无线LAN IPv6客户端部署指南

目录

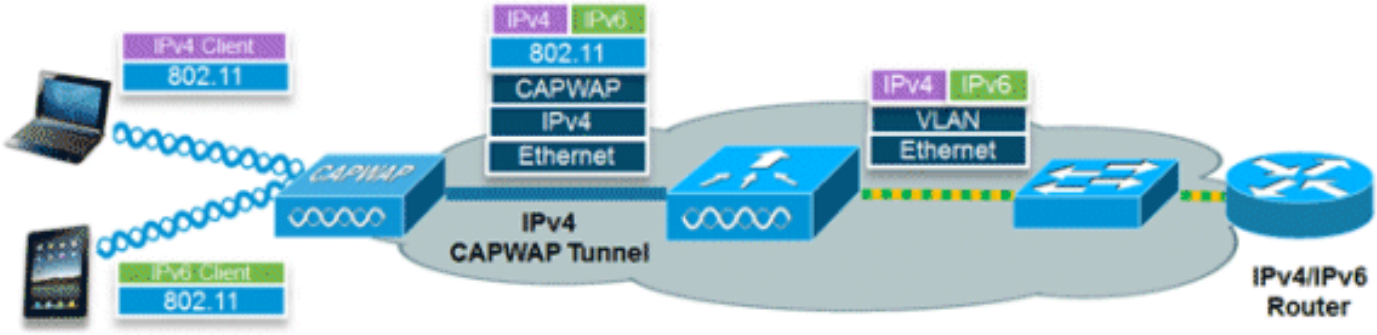
简介
先决条件
要求
使用的组件
规则
无线IPv6客户端连接的必备条件
SLAAC地址分配
DHCPv6地址分配
其他信息
IPv6客户端移动性
支持VLAN选择（接口组）
IPv6客户端的第一跳安全
路由器通告保护
DHCPv6服务器防护
IPv6源保护
IPv6地址记帐
IPv6访问控制列表
针对IPv6客户端的数据包优化
邻居发现缓存
路由器通告限制
IPv6访客访问
IPv6视频流
IPv6服务质量
IPv6和FlexConnect
FlexConnect — 本地交换WLAN
FlexConnect — 中央交换WLAN
NCS的IPv6客户端可视性
IPv6控制面板项目
监控IPv6客户端
无线IPv6客户端支持的配置
到AP的组播分布模式
配置IPv6移动性
配置IPv6组播
配置IPv6 RA防护
配置IPv6访问控制列表
为外部Web身份验证配置IPv6访客接入
配置IPv6 RA限制
配置IPv6邻居绑定表
配置IPv6 VideoFlow
排除IPv6客户端连接故障

[某些客户端无法传递IPv6流量](#)
[检验IPv6客户端的第3层漫游是否成功：](#)
[有用的IPv6 CLI命令：](#)
[常见问题解答](#)
[相关信息](#)

简介

本文档提供有关Cisco Unified Wireless LAN解决方案的操作和配置理论的信息，因为它涉及支持IPv6客户端。

IPv6无线客户端连接



Cisco Unified Wireless Network软件版本7.2中的IPv6功能集允许无线网络在同一无线网络上支持IPv4、双栈和仅IPv6客户端。将IPv6客户端支持添加到思科统一无线局域网的总体目标是维护IPv4和IPv6客户端之间的功能奇偶校验，包括移动性、安全性、访客接入、服务质量和终端可视性。

每台设备最多可跟踪八个IPv6客户端地址。这允许IPv6客户端具有本地链路、无状态地址自动配置(SLAAC)地址、IPv6动态主机配置协议(DHCPv6)地址，甚至备用前缀中的地址位于单个接口上。在WGB模式下连接到自主接入点(AP)上行链路的工作组网桥(WGB)客户端也可以支持IPv6。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 无线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系列网状AP
- 支持IPv6的路由器

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

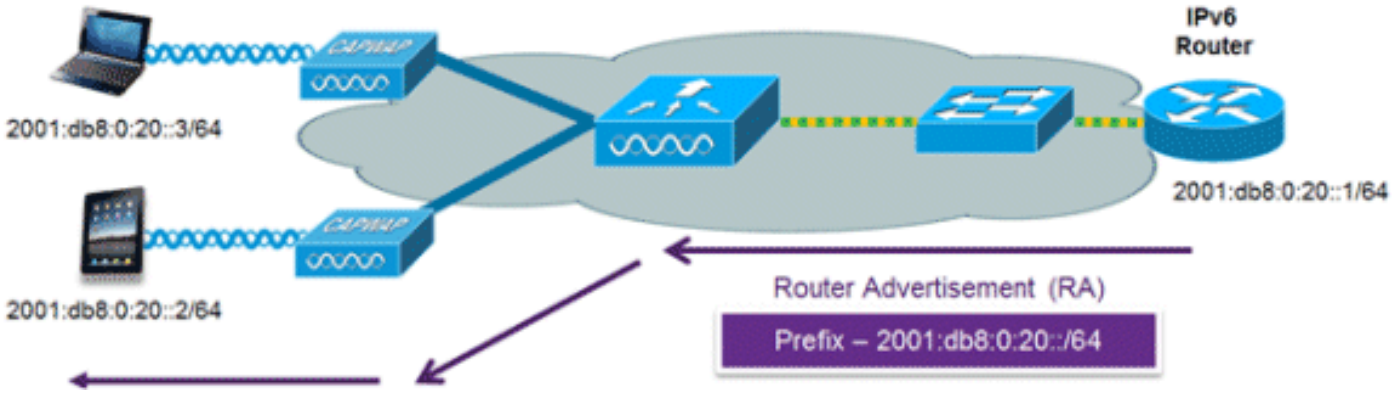
规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

无线IPv6客户端连接的必备条件

要启用无线IPv6客户端连接，底层有线网络必须支持IPv6路由和地址分配机制，例如SLAAC或DHCPv6。无线LAN控制器必须与IPv6路由器具有L2邻接关系，且数据包进入控制器时需要标记VLAN。AP不需要在IPv6网络上连接，因为所有流量都封装在AP和控制器之间的IPv4 CAPWAP隧道内。

SLAAC地址分配

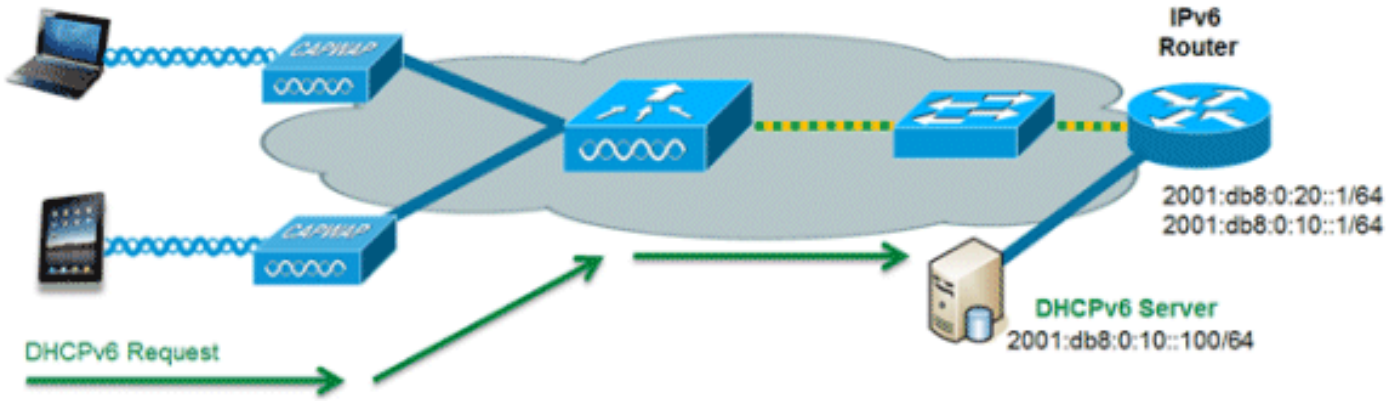


IPv6客户端地址分配的最常用方法是SLAAC。SLAAC提供简单的即插即用连接，客户端可根据IPv6前缀自行分配地址。当IPv6路由器定期发送路由器通告消息时，该消息会通知客户端正在使用的IPv6前缀（前64位）和IPv6默认网关。从这一点出发，客户端可以根据两种算法生成其IPv6地址的其余64位：基于接口MAC地址的EUI-64，或者随机生成的私有地址。算法的选择取决于客户端，并且通常是可配置的。重复地址检测由IPv6客户端执行，以确保选中的随机地址不会与其他客户端发生冲突。发送通告的路由器地址用作客户端的默认网关。

来自支持Cisco的IPv6路由器的以下Cisco IOS®配置命令用于启用SLAAC寻址和路由器通告：

```
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，则IPv6客户端连接不需要使用DHCPv6。DHCPv6有两种运行模式，分别称为无状态和有状态。

DHCPv6 Stateless模式用于为客户端提供路由器通告中不可用的其他网络信息，但不提供IPv6地址，因为SLAAC已提供该地址。此信息可包括DNS域名、DNS服务器和其他特定于DHCP供应商的选项。此接口配置适用于启用了SLAAC且实施无状态DHCPv6的Cisco IOS IPv6路由器：

```
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
```

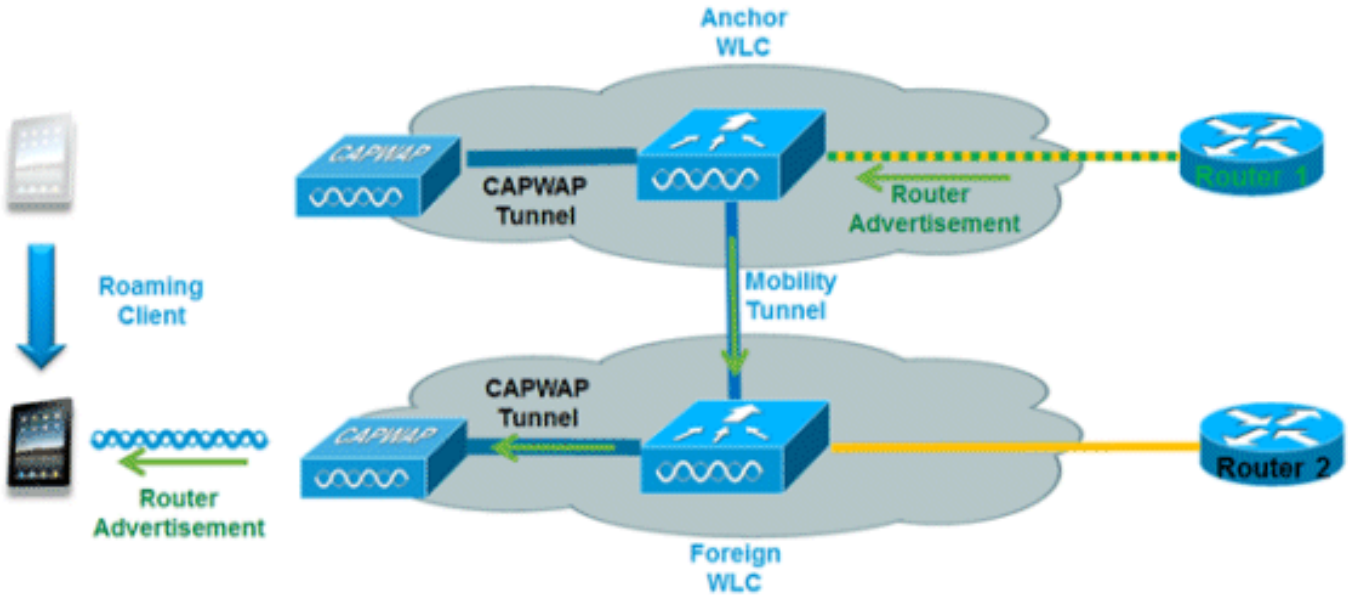
DHCPv6 Stateful选项（也称为管理模式）的操作类似于DHCPv4，因为它为每个客户端分配唯一的地址，而不是像SLAAC中那样为客户端生成地址的后64位。此接口配置适用于在禁用SLAAC的情况下实施有状态DHCPv6的Cisco IOS IPv6路由器：

