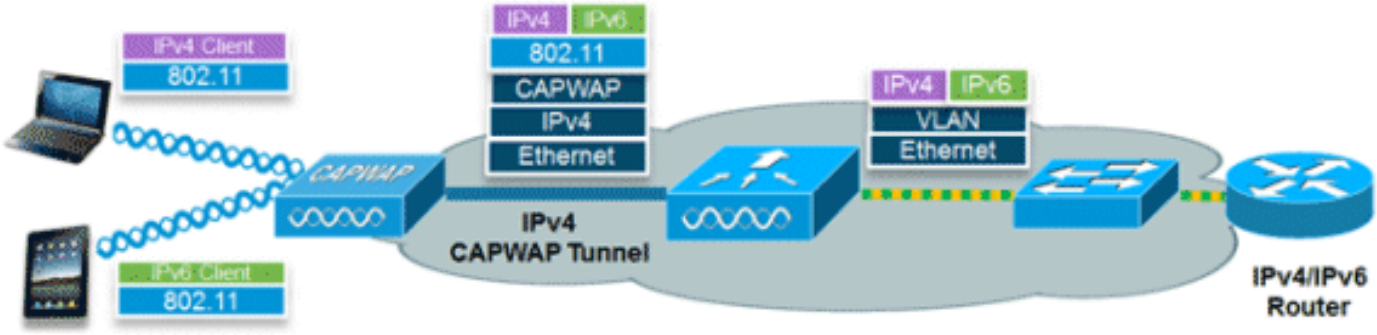
무선 LAN IPv6 클라이언트 구축 설명서

목차

소개

이 문서에서는 IPv6 클라이언트 지원과 관련된 Cisco Unified Wireless LAN 솔루션의 운영 및 구성 이론에 대한 정보를 제공합니다.

IPv6 무선 클라이언트 연결



Cisco Unified Wireless Network 소프트웨어 릴리스 v7.2에 설정된 IPv6 기능을 통해 무선 네트워크는 동일한 무선 네트워크에서 IPv4, 듀얼 스택 및 IPv6 전용 클라이언트를 지원할 수 있습니다. Cisco Unified Wireless LAN에 IPv6 클라이언트 지원을 추가하는 전체적인 목표는 모빌리티, 보안, 게스트 액세스, QoS(Quality of Service), 엔드포인트 가시성 등 IPv4와 IPv6 클라이언트 간의 기능 패리티를 유지하는 것이었습니다.

디바이스당 최대 8개의 IPv6 클라이언트 주소를 추적할 수 있습니다. 이를 통해 IPv6 클라이언트는 링크-로컬 SLAAC(Stateless Address Auto Configuration) 주소, IPv6(DHCPv6)용 Dynamic Host Configuration Protocol 주소, 그리고 단일 인터페이스에 있을 대체 접두사의 주소까지 가질 수 있습니다. WGB 모드에서 자동 AP(액세스 포인트)의 업링크에 연결된 WGB(작업 그룹 브리지) 클라이언트도 IPv6를 지원할 수 있습니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Wireless LAN Controller 2500 Series, 5500 Series 또는 WiSM2
- AP 1130, 1240, 1250, 1040, 1140, 1260, 3500, 3600 Series AP 및 1520 또는 1550 Series

Mesh AP

- IPv6 지원 라우터

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

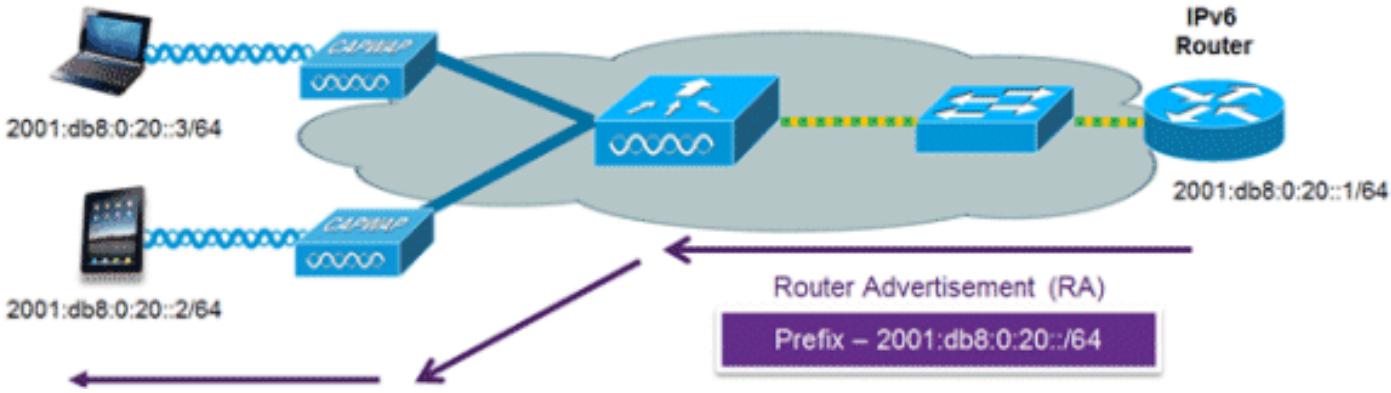
표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참고하십시오.

무선 IPv6 클라이언트 연결 사전 요구 사항

무선 IPv6 클라이언트 연결을 활성화하려면 기본 유선 네트워크에서 IPv6 라우팅 및 SLAAC 또는 DHCPv6와 같은 주소 할당 메커니즘을 지원해야 합니다. 무선 LAN 컨트롤러는 IPv6 라우터에 L2 인접성을 가져야 하며, 패킷이 컨트롤러에 들어올 때 VLAN에 태그를 지정해야 합니다. 모든 트래픽은 AP와 컨트롤러 간의 IPv4 CAPWAP 터널 내부에서 캡슐화되므로 AP는 IPv6 네트워크에서 연결할 필요가 없습니다.

SLAC 주소 할당

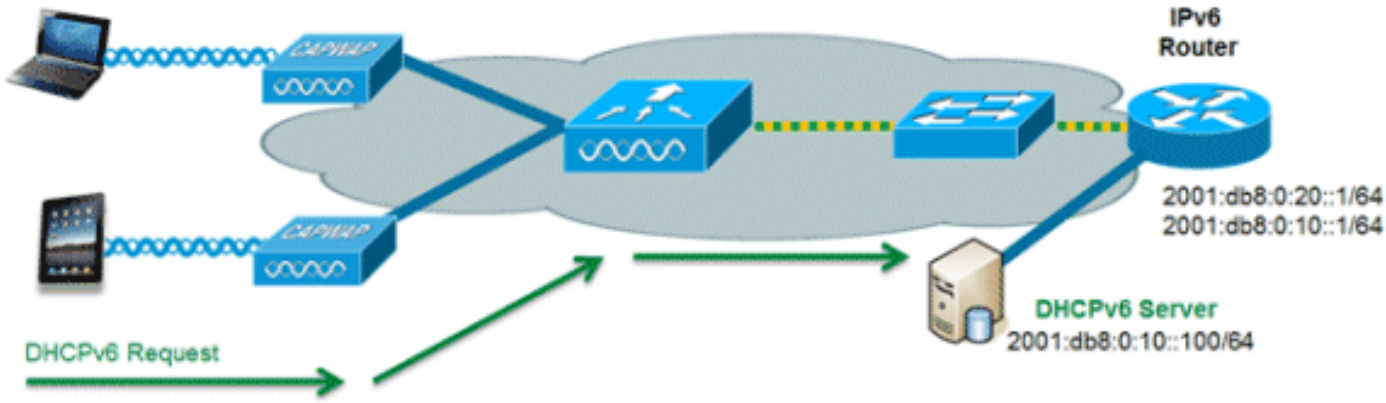


IPv6 클라이언트 주소 할당을 위한 가장 일반적인 방법은 SLAAC입니다. SLAAC는 클라이언트가 IPv6 접두사를 기반으로 주소를 자체 할당하는 간단한 플러그 앤 플레이 연결을 제공합니다. 이 프로세스는 IPv6 라우터가 사용 중인 IPv6 접두사(처음 64비트)와 IPv6 기본 게이트웨이를 클라이언트에 알리는 주기적인 라우터 알림 메시지를 전송할 때 구현됩니다. 이 시점부터 클라이언트는 인터페이스의 MAC 주소를 기반으로 하는 EUI-64 또는 임의로 생성되는 사설 주소 등 두 가지 알고리즘을 기반으로 IPv6 주소의 나머지 64비트를 생성할 수 있습니다. 알고리즘은 클라이언트에 따라 선택되며 종종 구성 가능합니다. 선택한 임의 주소가 다른 클라이언트와 충돌하지 않도록 IPv6 클라이언트에서 중복 주소 감지를 수행합니다. 광고를 전송하는 라우터의 주소는 클라이언트의 기본 게이트웨이로 사용됩니다.

Cisco-capable IPv6 라우터의 이러한 Cisco IOS® 컨피그레이션 명령은 SLAAC 주소 지정 및 라우터 광고를 활성화하는 데 사용됩니다.

```
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 주소 할당



SLAAC가 이미 구축된 경우 IPv6 클라이언트 연결에 DHCPv6를 사용할 필요가 없습니다. DHCPv6에는 스테이트리스(Stateless) 및 스테이트풀(Stateful)이라는 두 가지 운영 모드가 있습니다.

DHCPv6 상태 비저장 모드는 라우터 광고에서 사용할 수 없는 추가 네트워크 정보를 클라이언트에 제공하는 데 사용되지만 SLAAC에서 이미 제공한 IPv6 주소는 아닙니다. 이 정보에는 DNS 도메인 이름, DNS 서버 및 기타 DHCP 공급업체별 옵션이 포함될 수 있습니다. 이 인터페이스 컨피그레이션은 SLAAC가 활성화된 상태 비저장 DHCPv6를 구현하는 Cisco IOS IPv6 라우터를 위한 것입니다.

```
ipv6 unicast-routing
interface Vlan20
 description IPv6-DHCP-Stateless
 ip address 192.168.20.1 255.255.255.0
 ipv6 enable
 ipv6 address 2001:DB8:0:20::1/64
 ipv6 nd other-config-flag
 ipv6 dhcp relay destination 2001:DB8:0:10::100
end
```

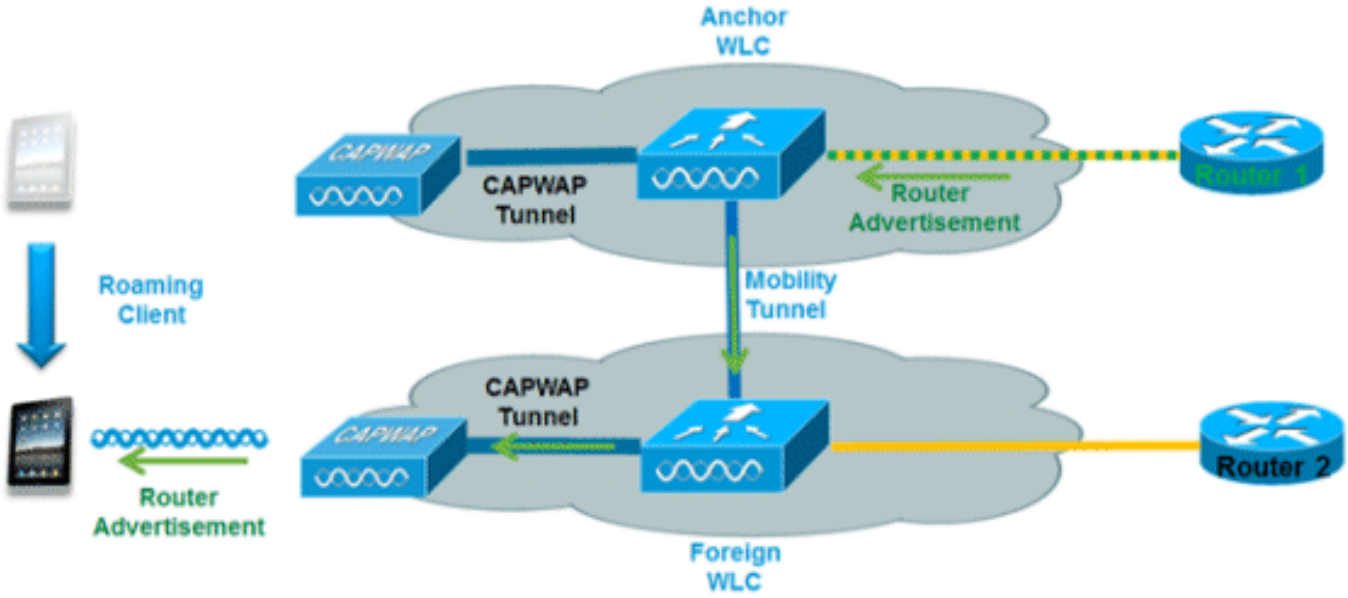
DHCPv6 상태 저장 옵션(관리 모드라고도 함)은 클라이언트가 SLAAC에서와 같이 주소의 마지막 64비트를 생성하는 대신 각 클라이언트에 고유한 주소를 할당한다는 점에서 DHCPv4와 유사하게 작동합니다. 이 인터페이스 컨피그레이션은 SLAAC가 비활성화된 상태 기반 DHCPv6를 구현하는 Cisco IOS IPv6 라우터를 위한 것입니다.

