Submitted to:
Manoj Tamang

Submitted by:
Nihangchha Rai

Abstract

This networking project covers the network design, routing protocols, and security measures within a three-tier architecture. The project begins with a design exploration, showcasing both logical and physical prototypes. Routing protocols, an essential part of network operation, are covered in detail, with special focus on Open Shortest Path First (**OSPF**), Routing Information Protocol (**RIP**), Enhanced Interior Gateway Routing Protocol (**EIGRP**), static routing, and Border Gateway Protocol (**BGP**). These protocols are implemented in a three-tier architecture and their features are explained. The project covers the access Layer, including Hot Standby Router Protocol (**HSRP**) for load balancing and redundancy, Spanning Tree Protocol (**STP**), PortFast, Virtual Local Area Network (**VLAN**) segregation, and EtherChannel. It provides a thorough explanation of Layer 2 (**L2**) security features such as Bridge Protocol Data Unit (BPDU) Guard, Port Security, Dynamic Host Configuration Protocol (**DHCP**) Snooping, Rate Limiting, and Dynamic Address Resolution Protocol (**ARP**) Inspection (**DAI**). The project covers Network Address Translation (**NAT**), Port Address Translation **(PAT)**, and Virtual Private Network (**VPN**) technologies, such as Internet Protocol Security (IPsec) and Generic Routing Encapsulation (**GRE**) over IPsec, with a thorough explanation of their verification processes for secure communication. Along with this, Firewalls, Network Time Protocol **(NTP)** servers, System Logging (Syslog) servers, Simple Network Management Protocol **(SNMP)**, Authentication, Authorization, and Accounting **(AAA)**, Domain Name System **(DNS)**, and Wireless LAN Controllers **(WLC)** were also implemented.

Furthermore, the project addresses modern networking trends like risk management, legal, social, and compliance issues. The impact of emerging trends and technologies on the conventional three-tier design is pointed out, with specific focus on Software Defined Networking **(SDN)**, Network Virtualization **(NV),** Cloud Computing, and Edge Computing.

Keywords

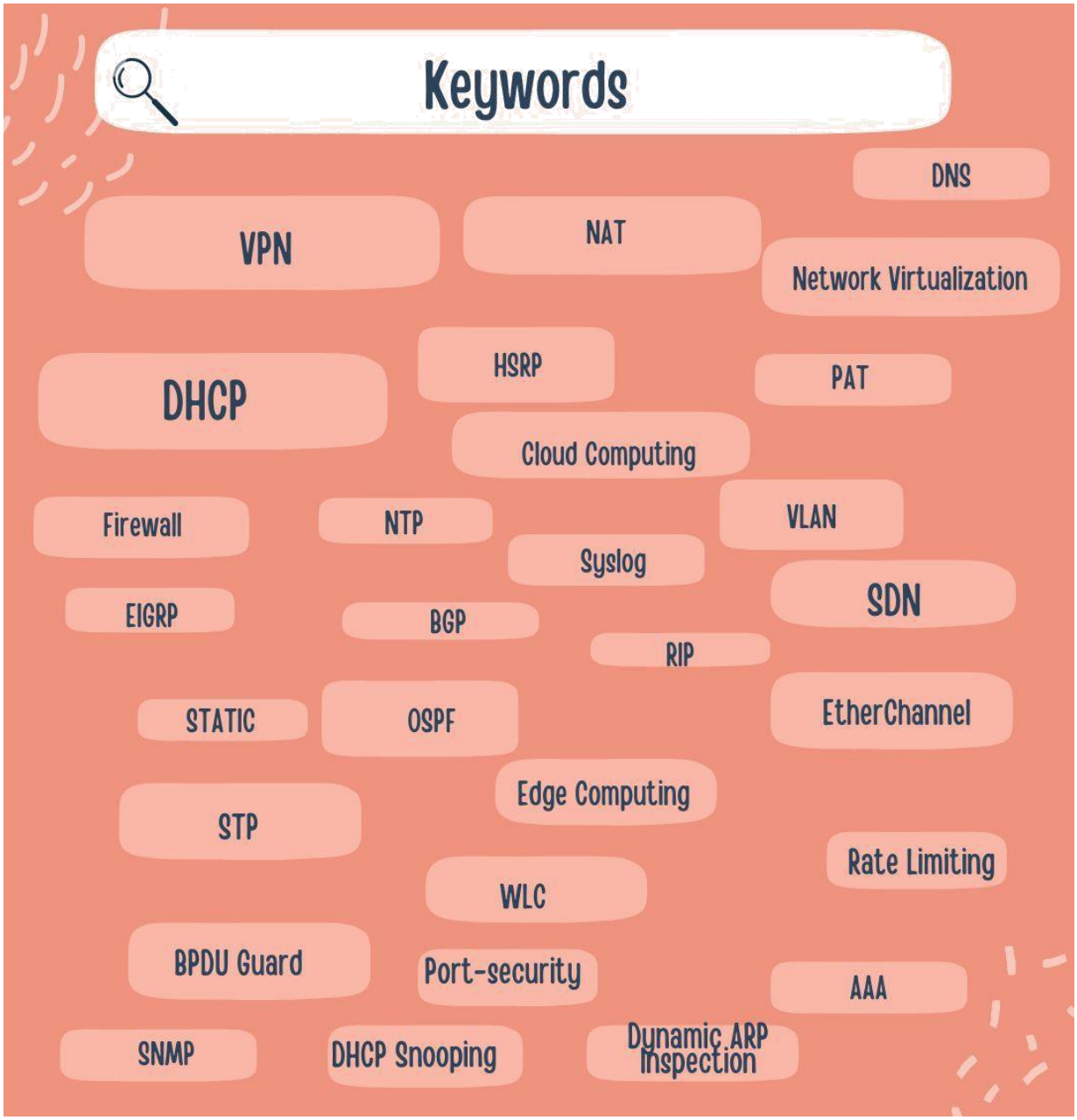


Figure 1: Keywords

Contents

Table of figure

Introduction

As a Network Engineer at NetworkHats, I have designed and implemented a robust network topology based on the traditional three-tier architecture, further enhanced with an edge layer to meet the specific scalability, performance, and security requirements of our client. The design was meticulously configured and tested using Cisco Packet Tracer and GNS3, ensuring accurate simulation and alignment with real-world deployment scenarios. The architecture includes the core layer for high-speed backbone connectivity, the distribution layer for routing and policy control, the access layer for end-device connectivity, and the edge layer for secure internet and external network access.

Objective

The objective of this project is to design, implement, and simulate a scalable, secure, and efficient enterprise network using a **traditional three-tier architecture** enhanced with an **edge layer**, tailored to meet the specific operational and security requirements of the client. The project aims to:

- Develop a comprehensive network design, including both logical and physical topologies, that ensures high availability, redundancy, and performance.
- Implement and evaluate various routing protocols—including OSPF, RIP, EIGRP, STATIC, and BGP—to determine the most suitable solutions for dynamic and static routing needs.
- Integrate advanced Layer 2 security mechanisms such as DHCP Snooping, Port Security, BPDU Guard, Rate Limiting, and Dynamic ARP Inspection to safeguard against common network threats.
- Configure network services including NAT, PAT, VPN (IPsec, GRE over IPsec), NTP, Syslog, SNMP, AAA, DNS, and WLC, to support secure and manageable communication across the network.
- Demonstrate load balancing and failover capabilities using HSRP, STP, PortFast, VLANs, and EtherChannel for resilient and segmented network operations.
- Explore and assess the impact of emerging technologies such as Software Defined Networking (SDN), Network Virtualization (NV), Cloud Computing, and Edge Computing on traditional network design.
- Address risk management, legal, social, and compliance issues, ensuring that the network design aligns with industry standards and best practices.
- Utilize Cisco Packet Tracer and GNS3 for accurate simulation, testing, and verification of network performance and security measures before real-world deployment.

Network Design

Logical Prototype

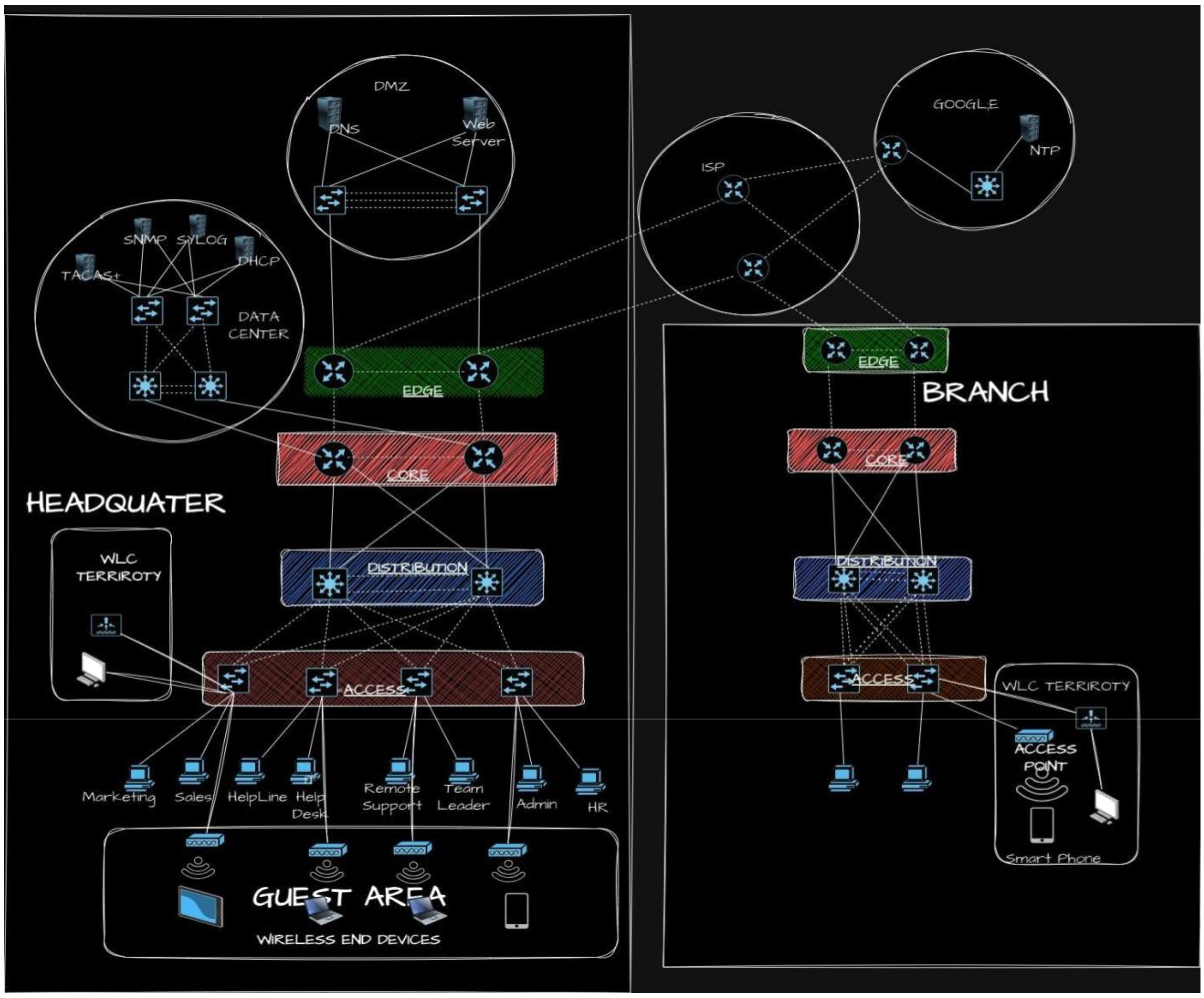


Figure 2: Logical Network prototype designed on draw.io

The logical prototype of this networking project shows the structured flow and interconnection of network components within a traditional three-tier architecture enhanced by an edge layer. It defines the functional design, including IP addressing, VLAN segmentation, and routing domains, without delving into physical device placement.

Physical Prototype

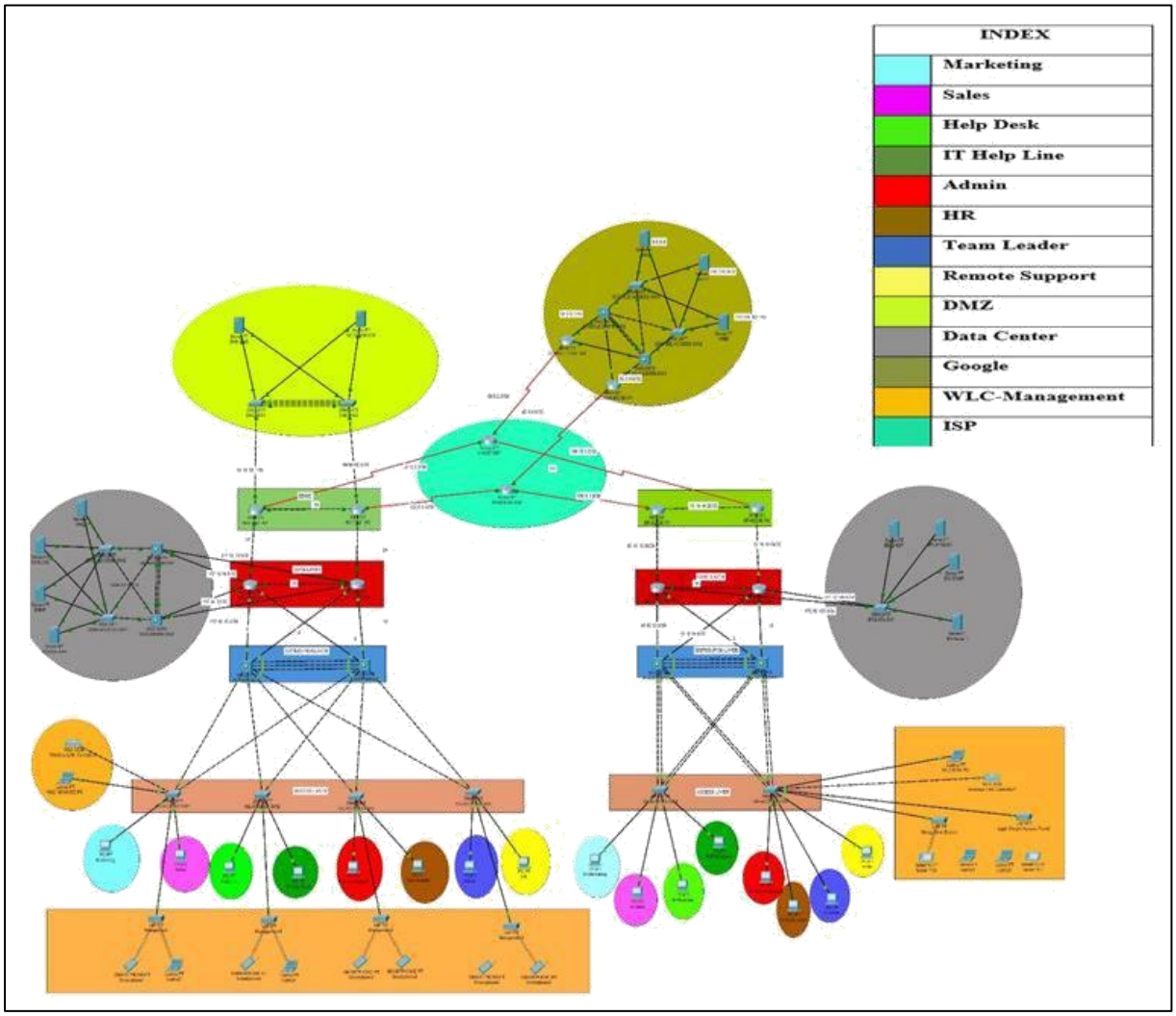


Figure 3: Physical Prototype of three-tier architecture with different LANs and WAN

It represents the actual layout and interconnection of network devices, showcasing the real-world implementation of the designed topology using Cisco routers, switches, firewalls, wireless access points, and end devices. It details how components are physically arranged, connected via Ethernet cables or fiber optics, and powered, ensuring optimal device placement, cable management, and accessibility for maintenance. The prototype includes Layer 3 switches at the distribution layer, core switches or routers at the core layer, and access switches at the access layer, with end devices like PCs, IP phones, and printers connected accordingly. Edge devices such as firewalls, VPN gateways, and internet routers are positioned at network boundaries for secure external connectivity. Moreover, servers for DHCP, DNS, NTP, Syslog, and AAA are centrally located for efficient service delivery, while Wireless LAN Controllers (WLC) manage access points to provide wireless connectivity. The physical setup, modeled and tested in Cisco Packet Tracer and GNS3, validates the logical design's feasibility and ensures network performance, reliability, and scalability in a real-world scenario.

ROUTING PROTOCOL

Various types of routing protocols such as, OSPF, static, BGP are implemented in this network topology based on the specific situation. There are multiple factors should be considered while choosing a routing protocol between three-tier architecture are as follows:

- **Network Size and Complexity**: This factor impacts the scalability and complexity of routing protocol. For a simple network we may manually configure the static routing for each fixed destination. But taking about the large network static routing is not efficient. So, in this kind of situation dynamic routing like EIGRP, OSPF, RIP, and BGP comes in handy because it can automatically learn the other neighbor routing table and find the best path based on the criteria.
- **Performance and Efficiency:** This aspect in the network topology is directly depend upon the speed, bandwidth, and load of the network. Various routing protocols have different impacts on this aspect. For example, RIP works on mechanism of distance vector protocol are easy and faster to converge but in exchange they consume high bandwidth for updates and may create a routing loop. Whereas Link-state like OSPF is more reliable than other IGP (Interior Gateway Protocol) but in exchange they require high performance power and memory for calculations of shortest path.
- **Security Policies and Enhancement**: This aspect involves the protection and control of network traffic. Misconfiguration of routing protocol can make the network vulnerable to attack that could lead to compromise and disturb the network integrity and availability. So, different methods like encryption, authentication, and filtering the network traffic coming from the public network through access-list are used for preventing unauthorized access.
- **Running protocol compatibility and interoperability**: Different routing protocols are used according to their requirement in network carries the information of routing table and network topology. This aspect covers the synchronization and redistribution of routing table information between the different routing protocol. For example, my company is linked to the ISP through BGP with distinct Autonomous System, if there is a need for my company to obtain the route to the ISP, the process involves redistributing information between different routing protocols.
- **Running protocol configuration and troubleshoot**: This aspect involves the maintenance of routing protocol through planning, implementation, and troubleshooting of routing protocols. Each routing protocol has best practice and guidelines such as network address, metric, timers, and parameter. Choosing an appropriate command for verifying, monitoring, and debugging for troubleshooting the routing protocol.

OSPF

In a three-tier architecture, OSPF offers several essential features that enhance network performance and reliability. One of the key features of OSPF is to allows routers in the network to dynamically share routing information. This is critical in a three-tier architecture because network modifications, such as adding or removing servers or network segments, are possible. OSPF guarantees that routers understand the existing network topology and can adapt to changes. It employs a link-state routing algorithm, in which routers keep track of network topology. Using this information, each router calculates the shortest path to a destination. In a three-tier architecture, where data may need to travel across many network segments, OSPF serves in selecting the most effective routes. OSPF allows for the setting up of several routes to the same destination. In a three-tier architecture, this can help to increase availability and fault tolerance. If one way becomes unavailable due to a network fault, OSPF can immediately divert traffic to another path. OSPF is meant to perform well in large networks. In a three-tier architecture, where the network infrastructure can cover numerous locations and include a large number of routers and switches.

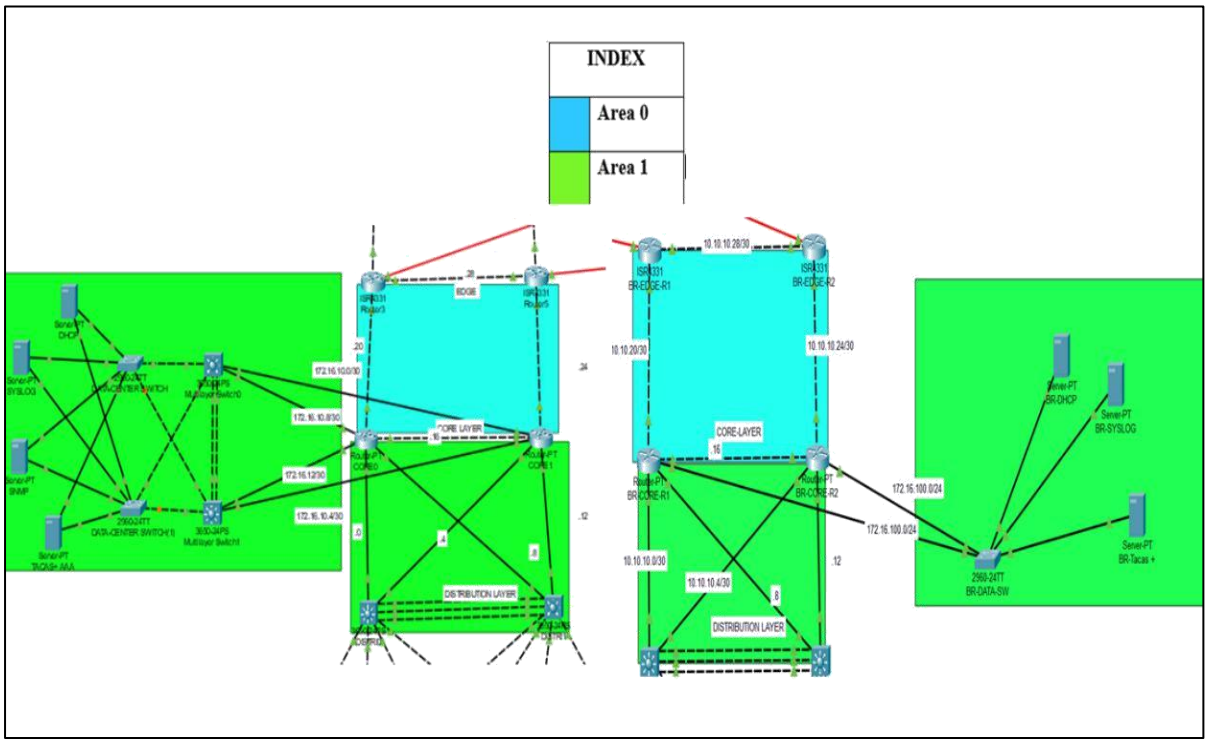


Figure 4: OSPF area sub-diving in headquarter and Branch

For the effective communication in between the tier, OSPF was implemented from Distribution layer to core layer, OSPF was selected due to its utilization of link-state information to build a comprehensive database, effectively managing the complexity of the network topology across a wide area. This approach enhances the scalability and efficiency of the network by providing a detailed understanding of the links and their states, facilitating quick adaptation to changes, and supporting optimal routing decisions. We utilize OSPF for efficient internal communication within the private network. However, when establishing connection to the ISP, BGP routing protocol is implemented in real world scenario because BGP is independent from Autonomous System and making it well suited for exchanging routes over long distances.

HEADQUARTER

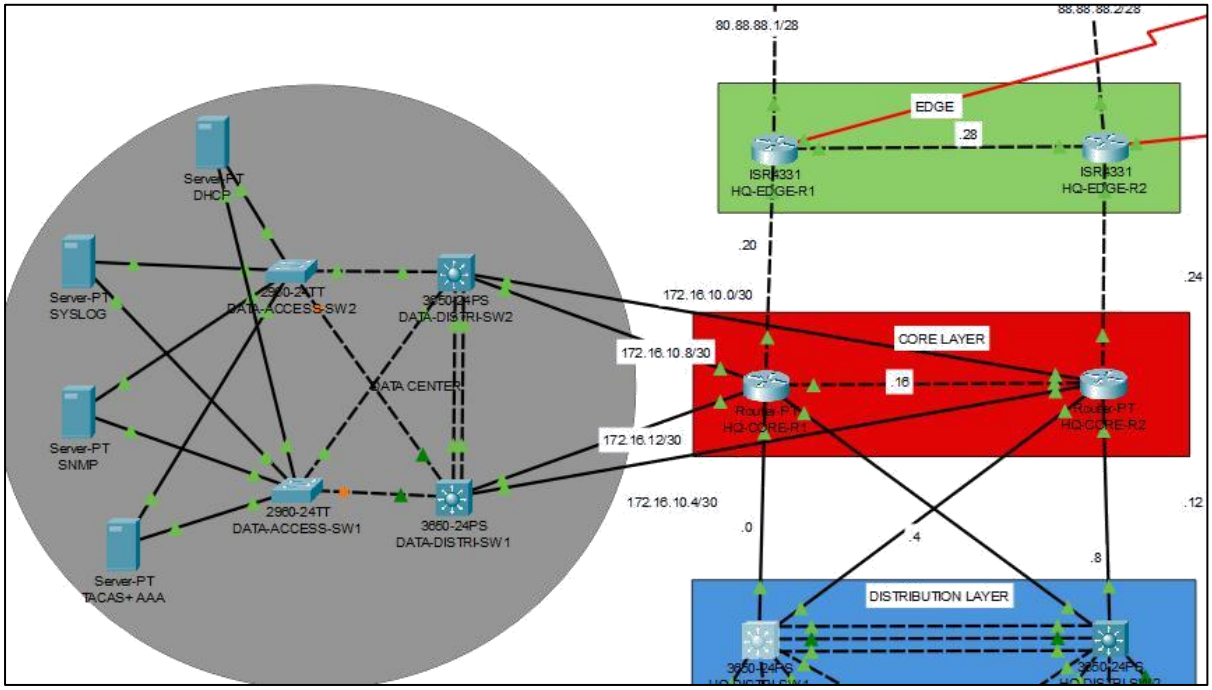


Figure 5: Physical diagram of headquarter

HQ-DISTRI-SW1

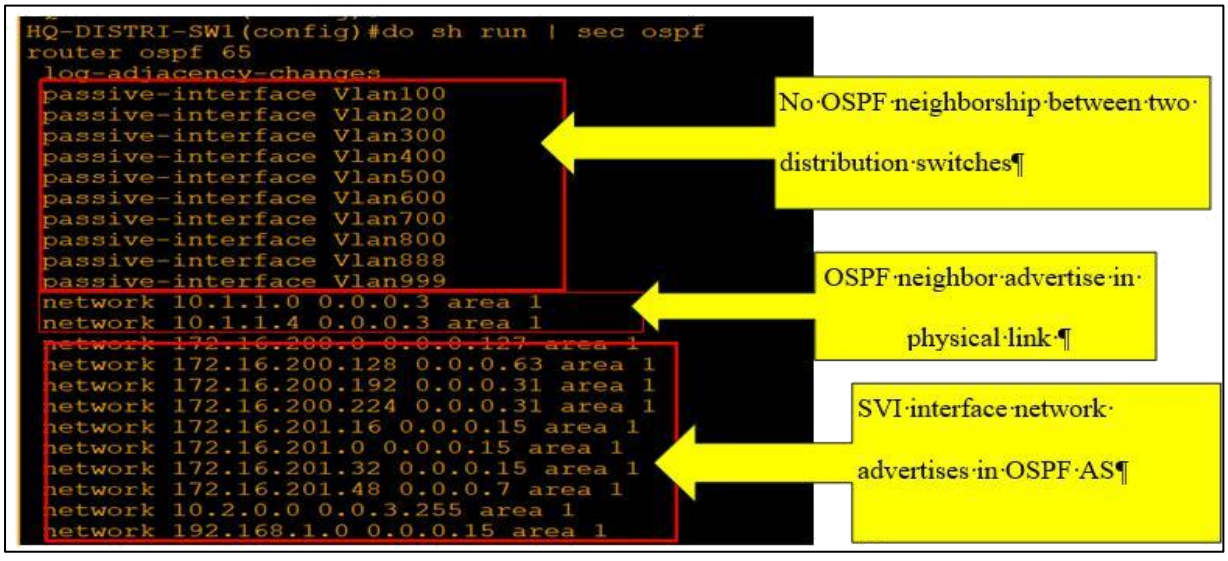


Figure 6: Running configuration of OSPF in AS of HQ-DISTRI-SW1

```
HQ-DISTRI-SW1(config-router)#do sh ip ospf neigh

Neighbor ID     Pri   State           Dead Time   Address         Interface
172.16.10.14      1   FULL/BDR        00:00:34    10.1.1.2        GigabitEthernet1/0/5
172.16.10.6       1   FULL/BDR        00:00:36    10.1.1.6        GigabitEthernet1/0/6
HQ-DISTRI-SW1(config-router)#
```

Figure 7: OSPF neighborship of HQ-DISTRI-SW1

HQ-DISTRI-SW2

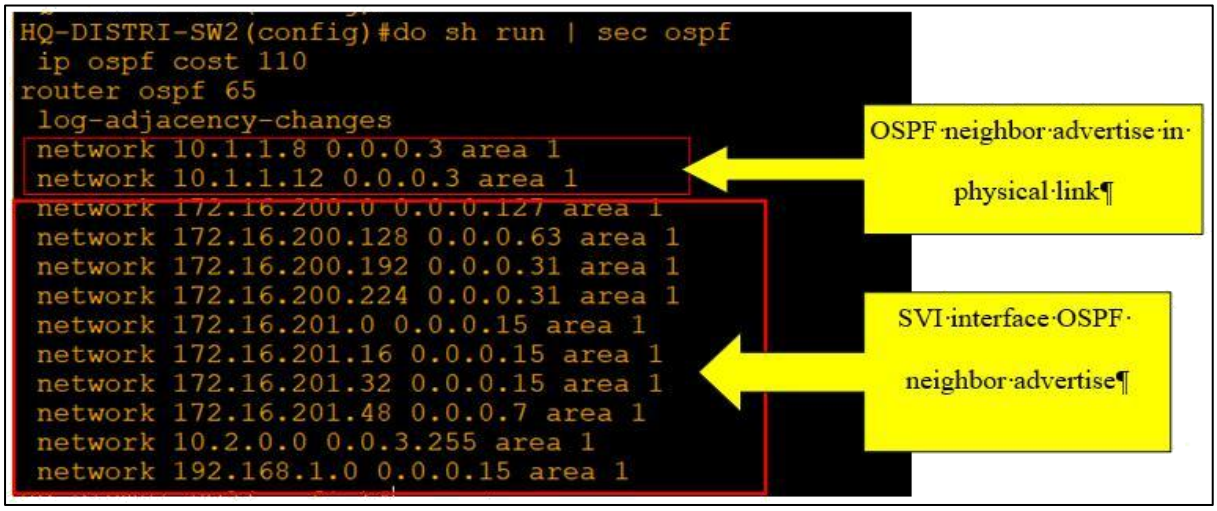


Figure 8: Running-config of HQ-DISTRI-SW2 section OSPF

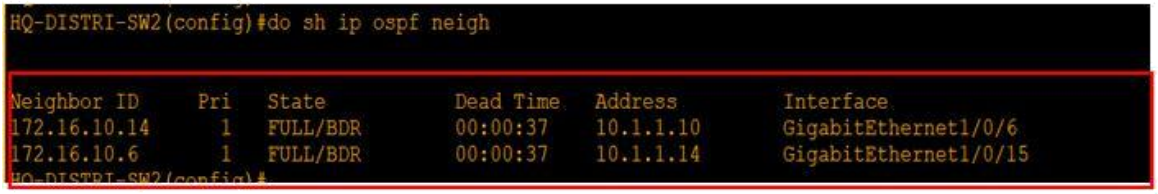


Figure 9: OSPF neighborship of HQ-DISTRI-SW2

HQ-CORE-R1

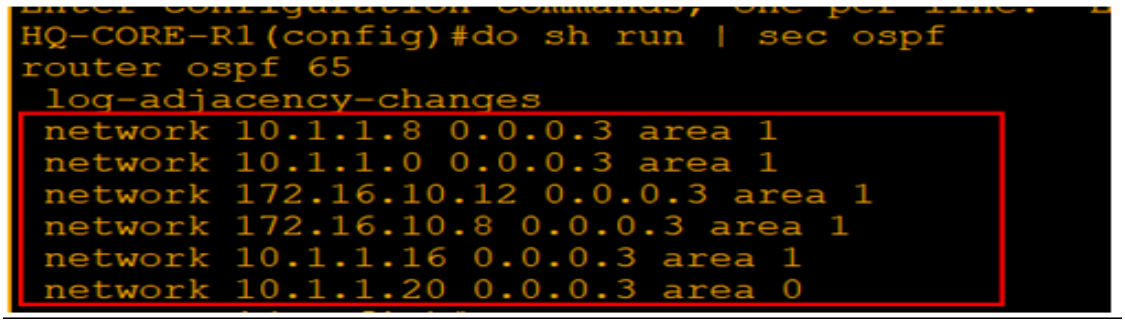


Figure 10: Running config of OSPF configuration of HQ-CORE-R1

Figure 11: OSPF neighborship of HQ-CORE-R1

HQ-CORE-R2

```
HQ-CORE-R2(config)#do sh run | sec ospf
router ospf 65
 log-adjacency-changes
 network 10.1.1.12 0.0.0.3 area 1
 network 10.1.1.4 0.0.0.3 area 1
 network 172.16.10.0 0.0.0.3 area 1
 network 172.16.10.4 0.0.0.3 area 1
 network 10.1.1.16 0.0.0.3 area 1
 network 10.1.1.24 0.0.0.3 area 0
```

Figure 12: Running-config of OSPF config on HQ-CORE-R2

```
HQ-CORE-R2(config)#do sh ip ospf neigh

Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.254.1     1   FULL/DR         00:00:31    172.16.10.1     GigabitEthernet0/0
192.168.254.2     1   FULL/DR         00:00:31    172.16.10.5     GigabitEthernet1/0
172.16.10.14      1   FULL/DR         00:00:31    10.1.1.17       GigabitEthernet3/0
192.168.1.2       1   FULL/DR         00:00:32    10.1.1.13       GigabitEthernet5/0
192.168.1.1       1   FULL/DR         00:00:31    10.1.1.5        GigabitEthernet6/0
145.0.0.2         1   FULL/BDR        00:00:30    10.1.1.26       GigabitEthernet7/0
```

Figure 13: OSPF neighborship of HQ-CORE-R2

HQ-EDGE-R1

```
HQ-EDGE-R1(config)#do sh run | sec ospf
router ospf 65
 log-adjacency-changes
 network 10.1.1.28 0.0.0.3 area 0
 network 10.1.1.20 0.0.0.3 area 0
 network 9.9.9.9 0.0.0.0 area 0
 default-information originate
```

Figure 14: OSPF config in HQ-EDGE-R1

```
HQ-EDGE-R1(config)#do sh ip ospf neigh

Neighbor ID     Pri   State           Dead Time   Address         Interface
172.16.10.14      1   FULL/DR         00:00:32    10.1.1.21       GigabitEthernet0/0/0
145.0.0.2         1   FULL/DR         00:00:34    10.1.1.29       GigabitEthernet0/0/2
```

Figure 15: OSPF neighborship of HQ-EDGE-R1

HQ-EDGE-R2

```
HQ-EDGE-R2(config)#DO SH run | sec ospf
router ospf 65
 log-adjacency-changes
 network 10.1.1.28 0.0.0.3 area 0
 network 10.1.1.24 0.0.0.3 area 0
 default-information originate
```

Figure 16: OSPF configuration in HQ-EDGE-R2

```
 default-information originate
HQ-EDGE-R2(config)#do sh ip ospf neigh

Neighbor ID     Pri   State           Dead Time   Address         Interface
9.9.9.9           1   FULL/BDR        00:00:30    10.1.1.30       GigabitEthernet0/0/2
172.16.10.6       1   FULL/DR         00:00:37    10.1.1.25       GigabitEthernet0/0/0
HQ-EDGE-R2(config)#
```

Figure 17: OSPF neighborship of HQ-EDGE-R2

Branch

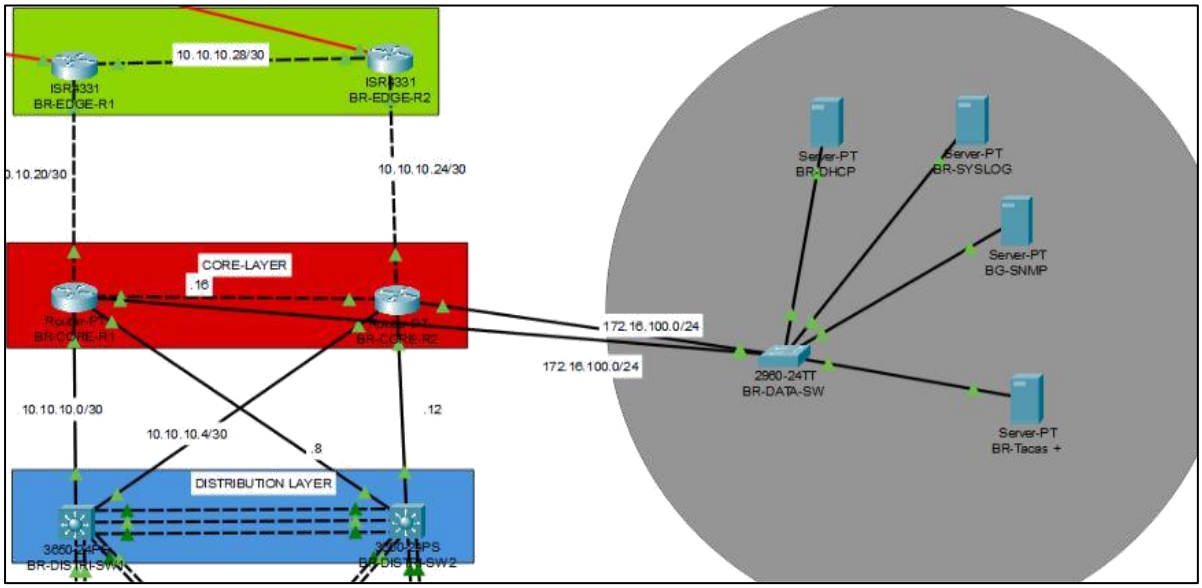


Figure 18: Physical diagram of branch

BR-DISTRI-SW1

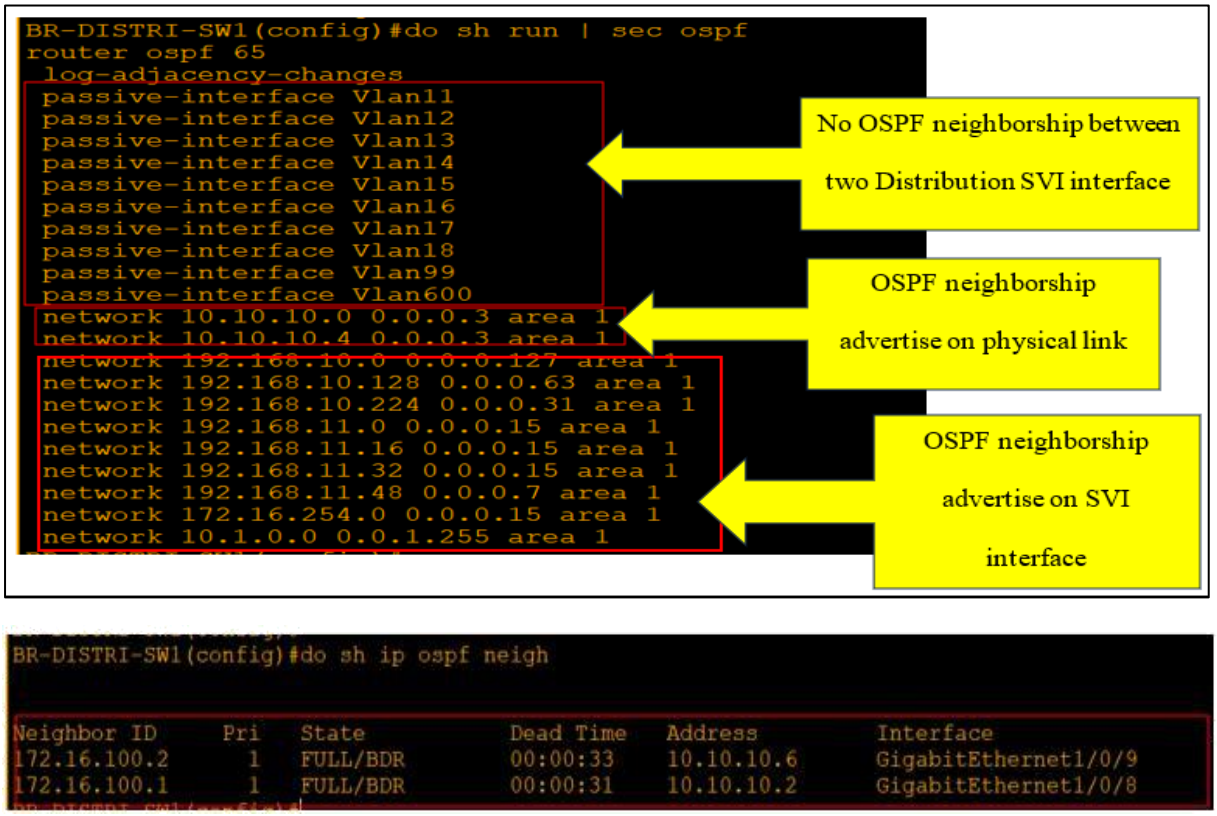


Figure 19: OSPF config and neighborship of BR-DISTRI-SW1

BR-DISTRI-SW2

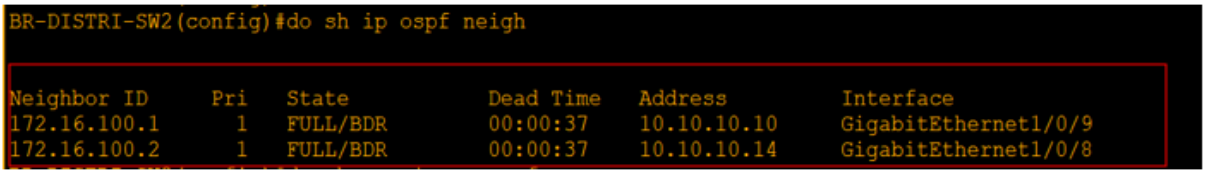


Figure 20: OSPF config and neighborship of BR-DISTRI-SW2

BR-CORE-R1

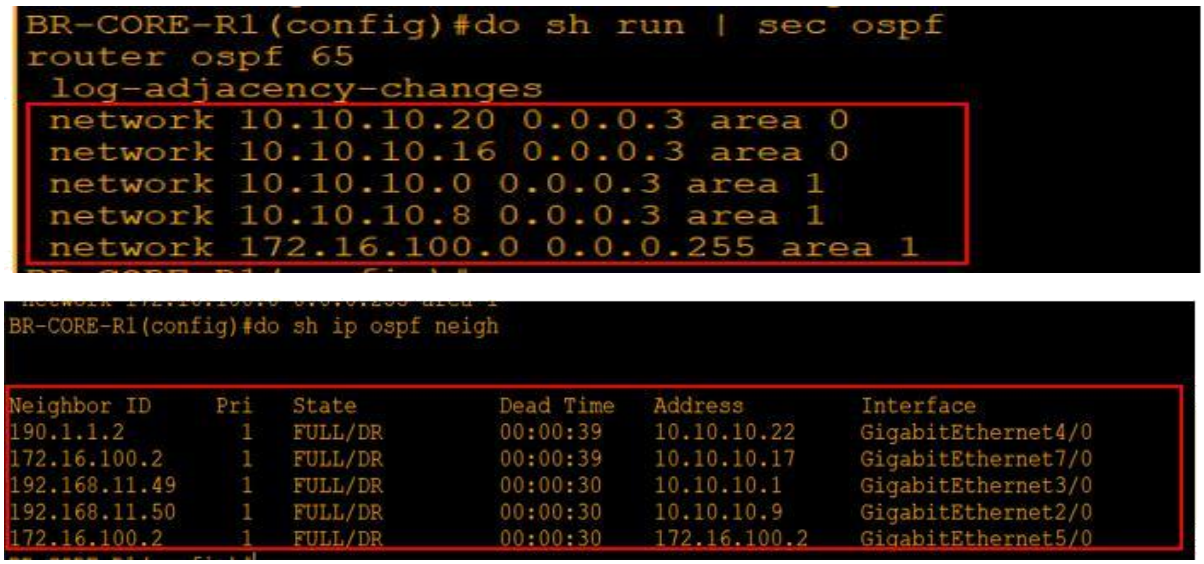


Figure 21: OSPF config and neighborship of BR-CORE-R1

BR-CORE-R2

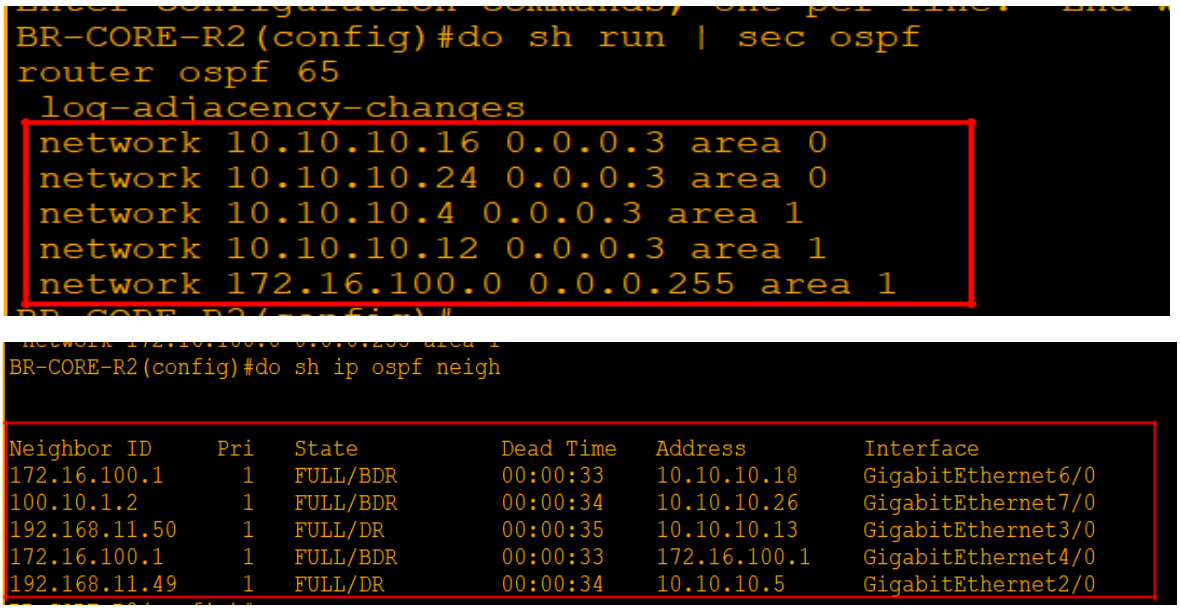


Figure 22: OSPF config and neighborship of BR-CORE-R2

BR-EDGE-R1

```
BR-EDGE-R1(config)#do sh run | sec ospf
router ospf 65
 log-adjacency-changes
 network 10.10.10.28 0.0.0.3 area 0
 network 10.10.10.20 0.0.0.3 area 0
 default-information originate
```

```
BR-EDGE-R1(config)#do sh ip ospf neigh

Neighbor ID     Pri   State           Dead Time   Address         Interface
172.16.100.1      1   FULL/BDR        00:00:30    10.10.10.21     GigabitEthernet0/0/0
100.10.1.2        1   FULL/BDR        00:00:32    10.10.10.29     GigabitEthernet0/0/1
```

Figure 23: OSPF config and neighborship of BR-EDGE-R1

BR-EDGE-R2

```
BR-EDGE-R2(config)#do sh run | sec ospf
router ospf 65
 log-adjacency-changes
 network 10.10.10.28 0.0.0.3 area 0
 network 10.10.10.24 0.0.0.3 area 0
 default-information originate
```

```
BR-EDGE-R2(config)#do sh ip ospf neigh

Neighbor ID     Pri   State           Dead Time   Address         Interface
190.1.1.2         1   FULL/DR         00:00:38    10.10.10.30     GigabitEthernet0/0/1
172.16.100.2      1   FULL/DR         00:00:36    10.10.10.25     GigabitEthernet0/0/0
```

