



Cisco Wireless LAN Controller IPv6 Deployment Guide, CUWN Release 8.0

Last Updated:

Phase 1–Client IPv6 Support in Release 7.2 to 7.6.

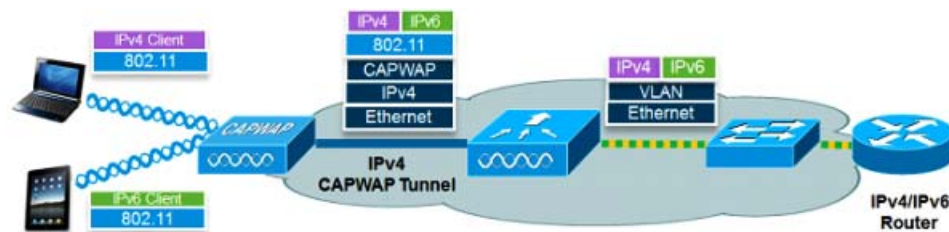
Phase 2–Infrastructure IPv6 Support in Release 8.0.

Phase 1–Client IPv6 Support in WLC Release 7.2 to 7.6

This document provides information about the theory of operation and configuration for Cisco’s Unified Wireless LAN solution as it pertains to supporting IPv6 clients.

The [Phase 2–Infrastructure IPv6 Support in WLC Release 8.0 and Later, page 19](#) section of this document provides information about the Infrastructure support for IPv6 protocols in the Unified controllers in Release 8.0.

IPv6 Wireless Client Connectivity Supported in Release 7.2 and Later



The IPv6 feature set within the Cisco Unified Wireless Network software release version 7.2 allows the wireless network to support IPv4, Dual-Stack, and IPv6-only clients on the same wireless network. The overall goal for the addition of IPv6 client support to the Cisco Unified Wireless LAN is to maintain feature parity between IPv4 and IPv6 clients including mobility, security, guest access, quality of service, and endpoint visibility.

Up to eight IPv6 client addresses can be tracked per client. This allows IPv6 clients to have a link-local, SLAAC address, DHCPv6 address, and even addresses in alternative prefixes to be on a single interface. Work Group Bridge (WGB) clients connected to the uplink of an Autonomous Access Point in WGB mode can also support IPv6.

Every IPv6 enabled interface must contain at least, 1 Loopback and 1 Link-Local address. Optionally, every interface can have multiple Unique-Local and Global IPv6 addresses.

Solution Components

- Wireless controllers 2500 series, 5500 series, WiSM2, 7500 series, 8500 series, and vWLC
- Cisco AP 1040, 1130 (feature parity with release 7.6; release 8.0 features are not supported), 1140, 1240 (feature parity with release 7.6; release 8.0 features are not supported), 1250, 1260, 1600, 2600, 2700, 3500, 3500p, 3600, 3700, Cisco 600 Series OfficeExtend Access Points, AP 702, AP 702W, AP 801, and AP 802

Phase 1–Client IPv6 Support in WLC Release 7.2 to 7.6

- Cisco Aironet 1530 series outdoor 802.11n mesh access points, Cisco Aironet 1550 (1552) series outdoor 802.11n mesh access points, Cisco Aironet 1520 (1522, 1524) series outdoor mesh access points

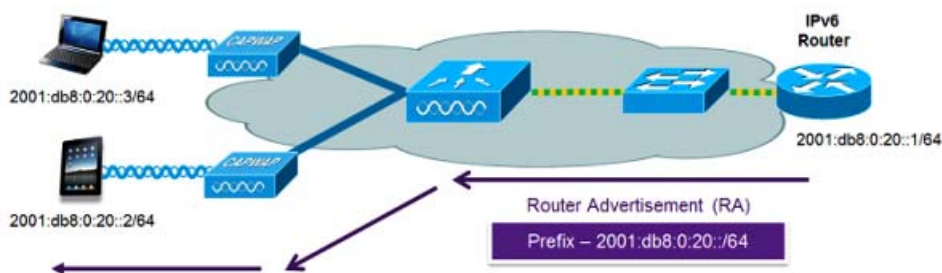
Note: The 1520 and 1550 series APs with 64 MB does not support PPPoE and PMIPv6.

- An IPv6-capable Router and/or Switch

Prerequisites for Wireless IPv6 Client Connectivity

To enable wireless IPv6 client connectivity, the underlying wired network must support IPv6 routing and an address assignment mechanism such as SLAAC or DHCPv6. The wireless LAN controller must have L2 adjacency to the IPv6 router, and the VLAN must be tagged when entering the controller interfaces. Prior to Release 8.0, APs did not require connectivity to an IPv6 network, as all traffic is encapsulated inside the IPv4 CAPWAP tunnel between the AP and the controller.

SLAAC Address Assignment

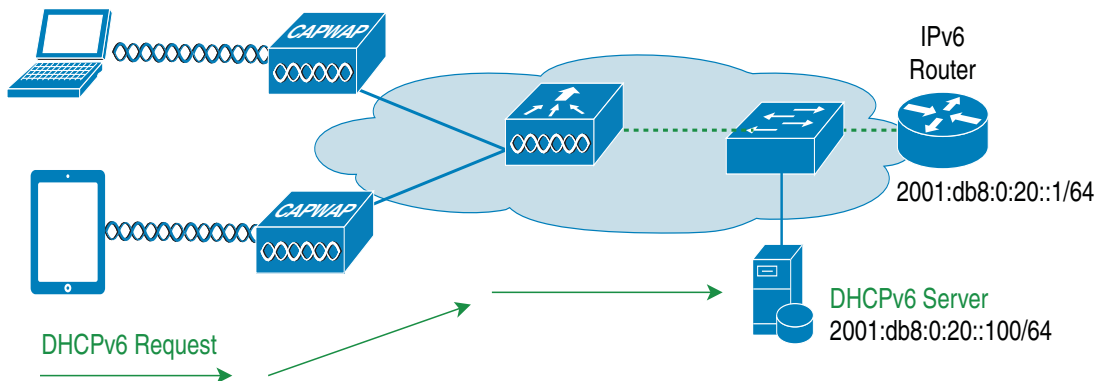


The most common method for IPv6 client address assignment is Stateless Address Auto Configuration (SLAAC). SLAAC provides simple plug and play connectivity where clients self-assign an address based on the IPv6 prefix. This process is achieved by the IPv6 router sending out periodic Router Advertisement messages which inform the client of the IPv6 prefix in use (the first 64 bits) and of the IPv6 default gateway. From that point, clients can generate the remaining 64 bits of their IPv6 address based on either the MAC address of the adapter or randomly. Duplicate address detection is performed by IPv6 clients to ensure random addresses that are picked do not collide with other clients. The address of the router sending advertisements is used as the default gateway for the client.

The following configuration example from a Cisco-capable IPv6 router has the necessary commands to enable SLAAC addressing and router advertisements:

```
interface Vlan20
description IPv6-SLAAC
ip address 192.168.20.1 255.255.255.0
ipv6 address 2001:DB8:0:20::1/64
ipv6 enable
end
```

DHCPv6 Address Assignment



353114

The use of DHCPv6 is not required for IPv6 client connectivity if SLAAC is already deployed. There are two modes of operation for DHCPv6 called **Stateless** and **Stateful**.

The DHCPv6 **Stateless** mode is used to provide clients with additional network information not available in the router advertisement. This information can include the DNS domain name, DNS server(s), and other vendor-specific options. The following interface configuration example is for an IPv6 router implementing stateless DHCPv6 with SLAAC enabled:

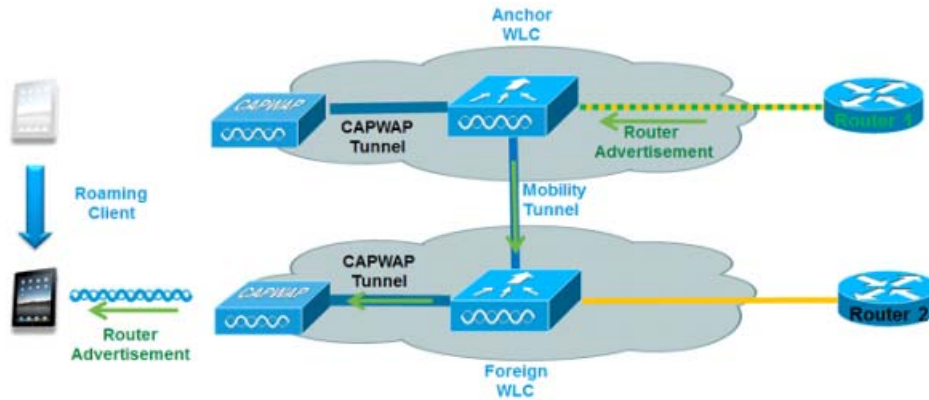
```
interface Vlan20
description IPv6-DHCP-Stateless
ip address 192.168.20.1 255.255.255.0
ipv6 enable
ipv6 address 2001:DB8:0:20::1/64
ipv6 nd other-config-flag
ipv6 dhcp relay destination 2001:DB8:0:20::100
end
```

The DHCPv6 **Stateful** mode operates similar to DHCPv4, that is, it assigns addresses to each client instead of the client generating the address as in SLAAC. The following interface configuration is for an IPv6 router implementing stateful DHCPv6 with SLAAC turned off:

```
interface Vlan20
description IPv6-DHCP-Stateful
ip address 192.168.20.1 255.255.255.0
ipv6 enable
ipv6 address 2001:DB8:0:20::1/64
ipv6 nd prefix 2001:DB8:0:20::/64 no-advertise
ipv6 nd managed-config-flag
ipv6 nd other-config-flag
ipv6 dhcp relay destination 2001:DB8:0:20::100
```

end

IPv6 Client Mobility



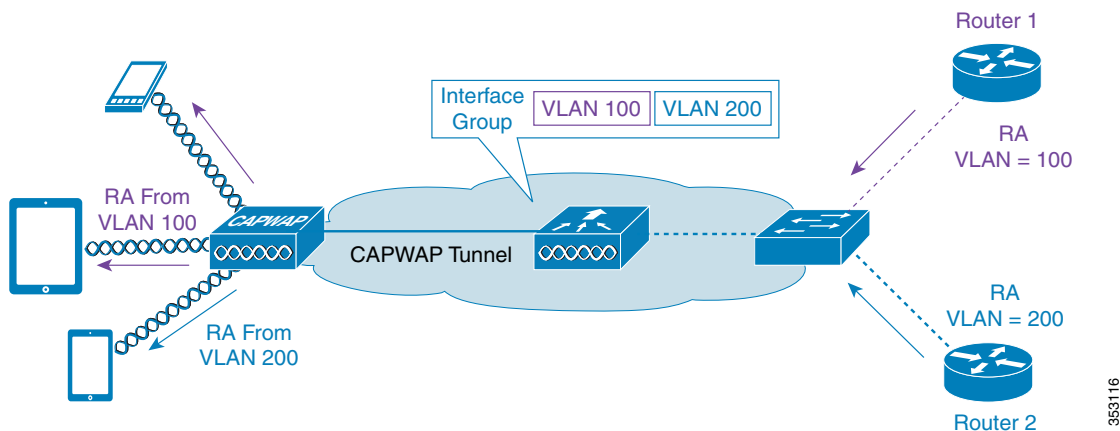
In order to deal with roaming IPv6 clients across controllers, the ICMPv6 messages such as NS, NA, RA, and RS must be dealt with specially to ensure that a client remains on the same Layer 3 network. The configuration for IPv6 mobility is the same as for IPv4 mobility and requires no separate software on the client side to achieve seamless roaming. The only required configuration is the controllers must be part of the same mobility group/domain.

The process of IPv6 client mobility across controllers is as follows:

1. If both controllers have access to the same VLAN the client was originally on, the roam is simply a Layer 2 roaming event where the client record is copied to the new controller and no traffic is tunneled back to the anchor controller.
2. If the second controller does not have access to the original VLAN the client was on, a Layer 3 roaming event will occur, meaning all traffic from the client must be tunneled via the mobility tunnel (Ethernet over IP) to the anchor controller. In a mixed deployment with Release 7.x and 8.x, Ethernet over IP is used. In pure 8.0 deployments, we support CAPWAP tunnel for IPv6 mobility tunnel.
 - a. To ensure that the client retains its original IPv6 address, the Router Advertisements from the original VLAN are sent by the anchor controller to the foreign controller where they are delivered to the client using L2 Unicast from the AP.
 - b. When the roamed client goes to renew its address via DHCPv6 or generate a new address via SLAAC, the Router Solicitation, Neighbor Advertisement, and Neighbor Solicitation packets continue to be tunneled to the original VLAN so that the client receives an IPv6 address that is applicable to that VLAN.

Note: Mobility is based on VLAN information. It is not based on the IPv4 subnet or IPv6 prefix in use. This means that IPv6 client mobility is not supported on untagged VLANs.

Support for Interface Groups

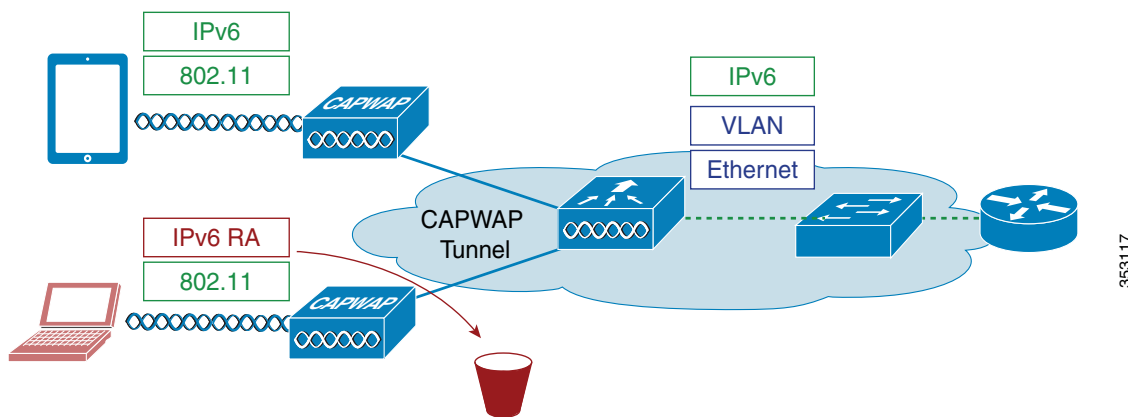


The interface groups feature allows an organization to have a single WLAN with multiple VLANs configured on the controller to permit load balancing of wireless clients across these VLANs. This feature is commonly used to keep IPv4 subnet sizes small while enabling a WLAN to scale to thousands of users across multiple VLANs in the group. To support IPv6 clients with interface groups, no additional configuration is required as the system automatically sends the correct router advertisement to the correct clients via L2 wireless unicast. By unicasting the router advertisement, clients on the same WLAN, but a different VLAN, do not receive the incorrect RA.

Note: It is not recommended to mix IPv4 and IPv6 dual stack clients in the same Interface Group.

First Hop Security for IPv6 Clients

Router Advertisement Guard



The RA Guard feature increases the security of the IPv6 network by dropping router advertisements coming from wireless clients. Without this feature, misconfigured or malicious IPv6 clients could announce themselves as a router for the network, often with a high priority, which could take precedence over legitimate IPv6 routers.

By default, RA guard is enabled at the AP (but can be disabled) and is always enabled on the controller. Dropping RAs at the AP is preferred as it is a more scalable solution and provides enhanced per-client RA drop counters. In all cases, the IPv6 RA is dropped at some point, protecting other wireless clients and upstream wired network from malicious or misconfigured IPv6 clients.

DHCPv6 Server Guard

The DHCPv6 Server guard feature prevents wireless clients from handing out IPv6 addresses to other wireless clients or wired clients upstream. To prevent DHCPv6 addresses from being handed out, all DHCPv6 advertise packets from wireless clients are dropped. This feature operates on the controller, requires no configuration and is enabled automatically.

IPv6 Source Guard

The IPv6 source guard feature prevents a wireless client spoofing an IPv6 address of another client. This feature is analogous to IPv4 source guard. IPv6 source guard is enabled by default.

IPv6 Access Control Lists

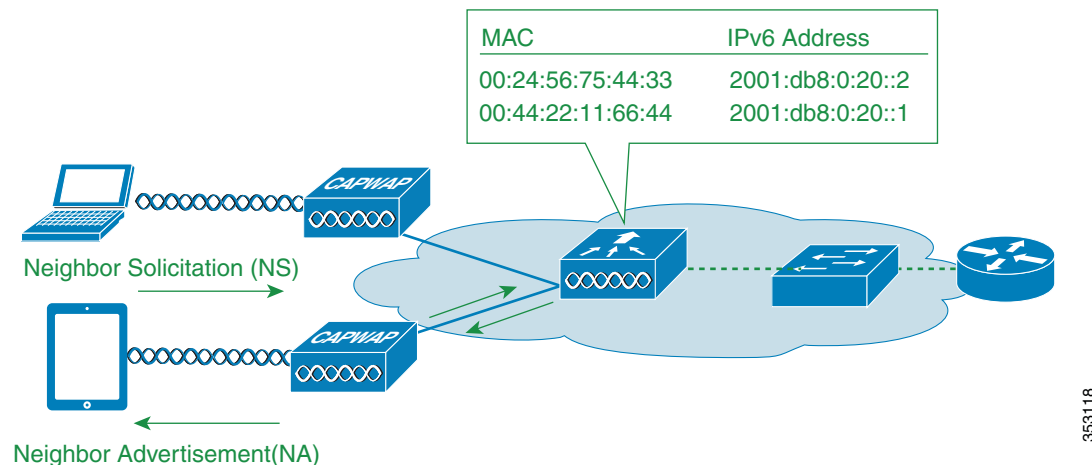
In order to restrict access to certain upstream wired resources or block certain applications, IPv6 Access Control lists can be used to identify traffic and permit or deny it. IPv6 Access Lists support the same options as IPv4 Access Lists including source, destination, source port, and destination port (port ranges are also supported). The wireless controller supports up to 64 unique IPv6 ACLs each with 64 unique rules in each. The wireless controller continues to support an additional 64 unique IPv4 ACLs with 64 unique rules in each for a total of 128 ACLs for a dual-stack client.

AAA Override for IPv6 ACLs

In order to support centralized access control through a centralized AAA server such as Cisco’s Identity Services Engine (ISE) or ACS, the IPv6 ACL can be provisioned on a per-client basis using AAA Override attributes. To use this feature, the IPv6 ACL must be configured on the controller and the WLAN must be configured with the **AAA Override** feature enabled. The actual named AAA attribute for an IPv6 ACL is **Airespace-IPv6-ACL-Name** similar to the **Airespace-ACL-Name** attribute used for provisioning an IPv4-based ACL. The AAA attribute contents must be equal to the name of the IPv6 ACL as configured in the controller.

Network Resource Efficiency for IPv6 Clients

Neighbor Discovery Caching



The IPv6 neighbor discovery protocol (NDP) utilizes Neighbor Advertisement (NA) and Neighbor Solicitation (NS) packets in place of ARP to allow IPv6 clients to resolve the MAC address of other clients on the network. The NDP process initially uses multicast addresses to perform address resolution. This process consumes valuable wireless airtime because the multicast addresses are sent to all the clients in the network segment.

Phase 1–Client IPv6 Support in WLC Release 7.2 to 7.6

To increase the efficiency of the NDP process, neighbor discovery caching allows the controller to act as a proxy and responds back to the NS queries that it can support address resolution and duplicate address detection. Neighbor discovery caching is made possible by the underlying neighbor binding table present in the controller. The neighbor binding table keeps track of each IPv6 address and its associated MAC address. When an IPv6 client attempts to resolve another client's link-layer address, the neighbor solicitation packet is intercepted by the controller that responds back with a neighbor advertisement packet.

