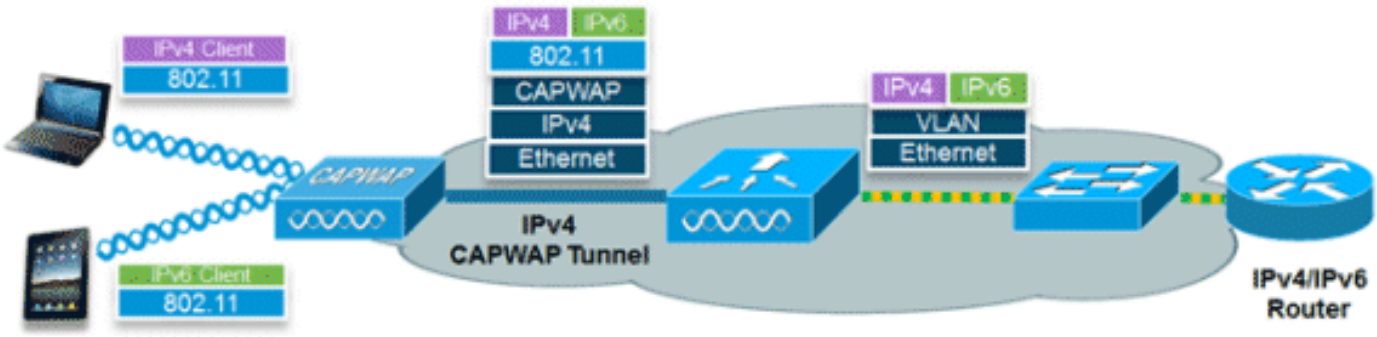
無線LAN IPv6客戶端部署指南

目錄

簡介

本文提供有關思科統一無線LAN解決方案的運行和配置理論的資訊，該理論適用於支援IPv6客戶端。

IPv6無線客戶端連線



思科統一無線網路軟體版本v7.2中的IPv6功能集允許無線網路在同一無線網路上支援IPv4、雙堆疊和僅IPv6客戶端。將IPv6客戶端支援新增到思科統一無線LAN的總體目標是維護IPv4和IPv6客戶端之間的功能奇偶校驗，包括移動性、安全性、訪客接入、服務品質和終端可視性。

每台裝置最多可以跟蹤八個IPv6客戶端地址。這允許IPv6客戶端具有本地鏈路、無狀態地址自動配置(SLAAC)地址、IPv6動態主機配置協定(DHCPv6)地址，甚至備用字首中的地址位於單個介面上。在WGB模式下連線到自主接入點(AP)上行鏈路的工作組網橋(WGB)客戶端還可以支援IPv6。

必要條件

需求

本文件沒有特定需求。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 無線LAN控制器2500系列、5500系列或WiSM2
- AP 1130、1240、1250、1040、1140、1260、3500、3600系列AP和1520或1550系列網狀AP
- 支援IPv6路由器

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

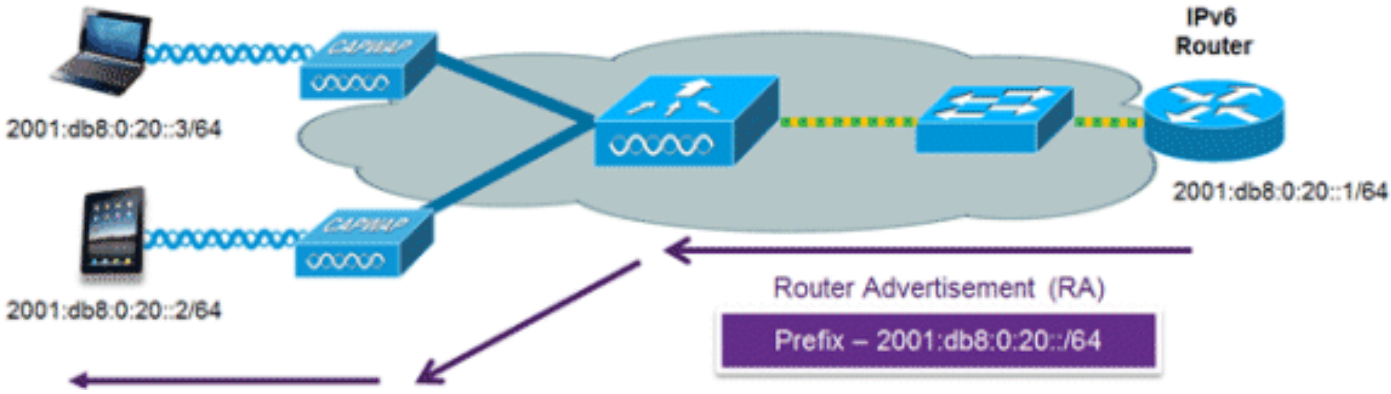
慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

無線IPv6客戶端連線的先決條件

為了啟用無線IPv6客戶端連線，底層有線網路必須支援IPv6路由和地址分配機制（如SLAAC或DHCPv6）。無線LAN控制器必須與IPv6路由器具有L2鄰接關係，且資料包進入控制器時需要標籤VLAN。AP不需要在IPv6網路上連線，因為所有流量都封裝在AP和控制器之間的IPv4 CAPWAP隧道中。

SLAAC地址分配

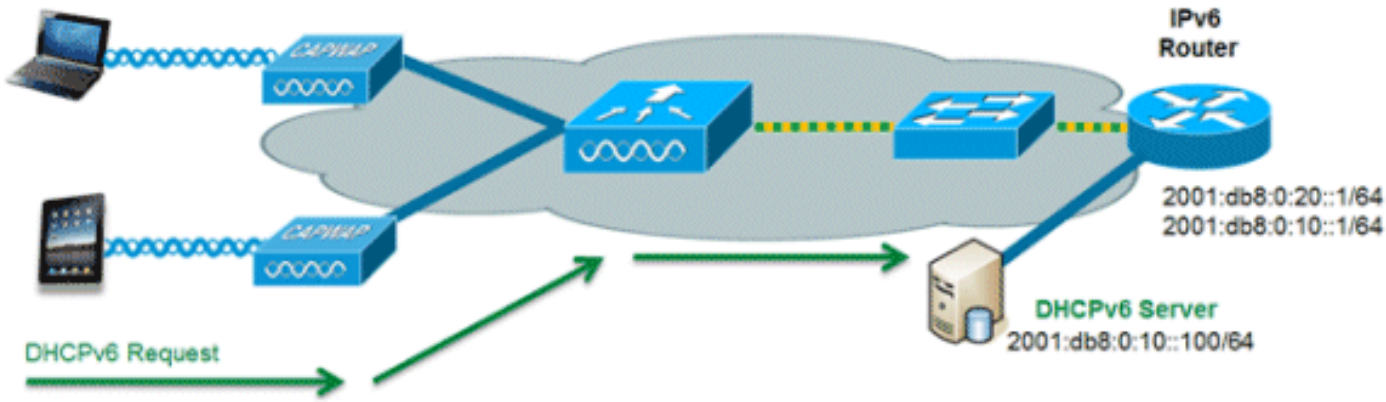


IPv6客戶端地址分配的最常見方法是SLAAC。SLAAC提供簡單的即插即用連線，客戶端可以根據IPv6字首自行分配地址。當IPv6路由器定期傳送路由器通告消息，通知客戶端正在使用的IPv6字首（前64位）和IPv6預設網關時，即可實現此過程。此後，客戶端可以根據兩種演算法生成其IPv6地址的其餘64位：基於介面MAC地址的EUI-64，或者隨機生成的私有地址。演算法的選擇由客戶端決定，並且通常是可配置的。重複地址檢測由IPv6客戶端執行，以確保選中的隨機地址不會與其他客戶端發生衝突。傳送通告的路由器的地址用作客戶端的預設網關。

來自支援Cisco的IPv6路由器的以下Cisco IOS®配置命令用於啟用SLAAC編址和路由器通告：

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

DHCPv6地址分配



如果已部署SLAAC，則不需要使用DHCPv6來進行IPv6客戶端連線。DHCPv6有兩種工作模式，分別稱為**無狀態**和**有狀態**。

DHCPv6 **Stateless**模式用於為客戶端提供路由器通告中不可用的其它網路資訊，但不提供IPv6地址，因為SLAAC已提供此地址。此資訊可包括DNS域名、DNS伺服器及其他DHCP供應商特定選項。此介面配置用於啟用了SLAAC的Cisco IOS IPv6路由器實施無狀態DHCPv6:

```
ipv6 unicast-routing
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:DB8:0:10::100
end
```

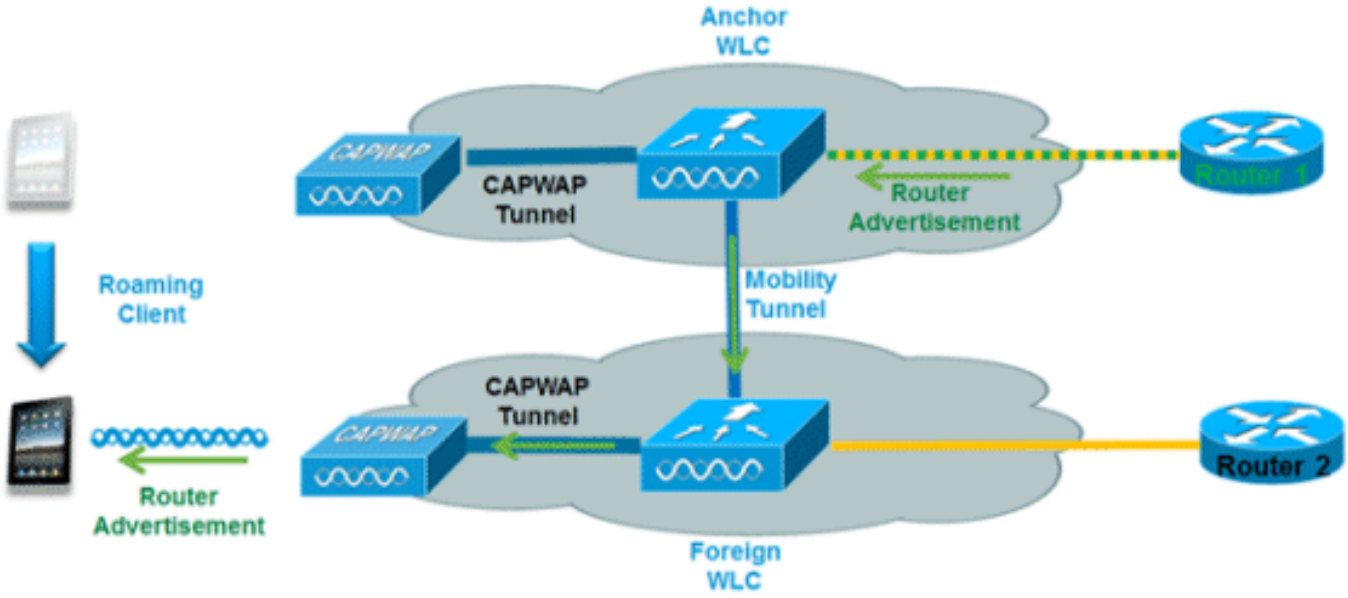
DHCPv6 **Stateful**選項（也稱為託管模式）的工作方式與DHCPv4類似，它為每個客戶端分配唯一的地址，而不是像在SLAAC中那樣為客戶端生成地址的最後64位。此介面配置適用於在禁用SLAAC的情況下實施有狀態DHCPv6的Cisco IOS IPv6路由器：

```
ipv6 unicast-routing
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:DB8:0:10::100
end
```

其他資訊

使用雙堆疊或隧道連線方法配置有線網路以實現完整的IPv6園區範圍連線，不在本文檔的討論範圍之內。有關詳細資訊，請參閱Cisco驗證的部署指南在園區網路中部署IPv6。

IPv6使用者端行動化



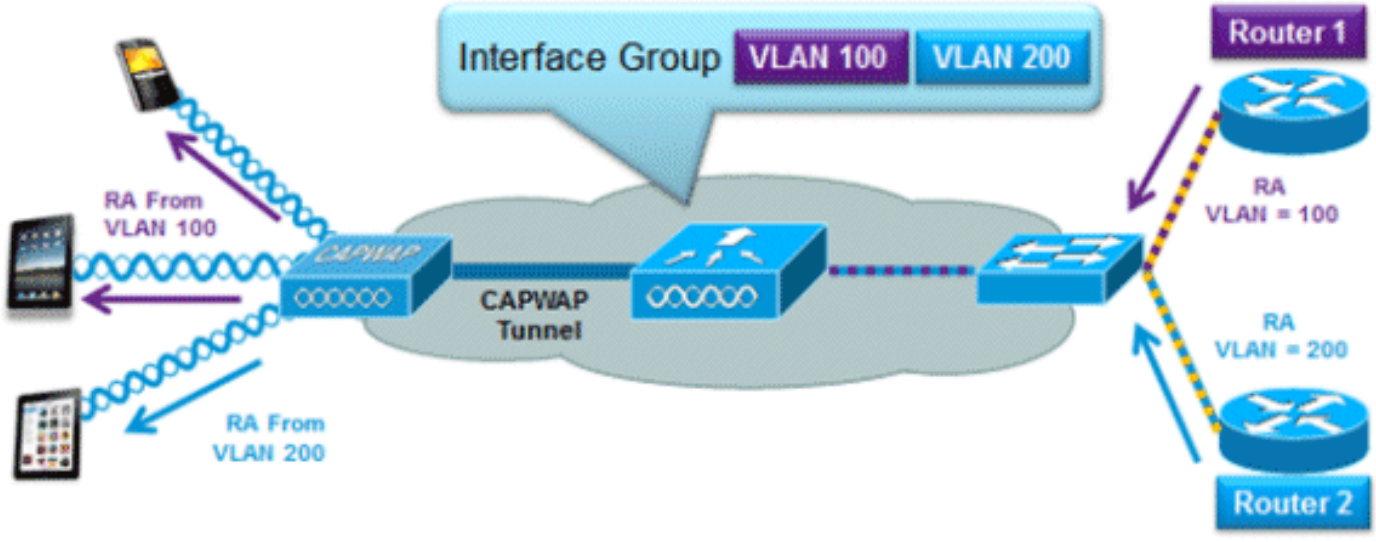
為了處理跨控制器的漫遊IPv6使用者端，必須特別處理ICMPv6訊息，例如鄰居請求(NS)、鄰居通告(NA)、路由器通告(RA)和路由器請求(RS)，以確保使用者端保留在同一第3層網路中。IPv6移動性的配置與IPv4移動性的配置相同，並且客戶端不需要單獨的軟體來實現無縫漫遊。唯一的必需配置是控制器必須屬於同一個移動組/域。

