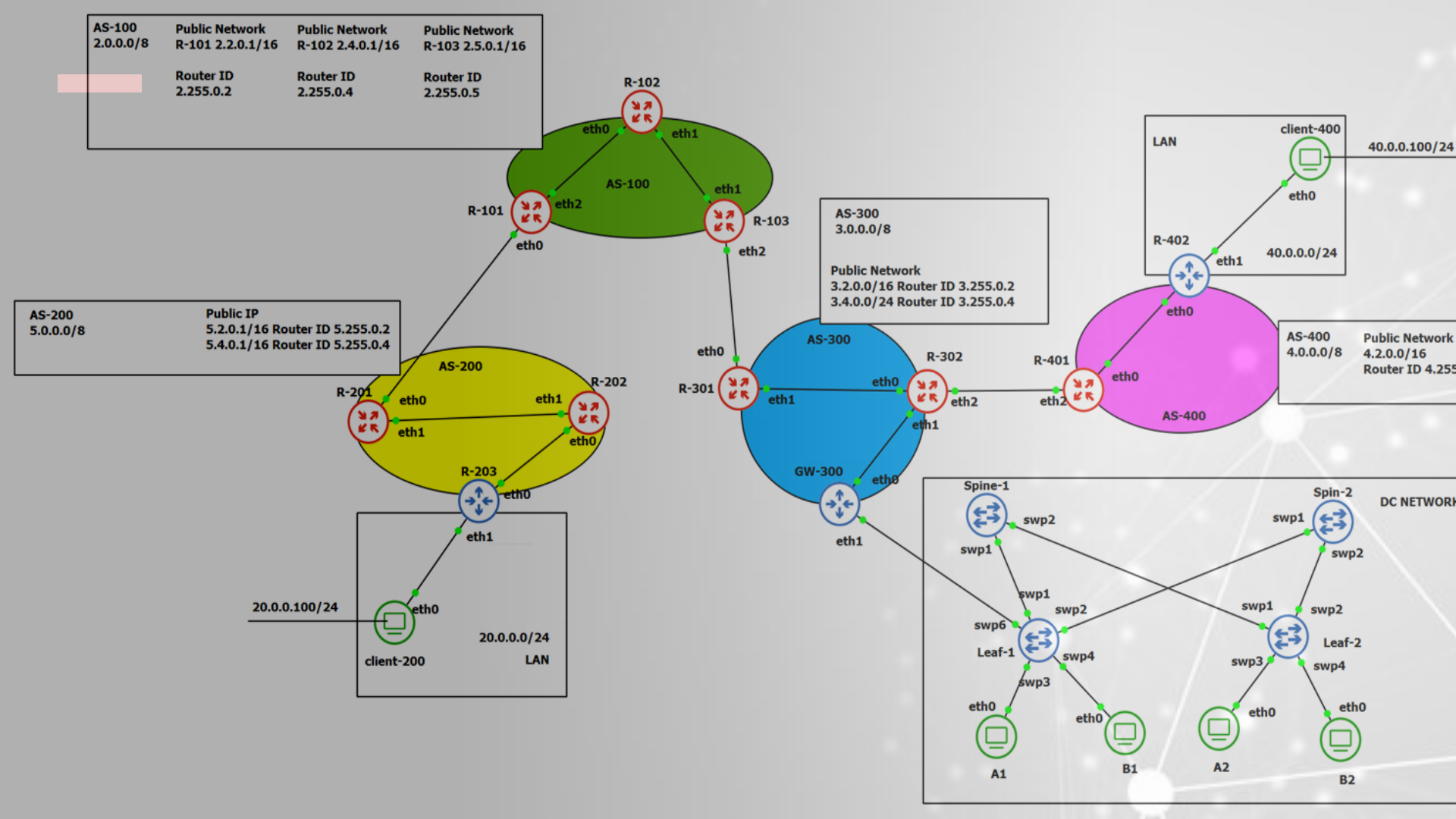
Objective of the project

The project involves designing a multi-AS network infrastructure. AS-100 serves as a transit AS, establishing eBGP peering with AS-200 and AS-300, implementing iBGP peering internally, and optimizing routing through OSPF and LDP/MPLS.

AS-200 configures eBGP peering with AS-100, while implementing dynamic NAT and a firewall on the non-BGP-router R-203. AS-300 establishes eBGP peering with AS100 and AS400, configuring iBGP internally. GW-300 server, acts as an Access Gateway for the Data Center network with dynamic NAT and an OpenVPN server.

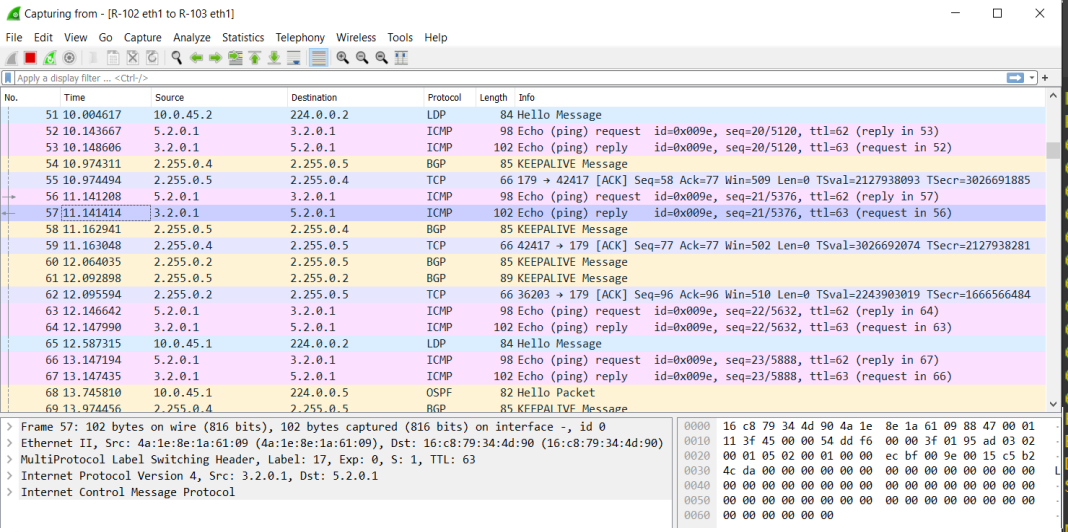
The Data Center network adopts VXLAN/EVPN forwarding, accommodating tenants A and B. AS-400, with lateral peering with AS-300, establishes eBGP peering. The project concludes with the implementation of OpenVPN, securing connections between Client-200, R402's LAN, and the Datacenter network, enhancing overall network security and connectivity.

