

Network Design and Security

Aarya Dahal

Bsc.Hons.Ethical Hacking and Cybersecurity, Softwarica College of IT and E-Commerce

ST5064CEM: Networking

Manoj Tamang

August 11, 2023

Abstract

This documentation abstract outlines the design of a robust and secure three-tier network for NetworkHats' headquarters and Kansas branch. The network architecture includes the implementation of VLANs, trunk and access links, OSPF and BGP routing protocol, NATing, ACL, VPN, EtherChannel, port security, DHCP, AAA, Syslog, SNMP, NTP and WLC. This comprehensive network design ensures seamless communication, efficient data transmission, and strong security measures, aligning perfectly with NetworkHats' reputation as a leading network and security consulting and deployment company in the USA.

Keywords

NETWORK
OSPF
HSRP ACCESS SWITCH ROUTER SECURITY
SYSLOG VLAN PORT SNMP
WLC AAA VPN
BGP VTP NAT
STP SSH DHCP STATIC TRUNK
SYSLOG SERVER SUBNETTING
FIREWALL IEEE

Table of Contents

Introduction.....	9
Network Architecture Guidelines	10
Three-Tier Network Architecture.....	10
Routing protocol.....	10
VLAN Segmentation.....	11
Trunk and Access links	11
EtherChannel for link aggregation	11
Port Security.....	11
DHCP for IP management.....	11
Network Address Translation (NAT).....	11
Access Control Lists (ACL).....	12
Virtual Private Network (VPN).....	12
Monitoring and Management services	12
Strategic Integration	12
Summary of Network.....	13
Redundancy	13
Bandwidth optimization	13
Scalability.....	13
Overview of network topology	14
Topology Discussion.....	14
Discussion on Physical Network.....	15
Access Layer	16
VLAN configuration	17
Trunk links	18
Vlan Trunking Protocol (VTP)	18
Port Security (Layer 2 security)	20
Distribution Layer	21
Subnetting.....	21
Routing Protocol	23
<i>OSPF</i>	23

Ether Channel	25
HSRP	26
Spanning Tree Protocol (STP)	27
Core Layer	28
IP assigned.....	28
EDGE.....	29
Assigned Networks in Edge	29
Routing Protocols in EDGE	30
<i>OSPF</i>	30
<i>BGP</i>	31
<i>Static Default</i>	33
Supernetting for Access Control Lists	33
<i>ACL for NAT</i>	33
<i>ACL for VPN</i>	34
Network Address Translation (NAT).....	34
Virtual Private Network (VPN).....	35
ISP	37
Assigned Networks in ISPs	37
BGP	38
Kansas Branch	41
Assigned Networks in Kansas branch.....	42
Routing Protocol	42
<i>OSPF</i>	42
<i>Static Default</i>	43
<i>BGP</i>	43
ACL for Kansas Branch	44
PAT for Kansas Branch.....	44
VPN.....	44
Services Configuration.....	45
DHCP	45
WLC	48

AAA	50
<i>SSH</i>	51
SMTP and POP3	52
SNMP	55
NTP	57
Syslog.....	58
Layer 2 security.....	59
DHCP snooping.....	59
BPDU guard	60
Firewall	61
Firewall configuration	61
<i>IP address assigned inside firewall</i>	62
<i>DHCP pool</i>	62
<i>ACL and Access groups</i>	63
<i>NAT</i>	64
<i>Static Default</i>	64
Router configuration	64
ICMP echo request	65
Software-Defined Networking (SDN)	66
Network Virtualization.....	66
Cloud computing	67
Impact on traditional three tier network	67
Risk Assessment and management	68
Enhancing Network Security: Comprehensive Policies and Procedures.....	69
Security in Network Architecture	69
Security via Configuration	69
Administrative Security.....	70
Adherence to Policy	70
Conclusion	71
References.....	72

Table of Figures

Figure 1	10
Figure 2	14
Figure 3	15
Figure 4	16
Figure 5	16
Figure 6	17
Figure 7	17
Figure 8	18
Figure 9	19
Figure 10	19
Figure 11	20
Figure 12	21
Figure 13	22
Figure 14	22
Figure 15	23
Figure 16	24
Figure 17	24
Figure 18	25
Figure 19	26
Figure 20	27
Figure 21	28
Figure 22	28
Figure 23	29
Figure 24	29
Figure 25	30
Figure 26	30
Figure 27	31
Figure 28	32
Figure 29	32
Figure 30	33
Figure 31	34
Figure 32	34
Figure 33	34
Figure 34	35
Figure 35	36
Figure 36	37
Figure 37	37
Figure 38	38
Figure 39	38
Figure 40	39
Figure 41	39
Figure 42	40
Figure 43	40

Figure 44	40
Figure 45	41
Figure 46	42
Figure 47	43
Figure 48	44
Figure 49	44
Figure 50	45
Figure 51	46
Figure 52	47
Figure 53	47
Figure 54	48
Figure 55	48
Figure 56	49
Figure 57	50
Figure 58	50
Figure 59	51
Figure 60	52
Figure 61	53
Figure 62	53
Figure 63	54
Figure 64	55
Figure 65	56
Figure 66	56
Figure 67	57
Figure 68	58
Figure 69	59
Figure 70	60
Figure 71	61
Figure 72	62
Figure 73	62
Figure 74	63
Figure 75	65
Figure 76	65

Introduction

NetworkHats, a renowned network and security consulting and deployment company, as a network engineer in the company, a sophisticated three-tier network for the headquarters and Kansas branch have been effectively designed.

The network design has encompassed three tiers: the core layer, distribution layer, and access layer. At the core layer, OSPF has been implemented to ensure efficient and scalable communication between network segments. Additionally, Border Gateway Protocol (BGP) has been configured to enhance network scalability and reliability by allowing dynamic routing updates between headquarters, Kansas branch and its ISPs.

The distribution layer has facilitated VLAN implementation to segment network traffic, optimizing performance and security for each department. Trunk and access links have been enabled for seamless data transfer between switches and end-user devices, while EtherChannel has enhanced bandwidth and redundancy. Port security mitigates unauthorized access attempts, and DHCP streamlines IP address assignment for efficient network management.

The architecture has included network address translation (NAT) to provide secure internet access for internal devices, hence protecting them from external threats. Security measures are a top priority in the design, featuring Access Control Lists (ACLs) that restrict network traffic ensuring only authorized communication to take place. To establish secure connections between headquarters and the Kansas branch, Virtual Private Networks (VPN) has been employed, safeguarding sensitive data during transmission.

