Fehlerbehebung bei LISP VXLAN Fabric auf Catalyst Switches der Serie 9000

Inhalt

Einleitung

In diesem Dokument werden die grundlegenden Komponenten einer VXLAN-basierten LISP-Fabric und deren Betrieb beschrieben.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

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

- Catalyst 9300
- Catalyst 9400
- Catalyst 9500
- Cisco IOS XE 17.9.3 oder spätere Version

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 kennen.

Hintergrundinformationen

LISP VXLAN-basierte Struktur

Der Zweck der Bereitstellung eines LISP VXLAN-Netzwerks besteht darin, eine Architektur erstellen zu können, in der mehrere Overlay-Netzwerke, auch Virtual Networks genannt, auf einem Underlay-Netzwerk definiert werden.

- Das Underlay-Netzwerk würde in einer solchen Topologie primär als Transportschicht fungieren und wüsste nicht, welche Overlay-Topologien darüber betrieben werden.
- Overlay-Netzwerke können ohne Beeinträchtigung des Underlay-Netzwerks hinzugefügt und entfernt werden.
- Durch den Einsatz von Overlay-Netzwerken werden die Benutzer effektiv vom Underlay-Netzwerk getrennt.

Technologien für den Aufbau einer LISP-VXLAN-Struktur

Locator Identity Separation Protocol (LISP)

- Das LISP-Protokoll ist das innerhalb der Fabric verwendete Kontrollebenenprotokoll. Sie wird auf allen Fabric-Geräten ausgeführt, um die Fabric zu erstellen und zu steuern, wie der Datenverkehr durch die Fabric gesendet wird.
- LISP erstellt 2 Adressräume. Eine ist für die Routing Locator (RLOCs) vorgesehen, mit denen die Erreichbarkeit angekündigt wird. Der andere Adressbereich ist für die Endpoint Identifiers (EIDs) vorgesehen, d. h. für Endpoints, die sich im Overlay befinden und für

dieses verwendet werden.
- Innerhalb von LISP werden die EIDs mit einem angekündigten RLOC angekündigt. Wenn eine EID nur den zugehörigen Routing Locator aktualisiert, muss diese nur verschoben werden.
- Um einen Endpunkt mit LISP-Datenverkehr zu einer EID zu erreichen, muss dieser gekapselt und in das RLOC getunnelt werden, das ihn entkapselt und an den Endpunkt weiterleitet.

Gruppenbasierte Richtlinien

- Dabei werden Richtlinien verwendet, die eine Segmentierung innerhalb einer Fabric-Gruppe ermöglichen.
- Wenn gruppenbasierte Richtlinien bereitgestellt werden, wird der Datenverkehr mit der sicheren Gruppe klassifiziert, anstatt auf der Quell-/Ziel-IP-Adresse zu basieren.
- Dadurch wird die Komplexität komplexer Zugriffskontrolllisten verringert. Anstelle von Listen mit IP-Adressen, die verwaltet werden müssen, werden IP-Adressen/Subnetze einem Secure Group Tag zugewiesen.
- Beim Eingang in die Fabric wird ein SGT getaggt, wenn der Datenverkehr die Fabric verlässt, und das Ziel des Frames wird nach seinem SGT gesucht.
- Mithilfe einer Matrix werden das Quell- und Ziel-SGT abgeglichen, und eine ACL für sichere Gruppen wird angewendet, um den Datenverkehr durchzusetzen, wenn er die Fabric verlässt.

VXLAN-Kapselung

- Innerhalb des Fabric wird VXLAN zur Kapselung des gesamten Datenverkehrs verwendet
- Der Vorteil von VXLAN gegenüber der früheren LISP-Kapselung besteht darin, dass der gesamte Layer-2-Frame und nicht nur der Layer-3-Frame gekapselt werden kann. Wenn der gesamte Frame gekapselt wird, können Overlays sowohl Layer 2 als auch Layer 3 sein.
- VXLAN nutzt UDP mit Zielport 4789. Dadurch können LISP VXLAN-Frames auch durch Geräte transportiert werden, die die Overlay-Topologie nicht kennen.
- Da VXLAN den gesamten Frame kapselt, muss die MTU erhöht werden, damit beim Senden von Datenverkehr zwischen RLOCs keine Fragmentierung erforderlich ist. Alle zwischengeschalteten Geräte müssen eine größere MTU unterstützen, um die gekapselten Frames zu transportieren.

Authentifizierung

- Um Endpunkte ihren jeweiligen Ressourcen zuweisen zu können, kann die Authentifizierung verwendet werden.
- Mithilfe von Protokollen wie 802.1x können MAB- und Webauth-Endpunkte authentifiziert und/oder anhand eines Radius-Servers in ein Profil eingebunden werden, um ihnen auf Grundlage ihrer Autorisierungsprofile Zugriff auf das Netzwerk zu gewähren.
- Mit ihren jeweiligen Radius-Attributen können Endpunkte ihrem jeweiligen VLAN, SGT und allen anderen Attributen zugewiesen werden, um einen Endpunkt-/Benutzer-Netzwerkzugriff zu ermöglichen.

Schlüsselkomponenten der LISP-VXLAN-Struktur

Knoten der Kontrollebene

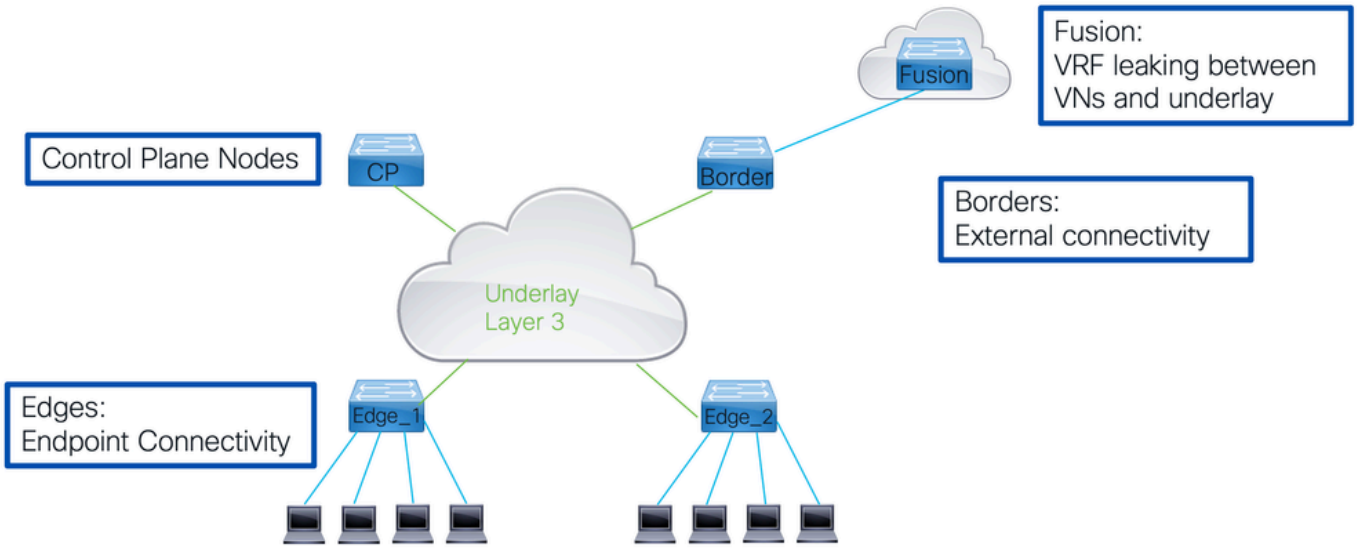
- enthält die Funktionen LISP Map Server und Map Resolver.
- Alle anderen Fabric-Geräte fragen den Standort der EID im Control Plane-Knoten ab und senden die Registrierungen für die EID an die Control Plane-Knoten.
- Dadurch erhalten die Control Plane-Knoten eine vollständige Übersicht über die Fabric und sehen, hinter welchem RLOC sich die verschiedenen EIDs befinden.

Randknoten

- Bietet Verbindungen außerhalb der Fabric entweder zu anderen Fabrics oder zur Außenwelt.
- Interne Grenzen importieren Routen in die Fabric und registrieren sie bei den Kontrollebenen-Knoten.
- Externe Grenzen stellen eine Verbindung mit der Außenwelt her und stellen einen Standardpfad außerhalb der Fabric für unbekannte IP-Ziele bereit.

Edge-Knoten

- Diese Knoten bieten Verbindungen zu Endpunkten innerhalb der Fabric.
- In der Definition von LISP sind dies XTRs, da sie sowohl die Funktion eines Eingangstunnel-Routers (ITR) als auch eines Ausgangstunnel-Routers (ETR) ausführen.



Knoten können nicht nur eine Aufgabe ausführen.

- Sie können eine Kombination oder sogar alle Funktionen innerhalb des Fabric ausführen.
- Wenn sich ein Grenzknoten und ein Knoten auf der Kontrollebene auf einem Gerät befinden, werden sie als angeordnet bezeichnet.
- Wenn dieser Knoten auch die Edge-Funktion bereitstellt, wird er als Fabric In A Box (FIAB)

bezeichnet.

Grenzen ermöglichen Übergaben an das übrige Netzwerk mithilfe von VRF Lite.

- Jedes Overlay oder virtuelle Netzwerk ist mit einer VRF-Instanz auf dem Grenzknoten verknüpft.
- Um diese verschiedenen VRFs miteinander zu verbinden, wird ein Fusion-Router verwendet. Dieser Fusion-Router ist nicht Teil des Fabric selbst, ist jedoch für den Betrieb der Overlay-Netzwerke mit dem Fabric entscheidend.

Ein weiteres wichtiges Konzept innerhalb einer LISP VXLAN-Fabric ist die Verwendung von IP Anycast.

- Das bedeutet, dass auf allen Edge-Geräten die IP-Adresse und die zugehörigen MAC-Adressen für die Switched Virtual Interfaces (SVI) repliziert werden.
- Jeder Edge hat in der SVI die gleiche Konfiguration in Bezug auf IPv4-, IPv6- und MAC-Adressen.
- Die Fehlerbehebung bringt einige Herausforderungen mit sich.
    - Um die Erreichbarkeit mit Ping zu testen, kann mit lokal verbundenen Geräten gearbeitet werden.
    - Remote-Ziele über die LISP VXLAN-Fabric zu erreichen, gibt keine Antwort zurück, da das Gerät, das eine Antwort sendet, dies ebenfalls an die Anycast-IP-Adresse sendet, die an das lokale Fabric-Gerät gesendet wird, das nicht weiß, welcher andere Fabric-Knoten den ursprünglichen Ping gesendet hat.

Endgeräteregistrierung

Damit eine LISP VXLAN-Fabric funktioniert, ist es wichtig, dass der Control Plane-Knoten weiß, wie alle Endpunkte über die Fabric erreichbar sind.

- Damit die Kontrollebene Informationen zu allen EIDs im Netzwerk erhält, müssen alle ihr bekannten EIDs von allen anderen Fabric-Geräten auf der Kontrollebene registriert werden.
- Ein Fabric-Knoten sendet LISP-Map-Register-Nachrichten an den Knoten der Kontrollebene. Zu den Informationen, die mit der Map-Register-Nachricht angekündigt werden.

Wichtige Informationen

LISP-Instanzkennung:

- Diese Kennung wird durch die Fabric übertragen und gibt an, welches virtuelle Netzwerk verwendet werden soll.
- In einer LISP VXLAN-Fabric pro Layer-3-Overlay wird eine Instanz pro verwendetem VLAN in der Fabric verwendet. Es gibt auch eine Layer-2-Instanz.

Endpunkt identifiziert (EID):

- Wenn es sich um eine Layer-2- oder Layer-3-Instanz handelt, handelt es sich um die MAC-Adresse, die IP-Hostroute (/32 oder /128) oder ein registriertes IP-Subnetz.

Routing Locator (RLOC):

- Dabei handelt es sich um die eigene IP-Adresse des Fabric-Knotens, mit der die Erreichbarkeit angekündigt wird, an die andere Fabric-Geräte gekapselten Datenverkehr senden, der die EID erreichen muss.