```
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
```

추가 정보

듀얼 스택 또는 터널링 연결 방식을 사용하여 캠퍼스 전체에 완전한 IPv6 연결을 제공하도록 유선 네트워크를 구성하는 것은 이 문서의 범위에 속하지 않습니다. 자세한 내용은 Cisco validated deployment guide Deploying IPv6 in Campus Networks를 참조하십시오.

IPv6 클라이언트 모빌리티



컨트롤러에서 로밍 IPv6 클라이언트를 처리하려면 클라이언트가 동일한 레이어 3 네트워크에 유지되도록 하기 위해 NS(Neighbor Solicitation), NA(Neighbor Advertisement), RA(Router Advertisement) 및 RS(Router Solicitation)와 같은 ICMPv6 메시지를 특별히 처리해야 합니다. IPv6 모빌리티의 컨피그레이션은 IPv4 모빌리티와 동일하며 원활한 로밍을 위해 클라이언트 측에 별도의 소프트웨어가 필요하지 않습니다. 컨트롤러가 동일한 모빌리티 그룹/도메인에 속해야 한다는 컨피그레이션만 필요합니다.

다음은 컨트롤러 간 IPv6 클라이언트 모빌리티를 위한 프로세스입니다.

1. 두 컨트롤러 모두 클라이언트가 원래 있던 동일한 VLAN에 액세스할 수 있는 경우 로밍은 단순히 클라이언트 레코드가 새 컨트롤러로 복사되고 트래픽이 앵커 컨트롤러로 다시 터널링되지 않는 레이어 2 로밍 이벤트입니다.

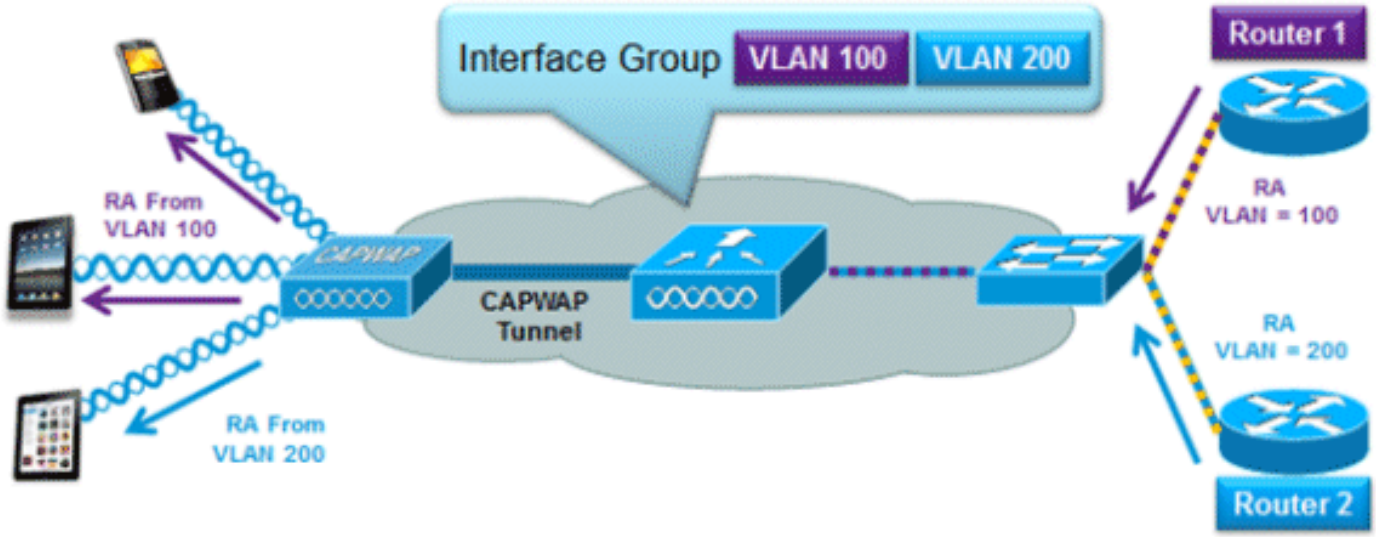
2. 두 번째 컨트롤러에서 클라이언트가 켜져 있던 원래 VLAN에 액세스할 수 없는 경우 레이어 3 로밍 이벤트가 발생합니다. 즉, 클라이언트의 모든 트래픽이 모빌리티 터널(Ethernet over IP)을 통해 앵커 컨트롤러로 터널링되어야 합니다.

   a. 클라이언트가 원래 IPv6 주소를 유지하도록 하기 위해 원래 VLAN의 RA는 앵커 컨트롤러에서 외부 컨트롤러로 전송되며, 여기서 AP의 L2 유니캐스트를 사용하여 클라이언트에 전달됩니다.

   b. 로밍된 클라이언트가 DHCPv6를 통해 주소를 갱신하거나 SLAAC를 통해 새 주소를 생성하면 RS, NA 및 NS 패킷은 원래 VLAN으로 계속 터널링되므로 클라이언트는 해당 VLAN에 적용할 수 있는 IPv6 주소를 받게 됩니다.

참고: IPv6 전용 클라이언트의 모빌리티는 VLAN 정보를 기반으로 합니다. 이는 IPv6 전용 클라이언트 모빌리티가 태그되지 않은 VLAN에서 지원되지 않음을 의미합니다.

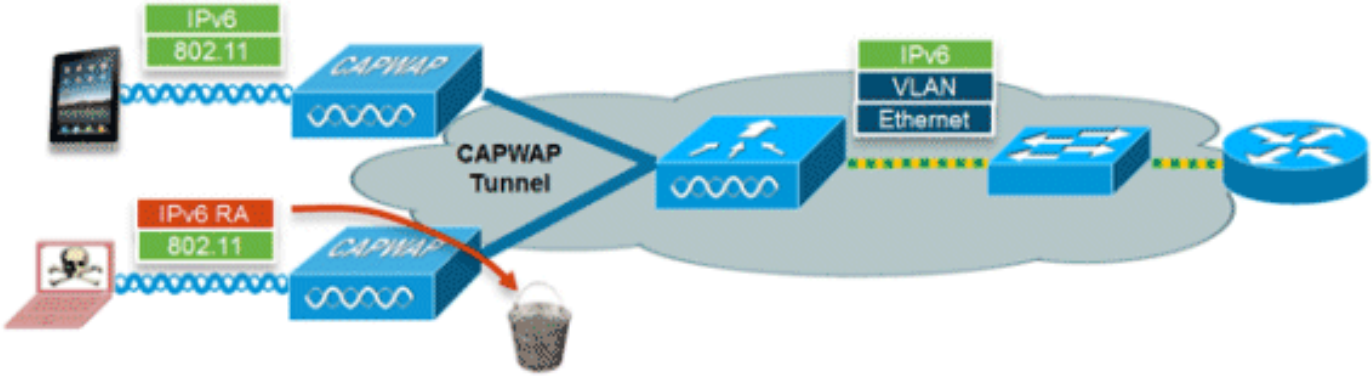
VLAN 선택 지원(인터페이스 그룹)



인터페이스 그룹 기능을 사용하면 조직에서 컨트롤러에 여러 VLAN이 구성된 단일 WLAN을 보유하여 이러한 VLAN에서 무선 클라이언트의 로드 밸런싱을 허용할 수 있습니다. 이 기능은 일반적으로 IPv4 서브넷 크기를 작게 유지하면서 그룹의 여러 VLAN에서 WLAN을 수천 명의 사용자로 확장할 수 있도록 하는 데 사용됩니다. 인터페이스 그룹이 있는 IPv6 클라이언트를 지원하기 위해, 시스템이 L2 무선 유니캐스트를 통해 올바른 클라이언트에 올바른 RA를 자동으로 전송하기 때문에 추가 컨피그레이션이 필요하지 않습니다. RA를 유니캐스트하면 동일한 WLAN에 있지만 다른 VLAN에 있는 클라이언트는 잘못된 RA를 수신하지 않습니다.

IPv6 클라이언트에 대한 첫 번째 홉 보안

라우터 알림 보호



RA Guard 기능은 무선 클라이언트에서 오는 RA를 삭제하여 IPv6 네트워크의 보안을 향상시킵니다. 이 기능이 없으면 잘못 구성되거나 악의적인 IPv6 클라이언트가 대개 우선순위가 높아서 합법적인 IPv6 라우터보다 우선할 수 있는 네트워크 라우터로 자신을 알릴 수 있습니다.

기본적으로 RA Guard는 AP에서 활성화되지만(그러나 AP에서 비활성화될 수 있음) 컨트롤러에서 항상 활성화됩니다. AP에서 RA를 삭제하는 것이 더 확장성이 뛰어난 솔루션이며 향상된 클라이언트당 RA 삭제 카운터를 제공하므로 선호됩니다. 모든 경우에 IPv6 RA는 어느 시점에 삭제되어 악의적이거나 잘못 구성된 IPv6 클라이언트로부터 다른 무선 클라이언트 및 업스트림 유선 네트워크를 보호합니다.

DHCPv6 서버 가드

DHCPv6 Server Guard 기능은 무선 클라이언트가 IPv6 주소를 다른 무선 클라이언트 또는 유선 클라이언트 업스트림에 전달하는 것을 방지합니다. DHCPv6 주소가 제공되지 않도록 하기 위해 무선 클라이언트의 DHCPv6 advertise 패킷이 삭제됩니다. 이 기능은 컨트롤러에서 작동하며 컨피그레이션이 필요하지 않으며 자동으로 활성화됩니다.

IPv6 소스 가드

IPv6 Source Guard 기능은 무선 클라이언트가 다른 클라이언트의 IPv6 주소를 스푸핑하는 것을 방지합니다. 이 기능은 IPv4 Source Guard와 유사합니다. IPv6 Source Guard는 기본적으로 활성화되어 있지만 CLI를 통해 비활성화할 수 있습니다.

IPv6 주소 계정 관리

RADIUS 인증 및 어카운팅의 경우 컨트롤러는 "Framed-IP-address" 특성을 사용하여 하나의 IP 주소를 다시 보냅니다. 이 경우 IPv4 주소가 사용됩니다.

컨트롤러의 "Call Station ID Type(호출 스테이션 ID 유형)"이 "IP Address(IP 주소)"로 구성된 경우 "Calling-Station-ID" 특성은 다음 알고리즘을 사용하여 IP 주소를 다시 전송합니다.

1. IPv4 주소
2. 전역 유니캐스트 IPv6 주소
3. 링크 로컬 IPv6 주소

클라이언트 IPv6 주소는 자주 변경될 수 있으므로(임시 또는 개인 주소) 시간이 지남에 따라 추적하

는 것이 중요합니다. Cisco NCS는 각 클라이언트에서 사용 중인 모든 IPv6 주소를 기록하고, 클라이언트가 로밍하거나 새 세션을 설정할 때마다 기록 방식으로 기록합니다. 이러한 레코드는 NCS에서 최대 1년까지 보유하도록 구성할 수 있습니다.

