in collaboration with

Networking

Arman shah

BSc (Hons) in Ethical Hacking and Cyber Security

Softwarica College of IT and E - Commerce | In Collaboration with Coventry University

ST5064CEM Networking

Manoj Tamang

February 2, 2024

Abstract

This is the report writing task for the networking module coursework. Both the branch side and the headquarters are constructing a three-tier network architecture. Every Lauer has different services and protocols defined, including DHCP, HSRO, spanning-tree, WLC, OSPF, ACL, Nat, VPN, firewall, and others. These configurations are made in the network topology. The paper also includes a thorough description of how three-tier design is affected by new networking developments.

Table of Contents

Introduction

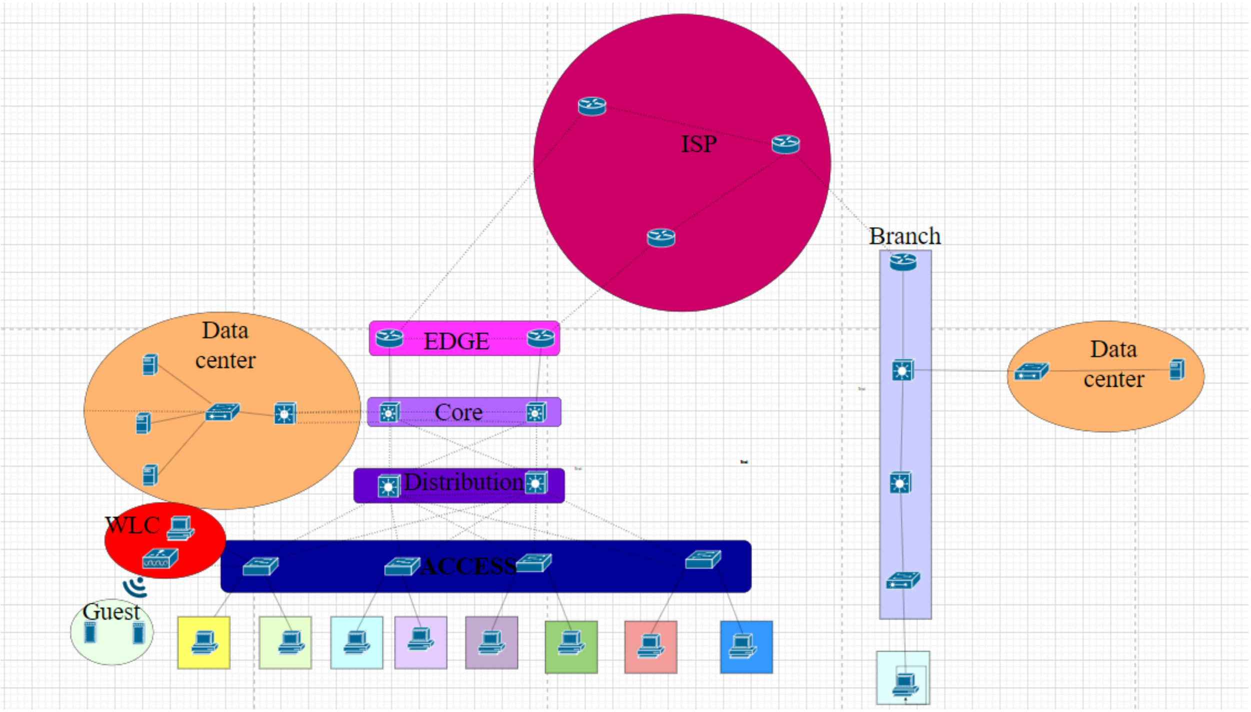
In the ever-evolving digital landscape, Network Hats stands as a leader in delivering top-tier network security solutions. This project showcases designing and implementing tailored security architectures, ensuring the protection of valuable assets and sensitive information for our clients. prioritizing the deployment of robust security solutions, vigilant network traffic monitoring, and proactive measures to address breaches promptly.

As a network engineer at Network Hats, I've used Cisco Packet to accurately match a bespoke network topology in a classic three-tier architecture with the demands of our clients. Access, distribution, core, and an additional edge layer are all included in this setup, which also integrates L2 security features like DHCP snooping, port security, BPDU guard, and NTP, SNMP, NAT, VPN, SYSLOG, and DHCP.

Part A

Designs

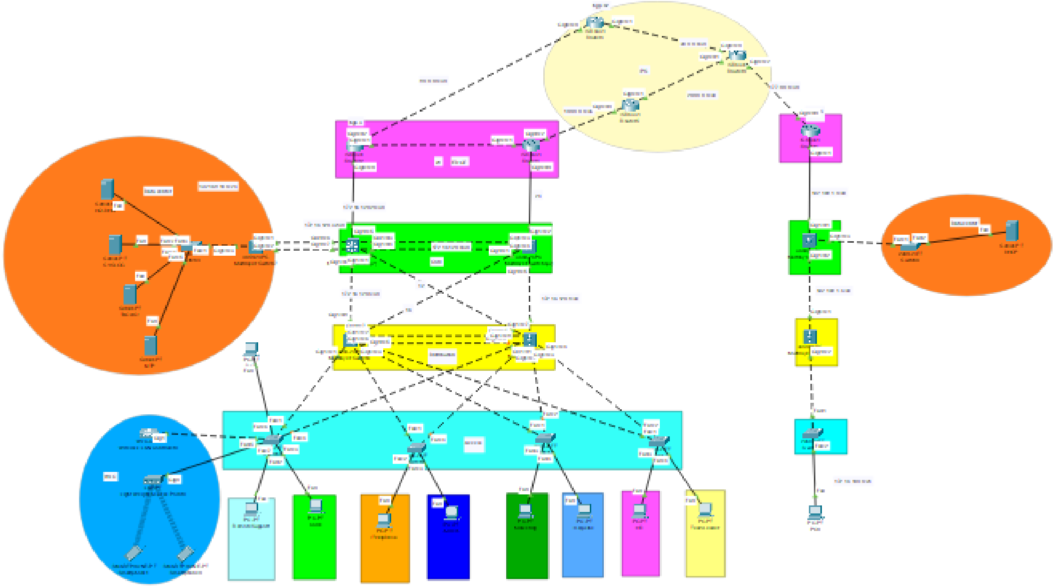
Figure 1: **Logical Network design**



As shown in the above figure, it consists of three tier architecture design implemented on headquarters and branch of company.

Physical Prototype

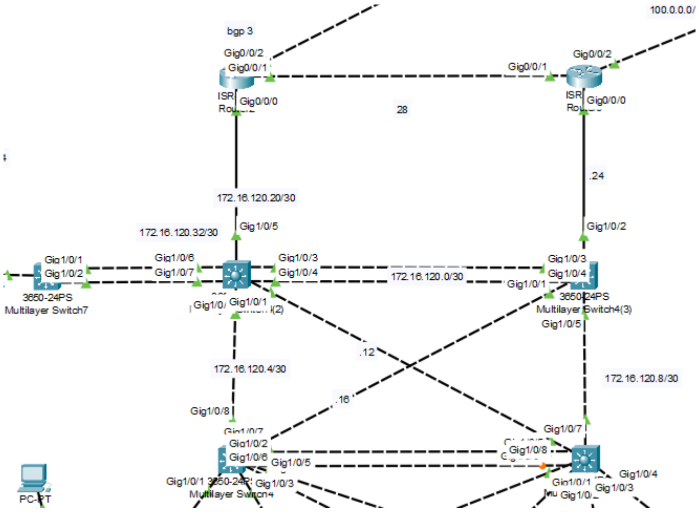
Figure 2: Physical Prototype of three-tier architecture

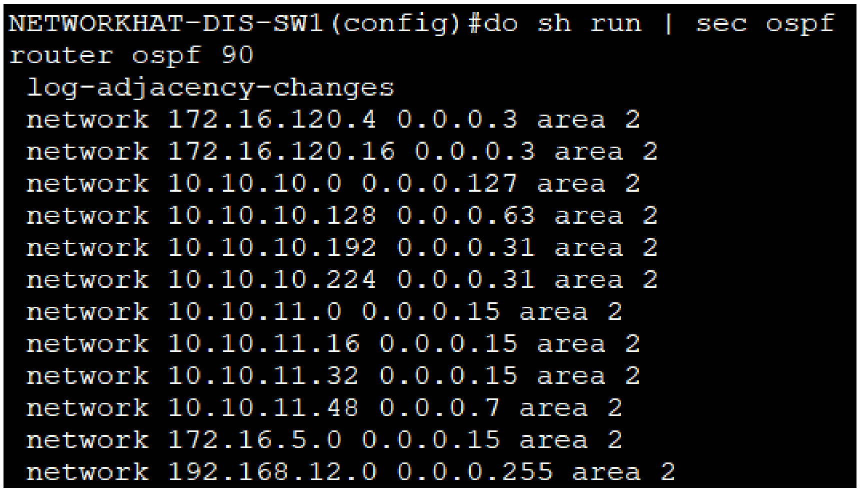


OSPF

In computer networks, Open Shortest Path First is a routing protocol that is frequently used to allow routers to dynamically share routing information and choose the best routes for data traffic. OSPF is an interior gateway protocol (IGP) designed for use within an autonomous system, such as a private corporate network.

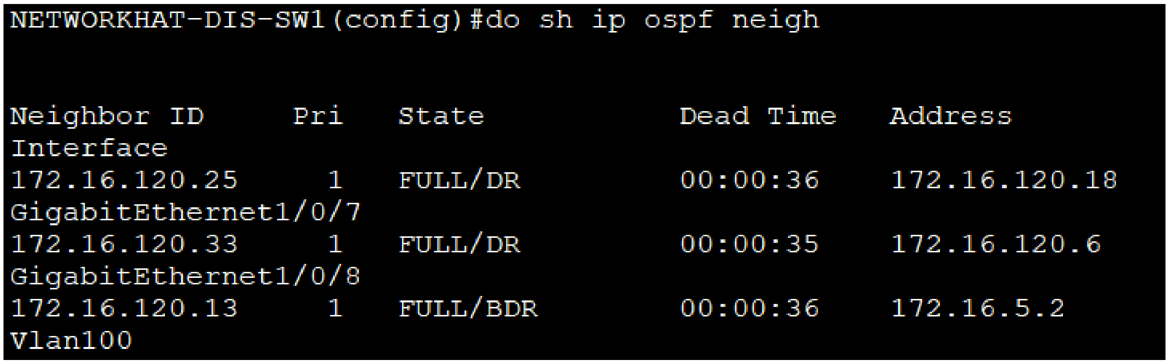
HQ





```
NETWORKHAT-DIS-SW1(config)#do sh run | sec ospf
router ospf 90
 log-adjacency-changes
 network 172.16.120.4 0.0.0.3 area 2
 network 172.16.120.16 0.0.0.3 area 2
 network 10.10.10.0 0.0.0.127 area 2
 network 10.10.10.128 0.0.0.63 area 2
 network 10.10.10.192 0.0.0.31 area 2
 network 10.10.10.224 0.0.0.31 area 2
 network 10.10.11.0 0.0.0.15 area 2
 network 10.10.11.16 0.0.0.15 area 2
 network 10.10.11.32 0.0.0.15 area 2
 network 10.10.11.48 0.0.0.7 area 2
 network 172.16.5.0 0.0.0.15 area 2
 network 192.168.12.0 0.0.0.255 area 2
```

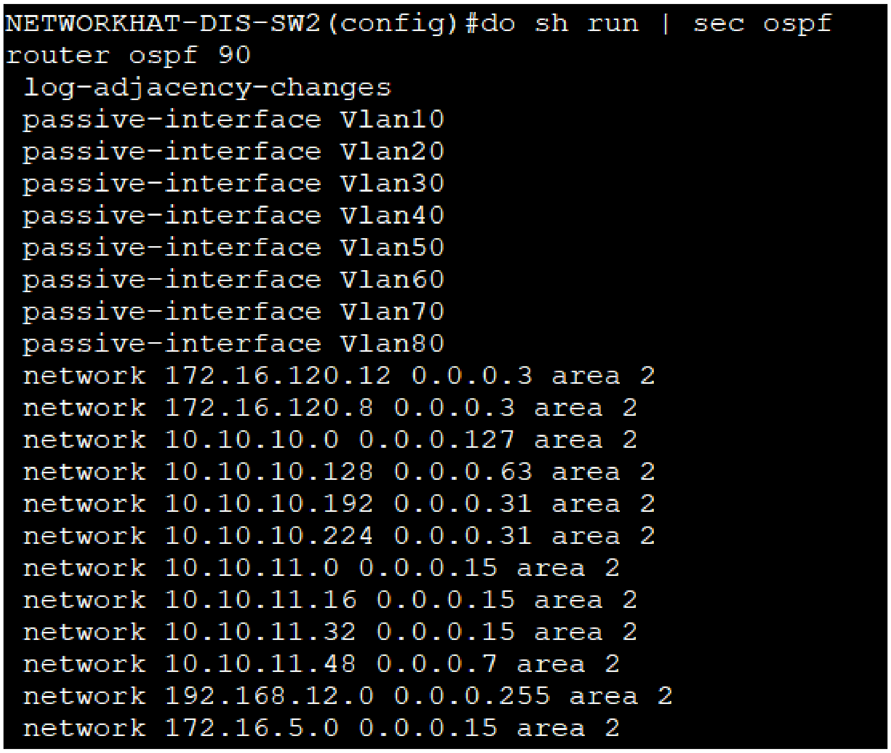
Svi interface network advertise In ospf



```
NETWORKHAT-DIS-SW1(config)#do sh ip ospf neigh


Neighbor ID     Pri   State           Dead Time   Address
Interface
172.16.120.25     1   FULL/DR         00:00:36    172.16.120.18
GigabitEthernet1/0/7
172.16.120.33     1   FULL/DR         00:00:35    172.16.120.6
GigabitEthernet1/0/8
172.16.120.13     1   FULL/BDR        00:00:36    172.16.5.2
Vlan100
```

OSPF neighborship of NETWPRKHAT-DIS-SW1

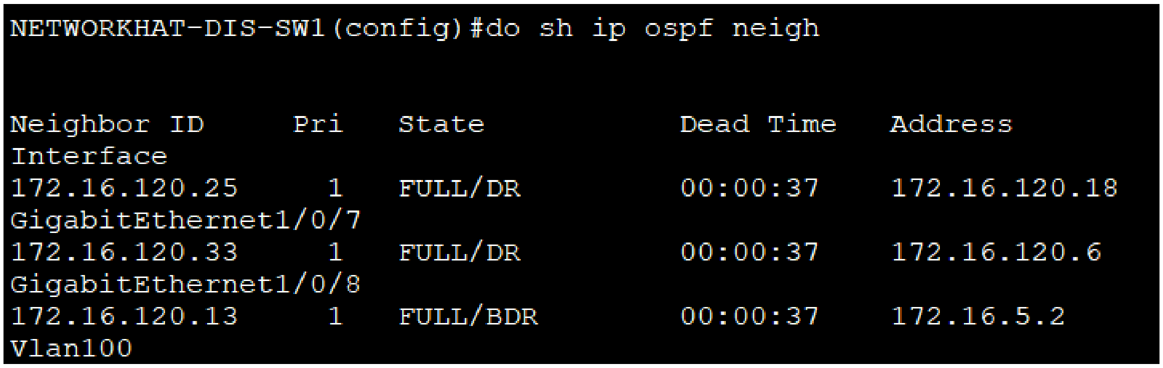
NETWORKHAT-DIS-SW2



```
NETWORKHAT-DIS-SW2(config)#do sh run | sec ospf
router ospf 90
 log-adjacency-changes
 passive-interface Vlan10
 passive-interface Vlan20
 passive-interface Vlan30
 passive-interface Vlan40
 passive-interface Vlan50
 passive-interface Vlan60
 passive-interface Vlan70
 passive-interface Vlan80
 network 172.16.120.12 0.0.0.3 area 2
 network 172.16.120.8 0.0.0.3 area 2
 network 10.10.10.0 0.0.0.127 area 2
 network 10.10.10.128 0.0.0.63 area 2
 network 10.10.10.192 0.0.0.31 area 2
 network 10.10.10.224 0.0.0.31 area 2
 network 10.10.11.0 0.0.0.15 area 2
 network 10.10.11.16 0.0.0.15 area 2
 network 10.10.11.32 0.0.0.15 area 2
 network 10.10.11.48 0.0.0.7 area 2
 network 192.168.12.0 0.0.0.255 area 2
 network 172.16.5.0 0.0.0.15 area 2
```

No of OSPF neighborship between two distribution switches

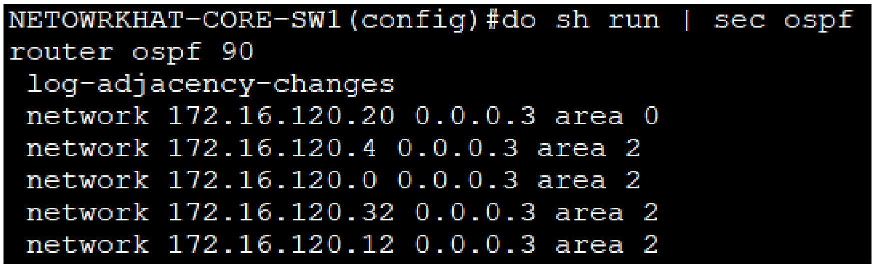
Svi interface network advertise In ospf



```
NETWORKHAT-DIS-SW1(config)#do sh ip ospf neigh


Neighbor ID     Pri   State           Dead Time   Address
Interface
172.16.120.25     1   FULL/DR         00:00:37    172.16.120.18
GigabitEthernet1/0/7
172.16.120.33     1   FULL/DR         00:00:37    172.16.120.6
GigabitEthernet1/0/8
172.16.120.13     1   FULL/BDR        00:00:37    172.16.5.2
Vlan100
```

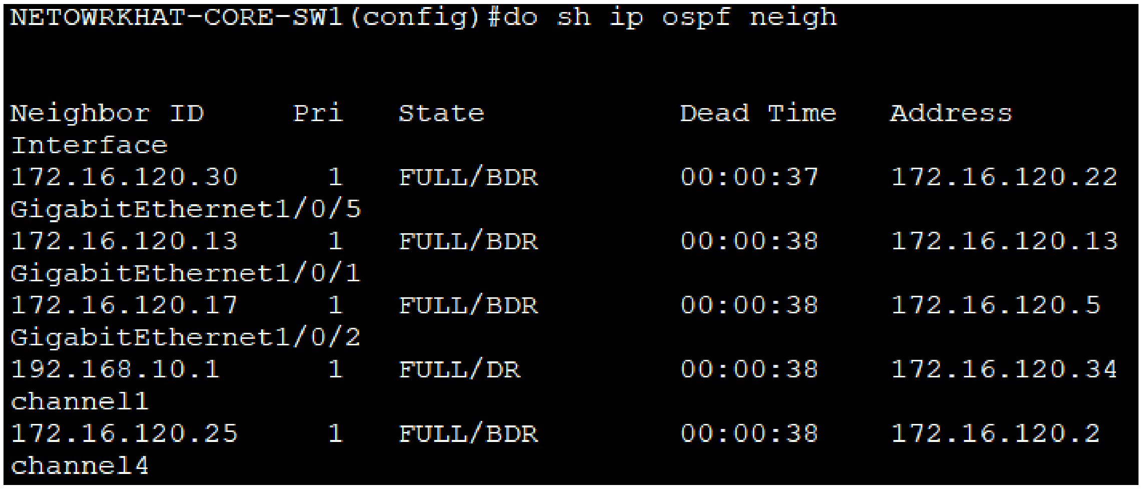
OSPF neighborship of NETWPRKHAT-DIS-SW1

Core R1



```
NETOWRKHAT-CORE-SW1(config)#do sh run | sec ospf
router ospf 90
 log-adjacency-changes
 network 172.16.120.20 0.0.0.3 area 0
 network 172.16.120.4 0.0.0.3 area 2
 network 172.16.120.0 0.0.0.3 area 2
 network 172.16.120.32 0.0.0.3 area 2
 network 172.16.120.12 0.0.0.3 area 2
```

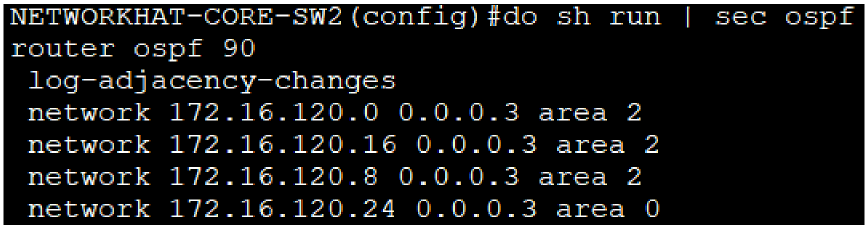
Running config of OSPF configuration of NETWORKHAT-CORE-SW1



```
NETOWRKHAT-CORE-SW1(config)#do sh ip ospf neigh


Neighbor ID     Pri   State           Dead Time   Address
Interface
172.16.120.30     1   FULL/BDR        00:00:37    172.16.120.22
GigabitEthernet1/0/5
172.16.120.13     1   FULL/BDR        00:00:38    172.16.120.13
GigabitEthernet1/0/1
172.16.120.17     1   FULL/BDR        00:00:38    172.16.120.5
GigabitEthernet1/0/2
192.168.10.1      1   FULL/DR         00:00:38    172.16.120.34
channel1
172.16.120.25     1   FULL/BDR        00:00:38    172.16.120.2
channel4
```

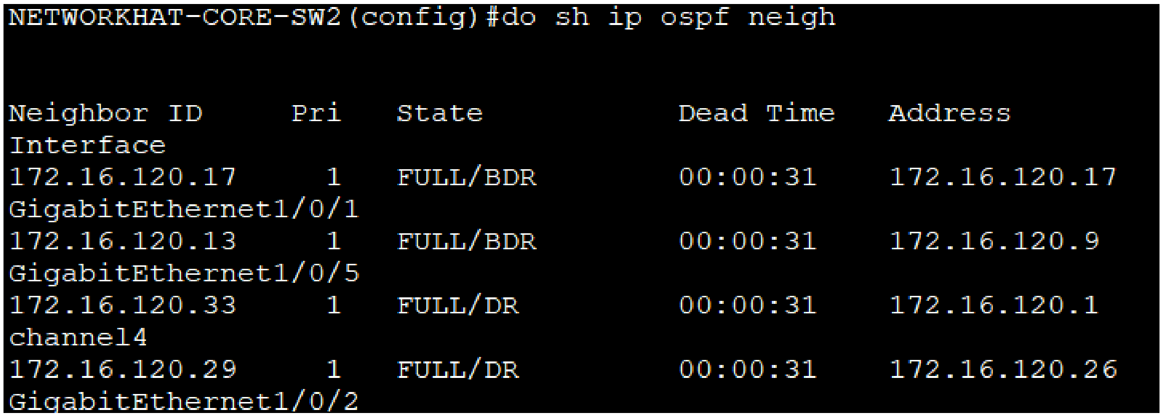
OSPF neighborship of NETWORKHAT-CORE-SW1

