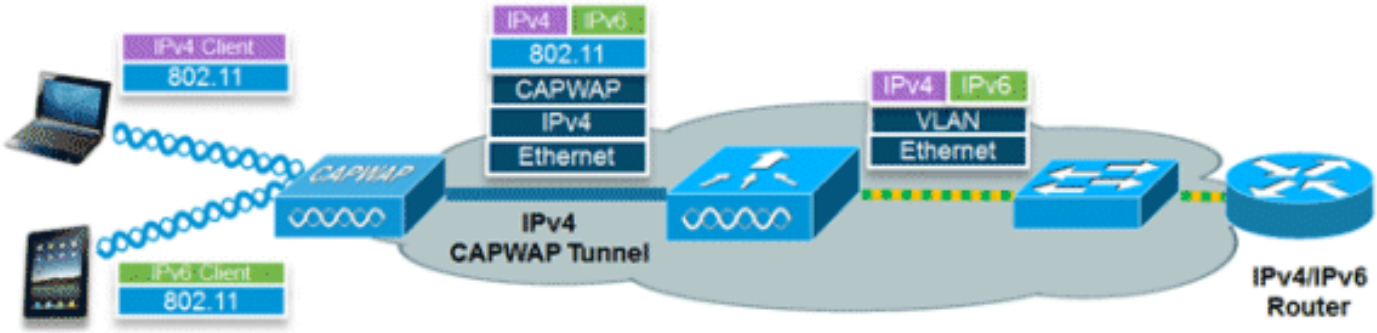
Implementierungsleitfaden für Wireless LAN IPv6-Clients

Inhalt

Einleitung

Dieses Dokument enthält Informationen zur Theorie des Betriebs und der Konfiguration der Cisco Unified Wireless LAN-Lösung für die Unterstützung von IPv6-Clients.

IPv6-Wireless-Client-Verbindungen



Dank der IPv6-Funktionen der Cisco Unified Wireless Network-Softwareversion 7.2 kann das Wireless-Netzwerk IPv4-, Dual-Stack- und IPv6-Clients in demselben Wireless-Netzwerk unterstützen. Das übergeordnete Ziel für die zusätzliche Unterstützung von IPv6-Clients für das Cisco Unified Wireless LAN war die Wahrung der Funktionsparität zwischen IPv4- und IPv6-Clients, einschließlich Mobilität, Sicherheit, Gastzugriff, Quality of Service und Endgerätetransparenz.

Pro Gerät können bis zu acht IPv6-Client-Adressen nachverfolgt werden. Dadurch können IPv6-Clients eine verbindungslokale Stateless Address Auto Configuration (SLAAC)-Adresse, ein Dynamic Host Configuration Protocol für IPv6 (DHCPv6)-Adresse sowie Adressen in alternativen Präfixen auf einer einzigen Schnittstelle nutzen. Work Group Bridge (WGB)-Clients, die mit dem Uplink eines autonomen Access Points (AP) im WGB-Modus verbunden sind, können auch IPv6 unterstützen.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Wireless LAN Controller der Serien 2500, 5500 oder WiSM2
- APs der Serien 1130, 1240, 1250, 1040, 1140, 1260, 3500, 3600 und 1520 oder 1550 Mesh APs
- IPv6-fähiger Router

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

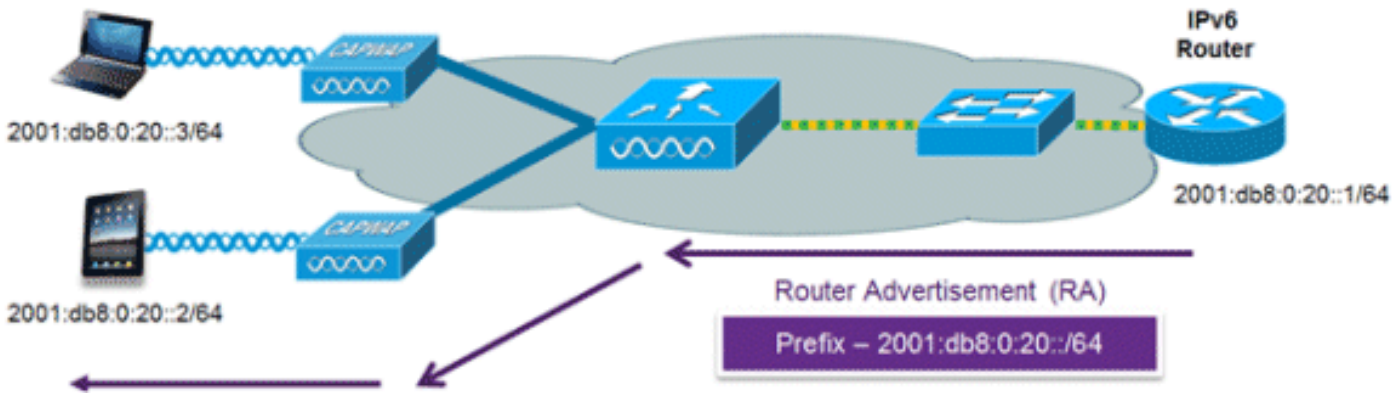
Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps von Cisco zu Konventionen).

Voraussetzungen für Wireless-IPv6-Client-Verbindungen

Um Wireless-IPv6-Client-Verbindungen zu ermöglichen, muss das zugrunde liegende kabelgebundene Netzwerk IPv6-Routing und einen Adresszuweisungsmechanismus wie SLAAC oder DHCPv6 unterstützen. Der Wireless LAN-Controller muss über eine L2-Adjacency zum IPv6-Router verfügen, und das VLAN muss gekennzeichnet werden, wenn die Pakete beim Controller eingehen. APs benötigen keine Verbindung in einem IPv6-Netzwerk, da der gesamte Datenverkehr innerhalb des IPv4-CAPWAP-Tunnels zwischen dem AP und dem Controller gekapselt wird.

SLAAC-Adressenzuweisung



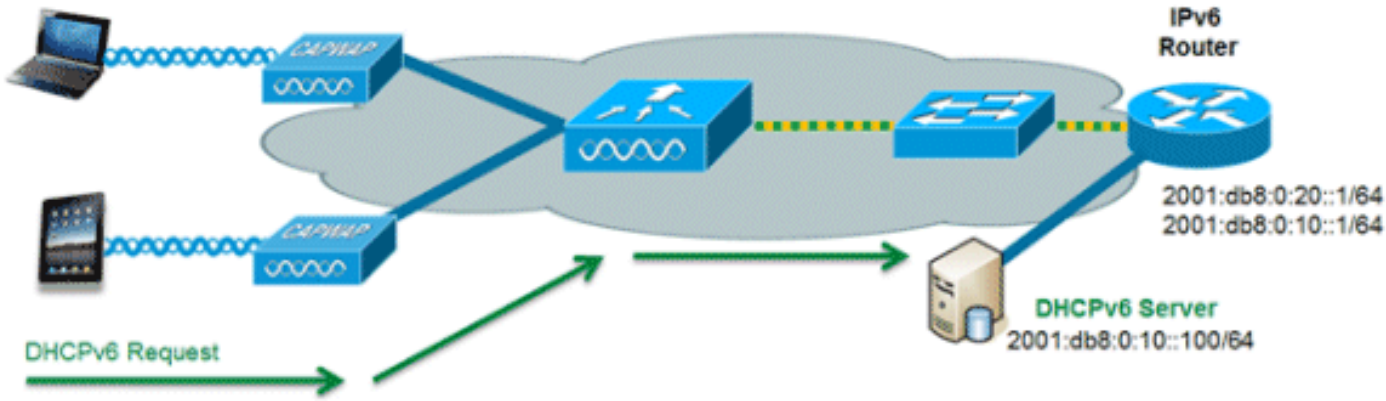
Die gängigste Methode für die Zuweisung von IPv6-Client-Adressen ist SLAAC. SLAAC bietet einfache Plug-and-Play-Verbindungen, bei denen Clients eine Adresse basierend auf dem IPv6-Präfix selbst zuweisen. Dieser Prozess wird erreicht, wenn der IPv6-Router regelmäßige Router Advertisement-Nachrichten versendet, die den Client über das verwendete IPv6-Präfix (die ersten 64 Bit) und das IPv6-Standard-Gateway informieren. Ab diesem Zeitpunkt können Clients die verbleibenden 64 Bit ihrer IPv6-Adresse auf der Grundlage von zwei Algorithmen generieren: EUI-64, die auf der MAC-Adresse der Schnittstelle basiert, oder private Adressen, die zufällig generiert werden. Die Wahl des Algorithmus hängt vom Client ab und ist häufig konfigurierbar. Die Erkennung doppelter Adressen wird von IPv6-Clients durchgeführt, um sicherzustellen, dass zufällige Adressen, die ausgewählt werden, nicht mit anderen Clients kollidieren. Die Adresse des

Routers, der Meldungen sendet, wird als Standard-Gateway für den Client verwendet.

Die folgenden Cisco IOS®-Konfigurationsbefehle von einem Cisco-fähigen IPv6-Router werden verwendet, um die SLAAC-Adressierung und Router Advertisements zu ermöglichen:

```
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-Adresszuweisung



Die Verwendung von DHCPv6 ist für die IPv6-Client-Konnektivität nicht erforderlich, wenn SLAAC bereits bereitgestellt ist. Es gibt zwei Betriebsmodi für DHCPv6: **Stateless** und **Stateful**.

Der DHCPv6 **Stateless**-Modus wird verwendet, um Clients zusätzliche Netzwerkinformationen bereitzustellen, die in der Router-Ankündigung nicht verfügbar sind, jedoch keine IPv6-Adresse, da diese bereits von der SLAAC bereitgestellt wird. Diese Informationen können den DNS-Domänennamen, DNS-Server(n) und andere anbieterspezifische DHCP-Optionen umfassen. Diese Schnittstellenkonfiguration ist für einen Cisco IOS IPv6-Router, der Stateless DHCPv6 mit aktivierter SLAAC implementiert:

```
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
```

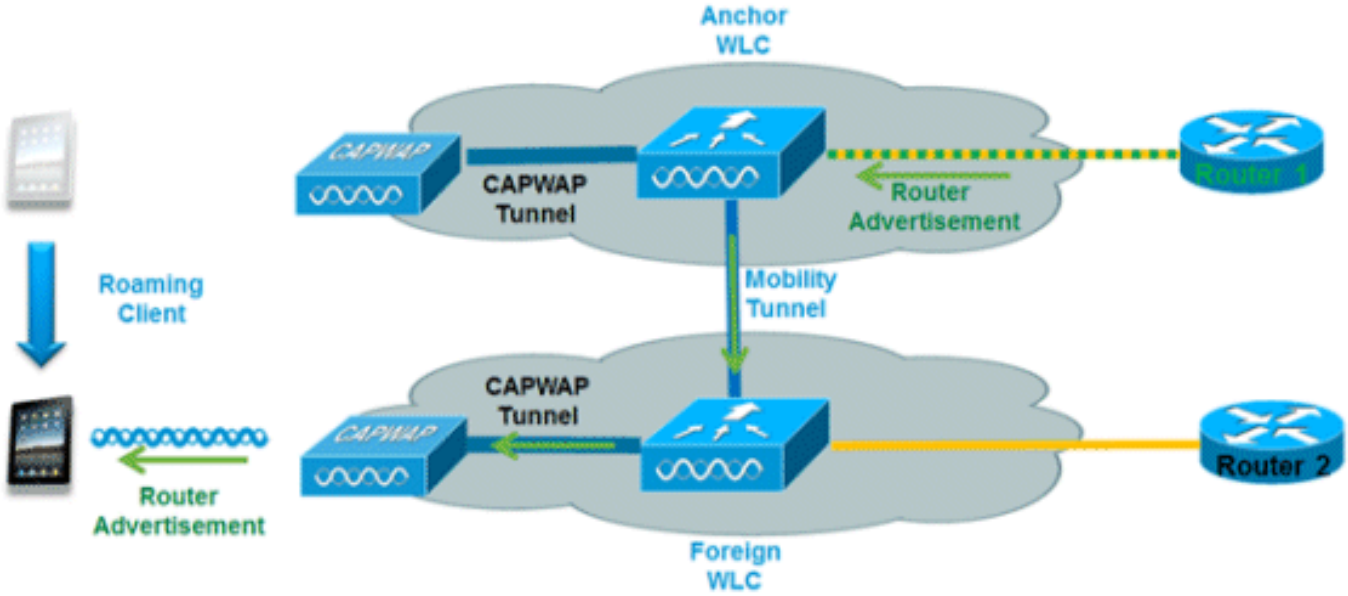
Die DHCPv6 **Stateful**-Option, auch als Managed Mode bezeichnet, funktioniert ähnlich wie DHCPv4, indem jedem Client eindeutige Adressen zugewiesen werden, anstatt dass der Client die letzten 64 Bit der Adresse wie in SLAAC generiert. Diese Schnittstellenkonfiguration ist für einen Cisco IOS IPv6-Router vorgesehen, der Stateful DHCPv6 implementiert, während SLAAC deaktiviert ist:

