Controller Tab

This tab on the menu bar enables you to access the Cisco WLC configuration details. Use the left navigation pane to access specific Cisco WLC parameters.

You can access the following page from the Controller tab:

- General
- Icons
- Inventory
- Interfaces
- Interface Groups
- Multicast
- Network Routes
- Redundancy
- Internal DHCP Server
- Mobility Management
- Ports
- NTP
- CDP
- PMIPv6
- Tunneling
- IPv6
- mDNS
- Advanced

General

Choose **CONTROLLER > General** to navigate to this page.

Table 4-1 Controller Configuration Parameters

Parameter	Description
Name	Controller name
802.3x Flow Control Mode	802.3x flow control mode that you enable or disable when you choose the corresponding line on the drop-down list. By default, this option is disabled.
LAG Mode on next reboot	Link Aggregation Group (LAG) mode that you can set as follows: Enabled—Enables link aggregation on the Cisco WLC. Disabled—Disables link aggregation on the Cisco WLC. LAG is disabled by default on the Cisco 5500 Series Controllers. LAG is supported on Cisco 2500, 2504, 8500, and Flex 7500 Series Controllers. For more information, see the Inventory topic.
Broadcast Forwarding	Broadcast forwarding that you can enable or disable. The default is disabled state.
AP Multicast Mode	IPv4 Packet forwarding policy that the controller uses. Choose one of the following options from the drop-down list: • Unicast—Enables the controller, when it receives a multicast packet, to forward the packet as a unicast packet to all associated access points. • Multicast—Enables the controller to forward a packet as a multicast packet. Enter the IPv4 address of the multicast group in the multicast group address text box. **Note** Cisco 2500 Series controllers support only multicast-multicast mode, and by default the multicast IP address is zero.
AP IPv6 Multicast Mode	IPv6 Packet forwarding policy that the controller uses. Choose one of the following options from the drop-down list: • Unicast—Enables the controller, when it receives a multicast packet, to forward the packet as a unicast packet to all associated access points. • Multicast—Enables the controller to forward a packet as a multicast packet. Enter the IPv6 address of the multicast group in the multicast group address text box. **Note** Cisco 2500 Series controllers support only multicast-multicast mode, and by default the multicast IP address is zero. You must configure the multicast address for IPv6 to function.
AP Fallback	Access point fallback that you can enable or disable. Determines whether or not an access point that lost a primary controller connection automatically returns to service when the primary controller becomes functional again.

Table 4-1 Controller Configuration Parameters

Parameter	Description
CAPWAP Preferred Mode	Select check box to configure CAPWAP Preferred Mode globally. The preferred mode can be either IPv4 or IPv6.
Fast SSID Change	Fast SSID Change that you can enable or disable. When you enable Fast SSID Change, the controller allows clients to move between SSIDs. When the client sends a new association request for a different SSID, the client entry in the controller connection table is cleared before the client is added to the new SSID. When FastSSID Change is disabled, the controller enforces a delay before clients are allowed to move to a new SSID.
Link Local Bridging	Enable to configure bridging of the link local traffic at local site.
Default Mobility Domain Name	Operator-defined Mobility Group Name.
RF Group Name	RF group name. The valid range for the RF group name is 8 to 19 characters. Radio Resource Management (RRM) neighbor packets are distributed among access points within an RF group. Cisco access points only accept RRM neighbor packets sent with this RF group name. The RRM neighbor packets sent with different RF group names are dropped.
User Idle Timeout	Timeout for idle clients in seconds. The factory default is 300. When the timeout expires, the client loses authentication, briefly disassociates from the access point, reassociates, and reauthenticates. The range is 15 to 100000.
ARP Timeout	Timeout in seconds for the Address Resolution Protocol. By default, this is set to 300. The range is 10 to 2147483647.
Web Radius Authentication	PAP, CHAP, or MD5-CHAP password authentication.
Operating Environment	Operating environment for the controller. **Note** Not supported in Cisco Flex 7500 Series Controllers.
Internal Temp Alarm Limits	Acceptable temperature range for operation of the controller. An alarm is triggered if the temperature raises or falls below the range. **Note** Not supported in Cisco Flex 7500 Series Controllers.

Table 4-1 Controller Configuration Parameters

Parameter	Description
WebAuth Proxy Redirection Mode	Mode that enables or disables the web authentication proxy redirection. This feature enables clients that have manual web proxy enabled in the browser to facilitate authentication with the controller. If the client's browser is configured with manual proxy settings (on 8080 or 3128) and if the client requests any URL, the controller responds with a web page prompting the user to change the Internet settings to automatically detect the proxy settings. This is to ensure that the browser's manual proxy settings information does not get lost. After enabling this settings, the user can get access to the network through the web authentication policy. This functionality is given for port 8080 and 3128 because these ports are the most commonly used ports for web proxy server.
WebAuth Proxy Redirection Port	Port numbers on which the controller listens to web authentication proxy redirection. The default ports are 80, 8080, and 3128. If you configured the web authentication redirection port to any port other than these values, you must specify that value.
Global IPv6 Config	Drop-down list from which you can enable or disable the global IPv6 configuration.
Web Color Theme	Drop-down list from which you can select red color as the UI default color.
HA SKU Secondary Unit	Enable or disable the high availability SKU secondary unit.
NAS-ID	Network Access Server identifier. The NAS-ID is sent to the RADIUS server by the controller (as a RADIUS client) using the authentication request, which is used to classify users to different groups. You can enter up to 32 alphanumeric characters. Beginning in Release 7.4 and later releases, you can configure the NAS-ID on the interface, WLAN, or an access point group. The order of priority is AP Group NAS-ID > WLAN NAS-ID > Interface NAS-ID.
HTTP Profiling Port	Enter the port number to be profiled by the WLC. Default value is 80.
DNS Server IP	IP address of the DNS server.
HTTP-Proxy IP Address	IP address of the HTTP-Proxy server.

Icons

Choose **CONTROLLER > Icons** to navigate to this page.

This page identifies icons to be used for the service provider.

Table 4-2 Icon Parameters

Parameter	Description
Filename	Filename of the icon.
File Type	File type of the icon.
Lang Code	Language code.
Width	Width of the icon.
Height	Height of the icon.
Size (KB)	Size of the icon in KB.

Click **Add** to add the icon details.

Inventory

Choose **CONTROLLER > Inventory** to navigate to this page.

This page identifies Cisco WLAN Solution product information assigned by the manufacturer.

Table 4-3 Inventory Parameters

Parameter	Description
Model No.	Model number as defined by the factory.
Burned-in MAC Address	Burned-in Ethernet MAC address for this Cisco WLC management interface.
Maximum number of APs supported	Maximum number of access points supported by the Cisco WLC.
FIPS Prerequisite Mode	Federal Information Processing Standards–US Government requirement for cryptographic modules.
WLANCC Prerequisite Mode	If the shared secret for IPSec is not configured, the default radius shared secret is used. If the authentication method is PSK, WLANCC should be enabled to use the IPSec shared secret.By default, WLANCC is disabled.
UCAPL Prerequisite Mode	If the shared secret for IPSec is not configured, the default radius shared secret is used. If the authentication method is PSK, UCAPL should be enabled to use the IPSec shared secret. By default, UCAPL is disabled.
UDI	
Product Identifier Description	Vendor-specific model name.
Version Identifier Description	Vendor-specific hardware revision.
Serial Number	Unique serial number for this Cisco WLC.
Entity Name	Textual name of the physical entity.
Entity Description	Textual description of the physical entity.

Interfaces

Choose **CONTROLLER > Interfaces** to navigate to this page.

- To edit the parameters for an interface, click the interface name (Interfaces > Edit).
- To remove an interface, hover your cursor over the blue drop-down arrow for the interface and choose **Remove**. You are prompted for confirmation of the interface removal.

Table 4-4 Controller Interface Parameters

Parameter	Description
Interface Name	Name of the interface: • Management—802.11 Distribution System wired network. • Redundancy-management—Interface used for peer to peer communication using a gateway. This interface appears irrespective of the state of redundancy. • Redundancy-port—Interface used for peer to peer communication. Role negotiation, config sync are done using this port. This interface appears irrespective of the state of redundancy. • Service-port—System Service interface. • Virtual—Unused IP address used as the virtual gateway address. • AP-manager—Can be on the same subnet as the management IP address, but must have a different IP address than the management interface. • <name>—Operator-Defined Interface assignment, without any spaces.
VLAN Identifier	Virtual LAN assignment of the interface.
IP Address	IPv4 address of the Cisco WLC and its distribution port.
Interface Type	Static—Management, AP-Manager, Service-Port, and Virtual interfaces. Dynamic—Operator-defined interfaces.
Dynamic AP Management	Dynamic access point management status. The status could be Enabled, Disabled, or Not Supported. This option is disabled by default when LAG is enabled, and any other user-defined dynamic interface is deleted.
IPv6 Address	IPv6 address of the Cisco WLCs management and service port.

Buttons

- New**:** Adds a new interface.

Interfaces > New

Choose **CONTROLLER > Interfaces** and then **New** to navigate to this page.

Add a new Cisco WLC operator-defined interface by entering the following parameters:

- Interface Name—Enter the name of the new operator-defined interface without any spaces. The interface name can be up to 32 characters and can include special characters.
- VLAN Id—Enter the VLAN identifier for this new interface, or enter **0** for an untagged VLAN.

Note IPv6 is not supported on Dynamic Interface.

Buttons

- Back: Returns to the previous page.
- Apply: Displays the Interfaces > Edit page and continues configuring the new operator-defined interface.

Interfaces > Edit

Choose **CONTROLLER > Interfaces** and then click on an interface name to navigate to this page.

The top of this page displays the operator-defined Interface Name, and may include the interface MAC address.

Edit Management, VLAN, Operator-Defined, Service Port, Virtual, and AP-Manager interfaces as described in the following tables.

Management Interface Parameters

Note If you made any changes to the management interface, reboot the controller so that your changes take effect.

Note The IPv4 and IPv6 configurations cannot be changed in redundancy mode.

Table 4-5 Management Interface Parameters

Parameter	Description
General Information	
Interface Name	Name of the interface.
MAC Address	MAC address of the interface.
Configuration	
Quarantine	Quarantine status. Check the check box to indicate that this VLAN is a quarantine VLAN. When a client is assigned to a quarantine VLAN, its data switching is always central.

