in collaboration with

Softwarica College of IT & E-commerce | Coventry University

Submitted to:
Manoj Tamang

Submitted by:
Nihangchha Rai

NETWORKING

Nihangchha Rai

BSc. (Hons.) Ethical hacking, Softwarica Collage of IT and E-commerce, Coventry University

ST5064CEM NETWORKING COURSE WORK 1

Mr. Manoj Tamang

Intake

March 2022

Feb 2nd, 2024

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 OSPF, RIP, EIGRP, STATIC, and BGP routing protocol. These protocols are implemented in a three-tier architecture and their features are explained. The project covers the Access Layer, including HSRP for load balancing and redundancy, STP, Portfast, VLAN segregation, and EtherChannel. It provides a thorough explanation of L2 security features such BPDU Guard, Port Security, DHCP Snooping, Rate Limiting, Dynamic ARP Inspection. The project cover NAT, PAT, and VPN technologies, such as IPsec and GRE over IPsec, with a thorough explanation of their verification processes for secure communication. Along with this Firewalls, NTP servers, Syslog servers, SNMP, AAA, 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 to Software Defined Networking (SDN), Network Virtualization (NV), Cloud Computing, and Edge Computing.

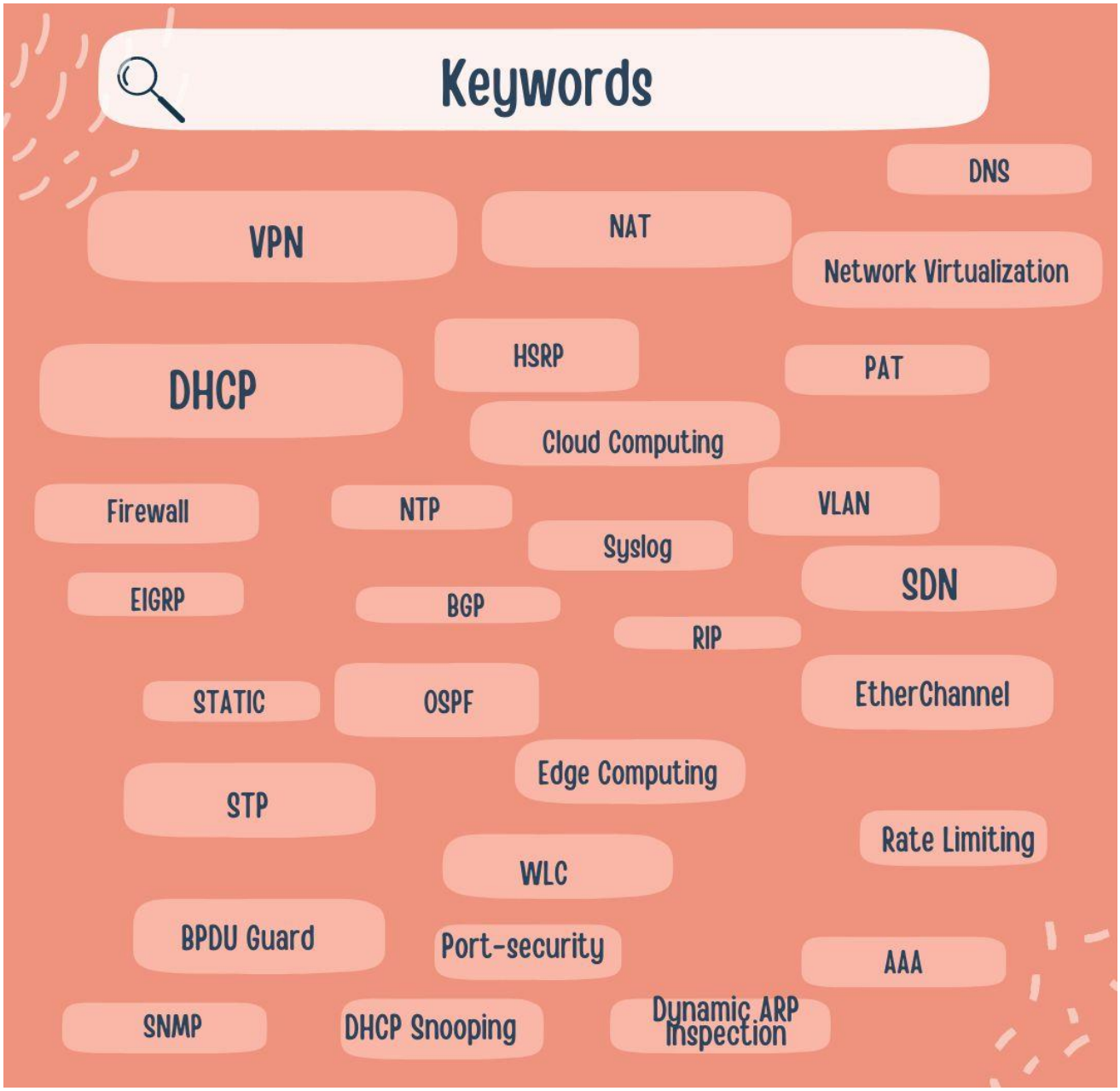

Keywords
DNS
VPN
NAT
Network Virtualization
HSRP
PAT
DHCP
Cloud Computing
Firewall
NTP
VLAN
Syslog
SDN
EIGRP
BGP
RIP
STATIC
OSPF
EtherChannel
Edge Computing
STP
Rate Limiting
WLC
BPDU Guard
Port-security
AAA
SNMP
DHCP Snooping
Dynamic ARP Inspection

Table of Contents

List of Tables

Table of Figure

Introduction

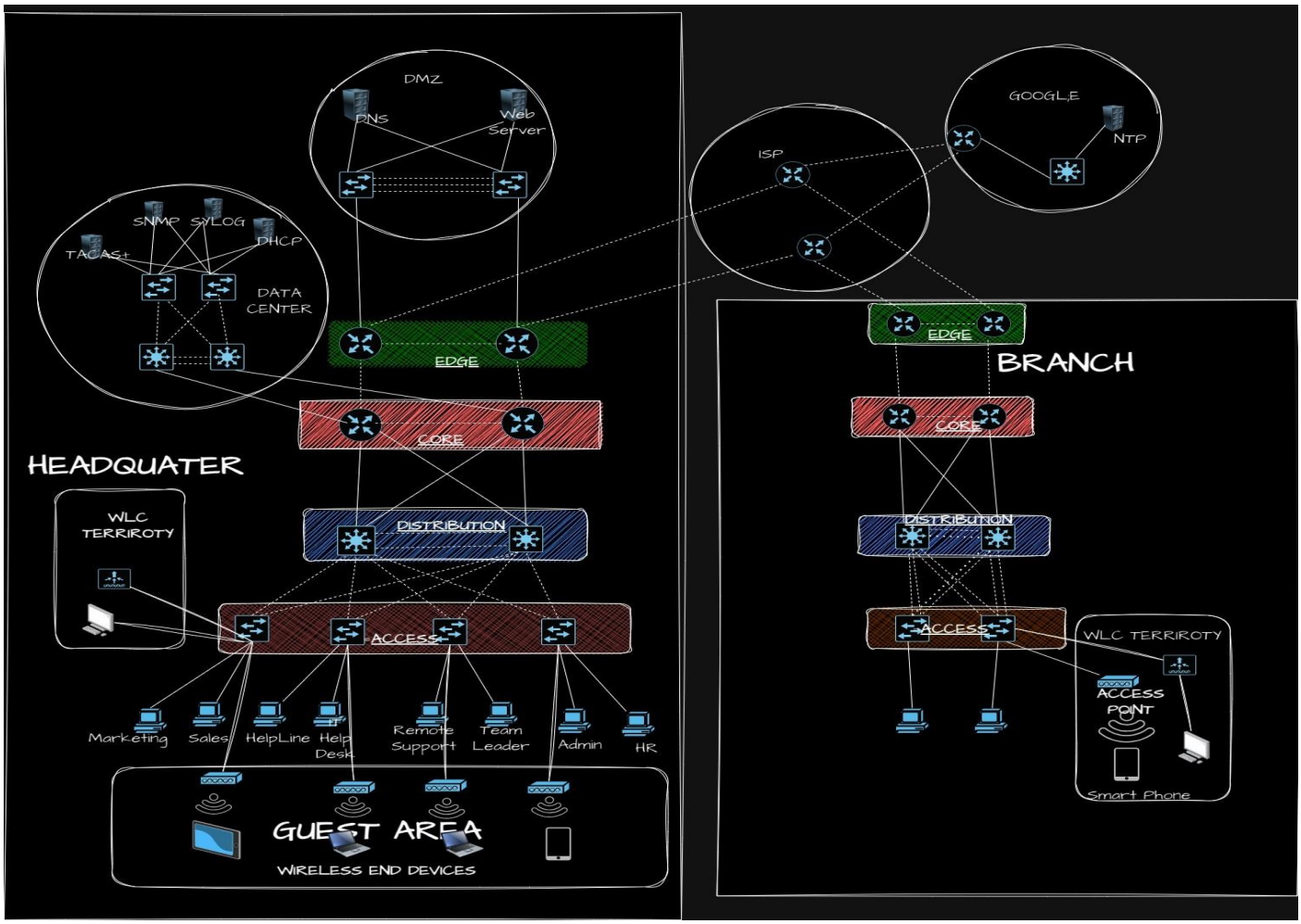
As a network engineer of 'NetworkHats' company, I have designed a network topology in traditional three-tier architecture and configure in Cisco Packet Tracer and GNS3 with proper indexing that aligns the specific requirement of our client. It consists of access layer, distribution layer, core layer, and additionally added an edge layer. In this network topology different features and components like NTP, SNMP, NAT, VPN, SYSLOG, DHCP and including L2 security feature like DHCP snooping, port security, BPDU guard and more are implemented in this project for increasing the effectiveness and efficiency of our client network.

PART A

Designs

Logical Prototype

Figure 1:Logical Network prototype designed on draw.io

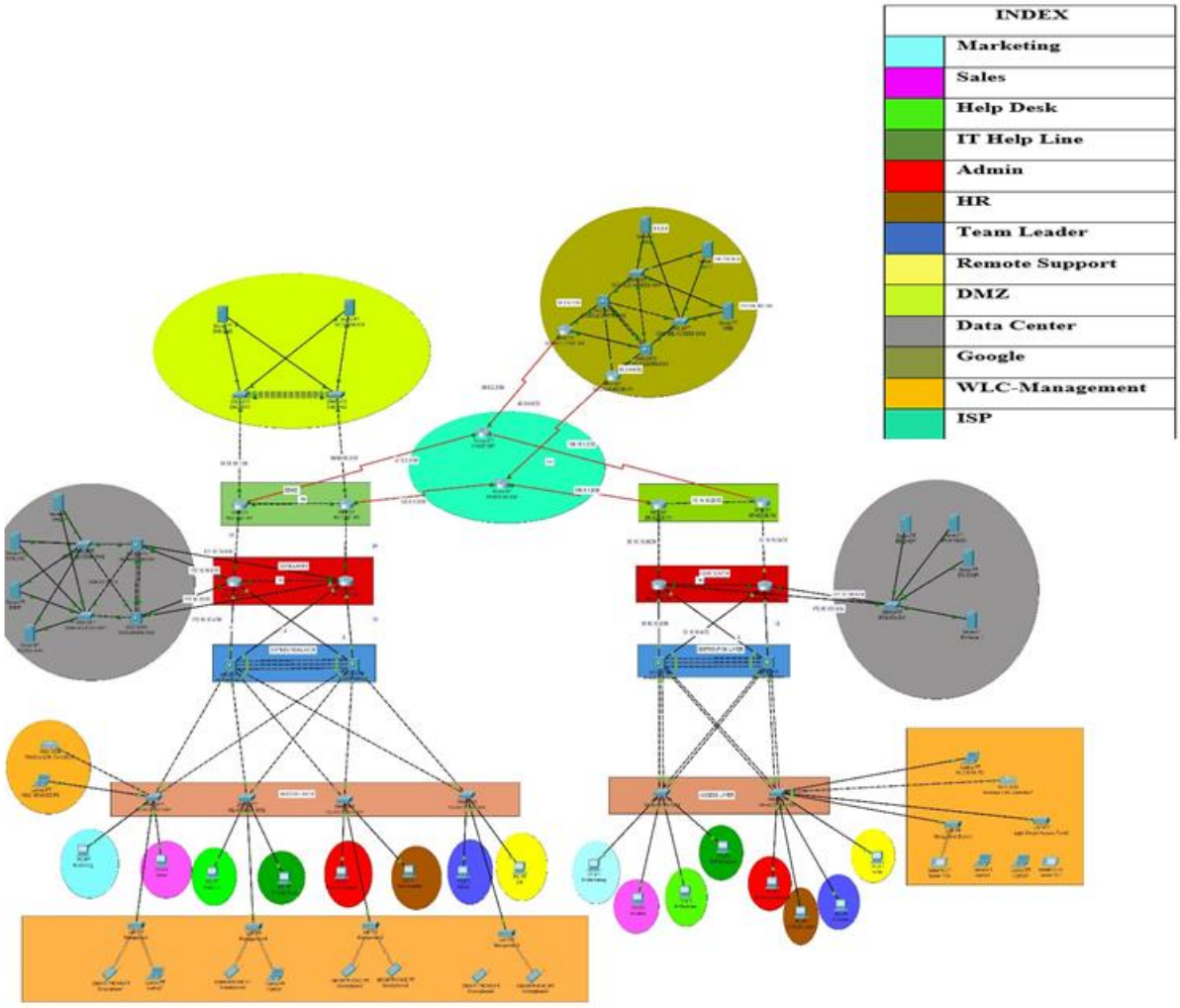


As shown in above figure, it consists of three tier architecture design implemented on headquarters and branch of company. By implementing the redundancy protocol on both sides.

Physical Prototype

Figure2

Figure 2:Physical Prototype of three-tier architecture with different LANs and WAN



ROUTING PROTOCOL

Various types of routing protocols such as, OSPF, static, BGP are implemented in this network topology based on the specific situation.

Factor consider while selecting routing protocol

Factor should be considered while choosing a routing protocol between three-tier architecture are as follows:

a. 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.

b. 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.

c. 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.

d. 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.

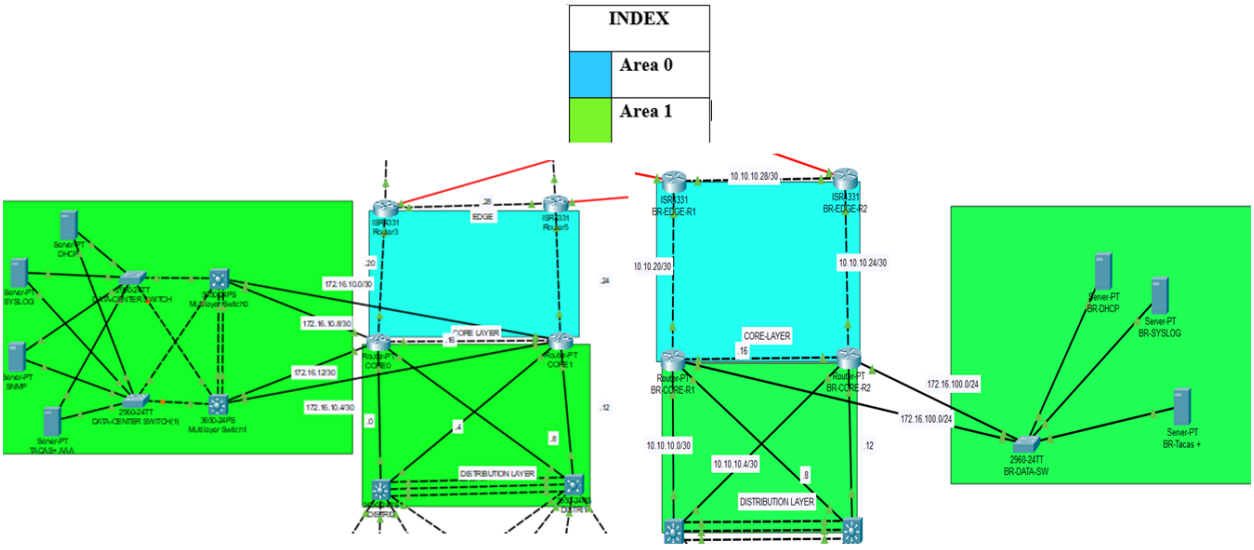
e. Running protocol configuration and troubleshoot

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

Figure

Figure 3:OSPF area sub-diving in headquarter and Branch



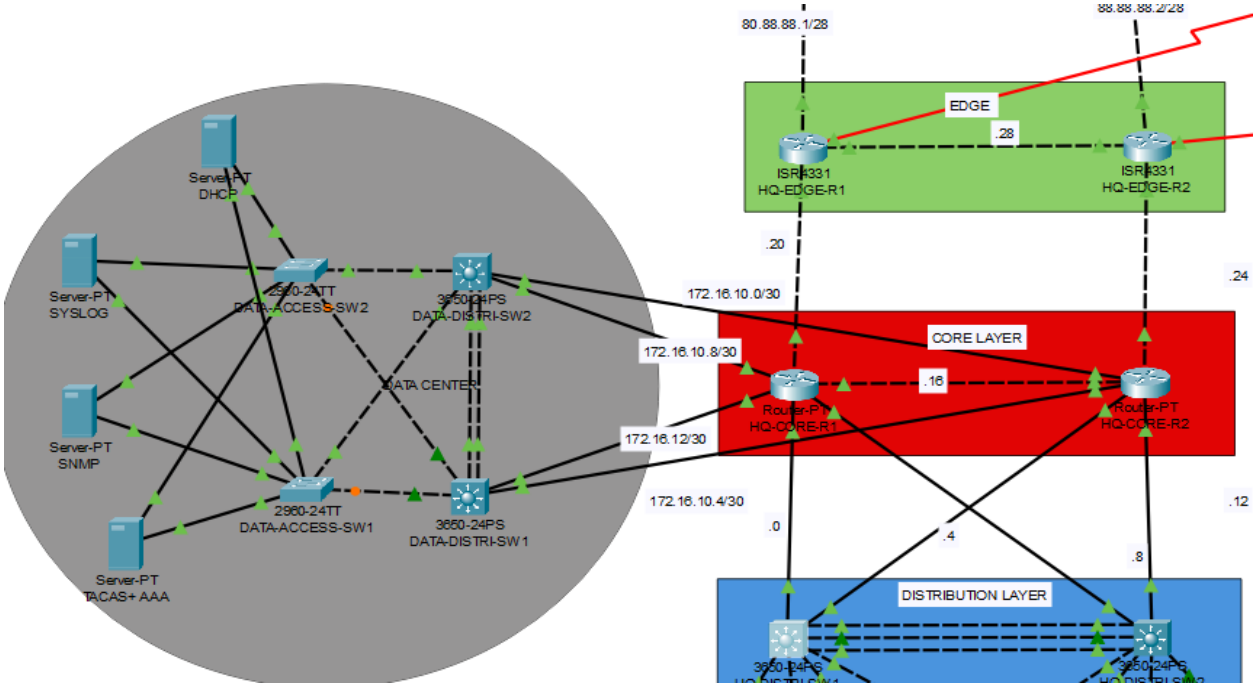
branch

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.

Figure 4:hq ospf

HEADQUARTER



HQ-DISTRI-SW1

Figure 5:Running configuration of OSPF in AS of HQ-DISTRI-SW1

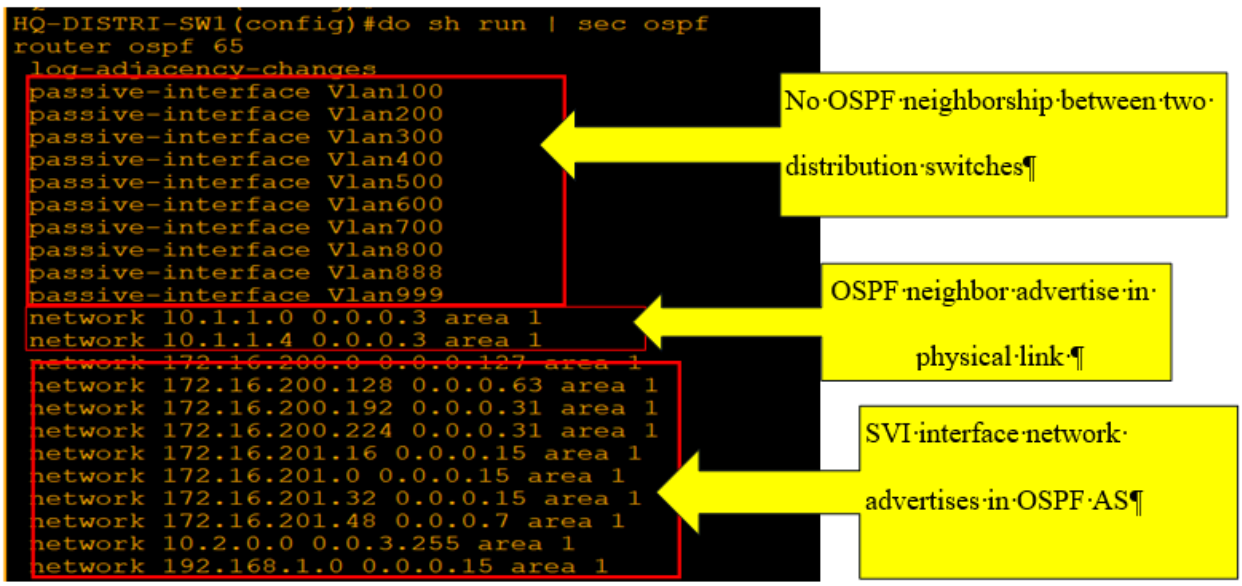


Figure 6: OSPF neighborship of HQ-DISTRI-SW1

```
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-SW2

Figure 7-Running-config of HQ-DISTRI-SW2 section OSPF

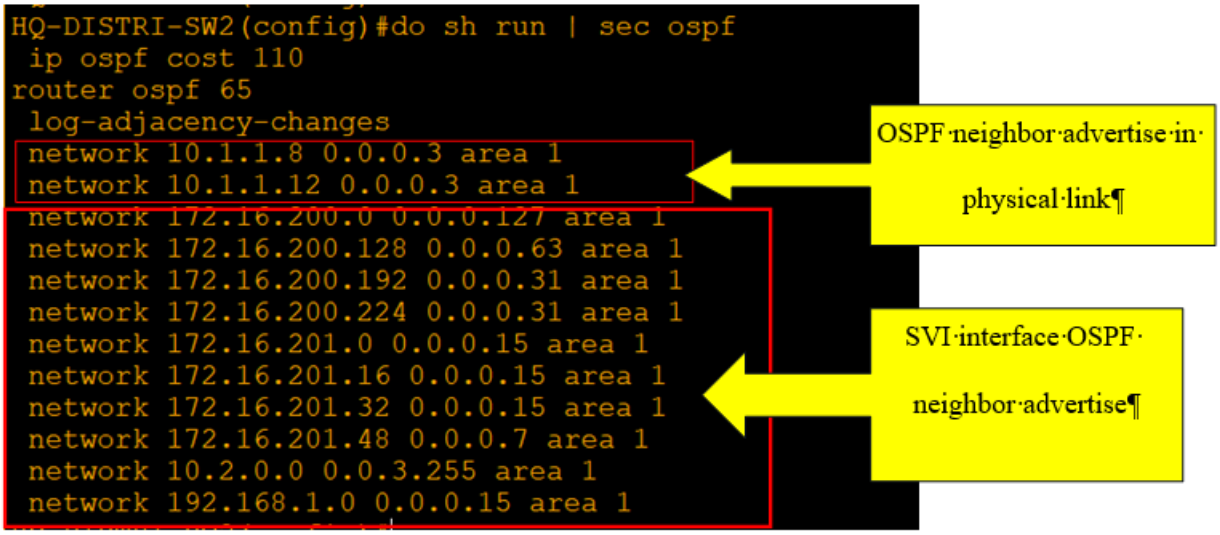


Figure 8-OSPF neighborship of HQ-DISTRI-SW2

```
HQ-DISTRI-SW2(config)#do sh ip ospf neigh

Neighbor ID     Pri   State           Dead Time   Address         Interface
172.16.10.14      1   FULL/BDR        00:00:37    10.1.1.10       GigabitEthernet1/0/6
172.16.10.6       1   FULL/BDR        00:00:37    10.1.1.14       GigabitEthernet1/0/15
```

HQ-CORE-R1

Figure 9-Running config of OSPF configuration of HQ-CORE-R1

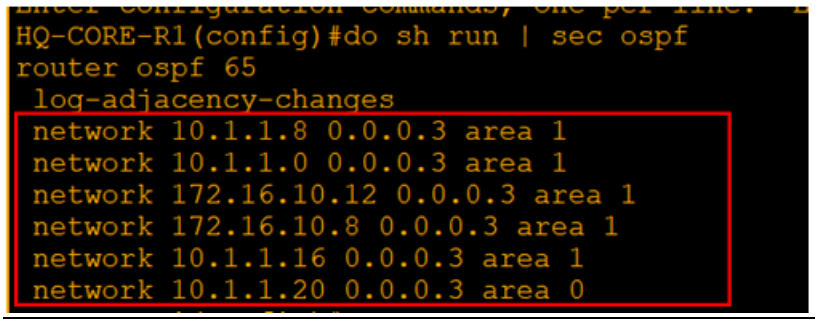
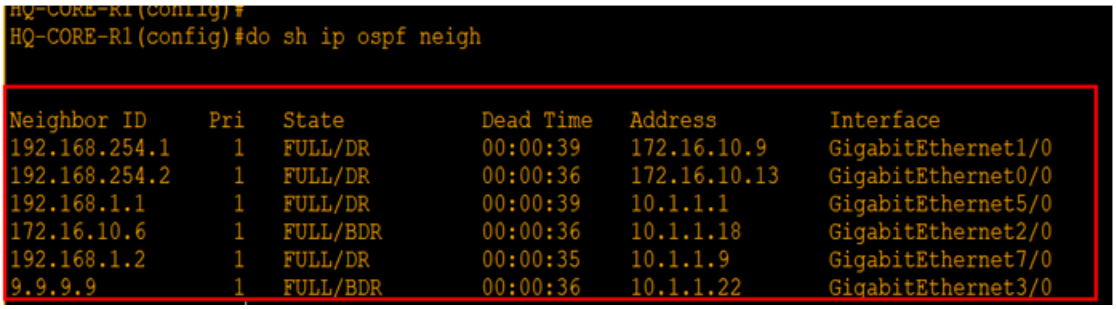


Figure 10-OSPF neighborship of HQ-CORE-R1



HQ-CORE-R2

Figure 11-Running-config of OSPF config on HQ-CORE-R2

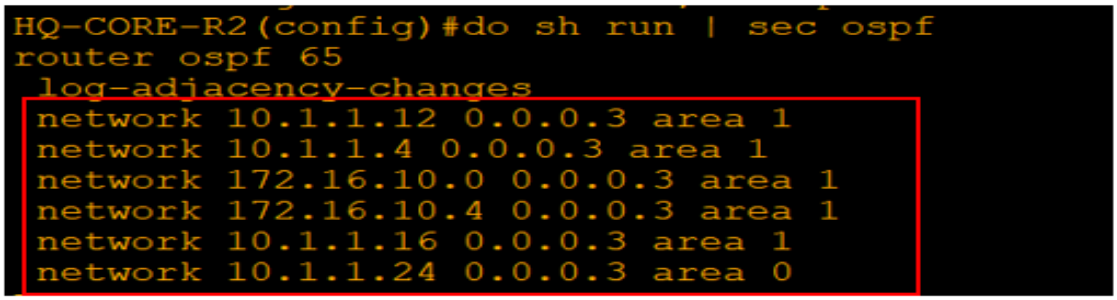
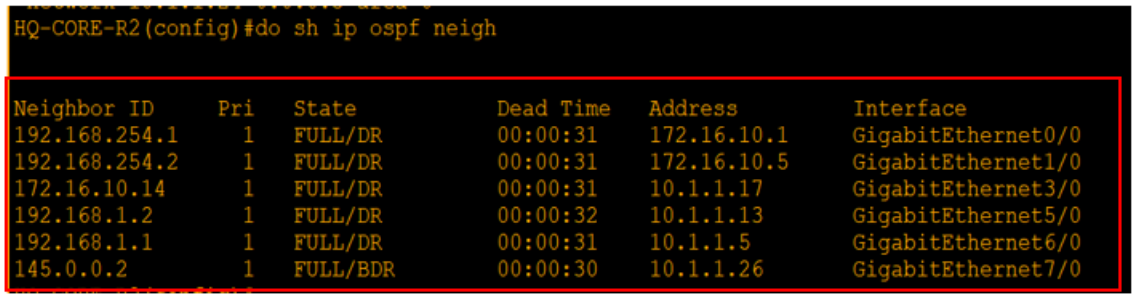


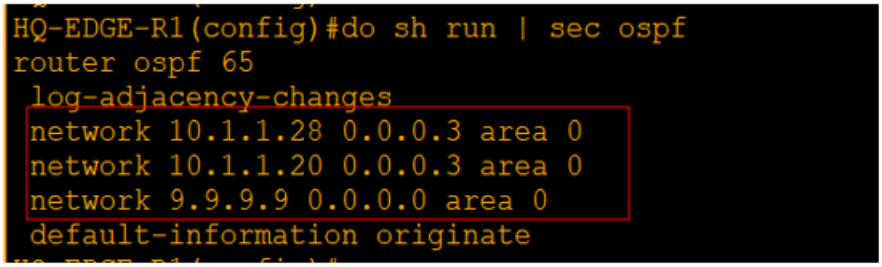
Figure 12-OSPF neighborship of HQ-CORE-R2



```
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
```

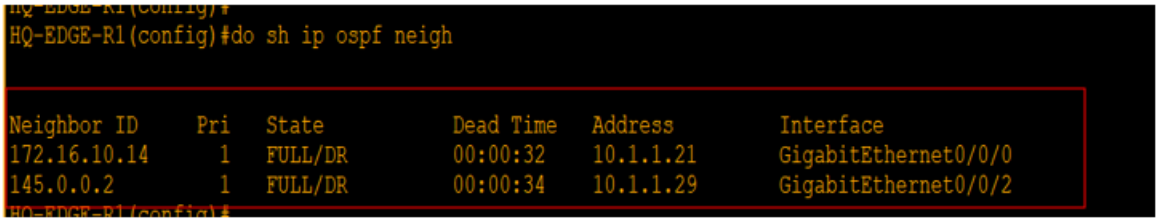
HQ-EDGE-R1

Figure 13-OSPF config in 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 neighborship of 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
```

HQ-EDGE-R2

Figure 15-OSPF configuration in HQ-EDGE-R2

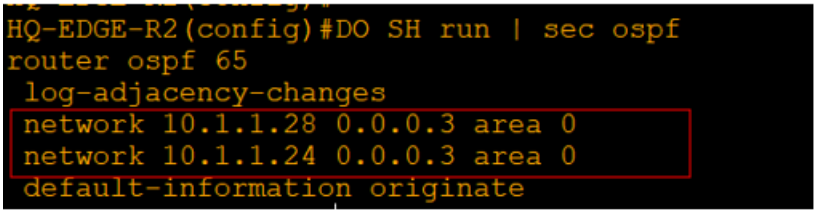
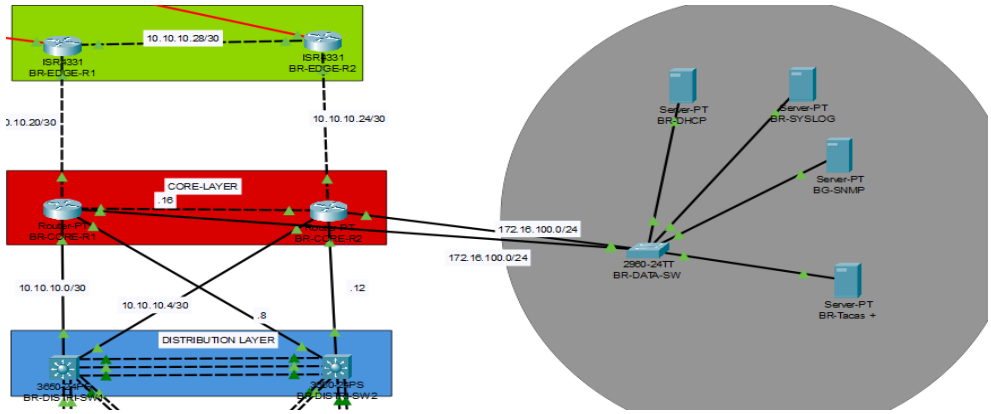


Figure 16-OSPF neighborship of HQ-EDGE-R2

BRANCH

Figure 17-branch ospf



BR-DISTRI-SW1

Figure 18-OSPF config in BR-DISTRI-SW1

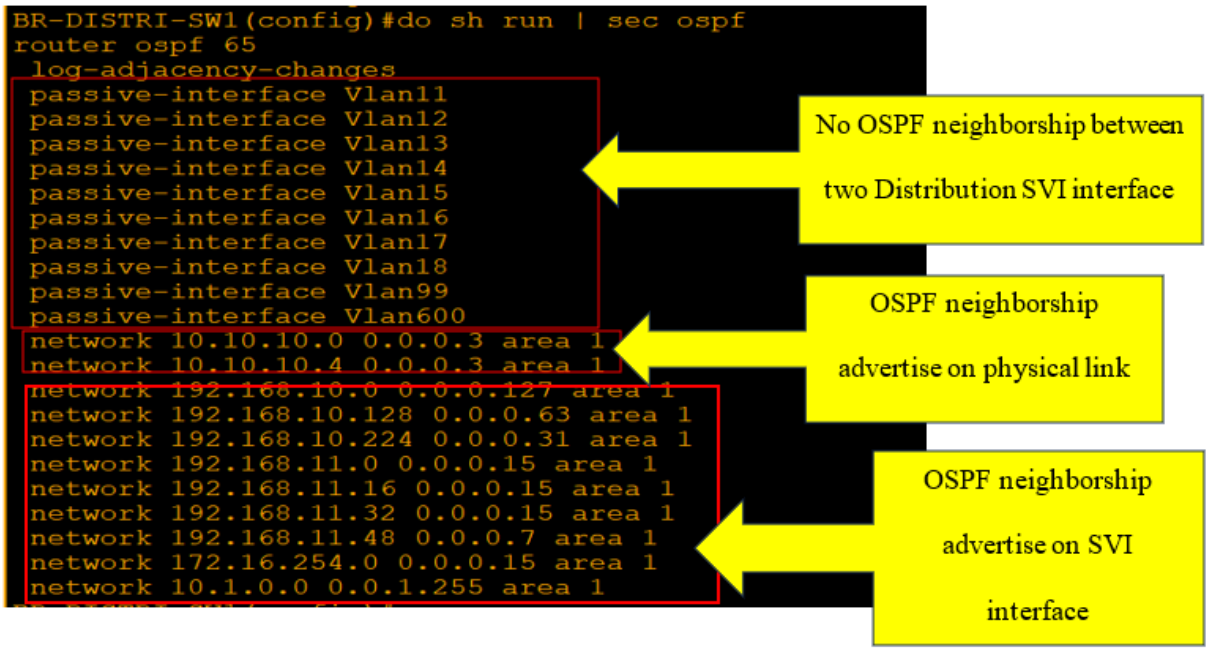


Figure 19-OSPF neighborship of BR-DISTRI-SW1

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

Neighbor ID     Pri   State           Dead Time   Address         Interface
172.16.100.2      1   FULL/BDR        00:00:33    10.10.10.6      GigabitEthernet1/0/9
172.16.100.1      1   FULL/BDR        00:00:31    10.10.10.2      GigabitEthernet1/0/8
```

BR-DISTRI-SW2

Figure 20-OSPF configuration in BR-DISTRI-SW2

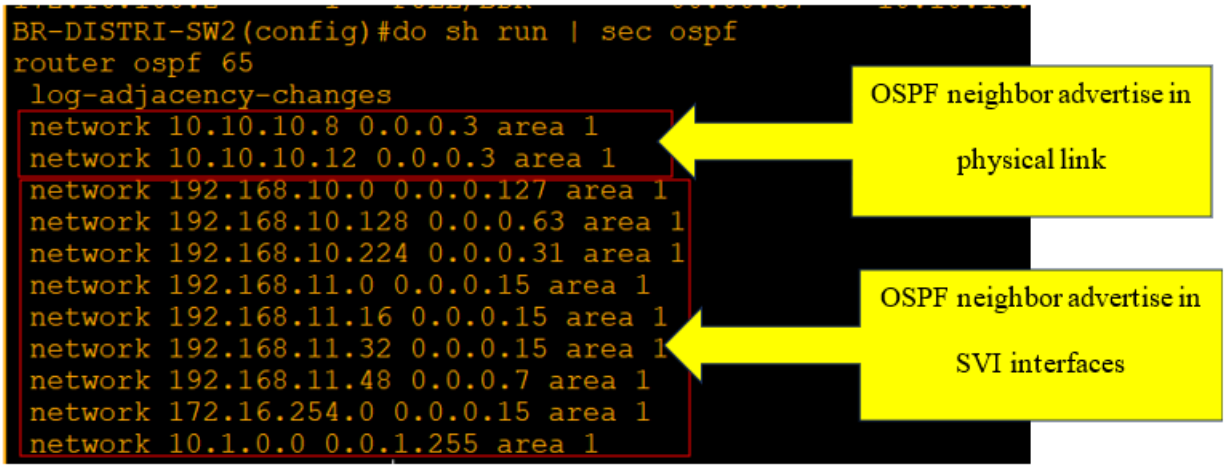


Figure 21-OSPF neighborship of BR-DISTRI-SW2

```
BR-DISTRI-SW2(config)#do sh ip ospf neigh

Neighbor ID     Pri   State           Dead Time   Address         Interface
172.16.100.1      1   FULL/BDR        00:00:37    10.10.10.10     GigabitEthernet1/0/9
172.16.100.2      1   FULL/BDR        00:00:37    10.10.10.14     GigabitEthernet1/0/8
```

BR-CORE-R1

Figure 22-OSPF config in BR-CORE-R1

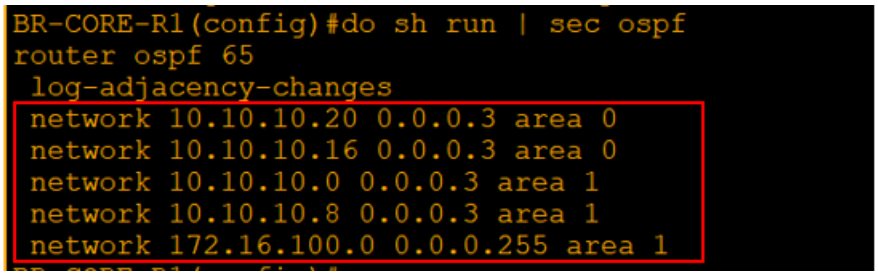
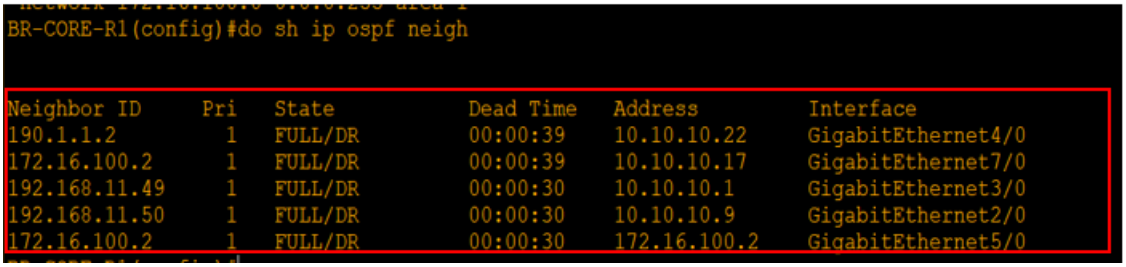


Figure 23-OSPF neighbor in BR-CORE-R1



BR-CORE-R2

Figure 24-OSPF config in BR-CORE-R2

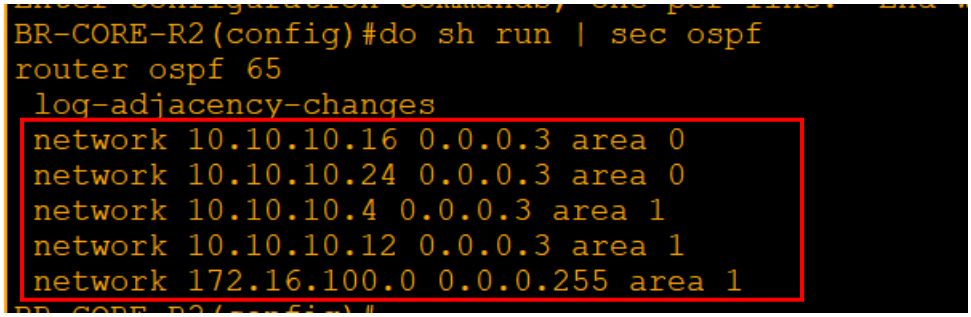
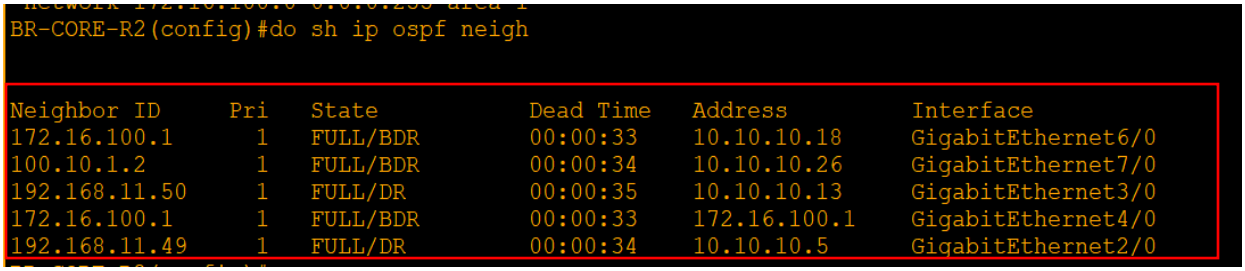


Figure 25OSPF neighborship of BR-CORE-R2



BR-EDGE-R1

Figure 26-OSPF config in HQ-EDGE-R1

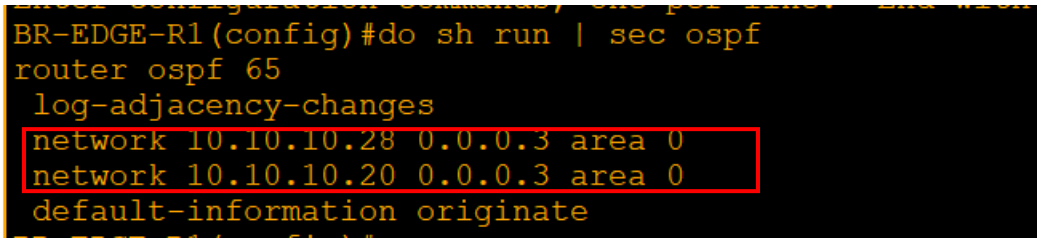
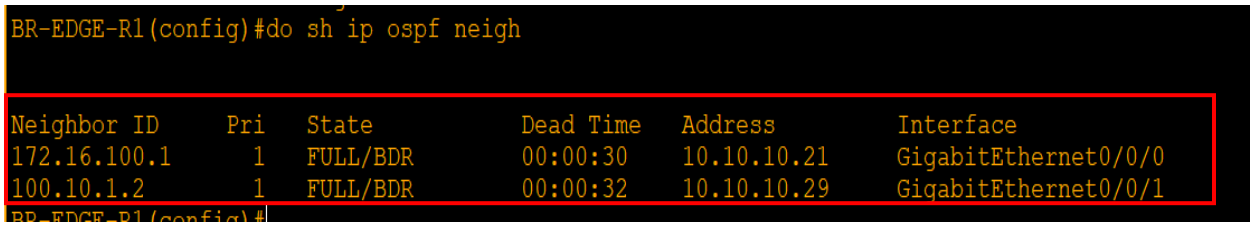


Figure 27-OSPF neighborship of BR-EDGE-R1



BR-EDGE-R2

Figure 28OSPF configuration in BR-EDGE-R2

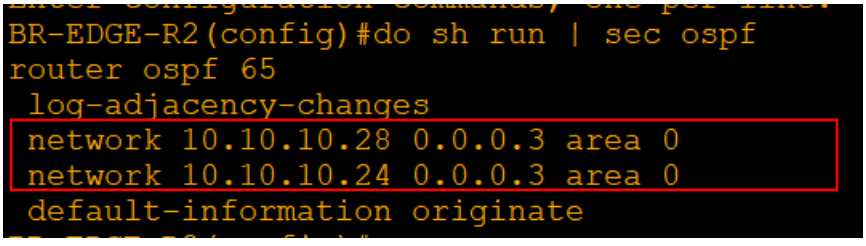
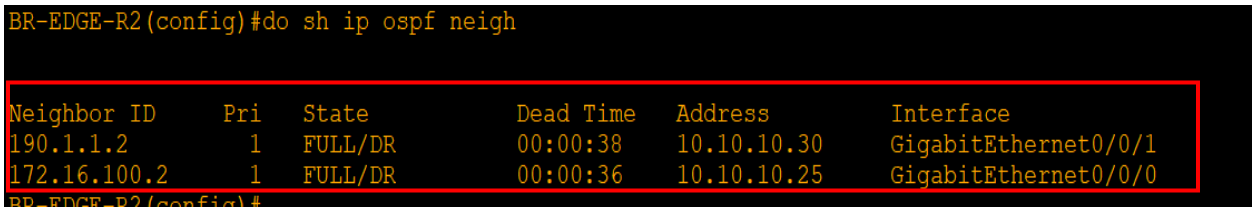


Figure 29OSPF neighborship of BR-EDGE-R2



Feature of OSPF in three tier architectures

OSPF cover the following feature in three tier architecture:

a. Dynamically Routing

   OSPF 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.

b. Efficient Routing

   Efficient Routing: OSPF 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.

c. High Availability

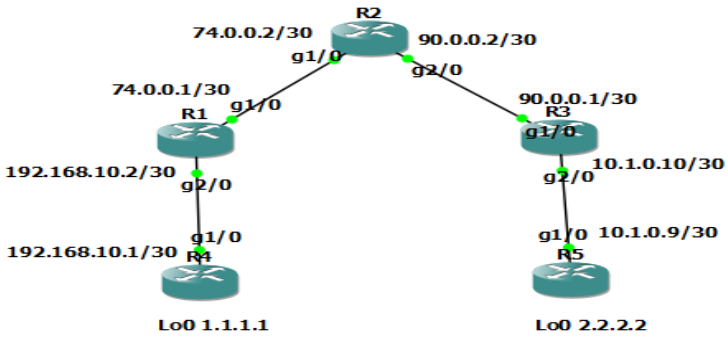
   OSPF allows for the setting up of several routes to the same destination. In a three-tier architecture, this can help to increase availability and fault tolerance. If one way becomes unavailable due to a network fault, OSPF can immediately divert traffic to another path.

d. Scalability

   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.

RIP

Figure 30-Simple physical network topology in GNS3



In RIP 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.

Figure 31-Rip configuring in R4

