

Probleme mit der ARP- oder CAM-Tabelle für Catalyst 6500/600-Switches

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konventionen](#)

[Hintergrundinformationen](#)

[Fehlerbehebung bei ARP- oder CAM-Problemen](#)

[Verlust dynamischer MAC-Adressen mit verteiltem Switching](#)

[CEF verwirft Pakete in regelmäßigen Abständen](#)

[All-Zero-MAC-Adressen für den Switch-Filter aus der CAM-Tabelle](#)

[Unicast Flooding im Netzwerk alle 5 Minuten](#)

[ARP-Probleme in Hybrid CatOS](#)

[Fehler EARL-2-EARL4LOOKUPRAMERROR während der CAM-Tabellensuche](#)

[Statische CAM-Einträge nach dem Switchover des Supervisors verloren](#)

[%ACL-5-TCAMFULL: Die TCAM-Tabelle der ACL-Engine ist vollständig.](#)

[Ping-Probleme treten auf, wenn die MSFC nicht auf die ARP-Anfrage bei Catalyst Switches der Serie 6500 reagiert.](#)

[Mehrere Einträge in der MAC-Adresstabelle](#)

[Die vom Microsoft Load Balancing verwendete virtuelle IP-Adresse ist nicht erreichbar.](#)

[Zugehörige Informationen](#)

[Einführung](#)

Dieses Dokument enthält Informationen zur Fehlerbehebung bei Tabellenproblemen mit dem Address Resolution Protocol (ARP) oder dem Content Addressable Memory (CAM) für Catalyst 6500/6000-Switches.

[Voraussetzungen](#)

[Anforderungen](#)

Für dieses Dokument bestehen keine speziellen Anforderungen.

[Verwendete Komponenten](#)

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

Konventionen

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

Hintergrundinformationen

Catalyst Switches verwalten mehrere Tabellen, die auf Layer-2-Switching oder Multilayer Switching (MLS) zugeschnitten sind und in sehr schnellem Speicher verbleiben, sodass viele Felder innerhalb eines Frames oder Pakets parallel verglichen werden können.

- **ARP**: Ordnet eine IP-Adresse einer MAC-Adresse zu, um eine IP-Kommunikation innerhalb einer Broadcast-Domäne von Layer 2 bereitzustellen. Host B möchte beispielsweise Informationen an Host A senden, hat jedoch nicht die MAC-Adresse von Host A im ARP-Cache. Host B generiert eine Broadcast-Nachricht für alle Hosts in der Broadcast-Domäne, um die MAC-Adresse abzurufen, die der IP-Adresse von Host A zugeordnet ist. Alle Hosts in der Broadcast-Domäne erhalten die ARP-Anforderung, und nur Host A antwortet mit seiner MAC-Adresse.
- **CAM** - Alle Catalyst Switch-Modelle verwenden eine CAM-Tabelle für Layer-2-Switching. Wenn Frames an Switch-Ports eingehen, werden die Quell-MAC-Adressen erfasst und in der CAM-Tabelle erfasst. Der Ankunftshafen und das VLAN werden zusammen mit einem Zeitstempel in der Tabelle aufgezeichnet. Wenn eine MAC-Adresse, die an einem Switch-Port erfasst wurde, an einen anderen Port verschoben wurde, werden die MAC-Adresse und der Zeitstempel für den letzten Ankunftsport aufgezeichnet. Anschließend wird der vorherige Eintrag gelöscht. Wenn eine MAC-Adresse bereits in der Tabelle für den richtigen Ankunftsport vorhanden ist, wird nur der Zeitstempel aktualisiert.
- **Ternary Content Addressable Memory (TCAM)** - In Multilayer-Switches werden alle Prozesse, die Zugriffskontrolllisten (ACLs) im herkömmlichen Routing bereitstellen, wie z. B. Abgleich, Filterung oder Steuerung von spezifischem Datenverkehr, in der Hardware implementiert. TCAM ermöglicht die Auswertung eines Pakets anhand einer vollständigen Zugriffsliste in einer einzigen Tabellensuche. Die meisten Switches verfügen über mehrere TCAMs, sodass sowohl die ein- als auch die ausgehende Sicherheit als auch QoS-ACLs gleichzeitig oder vollständig parallel zu einer Weiterleitungsentscheidung auf Layer 2 oder Layer 3 bewertet werden können.