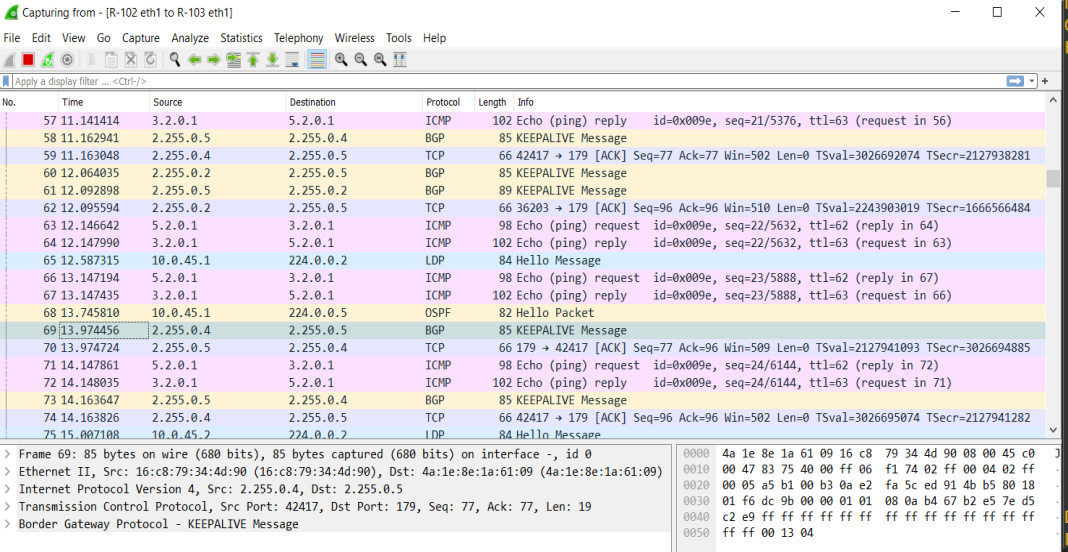

AS-100
2.0.0.0/8
Public Network
R-101 2.2.0.1/16
Router ID
2.255.0.2
Public Network
R-102 2.4.0.1/16
Router ID
2.255.0.4
Public Network
R-103 2.5.0.1/16
Router ID
2.255.0.5
R-102
eth0
eth1
AS-100
eth1
R-101
eth2
R-103
eth0
eth2
AS-300
3.0.0.0/8
Public Network
3.2.0.0/16 Router ID 3.255.0.2
3.4.0.0/24 Router ID 3.255.0.4
LAN
client-400
40.0.0.100/24
eth0
R-402
eth1
40.0.0.0/24
eth0
AS-200
5.0.0.0/8
Public IP
5.2.0.1/16 Router ID 5.255.0.2
5.4.0.1/16 Router ID 5.255.0.4
AS-200
R-201
eth0
eth1
R-202
eth1
eth0
R-203
eth0
eth1
20.0.0.100/24
eth0
client-200
20.0.0.0/24
LAN
eth0
R-301
eth1
AS-300
eth0
R-302
eth2
eth1
GW-300
eth0
eth1
R-401
eth2
eth0
AS-400
AS-400
4.0.0.0/8
Public Network
4.2.0.0/16
Router ID 4.255
Spine-1
swp2
swp1
Spin-2
swp1
swp2
DC NETWORK
swp1
swp2
swp6
Leaf-1
swp4
swp3
swp1
swp2
Leaf-2
swp3
swp4
eth0
A1
eth0
B1
eth0
A2
eth0
B2

AS-100
2.0.0.0/8

- The Autonomous system 100 has 3 routers R-101 R-102 and R-103.
- R-101 has eBGP peering with AS-200 R-202.
- R-102 has iBGP peering with internal routers.
- R-103 has eBGP peering with AS-300 R-301
- All router has Multi-Protocol Packet Switching MPLS and configure Open Shortest Path First OSPF
- Public Network of R-101 2.2.0.1/16 and Router ID 2.255.0.2
- Public Network of R-102 2.4.0.1/16 and Router ID 2.255.0.4
- Public Network of R-103 2.5.0.1/16 and Router ID 2.255.0.5