```
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 32-Configuration of RIP in R1

```
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 33-Configuration of RIP in R2

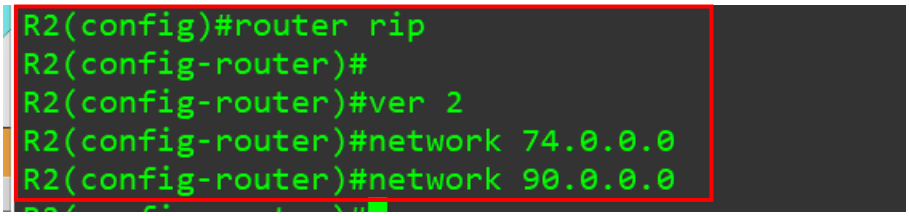


Figure 34-Rip configuration in R3

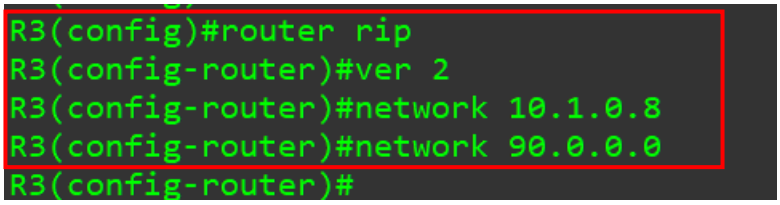


Figure 35-Rip configuration in R5

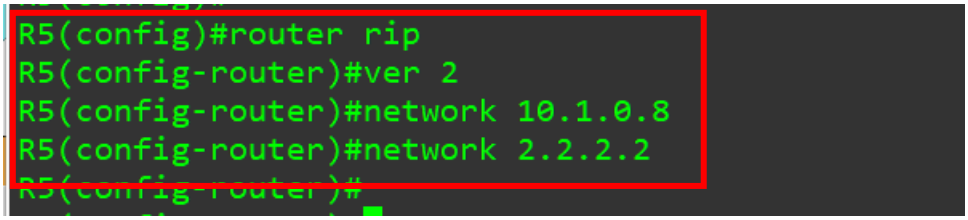


Figure 36-RIP database of R4

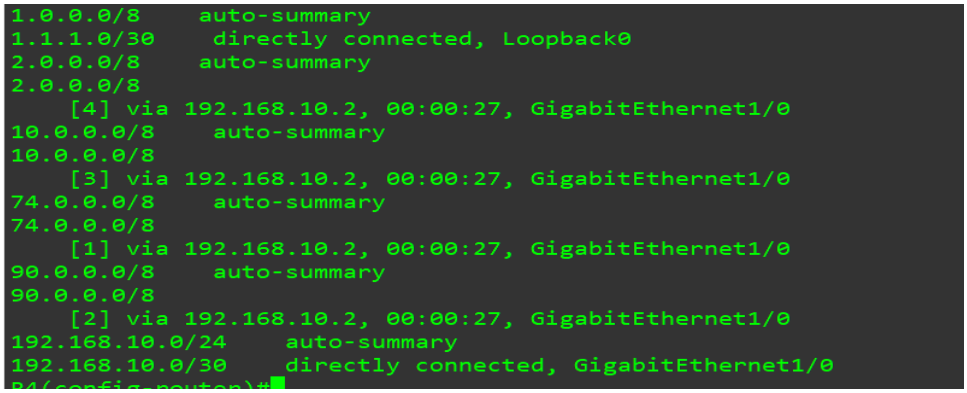
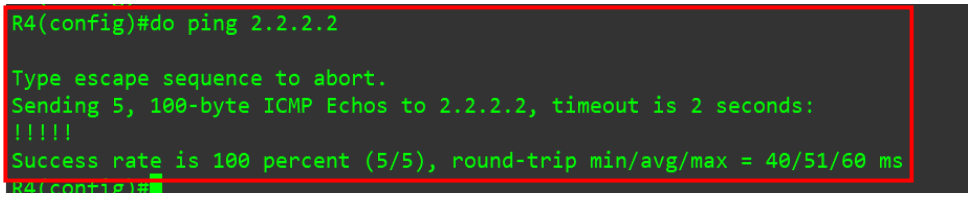


Figure 37-Verifying by pinging R5



EIGRP

Benefits

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

For static routing we need to specify the indirect network, subnet mask, and next hop or exit interfaces.

Ip route {indirect-network} {subnet-mask} {next-hop-IP-address || exit interface}

Configuring and designing static route in above Figure

Figure 38-Static configuration in R4

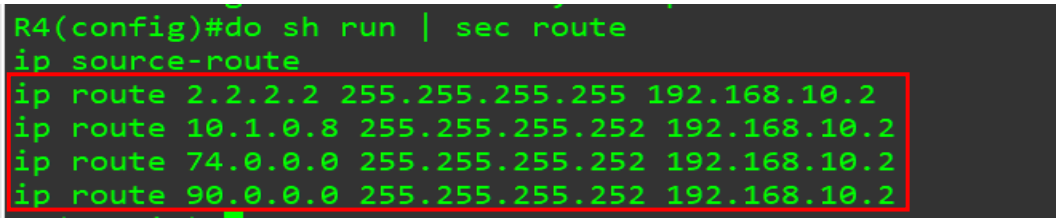


Figure 39-Static configuration in R1

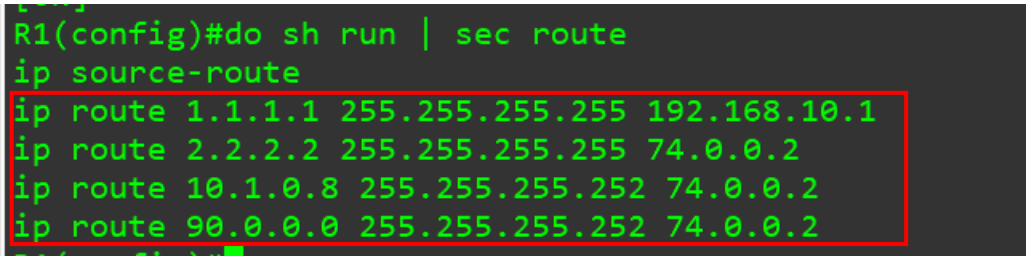


Figure 40-Static configuration in R2

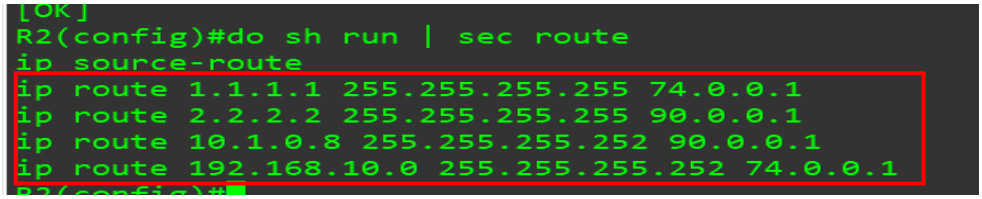


Figure 41-Static configuration in R3

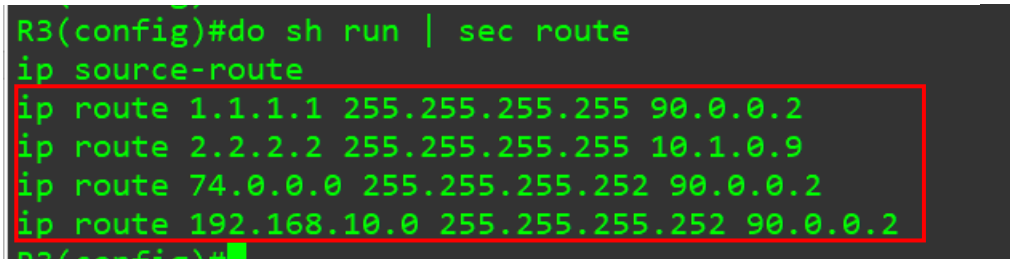


Figure 42-Static configuration in R5

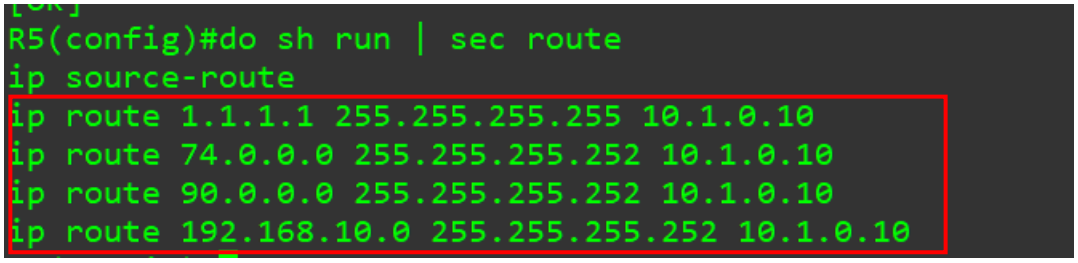


Figure 43-Ping to R5

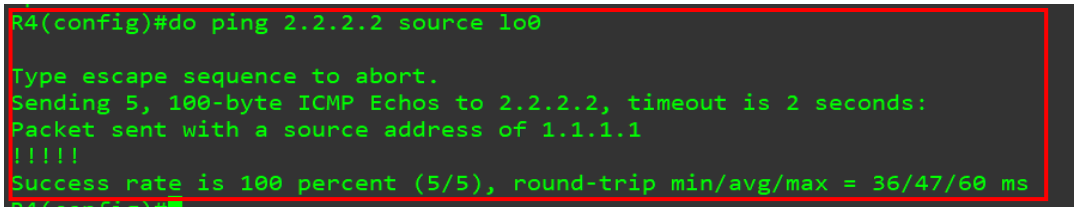
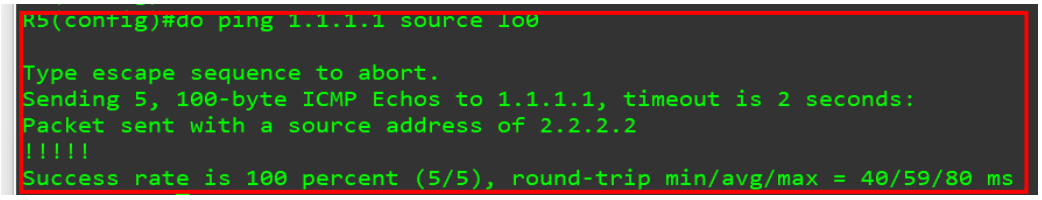


Figure 44-Ping to R4



From the above figures, 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.

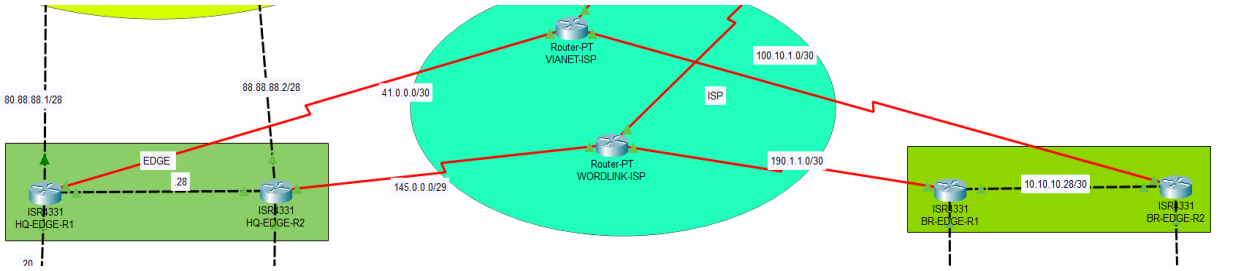
The main purpose of Static routing to create a direct route to the destination unlike dynamic routing need to share the route to each other. As a result, reduces the overhead by using the less CPU and memory usage and limit the exposure of routing information.

Default router 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 45-Edge router connection with ISP



HEADQUARTER

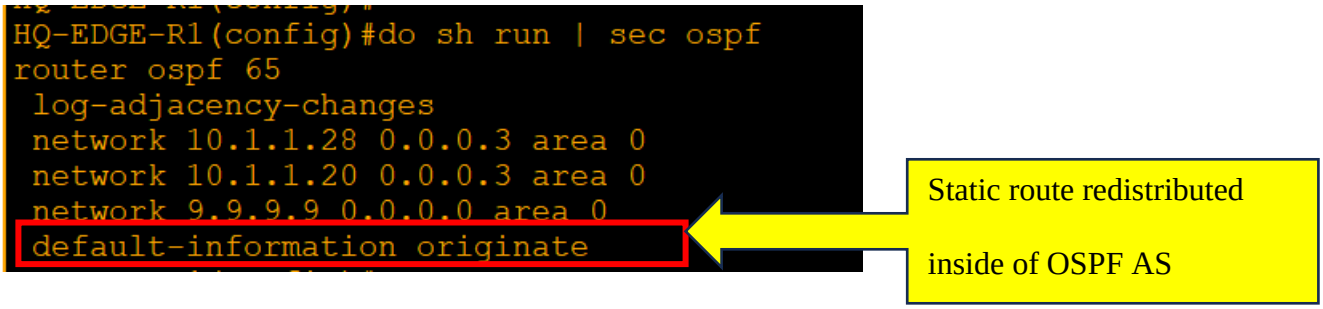
HQ-EDGE-R1

Figure 46-Default static route in HQ-EDGE-R1 to VIANET-ISP

```
HQ-EDGE-R1(config)#
HQ-EDGE-R1(config)#ip route 0.0.0.0 0.0.0.0 41.0.0.1
HQ-EDGE-R1(config)#
```

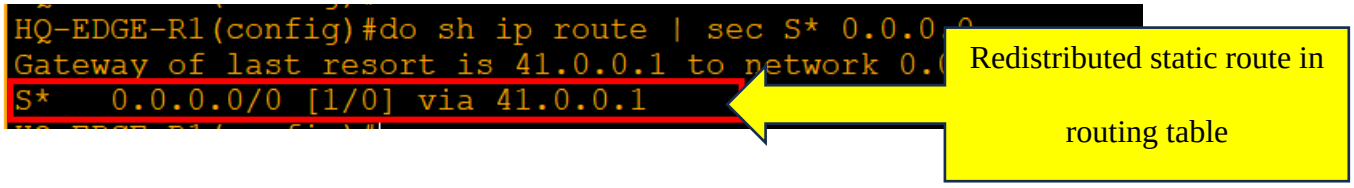
Default-static route is configured on HQ-EDGE-R1 on global configuration mode with the next hop ISP IP i.e. 41.0.0.1.

Figure 47-Running config OSPF of HQ-EDGE-R1



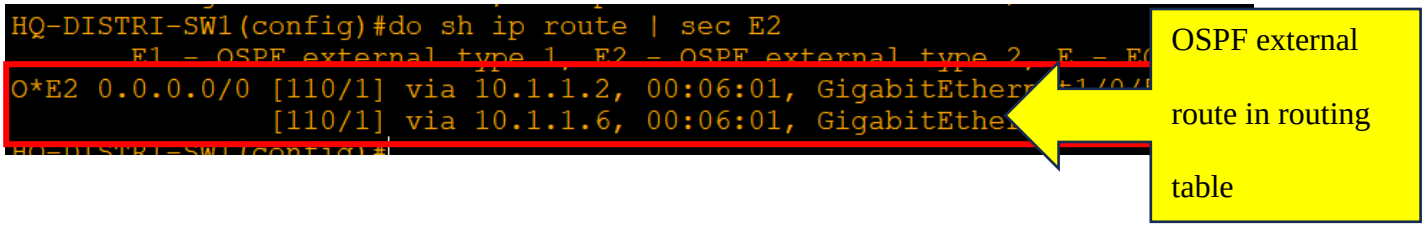
Static route configured in above figure which I have already redistributed in OSPF.

Figure 48-Routing table of HQ-EDGE-R1



The redistributed static route in OSPF appeared in routing table of HQ-EDGE-R1.

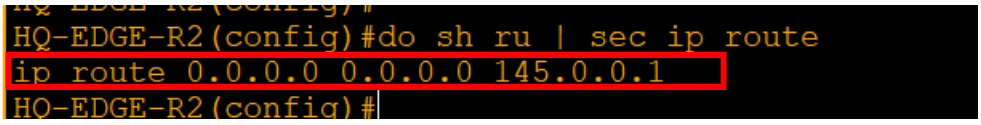
Figure 49-Routing table of HQ-DISTRI-SW1



Redistributed route in edger router added as a OSPF external type route in routing table of all L3 devices of Headquarter

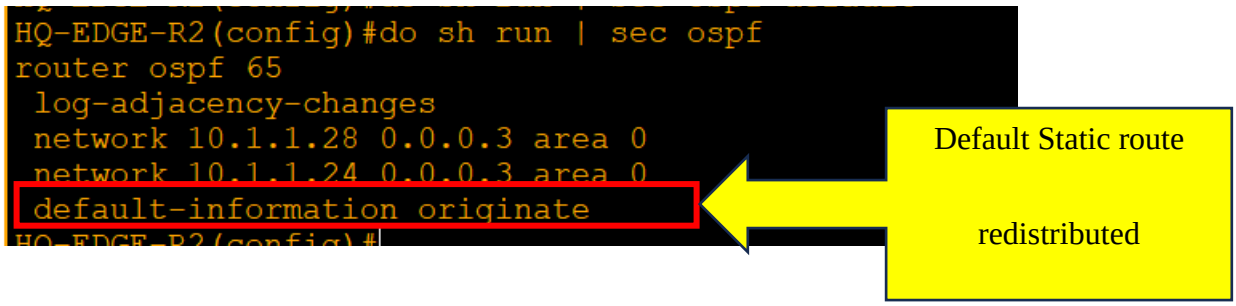
HQ-EDGE-R2

Figure 50-Running config of static route in HQ-EDGE-R2



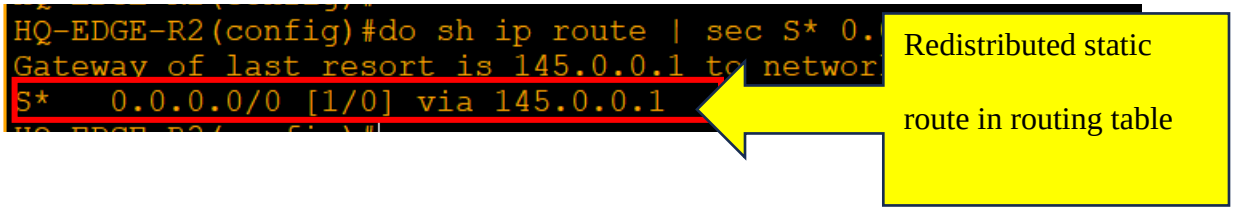
Default static route is configured with the next hop IP address of wordlink i.e 145.0.0.1.

Figure 51-Running-config filtering out OSPF of HQ-EDGE-R2



In OSPF AS static route configure in figure {} is redistributed as show in above figure {}.

Figure 52-Routing table of HQ-EDGE-R2 filtering out static route



Static route appeared in routing table of HQ-EDGE-R2

Figure 53Routing table of DISTRI-SW2

```
Enter configuration commands, one per line.  End with CNTL/Z.
HQ-DISTRI-SW2(config)#
HQ-DISTRI-SW2(config)#do sh ip route | sec E2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
O*E2  0.0.0.0/0 [110/1] via 10.1.1.10, 00:11:26, GigabitEthernet1/0/6
```

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 NATTING.

BRANCH

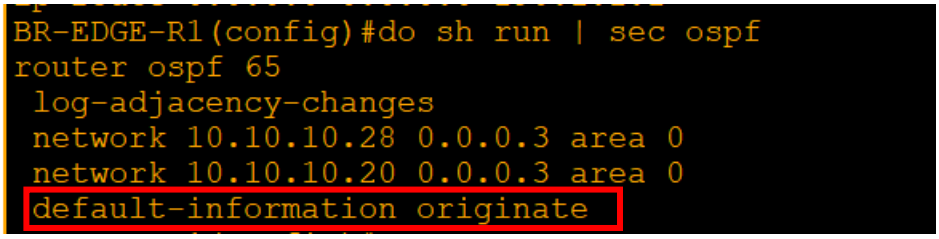
Similarly, with the same process as above the default router is configured in branch edge router.

Figure 54Running config of BR-EDGE-R1 filtering out static route

```
BR-EDGE-R1(config)#
BR-EDGE-R1(config)#do sh run | sec ip route
ip route 0.0.0.0 0.0.0.0 190.1.1.1
```

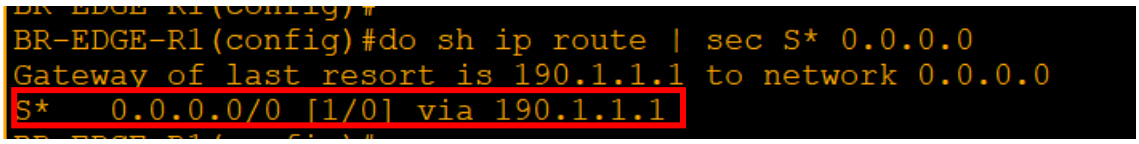
The default static route is configured in BR-EDGE-R1 with the next hop IP address of ‘wordlink’ ISP i.e., 190.1.1.1.

Figure 55Running config of OSPF



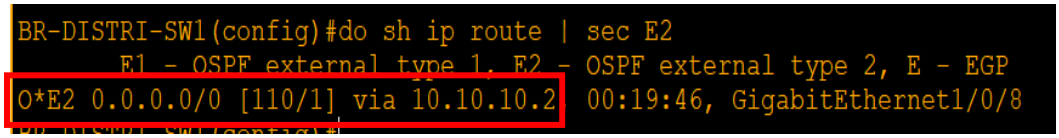
The default static route configured in above figure and redistributed in OSPF.

Figure 56-Routing table of BR-EDGE-R1 filtering out static route



The static route configured appeared in routing table of BR-EDGE-R1

Figure 57-Routing table of BR-DISTRI-SW1



The redistributed static route in the above figure appeared in routing table of all L3 devices in branch as E2 i.e., OSPF external type route.

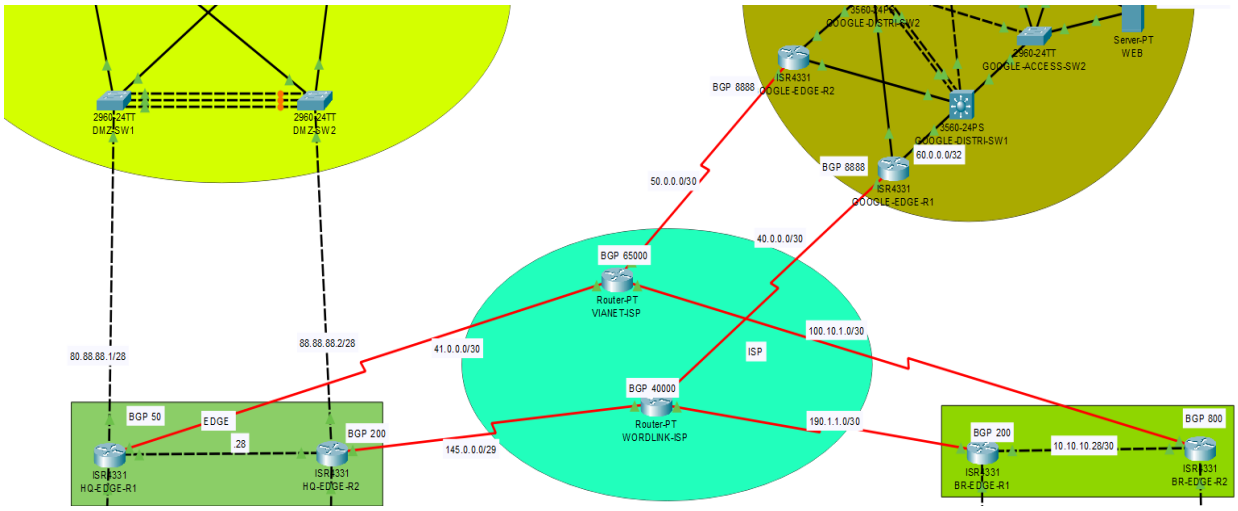
Now, the end devices of branch can access the internet with the help of NAT.

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 58BGP through ISP and GOOGLE



HEADQUARTER

HQ-EDGE-R1

Figure 59-Configuration of BGP in HQ-EDGE-R1

```
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 60-Network using BGP protocol

```
HQ-EDGE-R1(config)#do sh ip bgp
BGP table version is 13, local router ID is 9.9.9.9
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       41.0.0.1                 0      0      0 65000 8888 90 i
*> 10.0.0.0/30      41.0.0.1                 0      0      0 65000 8888 i
*> 41.0.0.0/30      0.0.0.0                  0      0  32768 i
*                   41.0.0.1                 0      0      0 65000 i
*> 44.0.0.0/30      41.0.0.1                 0      0      0 65000 8888 60 i
*> 50.0.0.0/30      41.0.0.1                 0      0      0 65000 i
*> 60.0.0.0/30      41.0.0.1                 0      0      0 65000 8888 90 i
*> 74.0.0.0/30      41.0.0.1                 0      0      0 65000 8888 i
*> 80.88.88.0/28    0.0.0.0                  0      0  32768 i
*> 100.10.1.0/30    41.0.0.1                 0      0      0 65000 i
*> 142.250.183.0/24 41.0.0.1                 0      0      0 65000 8888 90 i
*> 216.239.35.0/24  41.0.0.1                 0      0      0 65000 8888 90 i
```

Figure 61-BGP configuration in HQ-EDGE-R2

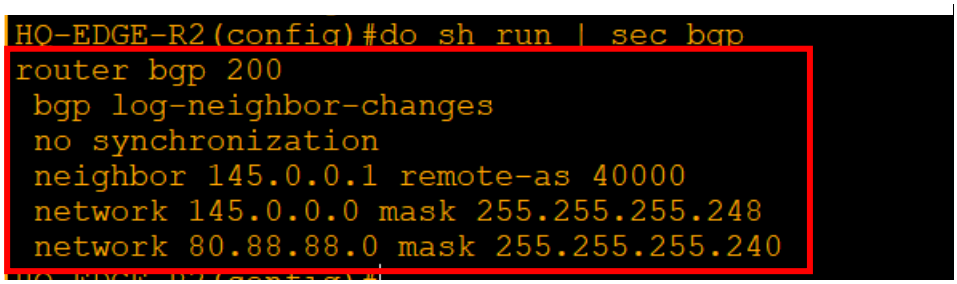
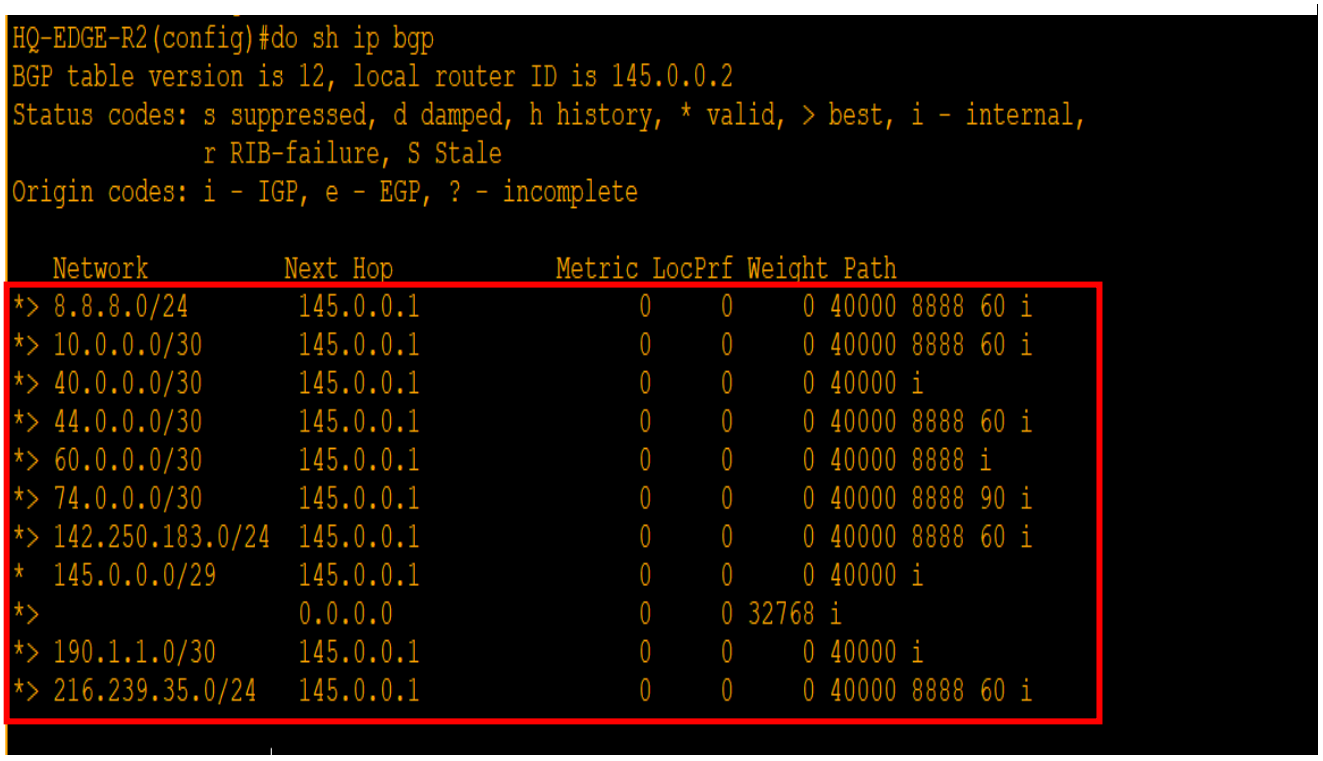


Figure 62-Network using BGP protocol



BRANCH

BR-EDGE-R1

Figure 63-BGP configuration in BR-EDGE-R1

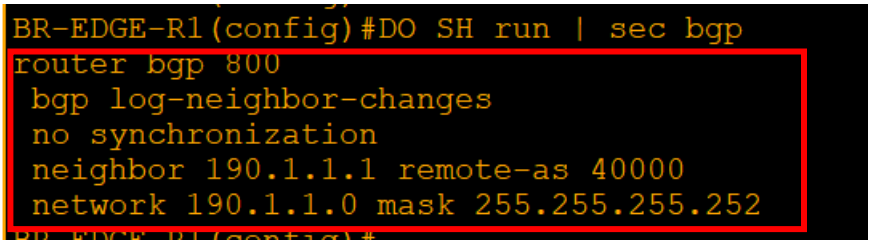
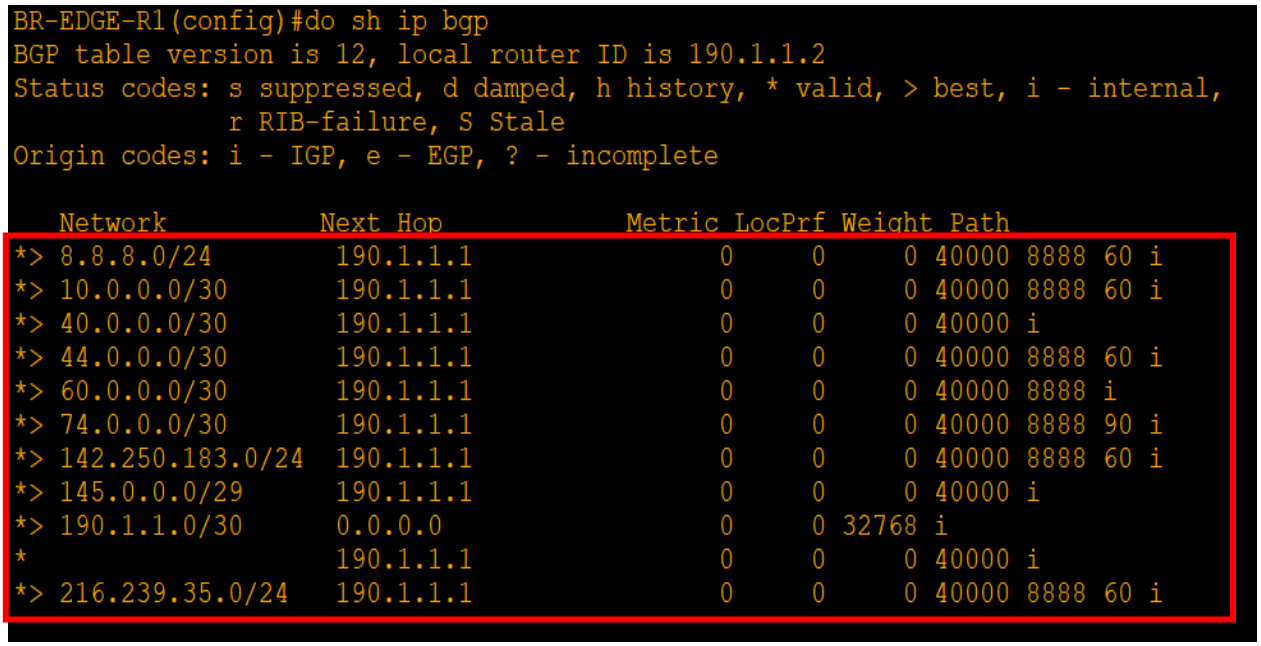


Figure 64-Networks using BGP as a routing protocol



BR-EDGE-R2

Figure 65-BGP configuration in BR-EDGE-R2

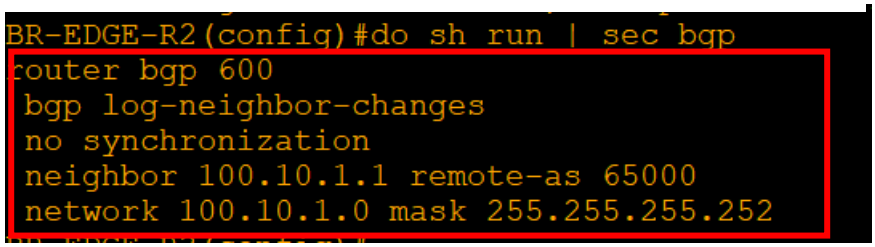
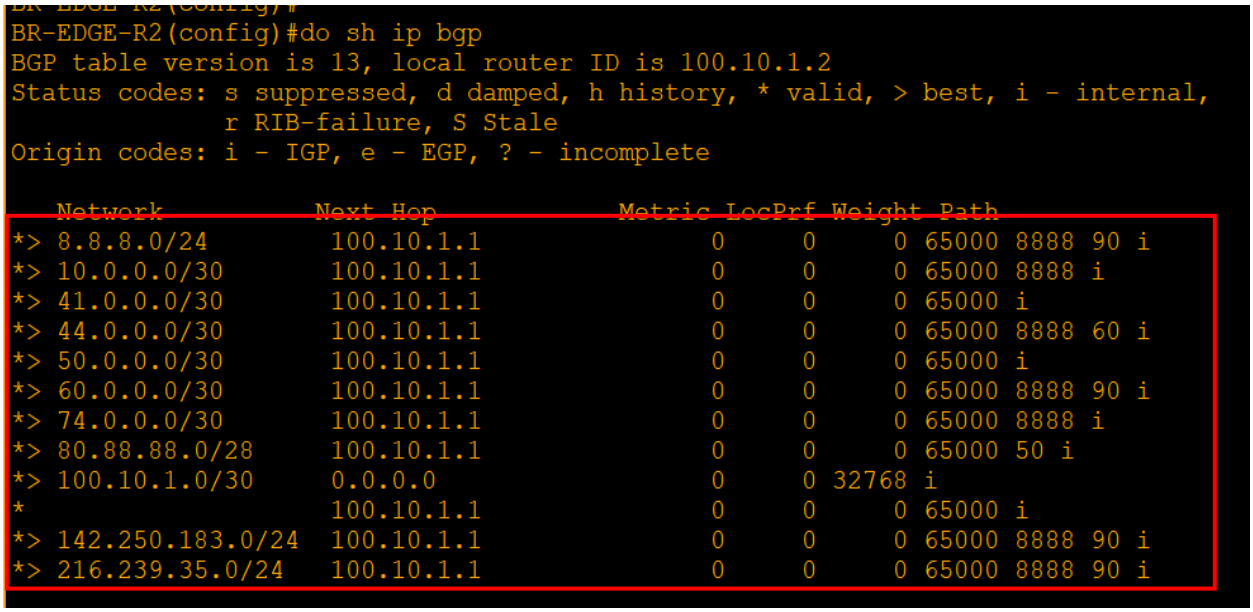


Figure 66-Network using BGP protocol



ISP (Internet Service Provider)

VIANET-ISP

Figure 67-Configuration of BGP in VIANET-ISP

```
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 68-Network using BGP protocol

```
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
```

WORDLINK-ISP

Figure 69-BGP Configuration in WORDLINK-ISP

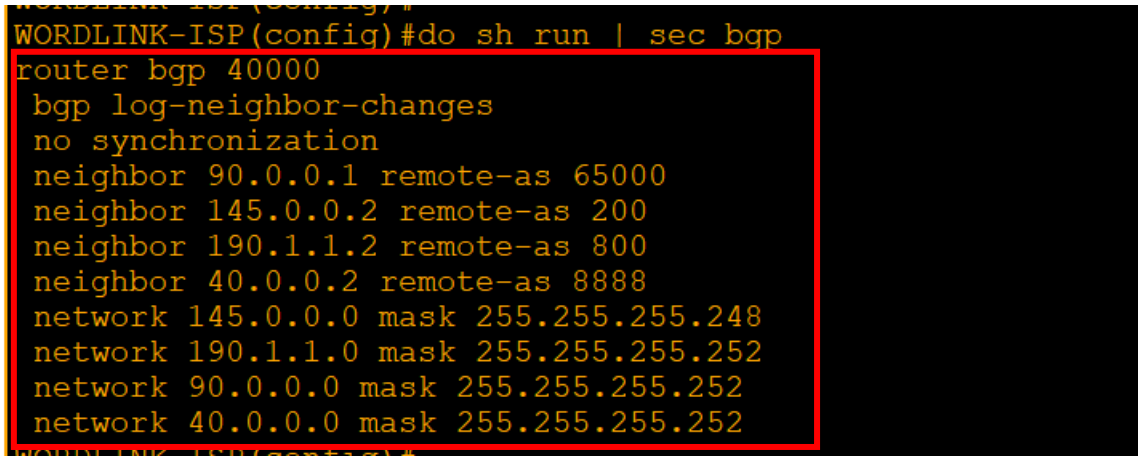
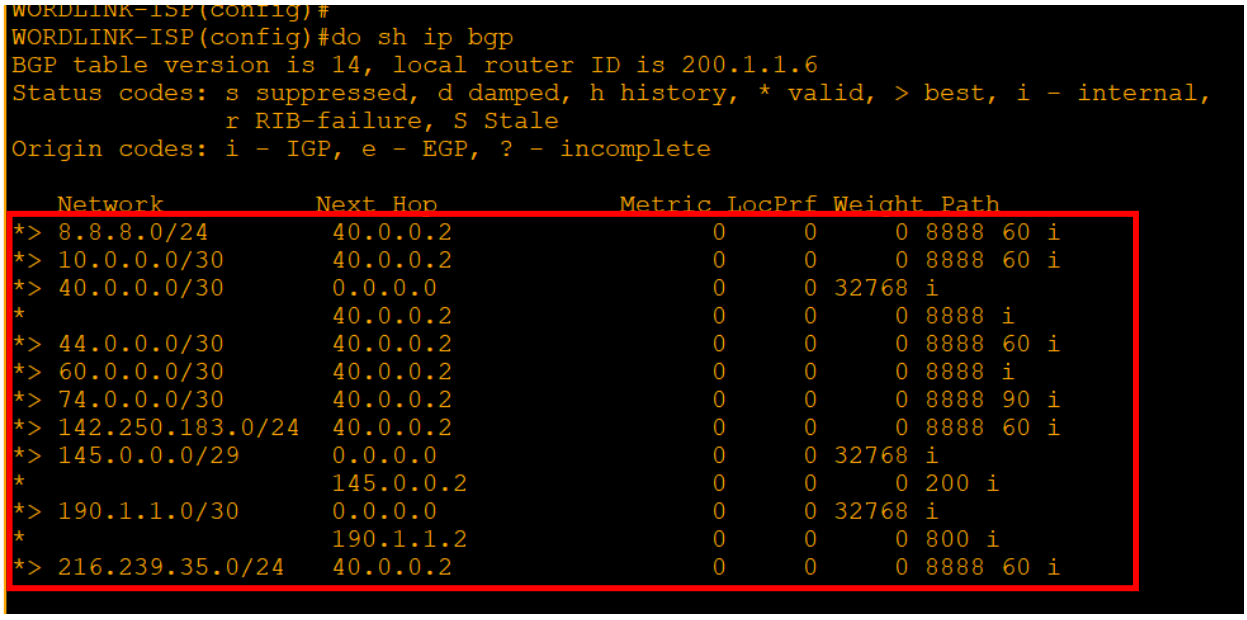


Figure 70-Networks using BGP protocol



Routing in Google

For a simple demonstration, I have implemented a google containing different server like NTP, Google Web, Google DNS etc.

GOOGLE-EDGE-R1

Figure 71-Configuration of BGP in GOOGLE-EDGE-R1

```
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 72-Different networks Using BGP

```
GOOGLE-EDGE-R1(config)#do sh ip bgp
BGP table version is 16, local router ID is 60.0.0.1
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       60.0.0.2                 0      0      0 90 i
*                   44.0.0.1                 0      0      0 60 i
*> 10.0.0.0/30      44.0.0.1                 0      0      0 60 i
*> 40.0.0.0/30      0.0.0.0                  0      0 32768 i
*                   40.0.0.1                 0      0      0 40000 i
*  44.0.0.0/30      44.0.0.1                 0      0      0 60 i
*> 60.0.0.0/30      0.0.0.0                  0      0 32768 i
*                   60.0.0.2                 0      0      0 90 i
*> 74.0.0.0/30      60.0.0.2                 0      0      0 90 i
*> 142.250.183.0/24 60.0.0.2                 0      0      0 90 i
*                   44.0.0.1                 0      0      0 60 i
*> 145.0.0.0/29     40.0.0.1                 0      0      0 40000 i
*> 190.1.1.0/30     40.0.0.1                 0      0      0 40000 i
*> 216.239.35.0/24  60.0.0.2                 0      0      0 90 i
*                   44.0.0.1                 0      0      0 60 i
```

