Konfigurieren von Multicast mit Wireless LAN Controllern (WLCs) und Access Points (CAPWAP)

Inhalt

Einleitung

In diesem Dokument wird die Konfiguration von Wireless LAN Controllern (WLCs) und Lightweight Access Points (LAPs) für Multicast beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Grundkenntnisse der Konfiguration von APs und Cisco WLCs
- Kenntnisse der Konfiguration von einfachem Routing und Multicasting in einem kabelgebundenen Netzwerk

Stellen Sie sicher, dass die folgenden Anforderungen erfüllt sind, bevor Sie diese Konfiguration ausprobieren.

Verwendete Komponenten

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

- Cisco 3504 WLC mit Firmware-Version 8.5
- Cisco LAPs der Serie 3702
- Microsoft Windows 10 Wireless Client mit Intel(R) Dual Band Wireless-AC 8265 Adapter
- Cisco Switch der Serie 6500 mit Cisco IOS® Softwareversion 12.2(18)
- Zwei Cisco Switches der Serie 3650 mit Cisco IOS Software, Version 16.3.7

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Multicast in WLCs

Wenn Ihr Netzwerk Packet Multicasting unterstützt, können Sie die vom Controller verwendete Multicast-Methode konfigurieren, um die Multicast-Pakete über CAPWAP gleichzeitig an alle oder mehrere Access Points zu übertragen. Der Controller führt Multicasting in zwei Modi durch:

- Unicast-Modus - In diesem Modus sendet der Controller jedes Multicast-Paket per Unicast an jeden AP, der dem Controller zugeordnet ist. Dieser Modus ist ineffizient, kann jedoch in Netzwerken erforderlich sein, die Multicasting nicht unterstützen.
- Multicast-Modus - In diesem Modus sendet der Controller Multicast-Pakete an eine CAPWAP-Multicast-Gruppe. Diese Methode reduziert den Overhead auf dem Controller-Prozessor und verlagert die Paketreplikation auf Ihr Netzwerk, was wesentlich effizienter ist als die Unicast-Methode. Wenn Sie ein anderes VLAN/Subnetz für den Access Point und den WLC verwenden, ist Multicast-Routing auf der kabelgebundenen Seite erforderlich, um die Weiterleitung des CAPWAP-Multicast-Downlink-Pakets von WLC an den Access Point zu unterstützen.

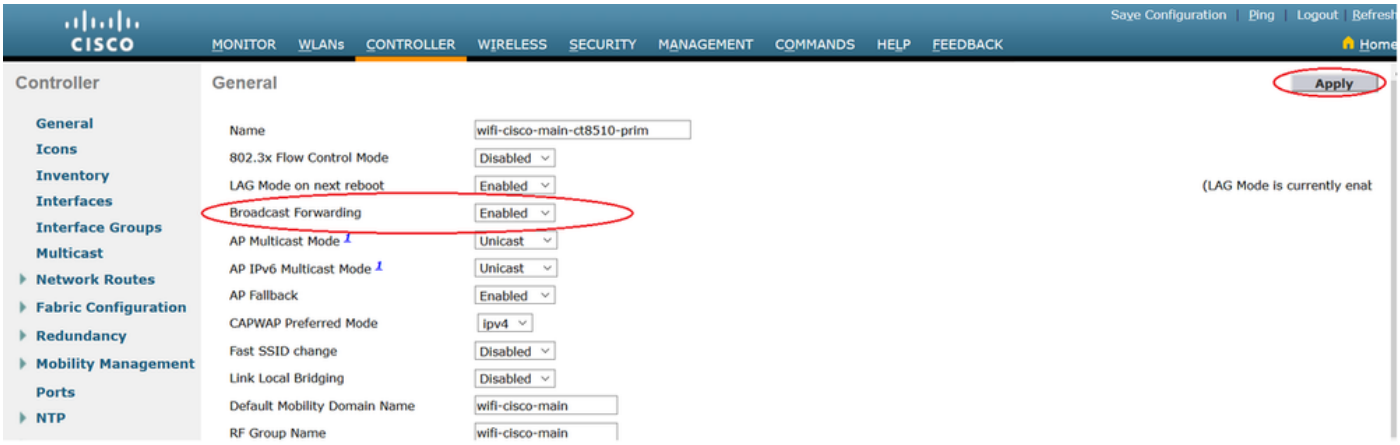
Wenn Sie den Multicast-Modus aktivieren und der Controller ein Multicast-Paket vom LAN empfängt, kapselt der Controller das Paket mithilfe von CAPWAP und leitet es an die Adresse der CAPWAP-Multicast-Gruppe weiter. Der Controller verwendet immer die Management-Schnittstelle, um Multicast-Pakete zu senden. Access Points in der Multicast-Gruppe empfangen das Paket und leiten es an alle BSSIDs weiter, die der Schnittstelle zugeordnet sind, auf der Clients Multicast-Datenverkehr empfangen. Aus Sicht des Access Points wird Multicast an alle SSIDs gesendet.

Broadcast-Verhalten in verschiedenen WLCs

Standardmäßig leitet der WLC keine Broadcast-Pakete (wie z. B. Upnp-Datenverkehr) weiter, es sei denn, die Broadcast-Weiterleitung ist aktiviert. Geben Sie diesen Befehl in der WLC-CLI ein, um Broadcast zu aktivieren:

```
config network broadcast enable
```

Oder aktivieren Sie es über die GUI:



Broadcast verwendet die **multicast mode** die auf dem WLC konfiguriert ist, auch wenn Multicast nicht aktiviert ist. Der Grund hierfür ist, dass Sie die IP-Adresse oder den Modus nur festlegen können, wenn Sie Multicast in der GUI aktivieren. Wenn der Multicast-Modus also Unicast ist und der Broadcast aktiviert ist, wird dieser Modus vom Broadcast verwendet (Broadcast-Datenverkehr wird am WLC repliziert und Unicast an jeden AP). Wenn der Multicast-Modus auf Multicast mit einer Multicast-Adresse festgelegt ist, verwendet der Broadcast diesen Modus (jedes Broadcast-Paket wird über die Multicast-Gruppe an die APs gesendet).