```
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
```

其他信息

使用双堆栈或隧道连接方法配置有线网络以实现完整的IPv6园区范围连接不在本文档的讨论范围之内。有关详细信息，请参阅思科验证部署指南在园区网络中部署IPv6。

IPv6客户端移动性



为了处理控制器间的IPv6客户端漫游，必须专门处理ICMPv6消息，如邻居请求(NS)、邻居通告(NA)、路由器通告(RA)和路由器请求(RS)，以确保客户端保持在同一第3层网络上。IPv6移动性的配置与IPv4移动性的配置相同，并且客户端不需要单独的软件来实现无缝漫游。唯一需要的配置是控制器必须属于同一个移动组/域。

以下是控制器间IPv6客户端移动性的流程：

1. 如果两个控制器都有权访问客户端最初所在的同一VLAN，则漫游只是第2层漫游事件，其中客户端记录被复制到新控制器，并且没有流量通过隧道传回锚点控制器。

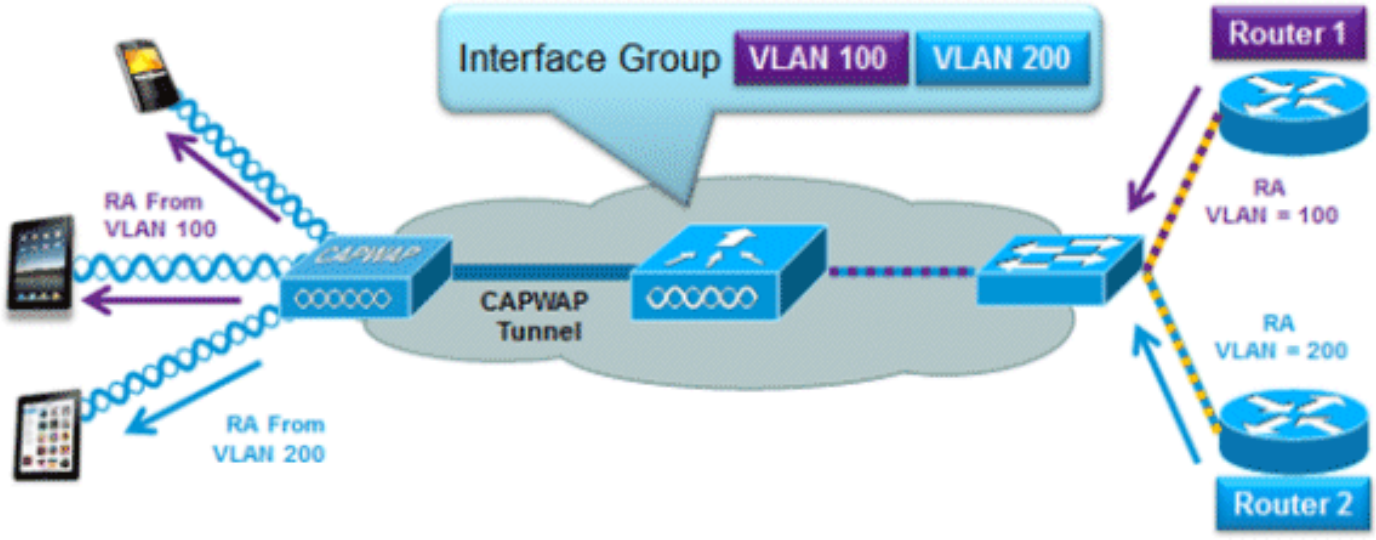
2. 如果第二个控制器无法访问客户端所在的原始VLAN，则会发生第3层漫游事件，这意味着所有来自客户端的流量必须通过移动隧道（IP以太网）传输到锚点控制器。

    a. 为了确保客户端保留其原始IPv6地址，锚点控制器会将来自原始VLAN的RA发送到外部控制器，然后使用来自AP的L2单播将其传送到客户端。

    b. 当漫游的客户端通过DHCPv6更新其地址或通过SLAAC生成新地址时，RS、NA和NS数据包将继续通过隧道传输到原始VLAN，因此客户端将收到适用于该VLAN的IPv6地址。

注意：仅IPv6客户端的移动性基于VLAN信息。这意味着无标记的VLAN不支持仅IPv6客户端移动。

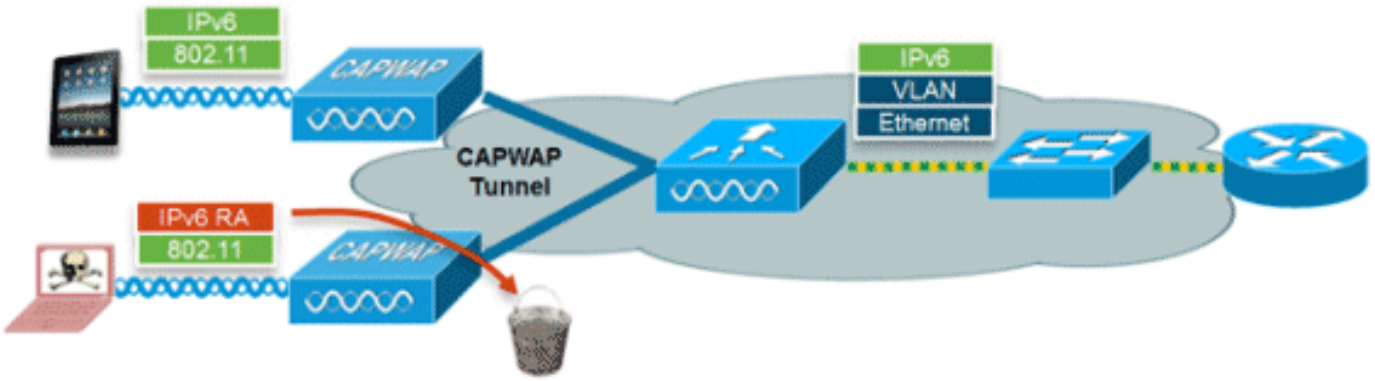
支持VLAN选择（接口组）



接口组功能允许组织使用单个WLAN在控制器上配置多个VLAN，以允许无线客户端在这些VLAN之间进行负载均衡。此功能通常用于使IPv4子网保持较小的规模，同时使WLAN能够跨组中的多个VLAN扩展到数千个用户。为了支持具有接口组的IPv6客户端，无需进行额外配置，因为系统通过L2无线单播自动将正确的RA发送到正确的客户端。通过单播RA，同一WLAN但不同VLAN上的客户端不会收到错误的RA。

IPv6客户端的第一跳安全

路由器通告保护



RA防护功能通过丢弃来自无线客户端的RA来提高IPv6网络的安全性。如果没有此功能，配置错误或恶意的IPv6客户端可能会将自己宣布为网络路由器，其优先级通常很高，可能优先于合法IPv6路由器。

默认情况下，RA防护在AP上启用（但在AP上可禁用），并且始终在控制器上启用。最好在AP上丢弃RA，因为这是一个更具可扩展性的解决方案，并提供增强的每客户端RA丢弃计数器。在所有情况下，IPv6 RA都将在某个点被丢弃，以保护其他无线客户端和上游有线网络免受恶意或配置错误的IPv6客户端的攻击。

DHCPv6服务器防护

DHCPv6 Server Guard功能可防止无线客户端将IPv6地址分配给上游的其他无线客户端或有线客户

端。为了防止分配DHCPv6地址，会丢弃来自无线客户端的任何DHCPv6通告数据包。此功能在控制器上运行，无需任何配置并自动启用。

IPv6源保护

IPv6源防护功能可防止无线客户端欺骗另一客户端的IPv6地址。此功能类似于IPv4源保护。IPv6源保护默认启用，但可以通过CLI禁用。

IPv6地址记帐

对于RADIUS身份验证和记帐，控制器使用“Framed-IP-address”属性发回一个IP地址。本例中使用IPv4地址。

当控制器上的“呼叫站ID类型”配置为“IP地址”时，“Calling-Station-ID”属性使用此算法来回发IP地址：

1. IPv4地址
2. 全局单播IPv6地址
3. 本地链路IPv6地址

由于客户端IPv6地址经常更改（临时或私有地址），因此随着时间的推移跟踪这些地址非常重要。思科NCS记录每个客户端使用的所有IPv6地址，并在每次客户端漫游或建立新会话时记录这些地址。这些记录可在NCS中配置，保留时间最长为一年。