GOOGLE-EDGE-R2

Figure 73-BGP configuration in GOOLGE-EDGE-R2

```
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 74-Network using BGP routing protocol

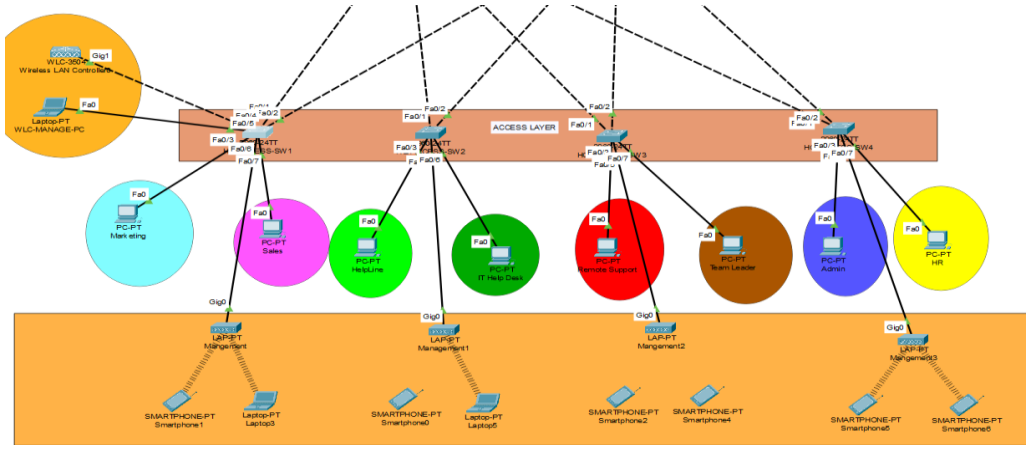
```
GOOGLE-EDGE-R2(config)#do sh ip bgp
BGP table version is 18, local router ID is 74.0.0.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   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
```

ACCESS LAYER

In this layer, end devices like PC, Printer, Access-point and WLC are connected.

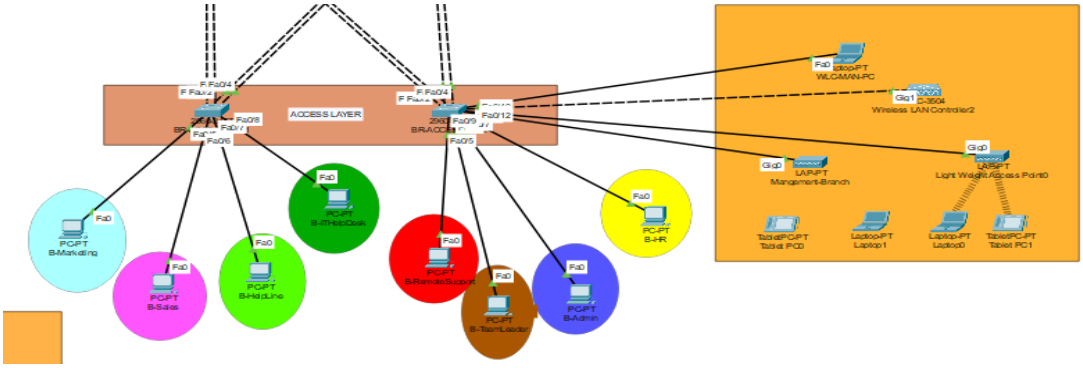
HEADQURTER

Figure 75-Access layer of headquarter



BRANCH

Figure 76-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 VLANs allocation for headquarter

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 2VLANs allocation for branch

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	-----

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.

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 address with 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 4 VLSM in Branch

No of Department	No of end user Host	No of Gateways (SVI 1 +SVI 2+V. IP)	No of Redundancy	Total required host	IP address with 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

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.

Figure 77-Showing PVST is enable by default in switch

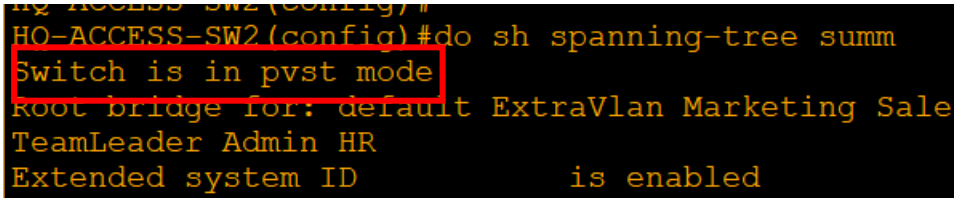
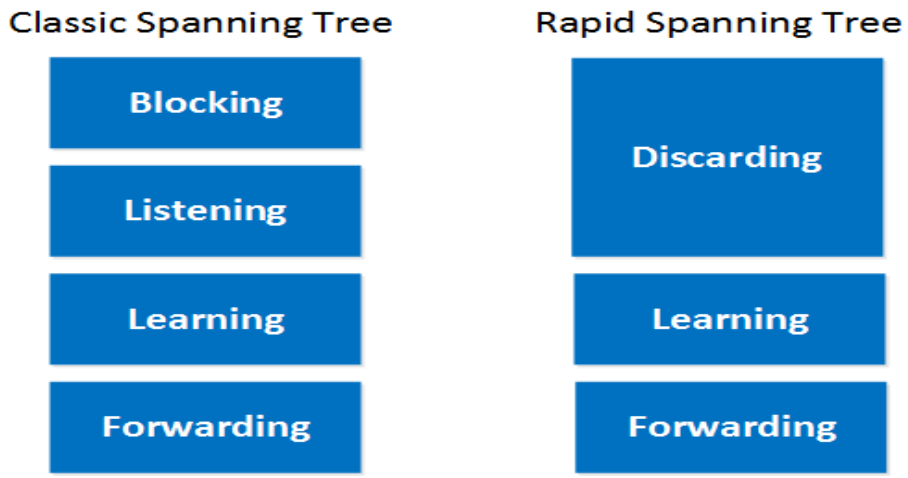


Figure 78-Normal spanning tree state vs Rapid Spanning-tree state

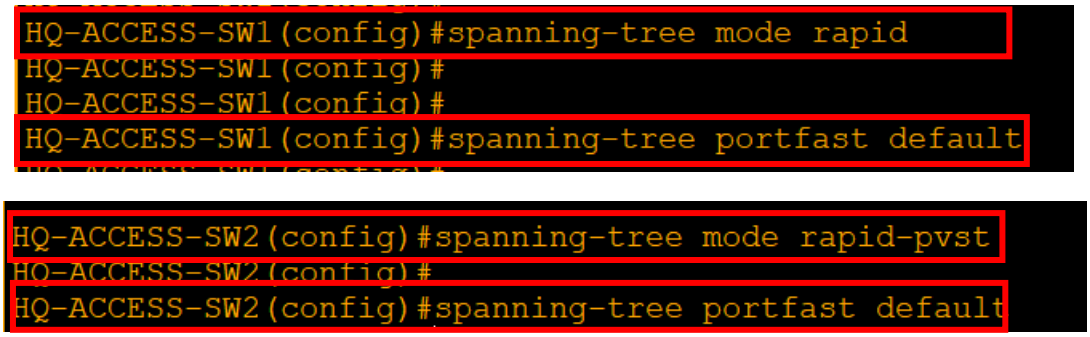


To connect to this network the end users must connect through this l2 switches, user must go through the STP states to access the network. To bypass the three states i.e., Blocking, Listening, and Learning. And initiates directly into the forwarding state. For example, if the user reloads or boots up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

HEADQUARTER

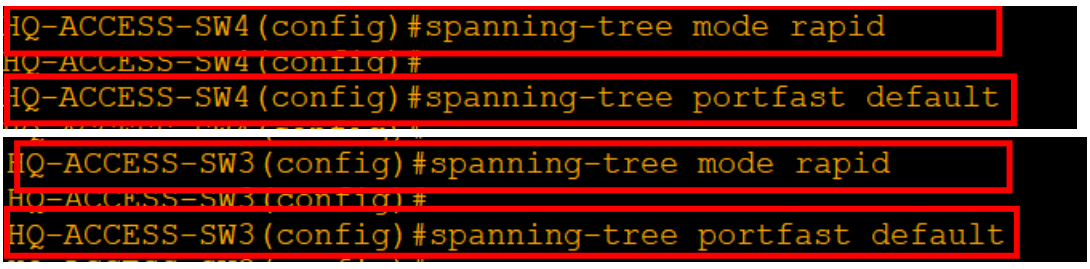
HQ-ACCESS-SW1 & HQ-ACCESS-SW2

Figure 79-Enabling rapid-pvst and Portfast in HQ-ACCESS-SW1 and HQ-ACCESS-SW2



HQ-ACCESS-SW3 & HQ-ACCESS-SW4

Figure 80-Enabling rapid-pvst and portfast in HQ-ACCESS-SW3 and HQ-ACCESS-S4



HQ-DISTRI-SW1

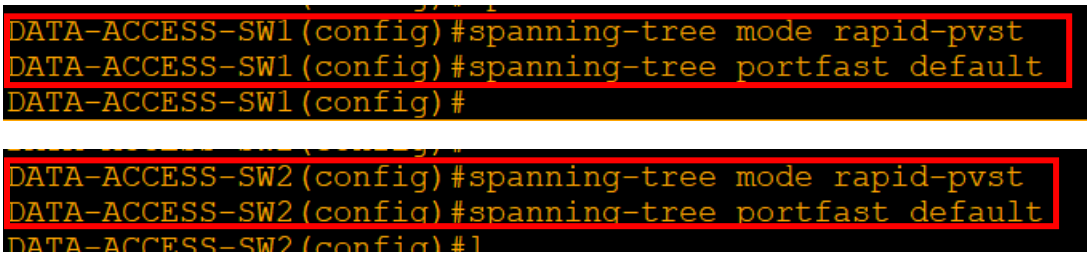
Figure 81-Only enabling rapid-pvst mode in HQ-DISTRI-SW1

Figure

Figure 82-Enabling rapid-pvst in HQ-DISTRI-SW2

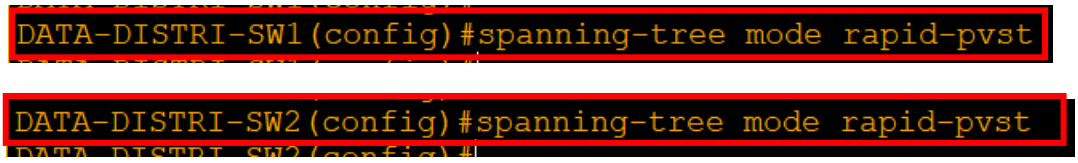
DATA-ACCESS-SW1 & DATA-ACCESS-SW2

Figure 83-Enabling rapid-pvst and Portfast mode in DATA-ACCESS-SW1 and DATA-ACCESS-SW2



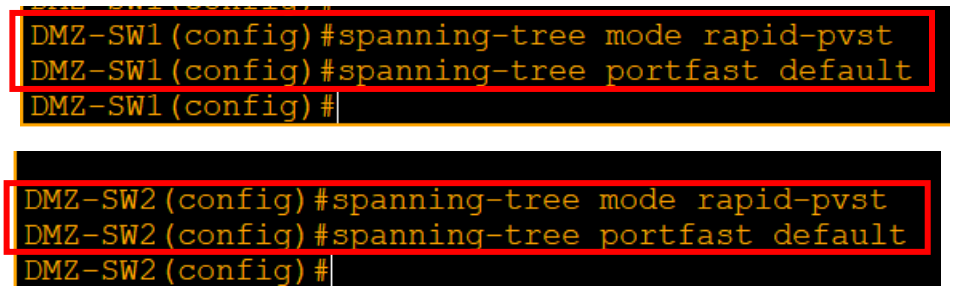
DATA-DISTRI-SW1 & DATA-DISTRI-SW2

Figure 84-Enabling rapid-pvst in DATA-DISTRI-SW1 and DATA-DISTRI-SW2



DMZ-SW1 & DMZ-SW2

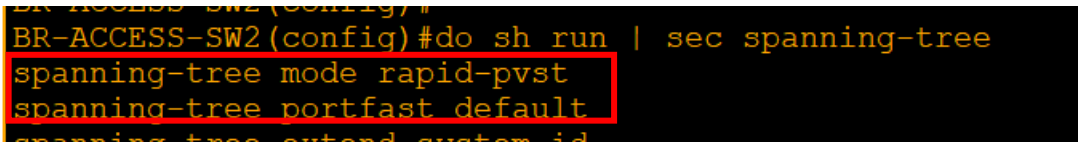
Figure 85-Enabling rapid-pvst and portfast mode in DMZ-ACCESS-SW1 and DMZ-ACCESS-SW2

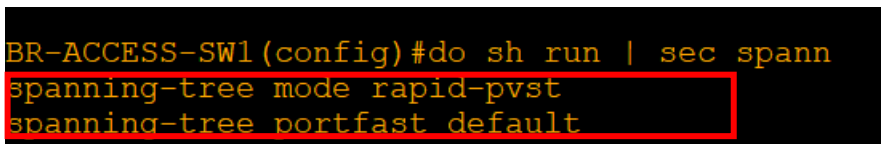


BRANCH

BR-ACCESS-SW1 & BR-ACCESS-SW2

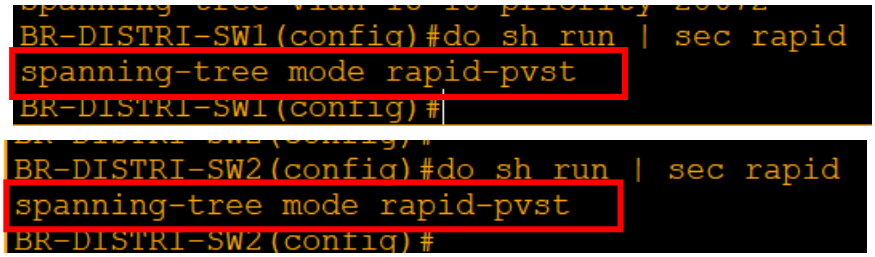
Figure 86-Enabling of rapid-pvst and portfast in BR-ACCESS-SW1 and BR-ACCESS-SW2





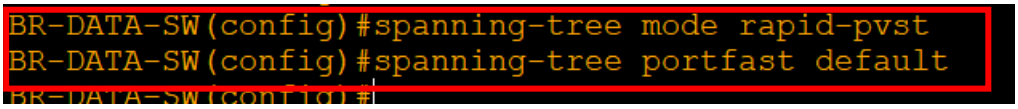
BR-DISTRI-SW1 & BR-DISTRI-SW2

Figure 87-Running config of enabling rapid-pvst in BR-DISTRI-SW1 and BR-DISTRI-SW2



BR-DATA-SW

Figure 88-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.

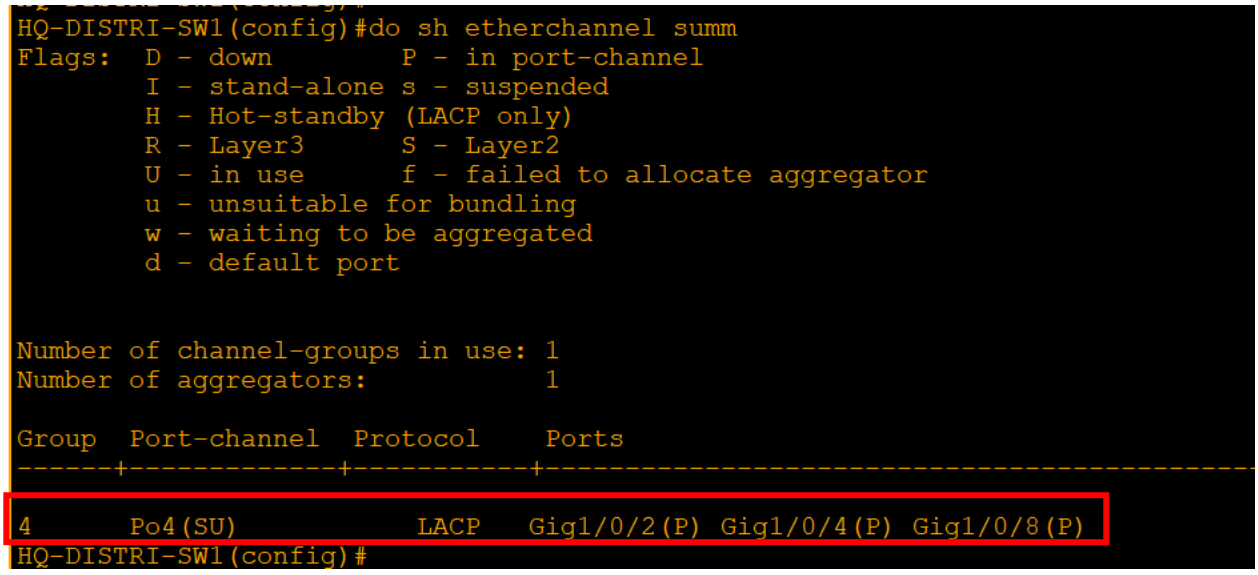
LACP over PAGP

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.

HEADQUARTER

HQ-DISTRI-SW1

Figure 89-Summary of ether-channel configuration in HQ-DISTRI-SW1



HQ-DISTRI-SW2

Figure 90-Ether-channel configuration summary of HQ-DISTRO-SW2

```
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)#
```

BRANCH

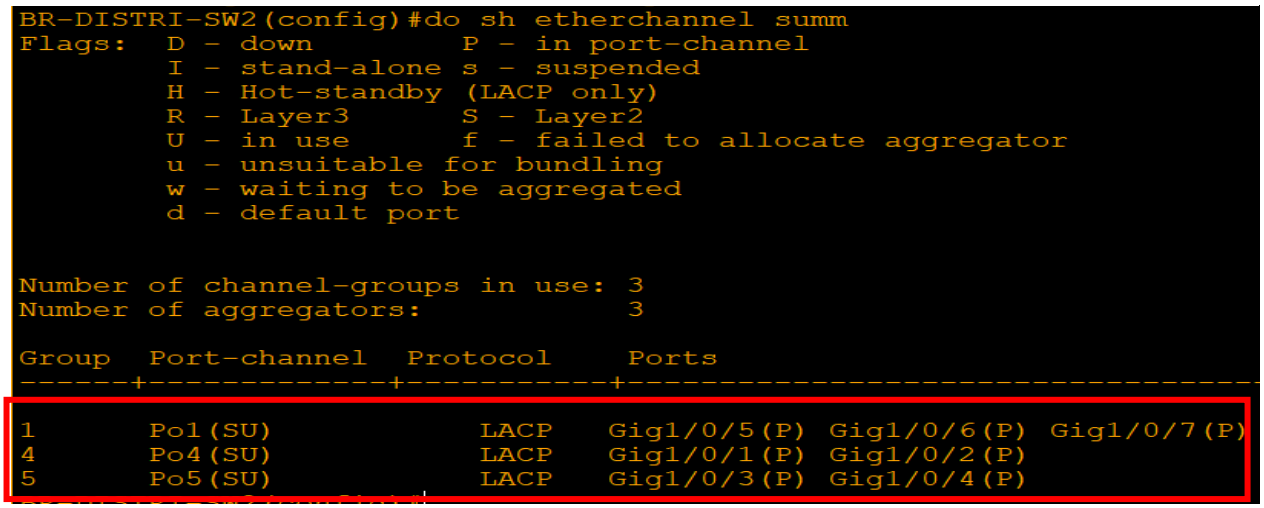
BR-DISTRI-SW1

Figure 91-Ether-channel configuration summary of BR-DISTRI-SW1

```
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)
```

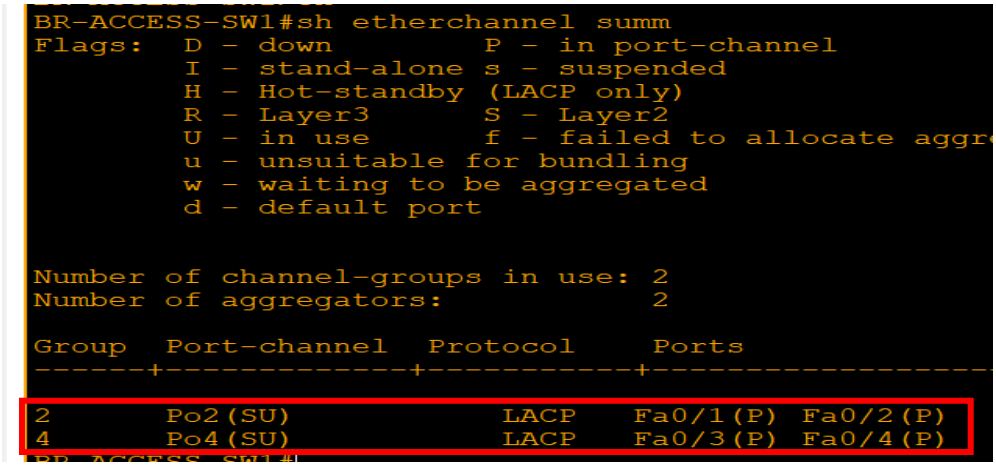
BR-DISTRI-SW2

Figure 92-Summary of ether-channel configuration



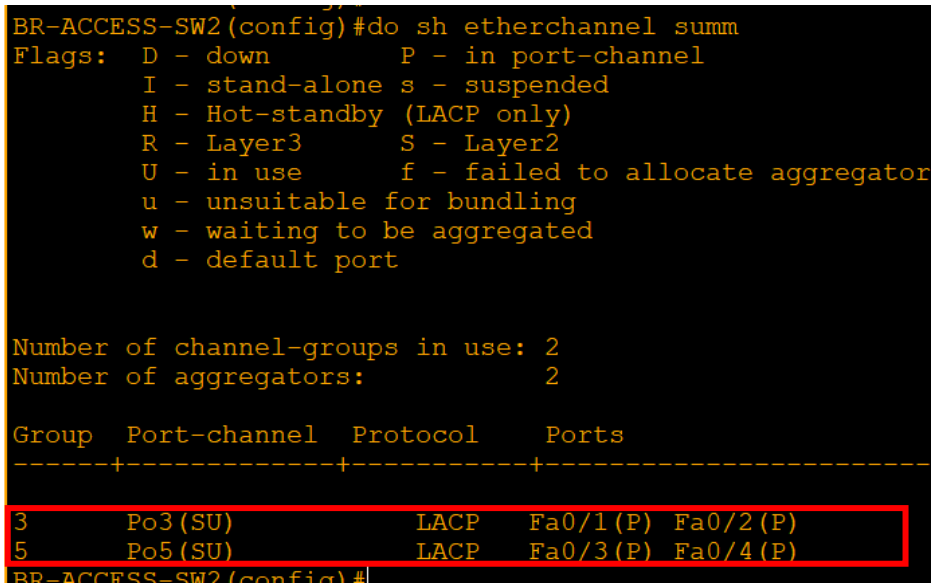
BR-ACCESS-SW1

Figure 93-Ether-channel configuration summary of BR-ACCESS-SW1



BR-ACCESS-SW2

Figure 94-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

Table 5 Gateway and virtual IP with HSRP of Headquarter

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 6 Gateway and virtual IP with HSRP of Branch

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 7 Redundancy in data center of HQ, Branch and DMZ

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 8 HSRP in google server

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**

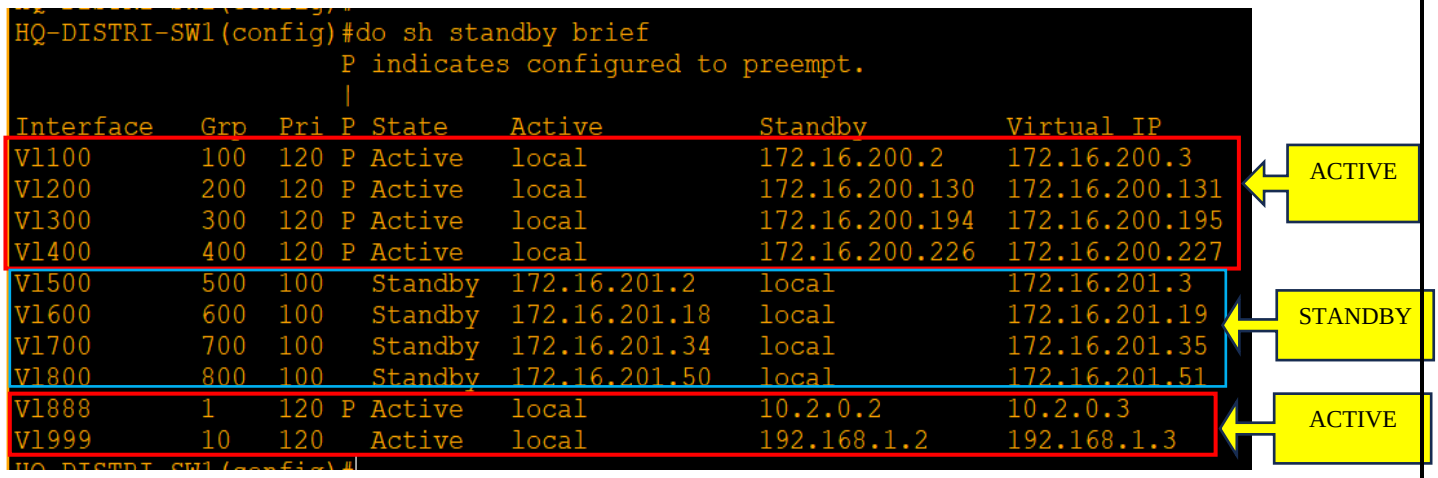
HEADQUARTER

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.

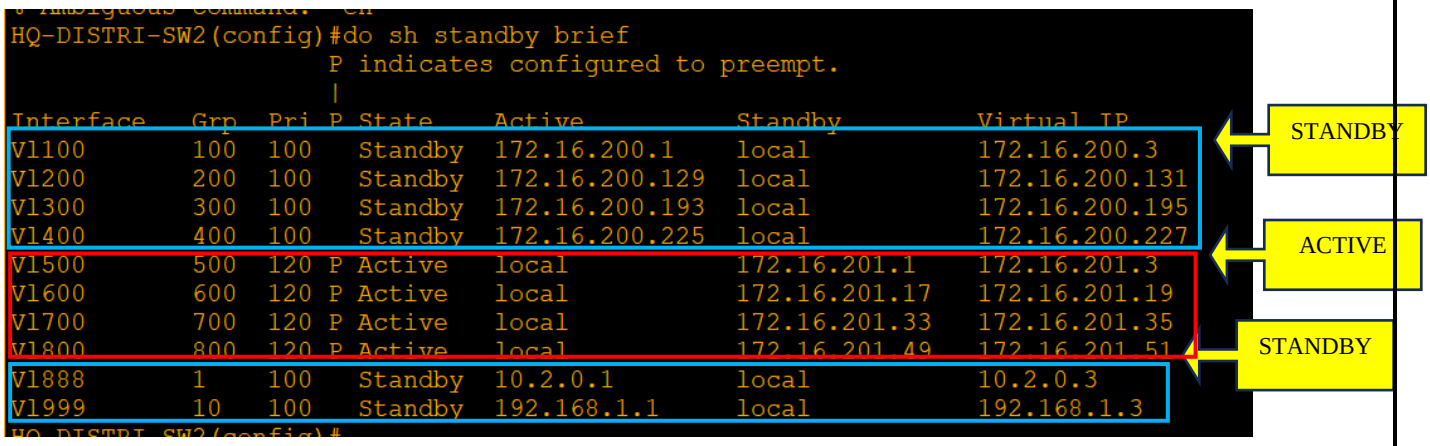
HQ-DISTRI-SW1

Figure 95-HSRP load balancing in HQ-DISTRI-SW1



HQ-DISTRI-SW2

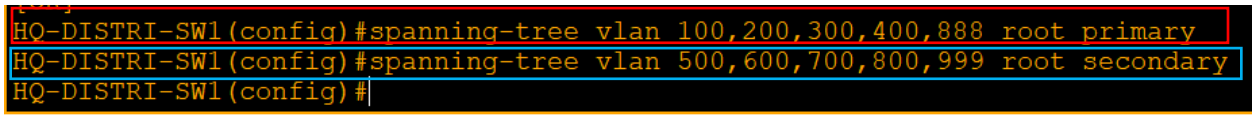
Figure 96-HSRP load balancing in HQ-DISTRI-SW2



Synchronizing HSRP with STP

HQ-DISTRI-SW1

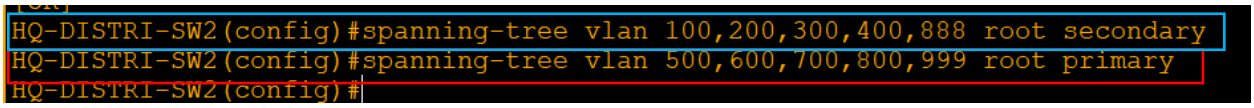
Figure 97-Root bridge configuration for each VLAN in HQ-DISTRI-SW



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

Figure 98-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.

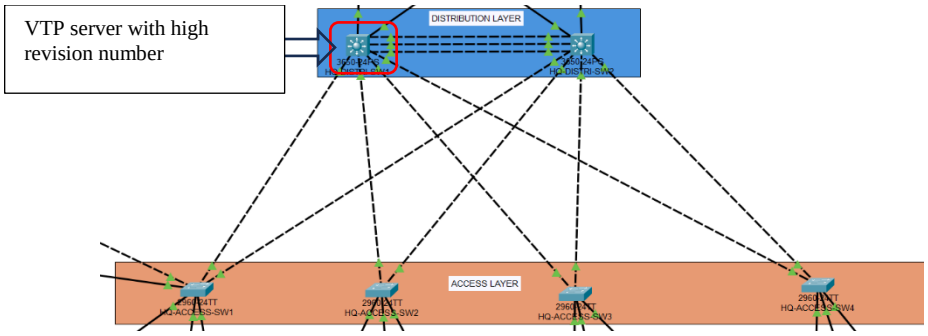
VTP and trunk port

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 99-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
```

HQ-DISTRI-SW1

Figure 100-VTP status of HQ-DISTRI-SW1

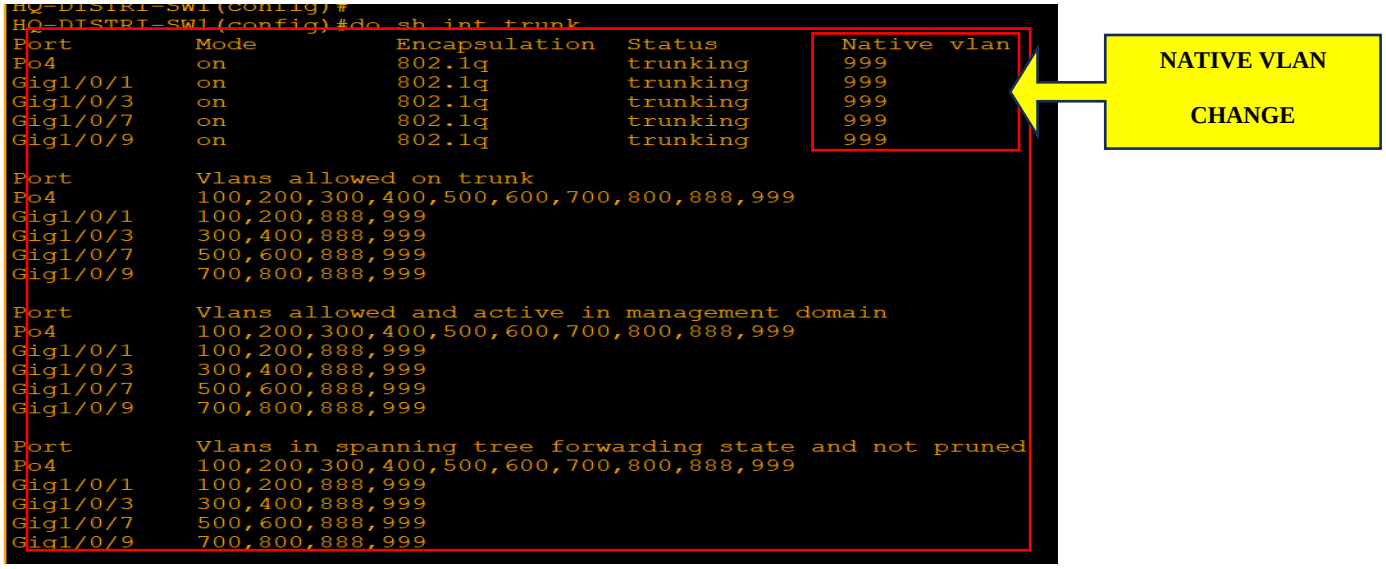
```
HQ-DISTRI-SW1(config)#do sh vtp status
VTP Version capable             : 1 to 2
VTP version running             : 2
VTP Domain Name                 : nihangchha.com
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : 0000.0CAC.1DC0
Configuration last modified by 172.16.200.1 at 3-1-93 00:06:24
Local updater ID is 172.16.200.1 on interface Vl100 (lowest numbered VLAN interface found)

Feature VLAN :
--------------
VTP Operating Mode              : Server
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 16
Configuration Revision          : 1275
MD5 digest                      : 0x6F 0xD1 0x99 0xB3
                                  0xD7 0x95 0x59 0xC8 0xA5 0xA6 0x82 0x14
```

DOMAIN NAME

VTP MODE

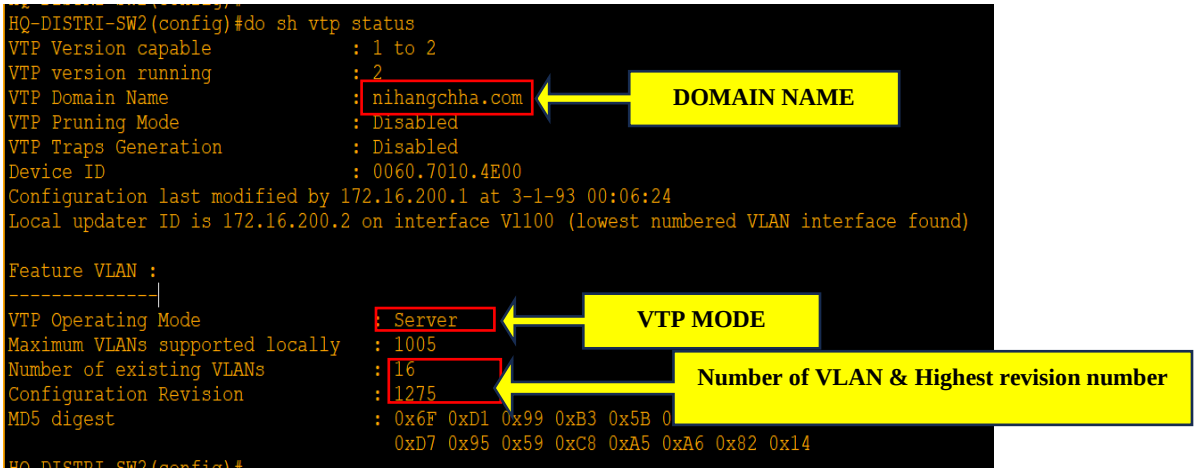
Highest Revision number

Figure 101-Trunking information of HQ-DISTRI-SW1



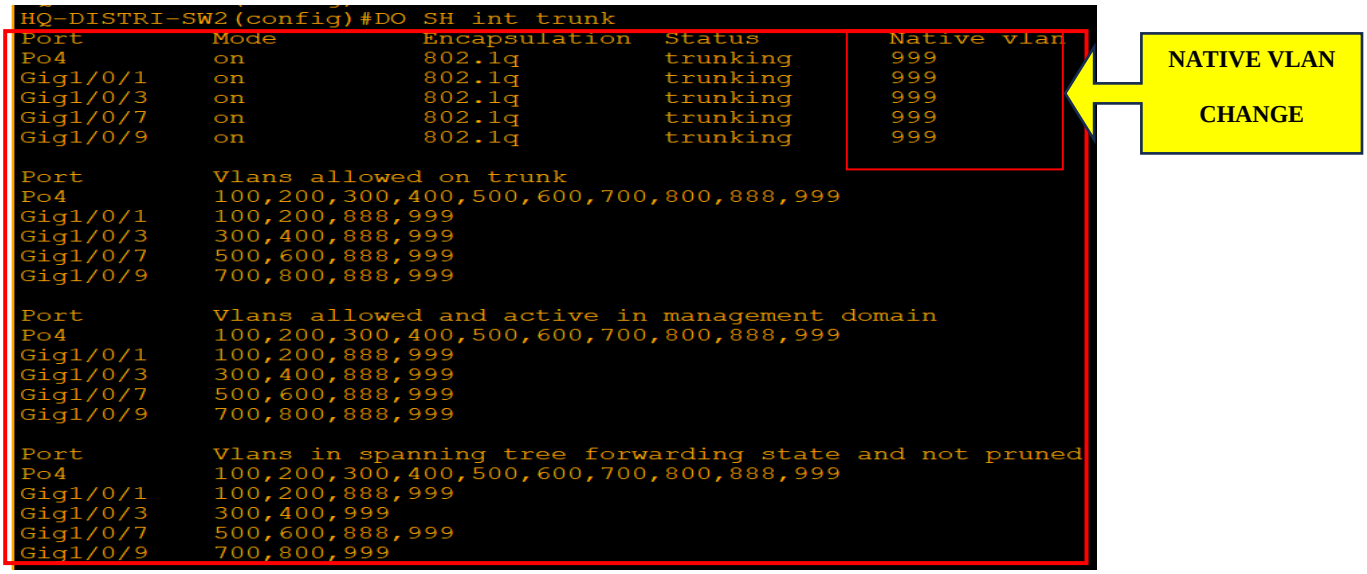
HQ-DISTRI-SW2

Figure 102-VTP status in HQ-DISTRI-SW2



From the above figure, VLAN information are synchronized through trunk port.

Figure 103-Trunking information of HQ-DISTRI-SW2



HQ-ACCESS-SW1

Figure 104-VTP status of HQ-ACCESS-SW1

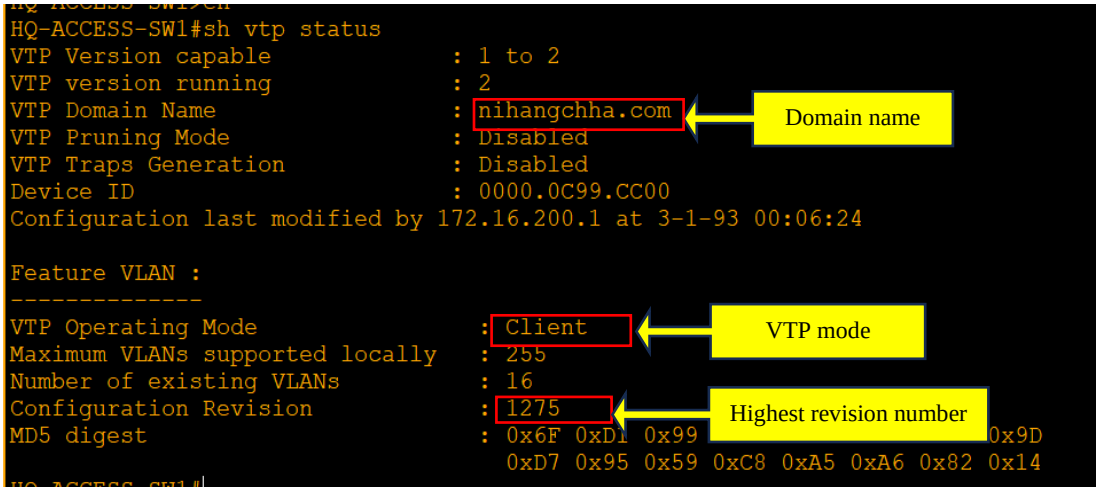
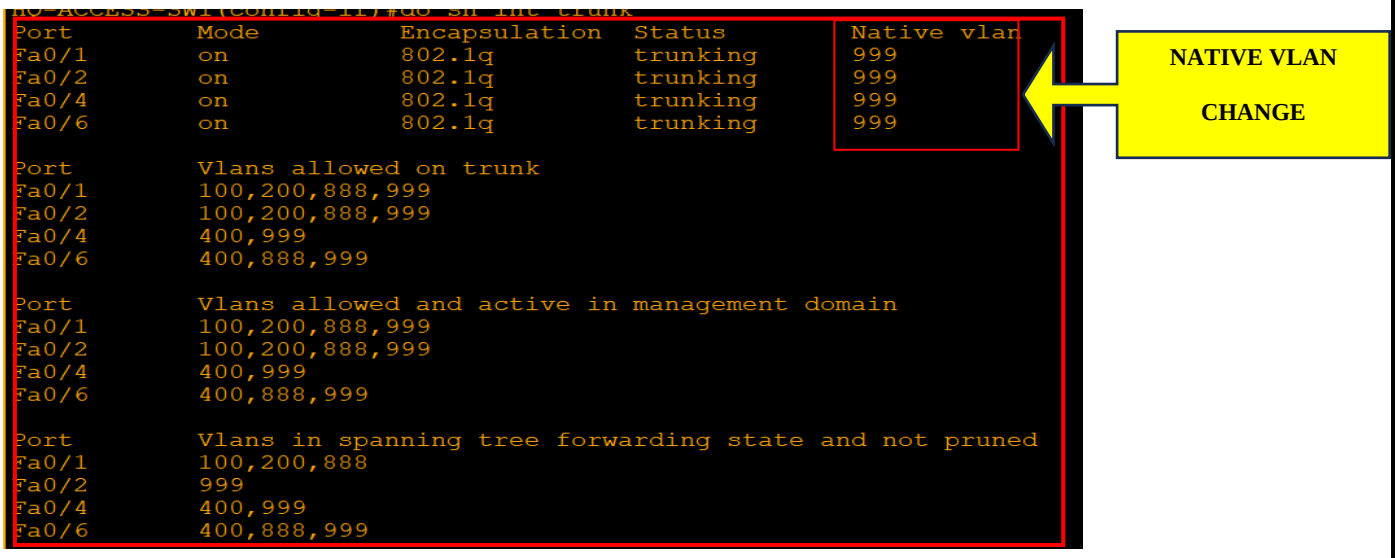


Figure 105-Trunking information of HQ-ACCESS-SW1



HQ-ACCESS-SW2

Figure 106-VTP status of HQ-ACCESS-SW2

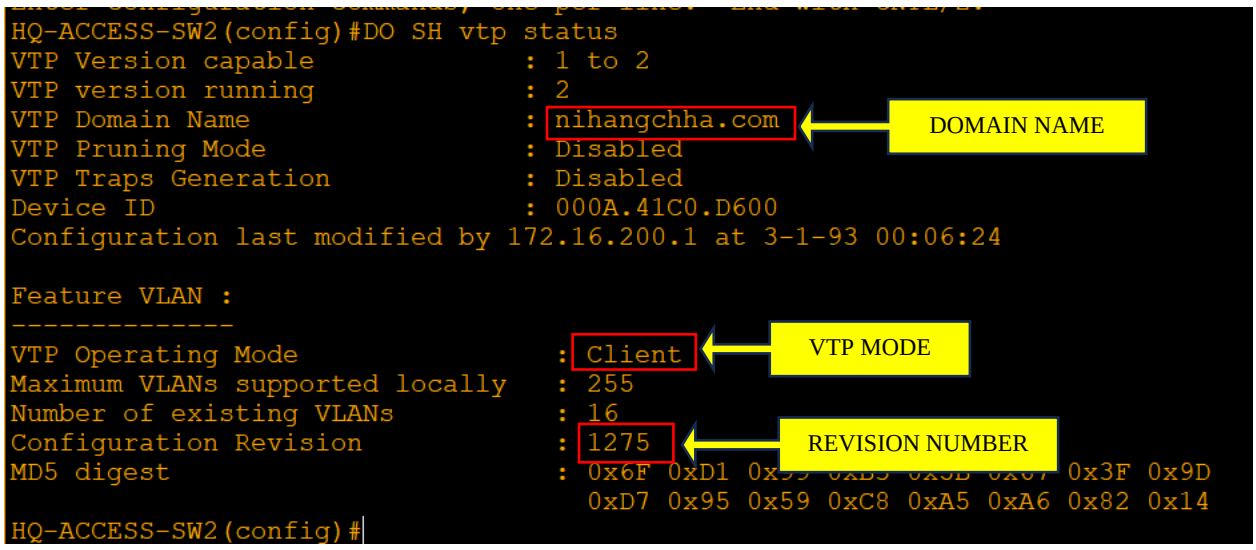
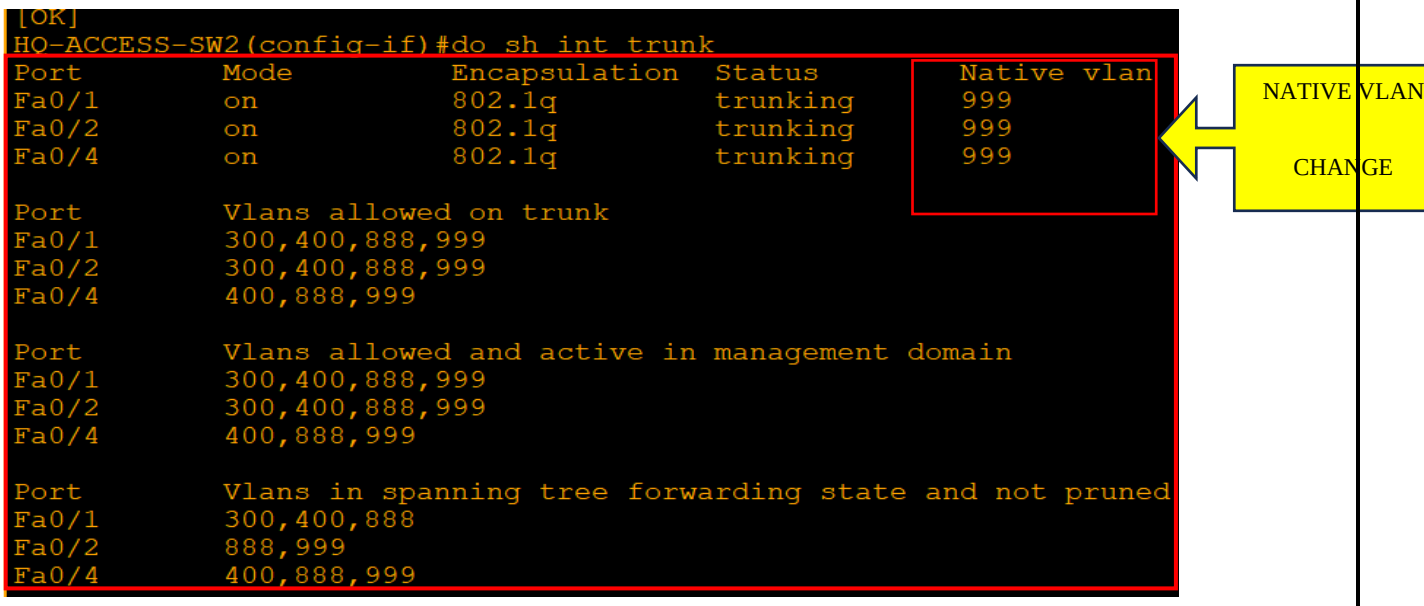