```
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
```

Zusätzliche Informationen

Die Konfiguration des kabelgebundenen Netzwerks für eine vollständige campusweite IPv6-Anbindung mithilfe von Dual-Stack- oder Tunneling-Verbindungsmethoden wird im vorliegenden Dokument nicht behandelt. Weitere Informationen finden Sie im Cisco Validated Deployment Guide Deploying IPv6 in Campus Networks.

IPv6-Client-Mobilität



Um Roaming-IPv6-Clients über mehrere Controller hinweg zu verwalten, müssen die ICMPv6-Meldungen wie Neighbor Solicitation (NS), Neighbor Advertisement (NA), Router Advertisement (RA) und Router Solicitation (RS) besonders behandelt werden, um sicherzustellen, dass sich ein Client im selben Layer-3-Netzwerk befindet. Die Konfiguration für IPv6-Mobilität ist dieselbe wie für IPv4-Mobilität und erfordert keine separate Software auf der Client-Seite, um ein nahtloses Roaming zu erreichen. Die einzige erforderliche Konfiguration besteht darin, dass die Controller derselben Mobilitätsgruppe/Domäne angehören müssen.

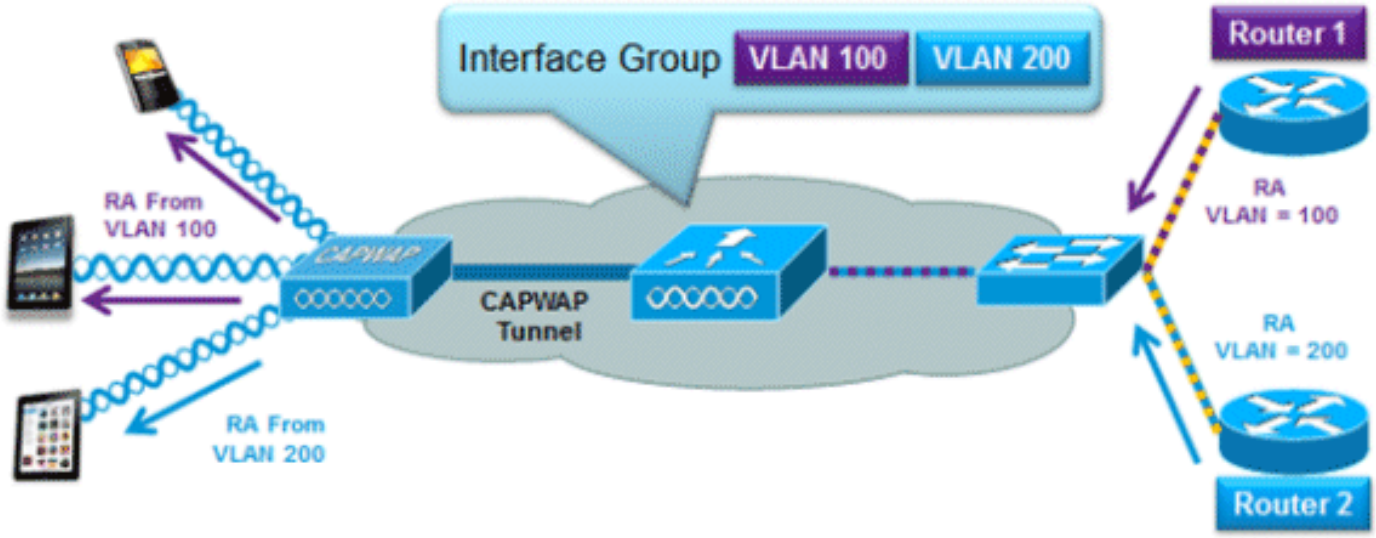
Nachfolgend finden Sie den Prozess für die Controller-übergreifende IPv6-Client-Mobilität:

1. Wenn beide Controller auf dasselbe VLAN zugreifen, auf dem sich der Client ursprünglich befand, handelt es sich bei dem Roaming lediglich um ein Layer-2-Roaming-Ereignis, bei dem der Client-Datensatz auf den neuen Controller kopiert wird und kein Datenverkehr zurück zum Anker-Controller geleitet wird.

2. Wenn der zweite Controller nicht auf das ursprüngliche VLAN des Clients zugreifen kann, tritt ein Layer-3-Roaming-Ereignis auf, d. h. der gesamte Datenverkehr vom Client muss über den Mobility-Tunnel (Ethernet over IP) zum Anker-Controller geleitet werden.Um sicherzustellen, dass die ursprüngliche IPv6-Adresse des Clients beibehalten wird, werden die RAs aus dem ursprünglichen VLAN vom Anker-Controller an den ausländischen Controller gesendet, wo sie mithilfe von L2-Unicast vom Access Point an den Client übermittelt werden.Wenn der Roaming-Client seine Adresse über DHCPv6 erneuert oder eine neue Adresse über SLAAC generiert, werden die RS-, NA- und NS-Pakete weiterhin an das ursprüngliche VLAN getunnelt, sodass der Client eine IPv6-Adresse erhält, die für dieses VLAN gilt.

Hinweis: Die Mobilität für Clients, die nur IPv6 unterstützen, basiert auf VLAN-Informationen. Das bedeutet, dass reine IPv6-Client-Mobilität auf nicht gekennzeichneten VLANs nicht unterstützt wird.

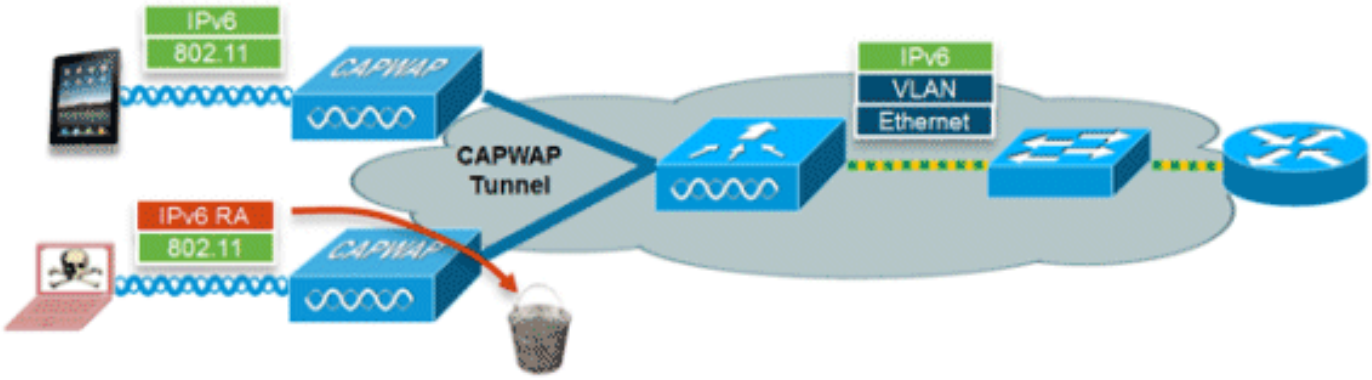
Unterstützung für VLAN Select (Schnittstellengruppen)



Die Schnittstellengruppen-Funktion ermöglicht einem Unternehmen, ein einzelnes WLAN mit mehreren auf dem Controller konfigurierten VLANs zu nutzen, um den Lastenausgleich von Wireless-Clients über diese VLANs hinweg zu ermöglichen. Diese Funktion wird häufig verwendet, um die Größe von IPv4-Subnetzen gering zu halten, während ein WLAN auf Tausende von Benutzern über mehrere VLANs in der Gruppe skaliert werden kann. Zur Unterstützung von IPv6-Clients mit Schnittstellengruppen ist keine zusätzliche Konfiguration erforderlich, da das System automatisch den richtigen RA über L2 Wireless Unicast an die richtigen Clients sendet. Durch Unicasting der RA erhalten Clients im selben WLAN, aber in einem anderen VLAN, nicht die falsche RA.

First-Hop-Sicherheit für IPv6-Clients

Router Advertisement Guard



Die RA Guard-Funktion erhöht die Sicherheit des IPv6-Netzwerks, indem RAs, die von Wireless-Clients ausgehen, entfernt werden. Ohne diese Funktion könnten sich falsch konfigurierte oder böswillige IPv6-Clients als Router für das Netzwerk ankündigen, der häufig eine hohe Priorität hat, die Vorrang vor legitimen IPv6-Routern haben könnte.

RA Guard ist standardmäßig am Access Point aktiviert (kann jedoch am Access Point deaktiviert werden) und immer am Controller aktiviert. Das Verwerfen von RAs am Access Point ist vorzuziehen, da es sich um eine besser skalierbare Lösung handelt, die verbesserte RA-Verwerfungszähler pro Client bereitstellt. In allen Fällen wird die IPv6-RA irgendwann entfernt, um andere Wireless-Clients und das Upstream-Netzwerk vor schädlichen oder falsch konfigurierten IPv6-Clients zu schützen.

DHCPv6-Serverschutz

Die DHCPv6 Server Guard-Funktion verhindert, dass Wireless-Clients IPv6-Adressen an andere Wireless-Clients oder kabelgebundene Clients im Upstream weitergeben. Um die Weiterleitung von DHCPv6-Adressen zu verhindern, werden alle DHCPv6-Weiterleitungspakete von Wireless-Clients verworfen. Diese Funktion wird auf dem Controller ausgeführt, erfordert keine Konfiguration und wird automatisch aktiviert.

IPv6 Source Guard

Die IPv6 Source Guard-Funktion verhindert, dass ein Wireless-Client Spoofing-Angriffe auf eine IPv6-Adresse eines anderen Clients ausführt. Diese Funktion entspricht IPv4 Source Guard. IPv6 Source Guard ist standardmäßig aktiviert, kann jedoch über die CLI deaktiviert werden.

IPv6-Adressabrechnung

Für die RADIUS-Authentifizierung und -Abrechnung sendet der Controller mithilfe des Attributs "Framed-IP-address" eine IP-Adresse zurück. Die IPv4-Adresse wird in diesem Fall verwendet.

Das Attribut "Calling-Station-ID" verwendet diesen Algorithmus, um eine IP-Adresse zurückzusenden, wenn "Call Station ID Type" auf dem Controller auf "IP Address" (IP-Adresse) konfiguriert ist:

1. IPv4-Adresse
2. Globale Unicast-IPv6-Adresse
