

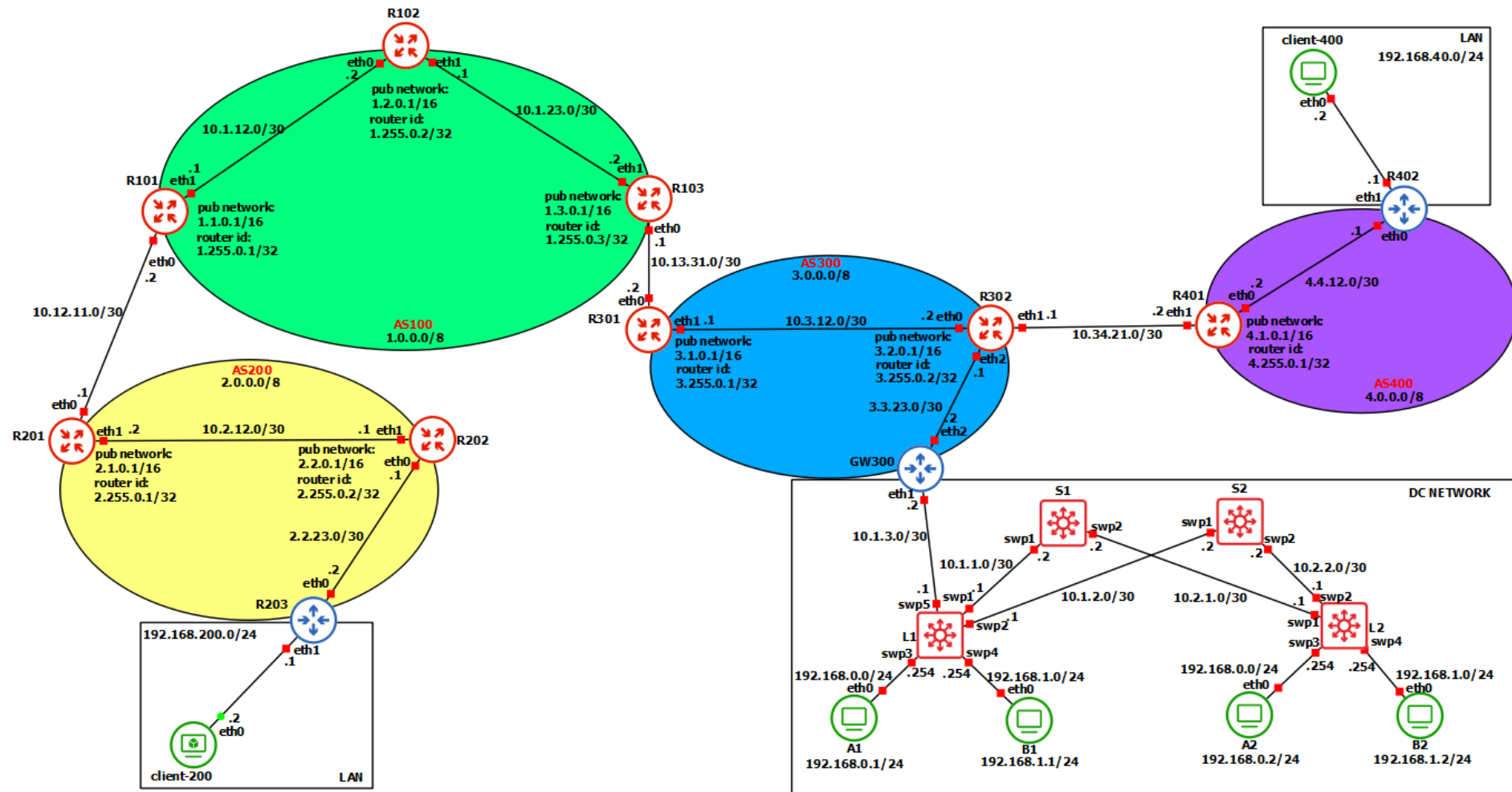
Network and System Defence

Valerio Crecco — 0320452

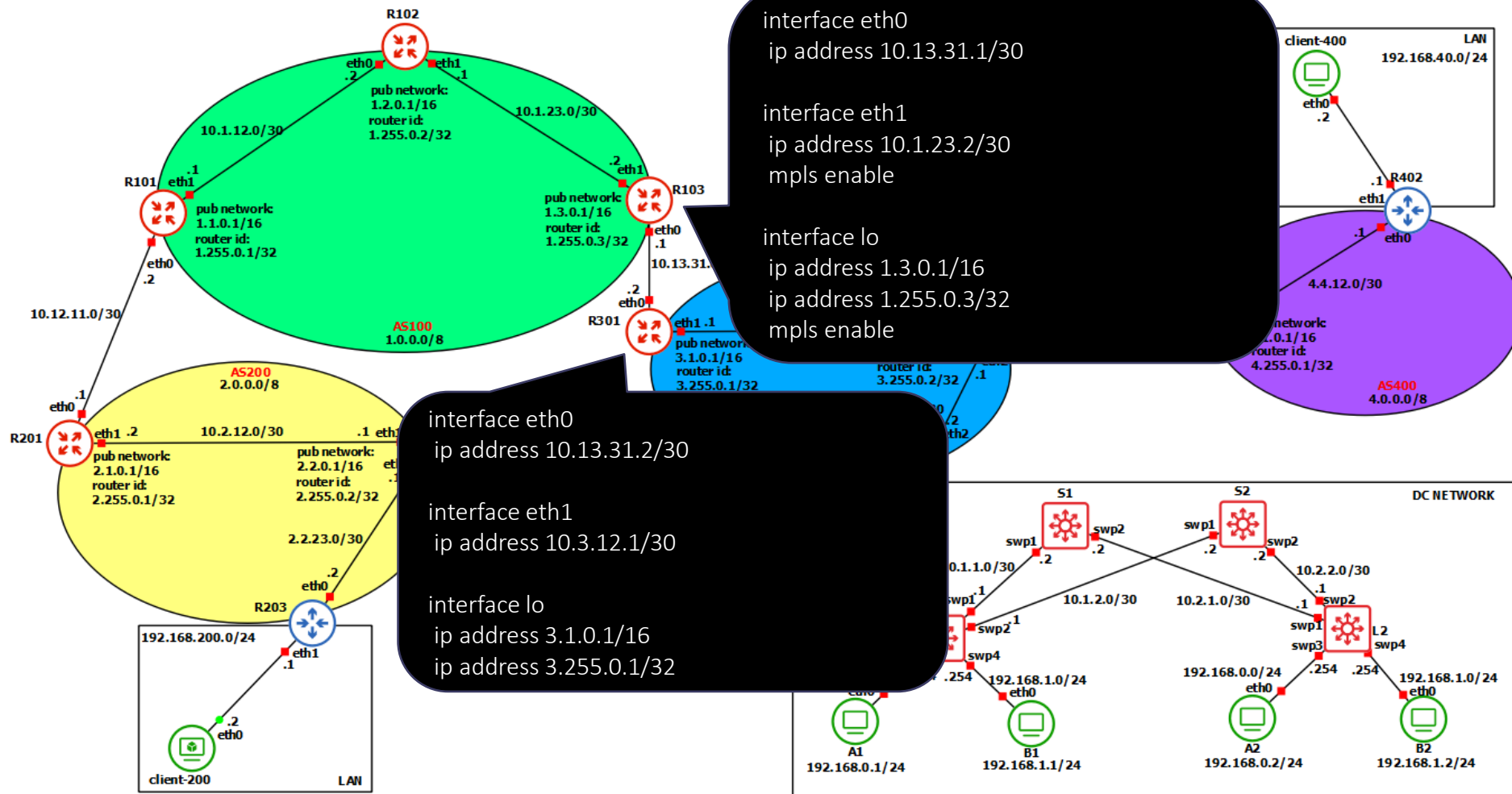
Ludovico De Santis — 0320460

Università degli studi di Roma Tor Vergata

Topologia



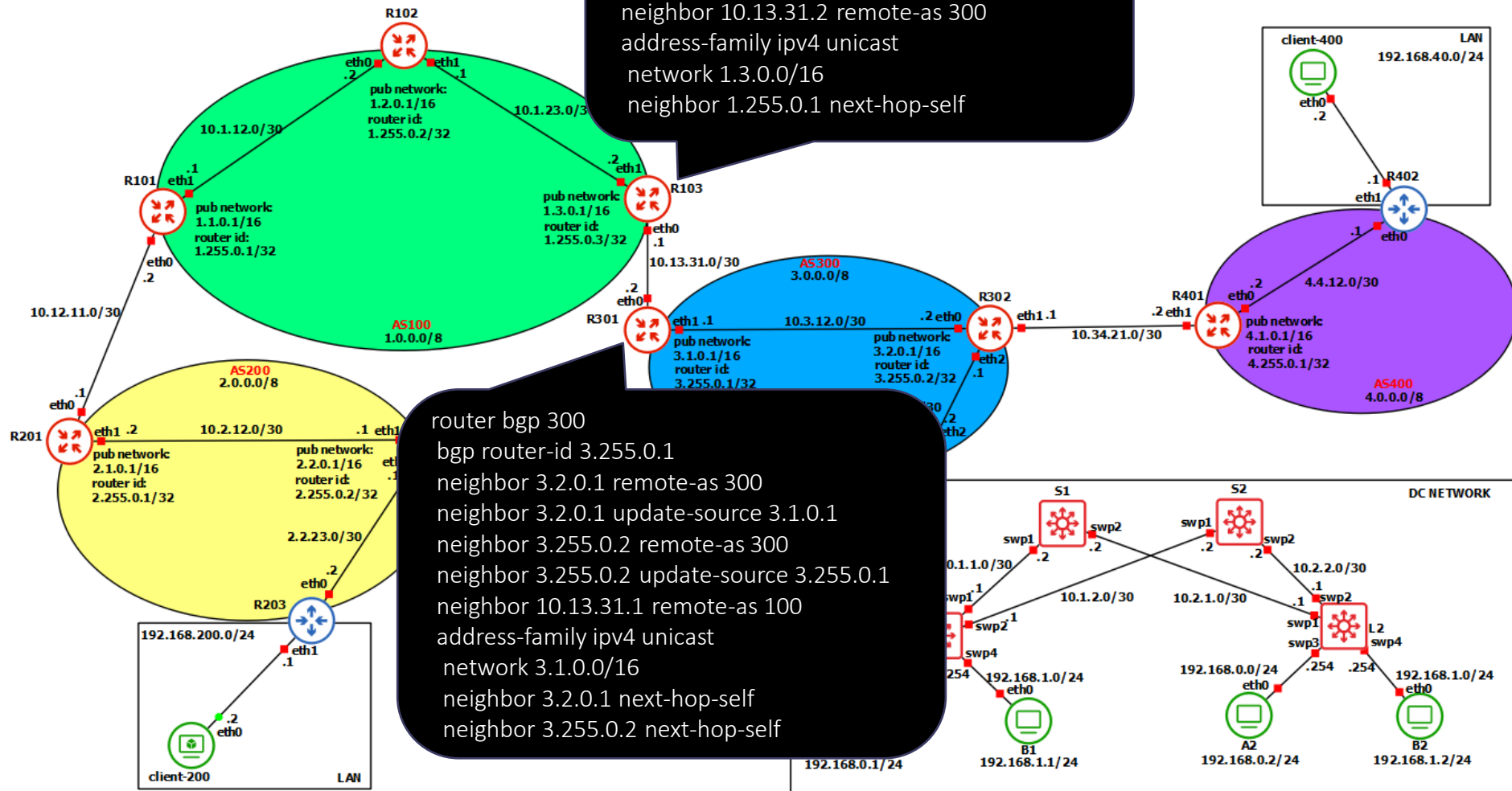
Configurazione interfacce



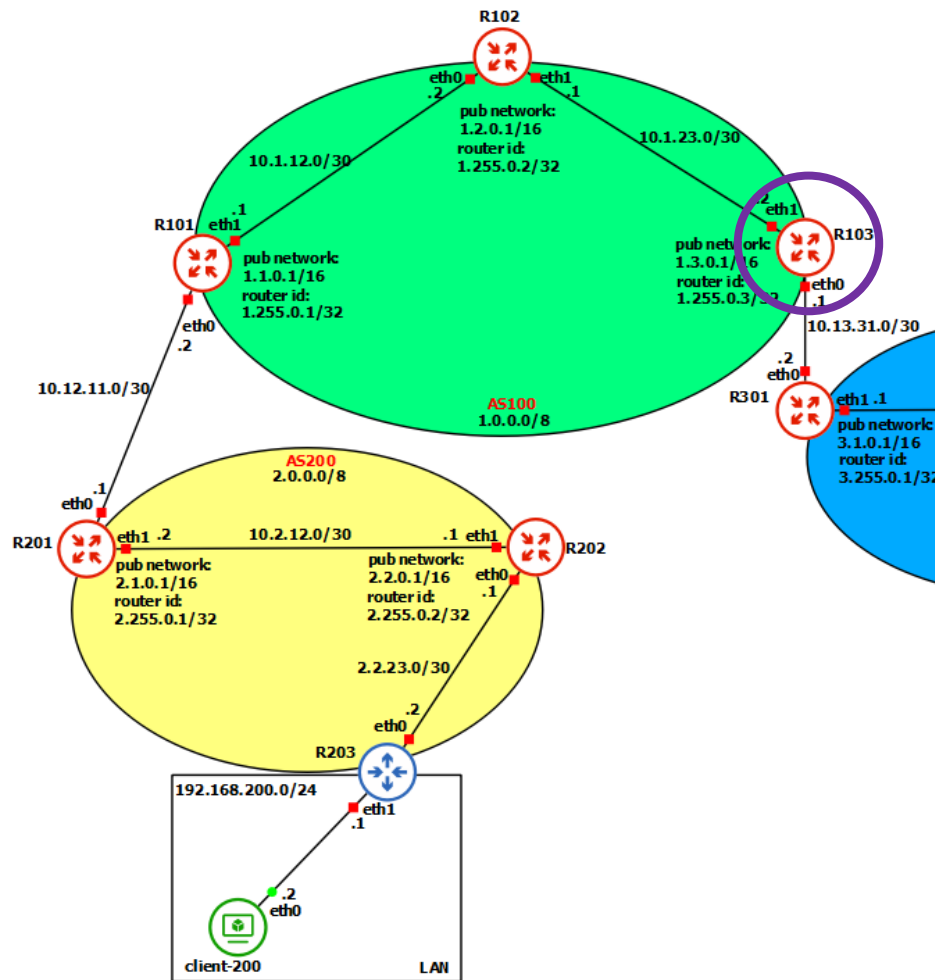
Protocolli – BGP (Border Gateway Protocol)

- **BGP** è un protocollo di instradamento, di tipo *distance vector*, utilizzato su Internet per scambiare informazioni di routing tra **Autonomous Systems** (AS).
- Consente a reti diverse di comunicare e instradare il traffico da un punto all'altro su larga scala;
- Individua i **migliori percorsi** per il traffico di rete basandosi su criteri come il numero di hop (salti) tra router o specifiche politiche di routing;
- Scambia informazioni di routing sotto forma di **annunci di rotte**, permettendo ai vari router di aggiornarsi reciprocamente sui migliori percorsi;

BGP



BGP

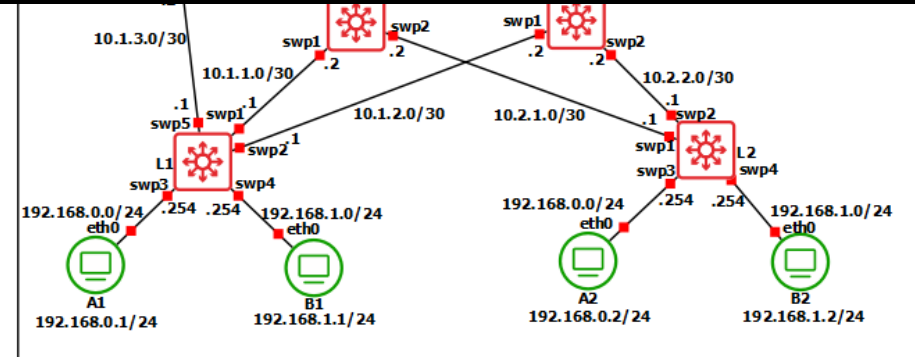


```

R103# show ip bgp
BGP table version is 10, local router ID is 1.255.0.3, 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
Next hop 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
*>i1.1.0.0/16      1.255.0.1(R101)      0      100      0 i
*> 1.3.0.0/16      0.0.0.0(R103)        0              32768 i
*>i2.1.0.0/16      1.255.0.1(R101)      0      100      0 200 i
*>i2.2.0.0/16      1.255.0.1(R101)      0      100      0 200 i
*>i2.2.23.0/30     1.255.0.1(R101)      0      100      0 200 i
*> 3.1.0.0/16      10.13.31.2(R301)     0              0 300 i
*> 3.2.0.0/16      10.13.31.2(R301)     0              0 300 i
*> 3.3.23.0/30     10.13.31.2(R301)     0              0 300 i
*> 4.1.0.0/16      10.13.31.2(R301)     0              0 300 400 i
*> 4.4.12.0/30     10.13.31.2(R301)     0              0 300 400 i

Displayed 10 routes and 10 total paths
R103#
```



Protocolli – OSPF (Open Shortest Path First)

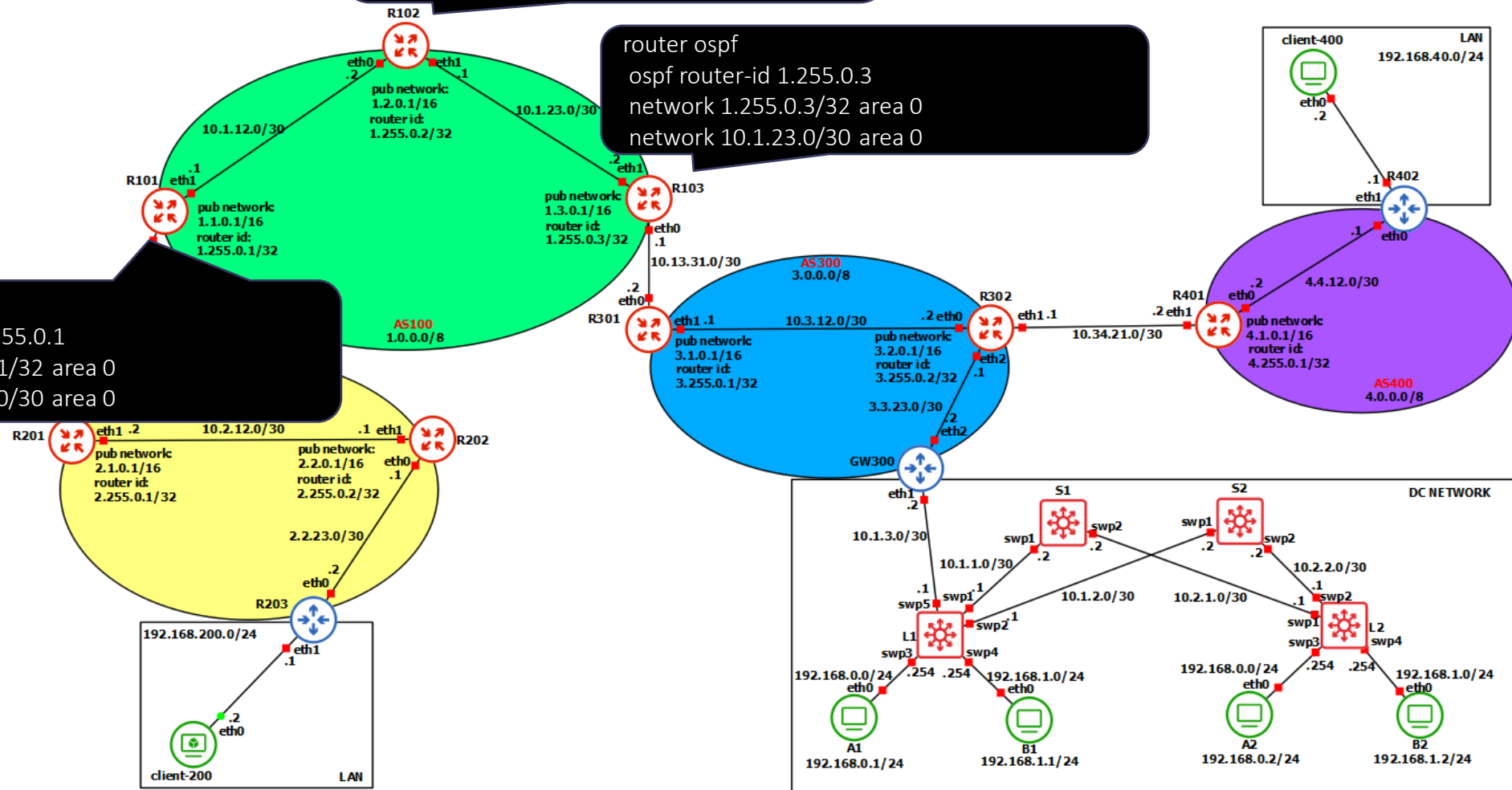
- OSPF è un protocollo IGP (Interior Gateway Protocol) di routing dinamico utilizzato all'interno di un AS;
- Protocollo Link-State, in cui ogni router ha una mappa completa della rete (topologia) e calcola il percorso più breve (Shortest Path First) verso ogni destinazione utilizzando l'algoritmo di Dijkstra;
- Uno dei vantaggi di OSPF è la sua capacità di convergere rapidamente, cioè di aggiornare la tabella di routing di tutti i router in risposta a cambiamenti nella rete;
- È altamente scalabile e supporta reti di grandi dimensioni suddivise in aree per migliorare l'efficienza e ridurre il traffico di aggiornamento;