注意：在版本7.2中，控制器上“呼叫站ID类型”的默认值已更改为“系统MAC地址”。升级时，应更改此值，以允许通过MAC地址对客户端进行唯一跟踪，因为IPv6地址可能会在会话期间发生更改，并且如果Calling-Station-ID设置为IP地址，则会导致记帐问题。

IPv6访问控制列表

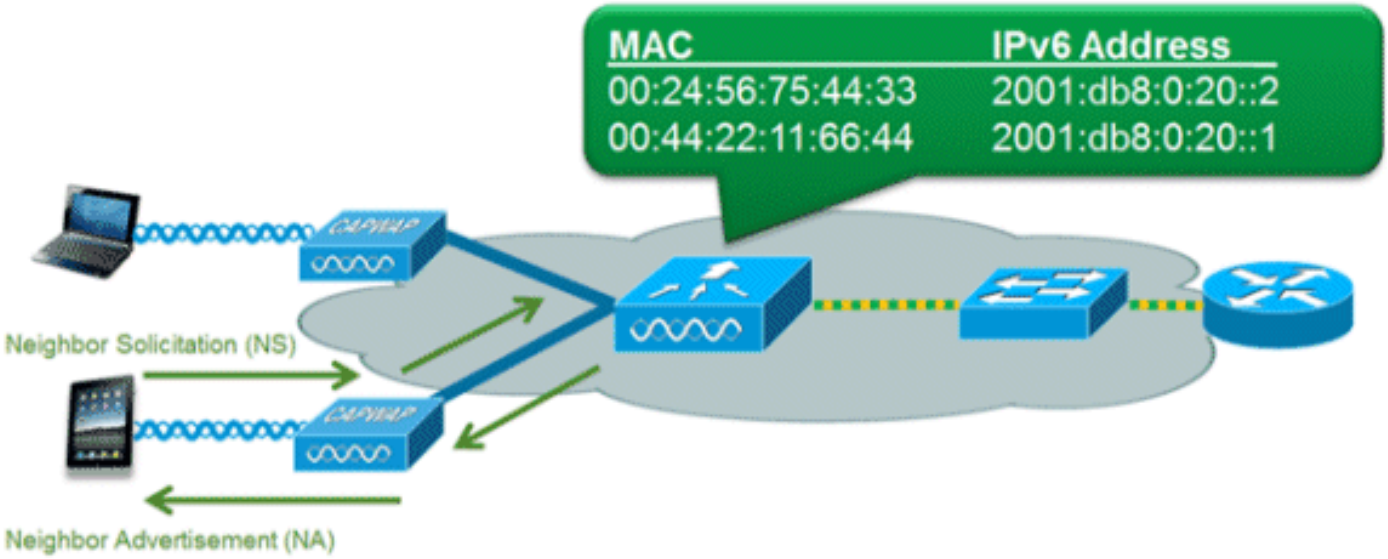
为了限制对某些上游有线资源的访问或阻止某些应用，可以使用IPv6访问控制列表(ACL)来识别流量并允许或拒绝该流量。IPv6 ACL支持与IPv4 ACL相同的选项，包括源、目标、源端口和目标端口（还支持端口范围）。还支持预身份验证ACL，以支持使用外部Web服务器的IPv6访客身份验证。无线控制器最多支持64个唯一IPv6 ACL，每个包含64个唯一规则。无线控制器继续支持64个唯一IPv4 ACL，每个中包含64个唯一规则，共128个ACL用于双堆栈客户端。

IPv6 ACL的AAA覆盖

为了通过集中式AAA服务器(如思科身份服务引擎(ISE)或ACS)支持集中式访问控制，可以使用AAA覆盖属性基于每个客户端调配IPv6 ACL。要使用此功能，必须在控制器上配置IPv6 ACL，并且必须在启用AAA覆盖功能的情况下配置WLAN。IPv6 ACL的实际命名AAA属性是Airespace-IPv6-ACL-Name，类似于用于调配基于IPv4的ACL的Airespace-ACL-Name属性。返回的AAA属性内容应该是一个字符串，该字符串等于控制器上配置的IPv6 ACL的名称。

针对IPv6客户端的数据包优化

邻居发现缓存



IPv6邻居发现协议(NDP)使用NA和NS数据包代替地址解析协议(ARP)，以允许IPv6客户端解析网络上其他客户端的MAC地址。NDP进程可能非常不稳定，因为它最初使用组播地址来执行地址解析；这会消耗宝贵的无线通话时间，因为组播数据包会发送到网段上的所有客户端。

为了提高NDP进程的效率，邻居发现缓存允许控制器充当代理，并响应它可以解决的NS查询。邻居发现缓存可通过控制器中的底层邻居绑定表实现。邻居绑定表会跟踪每个IPv6地址及其关联的MAC地址。当IPv6客户端尝试解析另一个客户端的链路层地址时，控制器会截取NS数据包，然后用NA数据包进行响应。

路由器通告限制

路由器通告限制允许控制器对朝向无线网络的RA实施速率限制。通过启用RA限制，配置为经常发送RA的路由器（例如每三秒）可以调整回最小频率，这样仍然可以保持IPv6客户端连接。这样可以通过减少必须发送的组播数据包数来优化通话时间。在所有情况下，如果客户端发送RS，则允许RA通过控制器并单播到请求客户端。这是为了确保新客户端或漫游客户端不会受到RA限制的不利影响。

IPv6访客访问

IPv4客户端的无线和有线访客功能与双堆栈和仅IPv6客户端的工作方式相同。访客用户关联后，它们将处于“WEB_AUTH_REQ”运行状态，直到客户端通过IPv4或IPv6强制网络门户进行身份验证。控制器将在此状态下拦截IPv4和IPv6 HTTP/HTTPS流量并将其重定向到控制器的虚拟IP地址。一旦通过强制网络门户对用户进行身份验证，其MAC地址将移至运行状态，IPv4和IPv6流量都允许通过。对于外部Web身份验证，预身份验证ACL允许使用外部Web服务器。

为支持仅IPv6客户端的重定向，控制器根据控制器上配置的IPv4虚拟地址自动创建IPv6虚拟地址。虚拟IPv6地址遵循`[::ffff:<virtual IPv4 address>]`约定。例如，虚拟IP地址1.1.1.1将转换为`[::ffff:1.1.1.1]`。

使用受信任SSL证书进行访客访问身份验证时，请确保在DNS中定义控制器的IPv4和IPv6虚拟地址

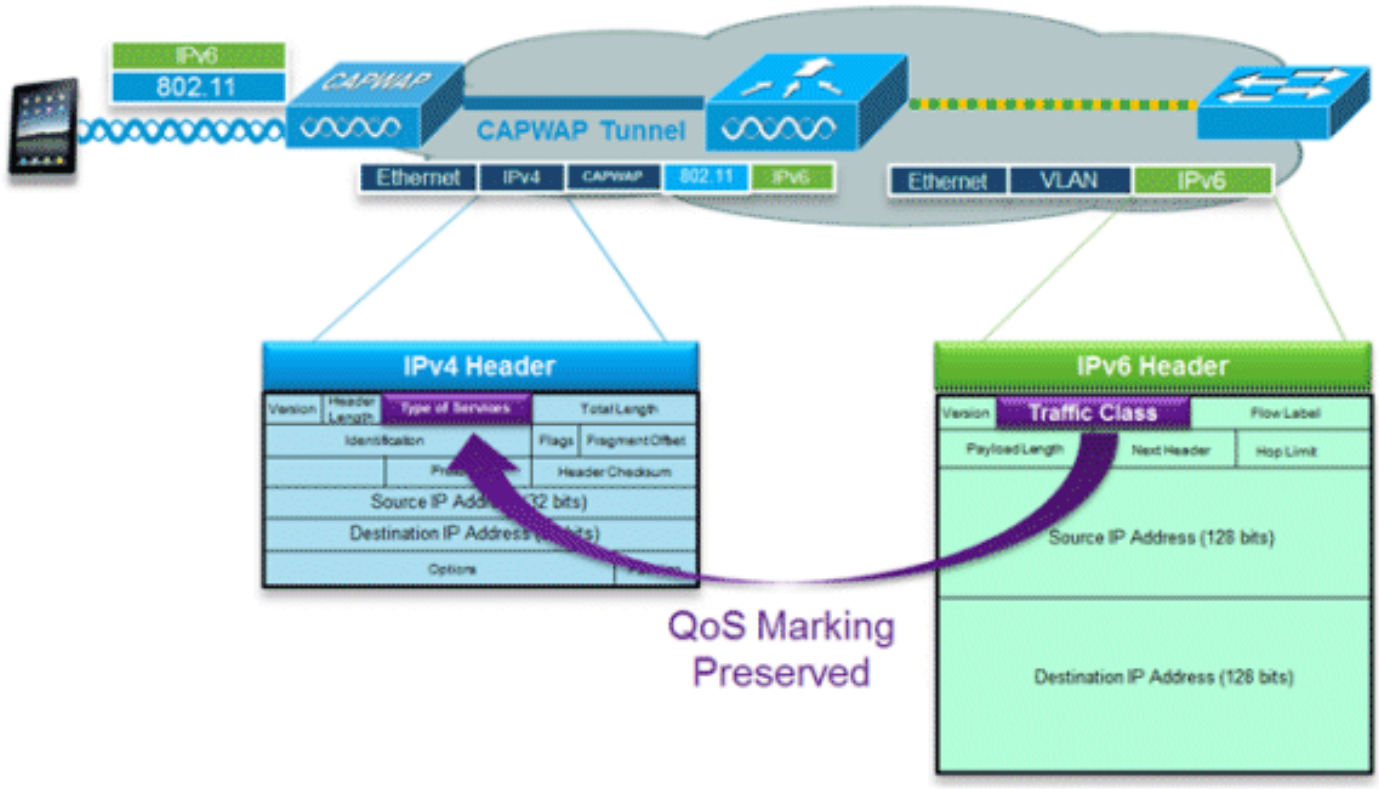
以匹配SSL证书主机名。这可确保客户端不会收到安全警告，说明证书与设备的主机名不匹配。

注意：控制器的自动生成的SSL证书不包含IPv6虚拟地址。这可能会导致某些Web浏览器显示安全警告。建议使用受信任SSL证书进行访客访问。

IPv6视频流

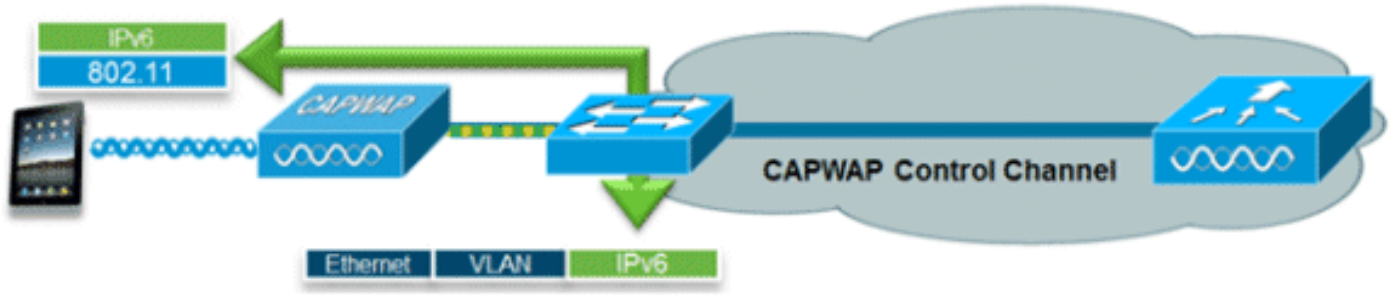
