

Cisco Wireless LAN Controller IPv6 Deployment Guide, CUWN Release 8.0

Last Updated:

Phase1-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

Cisco Wireless LAN Controller IPv6 Deployment Guide, CUWN Release 8.0

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

DHCPv6 Address Assignment



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

Cisco Wireless LAN Controller IPv6 Deployment Guide, CUWN Release 8.0

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

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.

Cisco Wireless LAN Controller IPv6 Deployment Guide, CUWN Release 8.0

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

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.

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

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



Neighbor Advertisement(NA)

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.

353118

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].

cisco	MONITOR	WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	нејр	EEEDBA
Controller General Inventory	Interface General I	s > Edit	on						
Interfaces Interface Groups Multicast > Network Routes > Redundancy > Internal DHCP Server	Interface MAC Add Interface IP Addres DNS Host	Name Iress Address ss t Name	virtual 00:24:9 192.0.2.1	7:69:9b:e0	$\widehat{\mathbf{A}}$				
Ports	Note: Chang of connectiv	ing the Int ity for som	erface parameters e clients.	causes the Wi	LANs to be terr	porarily disabled (and thus may rea	ult in los	36.21

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:

Cisco Wireless LAN Controller IPv6 Deployment Guide, CUWN Release 8.0

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



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.

Cisco Wireless LAN Controller IPv6 Deployment Guide, CUWN Release 8.0

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

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

Cisco Wireless LAN Controller IPv6 Deployment Guide, CUWN Release 8.0

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.

uluilu cisco	MONITOR WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	Sa <u>v</u> e Configural <u>F</u> EEDBACK	
Controller	General								
General	Name		5508-MA6						
Inventory	802.3x Flow Control Mode LAG Mode on next reboot		Disabled 💌						
Interfaces			Disabled 💌		(LAG	(LAG Mode is currently disabled).			
Multicast	Broadcast Forwardin	ng.	Disabled 💌						
Network Routes	AP Multicast Mode 4		Multicast 💙	239,100,100,9	4 Multicast Gro	up Address		and an and the	
Redundancy	AP IPv6 Multicast Mo	ode ք	Multicast 💌	ff1e::239:100	fle::239:100:100:94		IPv6 Multicast Group Address		
Internal DHCP Server	AP Fallback		Enabled 💌						
Mobility Management	Fast SSID change		Disabled 💌						
Ports	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.

،، ،،، ،، cısco	MONITOR WLANS CO	NTROLLER WIRELESS	SECURITY MAN	IAGEMENT	C <u>O</u> MMANDS	HELP	
Controller	General	50 C					
General	Name	5508-MA6					
Inventory	802.3x Flow Control Mode	Disabled 💌					
Interface Groups	LAG Mode on next reboot	Disabled 💌		(LAG M	lode is currently	disabled)	
Multicast	Broadcast Forwarding	Disabled 💌					
Network Routes	AP Multicast Mode ⁴	Unicast 💌					
▶ Redundancy	AP IPv6 Multicast Mode Z	Unicast 💌					
Internal DHCP Server	AP Fallback	Enabled 💌					
▶ Mobility Management	Fast SSID change	Disabled 💌				3124	
Ports	Link Local Bridging	Disabled 😒					

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

uluilu cisco	MONITOR	<u>W</u> LANs	CONTROLLER	WIRELESS	<u>s</u> ecurity	MANAGEMENT
Monitor Summary > Access Points	Clients >	Detail operties				
 Cisco CleanAir Statistics 	MAC Add IPv4 Add	ress	f8:1e:df:e3			
CDPRogues	IPv6 Add	ress	2001:db8: 2001:db8: fe80::fa1e	5:bbf8:f935, fee3:a76,		
Clients Multicast						

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

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:

 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.

uluilu cisco	MONITOR WLANS C	ONTROLLER V	VIRELESS	<u>S</u> ECURITY	MANAGEMENT
Controller	Multicast				
General Inventory	Enable Global Multicast	Mode	V		
Interfaces Interface Groups	Enable IGMP Snooping) seconds)	60		
Multicast	IGMP Query Interval (1	5-2400 seconds)	20	_	
Network Routes	Enable MLD Snooping		V		
Redundancy	MLD Timeout (30-7200	seconds)	60		
 Internal DHCP Server Mobility Management Ports 	MLD Query Interval (15	20			

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.

Cisco Wireless LAN Controller IPv6 Deployment Guide, CUWN Release 8.0

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

ululu cisco	MONITOR WLAP	Ns <u>C</u> ONTROLLER	WIRELESS	SECURITY	MANAGEMENT
Monitor Summary	Multicast Grou	ips Aulticast Group	ID) Mapping		
Cisco CleanAir	Group address	Vlan	MGID	IGMP/ML	0
> Statistics	224.0.0.251	20	1106	IGMP	
- statistics	224.0.0.252	20	1101	IGMP	
> CDP	239.255.255.250	20	1103	IGMP	
Rogues	ff02::c	20	1102	MLD	
Clients	ff02::fb	20	1105	MLD	
Multicast	ff02::1:3	20	1100	MLD	
	ff02::2:fbb5:a199	20	1110	MLD	

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.

cisco		<u>W</u> LANs		WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP
Controller General	IPv6 > RA	A Guard						
Inventory	IPv6 RA C	Guard on W	LC Enabled	_				
Interface Groups	IPv6 RA C	Guard on AS	Enable 👻					
Multicast Network Routes	RA Dropp	ed per clier	nt:					
 Internal DHCP Server Mobility Management 	MAC Addre	ess /	AP Name WL	AN		Number of RA	Dropped	
Ports								
▶ NTP								
+ CDP								
 IPv6 Neighbor Binding Timers RA Throttle Policy RA Guard 								

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

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.