以下是控制器間IPv6客戶端移動性的流程：

1. 如果兩個控制器都具有訪問客戶機原來所在的同一VLAN的許可權，則漫遊只是第2層漫遊事件，在此事件中，客戶機記錄被複製到新控制器，並且沒有流量通過隧道返回錨點控制器。
2. 如果第二個控制器無法訪問客戶端所在的原始VLAN，則會發生第3層漫遊事件，這意味著所有來自客戶端的流量都必須通過移動隧道（IP乙太網）傳輸到錨點控制器。為確保客戶端保留其原始IPv6地址，錨點控制器會將來自原始VLAN的RA傳送到外部控制器，然後使用來自AP的L2單播將其傳送到客戶端。當漫遊的客戶端通過DHCPv6更新其地址或通過SLAAC生成新地址時，RS、NA和NS資料包將繼續通過隧道傳輸到原始VLAN，以便客戶端接收到適用於該VLAN的IPv6地址。

注意：僅IPv6客戶端的移動性基於VLAN資訊。這意味著無標籤的VLAN不支援僅IPv6客戶端移動。

支援VLAN選擇（介面組）

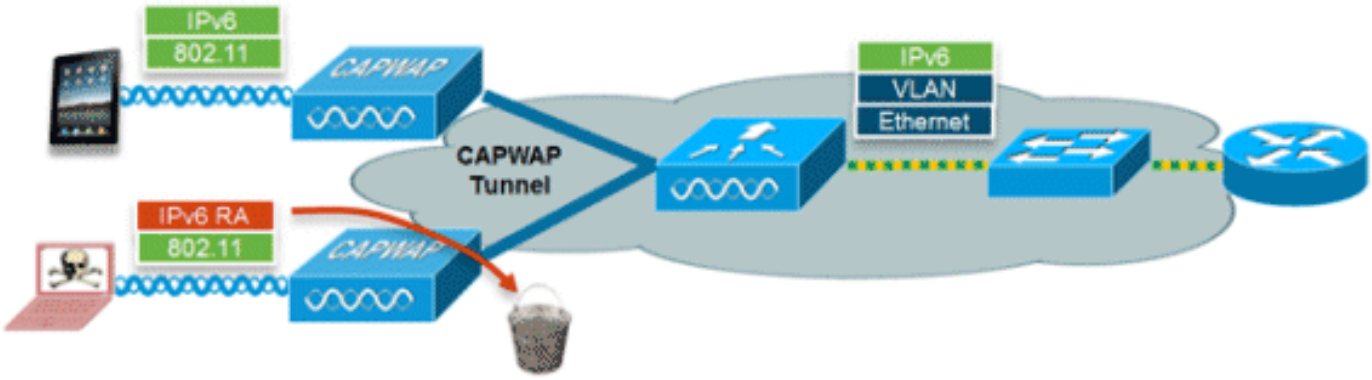


介面組功能允許組織具有在控制器上設定多個VLAN的單一WLAN，以便允許無線使用者端在這些

VLAN之間進行負載平衡。此功能通常用於將IPv4子網保持在較小的規模，同時使WLAN能夠擴展到組內多個VLAN中的數千個使用者。為了支援帶有介面組的IPv6客戶端，不需要額外的配置，因為系統會自動通過L2無線單播將正確的RA傳送到正確的客戶端。通過單播RA，相同WLAN但不同VLAN上的客戶端不會收到錯誤的RA。

IPv6客戶端的第一跳安全

路由器通告防護



RA防護功能通過丟棄來自無線客戶端的RA來提高IPv6網路的安全性。如果沒有此功能，配置錯誤或惡意的IPv6客戶端可能會將自己宣佈為網路路由器，其優先順序通常高於合法的IPv6路由器。

預設情況下，RA防護在AP上啟用（但在AP上可停用），且一律在控制器上啟用。最好在AP上丟棄RA，因為這是一個更具可擴充性的解決方案，並且提供了增強的每客戶端RA丟棄計數器。在任何情況下，IPv6 RA都會在某個時間點被丟棄，從而保護其他無線客戶端和上游有線網路免受惡意或配置錯誤的IPv6客戶端的侵害。

DHCPv6伺服器防護

DHCPv6 Server Guard功能可防止無線客戶端向上游的其他無線客戶端或有線客戶端分配IPv6地址。為了防止DHCPv6地址被分配，來自無線客戶端的任何DHCPv6通告資料包都會被丟棄。此功能在控制器上執行，無需任何配置並自動啟用。

IPv6來源防護

IPv6 Source Guard功能可防止無線客戶端偽造另一個客戶端的IPv6地址。此功能類似IPv4來源防護。IPv6 Source Guard預設啟用，但可以通過CLI禁用。

IPv6位址計費

若是RADIUS驗證和計量，控制器會使用「Framed-IP-address」屬性傳回一個IP位址。本例中使用的是IPv4地址。

當控制器上的「呼叫站ID型別」配置為「IP地址」時，「Calling-Station-ID」屬性使用此演算法來發回IP地址：

1. IPv4地址
2. 全域性單播IPv6地址
3. 鏈路本地IPv6地址

由於客戶端IPv6地址經常更改（臨時或私有地址），因此隨著時間的推移跟蹤這些地址非常重要。Cisco NCS記錄每個客戶端使用的所有IPv6地址，並在每次客戶端漫遊或建立新會話時記錄這些地址。這些記錄可以在NCS中配置為保留長達一年。

注意：在7.2版中，控制器上「呼叫站ID型別」的預設值已更改為「系統MAC地址」。在升級時，應更改該設定，以允許通過MAC地址對客戶端進行唯一跟蹤，因為IPv6地址可能會在會話中發生更改，並且如果Calling-Station-ID設定為IP地址，則會導致記帳問題。

IPv6存取控制清單

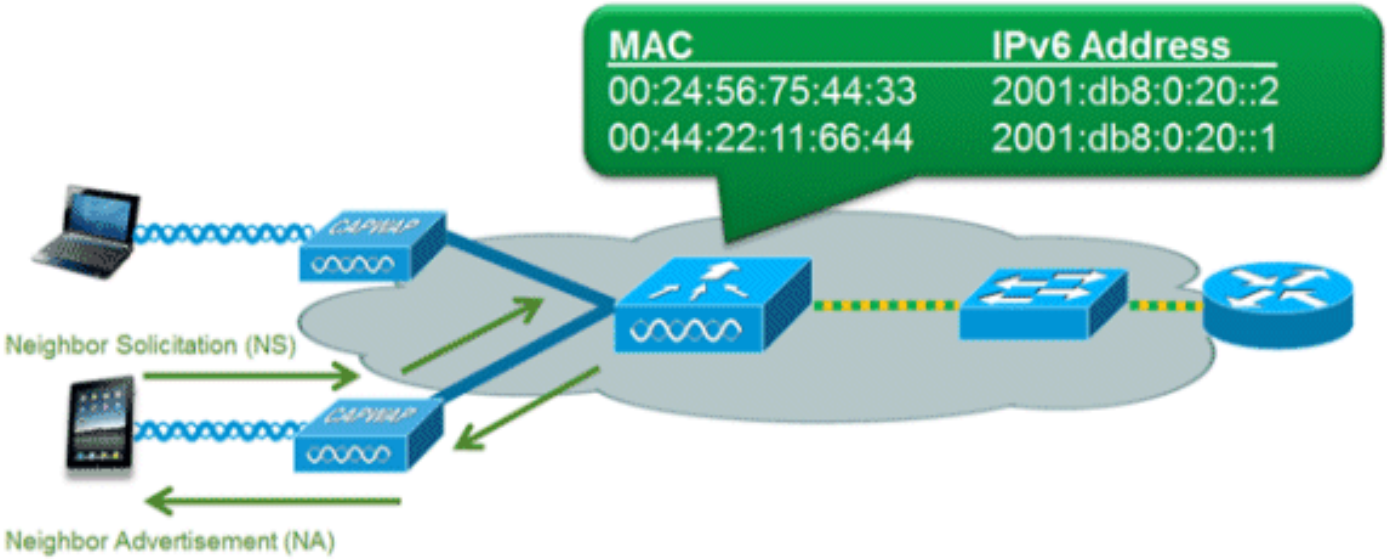
為了限制對某些上游有線資源的訪問或阻止某些應用，可以使用IPv6訪問控制清單(ACL)來識別流量並允許或拒絕該流量。IPv6 ACL支援的選項與IPv4 ACL相同，包括來源、目的地、來源連線埠和目的地連線埠（也支援連線埠範圍）。此外，還支援預身份驗證ACL以使用外部Web伺服器支援IPv6訪客身份驗證。無線控制器最多支援64個唯一IPv6 ACL，每個中都有64個唯一規則。無線控制器繼續支援額外的64個唯一的IPv4 ACL，每個控制器中包含64個唯一規則，雙堆疊客戶端共有128個ACL。

IPv6 ACL的AAA覆寫

為了支援通過集中式AAA伺服器(如思科身份服務引擎(ISE)或ACS)的集中式訪問控制，可以使用AAA覆蓋屬性按客戶端調配IPv6 ACL。若要使用此功能，必須在控制器上設定IPv6 ACL，且必須在啟用AAA覆寫功能的情況下設定WLAN。IPv6 ACL的實際命名AAA屬性是***Airespace-IPv6-ACL-Name***，與用於調配基於IPv4的ACL的*Airespace-ACL-Name*屬性類似。返回的內容的AAA屬性應為與控制器上配置的IPv6 ACL名稱相同的字串。

適用於IPv6使用者端的封包最佳化

鄰居發現快取



IPv6鄰居發現協定(NDP)利用NA和NS資料包代替地址解析協定(ARP)，以允許IPv6客戶端解析網路上其他客戶端的MAC地址。NDP進程可能非常不穩定，因為它最初使用組播地址來執行地址解析；當組播資料包傳送到網段上的所有客戶端時，這會消耗寶貴的無線通話時間。

為了提高NDP進程的效率，鄰居發現快取允許控制器充當代理，並響應它可以解決的NS查詢。鄰居發現快取可以通過控制器中存在的底層鄰居繫結表實現。鄰居繫結表跟蹤每個IPv6地址及其關聯的

MAC地址。當IPv6客戶端嘗試解析另一個客戶端的鏈路層地址時，控制器會擷取NS資料包，然後用NA資料包進行響應。

路由器通告限制

路由器通告限制允許控制器對通向無線網路的RA實施速率限制。通過啟用RA限制，配置為經常傳送RA的路由器（例如每三秒）可以調整回最低頻率，這樣仍然可以保持IPv6客戶端連線。這樣，通過減少必須傳送的組播資料包的數量，可以最佳化通話時間。在所有情況下，如果使用者端傳送一個RS，那麼將允許RA通過控制器並單播到發出請求的使用者端。這是為了確保新客戶端或漫遊客戶端不會受到RA限制的不利影響。

IPv6訪客存取

IPv4客戶端的無線和有線訪客功能與雙堆疊和僅IPv6客戶端的工作方式相同。訪客使用者建立關聯後，系統會將其置於「WEB_AUTH_REQ」執行狀態，直到使用者端透過IPv4或IPv6強制網路入口進行驗證為止。控制器將在此狀態下擷取IPv4和IPv6 HTTP/HTTPS流量，並將其重定向到控制器的虛擬IP地址。一旦使用者通過強制網路門戶進行身份驗證，其MAC地址將移至運行狀態，並且IPv4和IPv6流量都允許通過。對於外部Web驗證，預先驗證ACL允許使用外部Web伺服器。

為了支援僅IPv6客戶端的重定向，控制器根據控制器上配置的IPv4虛擬地址自動建立IPv6虛擬地址。虛擬IPv6地址遵循[::ffff:<IPv4>]。例如，1.1.1.1的虛擬IP地址將轉換為[::ffff:1.1.1.1]。

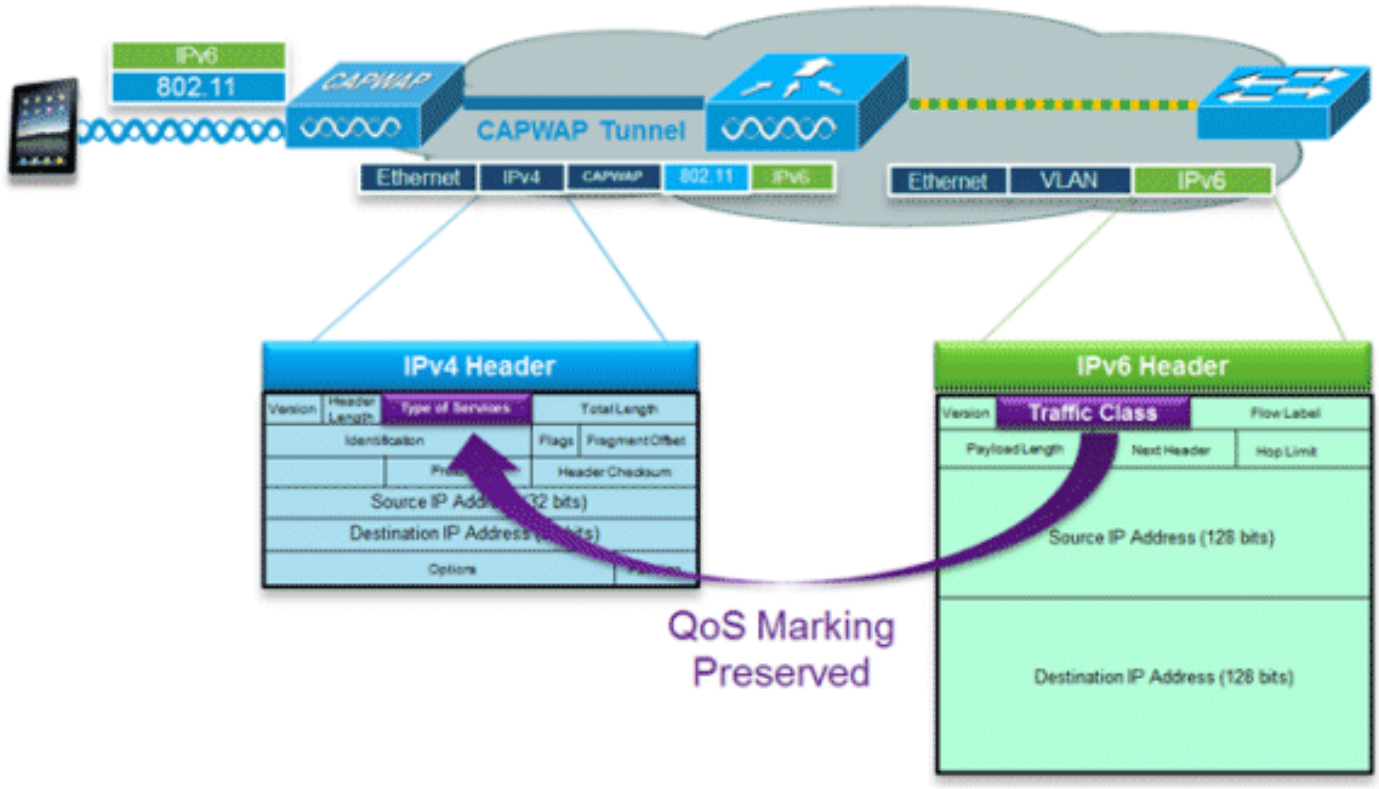
使用受信任SSL證書進行訪客訪問身份驗證時，請確保在DNS中定義了控制器的IPv4和IPv6虛擬地址，以匹配SSL證書主機名。這可確保客戶端不會收到安全警告，說明證書與裝置的主機名不匹配。