Figure 107-Trunk information of HQ-ACCESS-SW2



HQ-ACCESS-SW3

Figure 108-VTP status on HQ-ACCESS-SW3

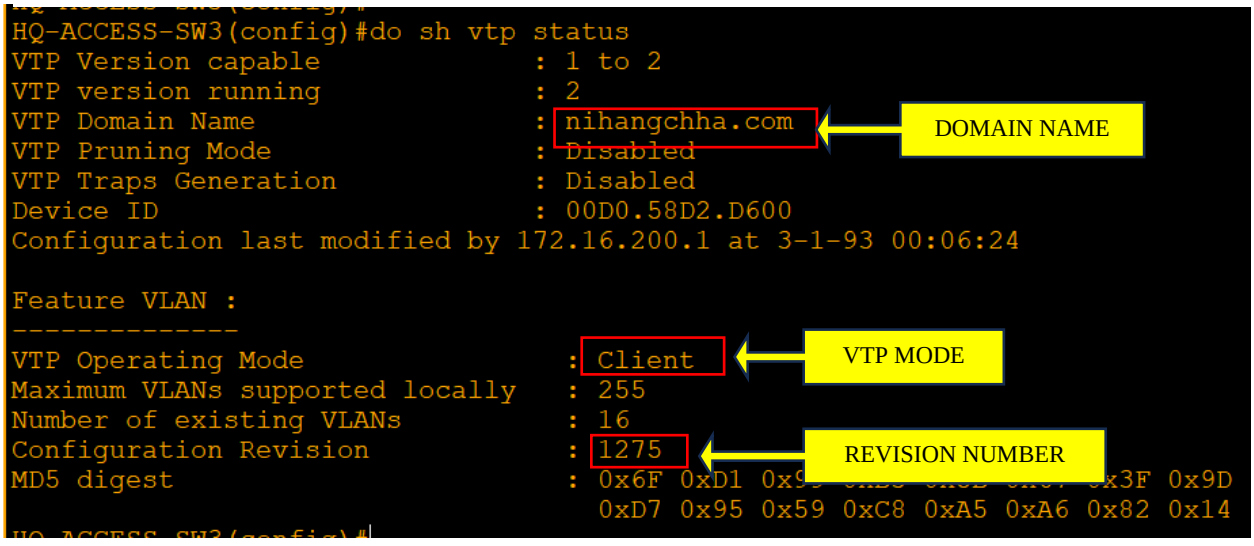
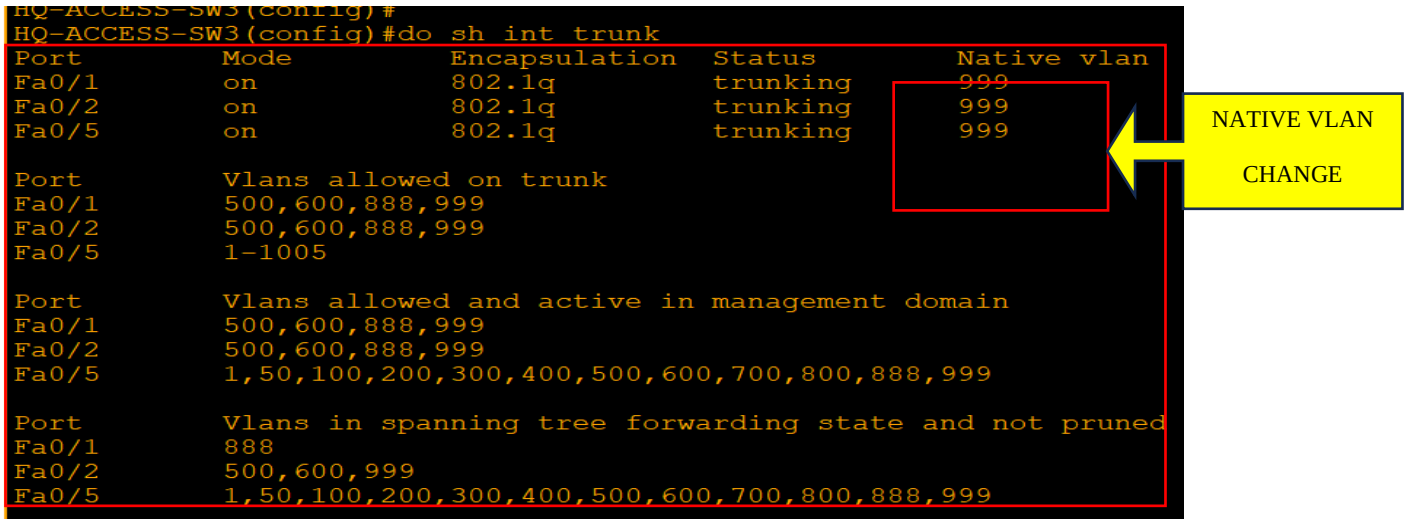


Figure 109Trunk mode on HQ-ACCESS-SW3



HQ-ACCESS-SW4

Figure 110-VTP status on HQ-ACCESS-SW4

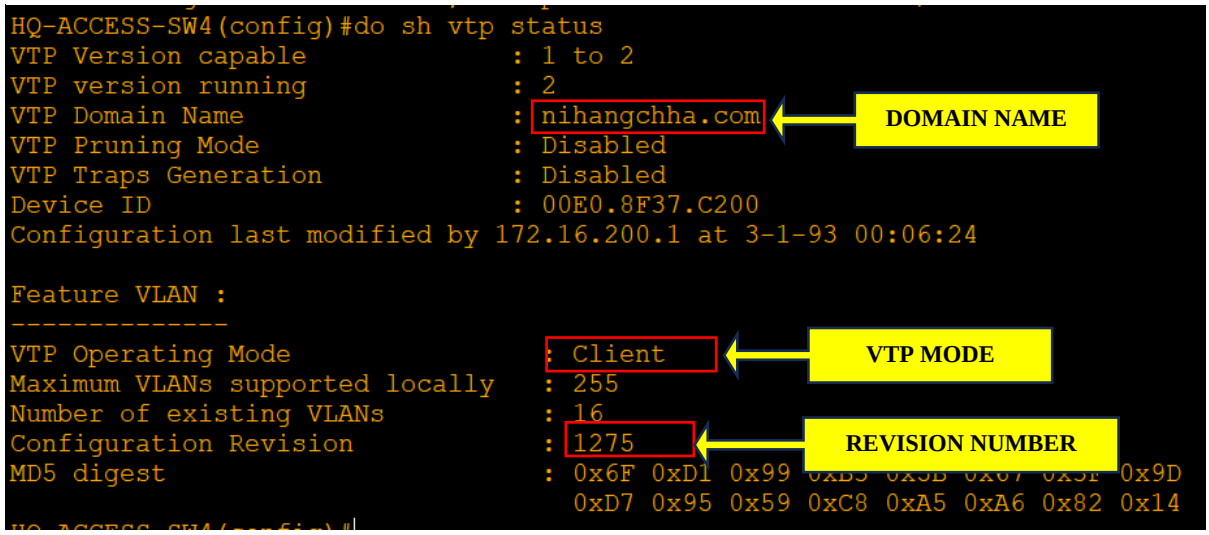
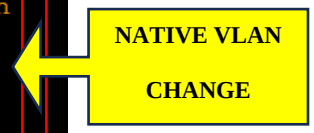


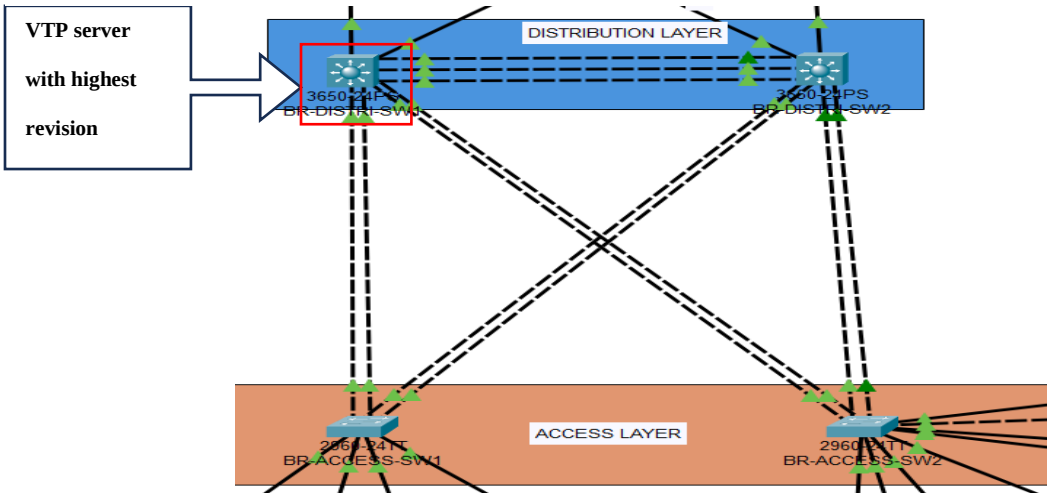
Figure 111-Trunking mode on HQ-ACCESS-SW4

```
HQ-ACCESS-SW4(config)#
HQ-ACCESS-SW4(config)#DO SH int trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      999
Fa0/2       on           802.1q         trunking      999
Fa0/6       on           802.1q         trunking      999

Port        Vlans allowed on trunk
Fa0/1       700,800,888,999
Fa0/2       700,800,888,999
Fa0/6       1-1005

Port        Vlans allowed and active in management domain
Fa0/1       700,800,888,999
Fa0/2       700,800,888,999
Fa0/6       1,50,100,200,300,400,500,600,700,800,888,999

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       888
Fa0/2       700,800,888,999
Fa0/6       1,50,100,200,300,400,500,600,700,800,888,999
```



BRANCH

Figure 112-L3 and L2 switches of branch



BR-DISTRI-SW1

Figure 113-VTP status of BR-DISTRI-SW1

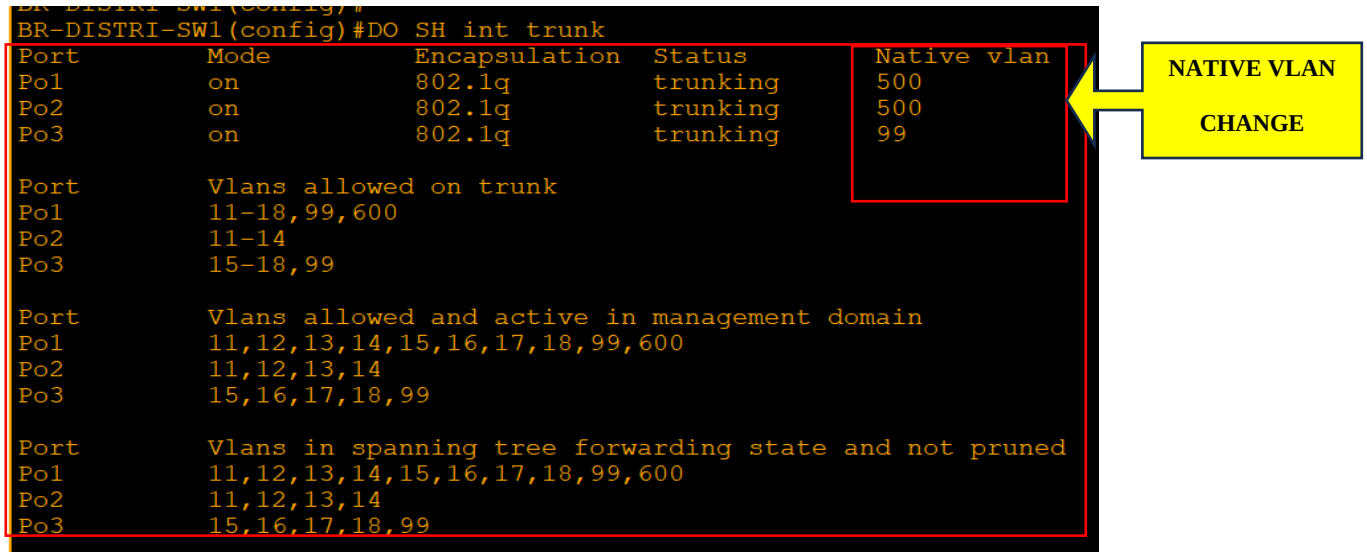
```
BR-DISTRI-SW1(config)#do sh vtp status
VTP Version capable             : 1 to 2
VTP version running             : 2
VTP Domain Name                 : nihangchha.com
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : 0003.E451.2590
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 0x51 0x15 0xD6 0x26 0xE6
                                  0x04 0xA9 0xD9 0xF9 0x30 0xA1 0x77 0xCB
BR-DISTRI-SW1(config)#
```

DOMAIN NAME

VTP MODE

REVISION NUMBER

Figure 114-Trunking information of BR-DISTRI-SW1



BR-DISTRI-SW2

Figure 115-VTP status of BR-DISTRI-SW2

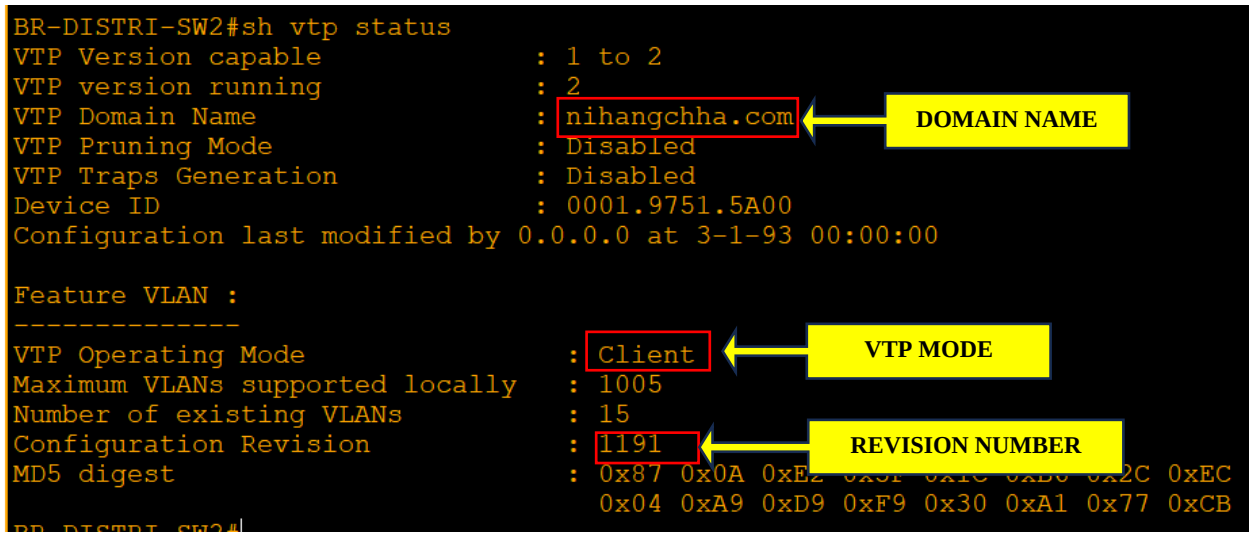
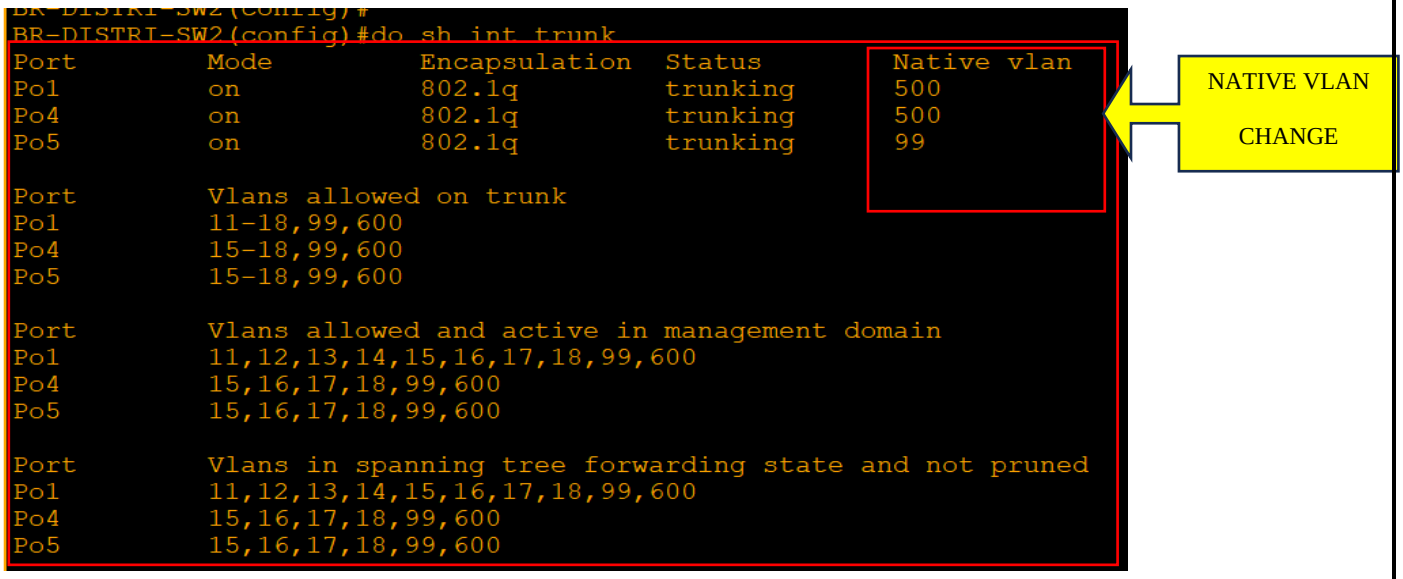


Figure 116-Trunking information of BR-DISTRI-SW2



BR-ACCESS-SW1

Figure 117-VTP status of BR-ACCESS-SW1

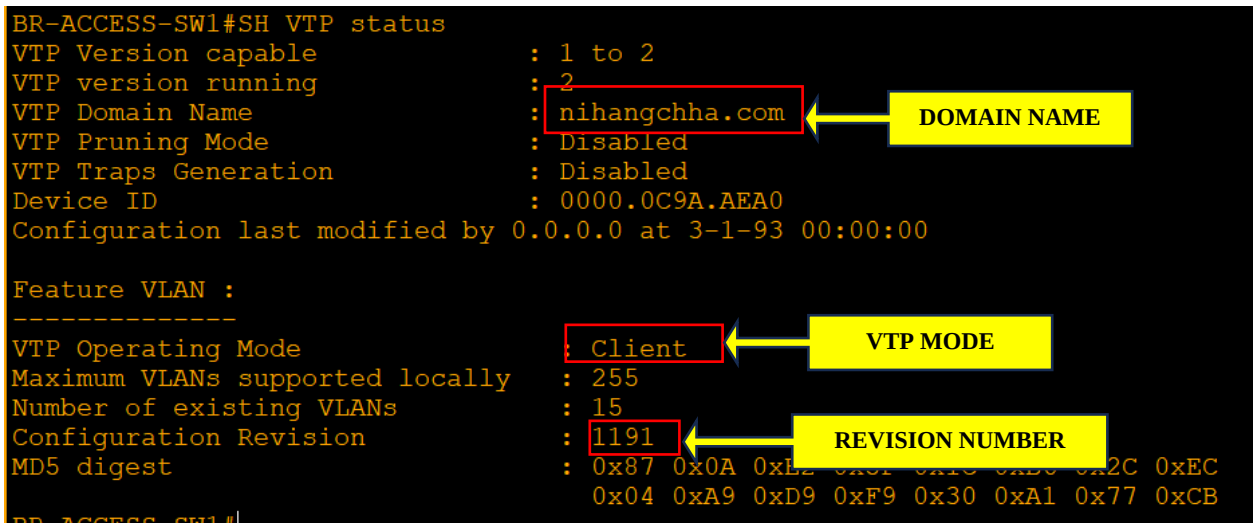
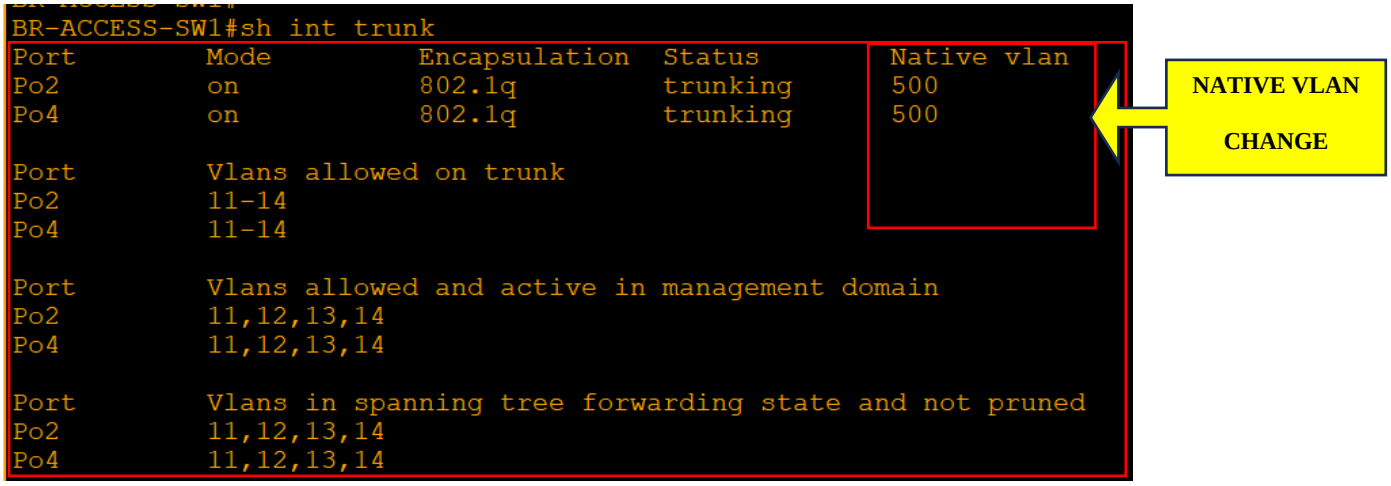


Figure 118-Trunking information of BR-ACCESS-SW1



BR-ACCESS-SW2

Figure 119-VTP status of BR-ACCESS-SW2

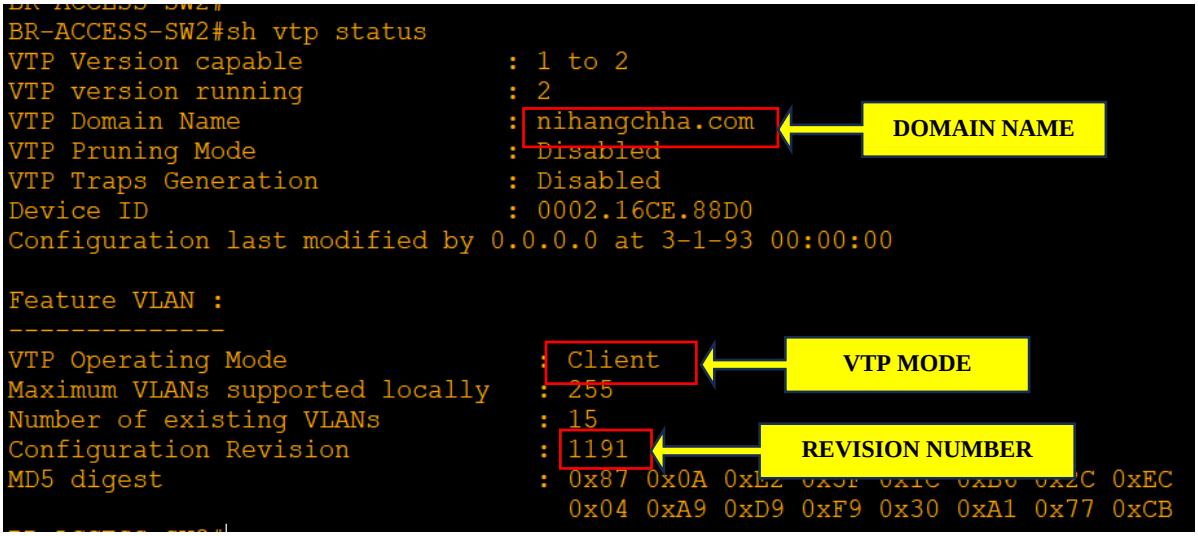
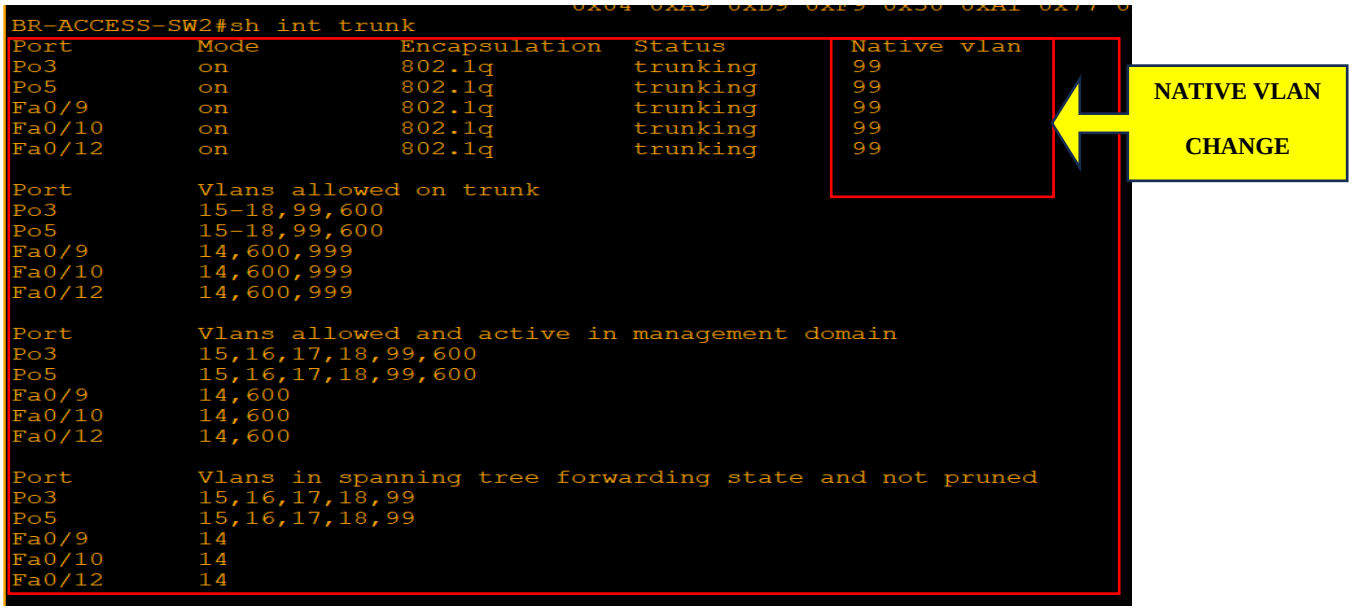


Figure 120-Trunking information of BR-ACCESS-SW2



DHCP (Dynamic Host Configuration Protocol)

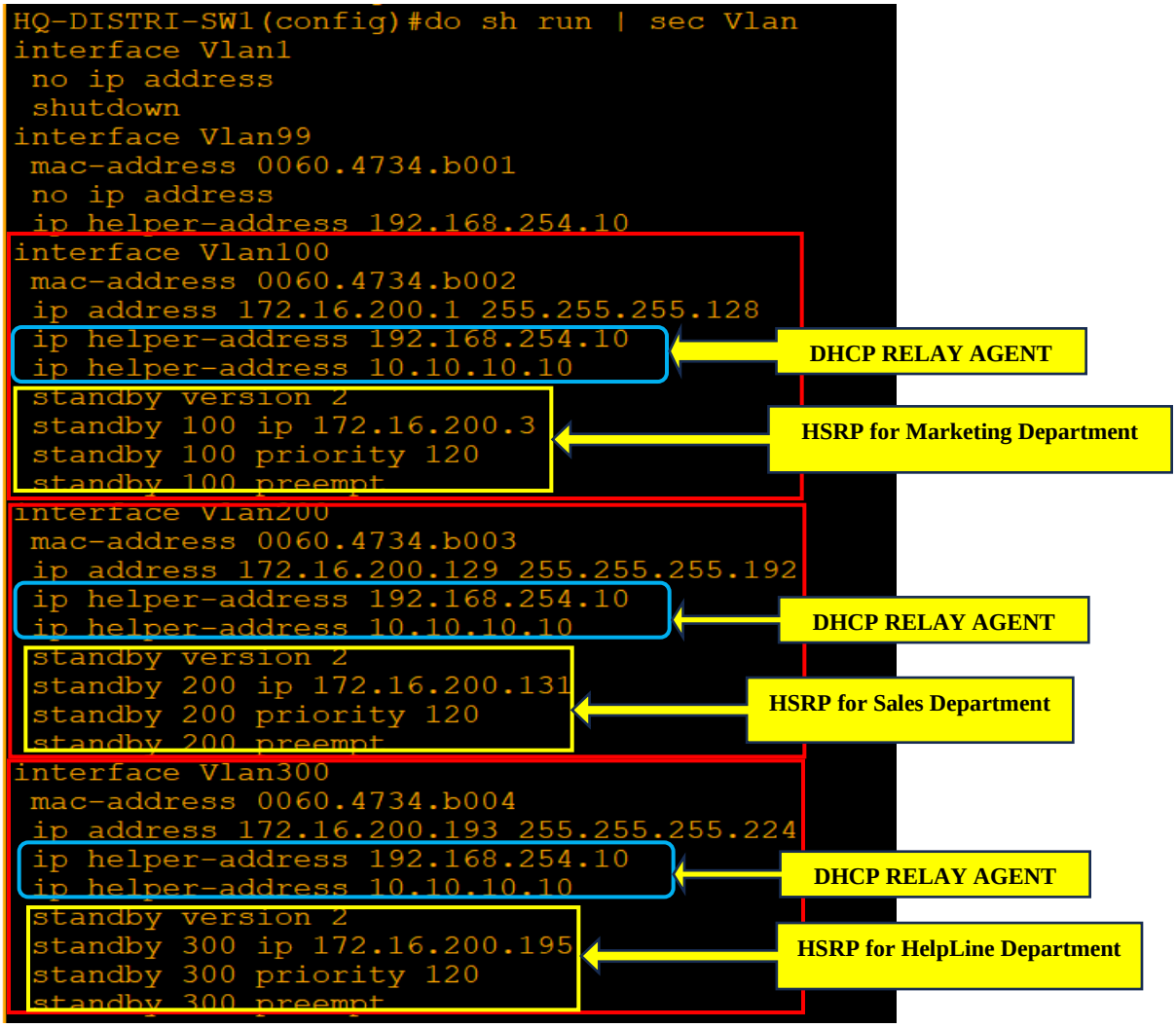
Assigning IP addresses statically to end devices may work well in small companies, but it becomes impractical in larger organizations where the number of users accessing the Internet can reach thousands. In such scenarios, DHCP becomes essential as it automates the process of assigning IP addresses to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

HEADQUARTER

Figure 121-DHCP configuration of each department in HQ server with DNS server and WLC address

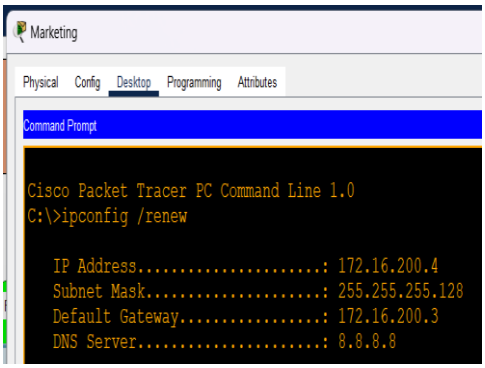
Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
Sales	172.16.200.131	80.88.88.4	172.16.200.131	255.255.255.192	50	0.0.0.0	192.168.1.4
HR	172.16.201.51	80.88.88.4	172.16.201.52	255.255.255.248	3	0.0.0.0	192.168.1.4
Admin	172.16.201.35	80.88.88.4	172.16.201.36	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
ITHelpDesk	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

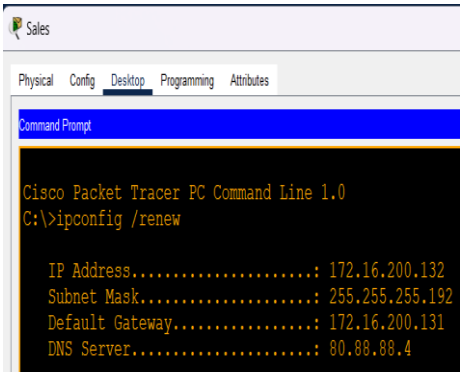
Figure 122-DHCP relay agent and HSRP

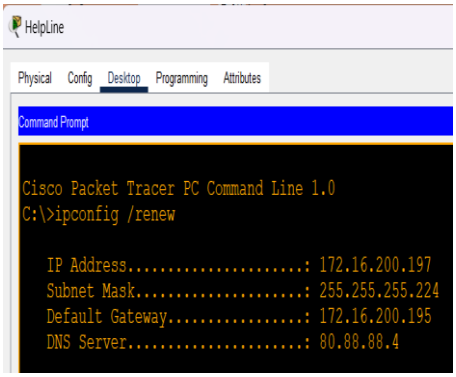


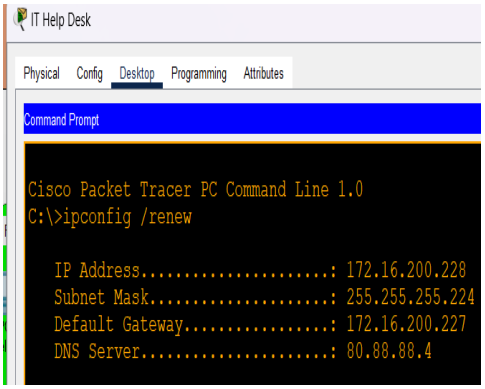

interface Vlan400
mac-address 0060.4734.b005
ip address 172.16.200.225 255.255.255.224
ip helper-address 192.168.254.10
ip helper-address 10.10.10.10
DHCP RELAY AGENT
standby version 2
standby 400 ip 172.16.200.227
standby 400 priority 120
standby 400 preempt
HSRP for ITHelpDesk Department
interface 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
DHCP RELAY AGENT
standby version 2
standby 500 ip 172.16.201.3
HSRP for RemoteSupport Department
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
DHCP RELAY AGENT
standby version 2
standby 600 ip 172.16.201.19
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
DHCP RELAY AGENT
standby version 2
standby 700 ip 172.16.201.35
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
DHCP RELAY AGENT
standby version 2
standby 800 ip 172.16.201.51
HSRP for HR Department
interface Vlan888
mac-address 0060.4734.b00a
ip address 10.2.0.1 255.255.252.0
ip helper-address 192.168.254.10
ip helper-address 10.10.10.10
DHCP RELAY AGENT
standby 1 ip 10.2.0.3
standby 1 priority 120
standby 1 preempt
HSRP for Guest Department
interface Vlan999
mac-address 0060.4734.b00b
ip address 192.168.1.1 255.255.255.240
ip helper-address 10.10.10.10
DHCP RELAY AGENT
standby 10 ip 192.168.1.3
standby 10 priority 120
HSRP for Management Department

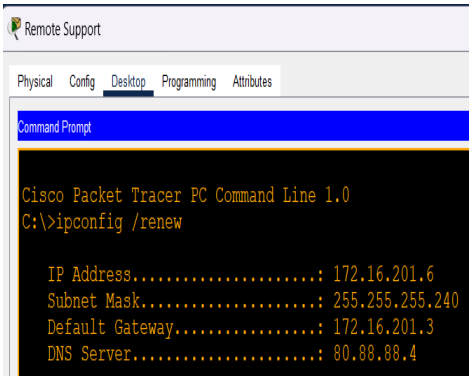
Figure 123-Eight department obtaining IP from DHCP server

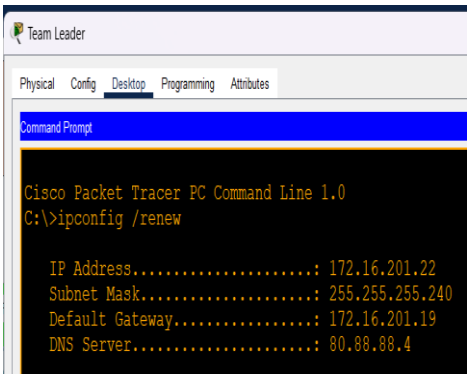


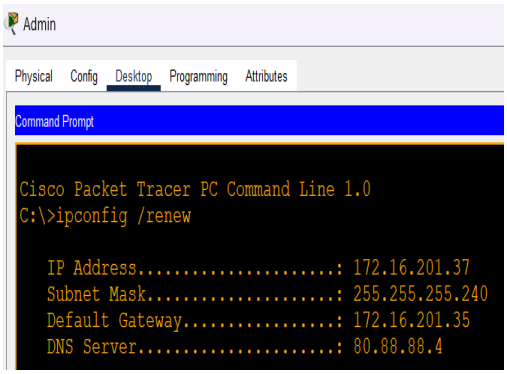


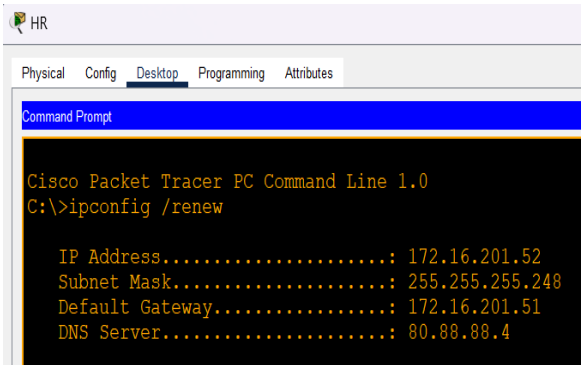










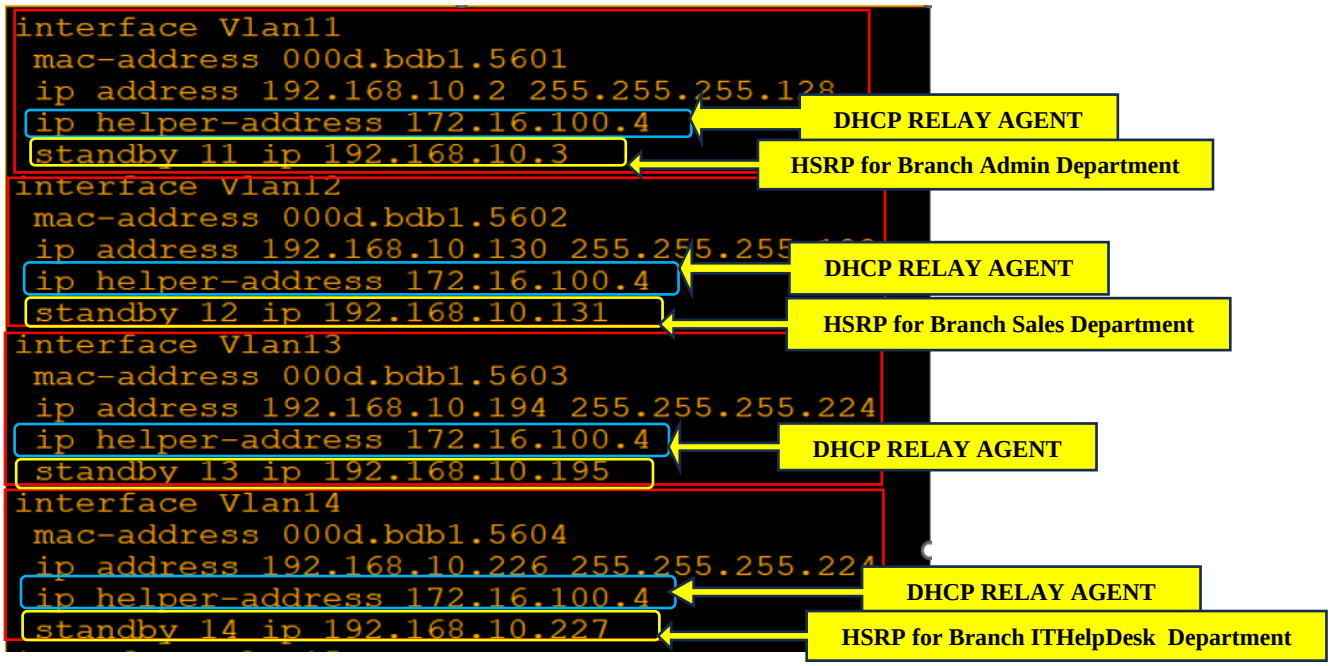


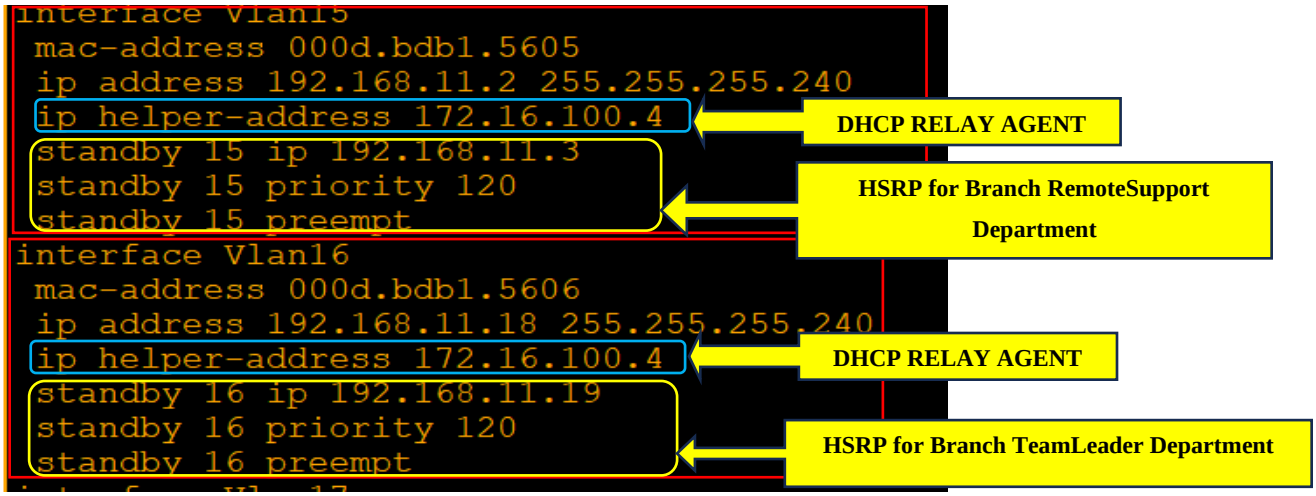
BRANCH

Figure 124-DHCP configuration in branch with different attributes

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 125-DHCP relay agent in branch




interface Vlan15
mac-address 000d.bdb1.5605
ip address 192.168.11.2 255.255.255.240
ip helper-address 172.16.100.4
standby 15 ip 192.168.11.3
standby 15 priority 120
standby 15 preempt
interface Vlan16
mac-address 000d.bdb1.5606
ip address 192.168.11.18 255.255.255.240
ip helper-address 172.16.100.4
standby 16 ip 192.168.11.19
standby 16 priority 120
standby 16 preempt
DHCP RELAY AGENT
HSRP for Branch RemoteSupport Department
DHCP RELAY AGENT
HSRP for Branch TeamLeader Department