Figure 24: OSPF config and neighborship of BR-EDGE-R2

RIP

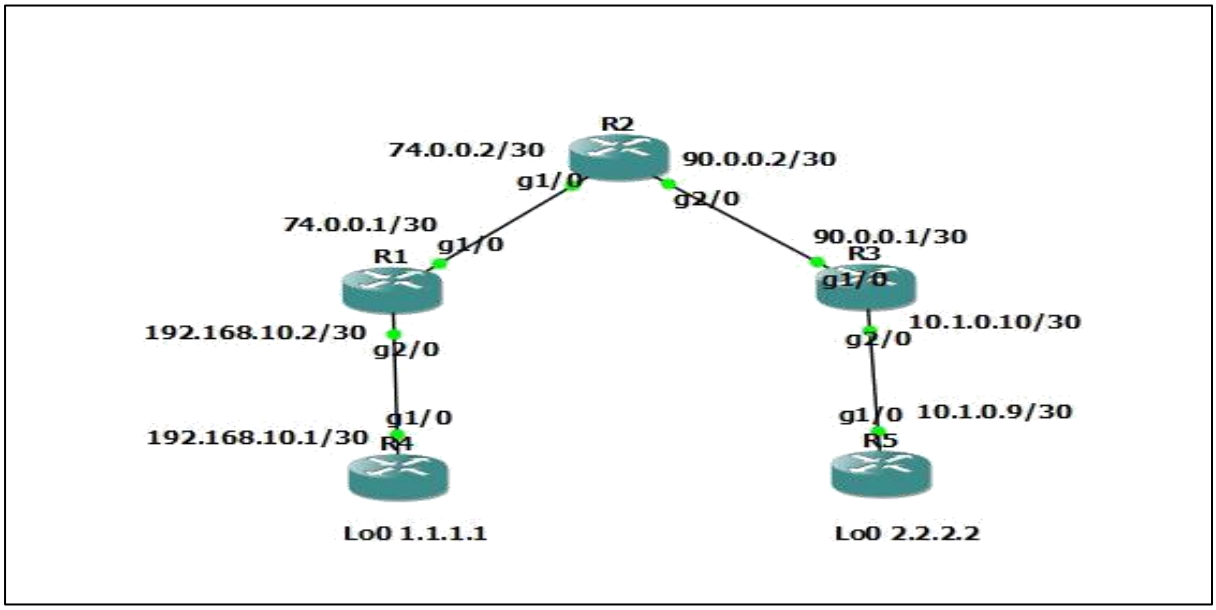


Figure 25: Simple physical network topology in GNS3

Note: In RIP routing protocol each devices need to specify the direct link connection network. By default, RIP runs in version 1 i.e., classful so, running classless version 2 should be mentioned in CLI.

```
R4(config)#router rip
R4(config-router)#ver 2
R4(config-router)#network 192.168.10.0
R4(config-router)#network 1.1.1.1
R4(config-router)#
```

Figure 26: RIP configuring in R4

```
R1(config)#router rip
R1(config-router)#
R1(config-router)#ver 2
R1(config-router)#
R1(config-router)#network 192.168.10.0
R1(config-router)#network 74.0.0.0
```

Figure 27: Configuration of RIP in R1

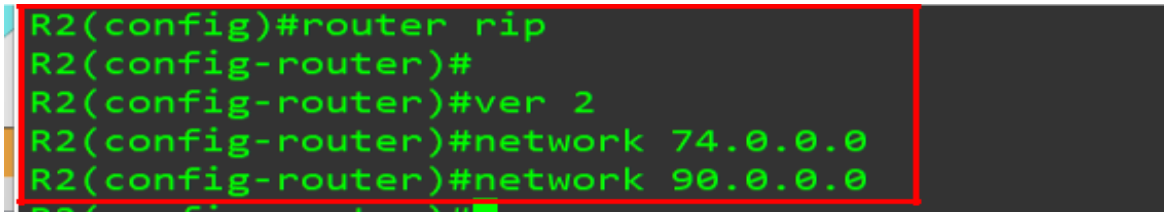


Figure 28: Configuration of RIP in R2

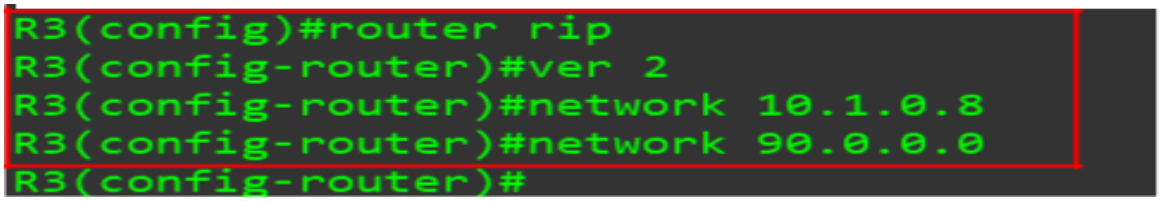


Figure 29: RIP configuration in R3

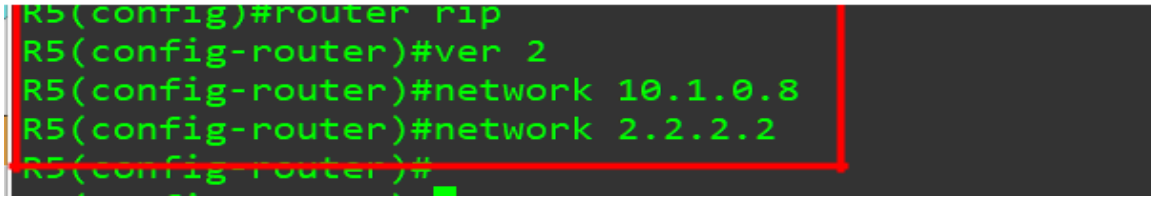


Figure 30: RIP configuration in R5

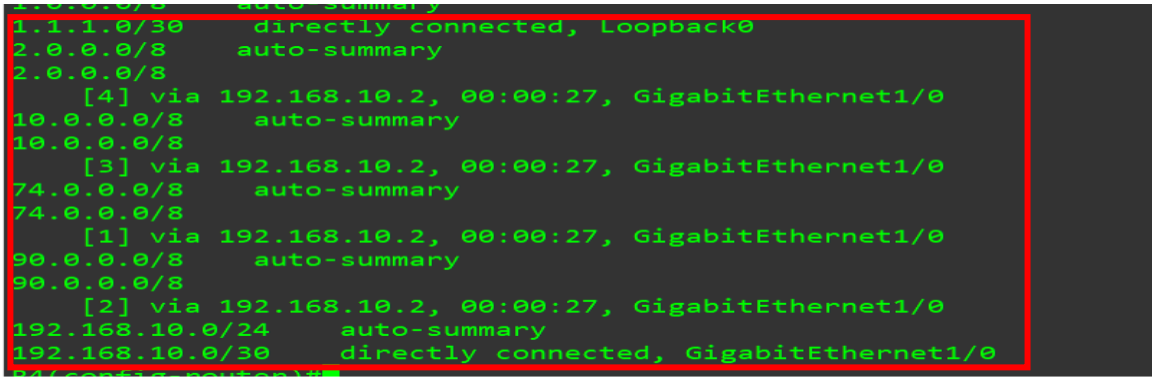


Figure 31: RIP database of R4

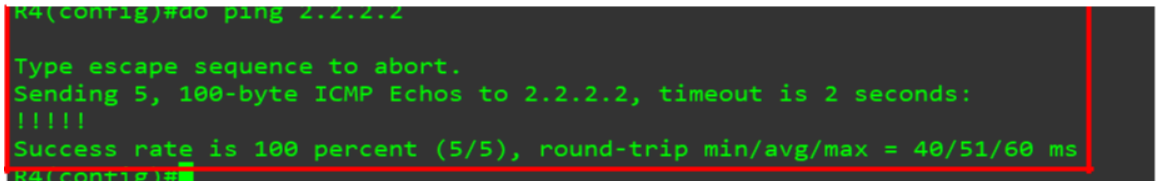


Figure 32: Verifying by pinging R5

Benifits

Maximum hop count of EIGRP is 255 whereas RIP is 15. So, EIGRP is better for medium size organization network topology. EIGRP supports an AS, which means the group of network chunks can be shared from one device to another whereas RIP does not that mean it does not support. EIGRP routes are preferable because the AD of EIGRP is 90 and RIP 120. EIGRP can calculate the shortest path through metric calculation like bandwidth, delay, reliability, effective bandwidth, and MTU whereas RIP only has hop count metric

Drawbacks

EIGRP is a cisco proprietary protocol and RIP is an industry standard routing protocol. EIGRP can cover up a larger network than RIP, but it might create an overhead by sending hello packets for the neighborship.

Static routing

For static routing we need to specify the indirect network, subnet mask, and next hop or exit interfaces. For static routing I have configure the settings according to its pre-requisite in above figure 25. every route should individually need to specify for building up the route so, implementing a static configuration in large network can be a time-intensive process. As a result, static route is more feasibility to implement in small network. The main purpose of Static routing to create a direct route to the destination unlike dynamic routing need to share the route to each other. As a result, reduces the overhead by using the less CPU and memory usage and limit the exposure of routing information

> **Example**: ip route {indirect-network} {subnet-mask} {next-hop-IP-address || exit interface}

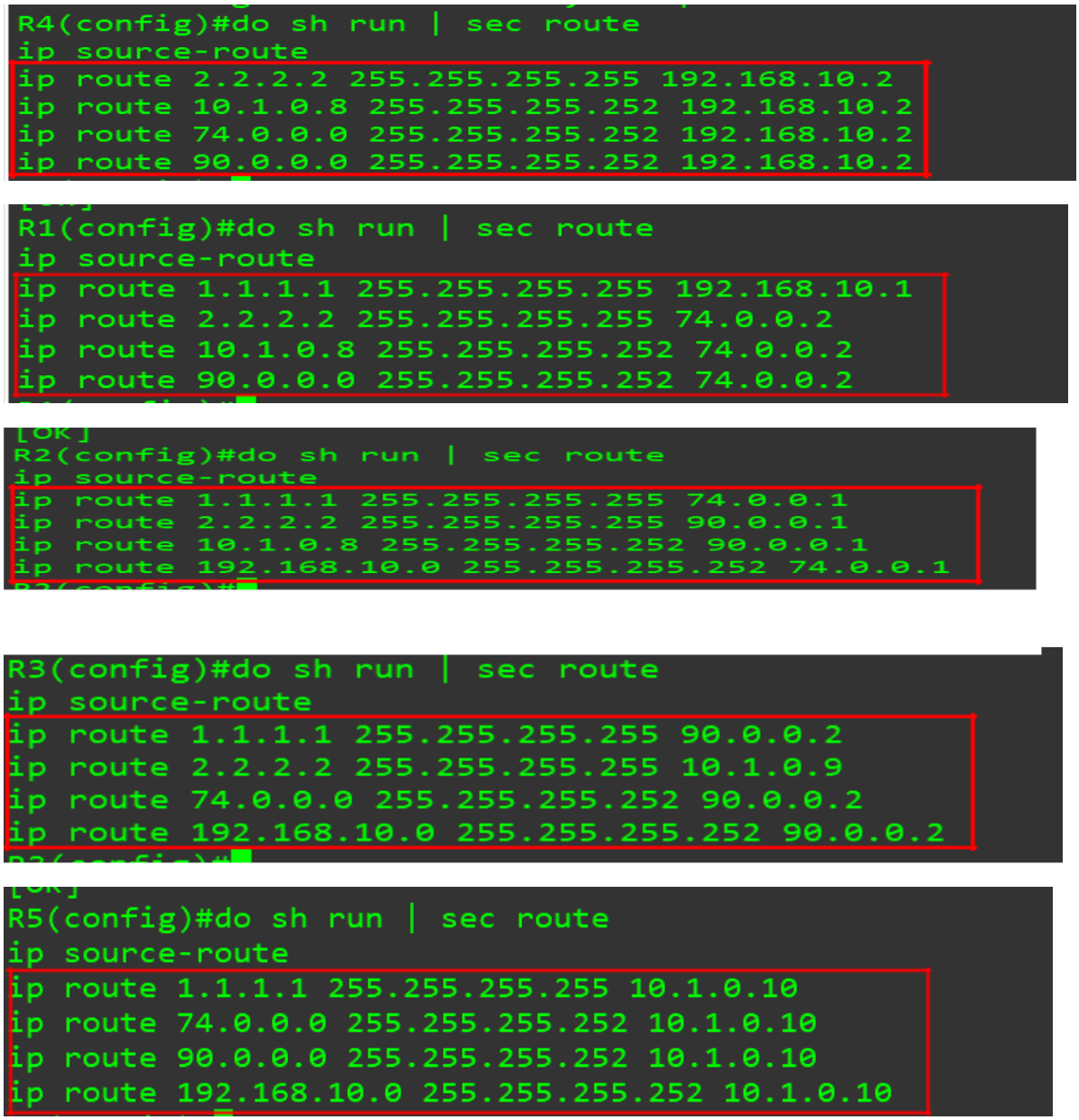


Figure 33: Static route configuration in R1, R2, R3, R4 & R5 routers

```
R4(config)#do ping 2.2.2.2 source lo0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 36/47/60 ms
```

Figure 34: Ping to R5

```
R5(config)#do ping 1.1.1.1 source lo0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:
Packet sent with a source address of 2.2.2.2
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/59/80 ms
```

Figure 35: Ping to R4

Default route in OSPF

Currently, the expansion of internet encompassing millions of routes available in internet so specifying each route or sharing information of each individual routes is not feasible which consume a lots resources to handle. In such situation, the use of default router proves to be beneficial. In real time scenario, the default router also known as static route is implemented at the edge of private network. This project utilizes the OSPF in private network and BGP in public network.

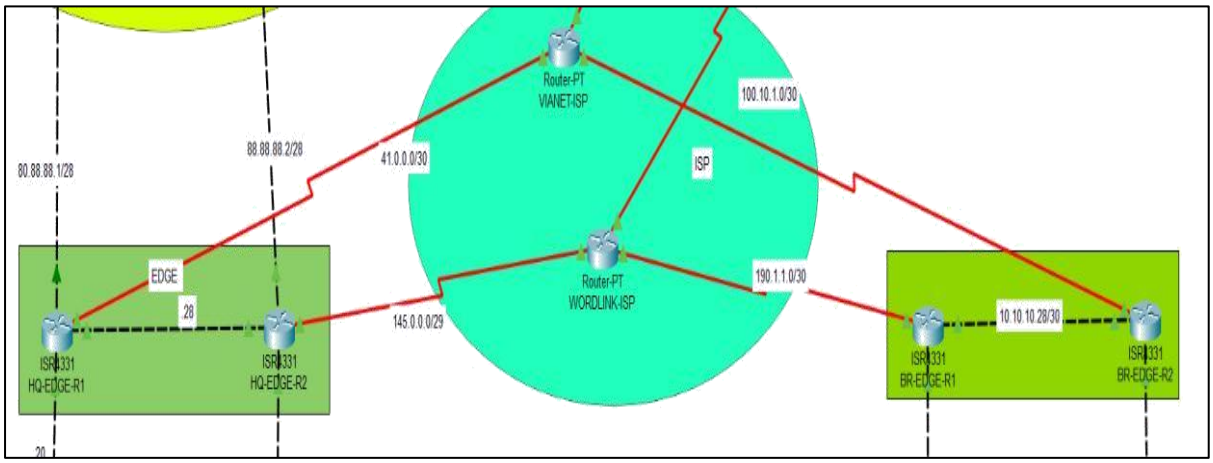


Figure 36: Edge router connection with ISP

HQ-EDGE-R1

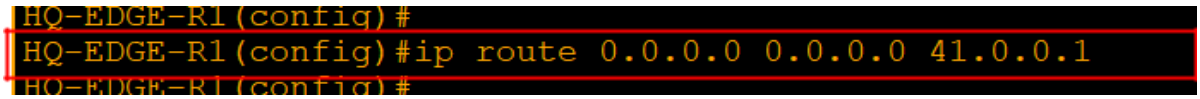


Figure 37: Default static route in HQ-EDGE-R1 to VIANET-ISP

Default-static route is configured on HQ-EDGE-R1 on global configuration mode with the next hop ISP IP i.e. 41.0.0.1

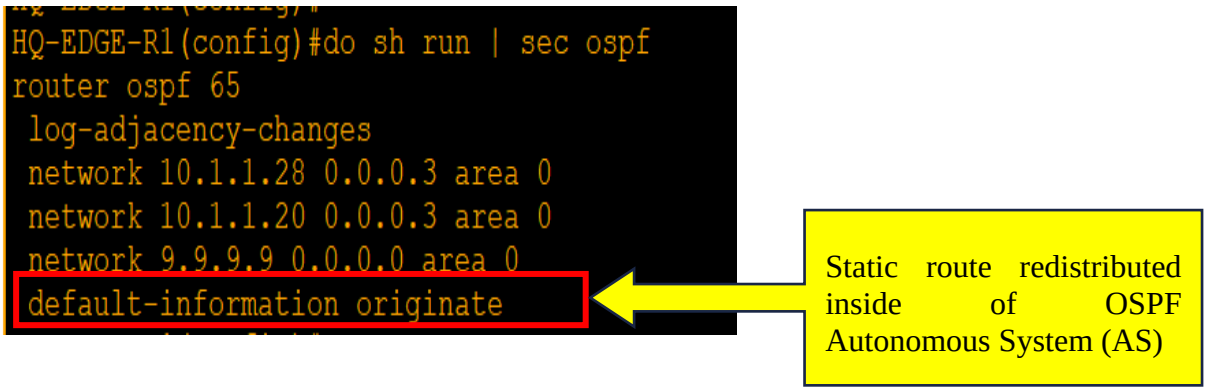


Figure 38: Running config OSPF of HQ-EDGE-R1

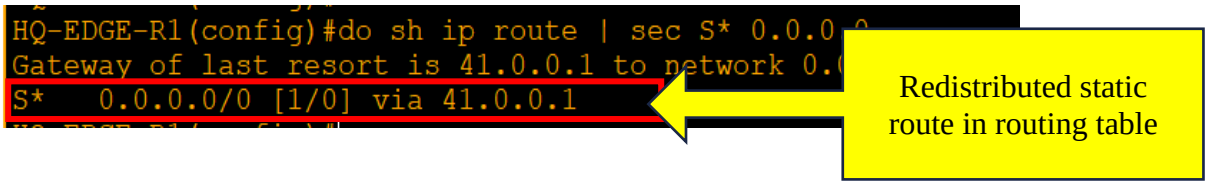


Figure 39: Routing table of HQ-EDGE-R1

Redistributed route in edger router added as a OSPF external type route in routing table of all Layer 3 **(L3)** devices of Headquarter. Same configuration on **HQ-EDGE-R2** was done except next hop i.e. 145.0.0.1 (**Wordlink IPS**).

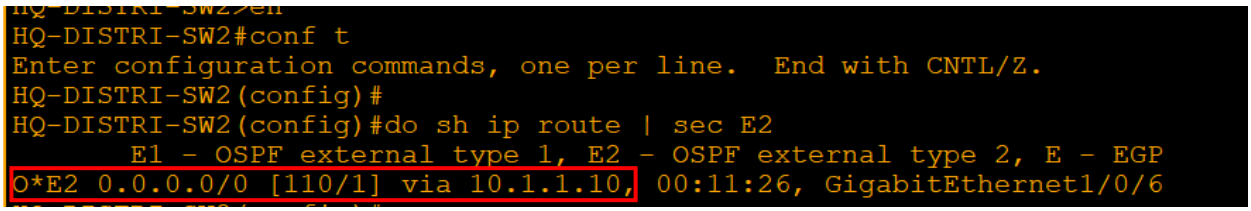


Figure 40: Routing table of DISTRI-SW2

Static route redistributed in OSPF at the edge router appeared as a E2 i.e., OSPF external type in routing table of all L3 devices in headquarter. Now from the headquarter, the end devices can access the internet with the help of **NAT** and **PAT**.

Similarly, with the same configure process of default route in OSPF I have done in headquarter are configure in branch.

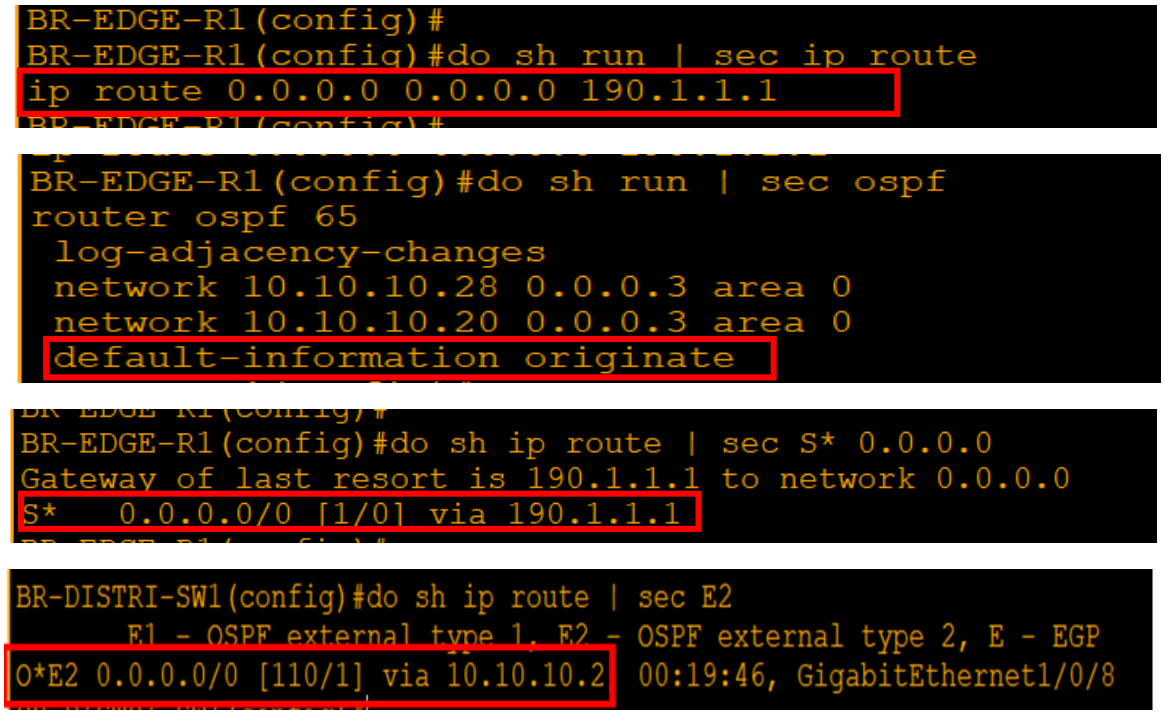


Figure 41: Configuring the default route in edge router of branch

BGP

BGP is only one routing protocol which established a neighborship by exchanging TCP packet between two distinct AS. So, it plays a vital role in the current generation. The external BGP AD is 20, the lowest among all dynamic routing protocols. When determining the best path to the destination can be leverage form 13 attributes available in this protocol. In this project, BGP is implemented on the edge router of Headquarter and Branch establishing a connection to the ISP i.e. Wordlink and Vianet. And ISP establishing a connection with Google.

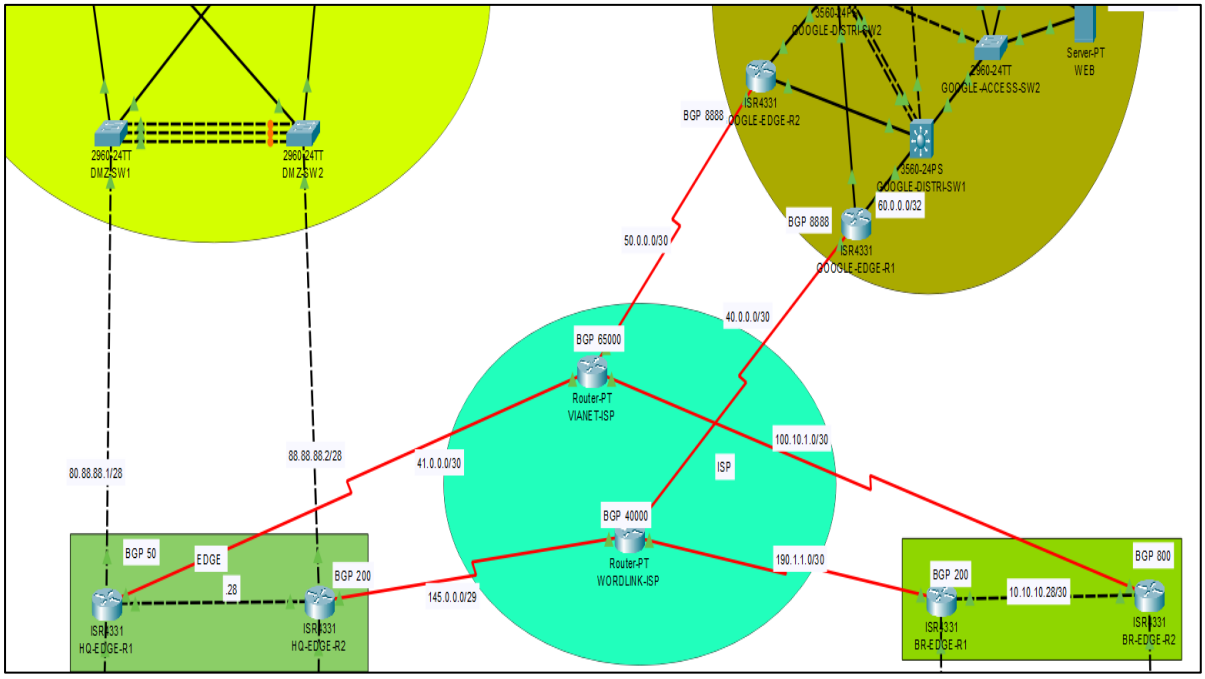


Figure 42:Physical diagram where BGP implemented on edge devices

HEADQUARTER

```
HQ-EDGE-R1(config)#do sh run | sec bgp
router bgp 50
 bgp log-neighbor-changes
 no synchronization
 neighbor 41.0.0.1 remote-as 65000
 network 41.0.0.0 mask 255.255.255.252
 network 80.88.88.0 mask 255.255.255.240
```

Figure 43: Configuration of BGP in HQ-EDGE R1

```
HQ-EDGE-R2(config)#do sh run | sec bgp
router bgp 200
 bgp log-neighbor-changes
 no synchronization
 neighbor 145.0.0.1 remote-as 40000
 network 145.0.0.0 mask 255.255.255.248
 network 80.88.88.0 mask 255.255.255.240
```

Figure 44: BGP configuration in HQ-EDGE-R2

```
HQ-EDGE-R2(config)#do sh ip bgp
BGP table version is 12, local router ID is 145.0.0.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 8.8.8.0/24       145.0.0.1                0     0      0 40000 8888 60 i
*> 10.0.0.0/30      145.0.0.1                0     0      0 40000 8888 60 i
*> 40.0.0.0/30      145.0.0.1                0     0      0 40000 i
*> 44.0.0.0/30      145.0.0.1                0     0      0 40000 8888 60 i
*> 60.0.0.0/30      145.0.0.1                0     0      0 40000 8888 i
*> 74.0.0.0/30      145.0.0.1                0     0      0 40000 8888 90 i
*> 142.250.183.0/24 145.0.0.1                0     0      0 40000 8888 60 i
*  145.0.0.0/29     145.0.0.1                0     0      0 40000 i
*>                  0.0.0.0                  0     0  32768 i
*> 190.1.1.0/30     145.0.0.1                0     0      0 40000 i
*> 216.239.35.0/24  145.0.0.1                0     0      0 40000 8888 60 i
```

Figure 45:Network using BGP routing protocol

BRANCH

BR-EDGE-R1

```
BR-EDGE-R1(config)#DO SH run | sec bgp
router bgp 800
 bgp log-neighbor-changes
 no synchronization
 neighbor 190.1.1.1 remote-as 40000
 network 190.1.1.0 mask 255.255.255.252
```

Figure 46: BGP configuration in BR-EDGE-R1

```
BR-EDGE-R2(config)#do sh run | sec bgp
router bgp 600
 bgp log-neighbor-changes
 no synchronization
 neighbor 100.10.1.1 remote-as 65000
 network 100.10.1.0 mask 255.255.255.252
```

Figure 47: BGP configuration in BR-EDGE-R2

```
BR-EDGE-R2(config)#do sh ip bgp
BGP table version is 13, local router ID is 100.10.1.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 8.8.8.0/24       100.10.1.1               0      0      0 65000 8888 90 i
*> 10.0.0.0/30      100.10.1.1               0      0      0 65000 8888 i
*> 41.0.0.0/30      100.10.1.1               0      0      0 65000 i
*> 44.0.0.0/30      100.10.1.1               0      0      0 65000 8888 60 i
*> 50.0.0.0/30      100.10.1.1               0      0      0 65000 i
*> 60.0.0.0/30      100.10.1.1               0      0      0 65000 8888 90 i
*> 74.0.0.0/30      100.10.1.1               0      0      0 65000 8888 i
*> 80.88.88.0/28    100.10.1.1               0      0      0 65000 50 i
*> 100.10.1.0/30    0.0.0.0                  0      0  32768 i
*                   100.10.1.1               0      0      0 65000 i
*> 142.250.183.0/24 100.10.1.1               0      0      0 65000 8888 90 i
*> 216.239.35.0/24  100.10.1.1               0      0      0 65000 8888 90 i
```

Figure 48: Network using BGP protocol

ISP (Internet Service Provider)

```
VIANET-ISP(config)#do sh run | sec bgp
router bgp 65000
 bgp log-neighbor-changes
 no synchronization
 neighbor 200.1.1.1 remote-as 50
 neighbor 50.0.0.2 remote-as 8888
 neighbor 100.10.1.2 remote-as 600
 neighbor 90.0.0.2 remote-as 40000
 neighbor 41.0.0.2 remote-as 50
 network 200.1.1.0 mask 255.255.255.248
 network 100.10.1.0 mask 255.255.255.252
 network 90.0.0.0 mask 255.255.255.252
 network 50.0.0.0 mask 255.255.255.252
 network 41.0.0.0 mask 255.255.255.252
```

Figure 49: BGP configuration in VIANET-ISP

```
WORDLINK-ISP(config)#do sh run | sec bgp
router bgp 40000
 bgp log-neighbor-changes
 no synchronization
 neighbor 90.0.0.1 remote-as 65000
 neighbor 145.0.0.2 remote-as 200
 neighbor 190.1.1.2 remote-as 800
 neighbor 40.0.0.2 remote-as 8888
 network 145.0.0.0 mask 255.255.255.248
 network 190.1.1.0 mask 255.255.255.252
 network 90.0.0.0 mask 255.255.255.252
 network 40.0.0.0 mask 255.255.255.252
```

Figure 50: BGP configuration in WORDLINK-ISP

```
VIANET-ISP(config)#DO sh ip bgp
BGP table version is 15, local router ID is 100.10.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 8.8.8.0/24       50.0.0.2                 0      0      0 8888 90 i
*> 10.0.0.0/30      50.0.0.2                 0      0      0 8888 i
*> 41.0.0.0/30      0.0.0.0                  0      0 32768 i
*                   41.0.0.2                 0      0      0 50 i
*> 44.0.0.0/30      50.0.0.2                 0      0      0 8888 60 i
*> 50.0.0.0/30      0.0.0.0                  0      0 32768 i
*                   50.0.0.2                 0      0      0 8888 i
*> 60.0.0.0/30      50.0.0.2                 0      0      0 8888 90 i
*> 74.0.0.0/30      50.0.0.2                 0      0      0 8888 i
*> 80.88.88.0/28    41.0.0.2                 0      0      0 50 i
*> 100.10.1.0/30    0.0.0.0                  0      0 32768 i
*                   100.10.1.2               0      0      0 600 i
*> 142.250.183.0/24 50.0.0.2                 0      0      0 8888 90 i
*> 216.239.35.0/24  50.0.0.2                 0      0      0 8888 90 i
```

Figure 51: List of networks using BGP as external routing protocol

```
GOOGLE-EDGE-R1(config)#do sh run | sec bgp
router bgp 8888
 bgp log-neighbor-changes
 no synchronization
 neighbor 40.0.0.1 remote-as 40000
 neighbor 60.0.0.2 remote-as 90
 neighbor 44.0.0.1 remote-as 60
 network 40.0.0.0 mask 255.255.255.252
 network 60.0.0.0 mask 255.255.255.252
```

Figure 52: BGP configuration in GOOLGE-EDGE-R1

```
GOOGLE-EDGE-R2(config)#do sh run | sec bgp
router bgp 8888
 bgp log-neighbor-changes
 no synchronization
 neighbor 50.0.0.1 remote-as 65000
 neighbor 10.0.0.2 remote-as 60
 neighbor 74.0.0.1 remote-as 90
 network 50.0.0.0 mask 255.255.255.252
 network 10.0.0.0 mask 255.255.255.252
 network 74.0.0.0 mask 255.255.255.252
```

Figure 53: BGP configuration in GOOLGE-EDGE-R2

```
GOOGLE-EDGE-R2(config)#do sh ip bgp
BGP table version is 18, local router ID is 74.0.0.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*  8.8.8.0/24       10.0.0.2                 0      0      0 60 i
*>                  74.0.0.1                 0      0      0 90 i
*> 10.0.0.0/30      0.0.0.0                  0      0 32768 i
*                   10.0.0.2                 0      0      0 60 i
*> 41.0.0.0/30      50.0.0.1                 0      0      0 65000 i
*> 44.0.0.0/30      10.0.0.2                 0      0      0 60 i
*> 50.0.0.0/30      0.0.0.0                  0      0 32768 i
*                   50.0.0.1                 0      0      0 65000 i
*> 60.0.0.0/30      74.0.0.1                 0      0      0 90 i
*> 74.0.0.0/30      0.0.0.0                  0      0 32768 i
*                   74.0.0.1                 0      0      0 90 i
*> 80.88.88.0/28    50.0.0.1                 0      0      0 65000 50 i
*> 100.10.1.0/30    50.0.0.1                 0      0      0 65000 i
*  142.250.183.0/24 10.0.0.2                 0      0      0 60 i
*>                  74.0.0.1                 0      0      0 90 i
*  216.239.35.0/24  10.0.0.2                 0      0      0 60 i
*>                  74.0.0.1                 0      0      0 90 i
```

Figure 54: Number of networks using BGP protocol broadcasted to GOOGLE-EDGE-R2

Access Layer

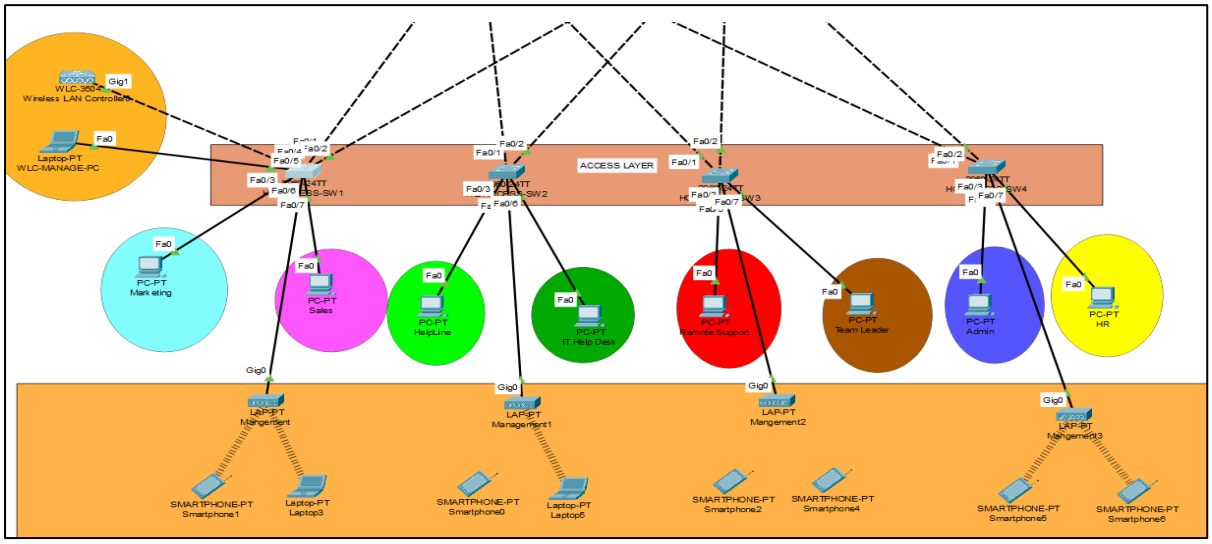


Figure 55: Physical diagram show casing the end devices connected to access layer of headquarter

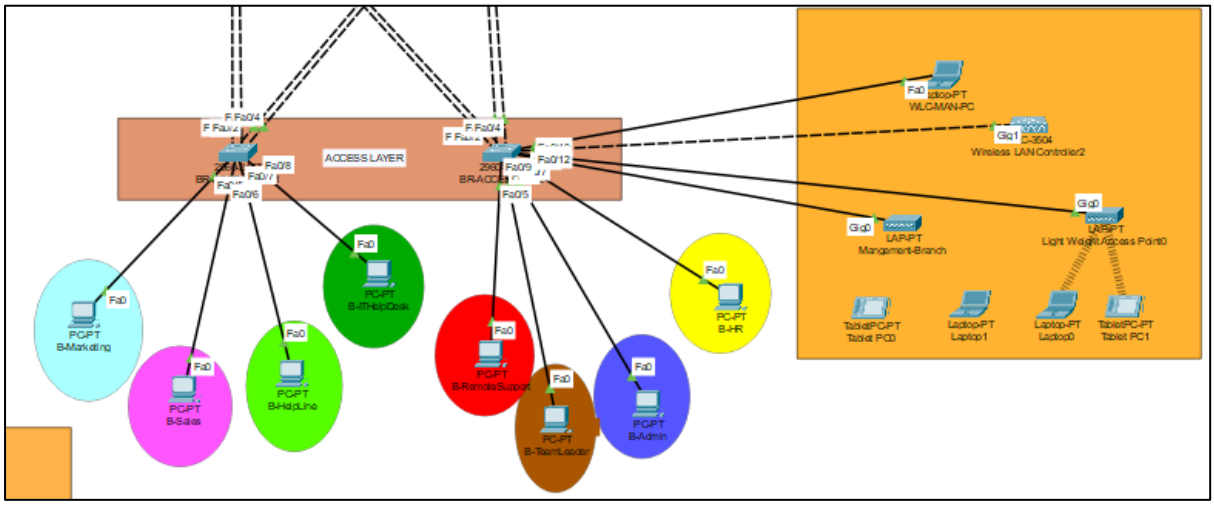


Figure 56:Physical diagram show casing the end devices connected to access layer of branch

VLANs segregation

Eight available department i.e. **Marketing, Sales, Help Line, IT Help Desk, Remote Support, Team Leader, Admin, and HR**. Additionally, VLANs for **Management department** also segregated for managing the L2 switches **and WLC with Guest department** also segregated for APs. L2 switches available in headquarter is 4 and in branch is 2. Each switches need to configure an L2 protocol like **STP**, **VTP**, **Trunking**, **Portfast**, **Ether channel, access port**. And security features like **DHCP snooping**, **ARP inspection**, **BPDU Guard**, **port-security** etc.

Table 1

Department name	VLAN allocation	No of end host
Marketing	100	65
Sales	200	50
Help Line	300	25
IT Helpdesk	400	15
Remote Support	500	10
Team Leader	600	6
Admin	700	5
HR	800	3
Management	999	-----
Guest	888	-----

Table 1: VLANs allocation for headquarter

Department name	VLAN allocation	No of end host
Marketing	11	65
Sales	12	50
Help Line	13	25
IT Helpdesk	14	15
Remote Support	15	10
Team Leader	16	6
Admin	17	5
HR	18	3
Management	99	-----
Guest	600	-----

Table 2: VLANs allocation for branch

Variable Length Subnet Mask (VLSM)

Our client has provided us of end host in 8 department, and instead of relying default subnet mask, we ‘ve implemented a CIDR (Classless Inter-Domain Routing) based on VLSM. This approach enhances flexibility in selecting subnet mask, instead of using classful subnet mask. VLSM enables more efficient utilization of IP address space by allowing of different size subnets based on the specific requirements of each department.

No of Department	No of end user Host	No of gateways (SVI 1 +SVI 2+V. IP)	No of redundancy	Total no. of required host	IP / prefix
Marketing	65	3	1	68	172.16.200.0/25
Sales	50	3	1	53	172.16.200.128/26
Help Desk	25	3	1	28	172.16.200.192/27
IT Help Line	15	3	1	18	172.16.200.224/27
Remote Support	10	3	1	13	172.16.201.0/28
Team Leader	6	3	1	9	172.16.200.16/28
Administration	5	3	1	8	172.16.200.32/28
Human Resource	3	3	1	6	172.16.200.48/29

Table 3: VLSM in headquarter

No of Department	No of end user Host	No of Gateways (SVI 1 +SVI 2+V. IP)	No of Redundancy	Total required host	IP / prefix
Marketing	65	3	1	68	192.168.10.0/25
Sales	50	3	1	53	192.168.10.128/26
Help Desk	25	3	1	28	192.168.10.192/27
IT Help Line	15	3	1	18	192.168.10.224/27
Remote Support	10	3	1	13	192.168.11.0/28
Team Leader	6	3	1	9	192.168.11.16/28
Administration	5	3	1	8	192.168.11.32/28
Human Resource	3	3	1	6	192.168.11.48/29

Table 4: VLSM in Branch

STP and Portfast

STP are enable on switches for preventing loop by designating a root bridge in network topology, result RB as a focal point for flowing all the data inside the topology which determines selection of port in forward or block state By default, switches utilize the Per VLAN Spanning-Tree (PVST) protocol, which typically takes 30 seconds to transition to the forwarding state. However, if a blocking state is encountered, an additional 20 seconds are added, extending the process to 50 seconds. This delay can be impractical in data centers and other areas, leading to the introduction to Rapid-PVST. It bypass the blocking state and listening state which directly initiates into learning state. As a result, the process is typically 15 seconds to forwarding state.

```
HQ-ACCESS-SW2(config)#do sh spanning-tree summ
Switch is in pvst mode
Root bridge for: default ExtraVlan Marketing Sale
TeamLeader Admin HR
Extended system ID           is enabled
```

Figure 57: Showing PVST is enable by default in switch

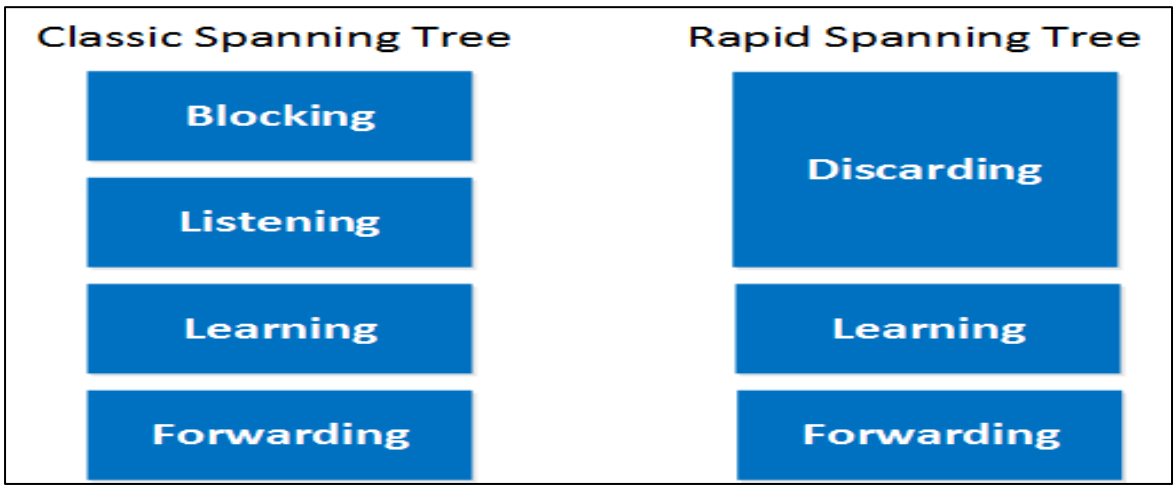


Figure 58L Normal spanning tree state vs Rapid Spanning-tree state

To connect to this network the end users must connect through this l2 switches, user must go through the STP states to access the network. To bypass the three states i.e., Blocking, Listening, and Learning. And initiates directly into the forwarding state. For example, if the user reloads or boots up the system then it goes through all STP states. To address this issue Portfast was introduced and implemented in this layer.