注意：控制器的自動生成的SSL證書不包含IPv6虛擬地址。這可能會導致某些Web瀏覽器顯示安全警告。建議為訪客訪問使用受信任SSL證書。

IPv6視訊流

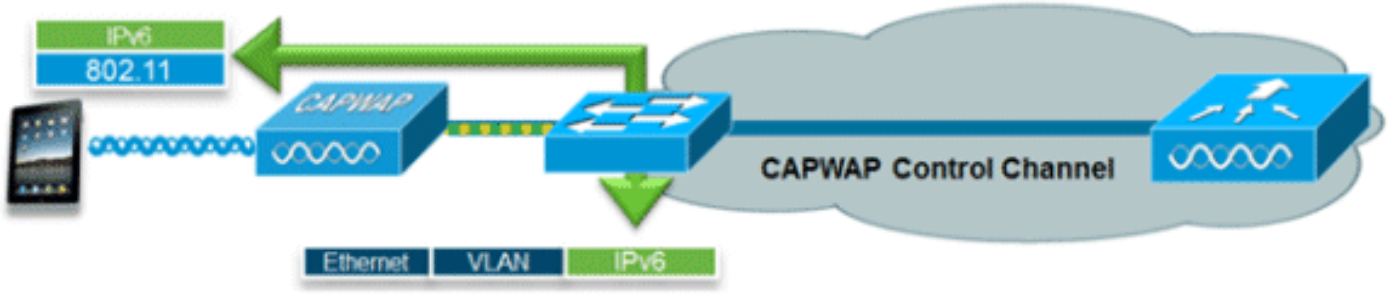
VideoStream支援可靠和可擴展的無線組播影片傳輸，以單播格式向每個客戶端傳送流。實際的組播到單播轉換(L2)發生在AP，提供可擴展的解決方案。控制器在IPv4 CAPWAP組播隧道內傳送IPv6影片流量，該隧道允許向AP進行有效的網路分配。

IPv6服務品質



IPv6資料包使用的標籤與IPv4使用的DSCP值類似，DSCP值最多支援64個不同的流量類(0-63)。對於來自有線網路的下游資料包，會將IPv6 Traffic Class值複製到CAPWAP隧道的報頭，以確保端到端地保留QoS。在上游方向上，IPv6流量類標籤於第3層的客戶端流量將通過標籤目的地為控制器的CAPWAP資料包來執行。

IPv6和FlexConnect



FlexConnect — 本地交換WLAN

本地交換模式下的FlexConnect通過將流量橋接到本地VLAN來支援IPv6客戶端，類似於IPv4操作。跨FlexConnect組的第2層漫遊支援客戶端移動性。

FlexConnect本地交換模式支援以下特定於IPv6的功能：

- IPv6 RA防護
- IPv6橋接
- IPv6訪客驗證（控制器託管）

FlexConnect本地交換模式中不支援這些特定於IPv6的功能：

- 第3層移動性

- IPv6視訊流
- IPv6存取控制清單
- IPv6來源防護
- DHCPv6伺服器防護
- 鄰居發現快取
- 路由器通告限制

FlexConnect — 中央交換WLAN

對於使用中央交換（將流量通道傳回控制器）且處於FlexConnect模式的AP，對於「AP組播模式」，必須將控制器設定為「組播 — 單播模式」。由於FlexConnect AP不加入控制器的CAPWAP組播組，因此必須在控制器上複製組播資料包，並分別單播到每個AP。此方法比「多點傳送 — 多點傳送模式」效率低，且會在控制器上施加額外負荷。

FlexConnect中央交換模式不支援此特定於IPv6的功能：

- IPv6視訊流

注意：Flex 7500系列控制器不支援運行IPv6的集中交換WLAN。

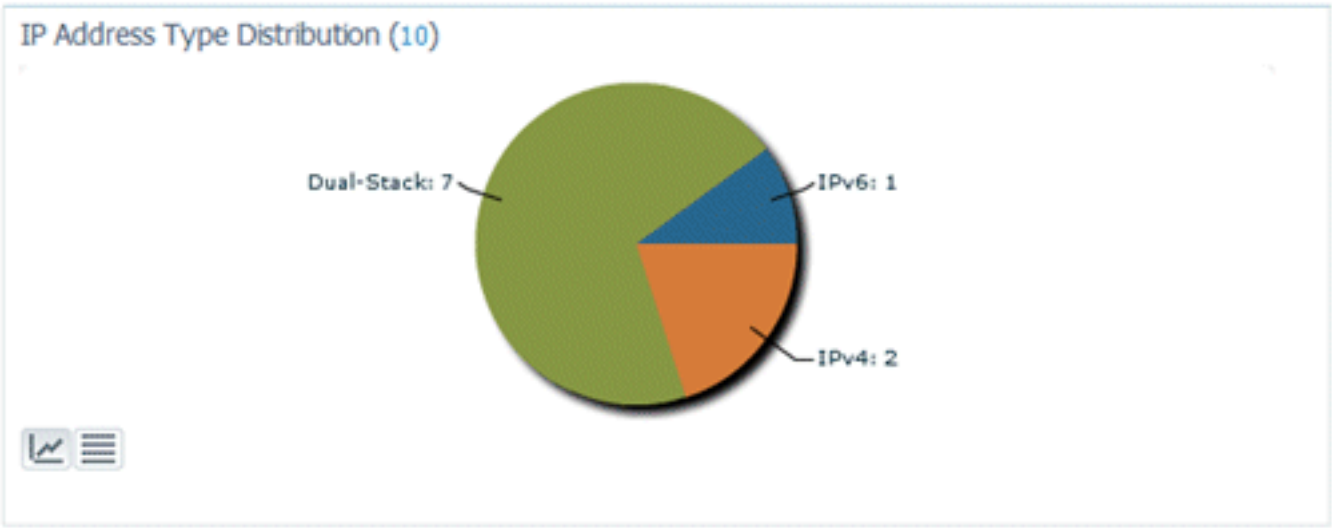
使用NCS的IPv6客戶端可視性

隨著NCS v1.1的發佈，增加了許多額外的IPv6特定功能，以監控和管理有線和無線網路上的IPv6客戶端網路。

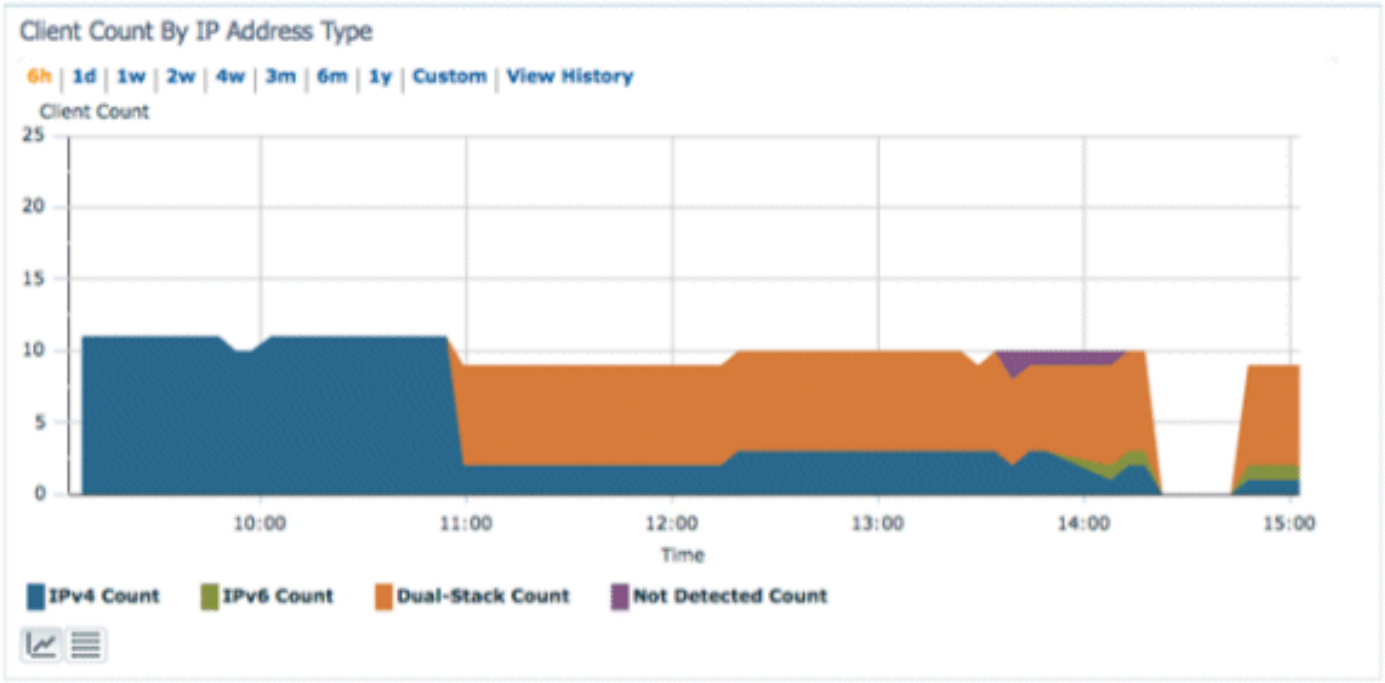
IPv6儀表板專案

為了檢視網路上存在的客戶端型別，NCS中提供了「Dashlet」以深入瞭解IPv6特定的統計資訊，並提供深入檢視IPv6客戶端的功能。

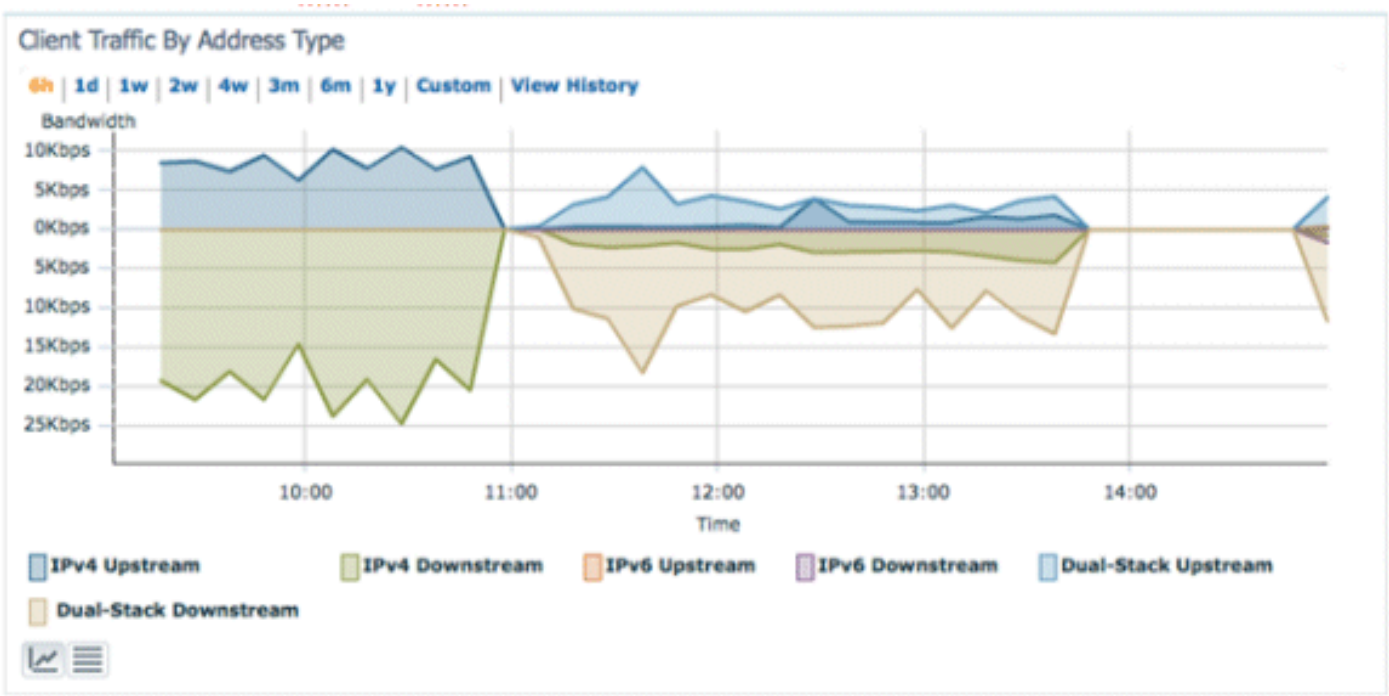
IP地址型別Dashlet — 顯示網路上IP客戶端的型別：



Client Count by IP Address Type — 顯示一段時間內的IP客戶端型別：



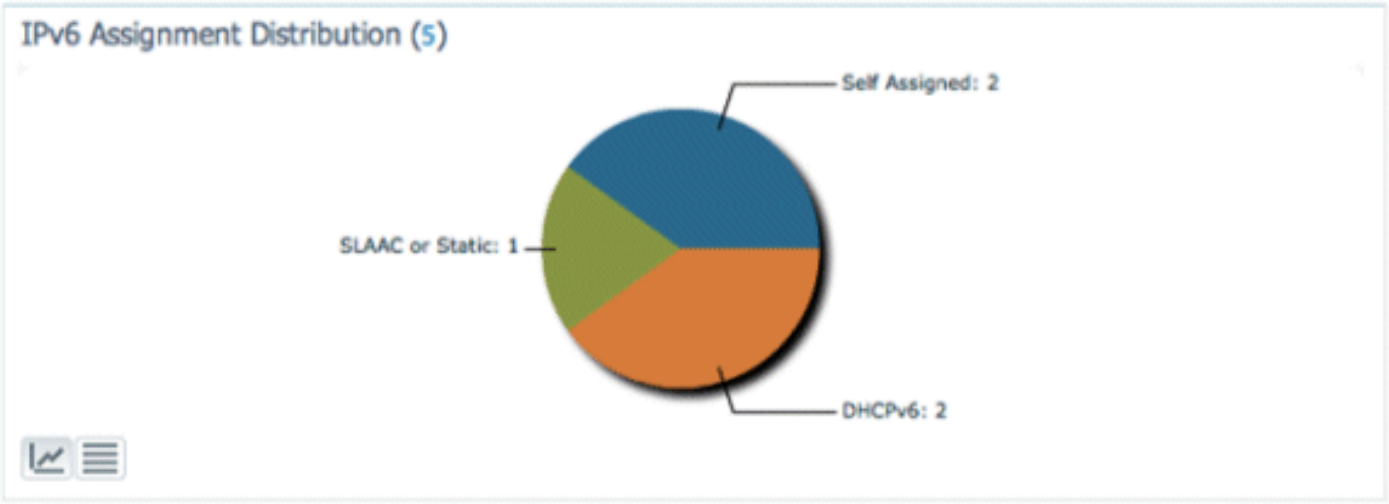
Client Traffic by IP Address Type — 顯示來自每種型別客戶端的流量。雙協定棧類別中的客戶端包括IPv4和IPv6流量：