OSPF

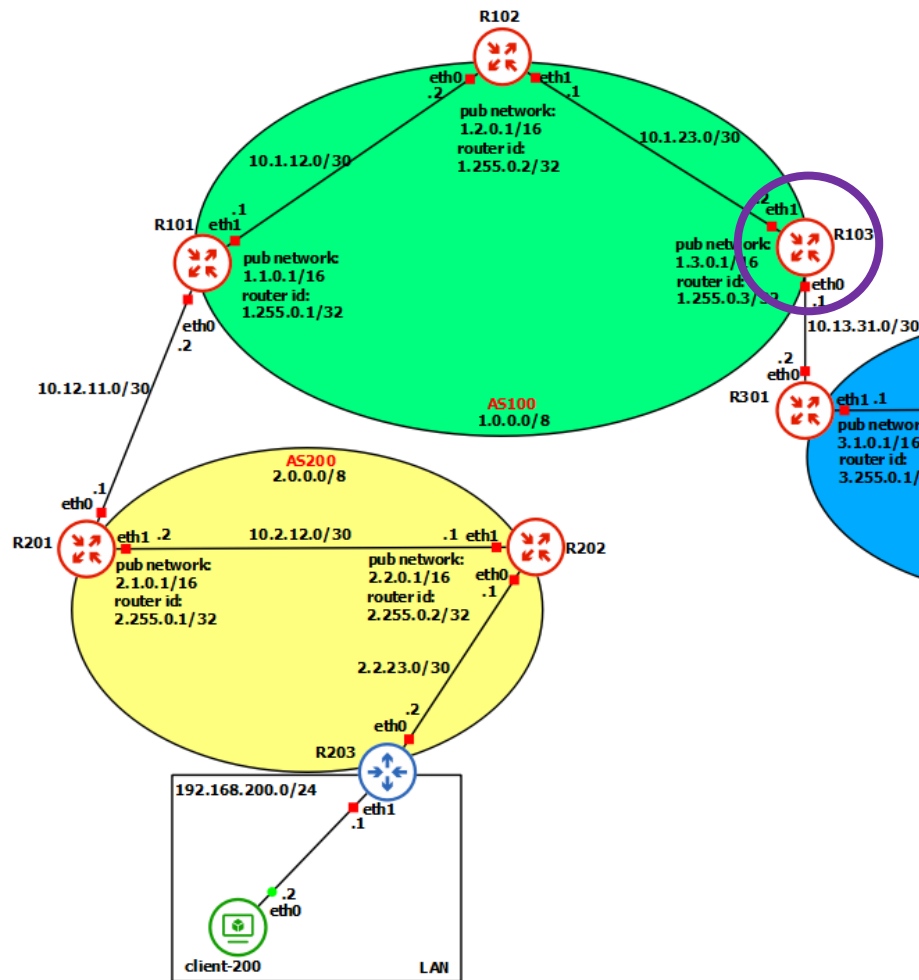
```
router ospf
ospf router-id 1.255.0.2
network 1.255.0.2/32 area 0
network 10.1.12.0/30 area 0
network 10.1.23.0/30 area 0
```

```
router ospf
ospf router-id 1.255.0.3
network 1.255.0.3/32 area 0
network 10.1.23.0/30 area 0
```

```
router ospf
ospf router-id 1.255.0.1
network 1.255.0.1/32 area 0
network 10.1.12.0/30 area 0
```



OSPF

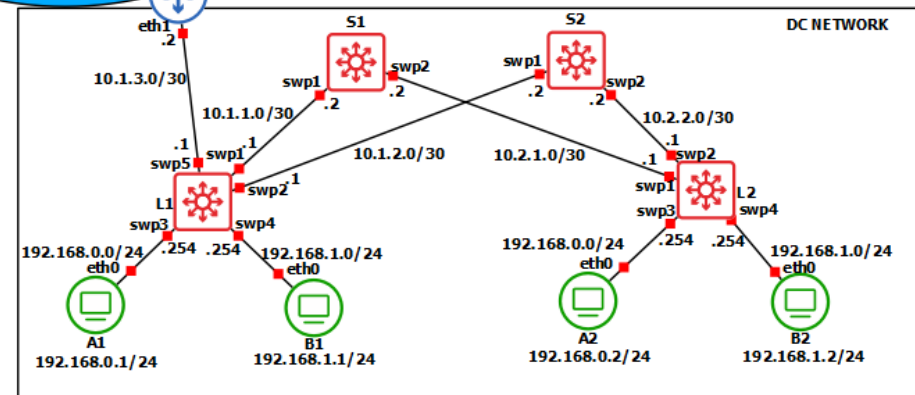


```
R103:~# vtysh
% Can't open configuration file /etc/frr/vtysh.conf due to 'No such file or directory'.
Configuration file[/etc/frr/frr.conf] processing failure: 11

Hello, this is FRRouting (version 9.0.1_git).
Copyright 1996-2005 Kunihiro Ishiguro, et al.

R103# 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>* 1.255.0.1/32 [110/20000] via 10.1.23.1, eth1, label 16, weight 1, 00:56:45
O>* 1.255.0.2/32 [110/10000] via 10.1.23.1, eth1, label implicit-null, weight 1, 00:56:45
O 1.255.0.3/32 [110/0] is directly connected, lo, weight 1, 00:57:30
O>* 10.1.12.0/30 [110/20000] via 10.1.23.1, eth1, label implicit-null, weight 1, 00:56:45
O 10.1.23.0/30 [110/10000] is directly connected, eth1, weight 1, 00:57:30
R103#
```



Protocolli – MPLS/LDP

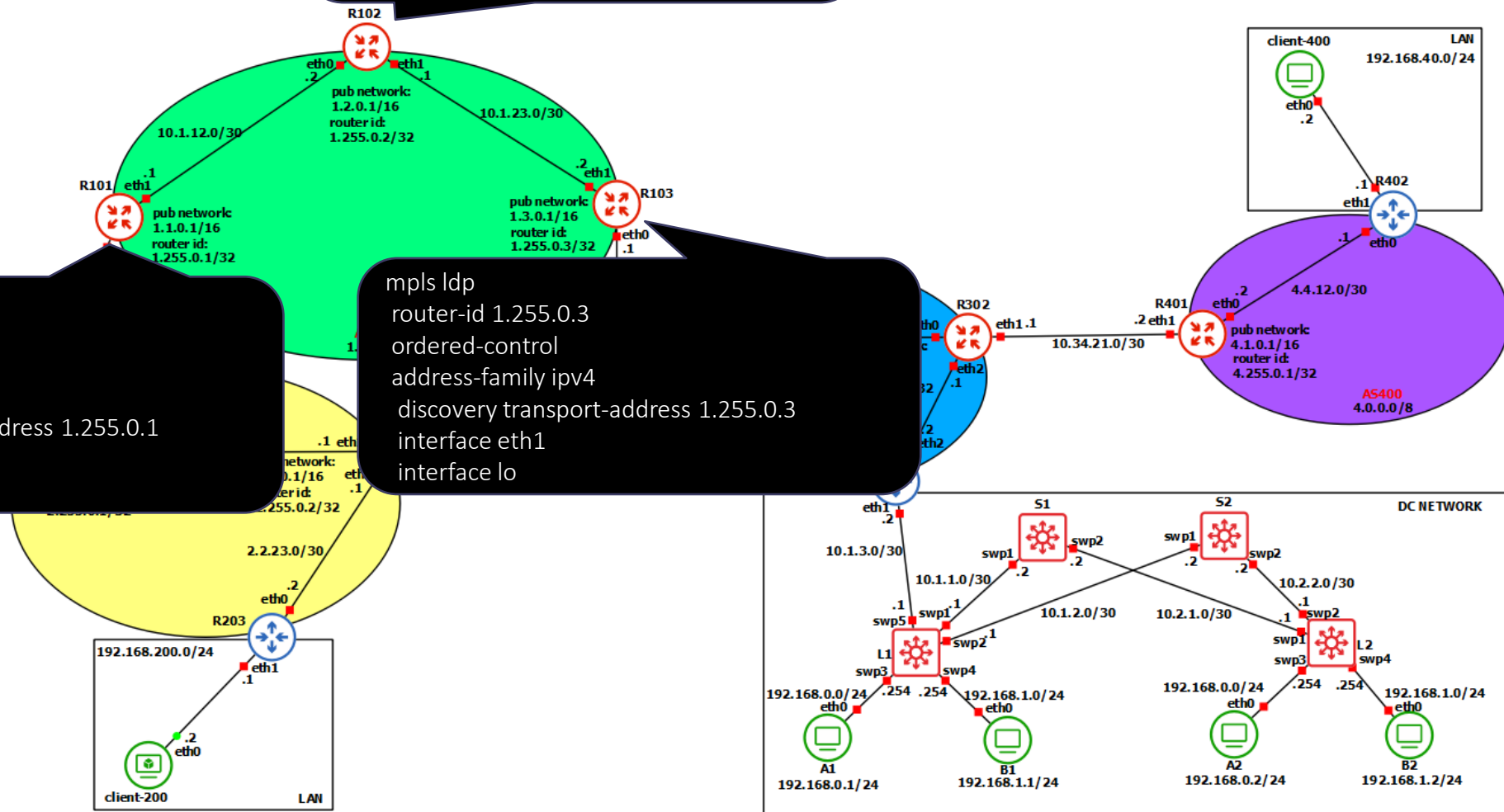
- **MPLS (Multiprotocol Label Switching)** è utilizzato per instradare dati in modo efficiente attraverso una rete utilizzando delle **labels**. Migliora la velocità di instradamento e la qualità del servizio (QoS), specialmente in reti di grandi dimensioni;
- **LDP (Label Distribution Protocol)**, è un protocollo utilizzato nelle reti MPLS per la distribuzione delle etichette (labels) tra i router;

MPLS/LDP

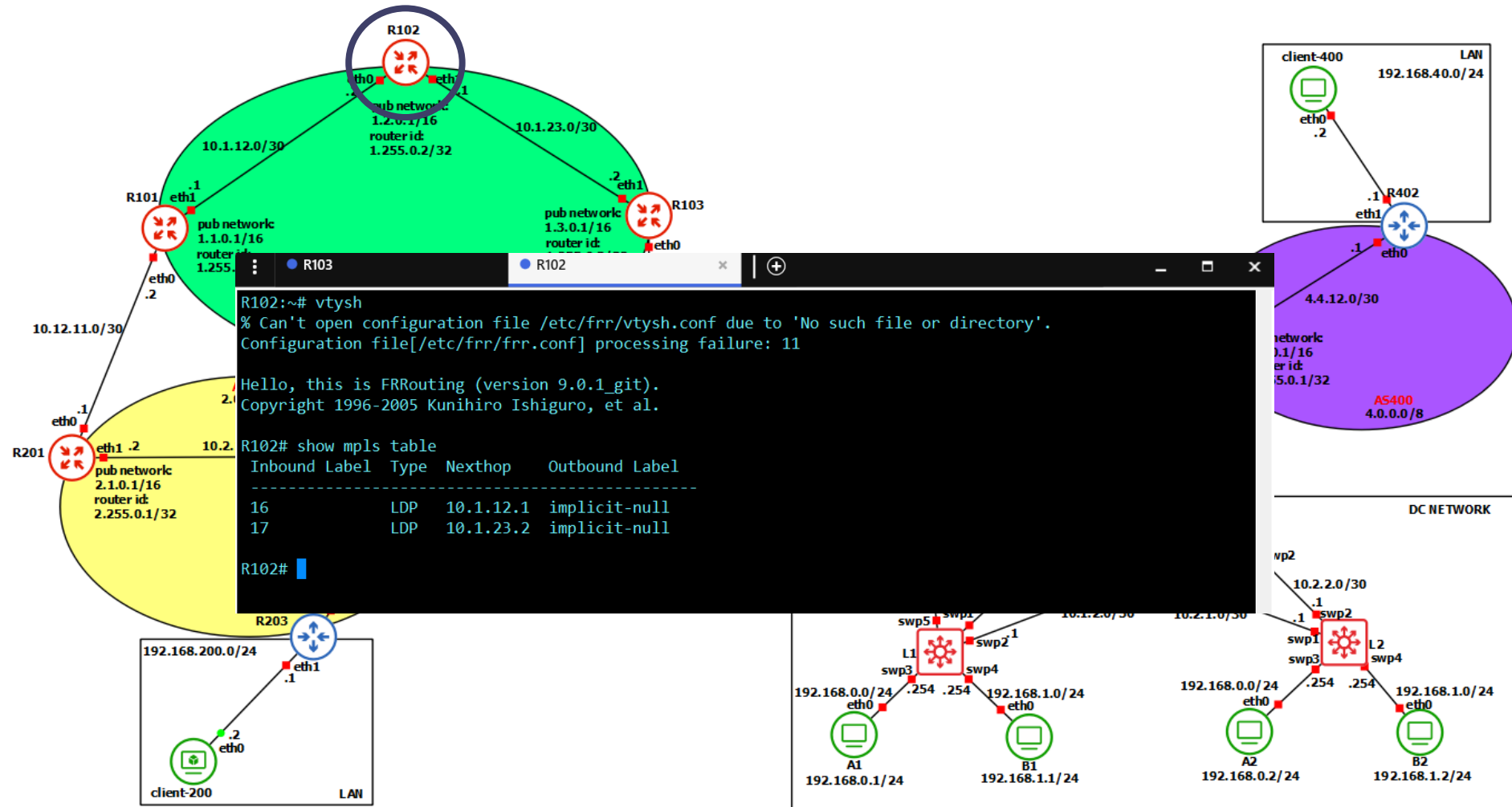
mpls ldp
router-id 1.255.0.2
ordered-control
address-family ipv4
discovery transport-address 1.255.0.2
interface eth0
interface eth1
interface lo

mpls ldp
router-id 1.255.0.1
ordered-control
address-family ipv4
discovery transport-address 1.255.0.1
interface eth1
interface lo

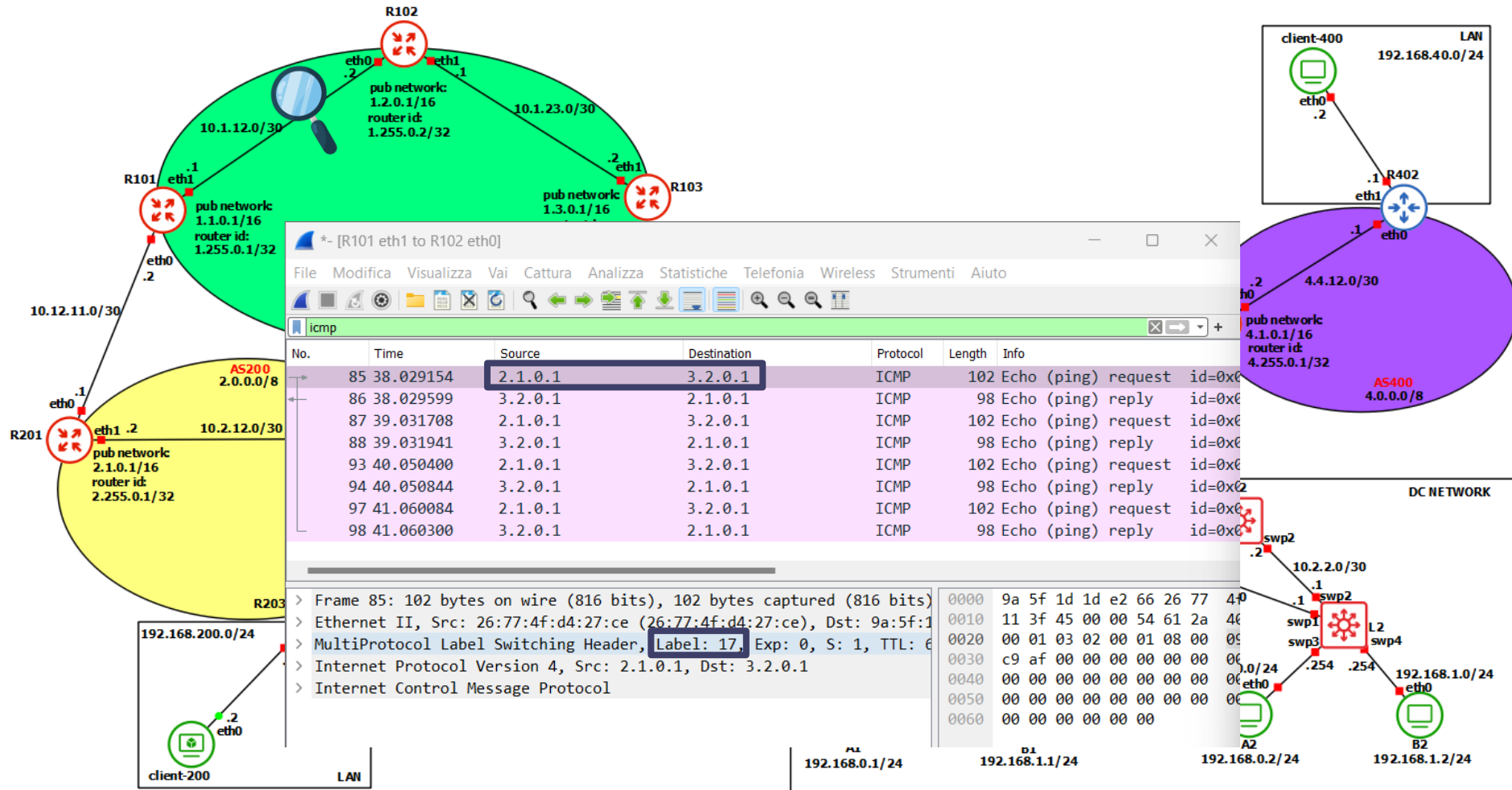
mpls ldp
router-id 1.255.0.3
ordered-control
address-family ipv4
discovery transport-address 1.255.0.3
interface eth1
interface lo