VideoStream支持可靠且可扩展的无线组播视频传输，以单播格式向每个客户端发送流。实际组播到单播(L2)的转换发生在AP，提供可扩展的解决方案。控制器在IPv4 CAPWAP组播隧道内发送IPv6视频流量，该隧道允许向AP进行有效的网络分配。

IPv6服务质量



IPv6数据包使用类似于IPv4的DSCP值标记，支持多达64个不同的流量类(0-63)。对于来自有线网络的下游数据包，IPv6 Traffic Class值会复制到CAPWAP隧道的报头中，以确保端到端保留QoS。在上游方向，同样发生的情况是，在第3层标记有IPv6流量类的客户端流量将通过标记发往控制器的CAPWAP数据包来执行。

IPv6和FlexConnect



FlexConnect — 本地交换WLAN

本地交换模式中的FlexConnect通过桥接流量到本地VLAN来支持IPv6客户端，类似于IPv4操作。跨FlexConnect组的第2层漫游支持客户端移动性。

FlexConnect本地交换模式支持以下特定于IPv6的功能：

- IPv6 RA防护
- IPv6桥接
- IPv6访客身份验证（控制器托管）

FlexConnect本地交换模式不支持以下特定于IPv6的功能：

- 第3层移动性
- IPv6视频流
- IPv6访问控制列表
- IPv6源保护
- DHCPv6服务器防护
- 邻居发现缓存
- 路由器通告限制

FlexConnect — 中央交换WLAN

对于使用中央交换的FlexConnect模式下的AP（将流量通过隧道传回控制器），对于“AP组播模式”，必须将控制器设置为“组播 — 单播模式”。由于FlexConnect AP不加入控制器的CAPWAP组播组，因此必须在控制器上复制组播数据包并单播到每个AP。此方法比“组播 — 组播模式”效率低，并且会在控制器上增加负载。

FlexConnect中央交换模式不支持此特定于IPv6的功能：

- IPv6视频流

注意：Flex 7500系列控制器不支持运行IPv6的集中交换WLAN。

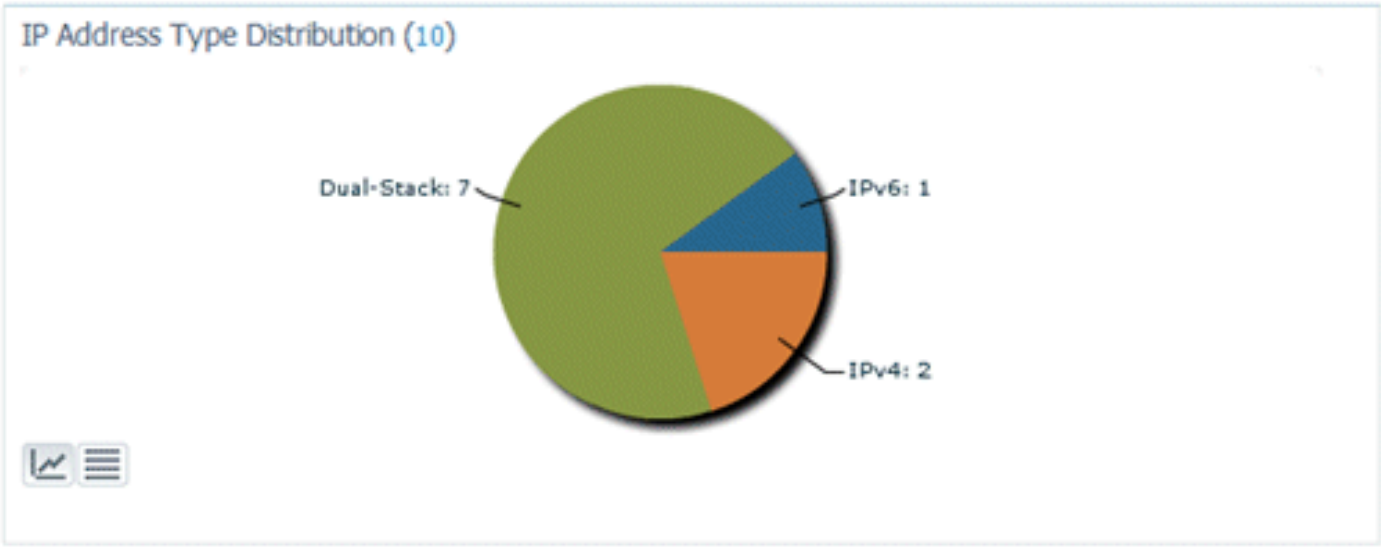
NCS的IPv6客户端可视性

随着NCS v1.1的发布，增加了许多额外的IPv6特定功能，以监控和管理有线和无线网络上的IPv6客户端网络。

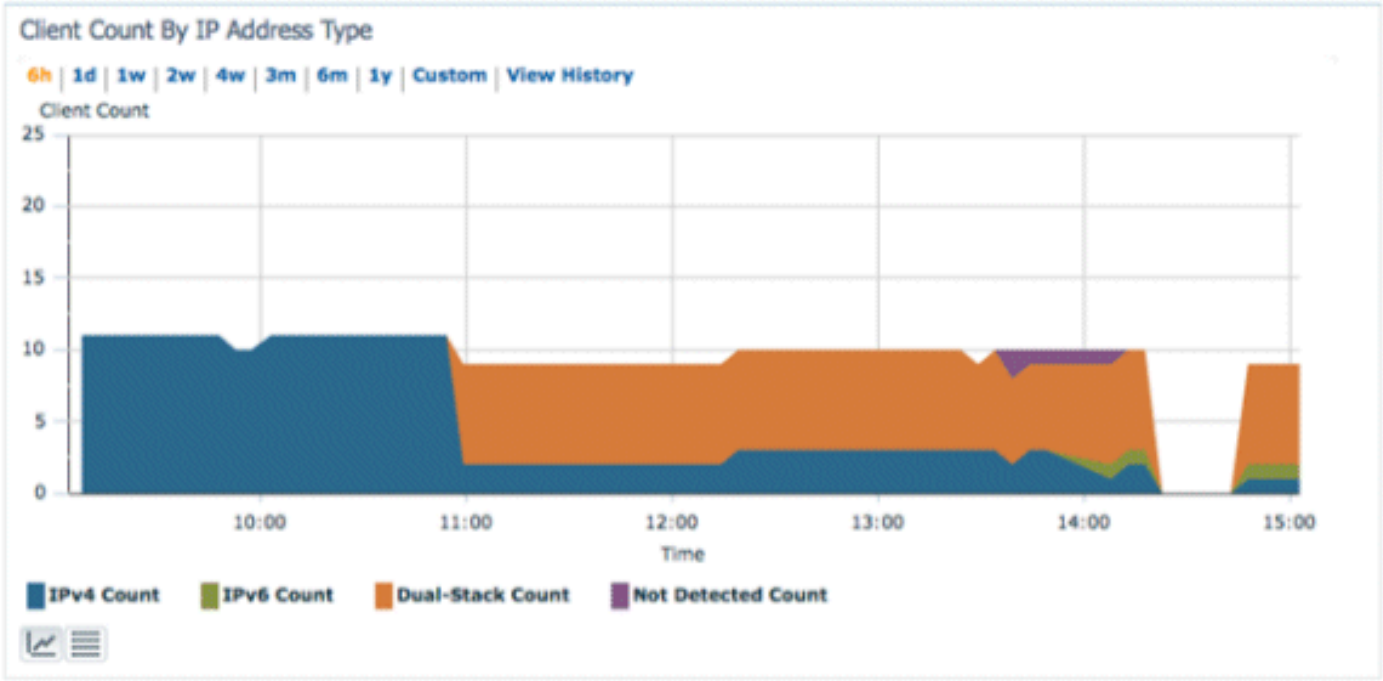
IPv6控制面板项目

要查看网络上存在的客户端类型，可以使用NCS中的“Dashlet”来深入了解IPv6特定统计信息，并提供深入查看IPv6客户端的功能。

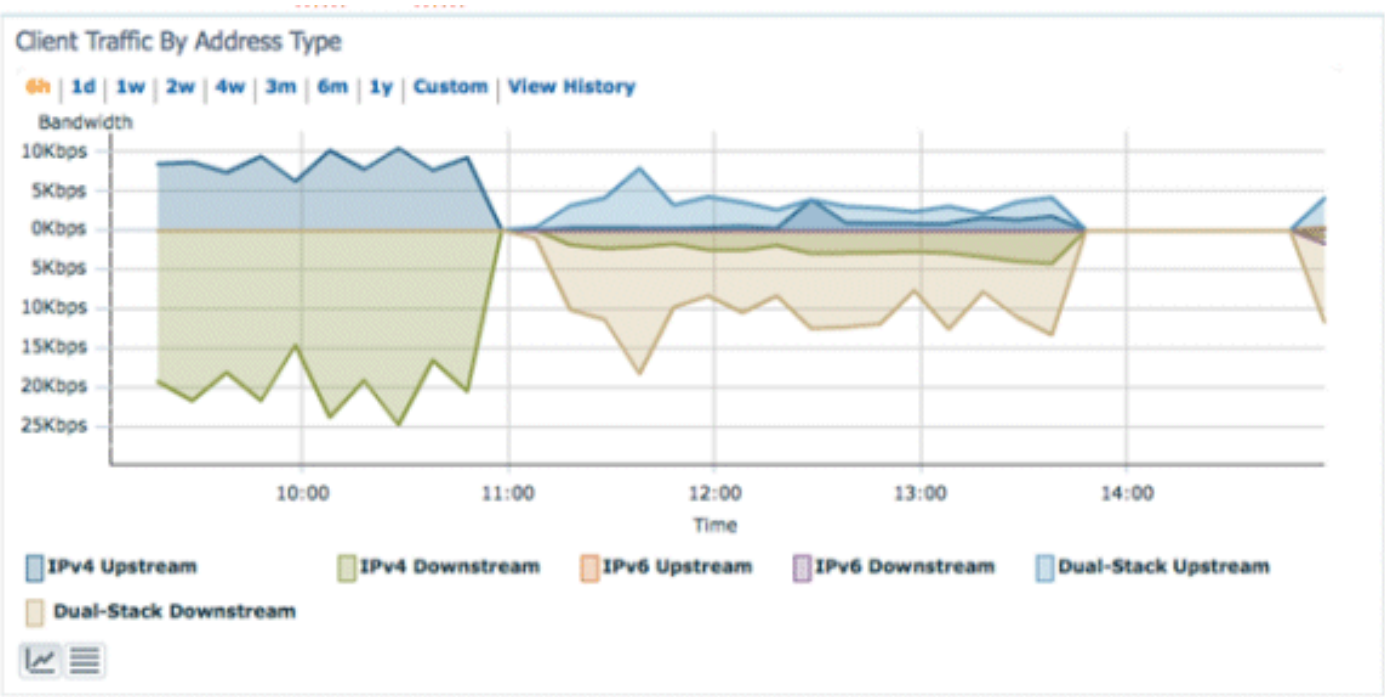
IP Address Type Dashlet — 显示网络上IP客户端的类型：



Client Count by IP Address Type — 显示随时间变化的IP客户端类型：



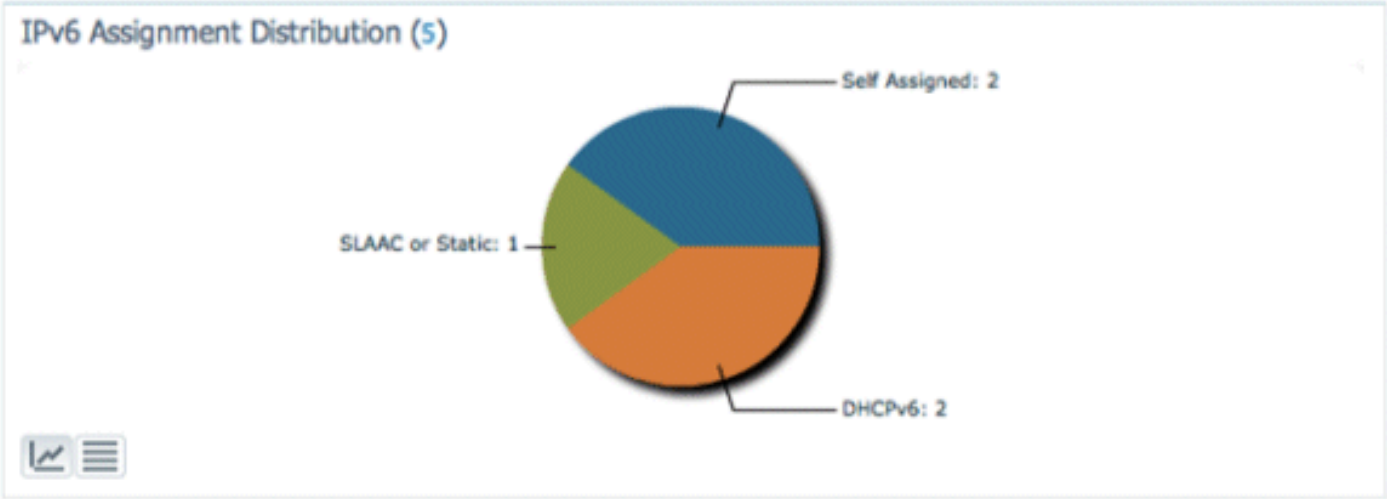
Client Traffic by IP Address Type — 显示来自每种客户端的流量。双协议栈类别中的客户端包括IPv4和IPv6流量：



IPv6 Address Assignment — 将每个客户端的地址分配方法显示为以下四个类别之一：

- DHCPv6 — 用于具有中央服务器分配地址的客户端。客户端也可能有SLAAC地址。
- SLAAC或静态 — 适用于使用无状态地址自动分配或使用静态配置地址的客户端。
- 未知 — 在某些情况下，无法发现IPv6地址分配。
    - 此情况仅发生在NCS中的有线客户端上，因为某些交换机不监听IPv6地址分配信息。
- Self-Assigned — 用于仅具有完全自动分配的本地链路地址的客户端。
    - 此类别中的客户端可能存在IPv6连接问题，因为它们缺少全局唯一地址或本地唯一地址。

饼图的每个部分均可点击，这样管理员就可以深入查看客户端列表。



监控IPv6客户端

为了监控和管理IPv6客户端信息，这些列已添加到Clients and Users页面：

- IP Type — 客户端的类型，取决于从客户端看到的IP地址。可能的选项是IPv4、IPv6或双协议栈，表示客户端同时具有IPv4和IPv6地址。