Fehlerbehebung bei ARP- oder CAM-Problemen

Verlust dynamischer MAC-Adressen mit verteiltem Switching

Bei verteilten Switches ist jede Distributed Feature Card (DFC) für die Pflege jeder eigenen CAM-Tabelle verantwortlich. Das bedeutet, dass jede DFC die MAC-Adresse erfasst und altert. Dies hängt von der CAM-Alterung und dem Datenverkehr ab, der mit diesem Eintrag übereinstimmt. Bei verteiltem Switching sieht die Supervisor Engine normalerweise eine Weile keinen Datenverkehr für eine bestimmte MAC-Adresse, sodass der Eintrag abläuft. Derzeit stehen zwei Mechanismen zur Verfügung, um die CAM-Tabellen zwischen den verschiedenen Engines konsistent zu halten, z. B. DFC (in Leitungsmodulen vorhanden) und Policy Feature Card (PFC) (in Supervisor-Modulen vorhanden):

- Flood to Fabric (FF)
- MAC-Benachrichtigung (MN)

Wenn ein MAC-Adresseneintrag im PFC ausgewiesen wird, zeigt der Befehl **show mac-address <MAC_Address> all** den Befehl DFC oder PFC an, der diese MAC-Adresse enthält.

Um zu verhindern, dass ein Eintrag in einer DFC- oder PFC-Adresse veraltet wird, aktivieren Sie die Synchronisierung der MAC-Adresse, selbst wenn kein Datenverkehr für diese MAC-Adresse vorliegt. Führen Sie die folgenden Befehle aus, um die Synchronisierung zu aktivieren:

```
!--- This is a global configuration command and is used to enable the synchronization. Cat6K-
IOS(config)#mac-address-table synchronize
```

```
!--- This is a privileged EXEC command and is used to clear dynamic MAC addresses. Cat6K-
IOS#clear mac-address-table dynamic
```

Der Befehl **MAC-Adresstabelle zur Synchronisierung** ist in den Cisco IOS® Software Releases 12.2(18)SXE4 und höher verfügbar. Nach der Aktivierung können Einträge angezeigt werden, die in PFC oder DFC nicht vorhanden sind. Das Modul kann es jedoch auch von anderen Benutzern lernen, die Ethernet Out of Band Channel (EOBC) verwenden.

Vorsicht: Der Befehl **"MAC-address-table synchronisieren"** löscht die gerouteten MAC-Einträge. Um dies zu vermeiden, deaktivieren Sie die geroutete MAC-Bereinigung mithilfe des globalen Konfigurationsbefehls **MAC-Adresstabelle aging-Time 0 routed-mac**.

CEF verwirft Pakete in regelmäßigen Abständen

Cisco Express Forwarding (CEF) ist eine Layer-3-IP-Switching-Technologie, die im Vergleich zu anderen Switching-Technologien eine überragende Leistung bietet, insbesondere in Netzwerken mit dynamischen Datenverkehrsmustern. CEF unterhält Datenstrukturen, die als Forwarding Information Base (FIB) und Adjacency-Tabellen bezeichnet werden. Die FIB-Tabelle spiegelt die Informationen in der Routing-Tabelle wider und wird für Weiterleitungsentscheidungen verwendet. Die Adjacency-Tabelle enthält den vorberechneten Link-Layer-Header für Next-Hop-Geräte. Auf Basis der nächsten Hop-Schnittstelle werden die Einträge in der FIB-Tabelle den Einträgen in der Adjacency-Tabelle zugeordnet. Ein Gerät kann CEF-Switch-Pakete nicht ausführen, wenn die Adjacency-Tabelle nicht mit den erforderlichen Informationen gefüllt wird.

Wenn CEF in regelmäßigen Abständen Pakete verwirft, die in Abständen voneinander liegen, die von normalen Betriebszeiten abweichen, ist dies vermutlich darauf zurückzuführen, dass die Adjacency-Tabelle regelmäßig gelöscht wird. Dies wird durch die Überalterung des ARP-Eintrags verursacht. Pakete werden für die Dauer, in der die Adjacency-Tabelle mit den erforderlichen Next-Hop-Informationen repliziert wird, nicht geschwächt. Während ARP-Einträge standardmäßig alle vier Stunden aktualisiert werden, beeinträchtigt die Konfiguration eines sehr kleinen ARP-Timeouts den CEF-Betrieb.