	<u>w</u> lans <u>c</u> ontroller	WIRELESS	SECURITY	Sa <u>v</u> e Co M <u>A</u> NAGEMENT	nfiguration Ping Lo COMMANDS HELP	gout <u>R</u> efresh <u>F</u> EEDBACK
Security	Access Control Li	sts > New			< Back	Apply
General RADIUS Authentication Accounting Fallback	Access Control List Name ACL Type	Block	K-HTTPv6-Serv IPv4 IPv6 IPv6	er		

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

Cisco Wireless LAN Controller IPv6 Deployment Guide, CUWN Release 8.0

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



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.

·I∣IIIIII CISCO MONITOR W	LANS <u>C</u> ONTROLLER	. W <u>I</u> RELESS	<u>S</u> ECURITY	Sa <u>v</u> e Ci M <u>A</u> NAGEMENT	onfiguration <u>P</u> i C <u>O</u> MMANDS	ing Logout <u>R</u> efresh HE <u>L</u> P <u>F</u> EEDBACK
Security	Access Control	Lists > Rule	s > New		< Bac	k Apply
▼ AAA	Sequence	1				
General ♥ RADIUS Authentication	Source I	P Address 🔻	1P 2	v6 Address 001:db8:0:20::		Prefix Length 64
Accounting Fallback TACACS+	Destination	IP Address 🔻	IP 2	v6 Address 001:db8:0:113::20	D	Prefix Length
LDAP Local Net Users MAC Filtering	Protocol	ТСР	•			
Disabled Clients User Login Policies	Source Port	Any	+			
AP Policies Password Policies	Destination Port	HTTP				
Local EAP Priority Order	DSCP	Any	•			
 Certificate 	Direction	Inbound	· ·			
 Access Control Lists Access Control Lists CPU Access Control Lists FlexConnect ACLs 	Action	Deny				

7. 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.

Cisco Wireless LAN Controller IPv6 Deployment Guide, CUWN Release 8.0

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

.ı ı.ı ı. cısco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT
WLANs	WLANs > Edit 'test'
WLANS	General Security QoS Policy-Mapping Advanced
Advanced	Allow AAA Override Enabled Coverage Hole Enabled Enable Session Imeout (secs) Aironet IE Enabled Diagnostic Channel Enabled Override Interface IPv4 None IPv6 Block_HTTPv6-Server Imeout
	Layer2 Acl None P2P Blocking Action Disabled Client Exclusion 2 Enabled 60 Timeout Value (secs) Maximum Allowed Clients 2 Static IP Tunneling If Wi-Fi Direct Clients Policy Disabled V

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.

Cisco Wireless LAN Controller IPv6 Deployment Guide, CUWN Release 8.0

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

Controller RA Throttle Policy > Edit General Enable RA Throttle Policy Image: Second Sec	ı. cısco	MONITOR W	LANS <u>C</u> ONTROLLER	WIRELESS	<u>S</u> ECURITY	MANAGEMENT	C <u>O</u> MMANDS
 PMIPv6 IPv6 	Controller General Inventory Interfaces Interface Groups Multicast Network Routes Redundancy Internal DHCP Server Mobility Management Ports NTP CDP PMIPv6 IPv6	RA Throttle Enable RA Th Throttle Perio Max Through Interval Optic Allow At-leas Allow At-mos	Policy > Edit mottle Policy od (10-86400 seconds) (0-256) on t (0-32) st (0-256)	 ✓ 600 10 No Limit Passthrough ✓ 1 1 No Limit 			

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.

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

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

،،ا،،،ا،، cısco				WIRELESS	SECURITY	MANAGEMENT
CISCO Controller General Inventory Interfaces Interface Groups Multicast Network Routes Redundancy Internal DHCP Server Mobility Management Ports	MONITOR Neighbor Down Life Reachabl Stale Life Unknown NA Multic	WLANS r Binding etime (0-86 the Lifetime etime (0-86 the Address N cast Forwar	CONTROLLER 6400 seconds) (0-86400 seconds) 400 seconds) fulticast NS Forward ding	30 300 86400 Disable Enable		MANAGEMENT
)					

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

uluilu cisco	MONITOR	<u>W</u> LANS	CONTROLLER	WIRELESS	SECURITY	Sa <u>x</u> MANAGEMENT	e Configuration COMMANDS	Eing HELP	Logout Befresh EEEDBACK
Wireless	Media St	reams						Add New	Delete All
 Access Points All APs Radios 802.11a/n 802.11b/g/n Gibbal Configuration 	Stream N	ame Star	rt IP Address E	nd IP Address	Operation	Status			
Advanced									
Mesh									
RF Profiles									
FlexConnect Groups FlexConnect ACLs									
▶ 802.11a/n									
▶ 802.11b/g/n									
 Media Stream General Streams 									

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.

cisco	MONITOR WLANS CONTROLLER WIRELES	Save Configuration Ping
Wireless	Media Stream > New	< Back
Access Points All APs Radios	Stream Name Multicast Destination Start IP Address(ipv4/ipv6)	Stream-A-IPv6 ff00:0:2::20
802.11a/n 802.11b/g/n Global Configuration	Multicast Destination End IP Address(ipv4/ipv6) Maximum Expected Bandwidth(1 to 35000 Kbps)	ff00:0:2::23
Advanced	Resource Reservation Control(RRC) Para	neters
Mesh RF Profiles FlexConnect Groups FlexConnect ACLs	Select from predefined templates Average Packet Size (100-1500 bytes) RRC Periodic update	Select - 1200
▶ 802.11a/n ▶ 802.11b/g/n	Traffic Profile Violation	a best-effort •

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

Cisco Wireless LAN Controller IPv6 Deployment Guide, CUWN Release 8.0

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 Of 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.



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.