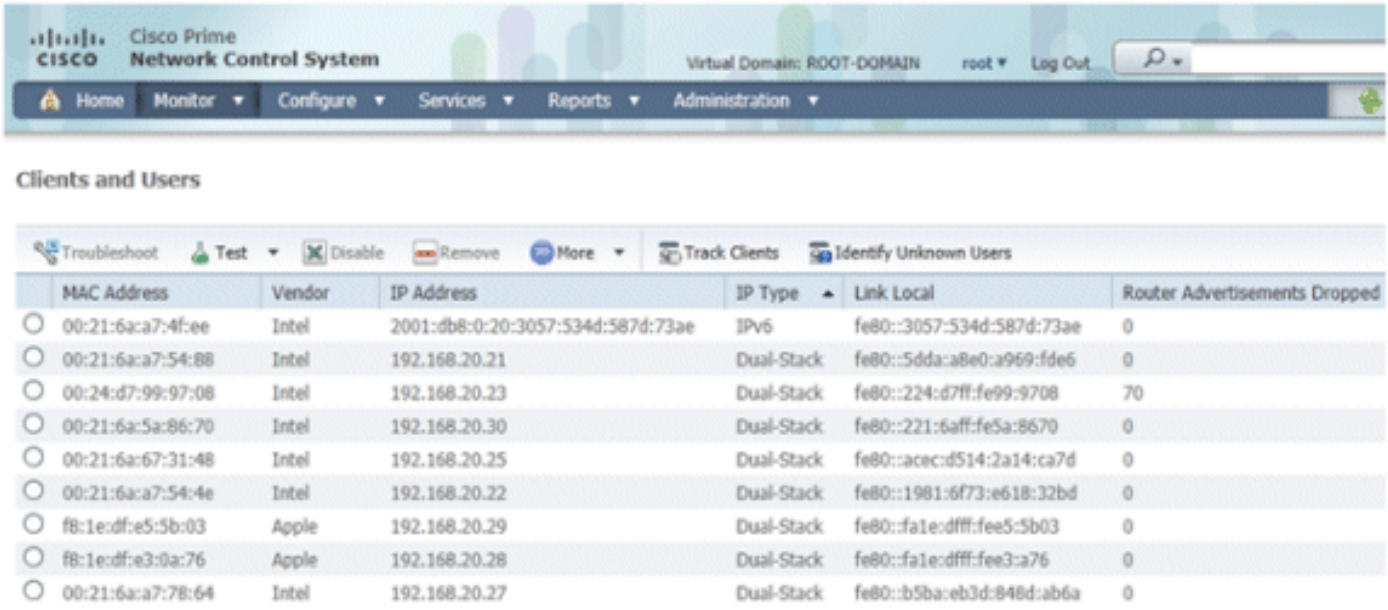
IPv6 Address Assignment — 將每個客戶端的地址分配方法顯示為以下四個類別之一：

- DHCPv6 — 適用於地址由中央伺服器分配的客戶端。客戶端也可能具有SLAAC地址。
- SLAAC或Static — 用於使用無狀態地址自動分配或使用靜態配置地址的客戶端。
- 未知 — 在某些情況下，無法發現IPv6地址分配。此情況僅發生在NCS中的有線客戶端上，因為某些交換機不監聽IPv6地址分配資訊。
- Self-Assigned — 僅具有完全自動分配的本地鏈路地址的客戶端。此類別中的客戶端可能存在IPv6連線問題，因為它們缺少全域性唯一地址或本地唯一地址。

餅圖的每個部分均可按一下，這樣管理員就可以向下鑽取到客戶端清單。

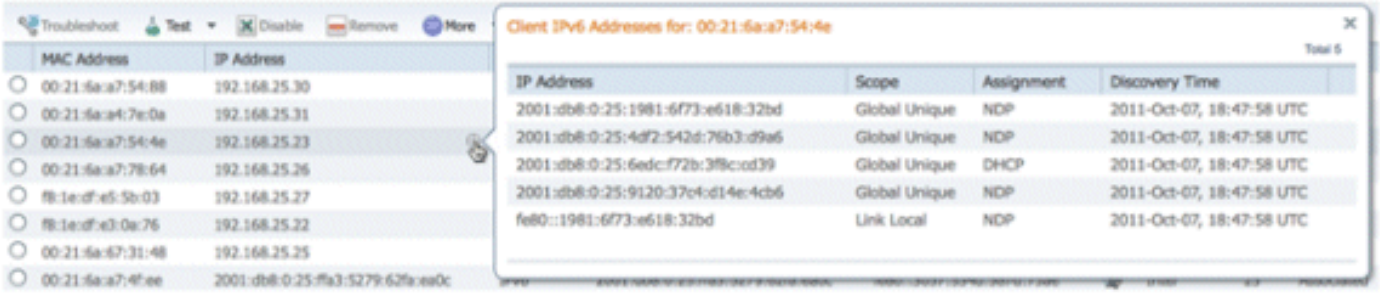


監控IPv6客戶端



為了監控和管理IPv6客戶端資訊，在Clients and Users頁中新增了以下列：

- IP Type — 客戶端的型別，基於從客戶端看到的IP地址。可能的選項包括IPv4、IPv6或Dual-Stack，表示客戶端同時具有IPv4和IPv6地址。
- IPv6分配型別 — NCS將地址分配方法檢測為SLAAC或Static、DHCPv6、Self-Assigned或Unknown。
- 全域性唯一 — 客戶端使用的最新IPv6全域性地址。將滑鼠懸停在列內容上可顯示客戶端使用的任何其他IPv6全域性唯一地址。
- Local Unique — 客戶端使用的最新IPv6本地唯一地址。將滑鼠懸停在列內容上可顯示客戶端使用的任何其他IPv6全域性唯一地址。
- Link Local — 客戶端的IPv6地址，該地址是自行分配的，用於在分配任何其他IPv6地址之前進行通訊。
- Router Advertisements Dropped — 客戶端傳送並在AP丟棄的路由器通告數。此列可用於跟蹤可能配置錯誤或惡意配置為像IPv6路由器一樣工作的客戶端。此列是可排序的，這樣可以輕鬆識別有問題的客戶端。

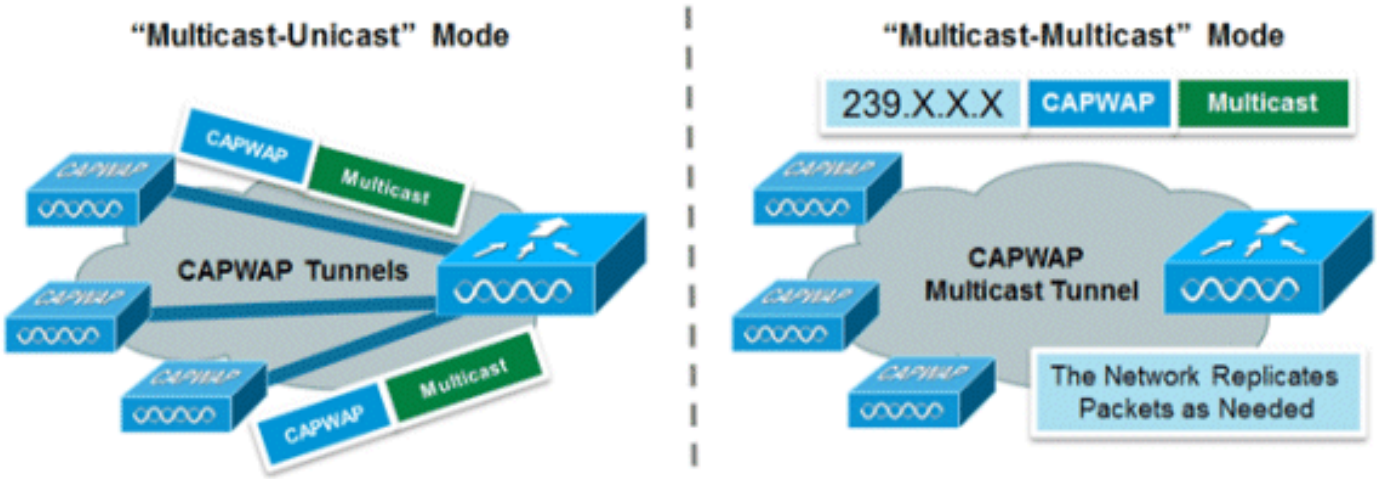


除了顯示IPv6特定列之外，「IP地址」列還會顯示客戶端的當前IP地址，優先顯示IPv4地址（如果是雙協定棧客戶端），或者只顯示IPv6客戶端的IPv6全域性唯一地址。

無線IPv6客戶端支援的配置

到AP的組播分發模式

思科統一無線網路支援將兩種組播分發到與控制器關聯的AP的方法。在這兩種模式下，來自有線網路的原始組播資料包都封裝在第3層CAPWAP資料包內，該資料包通過CAPWAP單播或組播傳送到AP。由於流量是CAPWAP封裝的，因此AP不必與客戶端流量位於同一個VLAN中。這裡比較了兩種組播分發方法：



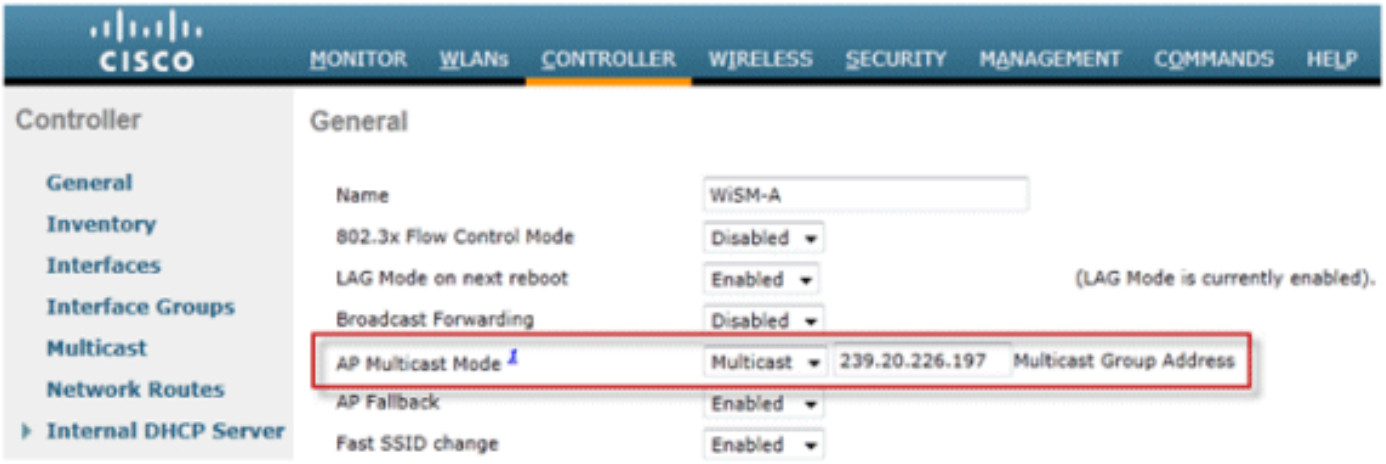
	Multicast-Unicast模式	Multicast-Multicast Mode
傳遞機制	控制器複製組播資料包，並將其傳送到單播CAPWAP隧道中的每個AP	控制器會傳送多點傳送封包的一個副本
支援的AP模式	FlexConnect和本地	僅本地模式
需要在有線網路上進行L3組播路由	否	是
控制器載入	高	低
有線網路載入	高	低

配置組播 — 組播分發模式

出於可擴充性和有線頻寬效率的原因，建議使用組播 — 組播模式。

注意：僅對2500系列無線控制器絕對需要此步驟，但此步驟支援更高效的組播傳輸，建議所有控制器平台都使用此步驟。

轉到「General」頁面下的「Controller」頁籤，確保AP組播模式已配置為使用**組播**模式，並且已配置有效的組地址。組地址是IPv4組播組，建議位於239.X.X.X-239.255.255.255範圍內，該範圍是專用組播應用範圍。

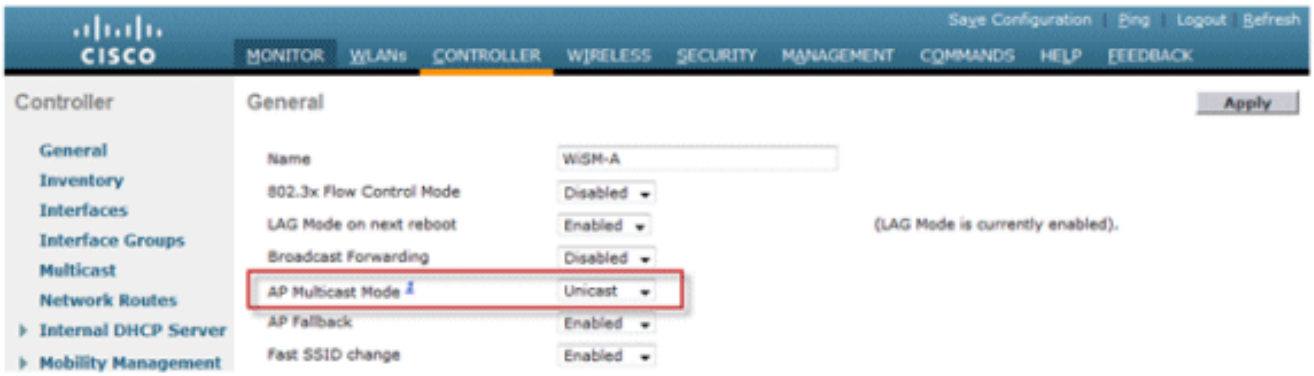


注意：請勿對組播組地址使用224.X.X.X、239.0.0.X或239.128.0.X地址範圍。這些範圍中的地址與鏈路本地MAC地址重疊，泛洪所有交換機埠，即使啟用了IGMP監聽。