> **Anmerkung:** Bis Version 7.5 war die für CAPWAP-Multicast verwendete Portnummer 12224. Ab Version 7.6 wird die für CAPWAP verwendete Portnummer in 5247 geändert.

Multicast mit AAA-Übersteuerung wird von Wireless LAN Controller Version 4.2 und höher unterstützt. Sie müssen IGMP-Snooping auf dem Controller aktivieren, damit Multicast mit AAA-Übersteuerung funktioniert.

IGMP-Snooping auf WLC

Internet Group Management Protocol (IGMP)-Snooping wird auf WLC unterstützt, um Multicast-Pakete besser leiten zu können. Wenn diese Funktion aktiviert ist, sammelt der Controller IGMP-Berichte von den Clients, verarbeitet die Berichte, erstellt eindeutige Multicast-Gruppen-IDs (MGIDs) aus den IGMP-Berichten, nachdem er die Layer-3-Multicast-Adresse und die VLAN-Nummer überprüft hat, und sendet die IGMP-Berichte an den Infrastruktur-Switch. Der Controller sendet diese Berichte mit der Quelladresse als Schnittstellenadresse, an der er die Berichte von den Clients empfangen hat.

Der Controller aktualisiert dann die MGID-Tabelle des Access Points auf dem AP mit der MAC-Adresse des Clients. Wenn der Controller Multicast-Datenverkehr für eine bestimmte Multicast-Gruppe empfängt, leitet er ihn an alle APs weiter. Allerdings senden nur die APs, die über aktive Clients verfügen, die diese Multicast-Gruppe überwachen oder abonnieren, Multicast-Datenverkehr in diesem speziellen WLAN. IP-Pakete werden mit einer eindeutigen MGID für ein Eingangs-VLAN und die Multicast-Zielgruppe weitergeleitet. Layer-2-Multicast-Pakete werden mit einer eindeutigen MGID für die Eingangsschnittstelle weitergeleitet.

Der Controller unterstützt Multicast Listener Discovery (MLD) v1 Snooping für IPv6 Multicast. Mit dieser Funktion werden IPv6-Multicast-Datenflüsse nachverfolgt und an die Clients weitergeleitet, die sie anfordern. Um IPv6-Multicast zu unterstützen, müssen Sie den globalen Multicast-Modus aktivieren.

> **Anmerkung:** Wenn Sie den globalen Multicast-Modus deaktivieren, leitet der Controller die

IPv6-ICMP-Multicast-Nachrichten weiter, z. B. Router-Ankündigungen und DHCPv6-Solicits, da diese für die Funktion von IPv6 erforderlich sind. Wenn der globale Multicast-Modus auf dem Controller aktiviert ist, hat dies keine Auswirkungen auf ICMPv6- und DHCPv6-Meldungen. Diese Nachrichten werden unabhängig davon weitergeleitet, ob der globale Multicast-Modus aktiviert ist oder nicht.

Wenn IGMP-Snooping deaktiviert ist, gilt Folgendes:

- Der Controller verwendet beim Senden von Multicast-Daten an den Access Point stets die Layer-2-MGID. Jeder erstellten Schnittstelle wird eine Layer-2-MGID zugewiesen. Die Verwaltungsschnittstelle hat beispielsweise eine MGID von 0, und der ersten erstellten dynamischen Schnittstelle wird eine MGID von 8 zugewiesen, die mit jeder erstellten dynamischen Schnittstelle inkrementiert wird.
- Die IGMP-Pakete der Clients werden an den Router weitergeleitet. Als Ergebnis wird die IGMP-Tabelle des Routers mit der IP-Adresse der Clients als letztem Reporter aktualisiert.

Wenn IGMP-Snooping aktiviert ist, gilt Folgendes:

- Der Controller verwendet immer Layer-3-MGID für den gesamten Layer-3-Multicast-Datenverkehr, der an den Access Point gesendet wird. Für den gesamten Layer-2-Multicast-Verkehr wird weiterhin Layer-2-MGID verwendet.
- IGMP-Berichtspakete von Wireless-Clients werden vom Controller verbraucht oder absorbiert, wodurch eine Abfrage für die Clients generiert wird. Nachdem der Router die IGMP-Abfrage gesendet hat, sendet der Controller die IGMP-Berichte mit der IP-Adresse der Schnittstelle als Listener-IP-Adresse für die Multicast-Gruppe. Daher wird die IGMP-Tabelle des Routers mit der IP-Adresse des Controllers als Multicast-Listener aktualisiert.
- Wenn der Client, der die Multicast-Gruppen abhört, von einem Controller zu einem anderen wechselt, überträgt der erste Controller alle Multicast-Gruppeninformationen für den abhörenden Client an den zweiten Controller. Dadurch kann der zweite Controller sofort die Multicast-Gruppeninformationen für den Client erstellen. Der zweite Controller sendet IGMP-Berichte an das Netzwerk für alle Multicast-Gruppen, auf die der Client hörte. Dieser Prozess unterstützt die nahtlose Übertragung von Multicast-Daten an den Client.
- Der WLC funktioniert hauptsächlich in IGMPv1 und v2. APs verwenden IGMPv2, um der CAPWAP-Multicast-Gruppe beizutreten. Wenn Wireless-Clients igmpv3-Berichte senden, werden diese vom WLC als igmpv2 übersetzt und an das kabelgebundene Netzwerk weitergeleitet. Von diesem Zeitpunkt an werden Antworten in IGMPv2 erwartet. Dies bedeutet, dass Wireless-Clients IGMPv3 verwenden können, aber IGMPv3-Funktionen für das kabelgebundene Netzwerk vom WLC nicht unterstützt werden.

Anmerkung:
- Die MGIDs sind controllerspezifisch. Dieselben Multicast-Gruppenpakete, die vom selben VLAN auf zwei verschiedenen Controllern stammen, können zwei verschiedenen MGIDs zugeordnet werden.
- Wenn Layer-2-Multicast aktiviert ist, wird allen Multicast-Adressen, die von einer Schnittstelle stammen, eine einzelne MGID zugewiesen.
- Die maximale Anzahl der pro VLAN für einen Controller unterstützten Multicast-Gruppen beträgt 100.