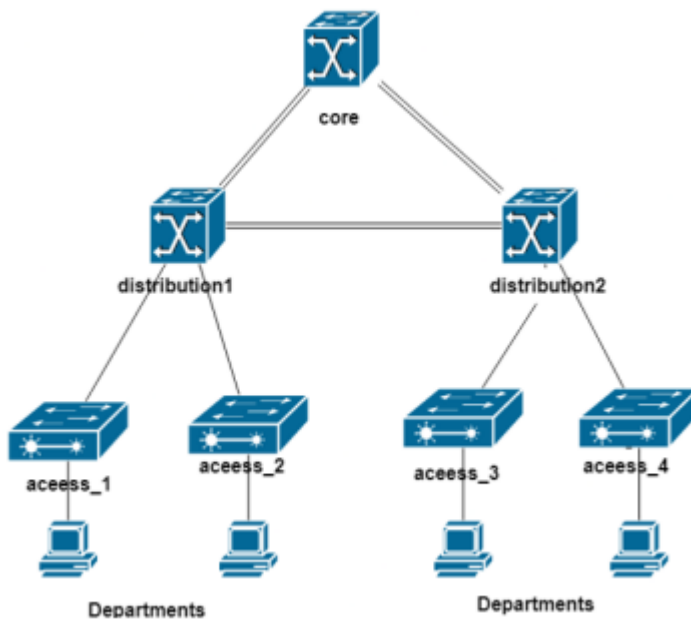
Services like AAA, SNMP, Syslog, NTP, WLC have been implemented. Each element has been strategically integrated to optimize communication, data transmission, and network security.

Network Architecture Guidelines

By adhering to the network architecture guidelines, the company can ensure a well-designed, efficient, and secure network that meets the unique needs of its clients and maintain its reputation as a leading network and security consulting and deployment company.

Figure 1

Three-tier network architecture



Three-Tier Network Architecture

Three-tier network architecture comprising the core layer, distribution layer, and access layer has been adopted. This design promotes scalability, flexibility, and efficient network management.

Routing protocol

Advanced routing protocols like OSPF to ensure efficient and scalable communication between network segments has been used. BGP has been implemented for dynamic routing updates between headquarters, branch, and ISPs to enhance network reliability.

VLAN Segmentation

VLANs has been used to logically segment network traffic, optimizing performance and security for different departments. This segregation enhances network efficiency and mitigates potential security risks.

Trunk and Access links

Trunk and access links has been enabled to facilitate seamless data transfer between switches and end-user devices. This enhances network efficiency and provides flexibility in managing multiple VLANs.

EtherChannel for link aggregation

EtherChannel technology has been adopted to combine multiple physical connections, increasing bandwidth and redundancy, thereby ensuring high availability and performance.

Port Security

Port security measures has been implemented to mitigate unauthorized access attempts and safeguard the network against potential security breaches. This adds an additional layer of protection to the network.

DHCP for IP management

DHCP services has been deployed to efficiently assign IP addresses to devices, streamlining network management and reducing manual configuration efforts.

Network Address Translation (NAT)

NAT has been incorporated to provide secure internet access for internal devices and protect them from external threats, ensuring data privacy and security.

Access Control Lists (ACL)

Utilize ACLs to restrict network traffic and control access, allowing only authorized communication and enhancing overall network security.

Virtual Private Network (VPN)

VPNs has been employed to establish secure connections between headquarters and the Kansas branch, safeguarding sensitive data during transmission over untrusted networks.

Monitoring and Management services

Services like AAA, SNMP, Syslog, NTP, and WLC has been implemented for centralized network monitoring, secure authentication, efficient management, and real-time alerts.

Strategic Integration

Each network element has been strategically integrated to optimize communication, data transmission, and network security, ensuring a robust and reliable network infrastructure.

Summary of Network

To ensure a highly stable and effective network, the advanced infrastructure prioritizes redundancy, bandwidth optimization, and scalability. The network offers smooth operations, optimal resource utilization, and the adaptability to meet changing business needs with its three-tier architecture, redundant links, VLAN segmentation, and dynamic routing protocols.

Redundancy

By employing a three-tier architecture with redundant links and devices at each layer, the network design prioritizes redundancy due to which data transfer can continue even if a connection or device fails. By merging multiple physical connections, boosting bandwidth, and providing alternative channels for data transfer, etherchannel further increases redundancy.

Bandwidth optimization

The network design optimizes bandwidth utilization through VLAN segmentation, logically isolating different types of network traffic. Advanced routing protocols like OSPF and BGP efficiently route data, dynamically calculating shortest paths and selecting optimal routes, minimizing congestion and maximizing bandwidth efficiency.

Scalability

The network design is highly scalable to accommodate future growth. VLAN implementation allows for easy addition of new departments without disruptions. Advanced routing protocols enable seamless expansion to additional branches or remote locations. VPNs provide a scalable solution for secure connections, facilitating network growth securely and efficiently.

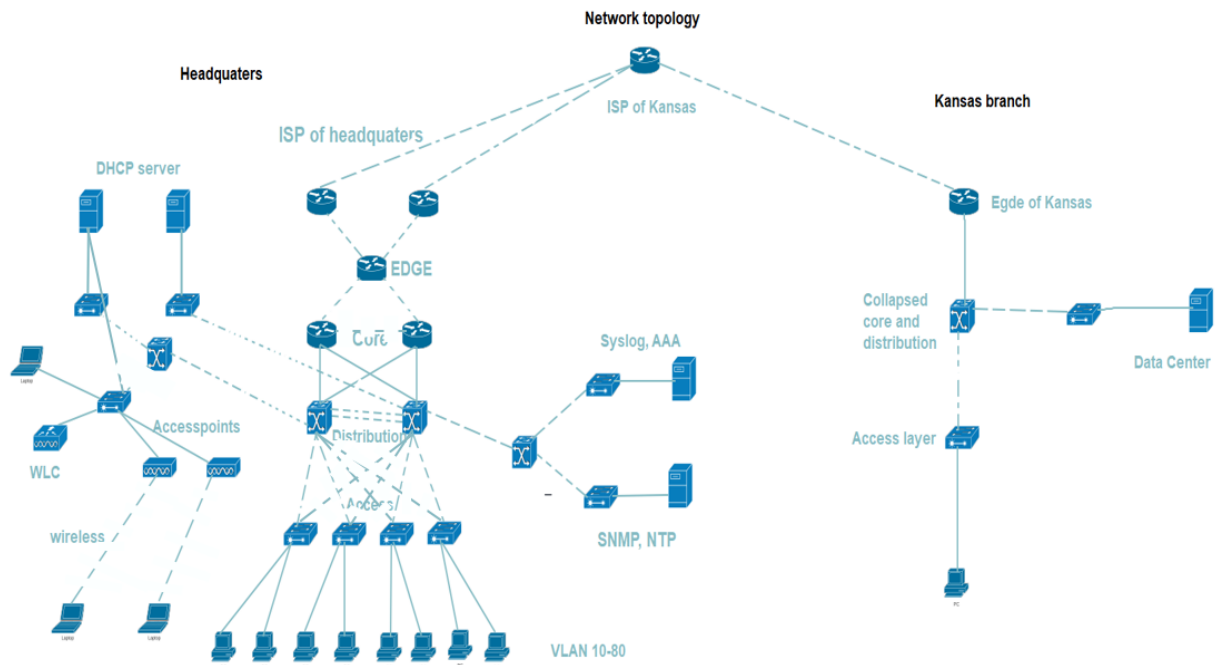
The following network was designed to provide redundancy and availability, which aid the firm in problem-solving.

Overview of network topology

The below topology represents the three-tier network architecture that has been implemented with the services enabled.

Figure 2

Logical Topological Diagram



Topology Discussion

The above three tier logical network topological diagram demonstrates the following fundamentals.