Core R2



```
NETWORKHAT-CORE-SW2(config)#do sh run | sec ospf
router ospf 90
 log-adjacency-changes
 network 172.16.120.0 0.0.0.3 area 2
 network 172.16.120.16 0.0.0.3 area 2
 network 172.16.120.8 0.0.0.3 area 2
 network 172.16.120.24 0.0.0.3 area 0
```

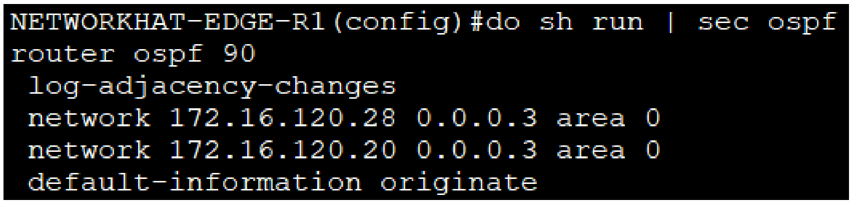
Running config of OSPF configuration of NETWORKHAT-CORE-SW2



```
NETWORKHAT-CORE-SW2(config)#do sh ip ospf neigh


Neighbor ID     Pri   State           Dead Time   Address
Interface
172.16.120.17     1   FULL/BDR        00:00:31    172.16.120.17
GigabitEthernet1/0/1
172.16.120.13     1   FULL/BDR        00:00:31    172.16.120.9
GigabitEthernet1/0/5
172.16.120.33     1   FULL/DR         00:00:31    172.16.120.1
channel4
172.16.120.29     1   FULL/DR         00:00:31    172.16.120.26
GigabitEthernet1/0/2
```

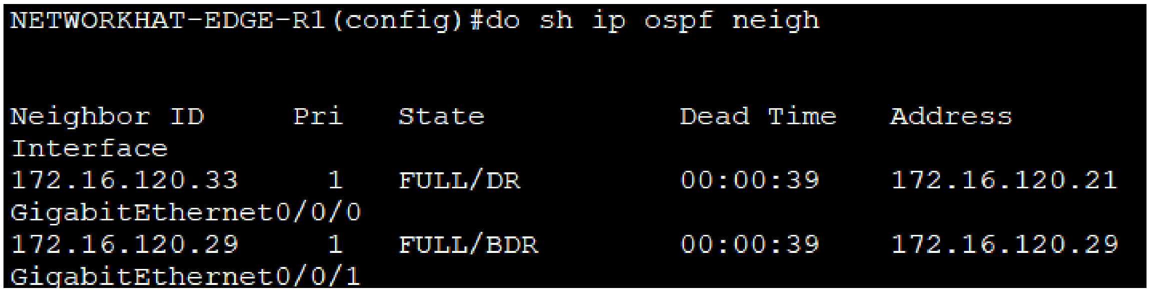
OSPF neighborship of NETWORKHAT-CORE-SW2

EDGE R1



```
NETWORKHAT-EDGE-R1(config)#do sh run | sec ospf
router ospf 90
 log-adjacency-changes
 network 172.16.120.28 0.0.0.3 area 0
 network 172.16.120.20 0.0.0.3 area 0
 default-information originate
```

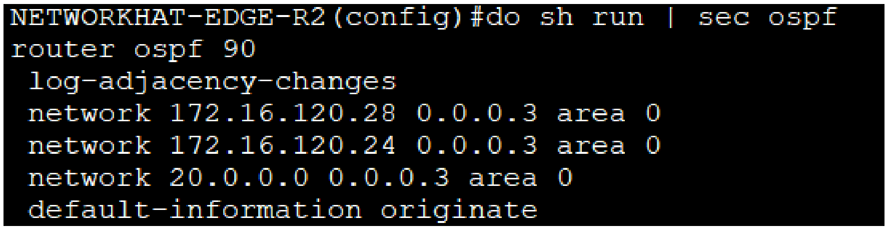
OSPF config in NETWORKHAT-EDGE-R1



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


Neighbor ID     Pri   State           Dead Time   Address
Interface
172.16.120.33     1   FULL/DR         00:00:39    172.16.120.21
GigabitEthernet0/0/0
172.16.120.29     1   FULL/BDR        00:00:39    172.16.120.29
GigabitEthernet0/0/1
```

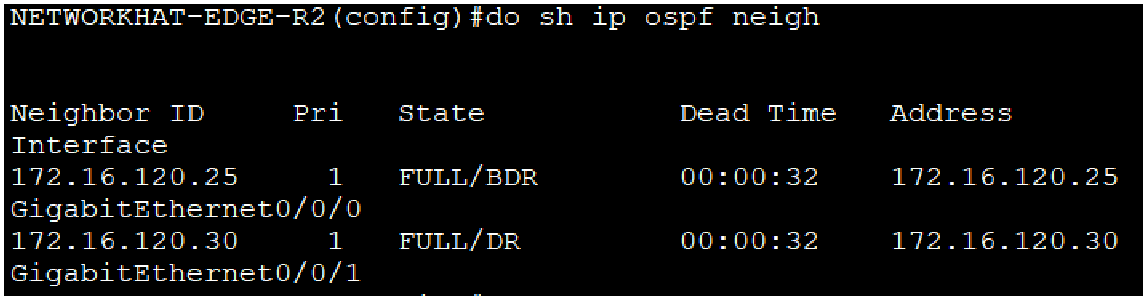
OSPF neighborship of NETWORKHAT-EDGE-R1

EDGE R2



```
NETWORKHAT-EDGE-R2(config)#do sh run | sec ospf
router ospf 90
 log-adjacency-changes
 network 172.16.120.28 0.0.0.3 area 0
 network 172.16.120.24 0.0.0.3 area 0
 network 20.0.0.0 0.0.0.3 area 0
 default-information originate
```

OSPF config in NETWORKHAT-EDGE-R2



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


Neighbor ID     Pri   State           Dead Time   Address
Interface
172.16.120.25     1   FULL/BDR        00:00:32    172.16.120.25
GigabitEthernet0/0/0
172.16.120.30     1   FULL/DR         00:00:32    172.16.120.30
GigabitEthernet0/0/1
```

OSPF neighborship of NETWORKHAT-EDGE-R2

RIP

One of the first and most basic distance-vector routing protocols used in computer networks is Routing Information Protocol. As a Part of the Interior Gateway Protocol (IGP) family, it was created to facilitate the dynamic exchange of routing data between routers on a local network.

Advantages of rip

- Simplicity: RIP is straightforward and easy to configure. Its simplicity makes it a good choice for small to medium-sized networks with relatively uncomplicated topologies.
- Low Overhead: RIP has low overhead in terms of processing power and memory requirements. This makes it suitable for less powerful routers or networks with resource constraints.
- Ease of Implementation: Setting up RIP is generally quick and easy. Its simplicity facilitates rapid implementation and troubleshooting, which can be advantageous in certain scenarios.

Disadvantages of RIP

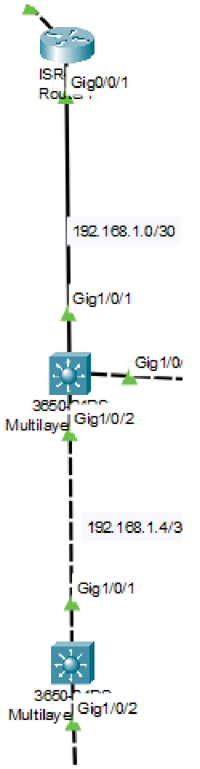
Hop Count Limitation: RIP has a maximum hop count limit of 15. If a route exceeds this limit, it is considered unreachable. This limitation makes RIP unsuitable for large networks or networks with complex topologies where the hop count may be greater than 15.

- Slow Convergence: RIP relies on periodic updates, typically every 30 seconds, to share routing information. In the event of a network topology change, it can take several update cycles for routers to converge to a new routing table. This slow convergence can result in suboptimal routing paths and increased downtime during network changes.

- Inefficient Use of Bandwidth: RIP sends periodic updates regardless of whether the network topology has changed or not. In larger networks, this continuous exchange of routing information consumes bandwidth that could be used for data traffic.
- Limited Scalability: RIP may struggle to scale effectively in larger networks with numerous routers and subnets. The frequent exchange of routing updates and the limited hop count can become significant issues in such environments.

EIGRP

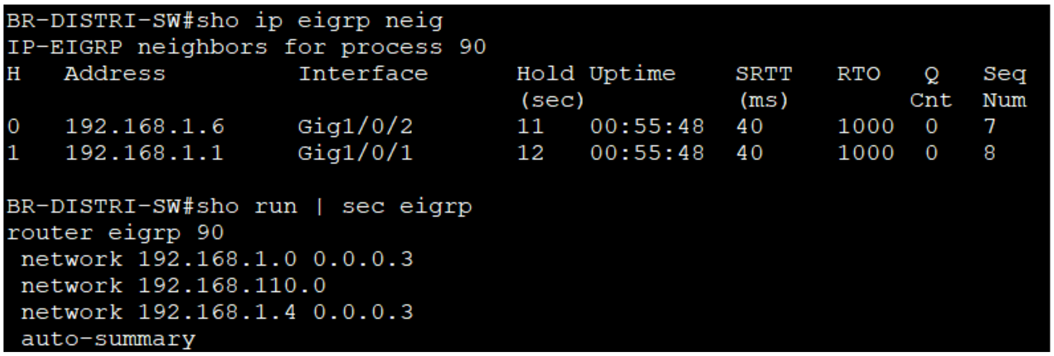
BRANCH



Cisco Systems created the sophisticated and exclusive Enhanced Interior Gateway Routing Protocol. It is designed for routing within enterprise networks and is classified as an Interior Gateway Protocol (IGP). EIGRP is an improvement upon the older IGRP (Interior Gateway Routing Protocol) and is known for its efficiency, fast convergence, and support for various network technologies.

Although both RIP (Routing Information Protocol) and EIGRP (Enhanced Interior Gateway Routing Protocol) are interior gateway protocols, their capabilities and design philosophies differ. EIGRP is often considered more advanced and offers several advantages over RIP, making it a better choice in certain network environments. Here are some reasons why EIGRP might be considered better than RIP:

- Advanced Metric Calculation: EIGRP uses a more sophisticated metric calculation compared to RIP. EIGRP's metric considers multiple factors such as bandwidth, delay, reliability, and load. This allows for more precise and informed routing decisions based on the actual characteristics of the network links.
- Fast Convergence: EIGRP is designed for fast convergence. It can quickly adapt to changes in the network topology, finding alternate routes and avoiding disruptions in network connectivity.
- Efficient Use of Bandwidth: EIGRP uses bandwidth efficiently by only sending updates when there is a change in the network. This reduces unnecessary traffic and is more scalable in larger networks compared to RIP, which sends periodic updates regardless of topology changes.



```
BR-DISTRI-SW#sho ip eigrp neig
IP-EIGRP neighbors for process 90
H   Address         Interface      Hold Uptime    SRTT   RTO   Q    Seq
                                   (sec)          (ms)        Cnt   Num
0   192.168.1.6     Gig1/0/2       11   00:55:48  40     1000  0    7
1   192.168.1.1     Gig1/0/1       12   00:55:48  40     1000  0    8

BR-DISTRI-SW#sho run | sec eigrp
router eigrp 90
 network 192.168.1.0 0.0.0.3
 network 192.168.110.0
 network 192.168.1.4 0.0.0.3
 auto-summary
```

Static routing

The process of manually setting up a computer's routing table or a network router to specify certain pathways for network traffic is known as static routing. Static routing requires administrators to manually define the routes, in contrast to dynamic routing protocols, which use information exchanged by routers to identify the optimal pathways automatically.

Static routing has both advantages and disadvantages. Understanding these can help network administrators make informed decisions about whether to use static routing in each network environment.

Advantages of Static Routing:

- Simplicity and Ease of Configuration: Static routing is easy to configure and understand. It is straightforward, making it a good choice for simple network topologies and for administrators who prefer manual control over routing decisions.
- Low Overhead: Static routing has lower processing overhead compared to dynamic routing protocols. There are no periodic updates or dynamic calculations, which can be beneficial in smaller networks with stable topologies.

Disadvantages of Static Routing

- Lack of Adaptability: Static routes do not adapt to changes in the network topology. If there are changes, such as link failures or additions, administrators must manually update the static routes. This lack of adaptability can be a significant limitation in dynamic environments.

- Maintenance Challenges: As the network grows or undergoes changes, maintaining static routes across numerous devices can become cumbersome. Keeping the routing information accurate and up to date may require more effort.

Default routing

Default route is a configuration on a router that defines a path to use for traffic when no specific route matches the destination address. In other words, it is a route that serves as a fallback or default path for packets that do not match any more specific routes in the router's routing table.

Default routing, like any networking concept, comes with its set of advantages and disadvantages. Comprehending these can aid in making knowledgeable selections about the implementation of default routing in any network setting.

Advantages of Default Routing

- Simplicity: Default routing simplifies network configuration by providing a single route to handle all traffic with no matching specific routes. This simplicity is especially valuable in smaller networks or for routers serving as the gateway to the Internet.
- Reduced Routing Table Size: By using a default route, the size of the routing table is reduced, especially in cases where there are many possible destinations. This can lead to more efficient memory usage on routers.

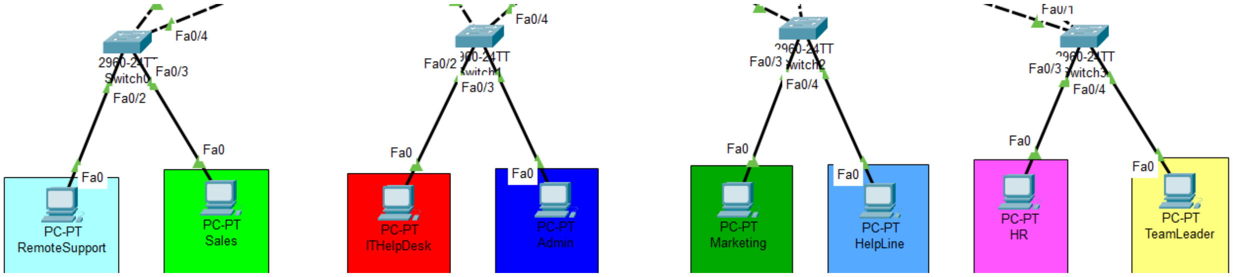
Disadvantages of Default Routing

Default routing has some downsides. It treats all unknown destinations the same, which might not work well for networks with different routing needs. There's a risk of security problems if not set up carefully – a mistake could send traffic to unauthorized or bad places. Depending only on one route is risky too; if that route fails, all the traffic using it is in trouble. Default routing also makes it hard for network administrators to see how traffic is moving through the network. In networks with multiple service providers, default routing might not give enough control for managing traffic efficiently across different exit points. So, while default routing is common, it's important to be aware of these issues and consider other options for better network performance and security.

Part B

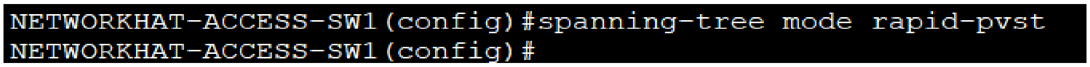
VLAN segregation

VLAN (Virtual Local Area Network) segregation is the process of setting up distinct VLANs for each network device to improve administration, performance, and security. VLANs are logical partitions within a physical network, allowing administrators to group devices based on their functional roles or security requirements. Segregating VLANs helps isolate broadcast domains, control network traffic, and improve overall network efficiency.

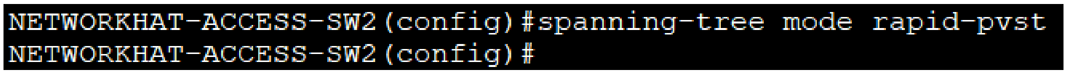


STP

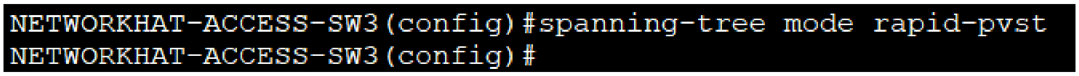
Spanning Tree Protocol is a network protocol used to prevent loops in Ethernet networks. Ethernet networks are susceptible to loops, which can cause broadcast storms and degrade network performance. STP is part of the IEEE 802.1D standard and is designed to ensure a loop-free topology in Ethernet networks.



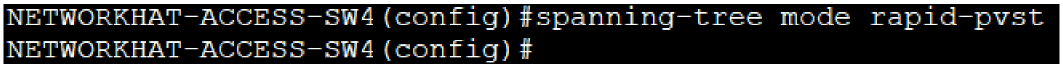
```
NETWORKHAT-ACCESS-SW1(config)#spanning-tree mode rapid-pvst
NETWORKHAT-ACCESS-SW1(config)#
```



```
NETWORKHAT-ACCESS-SW2(config)#spanning-tree mode rapid-pvst
NETWORKHAT-ACCESS-SW2(config)#
```



```
NETWORKHAT-ACCESS-SW3(config)#spanning-tree mode rapid-pvst
NETWORKHAT-ACCESS-SW3(config)#
```



```
NETWORKHAT-ACCESS-SW4(config)#spanning-tree mode rapid-pvst
NETWORKHAT-ACCESS-SW4(config)#
```

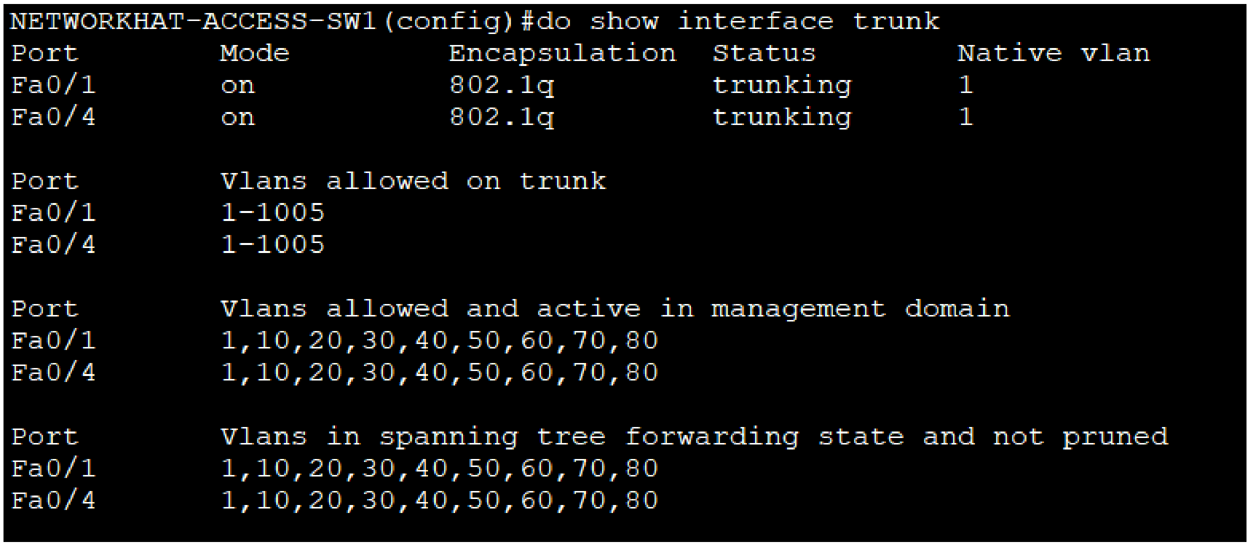
The Per-Vlan Spanning Tree Protocol is activated on each of the four access switches at the L2 layer of the network design. Every network VLAN is assigned a unique spanning tree instance. Because the switch will keep up a unique spanning tree for every VLAN, this enables VLAN-based redundancy and loop prevention.

Trunk port

A network port that is set up to simultaneously transport traffic for several VLANs (Virtual Local Area Networks) is known as a trunk port. Trunking is a technique used in network environments, especially in Ethernet networks, to enable the transportation of VLAN-tagged frames between network devices, such as switches and routers.

Trucking in L2 Switches

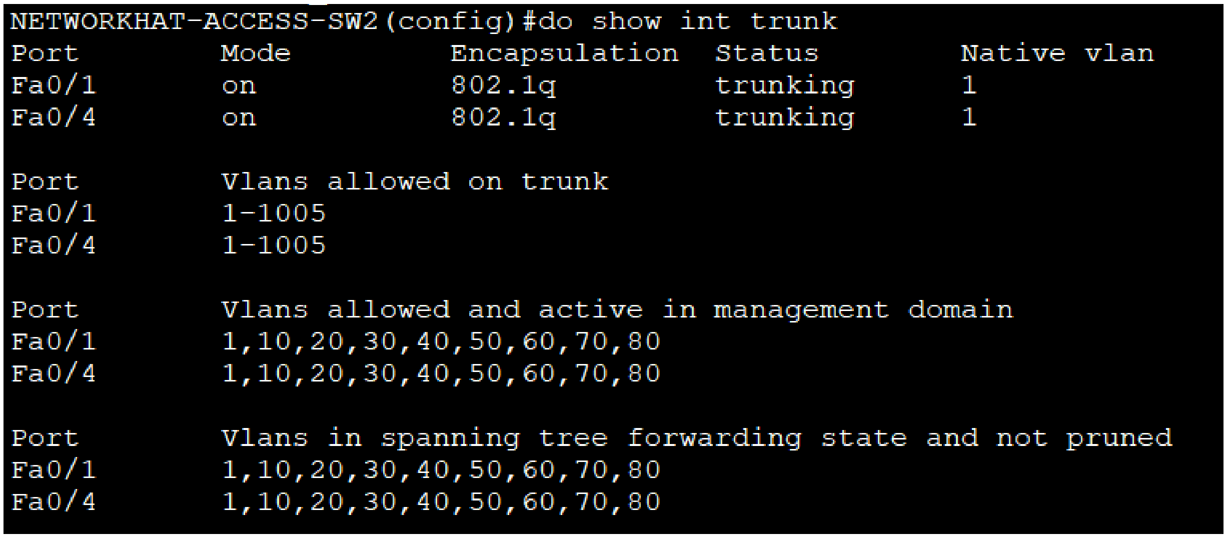
NETWORKHAT-ACCESS-SW1



```
NETWORKHAT-ACCESS-SW1(config)#do show interface trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      1
Fa0/4       on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/1       1-1005
Fa0/4       1-1005

Port        Vlans allowed and active in management domain
Fa0/1       1,10,20,30,40,50,60,70,80
Fa0/4       1,10,20,30,40,50,60,70,80

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,10,20,30,40,50,60,70,80
Fa0/4       1,10,20,30,40,50,60,70,80
```

To transfer information from various Vlans, the ports {Fa0/1 and Fa0/4} are configured as trunks. This snapshot displays the Vlan IDs that port {Fa0/1 & Fa0/4} carries. The topological network of the headquarters uses four L2 Access switches in total. Each of the other three access switches goes through a similar process.