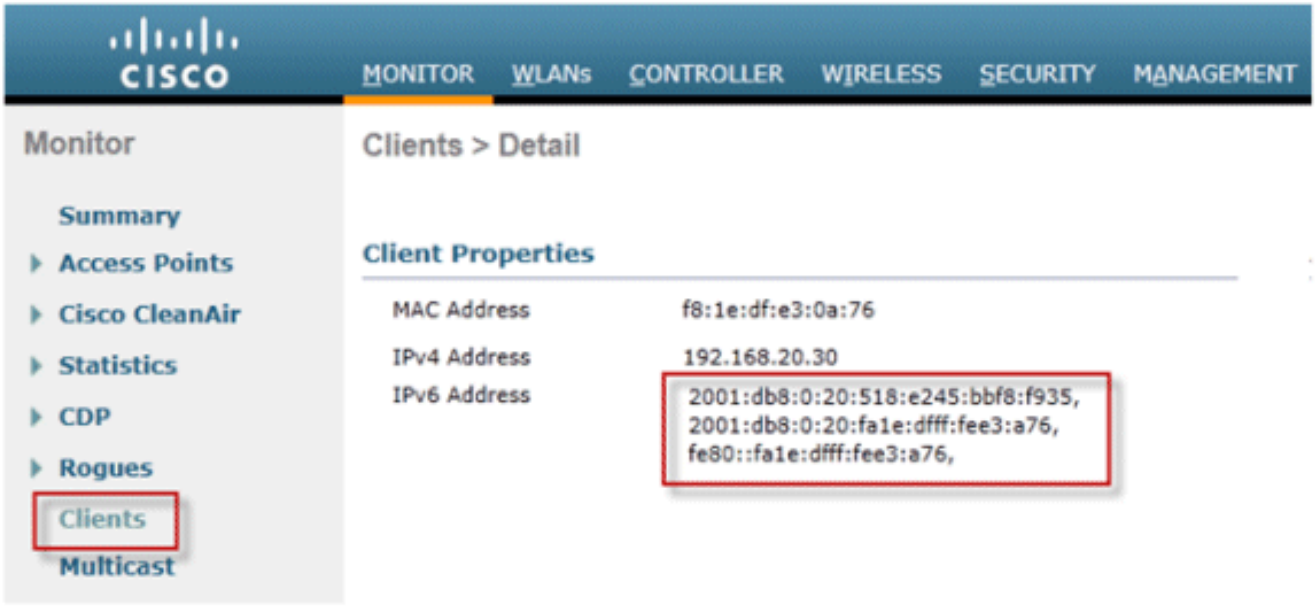
配置組播單播分發模式

如果有線網路未正確配置為在控制器和AP或FlexConnect模式之間傳送CAPWAP組播，並且AP將用於支援IPv6的集中交換WLAN，則需要單播模式。

1. 轉到General頁面下的**Controller**頁籤，確保AP組播模式已配置為使用**單播**模式。



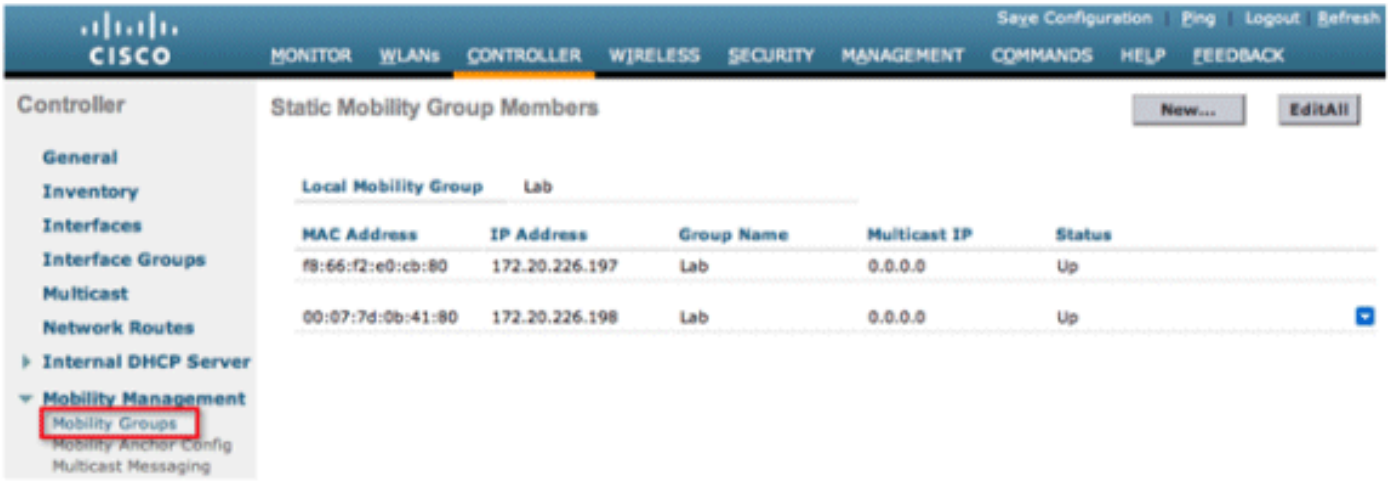
2. 將支援IPv6的客戶端連線到無線LAN。導航到**Monitor**頁籤，然後導航到**Clients**選單，驗證客戶端是否收到IPv6地址。



配置IPv6移動性

除了將控制器置於同一個移動組或同一個移動域內之外，沒有針對IPv6移動性的特定配置。這樣，最多可以有72個控制器加入移動域，即使對於最大的校園也提供了無縫的移動性。

前往**Controller**索引標籤> **Mobility Groups**，並依照MAC位址和IP位址將每個控制器新增到該群組中。這必須在行動群組中的所有控制器上完成。

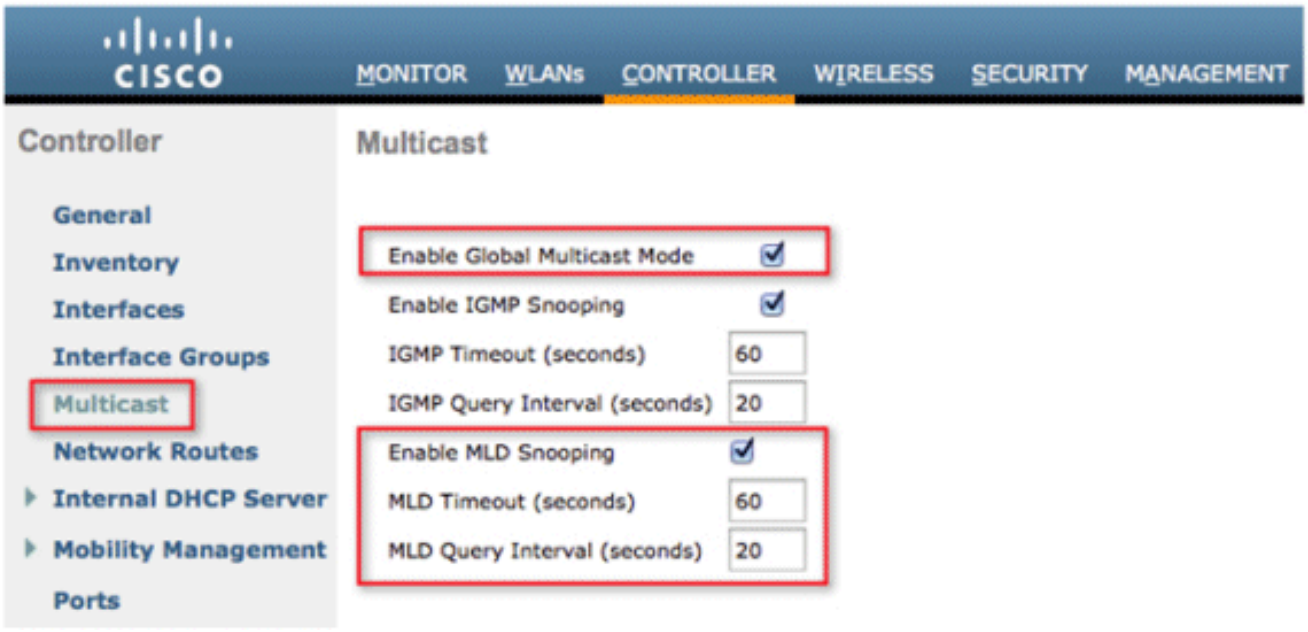


配置IPv6組播

控制器支援用於IPv6組播的MLDv1監聽，這樣它就可以智慧地跟蹤組播流並將其傳送給請求組播流的客戶端。

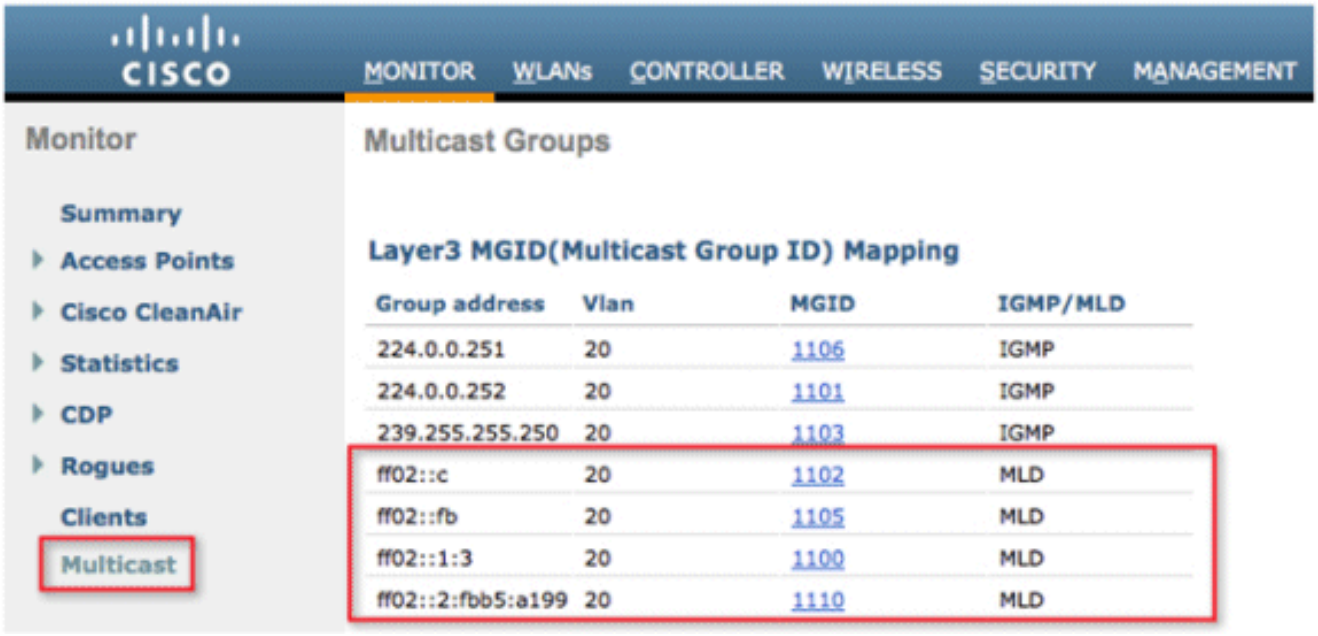
注意：與先前版本的版本不同，IPv6單播流量支援不要求在控制器上啟用「全域性組播模式」。自動啟用IPv6單播流量支援。

1. 前往**Controller**索引標籤> **Multicast**頁面和**Enable MLD Snooping**以支援多點傳送IPv6流量。若要啟用IPv6多點傳送，還必須啟用控制器的**全域多點傳送模式**。



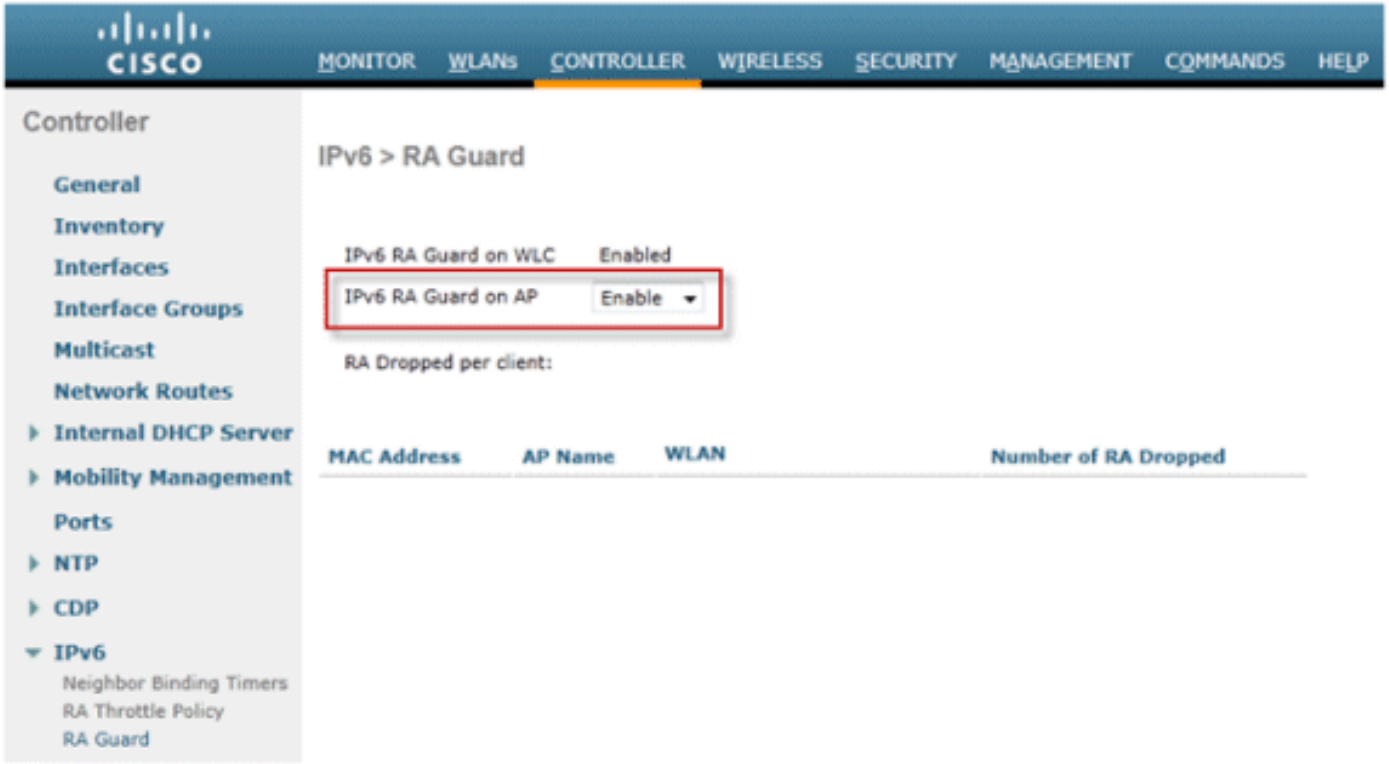
注意：如果需要點對點發現應用程式（如Apple的Bonjour），則應啟用全域性組播模式、IGMP和MLD監聽。

2. 要驗證IPv6組播流量是否被監聽，請轉到**Monitor**頁籤和**Multicast**頁面。請注意，同時列出了IPv4(IGMP)和IPv6(MLD)組播組。按一下MGID以檢視加入該組地址的無線客戶端。