- VLSM on IP-address for each department to its prevent loss.
- Primary and Secondary DHCP is configured for redundancy which provides IP for the vlans for effective network management.
- A WLC has also been configured which also pulls the IP from the DHCP pool which centrally manages and control access points (APs) in a wireless network.
- Access-points have been used to provide wireless internet services.

- HSRP and ether channel has been configured to provide redundancy.
- OSPF is implemented on the private network while BGP is enabled on the public network connection to direct traffic through various networks.
- ACL and NAT have been configured as security measure along with VPN connecting the headquarters and branch.
- Different services like SNMP, Syslog, AAA, NTP have been enabled.

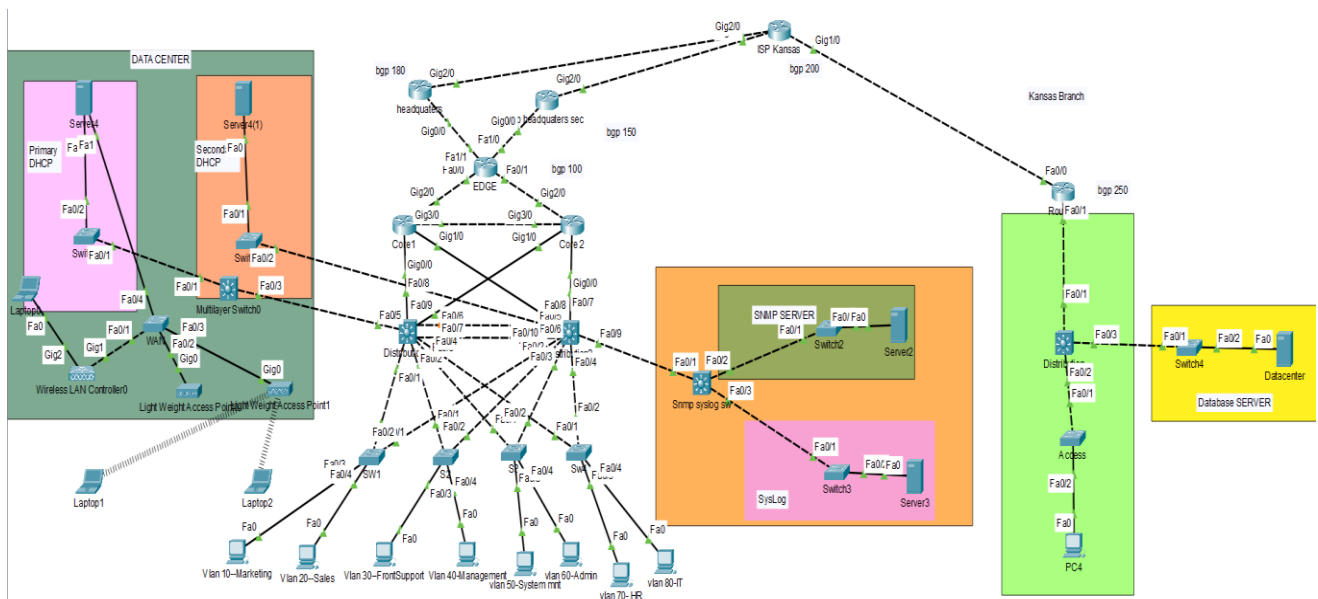
Discussion on Physical Network

Considering the three tier model, all the tiers with the services implemented on each has been briefly discussed.

- Edge
- Core Layer
- Distribution Layer
- Access Layer

Figure 3

Physical Diagram

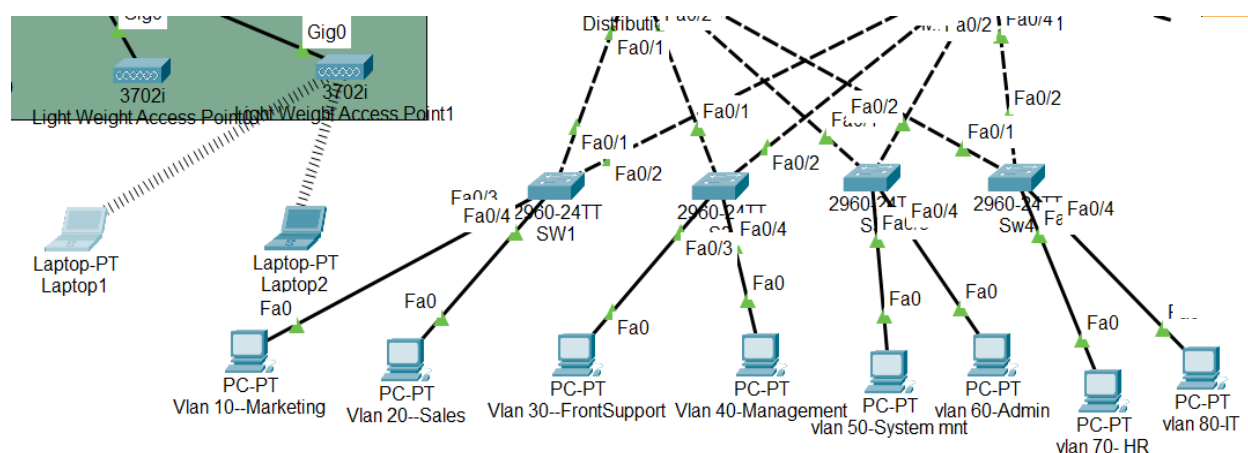


Access Layer

The first tier of three-tier network architecture consists of four switches and two light weight access point providing wireless network services.

Figure 4

Access Layer



8 vlans are created which is gets IP address through DHCP using DORA process. VLSM is done while assigning network to each branch whose information is shown below.

Figure 5

Network assigned for each vlan

Departments	VLAN	Network Address/CIDR	Hosts
Marketing	10	172.16.0.3-61/26	35
Sales	20	172.16.0.67-125/26	30
Front Support	30	172.16.0.131-157/27	20
Management	40	172.16.0.163-173/28	10
System Admin	50	172.16.0.179-189/28	8
Admin	60	172.16.0.195-205/28	8
HR	70	172.16.0.211-221/28	7
IT	80	172.16.0.277-237/28	7

VLAN configuration

In order to improve security, effectiveness, and management flexibility, network traffic is logically divided and isolated inside a physical network using VLANs (Virtual Local Area Networks). By establishing different divisions, it also simplifies network setup, and enhances overall organization.

Figure 6

Vlan information in sw1

```
Access1(config)#do sh 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	VLAN0010	active	Fa0/3
20	VLAN0020	active	Fa0/4
30	VLAN0030	active	
40	VLAN0040	active	
50	VLAN0050	active	
60	VLAN0060	active	
70	VLAN0070	active	

Figure 7

Vlan infomration in sw3

```
access3(config-if)#do sh 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	VLAN0010	active	
20	VLAN0020	active	
30	VLAN0030	active	
40	VLAN0040	active	
50	VLAN0050	active	Fa0/3
60	VLAN0060	active	Fa0/4
70	VLAN0070	active	
80	VLAN0080	active	

Likewise, all interfaces which are connected with each department have been changed to access links and separately divided into vlans.

Trunk links

Four access switched has been connected to multilayer switch and IEE standard trunk links are created to carry all VLANs over a single physical connection, enabling efficient communication between switches and optimizing bandwidth utilization in a network.