Table 4-5 Management Interface Parameters

Parameter	Description
Quarantine VLAN ID	Quarantine VLAN ID. Enter a nonzero value for the quarantine VLAN ID. **Note** We recommend that you configure unique quarantine VLANs throughout your network. If multiple controllers are configured in the same mobility group and access interfaces on all controllers are in the same subnet, you must have the same quarantine VLAN if there is only one NAC appliance in the network. If multiple controllers are configured in the same mobility group and access interfaces on all controllers are in different subnets, you must have different quarantine VLANs if there is only one NAC appliance in the network.
NAS-ID	ID that is sent to the RADIUS server by the controller through an authentication request to classify users to different groups so that the RADIUS server can send a customized authentication response.
NAT Address **Note** This option is available only for Cisco WLCs that are configured for dynamic AP management.	
Enable NAT Address	NAT addresses that you can enable. Check the check box to deploy the Cisco WLC behind a router or other gateway device that is using a one-to-one mapping network address translation (NAT). NAT allows a device, such as a router, to act as an agent between the Internet (public) and a local network (private). In this case, it maps the controller's Intranet IP addresses to a corresponding external address. The controller's dynamic AP-manager interface must be configured with the external NAT IP address so that the controller can send the correct IP address in the Discovery Response.
NAT IP Address	External NAT IP address.
Interface Address	
VLAN Identifier	Virtual LAN assigned to the interface. Enter **0** for an untagged VLAN or a nonzero value for a tagged VLAN. We recommend using tagged VLANs for the management interface. **Note** For Cisco 5500 Series Controllers in a nonlink-aggregation (non-LAG) configuration, the management interface must be on a different VLAN than any dynamic AP-manager interface. Otherwise, the management interface cannot fail over to the port that the AP-manager is on.
IP Address	IPv4 address of the interface.
Netmask	Interface subnet mask (IPv4).
Gateway	Interface gateway router IP address.
IPv6 Address	IPv6 address of the interface.
Prefix Length	Interface subnet mask (IPv6).
IPv6 Gateway	Link local address of the interface gateway router. **Note** An error is thrown when the IPv6 gateway is not a link local IPv6 address.

Table 4-5 Management Interface Parameters

Parameter	Description
Link Local IPv6 Address	IPv6 unicast address that is configured on the interface. Link local IPv6 address is used for addressing a single link for automatic address configuration or neighbor discovery protocol.
Physical Information	
Port Number	Primary port for the interface.
Backup Port	Backup port. If the primary port for an interface fails, the interface moves to the backup port.
Active Port	Active port for the interface.
Enable Dynamic AP Management	AP-manager interface. **Note** Only one AP-manager interface is allowed per physical port. A dynamic interface that is marked as an AP-manager interface cannot be used as a WLAN interface. ⚠ **Caution** Do not define a backup port for an AP-manager interface. Port redundancy is not supported for AP-manager interfaces. If the AP-manager interface fails, all of the access points connected to the controller through that interface are evenly distributed among the other configured AP-manager interfaces.
DHCP Information	
Primary DHCP Server	Interface that uses this DHCP server first to obtain an IPv4 address. **Note** IPv6 is not supported for DHCP.
Secondary DHCP Server	Interface that uses this DHCP server as a backup to obtain an IP address. **Note** IPv6 is not supported for DHCP.

Table 4-5 Management Interface Parameters

Parameter	Description
DHCP Proxy Mode	Drop-down list from which you can choose the DHCP Proxy Mode that can be one of the following: • Global—Uses the global DHCP proxy mode on the controller. • Enabled—Enables the DHCP proxy mode on the interface. When you enable DHCP proxy on the controller, the controller unicasts the DHCP requests from the client to the configured servers. You must configure at least one DHCP server on either the interface associated with the WLAN or on the WLAN. • Disabled—Disables the DHCP proxy mode on the interface. When you disable the DHCP proxy on the controller, the DHCP packets transmitted to and from the clients are bridged by the controller without any modification to the IP portion of the packet. Packets received from the client are removed from the CAPWAP tunnel and transmitted on the upstream VLAN. DHCP packets directed to the client are received on the upstream VLAN, converted to 802.11, and transmitted through a CAPWAP tunnel toward the client. As a result, the internal DHCP server cannot be used when DHCP proxy is disabled. **Note** The DHCP Proxy mode is disabled by default when the interface uses IPv6 address. DHCP does not support IPv6.
Enable DHCP Option 82	Check box that allows you to enable the DHCP Option 82 on the dynamic interface. DHCP option 82 provides additional security when DHCP is used to allocate network addresses.
Enable DHCP Option 82-Link Select	Option 82-Link Select pads the extra information to get the IP address in the required subnet.
Link Select relay source	Allows to specify the required interface/subnet on which the DHCP client require an IP address.
Enable DHCP Option 82 - VPN Select	Enables the VPN select. This is used in conjunction with the link select relay source.
VPN select - VRF Name	VPN Select-VRF Name is a string that is used to select a DHCP pool based on the VRF name.
VPN select - VPN ID	VPN Select-VPN ID is an ASCII value that is used to select a DHCP pool based on the identifier.
Access Control List	
ACL Name	Drop-down list from which you can choose an IPv4 ACL. **Note** Applying an ACL to the management interface does not affect wired devices. To block access to wired devices, you must configure an ACL on the upstream device port.
IPv6 ACL Name	Drop-down list from which you can choose an IPv6 ACL. **Note** Guest LAN does not support IPv6 ACL.

Table 4-5 Management Interface Parameters

Parameter	Description
URL ACL	Drop-down list from which you can choose the URL ACL profile for the interface. Interface URL ACL profiles have higher priority than WLAN URL ACL profiles.
mDNS	
mDNS Profile	Drop-down list from which you can choose the mDNS profile for the interface. Interface mDNS profiles have higher priority than WLAN mDNS profiles. Clients receive service advertisements only for the services associated with the profile.

Redundancy-Management Interface Parameters

Table 4-6 Redundancy-Management Interface Parameters

Parameter	Description
General Information	
Interface Name	Name of the interface.
Interface Address	
IP Address	IP address of the interface.

Service Port Interface Parameters

Table 4-7 Service Port Interface Parameters

Parameter	Description
General Information	
Interface Name	Name of the interface.
MAC Address	MAC address of the interface.
Interface Address	
IPv4	
DHCP Protocol	Check box that you check to have the Service Port interface use a DHCP server to obtain its IP address.
IP Address	IP address of the Service Port interface.
Netmask	Interface subnet mask.
Note The service port cannot be configured with the same IP address or on the same subnet as the network distribution system.	
IPv6	
SLACC	Enable SLACC to auto-configure the IPv6 address. You can configure a static IPv6 address by disabling the check box.
Primary Address	This field is enabled for static IPv6 configuration. Enter the IPv6 address. For SLACC, the service port generates the IPv6 address provided a valid prefix length is used.

Table 4-7 Service Port Interface Parameters

Parameter	Description
Prefix Length	Enter IPv6 prefix length of the management interface. The valid prefix length is between 1-127.
Link Local Address	The link-local IPv6 address.

Virtual Interface Parameters

Note If you made any changes to the virtual interface, reboot the controller so that your changes take effect.

Table 4-8 Virtual Interface Parameters

Parameter	Description
General Information	
Interface Name	Name of the interface.
MAC Address	MAC address of the interface.
Interface Address	
IP Address	Gateway IP address. Any fictitious, unassigned IP address (such as 10.1.10.1) to be used by Layer 3 Security and Mobility managers. Reboot the Cisco WLC to have this change take effect.
DNS Host Name	Gateway hostname. Used by Layer 3 Security and Mobility managers to verify the source of certificates when Web Auth is enabled. Reboot the Cisco WLC to have this change take effect.
Note You must configure the virtual gateway address to enable Layer 3 Web Auth, configured on the Editing WLANs page.	

AP-Manager Interface Parameter

Note For Cisco 5508 WLCs, you do not have to configure an AP-manager interface because the management interface acts like an AP-manager interface by default.

Table 4-9 AP Manager Interface Parameters

Parameter	Description
General Information	
Interface Name	Name of the interface.
MAC Address	MAC address of the interface.
Interface Address	
VLAN Identifier	Virtual LAN assigned to the interface.
IP Address	IP address of the Cisco WLC Layer 3 CAPWAP protocol manager. This IP address cannot be the same IP address used by the management interface.

Table 4-9 AP Manager Interface Parameters

Parameter	Description
Netmask	Interface subnet mask.
Gateway	Interface gateway router IP address.
Physical Information	
Port Number	Primary port for the interface.
Backup Port	Backup port. If the primary port for an interface fails, the interface moves to the backup port.
Active Port	Active port for the interface.
Enable Dynamic AP Management	AP-Manager interface. Select the check box to indicate that the interface is an AP-manager interface. **Note** This enables only IPv4 based AP manager for dynamic interface.
DHCP Information	
Primary DHCP Server	DHCP server that the interface uses first to obtain an IP address.
Secondary DHCP Server	DHCP server that the interface uses as a backup to obtain an IP address.
Access Control List	
ACL Name	Access control list names currently available on the Access Control Lists page.

Buttons

- Back: Returns to the previous page.
- Apply: Sends data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

Note Applying interface changes may cause WLANs to temporarily drop client connections. You are prompted to confirm the changes if this is the case.

Interface Groups

Interface groups are logical groups of interfaces. Interface groups facilitate user configuration where an interface group can be reused either while configuring multiple WLANs or while overriding a WLAN interface per AP group. An interface group can contain either quarantine or nonquarantine interfaces.

A WLAN can be mapped to a single interface or multiple interfaces using an interface group. Wireless clients that are associated to this WLAN get their IP addresses from a pool of subnets that are identified by the interfaces using a MAC based hashing algorithm.

VLAN select feature also enables you to associate a client to different subnets based on the foreign controller that they are connected to. The anchor controller maintains a mapping between the foreign MAC and the interface group.

Choose **CONTROLLER > Interface Groups** to navigate to this page.

- To edit the parameters for an interface, click the interface name (Interfaces > Edit).

- To remove an interface group, hover your cursor over the blue drop-down arrow for the interface group and choose **Remove**. You are prompted for confirmation of the interface group removal.

Note A WLAN can be mapped to a single interface or multiple interfaces. A maximum of 20 interfaces can be added to an interface group.

Table 4-10 Controller Interface Groups Parameters

Parameter	Description
Interface Group Name	Name of the interface group.
Description	Description for the interface group.
mDNS Profile	Drop-down list from which you can choose the mDNS profile for the interface group. Clients receive service advertisements only for the services associated with the profile. Interface group mDNS profiles have higher priority than WLAN mDNS profiles.

Buttons

Add Group**:** Adds a new interface group.

Interface Groups > Add Group

Choose **CONTROLLER > Interface Groups** and then click **Add Group** to navigate to this page.

Add a new Cisco WLC operator-defined interface group by entering the following parameters:

- Interface Group Name—Enter the name of the new operator-defined interface group. The interface group name can be up to 32 characters and can include special characters.
- Description—Enter the description for this new interface group.

Buttons

- Add: Adds a new interface group.
- Cancel: Disregards any settings or changes.