참고: 버전 7.2에서는 컨트롤러의 "Call Station ID Type(통화 스테이션 ID 유형)"의 기본값이 "System MAC Address(시스템 MAC 주소)"로 변경되었습니다. 업그레이드할 때 IPv6 주소가 세션 중간에 변경되어 Calling-Station-ID가 IP 주소로 설정된 경우 어카운팅에 문제가 발생할 수 있으므로 MAC 주소별로 클라이언트를 고유하게 추적할 수 있도록 변경해야 합니다.

IPv6 액세스 제어 목록

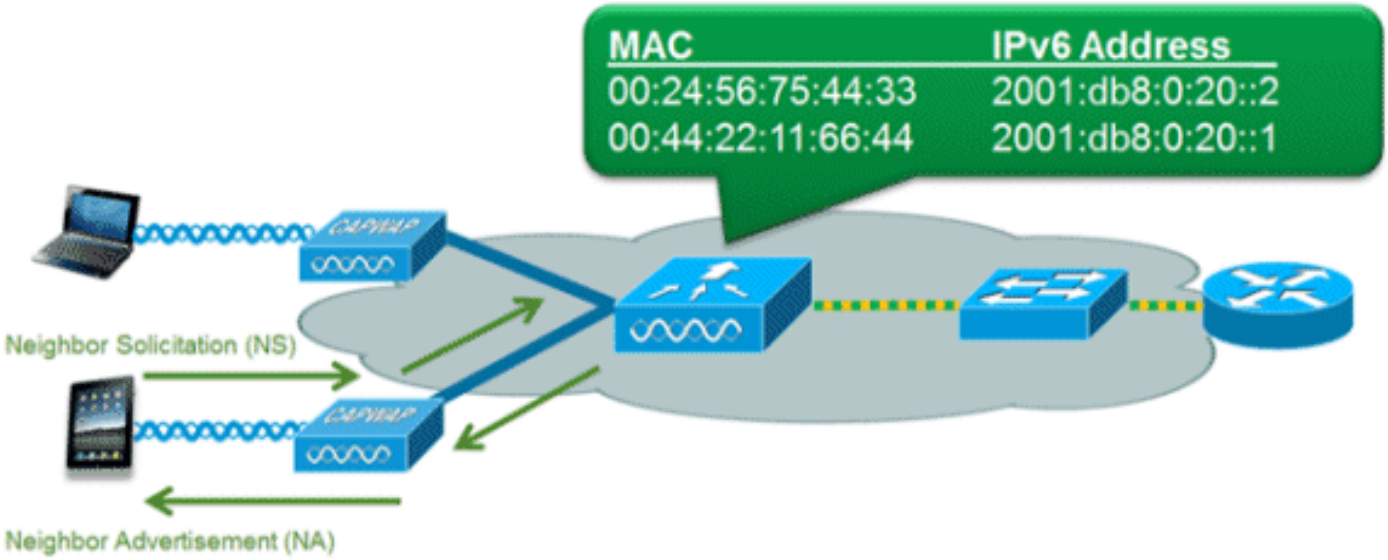
특정 업스트림 유선 리소스에 대한 액세스를 제한하거나 특정 애플리케이션을 차단하기 위해 IPv6 ACL(Access Control List)을 사용하여 트래픽을 식별하고 허용하거나 거부할 수 있습니다. IPv6 ACL은 IPv4 ACL과 동일한 옵션(소스, 목적지, 소스 포트, 목적지 포트)을 지원합니다(포트 범위도 지원됨). 외부 웹 서버를 사용한 IPv6 게스트 인증을 지원하기 위해 사전 인증 ACL도 지원됩니다. 무선 컨트롤러는 각각 64개의 고유한 규칙으로 최대 64개의 고유한 IPv6 ACL을 지원합니다. 무선 컨트롤러는 듀얼 스택 클라이언트에 대해 총 128개의 ACL에 대해 각각 64개의 고유한 규칙으로 추가 64개의 고유한 IPv4 ACL을 계속 지원합니다.

IPv6 ACL에 대한 AAA 재정의

Cisco ISE(Identity Services Engine) 또는 ACS와 같은 중앙 집중식 AAA 서버를 통한 중앙 집중식 액세스 제어를 지원하기 위해 AAA Override 특성을 사용하여 클라이언트별로 IPv6 ACL을 프로비저닝할 수 있습니다. 이 기능을 사용하려면 컨트롤러에서 IPv6 ACL을 구성해야 하고 AAA Override 기능을 활성화하여 WLAN을 구성해야 합니다. IPv6 ACL에 대한 실제 명명된 AAA 특성은 IPv4 기반 ACL을 프로비저닝하는 데 사용되는 Airespace-ACL-Name 특성과 유사한 Airespace-IPv6-ACL-Name입니다. 반환된 AAA 특성은 컨트롤러에 구성된 IPv6 ACL의 이름과 같은 문자열이어야 합니다.

IPv6 클라이언트에 대한 패킷 최적화

네이버 검색 캐싱



IPv6 NDP(Neighbor Discovery Protocol)는 IPv6 클라이언트가 네트워크에 있는 다른 클라이언트의 MAC 주소를 확인할 수 있도록 ARP(Address Resolution Protocol) 대신 NA 및 NS 패킷을 사용합니다. NDP 프로세스는 초기에 주소 확인을 수행하기 위해 멀티캐스트 주소를 사용하므로 매우 수다스러울 수 있습니다. 따라서 네트워크 세그먼트의 모든 클라이언트에 멀티캐스트 패킷이 전송되므로 귀중한 무선 통신 시간이 소모될 수 있습니다.

NDP 프로세스의 효율성을 높이기 위해 네이버 검색 캐싱을 사용하면 컨트롤러가 프록시 역할을 하고 해결할 수 있는 NS 쿼리에 다시 응답할 수 있습니다. 네이버 검색 캐싱은 컨트롤러에 있는 기본 네이버 바인딩 테이블에 의해 가능합니다. 네이버 바인딩 테이블은 각 IPv6 주소 및 연결된 MAC 주소를 추적합니다. IPv6 클라이언트가 다른 클라이언트의 링크 계층 주소를 확인하려고 시도할 때 NS 패킷이 컨트롤러에서 가로채기되며 컨트롤러는 NA 패킷으로 응답합니다.

라우터 광고 제한

라우터 광고 조절(Router Advertisement Throttling)을 통해 컨트롤러는 무선 네트워크로 향하는 RA의 속도 제한을 시행할 수 있습니다. RA 제한을 활성화하면 RA를 매우 자주(예: 3초마다) 전송하도록 구성된 라우터를 IPv6 클라이언트 연결을 유지하는 최소 주파수로 줄일 수 있습니다. 따라서 전송해야 하는 멀티캐스트 패킷의 수를 줄여 통신 시간을 최적화할 수 있습니다. 모든 경우 클라이언트가 RS를 전송하면 RA는 컨트롤러를 통해 허용되고 요청 클라이언트에 유니캐스트됩니다. 이는 새 클라이언트 또는 로밍 클라이언트가 RA 제한의 부정적인 영향을 받지 않도록 하기 위한 것입니다.

IPv6 게스트 액세스

IPv4 클라이언트에 제공되는 무선 및 유선 게스트 기능은 듀얼 스택 및 IPv6 전용 클라이언트에서도 동일하게 작동합니다. 게스트 사용자가 연결하면 클라이언트가 IPv4 또는 IPv6 종속 포털을 통해 인증될 때까지 "WEB_AUTH_REQ" 실행 상태가 됩니다. 컨트롤러는 이 상태에서 IPv4 및 IPv6 HTTP/HTTPS 트래픽을 모두 가로채서 컨트롤러의 가상 IP 주소로 리디렉션합니다. 사용자가 종속 포털을 통해 인증되면 MAC 주소가 실행 상태로 이동하며 IPv4 및 IPv6 트래픽 모두 통과가 허용됩니다. 외부 웹 인증의 경우 사전 인증 ACL을 통해 외부 웹 서버를 사용할 수 있습니다.

IPv6 전용 클라이언트의 리디렉션을 지원하기 위해 컨트롤러는 컨트롤러에 구성된 IPv4 가상 주소를 기반으로 IPv6 가상 주소를 자동으로 생성합니다. 가상 IPv6 주소는 `[::ffff:<virtual IPv4 address>]` 규칙을 따릅니다. 예를 들어 1.1.1.1의 가상 IP 주소는 `[::ffff:1.1.1.1]`로 변환됩니다.

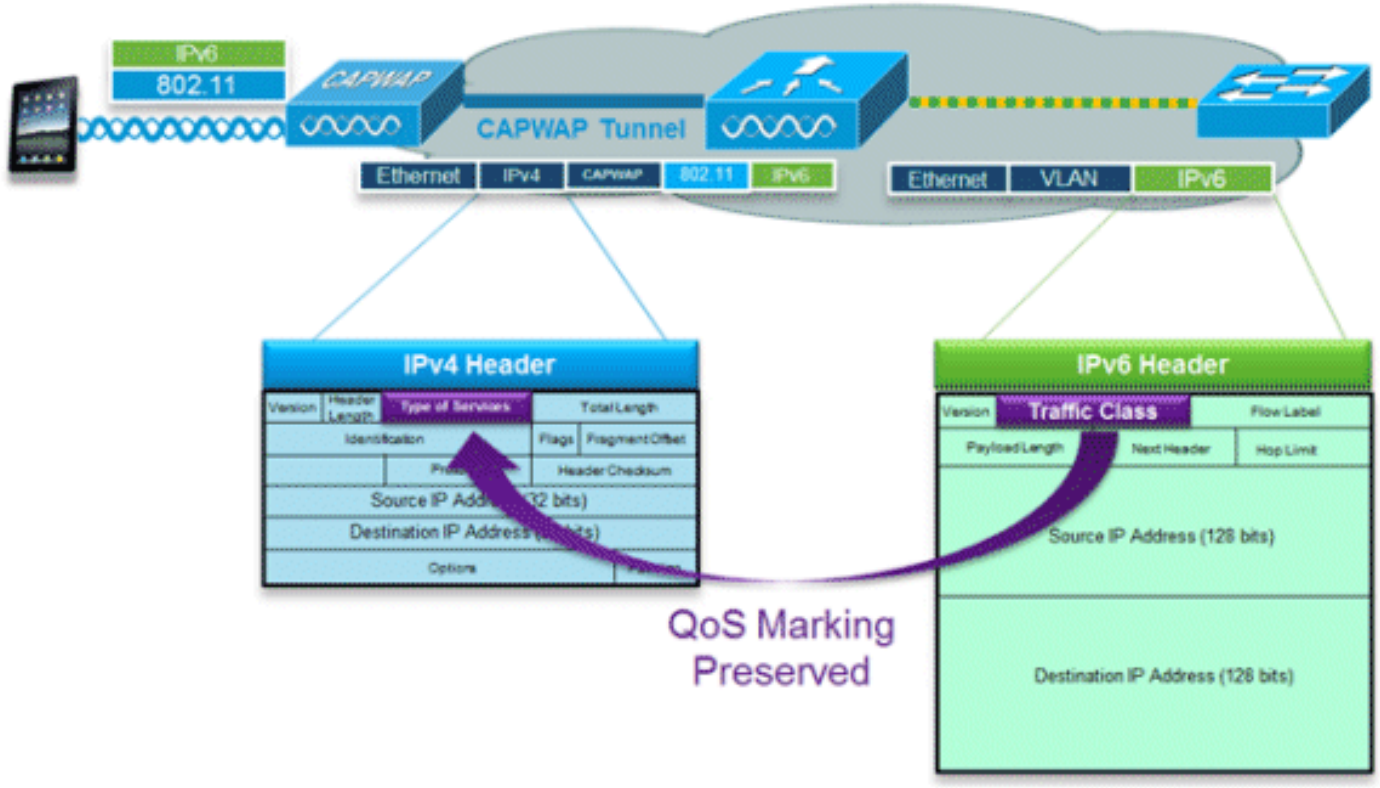
게스트 액세스 인증에 신뢰할 수 있는 SSL 인증서를 사용할 경우 컨트롤러의 IPv4 및 IPv6 가상 주소가 SSL 인증서 호스트 이름과 일치하도록 DNS에 정의되었는지 확인합니다. 이렇게 하면 인증서가 디바이스의 호스트 이름과 일치하지 않는다는 보안 경고가 클라이언트에 표시되지 않습니다.

참고: 컨트롤러의 자동 생성 SSL 인증서에는 IPv6 가상 주소가 포함되어 있지 않습니다. 이로 인해 일부 웹 브라우저에서 보안 경고가 표시될 수 있습니다. 게스트 액세스에 신뢰할 수 있는 SSL 인증서를 사용하는 것이 좋습니다.

IPv6 비디오 스트림

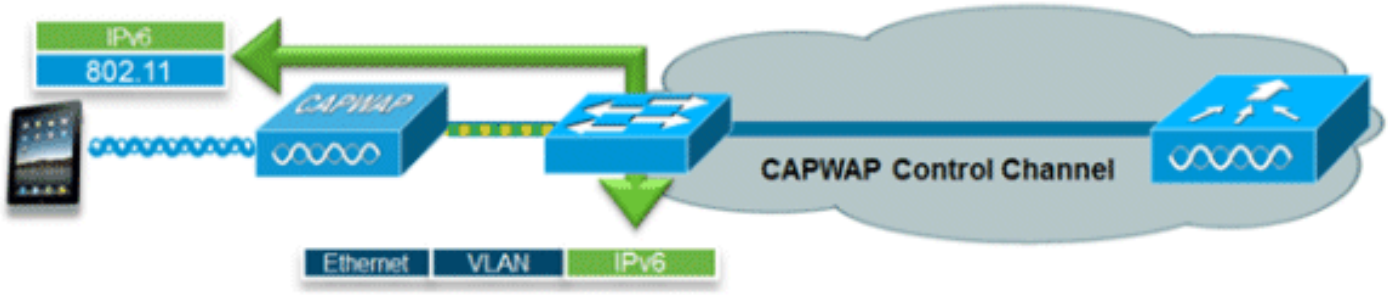