Figure 8

Trunk links

```
Access1(config)#do sh 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     10,20,30,40,50,60,70,80
Fa0/2     1,10,20,30,40,50,60,70,80
```

Similarly, all interface connected to the multilayer switch has been changed to trunk links in other access switches.

Vlan Trunking Protocol (VTP)

By managing and synchronizing VLAN configurations across several switches, VTP (VLAN Trunking Protocol) simplifies VLAN management and ensures consistency in a network environment. Here, VTP is enabled in all switches and two switches are set as server while the other as client. This enables only server VTP to configure vlan. It can also be taken as a security measure ([Understand VLAN Trunk Protocol \(VTP\), 2022](#)).

Figure 9*VTP server*


```

VTP Version capable      : 1 to 2
VTP version running      : 2
VTP Domain Name          : aarya
VTP Pruning Mode         : Disabled
VTP Traps Generation     : Disabled
Device ID                : 00D0.5872.B200
Configuration last modified by 0.0.0.0 at 8-7-23 17:13:58
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    : 361
MD5 digest               : 0x24 0x6C 0x2E 0x9B 0xD3 0x2D 0x01 0x7C
                        : 0x1B 0xBC 0xCC 0x42 0x0F 0x42 0xD1 0xCA

```

password of VTP domain



In terms of security, the server mode of VTP allows for VLAN configuration changes, so restricting access helps prevent unauthorized or accidental modifications that could impact network stability or security. Thus, server mode is connected with IT and admin departments.

Figure 10*VTP Client*


```

VTP Version capable      : 1 to 2
VTP version running      : 2
VTP Domain Name          : aarya
VTP Pruning Mode         : Disabled
VTP Traps Generation     : Disabled
Device ID                : 0060.47C4.BA00
Configuration last modified by 0.0.0.0 at 8-7-23 17:13:58

Feature VLAN :
-----
VTP Operating Mode       : Client
Maximum VLANs supported locally : 255
Number of existing VLANs : 13
Configuration Revision    : 361
MD5 digest               : 0x24 0x6C 0x2E 0x9B 0xD3 0x2D 0x01 0x7C
                        : 0x1B 0xBC 0xCC 0x42 0x0F 0x42 0xD1 0xCA

```

VTP encrypted password



The client mode is useful for enhancing security by ensuring that VLAN updates come from trusted sources (servers). By designating specific switches as clients, limited ability to make unauthorized changes to VLAN configurations is assured. Thus, reducing the risk of malicious alterations or configuration errors that could compromise network integrity.

Port Security (Layer 2 security)

Figure 11

Port Security in access switches of VLAN and DHCP

```
Access1(config)#do sh port-security int f0/3
Port Security           : Enabled
Port Status             : Secure-up
Violation Mode          : Restrict
Aging Time              : 0 mins
Aging Type              : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses   : 1
Total MAC Addresses     : 1
Configured MAC Addresses : 1
Sticky MAC Addresses    : 0
Last Source Address:Vlan : 0000.0000.0000:0
Security Violation Count : 0

DHCP-access-SW(config)#do sh port-security int f0/1
Port Security           : Enabled
Port Status             : Secure-up
Violation Mode          : Restrict
Aging Time              : 0 mins
Aging Type              : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses   : 1
Total MAC Addresses     : 1
Configured MAC Addresses : 1
Sticky MAC Addresses    : 0
Last Source Address:Vlan : 0000.0000.0000:0
Security Violation Count : 0

DHCP-access-SW(config) #
```

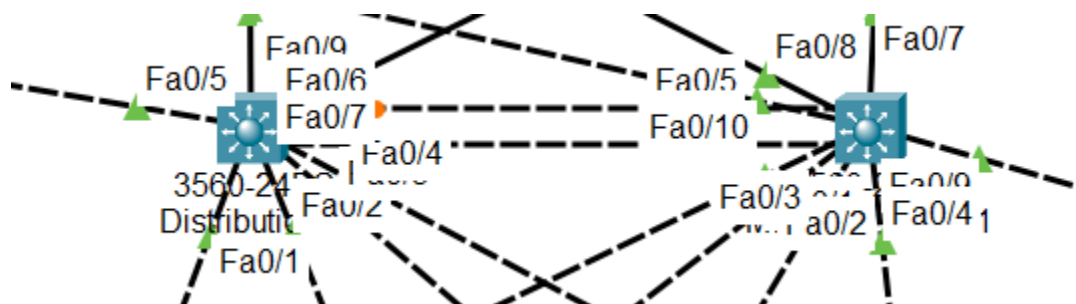
Port security is set up here to improve network security by limiting access to Ethernet ports on a switch, helping in prevention of unauthorized devices from joining to the network. Additionally, it lessens the chance of unauthorized data access, network breaches, or other security threats. Additionally, it guarantees that only approved devices contribute to network traffic and that network resources are used effectively ([Switchport Port Security Explained With Examples, n.d.](#)).

Distribution Layer

The second tier of the three-tier network is distribution layer. Multilayer switches have been used for this purpose since it provides both switching as well as routing services. The multilayer switches are used here to direct traffic between each department. It also provides redundancy since protocols HSRP (Hot Standby Router Protocol) has been implemented to ensure high availability. They also enable load balancing by distributing traffic across multiple paths, optimizing network performance. It also allows for the easy addition of new access layer switches or devices without affecting the core layer. Thus, supports network growth and expansion for additional users or departments.

Figure 12

Multilayer switches for distribution layer



Subnetting

The network of 172.16.0.0 was taken and further proceeded to VLSM. The sub vlan interface (SVI) was utilized to assign each department different subnetted network. ([Can Anyone Please Explain L3 SVI Configuration. What Is SVI and Where, 2021](#)). This optimizes address space utilization, reducing IP address wastage also conserving IP addresses and allocating them based on the actual requirements of each department. VLSM is also done since it enhances network performance, security, and management by isolating broadcast domains and controlling traffic flow.

Figure 13*VLSM on network 172.16.0.0*

Subnet Name	Needed Size	Allocated Size	Address	Mask	Dec Mask	Assignable Range
Marketing	35	62	172.16.0.0	/26	255.255.255.192	172.16.0.1 - 172.16.0.62
Sales	31	62	172.16.0.64	/26	255.255.255.192	172.16.0.65 - 172.16.0.126
FrontSupport	20	30	172.16.0.128	/27	255.255.255.224	172.16.0.129 - 172.16.0.158
Management	10	14	172.16.0.160	/28	255.255.255.240	172.16.0.161 - 172.16.0.174
System Admin	8	14	172.16.0.176	/28	255.255.255.240	172.16.0.177 - 172.16.0.190
Admin	7	14	172.16.0.192	/28	255.255.255.240	172.16.0.193 - 172.16.0.206
HR	7	14	172.16.0.208	/28	255.255.255.240	172.16.0.209 - 172.16.0.222
IT	7	14	172.16.0.224	/28	255.255.255.240	172.16.0.225 - 172.16.0.238