HQ-ACCESS-SW1 & HQ-ACCESS-SW2

Figure

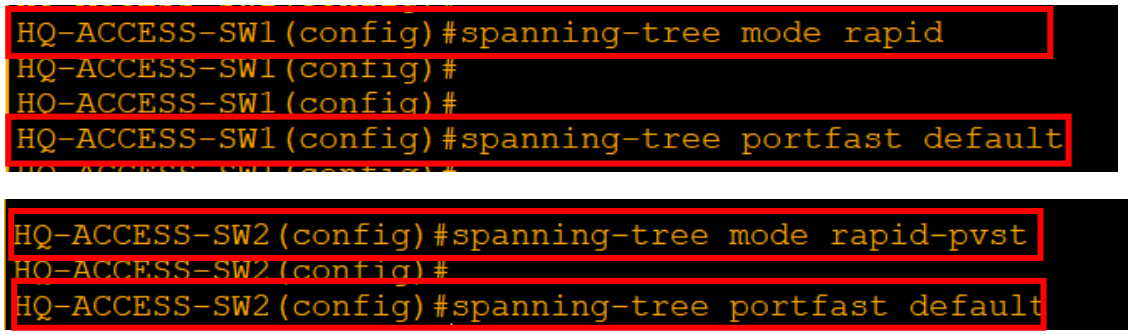


Figure 59: Enabling rapid-pvst and Portfast in HQ-ACCESS-SW1 and HQ-ACCESS-SW2

HQ-ACCESS-SW3 & HQ-ACCESS-SW4

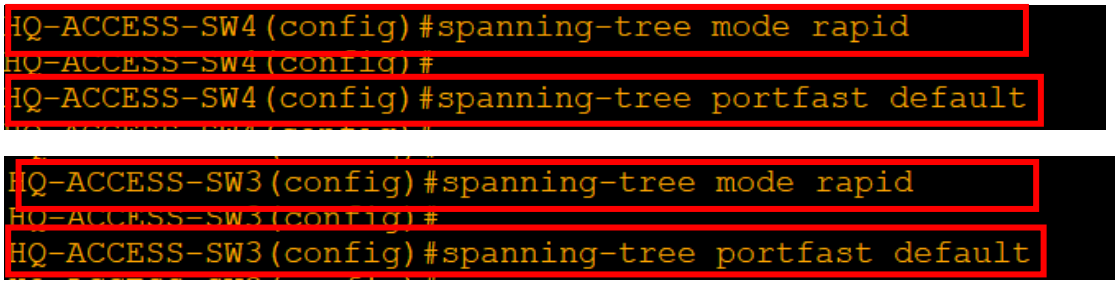


Figure 60: Enabling rapid-pvst and portfast in HQ-ACCESS-SW3 and HQ-ACCESS-S4

HQ-DISTRI-SW1 & HQ-DISTRI-SW2

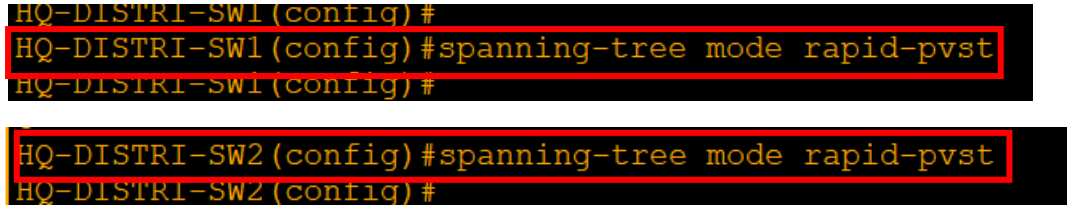


Figure 61: Only enabling rapid-pvst mode in HQ-DISTRI-SW1 & HQ-DISTRI-SW2

DATA-ACCESS-SW1 & DATA-ACCESS-SW2

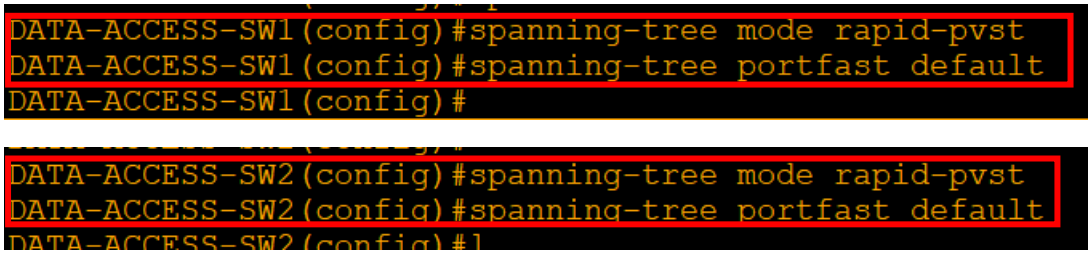


Figure 62: Enabling rapid-PVST and Portfast mode in DATA-ACCESS-SW1 and DATA-ACCESS-SW2

DATA-DISTRI-SW1 & DATA-DISTRI-SW2

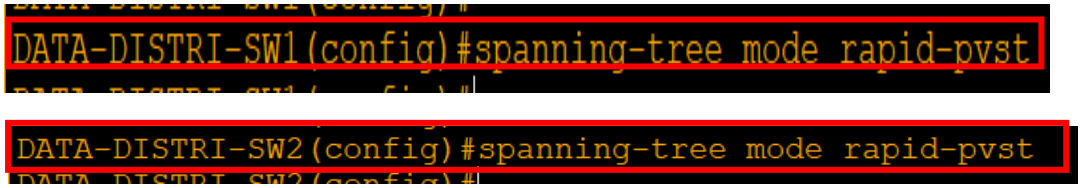


Figure 63: Enabling rapid-PVST in DATA-DISTRI-SW1 and DATA-DISTRI-SW2

DMZ-SW1 & DMZ-SW2

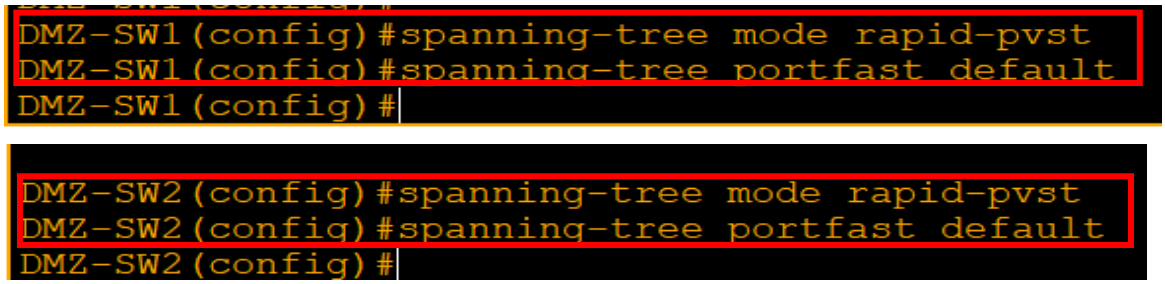


Figure 64: Enabling rapid-pvst and portfast mode in DMZ-ACCESS-SW1 and DMZ-ACCESS-SW2

BR-ACCESS-SW1 & BR-ACCESS-SW2

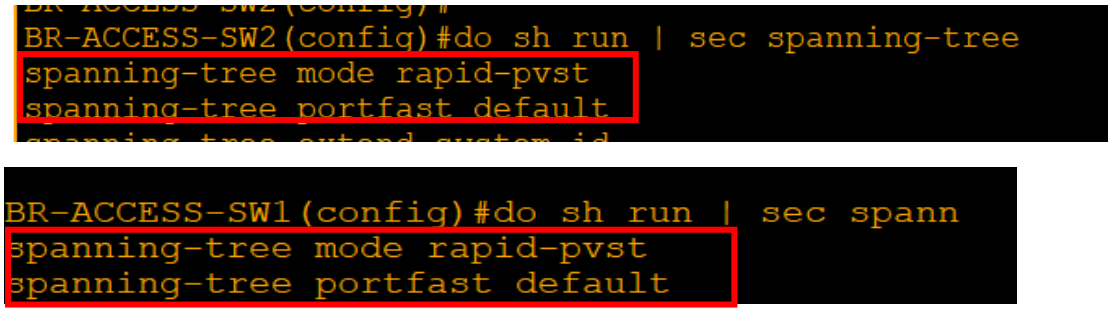


Figure 65: Enabling of rapid-pvst and portfast in BR-ACCESS-SW1 and BR-ACCESS-SW2

BR-DISTRI-SW1 & BR-DISTRI-SW2

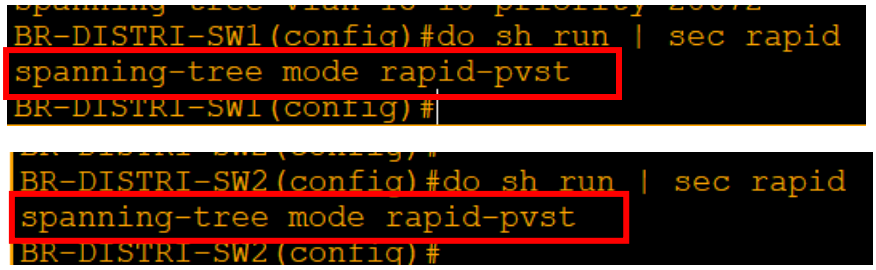


Figure 66: Running config of enabling rapid-pvst in BR-DISTRI-SW1 and BR-DISTRI-SW2

BR-DATA-SW

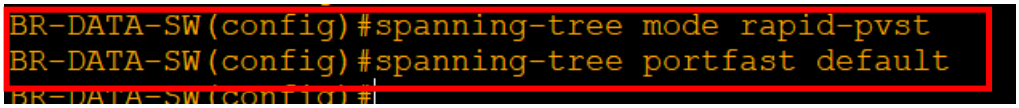


Figure 67: Enabling rapid-pvst and portfast in BR-DATA-SW

EtherChannel

Consider a scenario where the volume of end-user data surpasses the link's capacity for data transfer, leading to prolonged data transfer times and potential queuing. In response to this, EtherChannel is introduced at this layer, allowing the aggregation of multiple physical links up to 8 into a single logical link. This logical link operates as a unified, high-speed bandwidth which help to reduce fault tolerance and optimize the network performance.

LACP over PAGP

In simpler terms, both LACP and PAGP are used for link aggregation, where multiple physical links are combined into a single logical link. However, LACP is an open standard that offers flexibility and compatibility across different vendors devices. PAGP is designed specifically for Cisco equipment and is commonly implemented only in Cisco-centric setups. In scenarios involving devices from different manufacturers, LACP is typically the more favorable options.

HQ-DISTRI-SW1 & HQ-DISTRI-SW2

```
HQ-DISTRI-SW1(config)#do sh etherchannel summ
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------

4      Po4(SU)           LACP    Gig1/0/2(P) Gig1/0/4(P) Gig1/0/8(P)
HQ-DISTRI-SW1(config)#
```

Figure 68: Summary of ether-channel configuration in HQ-DISTRI-SW1

```
HQ-DISTRI-SW2(config)#do sh etherchannel summ
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------

4      Po4(SU)           LACP    Gig1/0/2(P) Gig1/0/4(P) Gig1/0/8(P)
HQ-DISTRI-SW2(config)#
```

Figure 69: Summary of ether-channel configuration in HQ-DISTRI-SW2

BR-DISTRI-SW1 & BR-DISTRI-SW2

```
BR-DISTRI-SW1#sh etherchannel summ
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 3
Number of aggregators:           3

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------

1      Po1(SU)           LACP   Gig1/0/5(P) Gig1/0/6(P) Gig1/0/7(P)
2      Po2(SU)           LACP   Gig1/0/1(P) Gig1/0/2(P)
3      Po3(SU)           LACP   Gig1/0/3(P) Gig1/0/4(P)
```

Figure 70: Ether-channel configuration summary of BR-DISTRI-SW1

```
BR-DISTRI-SW2(config)#do sh etherchannel summ
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 3
Number of aggregators:           3

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------

1      Po1(SU)           LACP   Gig1/0/5(P) Gig1/0/6(P) Gig1/0/7(P)
4      Po4(SU)           LACP   Gig1/0/1(P) Gig1/0/2(P)
5      Po5(SU)           LACP   Gig1/0/3(P) Gig1/0/4(P)
```

Figure 71: Summary of ether-channel configuration of BR-DISTRI-SW2

BR-ACCESS-SW1 & BR-ACCESS-SW2

```
BR-ACCESS-SW1#sh etherchannel summ
Flags:   D - down        P - in port-channel
         I - stand-alone s - suspended
         H - Hot-standby (LACP only)
         R - Layer3      S - Layer2
         U - in use      f - failed to allocate aggr
         u - unsuitable for bundling
         w - waiting to be aggregated
         d - default port


Number of channel-groups in use: 2
Number of aggregators:           2

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-------------------

2      Po2(SU)           LACP    Fa0/1(P) Fa0/2(P)
4      Po4(SU)           LACP    Fa0/3(P) Fa0/4(P)
```

Figure 72: Ether-channel configuration summary of BR-ACCESS-SW1

```
BR-ACCESS-SW2(config)#do sh etherchannel summ
Flags:   D - down        P - in port-channel
         I - stand-alone s - suspended
         H - Hot-standby (LACP only)
         R - Layer3      S - Layer2
         U - in use      f - failed to allocate aggregator
         u - unsuitable for bundling
         w - waiting to be aggregated
         d - default port


Number of channel-groups in use: 2
Number of aggregators:           2

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------

3      Po3(SU)           LACP    Fa0/1(P) Fa0/2(P)
5      Po5(SU)           LACP    Fa0/3(P) Fa0/4(P)
BR-ACCESS-SW2(config)#
```

Figure 73: Ether-channel summary of BR-ACCESS-SW2

Redundancy Gateway with SVI (Switched Virtual Interface)

SVI in distribution layer is used as gateways and redundancy gateway for different VLANs.

HSRP (Host Standby Routing Protocol)

Setting up a redundant gateway for each department is a critical aspect of designing and implementing a network topology. In Cisco Packet Tracer, HSRP is the available option. In this setup, one l3 device acts as the active gateway, while the other serves as the standby gateway, collectively creating a virtual IP to ensure continuous network availability

Department Name	**Gateways**		**Virtual IP**
	Active	**Standby**	
Marketing	172.16.200.1	172.16.200.2	172.16.200.3
Sales	172.16.200.129	172.16.200.130	172.16.200.131
Help Line	172.16.200.193	172.16.200.194	172.16.200.195
IT Help Desk	172.16.200.225	172.16.200.226	172.16.200.227
Remote Support	172.16.201.2	172.16.200.1	172.16.200.3
Team Leader	172.16.201.18	172.16.201.17	172.16.200.19
Admin	172.16.201.34	172.16.201.33	172.16.201.35
HR	172.16.201.50	172.16.201.49	172.16.201.51
Management	192.168.1.1	192.168.1.2	192.168.1.3
Guest	10.2.0.1	10.2.0.2	10.2.0.3

*Table **5:** Gateway and virtual IP with HSRP of Headquarter*

Department Name	**Gateway**		**Virtual IP**
	Active	**Standby**	
Marketing	192.168.10.1	192.168.10.2	192.168.10.3
Sales	192.168.10.129	192.168.10.130	192.168.10.131
Help Line	192.168.10.193	192.168.10.194	192.168.10.195
IT Help Desk	192.168.10.225	192.168.10.226	192.168.10.227
Remote Support	192.168.11.2	192.168.11.1	192.168.11.3
Team Leader	192.168.11.18	192.168.11.17	192.168.11.19
Admin	192.168.11.34	192.168.11.33	192.168.11.35
HR	192.168.11.50	192.168.11.49	192.168.11.51
Management	172.16.254.1	172.16.254.2	172.16.254.3
Guest	10.1.0.2	10.1.0.1	10.1.0.3

*Table 6**:** Gateway and virtual IP with HSRP of Branch*

Department Name	**Gateway**		**Virtual IP**
	Active	**Standby**	
Data Center (HQ)	192.168.254.1	192.168.254.2	192.168.254.254
	10.10.10.2	10.10.10.1	10.10.10.254
Data Center (BR)	172.16.100.1	172.16.100.2	172.16.100.254
DMZ	80.88.88.1	80.88.88.2	80.88.88.3

Table 6: Redundancy in data center of HQ, Branch and DMZ

Department	**Gateway**		**Virtual IP**
	Active	**Standby**	
DNS	8.8.8.1	8.8.8.2	8.8.8.3
NTP	216.239.35.1	216.239.35.2	216.239.35.3
WEB	142.250.183.1	142.250.183.2	142.250.183.3

Table 7: HSRP in google server

Load Balancing by HSRP

Directing all traffic through a single device can lead to high load management, elevated CPU and memory usage, and having one device on standby may not be practical in real-world scenarios. To address this, it's essential to implement traffic load balancing from end devices. In HSRP, two methods are available for load balancing: synchronizing HSRP with STP and using HSRP groups.

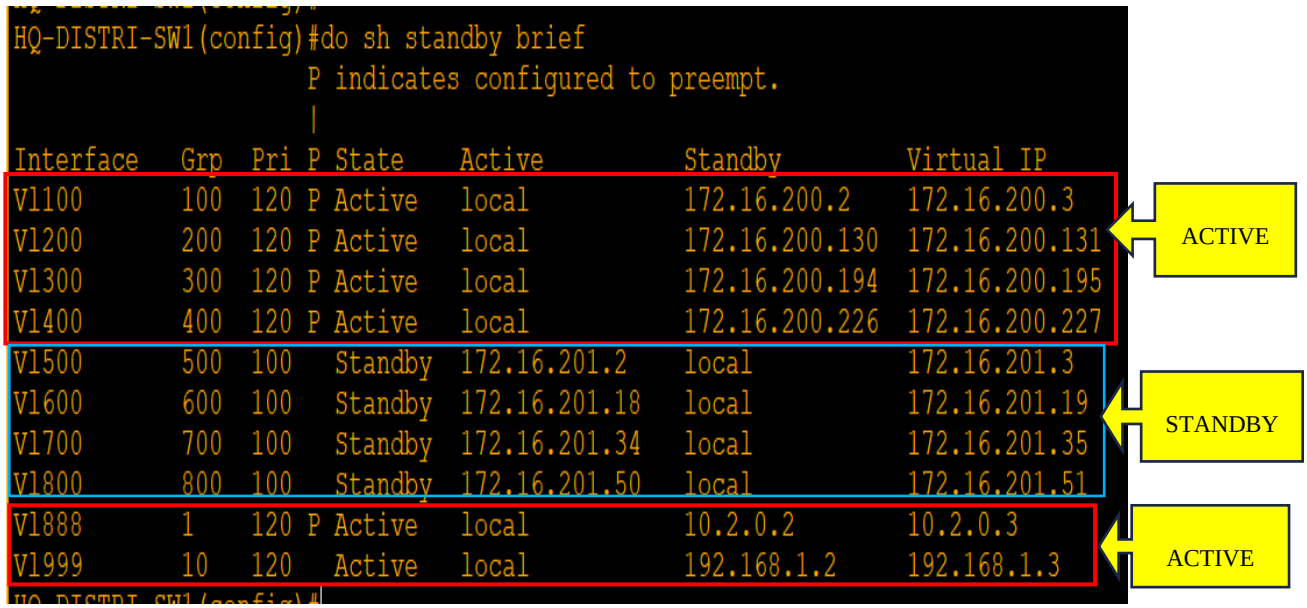


Figure 74: HSRP load balancing in HQ-DISTRI-SW1

Figure

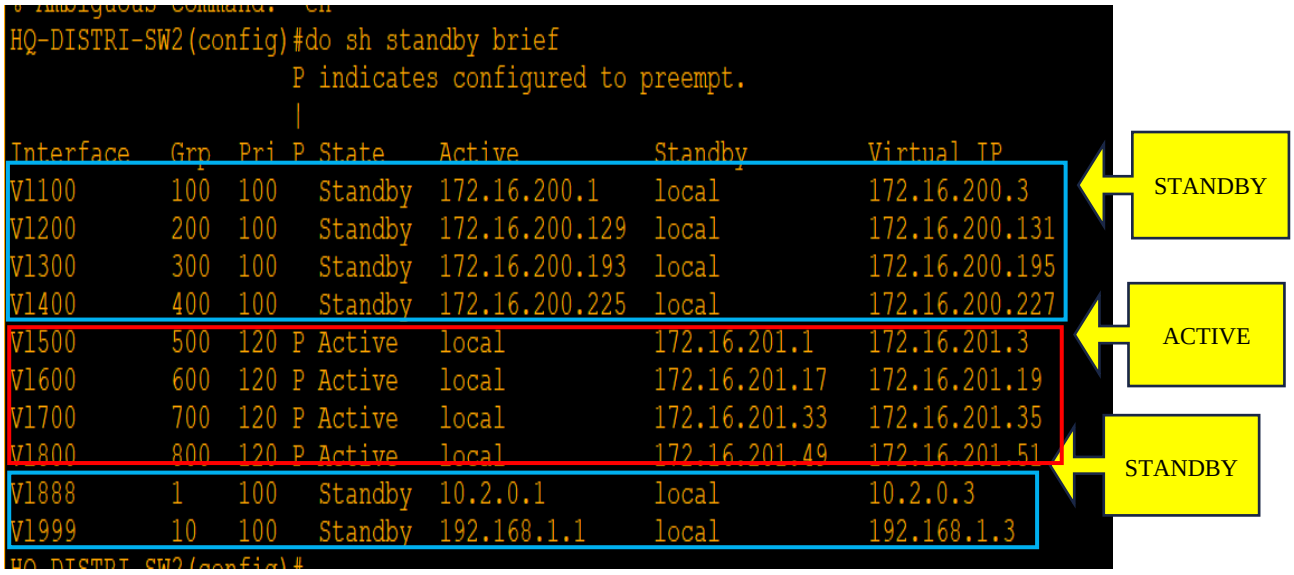


Figure 75: HSRP load balancing in HQ-DISTRI-SW2

Synchronizing HSRP with STP

```
HQ-DISTRI-SW1(config)#spanning-tree vlan 100,200,300,400,888 root primary
HQ-DISTRI-SW1(config)#spanning-tree vlan 500,600,700,800,999 root secondary
HQ-DISTRI-SW1(config)#
```

Figure 76: Root bridge configuration for each VLAN in HQ-DISTRI-SW

VLAN 100,200,300,400,888 are selected root bridge of HQ-DISTRI-SW1 whereas VLAN 500,600,700,800,999 are selected as secondary with lower priority, so all of the root primary data follows from HQ-DISTRI-SW1 until and unless redundant link are down.

```
HQ-DISTRI-SW2(config)#spanning-tree vlan 100,200,300,400,888 root secondary
HQ-DISTRI-SW2(config)#spanning-tree vlan 500,600,700,800,999 root primary
```

Figure 77: Root bridge configuration for each VLAN in HQ-DISTRI-SW2

VLAN 500,600,700,800,999 are selected as root bridge of HQ-DISTRI whereas VLAN 100, 200,300, 400,888 are selected as secondary with lower priority. So, the data of root primary only flow through HQ-DISTRI-SW2 until and unless redundant link are down. For branch same HSRP are implemented with same configuration with VLANs from **Table 2** and SVI from **Table 6** are used.

VTP and trunk port

Configuring and managing VLANs in each switch in network topology can be a challenging, particularly in large network. The manual process of creating VLANs on individual switches increases the error and can be time consuming. To address this kind of issue, VLAN trunking Protocol (VTP) is implemented on Cisco devices for manipulation and synchronization of VLANs information across switches. The process is centralized with a designated VTP server which revision number is higher than other switches within a same VTP domain. VTP information on different switches are carried out through the trunk port.

If there is multiple VLANs in network topology, the link connected to other devices like router, switches configured in trunk mode because it allows link to carry different VLAN information by tagging VLAN header within Ethernet frame. This tagging mechanism helps to identify VLANs information to which each frame belongs. Native VLAN also change for preventing VLAN hooping attacks.

Headquarter

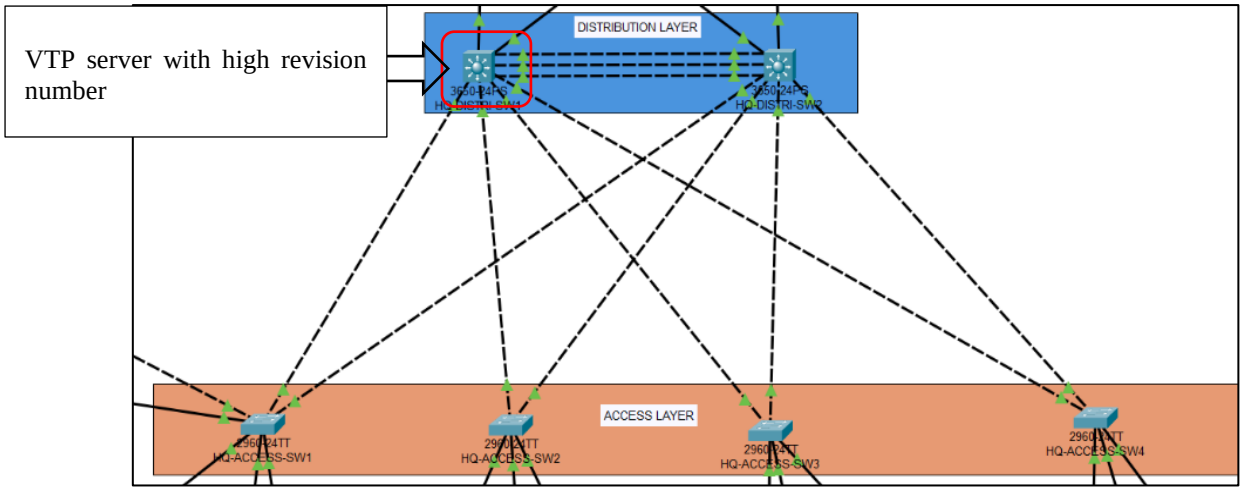


*Figure 78: **L2** and **L3** switches of headquarter*

VTP domain and password are configured for authentication on switches so, the VLANs information are synchronized through trunk link by authentication.

```
HQ-DISTRI-SW1(config)#vtp version 2
VTP mode already in V2.
HQ-DISTRI-SW1(config)#vtp domain nihangchha.com
Domain name already set to nihangchha.com.
HQ-DISTRI-SW1(config)#vtp password nihangchha
Password already set to nihangchha
```

Figure 79: Configuration of VTP version 2

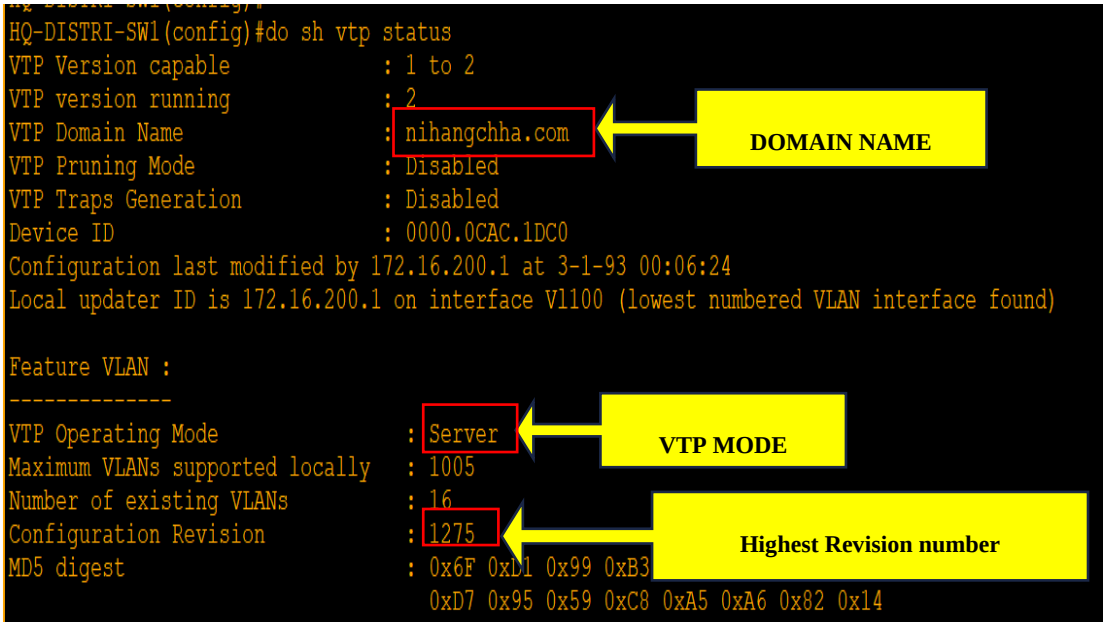


Figure 80: VTP status of HQ-DISTRI-SW1

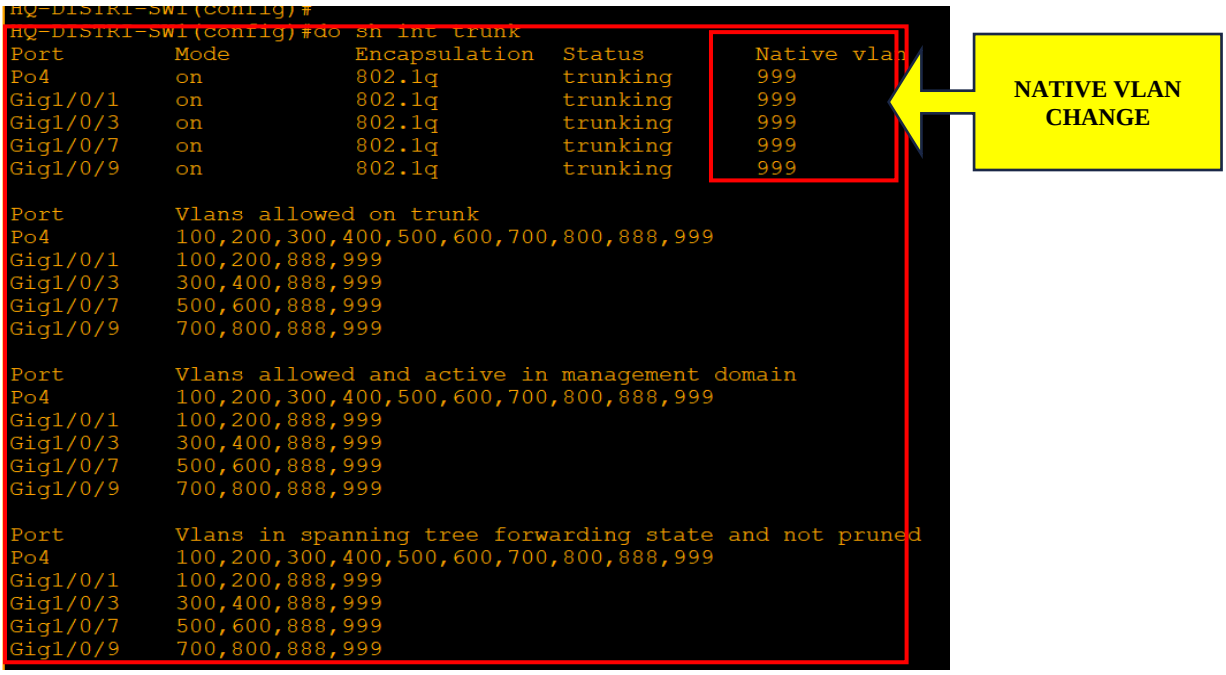


Figure 81:Trunking information of HQ-DISTRI-SW1

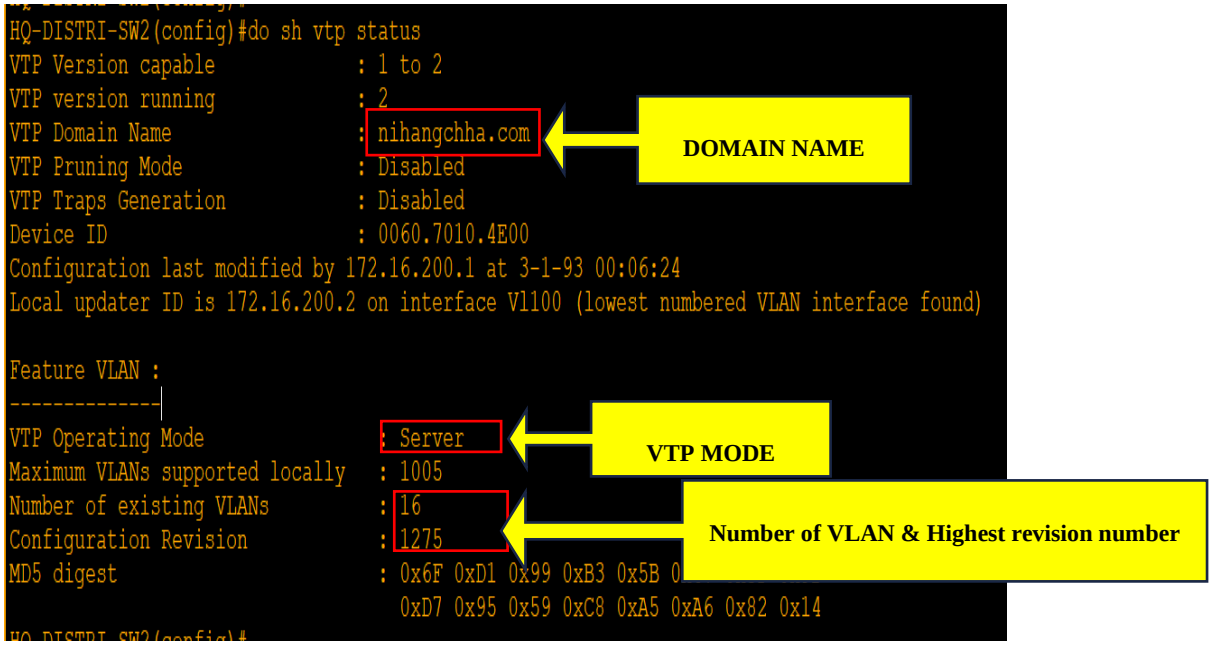


Figure 82: VTP status in HQ-DISTRI-SW2

From the above figures 80, 81 & 82, VLAN information are synchronized through trunk port.

