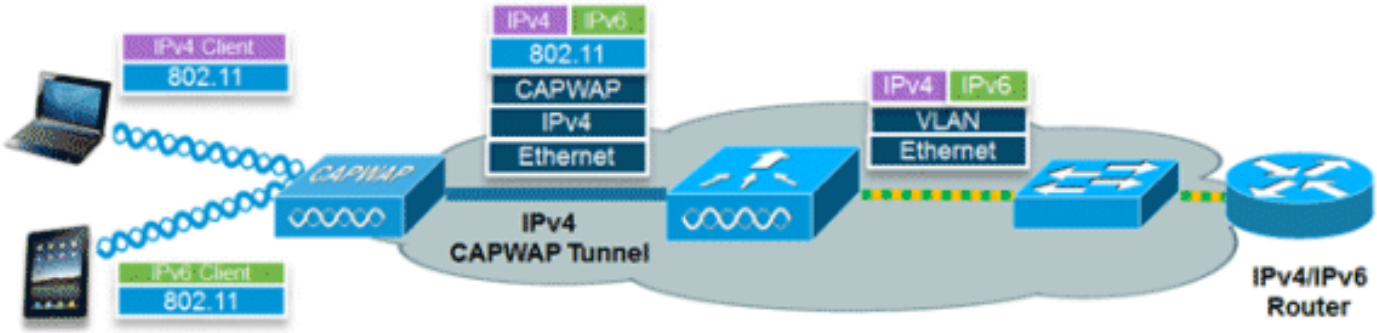
Guida all'installazione di client IPv6 per LAN wireless

Sommario

Introduzione

In questo documento viene illustrato il funzionamento e la configurazione della soluzione Cisco Unified Wireless LAN per il supporto dei client IPv6.

Connettività client wireless IPv6



La funzionalità IPv6 impostata nel software Cisco Unified Wireless Network versione 7.2 consente alla rete wireless di supportare client IPv4, Dual-Stack e solo IPv6 sulla stessa rete wireless. L'obiettivo generale dell'aggiunta del supporto client IPv6 alla LAN wireless unificata di Cisco era mantenere la parità delle funzionalità tra i client IPv4 e IPv6, inclusi mobilità, sicurezza, accesso guest, qualità del servizio e visibilità dell'endpoint.

Èpossibile tenere traccia di un massimo di otto indirizzi client IPv6 per dispositivo. In questo modo i client IPv6 possono avere un indirizzo locale del collegamento, un indirizzo SLAAC (Stateless Address Auto Configuration), un indirizzo DHCPv6 (Dynamic Host Configuration Protocol per IPv6) e persino indirizzi in prefissi alternativi su un'unica interfaccia. Anche i client WGB connessi all'uplink di un punto di accesso autonomo in modalità WGB possono supportare IPv6.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Wireless LAN Controller serie 2500, serie 5500 o WiSM2
- AP serie 1130, 1240, 1250, 1040, 1140, 1260, 3500, 3600 AP e serie 1520 o 1550 Mesh AP
- Router con supporto per IPv6

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

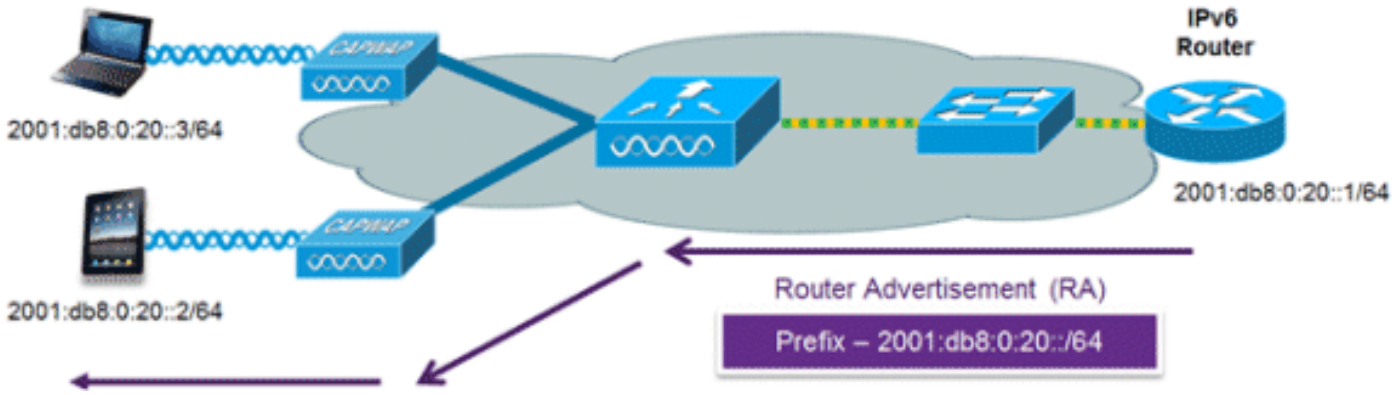
Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Prerequisiti per la connettività client IPv6 wireless

Per abilitare la connettività client IPv6 wireless, la rete cablata sottostante deve supportare il routing IPv6 e un meccanismo di assegnazione degli indirizzi, ad esempio SLAAC o DHCPv6. Il controller LAN wireless deve avere l'adiacenza L2 al router IPv6 e la VLAN deve essere contrassegnata quando i pacchetti entrano nel controller. I punti di accesso non richiedono la connettività su una rete IPv6, poiché tutto il traffico è incapsulato all'interno del tunnel CAPWAP IPv4 tra il punto di accesso e il controller.

Assegnazione indirizzo SLAAC

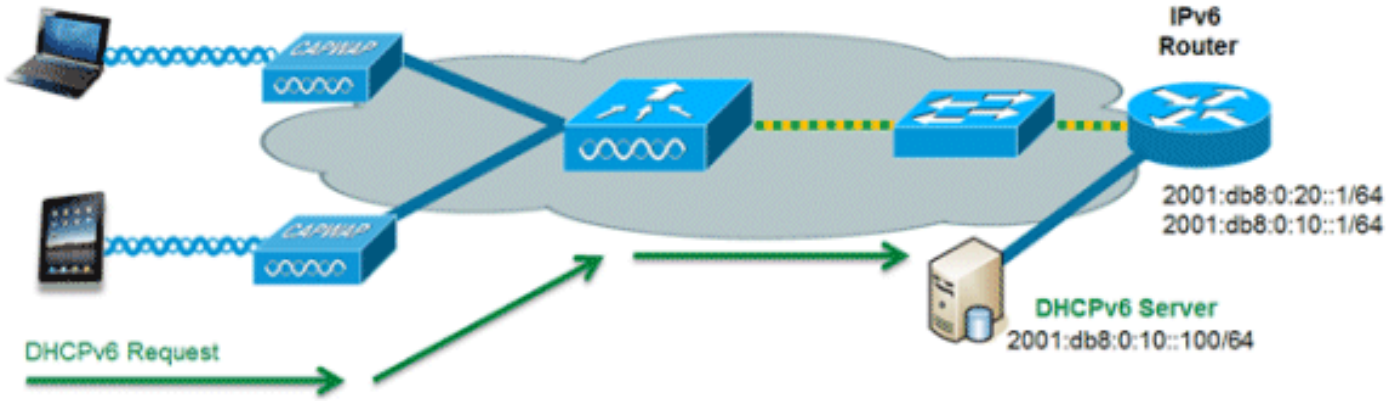


Il metodo più comune per l'assegnazione degli indirizzi dei client IPv6 è SLAAC. SLAAC offre una connettività plug-and-play semplice in cui i client assegnano automaticamente un indirizzo in base al prefisso IPv6. Questo processo viene eseguito quando il router IPv6 invia periodicamente messaggi di annuncio router che informano il client del prefisso IPv6 in uso (i primi 64 bit) e del gateway predefinito IPv6. Da quel momento, i client possono generare i restanti 64 bit del proprio indirizzo IPv6 sulla base di due algoritmi: EUI-64, basato sull'indirizzo MAC dell'interfaccia, o indirizzi privati generati in modo casuale. La scelta dell'algoritmo dipende dal client ed è spesso configurabile. Il rilevamento degli indirizzi duplicati viene eseguito dai client IPv6 per garantire che gli indirizzi casuali selezionati non entrino in conflitto con altri client. L'indirizzo del router che invia gli annunci è usato come gateway predefinito per il client.

I seguenti comandi di configurazione Cisco IOS® da un router IPv6 compatibile con Cisco vengono utilizzati per abilitare gli indirizzi SLAAC e gli annunci dei router:

```
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
```

Assegnazione indirizzo DHCPv6



L'utilizzo di DHCPv6 non è necessario per la connettività client IPv6 se SLAAC è già distribuito. Per DHCPv6 sono disponibili due modalità di funzionamento, ovvero **Stateless** e **Stateful**.

La modalità **senza stato** DHCPv6 viene utilizzata per fornire ai client informazioni di rete aggiuntive non disponibili nell'annuncio router, ma non un indirizzo IPv6, in quanto già fornito da SLAAC. Queste informazioni possono includere il nome del dominio DNS, i server DNS e altre opzioni specifiche del fornitore DHCP. Questa configurazione di interfaccia è per un router Cisco IOS IPv6 che implementa DHCPv6 senza stato con SLAAC abilitato:

```
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
```

L'opzione **Stateful di** DHCPv6, nota anche come modalità gestita, funziona in modo simile a DHCPv4 in quanto assegna indirizzi univoci a ogni client anziché al client che genera gli ultimi 64 bit dell'indirizzo come in SLAAC. Questa configurazione di interfaccia è per un router IPv6 Cisco IOS che implementa DHCPv6 con stato e SLAAC disabilitato:

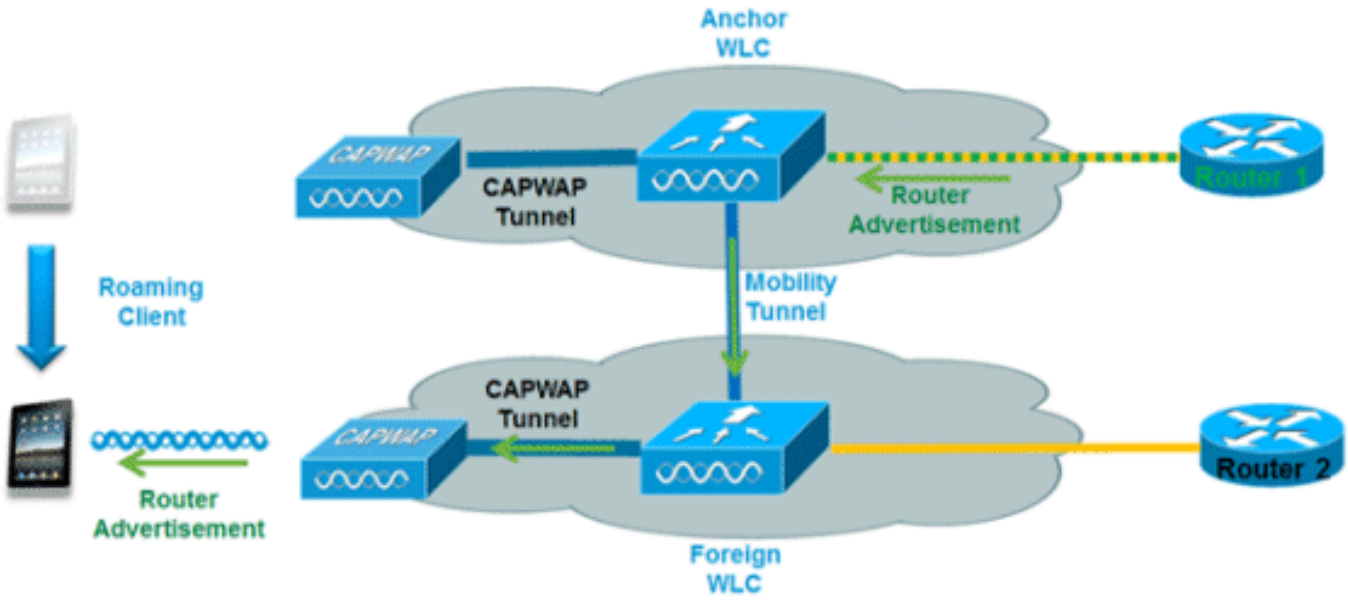
```
ipv6 unicast-routing
interface Vlan20
 description IPv6-DHCP-Stateful
 ip address 192.168.20.1 255.255.255.0
 ipv6 enable
 ipv6 address 2001:DB8:0:20::1/64
 ipv6 nd prefix 2001:DB8:0:20::/64 no-advertise
 ipv6 nd managed-config-flag
 ipv6 nd other-config-flag
```

```
 ipv6 dhcp relay destination 2001:DB8:0:10::100
end
```

Ulteriori informazioni

La configurazione della rete cablata per una connettività IPv6 completa a livello di campus utilizzando metodi di connettività a doppio stack o tunneling esula dall'ambito del presente documento. Per ulteriori informazioni, consultare la guida alla distribuzione convalidata da Cisco Deploying IPv6 in Campus Networks.

