ENTERPRISE NETWORK IMPLEMENTATION

ITQ TRAINING PROGRAM

CCNP ENCOR & DEVACS

FINAL PROJECT

IDAN NAVE

PROJECT INTRO

Intro | HW | Topology Design | Subnetting | Config. & Eval. | PVST & FHRP | ISP & BGP | Routing, VPN & NAT | Security | Automation | Summ.

TABLE OF CONTENTS

Overview of the Project

The following presentation is an effort to conclude the knowledge and skills acquired during the Network-Engineering Boot-Camp program, at ITQ College:

- Enterprise Network Specialty: Design & implementation of scalable campus networks, advanced routing & switching (OSPF, EIGRP, BGP), network security (firewalls, ACLs, VPNs).
- SDN Tools & Automation: Experience RESTFful APIs, Ansible, VMs, Linux.
- Hands-On Experience: 700 hours in network configuration, troubleshooting, and optimization.
- Cisco Certifications: CCNA, CCNP, DevNet.

Overview of the Development Env.

1. **GNS3** (Graphical Network Simulator 3)- simulation tool for designing, testing, and troubleshooting network topologies. **Emulates** routers, switches, firewalls.
2. **VirtualBox- Hosts** virtual machines for network and system simulations. Runs the IOS CSR Router VM for testing configurations and scripts.
3. IOS **CSR** Router VM- a virtualized IOS XE Router, Provides a realistic environment for network **testing** & validation.
4. **Python** & Bash Scripting- **Automates** network management and configuration tasks, interact with IOS CSR Router.
5. **Ansible-** Automation tool for configuration management and application deployment. Automates repetitive network tasks through '**playbooks**'.

Project Objectives

1. Design and implement an **enterprise** network model based on **Cisco** infrastructure.
2. Develop a **physical** (Campus, Branches) and **logical** (Hub&Spoke, VPN, VLANs) network topology.
3. Focus on creating a **robust** & **scalable** topology for three branches.
4. Ensure the network meets **security best practices** and **automation** requirements.
5. Address specific design considerations including **subnetting**, **hardening**, and **routing** protocols.

Project's Requirements

1. The network will include a total of **3 branches:** one **main** branch and two **secondary** branches.
2. Each branch will have a router. Main branch redundancy- 2 Routers for **HA** (High Availability)
3. Each router will connect to a Layer 3 switch that simulates **the Internet Service Provider.** Each router will be connected to a routed port on this switch.
4. **Main** branch will include 1 or 2 Access switches & 2 Distribution switches.
5. Each **Secondary** branch will have only **one Access switch** that connects directly to the router.
6. Each **Access** switch will be connected to **one PC.**

Scale Working Premise

- Each access switch in secondary branches should currently handle up to **48 devices** (and ~100 at main branch), but we will assume that this state represents close-to **maximum** capacity of connected Edge Nodes.
- Therefore, we will account **for 100% growth of edge-nodes** demand- by implementing **Tier-3 Campus** topology in the Main branch, and by reserving address space for inter-branch, when dealing with the **Subnetting** task.

HARDWARE

Historical Overview of Cisco Hardware

Early Years (1990s)

- **Series**: Cisco **2500** and **2600** Series
- **Use Cases**: Primarily used for small to **medium-sized** networks. Provided basic routing capabilities.
- **Technologies**: Introduced foundational networking protocols and technologies, including basic IP routing.

Growth and Expansion (2000s)

- **Series**: Cisco 2800, 2900, **3600**, and **3700** Series
- **Use Cases**: Suitable for **enterprise** and branch offices. Improved performance with more advanced routing and security features.
- **Technologies**: Enhanced support for **QoS** (Quality of Service), **VPNs**, and more robust security features **like integrated firewalls.**

Historical Overview of Cisco Hardware

Modernization (2010s)

Series: Cisco 3900, **4000** Series, and **Catalyst 9000** Series.
Use Cases: Designed for high-performance environments, including large enterprise networks and **data centers.**
Technologies: Introduced advanced capabilities such as integrated services, high **availability,** and support for software-defined networking (**SDN**).

Recent Developments (2020s)

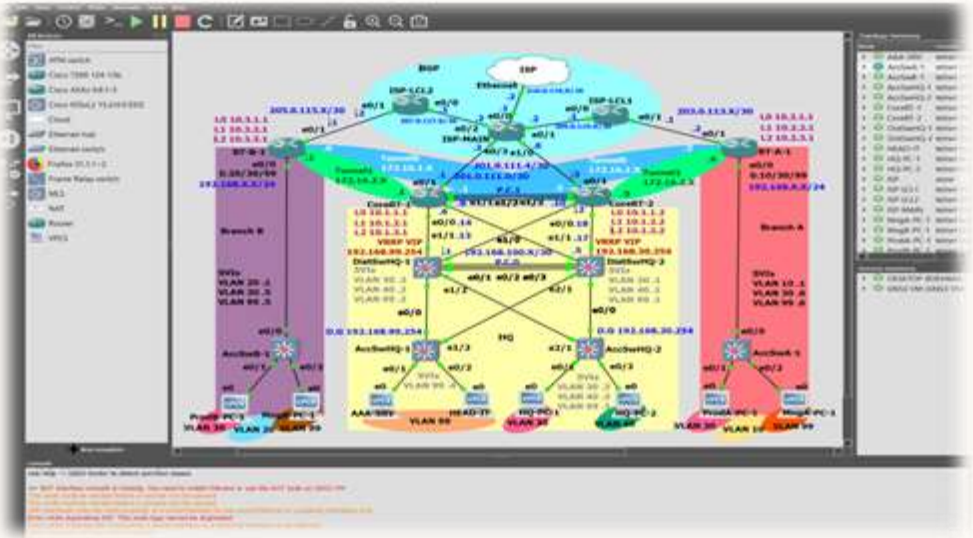
Series: Cisco **ASR 1000** Series, and Cisco **Nexus 9000** Series.
Use Cases: Cloud environments (**virtualized** routing capabilities), advanced security, and network programmability.
Technologies: Emphasizes **automation** and advanced **analytics.**

Conclusion - Hardware Selections

- **Routers** (Main & Sec. Branches): Cisco **ISR 4000** Series.
  High performance, modular design, supports **multiple WAN** interfaces, capable of handling high-throughput traffic.
  HA Capability- supports **HSRP** (Hot Standby Router Protocol) or **VRRP** (Virtual Router Redundancy Protocol).
- **Access Switches** (Main & Sec. Branches): Cisco **Catalyst 9300** Series.
  Up to **48 ports**, **PoE** (Power over Ethernet), up to **25 Gbps** Uplink.
- **Distribution Switches** (Sec. Branches): Cisco **Catalyst 9400** Series.
  High-performance, modular, up to **100 Gbps** Uplink.
- **All of which** support **SDN** capabilities through integration with **Cisco DNA**, **NETCONF/YANG**, and potentially OpenFlow.

Hardware Simulation with GNS3

Cisco Hardware | Hardware Selection | Emulation

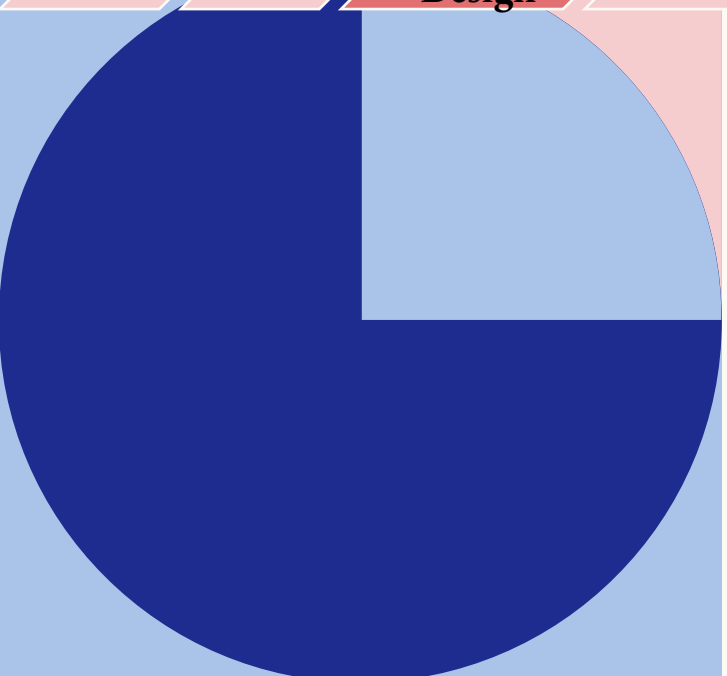


Overall, the topology consists of (Up-Down):

1. 4 Routers (2 Core, 2 Branch).
2. 6 MLSs (4 CAMPUS, 2 Branch).
3. 8 Edge PCs (Representing ~200 PCs across 5 VLANs).

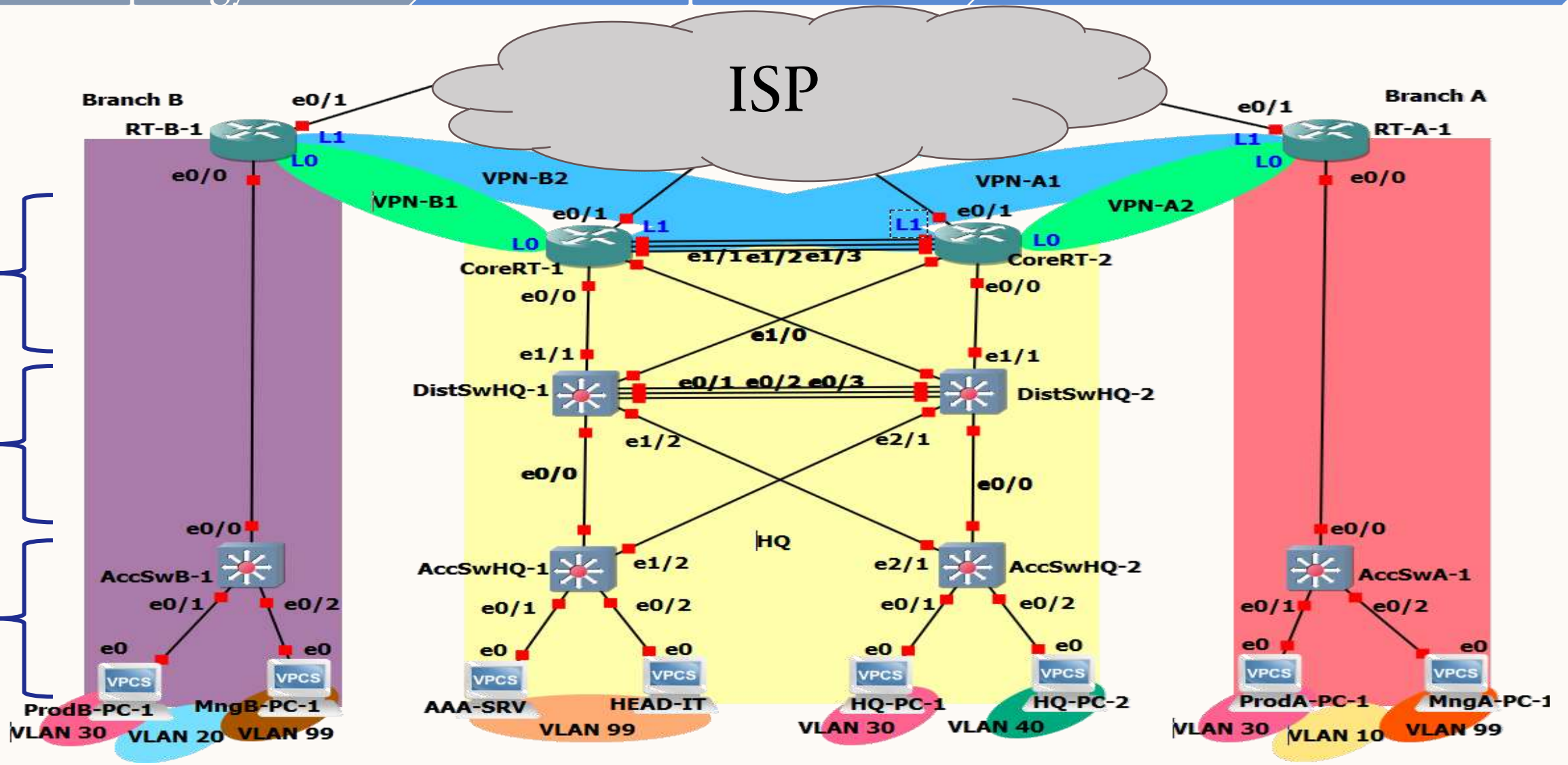
- The above will be replaced for **Cisco IOU** (IOS on UNIX) **modules** in GNS3 Emulator- which are **virtualized** versions of Cisco's IOS software.

TOPOLOGY DESIGN



Physical & Logical Topology

Topology | Enterprise-wise | Architecture-wise



Core Layer

Distrib. Layer

Access Layer

Enterprise-level Considerations

- **Hub & Spoke Topology** (Branch to Main Branch first)- all branches connect to the internet through a VPN tunnel meaning all **internet-bound traffic** is routed through the main branch, which can **handle security and monitoring.**
- **Main Branch to ISP**- The main branch connects to the ISP, which handles internet access for all branches. This represents the assumption that **a private leased WAN is not available** for the enterprise, thus internet access will be provided by the ISP by common means such as MPLS, broadband, etc.

Architecture-level Considerations

1. **ROAS** vs. Routed Port in **Secondary Branches**- simplifies VLAN management by centralizing routing on a single interface. This approach **reduces complexity** and the number of required routed interfaces.
2. **Layer 3 EtherChannel** Between Edge Routers- aggregates links to **increase intra-branch bandwidth** and provide redundancy. It also simplifies routing by treating the links as a single logical interface.
3. **Layer 2 EtherChannel** Between Distribution Switches- **enhances VLAN traffic** across multiple links & ensures stable connections within HQ branch.
4. **Loopback** Setup at VPN Edges- always-up IP address for **VPN endpoints**. This setup improves reliability and consistency in VPN connections.
5. **Full Mesh** Within the HQ- provides multiple redundant paths, improving network reliability & reduces latency by offering **direct connections** between network elements.
6. Implementing **VRRP** over FHRP within HQ- preferred for its **simplicity** and effective gateway redundancy. It ensures high availability with minimal configuration effort.

SUBNETTING

Subnetting Plan

To create a subnetting plan for our enterprise network with the given topology, we need to define subnets for each branch and VLAN, ensuring that IP addressing is both logical and scalable.

1 main branch with redundancy and **2 secondary** branches, 3 VLANs each:

- **VLAN 99:** Management- same across all branches.
- **VLAN 30:** Production- same across all branches.
- **VLAN X:** Unique to each branch (VLAN10, VLAN20, VLAN40).

Each VLAN will use **/24** subnet for simplification & growth (up to **254** hosts).

Address Allocation Table

192.168.0.0/**16** (255.255.0.0) provides:

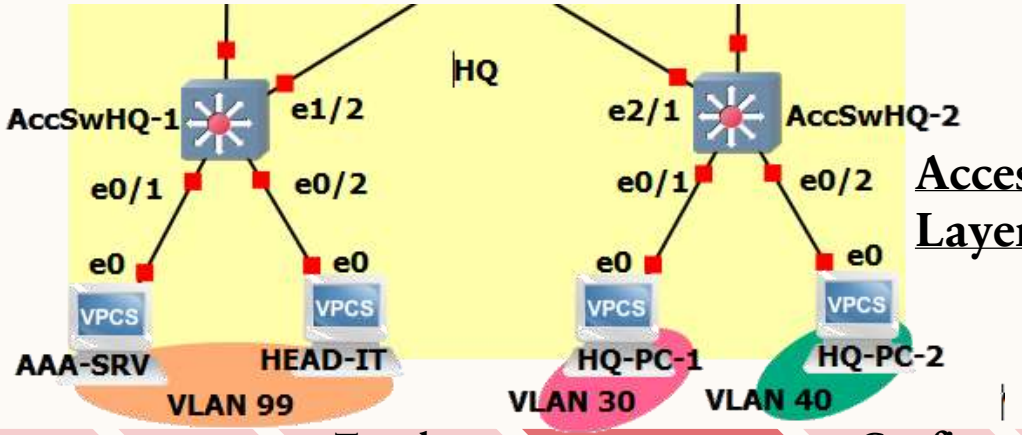
Branch	VLAN	Subnet	IP Range	Subnet Mask
Main Branch- HQ	99	192.168.99.0/24	192.168.99.1 - 192.168.99.254	255.255.255.0
	30	192.168.30.0/24	192.168.30.1 - 192.168.30.254	255.255.255.0
	40	192.168.40.0/24	192.168.40.1 - 192.168.40.254	255.255.255.0
Secondary Branch A	99	192.168.99.0/24	192.168.99.1 - 192.168.99.254	255.255.255.0
	30	192.168.30.0/24	192.168.30.1 - 192.168.30.254	255.255.255.0
	10	192.168.10.0/24	192.168.10.1 - 192.168.10.254	255.255.255.0
Secondary Branch B	99	192.168.99.0/24	192.168.99.1 - 192.168.99.254	255.255.255.0
	30	192.168.30.0/24	192.168.30.1 - 192.168.30.254	255.255.255.0
	20	192.168.20.0/24	192.168.20.1 - 192.168.20.254	255.255.255.0

Address Allocation Tasks

1. **Main Branch** handles BGP with ISP, VPN connections with Loopback IFs, VRRP, NAT for internal IPv4 addresses, and routes IPv6 to/from the internet.
2. **Secondary** Branches Connect to the main branch via VPN, with enterprise-level connectivity provided through OSPF.
3. **Dist. Switches** handles inter-VLAN routing in HQ.
4. **Access Switches** handles **VLANs** and **trunking** for internal segregation.
5. **PCs** to be configured with **default gateways**, and later with IPv4 addresses automatically **DHCP** services provided by the Gateway Router.

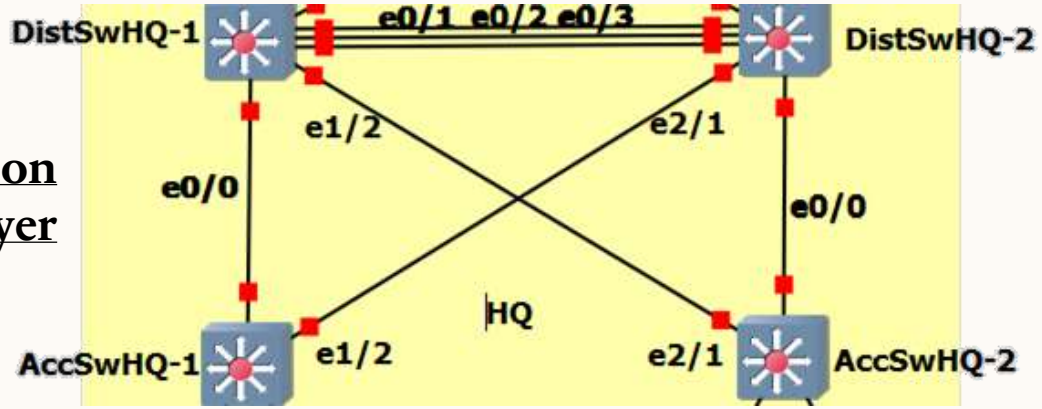
HQ SVI Addressing Table

Device	Interface	Heading	IP Address	S. Mask	Description
DistSwHQ-1	VLAN 99 (SVI)	Inside	192.168.99.1	255.255.255.0	Management VLAN Interface
	VLAN 30 (SVI)	Inside	192.168.30.1	255.255.255.0	Production VLAN Interface
	VLAN 40 (SVI)	Inside	192.168.40.1	255.255.255.0	Local VLAN Interface (AccSwHQ-2)
DistSwHQ-2	VLAN 99 (SVI)	Inside	192.168.99.2	255.255.255.0	Management VLAN Interface
	VLAN 30 (SVI)	Inside	192.168.30.2	255.255.255.0	Production VLAN Interface
	VLAN 40 (SVI)	Inside	192.168.40.2	255.255.255.0	Local VLAN Interface (AccSwHQ-1)
AccSwHQ-1	VLAN 99	Inside	192.168.99.3	255.255.255.0	Management VLAN Interface
AccSwHQ-2	VLAN 99	Inside	192.168.99.4	255.255.255.0	Management VLAN Interface
	VLAN 30	Inside	192.168.30.4	255.255.255.0	Production VLAN Interface
	VLAN 40	Inside	192.168.40.4	255.255.255.0	Local VLAN Interface



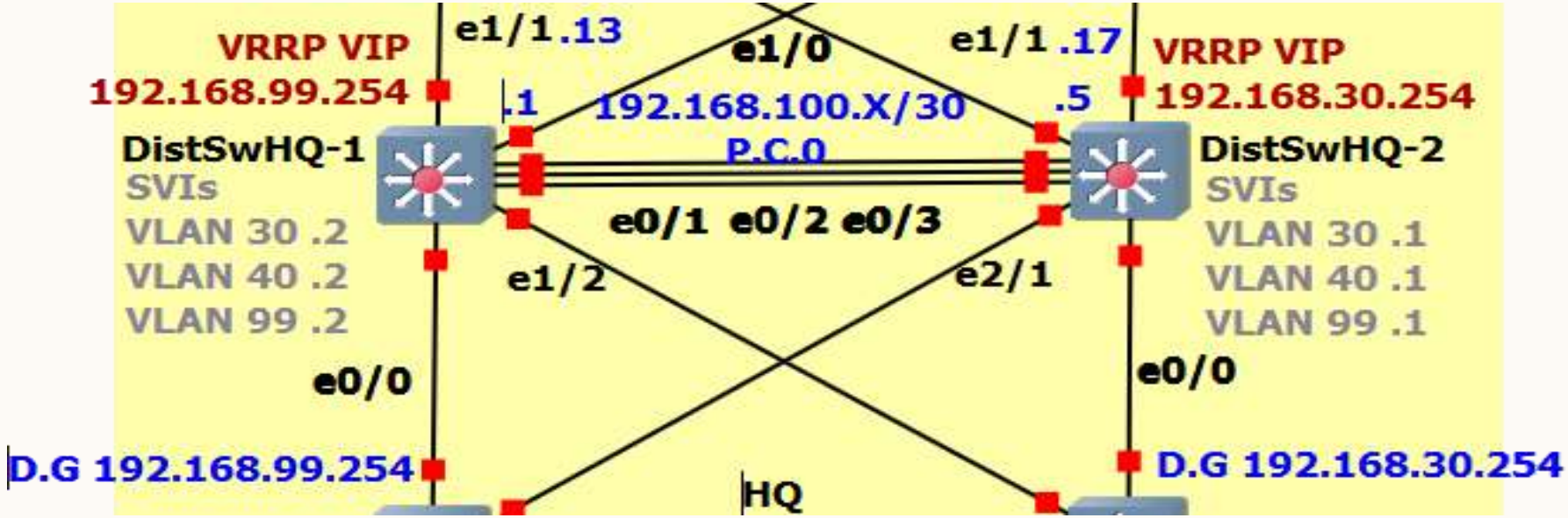
Access Layer

Distribution Layer



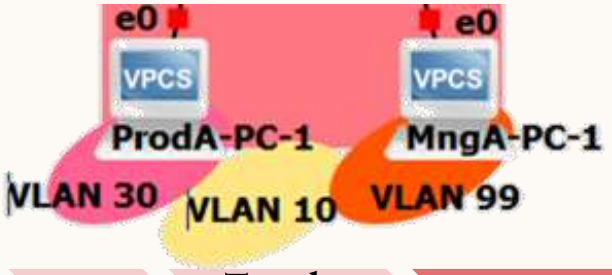
HQ Distribution Layer Addressing Table

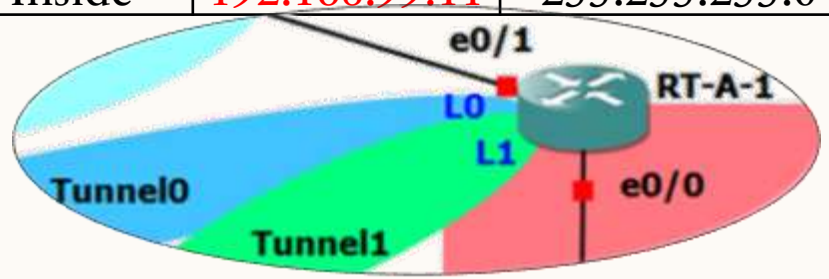
Device	Interface	Heading	IP Address	S. Mask	Description
DistSwHQ-1	GigabitEthernet1/1	Outside	192.168.100. 13	255.255.255.252	Internal Downlink
	GigabitEthernet1/0	Outside	192.168.100.1	255.255.255.252	Internal Downlink
	GigabitEthernet0/1-3	Both	-	-	L2 Ether Channel
DistSwHQ-2	GigabitEthernet1/1	Outside	192.168.100.17	255.255.255.252	Internal Downlink
	GigabitEthernet1/0	Outside	192.168.100.5	255.255.255.252	Internal Downlink
	GigabitEthernet0/1-3	Both	-	-	L2 Ether Channel