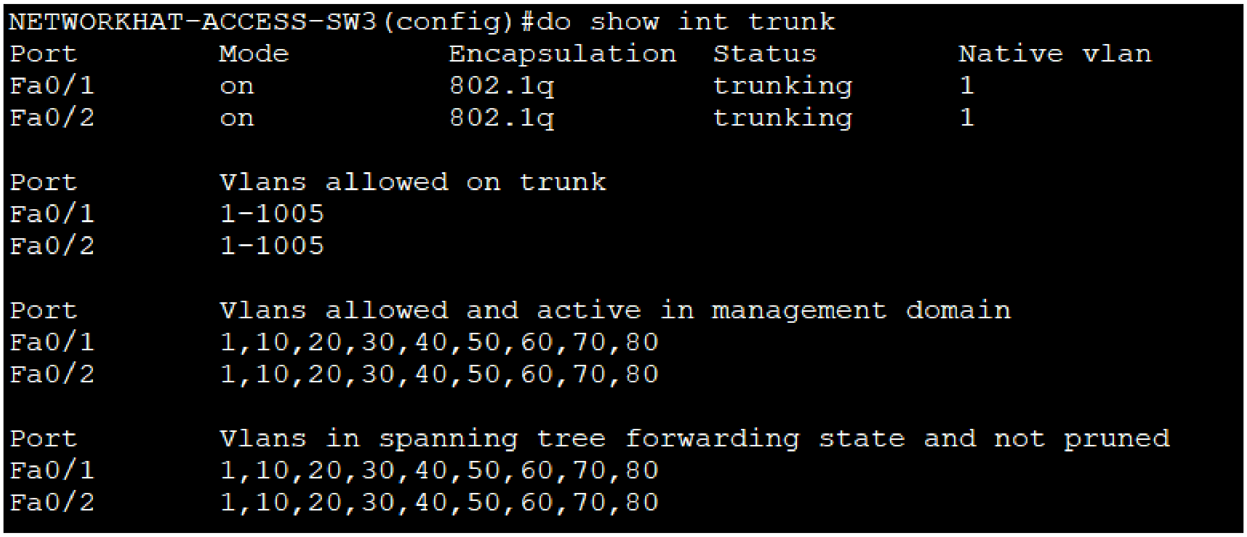
NETWORKHAT-ACCESS-SW2



```
NETWORKHAT-ACCESS-SW2(config)#do show int trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      1
Fa0/4       on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/1       1-1005
Fa0/4       1-1005

Port        Vlans allowed and active in management domain
Fa0/1       1,10,20,30,40,50,60,70,80
Fa0/4       1,10,20,30,40,50,60,70,80

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,10,20,30,40,50,60,70,80
Fa0/4       1,10,20,30,40,50,60,70,80
```

To transfer information from various Vlans, the ports {Fa0/1 and Fa0/4} are configured as trunks. This snapshot displays the Vlan IDs that port {Fa0/1 & Fa0/4} carries. The topological network of the headquarters uses four L2 Accessswitches in total. Each of the other three access switches goes through a similar process.

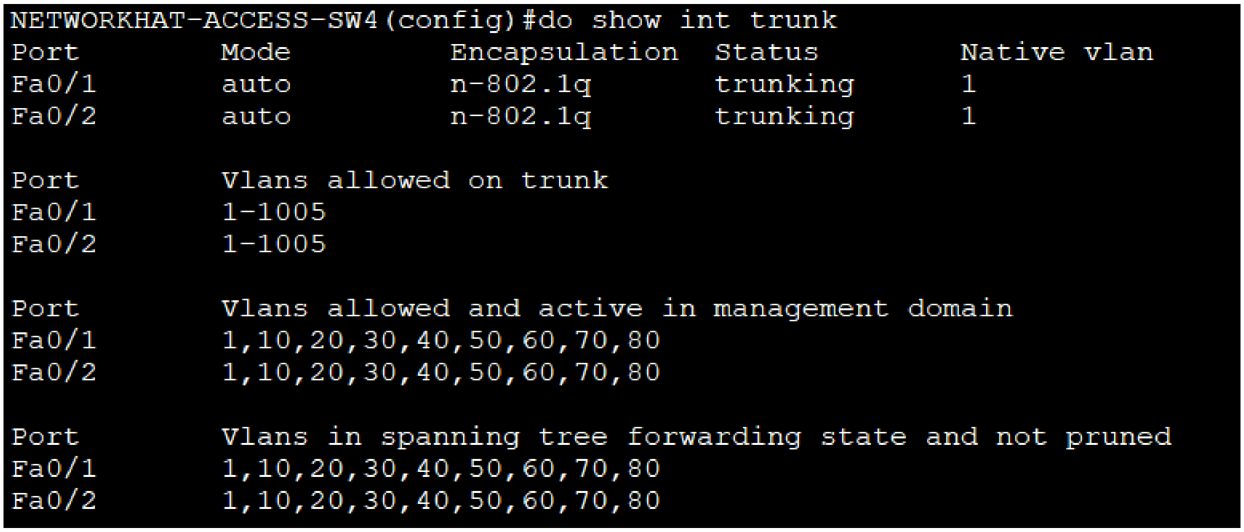
NETWORKHAT-ACCESS-SW3



```
NETWORKHAT-ACCESS-SW3(config)#do show int trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      1
Fa0/2       on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/1       1-1005
Fa0/2       1-1005

Port        Vlans allowed and active in management domain
Fa0/1       1,10,20,30,40,50,60,70,80
Fa0/2       1,10,20,30,40,50,60,70,80

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,10,20,30,40,50,60,70,80
Fa0/2       1,10,20,30,40,50,60,70,80
```

To transfer information from various Vlans, the ports {Fa0/1 and Fa0/2} are configured as trunks. This snapshot displays the Vlan IDs that port {Fa0/1 & Fa0/2} carries. The topological network of the headquarters uses four L2 Accessswitches in total. Each of the other three access switches goes through a similar process.

NETWORKHAT-ACCESS-SW4

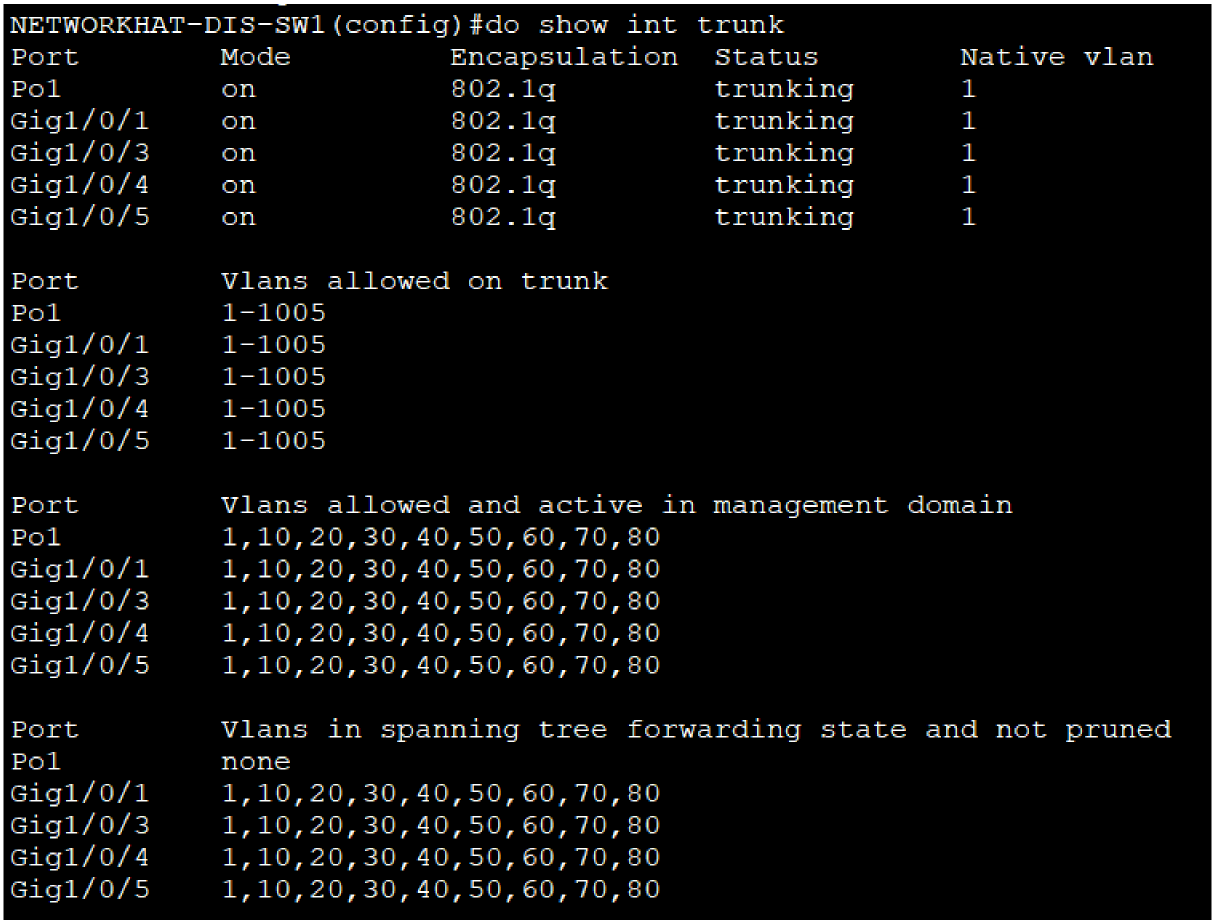


```
NETWORKHAT-ACCESS-SW4(config)#do show int trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       auto         n-802.1q       trunking      1
Fa0/2       auto         n-802.1q       trunking      1

Port        Vlans allowed on trunk
Fa0/1       1-1005
Fa0/2       1-1005

Port        Vlans allowed and active in management domain
Fa0/1       1,10,20,30,40,50,60,70,80
Fa0/2       1,10,20,30,40,50,60,70,80

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,10,20,30,40,50,60,70,80
Fa0/2       1,10,20,30,40,50,60,70,80
```

To transfer information from various Vlans, the ports {Fa0/1 and Fa0/2} are configured as trunks. This snapshot displays the Vlan IDs that port {Fa0/1 & Fa0/2} carries. The topological network of the headquarters uses four L2 Accessswitches in total. Each of the other three access switches goes through a similar process.

Trucking in L3 switches

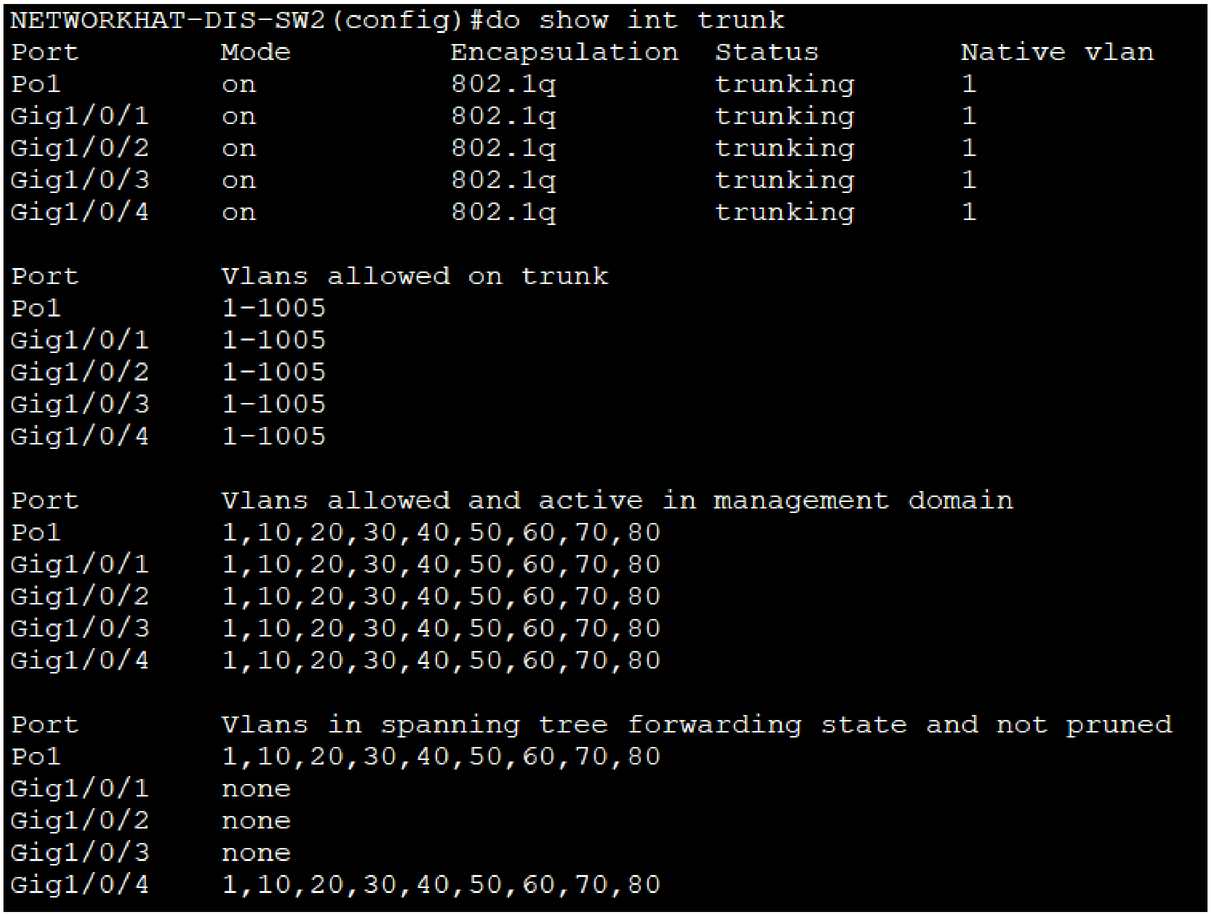
NETWORKHAT-DIS-SW1



```
NETWORKHAT-DIS-SW1(config)#do show int trunk
Port        Mode         Encapsulation  Status        Native vlan
Po1         on           802.1q         trunking      1
Gig1/0/1    on           802.1q         trunking      1
Gig1/0/3    on           802.1q         trunking      1
Gig1/0/4    on           802.1q         trunking      1
Gig1/0/5    on           802.1q         trunking      1

Port        Vlans allowed on trunk
Po1         1-1005
Gig1/0/1    1-1005
Gig1/0/3    1-1005
Gig1/0/4    1-1005
Gig1/0/5    1-1005

Port        Vlans allowed and active in management domain
Po1         1,10,20,30,40,50,60,70,80
Gig1/0/1    1,10,20,30,40,50,60,70,80
Gig1/0/3    1,10,20,30,40,50,60,70,80
Gig1/0/4    1,10,20,30,40,50,60,70,80
Gig1/0/5    1,10,20,30,40,50,60,70,80

Port        Vlans in spanning tree forwarding state and not pruned
Po1         none
Gig1/0/1    1,10,20,30,40,50,60,70,80
Gig1/0/3    1,10,20,30,40,50,60,70,80
Gig1/0/4    1,10,20,30,40,50,60,70,80
Gig1/0/5    1,10,20,30,40,50,60,70,80
```

The information about NETWORKHAT-DIS-SW1's trunking is seen above. It also yields information about the vlans that NETWORKHAT-DIS-SW1 carries. It is evident that the channel group created by NETWORKHAT-DIS-SW1 & NETWORKHAT-DIS-SW2, which is likewise made trunk

NETWORKHAT-DIS-SW2

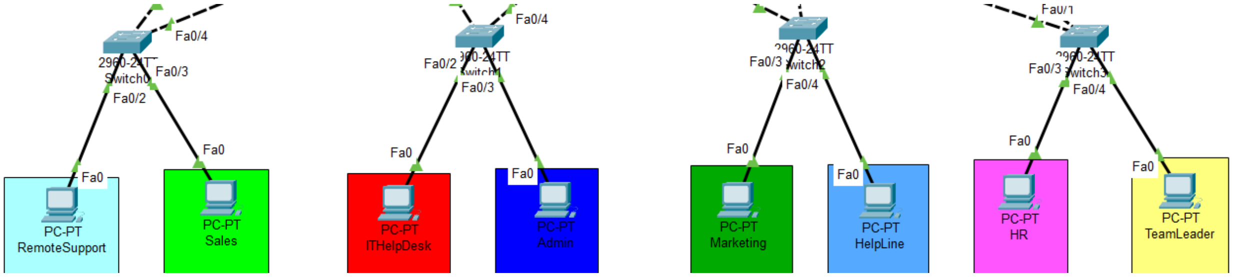


```
NETWORKHAT-DIS-SW2(config)#do show int trunk
Port        Mode         Encapsulation  Status        Native vlan
Po1         on           802.1q         trunking      1
Gig1/0/1    on           802.1q         trunking      1
Gig1/0/2    on           802.1q         trunking      1
Gig1/0/3    on           802.1q         trunking      1
Gig1/0/4    on           802.1q         trunking      1

Port        Vlans allowed on trunk
Po1         1-1005
Gig1/0/1    1-1005
Gig1/0/2    1-1005
Gig1/0/3    1-1005
Gig1/0/4    1-1005

Port        Vlans allowed and active in management domain
Po1         1,10,20,30,40,50,60,70,80
Gig1/0/1    1,10,20,30,40,50,60,70,80
Gig1/0/2    1,10,20,30,40,50,60,70,80
Gig1/0/3    1,10,20,30,40,50,60,70,80
Gig1/0/4    1,10,20,30,40,50,60,70,80

Port        Vlans in spanning tree forwarding state and not pruned
Po1         1,10,20,30,40,50,60,70,80
Gig1/0/1    none
Gig1/0/2    none
Gig1/0/3    none
Gig1/0/4    1,10,20,30,40,50,60,70,80
```

The information about NETWORKHAT-DIS-SW2's trunking is seen above. It also yields information about the vlans that NETWORKHAT-DIS-SW2 carries. It is evident that the channel group created by NETWORKHAT-DIS-SW1 & NETWORKHAT-DIS-SW2, which is likewise made trunk.

Access port

A switch's network port designated for a particular VLAN (Virtual Local Area Network) is known as an access port. An access port is set to belong to a single VLAN, hence giving connection to devices inside that VLAN, in contrast to trunk ports, which may transport traffic for many VLANs. Access ports are commonly used to connect end-user devices, such as computers, printers, or IP phones, to a switch.

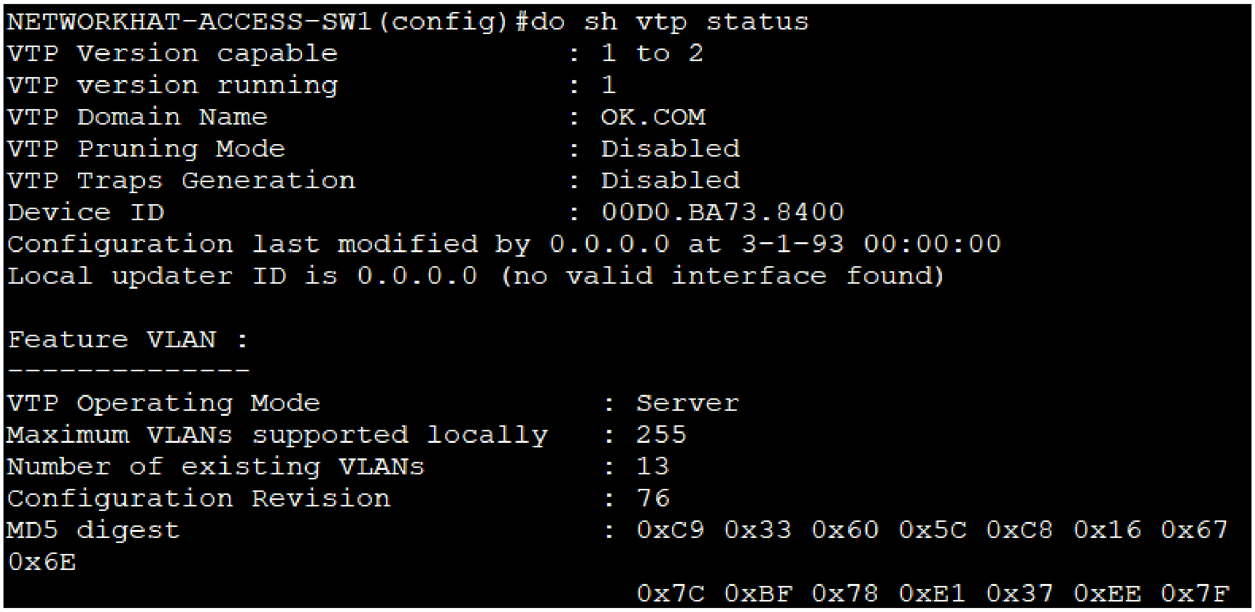


Within the network architecture, the Access Layer comprises four L2 switches and eight PCs, one per department. The configuration of Layer 2 Vlan will include stp, trunking, and Vlan Trunking Protocol (VTP).

