Review Wireless LAN Controller Mobility Groups FAQ

Contents

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

Background Information

Q. What is a Mobility Group?

Q.What are the Restrictions for Mobility Groups?

Q.What are the Prerequisites for a Mobility Group?

Q.How to Configure a Mobility Group on the WLC?

Q.How to Configure a Mobility Group with Prime Infrastructure?

Q.Is it Possible to Configure WLCs in Multiple Mobility Groups?

Q.Can the APs Join a WLC That Belongs to a Mobility Group That is Different From the Currently Associated Mobility Group?

Q. How are Mobility Messages Exchanged Between WLCs?

Q.Is There a Command to Troubleshoot Mobility Communication Between WLCs?

Q.How Many Controllers can be in a Mobility Group?

Q. What is a Mobility list? How Many Controllers can be Part of the Mobility List of a Controller?

Q.How to Secure or Encrypt the Mobility Messages Exchanged Between the WLCs?

Q. What are the Restrictions to Enable Encrypted Mobility Tunnel?

Q. What is a Mobility Anchor?

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

Q.Does Mobility Groups Work Between WLCs if There are One or More Controllers Behind a NAT Device?

Related Information

Introduction

This document describes Mobility Groups in AireOS Wireless LAN Controllers and provides information through the most frequently asked questions (FAQ).

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

This document is not restricted to specific software and hardware versions.

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, ensure that you understand the potential impact of any command.

Conventions

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

Background Information

A Mobility Group is a concept that is applicable to the Cisco Unified Wireless LAN environment.

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 load information, and can also forward data traffic among them, which enables inter-controller wireless LAN roam and controller redundancy. Refer to the Mobility Groups section of Cisco Wireless LAN Controller Configuration Guide, Release 8.10 for more information.

Q. What are the Restrictions for Mobility Groups?

A. You can find the restrictions to Mobility Groups in the Guidelines and Restrictions section of the Configuring Mobility Groups chapter of Cisco Wireless LAN Controller Configuration Guide, Release 8.10.

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 to 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. Refer to Configuring Mobility Groups GUI and CLI for detailed steps for CLI and GUI configuration.

Q. How to Configure a Mobility Group with Prime Infrastructure?

A. Mobility Groups can also be configured with the Prime Infrastructure (PI). This alternative method comes in handy when a large number of WLCs is deployed. Refer to the Configuring Mobility Groups section of Cisco Prime Infrastructure 3.10 User Guide for more information on how to configure the Mobility Groups with WCS.

Q. Is it Possible to Configure WLCs in Multiple Mobility Groups?

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

Q. Can the APs Join a WLC That Belongs to a Mobility Group That is Different From the Currently Associated Mobility Group?

A. Yes. By default , when a WLC goes **down**, the APs registered to this WLC failovers to another WLC of the same Mobility Group, if the LAP is configured for failover. However, if a backup Controller Support is configured, then it can be any WLC even outside the Mobility Group and the access points failovers to controllers even outside the Mobility Group. Refer to N+1 High Availability Deployment Guide for more information.

Q. How are Mobility Messages Exchanged Between WLCs?

A. The controller sends mobility messages to other member controllers and with that provides inter-subnet mobility for clients. Mobility Messages can be sent as unicast or multicast messages wherein only one copy of the Mobility Message is sent to reach all the WLCs in the Mobility Group.

Mobile Announce messages are sent within the same group first and then to other groups in the list.

Q. Is There a Command to Troubleshoot Mobility Communication Between WLCs?

A. Wireless LAN Controllers (WLCs) allow 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 8.10 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.

For example, if a controller supports 6000 access points, a mobility group that consists of 24 such controllers supports up to 144,000 access points (24 * 6000 = 144,000 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.

In a mobility list, these combinations of mobility groups and members are allowed:

- 3 mobility groups with 24 members in each group
- 12 mobility groups with 6 members in each group
- 24 mobility groups with 3 members in each group
- 72 mobility groups with 1 member in each 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 mobility list. 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                    Controller 2                    Controller 3
Mobility group: A               Mobility group: B               Mobility group: C
Mobility list:                  Mobility list:                  Mobility list:
     Controller 1 (group A)          Controller 1 (group A)          Controller 1 (group A)
     Controller 2 (group B)          Controller 2 (group B)          Controller 3 (group C)
     Controller 3 (group C)
```

WLCs supports up to 72 controllers in the mobility list of a controller and seamless roam across multiple mobility groups. Through 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 while a roam, the client is fully authenticated, but the IP address is maintained, and EtherIP tunneling is initiated for Layer 3 roaming.

Q. How to 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), you can enable the a secure link in which data is encrypted through CAPWAP DTLS protocol can be established between an anchor and a foreign controller. This secured link is called Encrypted Mobility Tunnel.

If encrypted mobility tunnel is in enabled state, the data traffic is encrypted and the controller uses UDP port 16667, instead of EoIP, to send the data traffic.

In order to do this, issue the **config mobility secure-mode enable** command.

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 are the Restrictions to Enable Encrypted Mobility Tunnel?

A. You can find the restrictions to enable Encrypted Mobility Tunnel in the Restrictions on Encrypted Mobility Tunnel section of Cisco Wireless LAN Controller Configuration Guide, Release 8.10.

Q. What is a 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 8.10 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 roam 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 8.10 for more information on RF Groups.

Q. Does Mobility Groups Work Between WLCs if There are One or More Controllers Behind a NAT Device?

A. Yes. 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 network address translation 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 WLCs 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 map created 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.

When you configure the mobility group in a network where NAT is enabled, enter the IP address that is sent to the controller from the NAT device rather than the controller management interface IP address.

Also, make sure that these ports are open on the firewall if you use a firewall such as PIX:

- UDP 16666 for tunnel control traffic
- IP protocol 97 for user data traffic
- UDP 161 and 162 for SNMP

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

Related Information

- Cisco Wireless LAN Controller Configuration Guide, Release 8.10
- **Cisco Technical Support & Downloads**