Figure 14*IP assigned in SVI interface of distribution switches.*

```

PrimaryDistribution(config)#do sh ip int brief | ex una
Interface                IP-Address      OK? Method Status      Protocol
FastEthernet0/5          111.10.0.1      YES manual up          up
FastEthernet0/8          11.0.0.2        YES manual up          up
FastEthernet0/9          14.0.0.2        YES manual up          up
Vlan10                   172.16.0.1      YES manual up          up
Vlan20                   172.16.0.65     YES manual up          up
Vlan30                   172.16.0.129    YES manual up          up
Vlan40                   172.16.0.161    YES manual up          up
Vlan50                   172.16.0.177    YES manual up          up
Vlan60                   172.16.0.193    YES manual up          up
Vlan70                   172.16.0.209    YES manual up          up
Vlan80                   172.16.0.225    YES manual up          up

DistributionStandby(config)#do sh ip int brief | ex una
Interface                IP-Address      OK? Method Status      Protocol
FastEthernet0/7          12.0.0.2        YES manual up          up
FastEthernet0/8          13.0.0.2        YES manual up          up
FastEthernet0/9          160.10.1.1      YES manual up          up
FastEthernet0/10         16.0.0.2        YES manual up          up
Vlan10                   172.16.0.2      YES manual up          up
Vlan20                   172.16.0.66     YES manual up          up
Vlan30                   172.16.0.130    YES manual up          up
Vlan40                   172.16.0.162    YES manual up          up
Vlan50                   172.16.0.178    YES manual up          up
Vlan60                   172.16.0.194    YES manual up          up
Vlan70                   172.16.0.210    YES manual up          up
Vlan80                   172.16.0.226    YES manual up          up
DistributionStandby(config)#

```

Routing Protocol

Routing protocols determine the best path for data packets to travel from the source to the destination and also provides redundancy, by offering alternate paths in case of link failures. This ensures uninterrupted connectivity and high availability, minimizing network downtime. It continuously updates routing tables to reflect changes in network conditions so that routers quickly adapt to topology changes, leading to faster convergence and minimal disruption in case of network changes or failures. [\(Keary, 2018\)](#)

OSPF

OSPF, a link-state routing protocol provides a range of benefits for network design and management. It's link-state algorithm ensures swift detection of network changes, leading to rapid convergence and minimal downtime during failures or topology adjustments. It's optimal routing calculations based on the Dijkstra algorithm which leads to efficient data transmission. It supports equal-cost load balancing which optimizes bandwidth usage and prevents congestion. Additionally, because OSPF is compatible with many different devices and works well together with other systems, it's a great option for all kinds of different networks. Overall, it contributes to resilient, efficient, and secure network operations.

Figure 15

OSPF configuration

```
PrimaryDistribution(config)#do sh run | sec ospf
router ospf 10
 log-adjacency-changes
 network 111.0.0.0 0.255.255.255 area 0
 network 172.16.0.0 0.0.0.63 area 0
 network 14.0.0.0 0.255.255.255 area 0
 network 11.0.0.0 0.255.255.255 area 0
 network 172.16.0.64 0.0.0.63 area 0
 network 172.16.0.128 0.0.0.63 area 0
 network 172.16.0.128 0.0.0.31 area 0
 network 172.16.0.160 0.0.0.15 area 0
 network 172.16.0.176 0.0.0.15 area 0
 network 172.16.0.192 0.0.0.15 area 0
 network 172.16.0.208 0.0.0.15 area 0
 network 172.16.0.224 0.0.0.15 area 0
PrimaryDistribution(config)#
```

Figure 16*OSPF neighbors*

```
DistributionStandby(config)#do sh ip ospf neigh
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
160.12.1.2	1	FULL/BDR	00:00:33	160.10.1.2	FastEthernet0/9
30.0.0.1	1	FULL/BDR	00:00:33	12.0.0.1	FastEthernet0/7
20.0.0.1	1	FULL/BDR	00:00:34	13.0.0.1	FastEthernet0/8
172.16.0.225	1	FULL/BDR	00:00:34	172.16.0.177	Vlan50
172.16.0.225	1	FULL/BDR	00:00:34	172.16.0.65	Vlan20
172.16.0.225	1	FULL/BDR	00:00:34	172.16.0.209	Vlan70
172.16.0.225	1	FULL/BDR	00:00:33	172.16.0.225	Vlan80
172.16.0.225	1	FULL/BDR	00:00:34	172.16.0.161	Vlan40
172.16.0.225	1	FULL/BDR	00:00:35	172.16.0.129	Vlan30
172.16.0.225	1	FULL/BDR	00:00:34	172.16.0.193	Vlan60

```
DistributionStandby(config)#
```

```
DistributionStandby(config)#
```

```
DistributionStandby(config)#do sh ip route
```

Figure 17*OSPF Routes*

```
O    10.0.0.0/8 [110/2] via 13.0.0.1, 00:4294967280:4294967295, FastEthernet0/8
O    11.0.0.0/8 [110/2] via 13.0.0.1, 00:4294967280:4294967295, FastEthernet0/8
    [110/2] via 172.16.0.65, 00:4294967280:4294967295, Vlan20
    [110/2] via 172.16.0.129, 00:4294967280:4294967295, Vlan30
    [110/2] via 172.16.0.161, 00:4294967280:4294967295, Vlan40
    [110/2] via 172.16.0.177, 00:4294967280:4294967295, Vlan50
    [110/2] via 172.16.0.193, 00:4294967280:4294967295, Vlan60
    [110/2] via 172.16.0.209, 00:4294967280:4294967295, Vlan70
    [110/2] via 172.16.0.225, 00:4294967280:4294967295, Vlan80

O    20.0.0.0/8 [110/2] via 13.0.0.1, 00:4294967280:4294967295, FastEthernet0/8
O    30.0.0.0/8 [110/2] via 12.0.0.1, 00:4294967281:4294967245, FastEthernet0/7
O    111.0.0.0/8 [110/2] via 172.16.0.65, 00:4294967281:4294967245, Vlan20
    [110/2] via 172.16.0.129, 00:4294967281:4294967245, Vlan30
    [110/2] via 172.16.0.161, 00:4294967281:4294967245, Vlan40
    [110/2] via 172.16.0.177, 00:4294967281:4294967245, Vlan50
    [110/2] via 172.16.0.193, 00:4294967281:4294967245, Vlan60
    [110/2] via 172.16.0.209, 00:4294967281:4294967245, Vlan70
    [110/2] via 172.16.0.225, 00:4294967281:4294967245, Vlan80

