

**L3 Data Centre**

**LEAF and SPINE**

991451344

Professor: Felix Carapaica

Timothy Pang

**Objectives:**

- Build the following network diagram implementing DC EVPN VXLAN.
- There are three VLAN-VXLAN 10, 20, and 30.
- On the tenant side, the three Cisco routers have three VRF matching each VLAN.
- The Cisco routers must reach all the tenant side networks.

## 1. R3# show ip route vrf 10

```
R3#sh ip route vrf 10

Routing Table: 10
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 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        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
        o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
        + - replicated route, % - next hop override

Gateway of last resort is not set

    10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
C       10.0.10.0/24 is directly connected, FastEthernet1/0.10
L       10.0.10.3/32 is directly connected, FastEthernet1/0.10
C       10.10.3.3/32 is directly connected, Loopback10
O       10.10.4.4/32 [110/2] via 10.0.10.4, 00:05:12, FastEthernet1/0.10
O       10.10.5.5/32 [110/2] via 10.0.10.5, 00:05:17, FastEthernet1/0.10
    192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.3.0/26 is directly connected, FastEthernet0/0.10
L       192.168.3.1/32 is directly connected, FastEthernet0/0.10
    192.168.4.0/26 is subnetted, 1 subnets
O       192.168.4.0 [110/2] via 10.0.10.4, 00:05:12, FastEthernet1/0.10
    192.168.5.0/26 is subnetted, 1 subnets
O       192.168.5.0 [110/2] via 10.0.10.5, 00:05:17, FastEthernet1/0.10
R3#
```

Figure 1.

## 2. R3# show ip route vrf 20

```
R3#sh ip route vrf 20

Routing Table: 20
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 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        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
        o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
        + - replicated route, % - next hop override

Gateway of last resort is not set

    10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
C       10.0.20.0/24 is directly connected, FastEthernet1/0.20
L       10.0.20.3/32 is directly connected, FastEthernet1/0.20
C       10.20.3.3/32 is directly connected, Loopback20
O       10.20.4.4/32 [110/2] via 10.0.20.4, 00:05:34, FastEthernet1/0.20
O       10.20.5.5/32 [110/2] via 10.0.20.5, 00:05:39, FastEthernet1/0.20
    192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.3.64/26 is directly connected, FastEthernet0/0.20
L       192.168.3.65/32 is directly connected, FastEthernet0/0.20
    192.168.4.0/26 is subnetted, 1 subnets
O       192.168.4.64 [110/2] via 10.0.20.4, 00:05:34, FastEthernet1/0.20
    192.168.5.0/26 is subnetted, 1 subnets
O       192.168.5.64 [110/2] via 10.0.20.5, 00:05:39, FastEthernet1/0.20
R3#
```

Figure 2.

### 3. R3# show ip route vrf 30

```
R3#sh ip route vrf 30

Routing Table: 30
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 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        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
        o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
        + - replicated route, % - next hop override

Gateway of last resort is not set

    10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
C       10.0.30.0/24 is directly connected, FastEthernet1/0.30
L       10.0.30.3/32 is directly connected, FastEthernet1/0.30
C       10.30.3.3/32 is directly connected, Loopback30
O       10.30.4.4/32 [110/2] via 10.0.30.4, 00:05:47, FastEthernet1/0.30
O       10.30.5.5/32 [110/2] via 10.0.30.5, 00:06:02, FastEthernet1/0.30
    192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.3.128/26 is directly connected, FastEthernet0/0.30
L       192.168.3.129/32 is directly connected, FastEthernet0/0.30
O       192.168.4.0/26 is subnetted, 1 subnets
O       192.168.4.128 [110/2] via 10.0.30.4, 00:05:47, FastEthernet1/0.30
O       192.168.5.0/26 is subnetted, 1 subnets
O       192.168.5.128 [110/2] via 10.0.30.5, 00:06:02, FastEthernet1/0.30
R3#
```

Figure 3.

### 4. R3# show ip ospf database

```
R3#sh ip ospf data

OSPF Router with ID (10.30.3.3) (Process ID 30)

  Router Link States (Area 0)

Link ID      ADV Router   Age         Seq#         Checksum Link count
10.30.3.3    10.30.3.3    385         0x80000002  0x004836  3
10.30.4.4    10.30.4.4    376         0x80000002  0x007402  3
10.30.5.5    10.30.5.5    386         0x80000002  0x00A0CD  3

  Net Link States (Area 0)

Link ID      ADV Router   Age         Seq#         Checksum
10.0.30.5    10.30.5.5    376         0x80000002  0x00DD67

OSPF Router with ID (10.20.3.3) (Process ID 20)

  Router Link States (Area 0)

Link ID      ADV Router   Age         Seq#         Checksum Link count
10.20.3.3    10.20.3.3    384         0x80000002  0x006A86  3
10.20.4.4    10.20.4.4    377         0x80000002  0x009652  3
10.20.5.5    10.20.5.5    384         0x80000002  0x00C21E  3

  Net Link States (Area 0)

Link ID      ADV Router   Age         Seq#         Checksum
10.0.20.5    10.20.5.5    377         0x80000002  0x003344

OSPF Router with ID (10.10.3.3) (Process ID 10)

  Router Link States (Area 0)

Link ID      ADV Router   Age         Seq#         Checksum Link count
10.10.3.3    10.10.3.3    383         0x80000002  0x008CD6  3
10.10.4.4    10.10.4.4    384         0x80000002  0x00B8A2  3
10.10.5.5    10.10.5.5    384         0x80000002  0x00E46E  3

  Net Link States (Area 0)

Link ID      ADV Router   Age         Seq#         Checksum
10.0.10.5    10.10.5.5    384         0x80000001  0x008A20
R3#
```

Figure 4.

## 5. CL1# net show bgp route

```
cumulus@cumulus:mgmt~$ net show bgp route
ERROR: Command not found.

net show bgp route
^ Invalid value here.

The following commands contain keyword(s) 'route', 'show', 'bgp'

net show bgp [l2vpn] evpn route [detail] [json]
net show bgp [l2vpn] evpn route [detail] type (ead|1|macip|2|multicast|3|es|4|prefix|5) [json]
net show bgp [l2vpn] evpn route rd <rd> [json]
net show bgp [l2vpn] evpn route rd <rd> mac <mac> [json]
net show bgp [l2vpn] evpn route rd <rd> mac <mac> ip <ip> [json]
net show bgp [l2vpn] evpn route rd <rd> prefix (<ipv4/prefixlen>|<ipv6/prefixlen>) [json]
net show bgp [l2vpn] evpn route rd <rd> type (ead|1|macip|2|multicast|3|es|4|prefix|5) [json]
net show bgp [l2vpn] evpn route vni <l-16777215> [json]
net show bgp [l2vpn] evpn route vni <l-16777215> mac <mac> [json]
net show bgp [l2vpn] evpn route vni <l-16777215> mac <mac> ip <ip> [json]
net show bgp [l2vpn] evpn route vni <l-16777215> multicast <ipv4> [json]
net show bgp [l2vpn] evpn route vni <l-16777215> type (ead|1|macip|2|multicast|3) [json]
net show bgp [l2vpn] evpn route vni <l-16777215> vtep <ipv4> [json]
net show bgp [l2vpn] evpn route vni all [detail] [json]
net show bgp [l2vpn] evpn route vni all [detail] vtep <ipv4> [json]
net show bgp ipv4 unicast route-leak [json]
net show bgp ipv6 unicast route-leak [json]
net show bgp vrf <text> ipv4 unicast route-leak [json]
net show bgp vrf <text> ipv6 unicast route-leak [json]
net show route (bgp|connected|kernel|ospf|ospf6|rip|static|supernets-only|table) [json]
net show route vrf <text> (bgp|connected|kernel|ospf|ospf6|rip|static|supernets-only|table) [json]

cumulus@cumulus:mgmt~$
```

Figure 5.