Mobilità client IPv6



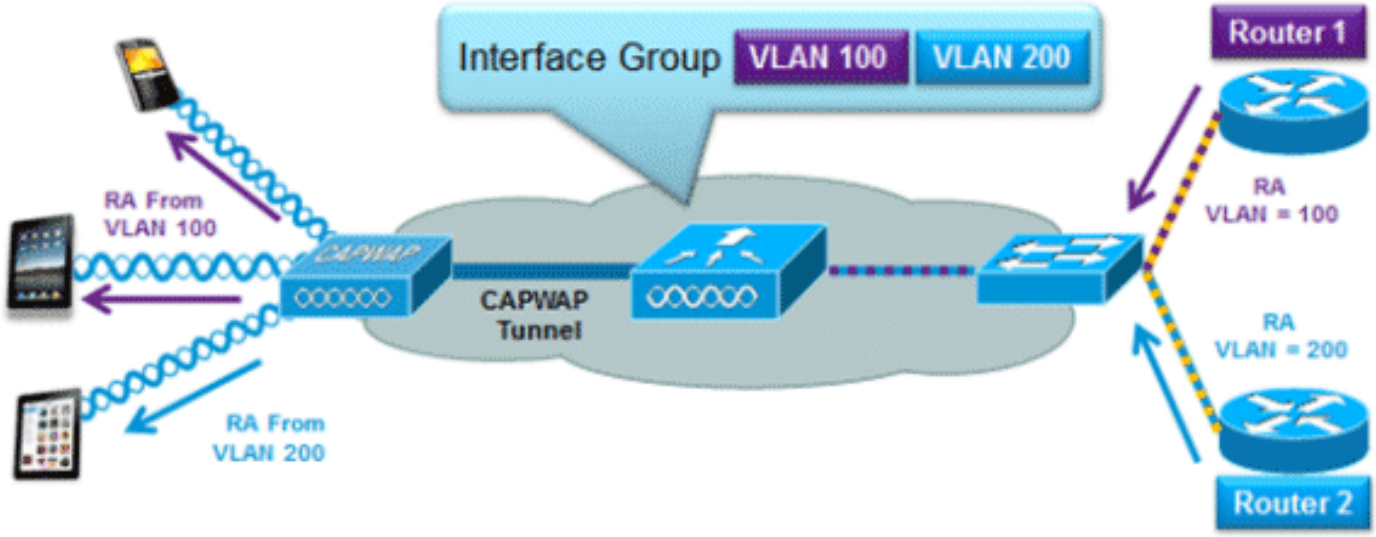
Per gestire i client IPv6 in roaming tra i controller, è necessario gestire in modo specifico i messaggi ICMPv6 quali NCS (Neighbor Solicitation), NAT (Neighbor Advertisement), RRA (Router Advertisement) e RS (Router Solicitation) per garantire che un client rimanga sulla stessa rete di layer 3. La configurazione per la mobilità IPv6 è identica a quella per la mobilità IPv4 e non richiede software separato sul lato client per ottenere un roaming senza problemi. L'unica configurazione richiesta è che i controller devono appartenere allo stesso gruppo/dominio di mobilità.

Di seguito è riportato il processo per la mobilità dei client IPv6 tra i controller:

1. Se entrambi i controller hanno accesso alla stessa VLAN su cui era originariamente il client, il roaming è semplicemente un evento di roaming di layer 2 in cui il record del client viene copiato sul nuovo controller e il traffico non viene tunneling al controller di ancoraggio.
2. Se il secondo controller non ha accesso alla VLAN originale su cui era il client, si verificherà un evento di roaming di layer 3, ossia tutto il traffico proveniente dal client deve essere tunneling attraverso il tunnel per la mobilità (Ethernet over IP) al controller di ancoraggio.Per garantire che il client conservi l'indirizzo IPv6 originale, gli ACL della VLAN originale vengono inviati dal controller di ancoraggio al controller esterno dove vengono consegnati al client utilizzando il protocollo unicast L2 dell'access point.Quando il client in roaming rinnova l'indirizzo tramite DHCPv6 o genera un nuovo indirizzo tramite SLAAC, i pacchetti RS, NA e NS continuano a essere tunneling sulla VLAN originale, quindi il client riceverà un indirizzo IPv6 applicabile a tale VLAN.

Nota: la mobilità per i client solo IPv6 è basata sulle informazioni VLAN. Ciò significa che la mobilità dei client solo IPv6 non è supportata sulle VLAN senza tag.

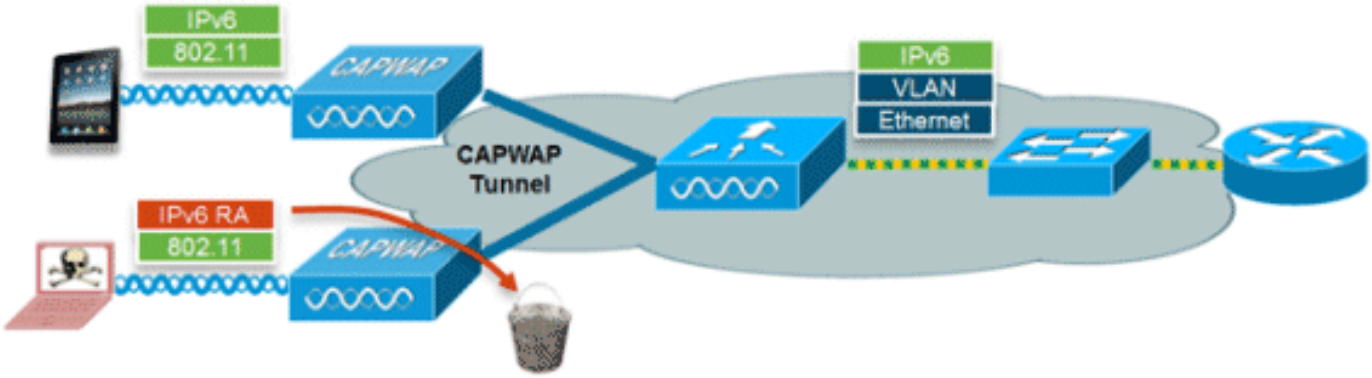
Supporto per VLAN Select (gruppi di interfacce)



La funzionalità dei gruppi di interfacce consente a un'organizzazione di avere una singola WLAN con più VLAN configurate sul controller per consentire il bilanciamento del carico dei client wireless su queste VLAN. Questa funzione viene in genere utilizzata per ridurre le dimensioni della subnet IPv4 e consentire la scalabilità di una WLAN a migliaia di utenti su più VLAN del gruppo. Per supportare i client IPv6 con gruppi di interfacce, non è necessaria alcuna configurazione aggiuntiva in quanto il sistema invia automaticamente l'indirizzo di rete corretto ai client corretti tramite l'unicast wireless L2. Con la funzione di unicast dell'Autorità di registrazione, i client sulla stessa WLAN ma su una VLAN diversa non ricevono l'Autorità di certificazione errata.

Sicurezza primo hop per client IPv6

Router Advertisement Guard



La funzionalità Protezione accesso alla rete aumenta la sicurezza della rete IPv6 eliminando gli avvisi di recapito provenienti dai client wireless. Senza questa funzionalità, i client IPv6 non configurati correttamente o dannosi potrebbero annunciarsi come router per la rete, spesso con un'alta priorità che potrebbe avere la precedenza sui router IPv6 legittimi.

Per impostazione predefinita, RA Guard è abilitato sull'access point (ma può essere disabilitato sull'access point) ed è sempre abilitato sul controller. È preferibile eliminare gli RA nell'access

point, in quanto si tratta di una soluzione più scalabile e offre contatori di rilascio degli RA ottimizzati per client. In tutti i casi, l'Autorità registrazione integrità IPv6 verrà eliminata a un certo punto, proteggendo altri client wireless e la rete cablata upstream da client IPv6 dannosi o non configurati correttamente.

Protezione server DHCPv6

La funzionalità Protezione server DHCPv6 impedisce ai client wireless di distribuire indirizzi IPv6 ad altri client wireless o cablati a monte. Per impedire la distribuzione degli indirizzi DHCPv6, tutti i pacchetti di annuncio DHCPv6 provenienti da client wireless vengono ignorati. Questa funzionalità funziona sul controller, non richiede alcuna configurazione e viene attivata automaticamente.

Protezione origine IPv6

La funzionalità Protezione origine IPv6 impedisce a un client wireless di eseguire lo spoofing di un indirizzo IPv6 di un altro client. Questa funzionalità è analoga a IPv4 Source Guard. IPv6 Source Guard è abilitato per impostazione predefinita ma può essere disabilitato tramite la CLI.

Accounting indirizzo IPv6

Per l'autenticazione e l'accounting RADIUS, il controller restituisce un indirizzo IP utilizzando l'attributo "Framed-IP-address". In questo caso, viene utilizzato l'indirizzo IPv4.

L'attributo "Calling-Station-ID" utilizza questo algoritmo per restituire un indirizzo IP quando "Call Station ID Type" sul controller è configurato su "IP Address":

1. Indirizzo IPv4
2. Indirizzo IPv6 unicast globale
3. Collega indirizzo IPv6 locale

Poiché gli indirizzi IPv6 dei client possono cambiare spesso (indirizzi temporanei o privati), è importante tenerne traccia nel tempo. Cisco NCS registra tutti gli indirizzi IPv6 in uso da ogni client e li registra in modo cronologico ogni volta che il client esegue il roaming o stabilisce una nuova sessione. Questi record possono essere configurati su NCS per essere conservati fino a un anno.

Nota: il valore predefinito per "Call Station ID Type" (Tipo di ID stazione di chiamata) sul controller è stato modificato in "System MAC Address" (Indirizzo MAC di sistema) nella versione 7.2. Durante l'aggiornamento, è necessario modificare questa impostazione per consentire la registrazione univoca dei client in base all'indirizzo MAC, in quanto gli indirizzi IPv6 possono cambiare a metà sessione e causare problemi di accounting se l'ID della stazione chiamante è impostato su indirizzo IP.

Access Control List IPv6

Per limitare l'accesso a determinate risorse cablate a monte o bloccare alcune applicazioni, è possibile utilizzare gli Access Control List (ACL) IPv6 per identificare il traffico e autorizzarlo o negarlo. Gli ACL IPv6 supportano le stesse opzioni degli ACL IPv4, tra cui origine, destinazione, porta di origine e porta di destinazione (sono supportati anche gli intervalli di porte). Gli ACL di preautenticazione sono inoltre supportati per supportare l'autenticazione guest IPv6 tramite un server Web esterno. Il controller wireless supporta fino a 64 ACL IPv6 univoci con 64 regole univoche in ognuno. Il controller wireless continua a supportare altri 64 ACL IPv4 univoci con 64

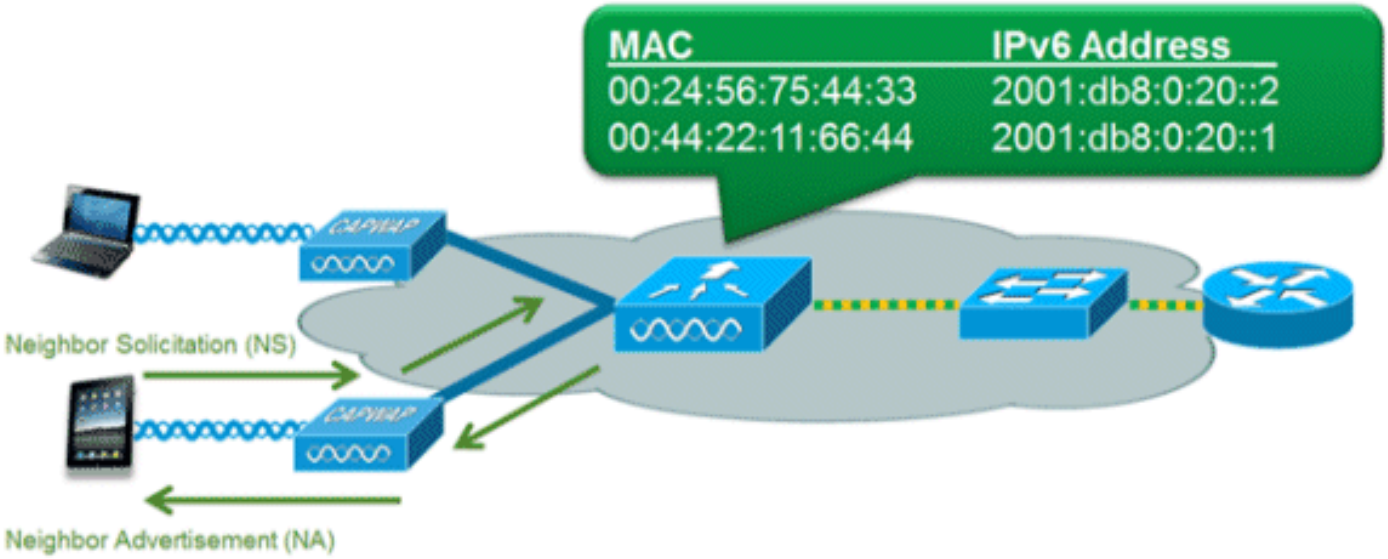
regole univoche in ciascuno, per un totale di 128 ACL per un client a doppio stack.

Override AAA per ACL IPv6

Per supportare il controllo dell'accesso centralizzato tramite un server AAA centralizzato, ad esempio Cisco Identity Services Engine (ISE) o ACS, è possibile eseguire il provisioning dell'ACL IPv6 per singolo client utilizzando gli attributi di override AAA. Per utilizzare questa funzionalità, è necessario configurare l'ACL IPv6 sul controller e configurare la WLAN con la funzionalità di sostituzione AAA abilitata. L'attributo AAA denominato effettivo per un ACL IPv6 è ***Airespace-IPv6-ACL-Name*** simile all'attributo *Airespace-ACL-Name* utilizzato per il provisioning di un ACL basato su IPv4. Il contenuto restituito dall'attributo AAA deve essere una stringa uguale al nome dell'ACL IPv6 configurato nel controller.

Ottimizzazione pacchetti per client IPv6

Memorizzazione nella cache di individuazione router adiacenti



Il protocollo NDP (Neighbor Discovery Protocol) IPv6 utilizza i pacchetti NA e NS al posto del protocollo ARP (Address Resolution Protocol) per consentire ai client IPv6 di risolvere l'indirizzo MAC di altri client nella rete. Il processo NDP può essere molto chiacchierato in quanto utilizza inizialmente indirizzi multicast per eseguire la risoluzione degli indirizzi; ciò può richiedere tempo di trasmissione wireless prezioso in quanto i pacchetti multicast vengono inviati a tutti i client sul segmento di rete.

Per aumentare l'efficienza del processo NDP, la memorizzazione nella cache di rilevamento dei router adiacenti consente al controller di agire come proxy e rispondere alle query NS risolte. La memorizzazione nella cache di individuazione dei router adiacenti è resa possibile dalla tabella di associazione dei nodi adiacenti sottostante presente nel controller. La tabella di binding adiacente tiene traccia di ogni indirizzo IPv6 e del relativo indirizzo MAC associato. Quando un client IPv6 tenta di risolvere l'indirizzo del livello di collegamento di un altro client, il pacchetto NS viene intercettato dal controller che risponde con un pacchetto NA.

Limitazione della larghezza di banda per l'annuncio router

La limitazione della pubblicità del router consente al controller di applicare la limitazione della

velocità degli RAS diretti alla rete wireless. Attivando la limitazione dell'accesso remoto, i router configurati per l'invio di server di accesso remoto molto spesso (ad esempio, ogni tre secondi) possono essere ridotti a una frequenza minima che manterrà la connettività client IPv6. Ciò consente di ottimizzare la trasmissione riducendo il numero di pacchetti multicast che devono essere inviati. In tutti i casi, se un client invia un RSA, quest'ultimo sarà autorizzato attraverso il controller e unicast al client richiedente. In questo modo si garantisce che i nuovi client o i client in roaming non siano influenzati negativamente dalla limitazione di RSA.