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

MONITOR WLANS CO	NTROLLER WIRELESS	SECURITY	MANAGEMENT
Interfaces > Edit			
General Information Interface Name MAC Address Configuration	management e0:2f:6d:5c:f0:40		5
Quarantine Quarantine Vlan Id NAT Address	0		
Enable NAT Address	8		
VLAN Identifier IP Address Netmask Gateway Primary IPv6 Address Prefix Length Primary IPv6 Gateway	10 10.10.10.2 255.255.255.0 10.10.10.1 2001:10:10:10:12 64 fe80::5e50:15ff:fe74:d	3c1	•
	MONITOR WLANS CO Interfaces > Edit General Information Interface Name MAC Address Configuration Quarantine Quarantine Vlan Id NAT Address Enable NAT Address VLAN Identifier IP Address Netmask Gateway Prefix Length Primary IPv6 Gateway Link Local IPv6 Address	MONITOR WLANS CONTROLLER WIRELESS Interfaces > Edit <	MONITOR WLANS CONTROLLER WIRELESS SECURITY Interfaces > Edit

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

Interfaces						
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] through your respective wired client connected to your controller.

Cisco Wireless LAN Controller IPv6 Deployment Guide, CUWN Release 8.0

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



4. 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.

ient Properties		AP Properties	
MAC Address	ac:fd:ec:3b:3b:74	AP Address	a8:0c:0d:db:d2:90
IPv4 Address	10.10.10.51	AP Name	POD1-AP2700
IPv6 Address	2001:10:10:10:4d0c:c7a1:2274:bbbc,	AP Type	802.11an
	2001:10:10:10:30:94/8:8281:5, 2001:10:10:10:c84:3221:5cca:737,	AP radio slot Id	1
	fe80::1cc5:39a:5108:f3ae,	WLAN Profile	POD1-PSK
		WLAN SSID	POD1-PSK
		Status	Associated
		Association ID	1
		802.11 Authentication	Open System
		Reason Code	1
-		// Status Code	0
Client Type	Regular	CF Pollable	Not Implemented
User Name		CF Poll Request	Not Implemented
Port Number	1	Short Preamble	Not Implemented
Interface	management	PBCC	Not Implemented
VLAN ID	10	Chappel Agility	Not Implemented

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.

353144

Cisco Wireless LAN Controller IPv6 Deployment Guide, CUWN Release 8.0

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

Status:	Connected Wi-Fi is connected to IP address 10.10.10	Turn Wi-Fi Off to POD1-PSK and has the 0.65.
Network Name:	POD1-PSK	* *
	🗌 Ask to join ne	w networks
	Known networks w If no known netwo have to manually s	vill be joined automatically. orks are available, you will select a network.

Wi-Fi	TCP/IP DNS WINS 802.1X Proxie	es Hardware
Configure IPv4:	Using DHCP	
IPv4 Address:	10.10.10.65	Renew DHCP Lease
Subnet Mask:	255.255.255.0 DHCP Client ID:	
Router:	10.10.10.1	(If required)
Configure IPv6:	Automatically \$	
Router:	fe80::5e50:15ff:fe74:d3c1	
	IPv6 Address	Prefix
	2001:10:10:10:8638:35ff:fe3e:818a	64
	2001:10:10:10:51d5:88f3:32:ba3d	64
	2001:10:10:10:801c:2ec4:3eec:f3f3	64

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

\varTheta 🕘 🕒 🏦 🖆 🖆 🖓 ali — bash — 80×24	
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.

Cisco Wireless LAN Controller IPv6 Deployment Guide, CUWN Release 8.0

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

cisco	MONITOR	WLANS O	ONTROLLE	R WIRELES	SS SECURITY	MANAGEMENT	COMMANDS	HELP	S42 EEEDBACK
Wireless	All APs >	Details for	AP3700_	TME_lab	11.				
* Access Points All APs	General	Credent	ials In	terfaces	High Availabilit	y Inventory	Advanced		
 Radios 802.11a/h/at 802.11b/g/h 	12200		Name	. Le	Han	agement IP Add	ress(Ipv4/Ipv	6)	
Dual-Band Radios Global Configuration	Primary Second	y Controller Iary Controller	5508-MA	-60	200	1:1:10:70::75			_
Advanced Mesh	Tertiary	Controller							
RF Profiles FlexConnect Groups	AP Failo	over Priority	High	×					-

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.

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



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.

Cisco Wireless LAN Controller IPv6 Deployment Guide, CUWN Release 8.0

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

uluulu cisco	MONITOR WLANS CO	NTROLLER WIRELESS	SECURITY M	ANAGEMENT	COMMANDS	HELP	Saya Configu EEEOBACK
Controller	General						
General Inventory Interfaces Interface Groups Multicast > Network Routes > Redundancy	Name 802.3x Flow Control Mode LAG Mode on next reboot Broadcast Forwarding AP Multicast Forwarding AP Multicast Mode I AP IPv6 Multicast Mode I AP Fallback	S508-MA6 Disabled V Disabled V Multicast V Multicast V Enabled V	239.100.100.94 #1e::239:100:100	(LAG M Multicast Group):94	tode is current p Address IPvd	y disabler Multicast	f). : Group Address
Mobility Management Ports NTP	CAPWAP Preferred Mode Fast SSID change Link Local Bridging	ipv4 × ipv6 × Disabled ×					

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:

cisco	MONITOR	<u>W</u> LANS (ONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	нејр	Sa EEEDBACK
WLANs	Ap Groups	s > Edit 'A	VC-group'						
WLANS	General	WLANS	RF Profile	APs	802.11u				
Advanced AP Groups	AP Groun	Name	AVC-00	-			Apply		
	AP Group	Description	APs in a	AVC group					
	NAS-ID		5508-M	IA6					
	Enable C	lient Traffic	QinQ 🔲						
	Enable D	HCPv4 QinQ	1 🖸						
	QinQ Ser	vice Vlan Id	0						
	CAPWAP	Preferred I	Mode V ipv ipv ipv	∧4 ♥ ∧4 /6					

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.

