High Availability

- Information About High Availability, page 1
- Restrictions on High Availability, page 6
- Configuring High Availability (GUI), page 9
- Configuring High Availability (CLI), page 10
- Monitoring High Availability Standby WLC, page 12

Information About High Availability

High availability (HA) in controllers allows you to reduce the downtime of the wireless networks that occurs due to the failover of controllers.

A 1:1 (Active:Standby-Hot) stateful switchover of access points (AP SSO) is supported. In an HA architecture, one controller is configured as the primary controller and another controller as the secondary controller.

After you enable HA, the primary and secondary controllers are rebooted. During the boot process, the role of the primary controller is negotiated as active and the role of the secondary controller as standby-hot. After a switchover, the secondary controller becomes the active controller and the primary controller becomes the standby-hot controller. After subsequent switchovers, the roles are interchanged between the primary and the secondary controllers. The reason for switchovers are either because of manual trigger, or a controller, or network failure.

During an AP SSO, all the AP sessions statefully switch over and all the clients are deauthenticated and reassocaited with the new active controller except for the locally switched clients in the FlexConnect mode.

The standby-hot controller continuously monitors the health of the active controller through a direct wired connection over a dedicated redundancy port. Both the controllers share the same configurations, including the IP address of the management interface.

Before you enable HA, ensure that both the controllers are physically connected through the redundant port using an Ethernet cable. Also, ensure that the uplink is connected to an infrastructure switch and that the gateway is reachable from both the controllers.

In HA architecture, the redundancy port and redundant management interfaces have been introduced.

A seamless transition of clients from the active controller to the standby controller is also supported. Clients that are not in the Run state are removed after the switchover. During the stateful switchover of a client (Client SSO), the information of the client is synchronized with the standby controller when the client is associated.
with the controller, or is configured. Clients that are fully authenticated, that is, clients that are in the Run state, are synchronized with the peer controller. The data structures of clients are synchronized based on the client state. Clients that are in the transient state are dissociated after a switchover.

In the Cisco Wireless LAN Controller Release 8.0 and later, the output of the `show ap join stats summary` command displays the status of the access points based on whether the access point joined the controller or it was synchronized from Active controller. One of the following statuses is displayed:

- **Synched**—The access point joined the controller before the SSO.
- **Connected**—The access point joined the controller after the SSO.
- **Joined**—The access point rejoined the controller, or a new AP has joined the controller after the SSO.

In Release 8.0 and later, the output of the `show redundancy summary` command displays the bulk synchronization status of access points and clients after the pair-up of active and standby controllers occurs. The values are:

- **Pending**—Indicates that synchronization of access points and the corresponding clients details from the active to standby controller is yet to begin.
- **In-progress**—Indicates that synchronization of access points and the corresponding clients details from the active to standby controller has begun and synchronization is in progress.
- **Complete**—Indicates that synchronization is complete and the standby controller is ready for a switchover to resume the services of the active controller.

From release 8.0 and later, in a High Availability scenario, the sleeping timer is synchronized between active and standby.

ACL and NAT IP configurations are synchronized to the HA standby controller when these parameters are configured before HA pair-up. If the NAT IP is set on the management interface, the access point sets the AP manager IP address as the NAT IP address. This issue is seen only when the NAT IP address and ACL are set on the management interface before you enable high availability.

The following are some guidelines for high availability:

- We recommend that you do not pair two controllers of different hardware models. If they are paired, the higher controller model becomes the active controller and the other controller goes into maintenance mode.
- We recommend that you do not pair two controllers on different controller software releases. If they are paired, the controller with the lower redundancy management address becomes the active controller and the other controller goes into maintenance mode.
- We recommend that you disable HA and add license in Cisco 5520, Flex 7510, 8510, and 8540 WLCs (RTU based). However, it is not mandatory to disable HA as AP licenses added in Primary WLC will be inherited to Secondary WLC.
- All download file types, such as image, configuration, web-authentication bundle, and signature files—are downloaded on the active controller first and then pushed to the standby-hot controller.
- Certificates should be downloaded separately on each controller before they are paired.
- You can upload file types such as configuration files, event logs, crash files, and so on, from the standby-hot controller using the GUI or CLI of the active controller. You can also specify a suffix to the filename to identify the uploaded file.
To perform a peer upload, use the service port. In a management network, you can also use the redundancy management interface (RMI) that is mapped to the redundancy port or RMI VLAN, or both, where the RMI is the same as the management VLAN. Note that the RMI and the redundancy port should be in two separate Layer2 VLANs, which is a mandatory configuration.