Interface Groups > Edit

Choose **CONTROLLER > Interface Groups** and then click on an interface group name to navigate to this page.

Table 4-11 Management Interface Parameters

Parameter	Description
Interface Group Name	Name of the interface group.
Property	Quarantine status of the VLAN.

Table 4-11 Management Interface Parameters

Parameter	Description
Interface Name	Name of the interface.
Add Interface	Add Interface button that allows you to add an interface to the interface group. You can choose the interface to add from the Interface Name drop-down list.

Buttons

- Back: Returns to the previous page.
- Apply: Sends data to the controller, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

Multicast

Choose **CONTROLLER** > **Multicast** to navigate to this page.

This page enables you to configure Internet Group Management Protocol (IGMP) snooping and to set the IGMP timeout.

When you enable IGMP snooping, the controller gathers IGMP reports from the clients and then sends each access point a list of the clients that are listening to any multicast group. The access points then forward multicast packets only to those clients.

Table 4-12 Multicast

Parameter	Description
Enable Global Multicast Mode	Multicast mode that you can enable or disable. Disabled—Disables multicast support on the Cisco WLC (default). Unicast—Enables the controller when it receives a multicast packet to forward the packet as a unicast packet to all the associated access points. FlexConnect supports only Unicast Mode. Multicast—Enables multicast support on the Cisco WLC. Enter the IP address of the multicast group in the Multicast Group Address text box.
Enable IGMP Snooping	IGMP snooping that you can enable or disable. The default is enable.
IGMP Timeout (seconds)	IGMP timeout, in seconds. Valid values are from 30 and 7200. When the timeout expires, the controller sends a query on all WLANs, causing all clients that are listening to a multicast group to send a packet back to the controller.
IGMP Query Interval (seconds)	IGMP query interval, in seconds that you can set. The query interval value is the frequency at which the controller sends the IGMP queries. Valid range is from 15 and 2400 seconds.
Enable MLD Snooping	Multicast Listener Discovery (MLD) that you can enable for efficient distribution of IPv6 multicast data to clients and routers in a switched network. By default it is enabled. To enable IPv6 multicast, both Global Multicast Mode and MLD snooping must be enabled.

Table 4-12 Multicast

Parameter	Description
MLD Timeout (seconds)	MLD timeout, in seconds. Valid values are from 30 and 7200. When the timeout expires, the controller sends a query on all WLANs, causing all clients that are listening to a multicast group to send a packet back to the controller.
MLD Query Interval (seconds)	MLD query interval, in seconds that you can set. The query interval value is the frequency at which the controller sends the MLD queries. Valid range is from 15 and 2400 seconds.

Buttons

- Apply: Sends data to the Cisco WLC but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

Network Routes

This page provides a summary of existing IPv4 and IPv6 based service port network routes to network or element management systems on a different subnet. You can choose **IP Address**, **IP Netmask**, or **Gateway IP Address**.

Network Routes > IPv4 Routes

This page provides a summary of existing IPv4 based service port network routes to network or element management systems on a different subnet. You can choose **IP Address**, **IP Netmask**, or **Gateway IP Address**.

- To remove a network route, hover your cursor over the blue drop-down arrow for the route and choose **Remove**. You are prompted to confirm the Network Route removal.

Buttons

New: Adds a new IPv4 based network route.

IPv4 Routes > New

Choose **CONTROLLER > Network Routes > IPv4 Routes** and then click **New** to navigate to this page.

To add a new network route for the service port.

- Route Type—Select IPv4 as the route type.

Enter the following information in the text boxes:

- IP Address—Destination network IP address range
- IP Netmask—Destination subnet mask
- Gateway IP Address—IP address of the service port gateway router

Buttons

- Back: Returns to the previous page.

Apply: Sends data to the Cisco WLC but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

Network Routes > IPv6 Routes

Choose **CONTROLLER** > **Network Routes > IPv6 Routes** to navigate to this page.

This page provides a summary of existing IPv6 based service port network routes to network or element management systems on a different subnet. You can choose **IP Address**, **IP Netmask**, or **Gateway IP Address**.

- To remove a network route, hover your cursor over the blue drop-down arrow for the route and choose **Remove**. You are prompted to confirm the Network Route removal.

Buttons

New: Adds a new IPv6 based network route.

IPv6 Routes > New

Choose **CONTROLLER** > **Network Routes > IPv6 Routes** and then click **New** to navigate to this page.

To add a new network route for the service port.

Route Type—Select IPv6 as the route type.

Enter the following information in the text boxes:

- IP Address—Destination network IP address range
- IP Netmask/Prefix Length—The prefix length assigned to the destination IPv6 address.
- Gateway IP Address—IP address of the service port gateway router

Buttons

- Back: Returns to the previous page.

Apply: Sends data to the Cisco WLC but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

Fabric Configuration > Control Plane

Choose **CONTROLLER** > **Fabric Configuration > Control Plane** to navigate to this page.

You can enable fabric and configure parameters on the enterprise and guest controllers, using the **Fabric Enable/Disable** button at the top of the screen.

Table 4-13 Fabric Control Plane Configuration Details

Parameter	Description
Enterprise	
Primary IP Address	Primary IP address for the enterprise fabric.
Pre Shared Key	The secret value for the pre-shared key.
Secondary IP Address	Secondary IP address for the enterprise fabric.
Pre Shared Key	The secret value for the pre-shared key.
Connection Status	Displays the connection status.
Guest	
Primary IP Address	Primary IP address for the guest fabric.
Pre Shared Key	The secret value for the pre-shared key.
Secondary IP Address	Secondary IP address for the guest fabric.
Pre Shared Key	The secret value for the pre-shared key.
Connection Status	Displays the connection status.

Fabric Configuration > Interface

Choose **CONTROLLER** > **Fabric Configuration > Interface** to navigate to this page.

This page provides a summary of existing fabric networks. You can view the Fabric Interface Name, L2 Instance ID, Network IP address, IP subnet mask, and L3 Instance ID. To remove a fabric interface, hover your cursor over the blue drop-down arrow for the interface and choose **Remove**. You are prompted to confirm the Fabric Interface removal.

Buttons

New: Adds a new fabric interface.

Table 4-14 Fabric Interface Configuration Details

Parameter	Description
Fabric Interface Name	Identifier for the enterprise fabric.
L2 Instance ID	Layer 2 instance ID.
Network IP	IP address of the network.
Subnet Mask	Subnet mask.
L2 Instance ID	Layer 3 instance ID.

Buttons

Apply: Commits your changes.

Fabric Configuration > Templates

Choose **CONTROLLER** > **Fabric Configuration > Templates** to navigate to this page.

This page provides a summary of existing fabric configuration templates. You can view the Fabric ACL templates and its Status. To remove a fabric template, hover your cursor over the blue drop-down arrow for the interface and choose **Remove**. You are prompted to confirm the Fabric Template removal.

Buttons

New: Adds a new fabric template.

Copy: Copies parameters from an existing template.

Table 4-15 Fabric Template Copy Details

Parameter	Description
Fabric Template Name	Identifier for the enterprise fabric template.
Existing Fabric Templates	Lists the existing templates.

Buttons

Apply: Commits your changes.

Redundancy

In a high availability (HA) architecture, one controller is in the Active state and a second controller is in the Standby state, which continuously monitors the health of the Active controller through a direct wired connection over a dedicated HA port. Both controllers share the same configurations including the IP address of the management interface.

Choose **CONTROLLER > Redundancy to configure the redundancy parameters and peer network routes:**

- To enable redundancy and configure redundancy parameters on the primary and secondary controllers, choose **CONTROLLER > Redundancy > Global Configuration**.
- To configure service port network routes for the peer controller, choose **CONTROLLER > Redundancy > Peer Network Route**.

Redundancy > Global Configuration

Choose **CONTROLLER** > **Redundancy > Global Configuration** to navigate to this page.

You can enable redundancy and configure redundancy parameters on the primary and secondary controllers.

The controllers reboot to negotiate the HA role based on the configuration. The standby controller downloads the configuration from the active controller and reboots. In the next bootup process, after the role of the controller is determined, the standby controller tries to validate the configuration again to establish itself as the controller in the Standby state.

After the controllers are rebooted and the XML configuration is synchronized, the active controller transitions to the Active state, and the standby controller transitions to the Standby HOT state. From this point, GUI, Telnet, and SSH for the standby controller on the management interface do not work because all the configurations and management have to be done through the active controller. The standby controller can only be managed through the console or the service port. Also, when a controller transitions to the Standby HOT state, the Standby keyword is automatically appended to the prompt of the controller.

To see the redundancy status of the active controller, choose **Monitor > Redundancy > Summary** to navigate the Redundancy Summary page.

Table 4-16 Global Configuration Parameters

Parameter	Description
Redundancy Mgmt IP	Redundancy Management IP address of the controller. Ensure that the Redundant Management IP address for both controllers is the same.
Peer Redundancy Mgmt IP	Redundancy Management IP address of the peer controller. Ensure that the Peer Redundant Management IP address for both the controllers is the same.
Redundancy port IP	IP address of the redundancy port of the controller. Controllers in a HA environment use the redundancy port to do HA role negotiation. The redundancy port is responsible for configuration and operational data synchronization between active and standby controllers.
Peer Redundancy port IP	IP address of the redundancy port of the peer controller. The redundancy port in standalone controllers and the redundancy VLAN in Cisco WiSM2 are assigned an automatically generated IP address where the last two octets are picked from the last two octets of the Redundancy Management Interface. The first two octets are always 169.254. For example, if the IP address of the Redundancy Management Interface is 209.165.200.225, the IP address of the redundancy port is 169.254.200.225.
Redundant Unit	Controller that can be primary or secondary.
Mobility MAC Address	MAC address that is an identifier for the active and standby controller pair. If an HA pair is 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	Timer that controls how often the primary controller sends a heartbeat keepalive signal to the standby controller. The range is from 100 to 1000 milliseconds, in multiples of 50.
Keep Alive Retries	The number of times keep alive packets are send between the HA peers. The valid range is between 100 to 1000 milliseconds.

Table 4-16 Global Configuration Parameters

Parameter	Description
Peer Search Timer	Timer that controls how often the primary controller sends a peer search signal to the standby controller. The range is from 60 to 300 seconds.
Management Gateway Failure	If the Management interface gateway is unreachable, then the HA tigger can be enabled /disabled.
SSO	Drop-down list from which you can choose **Enable** to enable AP and client SSO. After you enable an SSO, the service port peer IP address and the service port netmask appear on the configuration page. 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 high availability, 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 HA role through the redundant port based on the configuration. If the controllers cannot reach each other through the redundant port or through the Redundant Management Interface, the standby controller goes into the maintenance mode.
Service Port Peer IP	IP address of the service port of the peer controller. When the HA pair becomes available and operational, you can configure the peer service port IP address and netmask when 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 page.
Service Port Peer Netmask	Netmask of the service port of the peer controller.