Accesso guest IPv6

Le funzionalità guest wireless e cablate disponibili per i client IPv4 funzionano allo stesso modo per i client a doppio stack e solo IPv6. Una volta associati, gli utenti guest vengono inseriti in uno stato di esecuzione "WEB_AUTH_REQ" fino a quando il client non viene autenticato tramite il portale captive IPv4 o IPv6. Il controller intercetta il traffico HTTP/HTTPS IPv4 e IPv6 in questo stato e lo reindirizza all'indirizzo IP virtuale del controller. Dopo che l'utente è stato autenticato tramite il portale vincolato, il relativo indirizzo MAC viene spostato nello stato di esecuzione e viene consentito il passaggio del traffico IPv4 e IPv6. Per l'autenticazione Web esterna, l'ACL di preautenticazione consente di utilizzare un server Web esterno.

Per supportare il reindirizzamento dei client solo IPv6, il controller crea automaticamente un indirizzo virtuale IPv6 basato sull'indirizzo virtuale IPv4 configurato nel controller. L'indirizzo IPv6 virtuale segue la convenzione di `[::ffff:<indirizzo IPv4 virtuale>]`. Ad esempio, un indirizzo IP virtuale di 1.1.1.1 verrà convertito in `[::ffff:1.1.1.1]`.

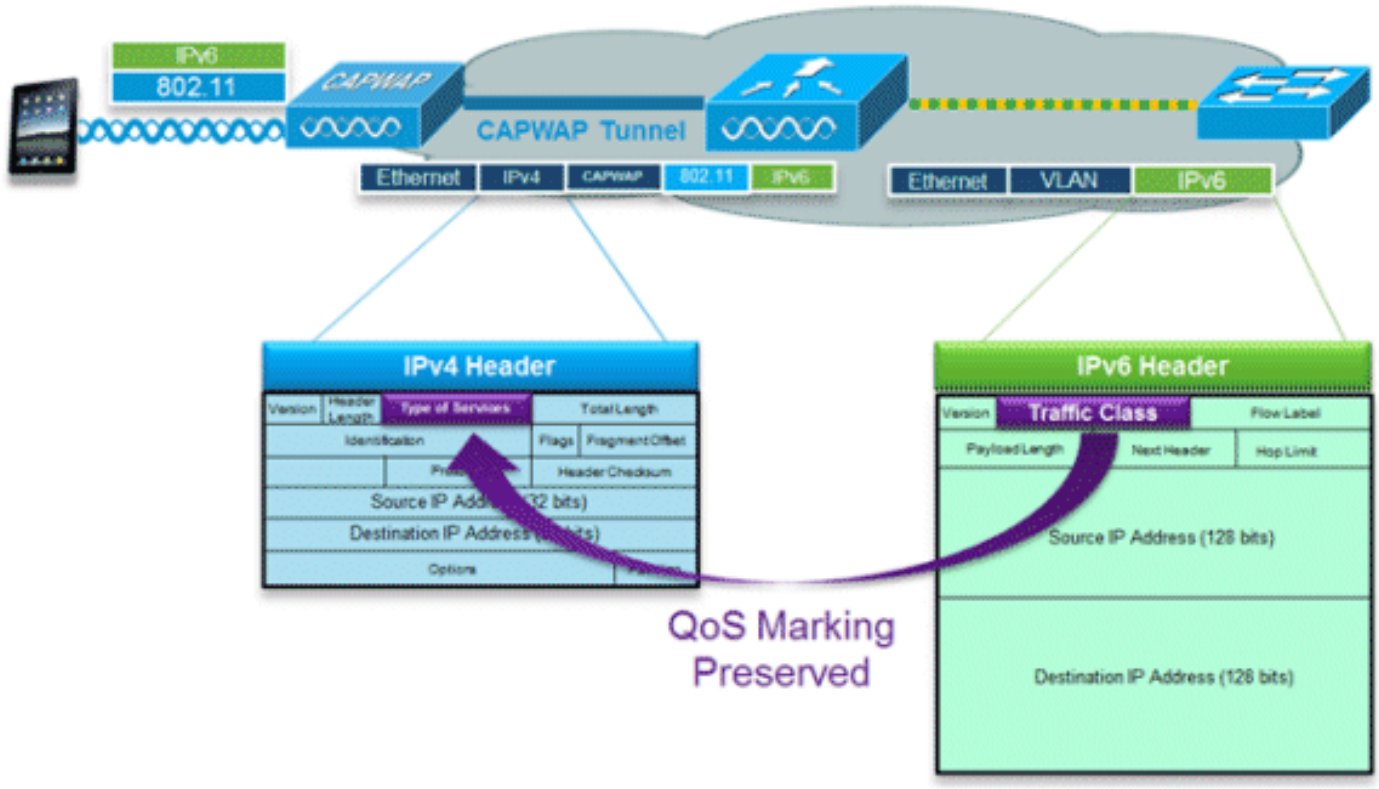
Quando si utilizza un certificato SSL attendibile per l'autenticazione di accesso guest, verificare che l'indirizzo virtuale IPv4 e IPv6 del controller sia definito nel DNS in modo che corrisponda al nome host dei certificati SSL. In questo modo si garantisce che i client non ricevano un avviso di protezione in cui viene indicato che il certificato non corrisponde al nome host del dispositivo.

Nota: il certificato SSL generato automaticamente dal controller non contiene l'indirizzo virtuale IPv6. Alcuni browser Web potrebbero pertanto visualizzare un avviso di protezione. È consigliabile utilizzare un certificato SSL attendibile per l'accesso guest.

VideoStream IPv6

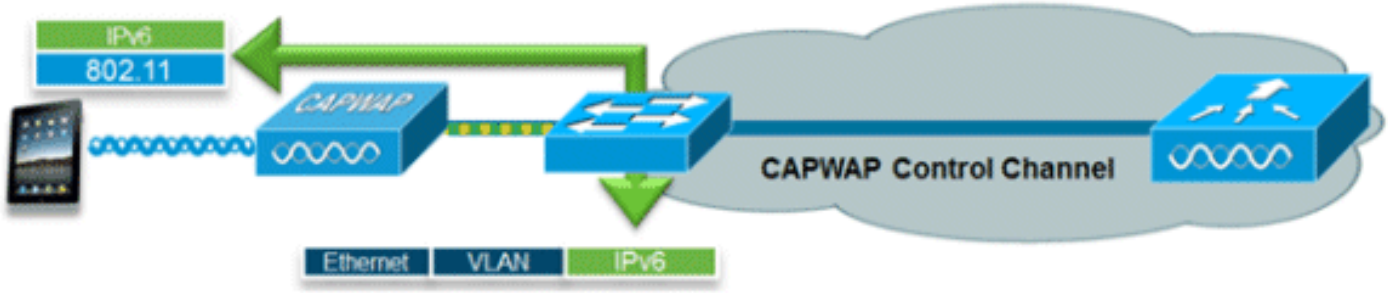
VideoStream consente la distribuzione di video multicast wireless, affidabile e scalabile, inviando il flusso a ciascun client in formato unicast. L'effettiva conversione da multicast a unicast (di L2) si verifica nell'access point, fornendo una soluzione scalabile. Il controller invia il traffico video IPv6 all'interno di un tunnel multicast CAPWAP IPv4 che consente una distribuzione di rete efficiente all'access point.

Qualità del servizio IPv6



I pacchetti IPv6 utilizzano un contrassegno simile all'uso da parte di IPv4 dei valori DSCP che supportano fino a 64 diverse classi di traffico (0-63). Per i pacchetti downstream provenienti dalla rete cablata, il valore della classe di traffico IPv6 viene copiato nell'intestazione del tunnel CAPWAP per garantire che la funzionalità QoS venga mantenuta end-to-end. Nella direzione a monte, lo stesso si verifica quando il traffico client contrassegnato al layer 3 con classe di traffico IPv6 viene rispettato contrassegnando i pacchetti CAPWAP destinati al controller.

IPv6 e FlexConnect



FlexConnect - WLAN di switching locale

FlexConnect in modalità di commutazione locale supporta i client IPv6 collegando il traffico alla VLAN locale, in modo simile al funzionamento di IPv4. La mobilità dei client è supportata per il roaming di layer 2 nel gruppo FlexConnect.

Le seguenti funzionalità specifiche di IPv6 sono supportate nella modalità di commutazione locale FlexConnect:

- Protezione RA IPv6
- Bridging IPv6
- Autenticazione guest IPv6 (ospitata dal controller)

Le seguenti funzionalità specifiche di IPv6 non sono supportate nella modalità di commutazione locale FlexConnect:

- Mobilità Layer 3
- VideoStream IPv6
- Access Control List IPv6
- Protezione origine IPv6
- Protezione server DHCPv6
- Memorizzazione nella cache di individuazione router adiacenti
- Limitazione della larghezza di banda per l'annuncio router

FlexConnect - WLAN di switching centrale

Per i punti di accesso in modalità FlexConnect che utilizzano la commutazione centrale (tunneling del traffico verso il controller), il controller deve essere impostato su "Multicast - Modalità unicast" per "Modalità multicast AP". Poiché i punti di accesso FlexConnect non si uniscono al gruppo multicast CAPWAP del controller, i pacchetti multicast devono essere replicati sul controller e unicast su ogni singolo punto di accesso. Questo metodo è meno efficiente della modalità "Multicast - Multicast" e comporta un carico aggiuntivo sul controller.

Questa funzionalità specifica di IPv6 non è supportata nella modalità di commutazione centrale FlexConnect:

- VideoStream IPv6

Nota: le WLAN a commutazione centrale con IPv6 non sono supportate sul controller Flex serie 7500.

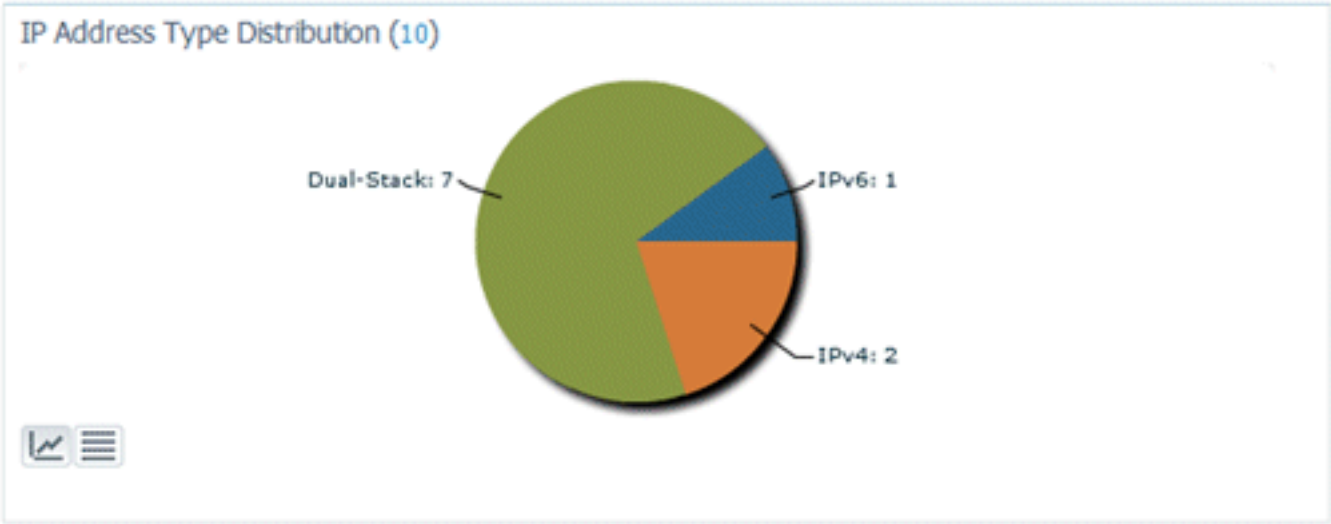
Visibilità dei client IPv6 con NCS

Con il rilascio di NCS v1.1, vengono aggiunte molte funzionalità aggiuntive specifiche di IPv6 per monitorare e gestire una rete di client IPv6 su reti cablate e wireless.

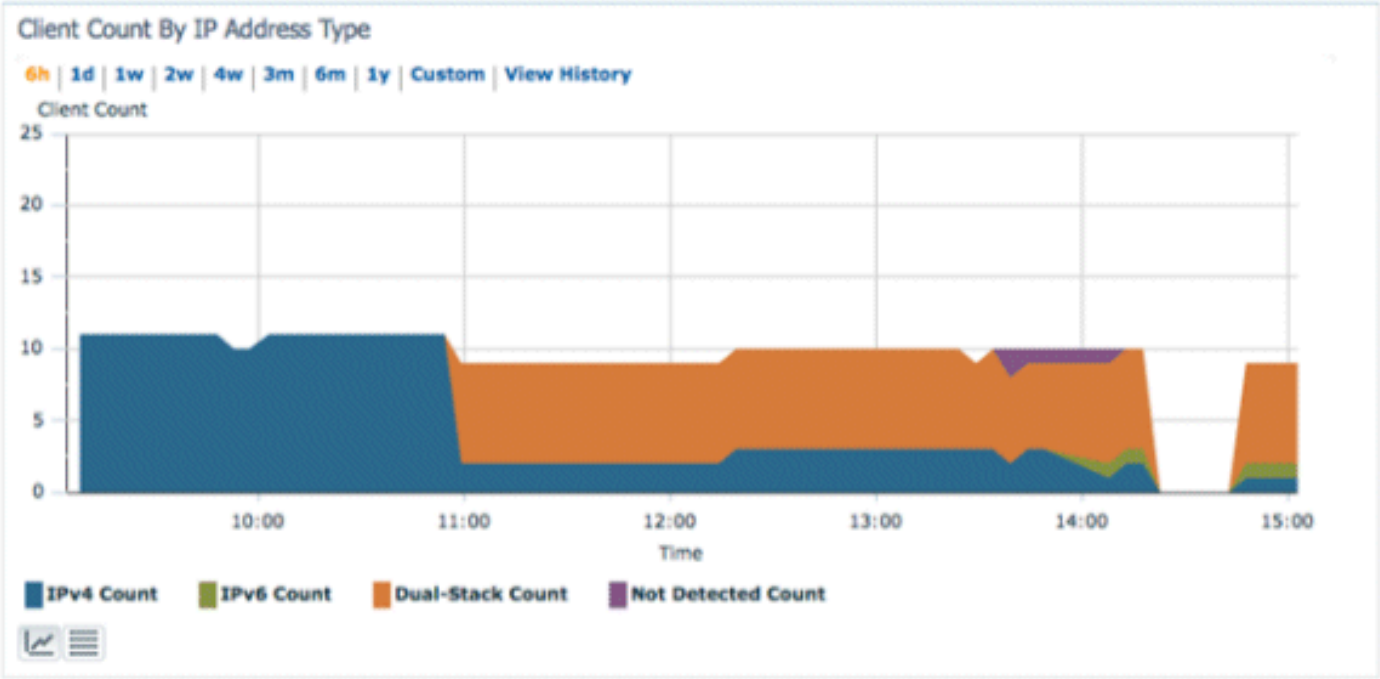
Elementi dashboard IPv6

Per visualizzare i tipi di client presenti nella rete, è disponibile una "dashlet" in NCS che consente di ottenere informazioni dettagliate sulle statistiche specifiche di IPv6 e di eseguire il drill-down dei client IPv6.