Geben Sie den Befehl [arp timeout im Schnittstellenkonfigurationsmodus aus, um die Zeit zu ändern, in der ein Eintrag im ARP-Cache verbleibt](#).

Weitere Informationen zu dieser Schwachstelle finden Sie unter Cisco Bug ID [CSCeb53542](#) (nur [registrierte](#) Kunden). Weitere Informationen zur [CEF-Adjacency](#) finden Sie unter [Troubleshooting](#)

[Incomplete Adjacencies with CEF](#) ([Fehlerbehebung bei unvollständigen Adjacencies mit CEF](#)).

All-Zero-MAC-Adressen für den Switch-Filter aus der CAM-Tabelle

Der Switch filtert Frames mit einer Quell-MAC-Adresse von 00-00-00-00-00, die eine ungültige Quell-MAC-Adresse aus der CAM-Tabelle darstellt. Dies ist ein Beispiel für die Syslog-Fehlerausgabe, wenn dies auftritt:

```
%SYS-4-P2_WARN: 1/Filtering MAC address 00-00-00-00-00-00 on port 2/48 from host table
```

Diese Meldungen enthalten Informationen und weisen darauf hin, dass ein Frame mit der Quell-MAC-Adresse 00-00-00-00-00 gefunden wurde, und der Switch wird dies niemals zur CAM-Tabelle hinzufügen. Der Switch leitet jedoch Datenverkehr, der von einer MAC-Adresse ohne MAC stammt, weiter.

Die Problemumgehung besteht darin, die Endstation zu identifizieren, die Frames mit einer rein Zero-Source-MAC-Adresse erzeugt. In der Regel überträgt eines dieser Geräte solche Frames:

- Ein Datenverkehrsgenerator, z. B. Spirent SmartBits
- Bestimmte Servertypen, z. B. IBM WebSphere-Server mit Lastenausgleich
- Ein falsch konfigurierter Router oder eine falsch konfigurierte Endstation, z. B. ein Gerät, das alle Nullen-Broadcasts überträgt
- Eine fehlerhafte Netzwerkkarte

Unicast Flooding im Netzwerk alle 5 Minuten

LAN-Switches verwenden Weiterleitungstabellen, z. B. Layer 2- und CAM-Tabellen, um Datenverkehr an bestimmte Ports weiterzuleiten, die auf der VLAN-Nummer und der MAC-Zieladresse des Frames basieren. Wenn kein Eintrag vorhanden ist, der der MAC-Zieladresse des Frames im eingehenden VLAN entspricht, wird der (Unicast-) Frame an alle Weiterleitungsporens innerhalb des entsprechenden VLAN gesendet. Das verursacht Überschwemmungen. Die eigentliche Ursache für Überflutungen ist, dass sich die MAC-Zieladresse des Pakets nicht in der Layer-2-Weiterleitungstabelle des Switches befindet. In diesem Fall wird das Paket von allen Weiterleitungsporens im VLAN außer dem Port, an dem es empfangen wird, überflutet.

Die Standardverweilzeit der ARP-Tabelle beträgt 4 Stunden, während der CAM die Einträge nur 5 Minuten lang aufbewahrt. Der Switch sendet einen Frame an alle Weiterleitungsporens im jeweiligen VLAN, wenn die MAC-Zieladresse aus der CAM-Tabelle herausgegeben wird. Sie benötigen einen CAM-Alterungs-Timer, der größer oder gleich dem ARP-Timeout ist, um Unicast-Flooding zu verhindern. Als Problemumgehung können Sie einen der folgenden Befehle ausgeben, um den CAM-Alterungs-Timer für das VLAN zu erhöhen, bei dem Sie Probleme haben, um die ARP-Alterungszeit anzupassen:

- Führen Sie für CatOS den [Befehl set cam agingtime aus](#).
- Geben Sie für die Cisco IOS-Software den [Befehl MAC-Adresstabelle zur Alterungszeit ein](#).

Hinweis: In jeder Catalyst-Umgebung, die ein Hot Standby Router Protocol (HSRP) ausführt, wird empfohlen, die CAM- und ARP-Timer zu synchronisieren.

