DYNAMIC SEGMENTATION:
Campus VXLAN/EVPN Architecture
Contents

Introduction ....................................................................................................................................................... 3
VXLAN Overview .............................................................................................................................................. 3
EVPN Overview ................................................................................................................................................ 3
Campus VXLAN/EVPN Architecture and Use Case .......................................................................................... 4
Underlay Network Details and Best Practices ................................................................................................... 5
  Campus Core .............................................................................................................................................. 5
  Campus Aggregation ................................................................................................................................. 6
  Campus Access .......................................................................................................................................... 7
Overlay Network Details and Best Practices ................................................................................................... 8
  Campus Core ............................................................................................................................................. 8
  Campus Aggregation ................................................................................................................................. 9
  Campus Access .......................................................................................................................................... 9
Underlay Network Traffic Flows ...................................................................................................................... 10
  In band Network Management and Routing on Access Switches .................................................................. 10
  Wireless AP Connectivity to Gateway Cluster ........................................................................................... 11
  IBGP EVPN Peering Between Access and Core VTEPs ........................................................................... 12
Overlay Network Traffic Flows ........................................................................................................................ 13
  Dynamic VXLAN Tunnels between VTEPs ................................................................................................. 13
  MAC Learning between VTEPs .................................................................................................................. 14
  Unicast L2 Traffic Forwarding between VTEPs ......................................................................................... 15
  Unicast L3 Traffic Forwarding between VTEPs ......................................................................................... 16
  BUM Traffic Forwarding between VTEPs ................................................................................................. 17
Appendix ......................................................................................................................................................... 18
  10.4 Scale Summary .................................................................................................................................. 18
  VXLAN Data Plane Packet Capture ........................................................................................................... 18
  EVPN Control Plane Packet Capture .......................................................................................................... 19
**Introduction**

To better handle business critical mobility and emerging IoT connectivity requirements, Aruba's innovative Dynamic Segmentation solution simplifies IT operations and improves security by dynamically applying unified policies and enforcing advanced services anywhere in the network. This ensures that appropriate access and security policies are seamlessly distributed, automatically applied, and independently enforced for all wireless and wired users and devices.

This document provides guidance on architecting a Dynamic Segmentation solution using VXLAN/EVPN in the Campus based on AOS-CX 10.4 with a focus on understanding the architecture and traffic flows.

**VXLAN Overview**

Virtual Extensible LAN (VXLAN) tunnels are standards-based, data plane “point to point” tunnels that provides L2 network overlay connectivity across a L3 underlay network as shown in Figure 1. Any device that supports VXLAN encapsulation/decapsulation is considered a VXLAN Tunnel End Point (VTEP). VXLAN supports multi-tenancy via VXLAN Network Identifiers (VNI) and traffic load sharing across Equal Cost Multi Pathing (ECMP) routes between VTEPs.

![VXLAN overlay tunnels](image)

VXLAN tunnels can be built via 1 of these methods:
- Static VXLAN
- Centralized control plane
- Distributed control plane

For details on VXLAN, refer to ArubaOS-CX 10.04 VXLAN Guide

The appendix has an example of a VXLAN data plane packet capture.

**EVPN Overview**

Multi-Protocol BGP (MP-BGP) Ethernet (EVPN) is a standards based distributed control plane protocol that builds dynamic VXLAN tunnels between VTEPs and provides MAC/IP address advertisements between VTEPs. EVPN is recommended for Campus deployments as it scales better than static VXLAN which uses MAC flood and learn in the data plane tunnel.

For details on EVPN, refer to ArubaOS-CX 10.04 IP Routing Guide

The appendix has an example of an EVPN control plane packet capture.
Dynamic Segmentation: Campus VXLAN/EVPN Architecture

Campus VXLAN/EVPN Architecture and Use Case

The Aruba switch to switch tunneling solution is based on VXLAN and is called Virtual Network Based Tunneling (VNBT), which compared to User Based Tunneling (UBT) is gateway based as shown in Figure 2.

Similar to UBT, VNBT also benefits from Aruba’s “colorless access” ports, it doesn’t matter what connects to the port as roles and policies are assigned per device from Aruba’s ClearPass Policy Manager, authentication takes place at the access port level and successful authentication enforces VLAN, port attributes and QoS/ACL policies. Either Local User Roles (LUR) or Downloadable User Roles (DUR) can be used.