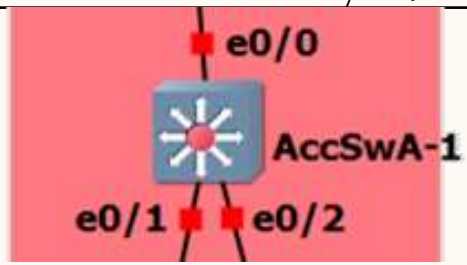


Branch A IP Addressing Table

Device	Interface	Heading	IP Address	S. Mask	Description
RT-A-1	GigabitEthernet0/0	Inside	**ROAS**	255.255.255.0	Internal network interface
	GigabitEthernet0/0.10	Outside	192.168.10.254	255.255.255.0	Subinterface
	GigabitEthernet0/0.30	Inside	192.168.30.1	255.255.255.0	Subinterface
	GigabitEthernet0/0.99	Outside	192.168.99.1	255.255.255.0	Subinterface
	Loopback0	Overlay	10.2.1.1	255.255.255.255	VPN Tunnel Endpoint for CoreRT-1
	Loopback1	Overlay	10.2.2.1	255.255.255.255	VPN Tunnel Endpoint for CoreRT-2
	Tunnel0	Overlay	172.16.1.2	255.255.255.252	VPN Tunnel to CoreRT-1
	Tunnel1	Overlay	172.16.2.6	255.255.255.252	VPN Tunnel to CoreRT-2
AccSwA-1	VLAN 99	Inside	192.168.99.6	255.255.255.0	Management VLAN Interface
	VLAN 30	Inside	192.168.**30**.6	255.255.255.0	Production VLAN Interface
	VLAN 10	Inside	192.168.**10**.1	255.255.255.0	Local VLAN Interface
ProdA-PC-1	GigabitEthernet0/0	Inside	192.168.30.11	255.255.255.0	Default Gateway: 192.168.30.1
MngA-PC-1	GigabitEthernet0/0	Inside	192.168.99.11	255.255.255.0	Default Gateway: 192.168.99.1

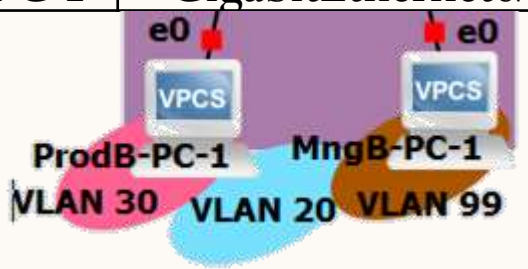


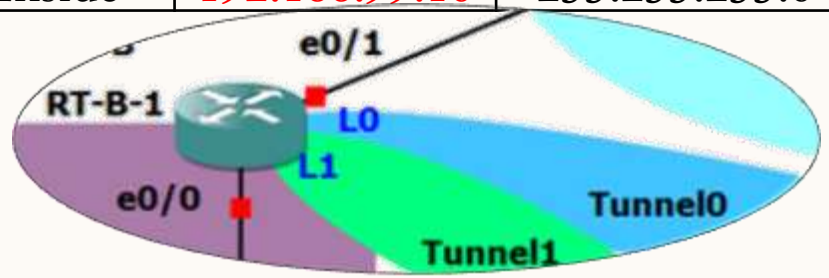


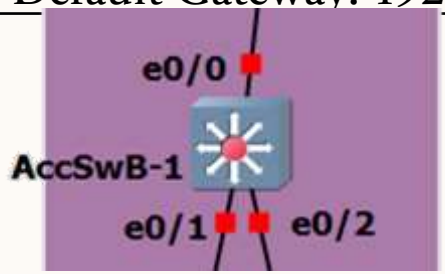


Branch B IP Addressing Table

Device	Interface	Heading	IP Address	S. Mask	Description
RT-B-1	GigabitEthernet0/0	Inside	**ROAS**	255.255.255.0	Internal network interface
	GigabitEthernet0/0.20	Outside	192.168.20. 254	255.255.255.0	Subinterface
	GigabitEthernet0/0.30	Inside	192.168.30.1	255.255.255.0	Subinterface
	GigabitEthernet0/0.99	Outside	192.168.99.1	255.255.255.0	Subinterface
	Loopback0	Overlay	10.3.1.1	255.255.255.255	VPN Tunnel Endpoint for CoreRT-2
	Loopback1	Overlay	10.3.2.1	255.255.255.255	VPN Tunnel Endpoint for CoreRT-1
	Tunnel0	Overlay	172.16.1.6	255.255.255.252	VPN Tunnel to CoreRT-2
	Tunnel1	Overlay	172.16.2.2	255.255.255.252	VPN Tunnel to CoreRT-1
AccSwB-1	VLAN 99	Inside	192.168.99.5	255.255.255.0	Management VLAN Interface
	VLAN 30	Inside	192.168.**30**.5	255.255.255.0	Production VLAN Interface
	VLAN 20	Inside	192.168.**20**.1	255.255.255.0	Local VLAN Interface
ProdB-PC-1	GigabitEthernet0/0	Inside	192.168.30.10	255.255.255.0	Default Gateway: 192.168.30.1
MngB-PC-1	GigabitEthernet0/0	Inside	192.168.99.10	255.255.255.0	Default Gateway: 192.168.99.1

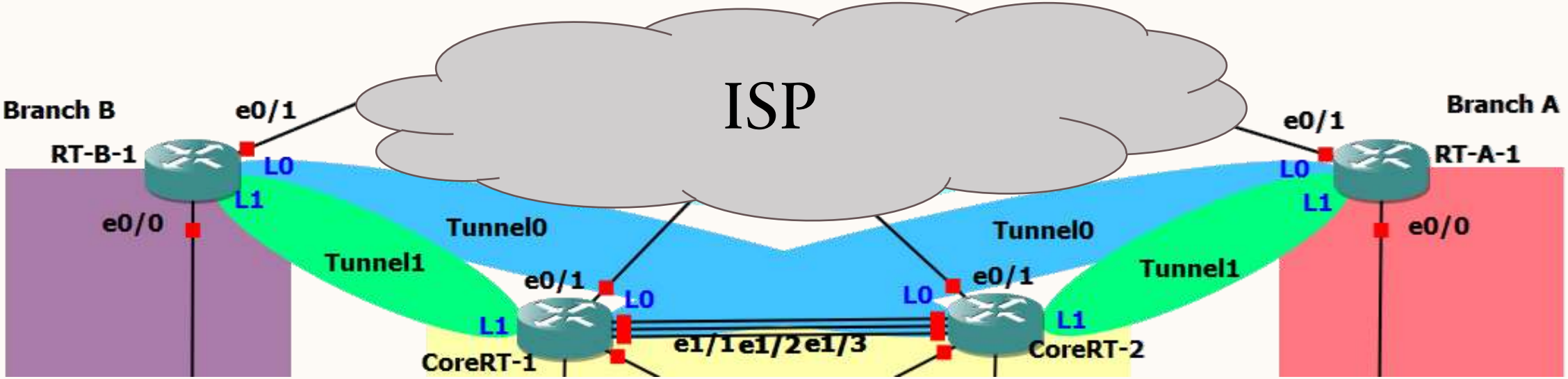






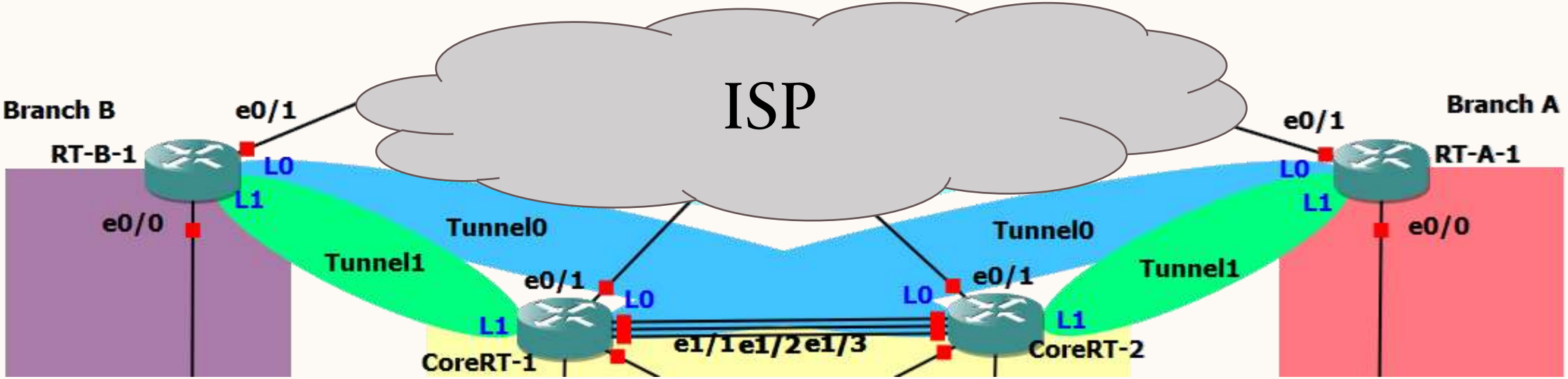
HQ Underlay Addressing Table

Device	Interface	Heading	IP Address	S. Mask	Description
CoreRT-1	GigabitEthernet0/1	Outside	201.0.111.0	255.255.255.252	Connection to ISP
	GigabitEthernet0/0	Inside	192.168.100.14	255.255.255.252	Internal Downlink
	GigabitEthernet1/0	Inside	192.168.100.6	255.255.255.252	Internal Downlink
	GigabitEthernet1/1-3	Both	192.168.100.9	255.255.255.252	L3 Ether Channel
CoreRT-2	GigabitEthernet0/1	Outside	201.0.111.4	255.255.255.252	Connection to ISP
	GigabitEthernet0/0	Inside	192.168.100.18	255.255.255.252	Internal Downlink
	GigabitEthernet1/0	Inside	192.168.100.2	255.255.255.252	Internal Downlink
	GigabitEthernet1/1-3	Both	192.168.100.10	255.255.255.252	L3 Ether Channel

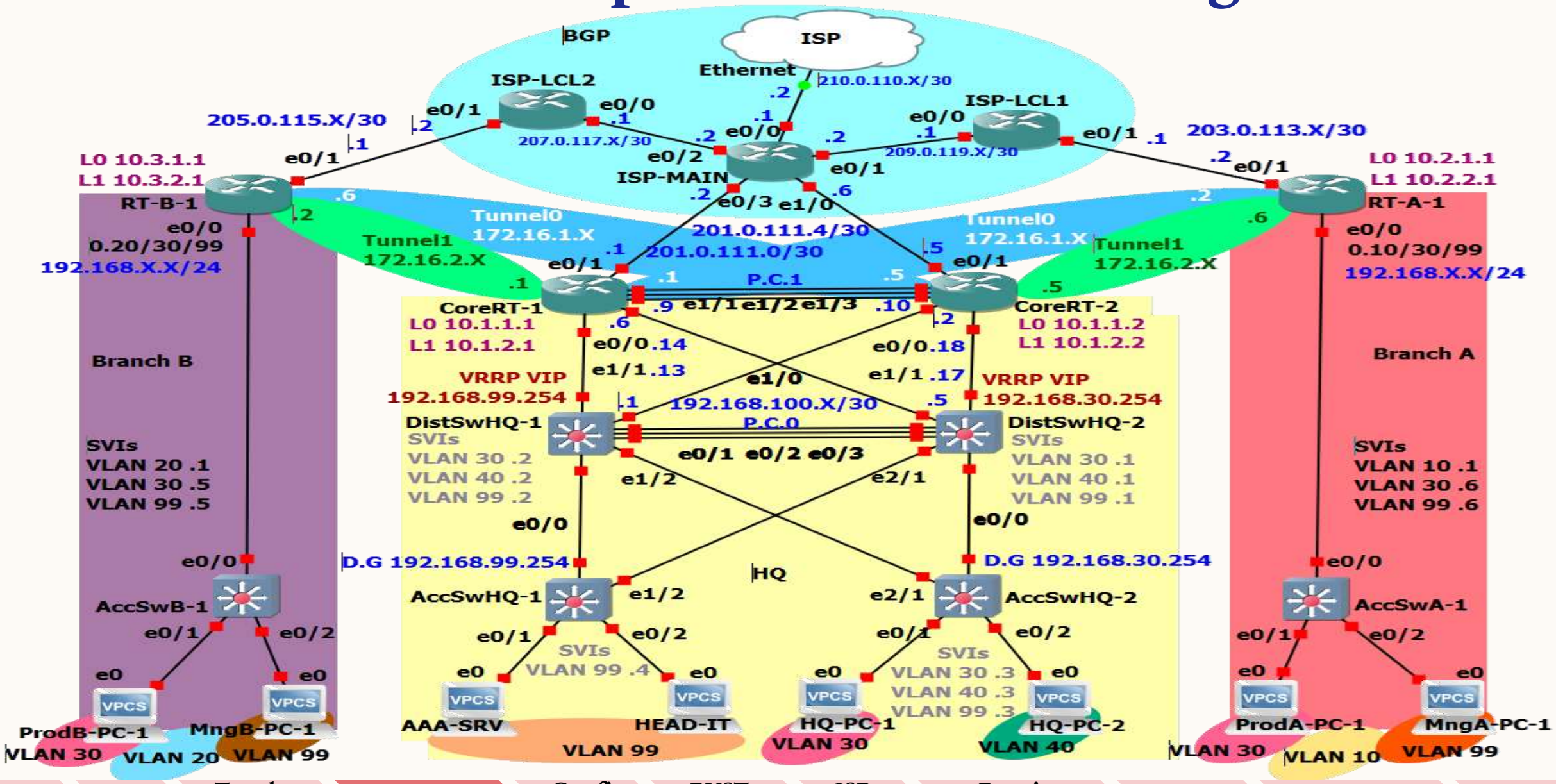


HQ Overlay Addressing Table

Device	Interface	Heading	IP Address	S. Mask	Description
CoreRT-1	Loopback0	Overlay	10.1.1.1	255.255.255.255	VPN Endpoint for RT-A-1
	Loopback1	Overlay	10.1.2.1	255.255.255.255	VPN Endpoint for RT-B-1
	Tunnel0	Overlay	172.16.1.1	255.255.255.252	VPN Tunnel to RT-A-1
	Tunnel1	Overlay	172.16.2.1	255.255.255.252	VPN Tunnel to RT-B-1
CoreRT-2	Loopback0	Overlay	10.1.1.2	255.255.255.255	VPN Endpoint for RT-B-1
	Loopback1	Overlay	10.1.2.2	255.255.255.255	VPN Endpoint for RT-A-1
	Tunnel0	Overlay	172.16.1.5	255.255.255.252	VPN Tunnel to RT-B-1
	Tunnel1	Overlay	172.16.2.5	255.255.255.252	VPN Tunnel to RT-A-1



Full Enterprise / ISP Subnetting



CONFIGURATION & EVALUATION

Configuration- SVIs

Branch Access SWs

```
! AccSwA-1
interface Vlan30
 ip address 192.168.30.6 255.255.255.0
 no shutdown
interface Vlan10
 ip address 192.168.10.1 255.255.255.0
 no shutdown
interface Vlan99
 ip address 192.168.99.6 255.255.255.0
 no shutdown
! AccSwB-1
interface Vlan30
 ip address 192.168.30.5 255.255.255.0
 no shutdown
interface Vlan20
 ip address 192.168.20.1 255.255.255.0
 no shutdown
interface Vlan99
 ip address 192.168.99.5 255.255.255.0
 no shutdown
```

HQ Access SWs

```
! AccSwHQ-1
interface Vlan30
 ip address 192.168.30.3 255.255.255.0
 no shutdown
interface Vlan40
 ip address 192.168.40.3 255.255.255.0
 no shutdown
interface Vlan99
 ip address 192.168.99.3 255.255.255.0
 no shutdown
! AccSwHQ-2
interface Vlan30
 ip address 192.168.30.4 255.255.255.0
 no shutdown
interface Vlan40
 ip address 192.168.40.4 255.255.255.0
 no shutdown
interface Vlan99
 ip address 192.168.99.4 255.255.255.0
 no shutdown
```

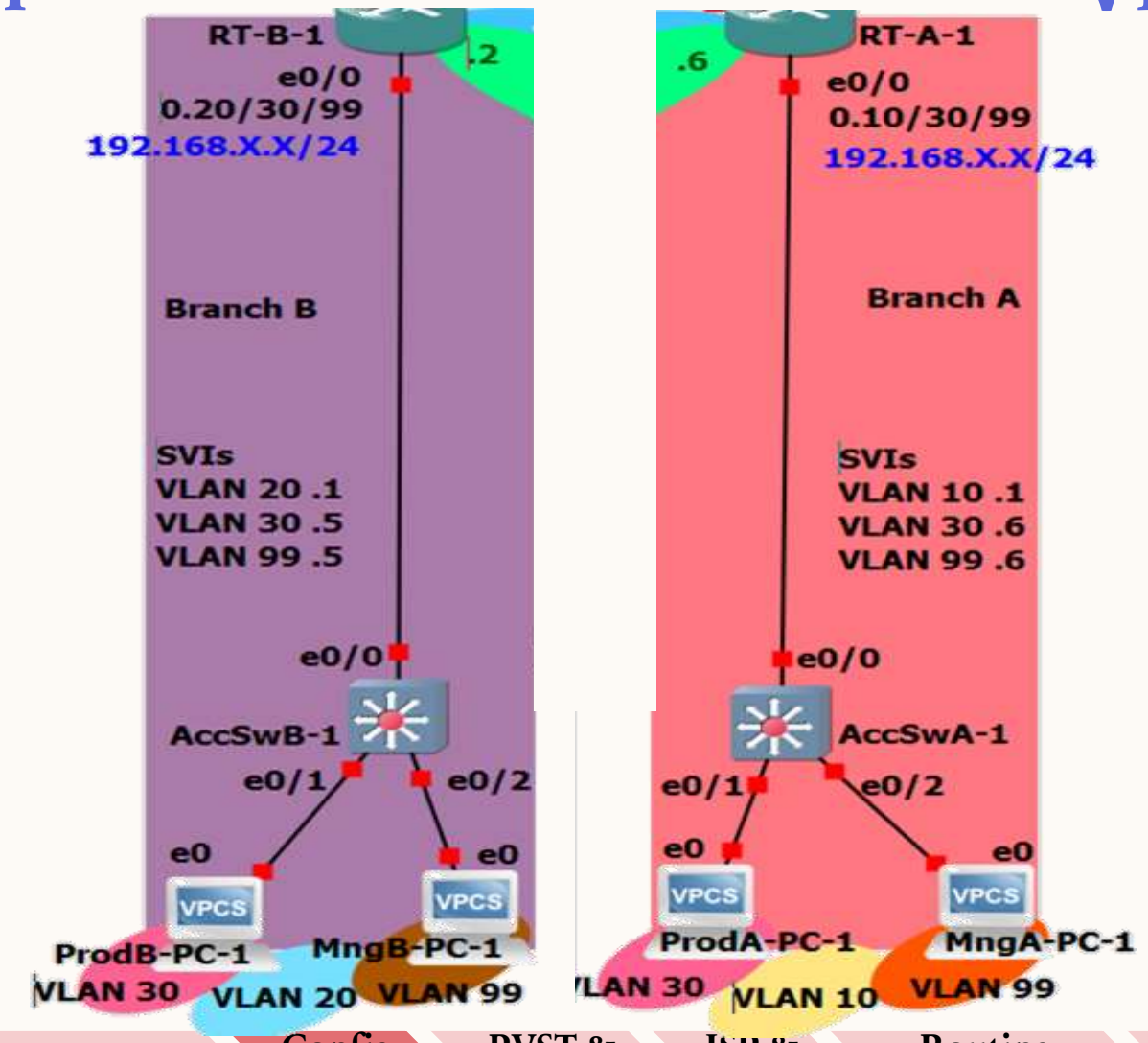
Dist. SWs

```
! DistSwHQ-1
interface Vlan30
 ip address 192.168.30.1 255.255.255.0
 no shutdown
interface Vlan40
 ip address 192.168.40.1 255.255.255.0
 no shutdown
interface Vlan99
 ip address 192.168.99.1 255.255.255.0
 no shutdown
! DistSwHQ-2
interface Vlan30
 ip address 192.168.30.2 255.255.255.0
 no shutdown
interface Vlan40
 ip address 192.168.40.2 255.255.255.0
 no shutdown
interface Vlan99
 ip address 192.168.99.2 255.255.255.0
 no shutdown
```

Configuration- VLAN assignment

VLANs creation

```
vlan 10
 name VLAN10-BranchA

vlan 20
 name VLAN20-BranchB

vlan 30
 name VLAN30-Production

vlan 40
 name VLAN40-Guest

vlan 99
 name VLAN99-Management

! Example static ip for tests
Ip 192.168.30.200 /24
192.168.99.1
```



VLANs assignment

```
! AccSwA-1
Interface E0/1
 switchport access vlan 30
Interface E0/2
 switchport access vlan 99
! AccSwB-1
Interface E0/1
 switchport access vlan 30
Interface E0/2
 switchport access vlan 99
! AccSwHQ-1
ip default-gateway 192.168.99.254
Interface range E0/1-2
 switchport access vlan 99
! AccSwHQ-2
ip default-gateway 192.168.30.254
Interface E0/1
 switchport access vlan 30
Interface E0/2
 switchport access vlan 40
```

Validation - VLANs

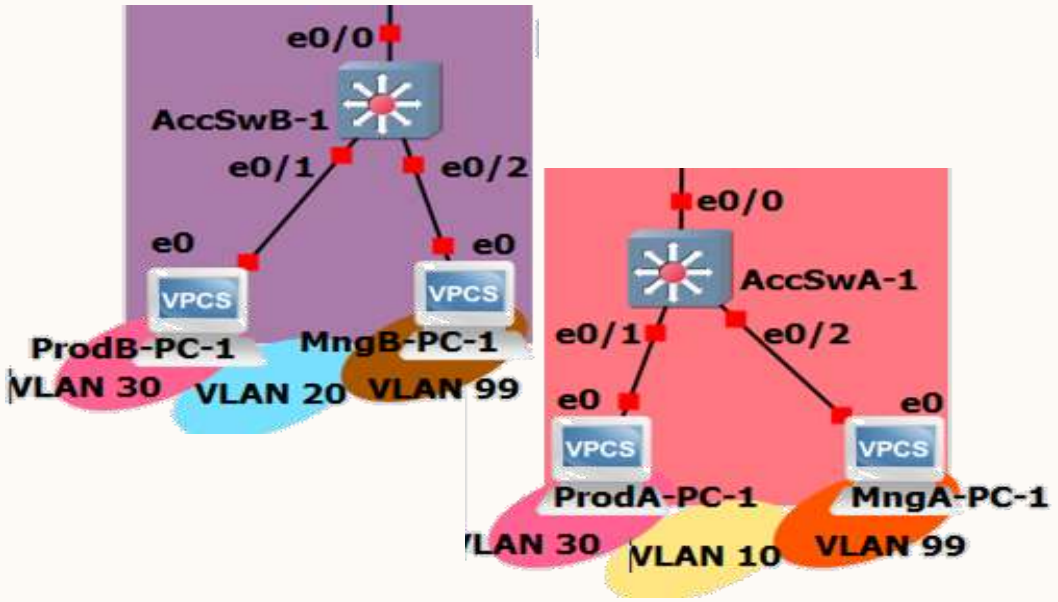

```
AccSwHQ-1#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Et0/0, Et0/3, Et1/0, Et1/1
                                                Et1/2, Et1/3, Et2/0, Et2/1
                                                Et2/2, Et2/3, Et3/0, Et3/1
                                                Et3/2, Et3/3
10   VLAN10-BranchA                   active
20   VLAN20-BranchB                   active
30   VLAN30-Production                active
40   VLAN40-Guest                     active
99   VLAN99-Management                active    Et0/1, Et0/2
```