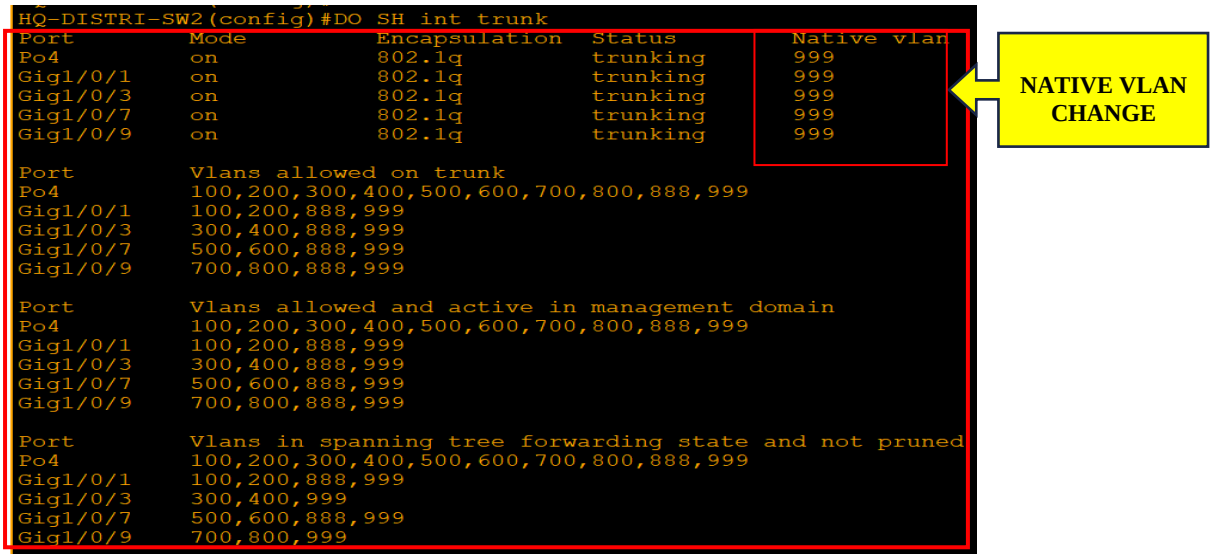


Figure 83: Trunking information of HQ-DISTRI-SW2

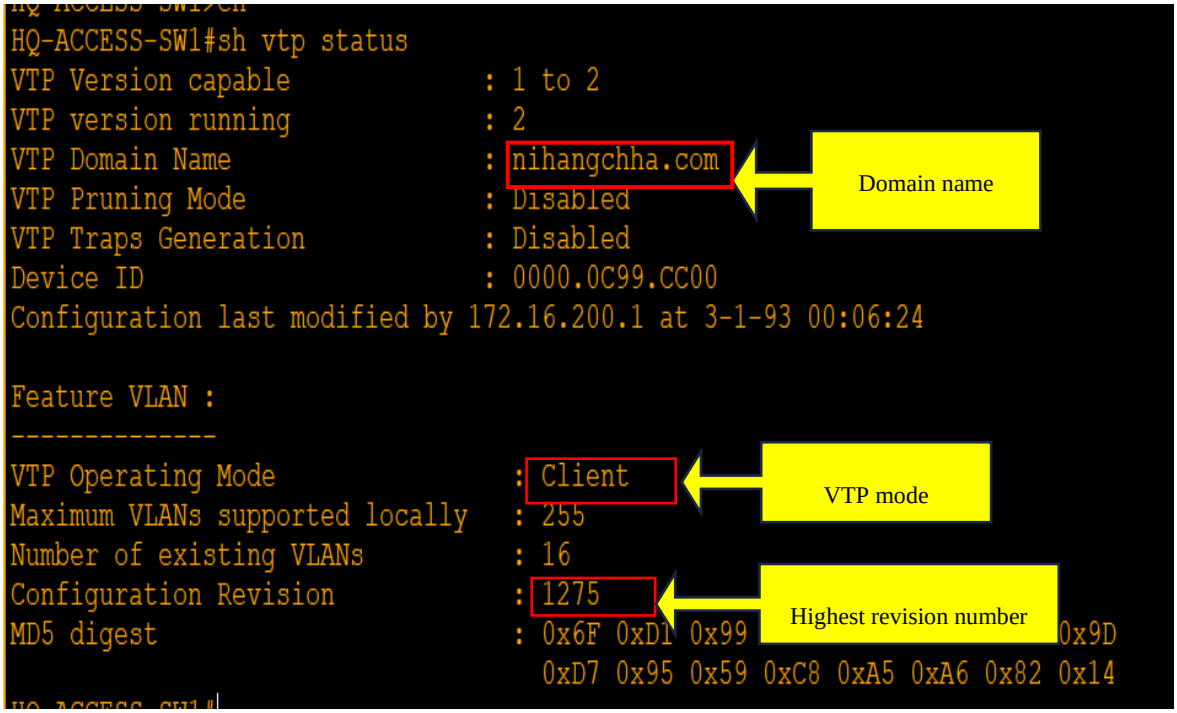


Figure 84: VTP status of HQ-ACCESS-SW1

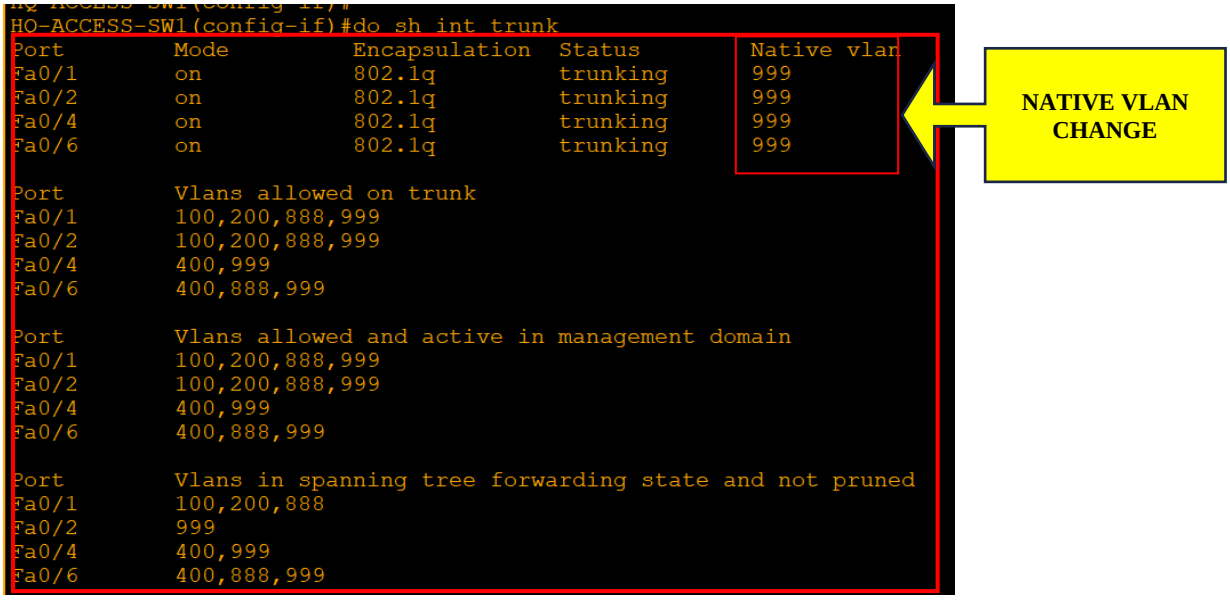


Figure 85: Trunking information of HQ-ACCESS-SW1

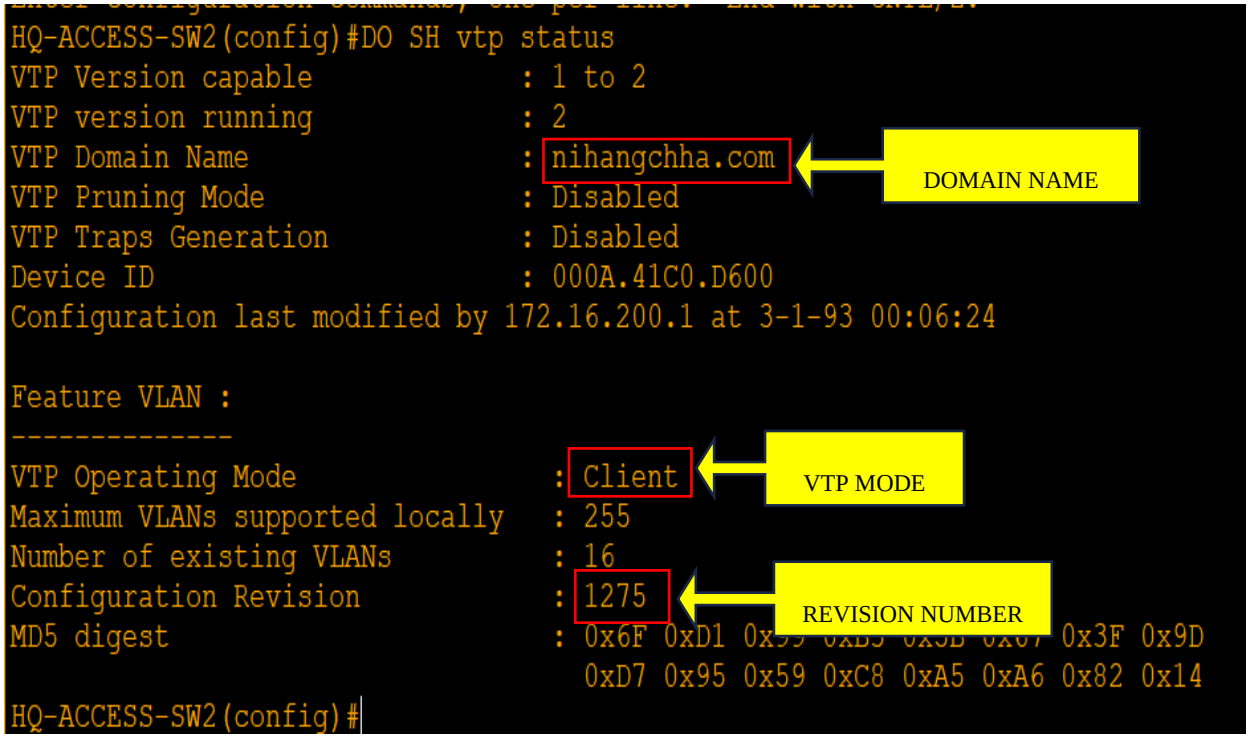


Figure 86: VTP status of HQ-ACCESS-SW2

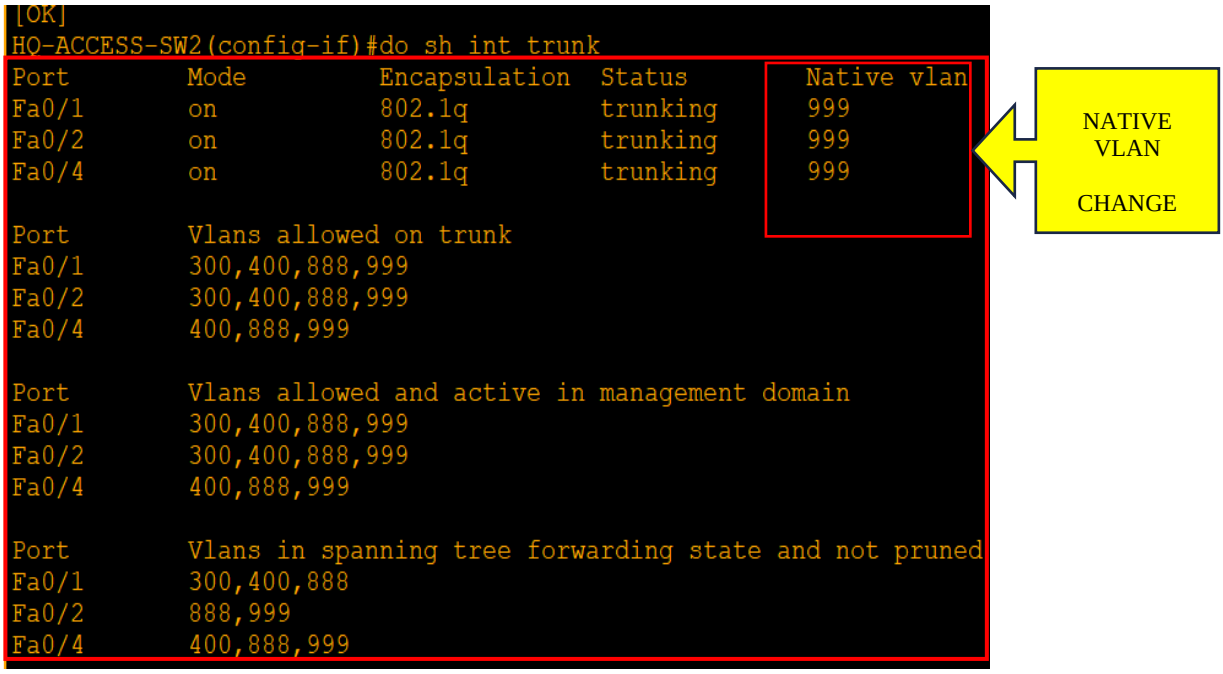


Figure 87: Trunk information of HQ-ACCESS-SW2

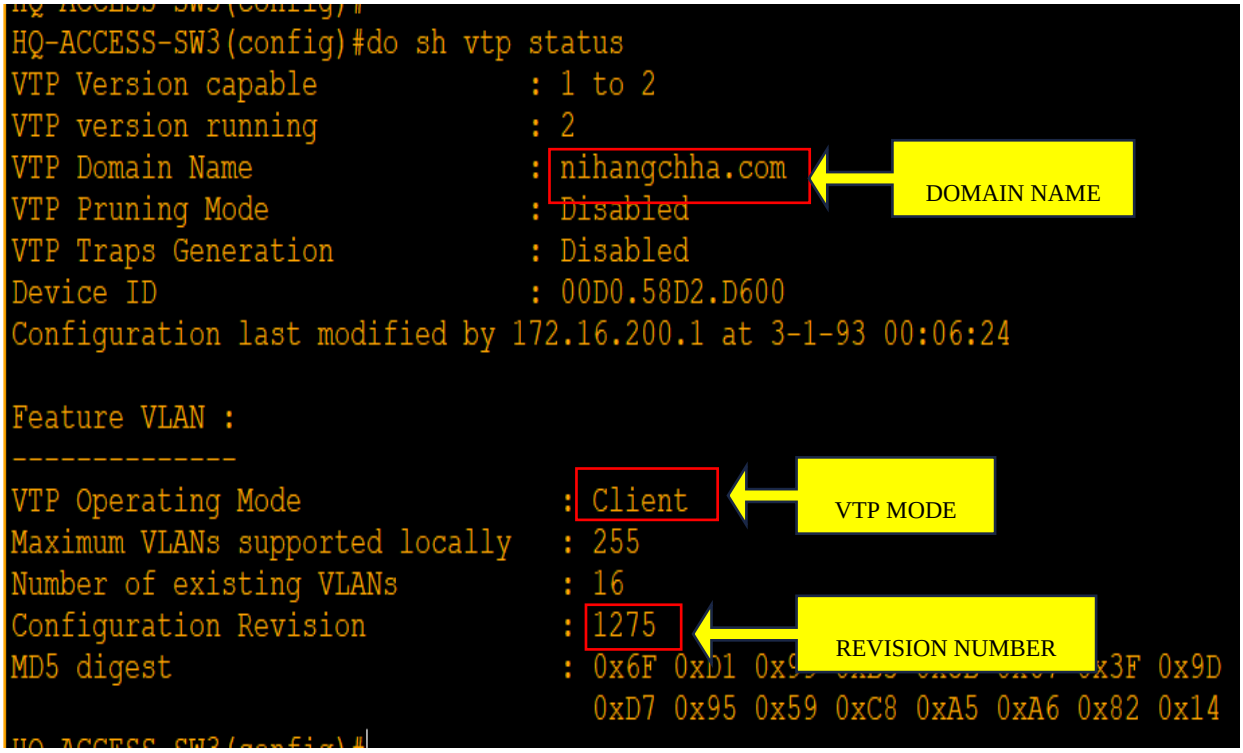


Figure 88: VTP status on HQ-ACCESS-SW3

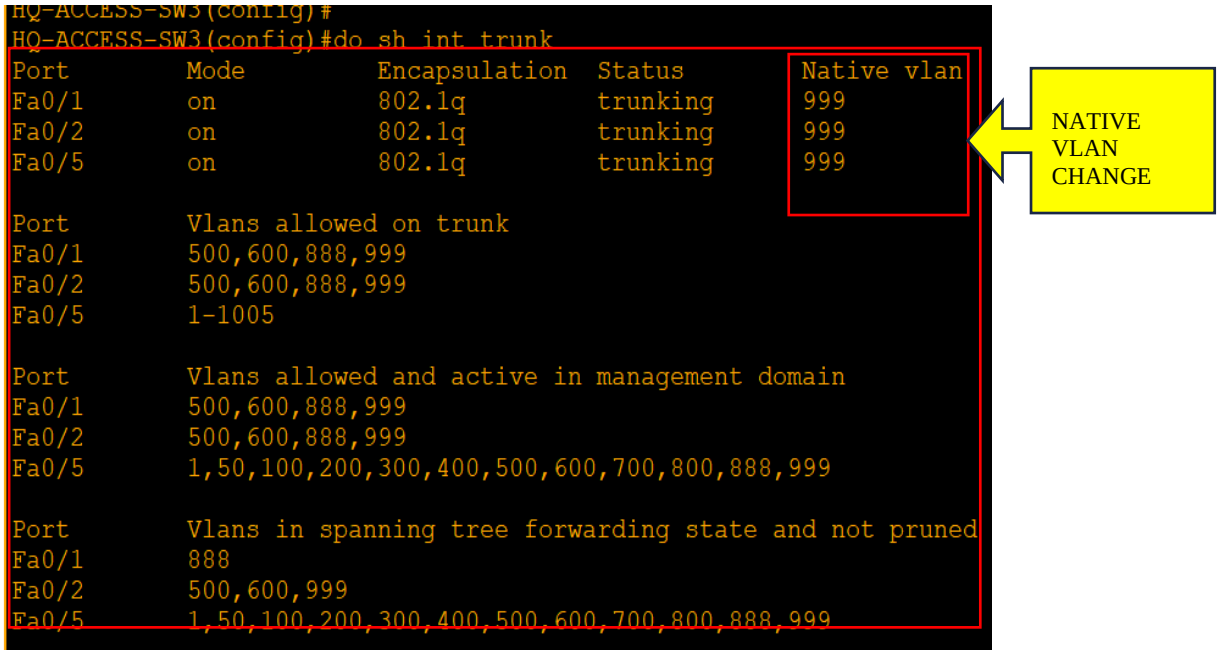


Figure 89: Trunk mode on HQ-ACCESS-SW3

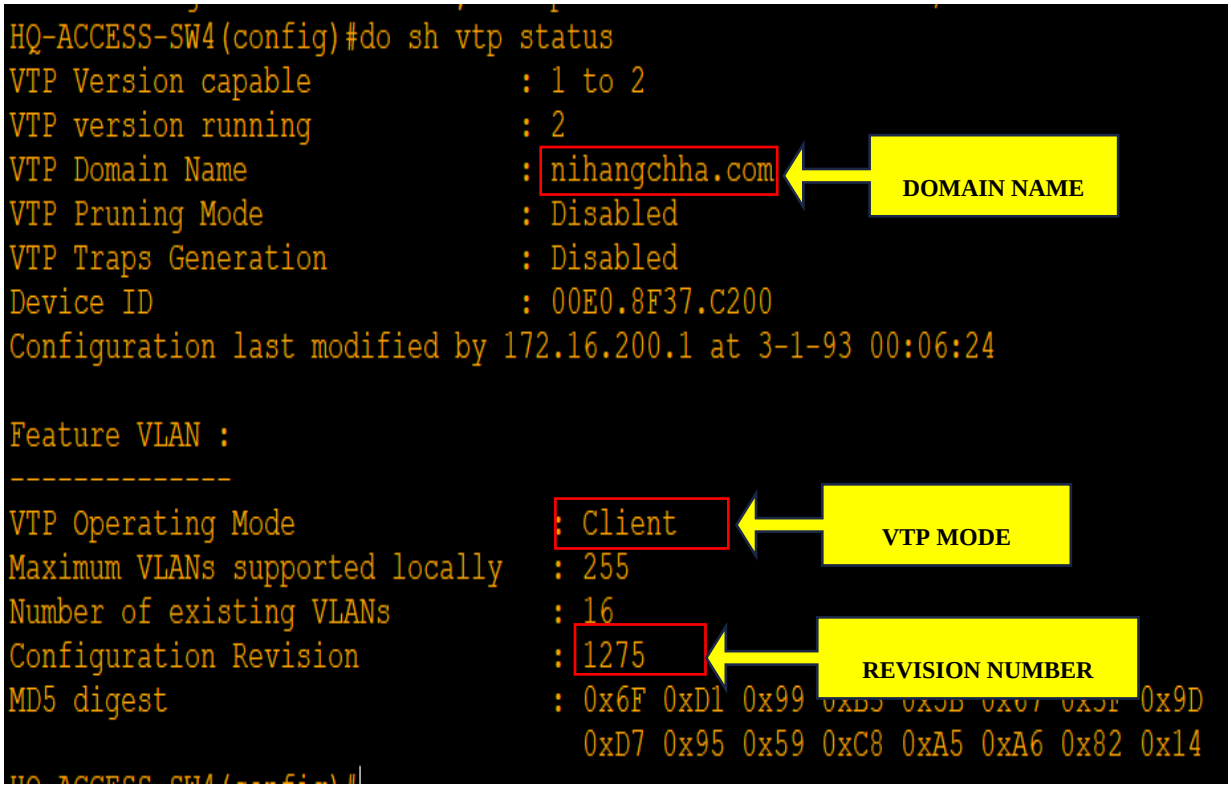


Figure 90: TP status on HQ-ACCESS-SW4

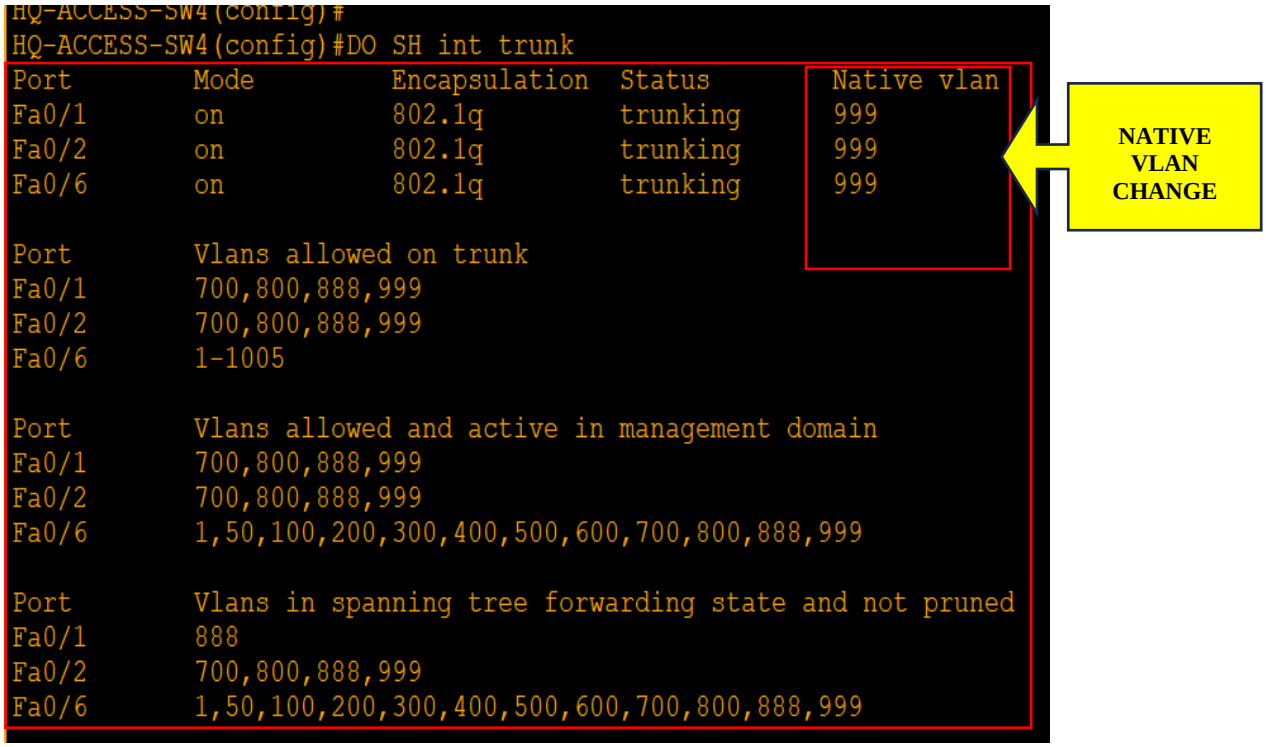


Figure 91: Trunking mode on HQ-ACCESS-SW4

Branch

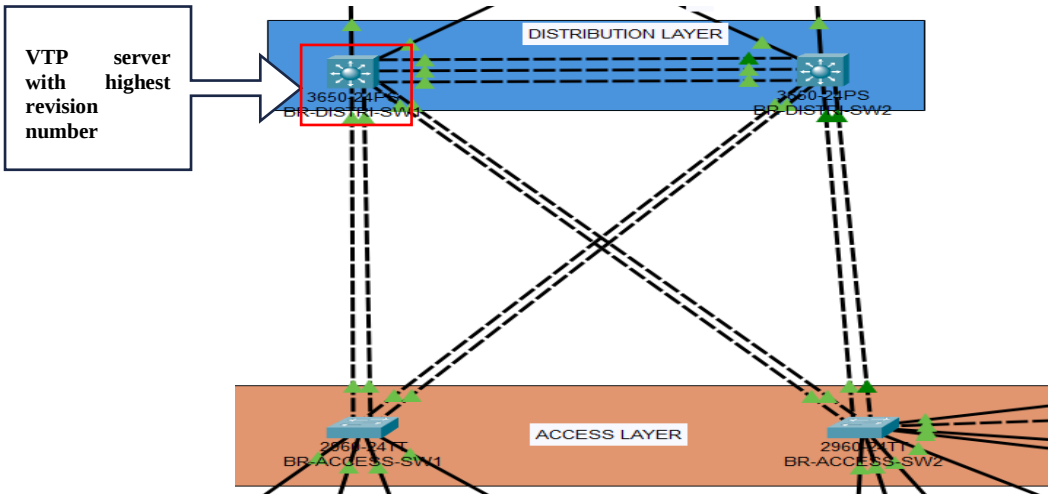


Figure 92: L3 and L2 switches of branch

```
BR-DISTRI-SW1(config)#do sh vtp status
VTP Version capable             : 1 to 2
VTP version running             : 2
VTP Domain Name                 : nihangchha.com
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : 0003.E451.2590
Configuration last modified by 0.0.0.0 at 3-1-93 00:00:00
Local updater ID is 192.168.10.1 on interface Vl11 (lowest numbered VLAN interface found)

Feature VLAN :
--------------
VTP Operating Mode              : Server
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 15
Configuration Revision          : 1191
MD5 digest                      : 0x87 0x0A 0xE2 0x01 0x10 0xD0 0x20 0xE0
                                  0x04 0xA9 0xD9 0xF9 0x30 0xA1 0x77 0xCB
BR-DISTRI-SW1(config)#
```

DOMAIN NAME

VTP MODE

REVISION NUMBER

Figure 93: VTP status of BR-DISTRI-SW1

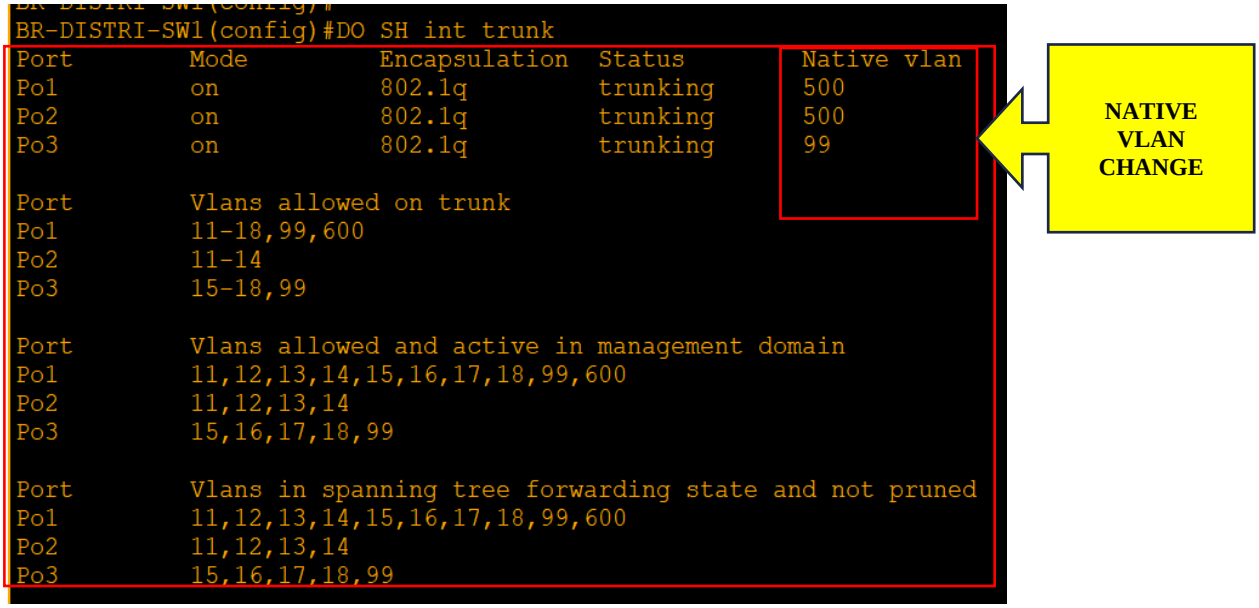


Figure 94: Trunking information of BR-DISTRI-SW1

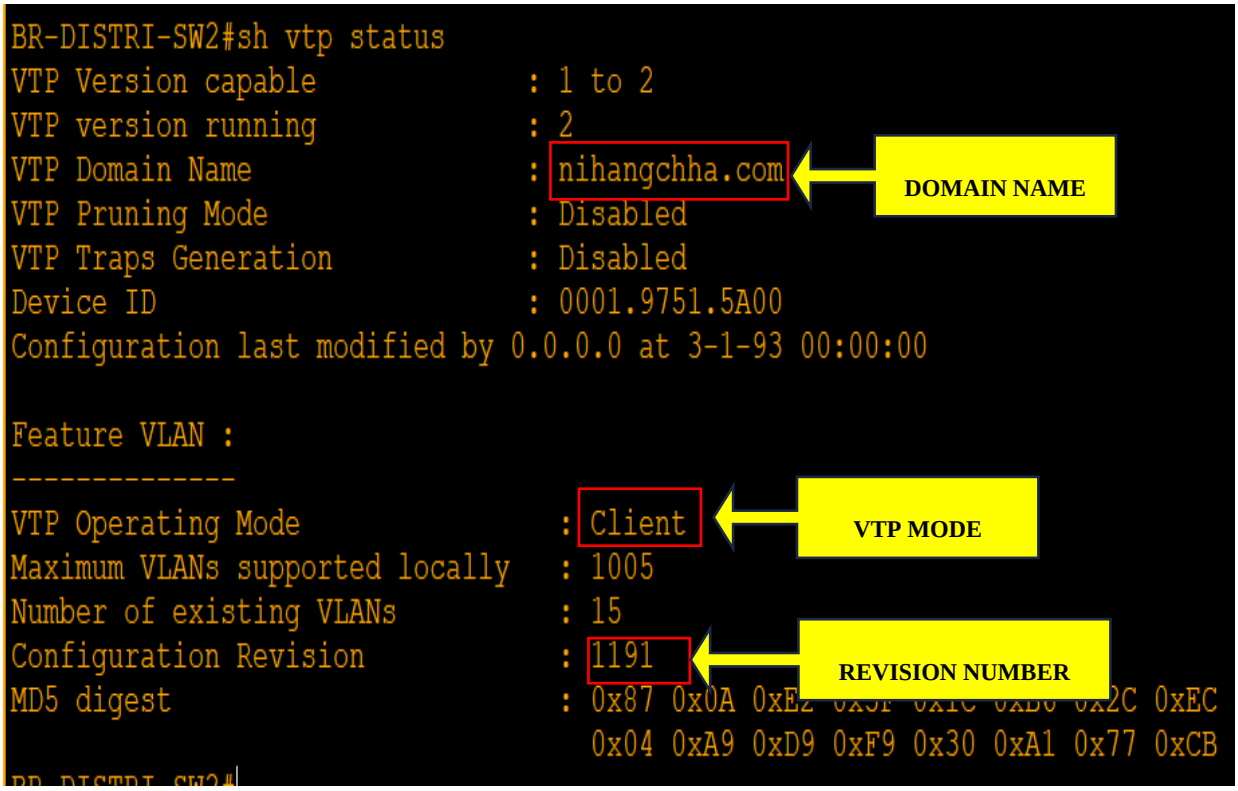


Figure 95: VTP status of BR-DISTRI-SW2

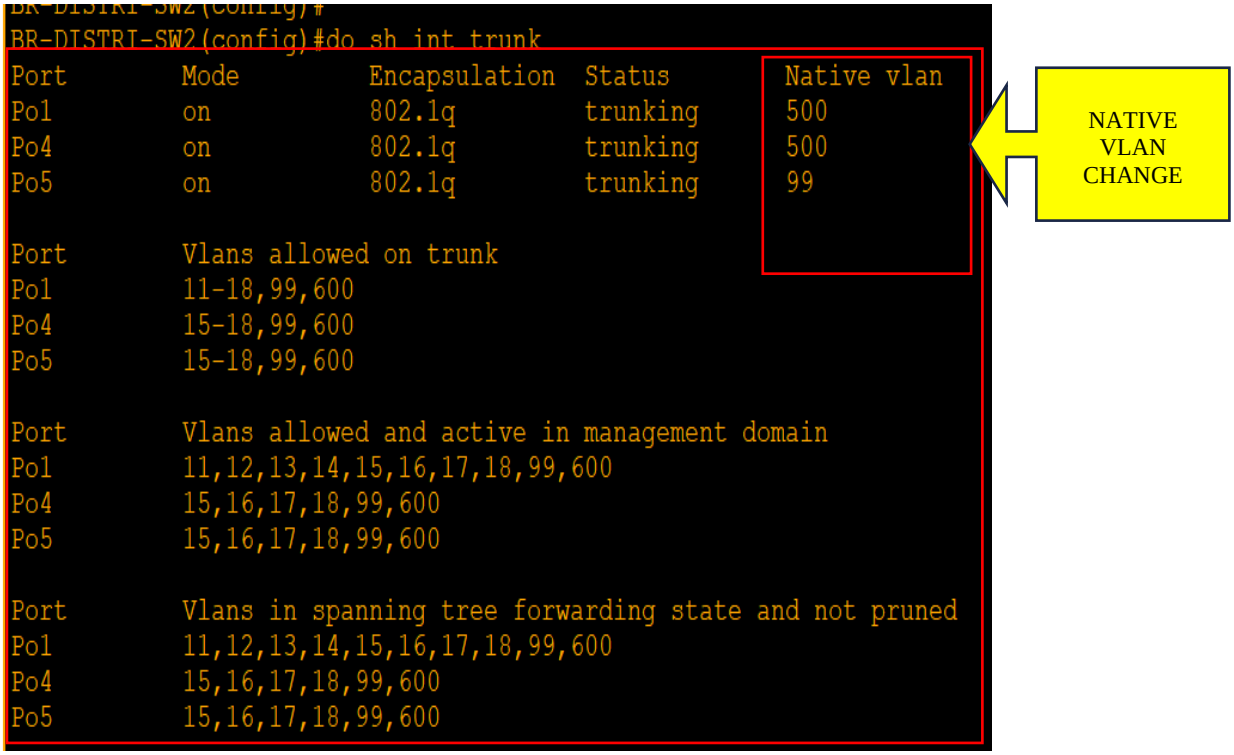


Figure 96: Trunking information of BR-DISTRI-SW2

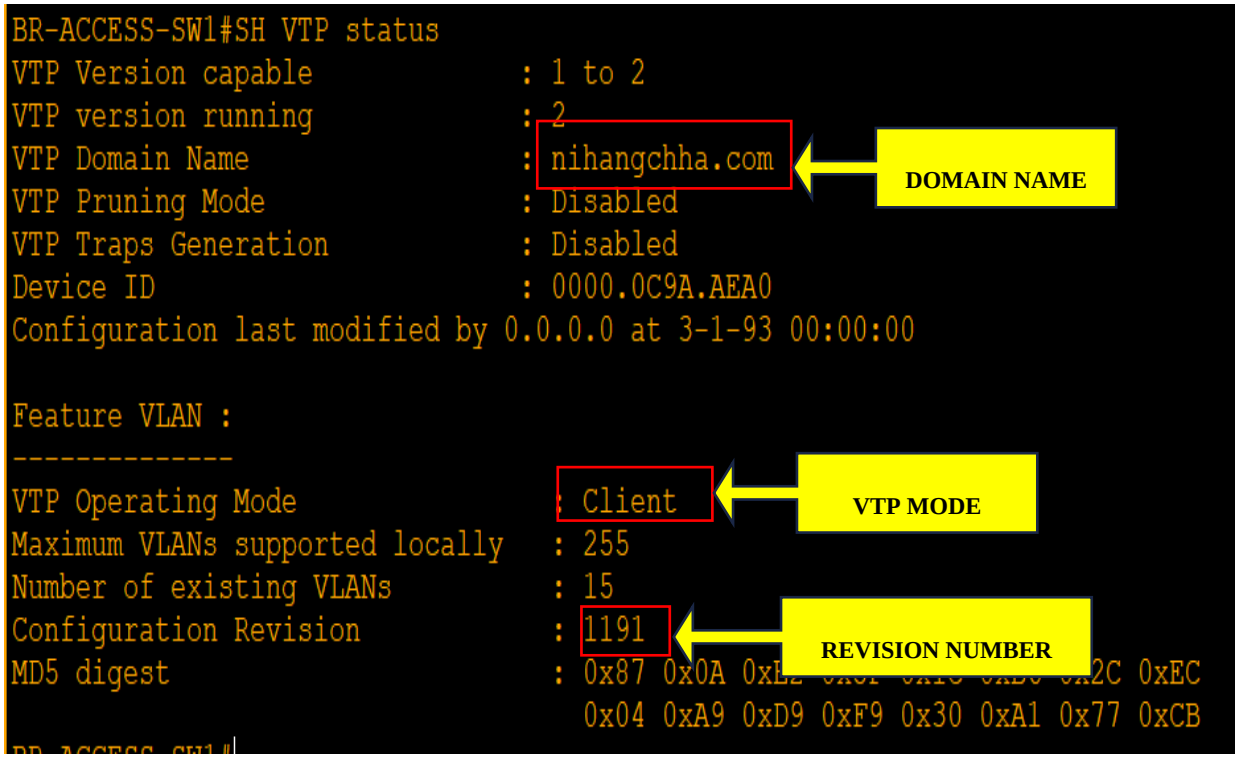


Figure 97: VTP status of BR-ACCESS-SW1

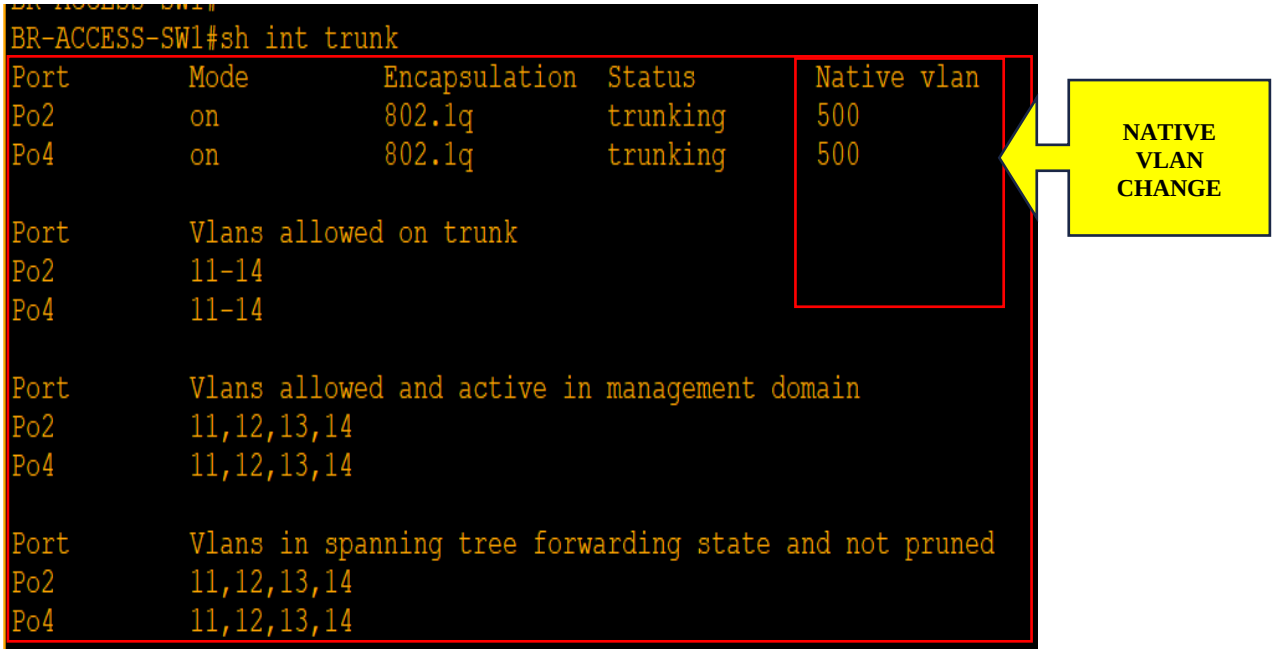


Figure 98: Trunking information of BR-ACCESS-SW1

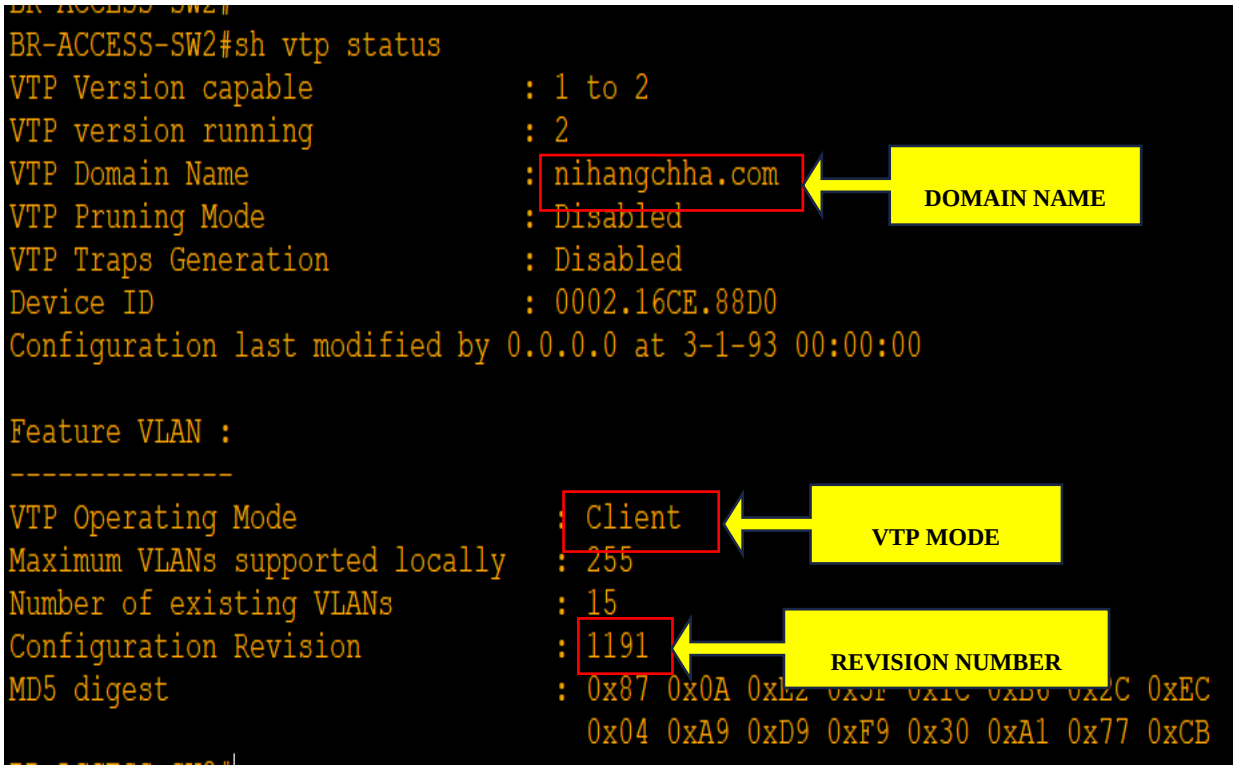


Figure 99: VTP status of BR-ACCESS-SW2

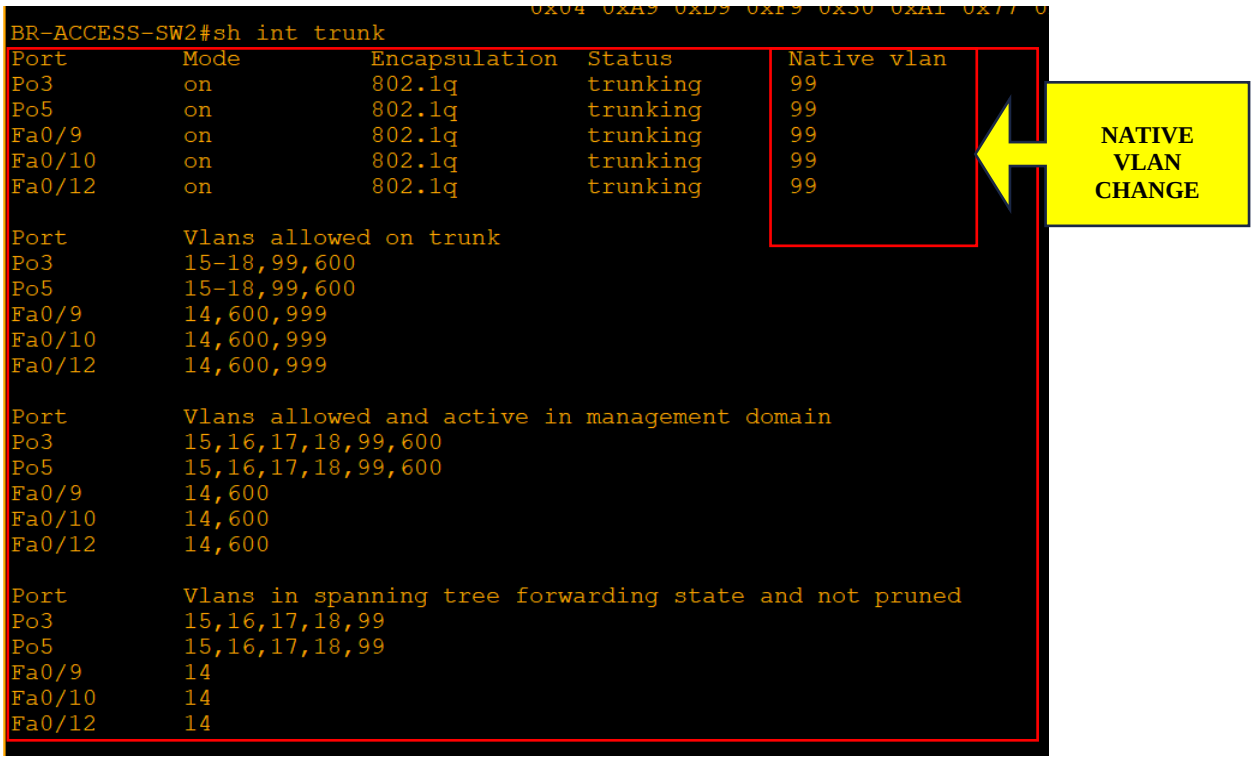


Figure 100: Trunking information of BR-ACCESS-SW2

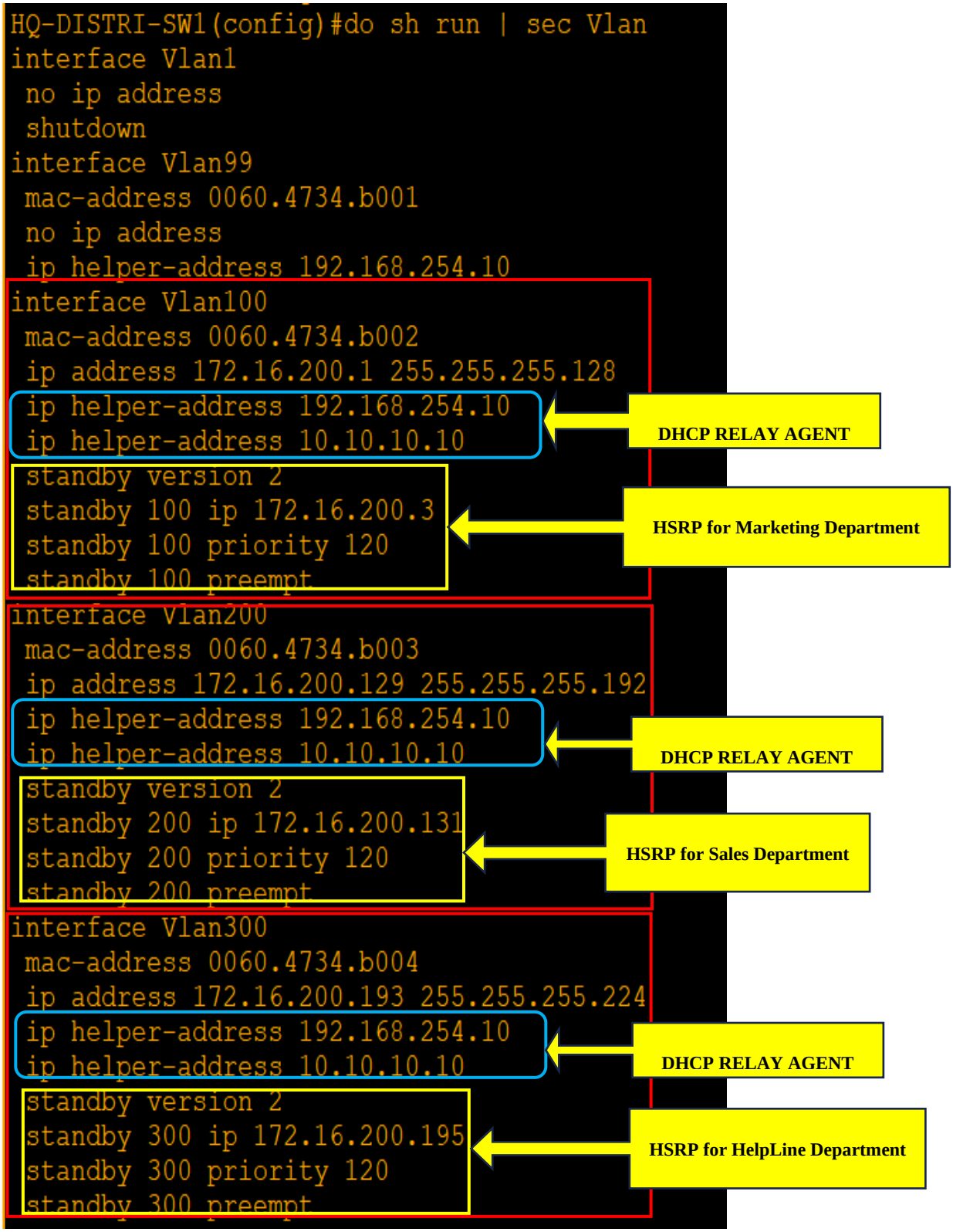
DHCP (Dynamic Host Configuration Protocol)

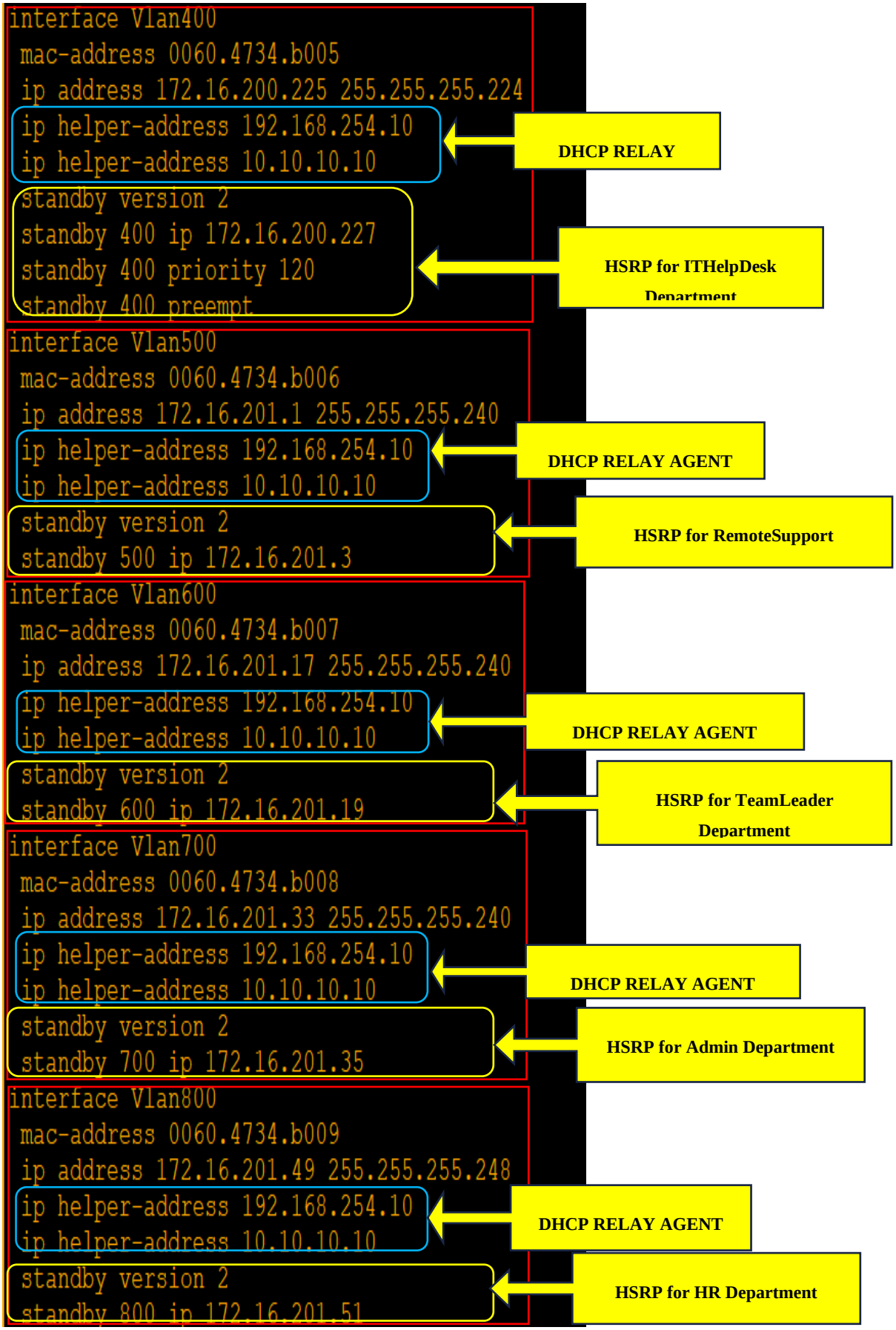
Assigning IP addresses statically to end devices may work well in small companies, but it becomes impractical in larger organizations where the number of users accessing the Internet can reach thousands. In such scenarios, DHCP becomes essential as it automates the process of assigning IP addresses to devices.

HEADQUARTER

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
Sales	172.16.200.131	80.88.88.4	172.16.200.131	255.255.255.192	50	0.0.0.0	192.168.1.4
HR	172.16.201.51	80.88.88.4	172.16.201.52	255.255.255.248	3	0.0.0.0	192.168.1.4
Admin	172.16.201.35	80.88.88.4	172.16.201.36	255.255.255.240	5	0.0.0.0	192.168.1.4
TeamLeader	172.16.201.19	80.88.88.4	172.16.201.20	255.255.255.240	6	0.0.0.0	192.168.1.4
RemoteSupport	172.16.201.3	80.88.88.4	172.16.201.4	255.255.255.240	10	0.0.0.0	192.168.1.4
Marketing	172.16.200.3	8.8.8.8	172.16.200.4	255.255.255.128	65	0.0.0.0	192.168.1.4
HelpLine	172.16.200.195	80.88.88.4	172.16.200.196	255.255.255.224	25	0.0.0.0	192.168.1.4
GUEST	10.2.0.3	80.88.88.4	10.2.0.4	255.255.252.0	1000	0.0.0.0	192.168.1.4
THelpDesk	172.16.200.227	80.88.88.4	172.16.200.225	255.255.255.224	15	0.0.0.0	192.168.1.4
Management(WLC) | access-point	192.168.1.3	80.88.88.4	192.168.1.4	255.255.255.240	12	0.0.0.0	192.168.1.4
serverPool	0.0.0.0	0.0.0.0	192.168.254.0	255.255.255.0	512	0.0.0.0	0.0.0.0

Figure 101: DHCP configuration of each department in HQ server with DNS server and WLC address


HQ-DISTRI-SW1(config)#do sh run | sec Vlan
interface Vlan1
 no ip address
 shutdown
interface Vlan99
 mac-address 0060.4734.b001
 no ip address
 ip helper-address 192.168.254.10
interface Vlan100
 mac-address 0060.4734.b002
 ip address 172.16.200.1 255.255.255.128
 ip helper-address 192.168.254.10
 ip helper-address 10.10.10.10
 standby version 2
 standby 100 ip 172.16.200.3
 standby 100 priority 120
 standby 100 preempt
interface Vlan200
 mac-address 0060.4734.b003
 ip address 172.16.200.129 255.255.255.192
 ip helper-address 192.168.254.10
 ip helper-address 10.10.10.10
 standby version 2
 standby 200 ip 172.16.200.131
 standby 200 priority 120
 standby 200 preempt
interface Vlan300
 mac-address 0060.4734.b004
 ip address 172.16.200.193 255.255.255.224
 ip helper-address 192.168.254.10
 ip helper-address 10.10.10.10
 standby version 2
 standby 300 ip 172.16.200.195
 standby 300 priority 120
 standby 300 preempt
DHCP RELAY AGENT
HSRP for Marketing Department
DHCP RELAY AGENT
HSRP for Sales Department
DHCP RELAY AGENT
HSRP for HelpLine Department


interface Vlan400
mac-address 0060.4734.b005
ip address 172.16.200.225 255.255.255.224
ip helper-address 192.168.254.10
ip helper-address 10.10.10.10
standby version 2
standby 400 ip 172.16.200.227
standby 400 priority 120
standby 400 preempt
DHCP RELAY
HSRP for ITHelpDesk Department
interface Vlan500
mac-address 0060.4734.b006
ip address 172.16.201.1 255.255.255.240
ip helper-address 192.168.254.10
ip helper-address 10.10.10.10
standby version 2
standby 500 ip 172.16.201.3
DHCP RELAY AGENT
HSRP for RemoteSupport
interface Vlan600
mac-address 0060.4734.b007
ip address 172.16.201.17 255.255.255.240
ip helper-address 192.168.254.10
ip helper-address 10.10.10.10
standby version 2
standby 600 ip 172.16.201.19
DHCP RELAY AGENT
HSRP for TeamLeader Department
interface Vlan700
mac-address 0060.4734.b008
ip address 172.16.201.33 255.255.255.240
ip helper-address 192.168.254.10
ip helper-address 10.10.10.10
standby version 2
standby 700 ip 172.16.201.35
DHCP RELAY AGENT
HSRP for Admin Department
interface Vlan800
mac-address 0060.4734.b009
ip address 172.16.201.49 255.255.255.248
ip helper-address 192.168.254.10
ip helper-address 10.10.10.10
standby version 2
standby 800 ip 172.16.201.51
DHCP RELAY AGENT
HSRP for HR Department

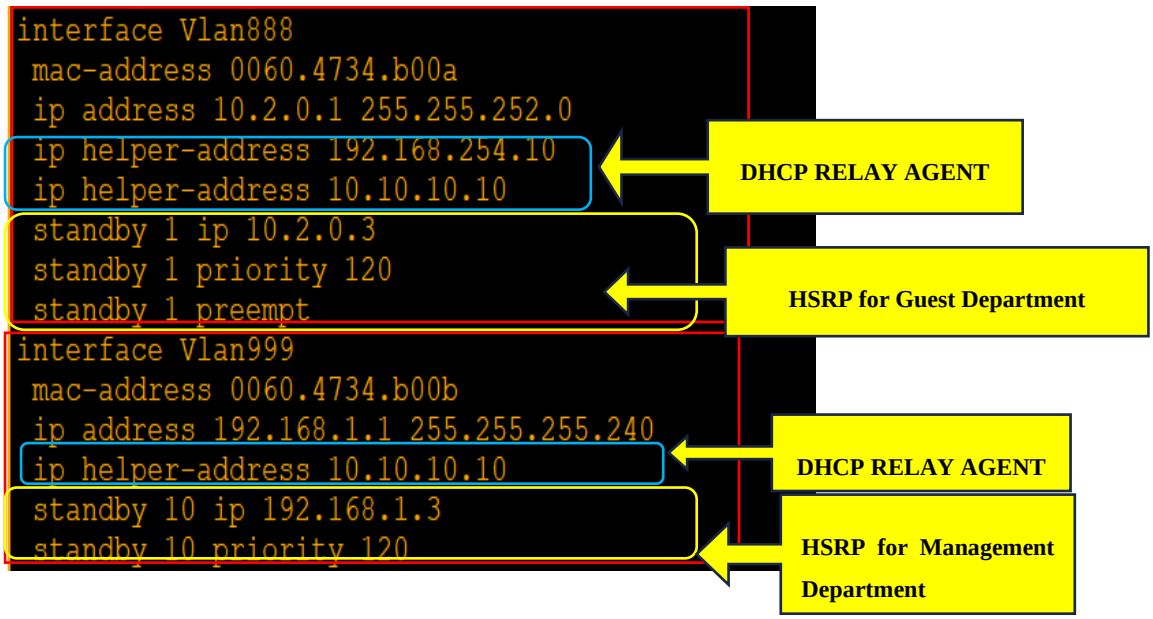


Figure 102: DHCP relay agent and HSRP of HQ

DHCP verification in headquarter

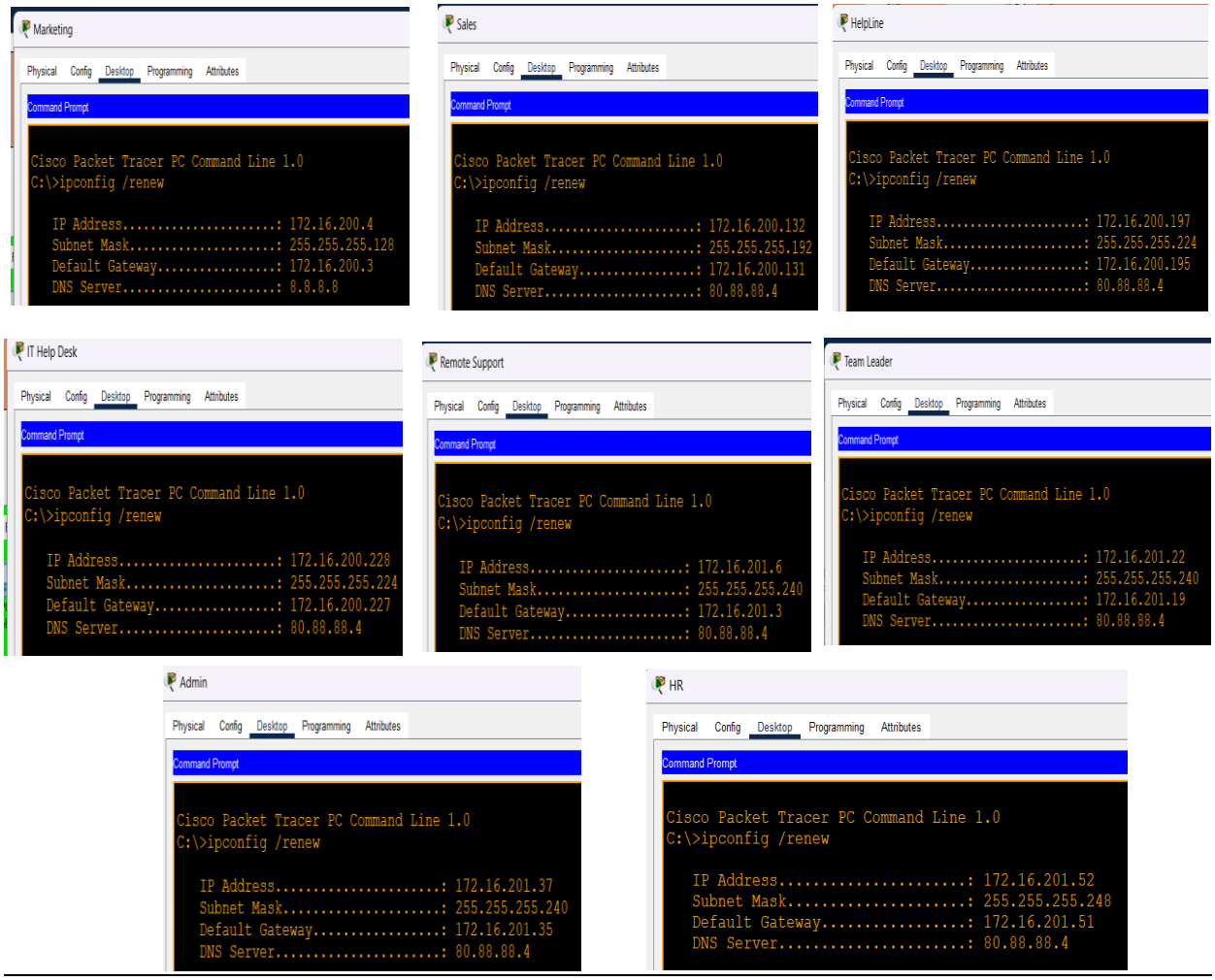
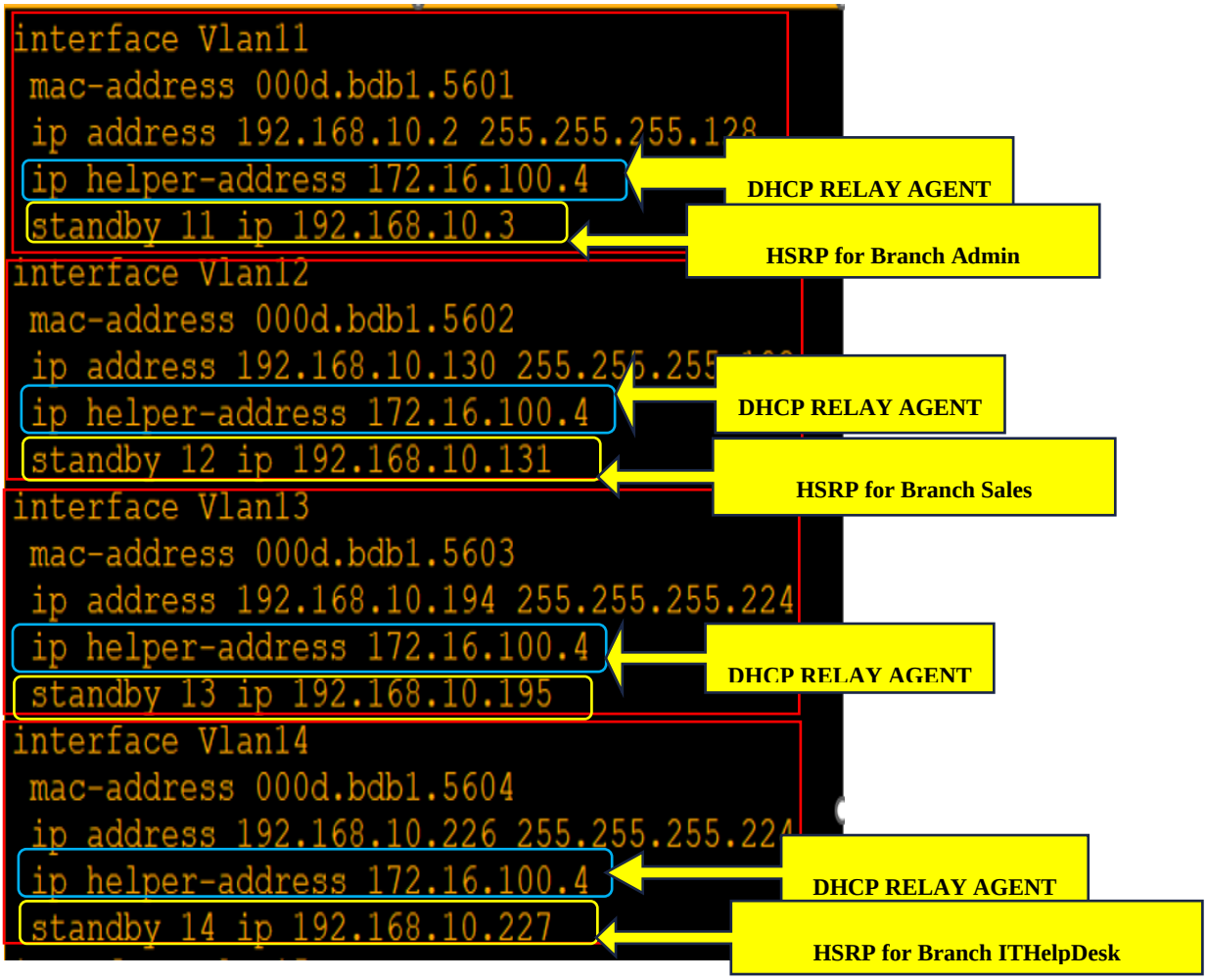