Informationen zu möglichen Ursachen und Auswirkungen von Unicast-Paketfluten in Switched Networks finden Sie unter [Unicast Flooding in Switched Campus Networks](#).

ARP-Probleme in Hybrid CatOS

Im Hybrid-Modus wird CatOS von der Supervisor Engine ausgeführt, und die Multilayer Switch Feature Card (MSFC) führt Cisco IOS aus. CatOS wird auf Layer 2 betrieben und erstellt die CAM-Adresstabelle, um Informationen über VLAN, MAC-Adresse und Portnummer zu speichern. Cisco IOS in MSFC wird in Layer 3 betrieben und erstellt die ARP-Tabelle, um die IP-Adresse in die MAC-Adressauflösung aufzunehmen. Wenn Sie die IP-Adresse eines Geräts (z. B. eines Druckers oder eines Servers) ändern, können Sie möglicherweise kein Ping an die neue IP-Adresse senden. Sie können die neue IP-Adresse jedoch vom gleichen VLAN aus pingen. Dies kann ein ARP-Problem bei der MSFC sein.

Diese Problemumgehung kann helfen, das Problem zu isolieren und zu beheben:

1. Löschen Sie die ARP-Tabelle auf der MSFC.

```
MSFC2#clear arp int vlan 40
```

2. Überprüfen Sie den ARP-Timeoutwert. Der Standardwert ist 4 Stunden. Wenn das ARP-Timeout im VLAN hoch ist, können Sie den Timeout-Wert auf den Standardwert oder den optimalen Wert zurücksetzen.

```
MSFC2#show int vlan 40
```

```
Vlan40 is up, line protocol is up
  Hardware is Cat6k RP Virtual Ethernet, address is 00d0.0050.33fc (bia 00d0.0050.33fc)
```

```
  Internet address is 40.40.40.3/24
```

```
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
```

```
    reliability 255/255, txload 1/255, rxload 1/255
```

```
  Encapsulation ARPA, loopback not set
```

```
  Keepalive not supported
```

```
  ARP type: ARPA, ARP Timeout 04:00:00
```

```
  Last input 00:00:00, output 00:01:44, output hang never
```

```
  Last clearing of "show interface" counters never
```

```
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
```

```
MSFC2#conf t
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
MSFC2(config)#int vlan 40
```

```
MSFC2(config-if)#arp timeout ?
```

```
<0-2147483> Seconds
```

```
MSFC2(config-if)#arp timeout 240
```

3. Laden Sie die MSFC neu.

```
MSFC2#write memory
```

```
Building configuration...
```

```
[OK]
```

```
MSFC2#reload
```

```
Proceed with reload? [confirm]
```

```
Supervisor> (enable)
```

Fehler EARL-2-EARL4LOOKUPRAMERROR während der CAM-Tabellensuche

Dies ist ein Beispiel für die Ausgabe eines Syslog-Fehlers, wenn Sie dieses Problem haben:

```
%EARL-2-EARL4LOOKUPRAMERROR:Address eac6, data 0-0-8000-0, count 8
```

Dies wird angezeigt, wenn Sie eine CAM-Tabellensuche durchführen. Dies ist auf einen

Paritätsfehler zurückzuführen, wenn Sie auf den Speicher zugreifen. Dieser Fehler wird in der Regel dann generiert, wenn Sie den [Befehl show cam ausführen, um auf die CAM-Tabelle zuzugreifen](#). In einigen Fällen wird der Switch auch zurückgesetzt, wenn der Befehl **show cam** ausgegeben wird.

```
%EARL-2-EARLLOOKUPRAMERROR: Address [hex], data [hex]-[hex]-[hex]-[hex], count [dec]
```

Diese Fehlermeldung weist darauf hin, dass ein Paritätsfehler bei der RAM-Suche erkannt wurde. Das address [hex]-Feld ist die Adresse in der Weiterleitungstabelle, an der der Fehler entdeckt wurde. Das Feld data [hex]-[hex]-[hex]-[hex] ist das Wort0, Wort1, Wort2 und Wort3 von RAM-Daten, das den Paritätsfehler generiert hat. Das count [dec]-Feld ist die Gesamtzahl der Paritätsfehler.