If the controllers cannot reach each other through the redundant port and the RMI, the primary controller becomes active and the standby-hot controller goes into the maintenance mode.

To achieve HA between two Cisco Wireless Services Module 2 (WiSM2) platforms, the controllers should be deployed on a single chassis, or on multiple chassis using a virtual switching system (VSS) and extending a redundancy VLAN between the multiple chassis.

A redundancy VLAN should be a nonroutable VLAN in which a Layer 3 interface should not be created for the VLAN, and the interface should be allowed on the trunk port to extend an HA setup between multiple chassis. Redundancy VLAN should be created like any other data VLAN on Cisco IOS-based switching software. A redundancy VLAN is connected to the redundant port on Cisco WiSM2 through the backplane. It is not necessary to configure the IP address for the redundancy VLAN because the IP address is automatically generated. Also, ensure that the redundancy VLAN is not the same as the management VLAN.

When the RMIs for two controllers that are a pair, and that are mapped to same VLAN and connected to same Layer3 switch stop working, the standby controller is restarted.

The "mobilityHaMac is out of range" XML message is seen during the active/standby second switchover in an HA setup. This occurs if mobility HA MAC field is more than 128.

When HA is enabled, the standby controller always uses the Remote Method Invocation (RMI), and all the other interfaces—dynamic and management, are invalid.

The RMI is meant to be used only for active and standby communications and not for any other purpose.

You must ensure that the maximum transmission unit (MTU) on RMI port is 1500 bytes or higher before you enable high availability.

When HA is enabled, ensure that you do not use the backed-up image. If this image is used, the HA feature might not work as expected:

- The service port and route information that is configured is lost after you enable SSO. You must configure the service port and route information again after you enable SSO. You can configure
the service port and route information for the standby-hot controller using the **peer-service-port** and **peer-route** commands.

- For Cisco WiSM2, service port reconfigurations are required after you enable redundancy. Otherwise, Cisco WiSM2 might not be able to communicate with the supervisor. We recommend that you enable DHCP on the service port before you enable redundancy.
- We recommend that you do not use the **reset** command on the standby-hot controller directly. If you use this, unsaved configurations will be lost.

- We recommend that you enable link aggregation configuration on the controllers before you enable the port channel in the infrastructure switches.
- All the configurations that require reboot of the active controller results in the reboot of the standby-hot controller.
- The Ignore AP list is not synchronized from the active controller to the standby-hot controller. The list is relearned through SNMP messages from Cisco Prime Infrastructure after the standby-hot controller becomes active.

- **Client SSO related guidelines:**
  - The standby controller maintains two client lists: one is a list of clients in the Run state and the other is a list of transient clients in all the other states.
  - Only the clients that are in the Run state are maintained during failover. Clients that are in transition, such as roaming, 802.1X key regeneration, web authentication logout, and so on, are dissociated.
  - As with AP SSO, Client SSO is supported only on WLANs. The controllers must be in the same subnet. Layer3 connection is not supported.

- In Release 7.3.x, AP SSO is supported, but client SSO is not supported, which means that after an HA setup that uses Release 7.3.x encounters a switchover, all the clients associated with the controller are deauthenticated and forced to reassociate.

- You must manually configure the mobility MAC address on the then active controller post switchover, when a peer controller has a controller software release that is prior to Release 7.2.

- To enable an access point to maintain controlled Quality of Service (QoS) for voice and video parameters, all the bandwidth-based or static call admission control (CAC) parameters are synchronized from active to standby when a switchover occurs.

- From 8.0 release and later, the standby controller does not reboot; instead enters the maintenance mode when unable to connect to the default gateway using the redundant port. Once the controller reconnects to the default gateway, the standby controller reboots and the HA pair with the active controller is initiated. However, the active controller still reboots before entering the maintenance mode.

