

Wireless LAN Controller (WLC) Mobility Groups FAQ

Document ID: 107188

Contents

Introduction

What is a Mobility Group?

What are the prerequisites for a Mobility Group?

How do I configure a Mobility Group on the WLC?

How do I configure a Mobility Group with WCS?

Can I configure WLCs in multiple Mobility Groups?

Can the LWAPPs join a WLC that belongs to a Mobility Group that is different from the currently associated Mobility Group?

How are Mobility Messages exchanged between WLCs?

Is there a command to troubleshoot mobility communication between WLCs?

How many controllers can be in a Mobility Group?

What is a mobility list? How many controllers can be part of the mobility list of a controller?

How do I secure or encrypt the Mobility Messages exchanged between the WLCs?

What is Mobility Anchor?

What is the difference between RF Groups and Mobility Groups?

Will Mobility Groups work between WLCs if I have one or more controllers behind a network address translation (NAT) device?

Related Information

Introduction

This document provides information on the most frequently asked questions (FAQ) about Mobility Groups. A Mobility Group is a relatively new concept that is applicable to the Cisco Unified Wireless LAN Environment.

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

Q. What is a Mobility Group?

A. A Mobility Group is a group of Wireless LAN Controllers (WLCs) in a network with the same Mobility Group name. These WLCs can dynamically share context and state of client devices, WLC loading information, and can also forward data traffic among them, which enables inter-controller wireless LAN roaming and controller redundancy. Refer to the Configuring Mobility Groups section of Cisco Wireless LAN Controller Configuration Guide, Release 7.0 for more information.

Q. What are the prerequisites for a Mobility Group?

A. Before you add controllers to a mobility group, you must verify that certain requirements are met for all controllers that are to be included in the group. Refer to the Prerequisites section of Configuring Mobility Groups for a list of these requirements.

Q. How do I configure a Mobility Group on the WLC?

A. A Mobility Group is configured manually. The IP and MAC address of the Wireless LAN Controllers (WLCs) that belong to the same Mobility Group are configured on each of the WLCs individually. Mobility Groups can be configured either through the CLI or the GUI.

Q. How do I configure a Mobility Group with WCS?

A. Mobility Groups can also be configured with the Wireless Control System (WCS). This alternative method comes in handy when a large number of WLCs is deployed. Refer to the Configuring Mobility Groups section of Cisco Wireless Control System Configuration Guide, Release 7.0 for more information on how to configure the Mobility Groups with WCS.

Q. Can I configure WLCs in multiple Mobility Groups?

A. No. Wireless LAN Controllers (WLCs) can be configured only in one Mobility Group.

Q. Can the LWAPPs join a WLC that belongs to a Mobility Group that is different from the currently associated Mobility Group?

A. In all Wireless LAN Controller (WLC) versions earlier than 4.2.61.0, when a WLC goes "down," the LAP registered to this WLC can failover only to another WLC of the same Mobility Group, if the LAP is configured for failover. From Cisco WLC version 4.2.61.0 and later, a new feature called Backup Controller Support is introduced for access points to failover to controllers even outside the Mobility Group. Refer to Wireless LAN Controller and Light Weight Access Points Failover Outside the Mobility Group Configuration Example for more information.

Q. How are Mobility Messages exchanged between WLCs?

A. In versions earlier than 5.0, WLCs send Mobility Messages with unicast mode, where the copies of Mobility Messages are unicast to all the WLCs in the Mobility Group. But in version 5.0, Mobility Messages can be sent as Multicast messages wherein only one copy of the Mobility Message is sent to reach all the WLCs in the Mobility Group. Refer to the Messaging among Mobility Groups section of Cisco Wireless LAN Controller Configuration Guide, Release 7.0 for more information.

Q. Is there a command to troubleshoot mobility communication between WLCs?

A. Wireless LAN Controllers (WLCs) software release 4.0 and later enables you to test the mobility communication environment with mobility ping tests. These tests can be used in order to validate connectivity between members of a Mobility Group, which includes guest WLCs. Two ping tests are available:

- ◆ Mobility ping over UDP This test runs over mobility UDP port 16666. It tests whether the mobility control packet can be reached over the management interface.
- ◆ Mobility ping over EoIP This test runs over EoIP. It tests the mobility data traffic over the management interface.

Make sure that the WLCs are configured in the same Mobility Group and ensure that you can ping the WLCs with the mobility pings. Refer to the Running Mobility Ping Tests section of Cisco Wireless LAN Controller Configuration Guide, Release 7.0 for more information.

Q. How many controllers can be in a Mobility Group?

A. A Mobility Group can include up to 24 WLCs of any type. The number of access points supported in a Mobility Group is bound by the number of WLCs and WLC types in the group.

Examples

- ◆ A 4404–100 WLC supports up to 100 access points. Therefore, a Mobility Group that consists of twenty–four 4404–100 WLCs supports up to 2400 access points ($24 * 100 = 2400$ access points).
- ◆ A 4402–25 WLC supports up to 25 access points, and a 4402–50 WLC supports up to 50 access points. Therefore, a Mobility Group that consists of twelve 4402–25 controllers and twelve 4402–50 WLCs supports up to 900 access points ($12 * 25 + 12 * 50 = 300 + 600 = 900$ access points).