Proxy-Flag:

- Wenn dieses Flag festgelegt ist, kann der Steuerungsebenenknoten direkt auf Zuordnungsanforderungen von anderen Fabric-Knoten reagieren, ohne dass das Proxy-Flag alle Anforderungen für die Weiterleitung an den Fabric-Knoten festgelegt hat, der die EID registriert hat.

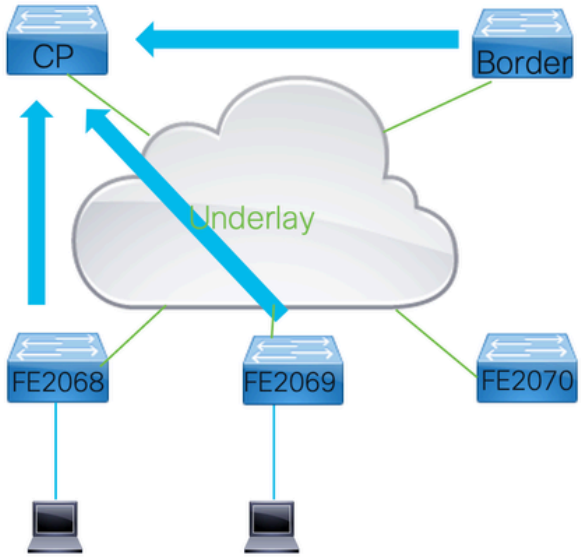
Registrierungsschritte

Schritt 1: Fabric-Geräte erhalten Informationen zu Endpunkt-IDs. Möglich ist dies über Konfigurationen, Routing-Protokolle oder über Informationen, die auf den Fabric-Geräten eingehen.

Schritt 2: Fabric-Geräte registrieren die ermittelten Endpunkte bei allen bekannten und erreichbaren Control Plane-Knoten im Fabric.

Schritt 3: Kontrollebenen-Knoten verwalten eine Tabelle der registrierten EIDs mit der zugehörigen Instanz-ID, dem RLOC und der erlernten EID.

Instance	RLOC	EID (mac address)
8189	FE2068	0019.3052.6d7f
8189	FE2069	0019.3052.6d7f
4099	FE2068	172.24.1.4/32
4099	FE2069	172.24.1.3/32
4099	Border	10.48.13.0/24



Überprüfung

1.1 MAC-Adresslernen

Bei Layer-2-Instanzen werden als EID die MAC-Adressen verwendet, die innerhalb des verknüpften VLAN gelernt werden. Fabric-Edges erlernen die Layer-2-Adressen mithilfe von Standardmethoden auf den Switches.

Suchen Sie nach dem VLAN, das einer bestimmten Layer-2-Instanz-ID zugeordnet ist. Die Konfiguration kann überprüft werden, oder verwenden Sie den folgenden Befehl:

Verwenden Sie "show lisp instance-id <instance> Ethernet"

```
<#root>

FE2068#

show lisp instance-id 8191 ethernet


  Instance ID:

8191


  Router-lisp ID:                         0
  Locator table:                          default
  EID table:

Vlan 150


  Ingress Tunnel Router (ITR):            enabled
  Egress Tunnel Router (ETR):             enabled
  ..
  Site Registration Limit:                0
  Map-Request source:                     derived from EID destination
  ITR Map-Resolver(s):                    172.30.250.19
  ETR Map-Server(s):                      172.30.250.19
```

Wie in der Ausgabe zu sehen ist, ist die Instanz-ID 8191 mit VLAN 150 verknüpft. Dies führt dazu, dass alle MAC-Adressen innerhalb des VLAN bei LISP registriert werden und Teil der LISP VXLAN-Struktur werden.

```
<#root>

FE2068#

show mac address-table vlan 150


          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

 150    0000.0c9f.f18e    STATIC      Vl150


 150    0050.5693.8930    DYNAMIC     Gi1/0/1


 150    2416.9db4.33fd    STATIC      Vl150
```

```
 150    0019.3052.6d7f    CP_LEARN    L2LI0

Total Mac Addresses for this criterion: 3
Total Mac Addresses installed by LISP: REMOTE: 1
```

Statische Einträge mit der Schnittstelle Vl150 sind die MAC-Adressen der Switch Virtual Interface (Schnittstelle VLAN 150).

- Diese MAC-Adressen sind nicht auf dem Steuerungsebenenknoten registriert, da sie auf allen Edge-Geräten identisch wären.
- Der angezeigte CP_LEARN-Eintrag sind Einträge, die über die Fabric erfasst werden. Für alle anderen Einträge, die dynamisch oder statisch sind, müssen sie auf dem Steuerungsebenenknoten registriert werden.

Sobald sie über ihre jeweiligen Mittel abgerufen werden, werden sie in den lisp-Datenbankausgaben angezeigt. Diese Ausgabe enthält alle lokalen Einträge auf diesem Fabric-Gerät.

<#root>

```
FE2068#

show lisp instance-id 8191 ethernet database


LISP ETR MAC Mapping Database for LISP 0 EID-table

Vlan 150 (IID 8191)

, LSBs: 0x1
Entries total 3, no-route 0, inactive 0, do-not-register 2

0000.0c9f.f18e/48

, dynamic-eid Auto-L2-group-8191,

do not register

, inherited from default locator-set rloc_hosts
  Uptime: 14:56:40, Last-change: 14:56:40
  Domain-ID: local
  Service-Insertion: N/A
  Locator        Pri/Wgt  Source     State


172.30.250.44

  10/10   cfg-intf   site-self, reachable

0050.5693.8930/48

, dynamic-eid Auto-L2-group-8191, inherited from default locator-set rloc_hosts
  Uptime: 14:03:06, Last-change: 14:03:06
  Domain-ID: local
  Service-Insertion: N/A
  Locator        Pri/Wgt  Source     State
```

```
172.30.250.44

  10/10   cfg-intf   site-self, reachable
2

416.9db4.33fd/48

, dynamic-eid Auto-L2-group-8191, do not register, inherited from default locator-set rloc_hosts
  Uptime: 14:56:50, Last-change: 14:56:50
  Domain-ID: local
  Service-Insertion: N/A
  Locator        Pri/Wgt  Source     State


172.30.250.44

   10/10   cfg-intf   site-self, reachable
```

Für alle bekannten lokalen MAC-Adressen in der Datenbank wird der Locator angezeigt.

- Dies ist der Locator, mit dem dieser Eintrag beim Control Plane Node registriert wird.
- Außerdem wurde der Status des Locators angegeben. Die 2 MAC-Adressen, die zur Switches-SVI gehörten, werden ebenfalls angezeigt, jedoch mit der Markierung "nicht registrieren", die eine Registrierung verhindert.
- Der Remote-Eintrag, der im Befehl show mac address table angezeigt wurde, ist keine lokale MAC-Adresse und wird daher nicht in der lisp-Datenbank angezeigt.

Für eine Layer-2-Instanz werden nicht nur die Layer-2-MAC-Adressen als EID gelernt, sondern es müssen auch Informationen zur Adressauflösung von ARP- und ND-Frames bezogen werden.

- Auf diese Weise kann die LISP VXLAN-Fabric diese Frames weiterleiten, wie sie normalerweise innerhalb des VLAN geflutet werden.
- Da eine Layer-2-Instanz-ID nicht immer die Möglichkeit hat, dorthin einen anderen Mechanismus zu fluten, der es Endpunkten ermöglichen würde, Adressenauflösungsinformationen für andere Endpunkte in derselben Instanz aufzulösen. Dazu lernen die Fabric-Geräte diese Informationen, die lokal durch die Geräteverfolgung erfasst werden, und registrieren sie.
- Diese wird dann auch bei den Kontrollebenen-Knoten registriert. Aufgrund von ND- oder ARP-Snooping werden diese Pakete an die CPU gesendet, um eine Anforderung an die Knoten auf der Kontrollebene auszulösen und festzustellen, ob eine bekannte MAC-Adresse vorhanden ist.
- Wenn eine positive Antwort eingeht, werden die ARP-/ND-Pakete neu geschrieben, sodass die MAC-Zieladresse von Broadcast- oder Multicast-Adresse in die Unicast-MAC-Adresse geändert wird.
- Dieses neu geschriebene Paket kann dann als Unicast-Frame über die LISP VXLAN-Fabric weitergeleitet werden.

Um die Informationen zur Adressenauflösung anzuzeigen, die auf dem Switch bekannt sind, kann der Befehl show device-tracking database verwendet werden.

- Hier werden alle Zuordnungen angezeigt, die von der Geräteverfolgung bekannt sind.
- Die Switch-eigenen IP-Adressen sind als L(Local) gekennzeichnet und müssen in der Geräteverfolgungsdatenbank vorhanden sein.

Remote-Einträge werden ebenfalls in dieser Ausgabe angezeigt.

- Da sie nach dem Snooping der ND- oder ARP-Anforderung aufgelöst werden, werden sie in die Geräteverfolgungsdatenbank mit der Link Layer-Adresse 0000.0000.00fd aufgenommen.
- Sobald sie aufgelöst sind, werden die Informationen zur aufgelösten MAC-Adresse und der Port zu Tu0 geändert.

Anzeigen der Geräteverfolgungsdatenbank

<#root>

```
FE2068#

show device-tracking database vlanid 150


vlanDB has 6 entries for vlan 150, 3 dynamic
Codes: L - Local, S - Static, ND - Neighbor Discovery, ARP - Address Resolution Protocol, DH4 - IPv4 DH
Preflevel flags (prlvl):
0001:MAC and LLA match     0002:Orig trunk            0004:Orig access
0008:Orig trusted trunk    0010:Orig trusted access   0020:DHCP assigned
0040:Cga authenticated     0080:Cert authenticated    0100:Statically assigned
    Network Layer Address                   Link Layer Address     Interface  vlan       prlvl      ag

ARP


172.24.1.3                                0050.5693.8930

        Gi1/0/1    150        0005       31s        REACHABLE  213 s try 0
RMT 172.24.1.4

0050.5693.3120

        Tu0    150        0005       51s        REACHABLE


API


172.24.1.99                               0000.0000.00fd

         Gi1/0/1    150        0000       5s         UNKNOWN   try 0 (25 s)
ND  FE80::1AE4:8804:5B8F:50F6               0050.5693.8930         Gi1/0/1    150        0005       12

ND


2001:DB8::E70B:E8E1:E368:BDB7             0050.5693.8930

         Gi1/0/1    150        0005       137s       REACHABLE  110 s try 0
L   172.24.1.254                            0000.0c9f.f18e         Vl150      150        0100       10
L   2001:DB8::1                             0000.0c9f.f18e         Vl150      150        0100       10
L   FE80::200:CFF:FE9F:F18E                 0000.0c9f.f18e         Vl150      150        0100       10
```

Zeigen Sie die lokal registrierten Zuordnungen mit dem Befehl "show lisp instance-id <Instanz> Ethernet-Datenbank address-resolution" an.

<#root>

```
FE2068#
show lisp instance-id 8191 ethernet database address-resolution

LISP ETR Address Resolution for LISP 0 EID-table Vlan 150 (IID 8191)
(*) -> entry being deleted
Hardware Address       L3 InstID Host Address
0000.0c9f.f18e              4099 FE80::200:CFF:FE9F:F18E/128

                            4099 2001:DB8::1/128

0050.5693.8930              4099 172.24.1.3/32

                            4099 2001:DB8::E70B:E8E1:E368:BDB7/128

                            4099 FE80::1AE4:8804:5B8F:50F6/128
```

1.2 Dynamische IP-Adressen - Lernen

Auf den Fabric-Geräten einer IP-Schicht wird ein virtuelles Netzwerk durch Zuordnen einer LISP-Instanz-ID zu einer VRF-Instanz gebildet.

- Diese VRF-Instanz wird dann unter den verschiedenen Switch Virtual Interfaces (SVI) konfiguriert und wird Teil des Layer 3 Overlay-Netzwerks
- In den meisten Fällen gehört diese SVI auch zu VLANs, die bei ihren jeweiligen Layer-2-Instanzen registriert sind.

Suchen Sie die Zuordnung zwischen VRF und LISP-Instanz-ID mit dem Befehl "show lisp instance-id <instance> ipv4".