VideoStream은 각 클라이언트에 스트림을 유니캐스트 형식으로 전송하여 안정적이고 확장 가능한 무선 멀티캐스트 비디오 전송을 지원합니다. (L2의) 실제 멀티캐스트 대 유니캐스트 변환은 확장 가능한 솔루션을 제공하는 AP에서 발생합니다. 컨트롤러는 IPv4 CAPWAP 멀티캐스트 터널 내에서 IPv6 비디오 트래픽을 전송하며, 이를 통해 AP에 효율적인 네트워크 배포가 가능합니다.

IPv6 서비스 품질



IPv6 패킷은 IPv4가 최대 64개의 서로 다른 트래픽 클래스(0~63)를 지원하는 DSCP 값을 사용하는 것과 유사한 표시를 사용합니다. 유선 네트워크의 다운스트림 패킷의 경우, QoS가 엔드 투 엔드로 유지되도록 하기 위해 IPv6 Traffic Class 값이 CAPWAP 터널의 헤더에 복사됩니다. 업스트림 방향에서는 IPv6 트래픽 클래스가 있는 레이어 3에서 표시된 클라이언트 트래픽이 컨트롤러로 향하는 CAPWAP 패킷을 표시하는 방식으로 처리되므로 동일한 현상이 발생합니다.

IPv6 및 FlexConnect



FlexConnect - 로컬 스위칭 WLAN

로컬 스위칭 모드의 FlexConnect는 IPv4 작업과 유사하게 트래픽을 로컬 VLAN에 브리징하여 IPv6 클라이언트를 지원합니다. 클라이언트 모빌리티는 FlexConnect 그룹 전반의 레이어 2 로밍에서 지원됩니다.

이러한 IPv6 관련 기능은 FlexConnect 로컬 스위칭 모드에서 지원됩니다.

- IPv6 RA 보호
- IPv6 브리징
- IPv6 게스트 인증(컨트롤러 호스팅)

다음 IPv6 관련 기능은 FlexConnect 로컬 스위칭 모드에서 지원되지 않습니다.

- 레이어 3 모빌리티
- IPv6 비디오 스트림
- IPv6 액세스 제어 목록
- IPv6 소스 가드
- DHCPv6 서버 가드
- 네이버 검색 캐싱
- 라우터 광고 제한

FlexConnect - 중앙 스위칭 WLAN

중앙 스위칭(컨트롤러로 트래픽을 다시 터널링)을 사용하는 FlexConnect 모드의 AP의 경우 컨트롤러는 "AP 멀티캐스트 모드"에 대해 "멀티캐스트 - 유니캐스트 모드"로 설정되어야 합니다. FlexConnect AP는 컨트롤러의 CAPWAP 멀티캐스트 그룹에 가입하지 않으므로 멀티캐스트 패킷은 컨트롤러에 복제하고 각 AP에 개별적으로 유니캐스트해야 합니다. 이 방법은 "Multicast - Multicast Mode(멀티캐스트 - 멀티캐스트 모드)"보다 효율적이지 않으며 컨트롤러에 추가 부하를 줍니다.

이 IPv6 관련 기능은 FlexConnect 중앙 스위칭 모드에서 지원되지 않습니다.

- IPv6 비디오 스트림

참고: Flex 7500 Series Controller에서는 IPv6를 실행하는 중앙 집중식 WLAN이 지원되지 않습니다
.

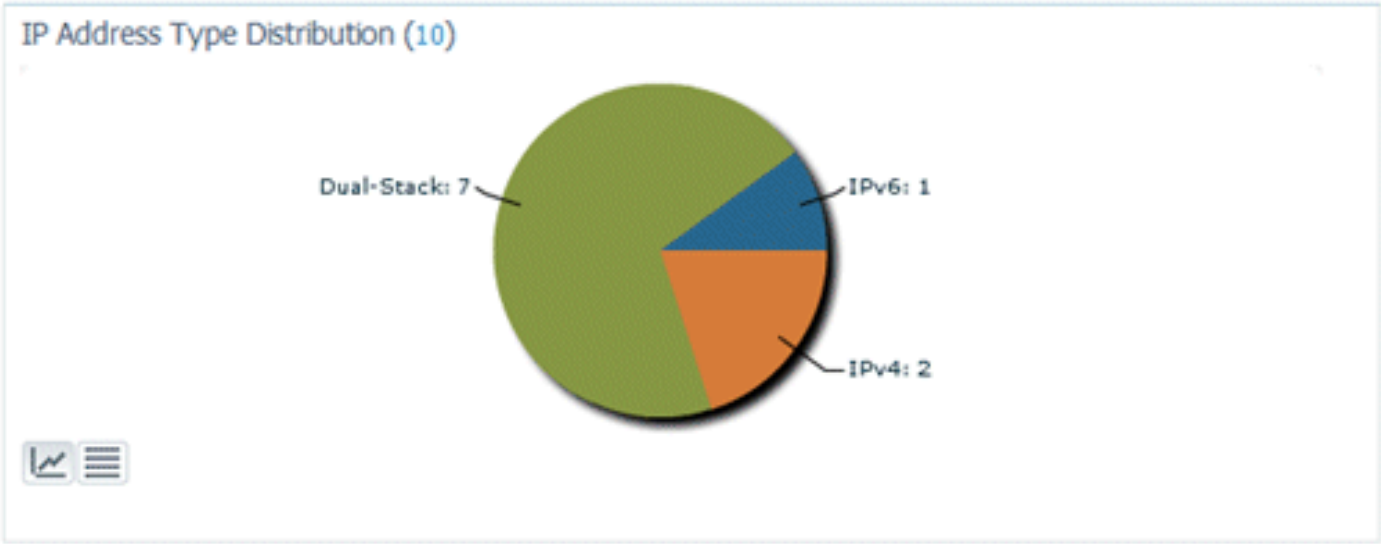
NCS를 통한 IPv6 클라이언트 가시성

NCS v1.1 릴리스에서는 유선 및 무선 네트워크 모두에서 IPv6 클라이언트 네트워크를 모니터링하고 관리하기 위해 다양한 IPv6 관련 기능이 추가되었습니다.

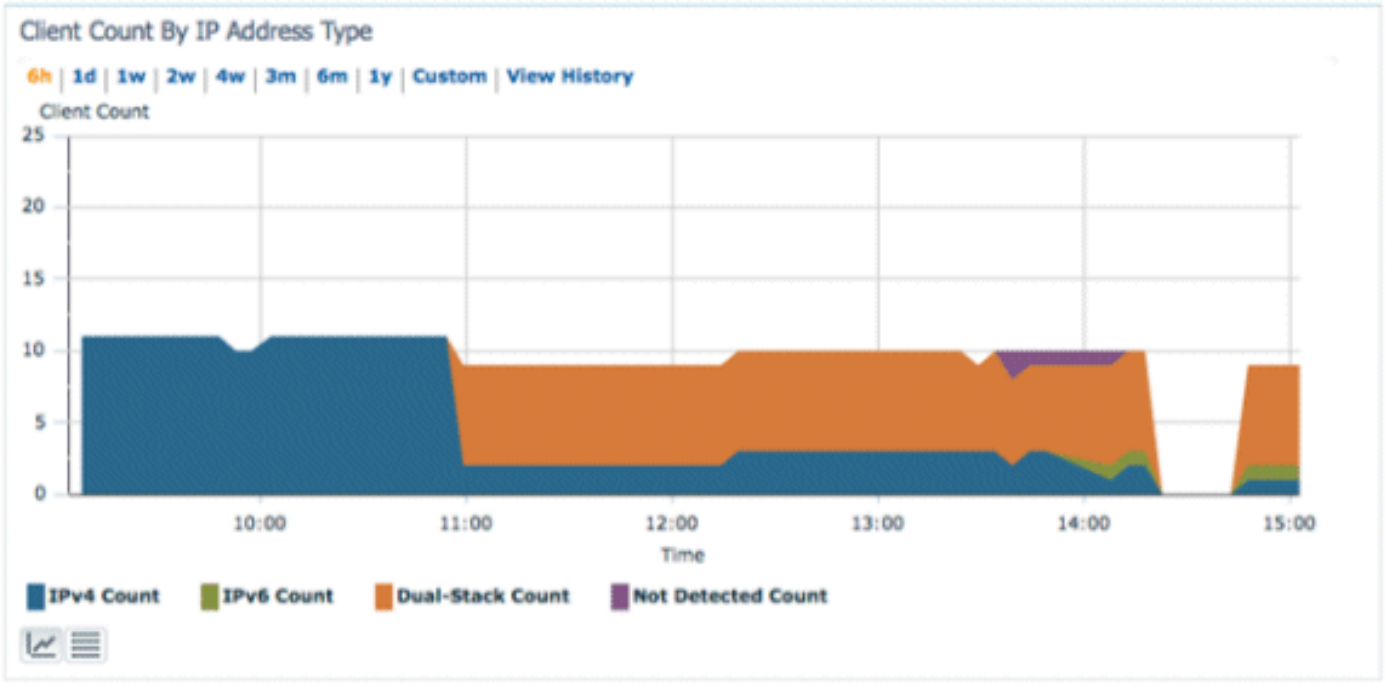
IPv6 대시보드 항목

네트워크에 어떤 유형의 클라이언트가 있는지 보기 위해 IPv6 관련 통계에 대한 통찰력을 제공하고 IPv6 클라이언트로 드릴다운할 수 있는 기능을 제공하기 위해 NCS의 "Dashlet"을 사용할 수 있습니다.

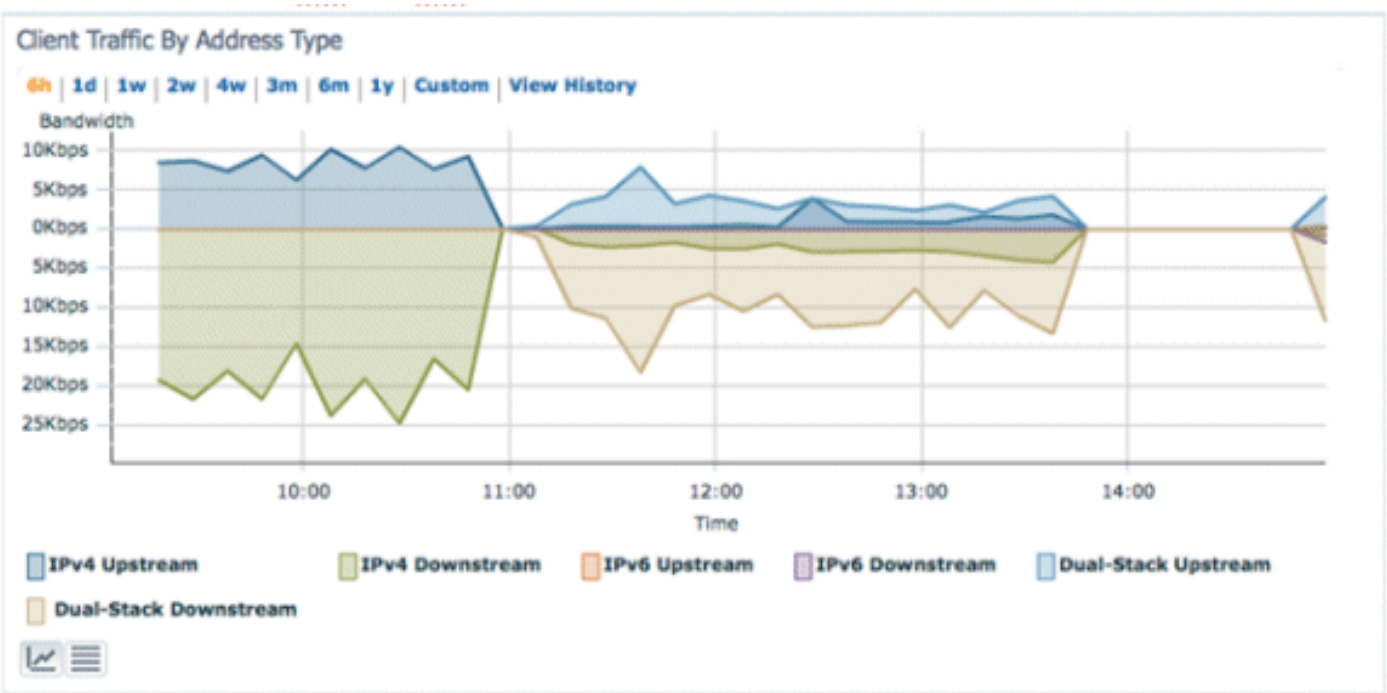
IP Address Type Dashlet - 네트워크에 있는 IP 클라이언트의 유형을 표시합니다.



Client Count by IP Address Type(IP 주소 유형별 클라이언트 수) - 시간에 따른 IP 클라이언트 유형을 표시합니다.



Client Traffic by IP Address Type(IP 주소 유형별 클라이언트 트래픽) - 각 클라이언트 유형의 트래픽을 표시합니다. 듀얼 스택 카테고리의 클라이언트에는 IPv4 및 IPv6 트래픽이 모두 포함됩니다.



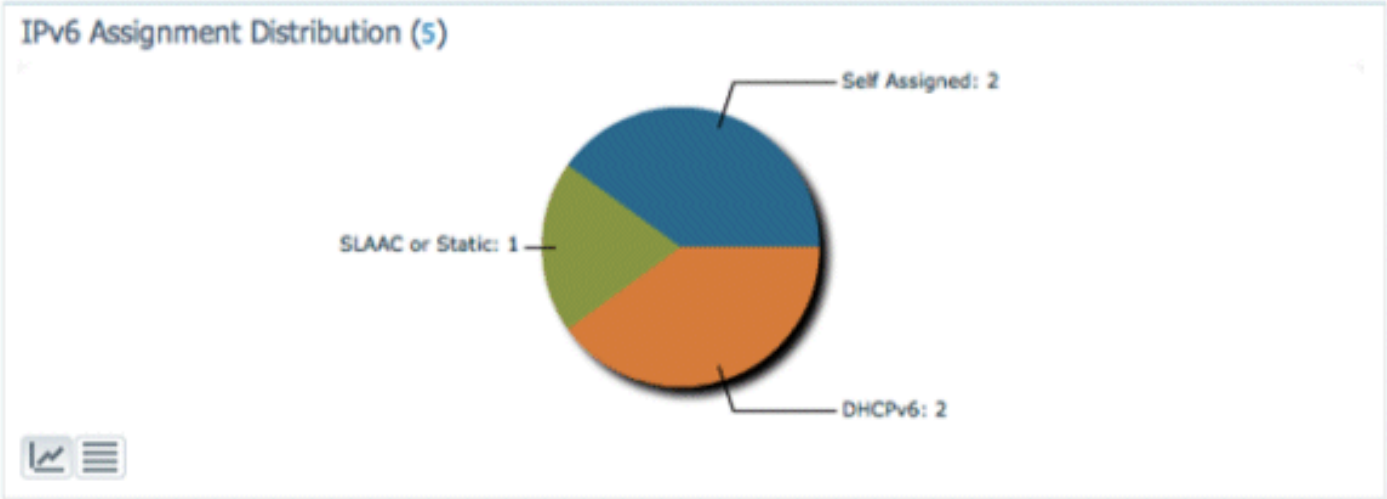
IPv6 Address Assignment(IPv6 주소 할당) - 각 클라이언트에 대한 주소 할당 방법을 다음 네 가지 범주 중 하나로 표시합니다.

- DHCPv6 - 중앙 서버에서 주소를 할당한 클라이언트입니다. 클라이언트는 SLAC 주소도 가질 수 있습니다.
- SLAAC 또는 Static - 상태 비저장 주소 자동 할당을 사용하거나 정적으로 구성된 주소를 사용하는 클라이언트에 해당합니다.
- Unknown(알 수 없음) - 경우에 따라 IPv6 주소 할당을 검색할 수 없습니다.

    - 이 조건은 일부 스위치가 IPv6 주소 할당 정보를 스누핑하지 않기 때문에 NCS의 유선 클라이언트에서만 발생합니다.

- Self-Assigned(자체 할당) - 링크-로컬 주소만 있고 전체가 자체 할당된 클라이언트입니다.
    - 이 범주의 클라이언트에는 Global Unique 또는 Local Unique 주소가 없기 때문에 IPv6 연결 문제가 발생할 수 있습니다.

파이 차트의 각 섹션은 클릭 가능하며, 이를 통해 관리자는 클라이언트 목록으로 드릴다운할 수 있습니다.



IPv6 클라이언트 모니터링

IPv6 클라이언트 정보를 모니터링하고 관리하기 위해 Clients and Users(클라이언트 및 사용자) 페이지에 다음 열이 추가되었습니다.

- IP Type(IP 유형) - 클라이언트에서 확인된 IP 주소를 기반으로 하는 클라이언트의 유형입니다. 가능한 옵션은 IPv4, IPv6 또는 Dual-Stack이며, 이는 IPv4 및 IPv6 주소가 모두 있는 클라이언트를 의미합니다.

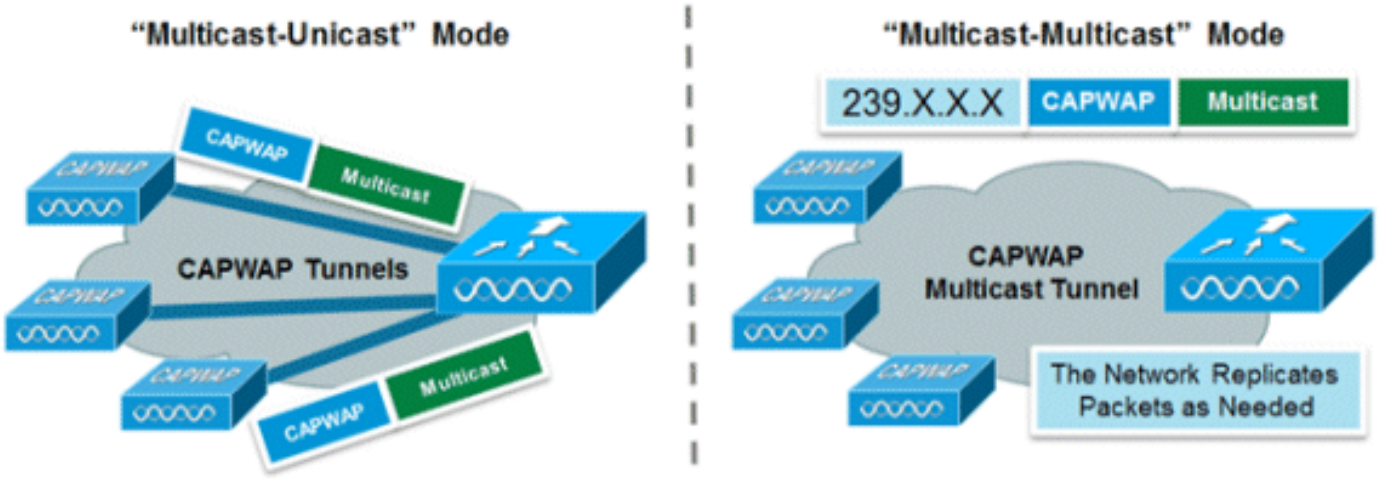
- IPv6 Assignment Type(IPv6 할당 유형) - NCS에서 주소 할당 방법이 SLAAC 또는 Static(정적), DHCPv6, Self-Assigned(셀프 할당) 또는 Unknown(알 수 없음)으로 탐지됩니다.
- Global Unique - 클라이언트에서 가장 최근에 사용한 IPv6 전역 주소입니다. 열 내용을 마우스 오버하면 클라이언트에서 사용하는 추가 IPv6 전역 고유 주소가 표시됩니다.