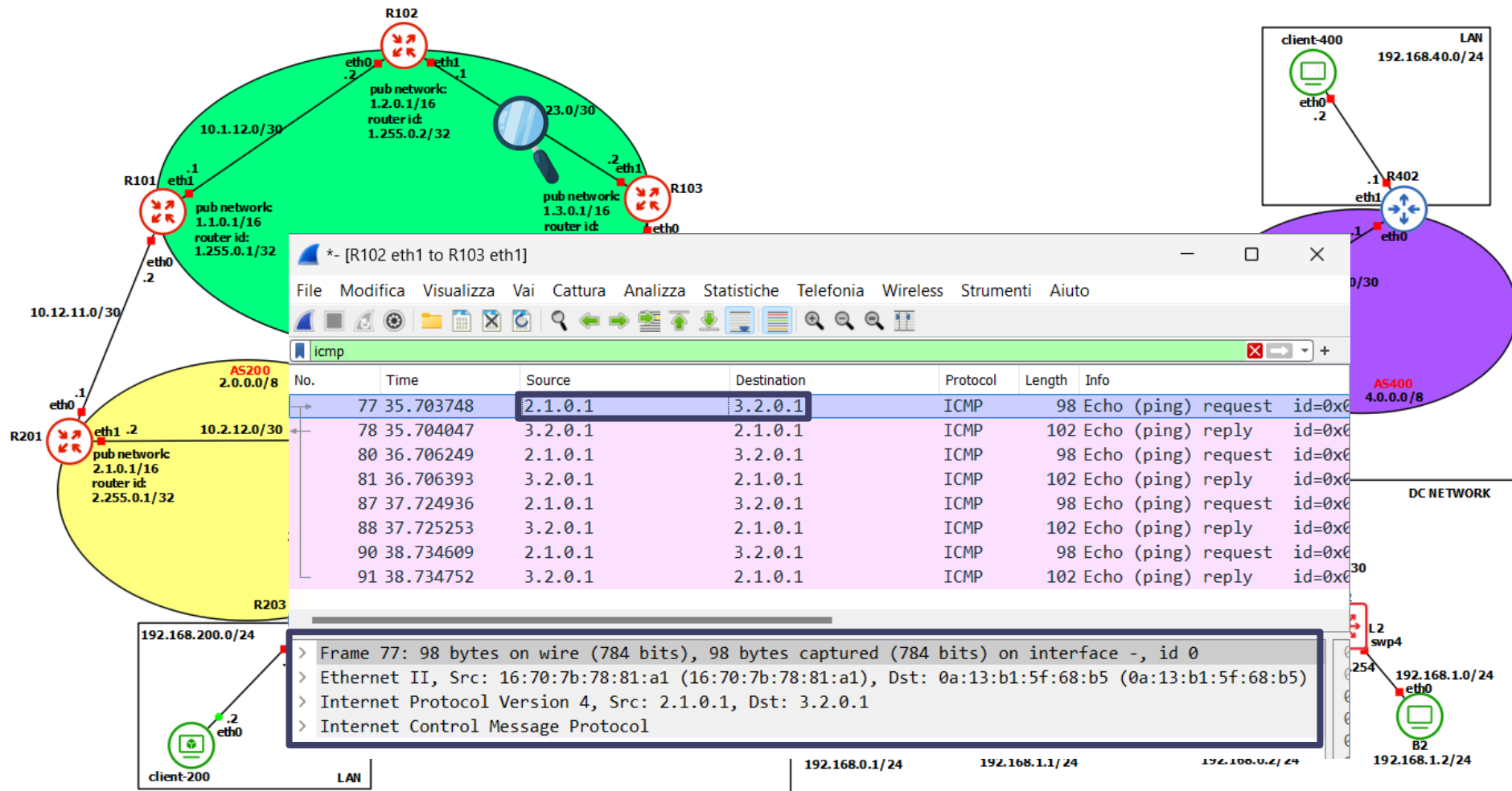
MPLS/LDP



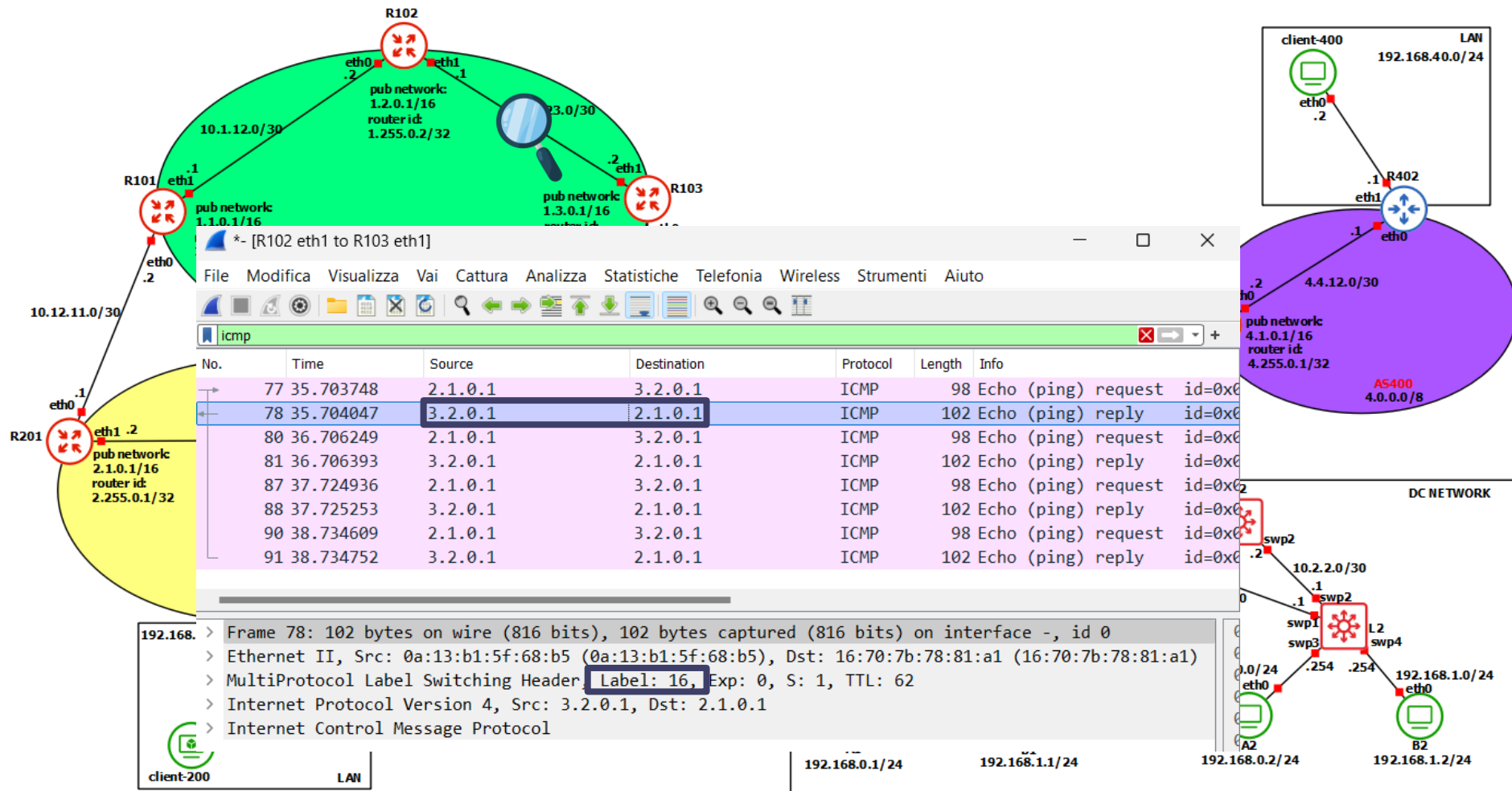
MPLS/LDP



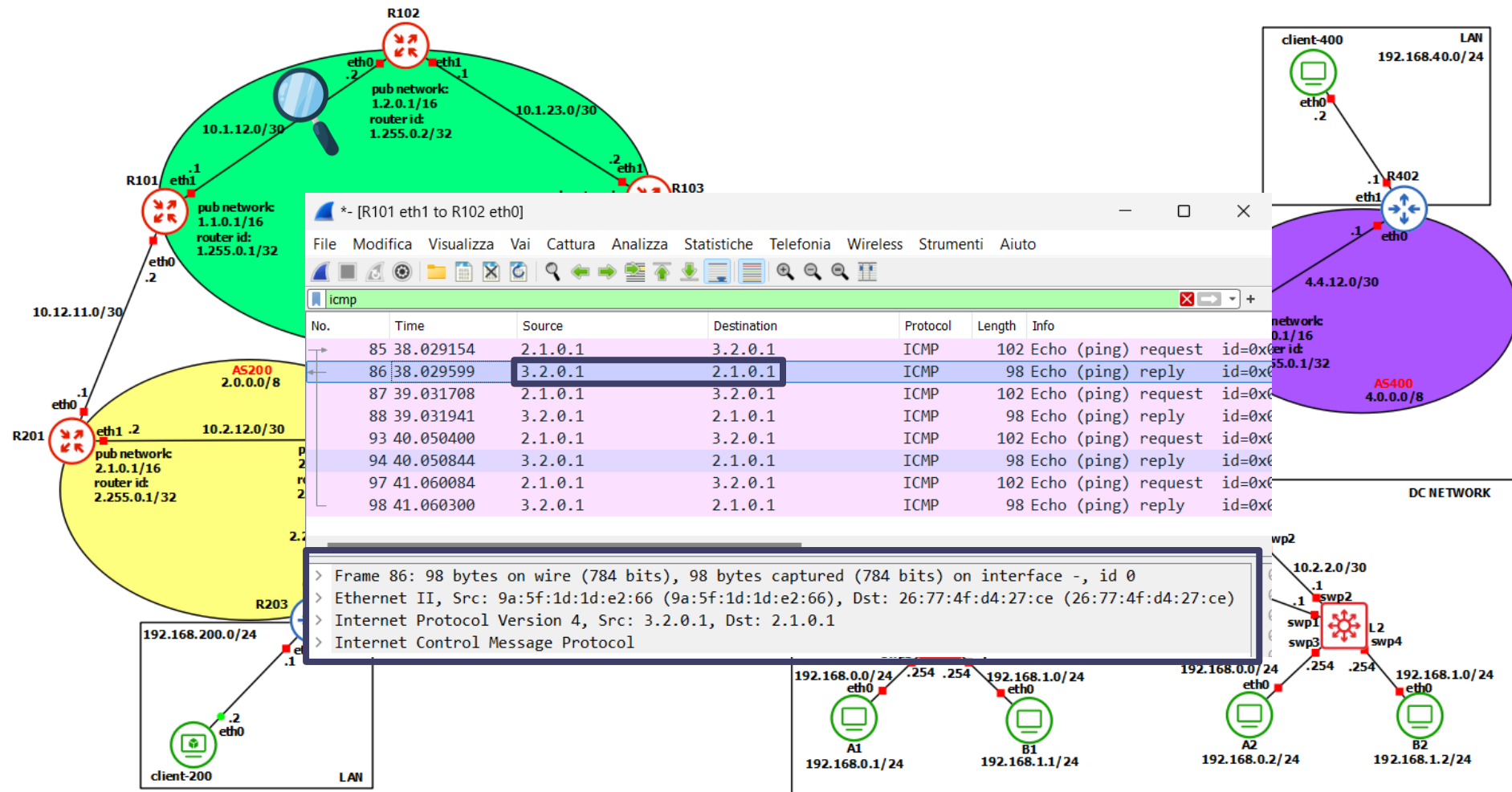
MPLS/LDP



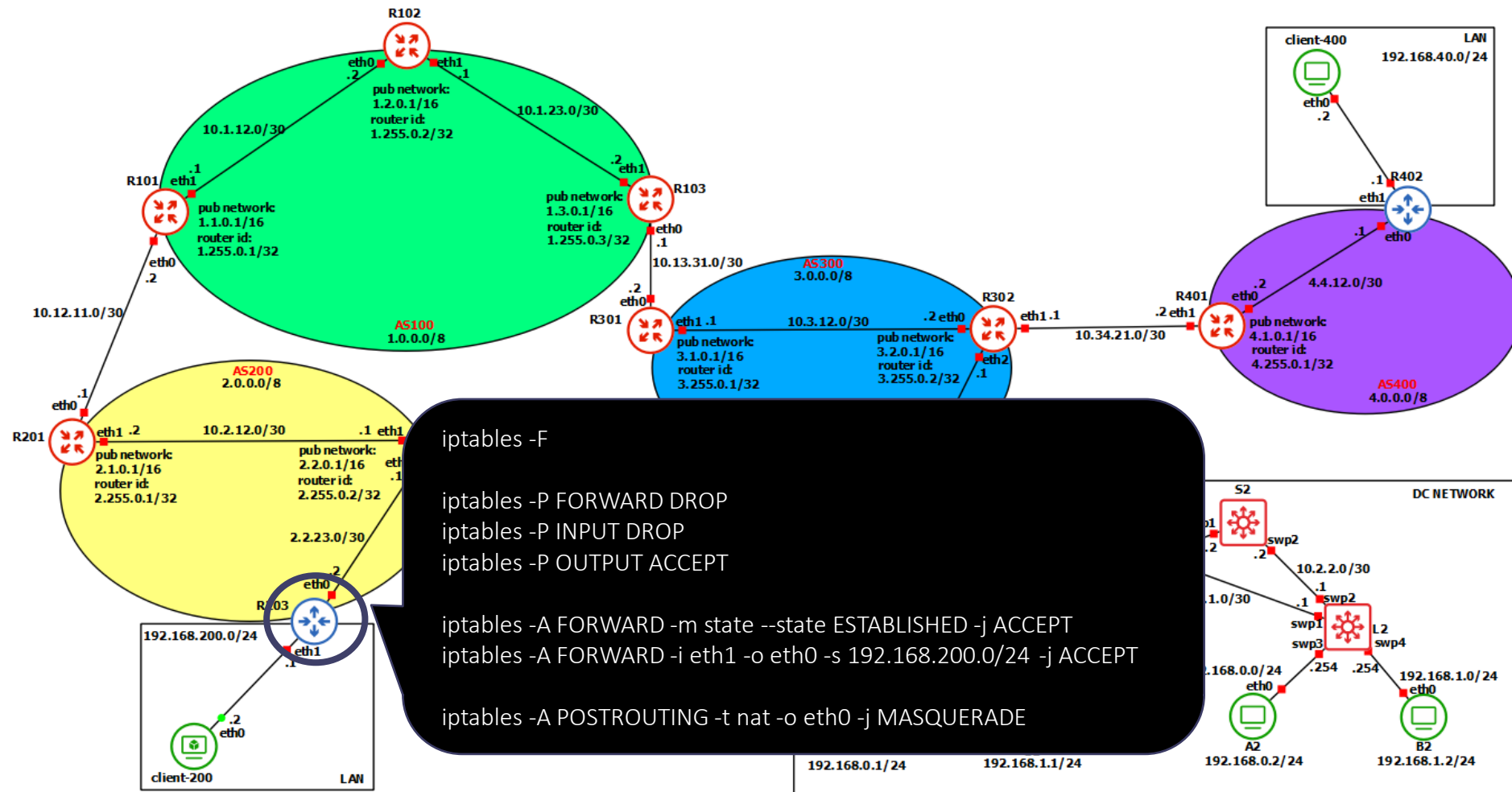
MPLS/LDP



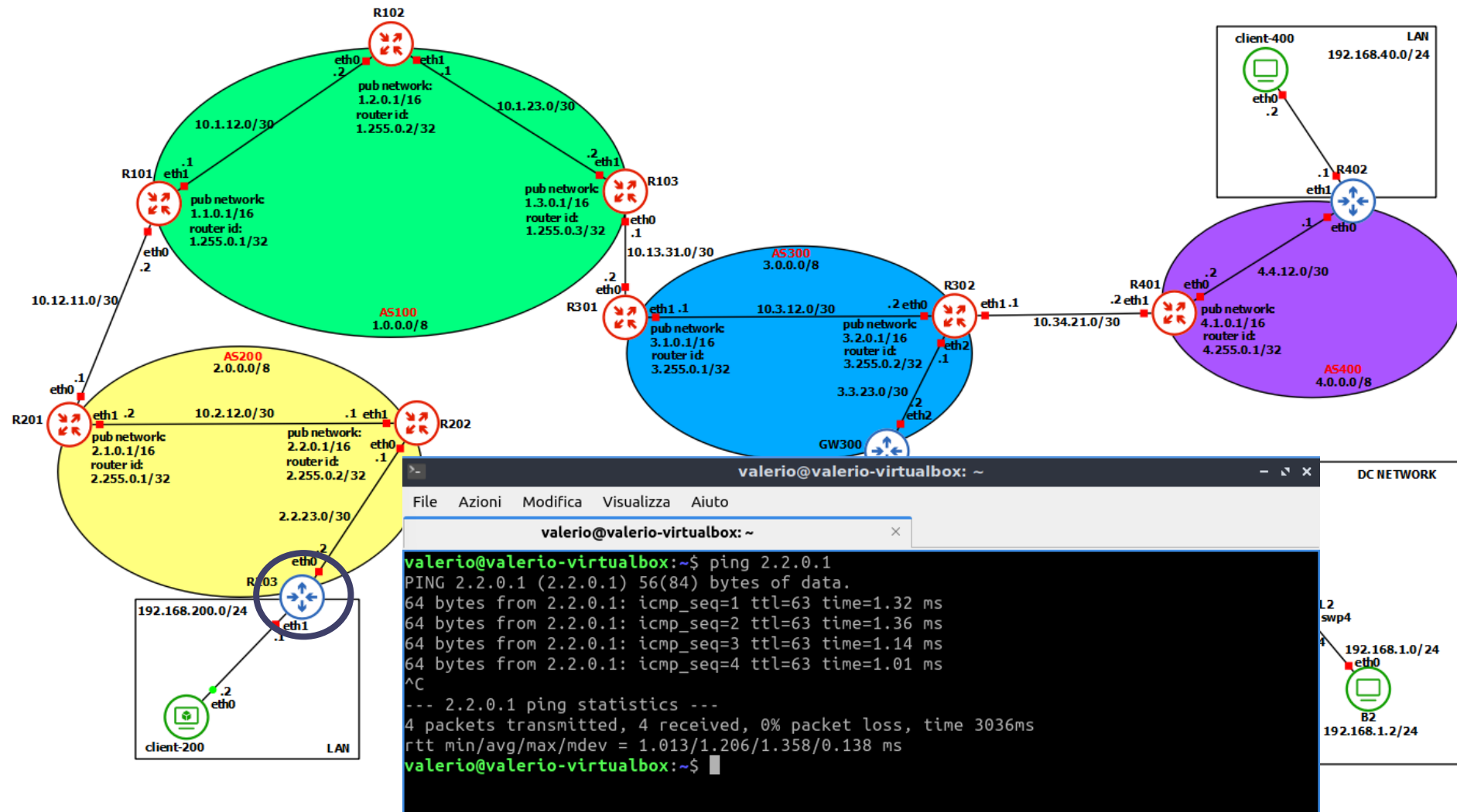
MPLS/LDP



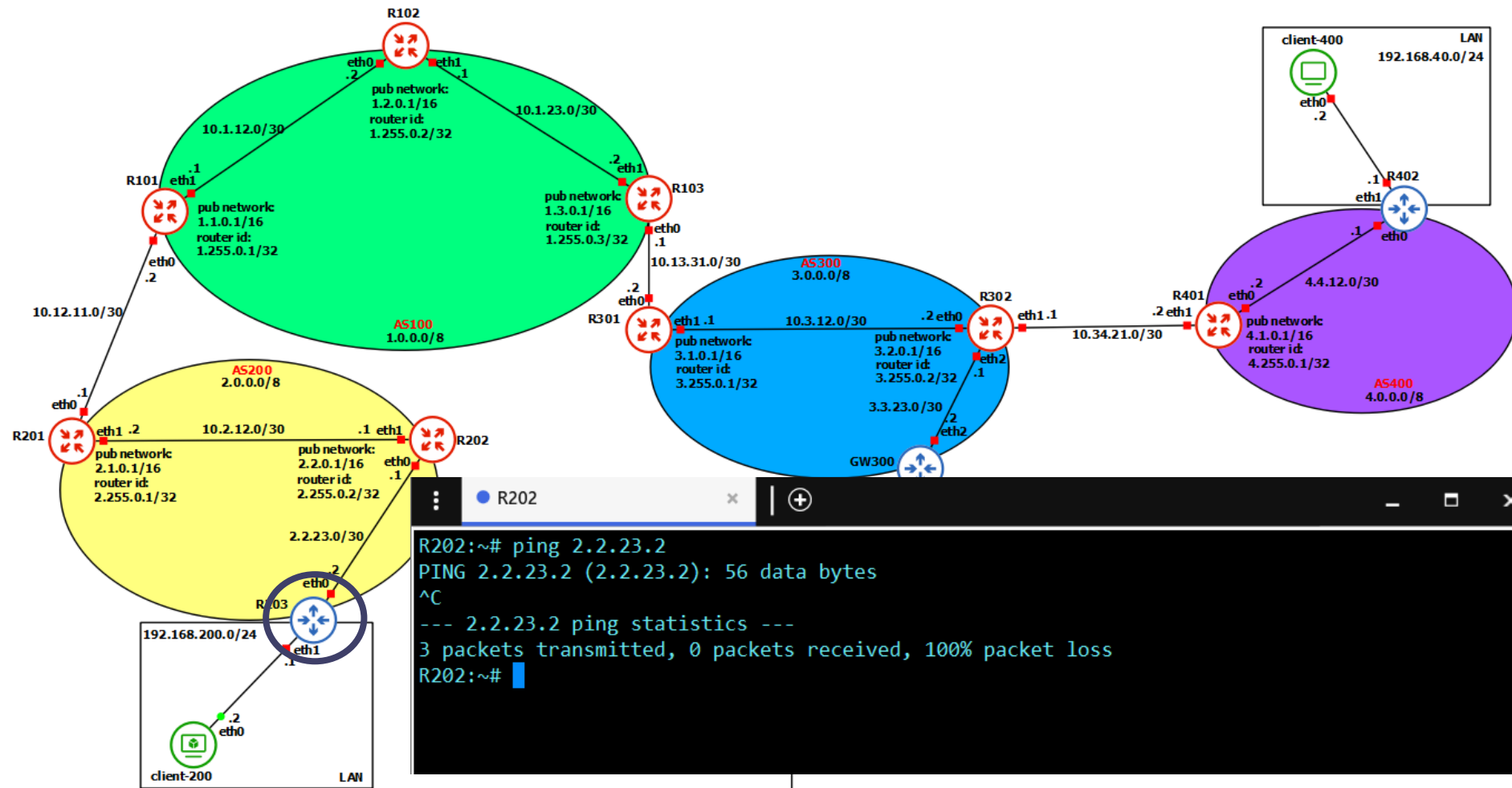
Firewall



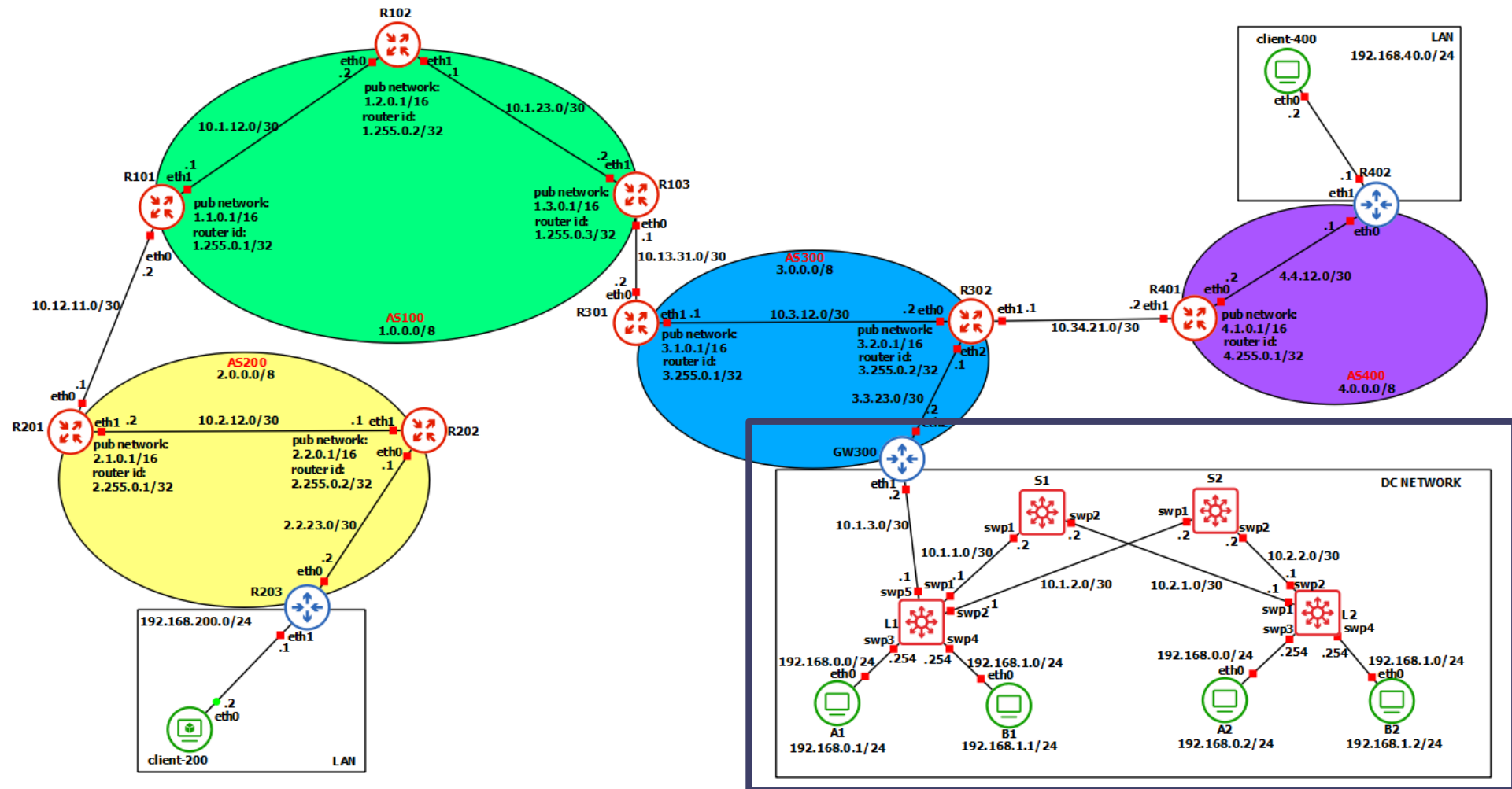
Firewall



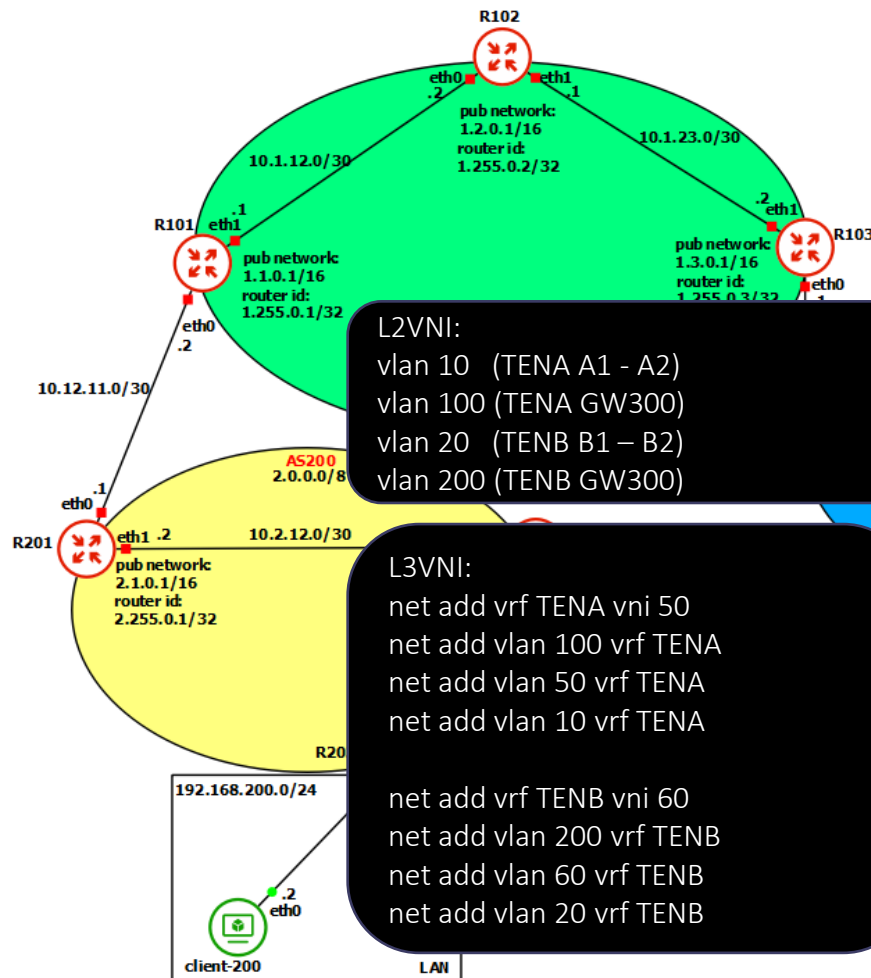
Firewall



DC Network



DC Network



L2VNI:
 vlan 10 (TENA A1 - A2)
 vlan 100 (TENA GW300)
 vlan 20 (TENB B1 - B2)
 vlan 200 (TENB GW300)

L3VNI:
 net add vrf TENA vni 50
 net add vlan 100 vrf TENA
 net add vlan 50 vrf TENA
 net add vlan 10 vrf TENA

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

Links with DC-Network

ip link add link eth1 name eth1.100 type vlan id 100

ip link add link eth1 name eth1.200 type vlan id 200

ip addr add 10.1.3.2/30 dev eth1.100

ip addr add 10.1.3.2/30 dev eth1.200

ip link set eth1.100 up

ip link set eth1.200 up

ip route add 192.168.0.0/24 via 10.1.3.1 dev eth1.100

ip route add 192.168.1.0/24 via 10.1.3.1 dev eth1.200

Configure NAT

iptables -t nat -A POSTROUTING -o eth2 -j MASQUERADE

Block traffic from/to 192.168.0.0/24 to/from 192.168.1.0/24

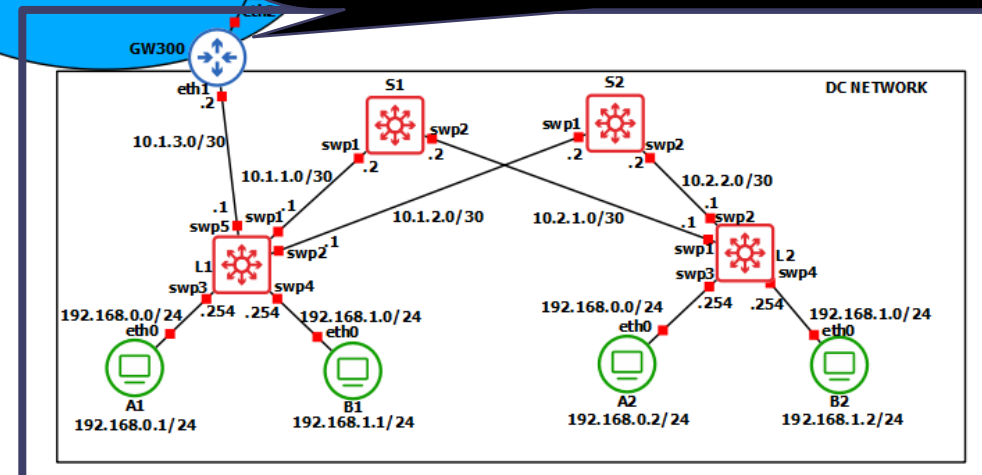
iptables -F FORWARD

iptables -P FORWARD ACCEPT

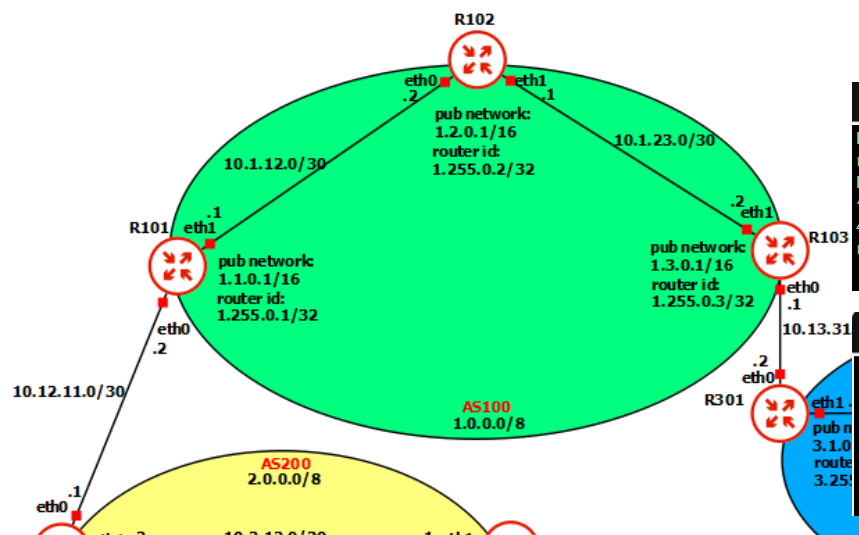
iptables -A FORWARD -m state --state ESTABLISHED -j ACCEPT

iptables -A FORWARD -s 192.168.0.0/24 -d 192.168.1.0/24 -j DROP

iptables -A FORWARD -s 192.168.1.0/24 -d 192.168.0.0/24 -j DROP



DC Network