Buttons

- Apply: Commits your changes.
- Save Configuration: Saves the changes

Redundancy > Peer Network Route

Choose **CONTROLLER** > **Redundancy > Peer Network Route** to navigate to this page.

This page provides a summary of 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. To remove a peer network route, hover your cursor over the blue drop-down arrow for the route and choose **Remove**. You are prompted to confirm the Network Route removal.

Buttons

- New: Adds a new peer network route.

Internal DHCP Server

Choose **CONTROLLER > Internal DHCP Server** to navigate to this page. From here you can choose the following:

- **CONTROLLER > Internal DHCP Server** > **DHCP Scope** to view the existing DHCP server scopes.

  See Internal DHCP Server > DHCP Scope for more information.
- **CONTROLLER > Internal DHCP Server** > **DHCP Allocated Lease** to view the MAC address, the IP address, and the remaining lease time for wireless clients.

  See Internal DHCP Server > DHCP Allocated Lease for more information.

Internal DHCP Server > DHCP Scope

Choose **CONTROLLER > Internal DHCP Server** > **DHCP Scope** to navigate to this page.

The controllers have built-in DHCP relay agents. However, when you want network segments that do not have a separate DHCP server, the controllers can have built-in DHCP scopes (Dynamic Host Configuration Protocol servers) that assign IP addresses and subnet masks to wireless clients, direct-connect access points, appliance-mode access points on the management interface, and DHCP requests that are relayed from access points. (Only lightweight access points are supported.)

Typically, one Cisco WLC can have one or more DHCP scopes that each provide a range of IP addresses. This page shows the existing DHCP server scope names.

Each DHCP Scope displays the following entries, which are a subset of those set on the DHCP Scope > Edit page:

- Scope Name
- Address Pool—IP address range. This pool must be unique for each DHCP scope and must not include the static IP addresses of routers and other servers
- Lease Time—Number of seconds that an IP address is granted to a client or access point
- Status—Scope is Enabled or Disabled

Click the scope name to go to the DHCP Scope > Edit page to change the DHCP scope settings.

Remove a DHCP Scope by hovering your cursor over the blue drop-down arrow and choosing **Remove**. You are prompted to confirm the DHCP Scope removal.

Buttons

- New**:** Creates a new DHCP Scope.

DHCP Scope > New

Choose **CONTROLLER > Internal DHCP Server** > **DHCP Scope** and then click **New** to navigate to this page.

The controllers have built-in DHCP relay agents. However, if you want network segments that do not have a separate DHCP server, the controllers also have built-in DHCP scopes (servers) that assign IP addresses and subnet masks to wireless clients, direct-connect access points, appliance-mode access points on the management interface, and DHCP requests that are relayed from access points. (Only lightweight access points are supported.)

Typically, one Cisco WLC can have one or more DHCP scopes that each provide a range of IP addresses. This page enables you to add a DHCP server scope name.

Add a new DHCP scope by entering the DHCP scope name and then clicking **Apply**. The Cisco WLAN Solution saves the DHCP scope name and returns you to the Internal DHCP Server > DHCP Scope page. On the Internal DHCP Server > DHCP Scope page, click the scope name to set the DHCP scope parameters on the DHCP Scope > Edit page.

Buttons

- Back: Returns to the previous page.
- Apply: Sends data to the Cisco WLC but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

DHCP Scope > Edit

Choose **CONTROLLER > Internal DHCP Server > DHCP Scope** and then click the scope name to navigate to this page.

The controllers have built-in DHCP relay agents. However, when you want network segments that do not have a separate DHCP server, the controllers also have built-in DHCP scopes (servers) that assign IP addresses and subnet masks to wireless clients, direct-connect access points, appliance-mode access points on the management interface, and DHCP requests that are relayed from access points. (Only lightweight access points are supported.)

Typically, one Cisco WLC can have one or more DHCP scopes that each provide a range of IP addresses. This page enables you to edit a DHCP server scope.

This page shows the name of the DHCP Scope you are editing.

Table 4-17 DHCP Scope Parameters

Parameters	Description
Pool Start Address	Starting IP address in the range assigned to clients and access points. This pool must be unique for each DHCP scope. The pool must not include the static IP addresses of routers and other servers.
Pool End Address	Ending IP address in the range assigned to clients and access points. This pool must be unique for each DHCP scope. The pool must not include the static IP addresses of routers and other servers.
Network	Network served by this DHCP scope. This IP address is used by the management interface with the netmask applied, listed on the Interfaces page.
Netmask	Subnet mask assigned to all clients and access points.

Table 4-17 DHCP Scope Parameters

Parameters	Description
Lease Time	How many seconds an IP address is granted to a client or access point, from 120 to 8640000.
DNS Domain Name	Optional DNS (Domain Name System) domain name of this DHCP scope for use with one or more DNS servers.
DNS Servers	IP address of the optional DNS servers. Each DNS server must be able to update a client DNS entry to match the IP address assigned by this DHCP scope.
NetBIOS Name Servers	IP address of the optional Microsoft NetBIOS (Network Basic Input Output System) name servers, such as a WINS (Windows Internet Naming Service) server.
Status	Setting that enables you to configure the DHCP scope. The values can be Enable or Disable.

Buttons

- Back: Returns to the previous page.
- Apply: Sends data to the Cisco WLC but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

Internal DHCP Server > DHCP Allocated Lease

Choose **CONTROLLER > Internal DHCP Server > DHCP Allocated Leases** to navigate to this page.

This page displays the MAC address, the IP address, and the remaining lease time for wireless clients.

Mobility Management

Choose **CONTROLLER > Mobility Management** to navigate to this page. From here you can choose the following:

- **CONTROLLER > Mobility Management > Mobility Configuration** to configure hierarchical mobility on the controller.

  See Mobility Management > Mobility Configuration for more information.
- **CONTROLLER > Mobility Management > Mobility Groups** to view existing mobility group members.

  See Mobility Management > Mobility Groups for more information.
- **CONTROLLER > Mobility Management > Mobility Anchor Config** to configure the symmetric mobility tunneling for mobile clients.

  See Mobility Management > Mobility Anchor Configuration for more information.

- **CONTROLLER > Mobility Management > Multicast Messaging** to configure the controller to use multicast to send the Mobile Announce messages.

  See Mobility Management > Mobility Multicast Messaging for more information.
- **CONTROLLER > Mobility Management > Switch Peer Group** to view existing mobility switch peer groups and their details.

  See Mobility Management > Switch Peer Group for more information.
- **CONTROLLER > Mobility Management > Switch Peer Group Member** to add or remove members to the switch peer group.

  See Mobility Management > Switch Peer Group Member for more information.
- **CONTROLLER > Mobility Management > Mobility Controller** to view all the mobility controllers and their link status.

  See Mobility Management > Mobility Controllers for more information.
- **CONTROLLER > Mobility Management > Mobility Clients** to view all the mobility clients and their parameters.

  See Mobility Management > Mobility Clients for more information.

Mobility Management > Mobility Configuration

Choose **CONTROLLER > Mobility Management > Mobility Configuration** to navigate to this page.

This page allows you to enable New Mobility and configure its parameters.

Table 4-18 Mobility Configuration Parameters

Parameter	Description
General	
Enable New Mobility	Check box that you can check to enable or disable New Mobility. **Note** When you enable hierarchical mobility, you must save the configuration and reboot the controller.
Mobility Parameters	
Mobility Oracle	Check box that you can select to enable the controller as a Mobility Oracle. The Mobility Oracle is optional, it maintains the client database under one complete mobility domain.
Multicast Mode	Check box that you can select to enable or disable multicast mode in a mobility group.
Multicast IP Address	Multicast IP address of the switch peer group.
Mobility Oracle IP Address	IP address of the Mobility Oracle. You cannot enter the value if you have checked the Mobility Oracle check box.
Mobility Controller Public IP Address	IP address of the controller, if there is no NAT. If the controller has NAT configured, the public IP address will be the NATed IP address.

Table 4-18 Mobility Configuration Parameters

Parameter	Description
Mobility Keep Alive Interval	Amount of time (in seconds) between each ping request sent to an peer controller. The valid range is 1 to 30 seconds, and the default value is 10 seconds.
Mobility Keep Alive Count	Number of times a ping request is sent to an peer controller before the peer is considered to be unreachable. The valid range is 3 to 20, and the default value is 3.
Mobility DSCP Value	DSCP value that you can set for the mobility controller. The valid range is 0 to 63, and the default value is 0.

Buttons

- Apply**:** Sends data to the controller but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

Mobility Management > Mobility Groups

Choose **CONTROLLER > Mobility Management > Mobility Groups** to navigate to this page.

This page lists existing mobility group members by their MAC address and IP address and also indicates whether the mobility group member is local (this Cisco WLC) or remote (any other mobility group member). The first entry is the local Cisco WLC, which cannot be deleted. The following entries are other controllers in the mobility group that can be deleted at any time by choosing **Remove**. You can also view the hash key of the virtual controller in your domain.

Note You can ping any of the static mobility group members by choosing **Ping**.

You set the Mobility Group Name that is set on the General page.

Buttons

- New**:** Adds a new mobility group member.
- Edit All: Displays the Mobility Group Member > Edit All page.

Mobility Group Member > New

Choose **CONTROLLER > Mobility Management > Mobility Groups** and then click **New** to navigate to this page.

This page enables you to add mobility group members.

- Member IP Address—Enables you to enter the management interface IP address of the controller to be added. Both, IPv4 and IPv6 are supported.

Note If you are configuring the mobility group in a network where network address translation (NAT) is enabled, enter the IP address sent to the controller from the NAT device rather than the controller's management interface IP address. Otherwise, mobility will fail among controllers in the mobility group.

Also, client mobility among controllers works only if you enable auto-anchor mobility or symmetric mobility tunneling. Asymmetric tunneling is not supported when mobility controllers are behind a NAT device.

- Public IP Address(IPv4/IPv6)—IP address of the Cisco WLC if there is no NAT.
- Member MAC Address—Enables you to enter the MAC address of the controller to be added. Both, IPv4 and IPv6 are supported.
- Group Name—Enables you to enter the name of the mobility group.

Note The mobility group name is case sensitive.

- Hash—Enables you to configure hash key of the peer mobility controller. This is not supported for IPv6 members.

Note You must configure the hash only if the peer mobility controller is a virtual controller.

Buttons

- Back: Returns to the previous page.
- Apply: Sends data to the Cisco WLC but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

Mobility Group Member > Edit All

Choose **CONTROLLER > Mobility Management > Mobility Groups** and then click **Edit All** to navigate to this page.