3. Lokale IPv6-Adresse verknüpfen

Da sich Client-IPv6-Adressen häufig ändern können (temporäre oder private Adressen), ist es wichtig, sie im Laufe der Zeit zu verfolgen. Das Cisco NCS zeichnet alle von den einzelnen Clients

verwendeten IPv6-Adressen auf und protokolliert sie in der Vergangenheit jedes Mal, wenn der Client Roaming durchführt oder eine neue Sitzung herstellt. Diese Datensätze können auf NCS so konfiguriert werden, dass sie bis zu ein Jahr gespeichert werden.

Hinweis: Der Standardwert für "Call Station ID Type" auf dem Controller wurde in Version 7.2 in "System MAC Address" (System-MAC-Adresse) geändert. Bei einem Upgrade sollte dies so geändert werden, dass die Clients anhand der MAC-Adresse eindeutig verfolgt werden können, da sich die IPv6-Adressen während der Sitzung ändern können und zu Problemen bei der Abrechnung führen können, wenn die Calling-Station-ID auf IP-Adresse gesetzt ist.

IPv6-Zugriffskontrolllisten

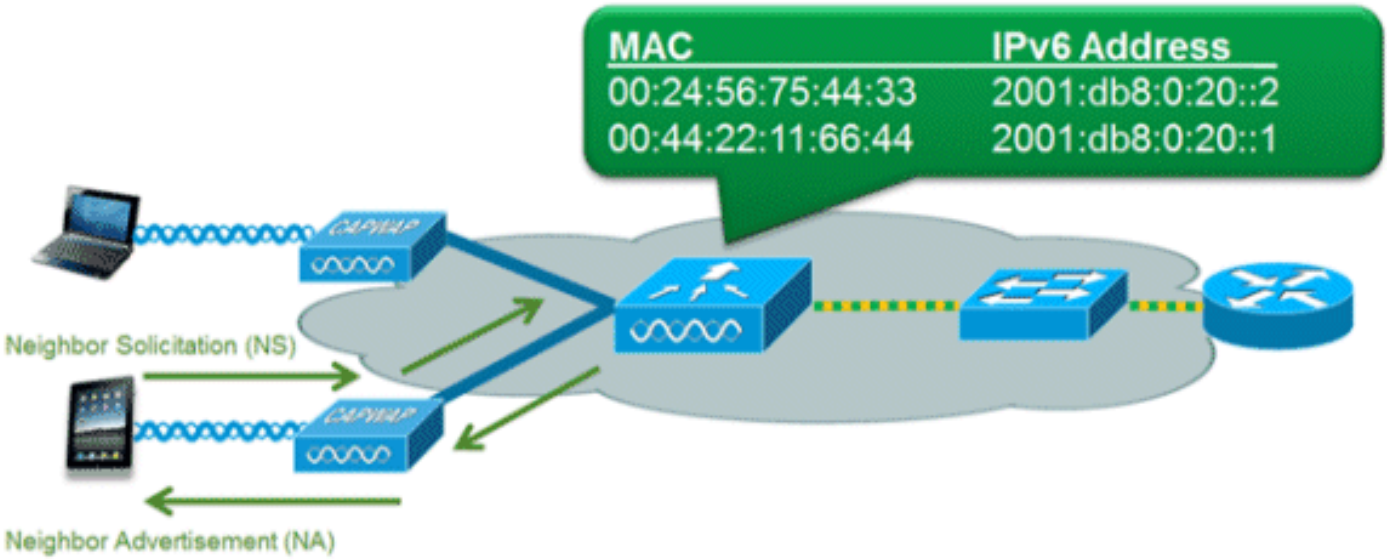
Um den Zugriff auf bestimmte kabelgebundene Upstream-Ressourcen zu beschränken oder bestimmte Anwendungen zu blockieren, können IPv6-Zugriffskontrolllisten (ACLs) verwendet werden, um Datenverkehr zu identifizieren und zuzulassen oder zu verweigern. IPv6-ACLs unterstützen dieselben Optionen wie IPv4-ACLs, einschließlich Quelle, Ziel, Quellport und Zielport (auch Portbereiche werden unterstützt). ACLs vor der Authentifizierung werden ebenfalls unterstützt, um die IPv6-Gastauthentifizierung über einen externen Webserver zu unterstützen. Der Wireless Controller unterstützt bis zu 64 eindeutige IPv6-ACLs mit jeweils 64 eindeutigen Regeln. Der Wireless Controller unterstützt weiterhin 64 zusätzliche eindeutige IPv4-ACLs mit jeweils 64 eindeutigen Regeln, sodass insgesamt 128 ACLs für einen Dual-Stack-Client verfügbar sind.

AAA-Aufhebung für IPv6-ACLs

Zur Unterstützung einer zentralisierten Zugriffskontrolle über einen zentralisierten AAA-Server wie die Cisco Identity Services Engine (ISE) oder ACS kann die IPv6-ACL auf Client-Basis mithilfe von AAA Override-Attributen bereitgestellt werden. Um diese Funktion nutzen zu können, muss die IPv6-ACL auf dem Controller konfiguriert und das WLAN mit aktivierter Funktion "AAA Override" konfiguriert werden. Das AAA-Attribut für eine IPv6-ACL lautet ***Airespace-IPv6-ACL-Name*** ähnlich dem *Airespace-ACL-Name*-Attribut, das für die Bereitstellung einer IPv4-basierten ACL verwendet wird. Beim zurückgegebenen AAA-Attribut sollte es sich um eine Zeichenfolge handeln, die dem Namen der IPv6-ACL entspricht, die auf dem Controller konfiguriert wurde.

Paketoptimierung für IPv6-Clients

Caching zur Ermittlung von Netznachbarn



Das IPv6 Neighbor Discovery Protocol (NDP) nutzt anstelle des Address Resolution Protocol (ARP) Netzwerkpakete und NS-Pakete, damit IPv6-Clients die MAC-Adresse anderer Clients im Netzwerk auflösen können. Der NDP-Prozess kann sehr chatty sein, da er anfänglich Multicast-Adressen für die Adressenauflösung verwendet. Dies kann wertvolle Wireless-Sendezeit beanspruchen, da die Multicast-Pakete an alle Clients im Netzwerksegment gesendet werden.

Um die Effizienz des NDP-Prozesses zu steigern, kann der Controller durch das Caching der Nachbarerkennung als Proxy agieren und auf NS-Abfragen reagieren, die er auflösen kann. Die Nachbar-Discovery-Zwischenspeicherung wird durch die zugrunde liegende Nachbar-Bindungstabelle ermöglicht, die im Controller vorhanden ist. Die Nachbar-Bindungstabelle verfolgt jede IPv6-Adresse und die ihr zugeordnete MAC-Adresse. Wenn ein IPv6-Client versucht, die Link Layer-Adresse eines anderen Clients aufzulösen, wird das NS-Paket vom Controller abgefangen, der mit einem NA-Paket antwortet.

Drosselung der Router-Ankündigung

Router Advertisement Throttling ermöglicht dem Controller die Durchsetzung einer Ratenbeschränkung für RAs, die auf das Wireless-Netzwerk zusteuern. Durch die Aktivierung der RA-Drosselung können Router, die so konfiguriert sind, dass sie sehr häufig (z. B. alle drei Sekunden) RAs senden, auf eine minimale Frequenz zurückgesetzt werden, die die IPv6-Client-Konnektivität weiterhin aufrechterhält. Auf diese Weise kann die Übertragungszeit optimiert werden, indem die Anzahl der zu sendenden Multicast-Pakete verringert wird. Wenn ein Client ein RS sendet, wird in allen Fällen ein RA über den Controller und Unicast an den anfordernden Client zugelassen. Auf diese Weise soll sichergestellt werden, dass neue Clients oder Roaming-Clients nicht durch RA-Drosselung beeinträchtigt werden.

IPv6-Gastzugriff

Die Wireless- und kabelgebundenen Gastfunktionen für IPv4-Clients funktionieren auf die gleiche Weise für Dual-Stack- und IPv6-Clients. Sobald der Gastbenutzer eine Zuweisung hergestellt hat, wird er in den Ausführungsstatus "WEB_AUTH_REQ" versetzt, bis der Client über das IPv4- oder IPv6-Captive-Portal authentifiziert wird. Der Controller fängt in diesem Zustand sowohl IPv4- als auch IPv6-HTTP-/HTTPS-Datenverkehr ab und leitet ihn an die virtuelle IP-Adresse des Controllers weiter. Nachdem der Benutzer über das Captive Portal authentifiziert wurde, wird seine MAC-Adresse in den Ausführungsstatus versetzt, und sowohl IPv4- als auch IPv6-Datenverkehr wird weitergeleitet. Für die externe Webauthentifizierung ermöglicht die

Zugriffskontrollliste vor der Authentifizierung die Verwendung eines externen Webservers.

