

ASR 1000 OTV Multicast - Konfigurationsbeispiel

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[Netzwerkdiagramm mit grundlegender L2/L3-Verbindung](#)

[Grundlegende L2/L3-Verbindungen](#)

[OTV Multicast - Mindestkonfiguration](#)

[OTV-Verifizierung](#)

[Netzwerkdiagramm mit OTV](#)

[Überprüfungsbefehle und erwartete Ausgabe](#)

[Häufiges Problem](#)

[Fehlerbehebung](#)

[Erstellen einer Paketerfassung an der Join-Schnittstelle, um OTV Hellos anzuzeigen](#)

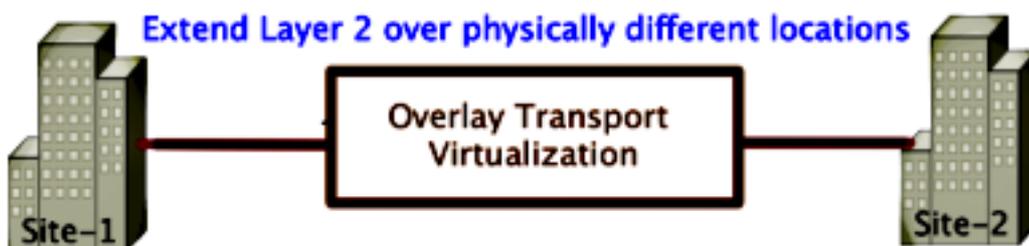
[Überprüfen Sie den Status der Weiterleitung auf dem OTV ASR.](#)

[Erstellen einer Paketerfassung auf der Join-Schnittstelle zum Anzeigen von OTV-Datenpaketen](#)

[Zugehörige Informationen](#)

Einführung

In diesem Dokument wird beschrieben, wie der Overlay Transport Virtualization (OTV)-Multicast-Modus auf der Cisco Aggregation Services Router (ASR) 1000-Plattform konfiguriert wird. OTV erweitert die Layer-2-Topologie (L2) über physisch unterschiedliche Standorte hinweg, sodass Geräte auf L2 über einen Layer-3-Provider (L3) kommunizieren können. Die Geräte in Site 1 glauben, dass sie sich in derselben Broadcast-Domäne befinden wie die Geräte in Site 2.



Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Konfiguration der Ethernet Virtual Connection (EVC)
- Grundlegende L2- und L3-Konfiguration auf der ASR-Plattform
- Grundkenntnisse der Konfiguration des Internet Group Management Protocol (IGMP) Version 3 und Protocol Independent Multicast (PIM)

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf dem ASR1002 mit der Cisco IOS® Version asr1000rp1-adventerprise.03.09.00.S.153-2.S.bin.

Ihr System muss die folgenden Anforderungen erfüllen, um die OTV-Funktion auf dem ASR 1000 zu implementieren:

- Cisco IOS-XE Version 3.5S oder höher
- MTU (Maximum Transmission Unit) größer/gleich 1542

Hinweis: OTV fügt allen gekapselten Paketen einen 42-Byte-Header mit dem DF-Bit (Do Not Fragment Bit) hinzu. Um 1500-Byte-Pakete durch das Overlay zu transportieren, muss das Transit-Netzwerk eine Maximum Transmission Unit (MTU) von 1542 oder höher unterstützen. Um eine Fragmentierung über OTV zu ermöglichen, müssen Sie die **Join-Interface** für die OTV-Fragmentierung aktivieren.

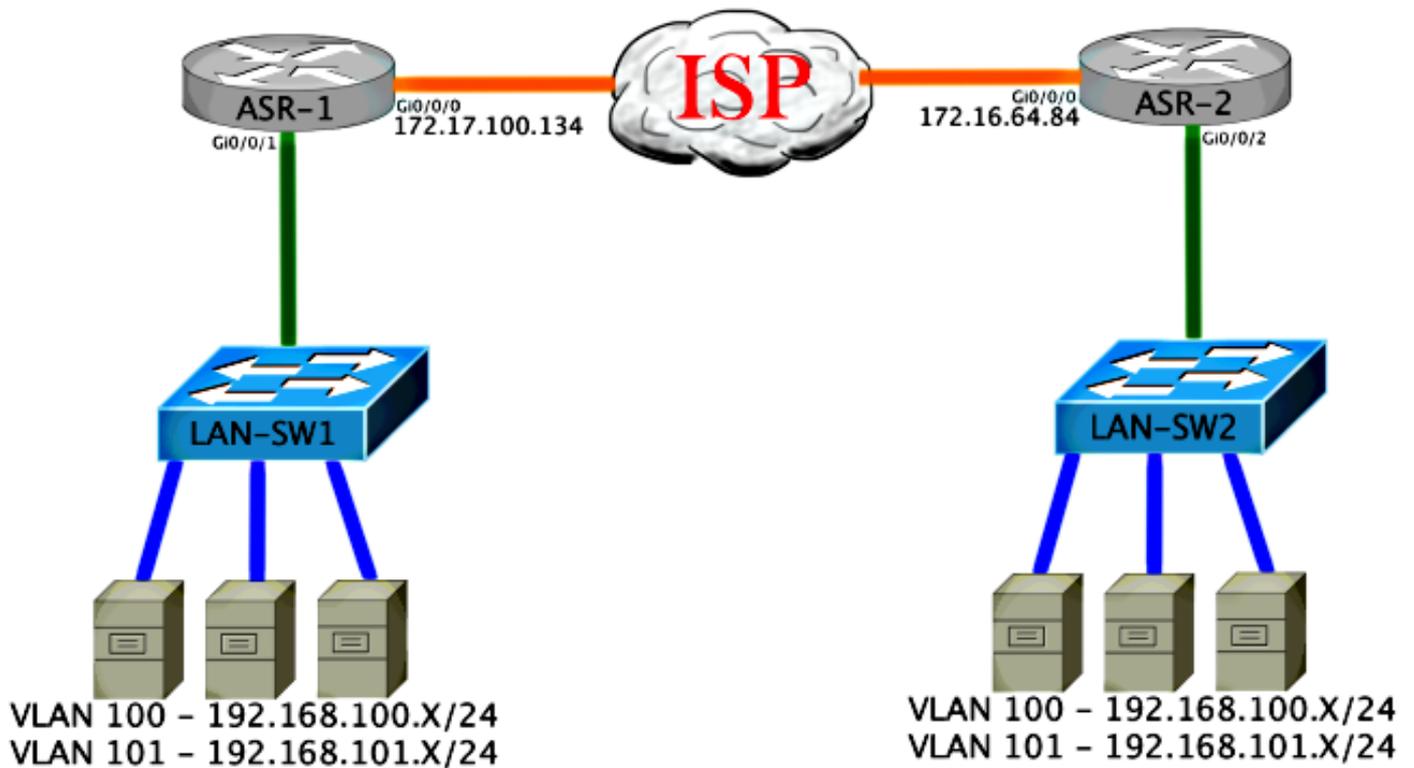
- Unicast- und Multicast-Erreichbarkeit zwischen Standorten