- The following are supported from Release 8.0:
  - **Static CAC synchronization**—To maintain controlled Quality-of-Service (QoS) for voice and video parameters, all the bandwidth-based or static CAC parameters services are readily available for clients when a switchover occurs.
  - **Internal DHCP server**—To serve wireless clients of the controller, the internal DHCP server data is synchronized from the active controller to the standby controller. All the assigned IP addresses remain valid, and IP address assignment continues when the role changes from active to standby occurs.
Enhanced debugging and serviceability—All the debugging and serviceability services are enhanced for users.

- The physical connectivity or topology of the access points on the switch are not synchronized from the active to the standby controller. The standby controller learns the details only when the synchronization is complete. Hence, you must execute the `show ap cdp neighbors all` command only after synchronization is complete, and only when the standby becomes the then active controller.

- To enable access points to join the HA-SKU secondary controller that has been reset to factory defaults, you must:
  - Configure the HA SKU controller as secondary controller. To do this, you must execute the `config redundancy unit secondary` command on the HA SKU controller.
  - Reboot the HA SKU controller after you successfully execute the `config redundancy unit secondary` command.

**Redundancy Management Interface**

The active and standby-hot controllers use the RMI to check the health of the peer controller and the default gateway of the management interface through network infrastructure.

The RMI is also used to send notifications from the active controller to the standby-hot controller if a failure or manual reset occurs. The standby-hot controller uses the RMI to communicate to the syslog, NTP/SNTP server, FTP, and TFTP server.

It is mandatory to configure the IP addresses of the Redundancy Management Interface and the Management Interface in the same subnet on both the primary and secondary controllers.

**Redundancy Port**

The redundancy port is used for configuration, operational data synchronization, and role negotiation between the primary and secondary controllers.

The redundancy port checks for peer reachability by sending UDP keepalive messages every 100 milliseconds (default frequency) from the standby-hot controller to the active controller. If a failure of the active controller occurs, the redundancy port is used to notify the standby-hot controller.

If an NTP/SNTP server is not configured, the redundancy port performs a time synchronization from the active controller to the standby-hot controller.

In Cisco WiSM2, the redundancy VLAN must be configured on the Cisco Catalyst 6000 Supervisor Engine because there is no physical redundancy port available on Cisco WiSM2.

The redundancy port and the redundancy VLAN in Cisco WiSM2 are assigned an automatically generated IP address in which the last two octets are obtained from the last two octets of the RMI. The first two octets are always 169.254. For example, if the IP address of the RMI is 209.165.200.225, the IP address of the redundancy port is 169.254.200.225.

The redundancy ports can connect over an L2 switch. Ensure that the redundancy port round-trip time is less than 80 milliseconds if the keepalive timer is set to default, that is, 100 milliseconds, or 80 percent of the keepalive timer if you have configured the keepalive timer in the range of 100 milliseconds to 400 milliseconds. The failure detection time is calculated, for example, if the keepalive timer is set to 100 milliseconds, as follows: $3 \times 100 = 300 + 60 = 360 + \text{jitter (12 milliseconds)} = -400 \text{ milliseconds}$. Also, ensure that the bandwidth between redundancy ports is 60 Mbps or higher. Ensure that the maximum transmission unit (MTU) is 1500 bytes or higher.
Restrictions on High Availability

- We recommend that you do not disable LAG physical ports when HA SSO is enabled.

- HA sync for Fabric related statistics is not supported.

- You should apply an access list for SSH to the redundancy interface on upper switch, if Cisco WLC is configured for HA SSO and redundancy management is configured over a dynamic interface. Failure to do so enables the SSH client to connect through the redundancy management interface regardless of the CPU ACL.

- When you configure the controller for HA SSO, the Cisco 600 Series OfficeExtend Access Points are not supported.

- In an HA environment using FlexConnect locally switched clients, the client information might not show the username. To get details about the client, you must use the MAC address of the client. This restriction does not apply to FlexConnect centrally switched clients or central (local) mode clients.