AS-100 Working





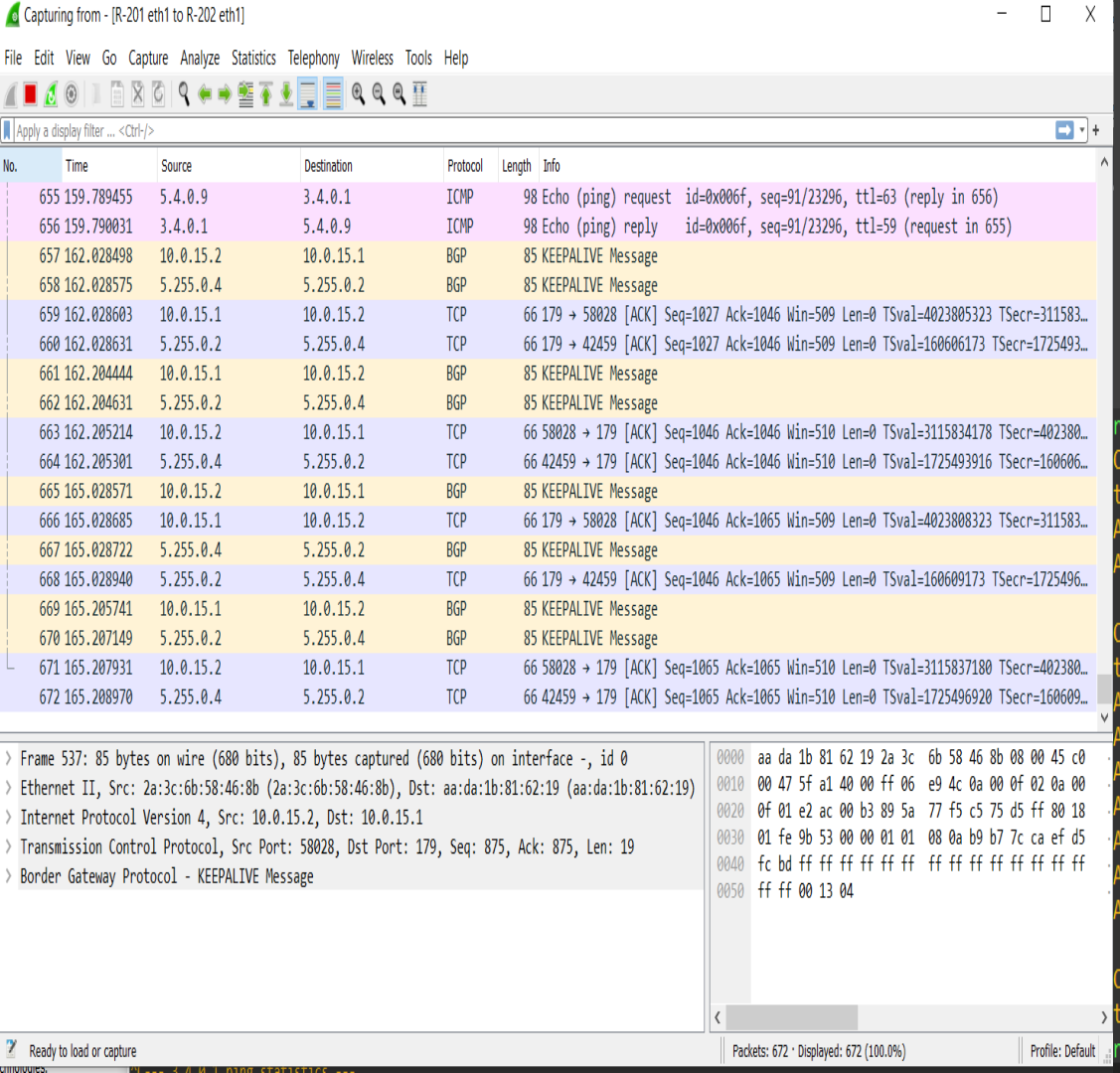

```
R-201:~# ping 3.2.0.1 -I 5.2.0.1
PING 3.2.0.1 (3.2.0.1) from 5.2.0.1: 56 data bytes
64 bytes from 3.2.0.1: seq=0 ttl=61 time=0.851 ms
64 bytes from 3.2.0.1: seq=1 ttl=61 time=4.737 ms
64 bytes from 3.2.0.1: seq=2 ttl=61 time=0.938 ms
64 bytes from 3.2.0.1: seq=3 ttl=61 time=0.896 ms
64 bytes from 3.2.0.1: seq=4 ttl=61 time=1.820 ms
64 bytes from 3.2.0.1: seq=5 ttl=61 time=0.820 ms
64 bytes from 3.2.0.1: seq=6 ttl=61 time=1.071 ms
64 bytes from 3.2.0.1: seq=7 ttl=61 time=0.860 ms
64 bytes from 3.2.0.1: seq=8 ttl=61 time=0.653 ms
64 bytes from 3.2.0.1: seq=9 ttl=61 time=0.552 ms
64 bytes from 3.2.0.1: seq=10 ttl=61 time=0.797 ms
64 bytes from 3.2.0.1: seq=11 ttl=61 time=0.905 ms
R-102# show ip bgp
BGP table version is 17, local router ID is 2.255.0.4, vrf id 0
Default local pref 100, local AS 100
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
RPKI validation codes: V valid, I invalid, N Not found

   Network          Next Hop            Metric LocPrf Weight Path
*>i2.2.0.0/16       2.255.0.2(R-101)
                                             0    100      0 i
*> 2.4.0.0/16       0.0.0.0(R-102)           0         32768 i
*>i2.5.0.0/16       2.255.0.5(R-103)
                                             0    100      0 i
*>i3.2.0.0/16       2.255.0.5(R-103)
                                             0    100      0 300 i
*>i3.4.0.0/16       2.255.0.5(R-103)
                                             0    100      0 300 i
*>i4.2.0.0/16       2.255.0.5(R-103)
                                             0    100      0 300 400 i
*>i5.2.0.0/16       2.255.0.2(R-101)
                                             0    100      0 200 i
*>i5.4.0.0/16       2.255.0.2(R-101)
                                             0    100      0 200 i
*>i10.0.37.0/30     2.255.0.5(R-103)
                                             0    100      0 300 i

Displayed  9 routes and 9 total paths
R-102#
```

AS-200 5.0.0.0/8

- The Autonomous system 200 has 3 routers R-201 R-202 and R-203.
- R-201 has eBGP peering with AS-100 R-101.
- R-202 has iBGP peering with internal router R-201.
- R-203 is absent from the BGP
- R-201 and R-202 configure with Open Shortest Path First OSPF
- R-203 has default route with R-202, and Access gateway of LAN attached to it, configuration of Dynamic NAT and a Simple firewall.
- Public Network of R-201 5.2.0.1/16 and Router ID 5.255.0.2
- Public Network of R-202 5.4.0.1/16 and Router ID 5.255.0.4
- Public Network of R-203 of AS-200 pool 5.4.0.8/30



AS-200 Working

R-203 Dynamic NAT conf

```
sysctl -w net.ipv4.ip_forward=1
ip addr add 20.0.0.1/24 dev eth1
ip addr add 5.4.0.9/30 dev eth0
ip route add default via 5.4.0.10
iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
echo 1 > /proc/sys/net/ipv4/ip_forward
```