### Alternate: CL1# net show bgp l2vpn evpn route

```
CL1 CL3
cumulus@cumulus:mgmt~$ net show bgp l2vpn evpn route
BGP table version is 2, local router ID is 10.0.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
EVPN type-1 prefix: [1]:[ESI]:[EthTag]:[IPlen]:[VTEP-IP]:[Frag-id]
EVPN type-2 prefix: [2]:[EthTag]:[MAClen]:[MAC]:[IPlen]:[IP]
EVPN type-3 prefix: [3]:[EthTag]:[IPlen]:[OrigIP]
EVPN type-4 prefix: [4]:[ESI]:[IPlen]:[OrigIP]
EVPN type-5 prefix: [5]:[EthTag]:[IPlen]:[IP]

Network Next Hop Metric LocPrf Weight Path
Extended Community
Route Distinguisher: 65003:10
*> [2]:[0]:[48]:[ca:01:30:ac:00:1c]
10.0.0.3 0 65003 i
RT:65003:10 ET:8
*> [3]:[0]:[32]:[10.0.0.3]
10.0.0.3 0 65003 i
RT:65003:10 ET:8
Route Distinguisher: 65003:20
*> [2]:[0]:[48]:[ca:01:30:ac:00:1c]
10.0.0.3 0 65003 i
RT:65003:20 ET:8
*> [3]:[0]:[32]:[10.0.0.3]
10.0.0.3 0 65003 i
RT:65003:20 ET:8
Route Distinguisher: 65003:30
*> [2]:[0]:[48]:[ca:01:30:ac:00:1c]
10.0.0.3 0 65003 i
RT:65003:30 ET:8
*> [3]:[0]:[32]:[10.0.0.3]
10.0.0.3 0 65003 i
RT:65003:30 ET:8
Route Distinguisher: 65004:10
*> [2]:[0]:[48]:[ca:02:07:60:00:1c]
10.0.0.4 0 65004 i
RT:65004:10 ET:8
*> [3]:[0]:[32]:[10.0.0.4]
10.0.0.4 0 65004 i
RT:65004:10 ET:8
Route Distinguisher: 65004:20
*> [2]:[0]:[48]:[ca:02:07:60:00:1c]
10.0.0.4 0 65004 i
RT:65004:20 ET:8
*> [3]:[0]:[32]:[10.0.0.4]
10.0.0.4 0 65004 i
RT:65004:20 ET:8
Route Distinguisher: 65004:30
*> [2]:[0]:[48]:[ca:02:07:60:00:1c]
10.0.0.4 0 65004 i
RT:65004:30 ET:8
*> [3]:[0]:[32]:[10.0.0.4]
10.0.0.4 0 65004 i
RT:65004:30 ET:8
Route Distinguisher: 65005:10
*> [2]:[0]:[48]:[ca:03:2f:28:00:1c]
10.0.0.5 0 65005 i
RT:65005:10 ET:8
*> [3]:[0]:[32]:[10.0.0.5]
10.0.0.5 0 65005 i
RT:65005:10 ET:8
```

```

Route Distinguisher: 65005:20
*> [2]:[0]:[48]:[ca:03:2f:28:00:1c]
10.0.0.5                                0 65005 i
RT:65005:20 ET:8
*> [3]:[0]:[32]:[10.0.0.5]
10.0.0.5                                0 65005 i
RT:65005:20 ET:8
Route Distinguisher: 65005:30
*> [2]:[0]:[48]:[ca:03:2f:28:00:1c]
10.0.0.5                                0 65005 i
RT:65005:30 ET:8
*> [3]:[0]:[32]:[10.0.0.5]
10.0.0.5                                0 65005 i
RT:65005:30 ET:8
Displayed 18 prefixes (18 paths)

```

Figure 6.

Alternatively: CL1# net show bgp

```

CL3  CL1
cumulus@cumulus:mgmt:~$ net show bgp
show bgp ipv4 unicast
=====
BGP table version is 4, local router ID is 10.0.0.1, vrf id 0
Default local pref 100, local AS 65000
Status codes: s suppressed, d damped, h history, * valid, > best, = multipath,
               i internal, r RIB-failure, S Stale, R Removed
NextHop codes: @NNN nextHop's vrf id, < announce-nh-self
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network        Next Hop        Metric LocPrf Weight Path
*> 10.0.0.1/32     0.0.0.0           0         32768 i
*> 10.0.0.3/32     swp1              0          0 65003 i
*> 10.0.0.4/32     swp4              0          0 65004 i
*> 10.0.0.5/32     swp2              0          0 65005 i

Displayed 4 routes and 4 total paths

show bgp ipv6 unicast
=====
No BGP prefixes displayed, 0 exist
cumulus@cumulus:mgmt:~$

```

Figure 7.

6. CL1# net show bgp l2vpn evpn route vni 10

```

CL1  CL2  CL3  CL4  CL5  R3
cumulus@cumulus:mgmt:~$ net show bgp l2vpn evpn route vni 10
VNI not found
cumulus@cumulus:mgmt:~$

```

Figure 8.

CL3# net show bgp l2vpn evpn route vni 10

```

CL3
CL1
The registered trademark Linux (R) is used pursuant to a sublicense from LMI,
the exclusive licensee of Linus Torvalds, owner of the mark on a world-wide
basis.
cumulus@cumulus:mgmt:~$ net show bgp l2vpn evpn route vni 10
BGP table version is 6, local router ID is 10.0.0.3
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
EVPN type-1 prefix: [1]:[ESI]:[EthTag]:[IPlen]:[VTEP-IP]:[Frag-id]
EVPN type-2 prefix: [2]:[EthTag]:[MAClen]:[MAC]:[IPlen]:[IP]
EVPN type-3 prefix: [3]:[EthTag]:[IPlen]:[OrigIP]
EVPN type-4 prefix: [4]:[ESI]:[IPlen]:[OrigIP]
EVPN type-5 prefix: [5]:[EthTag]:[IPlen]:[IP]

Network          Next Hop          Metric LocPrf Weight Path
*> [2]:[0]:[48]:[ca:01:30:ac:00:1c]
10.0.0.3
ET:8 RT:65003:10
32768 i
* [2]:[0]:[48]:[ca:02:07:60:00:1c]
10.0.0.4
0 65000 65004 i
RT:65004:10 ET:8
*> [2]:[0]:[48]:[ca:02:07:60:00:1c]
10.0.0.4
0 65000 65004 i
RT:65004:10 ET:8
* [2]:[0]:[48]:[ca:03:2f:28:00:1c]
10.0.0.5
0 65000 65005 i
RT:65005:10 ET:8
*> [2]:[0]:[48]:[ca:03:2f:28:00:1c]
10.0.0.5
0 65000 65005 i
RT:65005:10 ET:8
*> [3]:[0]:[32]:[10.0.0.3]
10.0.0.3
32768 i
ET:8 RT:65003:10
* [3]:[0]:[32]:[10.0.0.4]
10.0.0.4
0 65000 65004 i
RT:65004:10 ET:8
*> [3]:[0]:[32]:[10.0.0.4]
10.0.0.4
0 65000 65004 i
RT:65004:10 ET:8
* [3]:[0]:[32]:[10.0.0.5]
10.0.0.5
0 65000 65005 i
RT:65005:10 ET:8
*> [3]:[0]:[32]:[10.0.0.5]
10.0.0.5
0 65000 65005 i
RT:65005:10 ET:8

Displayed 6 prefixes (10 paths)
cumulus@cumulus:mgmt:~$

```

Figure 9.

## 7. CL2# net show bgp l2vpn evpn route vni 20

```

CL1
CL2
CL3
CL4
CL5
R3
cumulus@cumulus:mgmt:~$ net show bgp l2vpn evpn route vni 20
VNI not found
cumulus@cumulus:mgmt:~$

```

Figure 10.

## CL3# net show bgp l2vpn evpn route vni 20

```

cumulus@cumulus:mgmt~$ net show bgp l2vpn evpn route vni 20
BGP table version is 6, local router ID is 10.0.0.3
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
EVPN type-1 prefix: [1]:[ESI]:[EthTag]:[IPlen]:[VTEP-IP]:[Frag-id]
EVPN type-2 prefix: [2]:[EthTag]:[MAClen]:[MAC]:[IPlen]:[IP]
EVPN type-3 prefix: [3]:[EthTag]:[IPlen]:[OrigIP]
EVPN type-4 prefix: [4]:[ESI]:[IPlen]:[OrigIP]
EVPN type-5 prefix: [5]:[EthTag]:[IPlen]:[IP]

  Network          Next Hop          Metric LocPrf Weight Path
*> [2]:[0]:[48]:[ca:01:30:ac:00:1c]
    10.0.0.3
    ET:8 RT:65003:20
    32768 i
* [2]:[0]:[48]:[ca:02:07:60:00:1c]
    10.0.0.4
    RT:65004:20 ET:8
    0 65000 65004 i
*> [2]:[0]:[48]:[ca:02:07:60:00:1c]
    10.0.0.4
    RT:65004:20 ET:8
    0 65000 65004 i
* [2]:[0]:[48]:[ca:03:2f:28:00:1c]
    10.0.0.5
    RT:65005:20 ET:8
    0 65000 65005 i
*> [2]:[0]:[48]:[ca:03:2f:28:00:1c]
    10.0.0.5
    RT:65005:20 ET:8
    0 65000 65005 i
*> [3]:[0]:[32]:[10.0.0.3]
    10.0.0.3
    ET:8 RT:65003:20
    32768 i
* [3]:[0]:[32]:[10.0.0.4]
    10.0.0.4
    RT:65004:20 ET:8
    0 65000 65004 i
*> [3]:[0]:[32]:[10.0.0.4]
    10.0.0.4
    RT:65004:20 ET:8
    0 65000 65004 i
* [3]:[0]:[32]:[10.0.0.5]
    10.0.0.5
    RT:65005:20 ET:8
    0 65000 65005 i
*> [3]:[0]:[32]:[10.0.0.5]
    10.0.0.5
    RT:65005:20 ET:8
    0 65000 65005 i

Displayed 6 prefixes (10 paths)
cumulus@cumulus:mgmt~$

```

Figure 11.