<#root>

```
FE2068#
sh lisp instance-id 4099 ipv4

  Instance ID:                            4099
```

```
  Router-lisp ID:                       0
  Locator table:                        default
  EID table:                            vrf Fabric_VN_1

  Ingress Tunnel Router (ITR):          enabled
  Egress Tunnel Router (ETR):           enabled
  ..
  ITR Map-Resolver(s):                  172.30.250.19

  ETR Map-Server(s):                    172.30.250.19
```

Anmerkung: Dieser Befehl kann auch verwendet werden, um die verschiedenen Funktionen zu überprüfen, die für diese Instanz aktiviert werden könnten. Außerdem werden die verwendeten Kontrollebenenknoten in der LISP VXLAN-Struktur angezeigt.

Nachdem eine Layer-3-Instanz erstellt und mit einer VRF-Instanz verknüpft wurde, wird eine LISP 0 <Instanz-ID>-Schnittstelle erstellt, die in der aktuellen Konfiguration und unter "show vrf" angezeigt wird.

- Diese Schnittstelle muss NICHT manuell erstellt werden und muss in der Regel nicht konfiguriert werden (mit Ausnahme der Multicast-Konfiguration, wenn Underlay Multicast verwendet wird).

<#root>

```
FE2068#
show vrf Fabric_VN_1

  Name                              Default RD            Protocols   Interfaces

Fabric_VN_1

                    ipv4,ipv6
```

LI0.4099

Vl150

Vl151

Anders als bei Ethernet-Frames, bei denen alle MAC-Adressen in einem VLAN für IP verwendet werden, müssen IP-Adressen innerhalb eines dynamischen EID-Bereichs erfasst werden.

LISP-Instanz anzeigen

<#root>

FE2068#

sh lisp instance-id 4099 dynamic-eid

LISP Dynamic EID Information for router 0,

IID 4099, EID-table VRF "Fabric_VN_1"

Dynamic-EID name:

Fabric_VN_Subnet_1_IPv4

  Database-mapping EID-prefix: 172.24.1.0/24, locator-set rloc_hosts

  Registering more-specific dynamic-EIDs
  Map-Server(s): none configured, use global Map-Server
  Site-based multicast Map-Notify group: none configured

  Number of roaming dynamic-EIDs discovered: 2

  Last dynamic-EID discovered: 172.24.1.3, 21:17:45 ago

Dynamic-EID name: Fabric_VN_Subnet_1_IPv6

  Database-mapping EID-prefix: 2001:DB8::/64, locator-set rloc_hosts

  Registering more-specific dynamic-EIDs
  Map-Server(s): none configured, use global Map-Server

```
  Site-based multicast Map-Notify group: none configured
  Number of roaming dynamic-EIDs discovered: 2

  Last dynamic-EID discovered: 2001:DB8::E70B:E8E1:E368:BDB7, 21:17:44 ago


Dynamic-EID name: Fabric_VN_Subnet_2_IPv4

  Database-mapping EID-prefix: 172.24.2.0/24, locator-set rloc_hosts

  Registering more-specific dynamic-EIDs
  Map-Server(s): none configured, use global Map-Server
  Site-based multicast Map-Notify group: none configured
  Number of roaming dynamic-EIDs discovered: 2

  Last dynamic-EID discovered: 172.24.2.2, 21:55:56 ago
```

IP-Adressen außerhalb dieser definierten Bereiche gelten als nicht für die Fabric qualifiziert und werden nicht in die LISP-Datenbanken eingegeben und nicht bei den Knoten der Kontrollebene registriert.

```
<#root>

FE2068#
show lisp instance-id 4099 ipv4 database

LISP ETR IPv4 Mapping Database for LISP 0 EID-table vrf Fabric_VN_1 (IID 4099), LSBs: 0x1
Entries total 4, no-route 0, inactive 0, do-not-register 2

172.24.1.3/32, dynamic-eid Fabric_VN_Subnet_1_IPv4

, inherited from default locator-set rloc_hosts
  Uptime: 21:28:51, Last-change: 21:28:51
  Domain-ID: local
  Service-Insertion: N/A
  Locator        Pri/Wgt  Source     State

172.30.250.44

   10/10   cfg-intf   site-self, reachable

172.24.1.254/32, dynamic-eid Fabric_VN_Subnet_1_IPv4, do not register,

 inherited from default locator-set rloc_hosts
  Uptime: 22:22:35, Last-change: 22:22:35
  Domain-ID: local
  Service-Insertion: N/A
  Locator        Pri/Wgt  Source     State
```

172.30.250.44

10/10 cfg-intf site-self, reachable

172.24.2.2/32, dynamic-eid Fabric_VN_Subnet_2_IPv4

, inherited from default locator-set rloc_hosts
Uptime: 22:07:03, Last-change: 22:07:03
Domain-ID: local
Service-Insertion: N/A
Locator Pri/Wgt Source State

172.30.250.44

10/10 cfg-intf site-self, reachable

172.24.2.254/32, dynamic-eid Fabric_VN_Subnet_2_IPv4, do not register

, inherited from default locator-set rloc_hosts
Uptime: 22:22:35, Last-change: 22:22:35
Domain-ID: local
Service-Insertion: N/A
Locator Pri/Wgt Source State

172.30.250.44

10/10 cfg-intf site-self, reachable

Die Ausgabe zeigt alle lokal bekannten IP-Adressinformationen an.

- Bei Hosts sind dies in der Regel Host-Routen (/32 oder /128), sie können jedoch auch Subnetze sein, wenn diese in die LISP-Datenbank auf Basis des Grenzknotens importiert worden wären.
- Die IP-Adressen aus der SVI selbst werden als "nicht registrieren" markiert. Auf diese Weise wird vermieden, dass alle Fabric-Geräte die Anycast-IP-Adresse beim Control-Plane-Knoten registrieren.

<#root>

CP_BN_2071#

sh lisp instance-id 4099 ipv4 database

LISP ETR IPv4 Mapping Database for LISP 0 EID-table vrf Fabric_VN_1 (IID 4099), LSBs: 0x1
Entries total 2, no-route 0, inactive 0, do-not-register 0

0.0.0.0/0

, locator-set rloc_border, auto-discover-rlocs, default-ETR
Uptime: 2d17h, Last-change: 2d17h
Domain-ID: local
Metric: 0
Service-Insertion: N/A
Locator Pri/Wgt Source State

172.30.250.19

   10/10   cfg-intf   site-self, reachable

10.48.13.0/24, route-import

, inherited from default locator-set rloc_border, auto-discover-rlocs
  Uptime: 2d17h, Last-change: 2d16h
  Domain-ID: local, tag: 65101
  Service-Insertion: N/A
  Locator   Pri/Wgt Source   State

172.30.250.19

   10/10   cfg-intf   site-self, reachable

1.3 Registrierung der EID auf der Kontrollebene

Die Endpunktregistrierung in einer LISP VXLAN-basierten Struktur erfolgt über die zuverlässige LISP-Registrierung. Dies bedeutet, dass alle Registrierungen über eine eingerichtete TCP-Sitzung, die LISP-Sitzung, erfolgen. Von jedem Fabric-Gerät wird eine LISP-Sitzung mit jedem der Steuerungsebenenknoten in der Fabric eingerichtet. Bei dieser LISP-Sitzung werden alle Registrierungen durchgeführt. Wenn mehrere Control Plane-Knoten innerhalb einer Fabric vorhanden sind, müssen sie alle zur Registrierung von EIDs verwendet werden.

Der Status lautet "Down" (Abgeschaltet), wenn keine Registrierung auf dem Fabric-Gerät erforderlich ist, da dies in der Regel nur an Außengrenzen der Fall ist.
die keine IP-Bereiche beim Control Plane-Knoten oder auf Edge-Geräten ohne Endpunkte registrieren

Die Registrierung der EID erfolgt über LISP-Registrierungsnachrichten.
die an alle konfigurierten Kontrollebenen-Knoten gesendet werden.

Um die LISP-Sitzung auf einem Fabric-Gerät anzuzeigen, kann der Befehl show lisp session verwendet werden.
Es zeigt den Status der Sitzung und die Zeit, zu der sie verfügbar war.

<#root>

FE2068#

show lisp session

Sessions for VRF default, total: 1, established: 1
Peer   State   Up/Down   In/Out   Users

172.30.250.19:4342   **Up**

        22:06:07   9791/6531   10

Die als "Down" angezeigte LISP-Sitzung kann auf Geräten ausgeführt werden, die keine EID für die Registrierung beim Control Plane-Knoten aufweisen.
In der Regel handelt es sich dabei um Grenzknoten, die keine Routen in die Fabric- oder Edge-Geräte ohne verbundene Endpunkte importieren.

Detailliertere Informationen über eine LISP-Sitzung anzeigen mit dem Befehl "show lisp session vrf default <IP-Adresse>"

<#root>

```
FE2068#
show lisp vrf default session 172.30.250.19


Peer address:     172.30.250.19:4342
Local address:    172.30.250.44:13255
Session Type:
Active


Session State:
Up
 (22:07:24)
Messages in/out:  9800/6537
Bytes in/out:     616771/757326
Fatal errors:     0
Rcvd unsupported: 0
Rcvd invalid VRF: 0
Rcvd override:    0
Rcvd malformed:   0
Sent deferred:    1
SSO redundancy:   N/A
Auth Type:        None
Accepting Users:  0
Users:            10
  Type                    ID                                    In/Out    State
  Policy subscription     lisp 0 IID 4099 AFI IPv4               2/1      Established
  Pubsub subscriber       lisp 0 IID 4099 AFI IPv6               1/0      Idle
  Pubsub subscriber       lisp 0 IID 8191 AFI MAC                2/0      Idle
  Pubsub subscriber       lisp 0 IID 8192 AFI MAC                0/0      Idle


ETR Reliable Registration lisp 0 IID 4099 AFI IPv4
               6/5      TCP


ETR Reliable Registration lisp 0 IID 4099 AFI IPv6
                1/3      TCP


ETR Reliable Registration lisp 0 IID 8191 AFI MAC
              9769/6517   TCP
```

```
ETR Reliable Registration lisp 0 IID 8192 AFI MAC

            2/6      TCP
  ETR Reliable Registration lisp 0 IID 16777214 AFI IPv4             4/4      TCP
  Capability Exchange       N/A                                    1/1      waiting
```

Diese detaillierte Ausgabe der Sitzung zeigt, welche Instanzen mit EID aktiv sind, die bei den Knoten der Kontrollebene registriert sind.

<#root>

```
CP_BN_2071#

show lisp session


Sessions for VRF default, total: 7, established: 4
Peer                          State      Up/Down        In/Out    Users

172.30.250.19:4342            Up

         22:10:52   1198618/1198592 4

172.30.250.19:49270           Up

      22:10:52   1198592/1198618 3

172.30.250.30:25780           Up

        22:10:38     6534/9805   6

172.30.250.44:13255           Up

        22:10:44     6550/9820   7
```

Wenn man sich die Anzahl der Sitzungen auf einem Control Plane-Knoten anschaut, werden in der Regel mehr Sitzungen angezeigt, die aktiv sind.

- Wenn es sich um einen lokalisierten Border/CP-Knoten handelt, wird auch eine LISP-Sitzung zu sich selbst aufgebaut.
- In diesem Fall gibt es eine Sitzung vom 172.30.250.19:4342 bis zum 172.30.250.19:49270.
- In dieser Sitzung registriert die Border-Komponente ihre EID beim Control Plane Node.

1.4 Informationen zur Kontrollebene

Mithilfe der Informationen, die von den Fabric-Geräten durch die Registrierung bereitgestellt werden, kann der Steuerungsebenenknoten eine vollständige Ansicht der Fabric erstellen. Pro Instanz-ID wird eine Tabelle mit den abgefragten EIDs und den zugehörigen Routing Locators verwaltet.

Zeigt dies für die Layer-3-Instanzen an, die mit dem Befehl show lisp site angezeigt werden.