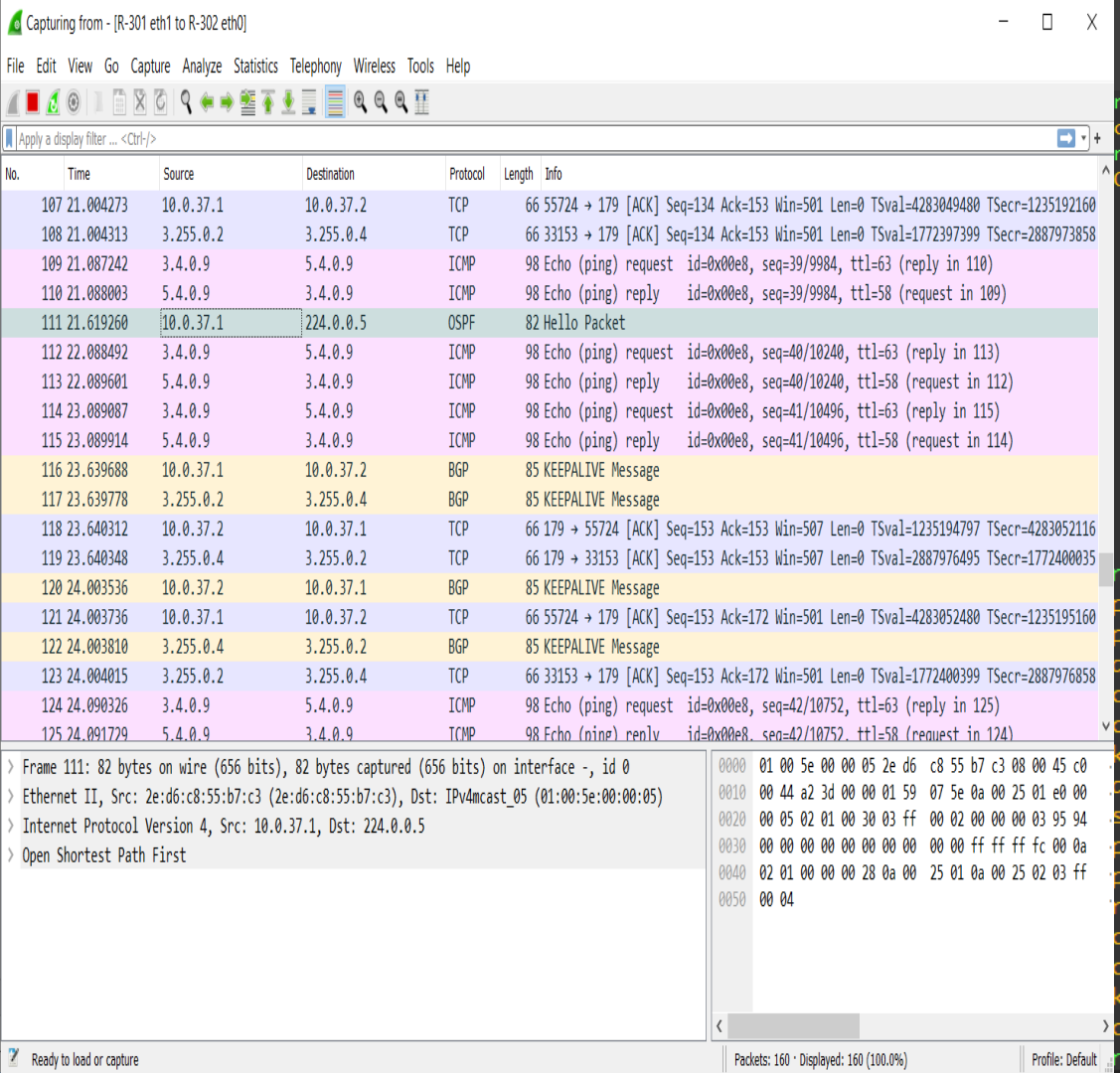
```
root@R-203:/# sudo iptables -L
Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere             state ESTABLISHED
ACCEPT     icmp --  anywhere             anywhere

Chain FORWARD (policy DROP)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere             state ESTABLISHED
ACCEPT     icmp --  anywhere             anywhere
ACCEPT     all  --  anywhere             anywhere
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:http
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:https
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:ssh
ACCEPT     udp  --  anywhere             anywhere             udp dpt:domain

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
root@R-203:/#
```

AS-300 3.0.0.0/8

- The Autonomous system 300 has 3 routers R-301 R-302 and GW-300.
- R-301 has eBGP peering with AS-100 R-103.
- R-302 has iBGP peering with internal router R-301.
- GW-300 is absent from the BGP
- GW-300 is the OpenVPN Server, It has default route via with R-302, and Access gateway of Data Center and a configuration of Dynamic NAT,
- GW-300 has client1(client-200), client(R-203) and Server(GW-300) certificates + dh parameters + OpenVPN conf
- Public Network of R-301 3.2.0.1/16 and Router ID 3.255.0.2
- Public Network of R-302 3.4.0.1/24 and Router ID 3.255.0.4
- Public Network of GW-300 of AS-300 pool 3.4.0.9/24



AS-300 Working

```
root@GW-300:~/CA/server# ls
ca.crt  ccd  dh.pem  server.crt  server.key  server.ovpn
root@GW-300:~/CA/server# cat server.crt
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            9b:9e:05:2d:06:63:89:49:d3:70:e0:2e:1c:ad:ba:4c
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: CN=OVPN_PRO_CA
        Validity
            Not Before: Jan 27 22:02:24 2024 GMT
            Not After : May  1 22:02:24 2026 GMT
        Subject: CN=server
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
root@GW-300:~/CA/server# cat server.ovpn
port 1194
proto udp
dev tun
ca ca.crt
cert server.crt
key server.key
dh dh.pem
server 192.168.100.0 255.255.255.0
push "route 40.0.0.0 255.255.255.0"
push "route 10.0.31.0 255.255.255.252"
route 40.0.0.0 255.255.255.0
client-config-dir ccd
client-to-client
keepalive 10 120
cipher AES-256-GCM
root@GW-300:~/CA/server#
```