Um die Umleitung von Nur-IPv6-Clients zu unterstützen, erstellt der Controller automatisch eine virtuelle IPv6-Adresse, die auf der auf dem Controller konfigurierten virtuellen IPv4-Adresse basiert. Die virtuelle IPv6-Adresse entspricht der Konvention von `[::ffff:<virtuelle IPv4-Adresse>]`. Beispiel: Eine virtuelle IP-Adresse von 1.1.1.1 wird in `[::ffff:1.1.1.1]` übersetzt.

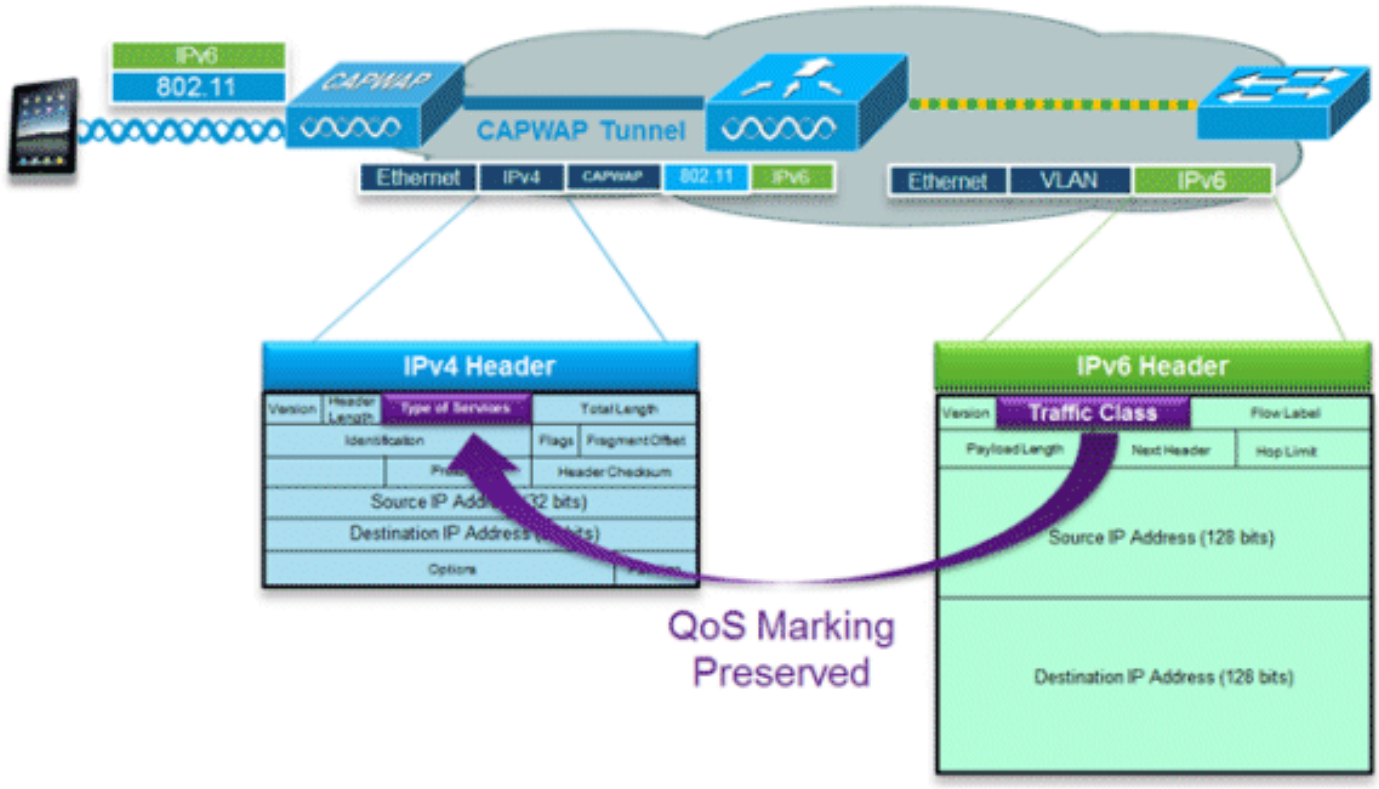
Wenn Sie ein vertrauenswürdiges SSL-Zertifikat für die Authentifizierung des Gastzugriffs verwenden, stellen Sie sicher, dass sowohl die IPv4- als auch die IPv6-Adresse des Controllers in DNS definiert sind, damit sie mit dem Hostnamen des SSL-Zertifikats übereinstimmen. Dadurch wird sichergestellt, dass Clients keine Sicherheitswarnung erhalten, die besagt, dass das Zertifikat nicht mit dem Hostnamen des Geräts übereinstimmt.

Hinweis: Das automatisch generierte SSL-Zertifikat des Controllers enthält nicht die virtuelle IPv6-Adresse. Dies kann dazu führen, dass einige Webbrowser eine Sicherheitswarnung anzeigen. Die Verwendung eines vertrauenswürdigen SSL-Zertifikats für den Gastzugriff wird empfohlen.

IPv6-VideoStream

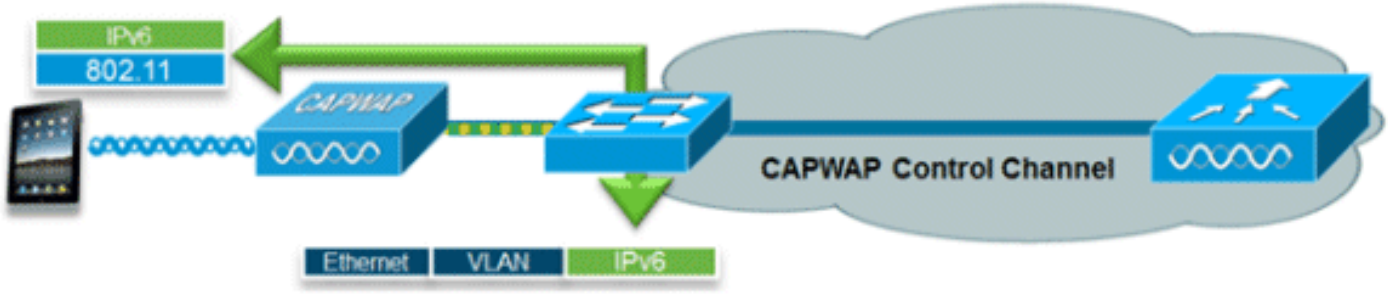
VideoStream ermöglicht eine zuverlässige und skalierbare Wireless-Multicast-Videobereitstellung, bei der jeder Client den Stream im Unicast-Format sendet. Die tatsächliche Multicast-zu-Unicast-Umwandlung (von L2) erfolgt am Access Point und stellt eine skalierbare Lösung dar. Der Controller sendet den IPv6-Videodatenverkehr innerhalb eines IPv4-CAPWAP-Multicast-Tunnels, der eine effiziente Netzwerkverteilung zum Access Point ermöglicht.

IPv6-QoS



IPv6-Pakete weisen eine ähnliche Markierung auf wie DSCP-Werte von IPv4, wodurch bis zu 64 verschiedene Datenverkehrsklassen (0-63) unterstützt werden. Bei Downstream-Paketen aus dem kabelgebundenen Netzwerk wird der Wert der IPv6-Verkehrsklasse in den Header des CAPWAP-Tunnels kopiert, um sicherzustellen, dass die durchgängige QoS erhalten bleibt. In Upstream-Richtung gilt das Gleiche, wie Client-Datenverkehr, der auf Layer 3 mit der IPv6-Datenverkehrsklasse markiert ist, durch Markierung der CAPWAP-Pakete für den Controller berücksichtigt wird.

IPv6 und FlexConnect



FlexConnect - Local Switching WLANs

FlexConnect im lokalen Switching-Modus unterstützt IPv6-Clients durch Bridging des Datenverkehrs zum lokalen VLAN, ähnlich dem IPv4-Betrieb. Client-Mobilität wird für Layer-2-Roaming in der gesamten FlexConnect-Gruppe unterstützt.

Diese IPv6-spezifischen Funktionen werden im lokalen FlexConnect-Switching-Modus unterstützt:

- IPv6 RA Guard
- IPv6-Bridging
- IPv6-Gastauthentifizierung (vom Controller gehostet)

Diese IPv6-spezifischen Funktionen werden im lokalen FlexConnect-Switching-Modus nicht unterstützt:

- Layer-3-Mobilität
- IPv6-VideoStream
- IPv6-Zugriffskontrolllisten
- IPv6 Source Guard
- DHCPv6-Serverschutz
- Caching zur Ermittlung von Netznachbarn
- Drosselung der Router-Ankündigung

FlexConnect - WLANs für zentrale Switches

Für APs im FlexConnect-Modus mit zentralem Switching (Tunneling-Datenverkehr zurück zum Controller) muss der Controller im "AP Multicast Mode" auf "Multicast - Unicast Mode" gesetzt werden. Da FlexConnect-APs nicht der CAPWAP-Multicast-Gruppe des Controllers angehören, müssen Multicast-Pakete auf dem Controller repliziert und an jeden AP einzeln übertragen werden. Diese Methode ist weniger effizient als "Multicast - Multicast Mode" und belastet den Controller zusätzlich.

Diese IPv6-spezifische Funktion wird im FlexConnect Central Switching Mode nicht unterstützt:

- IPv6-VideoStream

Hinweis: Zentrale WLANs mit IPv6 werden auf dem Flex Controller der Serie 7500 nicht unterstützt.

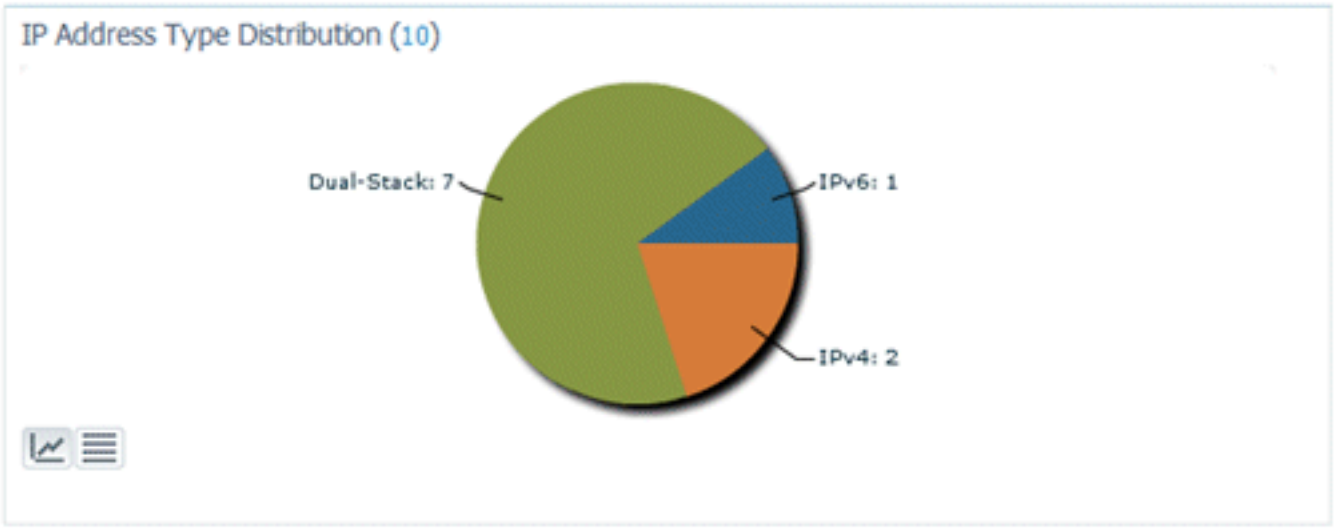
IPv6-Client-Transparenz mit NCS

Mit der Einführung von NCS v1.1 wurden zahlreiche zusätzliche IPv6-spezifische Funktionen hinzugefügt, um ein Netzwerk von IPv6-Clients in kabelgebundenen und Wireless-Netzwerken zu überwachen und zu verwalten.

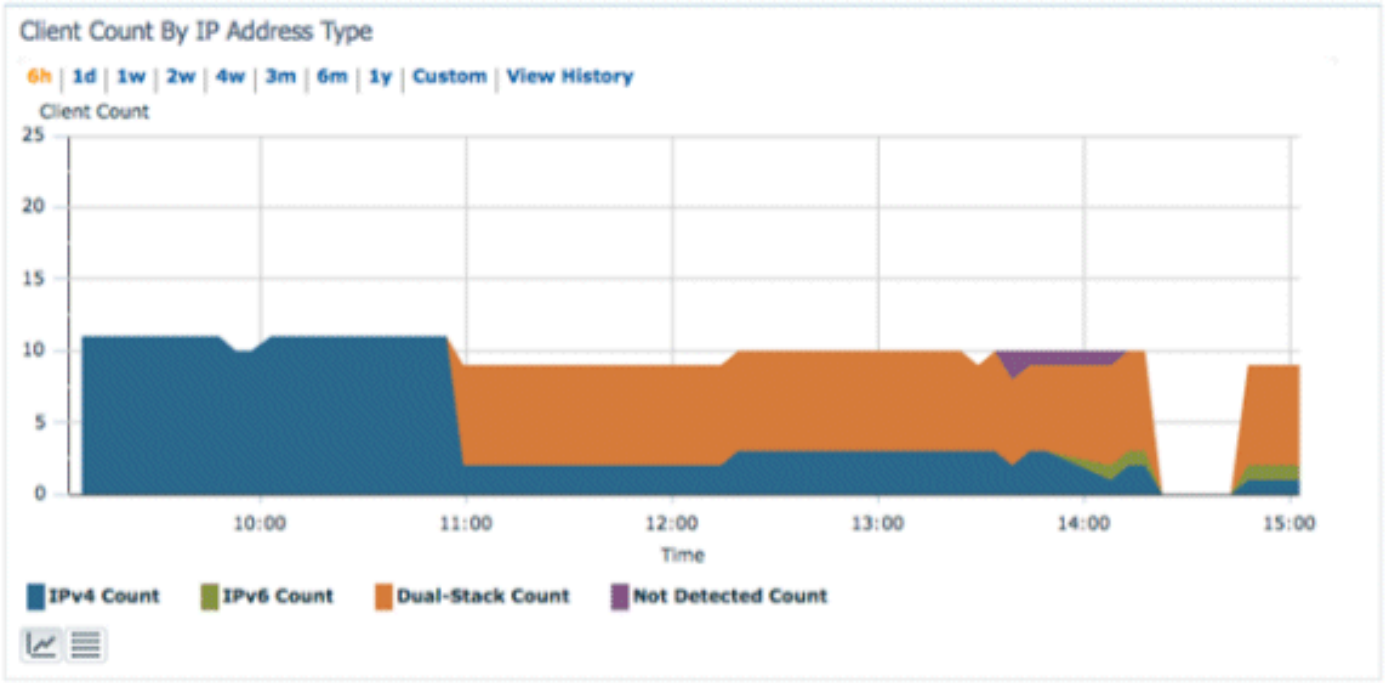
IPv6-Dashboard-Elemente

Um festzustellen, welche Clienttypen im Netzwerk vorhanden sind, steht im NCS ein "Dashlet" zur Verfügung, das Einblicke in IPv6-spezifische Statistiken bietet und detaillierte Informationen zu IPv6-Clients bereitstellt.

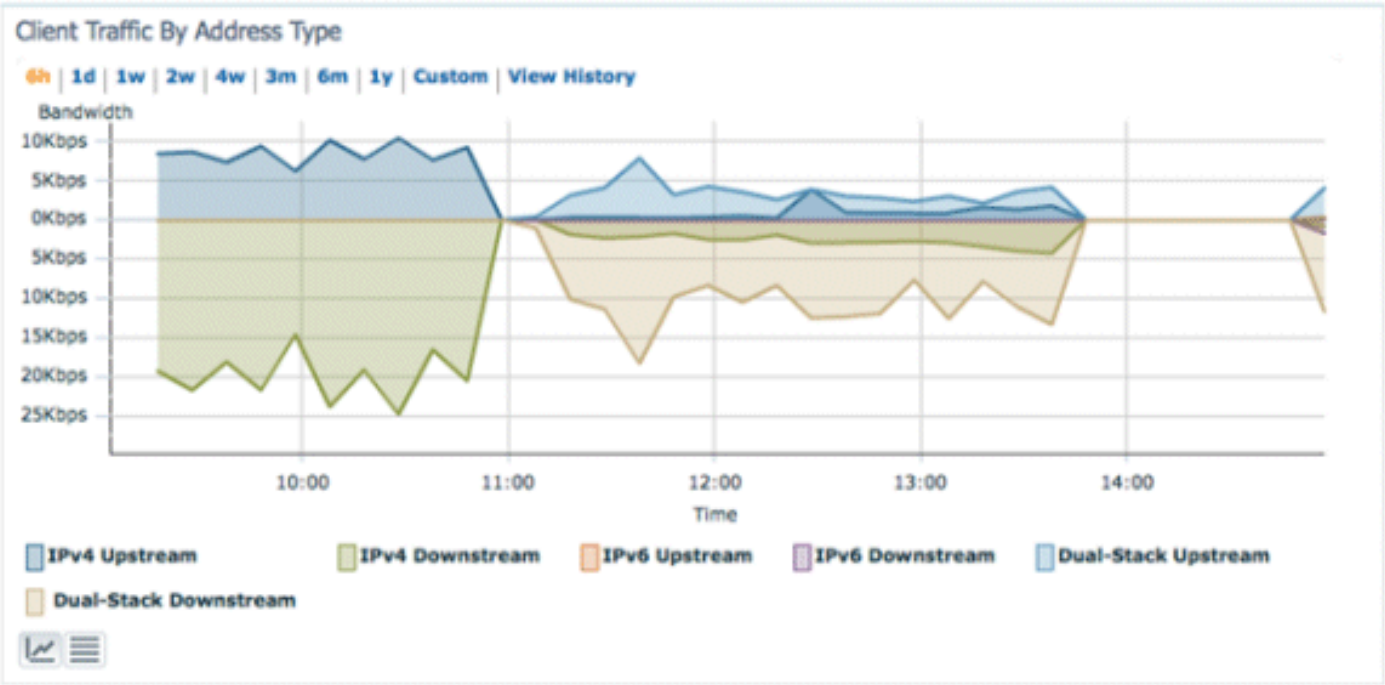
IP Address Type Dashlet - Zeigt die Typen der IP-Clients im Netzwerk an:



Client Count by IP Address Type (Client-Anzahl nach IP-Adresstyp): Zeigt den IP-Client-Typ im Zeitverlauf an:



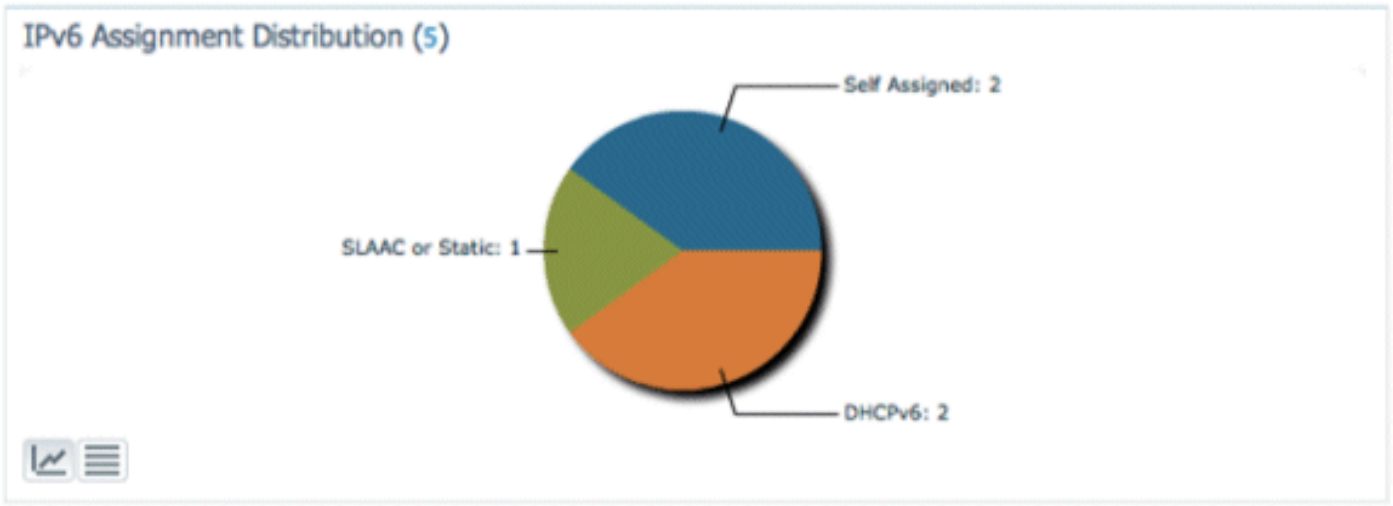
Client-Datenverkehr nach IP-Adresstyp - Zeigt den Datenverkehr von jedem Client-Typ an. Clients in der Dual-Stack-Kategorie umfassen sowohl IPv4- als auch IPv6-Datenverkehr:



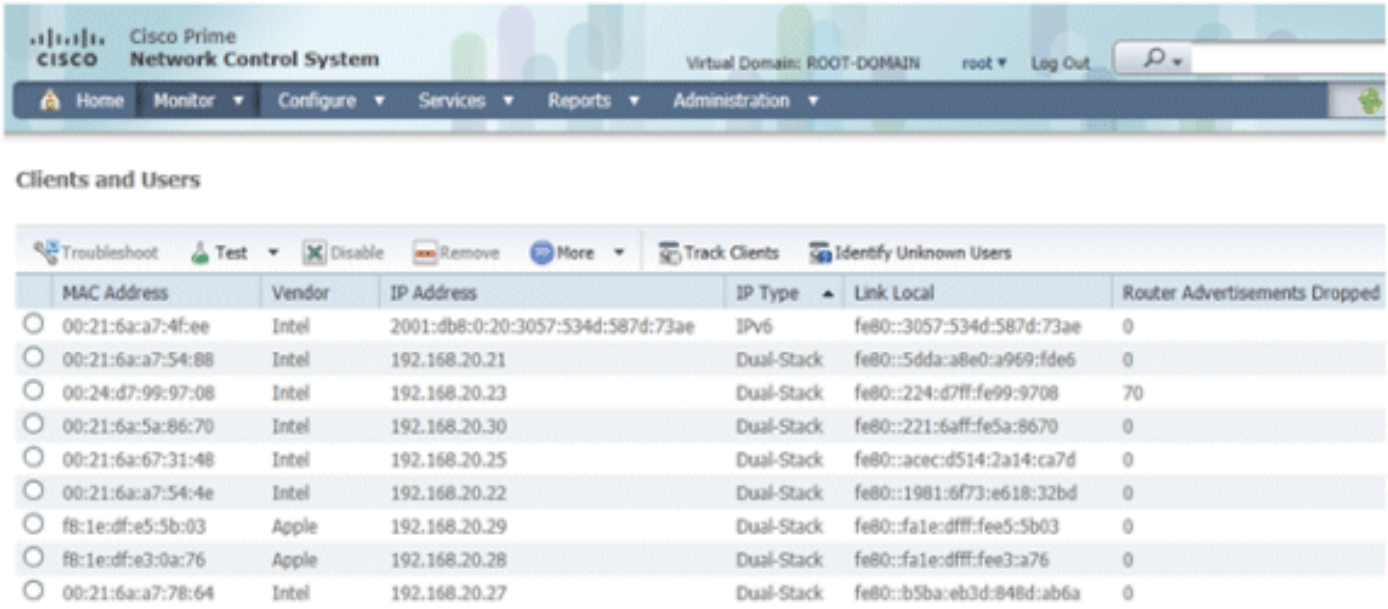
IPv6 Address Assignment (IPv6-Adressenzuweisung): Zeigt die Methode der Adressenzuweisung für jeden Client als eine der folgenden vier Kategorien an:

- DHCPv6 - Für Clients mit von einem zentralen Server zugewiesenen Adressen. Der Client verfügt möglicherweise auch über eine SLAAC-Adresse.
- SLAAC oder Statisch - Für Clients, die die automatische Zuweisung von zustandslosen Adressen oder die Verwendung statisch konfigurierter Adressen verwenden.
- Unbekannt - In einigen Fällen kann die IPv6-Adresszuweisung nicht erkannt werden.Diese Bedingung tritt nur bei kabelgebundenen Clients im NCS auf, da einige Switches keine IPv6-Adresszuordnungsinformationen abfragen.