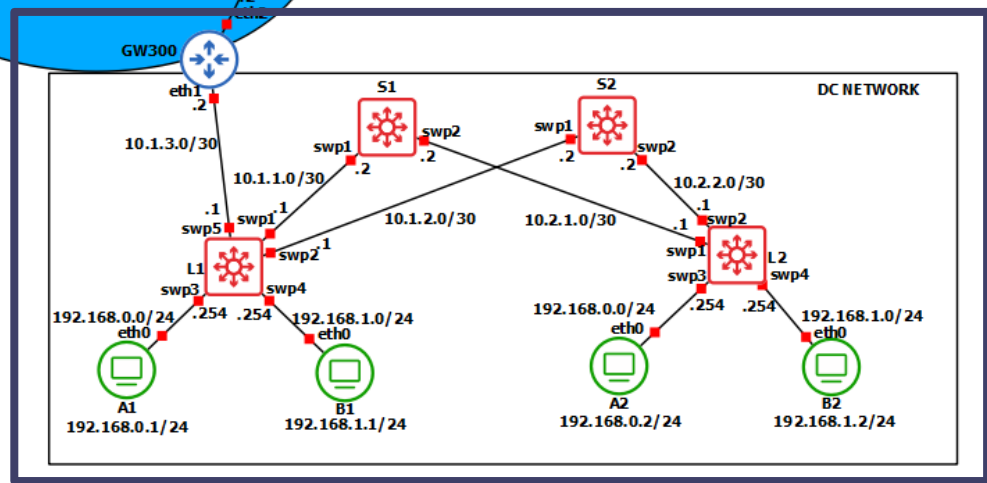


```
client-400 LAN 192.168.40.0/24
B2 console is now available... Press RETURN to get started.
root@B2:~# ping 192.168.0.1
PING 192.168.0.1 (192.168.0.1): 56 data bytes
^C--- 192.168.0.1 ping statistics ---
4 packets transmitted, 0 packets received, 100% packet loss
root@B2:~#
```

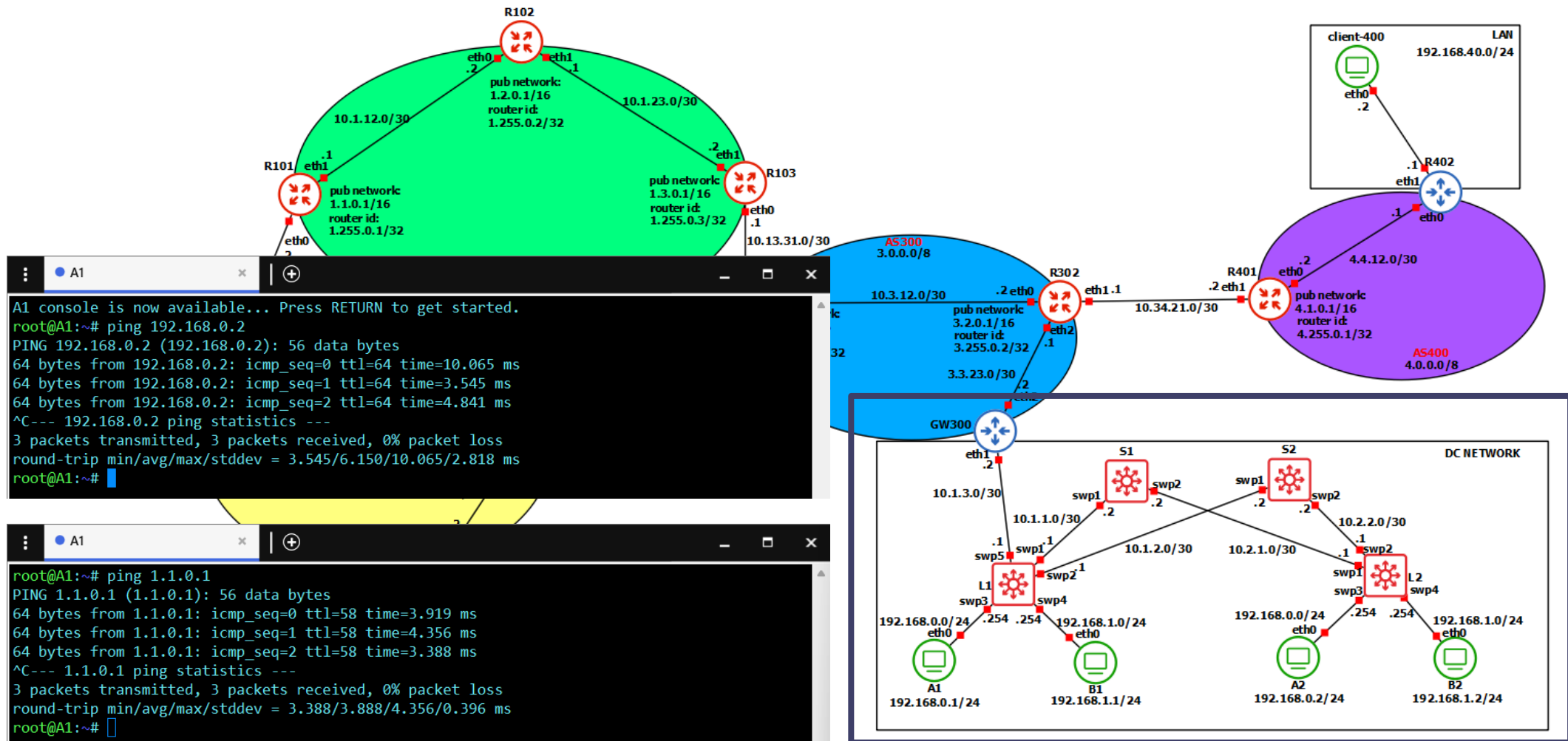
```
root@B2:~# ping 192.168.0.2
PING 192.168.0.2 (192.168.0.2): 56 data bytes
^C--- 192.168.0.2 ping statistics ---
3 packets transmitted, 0 packets received, 100% packet loss
root@B2:~#
```

```
root@A1:~# ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1): 56 data bytes
^C--- 192.168.1.1 ping statistics ---
4 packets transmitted, 0 packets received, 100% packet loss
root@A1:~#
```

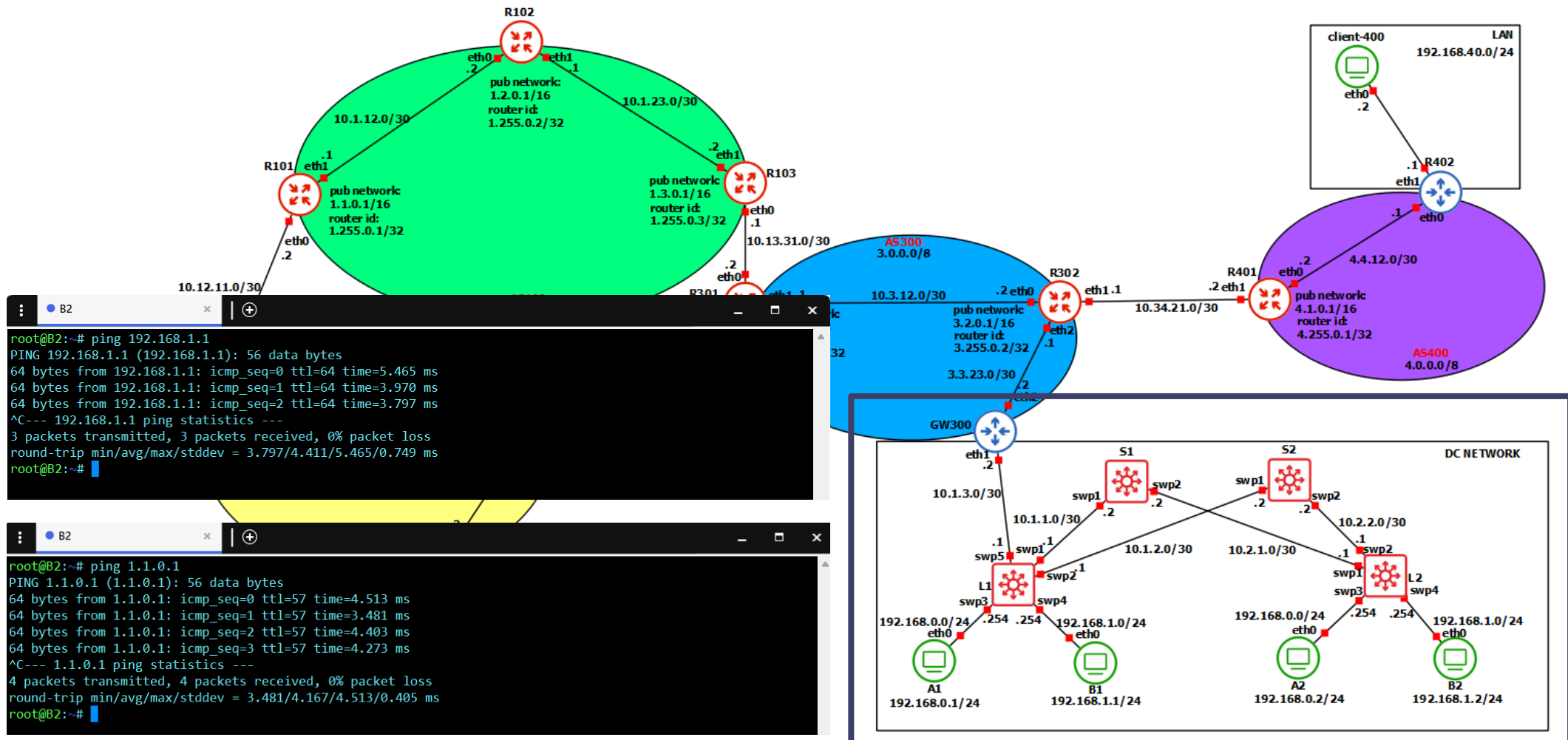
```
root@A1:~# ping 192.168.1.2
PING 192.168.1.2 (192.168.1.2): 56 data bytes
^C--- 192.168.1.2 ping statistics ---
2 packets transmitted, 0 packets received, 100% packet loss
root@A1:~#
```



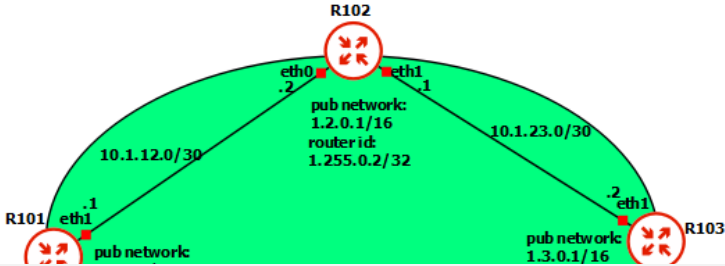
DC Network



DC Network



DC Network (B2 -> B1)



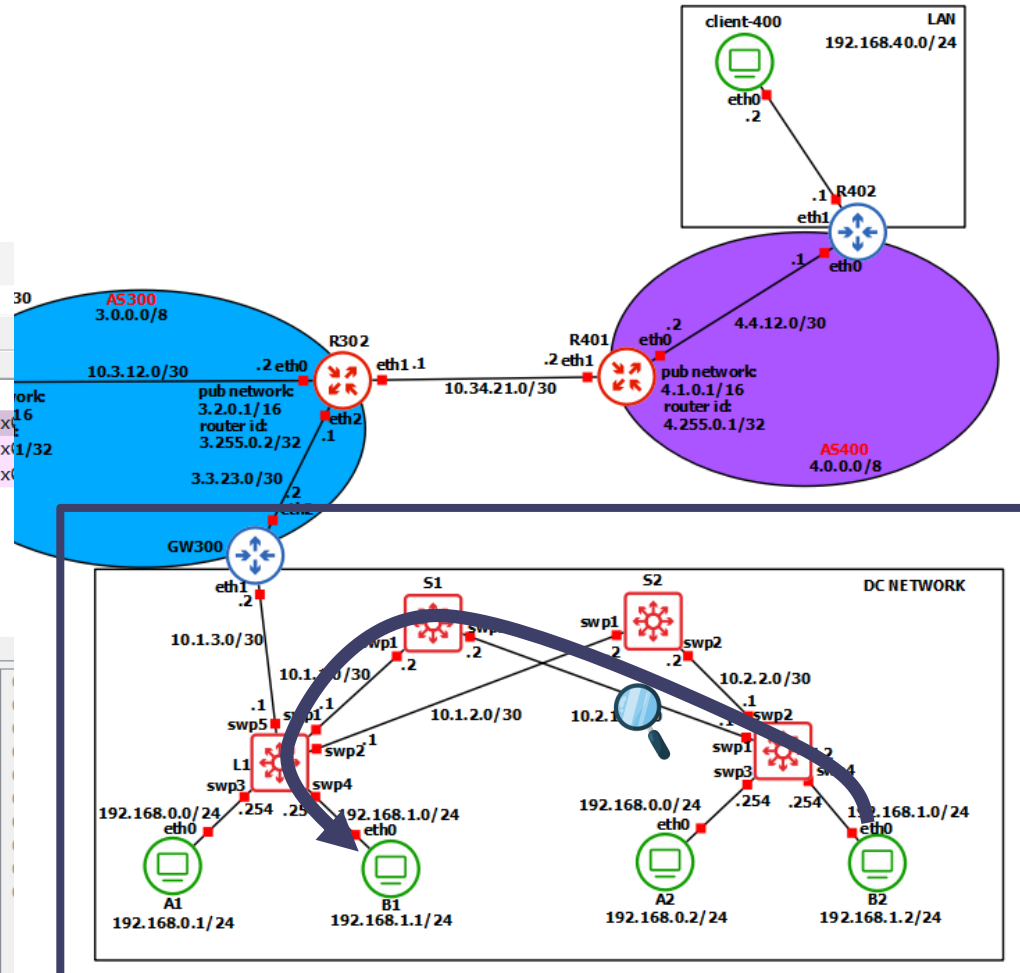
Network diagram showing three routers (R101, R102, R103) connected in a triangle. R102 is at the top, R101 at the bottom left, and R103 at the bottom right. Each router has a public network (1.2.0.1/16, 1.3.0.1/16, 1.255.0.2/32) and interfaces eth0 and eth1. The connections are labeled with IP ranges: 10.1.12.0/30 between R101 and R102, 10.1.23.0/30 between R102 and R103, and 10.1.3.0/30 between R101 and R103.