Router Advertisement Throttling

Router Advertisement (RA) throttling allows the controller to enforce rate limiting of RAs headed towards the wireless network. By enabling RA throttling, routers that are configured to send RAs frequently (every 3 seconds) can be trimmed back to a minimum frequency that will still maintain IPv6 client connectivity. This allows airtime to be optimized by reducing the number of multicast packets that must be sent. In all cases, if a client sends a Router Solicitation (RS), then an RA will be allowed through the controller and unicast to the requesting client. This is to ensure that new clients or roaming clients are not negatively impacted by RA throttling.

Note: When RA throttling occurs, only the first IPv6 capable router are allowed through. For networks that have multiple IPv6 prefixes being served by different routers, RA throttling must be disabled.

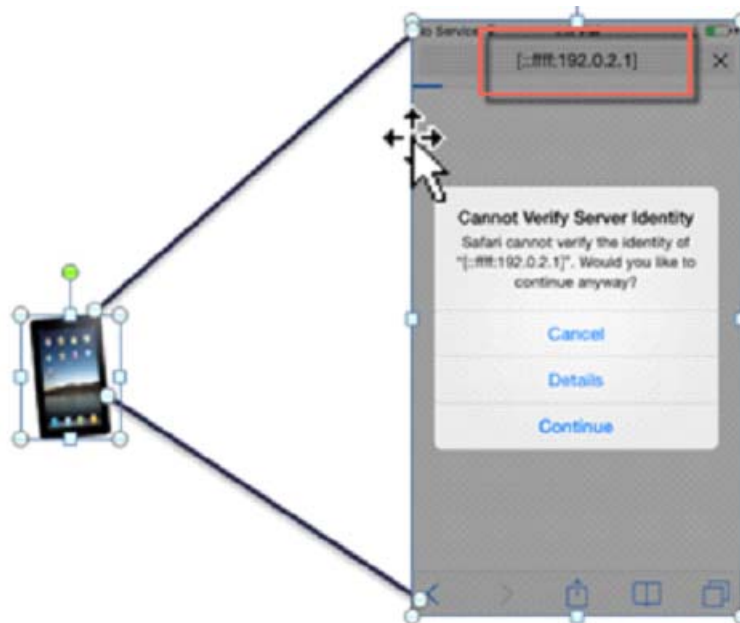
IPv6 Guest Access

The wireless and wired guest features present for IPv4 clients work in the same manner for dual-stack and IPv6-only clients. Once the guest user associates, they are placed in a “WEB_AUTH_REQ” run state until the client is authenticated via the IPv4 or IPv6 captive portal. The controller will intercept both IPv4 and IPv6 HTTP and HTTPS traffic in this state and redirect it to the virtual IP address of the controller. Once the user is authenticated via the captive portal, their MAC address is moved to the run state and both IPv4 and IPv6 traffic is allowed to pass.

To support the redirection of IPv6-only clients, the controller automatically creates an IPv6 virtual address based on the IPv4 virtual address configured on the controller. The virtual IPv6 address follows the convention of `[::ffff:<virtual IPv4 address>]`. For example, a virtual IP address of 192.0.2.1 would translate into `[::ffff:192.0.2.1]`.

The screenshot shows the Cisco WLC configuration page for a virtual interface. The interface name is 'virtual' and the MAC address is '00:24:97:69:9b:e0'. Under the 'Interface Address' section, the IP Address field is highlighted with a red box and contains the value '192.0.2.1'. The DNS Host Name field is empty. A note at the bottom states: 'Note: Changing the Interface parameters causes the WLANs to be temporarily disabled and thus may result in loss of connectivity for some clients.'

Enter an IPv6 enabled URL such as www.ipv6.google.com or an IPv6 address of a web site, for example—`[2001::120]`. The controller will intercept IPv6 HTTP and HTTPS traffic in this state and redirect it to the IPv6 virtual IP address of the controller as shown below:



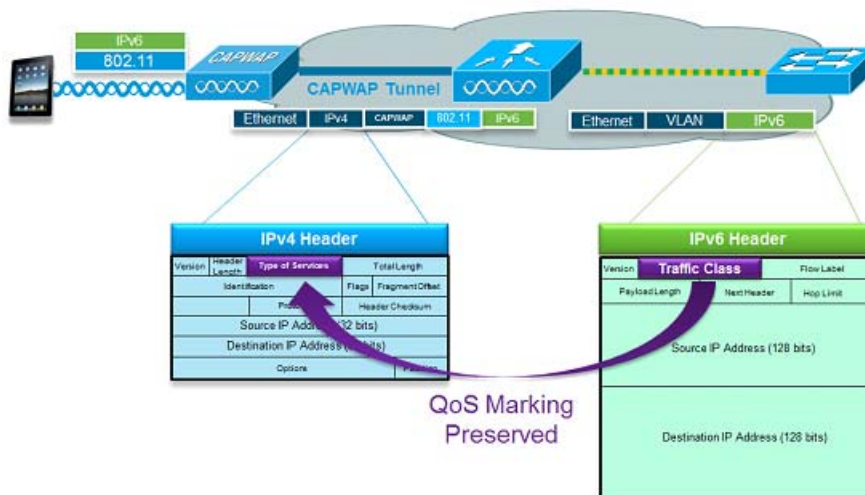
When using a trusted SSL certificate for guest access authentication, ensure that both the IPv4 and IPv6 virtual address of the controller is defined in DNS to match the SSL certificates hostname. This ensures that clients do not receive a security warning stating that the certificate does not match the hostname of the device.

IPv6 VideoStream



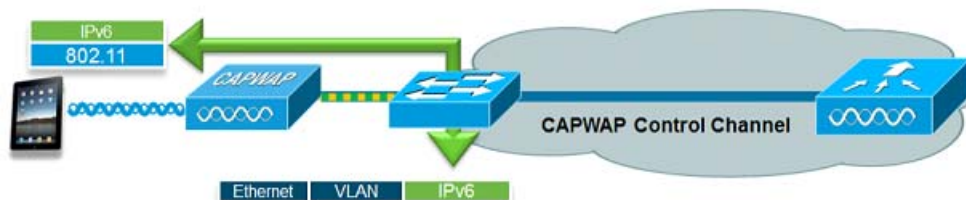
VideoStream enables reliable and scalable wireless multicast video delivery, sending each client VideoStream in a unicast format. The actual multicast to unicast conversion (of L2) occurs at the AP providing a scalable solution. In Release 8.0, the controller sends the IPv6 video traffic inside an IPv4 or IPv6 CAPWAP multicast tunnel which allows efficient network distribution to the AP.

IPv6 Quality of Service



IPv6 packets use a similar marking to IPv4’s use of DSCP values supporting up to 64 different traffic classes (0 – 63). For downstream packets from the wired network, the IPv6 “Traffic Class” value is copied to the header of CAPWAP tunnel to ensure that QoS is preserved end-to-end. In the upstream direction, the same occurs because client traffic marked at Layer 3 with IPv6 traffic class will be honored by marking the CAPWAP packets destined for the controller.

IPv6 and FlexConnect



FlexConnect–Local Switching WLANs

FlexConnect in local switching mode supports IPv6 clients by bridging the traffic to the local VLAN, similar to IPv4 operation. Client mobility is supported for Layer 2 roaming across the FlexConnect group.

The following IPv6-specific features are supported in FlexConnect mode:

- IPv6 RA Guard
- IPv6 Bridging
- IPv6 Guest Access

The following IPv6-specific features are not supported in FlexConnect local switching mode:

- IPv6 Access Control Lists
- IPv6 Source Guard
- Neighbor Discovery Caching

Phase 1–Client IPv6 Support in WLC Release 7.2 to 7.6

- DHCPv6 Server Guard
- Router Advertisement Throttling
- Layer 3 Mobility
- IPv6 VideoStream

FlexConnect–Central Switching WLANs

In release 8.0, FlexConnect can join CAPWAP multicast group. The controller should be set to **Multicast – Multicast mode** for both **AP Multicast mode** and **IPv6 AP Multicast mode**.

Note: FlexConnect mode APs will join IPv4 or IPv6 Multicast group if AP Multicast mode is configured as **Multicast** in release 8.0; however, there will be slight Data through-put degradation impact in the FlexConnect centrally switched scenario compared to AP Multicast mode configured as **Unicast**.

Note: Smart AP image upgrade does not work on the 7500 controllers when the primary AP is connected over CAPWAPv6.

The following IPv6 specific features are not supported in FlexConnect central switching mode:

- Layer 3 Mobility
- IPv6 VideoStream

Configuration for Wireless IPv6 Client Support

Configuring Global Controller (Screen Shots from Release 8.0)

Complete these steps:

1. Go to the **Controller** tab under the **General** page, do the following:
 - From the **AP Multicast Mode** drop-down list, choose **Multicast** and enter a valid multicast group address in the **Multicast Group Address** text box.
 - From the **AP IPv6 Multicast Mode** drop-down list, choose **Multicast** and enter a valid IPv6 multicast group address in the **IPv6 Multicast Group Address** text box. The IPv6 multicast group address must be in the **FFXX::/16** range which is scoped for IPv6 multicast applications.

The screenshot shows the Cisco WLC configuration interface. The 'Controller' tab is active, and the 'General' page is selected. The 'Multicast' section is expanded, showing the following configuration:

Field	Value	Label
Name	5508-MA6	
802.3x Flow Control Mode	Disabled	
LAG Mode on next reboot	Disabled	(LAG Mode is currently disabled).
Broadcast Forwarding	Disabled	
AP Multicast Mode	Multicast	Multicast Group Address
AP IPv6 Multicast Mode	Multicast	IPv6 Multicast Group Address
AP Fallback	Enabled	
Fast SSID change	Disabled	
Link Local Bridging	Disabled	

Phase 1–Client IPv6 Support in WLC Release 7.2 to 7.6

Note: It is important to perform this step for configuring the 2500 Series Wireless Controller. To enable efficient multicast transmission, perform this step in all wireless controller.

If the FlexConnect mode APs are used for centrally switched IPv6 WLANs, do the following:

- From the **AP Multicast Mode** drop-down list, choose **Unicast**.
- From the **AP IPv6 Multicast Mode** drop-down list, choose **Unicast**.

The screenshot shows the Cisco WLC configuration interface. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', and 'HELP'. The left sidebar lists various configuration categories, with 'Multicast' selected. The main area shows the 'General' configuration for a controller named '5508-MA6'. The following table summarizes the configuration items shown:

Configuration Item	Value
Name	5508-MA6
802.3x Flow Control Mode	Disabled
LAG Mode on next reboot	Disabled
Broadcast Forwarding	Disabled
AP Multicast Mode	Unicast
AP IPv6 Multicast Mode	Unicast
AP Fallback	Enabled
Fast SSID change	Disabled
Link Local Bridging	Disabled

A red box highlights the 'AP Multicast Mode' and 'AP IPv6 Multicast Mode' settings. A note indicates '(LAG Mode is currently disabled)'. The Cisco logo and version number '353124' are also visible.

2. Connect an IPv6 capable client to the wireless LAN. To validate that the client receives an IPv6 address, go to **Monitor > Clients > Detail**.

The screenshot shows the Cisco WLC Monitor interface. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', and 'MANAGEMENT'. The left sidebar lists 'Monitor' categories, with 'Clients' selected. The main area shows the 'Clients > Detail' page for a specific client. The following table summarizes the client properties shown:

Client Property	Value
MAC Address	f8:1e:df:e3:0a:76
IPv4 Address	192.168.20.30
IPv6 Address	2001:db8:0:20:518:e245:bbf8:f935, 2001:db8:0:20:fa1e:dfff:fee3:a76, fe80::fa1e:dfff:fee3:a76,

A red box highlights the IPv6 address field. The Cisco logo and version number '353125' are also visible.

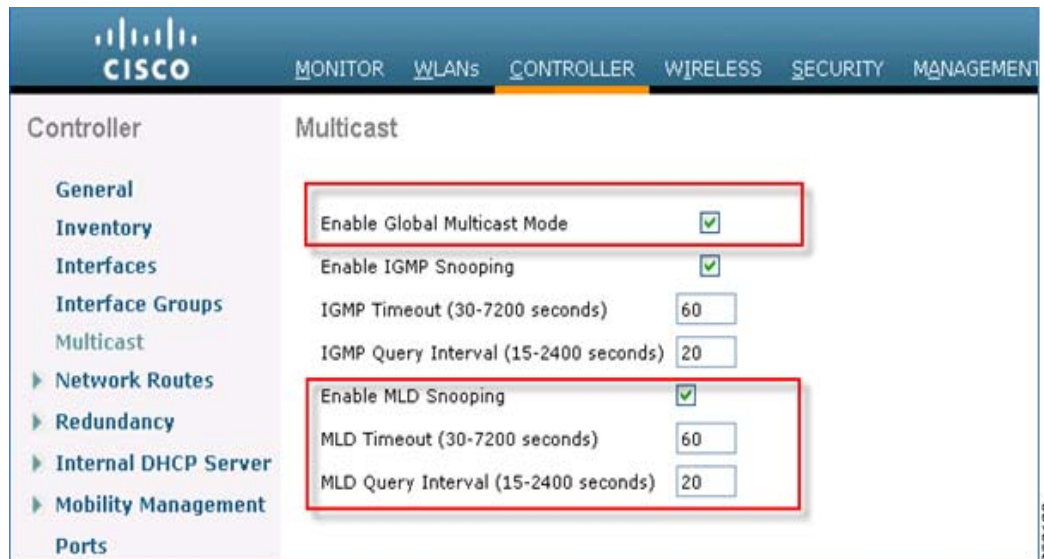
Configuring IPv6 Multicast

The controller supports MLDv1 snooping for IPv6 multicast allowing it to intelligently keep track of and deliver multicast flows to clients that request them.

Note: Unlike previous versions of releases, IPv6 Unicast traffic support does not mandate that “Global Multicast Mode” be enabled on the controller. IPv6 Unicast traffic support is enabled automatically.

Complete these steps:

1. Go to the **Controller** tab > **Multicast** page. To support multicast IPv6 traffic, check the **Enable MLD Snooping** check box. In order for IPv6 Multicast to be enabled, the **Enable Global Multicast Mode** of the controller must be enabled as well.



2. To verify that IPv6 multicast traffic is being snooped, go to the **Monitor** tab > **Multicast** page. Notice that both IPv4 (IGMP) and IPv6 (MLD) multicast groups are listed. Click the “MGID” to view the wireless clients joined to that group address.

The screenshot shows the Cisco WLC Monitor page with the 'Multicast' tab selected. The 'Layer3 MGID(Multicast Group ID) Mapping' table is displayed, showing the mapping between Group address, Vlan, MGID, and IGMP/MLD. The table is as follows:

Group address	Vlan	MGID	IGMP/MLD
224.0.0.251	20	1106	IGMP
224.0.0.252	20	1101	IGMP
239.255.255.250	20	1103	IGMP
ff02::c	20	1102	MLD
ff02::fb	20	1105	MLD
ff02::1:3	20	1100	MLD
ff02::2:fb5:a199	20	1110	MLD

The 'Multicast' tab in the left sidebar and the entire table are highlighted with a red box. The Cisco logo and navigation tabs (MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT) are visible at the top.

353127

Configuring IPv6 RA Guard

Complete these steps:

1. Go to the **Controller** tab and then **IPv6 > RA Guard** page.
2. From the **IPv6 RA Guard on AP** drop-down list, choose **Enable**. RA Guard on the controller cannot be disabled. Along with **RA Guard** configuration, this page also displays any clients that have been identified as sending RAs.

The screenshot shows the Cisco WLC Controller page with the 'IPv6 > RA Guard' configuration page. The 'IPv6 RA Guard on WLC' is set to 'Enabled' and 'IPv6 RA Guard on AP' is set to 'Enable'. Below this, there is a section for 'RA Dropped per client:' with a table header:

MAC Address	AP Name	WLAN	Number of RA Dropped

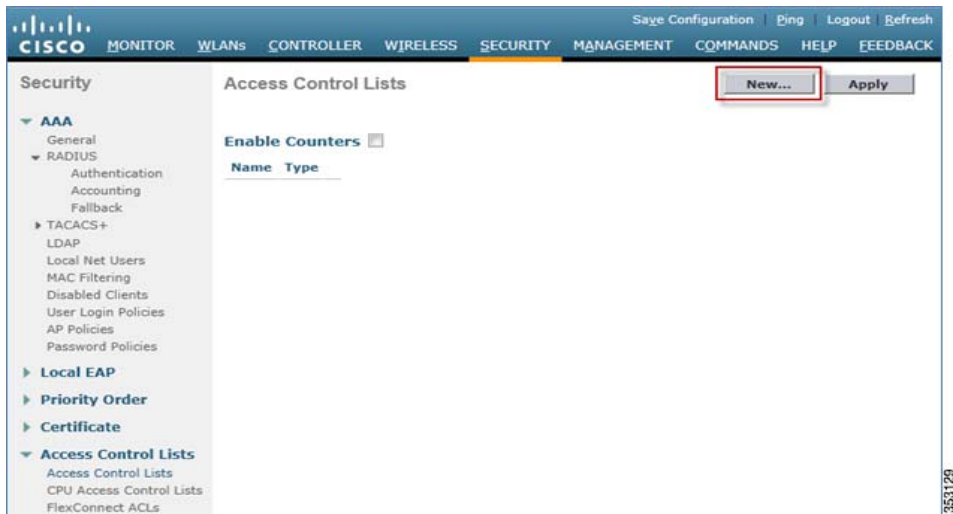
The 'IPv6 RA Guard on AP' dropdown menu is highlighted with a red box. The left sidebar shows the 'Controller' menu with 'IPv6' expanded. The Cisco logo and navigation tabs (MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, HELP) are visible at the top.