VPT

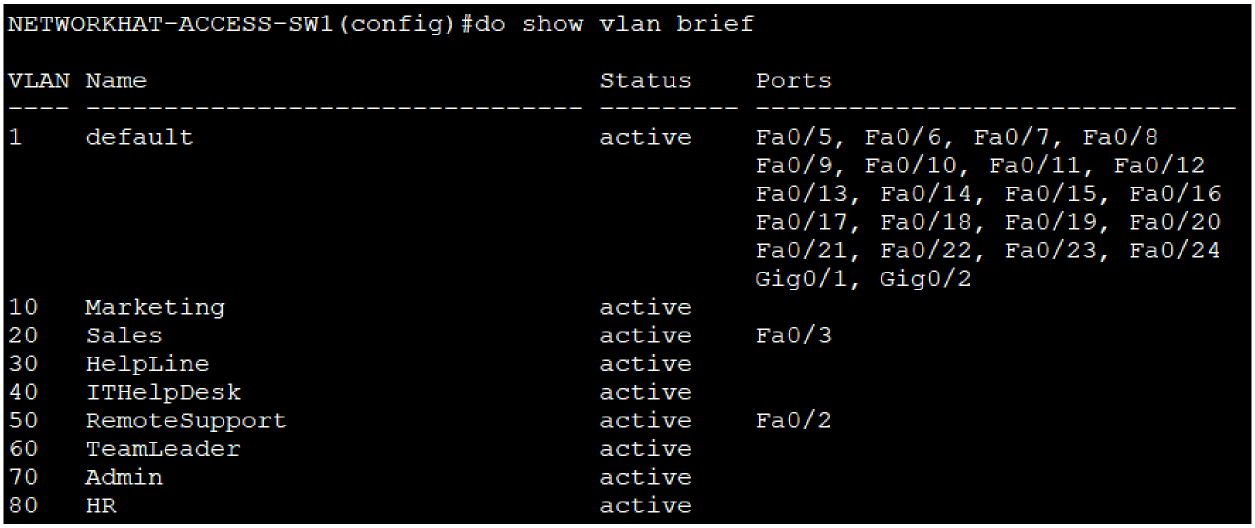
A proprietary protocol from Cisco called VLAN Trunking Protocol (VTP) spreads the definition of Virtual Local Area Networks (VLAN) over the whole local area network.

Virtual Local Area Networks (VLANs) are defined by a proprietary Cisco protocol called VLAN Trunking Protocol (VTP), which is applied throughout the whole local area network. VTP gives each switch inside a VTP domain access to VLAN information.



```
NETWORKHAT-ACCESS-SW1(config)#do sh vtp status
VTP Version capable             : 1 to 2
VTP version running             : 1
VTP Domain Name                 : OK.COM
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : 00D0.BA73.8400
Configuration last modified by 0.0.0.0 at 3-1-93 00:00:00
Local updater ID is 0.0.0.0 (no valid interface found)

Feature VLAN :
--------------
VTP Operating Mode                : Server
Maximum VLANs supported locally   : 255
Number of existing VLANs          : 13
Configuration Revision            : 76
MD5 digest                        : 0xC9 0x33 0x60 0x5C 0xC8 0x16 0x67
0x6E
                                    0x7C 0xBF 0x78 0xE1 0x37 0xEE 0x7F
```

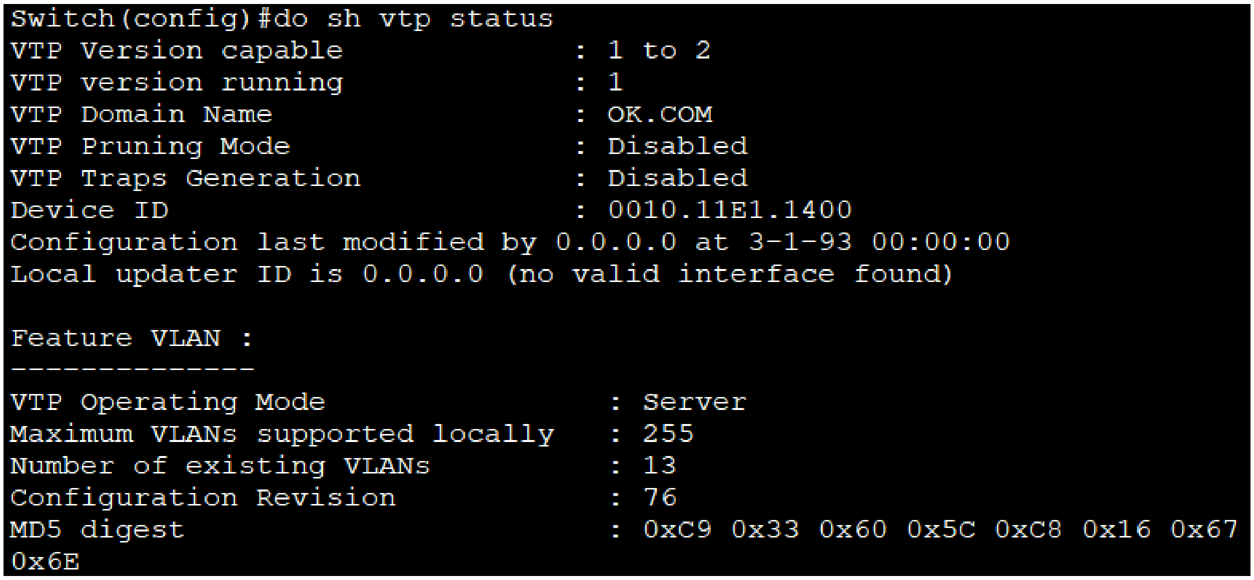
As you can see in the figure VTP 1 version is running with the domain name ok.com. The VTP is operating in server mode.



```
NETWORKHAT-ACCESS-SW1(config)#do show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                Gig0/1, Gig0/2
10   Marketing                        active
20   Sales                            active    Fa0/3
30   HelpLine                         active
40   ITHelpDesk                       active
50   RemoteSupport                    active    Fa0/2
60   TeamLeader                       active
70   Admin                            active
80   HR                               active
```

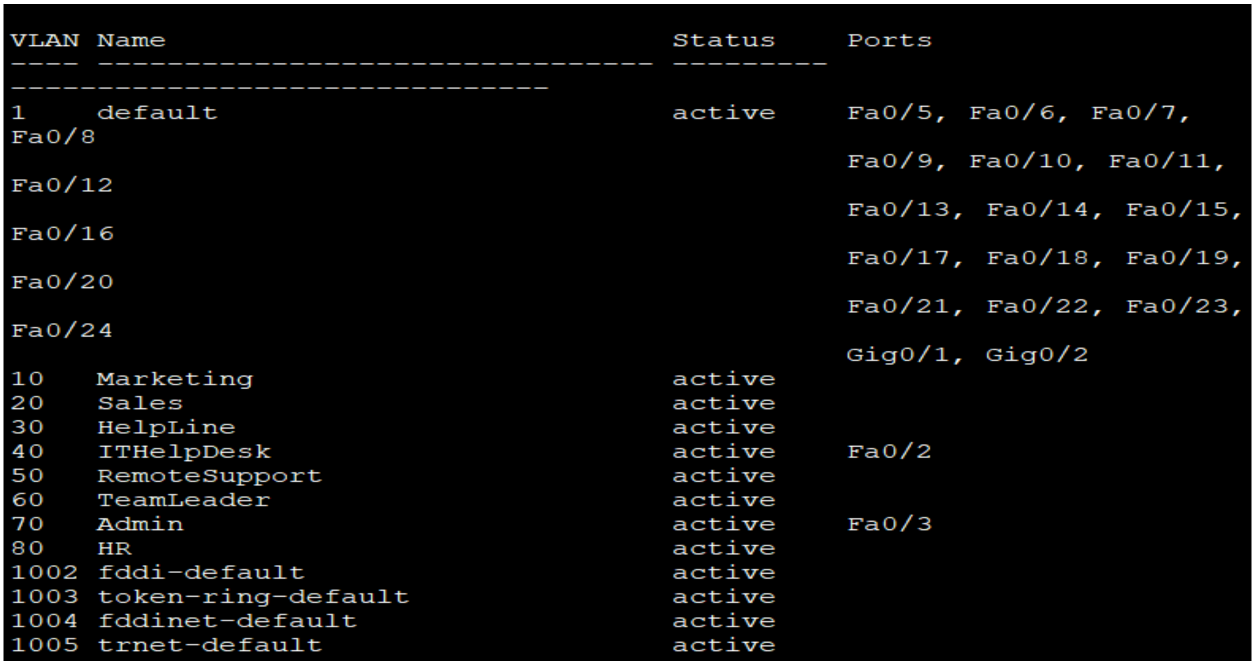
As VTP is implemented, the four L2 switches communicate vlan information, as seen in the image. As seen in the screenshot, traffic for vlans 50 and 20 is carried across access-ports {fa0/2} and {fa0/3}, respectively. Sales is the name of Vlan 20, while Remotesupport is the name of Vlan 50.

VTP in Networkhat-access-sw2



```
Switch(config)#do sh vtp status
VTP Version capable             : 1 to 2
VTP version running             : 1
VTP Domain Name                 : OK.COM
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : 0010.11E1.1400
Configuration last modified by 0.0.0.0 at 3-1-93 00:00:00
Local updater ID is 0.0.0.0 (no valid interface found)

Feature VLAN :
--------------
VTP Operating Mode                : Server
Maximum VLANs supported locally   : 255
Number of existing VLANs          : 13
Configuration Revision            : 76
MD5 digest                        : 0xC9 0x33 0x60 0x5C 0xC8 0x16 0x67
0x6E
```

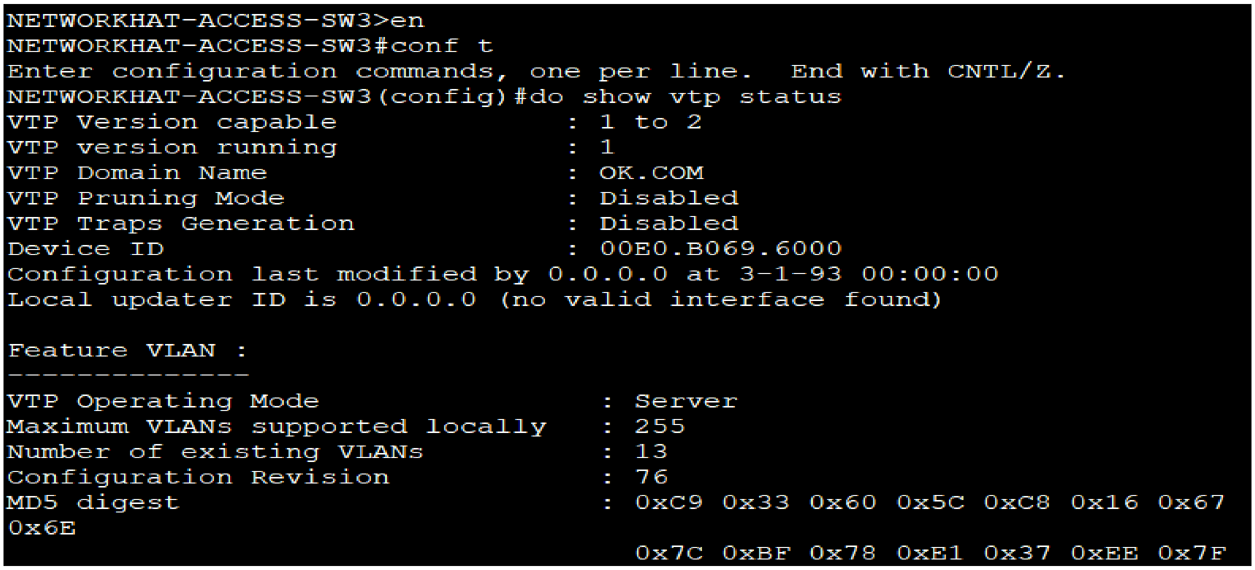
As you can see in the figure VTP 1 version is running with the domain name ok.com. The VTP is operating in server mode



```
VLAN Name                             Status    Ports
---- -------------------------------- ---------
-------------------------------
1    default                          active    Fa0/5, Fa0/6, Fa0/7,
Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11,
Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15,
Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19,
Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23,
Fa0/24
                                                Gig0/1, Gig0/2
10   Marketing                        active
20   Sales                            active
30   HelpLine                         active
40   ITHelpDesk                       active    Fa0/2
50   RemoteSupport                    active
60   TeamLeader                       active
70   Admin                            active    Fa0/3
80   HR                               active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

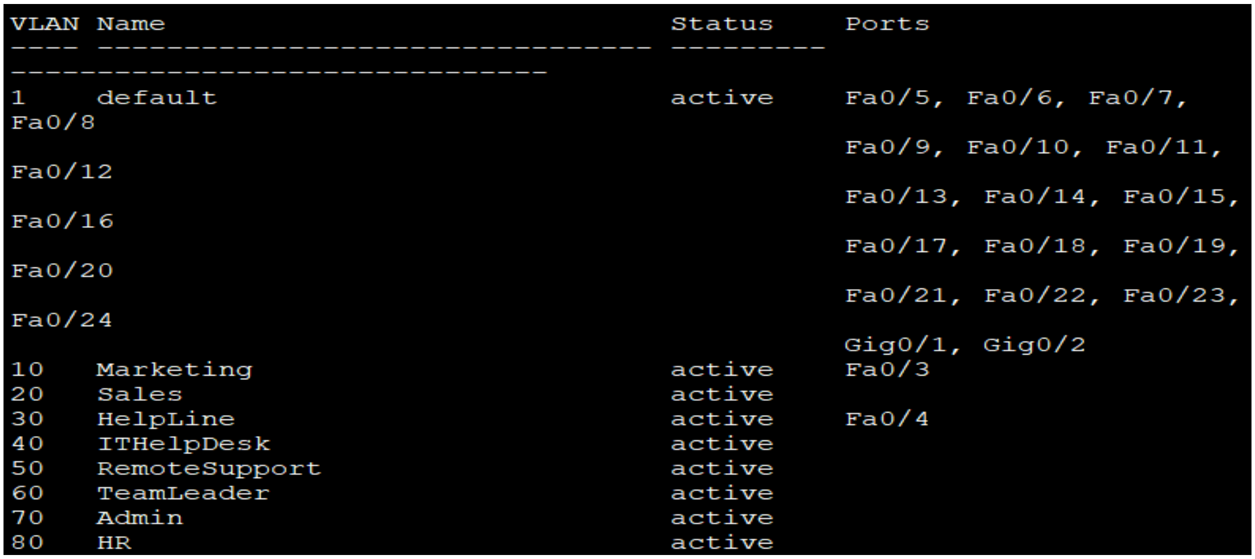
As VTP is deployed, vlan information is exchanged throughout the four L2 switches, as the screenshot illustrates. Traffic for vlans 40 and 70 is transported via access-ports, as can be seen in the screenshot. {fa0/2} and {fa0/3}, respectively. ITHelpDesk is the name of Vlan 40, while Admin is the name of Vlan 70.

VTP in Networkhat-access-sw3



```
NETWORKHAT-ACCESS-SW3>en
NETWORKHAT-ACCESS-SW3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
NETWORKHAT-ACCESS-SW3(config)#do show vtp status
VTP Version capable             : 1 to 2
VTP version running             : 1
VTP Domain Name                 : OK.COM
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : 00E0.B069.6000
Configuration last modified by 0.0.0.0 at 3-1-93 00:00:00
Local updater ID is 0.0.0.0 (no valid interface found)

Feature VLAN :
--------------
VTP Operating Mode                : Server
Maximum VLANs supported locally   : 255
Number of existing VLANs          : 13
Configuration Revision            : 76
MD5 digest                        : 0xC9 0x33 0x60 0x5C 0xC8 0x16 0x67
0x6E
                                    0x7C 0xBF 0x78 0xE1 0x37 0xEE 0x7F
```

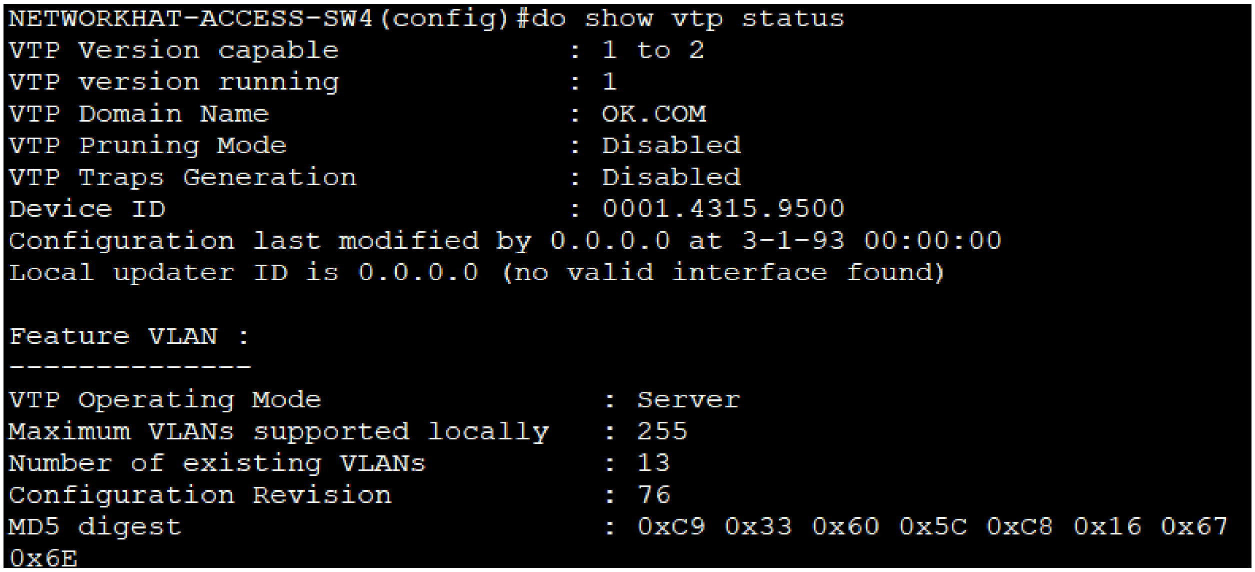
As you can see in the figure VTP 1 version is running with the domain name ok.com. The VTP is operating in server mode



```
VLAN Name                             Status    Ports
---- -------------------------------- ---------
-------------------------------
1    default                          active    Fa0/5, Fa0/6, Fa0/7,
Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11,
Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15,
Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19,
Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23,
Fa0/24
                                                Gig0/1, Gig0/2
10   Marketing                        active    Fa0/3
20   Sales                            active
30   HelpLine                         active    Fa0/4
40   ITHelpDesk                       active
50   RemoteSupport                    active
60   TeamLeader                       active
70   Admin                            active
80   HR                               active
```

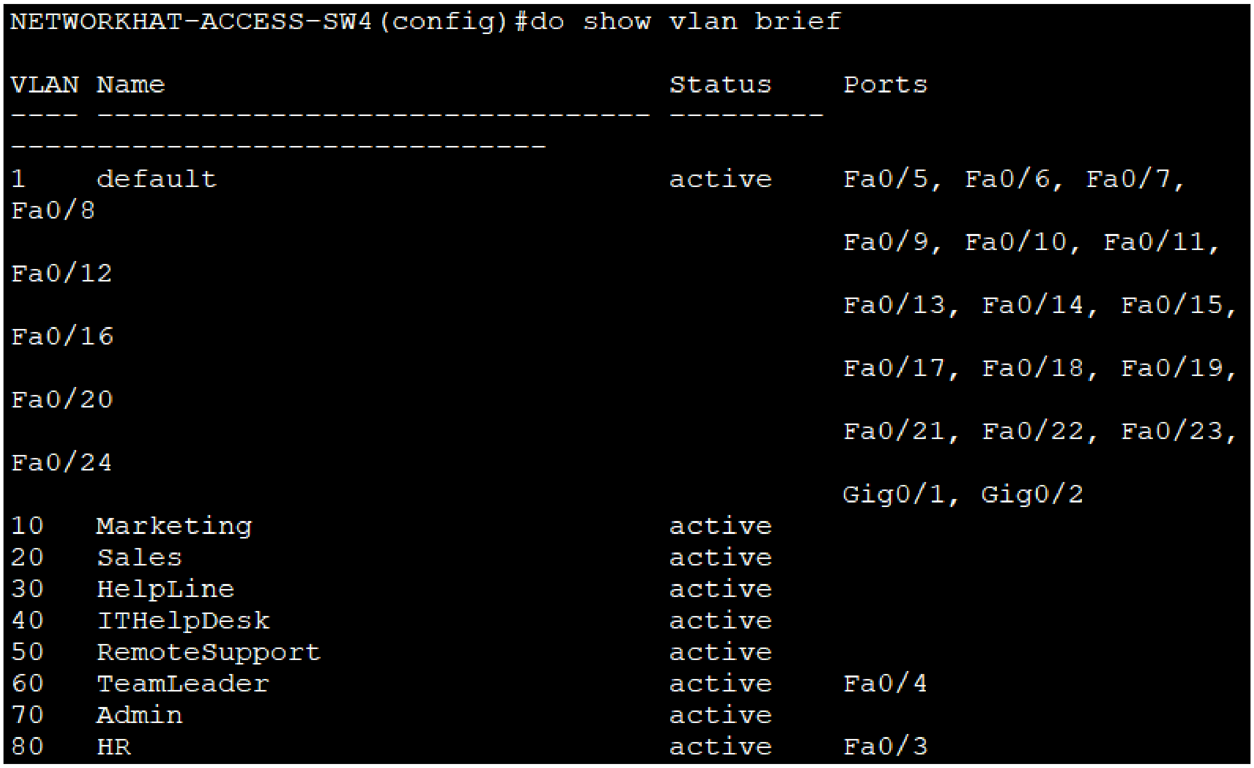
As VTP is deployed, vlan information is exchanged throughout the four L2 switches, as the screenshot illustrates Traffic for vlans 40 and 70 is transported via access-ports, as can be seen in the screenshot. {fa0/3} and {fa0/4}, respectively. Marketing is the name of Vlan 10, while Helpline is the name of Vlan 30.

VTP in Networkhat-access-sw4



```
NETWORKHAT-ACCESS-SW4(config)#do show vtp status
VTP Version capable             : 1 to 2
VTP version running             : 1
VTP Domain Name                 : OK.COM
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : 0001.4315.9500
Configuration last modified by 0.0.0.0 at 3-1-93 00:00:00
Local updater ID is 0.0.0.0 (no valid interface found)