Packet capture details for ICMP (ping) requests:

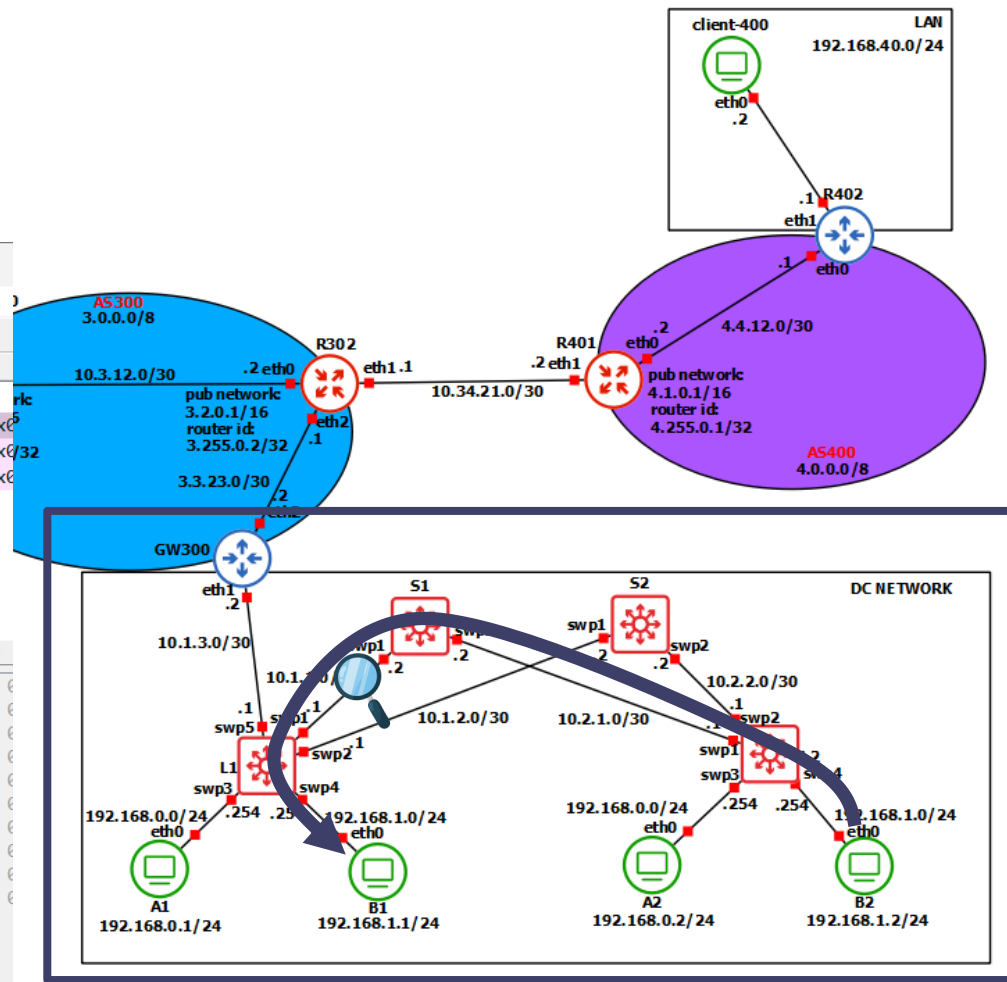
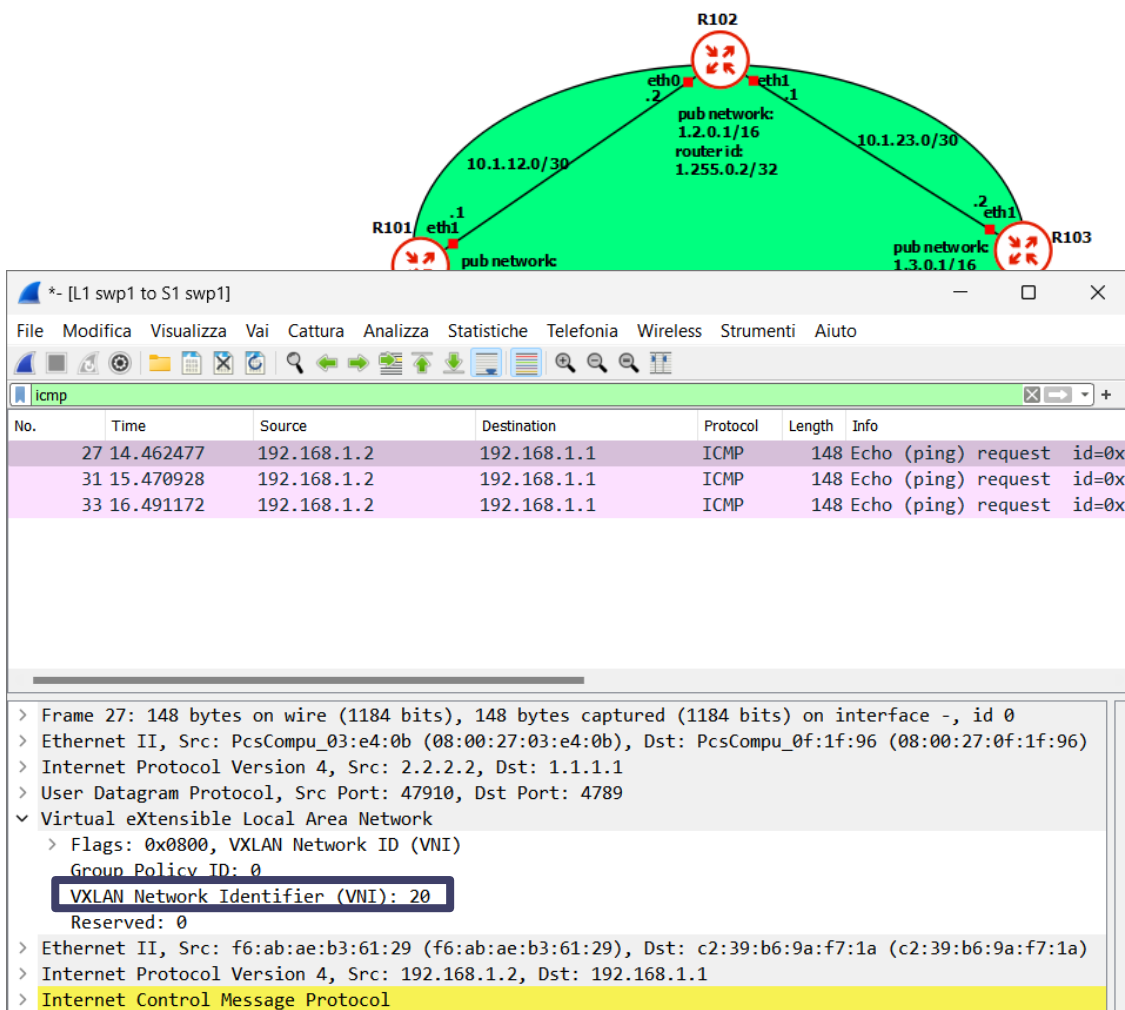
No.	Time	Source	Destination	Protocol	Length	Info
36	20.304300	192.168.1.2	192.168.1.1	ICMP	148	Echo (ping) request id=0xc...
38	21.312577	192.168.1.2	192.168.1.1	ICMP	148	Echo (ping) request id=0xc...
39	22.333101	192.168.1.2	192.168.1.1	ICMP	148	Echo (ping) request id=0xc...

Frame 36 details:

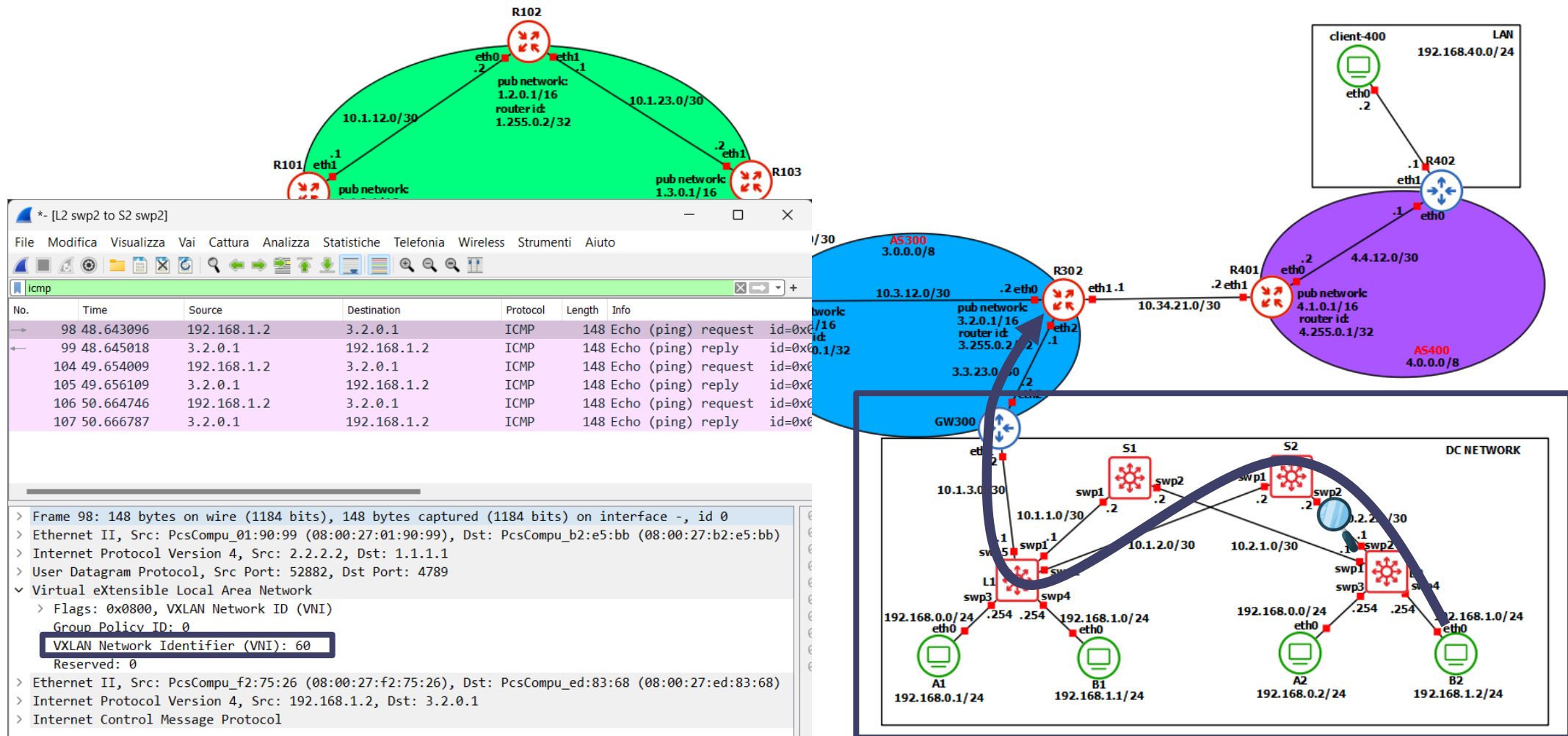
- Frame 36: 148 bytes on wire (1184 bits), 148 bytes captured (1184 bits) on interface -, id 0
- Ethernet II, Src: PcsCompu_b1:9f:d4 (08:00:27:b1:9f:d4), Dst: PcsCompu_42:2c:0e (08:00:27:42:2c:0e)
- Internet Protocol Version 4, Src: 2.2.2.2, Dst: 1.1.1.1
- User Datagram Protocol, Src Port: 47910, Dst Port: 4789
- Virtual eXtensible Local Area Network
 - Flags: 0x0800, VXLAN Network ID (VNI)
 - Group Policy ID: 0
 - VXLAN Network Identifier (VNI): 20**
 - Reserved: 0
- Ethernet II, Src: f6:ab:ae:b3:61:29 (f6:ab:ae:b3:61:29), Dst: c2:39:b6:9a:f7:1a (c2:39:b6:9a:f7:1a)
- Internet Protocol Version 4, Src: 192.168.1.2, Dst: 192.168.1.1
- Internet Control Message Protocol



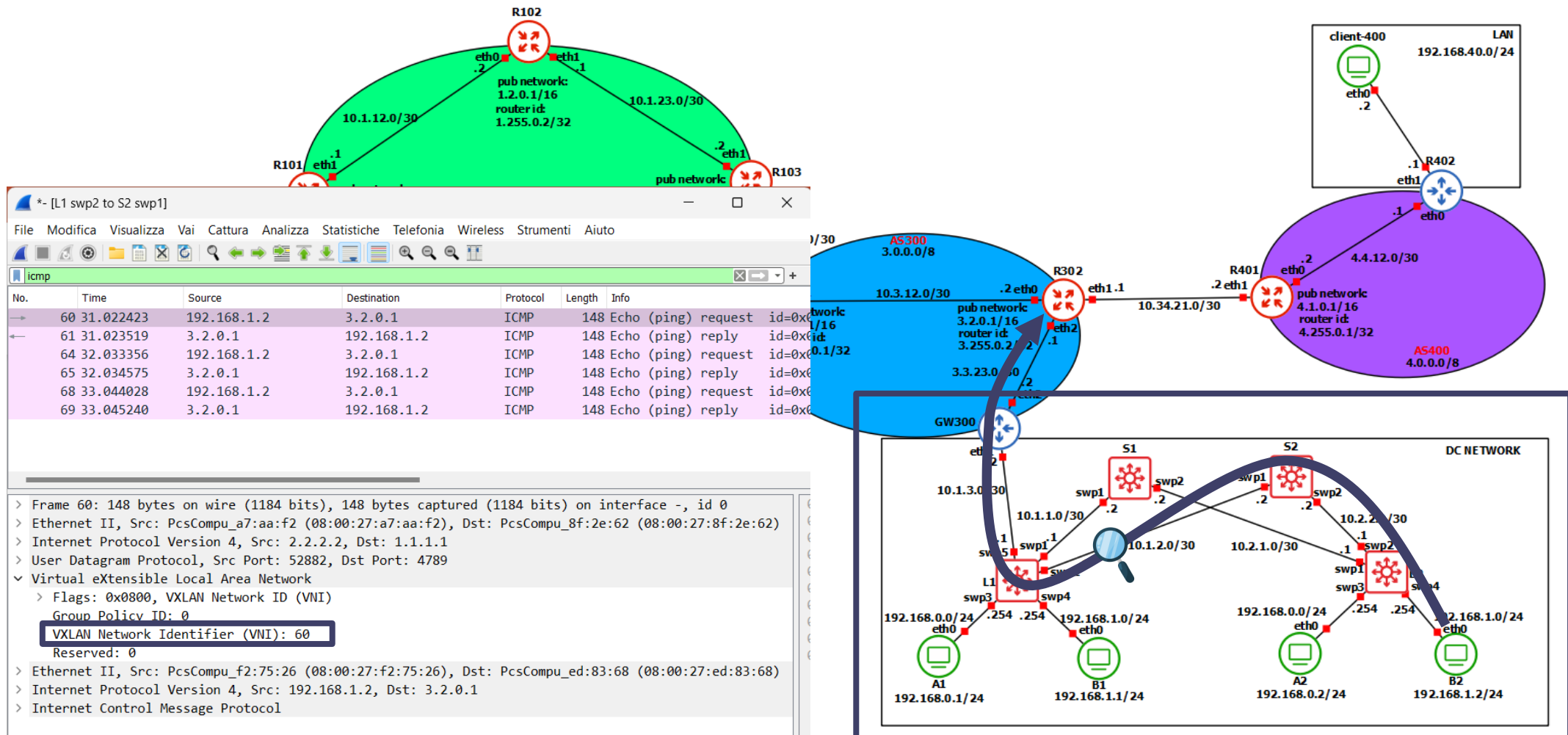
DC Network (B2 -> B1)



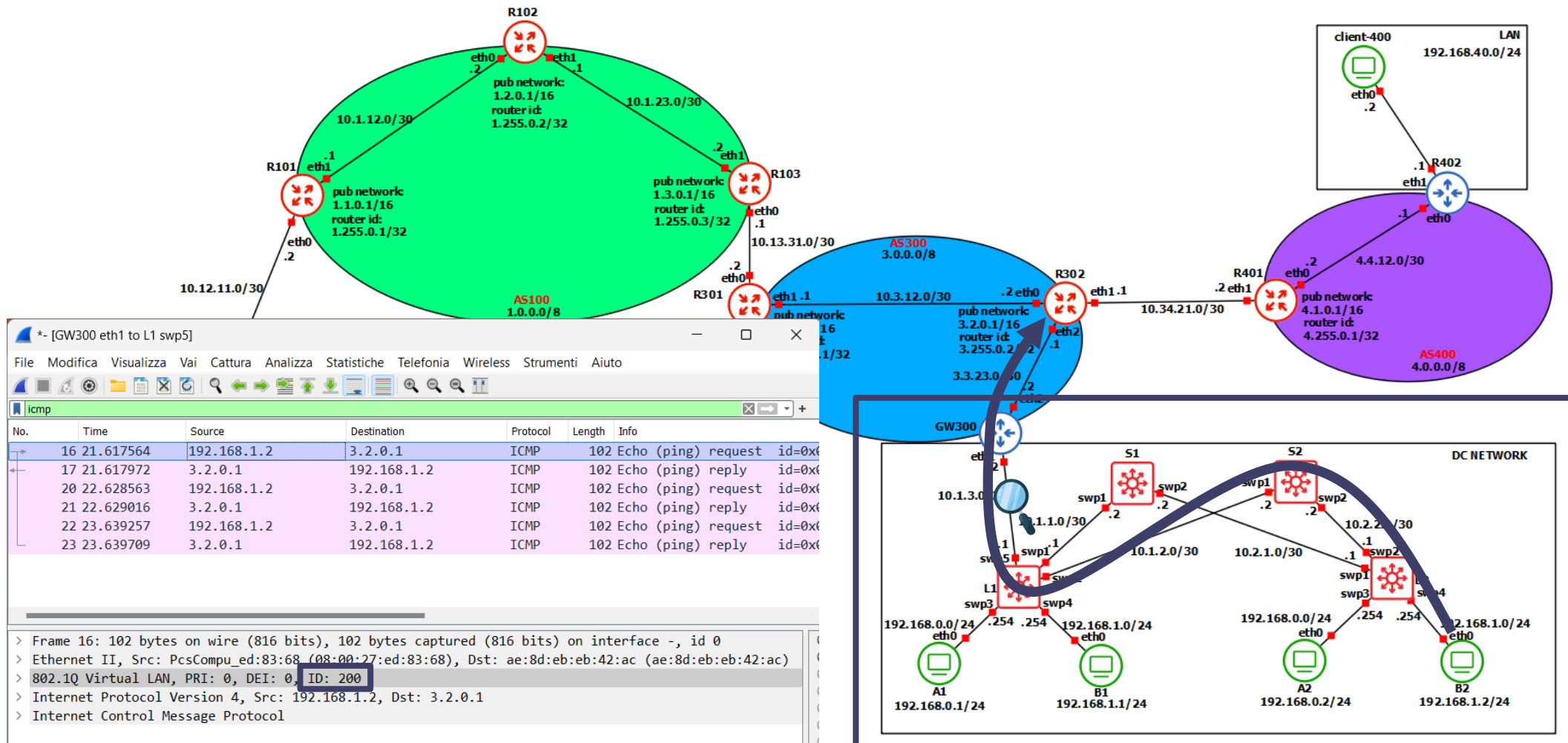
DC Network (B2 -> R302)



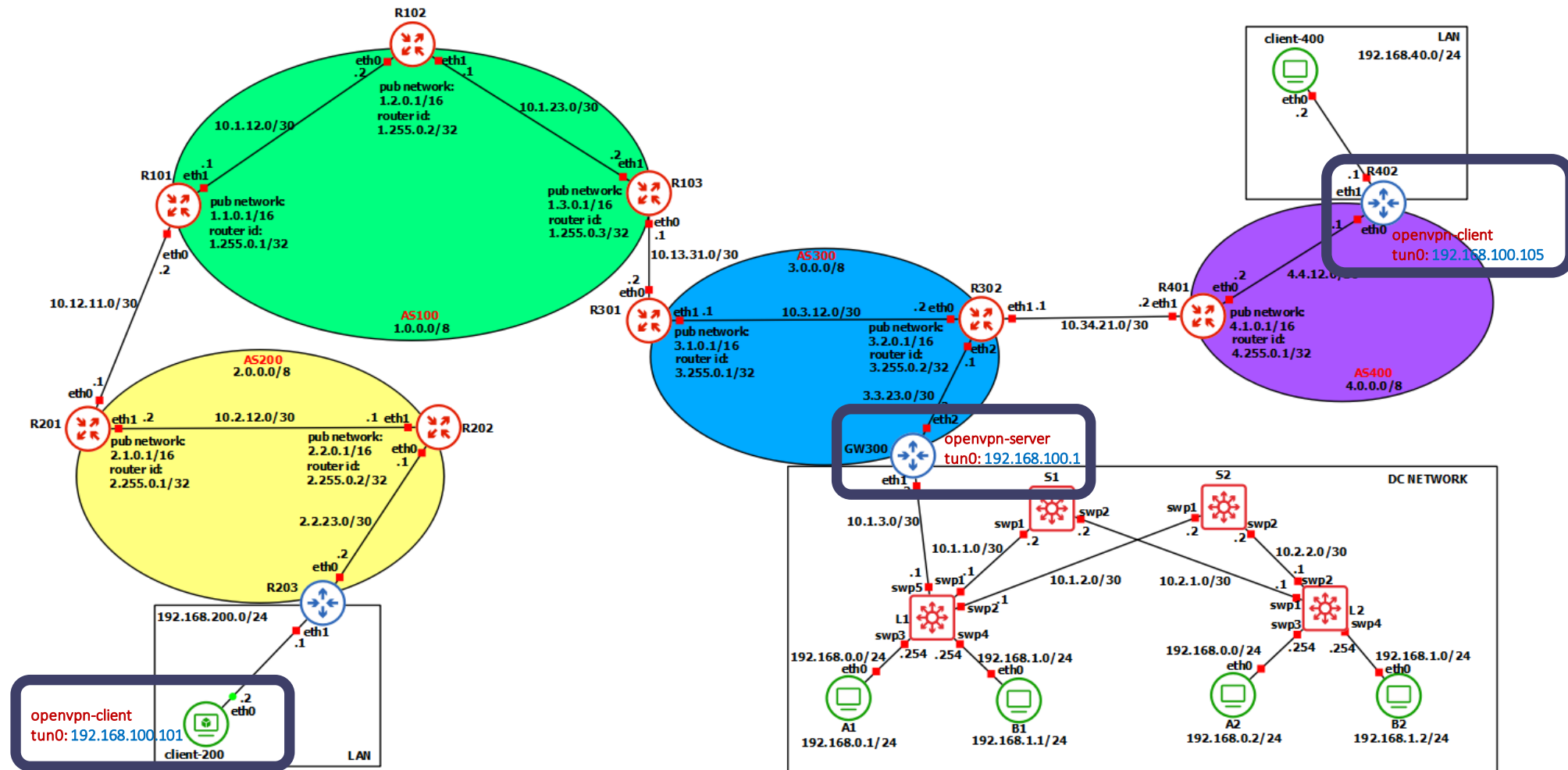
DC Network (B2 -> R302)