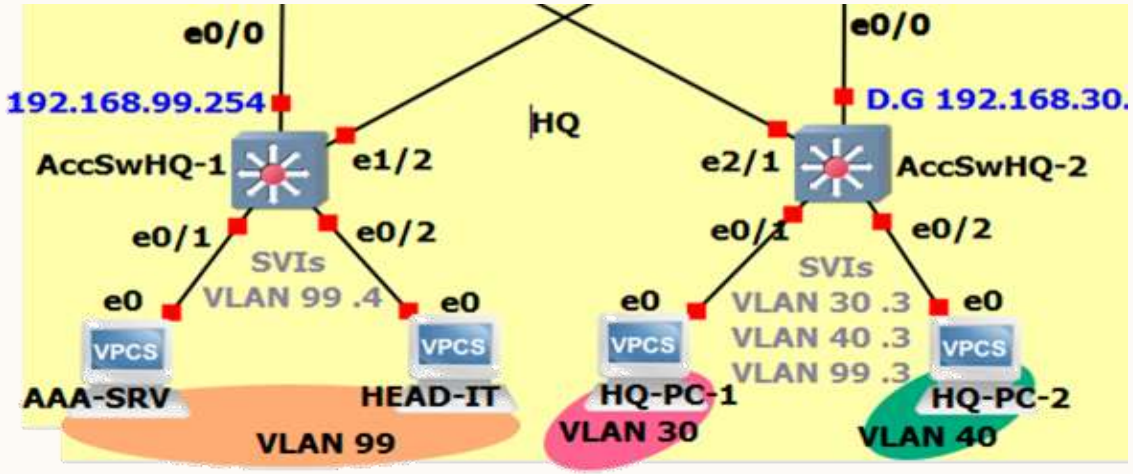
```
AccSwHQ-2#show int status

Port      Name               Status       Vlan       Duplex  Speed Type
Et0/0                        disabled     1            auto   auto RJ45
Et0/1                        disabled     30           auto   auto RJ45
Et0/2                        disabled     40           auto   auto RJ45
Et0/3                        disabled     1            auto   auto RJ45
```

Configuration- Access Layer

Branch Access SWs

```
! AccSwA-1
Interface range E0/1-2
 description Connection to PCs
 no shutdown
Interface E0/0
 description Uplink
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport trunk allowed vlan 30,10,99
 no shutdown
! AccSwB-1
Interface range E0/1-2
 description Connection to PCs
 no shutdown
Interface E0/0
 description Uplink
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport trunk allowed vlan 30,20,99
 no shutdown
```





HQ Access SWs

```
! AccSwHQ-1
Interface range E0/1-2
 description Connection to PCs
 no shutdown
Interface range E0/0, E1/2
 description Connection to Dist. SWs
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport trunk allowed vlan 99
 no shutdown
! AccSwHQ-2
Interface range E0/1-2
 description Connection to PCs
 no shutdown
Interface range E0/0, E2/1
 description Connection to Dist. SWs
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport trunk allowed vlan 30,40,99
 no shutdown
```

Validation - Access Layer


```
AccSwHQ-1#show int trunk

Port        Mode             Encapsulation  Status        Native vlan
Et0/0       on               802.1q         trunking      1
Et1/2       on               802.1q         trunking      1

Port        Vlans allowed on trunk
Et0/0       99
Et1/2       99
```

```
AccSwHQ-1#show int status

Port      Name               Status       Vlan       Duplex  Speed Type
Et0/0     Connection to Dist connected    trunk      a-full    auto RJ45
Et0/1     Connection to PCs  connected    99         a-full    auto RJ45
Et0/2     Connection to PCs  connected    99         a-full    auto RJ45
Et0/3                        disabled     1            auto    auto RJ45
Et1/0                        disabled     1            auto    auto RJ45
Et1/1                        disabled     1            auto    auto RJ45
Et1/2     Connection to Dist connected    trunk      a-full    auto RJ45
```

```
AccSwA-1#show int status

Port      Name               Status       Vlan       Duplex  Speed Type
Et0/0     Uplink             connected    trunk      a-full    auto RJ45
Et0/1     Connection to PCs  connected    30         a-full    auto RJ45
Et0/2     Connection to PCs  connected    99         a-full    auto RJ45
```

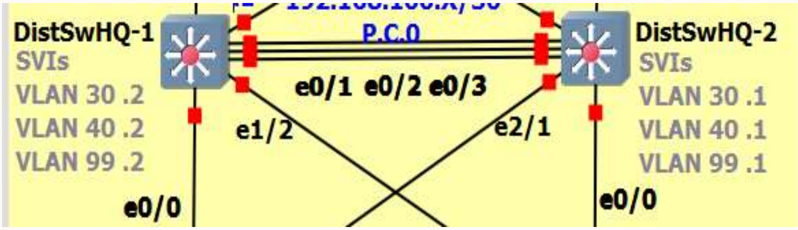
```
AccSwA-1#show interfaces switchport
Name: Et0/0
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
```

Configuration- Distribution Mesh

SVIs | VLANs | Access Layer | Distribution Layer | Core Layer

Access Links

```
! DistSwHQ-1
Interface range E0/0, E1/2
 description to Access SWs
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport trunk allowed vlan 30,40,99
 no shutdown

! DistSwHQ-2
Interface range E0/0, E2/1
 description to Access SWs
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport trunk allowed vlan 30,40,99
 no shutdown
```



Routed Uplinks

```
! DistSwHQ-1
Ip routing
interface range E1/0-1
 description Uplinks
 no switchport
 no shutdown
interface E1/0
 ip address 192.168.100.1 255.255.255.252
interface E1/1
 description VRRP 99 Subnet
 ip address 192.168.100.13 255.255.255.252
! DistSwHQ-2
Ip routing
interface range E1/0-1
 description Uplinks
 no switchport
 no shutdown
interface E1/0
 ip address 192.168.100.5 255.255.255.252
interface E1/1
 description VRRP 30 Subnet
 ip address 192.168.100.17 255.255.255.252
```

L2 Ether Channel

```
! DistSwHQ-1
interface range E0/1-3
 no shutdown
 description to DistSwHQ-2
 switchport
 channel-group 1 mode active
interface Port-channel1
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport trunk allowed vlan 30,40,99
 no shutdown
! DistSwHQ-2
interface range E0/1-3
 no shutdown
 description to DistSwHQ-1
 switchport
 channel-group 1 mode active
interface Port-channel1
switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport trunk allowed vlan 30,40,99
 no shutdown
```

Validation - Distribution Layer


```
DistSwHQ-1#show etherchannel summary | section 1
Number of channel-groups in use: 1
Number of aggregators:           1
1      Po1(SU)         LACP      Et0/1(P)    Et0/2(P)    Et0/3(P)
```

```
DistSwHQ-2#show etherchannel summary | section 1
Number of channel-groups in use: 1
Number of aggregators:           1
1      Po1(SU)         LACP      Et0/1(P)    Et0/2(P)    Et0/3(P)
```

```
DistSwHQ-2#show interfaces trunk

Port        Mode             Encapsulation  Status        Native vlan
Et0/0       on               802.1q         trunking      1
Et2/1       on               802.1q         trunking      1
Po1         on               802.1q         trunking      1
```

```
DistSwHQ-2#show ip int brief | include up
Ethernet0/0                unassigned      YES unset  up
Ethernet0/1                unassigned      YES unset  up
Ethernet0/2                unassigned      YES unset  up
Ethernet0/3                unassigned      YES unset  up
Ethernet1/0                192.168.100.5   YES manual up
Ethernet1/1                192.168.100.17  YES manual up
Ethernet2/1                unassigned      YES unset  up
Port-channel1      (L2)    unassigned      YES unset  up
Vlan30                     192.168.30.2    YES manual up
Vlan40                     192.168.40.2    YES manual up
Vlan99                     192.168.99.2    YES manual up
```

```
DistSwHQ-2#show interfaces status | include connected
Et0/0      Connection to Acce connected    trunk      a-full   auto RJ45
Et0/1      to DistSwHQ-1      connected    trunk      a-full   auto RJ45
Et0/2      to DistSwHQ-1      connected    trunk      a-full   auto RJ45
Et0/3      to DistSwHQ-1      connected    trunk      a-full   auto RJ45
Et1/0      Uplinks            connected    routed     a-full   auto RJ45
Et1/1      Uplinks            connected    routed     a-full   auto RJ45
Et2/1      Connection to Acce connected    trunk      a-full   auto RJ45
Po1                           connected    trunk      a-full   auto
```

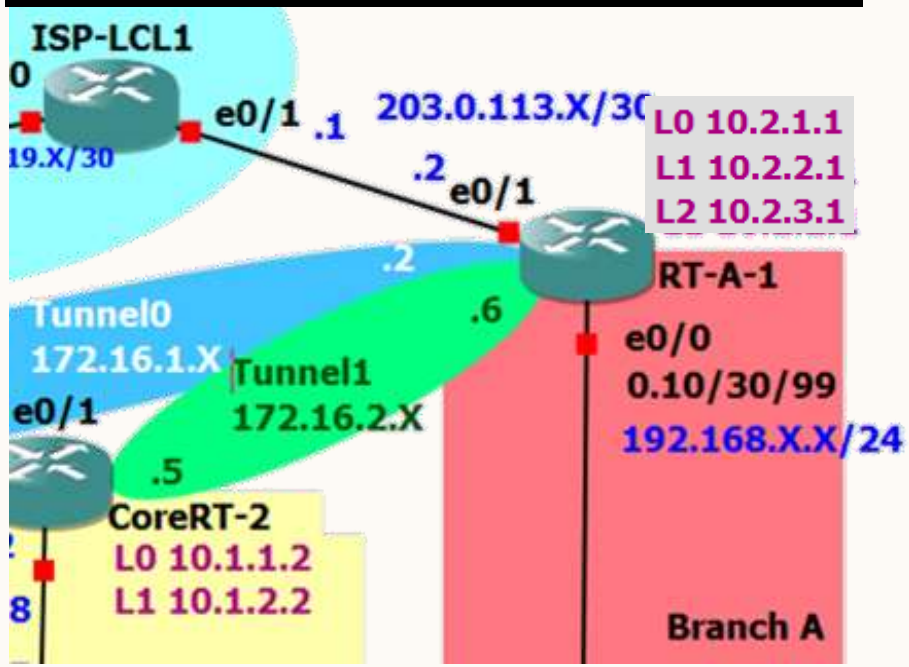
Configuration- Branch A L3 Setup

ROAS

```
interface E0/0
 description Downlink
 no shutdown

interface E0/0.10
 encapsulation dot1Q 10
 ip address 192.168.10.254 255.255.255.0

interface E0/0.30
 encapsulation dot1Q 30
 ip address 192.168.30.1 255.255.255.0

interface E0/0.99
 encapsulation dot1Q 99
 ip address 192.168.99.1 255.255.255.0
```

Underlay (to ISP)

```
interface E0/1
 description Uplink to ISP
 ip address 203.0.113.2 255.255.255.252
 no shutdown

interface Loopback2
 ip address 10.2.3.1 255.255.255.255
 no shutdown
```



Overlay (VPN)

```
interface Loopback0
 ip address 10.2.1.1 255.255.255.255
 no shutdown

interface Loopback1
 ip address 10.2.2.1 255.255.255.255
 no shutdown

interface Tunnel0
 description Link to CoreRT-1, E0/1
 ip address 172.16.1.2 255.255.255.252
 tunnel source E0/1
 tunnel destination 201.0.111.1
 no shutdown

interface Tunnel1
 description Link to CoreRT-2, E0/1
 ip address 172.16.2.6 255.255.255.252
 tunnel source E0/1
 tunnel destination 201.0.111.5
 no shutdown
```

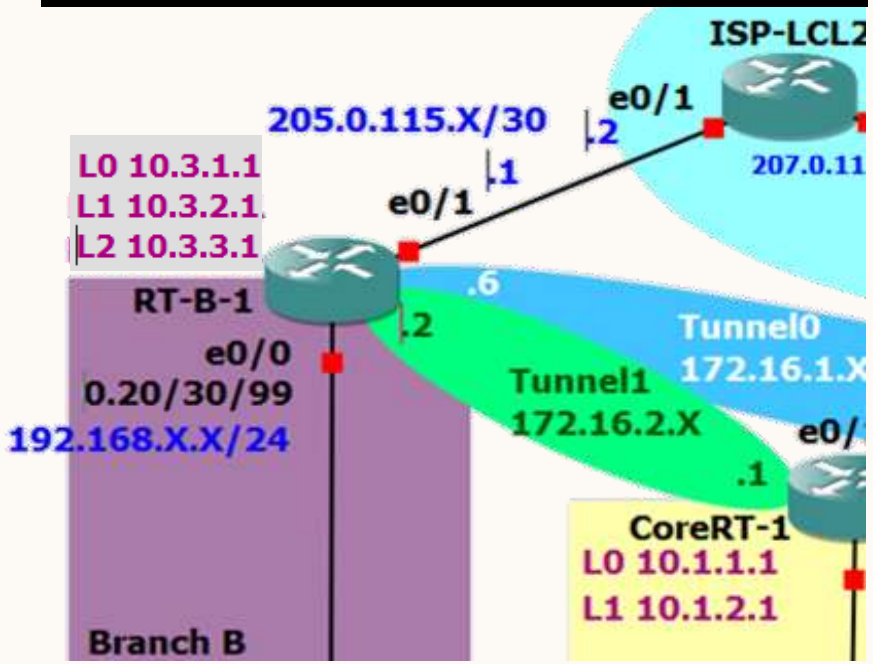
Configuration- Branch B L3 Setup

ROAS

```
interface E0/0
 description Downlink
 no shutdown

interface E0/0.20
 encapsulation dot1Q 20
 ip address 192.168.20.254 255.255.255.0

interface E0/0.30
 encapsulation dot1Q 30
 ip address 192.168.30.1 255.255.255.0

interface E0/0.99
 encapsulation dot1Q 99
 ip address 192.168.99.1 255.255.255.0
```

Underlay (to ISP)

```
interface E0/1
 description Uplink to ISP
 ip address 205.0.115.1 255.255.255.252
 no shutdown

interface Loopback2
 ip address 10.3.3.1 255.255.255.255
 no shutdown
```



Overlay (VPN)

```
interface Loopback0
 ip address 10.3.1.1 255.255.255.255
 no shutdown

interface Loopback1
 ip address 10.3.2.1 255.255.255.255
 no shutdown

interface Tunnel0
 description Link to CoreRT-2, E0/1
 ip address 172.16.1.6 255.255.255.252
 tunnel source E0/1
 tunnel destination 201.0.111.5
 no shutdown

interface Tunnel1
 description Link to CoreRT-1, E0/1
 ip address 172.16.2.2 255.255.255.252
 tunnel source E0/1
 tunnel destination 201.0.111.1
 no shutdown
```

Validation – Sec. Branch ROAS & VPN Endpoints


```
RT-A-1#show ip int bri | include manual
Ethernet0/0.10             192.168.10.254  YES manual up
Ethernet0/0.30             192.168.30.1    YES manual up
Ethernet0/0.99             192.168.99.1    YES manual up
Ethernet0/1                203.0.113.2     YES manual up
Loopback0                  10.2.1.1        YES manual up
Loopback1                  10.2.2.1        YES manual up
Tunnel0                    172.16.1.2      YES manual up
Tunnel1                    172.16.2.6      YES manual up
```

```
RT-A-1#show ip route | include ^C
Codes: L - local, C - connected, S - static, R - RIP, M - mobi
C        10.2.1.1 is directly connected, Loopback0
C        10.2.2.1 is directly connected, Loopback1
C        192.168.1.0/24 is directly connected, Ethernet0/0
C        192.168.10.0/24 is directly connected, Ethernet0/0.10
C        192.168.30.0/24 is directly connected, Ethernet0/0.30
C        192.168.99.0/24 is directly connected, Ethernet0/0.99
C        203.0.113.0/30 is directly connected, Ethernet0/1
```

```
RT-B-1#show ip int bri | include manual
Ethernet0/0.20             192.168.20.254  YES manual up
Ethernet0/0.30             192.168.30.1    YES manual up
Ethernet0/0.99             192.168.99.1    YES manual up
Ethernet0/1                205.0.115.1     YES manual up
Loopback0                  10.3.1.1        YES manual up
Loopback1                  10.3.2.1        YES manual up
Tunnel0                    172.16.1.6      YES manual up
Tunnel1                    172.16.2.2      YES manual up
```

```
RT-B-1#show ip route | include ^C
Codes: L - local, C - connected, S - static, R - RIP, M - mobi
C        10.3.1.1 is directly connected, Loopback0
C        10.3.2.1 is directly connected, Loopback1
C        192.168.1.0/24 is directly connected, Ethernet0/0
C        192.168.20.0/24 is directly connected, Ethernet0/0.20
C        192.168.30.0/24 is directly connected, Ethernet0/0.30
C        192.168.99.0/24 is directly connected, Ethernet0/0.99
C        205.0.115.0/30 is directly connected, Ethernet0/1
```

Configuration- HQ Master L3 Setup

Inter-Mesh

~~interface range E1/1-3~~
~~no shutdown~~
description **to CoreRT-2**
~~channel-group 1 mode active~~

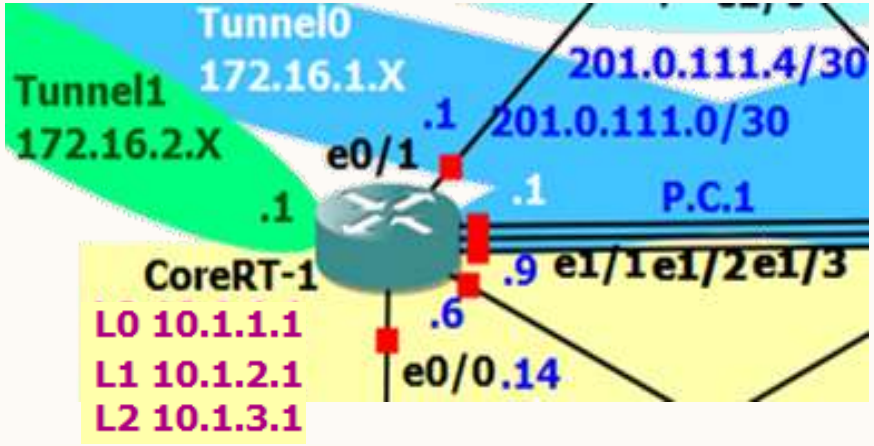
E1/1 is used over L3 ETH-CHN (GNS Incompatibility)

interface ~~Port-channel1~~ **E1/1**
ip address **192.168.100.9** 255.255.255.252
no shutdown
interface E**0/0**
description **VRRP 99 Subnet**
ip address 192.168.100.14 255.255.255.252
no shutdown
interface E**1/0**
ip address 192.168.100.6 255.255.255.252
no shutdown

Underlay (to ISP)

interface E**0/1**
description **Uplink to ISP**
ip address 201.0.111.1 255.255.255.252
no shutdown

interface Loopback2
ip address 10.1.3.**1** 255.255.255.255
no shutdown



Overlay (VPN)

interface Loopback0
ip address 10.1.1.**1** 255.255.255.255
no shutdown

interface Loopback1
ip address 10.1.2.**1** 255.255.255.255
no shutdown

interface Tunnel0
description **to RT-A-1, E0/1**
ip address 172.16.**1.1** 255.255.255.252
tunnel source Et0/1
tunnel destination **203.0.113.2**
no shutdown

interface Tunnel1
description **to RT-B-1, E0/1**
ip address 172.16.**2.1** 255.255.255.252
tunnel source Et0/1
tunnel destination **205.0.115.1**
no shutdown

Configuration- HQ Backup L3 Setup

Inter-Mesh

~~interface range E1/1-3~~
~~no shutdown~~
description **to CoreRT-1**
~~channel-group 1 mode active~~

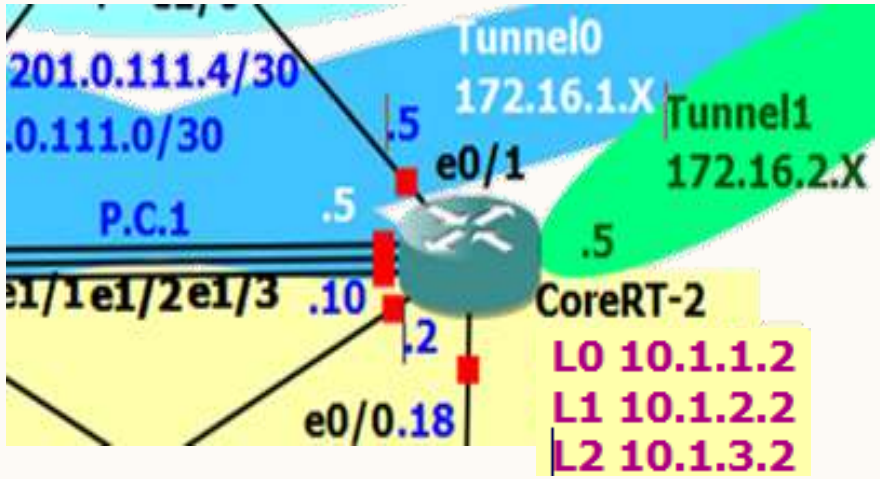
E1/1 is used over L3 ETH-CHN (GNS Incompatibility)

interface ~~Port-channel1~~ **E1/1**
ip address **192.168.100.10** 255.255.255.252
no shutdown
interface E**0/0**
description **VRRP 30 Subnet**
ip address 192.168.100.18 255.255.255.252
no shutdown
interface E**1/0**
ip address 192.168.100.2 255.255.255.252
no shutdown

Underlay (to ISP)

interface E**0/1**
description **Uplink to ISP**
ip address 201.0.111.5 255.255.255.252
no shutdown

interface Loopback2
ip address 10.1.3.**2** 255.255.255.255
no shutdown



Overlay (VPN)

interface Loopback0
ip address 10.1.1.**2** 255.255.255.255
no shutdown

interface Loopback1
ip address 10.1.2.**2** 255.255.255.255
no shutdown

interface Tunnel0
description **to RT-B-1, E0/1**
ip address 172.16.**1.5** 255.255.255.252
tunnel source Et0/1
tunnel destination **205.0.115.1**
no shutdown

interface Tunnel1
description **to RT-A-1, E0/1**
ip address 172.16.**2.5** 255.255.255.252
tunnel source Et0/1
tunnel destination **203.0.113.2**
no shutdown

Validation – HQ ISP & VPN Interfaces


```
CoreRT-1#show ip route | include ^C
Codes: L - local, C - connected, S - static, R - RIP, M - mobi
C        10.1.1.1 is directly connected, Loopback0
C        10.1.2.1 is directly connected, Loopback1
C        10.1.3.1 is directly connected, Loopback2
C        192.168.100.4/30 is directly connected, Ethernet1/0
C        192.168.100.8/30 is directly connected, Ethernet1/1
C        192.168.100.12/30 is directly connected, Ethernet0/0
C        201.0.111.0/30 is directly connected, Ethernet0/1
```

```
CoreRT-2#show ip route | include ^C
Codes: L - local, C - connected, S - static, R - RIP, M - mob
C        10.1.1.2 is directly connected, Loopback0
C        10.1.2.2 is directly connected, Loopback1
C        10.1.3.2 is directly connected, Loopback2
C        192.168.100.0/30 is directly connected, Ethernet1/0
C        192.168.100.8/30 is directly connected, Ethernet1/1
C        192.168.100.16/30 is directly connected, Ethernet0/0
C        201.0.111.4/30 is directly connected, Ethernet0/1
```

```
CoreRT-1#show ip int brief | include manual
Ethernet0/0                192.168.100.14  YES manual up
Ethernet0/1                201.0.111.1     YES manual up
Ethernet1/0                192.168.100.6   YES manual up
Ethernet1/1                192.168.100.9   YES manual up
Loopback0                  10.1.1.1        YES manual up
Loopback1                  10.1.2.1        YES manual up
Loopback2                  10.1.3.1        YES manual up
Tunnel0                    172.16.1.1      YES manual up
Tunnel1                    172.16.2.1      YES manual up
```

```
CoreRT-2#show ip int brief | include manual
Ethernet0/0                192.168.100.18  YES manual up
Ethernet0/1                201.0.111.5     YES manual up
Ethernet1/0                192.168.100.2   YES manual up
Ethernet1/1                192.168.100.10  YES manual up
Loopback0                  10.1.1.2        YES manual up
Loopback1                  10.1.2.2        YES manual up
Loopback2                  10.1.3.2        YES manual up
Tunnel0                    172.16.1.5      YES manual up
Tunnel1                    172.16.2.5      YES manual up
```

PVST & FHRP ALIGNMENT

Implementing PVST in a Tier 3 Architecture

A Tier 3 architecture involves multiple layers of network including:

1. Access Layer: Where end devices connect.
2. Distribution Layer: Aggregates access layer switches.
3. Core Layer: High-speed backbone providing external networks connectivity.