This page enables you to edit all the existing Mobility Group members' MAC addresses, IPv4 and IPv6 addresses in a text box and then to cut and paste all the entries from one Cisco WLC to the other controllers in the mobility group.

You can edit existing entries in the box and/or paste new entries into the box. In all cases, leave one space between the MAC address and IP address on each line.

The text box on this page makes it easy to avoid data-entry errors while copying the mobility group members list to all the controllers in the same mobility group. Some guidelines are as follows:

- Notice that the text box starts with the local Cisco WLC MAC address and IPv4/IPv6 address.
- In the text box, add the MAC addresses, IPv4/IPv6 addresses, and the mobility group name for the rest of the controllers in the same geographical location (such as a campus or building) that you want to add to the static mobility group.

- When you have added all the Cisco WLC MAC addresses and IP v4/IPv6 addresses to the static mobility group, you can cut and paste the complete list into the corresponding boxes in the Mobility Group Member > Edit All pages in other mobility group member Web User Interface pages.

Note The mobility Group supports a maximum of 72 mobility peers.

Buttons

- Back: Returns to the previous page.
- Apply: Sends data to the Cisco WLC but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

Mobility Management > Mobility Anchor Configuration

Choose **CONTROLLER > Mobility Management > Mobility Anchor Config** to navigate to this page. This page enables you to configure the symmetric mobility tunneling for mobile client features.

Guest N+1 Redundancy

The guest N+1 redundancy feature enables the foreign controller to periodically send ping requests to each anchor controller in the mobility group and enables you to configure the number and interval of requests sent to each anchor controller. Once a failed anchor controller is detected, all of the clients anchored to this controller are deauthenticated so that they can quickly become anchored to another controller.

When using the guest N+1 redundancy and mobility failover features with a firewall, ensure that the following ports are open:

- UDP 16666 for tunnel control traffic
- UDP 16667 for encrypted traffic
- IP Protocol 97 for user data traffic
- TCP 161 and 162 for SNMP

To view the current state of the data and control paths of controllers that have already been configured as mobility anchors, use the Mobility Anchors page.

Symmetric Mobility Tunneling

Note When controllers in the mobility list are running different software releases (such as 5.2, 6.0, and 7.0), Layer 2 or Layer 3 client roaming is not supported between them. It is supported only between controllers running the same release.

The controller provides inter-subnet mobility for clients roaming from one access point to another within a wireless LAN. This mobility is asymmetric so that the client traffic to the wired network is routed directly through the foreign controller.

This mechanism breaks when an upstream router has reverse path filtering (RPF) enabled. In this case, the client traffic is dropped at the router because the RPF check ensures that the path back to the source address matches the path from which the packet is coming.

When symmetric mobility tunneling is enabled, all client traffic is sent to the anchor controller and can then successfully pass the RPF check.

You should also enable symmetric mobility tunneling if a firewall installation in the client packet path may drop the packets whose source IP address does not match the subnet on which the packets are received.

Note Although a Cisco 2000 Series Controller cannot be designated as an anchor for a WLAN when using auto-anchor mobility, it can serve as an anchor in symmetric mobility tunneling to process and forward the upstream client data traffic tunneled from the foreign controller.

Mobility Anchor Config Parameters

Table 4-19 Mobility Anchor Config Parameters

Parameter	Description
Keep Alive Count	Number of times a ping request is sent to an anchor controller before the anchor is considered to be unreachable. The valid range is 3 to 20, and the default value is 3.
Keep Alive Interval	Amount of time (in seconds) between each ping request sent to an anchor controller. The valid range is 1 to 30 seconds, and the default value is 10 seconds.
Symmetric Mobility Tunneling mode	Enabled (Default).
DSCP Value	DSCP value that you can set for the mobility anchor. The valid range is 0 to 63.

Buttons

- Apply: Sends data to the Cisco WLC but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

Mobility Management > Mobility Multicast Messaging

Choose **CONTROLLER > Mobility Management > Multicast Messaging** to navigate to this page.

The controller provides inter-subnet mobility for clients by sending mobility messages to other member controllers. There can be up to 72 members in the list with up to 24 in the same mobility group. The controller sends a Mobile Announce message to members in the mobility list each time a new client associates to it.

You can configure the controller to use multicast to send the Mobile Announce messages. This behavior enables the controller to send only one copy of the message to the network, which designates it to the multicast group that contains all the mobility members. To derive the maximum benefit from multicast messaging, we recommend that it be enabled or disabled on all group members.

- Enable Multicast Messaging—Enables the controller to use multicast to send the Mobile Announce messages. If you leave it unselected, the controller uses unicast mode to send the Mobile Announce messages. The default value is unselected.
- Local Group Multicast IPv4 Address—Enables you to enter the multicast group IPv4 address for the local mobility group. This address is used for multicast mobility messaging.

Note To use multicast messaging, you must configure the IPv4 address for the local mobility group.

- Mobility Group—Lists the names of all the currently configured mobility groups.

Note IPv6 is not supported for mobility multicast.

Buttons

- Apply: Sends data to the Cisco WLC but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

Mobility Multicast Messaging > Edit

Choose **CONTROLLER > Mobility Management > Multicast Messaging** and then click the name of the local mobility group to navigate to this page.

- Mobility Group—Lists the name of all the mobility group.
- Local Group Multicast IP Address—Enables you to enter the multicast group IP address for the nonlocal mobility group. This address is used for multicast mobility messaging.

Note If you do not configure the multicast IP address for nonlocal groups, the controller uses unicast mode to send mobility messages to those members.

Buttons

- Back: Returns to the previous page.
- Apply: Sends data to the Cisco WLC but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

Mobility Management > Switch Peer Group

Choose **CONTROLLER > Mobility Management > Switch Peer Group** to navigate to this page.

This page lists all the switch peer groups and their details like bridge domain ID, multicast IP address, and status of the multicast mode. Click the name of the switch peer group to navigate to the Edit page and update the parameters if required.

Mobility Management > Switch Peer Group Member

Choose **CONTROLLER > Mobility Management > Switch Peer Member** to navigate to this page.

This page lists all the members of the switch peer group along with their group name, IP address, and public IP address.

Buttons

- New: Adds a new member to the switch peer group.

Mobility Management > Mobility Controllers

Choose **CONTROLLER > Mobility Management > Mobility Controllers** to navigate to this page.

This page lists all the mobility controllers. Mobility Controllers are controllers that provide mobility management services for an inter proximity group.

You can see the total number of mobility controllers and details like IP address, MAC address, client count, and link status.

Buttons

- New: Adds a new member to the switch peer group.

Mobility Management > Mobility Clients

Choose **CONTROLLER > Mobility Management > Mobility Clients** to navigate to this page.

This page lists the total number of mobility clients and their parameters.

Table 4-20 Mobility Client Parameters

Parameter	Description
Client MAC Address	MAC address of the mobility client.
Client IP Address	IP address of the mobility client.
Anchor MC IP Address	IP address of the anchor Mobility Controller.
Anchor MC Public IP Address	Public IP address of the anchor Mobility Controller.
Foreign MC IP Address	IP address of the foreign Mobility Controller.
Foreign MC Public IP Address	Public IP address of the foreign Mobility Controller.
Client Association Time	Time when the mobility client associated with the Mobility Controller.
Client Entry Update Timestamp	Timestamp when the client entry is updated.

Ports

Choose **CONTROLLER > Ports** to navigate to this page.

This page displays the status of each physical port on the Cisco WLC.

- To edit global parameters across all ports, click **Configure All** to open the Ports > Configure page.
- To edit the parameters for a single port, click the port number link for the port you want to configure. This action brings up a Ports > Configure page.

Note The physical mode and status may reflect different values depending on the link status. For example, the physical mode may be set to Auto while the actual link is running at 10 Mbps half duplex.

Table 4-21 Summary Parameters

Parameter	Description
Port No	Port number on the Cisco WLC.
Admin Status	State of the port as either Enabled or Disabled.
Physical Mode	Configuration of the port physical interface. Available values are as follows: • Auto • 100 Mbps Full Duplex • 100 Mbps Half Duplex • 10 Mbps Full Duplex • 10 Mbps Half Duplex **Note** In Cisco NM-AIR-WLC6-K9, Cisco 5500 Series, and Cisco Flex 7500 Series controllers, the physical mode is always set to Auto.
Physical Status	Displays the actual port physical interface. Available values are as follows: • Auto • 100 Mbps Full Duplex • 100 Mbps Half Duplex • 10 Mbps Full Duplex • 10 Mbps Half Duplex • 10000 Mbps Full Duplex
Link Status	Status of the link. Values are Link up or Link Down
Link Trap	Port that is set to send a trap when the link status changes. Values include Enable or Disable.

Buttons

- Configure All**:** Opens the Global Port configuration data page.

Ports > Configure

Choose **CONTROLLER > Ports** and then click **ConfigureAll** to navigate to this page.

This page enables you to change the parameters of all front-panel physical ports on the Cisco WLC simultaneously.

Table 4-22 Port Configuration Details

Parameter	Description	Range
Admin Status	Sets the state of all ports to Don’t Apply, Enable or Disable.	
Physical Mode	Displays the physical mode of all ports.	• Don’t Apply • Auto • 100 Mbps Full Duplex • 100 Mbps Half Duplex • 10 Mbps Full Duplex • 10 Mbps Half Duplex • 10000 Mbps Full Duplex **Note** In Cisco NM-AIR-WLC6-K9, 5500 series, and 7500 series controllers, the physical mode is always set to Auto.
Link Trap	Sets all ports to send or not to send a trap when link status changes. The factory default is Don’t Apply.	

Buttons

- Back: Returns to the previous page.
- Apply: Sends data to the Cisco WLC but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

Ports > Configure

Choose **CONTROLLER > Ports** and then click on a **Port No** to navigate to this page.

This page enables you to change the parameters of a single physical port on the Cisco WLC.

General Port Configuration

Table 4-23 General Port Configuration Parameters

Parameter	Description	Range
Port No	Identifies the current port.	13 for optional 1000Base-T or 1000Base-SX module 25 for optional 1000Base-T or 1000Base-SX module 1 for Cisco 4100 Series Wireless LAN Controller 1000Base-SX ports.
Admin Status	Sets the state of the port.	Enable Disable

Table 4-23 General Port Configuration Parameters

Parameter	Description	Range
Physical Mode	Sets the physical mode of the port.	Auto 100 Mbps Full Duplex 100 Mbps Half Duplex 10 Mbps Full Duplex 10 Mbps Half Duplex 10000 Mbps Full Duplex **Note** In Cisco NM-AIR-WLC6-K9, 5500 series, and 7500 series controllers, the physical mode is always set to Auto.
Physical Status	Displays the current physical port interface status.	100 Mbps Full Duplex 100 Mbps Half Duplex 10 Mbps Full Duplex 10 Mbps Half Duplex 10000 Mbps Full Duplex
Link Status	Displays the status of the link.	Link Up Link Down
Link Trap	Sets the port to send or not to send a trap when link status changes. The default is enabled.	Enable Disable

NTP

Choose **CONTROLLER > NTP** to navigate to this page. From here you can choose the following:

- **CONTROLLER > NTP > Server** to configure the Network Time Protocol parameters.