You can add different mobility members that are part of a different Mobility Group into the mobility list that is used for mobility anchors that can anchor within a different Mobility Group.

There can be up to 72 members in the list with up to 24 in the same Mobility Group.

Q. What is a mobility list? How many controllers can be part of the mobility list of a controller?

A. A mobility list is a group of controllers configured on a single controller that specifies members in different mobility groups. Controllers can communicate across mobility groups and clients can roam between access points in different mobility groups if the controllers are included in each other's mobility lists. In the example in this section, controller 1 can communicate with either controller 2 or 3, but controller 2 and controller 3 can communicate only with controller 1 and not with each other. Similarly, clients can roam between controller 1 and controller 2 or between controller 1 and controller 3 but not between controller 2 and controller 3.

Example:

Controller 1

Mobility group: A

Mobility list:

Controller 1 (group A)

Controller 2 (group B)

Controller 3 (group C)

Controller 2

Mobility group: B

Mobility list:

Controller 1 (group A)

Controller 2 (group B)

Controller 3

Mobility group: C

Mobility list:

Controller 1 (g

Controller 3 (g

Controller software release 5.1 supports up to 72 controllers in the mobility list of a controller and seamless roaming across multiple mobility groups. During seamless roaming, the client maintains its IP address across all mobility groups. However, Cisco Centralized Key Management (CCKM) and Proactive Key Caching (PKC) are supported only for intra–mobility–group roaming. When a client crosses a mobility group boundary during a roam, the client is fully authenticated, but the IP address is maintained, and EtherIP tunneling is initiated for Layer 3 roaming.

Note: Controller software release 5.0 supports up to 48 controllers in a mobility list.

Q. How do I secure or encrypt the Mobility Messages exchanged between the WLCs?

A. In order to secure the Mobility Messages exchanged between the Wireless LAN Controllers (WLCs), enable the Secure mode between the controllers. In order to do this, issue the **config mobility secure-mode enable** command. In this mode, WLCs use the UDP port 16667 in order to exchange the messages. If there is a firewall, ensure that the UDP port 16667 is opened. In order to ensure this mode is enabled, verify the Mobility Protocol Port from the output of the **show mobility summary** command. Port 16667 indicates secure-mode (encryption). Port 16666 indicates non secure-mode (no encryption).

Q. What is Mobility Anchor?

A. Mobility Anchor, also referred to as Guest tunneling or Auto Anchor Mobility, is a feature where all the client traffic that belongs to a WLAN (Specially Guest WLAN) is tunneled to a predefined WLC or set of controllers that are configured as Anchor for that specific WLAN. This feature helps to restrict clients to a specific subnet and have more control over the user traffic. Refer to the Configuring Auto-Anchor Mobility section of Cisco Wireless LAN Controller Configuration Guide, Release 7.0 for more information on this feature.

Q. What is the difference between RF Groups and Mobility Groups?

A. Mobility Groups:

- ◆ A Mobility Group is a group of WLCs in a network with the same Mobility Group name. It allows for seamless client roaming and WLC redundancy.
- ◆ A Mobility Group is formed statically.

Radio Frequency (RF) Groups:

- ◆ An RF Group, also known as an RF domain, is a cluster of WLCs for which Radio Resource Management (RRM) calculations are done on a whole. RF Groups also help you to discover Rogue APs.
- ◆ An RF Group is formed dynamically. Refer to the Overview of RF Groups section of Cisco Wireless LAN Controller Configuration Guide, Release 7.0. for more information on RF Groups.

Q. Will Mobility Groups work between WLCs if I have one or more controllers behind a network address translation (NAT) device?

A. In controller software releases earlier than 4.2, mobility between controllers in the same Mobility Group does not work if one of the controllers is behind a network address translation (NAT) device. This behavior creates a problem for the guest anchor feature where one controller is expected to be outside the firewall.

Mobility message payloads carry IP address information about the source controller. This IP address is validated with the source IP address of the IP header. This behavior poses a problem when a NAT device is introduced in the network because it changes the source IP address in the IP header. Hence, in the guest WLAN feature, any mobility packet that is routed through a NAT device is dropped because of the IP address mismatch.

In controller software release 4.2 or later, the Mobility Group lookup is changed to use the MAC address of the source controller. Because the source IP address is changed due to the mapping in the NAT device, the Mobility Group database is searched before a reply is sent to get the IP address of the controller that makes the request. This is done with the MAC address of the controller that makes the request.

Refer to Using Mobility Groups with NAT Devices for more information.

Related Information

- **How to configure the Lightweight Access Point in order to join the respective Wireless LAN Controller**
 - **Cisco Wireless LAN Controller Configuration Guide, Release 7.0**
 - **Cisco Wireless Control System Configuration Guide, Release 4.1**
 - **WLAN Controller Failover for Lightweight Access Points Configuration Example**
 - **Wireless Guest Access FAQ**
 - **Technical Support & Documentation – Cisco Systems**
-

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

© 2014 – 2015 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Sep 02, 2008

Document ID: 107188
