Configuring Backup Controllers

Backup Controllers

A single controller at a centralized location can act as a backup for access points when they lose connectivity with the primary controller in the local region. Centralized and regional controllers do not need to be in the same mobility group. You can specify a primary, secondary, and tertiary controller for specific access points in your network. Using the controller GUI or CLI, you can specify the IP addresses of the backup controllers, which allows the access points to fail over to controllers outside of the mobility group.

The following are some guidelines for configuring backup controllers:

• You can configure primary and secondary backup controllers (which are used if primary, secondary, or tertiary controllers are not specified or are not responsive) for all access points connected to the controller as well as various timers, including heartbeat timers and discovery request timers. To reduce the controller failure detection time, you can configure the fast heartbeat interval (between the controller and the access point) with a smaller timeout value. When the fast heartbeat timer expires (at every heartbeat interval), the access point determines if any data packets have been received from the controller within the last interval. If no packets have been received, the access point sends a fast echo request to the controller.

• The access point maintains a list of backup controllers and periodically sends primary discovery requests to each entry on the list. When the access point receives a new discovery response from a controller, the backup controller list is updated. Any controller that fails to respond to two consecutive primary discovery requests is removed from the list. If the access point's local controller fails, it chooses an available controller from the backup controller list in this order: primary, secondary, tertiary, primary backup, and secondary backup. The access point waits for a discovery response from the first available controller in the backup list and joins the controller if it receives a response within the time configured for the primary discovery request timer. If the time limit is reached, the access point assumes that the controller cannot be joined and waits for a discovery response from the next available controller in the list.

• When an access point's primary controller comes back online, the access point disassociates from the backup controller and reconnects to its primary controller. The access point falls back only to its primary controller and not to any available secondary controller for which it is configured. For example, if an access point is configured with primary, secondary, and tertiary controllers, it fails over to the tertiary controller when the primary and secondary controllers become unresponsive. If the secondary controller

comes back online while the primary controller is down, the access point does not fall back to the secondary controller and stays connected to the tertiary controller. The access point waits until the primary controller comes back online to fall back from the tertiary controller to the primary controller. If the tertiary controller fails and the primary controller is still down, the access point then falls back to the available secondary controller.

This section contains the following subsections:

Restrictions for Configuring Backup Controllers

• You can configure the fast heartbeat timer only for access points in local and FlexConnect modes.

Configuring Backup Controllers (GUI)

Step 1   Choose **Wireless** > **Access Points** > **Global Configuration** to open the Global Configuration page.

Step 2   From the Local Mode AP Fast Heartbeat Timer State drop-down list, choose **Enable** to enable the fast heartbeat timer for access points in local mode or choose **Disable** to disable this timer. The default value is Disable.

Step 3   If you chose Enable in Step 2, enter the Local Mode AP Fast Heartbeat Timeout text box to configure the fast heartbeat timer for access points in local mode. Specifying a small heartbeat interval reduces the amount of time it takes to detect a controller failure.

The range for the AP Fast Heartbeat Timeout value for Cisco Flex 7510 Controllers is 10–15 (inclusive) and is 1–10 (inclusive) for other controllers. The default value for the heartbeat timeout for Cisco Flex 7510 Controllers is 10. The default value for other controllers is 1 second.

Step 4   From the FlexConnect Mode AP Fast Heartbeat Timer State drop-down list, choose **Enable** to enable the fast heartbeat timer for FlexConnect access points or choose **Disable** to disable this timer. The default value is Disable.

Step 5   If you enable FlexConnect fast heartbeat, enter the FlexConnect Mode AP Fast Heartbeat Timeout value in the FlexConnect Mode AP Fast Heartbeat Timeout text box. Specifying a small heartbeat interval reduces the amount of time it takes to detect a controller failure.

The range for the FlexConnect Mode AP Fast Heartbeat Timeout value for Cisco Flex 7510 Controllers is 10–15 (inclusive) and is 1–10 for other controllers. The default value for the heartbeat timeout for Cisco Flex 7510 Controllers is 10. The default value for other controllers is 1 second.