Cisco Wireless LAN Controller IPv6 Deployment Guide, CUWN Release 8.0

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

/ireless	All APs > Details for A	All APs > Details for AP3700_TME_lab									
Access Points All APs Radios 802.11a/h/ac 802.11b/g/n	General Credentia	als Interfaces	High Availability	Inventory Versions	Advanced						
Dual-Band Radios Global Configuration Advanced Mesh RF Profiles FlexConnect Groups FlexConnect ACLs OEAP ACLs Network Lists 092 114/64cr	AP Name Location AP MAC Address Base Radio MAC Admin Status AP Mode AP Sub Mode Operational Status Port Number	AP3700_TME_lab Lab 7c:ad:74:ff:32:4e 08:cc:68:b4:1f:e0 Enable v local v None v REG 1		Primary Softwa Backup Softwa Predownload Sl Predownload M Predownload N Predownload R Boot Version 10S Version Mini 10S Version	re Version re Version tatus I Version ext Retry Tir etry Count n	0.0.72.221 0.0.00 None NA NA 15.2.2.4 15.3(20140629:191548)\$ 7.6.1.76					
002.110/g/n 002.11b/g/n Media Stream Application Visibility And Control Country Timers Netflow QoS	Venue Group Venue Type Venue Name Language Network Spactrum Interface Key GPS Location GPS Present	Unspecified Unspecified F971F0322FBA3EF3E0 No	×	IP Config CAPWAP Prefen DHCP Ipv4 Add Static IP (Ipv4/ Static IP (Ipv4/ Static IP (Ipv4/ Gateway (Ipv I DMst/Pref Address(Ipv4/I Domain Nem	red Mode dress /Ipv6) 4/Ipv6) ix Length r4/Ipv6) pv6) e	Ipv4 (Global Config) 10.70.0.254 255.255.255.0 10.70.0.1 0.0.0.0					

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
mDNS Query Interval
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	<u>W</u> LANs	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS
All APs						
Current Fil	ter		None		[Change]	Filter] [Clear Filter]
Number of	f APs		3			
AP Name		IP	Address(Ipv4	/Ipv6)	AP	Model
POD1-AP36	500	10.1	10.10.54		AIR	-CAP3602I-A-K9
POD1-AP37	/00-1	10.1	10.10.71		AIR	-CAP3702I-A-K9
POD1-AP27	700	200	1:10:10:10:7d	85:567d: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.

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



- 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



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 3	2001:1:1	0:70::75	
Send count=3, Rece	ive coun	=3 from	2001:1:10:70:	::75

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

Cisco Wireless LAN Controller IPv6 Deployment Guide, CUWN Release 8.0

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

- HTTP
- HTTPS



Dynamic interfaces do not have IPv6 addresses.

(Cisco Controller) >sho	w ipv	6 interfa	ce summary
Number of Interfaces			2
Interface Name	Port	Vlan Id	IPv6 Address/Prefix Length
management	1	70	fe80::1edf:fff:fec6:a1a0/64
	1	70	::/128
service-port	N/A	N/A	fe80::1edf:fff:fec6:a1a1/64
1.1.1.1	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.



Cisco Wireless LAN Controller IPv6 Deployment Guide, CUWN Release 8.0

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

SNMP Trap Receiver > Ne	W	
Community Name	private	
IP Address(Ipv4/Ipv6)	2001:db8:a::5	
Status	Enable \$	61
IPSec		3531

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.



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 Mulitcast CacheMiss Forwarding	Disabled
NA Mulitcast Forwarding	Enabled
IPv6 Capwap UDP Lite	Enabled
Operating System IPv6 state	Enabled

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 conne	ctions	_		
AP Name	Local Port	Peer IP	Peer Port	Ciph	ersuite
1-V6-AP-1600-2_P13 1-V6-AP-1600-2_P13 3-V4-AP-2602-1_P10 3-V4-AP-2602-1_P10	Capwap_Ctrl Capwap_Data Capwap_Ctrl Capwap_Data	2001:9:5:94:20 2001:9:5:94:20 2001:9:5:91:44 2001:9:5:91:44	6:f6ff:fe18:250c 6:f6ff:fe]8:250c 98:d688:1500:8d90 98:d688:1500:8d90	33361 33361 43476 43476	TLS_RSA_WI TLS_RSA_WI TLS_RSA_W TLS_RSA_W TLS_RSA_W
(mavora-wlc-5500-2) link-encryption link (mavora-wlc-5500-2) link-encryption link (mavora-wlc-5500-2)	<pre>>config ap li? c-latency >config ap link? c-latency >config ap link-</pre>	encryption ?			
enable Enabl disable Disab	es Data Link enc bles Data Link en	ryption cryption			
(mavora-wlc-5500-2)	>config ap link-	encryption enabl	e ?		
<cisco ap=""> Enter all Apply</cisco>	the name of the the configurati	Cisco AP. on for all capab	ole Cisco AP	-	
(mavora-wlc-5500-2)	>config ap link-	encryption enabl	e		

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>

Cisco Wireless LAN Controller IPv6 Deployment Guide, CUWN Release 8.0

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



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.

lonitor	Clients > Detail		< Back	Link Test Rem	ove
Summary Access Points Cisco CleanAir Statistics CDP Rogues Clients Sleeping Clients Multicast Applications	General AV Client Type User Name Port Number Interface VLAN ID CCX Version E2E Version Mobility Role Mobility Peer IP Address Policy Manager State Manager S	Regular 1 management 94 CCXv4 E2Ev1 Local N/A WEBAUTH_REQD No 226 OFF m15	*	CF Pollable CF Poll Request Short Preamble PBCC Channel Agility Timeout WEP State PMIP Properties Mobility type	м — ш
	Data RateSet	6.0,9.0,12.0,18.0,24.0,36.0 4.0	0,48.0,5		

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

Cisco Wireless LAN Controller IPv6 Deployment Guide, CUWN Release 8.0

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

No Service 훅	1:17 PM	* 💼 +
	[::ffff:192.0.2.1]	×
_		
Canno	t Verify Server Id	lentity
Safari o "[::ffff:19	cannot verify the ider 92.0.2.1]". Would you	ntity of J like to
	continue anyway?	
	Cancel	
	Details	
	Continue	
	* –	
$\langle \rangle$		

To verify that the WebAuth is in the $\ensuremath{\textbf{RUN}}$ state, check the controller.

