

Symbol Handheld Devices in Cisco Unified Environment

Document ID: 110363

Introduction

Prerequisites

Requirements

Components Used

Conventions

Suggestions to Improve Interoperability with Handheld Devices

Related Information

Introduction

This document lists suggestions that are helpful when Symbol handheld devices are deployed in a controller based environment.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Wireless LAN Controllers (WLCs)
- Basic knowledge of handheld devices

Components Used

The information in this document is based on the Wireless LAN Controller (WLC) 4400 that runs version 5.0.148.0.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Suggestions to Improve Interoperability with Handheld Devices

This is the list of suggestions that was found to improve interoperability of handheld devices in a controller based environment:

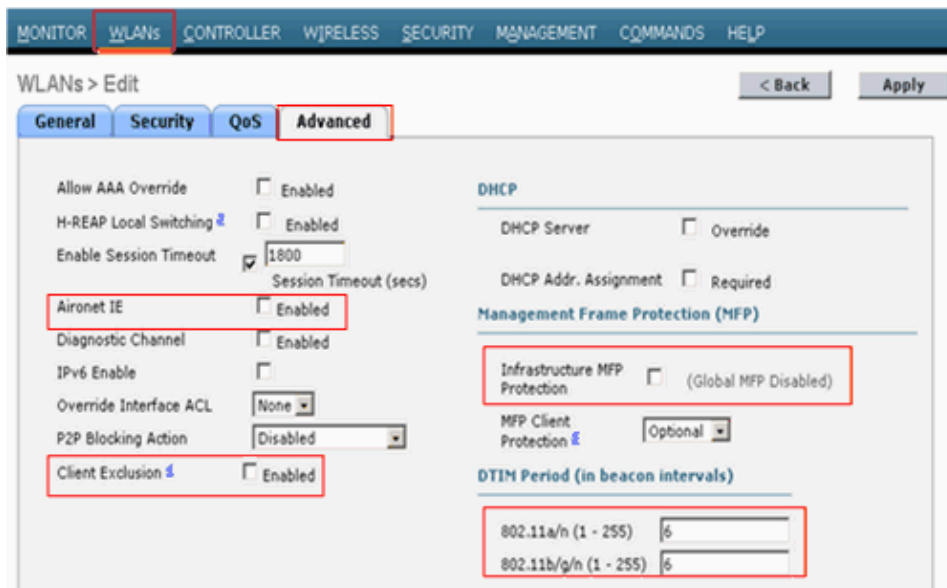
1. If you are in an environment where older switches are used, the access points (APs) will join the WLC but will not have enough power. Therefore, the radios will not come up. A power injector needs to be used to provide sufficient power.

```
config ap power injector enable <AP Name>
```

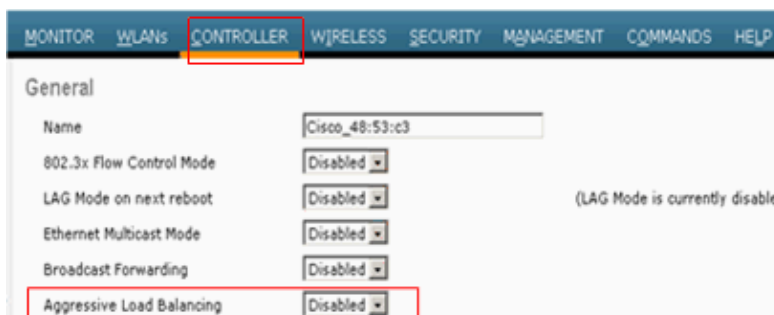
2. Make sure you are running WLC version 4.1.185.0 or later.
3. Symbol devices running earlier firmware version might not roam properly. It sticks to the AP originally associated. This is a known issue and Symbol has released a Beta Version to fix this. Download the Beta Version from Symbol.
4. **Aironet IE** Aironet IE is a Cisco proprietary attribute used by Cisco devices for better connectivity. Disable Aironet IE. From the WLC GUI go to the **WLANs** tab. Click on the WLAN to which the symbol devices connects. Go to the **Advanced** tab and uncheck Aironet IE.
5. Check if the device is CCX certified to ensure interoperability with Cisco WLCs. Certain symbol devices, such as MC75 and MC5590 (under MPA 1.5 platform), are CCXv4 certified.