Figure 2. UBT compared to VNBT

The main reason to deploy UBT would be to apply gateway applications (e.g. WebCC, Traffic Analysis) to tunneled clients while the main reason to deploy VNBT would be for traffic to traverse between switches across a campus network to directly access data center services or have traffic be inspected by an application layer firewall at the Data Center (DC). An authenticated client at the access switch can be forwarded in the underlay or placed into either a UBT or VNBT overlay tunnel based on ClearPass policies.

Figure 3. Campus VXLAN/EVPN architecture with parallel UBT and VNBT solutions
VNBT is complementary to gateway based GRE tunnels created by the UBT solution and can be deployed in parallel as shown in Figure 3.

The campus is in a single IBGP AS# for EVPN peering and all switches are part of OSPF area 0. It is also possible to implement multi-area OSPF if desired, e.g. buildings 1-4 in OSPF area 1, buildings 5-10 in OSPF area 2, core switches in OSPF area 0 to create separate OSPF failure domains.

NetEdit is the recommended centralized platform to manage and configure multiple AOS-CX switches.

For details on Virtual Switching Extension (VSX), VSX active gateway, Virtual Switching Framework (VSF), the various AOS-CX switches, NetEdit, refer to these URLs

- VSX Configuration Best Practices for Aruba CX 6400, 8320, 8325, 8400
- VSF Best Practices for Aruba CX 6300
- Software and Documentation on Aruba Support Portal
- NetEdit software download and installation guide
- AOS-CX 8325 datasheet
- AOS-CX 8320 datasheet
- AOS-CX 6400 datasheet
- AOS-CX 6300 datasheet

For AOS-CX 10.4 scale summary, refer to appendix.

**Underlay Network Details and Best Practices**

**Campus Core**

*Figure 4. Underlay network details*
At the Campus core layer, as shown in Figure 3 and 4:

- The AOS-CX 8325 switches participate in both underlay/overlay networks and function as the L3 Centralized Gateway VTEPs for all VNI/subnets in the overlay
- VTEP high availability is achieved via VSX, anycast Lo1 is used as the shared VXLAN tunnel source
- These switches will connect to multiple aggregation layer switches via L3 routed only ports with 9K MTU (to accommodate large MTU traffic with VXLAN overhead), /31 subnets and OSPF point to point networks
- These switches will also function as IBGP EVPN Route Reflectors (RRs) to simplify IBGP EVPN peering on the access VTEPs, a unique Lo0 on each switch is used for OSPF and BGP peering/router ID
- /32 Lo0 and Lo1 will be advertised by OSPF to enable access switches to peer IBGP EVPN with the RRs (Lo0) and establish a tunnel to the shared anycast IP (Lo1), examples of unique Lo0 and shared anycast Lo1 /32 IPs are shown
- Multiple physical links are recommended in the VSX ISL LAG to minimize the impact of a VSX split
- A dedicated VSX keepalive link is not mandatory as VSX keepalive using Lo0 can be established over the /31 routed only ports
- Overlay VXLAN traffic between the Core and access VTEPs will utilize ECMP routing in the underlay to load share traffic

**Campus Aggregation**

At the Campus aggregation (agg) layer, as shown in Figure 4 and 5:

- AOS-CX 6400/8325 switches will only participate in the underlay network
  - The appropriate switch model will depend on required features, port density and interfaces types
- These switches will connect northbound to multiple core layer switches via L3 routed only ports with 9K MTU (to accommodate large MTU traffic with VXLAN overhead), /31 subnets and OSPF point to point networks, L3 ECMP is used to load share traffic between buildings
- Overlay VXLAN traffic between the Core and access VTEPs will load share traffic via ECMP routing in the underlay
- /32 Lo0 will be advertised by OSPF for in band network management and function as OSPF router-ID, examples of Lo0
/32 IPs are shown