Key aspects of implementing PVST in a Tier 3 architecture:

1. Per-VLAN Optimization: Separate Spanning Tree Instances for optimizing path selection and **loop prevention** for each VLAN independently.
2. Root Placement: fit root bridges per-VLAN for **path balancing**.
3. Load Balancing: **Distribute traffic** across different links for improving overall network **performance** and **reliability**.
4. Failover & Redundancy: providing **multiple active** paths and quickly recalculating spanning tree paths in case of **link failures**.

Aligning PVST with First Hop Redundancy Protocol

FHRP protocols are used to provide redundancy and load balancing for the default gateway IP addresses.

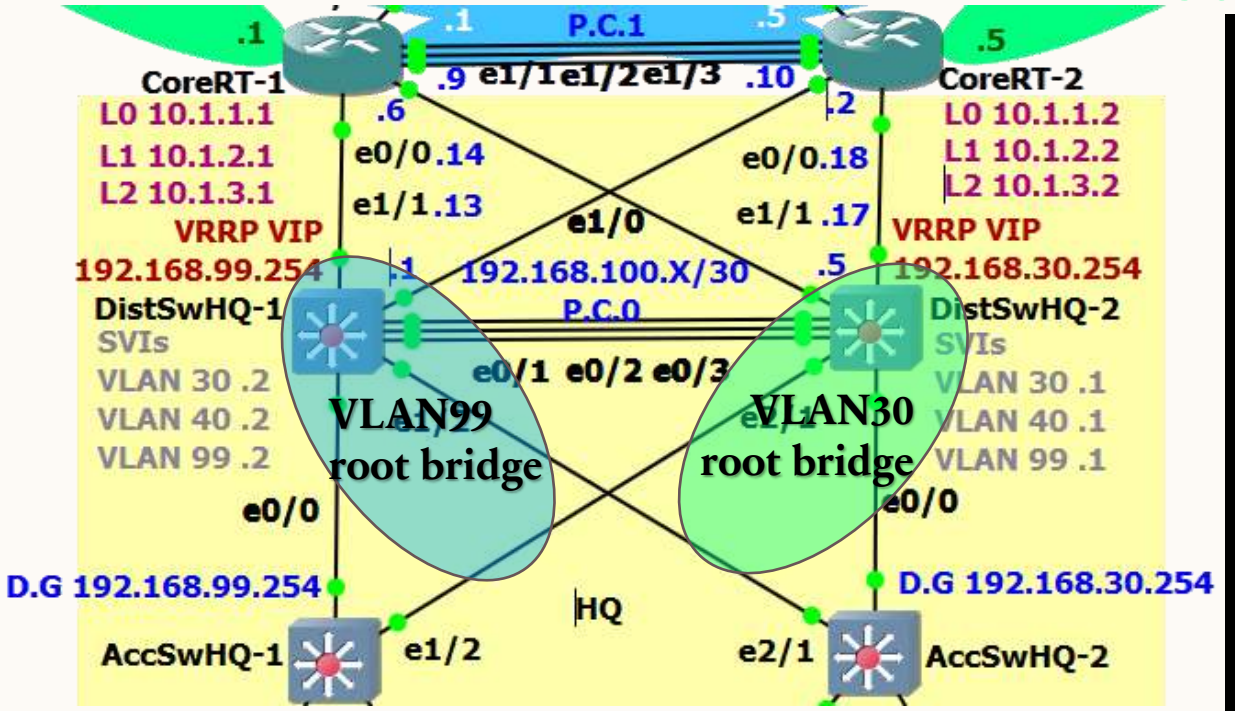
Integration with PVST is achieved by:

1. Switches (Access & Distribution)- Align **root bridge** configurations with **VLAN traffic** and FHRP virtual gateway addresses.
2. Multilayer Switches (Distribution & Core)- Ensure spanning tree and routing configurations are consistent with FHRP settings.
3. Routers- Coordinate FHRP configurations with routing protocols and align **VLAN interfaces** with spanning tree topology.
4. End Devices- Use the FHRP **virtual IP address as the default gateway**, ensuring that it aligns with the network's spanning tree design.

Configuration- PVST & VRRP

DistSwHQ-1 VRRP

```
! Configure VLAN 99 in PVST
spanning-tree vlan 99 priority 4096
spanning-tree vlan 30 priority 8192

! VRRP Configuration for VLAN 99
interface VLAN99
vrrp 99 ip 192.168.99.254
vrrp 99 priority 110
vrrp 99 preempt

! VRRP Configuration for VLAN 30
interface VLAN30
vrrp 30 ip 192.168.30.254
vrrp 30 priority 90
```



DistSwHQ-2 VRRP

```
! Configure VLAN 99 in PVST
spanning-tree vlan 99 priority 8192
spanning-tree vlan 30 priority 4096

! VRRP Configuration for VLAN 99
interface VLAN99
vrrp 99 ip 192.168.99.254
vrrp 99 priority 90

! VRRP Configuration for VLAN 30
interface VLAN30
vrrp 30 ip 192.168.30.254
vrrp 30 priority 110
vrrp 30 preempt
```

```
DistSwHQ-1(config)#spanning-tree vlan 99 priority 4096
DistSwHQ-1(config)#spanning-tree vlan 30 priority 8192
DistSwHQ-1(config)#
*Aug  5 06:07:30.256: %VRRP-6-STATECHANGE: Vl30 Grp 30 state Backup -> Master
DistSwHQ-1(config)#
*Aug  5 06:07:55.863: %VRRP-6-STATECHANGE: Vl30 Grp 30 state Master -> Backup
```

Validation – HQ PVST


```
DistSwHQ-1#show spanning-tree vlan 99

VLAN0099
  Spanning tree enabled protocol ieee
  Root ID     Priority    4195
              Address     aabb.cc00.0500
              This bridge is the root
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    4195   (priority 4096 sys-id-ext 99)
              Address     aabb.cc00.0500
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------
Et0/0               Desg FWD 100       128.1    P2p
Et1/2               Desg FWD 100       128.7    P2p
Po1                 Desg FWD 47        128.65   P2p
```

```
DistSwHQ-2#show spanning-tree vlan 30

VLAN0030
  Spanning tree enabled protocol ieee
  Root ID     Priority    4126
              Address     aabb.cc00.0400
              This bridge is the root
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    4126   (priority 4096 sys-id-ext 30)
              Address     aabb.cc00.0400
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------
Et0/0               Desg FWD 100       128.1    P2p
Et2/1               Desg FWD 100       128.10   P2p
Po1                 Desg FWD 47        128.65   P2p
```

PVST+ operates separately for each VLAN, so **none of the ports are in a blocking state** as topology is simple, with no loops.

Validation – HQ VRRP


```
DistSwHQ-1#show ip route | include ^C
Codes: L - local, C - connected, S - static, R - RIP, M - mobi
C        192.168.30.0/24 is directly connected, Vlan30
C        192.168.40.0/24 is directly connected, Vlan40
C        192.168.99.0/24 is directly connected, Vlan99
C        192.168.100.0/30 is directly connected, Ethernet1/0
C        192.168.100.12/30 is directly connected, Ethernet1/1
```

```
DistSwHQ-2#show ip route | include ^C
Codes: L - local, C - connected, S - static, R - RIP, M - mob
C        192.168.30.0/24 is directly connected, Vlan30
C        192.168.40.0/24 is directly connected, Vlan40
C        192.168.99.0/24 is directly connected, Vlan99
C        192.168.100.4/30 is directly connected, Ethernet1/0
C        192.168.100.16/30 is directly connected, Ethernet1/1
```

```
DistSwHQ-1#show ip int bri | include manual
Ethernet1/0                192.168.100.1   YES manual up
Ethernet1/1                192.168.100.13  YES manual up
Vlan30                     192.168.30.1    YES manual up
Vlan40                     192.168.40.1    YES manual up
Vlan99                     192.168.99.1    YES manual up
```

```
DistSwHQ-2#show ip int bri | include manual
Ethernet1/0                192.168.100.5   YES manual up
Ethernet1/1                192.168.100.17  YES manual up
Vlan30                     192.168.30.2    YES manual up
Vlan40                     192.168.40.2    YES manual up
Vlan99                     192.168.99.2    YES manual up
```

```
DistSwHQ-1#show vrrp brief
Interface          Grp Pri Time  Own Pre State   Master addr     Group addr
Vl30               30  90  3648        Y  Backup  192.168.30.2    192.168.30.254
Vl99               99  110 3570        Y  Master  192.168.99.1    192.168.99.254
```

```
DistSwHQ-2#show vrrp brief
Interface          Grp Pri Time  Own Pre State   Master addr     Group addr
Vl30               30  110 3570        Y  Master  192.168.30.2    192.168.30.254
Vl99               99  90  3648        Y  Backup  192.168.99.1    192.168.99.254
```

```
DistSwHQ-1#show int status | include routed
Et1/0     Uplinks                  connected    routed
Et1/1     VRRP 99 Subnet           connected    routed
```

```
DistSwHQ-2#show int status | include routed
Et1/0     Uplinks                  connected    routed
Et1/1     VRRP 30 Subnet           connected    routed
```

Configuration- DHCP Services

Branch A- RT-A-1

```
ip dhcp excluded-address 192.168.99.1 192.168.99.10
ip dhcp pool VLAN99
network 192.168.99.0 255.255.255.0
default-router 192.168.99.6        ! ROAS via SVI 99
exit
ip dhcp excluded-address 192.168.30.1 192.168.30.10
ip dhcp pool VLAN30
network 192.168.30.0 255.255.255.0
default-router 192.168.30.6        ! ROAS via SVI 30
exit
ip dhcp excluded-address 192.168.10.1 192.168.10.10
ip dhcp pool VLAN10
network 192.168.10.0 255.255.255.0
default-router 192.168.10.1        ! ROAS via SVI 10
```

HQ- DistSwHQs

```
! DistSwHQ-1
ip dhcp excluded-address 192.168.99.1 192.168.99.10
ip dhcp pool VLAN99
network 192.168.99.0 255.255.255.0
default-router 192.168.99.254      ! VRRP 90 VIP

! DistSwHQ-2
ip dhcp excluded-address 192.168.30.1 192.168.30.10
ip dhcp pool VLAN30
network 192.168.30.0 255.255.255.0
default-router 192.168.30.254      ! VRRP 30 VIP
exit
ip dhcp excluded-address 192.168.40.1 192.168.40.10
ip dhcp pool VLAN40
network 192.168.40.0 255.255.255.0
default-router 192.168.40.1        ! DistSwHQ-2
```

Branch B- RT-B-1

```
ip dhcp excluded-address 192.168.99.1 192.168.99.10
ip dhcp pool VLAN99
network 192.168.99.0 255.255.255.0
default-router 192.168.99.5        ! ROAS via SVI 99
exit
ip dhcp excluded-address 192.168.30.1 192.168.30.10
ip dhcp pool VLAN30
network 192.168.30.0 255.255.255.0
default-router 192.168.30.5        ! ROAS via SVI 30
exit
ip dhcp excluded-address 192.168.20.1 192.168.20.10
ip dhcp pool VLAN20
network 192.168.20.0 255.255.255.0
default-router 192.168.20.1        ! ROAS via SVI 20
```

Validation – DHCP Distribution

HQ- VLANS 30,40

```
DistSwHQ-2#show ip dhcp pool

Pool VLAN30 :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 1
 Excluded addresses             : 10
 Pending event                  : none
 1 subnet is currently in the pool :
 Current index        IP address range                  Leased/Excluded/Total
 192.168.30.12        192.168.30.1      - 192.168.30.254    1      / 10     / 254

Pool VLAN40 :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 1
 Excluded addresses             : 10
 Pending event                  : none
 1 subnet is currently in the pool :
 Current index        IP address range                  Leased/Excluded/Total
 192.168.40.12        192.168.40.1      - 192.168.40.254    1      / 10     / 254
```

```
DistSwHQ-1#show ip dhcp bind
Bindings from all pools not associated with VRF:
IP address      Client-ID/              Lease expiration        Type       State      Interface
                Hardware address/
                User name
192.168.99.11    0100.5079.6668.03       Aug 03 2024 08:59 PM    Automatic  Active     Vlan99
192.168.99.12    0100.5079.6668.02       Aug 03 2024 08:59 PM    Automatic  Active     Vlan99
```

Branch A

```
RT-A-1#show ip dhcp bind
Bindings from all pools not associated with VRF:
IP address          Client-ID/              Lease expiration        Type
                    Hardware address/
                    User name
192.168.30.11       0100.5079.6668.06       Aug 03 2024 08:13 PM    Automatic
192.168.99.11       0100.5079.6668.05       Aug 03 2024 08:14 PM    Automatic
```

Branch B

```
RT-B-1#show ip dhcp bind
Bindings from all pools not associated with VRF:
IP address          Client-ID/              Lease expiration        Type
                    Hardware address/
                    User name
192.168.30.11       0100.5079.6668.00       Aug 03 2024 08:15 PM    Automatic
192.168.99.11       0100.5079.6668.01       Aug 03 2024 08:15 PM    Automatic
```

HQ- VLAN 99

```
DistSwHQ-1#show ip dhcp pool

Pool VLAN99 :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 2
 Excluded addresses             : 10
 Pending event                  : none
 1 subnet is currently in the pool :
 Current index        IP address range                  Leased/Excluded/Total
 192.168.99.13        192.168.99.1      - 192.168.99.254    2      / 10     / 254
```

```
DistSwHQ-2#show ip dhcp bind
Bindings from all pools not associated with VRF:
IP address      Client-ID/              Lease expiration        Type       State      Interface
                Hardware address/
                User name
192.168.30.11    0100.5079.6668.07       Aug 03 2024 08:59 PM    Automatic  Active     Vlan30
192.168.40.11    0100.5079.6668.04       Aug 03 2024 08:59 PM    Automatic  Active     Vlan40
```

Validation – Per-Branch Inter-VLAN routing

```
MngB-PC-1> ip dhcp
DDORA IP 192.168.99.11/24 GW 192.168.99.2
```

```
ProdB-PC-1> ip dhcp
DDORA IP 192.168.30.11/24 GW 192.168.30.2
```

```
HQ-PC-1> ip dhcp
DDORA IP 192.168.30.11/24 GW 192.168.30.254
```

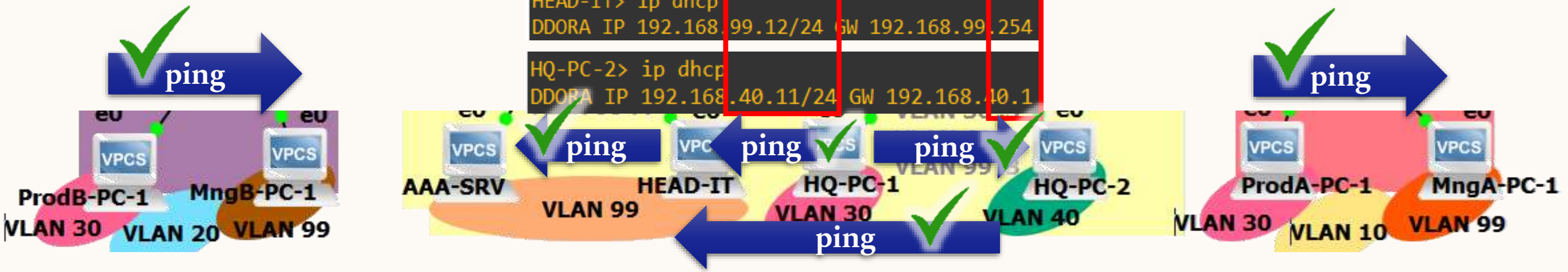
```
AAA-SRV> ip dhcp
DDORRA IP 192.168.99.11/24 GW 192.168.99.254
```

```
HEAD-IT> ip dhcp
DDORA IP 192.168.99.12/24 GW 192.168.99.254
```

```
HQ-PC-2> ip dhcp
DDORA IP 192.168.40.11/24 GW 192.168.40.1
```

```
MngA-PC-1> ip dhcp
DDORA IP 192.168.99.11/24 GW 192.168.99.2
```

```
ProdA-PC-1> ip dhcp
DDORA IP 192.168.30.11/24 GW 192.168.30.2
```



B ROAS

```
ProdB-PC-1> ping 192.168.99.11
192.168.99.11 icmp_seq=1 timeout
84 bytes from 192.168.99.11 icmp_seq=2 ttl=63
84 bytes from 192.168.99.11 icmp_seq=3 ttl=63
84 bytes from 192.168.99.11 icmp_seq=4 ttl=63
84 bytes from 192.168.99.11 icmp_seq=5 ttl=63
```

HQ MLS/SVI

```
HQ-PC-1> ping 192.168.99.11
192.168.99.11 icmp_seq=1 timeout
84 bytes from 192.168.99.11 icmp_seq=2 ttl=63
84 bytes from 192.168.99.11 icmp_seq=3 ttl=63
84 bytes from 192.168.99.11 icmp_seq=4 ttl=63
84 bytes from 192.168.99.11 icmp_seq=5 ttl=63
```

A ROAS

```
ProdA-PC-1> ping 192.168.99.11
192.168.99.11 icmp_seq=1 timeout
84 bytes from 192.168.99.11 icmp_seq=2 ttl=63
84 bytes from 192.168.99.11 icmp_seq=3 ttl=63
84 bytes from 192.168.99.11 icmp_seq=4 ttl=63
84 bytes from 192.168.99.11 icmp_seq=5 ttl=63
```

HQ MLS/SVI ARP

```
HQ-PC-1> ping 192.168.99.12
192.168.99.12 icmp_seq=1 timeout
192.168.99.12 icmp_seq=2 timeout
192.168.99.12 icmp_seq=3 timeout
84 bytes from 192.168.99.12 icmp_seq=4 ttl=63
84 bytes from 192.168.99.12 icmp_seq=5 ttl=63
```

HQ MLS/SVI

```
HQ-PC-2> ping 192.168.99.12
84 bytes from 192.168.99.12 icmp_seq=1 ttl=63
HQ-PC-2> trace 192.168.99.12 -P 1
trace to 192.168.99.12, 8 hops max (ICMP), press C
 1   192.168.40.1    1.401 ms  0.947 ms  6.375 ms
 2   192.168.99.12   8.634 ms  4.119 ms  5.345 ms
```

HQ MLS/SVI ARP

```
HQ-PC-1> ping 192.168.40.11
192.168.40.11 icmp_seq=1 timeout
192.168.40.11 icmp_seq=2 timeout
84 bytes from 192.168.40.11 icmp_seq=3 ttl=63
84 bytes from 192.168.40.11 icmp_seq=4 ttl=63
84 bytes from 192.168.40.11 icmp_seq=5 ttl=63
```

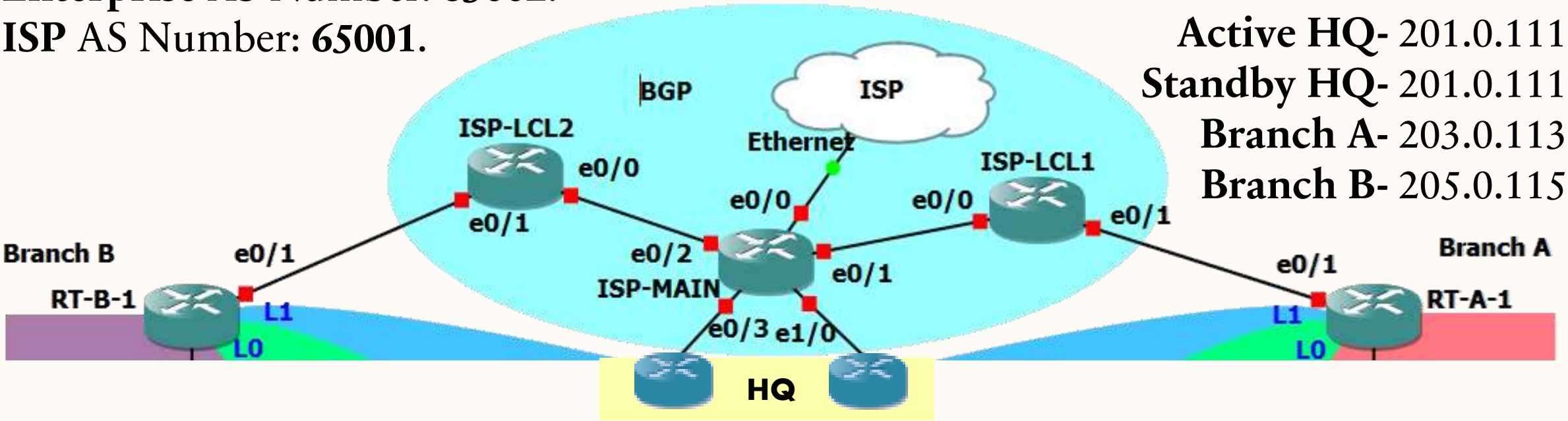
ISP & BGP IMPLEMENTATION

ISP Implementation

In order to account for a modern scenario, where Edge-routers of an enterprise network are involved with **BGP** routing & **NAT** translation, this project exceeds it's scope, and demonstrates an **ISP** topology implementation.

