Network and System Defence

MELISSA PETROLO

UNIVERSITÀ DI ROMA TOR VERGATA

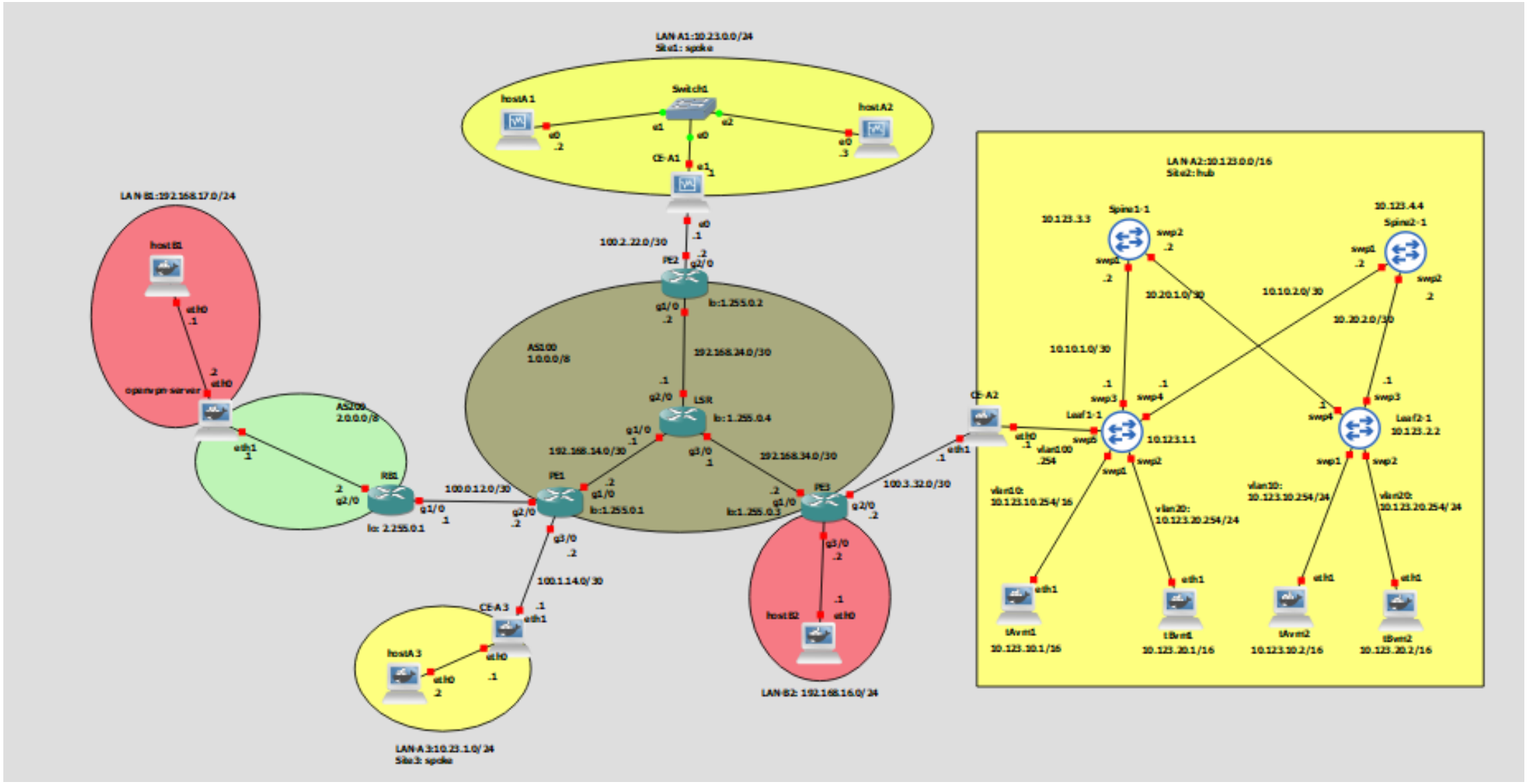
2023-2024

Specifica

In questo progetto, ci sono 2 sistemi autonomi che forniscono connettività di rete a cinque reti private.

AS100 fornisce un servizio BGP/MPLS VPN per i tre siti di VPN A.

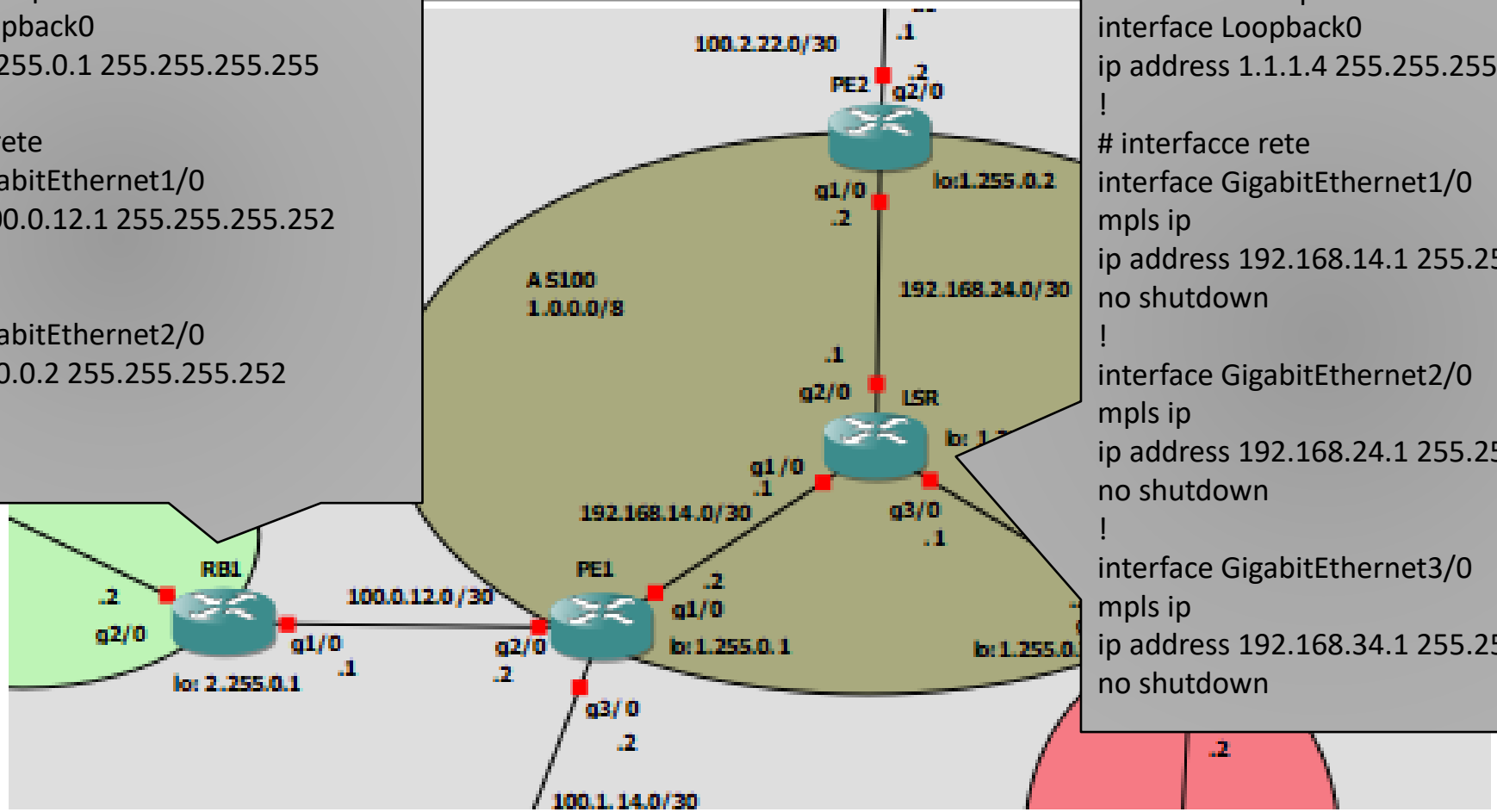
AS200 è un client di AS100 e ospita un server OpenVPN con un indirizzo IP pubblico, utilizzato per fornire una VPN overlay per il client VPN in LAN-B1.


LAN A1:10.23.0.0/24
Site1: spoke
hostA1
Switch1
hostA2
CE-A1
100.2.22.0/30
PE2
lo:1.255.0.2
AS100
10.0.0.0/8
192.168.24.0/30
LSR
lo:1.255.0.4
192.168.14.0/30
192.168.34.0/30
PE1
PE3
lo:1.255.0.1
lo:1.255.0.3
100.0.12.0/30
100.3.32.0/30
100.1.14.0/30
LAN B1:192.168.17.0/24
hostB1
openvpn server
AS200
2.0.0.0/8
RR1
lo: 2.255.0.1
CE-A3
hostA3
LAN A3:10.23.1.0/24
Site3: spoke
hostB2
LAN B2: 192.168.16.0/24
CE-A2
LAN A2:10.123.0.0/16
Site2: hub
Spine1-1
10.123.3.3
Spine2-1
10.123.4.4
10.20.1.0/30
10.10.2.0/30
10.20.2.0/30
10.10.1.0/30
Leaf1-1
10.123.1.1
Leaf2-1
10.123.2.2
vlan100
.254
vlan10:
10.123.10.254/16
vlan20:
10.123.20.254/24
tAvm1
10.123.10.1/16
tBvm1
10.123.20.1/16
tAvm2
10.123.10.2/16
tBvm2
10.123.20.2/16

Configurazione IP, BGP, OSPF

Configurazione IP

```
# interfacce loopback
interface Loopback0
ip address 2.255.0.1 255.255.255.255
!
# interfacce rete
interface GigabitEthernet1/0
ip address 100.0.12.1 255.255.255.252
no shutdown
!
interface GigabitEthernet2/0
ip address 2.0.0.2 255.255.255.252
no shutdown
!
```



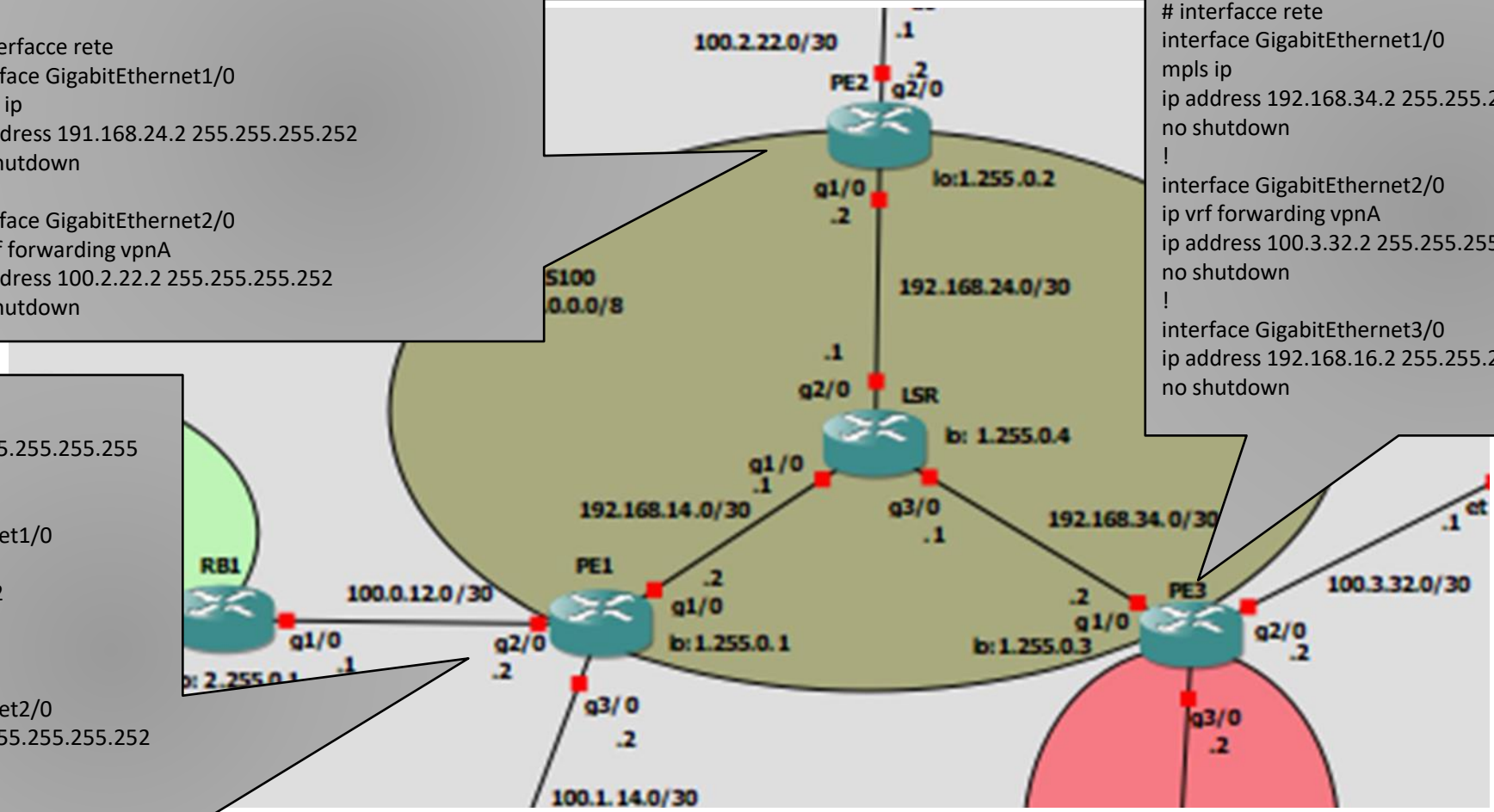

```
# interfacce loopback
interface Loopback0
ip address 1.1.1.4 255.255.255.255
!
# interfacce rete
interface GigabitEthernet1/0
mpls ip
ip address 192.168.14.1 255.255.255.252
no shutdown
!
interface GigabitEthernet2/0
mpls ip
ip address 192.168.24.1 255.255.255.252
no shutdown
!
interface GigabitEthernet3/0
mpls ip
ip address 192.168.34.1 255.255.255.252
no shutdown
```

Configurazione IP

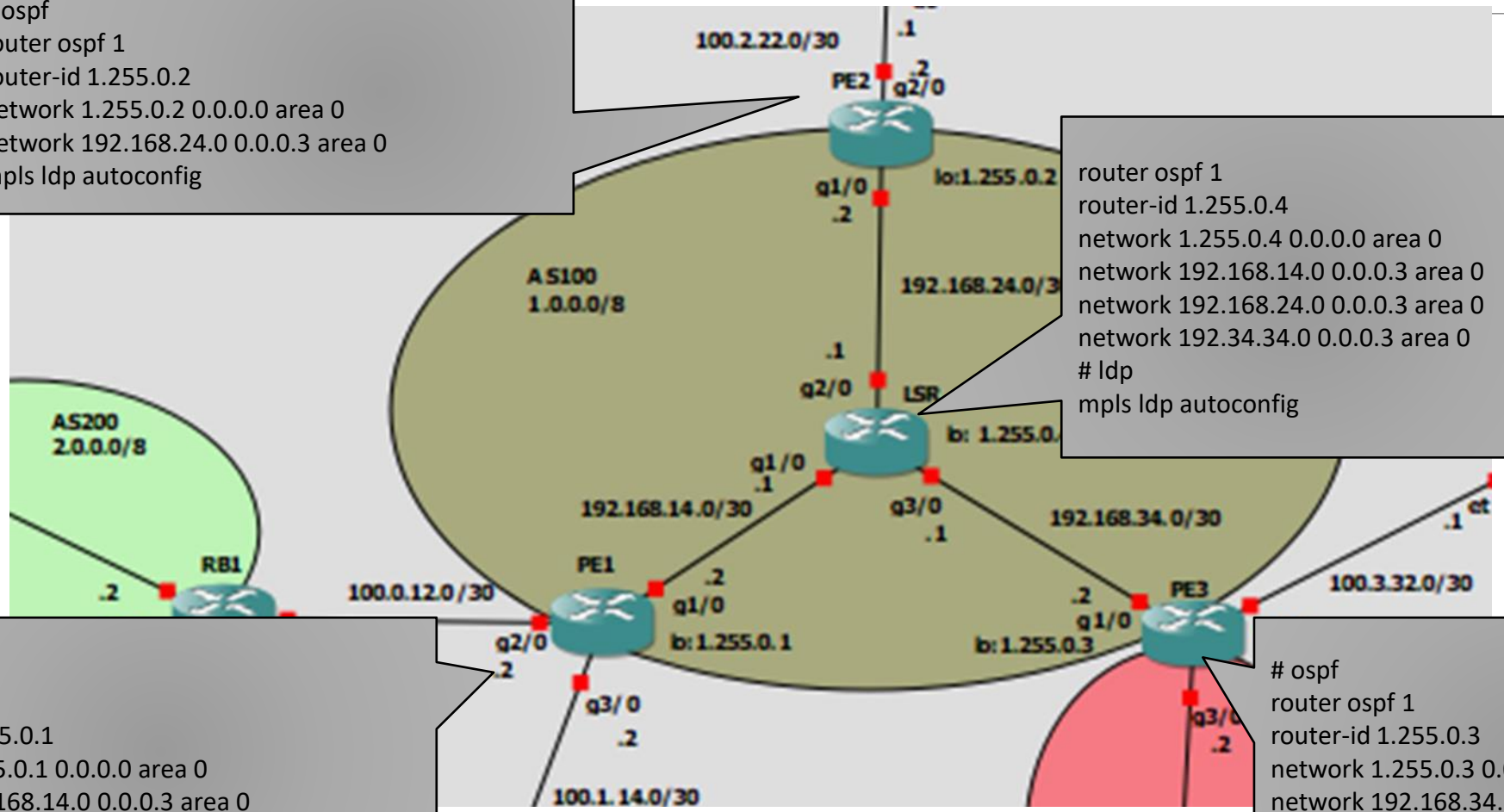
```
# interfacce loopback
interface Loopback0
ip address 1.255.0.2 255.255.255.255
!
# interfacce rete
interface GigabitEthernet1/0
mpls ip
ip address 191.168.24.2 255.255.255.252
no shutdown
!
interface GigabitEthernet2/0
ip vrf forwarding vpnA
ip address 100.2.22.2 255.255.255.252
no shutdown
```

```
# interfacce loopback
interface Loopback0
ip address 1.255.0.3 255.255.255.255
!
# interfacce rete
interface GigabitEthernet1/0
mpls ip
ip address 192.168.34.2 255.255.255.252
no shutdown
!
interface GigabitEthernet2/0
ip vrf forwarding vpnA
ip address 100.3.32.2 255.255.255.252
no shutdown
!
interface GigabitEthernet3/0
ip address 192.168.16.2 255.255.255.0
no shutdown
```

```
# interfacce loopback
interface Loopback0
ip address 1.255.0.1 255.255.255.255
!
# interfacce rete
interface GigabitEthernet1/0
mpls ip
ip address 192.168.14.2
255.255.255.252
no shutdown
!
interface GigabitEthernet2/0
ip address 100.0.12.2 255.255.255.252
no shutdown
!
interface GigabitEthernet3/0
ip vrf forwarding vpnA
ip address 100.1.14.2 255.255.255.252
no shutdown
```