353128

Configuring IPv6 Access Control Lists

Complete these steps:

1. Go to the **Security** tab.
2. In the left pane, click **Access Control Lists**.
3. Click **New**.



4. Enter a unique name for the ACL, change the ACL Type to **IPv6**, and click **Apply**.

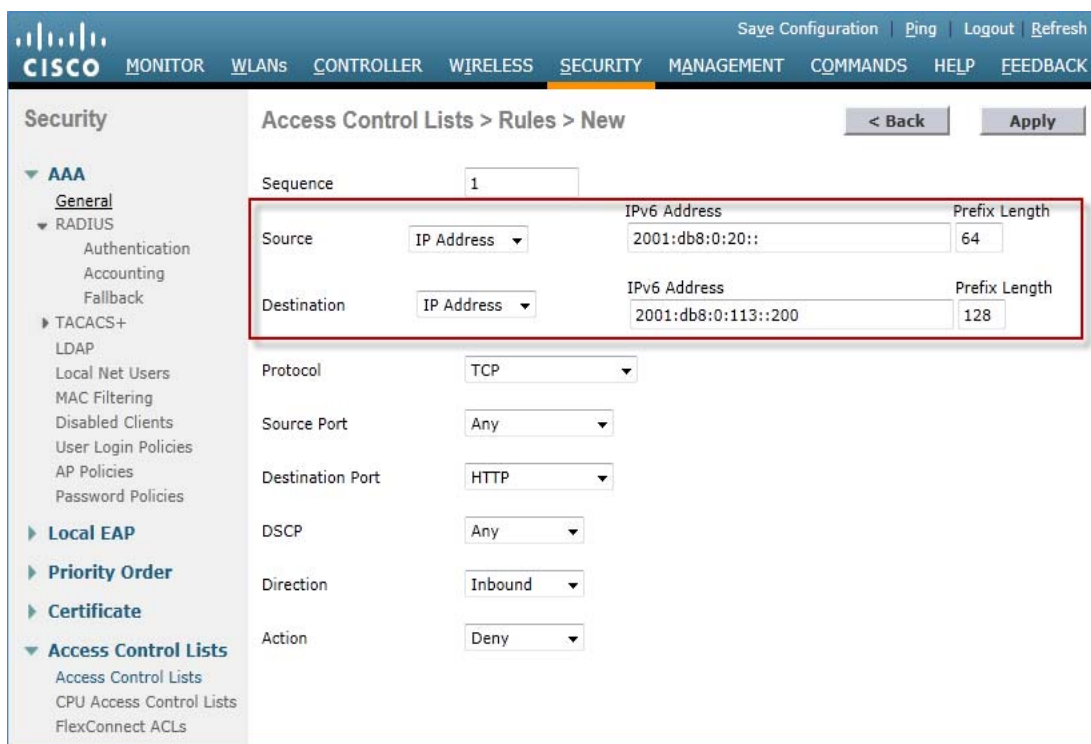


5. Click the new ACL that was created in the above steps.

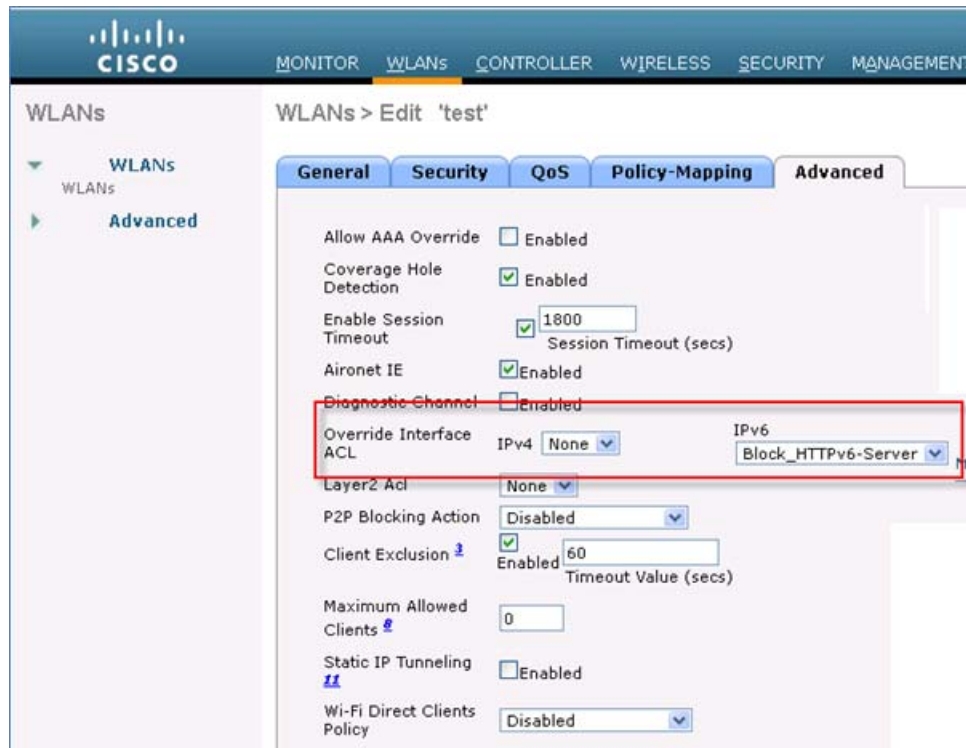
Phase 1–Client IPv6 Support in WLC Release 7.2 to 7.6



- Click **Add New Rule**, and enter the desired parameters for the rule, and click **Apply**. Leave the sequence number blank to place the rule at the end of the list. The **Direction** option of **Inbound** is used for traffic coming from the wireless network, and **Outbound** for traffic destined for wireless clients. Remember, the last rule in an ACL is an implicit deny-all.



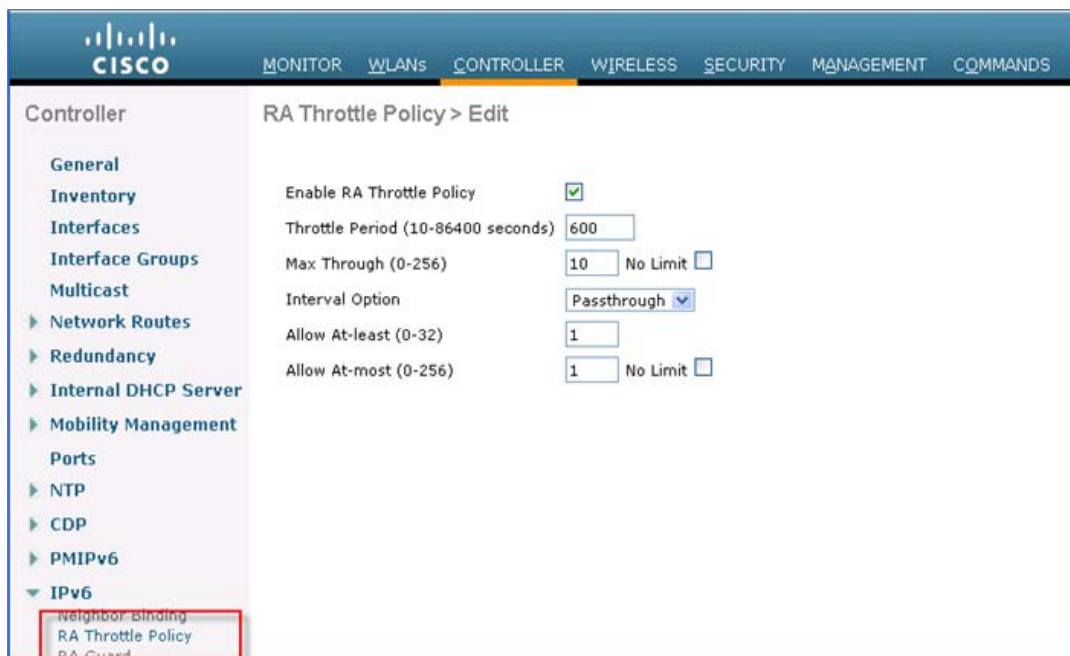
- IPv6 ACLs are applied on a per WLAN/SSID basis and can be used on multiple WLANs concurrently. To apply the IPv6 ACL, navigate to the **WLANs** tab and click the WLAN ID of the SSID in question. Click the **Advanced** tab and change the **Override Interface ACL for IPv6** to the ACL name.



Configuring IPv6 RA Throttling

Complete these steps:

1. Go to the **Controller** tab.
2. In the left pane, click **IPv6 > RA Throttle Policy**.
3. Check the **Enable RA Throttle Policy** check box. Adjust the throttle period and other options as required. However, the default is recommended for most deployments.



Each RA Throttling option is described below:

- Throttle Period: The period of time that throttling takes place. RA throttling takes effect only after the “Max Through” limit is reached for the VLAN.
- Max Through: This is the maximum number of Router Advertisements on the VLAN before throttling kicks in. The “No Limit” option allows an unlimited amount of RAs through with no throttling.
- Interval Option: The interval option allows the controller to act differently based on the RFC 3775 value set in the IPv6 RA.
 - Passthrough – This value allows any RAs with an RFC3775 interval option to go through without throttling.
 - Ignore – This value will cause the RA throttler to treat packets with the interval option to be treated as a regular RA and subject to throttling if in effect.
 - Throttle – This value will cause the RAs with the interval option to always be subject to rate limiting.
- Allow At-least: The minimum number of Router Advertisements per router that will be sent as multicast before throttling takes effect.
- Allow At-most: The maximum number of Router Advertisements per router that will be sent as multicast before throttling takes effect. The “No Limit” option will allow an unlimited amount of RAs through for that router.

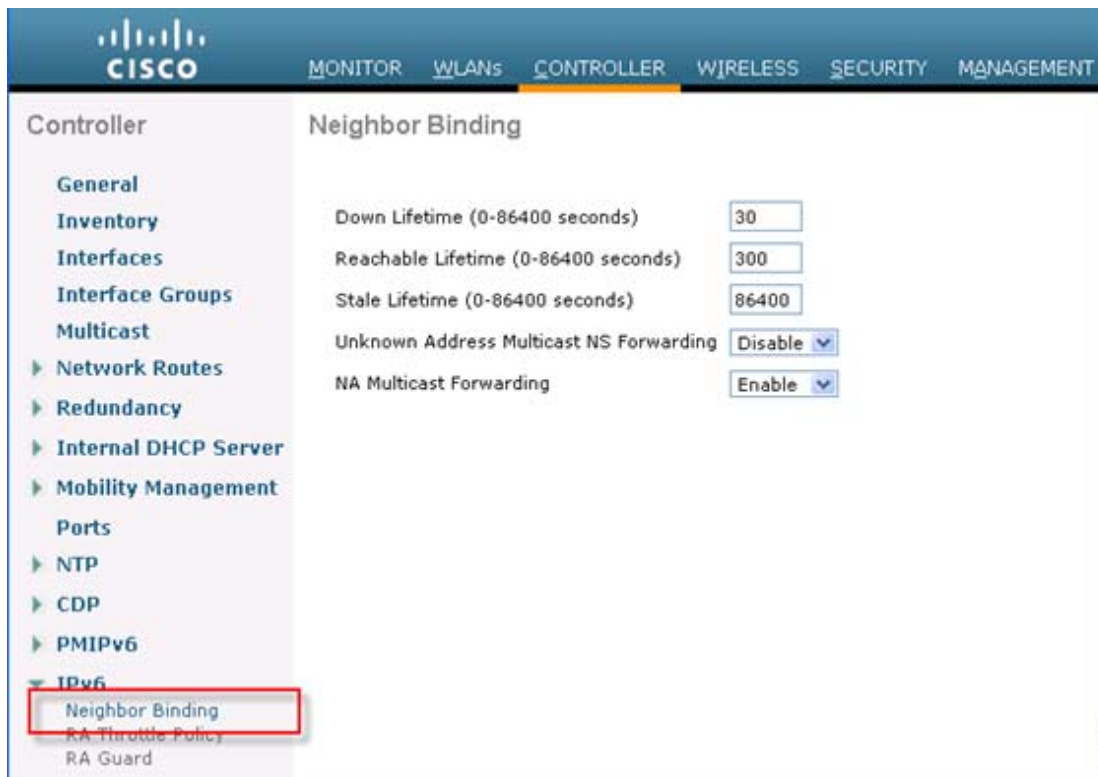
The numerical values of the **Allow At-least** option must be less than the **Allow At-most** option which should be less than **Max Through** option.

Configuring the IPv6 Neighbor Binding Table

Complete these steps:

1. Go to the **Controller** tab.

2. In the left pane, click **IPv6 > Neighbor Binding**.



3. Adjust the Down Lifetime, Reachable Lifetime, and Stale Lifetime as required. The default values should be sufficient for most deployments.

Each lifetime timer refers to the state that an IPv6 address can be in:

- **Down Lifetime** – The down timer specifies how long IPv6 cache entries should be kept if the interface goes down.
- **Reachable Lifetime** – This timer specifies how long an IPv6 address will be marked active, which means traffic has been received from this address recently.
- **Stale Lifetime** – This timer specifies how long to keep IPv6 addresses in the cache which have not been seen within the “Reachable Lifetime”.

Configuring IPv6 VideoStream

Complete these steps:

1. Ensure Global VideoStream features are enabled on the controller.

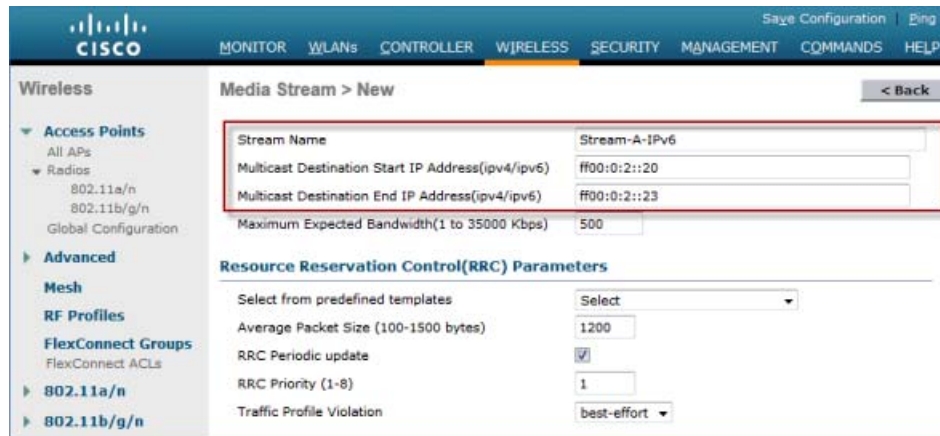
Refer to [Cisco Unified Wireless Network Solution: VideoStream Deployment Guide](#) for information on enabling VideoStream on the 802.11a/g/n network as well as the WLAN SSID.

2. Go to the **Wireless** tab on the controller.
3. In the left pane, click **Media Stream > Streams**.
4. Click **Add New** to create a new stream.

Phase 2–Infrastructure IPv6 Support in WLC Release 8.0 and Later



5. Name the stream and enter the start and end IPv6 addresses. When using only a single stream, the start and end addresses are equal. After adding the addresses, click **Apply** to create the stream.



Phase 2–Infrastructure IPv6 Support in WLC Release 8.0 and Later

This section provides a set of instructions to effectively configure native IPv6 features based on WLC Release 8.0.

The following are the Infrastructure IPv6 configuration items:

- Address assignment
- PING for IPv6
- Management access (Wired and Wireless)–Telnet/SSH/HTTP/HTTPs
- CAPWAPv6

Phase 2—Infrastructure IPv6 Support in WLC Release 8.0 and Later

- UDP Lite for IPv6
- Tunnel switch
- CAPWAP Preferred mode
- Data DTLS
- Mobility Configuration - L3
- Auto Anchor/Guest Access
- WebAuth for pure IPv6 client
- NTP over IPv6
- Syslog over IPv6
- Radius Over IPv6
- CDP v6
- Flex Connect Central/Local switching with CAPWAP IPv4/IPv6 but IPv4 clients only
- Service port SLAAC configuration

This section will not discuss standard controller features that were covered in earlier configuration and deployment guides.

Enabling IPv6 on Your IOS Infrastructure Device

Enabling IPv6 on an individual infrastructure device to which wireless controller will be connected.

Refer to the following Cisco documentations for configuring IPv6 on other IOS devices.

<http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6/configuration/15-2mt/ipv6-15-2mt-book.pdf>

http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750/software/release/12-2_55_se/configuration/guide/scg3750/swipv6.html

See [Appendix A, page 46](#) for sample IPv6 configurations on the 3750 switch.

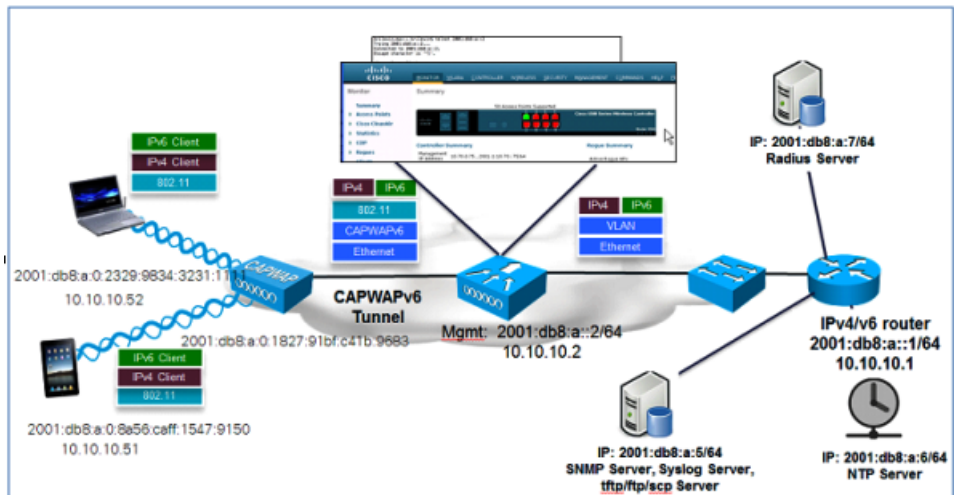
Controller Configuration for IPv6 Support

Controller configuration for the native IPv6 support is similar to that of the IPv4 controller with the exception of the few interfaces accepting the IPv6 addresses as demonstrated in the following examples:

- Management solution supports one IPv6 address (+ LLA address).
- Dynamic interfaces support only IPv4 addresses.
- Dynamic AP manager supports only IPv4 addresses.
- Redundancy management/Redundancy port (HA interfaces support IPv4 only) supports only IPv4 addresses.
- Service-port can get an IPv6 address statically or using SLAAC (Only SLAAC interface is supported on the WLC).
- LAG is required for IPv6 AP load balancing.

DHCPv6 Proxy is not supported on dynamic interfaces (Only IPv6 DHCP bridging is supported- like 7.6 legacy).

Phase 2—Infrastructure IPv6 Support in WLC Release 8.0 and Later



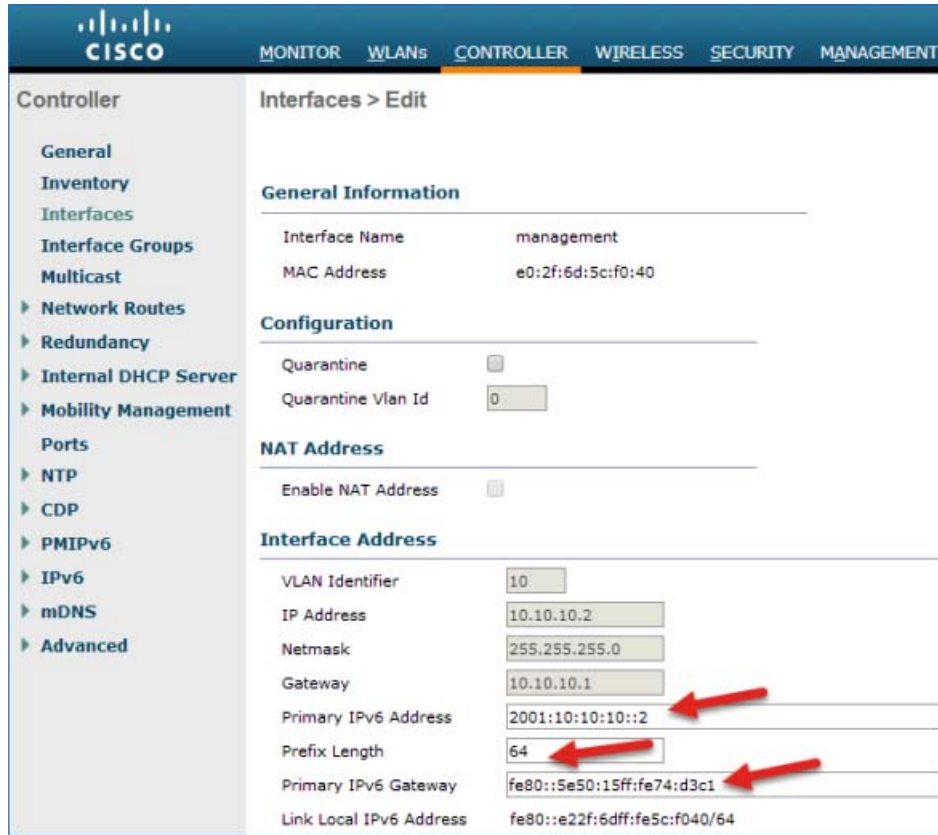
1. To configure the IPv6 address for WLC, from the WLC’s main menu, go to **Controller > Interfaces > Management**.
 - a. In the **Interface Address** area, enter the Primary IPv6 Address in the **2001:XX:XX:X0::XX** format. Enter the Prefix Length as **64**. In **Primary IPv6 Gateway** text box, assign the Link-Local address of the VLAN X0.
 - b. Login/telnet to the default gateway and run the command:

`show ipv6 int brief` Or `show ipv6 int vlanX0`.
 - c. Now, copy/paste the specific link-local address to the WLC Primary IPv6 Gateway.