<#root>

```
CP_BN_2071#
```

show lisp site

```
LISP Site Registration Information
* = Some locators are down or unreachable
# = Some registrations are sourced by reliable transport
Site Name      Last      Up     Who Last             Inst     EID Prefix
               Register         Registered           ID
site_uci       never     no     --                   4097     0.0.0.0/0
               never     no     --                   4097     172.23.255.0/24
               never     no     --                   4097     172.24.255.0/24
               never     no     --                   4099     0.0.0.0/0
               00:00:00
yes#   172.30.250.19:49270  4099     10.48.13.0/24

               never     no     --                   4099     172.23.1.0/24
               never     no     --                   4099     172.24.1.0/24
               21:35:06
yes#   172.30.250.44:13255  4099     172.24.1.3/32

               22:11:46
yes#   172.30.250.30:25780  4099     172.24.1.4/32

               never     no     --                   4099     172.24.2.0/24
               22:11:52
yes#   172.30.250.44:13255  4099     172.24.2.2/32
```

Dieser Befehl zeigt alle registrierten EIDs und die letzten registrierten EIDs an. Beachten Sie, dass dies in der Regel auch der verwendete RLOC ist. Dies kann jedoch abweichen. Auch EIDs können bei mehreren RLOCs registriert werden.

Um die vollständigen Details anzuzeigen, enthält der Befehl die EID und die Instanz

<#root>

```
CP_BN_2071#
```

show lisp site 172.24.1.3/32 instance-id 4099

```
LISP Site Registration Information
Site name: site_uci
Description: map-server
Allowed configured locators: any
Requested EID-prefix:
  EID-prefix:
```

172.24.1.3/32 instance-id 4099

```
    First registered:     21:35:53
    Last registered:      21:35:53
```

```
    Routing table tag:    0
    Origin:               Dynamic, more specific of 172.24.1.0/24
    Merge active:         No
    Proxy reply:
```

Yes

```
    Skip Publication:     No
    Force Withdraw:       No
    TTL:
```

1d00h

```
    State:
```

complete

```
    Extranet IID:         Unspecified
    Registration errors:
      Authentication failures:   0
      Allowed locators mismatch: 0
    ETR 172.30.250.44:13255, last registered 21:35:53, proxy-reply, map-notify
                             TTL 1d00h, no merge, hash-function sha1
                             state complete, no security-capability
                             nonce 0x6ED7000E-0xD4C608C5
                             xTR-ID 0x88F15053-0x40C0253D-0xAE5EA874-0x2551DB71
                             site-ID unspecified
                             Domain-ID local
                             Multihoming-ID unspecified
                             sourced by reliable transport
      Locator        Local  State      Pri/Wgt  Scope
```

172.30.250.44 yes   up

```
          10/10   IPv4 none
```

Anmerkung: Bei der detaillierten Ausgabe sind einige Punkte zu beachten:

- Proxy, mit diesem Satz antwortet der Control Plane Node direkt auf eine Map-Anfrage. Bei herkömmlichem LISP wird eine Map-Anfrage an den XTR weitergeleitet, der die EID registriert hat, aber bei einem Proxy-Set reagiert der Control-Plane-Knoten direkt
- TTL, dies ist die Lebensdauer der EID-Registrierung. Standardmäßig sind dies 24 Stunden
- ETR-Informationen. Diese beziehen sich auf das Fabric-Gerät, das die EID-Registrierung gesendet hat.
- RLOC-Informationen. Dies ist das RLOC, das zum Erreichen der EID verwendet wird. Diese enthält auch Statusinformationen wie oben/unten. Wenn das RLOC nicht verfügbar ist, wird es nicht verwendet. Darüber hinaus enthält es eine Gewichtung und eine Priorität, die verwendet werden kann, wenn mehrere RLOCs für eine EID vorhanden sind, um einem von ihnen den Vorzug zu geben.

Um den Registrierungsverlauf auf dem Knoten "Control Plane" anzuzeigen, kann der Befehl show lisp server registration history verwendet werden.

- Sie gibt einen Überblick über die registrierten und abgemeldeten EID.

Registrierungsverlauf anzeigen

<#root>

```
CP_BN_2071#
```

show lisp server registration-history last 10

```
Map-Server registration history
Roam = Did host move to a new location?
WLC = Did registration come from a Wireless Controller?
Prefix qualifier: + = Register Event, - = Deregister Event, * = AR register event
Timestamp (UTC)      Instance Proto Roam WLC Source
                                            EID prefix / Locator
*Mar 24 20:49:51.490     4099 TCP   No   No  172.30.250.19
                                          + 10.48.13.0/24
*Mar 24 20:49:51.491     4099 TCP   No   No  172.30.250.19
                                          - 10.48.13.0/24
*Mar 24 20:49:51.621     4099 TCP   No   No  172.30.250.19
                                          + 10.48.13.0/24
*Mar 24 20:49:51.622     4099 TCP   No   No  172.30.250.19
                                          - 10.48.13.0/24
*Mar 24 20:49:51.752     4099 TCP   No   No  172.30.250.19
                                          + 10.48.13.0/24
*Mar 24 20:49:51.754     4099 TCP   No   No  172.30.250.19
                                          - 10.48.13.0/24
*Mar 24 20:49:51.884     4099 TCP   No   No  172.30.250.19
                                          + 10.48.13.0/24
*Mar 24 20:49:51.886     4099 TCP   No   No  172.30.250.19
                                          - 10.48.13.0/24
*Mar 24 20:49:52.017     4099 TCP   No   No  172.30.250.19
                                          + 10.48.13.0/24
*Mar 24 20:49:52.019     4099 TCP   No   No  172.30.250.19
                                          - 10.48.13.0/24
```

Anzeige der registrierten EID für Ethernet. Der Befehl lautet show lisp instance-id <instance> Ethernet-Server (Dies ergibt eine ähnliche Ausgabe wie für Layer 3).

<#root>

```
CP_BN_2071#
```

show lisp instance-id 8191 ethernet server

```
LISP Site Registration Information
* = Some locators are down or unreachable
# = Some registrations are sourced by reliable transport
Site Name      Last      Up     Who Last             Inst     EID Prefix
               Register         Registered           ID
```

```
site_uci        never     no     --                   8191     any-mac
                00:00:04

yes#   172.30.250.44:13255  8191     0019.3052.6d7f/48


                21:36:41

yes#   172.30.250.44:13255  8191     0050.5693.8930/48


                22:13:20

yes#   172.30.250.30:25780  8191     0050.5693.f1b2/48
```

Hängen Sie die MAC-Adresse an, um detailliertere Informationen zu einer Registrierung zu erhalten.

<#root>

```
CP_BN_2071#

show lisp instance-id 8191 ethernet server 0019.3052.6d7f


LISP Site Registration Information
Site name: site_uci
Description: map-server
Allowed configured locators: any
Requested EID-prefix:
  EID-prefix:

0019.3052.6d7f/48 instance-id 8191


    First registered:     22:14:38
    Last registered:      00:00:03
    Routing table tag:    0
    Origin:               Dynamic, more specific of any-mac
    Merge active:         No
    Proxy reply:

Yes


    Skip Publication:     No
    Force Withdraw:       No
    TTL:

1d00h


    State:

complete


    Extranet IID:         Unspecified
    Registration errors:
      Authentication failures:   0
      Allowed locators mismatch: 0
```

```
    ETR 172.30.250.30:25780, last registered 00:00:03, proxy-reply, map-notify
                             TTL 1d00h, no merge, hash-function sha1
                             state complete, no security-capability
                             nonce 0x0465A327-0xA3A2974C
                             xTR-ID 0x280403CF-0x598BAAF1-0x3E70CE52-0xE8F09E6E
                             site-ID unspecified
                             Domain-ID local
                             Multihoming-ID unspecified
                             sourced by reliable transport
      Locator        Local  State      Pri/Wgt  Scope

172.30.250.30  yes

   up          10/10   IPv4 none
```

Anhängen des Registrierungsverlaufs, um den Registrierungsverlauf für die Ethernet-EID anzuzeigen

---

Anmerkung: Dieser Befehl ist sehr nützlich, wenn Geräte in der Fabric wechseln, um zu sehen, wo und wann die MAC-Adresse registriert wurde

---

<#root>

```
CP_BN_2071#

show lisp instance-id 8191 ethernet server registration-history


Map-Server registration history
Roam = Did host move to a new location?
WLC = Did registration come from a Wireless Controller?
Prefix qualifier: + = Register Event, - = Deregister Event, * = AR register event
Timestamp (UTC)      Instance Proto Roam WLC Source
                                            EID prefix / Locator
*Mar 24 20:47:10.291     8191 TCP   Yes  No  172.30.250.44
                                          + 0019.3052.6d7f/48
*Mar 24 20:47:10.296     8191 TCP   No   No  172.30.250.30
                                          - 0019.3052.6d7f/48
*Mar 24 20:47:18.644     8191 TCP   Yes  No  172.30.250.30
                                          + 0019.3052.6d7f/48
*Mar 24 20:47:18.647     8191 TCP   No   No  172.30.250.44
                                          - 0019.3052.6d7f/48
*Mar 24 20:47:20.700     8191 TCP   Yes  No  172.30.250.44
                                          + 0019.3052.6d7f/48
*Mar 24 20:47:20.702     8191 TCP   No   No  172.30.250.30
                                          - 0019.3052.6d7f/48
*Mar 24 20:47:31.914     8191 TCP   Yes  No  172.30.250.30
                                          + 0019.3052.6d7f/48
*Mar 24 20:47:31.918     8191 TCP   No   No  172.30.250.44
                                          - 0019.3052.6d7f/48
*Mar 24 20:47:40.206     8191 TCP   Yes  No  172.30.250.44
                                          + 0019.3052.6d7f/48
*Mar 24 20:47:40.210     8191 TCP   No   No  172.30.250.30
                                          - 0019.3052.6d7f/48
```

Um die registrierten Informationen zur Adressenauflösung auf dem Knoten "Kontrollebene" anzuzeigen, wird der Befehl mit der Adressenauflösung angehängt.

- Diese zeigt nur die Zuordnungen zwischen der MAC-Adresse und den zugehörigen Layer-3-Informationen und ist in erster Linie für die Fabric Edges zum Umschreiben der Layer-2-MAC-Zieladressen von Broadcast/Multicast zu Unicast zu verwenden.
- Das RLOC, das dieser Layer-2-MAC-Adresse entspricht, würde separat aufgelöst.

Hängen Sie 'address-resolution' an, um Informationen zur registrierten Adressauflösung auf dem Control Plane-Knoten anzuzeigen.

<#root>

```
CP_BN_2071#
sh lisp instance-id 8191 ethernet server address-resolution

Address-resolution data for router lisp 0 instance-id 8191
L3 InstID    Host Address                                Hardware Address

4099    172.24.1.3/32                                0050.5693.8930

    4099    172.24.1.4/32                                0050.5693.f1b2

    4099    2001:DB8::E70B:E8E1:E368:BDB7/128            0050.5693.8930

    4099    2001:DB8::F304:BCCD:6BF3:BFAF/128            0050.5693.f1b2

    4099    FE80::3EE:5111:BA77:E37D/128                 0050.5693.f1b2

    4099    FE80::1AE4:8804:5B8F:50F6/128                0050.5693.8930
```

Anmerkung: Auch wenn die lokalen IPv6-Adressen der Verbindung nicht mit der dynamischen IPv6-EID übereinstimmen, sind sie für die Adressauflösung zu erlernen, und würde dies auf dem Knoten "Kontrollebene" angezeigt. Diese würden nicht selbst unter der Layer-3-Instanz-ID registriert, sind jedoch für die Adressauflösung verfügbar.