- Selbst zugewiesen - Für Clients mit nur einer Link-Local-Adresse, die vollständig selbst zugewiesen ist.Clients in dieser Kategorie können IPv6-Verbindungsprobleme haben, da sie keine eindeutige globale oder lokale Adresse haben.

Auf jeden Abschnitt des Tortendiagramms kann geklickt werden, wodurch der Administrator einen Drilldown zu einer Liste von Clients durchführen kann.



Überwachung von IPv6-Clients



Um IPv6-Client-Informationen zu überwachen und zu verwalten, wurden die folgenden Spalten auf der Seite Clients und Benutzer hinzugefügt:

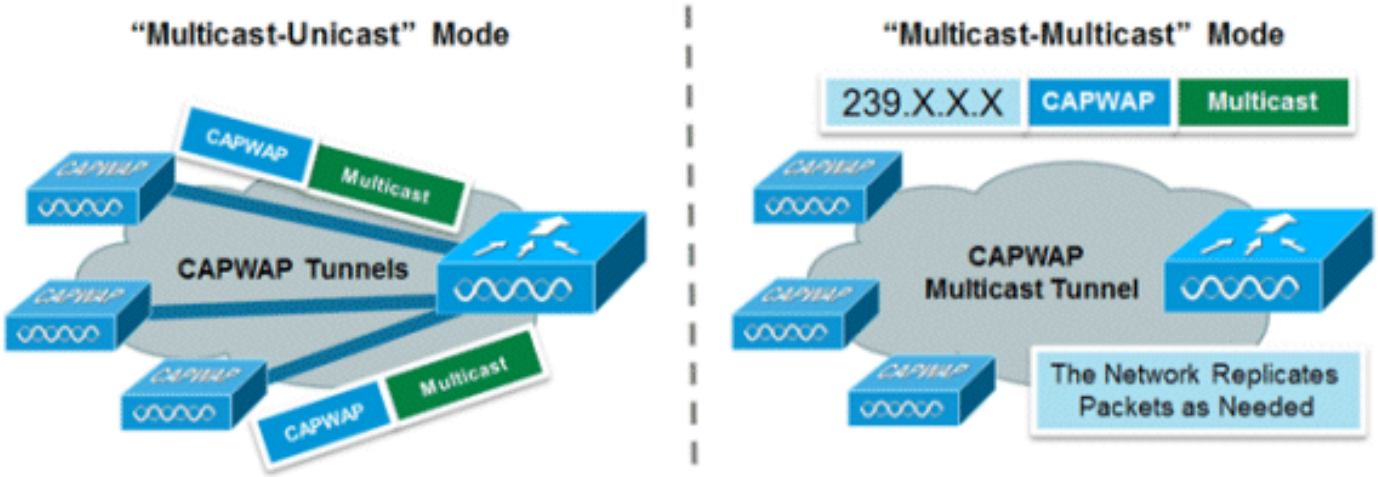
- IP Type (IP-Typ): Der Client-Typ, der auf den vom Client erkannten IP-Adressen basiert. Die möglichen Optionen sind IPv4, IPv6 oder Dual-Stack, was bedeutet, dass ein Client sowohl über IPv4- als auch über IPv6-Adressen verfügt.
- IPv6 Assignment Type (IPv6-Zuweisungstyp) - Die Adressenzuweisungsmethode wird vom NCS entweder als SLAAC oder Statisch, DHCPv6, Selbst zugewiesen oder Unbekannt erkannt.
- Global Unique - Die neueste globale IPv6-Adresse, die vom Client verwendet wird. Ein Mauszeiger über den Spalteninhalt zeigt alle zusätzlichen globalen eindeutigen IPv6-Adressen an, die vom Client verwendet werden.
- Local Unique (Lokal eindeutig) - Die neueste vom Client verwendete lokale IPv6-Adresse. Wenn Sie den Mauszeiger über den Spalteninhalt bewegen, werden alle zusätzlichen globalen eindeutigen IPv6-Adressen angezeigt, die vom Client verwendet werden.
- Link Local (Lokal verknüpfen) - Die IPv6-Adresse des Clients, der selbst zugewiesen ist und für die Kommunikation verwendet wird, bevor eine andere IPv6-Adresse zugewiesen wird.
- Verworfene Routerankündigungen - Die Anzahl der Routerankündigungen, die vom Client gesendet und am Access Point verworfen wurden. Diese Spalte kann zum Aufspüren von Clients verwendet werden, die möglicherweise falsch konfiguriert oder böswillig so konfiguriert sind, dass sie wie ein IPv6-Router funktionieren. Diese Spalte ist sortierbar, was die einfache Identifizierung von Clients ermöglicht, die einen Angriff auslösen.

Zusätzlich zur Anzeige von IPv6-spezifischen Spalten zeigt die Spalte "IP Address" (IP-Adresse) die aktuelle IP-Adresse des Clients mit einer Priorität an, um zuerst die IPv4-Adresse anzuzeigen (bei einem Dual-Stack-Client), oder die IPv6 Global Unique-Adresse (bei einem Nur-IPv6-Client).

Konfiguration für die Unterstützung von Wireless-IPv6-Clients

Multicast-Verteilungsmodus an APs

Das Cisco Unified Wireless Network unterstützt zwei Methoden der Multicast-Verteilung an die APs, die dem Controller zugeordnet sind. In beiden Modi wird das ursprüngliche Multicast-Paket aus dem kabelgebundenen Netzwerk in ein Layer-3-CAPWAP-Paket gekapselt, das entweder über CAPWAP-Unicast oder über Multicast an den AP gesendet wird. Da der Datenverkehr CAPWAP-gekapselt ist, müssen sich die Access Points nicht im selben VLAN wie der Client-Datenverkehr befinden. Hier werden die beiden Methoden der Multicast-Verteilung verglichen:



	Multicast-Unicast-Modus	Multicast-Multicast-Modus
Liefermechanismus	Der Controller repliziert das Multicast-Paket und sendet es in einem Unicast-CAPWAP-Tunnel an jeden AP.	Der Controller sendet eine Kopie des Multicast-Pakets.
Unterstützte AP-Modi	FlexConnect und lokal	Nur lokaler Modus
Erfordert L3-Multicast-Routing in einem kabelgebundenen Netzwerk	Nein	Ja
Controller wird geladen	Hoch	Niedrig
Laden kabelgebundener Netzwerke	Hoch	Niedrig

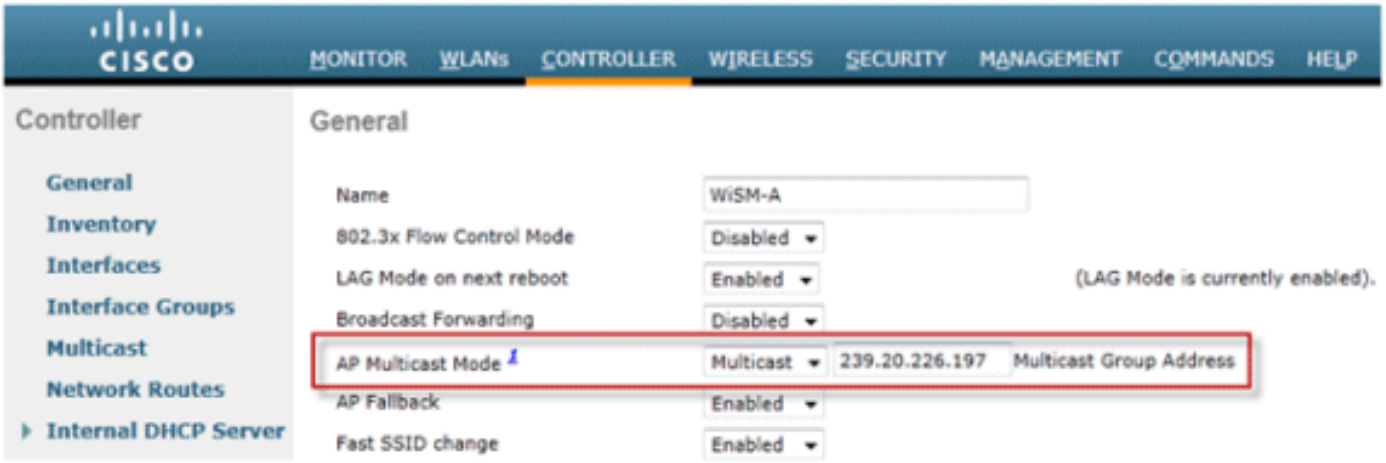
Konfigurieren des Multicast-Multicast-Verteilungsmodus

Aus Gründen der Skalierbarkeit und der kabelgebundenen Bandbreiteneffizienz wird der Multicast-

Multicast-Modus empfohlen.

Hinweis: Dieser Schritt ist nur für die Wireless-Controller der Serie 2500 zwingend erforderlich. Er ermöglicht jedoch eine effizientere Multicast-Übertragung und wird für alle Controller-Plattformen empfohlen.

Öffnen Sie die Registerkarte "Controller" auf der Seite "Allgemein", und stellen Sie sicher, dass der AP-Multicast-Modus für die Verwendung des **Multicast-**Modus konfiguriert und eine gültige Gruppenadresse konfiguriert ist. Die Gruppenadresse ist eine IPv4-Multicast-Gruppe und sollte im Bereich 239.X.X.X-239.255.255.255 liegen, der für private Multicast-Anwendungen gilt.

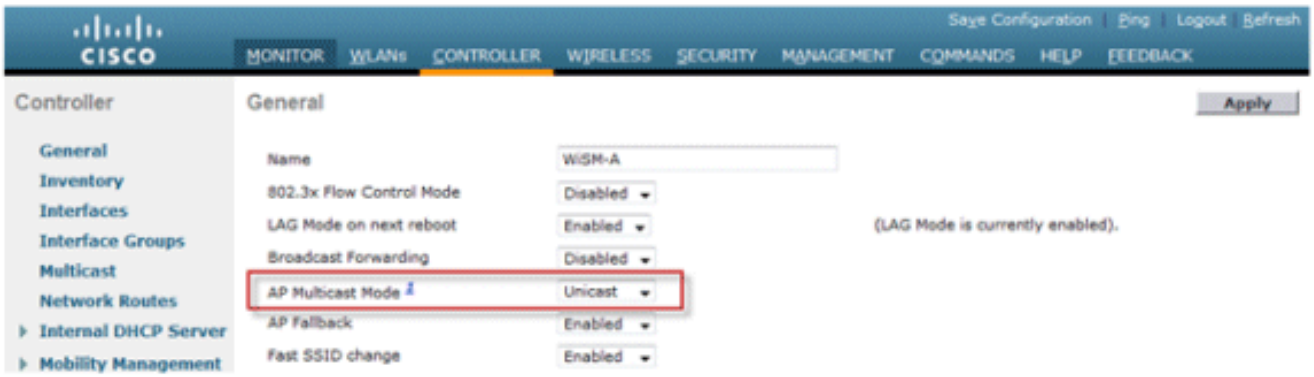


Hinweis: Verwenden Sie nicht die Adressbereiche 224.X.X.X, 239.0.0.X oder 239.128.0.X für die Multicast-Gruppenadresse. Die Adressen in diesen Bereichen überlappen sich mit den lokalen MAC-Adressen der Verbindungen und fluten alle Switch-Ports, selbst wenn IGMP-Snooping aktiviert ist.

Konfigurieren des Multicast-Unicast-Verteilungsmodus

Wenn das kabelgebundene Netzwerk nicht richtig konfiguriert ist, um CAPWAP-Multicast zwischen dem Controller und dem AP- oder FlexConnect-Modus bereitzustellen, und die APs für zentral geschaltete WLANs verwendet werden, die IPv6 unterstützen, ist der Unicast-Modus erforderlich.

1. Öffnen Sie die Registerkarte **Controller** im Register Allgemein, und stellen Sie sicher, dass der AP-Multicast-Modus für die Verwendung des **Unicast-**Modus konfiguriert ist.



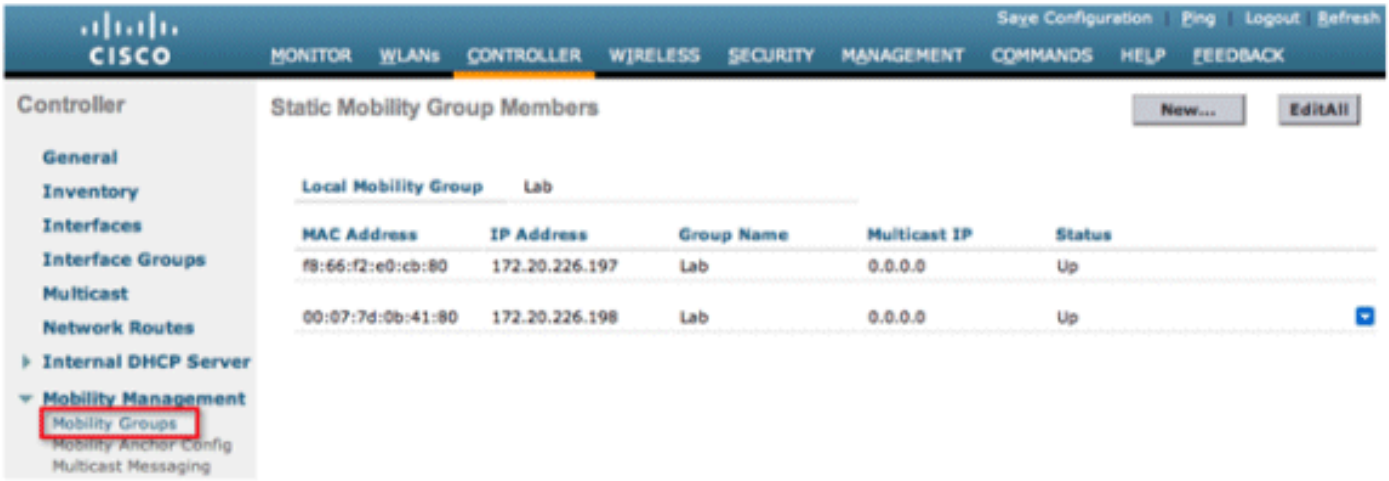
2. Verbinden Sie einen IPv6-fähigen Client mit dem WLAN. Überprüfen Sie, ob der Client eine IPv6-Adresse empfängt, indem Sie zur Registerkarte **Monitor** und dann zum Menü **Clients**

