ASR 1000 OTV Multicast Configuration Example

Document ID: 117157

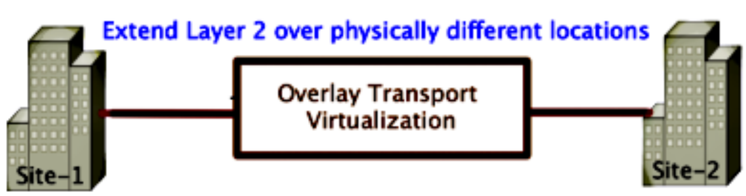
Contributed by Denny McLaughlin, Cisco TAC Engineer.

Apr 25, 2014

Contents

Introduction

This document describes how to configure Overlay Transport Virtualization (OTV) multicast mode on the Cisco Aggregation Services Router (ASR) 1000 platform. OTV extends the Layer 2 (L2) topology across the physically different sites, which allows devices to communicate at L2 across a Layer 3 (L3) provider. Devices in Site 1 believe they are on the same broadcast domain as those in Site 2.



Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Ethernet Virtual Connection (EVC) configuration
- Basic L2 and L3 configuration on the ASR platform

* Basic Internet Group Management Protocol (IGMP) Version 3 and Protocol Independent Multicast (PIM) configuration knowledge

Components Used

The information in this document is based on the ASR1002 with Cisco IOS® Version asr1000rp1−adventerprise.03.09.00.S.153−2.S.bin.

Your system must have these requirements in order to implement the OTV feature on the ASR 1000:

* Cisco IOS−XE Version 3.5S or later
* Maximum Transmission Unit (MTU) of 1542 or higher

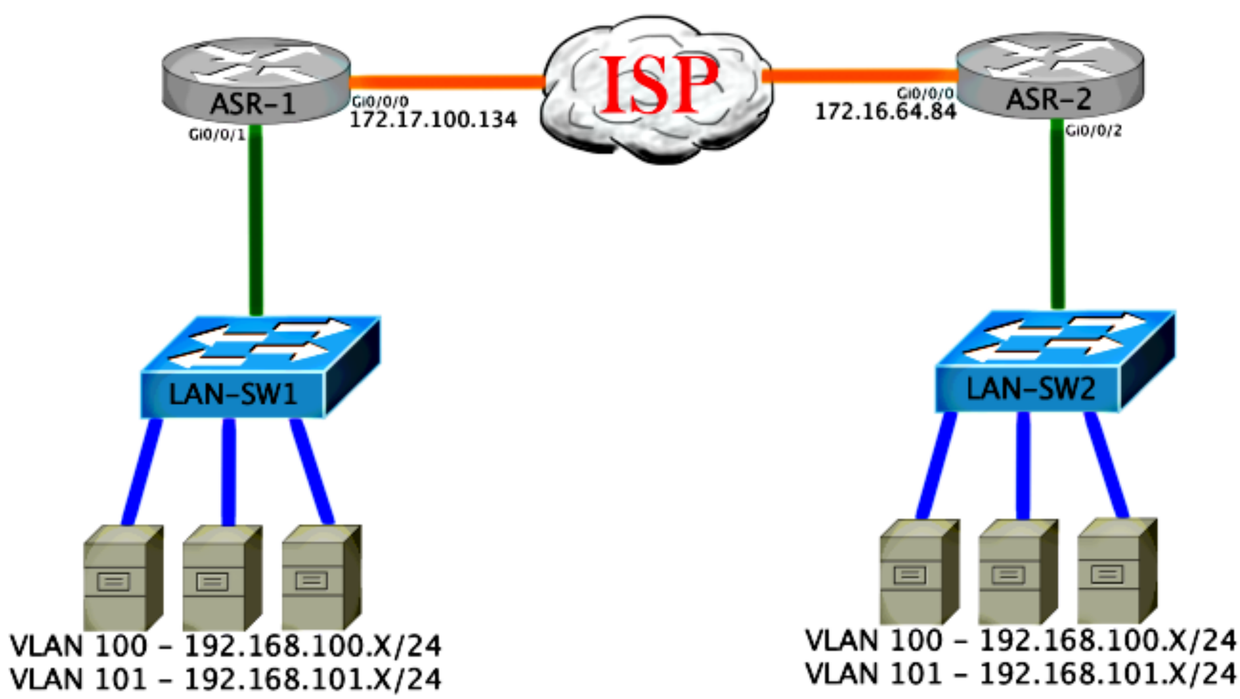
  Note: OTV adds a 42−byte header with the Do Not Fragment bit (DF−bit) to all encapsulated packets. In order to transport 1500−byte packets through the overlay, the transit network must support a Maximum Transmission Unit (MTU) of 1542 or higher. In order to allow for fragmentation accross OTV, you must enable ***otv fragmentation join−interface*** <interface>.
* Unicast and multicast reachability between sites