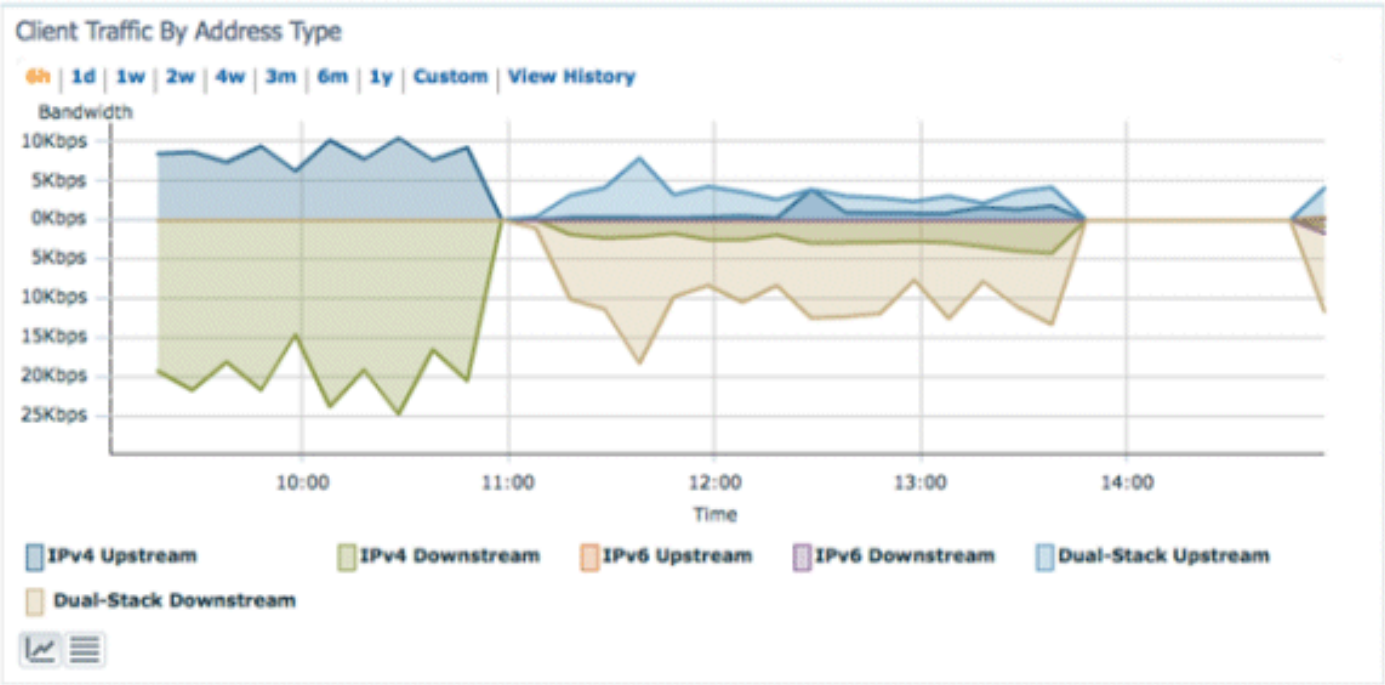
Dashlet del tipo di indirizzo IP: visualizza i tipi di client IP sulla rete:



Conteggio client per tipo di indirizzo IP: visualizza il tipo di client IP nel tempo:



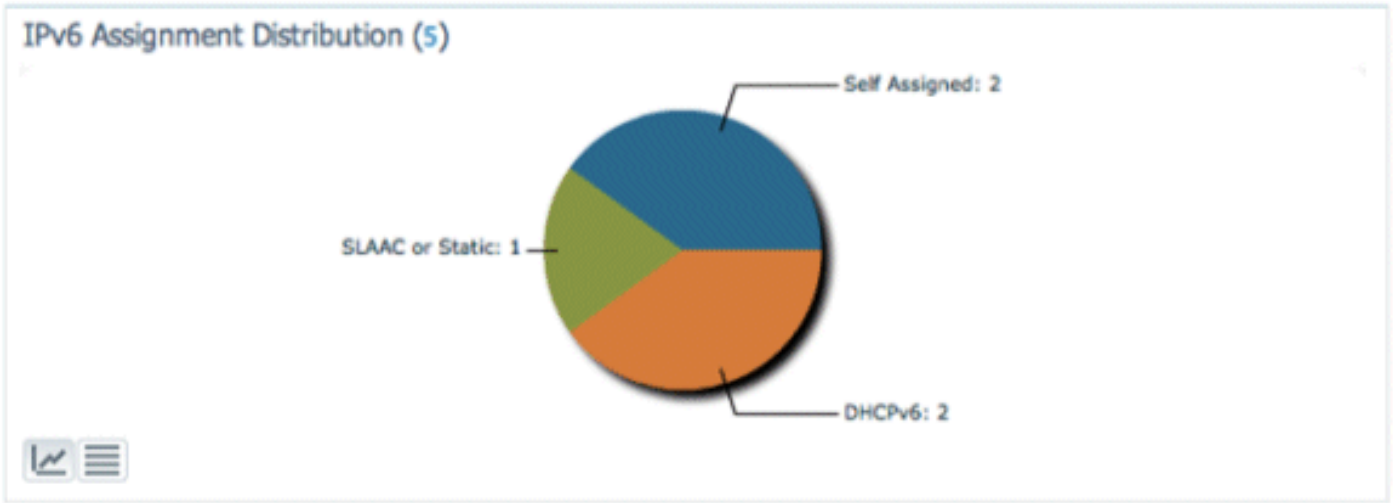
Traffico client per tipo di indirizzo IP: visualizza il traffico proveniente da ciascun tipo di client. I client della categoria a doppio stack includono sia il traffico IPv4 che il traffico IPv6:



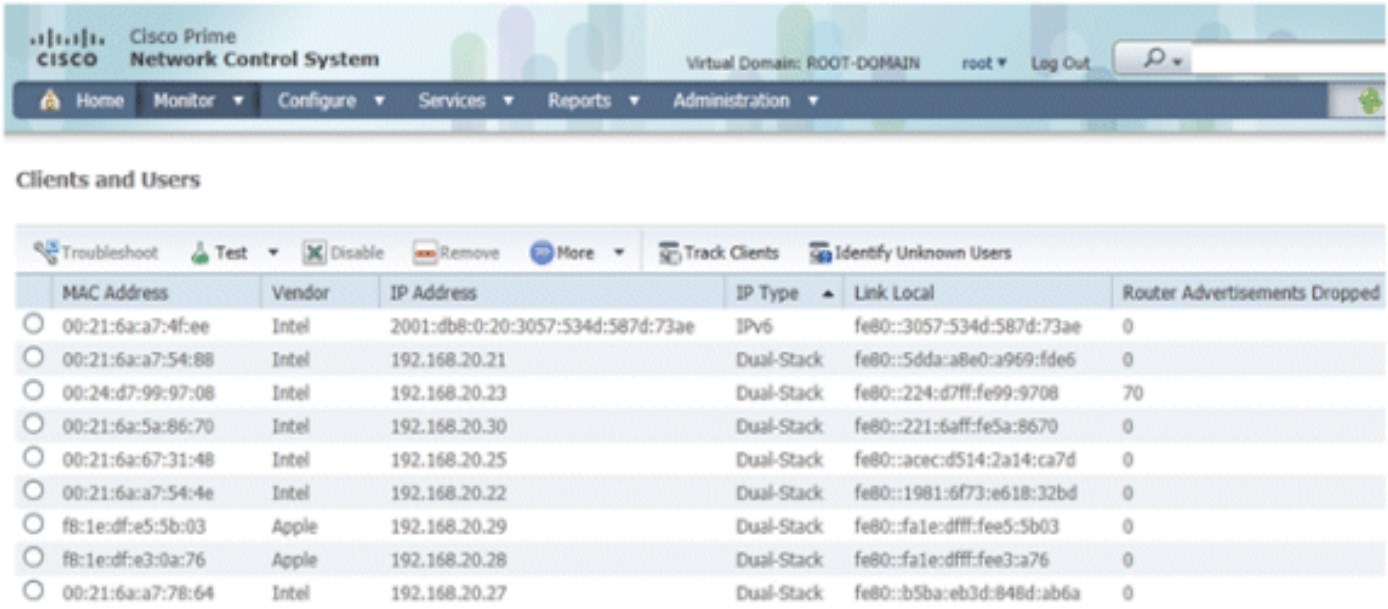
Assegnazione indirizzi IPv6: visualizza il metodo di assegnazione degli indirizzi per ogni client in una delle quattro categorie seguenti:

- DHCPv6 - Per client con indirizzi assegnati da un server centrale. Il client può anche avere un indirizzo SLAAC.
- SLAAC o Static - Per i client che utilizzano l'assegnazione automatica degli indirizzi senza stato o che utilizzano indirizzi configurati staticamente.
- Sconosciuto - In alcuni casi non è possibile individuare l'assegnazione dell'indirizzo IPv6.Questa condizione si verifica solo sui client cablati in NCS, in quanto alcuni switch non snooprono le informazioni di assegnazione degli indirizzi IPv6.
- Assegnazione automatica - Per i client con solo un indirizzo locale del collegamento interamente assegnato automaticamente.I client di questa categoria possono presentare problemi di connettività IPv6 poiché non dispongono di un indirizzo univoco globale o univoco locale.

Èpossibile fare clic su ciascuna sezione del grafico a torta per consentire all'amministratore di espandere un elenco di client.

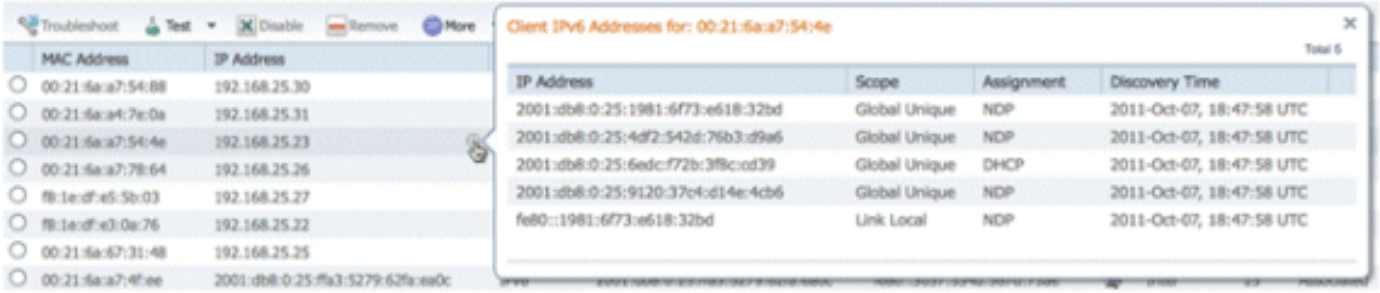


[Monitoraggio client IPv6]



Per monitorare e gestire le informazioni sul client IPv6, nella pagina Client e utenti sono state aggiunte le colonne seguenti:

- Tipo IP: il tipo di client in base agli indirizzi IP visualizzati dal client. Le opzioni possibili sono IPv4, IPv6 o Dual-Stack che indica un client con indirizzi IPv4 e IPv6.
- Tipo di assegnazione IPv6: il metodo di assegnazione degli indirizzi viene rilevato da NCS come SLAAC o Static, DHCPv6, Self-Assigned o Unknown.
- Univoco globale: l'indirizzo globale IPv6 più recente utilizzato dal client. Al passaggio del mouse sul contenuto della colonna vengono visualizzati tutti gli altri indirizzi univoci globali IPv6 utilizzati dal client.
- Univoco locale: l'indirizzo univoco locale IPv6 più recente utilizzato dal client. Al passaggio del mouse sul contenuto della colonna vengono visualizzati tutti gli altri indirizzi univoci globali IPv6 utilizzati dal client.
- Collegamento locale: l'indirizzo IPv6 del client assegnato automaticamente e utilizzato per la comunicazione prima dell'assegnazione di qualsiasi altro indirizzo IPv6.
- Annunci router interrotti: numero di annunci router inviati dal client e interrotti nell'access point. Questa colonna può essere utilizzata per tenere traccia dei client configurati in modo errato o in modo dannoso per operare come router IPv6. Questa colonna è ordinabile e consente di identificare facilmente i client in conflitto.