Configurazione OSPF



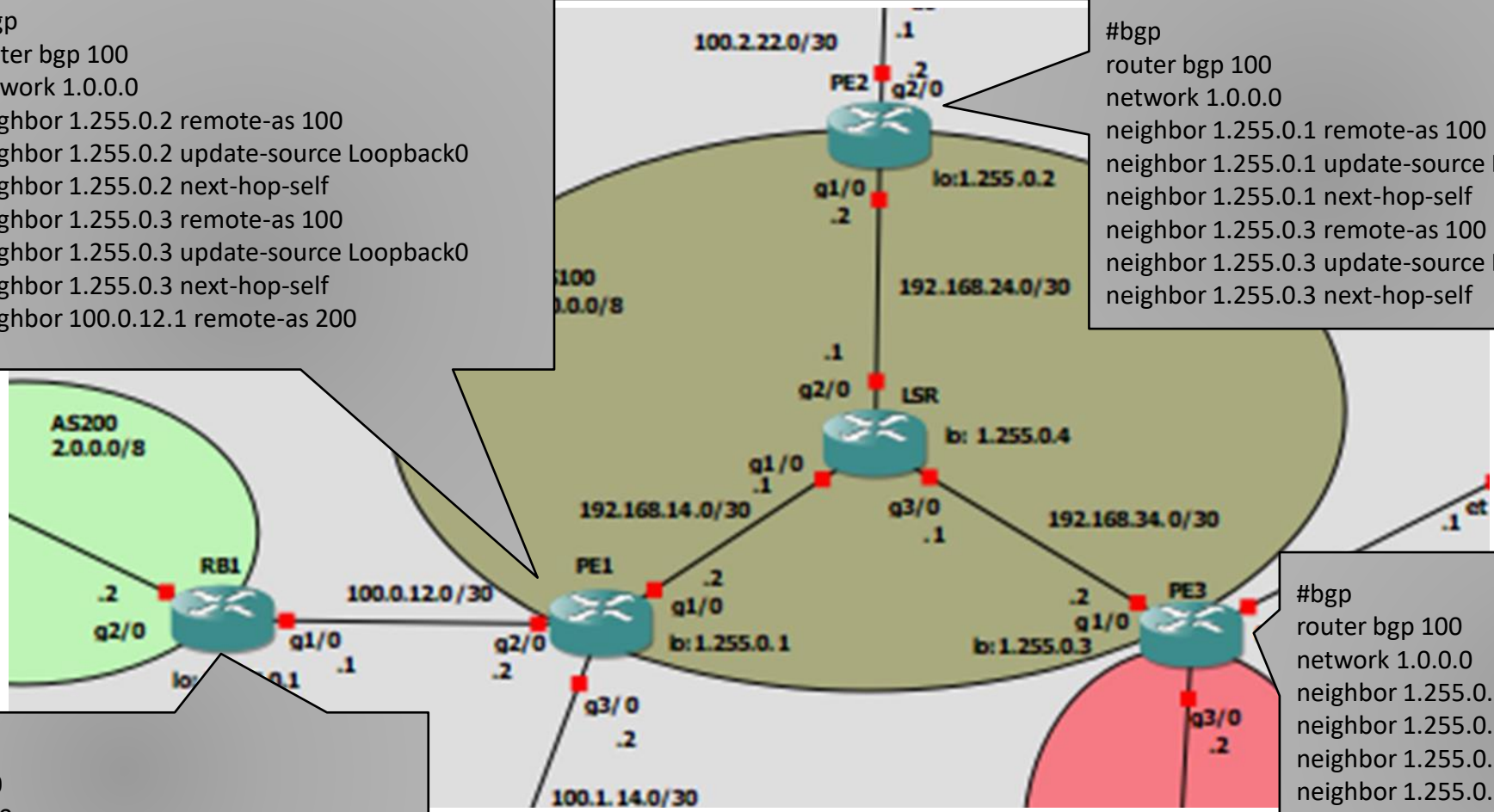
ospf
router ospf 1
router-id 1.255.0.2
network 1.255.0.2 0.0.0.0 area 0
network 192.168.24.0 0.0.0.3 area 0
mpls ldp autoconfig

router ospf 1
router-id 1.255.0.4
network 1.255.0.4 0.0.0.0 area 0
network 192.168.14.0 0.0.0.3 area 0
network 192.168.24.0 0.0.0.3 area 0
network 192.34.34.0 0.0.0.3 area 0
ldp
mpls ldp autoconfig

ospf
router ospf 1
router-id 1.255.0.1
network 1.255.0.1 0.0.0.0 area 0
network 192.168.14.0 0.0.0.3 area 0
mpls ldp autoconfig

ospf
router ospf 1
router-id 1.255.0.3
network 1.255.0.3 0.0.0.0 area 0
network 192.168.34.0 0.0.0.3 area 0
ldp
mpls ldp autoconfig

Configurazione BGP



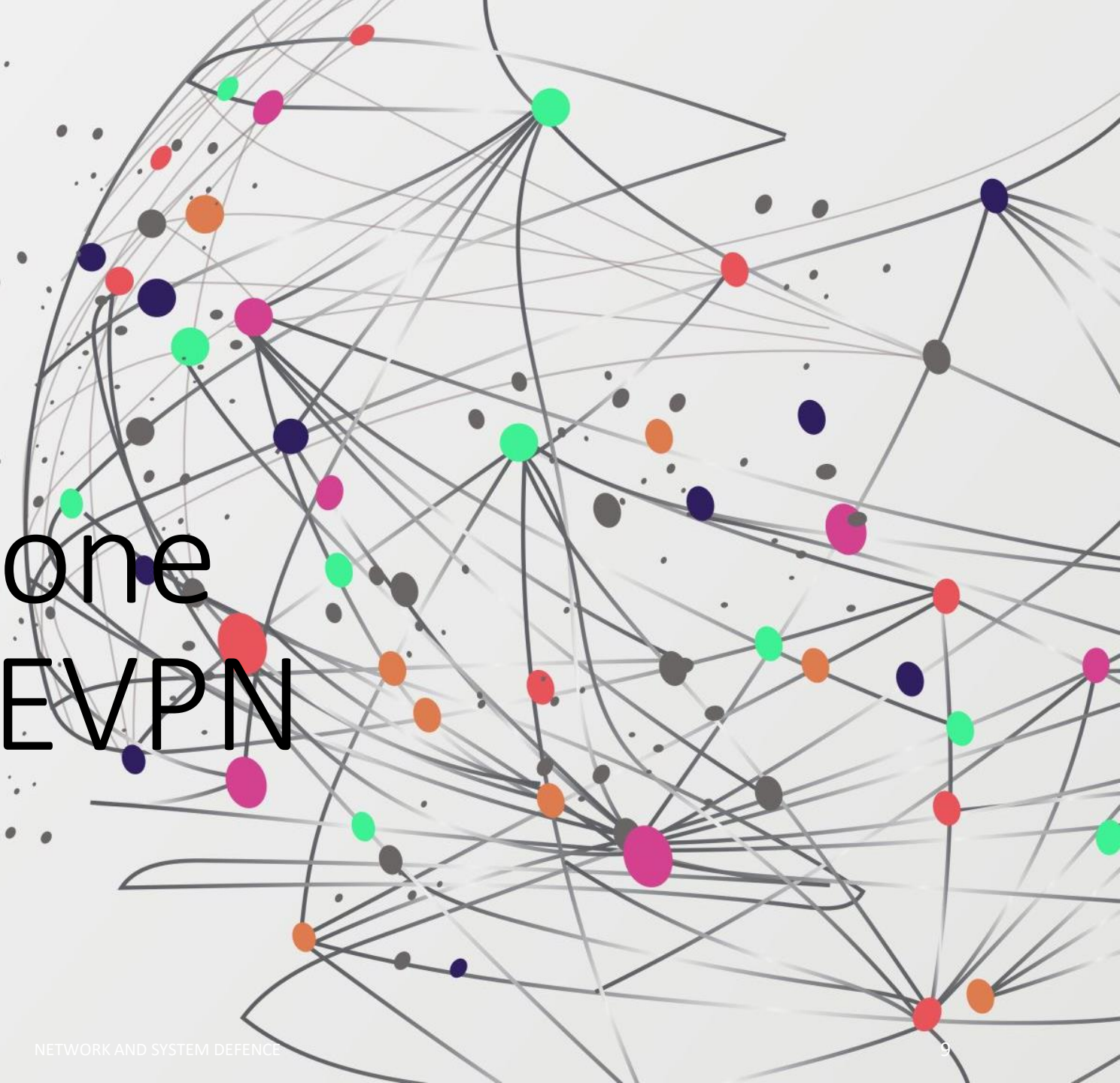
#bgp
router bgp 100
network 1.0.0.0
neighbor 1.255.0.2 remote-as 100
neighbor 1.255.0.2 update-source Loopback0
neighbor 1.255.0.2 next-hop-self
neighbor 1.255.0.3 remote-as 100
neighbor 1.255.0.3 update-source Loopback0
neighbor 1.255.0.3 next-hop-self
neighbor 100.0.12.1 remote-as 200

#bgp
router bgp 100
network 1.0.0.0
neighbor 1.255.0.1 remote-as 100
neighbor 1.255.0.1 update-source Loopback0
neighbor 1.255.0.1 next-hop-self
neighbor 1.255.0.3 remote-as 100
neighbor 1.255.0.3 update-source Loopback0
neighbor 1.255.0.3 next-hop-self

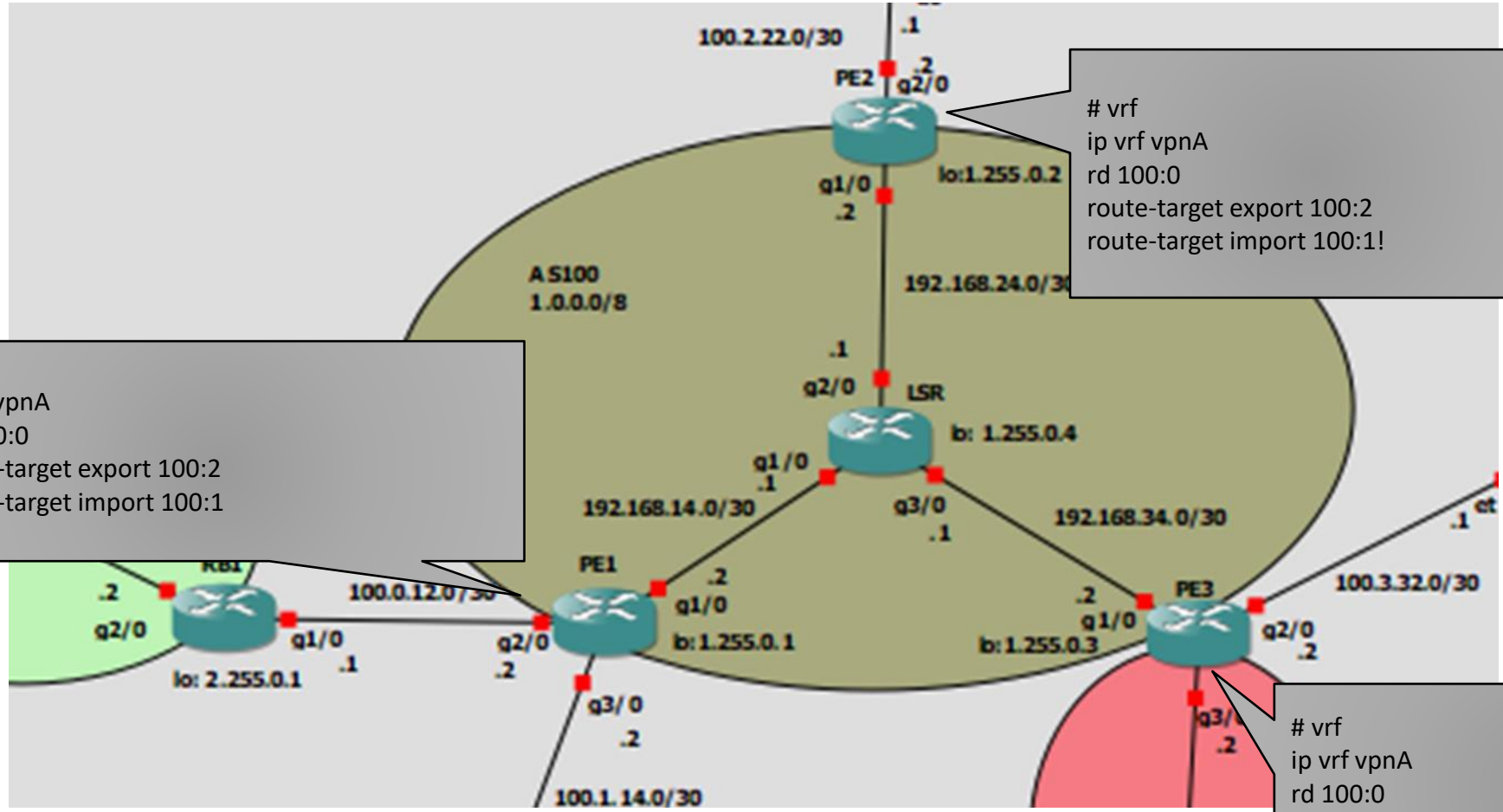
bgp
router bgp 200
network 2.0.0.0
neighbor 100.0.12.2 remote-as 100

#bgp
router bgp 100
network 1.0.0.0
neighbor 1.255.0.1 remote-as 100
neighbor 1.255.0.1 update-source Loopback0
neighbor 1.255.0.1 next-hop-self
neighbor 1.255.0.2 remote-as 100
neighbor 1.255.0.2 update-source Loopback0
neighbor 1.255.0.2 next-hop-self

Configurazione BGP/MPLS EVPN



Configurazione BGP/MPLS VPN



vrf
ip vrf vpnA
rd 100:0
route-target export 100:2
route-target import 100:1!

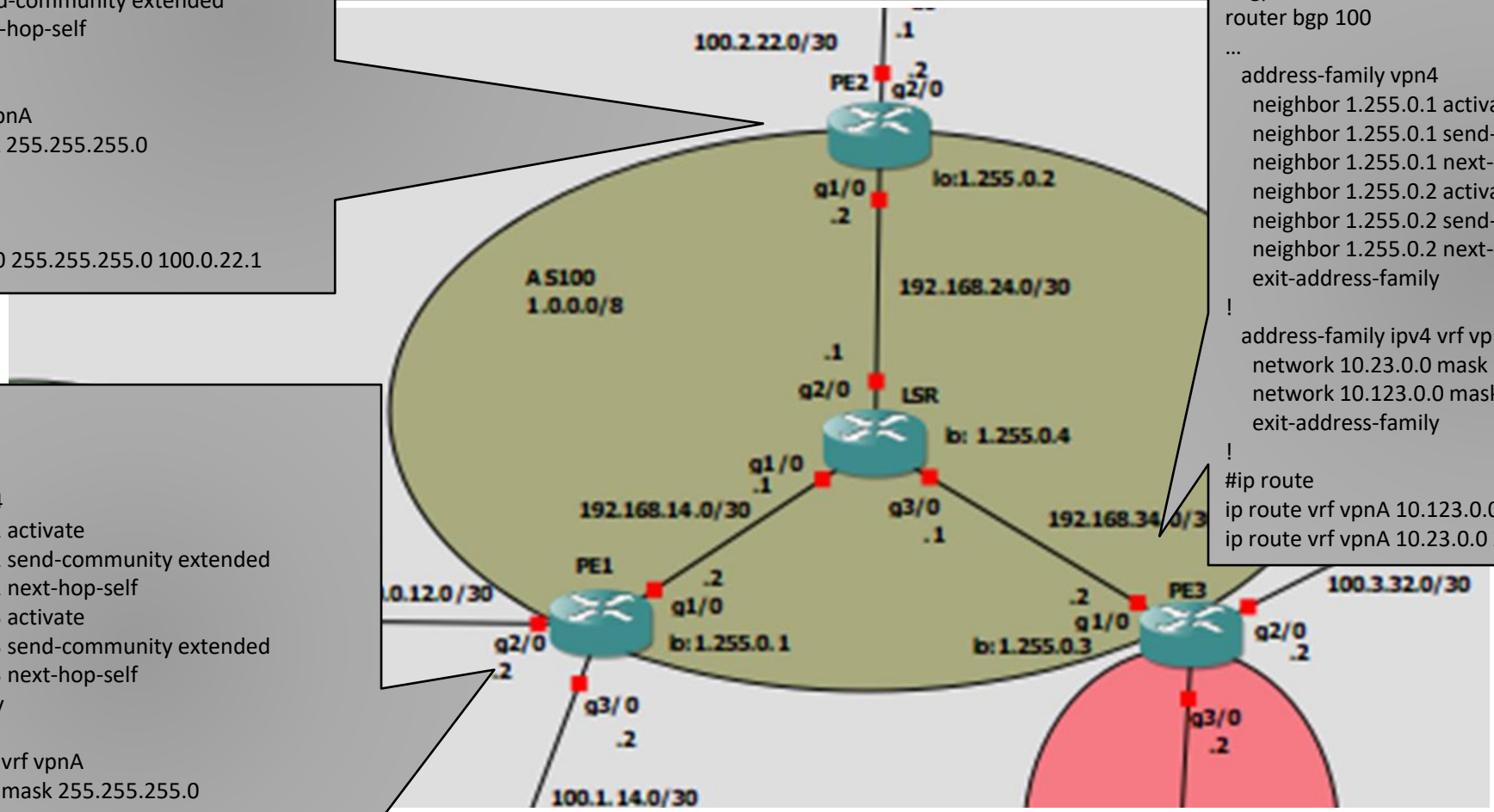
vrf
ip vrf vpnA
rd 100:0
route-target export 100:2
route-target import 100:1
!

vrf
ip vrf vpnA
rd 100:0
route-target export 100:1
route-target import 100:2!

Configurazione BGP/MPLS VPN

```
#bgp
router bgp 100
…
  address-family vpn4
   neighbor 1.255.0.1 activate
   neighbor 1.255.0.1 send-community extended
   neighbor 1.255.0.1 next-hop-self
   neighbor 1.255.0.3 activate
   neighbor 1.255.0.3 send-community extended
  neighbor 1.255.0.3 next-hop-self
  exit-address-family
!
 address-family ipv4 vrf vpnA
  network 10.23.0.0 mask 255.255.255.0
  exit-address-family
!
#ip route
ip route vrf vpnA 10.23.0.0 255.255.255.0 100.0.22.1
```

```
#bgp
router bgp 100
… !
  address-family vpn4
   neighbor 1.255.0.2 activate
   neighbor 1.255.0.2 send-community extended
   neighbor 1.255.0.2 next-hop-self
   neighbor 1.255.0.3 activate
   neighbor 1.255.0.3 send-community extended
   neighbor 1.255.0.3 next-hop-self
   exit-address-family
!
  address-family ipv4 vrf vpnA
   network 10.23.1.0 mask 255.255.255.0
   exit-address-family
!
ip route vrf vpnA 10.23.1.0 255.255.255.0 100.0.14.1
```

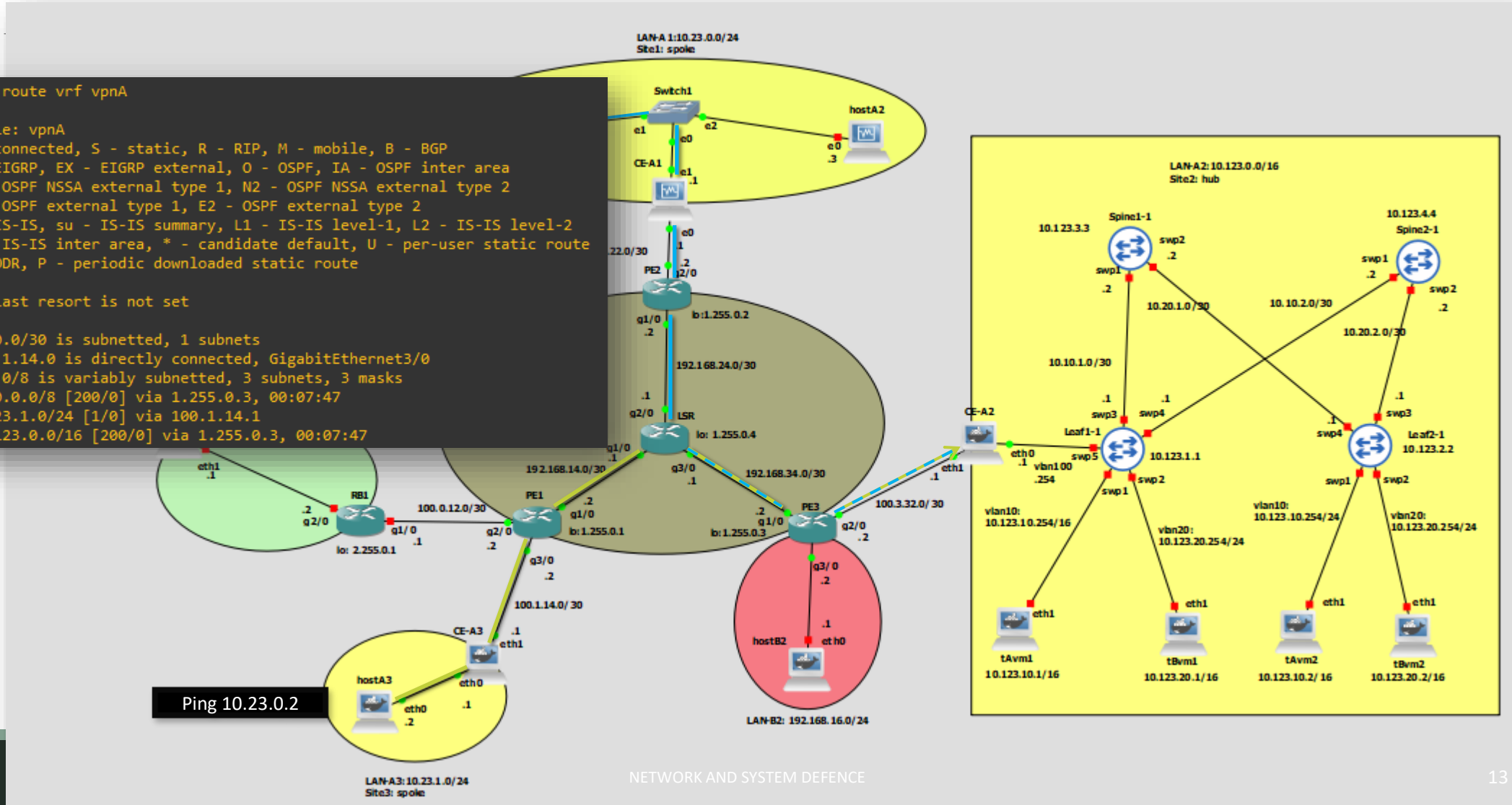



```
#bgp
router bgp 100
…
  address-family vpn4
   neighbor 1.255.0.1 activate
   neighbor 1.255.0.1 send-community extended
   neighbor 1.255.0.1 next-hop-self
   neighbor 1.255.0.2 activate
   neighbor 1.255.0.2 send-community extended
   neighbor 1.255.0.2 next-hop-self
   exit-address-family
!
  address-family ipv4 vrf vpnA
   network 10.23.0.0 mask 255.0.0.0
   network 10.123.0.0 mask 255.255.0.0
   exit-address-family
!
#ip route
ip route vrf vpnA 10.123.0.0 255.255.255.0 100.0.32.1
ip route vrf vpnA 10.23.0.0 255.0.0.0 100.0.32.1
```