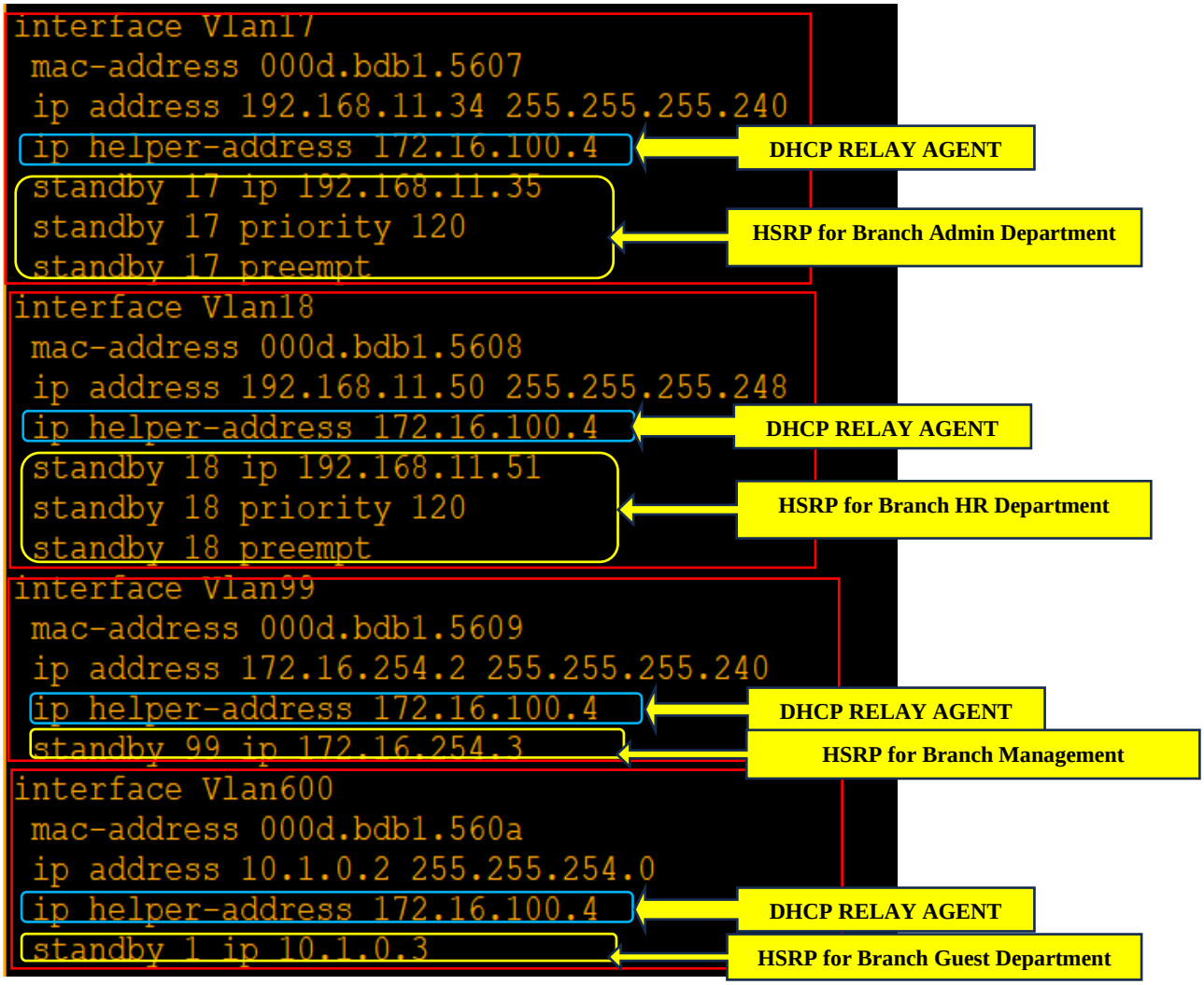
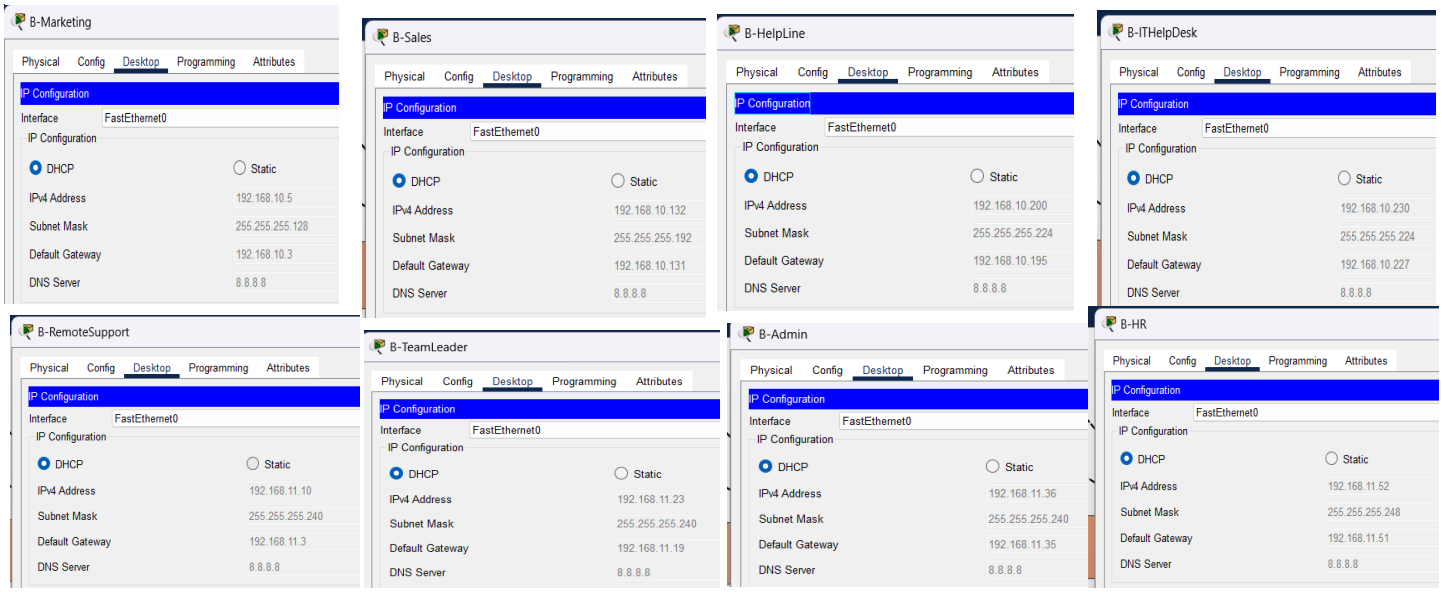

interface Vlan17
mac-address 000d.bdb1.5607
ip address 192.168.11.34 255.255.255.240
ip helper-address 172.16.100.4
standby 17 ip 192.168.11.35
standby 17 priority 120
standby 17 preempt
interface Vlan18
mac-address 000d.bdb1.5608
ip address 192.168.11.50 255.255.255.248
ip helper-address 172.16.100.4
standby 18 ip 192.168.11.51
standby 18 priority 120
standby 18 preempt
interface Vlan99
mac-address 000d.bdb1.5609
ip address 172.16.254.2 255.255.255.240
ip helper-address 172.16.100.4
standby 99 ip 172.16.254.3
interface Vlan600
mac-address 000d.bdb1.560a
ip address 10.1.0.2 255.255.254.0
ip helper-address 172.16.100.4
standby 1 ip 10.1.0.3
DHCP RELAY AGENT
HSRP for Branch Admin Department
DHCP RELAY AGENT
HSRP for Branch HR Department
DHCP RELAY AGENT
HSRP for Branch Management
DHCP RELAY AGENT
HSRP for Branch Guest Department

Figure 126-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 127-Physical diagram of access layer HQ

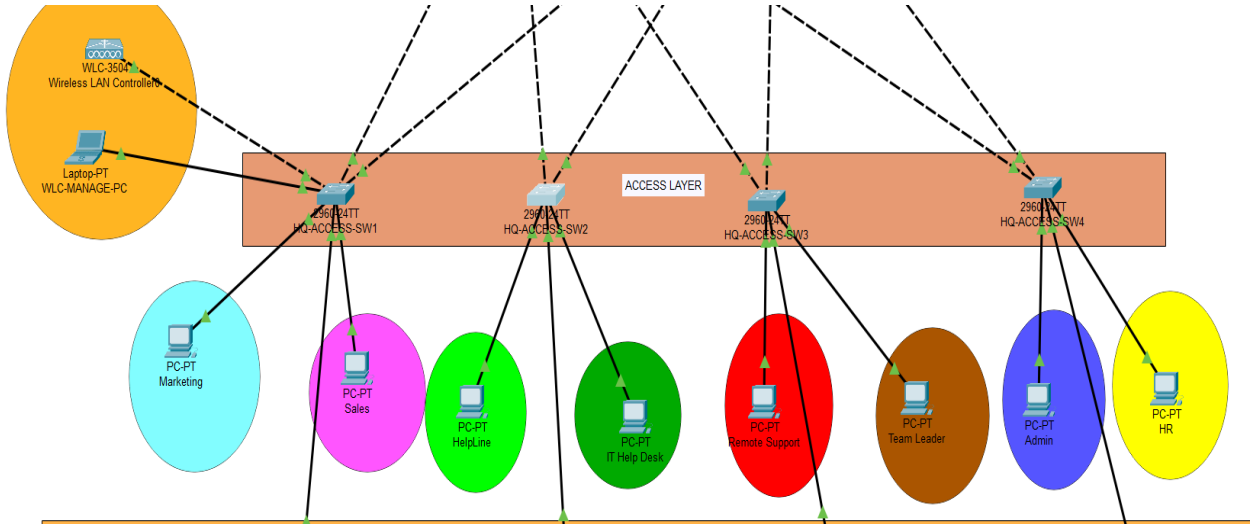


Figure 128-VLAN brief of HQ-ACCESS-SW1

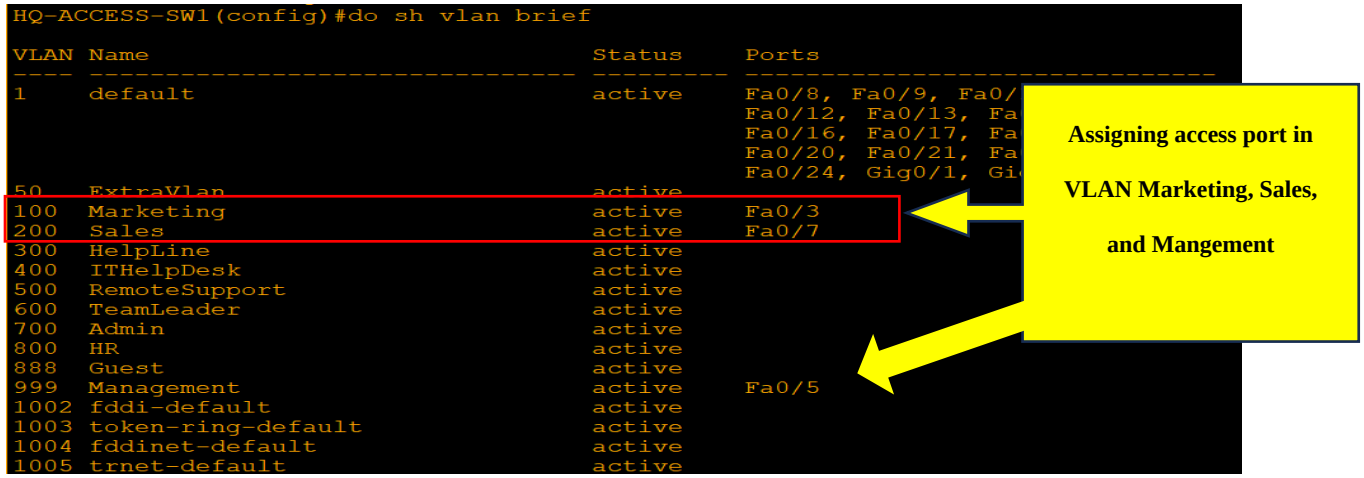


Figure 129-VLAN brief of HQ-ACCESS-SW2

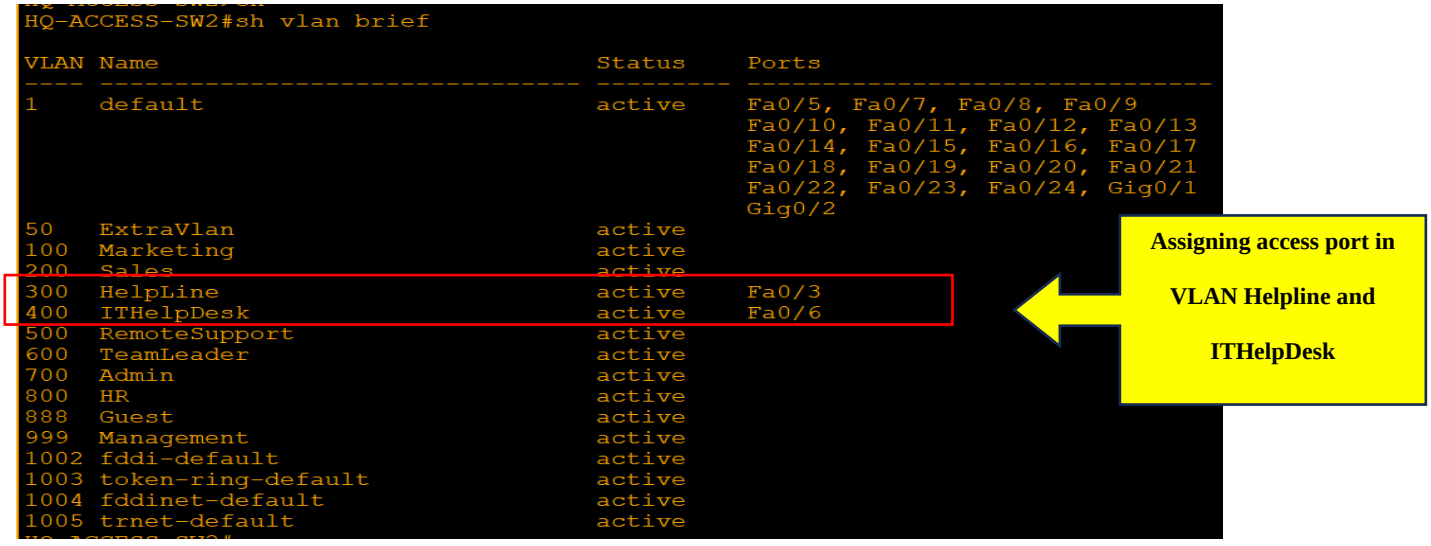


Figure 130-VLAN brief of HQ-ACCESS-SW3

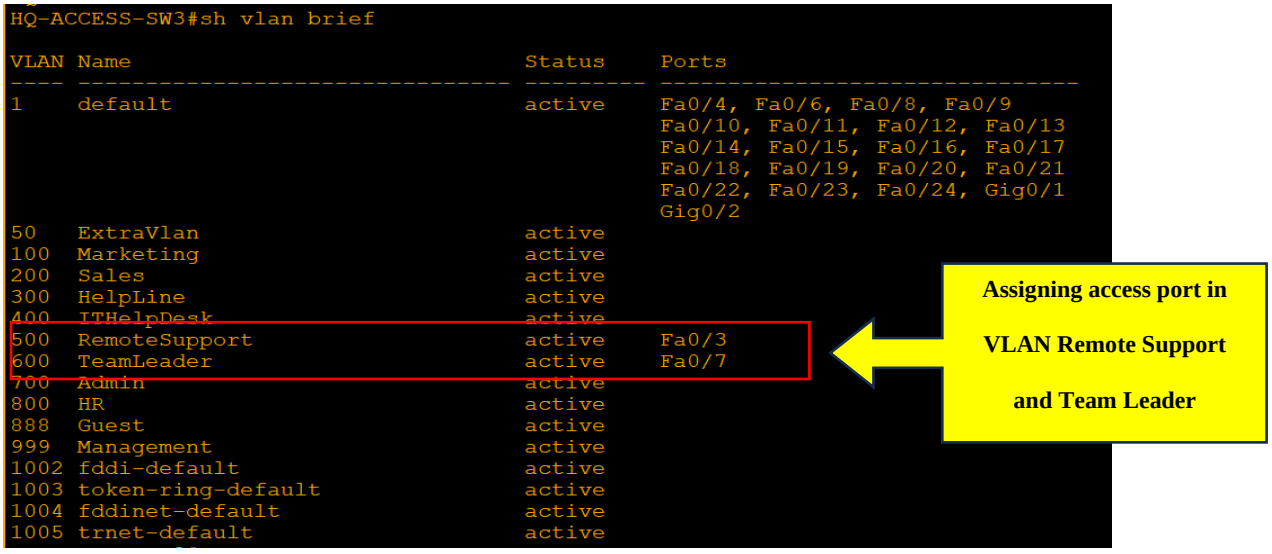
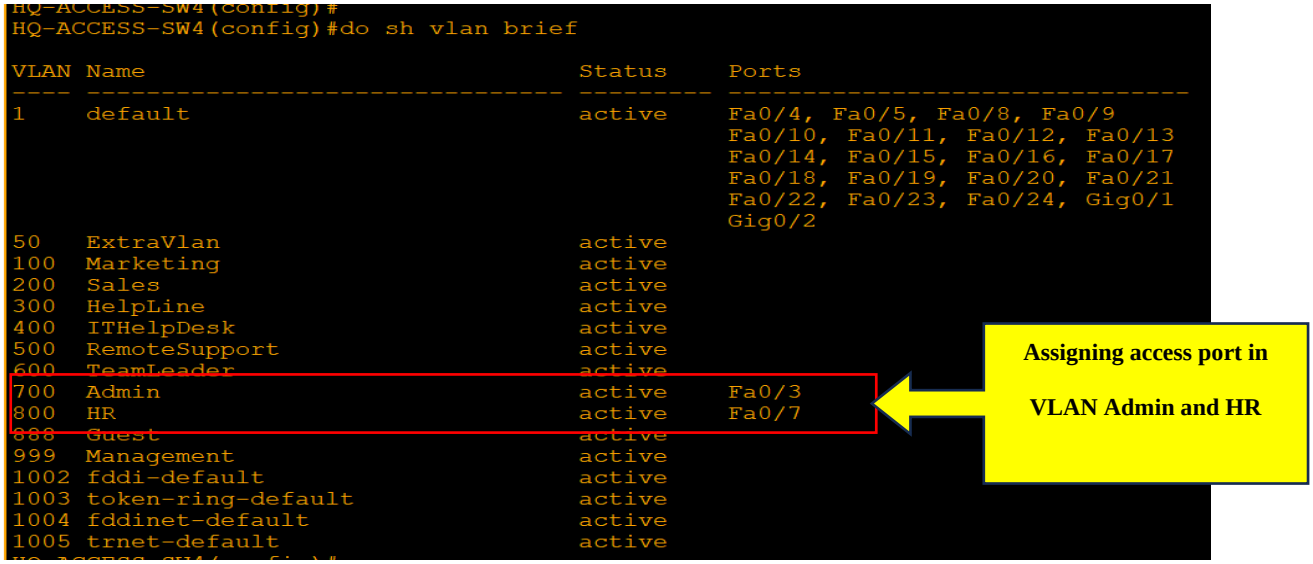


Figure 131-VLAN brief of HQ-ACCESS-S4



BRANCH

Figure 132-Physical diagram of access-layer Branch

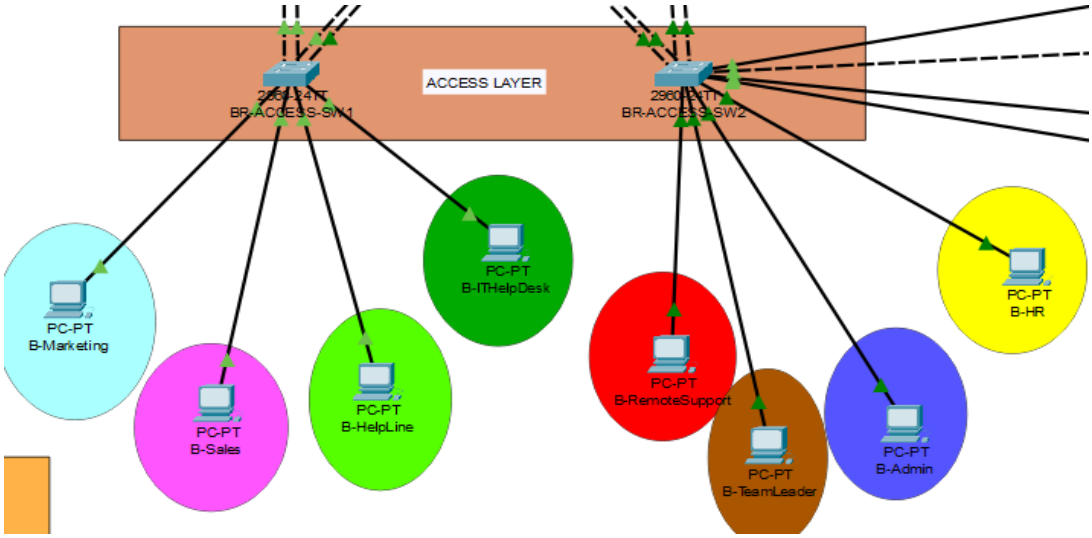


Figure 133-VLAN brief of BR-ACCESS-SW1

```
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

Figure 134-VLAN brief of BR-ACCESS-SW2

```
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
```

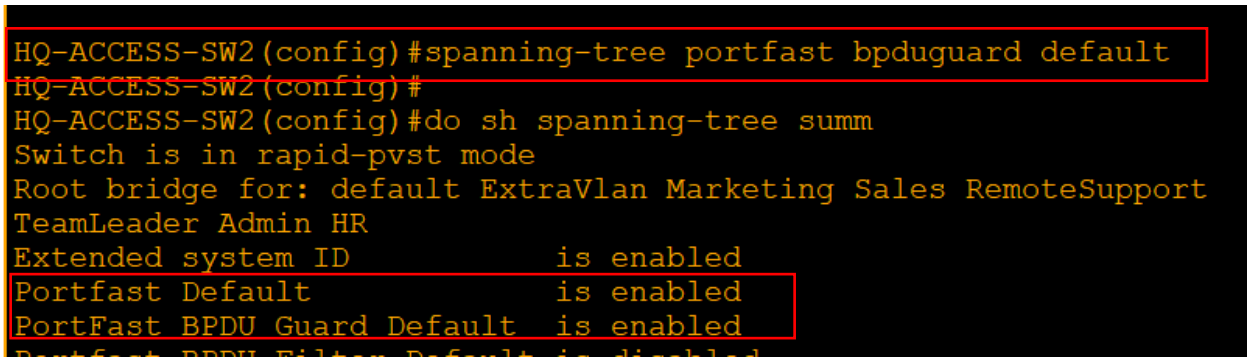
Assigning access port in VLAN Remote Support, Team Leader, Admin, HR, and WLC-management

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.

Figure 135-BPDU guard enable by default in HQ-ACCESS-SW2



HEADQUARTER

HQ-ACCESS-SW1 & HQ-ACCESS-SW2

Figure 136-Enabling BPDU Guard in HQ-ACCESS-SW1 and 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
```

HQ-ACCESS-SW3 & HQ-ACCESS-SW4

Figure 137-Enabling BPDU guard in HQ-ACCESS-SW3 and HQ-ACCESS-SW4

```
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
```

BRANCH

BR-ACCESS-SW1 & BR-ACCESS-SW2

Figure 138-BPDU Guard enabling in BR-ACCESS-SW1 and BR-ACCESS-SW2

```
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
```

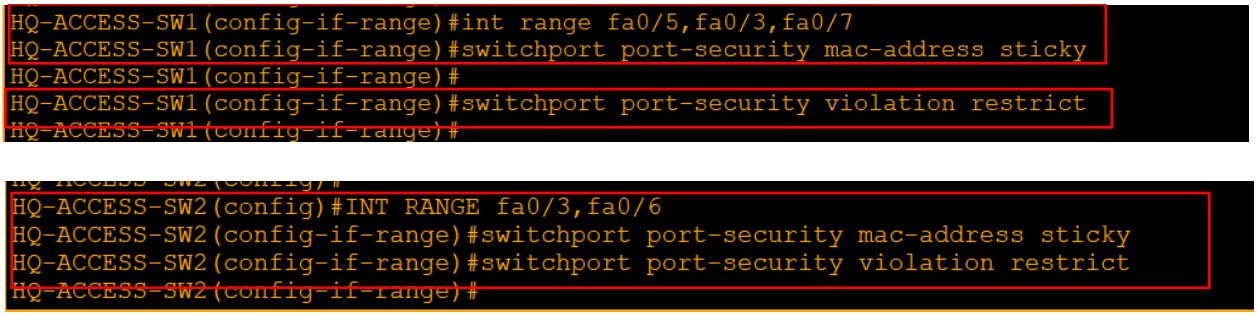
Port security

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 & HQ-ACCESS-SW2

Figure 139-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 & HQ-ACCESS-SW4

Figure 140-Configuration of port security in HQ-ACCESS-SW3 and HQ-ACCESS-SW4

```
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)#
```

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

Figure 141-BR-ACCESS-SW1 & BR-ACCESS-SW2

```
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)#
```

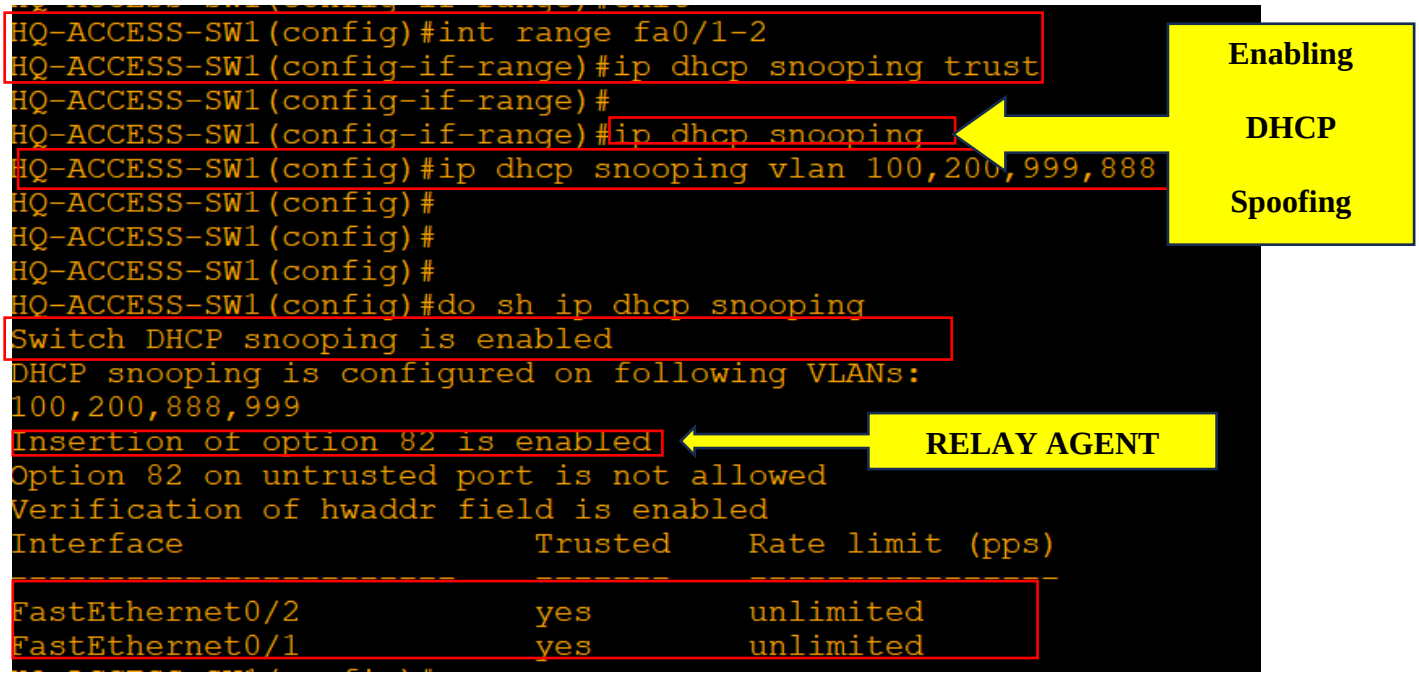
```
BR-ACCESS-SW2(config)#int range fa0/5-8,fa0/11
BR-ACCESS-SW2(config-if-range)#switchpor port-sec mac sticky
BR-ACCESS-SW2(config-if-range)#switchport port-security violation protect
BR-ACCESS-SW2(config-if-range)#
```

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

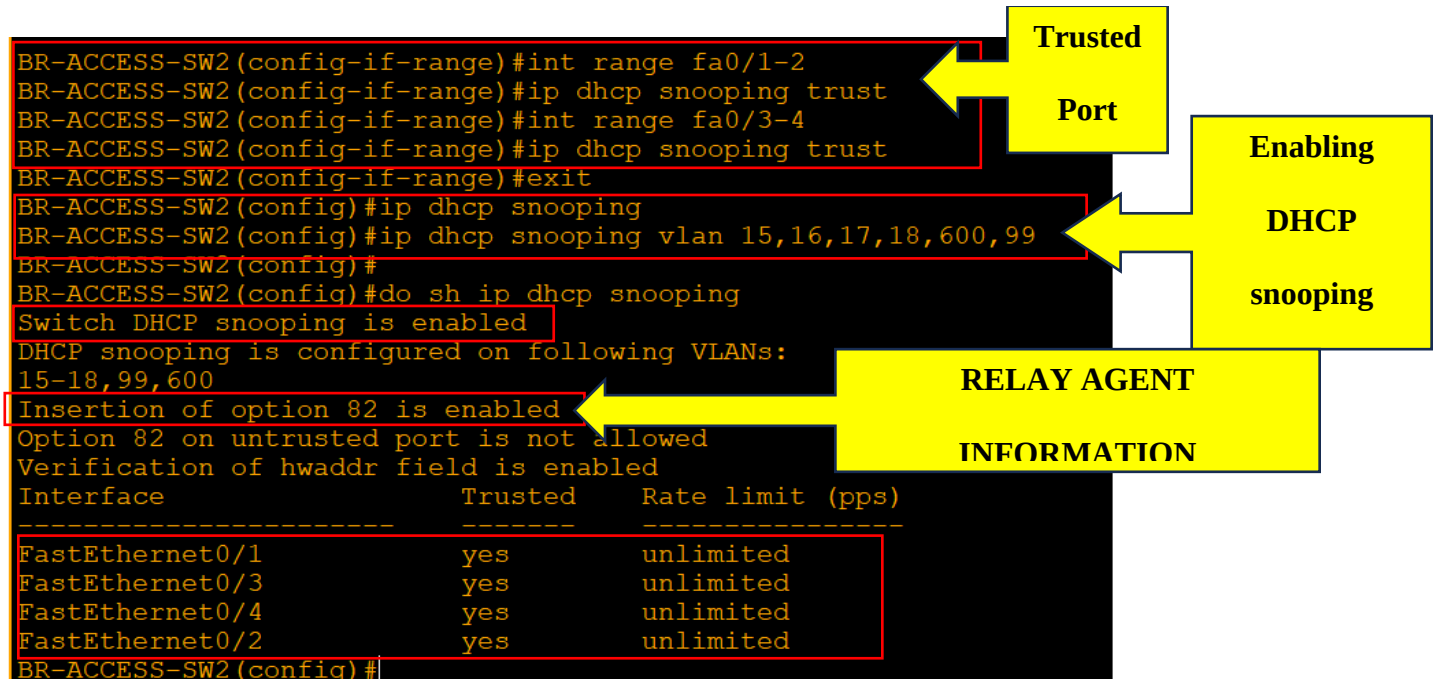
Relying on a DHCP server to provide IP address to end host can indeed offload of workload, but it introduces the risk of potential security threat, especially if a rouge DHCP server is present on the access layer. This unauthorized server might assign an incorrect or malicious IP configuration to end 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

Figure 142-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.

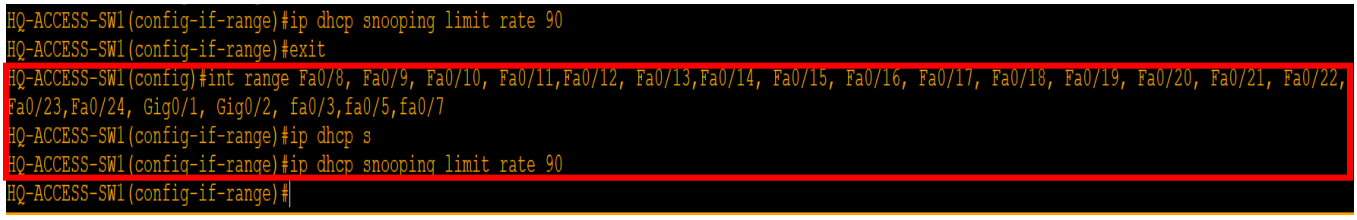
Figure 143-Configuration of DHCP snooping in Branch access-layer switch



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 144-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.

Figure 145-Configuration of DAI in Headquarter switch

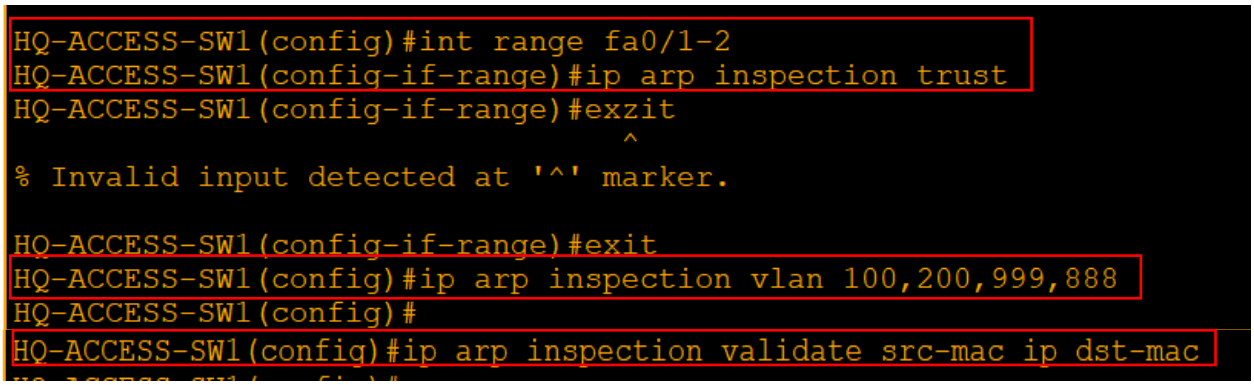


Figure 146-DHCP snooping binding table

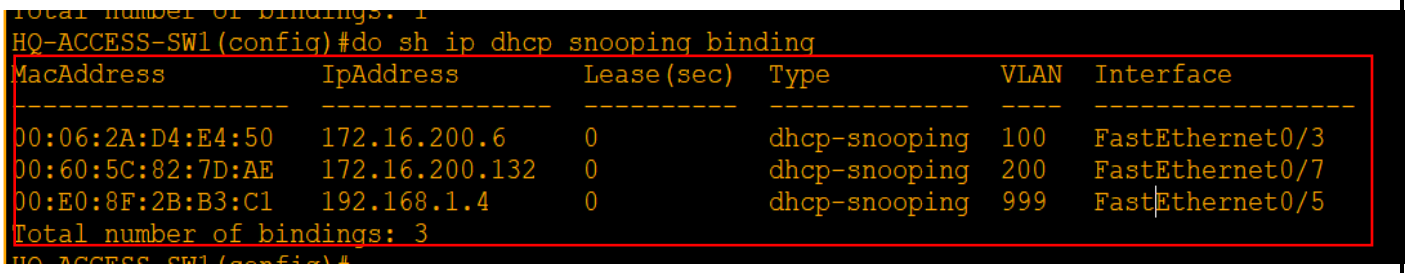
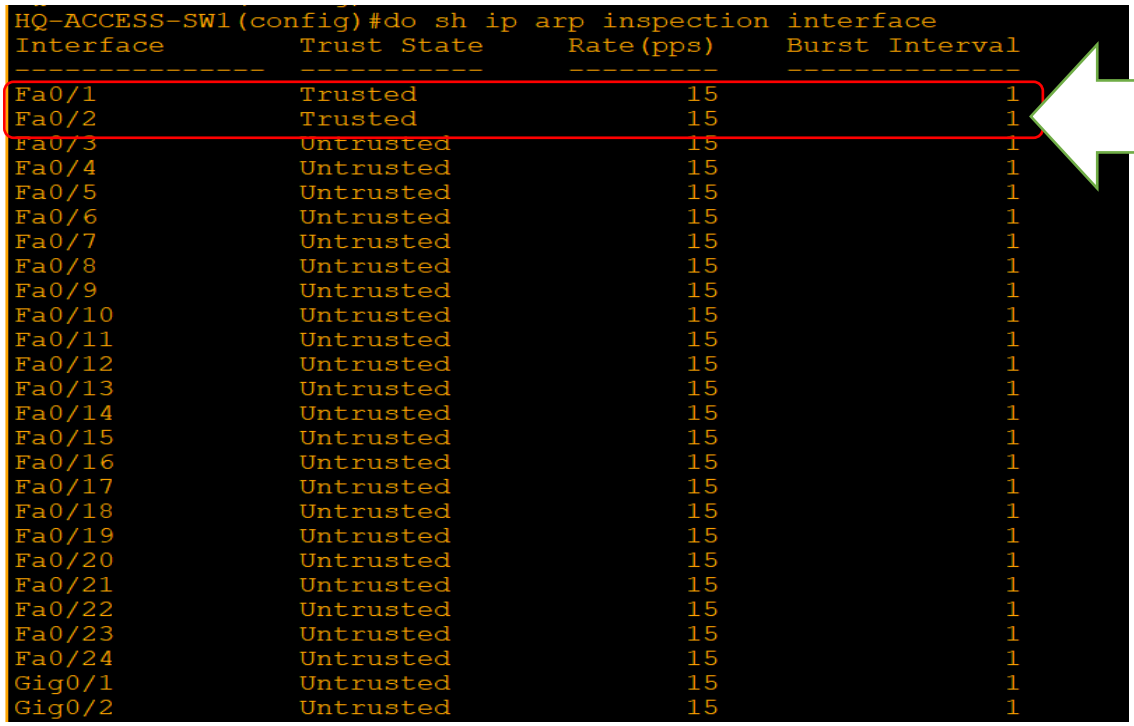


Figure 147-ARP inspection table of interface



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 148-PAT in HQ-EDGE-R1 & HQ-EDGE-R2

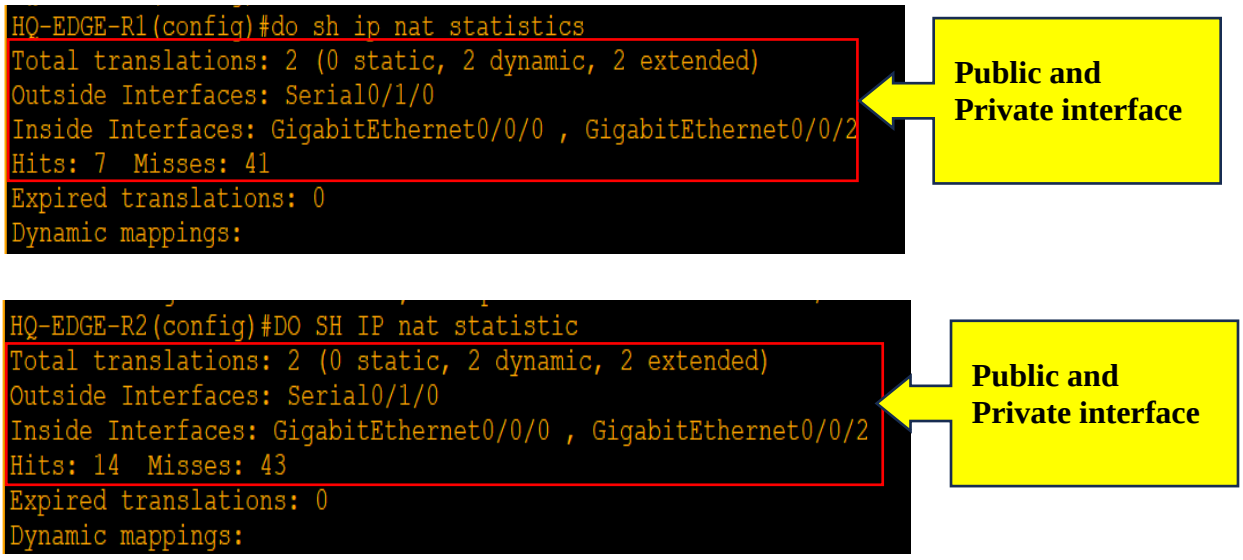
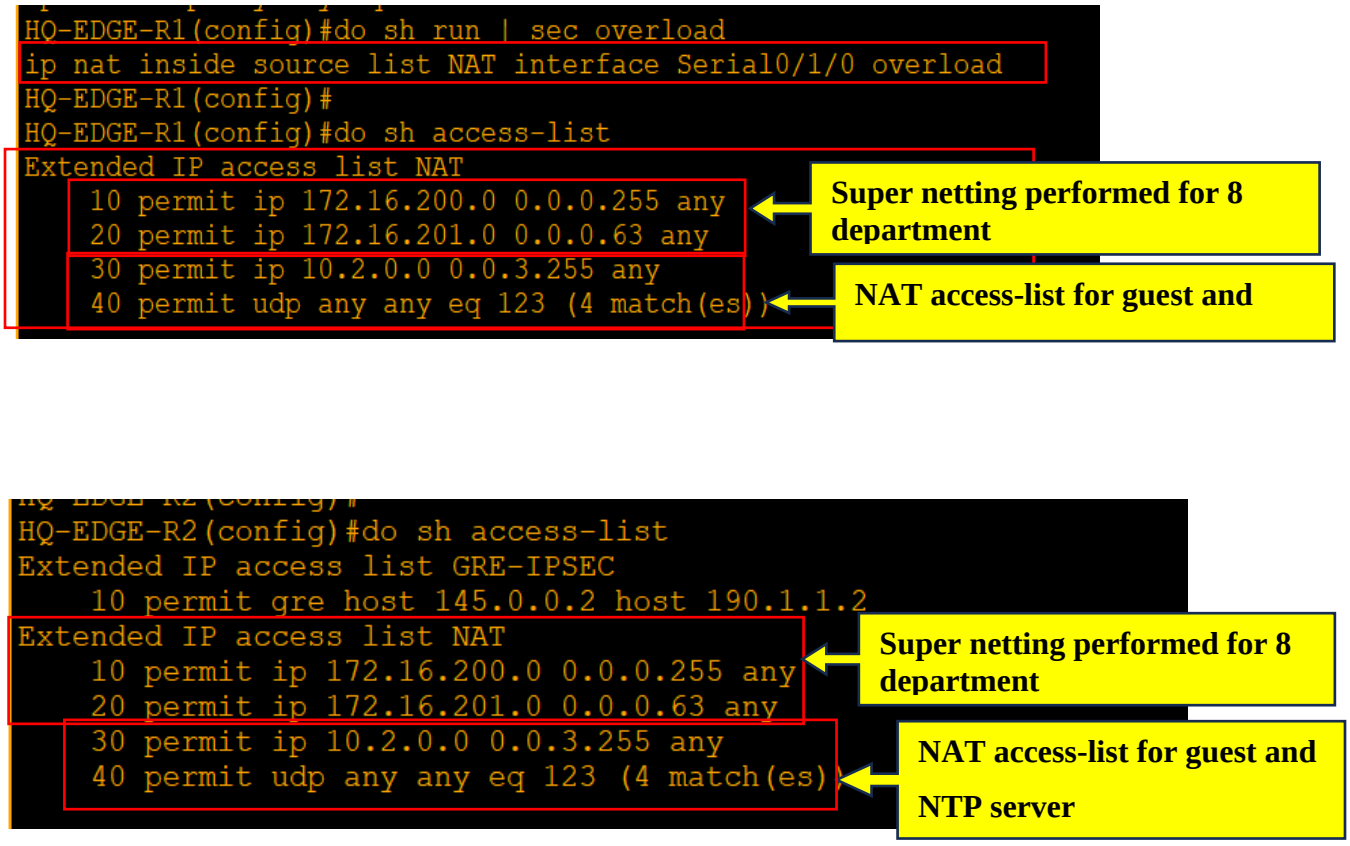


Figure 149-PAT applied in outside interface with access-list



BRANCH

Figure 150-PAT in BR-EDGE-R1 & BR-EDGE-R2

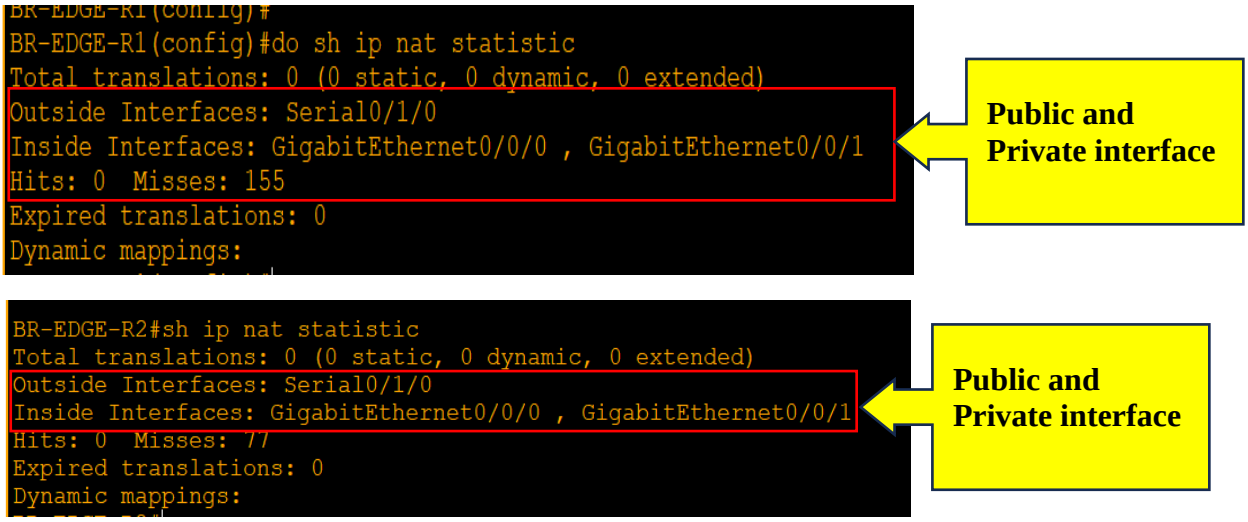
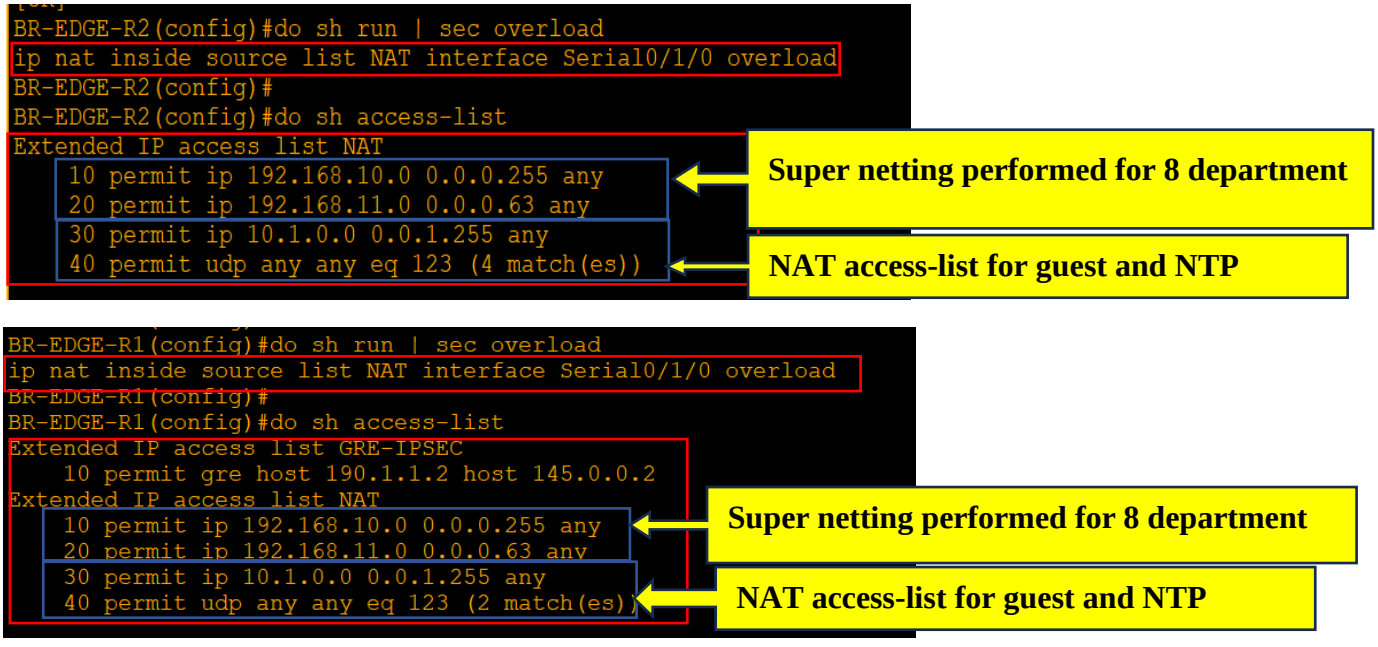


Figure 151-PAT applied on outside interface and access-list



NAT verification

Figure 152-Successful ping from Headquarter marketing department to Google

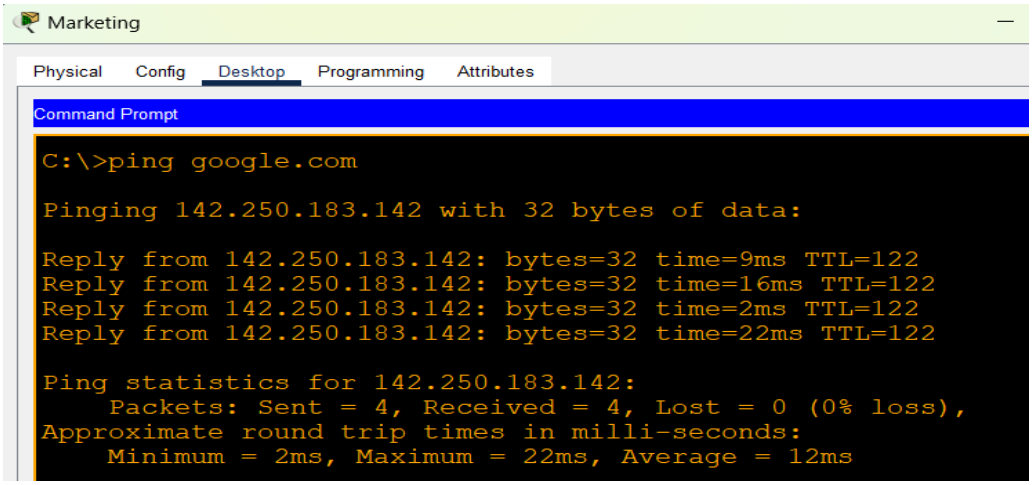
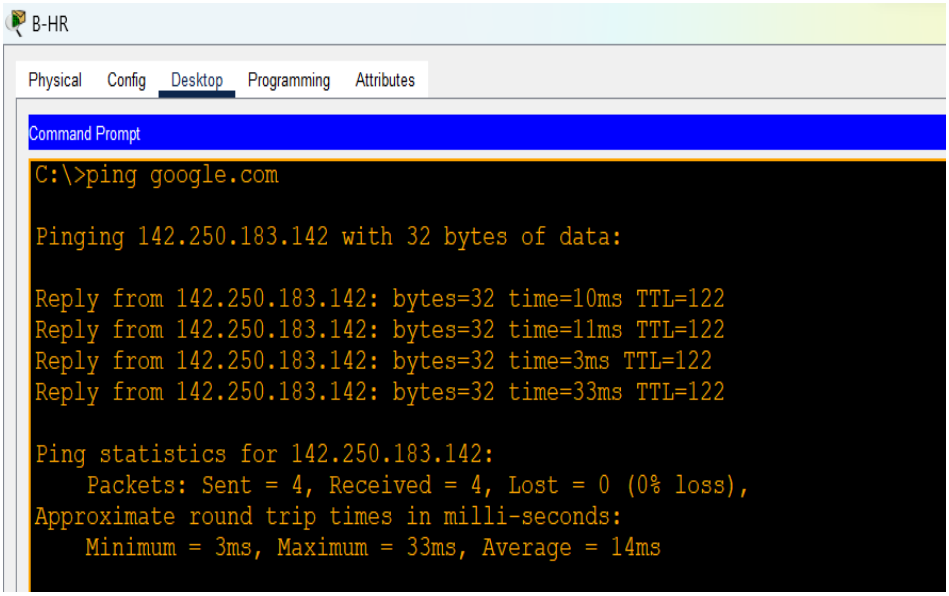


Figure 153-Successful ping from branch HR department to Google **Figure**



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 a 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.