## 8. CL3# net show bgp l2vpn evpn route vni 30

```

cumulus@cumulus:mgmt~$ net show bgp l2vpn evpn route vni 30
BGP table version is 6, local router ID is 10.0.0.3
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
EVPN type-1 prefix: [1]:[ESI]:[EthTag]:[IPlen]:[VTEP-IP]:[Frag-id]
EVPN type-2 prefix: [2]:[EthTag]:[MAClen]:[MAC]:[IPlen]:[IP]
EVPN type-3 prefix: [3]:[EthTag]:[IPlen]:[OrigIP]
EVPN type-4 prefix: [4]:[ESI]:[IPlen]:[OrigIP]
EVPN type-5 prefix: [5]:[EthTag]:[IPlen]:[IP]

  Network          Next Hop          Metric LocPrf Weight Path
*> [2]:[0]:[48]:[ca:01:30:ac:00:1c]
    10.0.0.3
    ET:8 RT:65003:30
    32768 i
* [2]:[0]:[48]:[ca:02:07:60:00:1c]
    10.0.0.4
    RT:65004:30 ET:8
    0 65000 65004 i
*> [2]:[0]:[48]:[ca:02:07:60:00:1c]
    10.0.0.4
    RT:65004:30 ET:8
    0 65000 65004 i
* [2]:[0]:[48]:[ca:03:2f:28:00:1c]
    10.0.0.5
    RT:65005:30 ET:8
    0 65000 65005 i
*> [2]:[0]:[48]:[ca:03:2f:28:00:1c]
    10.0.0.5
    RT:65005:30 ET:8
    0 65000 65005 i
*> [3]:[0]:[32]:[10.0.0.3]
    10.0.0.3
    ET:8 RT:65003:30
    32768 i
* [3]:[0]:[32]:[10.0.0.4]
    10.0.0.4
    RT:65004:30 ET:8
    0 65000 65004 i
*> [3]:[0]:[32]:[10.0.0.4]
    10.0.0.4
    RT:65004:30 ET:8
    0 65000 65004 i
* [3]:[0]:[32]:[10.0.0.5]
    10.0.0.5
    RT:65005:30 ET:8
    0 65000 65005 i
*> [3]:[0]:[32]:[10.0.0.5]
    10.0.0.5
    RT:65005:30 ET:8
    0 65000 65005 i

Displayed 6 prefixes (10 paths)
cumulus@cumulus:mgmt~$

```

Figure 12.



The first is the general bgp OPEN and UPDATE messages:

Figure 13.

The image shows a Wireshark packet capture window titled "[CLS swp] to CLS swp]. The packet list on the left shows a BGP packet (No. 48, Time 97.588847, Source fe80::ef3:b9ff:fe2c::, Destination fe80::e94:a1ff:fe7c::, Protocol BGP, Length 200) labeled "OPEN Message". The packet details pane on the right shows the following structure:

- Frame 48: 200 bytes on wire (1600 bits), 200 bytes captured (1600 bits) on interface ..., id 0
- Ethernet II, Src: 0c:f3:b9:2c:00:01 (0c:f3:b9:2c:00:01), Dst: 0c:94:a1:7c:00:01 (0c:94:a1:7c:00:01)
  - Destination: 0c:94:a1:7c:00:01 (0c:94:a1:7c:00:01)
  - Source: 0c:f3:b9:2c:00:01 (0c:f3:b9:2c:00:01)
  - Type: IPv6 (0x86dd)
- Internet Protocol Version 6, Src: fe80::ef3:b9ff:fe2c::1, Dst: fe80::e94:a1ff:fe7c::1
  - 0110 .... = Version: 6
  - .... 1100 0000 .... = Traffic Class: 0xc0 (DSCP: CS6, ECN: Not-ECT)
  - .... 0011 0001 0011 1100 1010 = Flow Label: 0x313ca
  - Payload Length: 146
  - Next Header: TCP (6)
  - Hop Limit: 1
  - Source Address: fe80::ef3:b9ff:fe2c::1
  - Destination Address: fe80::e94:a1ff:fe7c::1
  - [Source SA MAC: 0c:f3:b9:2c:00:01 (0c:f3:b9:2c:00:01)]
  - [Destination SA MAC: 0c:94:a1:7c:00:01 (0c:94:a1:7c:00:01)]
- Transmission Control Protocol, Src Port: 56602, Dst Port: 179, Seq: 1, Ack: 1, Len: 114
  - Source Port: 56602
  - Destination Port: 179
  - [Stream index: 0]
  - [TCP Segment Len: 114]
  - Sequence Number: 1 (relative sequence number)
  - Sequence Number (raw): 3478584576
  - [Next Sequence Number: 115 (relative sequence number)]
  - Acknowledgment Number: 1 (relative ack number)
  - Acknowledgment number (raw): 1284295222
  - 1000 .... = Header Length: 32 bytes (8)
  - Flags: 0xb18 (PSH, ACK)
  - Window: 251
  - [Calculated window size: 64256]
  - [Window size scaling factor: 256]
  - Checksum: 0xc520 [Unverified]
  - [Checksum Status: Unverified]
  - Urgent Pointer: 0
  - Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  - [SEQ/ACK analysis]
  - [Timestamps]
  - TCP payload (114 bytes)
- Border Gateway Protocol - OPEN Message
  - Marker: ffffffffffffffffffffffffffffffff
  - Length: 114
  - Type: OPEN Message (1)
  - Version: 4
  - My AS: 65000
  - Hold Time: 9
  - BGP Identifier: 10.0.0.1
  - Optional Parameters Length: 85
  - Optional Parameters

Figure 14.

When we open the UPDATE message, we see the MAC address IPv6 instead of IPv4 because the peer-group LEAF and SPINE are both running IPv6 to communicate with one another.

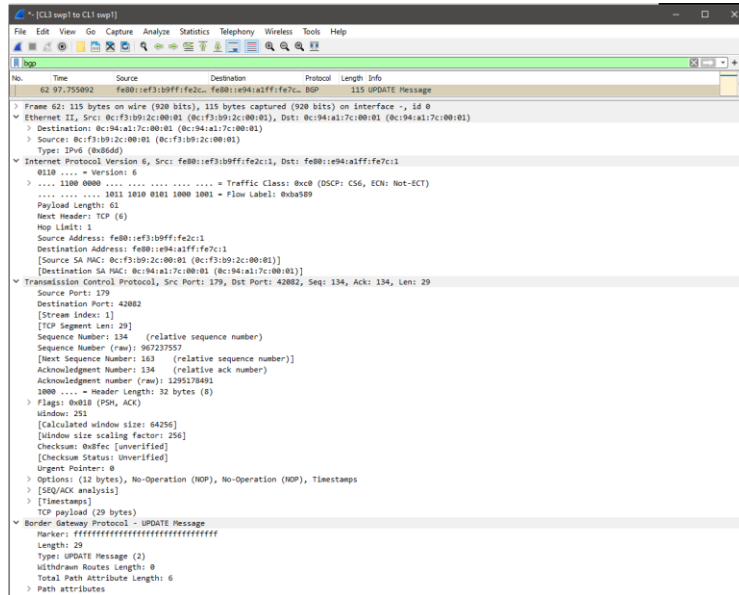


Figure 12.

When we open the next UPDATE message packet, we see multiple BGP update messages within the first UPDATE packet.