AS-400
4.0.0.0/8

- The Autonomous system 400 has 2 routers R-401 R-402
- R-401 has eBGP peering with AS-300 R-302.
- R-402 is absent from the BGP
- R-402 is the OpenVPN Client2, It has default route via with R-401, R-402 is an OpenVPN client, providing VPN access to and from the LAN attached to it. and Access gateway of LAN with a configuration of Dynamic NAT,
- Public Network of R-401 4.2.0.1/16 and Router ID 4.255.0.2
- Public Network of R-402 of AS-400 pool 4.4.0.9/24

```
root@R-402:~/ovpn# ls
ca.crt  client2.crt  client2.key  client2.ovpn
root@R-402:~/ovpn# cat client2.ovpn
client
dev tun
proto udp
remote 3.4.0.9 1194
resolv-retry infinite
ca ca.crt
cert client2.crt
key client2.key
remote-cert-tls server
cipher AES-256-GCM

root@R-402:~/ovpn#
```

```
R-401#
R-401# show running config
% Unknown command: show running config
R-401# show running-config
Building configuration...

Current configuration:
!
frr version 9.0.1_git
frr defaults datacenter
hostname R-401
no ipv6 forwarding
!
interface eth0
 ip address 4.2.0.10/24
exit
!
interface eth2
 ip address 10.0.41.1/30
exit
!
interface lo
 ip address 4.2.0.1/16
 ip address 4.255.0.2/32
exit
!
router bgp 400
 neighbor 10.0.41.2 remote-as 300
 !
 address-family ipv4 unicast
  network 4.2.0.0/16
  neighbor 10.0.41.2 next-hop-self
 exit-address-family
exit
!
router ospf
 ospf router-id 4.255.0.2
 network 4.2.0.0/16 area 4
 network 4.2.0.0/24 area 4
 network 4.255.0.2/32 area 4
 network 10.0.41.0/30 area 4
exit
!
end
R-401#
```

```
IPv4 Unicast Summary (VRF default):
BGP router identifier 4.255.0.2, local AS number 400 vrf-id 0
BGP table version 33
RIB entries 17, using 3264 bytes of memory
Peers 1, using 13 KiB of memory

Neighbor        V         AS   MsgRcvd   MsgSent   TblVer  InQ OutQ  Up/Down State/PfxRcd   PfxSnt Desc
R-302(10.0.41.2) 4        300     29717     29724       33    0    0 19:52:24            8        9 N/A

Total number of neighbors 1
R-401# show ip bgp
BGP table version is 33, local router ID is 4.255.0.2, vrf id 0
Default local pref 100, local AS 400
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
RPKI validation codes: V valid, I invalid, N Not found

    Network          Next Hop            Metric LocPrf Weight Path
 *> 2.2.0.0/16       10.0.41.2(R-302)                       0 300 100 i
 *> 2.4.0.0/16       10.0.41.2(R-302)                       0 300 100 i
 *> 2.5.0.0/16       10.0.41.2(R-302)                       0 300 100 i
 *> 3.2.0.0/16       10.0.41.2(R-302)                       0 300 i
 *> 3.4.0.0/16       10.0.41.2(R-302)                       0 300 i
 *> 4.2.0.0/16       0.0.0.0(R-401)                 0    32768 i
 *> 5.2.0.0/16       10.0.41.2(R-302)                       0 300 100 200 i
 *> 5.4.0.0/16       10.0.41.2(R-302)                       0 300 100 200 i
 *> 10.0.37.0/30     10.0.41.2(R-302)                       0 300 i

Displayed  9 routes and 9 total paths
R-401# exit
R-401:~# ping 5.4.0.9 -I 4.2.0.1
PING 5.4.0.9 (5.4.0.9) from 4.2.0.1: 56 data bytes
64 bytes from 5.4.0.9: seq=0 ttl=57 time=1.438 ms
64 bytes from 5.4.0.9: seq=1 ttl=57 time=1.369 ms
^C
--- 5.4.0.9 ping statistics ---
```

DC Network

- The Data Center contain a Leaf-Spine Network. two/two-tier topologies
- Configuration of VXLAN static tunnels
- Configuration of EVPN with MP-eBGP peering
- The two tenant connected to leaf-1 and leaf-2
- L3VNI → Layer 3 VXLAN Network Identifier for each tenant, and both are different broad cast domain
- A1 and B2 are same broadcast domain and A2 and B2 same broadcast domain
- L3VNI **1020**, common to both broadcast domain **L2VNI 100** and **L2VNI 200**
- Leaf-1 has connectivity of GW-300 server, with default route.

Leaf – 1 to GW-300

```
cumulus@cumulus:mgmt:~$ ip r
default via 10.0.31.1 dev swp6
2.2.2.2 proto ospf metric 20
        nexthop via 10.1.1.2 dev swp1 weight 1
        nexthop via 10.1.2.2 dev swp2 weight 1
3.4.0.0/24 via 10.0.31.1 dev swp6
4.4.4.4 via 10.1.1.2 dev swp1 proto ospf metric 20
5.5.5.5 via 10.1.2.2 dev swp2 proto ospf metric 20
10.0.31.0/30 dev swp6 proto kernel scope link src 10.0.31.2
10.1.1.0/30 dev swp1 proto kernel scope link src 10.1.1.1
10.1.2.0/30 dev swp2 proto kernel scope link src 10.1.2.1
10.2.1.0/30 via 10.1.1.2 dev swp1 proto ospf metric 20
10.2.2.0/30 via 10.1.2.2 dev swp2 proto ospf metric 20
cumulus@cumulus:mgmt:~$
```