- These switches will function as L3 default gateways for traffic that shouldn’t be placed into the overlay
  - Infrastructure devices such as wireless access points (APs)
- These switches will connect southbound to aggregate multiple access layer switches
  - Within 1 building with multiple floors
  - Or multiple buildings
  - via VSX L2 Link Aggregation Groups (LAGs) with 9K MTU and 802.1Q trunk allowing these VLANs
    - VLAN 2 would provide inband network management, OSPF/BGP peering and connectivity for Overlay VXLAN tunnels
    - VLAN 4 would provide access for Wireless APs
- The agg layer can be replicated to support different groups/blocks of buildings and access switches
- Multiple physical links are recommended in the VSX ISL LAG to minimize the impact of a VSX split
- A dedicated VSX keepalive link is not mandatory as VSX keepalive using Lo0 can be established over the /31 routed only ports
- These switches will provide network connectivity
  - Between VTEPs
  - Between wireless APs and gateway cluster (which could be connected to either Agg or Core layer switches)
- L3 default gateway redundancy is achieved via Active Gateways (for VLANs 2/4) which will allow both switches to function as active L3 default gateways at the same time but does not incur protocol exchange overhead when compared to VRRP
- A /24 subnet is used as an example for VLAN 2, this subnet is local to an agg block, other agg blocks can utilize different /24s in VLAN 2
- OSPF broadcast network will be enabled on “Int VLAN 2” towards access switches to learn Lo0 from the access switches, OSPF priority is recommend on the agg VSX switches to ensure they function as OSPF Designated Router (DR) and Backup Designated Router (BDR)
- A /23 subnet is used as an example for VLAN 4, this subnet is local to an agg block, other agg blocks can utilize different /23s in VLAN 4
- OSPF broadcast network will be enabled on “Int VLAN 4” towards wireless APs with OSPF set to passive as those devices do not typically have a routing protocol enabled

Campus Access

At the Campus access layer, as shown in Figure 4 and 5:

- AOS-CX 6300 VSF stacks are used in environments with a preference for multiple switches while AOS-CX 6400 is chosen when high density modular chassis are preferred
- AOS-CX 6400 supports VSX but is not typically enabled in the access layer as most wired access devices do not have dual homing capabilities
- These switches will connect to a pair of agg layer switches via VSX L2 LAGs with 9K MTU and 802.1Q trunk allowing these VLANs
  - VLAN 2 would provide inband network management, OSPF/BGP peering and connectivity for Overlay VXLAN tunnels, /32 Lo0 is advertised and used as the VXLAN tunnel source on these VTEPs
  - VLAN 4 would provide access for Wireless APs
Edge colorless ports would be enabled towards wired devices, e.g. Wireless APs, end user devices, IP Phones

Here is a switch config example

```
interface 1/1/1-1/1/48
no shutdown
no routing
vlan access 1
aaa authentication port-access mac-auth
enable
aaa authentication port-access dot1x authenticator
eapol-timeout 30
max-eapol-requests 1
max-retries 1
enable
```

The authenticated client can be forwarded in the underlay or placed into either a UBT or VNBT overlay tunnel based on ClearPass policies

### Overlay Network Details and Best Practices

#### Campus Core

At the Campus core layer, as shown in Figure 6:

- These switches function as the L3 Centralized Gateway VTEPs for all VNIs/subnets
  - Will learn remote MACs from other VTEPs as EVPN type 2 routes
  - Will advertise local MACs to other VTEPs as EVPN type 2 routes
  - Will respond to L3 default gateway ARP requests from end clients
  - Will forward Broadcast, Unknown Unicast, Multicast (BUM) traffic via Head End Replication, peers are learnt via
EVPN type 3 routes
- VTEP high availability is achieved via VSX, anycast Lo1 is used as the shared VXLAN tunnel source towards other VTEPs
- 1 pair of AOS-CX 8325 VSX switches is considered 1 VTEP as the remote peers only establish tunnels to the shared Lo1 address
- Multiple tenant L3 VRFs can be used for segmentation by department or group (e.g. Law, Biology, Engineering) while a shared VRF External can be used for connectivity to external/non overlay networks
- L3 default gateway redundancy is achieved via active gateways, in this example VRF A has active gateways configured with 10.10.10.1/24 on both core switches
- These switches will function as border VTEPs to provide network connectivity between the overlay and non-overlay networks
- VRF route-target import/export is used to control route advertisements between VRFs
- EVPN will dynamically create VXLAN tunnels towards all access VTEPs with a similar VNI configured (AOS-CX supports a 1:1 VLAN to VNI mapping), in this example VNI 10 mapped to VLAN 10 is configured on access/core VTEPs which will create full mesh L2 tunnels between them

Campus Aggregation
At the Campus agg layer, as shown in Figure 6:
- AOS-CX 6400/8320/8325 switches will only participate in the underlay network and function as a transit switch between the access/core VTEPs
- With IBGP EVPN, you do not require every switch to understand or participate in EVPN as the access switches only need to peer with core switches which function as EVPN RRs