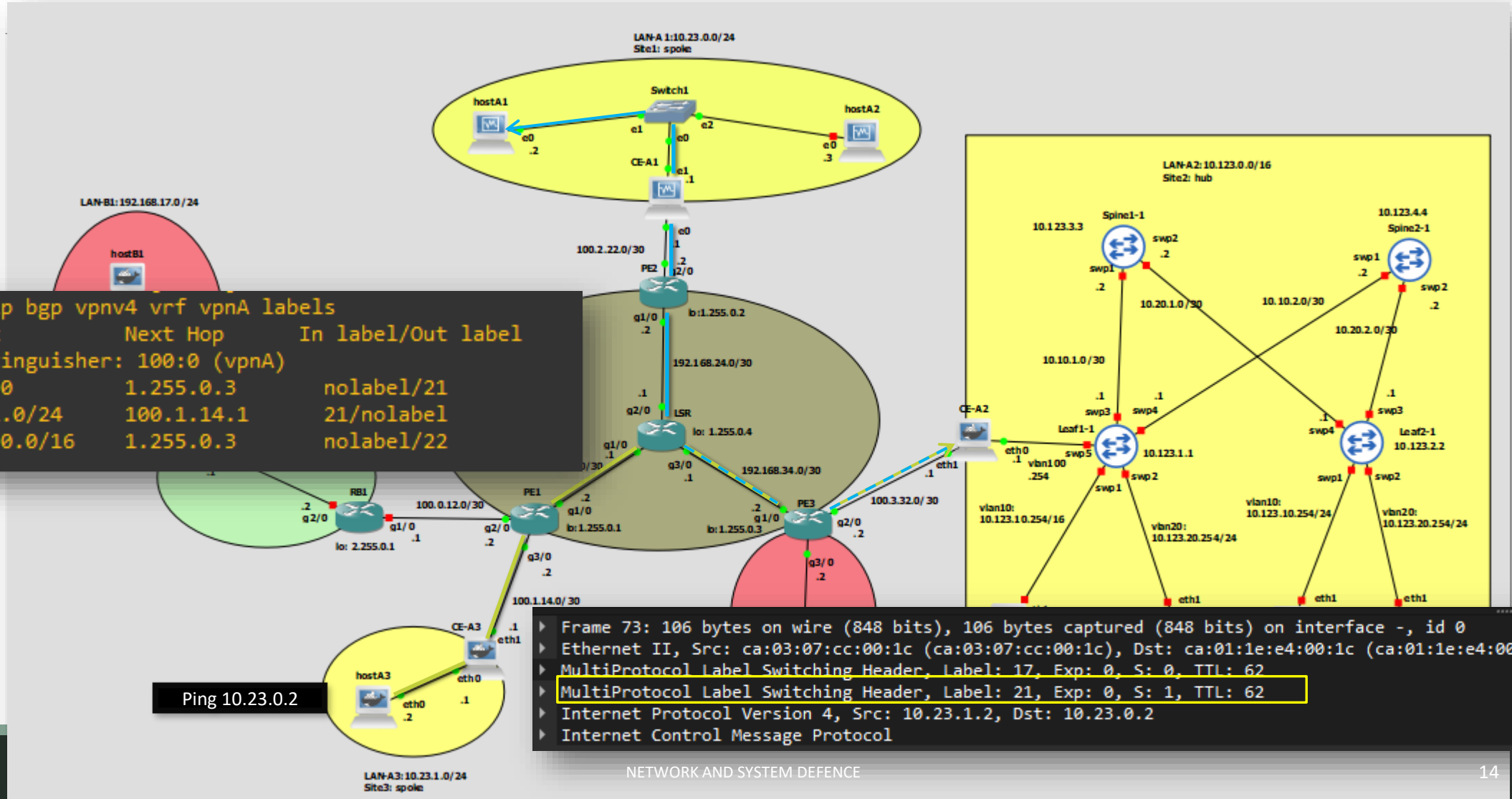
Test: Spoke To Spoke

TEST: HOSTA3 -> HOSTA1

```
PE1>show ip route vrf vpnA

Routing Table: vpnA
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     100.0.0.0/30 is subnetted, 1 subnets
C       100.1.14.0 is directly connected, GigabitEthernet3/0
     10.0.0.0/8 is variably subnetted, 3 subnets, 3 masks
B       10.0.0.0/8 [200/0] via 1.255.0.3, 00:07:47
S       10.23.1.0/24 [1/0] via 100.1.14.1
B       10.123.0.0/16 [200/0] via 1.255.0.3, 00:07:47
```



TEST: HOSTA3 -> HOSTA1

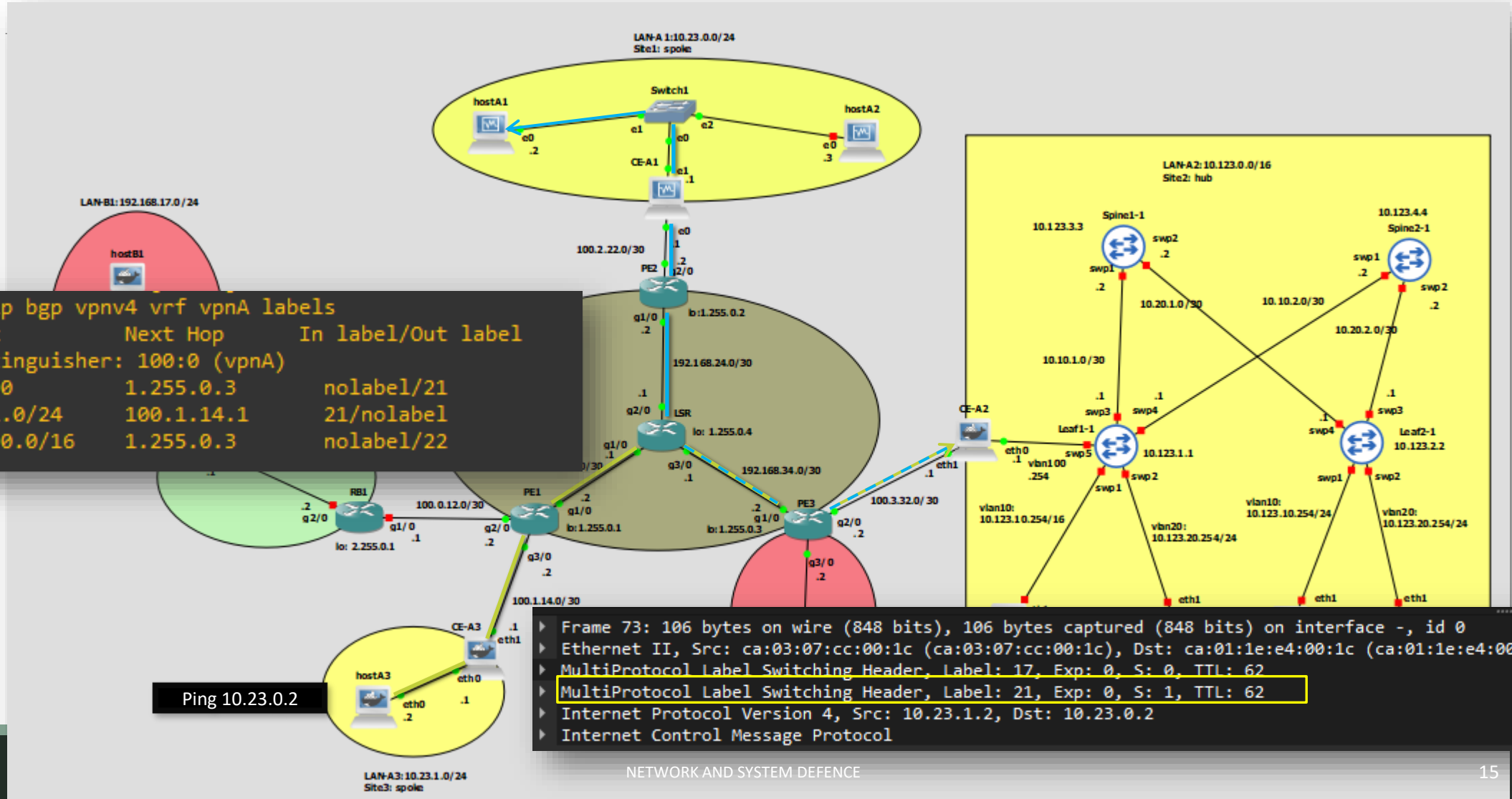



```
PE1>show ip bgp vpnv4 vrf vpnA labels
   Network          Next Hop      In label/Out label
Route Distinguisher: 100:0 (vpnA)
   10.0.0.0         1.255.0.3       nolabel/21
   10.23.1.0/24     100.1.14.1      21/nolabel
   10.123.0.0/16    1.255.0.3       nolabel/22
```

Ping 10.23.0.2

```
Frame 73: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface -, id 0
Ethernet II, Src: ca:03:07:cc:00:1c (ca:03:07:cc:00:1c), Dst: ca:01:1e:e4:00:1c (ca:01:1e:e4:00:1c)
MultiProtocol Label Switching Header, Label: 17, Exp: 0, S: 0, TTL: 62
MultiProtocol Label Switching Header, Label: 21, Exp: 0, S: 1, TTL: 62
Internet Protocol Version 4, Src: 10.23.1.2, Dst: 10.23.0.2
Internet Control Message Protocol
```

TEST: HOSTA3 -> HOSTA1

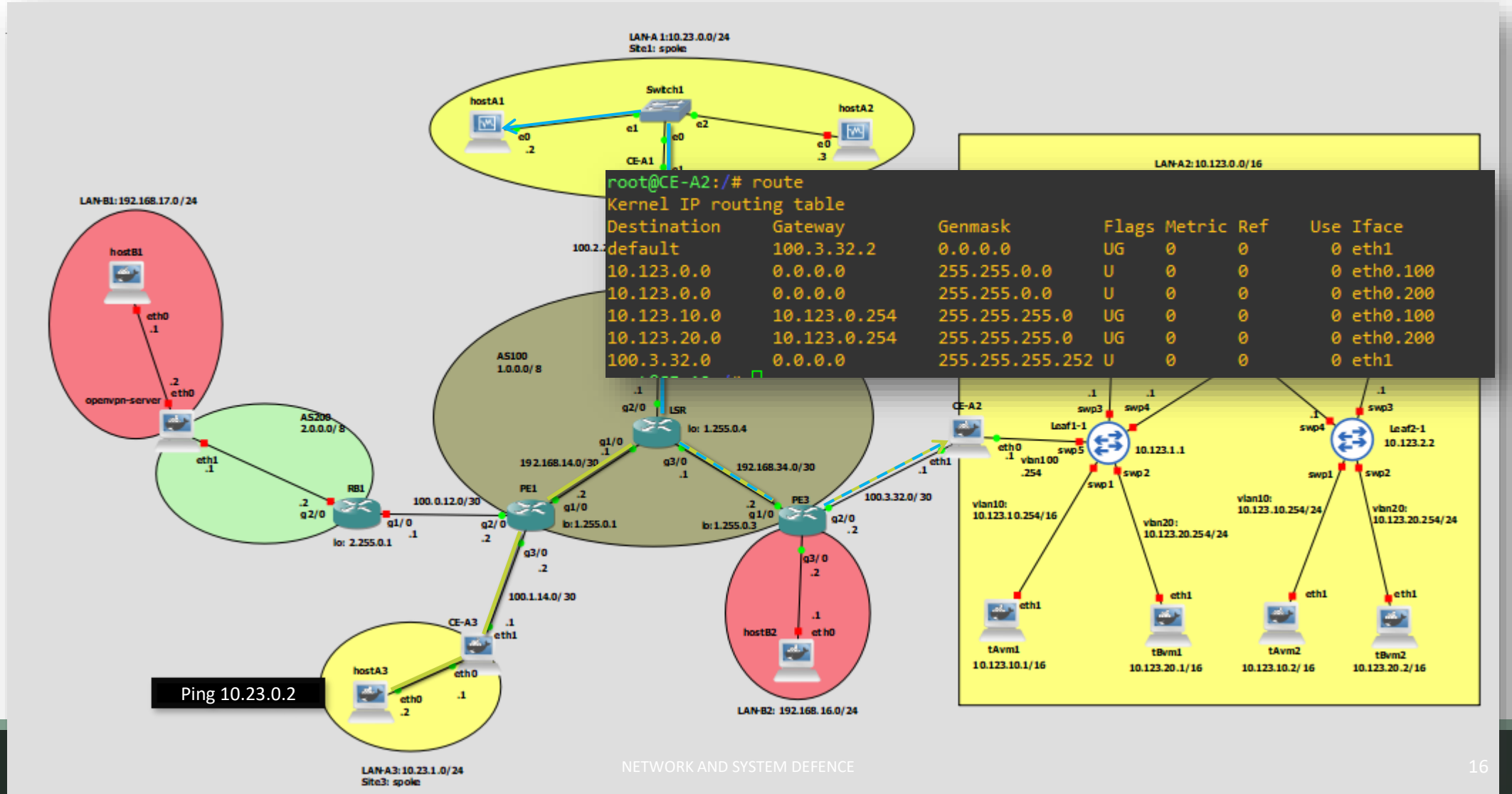



```
PE1>show ip bgp vpnv4 vrf vpnA labels
   Network          Next Hop      In label/Out label
Route Distinguisher: 100:0 (vpnA)
   10.0.0.0         1.255.0.3       nolabel/21
   10.23.1.0/24     100.1.14.1      21/nolabel
   10.123.0.0/16    1.255.0.3       nolabel/22
```

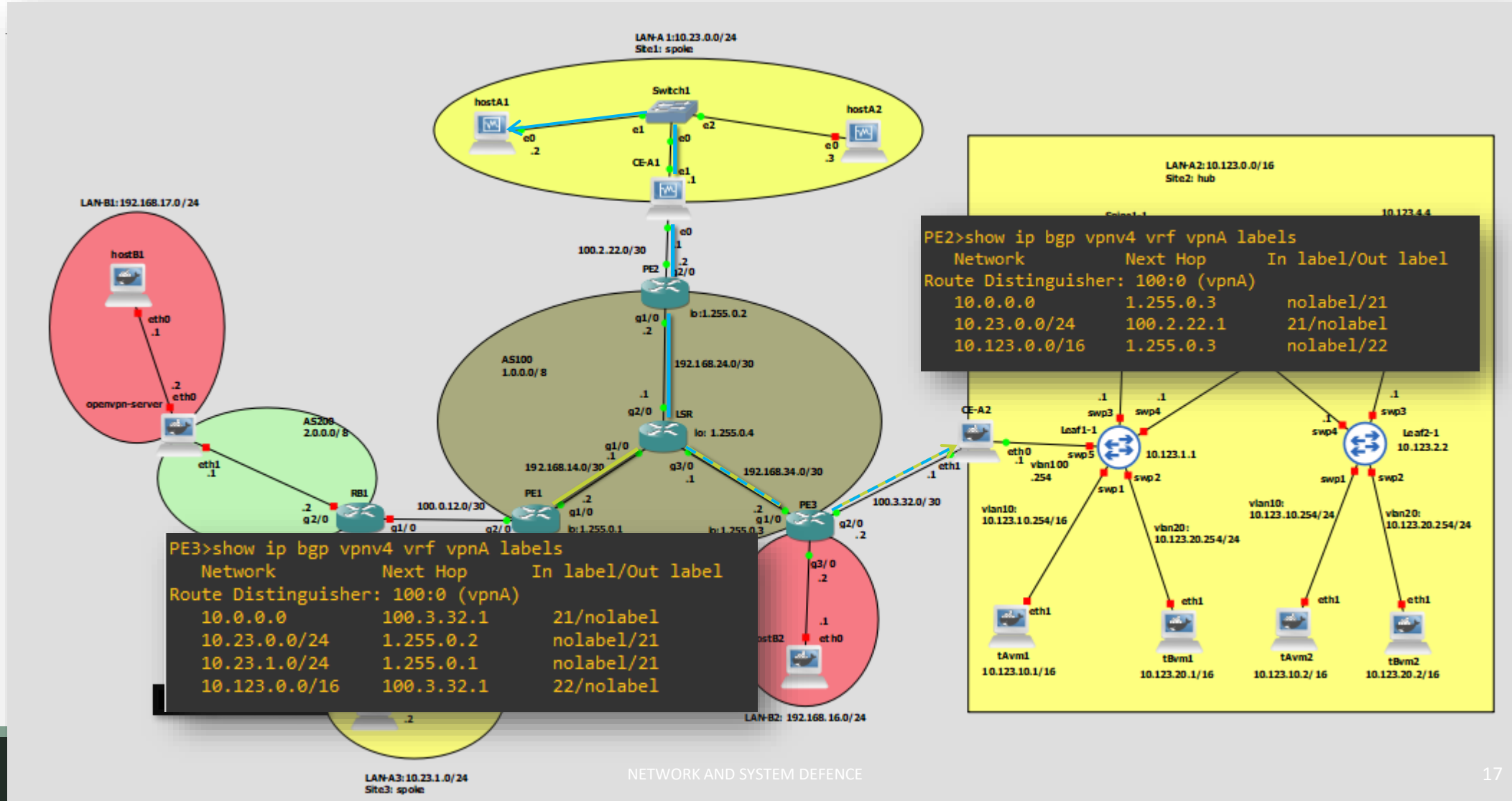
Ping 10.23.0.2

```
Frame 73: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface -, id 0
Ethernet II, Src: ca:03:07:cc:00:1c (ca:03:07:cc:00:1c), Dst: ca:01:1e:e4:00:1c (ca:01:1e:e4:00:1c)
MultiProtocol Label Switching Header, Label: 17, Exp: 0, S: 0, TTL: 62
MultiProtocol Label Switching Header, Label: 21, Exp: 0, S: 1, TTL: 62
Internet Protocol Version 4, Src: 10.23.1.2, Dst: 10.23.0.2
Internet Control Message Protocol
```

TEST: HOSTA3 -> HOSTA1



TEST: HOSTA3 -> HOSTA1




```
PE2>show ip bgp vpnv4 vrf vpnA labels
   Network          Next Hop      In label/Out label
Route Distinguisher: 100:0 (vpnA)
   10.0.0.0         1.255.0.3       nolabel/21
   10.23.0.0/24     100.2.22.1      21/nolabel
   10.123.0.0/16    1.255.0.3       nolabel/22
```

```
PE3>show ip bgp vpnv4 vrf vpnA labels
   Network          Next Hop      In label/Out label
Route Distinguisher: 100:0 (vpnA)
   10.0.0.0         100.3.32.1      21/nolabel
   10.23.0.0/24     1.255.0.2       nolabel/21
   10.23.1.0/24     1.255.0.1       nolabel/21
   10.123.0.0/16    100.3.32.1      22/nolabel
```

Firewall

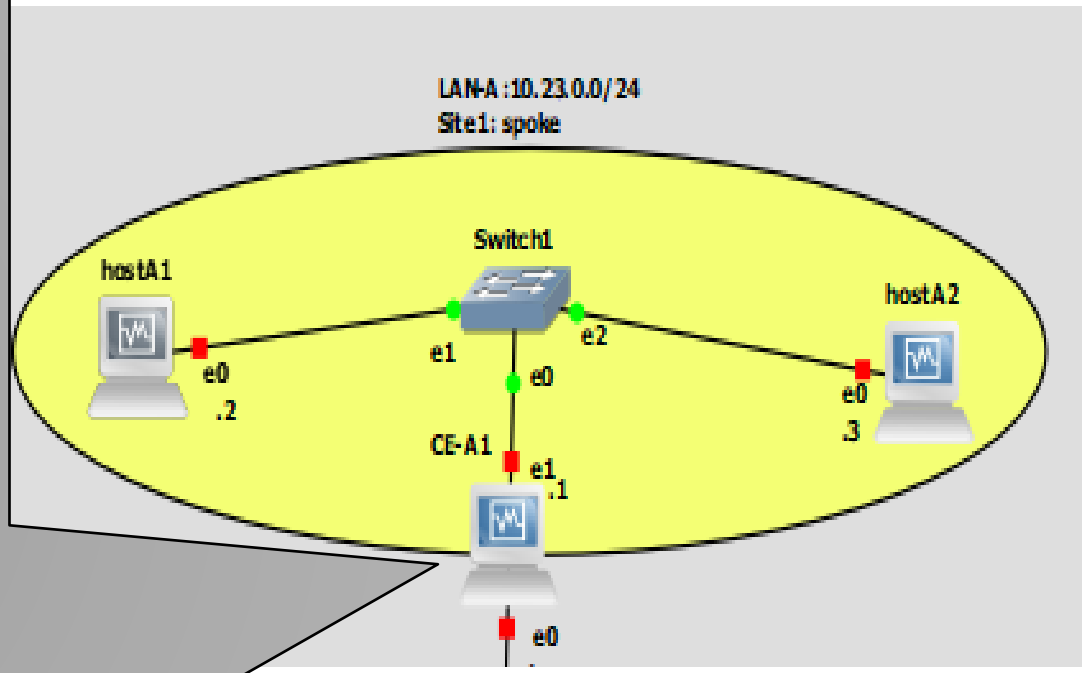
Firewall CE-A1

Realizzare un Firewall (con iptables/NETFILTER) in CE-A1 con le seguenti policy di sicurezza:

- Consentire il traffico tra LAN e rete esterna solo se avviato dalla LAN, con traduzione dinamica dell'indirizzo di origine
- Negare tutto il traffico a GW tranne ssh e ICMP solo se avviato dalla LAN
- Consentire il traffico da GW a qualsiasi luogo (e relativi pacchetti di risposta)
- Consentire il port forwarding con DNAT a hostA1 e hostA2 dalla rete esterna solo per il servizio HTTP

Firewall CE-A1

```
export AS=enp0s3
export LAN=macsec0

sudo iptables -F # flush already present entries
sudo iptables -F -t nat

sudo iptables -P FORWARD DROP
sudo iptables -P INPUT DROP
sudo iptables -P OUTPUT ACCEPT

# Consentire il traffico tra LAN e rete esterna solo se avviato dalla LAN,
sudo iptables -A FORWARD -i $LAN -o $AS -j ACCEPT
# con traduzione dinamica dell'indirizzo sorgente
sudo iptables -t nat -A POSTROUTING -o $AS -j MASQUERADE

# Nega tutto il traffico verso GW tranne
# ssh e ICMP solo se avviato dalla LAN
sudo iptables -A INPUT -i $LAN -p tcp --dport 22 -j ACCEPT
sudo iptables -A INPUT -i $LAN -p icmp -j ACCEPT

# Autorizza il traffico da GW verso qualsiasi luogo
# (e i relativi pacchetti di risposta)
sudo iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
sudo iptables -A FORWARD -m state --state ESTABLISHED -j ACCEPT
sudo iptables -A INPUT -i $AS -p tcp --dport 80 -j ACCEPT
sudo iptables -A INPUT -i $AS -p tcp --dport 8080 -j ACCEPT
sudo iptables -A FORWARD -i $AS -o $LAN -p tcp --dport 80 -j ACCEPT
sudo iptables -A FORWARD -i $AS -o $LAN -p tcp --dport 8080 -j ACCEPT

# Consenti il port forwarding con DNAT a
# hostA1 e hostA2 dalla rete esterna solo per il servizio HTTP
sudo iptables -t nat -A PREROUTING -i $AS -p tcp --dport 80 -j DNAT --to-destination 10.23.0.2
sudo iptables -t nat -A PREROUTING -i $AS -p tcp --dport 8080 -j DNAT --to-destination 10.23.0.3
```



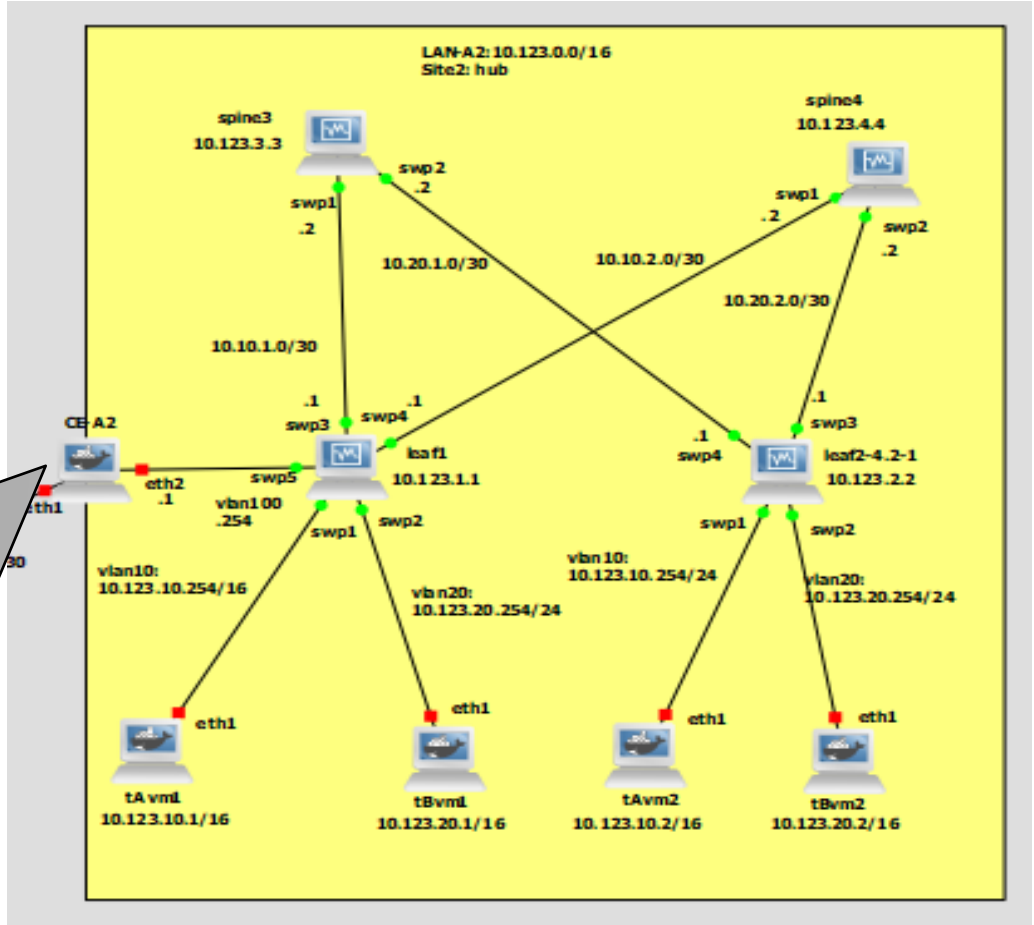
Firewall CE-A2

Politica di sicurezza (DROP predefinita):

- Consentire il traffico tra LAN-A2 e la rete esterna (incluse LAN-A1 e LAN-A3) solo se avviato da LAN-A2
- Permesso di inoltro tra gli spokes

Firewall CE-A2

```
iptables -F
iptables -t nat -F
iptables -X

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

export LAN=eth0
export NET=eth1

# Permetti il traffico in uscita dalla LAN-A2 verso la rete esterna
iptables -A FORWARD -i $LAN -o $NET -j ACCEPT
iptables -A FORWARD -s 10.123.0.0/16 -o $NET -j ACCEPT
# Permetti il traffico di risposta alle connessioni stabilite
iptables -A FORWARD -m state --state ESTABLISHED -j ACCEPT

# Configura il MASQUERADE per il traffico in uscita su eth1 (rete esterna)
iptables -A POSTROUTING -t nat -o eth1 -j MASQUERADE

# Permetti il traffico di forward tra gli spoke (LAN-A1 e LAN-A3)
iptables -A FORWARD -s 10.23.0.0/24 -d 10.23.1.0/24 -j ACCEPT
iptables -A FORWARD -s 10.23.1.0/24 -d 10.23.0.0/24 -j ACCEPT
```

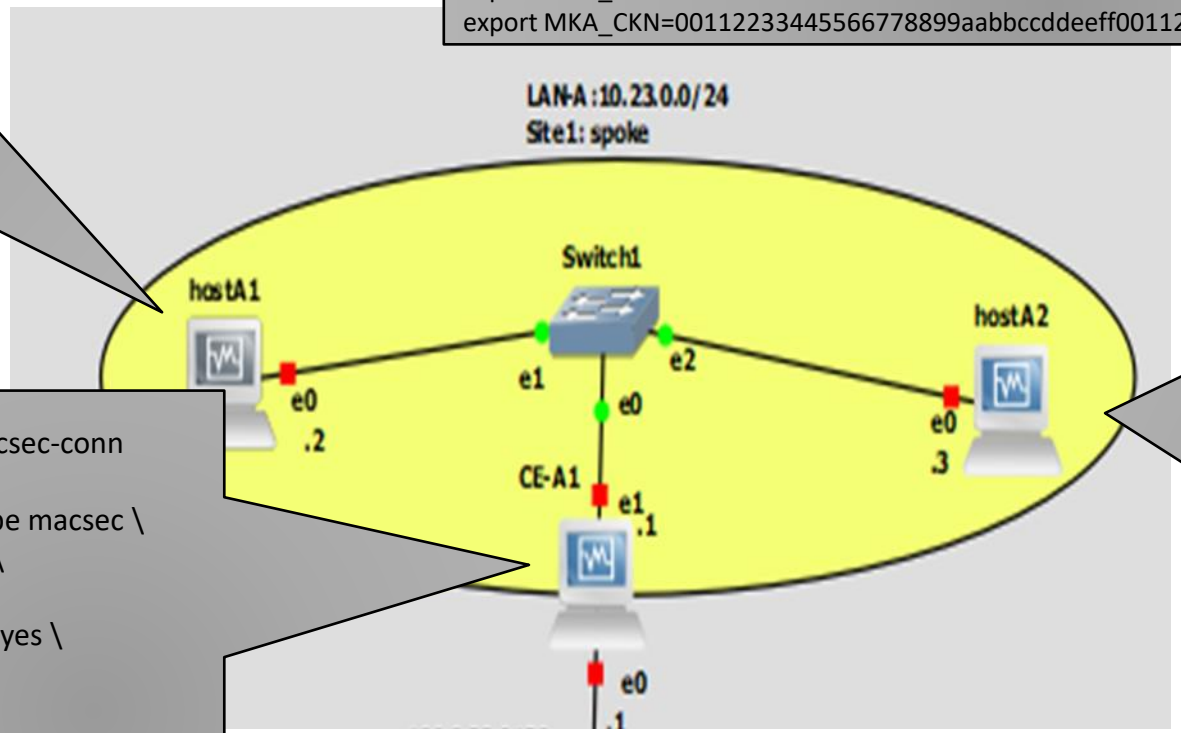


MACSEC

Macsec LAN-A1

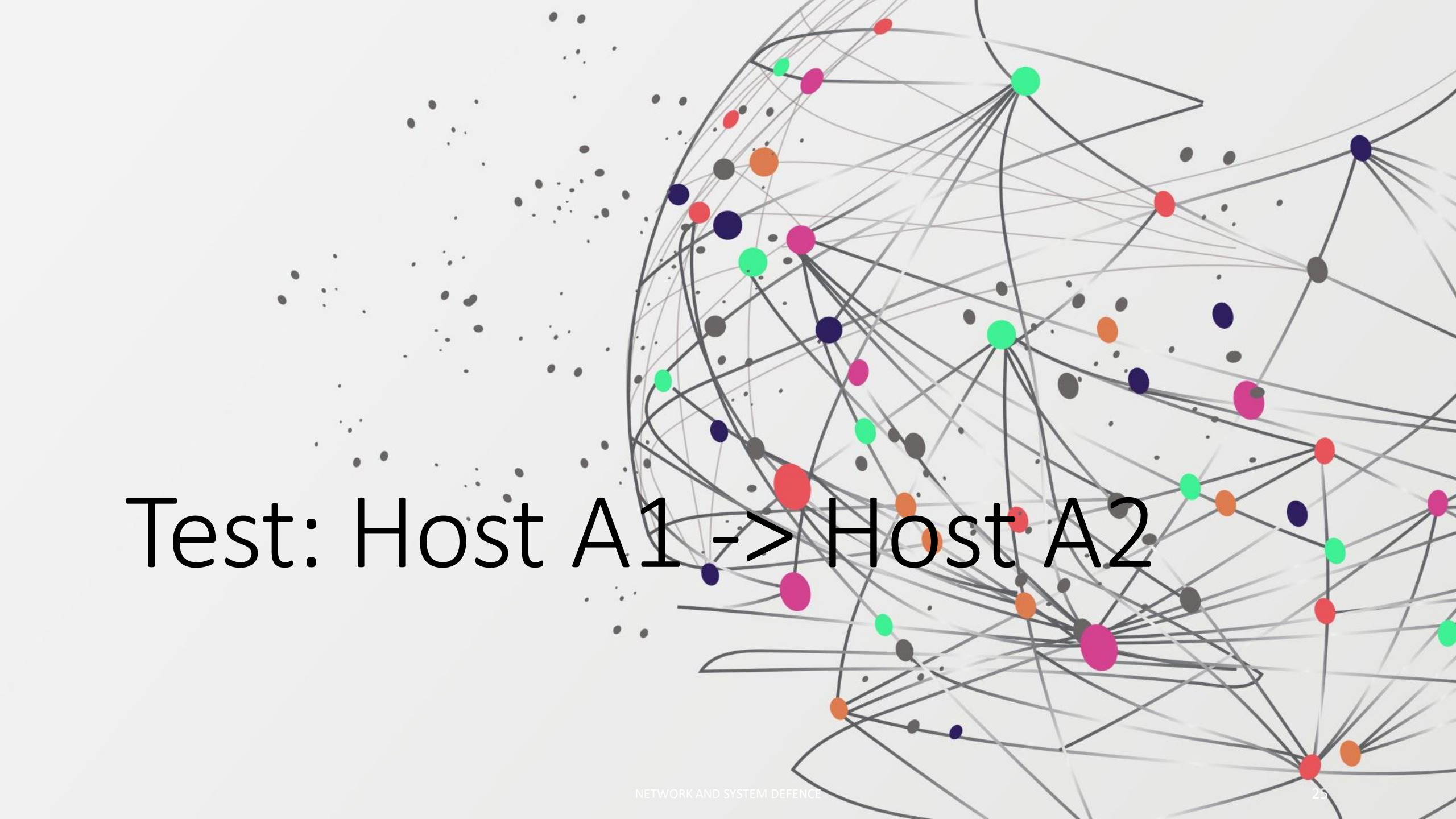
```
nmcli connection del macsec-conn

nmcli connection add type macsec \
con-name macsec-conn \
ifname macsec0 \
connection.autoconnect yes \
macsec.parent enp0s3 \
macsec.mode psk \
macsec.mka-cak $MKA_CAK \
macsec.mka-cak-flags 0 \
macsec.mka-ckn $MKA_CKN \
ipv4.method manual \
ipv4.addresses 10.23.0.2/24

nmcli connection up macsec-conn
```

```
export MKA_CAK=00112233445566778899aabbccddeeff
export MKA_CKN=00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff
```

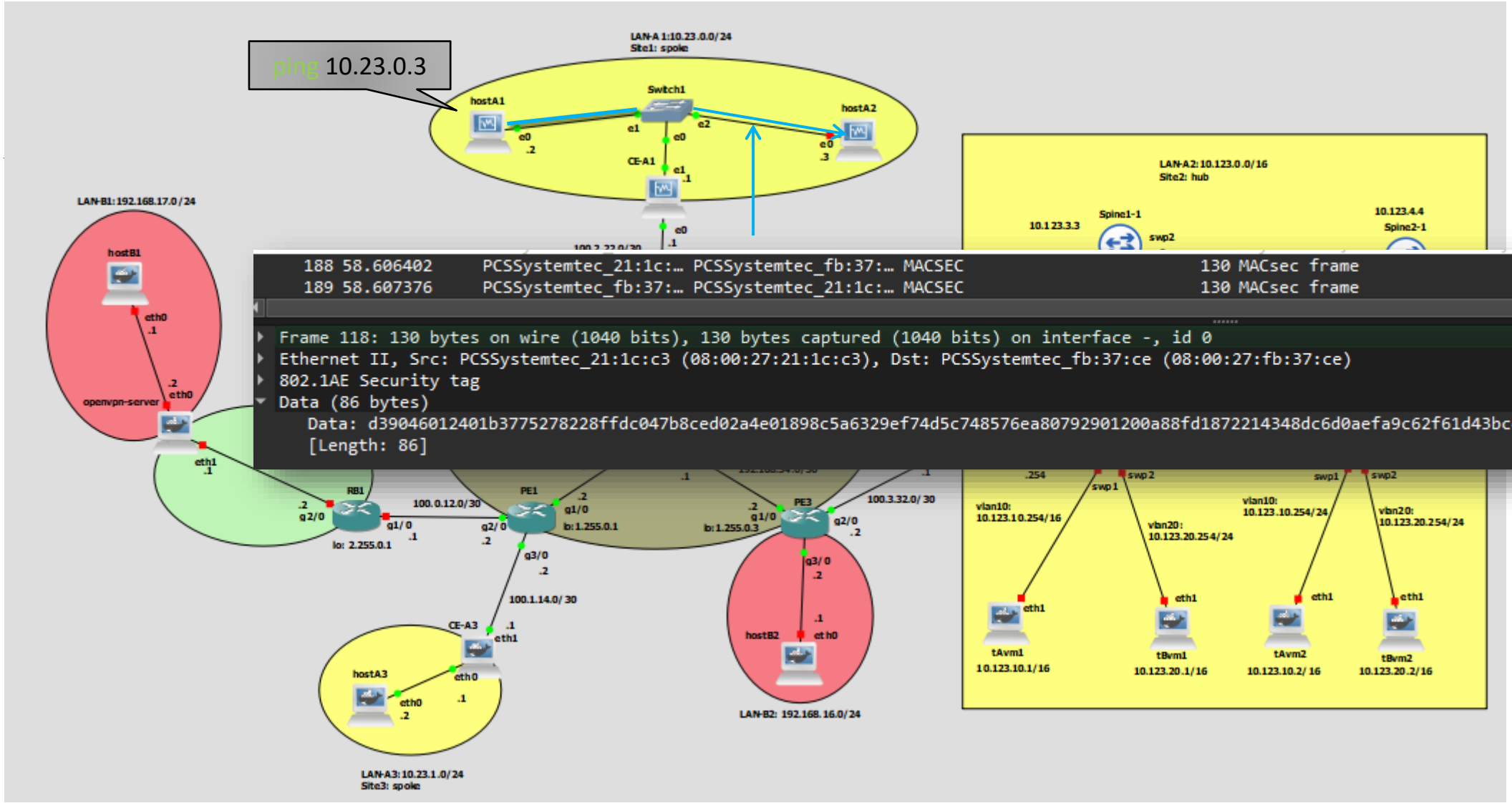


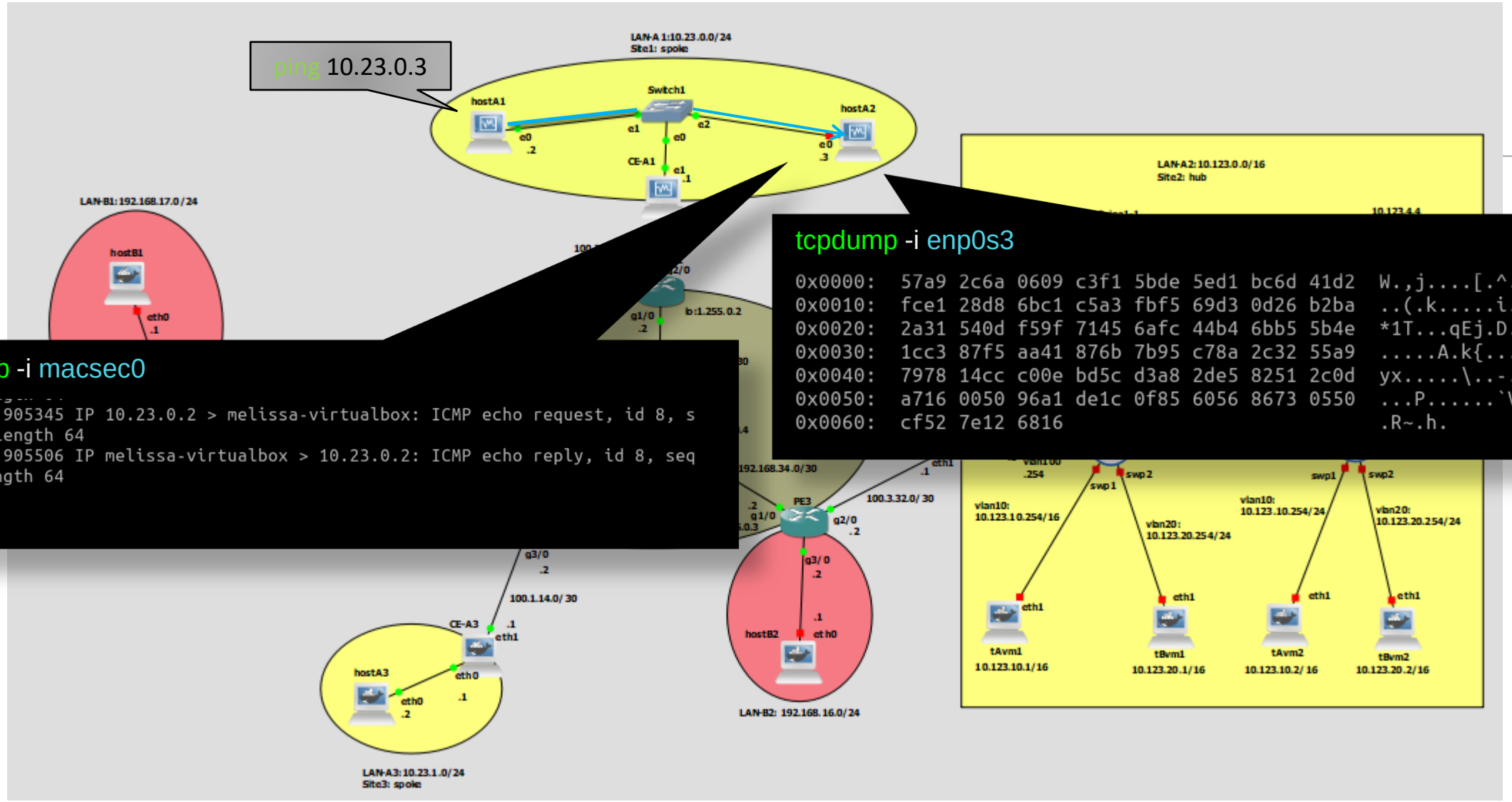

```
nmcli connection del macsec-conn

nmcli connection add type macsec \
con-name macsec-conn \
ifname macsec0 \
connection.autoconnect yes \
macsec.parent enp0s8 \
macsec.mode psk \
macsec.mka-cak $MKA_CAK \
macsec.mka-cak-flags 0 \
macsec.mka-ckn $MKA_CKN \
ipv4.method manual \
ipv4.addresses 10.23.0.1/24

nmcli connection up macsec-conn
```

```
nmcli connection del macsec-conn

nmcli connection add type macsec \
con-name macsec-conn \
ifname macsec0 \
connection.autoconnect yes \
macsec.parent enp0s3 \
macsec.mode psk \
macsec.mka-cak $MKA_CAK \
macsec.mka-cak-flags 0 \
macsec.mka-ckn $MKA_CKN \
ipv4.method manual \
ipv4.addresses 10.23.0.3/24

nmcli connection up macsec-conn
```



