Network and System Defence.

Final Project.

Pierpaolo Spaziani

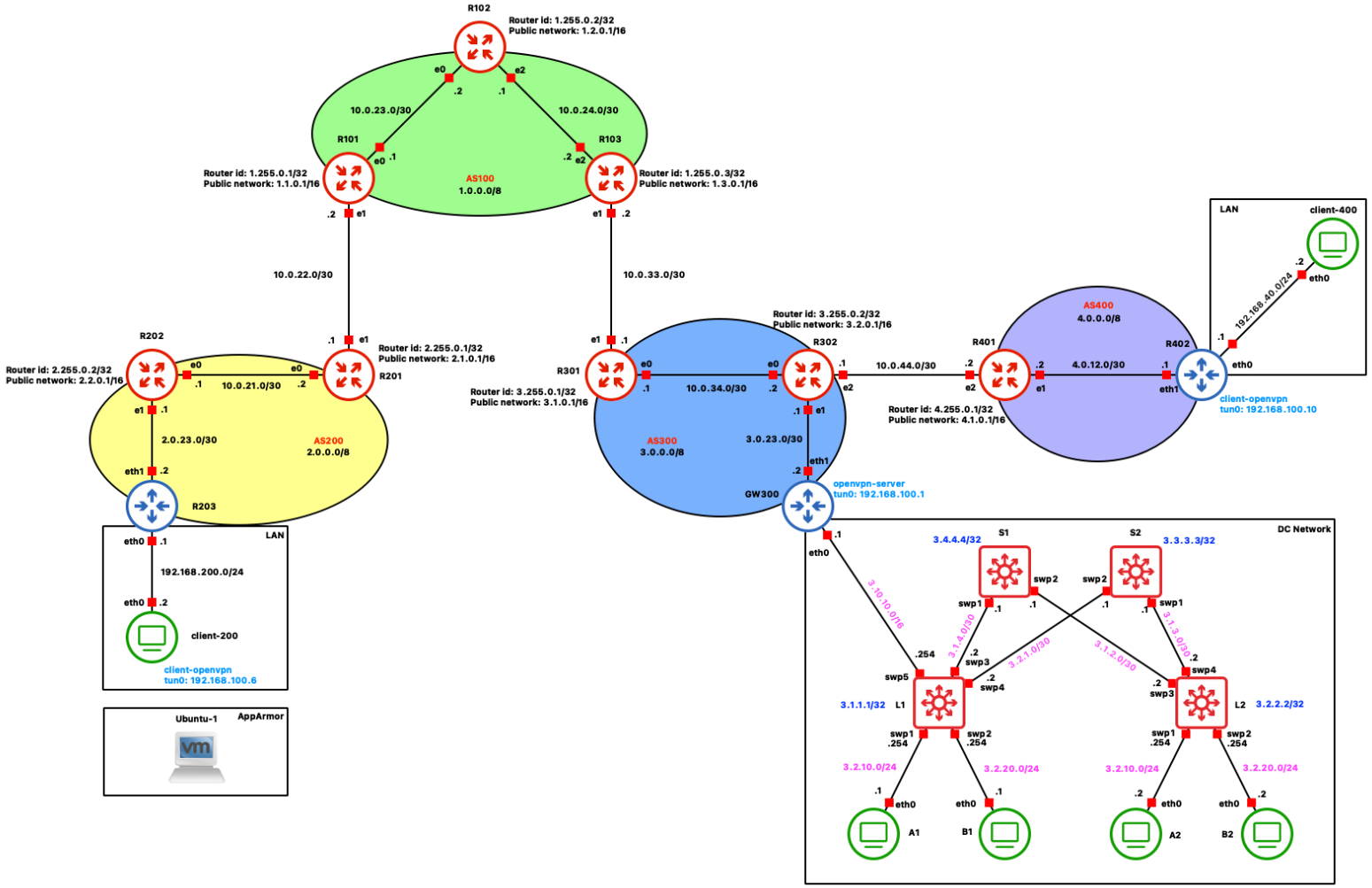
Matricola: 0316331

Università degli Studi di Roma Tor Vergata

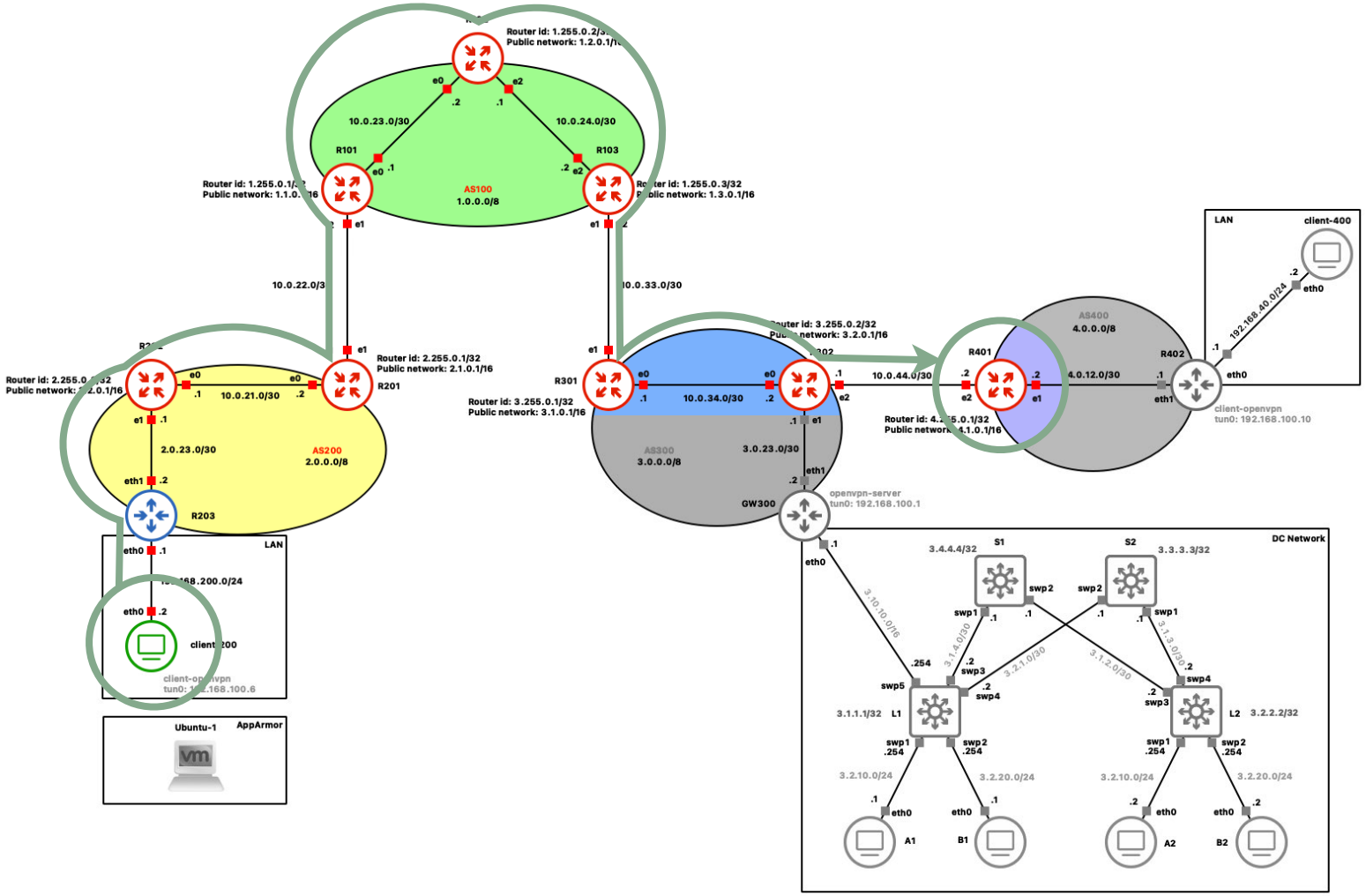
Indice.

- Comunicazione tra AS
- Protocolli:
  - BGP
  - OSPF
  - MPLS/LDP
- DC Network
- Firewall
- OpenVPN
- MAC → AppArmor

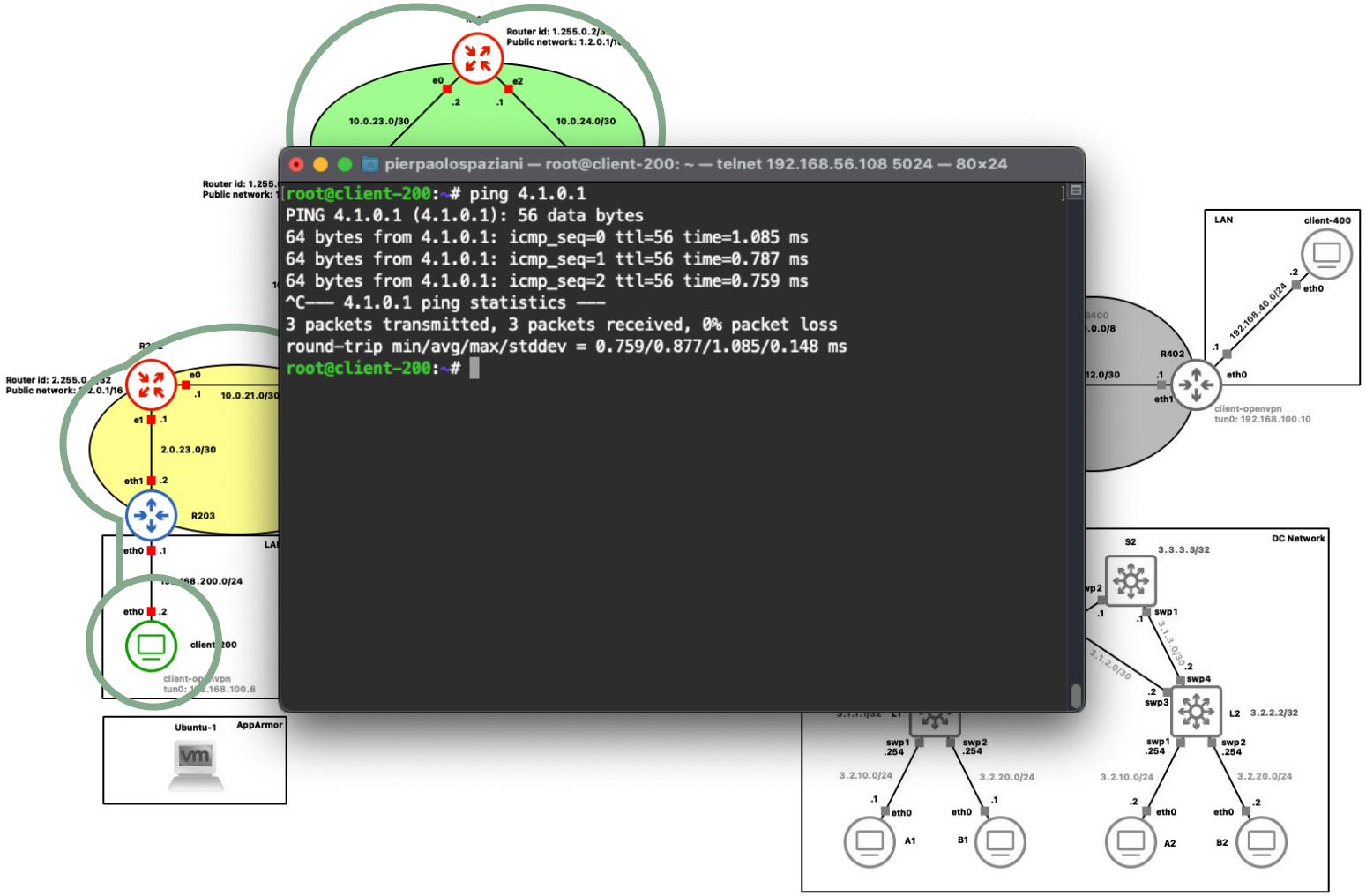
Topologia.


R102
Router id: 1.255.0.2/32
Public network: 1.2.0.1/16
e0
e2
.2
.1
10.0.23.0/30
10.0.24.0/30
R101
R103
e0 .1
.2 e2
Router id: 1.255.0.1/32
Public network: 1.1.0.1/16
AS100
1.0.0.0/8
Router id: 1.255.0.3/32
Public network: 1.3.0.1/16
.2 e1
e1 .2
10.0.22.0/30
10.0.33.0/30
R202
.1 e1
Router id: 2.255.0.1/32
Public network: 2.1.0.1/16
Router id: 2.255.0.2/32
Public network: 2.2.0.1/16
e0
e0
.1
10.0.21.0/30
.2
R201
e1 .1
2.0.23.0/30
AS200
2.0.0.0/8
eth1 .2
R203
eth0 .1
LAN
192.168.200.0/24
eth0 .2
client-200
client-openvpn
tun0: 192.168.100.6
Ubuntu-1
AppArmor
vm
Router id: 3.255.0.2/32
Public network: 3.2.0.1/16
e1 .1
R301
e0
e0
.1
10.0.34.0/30
.2
R302
.1
e2
10.0.44.0/30
Router id: 3.255.0.1/32
Public network: 3.1.0.1/16
AS300
3.0.0.0/8
.1 e1
3.0.23.0/30
eth1
.2
GW300
openvpn-server
tun0: 192.168.100.1
R401
.2
e2
.2
e1
4.0.12.0/30
.1
eth1
R402
AS400
4.0.0.0/8
Router id: 4.255.0.1/32
Public network: 4.1.0.1/16
LAN
client-400
.1
192.168.40.0/24
.2
eth0
eth0
client-openvpn
tun0: 192.168.100.10
eth0 .1
DC Network
3.4.4.4/32
S1
swp2
swp1 .1
.1
S2
3.3.3.3/32
swp2
.1
swp1
.1
3.10.10.0/16
3.1.4.0/30
3.1.3.0/30
.254
swp3
.2
swp4
.2
3.2.1.0/30
3.1.2.0/30
swp5
.2
swp3
swp4
.2
3.1.1.1/32
L1
L2
3.2.2.2/32
swp1
.254
swp2
.254
swp1
.254
swp2
.254
3.2.10.0/24
3.2.20.0/24
3.2.10.0/24
3.2.20.0/24
.1
eth0
eth0
.1
.2
eth0
eth0
.2
A1
B1
A2
B2

Comunicazione tra AS.



Comunicazione tra AS.



Protocolli.

BGP - Border Gateway Protocol.

BGP è un protocollo di routing *distance vector* ed il più comune tra gli *EGP*.

È fondamentale per il funzionamento di Internet in quanto permette ai diversi AS di comunicare tra loro e determinare i **percorsi migliori** per il traffico dati.

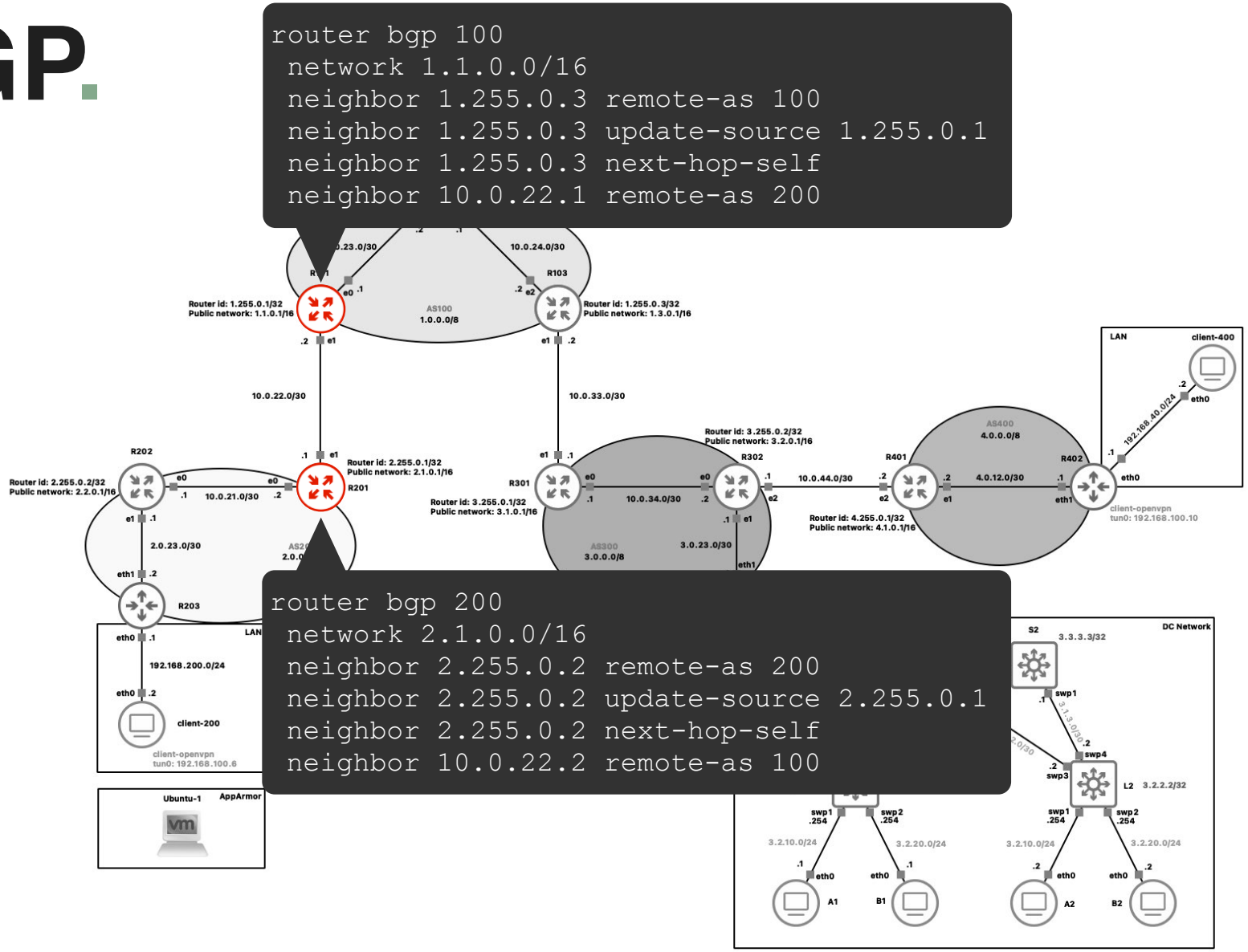
Si basa sulle informazioni passate dai ***downstream neighbors***, ovvero i vicini dai quali un router accetta le informazioni BGP.

Quando un router riceve una nuova informazione, decide se aggiornare la propria *routing table* o meno e se inoltrare queste informazioni ai suoi vicini (***upstream neighbors***).

BGP utilizza una **lista di AS** attraverso i quali un pacchetto deve passare per giungere a destinazione come metrica di distanza da **minimizzare**.

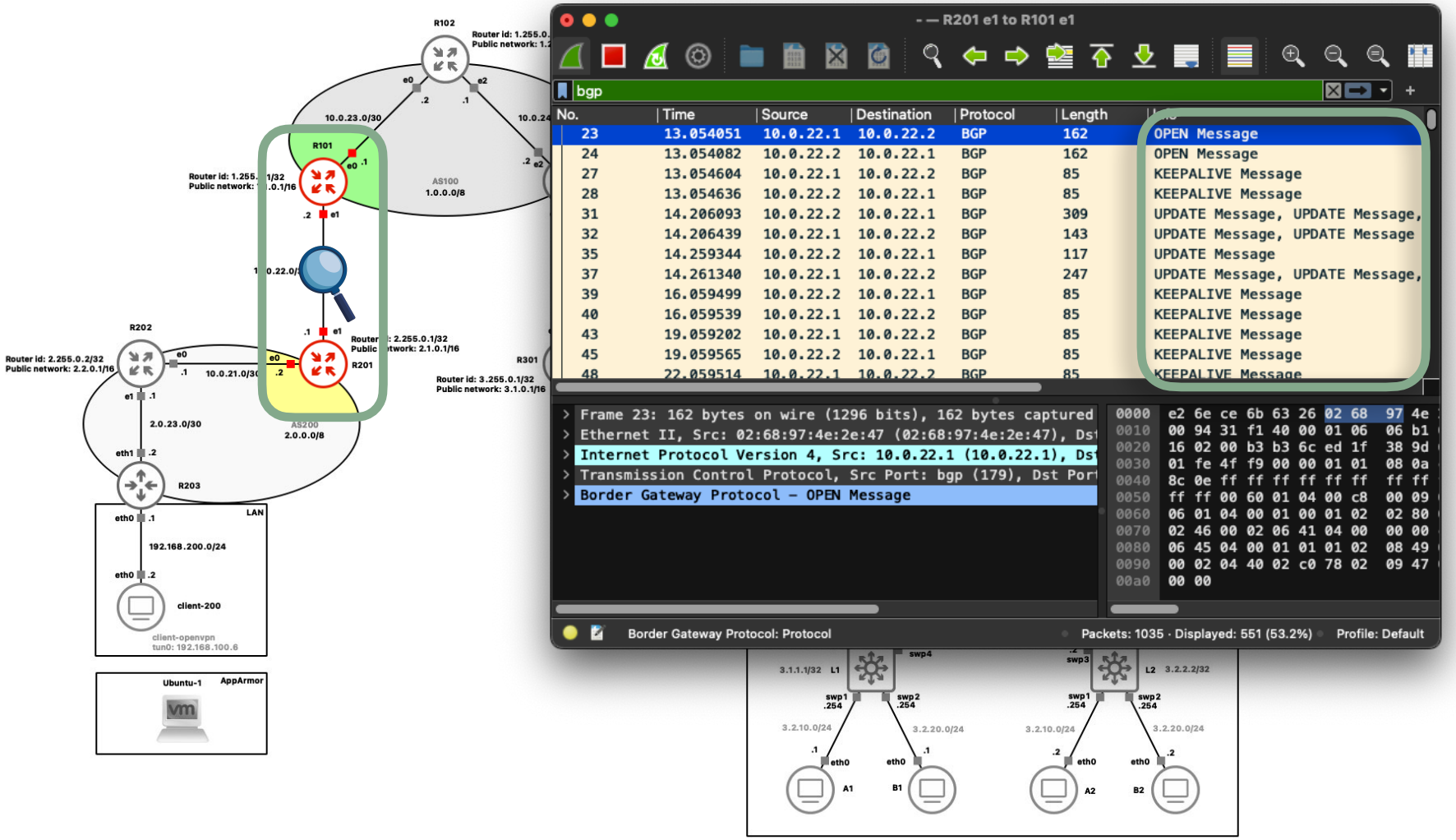
BGP.

```
router bgp 100
 network 1.1.0.0/16
 neighbor 1.255.0.3 remote-as 100
 neighbor 1.255.0.3 update-source 1.255.0.1
 neighbor 1.255.0.3 next-hop-self
 neighbor 10.0.22.1 remote-as 200
```

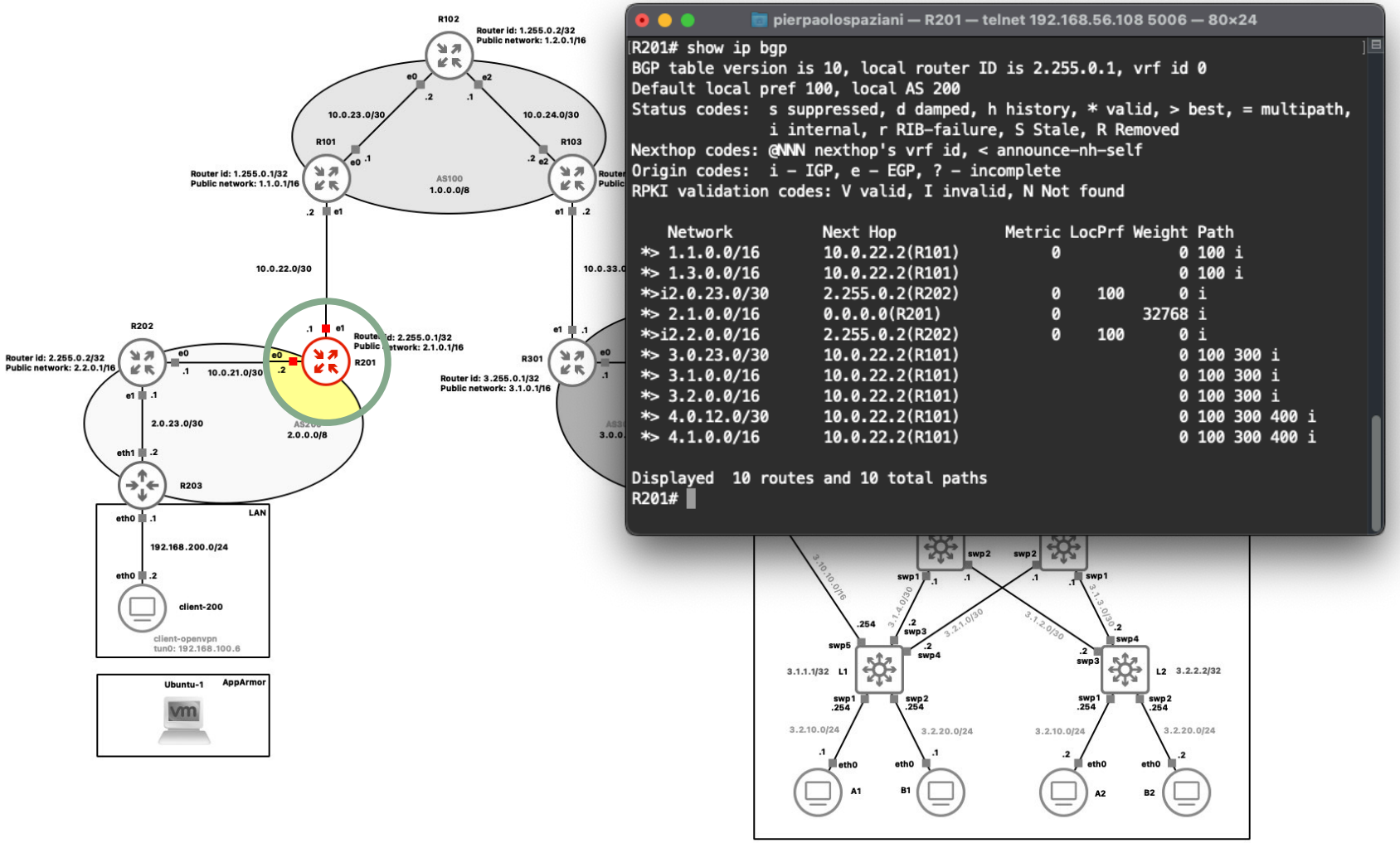



```
router bgp 200
 network 2.1.0.0/16
 neighbor 2.255.0.2 remote-as 200
 neighbor 2.255.0.2 update-source 2.255.0.1
 neighbor 2.255.0.2 next-hop-self
 neighbor 10.0.22.2 remote-as 100
```

BGP.


R102
R101
R202
R201
R203
R301
AS100
1.0.0.0/8
AS200
2.0.0.0/8
10.0.23.0/30
2.0.23.0/30
192.168.200.0/24
LAN
client-200
client-openvpn
tun0: 192.168.100.6
Ubuntu-1
AppArmor
- — R201 e1 to R101 e1
bgp
No. | Time | Source | Destination | Protocol | Length
23 13.054051 10.0.22.1 10.0.22.2 BGP 162 OPEN Message
24 13.054082 10.0.22.2 10.0.22.1 BGP 162 OPEN Message
27 13.054604 10.0.22.1 10.0.22.2 BGP 85 KEEPALIVE Message
28 13.054636 10.0.22.2 10.0.22.1 BGP 85 KEEPALIVE Message
31 14.206093 10.0.22.2 10.0.22.1 BGP 309 UPDATE Message, UPDATE Message,
32 14.206439 10.0.22.1 10.0.22.2 BGP 143 UPDATE Message, UPDATE Message
35 14.259344 10.0.22.2 10.0.22.1 BGP 117 UPDATE Message
37 14.261340 10.0.22.1 10.0.22.2 BGP 247 UPDATE Message, UPDATE Message,
39 16.059499 10.0.22.2 10.0.22.1 BGP 85 KEEPALIVE Message
40 16.059539 10.0.22.1 10.0.22.2 BGP 85 KEEPALIVE Message
43 19.059202 10.0.22.1 10.0.22.2 BGP 85 KEEPALIVE Message
45 19.059565 10.0.22.2 10.0.22.1 BGP 85 KEEPALIVE Message
48 22.059514 10.0.22.1 10.0.22.2 BGP 85 KEEPALIVE Message
Frame 23: 162 bytes on wire (1296 bits), 162 bytes captured
Ethernet II, Src: 02:68:97:4e:2e:47 (02:68:97:4e:2e:47), Dst
Internet Protocol Version 4, Src: 10.0.22.1 (10.0.22.1), Dst
Transmission Control Protocol, Src Port: bgp (179), Dst Port
Border Gateway Protocol – OPEN Message
0000 e2 6e ce 6b 63 26 02 68 97 4e
0010 00 94 31 f1 40 00 01 06 06 b1
0020 16 02 00 b3 b3 6c ed 1f 38 9d
0030 01 fe 4f f9 00 00 01 01 08 0a
0040 8c 0e ff ff ff ff ff ff ff ff
0050 ff ff 00 60 01 04 00 c8 00 09
0060 06 01 04 00 01 00 01 02 02 80
0070 02 46 00 02 06 41 04 00 00 00
0080 06 45 04 00 01 01 01 02 08 49
0090 00 02 04 40 02 c0 78 02 09 47
00a0 00 00
Border Gateway Protocol: Protocol
Packets: 1035 · Displayed: 551 (53.2%)
Profile: Default
3.1.1.1/32
L1
swp4
swp1
swp2
3.2.10.0/24
3.2.20.0/24
eth0
A1
B1
L2
3.2.2.2/32
swp3
A2
B2

BGP.



pierpaolospaziani — R201 — telnet 192.168.56.108 5006 — 80×24

```
R201# show ip bgp
BGP table version is 10, local router ID is 2.255.0.1, vrf id 0
Default local pref 100, local AS 200
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
*> 1.1.0.0/16       10.0.22.2(R101)          0             0 100 i
*> 1.3.0.0/16       10.0.22.2(R101)                        0 100 i
*>i2.0.23.0/30      2.255.0.2(R202)          0    100      0 i
*> 2.1.0.0/16       0.0.0.0(R201)            0         32768 i
*>i2.2.0.0/16       2.255.0.2(R202)          0    100      0 i
*> 3.0.23.0/30      10.0.22.2(R101)                        0 100 300 i
*> 3.1.0.0/16       10.0.22.2(R101)                        0 100 300 i
*> 3.2.0.0/16       10.0.22.2(R101)                        0 100 300 i
*> 4.0.12.0/30      10.0.22.2(R101)                        0 100 300 400 i
*> 4.1.0.0/16       10.0.22.2(R101)                        0 100 300 400 i

Displayed  10 routes and 10 total paths
R201#
```

Protocolli.

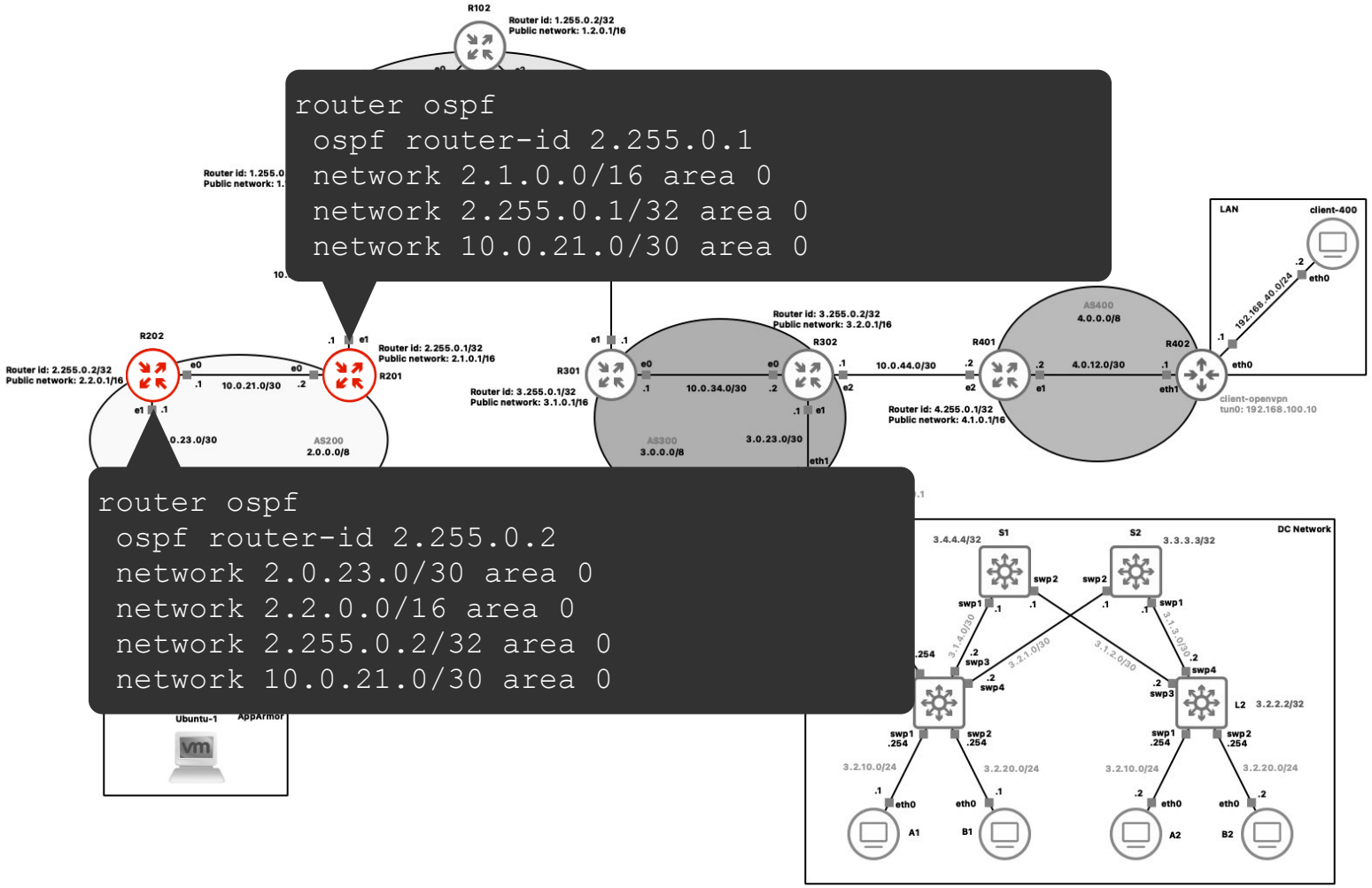
OSPF - Open Shortest Path First.

OSPF è un protocollo ***IGP*** (*Interior gateway protocols*) utilizzato per instradare i pacchetti IP all'interno di un singolo sistema autonomo (AS).

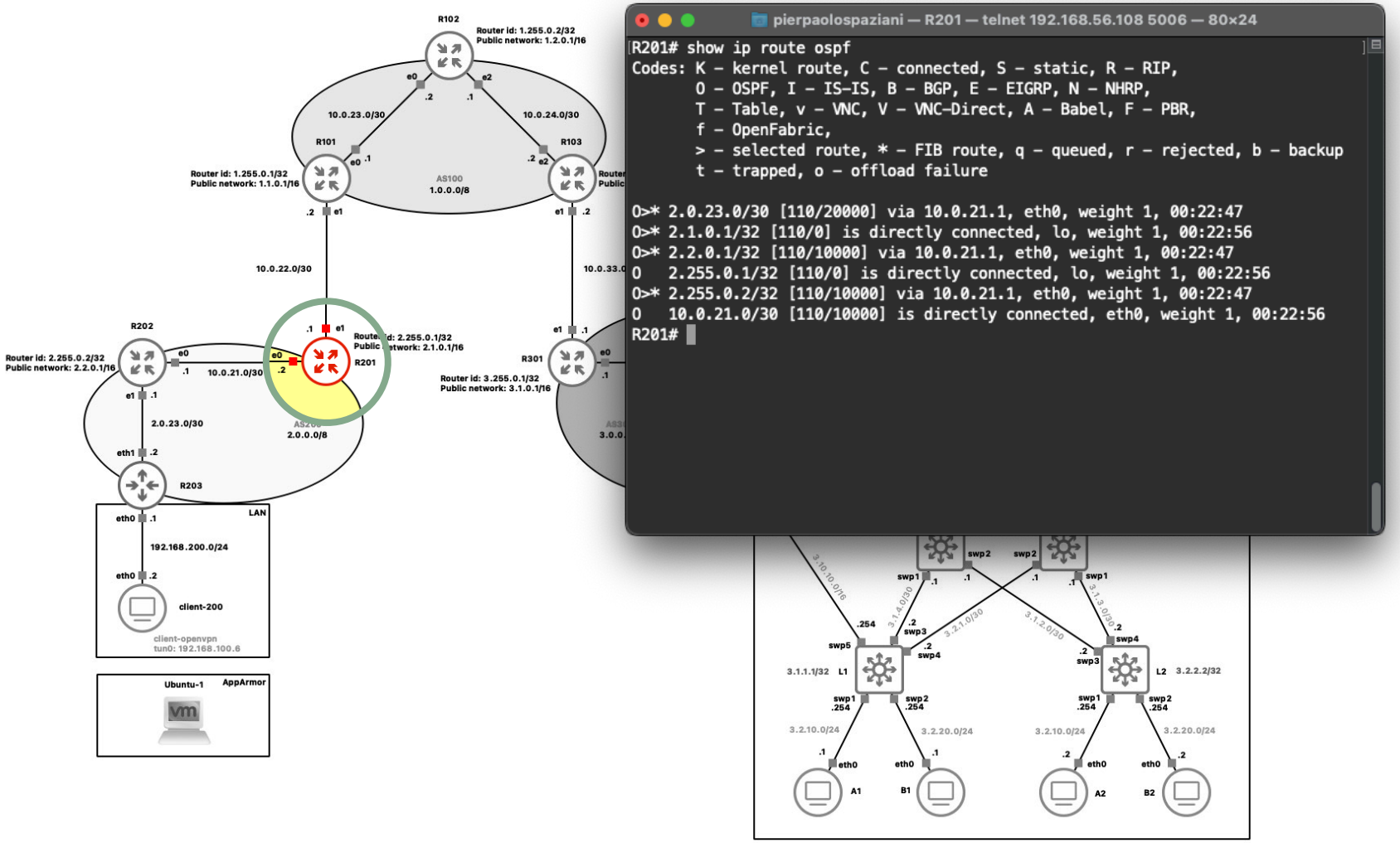
Utilizza l'algoritmo **SPF** (*Shortest Path First*) di Dijkstra per calcolare il percorso più breve tra i router.

OSPF è un protocollo di routing ***Link State*** che aggiorna le informazioni di routing dinamicamente e supporta il bilanciamento del carico e l'autenticazione dei messaggi. È altamente scalabile e supporta reti di grandi dimensioni suddivise in aree per migliorare l'efficienza e ridurre il traffico di aggiornamento.

OSPF.


router ospf
ospf router-id 2.255.0.1
network 2.1.0.0/16 area 0
network 2.255.0.1/32 area 0
network 10.0.21.0/30 area 0
router ospf
ospf router-id 2.255.0.2
network 2.0.23.0/30 area 0
network 2.2.0.0/16 area 0
network 2.255.0.2/32 area 0
network 10.0.21.0/30 area 0
R102
Router id: 1.255.0.2/32
Public network: 1.2.0.1/16
R202
Router id: 2.255.0.2/32
Public network: 2.2.0.1/16
R201
Router id: 2.255.0.1/32
Public network: 2.1.0.1/16
10.0.21.0/30
AS200
2.0.0.0/8
R301
Router id: 3.255.0.1/32
Public network: 3.1.0.1/16
10.0.34.0/30
R302
Router id: 3.255.0.2/32
Public network: 3.2.0.1/16
AS300
3.0.0.0/8
3.0.23.0/30
R401
Router id: 4.255.0.1/32
Public network: 4.1.0.1/16
10.0.44.0/30
AS400
4.0.0.0/8
4.0.12.0/30
R402
LAN
client-400
192.168.40.0/24
client-openvpn
tun0: 192.168.100.10
Ubuntu-1
AppArmor
DC Network
S1
3.4.4.4/32
S2
3.3.3.3/32
L2
3.2.2.2/32
3.1.4.0/30
3.2.1.0/30
3.1.2.0/30
3.1.3.0/30
3.2.10.0/24
3.2.20.0/24
A1
B1
A2
B2

OSPF.