Remote-Ziele auflösen

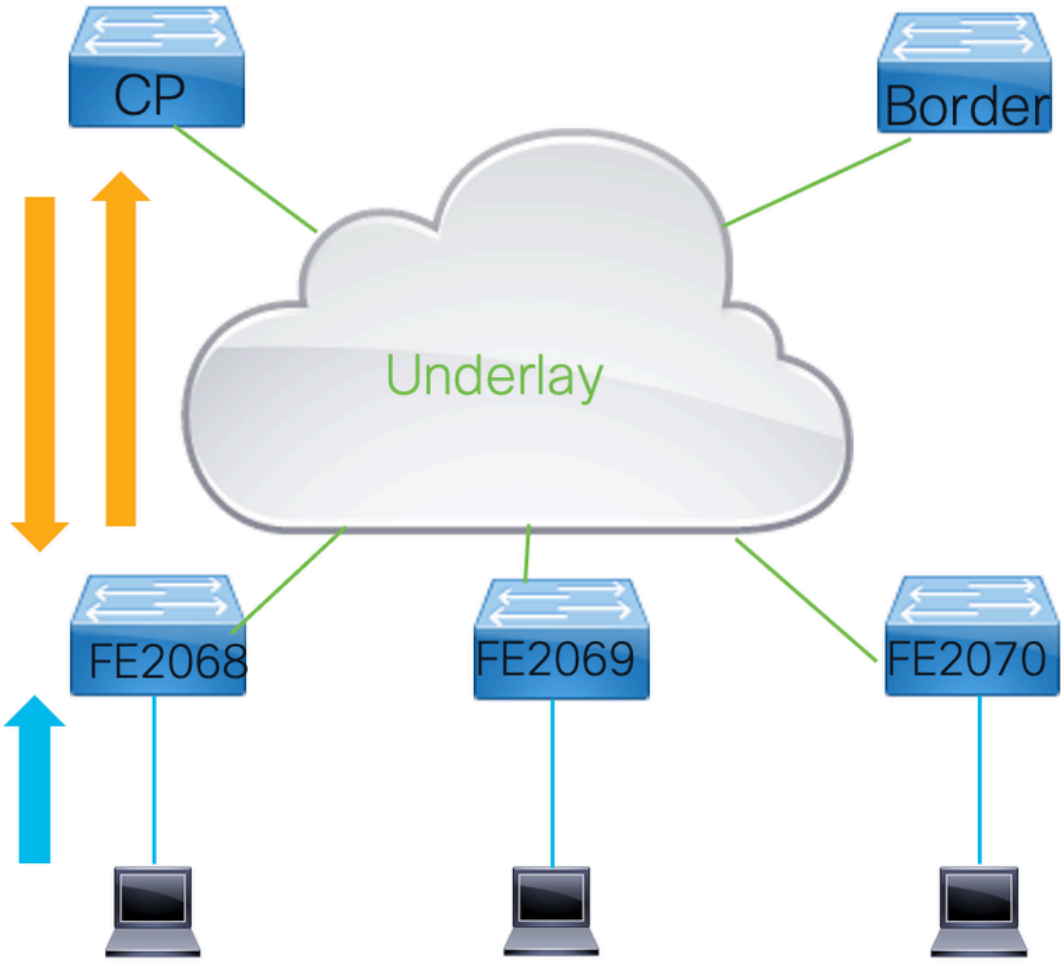
Damit Datenverkehr über eine LISP VXLAN-Fabric weitergeleitet werden kann, muss das RLOC eines Ziels aufgelöst werden. In einer LISP VXLAN-Fabric wird dazu ein Map-Cache verwendet, aus dem Informationen in die Forwarding Information Base (FIB) des Fabric-Geräts übertragen werden.

Bei LISP VXLAN-Fabrics sollen aufgrund von Datensignalen Map-Caches ausgelöst werden.

- Dies bedeutet, dass Datenverkehr an die CPU weitergeleitet wird und die CPU eine Map-Anfrage an den Control Plane Node erstellt, um die RLOC-Informationen abzufragen, an die Frames zu dieser EID gesendet werden müssen.
- Wenn der Kontrollplan eine Map-Anfrage empfängt, würde er entweder die mit dieser EID verknüpften Routing Locator-Informationen bereitstellen oder eine negative Map-Antwort zurücksenden.
- Wenn er eine negative Map-Antwort sendet, würde der Steuerungsebenenknoten nicht nur anzeigen, dass die angeforderte EID nicht bekannt ist, sondern den gesamten Block von EIDs anbieten, zu dem diese EID gehören würde, für den sie keine Registrierung hätte.

Mit den Informationen innerhalb der Map-Antwort vom Control Plane Node wird der Map-Cache aktualisiert.

- Die TTL für Kartenantworten beträgt in der Regel 24 Stunden. (Bei negativen Kartenantworten sind es in der Regel nur 15 Minuten).
- Bei Ethernet EID werden die negativen Map-Antworten nicht in den Map-Cache gelegt. (Dies geschieht nur bei Layer-3-Instanzen).



2.1 Ethernet-Map-Cache

Den Ethernet-Map-Cache mit dem Befehl show lisp instance-id <Instanz> map-cache anzeigen

<#root>

```
FE2067#

show lisp instance-id 8191 ethernet map-cache


LISP MAC Mapping Cache for LISP 0 EID-table

Vlan 150 (IID 8191)

, 1 entries
0

019.3052.6d7f/48

, uptime: 00:00:07, expires: 23:59:52, via map-reply, complete
  Locator         Uptime    State  Pri/Wgt     Encap-IID


172.30.250.44
```

```
 00:00:07  up      10/10        -
```

Dieser Befehl zeigt den Remote-MAC-Adresseintrag an, der aufgelöst worden wäre.

- Um einen Map-Cache-Eintrag für eine Ethernet-Instanz auszulösen, muss Datenverkehr an ein unbekanntes Ziel gesendet werden.
- Das Fabric-Gerät müsste dann versuchen, es über LISP aufzulösen.
- Sobald er über eine Map-Antwort gelernt wurde, wurde er in den Map-Cache verschoben, und die nachfolgenden Frames zu diesem Layer-2-Ziel wurden direkt an den gelernten Routing Locator gesendet.

In Layer-2-Instanzen kann optional eine Flut von BUM-Datenverkehr verwendet werden.

- LISP/VXLAN flutet den Datenverkehr nicht standardmäßig, da es eine Overlay-Technologie verwendet. Es kann jedoch eine IP-Multicast-Gruppe im Underlay-Netzwerk (GRT) konfiguriert werden, durch die Layer-2-Frames geflutet werden könnten.

Broadcast-Underlay-Gruppenadresse anzeigen

<#root>

```
FE2068#
```

sh run | sec instance-id 8191

```
 instance-id 8191
  remote-rloc-probe on-route-change
  service ethernet
   eid-table vlan 150
```

broadcast-underlay 239.0.1.19

```
   database-mapping mac locator-set rloc_hosts
   exit-service-ethernet
  !
  exit-instance-id
```

2.2 IP-Zuordnungscache

Für Layer-3-Instanzen ähneln die Map-Cache-Informationen dem Ethernet-Build, der von Datenverkehr an die CPU gesendet wird, um zu signalisieren, dass eine Map-Anforderung gesendet wird.

- Bei Layer 3 werden Pakete jedoch nur dann an die CPU gesendet, wenn dies eingerichtet werden soll. Dies erfolgt über den konfigurierten map-cache-Befehl. Für IPv4 ist dies 0.0.0.0/0 und ::0/0 für IPv6.
- Die Konfiguration dieses Map-Cache-Eintrags an Grenzknoten muss mit Vorsicht erfolgen.

Wenn ein Grenzknoten mit dem map-cache 0.0.0.0/0 oder ::0/0 map-cache-Eintrag konfiguriert wird, versucht er, unbekannte Ziele über die Fabric aufzulösen, anstatt sie außerhalb der Fabric zu routen.

Anzeigen der Map-Cache-Konfiguration

<#root>

FE2068#

sh run | sec instance-id 4099

```
 instance-id 4099
  remote-rloc-probe on-route-change
  dynamic-eid Fabric_VN_Subnet_1_IPv4
   database-mapping 172.24.1.0/24 locator-set rloc_hosts
   exit-dynamic-eid
  !
  dynamic-eid Fabric_VN_Subnet_1_IPv6
   database-mapping 2001:DB8::/64 locator-set rloc_hosts
   exit-dynamic-eid
  !
  service ipv4
   eid-table vrf Fabric_VN_1

map-cache 0.0.0.0/0 map-request

   exit-service-ipv4
  !
  service ipv6
   eid-table vrf Fabric_VN_1
   map-cache ::/0 map-request

   exit-service-ipv6
  !
  exit-instance-id
```

Die map-cache 0.0.0.0/0 und ::/0 map-request bewirken, dass ein map-cache Eintrag im map-cache mit den Aktionen "send-map-request" konfiguriert wird. Datenverkehr, der auf diesen Port trifft, löst Map-Requests aus. Da die Map-Cache-Einträge in die FIB eingefügt werden sollen, die auf der Grundlage der längsten Übereinstimmung arbeitet, wird dies auf den gesamten gerouteten IP-Datenverkehr angewendet, der keinen der spezifischeren Einträge trifft.

- Auf unterstützten Plattformen lautet die Aktion send-map-request + encapsulate to proxy ETR, um zu verhindern, dass das erste Paket verworfen wird.
  Dies führt dazu, dass das erste Paket an ein unbekanntes Ziel eine Map-Anfrage auslöst und dass das Paket ggf. an den Proxy-Eintrag weitergeleitet wird.

<#root>

FE2067#

show lisp instance-id 4099 ipv4 map-cache

LISP IPv4 Mapping Cache for LISP 0 EID-table vrf Fabric_VN_1 (IID 4099), 6 entries

0.0.0.0/0,

uptime: 22:28:18, expires: 00:13:41, via map-reply, unknown-eid-forward
action:

send-map-request + Encapsulating to proxy ETR

PETR	Uptime	State	Pri/Wgt	Encap-IID	Metric
172.30.250.19	22:28:18	up	10/10	-	0

10.48.13.0/24,

uptime: 02:31:26, expires: 21:28:34, via map-reply, complete

Locator	Uptime	State	Pri/Wgt	Encap-IID
172.30.250.19				
	02:31:26	up	10/10	-

172.24.1.0/24

, uptime: 22:31:34, expires: never, via dynamic-EID, send-map-request

Negative cache entry, action: send-map-request

172.24.2.0/24

, uptime: 22:31:34, expires: never, via dynamic-EID, send-map-request

Negative cache entry, action: send-map-request

172.24.2.2/32

, uptime: 00:00:21, expires: 23:59:38,

via map-reply, complet

e

Locator	Uptime	State	Pri/Wgt	Encap-IID
172.30.250.44				
	00:00:21	up	10/10	-

172.28.0.0/14,

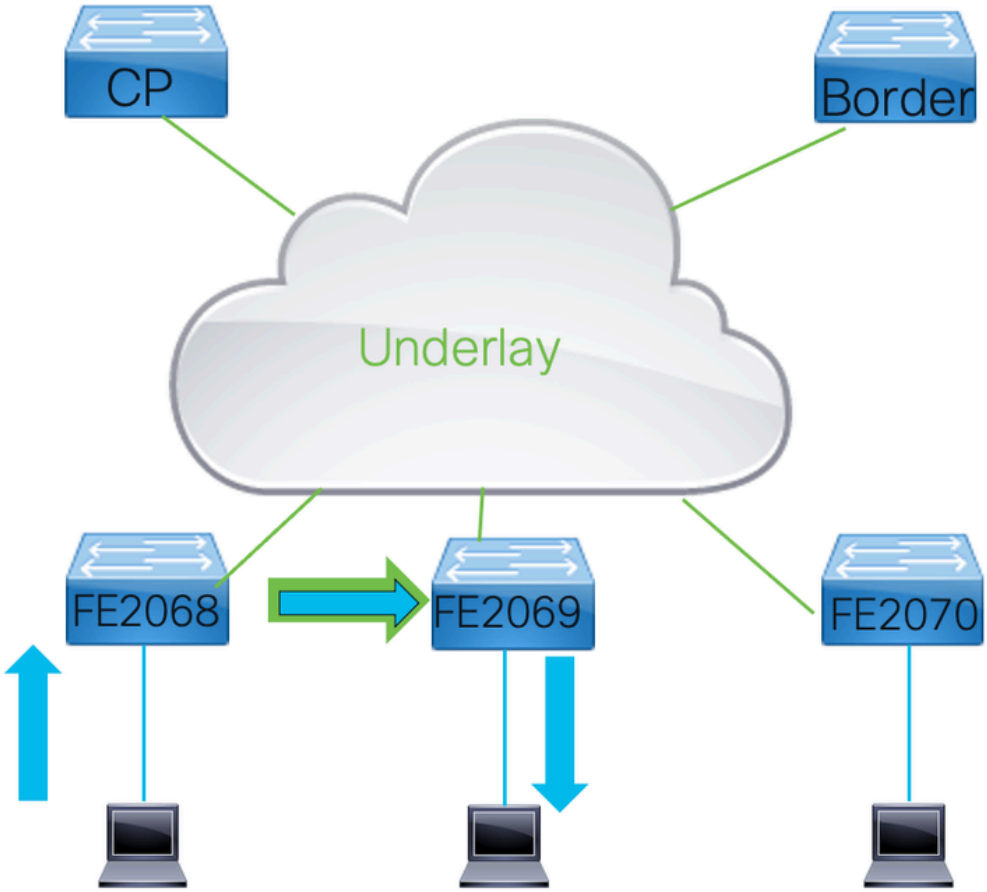
uptime: 22:28:22, expires: 00:13:39, via map-reply, unknown-eid-forward

PETR	Uptime	State	Pri/Wgt	Encap-IID	Metric
172.30.250.19					
	22:28:19	up	10/10	-	0

In dieser Ausgabe werden einige Einträge angezeigt.