Figure 103: Eight department obtaining IP from DHCP server

Branch

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
Sales	192.168.10.131	8.8.8.8	192.168.10.132	255.255.255.192	50	0.0.0.0	172.16.254.4
Marketing	192.168.10.3	8.8.8.8	192.168.10.4	255.255.255.128	65	0.0.0.0	172.16.254.4
HelpLine	192.168.10.195	8.8.8.8	192.168.10.196	255.255.255.224	25	0.0.0.0	172.16.254.4
ITHelpDesk	192.168.10.227	8.8.8.8	192.168.10.228	255.255.255.224	15	0.0.0.0	172.16.254.4
RemoteSupport	192.168.11.3	8.8.8.8	192.168.11.4	255.255.255.240	10	0.0.0.0	172.16.254.4
TeamLeader	192.168.11.19	8.8.8.8	192.168.11.20	255.255.255.240	6	0.0.0.0	172.16.254.4
Admin	192.168.11.35	8.8.8.8	192.168.11.36	255.255.255.240	5	0.0.0.0	172.16.254.4
HR	192.168.11.51	8.8.8.8	192.168.11.52	255.255.255.248	3	0.0.0.0	172.16.254.4
access-point	172.16.254.3	8.8.8.8	172.16.254.4	255.255.255.240	10	0.0.0.0	172.16.254.4
Guest	10.1.0.3	8.8.8.8	10.1.0.4	255.255.254.0	500	0.0.0.0	172.16.254.4

Figure 104: DHCP configuration in branch with different attributes



‘

Figure 105: DHCP relay agent in branch

DHCP verification in branch

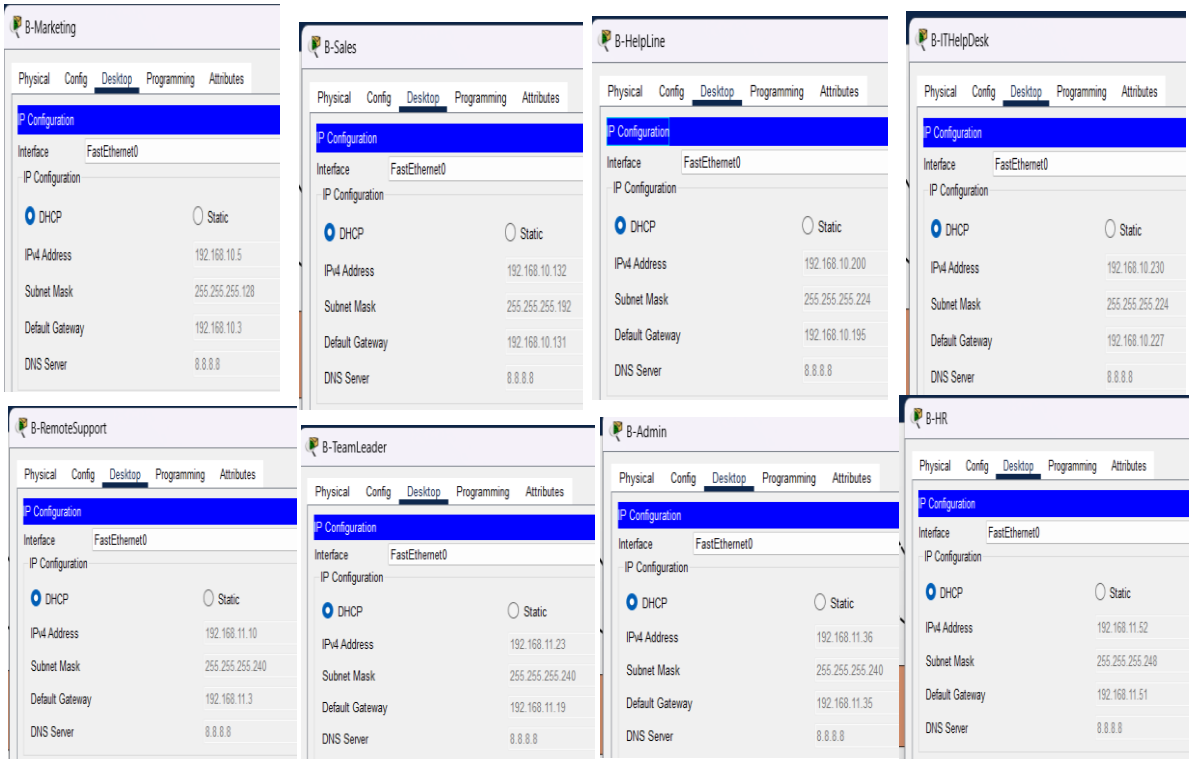


Figure 106: IP assigned to 8 department by DHCP server

ACCESS-PORT

At the end switches, access ports are configured to filter-out the Ethernet frames based on the VLAN memberships of the end devices. It ensures that each access port only relevant to VLAN traffic to pass through.

Headquarter

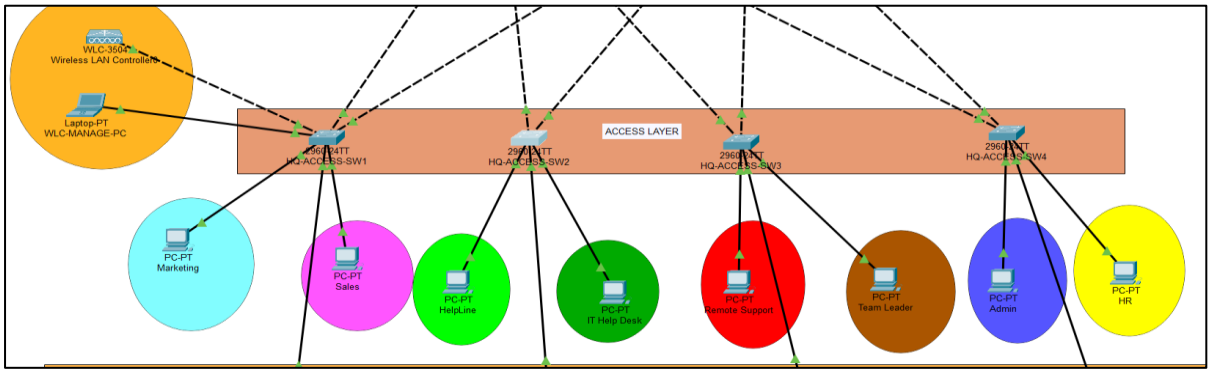


Figure 107: Physical diagram of access layer HQ

```
HQ-ACCESS-SW1(config)#do sh vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/8, Fa0/9, Fa0/
                                                Fa0/12, Fa0/13, Fa
                                                Fa0/16, Fa0/17, Fa
                                                Fa0/20, Fa0/21, Fa
                                                Fa0/24, Gig0/1, Gi
50   ExtraVlan                        active
100  Marketing                        active    Fa0/3
200  Sales                            active    Fa0/7
300  HelpLine                         active
400  ITHelpDesk                       active
500  RemoteSupport                    active
600  TeamLeader                       active
700  Admin                            active
800  HR                               active
888  Guest                            active
999  Management                       active    Fa0/5
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

Assigning access port in VLAN Marketing, Sales, and Management

```
HQ-ACCESS-SW2#sh vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/5, Fa0/7, Fa0/8, Fa0/9
                                                Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                Fa0/22, Fa0/23, Fa0/24, Gig0/1
                                                Gig0/2
50   ExtraVlan                        active
100  Marketing                        active
200  Sales                            active
300  HelpLine                         active    Fa0/3
400  ITHelpDesk                       active    Fa0/6
500  RemoteSupport                    active
600  TeamLeader                       active
700  Admin                            active
800  HR                               active
888  Guest                            active
999  Management                       active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

Assigning access port in VLAN Helpline and ITHelpDesk

Figure 108:: VLAN brief of HQ-ACCESS-SW1 and HQ-ACCESS-SW2

```
HQ-ACCESS-SW3#sh vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/4, Fa0/6, Fa0/8, Fa0/9
                                                Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                Fa0/22, Fa0/23, Fa0/24, Gig0/1
                                                Gig0/2
50   ExtraVlan                        active
100  Marketing                        active
200  Sales                            active
300  HelpLine                         active
400  ITHelpDesk                       active
500  RemoteSupport                    active    Fa0/3
600  TeamLeader                       active    Fa0/7
700  Admin                            active
800  HR                               active
888  Guest                            active
999  Management                       active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

Assigning access port in VLAN Remote Support and Team Leader

```
HQ-ACCESS-SW4(config)#
HQ-ACCESS-SW4(config)#do sh vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/4, Fa0/5, Fa0/8, Fa0/9
                                                Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                Fa0/22, Fa0/23, Fa0/24, Gig0/1
                                                Gig0/2
50   ExtraVlan                        active
100  Marketing                        active
200  Sales                            active
300  HelpLine                         active
400  ITHelpDesk                       active
500  RemoteSupport                    active
600  TeamLeader                       active
700  Admin                            active    Fa0/3
800  HR                               active    Fa0/7
888  Guest                            active
999  Management                       active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

Assigning access port in VLAN Admin and HR

Figure 109: VLAN brief of HQ-ACCESS-SW3 & HQ-ACCESS-SW4

Branch

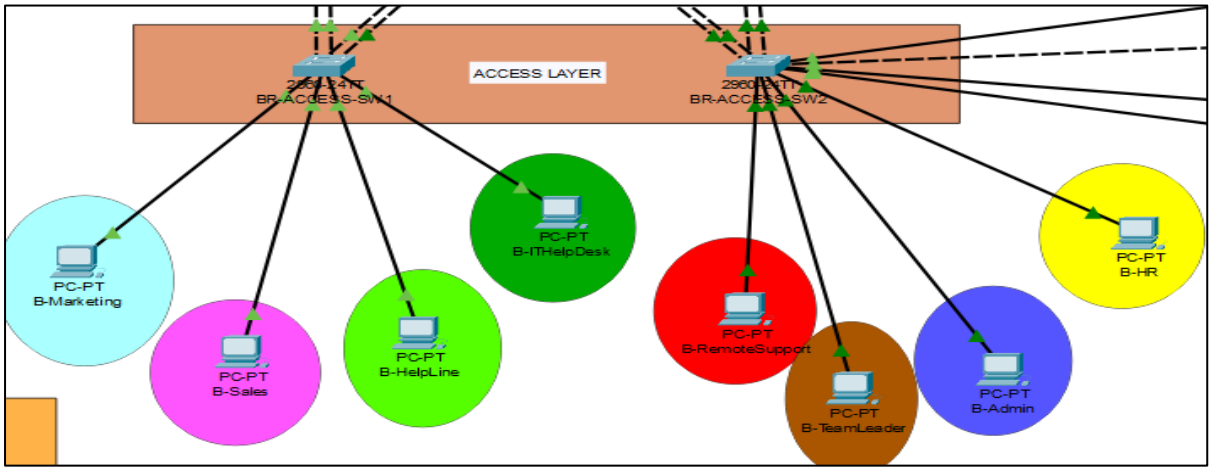


Figure 110: Physical diagram of access-layer Branch

```
BR-ACCESS-SW1#sh vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                 Gig0/1, Gig0/2
11   Marketing                         active    Fa0/5
12   Sales                             active    Fa0/6
13   HelpLine                          active    Fa0/7
14   ITHelpDesk                        active    Fa0/8
15   RemoteSupport                     active
16   TeamLeader                        active
17   Admin                             active
18   HR                                active
99   WLC-management                    active
600  Guest                             active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
BR-ACCESS-SW1#
```

Assigning access port in VLAN Marketing, Sales, Helpline, and ITHelpDesk

```
BR-ACCESS-SW2(config)#do sh vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                 Gig0/1, Gig0/2
11   Marketing                         active
12   Sales                             active
13   HelpLine                          active
14   ITHelpDesk                        active
15   RemoteSupport                     active    Fa0/5
16   TeamLeader                        active    Fa0/6
17   Admin                             active    Fa0/7
18   HR                                active    Fa0/8
99   WLC-management                    active    Fa0/11
600  Guest                             active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

Assigning access port in VLAN Remote Support, Team Leader, Admin, HR, and WLC-management

Figure 111: VLAN brief of BR-ACCESS-SW2

L2 SECURITY FEATURES

BPDU Guard

If an unauthorized switch is connected to the portfast-enabled switch or an access port on end switch, the unauthorized connection has the potential to disturb the spanning-tree in the network topology by altering the designated root bridge. This alteration could result in all VLAN data flowing to the unauthorized switch. To mitigate this risk, BPDU Guard is activated on the portfast-enabled switch. BPDU Guard responds to the reception of BPDU messages on the access port by deactivating the port There are two ways to configure BPDU i.e., pre-port and globally by default.

```
HQ-ACCESS-SW2(config)#spanning-tree portfast bpduguard default
HQ-ACCESS-SW2(config)#
HQ-ACCESS-SW2(config)#do sh spanning-tree summ
Switch is in rapid-pvst mode
Root bridge for: default ExtraVlan Marketing Sales RemoteSupport
TeamLeader Admin HR
Extended system ID           is enabled
Portfast Default             is enabled
PortFast BPDU Guard Default  is enabled
```

Figure 112: BPDU guard enable by default in HQ-ACCESS-SW2

```
HQ-ACCESS-SW1(config)#spanning-tree portfast bpduguard default
HQ-ACCESS-SW1(config)#do sh spanning-tree summ
Switch is in rapid-pvst mode
Root bridge for: default ExtraVlan HelpLine ITHelpDesk
RemoteSupport TeamLeader Admin HR
Extended system ID           is enabled
Portfast Default             is enabled
PortFast BPDU Guard Default  is enabled
```

```
HQ-ACCESS-SW2(config)#spanning-tree portfast bpduguard default
HQ-ACCESS-SW2(config)#
HQ-ACCESS-SW2(config)#do sh spanning-tree summ
Switch is in rapid-pvst mode
Root bridge for: default ExtraVlan Marketing Sales RemoteSupport
TeamLeader Admin HR
Extended system ID           is enabled
Portfast Default             is enabled
PortFast BPDU Guard Default  is enabled
```

Figure 113: Enabling BPDU Guard in HQ-ACCESS-SW1 and HQ-ACCESS-SW2

```
HQ-ACCESS-SW3(config)#spanning-tree portfast bpduguard default
HQ-ACCESS-SW3(config)#do sh spanning-tree summ
Switch is in rapid-pvst mode
Root bridge for: default ExtraVlan Marketing Sales HelpLine
ITHelpDesk Admin HR
Extended system ID           is enabled
Portfast Default             is enabled
PortFast BPDU Guard Default  is enabled
Portfast BPDU Filter Default is disabled
```

```
HQ-ACCESS-SW4(config)#SPANNING-TREE portfast bpduguard default
HQ-ACCESS-SW4(config)#
HQ-ACCESS-SW4(config)#do sh spanning-tree summ
Switch is in rapid-pvst mode
Root bridge for: default ExtraVlan Marketing Sales HelpLine ITHelpDesk RemoteSupport TeamLeader
Extended system ID          is enabled
Portfast Default            is enabled
PortFast BPDU Guard Default  is enabled
```

Figure 114: Enabling BPDU guard in HQ-ACCESS-SW3 and HQ-ACCESS-SW4

Branch

```
BR-ACCESS-SW1(config)#SPANNing-tree portfast bpduguard default
BR-ACCESS-SW1(config)#
BR-ACCESS-SW1(config)#do sh spanning-tree summ
Switch is in rapid-pvst mode
Root bridge for:
Extended system ID           is enabled
Portfast Default             is enabled
PortFast BPDU Guard Default  is enabled
Portfast BPDU Filter Default is disabled
```

```
BR-ACCESS-SW2(config)#spanning-tree portfast bpduguard default
BR-ACCESS-SW2(config)#
BR-ACCESS-SW2(config)#do sh spanning-tree summ
Switch is in rapid-pvst mode
Root bridge for: default Marketing Sales HelpLine ITHelpDesk
Extended system ID           is enabled
Portfast Default             is enabled
PortFast BPDU Guard Default  is enabled
Portfast BPDU Filter Default is disabled
```

Figure 115: BPDU Guard enabling in BR-ACCESS-SW1 and BR-ACCESS-SW2

Port security

Most of the malicious activities are involved from the access ports, implementing Layer 2 port security features is crucial in access port. These features add an extra layer of protection by ensuring that only authorized users can access the network through that port. If unauthorized device attempt to connect, L2 port security features can take action like disabling port, triggering alert. This proactive approach can help to prevent unauthorized access and improves the security posture of network.

Headquarter

```
HQ-ACCESS-SW1(config-if-range)#int range fa0/5,fa0/3,fa0/7
HQ-ACCESS-SW1(config-if-range)#switchport port-security mac-address sticky
HQ-ACCESS-SW1(config-if-range)#
HQ-ACCESS-SW1(config-if-range)#switchport port-security violation restrict
HQ-ACCESS-SW1(config-if-range)#
```

```
HQ-ACCESS-SW2(config)#INT RANGE fa0/3,fa0/6
HQ-ACCESS-SW2(config-if-range)#switchport port-security mac-address sticky
HQ-ACCESS-SW2(config-if-range)#switchport port-security violation restrict
HQ-ACCESS-SW2(config-if-range)#
```

Figure 116: Configuration of port-security in HQ-ACCESS-SW1 and HQ-ACCESS-SW2

Ports of HQ-ACCESS-SW1 fa0/, fa0/3, and fa0/7 and HQ-ACCESS-SW2 fa0/3, fa0/6 are access port so, port security feature is enabled on these ports. Sticky is enabled for dynamically learning secure mac address from the corresponding ports. The violation is set to restrict so, the port only restricts the unauthorized frame and generates a log message corresponds to unauthorized frames.

```
HQ-ACCESS-SW3(config)#int range fa0/3,fa0/7
HQ-ACCESS-SW3(config-if-range)#switchport port-security mac-address sticky
HQ-ACCESS-SW3(config-if-range)#switchport port-security violation restrict
HQ-ACCESS-SW3(config-if-range)#
```

```
HQ-ACCESS-SW4(config)#int ran fa0/3,fa0/7
HQ-ACCESS-SW4(config-if-range)#switchport port-security mac sticky
HQ-ACCESS-SW4(config-if-range)#switchport port-secu violatio restrict
HQ-ACCESS-SW4(config-if-range)#
```

Figure 117: Configuration of port security in HQ-ACCESS-SW3 and HQ-ACCESS-SW4

The following ports fa0/3, fa0/7 of two switches are access ports. Secure mac address is learned from sticky and violation is set to restrict.

Branch

```
BR-ACCESS-SW1(config)#int range fa0/5-8
BR-ACCESS-SW1(config-if-range)#switchport port-security mac-address sticky
BR-ACCESS-SW1(config-if-range)#switchport port-security violation protect
BR-ACCESS-SW1(config-if-range)#
```

```
BR-ACCESS-SW2(config)#int range fa0/5-8,fa0/11
BR-ACCESS-SW2(config-if-range)#switchpor port-sec mac sticky
BR-ACCESS-SW2(config-if-range)#switchport port-security violation protect
BR-ACCESS-SW2(config-if-range)#
```

Figure 118: Configuration of port security in BR-ACCESS-SW1 and BR-ACCESS-SW2

The ports fa0/5-8 of BR-ACCESS-SW1 and fa0/5-8, fa0/11 of BR-ACCESS-SW1 are access port. Sticky is set for dynamically learning sec mac address correspond to that port. Violation is set to protect for unauthorized frame to enter the ports without generating the logs.

DHCP Snooping

Relying on a DHCP server to provide IP address to end host can indeed offload of workload, but it introduces the risk of potential security threat, especially if a rouge DHCP server is present on the access layer. This unauthorized server might assign an incorrect or malicious IP configuration to end host leading to security vulnerabilities. To mitigate this risk, DHCP snooping is implemented on end switches. Normally, it filters out the client DHCP message i.e., Discover, Request, Decline, Release on untrusted ports

```
HQ-ACCESS-SW1(config)#int range fa0/1-2
HQ-ACCESS-SW1(config-if-range)#ip dhcp snooping trust
HQ-ACCESS-SW1(config-if-range)#
HQ-ACCESS-SW1(config-if-range)#ip dhcp snooping
HQ-ACCESS-SW1(config)#ip dhcp snooping vlan 100,200,999,888
HQ-ACCESS-SW1(config)#
HQ-ACCESS-SW1(config)#
HQ-ACCESS-SW1(config)#
HQ-ACCESS-SW1(config)#do sh ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
100,200,888,999
Insertion of option 82 is enabled
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Interface                  Trusted    Rate limit (pps)
-----------------------    -------    ----------------
FastEthernet0/2            yes        unlimited
FastEthernet0/1            yes        unlimited
```

Enabling DHCP Spoofing

RELAY AGENT

Figure 119: Configuration of DHCP snooping in headquarter access layer switch

All of the ports in DHCP snooping are untrusted, the ports fa0/, fa0/2 are uplink ports and set to trusted port so, DHCP message in these ports are not inspected. By default, option 82 message are added inside of DHCP client message.

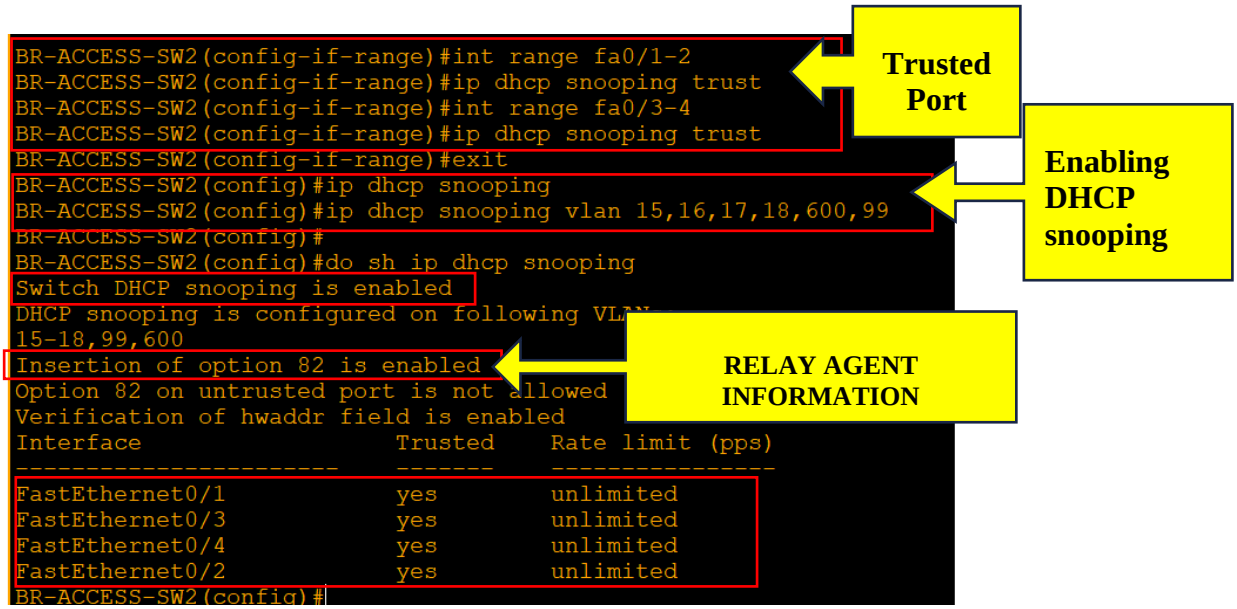


Figure 120: Configuration of DHCP snooping in Branch access-layer switch

Rate Limiting

To prevent such attacks like DHCP starvation which can result in denial of service, rate limiting is implemented on the untrusted ports of end switches. This measure controls the rate at which DHCP request are processed on these ports, preventing a numerous request in a second from attacker by setting up a threshold on the DHCP message.

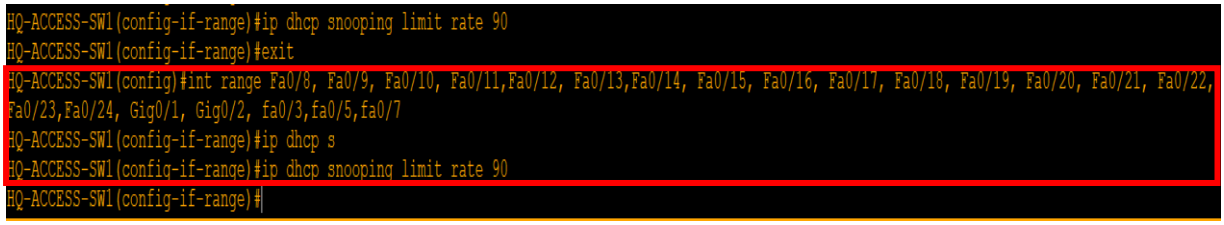


Figure 121: Rate limiting configuration in every access port of switch HQ-ACCESS-SW1

Dynamic ARP Inspection

With the help of DIA (Dynamic Arp Inspection) attack like Man-in-the-middle and ARP poisoning can be prevented. It inspects the ARP message on untrusted ports. Without the DHCP snooping it cannot be implemented. Simply it just binds the MAC address with IP address it belongs to.

```
HQ-ACCESS-SW1(config)#int range fa0/1-2
HQ-ACCESS-SW1(config-if-range)#ip arp inspection trust
HQ-ACCESS-SW1(config-if-range)#exzit
                              ^
% Invalid input detected at '^' marker.

HQ-ACCESS-SW1(config-if-range)#exit
HQ-ACCESS-SW1(config)#ip arp inspection vlan 100,200,999,888
HQ-ACCESS-SW1(config)#
HQ-ACCESS-SW1(config)#ip arp inspection validate src-mac ip dst-mac
```

Figure 122: Configuration of DAI in Headquarter switch

```
HQ-ACCESS-SW1(config)#do sh ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------------
00:06:2A:D4:E4:50   172.16.200.6     0           dhcp-snooping  100   FastEthernet0/3
00:60:5C:82:7D:AE   172.16.200.132   0           dhcp-snooping  200   FastEthernet0/7
00:E0:8F:2B:B3:C1   192.168.1.4      0           dhcp-snooping  999   FastEthernet0/5
Total number of bindings: 3
```

Figure 123: DHCP snooping binding table

```
HQ-ACCESS-SW1(config)#do sh ip arp inspection interface
Interface         Trust State      Rate(pps)     Burst Interval
----------------  -----------      ----------    --------------
Fa0/1             Trusted                  15                  1
Fa0/2             Trusted                  15                  1
Fa0/3             Untrusted                15                  1
Fa0/4             Untrusted                15                  1
Fa0/5             Untrusted                15                  1
Fa0/6             Untrusted                15                  1
Fa0/7             Untrusted                15                  1
Fa0/8             Untrusted                15                  1
Fa0/9             Untrusted                15                  1
Fa0/10            Untrusted                15                  1
Fa0/11            Untrusted                15                  1
Fa0/12            Untrusted                15                  1
Fa0/13            Untrusted                15                  1
Fa0/14            Untrusted                15                  1
Fa0/15            Untrusted                15                  1
Fa0/16            Untrusted                15                  1
Fa0/17            Untrusted                15                  1
Fa0/18            Untrusted                15                  1
Fa0/19            Untrusted                15                  1
Fa0/20            Untrusted                15                  1
Fa0/21            Untrusted                15                  1
Fa0/22            Untrusted                15                  1
Fa0/23            Untrusted                15                  1
Fa0/24            Untrusted                15                  1
Gig0/1            Untrusted                15                  1
Gig0/2            Untrusted                15                  1
```

Rate Limiting on trusted port are disable but might be bug or error of cisco packet tracer

Figure 124: ARP inspection table of interface

Note: By default, rate limiting on untrusted of ARP message is enabled by 15 message per second.

NAT (Network Address Translation)

To enable private network to access the internet, assigning each end host public IP address is impracticable. Therefore, NAT plays an important role translating private IP address to public IP address and vise-versa.

PAT (Port Address Translation)

Allocating a sperate public IP address to each end host of company would require a numerous number of public IP address. This public IP address can be bought from the ISP which is inefficient and impractical in real world scenario. PAT address this issue by translating multiple private IP address to single public IP address, with utilizing ephemeral port number.

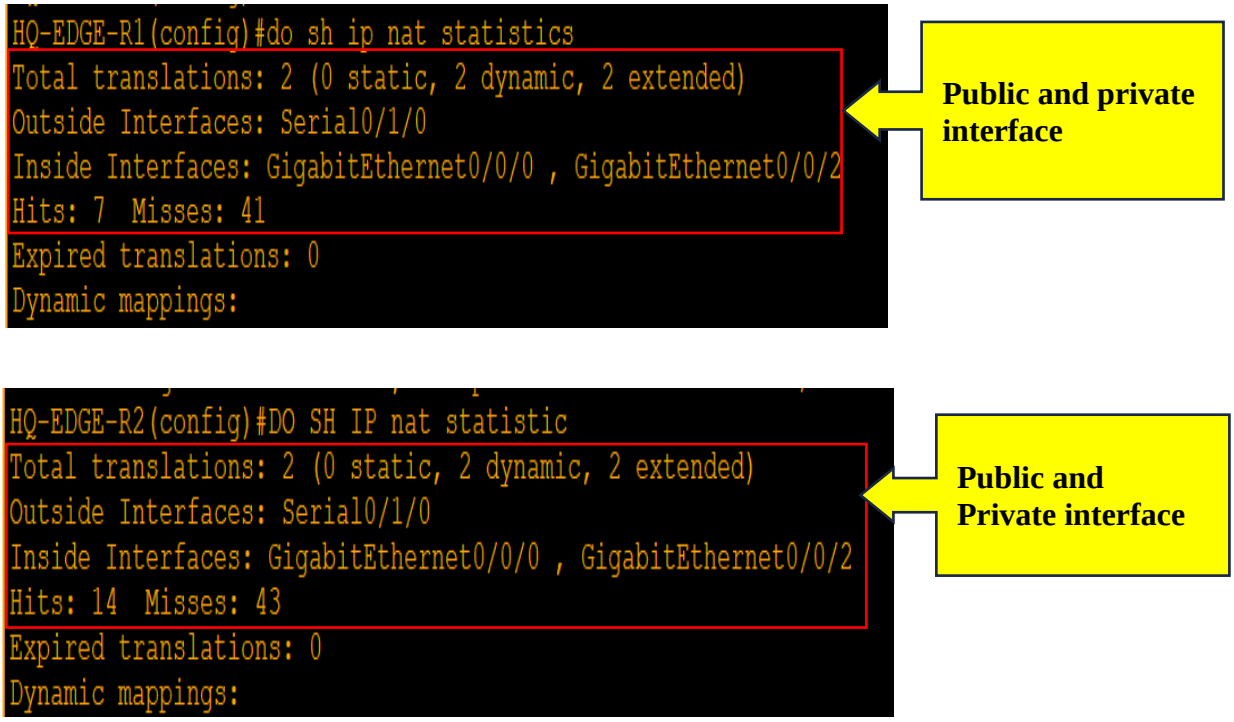


Figure 125: PAT in HQ-EDGE-R1 & HQ-EDGE-R2

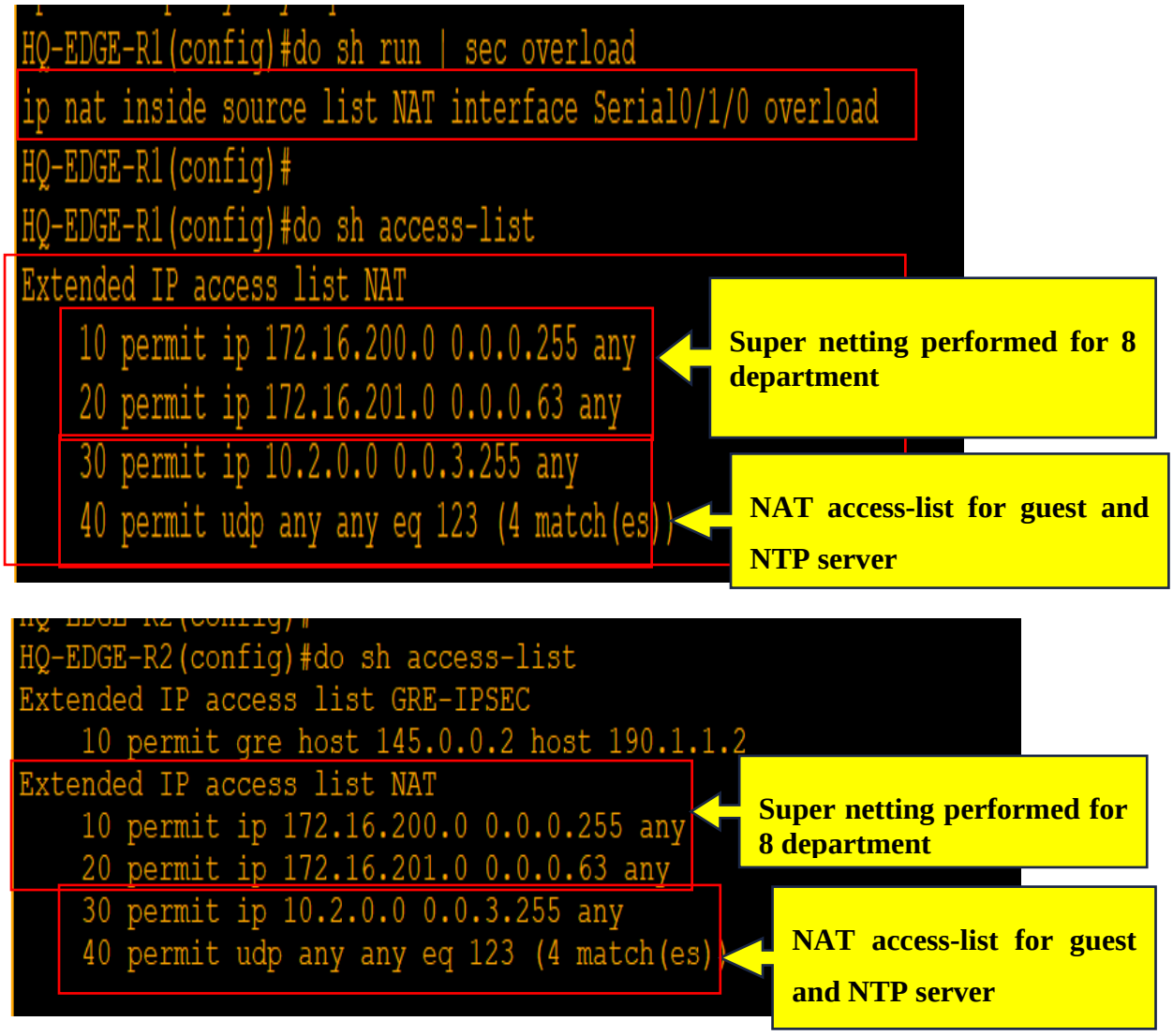


Figure 126: PAT applied in outside interface with access-list

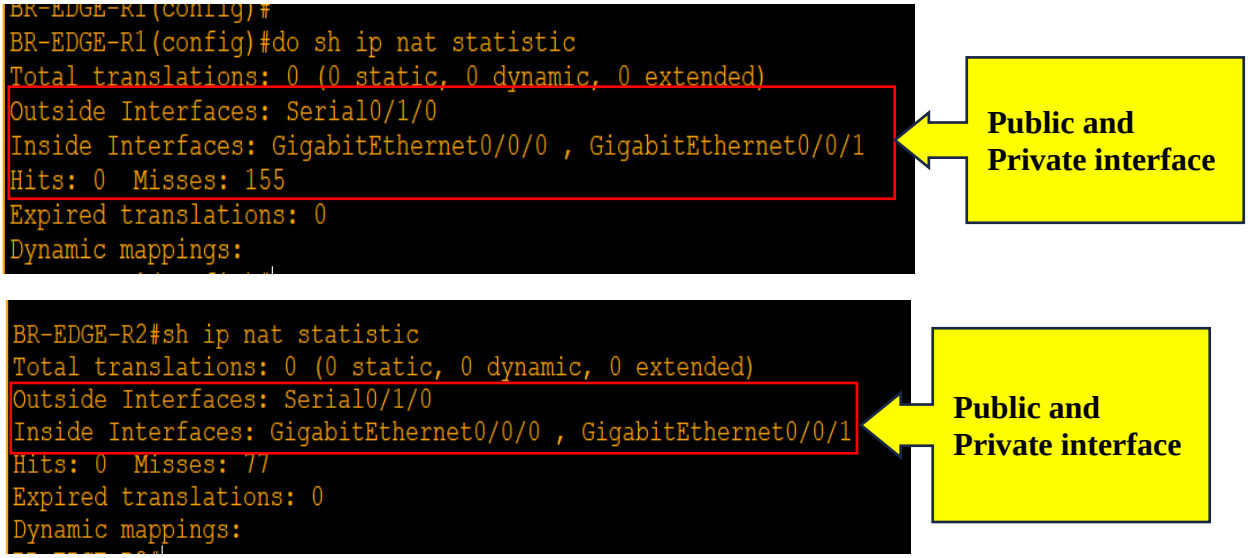


Figure 127: PAT in BR-EDGE-R1 & BR-EDGE-R2

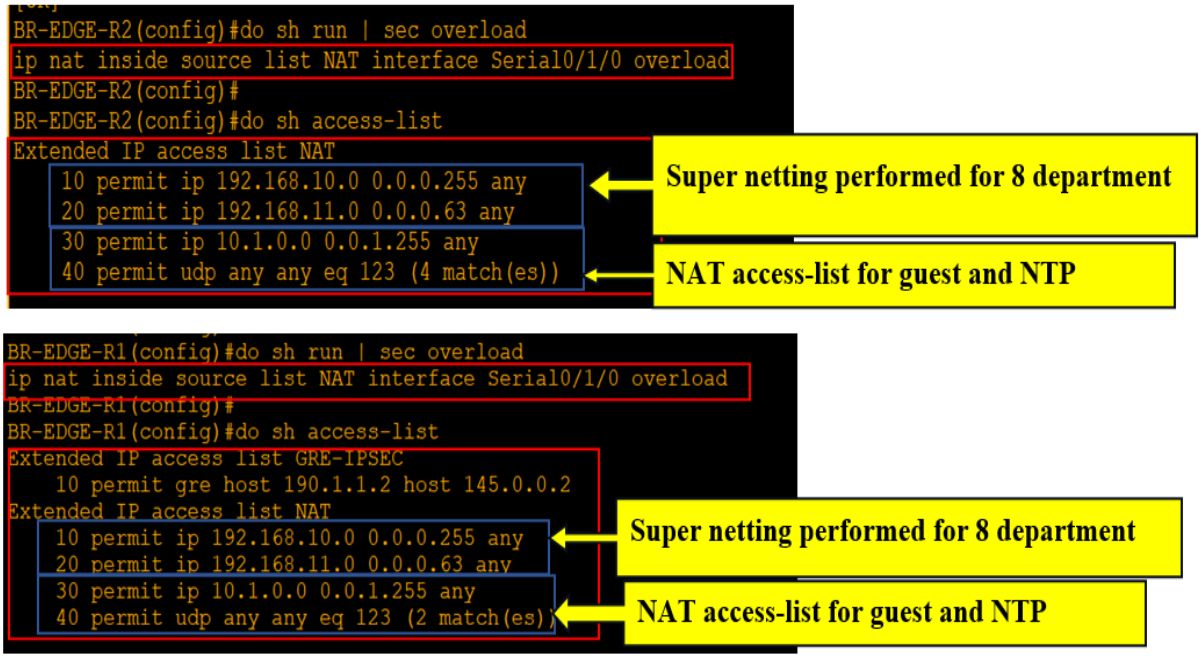


Figure 128: PAT applied on outside interface and access-list

NAT & PAT verification

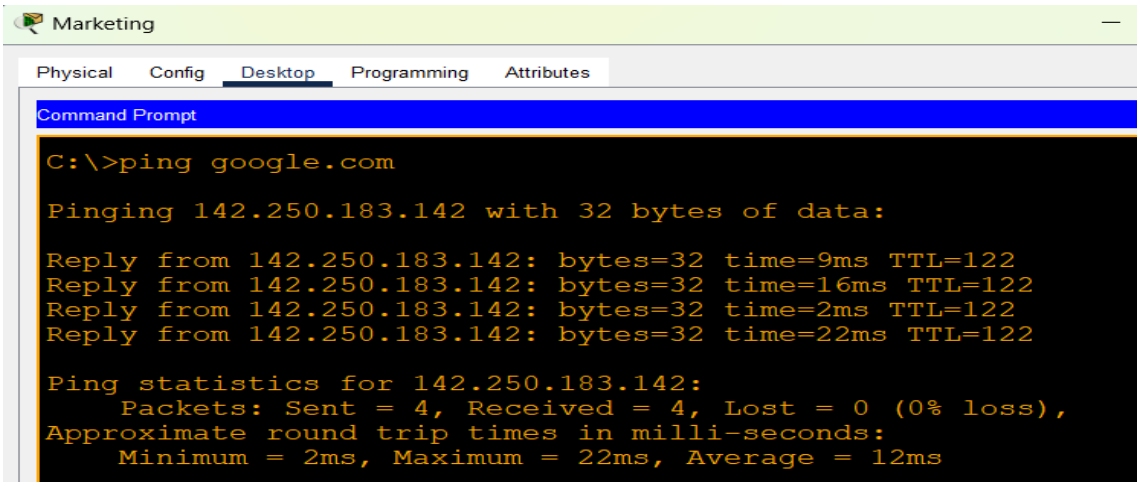


Figure 129: Successful ping from Headquarter marketing department to Google

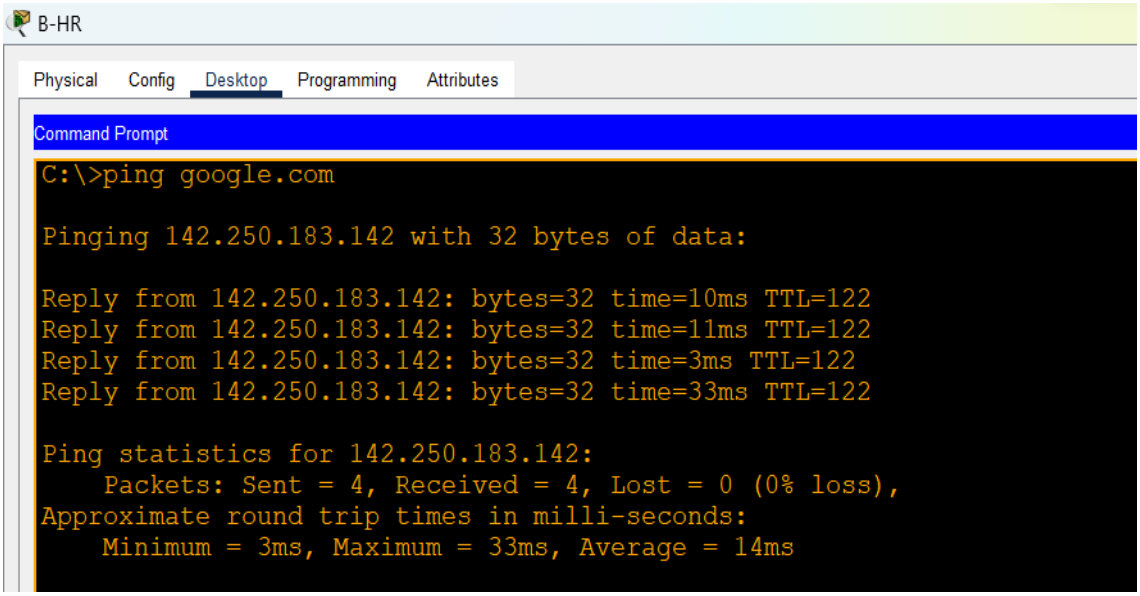


Figure 130: Successful ping from branch HR department to Google

VPN (Virtual Private Network)

Company operating from different geographical location, with headquarter and branches seeks a secure method to share sensitive data. Although internet can facilitate data transfer, this process leads to exposure of confidential information over the public address. To address this, VPN are implemented at the edge router or firewall. These VPN established a secure and encrypted tunnel over the internet between the headquarter and its branches. This encrypted tunnel ensures the confidentiality and integrity of the data which makes it harder for potential attackers to tamper it.

For this project I have implemented an IPsec site-to-site VPN configuration in cisco packet tracer and GRE over IPSEC which I have configured in GNS3 due some issue encountered with GRE tunnel in Cisco packet tracer.

IPsec

Networking protocols such as TCP/IP primarily focus on connection and delivery, transmitting messages openly without concealment. However, encryption protocols like IPsec add a security layer in data during transmission in networks, safeguarding it from unauthorized access and maintaining confidentiality and integrity.

In this project I have implemented an IPsec site-to-site VPN inside edge router in cisco packet tracer, IPsec have two phases:

Phase 1: ISAKMP (Internet Security Association Key Management Protocol)

- Making a Policy and configuring HAGLE (Hash, Authentication, Group, Lifetime, Encryption)
- Generating a ISAKMP pre-share key

Phase 2: IPsec.

- Creating a transform set
- Creating a crypto map and mapping all the argument inside it

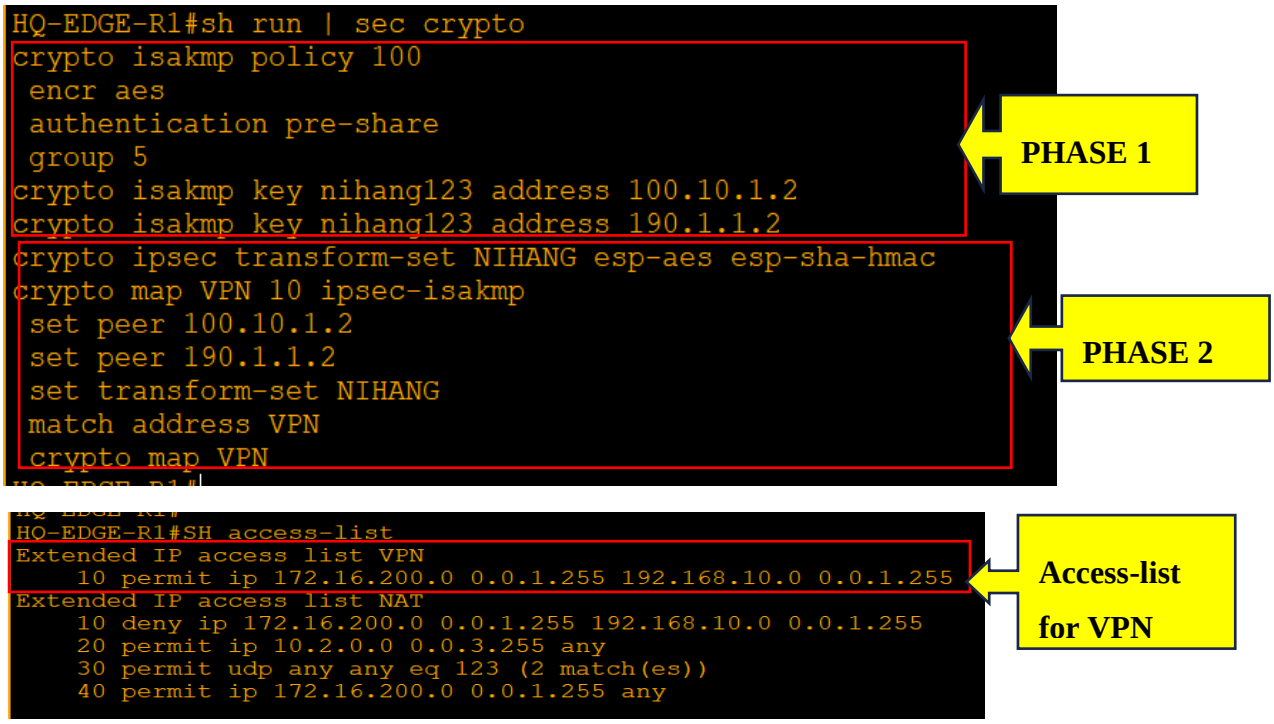


Figure 131: Configuration of IPsec VPN and access-list in HQ-EDGE-R1

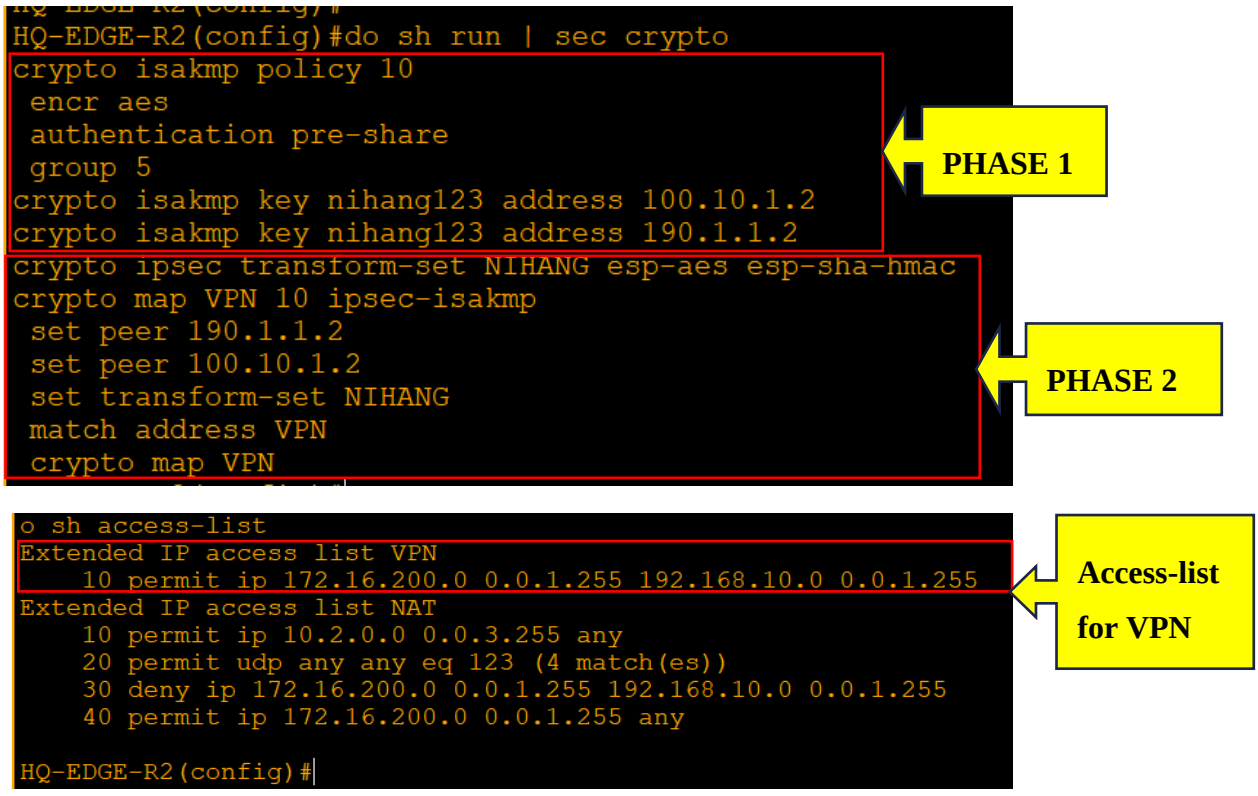


Figure 132: Configuration of IPsec VPN and access-list in HQ-EDGE-R2

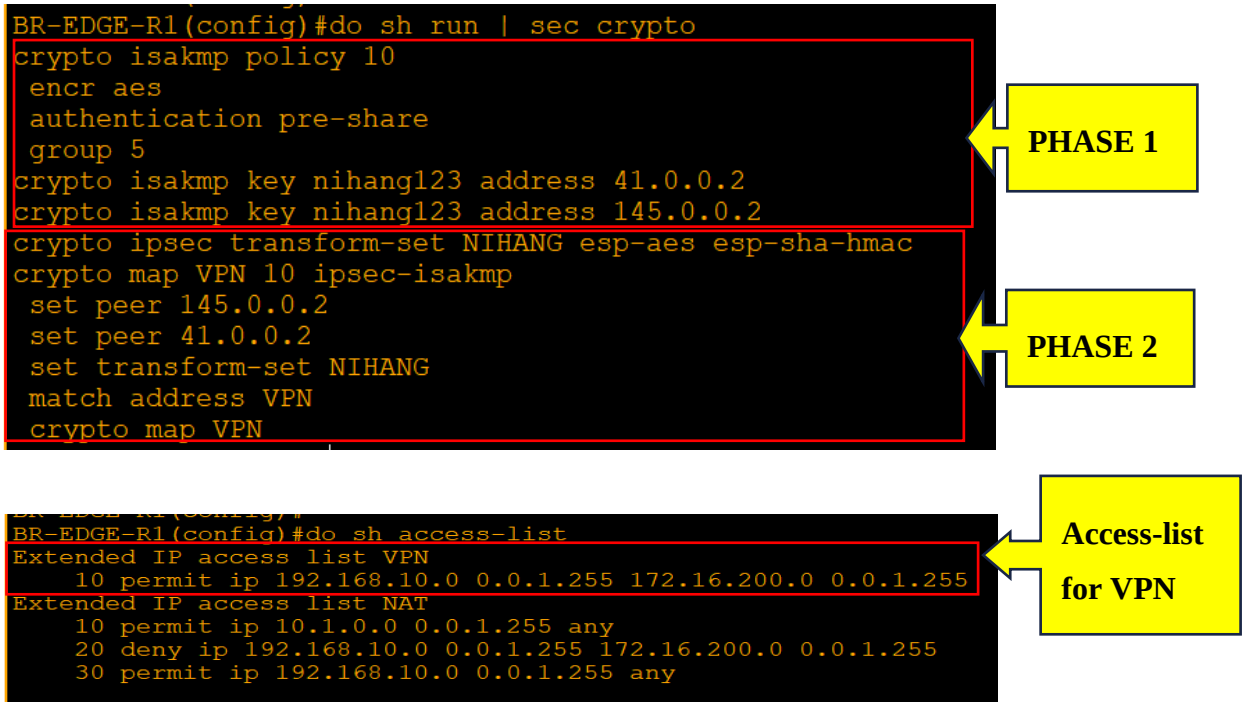


Figure 133: Configuration IPsec VPN and access-list in BR-EDGE-R1

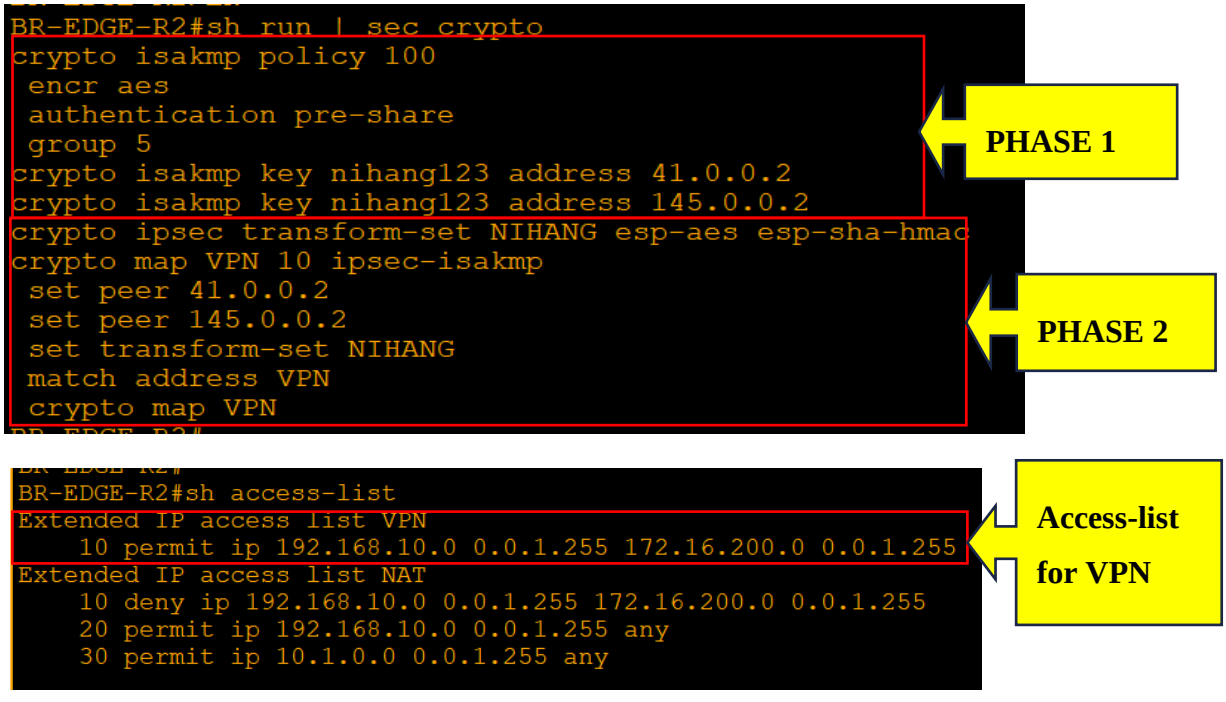


Figure 134: Configuration of IPsec VPN in BR-EDGE-R2 and access-list

Verification through IPsec site-to-site VPN

From HQ to Branch

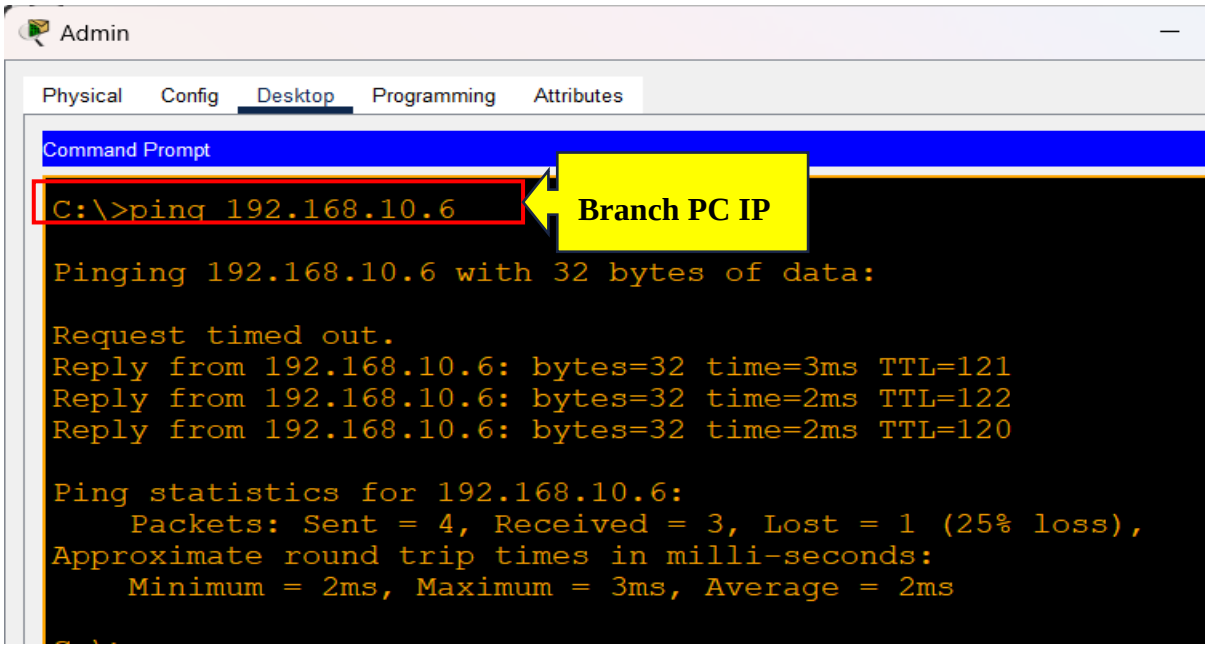


Figure 135: Ping from HQ admin department to Branch Marketing

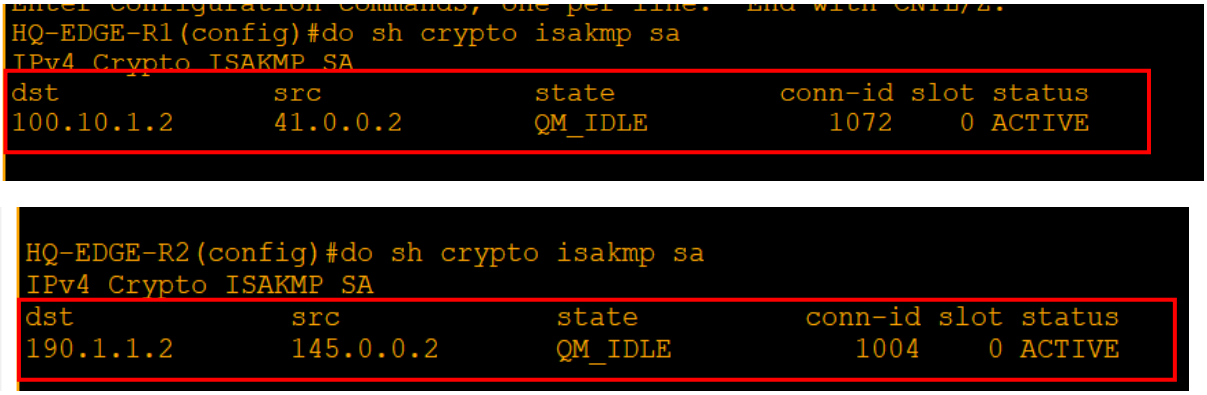


Figure 136: Successful ISAKMP tunnel formation between headquarter and branch