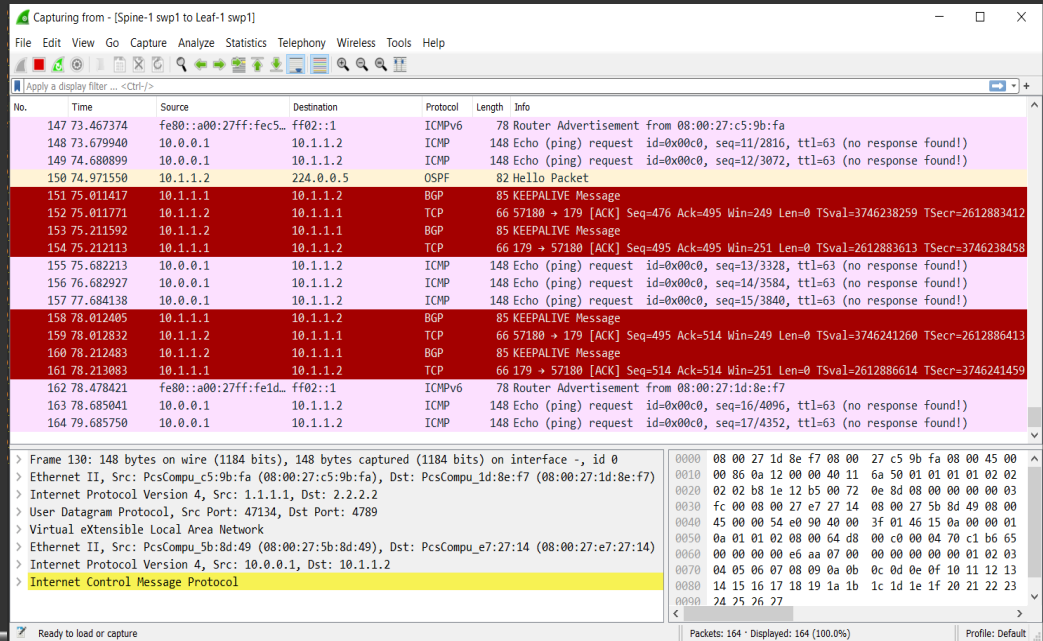
```
cumulus@cumulus:mgmt:~$ ping 3.4.0.9
vrf-wrapper.sh: switching to vrf "default"; use '--no-vrf-switch' to disable
PING 3.4.0.9 (3.4.0.9) 56(84) bytes of data.
64 bytes from 3.4.0.9: icmp_seq=1 ttl=64 time=0.969 ms
64 bytes from 3.4.0.9: icmp_seq=2 ttl=64 time=0.899 ms
64 bytes from 3.4.0.9: icmp_seq=3 ttl=64 time=0.952 ms
64 bytes from 3.4.0.9: icmp_seq=4 ttl=64 time=0.981 ms
64 bytes from 3.4.0.9: icmp_seq=5 ttl=64 time=1.02 ms
64 bytes from 3.4.0.9: icmp_seq=6 ttl=64 time=1.07 ms
64 bytes from 3.4.0.9: icmp_seq=7 ttl=64 time=2.05 ms
64 bytes from 3.4.0.9: icmp_seq=8 ttl=64 time=0.949 ms
^C
cumulus@cumulus:mgmt:~$ net show evpn vni
```

VNI	Type	VxLAN IF	# MACs	# ARPs	# Remote VTEPs	Tenant VRF
100	L2	vni100	3	6	1	TEN1
200	L2	vni200	3	6	1	TEN1
1020	L3	vni-1020	1	1	n/a	TEN1

```
cumulus@cumulus:mgmt:~$
```

A1 to A2 and A1 to B2

```
root@A1:/# ip r
default via 10.0.0.254 dev eth0
10.0.0.0/24 dev eth0 proto kernel scope link src 10.0.0.1
root@A1:/# ping 10.0.0.2
PING 10.0.0.2 (10.0.0.2): 56 data bytes
64 bytes from 10.0.0.2: icmp_seq=0 ttl=64 time=3.966 ms
64 bytes from 10.0.0.2: icmp_seq=1 ttl=64 time=7.860 ms
64 bytes from 10.0.0.2: icmp_seq=2 ttl=64 time=7.253 ms
64 bytes from 10.0.0.2: icmp_seq=3 ttl=64 time=3.966 ms
64 bytes from 10.0.0.2: icmp_seq=4 ttl=64 time=3.961 ms
^C--- 10.0.0.2 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max/stddev = 3.961/5.401/7.860/1.770 ms
root@A1:/#
```