Diese Meldung ist nicht katastrophal und kann nicht zu Ausfällen führen, wenn Sie nur einzelne Vorkommen davon haben. Wenn Sie diese Meldung permanent erhalten, weist dies darauf hin, dass der Switch versucht, in einen fehlerhaften DRAM-Sektor zu schreiben, wenn er der CAM-Tabelle einen neuen Eintrag hinzufügt. Anschließend müssen Sie das DRAM oder den Supervisor selbst ersetzen.

[Statische CAM-Einträge nach dem Switchover des Supervisors verloren](#)

Statische CAM-Einträge, die auf der aktiven Supervisor Engine konfiguriert sind, gehen nach einem schnellen Switchover verloren. Um dieses Problem zu umgehen, müssen Sie die CAM-Einträge nach einem schnellen Switchover neu konfigurieren.

Weitere Informationen zu dieser Schwachstelle finden Sie in den Cisco Bug-IDs [CSCed87627](#) (nur [registrierte](#) Kunden) und [CSCee2795](#) (nur [registrierte](#) Kunden).

[%ACL-5-TCAMFULL: Die TCAM-Tabelle der ACL-Engine ist vollständig.](#)

Wenn der TCAM vollständig ist und Sie versuchen, vorhandene ACLs oder Zugriffssteuerungseinträge (ACEs) zu Zugriffskontrolllisten hinzuzufügen, schlägt der Commit- oder Zuordnungsvorgang fehl. Alle vorherigen Konfigurationen bleiben in Kraft. Bei RACLs (Router Access Control Lists) wird die ACL in Software auf der Multilayer Switch Feature Card (MSFC) mit der entsprechenden Leistungseinbuße durchgesetzt.

Wenn Sie auf einem Switch, auf dem Hybrid-Software ausgeführt wird, eine Virtual Local Area Network Access Control List (VACL) oder QoS ACL ACEs konfigurieren, die die Muster- oder Maskenkapazität des TCAM überschreiten, wird eine ähnliche Syslog-Meldung an die Konsole ausgegeben:

```
%ACL-5-TCAMFULL: acl engine TCAM table is full
```

Auf Supervisor IOS-Systemen oder auf MSFC in einem Hybridsystem, wenn Sie RACL-ACEs konfigurieren, die die Kapazität des TCAM übersteigen, wird eine Syslog-Meldung ähnlich der folgenden auf der Konsole ausgegeben:

```
%FM-4-TCAM_ENTRY: Hardware TCAM entry capacity exceeded
```

Führen Sie auf Supervisor IOS-Systemen oder auf der MSFC in einem Hybridsystem den Befehl **show fm summary** aus, um zu sehen, welche Schnittstellen ACLs in der Hardware (ACTIVE) erzwingen und welche Schnittstellen ACLs in der Software (INACTIVE) erzwingen.

Die Lösung für dieses Problem besteht darin, die nicht verwendete ACL oder QoS aus der Switch-Konfiguration zu entfernen. Weitere Informationen finden Sie unter [Informationen zu ACL auf Catalyst Switches der Serie 6500](#).

[Ping-Probleme treten auf, wenn die MSFC nicht auf die ARP-Anfrage bei Catalyst Switches der Serie 6500 reagiert.](#)

Beim Pingen einer VLAN-Schnittstelle wird eine ARP-Anforderung mit einer Quell-IP dieses VLAN an den Standard-Router (MSFC) gesendet, der Router reagiert jedoch nicht auf die ARP-Anforderung, und das Debug-ARP zeigt folgende Fehlermeldung an:

```
IP ARP req filtered src [ip-address] [mac-address] dst [ip-address]
[mac-address] wrong cable, interface-id
```

Für jedes ARP-Datagramm wird eine ARP-Antwort verworfen, wenn die Ziel-IP-Adresse nicht mit der lokalen Host-Adresse übereinstimmt. Eine ARP-Anfrage wird verworfen, wenn sich die Quell-IP-Adresse nicht im gleichen Subnetz befindet. Es ist wünschenswert, dass dieser Test durch einen Konfigurationsparameter überschrieben wird, um die seltenen Fälle zu unterstützen, in denen mehrere Subnetze auf demselben Kabel vorhanden sein können.

