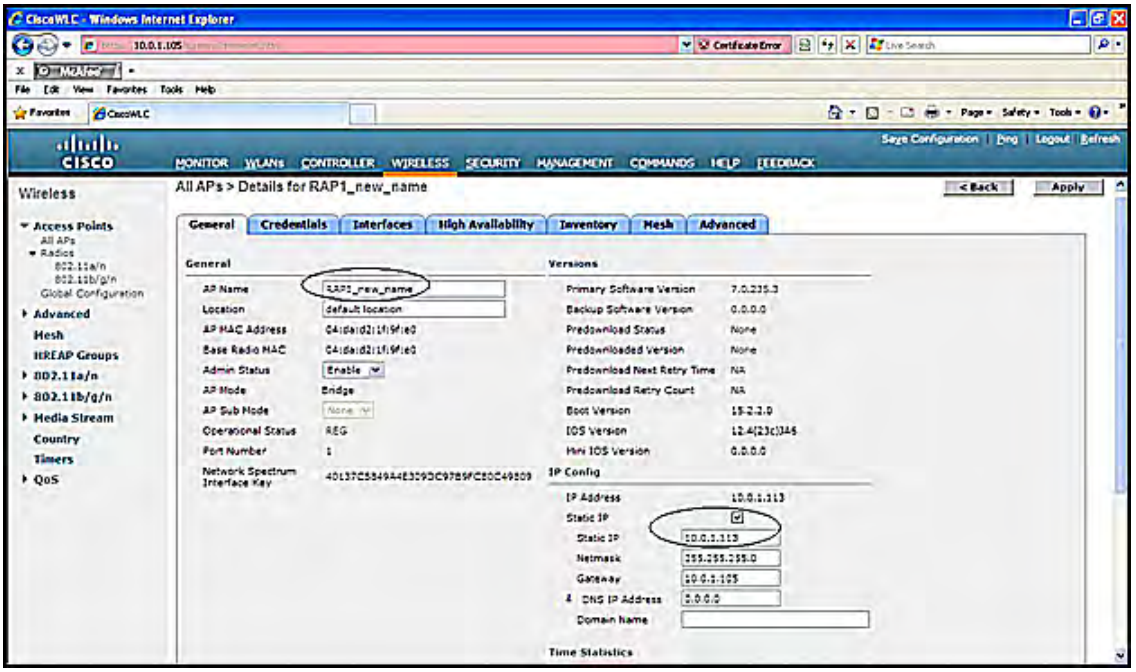



17 Perform the changes in the configuration file, for the following command **`config ap name RAP1_new_name APa8b1.d4d4.b500`**, where RAP1_new_name is a user configured name and APa8b1.d4d4.b500 is the existing name as displayed in **`show ap join status summary all`**.

After all the RAPs rejoin, choose **Transfer > Send Text File**. Browse to the file that was edited based on *`RAPConfig.txt`* and open the file.

The file enters commands into the WLC CLI and the RAP restarts.

From the Cisco web GUI, any advanced changes can be performed.



18 Verify the Windows HyperTerminal history for errors. Debug the errors and return to the step 17.

To monitor the WLC CLI for the rejoining status of the RAPs to the controller, run the command **`show ap join stats summary all`** . It should only take about 5 minutes to rejoin.

19 After all the RAPs rejoin, choose **Transfer>Send Text File** and browse to the file that was edited based on the *`RAPBridgingConfig.txt`*. Modify the RAPBridgingConfig file according to the new AP names, for example, RAP1_new_name.

20 Monitor the WLC CLI for the rejoining status of the RAP(s) to the controller. It should only take about 5 minutes to rejoin.

The MAPs can now be configured.

21 Power on all the MAPs. Provide a static IP address and other configurations in all the MAPs as mentioned in step 3 by connecting console serial cable in to the console port of 1552S AP, refer to the section, To configure 1552S Root Access Point (RAP) and Mesh Access Point (MAP).

After 5 to 15 minutes, the MAPs join the controller.

22 Use **`show ap join stats summary all`** command to monitor the join status of all the MAPs. Debug any MAPs that did not join the controller. Ensure that the MAC address in the initial WLC *`overallWLCConfig.txt`* based file matches the value on the MAP labels.

23 Perform the following step after all the RAPs rejoin.

a Choose **Transfer>Send Text File**. Browse and open the file that was edited based on the *`MAPConfig.txt`*. Edit the configuration files, similar to step 17.

The file enters commands into the WLC CLI and the MAPs restart and rejoin.