- IPv6分配类型 — 地址分配方法由NCS检测为SLAAC或Static、DHCPv6、Self-Assigned或Unknown。
- 全局唯一 — 客户端使用的最新IPv6全局地址。将鼠标悬停在列内容上可显示客户端使用的任何其他IPv6全局唯一地址。
- Local Unique — 客户端使用的最新IPv6本地唯一地址。将鼠标悬停在列内容上可显示客户端使用的任何其他IPv6全局唯一地址。
- 本地链路 — 客户端的IPv6地址，该地址是自行分配的，用于在分配任何其他IPv6地址之前进行通信。

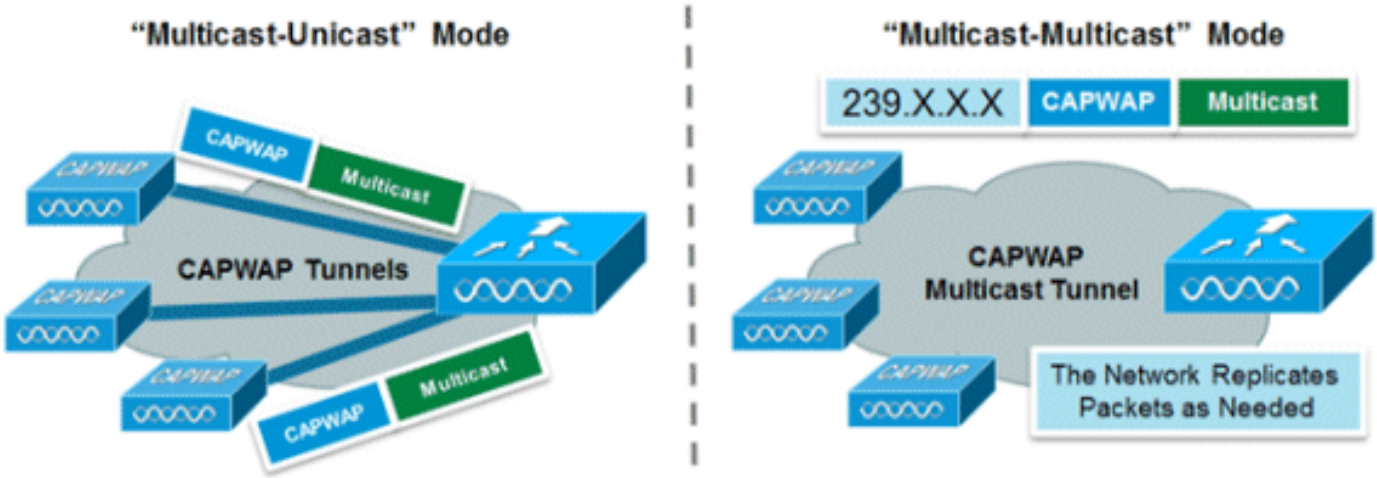
- Router Advertisements Dropped — 客户端发送并在AP上丢弃的路由器通告数。此列可用于跟踪可能配置错误或恶意配置为像IPv6路由器一样工作的客户端。此列是可排序的，这样可以轻松识别违规客户端。

除了显示IPv6特定列之外，“IP地址”列还会显示客户端的当前IP地址，优先显示IPv4地址（对于双协议栈客户端）或IPv6全局唯一地址（对于纯IPv6客户端）。

无线IPv6客户端支持的配置

到AP的组播分布模式

思科统一无线网络支持将组播分发到与控制器关联的AP的两种方法。在这两种模式下，来自有线网络的原始组播数据包都封装在第3层CAPWAP数据包内，该数据包通过CAPWAP单播或组播发送到AP。由于流量是CAPWAP封装的，因此AP不必与客户端流量位于同一个VLAN中。下面比较了两种组播分发方法：



	组播 — 单播模式	组播 — 组播模式
交付机制	控制器复制组播数据包并将其发送到单播CAPWAP隧道中的每个AP	控制器发送组播数据包的一个副本
支持的AP模式	FlexConnect和本地	仅本地模式
需要在有线网络上进行	无	Yes

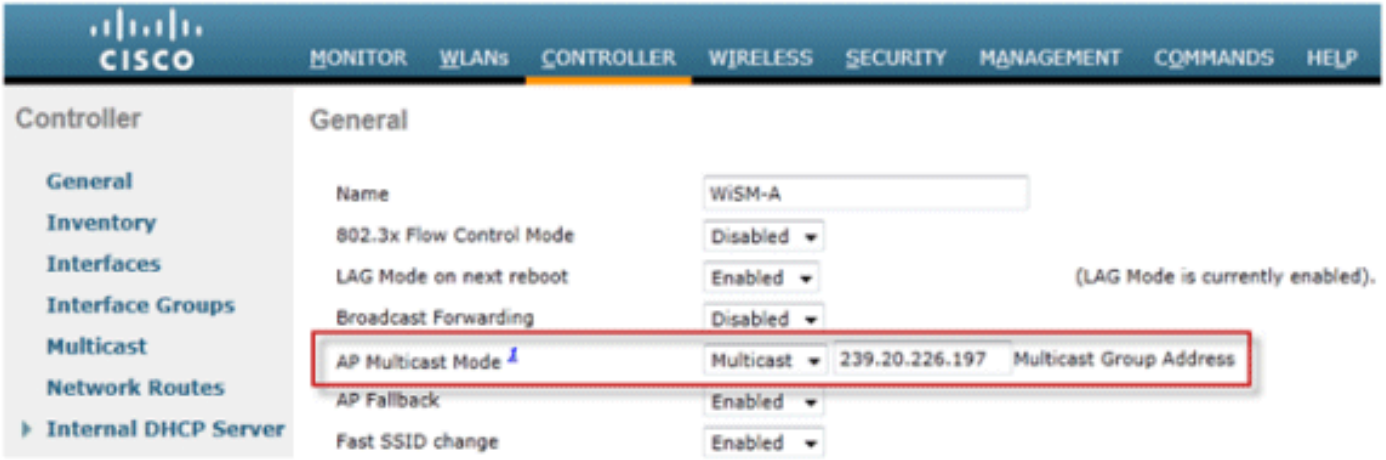
L3组播路由		
控制器加载	高	低
有线网络负载	高	低

配置组播 — 组播分布模式

出于可扩展性和有线带宽效率原因，建议选择组播 — 组播模式。

注意：仅对2500系列无线控制器绝对需要此步骤，但此步骤可实现更高效的组播传输，建议所有控制器平台都使用此步骤。

转到“General”页面下的“Controller”选项卡，确保AP组播模式已配置为使用Multicast模式，并且已配置有效的组地址。组地址是IPv4组播组，建议在239.X.X.X-239.255.255.255范围内，该范围适用于专用组播应用。

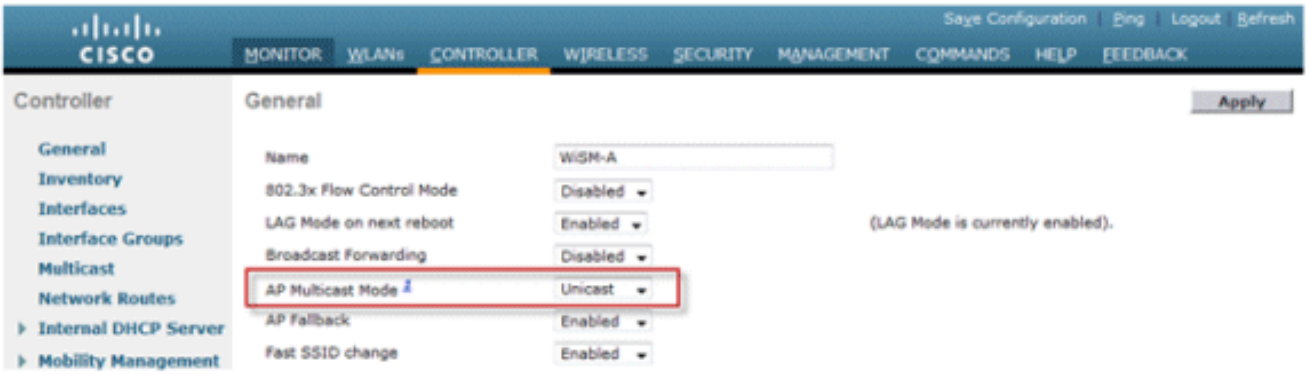


注意：请勿将224.X.X.X、239.0.0.X或239.128.0.X地址范围用于组播组地址。这些范围中的地址与本地链路 MAC 地址重叠并且泛洪所有交换机端口，即使 IGMP 监听已启用。

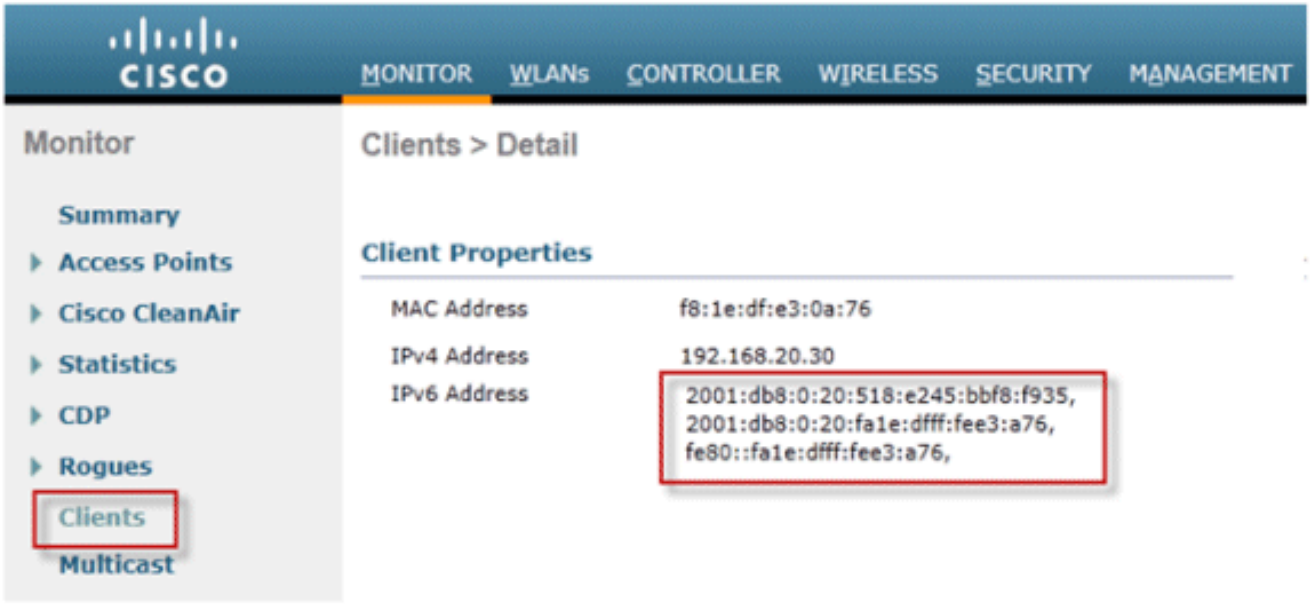
配置组播 — 单播分发模式

如果有线网络未正确配置为在控制器和AP或FlexConnect模式之间传输CAPWAP组播，并且AP将用于支持IPv6的集中交换WLAN，则需要单播模式。

1. 转至General页面下的Controller选项卡，确保AP组播模式已配置为使用单播模式。



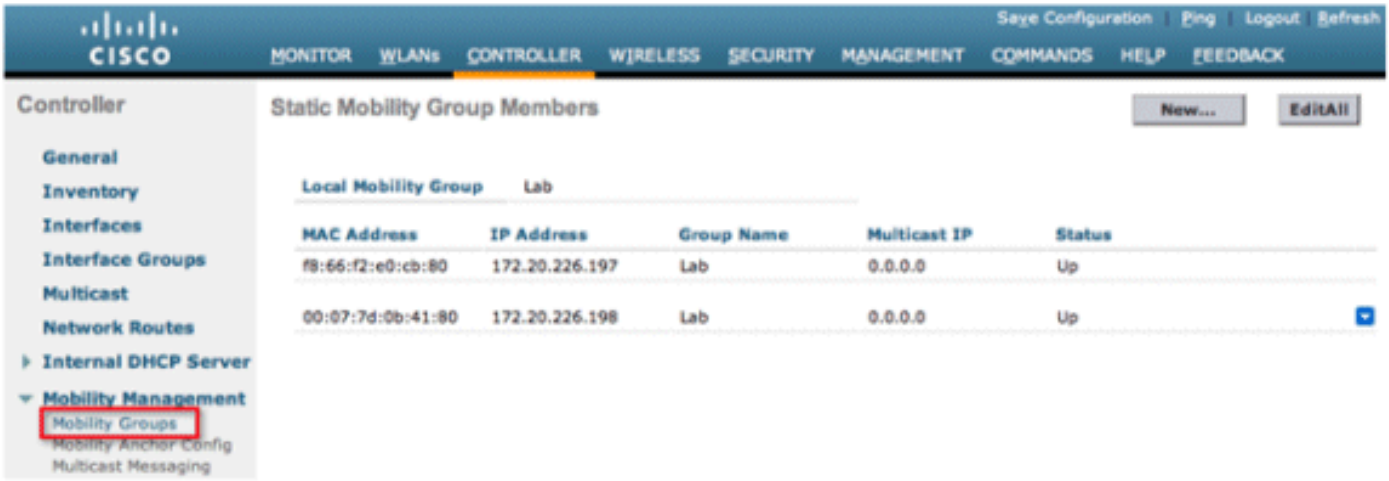
2. 将支持IPv6的客户端连接到无线局域网。通过导航到Monitor选项卡，然后导航到Clients菜单，验证客户端是否收到IPv6地址。



配置IPv6移动性

IPv6移动性没有特定配置，只是将控制器置于同一移动组或同一移动域中。这样，最多可以有72个控制器加入移动域，即使对于最大的园区，也能提供无缝的移动性。

转至Controller选项卡> Mobility Groups，并按MAC地址和IP地址将每个控制器添加到组中。这必须在移动组中的所有控制器上完成。

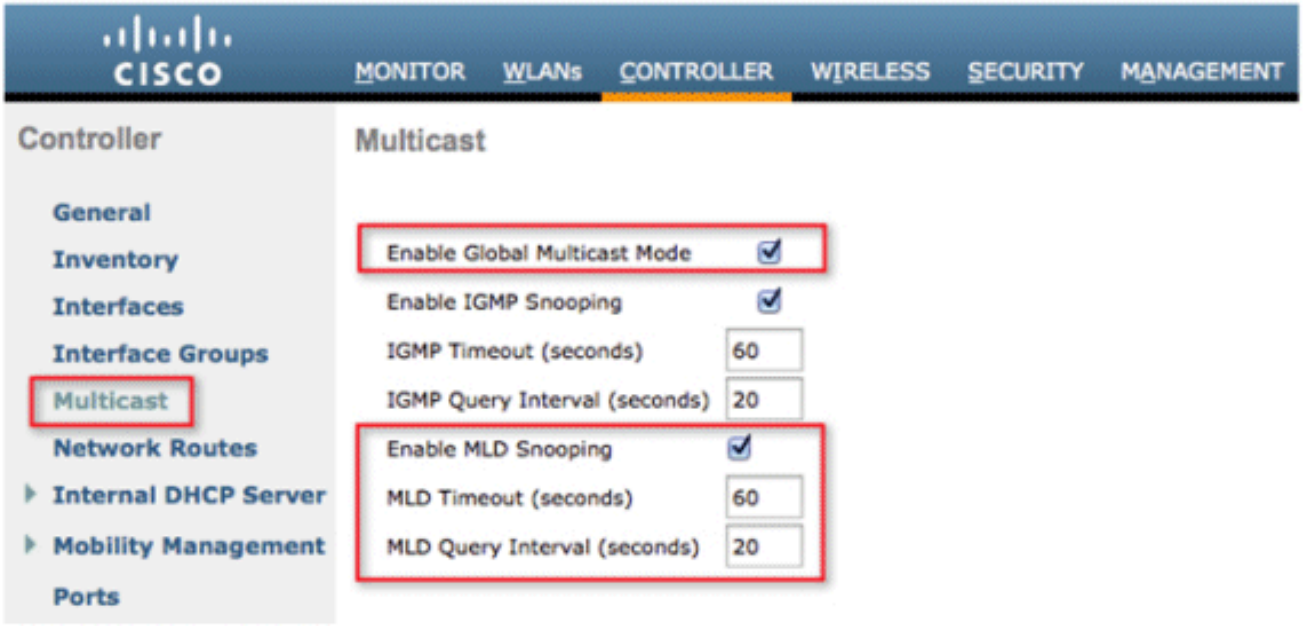


配置IPv6组播