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konfigurieren

In diesem Abschnitt wird beschrieben, wie der OTV-Multicast-Modus konfiguriert wird.

Netzwerkdiagramm mit grundlegender L2/L3-Verbindung



Grundlegende L2/L3-Verbindungen

Beginnen Sie mit einer Basiskonfiguration. Die interne Schnittstelle auf dem ASR wird für Dienstinstanzen für den dot1q-Datenverkehr konfiguriert. Die OTV-Join-Schnittstelle ist die externe WAN-L3-Schnittstelle.

```
ASR-1
interface GigabitEthernet0/0/0
  description OTV-WAN-Connection
  mtu 9216
  ip address 172.17.100.134 255.255.255.0
  negotiation auto
  cdp enable
```

```
ASR-2
interface GigabitEthernet0/0/0
  description OTV-WAN-Connection
  mtu 9216
  ip address 172.16.64.84 255.255.255.0
  negotiation auto
  cdp enable
```

Da OTV einen 42-Byte-Header hinzufügt, müssen Sie sicherstellen, dass der Internet Service Provider (ISP) die MTU-Mindestgröße von einem Standort zum anderen übergibt. Um diese Überprüfung durchzuführen, senden Sie eine Paketgröße von 1542 mit festgelegtem DF-Bit. Dadurch erhält der ISP die Payload, die er benötigt, und die **Fragment**-Tags auf dem Paket **werden nicht** zur Simulation eines OTV-Pakets hinzugefügt. Wenn Sie keinen Ping ohne DF-Bit durchführen können, liegt ein Routing-Problem vor. Wenn Sie ohne Ping senden können, jedoch kein Ping mit festgelegtem DF-Bit durchführen können, liegt ein MTU-Problem vor. Sobald der Vorgang erfolgreich abgeschlossen ist, können Sie den OTV-Unicast-Modus zu den ASRs Ihrer Website hinzufügen.

```
ASR-1#ping 172.17.100.134 size 1542 df-bit
```

```
Type escape sequence to abort.
```

```
Sending 5, 1514-byte ICMP Echos to 172.17.100.134, timeout is 2 seconds:
```

```
Packet sent with the DF bit set
```

```
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
```

Die interne Schnittstelle ist ein L2-Port, der mit Dienstinstanzen für die mit L2 dot1q gekennzeichneten Pakete konfiguriert wurde. Außerdem wird eine interne Site Bridge-Domäne erstellt. In diesem Beispiel handelt es sich um das nicht gekennzeichnete VLAN1. Die interne Site Bridge-Domäne wird für die Kommunikation mehrerer OTV-Geräte am gleichen Standort verwendet. Auf diese Weise können sie kommunizieren und bestimmen, welches Gerät das Authoritative Edge Device (AED) ist, für das die Bridge-Domäne gilt.

Die Dienstinstanz muss in einer Bridge-Domäne konfiguriert werden, die das Overlay verwendet.

```
ASR-1
```

```
interface GigabitEthernet0/0/1
```

```
no ip address
```

```
negotiation auto
```

```
cdp enable
```

```
service instance 1 ethernet
```

```
encapsulation untagged
```

```
bridge-domain 1
```

```
!
```

```
service instance 50 ethernet
```

```
encapsulation dot1q 100
```

```
bridge-domain 200
```

```
!
```

```
service instance 51 ethernet
```

```
encapsulation dot1q 101
```

```
bridge-domain 201
```

```
ASR-2
```

```
interface GigabitEthernet0/0/2
```

```
no ip address
```

```
negotiation auto
```

```
cdp enable
```

```
service instance 1 ethernet
```

```
encapsulation untagged
```

```
bridge-domain 1
```

```
!
```

```
service instance 50 ethernet
```

```
encapsulation dot1q 100
```

```
bridge-domain 200
```

```
!
```

```
service instance 51 ethernet
```

```
encapsulation dot1q 101
```

```
bridge-domain 201
```

OTV Multicast - Mindestkonfiguration

Hierbei handelt es sich um eine Basiskonfiguration, die nur wenige Befehle zum Einrichten von OTV und zum Verbinden bzw. Herstellen interner Schnittstellen erfordert.

Konfigurieren Sie die lokale Site Bridge-Domäne. In diesem Beispiel ist es VLAN1 im LAN. Die Standort-ID ist für jeden physischen Standort spezifisch. In diesem Beispiel gibt es zwei voneinander unabhängige Remote-Standorte. Standort 1 und 2 werden entsprechend konfiguriert.