The following screenshot displays an example of the link local address for VLAN10 on a sample Core-Switch.

```
SEUT-core-SW#sh ipv6 int br
Vlan1 [administratively down/down]
      unassigned
Vlan10 [up/up]
      FE80::5E50:15FF:FE74:D3C1
      2001:10:10:10::4
```

When you copy/paste the Link Local IPv6 address in the **Primary IPv6 Gateway** text box, ensure that there is no space in the beginning and end of the Link local IPv6 address. Click **Apply** to save the settings.



The Management Interface is assigned a Link Local address by default. Global Unicast or Unique Local address must be configured on the management interface.

Gateway must be the Link-Local address of the next hop router.

A Management Link-Local address is assigned automatically to the management interface, but the Primary address must be a globally unique address.

2. Configure Dynamic interfaces:

- No IPv6 address is used, IPv4 address is used on the Dynamic Interface.
- An IPv6 address can exist on an IPv6 enabled switch/router because traffic is bridged on the VLAN.
- A DHCPv6 server or relay must exist on the VLAN interface at the switch/router

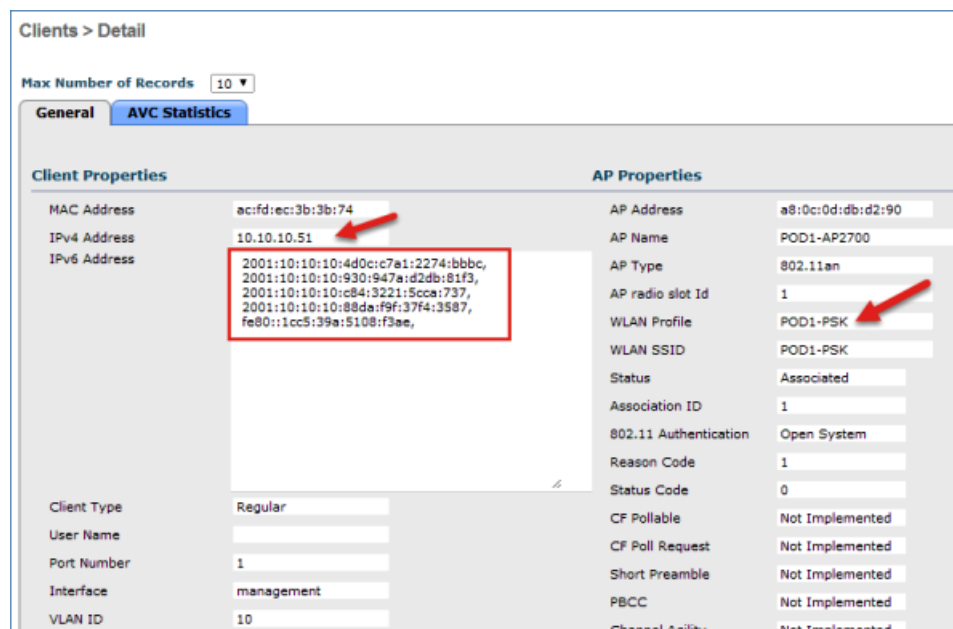
Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Management	IPv6 Address
management	10	10.10.10.2	Static	Enabled	2001:10:10:10::2/64
redundancy-management	10	10.10.10.10	Static	Not Supported	
redundancy-port	untagged	169.254.10.10	Static	Not Supported	
service-port	N/A	0.0.0.0	Static	Disabled	::/128
virtual	N/A	1.1.1.1	Static	Not Supported	

3. Once the IPv6 address is assigned to the WLC management interface, try accessing the WLC GUI, that is, launch [https://\[2001:10:10:X0::2\]](https://[2001:10:10:X0::2]) through your respective wired client connected to your controller.



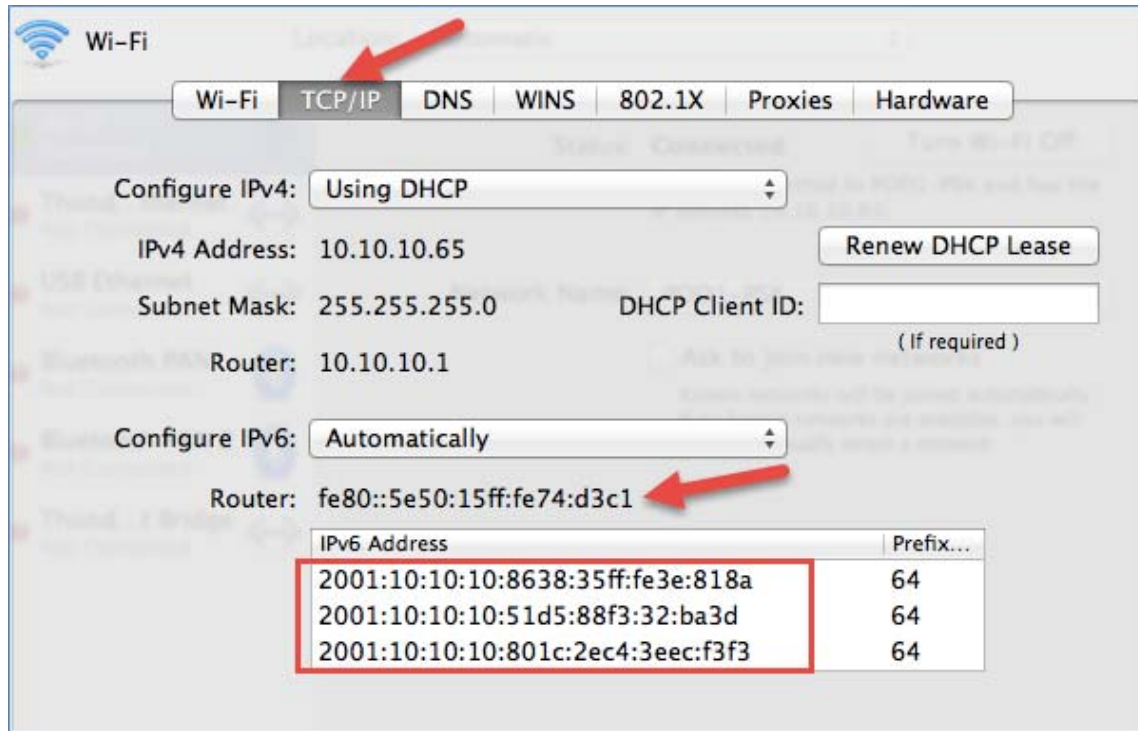
353142

- Associate a wireless client, that is, your iPhone/iPad/laptop, to your respective controller WLAN and check if the client is able to receive the IPv4 and IPv6 addresses. Also, go to **WLC > Monitor > Clients** and click the client MAC address to view the IPv4 and IPv6 addresses.



353143

The following screenshots display a client running MacOS, where the client is connected to the WLAN. The client receives both IPv4 and IPv6 addresses. Also, the client is able to ping the IPv6 address.



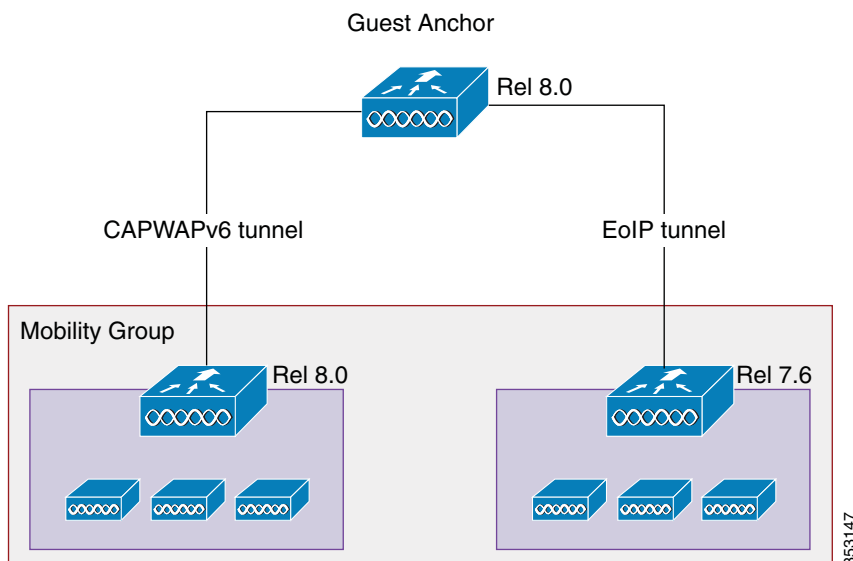
```

ali — bash — 80x24
Last login: Fri Mar 28 18:01:27 on ttys000
Alis-MacBook-Air:~ ali$ ping6 2001:10:10:10::1
PING6(56=40+8+8 bytes) 2001:10:10:10:8638:35ff:fe3e:818a --> 2001:10:10:10::1
16 bytes from 2001:10:10:10::1, icmp_seq=0 hlim=64 time=35.736 ms
16 bytes from 2001:10:10:10::1, icmp_seq=1 hlim=64 time=13.047 ms
16 bytes from 2001:10:10:10::1, icmp_seq=2 hlim=64 time=13.039 ms
16 bytes from 2001:10:10:10::1, icmp_seq=3 hlim=64 time=12.466 ms
16 bytes from 2001:10:10:10::1, icmp_seq=4 hlim=64 time=16.461 ms
16 bytes from 2001:10:10:10::1, icmp_seq=5 hlim=64 time=12.790 ms
16 bytes from 2001:10:10:10::1, icmp_seq=6 hlim=64 time=12.388 ms
16 bytes from 2001:10:10:10::1, icmp_seq=7 hlim=64 time=13.317 ms
^C
    
```

Mobility Group Configuration in Release 8.0

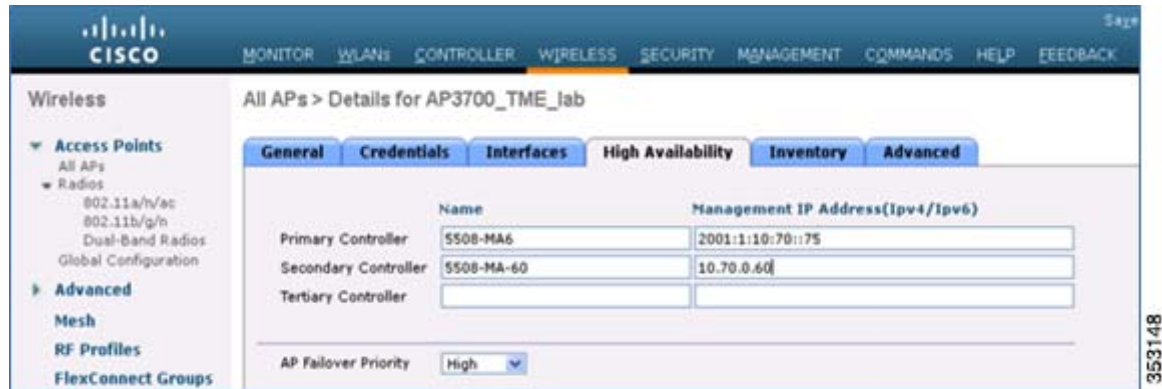
To support Mobility group configuration for Guest Anchor or Auto Anchor, the Guest Anchor should be on the 8.0 code to support controllers in release 8.0. This allows 8.0 WLCs sharing the mobility group to connect by using the CAPWAPv6 tunnel, and the WLCs running prior to release 8.0 will join by using the EoIP tunnel.

There is no need for New Mobility with this configuration. In this configuration mode, both ends of the Mobility tunnels have to be configured with IPv4 addresses. In pure 8.0 and later deployments, IPv6 addresses can be assigned and CAPWAPv6 can be used.



AP Join Prefer-Mode in Release 8.0

The Prefer-mode option allows administrators to configure IPv4 and IPv6 CAPWAP L3 transport through which APs will join the WLC based on the primary, secondary or tertiary configuration.

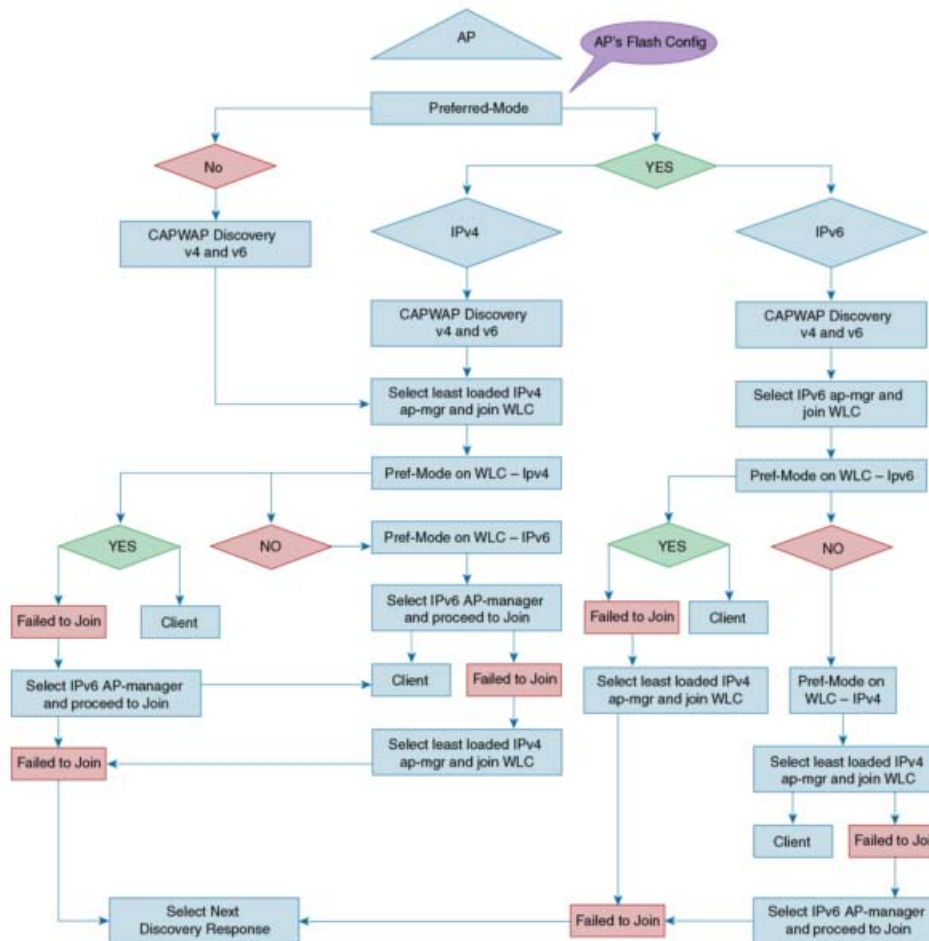


There are three levels of the prefer-mode option:

1. AP Group Specific
2. Global
3. Static IP configuration

CAPWAP Prefer-Mode Configuration

1. AP Group specific “prefer-mode” will be pushed to AP if the “prefer-mode” of the AP Group to which the AP belongs is configured.
2. Global prefer-mode will be pushed to default-group APs and to those AP Groups that do not have prefer-mode configured.
3. By default, AP Group prefer-mode will be un-configured and Global prefer-mode is set to IPv4.
4. If an AP tries to join the WLC with configured prefer-mode and it fails to join, then it will fall back to choose the AP manager of the other transport and joins the same WLC. When both transports fail, the AP will move to the next discovery response.



5. The Static IP configuration takes precedence over prefer-mode.

For example:

- Preferred mode configured as IPv4.
- Static IPv6 configuration on AP using CLI or GUI.
- AP joins the WLC using the IPv6 transport mode.

6. XML support of prefer-mode CLIs is provided.

7. Trap log is used when there is a failure in pushing the prefer-mode configuration to the AP.

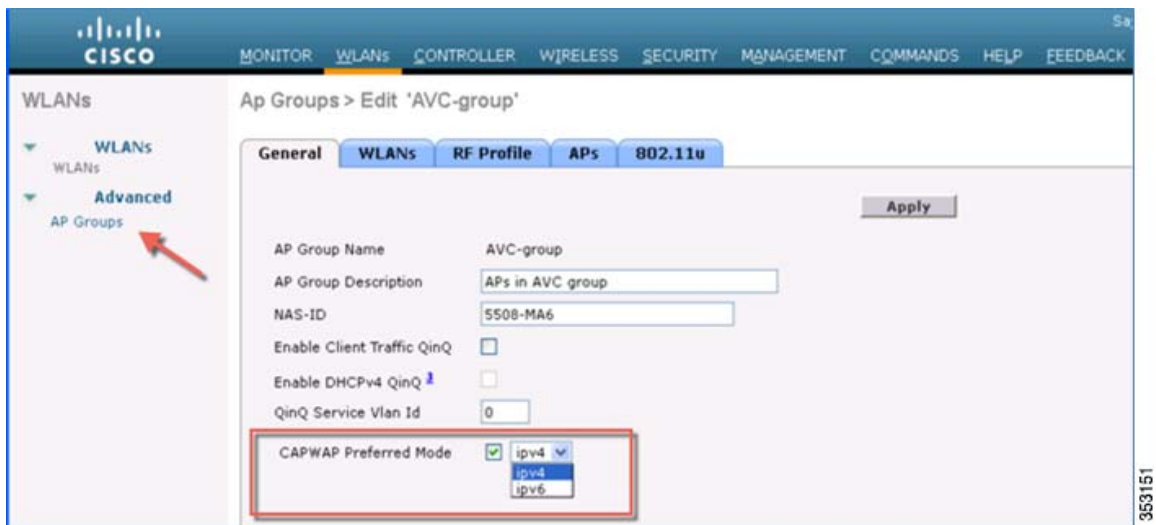
Configuring Preferred-Mode from the GUI

Complete these steps:

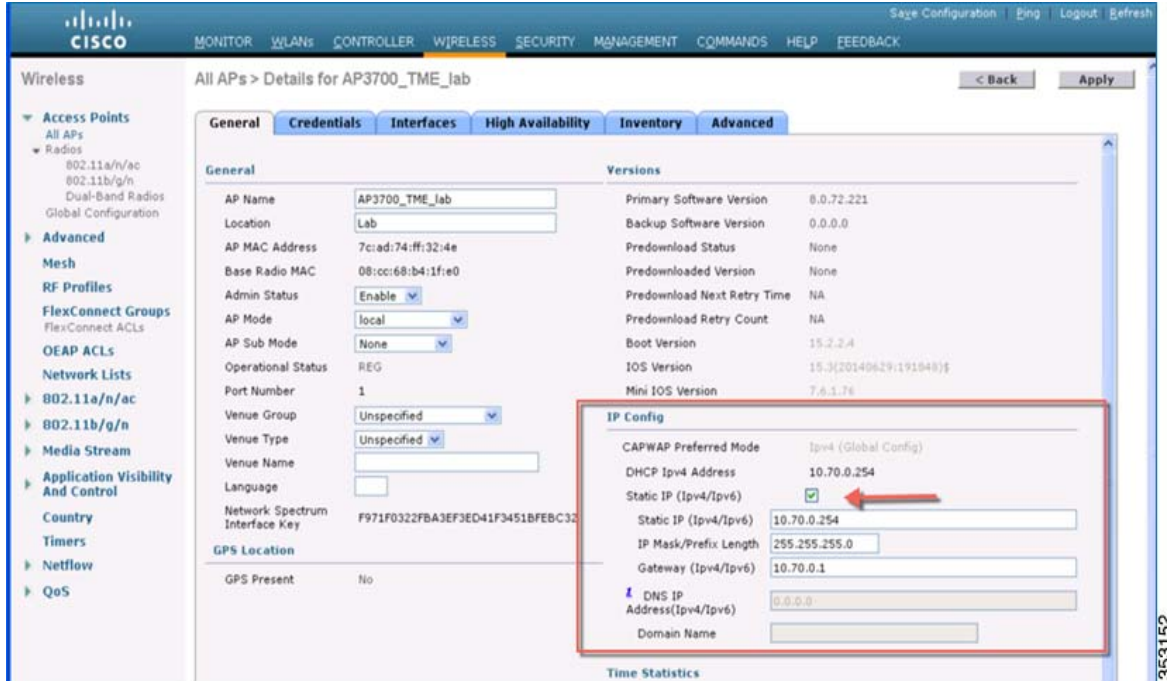
1. As indicated above, Global prefer-mode will be pushed to default-group APs and to those AP Groups that do not have prefer-mode configured. The following example displays the Global prefer-mode configuration in the GUI, where the IPv4 or IPv6 address is chosen for the CAPWAP preferred-mode.