```
HQ-EDGE-R1(config)#do sh crypto ipsec sa

interface: Serial0/1/0
    Crypto map tag: VPN, local addr 41.0.0.2

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (172.16.200.0/255.255.254.0/0/0)
   remote  ident (addr/mask/prot/port): (192.168.10.0/255.255.254.0/0/0)
   current_peer 100.10.1.2 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 11, #pkts encrypt: 11, #pkts digest: 0
   #pkts decaps: 3, #pkts decrypt: 3, #pkts verify: 0
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 1, #recv errors 0

     local crypto endpt.: 41.0.0.2, remote crypto endpt.:100.10.1.2
     path mtu 1500, ip mtu 1500, ip mtu idb Serial0/1/0
     current outbound spi: 0xF8F35DE0(4176698848)

     inbound esp sas:
      spi: 0x91D950D1(2446938321)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2008, flow_id: FPGA:1, crypto map: VPN
        sa timing: remaining key lifetime (k/sec): (4525504/3426)
        IV size: 16 bytes
        replay detection support: N
        Status: ACTIVE
```

```
HQ-EDGE-R2(config)#do sh crypto ipsec sa

interface: Serial0/1/0
    Crypto map tag: VPN, local addr 145.0.0.2

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (172.16.200.0/255.255.254.0/0/0)
   remote  ident (addr/mask/prot/port): (192.168.10.0/255.255.254.0/0/0)
   current_peer 190.1.1.2 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
   #pkts decaps: 8, #pkts decrypt: 8, #pkts verify: 0
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 0, #recv errors 0

     local crypto endpt.: 145.0.0.2, remote crypto endpt.:190.1.1.2
     path mtu 1500, ip mtu 1500, ip mtu idb Serial0/1/0
     current outbound spi: 0x5C4445EE(1547978222)

     inbound esp sas:
      spi: 0x42EDB022(1122873378)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2008, flow_id: FPGA:1, crypto map: VPN
        sa timing: remaining key lifetime (k/sec): (4525504/3349)
        IV size: 16 bytes
        replay detection support: N
        Status: ACTIVE
```

Figure 137: Encryption, encapsulation, decryption, and encapsulation by IPsec in HQ edge router

From Branch to HQ

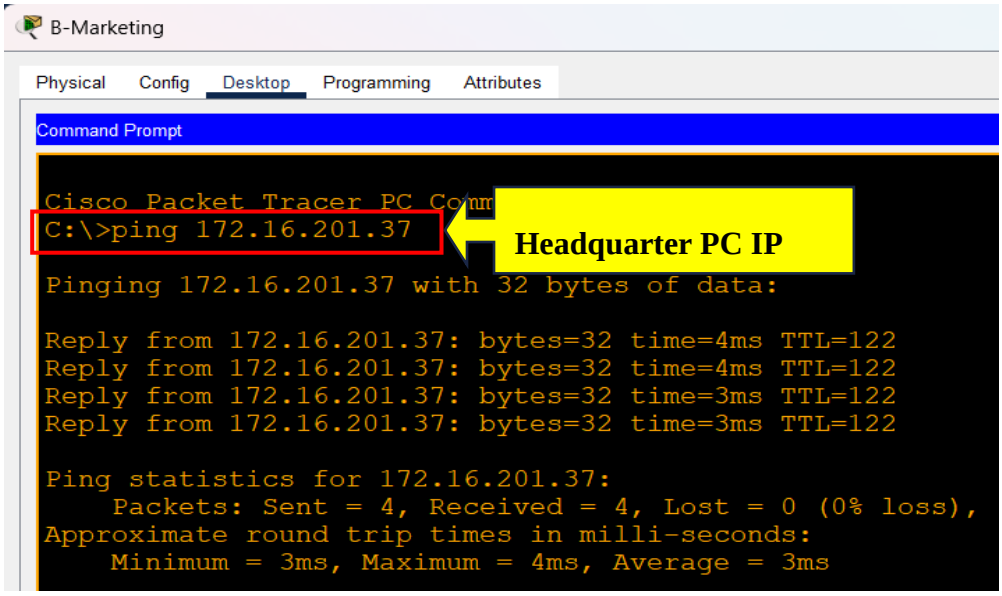


Figure 138: Ping from branch marketing department to headquarter admin department

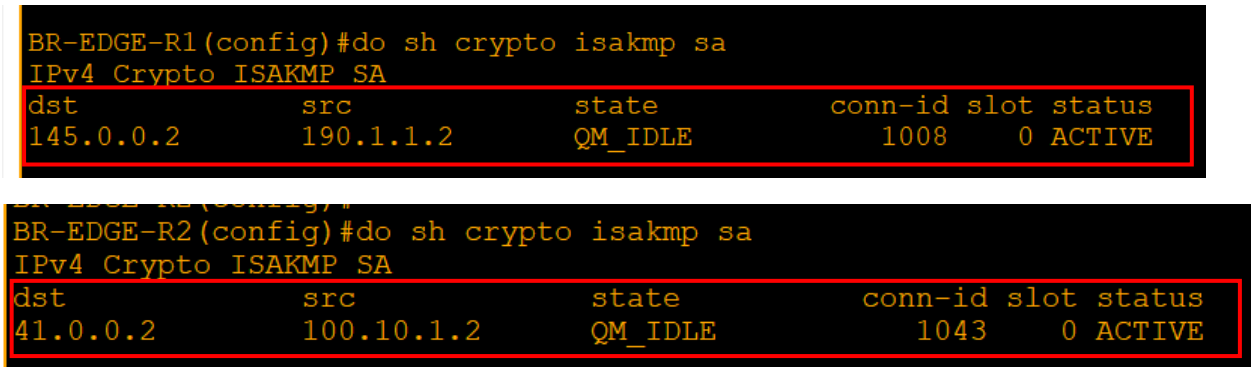


Figure 139: Successful ISAKMP tunnel creation in Branch edge router

```
BR-EDGE-R1(config)#do sh crypto ipsec sa

interface: Serial0/1/0
    Crypto map tag: VPN, local addr 190.1.1.2

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.10.0/255.255.254.0/0/0)
   remote  ident (addr/mask/prot/port): (172.16.200.0/255.255.254.0/0/0)
   current_peer 145.0.0.2 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 11, #pkts encrypt: 11, #pkts digest: 0
   #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 1, #recv errors 0

     local crypto endpt.: 190.1.1.2, remote crypto endpt.:145.0.0.2
     path mtu 1500, ip mtu 1500, ip mtu idb Serial0/1/0
     current outbound spi: 0x42EDB022(1122873378)

     inbound esp sas:
      spi: 0x5C4445EE(1547978222)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2008, flow_id: FPGA:1, crypto map: VPN
        sa timing: remaining key lifetime (k/sec): (4525504/3211)
        IV size: 16 bytes
        replay detection support: N
        Status: ACTIVE
```

```
BR-EDGE-R2(config)#do sh crypto ipsec sa

interface: Serial0/1/0
    Crypto map tag: VPN, local addr 100.10.1.2

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.10.0/255.255.254.0/0/0)
   remote  ident (addr/mask/prot/port): (172.16.200.0/255.255.254.0/0/0)
   current_peer 41.0.0.2 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 0
   #pkts decaps: 19, #pkts decrypt: 19, #pkts verify: 0
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 0, #recv errors 0

     local crypto endpt.: 100.10.1.2, remote crypto endpt.:41.0.0.2
     path mtu 1500, ip mtu 1500, ip mtu idb Serial0/1/0
     current outbound spi: 0x91D950D1(2446938321)

     inbound esp sas:
      spi: 0xF8F35DE0(4176698848)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2008, flow_id: FPGA:1, crypto map: VPN
        sa timing: remaining key lifetime (k/sec): (4525504/3183)
        IV size: 16 bytes
        replay detection support: N
        Status: ACTIVE
```

Figure 140: Encryption, decryption, encapsulation, and decapsulation through IPsec in Branch edge router

GRE over IPsec

GRE (Generic Routing Encapsulation) does not provide encryption between the tunnel, but it can encapsulate a wide variety of network layer protocol like multicast, broadcast, unicast, and more. So, it means different types of routing protocol like OSPF, EIGRP etc. can be used between the two parties. On the other hand, IPsec (Internet Protocol Security) is a separate protocol that can encrypt the data over the internet. By combining both GRE and IPsec, a secure VPN that can encapsulate wide variety of network layer protocol can be obtained know as GRE over IPsec

Things required for configuring GRE over IPsec

- Establishing an IPsec tunnel between headquarter edge and branch edge.
- Creating a GRE tunnel between headquarter edge and branch edge.

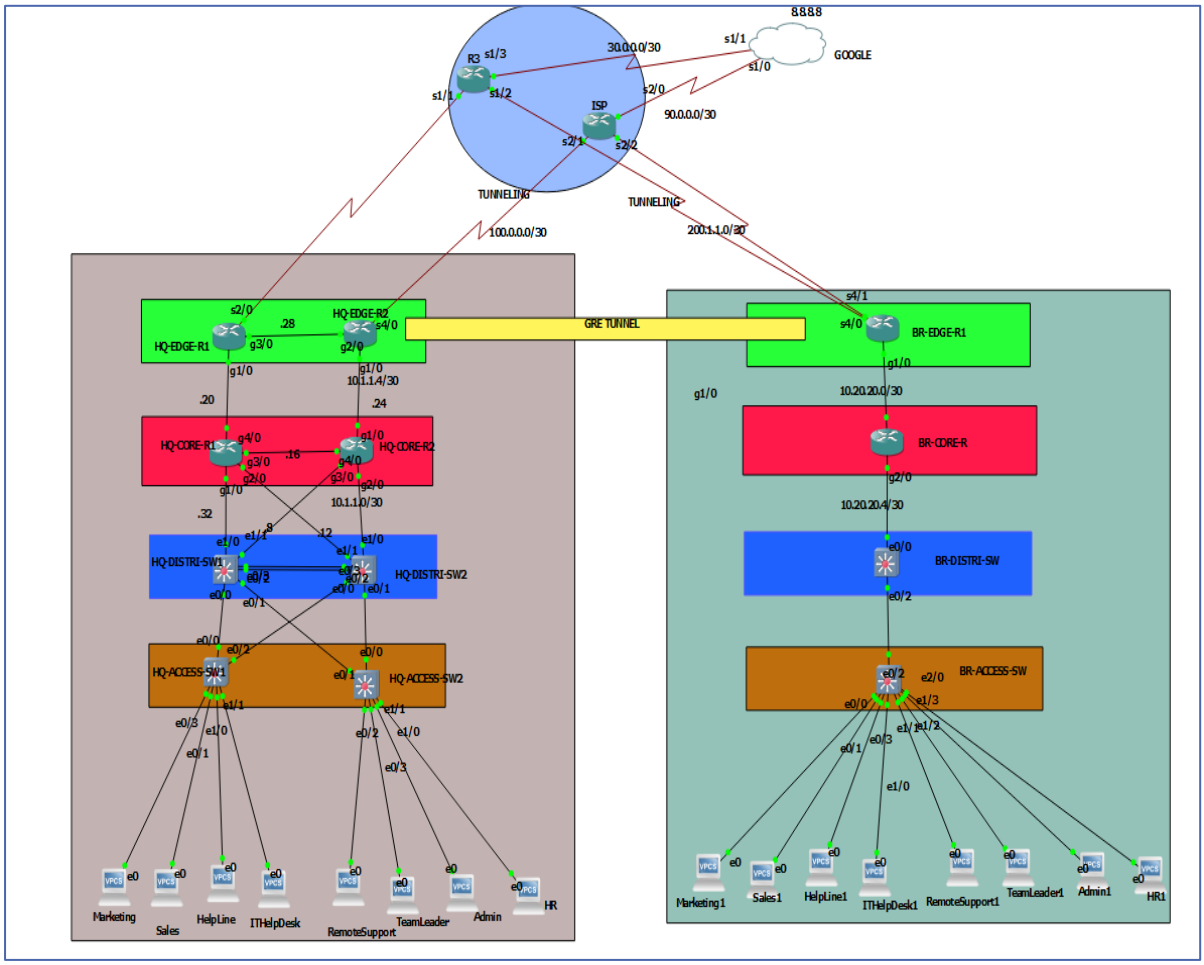


Figure 141: Physical diagram in GNS3

Headquarter

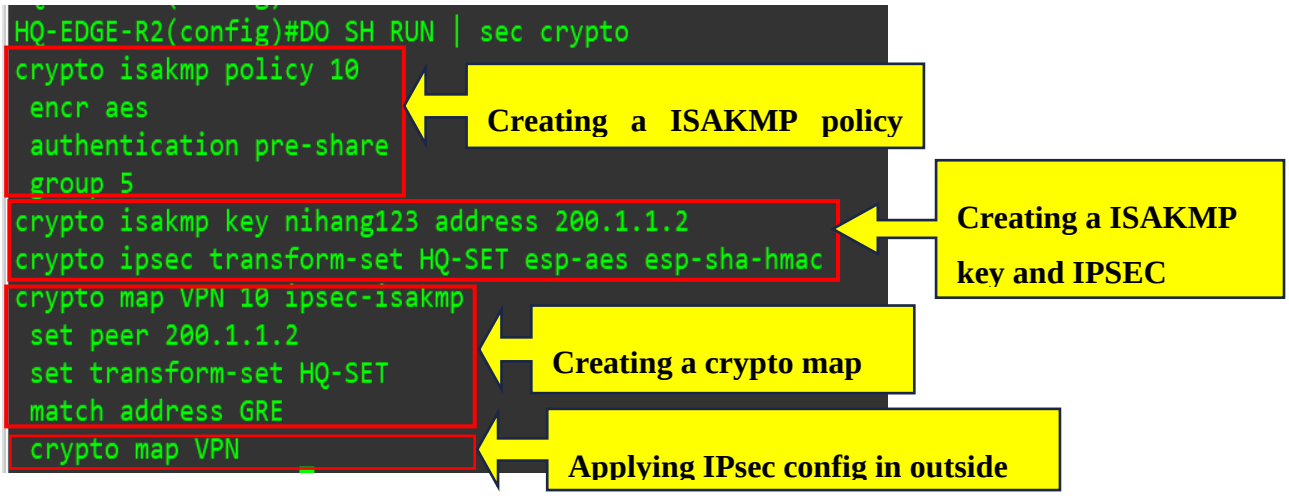


Figure 142: Running config of IPsec in HQ-EDGE-R2

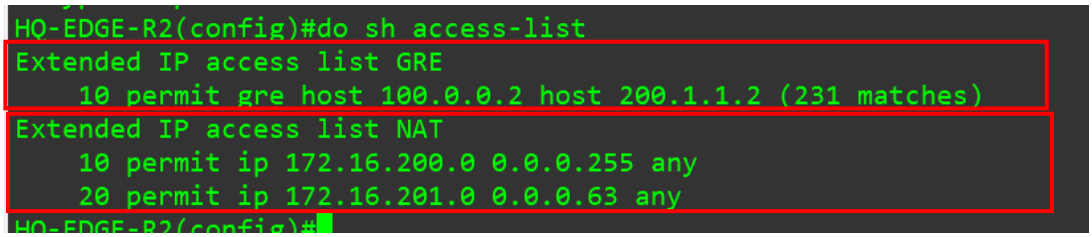


Figure 143: Access-list of GRE tunnel information and NAT

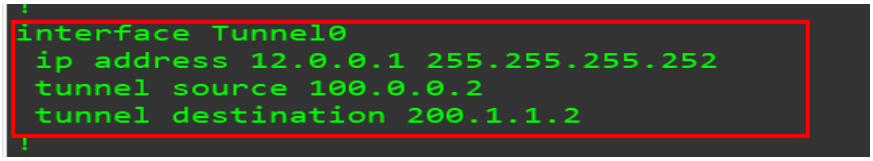


Figure 144: Running config of creating GRE Tunnel0

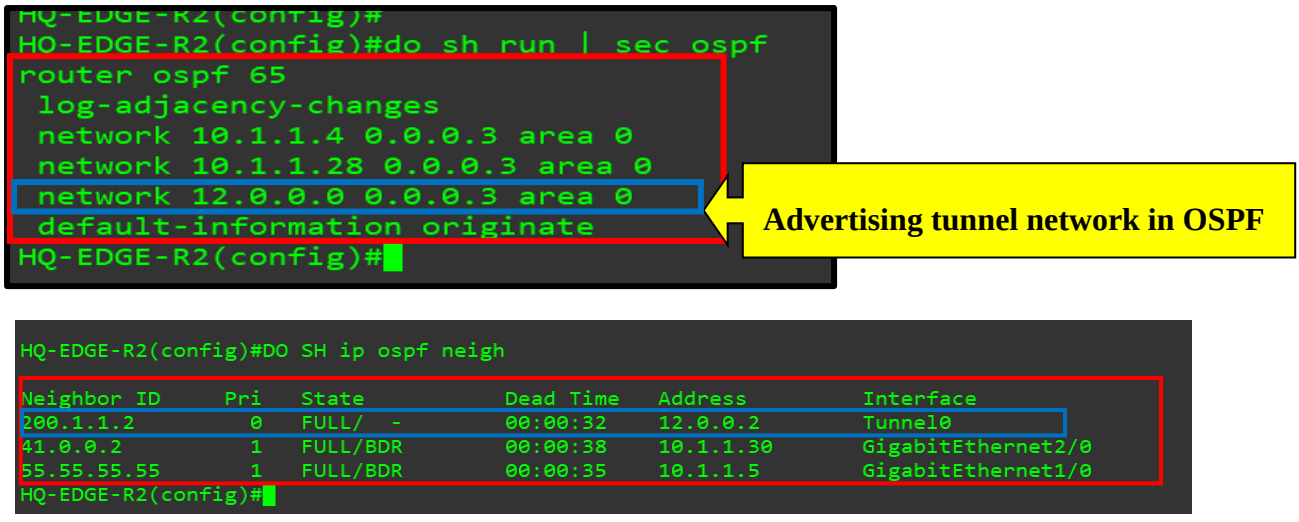


Figure 145: OSPF configuration and OSPF neighborship of HQ-EDGE-R2

Branch

Figure

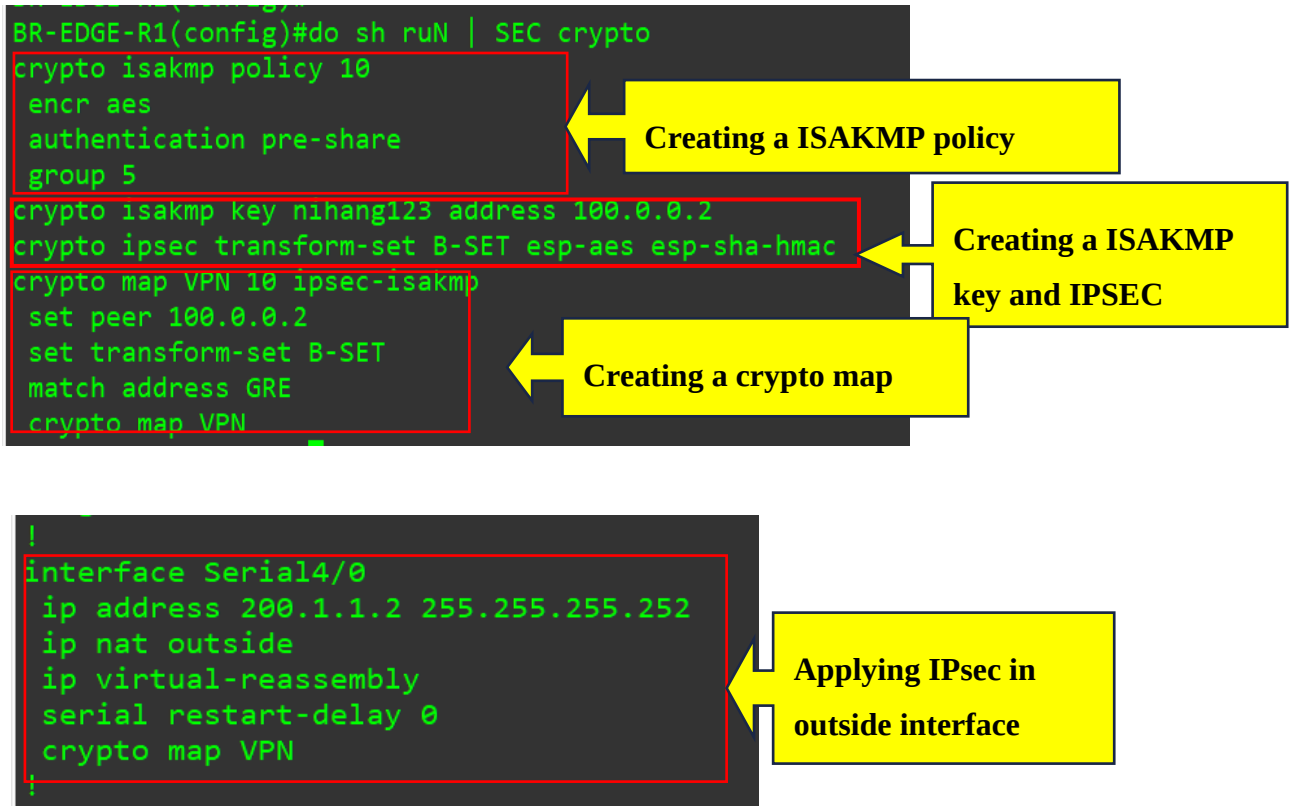


Figure 146: Running config of IPsec BR-EDGE-R

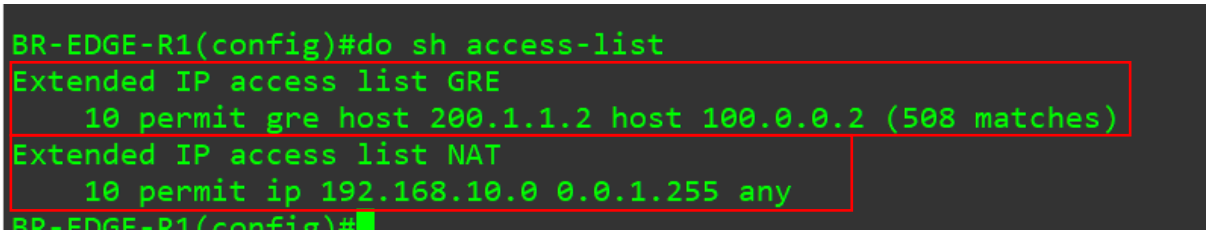


Figure 147: Access-list of GRE tunnel and NAT

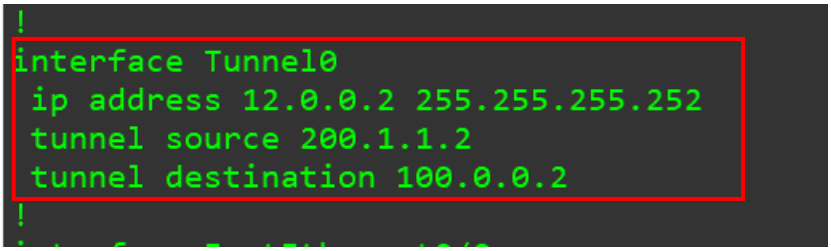


Figure 148: Running configuration of creating tunnel 0

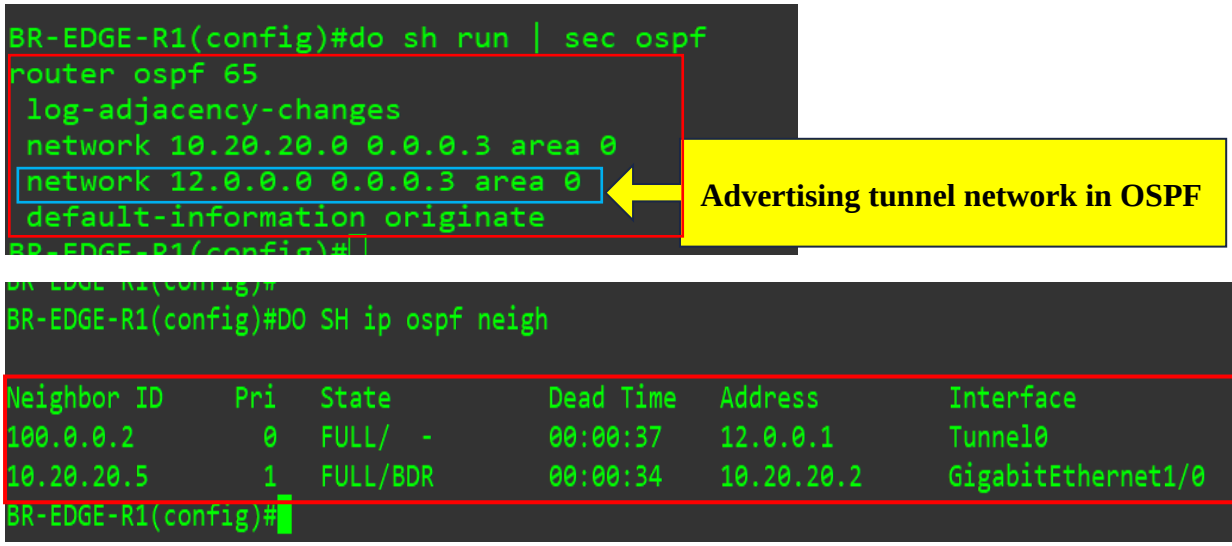


Figure 149: OSPF configuration and OSPF neighborship of BR-EDGE-R1

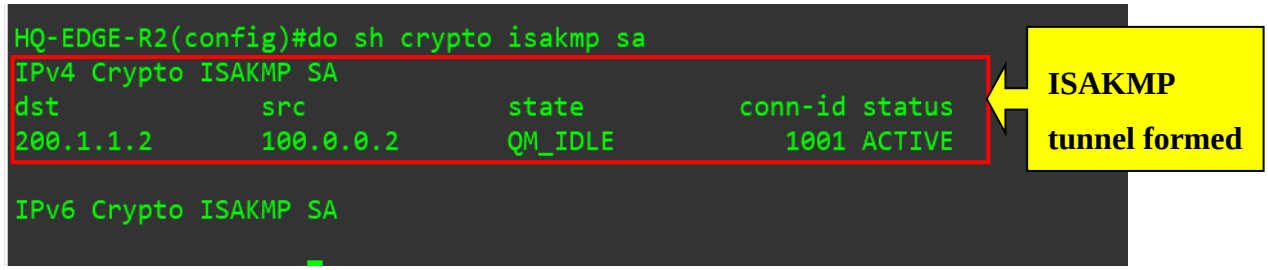


Figure 150: Successful secure tunnel creation in HQ-EDGE-R2

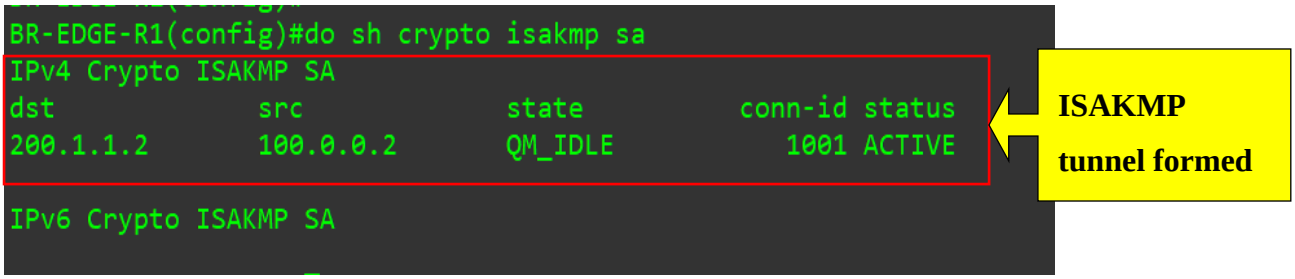


Figure 151: Successful secure tunnel creation in BR-EDGE-R1

GRE over IPsec VPN Verification

From Headquarter to Branch

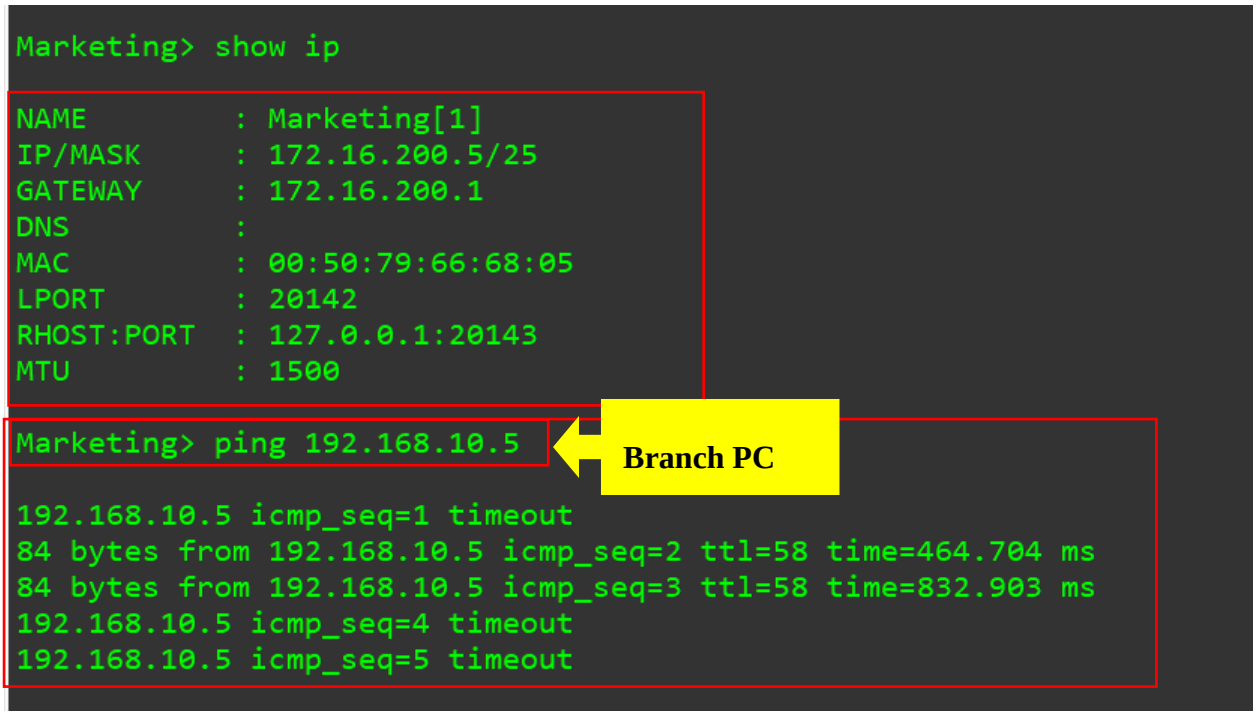


Figure 152: Pinging from Headquarter marketing to branch marketing department

From branch to headquarter

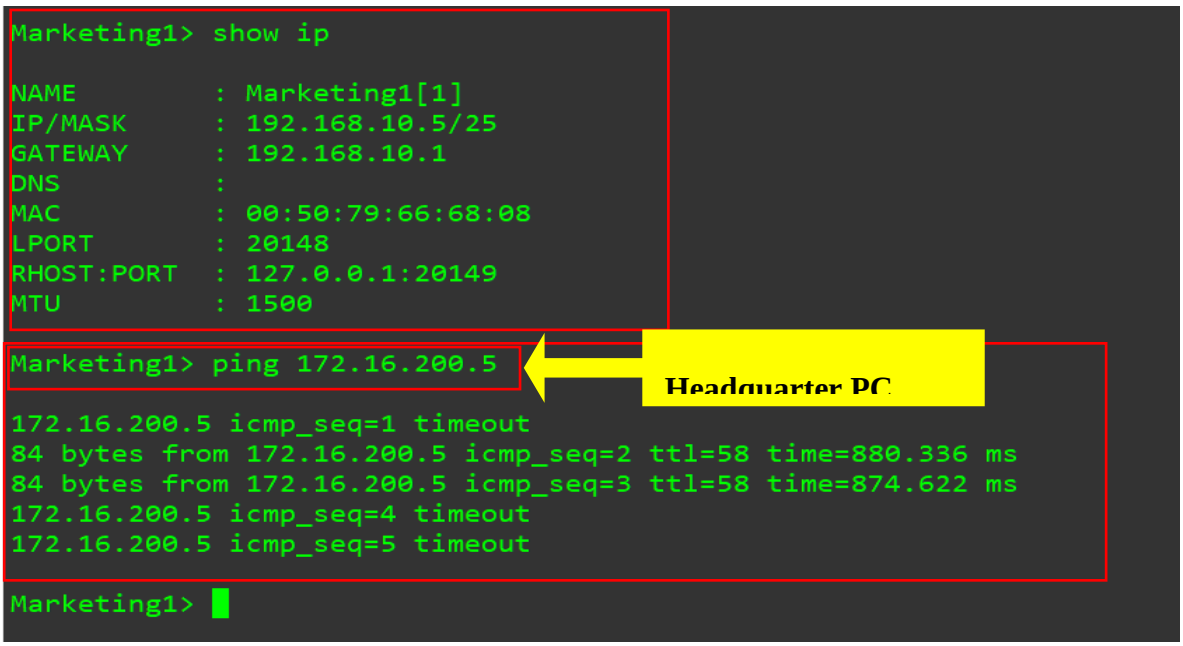


Figure 153: Pinging from branch marketing to headquarter marketing department

DHCP from HQ to branch