C    160.10.0.0/16 is directly connected, FastEthernet0/9
O    160.11.0.0/16 [110/2] via 160.10.1.2, 00:4294967281:4294967245, FastEthernet0/9
O    160.12.0.0/16 [110/2] via 160.10.1.2, 00:4294967281:4294967245, FastEthernet0/9
    172.16.0.0/16 is variably subnetted, 8 subnets, 3 masks
C    172.16.0.0/26 is directly connected, Vlan10
C    172.16.0.64/26 is directly connected, Vlan20
C    172.16.0.128/27 is directly connected, Vlan30
C    172.16.0.160/28 is directly connected, Vlan40
C    172.16.0.176/28 is directly connected, Vlan50
C    172.16.0.192/28 is directly connected, Vlan60
C    172.16.0.208/28 is directly connected, Vlan70
C    172.16.0.224/28 is directly connected, Vlan80
O*E2 0.0.0.0/0 [110/1] via 12.0.0.1, 00:4294967280:4294967295, FastEthernet0/7
    [110/1] via 13.0.0.1, 00:4294967280:4294967295, FastEthernet0/8
```


Ether Channel

In the context of these two distribution switches, EtherChannel serves as a powerful network enhancement. By creating an EtherChannel between these switches, two links are aggregated into a single logical connection. This configuration offers significant benefits, such as increasing the available bandwidth for data exchange between the distribution switches.

Redundancy is increased, as a failure in one link won't disrupt connectivity since traffic can seamlessly flow through the remaining operational links. Load balancing ensures that network traffic is efficiently distributed across the bundled links, preventing congestion and optimizing performance. The simplified management of the EtherChannel simplifies the configuration and monitoring of these connections, contributing to streamlined network operations ([EtherChannel in Computer Network - GeeksforGeeks, 2018](#)).

Figure 18

EtherChannel Summary

```
interface FastEthernet0/6
  no switchport
  no ip address
  channel-group 10 mode active
  duplex auto
  speed auto
interface FastEthernet0/7
  no switchport
  no ip address
  channel-group 10 mode active
  duplex auto
  speed auto

!
interface FastEthernet0/5
  no switchport
  no ip address
  channel-group 10 mode passive
  duplex auto
  speed auto
!
interface FastEthernet0/6
  no switchport
  no ip address
  channel-group 10 mode passive
  duplex auto
  speed auto
.
```

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

Group	Port-channel	Protocol	Ports
10	Po10 (RU)	LACP	Fa0/6 (P) Fa0/7 (P)

```
PrimaryDistribution(config)#
```

Here, two port was bundled together using LACP method which is a IEE standard. Active and passive mode was used to bundle the links together.

HSRP

In the context of the two distribution switches, Hot Standby Router Protocol (HSRP) plays a crucial role in ensuring network availability and redundancy. HSRP is configured here to make the switches work together as a high-availability pair. By configuring HSRP, one distribution switch becomes the active while the other functions as a standby. The active switch handles normal traffic operations, while the other takes over in case of failure. It also provides load sharing since both switches can distribute traffic, optimizing resource usage ([Understand the Hot Standby Router Protocol Features and Functionality, 2022](#)).

Figure 19

HSRP configuration

```
PrimaryDistribution(config)#do sh standby brief
P indicates configured to preempt.
```

Interface	Grp	Pri	P	State	Active	Standby	Virtual IP
Vl110	10	110	P	Active	local	172.16.0.2	172.16.0.62
Vl120	10	110	P	Active	local	172.16.0.66	172.16.0.126
Vl130	10	110	P	Active	local	172.16.0.130	172.16.0.158
Vl140	10	110	P	Active	local	172.16.0.162	172.16.0.174
Vl150	10	110	P	Active	local	172.16.0.178	172.16.0.190
Vl160	10	110	P	Active	local	172.16.0.194	172.16.0.206
Vl170	10	110	P	Active	local	172.16.0.210	172.16.0.222
Vl180	10	110	P	Active	local	172.16.0.226	172.16.0.238

```
PrimaryDistribution(config)#
```



```
DistributionStandby(config)#do sh standby br
P indicates configured to preempt.
```

Interface	Grp	Pri	P	State	Active	Standby	Virtual IP
Vl110	10	100	P	Standby	172.16.0.1	local	172.16.0.62
Vl120	10	100	P	Standby	172.16.0.65	local	172.16.0.126
Vl130	10	100	P	Standby	172.16.0.129	local	172.16.0.158
Vl140	10	100	P	Standby	172.16.0.161	local	172.16.0.174
Vl150	10	100	P	Standby	172.16.0.177	local	172.16.0.190
Vl160	10	100	P	Standby	172.16.0.193	local	172.16.0.206
Vl170	10	100	P	Standby	172.16.0.209	local	172.16.0.222
Vl180	10	100	P	Standby	172.16.0.225	local	172.16.0.238

```
DistributionStandby(config)#
```

Here, Virtual IP for each vlan is set so that, IP address remains constant regardless of which switch is active and serves as this point of contact, allowing devices to reach the network even in the case of one switch failure, allowing for efficient distribution of traffic. The primary distribution is given priority 110 so that it can remain as an active switch for data transfer.

Spanning Tree Protocol (STP)

The Rapid Per-VLAN Spanning Tree (Rapid PVST) mode is used in this network configuration. By providing distinct spanning tree instances for each VLAN, Rapid PVST, enables quicker convergence and greater utilization of network resources.

STP load balancing is used on the main distribution switch for VLANs 10, 20, 30, and 40. The secondary distribution switch balances STP load for VLANs 50, 60, 70, and 80 concurrently. This one improves network performance by strategically allocating traffic among the available paths for the particular VLANs in each switch.

Figure 20

RSTP and load balancing in primary distribution and distribution standby

```
VLAN0010
Spanning tree enabled protocol rstp
Root ID    Priority    10
           Address    0090.2BA5.0A9B
           This bridge is the root
           Hello Time 2 sec   Max Age 20 sec   Forward Delay 15 sec

           Bridge ID  Priority    10 (priority 0 sys-id-ext 10)
           Address    0090.2BA5.0A9B
           Hello Time 2 sec   Max Age 20 sec   Forward Delay 15 sec
           Aging Time 20

Interface    Role Sts Cost        Prio.Nbr Type
-----
Fa0/1        Desg FWD 19          128.1    P2p
Fa0/2        Desg FWD 19          128.2    P2p
Fa0/3        Desg FWD 19          128.3    P2p
Fa0/4        Desg FWD 19          128.4    P2p

VLAN0080
Spanning tree enabled protocol rstp
Root ID    Priority    80
           Address    0006.2AE4.11D9
           This bridge is the root
           Hello Time 2 sec   Max Age 20 sec   Forward Delay 15 sec

           Bridge ID  Priority    80 (priority 0 sys-id-ext 80)
           Address    0006.2AE4.11D9
           Hello Time 2 sec   Max Age 20 sec   Forward Delay 15 sec
           Aging Time 20

Interface    Role Sts Cost        Prio.Nbr Type
-----
Fa0/3        Desg FWD 19          128.3    P2p
Fa0/2        Desg FWD 19          128.2    P2p
Fa0/1        Desg FWD 19          128.1    P2p
Fa0/4        Desg FWD 19          128.4    P2p