控制器支持用于IPv6组播的MLDv1监听，这使其能够智能地跟踪组播流，并将组播流提供给请求组播流的客户端。

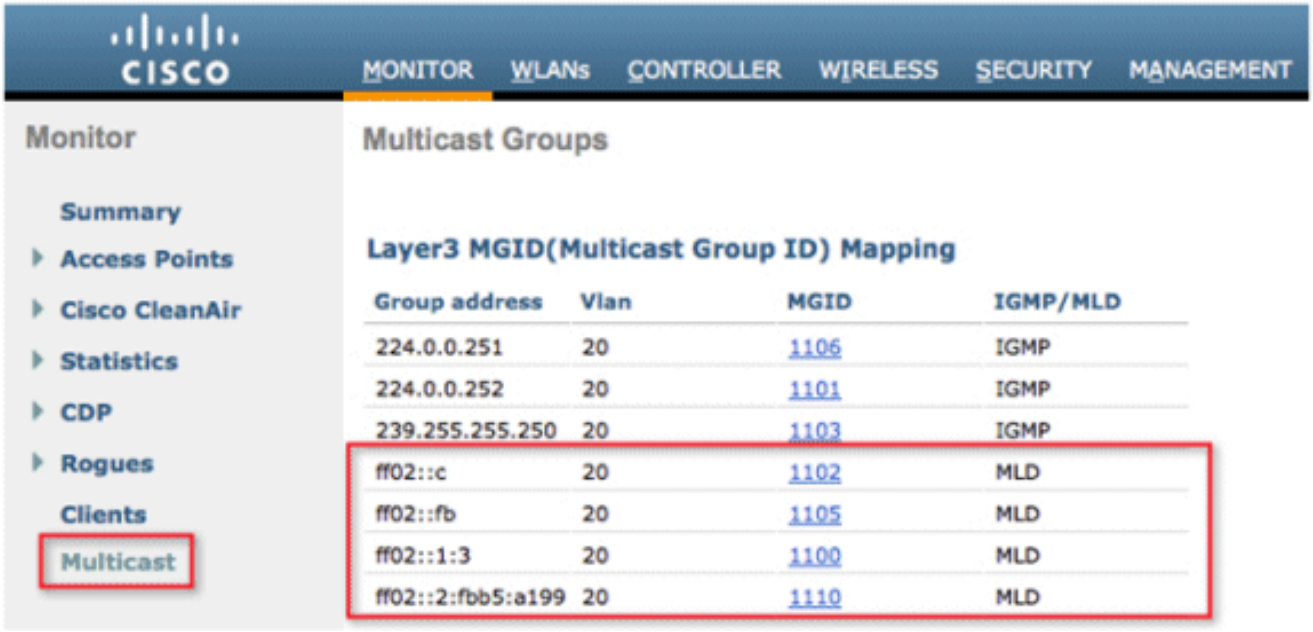
注意：与先前版本的版本不同，IPv6单播流量支持不要求在控制器上启用“全局组播模式”。自动启用IPv6单播流量支持。

1. 转至Controller选项卡> Multicast页和Enable MLD Snooping以支持组播IPv6流量。要启用IPv6组播，还必须启用控制器的全局组播模式。



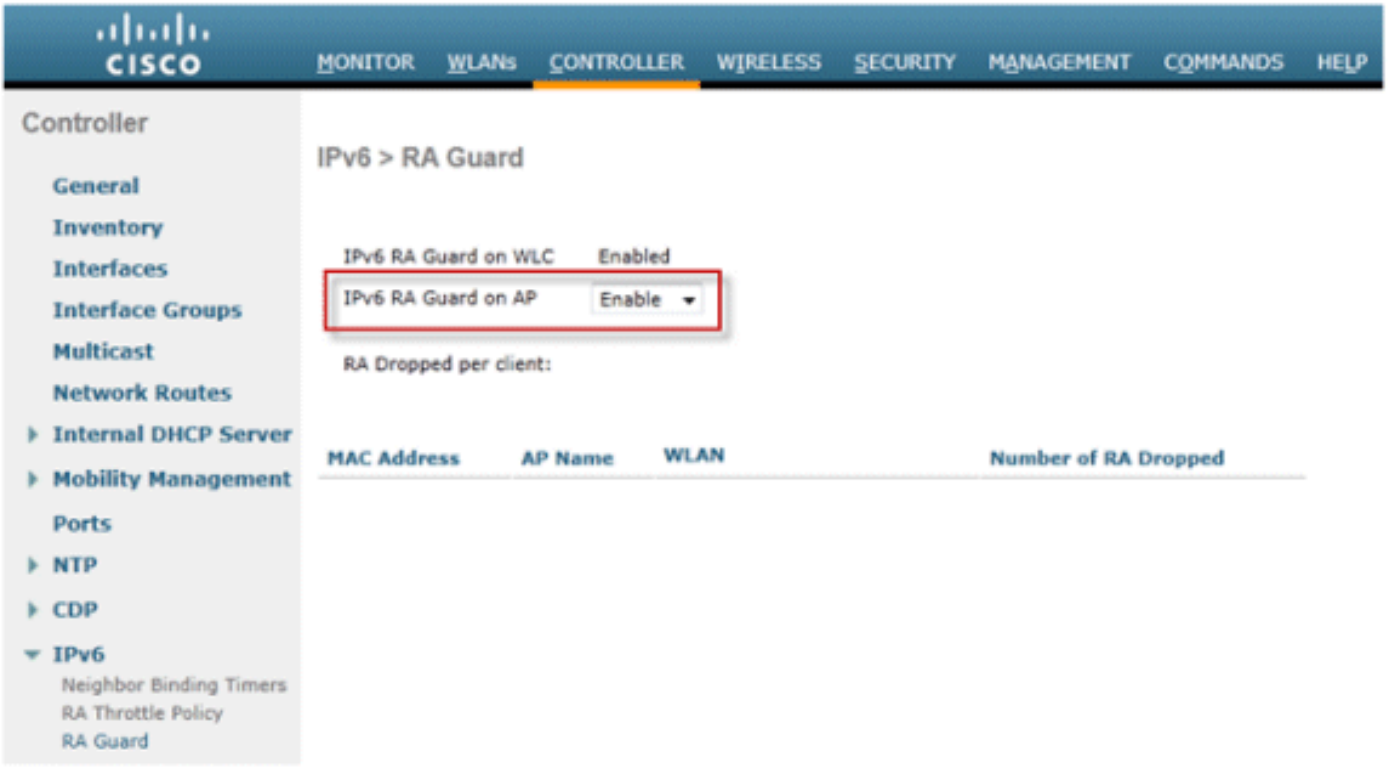
注：如果需要Apple的Bonjour等点对点发现应用，则应启用全局组播模式、IGMP和MLD监听。

2. 要验证IPv6组播流量是否被监听，请转到监控选项卡和组播页面。请注意，同时列出IPv4(IGMP)和IPv6(MLD)组播组。单击MGID以查看加入该组地址的无线客户端。



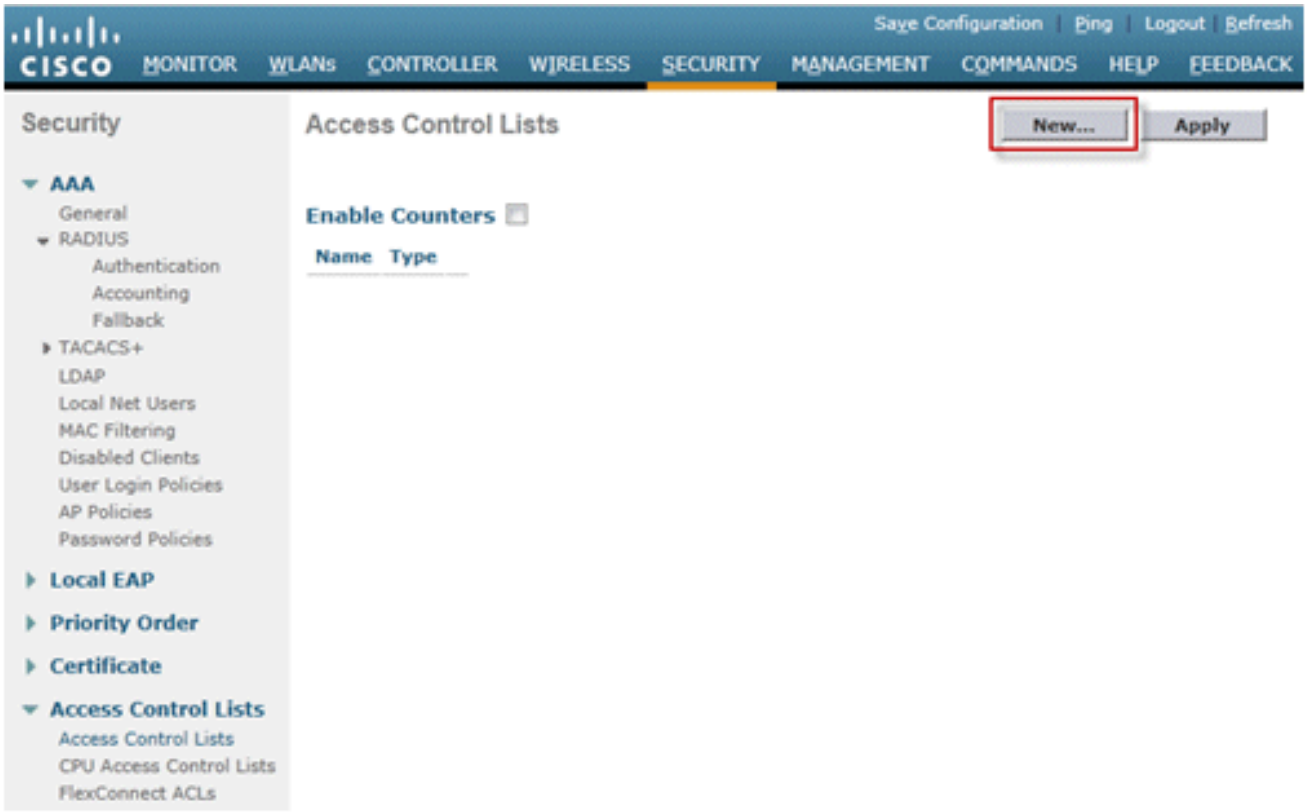
配置IPv6 RA防护

导航到Controller选项卡，然后在左侧菜单上导航到IPv6 > RA Guard。在AP上启用IPv6 RA防护。无法禁用控制器上的RA防护。除RA Guard配置之外，此页还显示已标识为发送RA的所有客户端。



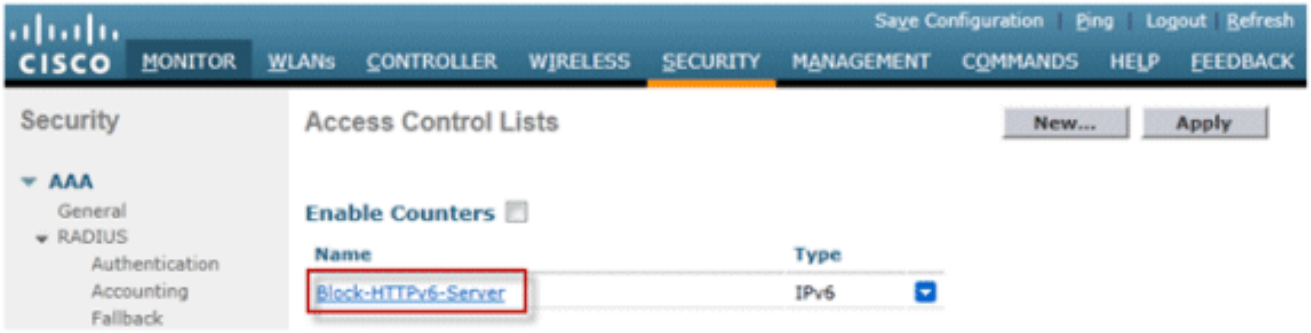
配置IPv6访问控制列表

1. 转至Security选项卡，打开Access Control Lists，然后单击New。

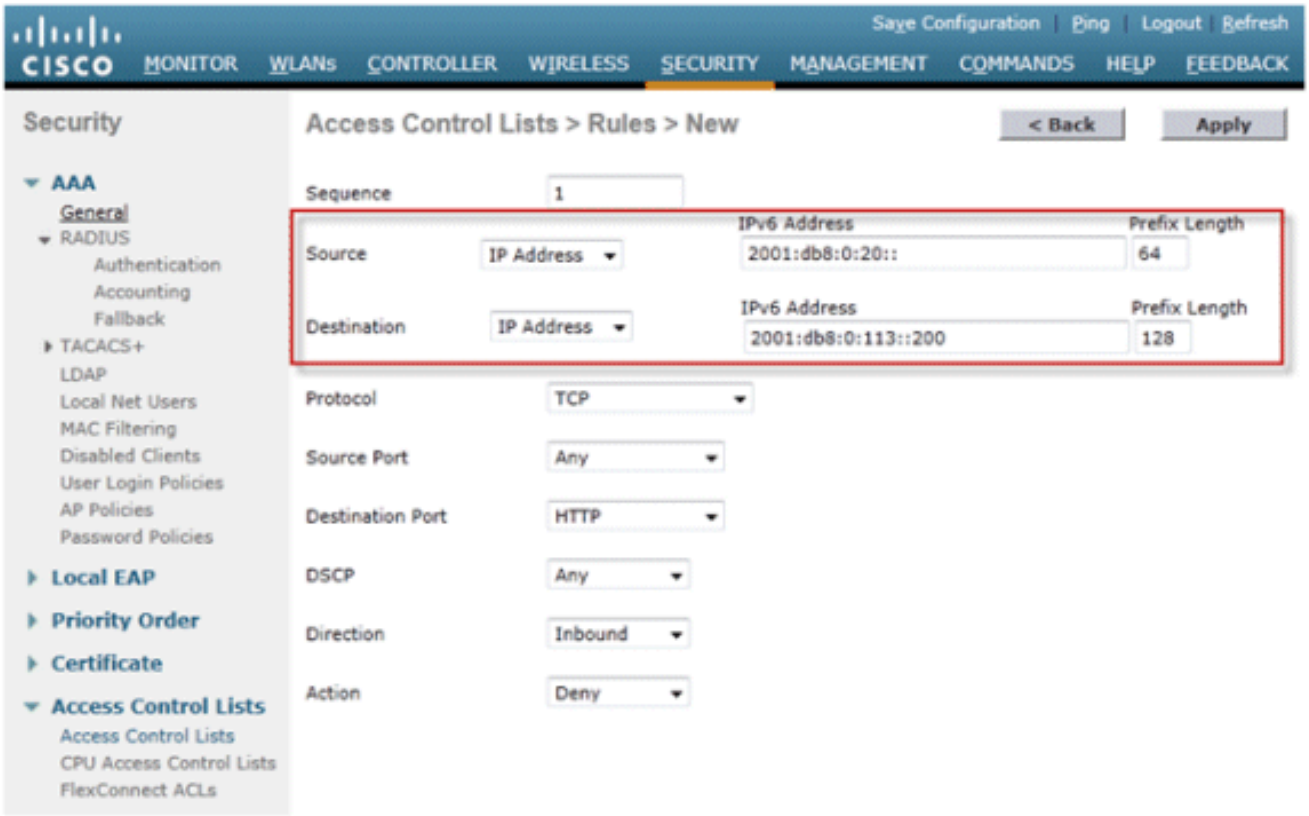


2. 输入ACL的唯一名称，将ACL Type更改为IPv6，然后单击Apply。

3. 单击在上述步骤中创建的新ACL。

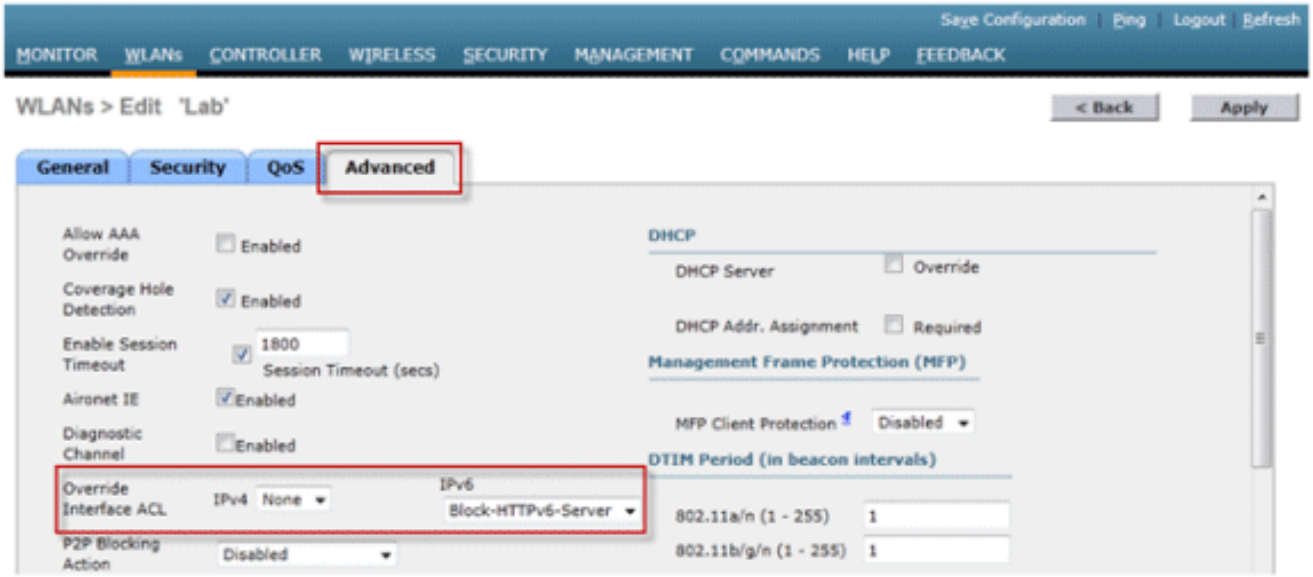


4. 单击Add New Rule，输入所需的规则参数，然后单击Apply。将序列号留空可将规则放置在列表的末尾。“Inbound”的“Direction”选项用于来自无线网络的流量，而“Outbound”用于发往无线客户端的流量。请记住，ACL中的最后一个规则是隐式的deny-all。前缀长度为64以匹配整个IPv6子网，前缀长度为128以唯一限制对单个地址的访问。



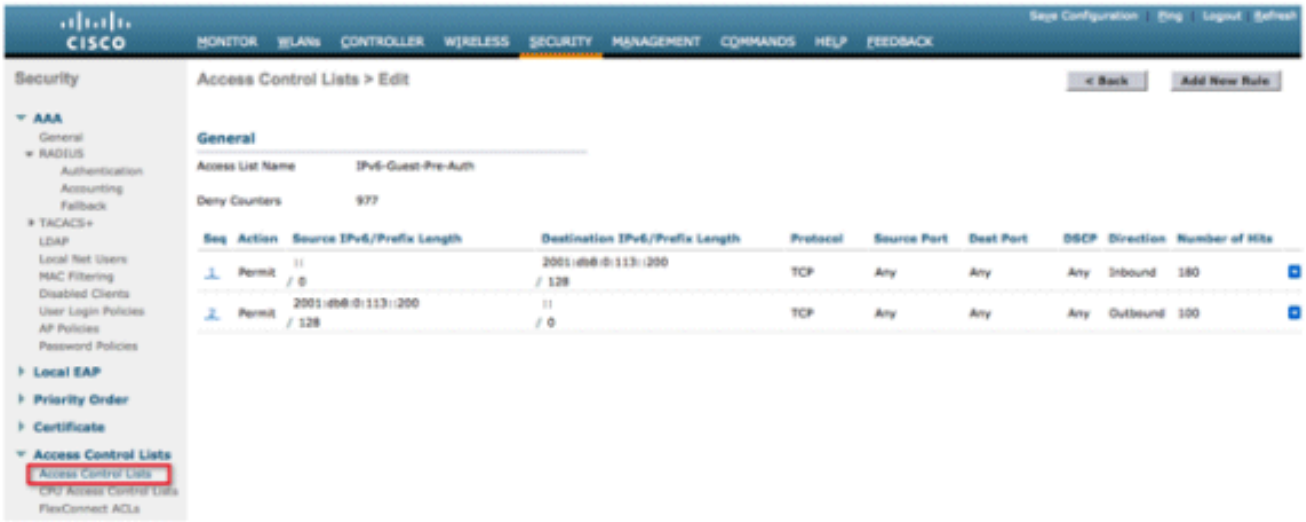
5. IPv6 ACL以每个WLAN/SSID为基础应用，并且可在多个WLAN上同时使用。导航到WLANs选

项卡，然后单击问题SSID的WLAN ID以应用IPv6 ACL。单击Advanced选项卡，将Override Interface ACL for IPv6更改为ACL名称。



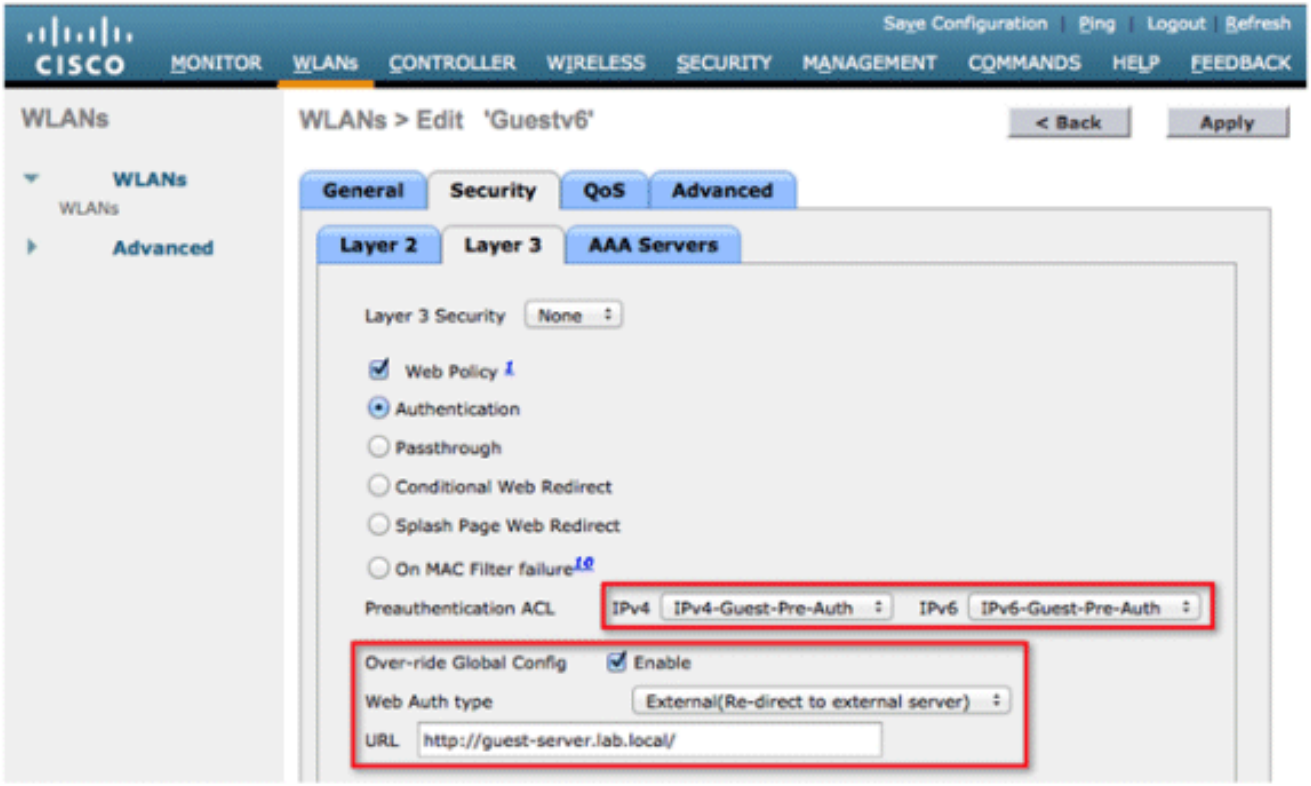
为外部Web身份验证配置IPv6访客接入

1. 为Web服务器配置IPv4和IPv6预身份验证ACL。这允许在客户端完全通过身份验证之前进出外部服务器的流量。



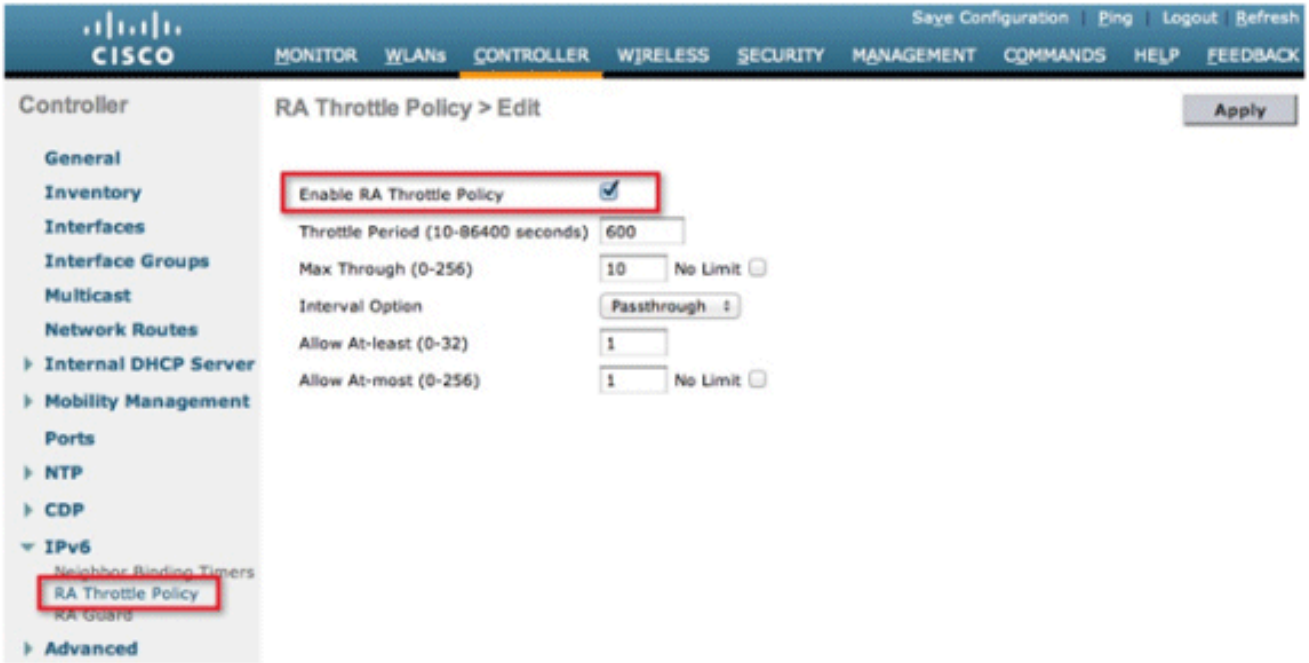
有关外部Web访问操作的详细信息，请参阅使用无线LAN控制器的外部Web身份验证配置示例。

2. 通过浏览到顶部的WLAN选项卡配置访客WLAN。创建访客SSID并使用第3层Web策略。为IPv4和IPv6选择步骤1中定义的预身份验证ACL。选中Over-ride Global Config部分，然后从Web Auth type下拉框中选择External。输入Web服务器的URL。外部服务器的主机名应在IPv4和IPv6 DNS中可解析。



配置IPv6 RA限制

1. 导航到Controller顶级菜单，然后单击左侧的IPv6 > RA Throttle Policy选项。通过点击复选框启用RA限制。



注意：发生RA限制时，仅允许第一个支持IPv6的路由器通过。对于由不同路由器提供多个IPv6前缀的网络，应禁用RA限制。

2. 仅在TAC的建议下调整限制时段和其他选项。但是，建议对大多数部署使用默认值。应牢记以下内容，调整RA限制策略的各种配置选项：