- Local Unique(로컬 고유) - 클라이언트에서 가장 최근에 사용한 IPv6 로컬 고유 주소입니다. 열 내용 위에 마우스를 놓으면 클라이언트에서 사용하는 추가 IPv6 전역 고유 주소가 표시됩니다.
- Link Local(링크 로컬) - 자체 할당되고 다른 IPv6 주소가 할당되기 전에 통신에 사용되는 클라이언트의 IPv6 주소입니다.
- Router Advertisements Dropped - 클라이언트에서 전송했으며 AP에서 삭제된 라우터 광고 수입니다. 이 열은 잘못 구성되었거나 악의적으로 구성되어 IPv6 라우터처럼 작동하는 클라이언트를 추적하는 데 사용할 수 있습니다. 이 열은 정렬 가능하므로 문제가 되는 클라이언트를 쉽게 식별할 수 있습니다.

IPv6 관련 열을 표시할 뿐만 아니라 IP Address 열에는 IPv4 주소(듀얼 스택 클라이언트의 경우)를 먼저 표시하는 우선 순위와 함께 클라이언트의 현재 IP 주소가 표시되거나 IPv6 전용 클라이언트의 경우 IPv6 전역 고유 주소가 표시됩니다.

무선 IPv6 클라이언트 지원을 위한 구성

AP에 대한 멀티캐스트 배포 모드

Cisco Unified Wireless Network는 컨트롤러와 연결된 AP에 멀티캐스트 배포하는 두 가지 방법을 지원합니다. 두 모드 모두에서 유선 네트워크의 원래 멀티캐스트 패킷은 CAPWAP 유니캐스트 또는 멀티캐스트를 통해 AP로 전송되는 레이어 3 CAPWAP 패킷 내에 캡슐화됩니다. 트래픽은 CAPWAP로 캡슐화되므로 AP가 클라이언트 트래픽과 동일한 VLAN에 있을 필요는 없습니다. 멀티캐스트 배포의 두 가지 방법은 여기에서 비교됩니다.



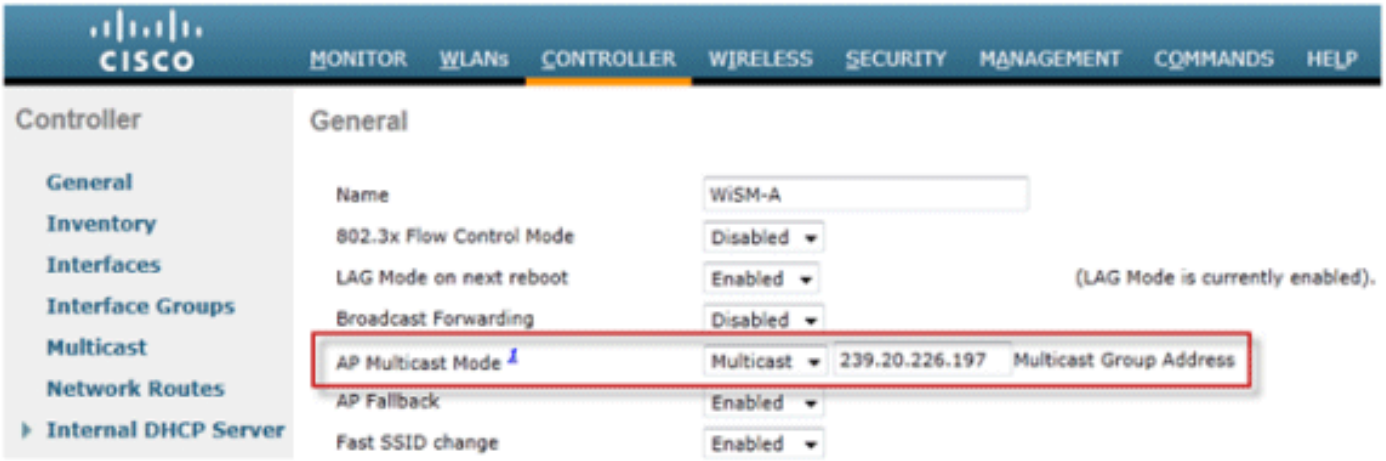
	멀티캐스트 유니캐스트 모드	멀티캐스트-멀티캐스트 모드
전달 메커니즘	컨트롤러는 멀티캐스트 패킷을 복제하여 유니캐스트 CAPWAP 터널의 각 AP에 전송합니다	컨트롤러는 멀티캐스트 패킷의 복사본 하나를 전송합니다
지원되는 AP 모드	FlexConnect 및 로컬	로컬 모드만
유선 네트워크에서 L3 멀티캐스트 라우팅 필요	아니요	예
컨트롤러 로딩	높음	낮음
유선 네트워크 로드	높음	낮음

멀티캐스트-멀티캐스트 배포 모드 구성

멀티캐스트-멀티캐스트 모드는 확장성 및 유선 대역폭 효율성을 위해 권장되는 옵션입니다.

참고: 이 단계는 2500 Series Wireless Controller에만 절대적으로 필요하지만, 멀티캐스트 전송을 보다 효율적으로 수행할 수 있도록 지원하며 모든 컨트롤러 플랫폼에 권장됩니다.

"General(일반)" 페이지의 "Controller(컨트롤러)" 탭으로 이동하여 AP Multicast Mode(AP 멀티캐스트 모드)가 Multicast mode(멀티캐스트 모드)를 사용하도록 구성되어 있고 유효한 그룹 주소가 구성되어 있는지 확인합니다. 그룹 주소는 IPv4 멀티캐스트 그룹이며 프라이빗 멀티캐스트 애플리케이션의 범위인 239.X.X.X-239.255.255.255 범위에 있는 것이 좋습니다.

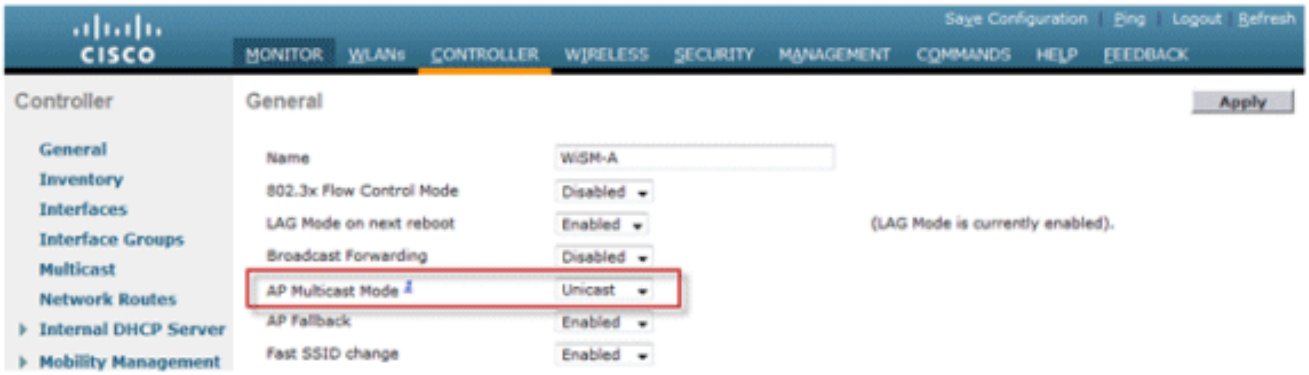


참고: 멀티캐스트 그룹 주소에는 224.X.X.X, 239.0.0.X 또는 239.128.0.X 주소 범위를 사용하지 마십시오. 이러한 범위의 주소는 링크 로컬 MAC 주소와 중첩되며, IGMP 스누핑이 활성화된 경우에도 모든 스위치 포트를 플러딩합니다.

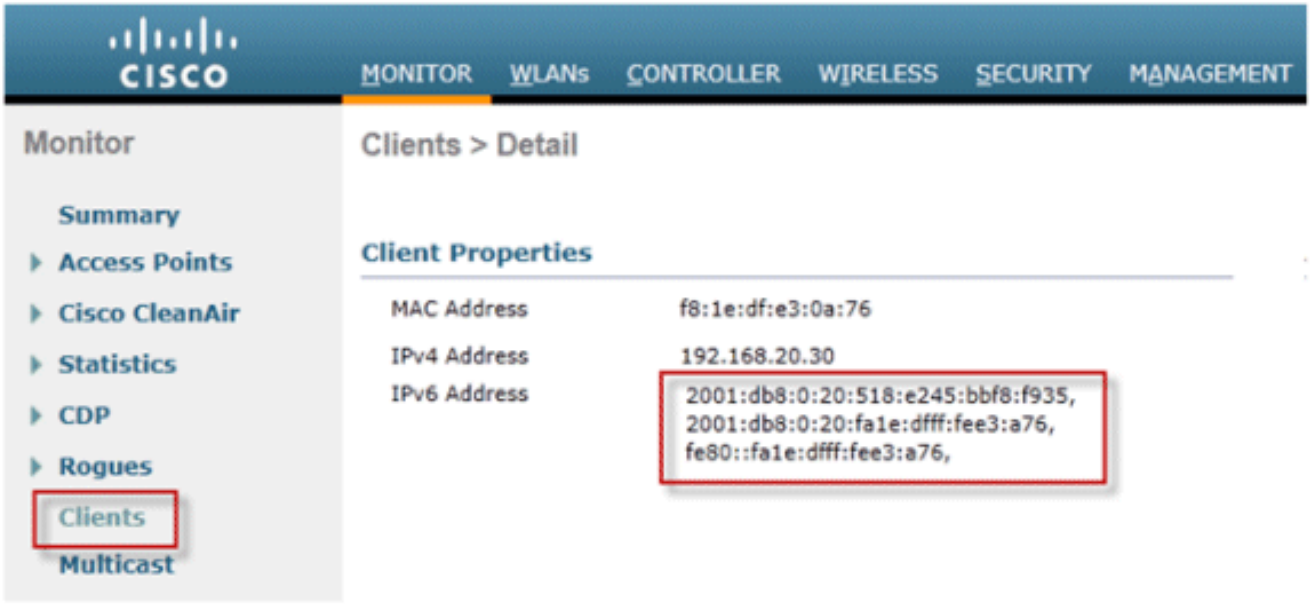
멀티캐스트 유니캐스트 배포 모드 구성

컨트롤러와 AP 또는 FlexConnect 모드 간에 CAPWAP 멀티캐스트를 전달하도록 유선 네트워크가 올바르게 구성되지 않은 경우, AP가 IPv6를 지원하는 중앙 집중식 스위치드 WLAN에 사용될 경우 유니캐스트 모드가 필요합니다.

1. General(일반) 페이지의 Controller(컨트롤러) 탭으로 이동하여 AP Multicast Mode(AP 멀티캐스트 모드)가 유니캐스트 모드를 사용하도록 구성되어 있는지 확인합니다.



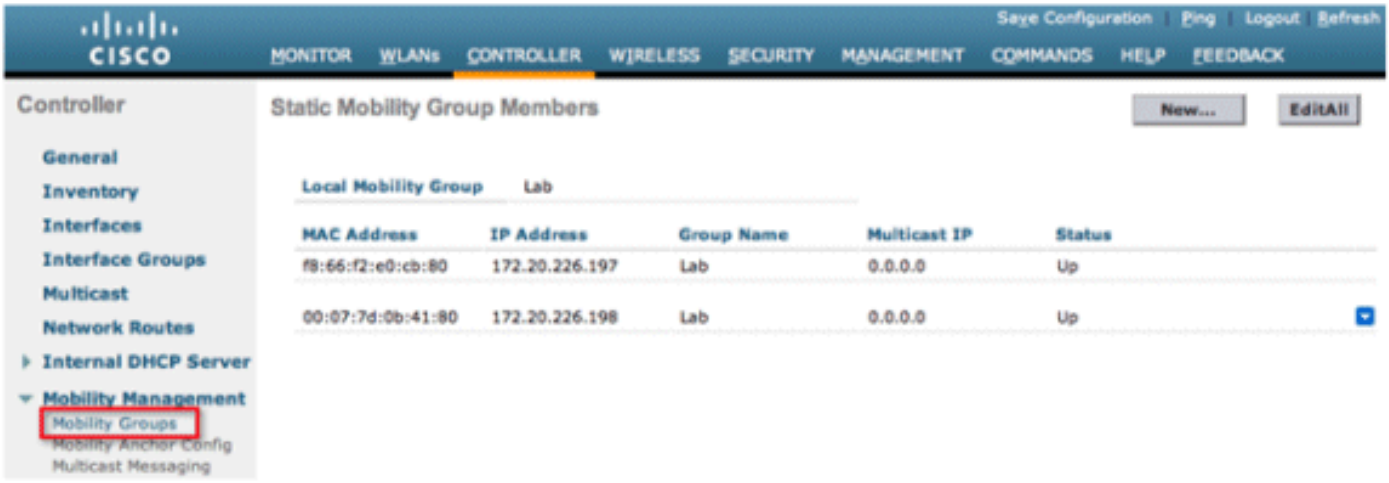
2. IPv6 지원 클라이언트를 무선 LAN에 연결합니다. Monitor 탭 및 Clients 메뉴로 이동하여 클라이언트가 IPv6 주소를 수신하는지 확인합니다.



IPv6 모빌리티 구성

컨트롤러를 동일한 모빌리티 그룹 또는 동일한 모빌리티 도메인 내에 배치하는 것 외에는 IPv6 모빌리티에 대한 특정 컨피그레이션이 없습니다. 이를 통해 최대 72개의 컨트롤러가 모빌리티 도메인에 참여하여 최대 규모의 캠퍼스에서도 원활한 모빌리티를 제공할 수 있습니다.

Controller(컨트롤러) 탭 > Mobility Groups(모빌리티 그룹)로 이동하여 MAC 주소와 IP 주소로 각 컨트롤러를 그룹에 추가합니다. 모빌리티 그룹의 모든 컨트롤러에서 이 작업을 수행해야 합니다.



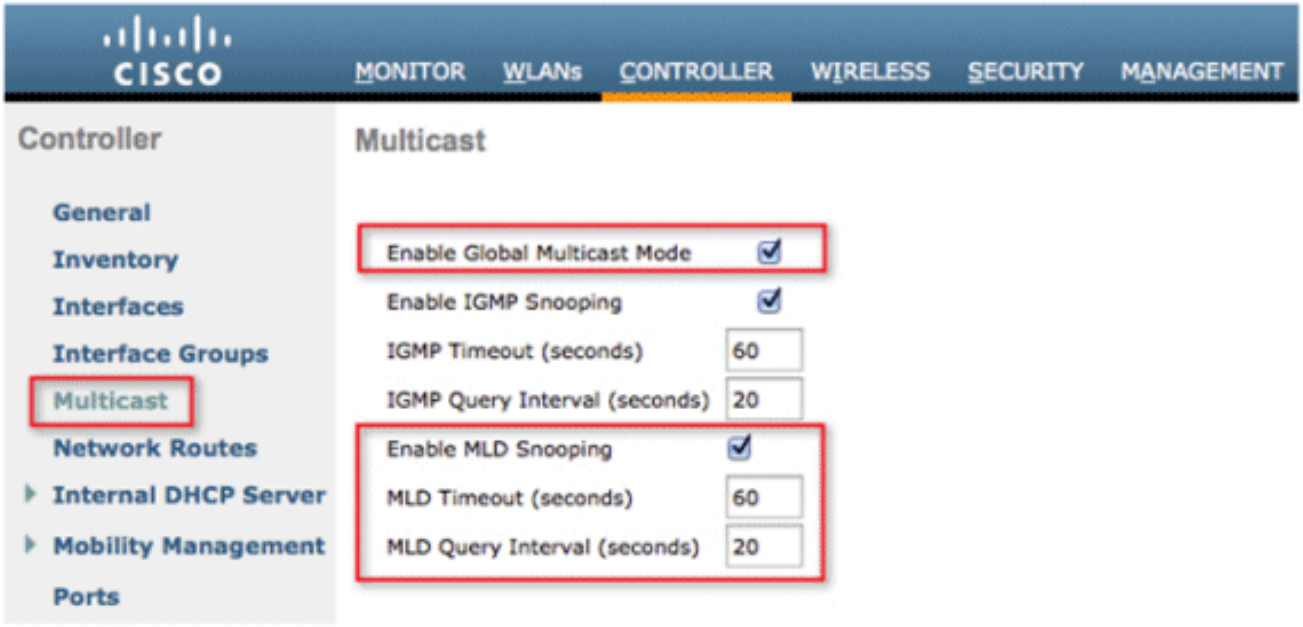
IPv6 멀티캐스트 구성

컨트롤러는 IPv6 멀티캐스트를 위한 MLDv1 스누핑을 지원하므로 지능적으로 멀티캐스트 흐름을 추적하고 이를 요청하는 클라이언트에 전달할 수 있습니다.

참고: 이전 버전의 릴리스와 달리 IPv6 유니캐스트 트래픽 지원에서는 컨트롤러에서 "Global Multicast Mode"를 사용하도록 설정하지 않아도 됩니다. IPv6 유니캐스트 트래픽 지원이 자동으로 활성화됩니다.

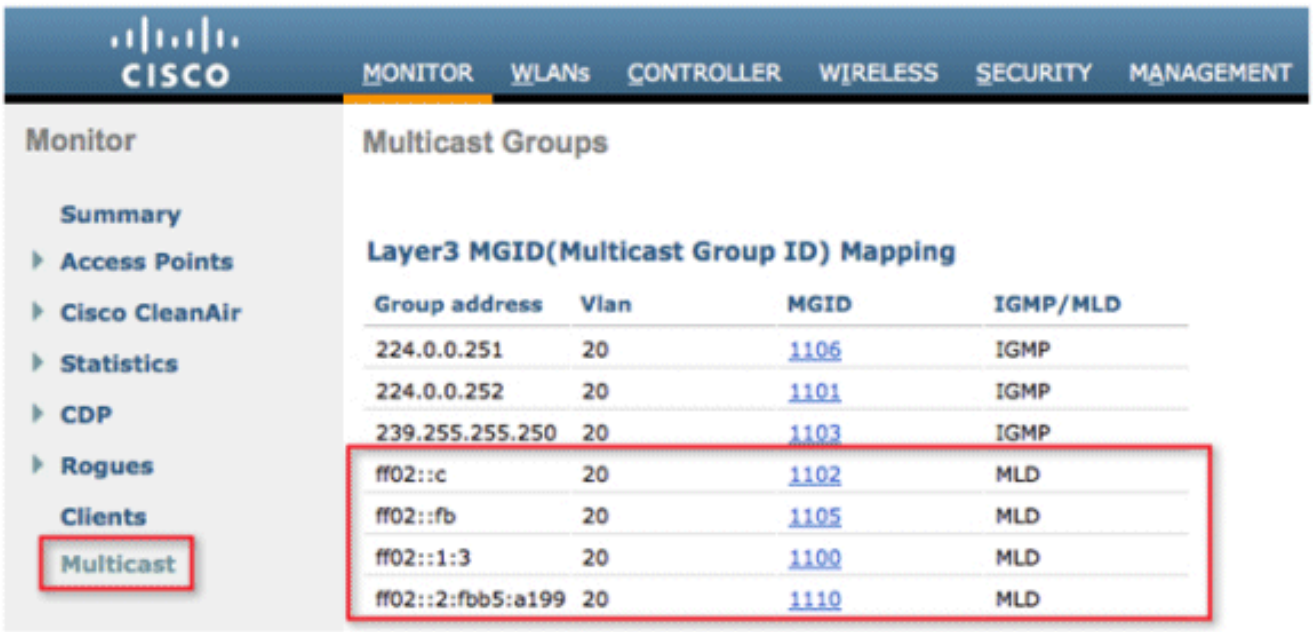
1. 멀티캐스트 IPv6 트래픽을 지원하려면 Controller(컨트롤러) 탭 > Multicast(멀티캐스트) 페이

지로 이동하여 Enable MLD Snooping(MLD 스누핑 활성화)을 클릭합니다. IPv6 멀티캐스트를 활성화하려면 컨트롤러의 전역 멀티캐스트 모드도 활성화해야 합니다.



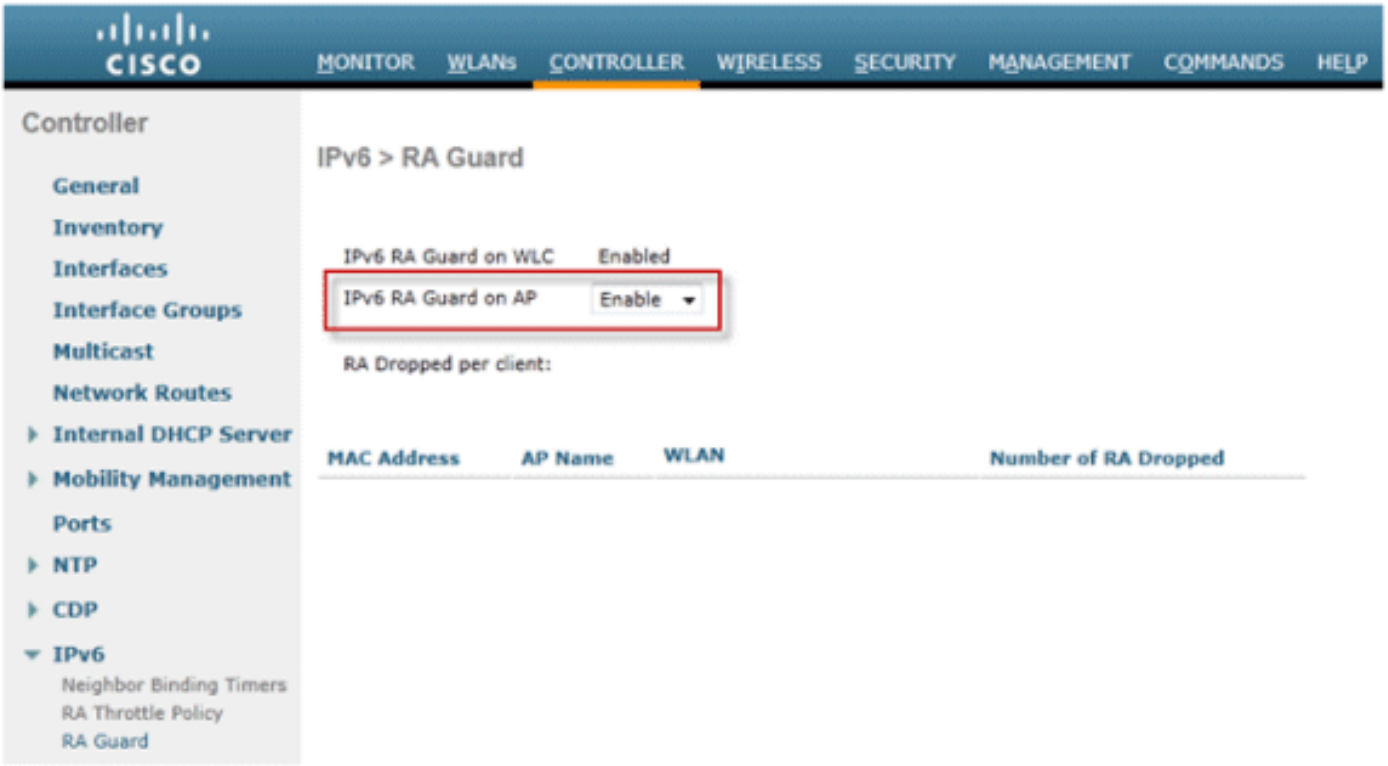
참고: Apple의 Bonjour와 같은 피어 투 피어 검색 애플리케이션이 필요한 경우 Global Multicast Mode, IGMP 및 MLD 스누핑을 활성화해야 합니다.