- 10.48.13.0/24 und 172.24.2.2/32 in dieser Ausgabe wird über map-reply gelernt und ist abgeschlossen. Der Datenverkehr zu diesen Zielen muss gekapselt und an die jeweiligen Standorte weitergeleitet werden.
- Das 172.28.0.0/14 ist ein Beispiel für eine negative Antwort auf eine Karte, die empfangen wurde, und für einen Block von IP-Adressen, der zurückgegeben wurde. Der Datenverkehr zu diesem Subnetz löst keine Map-Anfrage aus, solange sich dieser Eintrag im Map-Cache befindet.

Datenweiterleitung durch die Fabric



3.1 Layer-2- oder Layer-3-Weiterleitung

Datenverkehr in einer LISP/VXLAN-Fabric kann über Layer 2- oder Layer 3-Instanzen weitergeleitet werden.

- Die Entscheidung, welche Instanz verwendet wird, hängt von der MAC-Zieladresse der Frames ab.
- Frames, die an eine beliebige andere MAC-Adresse als diejenige gesendet werden, die

beim Switch registriert ist, müssen über Layer 2 weitergeleitet werden. Wenn das Ziel des Pakets der Switch ist, wird dieser über Layer 3 weitergeleitet.
- Dies ist die gleiche Logik, die auch für die normale Weiterleitung über einen Catalyst Switch der Serie 9000 gilt.

3.2 Layer-2-Weiterleitung

Die Layer-2-Weiterleitung über eine LISP VXLAN-Fabric erfolgt basierend auf der Layer-2-MAC-Zieladresse. Remote-Ziele werden in die MAC-Adresstabelle mit der Ausgangsschnittstelle L2LI0 eingefügt.

Anzeigen der lokalen und Remote-Layer-2-Schnittstellen

<#root>

FE2068#

show mac address-table vlan 150

```
          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
 150    0000.0c9f.f18e    STATIC      Vl150
 150    0050.5693.8930    DYNAMIC     Gi1/0/1
 150    2416.9db4.33fd    STATIC      Vl150
```

<- Local

```
 150    0019.3052.6d7f    CP_LEARN
```

L2LI0 <- Remote

```
Total Mac Addresses for this criterion: 3
Total Mac Addresses installed by LISP: REMOTE: 1
```

Bei unbekannten Zielen wird, sofern konfiguriert, Datenverkehr über die konfigurierte IP-Multicast-Gruppe im Underlay gesendet.

- Zur Gewährleistung einer korrekten Flut von Broadcast-, Unicast- und Multicast-Datenverkehr (nur bei selektivem Multicast-Flood) ist eine ordnungsgemäß funktionierende Multicast-Umgebung im Underlay erforderlich.
- Der Datenverkehr, der über diese Multicast-Underlay-Gruppe gesendet würde, muss in VXLAN gekapselt werden.
- Alle anderen Edges müssen der Multicast-Gruppe beitreten, Datenverkehr empfangen und den Datenverkehr für bekannte Layer-2-Instanzen entkapseln.

Anzeige der zugrunde liegenden IP-Multicast-Gruppe

<#root>

FE2068#

sh ip mroute 239.0.19.1

```
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, E - Extranet,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report,
       Z - Multicast Tunnel, z - MDT-data group sender,
       Y - Joined MDT-data group, y - Sending to MDT-data group,
       G - Received BGP C-Mroute, g - Sent BGP C-Mroute,
       N - Received BGP Shared-Tree Prune, n - BGP C-Mroute suppressed,
       Q - Received BGP S-A Route, q - Sent BGP S-A Route,
       V - RD & Vector, v - Vector, p - PIM Joins on route,
       x - VxLAN group, c - PFP-SA cache created entry,
       * - determined by Assert, # - iif-starg configured on rpf intf,
       e - encap-helper tunnel flag, l - LISP decap ref count contributor
Outgoing interface flags: H - Hardware switched, A - Assert winner, p - PIM Join
                          t - LISP transit group
 Timers: Uptime/Expires
 Interface state: Interface, Next-Hop or VCD, State/Mode
(*, 239.0.1.19), 00:02:36/stopped, RP 172.31.255.1, flags: SJCF
  Incoming interface: GigabitEthernet1/0/23, RPF nbr 172.30.250.42
  Outgoing interface list:
    L2LISP0.8191, Forward/Sparse-Dense, 00:02:35/00:00:24, flags:
(
```

172.30.250.44, 239.0.1.19

```
), 00:02:03/00:00:56, flags: FT
  Incoming interface:
```

Null0

```
, RPF nbr 0.0.0.0
  Outgoing interface list:
```

GigabitEthernet1/0/23

```
, Forward/Sparse, 00:02:03/00:03:23, flags:
(
```

172.30.250.30, 239.0.1.19

```
), 00:02:29/00:00:30, flags: JT
  Incoming interface:
```

GigabitEthernet1/0/23

```
, RPF nbr 172.30.250.42
  Outgoing interface list:
```

L2LISP0.8191

```
, Forward/Sparse-Dense, 00:02:29/00:00:30, flags:
```

Diese Ausgabe zeigt einen S,G-Eintrag für alle anderen Edges im Fabric an, in denen Clients

konfiguriert sind, die Datenverkehr mit Flooding senden würden. Außerdem wird ein S,G-Eintrag mit dem Loopback0 dieses Edge-Geräts als Quelle angezeigt.

Für die Empfängerseite des Datenverkehrs durch die zugrunde liegende Multicast-Gruppe zeigt der Befehl show ip mroute auch L2LISP0 an.<Instanz>
Dies würde angeben, für welche Layer-2-Instanzen dieses Edge-Gerät gefluteten Datenverkehr entkapselt und an seine
relevanten Schnittstellen.

3.3 Layer 3-Weiterleitungsinformationen

Um zu bestimmen, wie der Datenverkehr bei der Bereitstellung einer LISP VXLAN-Fabric weitergeleitet wird, muss CEF überprüft werden.

- Im Gegensatz zu herkömmlichen Routing-Protokollen fügt LISP die Routing-Richtung nicht in die Routing-Tabelle ein, sondern interagiert direkt mit CEF, um die FIB zu aktualisieren.

Die Map-Cache-Informationen enthalten für ein bestimmtes Remote-Ziel die zu verwendenden Locator-Informationen.

Lokatorinformationen anzeigen

<#root>

```
FE2067#
sh lisp instance-id 4099 ipv4 map-cache 172.24.2.2

LISP IPv4 Mapping Cache for LISP 0 EID-table vrf Fabric_VN_1 (IID 4099), 1 entries

172.24.2.2/32
, uptime: 11:19:02, expires: 12:40:57, via map-reply, complete
  Sources: map-reply
  State: complete, last modified: 11:19:02, map-source: 172.30.250.44
  Idle, Packets out: 2(1152 bytes), counters are not accurate (~ 11:18:35 ago)
  Encapsulating dynamic-EID traffic
  Locator        Uptime    State  Pri/Wgt     Encap-IID

172.30.250.44
  11:19:02  up      10/10        -
    Last up-down state change:         11:19:02, state change count: 1
    Last route reachability change:    11:19:02, state change count: 1
    Last priority / weight change:     never/never
    RLOC-probing loc-status algorithm:
      Last RLOC-probe sent:            11:19:02 (rtt 2ms)
```

Aus dem Map-Cache lautet der Locator für diese EID 172.30.250.44. Der Datenverkehr zu diesem

Ziel muss also gekapselt werden, und der äußere IP-Header hat die IP-Zieladresse 172.30.250.44.

In der Routing-Tabelle für die in dieser Instanz verwendete VRF-Instanz wird dieser Eintrag nicht angezeigt.

<#root>

FE2067#

show ip route vrf Fabric_VN_1

```
Routing Table: Fabric_VN_1
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type
       E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       H - NHRP, G - NHRP registered, g - NHRP registration summary
       o - ODR, P - periodic downloaded static route, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
       & - replicated local route overrides by connected
Gateway of last resort is not set
      172.24.0.0/16 is variably subnetted, 5 subnets, 2 masks
C        172.24.1.0/24 is directly connected, Vlan150
l        172.24.1.4/32 [10/1] via 172.24.1.4, 06:11:02, Vlan150
L        172.24.1.254/32 is directly connected, Vlan150
C        172.24.2.0/24 is directly connected, Vlan151
L        172.24.2.254/32 is directly connected, Vlan151
```

CEF-Ausgänge liefern weitere Informationen über die Weiterleitung über die LISP VXLAN-Fabric.

- Wenn das Stichwort detail zum Befehl show ip cef hinzugefügt wird, gibt es nicht nur das Ziel für den gekapselten Frame an, der gesendet werden soll.
- Die Ausgangsschnittstelle mit dieser Ausgabe ist LISP 0.<Instanz> gibt an, dass der Datenverkehr gekapselt gesendet wird.

<#root>

FE2067#

sh ip cef vrf Fabric_VN_1 172.24.2.2 detail

```
172.24.2.2/32, epoch 1, flags [subtree context, check lisp eligibility]
  SC owned,sourced: LISP remote EID - locator status bits 0x00000001
  LISP remote EID: 2 packets 1152 bytes
```

fwd action encap

```
, dynamic EID need encap
  SC inherited: LISP cfg dyn-EID - LISP configured dynamic-EID
```

```
  LISP EID attributes: localEID No, c-dynEID Yes, d-dynEID No, a-dynEID No
  SC inherited: LISP generalised SMR - [enabled, inheriting, 0x7FF95B3E0BE8 locks: 5]
  LISP source path list
```

nexthop 172.30.250.44 LISP0.4099

```
  2 IPL sources [no flags]
```

nexthop 172.30.250.44 LISP0.4099

Da der Datenverkehr gekapselt an den nächsten Hop gesendet wird, muss im nächsten Schritt show ip cef <next hop> ausgeführt werden, um die Ausgangsschnittstelle anzuzeigen, an die das Paket ebenfalls weitergeleitet wird.

Ausführen, um die Ausgangsschnittstelle anzuzeigen

<#root>

FE2067#

sh ip cef 172.30.250.44

172.30.250.44/32

nexthop 172.30.250.38 GigabitEthernet1/0/23

Anmerkung: Es gibt zwei verschiedene Ebenen von Equal Cost Multiple Path (ECMP)-Routing.

- Für den Datenverkehr kann im Overlay ein Load Balancing durchgeführt werden, wenn zwei angekündigte RLOCs vorhanden sind. Wenn redundante Pfade zum Erreichen einer RLOC-IP-Adresse vorhanden sind, kann ein Load Balancing im Underlay-Netzwerk erfolgen.
- Da der UDP-Zielport auf 4789 festgelegt ist und die Quell- und Ziel-IP-Adressen für alle Datenflüsse zwischen zwei Fabric-Geräten identisch sind, muss ein Anti-Polarisationsmechanismus eingerichtet werden, der verhindert, dass alle Pakete über denselben Pfad geleitet werden.
- Bei LISP VXLAN ist dies der UDP-Quell-Port im äußeren Header, der sich bei verschiedenen Datenflüssen im Überlaufnetzwerk unterscheiden würde.