2. AP Group specific prefer-mode will be pushed to AP if prefer-mode of the AP Group is configured to the AP it belongs. Global prefer-mode will be pushed to default-group APs and to those AP Groups that do not have prefer-mode configured. To configure in the GUI CAPWAP preferred mode for the AP Group, see the following example:



3. The following is an example of a Static IPv6 configuration for the CAPWAP preferred mode. As noted earlier, the Static IP configuration will take precedence over the prefer-mode.



Configuring Preferred-Mode from the CLI

```
config ap preferred-mode ipv4/ipv6 <apgroup>/<all>
```

This CLI command is used to configure the prefer-mode of the AP Group and all APs. Global prefer-mode is not applied to APs if the AP Group prefer-mode is already configured. After configuration, the AP restarts the CAPWAP to join with the configured prefer-mode after choosing the WLC based on its primary/secondary/tertiary configuration.

```
config ap preferred-mode disable <apgroup>
```

This CLI command is used to disable (unconfigure) the prefer-mode of the AP Group. APs that belong to <apgroup> restarts the CAPWAP and joins back with the global prefer-mode.

```
show ap prefer-mode stats
```

This CLI command is used to display the statistics of the prefer-mode configuration. Statistics are not cumulative, but is updated for the last executed CLI configuration of prefer-mode.

```
show wlan apgroups
```

This CLI command displays the prefer-modes that are configured for all the AP groups.

```
show network summary
```


Phase 2–Infrastructure IPv6 Support in WLC Release 8.0 and Later

```

WebPortal Online Client ..... 0
WebPortal NTF_LOGOUT Client ..... 0
mDNS snooping..... Disabled
mDNS Query Interval..... 15 minutes
Web Color Theme..... Default
Capwap Prefer Mode..... IPv4
(Cisco Controller) >
    
```

Ping IPv6 address of the GW in the AP using `ping 2001:10:10:x0::1`.

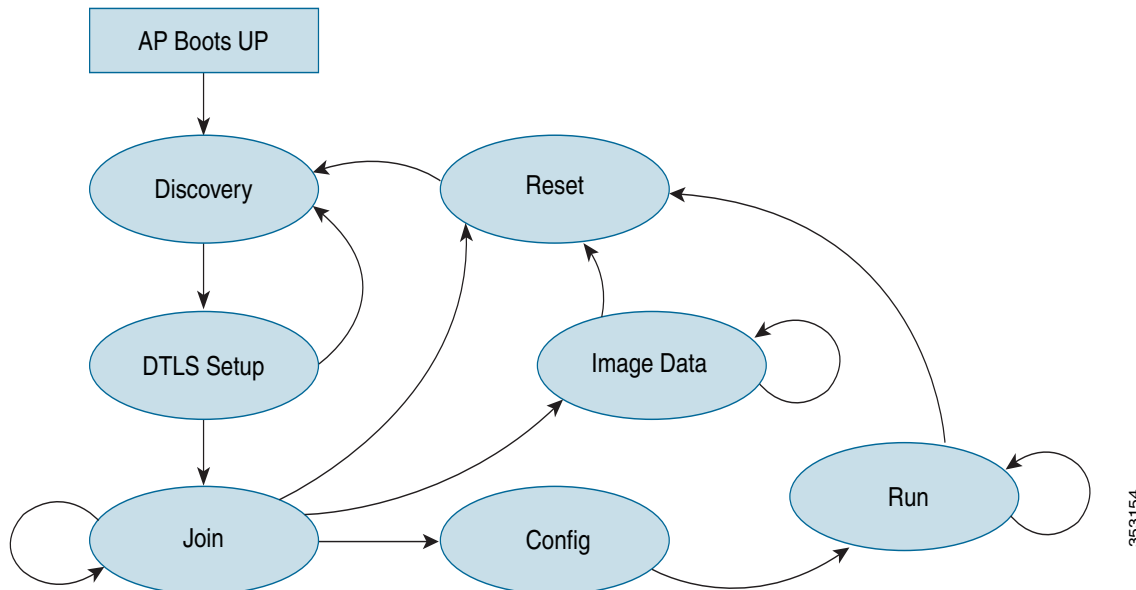
The AP rejoins the controller with pure IPv6 tunnel.

MONITOR	WLANs	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS
All APs						
Current Filter		None		[Change Filter] [Clear Filter]		
Number of APs		3				
AP Name	IP Address(Ipv4/Ipv6)	AP Model				
POD1-AP3600	10.10.10.54	AIR-CAP3602I-A-K9				
POD1-AP3700-1	10.10.10.71	AIR-CAP3702I-A-K9				
POD1-AP2700	2001:10:10:10:7d85:567d:beea:c636	AIR-CAP2702I-A-K9				

Configuring Additional IPv6 Features on the WLC

AP IPv6 Discovery Mechanism

Broadcasting is not supported in IPv6 addresses, so APs must use the following mechanisms to join a WLC via CAPWAPv6.



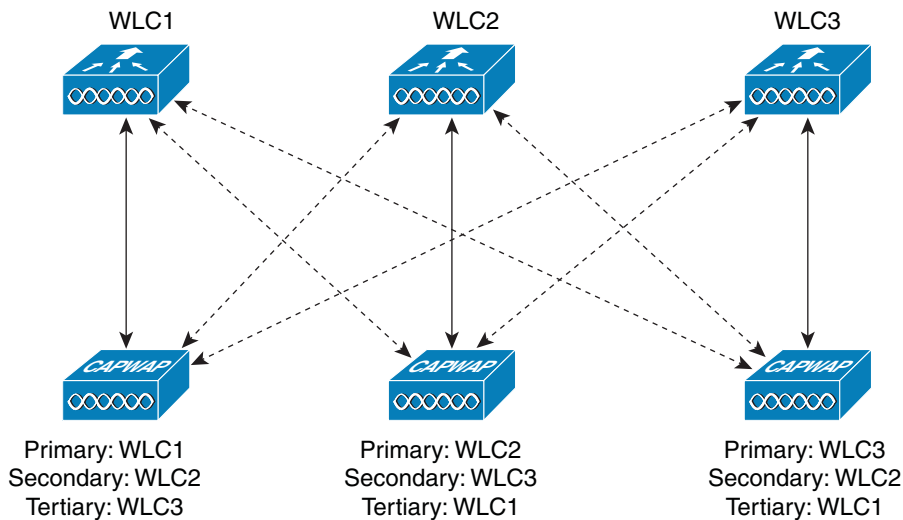
353154

- DHCPv6 Option 52:
 - OPTION_CAPWAP_AC_V6 (52) RFC 5417.
 - As part of the DHCPv6 response, the server provides the IPv6 WLC management IPv6 address.
 - The AP begins Unicast CAPWAP discovery.
- Multicast Discovery:
 - IPv6 address does not support broadcast.
 - Sends CAPWAP discovery messages to all APs multicast address (FF01::18C).
- Using DNS:
 - Configure the DNS server to resolve `cisco-capwap-controller.domain-name`
 - The `domain-name` is returned from the DHCPv6 server.
- AP Priming:
 - Preconfiguring the AP with a primary, secondary, and tertiary IPv6 address of the WLC management interface.

Selecting Primary, Secondary, and Tertiary Controllers

When selecting a primary, secondary, or tertiary controller, the process is similar to CAPWAPv4. The WLC management IP address can either be IPv4 or IPv6, it does not matter as long as the address is reachable. It is not possible to add both the IPv4 and IPv6 address because only one entry is allowed per WLC.

Phase 2–Infrastructure IPv6 Support in WLC Release 8.0 and Later



353155



353156

Once the AP selects a WLC, the AP chooses to join via CAPWAPv4 or CAPWAPv6, depending on the CAPWAP preferred-mode selected on the WLC.

PING IPv6 and IPv4 Addresses

You can ping IPv6 and IPv4 addresses from the controller interface. The following example shows how to use the ping protocol in an IPv6 management interface:

ping <ipv4/ipv6 address>

```
(Cisco Controller) >ping 2001:1:10:70::75

Send count=3, Receive count=3 from 2001:1:10:70::75
```

353157

Similar process can be followed in a switch interface.

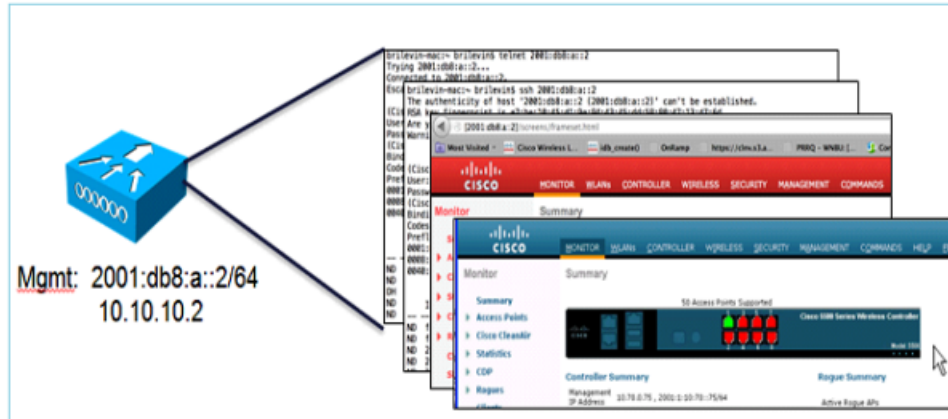
Management Access (Wired and Wireless)–Telnet/SSH/HTTP/HTTPs

The WLC (wired/wireless) is accessed in the IPv6 Management Interface using:

- Telnet
- SSH

Phase 2—Infrastructure IPv6 Support in WLC Release 8.0 and Later

- HTTP
- HTTPS



Dynamic interfaces do not have IPv6 addresses.

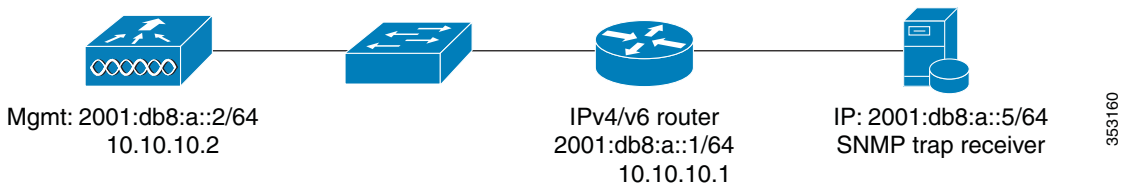
```
(Cisco Controller) >show ipv6 interface summary

Number of Interfaces..... 2

Interface Name      Port Vlan Id  IPv6 Address/Prefix Length
-----
management          1    70         fe80::1edf:fff:fec6:ala0/64
                   1    70         ::/128
service-port        N/A  N/A         fe80::1edf:fff:fec6:ala1/64
                   N/A  N/A         ::/128
```

SNMP Trap Receiver

In controller Release 8.0, SNMP MIBs are sent to the IPv6 destination. Prime Infrastructure will support IPv6 in Release 2.2 and later.



SNMP Trap Receiver > New

Community Name	<input type="text" value="private"/>
IP Address(Ipv4/Ipv6)	<input type="text" value="2001:db8:a::5"/>
Status	<input type="button" value="Enable"/> ▾
IPSec	<input type="checkbox"/>

353161

UDP Lite for IPv6

- Enabling UDP Lite speeds up the packet processing time.
- UDP Lite computes checksum on the pseudo header of the datagram.
- The IP protocol ID is 136 and it uses the same CAPWAP ports as UDP.
- Enabling UDP Lite requires that the network firewall allows protocol 136.
- Switching between UDP and UDP Lite causes all APs to re-join the WLC.
- UDP Lite is enabled by default.

Configuring UDP Lite

Complete these steps:

1. UDP lite can be configured per AP or globally for all APs.

```
(mavora-wlc-5500-2) >config ipv6 capwap udplite ?
enable      Enables IPv6 Capwap UDP Lite
disable     Disables IPv6 Capwap UDP Lite

(mavora-wlc-5500-2) >config ipv6 capwap udplite enable ?
all         Configure IPv6 Capwap UDP Lite on All Cisco APs
<Cisco AP> Enter Cisco AP name

(mavora-wlc-5500-2) >config ipv6 capwap udplite enable all
```

353162

2. Check the UDP Lite configuration using the `show ipv6 summary` command.

Phase 2—Infrastructure IPv6 Support in WLC Release 8.0 and Later

```
(Cisco Controller) >show ipv6 summary

Global Config..... Enabled
Reachable-lifetime value..... 300
Stale-lifetime value..... 86400
Down-lifetime value..... 30
RA Throttling..... Enabled
RA Throttling allow at-least..... 1
RA Throttling allow at-most..... 1
RA Throttling max-through..... 10
RA Throttling throttle-period..... 600
RA Throttling interval-option..... passthrough
NS Multicast CacheMiss Forwarding..... Disabled
NA Multicast Forwarding..... Enabled
IPv6 Capwap UDP Lite..... Enabled
Operating System IPv6 state ..... Enabled
```

353163

Data DTLS Enable

Like CAPWAPv6, DTLS also uses the AP's IPv6 address. DTLS is enabled by default on the APs. To verify this, enter the following command:

show dtls connections

```
(mavora-wlc-5500-2) >show dtls connections

  AP Name          Local Port    Peer IP          Peer Port        Ciphersuite
-----
1-V6-AP-1600-2_P13  Capwap_Ctrl  2001:9:5:94:206:f6ff:fe18:250c  33361            TLS_RSA_WI
1-V6-AP-1600-2_P13  Capwap_Data  2001:9:5:94:206:f6ff:fe18:250c  33361            TLS_RSA_WI
3-V4-AP-2602-1_P10  Capwap_Ctrl  2001:9:5:91:4498:d688:1500:8d90  43476            TLS_RSA_W
3-V4-AP-2602-1_P10  Capwap_Data  2001:9:5:91:4498:d688:1500:8d90  43476            TLS_RSA_W

(mavora-wlc-5500-2) >config ap li?
link-encryption link-latency
(mavora-wlc-5500-2) >config ap link?
link-encryption link-latency
(mavora-wlc-5500-2) >config ap link-encryption ?

enable      Enables Data Link encryption
disable     Disables Data Link encryption

(mavora-wlc-5500-2) >config ap link-encryption enable ?

<Cisco AP>   Enter the name of the Cisco AP.
all          Apply the configuration for all capable Cisco AP

(mavora-wlc-5500-2) >config ap link-encryption enable
```

353164

Configuring Data DTLS

DTLS can be enabled on an individual AP or globally for all APs with the command below:

config ap link-encryption <enable/disable>

Phase 2—Infrastructure IPv6 Support in WLC Release 8.0 and Later

```
(mavora-wlc-5500-2) >config ap link-encryption ?
enable      Enables Data Link encryption
disable     Disables Data Link encryption

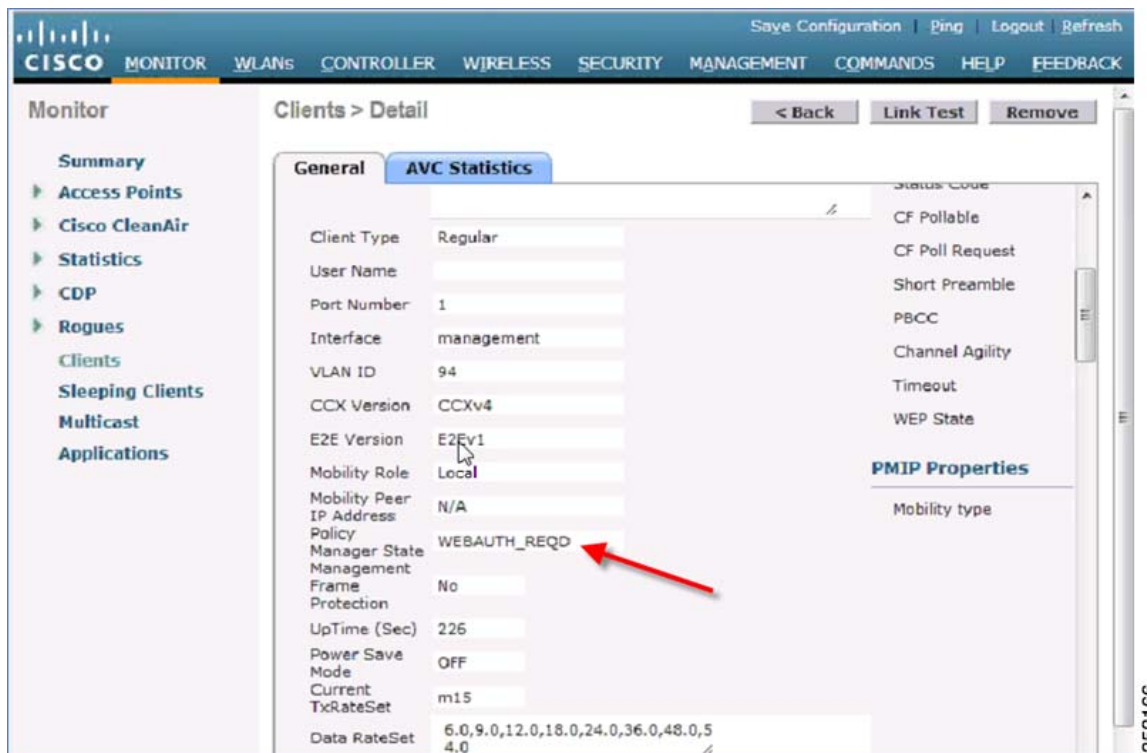
(mavora-wlc-5500-2) >config ap link-encryption enable ?

<Cisco AP>   Enter the name of the Cisco AP.
all          Apply the configuration for all capable Cisco AP
```

Note: Data DTLS for CAPWAP APs joining over IPv6 tunnel is not available in release 8.0 for vWLC platform.

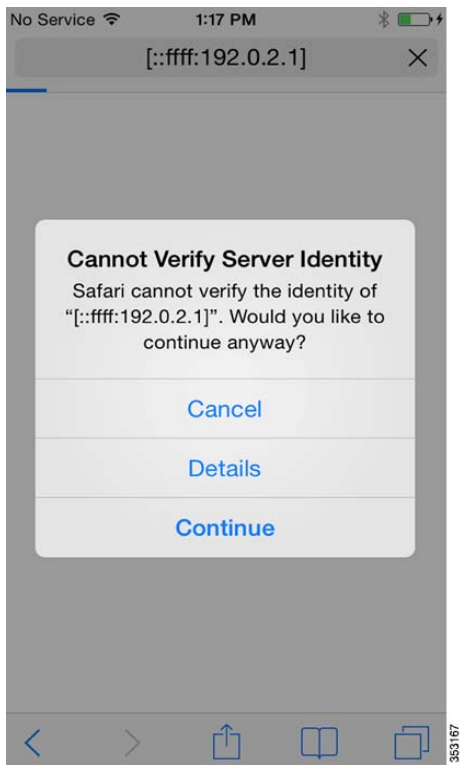
Web-Auth with Pure IPv6 Client

On the controller, the configuration is similar to IPv4. Before client authentication, it is displayed in the **WEBAUTH_REQD** state as shown below.