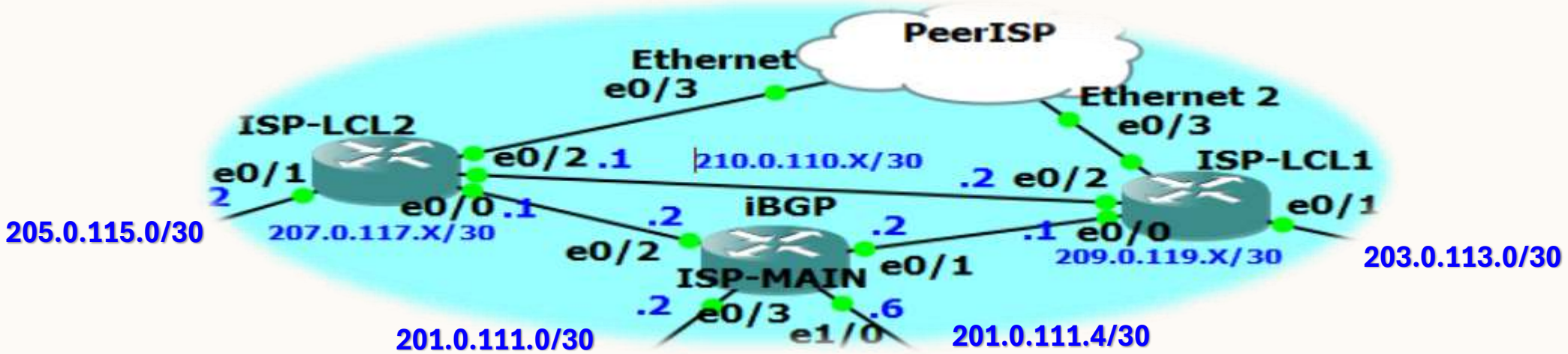
Enterprise AS Number: **65002.**
ISP AS Number: **65001.**

Outside-local IPv4 Allocation:
Active HQ- 201.0.111.0/30
Standby HQ- 201.0.111.4/30
Branch A- 203.0.113.0/30
Branch B- 205.0.115.0/30



ISP Addressing Table

Device	Interface	Heading	IP Address	S. Mask	Description
ISP-MAIN	GigabitEthernet0/0	Inside	210.0.110.1	255.255.255.252	Internet
	GigabitEthernet0/1	Inside	209.0.119.2	255.255.255.252	To ISP-LCL1
	GigabitEthernet0/2	Inside	201.0.111.6	255.255.255.252	Client AS 65002- CoreRT-2
	GigabitEthernet0/3	Client	207.0.117.2	255.255.255.252	To ISP-LCL2
	GigabitEthernet1/0	Client	201.0.111.2	255.255.255.252	Client AS 65002- CoreRT-1
ISP-LCL1	GigabitEthernet0/0	Inside	209.0.119.1	255.255.255.252	To ISP-MAIN
	GigabitEthernet0/1	Client	203.0.113.1	255.255.255.252	Client AS 65002- RT-A-1
	GigabitEthernet0/2	Inside	210.0.110.2	255.255.255.252	To ISP-LCL2
ISP-LCL2	GigabitEthernet0/0	Inside	207.0.117.1	255.255.255.252	To ISP-MAIN
	GigabitEthernet0/1	Client	205.0.115.2	255.255.255.252	Client AS 65002- RT-B-1
	GigabitEthernet0/2	Inside	210.0.110.1	255.255.255.252	To ISP-LCL1



Configuration- ISP Interfaces

ISP-LCL2

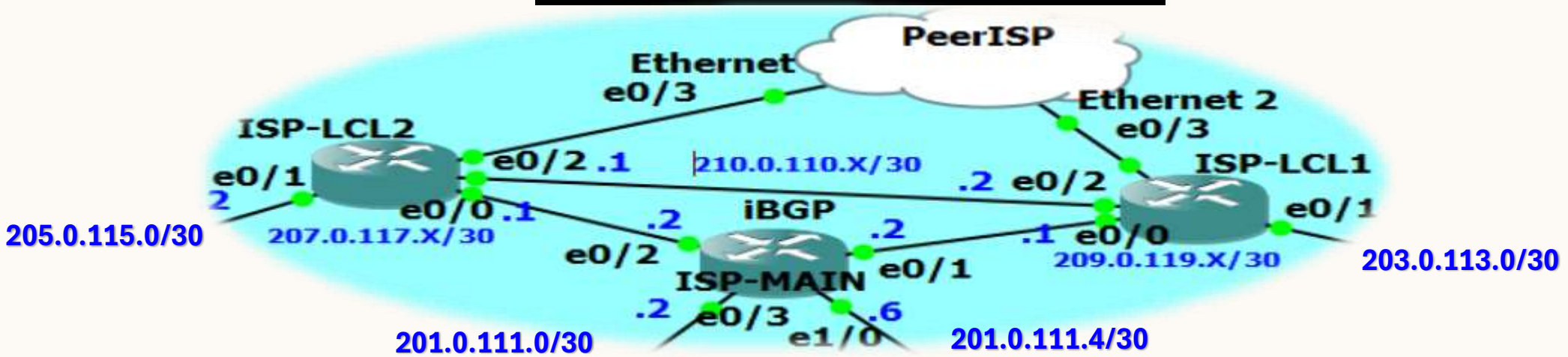
```
interface E0/0
ip address 207.0.117.1 255.255.255.252
no shutdown
interface E0/1
ip address 205.0.115.2 255.255.255.252
no shutdown
interface E0/2
ip address 210.0.110.1 255.255.255.252
no shutdown
```

ISP-MAIN

```
interface range E0/0-3, E1/0
no shutdown
interface E0/1
ip address 209.0.119.2 255.255.255.252
interface E0/2
ip address 207.0.117.2 255.255.255.252
interface E0/3
ip address 201.0.111.2 255.255.255.252
interface E1/0
ip address 201.0.111.6 255.255.255.252
```

ISP-LCL1

```
interface E0/0
ip address 209.0.119.1 255.255.255.252
no shutdown
interface E0/1
ip address 203.0.113.1 255.255.255.252
no shutdown
interface E0/2
ip address 210.0.110.2 255.255.255.252
no shutdown
```



Configuration- ISP i&eBGP

ISP-LCL2

```
router bgp 65001
 bgp log-neighbor-changes

! BGP Peers
 neighbor 207.0.117.2 remote-as 65001
 neighbor 205.0.115.1 remote-as 65002
 neighbor 210.0.110.2 remote-as 65001

! Advertise networks
network 207.0.117.0 mask 255.255.255.252
network 205.0.115.0 mask 255.255.255.252
network 210.0.110.0 mask 255.255.255.252
```

ISP-MAIN

```
router bgp 65001
 bgp log-neighbor-changes
! BGP Peers
 neighbor 207.0.117.1 remote-as 65001
 neighbor 209.0.119.1 remote-as 65001
 neighbor 201.0.111.1 remote-as 65002
 neighbor 201.0.111.5 remote-as 65002
! Advertise networks
network 207.0.117.0 mask 255.255.255.252
network 209.0.119.0 mask 255.255.255.252
network 201.0.111.0 mask 255.255.255.252
network 201.0.111.4 mask 255.255.255.252
```

ISP-LCL1

```
router bgp 65001
 bgp log-neighbor-changes

! BGP Peers
 neighbor 209.0.119.2 remote-as 65001
 neighbor 203.0.113.2 remote-as 65002
 neighbor 210.0.110.1 remote-as 65001

! Advertise networks
network 209.0.119.0 mask 255.255.255.252
network 203.0.113.0 mask 255.255.255.252
network 210.0.110.0 mask 255.255.255.252
```

RT-B-1

```
router bgp 65002
 bgp log-neighbor-changes

! eBGP Peers
 neighbor 205.0.115.2 remote-as 65001
```

CoreRT-1

```
router bgp 65002
 bgp log-neighbor-changes

! eBGP Peers
 neighbor 201.0.111.2 remote-as 65001
```

CoreRT-2

```
router bgp 65002
 bgp log-neighbor-changes

! eBGP Peers
 neighbor 201.0.111.6 remote-as 65001
```

RT-A-1

```
router bgp 65002
 bgp log-neighbor-changes

! eBGP Peers
 neighbor 203.0.113.1 remote-as 65001
```

Validation- ISPs iBGP


```
ISP-MAIN#show ip bgp summary
BGP router identifier 209.0.119.2, local AS number 65001
Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
201.0.111.1     4        65002       7       9        7    0    0 00:03:26        0
201.0.111.5     4        65002       7      11        7    0    0 00:03:12        0
207.0.117.1     4        65001       9       9        7    0    0 00:05:30        2
209.0.119.1     4        65001       9       9        7    0    0 00:05:29        2
```

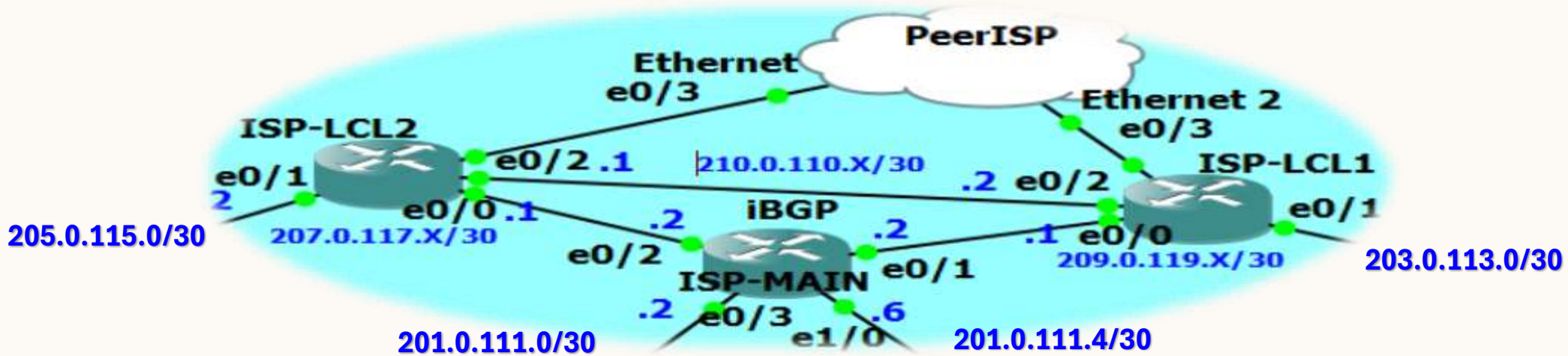
```
ISP-LCL1#show ip bgp summary
BGP router identifier 209.0.119.1, local AS number 65001
Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
203.0.113.2     4        65002      13      15        6    0    0 00:08:35        0
209.0.119.2     4        65001      14      14        6    0    0 00:09:52        4
```

```
ISP-LCL2#show ip bgp summary
BGP router identifier 207.0.117.1, local AS number 65001
Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
205.0.115.1     4        65002       0       0        1    0    0 never    Idle
207.0.117.2     4        65001      14      14        6    0    0 00:09:57        4
```

Validation- Enterprise-ISP eBGP Adjacency


```
RT-B-1#show ip route | include ^B
B        201.0.111.0 [20/0] via 205.0.115.2, 00:00:25
B        201.0.111.4 [20/0] via 205.0.115.2, 00:00:25
B        207.0.117.0 [20/0] via 205.0.115.2, 00:00:25
B        209.0.119.0 [20/0] via 205.0.115.2, 00:00:25
```

```
RT-A-1#show ip route | include ^B
B        201.0.111.0 [20/0] via 203.0.113.1, 00:24:17
B        201.0.111.4 [20/0] via 203.0.113.1, 00:24:17
B        207.0.117.0 [20/0] via 203.0.113.1, 00:24:17
B        209.0.119.0 [20/0] via 203.0.113.1, 00:24:17
```




```
CoreRT-1#show ip route | include ^B
B        201.0.111.4/30 [20/0] via 201.0.111.2, 00:23:43
B        203.0.113.0 [20/0] via 201.0.111.2, 00:23:43
B        205.0.115.0 [20/0] via 201.0.111.2, 00:23:43
B        207.0.117.0 [20/0] via 201.0.111.2, 00:23:43
B        209.0.119.0 [20/0] via 201.0.111.2, 00:23:43
```

```
CoreRT-2#show ip route | include ^B
B        201.0.111.0/30 [20/0] via 201.0.111.6, 00:23:08
B        203.0.113.0 [20/0] via 201.0.111.6, 00:23:08
B        205.0.115.0 [20/0] via 201.0.111.6, 00:23:08
B        207.0.117.0 [20/0] via 201.0.111.6, 00:23:08
B        209.0.119.0 [20/0] via 201.0.111.6, 00:23:08
```

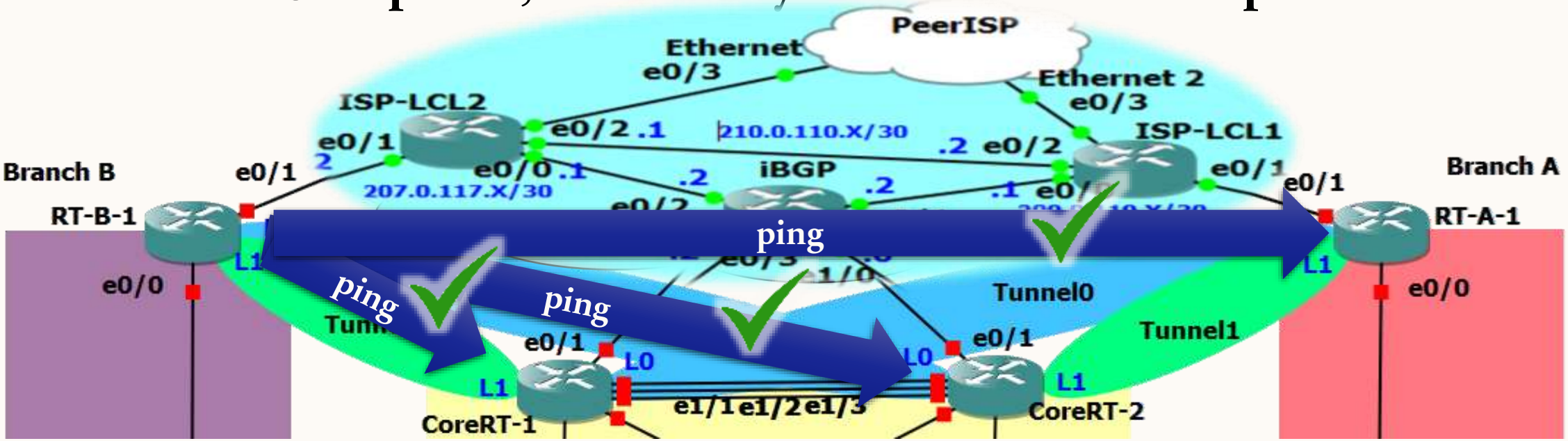
Validation- ISP inter-Routing


```
RT-B-1#trace 201.0.111.1
Type escape sequence to abort.
Tracing the route to 201.0.111.1
VRF info: (vrf in name/id, vrf out name/id)
  1 205.0.115.2 [AS 65001] 1 msec 5 msec 5 msec
  2 207.0.117.2 [AS 65001] 5 msec 6 msec 4 msec
  3 201.0.111.1 [AS 65001] 2 msec 5 msec 6 msec
```

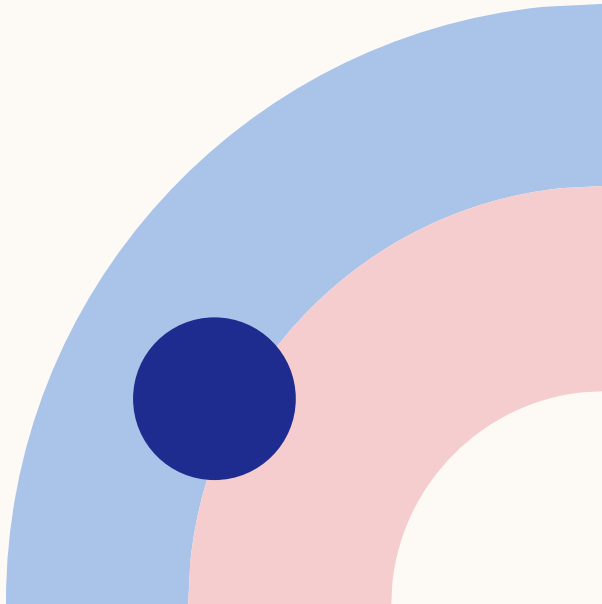
```
RT-B-1#trace 201.0.111.5
Type escape sequence to abort.
Tracing the route to 201.0.111.5
VRF info: (vrf in name/id, vrf out name/id)
  1 205.0.115.2 [AS 65001] 1 msec 0 msec 1 msec
  2 207.0.117.2 [AS 65001] 0 msec 2 msec 1 msec
  3 201.0.111.5 [AS 65001] 1 msec 0 msec 2 msec
```

```
RT-B-1#TRACE 203.0.113.2
Type escape sequence to abort.
Tracing the route to 203.0.113.2
VRF info: (vrf in name/id, vrf out name/id)
  1 205.0.115.2 [AS 65001] 131 msec 215 msec 136 msec
  2 210.0.110.2 [AS 65001] 386 msec 224 msec 570 msec
  3 203.0.113.2 [AS 65001] 609 msec 314 msec 366 msec
```

- **Simulated a 3-hops ISP, detailed by the trace-route output.**



ROUTING, VPN, NAT



Overlay vs. Underlay Networks

- Underlay Network: a physical or logical infrastructure that provides basic connectivity. It consists of physical routers & switches- transporting packets from one point to another.
- Overlay Network: a virtual network that is built on top of the underlay network. It uses tunneling (such as VPNs) to create logical networks that can operate independently of the underlying physical network, allowing for additional features like encryption, segmentation, and advanced routing.

Advantages of VPNs Between Enterprise Branches

- Security: VPNs provide a secure communication channel over **potentially untrusted networks** (like public internet). Data is encrypted.
- Privacy: VPNs ensure that sensitive data transmitted between branches remains **confidential** and is not visible to unauthorized parties.
- Isolation: VPNs allow branches to communicate **as if they are on the same local network**, simplifying access to file servers, applications, and databases.
- Access Control: VPNs can enforce **access policies** and ensure that only authorized users and devices can access the enterprise network.

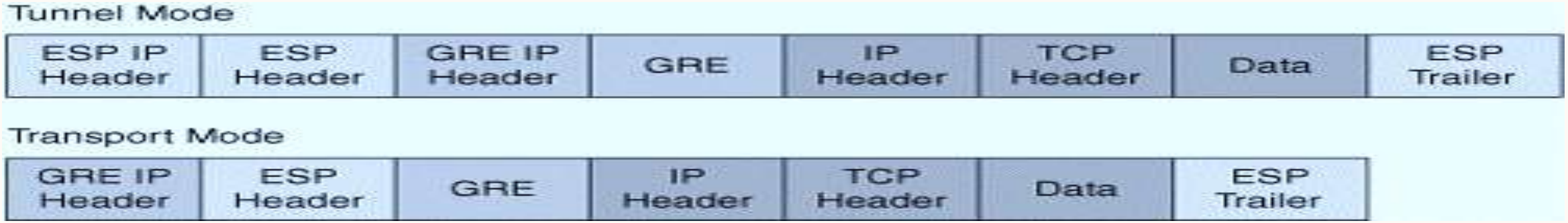
VPN Encapsulation Consequences

- Overhead: VPNs often use encapsulation techniques to **wrap data packets.** For instance, if a VPN uses protocols like **GRE** (Generic Routing Encapsulation) or **IPsec**, computational **resources** are needed to accommodate encrypted data**.**

- Fragmentation Avoidance: The standard **MTU** size for Ethernet is **1500** bytes. However, when VPN encapsulation is applied, the packet size increases due to the **extra headers.** If MTU size is not adjusted, it leads to packet **fragmentation**, degrading **performance** and increasing overhead. Setting the MTU to 1400 bytes- accommodates for final packet size.

GRE over IPsec

- In a normal IPsec tunnel, **static routes** are needed to direct IP packets into a IPsec tunnel.
- In a GRE-over-IPsec tunnel, GRE provides routing **connectivity**, while IPsec provides the **confidentiality** and **integrity**. With GRE, routing **protocols** can pass the IPsec tunnel.



- **Transport** mode is used if the original IP header can be exposed, while **Tunnel** mode protects the original IP header within a new IPsec IP header. When using GRE over IPsec, transport mode is often **sufficient**, because GRE and IPsec endpoints are **often the same.**

Branch A\HQ VPN - GRE over IPsec

Tunnel0- RT-A-1 / CoreRT-1

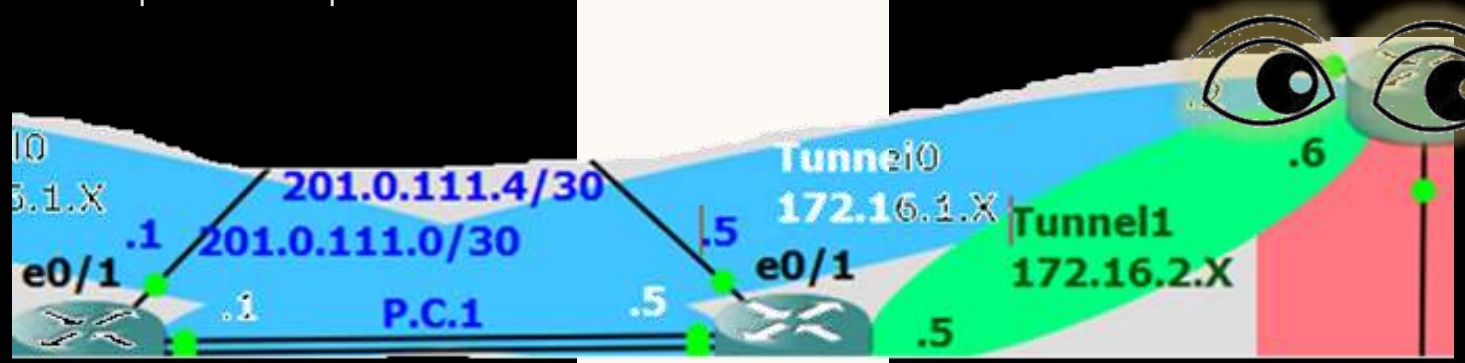
RT-A-1

```
! PHASE #1
crypto isakmp policy 10
  encryption aes 256
  authentication pre-share
  hash sha256
  group 2
  lifetime 3600
crypto isakmp key Tunnelkey address 201.0.111.1

! PHASE #2
crypto ipsec transform-set A-HQ1-VPN esp-aes 256 esp-sha256-hmac
  mode transport
  exit
crypto ipsec profile A-HQ1-GRE
 set transform-set A-HQ1-VPN

interface tunnel 0
  ip mtu 1400
  bandwidth 4000
  tunnel protection ipsec profile A-HQ1-GRE
```

Tunnel1- RT-A-1 / CoreRT-2

RT-A-1

```
! PHASE #1
crypto isakmp policy 20
  encryption aes 256
  authentication pre-share
  hash sha256
  group 2
  lifetime 3600
crypto isakmp key Tunnelkey address 201.0.111.5

! PHASE #2
crypto ipsec transform-set A-HQ2-VPN esp-aes 256 esp-sha256-hmac
  mode transport
  exit
crypto ipsec profile A-HQ2-GRE
 set transform-set A-HQ2-VPN

interface tunnel 1
  ip mtu 1400
  bandwidth 4000
  tunnel protection ipsec profile A-HQ2-GRE
```

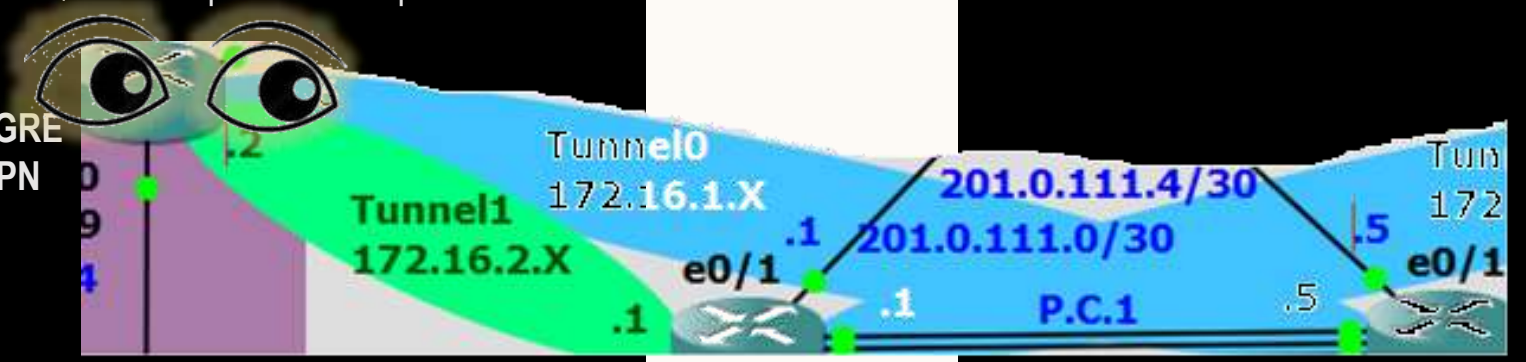


Branch B\HQ VPN - GRE over IPsec

Tunnel0- RT-B-1 / CoreRT-2

RT-B-1

```
! PHASE #1
crypto isakmp policy 10
 encryption aes 256
 authentication pre-share
 hash sha256
 group 2
 lifetime 3600
crypto isakmp key Tunnelkey address 201.0.111.5

! PHASE #2
crypto ipsec transform-set B-HQ2-VPN esp-aes 256 esp-sha256-hmac
 mode transport
 exit
crypto ipsec profile B-HQ2-GRE
 set transform-set B-HQ2-VPN

interface tunnel 0
 ip mtu 1400
 bandwidth 4000
 tunnel protection ipsec profile B-HQ2-GRE
```



Tunnel1- RT-B-1 / CoreRT-1

RT-B-1

```
! PHASE #1
crypto isakmp policy 20
 encryption aes 256
 authentication pre-share
 hash sha256
 group 2
 lifetime 3600
crypto isakmp key Tunnelkey address 201.0.111.1

! PHASE #2
crypto ipsec transform-set B-HQ1-VPN esp-aes 256 esp-sha256-hmac
 mode transport
 exit
crypto ipsec profile B-HQ1-GRE
 set transform-set B-HQ1-VPN

interface tunnel 1
 ip mtu 1400
 bandwidth 4000
 tunnel protection ipsec profile B-HQ1-GRE
```

HQ\Branch A VPN - GRE over IPsec

Tunnel0- CoreRT-1 / RT-A-1

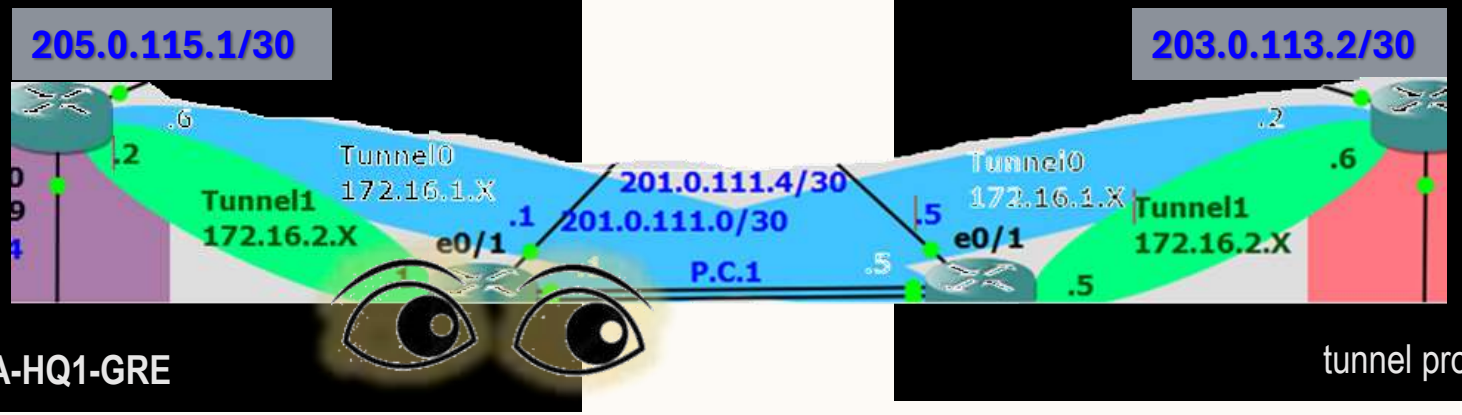
CoreRT-1

```
! PHASE #1
crypto isakmp policy 10
  encryption aes 256
  authentication pre-share
  hash sha256
  group 2
  lifetime 3600
crypto isakmp key Tunnelkey address 203.0.113.2

! PHASE #2
crypto ipsec transform-set A-HQ1-VPN esp-aes 256 esp-sha256-hmac
  mode transport
  exit
crypto ipsec profile A-HQ1-GRE
 set transform-set A-HQ1-VPN

interface tunnel 0
  ip mtu 1400
  bandwidth 4000
  tunnel protection ipsec profile A-HQ1-GRE
```