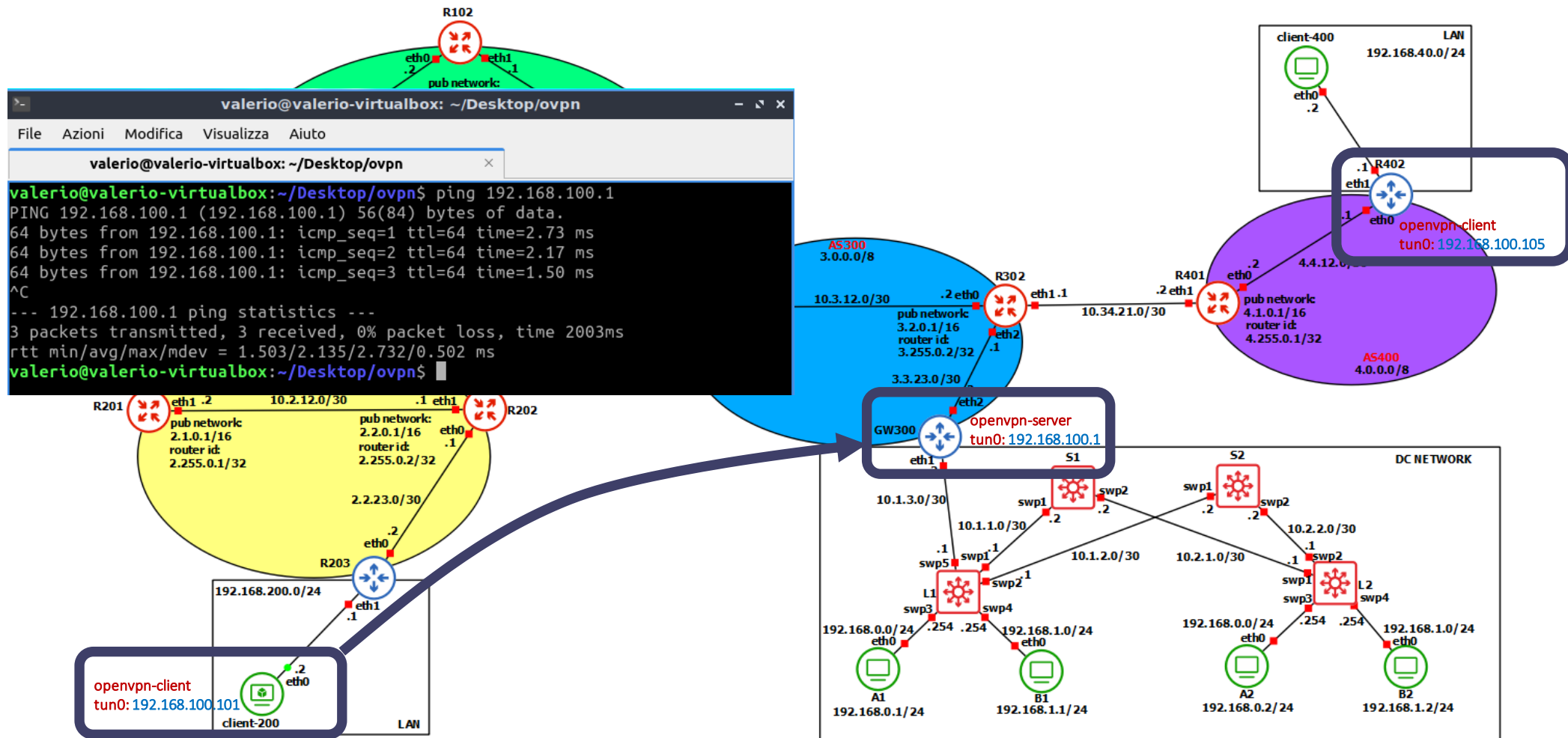
DC Network (B2 -> R302)



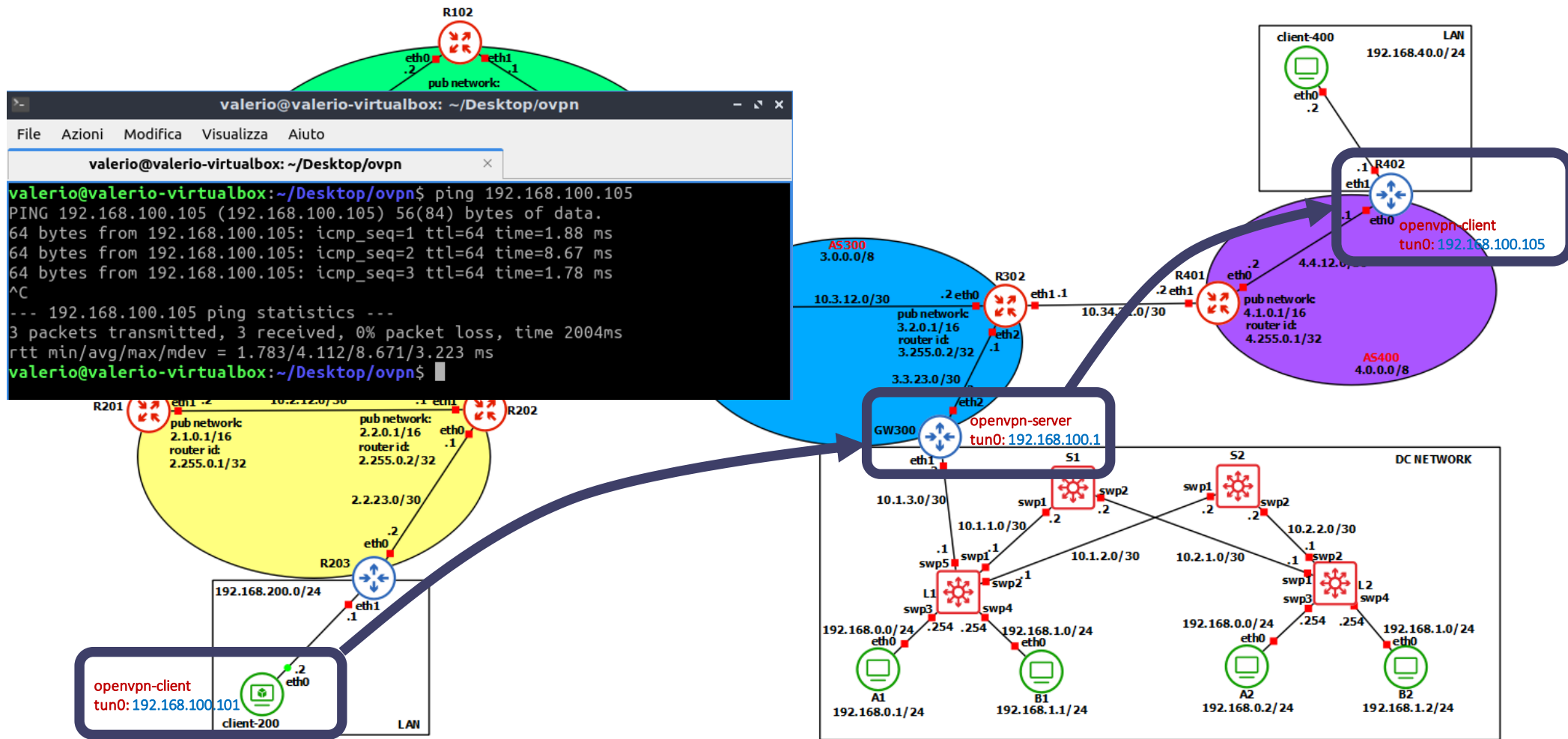
OpenVPN



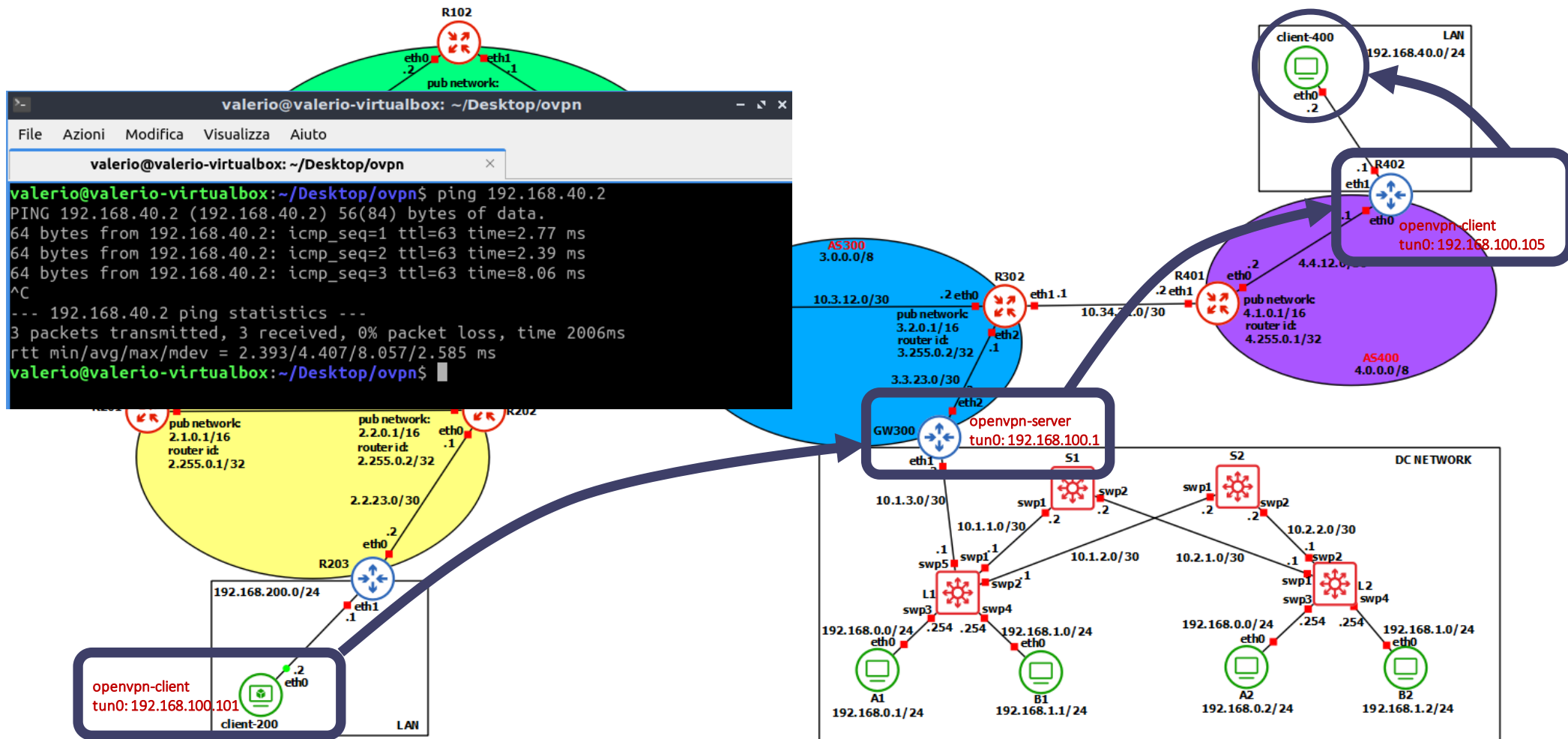
OpenVPN



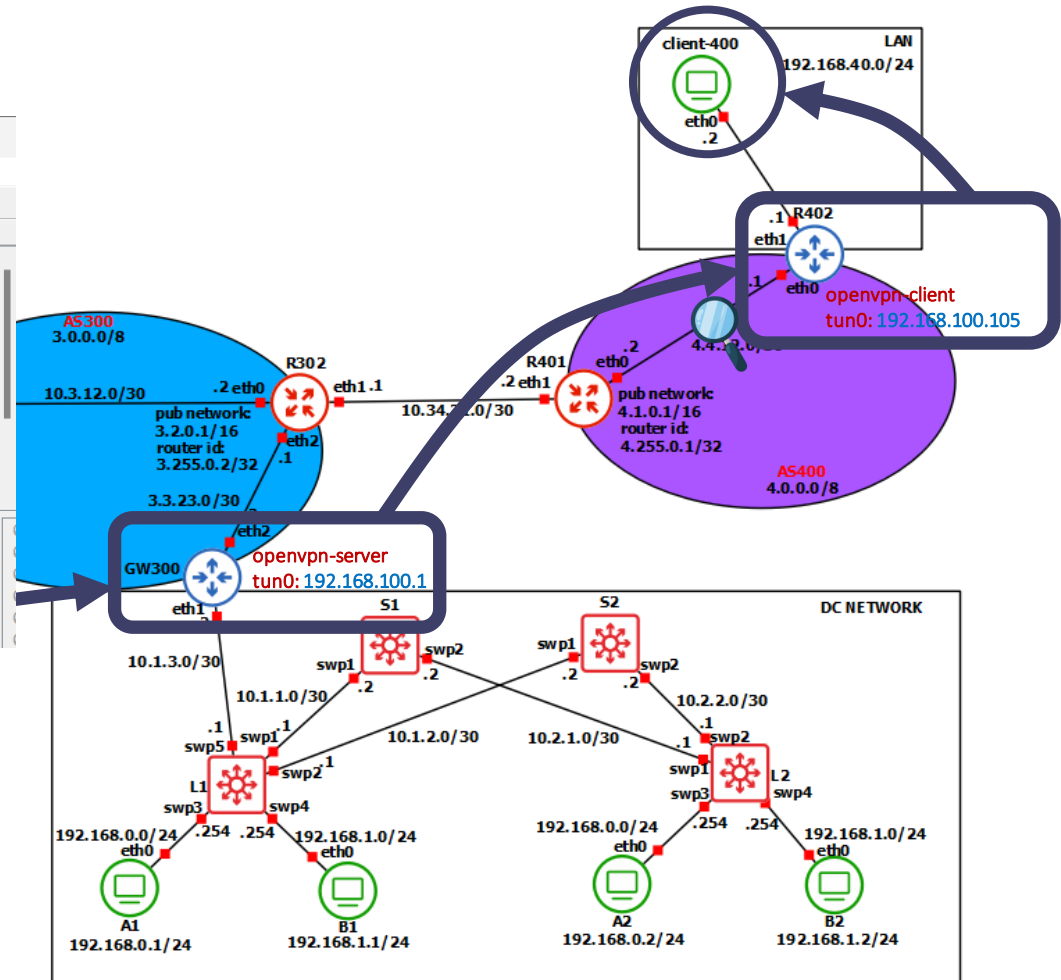
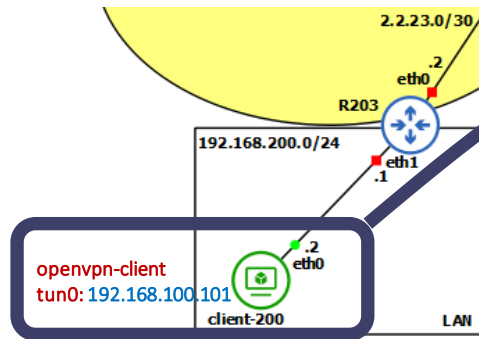
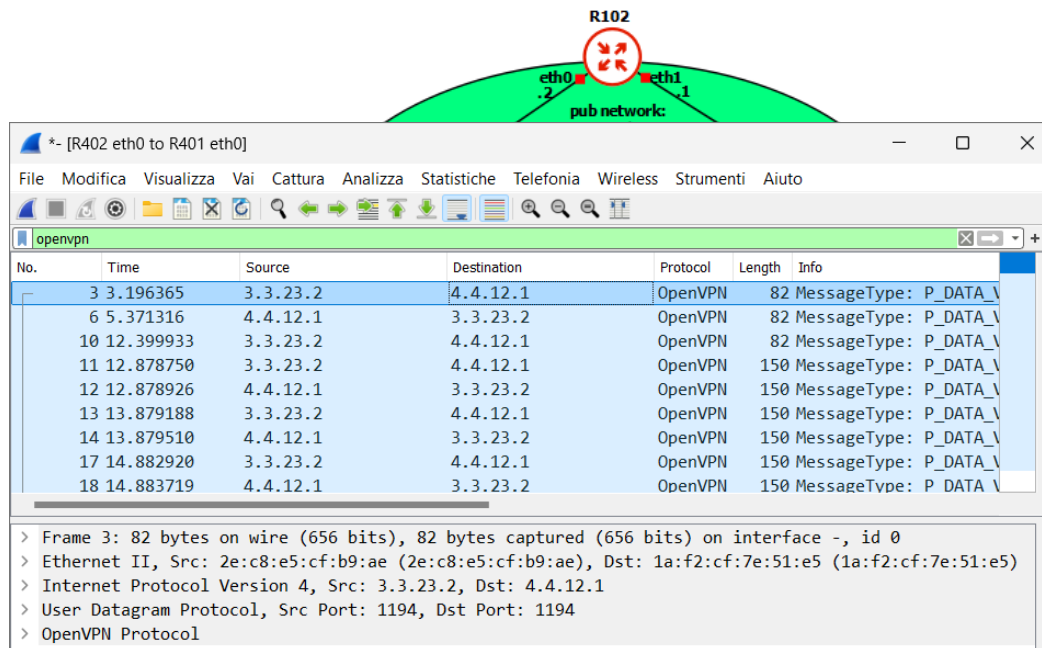
OpenVPN



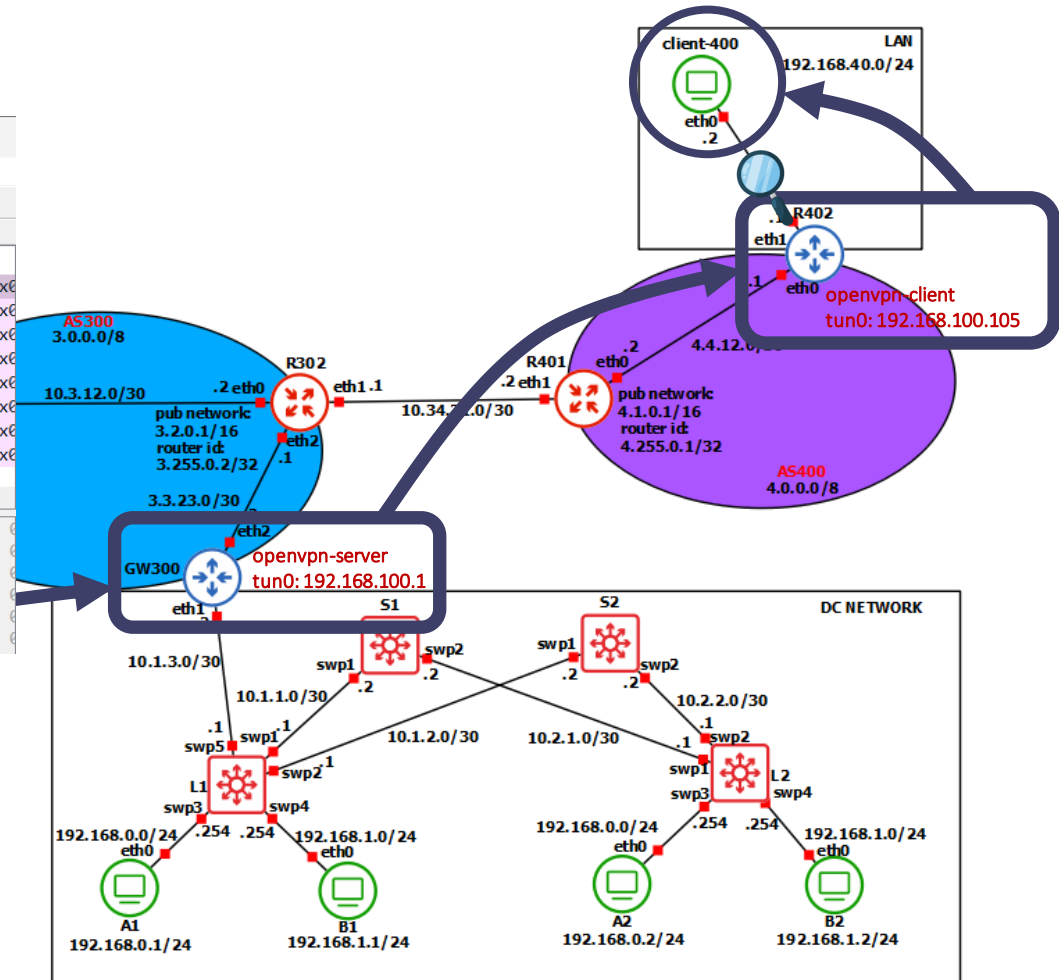
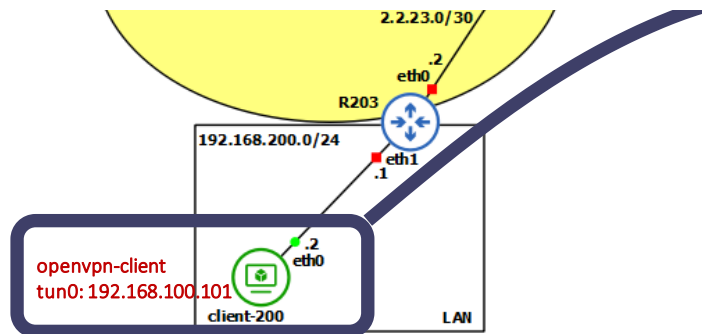
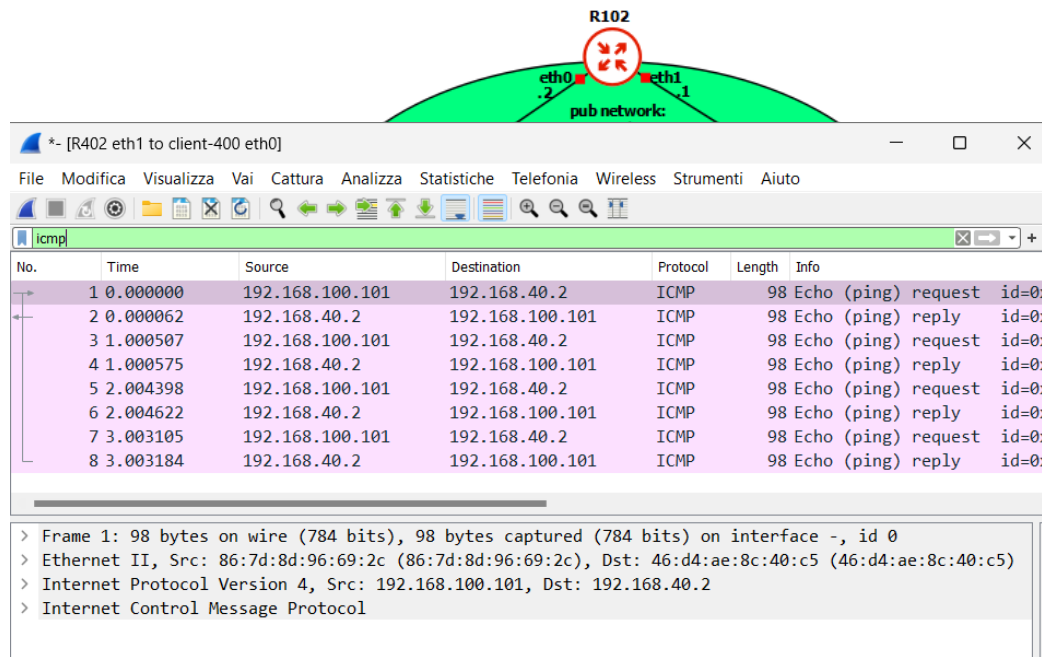
OpenVPN