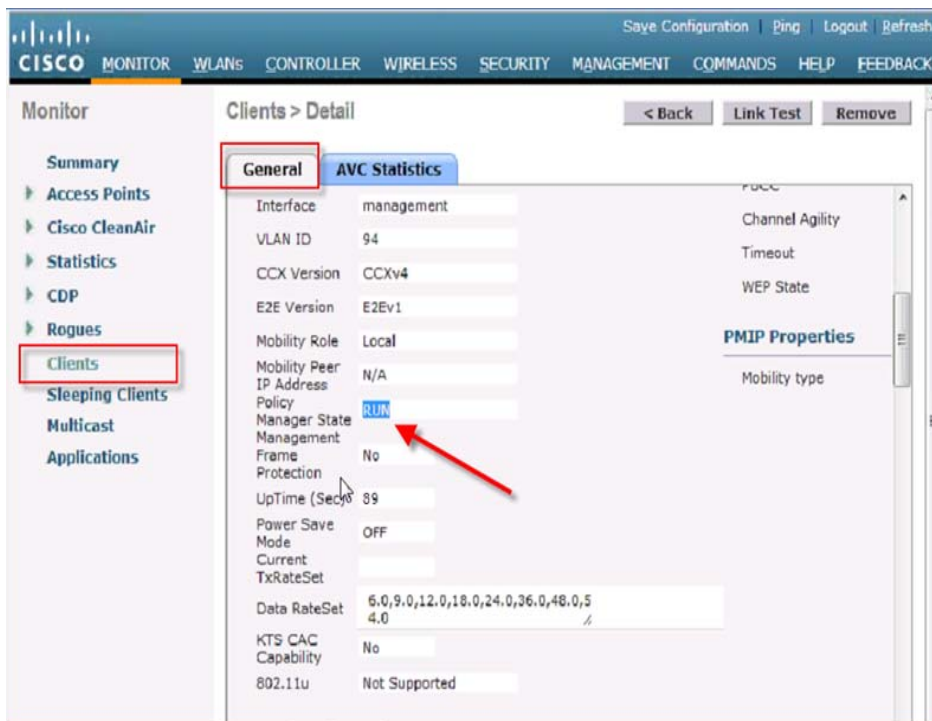


Access an IPv6 enabled website such as **www.ipv6.google.com** or enter an IPv6 address of a website, for example—**[2001::101]**.

Phase 2–Infrastructure IPv6 Support in WLC Release 8.0 and Later

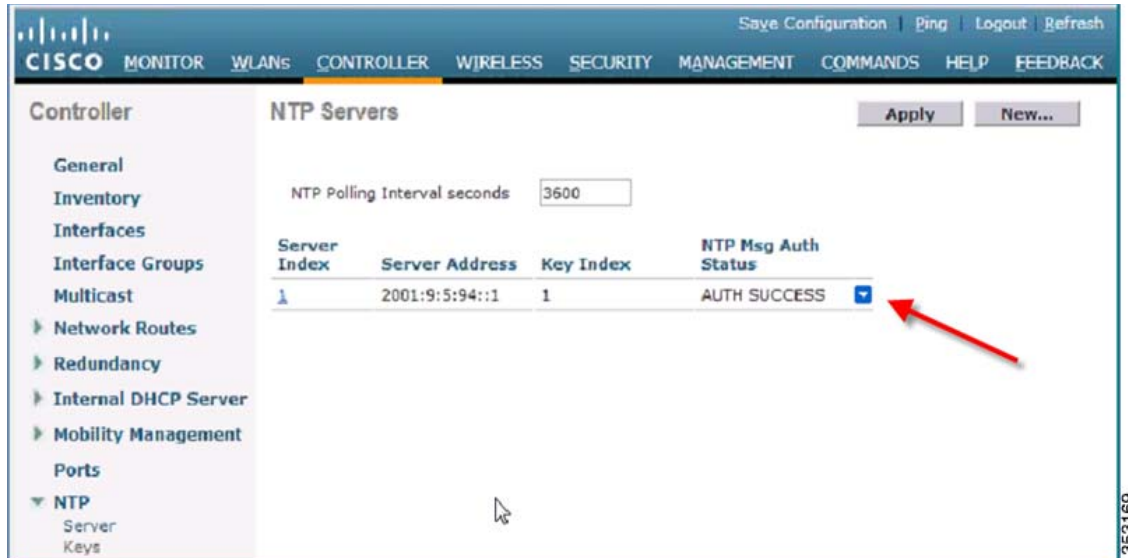


To verify that the WebAuth is in the **RUN** state, check the controller.



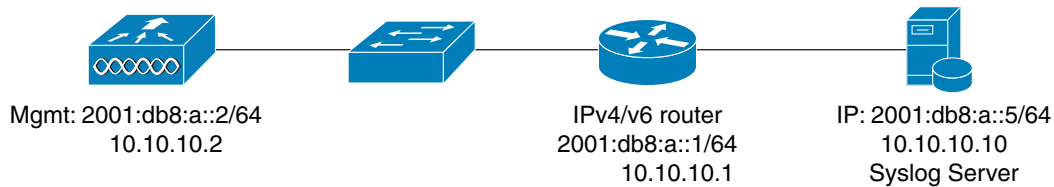
NTP Over IPv6

The NTP server configuration is supported on the controller in the native IPv6 mode, and NTP version 3 is now supported using MD5 encryption.



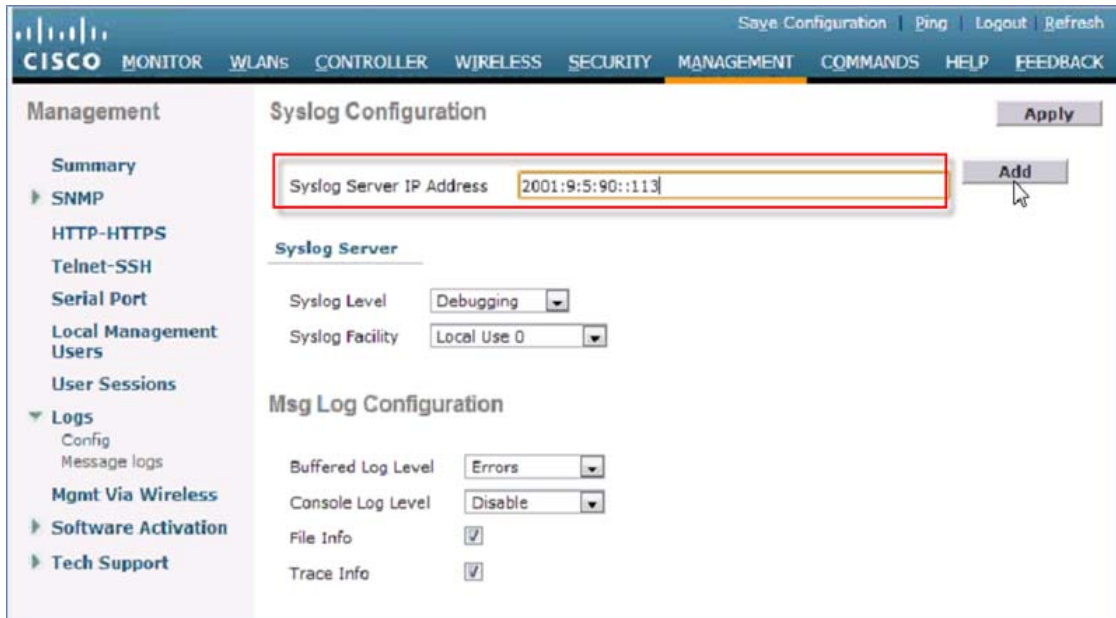
Syslog Over IPv6

In Release 8.0, the native IPv6 syslog server is supported.



The following is an example of the IPv6 Syslog Server configuration.

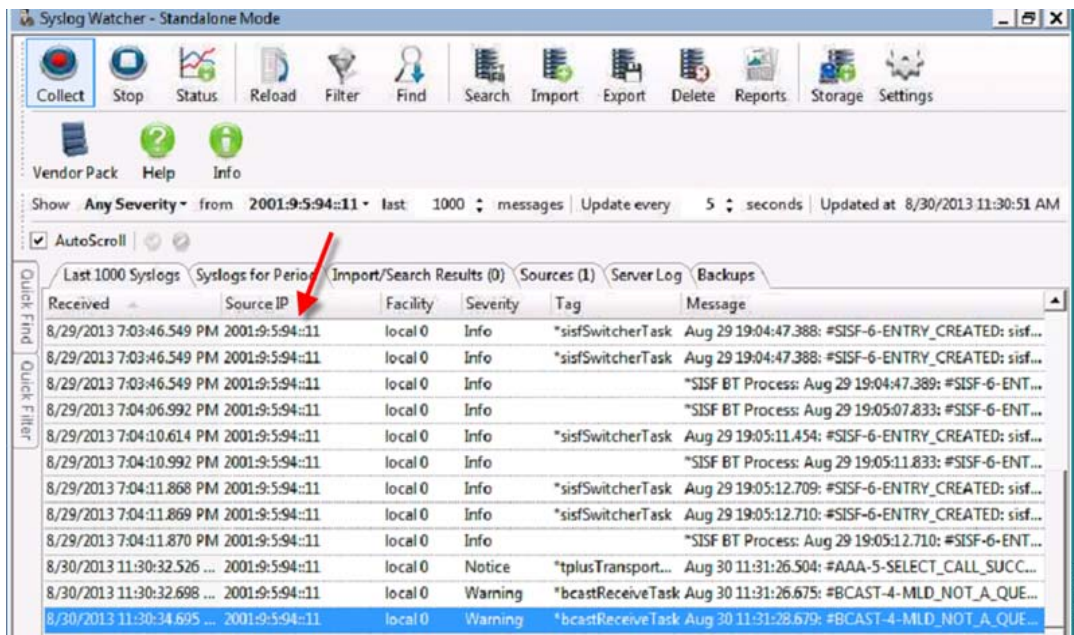
Phase 2-Infrastructure IPv6 Support in WLC Release 8.0 and Later



As an example, on Syslog Watcher you can see logs from the controllers. In this release, both syslog v4 and syslog v6 are generated.

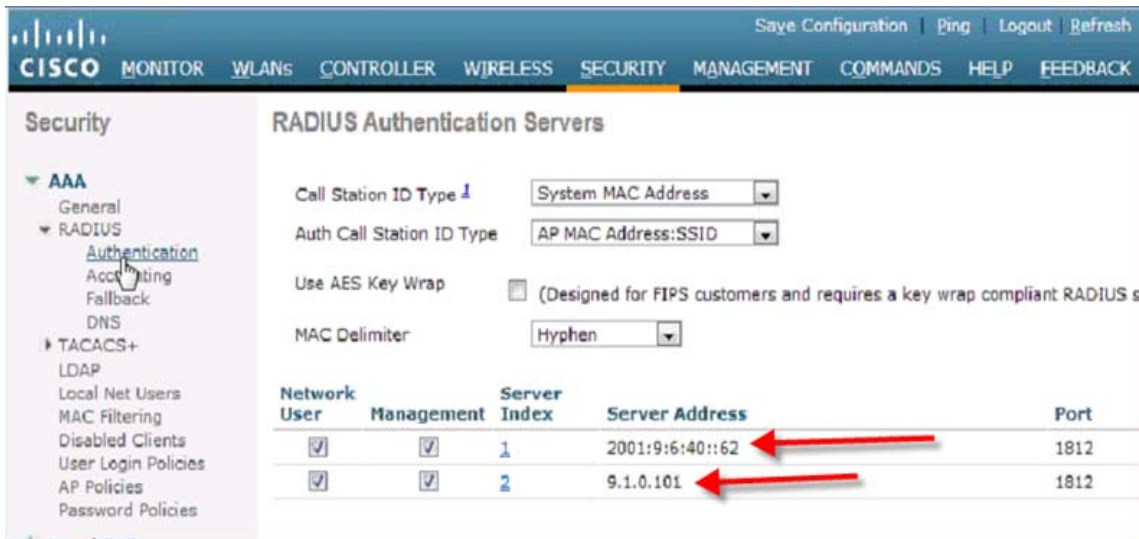


Phase 2-Infrastructure IPv6 Support in WLC Release 8.0 and Later

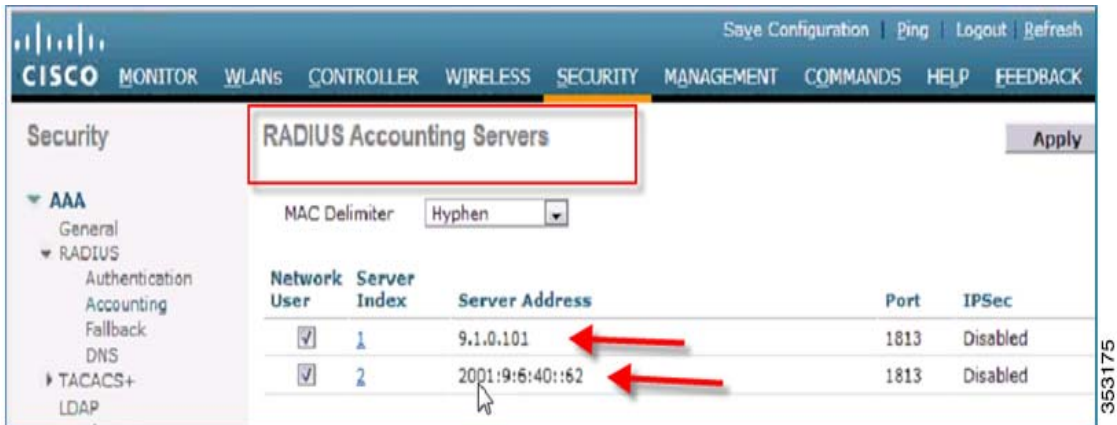


Radius Over IPv6

RADIUS authentication server IPv4 and IPv6 are supported in this release natively.



Accounting servers IPv4 and IPv6 are also supported.



In the figure below, the IPv6 servers are mapped to the WLAN.



CDP IPv6

CDPv6 works natively on the controller Release 8.0.

To see the CDPv6 on the controller, execute the following command:

Show cdp entry all

As shown in the example below, IPv4 and IPv6 neighbors are displayed:

Phase 2–Infrastructure IPv6 Support in WLC Release 8.0 and Later

```

Cisco Controller) >show cdp entry all
-----
Device ID: THE_3750_MA2
Entry address(es):
  IP address: 10.70.0.2
  IPv6 address: 2001:1:10:70::2 (global unicast)
  IPv6 address: fd01:1:10:70::2 (global unicast)
  IPv6 address: fe80::216:c7ff:fe96:2543 (link-local)
Platform: cisco WS-C3750G-24PS, Capabilities: Switch IGMP
Interface: GigabitEthernet0/0/1, Port ID (outgoing port): GigabitEthernet2/0/27
Holdtime : 161 sec

Version :
Cisco IOS Software, C3750 Software (C3750-IPSERVICESK9-M), Version 15.0(2)SE4, RELEASE
echsupport Copyright (c) 1986-2013 by Cisco Systems, Inc. Compiled Wed 26-Jun-13 02:41

Advertisement version: 2
Duplex: Full

```

The same can be executed from any neighbor switch and the controller will be displayed in the CDPv6 list.

The Controller CDP command can also be executed for APs:

show ap cdp neighbors

all–Displays cdp neighbor information for all Cisco APs.

ap-name–Displays cdp neighbor information for a specific Cisco AP.

detail–Displays detailed cdp neighbor information for a Cisco AP.

```

(Cisco Controller) >show ap cdp neighbors ?
all          Show cdp neighbor information for all Cisco APs.
ap-name     Show cdp neighbor information for a specific Cisco AP.
detail      Show detailed cdp neighbor information for Cisco AP

(Cisco Controller) >show ap cdp neighbors all

```

AP Name	AP IP	Neighbor Name	Neighbor Port
AP2600-Saba	10.70.0.110	THE_3750_MA2	GigabitEthernet2/0/3
	IP address: 10.70.0.2		
	IPv6 address: 2001:1:10:70::2 (global unicast)		
	IPv6 address: fd01:1:10:70::2 (global unicast)		
	IPv6 address: fe80::216:c7ff:fe96:2543 (link-local)		
AP3700_THE_lab	10.70.0.254	THE_3750_MA2	GigabitEthernet2/0/7
	IP address: 10.70.0.2		
	IPv6 address: 2001:1:10:70::2 (global unicast)		
	IPv6 address: fd01:1:10:70::2 (global unicast)		
	IPv6 address: fe80::216:c7ff:fe96:2543 (link-local)		

353178

Flex Connect Central/Local Switching with CAPWAP IPv4/IPv6 but IPv4 Clients Only

IPv6 and IPv4 are supported on the Flex Connect APs in the Centrally switched mode only. In the Locally switched mode, IPv4 clients work as before with no issues.

Service Port SLAAC

SLAAC is only applicable for the Service port.