R102
Router id: 1.255.0.2/32
Public network: 1.2.0.1/16
10.0.23.0/30
10.0.24.0/30
R101
R103
Router id: 1.255.0.1/32
Public network: 1.1.0.1/16
AS100
1.0.0.0/8
10.0.22.0/30
R202
Router id: 2.255.0.2/32
Public network: 2.2.0.1/16
10.0.21.0/30
R201
2.0.23.0/30
2.0.0.0/8
R203
LAN
192.168.200.0/24
client-200
client-openvpn
tun0: 192.168.100.6
Ubuntu-1
AppArmor
R301
Router id: 3.255.0.1/32
Public network: 3.1.0.1/16
pierpaolospaziani — R201 — telnet 192.168.56.108 5006 — 80×24
R201# show ip route ospf
Codes: K - kernel route, C - connected, S - static, R - RIP,
O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
T - Table, v - VNC, V - VNC-Direct, A - Babel, F - PBR,
f - OpenFabric,
> - selected route, * - FIB route, q - queued, r - rejected, b - backup
t - trapped, o - offload failure
O>* 2.0.23.0/30 [110/20000] via 10.0.21.1, eth0, weight 1, 00:22:47
O>* 2.1.0.1/32 [110/0] is directly connected, lo, weight 1, 00:22:56
O>* 2.2.0.1/32 [110/10000] via 10.0.21.1, eth0, weight 1, 00:22:47
O 2.255.0.1/32 [110/0] is directly connected, lo, weight 1, 00:22:56
O>* 2.255.0.2/32 [110/10000] via 10.0.21.1, eth0, weight 1, 00:22:47
O 10.0.21.0/30 [110/10000] is directly connected, eth0, weight 1, 00:22:56
R201#
swp1
swp2
swp3
swp4
swp5
3.1.1.1/32 L1
L2 3.2.2.2/32
3.2.10.0/24
3.2.20.0/24
A1
B1
A2
B2

Protocolli.

MPLS - Multi-Protocol Label Switching.

MPLS è una tecnologia di instradamento utilizzata per migliorare la velocità e l'efficienza del traffico dati su reti IP, soprattutto su reti di grandi dimensioni.

MPLS instrada i pacchetti di dati basandosi su etichette (**LABELS**) piuttosto che sugli indirizzi IP di destinazione, consentendo una gestione più flessibile e efficiente del traffico.

LDP - Label Distribution Protocol.

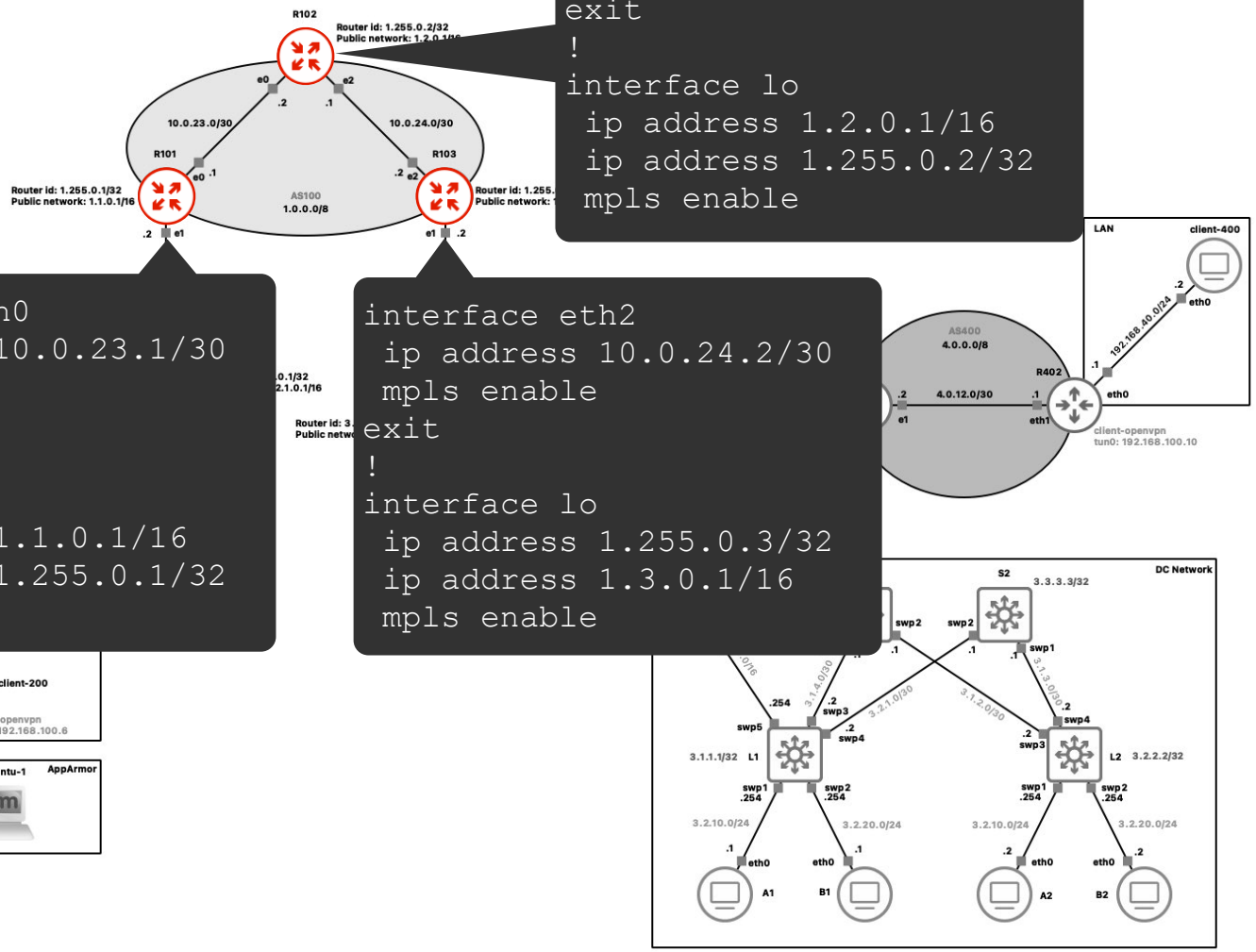
LDP è un protocollo utilizzato nelle reti MPLS per la distribuzione delle etichette tra router e permette ai router MPLS di stabilire, mantenere e terminare le LSP (*Label Switched Paths*) attraverso lo scambio di informazioni di etichettatura.

MPLS/LDP.

```
interface eth0
 ip address 10.0.23.2/30
 mpls enable
exit
!
interface eth2
 ip address 10.0.24.1/30
 mpls enable
exit
!
interface lo
 ip address 1.2.0.1/16
 ip address 1.255.0.2/32
 mpls enable
```

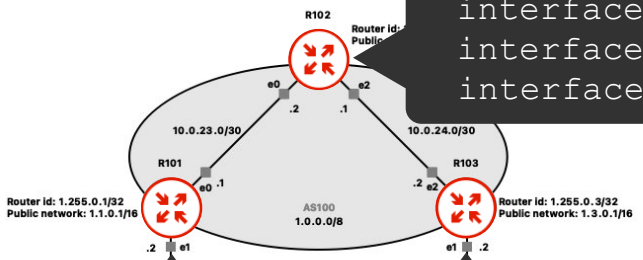
```
interface eth0
 ip address 10.0.23.1/30
 mpls enable
exit
!
interface lo
 ip address 1.1.0.1/16
 ip address 1.255.0.1/32
 mpls enable
```

```
interface eth2
 ip address 10.0.24.2/30
 mpls enable
exit
!
interface lo
 ip address 1.255.0.3/32
 ip address 1.3.0.1/16
 mpls enable
```



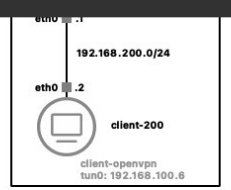
MPLS/LDP.

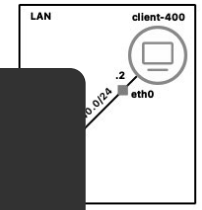
```
mpls ldp
 router-id 1.255.0.2
 ordered-control
 address-family ipv4
  discovery transport-address 1.255.0.2
  interface eth0
  interface eth2
  interface lo
```

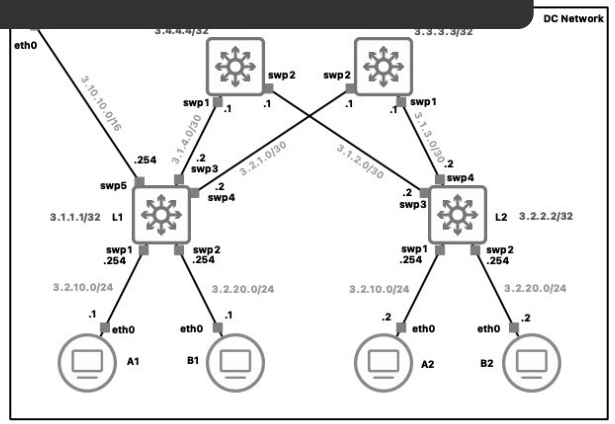



```
mpls ldp
 router-id 1.255.0.1
 ordered-control
 address-family ipv4
  discovery transport-address 1.255.0.1
  interface eth0
  interface lo
```

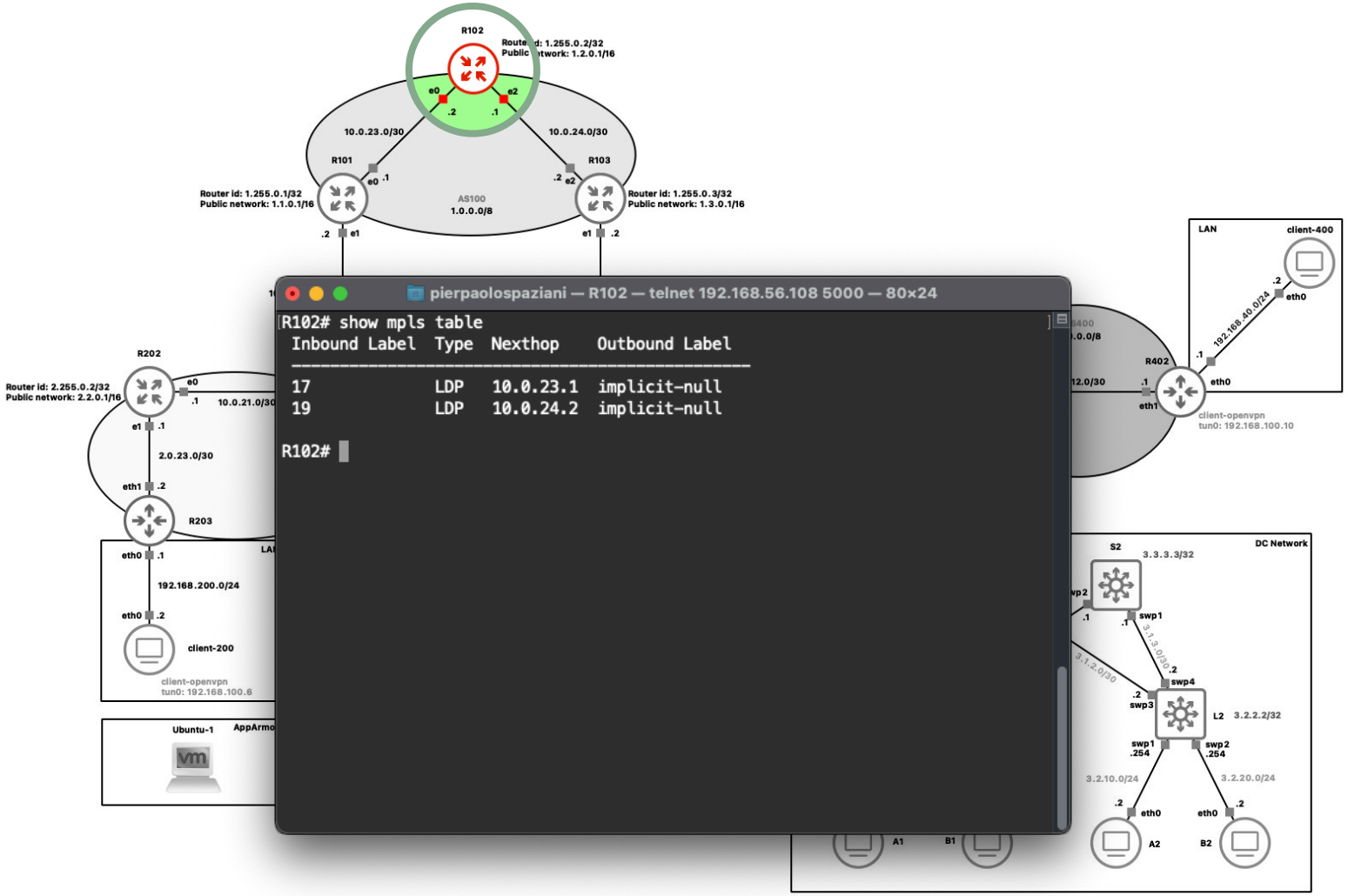
```
mpls ldp
 router-id 1.255.0.3
 ordered-control
 address-family ipv4
  discovery transport-address 1.255.0.3
  interface eth2
  interface lo
```



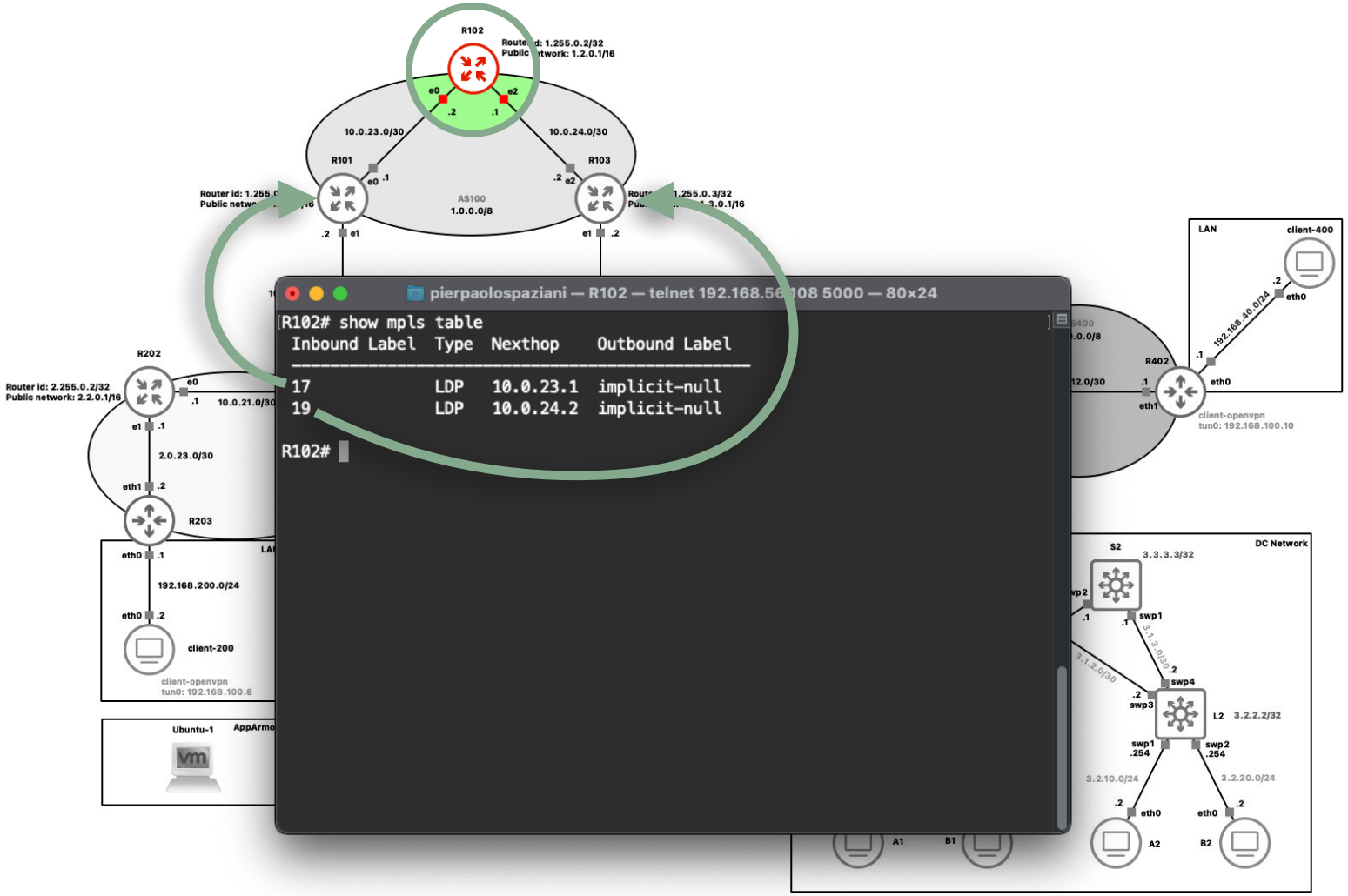




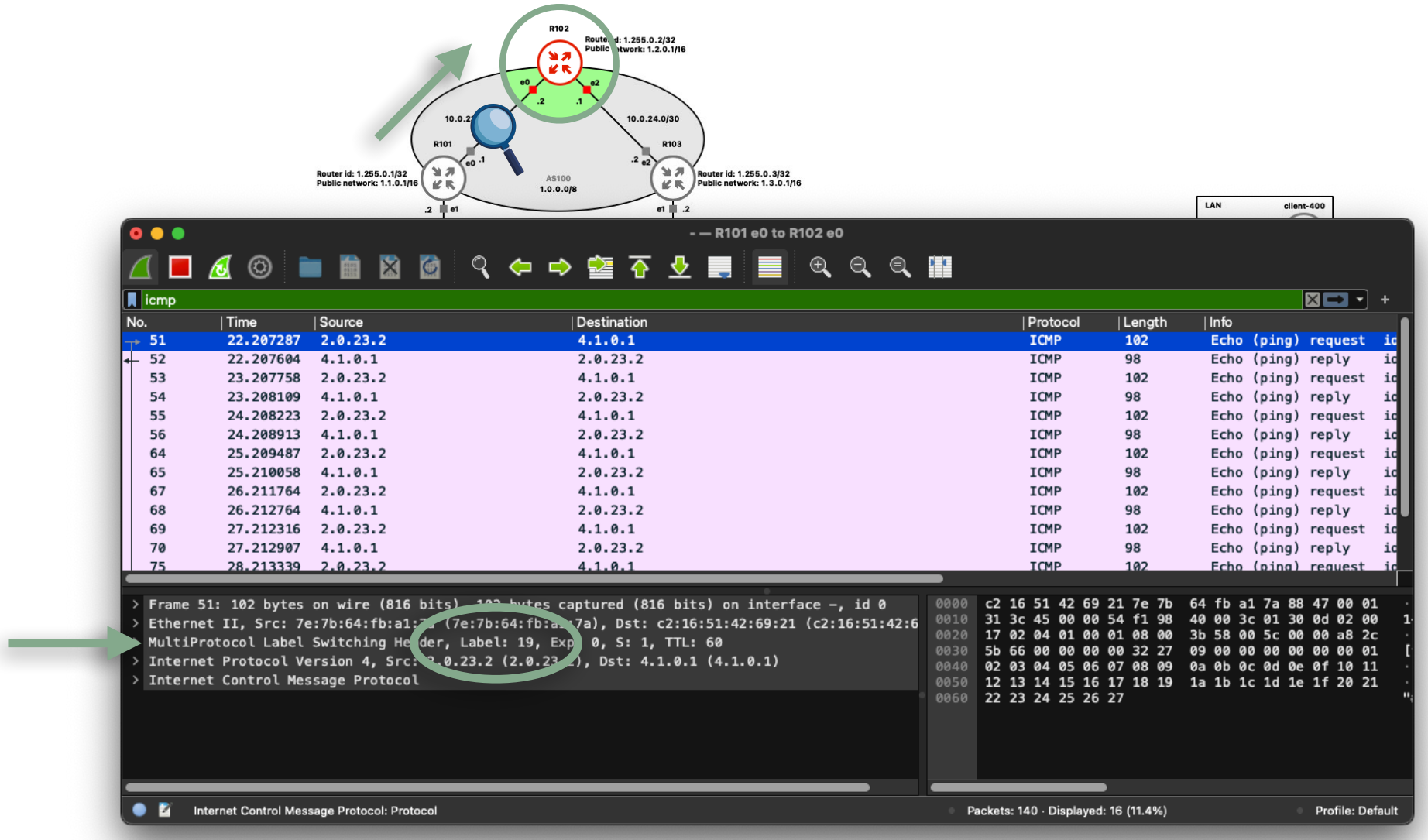
MPLS/LDP.


R102
Router id: 1.255.0.2/32
Public network: 1.2.0.1/16
e0
e2
.2
.1
10.0.23.0/30
10.0.24.0/30
R101
R103
e0 .1
.2 e2
Router id: 1.255.0.1/32
Public network: 1.1.0.1/16
AS100
1.0.0.0/8
Router id: 1.255.0.3/32
Public network: 1.3.0.1/16
.2 e1
e1 .2
pierpaolospaziani — R102 — telnet 192.168.56.108 5000 — 80×24
R102# show mpls table
Inbound Label Type Nexthop Outbound Label
17 LDP 10.0.23.1 implicit-null
19 LDP 10.0.24.2 implicit-null
R102#
R202
Router id: 2.255.0.2/32
Public network: 2.2.0.1/16
e0
.1
10.0.21.0/30
e1 .1
2.0.23.0/30
eth1 .2
R203
eth0 .1
192.168.200.0/24
eth0 .2
client-200
client-openvpn
tun0: 192.168.100.6
Ubuntu-1
AppArmo
vm
LAN
client-400
.2
192.168.40.0/24
eth0
.1
R402
eth0
.1
eth1
client-openvpn
tun0: 192.168.100.10
12.0/30
DC Network
S2
3.3.3.3/32
swp2
.1
swp1
.1
.2
swp4
.2
swp3
L2
3.2.2.2/32
swp1
.254
swp2
.254
3.2.10.0/24
3.2.20.0/24
.2
eth0
eth0
.2
A1
B1
A2
B2

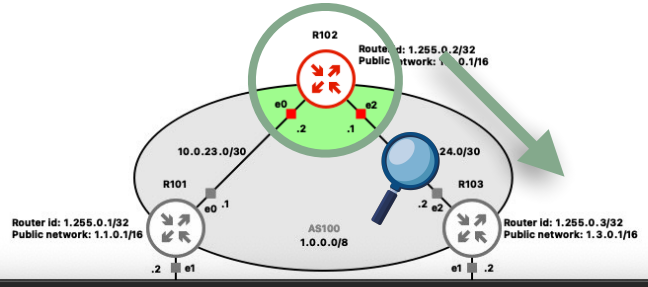
MPLS/LDP.

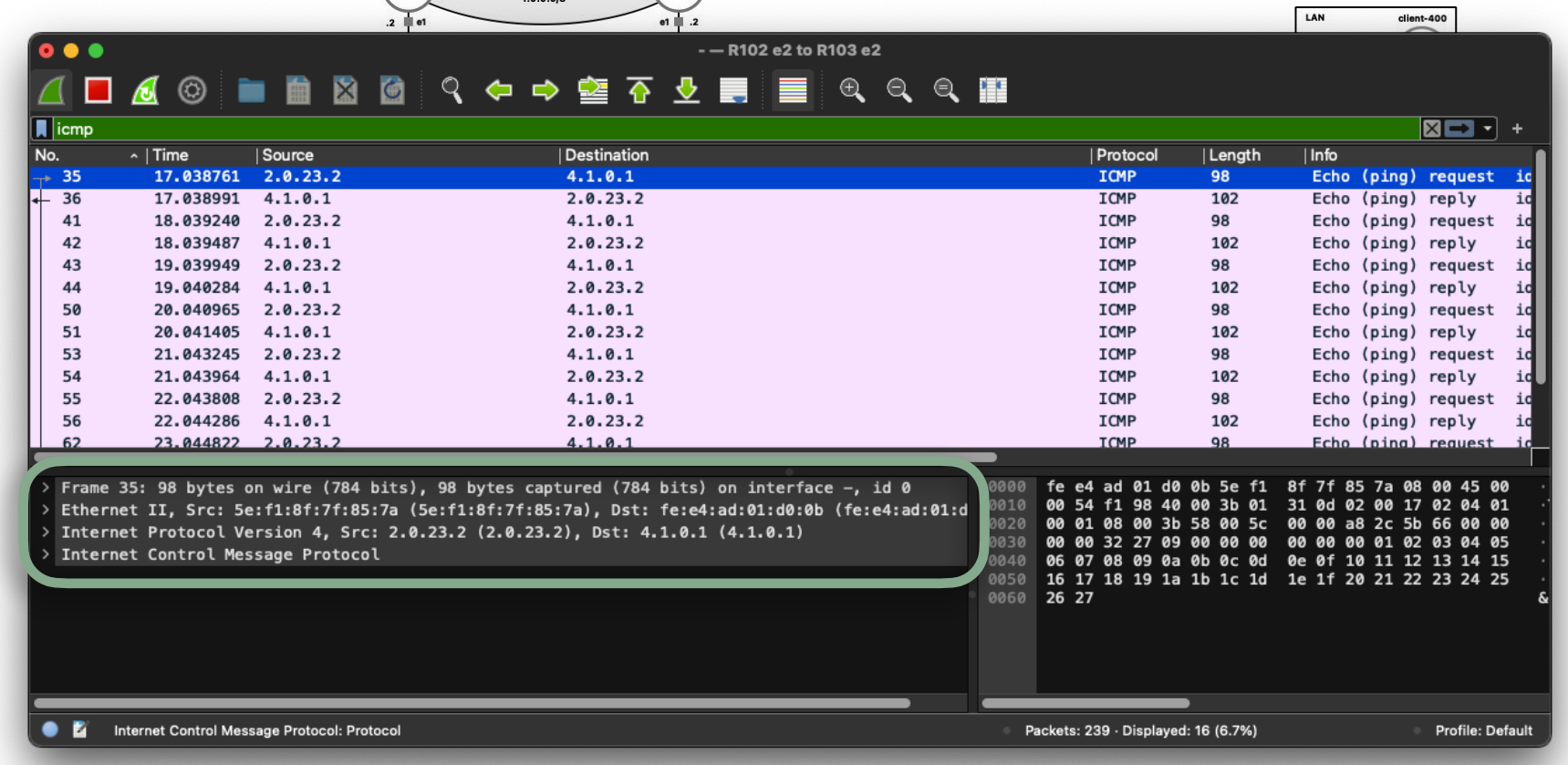

R102
10.0.23.0/30
10.0.24.0/30
R101
R103
AS100
1.0.0.0/8
pierpaolospaziani — R102 — telnet 192.168.56.108 5000 — 80×24
R102# show mpls table
Inbound Label Type Nexthop Outbound Label
17 LDP 10.0.23.1 implicit-null
19 LDP 10.0.24.2 implicit-null
R102#
R202
R203
2.0.23.0/30
192.168.200.0/24
client-200
R402
LAN
client-400
192.168.40.0/24
client-openvpn
tun0: 192.168.100.10
DC Network
S2
3.3.3.3/32
L2
3.2.2.2/32
3.2.10.0/24
3.2.20.0/24
A1
B1
A2
B2

MPLS/LDP.

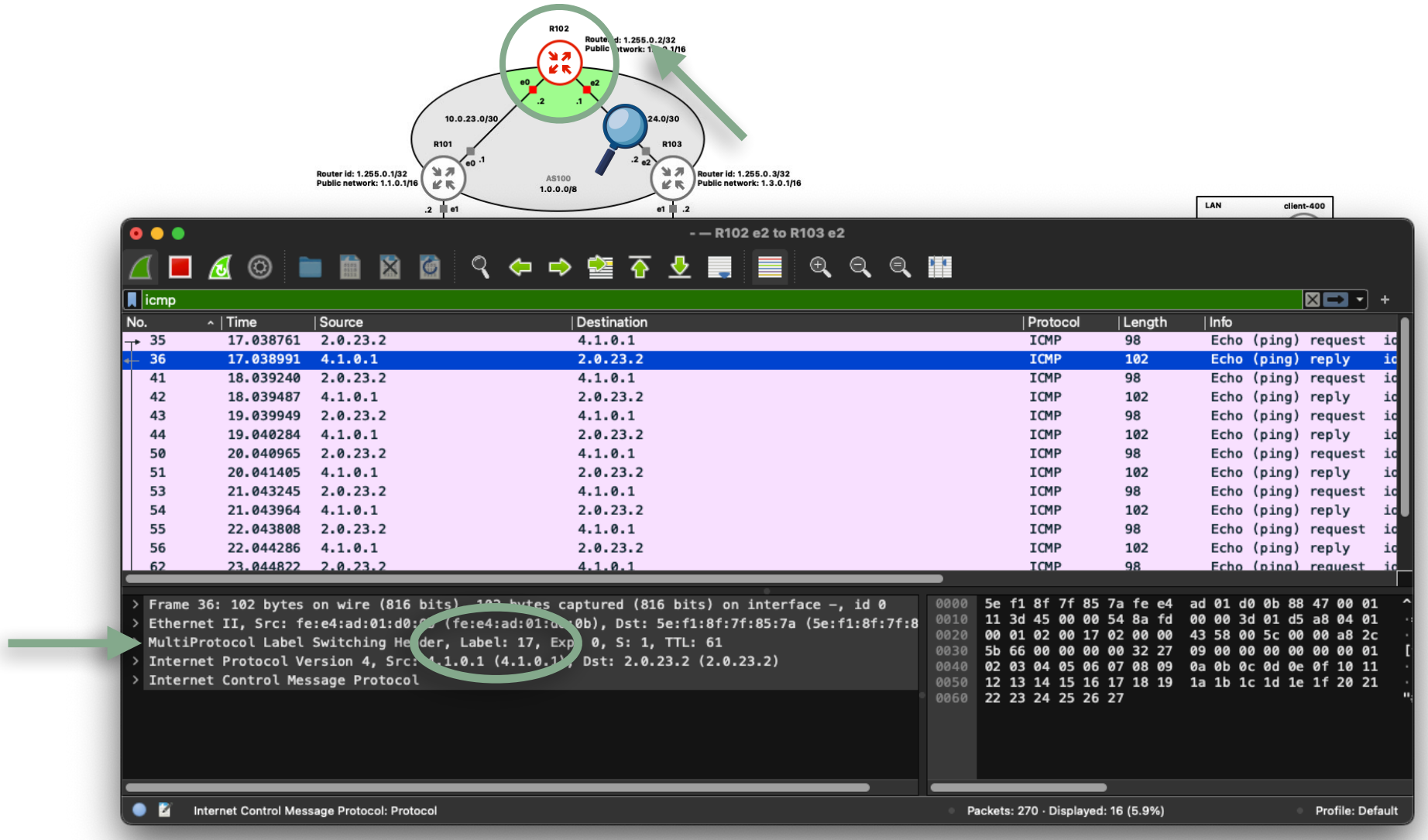

R102
Router id: 1.255.0.2/32
Public network: 1.2.0.1/16
e0
e2
.2
.1
10.0.24.0/30
R101
R103
e0 .1
.2 e2
AS100
1.0.0.0/8
Router id: 1.255.0.1/32
Public network: 1.1.0.1/16
Router id: 1.255.0.3/32
Public network: 1.3.0.1/16
.2 e1
e1 .2
LAN
client-400
- — R101 e0 to R102 e0
icmp
No. Time Source Destination Protocol Length Info
51 22.207287 2.0.23.2 4.1.0.1 ICMP 102 Echo (ping) request
52 22.207604 4.1.0.1 2.0.23.2 ICMP 98 Echo (ping) reply
53 23.207758 2.0.23.2 4.1.0.1 ICMP 102 Echo (ping) request
54 23.208109 4.1.0.1 2.0.23.2 ICMP 98 Echo (ping) reply
55 24.208223 2.0.23.2 4.1.0.1 ICMP 102 Echo (ping) request
56 24.208913 4.1.0.1 2.0.23.2 ICMP 98 Echo (ping) reply
64 25.209487 2.0.23.2 4.1.0.1 ICMP 102 Echo (ping) request
65 25.210058 4.1.0.1 2.0.23.2 ICMP 98 Echo (ping) reply
67 26.211764 2.0.23.2 4.1.0.1 ICMP 102 Echo (ping) request
68 26.212764 4.1.0.1 2.0.23.2 ICMP 98 Echo (ping) reply
69 27.212316 2.0.23.2 4.1.0.1 ICMP 102 Echo (ping) request
70 27.212907 4.1.0.1 2.0.23.2 ICMP 98 Echo (ping) reply
Frame 51: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface -, id 0
Ethernet II, Src: 7e:7b:64:fb:a1:7a (7e:7b:64:fb:a1:7a), Dst: c2:16:51:42:69:21 (c2:16:51:42:6
MultiProtocol Label Switching Header, Label: 19, Exp: 0, S: 1, TTL: 60
Internet Protocol Version 4, Src: 2.0.23.2 (2.0.23.2), Dst: 4.1.0.1 (4.1.0.1)
Internet Control Message Protocol
0000 c2 16 51 42 69 21 7e 7b 64 fb a1 7a 88 47 00 01
0010 31 3c 45 00 00 54 f1 98 40 00 3c 01 30 0d 02 00
0020 17 02 04 01 00 01 08 00 3b 58 00 5c 00 00 a8 2c
0030 5b 66 00 00 00 00 32 27 09 00 00 00 00 00 00 01
0040 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f 10 11
0050 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21
0060 22 23 24 25 26 27
Internet Control Message Protocol: Protocol
Packets: 140 · Displayed: 16 (11.4%)
Profile: Default

MPLS/LDP.

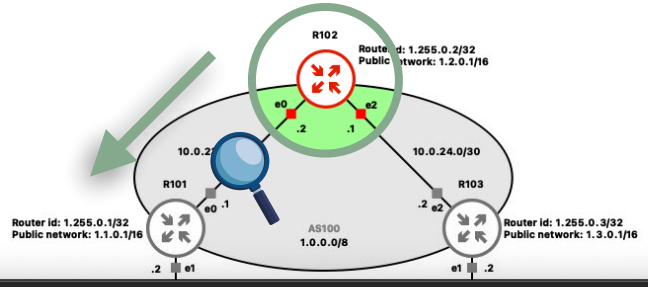

R102
e0
e2
.2
.1
10.0.23.0/30
24.0/30
R101
R103
e0 .1
.2 e2
AS100
1.0.0.0/8
Router id: 1.255.0.1/32
Public network: 1.1.0.1/16
Router id: 1.255.0.3/32
Public network: 1.3.0.1/16
.2 e1
e1 .2

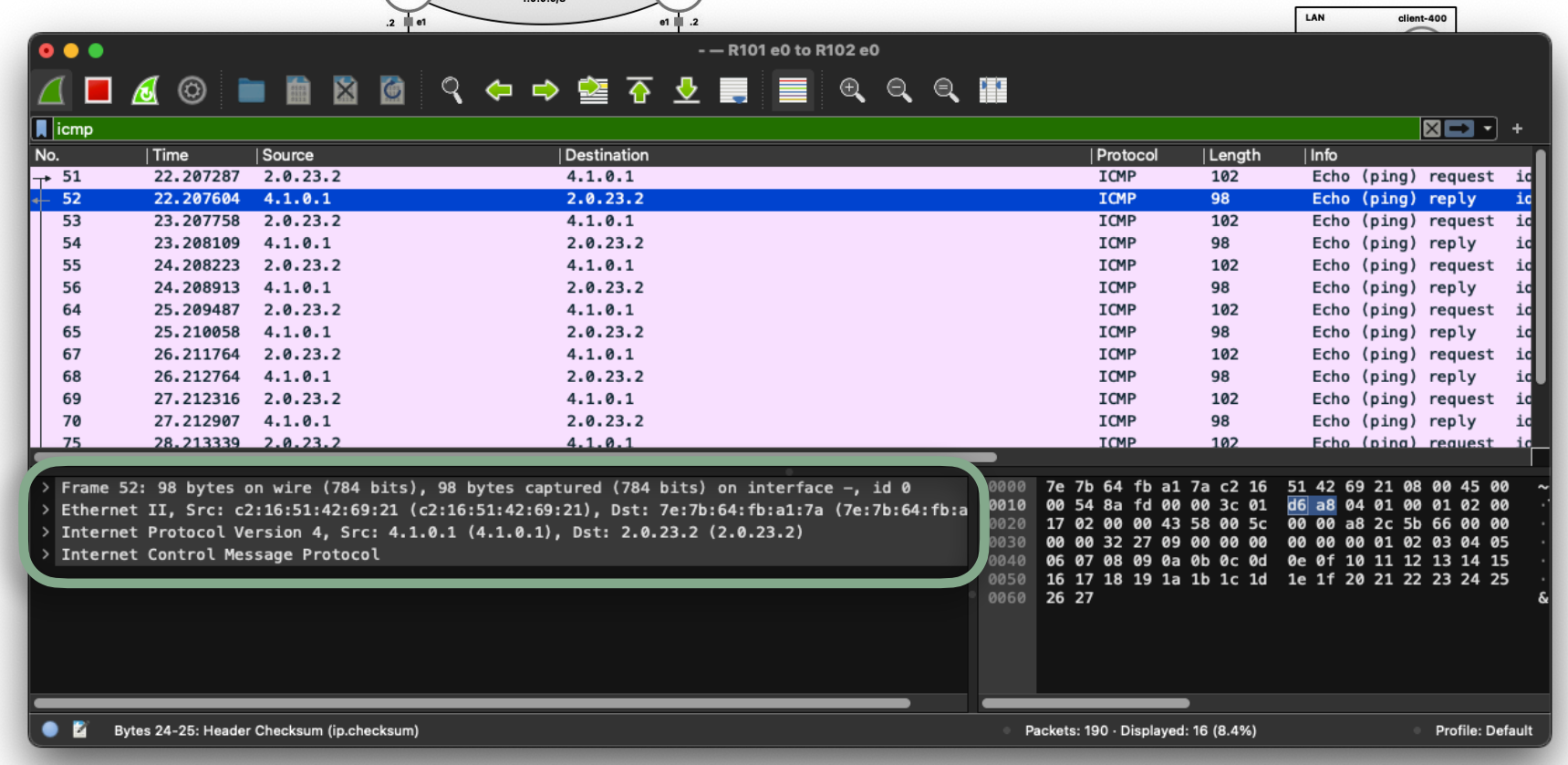

LAN
client-400
- — R102 e2 to R103 e2
icmp
No. | Time | Source | Destination | Protocol | Length | Info
35 17.038761 2.0.23.2 4.1.0.1 ICMP 98 Echo (ping) request
36 17.038991 4.1.0.1 2.0.23.2 ICMP 102 Echo (ping) reply
41 18.039240 2.0.23.2 4.1.0.1 ICMP 98 Echo (ping) request
42 18.039487 4.1.0.1 2.0.23.2 ICMP 102 Echo (ping) reply
43 19.039949 2.0.23.2 4.1.0.1 ICMP 98 Echo (ping) request
44 19.040284 4.1.0.1 2.0.23.2 ICMP 102 Echo (ping) reply
50 20.040965 2.0.23.2 4.1.0.1 ICMP 98 Echo (ping) request
51 20.041405 4.1.0.1 2.0.23.2 ICMP 102 Echo (ping) reply
53 21.043245 2.0.23.2 4.1.0.1 ICMP 98 Echo (ping) request
54 21.043964 4.1.0.1 2.0.23.2 ICMP 102 Echo (ping) reply
55 22.043808 2.0.23.2 4.1.0.1 ICMP 98 Echo (ping) request
56 22.044286 4.1.0.1 2.0.23.2 ICMP 102 Echo (ping) reply
Frame 35: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface -, id 0
Ethernet II, Src: 5e:f1:8f:7f:85:7a (5e:f1:8f:7f:85:7a), Dst: fe:e4:ad:01:d0:0b (fe:e4:ad:01:d
Internet Protocol Version 4, Src: 2.0.23.2 (2.0.23.2), Dst: 4.1.0.1 (4.1.0.1)
Internet Control Message Protocol
0000 fe e4 ad 01 d0 0b 5e f1 8f 7f 85 7a 08 00 45 00
0010 00 54 f1 98 40 00 3b 01 31 0d 02 00 17 02 04 01
0020 00 01 08 00 3b 58 00 5c 00 00 a8 2c 5b 66 00 00
0030 00 00 32 27 09 00 00 00 00 00 00 01 02 03 04 05
0040 06 07 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15
0050 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25
0060 26 27
Internet Control Message Protocol: Protocol
Packets: 239 · Displayed: 16 (6.7%)
Profile: Default

MPLS/LDP.