OpenVPN



OpenVPN



OpenVPN

```
valerio@valerio-virtualbox: ~/Desktop/ovpn
File Azioni Modifica Visualizza Aiuto

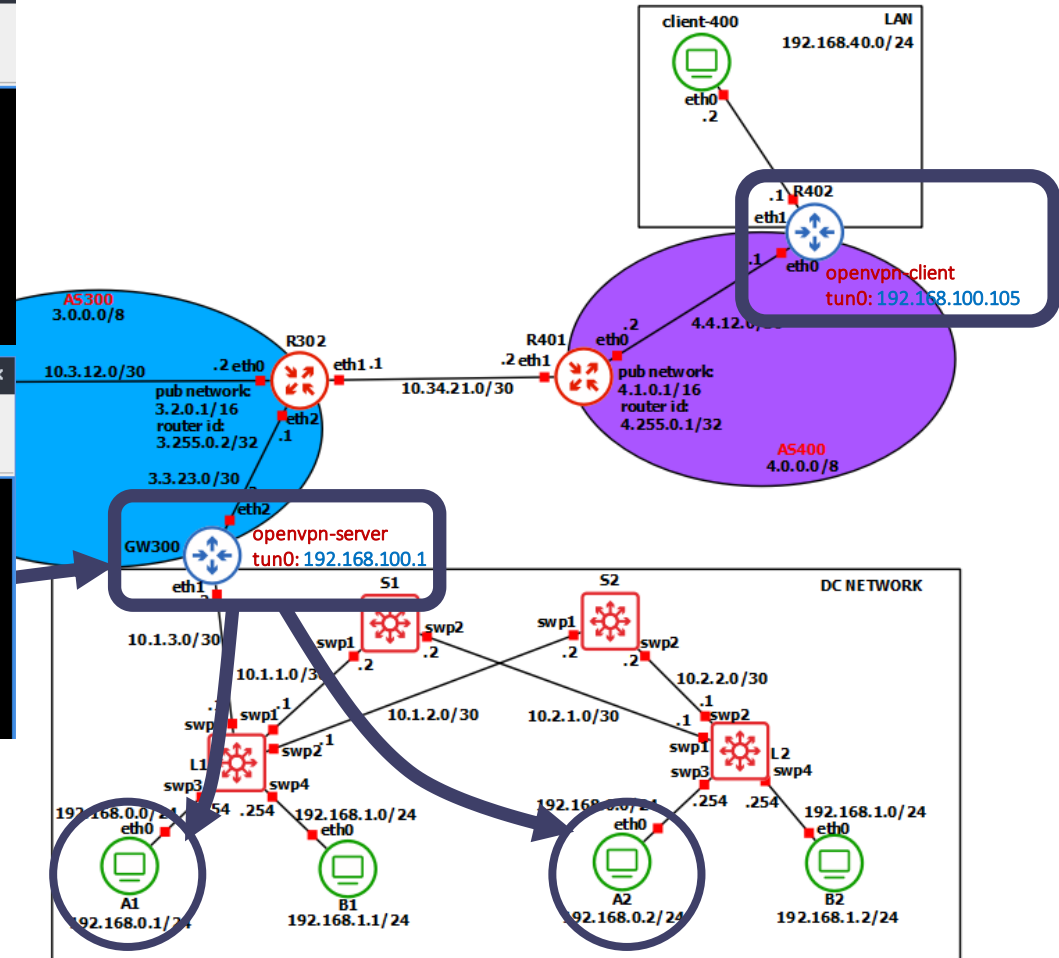
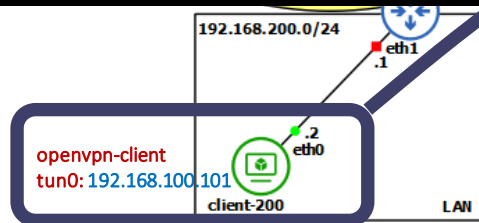
valerio@valerio-virtualbox: ~/Desktop/ovpn

valerio@valerio-virtualbox:~/Desktop/ovpn$ ping 192.168.0.1
PING 192.168.0.1 (192.168.0.1) 56(84) bytes of data.
64 bytes from 192.168.0.1: icmp_seq=1 ttl=62 time=3.48 ms
64 bytes from 192.168.0.1: icmp_seq=2 ttl=62 time=4.66 ms
^C
--- 192.168.0.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 3.477/4.066/4.656/0.589 ms
valerio@valerio-virtualbox:~/Desktop/ovpn$
```

```
valerio@valerio-virtualbox: ~/Desktop/ovpn
File Azioni Modifica Visualizza Aiuto

valerio@valerio-virtualbox: ~/Desktop/ovpn

valerio@valerio-virtualbox:~/Desktop/ovpn$ ping 192.168.0.2
PING 192.168.0.2 (192.168.0.2) 56(84) bytes of data.
64 bytes from 192.168.0.2: icmp_seq=1 ttl=61 time=6.73 ms
64 bytes from 192.168.0.2: icmp_seq=2 ttl=61 time=4.39 ms
^C
--- 192.168.0.2 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 4.394/5.560/6.726/1.166 ms
valerio@valerio-virtualbox:~/Desktop/ovpn$
```



OpenVPN

R102

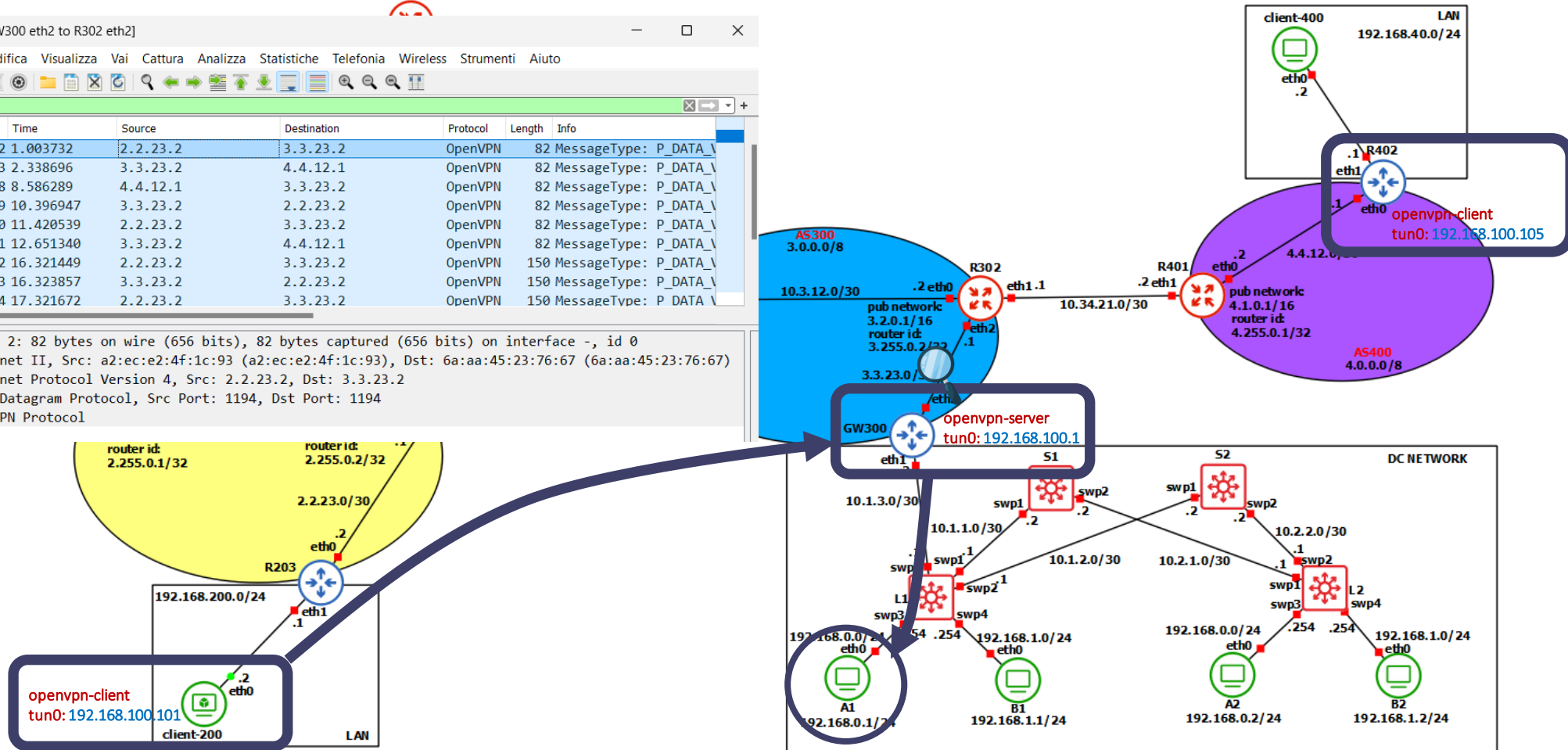
*- [GW300 eth2 to R302 eth2]

File Modifica Visualizza Vai Cattura Analizza Statistiche Telefonia Wireless Strumenti Aiuto

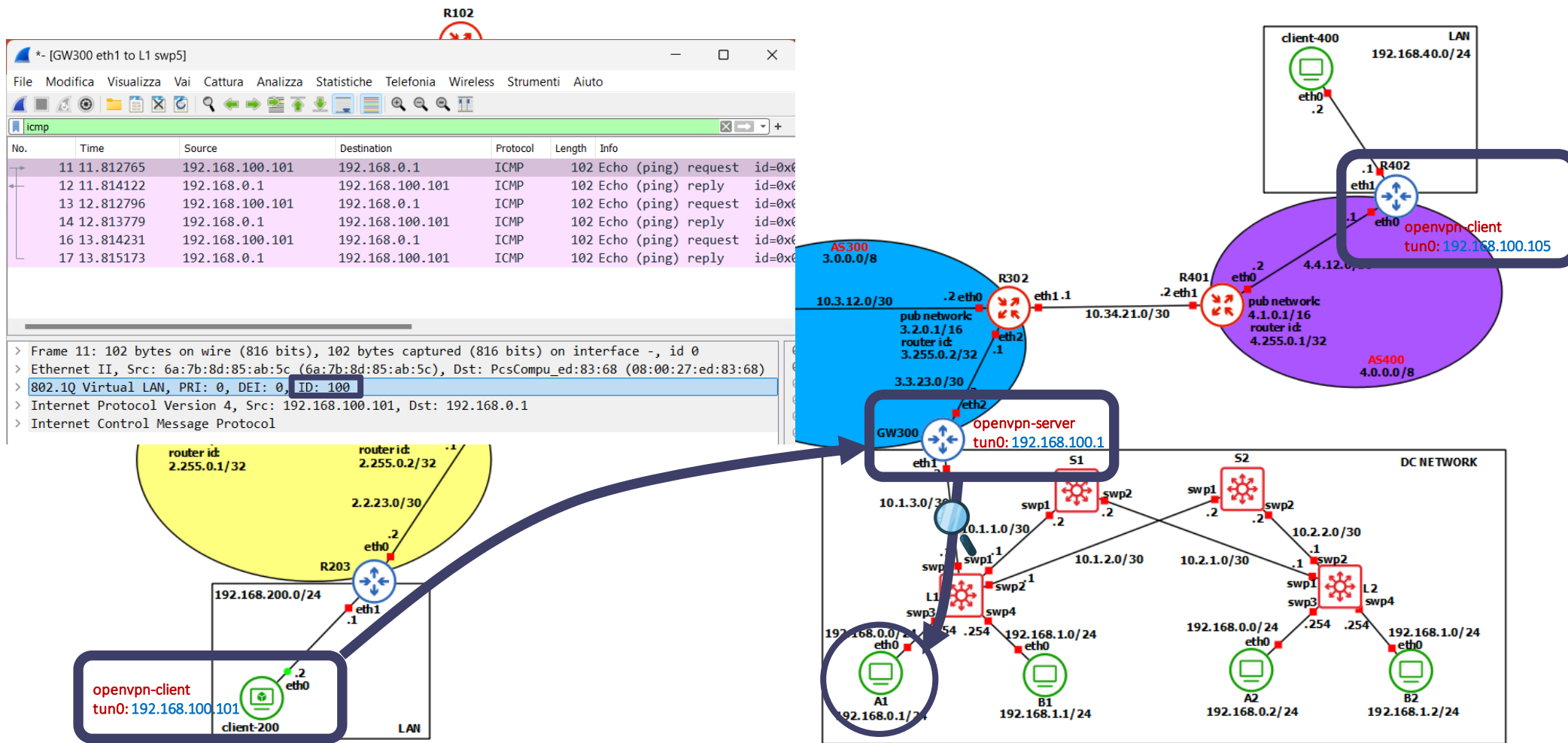
openvpn

No.	Time	Source	Destination	Protocol	Length	Info
2	1.003732	2.2.23.2	3.3.23.2	OpenVPN	82	MessageType: P_DATA_V
3	2.338696	3.3.23.2	4.4.12.1	OpenVPN	82	MessageType: P_DATA_V
8	8.586289	4.4.12.1	3.3.23.2	OpenVPN	82	MessageType: P_DATA_V
9	10.396947	3.3.23.2	2.2.23.2	OpenVPN	82	MessageType: P_DATA_V
10	11.420539	2.2.23.2	3.3.23.2	OpenVPN	82	MessageType: P_DATA_V
11	12.651340	3.3.23.2	4.4.12.1	OpenVPN	82	MessageType: P_DATA_V
12	16.321449	2.2.23.2	3.3.23.2	OpenVPN	150	MessageType: P_DATA_V
13	16.323857	3.3.23.2	2.2.23.2	OpenVPN	150	MessageType: P_DATA_V
14	17.321672	2.2.23.2	3.3.23.2	OpenVPN	150	MessageType: P_DATA_V

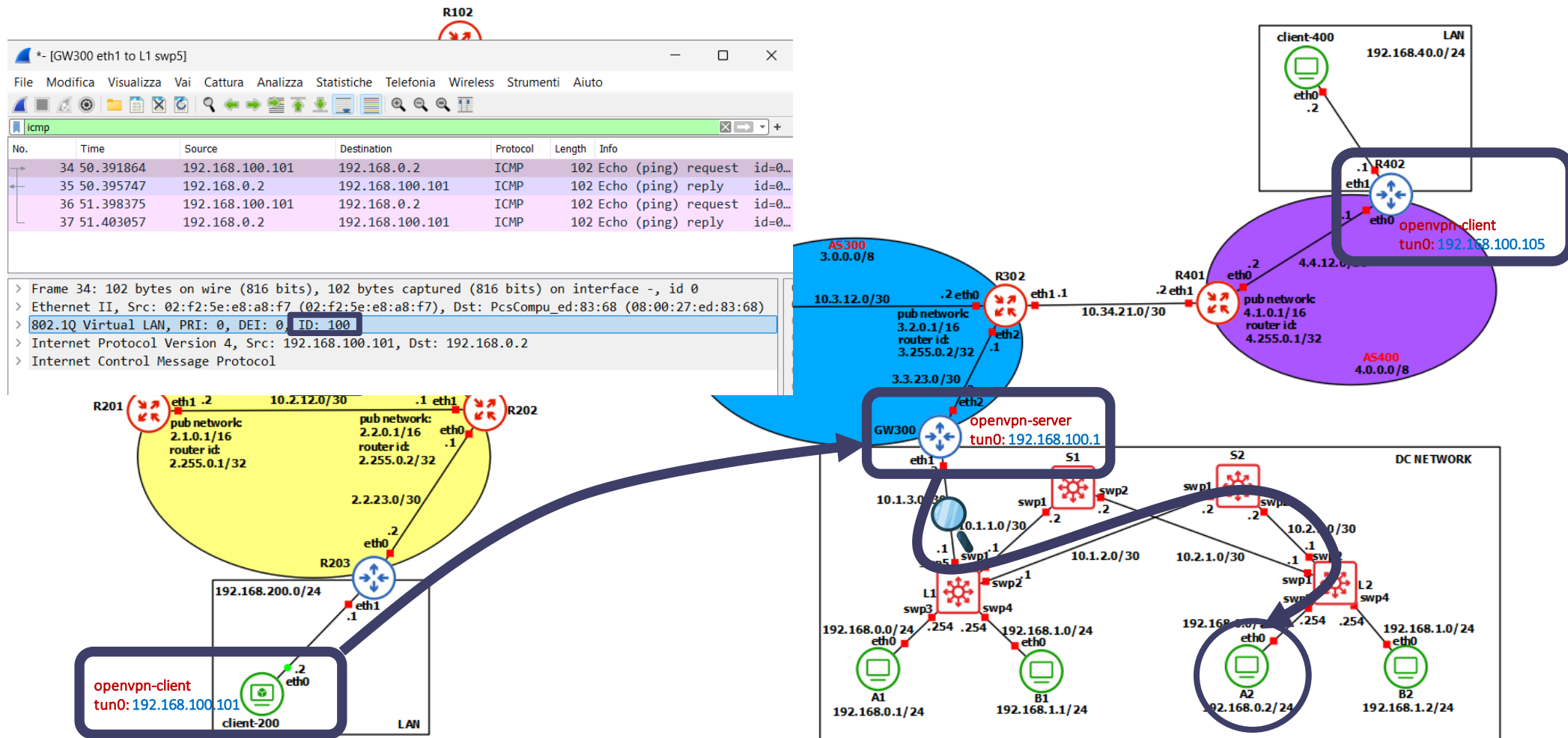
> Frame 2: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface -, id 0
> Ethernet II, Src: a2:ec:e2:4f:1c:93 (a2:ec:e2:4f:1c:93), Dst: 6a:aa:45:23:76:67 (6a:aa:45:23:76:67)
> Internet Protocol Version 4, Src: 2.2.23.2, Dst: 3.3.23.2
> User Datagram Protocol, Src Port: 1194, Dst Port: 1194
> OpenVPN Protocol