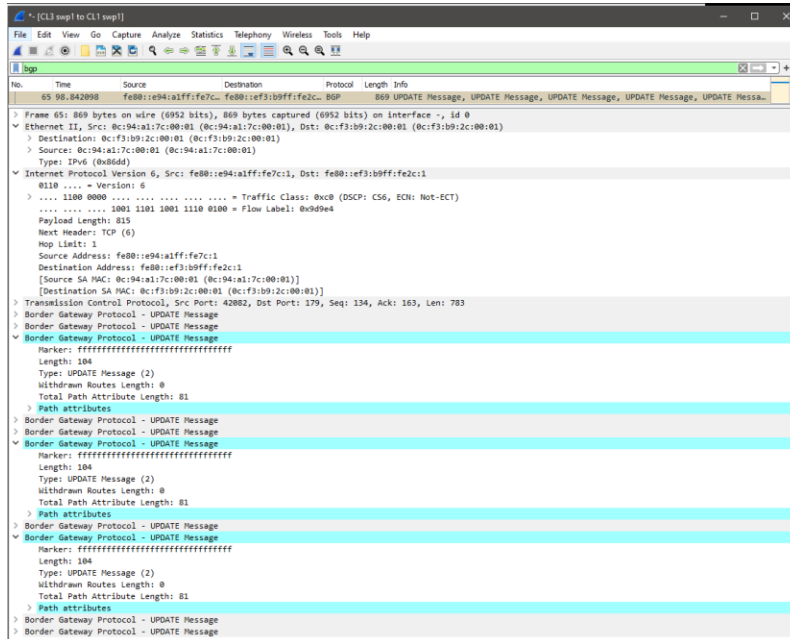
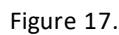
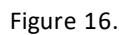


Figure 15.



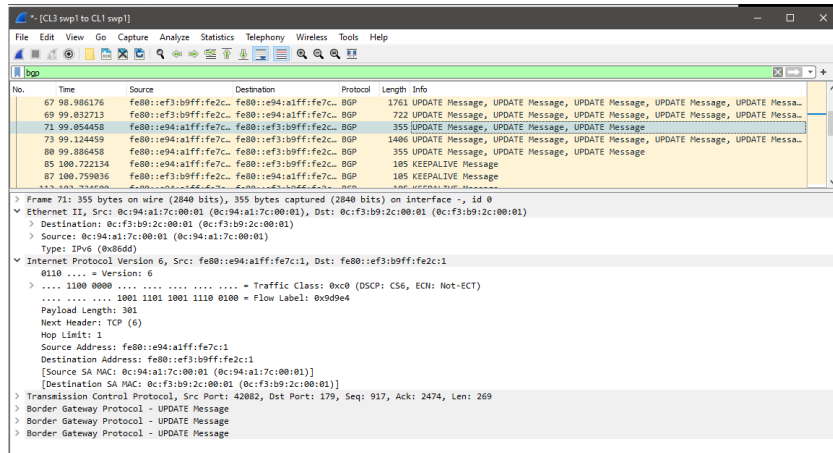


Figure 18.

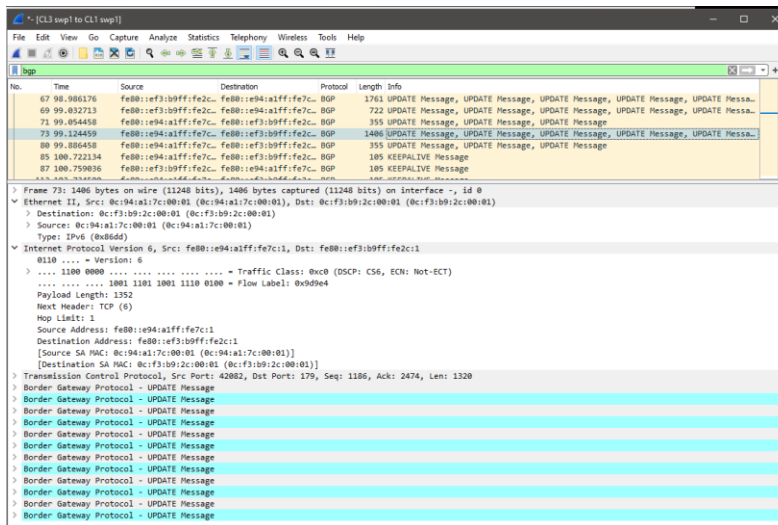


Figure 19.

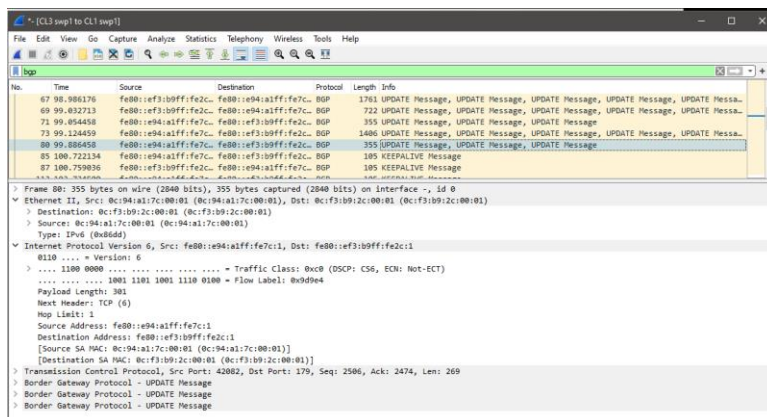


Figure 20.

The detailed explanation of the encapsulation of a ping from an VLAN-VRF in R3 to a destination in R5. The sniff is to be done on the interfaces out of CL3.

Out of CL3 to CL2:

28	10.006465	10.0.20.3	192.168.5.65	ICMP	164 Echo (ping) request	id=0x0002, seq=0/0, ttl=255 (reply in 29)
29	10.017739	192.168.5.65	10.0.20.3	ICMP	164 Echo (ping) reply	id=0x0002, seq=0/0, ttl=255 (request in 28)
30	10.028648	10.0.20.3	192.168.5.65	ICMP	164 Echo (ping) request	id=0x0002, seq=1/256, ttl=255 (reply in 31)
31	10.038719	192.168.5.65	10.0.20.3	ICMP	164 Echo (ping) reply	id=0x0002, seq=1/256, ttl=255 (request in 30)
32	10.049256	10.0.20.3	192.168.5.65	ICMP	164 Echo (ping) request	id=0x0002, seq=2/512, ttl=255 (reply in 33)
33	10.060362	192.168.5.65	10.0.20.3	ICMP	164 Echo (ping) reply	id=0x0002, seq=2/512, ttl=255 (request in 32)
34	10.070762	10.0.20.3	192.168.5.65	ICMP	164 Echo (ping) request	id=0x0002, seq=3/768, ttl=255 (reply in 35)
35	10.081644	192.168.5.65	10.0.20.3	ICMP	164 Echo (ping) reply	id=0x0002, seq=3/768, ttl=255 (request in 34)
36	10.092251	10.0.20.3	192.168.5.65	ICMP	164 Echo (ping) request	id=0x0002, seq=4/1024, ttl=255 (reply in 37)
37	10.103879	192.168.5.65	10.0.20.3	ICMP	164 Echo (ping) reply	id=0x0002, seq=4/1024, ttl=255 (request in 36)

Figure 21.

From CL3 to CL2 looking at the general ping, the icmp packets are sent multiple times back and forth, both request and reply from both parties.

28	10.006465	10.0.20.3	192.168.5.65	ICMP	164 Echo (ping) request	id=0x0002, seq=0/0, ttl=255 (reply in 29)
<pre> &gt; Frame 28: 164 bytes on wire (1312 bits), 164 bytes captured (1312 bits) on interface -, id 0 &gt; Ethernet II, Src: 0c:94:a1:7c:00:02 (0c:94:a1:7c:00:02), Dst: 0c:b0:aa:c3:00:02 (0c:b0:aa:c3:00:02) &gt; Internet Protocol Version 4, Src: 10.0.0.3, Dst: 10.0.0.5 &gt; User Datagram Protocol, Src Port: 59334, Dst Port: 4789   Virtual eXtensible Local Area Network     &gt; Flags: 0x0800, VXLAN Network ID (VNI)       Group Policy ID: 0       VXLAN Network Identifier (VNI): 20       Reserved: 0   Ethernet II, Src: ca:01:30:ac:00:1c (ca:01:30:ac:00:1c), Dst: ca:03:2f:28:00:1c (ca:03:2f:28:00:1c)     &gt; Destination: ca:03:2f:28:00:1c (ca:03:2f:28:00:1c)     &gt; Source: ca:01:30:ac:00:1c (ca:01:30:ac:00:1c)     Type: IPv4 (0x0800)   Internet Protocol Version 4, Src: 10.0.20.3, Dst: 192.168.5.65     0100 .... = Version: 4     .... 0101 = Header Length: 20 bytes (5)     &gt; Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)       Total Length: 100       Identification: 0x000a (10)     &gt; Flags: 0x00       Fragment Offset: 0       Time to Live: 255       Protocol: ICMP (1)       Header Checksum: 0xd7a2 [validation disabled]       [Header checksum status: Unverified]       Source Address: 10.0.20.3       Destination Address: 192.168.5.65   Internet Control Message Protocol     Type: 8 (Echo (ping) request)     Code: 0     Checksum: 0x2bb3 [correct]     [Checksum Status: Good]     Identifier (BE): 2 (0x0002)     Identifier (LE): 512 (0x0200)     Sequence Number (BE): 0 (0x0000)     Sequence Number (LE): 0 (0x0000)     [Response frame: 29]     &gt; Data (72 bytes) </pre>						

Figure 22.