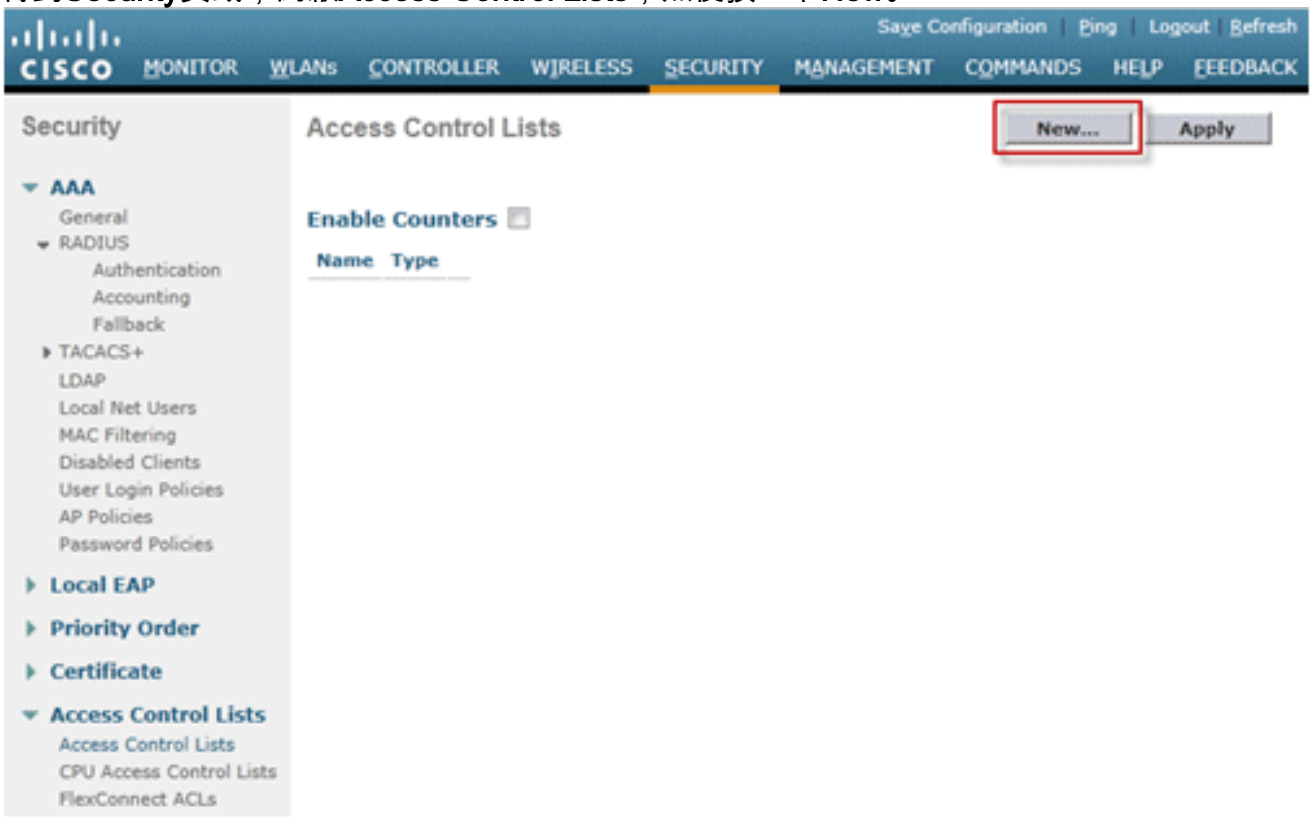
配置IPv6 RA防護

導航至**Controller**頁籤，然後在左側選單上導航至**IPv6 > RA Guard**。在AP上啟用IPv6 RA防護。無法禁用控制器上的RA防護。除RA Guard配置之外，此頁還顯示被標識為傳送RA的所有客戶端。



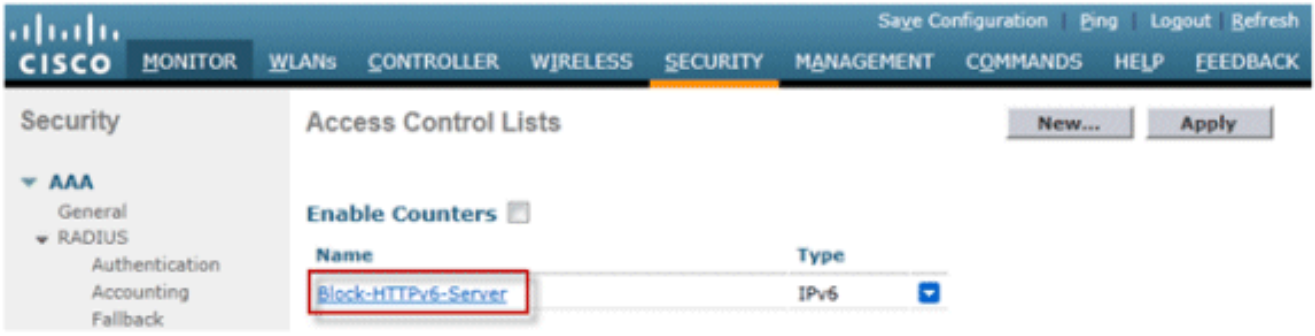
配置IPv6訪問控制清單

1. 轉到Security頁籤，開啟Access Control Lists，然後按一下New。

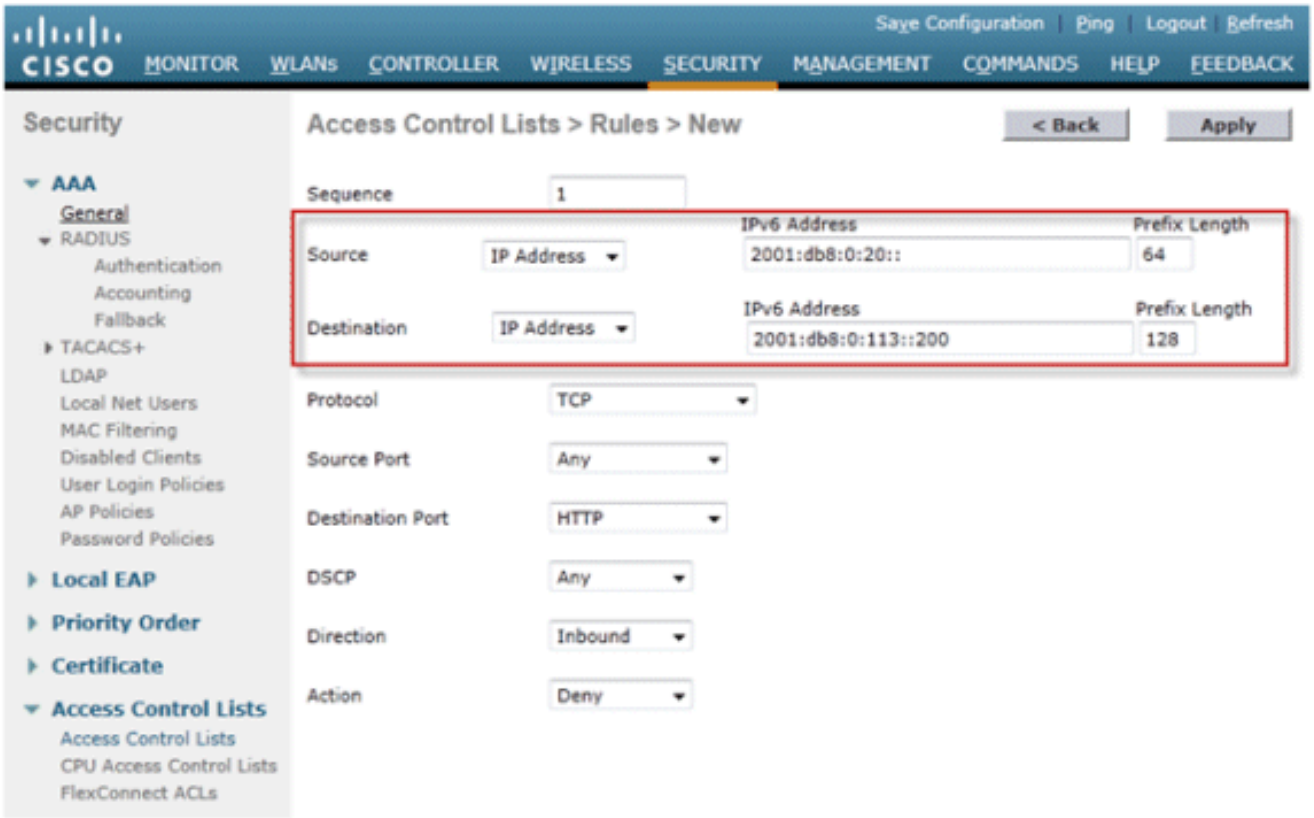


2. 輸入ACL的唯一名稱，將ACL型別更改為IPv6，然後按一下Apply。

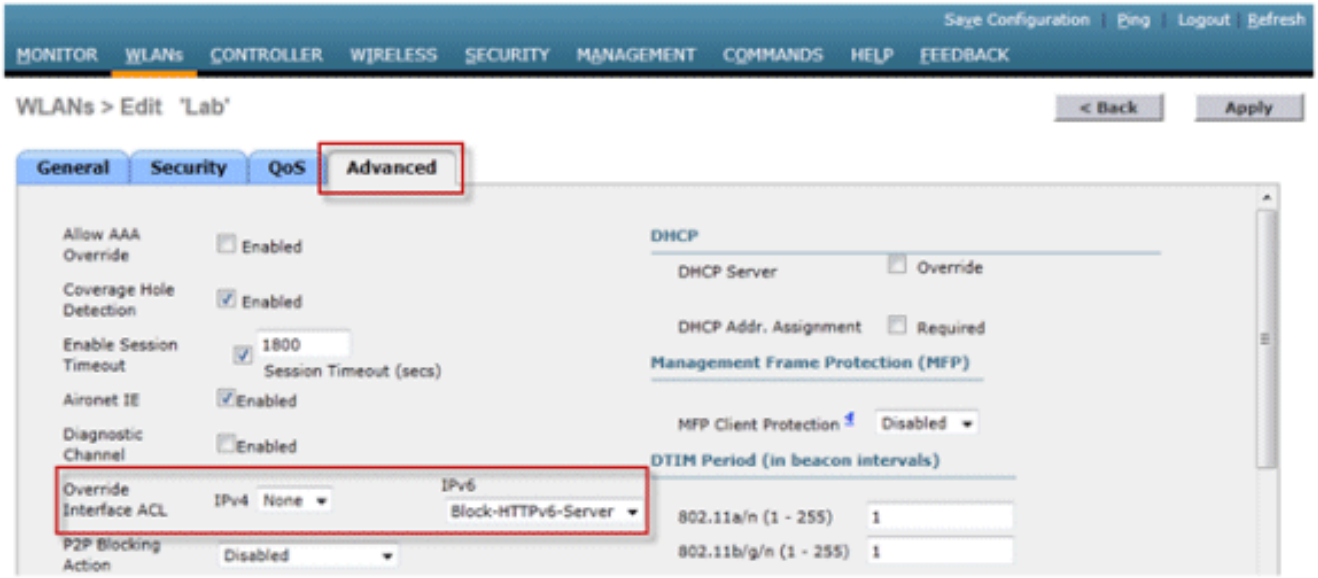
3. 按一下在上述步驟中建立的新ACL。



4. 按一下**Add New Rule**，輸入所需的規則引數，然後按一下**Apply**。將序列號留空，以便將該規則置於清單的末尾。「Inbound」的「Direction」選項用於來自無線網路的流量，而「Outbound」選項用於發往無線客戶端的流量。請記住，ACL中的最後一個規則是隱含的deny-all。字首長度為64與整個IPv6子網匹配，字首長度為128用於唯一限制對單個地址的訪問。

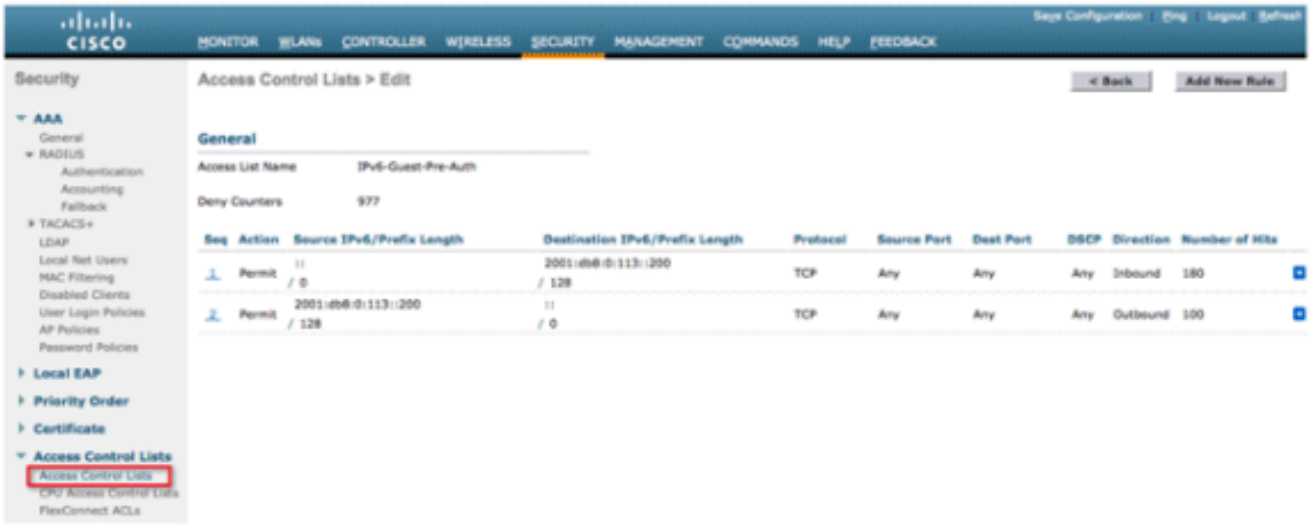


5. IPv6 ACL以每個WLAN/SSID為基礎應用，可以同時在多個WLAN上使用。導航到**WLANs**頁籤，然後按一下問題SSID的WLAN ID以應用IPv6 ACL。按一下**Advanced**頁籤，將Override Interface ACL for IPv6更改為ACL名稱。