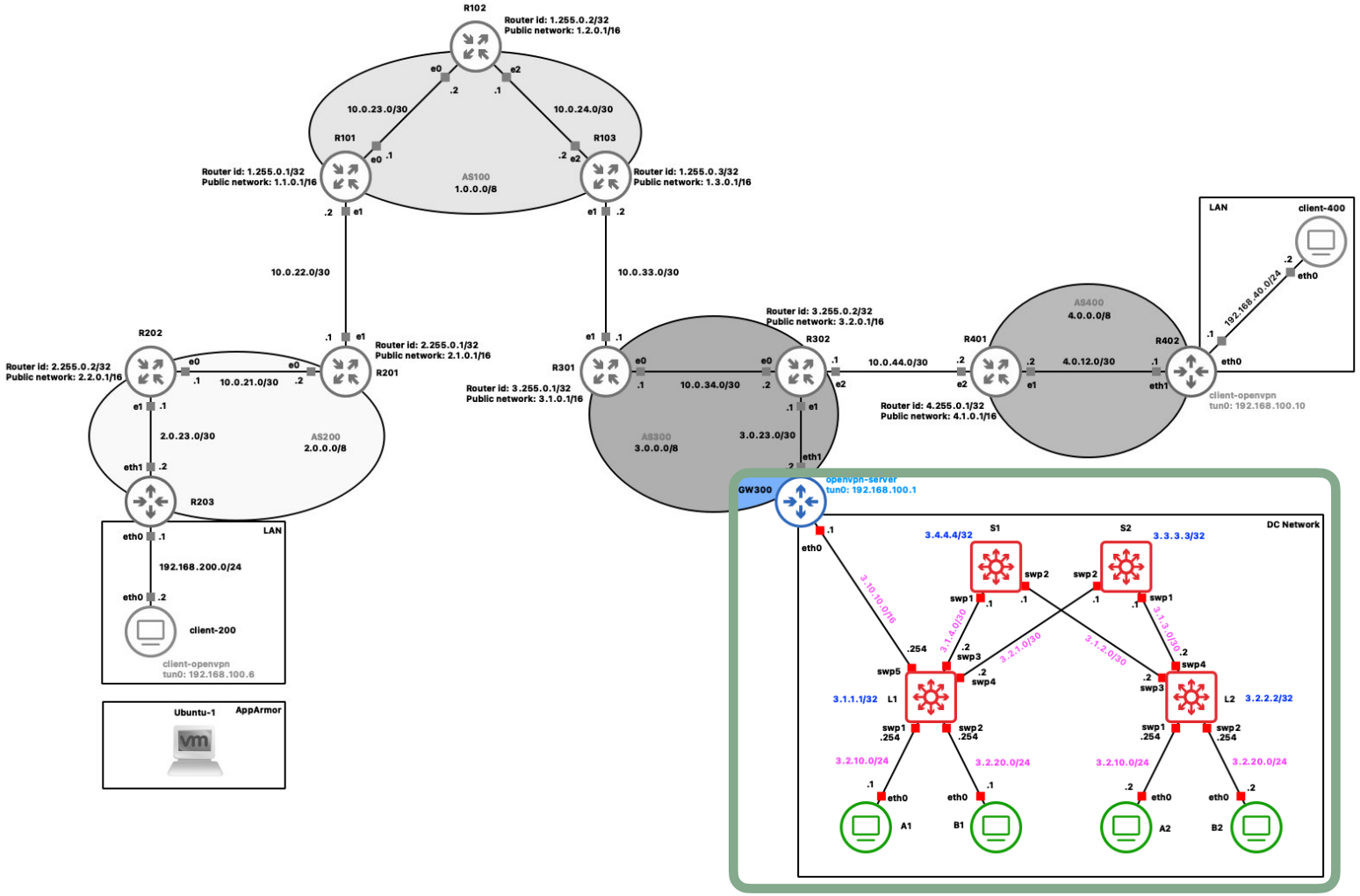

R102
e0
e2
.2
.1
10.0.23.0/30
24.0/30
R101
R103
e0 .1
.2 e2
AS100
1.0.0.0/8
Router id: 1.255.0.1/32
Public network: 1.1.0.1/16
Router id: 1.255.0.3/32
Public network: 1.3.0.1/16
.2 e1
e1 .2
LAN
client-400
- — R102 e2 to R103 e2
icmp
No. Time Source Destination Protocol Length Info
35 17.038761 2.0.23.2 4.1.0.1 ICMP 98 Echo (ping) request
36 17.038991 4.1.0.1 2.0.23.2 ICMP 102 Echo (ping) reply
41 18.039240 2.0.23.2 4.1.0.1 ICMP 98 Echo (ping) request
42 18.039487 4.1.0.1 2.0.23.2 ICMP 102 Echo (ping) reply
43 19.039949 2.0.23.2 4.1.0.1 ICMP 98 Echo (ping) request
44 19.040284 4.1.0.1 2.0.23.2 ICMP 102 Echo (ping) reply
50 20.040965 2.0.23.2 4.1.0.1 ICMP 98 Echo (ping) request
51 20.041405 4.1.0.1 2.0.23.2 ICMP 102 Echo (ping) reply
53 21.043245 2.0.23.2 4.1.0.1 ICMP 98 Echo (ping) request
54 21.043964 4.1.0.1 2.0.23.2 ICMP 102 Echo (ping) reply
55 22.043808 2.0.23.2 4.1.0.1 ICMP 98 Echo (ping) request
56 22.044286 4.1.0.1 2.0.23.2 ICMP 102 Echo (ping) reply
Frame 36: 102 bytes on wire (816 bits)
Ethernet II, Src: fe:e4:ad:01:d0:0b, Dst: 5e:f1:8f:7f:85:7a
MultiProtocol Label Switching Header, Label: 17, Exp 0, S: 1, TTL: 61
Internet Protocol Version 4, Src: 4.1.0.1 (4.1.0.1), Dst: 2.0.23.2 (2.0.23.2)
Internet Control Message Protocol
0000 5e f1 8f 7f 85 7a fe e4 ad 01 d0 0b 88 47 00 01
0010 11 3d 45 00 00 54 8a fd 00 00 3d 01 d5 a8 04 01
0020 00 01 02 00 17 02 00 00 43 58 00 5c 00 00 a8 2c
0030 5b 66 00 00 00 00 32 27 09 00 00 00 00 00 00 01
0040 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f 10 11
0050 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21
0060 22 23 24 25 26 27
Internet Control Message Protocol: Protocol
Packets: 270 · Displayed: 16 (5.9%)
Profile: Default

MPLS/LDP.

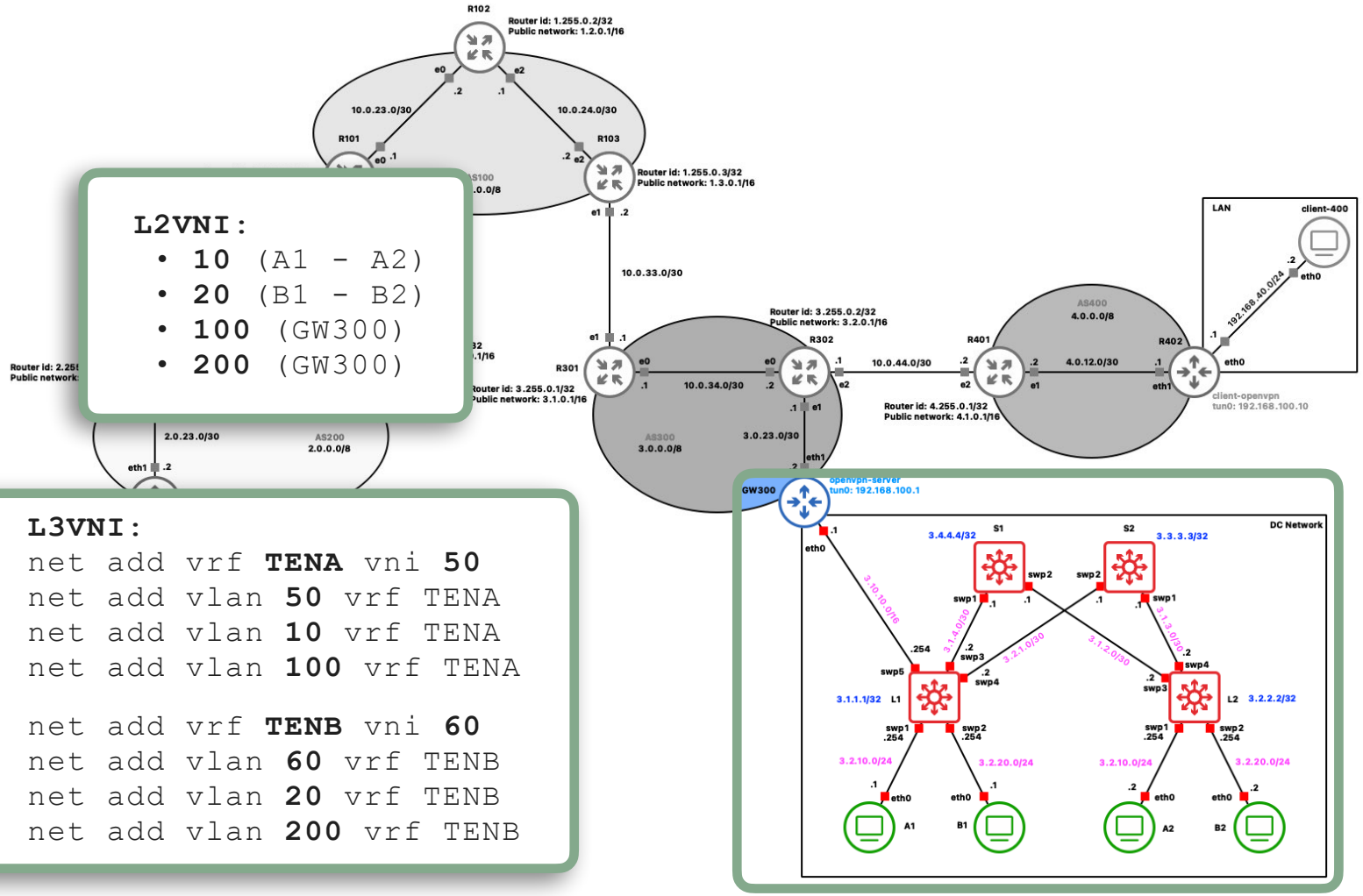

R102
Router id: 1.255.0.2/32
Public network: 1.2.0.1/16
e0
e2
.2
.1
10.0.2
10.0.24.0/30
R101
R103
e0 .1
.2 e2
AS100
1.0.0.0/8
Router id: 1.255.0.1/32
Public network: 1.1.0.1/16
Router id: 1.255.0.3/32
Public network: 1.3.0.1/16
.2 e1
e1 .2


LAN
client-400
- — R101 e0 to R102 e0
icmp
No. Time Source Destination Protocol Length Info
51 22.207287 2.0.23.2 4.1.0.1 ICMP 102 Echo (ping) request
52 22.207604 4.1.0.1 2.0.23.2 ICMP 98 Echo (ping) reply
53 23.207758 2.0.23.2 4.1.0.1 ICMP 102 Echo (ping) request
54 23.208109 4.1.0.1 2.0.23.2 ICMP 98 Echo (ping) reply
55 24.208223 2.0.23.2 4.1.0.1 ICMP 102 Echo (ping) request
56 24.208913 4.1.0.1 2.0.23.2 ICMP 98 Echo (ping) reply
64 25.209487 2.0.23.2 4.1.0.1 ICMP 102 Echo (ping) request
65 25.210058 4.1.0.1 2.0.23.2 ICMP 98 Echo (ping) reply
67 26.211764 2.0.23.2 4.1.0.1 ICMP 102 Echo (ping) request
68 26.212764 4.1.0.1 2.0.23.2 ICMP 98 Echo (ping) reply
69 27.212316 2.0.23.2 4.1.0.1 ICMP 102 Echo (ping) request
70 27.212907 4.1.0.1 2.0.23.2 ICMP 98 Echo (ping) reply
Frame 52: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface -, id 0
Ethernet II, Src: c2:16:51:42:69:21 (c2:16:51:42:69:21), Dst: 7e:7b:64:fb:a1:7a (7e:7b:64:fb:a
Internet Protocol Version 4, Src: 4.1.0.1 (4.1.0.1), Dst: 2.0.23.2 (2.0.23.2)
Internet Control Message Protocol
0000 7e 7b 64 fb a1 7a c2 16 51 42 69 21 08 00 45 00
0010 00 54 8a fd 00 00 3c 01 d6 a8 04 01 00 01 02 00
0020 17 02 00 00 43 58 00 5c 00 00 a8 2c 5b 66 00 00
0030 00 00 32 27 09 00 00 00 00 00 00 01 02 03 04 05
0040 06 07 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15
0050 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25
0060 26 27
Bytes 24-25: Header Checksum (ip.checksum)
Packets: 190 · Displayed: 16 (8.4%)
Profile: Default

DC Network.


R102
Router id: 1.255.0.2/32
Public network: 1.2.0.1/16
10.0.23.0/30
10.0.24.0/30
R101
R103
Router id: 1.255.0.1/32
Public network: 1.1.0.1/16
AS100
1.0.0.0/8
Router id: 1.255.0.3/32
Public network: 1.3.0.1/16
10.0.22.0/30
10.0.33.0/30
R202
Router id: 2.255.0.2/32
Public network: 2.2.0.1/16
10.0.21.0/30
R201
Router id: 2.255.0.1/32
Public network: 2.1.0.1/16
2.0.23.0/30
AS200
2.0.0.0/8
R203
LAN
192.168.200.0/24
client-200
client-openvpn
tun0: 192.168.100.6
Ubuntu-1
AppArmor
Router id: 3.255.0.2/32
Public network: 3.2.0.1/16
R301
R302
Router id: 3.255.0.1/32
Public network: 3.1.0.1/16
10.0.34.0/30
AS300
3.0.0.0/8
3.0.23.0/30
10.0.44.0/30
R401
R402
AS400
4.0.0.0/8
4.0.12.0/30
Router id: 4.255.0.1/32
Public network: 4.1.0.1/16
LAN
client-400
192.168.40.0/24
client-openvpn
tun0: 192.168.100.10
GW300
openvpn-server
tun0: 192.168.100.1
DC Network
S1
S2
3.4.4.4/32
3.3.3.3/32
3.10.10.0/16
3.1.4.0/30
3.1.3.0/30
3.1.2.0/30
3.1.1.1/32
L1
L2
3.2.2.2/32
3.2.10.0/24
3.2.20.0/24
A1
B1
A2
B2

DC Network.



L2VNI:

- **10** (A1 - A2)
- **20** (B1 - B2)
- **100** (GW300)
- **200** (GW300)

L3VNI:

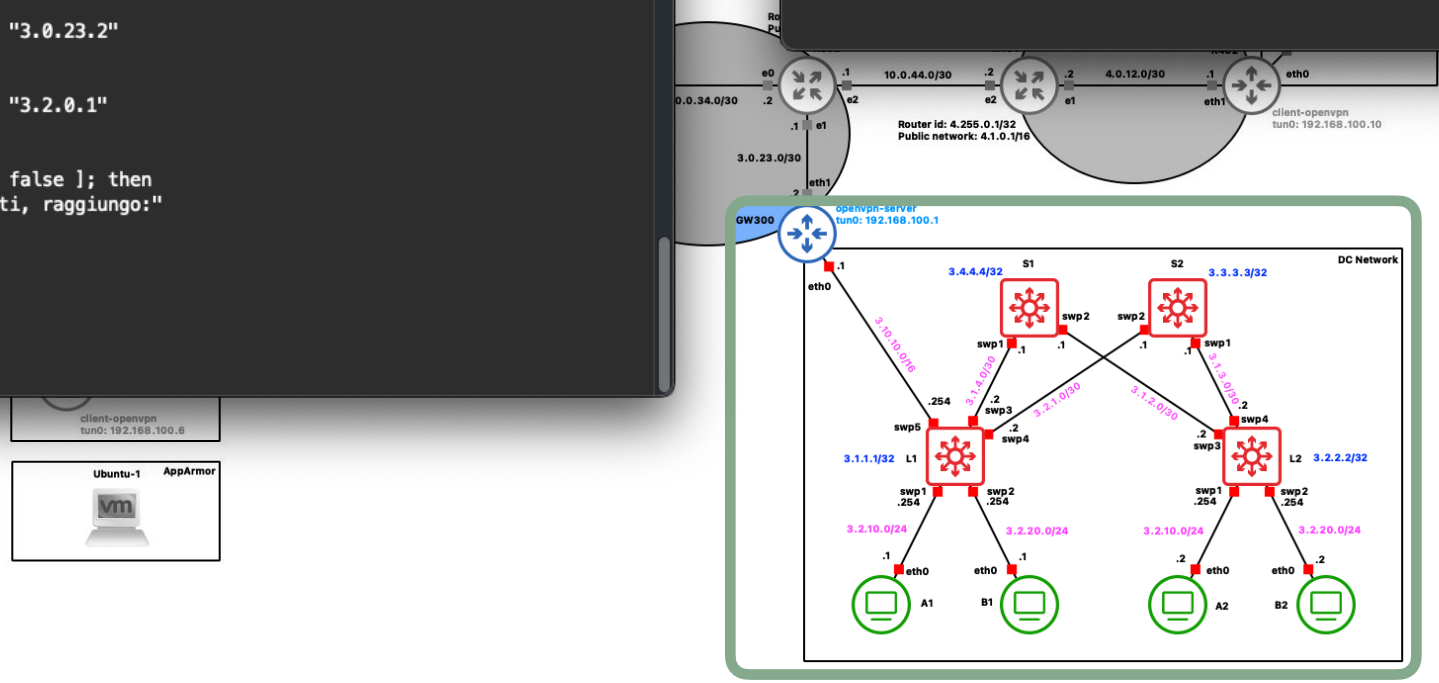
```
net add vrf TENA vni 50
net add vlan 50 vrf TENA
net add vlan 10 vrf TENA
net add vlan 100 vrf TENA

net add vrf TENB vni 60
net add vlan 60 vrf TENB
net add vlan 20 vrf TENB
net add vlan 200 vrf TENB
```

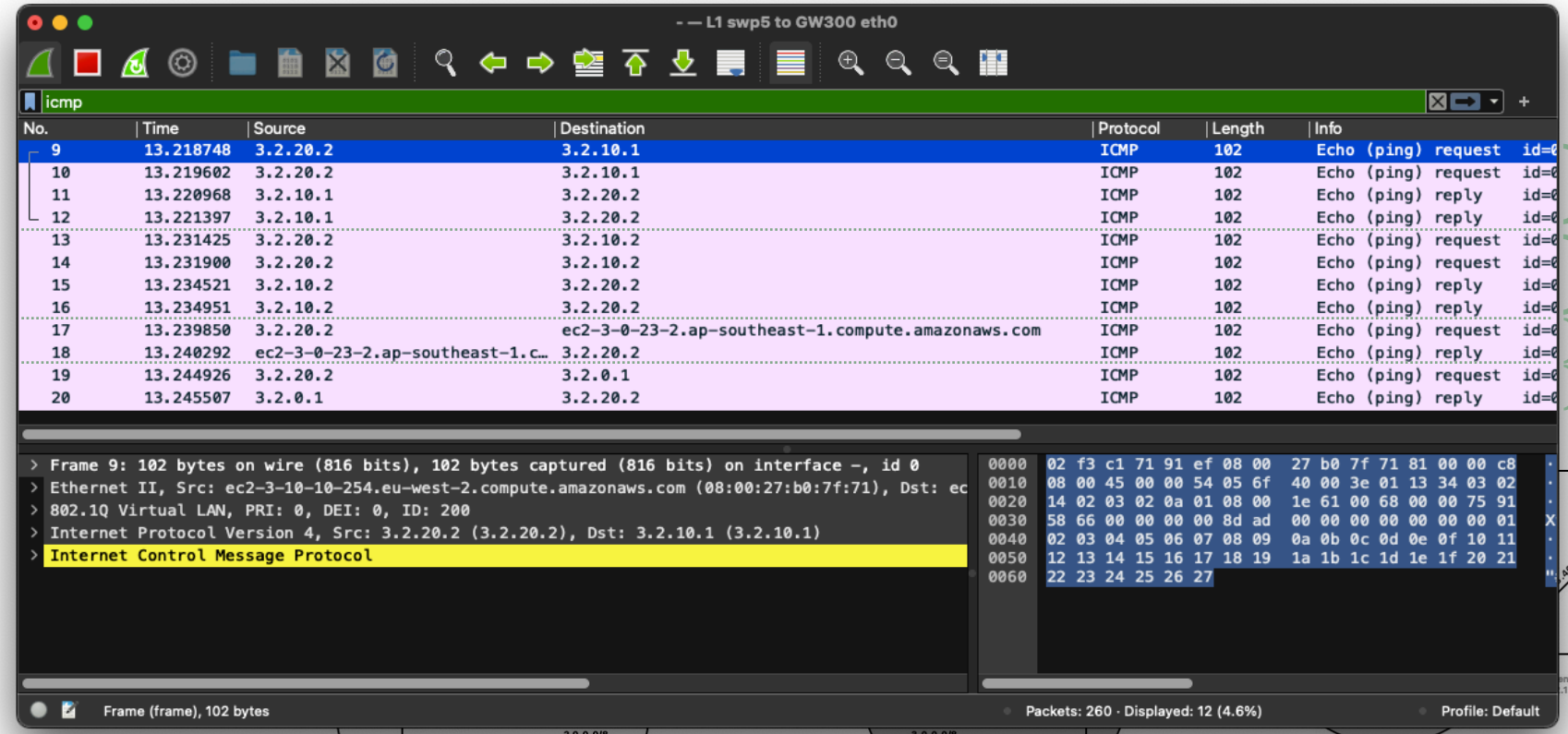
pierpaolospaziani — root@B2: / — telnet 192.168.56.108 5032 — 80×38

```
root@B2:/# cat root/test.sh
#!/bin/bash

test_failed=false

ping_and_print_result() {
    ip_address=$1
    if ! ping -c 1 -W 1 "$ip_address" >/dev/null 2>&1; then
        test_failed=true
        echo "Errore: Il test per $ip_address non è stato superato!"
    fi
}

# Test A1
ping_and_print_result "3.2.10.1"

# Test B1
ping_and_print_result "3.2.20.1"

#Test A2
ping_and_print_result "3.2.10.2"

#Test GW300
ping_and_print_result "3.0.23.2"

#Test R302
ping_and_print_result "3.2.0.1"

# Verifica finale
if [ "$test_failed" = false ]; then
    echo "Test superati, raggiungo:"
    echo " - A1"
    echo " - B1"
    echo " - A2"
    echo " - GW300"
    echo " - R302"
fi
root@B2:/#
```

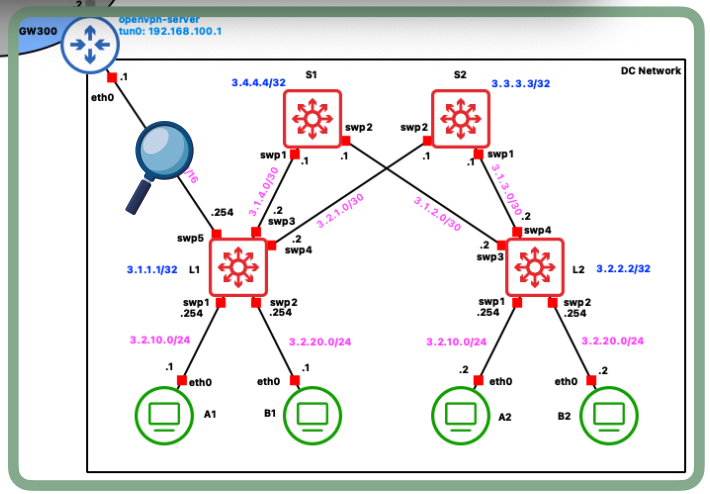
pierpaolospaziani — root@B2: ~ — telnet 192.168.56.108 5032 — 80×24

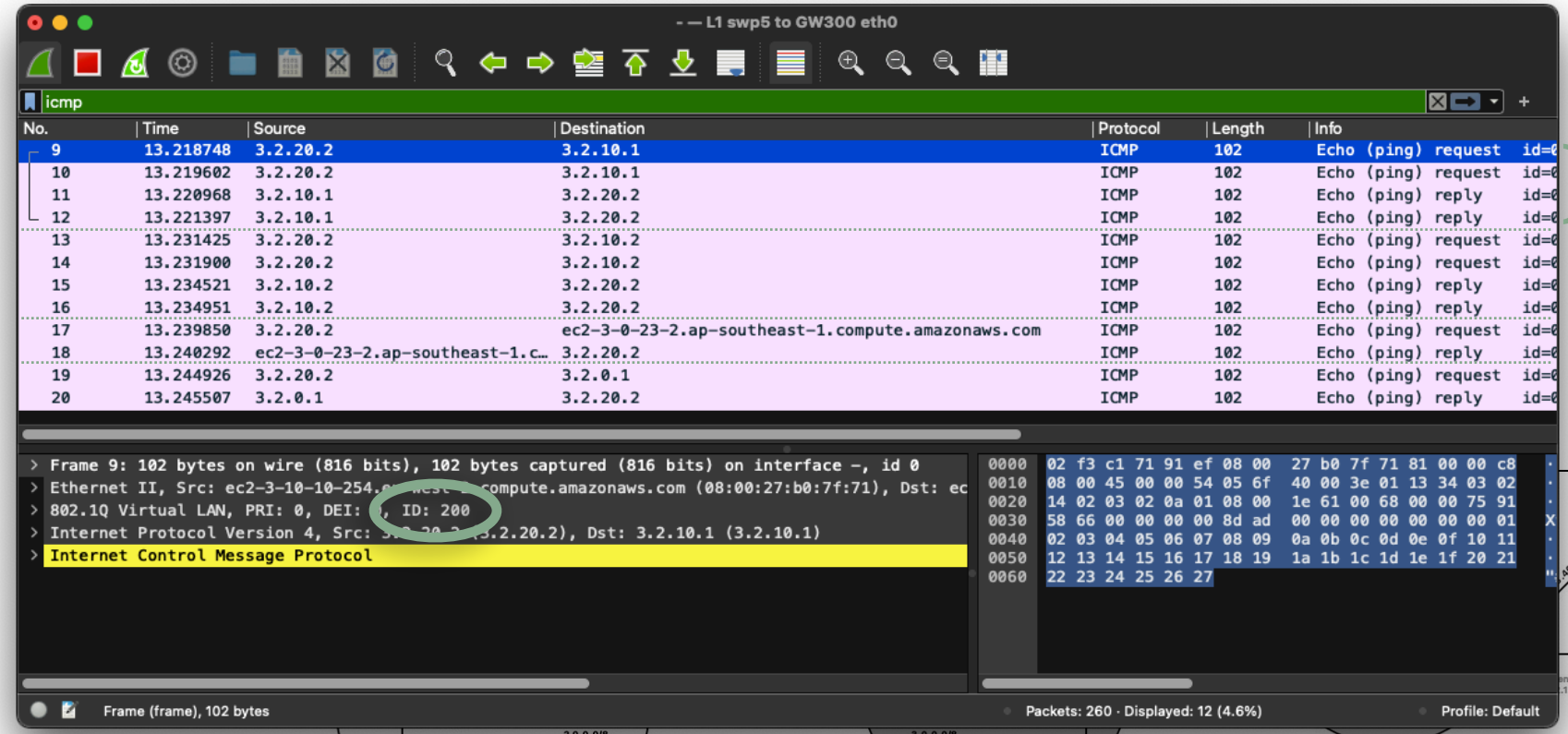
```
root@B2:~# ./test.sh
Test superati, raggiungo:
 - A1
 - B1
 - A2
 - GW300
 - R302
root@B2:~#
```



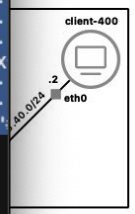



```
net add vrf TENA vni 50
net add vlan 50 vrf TENA
net add vlan 10 vrf TENA
net add vlan 100 vrf TENA

net add vrf TENB vni 60
net add vlan 60 vrf TENB
net add vlan 20 vrf TENB
net add vlan 200 vrf TENB
```

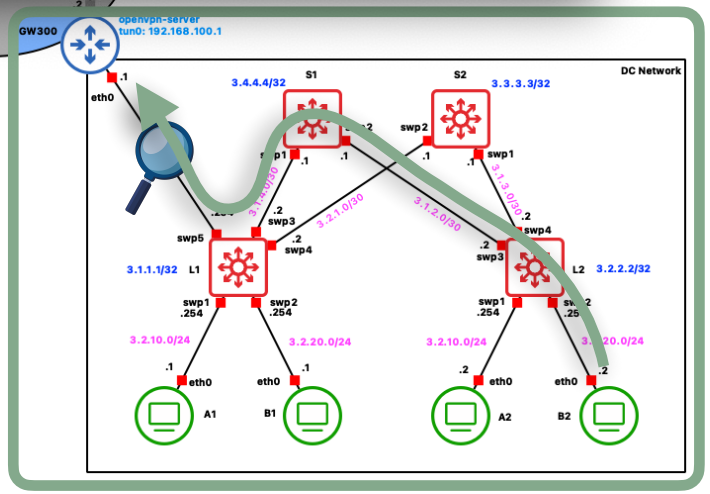


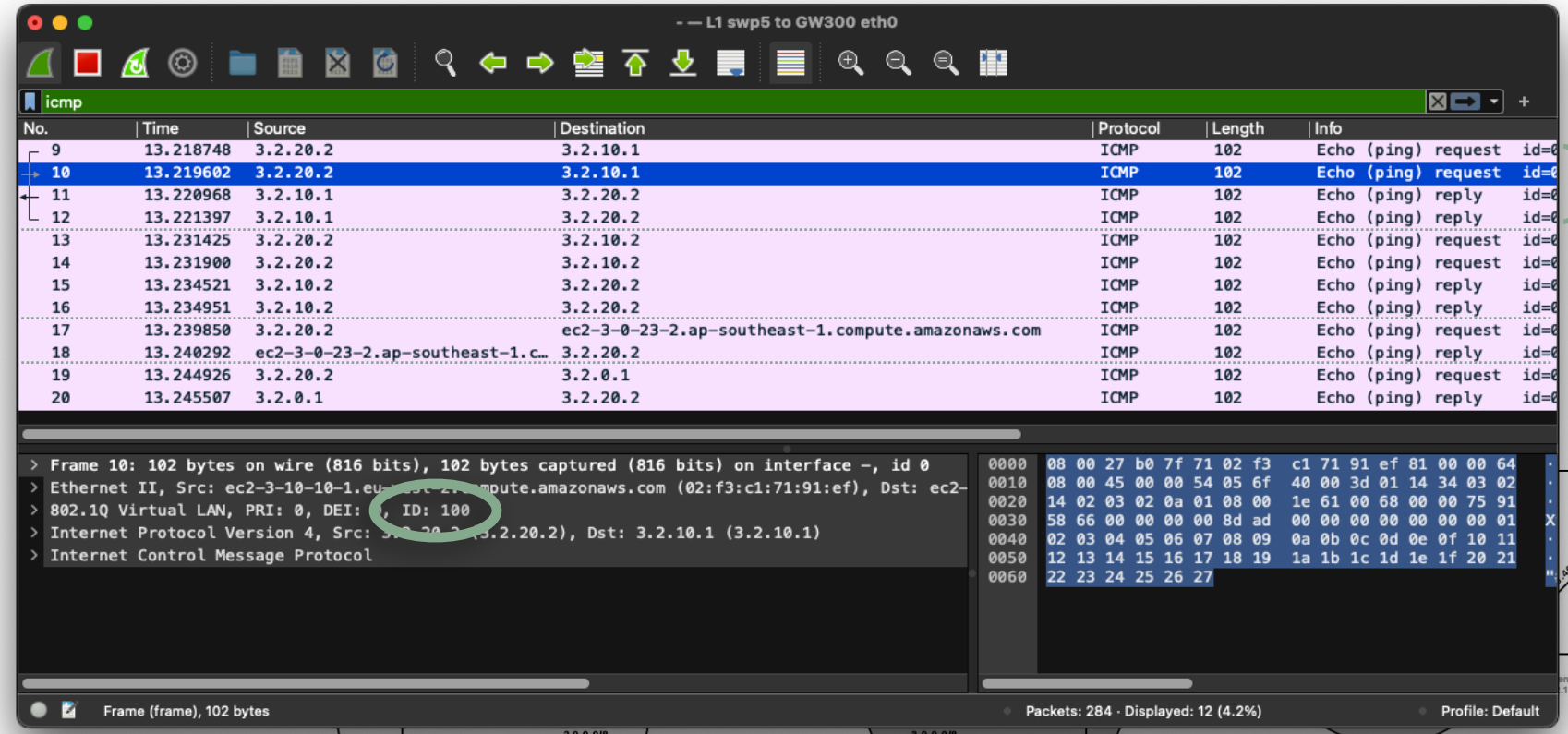


B2→A1

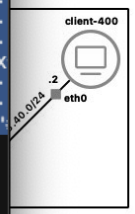



```
net add vrf TENA vni 50
net add vlan 50 vrf TENA
net add vlan 10 vrf TENA
net add vlan 100 vrf TENA

net add vrf TENB vni 60
net add vlan 60 vrf TENB
net add vlan 20 vrf TENB
net add vlan 200 vrf TENB
```

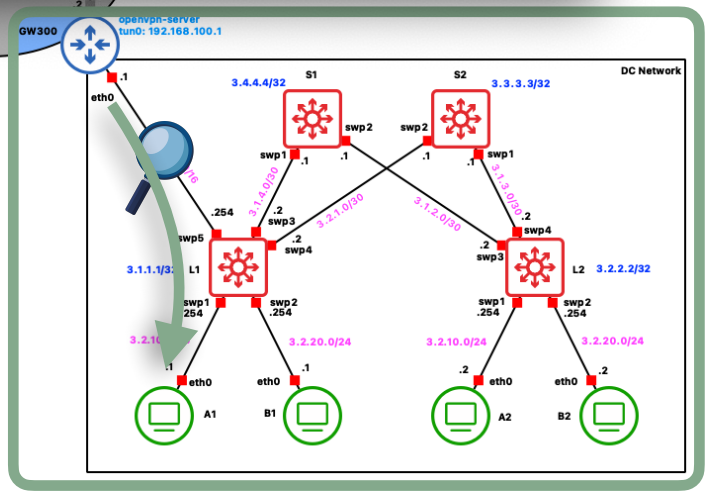


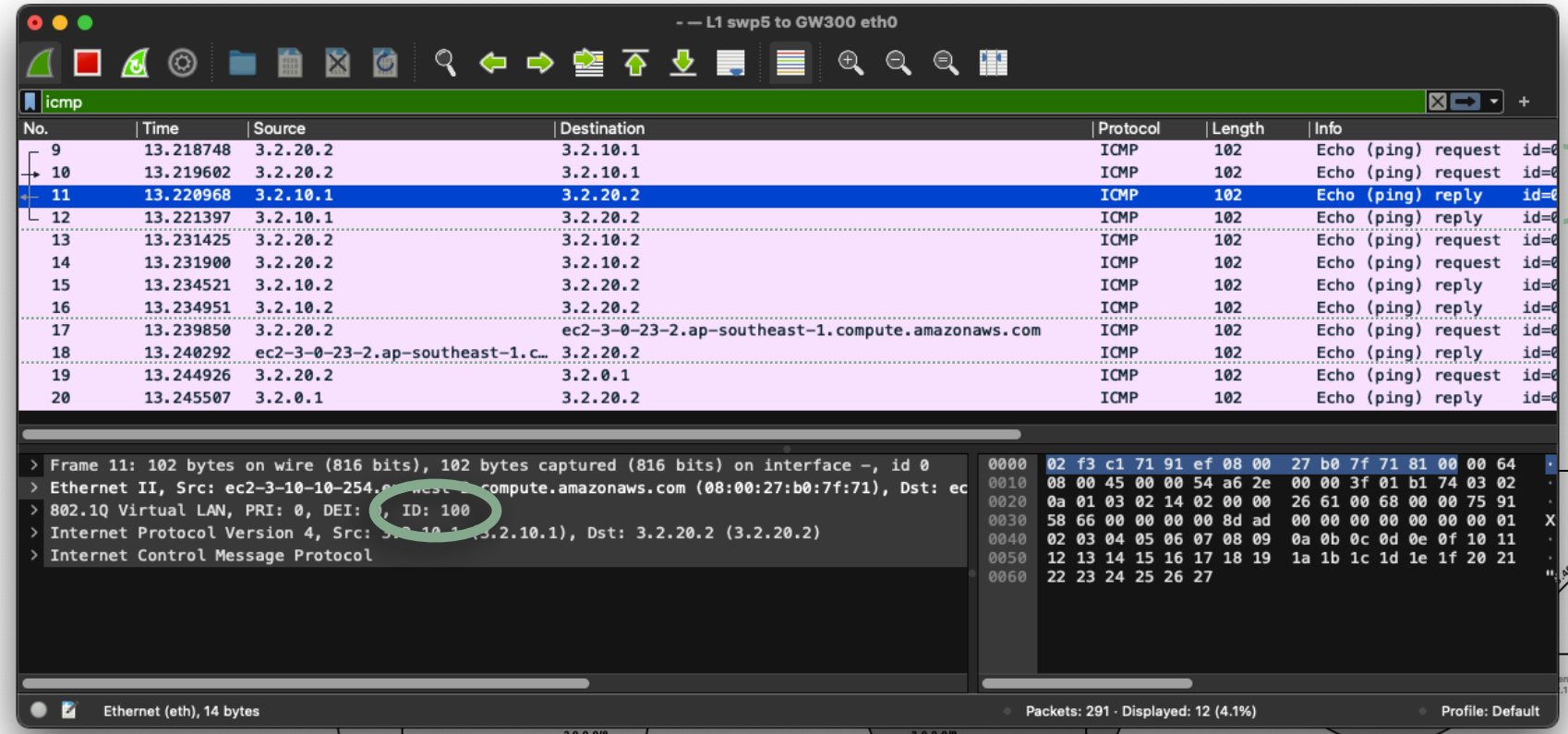


B2→A1

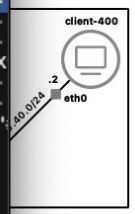



```
net add vrf TENA vni 50
net add vlan 50 vrf TENA
net add vlan 10 vrf TENA
net add vlan 100 vrf TENA

net add vrf TENB vni 60
net add vlan 60 vrf TENB
net add vlan 20 vrf TENB
net add vlan 200 vrf TENB
```