	WLANS CONTROLLER	WIRELESS SECURITY	Saye Configuration Ping Logout Br MANAGEMENT COMMANDS HELP FEED	efrash DBACK
Monitor Summary Access Points Cisco CleanAir Statistics COP Rogues Clients Sleeping Clients Multicast Applications	Clients > Detail General AV Interface VLAN ID CCX Version E2E Version Mobility Peer IP Address Policy Manager State Manager Stat	C Statistics management 94 CCXv4 E2Ev1 Local N/A RUN No 89 OFF 6.0,9.0,12.0,18.0,24.0,36.0,48. 4.0	<back link="" remove<br="" test="">Channel Agility Timeout WEP State PMIP Properties Mobility type</back>	
	802.11u	Not Supported		

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

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.

IIIIII CISCO MONITOR W	(LANS <u>C</u> ON	Troller Wirele	55 <u>s</u> ecurity	Saye Confi	iguration <u>P</u> C <u>O</u> MMANDS	ing Logout <u>R</u> efrast HELP <u>F</u> EEDBACK
Controller	NTP Ser	vers			Appl	y New
General Inventory Interfaces Interface Groups	NTP Polli Server Index	ing Interval seconds Server Address	3600 Key Index	NTP Msg Auth Status		
Multicast	1	2001:9:5:94::1	1	AUTH SUCCESS	; 🖬 🚤	
Network Routes						
Redundancy						
Internal DHCP Server						
Mobility Management						
Ports						
Server Keys		₽ A				

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.

Cisco Wireless LAN Controller IPv6 Deployment Guide, CUWN Release 8.0

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

halo					Saye Co	nfiguration Pi	ng Lo	out <u>R</u> efresh
CISCO MONITO	R WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	FEEDBACK
Management	Sy	slog Configu	ration					Apply
Summary SNMP	s	Syslog Server IP J	Address 200	1:9:5:90::113] =	Add
HTTP-HTTPS Telnet-SSH	Sy	slog Server						
Serial Port	S	yslog Level	Debugging	-				
Local Manageme Users	int s	syslog Facility	Local Use 0					
User Sessions * Logs Config Message logs	Ms	g Log Config	uration					
Momt Via Wirele	55 0	contered Log Leve	Disable					
Software Activa	tion	ionsole Log Level						
Tech Support	т	race Info						

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

syslog Server	
2001:9:5:90::113	Remove
9.5.90.113	Remove

Cisco Wireless LAN Controller IPv6 Deployment Guide, CUWN Release 8.0

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

5	Syslog V	latcher -	Standalo	one Mode										_ 8)
	Collect	O Stop	Status	Reload	Filter	Find	Search	Import	Export	Delete	Reports	Storage	े Settings	
				0										
1	endor Pa	ack He	elp 1	Info										
S	how A	ny Sever	ity - fro	om 2001:	9:5:94::11 •	last 10	000 ‡ me	ssages	Jpdate eve	ry 5	; second	Is Update	ed at 8/30/201	3 11:30:51 AM
6	AutoS	croll	0		11									
2	/Last 1	LOOO Syste	ogs Sys	logs for Pe	riog Impo	rt/Search R	esults (0)	Sources (1) Server	Log Bac	kups			
1 al	Receive	d +		Source IP		Facility	Severity	Tag		Mess	age			2
	8/29/20	137:03:4	6.549 PN	1 2001:9:5:9	4::11	local 0	Info	"sisf5	witcherTa	sk Aug 2	9 19:04:47.	388: #SISF-	6-ENTRY_CRE	ATED: sisf
	8/29/20	13 7:03:4	6.549 PN	1 2001:9:5:9	4:11	local 0	Info	*sisf\$	witcherTa	sk Aug 2	9 19:04:47.	388: #SISF-	6-ENTRY_CRE	ATED: sisf
	8/29/20	137:03:4	6.549 PN	1 2001:9:5:9	4::11	local 0	Info			*SISF	BT Process	: Aug 29 1	9:04:47.389: #SI	SF-6-ENT
	8/29/20	137:04:0	6.992 PN	1 2001:9:5:9	4::11	local 0	Info			*SISF	BT Process	: Aug 29 1	9:05:07.833: #SI	SF-6-ENT
	8/29/20	137:04:1	0.614 PN	1 2001:9:5:9	4::11	local 0	Info	"sisf5	witcherTa	sk Aug 2	9 19:05:11	454: #SISF-	6-ENTRY_CRE	ATED: sisf
	8/29/20	13 7:04:1	0.992 PN	1 2001:9:5:9	4::11	local 0	Info			*SISF	BT Process	: Aug 29 19	9:05:11.833: #5	SF-6-ENT
	8/29/20	137:04:1	1.868 PN	1 2001:9:5:9	4::11	local 0	Info	*sisf5	witcherTa	sk Aug 2	9 19:05:12.	709: #SISF-	6-ENTRY_CRE	ATED: sisf
	8/29/20	13 7:04:1	1.869 PN	1 2001:9:5:9	4::11	local 0	Info	*sisfS	witcherTa	sk Aug 2	9 19:05:12.	710: #SISF-	6-ENTRY_CRE	ATED: sisf
	8/29/20	137:04:1	1.870 PN	1 2001:9:5:9	4::11	local 0	Info			*SISF	BT Process	: Aug 29 1	9:05:12.710: #5	SF-6-ENT
	8/30/20	13 11:30:	32.526	2001:9:5:94	4:11	local 0	Notice	*tplu	Transport	t Aug 3	0 11:31:26.	504: #AAA	-5-SELECT_CA	LL_SUCC
	8/30/20	13 11:30:	32.698	2001:9:5:94	4::11	local 0	Warning	"bca	stReceiveT	ask Aug 3	0 11:31:26	675: #BCA	ST-4-MLD_NO	T_A_QUE
	8/30/20	13 11:30:	34.695	2001:9:5:9	ke11.	local 0	Warning	bca	stReceiveT	ask Aug	0 11:31:28	679: #BCA	ST-4-MLD_NO	T_A_QUE