Step 6   In the AP Primary Discovery Timeout text box, a value between 30 and 3600 seconds (inclusive) to configure the access point primary discovery request timer. The default value is 120 seconds.

Step 7   If you want to specify a primary backup controller for all access points, enter the IPv4/IPv6 address of the primary backup controller in the Back-up Primary Controller IP Address (IPv4/IPv6) text box and the name of the controller in the Back-up Primary Controller Name text box.

        Note   The default value for the IP address is 0.0.0.0, which disables the primary backup controller.

Step 8   If you want to specify a secondary backup controller for all access points, enter the IPv4/IPv6 address of the secondary backup controller in the Back-up Secondary Controller IP Address (IPv4/IPv6) text box and the name of the controller in the Back-up Secondary Controller Name text box.

        Note   The default value for the IP address is 0.0.0.0, which disables the secondary backup controller.

Step 9   Click **Apply** to commit your changes.

Step 10   Configure primary, secondary, and tertiary backup controllers for a specific access point as follows:

    a) Choose **Access Points** > **All APs** to open the All APs page.

    b) Click the name of the access point for which you want to configure primary, secondary, and tertiary backup controllers.

    c) Choose the **High Availability** tab to open the All APs > Details for (High Availability) page.

    d) If desired, enter the name and IP address of the primary controller for this access point in the Primary Controller text boxes.

> **Note**   Entering an IP address for the backup controller is optional in this step and the next two steps. If the backup controller is outside the mobility group to which the access point is connected (the primary controller), then you need to provide the IP address of the primary, secondary, or tertiary controller, respectively. The controller name and IP address must belong to the same primary, secondary, or tertiary controller. Otherwise, the access point cannot join the backup controller.

    e) If desired, enter the name and IP address of the secondary controller for this access point in the Secondary Controller text boxes.

    f) If desired, enter the name and IP address of the tertiary controller for this access point in the Tertiary Controller text boxes.

    g) Click **Apply** to commit your changes.

Step 11   Click **Save Configuration** to save your changes.

Configuring Backup Controllers (CLI)

Step 1   Configure a primary controller for a specific access point by entering this command:

config ap primary-base *controller_name Cisco_AP* [*controller_ip_address*]

> **Note**   The *controller_ip_address* parameter in this command and the next two commands is optional. If the backup controller is outside the mobility group to which the access point is connected (the primary controller), then you need to provide the IP address of the primary, secondary, or tertiary controller, respectively. In each command, the *controller_name* and *controller_ip_address* must belong to the same primary, secondary, or tertiary controller. Otherwise, the access point cannot join the backup controller.

Step 2   Configure a secondary controller for a specific access point by entering this command:

config ap secondary-base *controller_name Cisco_AP* [*controller_ip_address*]

Step 3   Configure a tertiary controller for a specific access point by entering this command:

config ap tertiary-base *controller_name Cisco_AP* [*controller_ip_address*]

Step 4   Configure a primary backup controller for all access points by entering this command:

config advanced backup-controller primary *system name ip_addr*

> **Note**   This command is valid for both IPv4 and IPv6

Step 5   Configure a secondary backup controller for all access points by entering this command:

config advanced backup-controller secondary *system name ip_addr*

Note To delete a primary or secondary backup controller entry, enter *0.0.0.0* for the controller IPv4/IPv6 address.

Note This command is valid for both IPv4 and IPv6

Step 6 Enable or disable the fast heartbeat timer for local or FlexConnect access points by entering this command:

config advanced timers ap-fast-heartbeat {**local** | **flexconnect** | **all**} {**enable** | **disable**} *interval*

where **all** is both local and FlexConnect access points, and *interval* is a value between 1 and 10 seconds (inclusive). Specifying a small heartbeat interval reduces the amount of time that it takes to detect a controller failure. The default value is disabled.Configure the access point heartbeat timer by entering this command:

config advanced timers ap-heartbeat-timeout *interval*

where *interval* is a value between 1 and 30 seconds (inclusive). This value should be at least three times larger than the fast heartbeat timer. The default value is 30 seconds.

Caution Do not enable the fast heartbeat timer with the high latency link. If you have to enable the fast heartbeat timer, the timer value must be greater than the latency.