Test: Host A1 -> Host A2


ping 10.23.0.3
LAN-A 1:10.23.0.0/24
Site1: spoke
hostA1
Switch1
hostA2
e0
e1
e2
.2
.3
CE-A1
.1
LAN-B1:192.168.17.0/24
hostB1
eth0
.1
.2
openvpn-server
eth1
RB1
100.0.12.0/30
PE1
PE3
100.3.32.0/30
lo: 2.255.0.1
lo:1.255.0.1
lo:1.255.0.3
q1/0
q2/0
q3/0
100.1.14.0/30
CE-A3
hostA3
hostB2
LAN-B2: 192.168.16.0/24
LAN-A3:10.23.1.0/24
Site3: spoke
LAN-A2:10.123.0.0/16
Site2: hub
Spine1-1
Spine2-1
10.123.3.3
10.123.4.4
swp1
swp2
vlan10:
10.123.10.254/16
vlan20:
10.123.20.254/24
tAvm1
10.123.10.1/16
tBvm1
10.123.20.1/16
tAvm2
10.123.10.2/16
tBvm2
10.123.20.2/16
188 58.606402 PCSSystemtec_21:1c:… PCSSystemtec_fb:37:… MACSEC 130 MACsec frame
189 58.607376 PCSSystemtec_fb:37:… PCSSystemtec_21:1c:… MACSEC 130 MACsec frame
Frame 118: 130 bytes on wire (1040 bits), 130 bytes captured (1040 bits) on interface -, id 0
Ethernet II, Src: PCSSystemtec_21:1c:c3 (08:00:27:21:1c:c3), Dst: PCSSystemtec_fb:37:ce (08:00:27:fb:37:ce)
802.1AE Security tag
Data (86 bytes)
Data: d39046012401b3775278228ffdc047b8ced02a4e01898c5a6329ef74d5c748576ea80792901200a88fd1872214348dc6d0aefa9c62f61d43bce472b3f2…
[Length: 86]


ping 10.23.0.3
LAN-A 1:10.23.0.0/24
Site1: spoke
hostA1
Switch1
hostA2
e0
.2
e1
e0
e2
e0
.3
CE-A1
e1
.1
LAN-B1:192.168.17.0/24
hostB1
eth0
.1
LAN-A2:10.123.0.0/16
Site2: hub
tcpdump -i macsec0
00:15:11.905345 IP 10.23.0.2 > melissa-virtualbox: ICMP echo request, id 8, seq 609, length 64
00:15:11.905506 IP melissa-virtualbox > 10.23.0.2: ICMP echo reply, id 8, seq 609, length 64
tcpdump -i enp0s3
0x0000: 57a9 2c6a 0609 c3f1 5bde 5ed1 bc6d 41d2 W.,j....[.^..mA.
0x0010: fce1 28d8 6bc1 c5a3 fbf5 69d3 0d26 b2ba ..(.k.....i..&..
0x0020: 2a31 540d f59f 7145 6afc 44b4 6bb5 5b4e *1T...qEj.D.k.[N
0x0030: 1cc3 87f5 aa41 876b 7b95 c78a 2c32 55a9 .....A.k{...,2U.
0x0040: 7978 14cc c00e bd5c d3a8 2de5 8251 2c0d yx.....\..-..Q,.
0x0050: a716 0050 96a1 de1c 0f85 6056 8673 0550 ...P.....`V.s.P
0x0060: cf52 7e12 6816 .R~.h.
192.168.34.0/30
PE3
100.3.32.0/30
q1/0
q2/0
q3/0
100.1.14.0/30
CE-A3
hostA3
eth0
LAN-A3:10.23.1.0/24
Site3: spoke
hostB2
LAN-B2: 192.168.16.0/24
vlan10:
10.123.10.254/16
vlan20:
10.123.20.254/24
swp1
swp2
tAvm1
10.123.10.1/16
tBvm1
10.123.20.1/16
tAvm2
10.123.10.2/16
tBvm2
10.123.20.2/16

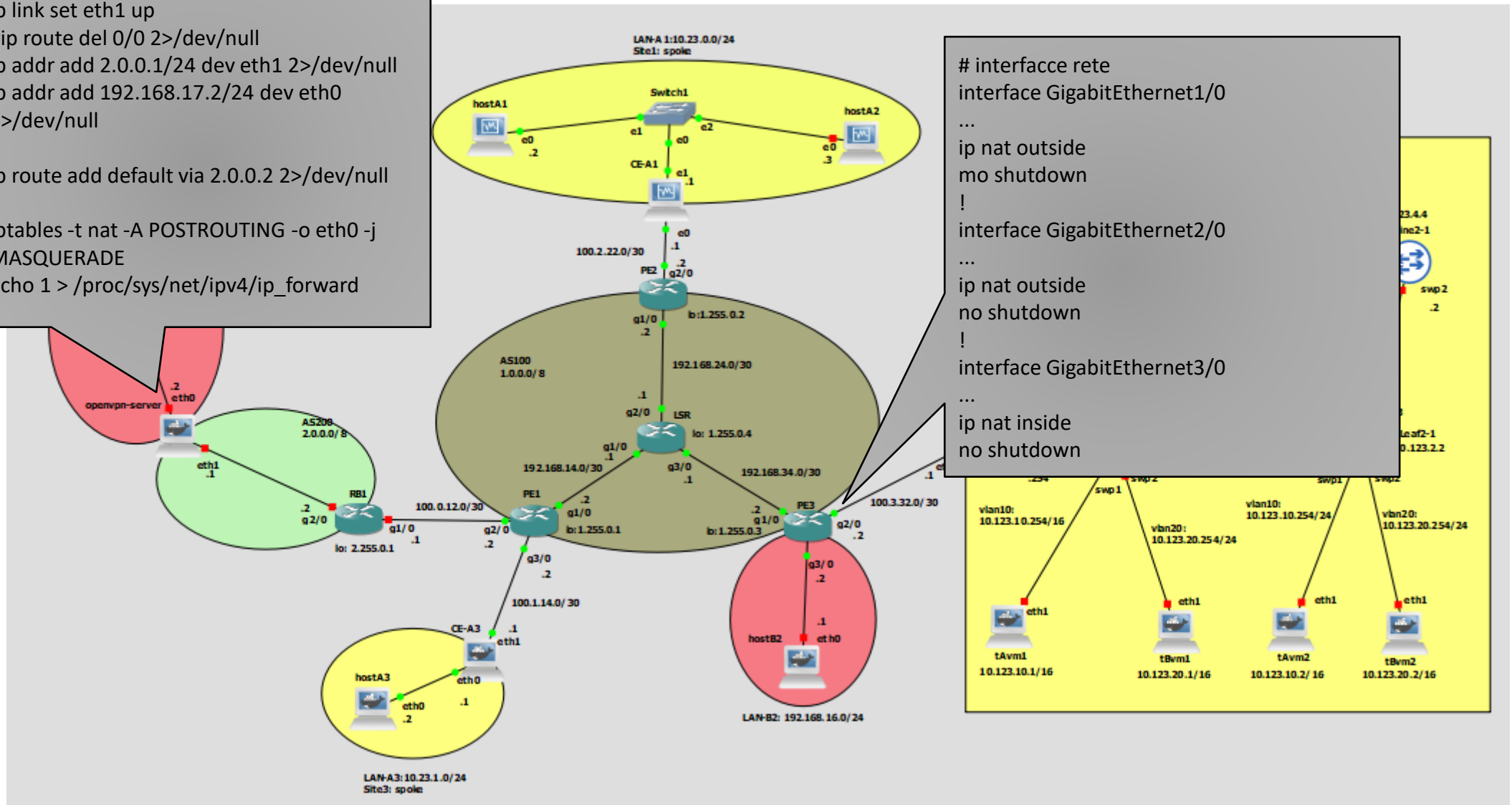
OPENVPN

OpenVPN

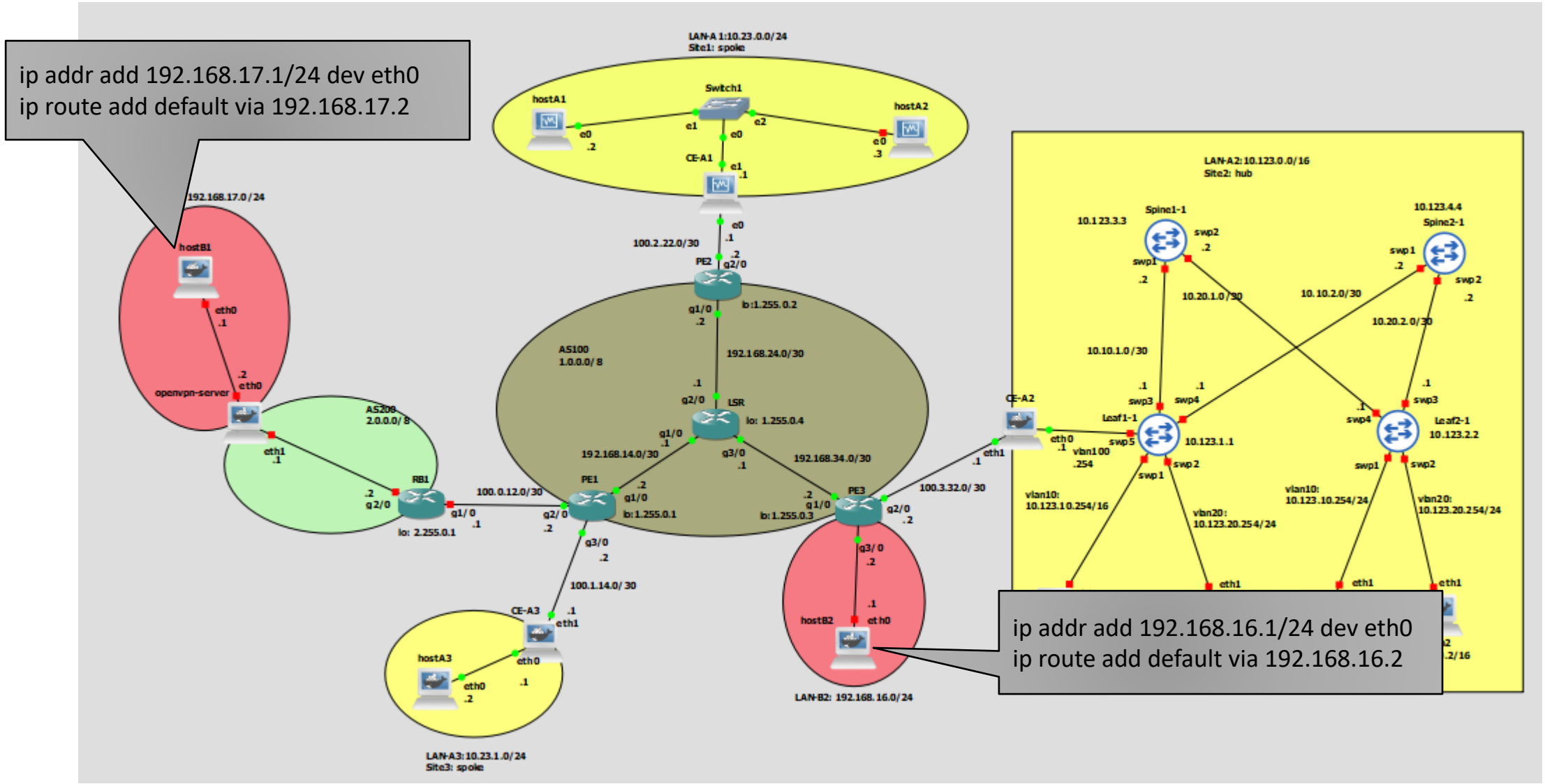
Configura OpenVPN con un server e un client. Il server è in AS200, con un IP pubblico preso dalla rete 2.0.0.0/8.

Il client è host-B2, dietro la rete privata in LAN-B2. Il server OpenVPN fornisce l'accesso a LAN-B1 a cui funge da gateway.

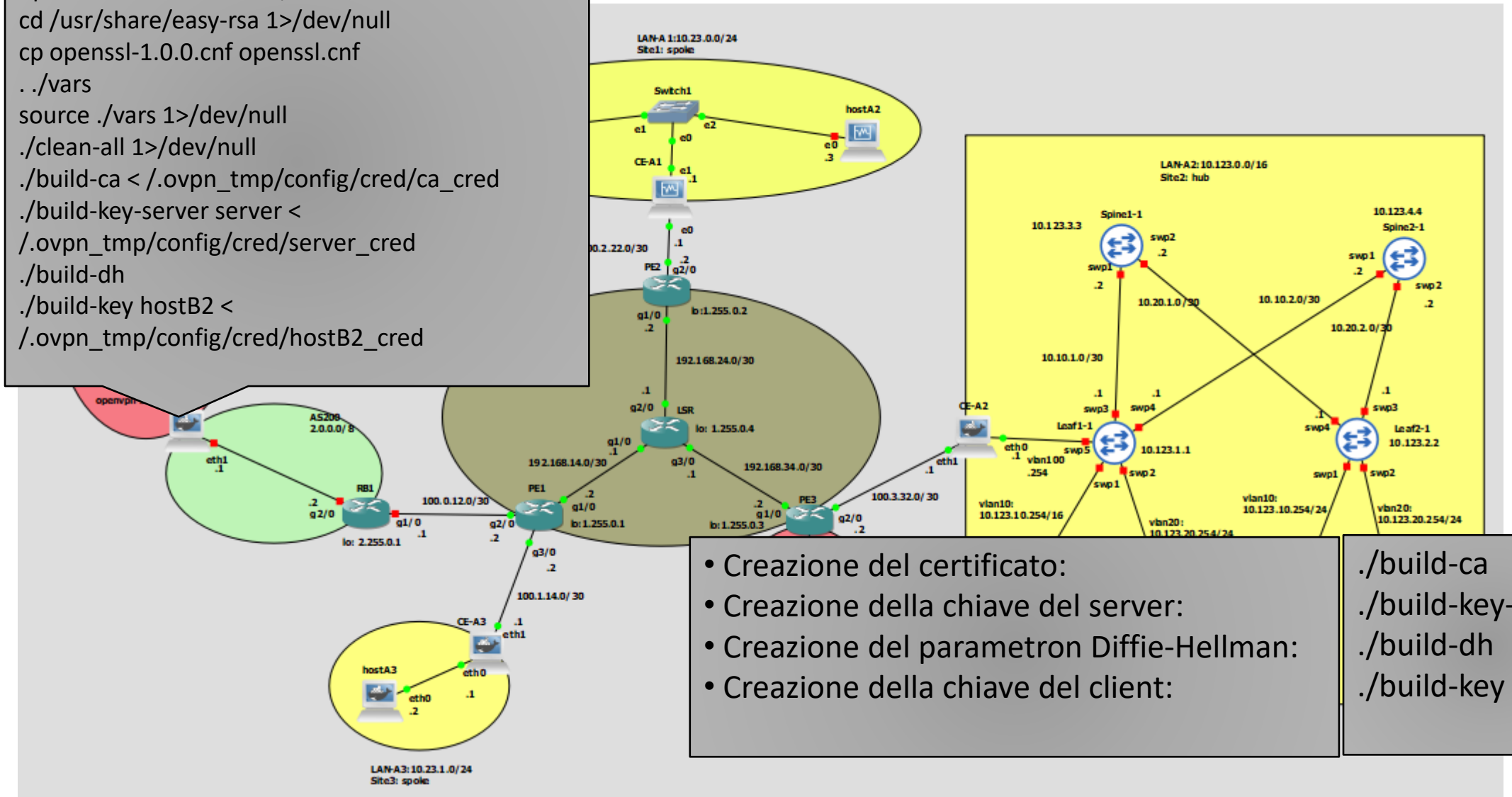
```
ip link set eth0 up
ip link set eth1 up
#ip route del 0/0 2>/dev/null
ip addr add 2.0.0.1/24 dev eth1 2>/dev/null
ip addr add 192.168.17.2/24 dev eth0
2>/dev/null

ip route add default via 2.0.0.2 2>/dev/null

iptables -t nat -A POSTROUTING -o eth0 -j
MASQUERADE
echo 1 > /proc/sys/net/ipv4/ip_forward
```




```
# interfacce rete
interface GigabitEthernet1/0
...
ip nat outside
mo shutdown
!
interface GigabitEthernet2/0
...
ip nat outside
no shutdown
!
interface GigabitEthernet3/0
...
ip nat inside
no shutdown
```


ip addr add 192.168.17.1/24 dev eth0
ip route add default via 192.168.17.2
LAN-A 1:10.23.0.0/24
Site1: spoke
hostA1
Switch1
hostA2
CE-A1
192.168.17.0/24
hostB1
openvpn-server
AS200
2.0.0.0/8
RB1
lo: 2.255.0.1
100.2.22.0/30
PE2
lo:1.255.0.2
AS100
1.0.0.0/8
192.168.24.0/30
LSR
lo: 1.255.0.4
192.168.14.0/30
192.168.34.0/30
100.0.12.0/30
PE1
lo:1.255.0.1
PE3
lo:1.255.0.3
100.3.32.0/30
100.1.14.0/30
CE-A3
hostA3
LAN-A3:10.23.1.0/24
Site3: spoke
CE-A2
hostB2
LAN-B2: 192.168.16.0/24
LAN-A2:10.123.0.0/16
Site2: hub
Spine1-1
10.123.3.3
Spine2-1
10.123.4.4
10.20.1.0/30
10.10.2.0/30
10.20.2.0/30
10.10.1.0/30
Leaf1-1
10.123.1.1
Leaf2-1
10.123.2.2
vlan100
.254
vlan10:
10.123.10.254/16
vlan20:
10.123.20.254/24
ip addr add 192.168.16.1/24 dev eth0
ip route add default via 192.168.16.2

```
# Configura chiavi e certificati openvpn sul Server
openssl rand -writerand /.rnd
cd /usr/share/easy-rsa 1>/dev/null
cp openssl-1.0.0.cnf openssl.cnf
. ./vars
source ./vars 1>/dev/null
./clean-all 1>/dev/null
./build-ca < /.ovpn_tmp/config/cred/ca_cred
./build-key-server server <
/.ovpn_tmp/config/cred/server_cred
./build-dh
./build-key hostB2 <
/.ovpn_tmp/config/cred/hostB2_cred
```