Wireless Multicast-Roaming

Eine große Herausforderung für einen Multicast-Client in einer Wireless-Umgebung besteht darin, die Mitgliedschaft in der Multicast-Gruppe auch dann aufrechtzuerhalten, wenn diese über das WLAN verschoben wird. Unterbrechungen in der Wireless-Verbindung, die vom Access Point zum Access Point übertragen werden, können eine Unterbrechung der Multicast-Anwendung eines Clients verursachen. IGMP spielt eine wichtige Rolle bei der Pflege dynamischer Gruppenmitgliedschaftsinformationen.

Ein grundlegendes Verständnis von IGMP ist wichtig, um zu verstehen, was mit der Multicast-Sitzung eines Clients passiert, wenn dieser das Netzwerk durchläuft. In einem Layer-2-Roaming werden Sitzungen einfach deshalb aufrechterhalten, weil der fremde WAP bei entsprechender Konfiguration bereits zur Multicast-Gruppe gehört und der Datenverkehr nicht an einen anderen Ankerpunkt im Netzwerk getunnelt wird. Layer-3-Roaming-Umgebungen sind auf diese Weise etwas komplexer, und je nachdem, welchen Tunneling-Modus Sie auf Ihren Controllern konfiguriert haben, können sich die IGMP-Meldungen auswirken, die von einem Wireless-Client gesendet werden. Der standardmäßige Mobility Tunneling-Modus auf einem Controller ist asymmetrisch. Das bedeutet, dass Datenrückverkehr zum Client an den Anker-WLC gesendet und dann an den ausländischen WLC weitergeleitet wird, wo sich die zugehörige Client-Verbindung befindet. Ausgehende Pakete werden von der ausländischen WLC-Schnittstelle weitergeleitet. Im symmetrischen Mobility Tunneling-Modus werden sowohl eingehender als auch ausgehender Datenverkehr an den Anker-Controller getunnelt.

Wenn der überwachende Client zu einem Controller in einem anderen Subnetz roamt, werden die Multicast-Pakete an den Anker-Controller des Clients getunnelt, um die RPF-Prüfung (Reverse Path Filtering) zu vermeiden. Der Anker leitet die Multicast-Pakete dann an den Infrastruktur-Switch weiter.

Richtlinien für die Verwendung des Multicast-Modus

- Die Cisco Wireless-Netzwerklösung verwendet einige IP-Adressbereiche für bestimmte Zwecke. Diese Bereiche müssen Sie bei der Konfiguration einer Multicast-Gruppe berücksichtigen: 224.0.0.0 bis 224.0.0.255 - Reservierte lokale Verbindungsadressen224.0.1.0 bis 238.255.255.255 - Adressen mit globalem Gültigkeitsbereich239.0.0.0 bis 239.255.x.y/16 - Adressen mit begrenztem Gültigkeitsbereich
- Wenn Sie den Multicast-Modus auf dem Controller aktivieren, müssen Sie auch eine CAPWAP-Multicast-Gruppenadresse konfigurieren. APs sind unter Verwendung von IGMP für die CAPWAP-Multicast-Gruppe zugelassen.
- APs im Überwachungs-, Sniffer- oder Rogue-Detektor-Modus werden nicht Teil der CAPWAP-Multicast-Gruppenadresse.
- Die auf den Controllern konfigurierte CAPWAP-Multicast-Gruppe muss für verschiedene Controller unterschiedlich sein.

CAPWAPs übertragen Multicast-Pakete mit einer der konfigurierten erforderlichen Datenraten.

Da Multicast-Frames auf der MAC-Ebene nicht erneut übertragen werden, können Clients am Zellenrand sie möglicherweise nicht erfolgreich empfangen. Wenn ein zuverlässiger Empfang ein Ziel ist, müssen Multicast-Frames mit einer niedrigen Datenrate übertragen werden, indem die höheren obligatorischen Datenraten deaktiviert werden. Wenn Unterstützung für Multicast-Frames mit hoher Datenrate erforderlich ist, kann es nützlich sein, die Zellengröße zu verkleinern und alle niedrigeren Datenraten zu deaktivieren oder Media Stream zu verwenden.

Je nach Ihren Anforderungen können Sie folgende Aktionen durchführen:

- Wenn Sie Multicast-Daten mit höchster Zuverlässigkeit übertragen müssen und keine große Multicast-Bandbreite erforderlich ist, konfigurieren Sie eine einzelne Basisrate, die niedrig genug ist, um die Ränder der Funkzellen zu erreichen.
- Wenn Sie Multicast-Daten mit einer bestimmten Datenrate übertragen müssen, um einen bestimmten Durchsatz zu erreichen, können Sie diese Rate als höchste Basisrate konfigurieren. Sie können auch eine niedrigere Basisrate für die Abdeckung von Nicht-Multicast-Clients festlegen.
- Konfigurieren des Medien-Streams