Tunnel1- CoreRT-1 / RT-B-1

CoreRT-1

```
! PHASE #1
crypto isakmp policy 20
  encryption aes 256
  authentication pre-share
  hash sha256
  group 2
  lifetime 3600
crypto isakmp key Tunnelkey address 205.0.115.1

! PHASE #2
crypto ipsec transform-set A-HQ2-VPN esp-aes 256 esp-sha256-hmac
  mode transport
  exit
crypto ipsec profile A-HQ2-GRE
 set transform-set A-HQ2-VPN

interface tunnel 1
  ip mtu 1400
  bandwidth 4000
  tunnel protection ipsec profile A-HQ2-GRE
```



HQ\Branch B VPN - GRE over IPsec

Tunnel0- CoreRT-2 / RT-B-1

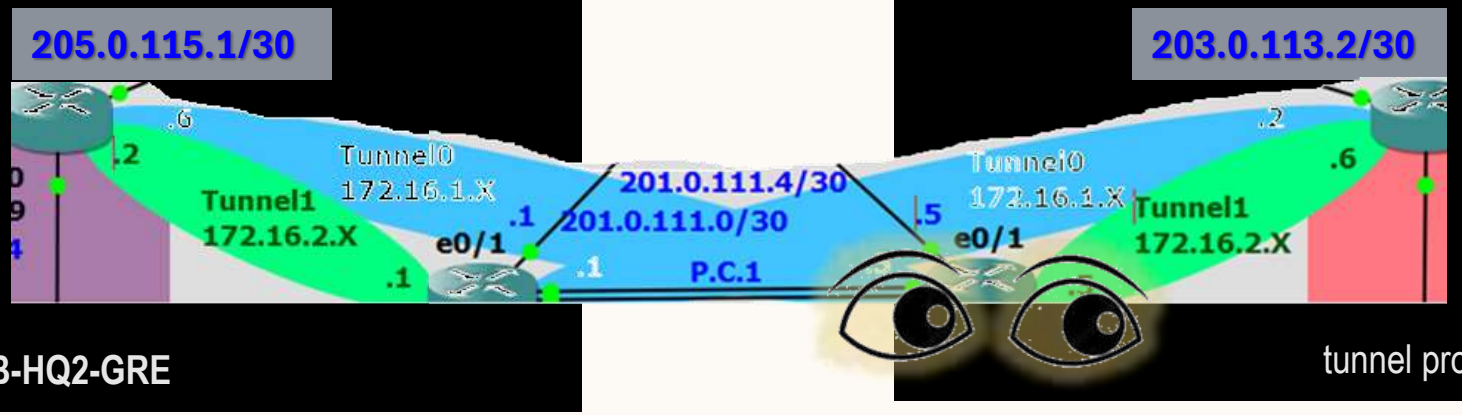
CoreRT-2

```
! PHASE #1
crypto isakmp policy 10
  encryption aes 256
  authentication pre-share
  hash sha256
  group 2
  lifetime 3600
crypto isakmp key Tunnelkey address 205.0.115.1

! PHASE #2
crypto ipsec transform-set B-HQ2-VPN esp-aes 256 esp-sha256-hmac
  mode transport
  exit
crypto ipsec profile B-HQ2-GRE
 set transform-set B-HQ2-VPN

interface tunnel 0
  ip mtu 1400
  bandwidth 4000
  tunnel protection ipsec profile B-HQ2-GRE
```

Tunnel1- CoreRT-2 / RT-A-1

CoreRT-2

```
! PHASE #1
crypto isakmp policy 20
  encryption aes 256
  authentication pre-share
  hash sha256
  group 2
  lifetime 3600
crypto isakmp key Tunnelkey address 203.0.113.2

! PHASE #2
crypto ipsec transform-set B-HQ1-VPN esp-aes 256 esp-sha256-hmac
  mode transport
  exit
crypto ipsec profile B-HQ1-GRE
 set transform-set B-HQ1-VPN

interface tunnel 1
  ip mtu 1400
  bandwidth 4000
tunnel protection ipsec profile B-HQ1-GRE
```



Validation- GRE over IPsec


```
CoreRT-1#show interfaces tunnel 0
Tunnel0 is up, line protocol is up
  Hardware is Tunnel
  Description: to RT-A-1, E0/1
  Internet address is 172.16.1.1/30
  MTU 17874 bytes, BW 4000 Kbit/sec, DLY 50000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel linestate evaluation up
  Tunnel source 201.0.111.1 (Ethernet0/1), destination 203.0.113.2
   Tunnel Subblocks:
      src-track:
         Tunnel0 source tracking subblock associated with Ethernet0/1
          Set of tunnels with source Ethernet0/1, 2 members (includes
  Tunnel protocol/transport GRE/IP
    Key disabled, sequencing disabled
    Checksumming of packets disabled
  Tunnel TTL 255, Fast tunneling enabled
  Tunnel transport MTU 1434 bytes
  Tunnel transmit bandwidth 8000 (kbps)
  Tunnel receive bandwidth 8000 (kbps)
  Tunnel protection via IPSec (profile "A-HQ1-GRE")
  Last input never, output never, output hang never
```

Overlay

Underlay

```
CoreRT-1#show crypto isakmp policy

Global IKE policy
Protection suite of priority 10
        encryption algorithm:   AES - Advanced Encryption Standard
        hash algorithm:         Secure Hash Standard 2 (256 bit)
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               3600 seconds, no volume limit
```

debug crypto isakmp
debug crypto ipsec

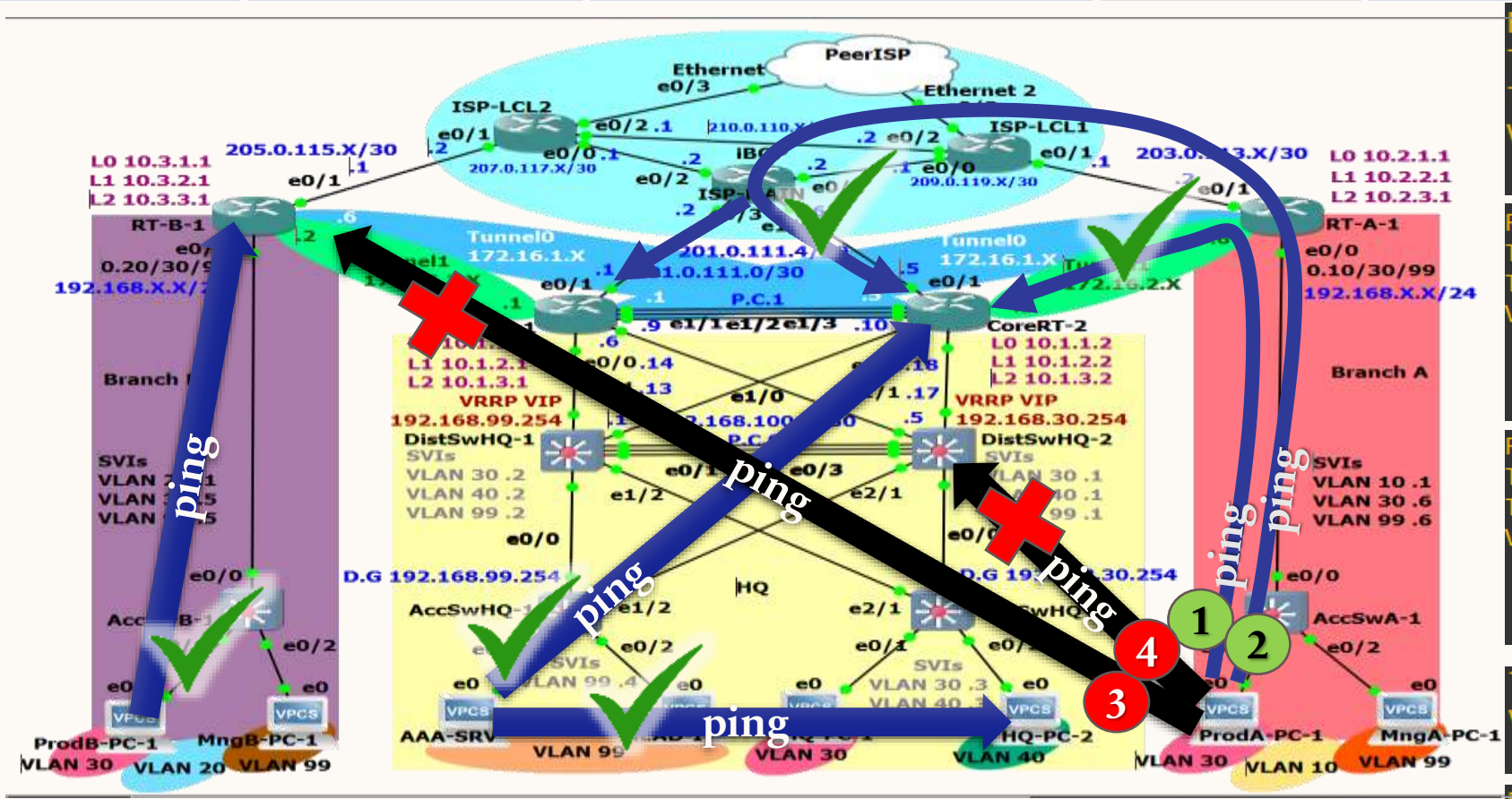
```
RT-A-1#show crypto ipsec transform-set
Transform set default: { esp-aes esp-sha-hmac  }
   will negotiate = { Transport,  },

Transform set A-HQ1-VPN: { esp-256-aes esp-sha256-hmac  }
   will negotiate = { Transport,  },

Transform set A-HQ2-VPN: { esp-256-aes esp-sha256-hmac  }
   will negotiate = { Transport,  },
```

```
RT-B-1#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
205.0.115.1     201.0.111.1     QM_IDLE           1001 ACTIVE
205.0.115.1     201.0.111.5     QM_IDLE           1002 ACTIVE
```

```
CoreRT-2#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
203.0.113.2     201.0.111.5     QM_IDLE           1002 ACTIVE
205.0.115.1     201.0.111.5     QM_IDLE           1001 ACTIVE
```

```
CoreRT-2#show crypto isakmp key
Keyring      Hostname/Address                          Preshared Key

default      205.0.115.1                               Tunnelkey
             203.0.113.2                               Tunnelkey
```

Inter-Branch Connectivity - Status



1
```
RT-A-1#trace 172.16.2.5
Type escape sequence to abort.
Tracing the route to 172.16.2.5
VRF info: (vrf in name/id, vrf out name/id)
  1 172.16.2.5 91 msec 24 msec 122 msec
```

2
```
RT-A-1#trace 205.0.115.1
Type escape sequence to abort.
Tracing the route to 205.0.115.1
VRF info: (vrf in name/id, vrf out name/id)
  1 203.0.113.1 [AS 65001] 45 msec 385 msec 144 msec
  2 210.0.110.1 [AS 65001] 191 msec 485 msec 778 msec
  3 205.0.115.1 [AS 65001] 686 msec 306 msec 429 msec
```

```
RT-A-1#trace 201.0.111.5
Type escape sequence to abort.
Tracing the route to 201.0.111.5
VRF info: (vrf in name/id, vrf out name/id)
  1 203.0.113.1 [AS 65001] 174 msec 178 msec 57 msec
  2 209.0.119.2 [AS 65001] 66 msec 176 msec 24 msec
  3 201.0.111.5 [AS 65001] 418 msec 450 msec 717 msec
```

3
```
Tracing the route to 172.16.1.6
VRF info: (vrf in name/id, vrf out name/id)
  1  *  *  *
```

4
```
RT-A-1#trace 192.168.100.17
Type escape sequence to abort.
Tracing the route to 192.168.100.17
VRF info: (vrf in name/id, vrf out name/id)
  1  *  *  *
  2
```

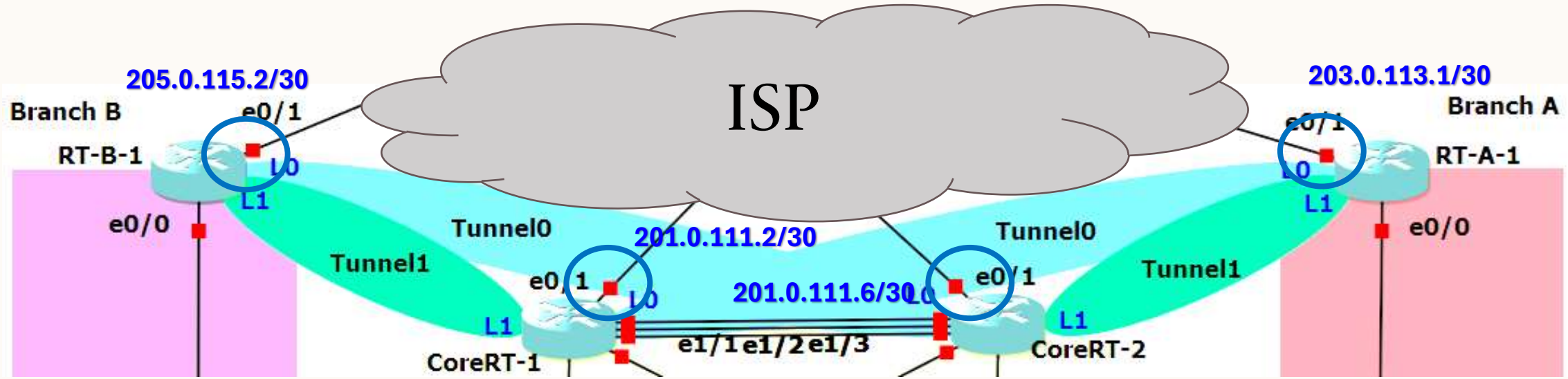
- Tunnel **encapsulation** is effective, masking the packet's trace along the underlay network.
- Motivation remains for **full** Inter-Branch Connectivity.

Configuration- Default Routes


```
RT-B-1(config-router)#ip route 0.0.0.0 0.0.0.0 205.0.115.2
RT-A-1(config-router)#ip route 0.0.0.0 0.0.0.0 203.0.113.1
CoreRT-1(config-router)#ip route 0.0.0.0 0.0.0.0 201.0.111.2
CoreRT-2(config-router)#ip route 0.0.0.0 0.0.0.0 201.0.111.6
```

A default route is needed for providing a way for routers to handle packets destined for networks **not explicitly listed** in their routing tables.

```
Gateway of last resort is 201.0.111.6 to network 0.0.0.0
```

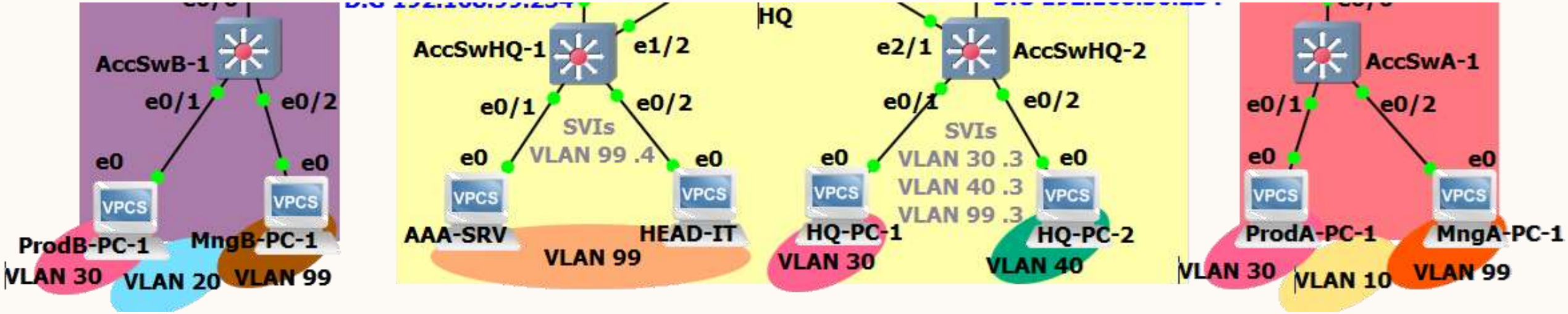


Configuration- Default Routes


```
AccWsA-1(config-router)#ip route 0.0.0.0 0.0.0.0 192.168.99.1
AccWsB-1(config-router)#ip route 0.0.0.0 0.0.0.0 192.168.99.1
AccWsHQ-1(config-router)#ip route 0.0.0.0 0.0.0.0 192.168.99.254
AccWsHQ-2(config-router)#ip route 0.0.0.0 0.0.0.0 192.168.30.254
```

```
Gateway of last resort is 192.168.99.1 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 192.168.99.1
```

```
Gateway of last resort is 192.168.99.254 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 192.168.99.254
```



Configuration- Single Area OSPF

RT-B-1

```
router ospf 1
router-id 4.4.4.4
network 192.168.20.0 0.0.0.255 area 0
network 192.168.30.0 0.0.0.255 area 0
network 192.168.99.0 0.0.0.255 area 0
network 172.16.1.4 0.0.0.3 area 0
network 172.16.2.0 0.0.0.3 area 0
```

CoreRT-1

```
router ospf 1
router-id 1.1.1.1
network 192.168.100.4 0.0.0.3 area 0
network 192.168.100.8 0.0.0.3 area 0
network 192.168.100.12 0.0.0.3 area 0
network 172.16.1.0 0.0.0.3 area 0
network 172.16.2.0 0.0.0.3 area 0
```

CoreRT-2

```
router ospf 1
router-id 2.2.2.2
network 192.168.100.0 0.0.0.3 area 0
network 192.168.100.8 0.0.0.3 area 0
network 192.168.100.16 0.0.0.3 area 0
network 172.16.1.4 0.0.0.3 area 0
network 172.16.2.4 0.0.0.3 area 0
```

RT-A-1

```
router ospf 1
router-id 3.3.3.3
network 192.168.10.0 0.0.0.255 area 0
network 192.168.30.0 0.0.0.255 area 0
network 192.168.99.0 0.0.0.255 area 0
network 172.16.1.0 0.0.0.3 area 0
network 172.16.2.4 0.0.0.3 area 0
```

```
CoreRT-1#show ip route | include ^C
Codes: L - local, C - connected, S - static, R - RIP, M - mobi
C        10.1.1.1 is directly connected, Loopback0
C        10.1.2.1 is directly connected, Loopback1
C        10.1.3.1 is directly connected, Loopback2
C        172.16.1.0/30 is directly connected, Tunnel0
C        172.16.2.0/30 is directly connected, Tunnel1
C        192.168.100.4/30 is directly connected, Ethernet1/0
C        192.168.100.8/30 is directly connected, Ethernet1/1
C        192.168.100.12/30 is directly connected, Ethernet0/0
C        201.0.111.0/30 is directly connected, Ethernet0/1
```

```
CoreRT-2#show ip route | include ^C
Codes: L - local, C - connected, S - static, R - RIP, M - mobi
C        10.1.1.2 is directly connected, Loopback0
C        10.1.2.2 is directly connected, Loopback1
C        10.1.3.2 is directly connected, Loopback2
C        172.16.1.4/30 is directly connected, Tunnel0
C        172.16.2.4/30 is directly connected, Tunnel1
C        192.168.100.0/30 is directly connected, Ethernet1/0
C        192.168.100.8/30 is directly connected, Ethernet1/1
C        192.168.100.16/30 is directly connected, Ethernet0/0
C        201.0.111.4/30 is directly connected, Ethernet0/1
```

```
RT-B-1#show ip route | include ^C
Codes: L - local, C - connected, S - static, R - RIP, M - mobile
C        10.3.1.1 is directly connected, Loopback0
C        10.3.2.1 is directly connected, Loopback1
C        10.3.3.1 is directly connected, Loopback2
C        172.16.1.4/30 is directly connected, Tunnel0
C        172.16.2.0/30 is directly connected, Tunnel1
C        192.168.1.0/24 is directly connected, Ethernet0/0
C        192.168.20.0/24 is directly connected, Ethernet0/0.20
C        192.168.30.0/24 is directly connected, Ethernet0/0.30
C        192.168.99.0/24 is directly connected, Ethernet0/0.99
C        205.0.115.0/30 is directly connected, Ethernet0/1
```

Underlay Networks are not to be published within the Overlay routing session, **for avoiding routing loops.**

```
RT-A-1#show ip route | include ^C
Codes: L - local, C - connected, S - static, R - RIP, M - mobi
C        10.2.1.1 is directly connected, Loopback0
C        10.2.2.1 is directly connected, Loopback1
C        10.2.3.1 is directly connected, Loopback2
C        172.16.1.0/30 is directly connected, Tunnel0
C        172.16.2.4/30 is directly connected, Tunnel1
C        192.168.1.0/24 is directly connected, Ethernet0/0
C        192.168.10.0/24 is directly connected, Ethernet0/0.10
C        192.168.30.0/24 is directly connected, Ethernet0/0.30
C        192.168.99.0/24 is directly connected, Ethernet0/0.99
C        203.0.113.0/30 is directly connected, Ethernet0/1
```

MLS Configuration- Single Area OSPF

DistSwHQ1

```
router ospf 1
router-id 5.5.5.5
network 192.168.40.0 0.0.0.255 area 0
network 192.168.30.0 0.0.0.255 area 0
network 192.168.99.0 0.0.0.255 area 0
network 192.168.100.0 0.0.0.3 area 0
network 192.168.100.12 0.0.0.3 area 0
```

```
DistSwHQ-1#show ip route | include ^C
Codes: L - local, C - connected, S - static, R - RIP, M - mobi
C        192.168.30.0/24 is directly connected, Vlan30
C        192.168.40.0/24 is directly connected, Vlan40
C        192.168.99.0/24 is directly connected, Vlan99
C        192.168.100.0/30 is directly connected, Ethernet1/0
C        192.168.100.12/30 is directly connected, Ethernet1/1
```

DistSwHQ2

```
router ospf 1
router-id 6.6.6.6
network 192.168.40.0 0.0.0.255 area 0
network 192.168.30.0 0.0.0.255 area 0
network 192.168.99.0 0.0.0.255 area 0
network 192.168.100.4 0.0.0.3 area 0
network 192.168.100.16 0.0.0.3 area 0
```

```
DistSwHQ-2#show ip route | include ^C
Codes: L - local, C - connected, S - static, R - RIP, M - mobi
C        192.168.30.0/24 is directly connected, Vlan30
C        192.168.40.0/24 is directly connected, Vlan40
C        192.168.99.0/24 is directly connected, Vlan99
C        192.168.100.4/30 is directly connected, Ethernet1/0
C        192.168.100.16/30 is directly connected, Ethernet1/1
```