Multicast muss ebenfalls entsprechend der OTV-Anforderungen konfiguriert werden.

ASR-1

```
Config t
otv site bridge-domain 1
otv site-identifier 0000.0000.0001
ip multicast-routing distributed
ip pim ssm default
interface GigabitEthernet0/0/0
    ip pim passive
    ip igmp version 3
```

ASR-2

```
Config t
otv site bridge-domain 1
otv site-identifier 0000.0000.0002
ip multicast-routing distributed
ip pim ssm default
interface GigabitEthernet0/0/0
    ip pim passive
    ip igmp version 3
```

Erstellen Sie das Overlay für jede Seite. Konfigurieren Sie das Overlay, wenden Sie die Join-Schnittstelle an, und fügen Sie das Steuerelement und die Datengruppen zu jeder Seite hinzu.

Fügen Sie die beiden Bridge-Domänen hinzu, die Sie erweitern möchten. Beachten Sie, dass Sie die Site Bridge-Domäne nicht erweitern, sondern nur die beiden erforderlichen VLANs. Sie erstellen eine separate Dienstinstanz für die Overlay-Schnittstellen, um die Bridge-Domäne 200 und 201 aufzurufen. Wenden Sie die dot1q-Tags 100 bzw. 101 an.

ASR-1

```
Config t
interface Overlay1
    no ip address
    otv join-interface GigabitEthernet0/0/0
otv control-group 225.0.0.1 otv data-group 232.10.10.0/24
    service instance 10 ethernet
        encapsulation dot1q 100
        bridge-domain 200
    service instance 11 ethernet
        encapsulation dot1q 101
        bridge-domain 201
```

ASR-2

```
Config t
interface Overlay1
    no ip address
    otv join-interface GigabitEthernet0/0/0
otv control-group 225.0.0.1 otv data-group 232.10.10.0/24
    service instance 10 ethernet
        encapsulation dot1q 100
        bridge-domain 200
    service instance 11 ethernet
        encapsulation dot1q 101
```

Hinweis: Erweitern Sie das Standort-VLAN NICHT auf die Overlay-Schnittstelle. Dies führt dazu, dass die beiden ASRs einen Konflikt haben, da sie der Meinung sind, dass sich jede entfernte Seite am gleichen Standort befindet.

In dieser Phase ist die ASR-zu-ASR OTV-Multicast-Adjacency vollständig und funktionsfähig. Die Nachbarn sind vorhanden, und der ASR sollte für die VLANs, die erweitert werden müssen, AED-fähig sein.

ASR-1#**show otv**

```
Overlay Interface Overlay1
  VPN name           : None
  VPN ID             : 2
  State              : UP
  AED Capable        : Yes
  IPv4 control group : 225.0.0.1
  Mcast data group range(s): 232.10.10.0/24
  Join interface(s)  : GigabitEthernet0/0/0
  Join IPv4 address   : 172.17.100.134
  Tunnel interface(s) : Tunnel0
  Encapsulation format : GRE/IPv4
  Site Bridge-Domain : 1
  Capability          : Multicast-reachable
  Is Adjacency Server : No
  Adj Server Configured : No
  Prim/Sec Adj Svr(s) : None
```

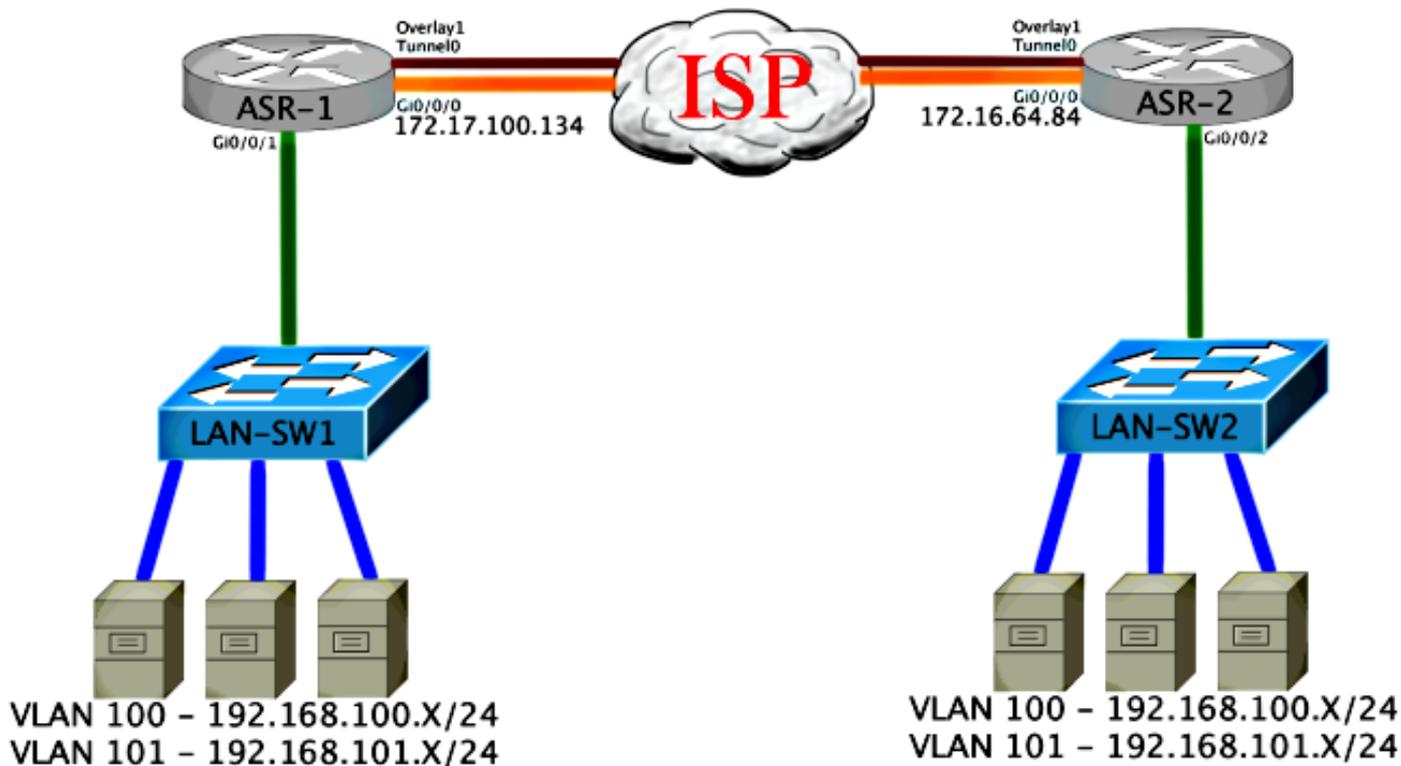
ASR-2#**show otv**

```
Overlay Interface Overlay1
  VPN name           : None
  VPN ID             : 2
  State              : UP
  AED Capable        : Yes
  IPv4 control group : 225.0.0.1
  Mcast data group range(s): 232.10.10.0/24
  Join interface(s)  : GigabitEthernet0/0/0
  Join IPv4 address   : 172.16.64.84
  Tunnel interface(s) : Tunnel0
  Encapsulation format : GRE/IPv4
  Site Bridge-Domain : 1
  Capability          : Multicast-reachable
  Is Adjacency Server : No
  Adj Server Configured : No
  Prim/Sec Adj Svr(s) : None
```