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configure

This section describes how to configure OTV multicast mode.

Network Diagram with Basic L2/L3 Connectivity



Basic L2/L3 Connectivity

Start with a base configuration. The internal interface on the ASR is configured for service instances for dot1q traffic. The OTV join interface is the external WAN L3 interface.

```
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
```

Since OTV adds a 42-byte header, you must verify that the Internet Service Provider (ISP) passes the minimum MTU size from site-to-site. In order to accomplish this verification, send a packet size of 1542 with the DF-bit set. This gives the ISP the payload required plus the ***do not fragment*** tag on the packet in order to simulate an OTV packet. If you cannot ping without the DF-bit, then you have a routing problem. If you can ping without it, but cannot ping with the DF-bit set, you have an MTU problem. Once successful, you are ready to add OTV unicast mode to your site ASRs.

```
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
```

The internal interface is a L2 port configured with service instances for the L2 dot1q tagged packets. It also builds an internal site bridge domain. In this example, it is the untagged VLAN1. The internal site bridge domain is used for the communication of multiple OTV devices at the same site. This allows them to communicate and determine which device is the Authoritative Edge Device (AED) for which bridge domain.

The service instance must be configured into a bridge domain that uses the overlay.

```
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 Minimum Configuration

This is a basic configuration that requires only a few commands in order to set up OTV and join / internal interfaces.

Configure the local site bridge domain. In this example, it is VLAN1 on the LAN. The site identifier is specific to each physical location. In this example, there are two remote locations that are physically independent of each other. Site 1 and Site 2 are configured accordingly. Multicast also must be configured in accordance with the requirements for OTV.

```
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
```

Build the overlay for each side. Configure the overlay, apply the join interface, and add the control and data groups to each side.

Add the two bridge domains that you want to extend. Notice that you do not extend the site bridge domain, only the two VLANs needed. You build a separate service instance for the overlay interfaces to call the bridge domain 200 and 201. Apply the dot1q tags 100 and 101 respectively.