Adjacency Bring-Up

```
CoreRT-1(config-router)#
*Aug  4 21:45:36.138: %OSPF-5-ADJCHG: Process 1, Nbr 4.4.4.4 on Tunnel1 from LOADING to FULL, Loading Done
*Aug  4 21:45:36.545: %OSPF-5-ADJCHG: Process 1, Nbr 3.3.3.3 on Tunnel0 from LOADING to FULL, Loading Done
CoreRT-1(config-router)#
*Aug  4 21:46:24.236: %OSPF-5-ADJCHG: Process 1, Nbr 6.6.6.6 on Ethernet1/0 from LOADING to FULL, Loading Done
*Aug  4 21:46:24.900: %OSPF-5-ADJCHG: Process 1, Nbr 2.2.2.2 on Ethernet1/1 from LOADING to FULL, Loading Done
```

```
*Aug  4 21:45:46.326: %OSPF-5-ADJCHG: Process 1, Nbr 3.3.3.3 on Tunnel1 from LOADING to FULL, Loading Done
*Aug  4 21:45:46.326: %OSPF-5-ADJCHG: Process 1, Nbr 4.4.4.4 on Tunnel0 from LOADING to FULL, Loading Done
CoreRT-2(config-router)#
*Aug  4 21:46:24.932: %OSPF-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Ethernet1/1 from LOADING to FULL, Loading Done
CoreRT-2(config-router)#
*Aug  4 21:46:57.361: %OSPF-5-ADJCHG: Process 1, Nbr 5.5.5.5 on Ethernet1/0 from LOADING to FULL, Loading Done
```

```
*Aug  4 21:45:36.592: %OSPF-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Tunnel0 from LOADING to FULL, Loading Done
RT-A-1(config-router)#
*Aug  4 21:45:46.715: %OSPF-5-ADJCHG: Process 1, Nbr 2.2.2.2 on Tunnel1 from LOADING to FULL, Loading Done
```

```
*Aug  4 21:45:36.514: %OSPF-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Tunnel1 from LOADING to FULL, Loading Done
RT-B-1(config-router)#
*Aug  4 21:45:46.442: %OSPF-5-ADJCHG: Process 1, Nbr 2.2.2.2 on Tunnel0 from LOADING to FULL, Loading Done
```

Validation- Single Area OSPF


```
CoreRT-1#show ip ospf interface
Tunnel1 is up, line protocol is up
  Internet Address 172.16.2.1/30, Area 0, Attached via Network Statement
  Process ID 1, Router ID 1.1.1.1, Network Type POINT_TO_POINT, Cost: 25
  Topology-MTID    Cost    Disabled    Shutdown      Topology Name
        0           25        no          no            Base
  Transmit Delay is 1 sec, State POINT_TO_POINT
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:00
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 1/5/5, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 3
  Last flood scan time is 0 msec, maximum is 13 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 4.4.4.4
  Suppress hello for 0 neighbor(s)
Tunnel0 is up, line protocol is up
  Internet Address 172.16.1.1/30, Area 0, Attached via Network Statement
```

1-Hop from HQ to Branch B

```
CoreRT-1#show ip route ospf
      172.16.0.0/16 is variably subnetted, 6 subnets, 2 masks
O        172.16.1.4/30 [110/35] via 192.168.100.10, 00:06:04, Ethernet1/1
O        172.16.2.4/30 [110/35] via 192.168.100.10, 00:06:04, Ethernet1/1
O     192.168.10.0/24 [110/35] via 172.16.1.2, 00:07:03, Tunnel0
O     192.168.20.0/24 [110/35] via 172.16.2.2, 00:07:03, Tunnel1
O     192.168.30.0/24 [110/11] via 192.168.100.5, 00:06:14, Ethernet1/0
O     192.168.40.0/24 [110/11] via 192.168.100.5, 00:06:14, Ethernet1/0
O     192.168.99.0/24 [110/11] via 192.168.100.5, 00:06:14, Ethernet1/0
      192.168.100.0/24 is variably subnetted, 8 subnets, 2 masks
O        192.168.100.0/30 [110/20] via 192.168.100.10, 00:05:40, Ethernet1/1
O        192.168.100.16/30 [110/20] via 192.168.100.10, 00:06:04, Ethernet1/1
                           [110/20] via 192.168.100.5, 00:06:14, Ethernet1/0
```

2 Tunnels, same IF

```
CoreRT-1#how ip ospf database
         ^
% Invalid input detected at '^' marker.

CoreRT-1#show ip ospf database

            OSPF Router with ID (1.1.1.1) (Process ID 1)

                Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link count
1.1.1.1         1.1.1.1         667         0x80000004 0x004EBE 7
2.2.2.2         2.2.2.2         640         0x80000004 0x008276 7
3.3.3.3         3.3.3.3         710         0x80000003 0x001552 7
4.4.4.4         4.4.4.4         711         0x80000003 0x00173E 7
5.5.5.5         5.5.5.5         621         0x80000006 0x008ADE 5
6.6.6.6         6.6.6.6         617         0x80000007 0x00D17E 5
```

All OSPF neighbors

Validation- Single Area OSPF


```
CoreRT-1#show ip route | exc ^L
      172.16.0.0/16 is variably subnetted, 6 subnets, 2 masks
C        172.16.1.0/30 is directly connected, Tunnel0
O        172.16.1.4/30 [110/35] via 192.168.100.10, 00:24:17, Ethernet1/1
C        172.16.2.0/30 is directly connected, Tunnel1
O        172.16.2.4/30 [110/35] via 192.168.100.10, 00:24:17, Ethernet1/1
O     192.168.10.0/24 [110/35] via 172.16.1.2, 00:25:16, Tunnel0
O     192.168.20.0/24 [110/35] via 172.16.2.2, 00:25:16, Tunnel1
O     192.168.30.0/24 [110/11] via 192.168.100.5, 00:24:27, Ethernet1/0
O     192.168.40.0/24 [110/11] via 192.168.100.5, 00:24:27, Ethernet1/0
O     192.168.99.0/24 [110/11] via 192.168.100.5, 00:24:27, Ethernet1/0
      192.168.100.0/24 is variably subnetted, 8 subnets, 2 masks
O        192.168.100.0/30 [110/20] via 192.168.100.10, 00:23:53, Ethernet1/1
C        192.168.100.4/30 is directly connected, Ethernet1/0
C        192.168.100.8/30 is directly connected, Ethernet1/1
C        192.168.100.12/30 is directly connected, Ethernet0/0
O        192.168.100.16/30 [110/20] via 192.168.100.10, 00:24:17, Ethernet1/1
                           [110/20] via 192.168.100.5, 00:24:27, Ethernet1/0
      201.0.111.0/24 is variably subnetted, 3 subnets, 2 masks
C        201.0.111.0/30 is directly connected, Ethernet0/1
B        201.0.111.4/30 [20/0] via 201.0.111.2, 01:27:24
     203.0.113.0/30 is subnetted, 1 subnets
B       203.0.113.0 [20/0] via 201.0.111.2, 01:27:24
     205.0.115.0/30 is subnetted, 1 subnets
B       205.0.115.0 [20/0] via 201.0.111.2, 01:27:24
     207.0.117.0/30 is subnetted, 1 subnets
B       207.0.117.0 [20/0] via 201.0.111.2, 01:27:24
     209.0.119.0/30 is subnetted, 1 subnets
B       209.0.119.0 [20/0] via 201.0.111.2, 01:27:24
     210.0.110.0/30 is subnetted, 1 subnets
B       210.0.110.0 [20/0] via 201.0.111.2, 01:27:24
```

Overlay

Underlay

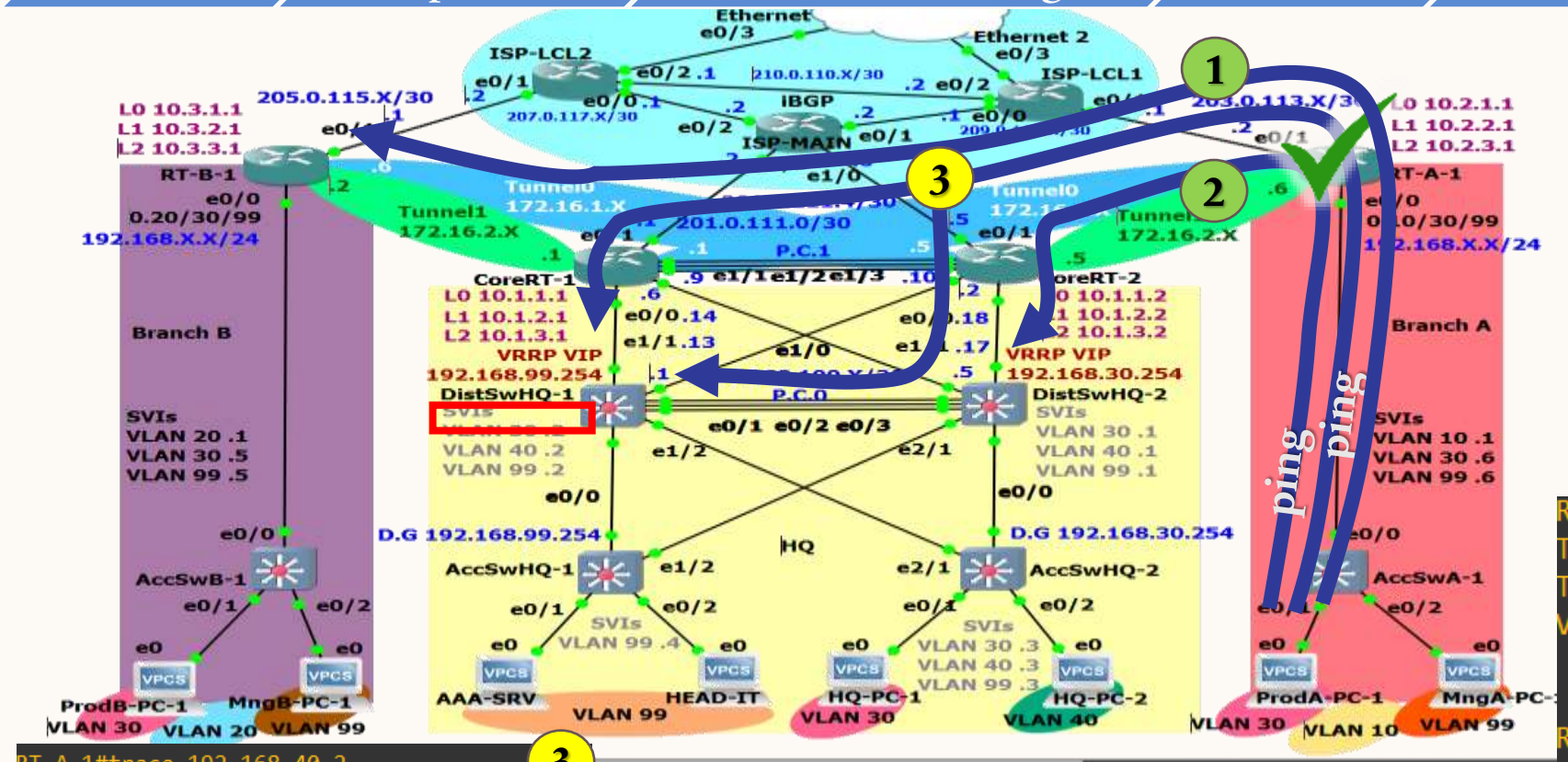
2 Tunnels are directly connected, 2 more are available through the standby router.

Networks .10 & .20 are external to HQ, and are available by 2 different tunnels.

HQ inter network, ECMP is supported due to full mesh connection.

ISP's routes learned through BGP.

Inter-Branch Connectivity - Status



Before OSPF

1

```
Tracing the route to 172.16.1.6
VRF info: (vrf in name/id, vrf out name/id)
  1  *  *  *
```

2

```
RT-A-1#trace 192.168.100.17
Type escape sequence to abort.
Tracing the route to 192.168.100.17
VRF info: (vrf in name/id, vrf out name/id)
  1  *  *  *
  2
```

After OSPF

1

```
RT-A-1#trace 192.168.100.17
Type escape sequence to abort.
Tracing the route to 192.168.100.17
VRF info: (vrf in name/id, vrf out name/id)
  1 172.16.2.5 747 msec 428 msec 790 msec
  2 192.168.100.17 451 msec 630 msec 583 msec
```

2

```
RT-A-1#trace 172.16.1.6
Type escape sequence to abort.
Tracing the route to 172.16.1.6
VRF info: (vrf in name/id, vrf out name/id)
  1 172.16.2.5 719 msec 223 msec 763 msec
  2 172.16.1.6 234 msec 536 msec 756 msec
```

3

```
RT-A-1#trace 192.168.40.2
Type escape sequence to abort.
Tracing the route to 192.168.40.2
VRF info: (vrf in name/id, vrf out name/id)
  1 172.16.1.1 816 msec
    172.16.2.5 1137 msec
    172.16.1.1 130 msec
  2 192.168.100.1 379 msec
    192.168.100.5 30 msec
    192.168.100.1 177 msec
```

3- Trace shows that ICMP packets use both ECMP routes

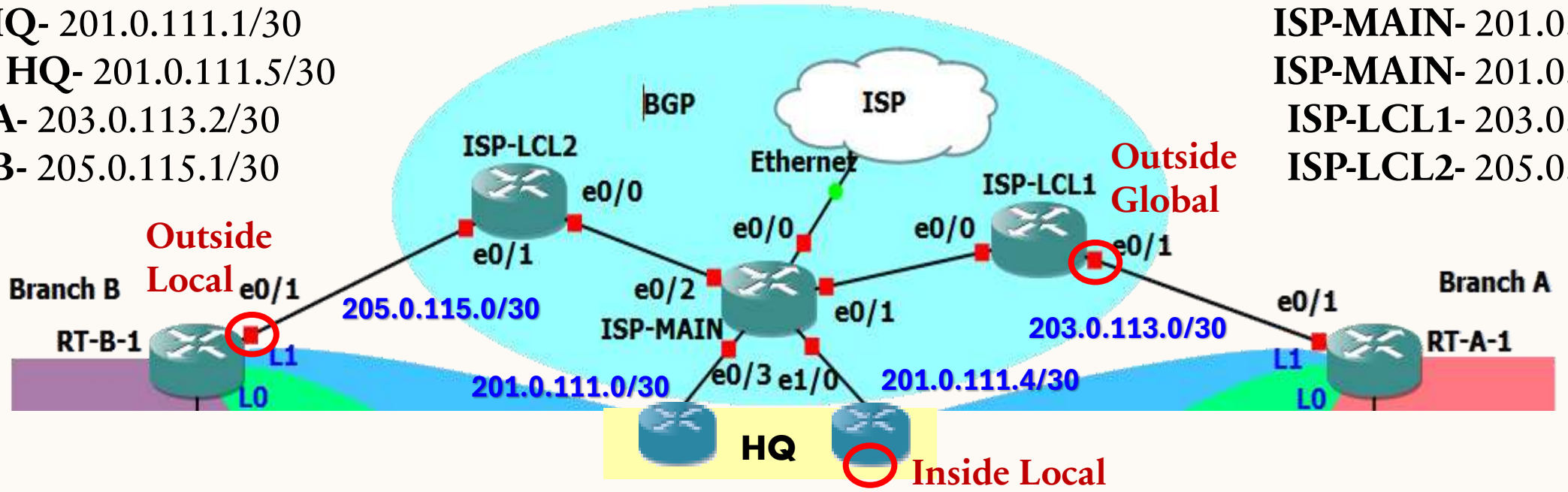
```
CoreRT-1#show ip route | exc ^L
O        192.168.100.16/30 [110/20] via 192.168.100.10, 00:24:17, Ethernet1/1
                           [110/20] via 192.168.100.5,  00:24:27, Ethernet1/0
```

NAT Implementation

NAT (Network Address Translation) translates between the enterprise's internal **private** IP addresses and the **public** IP addresses provided by your ISP, effectively acting as **a basic firewall** by only allowing return traffic from established connections and blocking unsolicited inbound traffic

Outside-Local IPv4 Allocation:
Active HQ- 201.0.111.1/30
Standby HQ- 201.0.111.5/30
Branch A- 203.0.113.2/30
Branch B- 205.0.115.1/30

Outside-Global IPv4 Allocation:
ISP-MAIN- 201.0.111.2/30
ISP-MAIN- 201.0.111.6/30
ISP-LCL1- 203.0.113.1/30
ISP-LCL2- 205.0.115.2/30



NAT for overlapping IP address ranges

- Our enterprise project implements GRE over IPsec VPN, so typically **NAT is Not Required, as a VPN Tunnel carry traffic securely** across an untrusted network.
- However, all branches are using an **overlapping** address range **192.168**.X.X/ 24.
- In that case NAT can be used to translate addresses to ensure unique addressing on both ends of the tunnel.
- NAT may be applied before packets enter the GRE tunnel if there is a need to translate internal addresses to public or different internal addresses
- Similarly, NAT might be used after decapsulation (i.e., when packets exit the VPN tunnel) if they need to be translated to fit the address space of the destination network.

Configuration- HQ NAT

CoreRT-1

```
! Inside locals allowed to be translated:
access-list 1 permit 192.168.0.0 0.0.255.255

! Define NAT Pool- Outside local
ip nat pool ISP_POOL_HQ1 201.0.111.1 201.0.111.1 netmask 255.255.255.252

! Configure NAT
ip nat inside source list 1 pool ISP_POOL_HQ1

! Configure Interfaces
interface range e0/0, e1/0-1
ip nat inside
interface e0/1
ip nat outside
```

CoreRT-2

```
! Inside locals allowed to be translated:
access-list 1 permit 192.168.0.0 0.0.255.255

! Define NAT Pool- Outside local
ip nat pool PUBLIC_POOL_HQ2 203.0.113.3 203.0.113.4 netmask 255.255.255.252

! Configure NAT
ip nat inside source list 1 pool ISP_POOL_HQ2

! Configure Interfaces
interface range e0/0, e1/0-1
ip nat inside
interface e0/1
ip nat outside
```

Configuration- Sec. Branches NAT

RT-A-1

```
! Inside locals allowed to be translated:
access-list 1 permit 192.168.0.0 0.0.255.255

! Define NAT Pool- Outside local
ip nat pool ISP_POOL_A1 203.0.113.2 203.0.113.2 netmask 255.255.255.252

! Configure NAT
ip nat inside source list 1 pool ISP_POOL_A1

! Configure Interfaces
interface range e0/0.99, e0/0.30, e0/0.10
ip nat inside
interface e0/1
ip nat outside
```

RT-B-1

```
! Inside locals allowed to be translated:
access-list 1 permit 192.168.0.0 0.0.255.255

! Define NAT Pool- Outside local
ip nat pool ISP_POOL_B1 205.0.115.1 205.0.115.1 netmask 255.255.255.252

! Configure NAT
ip nat inside source list 1 pool ISP_POOL_B1

! Configure Interfaces
interface range e0/0.99, e0/0.30, e0/0.10
ip nat inside
interface e0/1
ip nat outside
```

SECURITY

Basic Configurations & Hardening

Overall, the topology consists of (Up-Down):

1. 4 Routers (2 Core, 2 Branch).
2. 6 MLSs (4 CAMPUS, 2 Branch).
3. 8 Edge PCs (Representing ~200 PCs across 5 VLANs).

Although each have unique roles, all share basic resemblance with regards to **configurability & venerability potentials.**

The following setup was **initially duplicated** across whole hardware at startup (Router / L3-Switch, respectfully).

Basic Configurations & Hardening

- Set **Hostname.**
- Configure **Domain** Name as a requirement for SSH channel.
- Assign IP Address to the **SVI** / **Default Gateway** functionality respectively.
- Configure **Console** Line: Set Password and Enable Login
- Configure **VTY** Lines: Set Password, Enable Login, and **Restrict** to SSH only.

MLS VS. ROUTER

```
hostname AccessSwitch#
ip domain-name example.com

interface vlan 1
 ip address 192.168.1.10 255.255.255.0
 no shutdown
exit
ip default-gateway 192.168.1.1

line con 0
 password ConsolePassword
 login
exit

line vty 0 4
 password VTYPassword
 login
 transport input ssh
exit
```

```
hostname BranchRouter#
ip domain-name example.com

interface e0/0
 ip address 192.168.1.1 255.255.255.0
 no shutdown

ip default-gateway 192.168.1.254

line con 0
 password ConsolePassword
 login
exit

line vty 0 4
 password VTYPassword
 login
 transport input ssh
exit
```

Basic Configurations & Hardening

- Enable Encryption for SSH
- Create User Admin with elevated privilege
- **Apply L2 Hardening** Vs **L3 Access Control**:
  - Shutdown Ports
  - Set Switchport Mode- Access
  - Enable Port Security
  - Limit to 2 MAC Addresses
  - Restrict on Security Violation
  - Set Aging Time to 2 Minutes
  - Use Absolute Aging Type

- Configure Logging, Buffer size, Severity level.
- Disable Cisco Discovery Protocol
- Encrypt Stored Passwords & Alert unauthorized personnel.
- Store Configuration.

MLS VS. ROUTER

```
crypto key generate rsa
ip ssh version 2
username admin privilege 15 secret AdminPassword
interface range e0/0-3,e1/0-3,e2/0-3,e3/0-3
 shutdown
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security violation restrict
 switchport port-security aging time 2
 switchport port-security aging type absolute

logging buffered 4096
logging console debugging
no cdp run
service password-encryption
banner motd # Authorized Access Only!
write memory
```

```
crypto key generate rsa
ip ssh version 2
username admin privilege 15 secret AdminPassword
access-list 100 permit ip 192.168.1.0 0.0.0.255 any
interface e0/0
 ip access-group 100 in

logging buffered 4096
logging console debugging
no cdp run
service password-encryption
banner motd # Authorized Access Only!
Write memory
```

Template for L3 Access control

Validation - Basic Setup & L2 security


```
AccSwHQ-1#show port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
                 (Count)      (Count)         (Count)
---------------------------------------------------------------------------
      Et0/0            2            0                 0         Restrict
      Et0/1            2            0                 0         Restrict
      Et0/2            2            0                 0         Restrict
      Et0/3            2            0                 0         Restrict
      Et1/0            2            0                 0         Restrict
      Et1/1            2            0                 0         Restrict
      Et1/2            2            0                 0         Restrict
      Et1/3            2            0                 0         Restrict
      Et2/0            2            0                 0         Restrict
      Et2/1            2            0                 0         Restrict
      Et2/2            2            0                 0         Restrict
      Et2/3            2            0                 0         Restrict
      Et3/0            2            0                 0         Restrict
      Et3/1            2            0                 0         Restrict
      Et3/2            2            0                 0         Restrict
      Et3/3            2            0                 0         Restrict
---------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 4096
```

```
 Authorized Access Only!

User Access Verification

Password:
% Password:  timeout expired!
Password:
AccSwHQ-1#
```

```
AccSwHQ-1#show startup-conf
line con 0
 exec-timeout 0 0
 privilege level 15
 password 7 0625002F5F41051C351601181B0B382F
 logging synchronous
 login
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 password 7 0032273F345A1815182E5E4A
```

Spanning-Tree Security

DistSwHQ-1

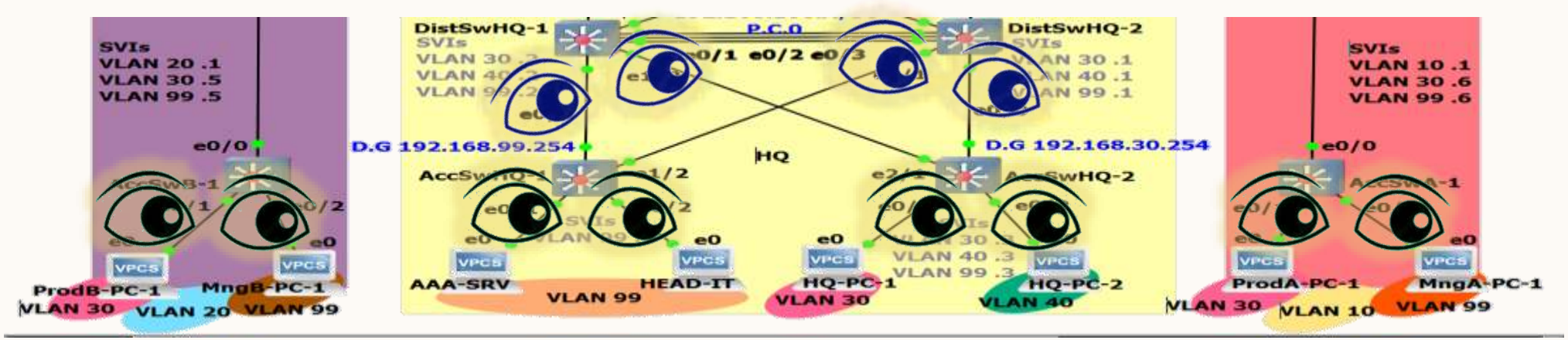
```
! Prevent potential Shadow-IT-Root
interface range E0/0, E1/2
spanning-tree guard root
```

DistSwHQ-2

```
! Prevent potential Shadow-IT-Root
interface range E0/0, E2/1
spanning-tree guard root
```

Access Switch (Downlinks)

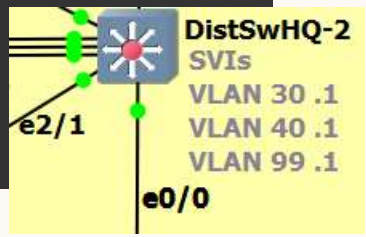
```
! Configure PortFast on all access ports
interface range E0/1 - 2
spanning-tree portfast
spanning-tree bpduguard enable
```



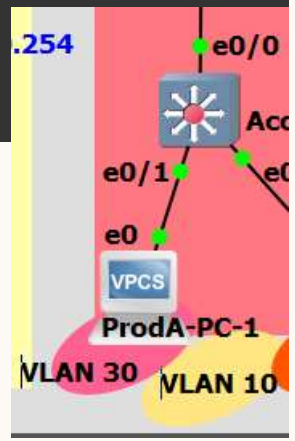
- **PortFast** speeds up the transition of a port from a blocking state to a forwarding state, useful in preventing delays in network connectivity.
- **BPDU Guard** disables a port if it receives BPDUs, which helps protect against potential STP attacks.
- **Root Guard** ensures that a port does not become a root port if it receives superior BPDUs, which maintains the intended root bridge.