OTV-Verifizierung

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Netzwerkdiagramm mit OTV



Überprüfungsbefehle und erwartete Ausgabe

Diese Ausgabe zeigt, dass die VLANs 100 und 101 erweitert wurden. Der ASR ist die AED, und in der Ausgabe werden die interne Schnittstelle und die Service-Instanz angezeigt, die die VLANs zuordnet.

```
ASR-1#show otv vlan
```

```
Key: SI - Service Instance
```

```
Overlay 1 VLAN Configuration Information
```

Inst	VLAN	Bridge-Domain	Auth	Site Interface(s)
0	100	200	yes	Gi0/0/1:SI50
0	101	201	yes	Gi0/0/1:SI51

```
Total VLAN(s): 2
```

```
Total Authoritative VLAN(s): 2
```

```
ASR-2#show otv vlan
```

```
Key: SI - Service Instance
```

```
Overlay 1 VLAN Configuration Information
```

Inst	VLAN	Bridge-Domain	Auth	Site Interface(s)
0	100	200	yes	Gi0/0/2:SI50
0	101	201	yes	Gi0/0/2:SI51

```
Total VLAN(s): 2
```

```
Total Authoritative VLAN(s): 2
```

Zur Validierung erweitern Sie die VLANs, und führen Sie einen Site-to-Site-Ping aus. Host 192.168.100.2 befindet sich an Standort 1, Host 192.168.100.3 befindet sich an Standort 2. Die ersten Pings werden vermutlich fehlschlagen, wenn Sie das Address Resolution Protocol (ARP) lokal und über OTV auf der anderen Seite erstellen.

```
LAN-SW1#ping 192.168.100.3
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.100.3, timeout is 2 seconds:
....!!
Success rate is 40 percent (2/5), round-trip min/avg/max = 1/5/10 ms
```

```
LAN-SW1#ping 192.168.100.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.100.3, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/10 ms
```

```
LAN-SW1#ping 192.168.100.3 size 1500 df-bit
Type escape sequence to abort.
Sending 5, 1500-byte ICMP Echos to 192.168.100.3, timeout is 2 seconds:
Packet sent with the DF bit set
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/10 ms
```

Um sicherzustellen, dass die MAC-Tabelle und die OTV-Routing-Tabellen korrekt mit dem lokalen Gerät erstellt werden, sollten Sie die MAC-Adresse des Remote-Geräts mithilfe des Befehls **show otv route** ermitteln.

```
LAN-SW1#show int vlan 100
Vlan100 is up, line protocol is up
  Hardware is Ethernet SVI, address is 0c27.24cf.abd1 (bia 0c27.24cf.abd1)
  Internet address is 192.168.100.2/24
```

```
LAN-SW2#show int vlan 100
Vlan100 is up, line protocol is up
  Hardware is Ethernet SVI, address is b4e9.b0d3.6a51 (bia b4e9.b0d3.6a51)
  Internet address is 192.168.100.3/24
```

```
ASR-1#show otv route vlan 100
```

```
Codes: BD - Bridge-Domain, AD - Admin-Distance,
       SI - Service Instance, * - Backup Route
```

```
OTV Unicast MAC Routing Table for Overlay1
```

Inst	VLAN	BD	MAC Address	AD	Owner	Next Hops(s)
0	100	200	0c27.24cf.abaf	40	BD Eng	Gi0/0/1:SI50
0	100	200	0c27.24cf.abd1	40	BD Eng	Gi0/0/1:SI50 <--- Local mac is pointing to the physical interface
0	100	200	b4e9.b0d3.6a04	50	ISIS	ASR-2
0	100	200	b4e9.b0d3.6a51	50	ISIS	ASR-2 <--- Remote mac is pointing across OTV to ASR-2

```
4 unicast routes displayed in Overlay1
```

```
-----
4 Total Unicast Routes Displayed
```

```
ASR-2#show otv route vlan 100
```

```
Codes: BD - Bridge-Domain, AD - Admin-Distance,
       SI - Service Instance, * - Backup Route
```