Phase 2—Infrastructure IPv6 Support in WLC Release 8.0 and Later

```
(Cisco Controller) >show ipv6 interface summary

Number of Interfaces..... 2

Interface Name      Port Vlan Id  IPv6 Address/Prefix Length
-----
management          1   untagged    fe80::224:97ff:fe69:93c0/64
                    1   untagged    2001:1:10:70::75/64
service-port        N/A  N/A         fe80::224:97ff:fe69:93c1/64
                    N/A  N/A         ::/128

(Cisco Controller) >
```

353179

To disable the SLAAC interface on the Service port, enter the following command:

```
(Cisco Controller) >config ipv6 interface slaac service-port disable

Requested State Configured Successfully .

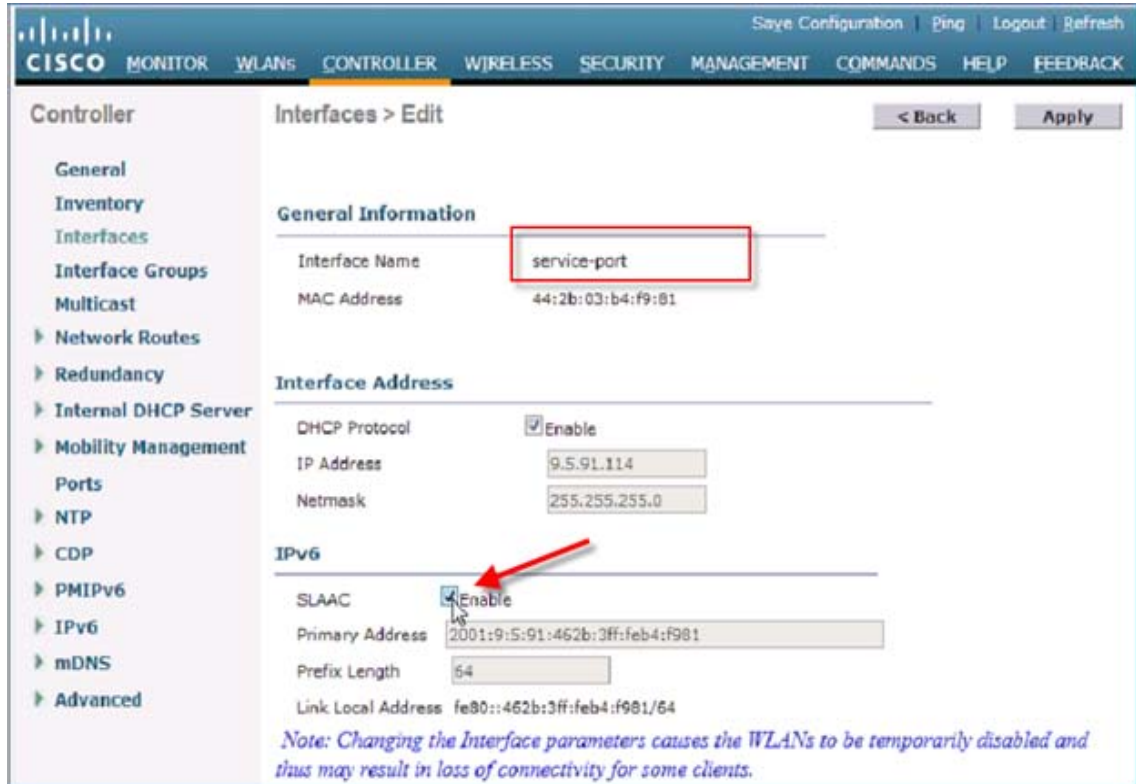
(Cisco Controller) >show ipv6 interface summary

Number of Interfaces..... 2

Interface Name      Port Vlan Id  IPv6 Address/Prefix Length
-----
management          1   untagged    fe80::224:97ff:fe69:93c0/64
                    1   untagged    2001:1:10:70::75/64
service-port        N/A  N/A         fe80::224:97ff:fe69:93c1/64
                    N/A  N/A         ::/128
```

353180

The SLAAC interface can also be enabled in the WebUI interface on the Service port as shown below:



Rogue APs Origin Based Service Discovery

Rogue services are working as before on the controller with IPv6. See example below:

```
(mavara-wlc-5500-2) >show rogue ap summary
```

```
Rogue Detection Security Level..... custom
Rogue Pending Time..... 180 secs
Rogue on wire Auto-Contain..... Disabled
Rogue using our SSID Auto-Contain..... Disabled
Valid client on rogue AP Auto-Contain..... Disabled
Rogue AP timeout..... 1200
Rogue Detection Report Interval..... 10
Rogue Detection Min Rssi..... -128
Rogue Detection Transient Interval..... 0
Rogue Detection Client Num Threshold..... 0
Total Rogues (AP+Ad-hoc) supported..... 2000
Total Rogues classified..... 951
```

MAC Address	Classification	# APs	# Clients	Last Heard
00:08:30:8e:76:7e	Unclassified	2	0	Fri Aug 30 11:44:34 2013
00:16:9c:91:10:3e	Pending	1	0	Fri Aug 30 11:41:53 2013
00:16:9c:91:10:3f	Unclassified	1	0	Fri Aug 30 11:32:53 2013
00:19:07:05:d5:b0	Unclassified	1	0	Fri Aug 30 11:42:52 2013
00:19:07:05:d5:b2	Unclassified	1	0	Fri Aug 30 11:42:22 2013
00:19:07:05:d5:b3	Unclassified	1	0	Fri Aug 30 11:35:52 2013

Features Not Supported in Release 8.0

- Deployment Modes:
 - Flexconnect - Local switched
 - Mesh/Outdoor
 - Teleworker/OEAP
 - Converged Access
- Services:
 - Bonjour
 - AVC
 - Trustsec
 - Mobility Multicast
- Unsupported APs:
 - Bridge mode APs/AP with 64 Mb RAM
 - OEAP 600
 - ISR 800/802
 - 1130/1240/1250
 - 1310/1410
 - 1550 with 64 Mb
 - 1520

Note: See Controller Release Notes for complete details.

- Misc. Configuration Options
 - Internal DHCPv6 Server
 - DHCPv6 Proxy
 - Auto configuration
 - Dynamic interfaces
 - RA Interfaces
 - OSCP and CA Server URL
 - VLAN pooling
- Protocols
 - NTP v4
 - MLD v2
 - IPsec v3 and IKE v2

Appendix A

- RLDP and CIDS
- PMIP v6 on the WLC
- New Mobility

Appendix A

Loading Images to Your IOS Switch

It is recommended that you download the entire **“universal” “tar”** image that has web-based access to the IOS switch as well.

For example, Cisco Catalyst 3750E IOS images can be downloaded from the link below:

<http://software.cisco.com/download/release.html?mdfid=280831063&flowid=2587&softwareid=280805680&release=15.0.2-SE6&reind=AVAILABLE&rellifecycle=ED&reltype=latest>

Cisco Catalyst 3750E-24PD-E Switch

Search...

Expand All | Collapse All

Release 15.0.2-SE6 ED [Release Note](#)

File Information	Release Date	DRAM/Flash
IP BASE c3750e-ipbasek9-mz.150-2.SE6.bin	28-APR-2014	256 / 64
IP BASE WITH WEB BASED DEV MGR c3750e-ipbasek9-tar.150-2.SE6.tar	28-APR-2014	256 / 64
UNIVERSAL c3750e-universalk9-mz.150-2.SE6.bin	28-APR-2014	256 / 64
UNIVERSAL WITH WEB BASE DEV MGR c3750e-universalk9-tar.150-2.SE6.tar	28-APR-2014	256 / 64

353183

It is recommended that IOS 15.2SE4 images or later be used for IPV6 support:

Catalyst 3750e - c3750e-c3750e-universalk9-tar.150-2.SE4

Catalyst 3750x - c3750e-c3750-ipservicesk9-tar.150-2.SE4

To install images on your IOS switch, use the following CLI under the **privilege** mode:

```
archive download-sw /overwrite /reload tftp://<tftp server ip>/<path>/<filename> flash:
```

For example:

```
archive download-sw /overwrite /reload  
tftp://9.1.0.150/wnbu/c3750e-universalk9-tar.150-2.SE.tar flash:
```

The IOS switch replaces the older IOS image and does the necessary delete and so on and reloads.

Appendix A

Switch	Ports	Model	SW Version	SW Image
*	1 28	WS-C3750G-24PS	15.0(2)SE4	C3750-IPSERVICESK9-M
	2 28	WS-C3750G-24PS	15.0(2)SE4	C3750-IPSERVICESK9-M

353184

Post IOS Switch Reboot

To enable the IPv4/IPv6 stack (dual) on your IOS switch, do the following:

enable

configure terminal

license boot level ipservices

sdm prefer dual-ipv4-and-ipv6 default

write memory

reload

yes

Before the sdm command:

```
TME_3750_MA2#sh sdm prefer
The current template is "desktop default" template.
The selected template optimizes the resources in
the switch to support this level of features for
8 routed interfaces and 1024 VLANs.

number of unicast mac addresses:          6K
number of IPv4 IGMP groups + multicast routes: 1K
number of IPv4 unicast routes:          8K
  number of directly-connected IPv4 hosts: 6K
  number of indirect IPv4 routes:       2K
number of IPv6 multicast groups:         0
number of directly-connected IPv6 addresses: 0
number of indirect IPv6 unicast routes:  0
number of IPv4 policy based routing aces: 0
number of IPv4/MAC qos aces:            0.5K
number of IPv4/MAC security aces:       1K
number of IPv6 policy based routing aces: 0
number of IPv6 qos aces:                20
number of IPv6 security aces:           25

On next reload, template will be "desktop IPv4 and IPv6 vlan" template.
```

353185

After: `sdm prefer dual-ipv4-and-ipv6 default`

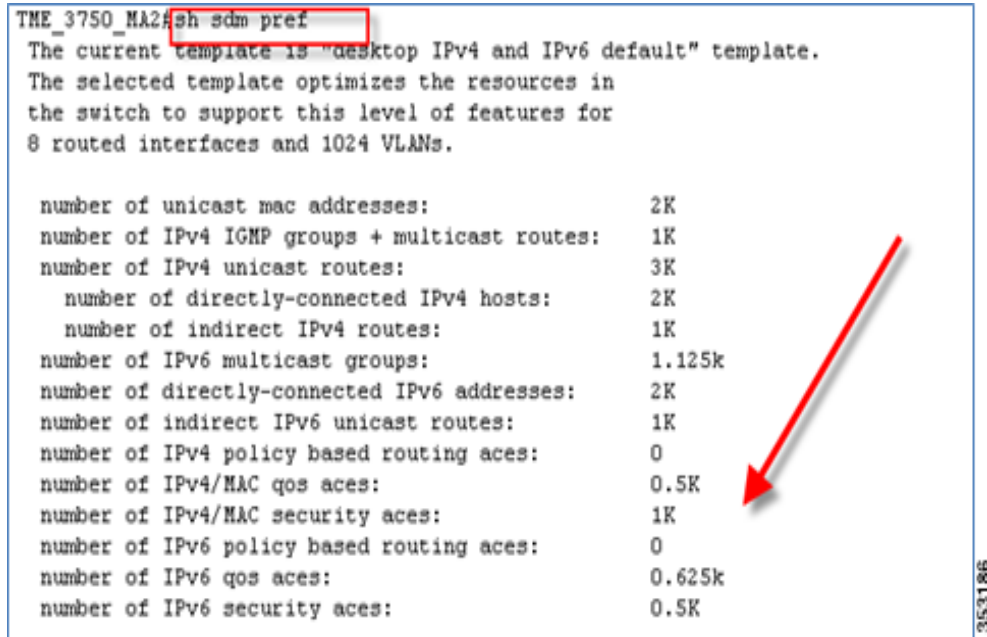
Appendix A

```

TME_3750_MA2#sh sdm pref
The current template is "desktop IPv4 and IPv6 default" template.
The selected template optimizes the resources in
the switch to support this level of features for
8 routed interfaces and 1024 VLANs.

number of unicast mac addresses:          2K
number of IPv4 IGMP groups + multicast routes: 1K
number of IPv4 unicast routes:          3K
  number of directly-connected IPv4 hosts: 2K
  number of indirect IPv4 routes:        1K
number of IPv6 multicast groups:         1.125k
number of directly-connected IPv6 addresses: 2K
number of indirect IPv6 unicast routes:   1K
number of IPv4 policy based routing aces: 0
number of IPv4/MAC qos aces:             0.5K
number of IPv4/MAC security aces:        1K
number of IPv6 policy based routing aces: 0
number of IPv6 qos aces:                 0.625k
number of IPv6 security aces:            0.5K

```



Enable IPv6 on the Required Interfaces

Example: Add an IPv6 address to the uplink port **interface gi 1/0/24** with the command `ipv6 address fd09:9:x::x/64`.

Add the IPv6 address to VLAN interfaces with `ipv6 address fd09:9:x::x/64`.

Add the IPv6 address to the VLAN interfaces with `ipv6 address 2001:9:x::x/64`.

Address fd09:: is an IPv6 Unique Local Address, that is used for private networks.

Address 2001:: is an IPv6 Global Address.

Enable IPv6 Routing on the Required Interfaces

The following commands are examples for RIP routing configuration:

IPv6 unicast-routing

IPv6 router RIP user_id (For example: Cisco-user, follow this strictly so there is no duplication.)

Example: Go to **interface gi 1/0/24** and run the `ipv6 rip cisco_user enable` command (this interface is the uplink of your own IOS switch Core, if it is different from **gi1/0/24**, replace with the appropriate uplink port).

Run the `ipv6 rip cisco_user enable` command in all the VLAN interfaces for routing.

Sample output of a IPv6 configured IOS switch:

Uplink Port Config

```

interface GigabitEthernet3/0/24
description ****Uplink to distribution switch *****
no switchport
ip address 9.12.0.26 255.255.255.0

```


Appendix A

```
ipv6 address FD09:9:12::26/64
```

```
ipv6 address 2001:9:12::26/64
```

```
ipv6 rip cisco-user enable
```

Global Config

```
ipv6 unicast-routing
```

```
ipv6 mld snooping
```

```
ipv6 router rip miadler
```

L3 Vlan Interface Config

```
interface Vlan128
```

```
ip address 9.12.128.1 255.255.255.0
```

```
ip helper address 9.1.0.100
```

```
ip pim sparse-dense-mode
```

```
ip igmp version 3
```

```
ipv6 address FD01:1:10:70::2/64
```

```
ipv6 address 2001:1:10:70::2/64
```

```
ipv6 enable
```

```
ipv6 nd autoconfig default-route
```

```
ipv6 nd managed-config-flag (for stateful DHCPv6 use)
```

```
ipv6 nd router-preference High
```

```
ipv6 dhcp relay destination 2001:9:6:40::XX
```

Configuring DHCPv6 Server Functions

The DHCPv6 server function can be enabled on individual IPv6-enabled interfaces.

The DHCPv6 server can provide those configuration parameters that do not require the server to maintain any dynamic state for individual clients, such as DNS server addresses and domain search list options. The DHCPv6 server may be configured to perform prefix delegation.

All the configuration parameters for clients are independently configured into the DHCPv6 configuration pools, which are stored in NVRAM. A configuration pool can be associated with a particular DHCPv6 server on an interface when it is started. Prefixes to be delegated to clients may be specified either as a list of preassigned prefixes for a particular client or as IPv6 local prefix pools that are also stored in NVRAM. The list of manually configured prefixes or IPv6 local prefix pools can be referenced and used by DHCPv6 configuration pools.

The DHCPv6 server maintains an automatic binding table in its memory to track the assignment of some configuration parameters, such as prefixes between the server and its clients. The automatic bindings can be stored permanently in the database agent, which can be for example, a remote TFTP server or local NVRAM file system.

Appendix A

Configuration Information Pool

A DHCPv6 configuration information pool is a named entity that includes information about available configuration parameters and policies that control assignment of the parameters to clients from the pool. A pool is configured independently of the DHCPv6 service and is associated with the DHCPv6 service through the command-line interface (CLI).

Each configuration pool can contain the following configuration parameters and operational information:

- Prefix delegation information, which could include:
 - A prefix pool name and associated preferred and valid lifetimes.
 - A list of available prefixes for a particular client and associated preferred and valid lifetimes.
- A list of IPv6 addresses of DNS servers.
- A domain search list, which is a string containing domain names for DNS resolution.

Configuring DHCPv6 Configuration Pool

This task explains how to create and configure the stateful DHCPv6 configuration pool and associate the pool with a server on an interface.

Summary Steps

1. enable
2. configure *terminal*
3. ipv6 dhcp pool vlan-90-clients
4. address prefix FD09:9:5:90::/64
5. address prefix 2001:9:5:90::/64
6. dns-server 2001:9:5:90::115
7. domain-name test.com
8. information refresh 1
9. exit
10. interface *type number*
11. ipv6 dhcp server *poolname* [rapid-commit] [preference *value*] [allow-hint]

Configuring DHCPv6 Relay on L3 VLAN Interfaces

A DHCP relay agent that resides on the client's link, is used to relay messages between the client and server. The DHCP relay agent operation is transparent to the client. A client locates a DHCP server using a reserved, link-scoped multicast address. Therefore, it is a requirement that for direct communication between the client and the server, the client and the server must be attached to the same link. However, in some situations where management, economy, or scalability is a concern, it is desirable to allow a DHCP client to send a message to a DHCP server that is not connected to the same link.

This task describes how to enable the DHCPv6 relay agent function and specify relay destination addresses on an interface.

Appendix A

Summary Steps:

1. enable
2. configure terminal
3. interface *type number*
4. ipv6 dhcp relay destination *ipv6-address [interface-type interface-number]*

For example, if you want to add DHCPv6 relay to Vlan128 in your IOS switch, do the following:

```
configure t
interface vlan128
ipv6 dhcp relay destination 2001:9:6:40::XX
```

Implementing DHCPv6 Option 52 on Microsoft and Linux Based DHCP Servers

DHCPv6 Option 52 Overview

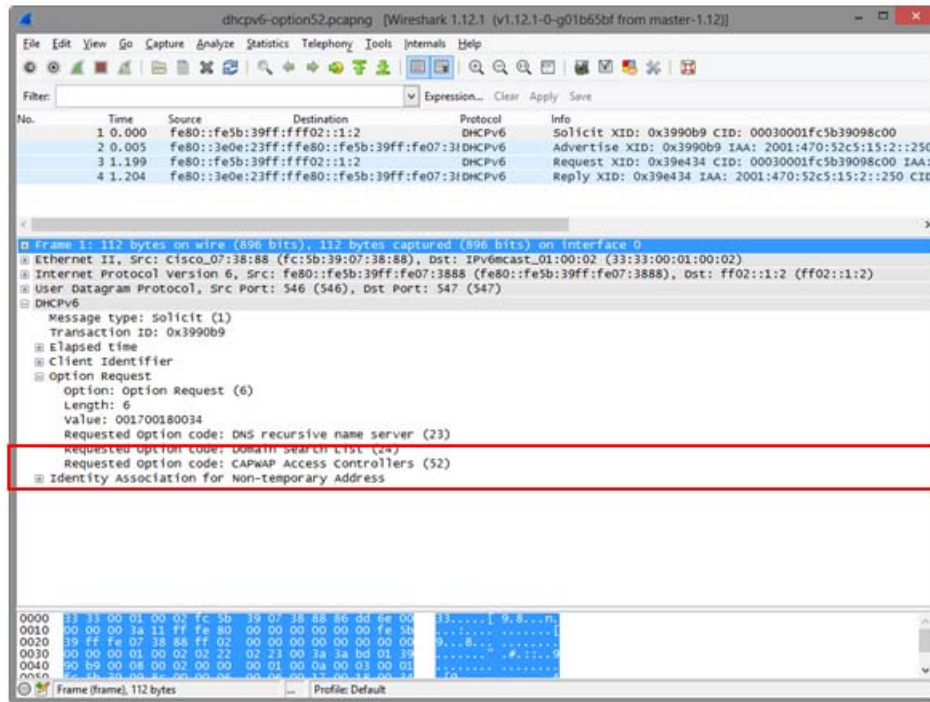
The CAPWAP protocol allows a lightweight access point (AP) to use DHCP to discover a wireless controller to which it is connected to. Cisco lightweight APs running 8.0 and above support DHCP discovery for both IPv4 and IPv6 networks:

- IPv4—Cisco lightweight APs implement DHCP option 43 to supply the IPv4 management interface addresses of the primary, secondary, and tertiary wireless controllers (see the [guide](#)).
- IPv6—Cisco lightweight APs implement DHCPv6 option 52 (RFC 5417) to supply the IPv6 management interface addresses of the primary, secondary, and tertiary wireless controllers.

In 8.0 and above, Cisco lightweight APs support both stateless and stateful DHCPv6 addressing modes. In stateless mode, the APs obtain an IPv6 addressing using SLAAC while additional network information (not obtained from router advertisements) is obtained from a DHCPv6 server. In stateful mode, the APs obtain both IPv6 addressing and additional network information exclusively from DHCPv6 (similar to DHCPv4). In both modes, a DHCPv6 server is required to provide option 52 if wireless controller discovery using DHCPv6 is required. If a DHCPv6 server is not available, an alternative discovery method such as DNS or AP Priming is required.