Feature VLAN :
--------------
VTP Operating Mode                : Server
Maximum VLANs supported locally   : 255
Number of existing VLANs          : 13
Configuration Revision            : 76
MD5 digest                        : 0xC9 0x33 0x60 0x5C 0xC8 0x16 0x67
0x6E
```

As you can see in the figure VTP 1 version is running with the domain name ok.com. The VTP is operating in server mode

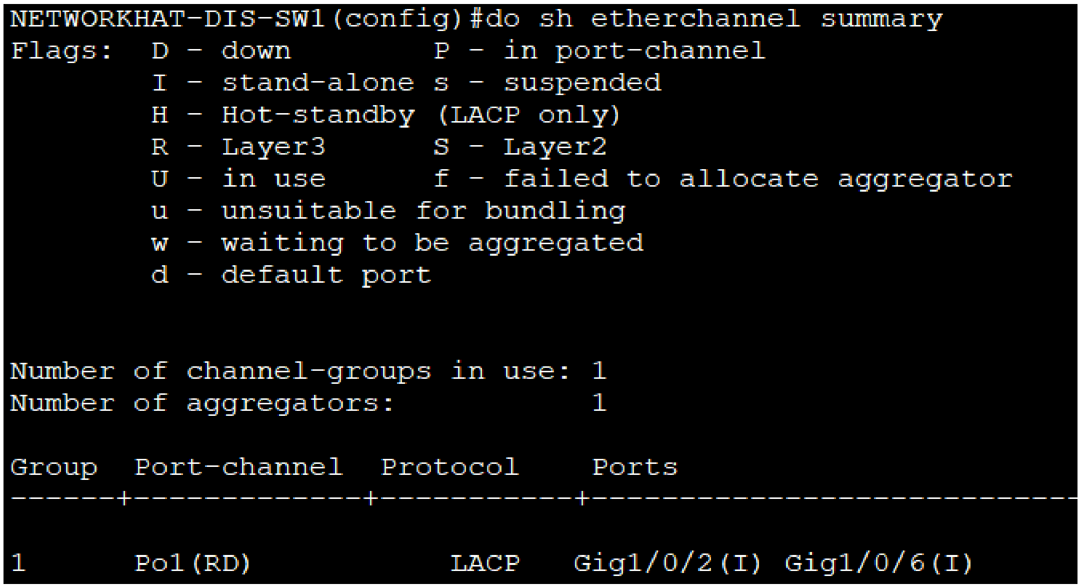


```
NETWORKHAT-ACCESS-SW4(config)#do show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- ---------
-------------------------------
1    default                          active    Fa0/5, Fa0/6, Fa0/7,
Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11,
Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15,
Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19,
Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23,
Fa0/24
                                                Gig0/1, Gig0/2
10   Marketing                        active
20   Sales                            active
30   HelpLine                         active
40   ITHelpDesk                       active
50   RemoteSupport                    active
60   TeamLeader                       active    Fa0/4
70   Admin                            active
80   HR                               active    Fa0/3
```

As VTP is deployed, vlan information is exchanged throughout the four L2 switches, as the screenshot illustrates. Traffic for vlans 60 and 80 is transported via access-ports, as can be seen in the screenshot. {fa0/4} and {fa0/3}, respectively. Teamleader is the name of Vlan 60, while Hr is the name of Vlan 80.

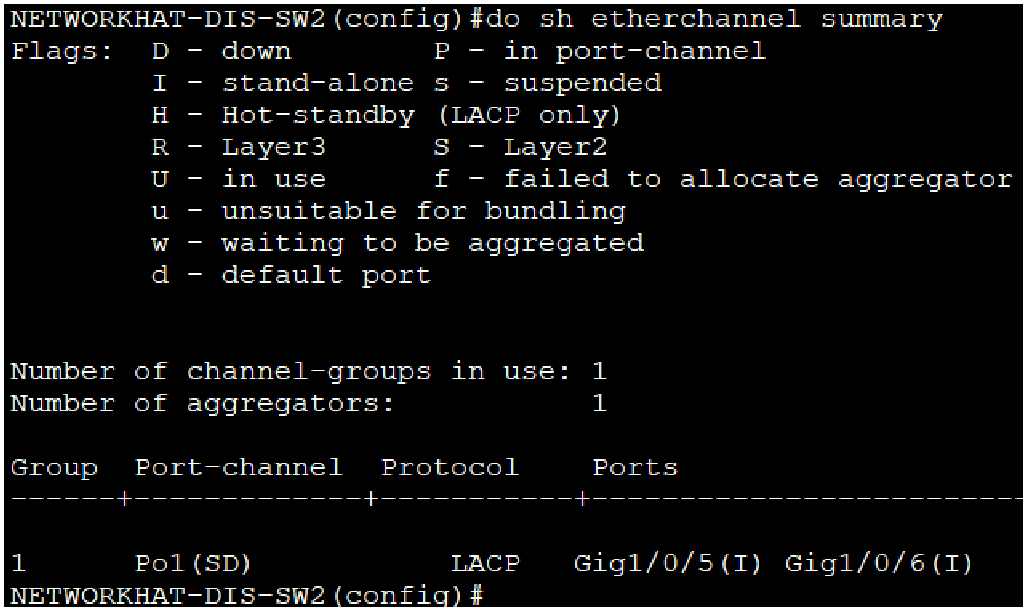
EtherChannel

In computer networking, etherchannel technology is used to merge many physical Ethernet cables into a single logical link. This logical link provides increased bandwidth, fault tolerance, and load balancing capabilities. EtherChannel is often employed between switches, routers, or servers to enhance network performance and resilience.



```
NETWORKHAT-DIS-SW1(config)#do sh etherchannel summary
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
------+-------------+-----------+----------------------------

1      Po1(RD)           LACP   Gig1/0/2(I) Gig1/0/6(I)
```

Networkhats-dis-sw1 has formed one EtherChannel-group. The first channel-group po1 is with networkhats-dis-sw2, the port {gig1/0/2 and gig1/0/6} are bundle together to form channel group.



```
NETWORKHAT-DIS-SW2(config)#do sh etherchannel summary
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
------+-------------+-----------+-----------------------

1      Po1(SD)           LACP   Gig1/0/5(I) Gig1/0/6(I)
NETWORKHAT-DIS-SW2(config)#
```

Networkhats-dis-sw2 has formed one EtherChannel-group. The first channel-group po1 is with networkhats-dis-sw1, the port {gig1/0/5 and gig1/0/6} are bundle together to form channel group.

BPDU protection

One characteristic of network switches that is frequently mentioned is BPDU (Bridge Protocol Data Unit) protection, especially when discussing spanning tree protocols. Spanning Tree Protocol (STP) is used in Ethernet networks to prevent loops in the network topology. BPDU is a frame exchanged between switches to convey information about the network topology and assist in the prevention of loops.

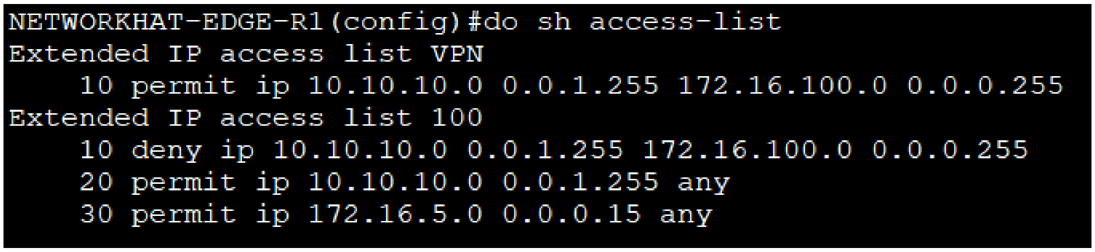
BPDU protection is a security mechanism implemented in switches to prevent the misuse or unauthorized introduction of BPDU frames. When BPDU protection is enabled on a switch port, the switch monitors the incoming frames on that port for BPDU frames. If the switch detects a BPDU frame, it takes specific actions to protect the network:

- Error Handling: The switch can log an error, generate a syslog message, or take some other action to alert administrators about the presence of a BPDU on a port where it shouldn't be.
- Port Shutdown: In more stringent configurations, the switch might automatically shut down the port when it detects a BPDU. This can help prevent accidental or malicious introduction of bridging devices that could disrupt the spanning tree topology.

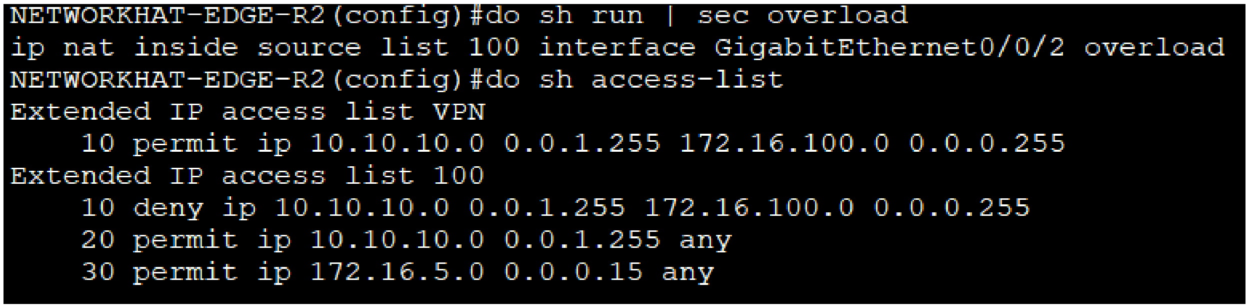
BPDU protection is especially useful in environments where the network topology is well-defined, and unexpected or unauthorized changes to the spanning tree could lead to network instability or security issues. It is often used in conjunction with other security features to enhance the overall robustness of the network.

NAT

In computer networking, network address translation maps private IP addresses inside a local network to a single public IP address. This makes it possible for several devices connected to a private network to connect to other networks, such the internet, using a single public IP address.



```
NETWORKHAT-EDGE-R1(config)#do sh access-list
Extended IP access list VPN
    10 permit ip 10.10.10.0 0.0.1.255 172.16.100.0 0.0.0.255
Extended IP access list 100
    10 deny ip 10.10.10.0 0.0.1.255 172.16.100.0 0.0.0.255
    20 permit ip 10.10.10.0 0.0.1.255 any
    30 permit ip 172.16.5.0 0.0.0.15 any
```



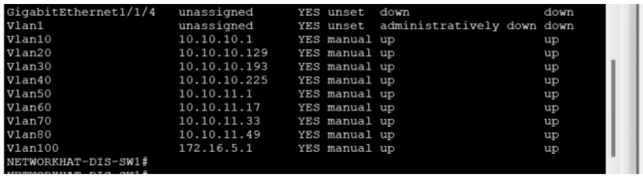
```
NETWORKHAT-EDGE-R2(config)#do sh run | sec overload
ip nat inside source list 100 interface GigabitEthernet0/0/2 overload
NETWORKHAT-EDGE-R2(config)#do sh access-list
Extended IP access list VPN
    10 permit ip 10.10.10.0 0.0.1.255 172.16.100.0 0.0.0.255
Extended IP access list 100
    10 deny ip 10.10.10.0 0.0.1.255 172.16.100.0 0.0.0.255
    20 permit ip 10.10.10.0 0.0.1.255 any
    30 permit ip 172.16.5.0 0.0.0.15 any
```

SVI

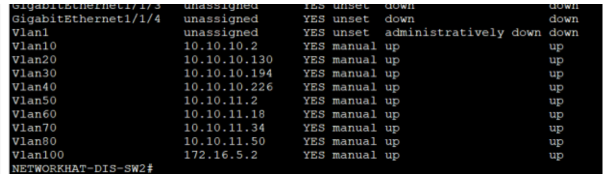
A virtual LAN (VLAN) interface is represented by this virtual interface on a layer 3 switch. Within a network, SVIs are used to facilitate communication and routing between various VLANs.

In a traditional layer 2 network, each VLAN is a separate broadcast domain, and devices within the same VLAN can communicate with each other. In case devices in separate VLANs need to communicate with one other, a layer 3 device like a router or a layer 3 switch is necessary.

SVIs allow a layer 3 switch to perform routing between VLANs without the need for an external router. Each SVI is associated with a specific VLAN and has an IP address assigned to it. The SVI acts as the default gateway for devices within the corresponding VLAN, enabling them to communicate with devices in other VLANs.



```
GigabitEthernet1/1/4   unassigned      YES unset  down                  down
Vlan1                  unassigned      YES unset  administratively down down
Vlan10                 10.10.10.1      YES manual up                    up
Vlan20                 10.10.10.129    YES manual up                    up
Vlan30                 10.10.10.193    YES manual up                    up
Vlan40                 10.10.10.225    YES manual up                    up
Vlan50                 10.10.11.1      YES manual up                    up
Vlan60                 10.10.11.17     YES manual up                    up
Vlan70                 10.10.11.33     YES manual up                    up
Vlan80                 10.10.11.49     YES manual up                    up
Vlan100                172.16.5.1      YES manual up                    up
NETWORKHAT-DIS-SW1#
NETWORKHAT-DIS-SW1#
```



```
GigabitEthernet1/1/3   unassigned      YES unset  down                  down
GigabitEthernet1/1/4   unassigned      YES unset  down                  down
Vlan1                  unassigned      YES unset  administratively down down
Vlan10                 10.10.10.2      YES manual up                    up
Vlan20                 10.10.10.130    YES manual up                    up
Vlan30                 10.10.10.194    YES manual up                    up
Vlan40                 10.10.10.226    YES manual up                    up
Vlan50                 10.10.11.2      YES manual up                    up
Vlan60                 10.10.11.18     YES manual up                    up
Vlan70                 10.10.11.34     YES manual up                    up
Vlan80                 10.10.11.50     YES manual up                    up
Vlan100                172.16.5.2      YES manual up                    up
NETWORKHAT-DIS-SW2#
```

HSRP

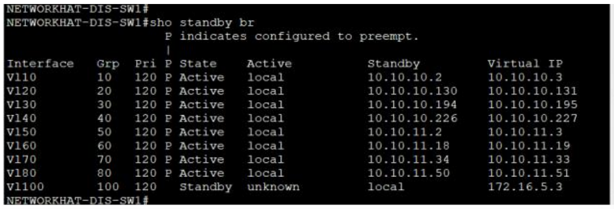
HSRP stands for Hot Standby Router Protocol. It is a Cisco proprietary redundancy protocol that provides high availability for routing in a network. HSRP allows multiple routers to work together to present a single virtual router IP address and a single virtual MAC address to the hosts on the network.

HSRP's main goal is to maintain network functionality by giving a backup router a means to take over in the event that the main router fails. HSRP is commonly used in environments where network uptime is critical, and a seamless failover mechanism is required.

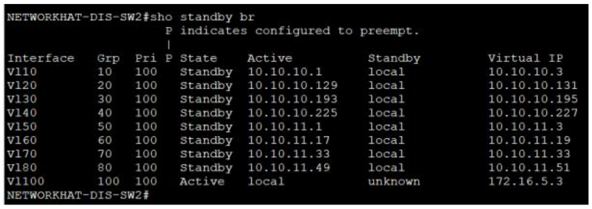
- Virtual IP Address (VIP): A virtual IP address is used by HSRP, and it moves between the routers in the HSRP group. Devices connected to the local network are set up with this IP address as their default gateway.
- Virtual MAC Address: HSRP employs a virtual MAC address that correlates to the virtual IP address in addition to the virtual IP address. The routers in the HSRP group share this virtual MAC address.
- Router Roles: In an HSRP group, one router is elected as the "Active" router, and another router is designated as the "Standby" router. The Active router is the one currently handling traffic for the virtual IP address, while the Standby router is ready to take over if the Active router fails.
- Hello Messages: Routers in an HSRP group exchange "Hello" messages at regular intervals to monitor the health of each other. If the Active router fails to send Hello messages, the Standby router can assume the Active role.

- Automatic Failover: In the event of a failure (such as a router going down or a network link failure), the Standby router can quickly take over the Active role, ensuring minimal disruption to network traffic.

HSRP is commonly used in scenarios where redundancy and fault tolerance are critical, such as in enterprise networks, data centers, or any environment where network uptime is a priority. Keep in mind that there are similar protocols, such as Virtual Router Redundancy Protocol (VRRP) and Gateway Load Balancing Protocol (GLBP), which offer similar functionality and are not vendor specific like HSRP.



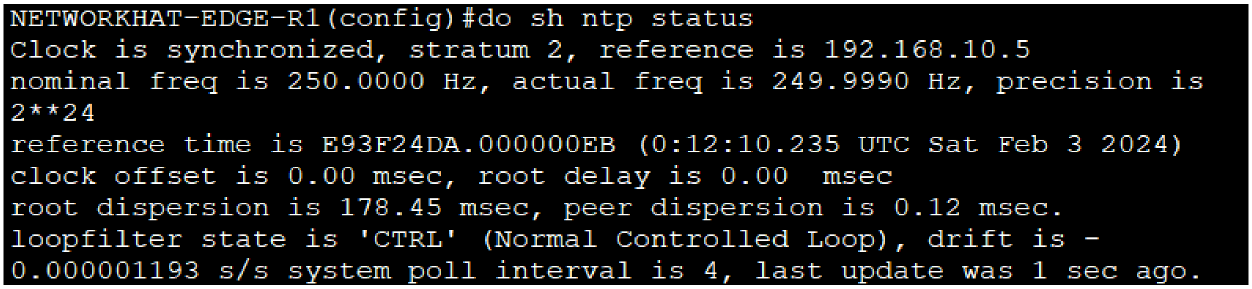
```
NETWORKHAT-DIS-SW1#
NETWORKHAT-DIS-SW1#sho standby br
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
V110        10   120 P Active   local           10.10.10.2      10.10.10.3
V120        20   120 P Active   local           10.10.10.130    10.10.10.131
V130        30   120 P Active   local           10.10.10.194    10.10.10.195
V140        40   120 P Active   local           10.10.10.226    10.10.10.227
V150        50   120 P Active   local           10.10.11.2      10.10.11.3
V160        60   120 P Active   local           10.10.11.18     10.10.11.19
V170        70   120 P Active   local           10.10.11.34     10.10.11.33
V180        80   120 P Active   local           10.10.11.50     10.10.11.51
V1100       100  120   Standby  unknown         local           172.16.5.3
NETWORKHAT-DIS-SW1#
```



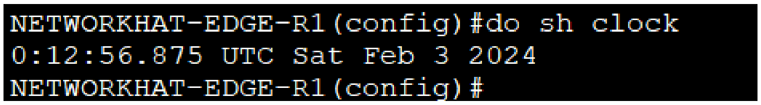
```
NETWORKHAT-DIS-SW2#sho standby br
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
V110        10   100   Standby  10.10.10.1      local           10.10.10.3
V120        20   100   Standby  10.10.10.129    local           10.10.10.131
V130        30   100   Standby  10.10.10.193    local           10.10.10.195
V140        40   100   Standby  10.10.10.225    local           10.10.10.227
V150        50   100   Standby  10.10.11.1      local           10.10.11.3
V160        60   100   Standby  10.10.11.17     local           10.10.11.19
V170        70   100   Standby  10.10.11.33     local           10.10.11.33
V180        80   100   Standby  10.10.11.49     local           10.10.11.51
V1100       100  100   Active   local           unknown         172.16.5.3
NETWORKHAT-DIS-SW2#
```

NTP server

Network Time Protocol is a protocol designed to synchronize the clocks of devices within a computer network. An NTP server is a device or software application that provides accurate time information to other devices in the network, ensuring that they all maintain a consistent and synchronized time.



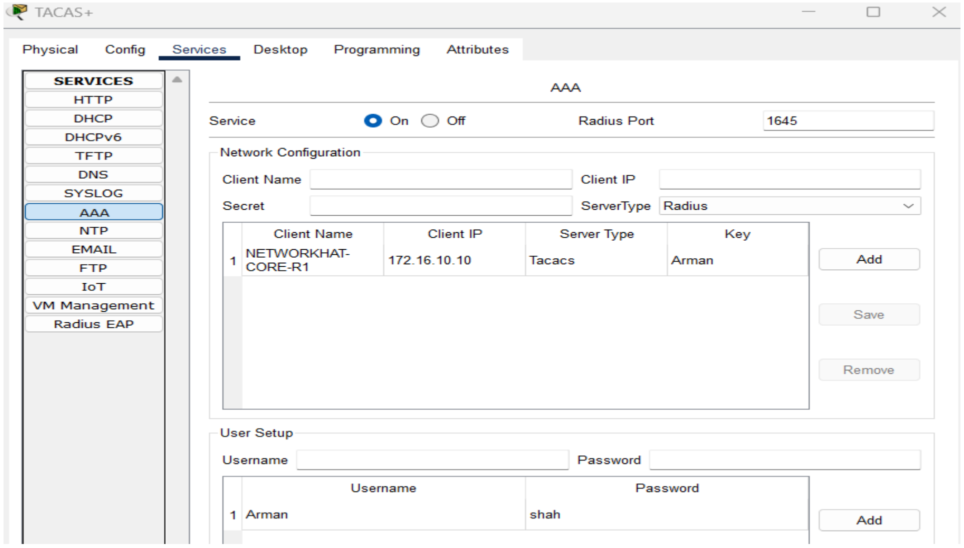
```
NETWORKHAT-EDGE-R1(config)#do sh ntp status
Clock is synchronized, stratum 2, reference is 192.168.10.5
nominal freq is 250.0000 Hz, actual freq is 249.9990 Hz, precision is
2**24
reference time is E93F24DA.000000EB (0:12:10.235 UTC Sat Feb 3 2024)
clock offset is 0.00 msec, root delay is 0.00  msec
root dispersion is 178.45 msec, peer dispersion is 0.12 msec.
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is -
0.000001193 s/s system poll interval is 4, last update was 1 sec ago.
```