```
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
    bridge-domain 201
```

Note: Do NOT extend the site VLAN on the overlay interface. This causes the two ASRs to have a conflict because they believe each remote side is in the same site.

At this stage, ASR to ASR OTV multicast adjacency is complete and functional. The neighbors are found, and the ASR should be AED−capable for the VLANs that need to be extended.

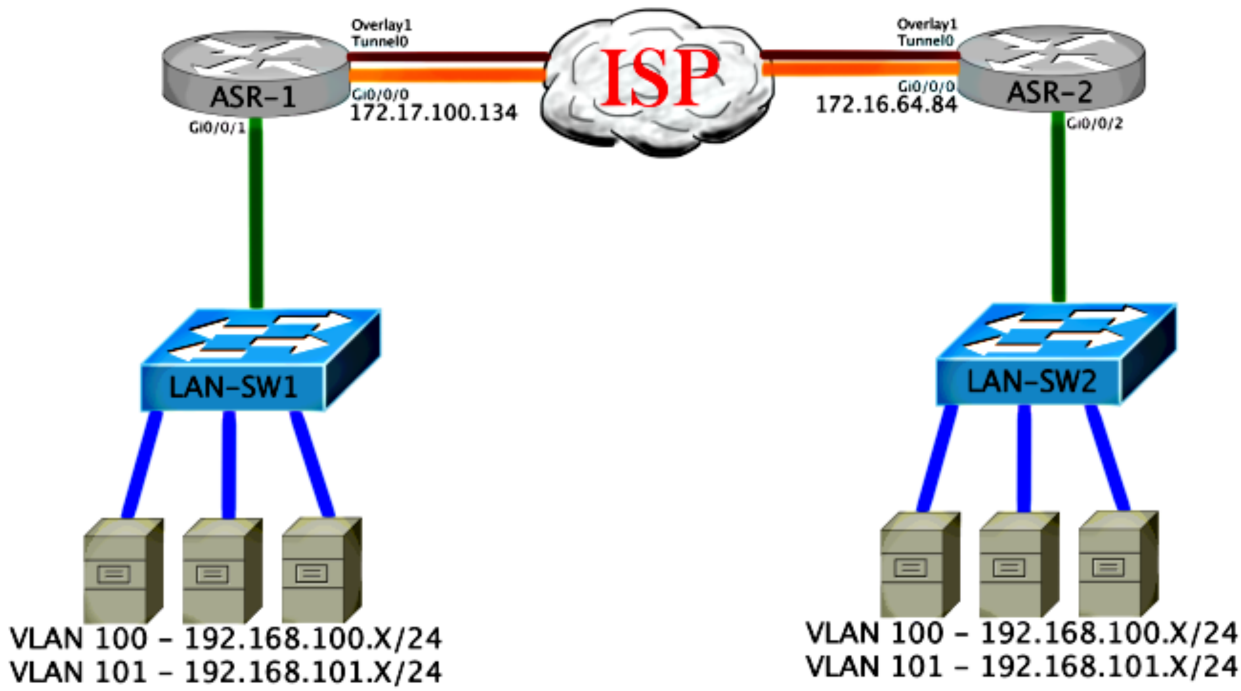
```
ASR-1#show otv
Overlay Interface Overlay1
 VPN name                  : None
 VPN ID                    : 2
 State                     : UP
 AED Capable               : Yes
 IPv4 control group        : 225.0.0.1
 Mcast data group range(s): 232.10.10.0/24
 Join interface(s)         : GigabitEthernet0/0/0
 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 Verification

Use this section in order to confirm that your configuration works properly.

Network Diagram with OTV



Verification Commands and Expected Output

This output shows that VLANs 100 and 101 are extended. The ASR is the AED, and the internal interface and Service Instance that maps the VLANs are displayed in the output.

```
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
```

In order to validate, extend the VLANs, and perform a site−to−site ping. Host 192.168.100.2 is located at Site 1, and Host 192.168.100.3 is located at Site 2. The first few pings are expected to fail as you build Address Resolution Protocol (ARP) locally and across OTV to the other side.

```
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
```

In order to ensure that the MAC table and OTV routing tables are built properly with the local device, learn the MAC address of the remote device with the use of the ***show otv route*** command.

```
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
```

Common Problem

The OTV Does Not Form error message in the output shows that the ASR is not AED−capable. This means that the ASR does not forward the VLANS across the OTV. There are several possible causes for this, but the most common is that the ASRs do not have connectivity between sites. Check for L3 connectivity and possible blocked multicast traffic. Another possible cause of this condition is when the internal site bridge domain is not configured. This creates a condition where the ASR cannot become the AED, because it is not certain if it is the only ASR on the site or not.

```
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
```

Troubleshoot

This section provides information you can use in order to troubleshoot your configuration.

Create a Packet Capture on the Join Interface in Order to See OTV Hellos

You can use the onboard packet capture device on the ASR in order to help troubleshoot possible problems.