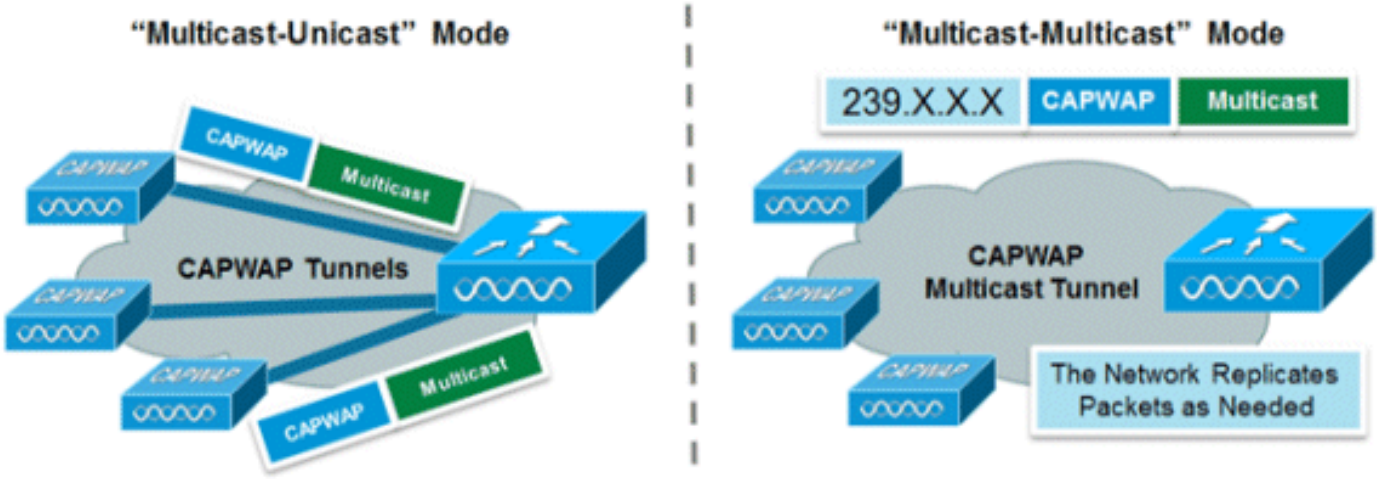


Oltre a visualizzare le colonne specifiche di IPv6, nella colonna Indirizzo IP verrà visualizzato l'indirizzo IP corrente del client con priorità di visualizzare prima l'indirizzo IPv4 (nel caso di un client Dual-Stack) o l'indirizzo univoco globale IPv6 nel caso di un client solo IPv6.

Configurazione per supporto client IPv6 wireless

Modalità di distribuzione multicast agli access point

Cisco Unified Wireless Network supporta due metodi di distribuzione multicast agli access point associati al controller. In entrambe le modalità, il pacchetto multicast originale proveniente dalla rete cablata viene incapsulato in un pacchetto CAPWAP di layer 3 inviato all'access point tramite CAPWAP Unicast o Multicast. Poiché il traffico è incapsulato in CAPWAP, i punti di accesso non devono trovarsi sulla stessa VLAN del traffico del client. I due metodi di distribuzione multicast sono confrontati di seguito:



	Modalità multicast-unicast	Modalità Multicast-Multicast
Meccanismo di consegna	Il controller replica il pacchetto multicast e lo invia a ciascun access point in un tunnel CAPWAP unicast	Il controller invia una copia del pacchetto multicast
Modalità AP supportate	FlexConnect e Local	Solo modalità locale
Richiede il routing multicast L3 su una rete cablata	No	Sì
Caricamento controller	Alta	Bassa
Caricamento rete cablata	Alta	Bassa

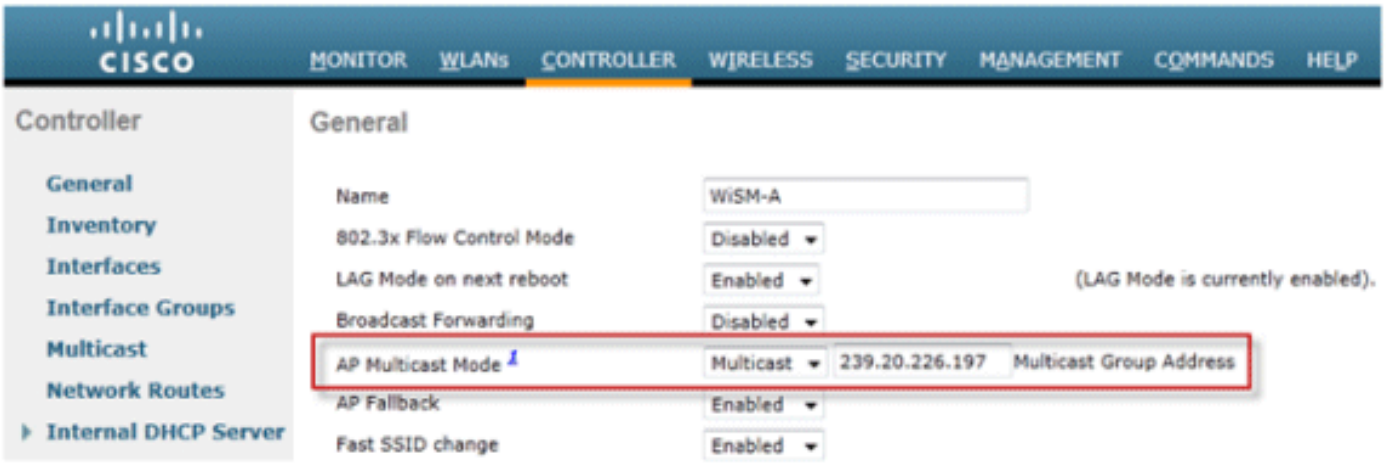
Configura modalità di distribuzione multicast

La modalità multicast è l'opzione consigliata per motivi di scalabilità e di efficienza della larghezza di banda cablata.

Nota: questo passaggio è assolutamente necessario solo per il controller wireless serie 2500, ma consente una trasmissione multicast più efficiente ed è consigliato per tutte le piattaforme di

controller.

Andare alla scheda "Controller" nella pagina "Generale" e verificare che la modalità multicast dell'access point sia configurata per l'utilizzo della modalità **multicast** e che sia configurato un indirizzo di gruppo valido. L'indirizzo del gruppo è un gruppo multicast IPv4 e si consiglia di essere compreso nell'intervallo 239.X.X.X-239.255.255.255, che è nell'ambito delle applicazioni multicast private.

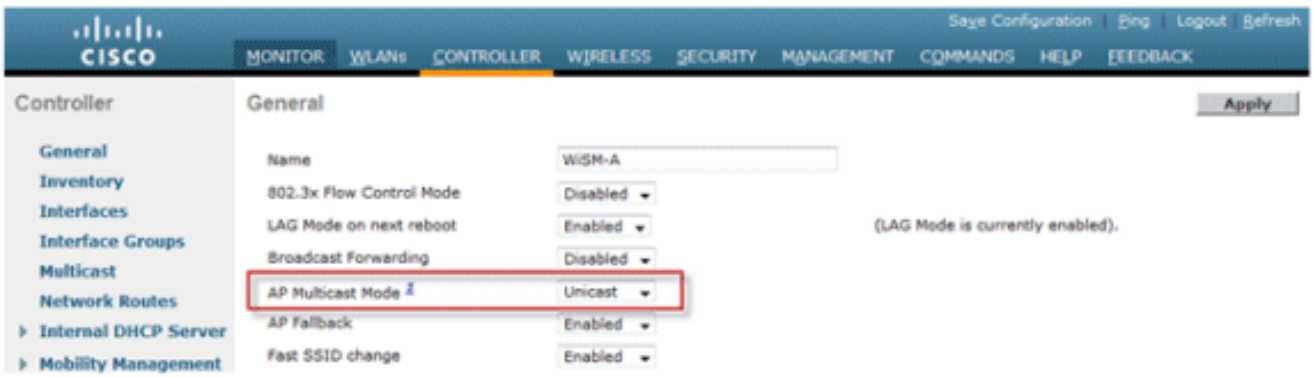


Nota: non utilizzare gli intervalli di indirizzi 224.X.X.X, 239.0.0.X o 239.128.0.X per l'indirizzo del gruppo multicast. Gli indirizzi in questi intervalli si sovrappongono agli indirizzi MAC locali del collegamento e invadono tutte le porte dello switch, anche se lo snooping IGMP è abilitato.

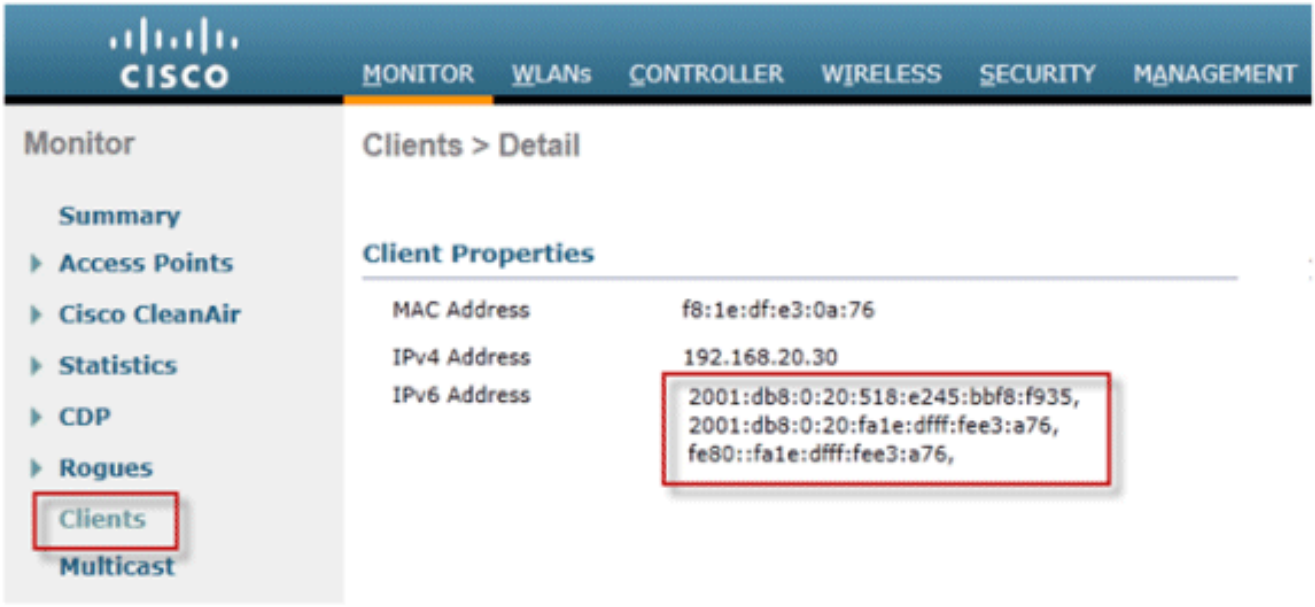
Configura modalità di distribuzione multicast-unicast

Se la rete cablata non è configurata correttamente per il trasferimento del multicast CAPWAP tra il controller e la modalità AP o FlexConnect e i punti di accesso vengono utilizzati per le WLAN a commutazione centrale che supportano IPv6, è necessaria la modalità unicast.

1. Andare alla scheda **Controller** nella pagina Generale e verificare che la modalità multicast AP sia configurata per l'utilizzo della modalità **unicast**.



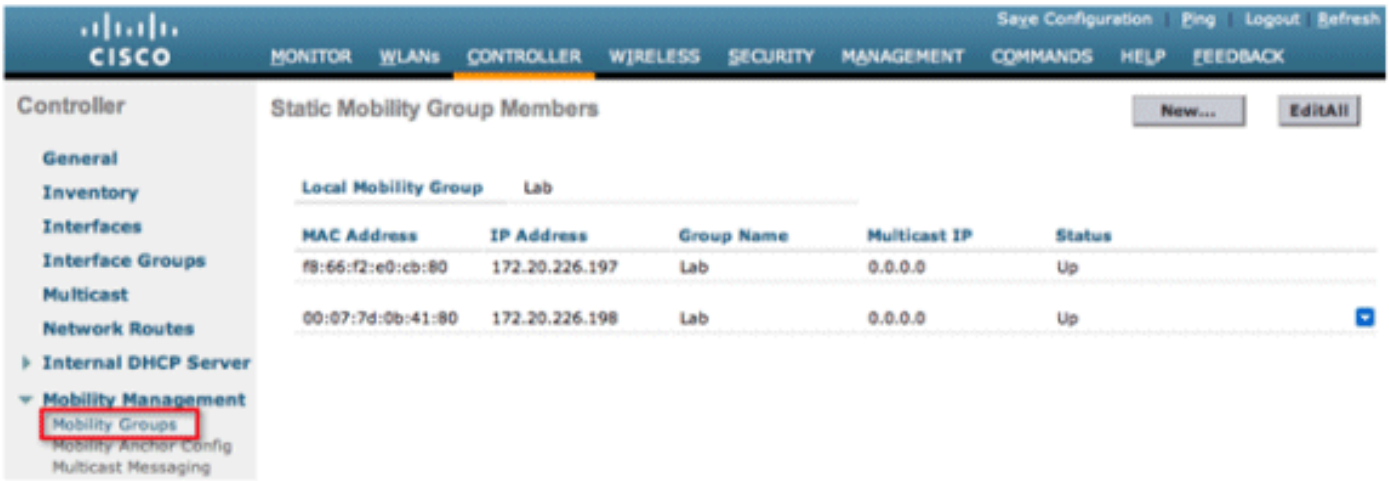
2. Connettere un client compatibile con IPv6 alla LAN wireless. Verificare che il client riceva un indirizzo IPv6 passando alla scheda **Monitoraggio** e quindi al menu **Client**.



Configurare la mobilità IPv6

Non esiste una configurazione specifica per la mobilità IPv6, ad eccezione del posizionamento dei controller nello stesso gruppo di mobilità o all'interno dello stesso dominio di mobilità. Ciò consente a un massimo di 72 controller di partecipare a un dominio di mobilità che fornisce una mobilità ottimale anche per il più grande dei campus.

Andare alla scheda **Controller** > **Mobility Groups** (Gruppi di mobilità) e aggiungere ciascun controller in base all'indirizzo MAC e all'indirizzo IP nel gruppo. Ciò deve essere fatto su tutti i controllori del gruppo di mobilità.