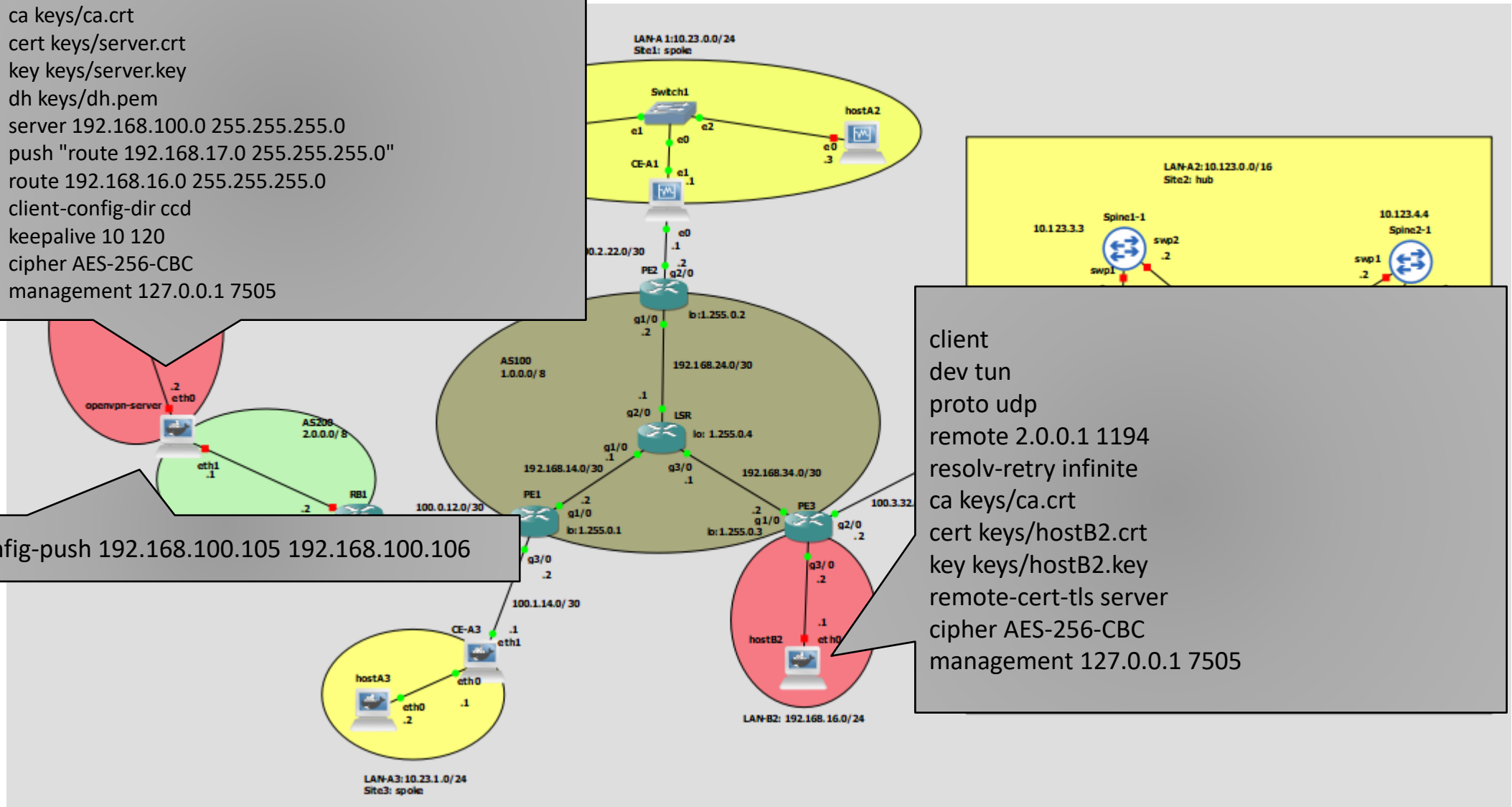
- Creazione del certificato:
- Creazione della chiave del server:
- Creazione del parametron Diffie-Hellman:
- Creazione della chiave del client:

```
./build-ca
./build-key-server
./build-dh
./build-key
```

Generazione chiave per CA

Nome file	Installazione
ca.crt	Server + client
ca.key	Chi genera il gertificato
dh.pem	Server
server.crt	Server
server.key	Server
client.crt	Client
client.key	Client

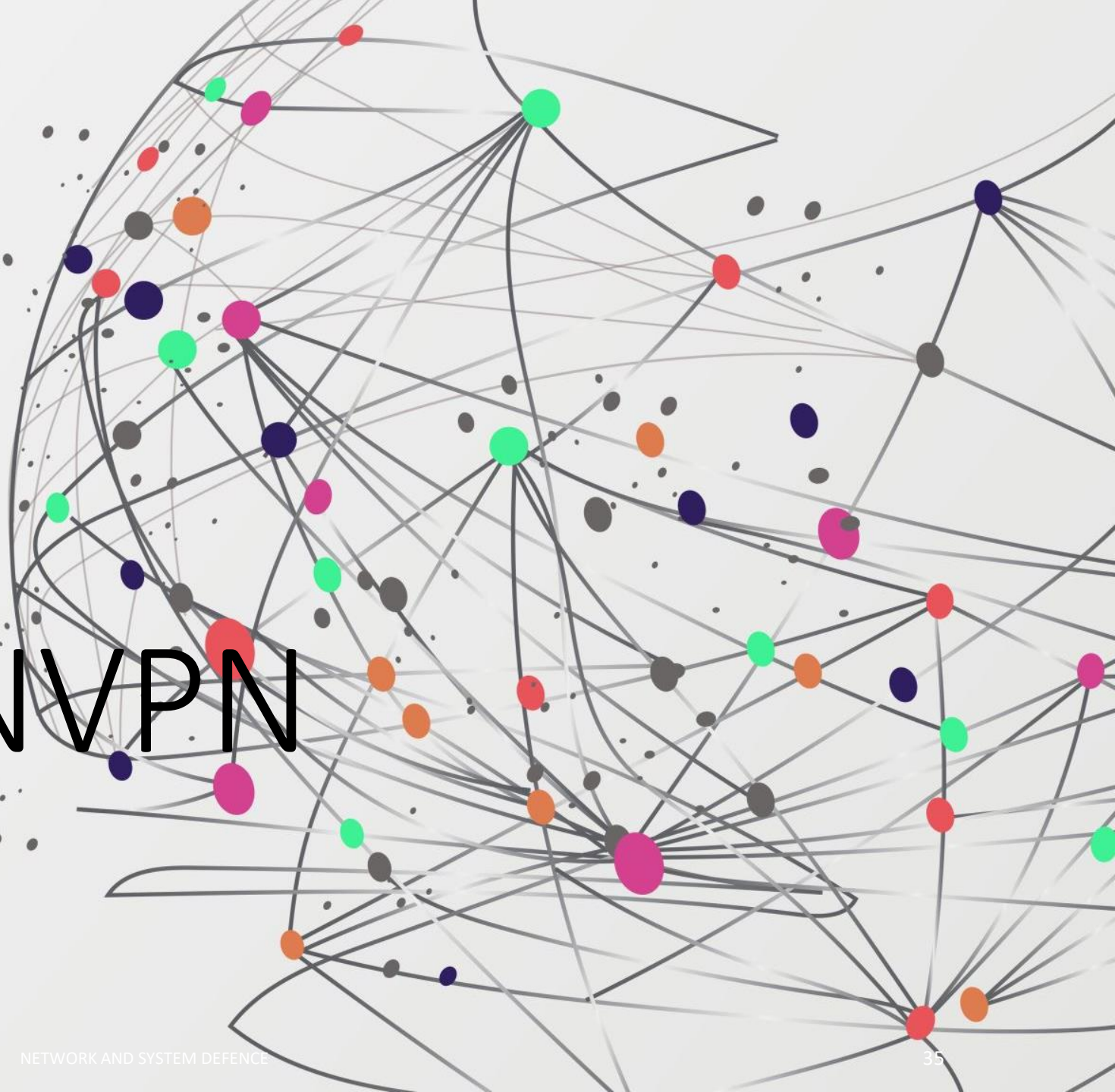
port 1194
proto udp
dev tun
ca keys/ca.crt
cert keys/server.crt
key keys/server.key
dh keys/dh.pem
server 192.168.100.0 255.255.255.0
push "route 192.168.17.0 255.255.255.0"
route 192.168.16.0 255.255.255.0
client-config-dir ccd
keepalive 10 120
cipher AES-256-CBC
management 127.0.0.1 7505

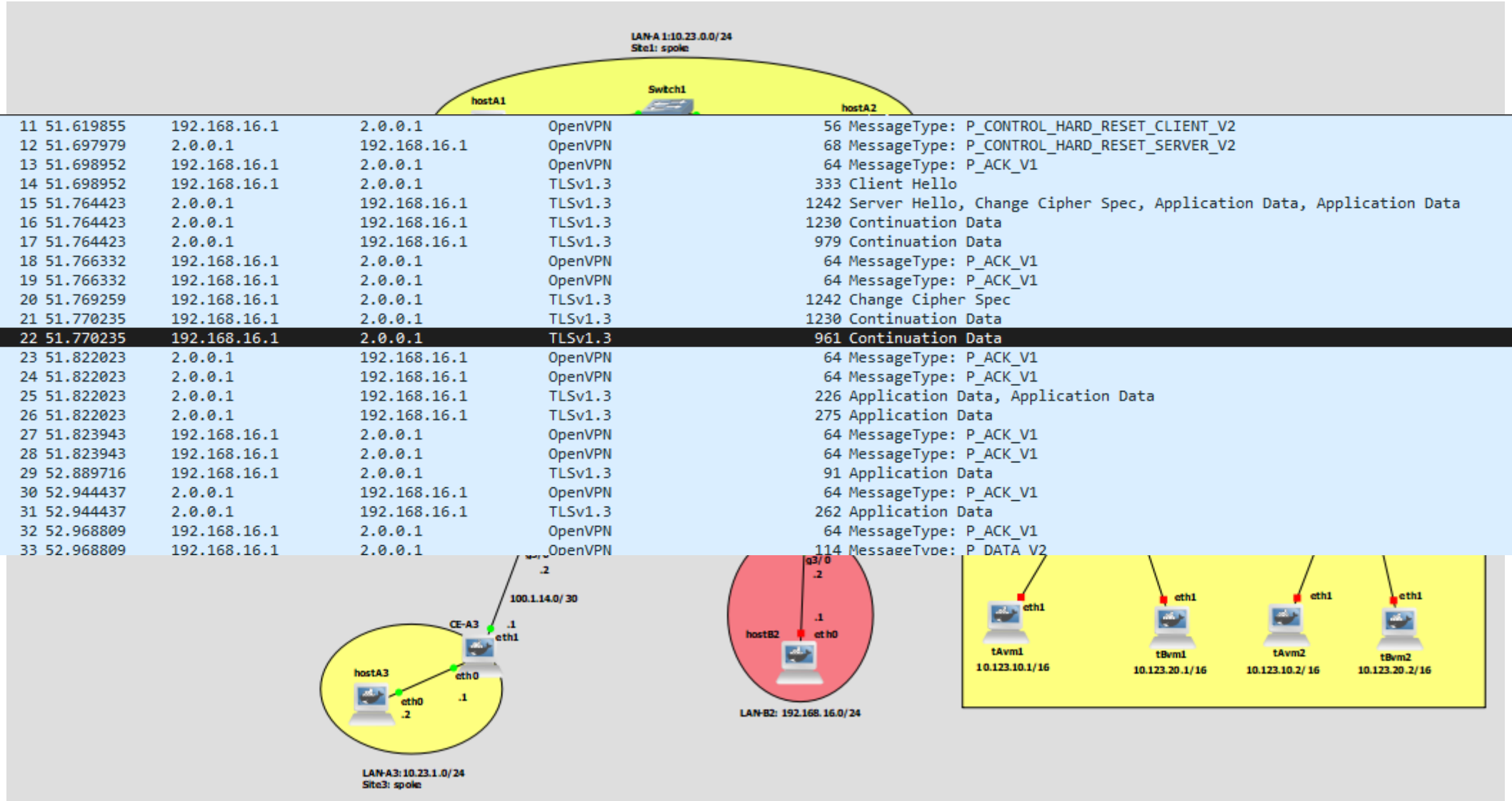


if-config-push 192.168.100.105 192.168.100.106

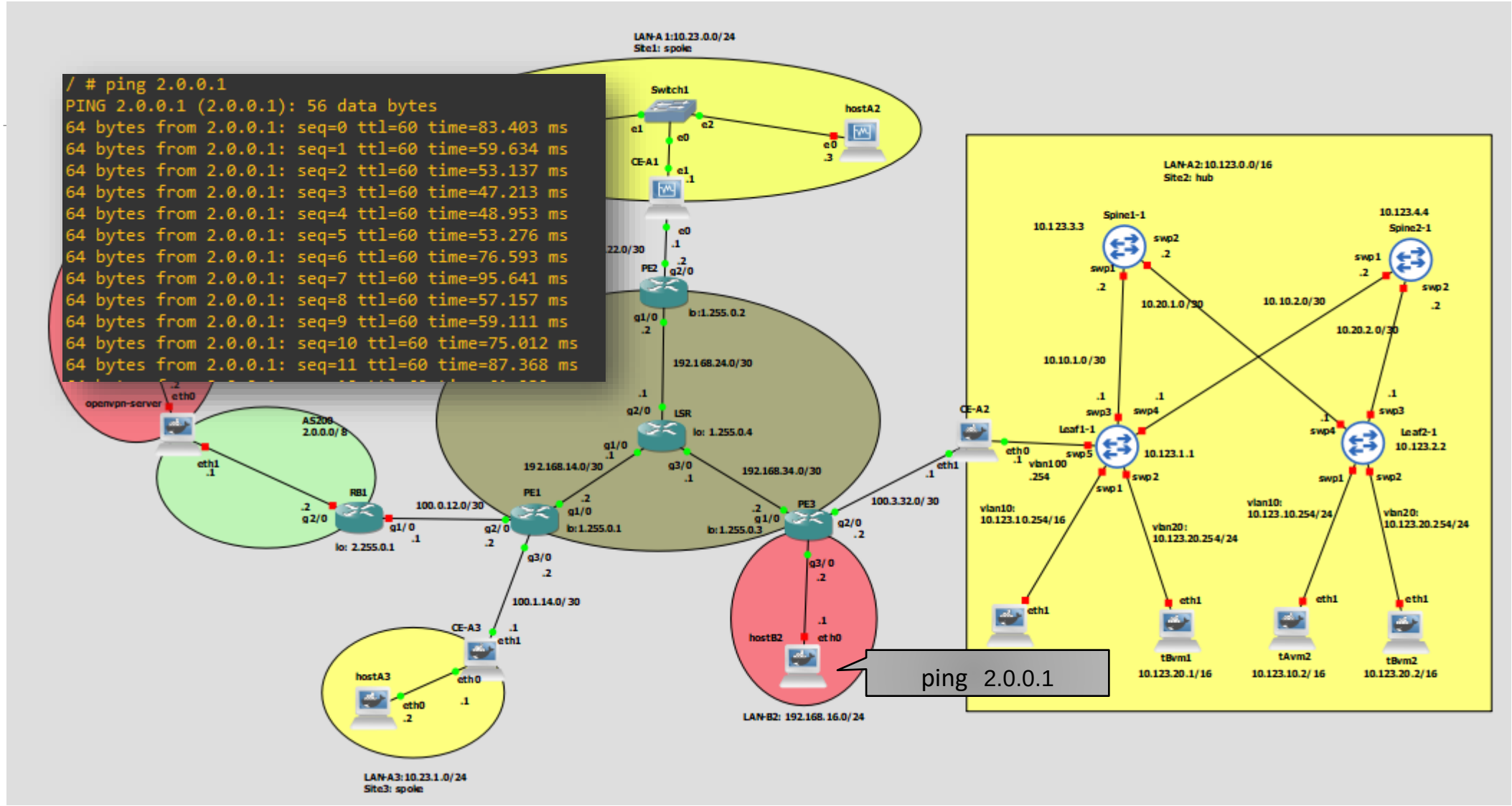
client
dev tun
proto udp
remote 2.0.0.1 1194
resolv-retry infinite
ca keys/ca.crt
cert keys/hostB2.crt
key keys/hostB2.key
remote-cert-tls server
cipher AES-256-CBC
management 127.0.0.1 7505

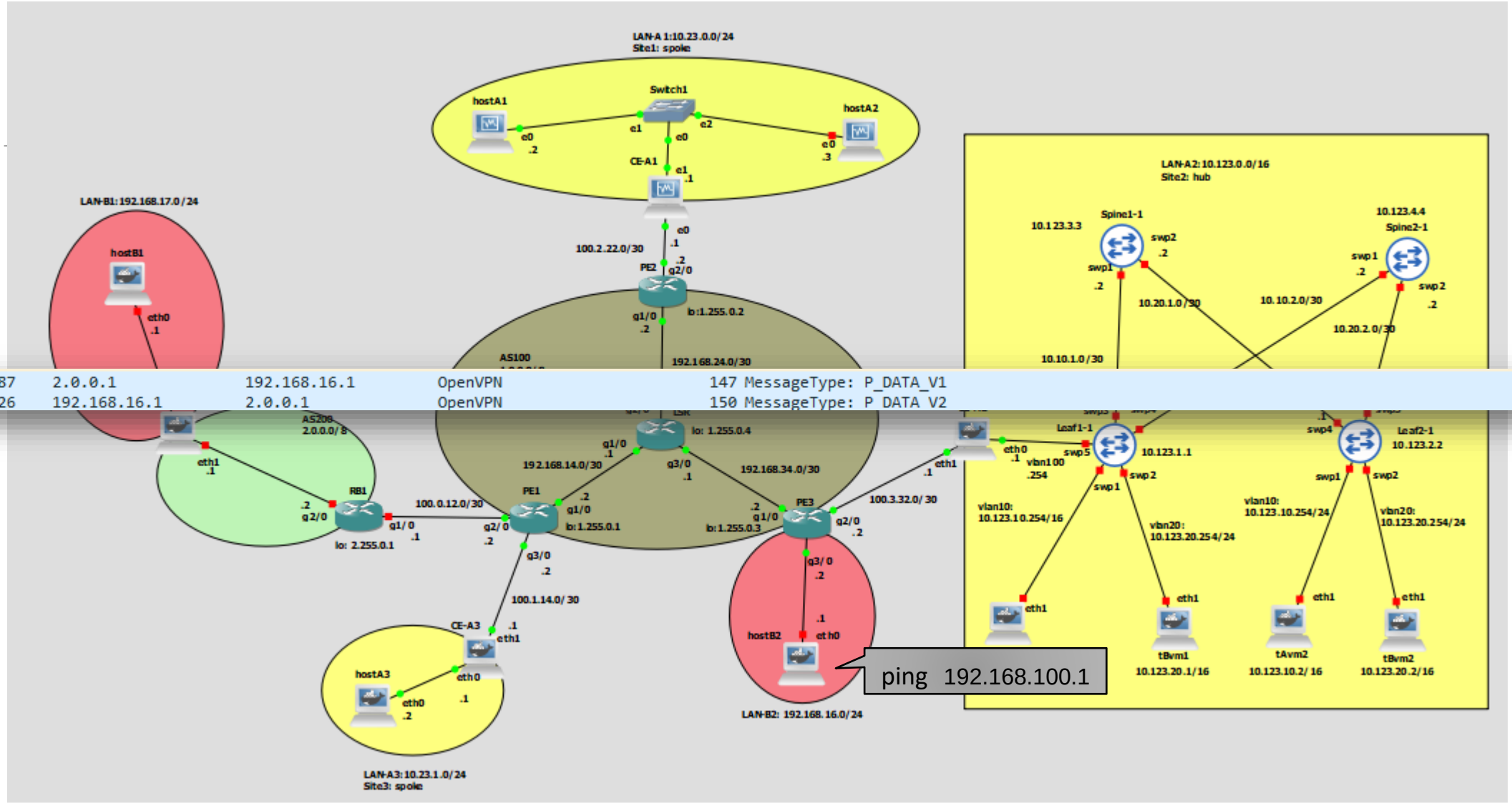
Test: OPENVPN





11	51.619855	192.168.16.1	2.0.0.1	OpenVPN	56 MessageType: P_CONTROL_HARD_RESET_CLIENT_V2
12	51.697979	2.0.0.1	192.168.16.1	OpenVPN	68 MessageType: P_CONTROL_HARD_RESET_SERVER_V2
13	51.698952	192.168.16.1	2.0.0.1	OpenVPN	64 MessageType: P_ACK_V1
14	51.698952	192.168.16.1	2.0.0.1	TLSv1.3	333 Client Hello
15	51.764423	2.0.0.1	192.168.16.1	TLSv1.3	1242 Server Hello, Change Cipher Spec, Application Data, Application Data
16	51.764423	2.0.0.1	192.168.16.1	TLSv1.3	1230 Continuation Data
17	51.764423	2.0.0.1	192.168.16.1	TLSv1.3	979 Continuation Data
18	51.766332	192.168.16.1	2.0.0.1	OpenVPN	64 MessageType: P_ACK_V1
19	51.766332	192.168.16.1	2.0.0.1	OpenVPN	64 MessageType: P_ACK_V1
20	51.769259	192.168.16.1	2.0.0.1	TLSv1.3	1242 Change Cipher Spec
21	51.770235	192.168.16.1	2.0.0.1	TLSv1.3	1230 Continuation Data
22	51.770235	192.168.16.1	2.0.0.1	TLSv1.3	961 Continuation Data
23	51.822023	2.0.0.1	192.168.16.1	OpenVPN	64 MessageType: P_ACK_V1
24	51.822023	2.0.0.1	192.168.16.1	OpenVPN	64 MessageType: P_ACK_V1
25	51.822023	2.0.0.1	192.168.16.1	TLSv1.3	226 Application Data, Application Data
26	51.822023	2.0.0.1	192.168.16.1	TLSv1.3	275 Application Data
27	51.823943	192.168.16.1	2.0.0.1	OpenVPN	64 MessageType: P_ACK_V1
28	51.823943	192.168.16.1	2.0.0.1	OpenVPN	64 MessageType: P_ACK_V1
29	52.889716	192.168.16.1	2.0.0.1	TLSv1.3	91 Application Data
30	52.944437	2.0.0.1	192.168.16.1	OpenVPN	64 MessageType: P_ACK_V1
31	52.944437	2.0.0.1	192.168.16.1	TLSv1.3	262 Application Data
32	52.968809	192.168.16.1	2.0.0.1	OpenVPN	64 MessageType: P_ACK_V1
33	52.968809	192.168.16.1	2.0.0.1	OpenVPN	114 MessageType: P_DATA_V2