Create an Access Control List (ACL) in order to minimize impact and oversaturated captures. The configuration is set up in order to only capture the multicast hellos between two sites. Adjust your IP address to match the join interfaces of the neighbors.

```
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
```

Set up the capture in order to sniff the join interface in both directions on both ASRs:

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

In order to start the capture, enter:

```
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
```

The buffer output shows that the hellos in the capture egress the captured interface. It shows the hellos destined to multicast address 225.0.0.1. This is the configured control group. See the first 13 packets in the capture, and notice how there is only a unidirectional output. Hellos from 172.17.100.134 are only seen out. Once the multicast problem in the core is resolved, the neighbor hello appears at packet number 14.

```
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
```

Verify the Mroute State on OTV ASR

When you build the multicast routing state between OTV neighbors, you must have the proper PIM state. Use this command in order to verify the expected PIM state on the ASRs:

```
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
```

Notice the same error as before: AED capable = No, overlay DIS not elected. What this means is that the ASR cannot become the AED forwarder, because it does not have enough information about its peer. It is possible that the internal interface is not up, the site bridge domain is down/not created, or the two sites cannot see each other accross the ISP.

Look at ASR−1 in order to identify the problem. It shows that no PIM neighbors are seen. This is expected even when it works. This is because PIM runs passive on the join interface. PIM passive is the only PIM mode supported on the join interface for OTV.

```
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
```

In order to verify that PIM interfaces are configured on the ASR−1, enter:

```
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
```

The mroute state of the ASR provides a wealth of information in regards to the multicast status of the link. In this output, you do not see the neighbor as an S,G entry on the local ASR mroute table. When you view the mroute count for the control group, you only see the local join interface as a source as well. Notice the count corresponds to packets received with the forwarded total. This means you are up and forwarding on the local side to the multicast domain.

```
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
```

When the core multicast problem is resolved, you see the expected output from the ASR.

```
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
```

There are still no PIM neighbors and the physical, overlay, and tunnel interfaces are local PIM interfaces.

```
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/   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.
```

The mroute table and counters provide information about the multicast state. The output shows the join interface as well as the OTV neighbor in the control group as sources. Make sure you see the Rendezvous Point (RP) in the remote site Reverse Path Forwarding (RPF) Neighbor (NBR) field as well. You also forward and receive matching counters. The two sources should total the group received total.

```
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
```

Create a Packet Capture on the Join−Interface to See OTV Data Packets

Because OTV is encapsulated traffic, it is seen as Generic Routing Encapsulation (GRE) traffic with a source of the join interface to the destination of remote join interface. There is not much you can do in order to see the traffic specifically. One method you can use in order to verify if your traffic makes it across OTV is to set up a packet capture, specifically with a packet size that is independent of your current traffic patterns. In this example, you can specify an Internet Control Message Protocol (ICMP) packet with a size of 700 and determine what you can filter out of the capture. This can be used in order to validate if a packet makes it across the OTV cloud.

In order to set up your access list filter between your two join interfaces, enter:

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

In order to set up your monitor session to filter out your specified size of 756, enter:

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

In order to start the capture, enter:

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

Send the specific ping with a specified size. Since OTV adds a 42−byte header along with an 8−byte ICMP with a 20−byte IP header, you can send a ping sized at 700 and expect to see the data reach the OTV cloud with a packet size of 756.

```
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
```

In order to stop the capture, enter:

```
ASR−1#mon cap 1 stop
*Nov 18 12:46:02.084: %BUFCAP−6−DISABLE: Capture Point 1 disabled.
```

In the capture buffer, you see all 100 packets reach the capture on the local side. You should see all 100 packets reach the remote side as well. If not, further investigation is required in the OTV cloud for packet loss.

```
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
```

Note: This test is not 100% reliable because any traffic that matches the length of 756 is captured, so use it with caution. This test is used in order to help gather data points only for possible OTV core issues.

Related Information

- ***Configuring Overlay Transport Virtualization***
- ***Understanding Ethernet Virtual Circuits (EVC)***
- ***Technical Support & Documentation − Cisco Systems***

Updated: Apr 25, 2014 Document ID: 117157