```
HQ-CORE-R2(config)#do sh run | sec BRANCH
ip dhcp pool BRANCH
   network 192.168.10.128 255.255.255.192
   default-router 192.168.10.129
   domain-name nihangchha.com
   dns-server 80.88.88.4
HQ-CORE-R2(config)#
```

DHCP pool

Figure 154: DHCP running Config of branch sales department in headquarter

```
HQ-CORE-R2(config)#do sh run | sec Loopback
interface Loopback0
 ip address 55.55.55.55 255.255.255.255
HQ-CORE-R2(config)#
```

Figure 155: Using loopback address for DHCP server in HQ-CORE-R2

```
interface Vlan20
 ip address 192.168.10.129 255.255.255.192
 ip helper-address 55.55.55.55
```

DHCP Relay Agent

Lookback interface of HQ

Figure 156: Running config of sales SVI in branch and relay agent in BR-DISTRI-SW

```
Sales1> ip dhcp
DDORA IP 192.168.10.130/26 GW 192.168.10.129

Sales1> show ip

NAME          : Sales1[1]
IP/MASK       : 192.168.10.130/26
GATEWAY       : 192.168.10.129
DNS           : 80.88.88.4
DHCP SERVER   : 10.1.1.5
DHCP LEASE    : 86391, 86400/43200/75600
DOMAIN NAME   : nihangchha.com
MAC           : 00:50:79:66:68:09
LPORT         : 20150
RHOST:PORT    : 127.0.0.1:20151
MTU           : 1500

Sales1> ping 172.16.200.5

172.16.200.5 icmp_seq=1 timeout
172.16.200.5 icmp_seq=2 timeout
172.16.200.5 icmp_seq=3 timeout
172.16.200.5 icmp_seq=4 timeout
84 bytes from 172.16.200.5 icmp_seq=5 ttl=58 time=444.761 ms
```

DORA process

Headquarter PC

Figure 157: IP obtained from headquarter DHCP server

```
HQ-EDGE-R2(config)#do sh crypto ipsec sa

interface: Serial4/0
    Crypto map tag: VPN, local addr 100.0.0.2

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (100.0.0.2/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (200.1.1.2/255.255.255.255/
   current_peer 200.1.1.2 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 653, #pkts encrypt: 653, #pkts digest: 653
    #pkts decaps: 621, #pkts decrypt: 621, #pkts verify: 621
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 9, #recv errors 0

     local crypto endpt.: 100.0.0.2, remote crypto endpt.: 200.1.1.2
     path mtu 1500, ip mtu 1500, ip mtu idb Serial4/0
     current outbound spi: 0x657227A4(1701980068)
     PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: 0x7FCECAE9(2144258793)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 3, flow_id: SW:3, sibling_flags 80000046, crypto map: VPN
        sa timing: remaining key lifetime (k/sec): (4586376/2225)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE
```

No. of GRE packets encapsulation, decapsulation, encryption, and decryption

Figure 158: Encryption of GRE packet by IPsec in HQ-EDGE-R2

```
BR-EDGE-R1(config)#DO SH crypto ipsec sa

interface: Serial4/0
    Crypto map tag: VPN, local addr 200.1.1.2

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (200.1.1.2/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (100.0.0.2/255.255.255.255/47/0)
   current_peer 100.0.0.2 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 639, #pkts encrypt: 639, #pkts digest: 639
    #pkts decaps: 671, #pkts decrypt: 671, #pkts verify: 671
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 4, #recv errors 0

     local crypto endpt.: 200.1.1.2, remote crypto endpt.: 100.0.0.2
     path mtu 1500, ip mtu 1500, ip mtu idb Serial4/0
     current outbound spi: 0x7FCECAE9(2144258793)
     PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: 0x657227A4(1701980068)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 3, flow_id: SW:3, sibling_flags 80000046, crypto map: VPN
        sa timing: remaining key lifetime (k/sec): (4540542/2052)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE
```

No. of GRE packets encapsulation, decapsulation, encryption, and decryption

Figure 159: GRE encrypted by IPsec protocol in BR-EDGE-R1

WLC (Wireless LAN Controller)

For configuring WLC and managing the guest who are using wireless device to connected the network, I have created a separate VLAN 888 in headquarter and VLAN 600 in branch. The AP connected to end switches link is made up trunk link and native VLAN 999 in HQ and VLAN 99 in branch because following management VLANs does not add VLAN tag header in ethernet frame instead VLAN 888 (Guest) in HQ and VLAN 600 (Guest) in branch added a VLAN tag header.

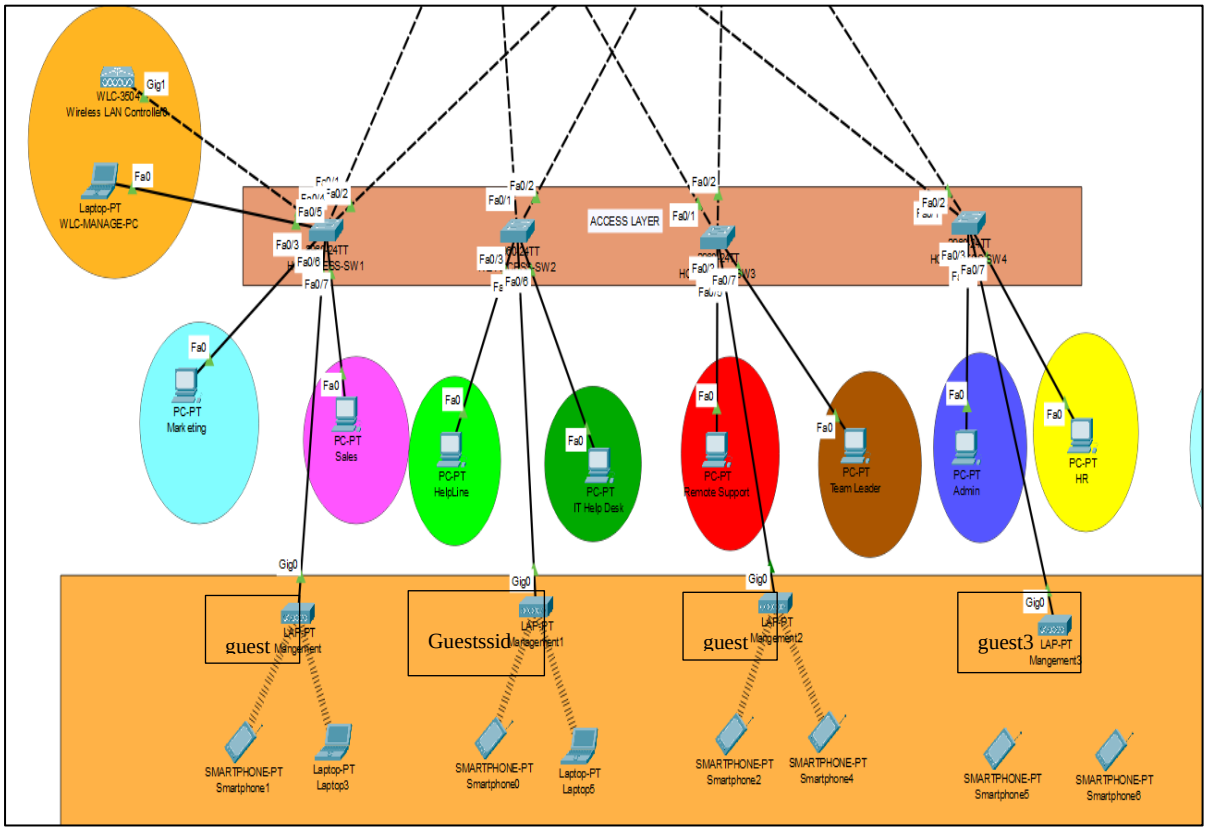


Figure 160: WLC and APS with different end PC and wireless device

WLC configuration

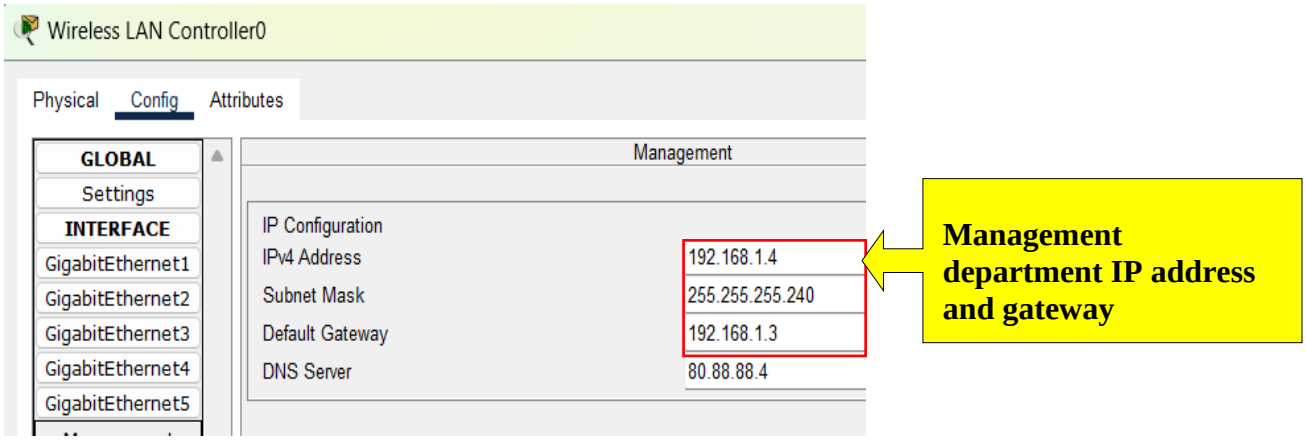


Figure 161: Assigning IP address to WLC in management VLAN

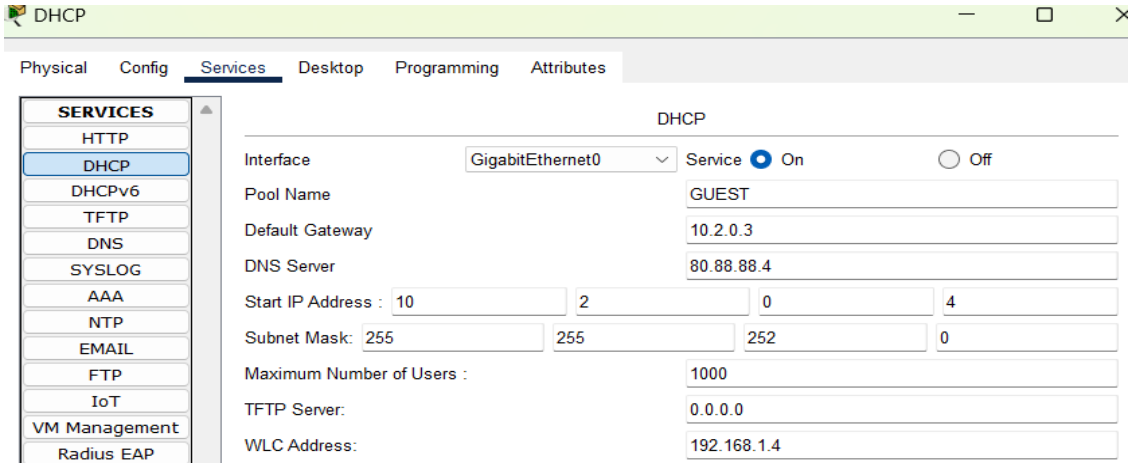


Figure 162: DHCP server guest VLAN configuration

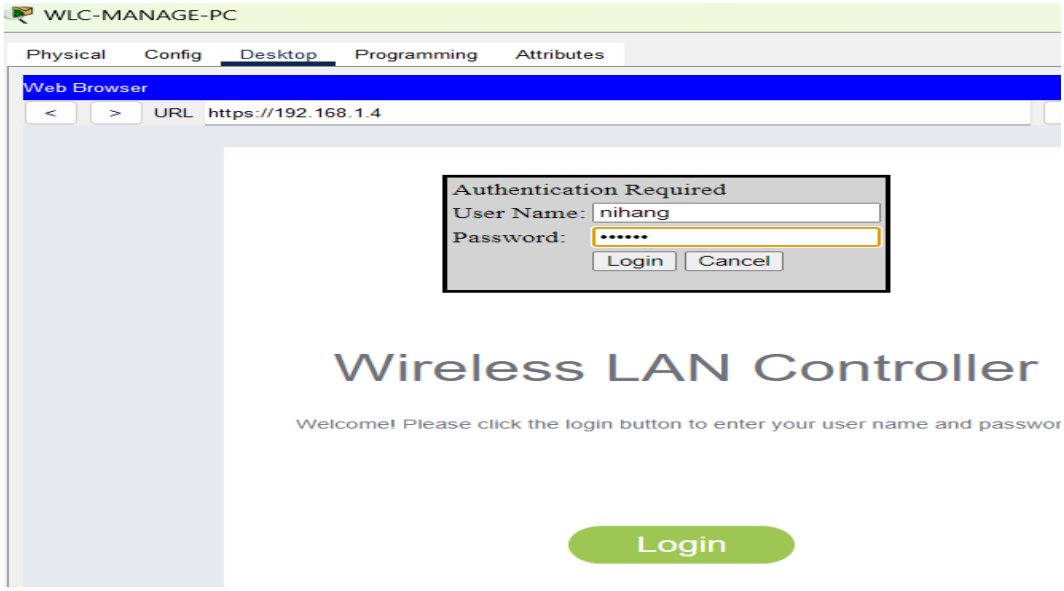


Figure 163: Configuring WLC from PC using web browser

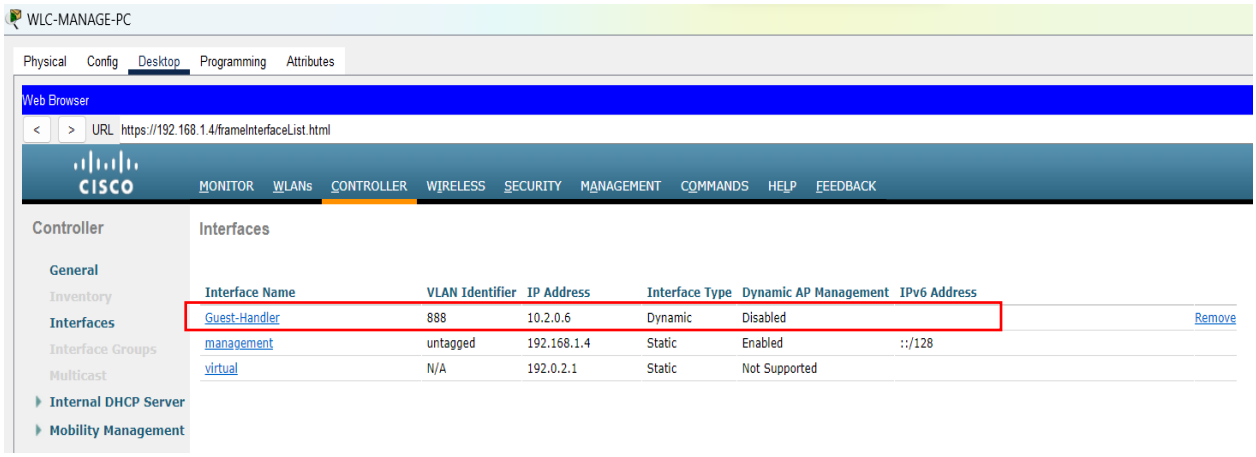


Figure 164: Creating a Guest-Handler interface

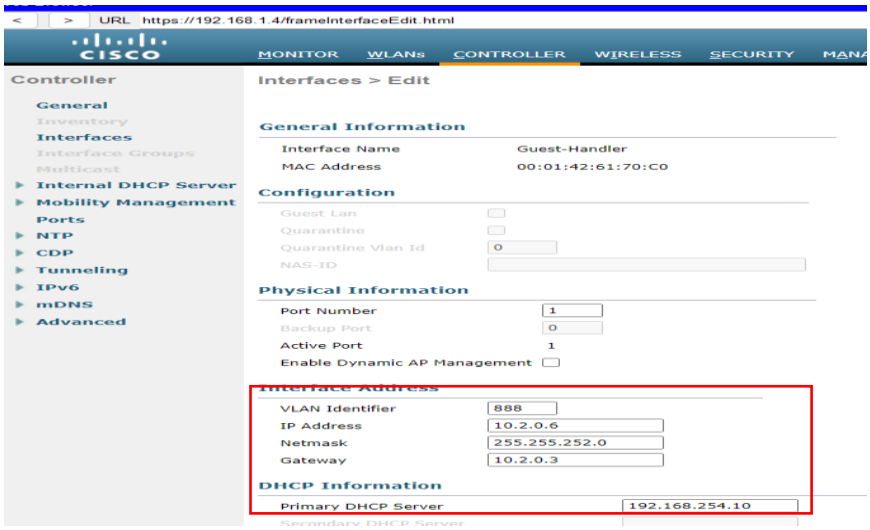


Figure 165: Interface information

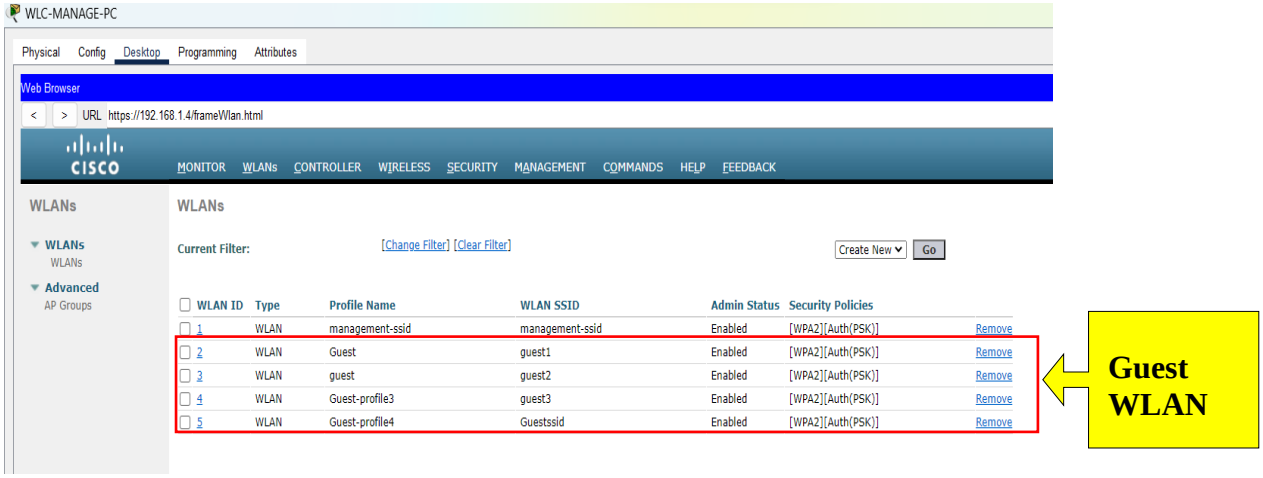


Figure 166: WLANs in WLC

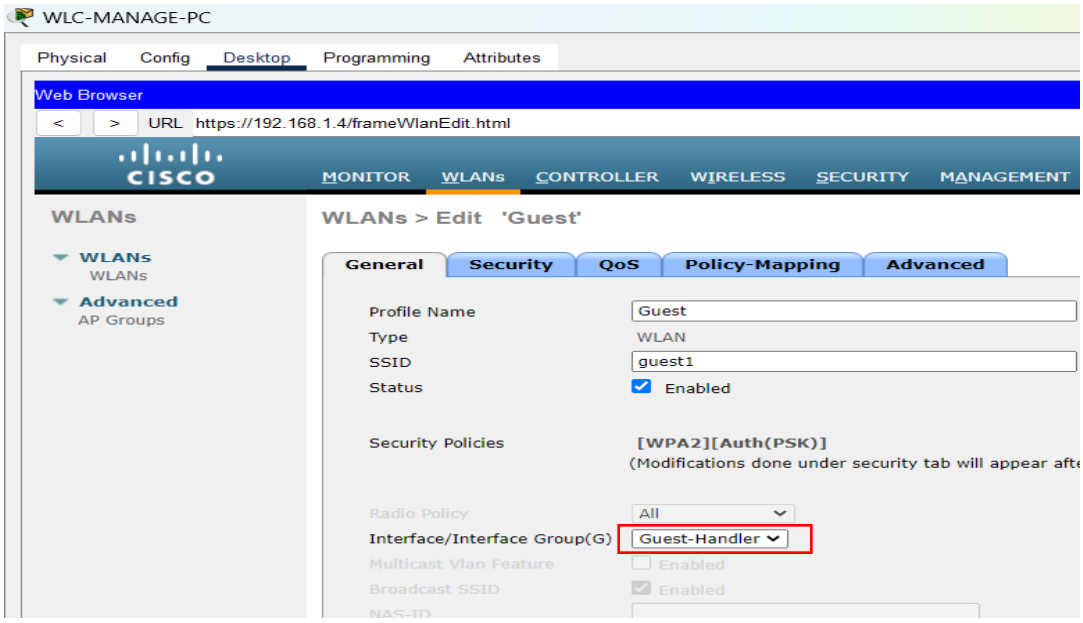


Figure 167: Create a WLAN as required and inside it add guest interface, SSID name, Profile Name.

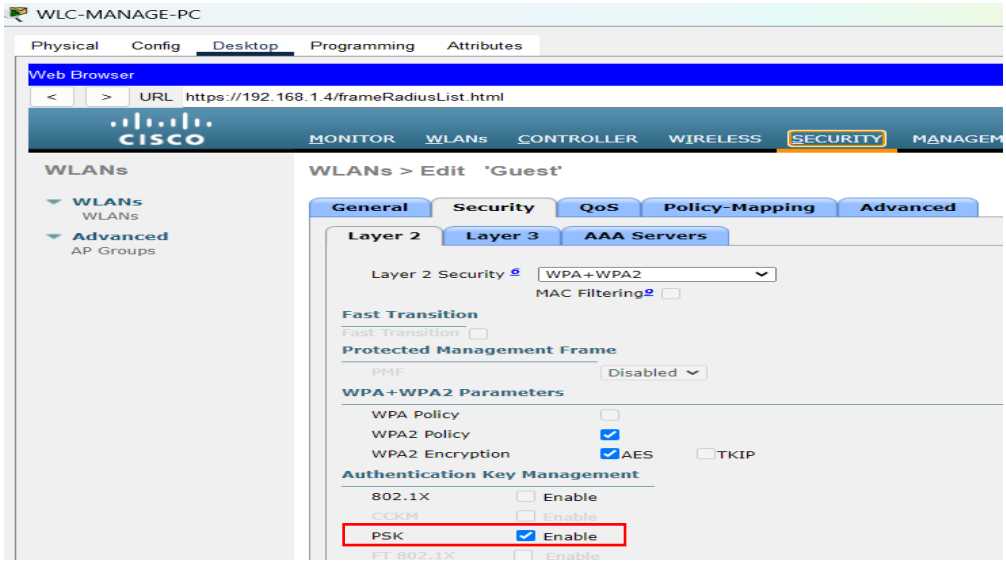


Figure 168: Security tab inside of WLAN

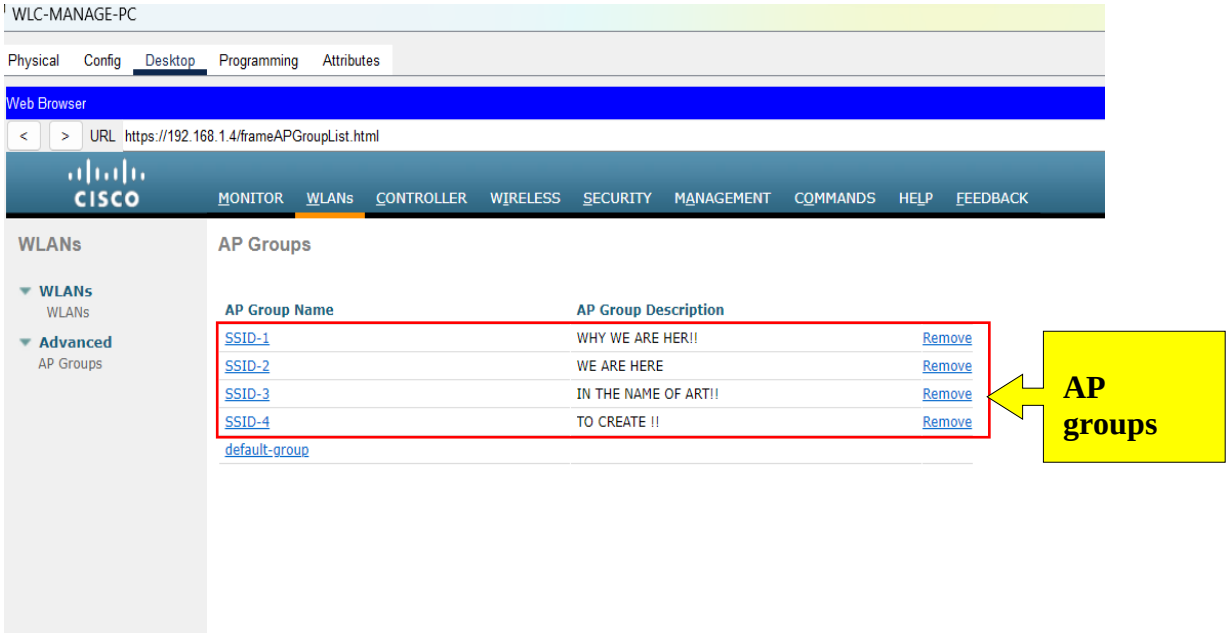


Figure 169: AP groups in WLANs

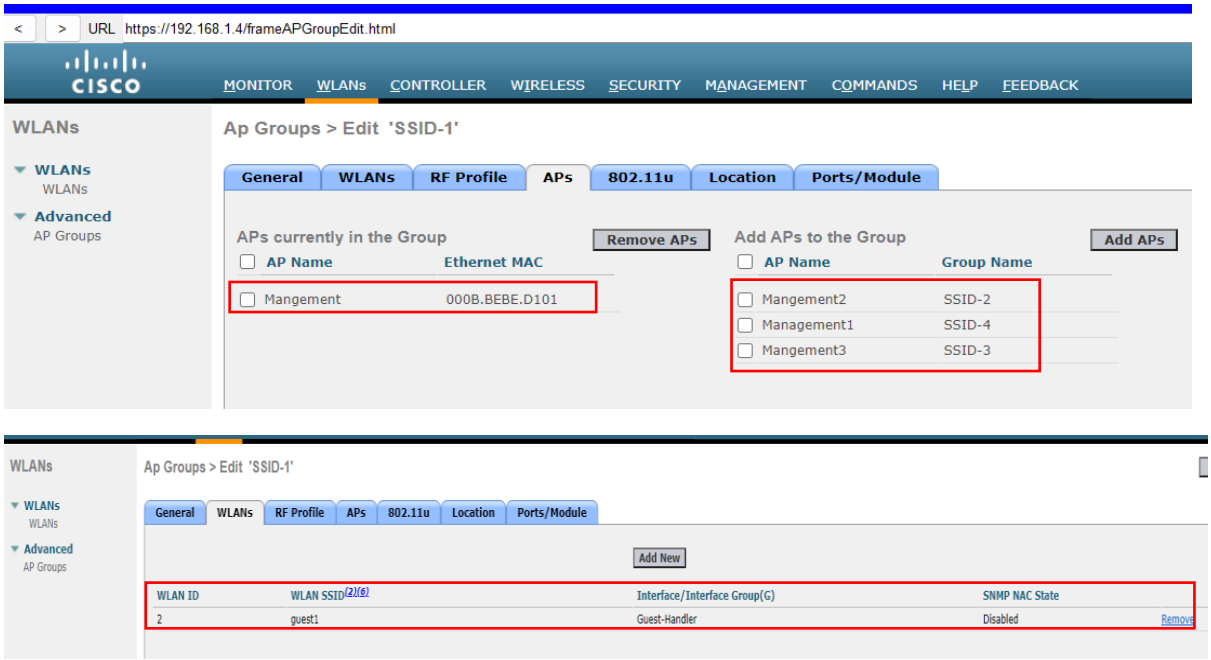


Figure 170: Inside AP groups add WLAN and Access-point

WLC Verification

Headquarter

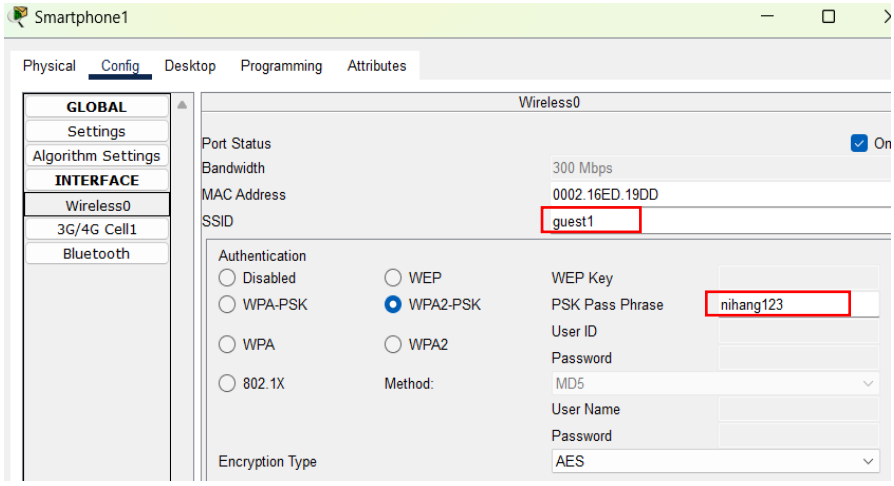


Figure 171: SSID name and password

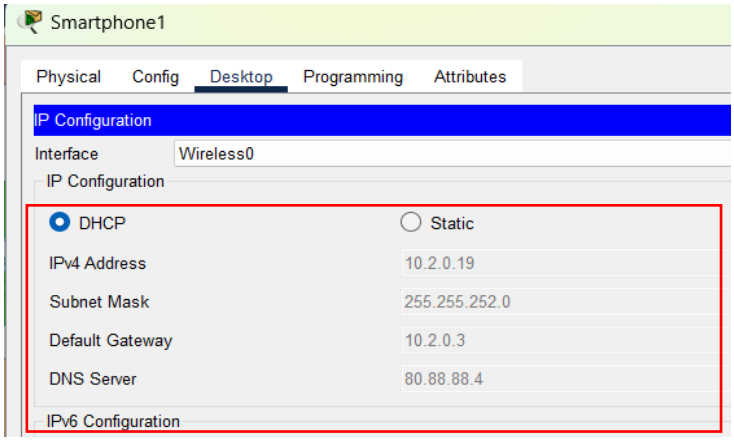


Figure 173: IP obtained from DHCP headquarter

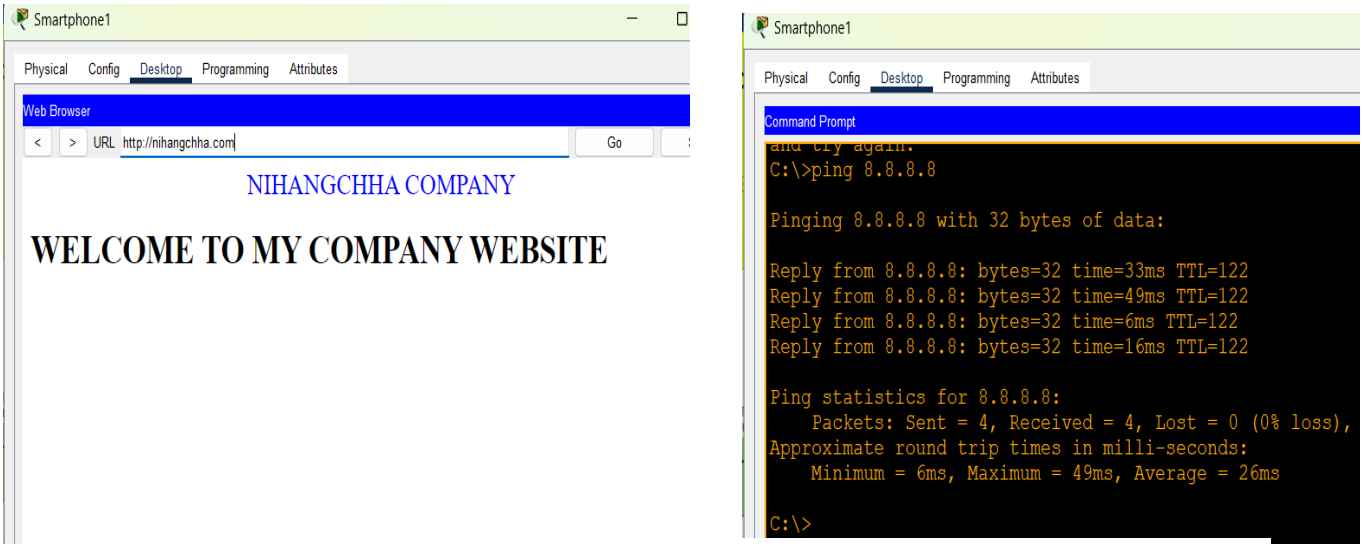


Figure 172: WLC verification in HQ through web browser and ping

Branch

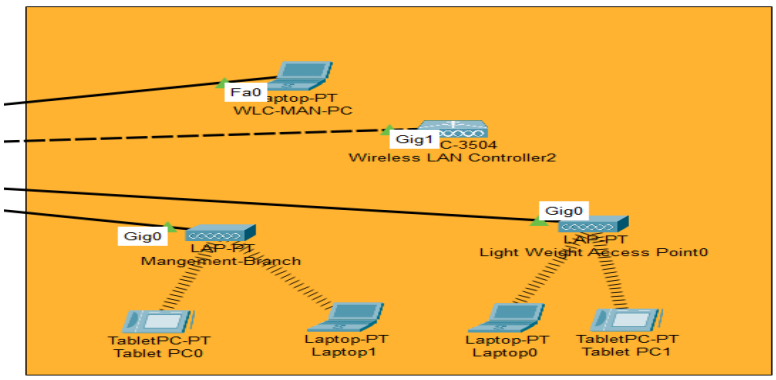


Figure 174: WLC region of Branch

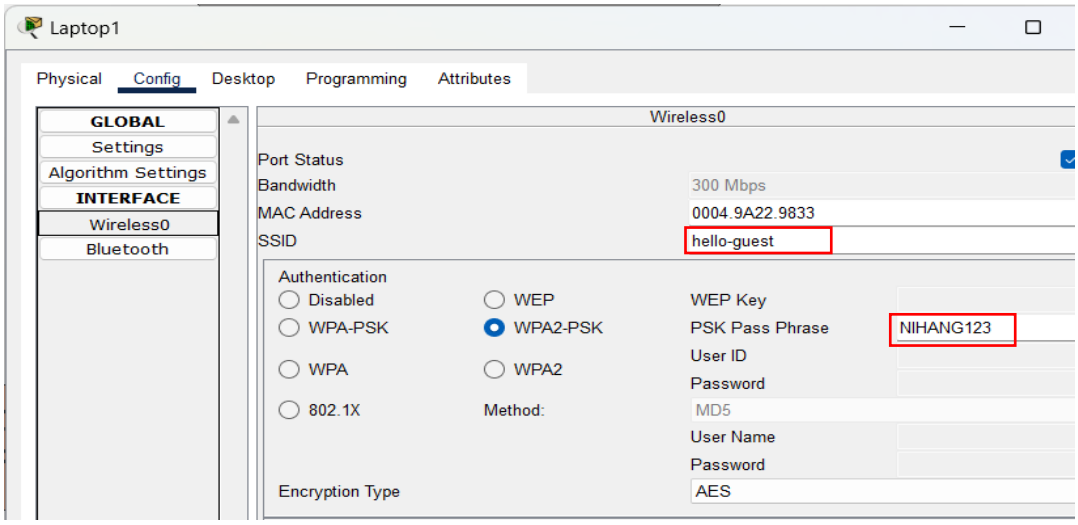


Figure 175: SSID and password

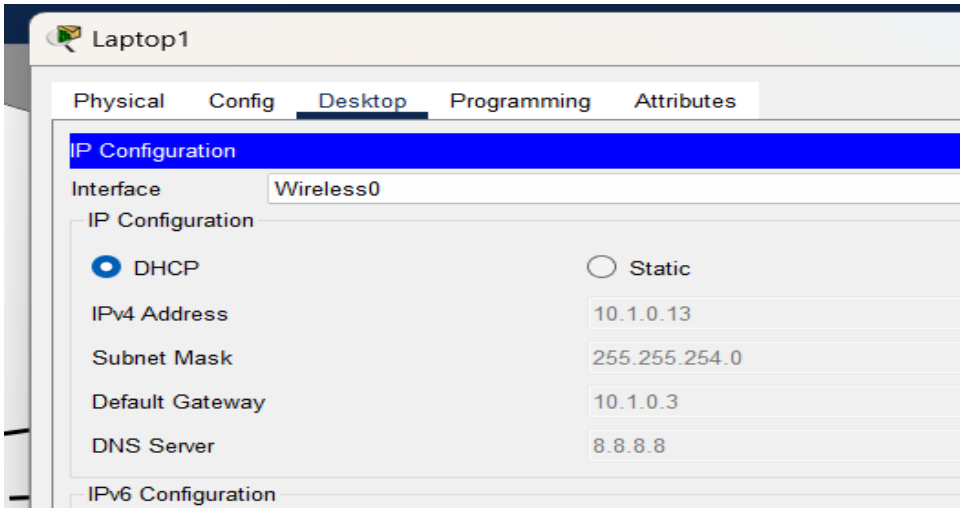


Figure 176: IP obtained from DHCP server in branch laptop

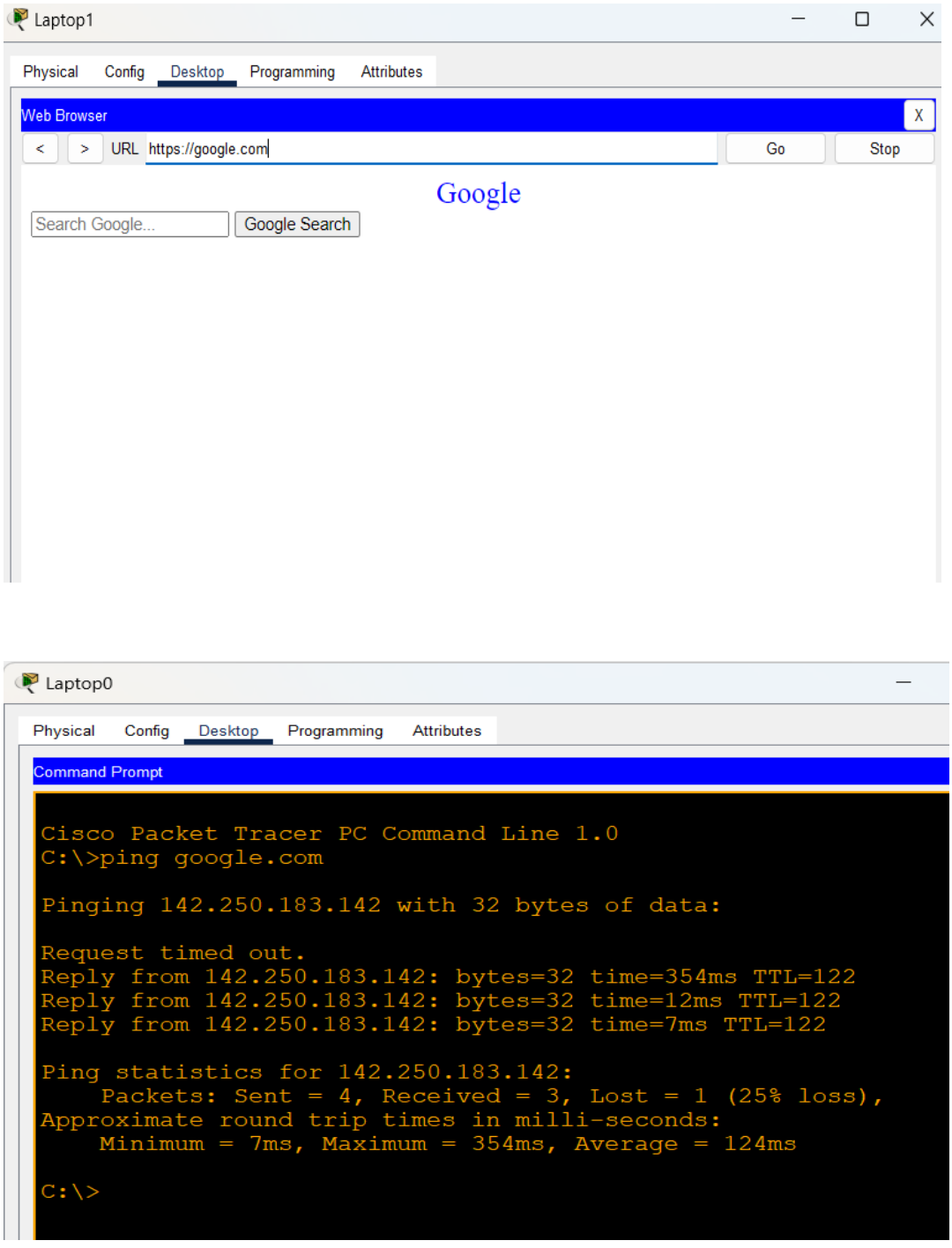


Figure 177: WLC verification in branch through web browser and ping

SERVER

NTP server

Time is essential for tracking events happening inside the system, so an NTP server is configured in the Google area where time and data are referenced from Google's time. Google updates its time from a reference clock and is known as stratum 1, while we update the clock from Google, making it stratum 2.

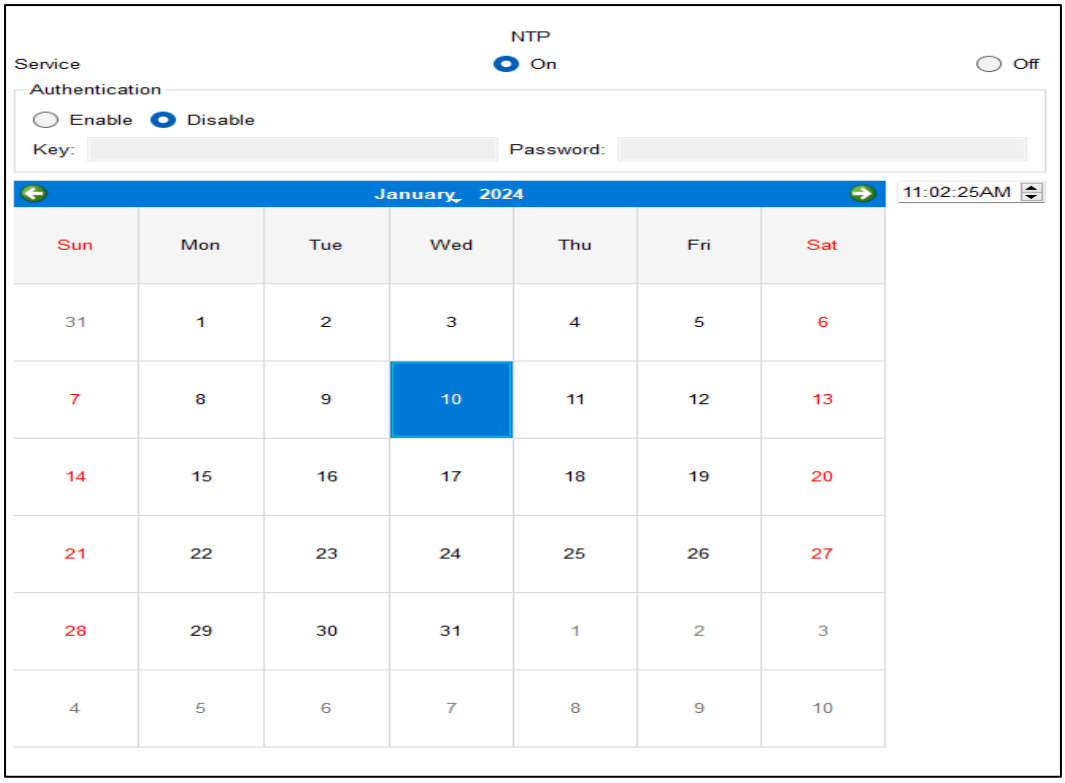


Figure 178: Google NTP server

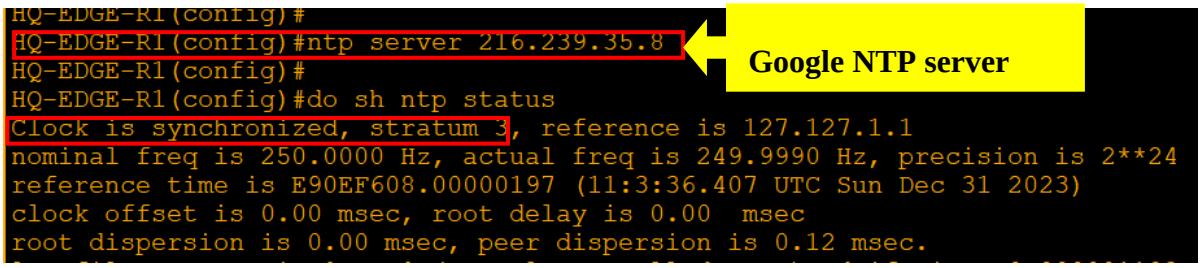


Figure 179: Synchronizing the HQ-EDGE-R1 and BR-EDGE-R2 with google NTP clock

```
HQ-EDGE-R1(config)#do sh clock
11:4:3.986 UTC Sun Dec 31 2023
HQ-EDGE-R1(config)#
```

```
HQ-EDGE-R1(config)#ntp update-calendar
HQ-EDGE-R1(config)#
```

Updating Software hardware clock

```
BR-EDGE-R1(config)#ntp server 216.239.35.8
BR-EDGE-R1(config)#do sh ntp status
Clock is synchronized, stratum 3, reference is 127.127.1.1
nominal freq is 250.0000 Hz, actual freq is 249.9990 Hz, precision is 2**24
reference time is E90EF62F.00000365 (11:4:15.869 UTC Sun Dec 31 2023)
clock offset is 0.00 msec, root delay is 0.00  msec
root dispersion is 0.00 msec, peer dispersion is 0.47 msec.
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is - 0.000001193 s/s system poll interval is 6, last update was 9 sec ago.
BR-EDGE-R1(config)#
BR-EDGE-R1(config)#ntp update-calendar
BR-EDGE-R1(config)#
BR-EDGE-R1(config)#do sh clock
11:4:21.733 UTC Sun Dec 31 2023
BR-EDGE-R1(config)#
BR-EDGE-R1(config)#do sh ntp associations

address         ref clock       st   when    poll    reach  delay        offset          disp
*~127.127.1.1   .LOCL.          2    13      64      377    0.00         0.00            0.47
 ~216.239.35.8  127.127.1.1     1    7       16      1      176.00       863405077.00    0.00
 * sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
```

Syslog Server

Syslog servers are implemented in the headquarter and branch devices for managing and storing the generated log from different devices during the time events.

Headquarter