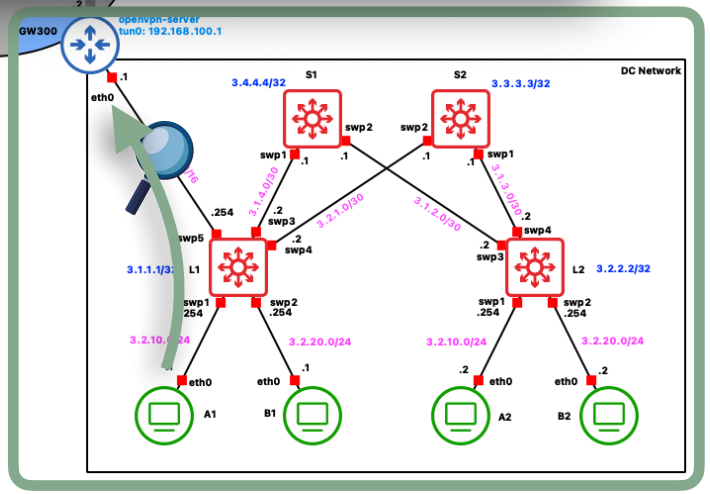


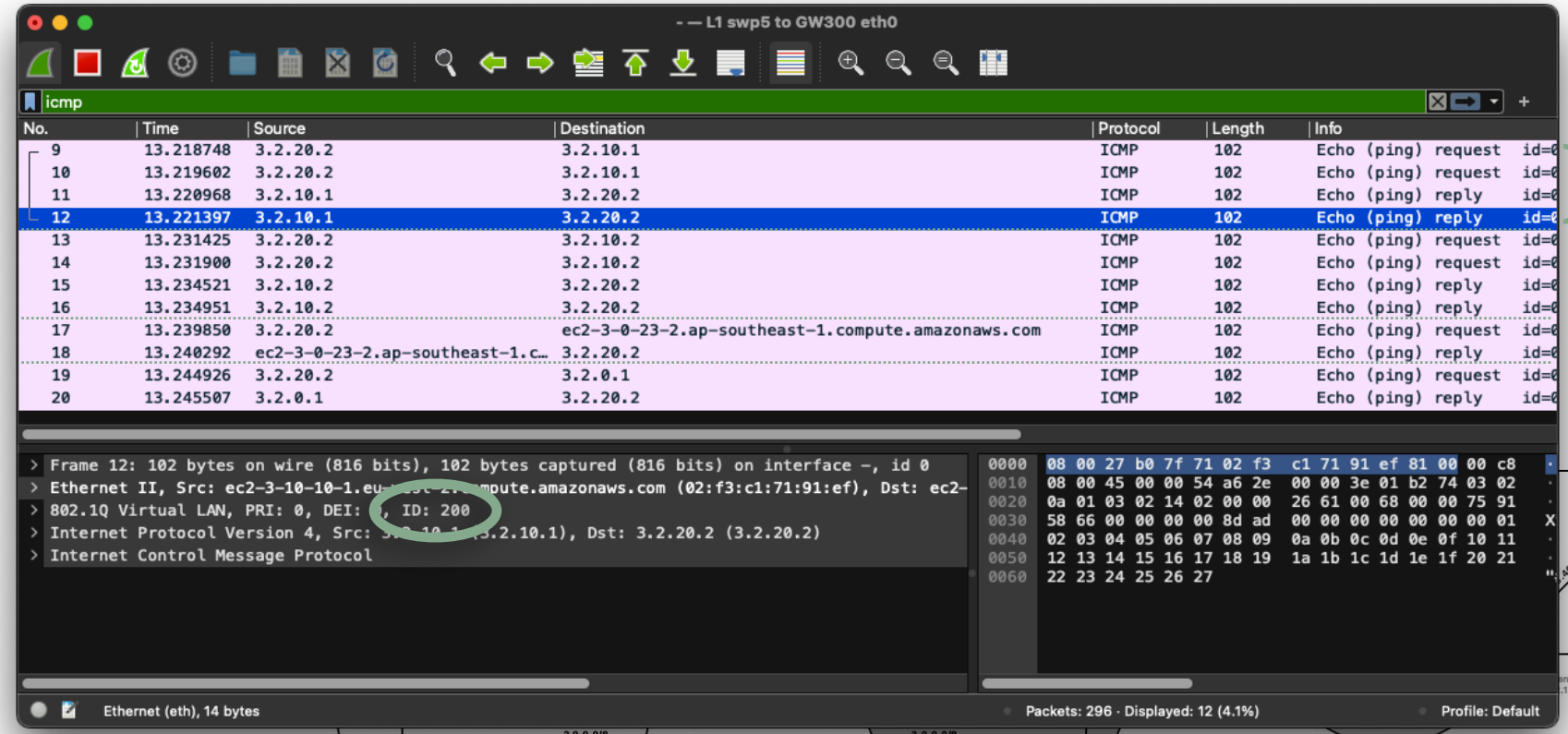


B2→A1

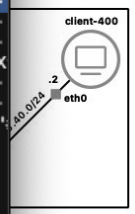



```
net add vrf TENA vni 50
net add vlan 50 vrf TENA
net add vlan 10 vrf TENA
net add vlan 100 vrf TENA

net add vrf TENB vni 60
net add vlan 60 vrf TENB
net add vlan 20 vrf TENB
net add vlan 200 vrf TENB
```

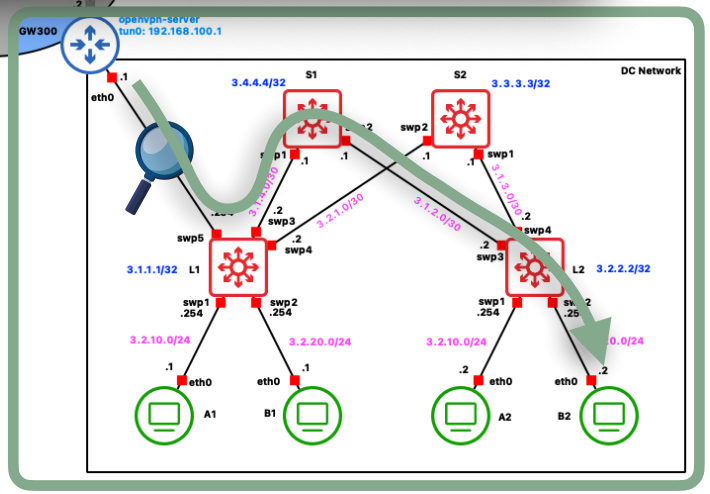


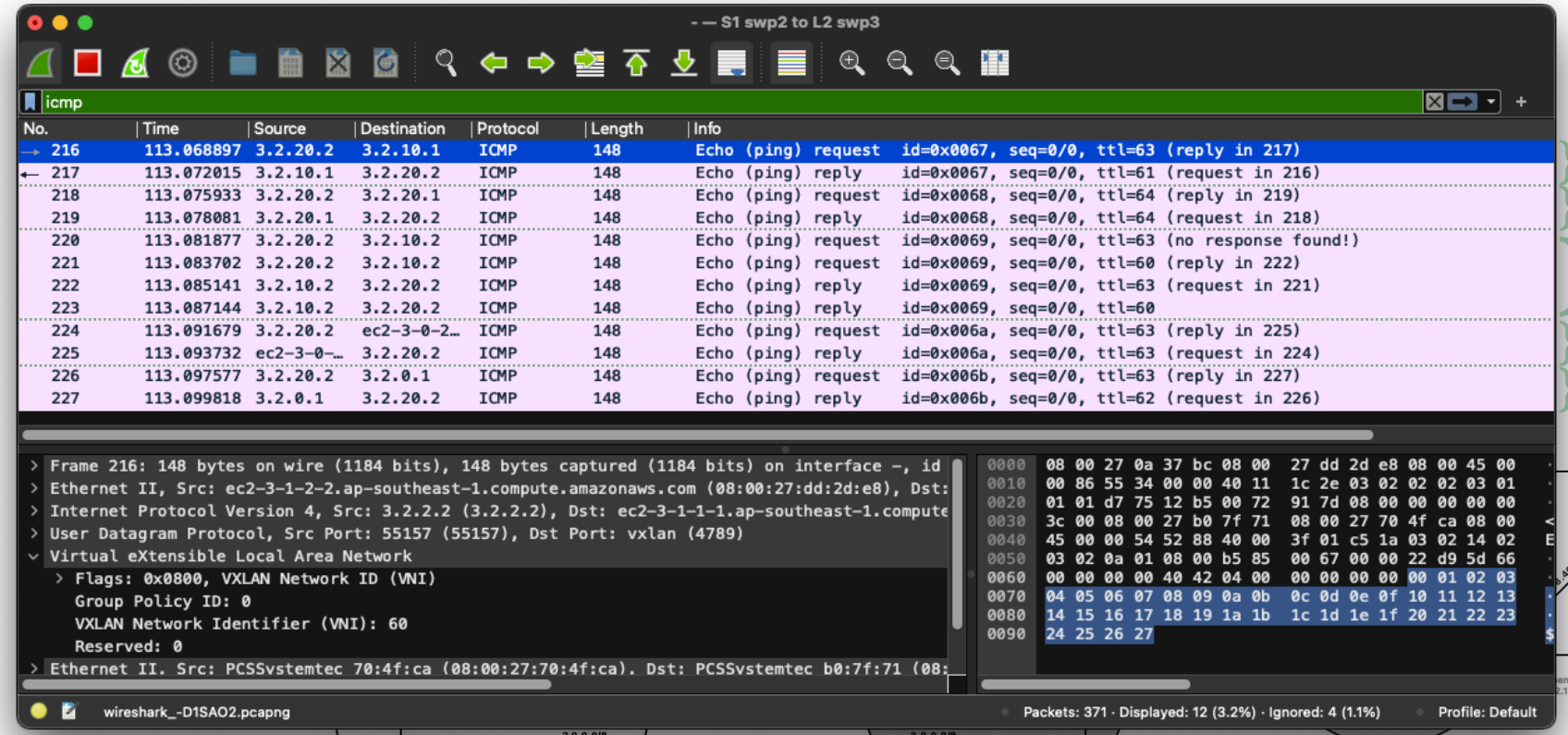


B2→A1



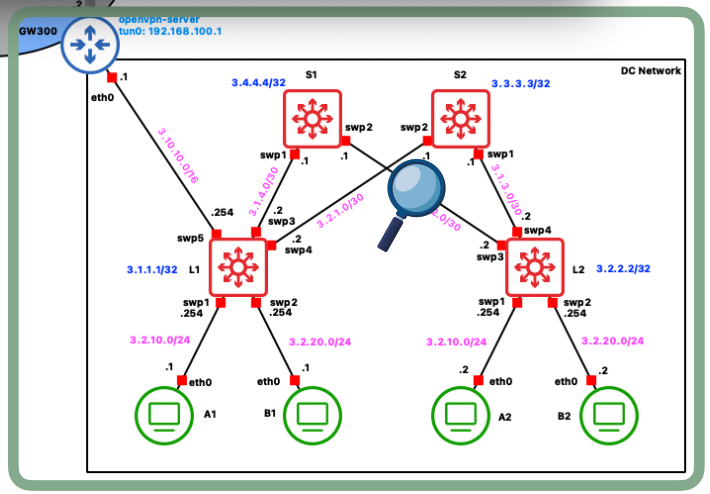

```
net add vrf TENA vni 50
net add vlan 50 vrf TENA
net add vlan 10 vrf TENA
net add vlan 100 vrf TENA

net add vrf TENB vni 60
net add vlan 60 vrf TENB
net add vlan 20 vrf TENB
net add vlan 200 vrf TENB
```

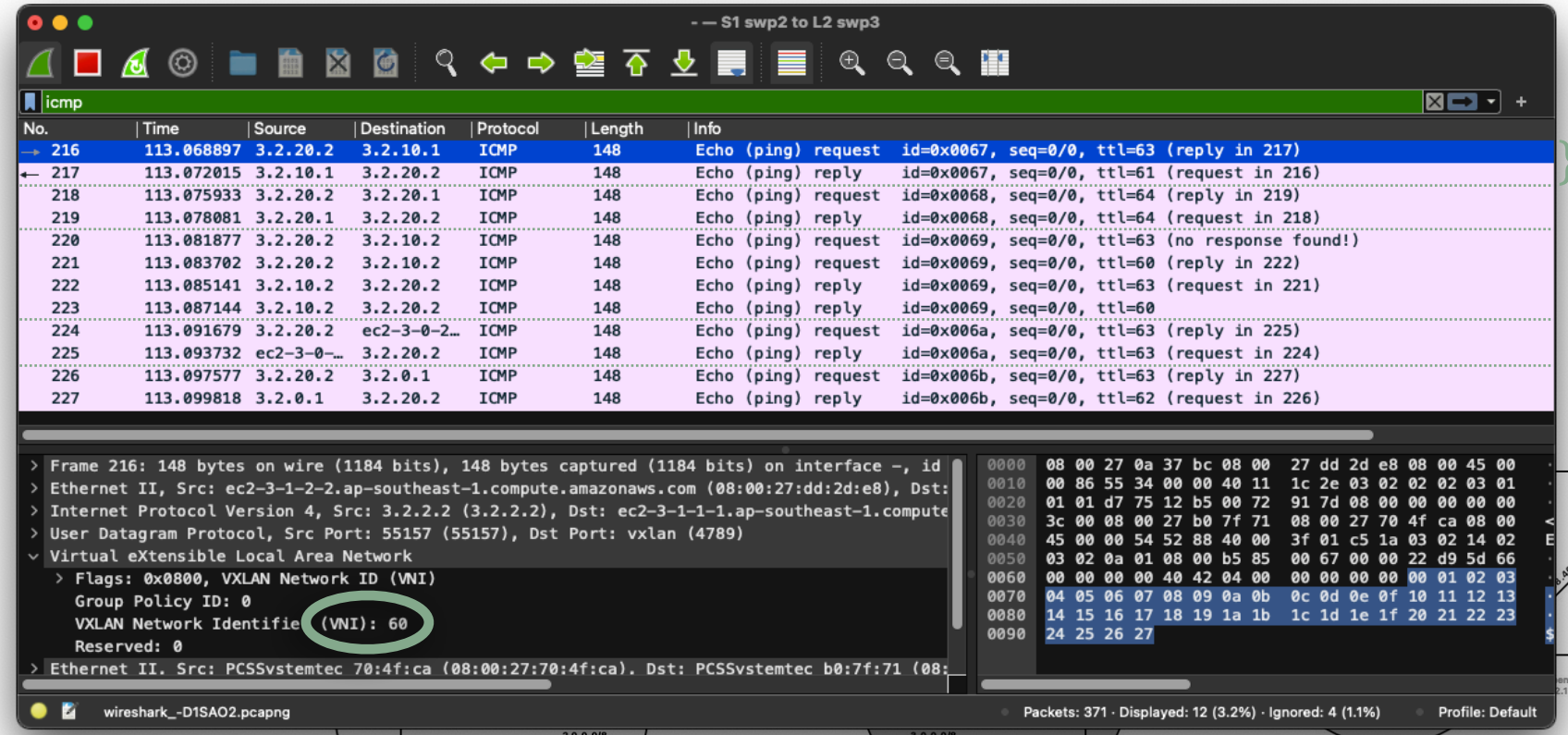




B2→A1
B2→B1
B2→A2
B2→GW300
B2→R302

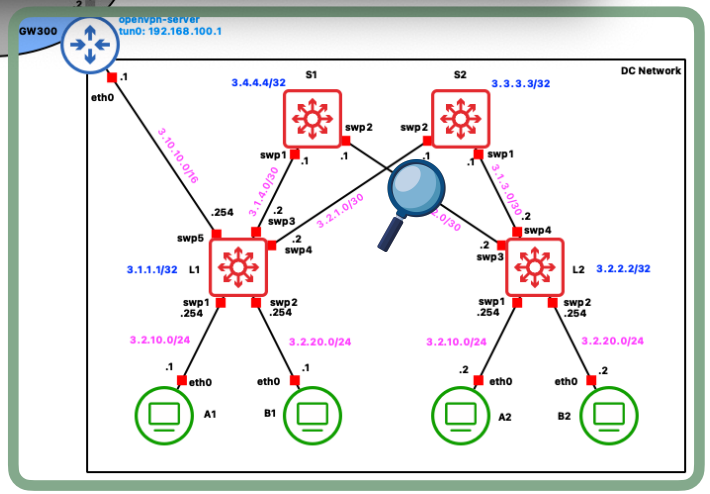

```
net add vrf TENA vni 50
net add vlan 50 vrf TENA
net add vlan 10 vrf TENA
net add vlan 100 vrf TENA

net add vrf TENB vni 60
net add vlan 60 vrf TENB
net add vlan 20 vrf TENB
net add vlan 200 vrf TENB
```

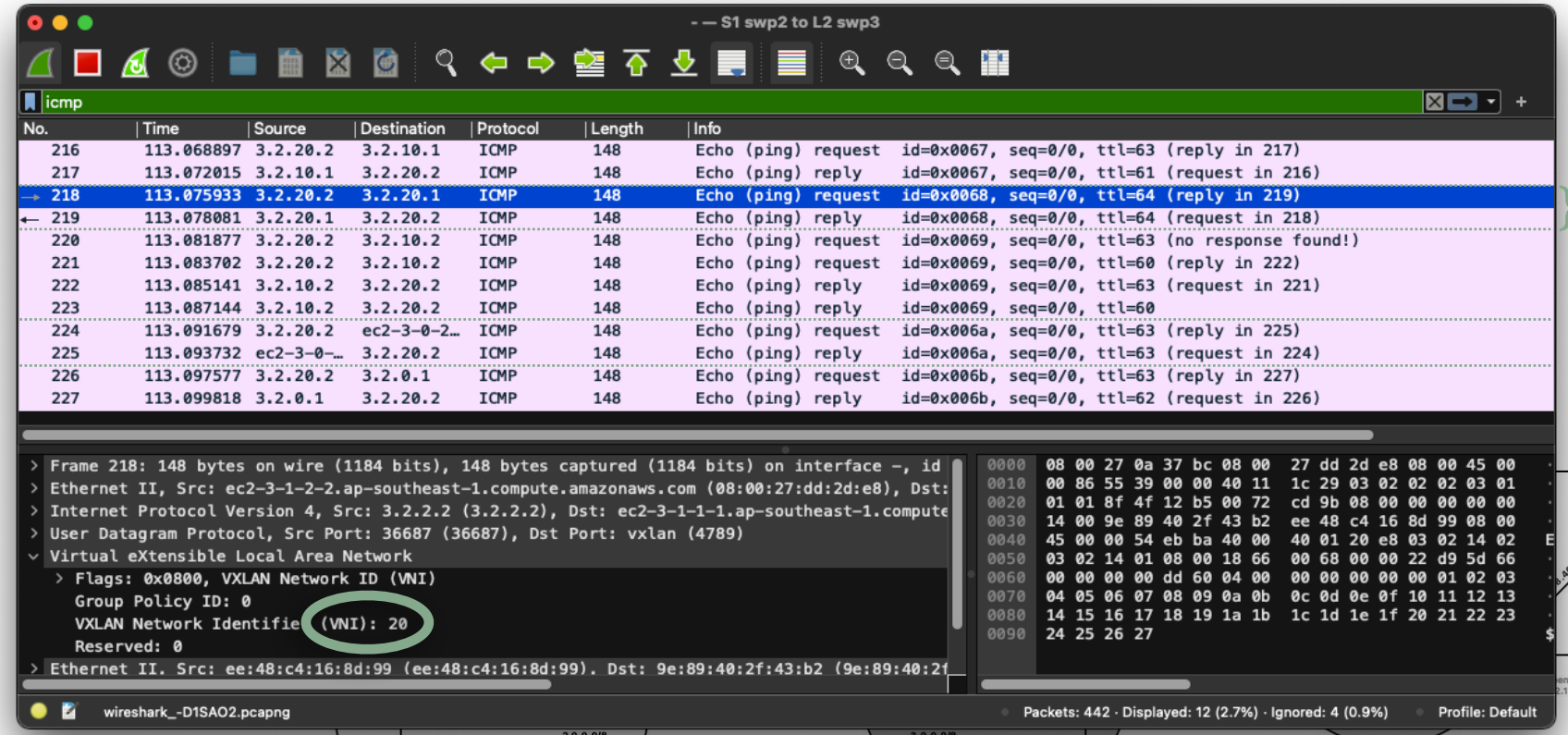




B2→A1

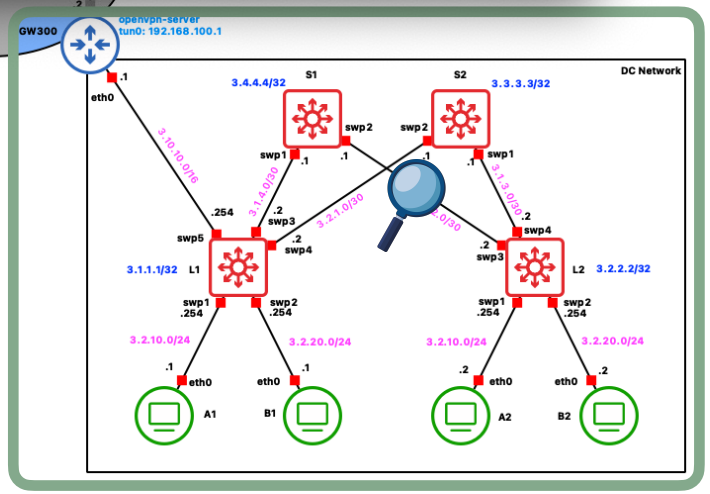

```
net add vrf TENA vni 50
net add vlan 50 vrf TENA
net add vlan 10 vrf TENA
net add vlan 100 vrf TENA

net add vrf TENB vni 60
net add vlan 60 vrf TENB
net add vlan 20 vrf TENB
net add vlan 200 vrf TENB
```

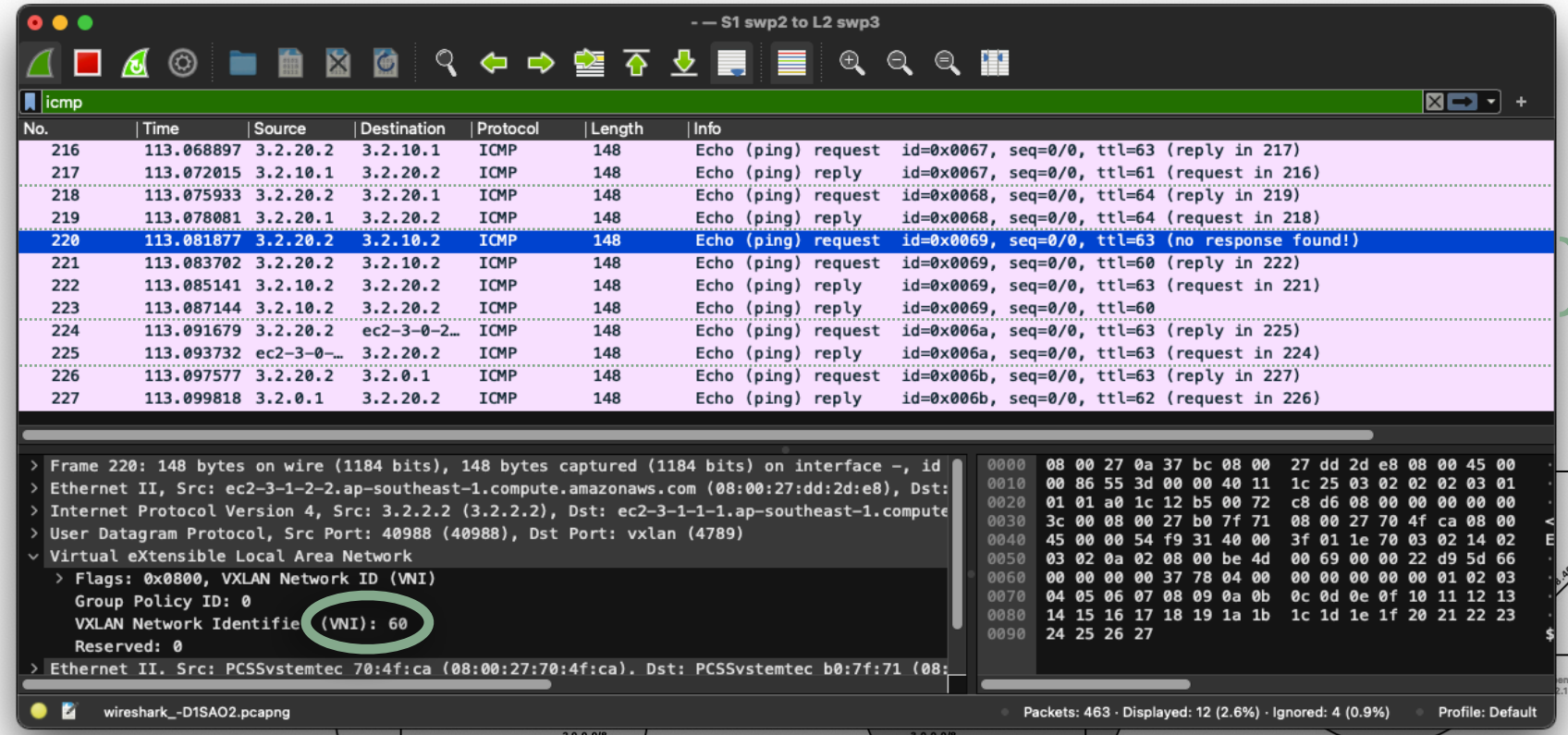




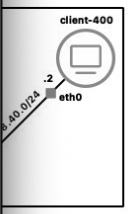
B2→B1


```
net add vrf TENA vni 50
net add vlan 50 vrf TENA
net add vlan 10 vrf TENA
net add vlan 100 vrf TENA

net add vrf TENB vni 60
net add vlan 60 vrf TENB
net add vlan 20 vrf TENB
net add vlan 200 vrf TENB
```

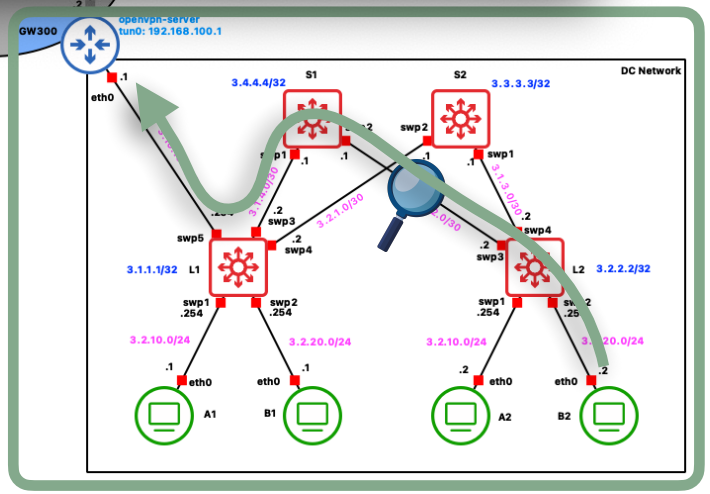


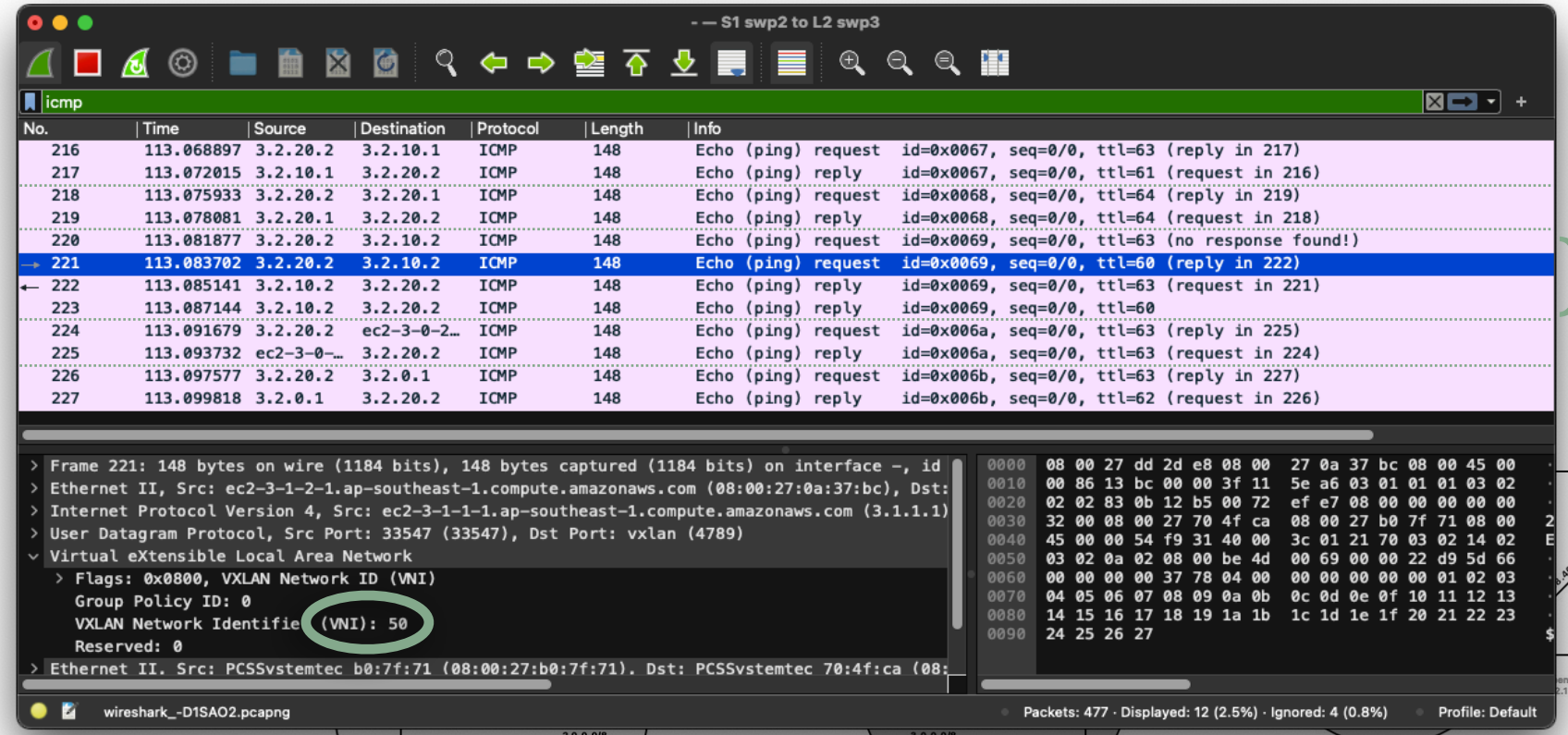


B2→A2



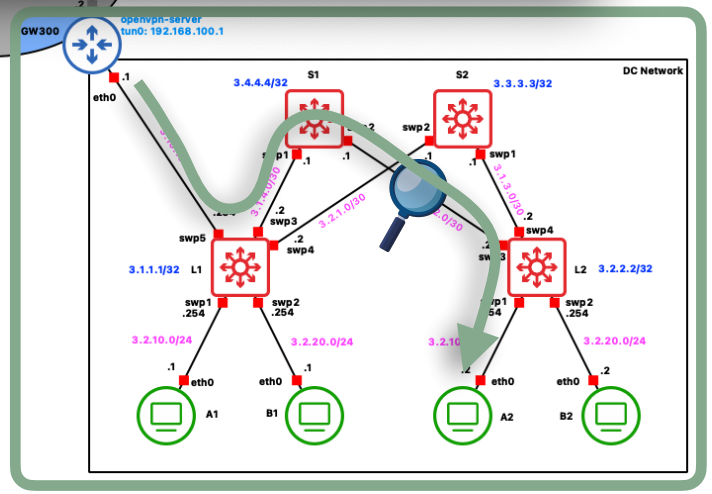

```
net add vrf TENA vni 50
net add vlan 50 vrf TENA
net add vlan 10 vrf TENA
net add vlan 100 vrf TENA

net add vrf TENB vni 60
net add vlan 60 vrf TENB
net add vlan 20 vrf TENB
net add vlan 200 vrf TENB
```

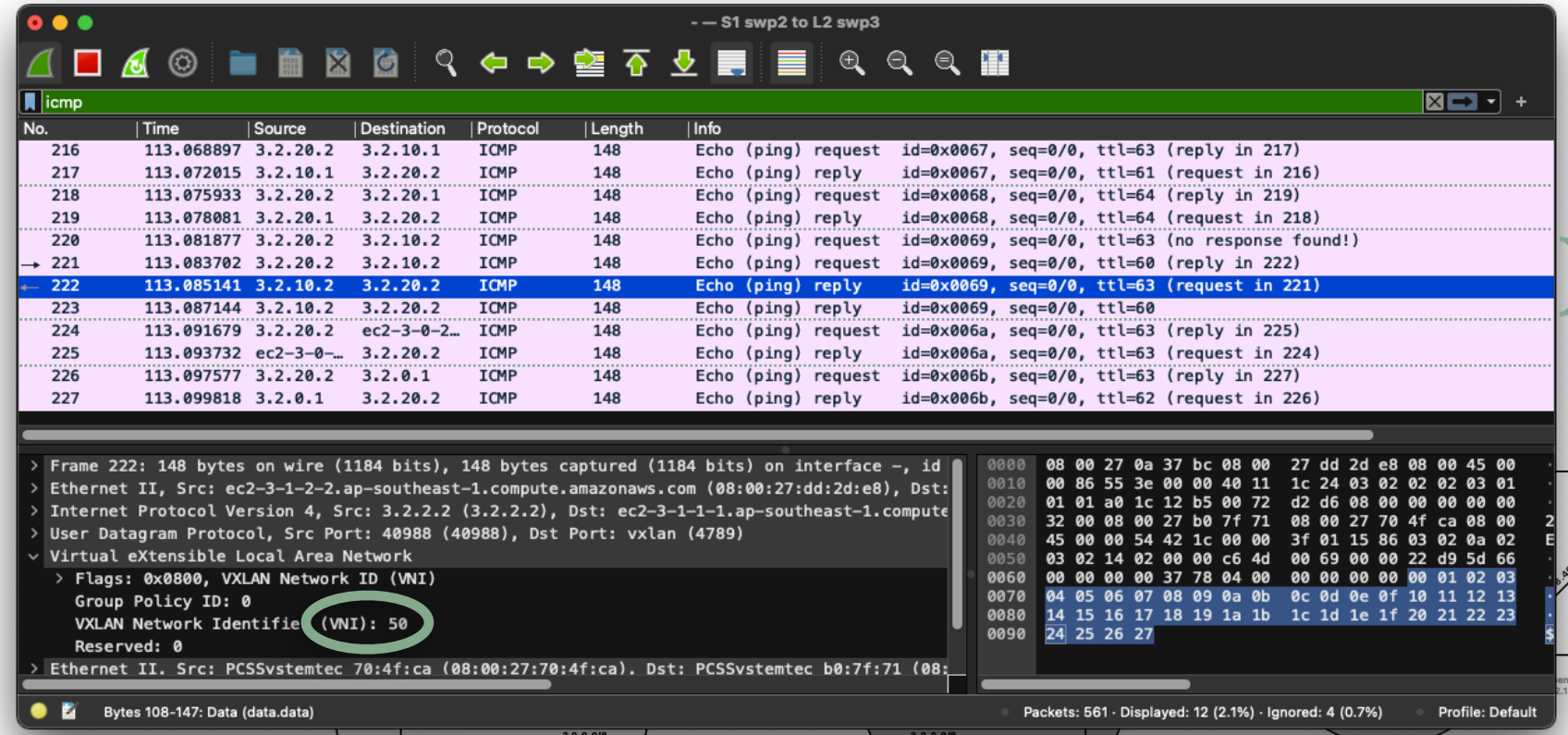




B2→A2

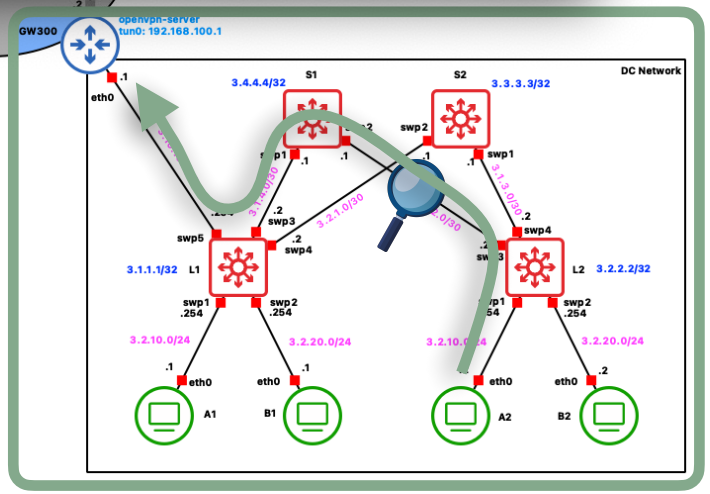

```
net add vrf TENA vni 50
net add vlan 50 vrf TENA
net add vlan 10 vrf TENA
net add vlan 100 vrf TENA

net add vrf TENB vni 60
net add vlan 60 vrf TENB
net add vlan 20 vrf TENB
net add vlan 200 vrf TENB
```