```
NETWORKHAT-EDGE-R1(config)#do sh clock
0:12:56.875 UTC Sat Feb 3 2024
NETWORKHAT-EDGE-R1(config)#
```

AAA (Authentication, Authorization, Accounting)

Authentication, Authorization, and Accounting are referred to as AAA. These are the three main parts of a security framework or system, which are frequently used to regulate access and keep an eye on activity in computer networks and systems.



AAA

Service ● On ○ Off Radius Port 1645

Network Configuration

Client Name Client IP

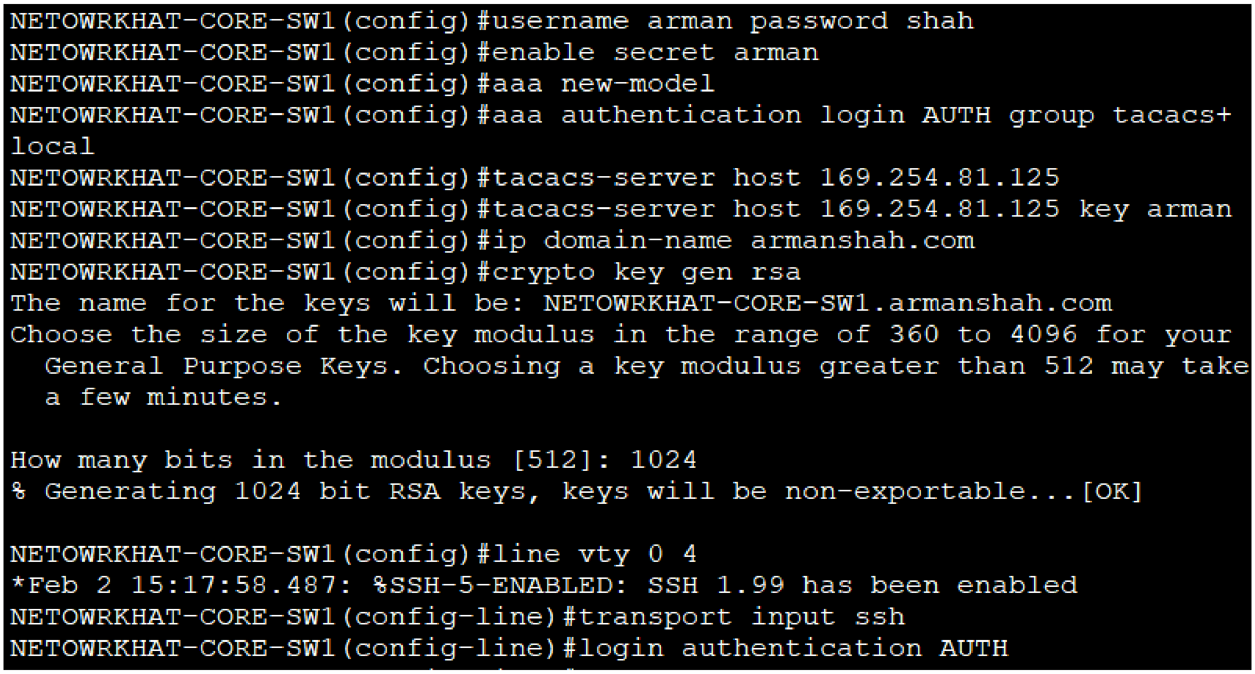
Secret ServerType Radius

	Client Name	Client IP	Server Type	Key
1	NETWORKHAT-CORE-R1	172.16.10.10	Tacacs	Arman

User Setup

Username Password

	Username	Password
1	Arman	shah



```
NETOWRKHAT-CORE-SW1(config)#username arman password shah
NETOWRKHAT-CORE-SW1(config)#enable secret arman
NETOWRKHAT-CORE-SW1(config)#aaa new-model
NETOWRKHAT-CORE-SW1(config)#aaa authentication login AUTH group tacacs+
local
NETOWRKHAT-CORE-SW1(config)#tacacs-server host 169.254.81.125
NETOWRKHAT-CORE-SW1(config)#tacacs-server host 169.254.81.125 key arman
NETOWRKHAT-CORE-SW1(config)#ip domain-name armanshah.com
NETOWRKHAT-CORE-SW1(config)#crypto key gen rsa
The name for the keys will be: NETOWRKHAT-CORE-SW1.armanshah.com
Choose the size of the key modulus in the range of 360 to 4096 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]

NETOWRKHAT-CORE-SW1(config)#line vty 0 4
*Feb 2 15:17:58.487: %SSH-5-ENABLED: SSH 1.99 has been enabled
NETOWRKHAT-CORE-SW1(config-line)#transport input ssh
NETOWRKHAT-CORE-SW1(config-line)#login authentication AUTH
```

VPN

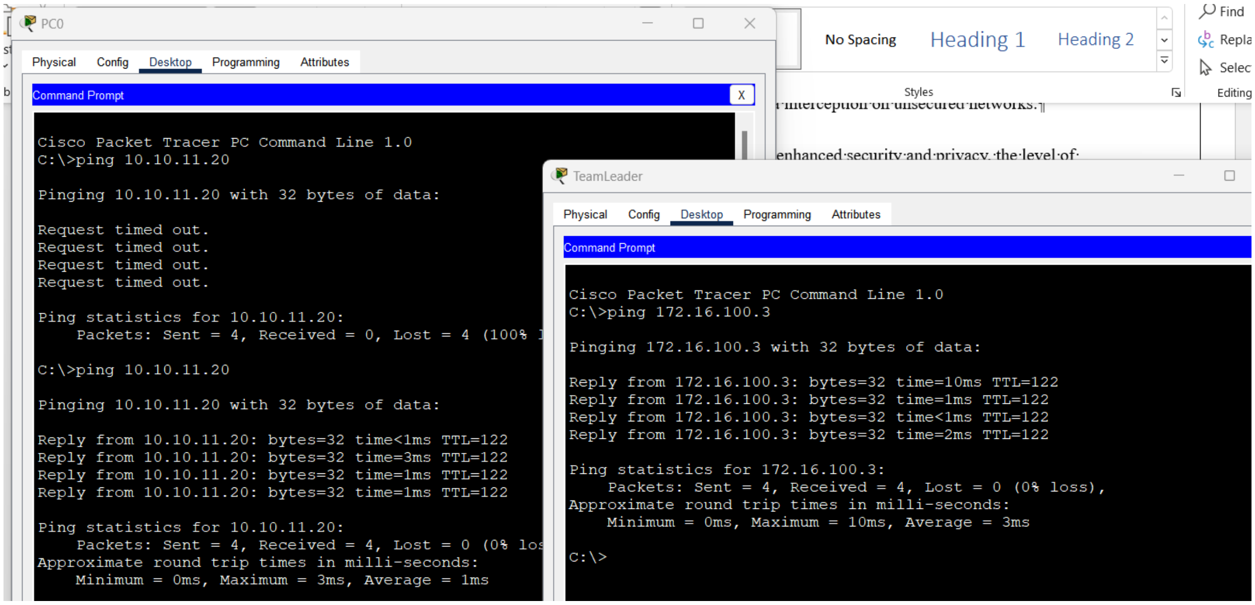
A virtual private network is a technology that makes it possible to connect to the internet securely and encrypted. It enables users to establish a secure, private network connection to another network—typically one that is located elsewhere. VPNs are commonly used for various purposes, including enhancing privacy, securing data transmission, and bypassing geographical restrictions.

Use of VPNs:

- Encryption: Encrypting data while it is sent between the user's device and the VPN server is one of a VPN's main purposes. This encryption ensures that even if the data is intercepted by unauthorized parties, it remains unreadable and secure.
- Tunneling: VPNs use a process called tunneling to create a secure pathway for data to travel between the user's device and the VPN server. Different tunneling protocols can be used, such as OpenVPN, IPSec, or L2TP/IPSec, each with its own strengths and characteristics.
- Anonymity and Privacy: By routing your internet traffic through a VPN server, your IP address is masked, and your online activities become more private. This assists in shielding your identity and private data from prying eyes, such as your internet service provider (ISP).
- Access Control and Bypassing Restrictions: VPNs enable users to access resources on a network as if they were physically present in the same location as the VPN server. This is particularly useful for remote workers accessing company resources or for individuals bypassing geographical restrictions imposed on certain content or services.

- Secure Remote Access: VPNs are commonly used by businesses to provide secure remote access for employees who need to connect to the corporate network from external locations. This is often achieved through technologies like SSL VPN or IPsec VPN.
- Public Wi-Fi Security: By encrypting your internet data, a VPN provides an additional degree of protection while utilizing public Wi-Fi networks, which might be susceptible to security concerns. This helps protect against potential data interception on unsecured networks.

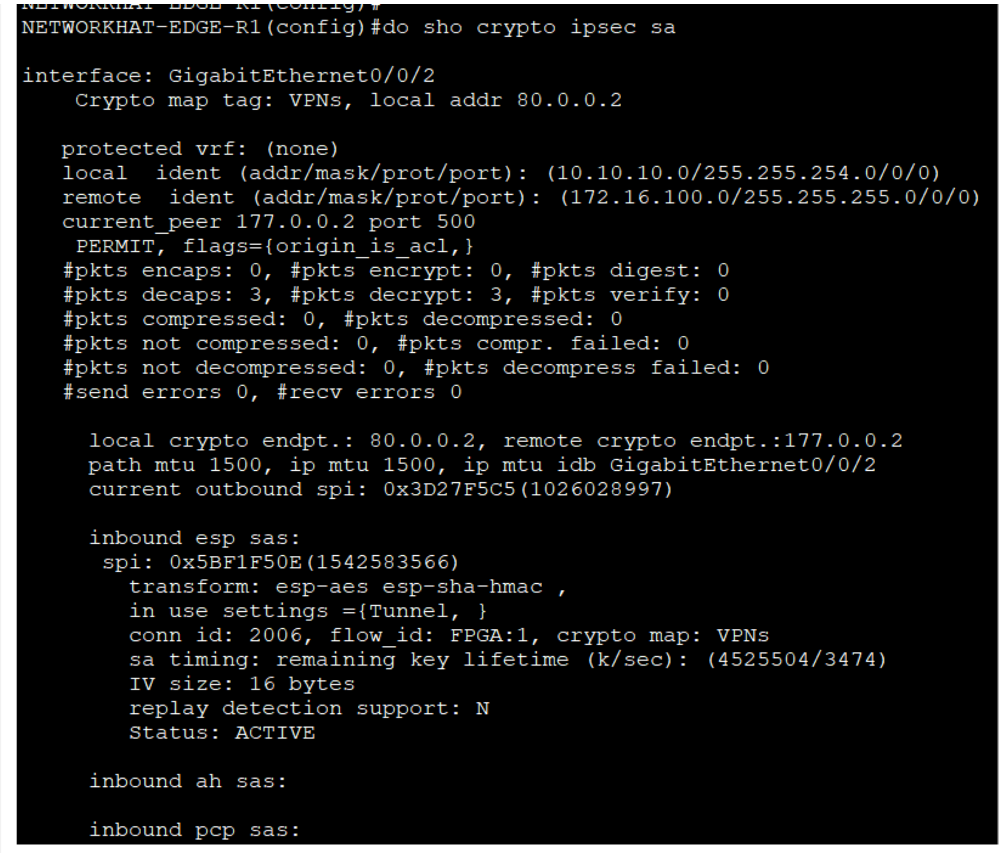
It's important to note that while VPNs provide enhanced security and privacy, the level of anonymity depends on the VPN service provider.



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.10.11.20

Pinging 10.10.11.20 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.10.11.20:
    Packets: Sent = 4, Received = 0, Lost = 4 (100%

C:\>ping 10.10.11.20

Pinging 10.10.11.20 with 32 bytes of data:

Reply from 10.10.11.20: bytes=32 time<1ms TTL=122
Reply from 10.10.11.20: bytes=32 time=3ms TTL=122
Reply from 10.10.11.20: bytes=32 time=1ms TTL=122
Reply from 10.10.11.20: bytes=32 time=1ms TTL=122

Ping statistics for 10.10.11.20:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% los
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 3ms, Average = 1ms
```

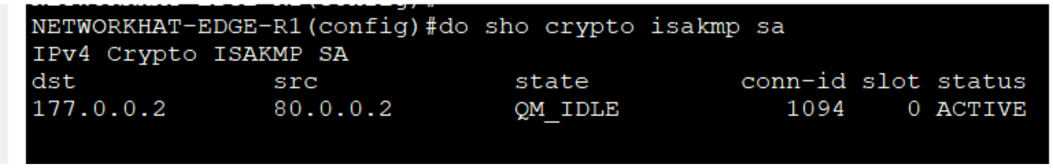
```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 172.16.100.3

Pinging 172.16.100.3 with 32 bytes of data:

Reply from 172.16.100.3: bytes=32 time=10ms TTL=122
Reply from 172.16.100.3: bytes=32 time=1ms TTL=122
Reply from 172.16.100.3: bytes=32 time<1ms TTL=122
Reply from 172.16.100.3: bytes=32 time=2ms TTL=122

Ping statistics for 172.16.100.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 10ms, Average = 3ms

C:\>
```

Successful tunnel formation between headquarter and branch.

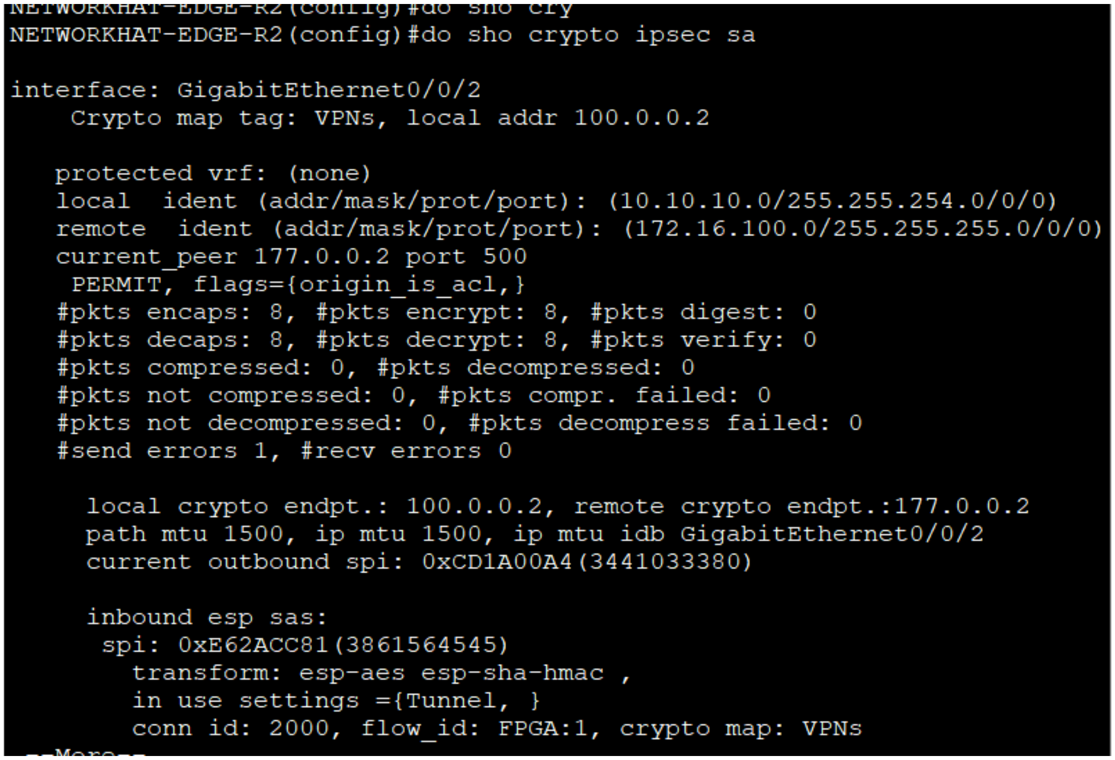


```
NETWORKHAT-EDGE-R1(config)#
NETWORKHAT-EDGE-R1(config)#do sho crypto ipsec sa

interface: GigabitEthernet0/0/2
    Crypto map tag: VPNs, local addr 80.0.0.2

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (10.10.10.0/255.255.254.0/0/0)
   remote  ident (addr/mask/prot/port): (172.16.100.0/255.255.255.0/0/0)
   current_peer 177.0.0.2 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 0, #pkts encrypt: 0, #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 0, #recv errors 0

     local crypto endpt.: 80.0.0.2, remote crypto endpt.:177.0.0.2
     path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/0/2
     current outbound spi: 0x3D27F5C5(1026028997)

     inbound esp sas:
      spi: 0x5BF1F50E(1542583566)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2006, flow_id: FPGA:1, crypto map: VPNs
        sa timing: remaining key lifetime (k/sec): (4525504/3474)
        IV size: 16 bytes
        replay detection support: N
        Status: ACTIVE

     inbound ah sas:

     inbound pcp sas:
```

Encryption, encapsulation, decryption, and encapsulation by IPsec in edge router

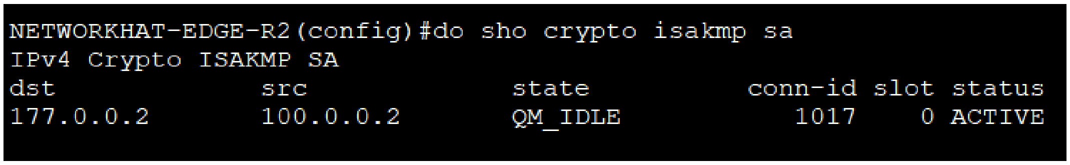


```
NETWORKHAT-EDGE-R1(config)#
NETWORKHAT-EDGE-R1(config)#do sho crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status
177.0.0.2       80.0.0.2        QM_IDLE           1094    0 ACTIVE
```

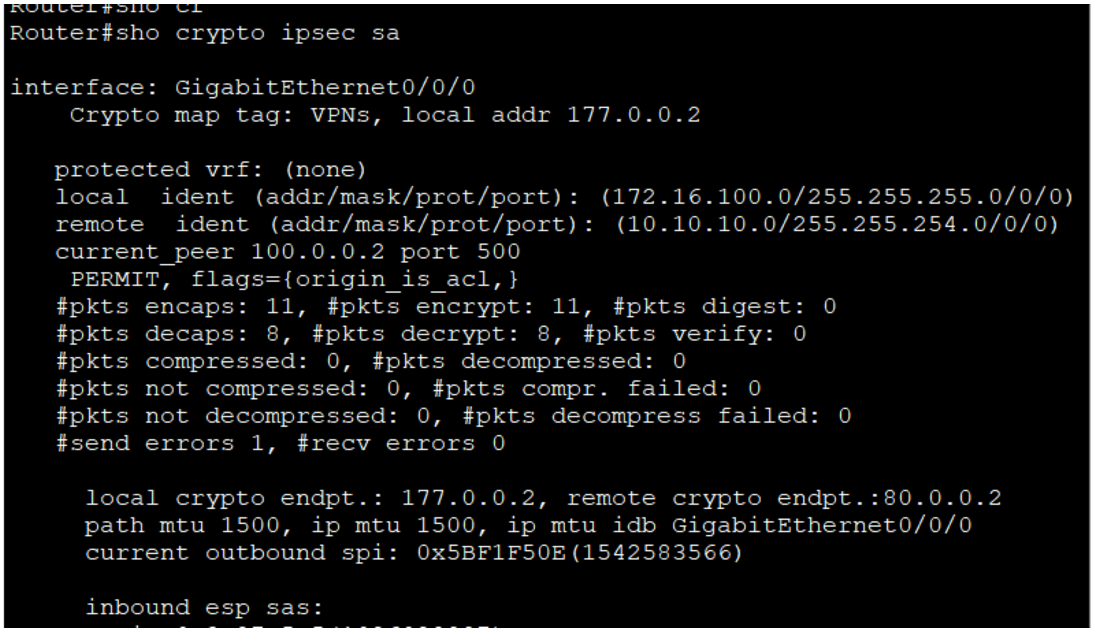


```
NETWORKHAT-EDGE-R2(config)#do sho cry
NETWORKHAT-EDGE-R2(config)#do sho crypto ipsec sa

interface: GigabitEthernet0/0/2
    Crypto map tag: VPNs, local addr 100.0.0.2

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (10.10.10.0/255.255.254.0/0/0)
   remote  ident (addr/mask/prot/port): (172.16.100.0/255.255.255.0/0/0)
   current_peer 177.0.0.2 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 8, #pkts encrypt: 8, #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 1, #recv errors 0

     local crypto endpt.: 100.0.0.2, remote crypto endpt.:177.0.0.2
     path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/0/2
     current outbound spi: 0xCD1A00A4(3441033380)

     inbound esp sas:
      spi: 0xE62ACC81(3861564545)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2000, flow_id: FPGA:1, crypto map: VPNs
 --More--
```

Encryption, encapsulation, decryption, and encapsulation by IPsec in edge router

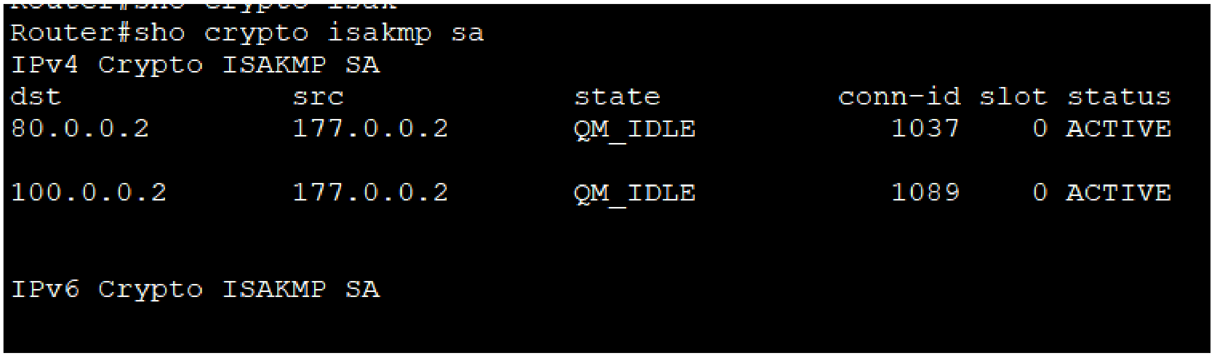


```
NETWORKHAT-EDGE-R2(config)#do sho crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status
177.0.0.2       100.0.0.2       QM_IDLE           1017    0 ACTIVE
```



```
Router#sho cr
Router#sho crypto ipsec sa

interface: GigabitEthernet0/0/0
    Crypto map tag: VPNs, local addr 177.0.0.2

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (172.16.100.0/255.255.255.0/0/0)
   remote  ident (addr/mask/prot/port): (10.10.10.0/255.255.254.0/0/0)
   current_peer 100.0.0.2 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 11, #pkts encrypt: 11, #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 1, #recv errors 0

     local crypto endpt.: 177.0.0.2, remote crypto endpt.:80.0.0.2
     path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/0/0
     current outbound spi: 0x5BF1F50E(1542583566)

     inbound esp sas:
```