Radius Over IPv6

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

սիսիս					Saye Co	nfiguration P	ing Log	out <u>R</u> efresh
	WLANS CON	Troller W]	RELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	FEEDBACK
Security	RADIUS	Authenticati	on Serve	ers				
 AAA General RADIUS Authentication Accolling Fallback DNS TACACS+ 	Call Stai Auth Ca Use AES MAC De	ion ID Type I I Station ID Type Key Wrap limiter	Syste AP M (Des Hyph	em MAC Addre AC Address:Si igned for FIPS en	ss v SID v customers and r	equires a key w	rrap compl	iant RADIUS si
LDAP Local Net Users MAC Filtering	Network User	Management	Server Index	Server A	idress			Port
Disabled Clients	V	V	1	2001:9:6:	40::62 🔶			1812
AP Policies Password Policies		V	2	9.1.0.101	-			1812

Accounting servers IPv4 and IPv6 are also supported.

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

սիսի։			Save Configuration Ping Logout Refresh			
	<u>w</u> lans <u>c</u> on	TROLLER	WIRELESS SECURITY	MANAGEMENT	COMMANDS	HELP FEEDBACK
Security	RADIUS	Accoun	ting Servers			Apply
General	MAC De	limiter [Hyphen 💌	i,		
Authentication Accounting	Network User	Server Index	Server Address		Port	IPSec
Fallback	V	1	9.1.0.101	_	1813	Disabled
TACACS+	V	2	2001:9:6:40::62	-	1813	Disabled

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

CISCO MONITOR	Saye Configuration Ping Logo WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP	ut <u>R</u> efresh FEEDBACK
WLANS	WLANs > Edit 'mavora-5500-2-IPv6-1-Management' < Back A General Security QoS Policy-Mapping Advanced	pply
	Select AAA servers below to override use of default servers on this WLAN Radius Servers Radius Server Overwrite interface	
	Authentication Servers	
	Server 1 IP:2001:9:6:40::62, Port:1812 IP:2001:9:6:40::62, Port:1 Server 2 None None	6

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:

Cisco Wireless LAN Controller IPv6 Deployment Guide, CUWN Release 8.0

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

Cisco Controller) >show cdp entry all
Device ID: THE 3750 HA2
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 Control	ler) >show ap cdp neigh	oors ?			
all	Show cdp neighbor info	mation for all Cisco A	Ps.		
ap-name	Show cdp neighbor info	mation for a specific	Cisco AP.		
detail	Show detailed cdp neig	abor information for Ci	sco AP		
(Cisco Control	ler) >show ap cdp neigh	ors all			
AP Name	AP IP		Neighbor Name	Neighbor Port	
AP2600-8aba	10.70.0.110		TME_3750_MA2	GigabitEthernet2/0/3	
IP address:	10.70.0.2				
IPv6 address	: 2001:1:10:70::2 (glo	al unicast)			
IPv6 address	: fd01:1:10:70::2 (glo	al unicast)			
IPv6 address	: fe80::216:c7ff:fe96:2	543 (link-local)			
AP3700_TME_1ab	10.70.0.254		TME_3750_MA2	GigabitEthernet2/0/7	
IP address:	10.70.0.2				
IPv6 address	: 2001:1:10:70::2 (glo	al unicast)			
IPv6 address	: fd01:1:10:70::2 (glo	al unicast)			20
IPv6 address	: fe80::216:c7ff:fe96:2	<pre>543 (link-local)</pre>			1020

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.

Cisco Wireless LAN Controller IPv6 Deployment Guide, CUWN Release 8.0

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

ow ipv	6 interfac	e summary
		2
Port	Vlan Id	IPv6 Address/Prefix Length
1	untagged	fe80::224:97ff:fe69:93c0/64
N/A N/A	N/A N/A	fe80::224:97ff:fe69:93c1/64 ::/128
	Port 1 N/A N/A	Port Vlan Id I untagged N/& N/& N/& N/&

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

(Cisco Controller) >con	fig ip	v6 inters	face slaac service-port disable	
Requested State Configu	red Su	ccessful	ly .	
(Cisco Controller) >sho	w ipv6	interfac	ce summary	
Number of Interfaces			2	
Interface Name	Port	Vlan Id	IPv6 Address/Prefix Length	
management	1 1	untagged untagged	fe80::224:97ff:fe69:93c0/64 2001:1:10:70::75/64	
service-port	N/ à N/ à	N/ A N/ A	fe80::224:97ff:fe69:93c1/64 .::/128	353180

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

Cisco Wireless LAN Controller IPv6 Deployment Guide, CUWN Release 8.0

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

CISCO MONITOR WL	ANS CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	FEEDBACK
General Inventory	Interfaces > Edit General Informatio	n			< Bac	k	Apply
Interfaces Interface Groups Multicast Network Routes Redundancy	Interface Name MAC Address Interface Address	servia 44:2b:	e-port 03:64:f9:81				
Internal DHCP Server Mobility Management Ports NTP CDP	DHCP Protocol IP Address Netmask	9.5. 255.	le 91.114 255.255.0				
PMIPv6 IPv6 mDNS Advanced	SLAAC Standard Standa	nable 01:9:5:91:462 4 80::462b:3ff:h Interface para	b:3ff:feb4:f9 eb4:f981/64 meters cat	181 uses the WLANs a clients.	to be temporal	rily disal	bled and