- Der Multicast-Modus funktioniert nicht bei Ereignissen, die die Mobilität zwischen Subnetzen betreffen, wie z. B. Gast-Tunneling. Sie kann jedoch über Layer-3-Roaming betrieben werden.
- Bei CAPWAP verwirft der Controller an die UDP-Steuerungs- und Datenports 5246 bzw. 5247 gesendete Multicast-Pakete. Daher können Sie diese Portnummern nicht für Multicast-Anwendungen in Ihrem Netzwerk verwenden. Cisco empfiehlt, die in dieser WLC-Protokolltabelle aufgeführten Multicast-UDP-Ports nicht als vom Controller verwendete UDP-Ports zu verwenden.
- Cisco empfiehlt, dass alle Multicast-Anwendungen im Netzwerk nicht die Multicast-Adresse verwenden, die auf dem Controller als CAPWAP-Multicast-Gruppenadresse konfiguriert wurde.
- Damit Multicast auf dem Cisco 2504 WLC funktioniert, müssen Sie die Multicast-IP-Adresse konfigurieren.
- Der Multicast-Modus wird auf Cisco Flex WLCs der Serie 7500 nicht unterstützt.
- IGMP- und MLD-Snooping werden auf Cisco Flex 7510 WLCs nicht unterstützt.
- Für Cisco 8510 WLCs: Sie müssen Multicast-Unicast aktivieren, wenn IPv6-Unterstützung auf FlexConnect-APs mit zentralen Switching-Clients erforderlich ist.Sie können nur dann vom Multicast-Modus in den Multicast-Unicast-Modus wechseln, wenn der globale Multicast-Modus deaktiviert ist. IGMP- oder MLD-Snooping werden daher nicht unterstützt.FlexConnect-APs sind keiner Multicast-Multicast-Gruppe zugeordnet.IGMP- oder MLD-Snooping wird auf FlexConnect APs nicht unterstützt. IGMP- und MLD-Snooping sind nur für APs im lokalen Modus im Multicast-Multicast-Modus zulässig.Da VideoStream IGMP- oder MLD-Snooping erfordert, funktioniert die VideoStream-Funktion nur auf APs im lokalen Modus, wenn Multicast-Multicast-Modus und Snooping aktiviert sind.
- Der Cisco Mobility Express Controller unterstützt den AP-Multicast-Modus nicht.
- Cisco empfiehlt, den Modus "Broadcast-Unicast" oder "Multicast-Unicast" nicht in der Controller-Konfiguration zu verwenden, wenn mehr als 50 APs verbunden sind.
- Bei Verwendung des lokalen und FlexConnect AP-Modus unterscheidet sich die Controller-Multicast-Unterstützung für verschiedene Plattformen.

Die folgenden Parameter wirken sich auf die Multicast-Weiterleitung aus:

- Controller-Plattform.
- Konfiguration des globalen AP-Multicast-Modus am Controller
- Modus des AP: Lokales FlexConnect-zentrales Switching
- Beim lokalen Switching sendet/empfängt er das Paket nicht an/vom Controller, sodass es unerheblich ist, welcher Multicast-Modus auf dem Controller konfiguriert ist. **Anmerkung:** FlexConnect-APs werden nur dann Mitglied der CAPWAP-Multicast-Gruppe, wenn sie über zentral geschaltete WLANs verfügen. Flex APs, die nur lokal geschaltete WLANs verwenden, werden nicht zur CAPWAP-Multicast-Gruppe hinzugefügt.

- Ab Version 8.2.100.0 ist es aufgrund der in dieser Version eingeführten Multicast- und IP-Adressen-Validierung nicht möglich, einige der früheren Konfigurationen vom Controller herunterzuladen. Die Plattformunterstützung für den globalen Multicast- und Multicast-Modus ist in dieser Tabelle aufgeführt. Tabelle 1: Plattformunterstützung für den globalen Multicast- und Multicast-Modus

Netzwerkeinrichtung

Alle Geräte und die Einrichtung sind in dem Diagramm dargestellt:

Die Geräte müssen für grundlegende IP-Verbindungen konfiguriert werden und Multicasting im Netzwerk ermöglichen. So können Benutzer Multicast-Datenverkehr von der kabelgebundenen zur Wireless-Seite und umgekehrt senden und empfangen.

In diesem Dokument werden die folgenden IP-Adressen für den WLC, den AP und die Wireless-Clients verwendet:

```
WLC Management Interface IP address: 10.63.84.48/23
LAP IP address: 172.16.16.0/23
Wireless Client C1 IP address: 192.168.47.17/24
Wired Client W1 IP address: 192.168.48.11/24
CAPWAP multicast IP address : 239.2.2.2
Stream multicast address : 239.100.100.100
```

Konfigurieren

Um die Geräte für diese Konfiguration zu konfigurieren, müssen folgende Schritte ausgeführt werden:

- Konfigurieren des Wireless-Netzwerks für Multicasting
- Konfigurieren des kabelgebundenen Netzwerks für Multicasting

Konfigurieren des Wireless-Netzwerks für Multicasting

Bevor Sie Multicasting auf WLCs konfigurieren, müssen Sie den WLC für den Basisbetrieb konfigurieren und die APs beim WLC registrieren. In diesem Dokument wird davon ausgegangen, dass der WLC für den Basisbetrieb konfiguriert ist und dass die LAPs beim WLC registriert sind. Wenn Sie ein neuer Benutzer sind, der versucht, den WLC für den Basisbetrieb mit LAPs einzurichten, finden Sie weitere Informationen unter Lightweight AP (LAP) Registration to a Wireless LAN Controller (WLC).