- “至少允许”的数值应小于“最多允许”，该数值应小于“最大通过”。
- RA限制策略不应使用超过1800秒的限制周期，因为这是大多数RA的默认生存时间。

下面介绍了每个RA限制选项：

- Throttle Period — 发生限制的时间段。RA限制仅在VLAN达到“最大通过”限制后生效。
- Max Through — 这是开始限制之前每个VLAN的最大RA数。“无限制”选项允许无限量的RA通过，无限制。
- Interval选项 — interval选项允许控制器根据IPv6 RA中设置的RFC 3775值以不同方式操作。
  - 直通 — 该值允许具有RFC3775间隔选项的任何RA在不限制的情况下通过。
  - 忽略 — 该值将导致RA节流器将具有interval选项的数据包视为常规RA，并在有效的情况下进行限制。
  - 限制 — 此值将导致具有间隔选项的RA始终受到速率限制。
- Allow At least — 每个路由器作为组播发送的最小RA数。
- Allow At-maximum — 在限制生效之前，作为组播发送的每台路由器的最大RA数。“No Limit”选项将允许该路由器通过RA的数量不受限制。

配置IPv6邻居绑定表

1. 转至Controller顶级菜单，然后在左侧菜单中单击IPv6 > Neighbor Binding Timers。

2. 根据需要调整Down Lifetime、Reachable Lifetime和Stale Lifetime。对于具有高度移动性的客户端的部署，应调整过时地址计时器的计时器。推荐值包括：

   - 关闭生存时间 — 30秒
   - 可达生存时间 — 300秒
   - 状态生存时间 — 86400秒

   每个生存时间计时器表示IPv6地址可以处于以下状态：

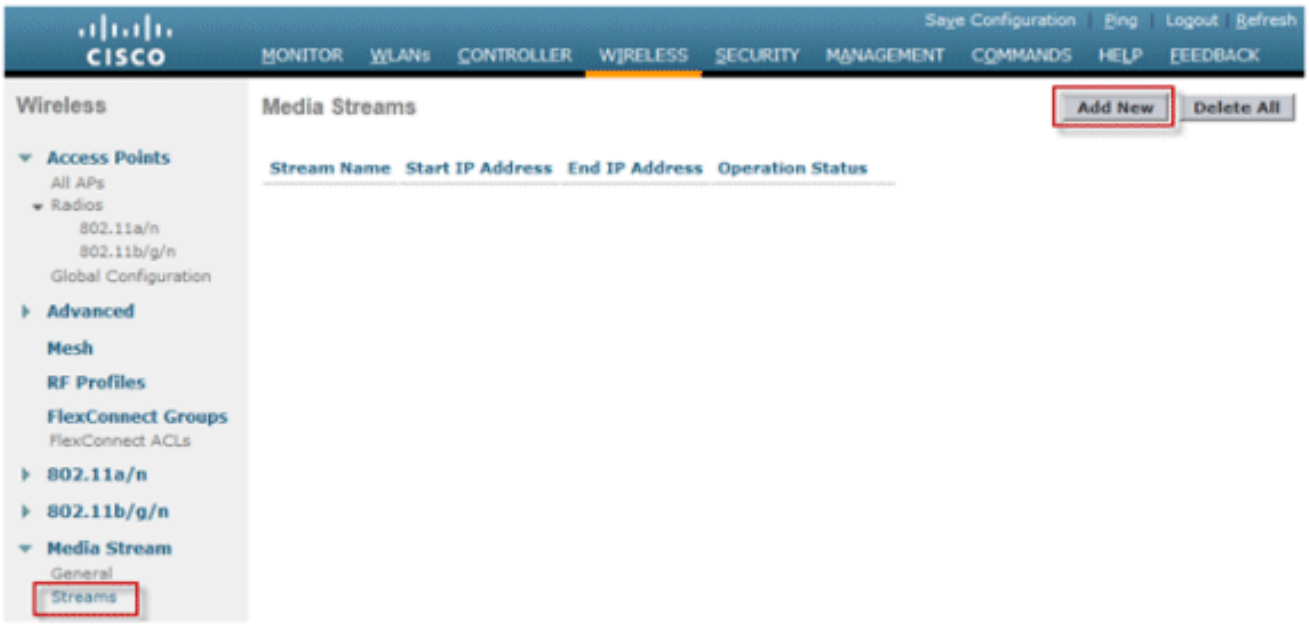
   - Down Lifetime — 关闭计时器指定如果控制器的上行链路接口关闭，应保留IPv6缓存条目的时间。
   - Reachable Lifetime — 此计时器指定IPv6地址将被标记为活动状态的时长，这意味着最近从此地址接收了流量。此计时器过期后，地址将变为“过时”状态。

- Stale Lifetime — 此计时器指定将“Reachable Lifetime”内未检测到的IPv6地址保留在缓存中的时间。在此生存期之后，将从绑定表中删除该地址。

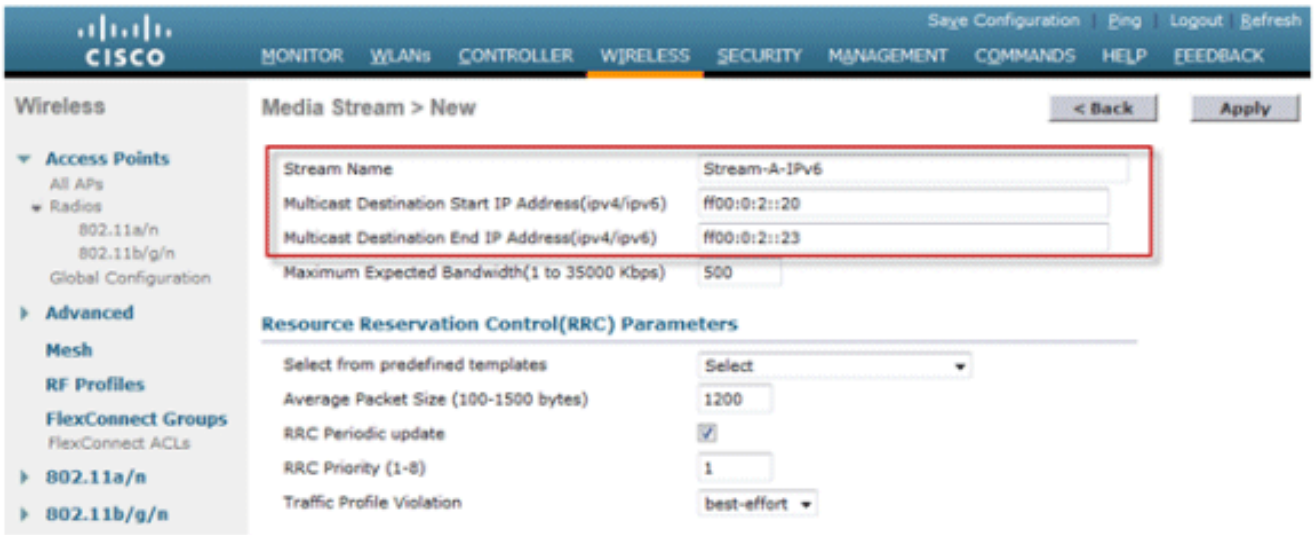
配置IPv6 VideoFlow

1. 确保在控制器上启用全局VideoStream功能。有关在802.11a/g/n网络和WLAN SSID上启用VideoStream的信息，请参阅思科统一无线网络解决方案：VideoStream部署指南。

2. 转至控制器上的Wireless选项卡，然后在左侧菜单中选择Media Stream > Streams。单击Add New以创建新流。



3. 为数据流命名并输入开始和结束IPv6地址。当仅使用单个数据流时，开始和结束地址相等。添加地址后，单击Apply以创建流。



排除IPv6客户端连接故障

某些客户端无法传递IPv6流量

有些客户端IPv6网络堆栈实施在进入网络时未正确通告自己，因此控制器不会适当地侦听其地址以将其放入邻居绑定表中。根据IPv6源防护功能，会阻止邻居绑定表中不存在的任何地址。要允许这些客户端传递流量，需要配置以下选项：

1. 通过CLI禁用IPv6源防护功能：

   <#root>

   config network ip-mac-binding disable

2. 通过CLI启用组播邻居请求转发：

   <#root>

   config ipv6 ns-mcast-fwd enable

检验IPv6客户端的第3层漫游是否成功：

在锚点和外部控制器上发出以下debug命令：

<#root>

debug client

<#root>

debug mobility handoff enable

<#root>

debug mobility packet enable

锚点控制器上的调试结果：

<#root>