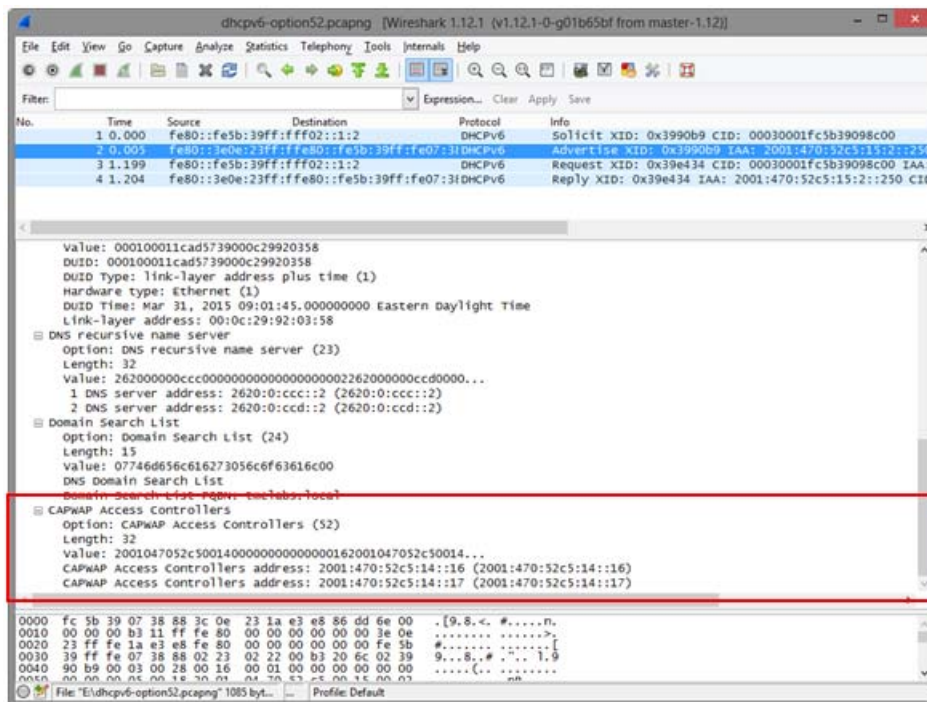
Cisco lightweight APs request DHCPv6 options using DHCPv6 Solicit and Request packets which are forwarded to all DHCP servers multicast address (FF02::1:2). Request packets are forwarded in stateless mode while both Solicit and Request packets are forwarded in stateful mode. The Solicit and Request packets include an Option Request field that the APs use to request additional network information from the DHCPv6 server. The requested options include option 23 (Name Server), option 24 (Domain Search List) and option 52 (CAPWAP access controllers).

Figure 1 Option Request Field in a Solicit and Request Packets



If the requested option 52 is defined within the IPv6 scope servicing the APs, the DHCPv6 server includes option 52 values in the DHCPv6 Advertise and Reply responses forwarded to the APs. The option 52 values forwarded to the APs may include up to three wireless controller management IPv6 addresses in order of preference.

Figure 2 DHCPv6 option 52 field in Advertise and Reply Packets



Option Formatting

Each DHCP server is unique and includes different pre-defined options from the server vendor. Unfortunately, option 52 is not pre-defined on Microsoft Windows Server 2008, Windows Server 2012, or Linux ISC which requires option 52 to be globally defined before the option and values can be assigned to a IPv6 scope.

When defining option 52 on DHCPv6 server, it is important to note that the option must be defined using a specific format. If not, the supplied wireless controller management interface IPv6 addresses will be rejected by the APs. To be supported by Cisco lightweight APs, option 52 must be defined as an array of IPv6 addresses and cannot be defined as a string or other type. If the option is not formatted correctly, the APs will reject the Advertise and Reply packets and fail to obtain an IPv6 address.

DHCPv6 Server Configuration Examples

Internet Systems Consortium (ISC) DHCP Server

This section describes the configurations necessary on a Linux ISC DHCP server (4.1 and above) to define DHCPv6 option 52 and then assign the option and values to an IPv6 scope.

Configuration File

1. Modify the `dhcpd6.conf` file (typically, `/etc/dhcp/dhcpd6.conf`). Define a new unique option name (example, `dhcp6.capwap-ac-v6`) as shown in the following example. The option **code** value must be set to 52 and type set to **array of ip6-address**:

Appendix A

```
option dhcp6.domain-search "tmelabs.local";
option dhcp6.name-servers 2620:0:ccc::2,2620:0:ccd::2;
option dhcp6.capwap-ac-v6 code 52 = array of ip6-address;
default-lease-time 86400;
max-lease-time 172800;
```

2. Locate the IPv6 scope servicing your Lightweight APs. Under the IPv6 range, add the newly defined option name (example, dhcp6.capwap-ac-v6) followed by the management interface IPv6 addresses of the primary WLC. Optionally, define secondary and tertiary management interface IPv6 addresses if required. Note that a comma must separate each IPv6 address.

```
# LAB1-APS
subnet6 2001:470:52c5:15::/64 {
    range6 2001:470:52c5:15:1::1 2001:470:52c5:15:2::254;
    option dhcp6.capwap-ac-v6 2001:470:52c5:14::16,2001:470:52c5:14::17;
}
```

3. Restart the ISC DHCPv6 Service:

```
root@linux-server1:/home/kevinmar# service isc-dhcp-server6 restart
isc-dhcp-server6 stop/waiting
isc-dhcp-server6 start/running, process 4822
```

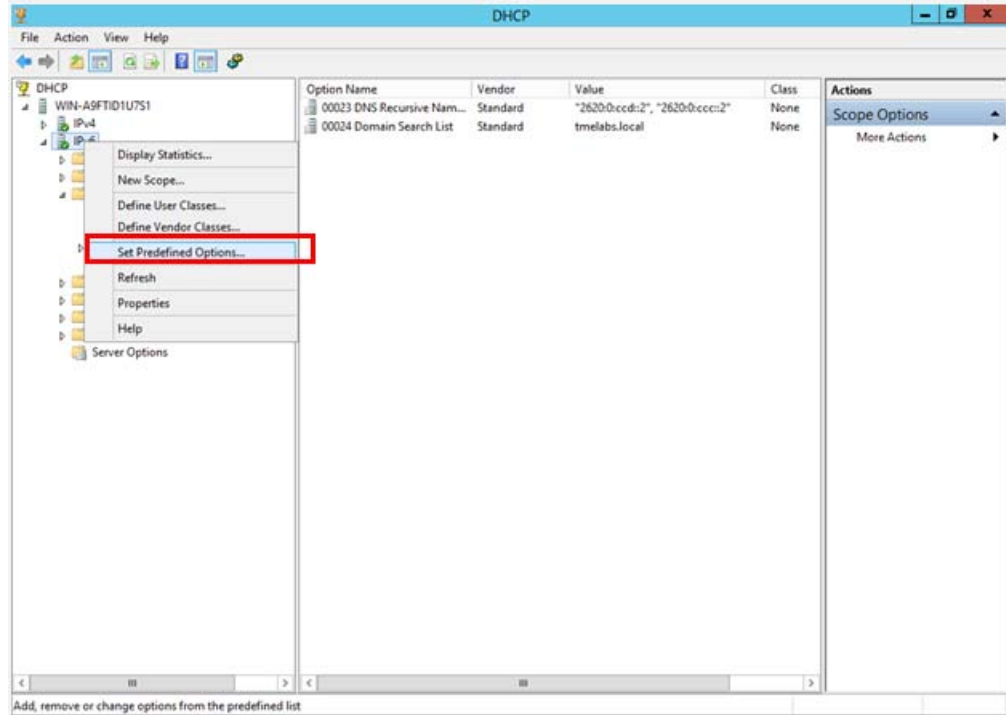
Microsoft Windows Server 2008 / 2012

This section describes the configurations necessary on a Microsoft Windows Server 2008 / 2012 to define DHCPv6 option 52 and then assign the option and values to a IPv6 scope.

Defining DHCPv6 Option 52 Globally

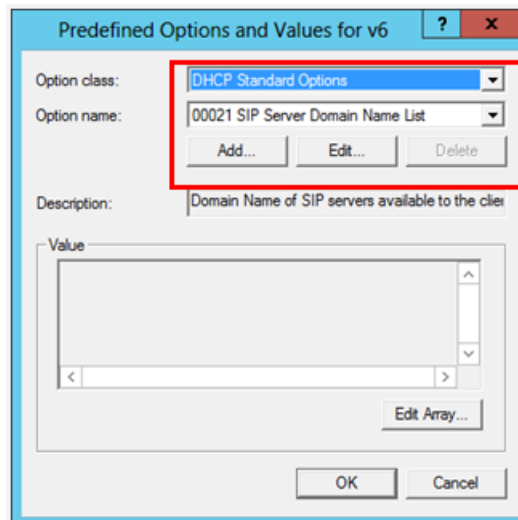
1. Open the **DHCP** Manager and expand the DHCP tree. Right-click **IPv6** and then select **Set Predefined Options**.

Appendix A



The **Predefined Options and Values for v6** window appears.

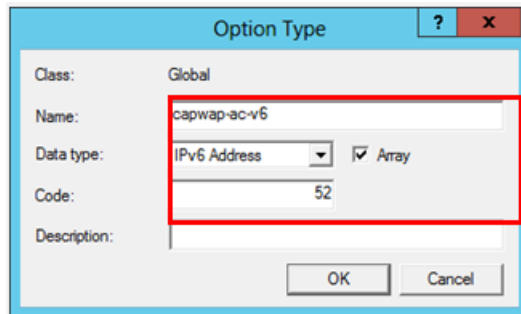
2. In the **Option class** drop-down list, select **DHCP Standard Options**, and then click **Add**.



The **Option Type** window appears.

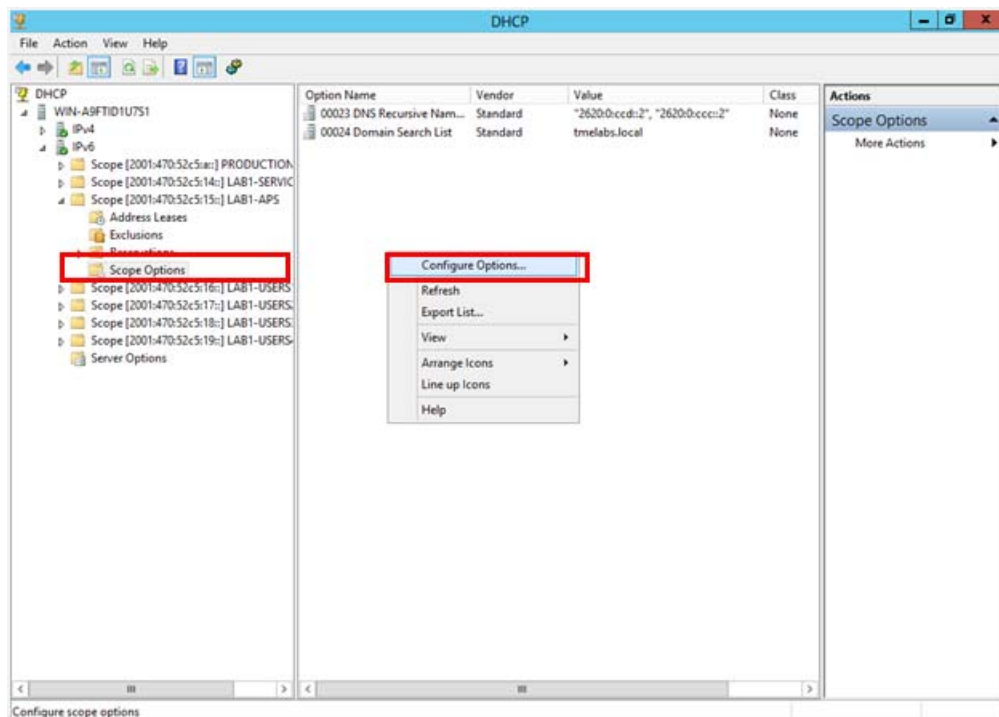
3. Enter a **Name** for the new option (for example, capwap-ac-v6), and then set the **Data type** to **IPv6 Address**. Check the **Array** check box, and then enter the **Code** value of **52**. Click **OK** and then **OK** again. The new option is now defined and can be assigned to IPv6 scopes.

Appendix A



Assigning the DHCPv6 Option 52 and Values to an IPv6 Scope

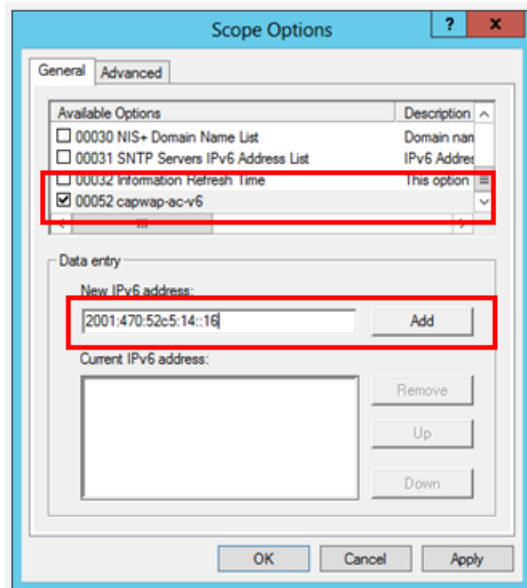
1. Expand the first IPv6 scope servicing your Lightweight APs. Right-click **Scope Options** and then select **Configure Options**.



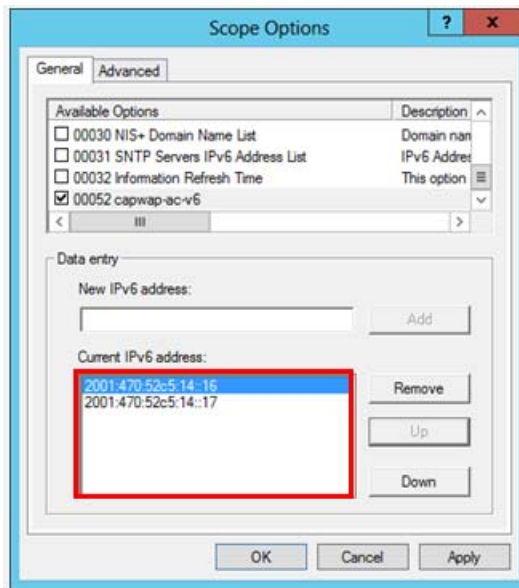
The **Scope Options** window appears.

2. In the **Available Options** list, select the option **00052 capwap-ac-v6**. In the **New IPv6 address** field, enter the management interface IPv6 address of the primary WLC and then click **Add**.

Appendix A



3. (Optional) Define secondary and tertiary IPv6 addresses if required. Click **Apply** and then **OK**.



The WLC management IPv6 addresses are assigned to the IPv6 scope servicing the Lightweight APs.

Appendix A

Option Name	Vendor	Value
00052 capwap-ac-v6	Standard	"2001:470:52c5:14::17", "2001:470:52c5:14::16"
00023 DNS Recursive Nam...	Standard	2620:0:ccd::2, 2620:0:ccc::2
00024 Domain Search List	Standard	tmelabs.local

Verifying Cisco Lightweight Access Points

You can verify that a Cisco Lightweight Access Point (AP) has received an IPv6 address and options by logging into an AP and issuing the **show ipv6 dhcp interface** command. The output displays any assigned IPv6 addresses along with options and values:

```
APfc5b.3907.3888# show ipv6 dhcp interface
```

```
BVI1 is in client mode
Prefix State is IDLE
Address State is OPEN
Renew for address will be sent in 3d22h
List of known servers:
  Reachable via address: FE80::3E0E:23FF:FE1A:E3E8
  DUID: 00010000551AF3C0000C29599CBC
  Preference: 0
Configuration parameters:
  IA NA: IA ID 0x00160001, T1 345600, T2 552960
  Address: 2001:470:52C5:15:808E:AE4:FE92:C4FE/128
  preferred lifetime 691200, valid lifetime 1036800
  expires at Apr 11 2015 07:26 PM (943382 seconds)
DNS server: 2620:0:CCD::2
DNS server: 2620:0:CCC::2
Domain name: tmelabs.local
CAPWAP Access Controller: 2001:470:52C5:14::16
CAPWAP Access Controller: 2001:470:52C5:14::17
Information refresh time: 0
Prefix Rapid-Commit: disabled
Address Rapid-Commit: disabled
```

Link Local IPv6 address of the 1st Hop Router performing DHCPv6 relay

APs IPv6 allocated by the DHCPv6 server

Received option 23 (name server) & 24 (domain-name)

Received option 52 (CAPWAP) values

IOS DHCPv6 Relay

In most enterprise deployments, the first hop router is configured to relay DHCPv6 messages to a centralized DHCP server. You can verify that the DHCPv6 packets are being exchanged between an AP and DHCPv6 server on an IOS device by issuing the **debug ipv6 dhcp relay** command.

Appendix A

```
DIST-1-1# debug ipv6 dhcp relay
```

```
IPv6 DHCP relay debugging is on
```

```
Mar 31 21:30:42.251: IPv6 DHCP_RELAY: Relaying SOLICIT from FE80::F27F:6FF:FEE8:1214 on Vlan21
Mar 31 21:30:42.252: IPv6 DHCP_RELAY: Packet forwarded to 2001:470:52C5:A::7
Mar 31 21:30:42.261: IPv6 DHCP_RELAY: Relaying RELAY-REPLY from 2001:470:52C5:A::7 on Vlan10
Mar 31 21:30:42.261: IPv6 DHCP_RELAY: Packet forwarded to FE80::F27F:6FF:FEE8:1214 via Vlan21
Mar 31 21:30:43.457: IPv6 DHCP_RELAY: Relaying REQUEST from FE80::F27F:6FF:FEE8:1214 on Vlan21
Mar 31 21:30:43.457: IPv6 DHCP_RELAY: Packet forwarded to 2001:470:52C5:A::7
Mar 31 21:30:43.460: IPv6 DHCP_RELAY: Relaying RELAY-REPLY from 2001:470:52C5:A::7 on Vlan10
Mar 31 21:30:43.460: IPv6 DHCP_RELAY: Packet forwarded to FE80::F27F:6FF:FEE8:1214 via Vlan21
```

In the above example, the DHCPv6 Solicit and Request packets from the AP are relayed to the DHCPv6 server with the IPv6 address 2001:470:52C5:A::7. The Advertise and Reply packets from the DHCPv6 server are relayed back to the APs link local address FE80::F27F:6FF:FEE8:1214.

Appendix A

Linux ISC (dhcpd.conf)

```
option dhcp6.domain-search "tme1abs.local";
option dhcp6.name-servers 2620:0:ccc::2,2620:0:ccd::2;
option dhcp6.capwap-ac-v6 code 52 = array of ip6-address;
default-lease-time 86400;
max-lease-time 172800;
# PRODUCTION-SERVICES
subnet6 2001:470:52c5:a::/64 {
    range6 2001:470:52c5:a:1::1 2001:470:52c5:a:2::254;
}

# LAB1-SERVICES
subnet6 2001:470:52c5:14::/64 {
    range6 2001:470:52c5:14:1::1 2001:470:52c5:14:2::254;
}

# LAB1-APS
subnet6 2001:470:52c5:15::/64 {
    range6 2001:470:52c5:15:1::1 2001:470:52c5:15:2::254;
    option dhcp6.capwap-ac-v6 2001:470:52c5:14::16,2001:470:52c5:14::17;
}

# LAB1-USERS1
subnet6 2001:470:52c5:16::/64 {
    range6 2001:470:52c5:16:1::1 2001:470:52c5:16:2::254;
}

# LAB1-USERS2
subnet6 2001:470:52c5:17::/64 {
    range6 2001:470:52c5:17:1::1 2001:470:52c5:17:2::254;
}

# LAB1-USERS3
subnet6 2001:470:52c5:18::/64 {
    range6 2001:470:52c5:18:1::1 2001:470:52c5:18:2::254;
}

# LAB1-USERS4
subnet6 2001:470:52c5:19::/64 {
    range6 2001:470:52c5:19:1::1 2001:470:52c5:19:2::254;
}
```