In the first packet, which is the request packet, the layers are Ethernet, IPv4, UDP, VXLAN, Ethernet, IPv4, and ICMP. It contains the source and destination IP as well as the VXLAN id that was configured in CL3. The VXLAN is added below UDP and above Ethernet II.

29	10.0.17739	192.168.5.65	10.0.20.3	ICMP	164 Echo (ping) reply	id=0x0002, seq=0/0, ttl=255 (request in 28)	
<							>
>	Frame 29: 164 bytes on wire (1312 bits), 164 bytes captured (1312 bits) on interface -, id 0						
▼	Ethernet II, Src: 0c:b0:aa:c3:00:02 (0c:b0:aa:c3:00:02), Dst: 0c:94:a1:7c:00:02 (0c:94:a1:7c:00:02)						
>	Destination: 0c:94:a1:7c:00:02 (0c:94:a1:7c:00:02)						
>	Source: 0c:b0:aa:c3:00:02 (0c:b0:aa:c3:00:02)						
	Type: IPv4 (0x0800)						
▼	Internet Protocol Version 4, Src: 10.0.0.5, Dst: 10.0.0.3						
	0100 .... = Version: 4						
	.... 0101 = Header Length: 20 bytes (5)						
>	Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)						
	Total Length: 150						
	Identification: 0xe795 (59285)						
>	Flags: 0x00						
	Fragment Offset: 0						
	Time to Live: 63						
	Protocol: UDP (17)						
	Header Checksum: 0x7fba [validation disabled]						
	[Header checksum status: Unverified]						
	Source Address: 10.0.0.5						
	Destination Address: 10.0.0.3						
>	User Datagram Protocol, Src Port: 52902, Dst Port: 4789						
▼	Virtual eXtensible Local Area Network						
>	Flags: 0x0000, VXLAN Network ID (VNI)						
	Group Policy ID: 0						
	VXLAN Network Identifier (VNI): 20						
	Reserved: 0						
▼	Ethernet II, Src: ca:03:2f:28:00:1c (ca:03:2f:28:00:1c), Dst: ca:01:30:ac:00:1c (ca:01:30:ac:00:1c)						
>	Destination: ca:01:30:ac:00:1c (ca:01:30:ac:00:1c)						
>	Source: ca:03:2f:28:00:1c (ca:03:2f:28:00:1c)						
	Type: IPv4 (0x0800)						
▼	Internet Protocol Version 4, Src: 192.168.5.65, Dst: 10.0.20.3						
	0100 .... = Version: 4						
	.... 0101 = Header Length: 20 bytes (5)						
>	Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)						
	Total Length: 100						
	Identification: 0x000a (10)						
>	Flags: 0x00						
	Fragment Offset: 0						
	Time to Live: 255						
	Protocol: ICMP (1)						
	Header Checksum: 0xd7a2 [validation disabled]						
	[Header checksum status: Unverified]						
	Source Address: 192.168.5.65						
	Destination Address: 10.0.20.3						
>	Internet Control Message Protocol						

Figure 23.

30	10.028648	10.0.20.3	192.168.5.65	ICMP	164 Echo (ping) request	id=0x0002, seq=1/256, ttl=255 (reply in 31)	
<							>
>	Frame 30: 164 bytes on wire (1312 bits), 164 bytes captured (1312 bits) on interface -, id 0						
▼	Ethernet II, Src: 0c:94:a1:7c:00:02 (0c:94:a1:7c:00:02), Dst: 0c:b0:aa:c3:00:02 (0c:b0:aa:c3:00:02)						
>	Destination: 0c:b0:aa:c3:00:02 (0c:b0:aa:c3:00:02)						
>	Source: 0c:94:a1:7c:00:02 (0c:94:a1:7c:00:02)						
	Type: IPv4 (0x0800)						
▼	Internet Protocol Version 4, Src: 10.0.0.3, Dst: 10.0.0.5						
	0100 .... = Version: 4						
	.... 0101 = Header Length: 20 bytes (5)						
>	Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)						
	Total Length: 150						
	Identification: 0x098d (2445)						
>	Flags: 0x00						
	Fragment Offset: 0						
	Time to Live: 64						
	Protocol: UDP (17)						
	Header Checksum: 0x5cc3 [validation disabled]						
	[Header checksum status: Unverified]						
	Source Address: 10.0.0.3						
	Destination Address: 10.0.0.5						
>	User Datagram Protocol, Src Port: 59334, Dst Port: 4789						
▼	Virtual eXtensible Local Area Network						
>	Flags: 0x0000, VXLAN Network ID (VNI)						
	Group Policy ID: 0						
	VXLAN Network Identifier (VNI): 20						
	Reserved: 0						
▼	Ethernet II, Src: ca:01:30:ac:00:1c (ca:01:30:ac:00:1c), Dst: ca:03:2f:28:00:1c (ca:03:2f:28:00:1c)						
>	Destination: ca:03:2f:28:00:1c (ca:03:2f:28:00:1c)						
>	Source: ca:01:30:ac:00:1c (ca:01:30:ac:00:1c)						
	Type: IPv4 (0x0800)						
▼	Internet Protocol Version 4, Src: 10.0.20.3, Dst: 192.168.5.65						
	0100 .... = Version: 4						
	.... 0101 = Header Length: 20 bytes (5)						
>	Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)						
	Total Length: 100						
	Identification: 0x000b (11)						
>	Flags: 0x00						
	Fragment Offset: 0						
	Time to Live: 255						
	Protocol: ICMP (1)						
	Header Checksum: 0xd7a1 [validation disabled]						
	[Header checksum status: Unverified]						
	Source Address: 10.0.20.3						
	Destination Address: 192.168.5.65						
>	Internet Control Message Protocol						

Figure 24.

31	10.038719	192.168.5.65	10.0.20.3	ICMP	164	Echo (ping) reply	id=0x0002, seq=1/256, ttl=255 (request in 30)
<div> <div>&lt;</div> <div>&gt;</div> </div>							
<div> <div>&gt;</div> <div>Frame 31: 164 bytes on wire (1312 bits), 164 bytes captured (1312 bits) on interface -, id 0</div> </div>							
<div> <div>&gt;</div> <div>Ethernet II, Src: 0c:b0:aa:c3:00:02 (0c:b0:aa:c3:00:02), Dst: 0c:94:a1:7c:00:02 (0c:94:a1:7c:00:02)</div> </div>							
<div> <div>&gt;</div> <div>Destination: 0c:94:a1:7c:00:02 (0c:94:a1:7c:00:02)</div> </div>							
<div> <div>&gt;</div> <div>Source: 0c:b0:aa:c3:00:02 (0c:b0:aa:c3:00:02)</div> </div>							
<div> <div>&gt;</div> <div>Type: IPv4 (0x0800)</div> </div>							
<div> <div>&gt;</div> <div>Internet Protocol Version 4, Src: 10.0.0.5, Dst: 10.0.0.3</div> </div>							
<div> <div>&gt;</div> <div>0100 .... = Version: 4</div> </div>							
<div> <div>&gt;</div> <div>.... 0101 = Header Length: 20 bytes (5)</div> </div>							
<div> <div>&gt;</div> <div>Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)</div> </div>							
<div> <div>&gt;</div> <div>Total Length: 150</div> </div>							
<div> <div>&gt;</div> <div>Identification: 0xe7a3 (59299)</div> </div>							
<div> <div>&gt;</div> <div>Flags: 0x00</div> </div>							
<div> <div>&gt;</div> <div>Fragment Offset: 0</div> </div>							
<div> <div>&gt;</div> <div>Time to Live: 63</div> </div>							
<div> <div>&gt;</div> <div>Protocol: UDP (17)</div> </div>							
<div> <div>&gt;</div> <div>Header Checksum: 0x7fac [validation disabled]</div> </div>							
<div> <div>&gt;</div> <div>[Header checksum status: Unverified]</div> </div>							
<div> <div>&gt;</div> <div>Source Address: 10.0.0.5</div> </div>							
<div> <div>&gt;</div> <div>Destination Address: 10.0.0.3</div> </div>							
<div> <div>&gt;</div> <div>User Datagram Protocol, Src Port: 52902, Dst Port: 4789</div> </div>							
<div> <div>&gt;</div> <div>Virtual eXtensible Local Area Network</div> </div>							
<div> <div>&gt;</div> <div>Flags: 0x0000, VXLAN Network ID (VNI)</div> </div>							
<div> <div>&gt;</div> <div>Group Policy ID: 0</div> </div>							
<div> <div>&gt;</div> <div>VXLAN Network Identifier (VNI): 20</div> </div>							
<div> <div>&gt;</div> <div>Reserved: 0</div> </div>							
<div> <div>&gt;</div> <div>Ethernet II, Src: ca:03:2f:28:00:1c (ca:03:2f:28:00:1c), Dst: ca:01:30:ac:00:1c (ca:01:30:ac:00:1c)</div> </div>							
<div> <div>&gt;</div> <div>Destination: ca:01:30:ac:00:1c (ca:01:30:ac:00:1c)</div> </div>							
<div> <div>&gt;</div> <div>Source: ca:03:2f:28:00:1c (ca:03:2f:28:00:1c)</div> </div>							
<div> <div>&gt;</div> <div>Type: IPv4 (0x0800)</div> </div>							
<div> <div>&gt;</div> <div>Internet Protocol Version 4, Src: 192.168.5.65, Dst: 10.0.20.3</div> </div>							
<div> <div>&gt;</div> <div>0100 .... = Version: 4</div> </div>							
<div> <div>&gt;</div> <div>.... 0101 = Header Length: 20 bytes (5)</div> </div>							
<div> <div>&gt;</div> <div>Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)</div> </div>							
<div> <div>&gt;</div> <div>Total Length: 100</div> </div>							
<div> <div>&gt;</div> <div>Identification: 0x000b (11)</div> </div>							
<div> <div>&gt;</div> <div>Flags: 0x00</div> </div>							
<div> <div>&gt;</div> <div>Fragment Offset: 0</div> </div>							
<div> <div>&gt;</div> <div>Time to Live: 255</div> </div>							
<div> <div>&gt;</div> <div>Protocol: ICMP (1)</div> </div>							
<div> <div>&gt;</div> <div>Header Checksum: 0xd7a1 [validation disabled]</div> </div>							
<div> <div>&gt;</div> <div>[Header checksum status: Unverified]</div> </div>							
<div> <div>&gt;</div> <div>Source Address: 192.168.5.65</div> </div>							
<div> <div>&gt;</div> <div>Destination Address: 10.0.20.3</div> </div>							
<div> <div>&gt;</div> <div>Internet Control Message Protocol</div> </div>							