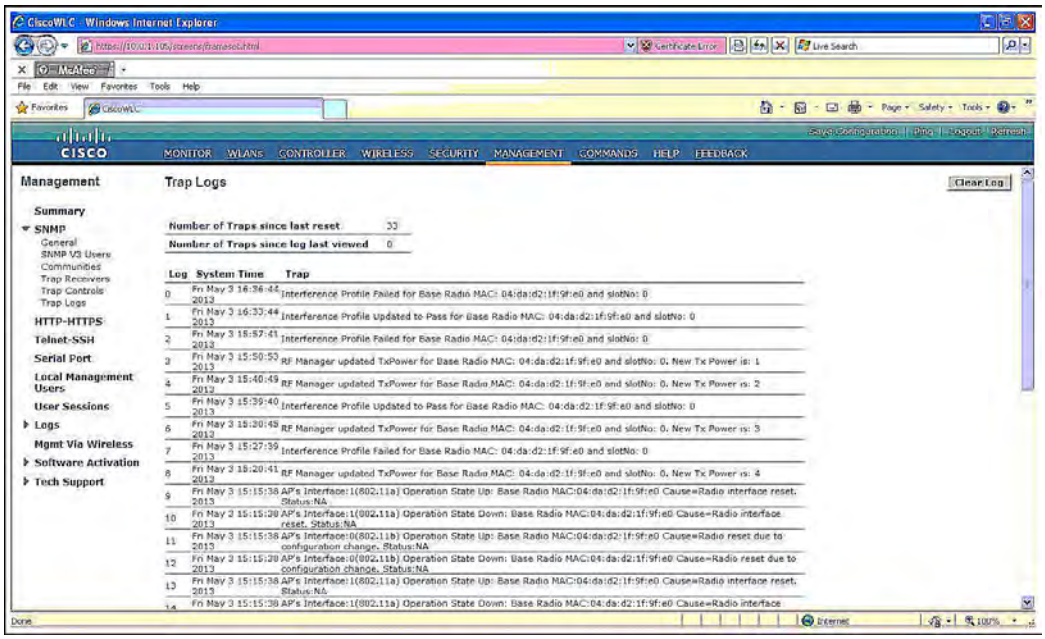
24 Perform the following step after all the MAPs rejoin.

a Choose **Transfer>Send Text File**. Browse and open the file that was edited based on the *`MAPBridgingConfig.txt`*. Edit the configuration files, similar to step 19.

The file enters commands into the WLC CLI and the MAPs restart.

25 Repeat steps 1 through 11 for the secondary WLC using the edited version of *`overallWLCSecConfig.txt`*. Ensure you modify the *`RAPConfig.txt`* and *`MAPConfig.txt`* files to contain the proper name and IP address of the secondary WLC.

From the Cisco web GUI, you can verify the logs of the Cisco system.



# 5 Glossary

Definition of terms and acronyms used throughout this guide.

| | |
|---|---|
| **Access Point** | Entity responsible for the receipt of data packets from the ISA100 Wireless wireless field device network. |
| **Backbone** | A backbone network is a part of the network infrastructure that interconnects various components of the network, providing a path for the exchange of information between different LANs or sub-networks. |
| **Backhaul** | Describes the primary function of the OneWireless Mesh network, which is to transport data from Wi-Fi clients and wireless field devices over the wireless mesh network to a wired network or wired process control network. Also referred to as backhaul mesh or wireless backhaul. |
| **CAPWAP** | Control and Provisioning of Wireless Access Points protocol |
| **CRC** | Cyclic Redundancy Check |
| **DCS** | Distributed Control System |
| **DD files** | Device Description files |
| **DHCP Server** | Dynamic Host Configuration Protocol (DHCP) Server assigns IP addresses to devices that join the network, from the range of IP addresses assigned to it during the configuration. |
| **DSSS** | Direct Sequence Spread Spectrum |
| **FDAP** | Field Device Access Point (FDAP) is a wireless infrastructure node that acts as an ISA100 Wireless access point and a mesh node member. FDAP can only communicate using ISA100 Wireless. |
| **Field device** | A general term for process sensor (input) or process actuator (output) device. |
| **HART** | Highway Addressable Remote Transducer |
| **HLAI** | High Level Analog Input |
| **IEEE** | Institute of Electrical and Electronic Engineers |
| **ISA** | International Society of Automation |
| **Line of sight** | A clear line from one antenna to another in a long-range wireless network. A line of sight is necessary for a long-range network to connect. An RF line of sight differs from a visual line of sight. |
| **MAP** | Mesh Access Point |
| **NTP** | Network Time Protocol |

| | |
|---|---|
| **Provisioning Device handheld** | Includes Personal Digital Assistant (PDA), mobile PCs, and so on. |
| **RAP** | Root Access Point |
| **RF** | Radio Frequency - Any frequency within the electromagnetic spectrum associated with radio wave propagation. When an RF current is supplied to an antenna, an electromagnetic field is created and then propagated through space. |
| **RSQI** | Receive Signal Quality Index |
| **RSSI** | Receive Signal Strength Index - A signal or circuit that indicates the strength of the incoming (received) signal in a receiver. |
| **Switch** | A switch is a multiport device that moves Ethernet packets at full wire speed within a network. |
| **WDM** | Wireless Device Manager is a device that manages the ISA100 Wireless wireless field device network and all the ISA100 Wireless components connected to the OneWireless network. |
| **Access Point** | Access Point provides access point, bridge, repeater, and mesh networking for wireless applications. They generally have field device network connectivity and also conforms to IEEE802.11a/b/g/n wireless standard or IEEE802.3 wired-Ethernet standards or both. Field devices using field device network delivers the process data to the backbone infrastructure through these infrastructure nodes. Multiple wireless infrastructure nodes provide a self-forming and self-healing mesh network. |
| **WLAN** | Wireless Local Area Network |

# 6 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.