DistributionStandby(config)#
DistributionStandby(config)#
```

Core Layer

In this network architecture, two routers are placed in the core layer. They play a critical role in facilitating efficient and high-speed communication between different parts of the network. The core layer routers serve as a central hub for data traffic from distribution switches and access layer. It uses advanced routing protocols OSPF and BGP to make routing decisions and ensure the most optimal paths for data to flow.

IP assigned

Figure 21

IP addresses in core routers

core1(config)#do sh ip int brief ex una					
Interface	IP-Address	OK?	Method	Status	Protocol
GigabitEthernet0/0	11.0.0.1	YES	manual	up	up
GigabitEthernet1/0	13.0.0.1	YES	manual	up	up
GigabitEthernet2/0	20.0.0.1	YES	manual	up	up
GigabitEthernet3/0	10.10.10.1	YES	manual	up	up
core1(config)#					
core2(config)#do sh ip int brief ex una					
Interface	IP-Address	OK?	Method	Status	Protocol
GigabitEthernet0/0	12.0.0.1	YES	manual	up	up
GigabitEthernet1/0	14.0.0.1	YES	manual	up	up
GigabitEthernet2/0	30.0.0.1	YES	manual	up	up
GigabitEthernet3/0	10.10.10.2	YES	manual	up	up
core2(config)#					

The four IP addresses assigned are in the links connecting the two distribution switch, another core and edge router. Here, OSPF is also used as a routing protocol.

OSPF

Figure 22

OSPF network in cores

<pre>core1(config)#do sh run sec ospf router ospf 10 log-adjacency-changes network 13.0.0.0 0.255.255.255 area 0 network 20.0.0.0 0.255.255.255 area 0 network 10.0.0.0 0.255.255.255 area 0 network 11.0.0.0 0.255.255.255 area 0</pre>	<pre>core2(config)#do sh run sec ospf router ospf 10 log-adjacency-changes network 12.0.0.0 0.255.255.255 area 0 network 14.0.0.0 0.255.255.255 area 0 network 30.0.0.0 0.255.255.255 area 0 core2(config)#</pre>
---	---

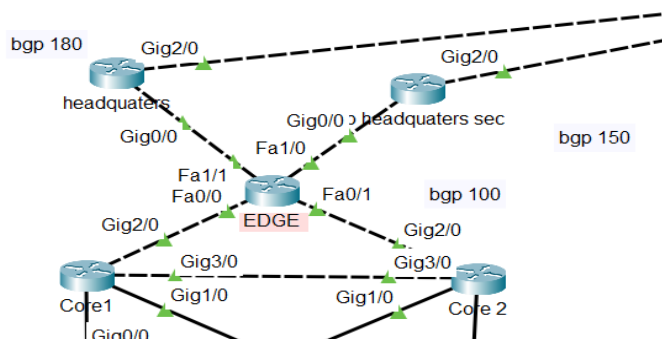
The network routed through ospf are shown above. The core layer is further connected to edge where nat and acl are configured.

EDGE

An edge router has been setup in the network to manage all routing functions of OSPF, default Static and BGP, directing traffic between the internal network and external networks. NAT has also been configured to allow multiple devices within the internal network to share a single public IP address when communicating with external networks. This enhances security and conserves IPv4 addresses. Access control policies have also been made to allow internal traffic to public IP. VPN has also been configured inside to connect headquarters and Kansas branch private IP. A separate ACL has been configured for VPN.

Figure 23

Edge Router



Assigned Networks in Edge

Networks 40.0.0.0/8 and 50.0.0.0/8 are configured on public interface towards ISP while 30.0.0.0/8 and 20.0.0.0/8 are configured inside private interface which are connected in the cores.

Figure 24

Networks inside Edge

```
EDGE(config)#do sh ip int brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/0	20.0.0.2	YES	manual	up	up
FastEthernet0/1	30.0.0.2	YES	manual	up	up
FastEthernet1/0	50.0.0.1	YES	manual	up	up
FastEthernet1/1	40.0.0.1	YES	manual	up	up
Vlan1	unassigned	YES	unset	administratively down	down

```
EDGE(config)#
```

Routing Protocols in EDGE

OSPF, Static default and BGP are used to route traffics in the EDGE router. OSPF is used in the private interface while BGP is configured in the public IP interface which is further connected to ISPs.

OSPF

OSPF is used to route all private traffic inside the headquarters. Traffic from access layer and distribution layer are also routed to OSPF in edge. Further, "default-information originate," is configured inside OSPF so that it advertises a default route (0.0.0.0/0) into the routing domain.

Figure 25

OSPF Routes

```
EDGE#show ip route ospf
O    10.0.0.0 [110/2] via 20.0.0.1, 02:06:50, FastEthernet0/0
O    11.0.0.0 [110/2] via 20.0.0.1, 02:06:50, FastEthernet0/0
O    12.0.0.0 [110/2] via 30.0.0.1, 02:06:50, FastEthernet0/1
O    13.0.0.0 [110/2] via 20.0.0.1, 02:06:50, FastEthernet0/0
O    14.0.0.0 [110/2] via 30.0.0.1, 02:06:50, FastEthernet0/1
O    15.0.0.0 [110/4] via 20.0.0.1, 02:06:50, FastEthernet0/0
O    16.0.0.0 [110/4] via 30.0.0.1, 02:06:50, FastEthernet0/1
O    16.0.0.0 [110/3] via 20.0.0.1, 02:06:50, FastEthernet0/0
O    16.0.0.0 [110/3] via 30.0.0.1, 02:06:50, FastEthernet0/1
O    111.0.0.0 [110/3] via 20.0.0.1, 02:06:50, FastEthernet0/0
O    160.10.0.0 [110/3] via 30.0.0.1, 02:06:50, FastEthernet0/1
O    160.11.0.0 [110/3] via 20.0.0.1, 02:06:50, FastEthernet0/0
O    160.12.0.0 [110/4] via 30.0.0.1, 02:06:50, FastEthernet0/1
O    160.12.0.0 [110/4] via 20.0.0.1, 02:06:50, FastEthernet0/0
O    160.12.0.0 [110/4] via 30.0.0.1, 02:06:50, FastEthernet0/1
O    172.16.0.0/16 is variably subnetted, 8 subnets, 3 masks
O    172.16.0.0 [110/3] via 20.0.0.1, 02:06:50, FastEthernet0/0
O    172.16.0.0 [110/3] via 30.0.0.1, 02:06:50, FastEthernet0/1
O    172.16.0.64 [110/3] via 20.0.0.1, 02:06:50, FastEthernet0/0
O    172.16.0.64 [110/3] via 30.0.0.1, 02:06:50, FastEthernet0/1
O    172.16.0.128 [110/3] via 20.0.0.1, 02:06:50, FastEthernet0/0
O    172.16.0.128 [110/3] via 30.0.0.1, 02:06:50, FastEthernet0/1
O    172.16.0.160 [110/3] via 20.0.0.1, 02:06:50, FastEthernet0/0
O    172.16.0.160 [110/3] via 30.0.0.1, 02:06:50, FastEthernet0/1
O    172.16.0.176 [110/3] via 20.0.0.1, 02:06:50, FastEthernet0/0
O    172.16.0.176 [110/3] via 30.0.0.1, 02:06:50, FastEthernet0/1
O    172.16.0.192 [110/3] via 20.0.0.1, 02:06:50, FastEthernet0/0
O    172.16.0.192 [110/3] via 30.0.0.1, 02:06:50, FastEthernet0/1
O    172.16.0.208 [110/3] via 20.0.0.1, 02:06:50, FastEthernet0/0
O    172.16.0.208 [110/3] via 30.0.0.1, 02:06:50, FastEthernet0/1
O    172.16.0.224 [110/3] via 20.0.0.1, 02:06:50, FastEthernet0/0
O    172.16.0.224 [110/3] via 30.0.0.1, 02:06:50, FastEthernet0/1
```