2. IPv6 멀티캐스트 트래픽이 스누핑되고 있는지 확인하려면 Monitor(모니터) 탭과 Multicast(멀티캐스트) 페이지로 이동합니다. IPv4(IGMP) 및 IPv6(MLD) 멀티캐스트 그룹이 모두 나열됩니다. 해당 그룹 주소에 가입된 무선 클라이언트를 보려면 MGID를 클릭합니다.



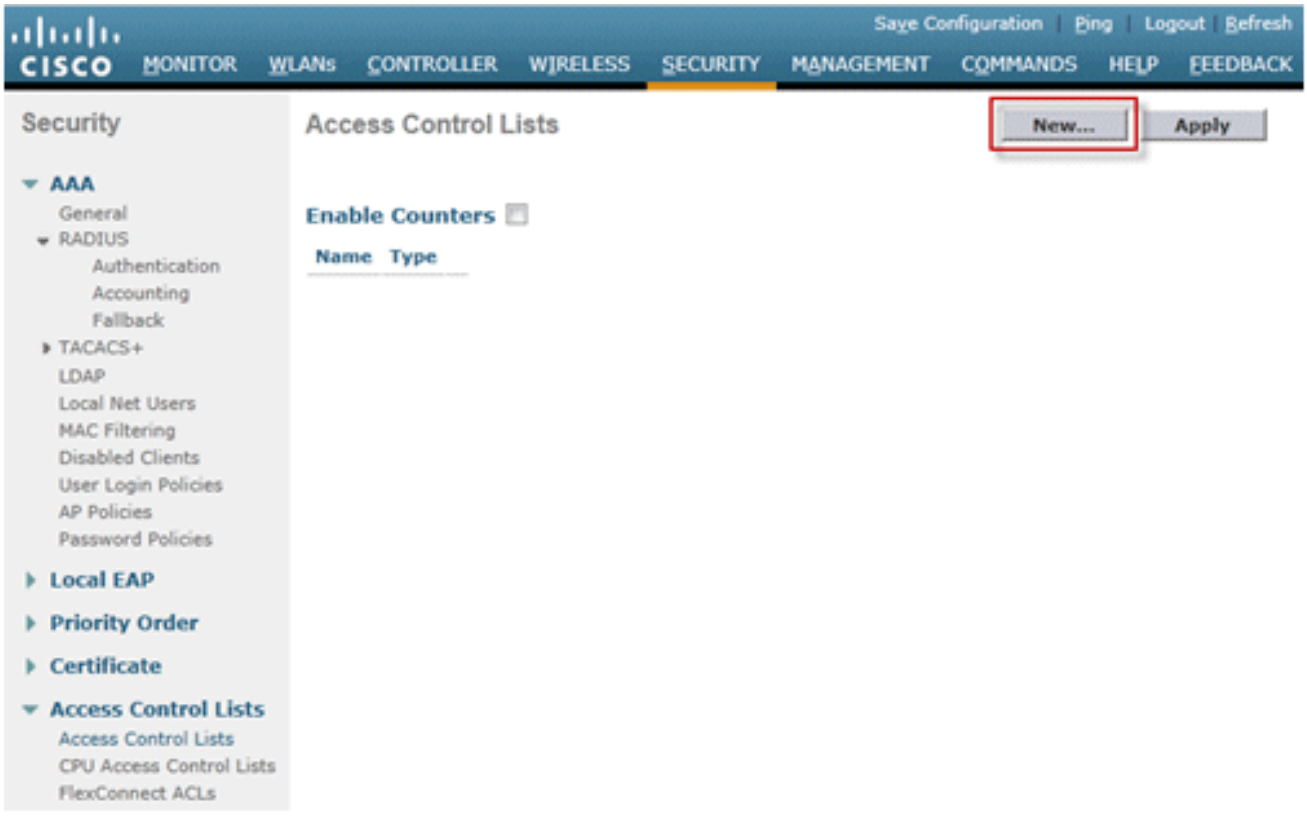
IPv6 RA Guard 구성

Controller(컨트롤러) 탭으로 이동한 다음 왼쪽 메뉴에서 IPv6 > RA Guard로 이동합니다. AP에서 IPv6 RA Guard를 활성화합니다. 컨트롤러의 RA Guard를 비활성화할 수 없습니다. RA Guard 컨피그레이션 외에도 이 페이지에는 RA를 전송하는 것으로 식별된 모든 클라이언트도 표시됩니다.



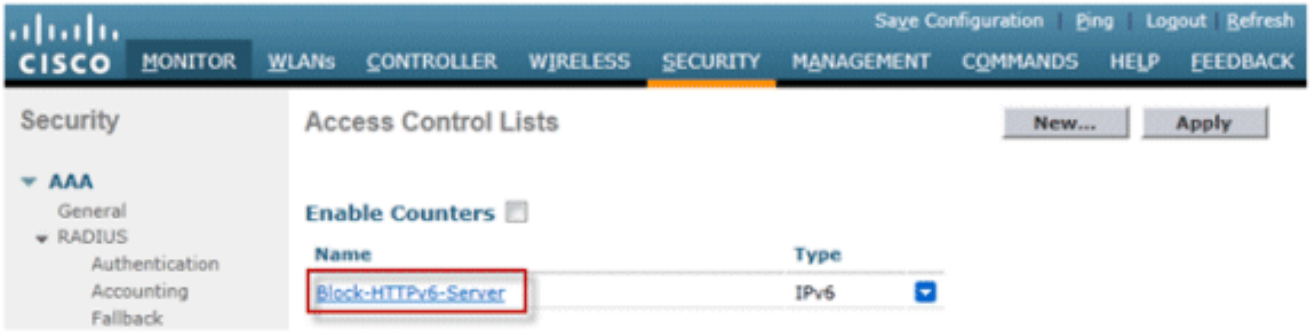
IPv6 액세스 제어 목록 구성

1. 보안 탭으로 이동하여 Access Control Lists(액세스 제어 목록)를 열고 New(새로 만들기)를 클릭합니다.

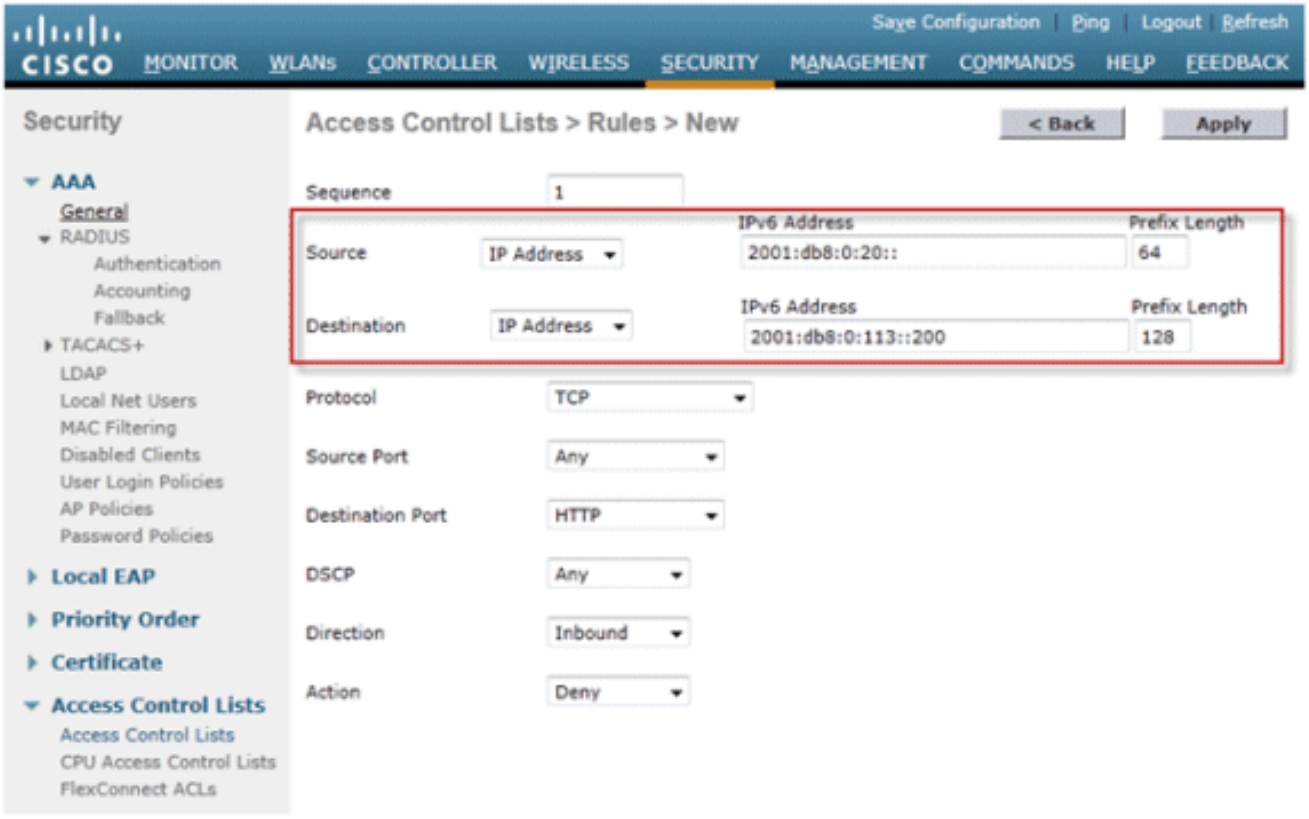


2. ACL의 고유한 이름을 입력하고 ACL Type(ACL 유형)을 IPv6로 변경한 다음 Apply(적용)를 클릭합니다.

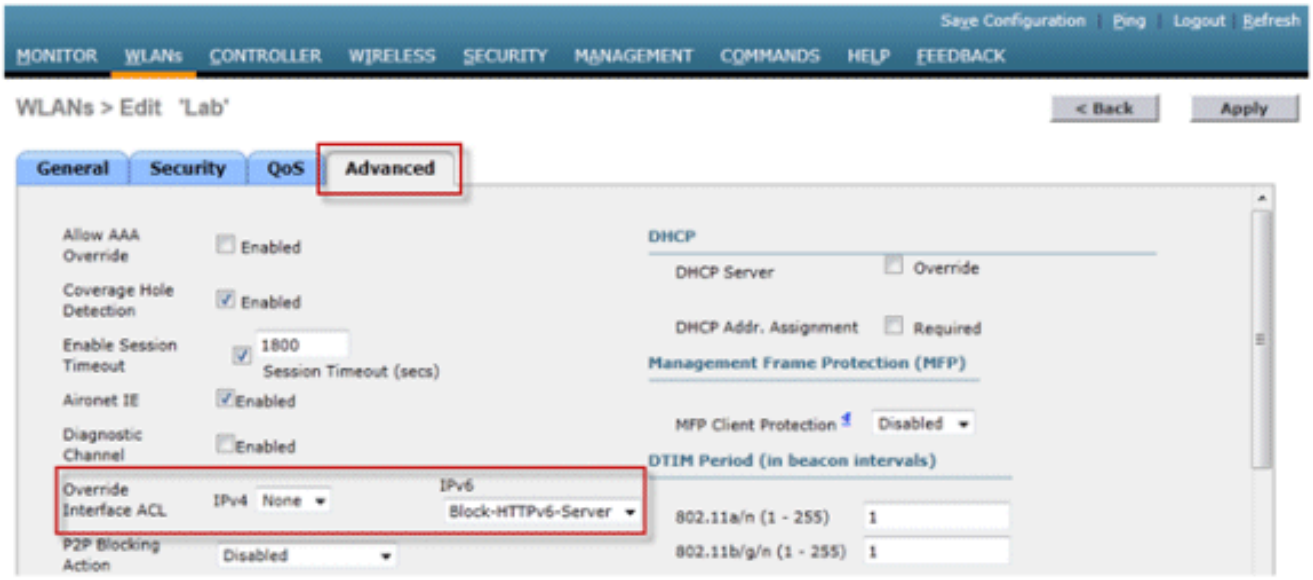
3. 위 단계에서 생성한 새 ACL을 클릭합니다.



4. Add New Rule(새 규칙 추가)을 클릭하고 규칙에 대해 원하는 매개변수를 입력한 다음 Apply(적용)를 클릭합니다. 목록 끝에 규칙을 배치하려면 시퀀스 번호를 비워 둡니다. "Inbound(인바운드)"의 "Direction(방향)" 옵션은 무선 네트워크에서 들어오는 트래픽에 사용되고, "Outbound(아웃바운드)"는 무선 클라이언트로 향하는 트래픽에 사용됩니다. ACL의 마지막 규칙은 암시적 모두 거부입니다. 전체 IPv6 서브넷을 매칭하려면 접두사 길이 64를 사용하고, 개별 주소에 대한 액세스를 고유하게 제한하려면 접두사 길이 128을 사용합니다.

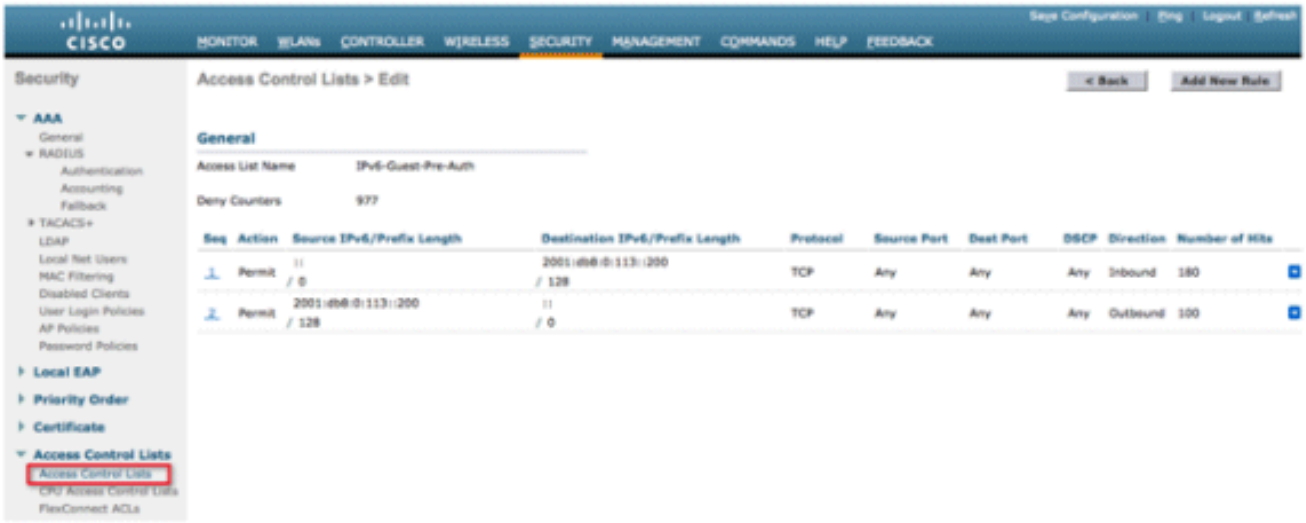


5. IPv6 ACL은 WLAN/SSID별로 적용되며 여러 WLAN에서 동시에 사용할 수 있습니다. WLANs(WLAN) 탭으로 이동하여 IPv6 ACL을 적용하려면 해당 SSID의 WLAN ID를 클릭합니다. Advanced(고급) 탭을 클릭하고 IPv6에 대한 Override Interface ACL(인터페이스 ACL 재정의 ACL)을 ACL 이름으로 변경합니다.



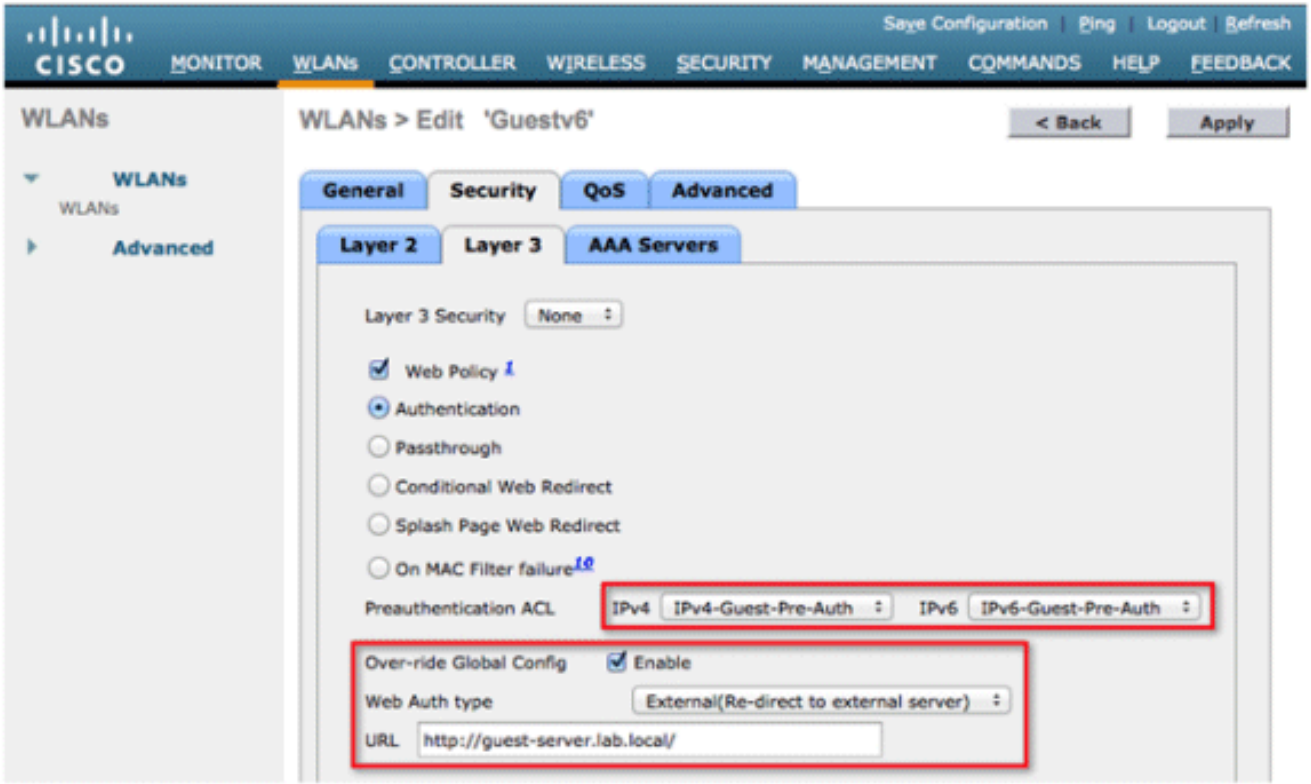
외부 웹 인증을 위한 IPv6 게스트 액세스 구성

1. 웹 서버에 대한 IPv4 및 IPv6 사전 인증 ACL을 구성합니다. 이렇게 하면 클라이언트가 완전히 인증되기 전에 외부 서버에서 트래픽을 주고받을 수 있습니다.



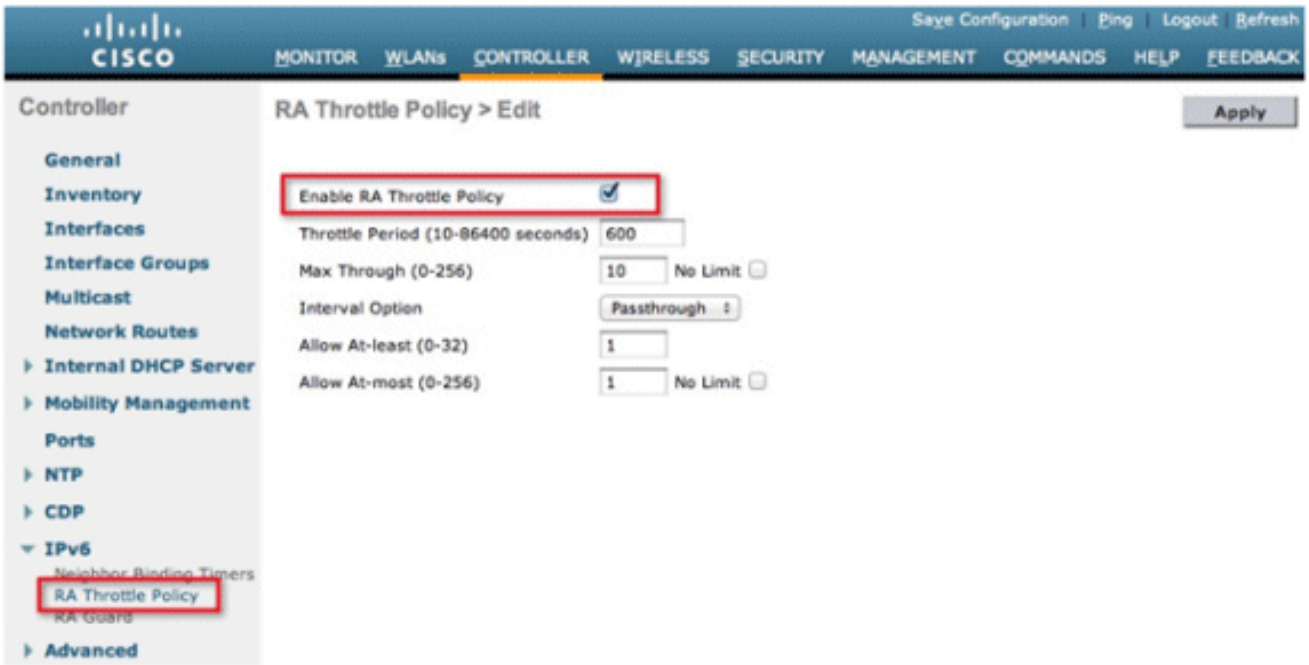
외부 웹 액세스 작동에 대한 자세한 내용은 [무선 LAN 컨트롤러를 사용한 외부 웹 인증 컨피그레이션 예를 참조하십시오](#).

2. 상단의 WLANs(WLAN) 탭으로 이동하여 게스트 WLAN을 구성합니다. 게스트 SSID를 생성하고 Layer 3 웹 정책을 사용합니다. 1단계에서 정의한 사전 인증 ACL은 IPv4 및 IPv6에 대해 선택됩니다. Over-ride Global Config 섹션을 선택하고 Web Auth type 드롭다운 상자에서 External을 선택합니다. 웹 서버의 URL을 입력합니다. 외부 서버의 호스트 이름은 IPv4 및 IPv6 DNS에서 확인할 수 있어야 합니다.



IPv6 RA 제한 구성

1. Controller(컨트롤러) 최상위 메뉴로 이동하고 왼쪽에서 IPv6 > RA Throttle Policy(RA 스로틀 정책) 옵션을 클릭합니다. 확인란을 클릭하여 RA Throttling을 활성화합니다.



참고: RA 제한이 발생하면 첫 번째 IPv6 지원 라우터만 통과가 허용됩니다. 여러 IPv6 접두사가 서로 다른 라우터에서 제공되는 네트워크의 경우 RA 제한을 비활성화해야 합니다.

2. 스로틀 기간 및 기타 옵션은 TAC의 권고에 따라 조정해야 합니다. 그러나 대부분의 구축에는 기본값이 권장됩니다. RA 제한 정책의 다양한 컨피그레이션 옵션은 다음 사항을 염두에 두고

조정해야 합니다.

- "Allow At-least(최소 허용)"의 숫자 값은 "Allow At-most(최대 허용)"보다 작아야 하며 "Max Through(최대 통과)"보다 작아야 합니다.
- RA 제한 정책은 대부분의 RA의 기본 수명이므로 1800초를 초과하는 제한 기간을 사용해서는 안 됩니다.

각 RA Throttling 옵션에 대한 설명은 다음과 같습니다.

- Throttle Period(조절 기간) - 조절이 발생하는 기간입니다. RA 제한은 VLAN에 대한 "최대 통과(Max Through)" 제한에 도달한 후에만 적용됩니다.
- Max Through(최대 통과) - 스로틀링이 시작되기 전 VLAN당 최대 RA 수입니다. "No Limit" 옵션은 제한 없이 무제한의 RA를 통과하도록 허용합니다.
- Interval Option(간격 옵션) - 간격 옵션을 사용하면 컨트롤러가 IPv6 RA에 설정된 RFC 3775 값에 따라 다르게 작동할 수 있습니다.
  - Passthrough - 이 값을 사용하면 RFC3775 간격 옵션이 있는 모든 RA가 제한 없이 통과할 수 있습니다.
  - Ignore(무시) - 이 값을 사용하면 RA 스로틀러가 interval(간격) 옵션이 포함된 패킷을 일반 RA로 취급하며, 유효한 경우 스로틀링에 종속됩니다.
  - Throttle - 이 값을 사용하면 interval 옵션을 사용하는 RA가 항상 속도 제한을 받게 됩니다.
- Allow At-least - 멀티캐스트로 전송할 라우터당 최소 RA 수입니다.