- It is not possible to access the Cisco WiSM2 GUI through the service interface when you have enabled HA. The workaround is to create a service port interface again after HA is established.

- In an HA environment, an upgrade from an LDPE image to a non-LDPE image is not supported.

- It is not possible to pair two primary controllers or two secondary controllers.

- Standby controllers are unavailable on the APs connected switch port

- An HA-SKU controller with an evaluation license cannot become a standby controller. However, an HA-SKU controller with zero license can become a standby controller.

- Service VLAN configuration is lost when moving from HA mode to non-HA mode and vice versa. You should configure the service IP address manually again.

- The following scenario is not supported: The primary controller has the management address and the redundancy management address in the same VLAN, and the secondary controller has the management address in the same VLAN as the primary one, and the redundancy management address in a different VLAN.

- The following is a list of some software upgrade scenarios:
  - A software upgrade on the active controller ensures the upgrade of the standby-hot controller.
  - An in-service upgrade is not supported. Therefore, you should plan your network downtime before you upgrade the controllers in an HA environment.
  - Rebooting the active controller after a software upgrade also reboots the standby-hot controller.
  - We recommend that both active and standby-hot controllers have the same software image in the backup before running the `config boot backup` command. If both active and standby-hot controllers have different software images in the backup, and if you run the `config boot backup` command in the active controller, both the controllers reboot with their respective backup images breaking the HA pair due to a software mismatch.
  - A schedule reset applies to both the controllers in an HA environment. The peer controller reboots a minute before the scheduled time expires on the active controller.
  - You can reboot the standby-hot controller from the active controller by entering the `reset peer-system` command if the scheduled reset is not planned. If you reset only the standby-hot
controller with this command, any unsaved configurations on the standby-hot controller is lost. Therefore, ensure that you save the configurations on the active controller before you reset the standby-hot controller.

- A preimage download is reinitiated if an SSO is triggered at the time of the image transfer.
- Only `debug` and `show` commands are allowed on the standby-hot controller.
- After a switchover, if a peer controller has a controller software release that is prior to Release 7.5, all the mobility clients are deauthenticated.

• It is not possible to access the standby-hot controller through the controller GUI, Cisco Prime Infrastructure, or Telnet. You can access the standby-hot controller only on its console.

• When a failover occurs, the standby controller must be in a standby-hot state and the redundant port in a terminal state in SSO for successful switchover to occur.

• To enable or disable LAG, you must disable HA.

**Note**

If LAG is disabled and both primary and backup ports are connected to the management interface and if the primary port becomes nonoperational, a switchover might occur because the default gateway is not reachable and backup port failover might exceed 12 seconds.

• When a failover occurs and the standby controller becomes the new active controller, it takes approximately 15 to 20 minutes to synchronize the database (AP, client, and multicast) between the two controllers. If another failover occurs during this time, the HA structures would not yet be synchronized. Therefore, the APs and clients would have to get reassociated and reauthenticated respectively.

• Pairwise Master Key (PMK) cache synchronization is not supported on FlexConnect local-authenticated clients.

• Client SSO restrictions:
  - New mobility is not supported.
  - Posture and network admission control out-of-band are not supported because the client is not in the Run state.
  - The following are not synchronized between the active and standby controller:
    - Cisco Compatible Extension-based applications
    - Client statistics
    - Proxy Mobile IPv6, Application Visibility and Control, session initiation protocol (SIP), and static call admission control (CAC) tree
    - Workgroup bridges and the clients associated with them
    - Clients that are associated with Cisco 600 Series OfficeExtend Access Points
    - Passive clients

  - Encryption is supported
• Encryption is supported only if the active and standby controllers communicate through the Redundancy Management Interface on the management ports. Encryption is not supported if the redundancy port is used for communication between the active and standby controllers.

• You cannot change the NAT address configuration of the management interface when the controllers are in redundancy mode. To enable NAT address configuration on the management interface, you must remove the redundancy configuration first, make the required changes on the primary controller, and then reenable the redundancy configuration on the same controller.