OTV Unicast MAC Routing Table for Overlay1

```
Inst VLAN BD      MAC Address      AD      Owner  Next Hops(s)
-----
0   100  200    0c27.24cf.abaf 50      ISIS   ASR-1
0   100  200    0c27.24cf.abd1 50      ISIS   ASR-1      <--- Remote mac is
pointing across OTV to ASR-1
0   100  200    b4e9.b0d3.6a04 40      BD Eng Gi0/0/2:SI50
0   100  200    b4e9.b0d3.6a51 40      BD Eng Gi0/0/2:SI50  <--- Local mac is
pointing to the physical interface
```

4 unicast routes displayed in Overlay1

4 Total Unicast Routes Displayed

Häufiges Problem

Die Fehlermeldung OTV Not Form (OTV wird nicht gesendet) in der Ausgabe zeigt, dass der ASR nicht AED-fähig ist. Das bedeutet, dass der ASR die VLANs nicht über das OTV weiterleitet. Es gibt mehrere mögliche Ursachen, aber die häufigste ist, dass die ASRs keine Verbindung zwischen den Standorten haben. Überprüfen Sie, ob L3-Verbindungen vorhanden und möglicherweise blockierter Multicast-Datenverkehr vorhanden sind. Eine weitere mögliche Ursache für diese Bedingung ist, dass die interne Site Bridge-Domäne nicht konfiguriert ist. Dies schafft eine Bedingung, bei der der ASR nicht zum AED werden kann, da nicht sicher ist, ob er der einzige ASR auf dem Standort ist oder nicht.

ASR-1#**show otv**

```
Overlay Interface Overlay1
  VPN name           : None
  VPN ID             : 2
  State              : UP
  AED Capable        : No, overlay DIS not elected      <--- Not Forwarding
  IPv4 control group : 225.0.0.1
  Mcast data group range(s): 232.0.0.0/8
  Join interface(s)  : GigabitEthernet0/0/0
  Join IPv4 address  : 172.17.100.134
  Tunnel interface(s): Tunnel0
  Encapsulation format : GRE/IPv4
  Site Bridge-Domain : 1
  Capability          : Multicast-reachable
  Is Adjacency Server : No
  Adj Server Configured : No
  Prim/Sec Adj Svr(s) : None
```

ASR-2#**show otv**

```
Overlay Interface Overlay1
  VPN name           : None
  VPN ID             : 2
  State              : UP
  AED Capable        : No, overlay DIS not elected      <--- Not Forwarding
  IPv4 control group : 225.0.0.1
  Mcast data group range(s): 232.0.0.0/8
  Join interface(s)  : GigabitEthernet0/0/0
  Join IPv4 address  : 172.16.64.84
  Tunnel interface(s): Tunnel0
  Encapsulation format : GRE/IPv4
  Site Bridge-Domain : 1
```

```
Capability : Multicast-reachable
Is Adjacency Server : No
Adj Server Configured : No
Prim/Sec Adj Svr(s) : None
```

Fehlerbehebung

Dieser Abschnitt enthält Informationen, die Sie zur Fehlerbehebung bei Ihrer Konfiguration verwenden können.

Erstellen einer Paketerfassung an der Join-Schnittstelle, um OTV Hellos anzuzeigen

Sie können das integrierte Paketerfassungsgerät im ASR verwenden, um mögliche Probleme zu beheben.

Erstellen Sie eine Zugriffskontrollliste (ACL), um die Auswirkungen und die Aufnahme von Dateien mit hoher Sättigung zu minimieren. Die Konfiguration ist so eingerichtet, dass nur die Multicast-Hellos zwischen zwei Standorten erfasst werden. Passen Sie Ihre IP-Adresse an die Join-Schnittstellen der Nachbarn an.

```
ip access-list extended CAPTURE
 permit ip host 172.16.64.84 host 225.0.0.1
 permit ip host 172.17.100.134 host 225.0.0.1
```

Richten Sie die Erfassung ein, um die Join-Schnittstelle in beide Richtungen auf beiden ASRs zu schnüffeln:

```
monitor capture 1 buffer circular access-list CAPTURE interface g0/0/0 both
```

Um die Erfassung zu starten, geben Sie Folgendes ein:

```
monitor capture 1 start
```

```
*Nov 14 15:21:37.746: %BUFCAP-6-ENABLE: Capture Point 1 enabled.
```

```
<wait a few min>
```

```
monitor capture 1 stop
```

```
*Nov 14 15:22:03.213: %BUFCAP-6-DISABLE: Capture Point 1 disabled.
```

```
show mon cap 1 buffer brief
```