OPENVPN Client-200 GW-300 R-402

```
root@R-402:~/ovpn# openvpn client2.ovpn &
[1] 210
root@R-402:~/ovpn# 2024-01-28 22:23:52 WARNING: file 'client2.key' is group or ot
2024-01-28 22:23:52 OpenVPN 2.5.5 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4
2024-01-28 22:23:52 library versions: OpenSSL 3.0.2 15 Mar 2022, LZO 2.10
2024-01-28 22:23:52 TCP/UDP: Preserving recently used remote address: [AF_INET]3
2024-01-28 22:23:52 UDP link local (bound): [AF_INET][undef]:1194
2024-01-28 22:23:52 UDP link remote: [AF_INET]3.4.0.9:1194
2024-01-28 22:23:52 [server] Peer Connection Initiated with [AF_INET]3.4.0.9:119
2024-01-28 22:23:52 TUN/TAP device tun0 opened
2024-01-28 22:23:52 net_iface_mtu_set: mtu 1500 for tun0
2024-01-28 22:23:52 net_iface_up: set tun0 up
2024-01-28 22:23:52 net_addr_ptp_v4_add: 192.168.100.6 peer 192.168.100.5 dev tun
2024-01-28 22:23:52 WARNING: this configuration may cache passwords in memory --
2024-01-28 22:23:52 Initialization Sequence Completed
root@client-200:~/ovpn# ls
ca.crt  client1.crt  client1.key  client1.ovpn
root@client-200:~/ovpn# openvpn client1.ovpn &
[1] 147
root@client-200:~/ovpn# 2024-01-28 22:24:58 WARNING: file 'client1.key' is group or others accessible
2024-01-28 22:24:58 OpenVPN 2.5.5 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PK
TINFO] [AEAD] built on Jul 14 2022
2024-01-28 22:24:58 library versions: OpenSSL 3.0.2 15 Mar 2022, LZO 2.10
2024-01-28 22:24:58 TCP/UDP: Preserving recently used remote address: [AF_INET]3.4.0.9:1194
2024-01-28 22:24:58 UDP link local (bound): [AF_INET][undef]:1194
2024-01-28 22:24:58 UDP link remote: [AF_INET]3.4.0.9:1194
2024-01-28 22:24:58 [server] Peer Connection Initiated with [AF_INET]3.4.0.9:1194
2024-01-28 22:24:58 TUN/TAP device tun0 opened
2024-01-28 22:24:58 net_iface_mtu_set: mtu 1500 for tun0
2024-01-28 22:24:58 net_iface_up: set tun0 up
2024-01-28 22:24:58 net_addr_ptp_v4_add: 192.168.100.10 peer 192.168.100.9 dev tun0
2024-01-28 22:24:58 WARNING: this configuration may cache passwords in memory -- use the auth-nocache opt
ion to prevent this
2024-01-28 22:24:58 Initialization Sequence Completed
```

```
root@GW-300:~/CA/server# 2024-01-28 22:23:40 WARNING: --topology net30 support for server configs wit
2024-01-28 22:23:40 OpenVPN 2.5.5 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [M
2024-01-28 22:23:40 library versions: OpenSSL 3.0.2 15 Mar 2022, LZO 2.10
2024-01-28 22:23:40 TUN/TAP device tun0 opened
2024-01-28 22:23:40 net_iface_mtu_set: mtu 1500 for tun0
2024-01-28 22:23:40 net_iface_up: set tun0 up
2024-01-28 22:23:40 net_addr_ptp_v4_add: 192.168.100.1 peer 192.168.100.2 dev tun0
2024-01-28 22:23:40 Could not determine IPv4/IPv6 protocol. Using AF_INET
2024-01-28 22:23:40 UDPv4 link local (bound): [AF_INET][undef]:1194
2024-01-28 22:23:40 UDPv4 link remote: [AF_UNSPEC]
2024-01-28 22:23:40 Initialization Sequence Completed
2024-01-28 22:23:52 4.2.0.9:1194 peer info: IV_VER=2.5.5
2024-01-28 22:23:52 4.2.0.9:1194 peer info: IV_PLAT=linux
2024-01-28 22:23:52 4.2.0.9:1194 peer info: IV_PROTO=6
2024-01-28 22:23:52 4.2.0.9:1194 peer info: IV_NCP=2
2024-01-28 22:23:52 4.2.0.9:1194 peer info: IV_CIPHERS=AES-256-GCM:AES-128-GCM
2024-01-28 22:23:52 4.2.0.9:1194 peer info: IV_LZ4=1
2024-01-28 22:23:52 4.2.0.9:1194 peer info: IV_LZ4v2=1
2024-01-28 22:23:52 4.2.0.9:1194 peer info: IV_LZO=1
2024-01-28 22:23:52 4.2.0.9:1194 peer info: IV_COMP_STUB=1
2024-01-28 22:23:52 4.2.0.9:1194 peer info: IV_COMP_STUBv2=1
2024-01-28 22:23:52 4.2.0.9:1194 peer info: IV_TCPNL=1
2024-01-28 22:23:52 4.2.0.9:1194 [client2] Peer Connection Initiated with [AF_INET]4.2.0.9:1194
2024-01-28 22:23:52 client2/4.2.0.9:1194 MULTI_sva: pool returned IPv4=192.168.100.6, IPv6=(Not enabl
2024-01-28 22:24:58 5.4.0.9:1194 peer info: IV_VER=2.5.5
2024-01-28 22:24:58 5.4.0.9:1194 peer info: IV_PLAT=linux
2024-01-28 22:24:58 5.4.0.9:1194 peer info: IV_PROTO=6
2024-01-28 22:24:58 5.4.0.9:1194 peer info: IV_NCP=2
2024-01-28 22:24:58 5.4.0.9:1194 peer info: IV_CIPHERS=AES-256-GCM:AES-128-GCM
2024-01-28 22:24:58 5.4.0.9:1194 peer info: IV_LZ4=1
2024-01-28 22:24:58 5.4.0.9:1194 peer info: IV_LZ4v2=1
2024-01-28 22:24:58 5.4.0.9:1194 peer info: IV_LZO=1
2024-01-28 22:24:58 5.4.0.9:1194 peer info: IV_COMP_STUB=1
2024-01-28 22:24:58 5.4.0.9:1194 peer info: IV_COMP_STUBv2=1
2024-01-28 22:24:58 5.4.0.9:1194 peer info: IV_TCPNL=1
2024-01-28 22:24:58 5.4.0.9:1194 [client1] Peer Connection Initiated with [AF_INET]5.4.0.9:1194
2024-01-28 22:24:58 client1/5.4.0.9:1194 MULTI_sva: pool returned IPv4=192.168.100.10, IPv6=(Not enab
```

Client-200 to Client-400

```
root@client-200:/# ip r
default via 20.0.0.1 dev eth0
10.0.31.0/30 via 192.168.100.9 dev tun0
20.0.0.0/24 dev eth0 proto kernel scope link src 20.0.0.100
40.0.0.0/24 via 192.168.100.9 dev tun0
192.168.100.0/24 via 192.168.100.9 dev tun0
192.168.100.9 dev tun0 proto kernel scope link src 192.168.100.10
root@client-200:/# ping 40.0.0.100
PING 40.0.0.100 (40.0.0.100): 56 data bytes
64 bytes from 40.0.0.100: icmp_seq=0 ttl=63 time=3.051 ms
64 bytes from 40.0.0.100: icmp_seq=1 ttl=63 time=2.445 ms
64 bytes from 40.0.0.100: icmp_seq=2 ttl=63 time=2.610 ms
64 bytes from 40.0.0.100: icmp_seq=3 ttl=63 time=2.683 ms
64 bytes from 40.0.0.100: icmp_seq=4 ttl=63 time=2.862 ms
64 bytes from 40.0.0.100: icmp_seq=5 ttl=63 time=3.617 ms
64 bytes from 40.0.0.100: icmp_seq=6 ttl=63 time=3.588 ms
64 bytes from 40.0.0.100: icmp_seq=7 ttl=63 time=2.602 ms
64 bytes from 40.0.0.100: icmp_seq=8 ttl=63 time=3.251 ms
64 bytes from 40.0.0.100: icmp_seq=9 ttl=63 time=2.745 ms
64 bytes from 40.0.0.100: icmp_seq=10 ttl=63 time=3.317 ms
64 bytes from 40.0.0.100: icmp_seq=11 ttl=63 time=3.126 ms
64 bytes from 40.0.0.100: icmp_seq=12 ttl=63 time=2.752 ms
```