- Allow At-most - 제한이 적용되기 전에 멀티캐스트로 전송될 라우터당 최대 RA 수입니다. "No Limit(제한 없음)" 옵션을 사용하면 해당 라우터에 대해 RA를 무제한으로 통과시킬 수 있습니다.

IPv6 인접 디바이스 바인딩 테이블 구성

1. Controller(컨트롤러) 최상위 메뉴로 이동하고 왼쪽 메뉴에서 IPv6 > Neighbor Binding Timers를 클릭합니다.

2. 필요에 따라 다운 수명, 도달 가능 수명 및 부실 수명을 조정합니다. 고도로 모바일화된 클라이언트가 있는 구축의 경우 오래된 주소 타이머의 타이머를 조정해야 합니다. 권장되는 값은 다음과 같습니다.

   - 다운 수명 - 30초
   - 연결 가능 수명 - 300초
   - 상태 수명 - 86400초

   각 수명 타이머는 IPv6 주소가 다음 상태에 있을 수 있는 상태를 나타냅니다.

   - Down Lifetime - 다운 타이머는 컨트롤러의 업링크 인터페이스가 다운될 경우 IPv6 캐시 엔트리를 유지할 기간을 지정합니다.
   - Reachable Lifetime - 이 타이머는 IPv6 주소가 활성으로 표시되는 기간을 지정하며, 이

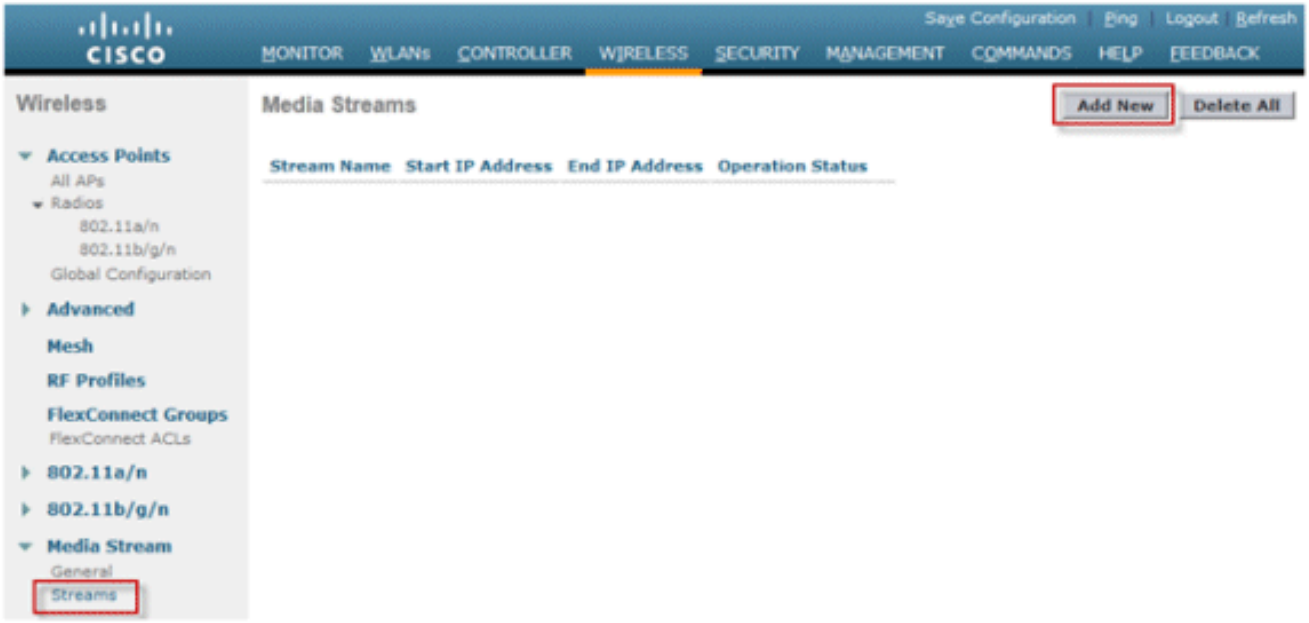
는 최근에 이 주소에서 트래픽이 수신되었음을 의미합니다. 이 타이머가 만료되면 주소가 "Stale(부실)" 상태로 이동합니다.

- Stale Lifetime - 이 타이머는 "Reachable Lifetime" 내에 표시되지 않은 IPv6 주소를 캐시에 유지할 기간을 지정합니다. 이 수명이 지나면 바인딩 테이블에서 주소가 제거됩니다.

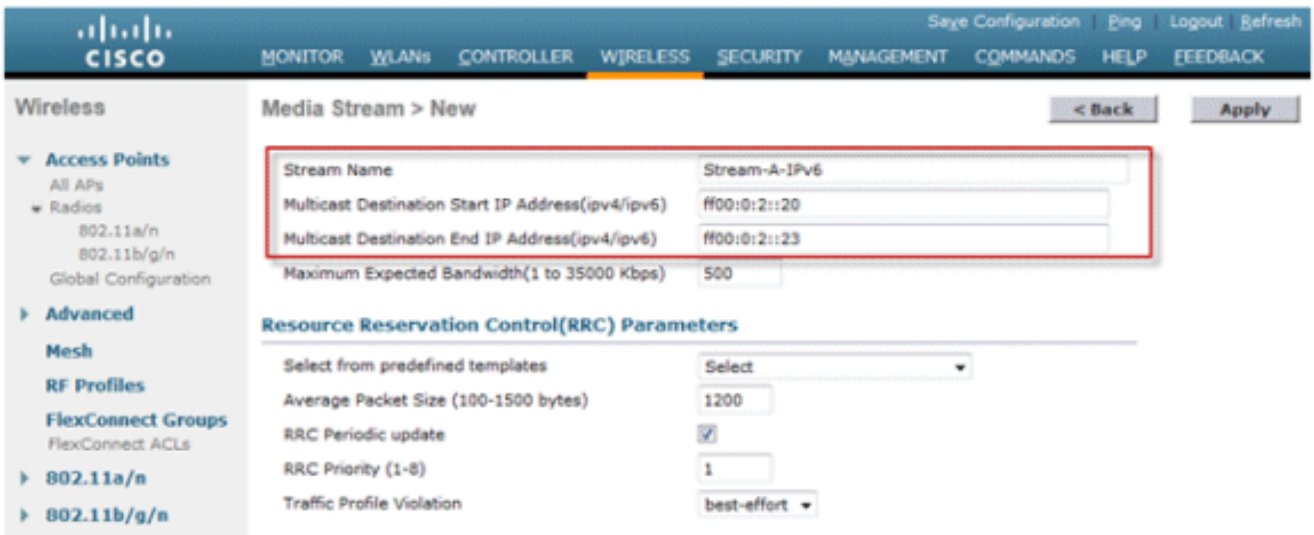
IPv6 VideoStream 구성

1. 컨트롤러에서 전역 VideoStream 기능이 활성화되어 있는지 확인합니다. 802.11a/g/n 네트워크 및 WLAN SSID에서 VideoStream을 활성화하는 방법에 대한 자세한 내용은 Cisco Unified Wireless Network Solution: VideoStream Deployment Guide를 참조하십시오.

2. 컨트롤러의 Wireless(무선) 탭으로 이동하고 왼쪽 메뉴에서 Media Stream(미디어 스트림) > Streams를 선택합니다. 새 스트림을 생성하려면 Add New(새로 추가)를 클릭합니다.



3. 스트림의 이름을 지정하고 시작 및 종료 IPv6 주소를 입력합니다. 단일 스트림만 사용하는 경우 시작 주소와 끝 주소가 같습니다. 주소를 추가한 후 Apply를 클릭하여 스트림을 생성합니다.



IPv6 클라이언트 연결 문제 해결

특정 클라이언트가 IPv6 트래픽을 전달할 수 없음

일부 클라이언트 IPv6 네트워킹 스택 구현은 네트워크에 들어올 때 자신을 제대로 알리지 않으므로 인접 디바이스 바인딩 테이블에 배치할 때 컨트롤러에 의해 주소가 제대로 스누핑되지 않습니다. 인접 디바이스 바인딩 테이블에 없는 주소는 IPv6 소스 가드 기능에 따라 차단됩니다. 이러한 클라이언트가 트래픽을 전달하도록 허용하려면 다음 옵션을 구성해야 합니다.

1. CLI를 통해 IPv6 Source Guard 기능을 비활성화합니다.

   <#root>

   config network ip-mac-binding disable

2. CLI를 통해 멀티캐스트 네이버 요청 전달을 활성화합니다.

   <#root>

   config ipv6 ns-mcast-fwd enable

IPv6 클라이언트에 대한 성공적인 레이어 3 로밍 확인:

앵커 및 외부 컨트롤러에서 다음 debug 명령을 실행합니다.

<#root>

debug client

<#root>

debug mobility handoff enable

<#root>

debug mobility packet enable

앵커 컨트롤러의 디버그 결과:

<#root>

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

00:21:6a:a7:4f:ee Set symmetric mobility tunnel for 00:21:6a:a7:4f:ee as in
  Anchor role

00:21:6a:a7:4f:ee 0.0.0.0 Added NPU entry of type 1, dtlFlags 0x1

00:21:6a:a7:4f:ee Pushing IPv6: fe80:0000:0000:0000: 3057:534d:587d:73ae , and
  MAC: 00:21:6A:A7:4F:EE , Binding to Data Plane. SUCCESS !!
00:21:6a:a7:4f:ee Pushing IPv6: 2001:0db8:0000:0020: 3057:534d:587d:73ae , and
  MAC: 00:21:6A:A7:4F:EE , Binding to Data Plane. SUCCESS !!

00:21:6a:a7:4f:ee 0.0.0.0, VLAN Id 20 Not sending gratuitous ARP
00:21:6a:a7:4f:ee Copy AP LOCP - mode:0 slotId:0, apMac 0x0:0:0:0:0:0
00:21:6a:a7:4f:ee Copy WLAN LOCP EssIndex:3 aid:0 ssid:    Roam
00:21:6a:a7:4f:ee Copy Security LOCP ecypher:0x0 ptype:0x2, p:0x0, eaptype:0x6
  w:0x1 aalg:0x0, PMState:        RUN
00:21:6a:a7:4f:ee Copy 802.11 LOCP a:0x0 b:0x0 c:0x0 d:0x0 e:0x0 protocol2:0x5
  statuscode 0, reasoncode 99, status 3
00:21:6a:a7:4f:ee Copy CCX LOCP 4
00:21:6a:a7:4f:ee Copy e2e LOCP 0x1
00:21:6a:a7:4f:ee Copy MobilityData LOCP status:2, anchorip:0xac14e2c6
00:21:6a:a7:4f:ee Copy IPv6 LOCP: fe80::3057:534d:587d:73ae
```