Campus Access
At the Campus access layer, as shown in Figure 6:
- These switches function as L2 VTEPs for desired VNIs
  - There is no requirement to configure all VNIs like the core VTEPs which function as L3 centralized gateways
  - Will learn remote MACs from other VTEPs as EVPN type 2 routes
  - Will advertise local MACs to other VTEPs as EVPN type 2 routes
  - Will forward Broadcast, Unknown Unicast, Multicast (BUM) traffic via Head End Replication, peers are learnt via EVPN type 3 routes
- Lo0 is used as the VXLAN tunnel source on these VTEPs
- EVPN will dynamically create VXLAN tunnels towards all other VTEPs with the same VNI configured, in this example VNI 10 mapped to VLAN 10 is configured on access/core VTEPs which will create full mesh L2 tunnels between them
- 1 x AOS-CX 6300 VSF stack is considered 1 VTEP
- 1 x AOS-CX 6400 modular switch is also considered 1 VTEP
Underlay Network Traffic Flows

The objective of this section is to provide examples to help further your understanding on the traffic flows in the underlay.

In band Network Management and Routing on Access Switches

Refer to Figure 7

1. Access switch has "Int VLAN 2" with an IP which will establish OSPF peering with DR/BDR (agg primary VSX/ agg secondary VSX) on that subnet
2. Access switch learns remote subnets and core loopback address via OSPF
3. Access switch advertises Lo0 to OSPF which will be used as VXLAN tunnel source and in band management IP
Wireless AP Connectivity to Gateway Cluster

Figure 8. Wireless AP to Gateway Cluster

Refer to Figure 8

1. Wireless AP connects to colorless port on access switch and sends out DHCP request
2. Access switch places device into wireless AP VLAN 4 based on ClearPass policy
3. Access switch forwards DHCP discover on uplinks to agg switches with Active Gateways
4. Primary VSX Agg switch forwards DHCP discover/request via DHCP relay to remote DHCP server
5. Agg switch receives DHCP responses (offer/ack) from DHCP server and forwards to wireless AP
6. Wireless AP uses DHCP options to communicate with gateway cluster and sets up GRE tunnel to gateway cluster

Take note that active gateways on the agg switches will allow both agg switches to forward traffic from the wireless AP to the gateway cluster, it is only the DHCP relay feature that requires the primary VSX agg switch to forward traffic
**IBGP EVPN Peering Between Access and Core VTEPs**

Refer to Figure 9

1. OSPF is used to exchange Loopback IPs between all VTEPs
2. For redundancy, each access VTEP will utilize Lo0 as source IP and peer IBGP EVPN to both core switches Lo0
3. Both core switch VTEPs will utilize Lo0 as source IP, configured as IBGP EVPN RRs and peer with all access VTEPs Lo0

Route Distinguisher (RD), Route Target (RT) can be set to auto when IBGP EVPN is used.

When configuring EVPN peers, "send-community extended" is required to ensure RD/RT is exchanged between VTEPs.
Overlay Network Traffic Flows

The objective of this section is to provide examples to help further your understanding on the traffic flows in the overlay.

Dynamic VXLAN Tunnels between VTEPs

Refer to Figure 10

1. Assuming IBGP EVPN is configured correctly in the underlay, VTEPs are configured next with:
   a. VXLAN tunnel interface and source IP (Lo 0 for access VTEPs, Lo 1 for VSX core VTEPs)
   b. VLANs configured globally in each VTEP, VLAN 10 is used in this example
   c. Desired VLAN to VNI mapping, VLAN 10 is mapped to VNI 10 in this example

   Tunnel source IPs will be used as next hop IP in the EVPN routing table

2. With VNI information exchanged between VTEPs via EVPN, VTEPs that are interested in the same VNI will dynamically establish VXLAN tunnels between them
MAC Learning between VTEPs

Figure 11. MAC learning between VTEPs

Refer to Figure 11

1. Wired device connects to colorless port on access VTEP, is placed into VLAN 10 and assigned ACLs/QoS based on ClearPass policy.

2. Access VTEP populates local MAC table and sends MAC advertisement out as EVPN type 2 route to other VTEPs interested in the same VNI through IBGP EVPN in the underlay.
3. Other VTEPs populate their EVPN route table with learned MAC and next hop (NH) set to the originating VTEP Lo0.

4. MACs learnt from other VTEPs are populated the same way, MAC 4 refers to the active gateway virtual MAC on the centralized gateway for VLAN 10.

**Unicast L2 Traffic Forwarding between VTEPs**

Assuming local and remote MACs are learnt via EVPN, Access1 VTEP needs to forward traffic from MAC 1 to MAC 3 in a different building.

Refer to Figure 12.