Figure 25.

32	10.049256	10.0.20.3	192.168.5.65	ICMP	164	Echo (ping) request	id=0x0002, seq=2/512, ttl=255 (reply in 33)
<div> <div>&lt;</div> <div>&gt;</div> </div>							
<div> <div>&gt;</div> <div>Frame 32: 164 bytes on wire (1312 bits), 164 bytes captured (1312 bits) on interface -, id 0</div> </div>							
<div> <div>&gt;</div> <div>Ethernet II, Src: 0c:94:a1:7c:00:02 (0c:94:a1:7c:00:02), Dst: 0c:b0:aa:c3:00:02 (0c:b0:aa:c3:00:02)</div> </div>							
<div> <div>&gt;</div> <div>Destination: 0c:b0:aa:c3:00:02 (0c:b0:aa:c3:00:02)</div> </div>							
<div> <div>&gt;</div> <div>Source: 0c:94:a1:7c:00:02 (0c:94:a1:7c:00:02)</div> </div>							
<div> <div>&gt;</div> <div>Type: IPv4 (0x0800)</div> </div>							
<div> <div>&gt;</div> <div>Internet Protocol Version 4, Src: 10.0.0.3, Dst: 10.0.0.5</div> </div>							
<div> <div>&gt;</div> <div>0100 .... = Version: 4</div> </div>							
<div> <div>&gt;</div> <div>.... 0101 = Header Length: 20 bytes (5)</div> </div>							
<div> <div>&gt;</div> <div>Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)</div> </div>							
<div> <div>&gt;</div> <div>Total Length: 150</div> </div>							
<div> <div>&gt;</div> <div>Identification: 0x09a1 (2465)</div> </div>							
<div> <div>&gt;</div> <div>Flags: 0x00</div> </div>							
<div> <div>&gt;</div> <div>Fragment Offset: 0</div> </div>							
<div> <div>&gt;</div> <div>Time to Live: 64</div> </div>							
<div> <div>&gt;</div> <div>Protocol: UDP (17)</div> </div>							
<div> <div>&gt;</div> <div>Header Checksum: 0x5caf [validation disabled]</div> </div>							
<div> <div>&gt;</div> <div>[Header checksum status: Unverified]</div> </div>							
<div> <div>&gt;</div> <div>Source Address: 10.0.0.3</div> </div>							
<div> <div>&gt;</div> <div>Destination Address: 10.0.0.5</div> </div>							
<div> <div>&gt;</div> <div>User Datagram Protocol, Src Port: 59334, Dst Port: 4789</div> </div>							
<div> <div>&gt;</div> <div>Virtual eXtensible Local Area Network</div> </div>							
<div> <div>&gt;</div> <div>Flags: 0x0000, VXLAN Network ID (VNI)</div> </div>							
<div> <div>&gt;</div> <div>Group Policy ID: 0</div> </div>							
<div> <div>&gt;</div> <div>VXLAN Network Identifier (VNI): 20</div> </div>							
<div> <div>&gt;</div> <div>Reserved: 0</div> </div>							
<div> <div>&gt;</div> <div>Ethernet II, Src: ca:01:30:ac:00:1c (ca:01:30:ac:00:1c), Dst: ca:03:2f:28:00:1c (ca:03:2f:28:00:1c)</div> </div>							
<div> <div>&gt;</div> <div>Destination: ca:03:2f:28:00:1c (ca:03:2f:28:00:1c)</div> </div>							
<div> <div>&gt;</div> <div>Source: ca:01:30:ac:00:1c (ca:01:30:ac:00:1c)</div> </div>							
<div> <div>&gt;</div> <div>Type: IPv4 (0x0800)</div> </div>							
<div> <div>&gt;</div> <div>Internet Protocol Version 4, Src: 10.0.20.3, Dst: 192.168.5.65</div> </div>							
<div> <div>&gt;</div> <div>0100 .... = Version: 4</div> </div>							
<div> <div>&gt;</div> <div>.... 0101 = Header Length: 20 bytes (5)</div> </div>							
<div> <div>&gt;</div> <div>Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)</div> </div>							
<div> <div>&gt;</div> <div>Total Length: 100</div> </div>							
<div> <div>&gt;</div> <div>Identification: 0x000c (12)</div> </div>							
<div> <div>&gt;</div> <div>Flags: 0x00</div> </div>							
<div> <div>&gt;</div> <div>Fragment Offset: 0</div> </div>							
<div> <div>&gt;</div> <div>Time to Live: 255</div> </div>							
<div> <div>&gt;</div> <div>Protocol: ICMP (1)</div> </div>							
<div> <div>&gt;</div> <div>Header Checksum: 0xd7a0 [validation disabled]</div> </div>							
<div> <div>&gt;</div> <div>[Header checksum status: Unverified]</div> </div>							
<div> <div>&gt;</div> <div>Source Address: 10.0.20.3</div> </div>							
<div> <div>&gt;</div> <div>Destination Address: 192.168.5.65</div> </div>							
<div> <div>&gt;</div> <div>Internet Control Message Protocol</div> </div>							

Figure 26.