Rogue APs Origin Based Service Discovery

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

(mavora-wlc-5500-2) >show rogue ap su	ummary	
Rogue Detection Security Level		custom
Rogue Fending 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 Thershold.		0
Total Rogues (AP+Ad-hoc) supported	.	2000
Total Rogues classified		951
		and the second
MAC Address Classification	# AP5 # CI1	ents Last Heard
00:08:30:8e:76:7e Unclassified	2 0 т	Fri Aug 30 11:44:34 2013
00:16:9c:91:10:3e Pending	1 0 1	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

Cisco Wireless LAN Controller IPv6 Deployment Guide, CUWN Release 8.0

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

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

Cisco Wireless LAN Controller IPv6 Deployment Guide, CUWN Release 8.0

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&relind=AVAILABLE&rellifecycle=ED&reltype=latest

Cisco Catalyst 3750E-24PD-E Switch								
Search 🔊	Release 15.0.2-SE6 ED 습습습습	·	Release Note					
	15.0(2)SE6							
12.2.55-SE9(ED)	File Information	Release Date	DRAM/Flash					
15.0.2-SE6(ED) 12.2.58-SE2(ED) 12.2.55-EY(ED)	IP BASE c3750e-ipbasek9-mz.150-2.SE6.bin	28-APR-2014	256 / 64					
✓ All Releases ✓ 15.0								
▼ 15.0SE 15.0.2-SE6(ED) 15.0.2-SE5(ED) 15.0.2-SE4(ED) 15.0.2-SE2(ED)	IP BASE WITH WEB BASED DEV MGR c3750e-ipbasek9-tar.150-2.SE6.tar	28-APR-2014	256 / 64					
15.0.2-SE1(ED) 15.0.2-SE(ED) 15.0.1-SE3(ED) 15.0.1-SE2(ED) 15.0.1-SE2(ED)	UNIVERSAL c3750e-universalk9-mz.150-2.SE6.bin	28-APR-2014	256 / 64					
15.0.1-SE(ED) ▼12.2	UNIVERSAL WITH WEB BASE DEV MGR c3750e-universalk9-tar.150-2.SE6.tar	28-APR-2014	256 / 64					

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.

Cisco Wireless LAN Controller IPv6 Deployment Guide, CUWN Release 8.0

Appendix A

Swit	ch	Ports	Model	SW Version	SV 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	35318/

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_NA2 #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 gos aces:	0.5K
number of IPv4/MAC security aces:	1K
number of IPv6 policy based routing aces:	0
number of IPv6 gos aces:	20
number of IPv6 security aces:	25
-	
On next reload, template will be "desktop IPv4 and	IPv6 vlan" template.

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

Cisco Wireless LAN Controller IPv6 Deployment Guide, CUWN Release 8.0

Appendix A

THE 3750 MA2#sh sdm pref	ault" template.
The selected template optimizes the resources in	and companyed
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:	зк
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::x/64.

Add the IPv6 address to the VLAN interfaces with ipv6 address 2001:9:x: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

Cisco Wireless LAN Controller IPv6 Deployment Guide, CUWN Release 8.0

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.

Cisco Wireless LAN Controller IPv6 Deployment Guide, CUWN Release 8.0

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).

Appendix A

Figure 1 Option Request Field in a Solicit and Request Packets

Eile Edit View Go Capture Analyze Statistics Telephony Iools Internals Help O O I I I I I I I I I I I I I I I I I	1 I I I I I I I I I I I I I I I I I I I
	E 8 9 5 % 1 5
Filter: v Expression Clear A	
No. Time Service Destination Bustered	Apply Save
Image Description Description 10.000 fe80::fe5b:39ff:ff02::1:2 DHCPv6 20.005 fe80::fe5b:39ff:ff02::1:2 DHCPv6 31.199 fe80::fe5b:39ff:ff02::1:2 DHCPv6 41.204 fe80::3e0e:23ff:ff680::fe5b:39ff:fe07:31DHCPv6	Info Solicit XID: 0x3990b9 CID: 00030001fc5b39098c00 Advertise XID: 0x3990b9 IAA: 2001:470:52c5:15:2::250 Request XID: 0x39e434 CID: 00030001fc5b39098c00 IAA: Reply XID: 0x39e434 IAA: 2001:470:52c5:15:2::250 CID
<	
n Frame 1: 112 bures on wire (596 birs) 112 bures contured (596 birs)	on interface 0
m internet Protocol version 6, art. 1460.11(50.391)140/13888 (1460.11) © User Datagram Protocol, Src Port: 546 (546), Dst Port: 547 (547) © DRCPv6 Message type: Solicit (1) Transaction 10: 0x3990b9 ■ Elapsed time ■ Client Identifier ■ Option Request Option Request Option Request (6) Length: 6 Value: 001700180034 Requested Option code: DMS recursive name server (23) Pennetted Option code: DMS recursive name server (23)	esu:sun:new/isees), ust: nu2:si2 (nu2:si2)
Requested option code: CAPWAP Access Controllers (52) # Identity Association for Non-temporary Address	
0000 23 33 00 01 00 02 fc 3b 39 07 38 88 86 6d 6e 00 33[9.8. 0010 00 00 00 3a 11 ff fe 80 00 00 00 00 00 00 00 fe 3b	

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.