외부 컨트롤러의 디버그 결과:

<#root>

```
00:21:6a:a7:4f:ee Adding mobile on LWAPP AP f0:25:72:3c:0f:20(1)
00:21:6a:a7:4f:ee Reassociation received from mobile on AP f0:25:72:3c:0f:20
00:21:6a:a7:4f:ee 0.0.0.0 START (0) Changing IPv4 ACL 'none' (ACL ID 255) ===>
  'none' (ACL ID 255) --- (caller apf_policy.c:1697)
```

```
00:21:6a:a7:4f:ee 0.0.0.0 START (0) Changing IPv6 ACL 'none' (ACL ID 255) ===>
  'none' (ACL ID 255) --- (caller apf_policy.c:1864)
00:21:6a:a7:4f:ee Applying site-specific Local Bridging override for station
  00:21:6a:a7:4f:ee - vapId 3, site 'default-group', interface 'client-b1'
00:21:6a:a7:4f:ee Applying Local Bridging Interface Policy for station
  00:21:6a:a7:4f:ee - vlan 25, interface id 12, interface 'client-b1'
00:21:6a:a7:4f:ee processSsidIE  statusCode is 0 and status is 0
00:21:6a:a7:4f:ee processSsidIE  ssid_done_flag is 0 finish_flag is 0
00:21:6a:a7:4f:ee STA - rates (8): 140 18 152 36 176 72 96 108 0 0 0 0 0 0 0 0
*apfMsConnTask_4: Jan 22 20:37:45.370: 00:21:6a:a7:4f:ee suppRates  statusCode
  is 0 and gotSuppRatesElement is 1
00:21:6a:a7:4f:ee Processing RSN IE type 48, length 22 for mobile
  00:21:6a:a7:4f:ee
00:21:6a:a7:4f:ee 0.0.0.0 START (0) Initializing policy
00:21:6a:a7:4f:ee 0.0.0.0 START (0) Change state to AUTHCHECK (2) last state
  AUTHCHECK (2)
00:21:6a:a7:4f:ee 0.0.0.0 AUTHCHECK (2) Change state to 8021X_REQD (3) last
  state 8021X_REQD (3)
00:21:6a:a7:4f:ee 0.0.0.0 8021X_REQD (3) DHCP Not required on AP
  f0:25:72:3c:0f:20 vapId 3 apVapId 3for this client
00:21:6a:a7:4f:ee Not Using WMM Compliance code qosCap 00
00:21:6a:a7:4f:ee 0.0.0.0 8021X_REQD (3) Plumbed mobile LWAPP rule on AP
  f0:25:72:3c:0f:20 vapId 3 apVapId 3
00:21:6a:a7:4f:ee apfMsAssoStateInc
00:21:6a:a7:4f:ee apfPemAddUser2 (apf_policy.c:268) Changing state for mobile
  00:21:6a:a7:4f:ee on AP f0:25:72:3c:0f:20 from Idle to Associated
00:21:6a:a7:4f:ee Scheduling deletion of Mobile Station:  (callerId: 49) in 1800
  seconds
00:21:6a:a7:4f:ee Sending Assoc Response to station on BSSID f0:25:72:3c:0f:20
  (status 0) ApVapId 3 Slot 1
00:21:6a:a7:4f:ee apfProcessAssocReq (apf_80211.c:6290) Changing state for
  mobile 00:21:6a:a7:4f:ee on AP f0:25:72:3c:0f:20 from Associated to Associated
<…SNIP…>
00:21:6a:a7:4f:ee 0.0.0.0 8021X_REQD (3) Change state to L2AUTHCOMPLETE (4) last
  state L2AUTHCOMPLETE (4)
00:21:6a:a7:4f:ee 0.0.0.0 L2AUTHCOMPLETE (4) DHCP Not required on AP
  f0:25:72:3c:0f:20 vapId 3 apVapId 3for this client
00:21:6a:a7:4f:ee Not Using WMM Compliance code qosCap 00
00:21:6a:a7:4f:ee 0.0.0.0 L2AUTHCOMPLETE (4) Plumbed mobile LWAPP rule on AP
  f0:25:72:3c:0f:20 vapId 3 apVapId 3
00:21:6a:a7:4f:ee 0.0.0.0 L2AUTHCOMPLETE (4) Change state to DHCP_REQD (7) last
  state DHCP_REQD (7)
00:21:6a:a7:4f:ee 0.0.0.0 DHCP_REQD (7) pemAdvanceState2 5253, Adding TMP rule
00:21:6a:a7:4f:ee 0.0.0.0 DHCP_REQD (7) Adding Fast Path rule
  type = Airespace AP - Learn IP address
  on AP f0:25:72:3c:0f:20, slot 1, interface = 13, QOS = 0
  IPv4 ACL ID = 255, IP
00:21:6a:a7:4f:ee 0.0.0.0 DHCP_REQD (7) Fast Path rule (contd...) 802.1P = 0,
  DSCP = 0, TokenID = 7006  Local Bridging Vlan = 25, Local Bridging intf id =
  12
00:21:6a:a7:4f:ee 0.0.0.0 DHCP_REQD (7) Successfully plumbed mobile rule (IPv4
  ACL ID 255, IPv6 ACL ID 255)
00:21:6a:a7:4f:ee Stopping retransmission timer for mobile 00:21:6a:a7:4f:ee
00:21:6a:a7:4f:ee 0.0.0.0 Added NPU entry of type 9, dtlFlags 0x0
00:21:6a:a7:4f:ee Sent an XID frame
00:21:6a:a7:4f:ee Username entry () already exists in name table, length = 253
00:21:6a:a7:4f:ee Username entry () created in mscb for mobile, length = 253
00:21:6a:a7:4f:ee Applying post-handoff policy for station 00:21:6a:a7:4f:ee -
  valid mask 0x1000
00:21:6a:a7:4f:ee QOS Level: -1, DSCP: -1, dot1p: -1, Data Avg: -1, realtime
  Avg: -1, Data Burst -1, Realtime Burst -1
00:21:6a:a7:4f:ee     Session: -1, User session: -1, User elapsed -1 Interface:
```

```
  N/A, IPv4 ACL: N/A, IPv6 ACL:
00:21:6a:a7:4f:ee 0.0.0.0 DHCP_REQD (7) Change state to DHCP_REQD (7) last state
  DHCP_REQD (7)
00:21:6a:a7:4f:ee 0.0.0.0 DHCP_REQD (7) pemCreateMobilityState 6370, Adding TMP
  rule
00:21:6a:a7:4f:ee 0.0.0.0 DHCP_REQD (7) Replacing Fast Path rule type =
  Airespace AP - Learn IP address on AP f0:25:72:3c:0f:20, slot 1, interface =
  13, QOS = 0 IPv4 ACL ID = 255,
00:21:6a:a7:4f:ee 0.0.0.0 DHCP_REQD (7) Fast Path rule (contd...) 802.1P = 0,
  DSCP = 0, TokenID = 7006  Local Bridging Vlan = 25, Local Bridging intf id =
  12
00:21:6a:a7:4f:ee 0.0.0.0 DHCP_REQD (7) Successfully plumbed mobile rule (IPv4
  ACL ID 255, IPv6 ACL ID 255)
00:21:6a:a7:4f:ee Scheduling deletion of Mobile Station:  (callerId: 55) in 1800
  seconds
00:21:6a:a7:4f:ee Pushing IPv6: fe80:0000:0000:0000: 3057:534d:587d:73ae , and
  MAC: 00:21:6A:A7:4F:EE , Binding to Data Plane. SUCCESS !!
00:21:6a:a7:4f:ee apfMsRunStateInc
00:21:6a:a7:4f:ee 0.0.0.0 DHCP_REQD (7) Change state to RUN (20) last state RUN
  (20)
00:21:6a:a7:4f:ee 0.0.0.0 RUN (20) Reached PLUMBFASTPATH: from line 5776
00:21:6a:a7:4f:ee 0.0.0.0 RUN (20) Change state to RUN (20) last state RUN (20)
00:21:6a:a7:4f:ee Pushing IPv6: 2001:0db8:0000:0020: 3057:534d:587d:73ae , and
  MAC: 00:21:6A:A7:4F:EE , Binding to Data Plane. SUCCESS !!

00:21:6a:a7:4f:ee 0.0.0.0 RUN (20) State Update from Mobility-Incomplete to
  Mobility-Complete, mobility role=Foreign, client state=APF_MS_STATE_ASSOCIATED

00:21:6a:a7:4f:ee 0.0.0.0 RUN (20) Change state to RUN (20) last state RUN (20)
00:21:6a:a7:4f:ee 0.0.0.0 RUN (20) Reached PLUMBFASTPATH: from line 4968
00:21:6a:a7:4f:ee 0.0.0.0 RUN (20) Replacing Fast Path rule
  type = Airespace AP Client
  on AP f0:25:72:3c:0f:20, slot 1, interface = 13, QOS = 0
  IPv4 ACL ID = 255, IPv6 ACL ID = 25
00:21:6a:a7:4f:ee 0.0.0.0 RUN (20) Fast Path rule (contd...) 802.1P = 0, DSCP =
  0, TokenID = 7006  Local Bridging Vlan = 25, Local Bridging intf id = 12
00:21:6a:a7:4f:ee 0.0.0.0 RUN (20) Successfully plumbed mobile rule (IPv4 ACL ID
  255, IPv6 ACL ID 255)
00:21:6a:a7:4f:ee 0.0.0.0 Added NPU entry of type 9, dtlFlags 0x0

00:21:6a:a7:4f:ee Set symmetric mobility tunnel for 00:21:6a:a7:4f:ee as in
  Foreign role

00:21:6a:a7:4f:ee 0.0.0.0 Added NPU entry of type 1, dtlFlags 0x1

00:21:6a:a7:4f:ee Pushing IPv6: fe80:0000:0000:0000: 3057:534d:587d:73ae , and
  MAC: 00:21:6A:A7:4F:EE , Binding to Data Plane. SUCCESS !!
00:21:6a:a7:4f:ee Pushing IPv6: 2001:0db8:0000:0020: 3057:534d:587d:73ae , and
  MAC: 00:21:6A:A7:4F:EE , Binding to Data Plane. SUCCESS !!

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

유용한 IPv6 CLI 명령:

<#root>

Show ipv6 neighbor-binding summary

<#root>

Debug ipv6 neighbor-binding filter client

enable

<#root>

Debug ipv6 neighbor-binding filter errors enable

자주 묻는 질문(FAQ)

Q: 브로드캐스트 도메인을 제한하기 위한 최적의 IPv6 접두사 크기는 어떻게 됩니까?

A: IPv6 서브넷을 /64 아래로 세분화할 수 있지만 이 컨피그레이션은 SLAAC를 중단하고 클라이언트 연결에 문제를 일으킵니다. 호스트 수를 줄이기 위해 세그먼테이션이 필요한 경우, 인터페이스 그룹 기능을 사용하여 서로 다른 IPv6 접두사를 사용하는 서로 다른 백엔드 VLAN 간에 클라이언트를 로드 밸런싱할 수 있습니다.

Q: IPv6 클라이언트 지원과 관련하여 확장성 제한이 있습니까?

A: IPv6 클라이언트 지원에 대한 주요 확장성 제한은 모든 무선 클라이언트 IPv6 주소를 추적하는 인접 디바이스 바인딩 테이블입니다. 이 테이블은 최대 클라이언트 수에 8을 곱한 값(클라이언트당 최대 주소 수)을 지원하기 위해 컨트롤러 플랫폼별로 확장됩니다. IPv6 바인딩 테이블을 추가하면 플랫폼에 따라 풀 로드 상태에서 컨트롤러의 메모리 사용량이 약 10-15% 증가할 수 있습니다.

무선 컨트롤러	최대 클라이언트 수	IPv6 네이버 바인딩 테이블 크기
2500	500	4,000
5500	7,000	56,000
WiSM2	15,000	120,000

Q: IPv6 기능이 컨트롤러의 CPU 및 메모리에 미치는 영향은 무엇입니까?

A: CPU에 컨트롤 플레인을 처리하기 위한 여러 코어가 있으므로 영향이 미미합니다. 각각 8개의 IPv6 주소를 사용하는 지원되는 최대 클라이언트를 테스트한 결과, CPU 사용량은 30% 미만이었고 메모리 사용량은 75% 미만이었습니다.

Q: IPv6 클라이언트 지원을 비활성화할 수 있습니까?

A: 네트워크에서 IPv4만 활성화하고 IPv6를 차단하려는 고객의 경우, WLAN별로 모든 거부 트래픽의 IPv6 ACL을 사용하고 적용할 수 있습니다.

Q: IPv4용 WLAN과 IPv6용 WLAN을 하나씩 둘 수 있습니까?

A: 동일한 AP에서 작동하는 서로 다른 두 WLAN에 대해 동일한 SSID 이름 및 보안 유형을 사용할 수 없습니다. IPv6 클라이언트에서 IPv4 클라이언트를 분리하려면 두 개의 WLAN을 생성해야 합니다. 각 WLAN은 모든 IPv4 또는 IPv6 트래픽을 각각 차단하는 ACL을 사용하여 구성해야 합니다.

Q: 클라이언트당 여러 IPv6 주소를 지원하는 것이 중요한 이유는 무엇입니까?

A: 클라이언트에는 인터페이스당 고정, SLAAC 또는 DHCPv6가 할당될 수 있는 IPv6 주소가 여러 개 있을 수 있으며, 항상 자체 할당된 링크-로컬 주소도 있을 수 있습니다. 클라이언트는 다른 IPv6 접두사를 사용하여 추가 주소를 가질 수도 있습니다.

Q: IPv6 개인 주소란 무엇이며, 추적해야 하는 이유는 무엇입니까?

A: SLAAC 주소 할당이 사용 중일 때 클라이언트에 의해 프라이빗(임시) 주소가 임의로 생성됩니다. 이러한 주소는 항상 동일한 호스트 후위(최근 64비트)를 사용하는 호스트 추적이 발생하지 않도록 하루 정도의 빈도로 순환되는 경우가 많습니다. 저작권 침해 추적과 같은 감사 목적으로 이러한 개인 주소를 추적하는 것이 중요합니다. Cisco NCS는 각 클라이언트에서 사용 중인 모든 IPv6 주소를 기록하고, 클라이언트가 로밍하거나 새 세션을 설정할 때마다 기록 방식으로 기록합니다. 이러한 레코드는 NCS에서 최대 1년까지 보유하도록 구성할 수 있습니다.

관련 정보

- 기술 지원 및 문서 – Cisco Systems

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.