• On Cisco WiSM2 and Cisco Catalyst 6500 Series Supervisor Engine 2T, if HA is enabled, post switchover, the APs might disconnect and reassociate with the WiSM2 controller. To prevent this from occurring, before you configure HA, we recommend that you verify, in the port channel, the details of both the active and standby Cisco WiSM2 controllers that the ports are balanced in the same order and the port channel hash distribution uses fixed algorithm. If they are not in order, you must change the port channel distribution to be fixed and reset Cisco WiSM2 from the Cisco Catalyst 6500 Series Supervisor Engine 2T.

• After you enable SSO, you must access both the standby and active controller using:
  ◦ The console connection
  ◦ SSH facility on the service port
  ◦ SSH facility on the redundant management interface

• After the switch over of controller, clients along with children mesh access points (MAPs) are disconnected and are rejoined with the new active controller. The entire mesh tree is rebuilt. The clients of root access points (RAPs) are also disconnected but the RAPs are intact with the controller.

• Synchronization of bulk configurations is supported only for the configurations that are stored in XMLs. Scheduled reboot is a configuration that is not stored in XMLs or Flash. Therefore, the scheduled reboot configuration is not included in the synchronization of bulk configurations.

• When a switchover occurs, the controller does not synchronize the information on DHCP dirty bit from the active to standby controller even when DHCP dirty bit is set on the active controller. After a switchover, the controller populates the DHCP dirty bit based on the client DHCP retries.

• If you are using Cisco WiSM2, we recommend that you use the following release versions of Cisco IOS on Cisco Catalyst 6500 Series Supervisor Engine 2T:
  ◦ 15.1(02)SY
  ◦ 15.1(01)ICB40.1
  ◦ 15.1(01)ICB29.36
  ◦ 15.1(01)ICB29.1
  ◦ 15.1(01)IC66.25
  ◦ 15.1(01)IB273.72
Configuring High Availability (GUI)

Before You Begin

Ensure that the management interfaces of both controllers are in the same subnet. You can verify this on the GUI of both the controllers by choosing Controllers > Interfaces and viewing the IP addresses of the management interface.

Step 1
On the GUI of both the controllers, choose Controller > Redundancy > Global Configuration. The Global Configuration window is displayed.

Step 2
Enter the addresses of the controllers in the Redundant Management IP field and the Peer Redundant Management IP field.

Note
Ensure that the Redundant Management Interface IP address of one controller is the same as the Redundant Management Interface IP address of the peer controller.

Step 3
From the Redundant Unit drop-down list, choose one of the controllers as primary and the other as secondary.

Step 4
On the GUI of both the controllers, set the SSO to Enabled state.

Note
After you enable an SSO, the service port peer IP address and the service port netmask appear on the configuration window. Note that the service port peer IP address and the netmask can be pushed to the peer only if the HA peer is available and operational. When you enable HA, you do not have to configure the service port peer IP address and the service port netmask parameters. You must configure the parameters only when the HA peer is available and operational. After you enable SSO, both the controllers are rebooted. During the reboot process, the controllers negotiate the redundancy role through the redundant port, based on the configuration. The primary controller becomes the active controller and the secondary controller becomes the standby controller.

Step 5
(Optional) After the HA pair becomes available and operational, you can configure the peer service port IP address and the netmask after the service port is configured as static. If you enable DHCP on the service port, you do not have to configure these parameters on the Global Configuration window:

- **Service Port Peer IP**—IP address of the service port of the peer controller.
- **Service Port Peer Netmask**—Netmask of the service port of the peer controller.
- **Mobility MAC Address**—A common MAC address for both the active and standby controllers that is used in the mobility protocol. If an HA pair has to be added as a mobility member for a mobility group, the mobility MAC address (instead of the system MAC address of the active or standby controller) should be used. Normally, the mobility MAC address is chosen as the MAC address of the active controller and you do not have to manually configure this.
- **Keep Alive Timer**—The timer that controls how often the standby controller sends keepalive messages to the active controller. The valid range is between 100 to 1000 milliseconds.
- **Peer Search Timer**—The timer that controls how often the active controller sends peer search messages to the standby controller. The valid range is between 60 to 300 seconds.