Client-200 to Leaf-1

```
root@client-200:/# ping 10.0.31.2
PING 10.0.31.2 (10.0.31.2): 56 data bytes
64 bytes from 10.0.31.2: icmp_seq=0 ttl=63 time=3.878 ms
64 bytes from 10.0.31.2: icmp_seq=1 ttl=63 time=2.929 ms
64 bytes from 10.0.31.2: icmp_seq=2 ttl=63 time=3.115 ms
64 bytes from 10.0.31.2: icmp_seq=3 ttl=63 time=2.619 ms
64 bytes from 10.0.31.2: icmp_seq=4 ttl=63 time=3.372 ms
64 bytes from 10.0.31.2: icmp_seq=5 ttl=63 time=3.297 ms
64 bytes from 10.0.31.2: icmp_seq=6 ttl=63 time=5.488 ms
^C--- 10.0.31.2 ping statistics ---
7 packets transmitted, 7 packets received, 0% packet loss
round-trip min/avg/max/stddev = 2.619/3.528/5.488/0.878 ms
```

Capturing from - [R-302 eth1 to GW-300 eth0]

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
71	16.056471	a2:2b:e9:7b:2f:21	7a:b2:8d:e1:3c:0f	ARP	42	Who has 3.4.0.9? Tell 3.
72	16.056660	7a:b2:8d:e1:3c:0f	a2:2b:e9:7b:2f:21	ARP	42	3.4.0.9 is at 7a:b2:8d:e
73	17.028218	5.4.0.9	3.4.0.9	OpenVPN	150	MessageType: P_DATA_V2
74	17.028576	3.4.0.9	4.2.0.9	OpenVPN	150	MessageType: P_DATA_V2
75	17.029389	4.2.0.9	3.4.0.9	OpenVPN	150	MessageType: P_DATA_V2
76	17.029640	3.4.0.9	5.4.0.9	OpenVPN	150	MessageType: P_DATA_V2
77	18.030797	5.4.0.9	3.4.0.9	OpenVPN	150	MessageType: P_DATA_V2
78	18.031203	3.4.0.9	4.2.0.9	OpenVPN	150	MessageType: P_DATA_V2
79	18.032038	4.2.0.9	3.4.0.9	OpenVPN	150	MessageType: P_DATA_V2
80	18.032462	3.4.0.9	5.4.0.9	OpenVPN	150	MessageType: P_DATA_V2
81	19.032353	5.4.0.9	3.4.0.9	OpenVPN	150	MessageType: P_DATA_V2
82	19.032778	3.4.0.9	4.2.0.9	OpenVPN	150	MessageType: P_DATA_V2
83	19.033311	4.2.0.9	3.4.0.9	OpenVPN	150	MessageType: P_DATA_V2
84	19.033522	3.4.0.9	5.4.0.9	OpenVPN	150	MessageType: P_DATA_V2
85	20.034296	5.4.0.9	3.4.0.9	OpenVPN	150	MessageType: P_DATA_V2
86	20.034579	3.4.0.9	4.2.0.9	OpenVPN	150	MessageType: P_DATA_V2
87	20.035199	4.2.0.9	3.4.0.9	OpenVPN	150	MessageType: P_DATA_V2
88	20.035409	3.4.0.9	5.4.0.9	OpenVPN	150	MessageType: P_DATA_V2

```
Frame 1: 150 bytes on wire (1200 bits), 150 bytes captured (1200 bits) on interface -, id 0
Ethernet II, Src: a2:2b:e9:7b:2f:21 (a2:2b:e9:7b:2f:21), Dst: 7a:b2:8d:e1:3c:0f (7a:b2:8d:e1:3c:0f)
Internet Protocol Version 4, Src: 5.4.0.9, Dst: 3.4.0.9
User Datagram Protocol, Src Port: 1194, Dst Port: 1194
OpenVPN Protocol
```

Capturing from - [GW-300 eth1 to Leaf-1 swp6]

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
21	7.817029	fe80::a00:27ff:fee1...	ff02::1	ICMPv6	78	Router Advertisement
22	8.013923	192.168.100.10	10.0.31.2	ICMP	98	Echo (ping) request
23	8.014449	10.0.31.2	192.168.100.10	ICMP	98	Echo (ping) reply
24	9.014745	192.168.100.10	10.0.31.2	ICMP	98	Echo (ping) request
25	9.015281	10.0.31.2	192.168.100.10	ICMP	98	Echo (ping) reply
26	10.016502	192.168.100.10	10.0.31.2	ICMP	98	Echo (ping) request
27	10.016928	10.0.31.2	192.168.100.10	ICMP	98	Echo (ping) reply
28	11.017236	192.168.100.10	10.0.31.2	ICMP	98	Echo (ping) request
29	11.017611	10.0.31.2	192.168.100.10	ICMP	98	Echo (ping) reply
30	11.848148	10.0.31.2	224.0.0.5	OSPF	78	Hello Packet
31	12.018784	192.168.100.10	10.0.31.2	ICMP	98	Echo (ping) request
32	12.019234	10.0.31.2	192.168.100.10	ICMP	98	Echo (ping) reply
33	13.020199	192.168.100.10	10.0.31.2	ICMP	98	Echo (ping) request
34	13.020547	10.0.31.2	192.168.100.10	ICMP	98	Echo (ping) reply
35	14.021604	192.168.100.10	10.0.31.2	ICMP	98	Echo (ping) request
36	14.022097	10.0.31.2	192.168.100.10	ICMP	98	Echo (ping) reply
37	15.022569	192.168.100.10	10.0.31.2	ICMP	98	Echo (ping) request
38	15.023063	10.0.31.2	192.168.100.10	ICMP	98	Echo (ping) reply