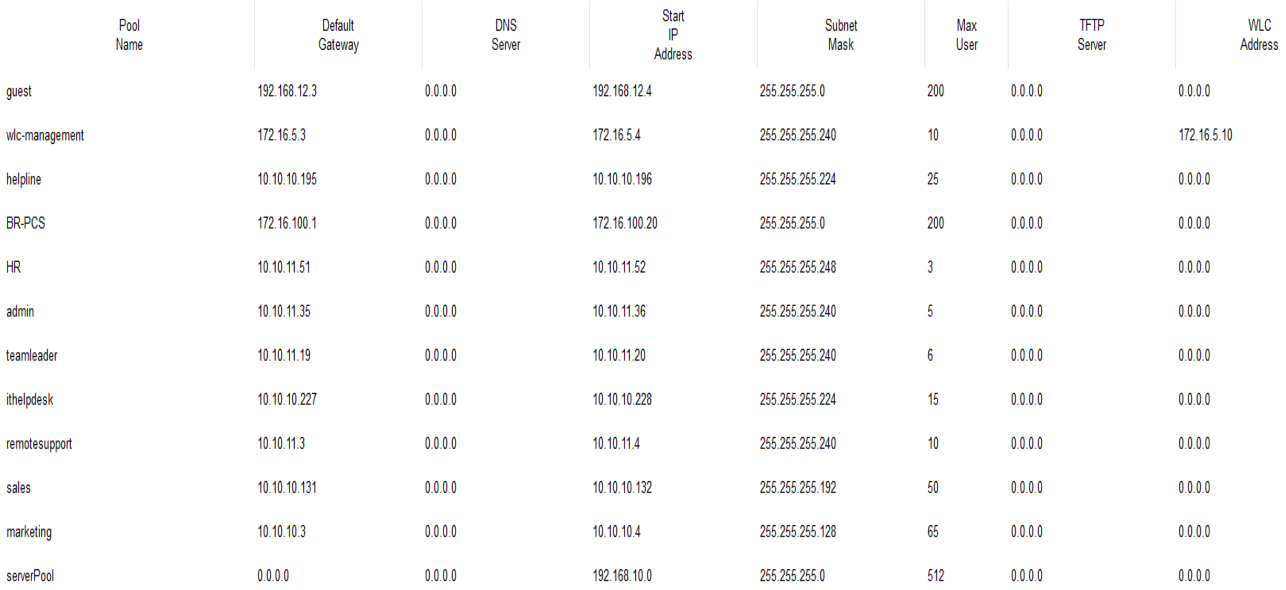
Encryption, encapsulation, decryption, and encapsulation by IPsec in edge router



```
Router#sho crypto isak
Router#sho crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status
80.0.0.2        177.0.0.2       QM_IDLE           1037    0 ACTIVE

100.0.0.2       177.0.0.2       QM_IDLE           1089    0 ACTIVE


IPv6 Crypto ISAKMP SA
```

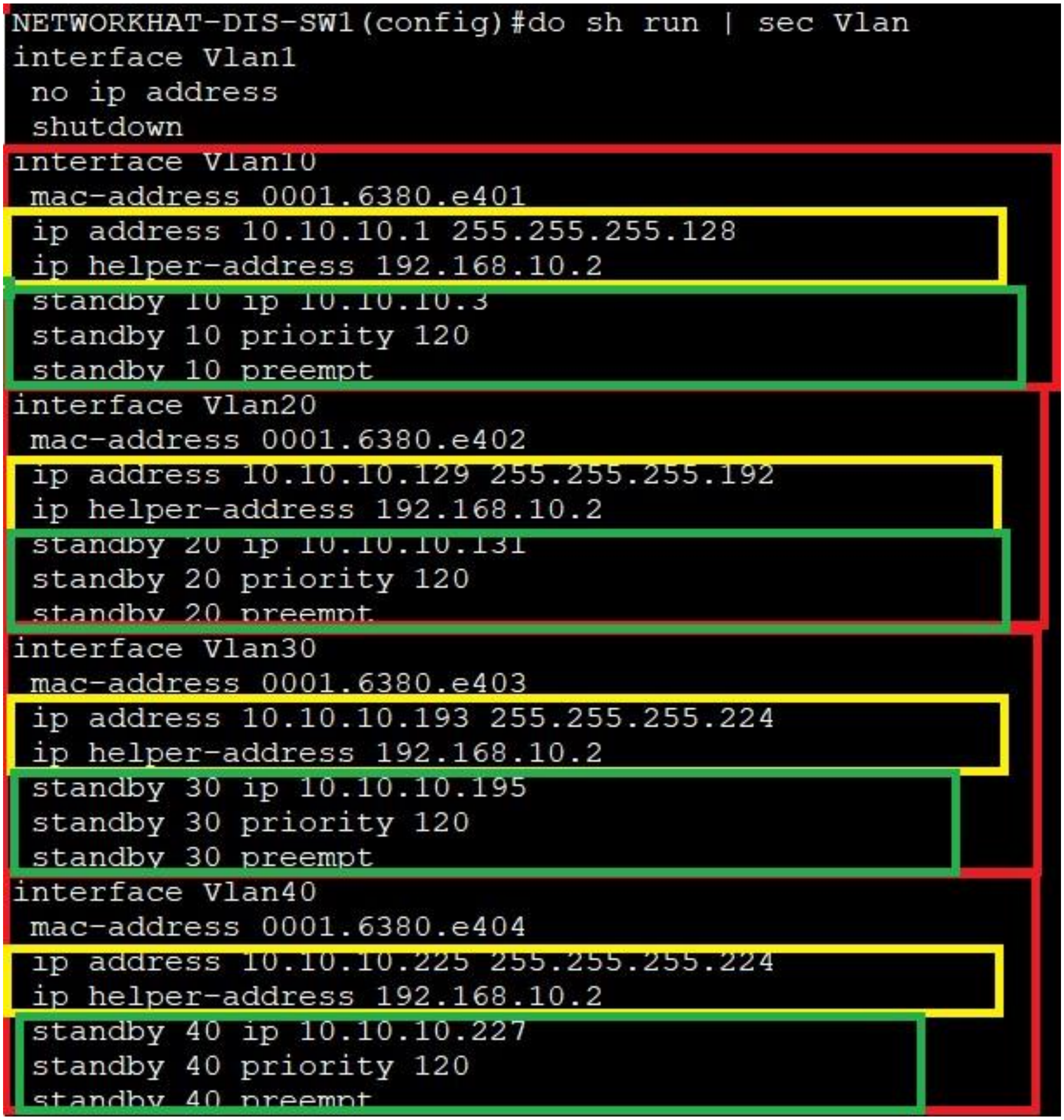
DHCP

It is a network management protocol commonly used to automatically assign and manage IP addresses within a network. DHCP eliminates the need for manual configuration of network devices by automatically providing them with essential information.



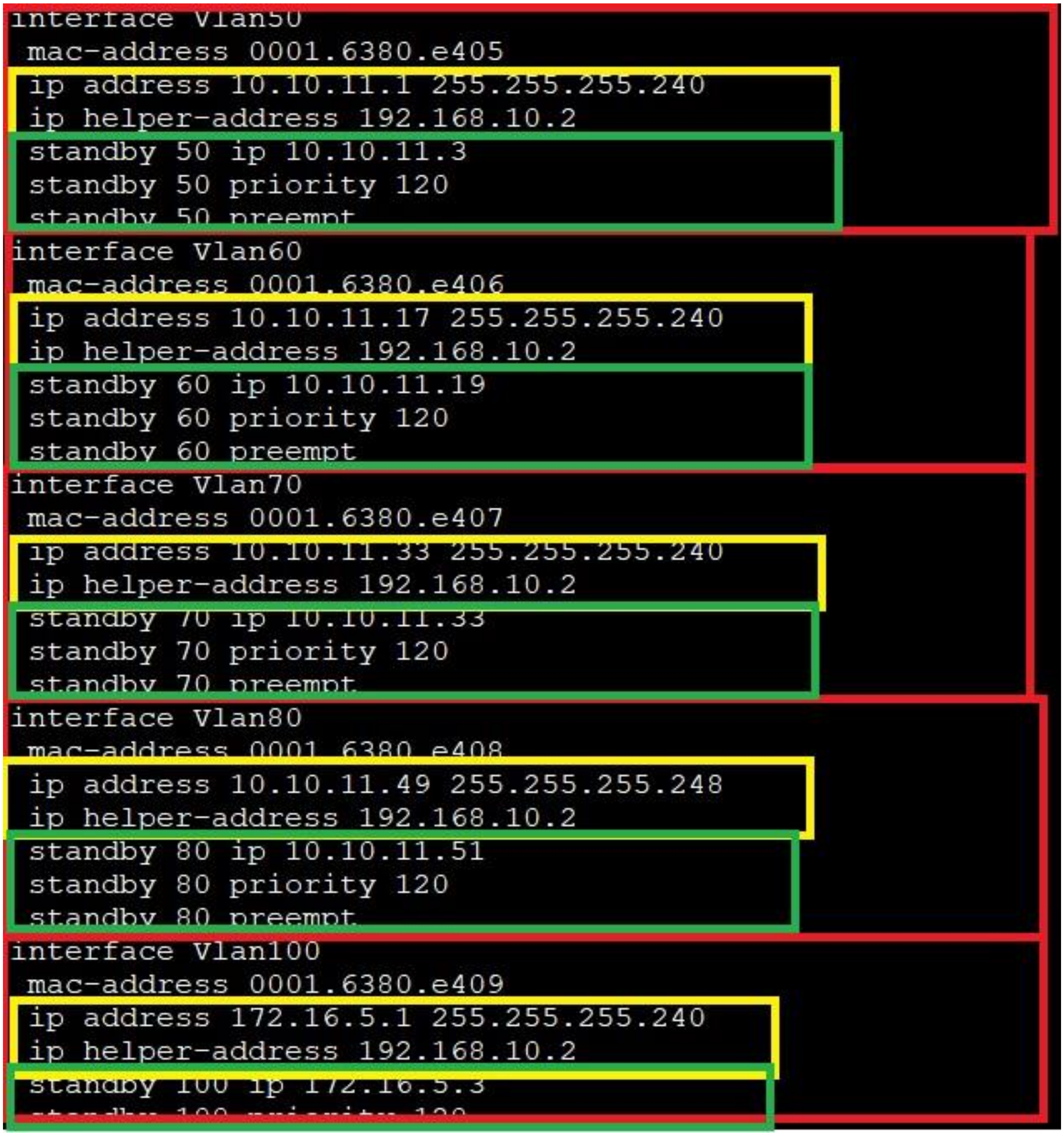
Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
guest	192.168.12.3	0.0.0.0	192.168.12.4	255.255.255.0	200	0.0.0.0	0.0.0.0
wlc-management	172.16.5.3	0.0.0.0	172.16.5.4	255.255.255.240	10	0.0.0.0	172.16.5.10
helpline	10.10.10.195	0.0.0.0	10.10.10.196	255.255.255.224	25	0.0.0.0	0.0.0.0
BR-PCS	172.16.100.1	0.0.0.0	172.16.100.20	255.255.255.0	200	0.0.0.0	0.0.0.0
HR	10.10.11.51	0.0.0.0	10.10.11.52	255.255.255.248	3	0.0.0.0	0.0.0.0
admin	10.10.11.35	0.0.0.0	10.10.11.36	255.255.255.240	5	0.0.0.0	0.0.0.0
teamleader	10.10.11.19	0.0.0.0	10.10.11.20	255.255.255.240	6	0.0.0.0	0.0.0.0
ithelpdesk	10.10.10.227	0.0.0.0	10.10.10.228	255.255.255.224	15	0.0.0.0	0.0.0.0
remotesupport	10.10.11.3	0.0.0.0	10.10.11.4	255.255.255.240	10	0.0.0.0	0.0.0.0
sales	10.10.10.131	0.0.0.0	10.10.10.132	255.255.255.192	50	0.0.0.0	0.0.0.0
marketing	10.10.10.3	0.0.0.0	10.10.10.4	255.255.255.128	65	0.0.0.0	0.0.0.0
serverPool	0.0.0.0	0.0.0.0	192.168.10.0	255.255.255.0	512	0.0.0.0	0.0.0.0

DHCP relay agent



```
NETWORKHAT-DIS-SW1(config)#do sh run | sec Vlan
interface Vlan1
 no ip address
 shutdown
interface Vlan10
 mac-address 0001.6380.e401
 ip address 10.10.10.1 255.255.255.128
 ip helper-address 192.168.10.2
 standby 10 ip 10.10.10.3
 standby 10 priority 120
 standby 10 preempt
interface Vlan20
 mac-address 0001.6380.e402
 ip address 10.10.10.129 255.255.255.192
 ip helper-address 192.168.10.2
 standby 20 ip 10.10.10.131
 standby 20 priority 120
 standby 20 preempt
interface Vlan30
 mac-address 0001.6380.e403
 ip address 10.10.10.193 255.255.255.224
 ip helper-address 192.168.10.2
 standby 30 ip 10.10.10.195
 standby 30 priority 120
 standby 30 preempt
interface Vlan40
 mac-address 0001.6380.e404
 ip address 10.10.10.225 255.255.255.224
 ip helper-address 192.168.10.2
 standby 40 ip 10.10.10.227
 standby 40 priority 120
 standby 40 preempt
```

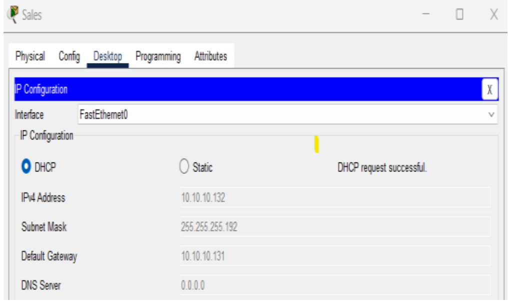
As you can see this above picture that we have configure DHCP and HSRP Yellow line represent DHCP replay agent and the green line represent HSRP



```
interface Vlan50
 mac-address 0001.6380.e405
 ip address 10.10.11.1 255.255.255.240
 ip helper-address 192.168.10.2
 standby 50 ip 10.10.11.3
 standby 50 priority 120
 standby 50 preempt
interface Vlan60
 mac-address 0001.6380.e406
 ip address 10.10.11.17 255.255.255.240
 ip helper-address 192.168.10.2
 standby 60 ip 10.10.11.19
 standby 60 priority 120
 standby 60 preempt
interface Vlan70
 mac-address 0001.6380.e407
 ip address 10.10.11.33 255.255.255.240
 ip helper-address 192.168.10.2
 standby 70 ip 10.10.11.33
 standby 70 priority 120
 standby 70 preempt
interface Vlan80
 mac-address 0001.6380.e408
 ip address 10.10.11.49 255.255.255.248
 ip helper-address 192.168.10.2
 standby 80 ip 10.10.11.51
 standby 80 priority 120
 standby 80 preempt
interface Vlan100
 mac-address 0001.6380.e409
 ip address 172.16.5.1 255.255.255.240
 ip helper-address 192.168.10.2
 standby 100 ip 172.16.5.3
 standby 100 priority 120
```

As you can see this above picture that we have configure DHCP and HSRP Yellow line represent DHCP replay agent and the green line represent HSRP

departments obtaining IP from DHCP server



IP Configuration

Interface: FastEthernet0

IP Configuration

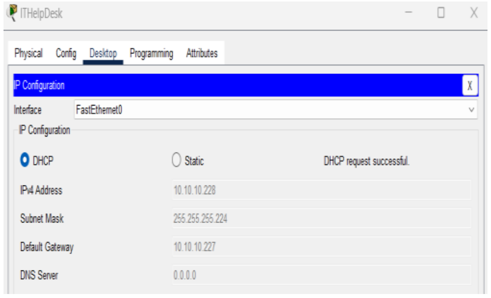
● DHCP ○ Static DHCP request successful.

IPv4 Address: 10.10.10.132

Subnet Mask: 255.255.255.192

Default Gateway: 10.10.10.131

DNS Server: 0.0.0.0



IP Configuration

Interface: FastEthernet0

IP Configuration

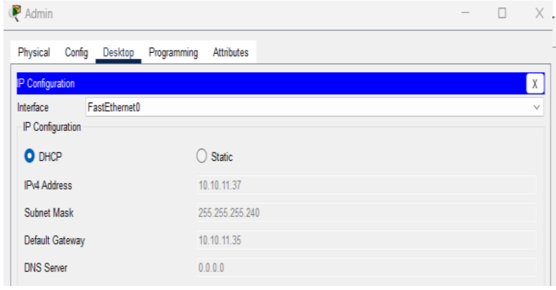
● DHCP ○ Static DHCP request successful.

IPv4 Address: 10.10.10.228

Subnet Mask: 255.255.255.224

Default Gateway: 10.10.10.227

DNS Server: 0.0.0.0



IP Configuration

Interface: FastEthernet0

IP Configuration

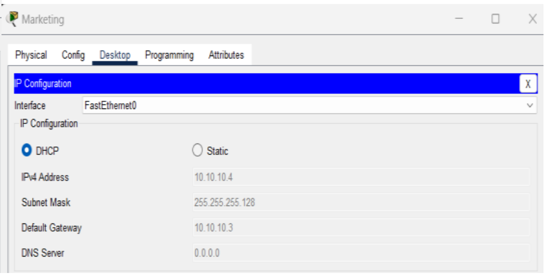
● DHCP ○ Static

IPv4 Address: 10.10.11.37

Subnet Mask: 255.255.255.240

Default Gateway: 10.10.11.35

DNS Server: 0.0.0.0



IP Configuration

Interface: FastEthernet0

IP Configuration

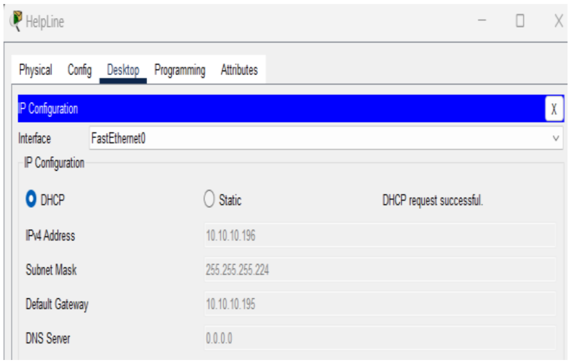
● DHCP ○ Static

IPv4 Address: 10.10.10.4

Subnet Mask: 255.255.255.128

Default Gateway: 10.10.10.3

DNS Server: 0.0.0.0



IP Configuration

Interface: FastEthernet0

IP Configuration

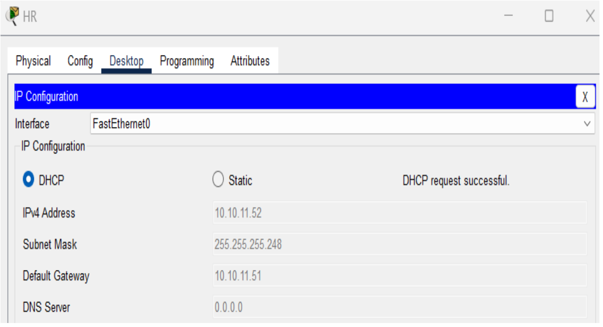
● DHCP ○ Static DHCP request successful.

IPv4 Address: 10.10.10.196

Subnet Mask: 255.255.255.224

Default Gateway: 10.10.10.195

DNS Server: 0.0.0.0



IP Configuration

Interface: FastEthernet0

IP Configuration

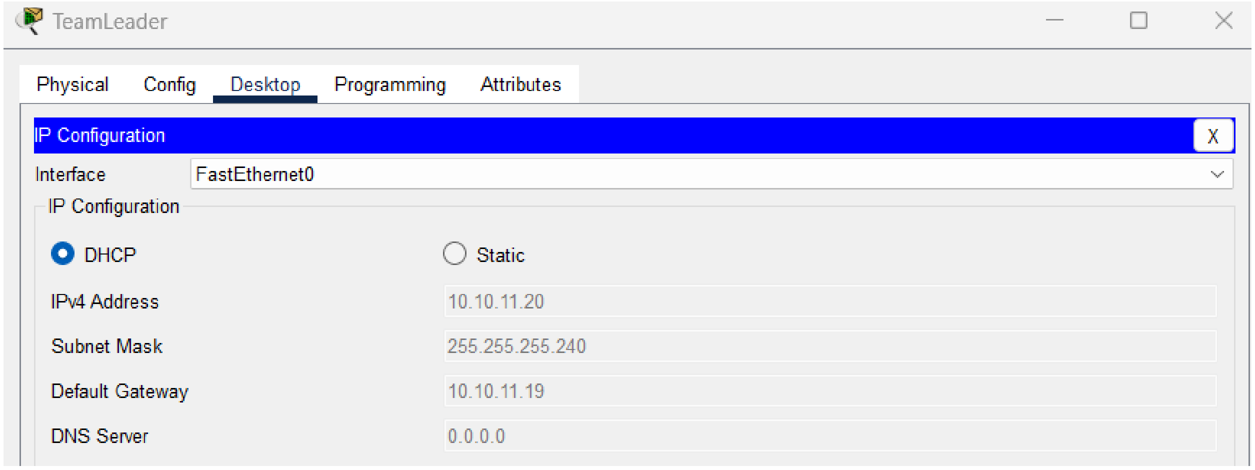
● DHCP ○ Static DHCP request successful.