/ # ping 2.0.0.1
PING 2.0.0.1 (2.0.0.1): 56 data bytes
64 bytes from 2.0.0.1: seq=0 ttl=60 time=83.403 ms
64 bytes from 2.0.0.1: seq=1 ttl=60 time=59.634 ms
64 bytes from 2.0.0.1: seq=2 ttl=60 time=53.137 ms
64 bytes from 2.0.0.1: seq=3 ttl=60 time=47.213 ms
64 bytes from 2.0.0.1: seq=4 ttl=60 time=48.953 ms
64 bytes from 2.0.0.1: seq=5 ttl=60 time=53.276 ms
64 bytes from 2.0.0.1: seq=6 ttl=60 time=76.593 ms
64 bytes from 2.0.0.1: seq=7 ttl=60 time=95.641 ms
64 bytes from 2.0.0.1: seq=8 ttl=60 time=57.157 ms
64 bytes from 2.0.0.1: seq=9 ttl=60 time=59.111 ms
64 bytes from 2.0.0.1: seq=10 ttl=60 time=75.012 ms
64 bytes from 2.0.0.1: seq=11 ttl=60 time=87.368 ms
LAN-A 1:10.23.0.0/24
Site1: spoke
Switch1
hostA2
CE-A1
PE2
lo:1.255.0.2
192.168.24.0/30
LSR
lo: 1.255.0.4
openvpn-server
AS200
2.0.0.0/8
RB1
lo: 2.255.0.1
100.0.12.0/30
PE1
lo:1.255.0.1
192.168.14.0/30
192.168.34.0/30
PE3
lo:1.255.0.3
100.3.32.0/30
CE-A2
CE-A3
100.1.14.0/30
hostA3
hostB2
LAN-B2: 192.168.16.0/24
LAN-A3:10.23.1.0/24
Site3: spoke
LAN-A2:10.123.0.0/16
Site2: hub
Spine1-1
10.123.3.3
Spine2-1
10.123.4.4
10.20.1.0/30
10.10.2.0/30
10.20.2.0/30
10.10.1.0/30
Leaf1-1
10.123.1.1
Leaf2-1
10.123.2.2
vlan10:
10.123.10.254/16
vlan20:
10.123.20.254/24
tBvm1
10.123.20.1/16
tAvm2
10.123.10.2/16
tBvm2
10.123.20.2/16
ping 2.0.0.1



192 265.482187	2.0.0.1	192.168.16.1	OpenVPN	147 MessageType: P_DATA_V1
193 266.434426	192.168.16.1	2.0.0.1	OpenVPN	150 MessageType: P_DATA_V2

VXLAN/EVPN

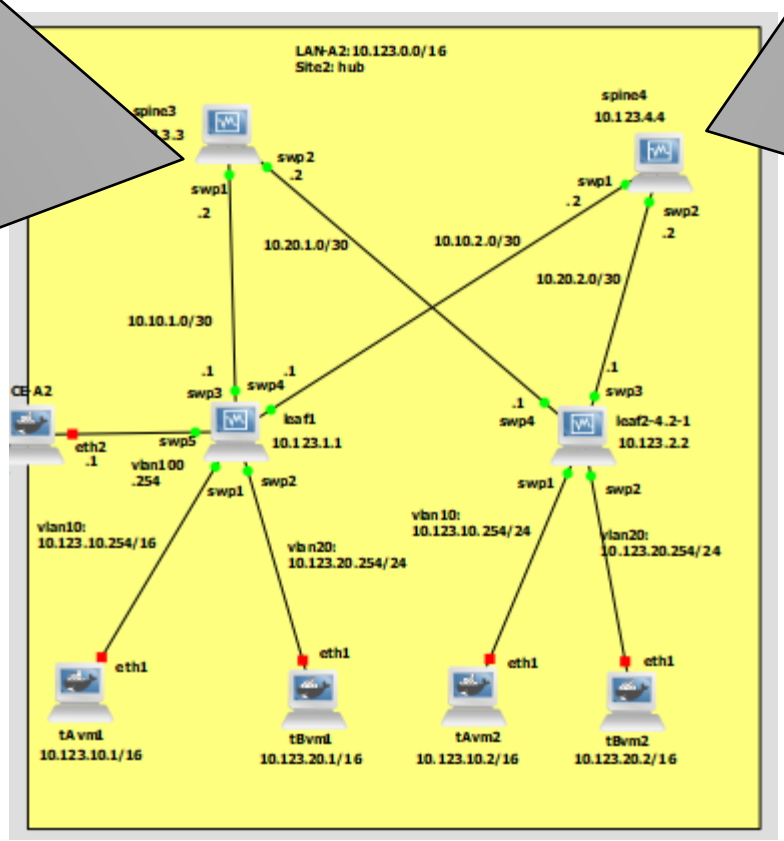
VXLAN EVPN

LAN A2 è una rete di Datacenter leaf-spine con due foglie e due spine. Nella rete cloud sono presenti 2 tenant, ognuno dei quali ospita due macchine connesse, una a leaf1 e l'altra a leaf2.

Ai tenant viene assegnato un dominio broadcast ciascuno

Spines

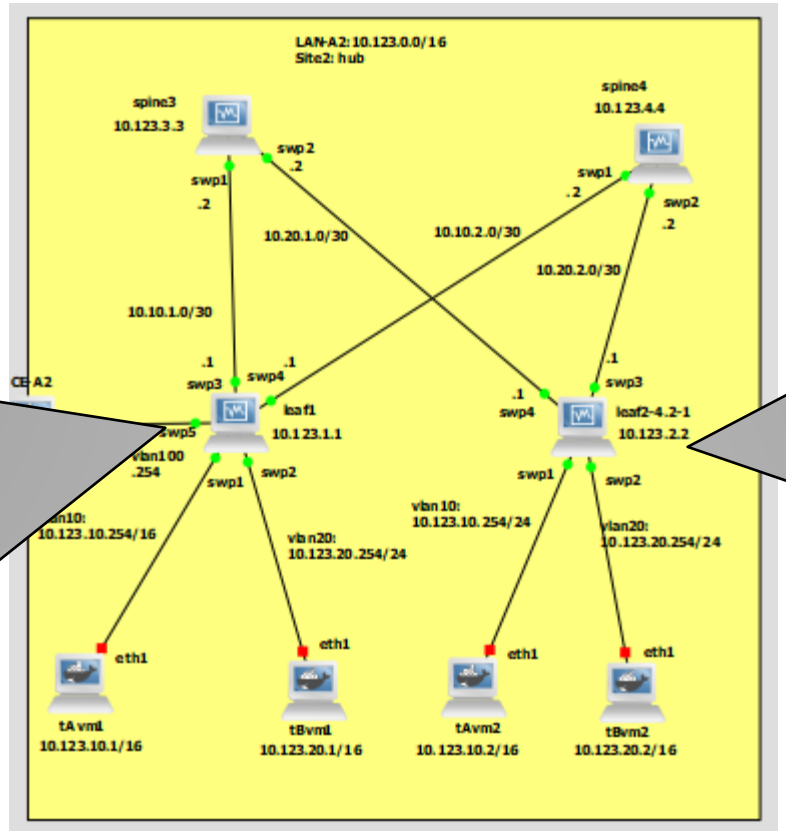
```
#!/bin/sh

net add hostname spine1

# spine - ip addresses
net add interface swp1 ip add 10.10.1.2/30
net add interface swp2 ip add 10.20.1.2/30
net add loopback lo ip add 10.123.3.3/32

# ospf
net add ospf router-id 10.123.3.3
net add ospf network 10.123.3.3/32 area 0
net add ospf network 10.10.1.0/30 area 0
net add ospf network 10.20.1.0/30 area 0
net add ospf network 0.0.0.0/0 area 0

# ebgp
net add bgp autonomous-system 65000
net add bgp router-id 10.123.3.3
net add bgp neighbor swp1 remote-as
external
net add bgp neighbor swp2 remote-as
external
net add bgp evpn neighbor swp1 activate
net add bgp evpn neighbor swp2 activate

net pending
net commit
```




```
#!/bin/bash

net add hostname spine2

# spine - ip addresses
net add interface swp1 ip add 10.10.2.2/30
net add interface swp2 ip add 10.20.2.2/30
net add loopback lo ip add 10.123.4.4/32

# ospf
net add ospf router-id 10.123.4.4
net add ospf network 10.123.4.4/32 area 0
net add ospf network 10.10.2.0/30 area 0
net add ospf network 10.20.2.0/30 area 0
net add ospf network 0.0.0.0/0 area 0

# ebgp
net add bgp autonomous-system 65000
net add bgp router-id 10.123.4.4
net add bgp neighbor swp1 remote-as
external
net add bgp neighbor swp2 remote-as
external
net add bgp evpn neighbor swp1 activate
net add bgp evpn neighbor swp2 activate

net pending
net commit
```

Leaf

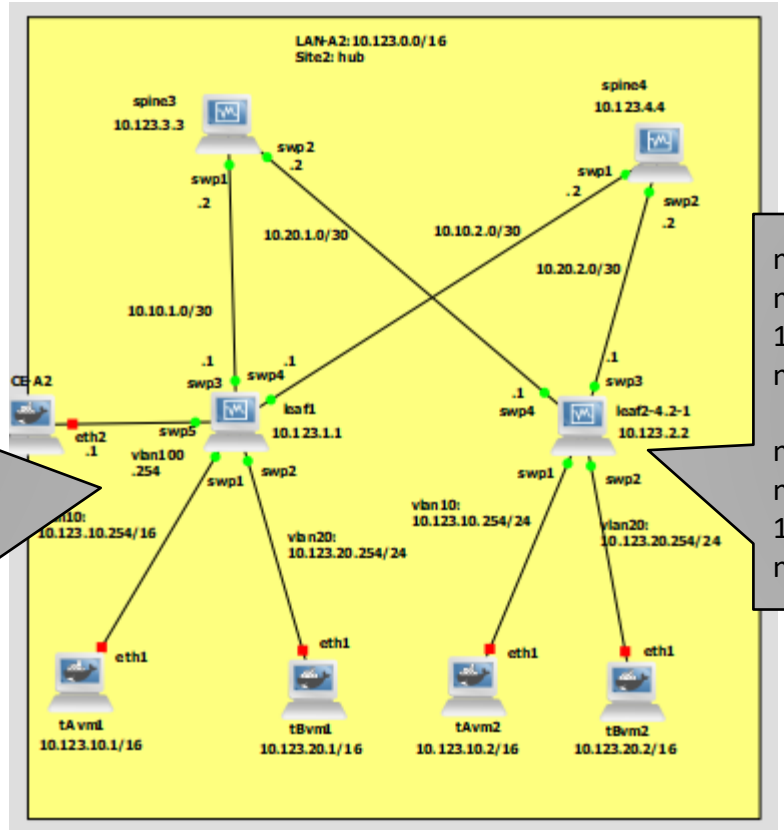
```
net add bridge bridge ports swp1,swp2,swp5
net add bridge bridge vids 10,20,100,200
net add interface swp1 bridge access 10
net add interface swp2 bridge access 20

# leaves - ip addresses
net add interface swp3 ip add 10.10.1.1/30
net add interface swp4 ip add 10.10.2.1/30
net add loopback lo ip add 10.123.1.1/32

# ospf
net add ospf router-id 10.123.1.1
net add ospf network 10.10.1.0/30 area 0
net add ospf network 10.10.2.0/30 area 0
net add ospf network 10.123.1.1/32 area 0
net add ospf passive-interface swp1
net add ospf passive-interface swp2
```




```
net add bridge bridge ports swp1,swp2
net add interface swp1 bridge access 10
net add interface swp2 bridge access 20

# ip address leaf
net add interface swp4 ip add 10.20.1.1/30
net add interface swp3 ip add 10.20.2.1/30
net add loopback lo ip add 10.123.2.2/32

# ospf
net add ospf router-id 10.123.2.2
net add ospf network 10.20.1.0/30 area 0
net add ospf network 10.20.2.0/30 area 0
net add ospf network 10.123.2.2/32 area 0
net add ospf passive-interface swp1
net add ospf passive-interface swp2
```

Leaf

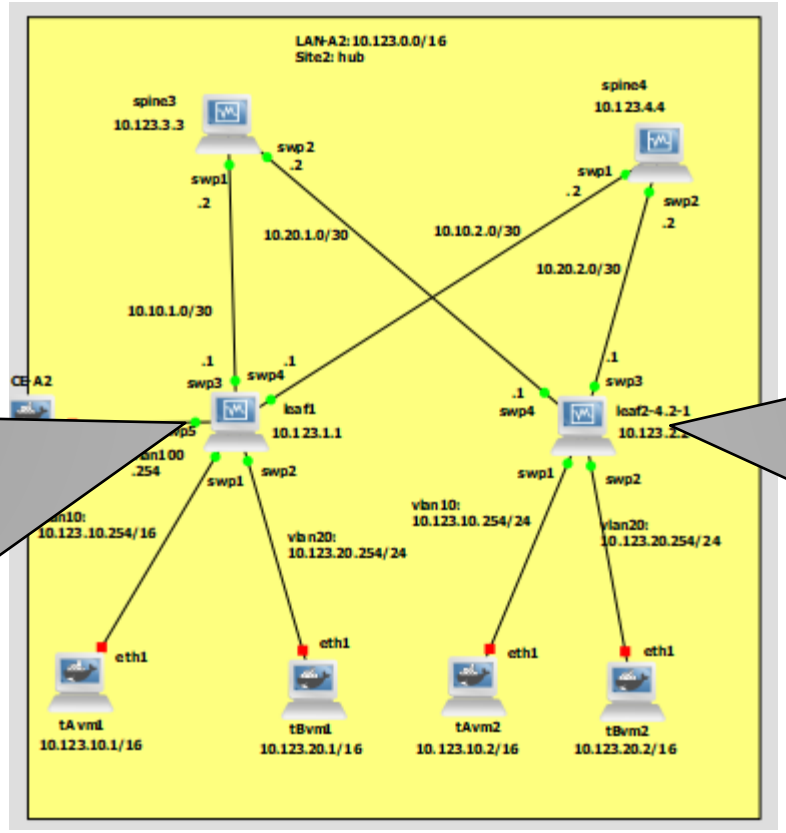
```
# vxlan
net add vxlan vni10 vxlan id 10
net add vxlan vni10 vxlan local-tunnelip
10.123.1.1
net add vxlan vni10 bridge access 10

net add vxlan vni20 vxlan id 20
net add vxlan vni20 vxlan local-tunnelip
10.123.1.1
net add vxlan vni20 bridge access 20

net add vxlan vni100 vxlan id 100
net add vxlan vni100 vxlan local-tunnelip
10.123.1.1
net add vxlan vni100 bridge access 100

net add vxlan vni200 vxlan id 200
net add vxlan vni200 vxlan local-tunnelip
10.123.1.1
net add vxlan vni200 bridge access 200
```




```
net add vxlan vni10 vxlan id 10
net add vxlan vni10 vxlan local-tunnelip
10.123.2.2
net add vxlan vni10 bridge access 10

net add vxlan vni20 vxlan id 20
net add vxlan vni20 vxlan local-tunnelip
10.123.2.2
net add vxlan vni20 bridge access 20
```

Leaf

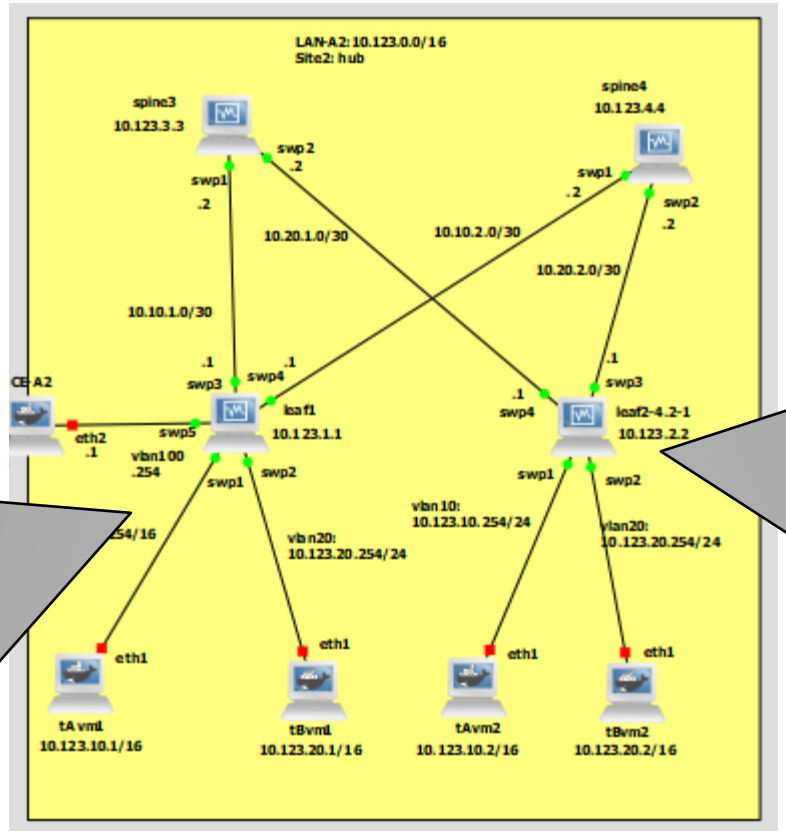
```
# ebgp
net add bgp autonomous-system 65001
net add bgp router-id 10.123.1.1
net add bgp neighbor swp3 remote-as 65000
net add bgp neighbor swp4 remote-as 65000
net add bgp evpn neighbor swp3 activate
net add bgp evpn neighbor swp4 activate
net add bgp evpn advertise-all-vni

# add ip address in vteps
net add vlan 10 ip address 10.123.10.254/24
net add vlan 20 ip address 10.123.20.254/24

net add vlan 100 ip address 10.123.0.254/16
net add vlan 100 ip gateway 10.123.0.1

net add vlan 200 ip address 10.123.0.254/16
net add vlan 200 ip gateway 10.123.0.1
```




```
# ebgp
net add bgp autonomous-system 65002
net add bgp router-id 10.123.2.2
net add bgp neighbor swp3 remote-as 65000
net add bgp neighbor swp4 remote-as 65000
net add bgp evpn neighbor swp3 activate
net add bgp evpn neighbor swp4 activate
net add bgp evpn advertise-all-vni

# default route end-host
net add vlan 10 ip address 10.123.10.254/24
net add vlan 20 ip address 10.123.20.254/24
```