1. Access1 VTEP will encapsulate inner packet from MAC 1 with outer header which includes VNI, VTEP Source IP (S-IP), VTEP Destination IP (D-IP), VTEP Source MAC (S-MAC) and VTEP Destination MAC (D-MAC).

2. Intermediate transit switches will forward traffic based on outer header to the destination Access3 VTEP.

3. Destination VTEP will receive, decapsulate traffic and forward out local interface towards MAC 3, the reverse happens for traffic from MAC 3 to MAC 1.
Unicast L3 Traffic Forwarding between VTEPs

Figure 13. Unicast L3 traffic forwarding between VTEPs

Assuming local and remote MACs are learnt via EVPN, Access1 VTEP needs to forward traffic from MAC 1 to MAC 4 (Int VLAN 10 Active Gateway MAC) in order for the VSX L3 Centralized Gateway to route traffic out to different subnet.

In this example, the destination subnet is remote, not in the overlay and learnt via EBGP.

If destination subnet is in the overlay, it will be similar but without a routing protocol since all overlay subnets are directly connected.

Refer to Figure 13

1. Access1 VTEP will encapsulate inner packet from MAC 1 with outer header which includes VNI, VTEP Source IP (S-IP), VTEP Destination IP (D-IP), VTEP Source MAC (S-MAC) and VTEP Destination MAC (D-MAC)
2. Intermediate transit switches will forward traffic based on outer header to the destination Core VTEP Lo 1
3. Destination VTEP will receive, decapsulate traffic and forward out local interface towards destination subnet 220.220.0.0/24, the reverse happens for traffic from 220.220.0.0/24 to MAC 1
Assuming EVPN type 3 routes are exchanged via EVPN, each VTEP is now aware which peers are interested in the same VNI and where BUM traffic should be sent.

Refer to Figure 14

1. 10.10.10.10 sends ARP broadcast for 10.10.10.12
2. Access1 VTEP will encapsulate ARP broadcast into VXLAN tunnel, perform Head End Replication
3. ARP broadcast will be replicated and sent to all VTEPs interested in the same VNI based on EVPN type 3 routes
4. Destination VTEPs will decapsulate ARP broadcast and send out all local ports in the VLAN
## Appendix

### 10.4 Scale Summary

<table>
<thead>
<tr>
<th>Switch Model</th>
<th>6300</th>
<th>6400</th>
<th>8320</th>
<th>8325</th>
<th>8400</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switching Capacity</td>
<td>880 Gbps</td>
<td>14 Tbps or 28 Tbps</td>
<td>2.5 Tbps</td>
<td>6.4 Tbps</td>
<td>19.2 Tbps</td>
</tr>
<tr>
<td>MAC</td>
<td>32,768</td>
<td>32,768</td>
<td>98,304</td>
<td>98,304</td>
<td>768,000</td>
</tr>
<tr>
<td>IPv4 Host Table (ARP)</td>
<td>49,152</td>
<td>49,152</td>
<td>120,000</td>
<td>120,000</td>
<td>756,000</td>
</tr>
<tr>
<td>IPv6 Host Table (ND)</td>
<td>32,768</td>
<td>32,768</td>
<td>52,000</td>
<td>52,000</td>
<td>524,000</td>
</tr>
<tr>
<td>IPv4 Unicast Routes</td>
<td>61,000</td>
<td>61,000</td>
<td>130,993</td>
<td>131,072</td>
<td>1,011,712</td>
</tr>
<tr>
<td>IPv6 Unicast Routes</td>
<td>61,000</td>
<td>61,000</td>
<td>32,768</td>
<td>32,732</td>
<td>524,288</td>
</tr>
<tr>
<td>IPv4 Multicast Routes</td>
<td>8,000</td>
<td>8,000</td>
<td>4,094</td>
<td>4,094</td>
<td>32767</td>
</tr>
<tr>
<td>IPv6 Multicast Routes</td>
<td>8,000</td>
<td>8,000</td>
<td>4,094</td>
<td>4,094</td>
<td>32767</td>
</tr>
<tr>
<td>VRF</td>
<td>64</td>
<td>64</td>
<td>64</td>
<td>64</td>
<td>64</td>
</tr>
<tr>
<td>VXLAN VTEP Peers</td>
<td>256</td>
<td>256</td>
<td>NA</td>
<td>1,000</td>
<td>NA</td>
</tr>
<tr>
<td>VXLAN L2 VNI (VLANs)</td>
<td>1,024</td>
<td>1,024</td>
<td>NA</td>
<td>4,039 (VLAN 1 not supported)</td>
<td>NA</td>
</tr>
</tbody>
</table>