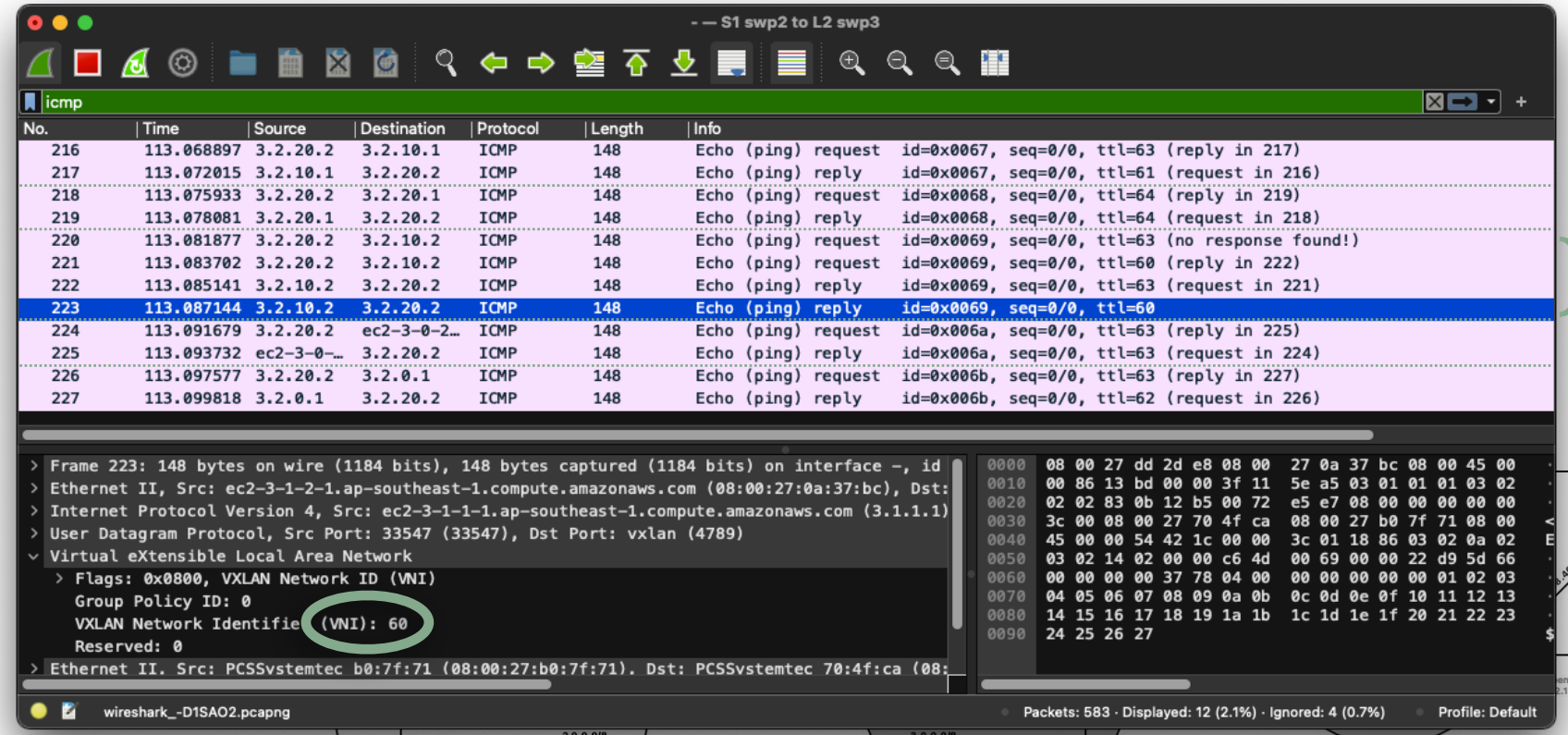




B2→A2

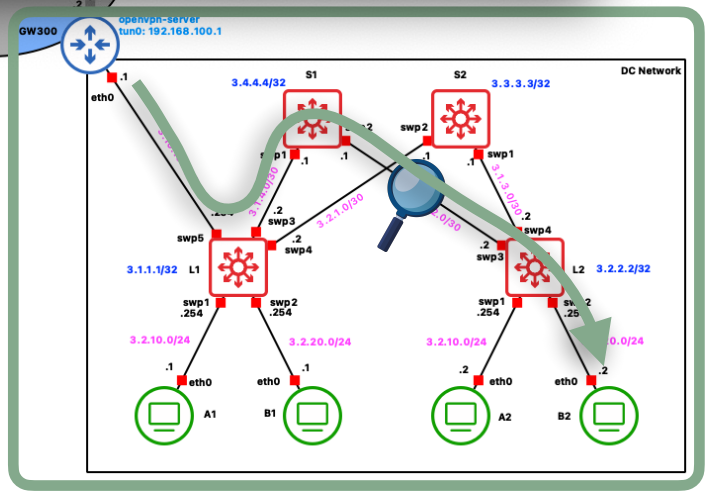

```
net add vrf TENA vni 50
net add vlan 50 vrf TENA
net add vlan 10 vrf TENA
net add vlan 100 vrf TENA

net add vrf TENB vni 60
net add vlan 60 vrf TENB
net add vlan 20 vrf TENB
net add vlan 200 vrf TENB
```

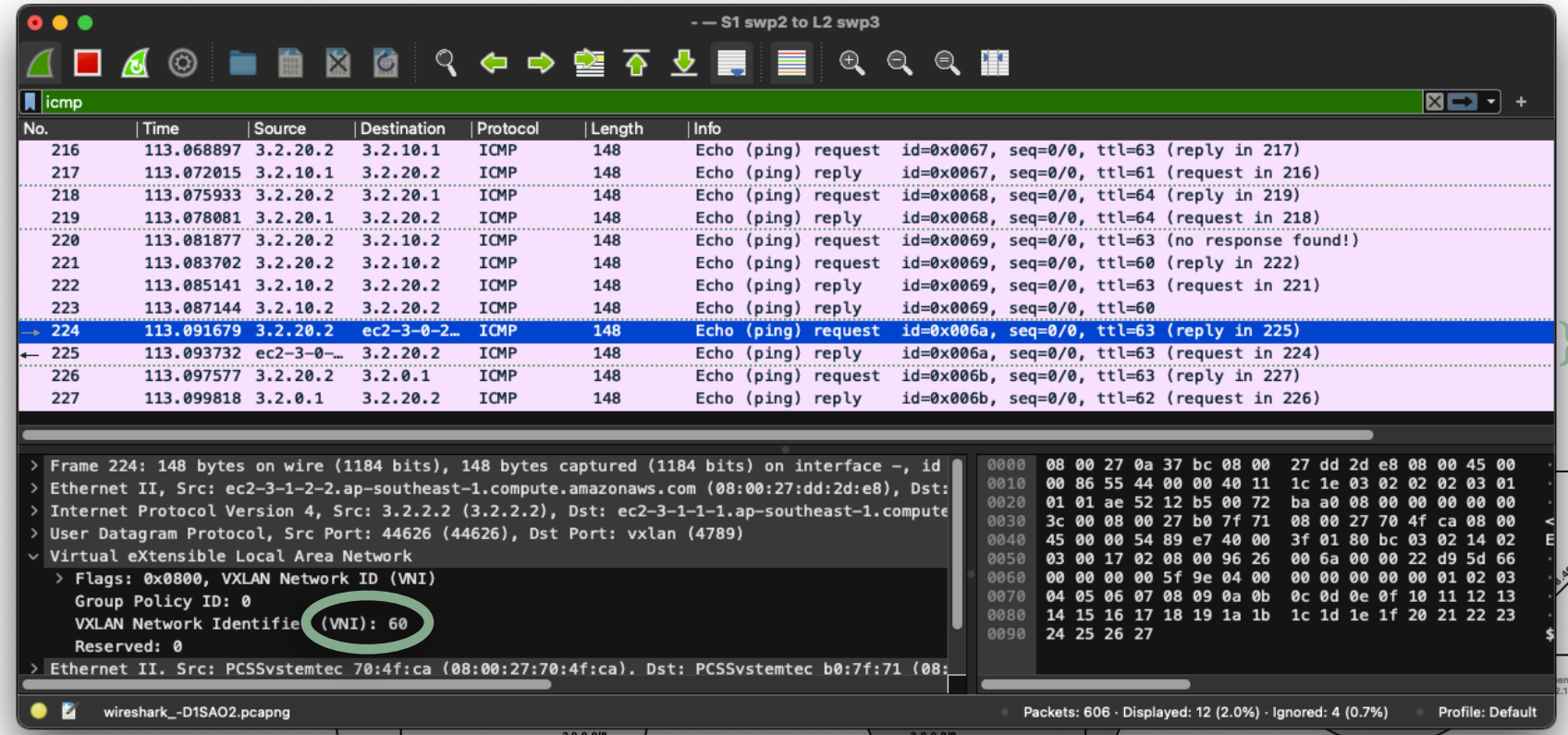




B2→A2

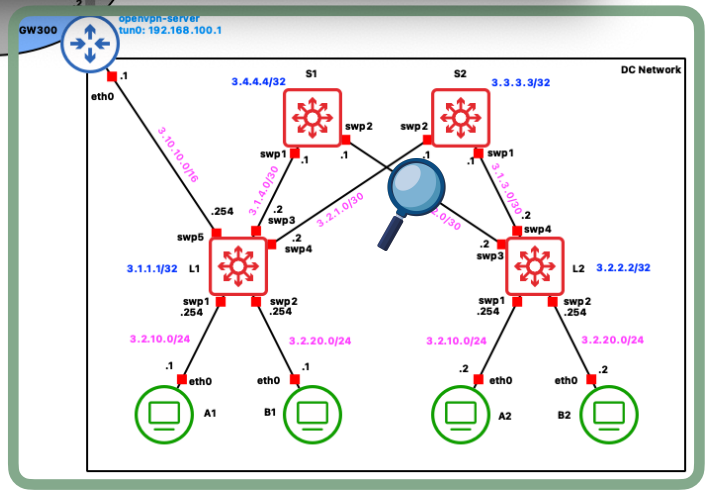

```
net add vrf TENA vni 50
net add vlan 50 vrf TENA
net add vlan 10 vrf TENA
net add vlan 100 vrf TENA

net add vrf TENB vni 60
net add vlan 60 vrf TENB
net add vlan 20 vrf TENB
net add vlan 200 vrf TENB
```

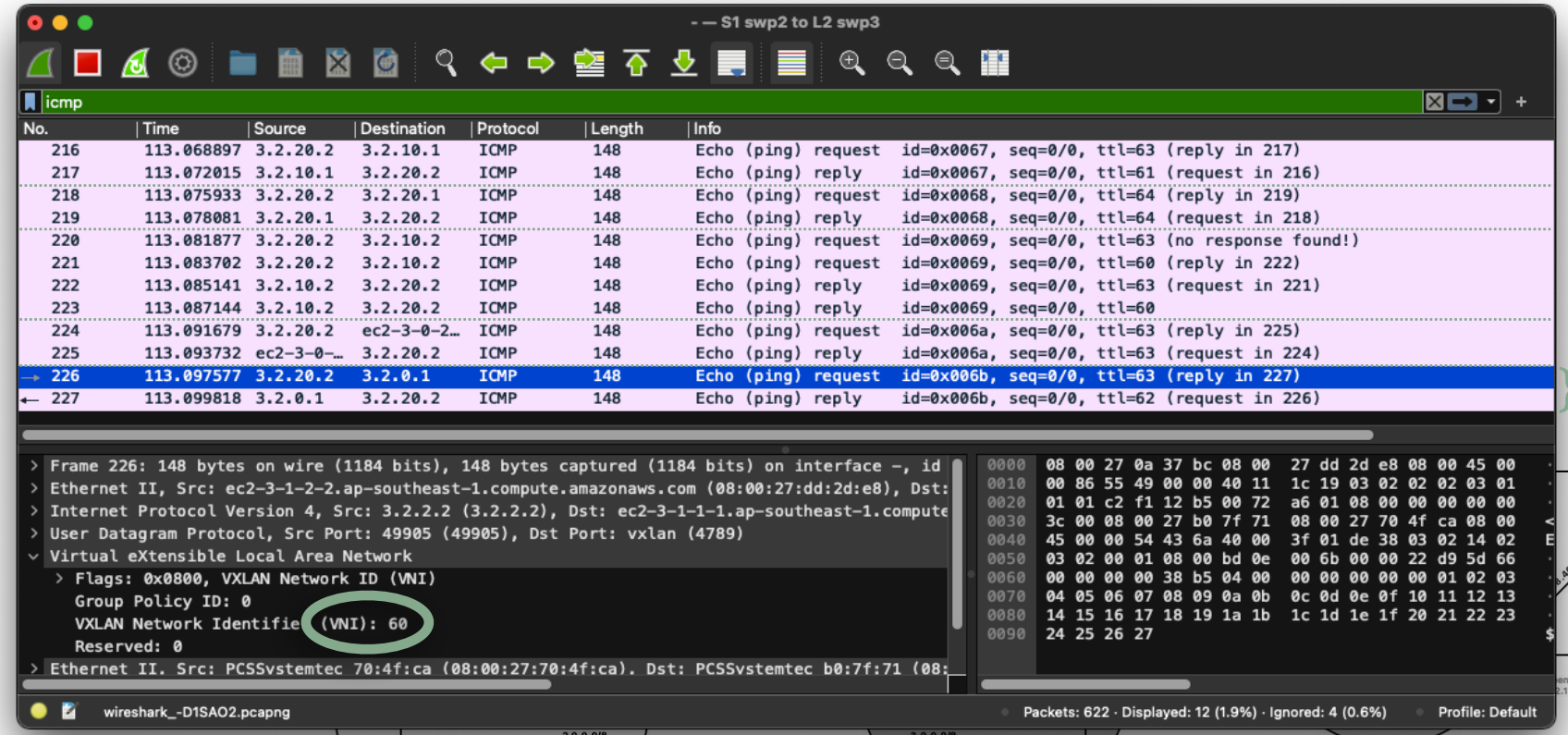




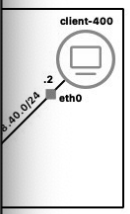
B2→GW300


```
net add vrf TENA vni 50
net add vlan 50 vrf TENA
net add vlan 10 vrf TENA
net add vlan 100 vrf TENA

net add vrf TENB vni 60
net add vlan 60 vrf TENB
net add vlan 20 vrf TENB
net add vlan 200 vrf TENB
```

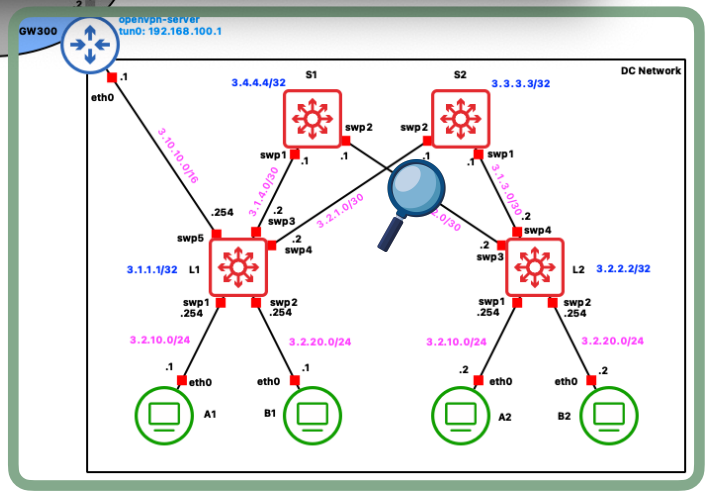


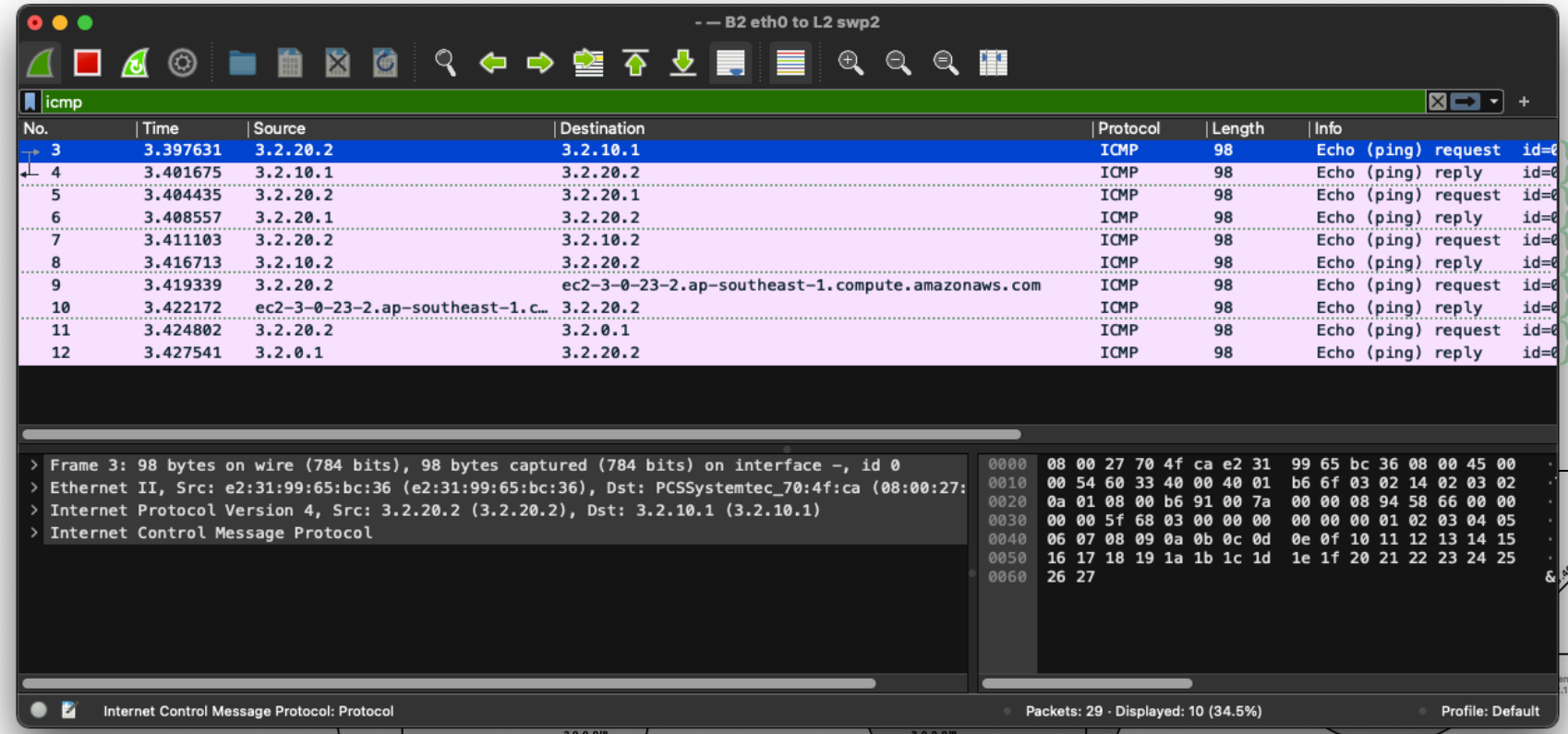


B2→R302

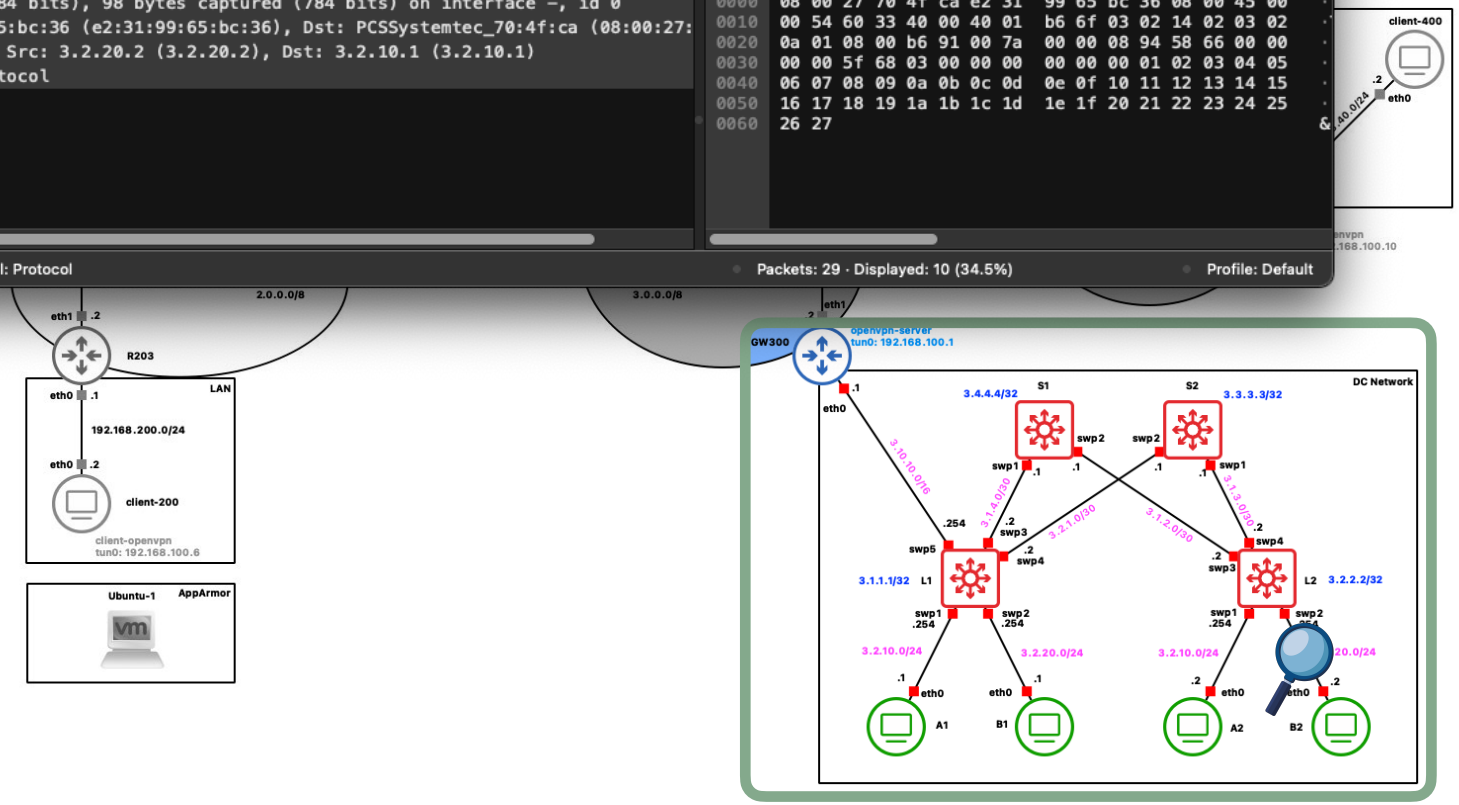



```
net add vrf TENA vni 50
net add vlan 50 vrf TENA
net add vlan 10 vrf TENA
net add vlan 100 vrf TENA

net add vrf TENB vni 60
net add vlan 60 vrf TENB
net add vlan 20 vrf TENB
net add vlan 200 vrf TENB
```

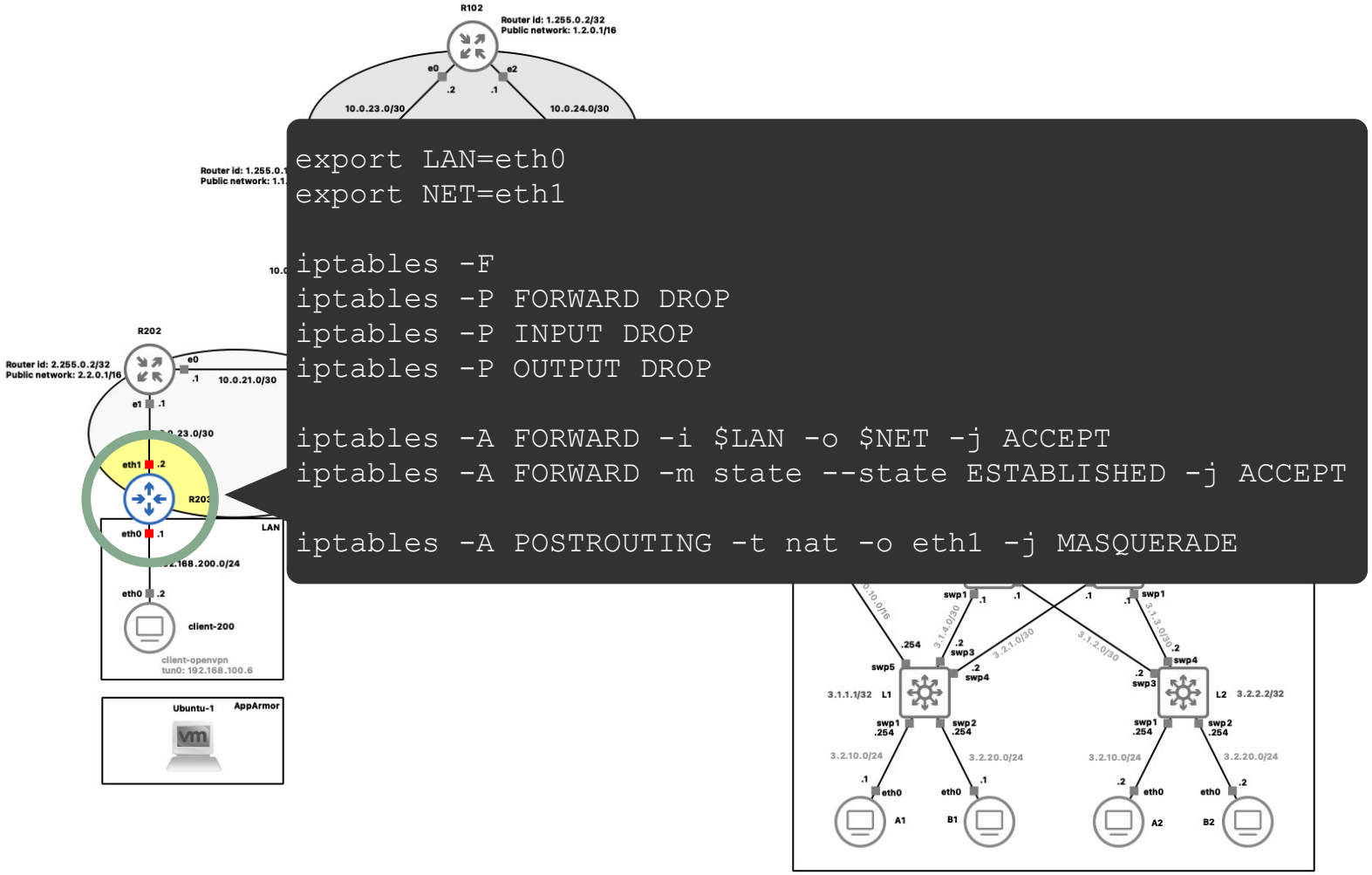




B2→A1
B2→B1
B2→A2
B2→GW300
B2→R302

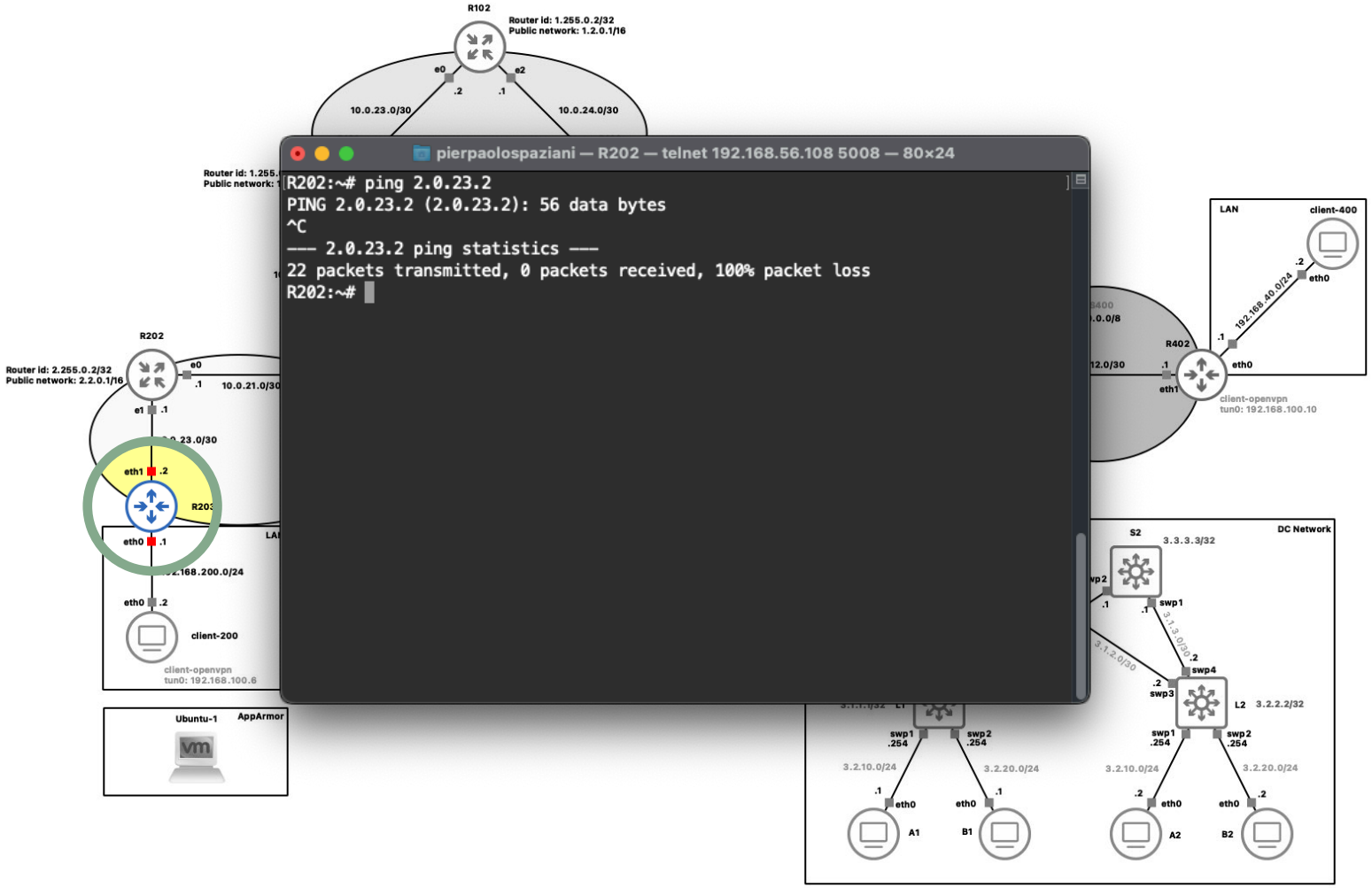


Firewall.

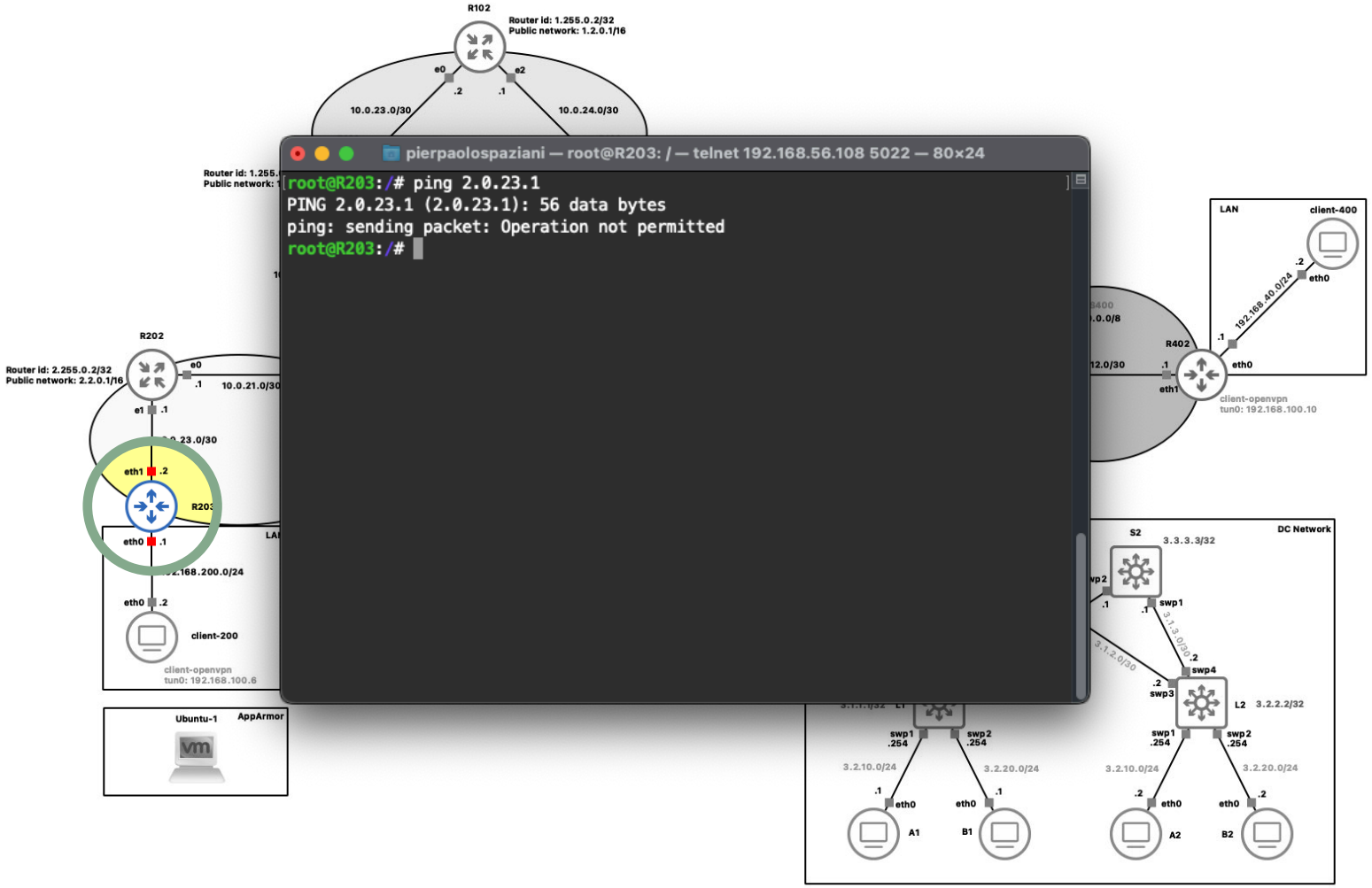



```
export LAN=eth0
export NET=eth1

iptables -F
iptables -P FORWARD DROP
iptables -P INPUT DROP
iptables -P OUTPUT DROP

iptables -A FORWARD -i $LAN -o $NET -j ACCEPT
iptables -A FORWARD -m state --state ESTABLISHED -j ACCEPT

iptables -A POSTROUTING -t nat -o eth1 -j MASQUERADE
```

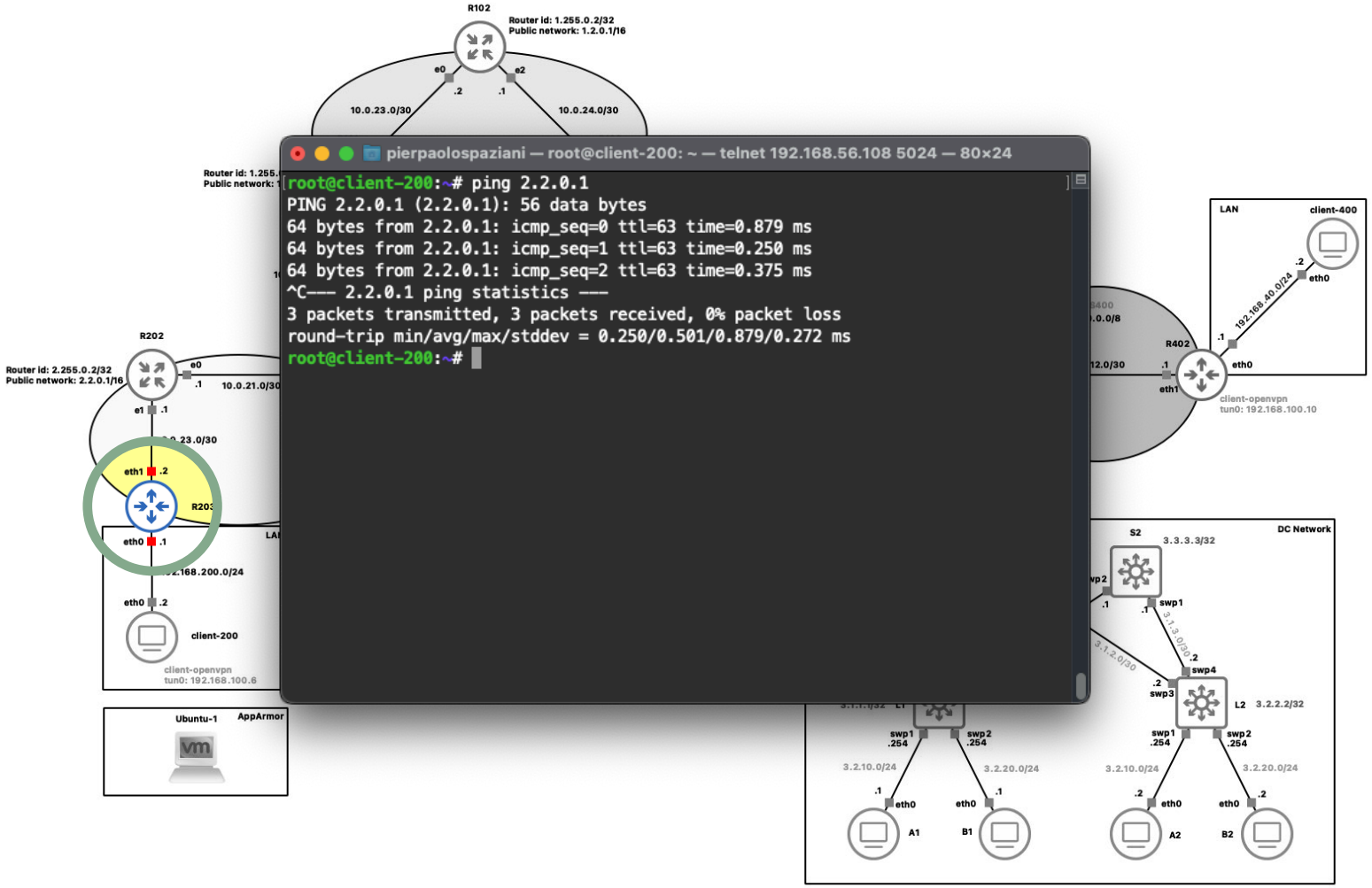
Firewall.


R102
Router id: 1.255.0.2/32
Public network: 1.2.0.1/16
e0
e2
.2
.1
10.0.23.0/30
10.0.24.0/30
pierpaolospaziani — R202 — telnet 192.168.56.108 5008 — 80×24
R202:~# ping 2.0.23.2
PING 2.0.23.2 (2.0.23.2): 56 data bytes
^C
--- 2.0.23.2 ping statistics ---
22 packets transmitted, 0 packets received, 100% packet loss
R202:~#
R202
Router id: 2.255.0.2/32
Public network: 2.2.0.1/16
e0
.1
10.0.21.0/30
e1
.1
eth1
.2
R203
eth0
.1
eth0
.2
client-200
client-openvpn
tun0: 192.168.100.6
Ubuntu-1
AppArmor
vm
LAN
client-400
.2
192.168.40.0/24
.1
eth0
R402
.1
eth1
eth0
client-openvpn
tun0: 192.168.100.10
DC Network
S2
3.3.3.3/32
swp1
swp4
swp3
L2
3.2.2.2/32
swp1
.254
swp2
.254
3.2.10.0/24
3.2.20.0/24
A1
B1
A2
B2

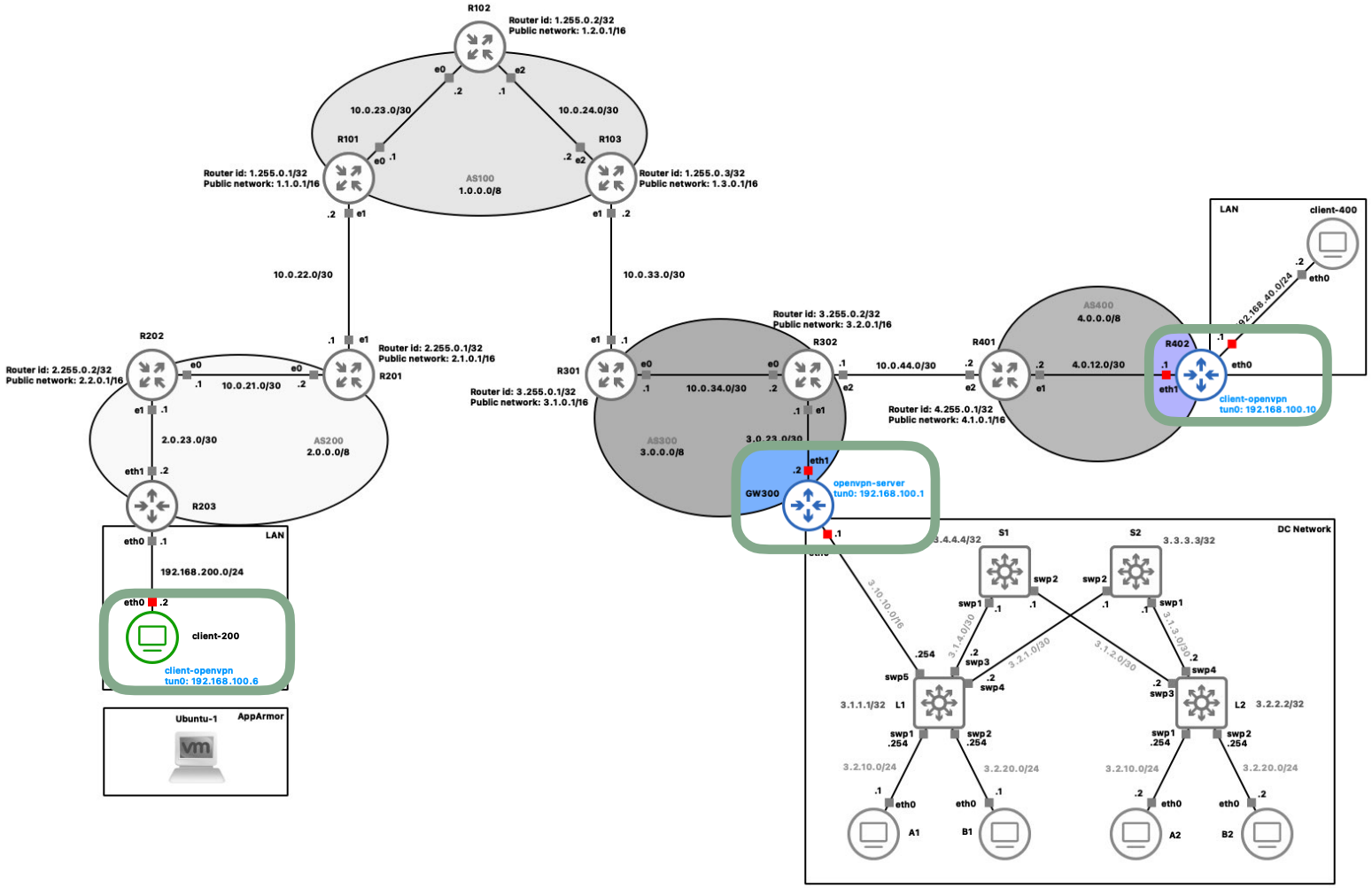
Firewall.