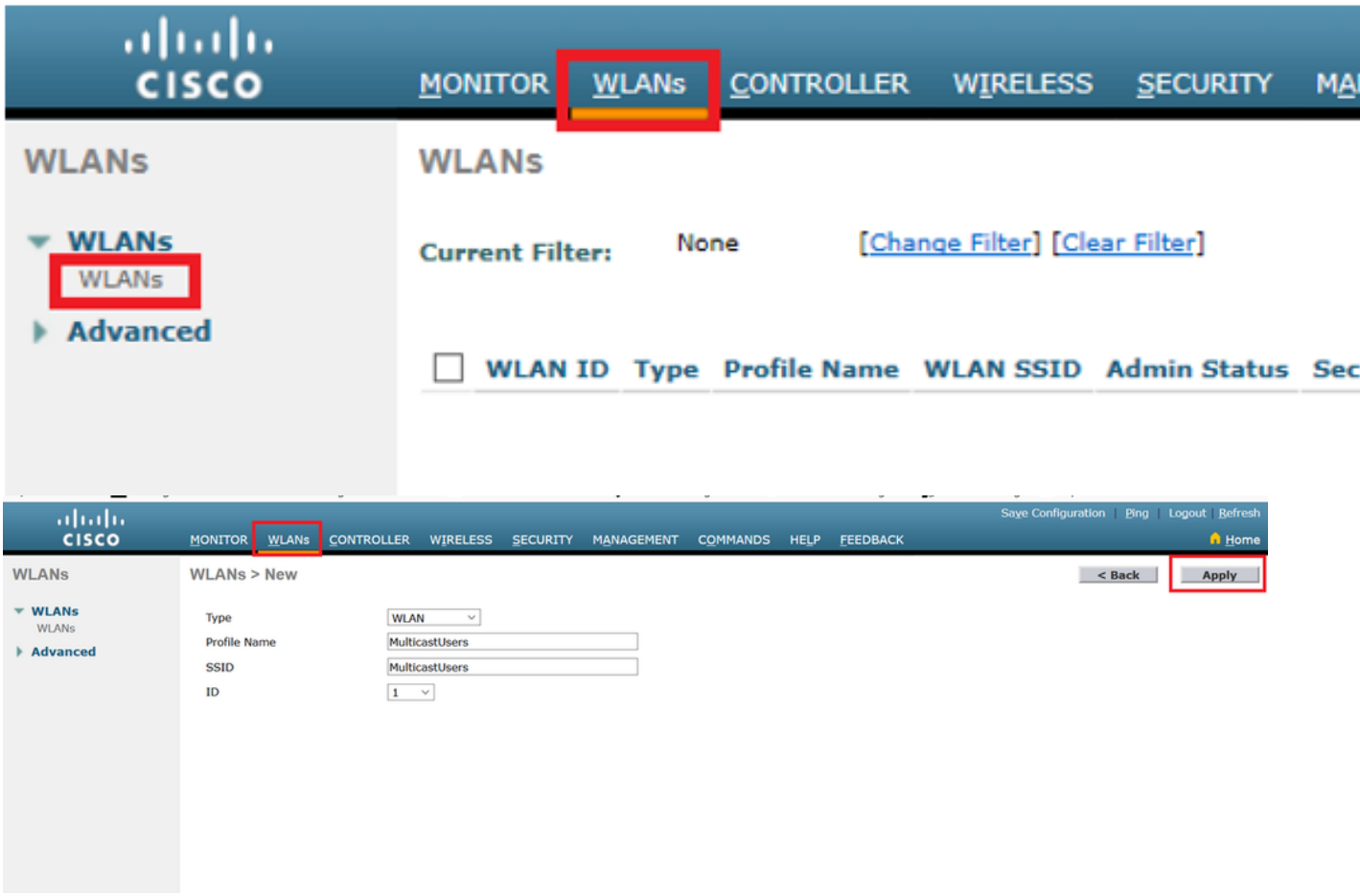
Nachdem die LAPs beim WLC registriert wurden, führen Sie die folgenden Schritte aus, um die LAPs und den WLC für diese Einrichtung zu konfigurieren:

1. WLAN für Clients konfigurieren
2. Ethernet-Multicast-Modus über die Benutzeroberfläche aktivieren

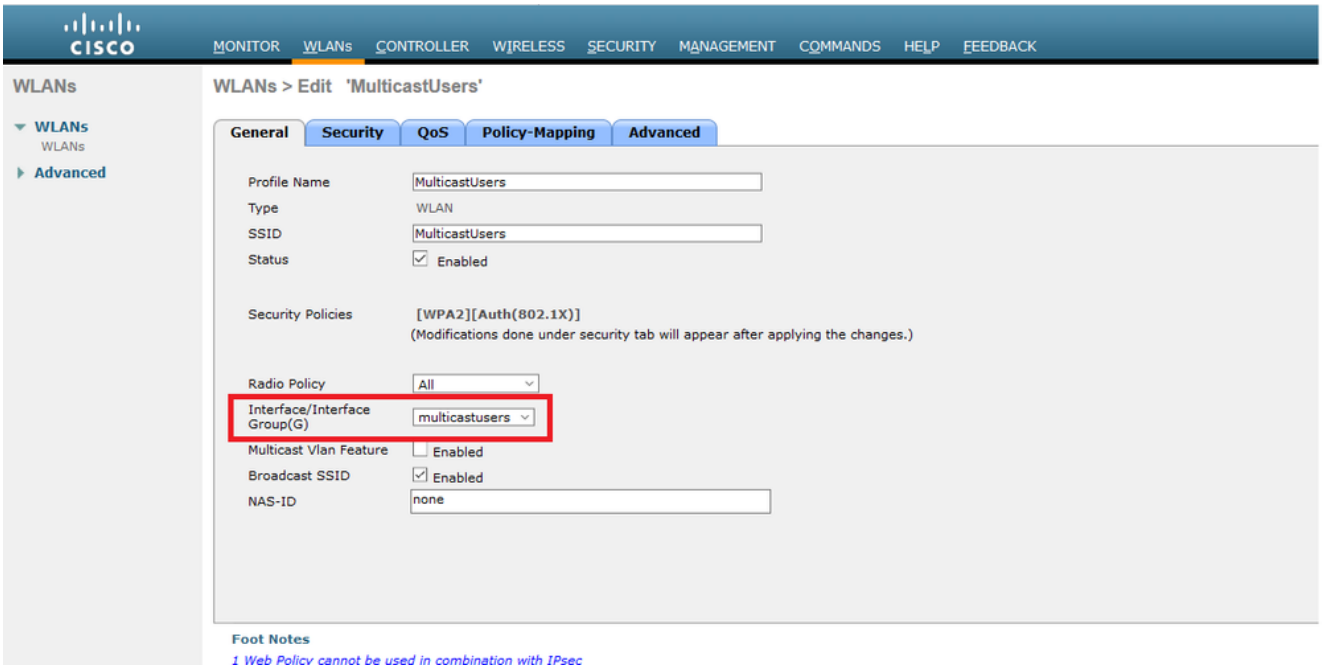
WLAN für Clients konfigurieren

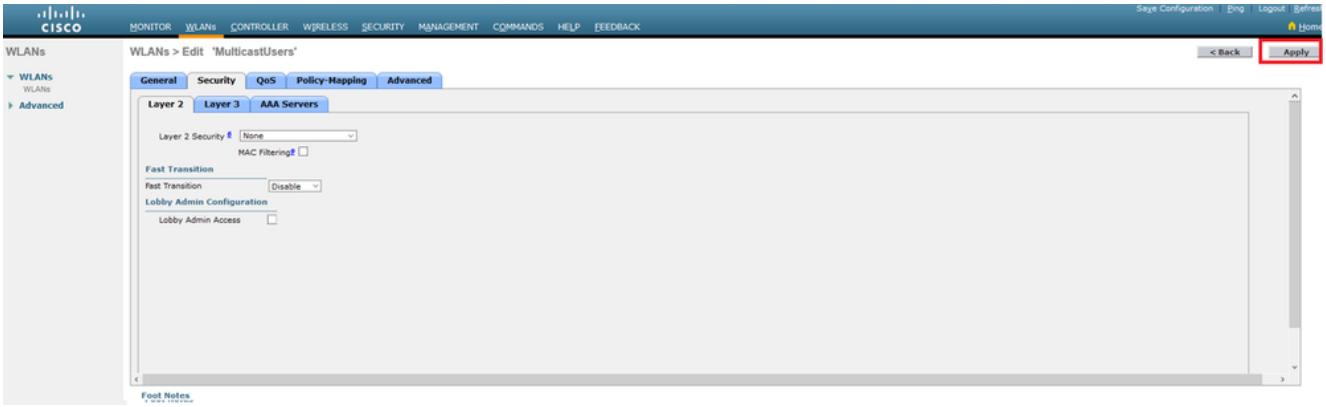
Der erste Schritt besteht darin, ein WLAN zu erstellen, mit dem sich die Wireless-Clients verbinden und Zugriff auf das Netzwerk erhalten können. Gehen Sie wie folgt vor, um ein WLAN auf dem WLC zu erstellen:

1. Klicken Sie auf **WLANs** von der Controller-GUI aus, um ein WLAN zu erstellen.
2. Klicken Sie auf **New** um ein neues WLAN zu konfigurieren.
   In diesem Beispiel erhält das WLAN den Namen **MulticastUsers** und die WLAN-ID ist 1.



3. Klicken Sie auf **Apply**.
4. Im **WLAN > Edit Window**definieren die WLAN-spezifischen Parameter.
5. Wählen Sie für das WLAN die entsprechende Schnittstelle aus dem **Interface Name** feld.In diesem Beispiel wird die MulticastUsers-Schnittstelle (192.168.47.0/24) dem WLAN zugeordnet.
6. Wählen Sie die anderen Parameter aus, die von den Konstruktionsanforderungen abhängen.In diesem Beispiel können Sie ein WLAN ohne L2-Sicherheit verwenden (offenes WLAN).





7. Klicken Sie auf **Apply**.

Führen Sie die folgenden Befehle aus, um die WLANs auf dem WLC mithilfe der CLI zu konfigurieren:

1. Stellen Sie die **config wlan create** um ein neues WLAN zu erstellen. Geben Sie für "wlan-id" eine ID zwischen 1 und 16 ein. Geben Sie für "wlan-name" eine SSID mit bis zu 31 alphanumerischen Zeichen ein.
2. Stellen Sie die **config wlan enable** , um ein WLAN zu aktivieren.Für das Beispiel in diesem Dokument lauten die Befehle:

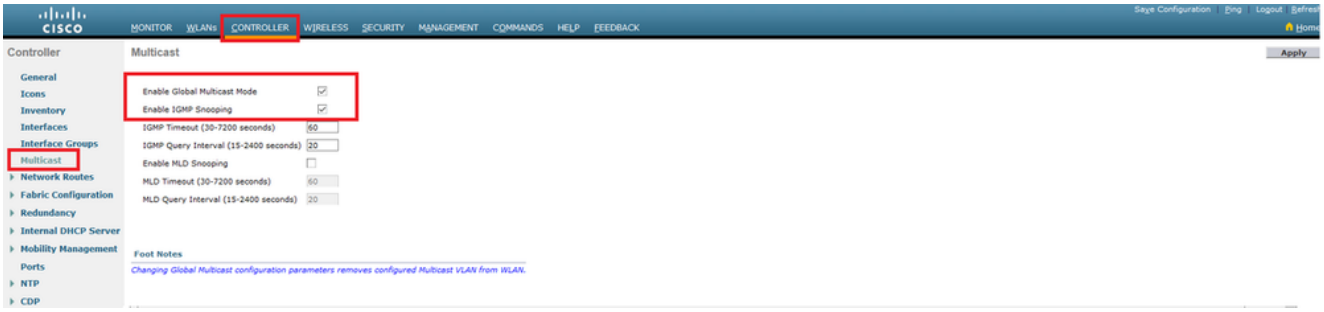
```
config wlan create 1 MulticastUsers
config wlan enable 1
```

Konfigurieren des Multicast-Modus über die Benutzeroberfläche

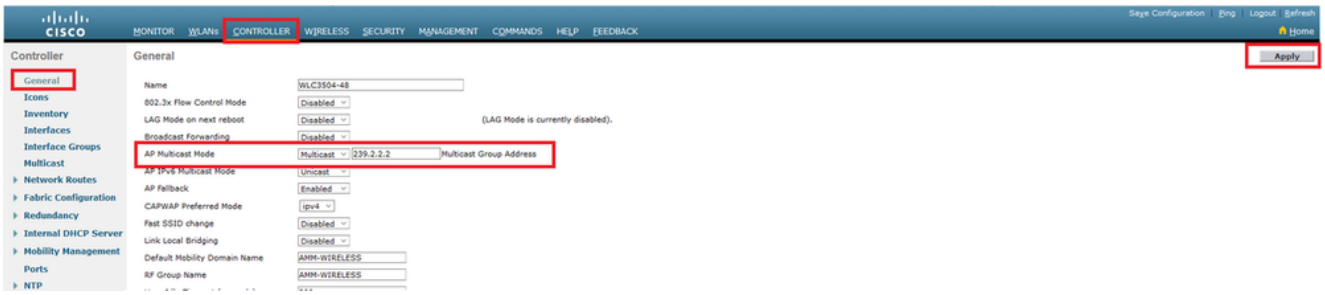
Im nächsten Schritt wird der WLC für Multicasting konfiguriert. Führen Sie diese Schritte aus:

1. Navigieren Sie zu **Controller > Multicast**. Daraufhin wird die Multicast-Seite geöffnet.
2. Wählen Sie **Enable Global Multicast Mode** Kontrollkästchen, um den WLC für die Weiterleitung von Multicast-Paketen zu konfigurieren. Der Standardwert ist deaktiviert.
3. Wenn Sie IGMP-Snooping aktivieren möchten, wählen Sie **Enable IGMP snooping**

Kontrollkästchen. Wenn Sie IGMP-Snooping deaktivieren möchten, lassen Sie das Kontrollkästchen deaktiviert. Der Standardwert ist deaktiviert:



4. Navigieren Sie zu **Controller > General**. Wählen Sie für den AP Multicast Mode aus dem Dropdown-Menü **Multicast** und die Multicast-IP-Adresse konfigurieren. In diesem Beispiel wird 239.2.2.2 verwendet:



5. Klicken Sie auf **Apply**.

Konfigurieren des Multicast-Modus über die CLI

Führen Sie die folgenden Befehle aus, um Multicast über die CLI zu aktivieren:

1. Geben Sie in der Befehlszeile den Befehl **config network multicast global enable** aus.
2. Geben Sie in der Befehlszeile den Befehl **config network multicast mode multicast <multicast-group-ip-address>** aus.Für das Beispiel in diesem Dokument lauten die Befehle:
   `config network multicast global enable config network multicast mode multicast 239.2.2.2`

Nachdem der Administrator Multicast aktiviert hat (der Multicast-Modus ist standardmäßig deaktiviert) und die CAPWAP-Multicast-Gruppe konfiguriert hat, hat der neue Multicast-Algorithmus eine der folgenden Möglichkeiten:

Wenn sich die Quelle der Multicast-Gruppe im LAN befindet:

Ein Multicast wird aktiviert, und die CAPWAP-Multicast-Gruppe wird konfiguriert. Der WAP sendet eine IGMP-Anfrage, um der CAPWAP-Multicast-Gruppe des Controllers beizutreten. Dies löst die normale Einrichtung für den Multicast-Status auf den Multicast-fähigen Routern zwischen dem Controller und den APs aus. Die Quell-IP-Adresse für die Multicast-Gruppe ist die IP-Adresse der Verwaltungsschnittstelle des Controllers.

Wenn der Controller ein Multicast-Paket von einem der Client-VLANs auf dem ersten Hop-Router empfängt, überträgt er das Paket über die Verwaltungsschnittstelle auf der niedrigsten QoS-Ebene an die CAPWAP-Multicast-Gruppe. Die QoS-Bits für das CAPWAP-Multicast-Paket sind auf der niedrigsten Ebene fest codiert und können vom Benutzer nicht geändert werden.

Das Multicast-fähige Netzwerk sendet das CAPWAP-Multicast-Paket an jeden APs, der der

CAPWAP-Multicast-Gruppe beigetreten ist. Das Multicast-fähige Netzwerk nutzt die üblichen Multicast-Mechanismen auf den Routern, um das Paket auf dem Weg zu replizieren, falls erforderlich, sodass das Multicast-Paket alle APs erreicht. Dadurch entfällt die Replikation von Multicast-Paketen durch den Controller.

APs können andere Multicast-Pakete empfangen, aber nur die Multicast-Pakete verarbeiten, die von dem Controller stammen, dem sie aktuell angehören. Alle anderen Kopien werden verworfen. Wenn dem VLAN, von dem aus das ursprüngliche Multicast-Paket gesendet wurde, mehr als eine WLAN-SSID zugeordnet ist, überträgt der WAP das Multicast-Paket über jede WLAN-SSID (zusammen mit der WLAN-Bitmap im CAPWAP-Header). Wenn sich diese WLAN-SSID zudem auf beiden Funkmodulen (802.11g und 802.11a) befindet, übertragen beide Funkmodule das Multicast-Paket auf der WLAN-SSID, wenn ihr Clients zugeordnet sind, auch wenn diese Clients den Multicast-Datenverkehr nicht angefordert haben.

Wenn die Quelle der Multicast-Gruppe ein Wireless-Client ist:

Das Multicast-Paket wird vom AP zum Controller per Unicast (CAPWAP-gekapselt) übertragen, ähnlich wie beim standardmäßigen Datenverkehr der Wireless-Clients.

Der Controller erstellt zwei Kopien des Multicast-Pakets. Eine Kopie wird an das VLAN gesendet, das der WLAN-SSID zugeordnet ist, auf der sie empfangen wurde. Auf diese Weise können Empfänger im LAN den Multicast-Stream empfangen, und der Router kann sich über die neue Multicast-Gruppe informieren. Die zweite Kopie des Pakets ist CAPWAP-gekapselt und wird an die CAPWAP-Multicast-Gruppe gesendet, damit Wireless-Clients den Multicast-Stream empfangen können.

Konfigurieren des kabelgebundenen Netzwerks für Multicasting

Um das kabelgebundene Netzwerk für diese Konfiguration zu konfigurieren, müssen Sie den L3-Core-Switch für einfaches Routing konfigurieren und Multicast-Routing aktivieren.

Im kabelgebundenen Netzwerk kann jedes beliebige Multicast-Protokoll verwendet werden. In diesem Dokument wird PIM-DM als Multicast-Protokoll verwendet. Detaillierte Informationen zu den verschiedenen Protokollen, die in einem kabelgebundenen Netzwerk für Multicasting verwendet werden können, finden Sie im Cisco IOS IP Multicast Configuration Guide.

Core Switch-Konfiguration

```
ip multicast-routing !--- Enables IP Multicasting on the network. interface Vlan16
description AP Management VLAN
ip address 172.16.16.1 255.255.254.0
ip helper-address 10.63.84.5
ip pim dense-mode
!--- Enables PIM-Dense Mode Multicast Protocol on the interface.
interface Vlan47
description Wireless Client
ip address 192.168.47.1 255.255.255.0
ip helper-address 10.63.84.5
ip pim dense-mode !--- Enables PIM-Dense Mode Multicast Protocol on the interface. ! interface Vlan48
description Wired Client
ip address 192.168.48.1 255.255.255.0
ip helper-address 10.63.84.5
ip pim dense-mode !--- Enables PIM-Dense Mode Multicast Protocol on the interface. interface Vlan84
description Wireless Management VLAN
ip address 10.63.84.1 255.255.254.0
ip pim dense-mode ! end
```

Auf dem L2 Access Switch ist keine Konfiguration erforderlich, da IGMP-Snooping auf Cisco Switches standardmäßig aktiviert ist.