Cisco Wireless LAN Controller IPv6 Deployment Guide, CUWN Release 8.0

Appendix A

Figure 2 DHCPv6 option 52 field in Advertise and Reply Packets

dhcpv6-option52.pcapng_[Wireshark 1.12.1 (v1.12.1-0-g01b65bf from master-1.12)] – 🗖 🎫								
Eile Edit	Yiew Go	Capture A	nalyze Statist	ics Telephony Iools	Internals Help			
OOA	a a	18 11 3	t B d	******		qqe	📾 🖄 🤫 36 1 🖽	
Filten				0-0-0-0	v Expression	Clear Apply 5	iave	
No.	1 0.0	Source 00 fe80:	:fe5b:39ff	Destination F:fff02::1:2	Proto DHCI	col Info Pv6 So7	icit XID: 0x3990b9 CID: 00030001fc5b39098c	00
	3 1.19 4 1.20	99 fe80: 04 fe80:	:fe5b:39ff :3e0e:23ff	:fff02::1:2 :ffe80::fe5b:39f	DHCI f:fe07:3iDHCI	PV6 Req PV6 Rep	uest XID: 0x39e434 CID: 00030001fc5b39098c Ny XID: 0x39e434 IAA: 2001:470:52c5:15:2::	00 IAA 250 CI
<								19
DUS DUS Har DUS Lir DNS r Opt Ler Val 2 B Domai Opt Ler Val DNS	ID: 0001 ID: 0001 ID: Tope: rdware t ID Time: rdware t ID Time: recursiv for: DM ngth: 32 lue: 262 DNS ser DNS ser IN Sear Construction: DC ngth: 15 lue: 077 S Domain	000011cad5 link-layy ype: Ethee Mar 31, : address: e name ser is recursin 000000cccc ver addres h List main Search 46d656c614 1 Search Li	139000229 ir address inet (1) 00:00:29: Ver ve name se 0000000000 is: 2620:0 is: 2620:0 ch List (2 6273056c6f ist	20038 plus time (1) :45.00000000 Eas 92:03:58 rver (23) 0000000002262000 :ccc::2 (2620:0:: :ccc::2 (2620:0:: 4) 63616c00	stern Dayligh DOOccdDOOO scc::2) scd::2)	it Time		
E CAPWA Opt Ler Val CAP CAP	AP Acces tion: CA ngth: 32 lue: 200 PWAP Acc PWAP Acc	s Controll PWAP Acces 1047052c50 ess Contro ess Contro	lers Is Control 0014000000 ollers add ollers add	lers (52) 00000000162001047 ress: 2001:470:55 ress: 2001:470:55	7052c50014 2c5:14::16 (2 2c5:14::17 (2	001:470:52c5 001:470:52c5	::14::16) ::14::17)	

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 addresses.

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

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:

Cisco Wireless LAN Controller IPv6 Deployment Guide, CUWN Release 8.0

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;
detault-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, dhcpv6.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.

Cisco Wireless LAN Controller IPv6 Deployment Guide, CUWN Release 8.0

Appendix A

2 DHCP	Carlo co cas i en Creat 🔺	Onting Name	Vendor	Value	Class	Actions	-
WIN-A	GFTID1U7S1	00023 DNS Recursive Nam	Standard Standard	*2620.0.ccd::2*, *2620.0.ccc::2* tmelabs.local	None	Scope Options	
4 10 19	Display Statistics					More Actions	
p (11	New Scope						
1	Define User Classes Define Vendor Classes						
Þ	Set Predefined Options						
	Refresh						
p 🛄	Properties Help						
P							
					Es.		

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.

Predefined C	ptions and Values for v6 ? ×
Option class: Option name:	DHCP. Standard Options 00021 SIP Server Domain Name List Add Edit
Description:	Domain Name of SIP servers available to the clier
Value	► Edt Array
	OK Cancel

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.

Cisco Wireless LAN Controller IPv6 Deployment Guide, CUWN Release 8.0

Appendix A

	Option Type ? X
Class:	Global
Name:	сарwар-ас-v6
Data type:	IPv6 Address 💽 🔽 Array
Code:	52
Description:	
	OK Cancel

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.

2		DHCP			- 0	×
File Action View Help						
🗢 🔿 🙍 🐻 🙆 🖬 🛷						
	Option Name 00023 DNS Recursive Nam 00024 Domain Search List Configur Refresh Eport View Arrange I Line up lo Help	Vendor Standard Standard t cons cons	Value "2620.0ccd::2", "2620.0ccc::2" tmelabs.local	Class None None	Actions Scope Options More Actions	
< m >	8			3		
				10		

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.

Cisco Wireless LAN Controller IPv6 Deployment Guide, CUWN Release 8.0

Appendix A

Scope Options	? X
General Advanced	
Available Options	Description A
00030 NIS+ Domain Name List	Domain nan
00031 SNTP Servers IPv6 Address List	IPv6 Addres
U 00032 Information Refresh Time	This option =
☑ 00052 capwap-ac-v6	~
	12
Data entry	
New IPv6 address:	
New IPV6 address.	
2001:470:52c5:14::16	Add
Current IPv6 address:	
	1
	Hemove
	Un
	0
	Down

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

	Advanced		
Availa	able Options	Description	~
00	030 NIS+ Domai	n Name List Domain nam	
00	031 SNTP Serve	ers IPv6 Address List IPv6 Addres	_
00	032 Information	Refresh Time This option	Ξ
₩ 00	052 capwap-ac-	v6	~
<		>	
0	urrent IPv6 addre 2001 470 52c5 1	ess: 4=15 Remove	
1	2001:470:52c5:1	4:17	
		Up	
		Down	F

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

Cisco Wireless LAN Controller IPv6 Deployment Guide, CUWN Release 8.0

Appendix A

Option Name	Vendor	Value
00052 capwap-ac-v6	Standard	"2001:470:52c5:14::17", "2001:470:52c5:14::16"
00023 DINS 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:



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.

Cisco Wireless LAN Controller IPv6 Deployment Guide, CUWN Release 8.0

Appendix A

DIST-1-1# debug ipv6 dhcp relay

IP∨6 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 21:30:43.457: 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 Mar 31 21:30:43.460: IPV6 DHCP_RELAY: Relaying RELAY-REPLY from 2001:470:52C5:A::7 Mar 31 21:30:43.460: IPV6 DHCP_RELAY: Packet forwarded to FE80::F27F:6FF:FEE8:1214 via Vlan20

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)

```
Dption 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;
# 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;
3
# 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;
ł
# 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;
}
```