Die Pufferausgabe zeigt, dass die Hellos in der Erfassung die erfasste Schnittstelle ausgehen. Es zeigt die Hellos, die für die Multicast-Adresse 225.0.0.1 bestimmt sind. Dies ist die konfigurierte Kontrollgruppe. Sehen Sie sich die ersten 13 Pakete in der Erfassung an, und beachten Sie, dass es nur eine unidirektionale Ausgabe gibt. Hellos von 172.17.100.134 sind nur sichtbar. Sobald das Multicast-Problem im Core behoben ist, wird der Nachbarn hello unter Paketnummer 14 angezeigt.

```
ASR-1#show mon cap 1 buff bri
```

```
-----
```

```

#   size   timestamp      source                destination  protocol
-----
0 1456    0.000000  172.17.100.134    -> 225.0.0.1      GRE
1 1456    8.707016  172.17.100.134    -> 225.0.0.1      GRE
2 1456   16.880011  172.17.100.134    -> 225.0.0.1      GRE
3 1456   25.873008  172.17.100.134    -> 225.0.0.1      GRE
4 1456   34.645023  172.17.100.134    -> 225.0.0.1      GRE
5 1456   44.528024  172.17.100.134    -> 225.0.0.1      GRE
6 1456   52.137002  172.17.100.134    -> 225.0.0.1      GRE
7 1456   59.819010  172.17.100.134    -> 225.0.0.1      GRE
8 1456   68.641025  172.17.100.134    -> 225.0.0.1      GRE
9 1456   78.168998  172.17.100.134    -> 225.0.0.1      GRE
10 1456  85.966005  172.17.100.134    -> 225.0.0.1      GRE
11 1456  94.629032  172.17.100.134    -> 225.0.0.1      GRE
12 1456 102.370043  172.17.100.134    -> 225.0.0.1      GRE
13 1456 110.042005  172.17.100.134    -> 225.0.0.1      GRE
14 1456 111.492031  172.16.64.84    -> 225.0.0.1      GRE <---Mcast core
fixed and now see neighbor hellos
15 1456 111.493038  172.17.100.134    -> 225.0.0.1      GRE
16 1456 112.491039  172.16.64.84      -> 225.0.0.1      GRE
17 1456 112.501033  172.17.100.134    -> 225.0.0.1      GRE
18 116   112.519037  172.17.100.134    -> 225.0.0.1      GRE
19 114   112.615026  172.16.64.84      -> 225.0.0.1      GRE
20 114   112.618031  172.17.100.134    -> 225.0.0.1      GRE
21 1456 113.491039  172.16.64.84      -> 225.0.0.1      GRE
22 1456 115.236047  172.17.100.134    -> 225.0.0.1      GRE
23 142   116.886008  172.17.100.134    -> 225.0.0.1      GRE
24 102   117.290045  172.17.100.134    -> 225.0.0.1      GRE
25 1456 118.124002  172.17.100.134    -> 225.0.0.1      GRE
26 1456 121.192043  172.17.100.134    -> 225.0.0.1      GRE
27 1456 122.443037  172.16.64.84      -> 225.0.0.1      GRE
28 1456 124.497035  172.17.100.134    -> 225.0.0.1      GRE
29 102   126.178052  172.17.100.134    -> 225.0.0.1      GRE
30 142   126.629032  172.17.100.134    -> 225.0.0.1      GRE
31 1456 127.312047  172.17.100.134    -> 225.0.0.1      GRE
32 1456 130.029997  172.17.100.134    -> 225.0.0.1      GRE
33 1456 131.165000  172.16.64.84      -> 225.0.0.1      GRE
34 1456 132.591025  172.17.100.134    -> 225.0.0.1      GRE
35 102   134.832010  172.17.100.134    -> 225.0.0.1      GRE
36 1456 135.856010  172.17.100.134    -> 225.0.0.1      GRE
37 142   136.174054  172.17.100.134    -> 225.0.0.1      GRE
38 1456 138.442030  172.17.100.134    -> 225.0.0.1      GRE
39 1456 140.769025  172.16.64.84      -> 225.0.0.1      GRE
40 1456 141.767010  172.17.100.134    -> 225.0.0.1      GRE
41 102   144.277046  172.17.100.134    -> 225.0.0.1      GRE
42 1456 144.996003  172.17.100.134    -> 225.0.0.1      GRE

```

ASR-1#

2#show mon cap 1 buff bri

Überprüfen Sie den Status der Weiterleitung auf dem OTV ASR.

Wenn Sie den Multicast-Routing-Status zwischen OTV-Nachbarn erstellen, müssen Sie über den richtigen PIM-Status verfügen. Verwenden Sie diesen Befehl, um den erwarteten PIM-Status auf den ASRs zu überprüfen:

ASR-1#show otv

Overlay Interface Overlay1

```

VPN name      : None
VPN ID        : 2
State         : UP

```

```

AED Capable           : No, overlay DIS not elected
IPv4 control group    : 225.0.0.1
Mcast data group range(s) : 232.0.0.0/8
Join interface(s)     : GigabitEthernet0/0/0
Join IPv4 address     : 172.17.100.134
Tunnel interface(s)  : Tunnel0
Encapsulation format  : GRE/IPv4
Site Bridge-Domain   : 1
Capability            : Multicast-reachable
Is Adjacency Server   : No
Adj Server Configured : No
Prim/Sec Adj Svr(s)  : None

```

Beachten Sie den gleichen Fehler wie zuvor: AED-fähig = Nein, Overlay DIS nicht gewählt. Das bedeutet, dass der ASR nicht zum AED-Forwarder werden kann, da er nicht über genügend Informationen zu seinem Peer verfügt. Es ist möglich, dass die interne Schnittstelle nicht aktiv ist, die Site-Bridge-Domäne deaktiviert/nicht erstellt wurde oder die beiden Standorte einander über den ISP nicht sehen.

ASR-1 erkennt das Problem. Es zeigt, dass keine PIM-Nachbarn sichtbar sind. Dies ist auch bei einer erfolgreichen Umsetzung zu erwarten. Dies liegt daran, dass PIM passiv auf der Join-Schnittstelle ausgeführt wird. PIM passive ist der einzige PIM-Modus, der auf der Join-Schnittstelle für OTV unterstützt wird.

```
ASR-1#show ip pim neigh
```

```
PIM Neighbor Table
```

```
Mode: B - Bidir Capable, DR - Designated Router, N - Default DR Priority,
      P - Proxy Capable, S - State Refresh Capable, G - GenID Capable
```

```
Neighbor      Interface      Uptime/Expires   Ver   DR
Address                               Prio/Mode
```

Um zu überprüfen, ob PIM-Schnittstellen auf dem ASR-1 konfiguriert sind, geben Sie Folgendes ein:

```
ASR-1#show ip pim int
```

```
Address          Interface          Ver/   Nbr   Query  DR    DR
                  Mode      Count  Intvl Prior
172.17.100.134   GigabitEthernet0/0/0  v2/P   0     30     1     172.17.100.134
172.17.100.134   Tunnel0             v2/P   0     30     1     172.17.100.134
0.0.0.0          Overlay1            v2/P   0     30     1     0.0.0.0
```