```
HQ-DISTRI-SW2(config)#logging 192.168.254.11
HQ-DISTRI-SW2(config)#logging trap debugging
```

Syslog server and log generate in remote server up to debugging

```
HQ-DISTRI-SW1(config)#
HQ-DISTRI-SW1(config)# logging 192.168.254.11
HQ-DISTRI-SW1(config)#  logging trap debugging
HQ-DISTRI-SW1(config)#
```

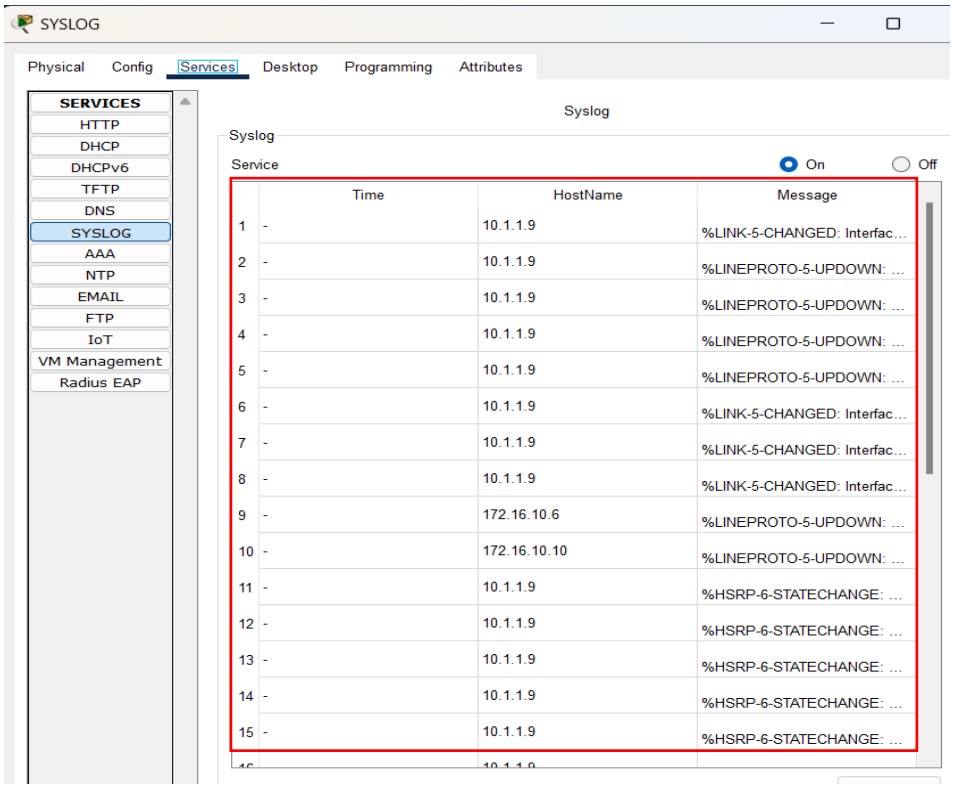


Figure 180: Log stored in Syslog server of Headquarter

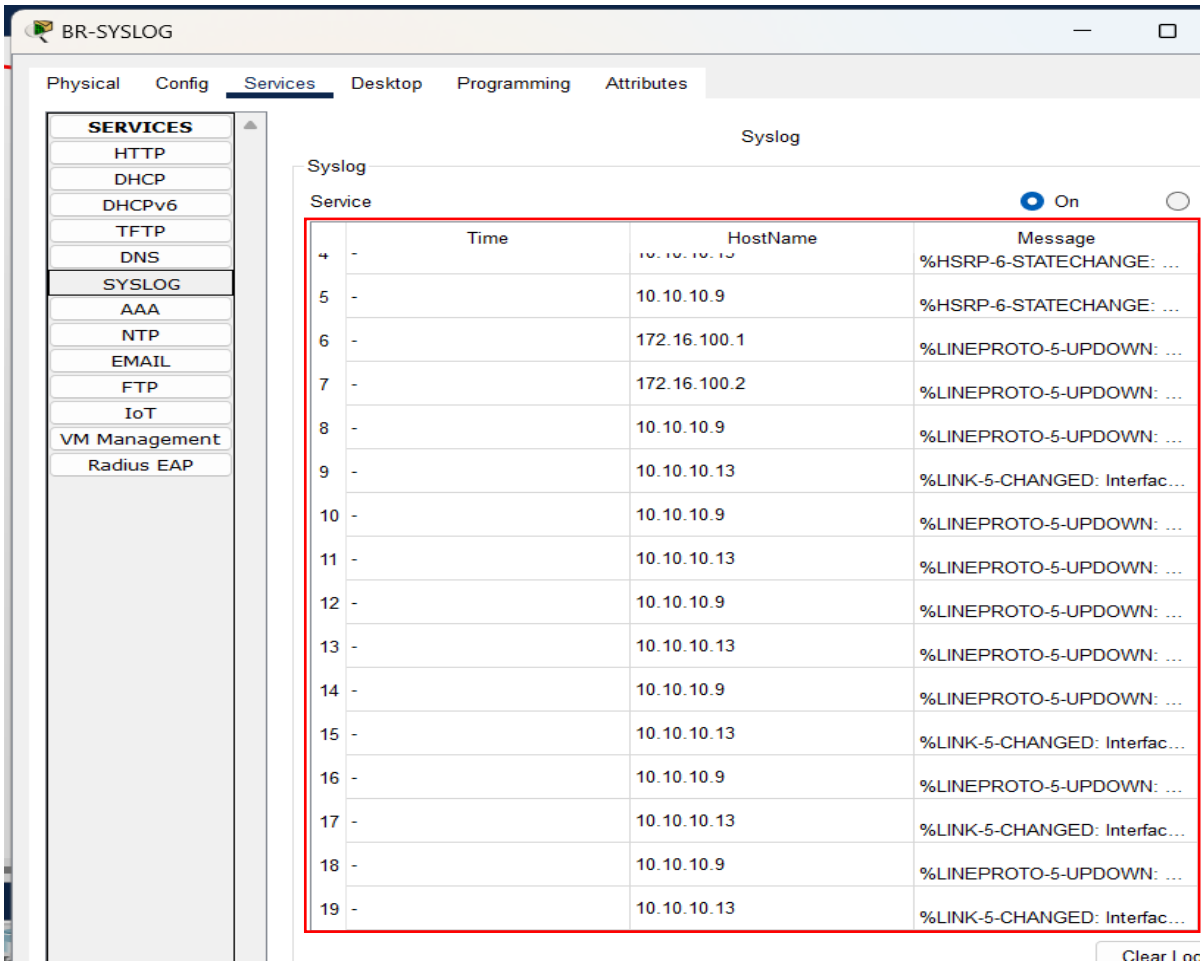
Branch

```
BR-DISTRI-SW1(config)#logging 172.16.100.60
BR-DISTRI-SW1(config)#logging trap debugging
BR-DISTRI-SW1(config)#
```

```
BR-DISTRI-SW2(config)#logging 172.16.100.60
BR-DISTRI-SW2(config)#  logging trap debugging
BR-DISTRI-SW2(config)#
```

Figure

Log stored in syslog server of Branch



SNMP (Simple Network Management Protocol)

Monitoring and managing network devices by the network administrator device, known as Network Management Stations (NMS), through remote access can simplify the process of checking and altering the status of managed devices like router, switch, including monitoring performance, health, and overall status. Network administrators can efficiently perform these tasks without the need to manually inspect and debug each device within the system. SNMP service can be used form the MIB browser.

```
down down
HQ-EDGE-R1(config)#snmp-server community canread ro
HQ-EDGE-R1(config)#snmp-server community canwrite rw
HQ-EDGE-R1(config)#
```

Figure 181: SNMP configuration in HQ-EDGE-R1

Configuring the read only in first command and read and write in second command with authentication key.

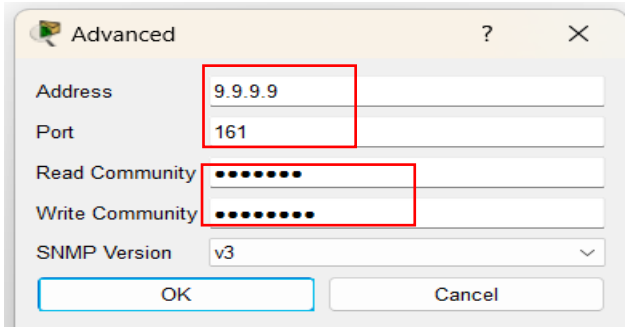


Figure 182: Authentication of read and write community of Managed Device in MIB browser

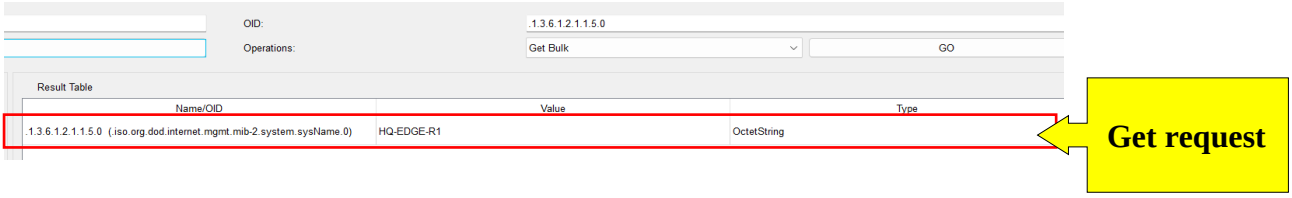


Figure 183: GET and SET request from the SNMP NMS (Network Management System)

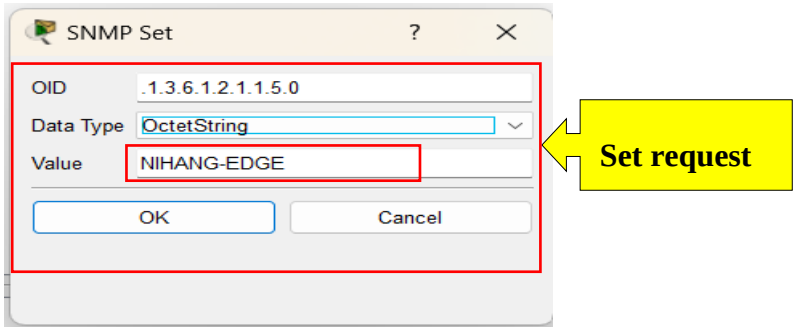


Figure 184: Changing hostname of HQ-EDGE-R1 by SNMP

```
NIHANG-EDGE(config)#do sh run | sec hostname
hostname NIHANG-EDGE
NIHANG-EDGE(config)#
```

Figure 185: Hostname change also takes effect in running config

```
BR-CORE-R2(config)#snmp-server community hehe rw
%SNMP-5-WARMSTART: SNMP agent on host BR-CORE-R2 is undergoing a
warm start
BR-CORE-R2(config)#snmo
BR-CORE-R2(config)#snmp-server community hehehe ro
```

Figure 186: SNMP configuration in BR-CORE-R2

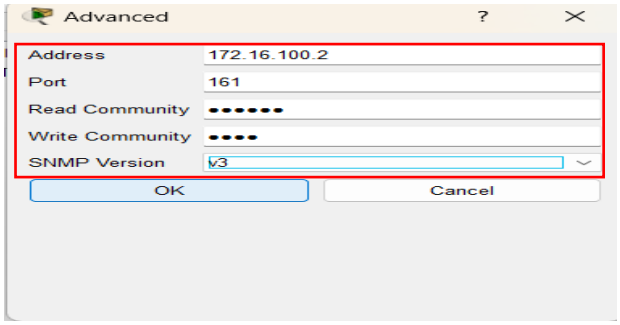


Figure 187: Authentication of Managed device in MIB browser

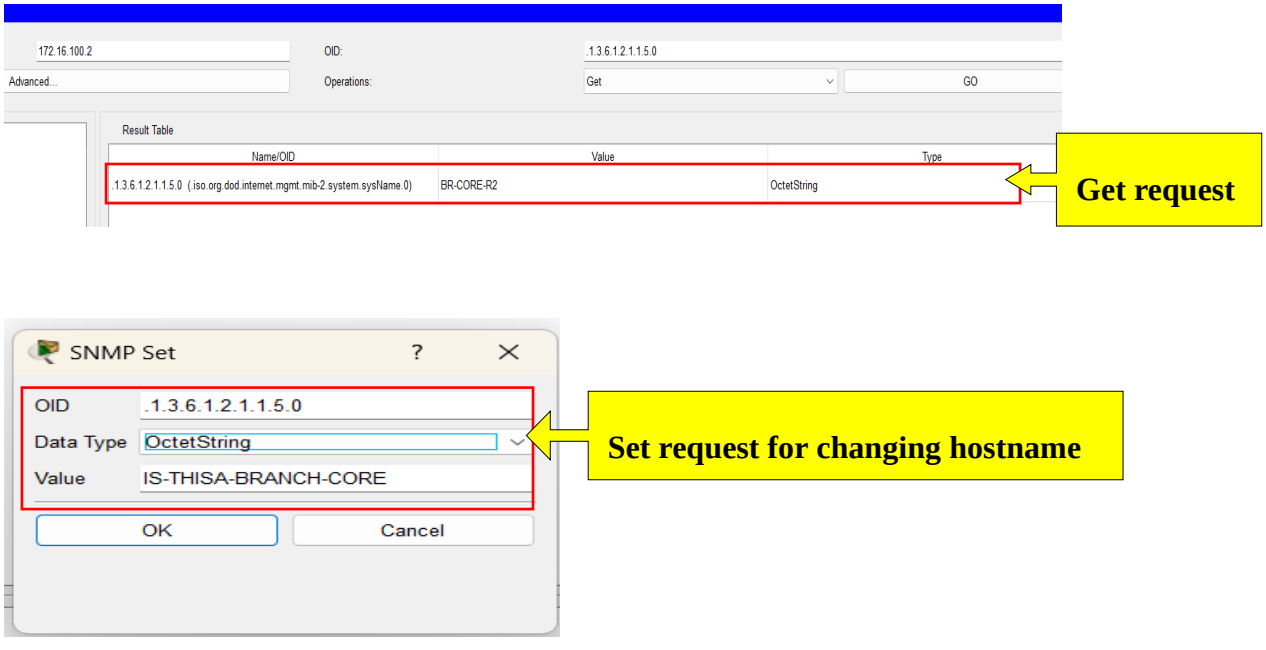


Figure 188: Requesting GET and SET from SNMP NMS

```
IS-THISA-BRANCH-CORE(config)#do sh run | sec hostname
hostname IS-THISA-BRANCH-CORE
IS-THISA-BRANCH-CORE(config)#
```

Figure 189: Hostname change also takes effect in running config of Branch

AAA (Authentication, Authorization, Accounting)

Configuring login authentication services setting like SSH or Telnet across network devices can be time-consuming and may lead to the risk of forgetting authentication information. To address these challenges, most of the big company implements AAA TACACS+ server in private network. This server effectively manages all credentials, providing a centralized and secure way to handle authentication, authorization, and accounting for various network devices.

```
HQ-CORE-R1(config)#username nihang password nihang
HQ-CORE-R1(config)#enable secret nihang
HQ-CORE-R1(config)#
HQ-CORE-R1(config)#aaa new-model
HQ-CORE-R1(config)#
HQ-CORE-R1(config)#aaa authentication login AUTH group tacacs+ local
HQ-CORE-R1(config)#tacacs-server host 192.168.254.200 key nihang123
HQ-CORE-R1(config)#
```

Figure 190: Configuration of TACAS+ client in HQ-CORE-R1

```
HQ-CORE-R1(config)#ip domain-name nihangchha.com
HQ-CORE-R1(config)#crypto key gen rsa
The name for the keys will be: HQ-CORE-R1.nihangchha.com
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
```

```
HQ-CORE-R1(config)#line vty 0 4
*Dec 31 11:34:12.113: %SSH-5-ENABLED: SSH 1.99 has been enabled
HQ-CORE-R1(config-line)#transport input ssh
HQ-CORE-R1(config-line)#login authentication AUTH
```

Figure 191: Configuration of SSH in HQ-CORE-R1

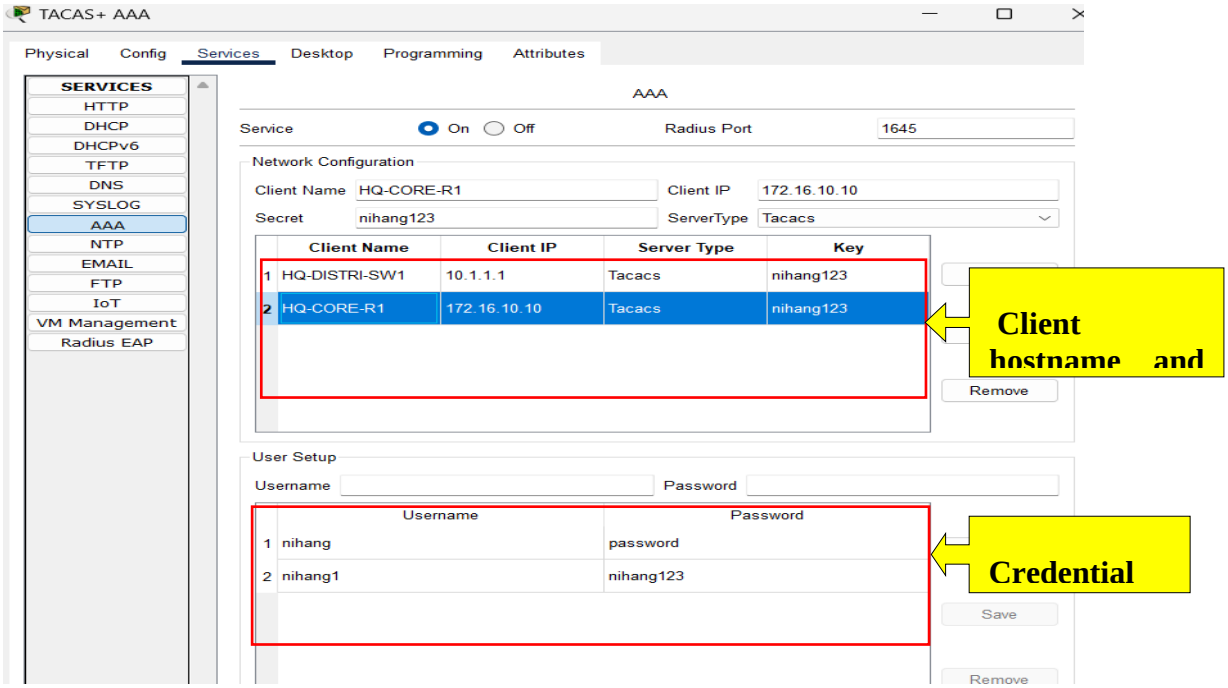


Figure 192: Configuration of TACAS+ server

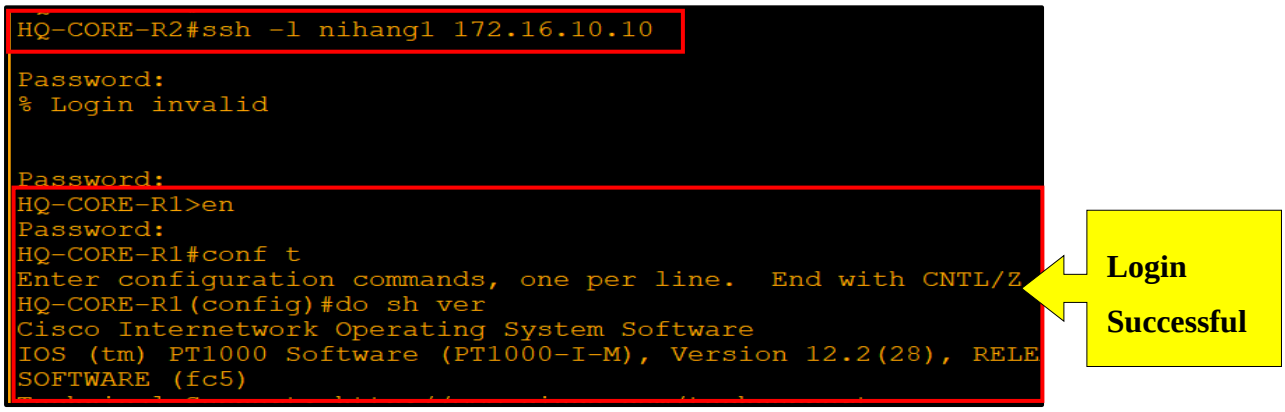


Figure 193: AAA verification

DNS (Domain Name System)

In today's internet, expecting an individual to memorize the IP addresses of every webpage is both challenging and impractical. To overcome this difficulty, DNS (Domain Name System) plays a vital role by translating the domain names of web servers into IP addresses and vice versa. In this project, a DNS server is implemented in the DMZ area and Google area.

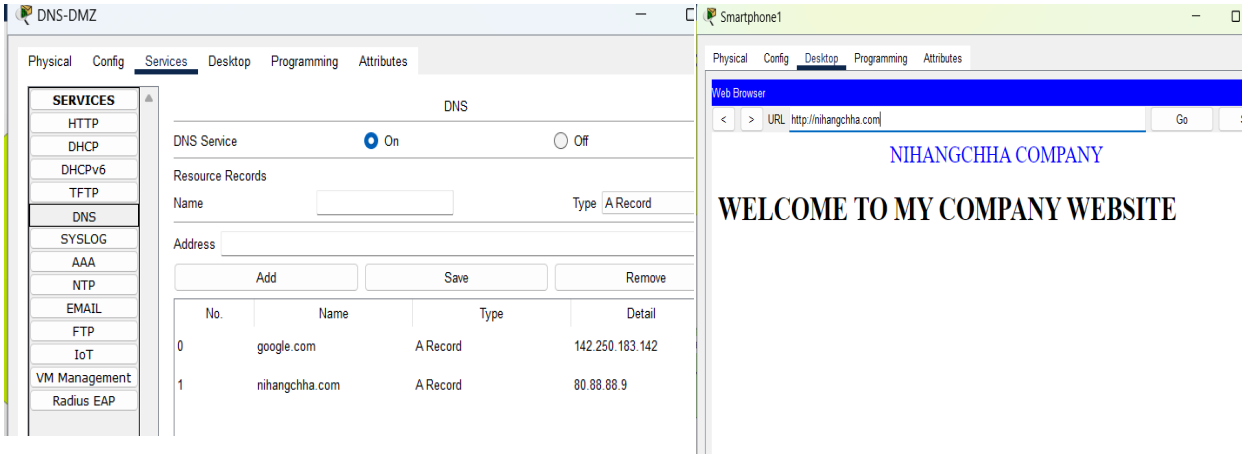


Figure 194: DNS server of DMZ and webserver hosting in DMZ area

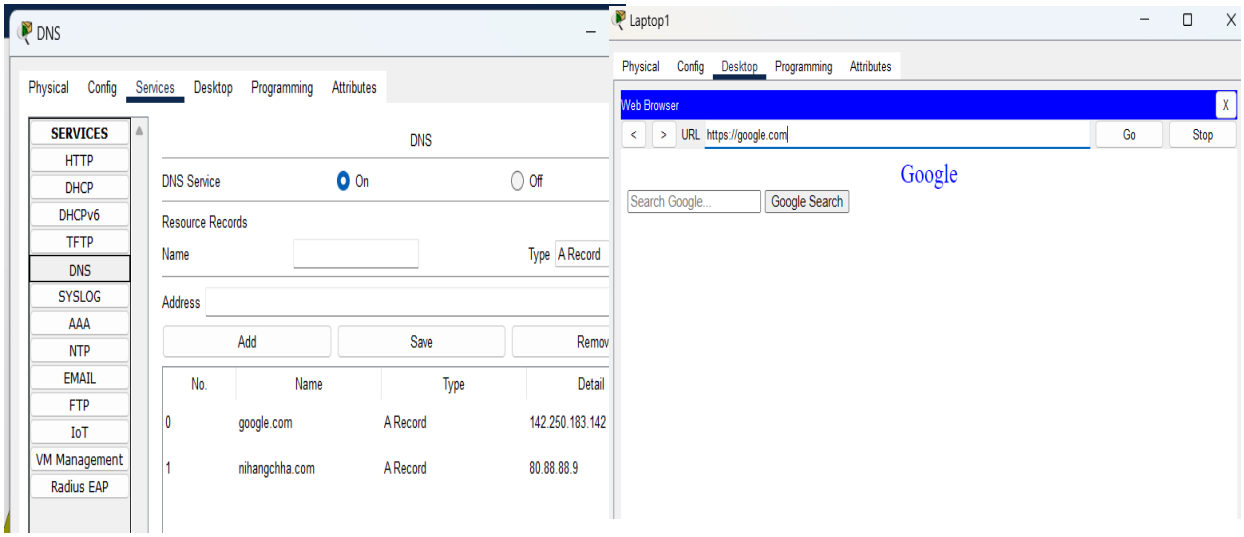


Figure 195: DNS server of Google and webserver hosting in google area

Firewall

A firewall is implemented in this network to provide a critical layer of security and traffic control between the internal network and external networks such as the internet. It acts as a barrier, monitoring and filtering incoming and outgoing traffic based on predefined security rules, helping to prevent unauthorized access, cyberattacks, and the spread of malware. By controlling what traffic is allowed or denied, the firewall ensures that only legitimate, safe communications occur, protecting sensitive data and maintaining network integrity. Firewall was implemented at different physical diagram due to some issue with the cisco packet tracer.

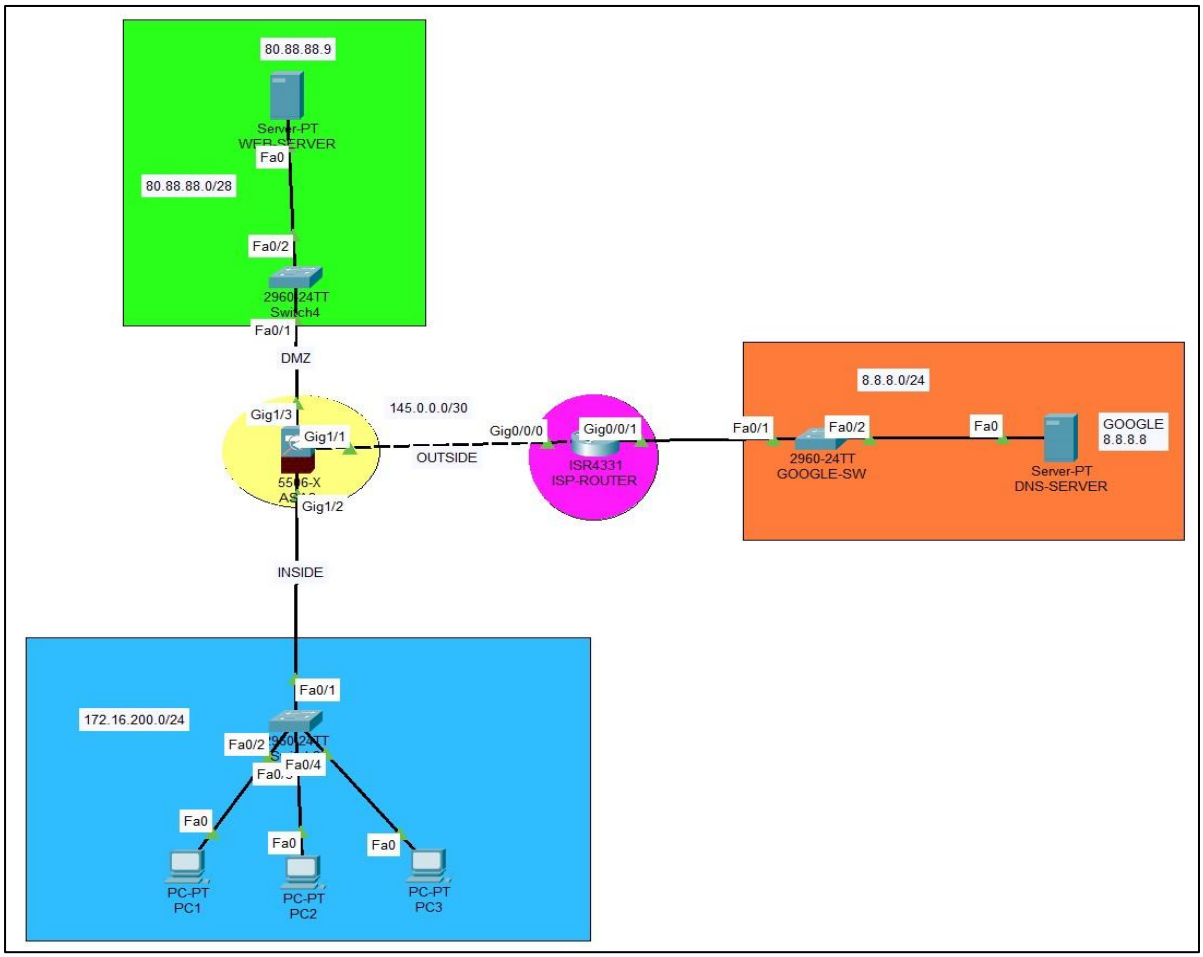


Figure 196: Physical diagram with implementation of firewall

In this topology, there are three area ‘inside’ where private network of company is placed, ‘DMZ’ company web server is placed, and ‘outside’ a simple google DNS server is placed.

Firewall

```
!
interface GigabitEthernet1/1
 nameif outside
 security-level 0
 ip address 145.0.0.2 255.255.255.252
!
interface GigabitEthernet1/2
 nameif inside
 security-level 100
 ip address 172.16.200.1 255.255.255.0
!
interface GigabitEthernet1/3
 nameif DMZ
 security-level 50
 ip address 80.88.88.1 255.255.255.240
!
```

Figure 197: Assigning name, security, and IP address to interfaces

```
!
dhcpd address 172.16.200.10-172.16.200.255 inside
dhcpd dns 8.8.8.8 interface inside
dhcpd lease 8080 interface inside
dhcpd domain nihangchha.com interface inside
dhcpd enable inside
!
```

Figure 198: DHCP server pool creation in firewall

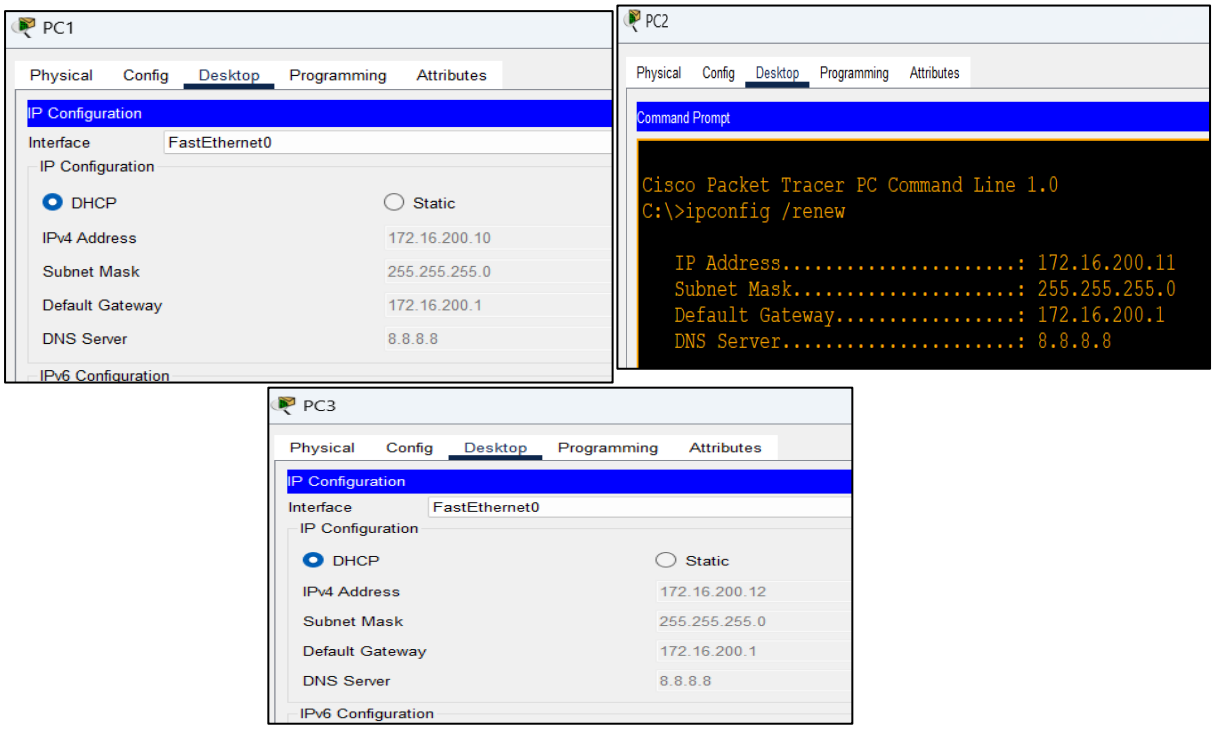


Figure 199: DHCP server verification from firewall

Figure 200: Creating a default static route to outside in firewall

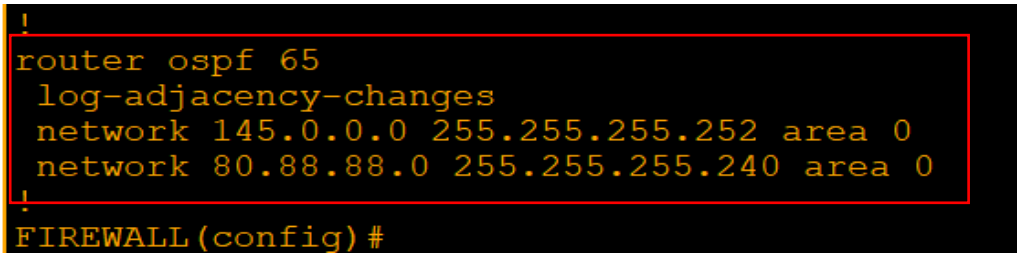


Figure 201: OSPF configuration in firewall

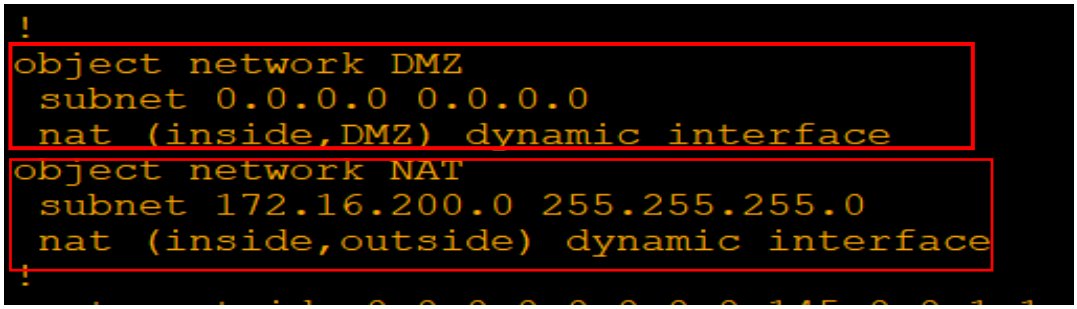


Figure 202: Dynamic NAT config on Firewall

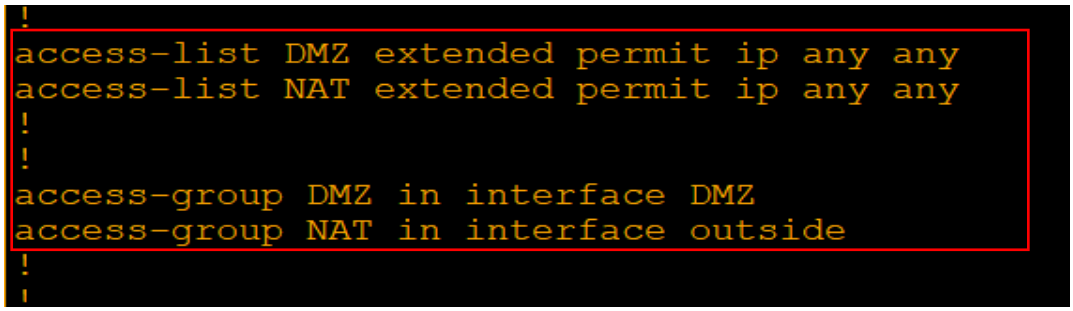


Figure 203: Access list of firewalls

ISP (Internet Service Provider)

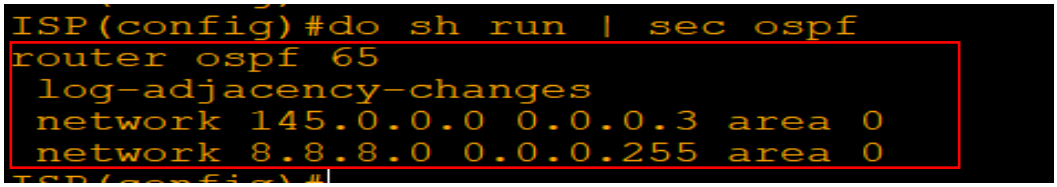


Figure 204: OSPF configuration in ISP router

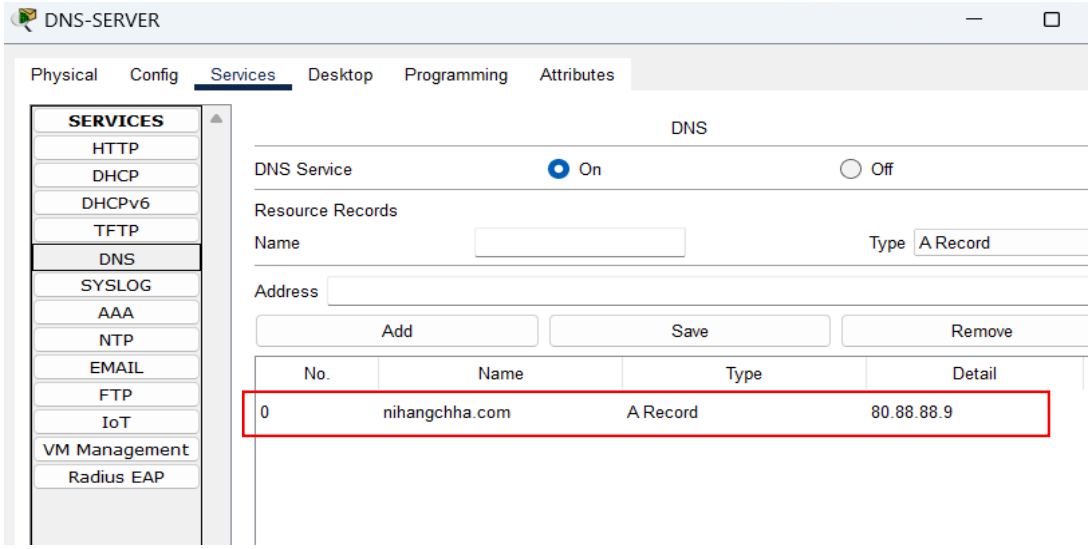


Figure 205: DNS server config

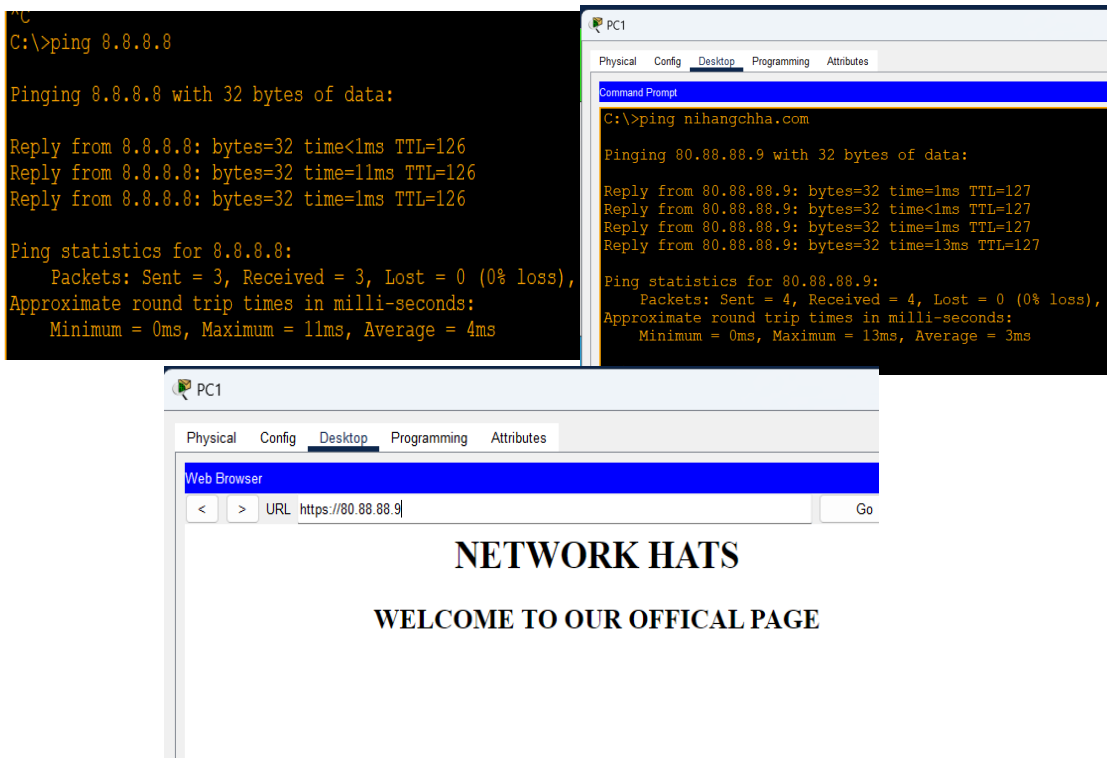


Figure 206: Verification through ping and browser

Risk Management, Compliance, social, and legal issue in networking

The term ‘risk management’ is a pro-active process of identifying, analyzing, monitoring, and managing the potential threat and vulnerabilities that may reside within the organization software or employee, minimizing the total negative impact on organization infrastructures. Compliance is the process of adhering the industrial regulation, standard, and legal requirement to ensure the network data integrity and protect the sensitive data. Social issue concern about the impact of networking technology in society addressing the ethical concerns. Whereas legal issue encompass adherence to laws and regulation governing data protection, privacy, and cybersecurity.

Risk Management

- Identifying and mitigating risks helps ensure the continuous operation of the organization's network infrastructure.
- Effective risk management safeguards sensitive data from potential threats, ensuring the confidentiality, integrity, and availability of critical information.

Compliance:

- Compliance with laws and regulations is essential to avoid legal consequences, fines, and reputational damage, demonstrating the organization commitment to ethical practices and responsible conduct.
- Adhering to industry-specific standards ensures that the organization meets the expectations of customers and partners.

Social Issues:

- Addressing social issues involves making ethical decisions regarding data privacy, user consent, and the social impact of technological.
- Considering the social implications of networking practices helps in building and maintaining trust among users and the broader community.

Legal Issues:

- Navigating legal complexities helps organizations avoid legal challenges and associated financial penalties. It safeguards the organization against legal actions resulting from non-compliance.
- Adhering to legal standards protects the organization's reputation, as legal issues can have a significant impact on how the organization is perceived by the public.

Emerging Trends and technology

Landscape of networking is evolving day by day with a several emerging trends and technology reshaping the traditional network infrastructure. Those advancement include are as follows:

SDN (Software Defined Network)

In traditional network infrastructure, Controlling and managing the network was quitter challenging and inefficient because all of the expertise needs to manage network devices through management plane of device SDN plays a crucial role in addressing this challenge by separating the control plane from the data plane, situated in the southbound interface, facilitating communication between the SDN controller and network devices through APIs like OpenFlow and Floodlight. Control plane can direct the network traffic whereas data plane forwards the user data information to another network devices. The centralized SDN controller manages the control plane allowing the installation of application software in the northbound interface, facilitating communication between the installed application and SDN controller through an APIs where network devices can be controlled through application. SDN-WAN and SDN-access are the specific application of SDN that represent trends in networking.

NV (Network Virtualization)

The traditional model where a single network providing the specific services owns the entire physical infrastructure proved to be inefficient and expensive, particularly in managing physical servers. To overcome these challenges, Network Virtualization has emerged as a solution in the modern digital landscape. Network Virtualization enables the operation of multiple servers through virtualization within a single physical infrastructure. It achieves this by partitioning the physical resources and installing software as needed to deliver services. This approach improves resource utilization, simplifies network management, and accelerate the deployment of services.

Cloud Computing

Cloud computing revolutionizes the way of computing resources are accessed, delivered, and managed. In traditional computing environment, organizationally typically maintain and manage their own physical server. However, with the help of cloud computing services like data storage, servers, edge computing, and networking are possible through the internet provided by third parties vendor by exchanging services with money. It offers, scalability, flexibility, and cost efficiency because it offloads the burden of managing the storage in organization.

Edge computing

The widespread use of billions of IoT devices in our daily lives often need to retrieve data from the cloud which needed real-time processing. Instead of relying on cloud server for data retrieval, edge computing process data locally within edge devices. This allows processing and analysis data closer to the source of its generation rather than relying on centralized cloud server. This particularly beneficial for application that require quick decision making, such as autonomous vehicles, industrial automation etc.

Impact on three-tier architecture

Simplified and efficient on managing network devices: In a three-tier architecture, the centralized management of network devices through an application is simplified with the implementation of SDN. This approach provides a more efficient and centralized control over the network, allowing for easier configuration, monitoring, and optimization of network resources.

Effective Utilization of resource: Within the three-tier architecture, network virtualization enables the installation of different servers with distinct networks on a single physical infrastructure using type 1 hypervisor software. This approach ensures efficient utilization of all physical resources for hosting servers.

Less Costing and area required: In term of cost and area, it is more advantageous to leverage cloud computing for host the server instead of acquiring a physical infrastructure server within the three-tier architecture.

Decrease latency and improved performance speed: The integration of SDN and edge computing within the three-tier architecture optimizes data handling for IoT and other devices. This eliminates the necessity for these devices to retrieve data from the cloud, resulting in accelerated speed, reduced latency, and enhanced overall network performance.

Conclusion

This report offers a full description prepared by the network engineer of 'NetworkHats' regarding the planning and configuration of various network devices in a three-tier architecture with redundancy applied in both the headquarters and branches. In order to meet the specific requirements of the customer, many services and protocols such as NAT, VPN, SNMP, SYLOG, DNS, DHCP, STP, VLAN, and WLC were successfully employed. With prioritizing the access layer, a wide range of L2 security features such as BPDU Guard, Port Security, DHCP snooping, ARP inspection, and so on were enabled. Moreover, different emerging networking trends and their impact on three-tier architecture in today's digital realm were discussed.

Reference

2 - Tier and 3 - Tier architecture in networking - GeeksforGeeks. (2022, October 28). GeeksforGeeks. https://www.geeksforgeeks.org/2-tier-and-3-tier-architecture-in-networking/

How do you choose the best routing protocol for your network? (2023, May 2). LinkedIn. https://www.linkedin.com/advice/0/how-do-you-choose-best-routing-protocol-your-network

Daniel. (2022, December 27). OSPF default-information originate and the default route. Study CCNA. https://study-ccna.com/ospf-default-information-originate/

Just a moment... (n.d.). Cloudflare - The Web Performance & Security Company | Cloudflare. https://www.cloudflare.com/learning/network-layer/what-is-sdn/

What is network virtualization? (n.d.). Red Hat - We make open source technologies for the enterprise. https://www.redhat.com/en/topics/virtualization/what-is-network-virtualization

Davis, L. (2022, October 19). What is cloud computing? The ultimate guide. Forbes Advisor. https://www.forbes.com/advisor/business/what-is-cloud-computing/

Just a moment... (n.d.). Connect & protect with the connectivity cloud | Cloudflare. https://www.cloudflare.com/learning/serverless/glossary/what-is-edge-computing/