Eine ARP-Antwort wird nur generiert, wenn die IP-Adresse des Zielprotokolls vom lokalen Host erreichbar ist, wie vom Routing-Algorithmus bestimmt, und der nächste Hop nicht über dieselbe Schnittstelle erfolgt. Wenn der lokale Host als Gateway fungiert, kann dies zu ARP-Antworten für Ziele führen, die sich nicht im gleichen Subnetz befinden. Dies zeigt, dass das Verwerfen der ARP-Anfrage gerechtfertigt ist.

Dies kann behoben werden, indem der Catalyst 6500 nicht auf alle ARP-Anfragen reagiert, da sich die Quell-IP-Adresse in der ARP-Anfrage in einem anderen Subnetz befindet als die Ziel-IP-Adresse im ARP. Daher kommt der MSFC/Router zu dem Schluss, dass die ARP nicht in derselben Layer-2-Domäne verbleibt und den falschen Kabeltyp anzeigt. Mit anderen Worten, die falsche Kabeldebugmeldung wird generiert, wenn die Quelle und das Ziel des ARP nicht derselben Layer-2-Domäne angehören. Damit ARP in diesem Szenario funktioniert, muss die IP-Zielprotokoll-Adresse unter Verwendung der statischen Route als Problemumgehung erreichbar sein.

[Mehrere Einträge in der MAC-Adresstabelle](#)

In der MAC-Adresstabelle werden zwei Einträge für die MAC-Adresse angezeigt.

```
Cat6K#show mac-address-table int gi 6/11
Displaying entries from Line card 6:
```

```
Legend: * - primary entry
         age - seconds since last seen
         n/a - not available
```

vlan	mac address	type	learn	age	ports
-----+-----+-----+-----+-----+-----					
[FE 1]:					
* 100	0011.857c.4d10	dynamic	Yes	0	Gi6/11
[FE 2]:					
* 100	0011.857c.4d10	dynamic	Yes	95	Gi6/11

Cat6K#show module 6

```
Mod Ports Card Type                               Model                               Serial No.
-----
 6   48  CEF720 48 port 10/100/1000mb Ethernet WS-X6748-GE-TX SADxxxxxxxx

Mod MAC addresses                               Hw   Fw           Sw           Status
-----
 6   001d.45fd.xx4a to 001d.45fd.xx79  2.6  12.2(14r)S5  12.2(18)SXF8 Ok

Mod Sub-Module                               Model                               Serial           Hw   Status
-----
 6   Distributed Forwarding Card WS-F6700-DFC3B  SALxxxxxxxxx  4.6  Ok

Mod Online Diag Status
-----
 6   Pass
```

In der DFC-Umgebung gibt es zwei Engines für die Layer-2-Weiterleitungssuche. In der dCEF-Umgebung erhalten FE1 und FE2 häufig dieselbe MAC-Adresse auf demselben Port auf Line Cards der Architektur CEF720/dCEF720.

[Die vom Microsoft Load Balancing verwendete virtuelle IP-Adresse ist nicht erreichbar.](#)

Für Cisco Router ist für jede virtuelle IP-Adresse ein ARP-Eintrag (Address Resolution Protocol) erforderlich. Beim Netzwerk-Lastenausgleich wird Level-2-Multicast für die Paketübermittlung verwendet. Bei der RFC-Implementierung von Cisco wird Multicast nur für IP-Multicast verwendet. Wenn der Router keine Multicast-IP-Adresse anzeigt, wird daher kein automatisch erstellter ARP-Eintrag erstellt, und Sie müssen diesen dem Router manuell hinzufügen.

In der Regel legen Cisco Geräte keine Multicast-MAC-Adresse (virtuelle MAC-Adresse des Clusters) in die ARP-Tabelle, wenn sie durch eine Unicast-IP-Adresse (virtuelle Adresse des Clusters) aufgelöst wurde. Um dieses Problem zu beheben, benötigen Sie eine statische Zuordnung der virtuellen Unicast-IP-Adresse zur Multicast-MAC-Adresse.

Weitere Informationen finden Sie im [Multicast-Modus](#) im Abschnitt *Catalyst Switches for Microsoft Network Load Balancing Configuration Example*.

[Zugehörige Informationen](#)

- [Fehlerbehebung bei unvollständigen Adjacencies mit CEF](#)
- [Unicast Flooding in Switched Campus-Netzwerken](#)
- [LAN-Produktunterstützung](#)
- [Unterstützung der LAN Switching-Technologie](#)
- [Technischer Support und Dokumentation - Cisco Systems](#)