Der mroute-Status des ASR bietet eine Vielzahl von Informationen zum Multicast-Status der Verbindung. In dieser Ausgabe wird der Nachbar in der lokalen ASR-Routing-Tabelle nicht als S,G-Eintrag angezeigt. Wenn Sie die mroute-Anzahl für die Steuerelementgruppe anzeigen, wird nur die lokale Join-Schnittstelle als Quelle angezeigt. Beachten Sie, dass die Anzahl den Paketen entspricht, die mit der weitergeleiteten Gesamtzahl empfangen wurden. Dies bedeutet, dass Sie auf der lokalen Seite aktiv sind und die Multicast-Domäne weiterleiten.

```
ASR-1#show ip mroute
```

```
IP Multicast Routing Table
```

```
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry, 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,
Q - Received BGP S-A Route, q - Sent BGP S-A Route,
V - RD & Vector, v - Vector

Outgoing interface flags: H - Hardware switched, A - Assert winner
Timers: Uptime/Expires
Interface state: Interface, Next-Hop or VCD, State/Mode

(*, 225.0.0.1), 00:20:29/stopped, RP 0.0.0.0, flags: DC
Incoming interface: Null, RPF nbr 0.0.0.0
Outgoing interface list:
Tunnel0, Forward/Sparse-Dense, 00:20:29/00:02:55
GigabitEthernet0/0/0, Forward/Sparse-Dense, 00:20:29/Proxy

(172.17.100.134, 225.0.0.1), 00:16:25/00:02:19, flags: T
Incoming interface: GigabitEthernet0/0/0, RPF nbr 0.0.0.0
Outgoing interface list:
GigabitEthernet0/0/0, Forward/Sparse-Dense, 00:16:25/Proxy
Tunnel0, Forward/Sparse-Dense, 00:16:25/00:02:55

(*, 224.0.1.40), 00:20:09/00:02:53, RP 0.0.0.0, flags: DPC
Incoming interface: Null, RPF nbr 0.0.0.0
Outgoing interface list: Null

ASR-1#show ip mroute count

Use "show ip mfib count" to get better response time for a large number of mroutes.

IP Multicast Statistics

3 routes using 1828 bytes of memory
2 groups, 0.50 average sources per group
Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kilobits per second
Other counts: Total/RPF failed/Other drops(OIF-null, rate-limit etc)

Group: 225.0.0.1, Source count: 1, Packets forwarded: 116, Packets received: 117
Source: 172.17.100.134/32, Forwarding: 116/0/1418/1, Other: 117/1/0

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

Wenn das Multicast-Kernproblem gelöst ist, wird die erwartete Ausgabe vom ASR angezeigt.

ASR-1#show otv

Overlay Interface Overlay1
VPN name : None
VPN ID : 2
State : UP
AED Capable : Yes
IPv4 control group : 225.0.0.1
Mcast data group range(s): 232.0.0.0/8
Join interface(s) : GigabitEthernet0/0/0
Join IPv4 address : 172.17.100.134
Tunnel interface(s) : Tunnel0
Encapsulation format : GRE/IPv4
Site Bridge-Domain : 1
Capability : Multicast-reachable
Is Adjacency Server : No
Adj Server Configured : No
Prim/Sec Adj Svr(s) : None

Es gibt immer noch keine PIM-Nachbarn, und die physischen, Overlay- und Tunnelschnittstellen sind lokale PIM-Schnittstellen.

ASR-1#show ip pim neigh

PIM Neighbor Table

Mode: B - Bidir Capable, DR - Designated Router, N - Default DR Priority,
 P - Proxy Capable, S - State Refresh Capable, G - GenID Capable
 Neighbor Interface Uptime/Expires Ver DR
 Address Prio/Mode
 ASR-1#show ip pim int

Address	Interface	Ver/ Mode	Nbr Count	Query Intvl	DR Prior	DR
172.17.100.134	GigabitEthernet0/0/0	v2/P	0	30	1	172.17.100.134
172.17.100.134	Tunnel0	v2/P	0	30	1	172.17.100.134
0.0.0.0	Overlay1	v2/P	0	30	1	0.0.0.0

Die mroute-Tabelle und die Zähler stellen Informationen über den Multicast-Status bereit. Die Ausgabe zeigt die Join-Schnittstelle sowie den OTV-Nachbarn in der Kontrollgruppe als Quellen an. Stellen Sie sicher, dass Sie den Rendezvous Point (RP) auch im Feld Reverse Path Forwarding (RPF) Neighbor (NBR) des Remote-Standorts sehen. Sie leiten außerdem übereinstimmende Zähler weiter und empfangen diese. Die beiden Quellen sollten die Gesamtzahl der empfangenen Gruppen insgesamt angeben.

ASR-1#show ip mroute

IP Multicast Routing Table

Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
 L - Local, P - Pruned, R - RP-bit set, F - Register flag,
 T - SPT-bit set, J - Join SPT, M - MSDP created entry, 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,
 Q - Received BGP S-A Route, q - Sent BGP S-A Route,
 V - RD & Vector, v - Vector

Outgoing interface flags: H - Hardware switched, A - Assert winner

Timers: Uptime/Expires

Interface state: Interface, Next-Hop or VCD, State/Mode

(* , 225.0.0.1), 00:25:16/stopped, RP 0.0.0.0, flags: DC
 Incoming interface: Null, RPF nbr 0.0.0.0
 Outgoing interface list:
 Tunnel0, Forward/Sparse-Dense, 00:25:16/00:02:06
 GigabitEthernet0/0/0, Forward/Sparse-Dense, 00:25:16/Proxy

(172.16.64.84, 225.0.0.1), 00:04:09/00:02:50, flags: T
 Incoming interface: GigabitEthernet0/0/0, **RPF nbr 172.17.100.1**
 Outgoing interface list:
 Tunnel0, Forward/Sparse-Dense, 00:04:09/00:02:06

(172.17.100.134, 225.0.0.1), 00:21:12/00:01:32, flags: T
 Incoming interface: GigabitEthernet0/0/0, **RPF nbr 0.0.0.0**
 Outgoing interface list:
 GigabitEthernet0/0/0, Forward/Sparse-Dense, 00:21:12/Proxy
 Tunnel0, Forward/Sparse-Dense, 00:21:12/00:02:06

(* , 224.0.1.40), 00:24:56/00:02:03, RP 0.0.0.0, flags: DPC
 Incoming interface: Null, RPF nbr 0.0.0.0
 Outgoing interface list: Null

ASR-1#show ip mroute count

Use "show ip mfib count" to get better response time for a large number of mroutes.

IP Multicast Statistics

4 routes using 2276 bytes of memory

2 groups, 1.00 average sources per group

Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kilobits per second
Other counts: Total/RPF failed/Other drops(OIF-null, rate-limit etc)

Group: 225.0.0.1, Source count: 2, **Packets forwarded: 295**, Packets received:
297<----- **32 + 263 = 295**
Source: 172.16.64.84/32, Forwarding: 32/0/1372/1, Other: 32/0/0
Source: 172.17.100.134/32, Forwarding: 263/0/1137/3, Other: 264/1/0

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

Erstellen einer Paketerfassung auf der Join-Schnittstelle zum Anzeigen von OTV-Datenpaketen

Da OTV gekapselter Datenverkehr ist, wird er als Generic Routing Encapsulation (GRE)-Datenverkehr mit einer Quelle der Join-Schnittstelle zum Ziel der Remote-Join-Schnittstelle angesehen. Es gibt nicht viel, was Sie tun können, um den Datenverkehr speziell zu sehen. Eine Möglichkeit zur Überprüfung, ob Ihr Datenverkehr über OTV verläuft, besteht darin, eine Paketerfassung einzurichten, insbesondere mit einer Paketgröße, die von Ihren aktuellen Datenverkehrsmustern unabhängig ist. In diesem Beispiel können Sie ein ICMP-Paket (Internet Control Message Protocol) mit einer Größe von 700 angeben und festlegen, was aus der Erfassung herausgefiltert werden kann. Dies kann verwendet werden, um zu überprüfen, ob ein Paket über die OTV-Cloud übertragen wird.

Um den Access List Filter zwischen Ihren beiden Join-Schnittstellen einzurichten, geben Sie Folgendes ein:

```
ip access-list extended CAPTURE
 permit ip host 172.17.100.134 host 172.16.64.84
```

Geben Sie Folgendes ein, um die Überwachungssitzung so einzurichten, dass die angegebene Größe von 756 herausgefiltert wird:

```
monitor capture 1 buffer size 1 access-list CAPTURE limit packet-len 756
interface g0/0/0 out
```

Um die Erfassung zu starten, geben Sie Folgendes ein:

```
ASR-1#mon cap 1 start
*Nov 18 12:45:50.162: %BUFCAP-6-ENABLE: Capture Point 1 enabled.
```

Senden Sie das spezifische Ping mit einer angegebenen Größe. Da OTV einen 42-Byte-Header zusammen mit einem 8-Byte-ICMP mit einem 20-Byte-IP-Header hinzufügt, können Sie einen Ping mit einer Größe von 700 senden und erwarten, dass die Daten mit einer Paketgröße von 756 in die OTV-Cloud gelangen.

```
LAN-Sw2#ping 192.168.100.2 size 700 repeat 100
Type escape sequence to abort.
Sending 100, 700-byte ICMP Echos to 192.168.100.2, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 10/19/30 ms
```

Um die Erfassung zu stoppen, geben Sie Folgendes ein:

```
ASR-1#mon cap 1 stop
```

*Nov 18 12:46:02.084: %BUFCAP-6-DISABLE: Capture Point 1 disabled.

Im Erfassungspuffer sehen Sie, dass alle 100 Pakete die Erfassung auf der lokalen Seite erreichen. Sie sollten sehen, dass alle 100 Pakete auch die Außenseite erreichen. Andernfalls ist in der OTV-Cloud eine weitere Untersuchung auf Paketverluste erforderlich.

ASR-1#show mon cap 1 buff bri

```
-----  
#   size  timestamp      source           destination      protocol  
-----  
0   756    0.000000    172.17.100.134  -> 172.16.64.84    GRE  
1   756    0.020995    172.17.100.134  -> 172.16.64.84    GRE  
2   756    0.042005    172.17.100.134  -> 172.16.64.84    GRE  
3   756    0.052991    172.17.100.134  -> 172.16.64.84    GRE  
<Output Omitted>  
97  756    1.886999    172.17.100.134  -> 172.16.64.84    GRE  
98  756    1.908009    172.17.100.134  -> 172.16.64.84    GRE  
99  756    1.931003    172.17.100.134  -> 172.16.64.84    GRE
```

Hinweis: Dieser Test ist nicht zu 100 % zuverlässig, da jeder Datenverkehr, der der Länge von 756 entspricht, erfasst wird. Verwenden Sie ihn daher mit Vorsicht. Dieser Test dient dazu, Datenpunkte nur bei möglichen OTV-Kernproblemen zu sammeln.

Zugehörige Informationen

- [Konfigurieren der Overlay Transport Virtualization](#)
- [Ethernet Virtual Circuits \(EVC\)](#)
- [Technischer Support und Dokumentation - Cisco Systems](#)