```
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
```

外部控制器的调试结果：

<#root>

```
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：

<#root>

```
Show ipv6 neighbor-binding summary
```

<#root>

```
Debug ipv6 neighbor-binding filter client

        enable
```

<#root>

```
Debug ipv6 neighbor-binding filter errors enable
```

常见问题解答

问：限制广播域的最佳IPv6前缀大小是多少？

答：尽管可以将IPv6子网细分到/64以下，但此配置将中断SLAAC并导致客户端连接问题。如果需要分段以减少主机数量，可以使用接口组功能在不同后端VLAN之间负载均衡客户端，每个后端VLAN使用不同的IPv6前缀。

问：在支持IPv6客户端方面，是否存在任何可扩展性限制？

答：IPv6客户端支持的主要可扩展性限制是跟踪所有无线客户端IPv6地址的邻居绑定表。此表按控制器平台进行扩展，以支持客户端的最大数量乘以八（每个客户端的最大地址数量）。添加IPv6绑定表可将控制器的内存使用率提高大约10-15%（满载时不同），具体取决于平台。

无线控制器	最大客户端数量	IPv6邻居绑定表大小
2500	500	4,000
5500	7,000	56,000
WiSM2	15,000	120,000

问：IPv6功能对控制器的CPU和内存有何影响？

答：由于CPU有多个处理控制平面的核心，因此影响最小。当测试支持的最大客户端数（每个客户端有8个IPv6地址）时，CPU使用率低于30%，内存使用率低于75%。

问：是否可以禁用IPv6客户端支持？

答：对于希望在网络中仅启用IPv4并阻止IPv6的客户，可以在每个WLAN上使用和应用拒绝所有流量的IPv6 ACL。

问：是否可能有一个用于IPv4的WLAN和另一个用于IPv6的WLAN?

答：对于运行在相同AP上的两个不同WLAN，不能使用相同的SSID名称和安全类型。要将IPv4客户端与IPv6客户端分段，必须创建两个WLAN。每个WLAN必须配置一个ACL，该ACL分别阻止所有IPv4或IPv6流量。

问：为什么每个客户端支持多个IPv6地址很重要？

答：客户端可以为每个接口分配多个IPv6地址，这些地址可以是静态、SLAAC或DHCPv6，也可以始终具有自行分配的本地链路地址。客户端还可以使用不同的IPv6前缀来拥有其他地址。

问：什么是IPv6私有地址？为什么必须跟踪它们？

答：使用SLAAC地址分配时，客户端随机生成私有（也称为临时）地址。这些地址通常以一天左右的频率轮换，以防止主机可跟踪性始终因使用同一主机后缀（最后64位）而发生。跟踪这些私有地址对于跟踪版权侵犯等审计目的非常重要。思科NCS记录每个客户端使用的所有IPv6地址，并在每次客户端漫游或建立新会话时记录这些地址。这些记录可在NCS中配置，保留时间最长为一年。

相关信息

- 技术支持和文档 - Cisco Systems

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。