### VXLAN Data Plane Packet Capture

59 89, 299932... 10.10.10.1 10.10.10.2 ICMP 148 Echo (ping) reply id=0x0010, seq=2/512, ttl=64 (request in 58)
---
61 89, 333050... 10.10.10.1 10.10.10.2 ICMP 148 Echo (ping) request id=0x0020, seq=3/768, ttl=64 (request in 60)
---
62 90, 348965... 10.10.10.2 10.10.1.1 ICMP 148 Echo (ping) reply id=0x0030, seq=4/1024, ttl=64 (reply in 63)
---
63 90, 309999... 10.10.10.2 10.10.10.1 ICMP 148 Echo (ping) reply id=0x0040, seq=5/1280, ttl=64 (reply in 65),
---
64 91, 448740... 10.10.10.2 10.10.10.1 ICMP 148 Echo (ping) request id=0x0040, seq=5/1280, ttl=64 (request in 65)
EVPN Control Plane Packet Capture

| Frame 41: 184 bytes on wire (1472 bits), 184 bytes captured (1472 bits) on interface 0 |
| Ethernet II, Src: HewlettP 4c:fb:56 (08:00:09:4c:fb:56), Dst: HewlettP_c8:82:c9 (08:00:09:c8:82:c9) |
| Border Gateway Protocol - UPDATE Message |

Marker: fxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
Length: 118
Type: UPDATE Message (2)
Withdrawn Routes Length: 0
Total Path Attribute Length: 95

Path attributes
- Origin: INCOMPLETE
- Path Attribute - AS PATH: empty
- Path Attribute - LOCAL PREF: 100
- Path Attribute - ORIGINATOR ID: 192.168.1.2
- Path Attribute - CLUSTER LIST: 192.168.1.11
- Path Attribute - EXTENDED COMMUNITIES

Path Attribute - MP REACH NLRI
- Flags: 0x00, Optional, Extended-Length, Non-transitive, Complete
- Type Code: MP REACH NLRI (14)
- Length: 44
- Address family identifier (AFI): Layer-2 VPN (25)
- Subsequent address family identifier (SAFI): EVPN (70)
- Next hop network address (4 bytes)
- Number of Subnetwork points of attachment (SNPA): 0
- Network layer reachability information (35 bytes)
- EVPN NLRI: MAC Advertisement Route

Route Type: MAC Advertisement Route (2)
- Length: 33
- Route Distinguisher: 0001:0a00120000a (192.168.1.2:10)
- ESI: 00:00:00:00:00:00:00:00
- Ethernet Tag ID: 0
- MAC Address Length: 48
- IP Address Length: 0
- IP Address: NOT INCLUDED
- 0000 0000 0000 0000 0000 0000 0000 0000 .... = MPLS Label 1: 0

| Frame 43: 188 bytes on wire (1440 bits), 188 bytes captured (1440 bits) on interface 0 |
| Ethernet II, Src: HewlettP 4c:fb:56 (08:00:09:4c:fb:56), Dst: HewlettP_c8:82:c9 (08:00:09:c8:82:c9) |
| Border Gateway Protocol - UPDATE Message |

Marker: fxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
Length: 114
Type: UPDATE Message (2)
Withdrawn Routes Length: 0
Total Path Attribute Length: 91

Path attributes
- Origin: INCOMPLETE
- Path Attribute - AS PATH: empty
- Path Attribute - LOCAL PREF: 100
- Path Attribute - ORIGINATOR ID: 192.168.1.2
- Path Attribute - CLUSTER LIST: 192.168.1.11
- Path Attribute - EXTENDED COMMUNITIES
- Path Attribute - PMSI TUNNEL ATTRIBUTE

Path Attribute - MP REACH NLRI
- Flags: 0x00, Optional, Extended-Length, Non-transitive, Complete
- Type Code: MP REACH NLRI (14)
- Length: 28
- Address family identifier (AFI): Layer-2 VPN (25)
- Subsequent address family identifier (SAFI): EVPN (70)
- Next hop network address (4 bytes)
- Number of Subnetwork points of attachment (SNPA): 0
- Network layer reachability information (19 bytes)
- EVPN NLRI: Inclusive Multicast Route

Route Type: Inclusive Multicast Route (3)
- Length: 17
- Route Distinguisher: 0001:0a00120000a (192.168.1.2:10)
- Ethernet Tag ID: 0
- IP Address Length: 32
- IPv4 address: 192.168.1.12

EVPN type 2 route

EVPN type 3 route