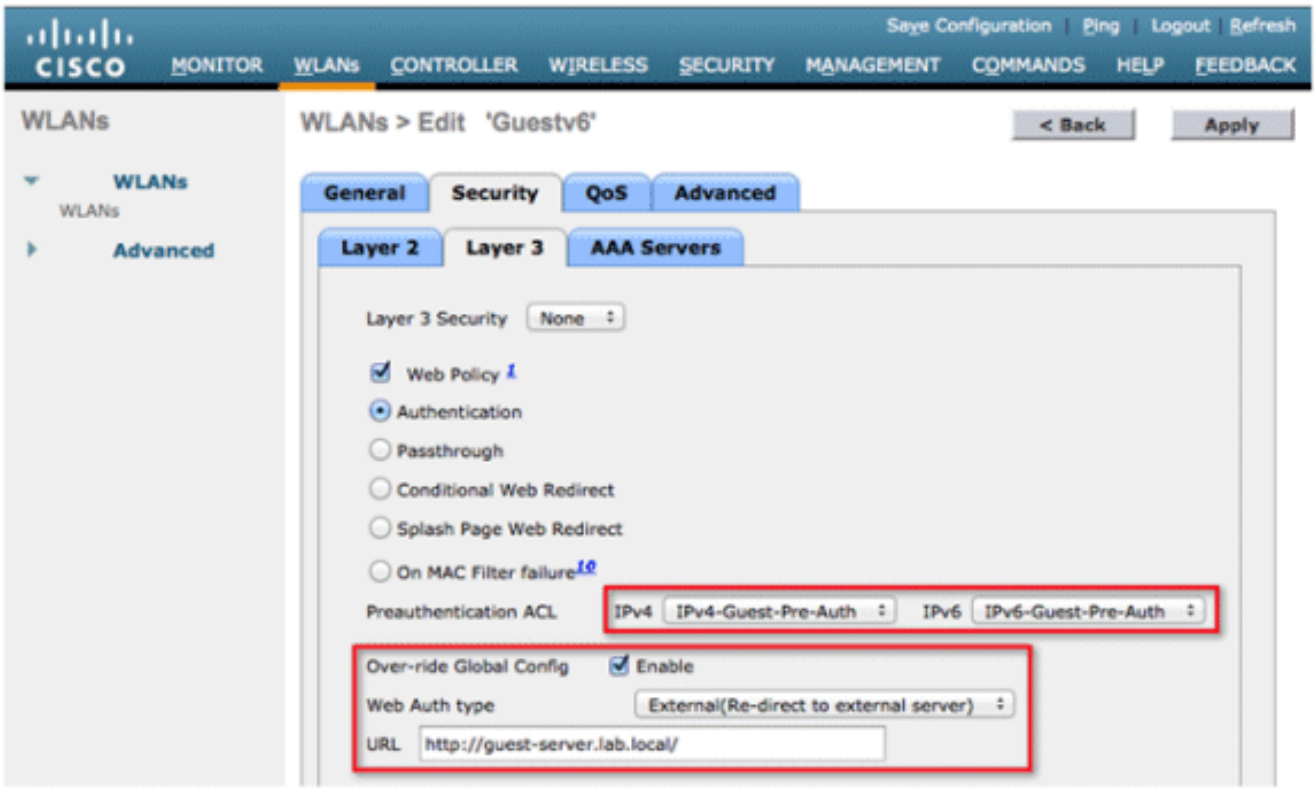
為外部Web身份驗證配置IPv6訪客訪問

1. 為Web伺服器配置IPv4和IPv6預身份驗證ACL。這樣會在使用者端完全通過驗證之前，允許流量進出外部伺服器。



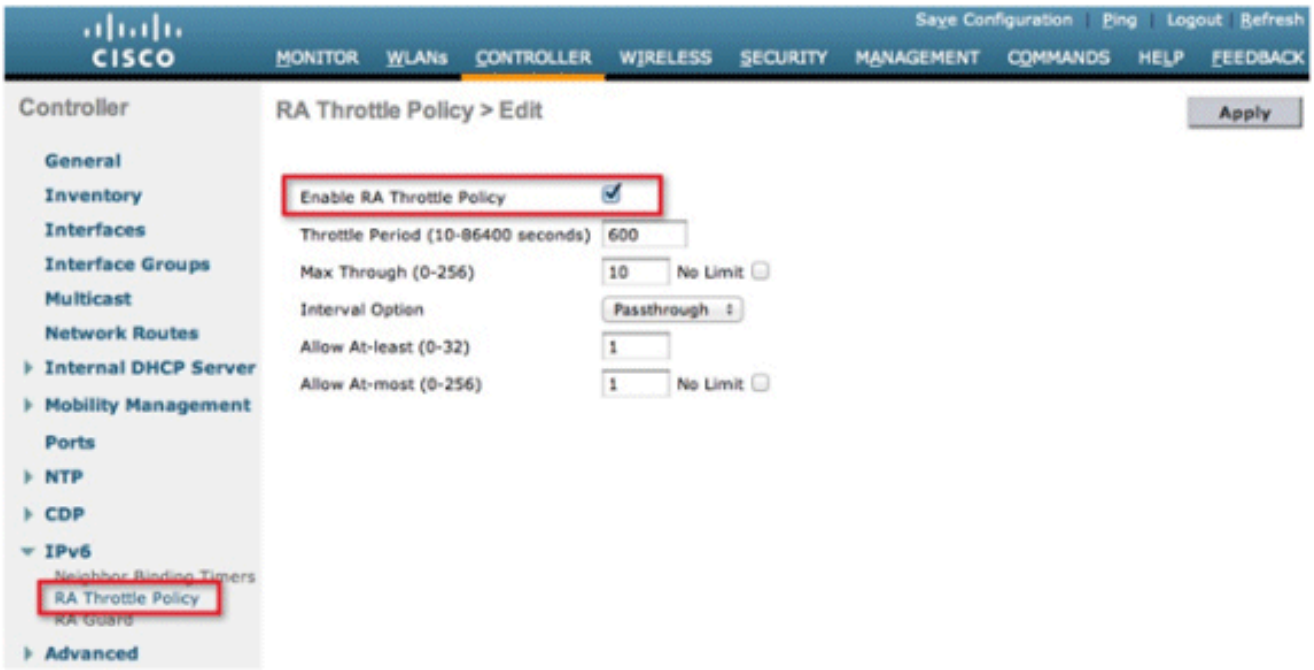
如需外部Web存取運作的詳細資訊，請參閱使用無線LAN控制器的外部Web驗證組態範例。

2. 瀏覽至頂部的WLANs索引標籤以設定訪客WLAN。建立訪客SSID並使用第3層Web策略。為IPv4和IPv6選擇步驟1中定義的預身份驗證ACL。檢查Over-ride Global Config部分，然後從Web Auth type下拉框中選擇**External**。輸入Web伺服器的URL。外部伺服器的主機名應在IPv4和IPv6 DNS中可解析。



配置IPv6 RA限制

1. 導覽至**Controller**頂級選單，然後按一下左側的**IPv6 > RA Throttle Policy**選項。通過按一下覈取方塊啟用RA限制。



注意：發生RA限制時，只允許第一個支援IPv6的路由器通過。對於具有不同路由器提供多個IPv6字首的網路，應禁用RA限制。

2. 僅在TAC的建議下調整限制時段和其他選項。但是，對於大多數部署，建議使用預設值。請牢記，調整RA限制策略的各種配置選項：「至少允許」的數值應小於「最多允許」，該數值應小於「最大通過」。RA限制策略不應使用超過1800秒的限制週期，因為這是大多數RA的預設生存時間。

每個RA限制選項說明如下：

- Throttle Period — 發生調節的時間段。RA限制僅在達到VLAN的「最大通過」限制後生效。
- Max Through — 這是開始限制之前每個VLAN的最大RA數。「無限制」選項允許無限制數量的RA通過，無限制。
- Interval選項 — interval選項允許控制器根據IPv6 RA中設定的RFC 3775值執行不同的操作。Passthrough — 此值允許具有RFC3775間隔選項的任何RA順利通過，而不會進行限制。Ignore — 該值將導致RA扼殺器將具有interval選項的資料包視為常規RA，並在有效的情況下進行扼殺。Throttle — 該值將導致帶間隔選項的RA始終受速率限制。
- Allow至少 — 每台路由器將以組播形式傳送的最小RA數。
- Allow At-maximum — 在限制生效之前作為組播傳送的每個路由器的最大RA數。「無限制」選項將允許該路由器無限數量的RA。

配置IPv6鄰居繫結表

1. 轉到控制器頂級選單，然後按一下左側選單上的**IPv6 > Neighbor Binding Timers**。

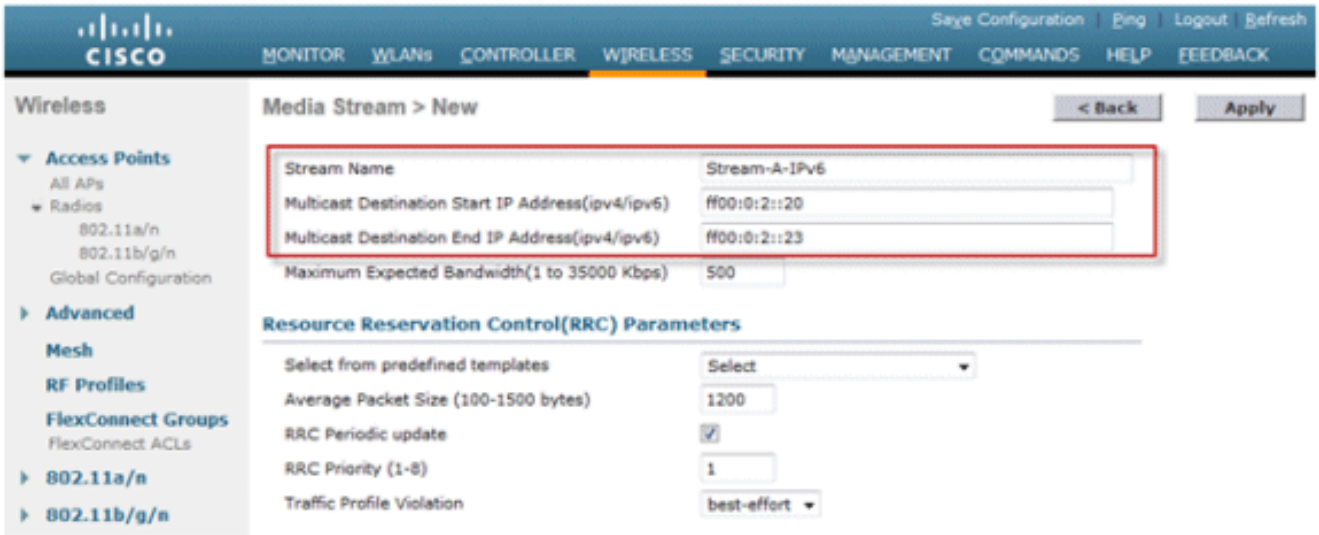
2. 根據需要調整Down Lifetime、Reachable Lifetime和Stale Lifetime。對於具有高度移動性客戶端的部署，應調整過時地址計時器的計時器。建議的值為：Down Lifetime - 30秒可達生存時

間 — 300秒狀態生存時間 — 86400秒每個生存期計時器都表示IPv6地址可以處於以下狀態：**Down Lifetime** — 關閉計時器指定如果控制器的上行鏈路介面關閉，應保留IPv6快取條目的時間。**Reachable Lifetime** — 此計時器指定IPv6地址將被標籤為活動狀態的時間長度，這意味著最近從該地址接收了流量。此計時器到期後，地址將移至「過時」狀態。**Stale Lifetime** — 此計時器指定將IPv6地址保留在「可訪問生存期」內未發現的快取中的時間。在此生存期之後，該地址將從繫結表中刪除。

配置IPv6影片流

1. 確保在控制器上啟用全域性VideoStream功能。有關在802.11a/g/n網路以及WLAN SSID上啟用VideoStream的資訊，請參閱思科統一無線網路解決方案：VideoStream部署指南。
2. 前往控制器上的**Wireless**索引標籤，並在左側選單中選擇**Media Stream > Streams**。按一下「**Add New**」以建立一個新流。

3. 命名資料流並輸入起始和結束IPv6地址。當僅使用單個流時，起始地址和結束地址相同。新增地址後，按一下**Apply**以建立流。



排除IPv6客戶端連線故障

某些客戶端無法傳遞IPv6流量

某些客戶端IPv6網路堆疊實現在進入網路時無法正確通告自己，因此控制器不會適當地偵聽其地址以將其置於鄰居繫結表中。根據IPv6源防護功能，會阻止鄰居繫結表中不存在的任何地址。若要允許這些使用者端傳遞流量，需要設定以下選項：

1. 通過CLI禁用IPv6源防護功能：

   config network ip-mac-binding disable

2. 通過CLI啟用組播鄰居請求轉發：

   config ipv6 ns-mcast-fwd enable

驗證IPv6客戶端的第3層漫遊是否成功：

在錨點和外部控制器上發出以下debug命令：

debug client

debug mobility handoff enable

debug mobility packet enable

錨點控制器上的調試結果：

```
00:21:6a:a7:4f:ee 0.0.0.0 RUN (20) State Update from Mobility-Complete to
  Mobility-Incomplete
00:21:6a:a7:4f:ee 0.0.0.0 RUN (20) Setting handles to 0x00000000
00:21:6a:a7:4f:ee pemApfDeleteMobileStation2: APF_MS_PEM_WAIT_L2_AUTH_COMPLETE =
  0.
00:21:6a:a7:4f:ee 0.0.0.0 RUN (20) Deleted mobile LWAPP rule on AP
  [04:fe:7f:49:03:30]
00:21:6a:a7:4f:ee Updated location for station old AP 04:fe:7f:49:03:30-1, new
  AP 00:00:00:00:00:00-0
00:21:6a:a7:4f:ee Stopping deletion of Mobile Station: (callerId: 42)
00:21:6a:a7:4f:ee 0.0.0.0 RUN (20) State Update from Mobility-Incomplete to
  Mobility-Complete, mobility role=Anchor, client state=APF_MS_STATE_ASSOCIATED
00:21:6a:a7:4f:ee 0.0.0.0 RUN (20) Change state to RUN (20) last state RUN (20)
00:21:6a:a7:4f:ee 0.0.0.0 RUN (20) Reached PLUMBFASTPATH: from line 4968
00:21:6a:a7:4f:ee 0.0.0.0 RUN (20) Adding Fast Path rule type = Airespace AP
  Client on AP 00:00:00:00:00:00, slot 0, interface = 13, QOS = 0
  IPv4 ACL ID = 255, IPv6 ACL ID = 255,
00:21:6a:a7:4f:ee 0.0.0.0 RUN (20) Fast Path rule (contd...) 802.1P = 0, DSCP =
  0, TokenID = 7006  Local Bridging Vlan = 20, Local Bridging intf id = 13
00:21:6a:a7:4f:ee 0.0.0.0 RUN (20) Successfully plumbed mobile rule (IPv4 ACL ID
  255, IPv6 ACL ID 255)
00:21:6a:a7:4f:ee 0.0.0.0 Removed NPU entry.
00:21:6a:a7:4f:ee Set symmetric mobility tunnel for 00:21:6a:a7:4f:ee as in
  Anchor role
00:21:6a:a7:4f:ee 0.0.0.0 Added NPU entry of type 1, dtlFlags 0x1
00:21:6a:a7:4f:ee Pushing IPv6: fe80:0000:0000:0000: 3057:534d:587d:73ae , and
```

```
  MAC: 00:21:6A:A7:4F:EE , Binding to Data Plane. SUCCESS !!
00:21:6a:a7:4f:ee Pushing IPv6: 2001:0db8:0000:0020: 3057:534d:587d:73ae , and
  MAC: 00:21:6A:A7:4F:EE , Binding to Data Plane. SUCCESS !!
00:21:6a:a7:4f:ee 0.0.0.0, VLAN Id 20 Not sending gratuitous ARP
00:21:6a:a7:4f:ee Copy AP LOCP - mode:0 slotId:0, apMac 0x0:0:0:0:0:0
00:21:6a:a7:4f:ee Copy WLAN LOCP EssIndex:3 aid:0 ssid:    Roam
00:21:6a:a7:4f:ee Copy Security LOCP ecypher:0x0 ptype:0x2, p:0x0, eaptype:0x6
  w:0x1 aalg:0x0, PMState:        RUN
00:21:6a:a7:4f:ee Copy 802.11 LOCP a:0x0 b:0x0 c:0x0 d:0x0 e:0x0 protocol2:0x5
  statuscode 0, reasoncode 99, status 3
00:21:6a:a7:4f:ee Copy CCX LOCP 4
00:21:6a:a7:4f:ee Copy e2e LOCP 0x1
00:21:6a:a7:4f:ee Copy MobilityData LOCP status:2, anchorip:0xac14e2c6
00:21:6a:a7:4f:ee Copy IPv6 LOCP: fe80::3057:534d:587d:73ae
```