Validation - Spanning-Tree Security


```
DistSwHQ-2#show spanning-tree detail
 Port 1 (Ethernet0/0) of VLAN0030 is designated forwarding
   Port path cost 100, Port priority 128, Port Identifier 128.1.
   Designated root has priority 4126, address aabb.cc00.0400
   Designated bridge has priority 4126, address aabb.cc00.0400
   Designated port id is 128.1, designated path cost 0
   Timers: message age 0, forward delay 0, hold 0
   Number of transitions to forwarding state: 1
   Link type is point-to-point by default
   Root guard is enabled on the port
   BPDU: sent 46876, received 136122

 Port 10 (Ethernet2/1) of VLAN0030 is designated forwarding
   Port path cost 100, Port priority 128, Port Identifier 128.10
   Designated root has priority 4126, address aabb.cc00.0400
   Designated bridge has priority 4126, address aabb.cc00.0400
   Designated port id is 128.10, designated path cost 0
   Timers: message age 0, forward delay 0, hold 0
   Number of transitions to forwarding state: 1
   Link type is point-to-point by default
   Root guard is enabled on the port
   BPDU: sent 182990, received 0
```




```
AccSwA-1# show spanning-tree int e0/1 detail
 Port 2 (Ethernet0/1) of VLAN0030 is designated forwarding
   Port path cost 100, Port priority 128, Port Identifier 128.2.
   Designated root has priority 32798, address aabb.cc00.0800
   Designated bridge has priority 32798, address aabb.cc00.0800
   Designated port id is 128.2, designated path cost 0
   Timers: message age 0, forward delay 0, hold 0
   Number of transitions to forwarding state: 1
   The port is in the portfast edge mode
   Link type is point-to-point by default
   Bpdu guard is enabled
   BPDU: sent 183573, received 0
```



DHCP Security

DHCP Snooping helps to prevent **unauthorized** DHCP servers from providing IP addresses and configuring clients. It maintains a table of trusted DHCP servers and valid DHCP lease bindings.
It enforce a **rate** at which DHCP messages are processed.

DistSwHQ-1

```
ip dhcp snooping
ip dhcp snooping vlan 99
interface range E0/0, E1/2
ip dhcp snooping trust
interface range E0/1-2
ip dhcp snooping limit rate 15
```

DistSwHQ-2

```
ip dhcp snooping
ip dhcp snooping vlan 30,40
interface range E0/0, E2/1
ip dhcp snooping trust
interface range E0/1-2
ip dhcp snooping limit rate 15
```

AccSwA-1

```
ip dhcp snooping
ip dhcp snooping vlan 10,30,99
interface E0/0
ip dhcp snooping trust
interface range E0/1-2
ip dhcp snooping limit rate 15
```

AccSwHQ-1

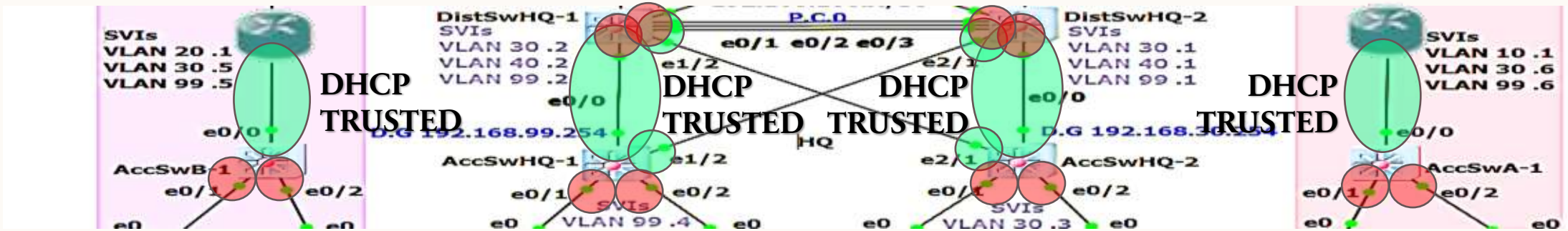
```
ip dhcp snooping
ip dhcp snooping vlan 99
interface range E0/0, E1/2
ip dhcp snooping trust
interface range E0/1-2
ip dhcp snooping limit rate 15
```

AccSwHQ-2

```
ip dhcp snooping
ip dhcp snooping vlan 30,40
interface range E0/0, E2/1
ip dhcp snooping trust
interface range E0/1-2
ip dhcp snooping limit rate 15
```

AccSwB-1

```
ip dhcp snooping
ip dhcp snooping vlan 20,30,99
interface E0/0
ip dhcp snooping trust
interface range E0/1-2
ip dhcp snooping limit rate 15
```



Validation - DHCP Security


```
AccSwB-1#show ip dhcp snooping
Switch DHCP snooping is enabled
Switch DHCP gleaning is disabled
DHCP snooping is configured on following VLANs:
20,30,99
DHCP snooping is operational on following VLANs:
20,30,99
DHCP snooping is configured on the following L3 Interfaces:

Insertion of option 82 is enabled
   circuit-id default format: vlan-mod-port
   remote-id: aabb.cc00.0900 (MAC)
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Verification of giaddr field is enabled
DHCP snooping trust/rate is configured on the following Interfaces:

Interface                  Trusted    Allow option    Rate limit (pps)
-----------------------    -------    ------------    ----------------
Ethernet0/0                yes        yes             unlimited
  Custom circuit-ids:
Ethernet0/1                no         no              15
  Custom circuit-ids:
Ethernet0/2                no         no              15
```

ARP Security

ARP Snooping prevents ARP spoofing attacks by maintaining a table of IP-to-MAC address mappings based on ARP traffic. **Dynamic ARP Inspection** (**DAI**) uses the DHCP snooping binding table to ensure that only valid ARP requests and responses are relayed & within allowed **rate**.

DistSwHQ-1

```
ip arp inspection vlan 99
interface range E0/0, E1/2
ip arp inspection limit rate 100
```

DistSwHQ-2

```
ip arp inspection vlan 30,40
interface range E0/0, E2/1
ip arp inspection limit rate 100
```

AccSwA-1

```
ip arp inspection vlan 10,30,99
interface range E0/1-2
ip arp inspection limit rate 100
```

AccSwHQ-1

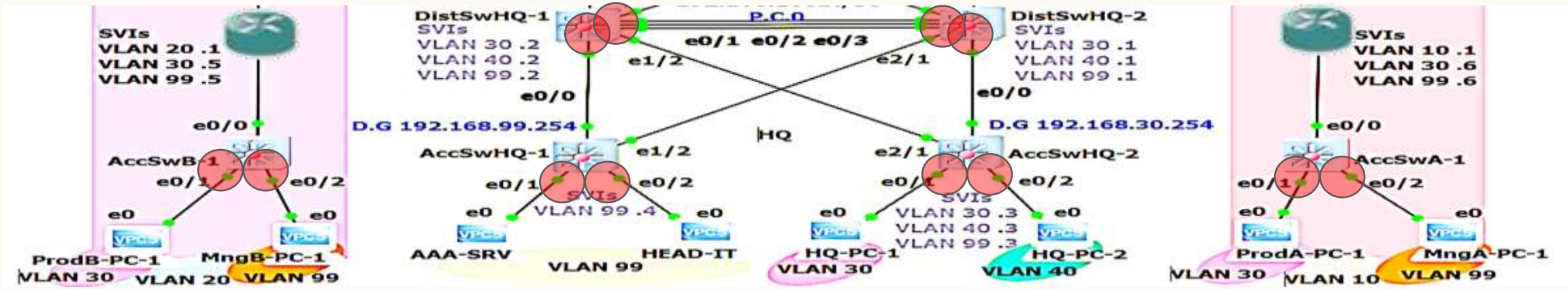
```
ip arp inspection vlan 99
interface range E0/1-2
ip arp inspection limit rate 100
```

AccSwHQ-2

```
ip arp inspection vlan 30,40
interface range E0/1-2
ip arp inspection limit rate 100
```

AccSwB-1

```
ip arp inspection vlan 20,30,99
interface range E0/1-2
ip arp inspection limit rate 100
```



Validation - ARP Security


```
AccSwHQ-2#show ip arp inspection

Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled

 Vlan     Configuration    Operation   ACL Match          Static ACL
 ----     -------------    ---------   ---------          ----------
   30     Enabled          Active
   40     Enabled          Active

 Vlan     ACL Logging      DHCP Logging      Probe Logging
 ----     -----------      ------------      -------------
   30     Deny             Deny              Off
   40     Deny             Deny              Off

 Vlan      Forwarded        Dropped     DHCP Drops      ACL Drops
 ----      ---------        -------     ----------      ---------
   30              2              0              0              0
   40              2              0              0              0
```

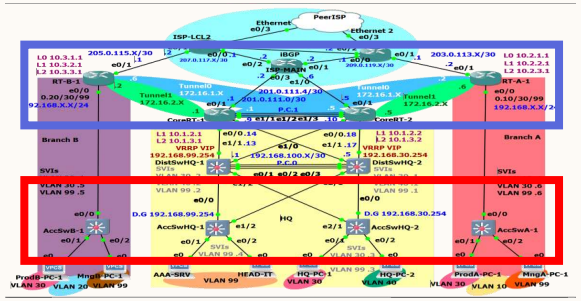
AUTOMATION

Automation Demonstration using Ansible

- Lastly, let us explore automation tasks for both L2 & L3 layers:
  1. Repeatable L2-Hardening configuration of the entire **Access-Layer** interfaces of the topology.
  2. IPv4 Address configuration for all **VPN Tunnels**.
- A common tool for this task is **Ansible-** which allows for consistent, repeatable & efficient configuration across multiple devices.

Inventory file for the Enterprise's Topology

```
# inventory.yml
all:
  vars:
    ansible_user: admin
    ansible_password: AdminPassword
    ansible_network_os: cisco.ios.ios
  children:
    HQ_branch:
      hosts:
        AccSwHQ-1:
          ansible_host: 192.168.99.4
        AccSwHQ-2:
          ansible_host: 192.168.99.3
        DistSwHQ-1:
          ansible_host: 192.168.99.2
        DistSwHQ-2:
          ansible_host: 192.168.99.1
        CoreRT-1:
          ansible_host: 201.0.111.1
        CoreRT-2:
          ansible_host: 201.0.111.5
    secondary_branch_A:
      hosts:
        RT-A-1:
          ansible_host: 203.0.113.2
        AccSwA-1:
          ansible_host: 192.168.99.6
    secondary_branch_B:
      hosts:
        RT-B-1:
          ansible_host: 205.0.115.1
        AccSwB-1:
          ansible_host: 192.168.99.5
```



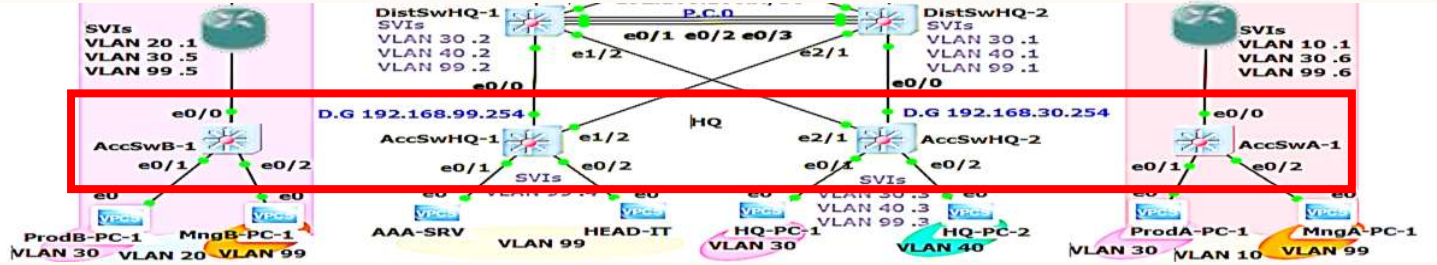
- '**inventory.yml**' is based on the enterprise's network topology, it defines the 'inventory' of hosts at all branches intended to be configured, organizing them in native groups.
- '**vars**' defines credentials of SSH connection shared by all devices.
- '**ansible_host**' is the management SVI defined initially.

Ansible Playbook file for L2

```
# configure_access_ifs.yml
---
- name: Configure access layer switches
  hosts:
    - AccSwHQ-1
    - AccSwHQ-2
    - AccSwB-1
    - AccSwA-1
  gather_facts: no
  tasks:
    - name: Configure portfast, BPDU guard, and sticky MACs on e0/1 and e0/2
      cisco.ios.ios_interface:
        name: "{{ item.interface }}"
        access_vlan: "{{ item.vlan }}"
        spanning_tree_portfast: true
        spanning_tree_bpduguard_enable: true
        switchport_mode: access
        mac_address_table: "{{ item.mac_table }}"
      loop:
        - { interface: "Ethernet0/1", vlan: 30, mac_table: "sticky" }
        - { interface: "Ethernet0/2", vlan: 99, mac_table: "sticky" }
      vars:
        ansible_network_os: cisco.ios.ios
```

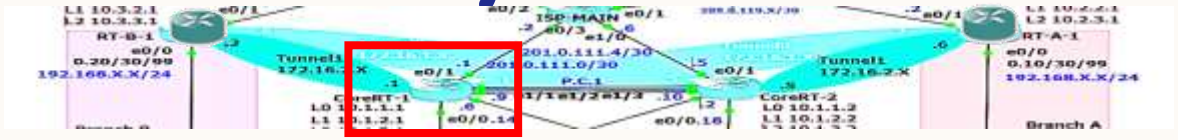
Strictly Access Layer devices selected

Loopin through all of the devices, applying L2 settings



- **'configure_access_ifs.yml'** uses cisco.ios.ios_interface module- a component of Ansible's collection for managing Cisco IOS devices.
- It is used here to configure spanning-tree settings such as portfast & bpduguard.

Ansible Playbook file for L3



 # configure_vpn_ifs.yml

```
---
- name: Configure VPN Tunnels
  hosts: all
  gather_facts: no
  tasks:
```

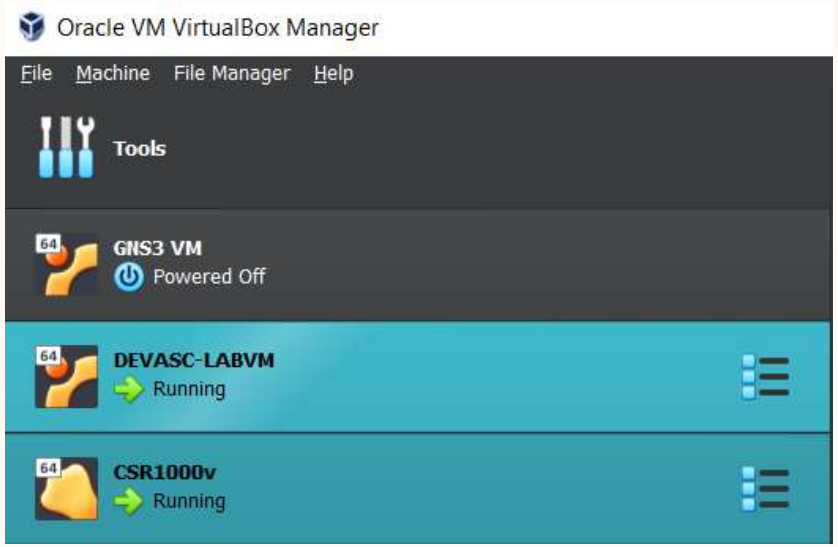
```
  - name: Configure Tunnel 0 on Branch A
    cisco.ios.ios_interface:
      name: Tunnel0
      description: "Link to CoreRT-1, E0/1"
      ipv4:
        address: 172.16.1.2
        mask: 255.255.255.252
      tunnel_source: E0/1
      tunnel_destination: 201.0.111.1
      state: present
    when: inventory_hostname == 'RT-A-1'

  - name: Configure Tunnel 1 on Branch A
    cisco.ios.ios_interface:
      name: Tunnel1
      description: "Link to CoreRT-2, E0/1"
      ipv4:
        address: 172.16.2.6
        mask: 255.255.255.252
      tunnel_source: E0/1
      tunnel_destination: 201.0.111.5
      state: present
    when: inventory_hostname == 'RT-A-1'
```

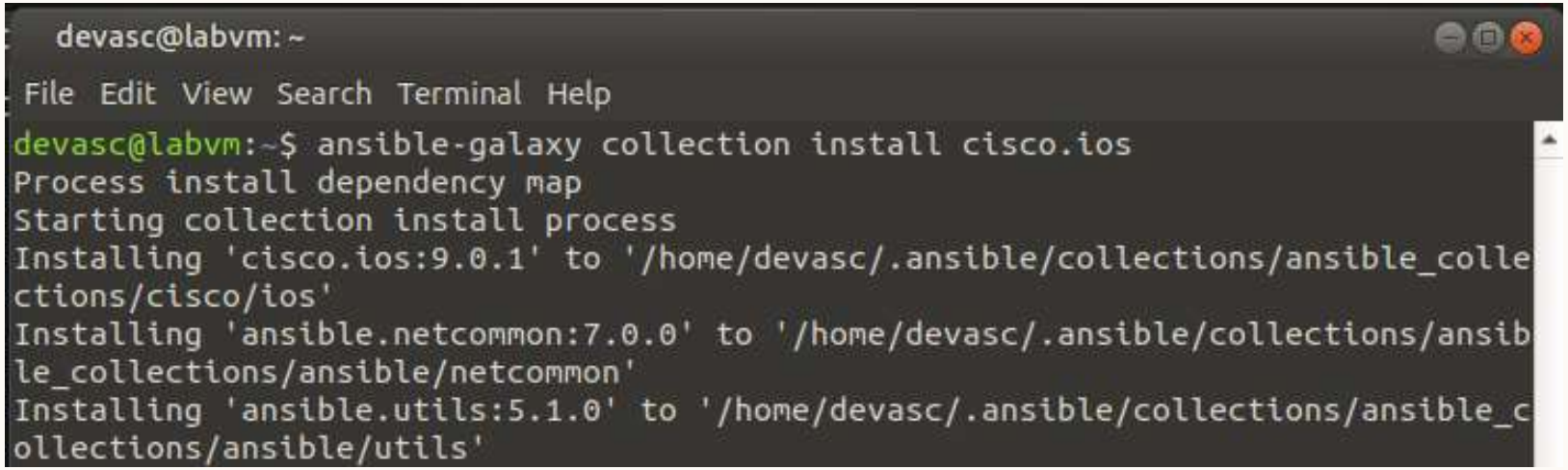
```
- name: Configure Tunnel 0 on Branch B
  cisco.ios.ios_interface:
    name: Tunnel0
    description: "Link to CoreRT-2, E0/1"
    ipv4:
      address: 172.16.1.6
      mask: 255.255.255.252
    tunnel_source: E0/1
    tunnel_destination: 201.0.111.5
    state: present
  when: inventory_hostname == 'RT-B-1'

- name: Configure Tunnel 1 on Branch B
  cisco.ios.ios_interface:
    name: Tunnel1
    description: "Link to CoreRT-1, E0/1"
    ipv4:
      address: 172.16.2.2
      mask: 255.255.255.252
    tunnel_source: E0/1
    tunnel_destination: 201.0.111.1
    state: present
  when: inventory_hostname == 'RT-B-1'
```

```
- name: Configure Tunnel 0 on HQ CoreRT-1
  cisco.ios.ios_interface:
    name: Tunnel0
    description: "to RT-A-1, E0/1"
    ipv4:
      address: 172.16.1.1
      mask: 255.255.255.252
    tunnel_source: Et0/1
    tunnel_destination: 203.0.113.2
    state: present
  when: inventory_hostname == 'CoreRT-1'

- name: Configure Tunnel 1 on HQ CoreRT-1
  cisco.ios.ios_interface:
    name: Tunnel1
    description: "to RT-B-1, E0/1"
    ipv4:
      address: 172.16.2.1
      mask: 255.255.255.252
    tunnel_source: Et0/1
    tunnel_destination: 205.0.115.1
    state: present
  when: inventory_hostname == 'CoreRT-1'
```

```
- name: Configure Tunnel 0 on HQ CoreRT-2
  cisco.ios.ios_interface:
    name: Tunnel0
    description: "to RT-B-1, E0/1"
    ipv4:
      address: 172.16.1.5
      mask: 255.255.255.252
    tunnel_source: Et0/1
    tunnel_destination: 205.0.115.1
    state: present
  when: inventory_hostname == 'CoreRT-2'

- name: Configure Tunnel 1 on HQ CoreRT-2
  cisco.ios.ios_interface:
    name: Tunnel1
    description: "to RT-A-1, E0/1"
    ipv4:
      address: 172.16.2.5
      mask: 255.255.255.252
    tunnel_source: Et0/1
    tunnel_destination: 203.0.113.2
    state: present
  when: inventory_hostname == 'CoreRT-2'
```

Environment Preperation





- Run Both a Linux dev. VM & Cisco's virtual router, both using NAT.
- Ensure that the cisco.ios collection is installed. You can install it using Ansible Galaxy:

Ansible Playbook Execution

```
devasc@labvm:~$ ansible-playbook -i inventory_file configure_vpn_ifs.yml

TASK [Configure Tunnel 1 on Branch A] ********************************
ok: [RT-A-1] => (item=None)

PLAY RECAP ***********************************************************************
RT-A-1      : ok=2    changed=0    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0
```

```
RT-A-1#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet1       10.0.2.15       YES DHCP   up                    up
Tunnel0                172.16.1.2      YES manual up                    up
Tunnel1                172.16.2.6      YES manual up                    up
```

```
RT-A-1#show ip route | include ^C
Codes: L - local, C - connected, S - static, R - RIP, M - mol
C        10.0.2.0/24 is directly connected, GigabitEthernet1
C        172.16.1.0/30 is directly connected, Tunnel0
C        172.16.2.4/30 is directly connected, Tunnel1
```

PROJECT SUMMARY

Project Summary

Objectives Completed:

- ✓ Design and implement an **enterprise** network based on **Cisco** infrastructure.
- ✓ Develop a **physical** (Campus, Branches) and **logical** (Hub&Spoke, VPN, VLANs) network topology.
- ✓ Focus on creating a **robust** & **scalable** topology for three branches.
- ✓ Ensure the network meets **security best practices** and **automation** requirements.
- ✓ Address specific design considerations including **subnetting**, **hardening**, and **routing** protocols.

Out-of-Scope Achievements:

- ✓ Design and implement an **ISP** network using BGP protocol.
- ✓ Considerable growth-freedom of 100% in edge-nodes, made possible by a Tier-3 Campus topology in the Main branch.

Project Files

- AccSwA-1_startup-config.cfg
- AccSwB-1_startup-config.cfg
- AccSwHQ-2_startup-config.cfg
- CoreRT-1_startup-config.cfg
- CoreRT-2_startup-config.cfg
- DistSwHQ-1_startup-config.cfg
- DistSwHQ-2_startup-config.cfg
- ISP-LCL1_startup-config.cfg
- ISP-LCL2_startup-config.cfg
- ISP-MAIN_startup-config.cfg
- MLS_base_config.txt
- RTA_base_config.txt
- RT-A-1_startup-config.cfg
- RT-B-1_startup-config.cfg

- Final_Project_Hub_and_Spoke_Enterprose-Presentation.pdf
- Final_Project_Hub_and_Spoke_Enterprose-Requirements.pdf
- Final_Project_Hub_and_Spoke_Enterprose-Topolgy.png

- CSR1000v_for_VirtualBox.ova
- DEVASC_VM_vbox.ova
- GNS3_VM_vbox.ova

- configure_access_ifs.yml
- configure_vpn_ifs.yml
- inventory.yml

- Hub_and_Spoke_Enterprise.gns3

- i86bi_linux_l2-adventerprisek9-ms.SSA.high_iron_20180510.bin
- i86bi_linux-adventerprisek9-ms.155-2.T.bin