Überprüfung und Fehlerbehebung

Nutzen Sie diesen Abschnitt, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Um die Konfiguration zu überprüfen, müssen Sie Multicast-Datenverkehr von der Quelle W1 senden und überprüfen, ob Multicast-Datenverkehr durch das kabelgebundene Netzwerk fließt und die Mitglieder der kabelgebundenen und drahtlosen Gruppe (C1) erreicht.

Führen Sie diese Aufgabe aus, um zu testen, ob IP-Multicast in Ihrem Netzwerk richtig konfiguriert ist.

Überprüfen Sie mithilfe der Befehle das Multicast-Routing auf dem Core-Switch und die IGMP-Zugehörigkeit. **show ip mroute** und **show ip igmp membership** . Die Ausgabe des vorherigen Beispiels wird hier angezeigt:

```
CORE1-R1#show ip mroute
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
L - Local, P - Pruned, R - RP-bit set, F - Register flag,
T - SPT-bit set, J - Join SPT, M - MSDP created entry,
X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
U - URD, I - Received Source Specific Host Report, Z - Multicast Tunnel
Y - Joined MDT-data group, y - Sending to MDT-data group
Outgoing interface flags: H - Hardware switched, A - Assert winner
Timers: Uptime/Expires
Interface state: Interface, Next-Hop or VCD, State/Mode

(*, 239.255.255.250), 21:19:09/00:02:55, RP 0.0.0.0, flags: DC
Incoming interface: Null, RPF nbr 0.0.0.0
Outgoing interface list:
Vlan48, Forward/Dense, 00:04:48/00:00:00
Vlan84, Forward/Sparse-Dense, 21:19:09/00:00:00

(*, 239.100.100.100), 00:01:58/stopped, RP 0.0.0.0, flags: DC
Incoming interface: Null, RPF nbr 0.0.0.0
Outgoing interface list:
Vlan47, Forward/Dense, 00:01:29/00:00:00
(192.168.48.11, 239.100.100.100), 00:01:58/00:02:58, flags: T
Incoming interface: Vlan48, RPF nbr 0.0.0.0, RPF-MFD
Outgoing interface list:
Vlan47, Forward/Dense, 00:01:29/00:00:00, H

(*, 224.0.1.40), 1d21h/00:02:54, RP 0.0.0.0, flags: DCL
Incoming interface: Null, RPF nbr 0.0.0.0
Outgoing interface list:
Vlan84, Forward/Sparse-Dense, 1d01h/00:00:00

(*, 239.2.2.2), 01:21:13/stopped, RP 0.0.0.0, flags: DC
Incoming interface: Null, RPF nbr 0.0.0.0
Outgoing interface list:
Vlan16, Forward/Dense, 00:33:10/00:00:00

(10.63.84.48, 239.2.2.2), 00:33:46/00:02:51, flags: T
```

```
Incoming interface: Vlan84, RPF nbr 0.0.0.0, RPF-MFD
Outgoing interface list:
Vlan16, Forward/Dense, 00:33:10/00:00:00, H
```

```
CORE1-R1#show ip igmp membership
Flags: A - aggregate, T - tracked
L - Local, S - static, V - virtual, R - Reported through v3
I - v3lite, U - Urd, M - SSM (S,G) channel
1,2,3 - The version of IGMP, the group is in

hannel/Group-Flags:
/ - Filtering entry (Exclude mode (S,G), Include mode (G))
Reporter:
<mac-or-ip-address> - last reporter if group is not explicitly tracked
<n>/<m> - <n> reporter in include mode, <m> reporter in exclude

Channel/Group Reporter Uptime Exp. Flags Interface
*,239.2.2.2 172.16.16.17 00:33:25 02:48 2A Vl16 !--- AP membership to CAPWAP multicast address.
*,224.0.1.40 10.63.84.1 1d01h 02:38 2LA Vl84
*,239.100.100.100 192.168.47.10 00:01:45 02:56 2A Vl47 !--- Wireless Client C1 to Stream
multicast address .
*,239.255.255.250 192.168.48.11 00:05:03 02:58 2A Vl48
*,239.255.255.250 10.63.85.163 21:19:25 02:40 2A Vl84
```

Sie können den Befehl **show ip mroute count** um sicherzustellen, dass Multicast-Routing ordnungsgemäß funktioniert:

```
CORE1-R1#show ip mroute count
IP Multicast Statistics
10 routes using 5448 bytes of memory
6 groups, 0.66 average sources per group
Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kilobits per second
Other counts: Total/RPF failed/Other drops(OIF-null, rate-limit etc)

Group: 239.255.255.250, Source count: 0, Packets forwarded: 0, Packets received: 0

Group: 239.100.100.100, Source count: 1, Packets forwarded: 1351, Packets received: 1491
Source: 192.168.48.11/32, Forwarding: 1351/14/1338/151, Other: 1491/0/140

Group: 224.0.1.40, Source count: 0, Packets forwarded: 0, Packets received: 0

Group: 239.2.2.2, Source count: 1, Packets forwarded: 3714, Packets received: 3726
Source: 10.63.84.48/32, Forwarding: 3714/28/551/163, Other: 3726/0/12
```

Anhand dieser Ausgaben können Sie erkennen, dass Multicast-Datenverkehr von der Quelle W1 stammt und von den Gruppenmitgliedern empfangen wird.

Zugehörige Informationen

- Enterprise Mobility 8.5 - Designleitfaden
- Konfigurationsbeispiel für VLANs auf einem Wireless LAN Controller
- Wireless LAN-Controller und Lightweight Access Point - Konfigurationsbeispiel
- IP-Multicast: Whitepaper
- Technischer Support und Dokumentation für Cisco Systeme

Informationen zu dieser Übersetzung

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