33	10.060362	192.168.5.65	10.0.20.3	ICMP	164	Echo (ping) reply	id=0x0002, seq=2/512, ttl=255 (request in 32)
<div> <div>&lt;</div> <div>&gt;</div> </div>							
<div> <div>&gt; Frame 33: 164 bytes on wire (1312 bits), 164 bytes captured (1312 bits) on interface -, id 0</div> <div> <div>&gt; Ethernet II, Src: 0c:b0:aa:c3:00:02 (0c:b0:aa:c3:00:02), Dst: 0c:94:a1:7c:00:02 (0c:94:a1:7c:00:02)</div> <div> <div>&gt; Destination: 0c:94:a1:7c:00:02 (0c:94:a1:7c:00:02)</div> <div>&gt; Source: 0c:b0:aa:c3:00:02 (0c:b0:aa:c3:00:02)</div> <div>Type: IPv4 (0x0800)</div> </div> </div> </div>							
<div> <div>&gt; Internet Protocol Version 4, Src: 10.0.0.5, Dst: 10.0.0.3</div> <div> <div>0100 .... = Version: 4</div> <div>.... 0101 = Header Length: 20 bytes (5)</div> <div>&gt; Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)</div> <div>Total Length: 150</div> <div>Identification: 0xe7ae (59310)</div> <div>&gt; Flags: 0x00</div> <div>Fragment Offset: 0</div> <div>Time to Live: 63</div> <div>Protocol: UDP (17)</div> <div>Header Checksum: 0x7fa1 [validation disabled]</div> <div>[Header checksum status: Unverified]</div> <div>Source Address: 10.0.0.5</div> <div>Destination Address: 10.0.0.3</div> </div> </div>							
<div> <div>&gt; User Datagram Protocol, Src Port: 52902, Dst Port: 4789</div> <div> <div>&gt; Virtual eXtensible Local Area Network</div> <div> <div>&gt; Flags: 0x0000, VXLAN Network ID (VNI)</div> <div>Group Policy ID: 0</div> <div>VXLAN Network Identifier (VNI): 20</div> <div>Reserved: 0</div> </div> </div> </div>							
<div> <div>&gt; Ethernet II, Src: ca:03:2f:28:00:1c (ca:03:2f:28:00:1c), Dst: ca:01:30:ac:00:1c (ca:01:30:ac:00:1c)</div> <div> <div>&gt; Destination: ca:01:30:ac:00:1c (ca:01:30:ac:00:1c)</div> <div>&gt; Source: ca:03:2f:28:00:1c (ca:03:2f:28:00:1c)</div> <div>Type: IPv4 (0x0800)</div> </div> </div>							
<div> <div>&gt; Internet Protocol Version 4, Src: 192.168.5.65, Dst: 10.0.20.3</div> <div> <div>0100 .... = Version: 4</div> <div>.... 0101 = Header Length: 20 bytes (5)</div> <div>&gt; Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)</div> <div>Total Length: 100</div> <div>Identification: 0x000c (12)</div> <div>&gt; Flags: 0x00</div> <div>Fragment Offset: 0</div> <div>Time to Live: 255</div> <div>Protocol: ICMP (1)</div> <div>Header Checksum: 0xd7a0 [validation disabled]</div> <div>[Header checksum status: Unverified]</div> <div>Source Address: 192.168.5.65</div> <div>Destination Address: 10.0.20.3</div> </div> </div>							
<div> <div>&gt; Internet Control Message Protocol</div> </div>							

Figure 27.

34	10.070762	10.0.20.3	192.168.5.65	ICMP	164	Echo (ping) request	id=0x0002, seq=3/768, ttl=255 (reply in 35)
<div> <div>&lt;</div> <div>&gt;</div> </div>							
<div> <div>&gt; Frame 34: 164 bytes on wire (1312 bits), 164 bytes captured (1312 bits) on interface -, id 0</div> <div> <div>&gt; Ethernet II, Src: 0c:b0:aa:c3:00:02 (0c:b0:aa:c3:00:02), Dst: 0c:b0:aa:c3:00:02 (0c:b0:aa:c3:00:02)</div> <div> <div>&gt; Destination: 0c:b0:aa:c3:00:02 (0c:b0:aa:c3:00:02)</div> <div>&gt; Source: 0c:94:a1:7c:00:02 (0c:94:a1:7c:00:02)</div> <div>Type: IPv4 (0x0800)</div> </div> </div> </div>							
<div> <div>&gt; Internet Protocol Version 4, Src: 10.0.0.3, Dst: 10.0.0.5</div> <div> <div>0100 .... = Version: 4</div> <div>.... 0101 = Header Length: 20 bytes (5)</div> <div>&gt; Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)</div> <div>Total Length: 150</div> <div>Identification: 0x09b1 (2481)</div> <div>&gt; Flags: 0x00</div> <div>Fragment Offset: 0</div> <div>Time to Live: 64</div> <div>Protocol: UDP (17)</div> <div>Header Checksum: 0x5c9f [validation disabled]</div> <div>[Header checksum status: Unverified]</div> <div>Source Address: 10.0.0.3</div> <div>Destination Address: 10.0.0.5</div> </div> </div>							
<div> <div>&gt; User Datagram Protocol, Src Port: 59334, Dst Port: 4789</div> <div> <div>&gt; Virtual eXtensible Local Area Network</div> <div> <div>&gt; Flags: 0x0000, VXLAN Network ID (VNI)</div> <div>Group Policy ID: 0</div> <div>VXLAN Network Identifier (VNI): 20</div> <div>Reserved: 0</div> </div> </div> </div>							
<div> <div>&gt; Ethernet II, Src: ca:01:30:ac:00:1c (ca:01:30:ac:00:1c), Dst: ca:03:2f:28:00:1c (ca:03:2f:28:00:1c)</div> <div> <div>&gt; Destination: ca:03:2f:28:00:1c (ca:03:2f:28:00:1c)</div> <div>&gt; Source: ca:01:30:ac:00:1c (ca:01:30:ac:00:1c)</div> <div>Type: IPv4 (0x0800)</div> </div> </div>							
<div> <div>&gt; Internet Protocol Version 4, Src: 10.0.20.3, Dst: 192.168.5.65</div> <div> <div>0100 .... = Version: 4</div> <div>.... 0101 = Header Length: 20 bytes (5)</div> <div>&gt; Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)</div> <div>Total Length: 100</div> <div>Identification: 0x000d (13)</div> <div>&gt; Flags: 0x00</div> <div>Fragment Offset: 0</div> <div>Time to Live: 255</div> <div>Protocol: ICMP (1)</div> <div>Header Checksum: 0xd79f [validation disabled]</div> <div>[Header checksum status: Unverified]</div> <div>Source Address: 10.0.20.3</div> <div>Destination Address: 192.168.5.65</div> </div> </div>							
<div> <div>&gt; Internet Control Message Protocol</div> </div>							

Figure 28.



35	10.081644	192.168.5.65	10.0.20.3	ICMP	164	Echo (ping) reply	id=0x0002, seq=3/768, ttl=255 (request in 34)
<							
>							
Frame 35: 164 bytes on wire (1312 bits), 164 bytes captured (1312 bits) on interface -, id 0							
Ethernet II, Src: 0c:b0:aa:c3:00:02 (0c:b0:aa:c3:00:02), Dst: 0c:94:a1:7c:00:02 (0c:94:a1:7c:00:02)							
Destination: 0c:94:a1:7c:00:02 (0c:94:a1:7c:00:02)							
Source: 0c:b0:aa:c3:00:02 (0c:b0:aa:c3:00:02)							
Type: IPv4 (0x0800)							
Internet Protocol Version 4, Src: 10.0.0.5, Dst: 10.0.0.3							
0100 .... = Version: 4							
.... 0101 = Header Length: 20 bytes (5)							
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)							
Total Length: 150							
Identification: 0xe7bc (59324)							
Flags: 0x00							
Fragment Offset: 0							
Time to Live: 63							
Protocol: UDP (17)							
Header Checksum: 0x7f93 [validation disabled]							
[Header checksum status: Unverified]							
Source Address: 10.0.0.5							
Destination Address: 10.0.0.3							
User Datagram Protocol, Src Port: 52902, Dst Port: 4789							
Virtual eXtensible Local Area Network							
Flags: 0x0000, VXLAN Network ID (VNI)							
Group Policy ID: 0							
VXLAN Network Identifier (VNI): 20							
Reserved: 0							
Ethernet II, Src: ca:03:2f:28:00:1c (ca:03:2f:28:00:1c), Dst: ca:01:30:ac:00:1c (ca:01:30:ac:00:1c)							
Destination: ca:01:30:ac:00:1c (ca:01:30:ac:00:1c)							
Source: ca:03:2f:28:00:1c (ca:03:2f:28:00:1c)							
Type: IPv4 (0x0800)							
Internet Protocol Version 4, Src: 192.168.5.65, Dst: 10.0.20.3							
0100 .... = Version: 4							
.... 0101 = Header Length: 20 bytes (5)							
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)							
Total Length: 100							
Identification: 0x000d (13)							
Flags: 0x00							
Fragment Offset: 0							
Time to Live: 255							
Protocol: ICMP (1)							
Header Checksum: 0xd79f [validation disabled]							
[Header checksum status: Unverified]							
Source Address: 192.168.5.65							
Destination Address: 10.0.20.3							
Internet Control Message Protocol							

Figure 29.