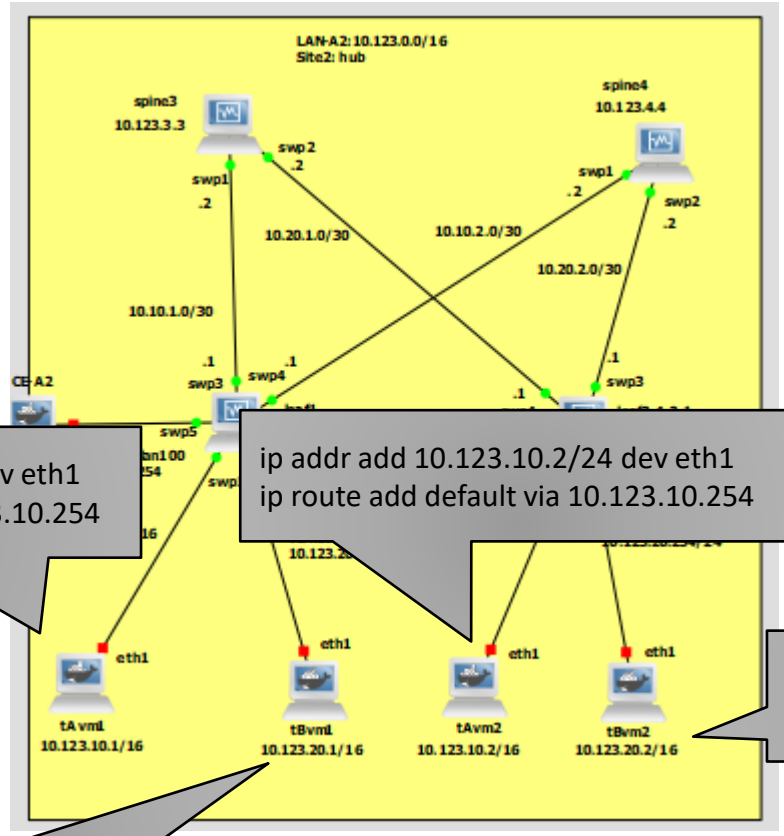
Leaf

```
net add vxlan vni50 vxlan id 50
net add vxlan vni50 vxlan local-tunnelip 10.123.1.1
net add vxlan vni50 bridge access 50
net add vxlan vni60 vxlan id 60
net add vxlan vni60 vxlan local-tunnelip 10.123.1.1
net add vxlan vni60 bridge access 60

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

net add bgp vrf TENA autonomous-system 65001
net add bgp vrf TENA l2vpn evpn advertise ipv4 unicast
net add bgp vrf TENA l2vpn evpn default-originate ipv4

net add bgp vrf TENB autonomous-system 65001
net add bgp vrf TENB l2vpn evpn advertise ipv4 unicast
net add bgp vrf TENB l2vpn evpn default-originate ipv4
```




```
net add vxlan vni50 vxlan id 50
net add vxlan vni50 vxlan local-tunnelip
10.123.2.2
net add vxlan vni50 bridge access 50
net add vxlan vni60 vxlan id 60
net add vxlan vni60 vxlan local-tunnelip
10.123.2.2
net add vxlan vni60 bridge access 60

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

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

Tenants



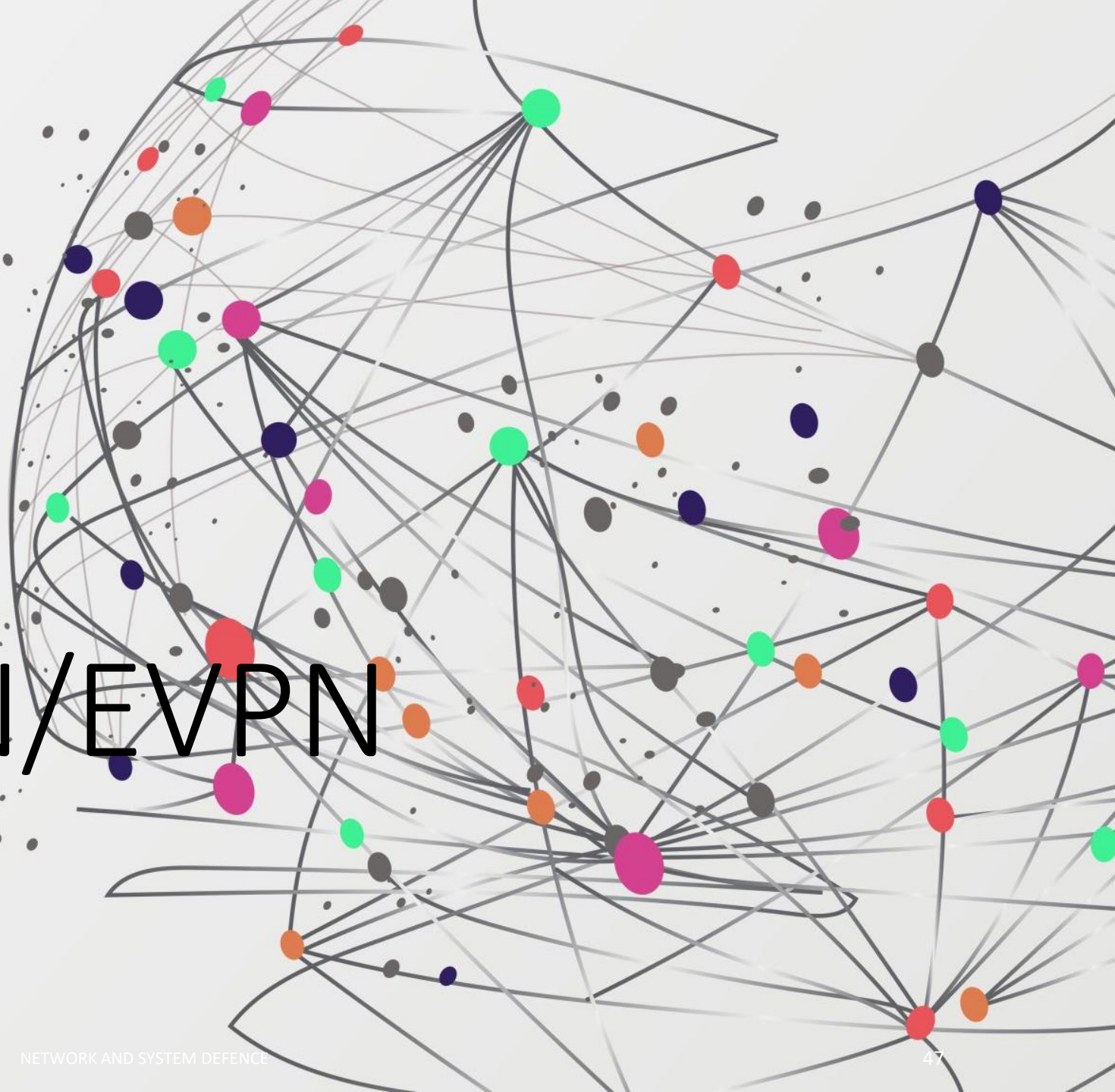
ip addr add 10.123.10.1/24 dev eth1
ip route add default via 10.123.10.254

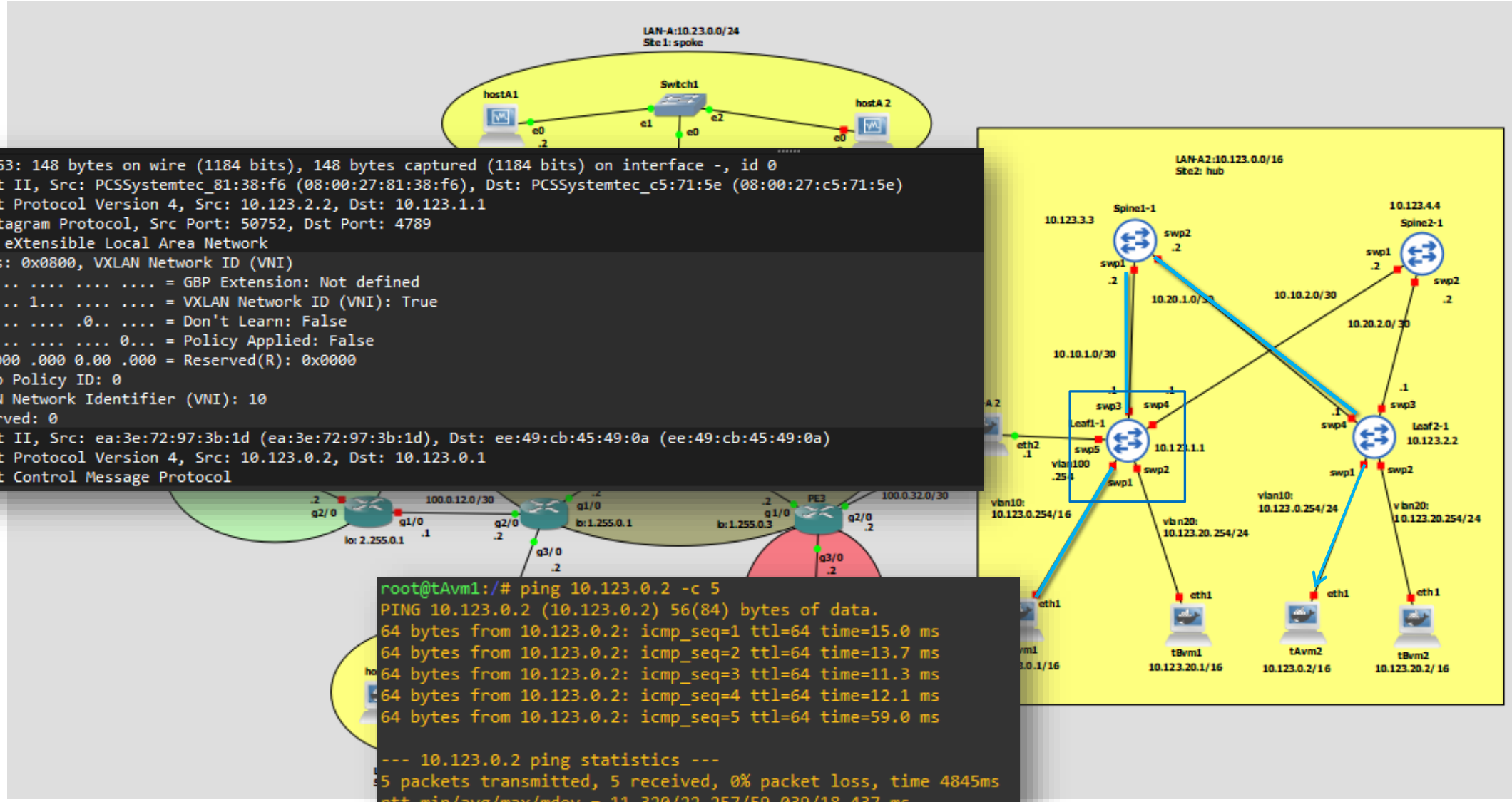
ip addr add 10.123.10.2/24 dev eth1
ip route add default via 10.123.10.254

ip addr add 10.123.20.2/24 dev eth1
ip route add default via 10.123.20.254

ip addr add 10.123.20.1/24 dev eth1
ip route add default via 10.123.20.254

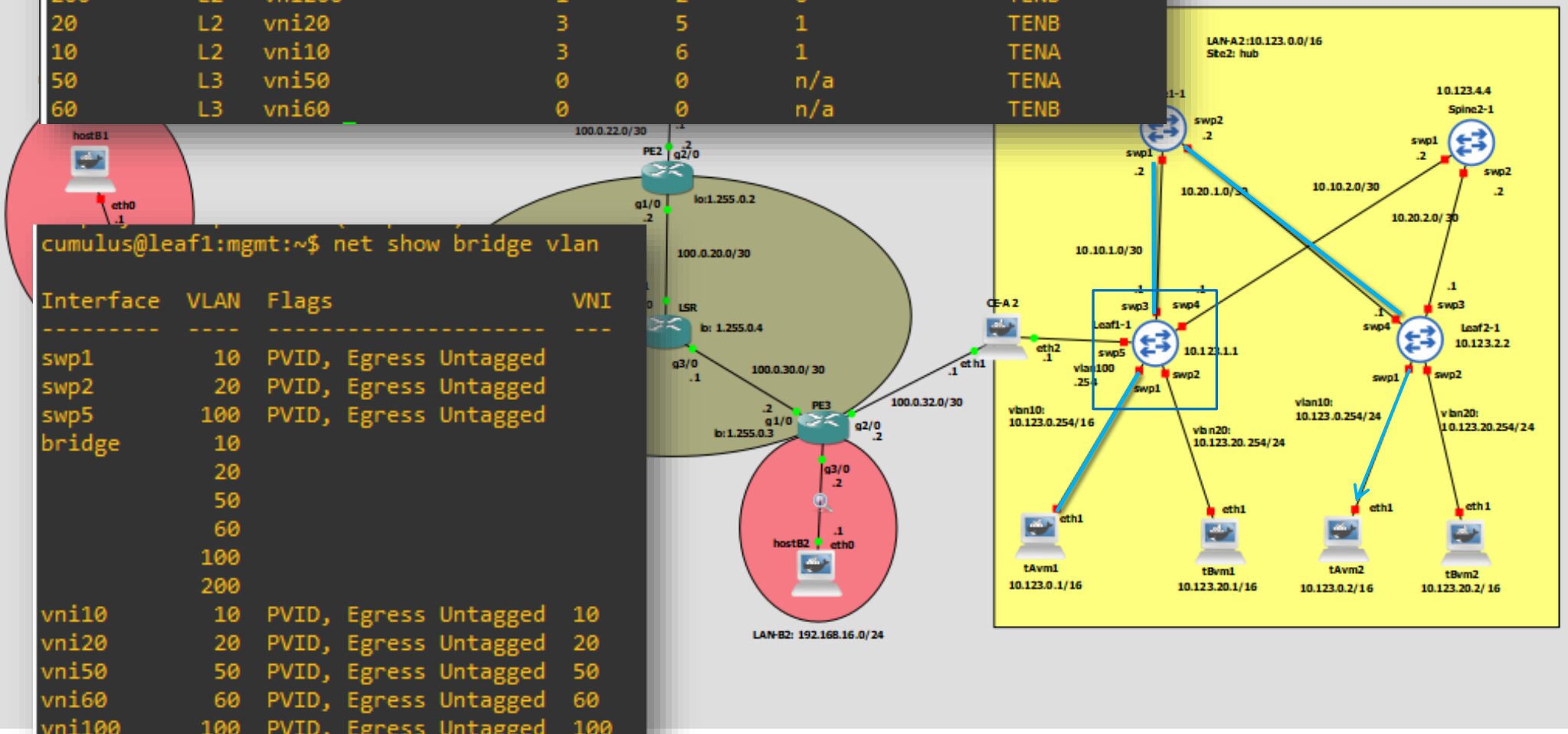
Test: VXLAN/EVPN




LAN-A:10.23.0.0/24
Site 1: spoke
hostA1
Switch1
hostA 2
e0
e1
e2
.2
Frame 463: 148 bytes on wire (1184 bits), 148 bytes captured (1184 bits) on interface -, id 0
Ethernet II, Src: PCSSystemtec_81:38:f6 (08:00:27:81:38:f6), Dst: PCSSystemtec_c5:71:5e (08:00:27:c5:71:5e)
Internet Protocol Version 4, Src: 10.123.2.2, Dst: 10.123.1.1
User Datagram Protocol, Src Port: 50752, Dst Port: 4789
Virtual eXtensible Local Area Network
Flags: 0x0800, VXLAN Network ID (VNI)
0... .... = GBP Extension: Not defined
.... 1... .... = VXLAN Network ID (VNI): True
.... .0.. .... = Don't Learn: False
.... 0... = Policy Applied: False
.000 .000 0.00 .000 = Reserved(R): 0x0000
Group Policy ID: 0
VXLAN Network Identifier (VNI): 10
Reserved: 0
Ethernet II, Src: ea:3e:72:97:3b:1d (ea:3e:72:97:3b:1d), Dst: ee:49:cb:45:49:0a (ee:49:cb:45:49:0a)
Internet Protocol Version 4, Src: 10.123.0.2, Dst: 10.123.0.1
Internet Control Message Protocol
LAN-A2:10.123.0.0/16
Site2: hub
Spine1-1
10.123.3.3
Spine2-1
10.123.4.4
swp1
swp2
10.10.1.0/30
10.10.2.0/30
10.20.1.0/30
10.20.2.0/30
Leaf1-1
Leaf2-1
10.123.1.1
10.123.2.2
swp3
swp4
swp5
eth2
vlan100
.254
vlan10:
10.123.0.254/16
vlan20:
10.123.20.254/24
eth1
tBvm1
10.123.20.1/16
tAvm2
10.123.0.2/16
tBvm2
10.123.20.2/16
100.0.12.0/30
100.0.32.0/30
PE3
lo: 2.255.0.1
lo: 1.255.0.1
lo: 1.255.0.3
q1/0
q2/0
q3/0
root@tAvm1:/# ping 10.123.0.2 -c 5
PING 10.123.0.2 (10.123.0.2) 56(84) bytes of data.
64 bytes from 10.123.0.2: icmp_seq=1 ttl=64 time=15.0 ms
64 bytes from 10.123.0.2: icmp_seq=2 ttl=64 time=13.7 ms
64 bytes from 10.123.0.2: icmp_seq=3 ttl=64 time=11.3 ms
64 bytes from 10.123.0.2: icmp_seq=4 ttl=64 time=12.1 ms
64 bytes from 10.123.0.2: icmp_seq=5 ttl=64 time=59.0 ms
--- 10.123.0.2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4845ms
rtt min/avg/max/mdev = 11.320/22.257/59.039/18.437 ms

```
cumulus@leaf1:mgmt:~$ net show evpn vni
VNI        Type VxLAN IF              # MACs   # ARPs   # Remote VTEPs  Tenant VRF
100        L2   vni100                2        3        0               TENA
200        L2   vni200                1        2        0               TENB
20         L2   vni20                 3        5        1               TENB
10         L2   vni10                 3        6        1               TENA
50         L3   vni50                 0        0        n/a             TENA
60         L3   vni60                 0        0        n/a             TENB
```

```
cumulus@leaf1:mgmt:~$ net show bridge vlan

Interface  VLAN  Flags                    VNI
---------  ----  -----------------------  ---
swp1         10  PVID, Egress Untagged
swp2         20  PVID, Egress Untagged
swp5        100  PVID, Egress Untagged
bridge       10
             20
             50
             60
            100
            200
vni10        10  PVID, Egress Untagged  10
vni20        20  PVID, Egress Untagged  20
vni50        50  PVID, Egress Untagged  50
vni60        60  PVID, Egress Untagged  60
vni100      100  PVID, Egress Untagged  100
vni200      200  PVID, Egress Untagged  200
```

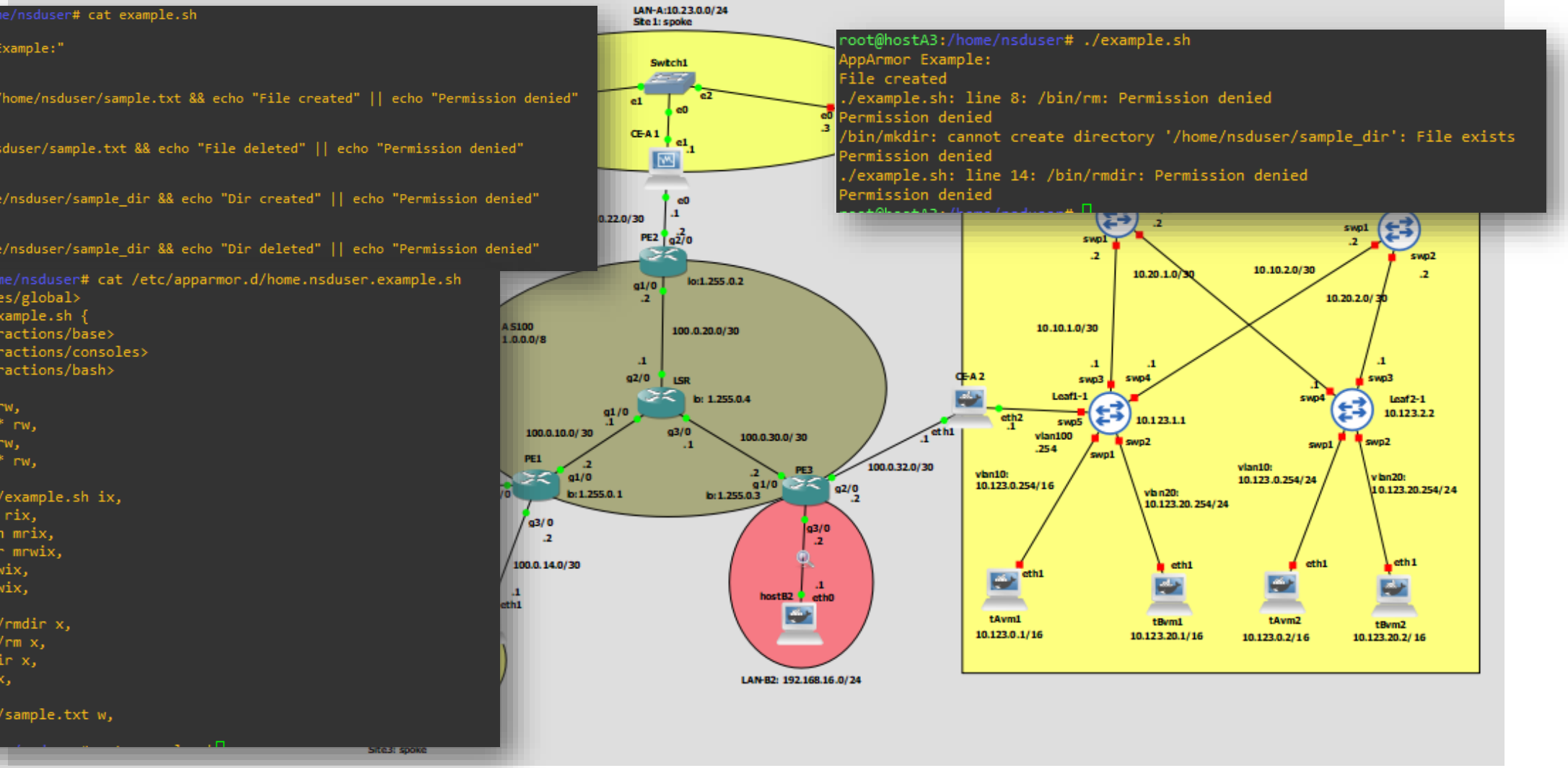


Apparmor

```
root@hostA3:/home/nsduser# cat example.sh
#!/bin/bash
echo "AppArmor Example:"

# Test touch
/usr/bin/touch /home/nsduser/sample.txt && echo "File created" || echo "Permission denied"

# Test rm
/bin/rm /home/nsduser/sample.txt && echo "File deleted" || echo "Permission denied"

# Test mkdir
/bin/mkdir /home/nsduser/sample_dir && echo "Dir created" || echo "Permission denied"

# Test rmdir
/bin/rmdir /home/nsduser/sample_dir && echo "Dir deleted" || echo "Permission denied"
```

```
root@hostA3:/home/nsduser# cat /etc/apparmor.d/home.nsduser.example.sh
include <tunables/global>
/home/nsduser/example.sh {
  include <abstractions/base>
  include <abstractions/consoles>
  include <abstractions/bash>

  owner /home/ rw,
  owner /home/** rw,
  owner /root/ rw,
  owner /root/** rw,

  /home/nsduser/example.sh ix,
  /usr/bin/bash rix,
  /usr/bin/touch mrix,
  /usr/bin/mkdir mrwix,
  /bin/touch mrwix,
  /bin/mkdir mrwix,

  deny /usr/bin/rmdir x,
  deny /usr/bin/rm x,
  deny /bin/rmdir x,
  deny /bin/rm x,

  owner /home/*/sample.txt w,
}
```

```
root@hostA3:/home/nsduser# ./example.sh
AppArmor Example:
File created
./example.sh: line 8: /bin/rm: Permission denied
Permission denied
/bin/mkdir: cannot create directory '/home/nsduser/sample_dir': File exists
Permission denied
./example.sh: line 14: /bin/rmdir: Permission denied
Permission denied
```



Grazie dell’attenzione!