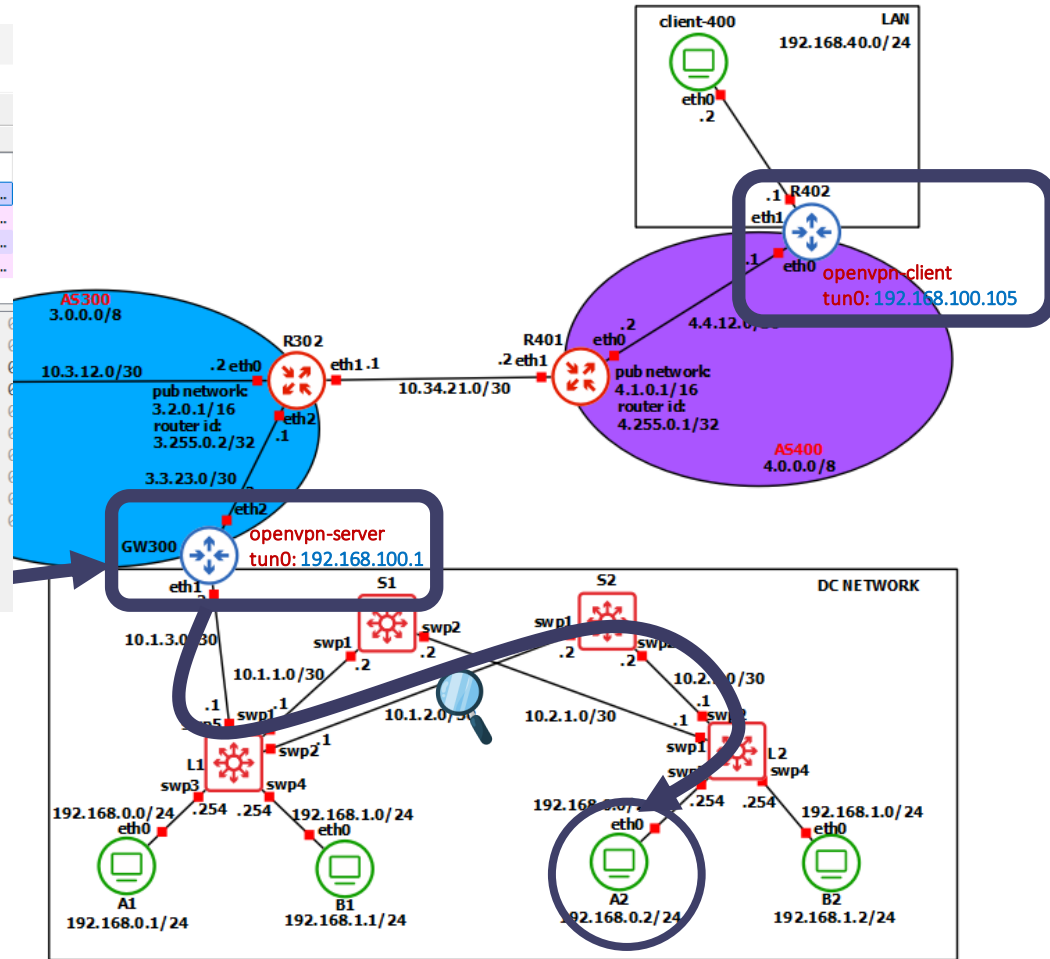
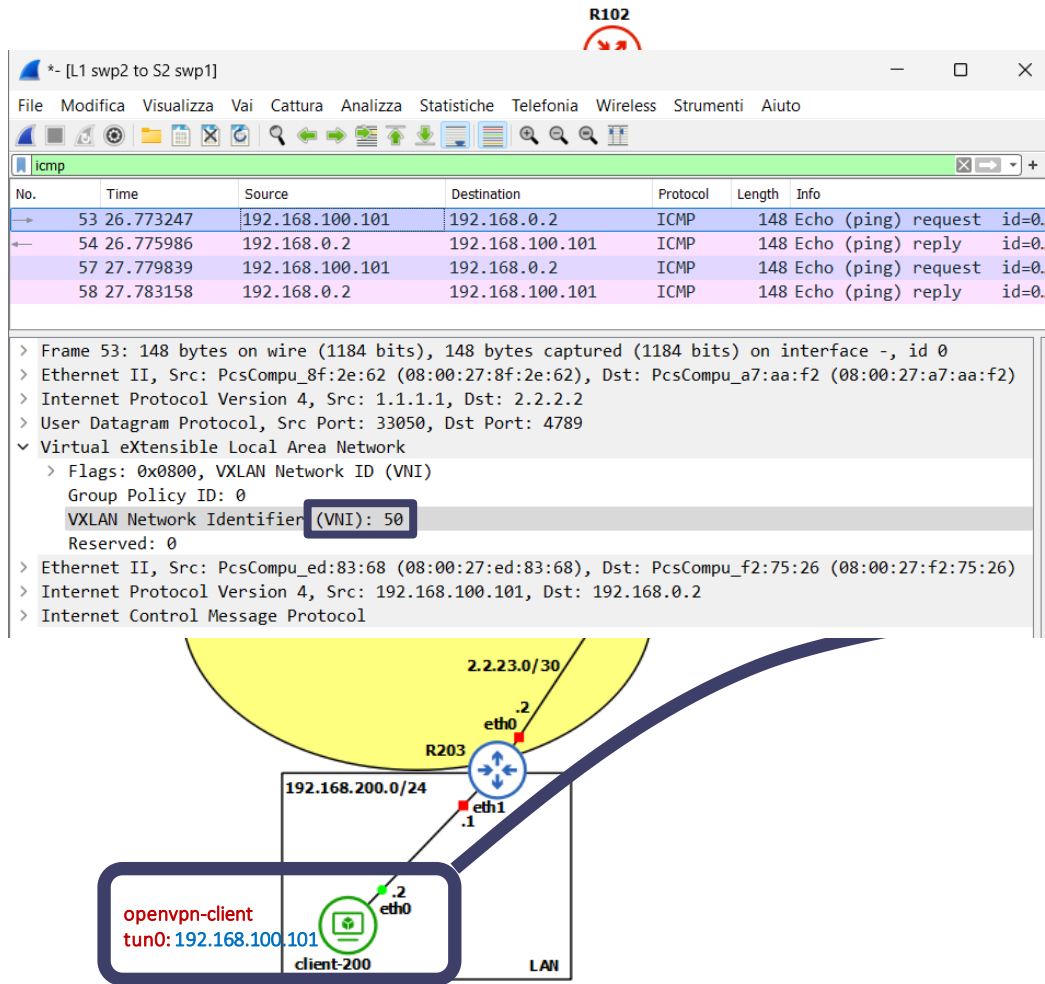
OpenVPN



OpenVPN

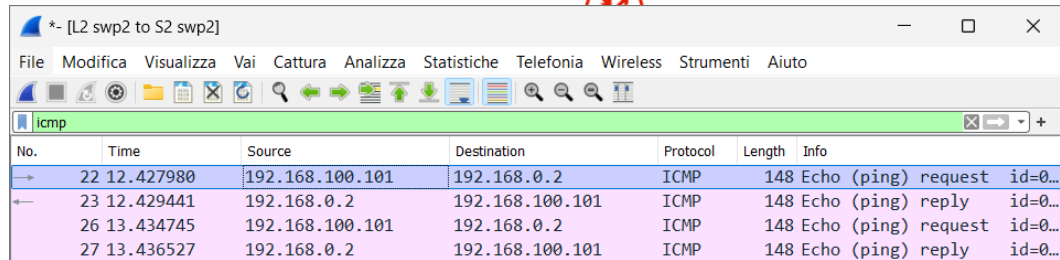


OpenVPN



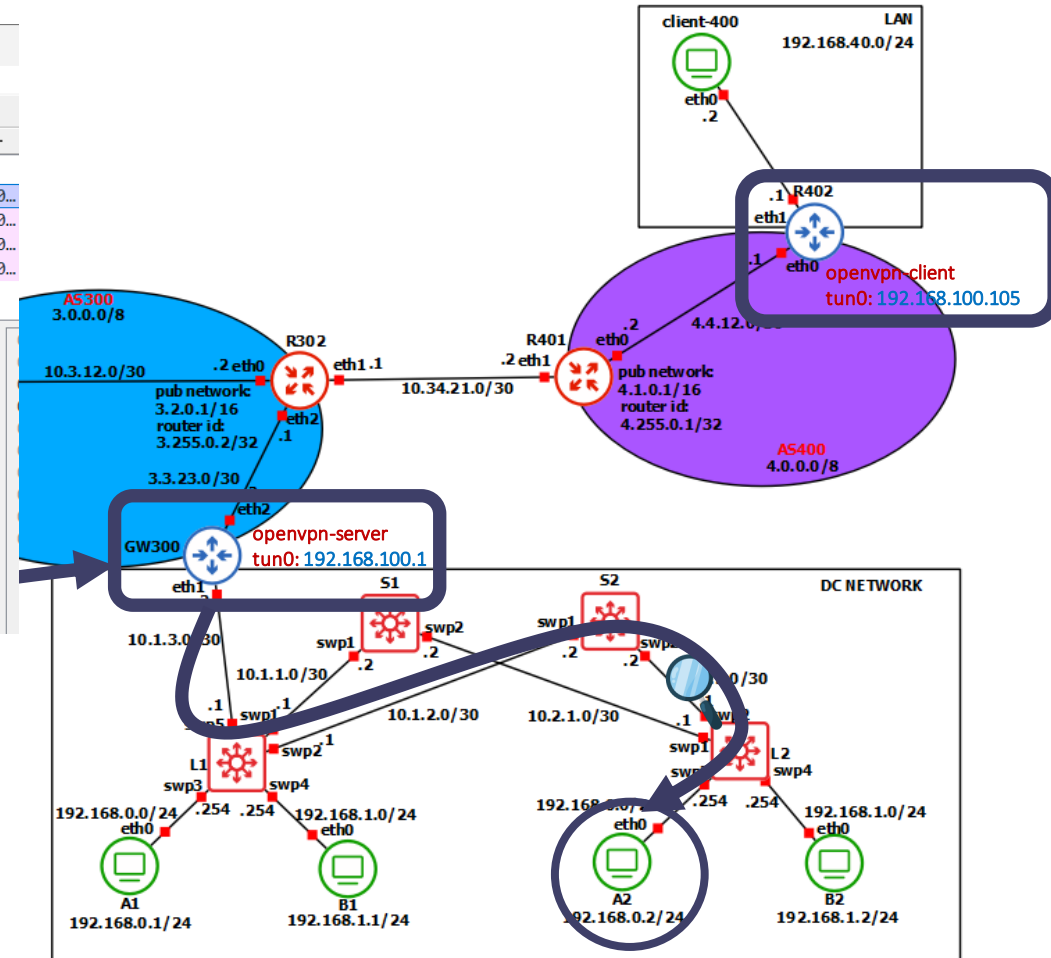
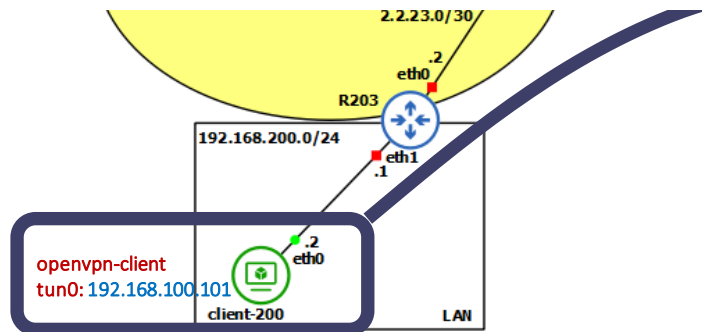
OpenVPN

R102

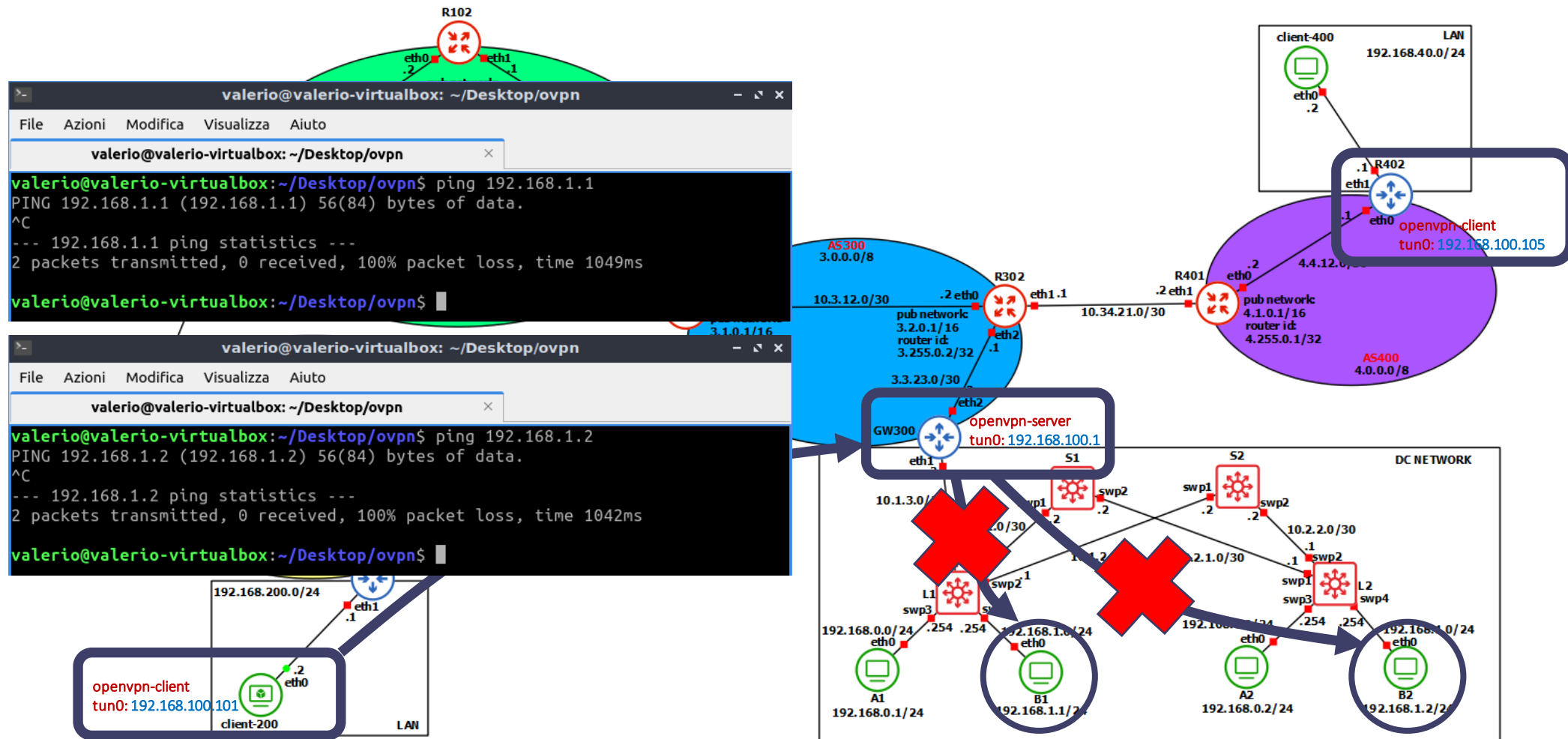


No.	Time	Source	Destination	Protocol	Length	Info
22	12.427980	192.168.100.101	192.168.0.2	ICMP	148	Echo (ping) request id=0...
23	12.429441	192.168.0.2	192.168.100.101	ICMP	148	Echo (ping) reply id=0...
26	13.434745	192.168.100.101	192.168.0.2	ICMP	148	Echo (ping) request id=0...
27	13.436527	192.168.0.2	192.168.100.101	ICMP	148	Echo (ping) reply id=0...

> Frame 22: 148 bytes on wire (1184 bits), 148 bytes captured (1184 bits) on interface -, id 0
> Ethernet II, Src: PcsCompu_b2:e5:bb (08:00:27:b2:e5:bb), Dst: PcsCompu_01:90:99 (08:00:27:01:90:99)
> Internet Protocol Version 4, Src: 1.1.1.1, Dst: 2.2.2.2
> User Datagram Protocol, Src Port: 33050, Dst Port: 4789
> Virtual eXtensible Local Area Network
 > Flags: 0x0800, VXLAN Network ID (VNI)
 Group Policy ID: 0
 VXLAN Network Identifier (VNI): 50
 Reserved: 0
> Ethernet II, Src: PcsCompu_ed:83:68 (08:00:27:ed:83:68), Dst: PcsCompu_f2:75:26 (08:00:27:f2:75:26)
> Internet Protocol Version 4, Src: 192.168.100.101, Dst: 192.168.0.2
> Internet Control Message Protocol



OpenVPN



MAC - AppArmor

- AppArmor si basa sulla creazione di **profili** al fine di confinare un programma ad un insieme di file, capabilities, accessi di rete ed insieme di risorse.
- AppArmor può lavorare in due modalità: **enforcement** (applica le regole di sicurezza definite nel profilo bloccando qualsiasi tentativo di accesso a risorse non consentite), oppure, **complain** (monitora le violazioni delle regole definite, registrando però un avviso nel log del sistema).
- Il profilo creato è relativo al programma **/usr/bin/nano**.

MAC - AppArmor

Nel profilo troviamo:

- dei *files* e *cartelle* accessibili in sola lettura (e.g: *r_dir*, *r_file.txt*);
- dei *files* e *cartelle* accessibili in sola scrittura (e.g: *w_dir*);
- restrizioni in lettura e scrittura sulle principali cartelle di sistema (e.g: */root*, */etc*, */var*, */bin*, */sbin*, */proc*, */sys*);

```
/usr/bin/nano {
  include <abstractions/base>
  include <abstractions/bash>
  include <abstractions/consoles>

  capability dac_override,
  capability dac_read_search,

  /usr/bin/nano mrrix,

  deny /home/*/Desktop/mac_dir/r_dir/** w,
  deny /home/*/Desktop/mac_dir/w_dir/** r,
  /home/*/Desktop/mac_dir/r_dir/** r,
  /home/*/Desktop/mac_dir/w_dir/** w,
  /home/*/Desktop/mac_dir/r_dir/r_file.txt r,
  /home/**/* rw,
  owner /home/**/* rw,

  # Permessi di base
  /lib/** r,
  /usr/lib/** r,
  /usr/share/nano/ r,
  /usr/share/nano/** r,
  /tmp/** rw,
  /run/** rw,
  /dev/tty rw,
  /dev/pts/ rw,
  /etc/** r,
  /var/** r,

  # Bloccare l'accesso ad altre directory sensibili del sistema
  deny /root/** rw,
  deny /etc/** w,
  deny /var/** rw,
  deny /bin/** rw,
  deny /sbin/** rw,
  deny /proc/** rw,
  deny /sys/** rw,
}
```

MAC - AppArmor

```
valerio@valerio-virtualbox: /etc/apparmor.d × valerio@valerio-virtualbox: ~/Desktop/mac_dir/r_dir × < >  
valerio@valerio-virtualbox:~/Desktop/mac_dir/r_dir$ ls -al  
totale 16  
drwxrwxr-x 2 valerio valerio 4096 ago 28 15:22 .  
drwxrwxr-x 4 valerio valerio 4096 ago 19 13:07 ..  
-rw-rw-r-- 1 valerio valerio 6 ago 19 15:32 r_file.txt  
-rw-rw-r-- 1 valerio valerio 6 ago 28 15:22 try.txt  
valerio@valerio-virtualbox:~/Desktop/mac_dir/r_dir$
```

```
valerio@valerio-virtualbox: /etc/apparmor.d × valerio@valerio-virtualbox: ~/Desktop/mac_dir/r_dir × < >  
valerio@valerio-virtualbox:~/Desktop/mac_dir/r_dir$ cat r_file.txt  
aloha  
valerio@valerio-virtualbox:~/Desktop/mac_dir/r_dir$ cat try.txt  
aloha  
valerio@valerio-virtualbox:~/Desktop/mac_dir/r_dir$
```

MAC - AppArmor

```
GNU nano 6.2 r_file.txt *
aloha hello

[ Errore durante la scrittura di r_file.txt: Permesso negato ]
^G Guida      ^O Salva      ^W Cerca      ^K Taglia      ^T Esegui      ^C Posizione
^X Esci      ^R Inserisci  ^\ Sostituisci ^U Incolla     ^J Giustifica  ^/ Vai a riga
```

```
GNU nano 6.2 try.txt *
aloha hello

[ Errore durante la scrittura di try.txt: Permesso negato ]
^G Guida      ^O Salva      ^W Cerca      ^K Taglia      ^T Esegui      ^C Posizione
^X Esci      ^R Inserisci  ^\ Sostituisci ^U Incolla     ^J Giustifica  ^/ Vai a riga
```

MAC - AppArmor

```
valerio@valerio-virtualbox: /etc/apparmor.d × valerio@valerio-virtualbox: ~/Desktop/mac_dir/w_dir × < >  
valerio@valerio-virtualbox:~/Desktop/mac_dir/w_dir$ ls -al  
totale 12  
drwxrwxr-x 2 valerio valerio 4096 set  2 23:55 .  
drwxrwxr-x 4 valerio valerio 4096 ago 19 13:07 ..  
-rw-rw-r-- 1 valerio valerio   6 ago 28 15:51 w_file.txt  
valerio@valerio-virtualbox:~/Desktop/mac_dir/w_dir$ █
```

```
valerio@valerio-virtualbox: /etc/apparmor.d × valerio@valerio-virtualbox: ~/Desktop/mac_dir/w_dir × < >  
valerio@valerio-virtualbox:~/Desktop/mac_dir/w_dir$ cat w_file.txt  
aloha  
valerio@valerio-virtualbox:~/Desktop/mac_dir/w_dir$ █
```

MAC - AppArmor

```
GNU nano 6.2          Nuovo buffer
[ Errore durante la lettura di w_file.txt: Permesso negato ]
^G Guida      ^O Salva      ^W Cerca      ^K Taglia     ^T Esegui     ^C Posizione
^X Esci       ^R Inserisci  ^\ Sostituisci ^U Incolla    ^J Giustifica ^/ Vai a riga
```


MAC - AppArmor

```
valerio@valerio-virtualbox: /etc/apparmor.d × valerio@valerio-virtualbox: ~/Desktop × < >  
valerio@valerio-virtualbox:~/Desktop$ cat mac_file.txt  
aloha  
valerio@valerio-virtualbox:~/Desktop$ █
```

```
valerio@valerio-virtualbox: /etc/apparmor.d × valerio@valerio-virtualbox: ~/Desktop × < >  
GNU nano 6.2 mac_file.txt  
aloha hello █  
[ Scritta 1 riga ]  
^G Guida      ^O Salva      ^W Cerca      ^K Taglia      ^T Esegui      ^C Posizione  
^X Esci       ^R Inserisci  ^\ Sostituisci ^U Incolla     ^J Giustifica  ^/ Vai a riga
```

Grazie per l'attenzione!

Valerio Crecco 0320452

Ludovico De Santis 0320460