  See NTP > NTP Servers for more information.

- **CONTROLLER > NTP > Keys** to configure the Network Time Protocol keys.

  See NTP > NTP Keys for more information.

NTP > NTP Servers

Choose **CONTROLLER > NTP > Server** to navigate to this page. Use this page to set the Network Time Protocol parameters.

Table 4-24 NTP Parameters

Parameter	Description
NTP Polling Interval Seconds	Network polling time interval in seconds.
Server Index	NTP server index. The Cisco WLC tries Index 1 first, and then Index 2 through 3, in a descending order. If your network is using only one NTP server, you should use Index 1.
Server Address (IPv4/IPv6)	IP address or a Fully Qualified Domain Name (FQDN) of the NTP server.
Key Index	NTP key index.
NTP Msg Auth Status	Authentication Status of NTP message. It could either be AUTH SUCCESS or AUTH DISABLE.

Click a server index number to go to the NTP Server > Edit page to change the NTP server IP address.

Remove an NTP server entry by hovering your cursor over the blue drop-down arrow and choosing **Remove**. You are prompted for confirmation of the NTP server removal.

Ping the NTP server by hovering your cursor over the blue drop-down arrow and choosing **Ping**.

Buttons

- Apply: Sends data to the Cisco WLC but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.
- New: Adds a new item to a list. To set up a new NTP server, click to open the NTP Server > New page.

NTP Server > New

Choose **CONTROLLER > NTP > Server** and click **New** to navigate to this page. This page enables you to add a new NTP server.

Table 4-25 New Network Time Protocol Server Configuration

Parameter	Description
Server Index (Priority)	NTP server index. The Cisco WLC tries Index 1 first, and then Index 2 through 3, in a descending order. Set this to 1 if your network is using only one NTP server.
Server IP Address (IPv4/IPv6)	IP address or a Fully Qualified Domain Name (FQDN) of the NTP server
Enable NTP Authentication	Select or uncheck the check box to enable or disable NTP authentication
Key Index	Key index of the NTP server. This parameter is available when you enable NTP authentication.

Buttons

- Back: Returns to the previous page.
- Apply: Sends data to the Cisco WLC but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

NTP Server > Edit

Choose **CONTROLLER > NTP** and then click the server index number to navigate to this page. This page enables you to change the NTP server.

Table 4-26 Network Time Protocol Server Configuration Parameters

Parameter	Description
Server Address (IPv4/IPv6)	IP address or a Fully Qualified Domain Name (FQDN) of the NTP server
Enable NTP Authentication	Check box that you can select to enable or disable NTP authentication

Buttons

- Back: Returns to the previous page.
- Apply: Sends data to the Cisco WLC but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

NTP > NTP Keys

Choose **CONTROLLER > NTP > Keys** to navigate to this page. This page enables you to set the Network Time Protocol keys.

Table 4-27 NTP Key Parameters

Parameter	Description
Index	NTP server index
Key Index	NTP key index

Click a index number to go to the NTP Keys > Edit page to change the NTP key details.

Remove an NTP key entry by hovering your cursor over the blue drop-down arrow and choosing **Remove**. You are prompted for confirmation of the NTP key removal.

Buttons

New: Adds a new item to a list. To add a new NTP key, click to open the NTP Keys > New page.

NTP Keys > New

Choose **CONTROLLER > NTP > Keys** and then click **New** to navigate to this page. This page enables you to associate a new NTP key to a Server index.

Table 4-28 New Network Time Protocol Key Configuration

Parameter	Description
Key Index	NTP server index to which you want to associate the NTP key
Checksum	Checksum that is md5 by default
Key Format	Format of the key Choose either ASCII or HEX from the drop-down list.
Key	NTP key value

Buttons

- Back: Returns to the previous page.
- Apply: Sends data to the Cisco WLC but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

NTP Keys > Edit

Choose **CONTROLLER > NTP > Keys** and then click the index number to navigate to this page. This page enables you to change the NTP key.

Table 4-29 Network Time Protocol Key Configuration Parameters

Parameter	Description
Key Index	NTP server index to which you want to associate the NTP key.
Key Format	Format of the key. Choose either ASCII or HEX from the drop-down list.
Key	NTP key value.

Buttons

- Back: Returns to the previous page.
- Apply: Sends data to the Cisco WLC but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

CDP

Controller Configuration

Choose **CONTROLLER** > **CDP** > **Controller Configuration** to navigate to this page. This page enables you to configure the Cisco Discovery Protocol (CDP).

Cisco Discovery Protocol Overview

The Cisco Discovery Protocol (CDP) is a device discovery protocol that runs on all Cisco-manufactured equipment. A device enabled with CDP sends out periodic interface updates to a multicast address in order to make itself known to neighboring devices.

The default value for the frequency of periodic transmissions is 60 seconds, and the default advertised time-to-live value is 180 seconds. The second and latest version of the protocol, CDPv2, introduces new time-length-values (TLVs) and provides a reporting mechanism that allows for more rapid error tracking, reducing down time.

CDPv1 and CDPv2 are supported on the following devices:

- Cisco Flex 7500 and 5500 Series Controllers
- Lightweight access points
- An access point connected directly to a Cisco Flex 7500 and 5500 Series Controller

This support enables network management applications to discover Cisco devices.

The following TLVs are supported by both the controller and the access point:

- Device-ID TLV: 0x0001—The hostname of the controller, the access point, or the CDP neighbor.
- Address TLV: 0x0002—The IP address of the controller, the access point, or the CDP neighbor.
- Port-ID TLV: 0x0003—The name of the interface on which CDP packets are sent out.
- Capabilities TLV: 0x0004—The capabilities of the device. The controller sends out this TLV with a value of Host: 0x10, and the access point sends out this TLV with a value of Transparent Bridge: 0x02.
- Version TLV: 0x0005—The software version of the controller, the access point, or the CDP neighbor.
- Platform TLV: 0x0006—The hardware platform of the controller, the access point, or the CDP neighbor.
- Power Available TLV: 0x001a—The amount of power available to be transmitted by Power Sourcing Equipment to permit a device to negotiate and select an appropriate power setting.

The following TLVs are supported only by the access point:

- Full/Half Duplex TLV: 0x000b—The full- or half-duplex mode of the Ethernet link on which CDP packets are sent out. This TLV is not supported on access points that are connected directly to a Cisco 5500 Series Controller.
- Power Consumption TLV: 0x0010—The maximum amount of power consumed by the access point. This TLV is not supported on access points that are connected directly to a Cisco Flex 7500, 5500, Series Controllers.
- Power Request TLV:0x0019—The amount of power to be transmitted by a powerable device in order to negotiate a suitable power level with the supplier of the network power.

Note Changing the CDP configuration on the controller does not change the CDP configuration on the access points that are connected to the controller. You must enable and disable CDP separately for each access point.

Parameters and Descriptions

Table 4-30 CDP Global Configuration Parameters

Parameter	Description	Range	Default
CDP Protocol Status	Parameter that allows you to enable or disable CDP on the controller. **Note** You also need to enable CDP on the access point. **Note** Enabling or disabling this feature will be applicable to all the controller ports.	—	Enabled
CDP Advertisement Version	Highest CDP version supported on the controller.	Version 1 (v1) or version 2 (v2)	v1
Refresh-time Interval (seconds)	Interval at which CDP messages are to be generated.	5 to 254 seconds	60 seconds
Holdtime (seconds)	Amount of time to be advertised as the time-to-live value in generated CDP packets.	10 to 255 seconds	180 seconds

For information on displaying CDP neighbor information, see the following topics:

- CDP Neighbors Details
- CDP Neighbors
- CDP AP Neighbors
- CDP Traffic Metrics

Buttons

- Apply**:** Sends data to the Cisco WLC but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

PMIPv6

Proxy Mobile IPv6 (PMIPv6) is a network-based mobility management protocol. The controller uses the PMIPv6 protocol and works with the Mobile Access Gateway (MAG) and ASR5K, the partner Local Mobility Anchor (LMA), to provide seamless mobility of mobile clients. MAG tracks the mobile node and signals the mobile node’s LMA.

Choose **CONTROLLER > PMIP** to navigate to this page. From here you can choose the following:

- **CONTROLLER > PMIP > General** to configure global parameters for PMIPv6.

See PMIPv6 > General for more information.

- **CONTROLLER > PMIP > LMA** to add new and view existing Local Mobility Anchor (LMA) to the controller.

  See PMIPv6 > LMA for more information.
- **CONTROLLER > PMIPv6 > Profile** to view existing PMIPv6 profiles.

  See PMIPv6 > Profile for more information.

PMIPv6 > General

Choose **CONTROLLER > PMIP > General** to configure global parameters for PMIPv6.

Note For timer parameters, default values appear in the UI when you reconfigure the domain name.

Table 4-31 General Parameters

Parameter	Description
Domain Name	Name of the PMIPv6 domain. The domain name can be up to 127 case-sensitive, alphanumeric characters.
MAG Name	Name of the MAG.
Interface	Interface of the controller used for PMIPv6.
MAG APN	Access Point Name (APN) if you subscribe to a MAG. MAG can be configured for one of the following roles: • 3gpp—Specifies the role as 3GPP (Third Generation Partnership Project standard) • lte—Specifies the role as Long Term Evolution (LTE) standard • wimax—Specifies the role as WiMax • wlan—Specifies the role as WLAN By default, the MAG role is WLAN. However, for lightweight access points, the MAG role should be configured as 3GPP. If the MAG role is 3GPP, it is mandatory to specify an APN for the MAG.
Maximum Bindings Allowed	Maximum number of binding entries in the MAG. The range is from 0 to 40000. The default value is 10000.
Binding Lifetime	Lifetime of the binding entries in the controller. The binding lifetime should be a multiple of 4 seconds. The range is from 10 to 65535 seconds. The default value is 3600.
Binding Refresh Time	Refresh time of the binding entries in the MAG. The binding refresh time should be a multiple of 4 seconds. The range is from 4 to 65535 seconds. The default value is 300 seconds.
Binding Initial Retry Timeout	Initial timeout between the proxy binding updates (PBUs) when the MAG does not receive the proxy binding acknowledgements (PBAs). The range is from 100 to 65535 seconds. The default value is 1000 seconds.