R102
Router id: 1.255.0.2/32
Public network: 1.2.0.1/16
e0
e2
.2
.1
10.0.23.0/30
10.0.24.0/30
pierpaolospaziani — root@R203: / — telnet 192.168.56.108 5022 — 80×24
root@R203:/# ping 2.0.23.1
PING 2.0.23.1 (2.0.23.1): 56 data bytes
ping: sending packet: Operation not permitted
root@R203:/#
R202
Router id: 2.255.0.2/32
Public network: 2.2.0.1/16
10.0.21.0/30
eth1
R203
eth0
client-200
client-openvpn
tun0: 192.168.100.6
Ubuntu-1
AppArmor
LAN
client-400
192.168.40.0/24
R402
eth1
client-openvpn
tun0: 192.168.100.10
DC Network
S2
3.3.3.3/32
swp1
swp2
swp3
swp4
3.1.3.0/30
3.1.2.0/30
L2
3.2.2.2/32
swp1 .254
swp2 .254
3.2.10.0/24
3.2.20.0/24
A1
B1
A2
B2

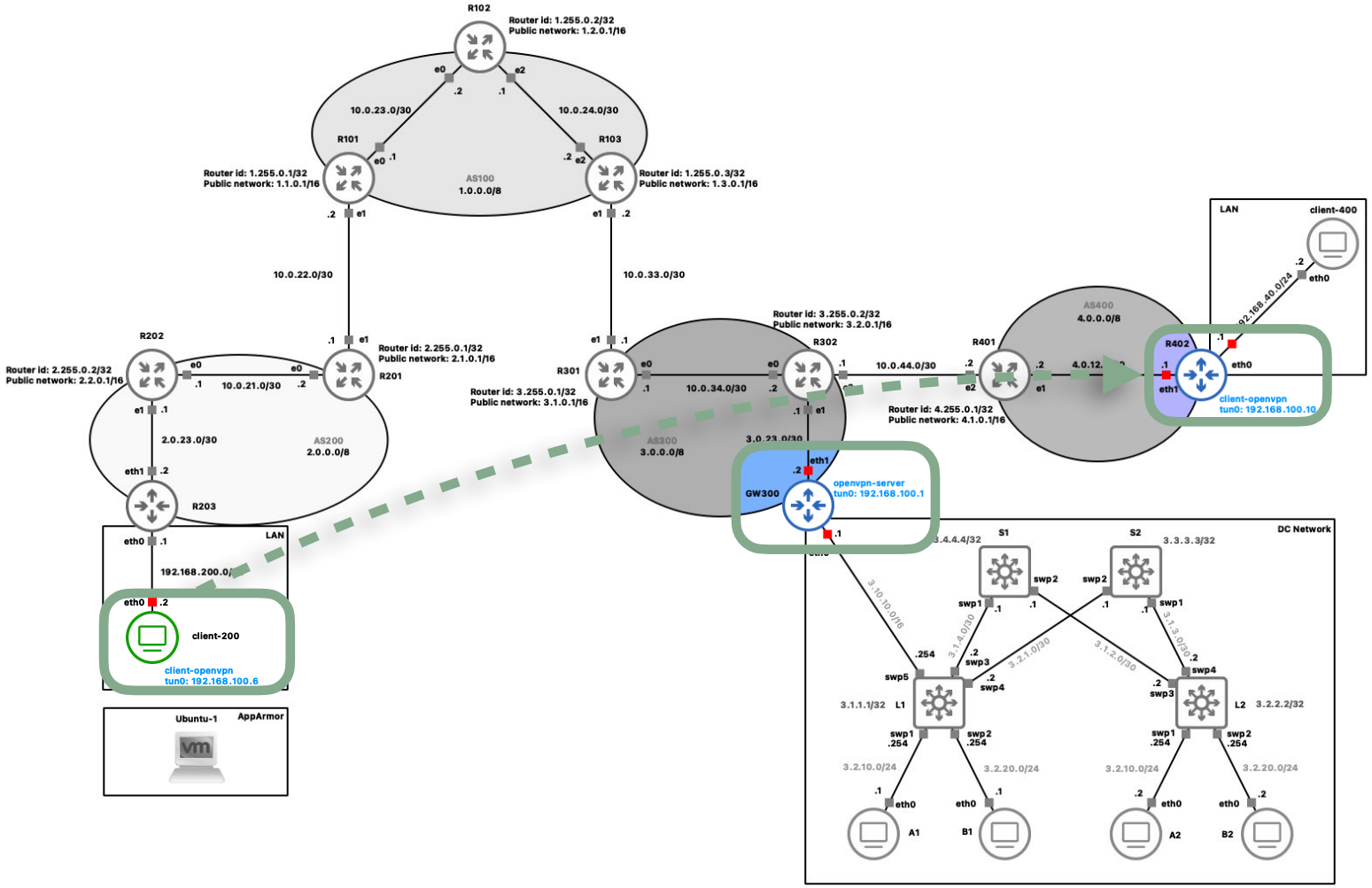
Firewall.


R102
Router id: 1.255.0.2/32
Public network: 1.2.0.1/16
e0
e2
.2
.1
10.0.23.0/30
10.0.24.0/30
pierpaolospaziani — root@client-200: ~ — telnet 192.168.56.108 5024 — 80×24
root@client-200:~# ping 2.2.0.1
PING 2.2.0.1 (2.2.0.1): 56 data bytes
64 bytes from 2.2.0.1: icmp_seq=0 ttl=63 time=0.879 ms
64 bytes from 2.2.0.1: icmp_seq=1 ttl=63 time=0.250 ms
64 bytes from 2.2.0.1: icmp_seq=2 ttl=63 time=0.375 ms
^C--- 2.2.0.1 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.250/0.501/0.879/0.272 ms
root@client-200:~#
R202
Router id: 2.255.0.2/32
Public network: 2.2.0.1/16
e0
e1
10.0.21.0/30
eth1
.2
eth0
client-200
client-openvpn
tun0: 192.168.100.6
Ubuntu-1
AppArmor
LAN
client-400
192.168.40.0/24
eth0
R402
eth1
client-openvpn
tun0: 192.168.100.10
DC Network
S2
3.3.3.3/32
swp1
swp4
swp3
L2
3.2.2.2/32
swp2
.254
3.2.10.0/24
3.2.20.0/24
A1
B1
A2
B2

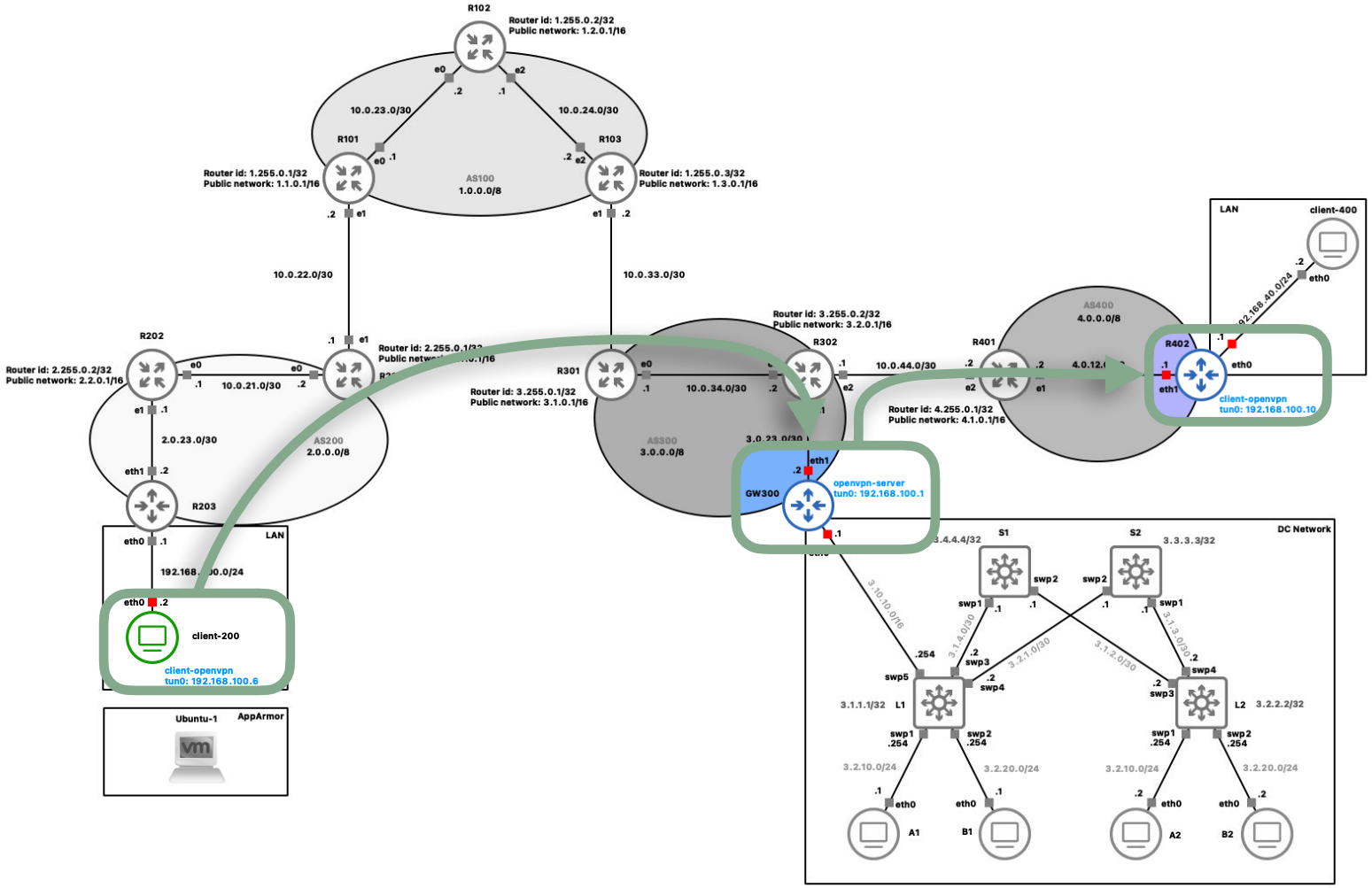
OpenVPN.


R102
Router id: 1.255.0.2/32
Public network: 1.2.0.1/16
10.0.23.0/30
10.0.24.0/30
R101
R103
Router id: 1.255.0.1/32
Public network: 1.1.0.1/16
AS100
1.0.0.0/8
Router id: 1.255.0.3/32
Public network: 1.3.0.1/16
10.0.22.0/30
10.0.33.0/30
R202
Router id: 2.255.0.2/32
Public network: 2.2.0.1/16
10.0.21.0/30
R201
Router id: 2.255.0.1/32
Public network: 2.1.0.1/16
2.0.23.0/30
AS200
2.0.0.0/8
R203
LAN
192.168.200.0/24
client-200
client-openvpn
tun0: 192.168.100.6
Ubuntu-1
AppArmor
Router id: 3.255.0.2/32
Public network: 3.2.0.1/16
R301
R302
Router id: 3.255.0.1/32
Public network: 3.1.0.1/16
10.0.34.0/30
AS300
3.0.0.0/8
3.0.23.0/30
GW300
openvpn-server
tun0: 192.168.100.1
10.0.44.0/30
R401
Router id: 4.255.0.1/32
Public network: 4.1.0.1/16
AS400
4.0.0.0/8
4.0.12.0/30
R402
LAN
client-400
192.168.40.0/24
client-openvpn
tun0: 192.168.100.10
DC Network
3.4.4.4/32
S1
3.3.3.3/32
S2
3.10.10.0/16
3.1.4.0/30
3.1.2.0/30
3.1.3.0/30
3.1.1.1/32
L1
L2
3.2.2.2/32
3.2.10.0/24
3.2.20.0/24
A1
B1
A2
B2

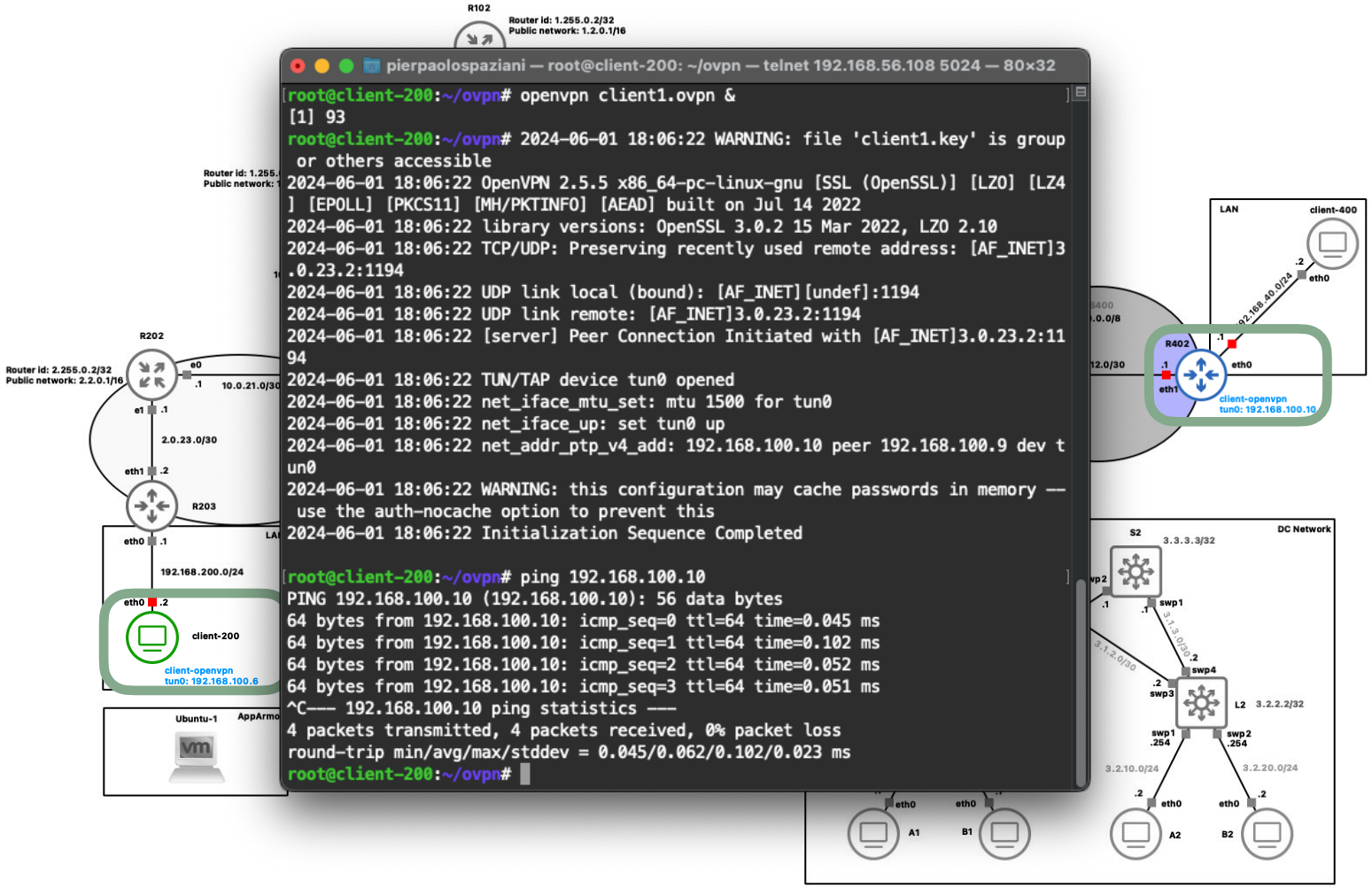
OpenVPN.


R102
Router id: 1.255.0.2/32
Public network: 1.2.0.1/16
10.0.23.0/30
10.0.24.0/30
R101
R103
Router id: 1.255.0.1/32
Public network: 1.1.0.1/16
AS100
1.0.0.0/8
Router id: 1.255.0.3/32
Public network: 1.3.0.1/16
10.0.22.0/30
10.0.33.0/30
R202
Router id: 2.255.0.2/32
Public network: 2.2.0.1/16
Router id: 2.255.0.1/32
Public network: 2.1.0.1/16
R201
10.0.21.0/30
2.0.23.0/30
AS200
2.0.0.0/8
R203
LAN
192.168.200.0/
client-200
client-openvpn
tun0: 192.168.100.6
Ubuntu-1
AppArmor
Router id: 3.255.0.2/32
Public network: 3.2.0.1/16
R301
R302
Router id: 3.255.0.1/32
Public network: 3.1.0.1/16
10.0.34.0/30
AS300
3.0.0.0/8
10.0.44.0/30
R401
Router id: 4.255.0.1/32
Public network: 4.1.0.1/16
AS400
4.0.0.0/8
LAN
client-400
R402
client-openvpn
tun0: 192.168.100.10
GW300
openvpn-server
tun0: 192.168.100.1
DC Network
S1
S2
3.3.3.3/32
swp1
swp2
swp3
swp4
swp5
3.1.1.1/32
L1
L2
3.2.2.2/32
3.2.10.0/24
3.2.20.0/24
A1
B1
A2
B2

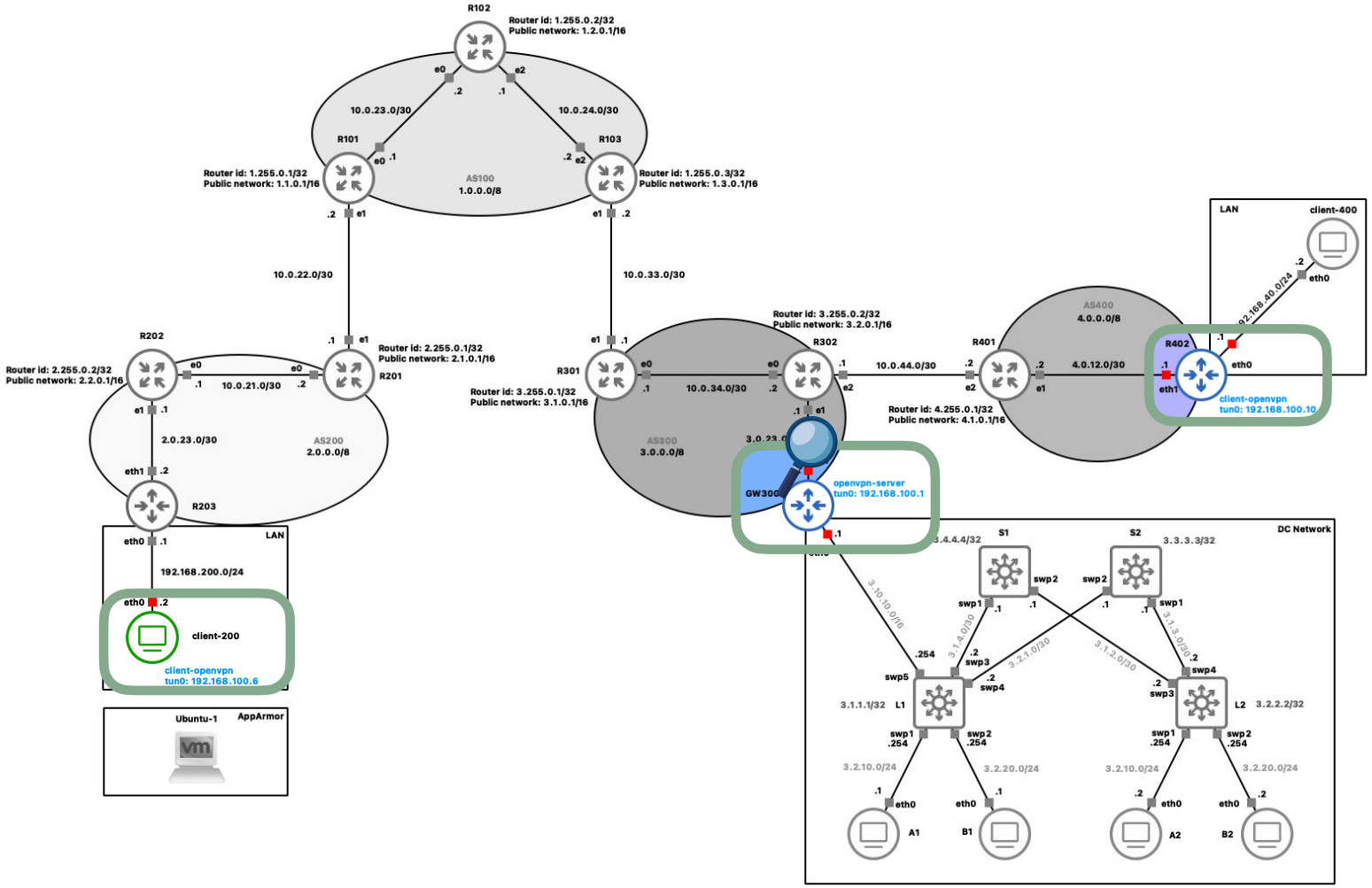
OpenVPN.


R102
Router id: 1.255.0.2/32
Public network: 1.2.0.1/16
10.0.23.0/30
10.0.24.0/30
R101
R103
Router id: 1.255.0.1/32
Public network: 1.1.0.1/16
AS100
1.0.0.0/8
Router id: 1.255.0.3/32
Public network: 1.3.0.1/16
10.0.22.0/30
10.0.33.0/30
R202
Router id: 2.255.0.2/32
Public network: 2.2.0.1/16
10.0.21.0/30
2.0.23.0/30
AS200
2.0.0.0/8
R203
LAN
client-200
client-openvpn
tun0: 192.168.100.6
Ubuntu-1
AppArmor
Router id: 3.255.0.2/32
Public network: 3.2.0.1/16
R301
R302
Router id: 3.255.0.1/32
Public network: 3.1.0.1/16
10.0.34.0/30
AS300
3.0.0.0/8
GW300
openvpn-server
tun0: 192.168.100.1
R401
10.0.44.0/30
Router id: 4.255.0.1/32
Public network: 4.1.0.1/16
AS400
4.0.0.0/8
R402
LAN
client-400
client-openvpn
tun0: 192.168.100.10
DC Network
S1
S2
3.4.4.4/32
3.3.3.3/32
3.10.10.0/16
3.1.4.0/30
3.2.1.0/30
3.1.2.0/30
3.1.3.0/30
3.1.1.1/32
L1
L2
3.2.2.2/32
3.2.10.0/24
3.2.20.0/24
A1
B1
A2
B2

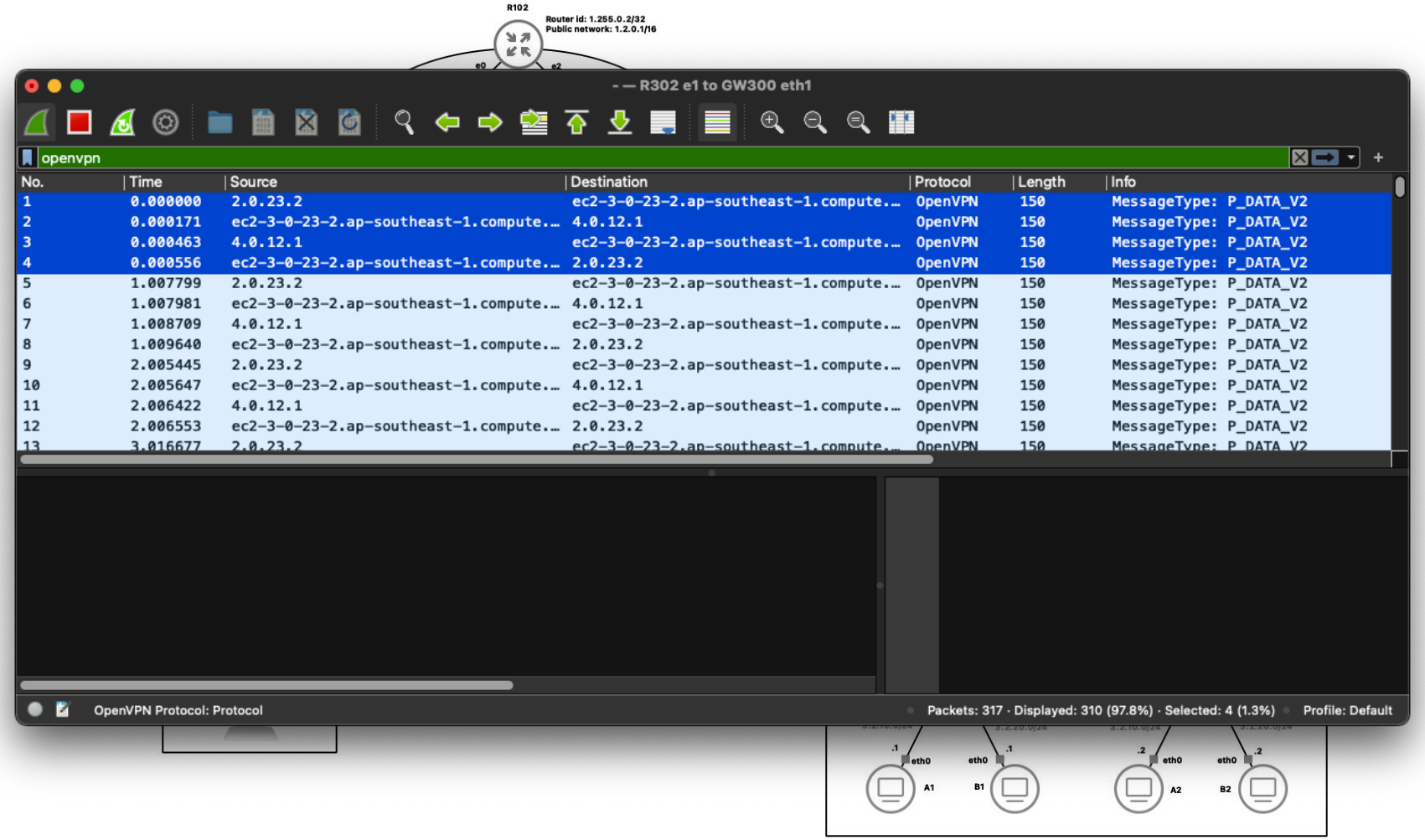
OpenVPN.


pierpaolospaziani — root@client-200: ~/ovpn — telnet 192.168.56.108 5024 — 80×32
root@client-200:~/ovpn# openvpn client1.ovpn &
[1] 93
root@client-200:~/ovpn# 2024-06-01 18:06:22 WARNING: file 'client1.key' is group or others accessible
2024-06-01 18:06:22 OpenVPN 2.5.5 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] built on Jul 14 2022
2024-06-01 18:06:22 library versions: OpenSSL 3.0.2 15 Mar 2022, LZO 2.10
2024-06-01 18:06:22 TCP/UDP: Preserving recently used remote address: [AF_INET]3.0.23.2:1194
2024-06-01 18:06:22 UDP link local (bound): [AF_INET][undef]:1194
2024-06-01 18:06:22 UDP link remote: [AF_INET]3.0.23.2:1194
2024-06-01 18:06:22 [server] Peer Connection Initiated with [AF_INET]3.0.23.2:1194
2024-06-01 18:06:22 TUN/TAP device tun0 opened
2024-06-01 18:06:22 net_iface_mtu_set: mtu 1500 for tun0
2024-06-01 18:06:22 net_iface_up: set tun0 up
2024-06-01 18:06:22 net_addr_ptp_v4_add: 192.168.100.10 peer 192.168.100.9 dev tun0
2024-06-01 18:06:22 WARNING: this configuration may cache passwords in memory — use the auth-nocache option to prevent this
2024-06-01 18:06:22 Initialization Sequence Completed
root@client-200:~/ovpn# ping 192.168.100.10
PING 192.168.100.10 (192.168.100.10): 56 data bytes
64 bytes from 192.168.100.10: icmp_seq=0 ttl=64 time=0.045 ms
64 bytes from 192.168.100.10: icmp_seq=1 ttl=64 time=0.102 ms
64 bytes from 192.168.100.10: icmp_seq=2 ttl=64 time=0.052 ms
64 bytes from 192.168.100.10: icmp_seq=3 ttl=64 time=0.051 ms
^C--- 192.168.100.10 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.045/0.062/0.102/0.023 ms
root@client-200:~/ovpn#
R102
Router id: 1.255.0.2/32
Public network: 1.2.0.1/16
R202
Router id: 2.255.0.2/32
Public network: 2.2.0.1/16
2.0.23.0/30
R203
192.168.200.0/24
client-200
client-openvpn
tun0: 192.168.100.6
LAN
client-400
R402
client-openvpn
tun0: 192.168.100.10
DC Network
S2
3.3.3.3/32
L2
3.2.2.2/32
3.2.10.0/24
3.2.20.0/24
A1
B1
A2
B2
Ubuntu-1

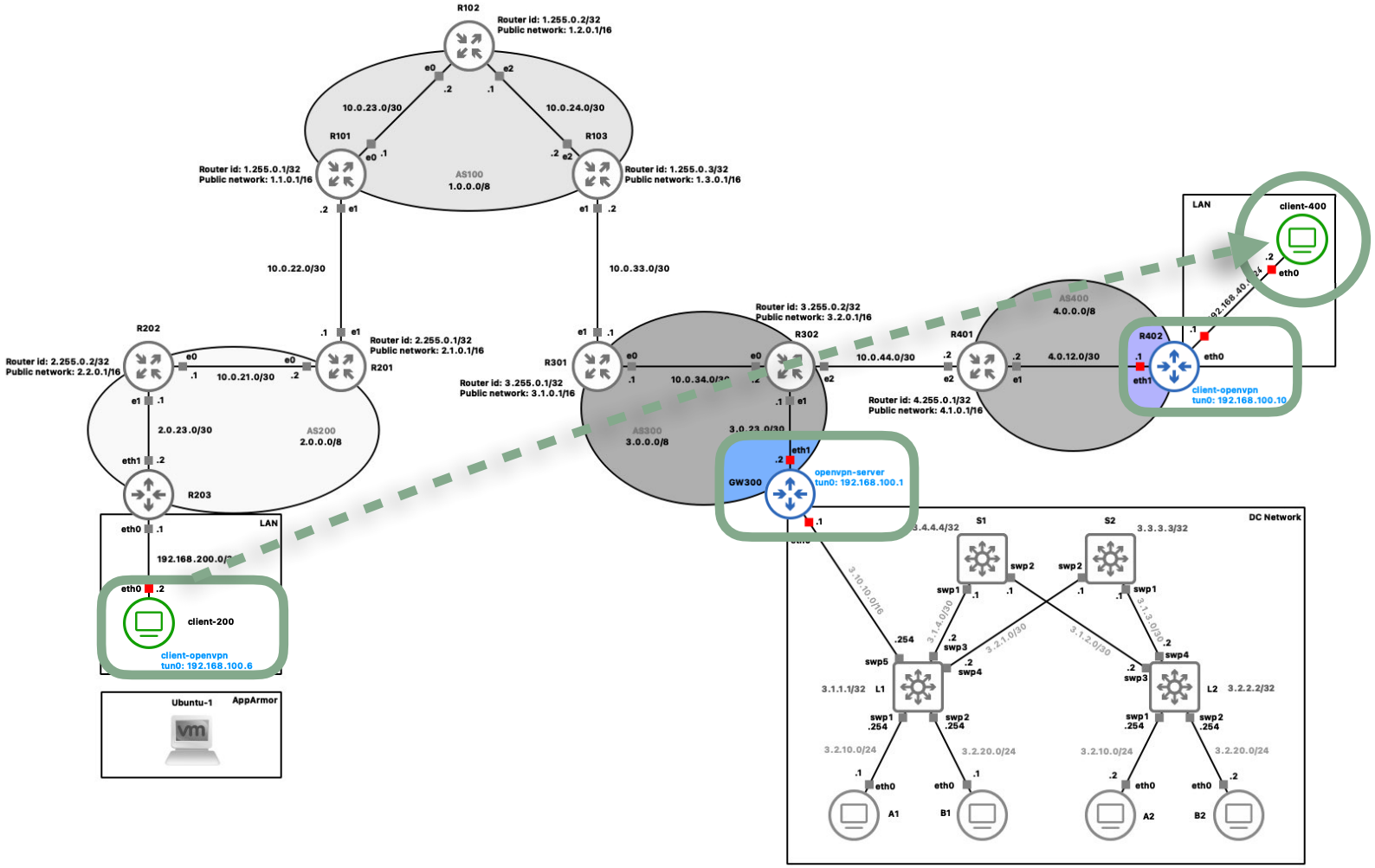
OpenVPN.


R102
Router id: 1.255.0.2/32
Public network: 1.2.0.1/16
10.0.23.0/30
10.0.24.0/30
R101
R103
Router id: 1.255.0.1/32
Public network: 1.1.0.1/16
AS100
1.0.0.0/8
Router id: 1.255.0.3/32
Public network: 1.3.0.1/16
10.0.22.0/30
10.0.33.0/30
R202
Router id: 2.255.0.2/32
Public network: 2.2.0.1/16
10.0.21.0/30
R201
Router id: 2.255.0.1/32
Public network: 2.1.0.1/16
2.0.23.0/30
AS200
2.0.0.0/8
R203
LAN
192.168.200.0/24
client-200
client-openvpn
tun0: 192.168.100.6
Ubuntu-1
AppArmor
Router id: 3.255.0.2/32
Public network: 3.2.0.1/16
R301
R302
Router id: 3.255.0.1/32
Public network: 3.1.0.1/16
10.0.34.0/30
AS300
3.0.0.0/8
GW300
openvpn-server
tun0: 192.168.100.1
10.0.44.0/30
R401
AS400
4.0.0.0/8
4.0.12.0/30
Router id: 4.255.0.1/32
Public network: 4.1.0.1/16
R402
LAN
client-400
eth0
eth1
client-openvpn
tun0: 192.168.100.10
DC Network
S1
S2
swp1
swp2
swp3
swp4
swp5
3.10.10.0/16
3.1.4.0/30
3.1.2.0/30
3.1.3.0/30
3.1.1.1/32
L1
L2
3.2.2.2/32
3.2.10.0/24
3.2.20.0/24
A1
B1
A2
B2

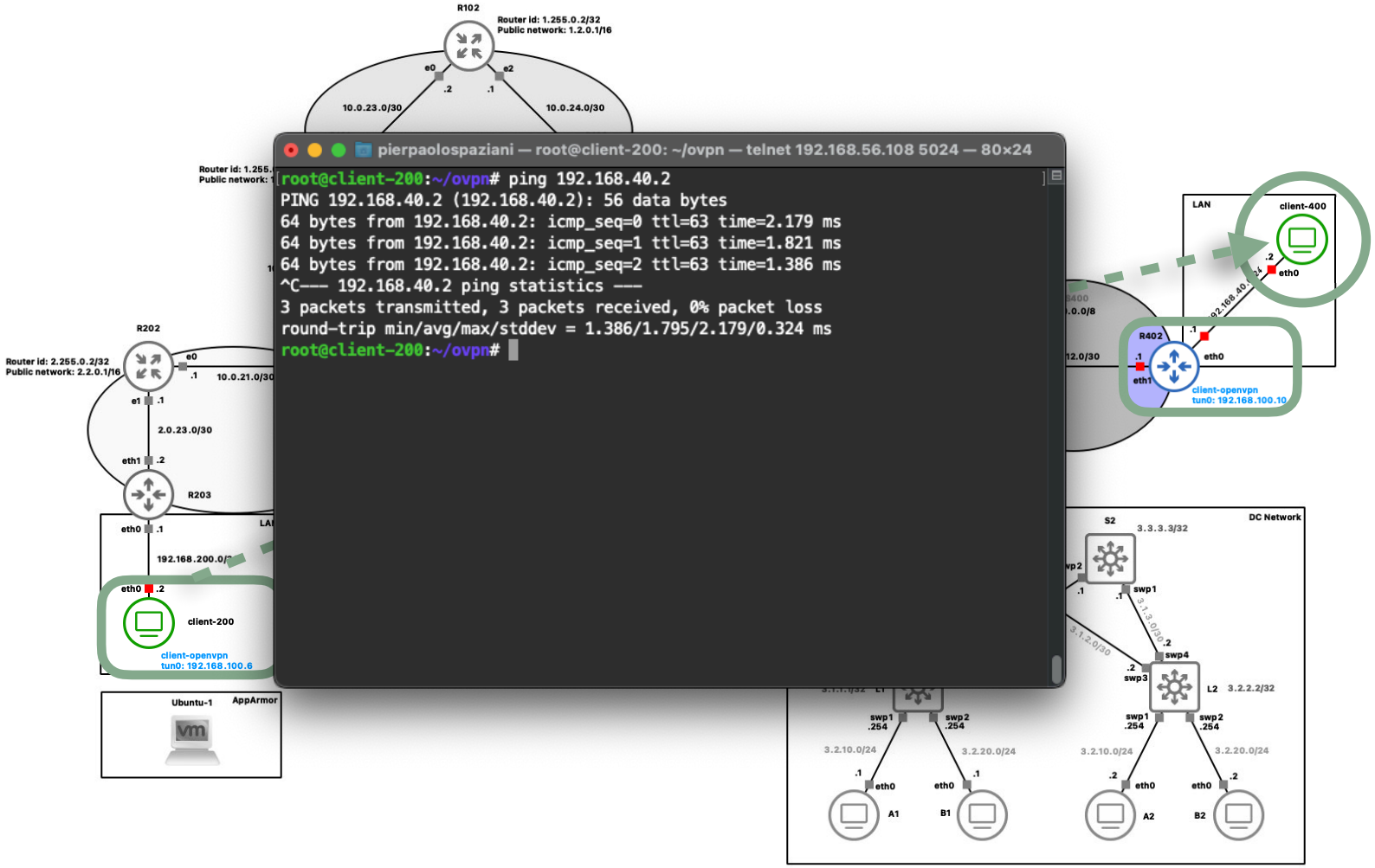
OpenVPN.