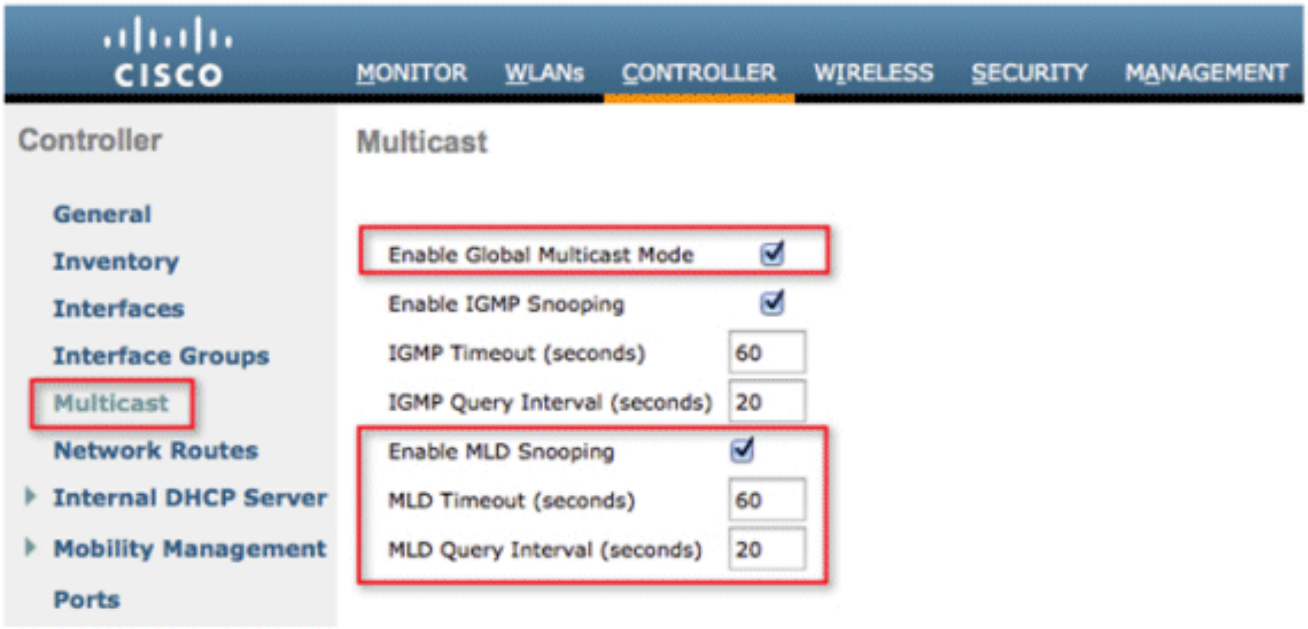
Configura multicast IPv6

Il controller supporta lo snooping MLDv1 per il multicast IPv6, che consente di tenere traccia in modo intelligente dei flussi multicast e di inviarli ai client che li richiedono.

Nota: a differenza delle versioni precedenti delle release, il supporto del traffico unicast IPv6 non richiede l'attivazione della modalità multicast globale nel controller. Il supporto per il traffico unicast IPv6 viene attivato automaticamente.

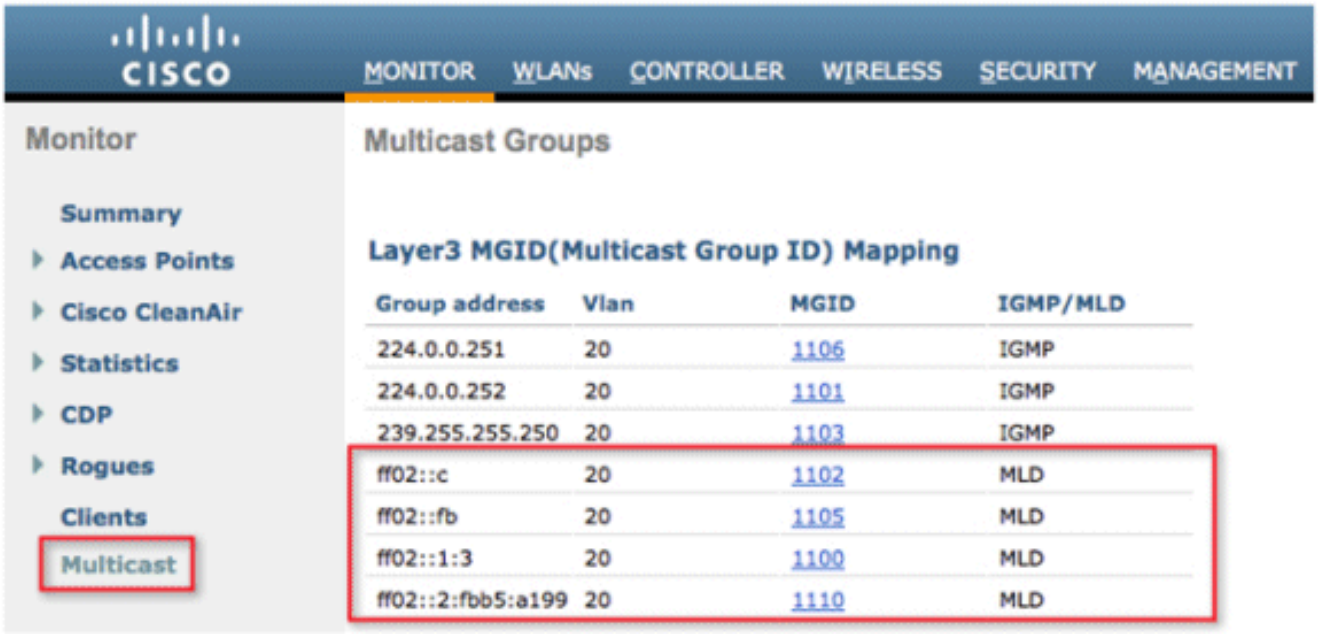
1. Per supportare il traffico IPv6 multicast, andare alla scheda **Controller** > pagina **Multicast** e

Abilitare lo snooping MLD. Affinché il multicast IPv6 sia abilitato, è necessario che sia attivata anche la **modalità multicast globale** del controller.



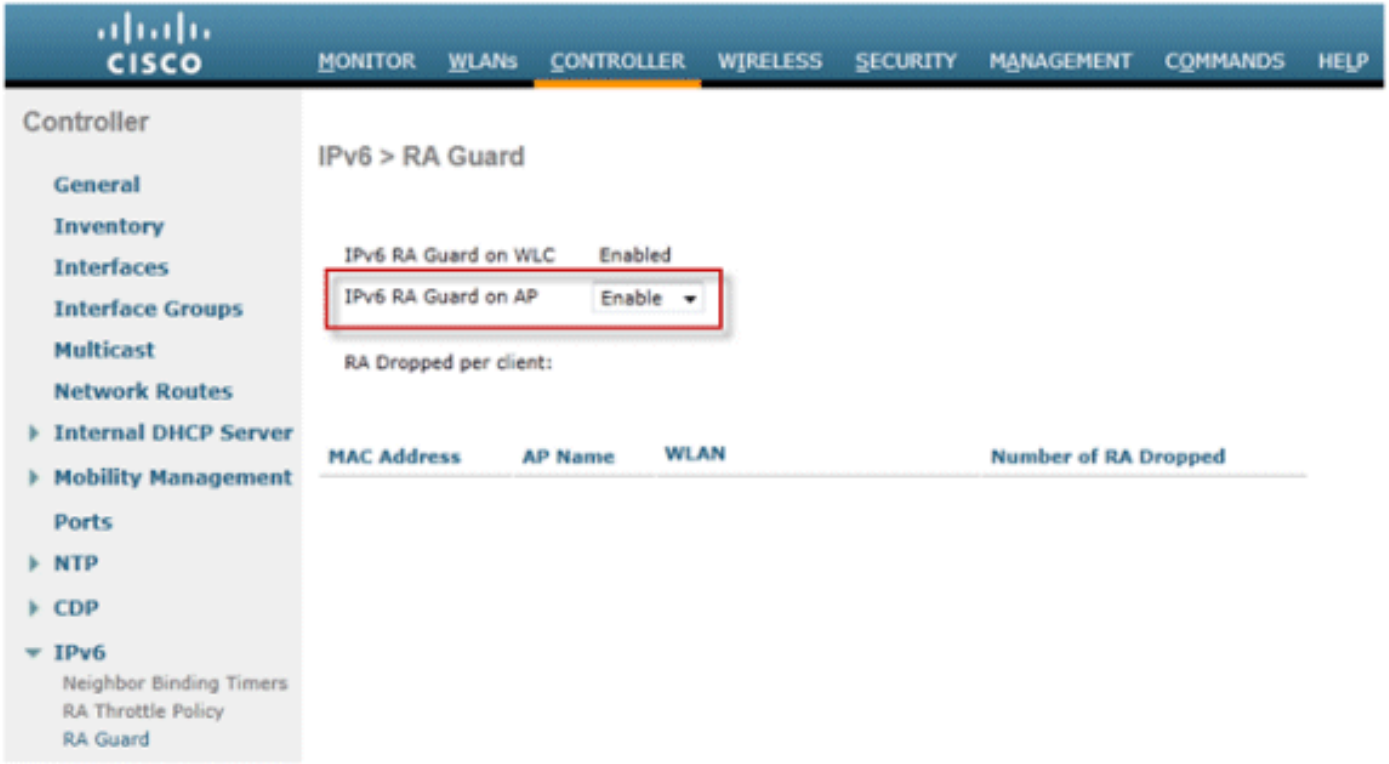
Nota: lo snooping Global Multicast Mode, IGMP e MLD deve essere abilitato se sono richieste applicazioni di rilevamento peer-to-peer come Apple Bonjour.

2. Per verificare che il traffico multicast IPv6 sia in fase di snooping, passare alla scheda **Monitor** e alla pagina **Multicast**. Si noti che sono elencati sia i gruppi multicast IPv4 (IGMP) che IPv6 (MLD). Fare clic sul MGID per visualizzare i client wireless aggiunti all'indirizzo del gruppo.



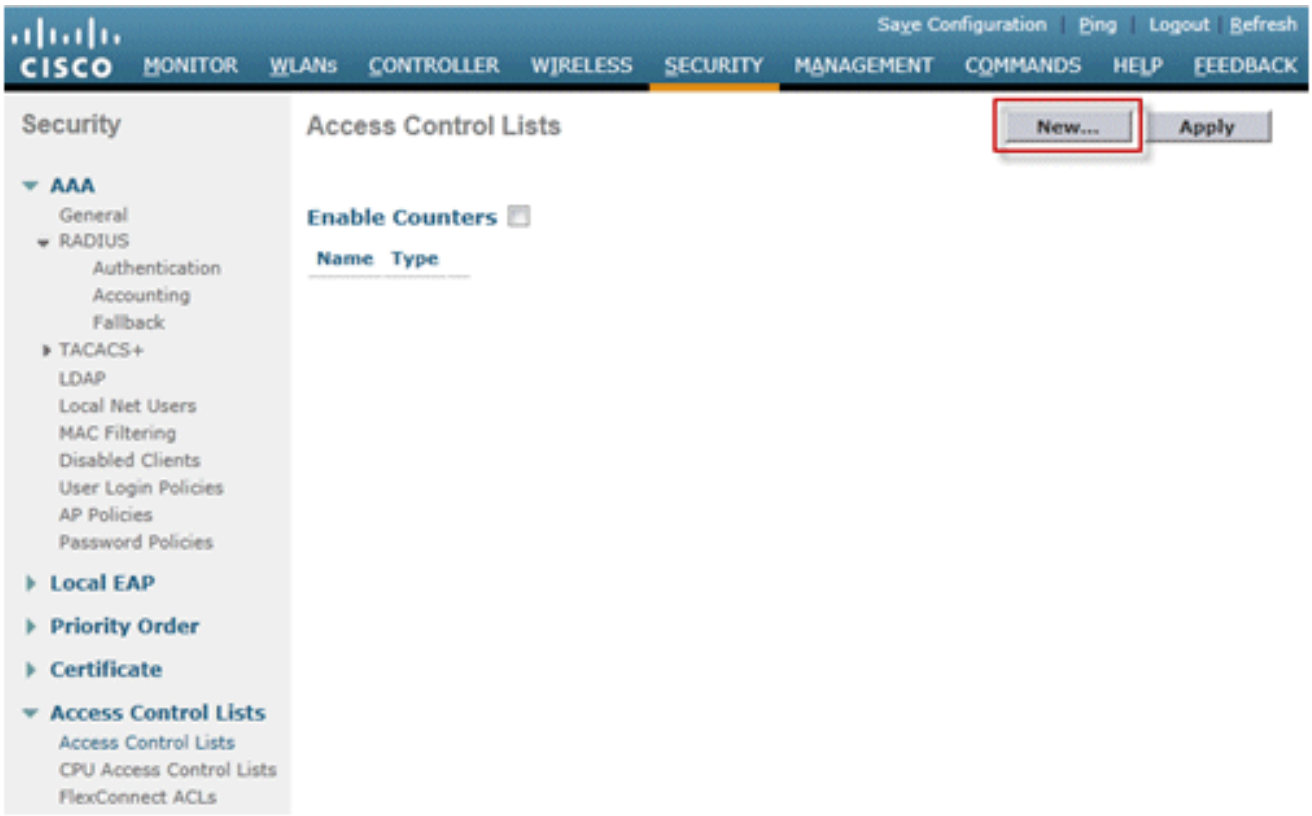
Configura Protezione Autorità registrazione integrità IPv6

Passare alla scheda **Controller**, quindi **IPv6 > RA Guard** nel menu a sinistra. **Abilitare** IPv6 RA Guard sull'access point. Impossibile disabilitare RA Guard sul controller. Oltre alla configurazione di RA Guard, questa pagina mostra anche tutti i client identificati come server di accesso remoto che inviano.