Note
After you enable the HA and pair the controllers, there is only one unified GUI to manage the HA pair through the management port. GUI access through the service port is not feasible for both the active and standby controllers. The standby controller can be managed only through the console port or the service port. Only Telnet and SSH sessions are allowed through the service port of the active and standby controllers.
Step 6  Click **Apply**.

Step 7  Click **Save Configuration**.

Step 8  View the redundancy status of the HA pair by choosing **Monitor > Redundancy > Summary**. The **Redundancy Summary** window is displayed.

Step 9  View the redundancy status of the HA pair by choosing **Monitor > Redundancy > Detail**. The **Redundancy Detail** page is displayed.

Step 10  View the redundancy statistics information of the HA pair by choosing **Monitor > Redundancy > Statistics**. The **Redundancy Statistics** page is displayed.

Step 11  Perform these steps to configure the peer network route:
   a) Choose **Controller > Redundancy > Peer Network Route**. The **Network Routes Peer** window is displayed.
      This window provides a summary of the existing service port network routes of the peer controller to network or element management systems on a different subnet. You can view the IP address, IP netmask, and gateway IP address.
   b) To create a new peer network route, click **New**.
   c) Enter the **IP address**, **IP netmask**, and the **Gateway IP address** of the route.
   d) Click **Apply**.

---

**Configuring High Availability (CLI)**

**Before You Begin**

Ensure that the management interfaces of both controllers are in the same subnet.

To configure HA in controllers, you must:

- Configure a local-redundancy IP address and a peer-redundancy management IP address by running this command:
  
  ```
  config interface address redundancy-management ip-addr1 peer-redundancy-management ip-addr2
  ```
  
- Configure the role of a controller by entering this command:
  
  ```
  config redundancy unit {primary | secondary}
  ```
  
- Configure the redundancy mode by entering this command:
  
  ```
  config redundancy mode {sso | none}
  ```

**Note** Both controllers reboot and then negotiate the roles of active and standby-hot controllers.

- Configure redundancy by entering this command:
  
  ```
  config redundancy mode {sso {ap | client} | disable}
  ```
You can choose between an AP SSO and a client SSO.

- Configure the route configurations of the standby controller by entering this command:
  ```
  config redundancy peer-route {add network-ip-addr ip-mask | delete network-ip-addr}
  ```

Note

- This command can be run only if the HA peer controller is available and operational.

- Configure a mobility MAC address by entering this command:
  ```
  config redundancy mobilitymac mac-addr
  ```

Note

- This command can be run only when SSO is disabled.
- If you upgrade from Release 8.0.110.0 to a later release, this command's setting is removed. You must manually reconfigure the mobility MAC address after the upgrade.

- Configure the IP address and netmask of the peer service port of the standby controller by entering this command:
  ```
  config redundancy interface address peer-service-port ip-address netmask
  ```
  This command can be run only if the HA peer controller is available and operational.

- Initiate a manual switchover by entering this command:
  ```
  redundancy force-switchover
  ```

Note

- Execute this command only when you require a manual switchover.

- Configure a redundancy timer by entering this command:
  ```
  config redundancy timer {keep-alive-timer time-in-milliseconds | peer-search-timer time-in-seconds}
  ```

- Configure encryption of communication between controllers by entering this command:
  ```
  config redundancy link-encryption {enable | disable}
  ```

- Configure the hash distribution as fixed by entering this command:
  ```
  config port-channel hash-distribution fixed
  ```

- Verify a port channel member order and load value by entering this command:
  ```
  show etherchannel port-channel
  ```

- View the status of the redundancy by entering this command:
  ```
  show redundancy summary
  ```

- View information about the redundancy management interface by entering this command:
  ```
  show interface detailed redundancy-management
  ```

- View information about the redundancy port by entering this command:
  ```
  show interface detailed redundancy-port
  ```
• Reboot a peer controller by entering this command:
  `reset peer-system`

• Start the upload of file types, such as configuration, event logs, crash files, and so on from the standby-hot
  controller by entering this command on the active controller:
  `transfer upload peer-start`

• View information about sleeping clients after a switchover, by entering this command on the then active
  controller:
  `show custom-web sleep-client summary`