36	10.092251	10.0.20.3	192.168.5.65	ICMP	164	Echo (ping) request	id=0x0002, seq=4/1024, ttl=255 (reply in 37)
<							
>							
Frame 36: 164 bytes on wire (1312 bits), 164 bytes captured (1312 bits) on interface -, id 0							
Ethernet II, Src: 0c:94:a1:7c:00:02 (0c:94:a1:7c:00:02), Dst: 0c:b0:aa:c3:00:02 (0c:b0:aa:c3:00:02)							
Destination: 0c:b0:aa:c3:00:02 (0c:b0:aa:c3:00:02)							
Source: 0c:94:a1:7c:00:02 (0c:94:a1:7c:00:02)							
Type: IPv4 (0x0800)							
Internet Protocol Version 4, Src: 10.0.0.3, Dst: 10.0.0.5							
0100 .... = Version: 4							
.... 0101 = Header Length: 20 bytes (5)							
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)							
Total Length: 150							
Identification: 0x09bd (2493)							
Flags: 0x00							
Fragment Offset: 0							
Time to Live: 64							
Protocol: UDP (17)							
Header Checksum: 0x5c93 [validation disabled]							
[Header checksum status: Unverified]							
Source Address: 10.0.0.3							
Destination Address: 10.0.0.5							
User Datagram Protocol, Src Port: 59334, Dst Port: 4789							
Virtual eXtensible Local Area Network							
Flags: 0x0000, VXLAN Network ID (VNI)							
Group Policy ID: 0							
VXLAN Network Identifier (VNI): 20							
Reserved: 0							
Ethernet II, Src: ca:01:30:ac:00:1c (ca:01:30:ac:00:1c), Dst: ca:03:2f:28:00:1c (ca:03:2f:28:00:1c)							
Destination: ca:03:2f:28:00:1c (ca:03:2f:28:00:1c)							
Source: ca:01:30:ac:00:1c (ca:01:30:ac:00:1c)							
Type: IPv4 (0x0800)							
Internet Protocol Version 4, Src: 10.0.20.3, Dst: 192.168.5.65							
0100 .... = Version: 4							
.... 0101 = Header Length: 20 bytes (5)							
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)							
Total Length: 100							
Identification: 0x000e (14)							
Flags: 0x00							
Fragment Offset: 0							
Time to Live: 255							
Protocol: ICMP (1)							
Header Checksum: 0xd79e [validation disabled]							
[Header checksum status: Unverified]							
Source Address: 10.0.20.3							
Destination Address: 192.168.5.65							
Internet Control Message Protocol							

Figure 30.

37	10.103879	192.168.5.65	10.0.20.3	ICMP	164	Echo (ping) reply	id=0x0002, seq=4/1024, ttl=255 (request in 36)
> Frame 37: 164 bytes on wire (1312 bits), 164 bytes captured (1312 bits) on interface -, id 0 > Ethernet II, Src: 0c:b0:aa:c3:00:02 (0c:b0:aa:c3:00:02), Dst: 0c:94:a1:7c:00:02 (0c:94:a1:7c:00:02) > Destination: 0c:94:a1:7c:00:02 (0c:94:a1:7c:00:02) > Source: 0c:b0:aa:c3:00:02 (0c:b0:aa:c3:00:02) Type: IPv4 (0x0800) > Internet Protocol Version 4, Src: 10.0.0.5, Dst: 10.0.0.3 0100 .... = Version: 4 .... 0101 = Header Length: 20 bytes (5) > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT) Total Length: 150 Identification: 0xe7ce (59342) > Flags: 0x00 Fragment Offset: 0 Time to Live: 63 Protocol: UDP (17) Header Checksum: 0x7f81 [validation disabled] [Header checksum status: Unverified] Source Address: 10.0.0.5 Destination Address: 10.0.0.3 > User Datagram Protocol, Src Port: 52902, Dst Port: 4789 > Virtual eXtensible Local Area Network > Flags: 0x0000, VXLAN Network ID (VNI) Group Policy ID: 0 VXLAN Network Identifier (VNI): 20 Reserved: 0 > Ethernet II, Src: ca:03:2f:28:00:1c (ca:03:2f:28:00:1c), Dst: ca:01:30:ac:00:1c (ca:01:30:ac:00:1c) > Destination: ca:01:30:ac:00:1c (ca:01:30:ac:00:1c) > Source: ca:03:2f:28:00:1c (ca:03:2f:28:00:1c) Type: IPv4 (0x0800) > Internet Protocol Version 4, Src: 192.168.5.65, Dst: 10.0.20.3 0100 .... = Version: 4 .... 0101 = Header Length: 20 bytes (5) > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT) Total Length: 100 Identification: 0x000e (14) > Flags: 0x00 Fragment Offset: 0 Time to Live: 255 Protocol: ICMP (1) Header Checksum: 0xd79e [validation disabled] [Header checksum status: Unverified] Source Address: 192.168.5.65 Destination Address: 10.0.20.3 > Internet Control Message Protocol							

Figure 31.

## Out of CL3 to CL1:

129	55.044226	10.0.10.5	224.0.0.5	OSPF	148	Hello Packet
130	55.818687	fe80::e94:a1ff:fe7c...	ff02::1	ICMPv6	78	Router Advertisement from 0c:94:a1
131	55.884083	10.0.20.4	224.0.0.5	OSPF	148	Hello Packet
132	56.945972	10.0.10.3	224.0.0.5	OSPF	148	Hello Packet
133	57.004739	fe80::ef3:b9ff:fe2c...	fe80::e94:a1ff:fe7c...	BGP	105	KEEPALIVE Message
134	57.005348	fe80::e94:a1ff:fe7c...	fe80::ef3:b9ff:fe2c...	TCP	86	42082 → 179 [ACK] Seq=362 Ack=381
135	57.164946	fe80::e94:a1ff:fe7c...	fe80::ef3:b9ff:fe2c...	BGP	105	KEEPALIVE Message
136	57.165233	fe80::ef3:b9ff:fe2c...	fe80::e94:a1ff:fe7c...	TCP	86	179 → 42082 [ACK] Seq=381 Ack=381

Figure 32.

129	55.044226	10.0.10.5	224.0.0.5	OSPF	148 Hello Packet
130	55.818687	fe80::e94:a1ff:fe7c...	ff02::1	ICMPv6	78 Router Advertisement from 0c:94:a1
131	55.884083	10.0.20.4	224.0.0.5	OSPF	148 Hello Packet
132	56.945972	10.0.10.3	224.0.0.5	OSPF	148 Hello Packet

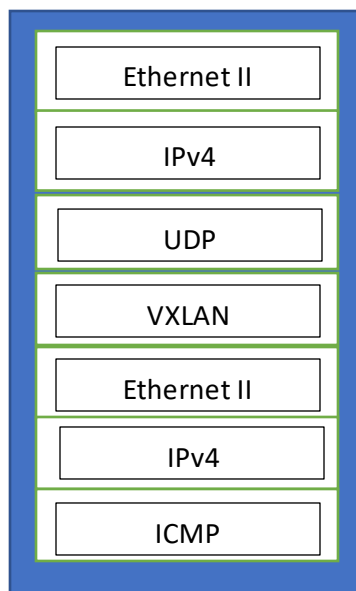
```

> Frame 130: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface -, id 0
▼ Ethernet II, Src: 0c:94:a1:7c:00:01 (0c:94:a1:7c:00:01), Dst: IPv6mcast_01 (33:33:00:00:00:01)
  > Destination: IPv6mcast_01 (33:33:00:00:00:01)
  > Source: 0c:94:a1:7c:00:01 (0c:94:a1:7c:00:01)
  Type: IPv6 (0x86dd)
▼ Internet Protocol Version 6, Src: fe80::e94:a1ff:fe7c:1, Dst: ff02::1
  0110 .... = Version: 6
  > .... 0000 0000 .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
  .... .... 0001 0101 0110 1001 0011 = Flow Label: 0x15693
  Payload Length: 24
  Next Header: ICMPv6 (58)
  Hop Limit: 255
  Source Address: fe80::e94:a1ff:fe7c:1
  Destination Address: ff02::1
  [Source SA MAC: 0c:94:a1:7c:00:01 (0c:94:a1:7c:00:01)]
▼ Internet Control Message Protocol v6
  Type: Router Advertisement (134)
  Code: 0
  Checksum: 0xdde5 [correct]
  [Checksum Status: Good]
  Cur hop limit: 64
  > Flags: 0x00, Prf (Default Router Preference): Medium
  Router lifetime (s): 30
  Reachable time (ms): 0
  Retrans timer (ms): 0
  > ICMPv6 Option (Source link-layer address : 0c:94:a1:7c:00:01)

```

Figure 33.

Looking at the Wireshark capture at the time that the ping from R3 to one of the vrf's in R5 was delivered, in the output of CL3 to CL2, we can see that there is where the request and reply packets are initiated, whereas looking at the captures for CL3 to CL1 the only packet seen during that time is an ICMPv6 packet, as well as some hello packets. Within each of the request and reply packets going between CL3 and CL2, the structure inside is all the same even with multiples of the same packet.



The packet is structured as followed above for each of the request and reply packets. Most of the ping work goes through CL3 and CL2 rather than CL3 to CL1. The SPINES collect all the routing information from the LEAF routers and is then redistributed to each of the LEAF routers.