IPv4 Address: 10.10.11.52

Subnet Mask: 255.255.255.248

Default Gateway: 10.10.11.51

DNS Server: 0.0.0.0



IP Configuration

Interface: FastEthernet0

IP Configuration

● DHCP ○ Static

IPv4 Address: 10.10.11.20

Subnet Mask: 255.255.255.240

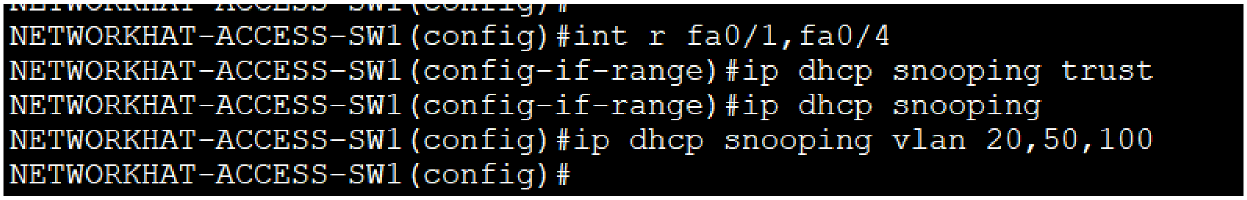
Default Gateway: 10.10.11.19

DNS Server: 0.0.0.0

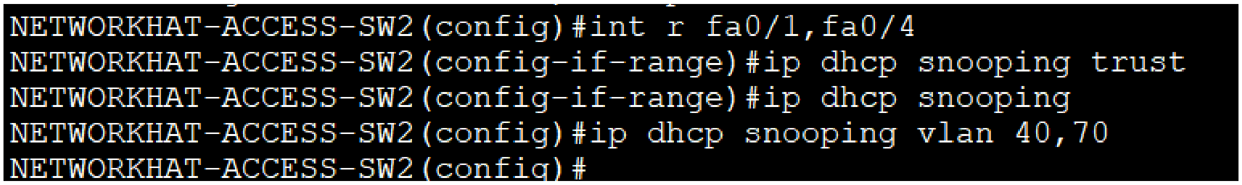
DHCP snooping.

Deploying DHCP servers introduces inherent risks such as DHCP starvation and poisoning, which allow attackers to steal address pools or modify configurations. To protect against these dangers, DHCP snooping is used as a security measure. This method selectively allows switches to forward DHCP requests, preventing rogue servers and ensuring the integrity of IP assignments. It creates a binding database, records MAC-to-IP associations, and prevents denial-of-service incidents by reducing DHCP requests.

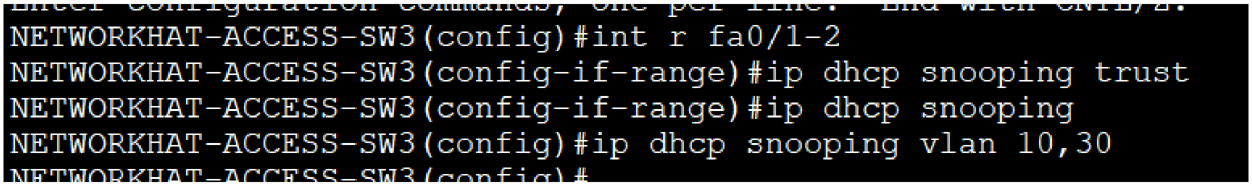
Figures: configuring DHCP snooping in HQ switches



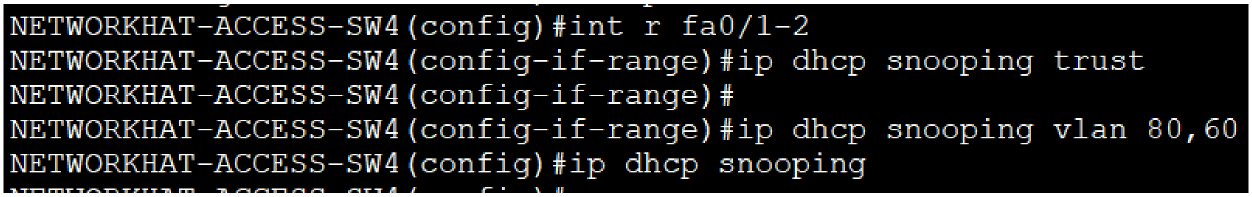
```
NETWORKHAT-ACCESS-SW1(config)#
NETWORKHAT-ACCESS-SW1(config)#int r fa0/1,fa0/4
NETWORKHAT-ACCESS-SW1(config-if-range)#ip dhcp snooping trust
NETWORKHAT-ACCESS-SW1(config-if-range)#ip dhcp snooping
NETWORKHAT-ACCESS-SW1(config)#ip dhcp snooping vlan 20,50,100
NETWORKHAT-ACCESS-SW1(config)#
```



```
NETWORKHAT-ACCESS-SW2(config)#int r fa0/1,fa0/4
NETWORKHAT-ACCESS-SW2(config-if-range)#ip dhcp snooping trust
NETWORKHAT-ACCESS-SW2(config-if-range)#ip dhcp snooping
NETWORKHAT-ACCESS-SW2(config)#ip dhcp snooping vlan 40,70
NETWORKHAT-ACCESS-SW2(config)#
```



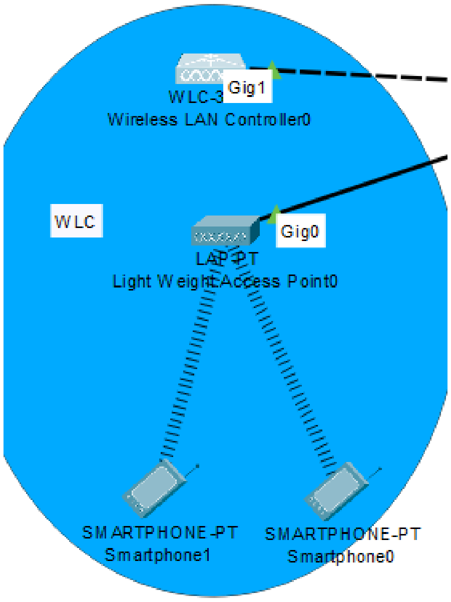
```
Enter configuration commands, one per line.  End with CNTL/Z.
NETWORKHAT-ACCESS-SW3(config)#int r fa0/1-2
NETWORKHAT-ACCESS-SW3(config-if-range)#ip dhcp snooping trust
NETWORKHAT-ACCESS-SW3(config-if-range)#ip dhcp snooping
NETWORKHAT-ACCESS-SW3(config)#ip dhcp snooping vlan 10,30
NETWORKHAT-ACCESS-SW3(config)#
```

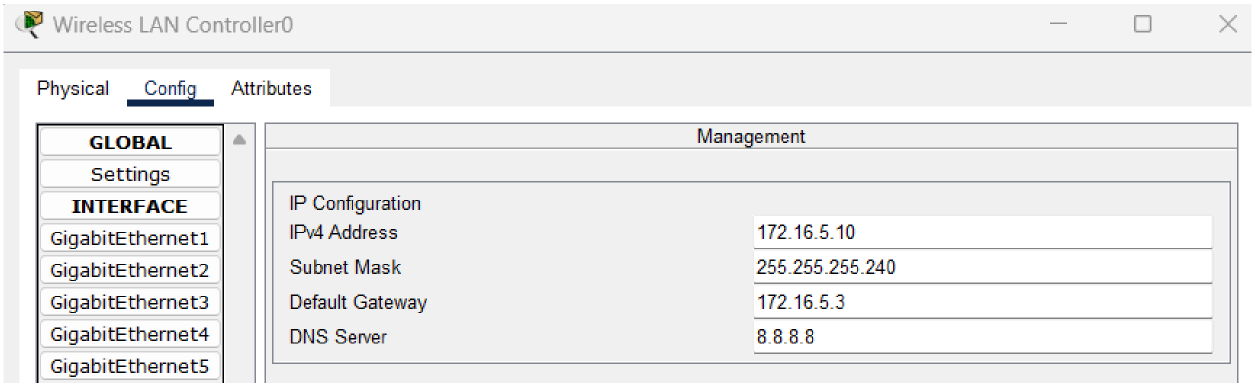


```
NETWORKHAT-ACCESS-SW4(config)#int r fa0/1-2
NETWORKHAT-ACCESS-SW4(config-if-range)#ip dhcp snooping trust
NETWORKHAT-ACCESS-SW4(config-if-range)#
NETWORKHAT-ACCESS-SW4(config-if-range)#ip dhcp snooping vlan 80,60
NETWORKHAT-ACCESS-SW4(config)#ip dhcp snooping
NETWORKHAT-ACCESS-SW4(config)#
```

WLC (Wireless LAN controller)

A wireless networking device called a WLC is used to manage and control several wireless access points (APs) inside a network. Its primary function is to centralize the management of the wireless network, providing a more efficient and scalable solution.

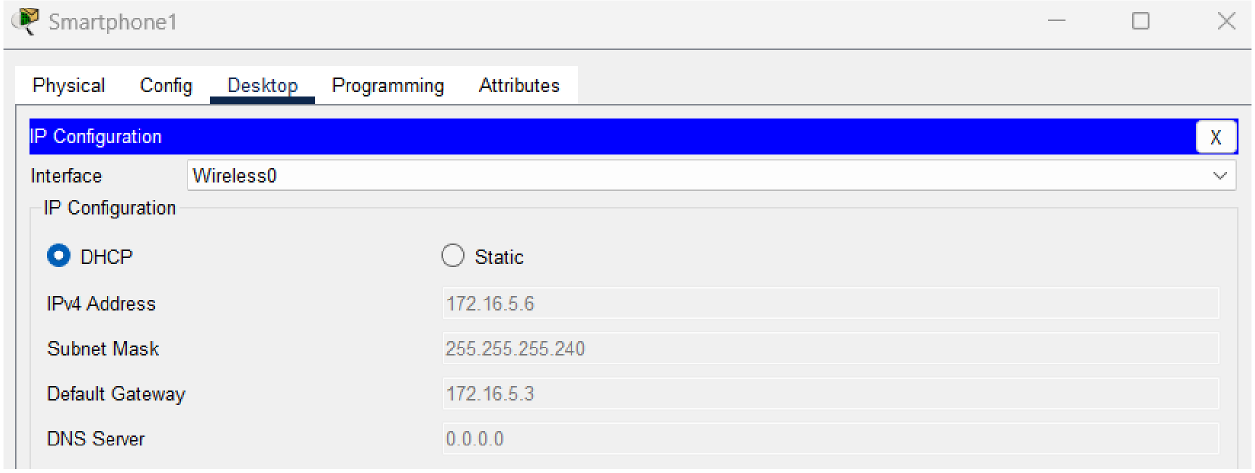




Management

IP Configuration

IPv4 Address	172.16.5.10
Subnet Mask	255.255.255.240
Default Gateway	172.16.5.3
DNS Server	8.8.8.8



Interface: Wireless0

IP Configuration

● DHCP ○ Static

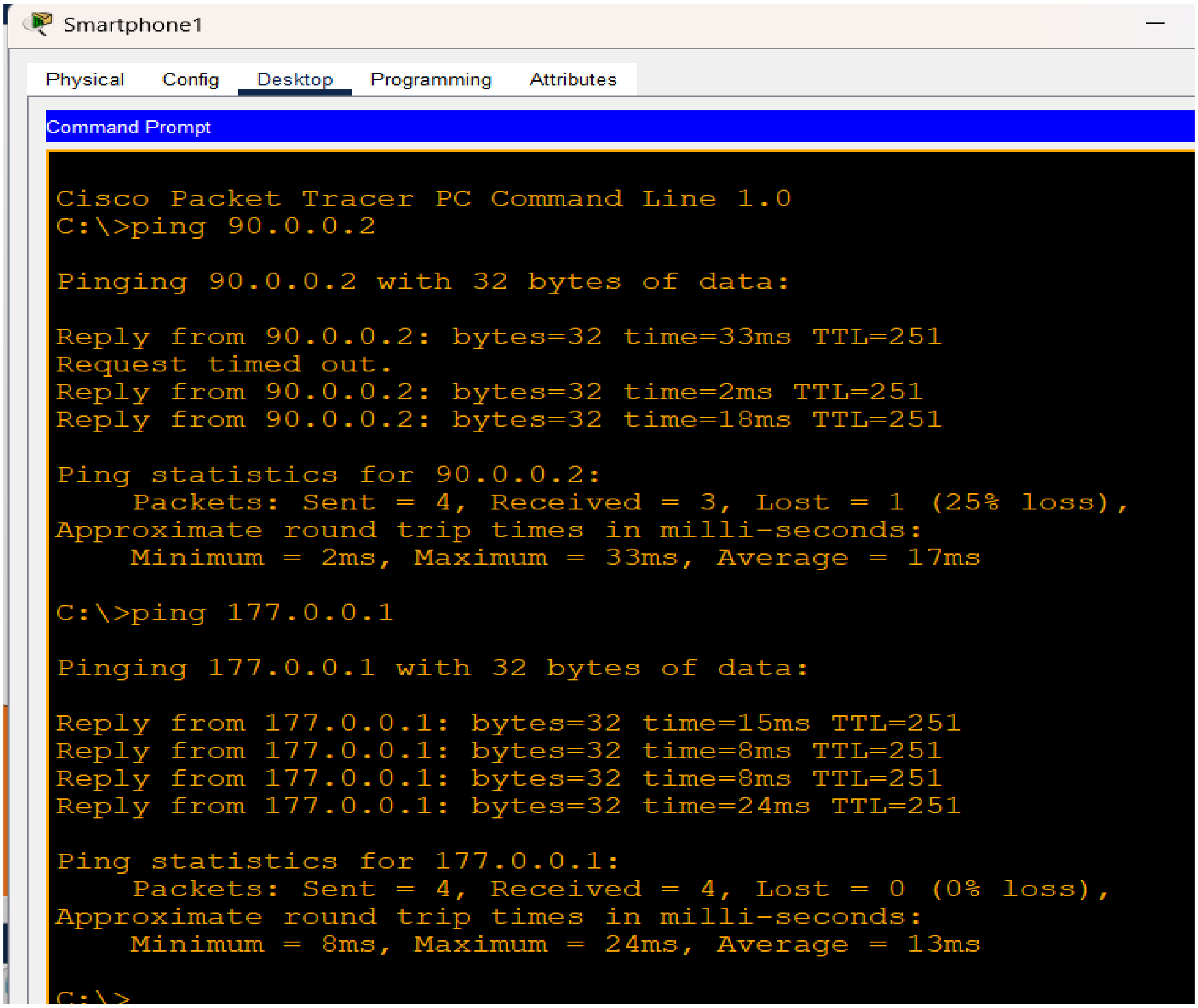
IPv4 Address: 172.16.5.6

Subnet Mask: 255.255.255.240

Default Gateway: 172.16.5.3

DNS Server: 0.0.0.0

Figure: Guest smartphone accessing internet



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 90.0.0.2

Pinging 90.0.0.2 with 32 bytes of data:

Reply from 90.0.0.2: bytes=32 time=33ms TTL=251
Request timed out.
Reply from 90.0.0.2: bytes=32 time=2ms TTL=251
Reply from 90.0.0.2: bytes=32 time=18ms TTL=251

Ping statistics for 90.0.0.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 33ms, Average = 17ms

C:\>ping 177.0.0.1

Pinging 177.0.0.1 with 32 bytes of data:

Reply from 177.0.0.1: bytes=32 time=15ms TTL=251
Reply from 177.0.0.1: bytes=32 time=8ms TTL=251
Reply from 177.0.0.1: bytes=32 time=8ms TTL=251
Reply from 177.0.0.1: bytes=32 time=24ms TTL=251

Ping statistics for 177.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 8ms, Maximum = 24ms, Average = 13ms

C:\>
```

Part C

Syslog and SNMP Servers:

A common protocol for transmitting and receiving log and event messages across a network is called Syslog. It allows various devices, such as routers, switches, servers, and security appliances, to generate and send log information to a centralized syslog server.

SNMP is a protocol used for network management and monitoring. It allows network administrators to monitor and control network devices, such as routers, switches, servers, printers, and more, from a central location.

Benefits: of Syslog Servers:

- Centralized Logging: Syslog servers centralize logs from various network devices, aiding in efficient monitoring and troubleshooting.
- Event Correlation: Syslog helps in correlating events across the network, allowing administrators to identify patterns and potential issues.
- Compliance and Auditing: Centralized logging assists in meeting compliance requirements and supports auditing activities.

SNMP Servers:

- Network Monitoring: SNMP servers facilitate real-time monitoring of network devices, providing insights into performance, bandwidth usage, and device health.
- Alerts and Notifications: SNMP enables the generation of alerts and notifications based on predefined thresholds, allowing proactive issue resolution.

- Capacity Planning: SNMP data assists in capacity planning by tracking resource utilization and trends over time.

Benefits of Implementation of Authentication Server:

- Centralized Authentication: Centralized authentication simplifies user management by allowing users to log in with a single set of credentials across the network.
- Enhanced Security: Authentication servers use robust protocols (e.g., RADIUS, LDAP) for secure user authentication, reducing the risk of unauthorized access.
- User Accountability: Centralized authentication facilitates user accountability and auditing, tracking who accessed the network and when.

Addressing Potential Security Challenges:

- Secure Transport: Use encrypted protocols (e.g., TLS) for transporting syslog and SNMP data to protect against interception and tampering.
- Access Control: Implement proper access controls for syslog and SNMP servers to restrict unauthorized access and ensure data confidentiality.
- Strong Encryption: Ensure strong encryption protocols for communication between network devices and the authentication server to safeguard user credentials.
- Two-Factor Authentication: Implement two-factor authentication to add an extra layer of security, requiring both a password and a secondary verification method.

Risk management, compliance, social, and legal issues in networking

In the ever-evolving landscape of networking technology, organizations faces some challenges that extend beyond the technical realm. Addressing issues related to risk management, compliance, social considerations, and legal aspects is crucial for the sustainable and secure deployment of networking technologies.

Risk Management:

Identification, evaluation, and mitigation of any hazards that could have an effect on a company's networking infrastructure are all part of risk management.By recognizing and controlling networking technology risks, a business may reduce the possibility of network outages, secure sensitive data, and maintain its good name.

Compliance:

Compliance refers to adhering to relevant laws, regulations, and industry standards that govern the use of networking technologies. Achieving compliance ensures that organizations operate ethically, avoid legal repercussions, and build trust with stakeholders. It also establishes a framework for data protection and privacy.

Social Issues:

Social issues in networking encompass the impact of technology on human interactions, privacy concerns, and the ethical implications of data usage. Addressing social issues fosters a positive organizational image, enhances customer trust, and promotes responsible use of technology. It also contributes to a healthy and ethical work culture.

Legal Issues:

Legal issues pertain to the laws and regulations governing the use of networking technology, including data protection, intellectual property, and cybersecurity laws.Adherence to legal frameworks ensures that organizations operate within the boundaries of the law, mitigating the risk of legal actions, fines, and reputational damage.

In a technology-driven era, networking is integral to organizational success, but it comes with inherent challenges beyond technical complexities. Effectively managing risks, ensuring compliance, addressing social considerations, and navigating legal landscapes are paramount for organizations that leverage networking technology. By doing so, organizations not only safeguard their assets and reputation but also contribute to a responsible and sustainable technological ecosystem.

Emerging Trends and Technologies in Networking:

Software-Defined Networking (SDN):

With the help of SDN, network devices' control plane and data plane may be separated, enabling centralized programmable control over the infrastructure.

Effect on the Architecture of Three-Tier Networks:

- Centralized Control: SDN centralizes network control, providing a more dynamic and programmable network infrastructure.
- Increased Agility: SDN enables quick and automated adjustments to network configurations, enhancing agility in response to changing requirements.
- Optimized Resource Utilization: Centralized control facilitates efficient resource allocation, optimizing the use of network resources across the three tiers.

Network Virtualization:

Creating many virtual networks on a single physical network infrastructure is known as network virtualization.

Effect on the Architecture of Three-Tier Networks:

- Isolation and Segmentation: Virtualization allows the creation of isolated network segments within the three-tier architecture, enhancing security and segmentation.
- Resource Efficiency: Virtualization makes it possible to use physical network resources more effectively by generating virtual instances that may be distributed dynamically in response to demand.

- Simplified Management: Virtual networks can be managed independently, simplifying administration within the three-tier architecture.

Cloud Computing:

Delivering computer services via the internet, such as networking, storage, and applications, is known as cloud computing.

Effect on the Architecture of Three-Tier Networks:

- Scalability: Cloud computing facilitates the seamless scalability of network resources, accommodating varying workloads within the three-tier architecture.
- Resource Accessibility: Cloud services provide ubiquitous access to network resources, allowing for flexible and distributed access points.
- Cost Efficiency: Cloud-based networking solutions may offer cost-effective alternatives for network infrastructure components, impacting the financial aspects of the three-tier architecture.

Emerging trends and technologies like SDN, network virtualization, and cloud computing are transforming traditional networking architectures. In the context of the three-tier network architecture, these advancements bring about increased flexibility, centralized control, and improved resource utilization. The impact is substantial, influencing the design and implementation of networks to meet the demands of modern, dynamic, and scalable computing environments. Organizations adopting these technologies within their three-tier architecture gain advantages in terms of efficiency, adaptability, and cost-effectiveness.

Conclusion

This report outlines the successful implementation of a comprehensive three-tier network architecture using Cisco Packet Tracer, incorporating advanced services. The architecture strategically employs OSPF for dynamic routing, enhancing network efficiency, and NAT for seamless internal and external network communication. VPN services add a layer of security, ensuring protected communication over public networks, while DHCP simplifies IP address management. The integration of STP contributes to network stability by preventing loop formation. WLC is incorporated for efficient wireless LAN control. The paper delves into cutting-edge technologies that go beyond traditional services, such as cloud computing, edge computing, software-defined networking (SDN), and network virtualization (NV). SDN brings centralized control and flexibility.

The report also delves into the integration of emerging technologies, such as Software-Defined Networking (SDN), Network Virtualization (NV), cloud computing, and edge computing. SDN brings flexibility and centralized control to the network, while NV optimizes resource utilization through virtualization. Cloud computing services enhance scalability, accessibility, and resource efficiency, while edge computing reduces latency by processing data closer to its source.

References

Three tier architectures: https://www.ibm.com/topics/three-tier-architecture

VLAN: https://www.practicalnetworking.net/stand-alone/configuring-vlans/

STP: https://www.techtarget.com/searchnetworking/definition/spanning-tree-protocol

HSRP: https://www.geeksforgeeks.org/hot-standby-router-protocol-hsrp/

NAT: https://www.manageengine.com/network-configuration-manager/configlets/configure-dynamic-nat-cisco.html

VPN: https://linuxtiwary.com/2016/03/26/vpn-configuration-lab-using-routers-in-cisco-packet-tracer/

Firewall: https://www.geeksforgeeks.org/basic-firewall-configuration-in-cisco-packet-tracer/

OSPF: https://study-ccna.com/ospf-configuration/

EIGRP:https://sites.radford.edu/~hlee3/classes/itec453_spring2023/Labs/Cisco_ScalingNetworks/Student%20Packet%20Tracer%20Source%20Files/7.2.2.4%20Packet%20Tracer%20-%20Configuring%20Basic%20EIGRP%20with%20IPv4%20Instructions.pdf