• Debug the redundancy modules by entering these commands:

  ```
  debug redundancy {infra | facilitator | transport | keepalive | gw-reachability | config-sync | ap-sync
  | client-sync | mobility}
  ```

  - `infra`—Configures debug of the Redundancy Infra Module.
  - `facilitator`—Configures debug of the Redundancy Facilitator Module.
  - `transport`—Configures debug of the Redundancy Transport Module.
  - `keepalive`—Configures debug of the Redundancy Keepalive Module.
  - `config-sync`—Configures debug of the Redundancy Config-Sync Module.
  - `ap-sync`—Configures debug of the Redundancy AP-Sync Module.
  - `client-sync`—Configures debug of the Redundancy Client-Sync Module.
  - `mobility`—Configures debug of the Redundancy Mobility Module.

**Note**

Ensure that SSO is enabled to use these debug commands. Enter `config redundancy mode SSO` command
to enable SSO.

---

**Monitoring High Availability Standby WLC**

You can view the status and health information of active and standby WLC separately. This section describes
the details of getting health information and traps from the standby WLC.

The standby WLC uses the redundancy management interface for any external communications such as when
talking to Syslog, NTP server, TFTP server, and so on. On the standby WLC, the management user
authentication and accounting is performed on the redundancy management interface. RADIUS or TACACS+
server can be used for user authentication, apart from a local management user account. To support this, the
redundancy interface IP address(es) should be added as network device on the RADIUS or TACACS+ server.
The authentication request is sent to RADIUS or TACACS+ server over redundancy management interface.
Whenever you log on to the standby WLC, accounting message is sent to the RADIUS server. The purpose
of the accounting message is to log the admin logon events on the standby WLC console.

This feature is supported on all WLC models supporting HA SSO feature:

- Cisco 8500 Series WLCs
• Cisco Flex 7500 Series WLCs
• Cisco 5500 Series WLCs
• Cisco WiSM2

Events and Notifications

• Trap when WLC becomes Hot Standby—A trap is reported with time stamp when HA peer becomes Hot Standby and the trap shown below is reported

"RF notification EventType:37 Reason :HA peer is Hot-Standby...At:...

A new trap type is added in CISCO-RF-SUPPLEMENTAL-MIB.my

• Trap when Bulk Sync Complete—After the HA pairing is done and Bulk sync is complete, the following trap is reported:

"RF notification EventType:36 Reason :Bulk Sync Completed...At:...

A new trap type is added in CISCO-RF-SUPPLEMENTAL-MIB.my

• Trap when Standby WLC goes down—When the standby peer goes down due to manual reset, crash, memory leak/hang, or moving to maintenance mode, the following trap is reported:

"RF failure notification ErrorType: 34 Reason :Lost Peer, Moving to Active-No-Peer State!

On the CLI, you can view the trap by entering the show traplog command.

• Syslog notification when Admin login on Standby

  1 Admin login to Standby via SSH generates an event in msglog/syslog. The following is a sample system message:

  *emWeb: Mar 06 20:34:42.675: #CLI-3-LOGIN_STANDBY: [SS] cli_lvl7.c:4520 [USER@9 name="admin" from="SSH"] user login success on standby controller.

  You can view this message on the standby WLC by entering the show msglog command.

  2 Admin login to Standby via console generates an event in msglog/syslog. The following is a sample system message:

  *emWeb: Mar 06 20:34:42.675: #CLI-3-LOGIN_STANDBY: [SS] cli_lvl7.c:4520 [USER@9 name="admin" from="console"] user login success on standby controller.

  You can view this message on the standby WLC by entering the show msglog command.

• Peer Process Statistics—The CPU and Memory statistics of all the threads of the standby WLC are synchronized with the active WLC every 10 seconds. This information is displayed when you query for the Peer statistics on the active WLC.

Enter these commands on the active WLC to view the peer process system, CPU, and memory statistics:

  • show redundancy peer-system statistics
  • show redundancy peer-process cpu
  • show redundancy peer-process memory

On the GUI, choose Monitor > Redundancy > Peer Statistics to view the peer process system, CPU, and memory statistics.