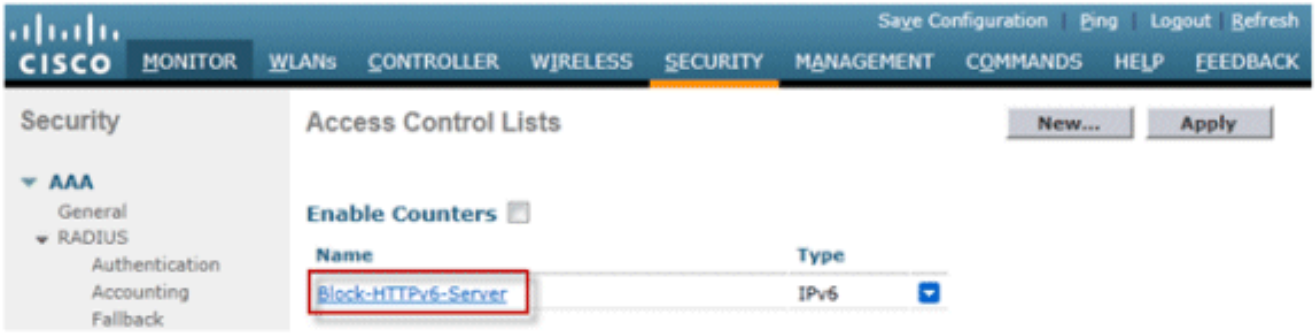
Configura elenchi di controllo di accesso IPv6

1. Passare alla scheda **Protezione**, aprire **Access Control Lists** e fare clic su **Nuovo**.

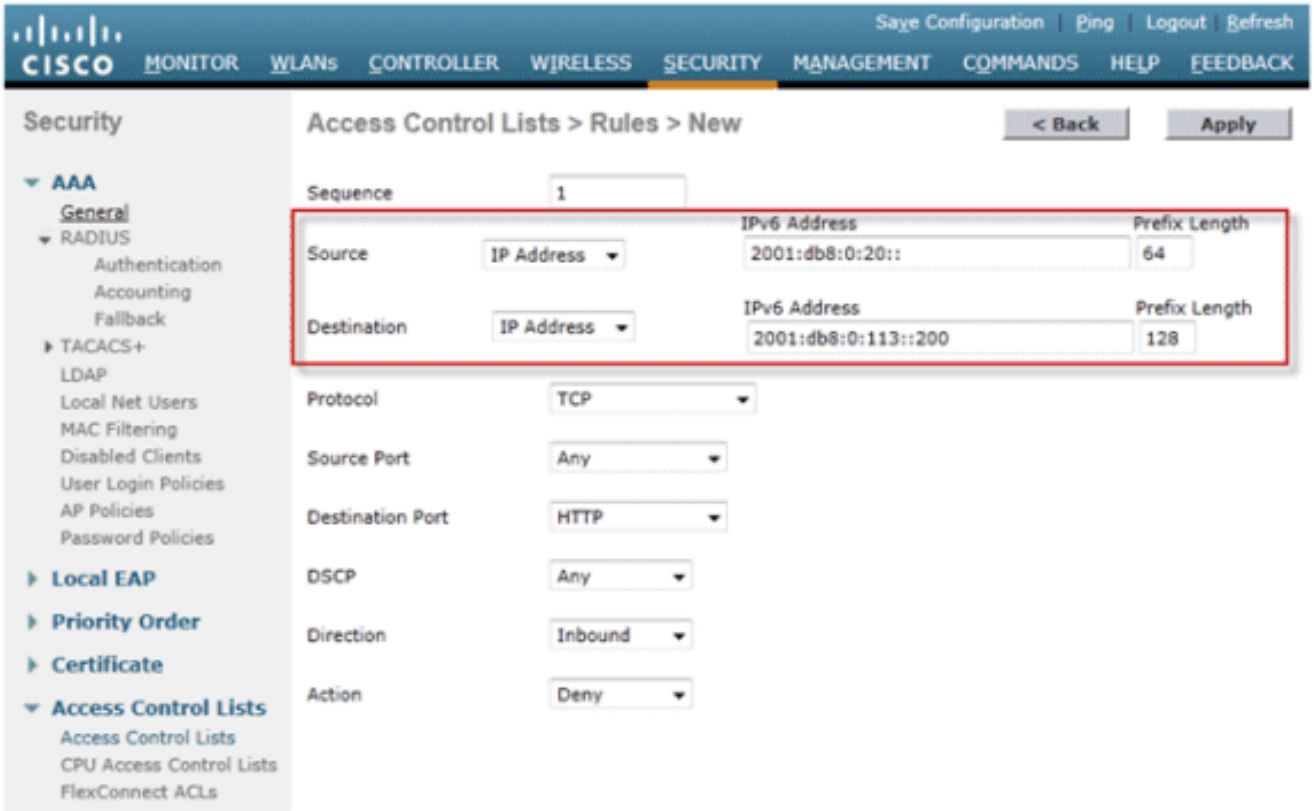


2. Immettere un nome univoco per l'ACL, modificare il tipo di ACL in **IPv6** e fare clic su **Applica**.

3. Fare clic sul nuovo ACL creato nei passaggi precedenti.

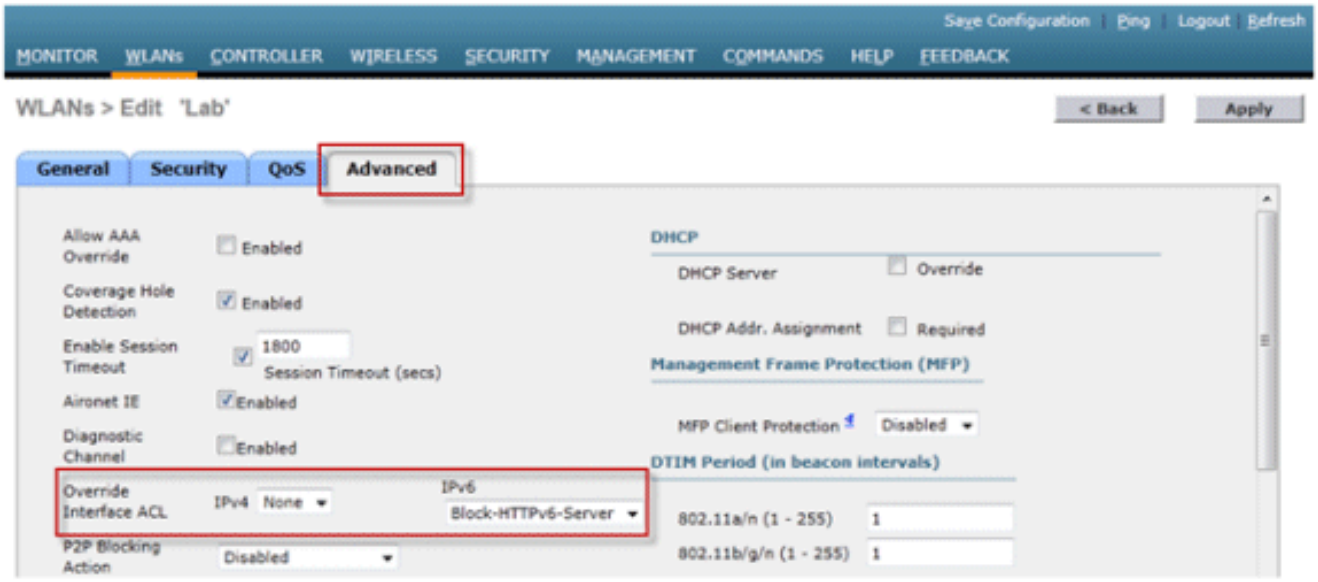


4. Fare clic su **Aggiungi nuova regola**, immettere i parametri desiderati per la regola e fare clic su **Applica**. Lasciare vuoto il numero di sequenza per inserire la regola alla fine dell'elenco. L'opzione "Direzione" di "In entrata" viene utilizzata per il traffico proveniente dalla rete wireless e "In uscita" per il traffico destinato ai client wireless. Tenere presente che l'ultima regola di un ACL è una negazione implicita di tutto. Utilizzare un prefisso di lunghezza 64 per trovare una corrispondenza con un'intera subnet IPv6 e un prefisso di lunghezza 128 per limitare in modo univoco l'accesso a un singolo indirizzo.



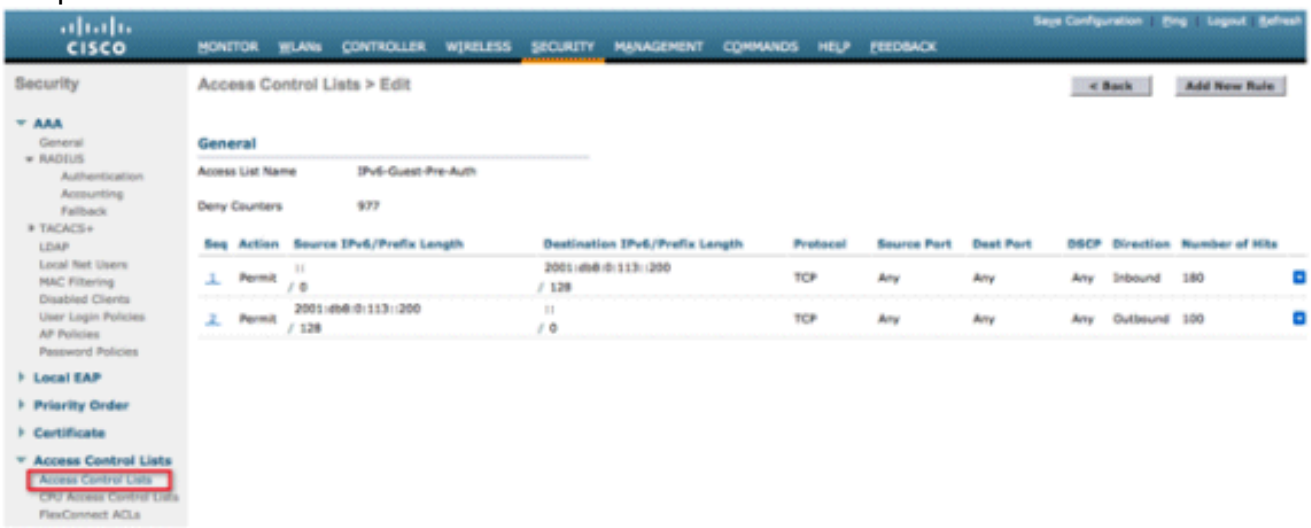
5. Gli ACL IPv6 vengono applicati per singola WLAN/SSID e possono essere utilizzati su più WLAN contemporaneamente. Per applicare l'ACL IPv6, selezionare la scheda **WLAN** e fare

clic sull'ID WLAN dell'SSID in questione. Fare clic sulla scheda **Advanced** (Avanzate) e modificare Override Interface ACL for IPv6 (Sostituisci ACL interfaccia per IPv6) nel nome ACL.

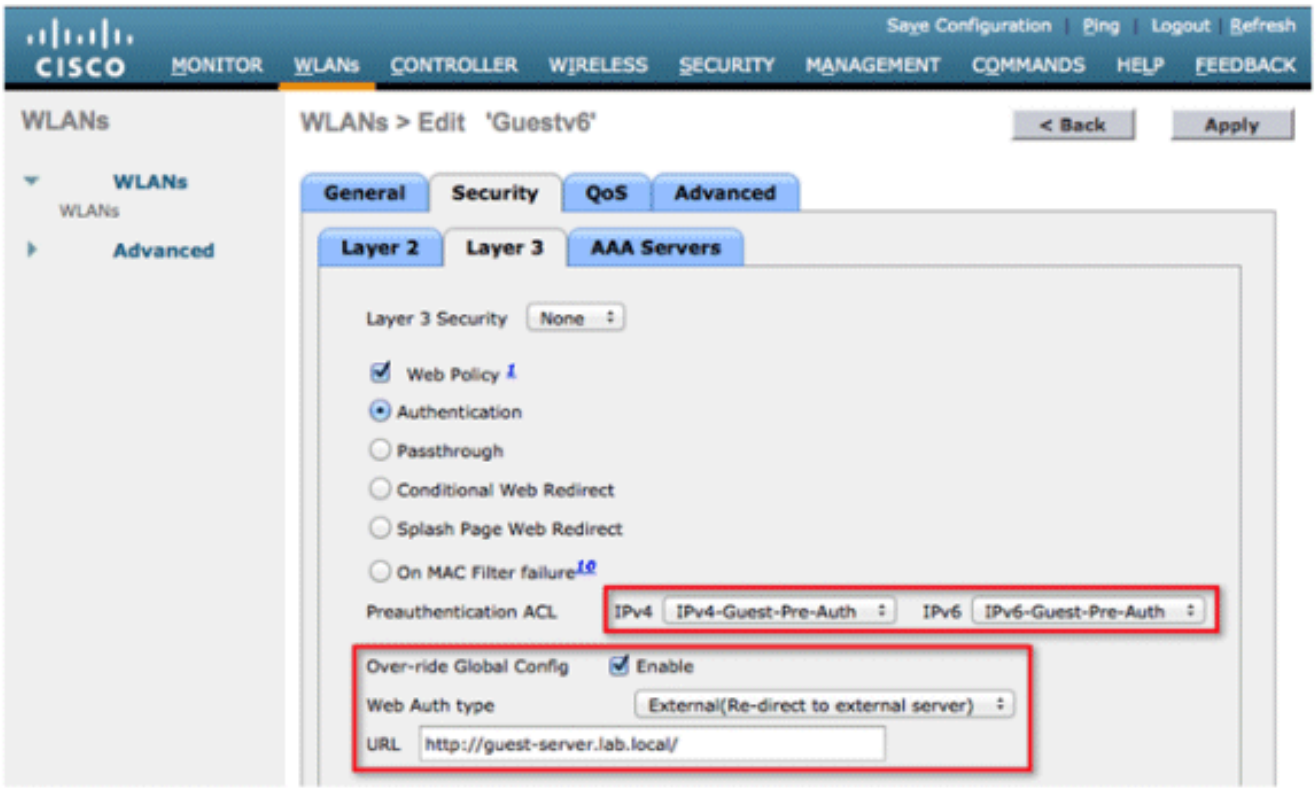


Configura accesso guest IPv6 per autenticazione Web esterna

1. Configurare l'ACL di preautenticazione IPv4 e IPv6 per il server Web. In questo modo viene consentito il traffico da e verso il server esterno prima che il client venga autenticato completamente.