R102
Router Id: 1.255.0.2/32
Public network: 1.2.0.1/16
- — R302 e1 to GW300 eth1
openvpn
No. | Time | Source | Destination | Protocol | Length | Info
1 0.000000 2.0.23.2 ec2-3-0-23-2.ap-southeast-1.compute.… OpenVPN 150 MessageType: P_DATA_V2
2 0.000171 ec2-3-0-23-2.ap-southeast-1.compute.… 4.0.12.1 OpenVPN 150 MessageType: P_DATA_V2
3 0.000463 4.0.12.1 ec2-3-0-23-2.ap-southeast-1.compute.… OpenVPN 150 MessageType: P_DATA_V2
4 0.000556 ec2-3-0-23-2.ap-southeast-1.compute.… 2.0.23.2 OpenVPN 150 MessageType: P_DATA_V2
5 1.007799 2.0.23.2 ec2-3-0-23-2.ap-southeast-1.compute.… OpenVPN 150 MessageType: P_DATA_V2
6 1.007981 ec2-3-0-23-2.ap-southeast-1.compute.… 4.0.12.1 OpenVPN 150 MessageType: P_DATA_V2
7 1.008709 4.0.12.1 ec2-3-0-23-2.ap-southeast-1.compute.… OpenVPN 150 MessageType: P_DATA_V2
8 1.009640 ec2-3-0-23-2.ap-southeast-1.compute.… 2.0.23.2 OpenVPN 150 MessageType: P_DATA_V2
9 2.005445 2.0.23.2 ec2-3-0-23-2.ap-southeast-1.compute.… OpenVPN 150 MessageType: P_DATA_V2
10 2.005647 ec2-3-0-23-2.ap-southeast-1.compute.… 4.0.12.1 OpenVPN 150 MessageType: P_DATA_V2
11 2.006422 4.0.12.1 ec2-3-0-23-2.ap-southeast-1.compute.… OpenVPN 150 MessageType: P_DATA_V2
12 2.006553 ec2-3-0-23-2.ap-southeast-1.compute.… 2.0.23.2 OpenVPN 150 MessageType: P_DATA_V2
13 3.016677 2.0.23.2 ec2-3-0-23-2.ap-southeast-1.compute.… OpenVPN 150 MessageType: P_DATA_V2
OpenVPN Protocol: Protocol
Packets: 317 · Displayed: 310 (97.8%) · Selected: 4 (1.3%)
Profile: Default
.1
eth0
A1
eth0
.1
B1
.2
eth0
A2
eth0
.2
B2

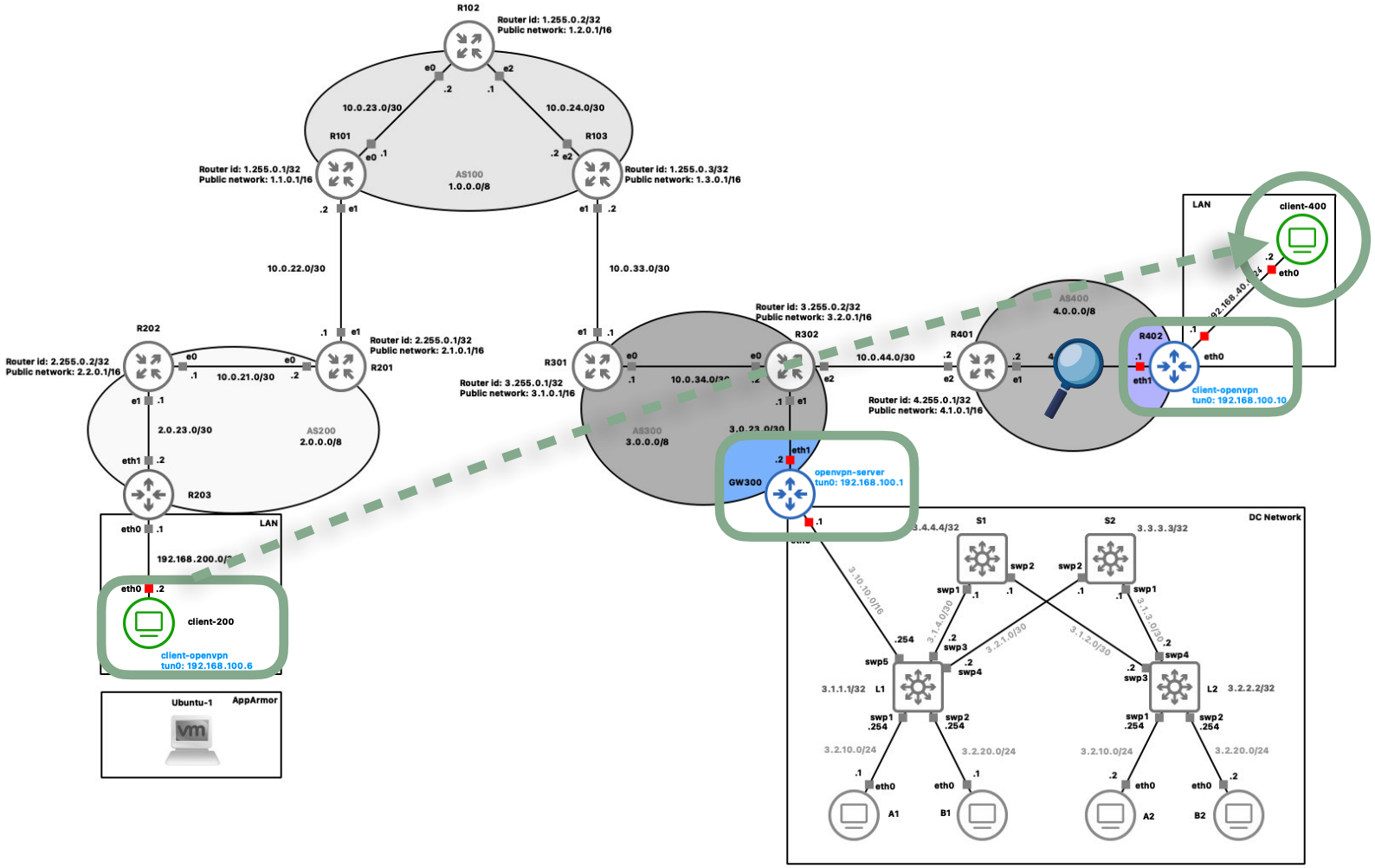
OpenVPN.


R102
Router id: 1.255.0.2/32
Public network: 1.2.0.1/16
10.0.23.0/30
10.0.24.0/30
R101
R103
Router id: 1.255.0.1/32
Public network: 1.1.0.1/16
AS100
1.0.0.0/8
Router id: 1.255.0.3/32
Public network: 1.3.0.1/16
10.0.22.0/30
10.0.33.0/30
R202
R201
Router id: 2.255.0.2/32
Public network: 2.2.0.1/16
Router id: 2.255.0.1/32
Public network: 2.1.0.1/16
10.0.21.0/30
2.0.23.0/30
AS200
2.0.0.0/8
R203
LAN
client-200
client-openvpn
tun0: 192.168.100.6
Ubuntu-1
AppArmor
R301
R302
Router id: 3.255.0.1/32
Public network: 3.1.0.1/16
Router id: 3.255.0.2/32
Public network: 3.2.0.1/16
AS300
3.0.0.0/8
GW300
openvpn-server
tun0: 192.168.100.1
R401
R402
Router id: 4.255.0.1/32
Public network: 4.1.0.1/16
10.0.44.0/30
4.0.12.0/30
AS400
4.0.0.0/8
client-400
client-openvpn
tun0: 192.168.100.10
DC Network
S1
S2
3.4.4.4/32
3.3.3.3/32
3.10.10.0/16
3.1.4.0/30
3.1.2.0/30
3.1.3.0/30
3.1.1.1/32
L1
L2
3.2.2.2/32
3.2.10.0/24
3.2.20.0/24
A1
B1
A2
B2

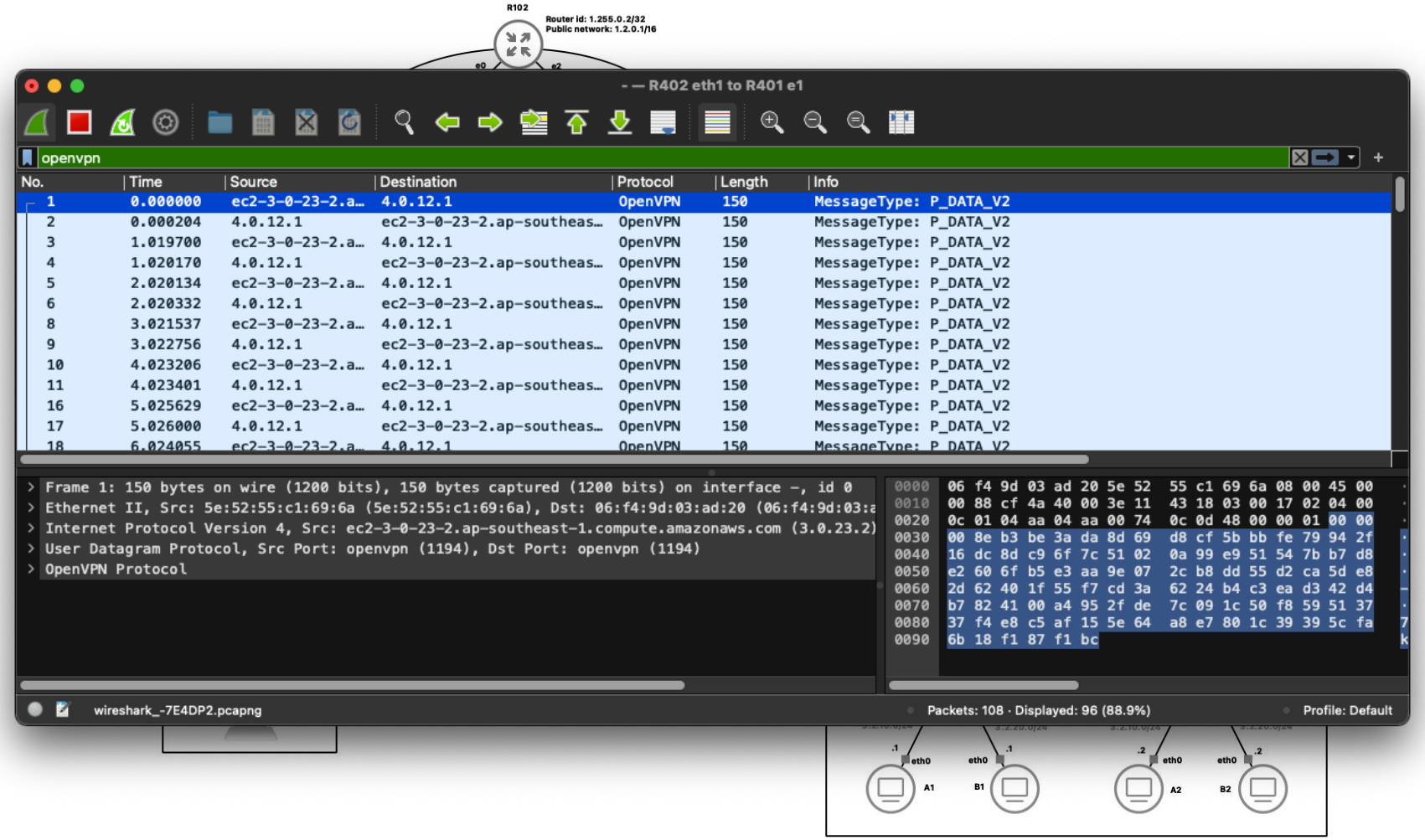
OpenVPN.


R102
Router id: 1.255.0.2/32
Public network: 1.2.0.1/16
e0
e2
.2
.1
10.0.23.0/30
10.0.24.0/30
pierpaolospaziani — root@client-200: ~/ovpn — telnet 192.168.56.108 5024 — 80×24
root@client-200:~/ovpn# ping 192.168.40.2
PING 192.168.40.2 (192.168.40.2): 56 data bytes
64 bytes from 192.168.40.2: icmp_seq=0 ttl=63 time=2.179 ms
64 bytes from 192.168.40.2: icmp_seq=1 ttl=63 time=1.821 ms
64 bytes from 192.168.40.2: icmp_seq=2 ttl=63 time=1.386 ms
^C--- 192.168.40.2 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max/stddev = 1.386/1.795/2.179/0.324 ms
root@client-200:~/ovpn#
R202
Router id: 2.255.0.2/32
Public network: 2.2.0.1/16
e0
.1
10.0.21.0/30
e1
.1
2.0.23.0/30
eth1
.2
R203
eth0
.1
192.168.200.0/
eth0
.2
client-200
client-openvpn
tun0: 192.168.100.6
Ubuntu-1
AppArmor
vm
LAN
client-400
.2
eth0
R402
.1
eth0
eth1
client-openvpn
tun0: 192.168.100.10
DC Network
S2
3.3.3.3/32
swp1
swp4
swp3
L2
3.2.2.2/32
swp1
.254
swp2
.254
3.2.10.0/24
3.2.20.0/24
eth0
A1
B1
A2
B2

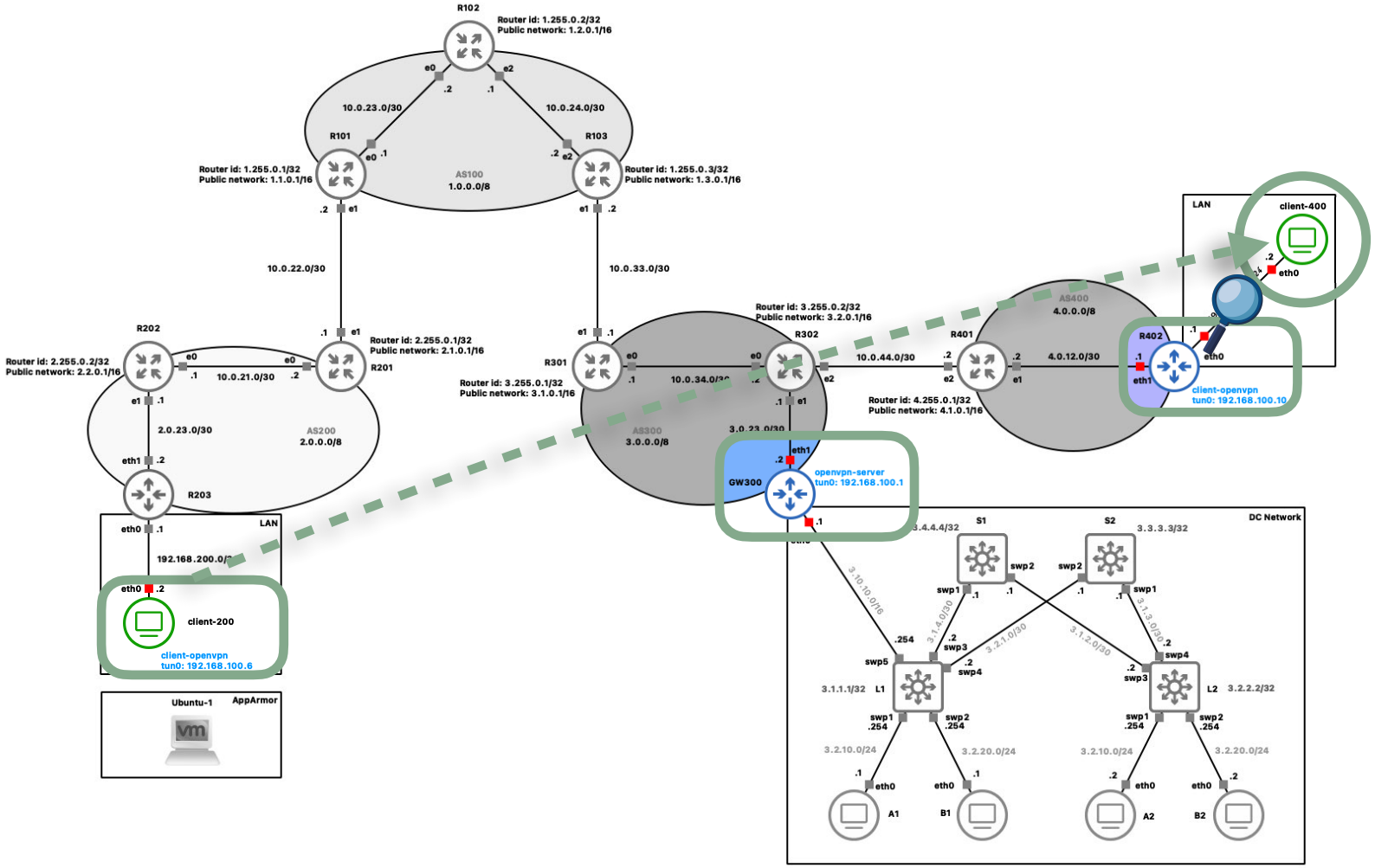
OpenVPN.


R102
Router id: 1.255.0.2/32
Public network: 1.2.0.1/16
10.0.23.0/30
10.0.24.0/30
R101
R103
Router id: 1.255.0.1/32
Public network: 1.1.0.1/16
AS100
1.0.0.0/8
Router id: 1.255.0.3/32
Public network: 1.3.0.1/16
10.0.22.0/30
10.0.33.0/30
R202
R201
Router id: 2.255.0.2/32
Public network: 2.2.0.1/16
Router id: 2.255.0.1/32
Public network: 2.1.0.1/16
10.0.21.0/30
2.0.23.0/30
AS200
2.0.0.0/8
R203
LAN
client-200
client-openvpn
tun0: 192.168.100.6
Ubuntu-1
AppArmor
R301
R302
Router id: 3.255.0.2/32
Public network: 3.2.0.1/16
Router id: 3.255.0.1/32
Public network: 3.1.0.1/16
AS300
3.0.0.0/8
GW300
openvpn-server
tun0: 192.168.100.1
R401
10.0.44.0/30
AS400
4.0.0.0/8
Router id: 4.255.0.1/32
Public network: 4.1.0.1/16
R402
LAN
client-400
client-openvpn
tun0: 192.168.100.10
DC Network
S1
S2
3.4.4.4/32
3.3.3.3/32
3.10.10.0/16
3.1.4.0/30
3.2.1.0/30
3.1.2.0/30
3.1.3.0/30
3.1.1.1/32
L1
L2
3.2.2.2/32
3.2.10.0/24
3.2.20.0/24
A1
B1
A2
B2

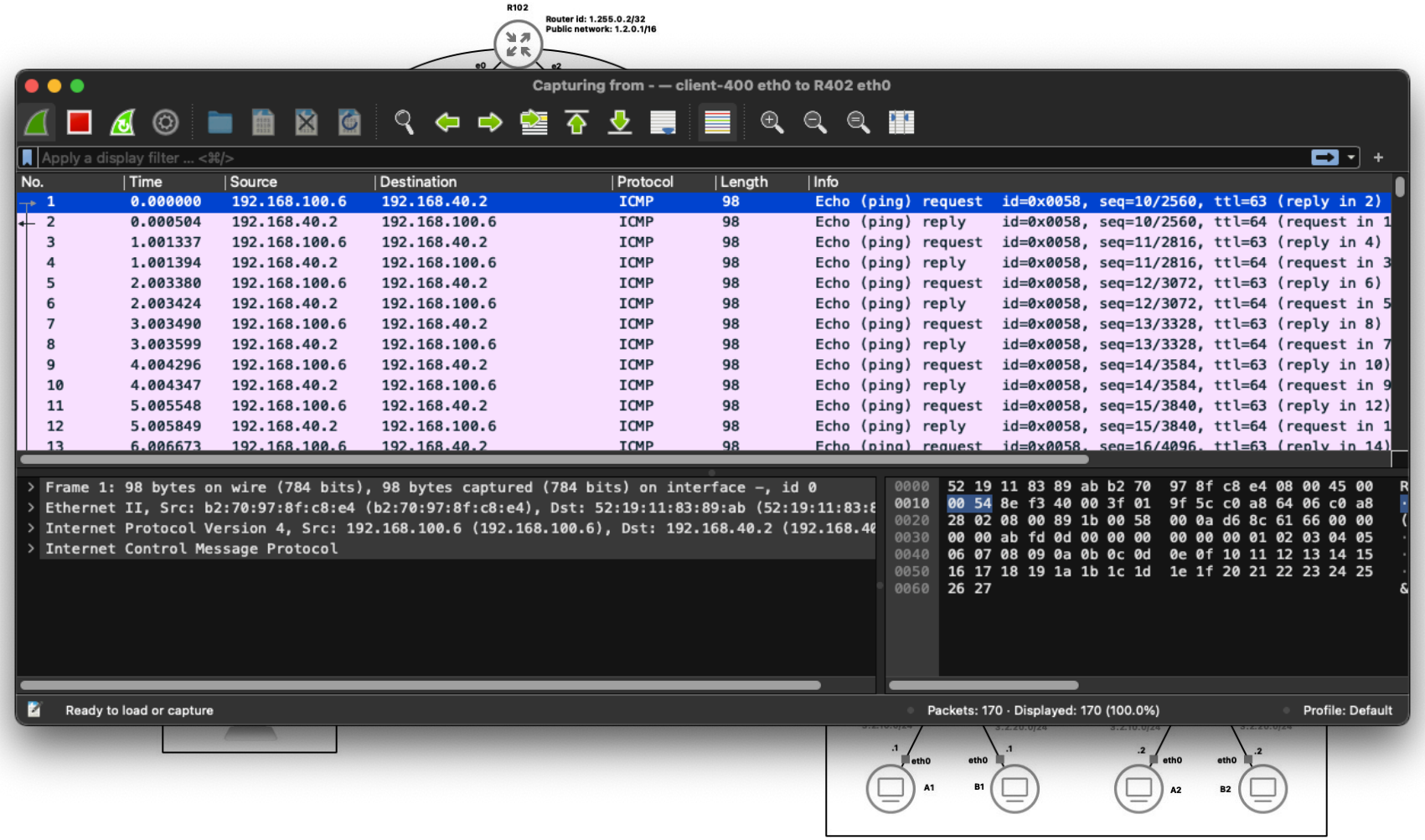
OpenVPN.


R102
Router Id: 1.255.0.2/32
Public network: 1.2.0.1/16
- — R402 eth1 to R401 e1
openvpn
No. | Time | Source | Destination | Protocol | Length | Info
1 0.000000 ec2-3-0-23-2.a… 4.0.12.1 OpenVPN 150 MessageType: P_DATA_V2
2 0.000204 4.0.12.1 ec2-3-0-23-2.ap-southeas… OpenVPN 150 MessageType: P_DATA_V2
3 1.019700 ec2-3-0-23-2.a… 4.0.12.1 OpenVPN 150 MessageType: P_DATA_V2
4 1.020170 4.0.12.1 ec2-3-0-23-2.ap-southeas… OpenVPN 150 MessageType: P_DATA_V2
5 2.020134 ec2-3-0-23-2.a… 4.0.12.1 OpenVPN 150 MessageType: P_DATA_V2
6 2.020332 4.0.12.1 ec2-3-0-23-2.ap-southeas… OpenVPN 150 MessageType: P_DATA_V2
8 3.021537 ec2-3-0-23-2.a… 4.0.12.1 OpenVPN 150 MessageType: P_DATA_V2
9 3.022756 4.0.12.1 ec2-3-0-23-2.ap-southeas… OpenVPN 150 MessageType: P_DATA_V2
10 4.023206 ec2-3-0-23-2.a… 4.0.12.1 OpenVPN 150 MessageType: P_DATA_V2
11 4.023401 4.0.12.1 ec2-3-0-23-2.ap-southeas… OpenVPN 150 MessageType: P_DATA_V2
16 5.025629 ec2-3-0-23-2.a… 4.0.12.1 OpenVPN 150 MessageType: P_DATA_V2
17 5.026000 4.0.12.1 ec2-3-0-23-2.ap-southeas… 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: 5e:52:55:c1:69:6a (5e:52:55:c1:69:6a), Dst: 06:f4:9d:03:ad:20 (06:f4:9d:03:a
Internet Protocol Version 4, Src: ec2-3-0-23-2.ap-southeast-1.compute.amazonaws.com (3.0.23.2)
User Datagram Protocol, Src Port: openvpn (1194), Dst Port: openvpn (1194)
OpenVPN Protocol
0000 06 f4 9d 03 ad 20 5e 52 55 c1 69 6a 08 00 45 00
0010 00 88 cf 4a 40 00 3e 11 43 18 03 00 17 02 04 00
0020 0c 01 04 aa 04 aa 00 74 0c 0d 48 00 00 01 00 00
0030 00 8e b3 be 3a da 8d 69 d8 cf 5b bb fe 79 94 2f
0040 16 dc 8d c9 6f 7c 51 02 0a 99 e9 51 54 7b b7 d8
0050 e2 60 6f b5 e3 aa 9e 07 2c b8 dd 55 d2 ca 5d e8
0060 2d 62 40 1f 55 f7 cd 3a 62 24 b4 c3 ea d3 42 d4
0070 b7 82 41 00 a4 95 2f de 7c 09 1c 50 f8 59 51 37
0080 37 f4 e8 c5 af 15 5e 64 a8 e7 80 1c 39 39 5c fa
0090 6b 18 f1 87 f1 bc
wireshark_-7E4DP2.pcapng
Packets: 108 · Displayed: 96 (88.9%)
Profile: Default
.1
eth0
A1
eth0
.1
B1
.2
eth0
A2
eth0
.2
B2

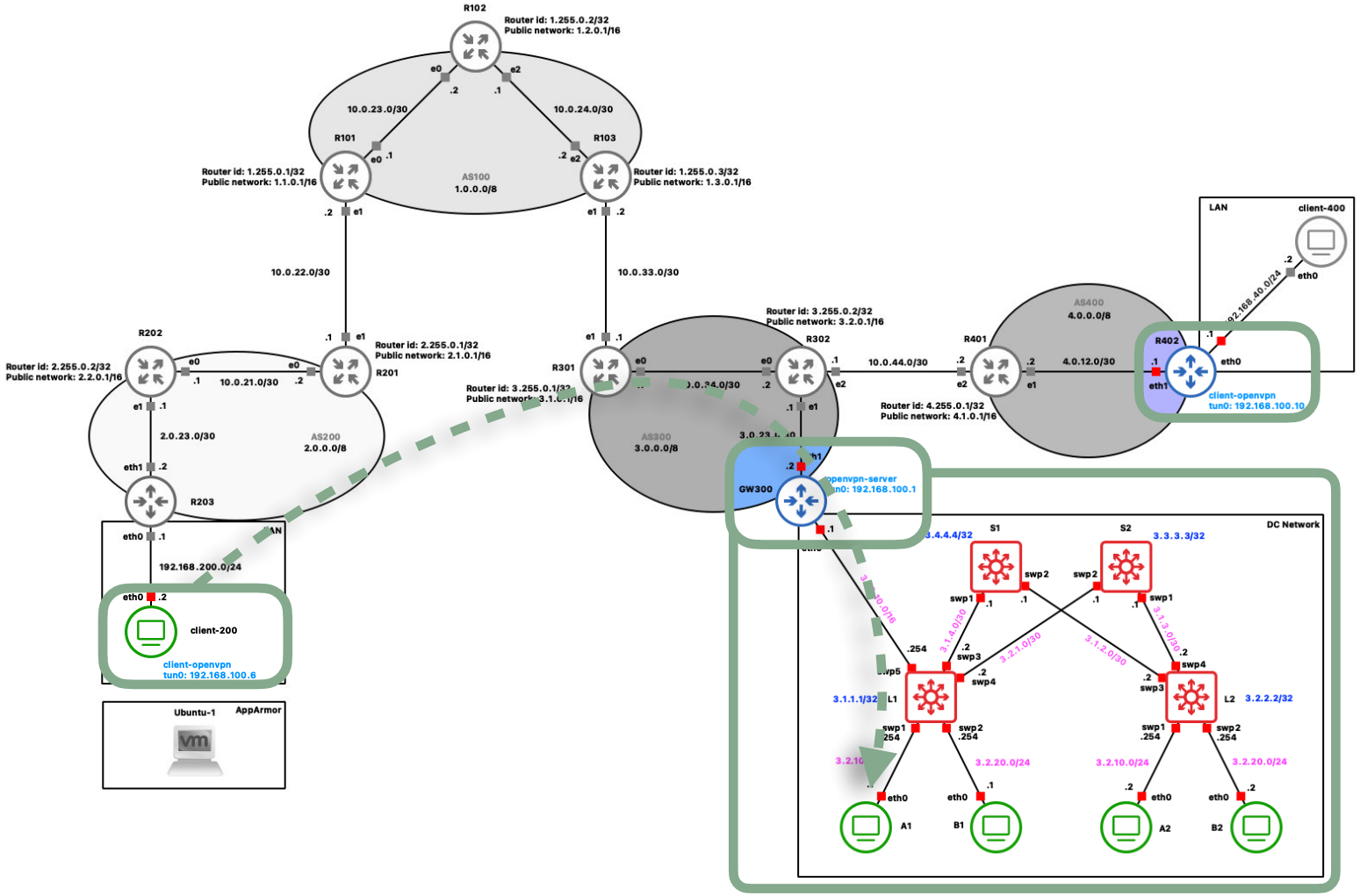
OpenVPN.


R102
Router id: 1.255.0.2/32
Public network: 1.2.0.1/16
e0
e2
.2
.1
10.0.23.0/30
10.0.24.0/30
R101
R103
e0 .1
.2 e2
Router id: 1.255.0.1/32
Public network: 1.1.0.1/16
AS100
1.0.0.0/8
Router id: 1.255.0.3/32
Public network: 1.3.0.1/16
.2 e1
e1 .2
10.0.22.0/30
10.0.33.0/30
R202
.1 e1
Router id: 2.255.0.1/32
Public network: 2.1.0.1/16
Router id: 2.255.0.2/32
Public network: 2.2.0.1/16
e0
e0
.1
10.0.21.0/30
.2
R201
e1 .1
2.0.23.0/30
AS200
2.0.0.0/8
eth1 .2
R203
eth0 .1
LAN
192.168.200.0/
eth0 .2
client-200
client-openvpn
tun0: 192.168.100.6
Ubuntu-1
AppArmor
vm
Router id: 3.255.0.2/32
Public network: 3.2.0.1/16
R301
e1 .1
Router id: 3.255.0.1/32
Public network: 3.1.0.1/16
e0
e0
.1
10.0.34.0/30
.2
R302
.1 e1
AS300
3.0.0.0/8
3.0.23.0/30
eth1
.2
GW300
openvpn-server
tun0: 192.168.100.1
.1
10.0.44.0/30
.2
e2
R401
e2
.2
e1
4.0.12.0/30
Router id: 4.255.0.1/32
Public network: 4.1.0.1/16
AS400
4.0.0.0/8
R402
.1
eth1
.1
eth0
client-openvpn
tun0: 192.168.100.10
LAN
client-400
.2
eth0
DC Network
3.4.4.4/32
S1
S2
3.3.3.3/32
swp2
swp2
swp1
.1
.1
.1
.1
swp1
3.10.10.0/16
3.1.4.0/30
3.2.1.0/30
3.1.2.0/30
3.1.3.0/30
.254
.2
swp3
.2
swp4
swp5
.2
swp3
.2
swp4
3.1.1.1/32
L1
L2
3.2.2.2/32
swp1
.254
swp2
.254
swp1
.254
swp2
.254
3.2.10.0/24
3.2.20.0/24
3.2.10.0/24
3.2.20.0/24
.1
eth0
eth0
.1
.2
eth0
eth0
.2
A1
B1
A2
B2

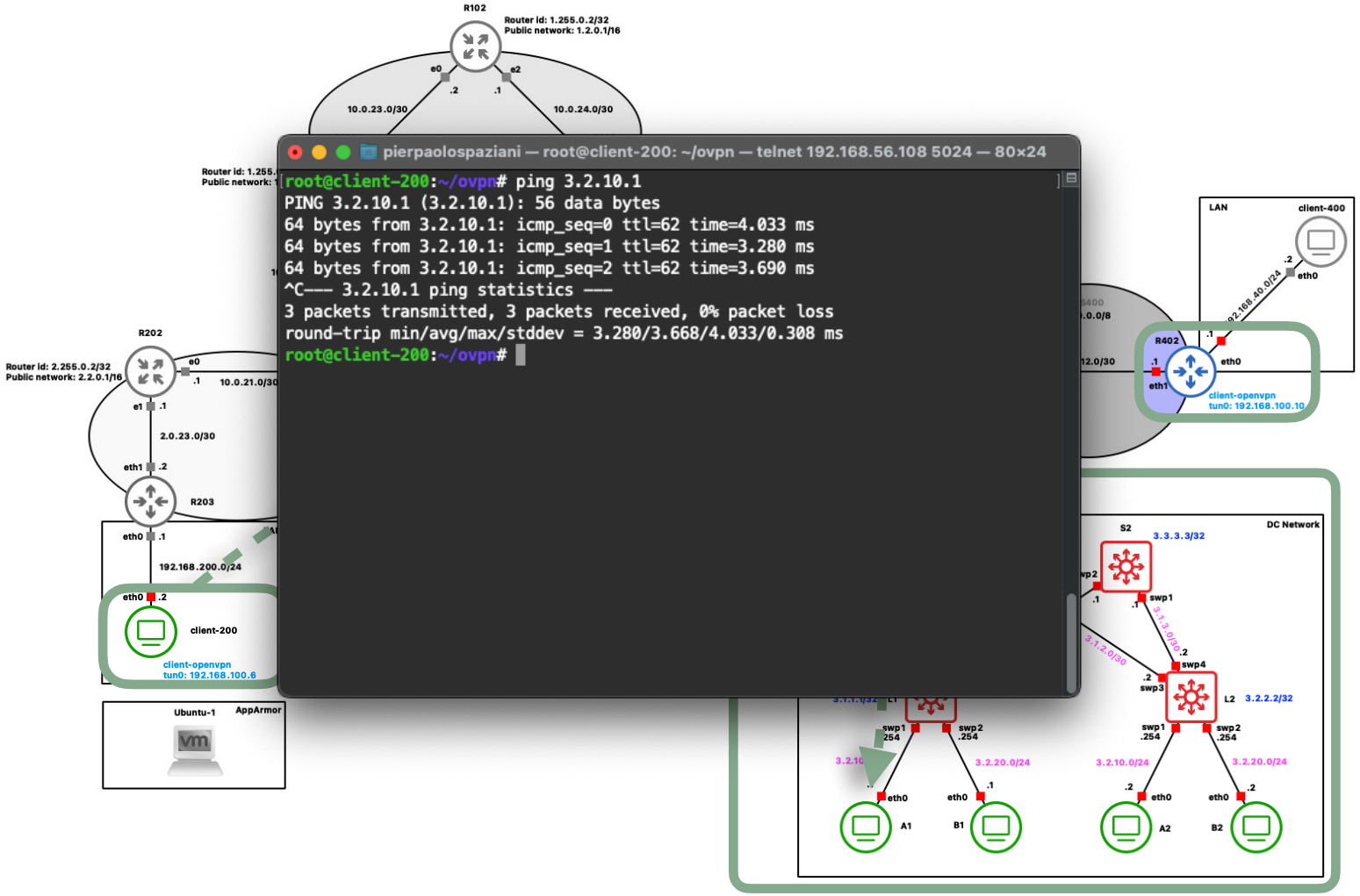
OpenVPN.


R102
Router Id: 1.255.0.2/32
Public network: 1.2.0.1/16
Capturing from - — client-400 eth0 to R402 eth0
Apply a display filter ... <⌘/>
No. Time Source Destination Protocol Length Info
1 0.000000 192.168.100.6 192.168.40.2 ICMP 98 Echo (ping) request id=0x0058, seq=10/2560, ttl=63 (reply in 2)
2 0.000504 192.168.40.2 192.168.100.6 ICMP 98 Echo (ping) reply id=0x0058, seq=10/2560, ttl=64 (request in 1
3 1.001337 192.168.100.6 192.168.40.2 ICMP 98 Echo (ping) request id=0x0058, seq=11/2816, ttl=63 (reply in 4)
4 1.001394 192.168.40.2 192.168.100.6 ICMP 98 Echo (ping) reply id=0x0058, seq=11/2816, ttl=64 (request in 3
5 2.003380 192.168.100.6 192.168.40.2 ICMP 98 Echo (ping) request id=0x0058, seq=12/3072, ttl=63 (reply in 6)
6 2.003424 192.168.40.2 192.168.100.6 ICMP 98 Echo (ping) reply id=0x0058, seq=12/3072, ttl=64 (request in 5
7 3.003490 192.168.100.6 192.168.40.2 ICMP 98 Echo (ping) request id=0x0058, seq=13/3328, ttl=63 (reply in 8)
8 3.003599 192.168.40.2 192.168.100.6 ICMP 98 Echo (ping) reply id=0x0058, seq=13/3328, ttl=64 (request in 7
9 4.004296 192.168.100.6 192.168.40.2 ICMP 98 Echo (ping) request id=0x0058, seq=14/3584, ttl=63 (reply in 10)
10 4.004347 192.168.40.2 192.168.100.6 ICMP 98 Echo (ping) reply id=0x0058, seq=14/3584, ttl=64 (request in 9
11 5.005548 192.168.100.6 192.168.40.2 ICMP 98 Echo (ping) request id=0x0058, seq=15/3840, ttl=63 (reply in 12)
12 5.005849 192.168.40.2 192.168.100.6 ICMP 98 Echo (ping) reply id=0x0058, seq=15/3840, ttl=64 (request in 1
13 6.006673 192.168.100.6 192.168.40.2 ICMP 98 Echo (ping) request id=0x0058, seq=16/4096, ttl=63 (reply in 14)
Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface –, id 0
Ethernet II, Src: b2:70:97:8f:c8:e4 (b2:70:97:8f:c8:e4), Dst: 52:19:11:83:89:ab (52:19:11:83:8
Internet Protocol Version 4, Src: 192.168.100.6 (192.168.100.6), Dst: 192.168.40.2 (192.168.40
Internet Control Message Protocol
0000 52 19 11 83 89 ab b2 70 97 8f c8 e4 08 00 45 00
0010 00 54 8e f3 40 00 3f 01 9f 5c c0 a8 64 06 c0 a8
0020 28 02 08 00 89 1b 00 58 00 0a d6 8c 61 66 00 00
0030 00 00 ab fd 0d 00 00 00 00 00 00 01 02 03 04 05
0040 06 07 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15
0050 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25
0060 26 27
Ready to load or capture
Packets: 170 · Displayed: 170 (100.0%)
Profile: Default
.1 eth0 A1
eth0 .1 B1
.2 eth0 A2
eth0 .2 B2

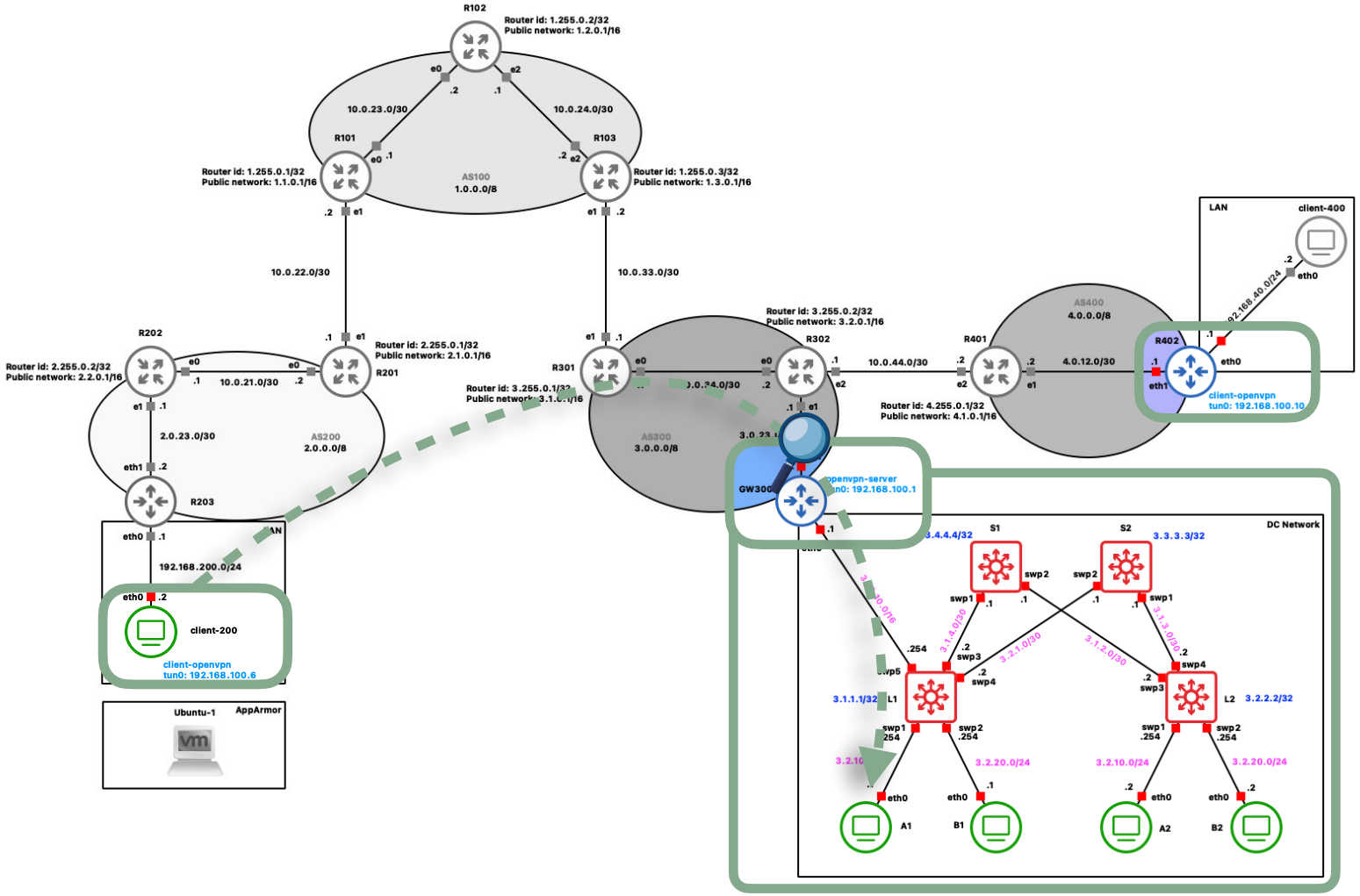
OpenVPN.