navigieren.

IPv6-Mobilität konfigurieren

Es gibt keine spezielle Konfiguration für IPv6-Mobilität, außer dass Controller in derselben Mobilitätsgruppe oder innerhalb derselben Mobilitätsdomäne angeordnet sind. Damit können insgesamt bis zu 72 Controller in einer Mobilitätsdomäne zusammengefasst werden, die selbst den größten Campus mit nahtloser Mobilität ausstattet.

Öffnen Sie die Registerkarte **Controller > Mobility Groups**, und fügen Sie jeden Controller nach MAC-Adresse und IP-Adresse zur Gruppe hinzu. Dies muss auf allen Controllern der Mobilitätsgruppe erfolgen.

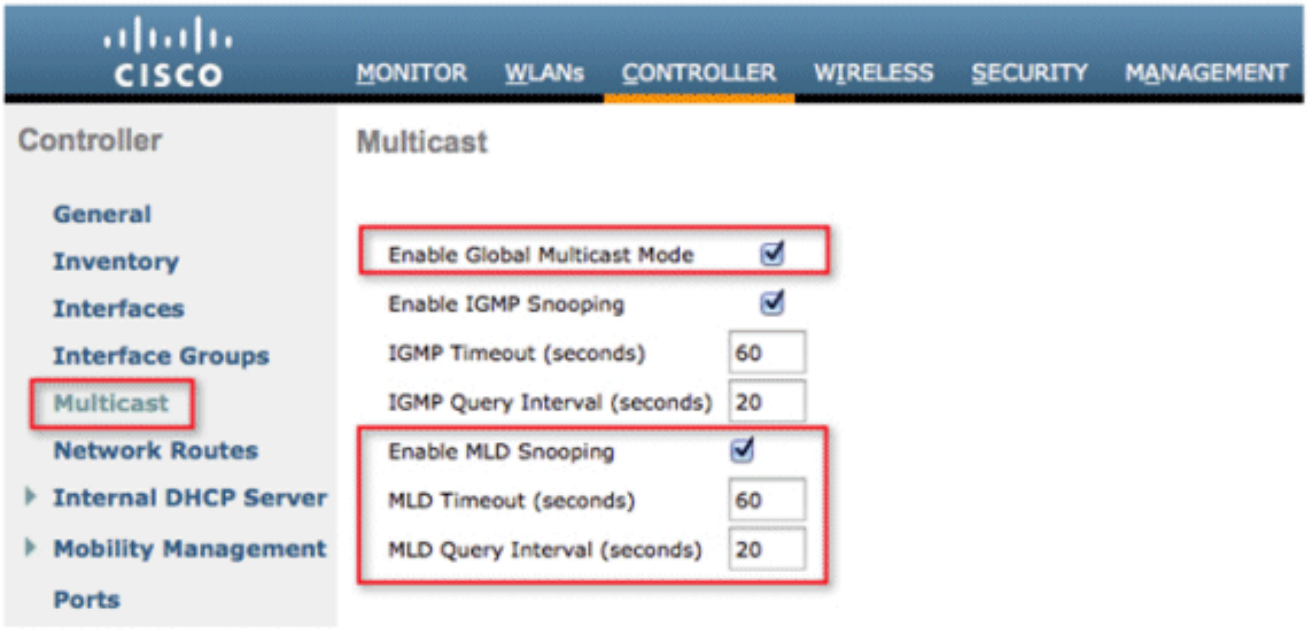


Konfigurieren von IPv6 Multicast

Der Controller unterstützt MLDv1-Snooping für IPv6-Multicast, wodurch er auf intelligente Weise den Überblick über Multicast-Datenflüsse behalten und diese an Clients weiterleiten kann, die sie anfordern.

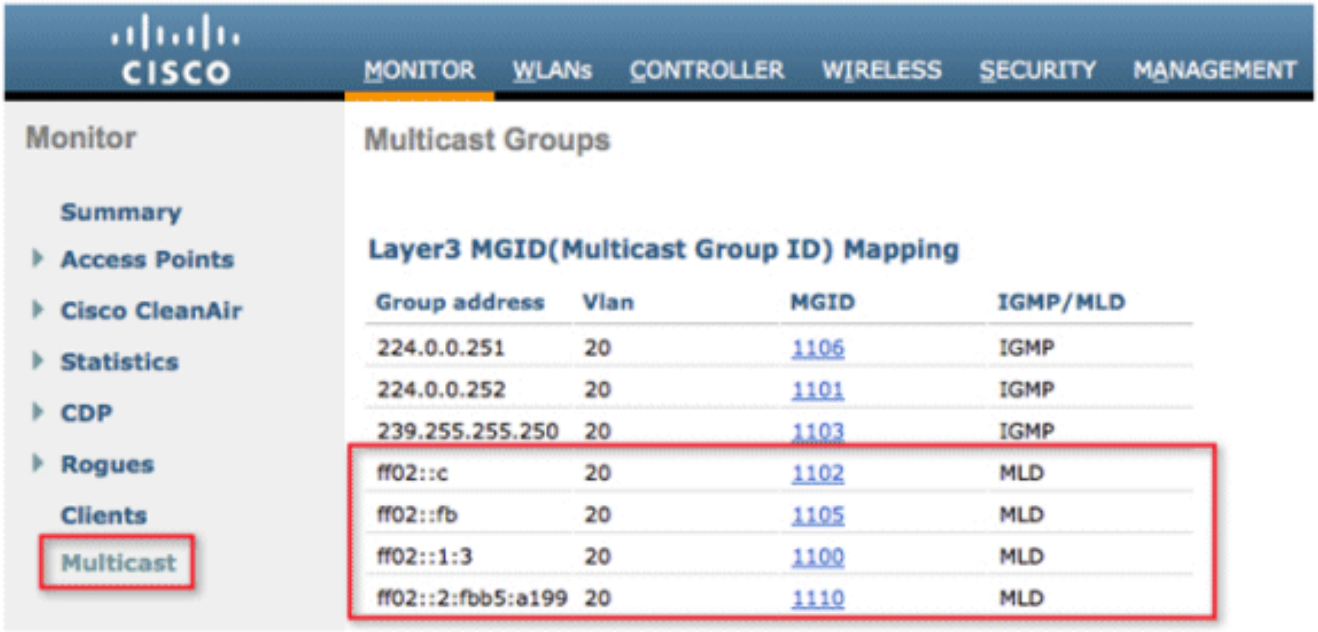
Hinweis: Anders als bei früheren Versionen von wird bei der Unterstützung von IPv6-Unicast-Datenverkehr nicht die Aktivierung des "globalen Multicast-Modus" auf dem Controller verlangt. Die Unterstützung für IPv6-Unicast-Datenverkehr wird automatisch aktiviert.

1. Gehen Sie zur Registerkarte **Controller** > **Multicast**-Seite, und **aktivieren Sie MLD-Snooping**, um Multicast-IPv6-Datenverkehr zu unterstützen. Damit IPv6-Multicast aktiviert werden kann, muss auch der **globale Multicast-Modus** des Controllers aktiviert sein.



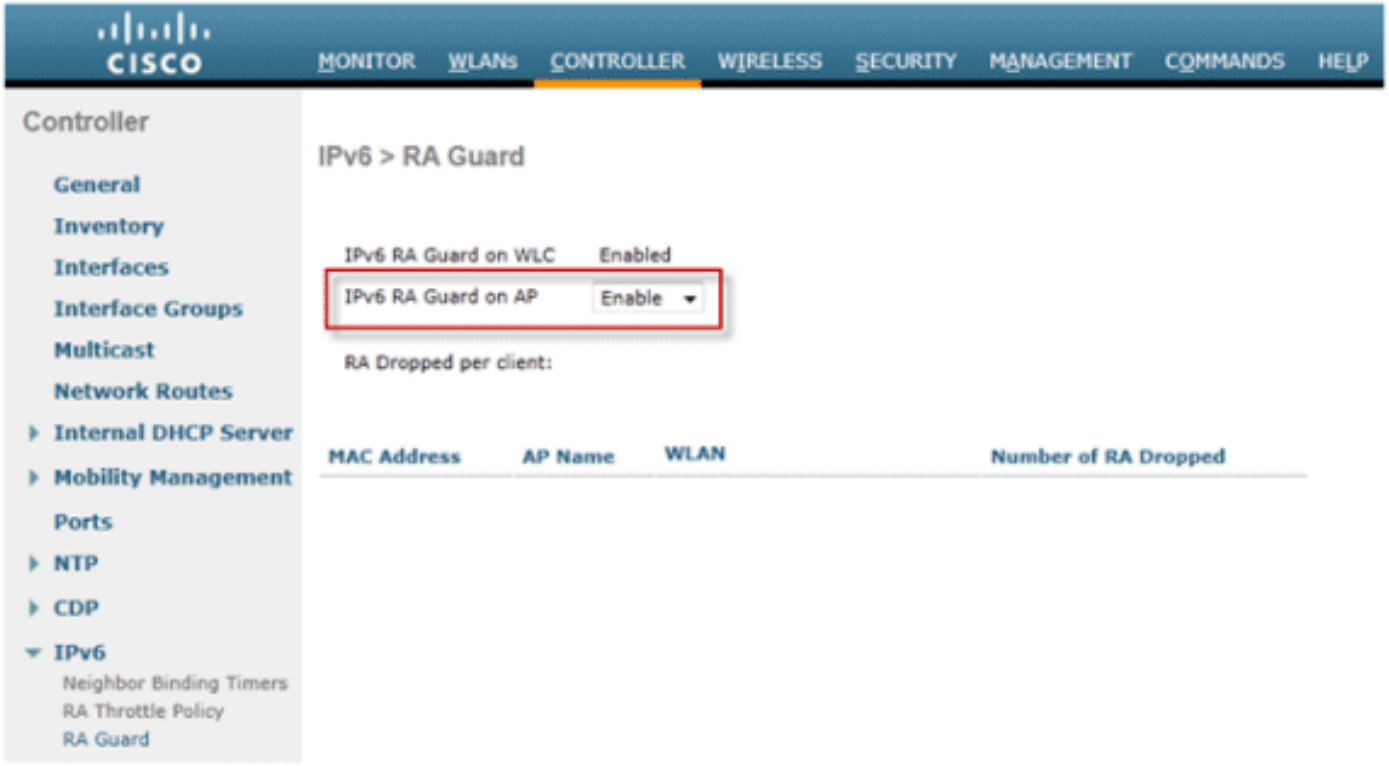
Hinweis: Wenn Peer-to-Peer-Erkennungsanwendungen wie Apple Bonjour erforderlich sind, sollten der globale Multicast-Modus, IGMP und MLD-Snooping aktiviert werden.

2. Um sicherzustellen, dass IPv6-Multicast-Datenverkehr überwacht wird, wechseln Sie zur Registerkarte **Monitor** und zur Seite **Multicast**. Beachten Sie, dass sowohl IPv4 (IGMP)- als auch IPv6 (MLD)-Multicast-Gruppen aufgeführt werden. Klicken Sie auf die MGID, um die Wireless-Clients anzuzeigen, die dieser Gruppenadresse angehören.



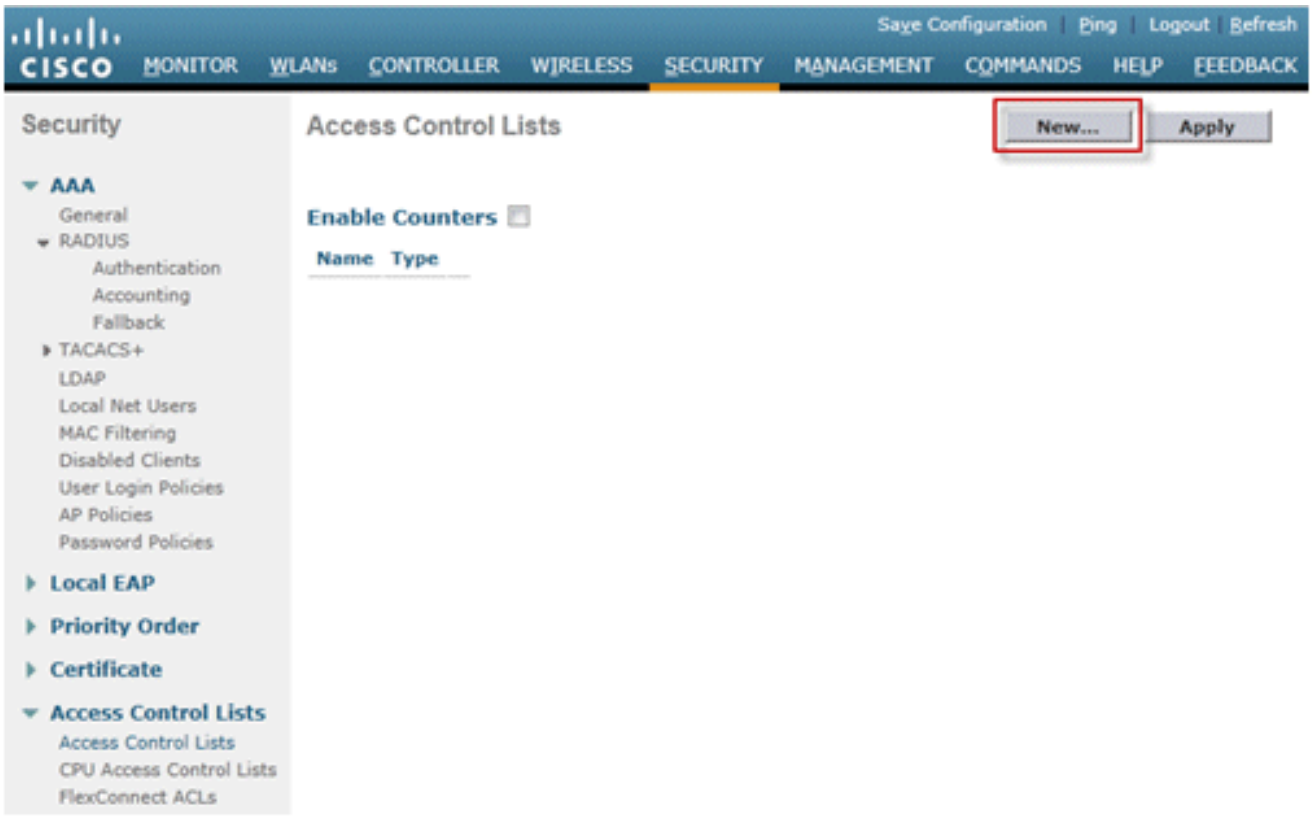
Konfigurieren von IPv6 RA Guard

Navigieren Sie zur Registerkarte **Controller** und dann im Menü auf der linken Seite zu **IPv6 > RA Guard**. **Aktivieren Sie** IPv6 RA Guard auf dem Access Point. RA Guard auf dem Controller kann nicht deaktiviert werden. Zusätzlich zur RA Guard-Konfiguration werden auf dieser Seite auch alle Clients angezeigt, die RAs senden.



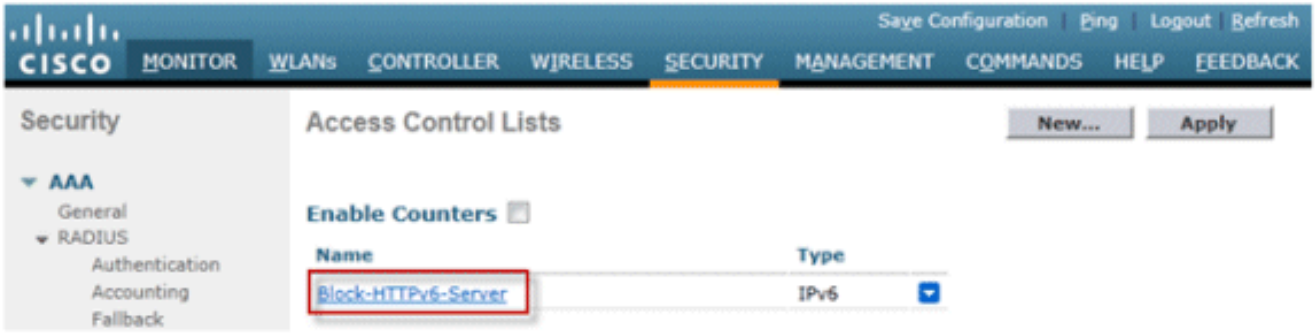
Konfigurieren von IPv6-Zugriffskontrolllisten

1. Öffnen Sie die Registerkarte **Sicherheit**, öffnen Sie **Zugriffskontrolllisten,** und klicken Sie auf **Neu**.

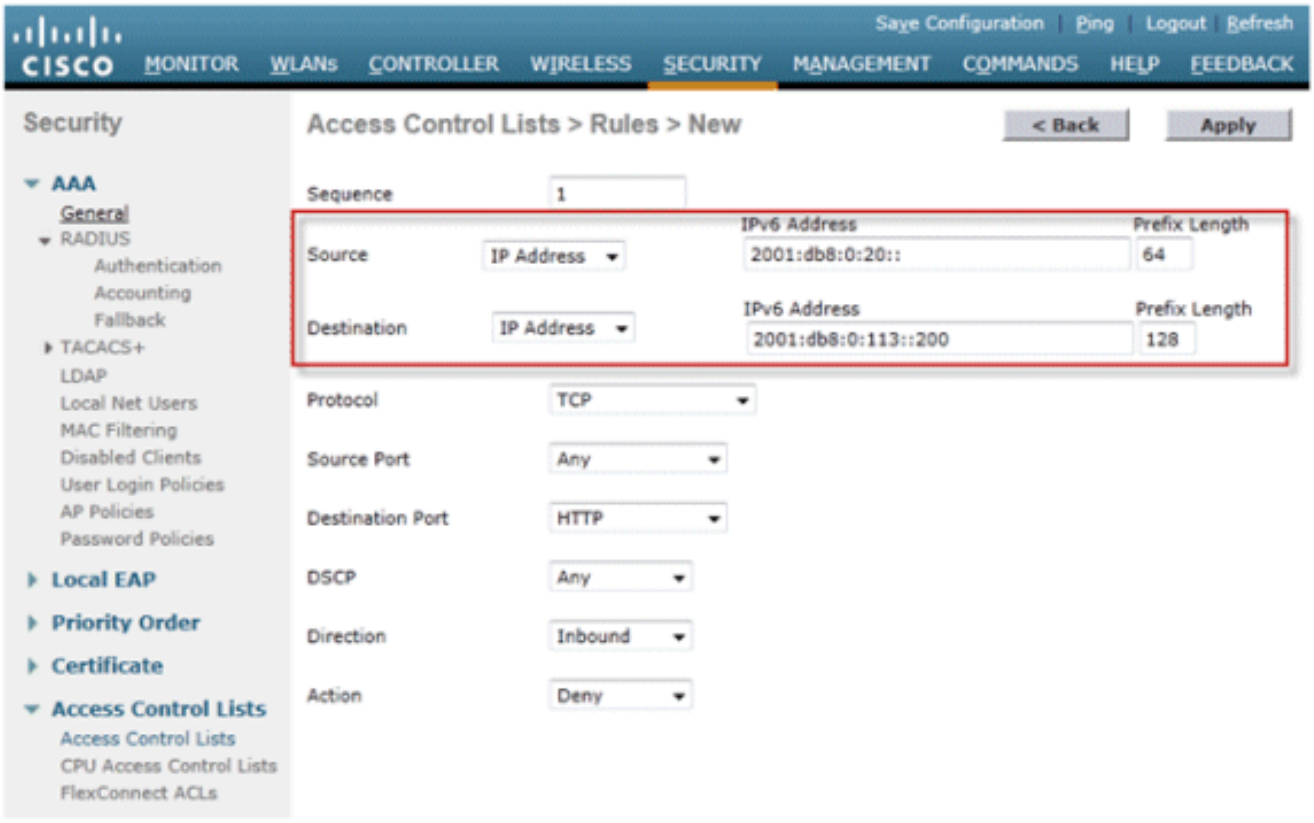


2. Geben Sie einen eindeutigen Namen für die ACL ein, ändern Sie den ACL-Typ in **IPv6**, und klicken Sie auf
Apply.

3. Klicken Sie auf die neue ACL, die mit den obigen Schritten erstellt wurde.

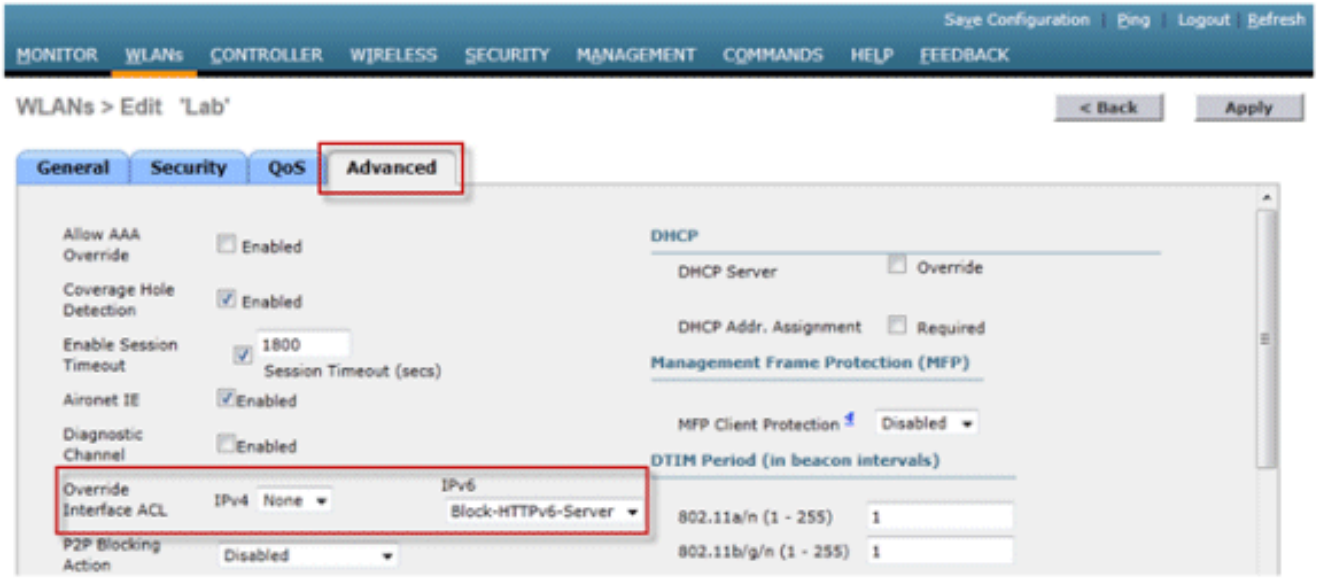


4. Klicken Sie auf **Neue Regel hinzufügen**, geben Sie die gewünschten Parameter für die Regel ein, und klicken Sie auf **Anwenden**. Lassen Sie das Feld leer, um die Regel am Ende der Liste anzuzeigen. Die Option "Direction" (Richtung) von "Inbound" (Eingehend) wird für Datenverkehr aus dem Wireless-Netzwerk und "Outbound" (Ausgehend) für Datenverkehr von Wireless-Clients verwendet. Denken Sie daran, dass die letzte Regel in einer ACL eine implizite "Deny-All"-Regel ist. Verwenden Sie eine Präfixlänge von 64, um ein gesamtes IPv6-Subnetz abzugleichen, und eine Präfixlänge von 128, um den Zugriff eindeutig auf eine einzelne Adresse zu beschränken.



5. IPv6-ACLs werden pro WLAN/SSID angewendet und können in mehreren WLANs

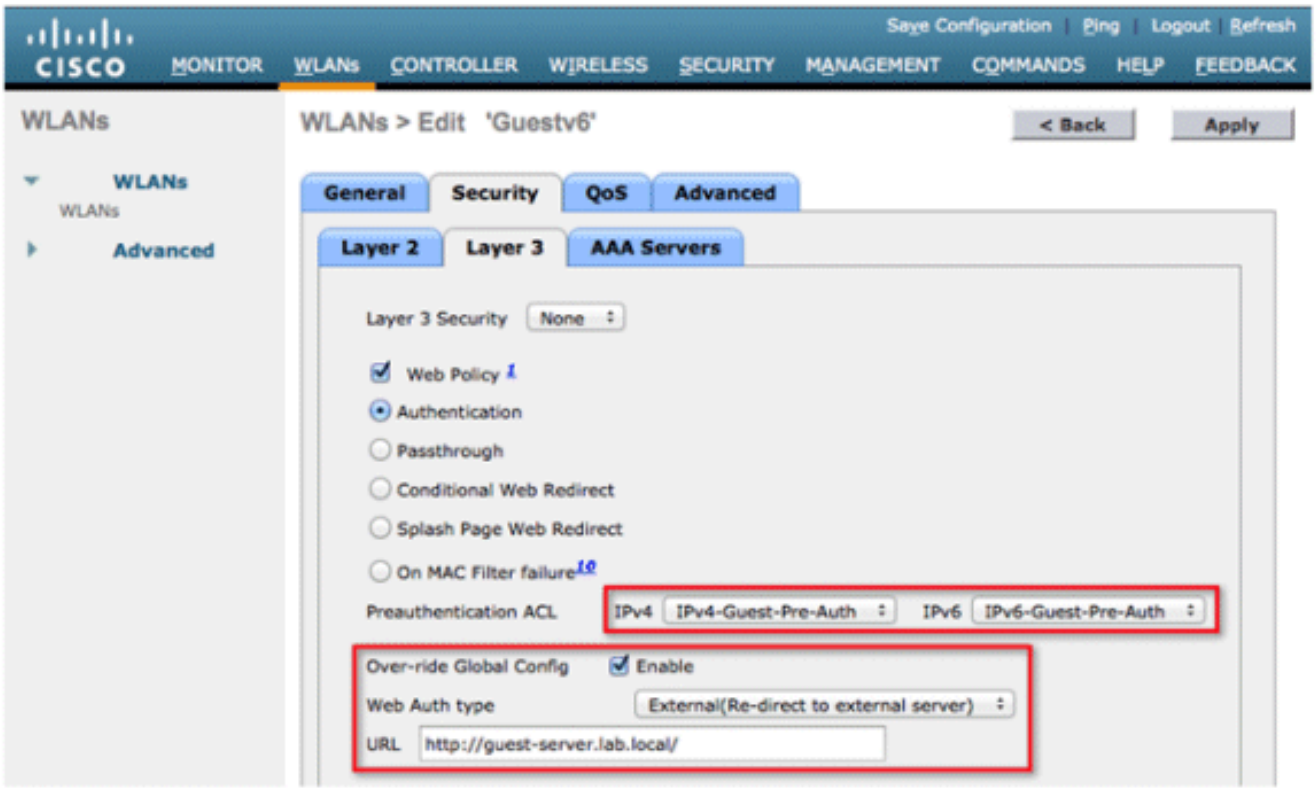
gleichzeitig verwendet werden. Navigieren Sie zur Registerkarte **WLANs**, und klicken Sie auf die WLAN-ID der betreffenden SSID, um die IPv6-ACL anzuwenden. Klicken Sie auf die Registerkarte **Advanced (Erweitert)**, und ändern Sie die Override Interface ACL (SchnittstellenACL für IPv6 überschreiben) in den Namen der ACL.



Konfigurieren von IPv6-Gastzugriff für die externe Webauthentifizierung

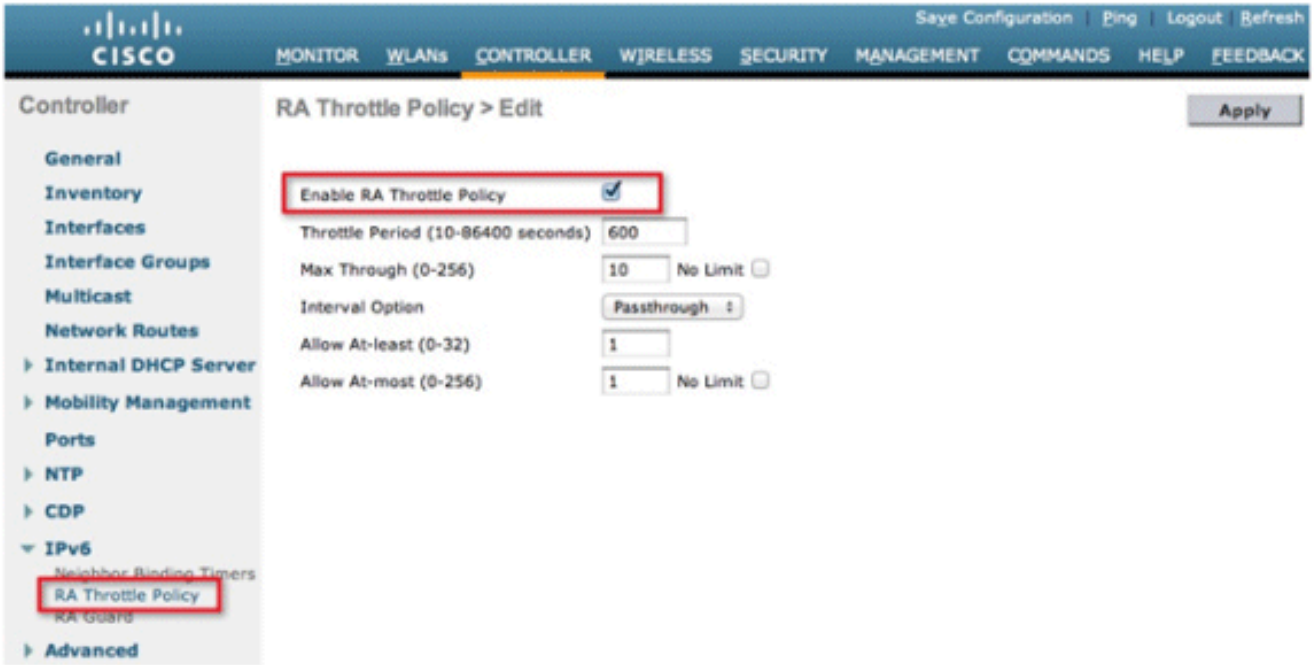
1. Konfigurieren Sie die Zugriffskontrollliste für die IPv4- und IPv6-Vorauthentifizierung für den Webserver. Dadurch wird der Datenverkehr zum und vom externen Server zugelassen, bevor der Client vollständig authentifiziert wird.

   Weitere Informationen zum Betrieb eines externen Webzugriffs finden Sie unter Konfigurationsbeispiel für externe Webauthentifizierung mit Wireless LAN-Controllern.
2. Konfigurieren Sie das Gast-WLAN, indem Sie zur Registerkarte WLANs oben navigieren. Erstellen Sie die Gast-SSID, und verwenden Sie eine Layer-3-Webrichtlinie. Die in Schritt 1 definierten ACLs vor der Authentifizierung werden für IPv4 und IPv6 ausgewählt. Aktivieren Sie den Abschnitt "Globale Konfiguration überschreiben", und wählen Sie im Dropdown-Feld "Webauthentifizierungstyp" die Option **Extern** aus. Geben Sie die URL des Webservers ein. Der Hostname des externen Servers sollte in IPv4- und IPv6-DNS auflösbar sein.



Konfigurieren der IPv6-RA-Einschränkung

1. Navigieren Sie zum Menü **Controller** auf oberster Ebene, und klicken Sie links auf die Option **IPv6 > RA Throttle Policy** (**IPv6 >** Richtlinie zur **RA-Drosselung**). Aktivieren Sie RA Throttling durch Klicken auf das Kontrollkästchen.