Step 7 Configure the access point primary discovery request timer by entering this command:

config advanced timers ap-primary-discovery-timeout *interval*

where *interval* is a value between 30 and 3600 seconds. The default value is 120 seconds.

Step 8 Configure the access point discovery timer by entering this command:

config advanced timers ap-discovery-timeout *interval*

where *interval* is a value between 1 and 10 seconds (inclusive). The default value is 10 seconds.

Step 9 Configure the 802.11 authentication response timer by entering this command:

config advanced timers auth-timeout *interval*

where *interval* is a value between 5 and 600 seconds (inclusive). The default value is 10 seconds.

Step 10 Save your changes by entering this command:

save config

Step 11 See an access point's configuration by entering these commands:

- **show ap config general** *Cisco_AP*

- **show advanced backup-controller**

- **show advanced timers**

Information similar to the following appears for the **show ap config general** *Cisco_AP* command for Primary Cisco Switch IP Address using IPv4:

```
Cisco AP Identifier.............................. 1
Cisco AP Name.................................... AP5
Country code..................................... US  - United States
Regulatory Domain allowed by Country............. 802.11bg:-AB    802.11a:-AB
AP Country code.................................. US  - United States
AP Regulatory Domain............................. 802.11bg:-A    802.11a:-N
Switch Port Number .............................. 1
```

```
MAC Address...................................... 00:13:80:60:48:3e
IP Address Configuration......................... DHCP
IP Address....................................... 1.100.163.133
...
Primary Cisco Switch Name........................ 1-5520
Primary Cisco Switch IP Address.................. 2.2.2.2
Secondary Cisco Switch Name...................... 1-8540
Secondary Cisco Switch IP Address................ 2.2.2.2
Tertiary Cisco Switch Name....................... 2-8540
Tertiary Cisco Switch IP Address................. 1.1.1.4
...
```

Information similar to the following appears for the **show ap config general** *Cisco_AP* command for Primary Cisco Switch IP Address using IPv6:

```
Cisco AP Identifier.............................. 1
Cisco AP Name.................................... AP6
Country code..................................... US - United States
Regulatory Domain allowed by Country............. 802.11bg:-A 802.11a:-A
AP Country code.................................. US - United States
AP Regulatory Domain............................. 802.11bg:-A 802.11a:-A
Switch Port Number .............................. 13
MAC Address...................................... 44:2b:03:9a:9d:30
IPv6 Address Configuration....................... DHCPv6
IPv6 Address..................................... 2001:9:5:96:295d:3b2:2db2:9b47
IPv6 Prefix Length............................... 128
Gateway IPv6 Addr................................ fe80::6abd:abff:fe8c:764a
NAT External IP Address.......................... None
CAPWAP Path MTU.................................. 1473
Telnet State..................................... Globally Disabled
Ssh State........................................ Globally Disabled
Cisco AP Location................................ _5500
Cisco AP Floor Label............................. 0
Cisco AP Group Name.............................. IPv6-Same_VLAN
Primary Cisco Switch Name........................ Maulik_WLC_5500-HA
Primary Cisco Switch IP Address.................. 2001:9:5:95::11
```

Information similar to the following appears for the **show advanced backup-controller** command when configured using IPv4:

```
AP primary Backup Controller .................... controller1 10.10.10.10
AP secondary Backup Controller ................ 0.0.0.0
```

Information similar to the following appears for the **show advanced backup-controller** command when configured using IPv6:

```
AP primary Backup Controller .................... WLC_5500-2 fd09:9:5:94::11
AP secondary Backup Controller .................. vWLC 9.5.92.11
```

Information similar to the following appears for the **show advanced timers** command:

```
Authentication Response Timeout (seconds)........ 10
Rogue Entry Timeout (seconds).................... 1300
AP Heart Beat Timeout (seconds).................. 30
AP Discovery Timeout (seconds)................... 10
AP Local mode Fast Heartbeat (seconds)........... 10 (enable)
AP flexconnect mode Fast Heartbeat (seconds)........... disable
```

```
AP Primary Discovery Timeout (seconds)........... 120
```