Table 4-31 General Parameters

Parameter	Description
Binding Maximum Retry Timeout	Maximum timeout between the proxy binding updates (PBUs) when the MAG does not receive the proxy binding acknowledgments (PBAs). The range is from 100 to 65535 seconds. The default value is 32000 seconds.
Replay Protection Timestamp	Maximum amount of time difference between the timestamp in the received proxy binding acknowledgment and the current time of the day. The range is from 1 to 255 milliseconds. The default value is 7 milliseconds.
Minimum BRI Retransmit Timeout	Minimum amount of time that the MAG waits before retransmitting the BRI message. The range is from 500 to 65535 seconds. The default value is 1000 seconds.
Maximum BRI Retransmit Timeout	Maximum amount of time that the MAG waits before retransmitting the Binding Revocation Indication (BRI) message. The range is from 500 to 65535 seconds. The default value is 2000 seconds.
BRI Retries	Maximum number of times that the MAG retransmits the BRI message before receiving the Binding Revocation Acknowledgment (BRA) message. The range is from 1 to 10. The default value is 1.

PMIPv6 > LMA

Choose **CONTROLLER > PMIP > LMA** to add new and view existing Local Mobility Anchor (LMA) to the controller.

Click **New** to add a new LMA to the controller.

Table 4-32 LMA Parameters

Parameter	Description
Member Name	Name of the LMA connected to the controller. The LMA name can be up to 127 case-sensitive, alphanumeric characters.
Member IP Address	IP address of the LMA connected to the controller.

Buttons

Apply: Adds a new LMA member.

PMIPv6 > Profile

Choose **CONTROLLER > PMIPv6 > Profile** to navigate to this page. This page lists existing PMIPv6 profiles.

Buttons

- New**:** Adds a new PMIPv6 profile.

Click a PMIPv6 profile to edit the configurations of the PMIPv6 profile.

PMIPv6 Profile > New

Choose **CONTROLLER > PMIPv6 > Profile** and then click **New** to navigate to this page. This page allows you to create a new PMIPv6 profile.

Table 4-33 Profile Parameters

Parameter	Description
Profile Name	Name of the PMIPv6 profile.
Network Access Identifier	Name of the Network Access Identifier (NAI) associated with the profile. The NAI can be up to 127 case-sensitive alphanumeric characters.
LMA Name	Name of the LMA to which the profile is associated. The LMA name can be up to 127 alphanumeric, case-sensitive characters.
Access point node	Name of the access point node connected to the controller.

Buttons

- Back: Returns to the previous page.
- Apply: Sends data to the Cisco WLC but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

PMIPv6 Profile > Edit

Choose **CONTROLLER > PMIP > Profile** and then click on any profile to navigate to this page. This page allows you to add more NAIs and remove any of the existing NAIs.

Button

- Add NAI: Allows you to add more NAIs.

Tunneling

EoGRE

Choose **CONTROLLER > Tunneling > EoGRE** to navigate to this page.

Table 4-34 EoGRE Parameters

Parameter	Description
Interface Name	Name of the interface that is used as the tunnel interface
Heartbeat Interval (Seconds)	The heartbeat is used by Cisco WLC and Cisco AP to check the status of the tunnel gateway depending on the mode. • If the AP is in Local mode and WLAN is centrally switched, the heartbeat is from Cisco WLC. • If the AP is in FlexConnect mode and the WLAN is locally switched, the AP checks the tunnel gateway connectivity.
Max Heartbeat Skip Count	Number of consecutive keepalive retries before a member status is marked ‘Down’.
Add New TGW	
TGW Name	Name of the tunnel gateway.
TGW IP Address	IPv4 or IPv6 address of the tunnel gateway.
TGW List	Shows details of the tunnel gateways added. The details include name of the TGW, IPv4 or IPv6 address of the TGW, status of TGW (Up or Down), and the total number of clients associated. Click **Get Statistics** to view tunnel gateway statistics.
Add New Domain	
Domain Name	Name of the domain
TGW-1	Specify the name of TGW and the role as either primary/active or secondary/standby TGW. **Note** In a domain, the primary gateway is active by default. When the primary gateway is not operational, the secondary gateway becomes the active or primary gateway. Clients will have to associate again with the secondary gateway. During and after failover, Cisco WLC continues to ping the primary gateway. When the primary gateway is operational again, the primary gateway becomes the active gateway. Clients then fall back to the primary gateway. The same option is available for the TGW from FlexConnect in local switched mode. EoGRE tunnels can be DTLS encrypted CAPWAP IPv4 or IPv6. This feature is supported on all Wave 1 and Wave 2 APs that are supported in this release.
TGW-2	Specify the name of TGW and the role as either primary/active or secondary/standby TGW.
Domain List	Shows details of the domains added. The details include domain name, the two TGWs associated with the domain, the name of the active TGW, and its role as either the primary or secondary gateway.

Profiles

Choose **CONTROLLER > Tunneling > Profiles** to navigate to this page.

Table 4-35 Profile Parameters

Parameter	Description
Add New	
Profile Name	The heartbeat is used in the failover mechanism for the AP to detect if the Active TGW went down

IPv6

Neighbor Binding Timers

Choose **CONTROLLER** > **IPv6** > **Neighbor Binding Timers** to navigate to this page. This page enables you to configure the Neighbor Binding timers.

Parameters and Descriptions

Table 4-36 Neighbor Binding Timer Parameters

Parameter	Description	Range	Default
Down Lifetime	Maximum time, in seconds, that an entry learned from a down interface is kept in the binding table before the entry is deleted or proof is received that the entry is reachable.	0–86400 seconds	300 seconds
Reachable Lifetime	Maximum time, in seconds, that an entry is considered reachable without getting a proof of reachability (direct reachability through tracking or indirect reachability through Neighbor Discovery protocol [NDP] inspection). After that, the entry is moved to stale.	0–86400 seconds	300 seconds
Stale Lifetime	Maximum time, in seconds, that a stale entry is kept in the binding table before the entry is deleted or proof is received that the entry is reachable.	0–86400 seconds	86400 seconds
Unknown Address Multicast NS Forwarding	The controller forwards the IPv6 packets without validating the multicast Neighbor Solicitation (NS) frame.	—	—

Buttons

- Apply**:** Sends data to the Cisco WLC but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

RA Throttle Policy

Choose **CONTROLLER** > **IPv6** > **RA Throttle Policy** to navigate to this page. This page enables you to configure the RA Throttle Policy.

The purpose of the RA Throttle Policy is to limit the amount of multicast Router Advertisements (RA) circulating on the wireless network.

Parameters and Descriptions

Table 4-37 RA Throttle Policy Parameters

Parameter	Description	Range	Default
Enable RA Throttle Policy	IPv6 RA throttling.	–	Disabled
Throttle Period	Duration of throttle period in seconds.	10–86400 seconds	600 seconds
Max Through	Number of RAs that will pass through over a period.	0–256	10
Interval Option	Behavior RAs that have an interval option.	Ignore, Passthrough, or Throttle	Passthrough
Allow At-least	Minimum number of RAs that will not be throttled per router.	0–32	1
Allow At-most	Maximum number of RAs that will not be throttled per router.	0–256	1
No Limit	No limit to be placed on the maximum number of RAs that will not be throttled per router.	–	Disabled

Buttons

- Apply**:** Sends data to the Cisco WLC but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

RA Guard

Choose **CONTROLLER > IPv6 > RA Guard** to navigate to this page. This page enables you to configure router advertisement (RA) filtering.

RA Guard is a Unified Wireless solution to drop RA from wireless clients. It is configured globally, and by default it is enabled.

Buttons

- Apply: Sends data to the Cisco WLC but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

mDNS

Multicast DNS (mDNS) Service Discovery provides a way to announce and discover devices like printers, computers, and services on the local network. mDNS performs DNS queries over IP multicast. mDNS supports zero configuration IP networking. mDNS uses the multicast IP address 224.0.0.251 as the destination address and 5353 as the UDP destination port.

Choose **CONTROLLER > mDNS > General** to navigate to this page. From here, you can choose the following:

- **CONTROLLER > mDNS** to configure the global mDNS parameters.

  See mDNS > General for more information.
- **CONTROLLER > mDNS > Profiles** to view the mDNS profiles configured on the controller and create new mDNS profiles.

  See mDNS > Profiles for more information.
- **CONTROLLER > mDNS > Domain Names** to view the domain names and other details of the service providers.

  See mDNS > Domain Names for more information.
- **CONTROLLER > mDNS > mDNS Browser t**o view the domain names and other details of the service providers.

  See mDNS Browser for more information.
- **CONTROLLER > mDNS > mDNS Policies** to view the total number of mDNS Service groups.

  See mDNS Service Groups for more information.

mDNS > General

Choose **CONTROLLER > mDNS > General** to navigate to this page. This page enables you to configure the global mDNS parameters and update the Master Services database.

,

Table 4-38 Profile Parameters

Parameter	Description
Global Configuration	
mDNS Global Snooping	Check box that you can check to enable snooping of mDNS packets. **Note** The controller does not support IPv6 mDNS packets even when you enable mDNS snooping.
mDNS Policy	Check box that you can check to enable mDNS policy. **Note** If global mDNS access policy is enabled, LSS will be ignored.
Query Interval	mDNS query interval, in minutes, that you can set. The query interval is the frequency at which the Cisco WLC sends periodic queries to all the services defined in the Master Service database. The range is from 10 to 120 minutes. The default value is 15 minutes.
Master Services Database	

Table 4-38 Profile Parameters

Parameter	Description
Service	Drop-down list from which you can choose the supported services that can be queried. The following services are available: • Air Tunes • Apple File Sharing Protocol (AFP) • Scanner • FTP • NFS • iTunes Music Sharing • iTunes Home Sharing • iTunes Wireless Device Syncing • Apple Remote Desktop • Apple CD/DVD Sharing • Time Capsule Backup Click **Add** after you choose a service. To add a new mDNS-supported service, choose **Other**. Specify the service name and service string. The controller snoops and learns about the mDNS service advertisements only if the service is available in the Master Services database.The controller can snoop and learn a maximum of 64 services.
Service Name	Name of the mDNS service.
Service String	Unique string associated to an mDNS service. For example,” _airplay._tcp.local.” is the service string associated to Apple TV.
Query Status	Check box that you can check to enable an mDNS query for a service.
LSS Status	Check box that you can check to enable LSS status.
Origin	Specify the origin of the service from the following options: • All • Wireless • Wired

To view the details of an mDNS service, hover your cursor over the blue drop-down arrow of a service, and choose **Details**. The mDNS > Service > Detail page appears, for more information, see mDNS > Service > Detail.

mDNS > Service > Detail

Choose **CONTROLLER > mDNS > General**, hover your cursor over the blue drop-down arrow for a service, and choose **Details** to navigate to this page. This page enables you to view the details of each service.