3.4 Paketformat

- In LISP VXLAN-Fabrics ist der gesamte Datenverkehr vollständig in VXLAN gekapselt. Dies

umfasst den gesamten Layer-2-Frame, um Layer-2- und Layer-3-Overlays unterstützen zu können.
Bei Layer-2-Frames wird der ursprüngliche Header gekapselt. Für Frames, die über eine Layer-3-Instanz gesendet werden, wird ein Dummy-Layer-2-Header verwendet.

<#root>

```
Ethernet II, Src: 24:16:9d:3d:56:67 (24:16:9d:3d:56:67), Dst: 6c:31:0e:f6:21:c7 (6c:31:0e:f6:21:c7)
 Internet Protocol Version 4, Src: 172.30.250.30, Dst: 172.30.250.44
  User Datagram Protocol, Src Port: 65288, Dst Port: 4789
   Virtual eXtensible Local Area Network
   Flags: 0x8800, GBP Extension, VXLAN Network ID (VNI)
   1... .... .... .... = GBP Extension: Defined
   .... .... .0.. .... = Don't Learn: False
   .... 1... .... .... = VXLAN Network ID (VNI): True
   .... .... .... 0... = Policy Applied: False
   .000 .000 0.00 .000 = Reserved(R): 0x0000
   Group Policy ID: 16


   VXLAN Network Identifier (VNI): 4099


   Reserved: 0
    Ethernet II, Src: 00:00:00:00:80:a3 (00:00:00:00:80:a3), Dst: ba:25:cd:f4:ad:38 (ba:25:cd:f4:ad:38)
     Internet Protocol Version 4, Src: 172.24.1.4, Dst: 172.24.2.2
      Internet Control Message Protocol
```

Wie die Beispielerfassung eines Frames zeigt, der durch eine LISP VXLAN-Fabric übertragen wird, befindet sich der vollständig gekapselte Frame im VXLAN-Paket. Als Layer-3-Frame ist der Ethernet-Header ein Dummy-Header.

Im VXLAN-Header enthält das Feld "VLAN Network Identifier" die LISP-Instanz-ID, zu der der Frame gehört.

- Über das Feld "Group Policy ID" (Gruppenrichtlinien-ID) wird der SGT-Tag des Frames übertragen.
- Diese wird beim Eingang in die Fabric festgelegt und zur Fabric weitergeleitet, bis eine gruppenbasierte Richtliniendurchsetzung erfolgt ist.

Authentifizierung und Sicherheitsdurchsetzung

4.1 Switch-Port-Authentifizierung

Für die dynamische Zuweisung von Endpunkten zu den jeweiligen VLANs und die Zuweisung eines SGT-Tags kann eine Authentifizierung verwendet werden.

- Authentifizierungsprotokolle wie Dot1x/MAB/zentrale Webauthentifizierung können implementiert werden, um Benutzer und Endpunkte auf einem Radius-Server zu

authentifizieren und zu autorisieren, der Attribute zurück an den Switch sendet, um den Netzwerkzugriff auf den Client/Endpunkt im richtigen Pool und mit der richtigen Netzwerkzugriffsautorisierung zu ermöglichen.

Für die LISP-VXLAN-Fabric gibt es nur wenige gemeinsame RADIUS-Attribute:

- VLAN-Zuweisung: Dieses Attribut wird auf die VLAN-ID oder den Namen vom Radius-Server für die Switches festgelegt, denen ein Endpunkt einer bestimmten Layer 2-/Layer 3-LISP-Instanz zugewiesen werden kann.
- SGT-Wert: Dieses Attribut legt fest, dass ein SGT diesem SGT einen Endpunkt zuweist. Dies wird für gruppenbasierte Richtlinien für diesen Endpunkt verwendet und weist allen Frames, die von diesem Endpunkt über die Fabric gesendet werden, einen SGT-Wert zu.
- Sprachautorisierung: Sprachgeräte arbeiten mit dem Sprach-VLAN. Dadurch wird die Sprachautorisierung festgelegt, die das Senden und Empfangen von Datenverkehr durch den Endpunkt in dem für einen Port konfigurierten Sprach-VLAN zulässt. Trennung von Sprach- und Datenverkehr in den jeweiligen VLANs
- Sitzungs-Timeout: Verschiedene Endpunkte haben ihre eigenen Timeouts für die Sitzungen. Ein Timeout kann vom Radius-Server gesendet werden, um anzugeben, wie oft ein Client sich erneut authentifizieren muss
- Vorlage: Für einige Endpunkte muss eine andere Vorlage auf einen Port angewendet werden, um ordnungsgemäß zu funktionieren. Ein Vorlagenname kann vom Radius-Server gesendet werden, der angibt, was auf den Port angewendet werden muss.

Überprüfen Sie das Ergebnis der Authentifizierung an einem Port mithilfe des Befehls show access-session

<#root>

```
FE2067#
```

show access-session interface Gi1/0/1 details

```
Interface: GigabitEthernet1/0/1
IIF-ID: 0x1FF97CF7
MAC Address: 0050.5693.f1b2
IPv6 Address: FE80::3EE:5111:BA77:E37D
IPv4 Address: 172.24.1.4
User-Name: 00-50-56-93-F1-B2
Device-type: Microsoft-Workstation
Device-name: W7180-PC
Status:
```

Authorized

```
Domain:
```

DATA

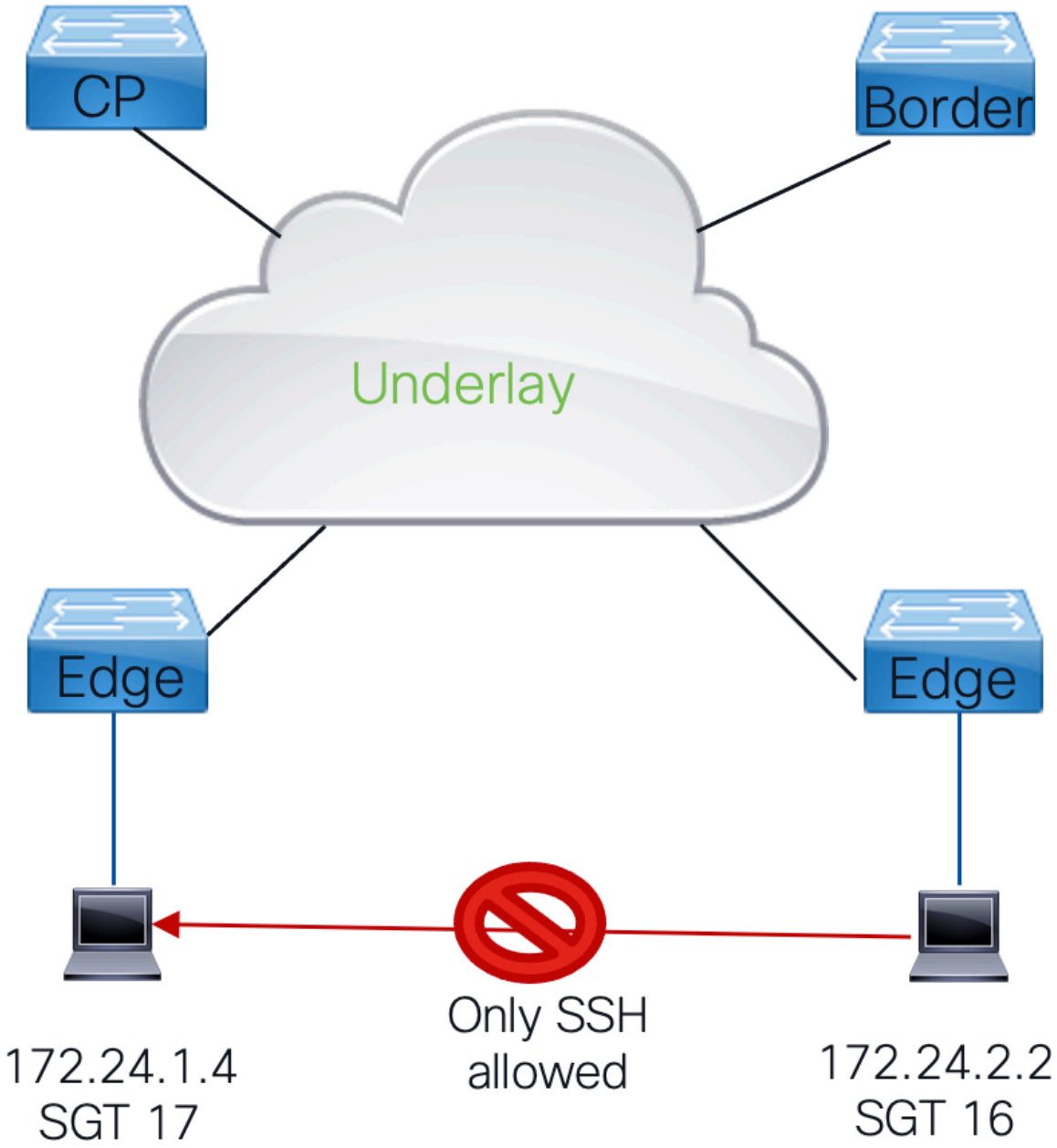
```
Oper host mode: multi-auth
Oper control dir: both
```

```
Session timeout: N/A
Acct update timeout: 172800s (local), Remaining: 172678s
Common Session ID: 9256300A000057B8376D924C
Acct Session ID: 0x00016d77
Handle: 0x85000594
Current Policy: PMAP_DefaultWiredDot1xClosedAuth_1X_MAB

Local Policies:

Server Policies:

Vlan Group: Vlan: 150


SGT Value: 16



Method status list:
Method State
dot1x

Stopped


mab Authc

Success
```

Beachten Sie folgende Schlüsselfelder:

- IPv4- und IPv6-Adressen: Wird normalerweise durch die Geräteverfolgung gelernt.
- Benutzername: Dies ist der Benutzername für die Authentifizierung.
    - Für Dot1x ist dies normalerweise der Benutzer, der sich authentifiziert.
    - Wenn MAB verwendet wird, ist dies die MAC-Adresse der Station, die als Benutzername und Kennwort zur Authentifizierung an Radius gesendet wird.
- Status: Zeigt den Status der Authentifizierung und des Authentifizierungsergebnisses an.
- Domäne: Bei normalen Endgeräten wäre dies die Daten-Domäne, sodass der Datenverkehr über den Port ohne Tags gesendet/empfangen wird. (Für Sprachgeräte kann dies auf "Voice" (Sprache) eingestellt werden)
- Serverrichtlinien: Hier werden die Informationen vom Radius-Server wie VLAN-Zuweisung und SGT-Zuweisung angezeigt.
- Methodenstatusliste: Dies zeigt eine Übersicht der ausgeführten Methoden.
    - Der Standard dot1x läuft vor MAB.
    - Wenn ein Endpunkt nicht auf EAPOL-Frames reagiert, wird ein Failover zu mab durchgeführt.
    - Dies würde dann zeigen, dass Punkt1x ausgefallen ist.
    - MAB zeigt, dass die erfolgreiche Authentifizierung auf eine verwaltete Authentifizierung hinweist. Es wird nicht angezeigt, ob das Authentifizierungsergebnis ein Akzeptieren oder Ablehnen des Zugriffs sein würde.

4.2 Datenverkehrsrichtlinien und gruppenbasierte Richtlinien (CTS)



Innerhalb eines LISP VXLAN-Fabric wird CTS verwendet, um Datenverkehrsrichtlinien durchzusetzen:

- Die gruppenbasierte Richtlinienarchitektur basiert auf sicheren Gruppen-Tags.
- Der gesamte Datenverkehr innerhalb der Fabric wird mit einem Eingangs- und einem SGT-Tag zugewiesen, der in jedem Frame durch die Fabric geleitet wird.
- Wenn dieser Datenverkehr die Fabric verlässt, werden die Datenverkehrsrichtlinien durchgesetzt.
- Dies erfolgt in gruppenbasierten Richtlinien, die die Quell- und Zielgruppentags des Pakets mit der Matrix abgleichen, die aus Quell-Ziel-SGTs besteht, wobei das Ergebnis eine SGACL ist, die definiert, welcher Datenverkehr zulässig wäre oder nicht.
- Wenn innerhalb der Matrix keine spezifische Übereinstimmung für das Quell-Ziel-SGT

besteht, muss die definierte Standardaktion angewendet werden.