R102
Router id: 1.255.0.2/32
Public network: 1.2.0.1/16
10.0.23.0/30
10.0.24.0/30
R101
R103
Router id: 1.255.0.1/32
Public network: 1.1.0.1/16
AS100
1.0.0.0/8
Router id: 1.255.0.3/32
Public network: 1.3.0.1/16
10.0.22.0/30
10.0.33.0/30
R202
Router id: 2.255.0.2/32
Public network: 2.2.0.1/16
Router id: 2.255.0.1/32
Public network: 2.1.0.1/16
R201
10.0.21.0/30
2.0.23.0/30
AS200
2.0.0.0/8
R203
192.168.200.0/24
client-200
client-openvpn
tun0: 192.168.100.6
Ubuntu-1
AppArmor
R301
Router id: 3.255.0.1/32
Public network: 3.1.0.1/16
Router id: 3.255.0.2/32
Public network: 3.2.0.1/16
R302
AS300
3.0.0.0/8
10.0.44.0/30
R401
AS400
4.0.0.0/8
4.0.12.0/30
Router id: 4.255.0.1/32
Public network: 4.1.0.1/16
LAN
client-400
R402
client-openvpn
tun0: 192.168.100.10
GW300
openvpn-server
tun0: 192.168.100.1
DC Network
S1
S2
3.4.4.4/32
3.3.3.3/32
swp1
swp2
swp3
swp4
swp5
3.1.1.1/32
L1
L2
3.2.2.2/32
3.2.20.0/24
3.2.10.0/24
A1
B1
A2
B2
eth0

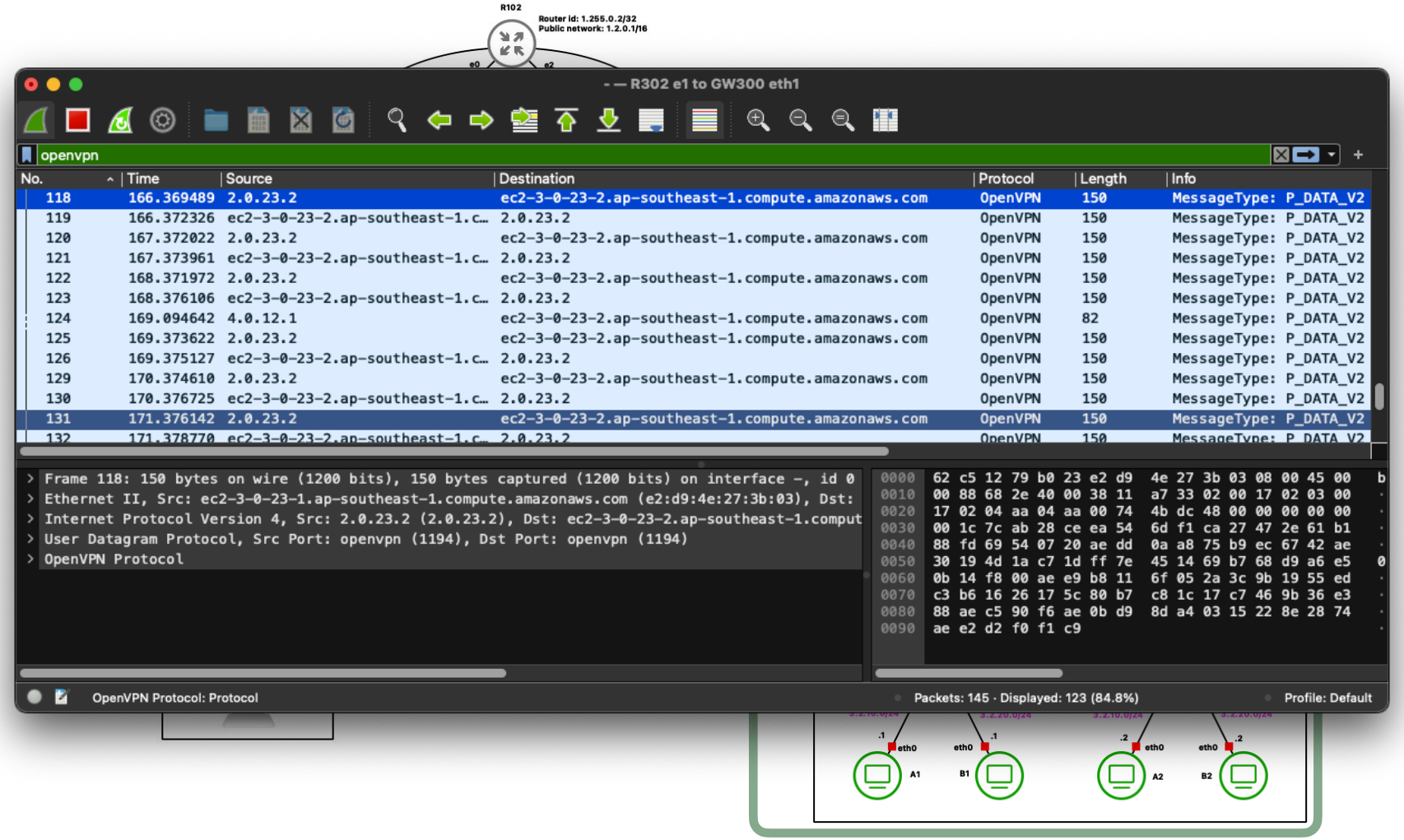
OpenVPN.


R102
Router id: 1.255.0.2/32
Public network: 1.2.0.1/16
e0
e2
.2
.1
10.0.23.0/30
10.0.24.0/30
pierpaolospaziani — root@client-200: ~/ovpn — telnet 192.168.56.108 5024 — 80×24
root@client-200:~/ovpn# ping 3.2.10.1
PING 3.2.10.1 (3.2.10.1): 56 data bytes
64 bytes from 3.2.10.1: icmp_seq=0 ttl=62 time=4.033 ms
64 bytes from 3.2.10.1: icmp_seq=1 ttl=62 time=3.280 ms
64 bytes from 3.2.10.1: icmp_seq=2 ttl=62 time=3.690 ms
^C--- 3.2.10.1 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max/stddev = 3.280/3.668/4.033/0.308 ms
root@client-200:~/ovpn#
R202
Router id: 2.255.0.2/32
Public network: 2.2.0.1/16
e0
.1
10.0.21.0/30
e1
.1
2.0.23.0/30
eth1
.2
R203
eth0
.1
192.168.200.0/24
eth0
.2
client-200
client-openvpn
tun0: 192.168.100.6
Ubuntu-1
AppArmor
vm
LAN
client-400
.2
eth0
R402
.1
eth0
eth1
client-openvpn
tun0: 192.168.100.10
DC Network
S2
3.3.3.3/32
swp1
swp4
swp3
L2
3.2.2.2/32
swp1
.254
swp2
.254
3.2.20.0/24
3.2.10.0/24
eth0
A1
B1
A2
B2

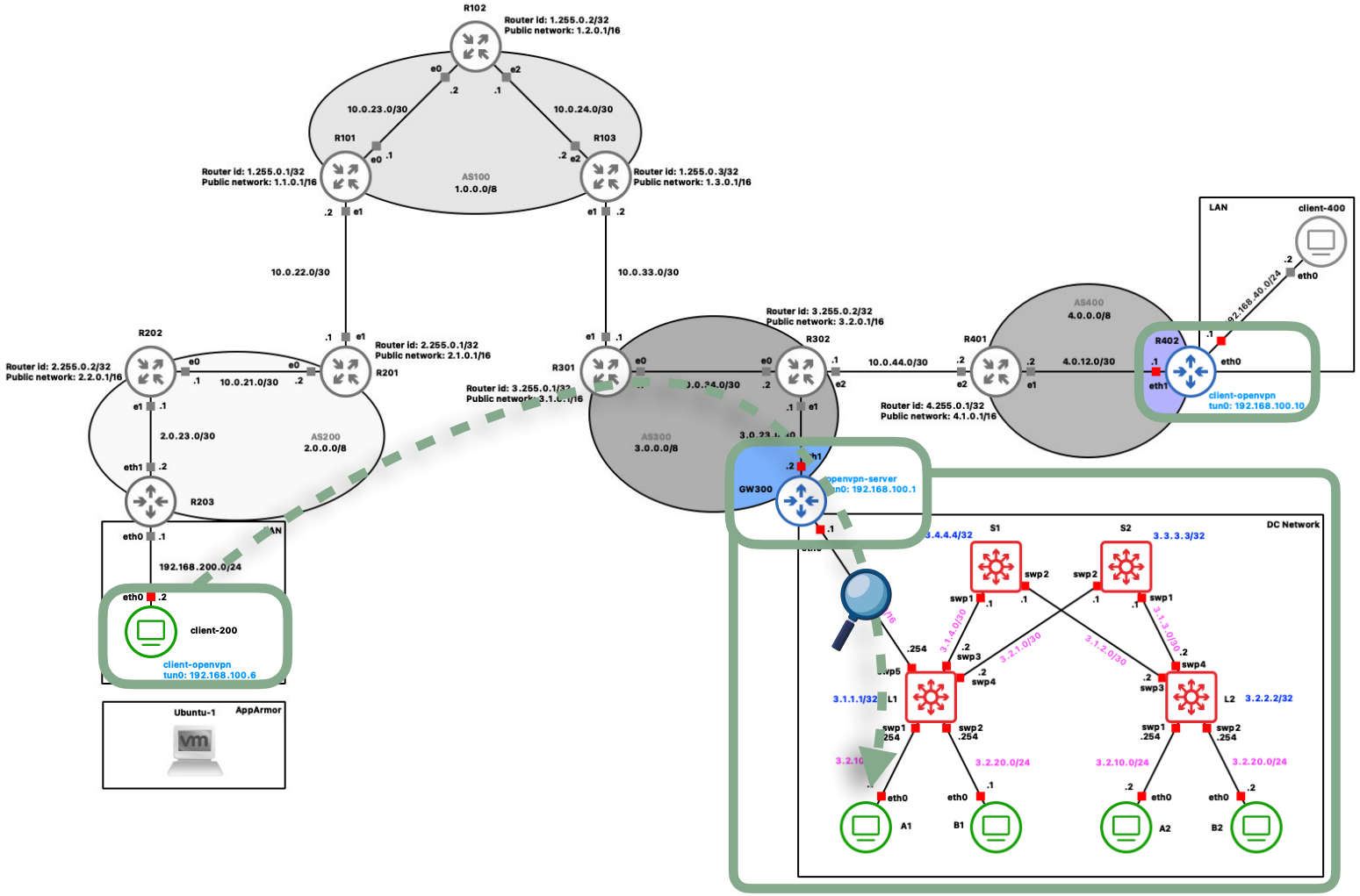
OpenVPN.


R102
Router id: 1.255.0.2/32
Public network: 1.2.0.1/16
10.0.23.0/30
10.0.24.0/30
R101
R103
Router id: 1.255.0.1/32
Public network: 1.1.0.1/16
AS100
1.0.0.0/8
Router id: 1.255.0.3/32
Public network: 1.3.0.1/16
10.0.22.0/30
10.0.33.0/30
R202
Router id: 2.255.0.2/32
Public network: 2.2.0.1/16
10.0.21.0/30
Router id: 2.255.0.1/32
Public network: 2.1.0.1/16
R201
2.0.23.0/30
AS200
2.0.0.0/8
R203
192.168.200.0/24
client-200
client-openvpn
tun0: 192.168.100.6
Ubuntu-1
AppArmor
R301
Router id: 3.255.0.2/32
Public network: 3.2.0.1/16
R302
10.0.44.0/30
R401
AS400
4.0.0.0/8
4.0.12.0/30
Router id: 4.255.0.1/32
Public network: 4.1.0.1/16
LAN
client-400
R402
client-openvpn
tun0: 192.168.100.10
AS300
3.0.0.0/8
GW300
openvpn-server
tun0: 192.168.100.1
DC Network
S1
S2
3.4.4.4/32
3.3.3.3/32
L1
L2
3.1.1.1/32
3.2.2.2/32
3.2.20.0/24
3.2.10.0/24
A1
B1
A2
B2

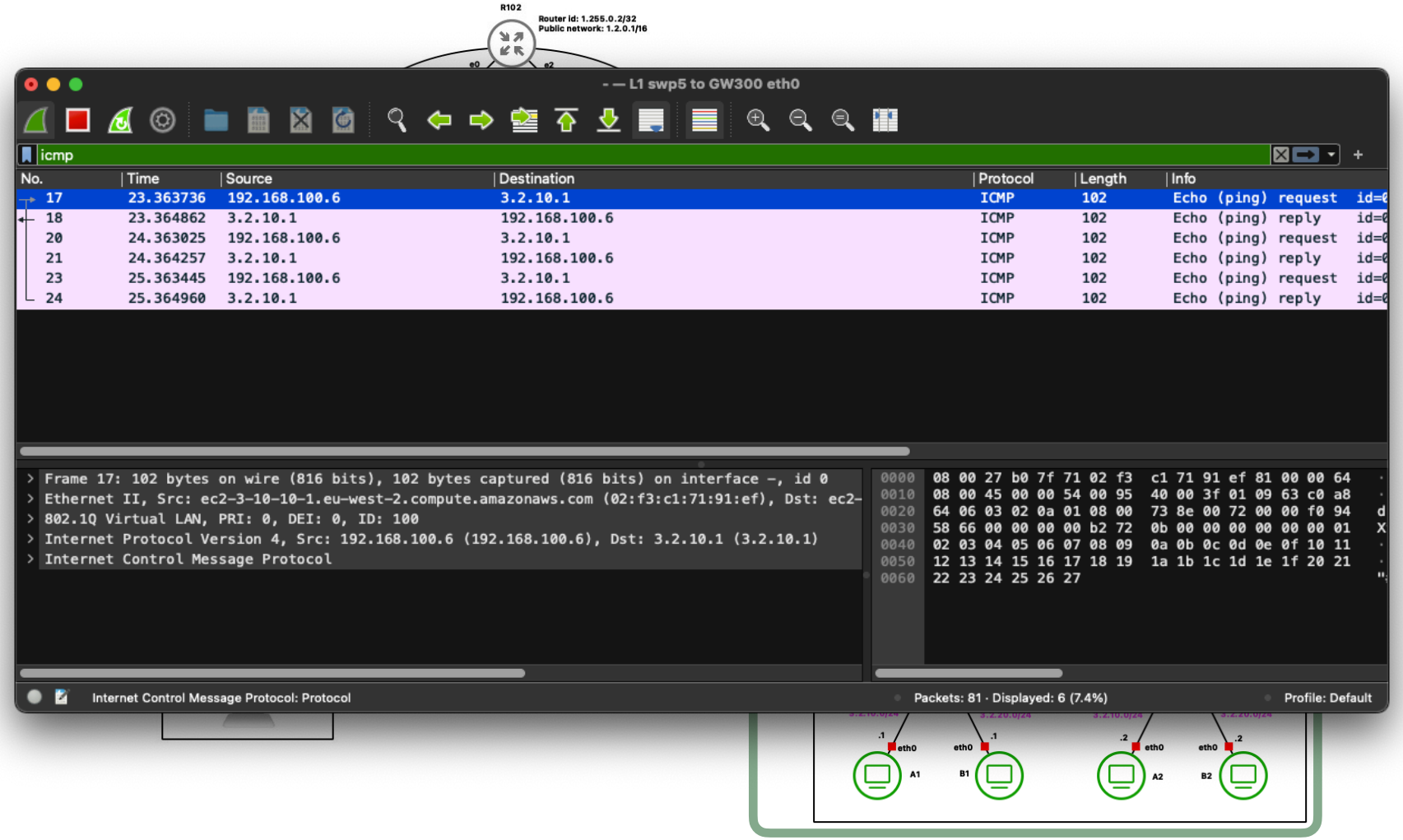
OpenVPN.


R102
Router Id: 1.255.0.2/32
Public network: 1.2.0.1/16
- — R302 e1 to GW300 eth1
openvpn
No. | Time | Source | Destination | Protocol | Length | Info
118 166.369489 2.0.23.2 ec2-3-0-23-2.ap-southeast-1.compute.amazonaws.com OpenVPN 150 MessageType: P_DATA_V2
119 166.372326 ec2-3-0-23-2.ap-southeast-1.c… 2.0.23.2 OpenVPN 150 MessageType: P_DATA_V2
120 167.372022 2.0.23.2 ec2-3-0-23-2.ap-southeast-1.compute.amazonaws.com OpenVPN 150 MessageType: P_DATA_V2
121 167.373961 ec2-3-0-23-2.ap-southeast-1.c… 2.0.23.2 OpenVPN 150 MessageType: P_DATA_V2
122 168.371972 2.0.23.2 ec2-3-0-23-2.ap-southeast-1.compute.amazonaws.com OpenVPN 150 MessageType: P_DATA_V2
123 168.376106 ec2-3-0-23-2.ap-southeast-1.c… 2.0.23.2 OpenVPN 150 MessageType: P_DATA_V2
124 169.094642 4.0.12.1 ec2-3-0-23-2.ap-southeast-1.compute.amazonaws.com OpenVPN 82 MessageType: P_DATA_V2
125 169.373622 2.0.23.2 ec2-3-0-23-2.ap-southeast-1.compute.amazonaws.com OpenVPN 150 MessageType: P_DATA_V2
126 169.375127 ec2-3-0-23-2.ap-southeast-1.c… 2.0.23.2 OpenVPN 150 MessageType: P_DATA_V2
129 170.374610 2.0.23.2 ec2-3-0-23-2.ap-southeast-1.compute.amazonaws.com OpenVPN 150 MessageType: P_DATA_V2
130 170.376725 ec2-3-0-23-2.ap-southeast-1.c… 2.0.23.2 OpenVPN 150 MessageType: P_DATA_V2
131 171.376142 2.0.23.2 ec2-3-0-23-2.ap-southeast-1.compute.amazonaws.com OpenVPN 150 MessageType: P_DATA_V2
132 171.378770 ec2-3-0-23-2.ap-southeast-1.c… 2.0.23.2 OpenVPN 150 MessageType: P_DATA_V2
> Frame 118: 150 bytes on wire (1200 bits), 150 bytes captured (1200 bits) on interface -, id 0
> Ethernet II, Src: ec2-3-0-23-1.ap-southeast-1.compute.amazonaws.com (e2:d9:4e:27:3b:03), Dst:
> Internet Protocol Version 4, Src: 2.0.23.2 (2.0.23.2), Dst: ec2-3-0-23-2.ap-southeast-1.comput
> User Datagram Protocol, Src Port: openvpn (1194), Dst Port: openvpn (1194)
> OpenVPN Protocol
0000 62 c5 12 79 b0 23 e2 d9 4e 27 3b 03 08 00 45 00 b
0010 00 88 68 2e 40 00 38 11 a7 33 02 00 17 02 03 00
0020 17 02 04 aa 04 aa 00 74 4b dc 48 00 00 00 00 00
0030 00 1c 7c ab 28 ce ea 54 6d f1 ca 27 47 2e 61 b1
0040 88 fd 69 54 07 20 ae dd 0a a8 75 b9 ec 67 42 ae
0050 30 19 4d 1a c7 1d ff 7e 45 14 69 b7 68 d9 a6 e5 0
0060 0b 14 f8 00 ae e9 b8 11 6f 05 2a 3c 9b 19 55 ed
0070 c3 b6 16 26 17 5c 80 b7 c8 1c 17 c7 46 9b 36 e3
0080 88 ae c5 90 f6 ae 0b d9 8d a4 03 15 22 8e 28 74
0090 ae e2 d2 f0 f1 c9
OpenVPN Protocol: Protocol
Packets: 145 · Displayed: 123 (84.8%)
Profile: Default
.1 eth0 A1
eth0 .1 B1
.2 eth0 A2
eth0 .2 B2

OpenVPN.


R102
Router id: 1.255.0.2/32
Public network: 1.2.0.1/16
10.0.23.0/30
10.0.24.0/30
R101
R103
Router id: 1.255.0.1/32
Public network: 1.1.0.1/16
AS100
1.0.0.0/8
Router id: 1.255.0.3/32
Public network: 1.3.0.1/16
10.0.22.0/30
10.0.33.0/30
R202
Router id: 2.255.0.2/32
Public network: 2.2.0.1/16
Router id: 2.255.0.1/32
Public network: 2.1.0.1/16
R201
10.0.21.0/30
2.0.23.0/30
AS200
2.0.0.0/8
R203
192.168.200.0/24
client-200
client-openvpn
tun0: 192.168.100.6
Ubuntu-1
AppArmor
Router id: 3.255.0.2/32
Public network: 3.2.0.1/16
R301
R302
AS300
3.0.0.0/8
10.0.44.0/30
R401
AS400
4.0.0.0/8
4.0.12.0/30
Router id: 4.255.0.1/32
Public network: 4.1.0.1/16
LAN
client-400
R402
client-openvpn
tun0: 192.168.100.10
GW300
openvpn-server
tun0: 192.168.100.1
DC Network
S1
S2
3.4.4.4/32
3.3.3.3/32
swp1
swp2
swp3
swp4
3.1.4.0/30
3.1.3.0/30
3.1.2.0/30
L1
L2
3.1.1.1/32
3.2.2.2/32
3.2.20.0/24
3.2.10.0/24
A1
B1
A2
B2
eth0

OpenVPN.


R102
Router Id: 1.255.0.2/32
Public network: 1.2.0.1/16
- — L1 swp5 to GW300 eth0
icmp
No. | Time | Source | Destination | Protocol | Length | Info
17 23.363736 192.168.100.6 3.2.10.1 ICMP 102 Echo (ping) request id=0
18 23.364862 3.2.10.1 192.168.100.6 ICMP 102 Echo (ping) reply id=0
20 24.363025 192.168.100.6 3.2.10.1 ICMP 102 Echo (ping) request id=0
21 24.364257 3.2.10.1 192.168.100.6 ICMP 102 Echo (ping) reply id=0
23 25.363445 192.168.100.6 3.2.10.1 ICMP 102 Echo (ping) request id=0
24 25.364960 3.2.10.1 192.168.100.6 ICMP 102 Echo (ping) reply id=0
> Frame 17: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface -, id 0
> Ethernet II, Src: ec2-3-10-10-1.eu-west-2.compute.amazonaws.com (02:f3:c1:71:91:ef), Dst: ec2-
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 100
> Internet Protocol Version 4, Src: 192.168.100.6 (192.168.100.6), Dst: 3.2.10.1 (3.2.10.1)
> Internet Control Message Protocol
0000 08 00 27 b0 7f 71 02 f3 c1 71 91 ef 81 00 00 64
0010 08 00 45 00 00 54 00 95 40 00 3f 01 09 63 c0 a8
0020 64 06 03 02 0a 01 08 00 73 8e 00 72 00 00 f0 94
0030 58 66 00 00 00 00 b2 72 0b 00 00 00 00 00 00 01
0040 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f 10 11
0050 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21
0060 22 23 24 25 26 27
Internet Control Message Protocol: Protocol
Packets: 81 · Displayed: 6 (7.4%)
Profile: Default
eth0
A1
B1
A2
B2

AppArmor.

I **security modules** forniscono framework di sicurezza nel kernel Linux.

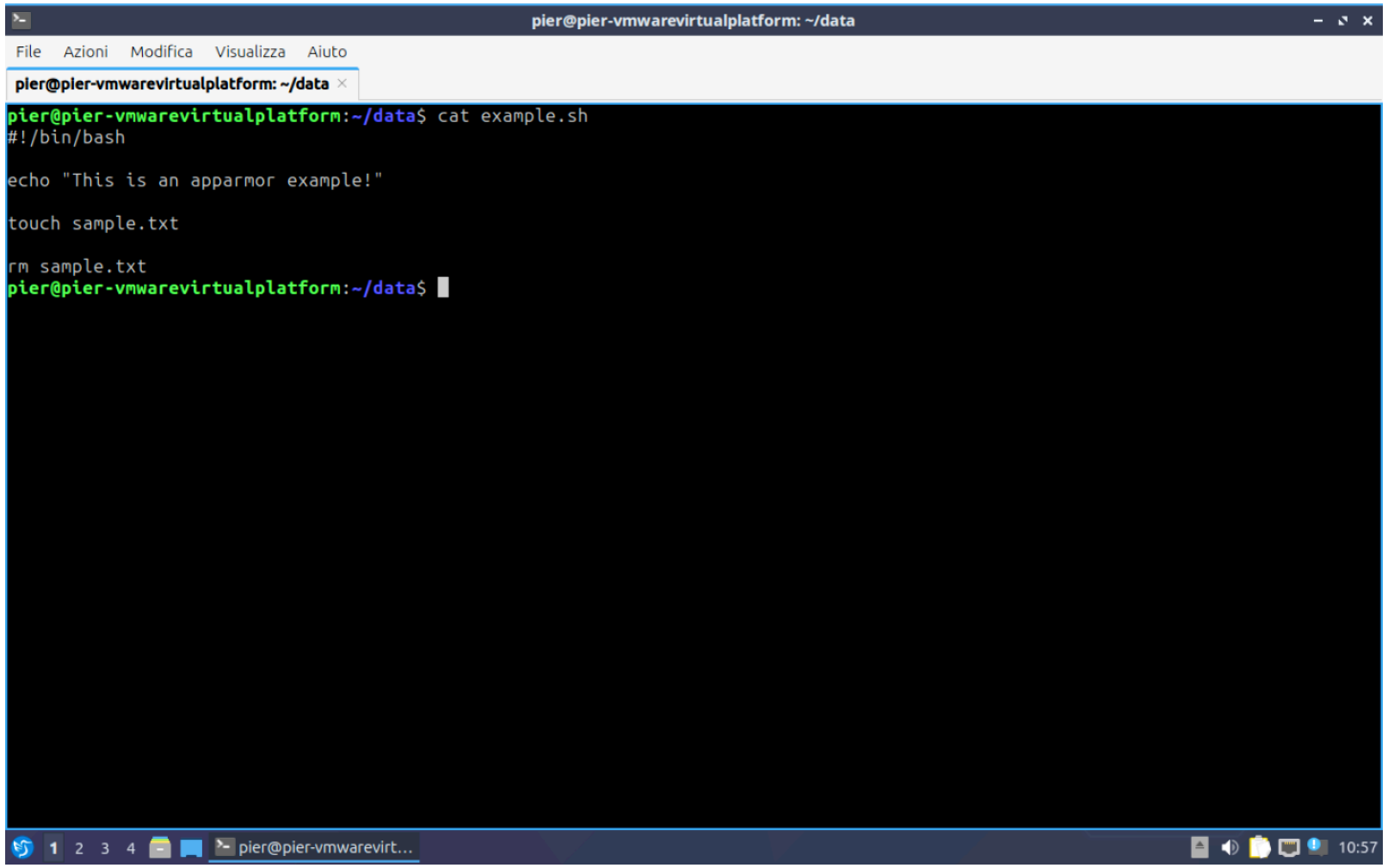
Di default Linux offre soltanto il meccanismo **DAC**, tuttavia è stato realizzato un framework di sicurezza che permette di caricare alcuni moduli nel kernel per implementare una sorta di schema **MAC**.

AppArmor è un sistema di controllo degli accessi per il kernel Linux che permette di limitare le capacità dei programmi tramite **profili di sicurezza**.

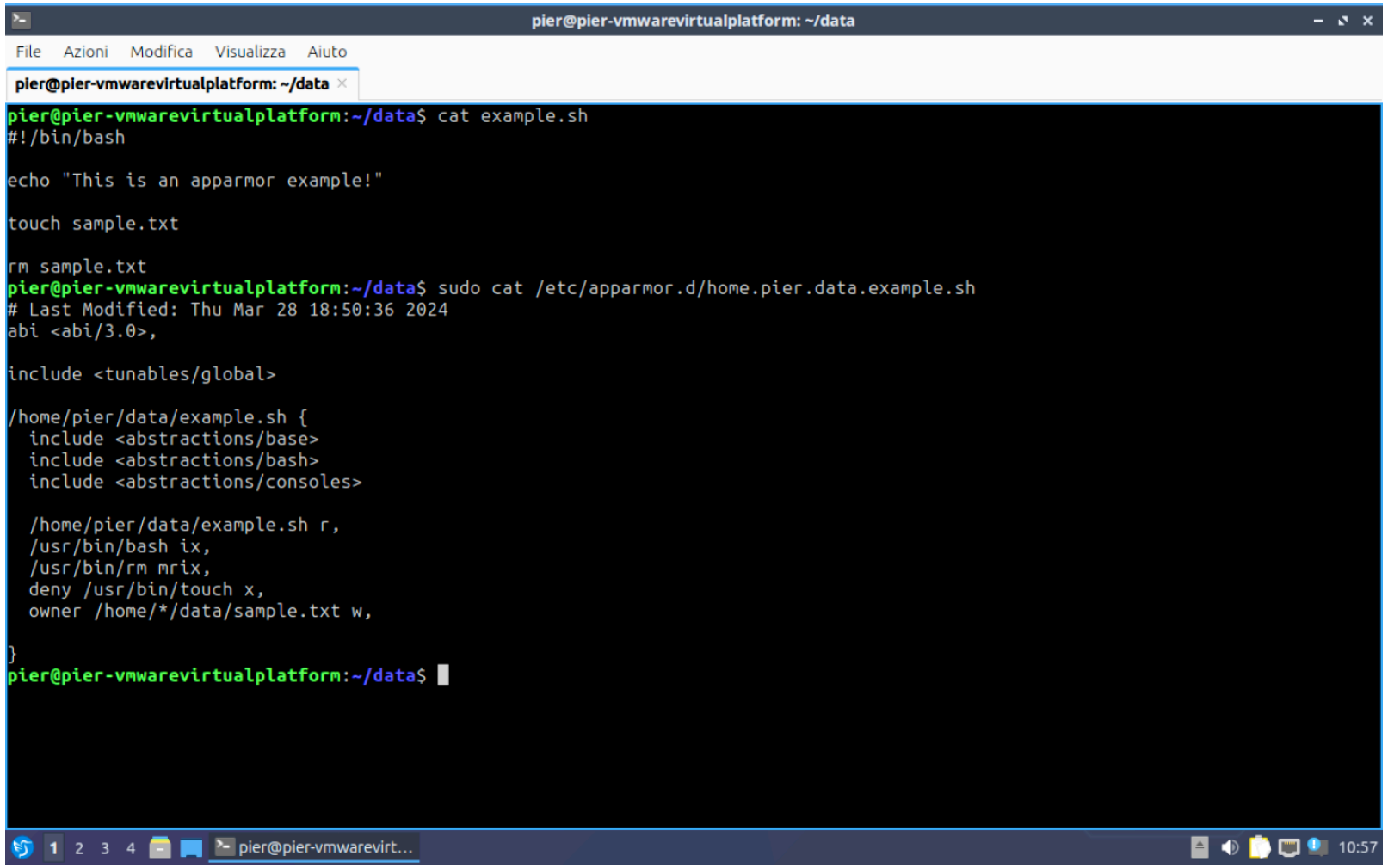
Utilizza **regole basate su percorsi** per restringere le operazioni di file e risorse di sistema che le applicazioni possono eseguire, migliorando la sicurezza complessiva del sistema.

Viene configurato tramite profili scritti in un **linguaggio semplice e leggibile**, che specificano le autorizzazioni consentite per ogni programma.

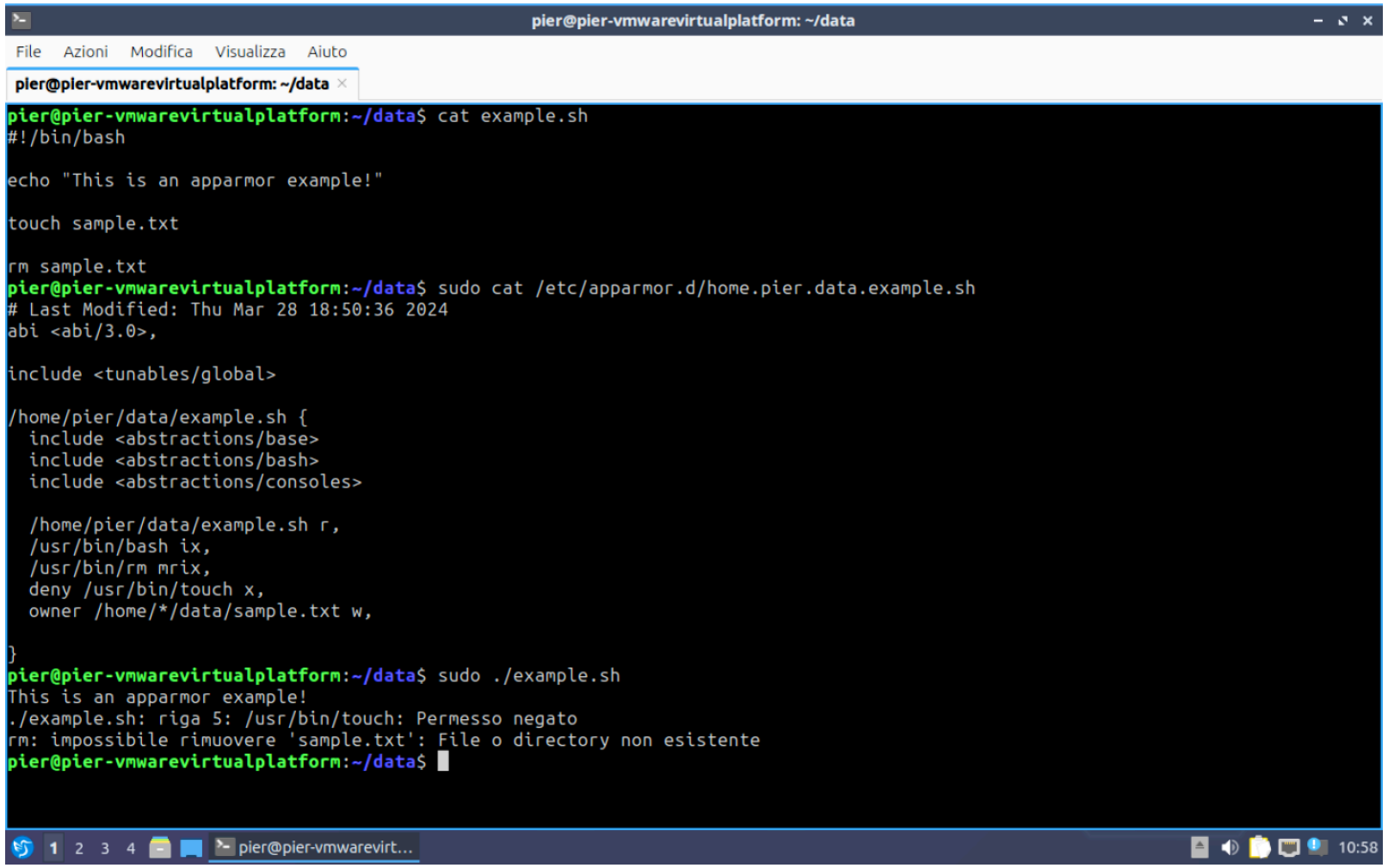
AppArmor.


pier@pier-vmwarevirtualplatform: ~/data
File Azioni Modifica Visualizza Aiuto
pier@pier-vmwarevirtualplatform: ~/data
pier@pier-vmwarevirtualplatform:~/data$ cat example.sh
#!/bin/bash
echo "This is an apparmor example!"
touch sample.txt
rm sample.txt
pier@pier-vmwarevirtualplatform:~/data$
1 2 3 4
pier@pier-vmwarevirt...
10:57

AppArmor.


pier@pier-vmwarevirtualplatform: ~/data
File Azioni Modifica Visualizza Aiuto
pier@pier-vmwarevirtualplatform: ~/data
pier@pier-vmwarevirtualplatform:~/data$ cat example.sh
#!/bin/bash
echo "This is an apparmor example!"
touch sample.txt
rm sample.txt
pier@pier-vmwarevirtualplatform:~/data$ sudo cat /etc/apparmor.d/home.pier.data.example.sh
Last Modified: Thu Mar 28 18:50:36 2024
abi <abi/3.0>,
include <tunables/global>
/home/pier/data/example.sh {
include <abstractions/base>
include <abstractions/bash>
include <abstractions/consoles>
/home/pier/data/example.sh r,
/usr/bin/bash ix,
/usr/bin/rm mrix,
deny /usr/bin/touch x,
owner /home/*/data/sample.txt w,
}
pier@pier-vmwarevirtualplatform:~/data$
1 2 3 4
pier@pier-vmwarevirt...
10:57

AppArmor.


pier@pier-vmwarevirtualplatform: ~/data
File Azioni Modifica Visualizza Aiuto
pier@pier-vmwarevirtualplatform: ~/data
pier@pier-vmwarevirtualplatform:~/data$ cat example.sh
#!/bin/bash
echo "This is an apparmor example!"
touch sample.txt
rm sample.txt
pier@pier-vmwarevirtualplatform:~/data$ sudo cat /etc/apparmor.d/home.pier.data.example.sh
Last Modified: Thu Mar 28 18:50:36 2024
abi <abi/3.0>,
include <tunables/global>
/home/pier/data/example.sh {
include <abstractions/base>
include <abstractions/bash>
include <abstractions/consoles>
/home/pier/data/example.sh r,
/usr/bin/bash ix,
/usr/bin/rm mrix,
deny /usr/bin/touch x,
owner /home/*/data/sample.txt w,
}
pier@pier-vmwarevirtualplatform:~/data$ sudo ./example.sh
This is an apparmor example!
./example.sh: riga 5: /usr/bin/touch: Permesso negato
rm: impossibile rimuovere 'sample.txt': File o directory non esistente
pier@pier-vmwarevirtualplatform:~/data$
1 2 3 4
pier@pier-vmwarevirt...
10:58

Grazie per l'attenzione!

GitHub

https://github.com/pierpaolospaziani/NSD-project

Pierpaolo Spaziani

Matricola: 0316331

Università degli Studi di Roma Tor Vergata