外部控制器上的調試結果：

```
00:21:6a:a7:4f:ee Adding mobile on LWAPP AP f0:25:72:3c:0f:20(1)
00:21:6a:a7:4f:ee Reassociation received from mobile on AP f0:25:72:3c:0f:20
00:21:6a:a7:4f:ee 0.0.0.0 START (0) Changing IPv4 ACL 'none' (ACL ID 255) ===>
  'none' (ACL ID 255) --- (caller apf_policy.c:1697)
00:21:6a:a7:4f:ee 0.0.0.0 START (0) Changing IPv6 ACL 'none' (ACL ID 255) ===>
  'none' (ACL ID 255) --- (caller apf_policy.c:1864)
00:21:6a:a7:4f:ee Applying site-specific Local Bridging override for station
  00:21:6a:a7:4f:ee - vapId 3, site 'default-group', interface 'client-b1'
00:21:6a:a7:4f:ee Applying Local Bridging Interface Policy for station
  00:21:6a:a7:4f:ee - vlan 25, interface id 12, interface 'client-b1'
00:21:6a:a7:4f:ee processSsidIE  statusCode is 0 and status is 0
00:21:6a:a7:4f:ee processSsidIE  ssid_done_flag is 0 finish_flag is 0
00:21:6a:a7:4f:ee STA - rates (8): 140 18 152 36 176 72 96 108 0 0 0 0 0 0 0 0
*apfMsConnTask_4: Jan 22 20:37:45.370: 00:21:6a:a7:4f:ee suppRates  statusCode
  is 0 and gotSuppRatesElement is 1
00:21:6a:a7:4f:ee Processing RSN IE type 48, length 22 for mobile
  00:21:6a:a7:4f:ee
00:21:6a:a7:4f:ee 0.0.0.0 START (0) Initializing policy
00:21:6a:a7:4f:ee 0.0.0.0 START (0) Change state to AUTHCHECK (2) last state
  AUTHCHECK (2)
00:21:6a:a7:4f:ee 0.0.0.0 AUTHCHECK (2) Change state to 8021X_REQD (3) last
  state 8021X_REQD (3)
00:21:6a:a7:4f:ee 0.0.0.0 8021X_REQD (3) DHCP Not required on AP
  f0:25:72:3c:0f:20 vapId 3 apVapId 3for this client
00:21:6a:a7:4f:ee Not Using WMM Compliance code qosCap 00
00:21:6a:a7:4f:ee 0.0.0.0 8021X_REQD (3) Plumbed mobile LWAPP rule on AP
  f0:25:72:3c:0f:20 vapId 3 apVapId 3
00:21:6a:a7:4f:ee apfMsAssoStateInc
00:21:6a:a7:4f:ee apfPemAddUser2 (apf_policy.c:268) Changing state for mobile
  00:21:6a:a7:4f:ee on AP f0:25:72:3c:0f:20 from Idle to Associated
00:21:6a:a7:4f:ee Scheduling deletion of Mobile Station:  (callerId: 49) in 1800
  seconds
00:21:6a:a7:4f:ee Sending Assoc Response to station on BSSID f0:25:72:3c:0f:20
  (status 0) ApVapId 3 Slot 1
00:21:6a:a7:4f:ee apfProcessAssocReq (apf_80211.c:6290) Changing state for
  mobile 00:21:6a:a7:4f:ee on AP f0:25:72:3c:0f:20 from Associated to Associated
<…SNIP…>
00:21:6a:a7:4f:ee 0.0.0.0 8021X_REQD (3) Change state to L2AUTHCOMPLETE (4) last
  state L2AUTHCOMPLETE (4)
00:21:6a:a7:4f:ee 0.0.0.0 L2AUTHCOMPLETE (4) DHCP Not required on AP
  f0:25:72:3c:0f:20 vapId 3 apVapId 3for this client
00:21:6a:a7:4f:ee Not Using WMM Compliance code qosCap 00
00:21:6a:a7:4f:ee 0.0.0.0 L2AUTHCOMPLETE (4) Plumbed mobile LWAPP rule on AP
  f0:25:72:3c:0f:20 vapId 3 apVapId 3
00:21:6a:a7:4f:ee 0.0.0.0 L2AUTHCOMPLETE (4) Change state to DHCP_REQD (7) last
```

```
  state DHCP_REQD (7)
00:21:6a:a7:4f:ee 0.0.0.0 DHCP_REQD (7) pemAdvanceState2 5253, Adding TMP rule
00:21:6a:a7:4f:ee 0.0.0.0 DHCP_REQD (7) Adding Fast Path rule
  type = Airespace AP - Learn IP address
  on AP f0:25:72:3c:0f:20, slot 1, interface = 13, QOS = 0
  IPv4 ACL ID = 255, IP
00:21:6a:a7:4f:ee 0.0.0.0 DHCP_REQD (7) Fast Path rule (contd...) 802.1P = 0,
  DSCP = 0, TokenID = 7006  Local Bridging Vlan = 25, Local Bridging intf id =
  12
00:21:6a:a7:4f:ee 0.0.0.0 DHCP_REQD (7) Successfully plumbed mobile rule (IPv4
  ACL ID 255, IPv6 ACL ID 255)
00:21:6a:a7:4f:ee Stopping retransmission timer for mobile 00:21:6a:a7:4f:ee
00:21:6a:a7:4f:ee 0.0.0.0 Added NPU entry of type 9, dtlFlags 0x0
00:21:6a:a7:4f:ee Sent an XID frame
00:21:6a:a7:4f:ee Username entry () already exists in name table, length = 253
00:21:6a:a7:4f:ee Username entry () created in mscb for mobile, length = 253
00:21:6a:a7:4f:ee Applying post-handoff policy for station 00:21:6a:a7:4f:ee -
  valid mask 0x1000
00:21:6a:a7:4f:ee QOS Level: -1, DSCP: -1, dot1p: -1, Data Avg: -1, realtime
  Avg: -1, Data Burst -1, Realtime Burst -1
00:21:6a:a7:4f:ee     Session: -1, User session: -1, User elapsed -1 Interface:
  N/A, IPv4 ACL: N/A, IPv6 ACL:
00:21:6a:a7:4f:ee 0.0.0.0 DHCP_REQD (7) Change state to DHCP_REQD (7) last state
  DHCP_REQD (7)
00:21:6a:a7:4f:ee 0.0.0.0 DHCP_REQD (7) pemCreateMobilityState 6370, Adding TMP
  rule
00:21:6a:a7:4f:ee 0.0.0.0 DHCP_REQD (7) Replacing Fast Path rule type =
  Airespace AP - Learn IP address on AP f0:25:72:3c:0f:20, slot 1, interface =
  13, QOS = 0 IPv4 ACL ID = 255,
00:21:6a:a7:4f:ee 0.0.0.0 DHCP_REQD (7) Fast Path rule (contd...) 802.1P = 0,
  DSCP = 0, TokenID = 7006  Local Bridging Vlan = 25, Local Bridging intf id =
  12
00:21:6a:a7:4f:ee 0.0.0.0 DHCP_REQD (7) Successfully plumbed mobile rule (IPv4
  ACL ID 255, IPv6 ACL ID 255)
00:21:6a:a7:4f:ee Scheduling deletion of Mobile Station:  (callerId: 55) in 1800
  seconds
00:21:6a:a7:4f:ee Pushing IPv6: fe80:0000:0000:0000: 3057:534d:587d:73ae , and
  MAC: 00:21:6A:A7:4F:EE , Binding to Data Plane. SUCCESS !!
00:21:6a:a7:4f:ee apfMsRunStateInc
00:21:6a:a7:4f:ee 0.0.0.0 DHCP_REQD (7) Change state to RUN (20) last state RUN
  (20)
00:21:6a:a7:4f:ee 0.0.0.0 RUN (20) Reached PLUMBFASTPATH: from line 5776
00:21:6a:a7:4f:ee 0.0.0.0 RUN (20) Change state to RUN (20) last state RUN (20)
00:21:6a:a7:4f:ee Pushing IPv6: 2001:0db8:0000:0020: 3057:534d:587d:73ae , and
  MAC: 00:21:6A:A7:4F:EE , Binding to Data Plane. SUCCESS !!
00:21:6a:a7:4f:ee 0.0.0.0 RUN (20) State Update from Mobility-Incomplete to
  Mobility-Complete, mobility role=Foreign, client state=APF_MS_STATE_ASSOCIATED
00:21:6a:a7:4f:ee 0.0.0.0 RUN (20) Change state to RUN (20) last state RUN (20)
00:21:6a:a7:4f:ee 0.0.0.0 RUN (20) Reached PLUMBFASTPATH: from line 4968
00:21:6a:a7:4f:ee 0.0.0.0 RUN (20) Replacing Fast Path rule
  type = Airespace AP Client
  on AP f0:25:72:3c:0f:20, slot 1, interface = 13, QOS = 0
  IPv4 ACL ID = 255, IPv6 ACL ID = 25
00:21:6a:a7:4f:ee 0.0.0.0 RUN (20) Fast Path rule (contd...) 802.1P = 0, DSCP =
  0, TokenID = 7006  Local Bridging Vlan = 25, Local Bridging intf id = 12
00:21:6a:a7:4f:ee 0.0.0.0 RUN (20) Successfully plumbed mobile rule (IPv4 ACL ID
  255, IPv6 ACL ID 255)
00:21:6a:a7:4f:ee 0.0.0.0 Added NPU entry of type 9, dtlFlags 0x0
00:21:6a:a7:4f:ee Set symmetric mobility tunnel for 00:21:6a:a7:4f:ee as in
  Foreign role
00:21:6a:a7:4f:ee 0.0.0.0 Added NPU entry of type 1, dtlFlags 0x1
00:21:6a:a7:4f:ee Pushing IPv6: fe80:0000:0000:0000: 3057:534d:587d:73ae , and
  MAC: 00:21:6A:A7:4F:EE , Binding to Data Plane. SUCCESS !!
00:21:6a:a7:4f:ee Pushing IPv6: 2001:0db8:0000:0020: 3057:534d:587d:73ae , and
```

```
  MAC: 00:21:6A:A7:4F:EE , Binding to Data Plane. SUCCESS !!
00:21:6a:a7:4f:ee Copy AP LOCP - mode:0 slotId:1, apMac 0xf0:25:72:3c:f:20
00:21:6a:a7:4f:ee Copy WLAN LOCP EssIndex:3 aid:1 ssid:    Roam
00:21:6a:a7:4f:ee Copy Security LOCP ecypher:0x0 ptype:0x2, p:0x0, eaptype:0x6
  w:0x1 aalg:0x0, PMState:        RUN
00:21:6a:a7:4f:ee Copy 802.11 LOCP a:0x0 b:0x0 c:0x0 d:0x0 e:0x0 protocol2:0x7
  statuscode 0, reasoncode 99, status 3
00:21:6a:a7:4f:ee Copy CCX LOCP 4
00:21:6a:a7:4f:ee Copy e2e LOCP 0x1
00:21:6a:a7:4f:ee Copy MobilityData LOCP status:3, anchorip:0xac14e2c5
00:21:6a:a7:4f:ee Copy IPv6 LOCP: fe80::3057:534d:587d:73ae
00:21:6a:a7:4f:ee Copy IPv6 LOCP: 2001:db8:0:20:3057:534d:587d:73ae
```

有用的IPv6 CLI命令：

Show ipv6 neighbor-binding summary

Debug ipv6 neighbor-binding filter client enable

Debug ipv6 neighbor-binding filter errors enable

常見問題

問：限制廣播域的最佳IPv6字首大小是多少？

答：雖然IPv6子網可以細分為小於/64的子網，但此配置將中斷SLAAC並引起客戶端連線問題。如果需要分段以減少主機數量，可以使用介面組功能在不同後端VLAN之間負載均衡客戶端，每個後端VLAN使用不同的IPv6字首。

問：在支援IPv6客戶端方面是否存在可擴充性限制？

答：IPv6客戶端支援的主要可擴充性限制是跟蹤所有無線客戶端IPv6地址的鄰居繫結表。此表按控制器平台進行縮放，以便支援最大客戶端數乘以八（每個客戶端的最大地址數）。新增IPv6繫結表可使控制器在全負載下的記憶體使用率提高大約10-15%，具體取決於平台。

無線控制器	最大客戶端數量	IPv6鄰居繫結表大小
2500	500	4,000
5500	7,000	56,000
WiSM2	15,000	120,000

問：IPv6功能對控制器的CPU和內存有何影響？

答：由於CPU擁有多個處理控制平面的核心，因此影響最小。當測試支援的最大客戶端數（每個客戶端有8個IPv6地址）時，CPU使用率低於30%，記憶體使用率低於75%。

問：是否可以禁用IPv6客戶端支援？

答：對於希望在其網路中僅啟用IPv4並阻止IPv6的客戶，可以在每個WLAN上使用和應用拒絕所有流量的IPv6 ACL。

問：是否可能有一個用於IPv4的WLAN和一個用於IPv6的WLAN?

答：對於在同一AP上運行的兩個不同的WLAN，不能使用相同的SSID名稱和安全型別。要將IPv4客戶端與IPv6客戶端進行分段，必須建立兩個WLAN。每個WLAN必須配置一個分別阻止所有IPv4或IPv6流量的ACL。

問：為什麼每個客戶端支援多個IPv6地址非常重要？

答：客戶端可以每個介面具有多個IPv6地址，這些地址可以是靜態的、SLAAC或DHCPv6分配的，而且始終具有自行分配的本地鏈路地址。客戶端還可以使用其他IPv6字首來獲得其他地址。

問：什麼是IPv6私有地址？為什麼這些地址對跟蹤很重要？

A:使用SLAAC地址分配時，客戶端隨機生成私有（也稱為臨時）地址。這些地址通常以一天左右的頻率旋轉，以防止主機可跟蹤性因為始終使用同一主機字尾（最後64位）而產生。跟蹤這些私有地址對於跟蹤版權侵權等審計用途非常重要。Cisco NCS記錄每個客戶端使用的所有IPv6地址，並在每次客戶端漫遊或建立新會話時記錄這些地址。這些記錄可以在NCS中配置為保留長達一年。

相關資訊

- 技術支援與文件 - Cisco Systems

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。