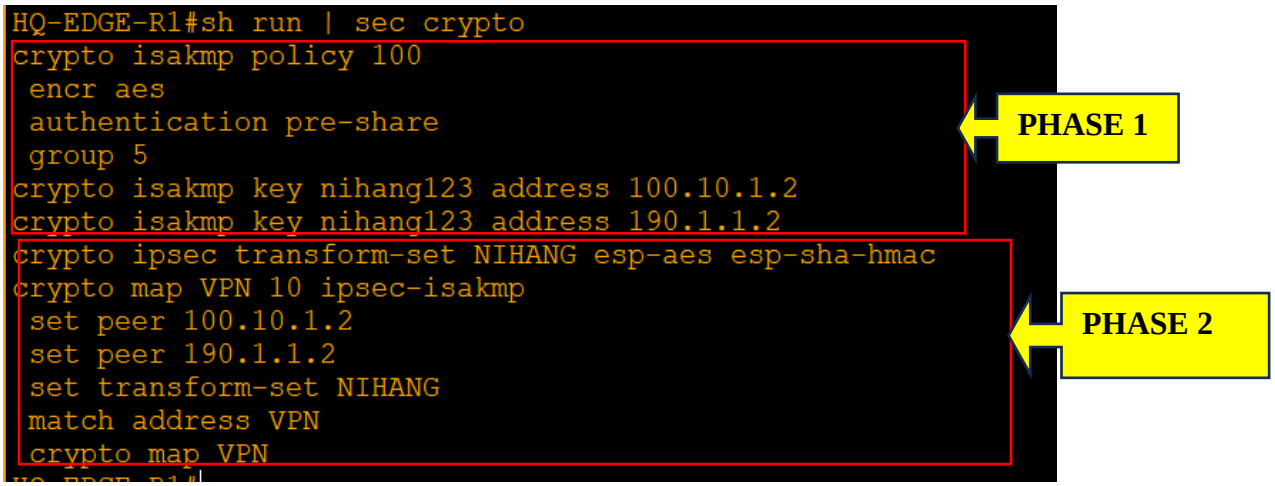
In this project I have implemented an IPsec site-to-site VPN inside edge router in cisco packet tracer.

IPsec have two phases:

1. 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

2. Phase 2 called IPsec.
   - Creating a transform set
   - Creating a crypto map and mapping all the argument inside it
   -

Figure 154-Configuration of IPsec VPN and access-list in HQ-EDGE-R1



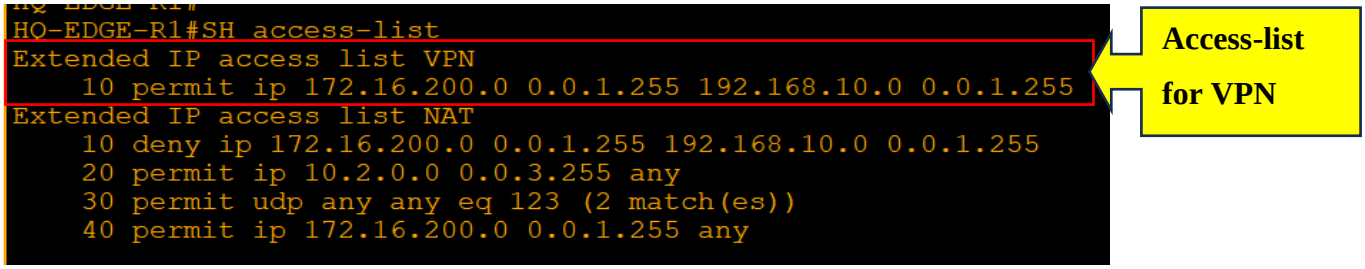


Figure 155-Configuration of IPsec VPN and access-list in HQ-EDGE-R2

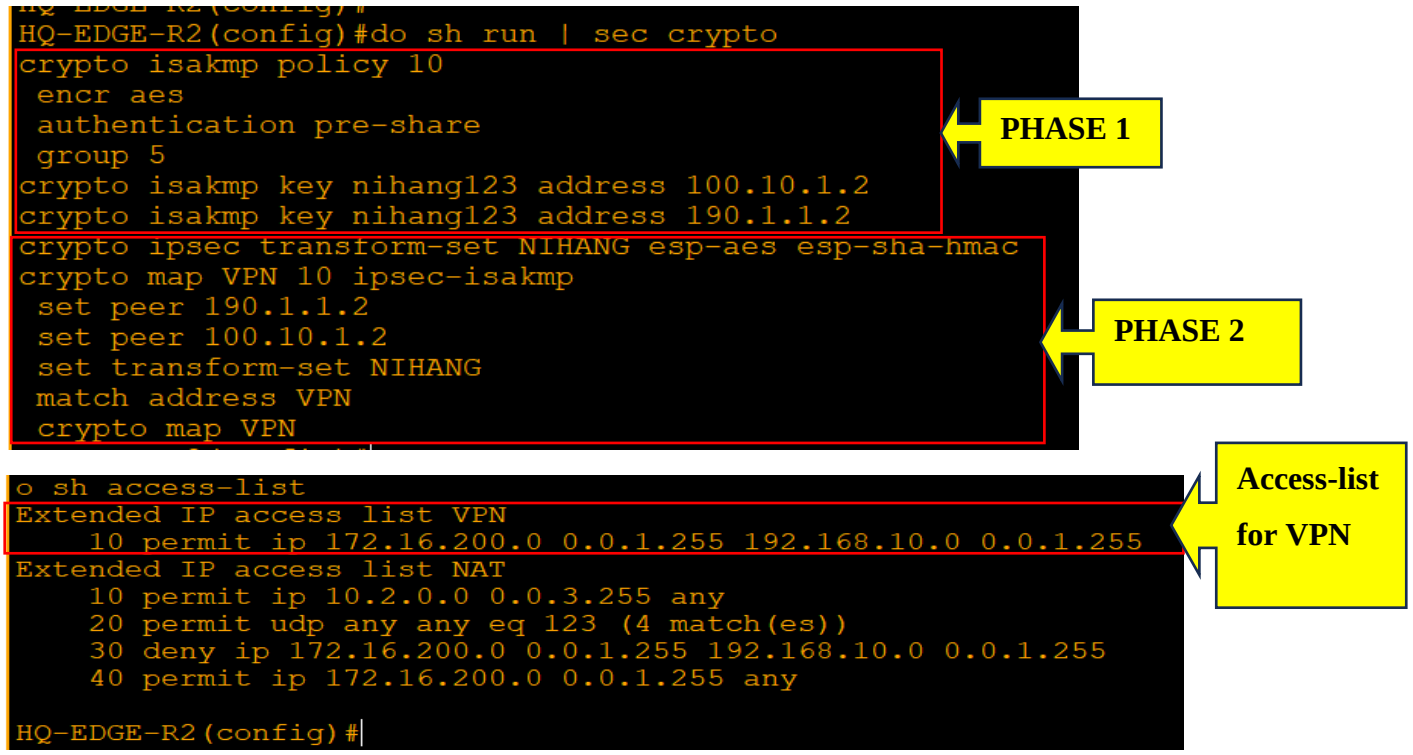
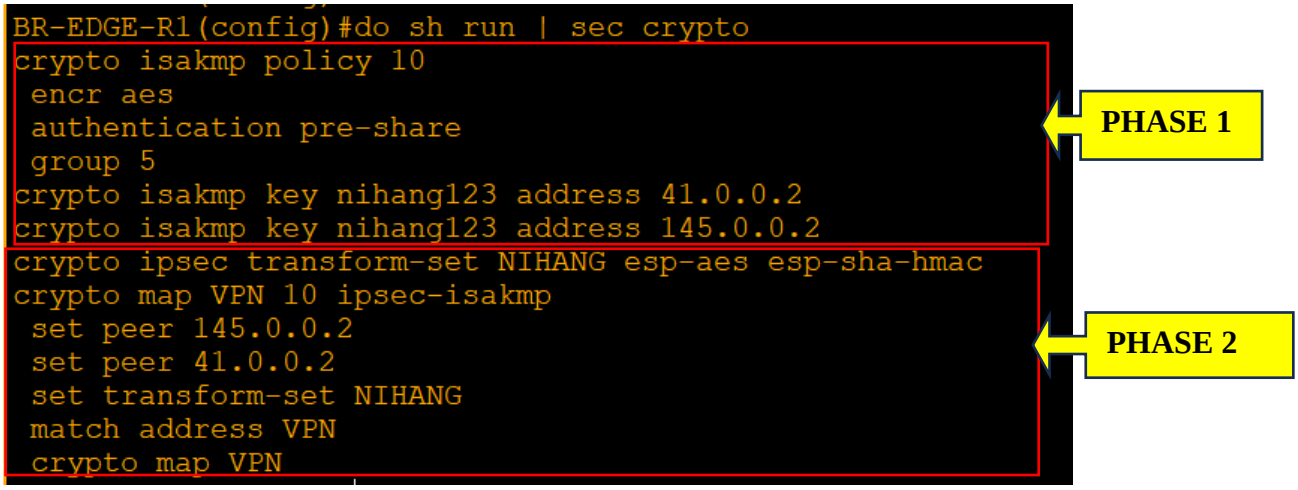


Figure 156-Configuration IPsec VPN and access-list in BR-EDGE-R1



```
BR-EDGE-R1(config)#do sh access-list
Extended IP access list VPN
    10 permit ip 192.168.10.0 0.0.1.255 172.16.200.0 0.0.1.255
Extended IP access list NAT
    10 permit ip 10.1.0.0 0.0.1.255 any
    20 deny ip 192.168.10.0 0.0.1.255 172.16.200.0 0.0.1.255
    30 permit ip 192.168.10.0 0.0.1.255 any
```

Access-list for VPN

Figure 157-Configuration of IPsec VPN in BR-EDGE-R2 and access-list

```
BR-EDGE-R2#sh run | sec crypto
crypto isakmp policy 100
 encr aes
 authentication pre-share
 group 5
crypto isakmp key nihang123 address 41.0.0.2
crypto isakmp key nihang123 address 145.0.0.2
crypto ipsec transform-set NIHANG esp-aes esp-sha-hmac
crypto map VPN 10 ipsec-isakmp
 set peer 41.0.0.2
 set peer 145.0.0.2
 set transform-set NIHANG
 match address VPN
 crypto map VPN
```

PHASE 1

PHASE 2

```
BR-EDGE-R2#sh access-list
Extended IP access list VPN
    10 permit ip 192.168.10.0 0.0.1.255 172.16.200.0 0.0.1.255
Extended IP access list NAT
    10 deny ip 192.168.10.0 0.0.1.255 172.16.200.0 0.0.1.255
    20 permit ip 192.168.10.0 0.0.1.255 any
    30 permit ip 10.1.0.0 0.0.1.255 any
```

Access-list for VPN

Verification through IPsec site-to-site VPN

From HQ to Branch

Figure 158-Ping from HQ admin department to Branch Marketing

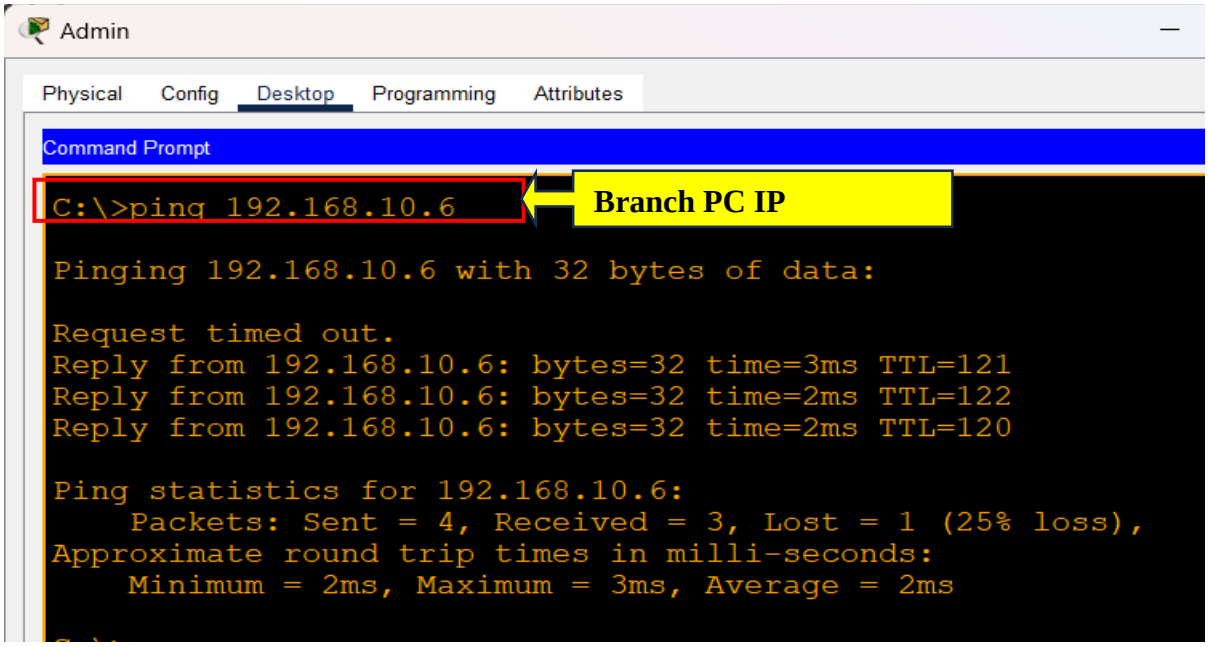
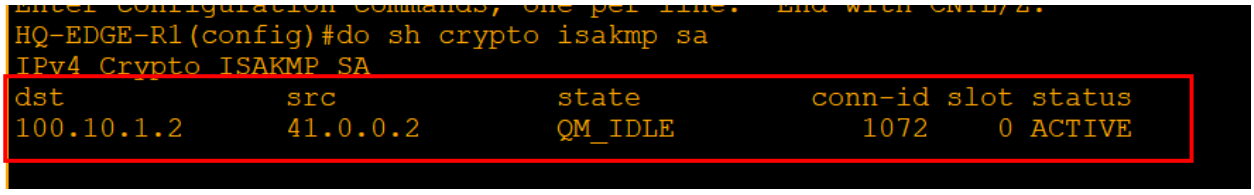


Figure 159-Successful ISAKMP tunnel formation between headquarter and branch



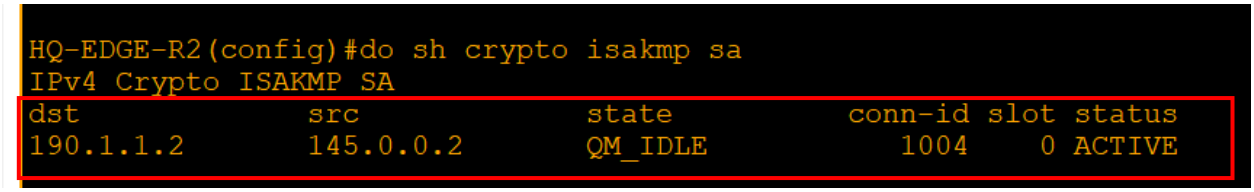


Figure 160-Encryption, encapsulation, decryption, and encapsulation by IPsec in HQ edge router

```
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
```

From Branch to HQ

Figure 161-Ping from branch marketing department to headquarter admin department

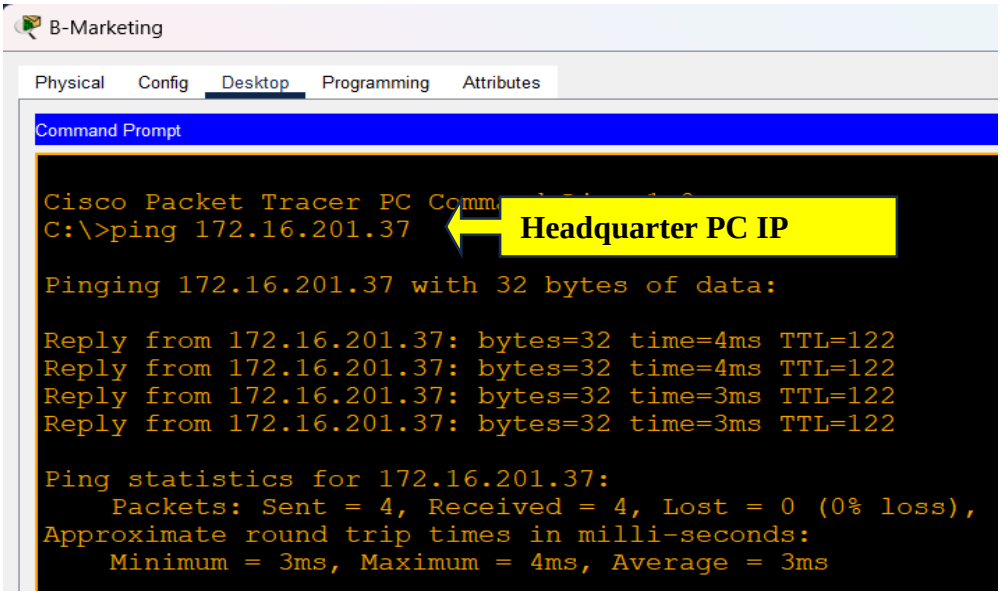
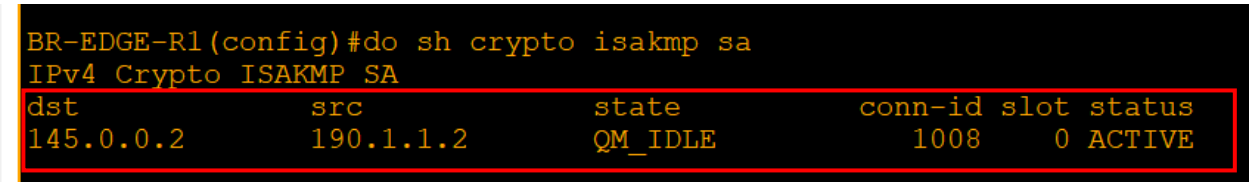


Figure 162-Successful ISAKMP tunnel creation in Branch edge router



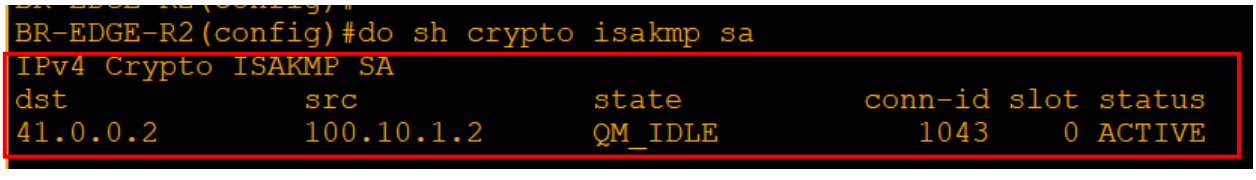


Figure 163-Encryption, decryption, encapsulation, and decapsulation through IPsec in Branch edge router

```
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
```

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

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

Figure 164-Physical diagram in GNS3

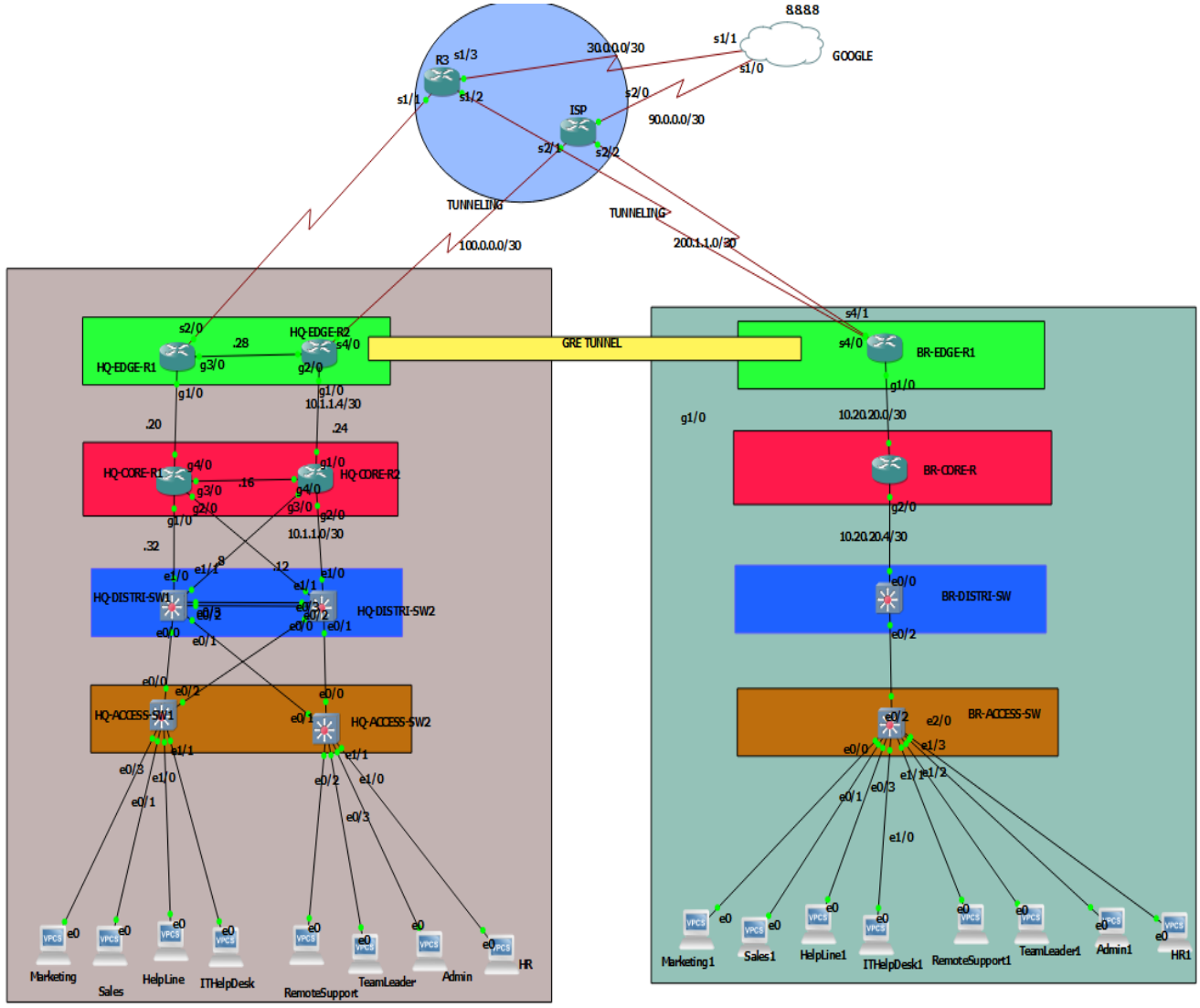


Figure 165-Running config of IPsec in HQ-EDGE-R2

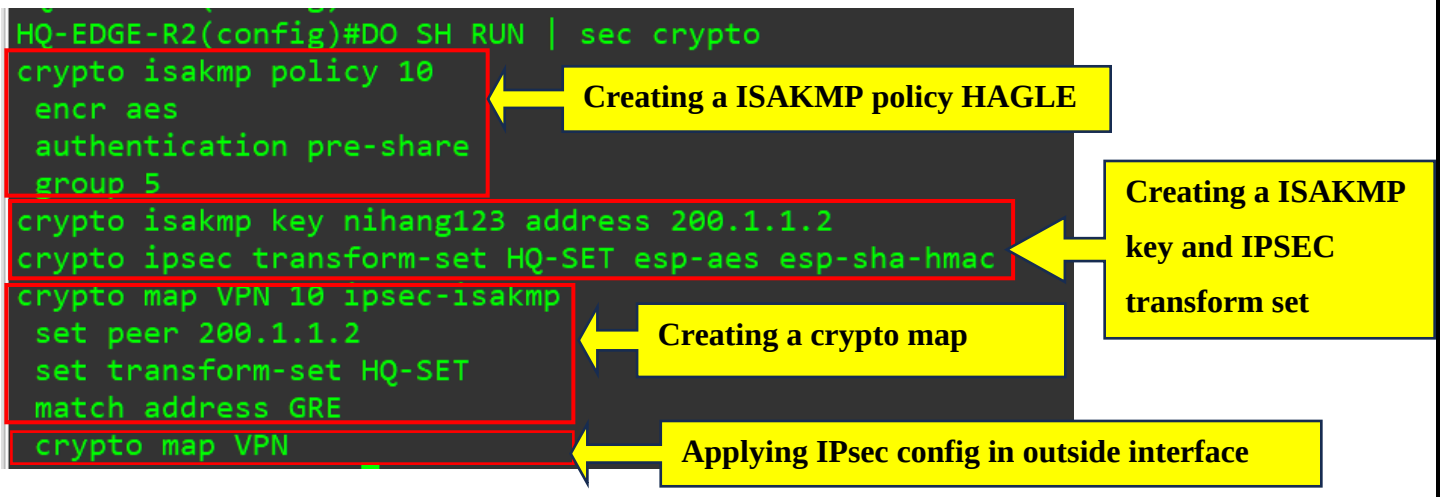


Figure 166-Access-list of GRE tunnel information and NAT

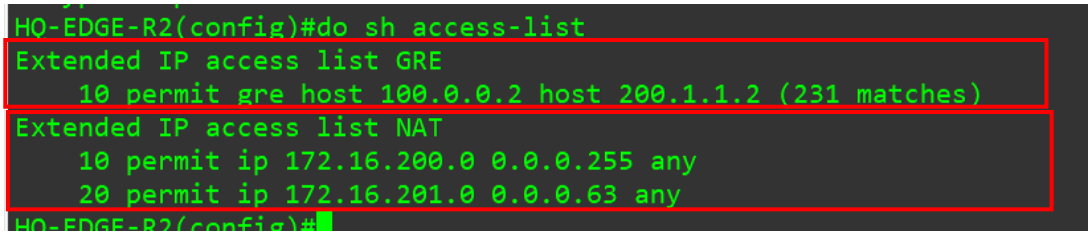


Figure 167-Running config of creating GRE Tunnel0

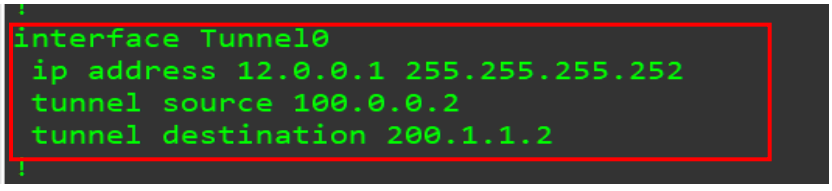
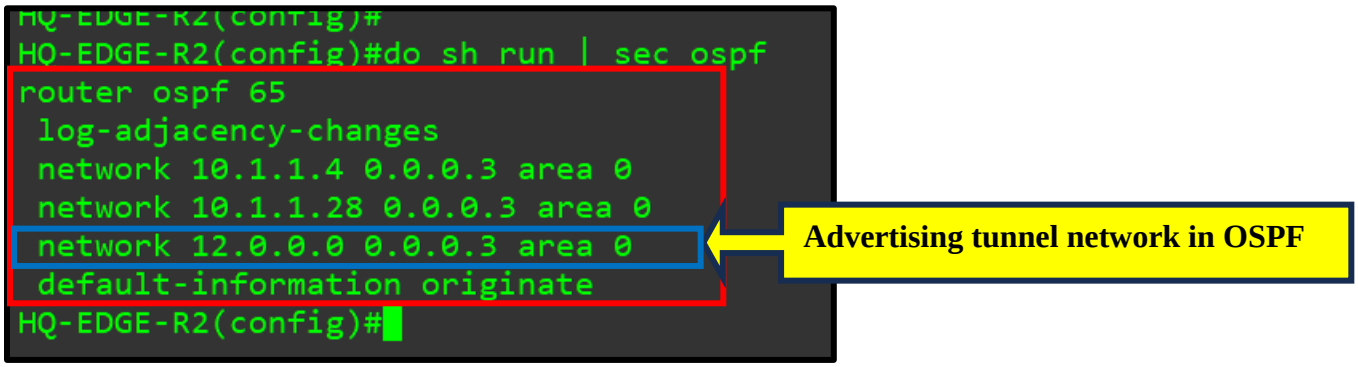
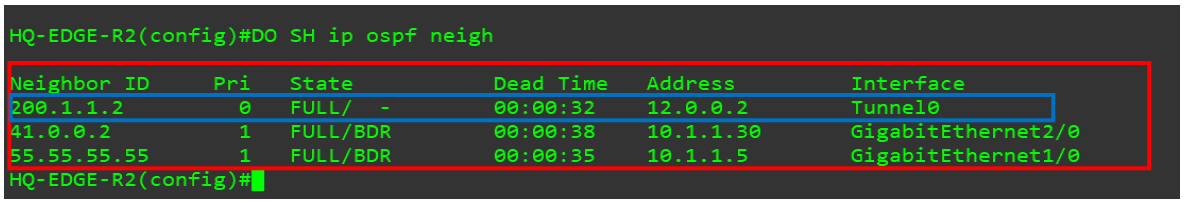


Figure 168-OSPF configuration and OSPF neighborship of HQ-EDGE-R2





BRANCH

Figure 169-Running config of IPsec BR-EDGE-R

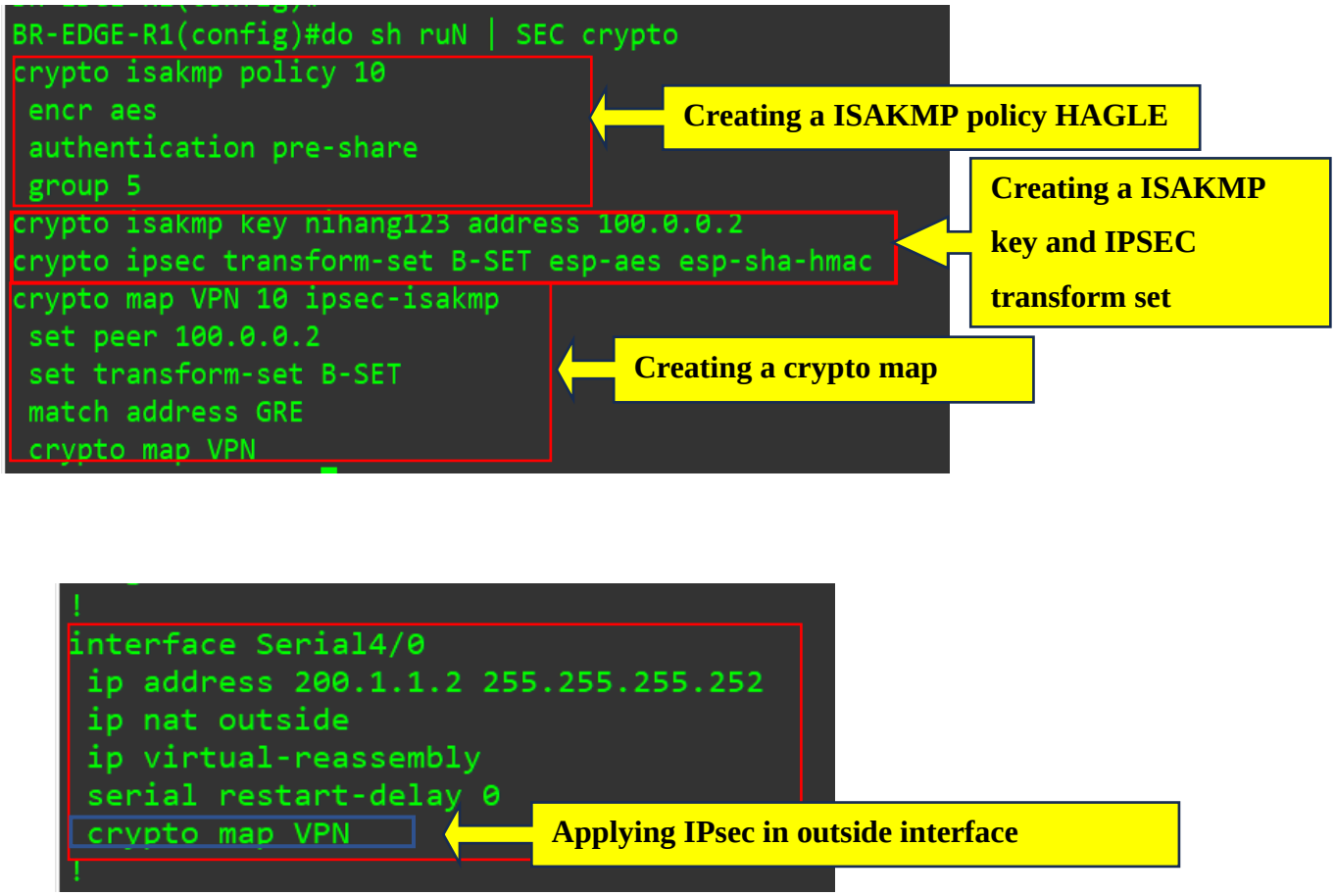


Figure 170-Access-list of GRE tunnel and NAT

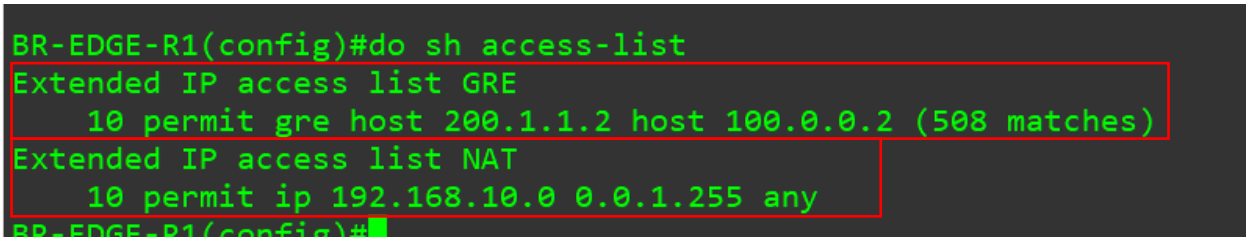


Figure 171-Running configuration of creating tunnel 0

```
!
interface Tunnel0
 ip address 12.0.0.2 255.255.255.252
 tunnel source 200.1.1.2
 tunnel destination 100.0.0.2
!
```

Figure 172-OSPF configuration and OSPF neighborship of BR-EDGE-R1

```
BR-EDGE-R1(config)#do sh run | sec ospf
router ospf 65
 log-adjacency-changes
 network 10.20.20.0 0.0.0.3 area 0
 network 12.0.0.0 0.0.0.3 area 0
 default-information originate
```

Advertising tunnel network in OSPF

```
BR-EDGE-R1(config)#DO SH ip ospf neigh

Neighbor ID     Pri   State           Dead Time   Address         Interface
100.0.0.2         0   FULL/  -        00:00:37    12.0.0.1        Tunnel0
10.20.20.5        1   FULL/BDR        00:00:34    10.20.20.2      GigabitEthernet1/0
BR-EDGE-R1(config)#
```

Figure 173-Successful secure tunnel creation in HQ-EDGE-R2

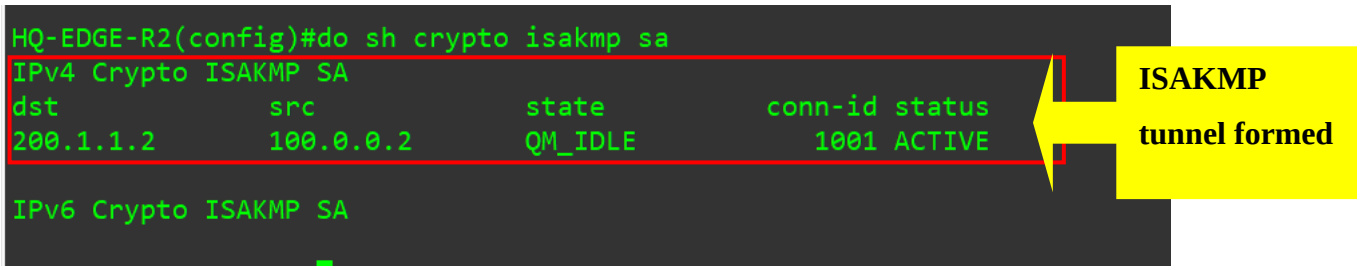
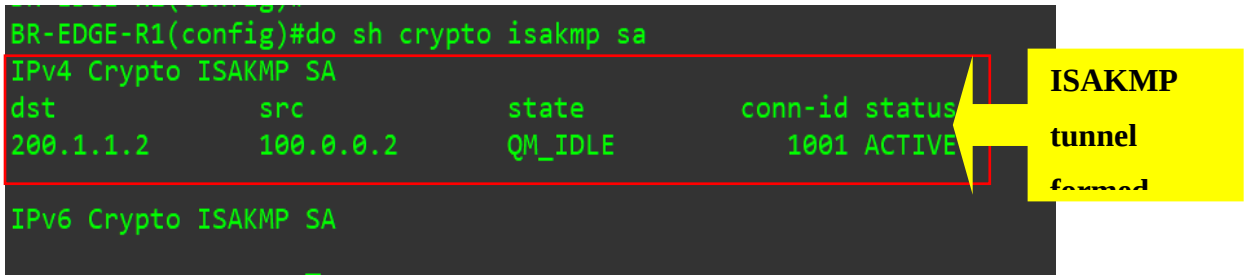


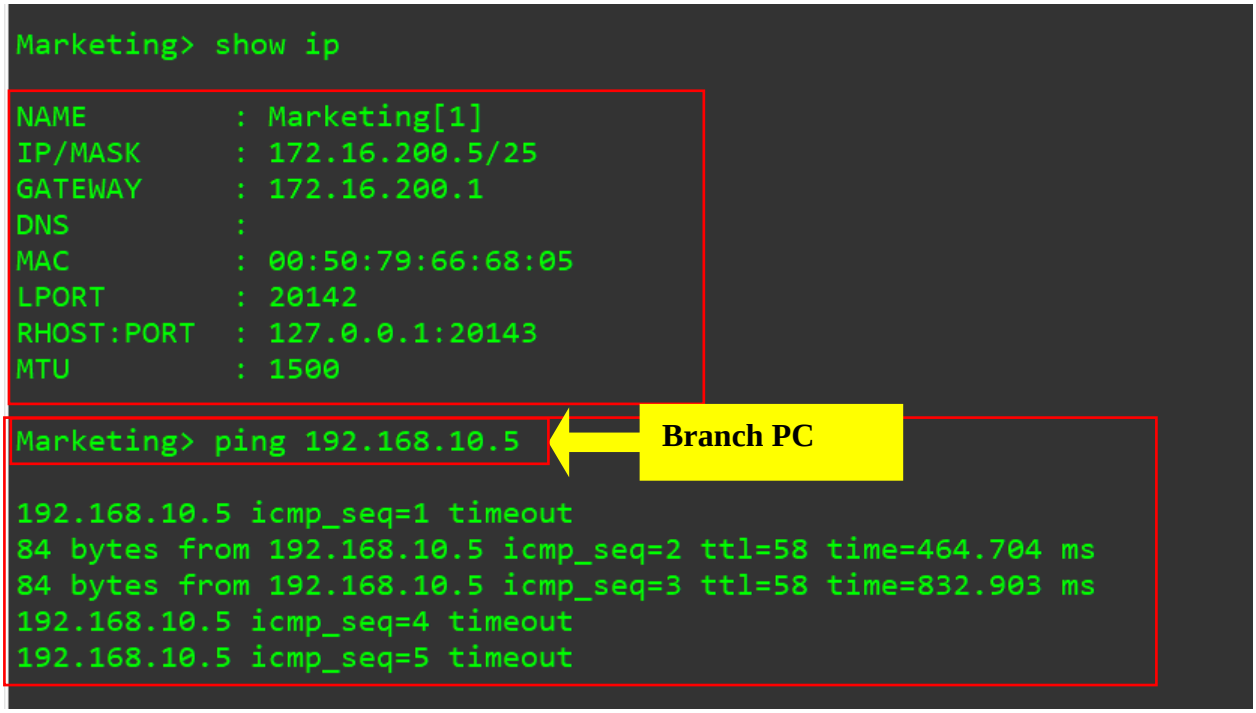
Figure 174-Successful secure tunnel creation in BR-EDGE-R1