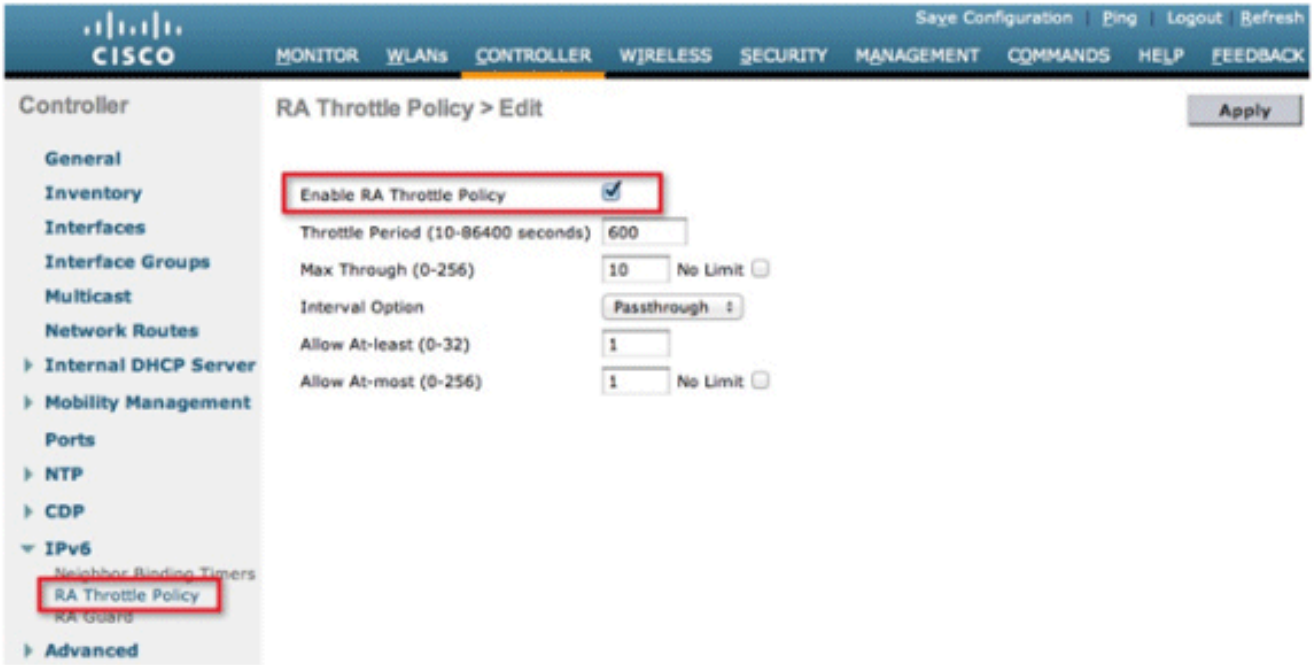


   Per ulteriori informazioni sul funzionamento dell'accesso Web esterno, fare riferimento all'esempio di configurazione dell'autenticazione Web esterna con i controller LAN wireless.
2. Configurare la WLAN guest selezionando la scheda WLAN nella parte superiore. Creare il SSID guest e utilizzare un criterio Web di layer 3. Gli ACL di preautenticazione definiti nel passaggio 1 vengono selezionati per IPv4 e IPv6. Selezionare la sezione Override Global Config e selezionare **External** dall'elenco a discesa Web Auth type (Tipo autenticazione Web). Immettere l'URL del server Web. Il nome host del server esterno deve essere risolvibile nel DNS IPv4 e
   IPv6.



Configura limitazione RA IPv6

1. Passare al menu di primo livello **Controller** e fare clic sull'opzione **IPv6 > RSA Throttle Policy** sul lato sinistro. Abilitare la limitazione RA facendo clic sulla casella di controllo.



Nota: quando si verifica la limitazione RSA, è consentito l'accesso solo al primo router compatibile con IPv6. Per le reti con più prefissi IPv6 serviti da router diversi, la limitazione di RSA deve essere disabilitata.

2. Regolare il periodo di limitazione e altre opzioni solo in base ai consigli forniti da TAC. L'impostazione predefinita è tuttavia consigliata per la maggior parte delle distribuzioni. Le varie opzioni di configurazione del criterio di limitazione RA devono essere regolate tenendo presente quanto segue:I valori numerici di "Consenti almeno" devono essere minori di

"Consenti al massimo" che devono essere minori di "Max fino a".Il criterio di limitazione RA non deve utilizzare un periodo di limitazione superiore a 1800 secondi, in quanto si tratta della durata predefinita della maggior parte degli RA.

Di seguito è descritta ciascuna opzione di limitazione RA:

- Periodo di limitazione: il periodo di tempo durante il quale viene applicata la limitazione. La limitazione della VLAN ha effetto solo dopo il raggiungimento del limite "Max Through" per la VLAN.
- Max Through: il numero massimo di Autorità di registrazione per VLAN prima che la limitazione entri. L'opzione "No Limit" consente un numero illimitato di server di registrazione attraverso senza limitazione.
- Interval Option: l'opzione interval consente al controller di agire in modo diverso in base al valore RFC 3775 impostato nell'RA IPv6.Pass-through: questo valore consente a qualsiasi RMA con un'opzione di intervallo RFC3775 di passare senza limitazioni.Ignora: questo valore fa sì che il throttler RSA consideri i pacchetti con l'opzione Intervallo come RSA normale e, se attivo, li sottoponga a limitazione.Velocità: questo valore fa sì che gli RA con l'opzione Intervallo siano sempre soggetti a limitazione della velocità.
- Consenti almeno: il numero minimo di Autorità registrazione per router che verranno inviati come multicast.
- Consenti al massimo: il numero massimo di Autorità registrazione (RA) per router che verranno inviati come multicast prima che la limitazione abbia effetto. L'opzione "No Limit" (Nessun limite) consente il passaggio di un numero illimitato di RAS per il router.

Configurare la tabella di binding adiacente IPv6

1. Andare al menu di livello superiore Controller e fare clic su **IPv6 > Neighbor Binding Timers** (Timer di binding router adiacenti) sul menu a sinistra.

2. Regolare Durata precedente, Durata raggiungibile e Durata non aggiornata in base alle esigenze. Per le distribuzioni con client altamente mobili, i timer per un timer di indirizzi non aggiornato devono essere modificati. I valori consigliati sono:Durata inattività - 30 secondiDurata raggiungibile - 300 secondiDurata stato - 86400 secondiOgni timer di durata fa riferimento allo stato in cui un indirizzo IPv6 può trovarsi:**Durata inattività** - Il timer inattivo specifica per quanto tempo le voci della cache IPv6 devono essere mantenute in caso di interruzione dell'interfaccia uplink del controller.**Durata raggiungibile**: questo timer specifica per quanto tempo un indirizzo IPv6 verrà contrassegnato come attivo, il che significa che di recente è stato ricevuto traffico da questo indirizzo. Una volta scaduto il timer, l'indirizzo viene spostato nello stato "Non aggiornato".**Durata non aggiornata**: questo timer specifica per quanto tempo conservare nella cache gli indirizzi IPv6 che non sono stati rilevati entro la durata raggiungibile. Trascorso questo periodo di tempo, l'indirizzo viene rimosso dalla tabella di binding.

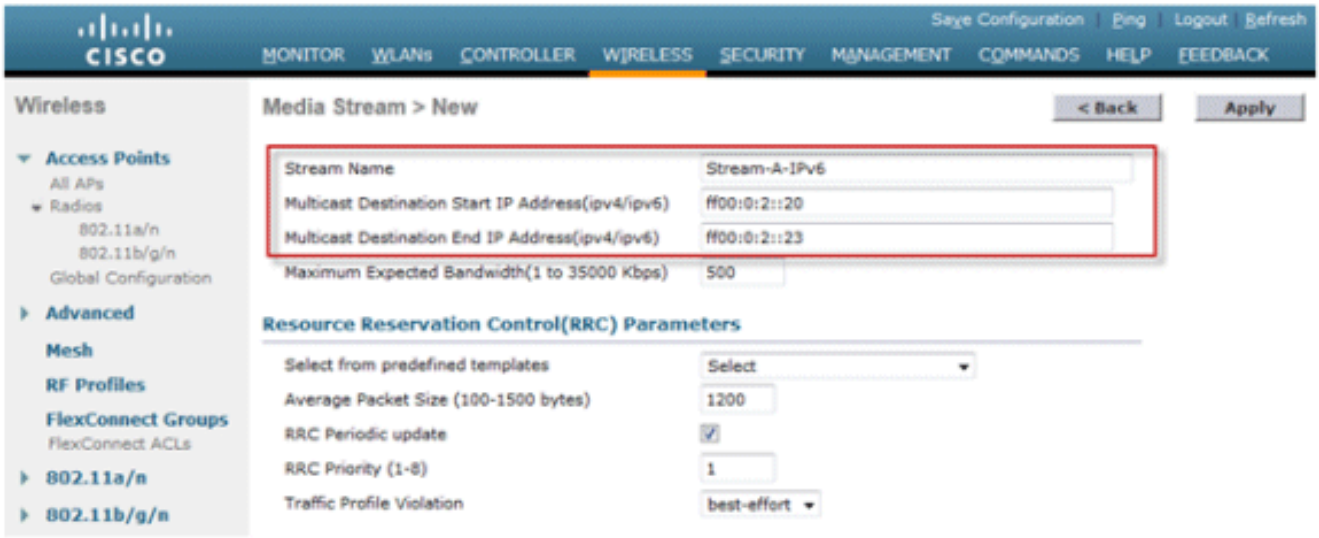
Configura VideoStream IPv6

1. Assicurarsi che le funzionalità Global VideoStream siano abilitate sul controller. Per

informazioni sull'abilitazione di VideoStream sulla rete 802.11a/g/n e sull'SSID WLAN, fare riferimento alla Cisco Unified Wireless Network Solution: VideoStream Deployment Guide.

2. Andare alla scheda **Wireless** sul controller e nel menu a sinistra, scegliere **Media Stream** > **Streams**. Per creare un nuovo flusso, fare clic su **Add New** (Aggiungi nuovo).

3. Denominare il flusso e immettere gli indirizzi IPv6 iniziale e finale. Quando si utilizza un solo flusso, gli indirizzi iniziale e finale sono uguali. Dopo aver aggiunto gli indirizzi, fare clic su **Apply** (Applica) per creare il flusso.



Risoluzione dei problemi di connettività client IPv6

Alcuni client non sono in grado di passare il traffico IPv6

Alcune implementazioni dello stack di rete IPv6 del client non si annunciano correttamente quando entrano nella rete e pertanto il relativo indirizzo non viene snooping appropriato dal controller per il posizionamento nella tabella di binding dei nodi adiacenti. Tutti gli indirizzi non presenti nella tabella di binding dei nodi adiacenti vengono bloccati in base alla funzionalità di protezione origine IPv6. Per consentire a questi client di passare il traffico, è necessario configurare le seguenti opzioni:

1. Disabilitare la funzionalità IPv6 Source Guard dalla CLI:

   config network ip-mac-binding disable

2. Abilitare l'inoltro di richieste router adiacenti multicast tramite la CLI:

   config ipv6 ns-mcast-fwd enable

Verificare che il roaming di layer 3 per un client IPv6 sia riuscito:

Utilizzare i seguenti comandi di **debug** sull'ancoraggio e sul controller esterno:

debug client

debug mobility handoff enable

debug mobility packet enable

Risultati di debug sul controller di ancoraggio:

```
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
```

Risultati di debug sul controller esterno:

```
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
```

Comandi CLI IPv6 utili:

Show ipv6 neighbor-binding summary

Debug ipv6 neighbor-binding filter client enable

Debug ipv6 neighbor-binding filter errors enable

Domande frequenti

D: Qual è la dimensione ottimale del prefisso IPv6 per limitare il dominio di broadcast?

R: Sebbene sia possibile suddividere una subnet IPv6 al di sotto di /64, questa configurazione interromperà lo SLAAC e causerà problemi di connettività del client. Se è necessaria la segmentazione per ridurre il numero di host, è possibile utilizzare la funzionalità Gruppi di interfacce per bilanciare il carico dei client tra VLAN back-end diverse, ognuna delle quali utilizza un prefisso IPv6 diverso.

D. Esistono limiti di scalabilità quando si tratta di supportare i client IPv6?

R: La principale limitazione di scalabilità per il supporto dei client IPv6 è rappresentata dalla tabella di binding adiacente che tiene traccia di tutti gli indirizzi IPv6 dei client wireless. Questa tabella viene ridimensionata per piattaforma controller in modo da supportare il numero massimo di client moltiplicato per otto (il numero massimo di indirizzi per client). L'aggiunta della tabella di binding IPv6 può aumentare l'utilizzo della memoria del controller di circa il 10-15% a pieno carico, a seconda della piattaforma.

Controller wireless	Numero massimo di client	Dimensione tabella di binding adiacente IPv6
2500	500	4,000
5500	7,000	56,000
WiSM2	15,000	120,000

D: Qual è l'impatto delle funzionalità IPv6 sulla CPU e la memoria del controller?

R: L'impatto è minimo in quanto la CPU dispone di più core per l'elaborazione del control plane. Durante i test eseguiti con il numero massimo di client supportati, ciascuno con 8 indirizzi IPv6,

l'utilizzo della CPU è stato inferiore al 30% e quello della memoria al 75%.

D: È possibile disabilitare il supporto client IPv6?

R: Per i clienti che desiderano abilitare solo IPv4 nella rete e bloccare IPv6, è possibile utilizzare e applicare un ACL IPv6 di traffico "deny-all" per singola WLAN.

D: È possibile avere una WLAN per IPv4 e un'altra per IPv6?

R: Non è possibile avere lo stesso nome SSID e lo stesso tipo di sicurezza per due diverse WLAN che operano sullo stesso access point. Per la segmentazione dei client IPv4 dai client IPv6, è necessario creare due WLAN. Ogni WLAN deve essere configurata con un ACL che blocchi tutto il traffico IPv4 o IPv6, rispettivamente.

D. Perché è importante supportare più indirizzi IPv6 per client?

R: I client possono avere più indirizzi IPv6 per interfaccia, che possono essere statici, SLAAC o DHCPv6, oltre a disporre sempre di un indirizzo Link-Local autoassegnato. I client possono inoltre disporre di indirizzi aggiuntivi utilizzando prefissi IPv6 diversi.

D: Che cosa sono gli indirizzi privati IPv6 e perché sono importanti da tenere traccia?

R: Gli indirizzi privati (anche noti come temporanei) vengono generati in modo casuale dal client quando è in uso l'assegnazione degli indirizzi SLAAC. Questi indirizzi vengono spesso ruotati alla frequenza di un giorno o giù di lì, in modo da impedire la tracciabilità dell'host che deriverebbe dall'utilizzo dello stesso suffisso host (ultimi 64 bit) in qualsiasi momento. È importante tenere traccia di questi indirizzi privati a scopo di verifica, ad esempio per individuare le violazioni del copyright. Cisco NCS registra tutti gli indirizzi IPv6 in uso da ogni client e li registra in modo cronologico ogni volta che il client esegue il roaming o stabilisce una nuova sessione. Questi record possono essere configurati su NCS per essere conservati fino a un anno.

Informazioni correlate

- Documentazione e supporto tecnico – Cisco Systems

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).