Hinweis: Bei einer RA-Drosselung wird nur der erste IPv6-fähige Router zugelassen. In Netzwerken mit mehreren IPv6-Präfixen, die von verschiedenen Routern bedient werden, sollte die RA-Einschränkung deaktiviert werden.

2. Die Drosselung und andere Optionen nur nach Beratung durch das TAC anpassen. Für die meisten Bereitstellungen wird jedoch die Standardeinstellung empfohlen. Die verschiedenen Konfigurationsoptionen der RA Throttling-Richtlinie sollten unter Berücksichtigung der

folgenden Punkte angepasst werden:Die numerischen Werte von "Allow At-least" sollten kleiner als "Allow At-most" sein, was kleiner als "Max Through" sein sollte.Die RA-Drosselungsrichtlinie sollte keine Drosselungsdauer von mehr als 1800 Sekunden verwenden, da dies die Standardlebensdauer der meisten RAs ist.

Jede RA-Drosselungsoption wird im Folgenden beschrieben:

- Drosselungszeitraum - Der Zeitraum, in dem die Drosselung stattfindet. Die RA-Drosselung wird erst wirksam, wenn der "Max Through"-Grenzwert für das VLAN erreicht ist.
- Max Through (Max bis) - Dies ist die maximale Anzahl von RAs pro VLAN, bevor die Drosselung beginnt. Die Option "No Limit" ermöglicht eine unbegrenzte Anzahl von RAs ohne Einschränkung.
- Intervalloption - Mit der Intervalloption kann der Controller auf Basis des in der IPv6-RA festgelegten RFC 3775-Werts unterschiedlich agieren.Passthrough: Mit diesem Wert können RAs mit einer RFC3775-Intervalloption ohne Einschränkung durchlaufen werden.Ignore (Ignorieren) - Dieser Wert bewirkt, dass der RA-Throttler Pakete mit der Option interval (Intervall) als reguläre RA behandelt und ggf. einer Drosselung unterliegt.Drossel - Dieser Wert bewirkt, dass die RAs mit der Option interval (Intervall) immer einer Ratenbeschränkung unterliegen.
- Allow Mindestens - Die Mindestanzahl an RAs pro Router, die als Multicast gesendet werden.
- Maximal zulassen - Die maximale Anzahl von RAs pro Router, die als Multicast gesendet werden, bevor die Drosselung wirksam wird. Mit der Option "No Limit" (Keine Begrenzung) kann eine unbegrenzte Anzahl von RAs für diesen Router durchgelassen werden.

Konfigurieren der Tabelle für die IPv6-Nachbar-Bindung

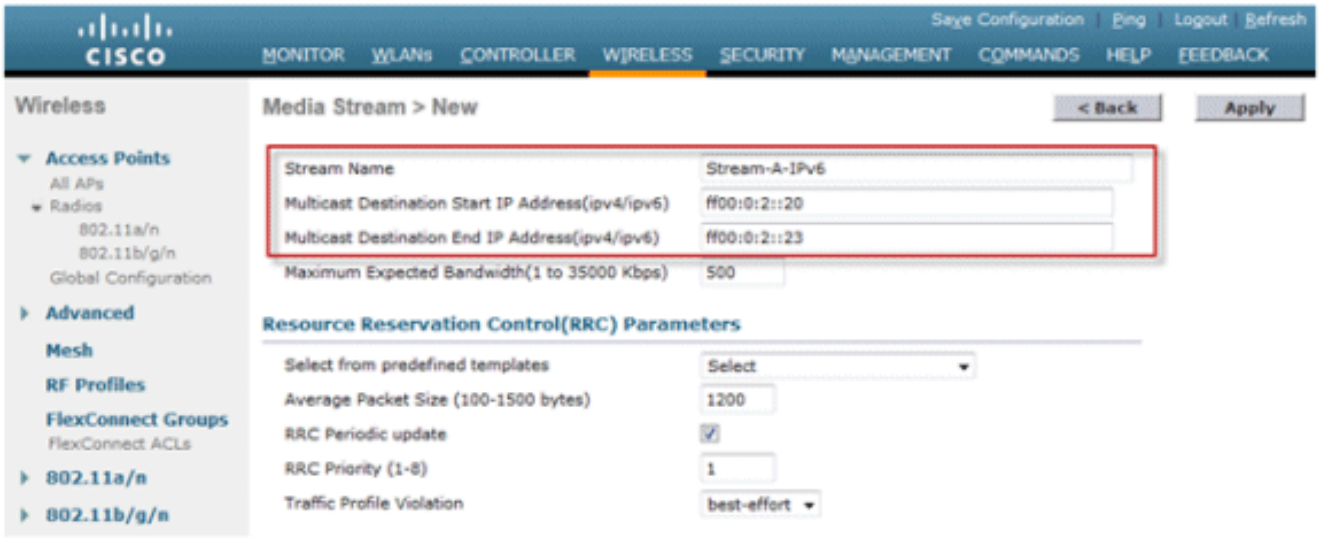
1. Gehen Sie zum Menü auf der obersten Ebene des Controllers, und klicken Sie im Menü auf der linken Seite auf **IPv6 > Neighbor Binding**
   Timers.

2. Passen Sie die Ausfallzeit, die Erreichbarkeit und die veraltete Lebensdauer je nach Bedarf an. Bei Bereitstellungen mit Clients, die hochgradig mobil sind, sollten die Timer für einen veralteten Adress-Timer angepasst werden. Empfohlene Werte:Ausfallzeit: 30 SekundenErreichbare Lebensdauer - 300 SekundenStatuslebensdauer: 86400 SekundenJeder Lebensdauertimer bezieht sich auf den Status, in dem sich eine IPv6-Adresse befinden kann:**Ausfallzeit** - Der Ausfallzeitgeber gibt an, wie lange IPv6-Cache-Einträge gespeichert werden sollen, wenn die Uplink-Schnittstelle des Controllers ausfällt.**Reachable Lifetime** (Erreichbare Lebensdauer): Dieser Timer gibt an, wie lange eine IPv6-Adresse als aktiv markiert wird, was bedeutet, dass Datenverkehr von dieser Adresse vor kurzem empfangen wurde. Nach Ablauf dieses Zeitraums wird die Adresse in den Status "Veraltet" versetzt.**Veraltete Lebensdauer** - Dieser Timer gibt an, wie lange IPv6-Adressen im Cache gespeichert werden sollen, die nicht innerhalb der "Reachable Lifetime" (Erreichbare Lebensdauer) angezeigt wurden. Nach dieser Lebensdauer wird die Adresse aus der Bindungstabelle entfernt.

Konfigurieren von IPv6 VideoStream

1. Stellen Sie sicher, dass die Global VideoStream-Funktionen auf dem Controller aktiviert sind. Weitere Informationen zur Aktivierung von VideoStream im 802.11a/g/n-Netzwerk sowie der WLAN-SSID finden Sie im Cisco Unified Wireless Network Solution: VideoStream Deployment Guide.
2. Öffnen Sie die Registerkarte **Wireless** des Controllers, und wählen Sie im Menü auf der linken Seite **Media Stream > Streams** aus. Klicken Sie auf **Add New**, um einen neuen Stream zu
erstellen.

3. Nennen Sie den Stream, und geben Sie die Start- und End-IPv6-Adresse ein. Wenn nur ein einziger Stream verwendet wird, sind Start- und Endadresse gleich. Nachdem Sie die Adressen hinzugefügt haben, klicken Sie auf **Apply**, um den Stream zu
erstellen.



Problembehandlung bei IPv6-Client-Verbindungen

Bestimmte Clients können IPv6-Datenverkehr nicht weiterleiten

Einige Client-IPv6-Netzwerk-Stack-Implementierungen melden sich nicht richtig an, wenn sie in das Netzwerk eingebunden werden, und deshalb wird ihre Adresse vom Controller nicht

entsprechend durchsucht, um in der Nachbarbindungstabelle platziert zu werden. Alle Adressen, die nicht in der Nachbar-Bindungstabelle vorhanden sind, werden entsprechend der IPv6-Funktion "Source Guard" blockiert. Damit diese Clients Datenverkehr weiterleiten können, müssen die folgenden Optionen konfiguriert werden:

1. Deaktivieren Sie die IPv6 Source Guard-Funktion über die CLI:

   config network ip-mac-binding disable

2. Aktivieren Sie die Multicast Neighbor Solicitation-Weiterleitung über die CLI:

   config ipv6 ns-mcast-fwd enable

Überprüfung des erfolgreichen Layer-3-Roaming für einen IPv6-Client:

Führen Sie die folgenden **Debug**-Befehle sowohl für den Anker als auch für den Fremdcontroller aus:

debug client

debug mobility handoff enable

debug mobility packet enable

Debugergebnisse auf Ankercontroller:

```
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
```

Debugergebnisse auf einem ausländischen Controller:

```
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
```

Nützliche IPv6-CLI-Befehle:

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

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

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

Häufig gestellte Fragen

F: Welche IPv6-Präfixgröße ist optimal, um die Broadcast-Domäne einzuschränken?

A: Obwohl ein IPv6-Subnetz unter /64 unterteilt werden kann, führt diese Konfiguration zu einer Unterbrechung der SLAAC und verursacht Probleme mit der Client-Verbindung. Wenn eine Segmentierung erforderlich ist, um die Anzahl der Hosts zu reduzieren, können mithilfe der Schnittstellengruppen Clients auf verschiedenen Back-End-VLANs mit jeweils einem anderen IPv6-Präfix verteilt werden.

Frage: Gibt es Einschränkungen hinsichtlich der Skalierbarkeit, wenn es um die Unterstützung von IPv6-Clients geht?

A: Die wichtigste Einschränkung hinsichtlich der Skalierbarkeit für die IPv6-Client-Unterstützung ist die Nachbar-Binding-Tabelle, die alle IPv6-Adressen der Wireless-Clients erfasst. Diese Tabelle wird pro Controller-Plattform skaliert, um die maximale Anzahl von Clients multipliziert mit acht (die maximale Anzahl von Adressen pro Client) zu unterstützen. Durch Hinzufügen der IPv6-Bindungstabelle kann sich die Speichernutzung des Controllers bei voller Auslastung je nach Plattform um ca. 10-15 % erhöhen.

Wireless-Controller	Maximale Anzahl Clients	Größe der IPv6-Nachbarbindungstabelle
2500	500	4,000

5500	7,000	56,000
WiSM2	15,000	120,000

F: Welche Auswirkungen haben IPv6-Funktionen auf die CPU und den Speicher des Controllers?

A: Die Auswirkungen sind minimal, da die CPU mehrere Kerne für die Verarbeitung der Kontrollebene hat. Bei Tests mit maximal unterstützten Clients mit jeweils 8 IPv6-Adressen lag die CPU-Auslastung unter 30 % und die Speichernutzung unter 75 %.

Frage: Kann die IPv6-Client-Unterstützung deaktiviert werden?

A: Kunden, die nur IPv4 in ihrem Netzwerk aktivieren und IPv6 blockieren möchten, können eine IPv6-ACL für die Ablehnung von Datenverkehr verwenden und auf WLAN-Basis anwenden.

Frage: Ist es möglich, ein WLAN für IPv4 und ein anderes für IPv6 zu nutzen?

A: Es ist nicht möglich, denselben SSID-Namen und denselben Sicherheitstyp für zwei verschiedene WLANs zu verwenden, die auf demselben WAP betrieben werden. Zur Segmentierung von IPv4-Clients von IPv6-Clients müssen zwei WLANs erstellt werden. Jedes WLAN muss mit einer ACL konfiguriert werden, die den gesamten IPv4- bzw. IPv6-Datenverkehr blockiert.

Frage: Warum ist es wichtig, mehrere IPv6-Adressen pro Client zu unterstützen?

A: Clients können mehrere IPv6-Adressen pro Schnittstelle haben, die statisch, SLAAC oder DHCPv6 zugewiesen werden können, zusätzlich zu der stets zugewiesenen Link-Local-Adresse. Clients können auch über zusätzliche Adressen mit verschiedenen IPv6-Präfixen verfügen.

F: Was sind private IPv6-Adressen und warum ist ihre Nachverfolgung wichtig?

A: Private (auch als temporäre) Adressen werden vom Client zufällig generiert, wenn die SLAAC-Adresszuweisung verwendet wird. Diese Adressen werden häufig mit einer Häufigkeit von etwa einem Tag rotiert, um die Rückverfolgbarkeit des Hosts zu verhindern, der immer den gleichen Host-Postfix (die letzten 64 Bit) verwenden würde. Es ist wichtig, diese privaten Adressen für Prüfzwecke wie die Rückverfolgung von Urheberrechtsverletzungen zu verfolgen. Das Cisco NCS zeichnet alle von den einzelnen Clients verwendeten IPv6-Adressen auf und protokolliert sie in der Vergangenheit jedes Mal, wenn der Client Roaming durchführt oder eine neue Sitzung herstellt. Diese Datensätze können auf NCS so konfiguriert werden, dass sie bis zu ein Jahr gespeichert werden.

Zugehörige Informationen

- Technischer Support und Dokumentation für Cisco Systeme

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.