GRE over IPsec VPN Verification

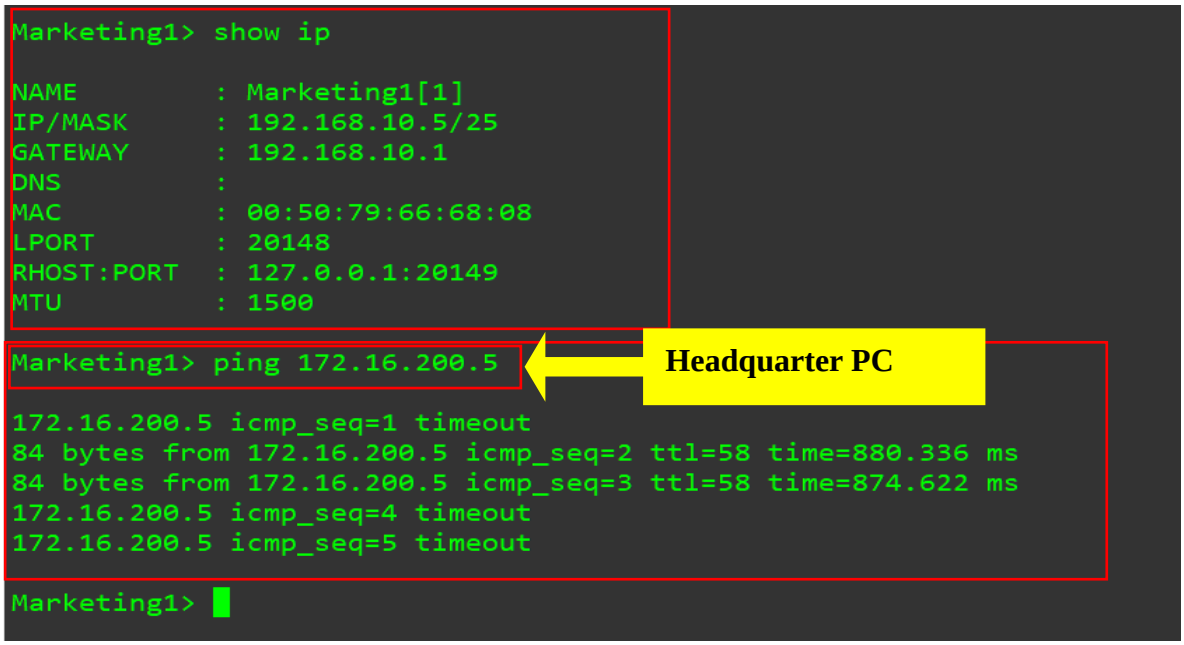
From Headquarter to Branch

Figure 175-Pinging from Headquarter marketing to branch marketing department



From branch to headquarter

Figure 176-Pinging from branch marketing to headquarter marketing department



DHCP from HQ to Branch

Figure 177-DHCP running Config of branch sales department in headquarter

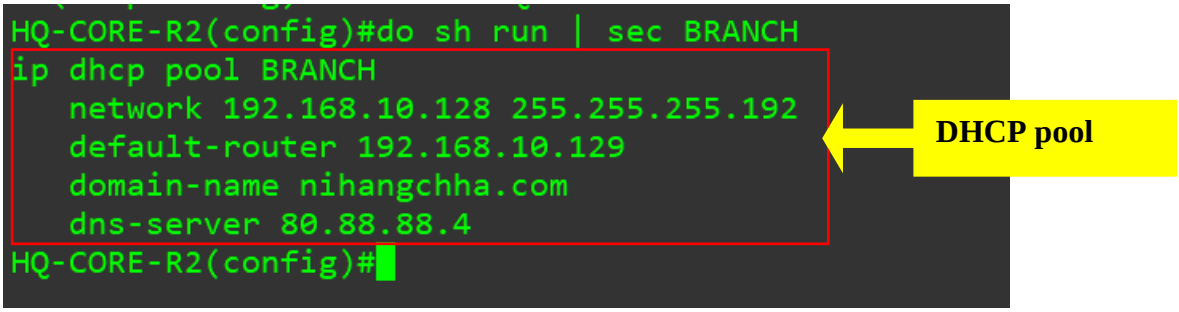


Figure 178-Using loopback address for DHCP server in HQ-CORE-R2

```
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 179-Running config of sales SVI in branch and relay agent in BR-DISTRI-SW

```
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 180-IP obtained from headquarter DHCP server

```
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 181-Encryption of GRE packet by IPsec in HQ-EDGE-R2

```
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): (200.1.1.2/255.255.255.255/47/0)
   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,

Figure 182-GRE encrypted by IPsec protocol in BR-EDGE-R1

```
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,

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 183-WLC and APS with different end PC and wireless device

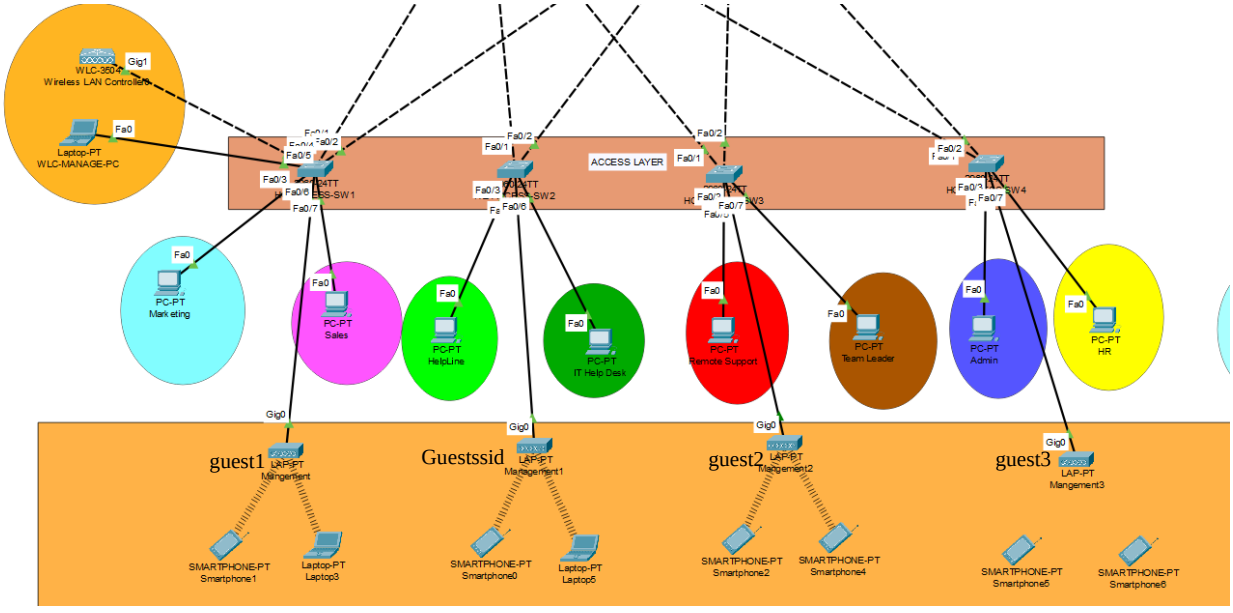


Figure 184-Assigning IP address to WLC in management VLAN

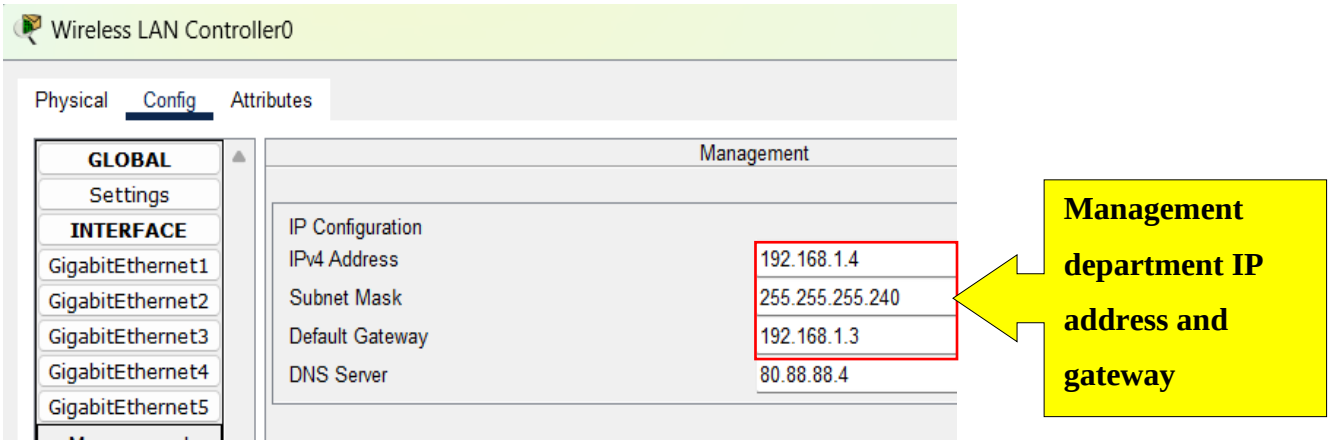


Figure 185-DHCP server guest VLAN configuration

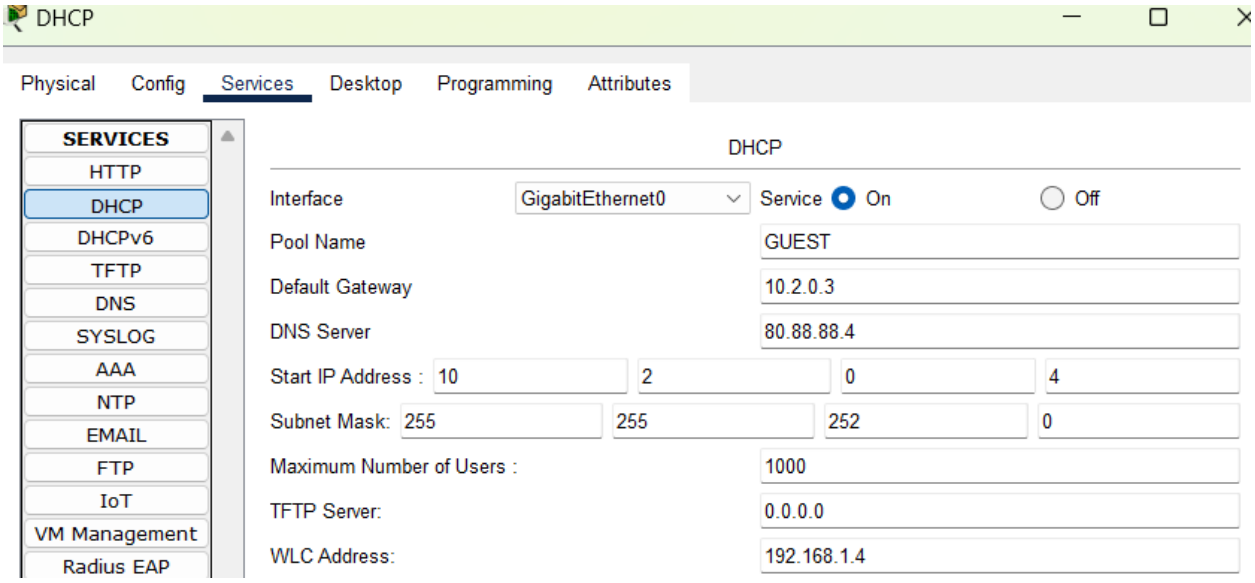


Figure 186-Configuring WLC from PC using web browser

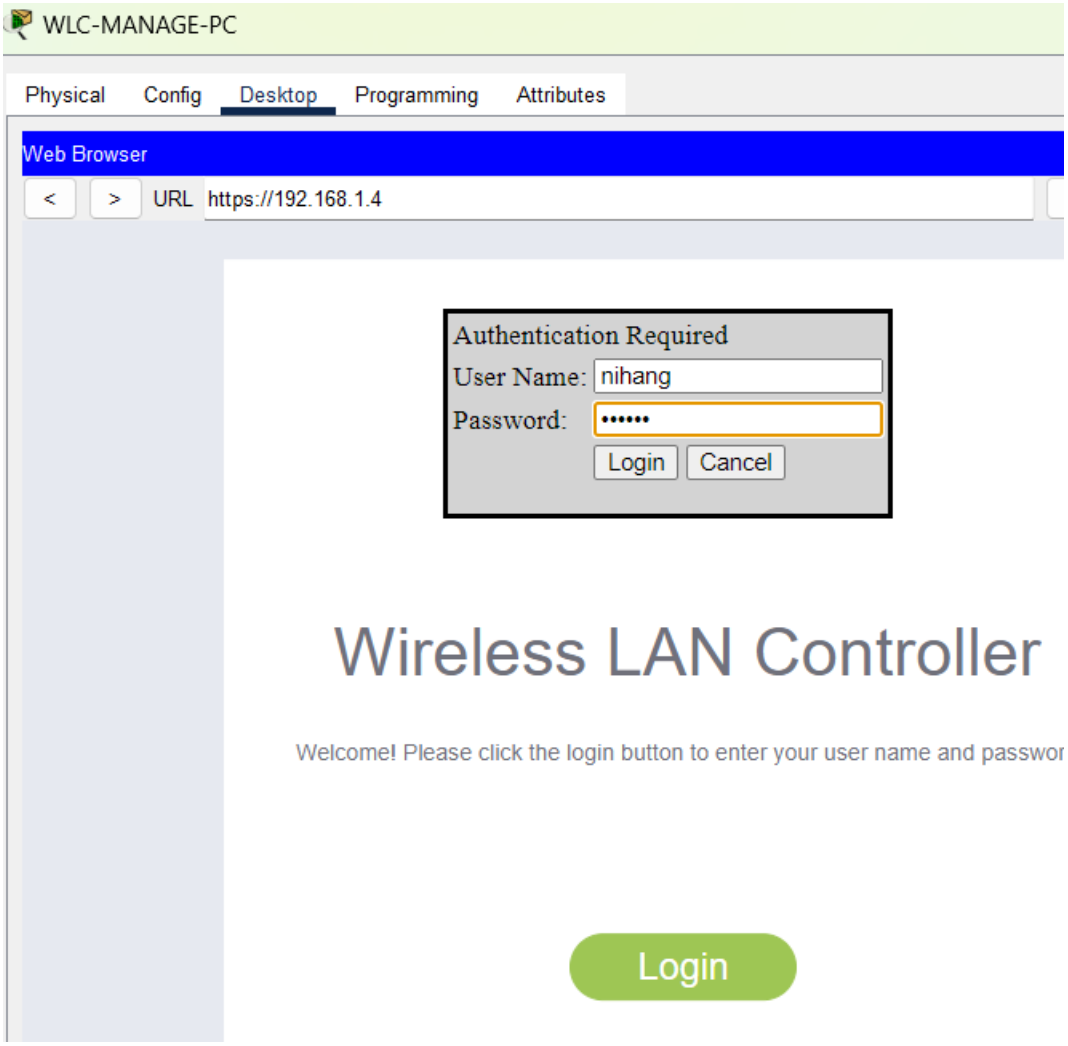


Figure 187-Creating a Guest-Handler interface

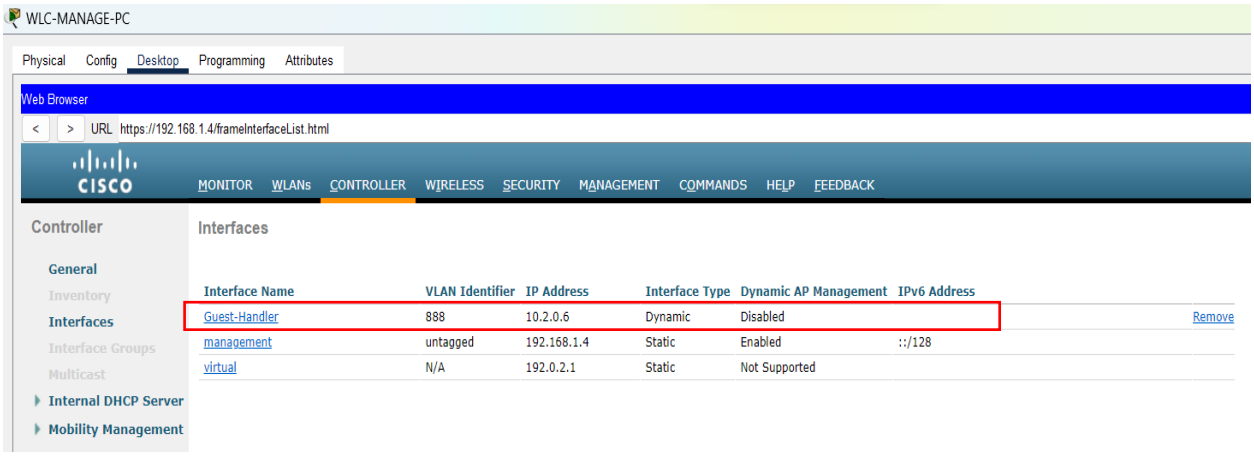


Figure 188-Interface information

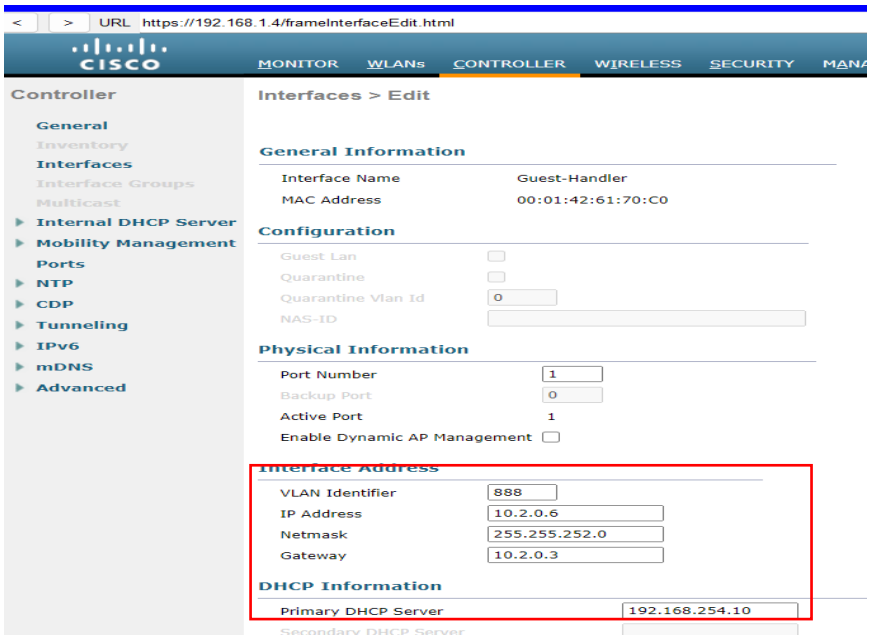


Figure 189 WLANs in WLC

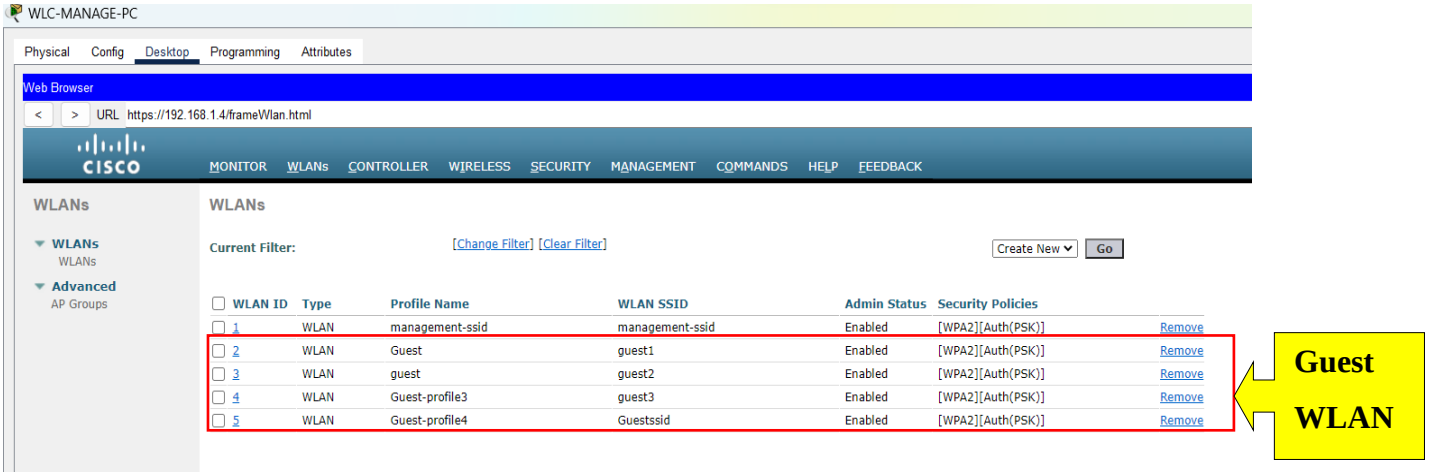


Figure 190-Create a WLAN as required and inside it add guest interface, SSID name, Profile Name

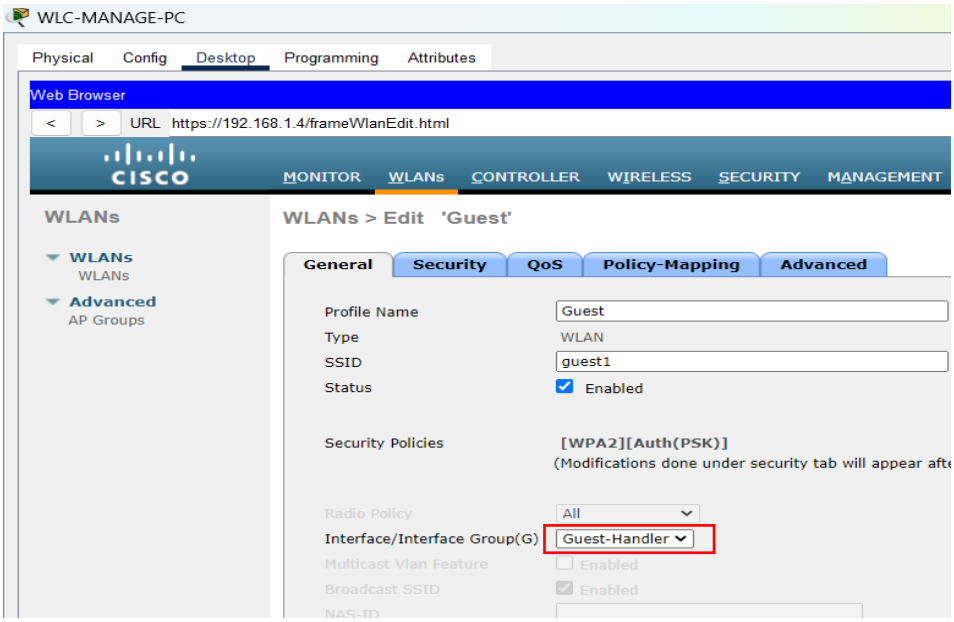


Figure 191Security tab inside of WLAN

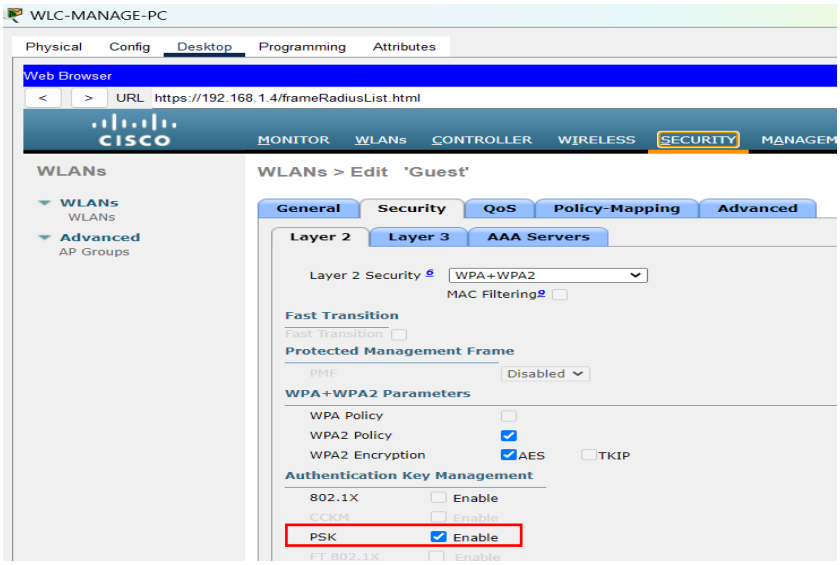


Figure 192-AP groups in WLANs

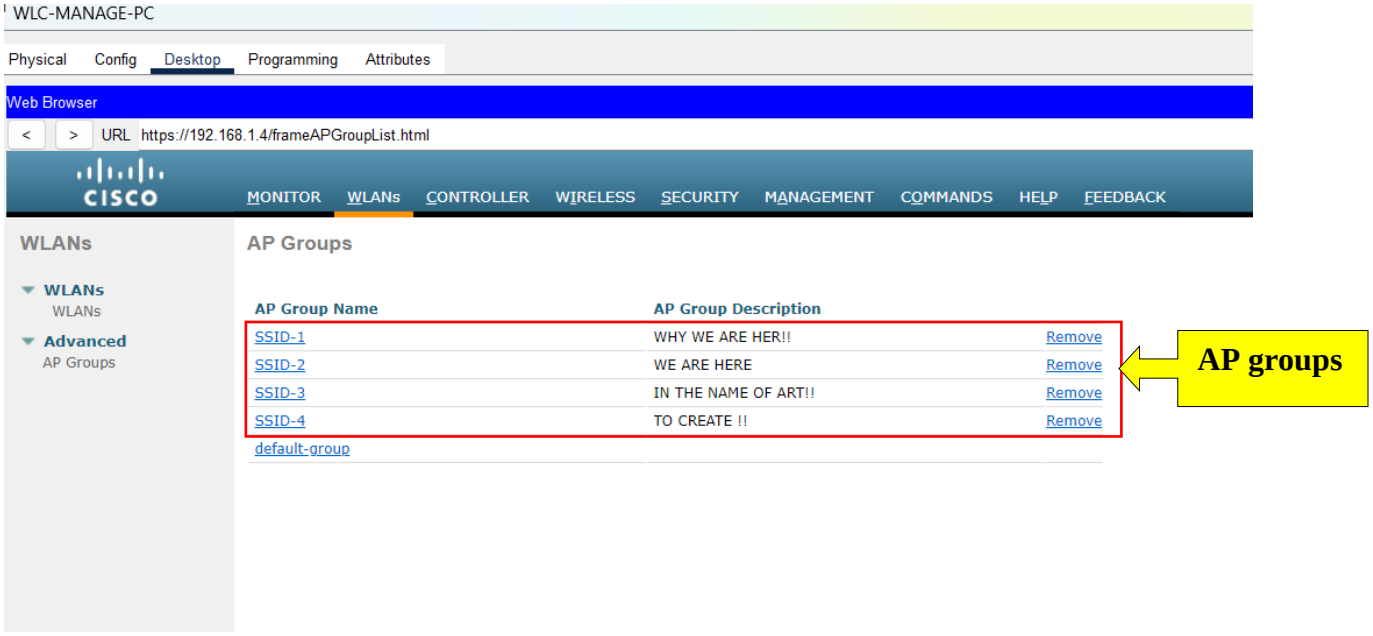
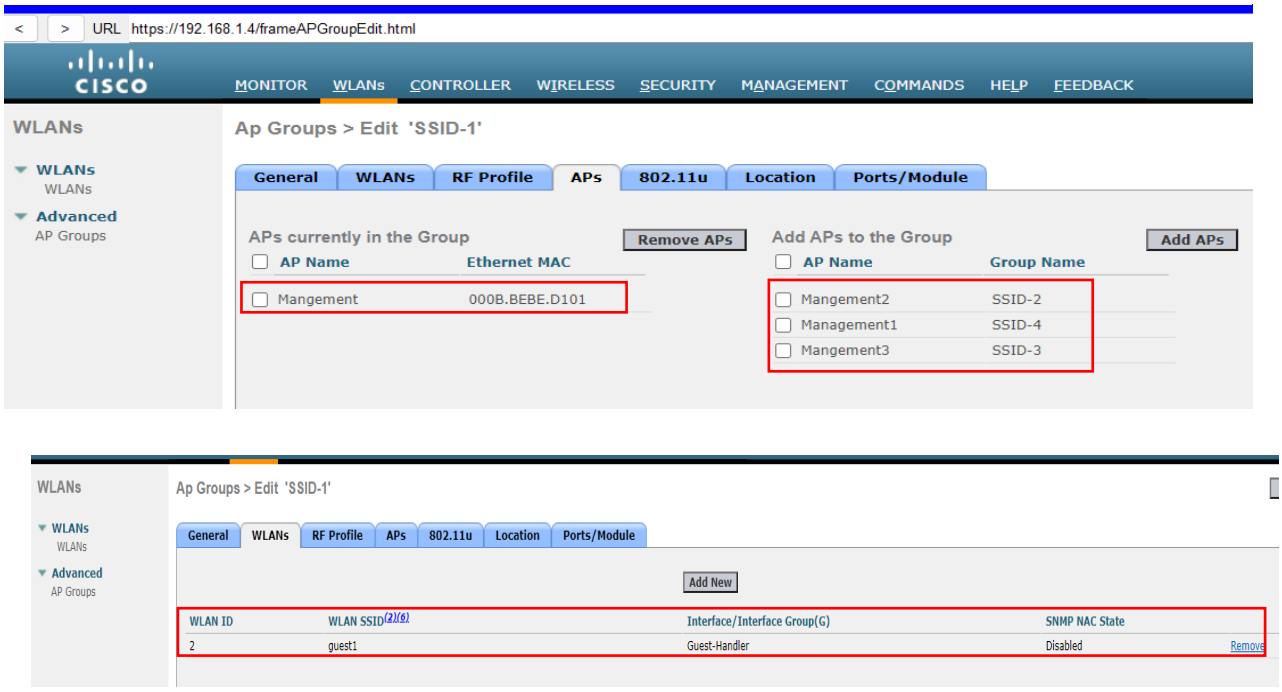


Figure 193-Inside AP groups add WLAN and Access-point



WLC Verification

HEADQUARTER

Figure 194-SSID name and password

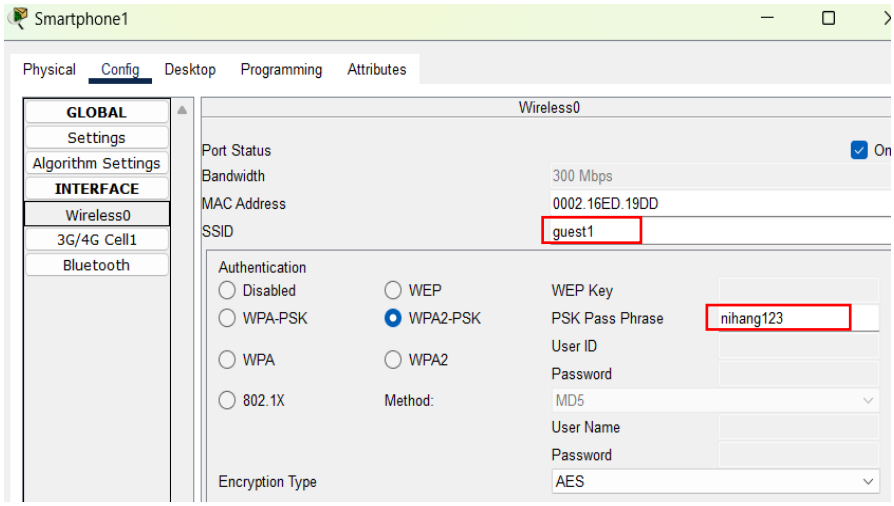
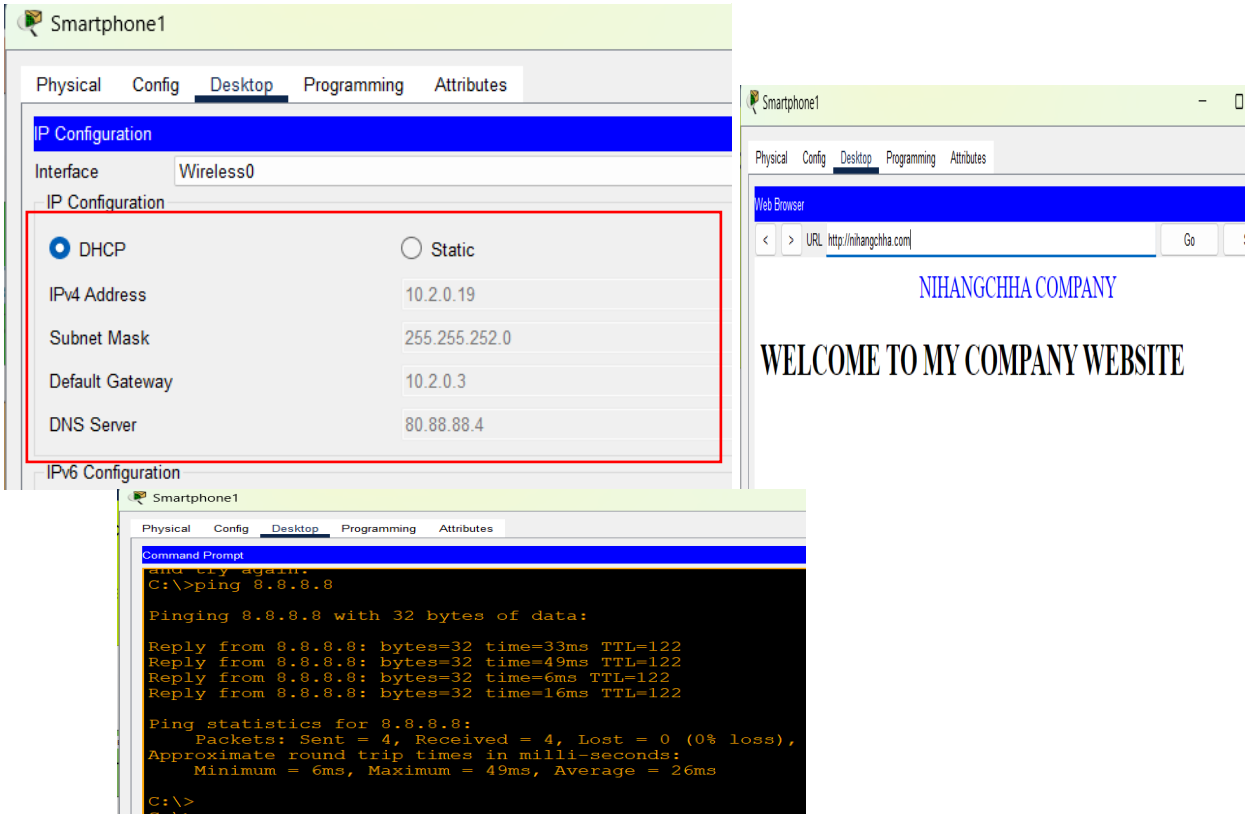


Figure 195-IP obtained from DHCP headquarter



BRANCH

Figure 196-WLC region of Branch

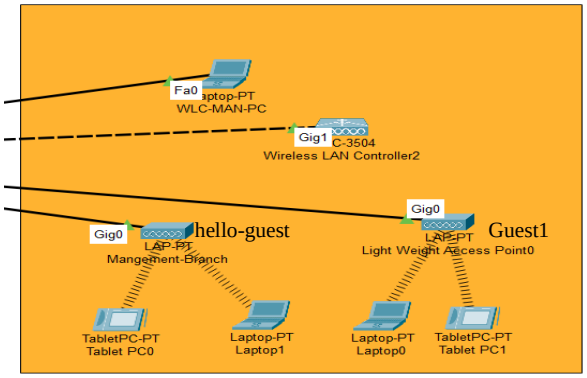


Figure 197-SSID and password

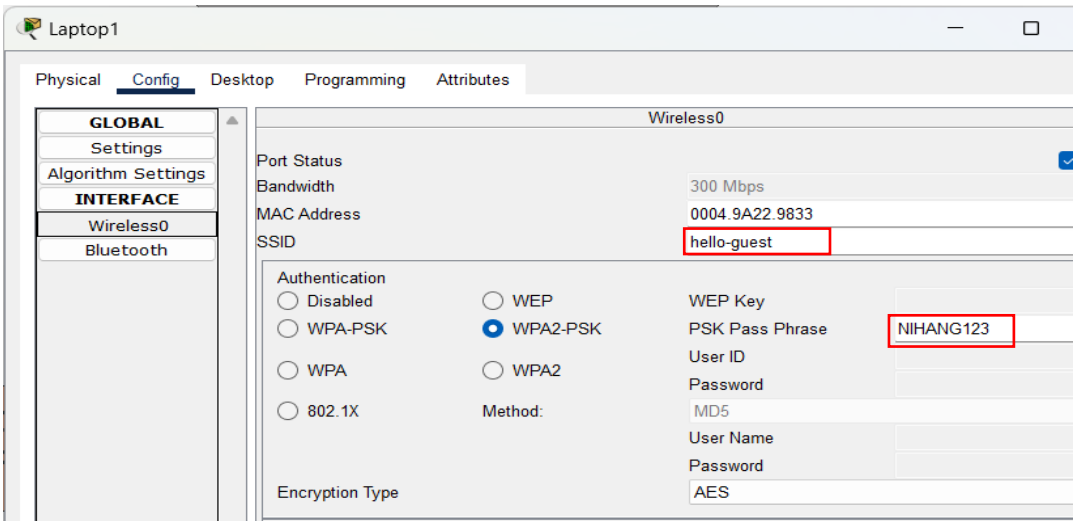


Figure 198-IP obtained from DHCP server in branch laptop

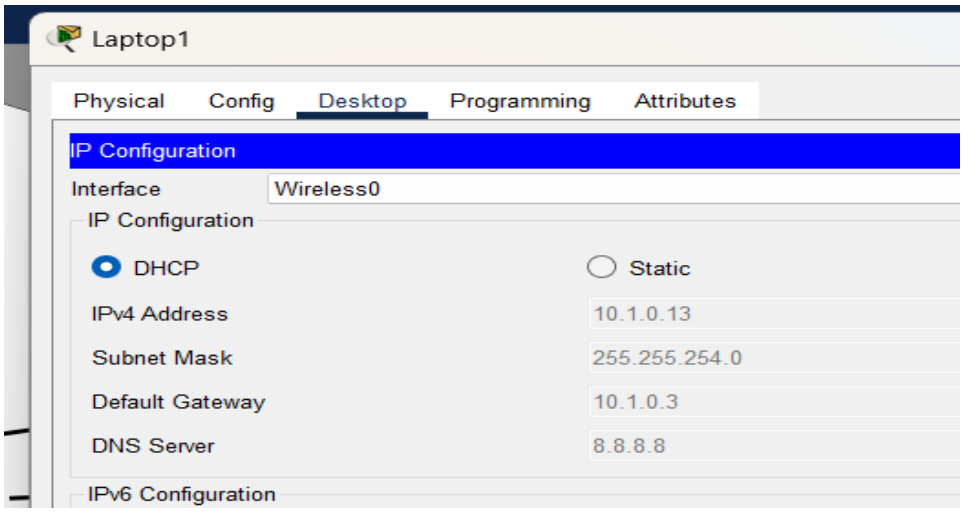
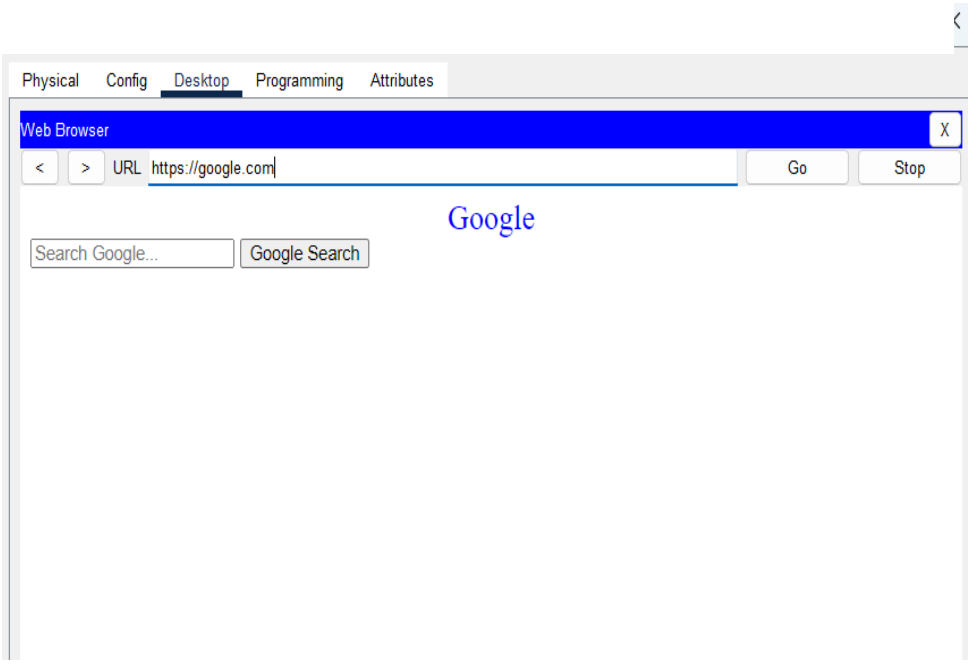
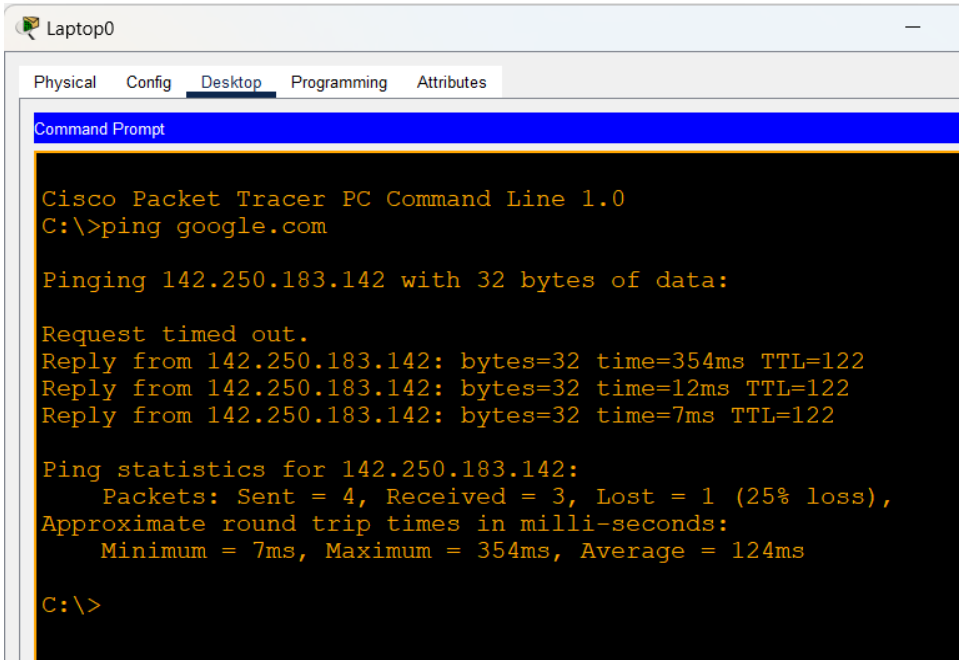


Figure 199-WLC verification in branch through web browser and ping




Laptop0
Physical
Config
Desktop
Programming
Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping google.com
Pinging 142.250.183.142 with 32 bytes of data:
Request timed out.
Reply from 142.250.183.142: bytes=32 time=354ms TTL=122
Reply from 142.250.183.142: bytes=32 time=12ms TTL=122
Reply from 142.250.183.142: bytes=32 time=7ms TTL=122
Ping statistics for 142.250.183.142:
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
Minimum = 7ms, Maximum = 354ms, Average = 124ms
C:\>

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

Figure 200-Google NTP server

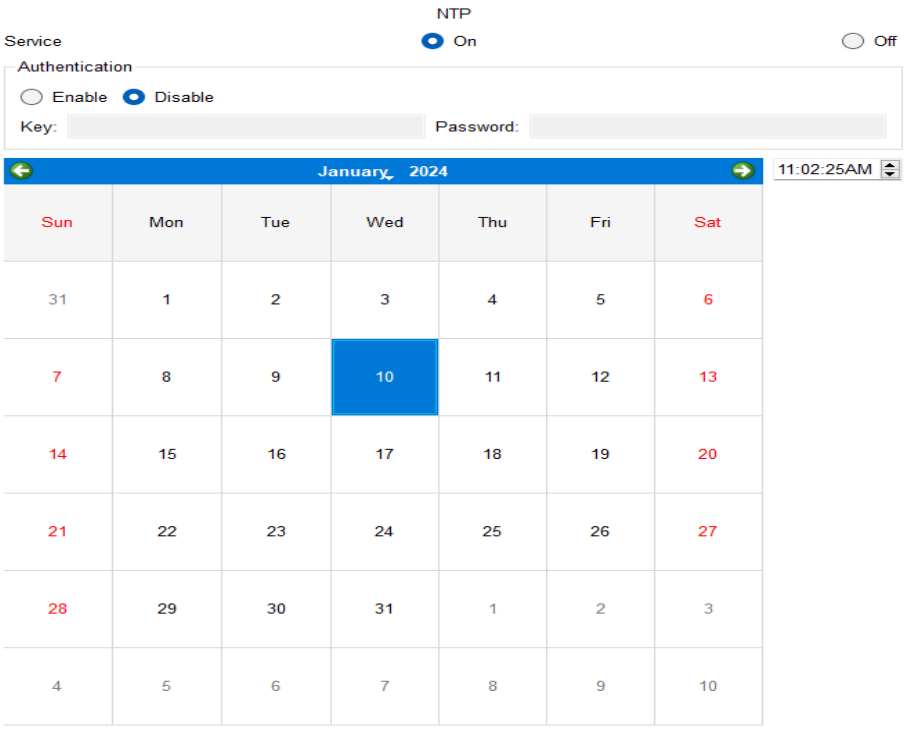
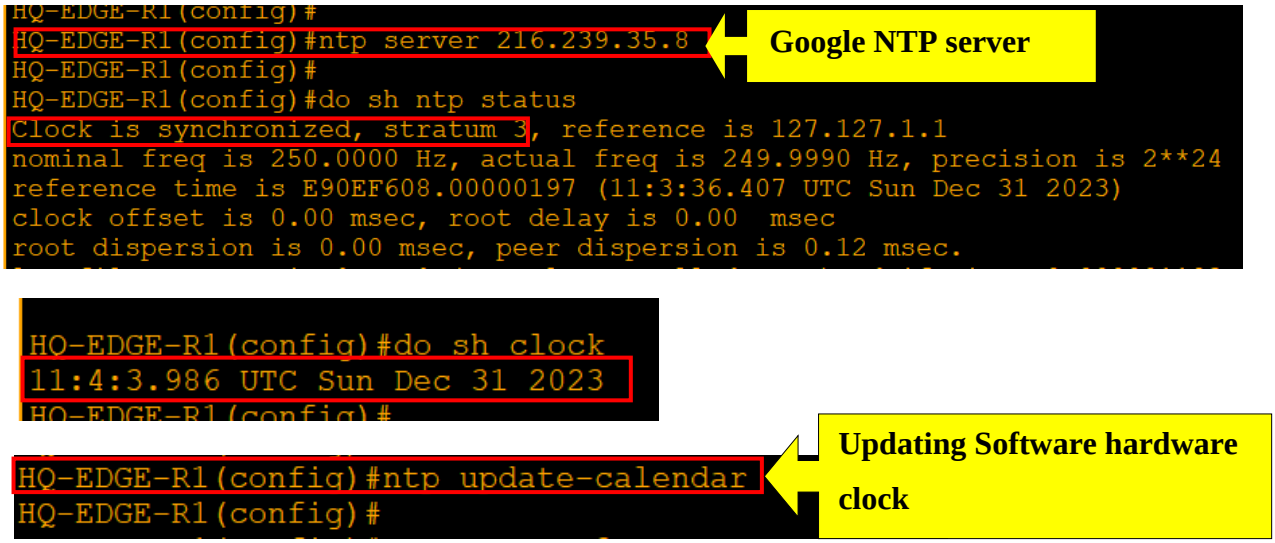


Figure 201-Synchronizing the HQ-EDGE-R1 and BR-EDGE-R2 with google NTP clock