Devices such as MC9090 WM 6.1, MC9090 – VGA WM 6.1, MC9094 WM 6.1, MC7090 WM 6.1, MC7095 WM 6.1, MC7090 WM 6.1, MC7095 WM 6.1, MC70x4 WM 6.1, MC7598 WM 6.1, MC3090 CE5 Pro, MC3090 CE5 Core, WT4090 CE 5.0(MPA 1.0), and VC5090 CE5.0(MPA 1.0) are CCXv3 certified.

6. Modify the **DTIM** interval. Good performance has been seen with the DTIM setting of 6.
7. **Client Exclusion per WLAN** This option is normally used to exclude certain clients from accessing the WLAN. Disable client exclusion to make sure that Symbol device is not in the excluded list.
8. **MFP** Management Frame Protection is a Cisco proprietary feature introduced to ensure the integrity of the management frames, such as de-authentication, disassociation, beacons, and probes wherein the AP protects the management frames that it transmits when it adds a Message Integrity Check Information Element (MIC IE) to each frame. Any attempt made by the intruders to copy, alter, or replay the frame invalidates the MIC, which causes any receiving AP that is configured to detect MFP frames, to report the discrepancy. **Disable** MFP on the WLC.



9. **Load balancing** This feature is used to prevent too many clients from associating to the WLC. Disable this feature to ensure that the device is not rejected by any chance. Click on the **Controller** tab. Navigate to the **General** menu to disable Aggressive Load Balancing.



10. **Radio Preambles** The radio preamble (sometimes called a header) is a section of data at the head of a packet that contains information that the wireless device and client devices need to send and receive packets. **Long Preamble** increases interoperability between the WLC and the client. Click on the **Wireless** tab.

Navigate to **802.11 b/g/n** and click the **Network** option, then uncheck **Short Preamble**.

The screenshot shows the Cisco WLC configuration interface. The 'WIRELESS' tab is active. The left sidebar shows the navigation tree with '802.11b/g/n' selected, and 'Network' highlighted. The main content area displays '802.11b/g Global Parameters' with a 'General' section. The 'Short Preamble' checkbox is unchecked. The 'Data Rates' section shows various rates with their respective policies.

Parameter	Value	Policy
802.11b/g Network Status	Enabled	Mandatory
802.11g Support	Enabled	Mandatory
Beacon Period (milliseconds)	100	Mandatory
Short Preamble	Disabled	Supported
Fragmentation Threshold (bytes)	2346	Supported
DTPC Support	Enabled	Mandatory
1 Mbps		Mandatory
2 Mbps		Mandatory
5.5 Mbps		Mandatory
6 Mbps		Supported
9 Mbps		Supported
11 Mbps		Mandatory
12 Mbps		Supported
18 Mbps		Supported

11. Disable the Client Exclusion Policies Globally. Click on the **Security** tab and navigate to **Client Exclusion Policies** under the Wireless Protection Policies menu.

Uncheck the options under **Client Exclusion Policies**.

The screenshot shows the Cisco WLC configuration interface with the 'SECURITY' tab active. The left sidebar shows the navigation tree with 'Wireless Protection Policies' expanded and 'Client Exclusion Policies' highlighted. The main content area displays 'Client Exclusion Policies' with five unchecked checkboxes.

- Excessive 802.11 Association Failures
- Excessive 802.11 Authentication Failures
- Excessive 802.1X Authentication Failures
- IP Theft or IP Reuse
- Excessive Web Authentication Failures

Related Information

- **Troubleshooting Client Issues in the Cisco Unified Wireless Network**
 - **Troubleshooting Connectivity in a Wireless LAN Network**
 - **Fixing a Broken Wireless LAN Connection**
 - **Technical Support & Documentation – Cisco Systems**
-

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 – 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: May 19, 2009

Document ID: 110363