4.3 CTS-Umgebung

Um mit gruppenbasierten Richtlinien arbeiten zu können, müssen Fabric-Geräte zunächst ein CTS-Paket erhalten.

- Dieses Paket wird innerhalb von RADIUS-Frames verwendet, um die RADIUS-Frames auf der Cisco ISE zu autorisieren. Mit dieser Eigenschaft wird das cts-pac-opaque-Feld innerhalb der Radius-Frames festgelegt.

Anzeigen der CTS-Paketinformationen

<#root>

FE2067#

sh cts pacs

AID:

C7105D0DA108B6AE0FB00499233B9C6A

PAC-Info:
PAC-type = Cisco Trustsec
AID: C7105D0DA108B6AE0FB00499233B9C6A
I-ID: FOC2410L1ZZ
A-ID-Info: Identity Services Engine
Credential Lifetime:

18:05:51 UTC Sat Jun 24 2023

PAC-Opaque: 000200B80003000100040010C7105D0DA108B6AE0FB00499233B9C6A0006009C00030100C5C0B998FB5E8C106F6

Refresh timer is set for 12w0d

Es muss sichergestellt werden, dass der CTS-Paket konfiguriert und gültig ist. Diese wird vom Fabric-Gerät automatisch aktualisiert.

Anmerkung: Um manuell eine Aktualisierung auszulösen, kann der Befehl "cts refresh pac" ausgegeben werden.

Für den Betrieb durch gruppenbasierte Richtlinien werden sowohl Umgebungsdaten als auch die erforderlichen Richtlinieninformationen heruntergeladen.

- Diese Umgebungsdaten enthalten sowohl das vom Switch selbst verwendete CTS-Tag als auch die Tabelle aller auf dem Radius-Server bekannten gruppenbasierten

Richtliniengruppen.

Anzeigen von CTS-Umgebungsdaten

```
<#root>

FE2067#

sh cts environment-data


CTS Environment Data
====================
Current state =

COMPLETE


Last status =

Successful


Service Info Table:
Local Device SGT:
SGT tag =

2-00:TrustSec_Devices


Server List Info:
Installed list: CTSServerList1-0001, 1 server(s):
*Server:

10.48.13.221

, port 1812,

A-ID C7105D0DA108B6AE0FB00499233B9C6A


Status = ALIVE
auto-test = TRUE, keywrap-enable = FALSE, idle-time = 60 mins, deadtime = 20 secs
Security Group Name Table:
0-00:Unknown
2-00:TrustSec_Devices
3-00:Network_Services
4-00:Employees
5-00:Contractors
6-00:Guests
7-00:Production_Users
8-00:Developers
9-00:Auditors
10-00:Point_of_Sale_Systems
11-00:Production_Servers
12-00:Development_Servers
13-00:Test_Servers
14-00:PCI_Servers
15-00:BYOD
16-00:Fabric_Client_1
17-00:Fabric_Client_2
255-00:Quarantined_Systems
Environment Data Lifetime = 86400 secs
```

```
Last update time = 11:46:41 UTC Fri Mar 31 2023
Env-data expires in 0:19:17:04 (dd:hr:mm:sec)
Env-data refreshes in 0:19:17:04 (dd:hr:mm:sec)
Cache data applied = NONE
State Machine is running
Retry_timer (60 secs) is not running
```

Wenn gruppenbasierte Richtlinien verwendet werden, werden nur die CTS-Tags heruntergeladen, mit denen das Gerät lokale Endpunkte hat und die durchgesetzt werden müssen.

- Um die Zuordnung von einer IP-Adresse (oder einem Subnetz) zu einer gruppenbasierten Richtliniengruppe überprüfen zu können, kann der Befehl "show cts role-based sgt-map vrf <vrf> all" verwendet werden.

Anzeige aller bekannten IP-To-SGT-Informationen für eine VRF-Instanz

<#root>

FE2067#

sh cts role-based sgt-map vrf Fabric_VN_1 all

```
Active IPv4-SGT Bindings Information
IP Address SGT Source
========================================
```

172.24.1.4 17 LOCAL

172.24.1.254 2 INTERNAL

172.24.2.254 2 INTERNAL

```
IP-SGT Active Bindings Summary
========================================
Total number of LOCAL bindings = 1
Total number of INTERNAL bindings = 2
Total number of active bindings = 3
Active IPv6-SGT Bindings Information
IP Address SGT Source
========================================================================
```

2001:DB8::1 2 INTERNAL

2001:DB8::F304:BCCD:6BF3:BFAF 17 LOCAL

```
IP-SGT Active Bindings Summary
========================================
Total number of LOCAL bindings = 1
Total number of INTERNAL bindings = 1
Total number of active bindings = 2
```

Diese Ausgabe zeigt alle bekannten IP-Adressen (und Subnetze) für eine bestimmte VRF-Instanz und deren gruppenbasierte Richtlinienzuordnungen an.

- Wie hier zu sehen ist, wird eine IP-Adresse eines Endpunkts der Gruppe 17 auf Gruppenbasis zugewiesen und lokal bezogen.
- Dies ist das Ergebnis der Authentifizierung, die auf dem Port stattfindet, und bei der die Ergebnisse anzeigen, dass das mit dem Endpunkt verknüpfte Tag.
- Außerdem werden die Switch-eigenen IP-Adressen hervorgehoben, denen das Device-sgt-Tag als interne Quelladresse zugewiesen wird.
- Gruppenbasierte Richtlinien-Tags können auch über eine Konfiguration oder eine SXP-Sitzung zur ISE zugewiesen werden.

Wenn ein Gerät von einem SGT-Tag erfährt, versucht es, die ihm zugeordneten Richtlinien vom ISE-Server herunterzuladen.

- Der Befehl show cts -Autorisierungseinträge gibt einen Überblick darüber, wann versucht wurde, diese herunterzuladen, und ob sie nacheinander heruntergeladen wurden oder nicht.

Anmerkung: Richtlinien müssen regelmäßig aktualisiert werden, falls sie sich ändern. Die ISE kann auch einen CoA-Befehl eingeben, damit der Switch bei jeder Änderung neue Richtlinien herunterladen kann. Um die Richtlinien manuell zu aktualisieren, wird der Befehl "cts refresh policy" ausgegeben.

Zeigt eine Übersicht über die Richtlinien an, die heruntergeladen werden sollen, und ob sie nacheinander heruntergeladen wurden oder nicht.

<#root>

```
FE2067#

show cts authorization entries


Authorization Entries Info
==========================
Peer name = Unknown-0
Peer SGT =

0-00:Unknown


Entry State =

COMPLETE


Entry last refresh = 22:14:46 UTC Thu Mar 30 2023
SGT policy last refresh = 22:14:46 UTC Thu Mar 30 2023
```

```
SGT policy refresh time = 86400
Policy expires in 0:05:23:44 (dd:hr:mm:sec)
Policy refreshes in 0:05:23:44 (dd:hr:mm:sec)
Retry_timer = not running
Cache data applied = NONE
Entry status =
```

SUCCEEDED

```
AAA Unique-ID = 11

Peer name = Unknown-17
Peer SGT =
```

17-01:Fabric_Client_2

```
Entry State =
```

COMPLETE

```
Entry last refresh = 11:47:31 UTC Fri Mar 31 2023
SGT policy last refresh = 11:47:31 UTC Fri Mar 31 2023
SGT policy refresh time = 86400
Policy expires in 0:18:56:29 (dd:hr:mm:sec)
Policy refreshes in 0:18:56:29 (dd:hr:mm:sec)
Retry_timer = not running
Cache data applied = NONE
Entry status =
```

SUCCEEDED

```
AAA Unique-ID = 4031
```

Falls Richtlinien heruntergeladen wurden, können diese mit dem Befehl "show cts rolebased policies" angezeigt werden.

<#root>

```
FE2067#
```

sh cts role-based permissions

```
IPv4 Role-based permissions
```

default

```
:
```

Permit IP-00

```
IPv4 Role-based permissions from
```

group 17:Fabric_Client_2 to group 16:Fabric_Client_1

```
:
```

PermitWeb-02

```
RBACL Monitor All for Dynamic Policies : FALSE
RBACL Monitor All for Configured Policies : FALSE
```

Dieser Befehl zeigt alle Richtlinien an, die das Gerät gelernt hat. Auf dem ISE-Server sind potenziell mehr Richtlinien für verschiedene Gruppen vorhanden, aber das Gerät versucht nur, Richtlinien herunterzuladen, für die es Endpunkte kennt. So werden wertvolle Hardwareressourcen geschont.

Dieser Befehl zeigt auch die Standardaktion an, die auf Datenverkehr angewendet werden soll, für den kein spezifischer Eintrag bekannt ist. In diesem Fall ist die Permit IP, sodass der gesamte Datenverkehr, der nicht mit einem bestimmten Eintrag in der Tabelle übereinstimmt, passieren darf.

Führen Sie show cts rbacl <name> aus, um weitere Informationen zum genauen Inhalt der heruntergeladenen RBACL zu erhalten.

<#root>

```
FE2067#
```

sh cts rbacl permitssh

```
CTS RBACL Policy
================
RBACL IP Version Supported: IPv4 & IPv6
name =
```

permitssh

```
-03
IP protocol version = IPV4
refcnt = 2
flag = 0x41000000
stale = FALSE
RBACL ACEs:
```

permit tcp dst eq 22

permit tcp dst eq 23

deny ip

In diesem Fall darf nur der Datenverkehr, der mit dieser RBACL an den Endpunkt gesendet wird, TCP-Pakete zu 22 (SSH) und 23 (Telnet) sein.

Anmerkung: RBACL funktioniert nur in eine Richtung. Sofern der Datenrückverkehr keine

---

Richtlinie enthält, wird er mit der Standardrichtlinie durchgesetzt. Datenverkehr, der in die Fabric eingeht, wird nicht erzwungen. Der Datenverkehr wird mit dem auf dem Eingangsknoten bekannten SGT-Tag durch die Fabric gesendet. Sie wird nur erzwungen, wenn sie die Fabric verlässt, und sie muss für die Richtlinien erzwungen werden, die auf diesem Gerät vorhanden sind. In der Regel sind diese Richtlinien identisch, aber es ist möglich, die CTS-Domäne z. B. durch eine Firewall zu erweitern, bei der andere Richtlinien definiert werden könnten, hängt von den bereitgestellten Sicherheitsrichtlinien ab.

Führen Sie 'show cts role-based counters' aus, um zu überprüfen, ob Frames verworfen wurden oder nicht.

- Dieser Befehl zeigt die kumulierten Zähler für den gesamten Switch an. Für jede Schnittstelle ist kein entsprechender Befehl vorhanden.

<#root>

```
FE2067#
sh cts role-based counters

Role-based IPv4 counters
From    To      SW-Denied  HW-Denied  SW-Permitt HW-Permitt SW-Monitor HW-Monitor

*       *

0          0          3565235    7777106
   0          0

17      16

 0
         3          0          3412       0
         0

16      17

0          5812       0          871231     0
```

0

Diese Übersicht zeigt alle bekannten Einträge, die dem Switch in diesem Fall bekannt sind, um den Datenverkehr zwischen 17 und 16 und zwischen 16 und 17 abgleichen zu können.

- Jede andere Übereinstimmung, die unter das Sternchen (*) fällt und die Standardaktion erhält, wird angewendet. Wenn also Datenverkehr z. B. von 18 bis 16 kommt, stimmt er nicht mit der Matrix überein, die auf dem Switch bekannt ist, und es wird die Standardaktion angewendet.

Auch wenn die Zähler kumulativ sind, geben sie doch einen guten Hinweis darauf, ob Datenverkehr verloren geht.

- Um zu bestimmen, welcher Datenverkehr einen Eintrag treffen würde, kann das Schlüsselwort log auf dem ISE-Server zu den entsprechenden Richtlinien hinzugefügt werden. Dies führt dazu, dass der Switch Protokollmeldungen bereitstellt, wenn dieser Eintrag getroffen wird.
- Dies kann sowohl für die Standardaktion (* *) als auch für einen der spezifischeren Einträge in der Matrix erfolgen.

Zugehörige Informationen

- Technischer Support und Dokumentation für Cisco Systeme

Informationen zu dieser Übersetzung

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