```
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

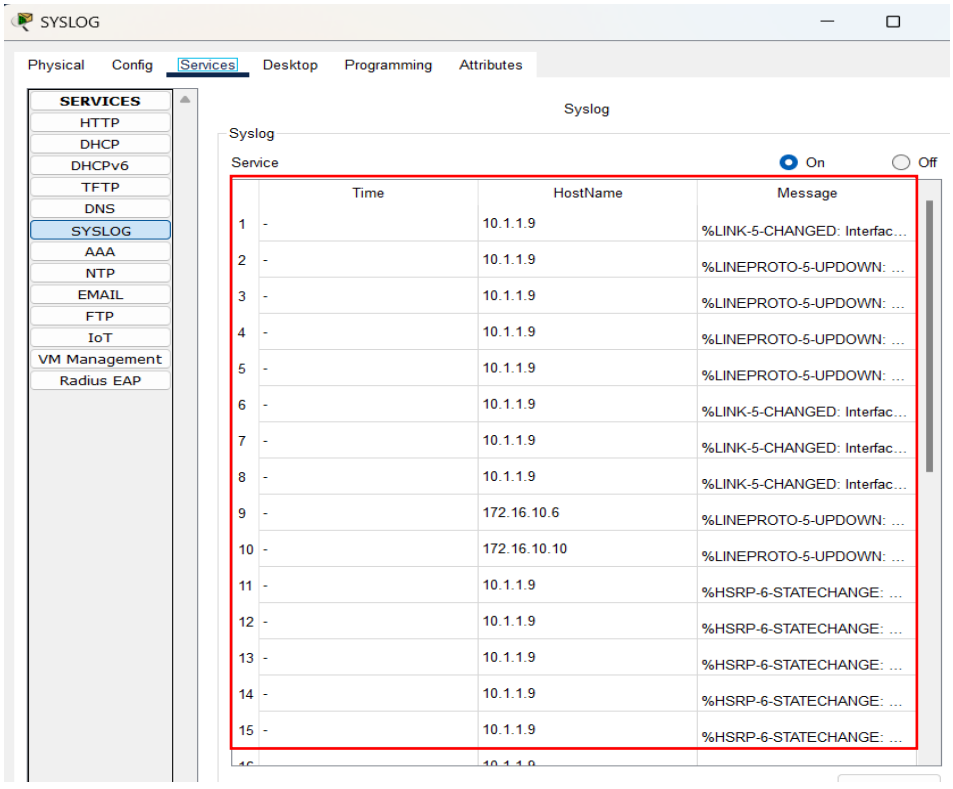
```
 logging synchronous
HQ-DISTRI-SW2(config)#logging 192.168.254.11
HQ-DISTRI-SW2(config)#logging trap debugging
```

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

Figure 202-Log stored in Syslog server of Headquarter

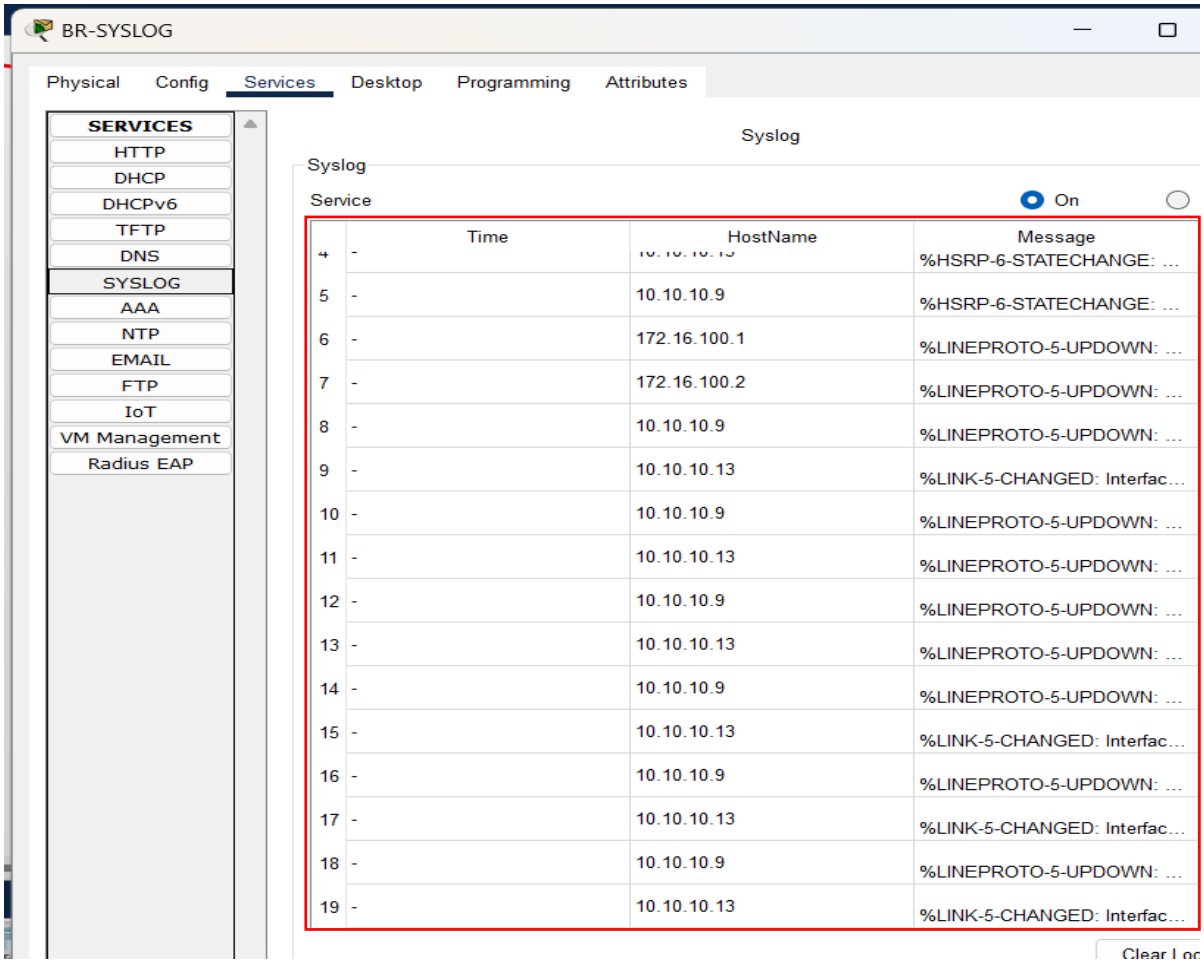


BRANCH

```
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 203-Log stored in syslog server of Branch



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.

Figure 204-SNMP configuration in HQ-EDGE-R1

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

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

Figure 205-Authentication of read and write community of Managed Device in MIB browser

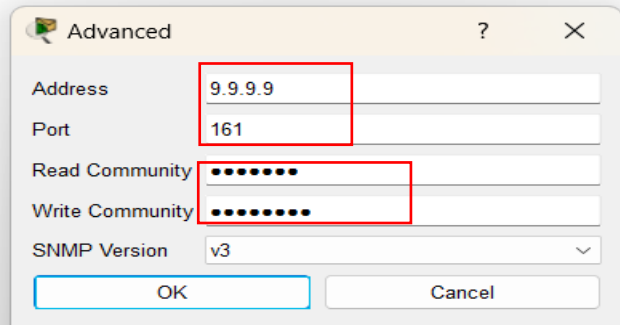


Figure 206-GET and SET request from the SNMP NMS (Network

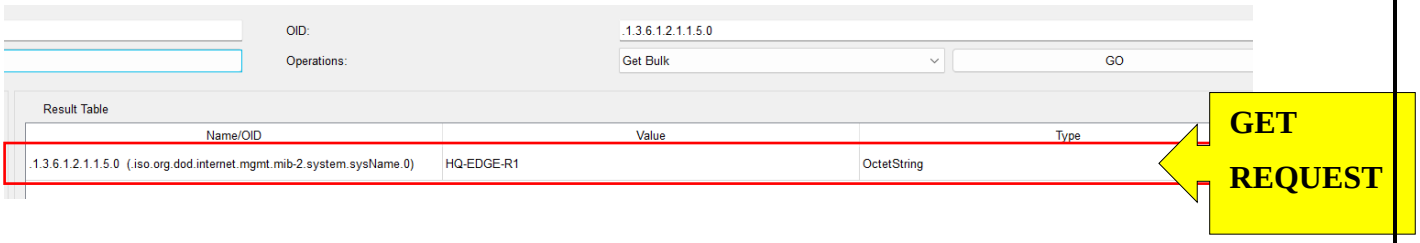
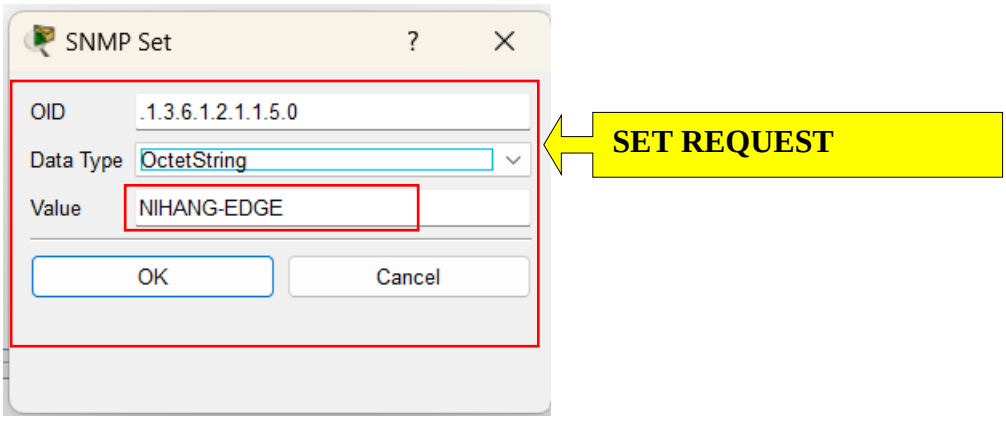
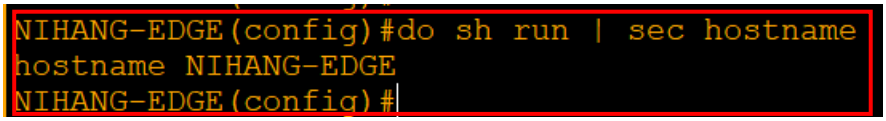


Figure 207-Changing hostname of HQ-EDGE-R1 by SNMP





Hostname change also takes effect in running config

Figure 208-SNMP configuration in BR-CORE-R2

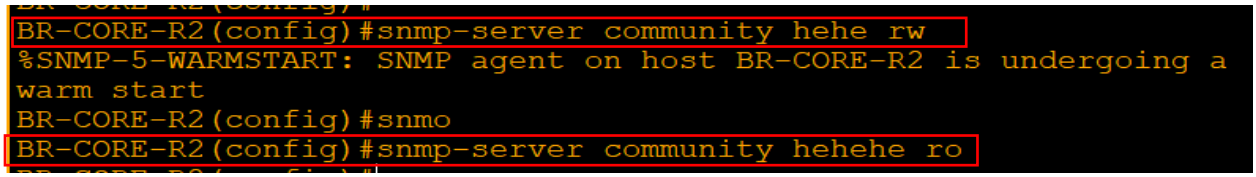


Figure 209-Authentication of Managed device in MIB browser

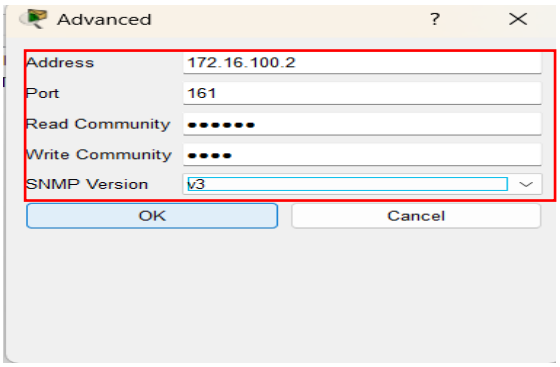
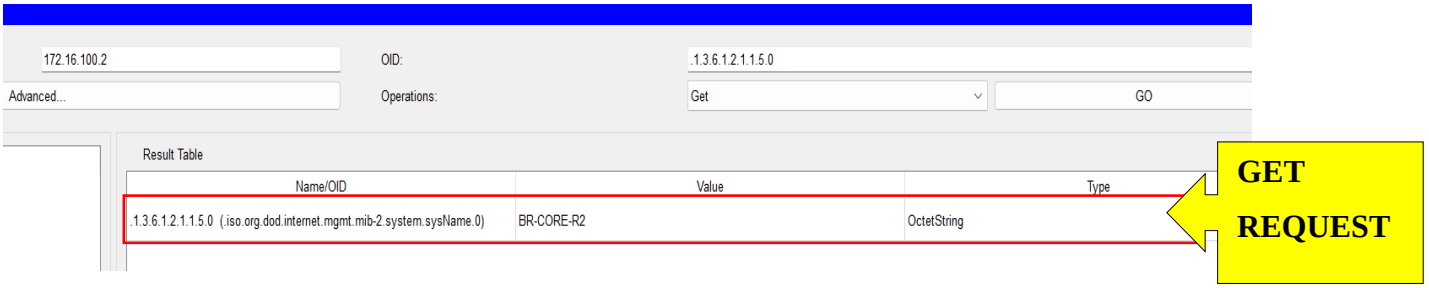
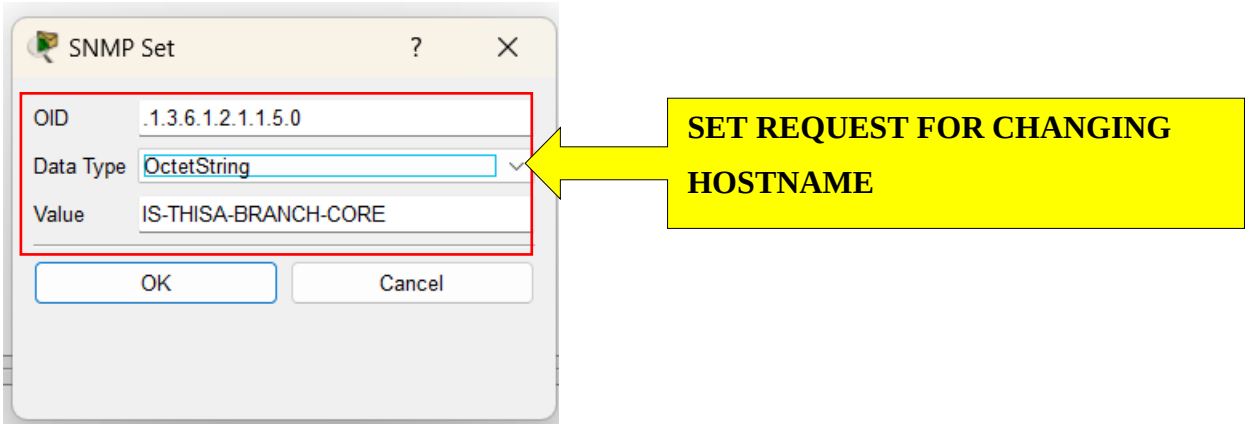
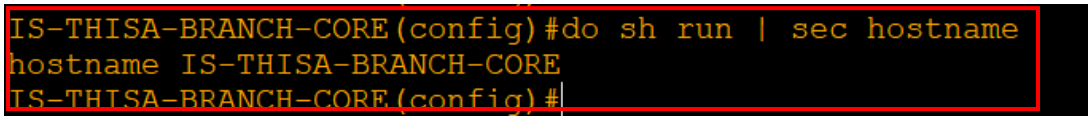


Figure 210-Requesting GET and SET from SNMP NMS







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.

Figure 211-Configuration of TACAS+ client in HQ-CORE-R1

```
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 212-Configuration of SSH 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 213-Configuration of TACAS+ server

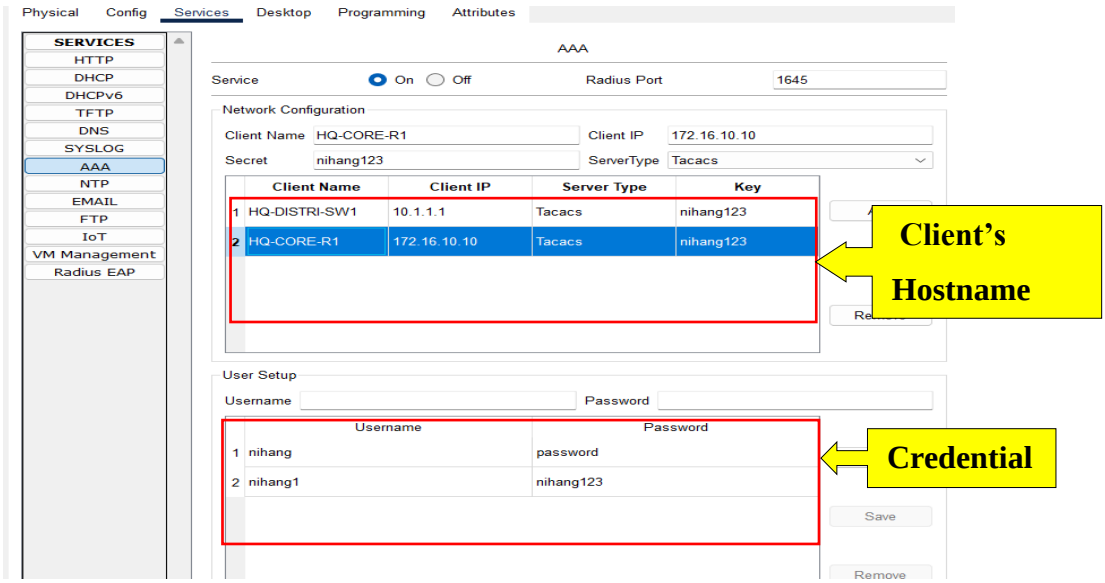
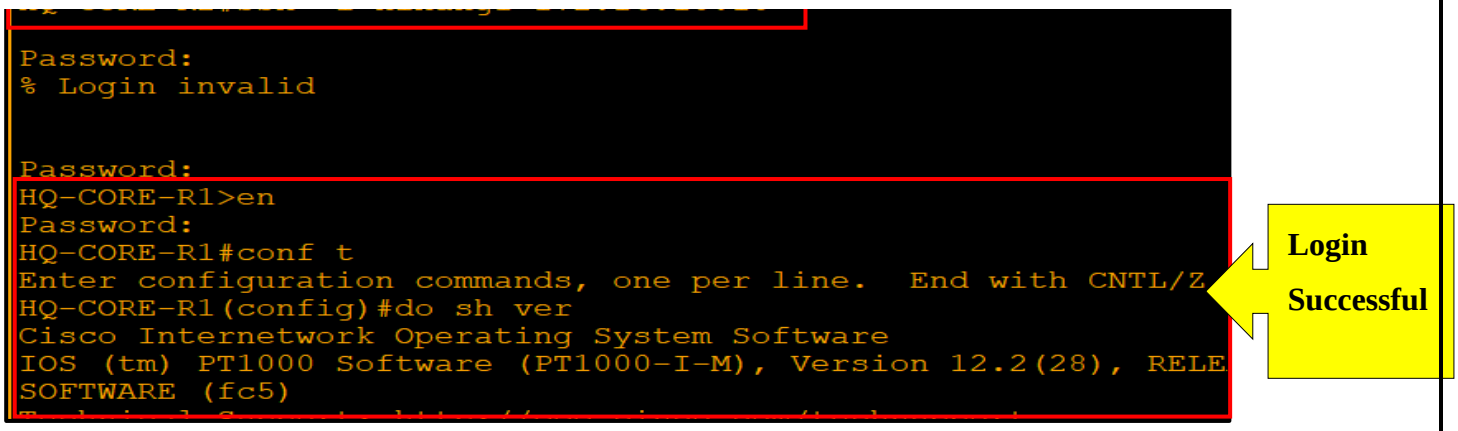


Figure 214-AAA verification



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 215-DNS server of DMZ and webserver hosting in DMZ area

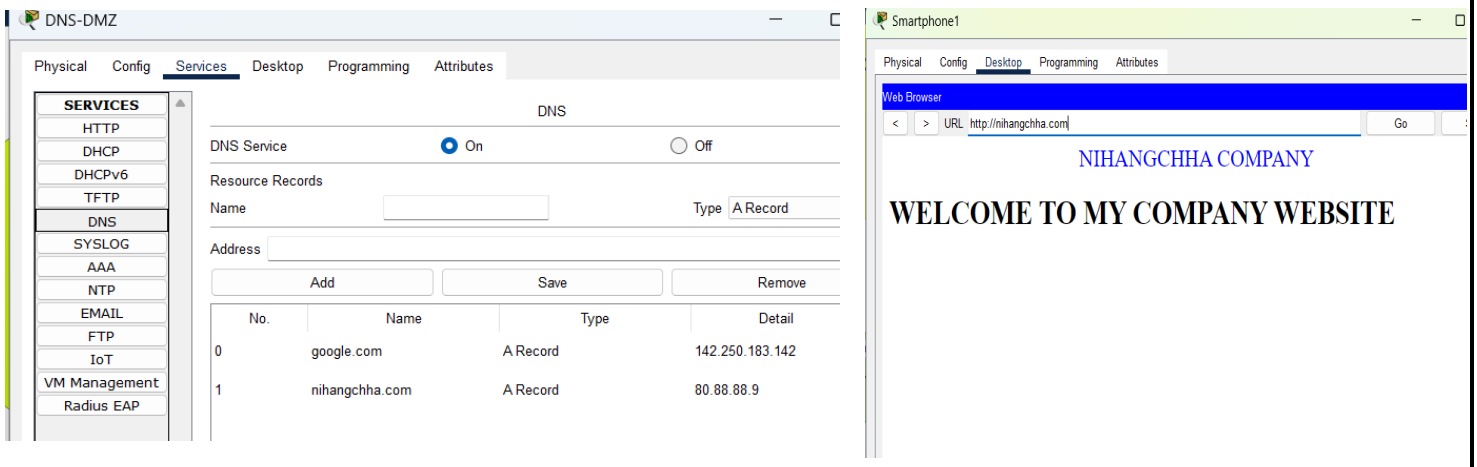
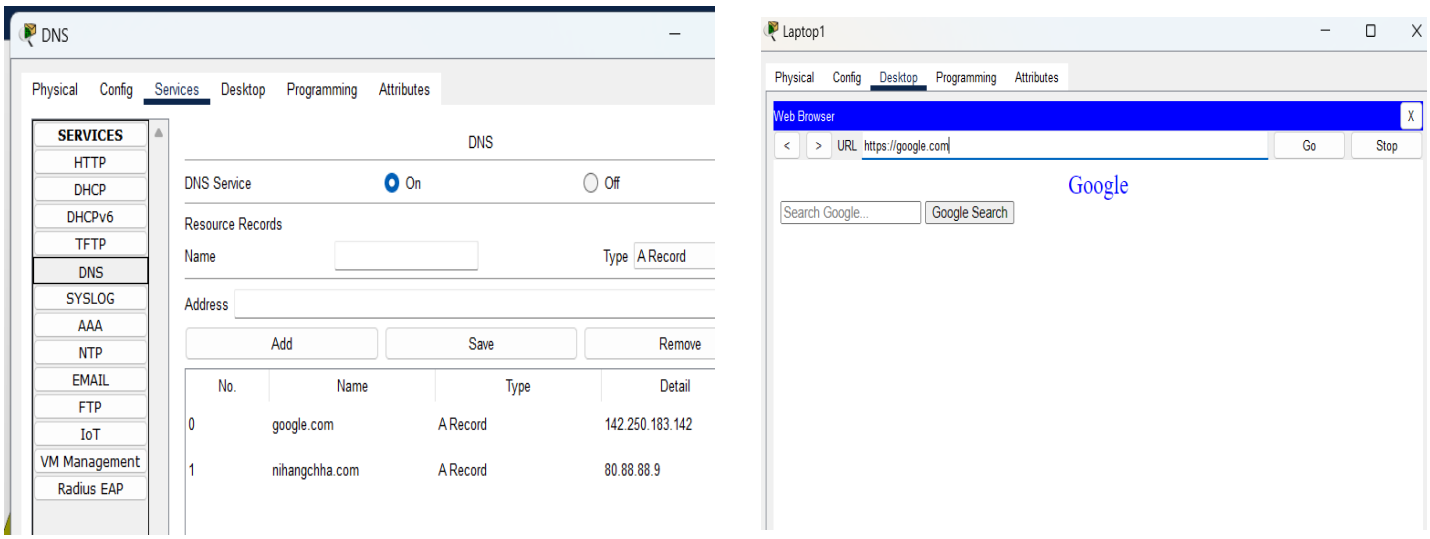


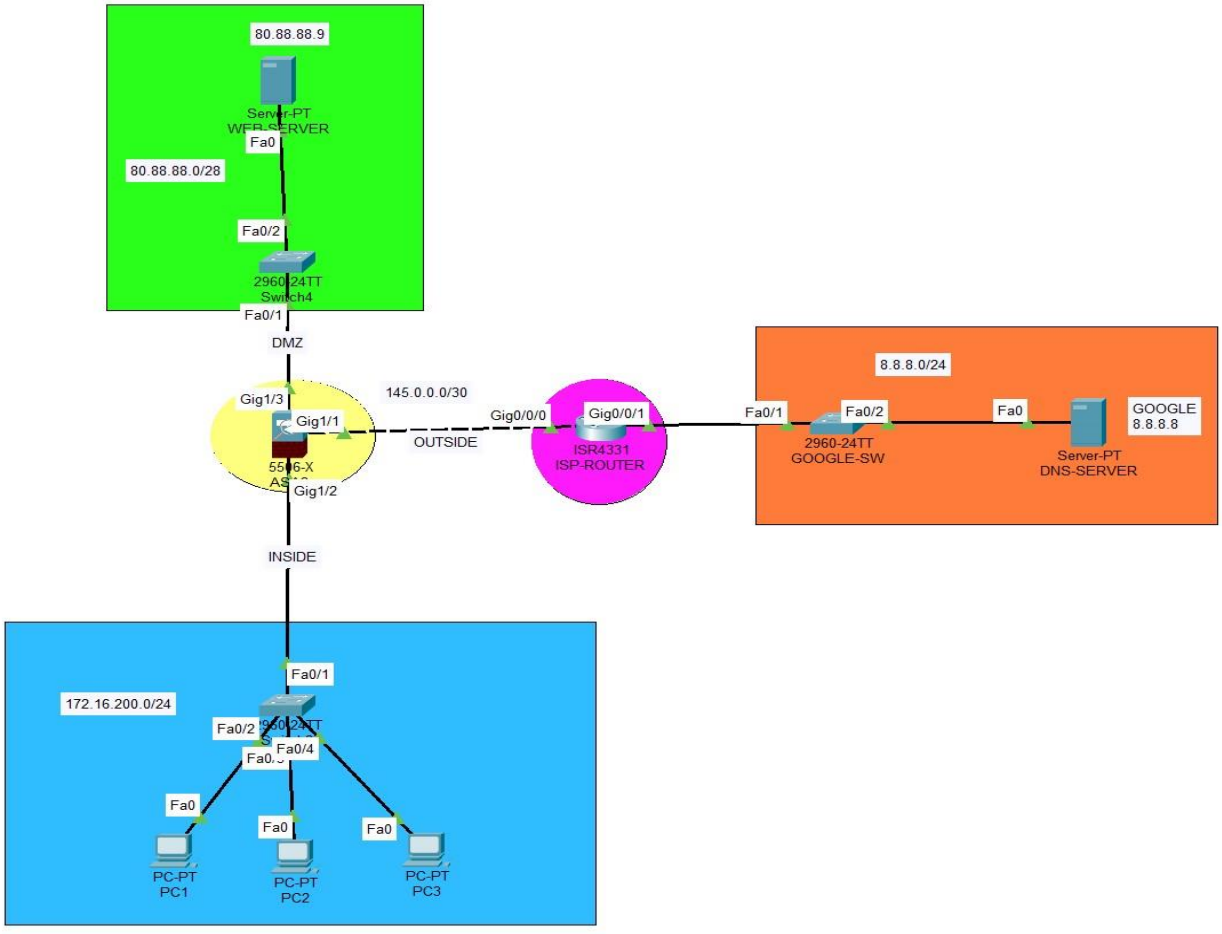
Figure 216-DNS server of Google and webserver hosting in google area



FIREWALL

Firewall was implemented at different physical diagram due to some issue with the cisco packet tracer.

Figure 217-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

Figure 218-Assigning name, security, and IP address to interfaces

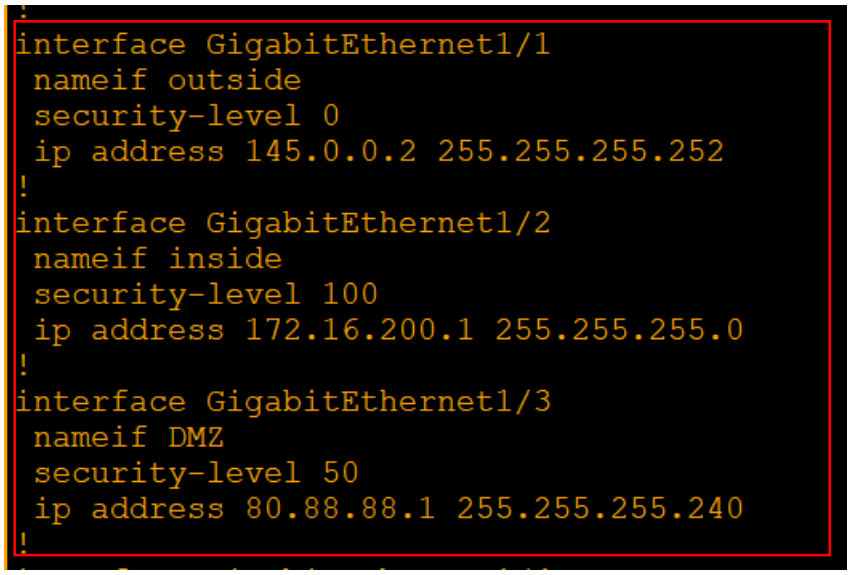


Figure 219-DHCP server pool creation in firewall

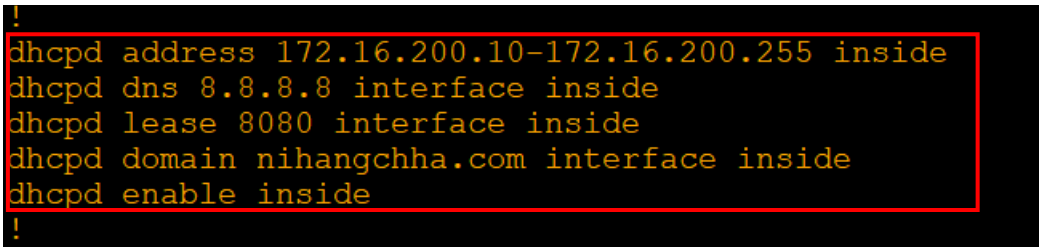


Figure 220-DHCP server verification from firewall

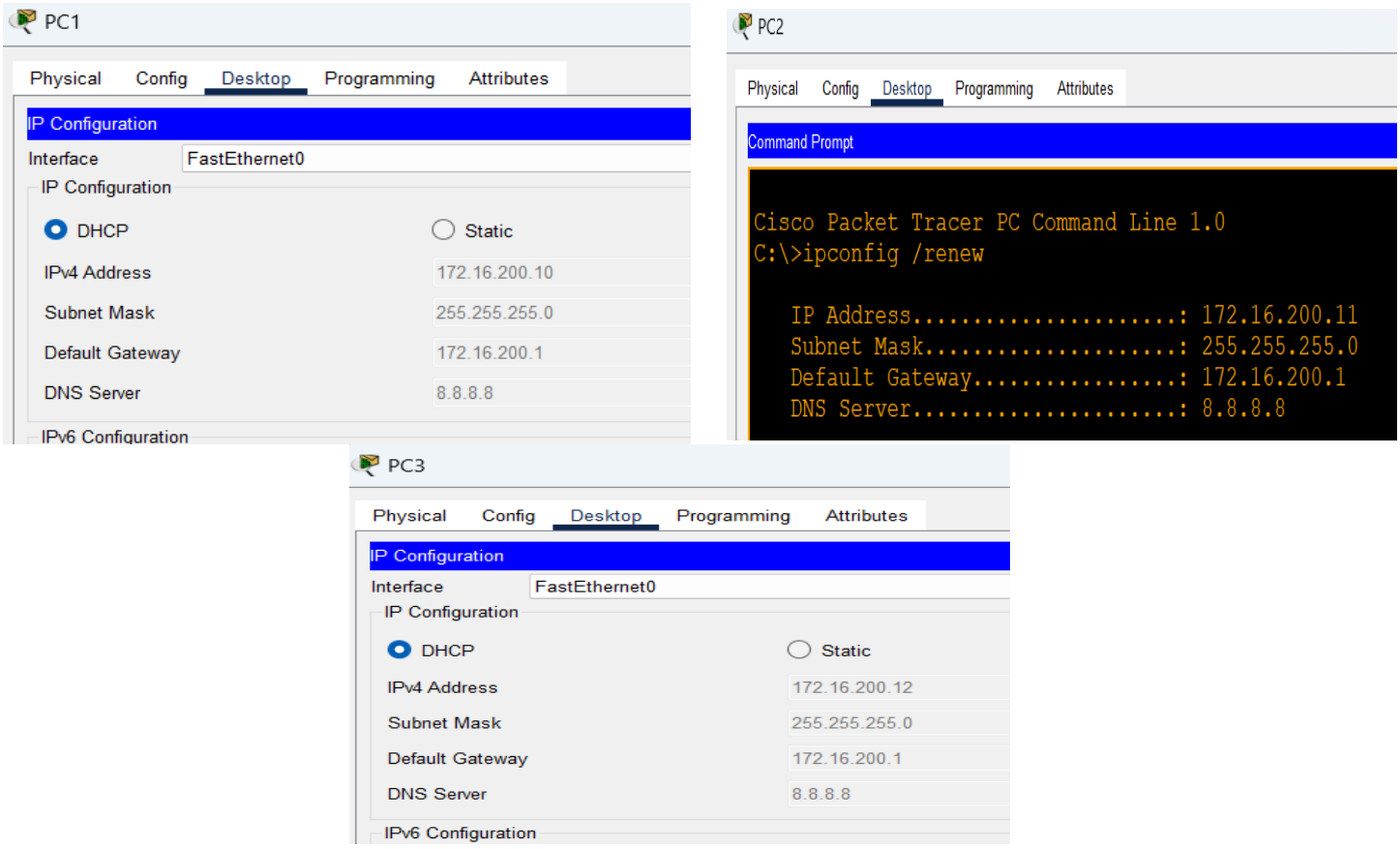


Figure 221-Creating a default static route to outside in firewall

Figure 222-OSPF configuration in FIREWALL

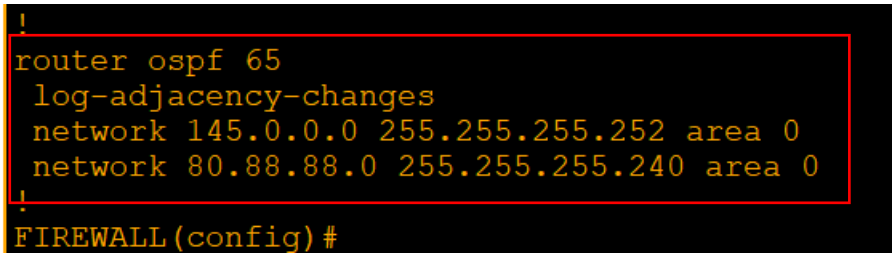


Figure 223-Dynamic NAT config on Firewall

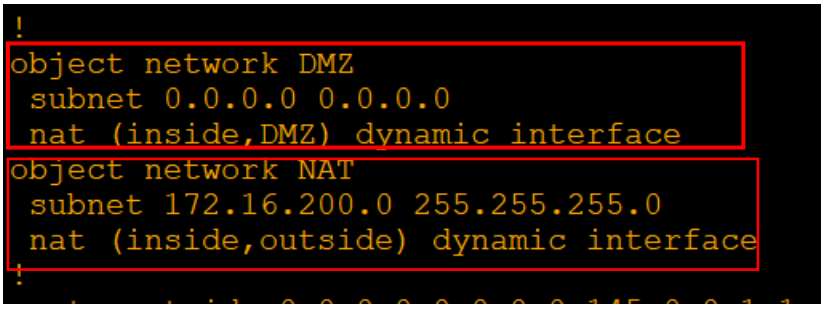
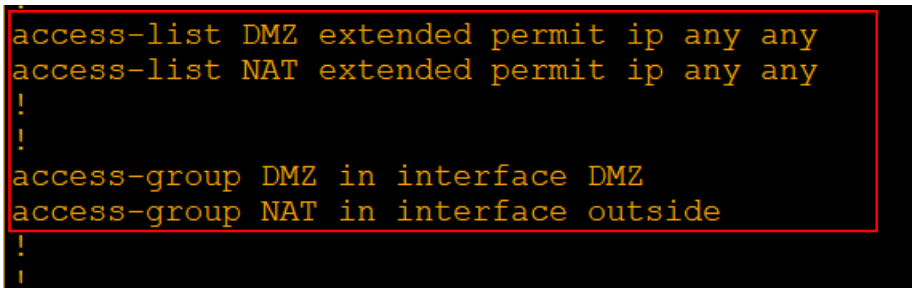


Figure 224-Access list of FIREWALLS



ISP

Figure 225-OSPF configuration in ISP router

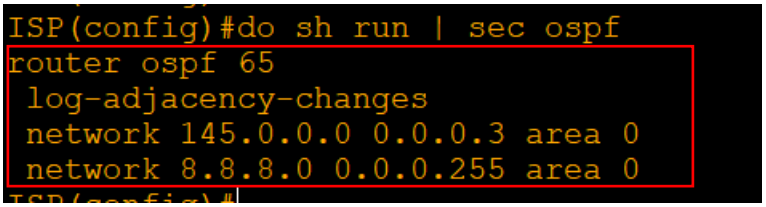


Figure 226-DNS server config

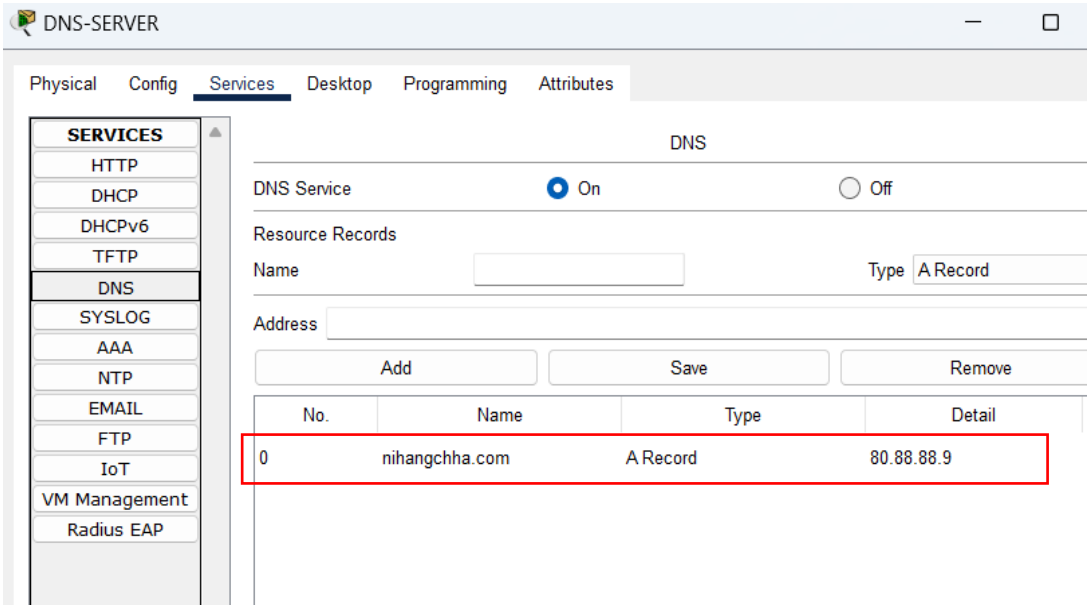
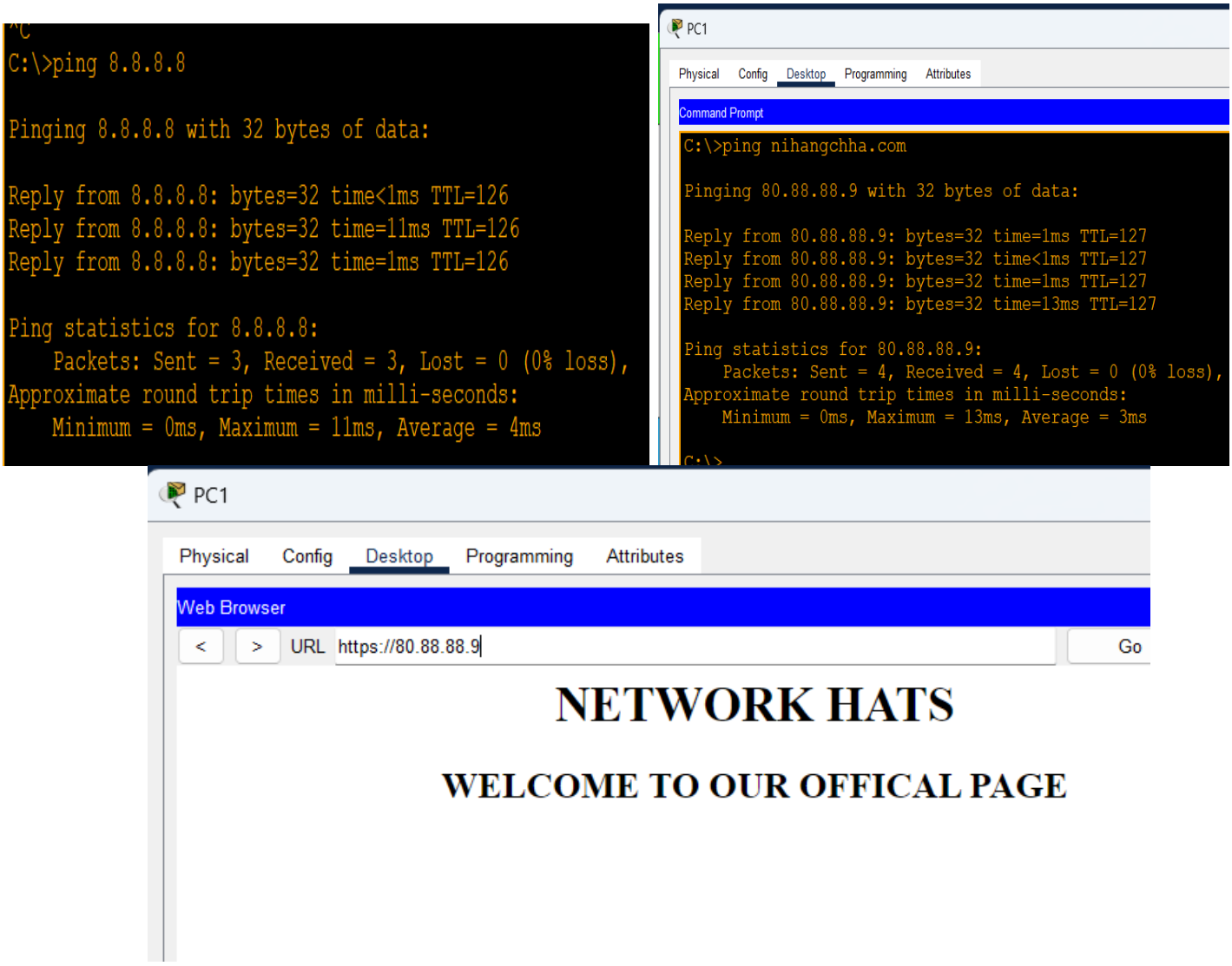


Figure 227-Verification through ping and browser



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.

Importance

Risk Management

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

Compliance:

a. 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.
b. Adhering to industry-specific standards ensures that the organization meets the expectations of customers and partners.

Social Issues:

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

Legal Issues:

a. Navigating legal complexities helps organizations avoid legal challenges and associated financial penalties. It safeguards the organization against legal actions resulting from non-compliance.
b. 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, Controlloing 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 mange 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. As a result, they can focus on their other business while leveraging the power of cloud computing.

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

a. **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.

b. **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.

c. **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.

d. **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

To sum up, this report, created by me, explains how we set up and organized different network devices in a three-tier system with backups at the main headquarter and branch. We used essential services like NAT, VPN, SNMP, SYLOG, DNS, DHCP, STP, VLAN, and WLC to specific requirement of customer. Prioritizing the access layer, we added strong security features like BPDU Guard, Port Security, DHCP snooping, and ARP inspection.

Beyond the technical stuff, we also looked at risk management, rules, and social and legal concerns, showing a well-rounded view. The report talks about new and emerging tech trends like Software Defined Networking (SDN), Network Virtualization (NV), Cloud Computing, and Edge Computing.

By covering all these details, the report not only meets the tech needs but also deals with bigger challenges, making sure the network is strong against issues and follows the rules. Adapting to new trends keeps the network working well in today's digital world.

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/