Table 4-39 Service Detail Parameters

Parameter	Description
Service Name	Name of the mDNS service.
Service String	Unique string associated to an mDNS service. For example,” _airplay._tcp.local.” is the service string associated to Apple TV.
Service ID	Unique service ID associated to an mDNS service.
Service Query Status	Status of the service query that indicates if the service can be queried by the Cisco WLC. The Cisco WLC queries the service only if the query status is enabled for the service.
Profile Count	Number of profiles associated with the service. You can associate multiple services to a profile and map the profile to a WLAN, interface, or an interface group.
Service Provider Count	Number of service providers or hosts that provide the service.
Profile Information	
Profile Name	Names of the profiles associated with the service.
Service Provider Information	
MAC Address	MAC address of the service provider.
Service Provider Name	Name of the service provider. Beginning in Release 8.0 and later releases, the maximum number of service providers for different controller models are as follows: • Cisco 5500 and 2500 Series Controllers—6400 • Cisco Wireless Services Module 2—6400 • Cisco 8500 and 7500 Series Controllers—16000
VLAN ID	VLAN ID of the service provider.
Type	Type of service provider that is one of the following: • Wired— Service provider is on the infrastructure side. • Wireless— Service provider is a wireless client. • Wired guest— Service provider is on a guest LAN.
TTL	Time to Live (TTL) value in seconds that determines the validity of the service offered by the service provider. The service provider is removed from the controller when the TTL expires.
Time Left	Time left in seconds before the service provider is removed from the controller.

mDNS > Profiles

Choose **CONTROLLER > mDNS > Profiles** to view the mDNS profiles configured on the controller and create new mDNS profiles.

After creating a new profile, you must map the profile to an interface group, an interface, or a WLAN. Clients receive service advertisements only for the services associated with the profile. The controller gives the highest priority to the profiles associated to interface groups, followed by the interface profiles, and then the WLAN profiles. Each client is mapped to a profile based on the order of priority.

By default, the controller has an mDNS profile, default-mdns-profile. You cannot delete this default profile.

For more information, see the following topics:

- Mapping mDNS Profiles to an Interface Group
- Mapping mDNS Profiles to an Interface
- Mapping mDNS Profiles to a WLAN

Table 4-40 mDNS Profile Parameters

Parameter	Description
Number of profiles	Number of mDNS profiles configured on the controller.
Profile Name	Name of the mDNS profile. You can create a maximum of 16 profiles.
Number of Services	Number of services in an mDNS profile.

Buttons

New: Creates a new mDNS profile.

Mapping mDNS Profiles to an Interface Group

To map a profile to an interface group, follow these steps:

Step 1 Choose **CONTROLLER > Interface Groups** and click the Interface Group name to navigate to the Interface Groups > Edit page.

Step 2 Choose an mDNS profile from the drop-down list.

Mapping mDNS Profiles to an Interface

To map a profile to an interface, follow these steps:

Step 1 Choose **CONTROLLER > Interfaces** and then click on an interface name to navigate to the Interfaces > Edit page.

Step 2 Choose an mDNS profile from the drop-down list.

Mapping mDNS Profiles to a WLAN

To map a profile to a WLAN, follow these steps:

Step 1 Choose **WLANs** and click the Profile name to navigate to the WLANs > Edit page.

Step 2 Select the mDNS check box.

Step 3 Choose an mDNS profile from the drop-down list.

mDNS Profile > Edit

Choose **CONTROLLER > mDNS > Profiles** and click the profile name to navigate to the **mDNS Profile > Edit** page. You can view the following details of the profile:

- Profile Name
- Profile ID
- Service Count
- Number of interfaces attached
- Number of interface groups attached
- Interface groups
- Number of WLANs attached
- WLAN IDs
- Number of Guest LANs attached
- Guest LAN IDs
- Number of Local Policies attached
- Local Policy IDs

To add more services to the profile, choose a service from the **Service Name** drop-down list and click **Add**. You can choose from a list of services that are configured in the Master service database. To update the Master service database, choose **CONTROLLER > mDNS > General**.

mDNS > Domain Names

Choose **CONTROLLER > mDNS > Domain Names** to view the domain names and other details of the service providers.

Each service advertisement contains a record that maps the domain name of the service provider to the IP address. The mapping also contains details such as the client MAC address, the VLAN ID, the TTL, and the IPv4 address.

Table 4-41 Domain Names Parameters

Parameter	Description
Number of Domain Name-IP Entries	Count of the domain name IP address mappings.
Domain Name	Hostname assigned to each service provider machine.
MAC Address	MAC address of the service provider machine.
IP Address	IP address of the service provider.
VLAN ID	VLAN ID of the service provider.

Table 4-41 Domain Names Parameters

Parameter	Description
Type	Origin of service that can be one of the following: • Wired • Wireless • Wired guest
TTL	Time to Live (TTL) value in seconds that determines the validity of the service offered by the service provider. The service provider is removed from the controller when the TTL expires.
Time Left	Time left in seconds before the service provider is removed from the controller.

mDNS Browser

Choose **CONTROLLER > mDNS > mDNS Browser** to view the total number of services added in the master database.

Table 4-42 mDNS Browser Parameters

Parameter	Description
Number of Services	Total number of services added in the Master database.
Origin	From where mDNS service instances are snooped (source). Can be WIRED/WIRELESS/mDNS-AP/WIRED GUEST.
VLAN	Snooped Service instance VLAN.
TTL (seconds)	Service instance advertised that service will be available for TTL seconds (time to live).
TTL Left (seconds)	Service instance available run time.
Client MAC	MAC address of service instance.
AP MAC	Service instance joined AP Base MAC.
Service String	Unique string associated to an mDNS service, for example, _airplay._tcp.local. is the service string associated with Apple TV.

mDNS Service Groups

Choose **CONTROLLER > mDNS > mDNS Policies** to view total number of mDNS Service groups.

Table 4-43 mDNS Service Groups Parameters

Parameter	Description
Number of mDNS Policies	Total number of mDNS Service groups. This includes admin created / ISE dynamic policy / SNMP.
Number of Admin Created Policies	Total number of mDNS service groups created by WLC admin.
mDNS Service Group Name	Service group name.
Description	Service group description.
Origin	Service group origin that is created by WLC admin/ISE/SNMP.

Creating mDNS Service Group

Step 1 Choose **CONTROLLER > mDNS > mDNS Policies** and click the **Add Group** button.

Step 2 Enter a service group name in the **mDNS Service Group Name** box.

Step 3 Add a description for the service group in the **Description** box.

Step 4 Click **Add** to create a new mDNS Service Group.

mDNS Service Group > Edit

Choose **CONTROLLER > mDNS > Policies** and click the mDNS Service Group Name to navigate to the **mDNS Service Groups > Edit** page. You can add a MAC Address and a rule to the Service Group.

Table 4-44 mDNS Service Group > Edit Parameters

Parameters	Description
mDNS Service Group Name	Displays the name of the mDNS Service Group selected for editing.
Service Instance List	
MAC Address	MAC address of the service provider
Name	Name of the service provider
Location Type	Choose from the following options: • AP Group • AP Name • AP Location

Table 4-44 mDNS Service Group > Edit Parameters

Parameters	Description
Location	Location to be specified. If the Location is specified as Any, the policy checks on the Location attribute are not performed. **Note** In the case of mDNS policy filtered by AP groups, the design is for substring match. The policy is applied on the first substring match.
Policy/Rule	
Role Names	User type or user group of the user, for example, student, employee.
User Names	Name of the user.

Advanced

This section contains the following topics:

- DHCP, page 4-53
- Master Controller Mode, page 4-55

DHCP

Choose **CONTROLLER > Advanced > DHCP** to navigate to this page. This page enables you to set the following DHCP parameters:

Table 4-45 DHCP Parameters

Parameter	Description
Enable DHCP Proxy	Drop-down list from which you can choose to enable or disable DHCP proxy on a global basis, rather than on a WLAN basis. DHCP proxy is enabled by default. When DHCP proxy is enabled on the controller, the controller unicasts DHCP requests from the client to the configured servers. Consequently, at least one DHCP server must be configured on either the interface associated with the WLAN or the WLAN itself. **Note** IPv6 is not supported for DHCP.
DHCP Option 82 Remote Id field format	Provides additional security when DHCP is used to allocate network addresses. Specifically, it enables the controller to act as a DHCP relay agent to prevent DHCP client requests from untrusted sources. The controller can be configured to add option 82 information to DHCP requests from clients before forwarding the requests to the DHCP server. **Note** For DHCP option 82 to work as expected, you must enable DHCP proxy. **Note** DHCP option 82 is not supported for use with auto-anchor mobility. See Mobility Anchors for information about anchor mobility. • AP-MAC—Adds the MAC address of the access point to the DHCP option 82 payload. This is the default value. • AP-MAC-SSID—Adds the MAC address and SSID of the access point to the DHCP option 82 payload. • AP-ETHMAC—Adds the Ethernet MAC address of the access point to the DHCP option 82 payload. • AP-NAME-SSID—Adds the name and SSID of the access point to the DHCP option 82 payload. • AP-GROUP-NAME—Adds the AP group name of the access point to the DHCP option 82 payload. • FLEX-GROUP-NAME—Adds the FlexConnect group name of the access point to the DHCP option 82 payload. • AP-LOCATION—Adds the location of the access point to the DHCP option 82 payload. • AP-MAC-VLAN-ID—Adds the MAC address and VLAN ID of the access point to the DHCP option 82 payload. • AP-NAME-VLAN-ID—Adds the name and VLAN ID of the access point to the DHCP option 82 payload. • AP-ETHMAC-SSID—Adds the MAC address and SSID of the access point to the DHCP option 82 payload.
DHCP Timeout	Sets the DHCP timeout in seconds. This value is applicable globally. The valid range is 5 to 120 seconds.

Buttons

- Apply: Sends data to the Cisco WLC but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

Master Controller Mode

Choose **CONTROLLER > Advanced > Master Controller Mode** to navigate to this page.

This page enables the Cisco WLC to be configured as the master Cisco WLC for your access points that are connected in appliance mode. When there is a master Cisco WLC enabled, all newly added access points with no primary, secondary, or tertiary controllers assigned associate with the master Cisco WLC on the same subnet. This feature enables you to verify the access point configuration and assign primary, secondary, and tertiary controllers to the access point using the All AP Details page.

Note The master Cisco WLC is normally used only while adding new access points to the Cisco Wireless LAN Solution (Cisco WLAN Solution). When no more access points are being added to the network, you should disable the master Cisco WLC.

Note Because the master Cisco WLC is normally not used in a deployed network, the master Cisco WLC setting is disabled upon reboot or OS code upgrade.

Buttons

- Apply: Sends data to the Cisco WLC but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.