Figure 26

OSPF neighbors

```
EDGE(config)#do show ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
20.0.0.1	1	FULL/BDR	00:00:31	20.0.0.1	FastEthernet0/0
30.0.0.1	1	FULL/BDR	00:00:32	30.0.0.1	FastEthernet0/1

```
EDGE(config)#
```

Figure 27*OSPF Database*

```

-----
EDGE#show ip ospf database
      OSPF Router with ID (50.0.0.1) (Process ID 10)

      Router Link States (Area 0)

Link ID      ADV Router    Age      Seq#       Checksum Link count
50.0.0.1     50.0.0.1      458      0x80000015 0x00c695 2
30.0.0.1     30.0.0.1      458      0x80000018 0x00fb6a 3
160.12.1.2   160.12.1.2    458      0x80000012 0x0062ad 3
111.10.0.2   111.10.0.2    457      0x80000011 0x0086b1 2
20.0.0.1     20.0.0.1      456      0x80000019 0x003541 4
172.16.0.225 172.16.0.225  443      0x80000035 0x009992 11
172.16.0.226 172.16.0.226  438      0x80000043 0x006bb2 11

      Net Link States (Area 0)

Link ID      ADV Router    Age      Seq#       Checksum
30.0.0.2     50.0.0.1      1248     0x80000017 0x00066c
20.0.0.2     50.0.0.1      1242     0x80000018 0x006e62
14.0.0.2     172.16.0.225  1248     0x8000003e 0x00fad7
111.10.0.1   172.16.0.225  1247     0x8000003f 0x00ba50
160.10.1.1   172.16.0.226  1244     0x8000005a 0x00c0c3
13.0.0.2     172.16.0.226  1244     0x8000005b 0x00d5e5
12.0.0.2     172.16.0.226  1244     0x8000005c 0x00f86d
11.0.0.2     172.16.0.225  1243     0x80000040 0x00aab1
172.16.0.177 172.16.0.225  453      0x80000041 0x009c06
172.16.0.65  172.16.0.225  453      0x80000042 0x000558
172.16.0.161 172.16.0.225  448      0x80000043 0x00aedf
172.16.0.129 172.16.0.225  448      0x80000044 0x007e9c
172.16.0.225 172.16.0.225  448      0x80000045 0x00b624
172.16.0.193 172.16.0.225  443      0x80000046 0x00f7e0
172.16.0.209 172.16.0.225  443      0x80000047 0x005395

      Type-5 AS External Link States

Link ID      ADV Router    Age      Seq#       Checksum Tag
0.0.0.0      50.0.0.1      1287     0x8000000c 0x003d57 1
EDGE#
-----

```

BGP

In the network setup, Border Gateway Protocol (BGP) has been configured on the edge router to establish connections with two Internet Service Providers (ISPs) that operate in separate autonomous systems (ASes). These ASes are designated as AS 150 and AS 180. The edge router itself is assigned an autonomous system number of 100, which differentiates it from the ISPs. To facilitate communication with the ISPs, specific IP addresses, namely 50.0.0.2 and 40.0.0.2, have been allocated for BGP peering. These IP addresses are used to establish connections with the respective ISPs in AS 150 and AS 180. This BGP configuration serves to create links between the edge router and the ISPs, enabling effective routing and data exchange across distinct autonomous systems.

This setup brings a range of benefits, including enhanced redundancy, load balancing, traffic optimization and scalability to the network. It allows the network to make optimal use of multiple ISP connections, streamline data routing, and ensure reliable connectivity within the broader internet context.

Figure 28*BGP networks*

```

EDGE#show ip bgp
BGP table version is 35, local router ID is 50.0.0.1
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
*> 40.0.0.0/8       0.0.0.0              0      0 32768 i
*                   40.0.0.2              0      0    180 i
*                   50.0.0.2              0      0    150 200 180 i
*> 50.0.0.0/8       0.0.0.0              0      0 32768 i
*                   50.0.0.2              0      0    150 i
*                   40.0.0.2              0      0    180 200 150 i
*> 60.0.0.0/8       40.0.0.2              0      0    180 i
*                   50.0.0.2              0      0    150 200 i
*> 70.0.0.0/8       50.0.0.2              0      0    150 i
*                   40.0.0.2              0      0    180 200 i
* 170.10.0.0/16     50.0.0.2              0      0    150 200 i
*>                   40.0.0.2              0      0    180 200 i

```

Figure 29*BGP neighbors*

```

EDGE#show ip bgp neighbors
BGP neighbor is 50.0.0.2, remote AS 150, external link
BGP version 4, remote router ID 2.2.2.2
BGP state = Established, up for 02:17:45
Last read 02:17:45, last write 02:17:45, hold time is 180, keepalive interval is 60 seconds
Neighbor capabilities:
  Route refresh: advertised and received(new)
  Address family IPv4 Unicast: advertised and received
Message statistics:
  InQ depth is 0
  OutQ depth is 0

      Sent      Rcvd
Opens:          3        3
Notifications:  1        1
Updates:        24       21
Keepalives:     363      363
Route Refresh:   0        6
Total:          391      394
Default minimum time between advertisements runs is 30 seconds

BGP neighbor is 40.0.0.2, remote AS 180, external link
BGP version 4, remote router ID 1.1.1.1
BGP state = Established, up for 02:18:45
Last read 02:18:45, last write 02:18:45, hold time is 180, keepalive interval is 60 seconds
Neighbor capabilities:
  Route refresh: advertised and received(new)
  Address family IPv4 Unicast: advertised and received
Message statistics:
  InQ depth is 0
  OutQ depth is 0

      Sent      Rcvd
Opens:          3        3
Notifications:  1        1
Updates:        23       21
Keepalives:     364      363
Route Refresh:   0        6
Total:          391      394
Default minimum time between advertisements runs is 30 seconds

```


Static Default

The default static route in edge router acts as a "gateway of last resort" for traffic that is not explicitly defined by either OSPF or BGP. When the edge router receives traffic destined for a location outside the OSPF network and the ISP's BGP network, it doesn't have a specific route in its routing tables to guide the traffic. In this case, the default static route comes into play

[\(2019\).](#)

Figure 30

Static route

```

[110/3] via 30.0
S* 0.0.0.0/0 [1/0] via 50.0.0.2
[1/0] via 40.0.0.2
EDGE(config)#
EDGE(config)#

```

Supernetting for Access Control Lists

A networking technique called supernetting, entails joining several smaller, contiguous IP address blocks into a single, bigger address block. This is done to make access control list (ACL) configurations simpler. Supernetting represent a range of IP addresses in your ACL rules using a single condensed address block. As a result, the ACL configuration is made simpler, has fewer entries, and is simpler to manage.

ACL for NAT

The IP addresses assigned to individual departments have been supernetted to the CIDR of /24 and have been permitted the access to any ISP while denying the access to the network of private IP of branch Kansas. The access list used is extended ACLs to enable more precise network traffic filtering source and destination IP addresses, designing intricate filtering rules that are specific to network needs.

Figure 31

ACL configuration on Headquarters EDGE

```
access-list 102 deny ip 172.16.0.0 0.0.0.255 192.168.3.0 0.0.0.255
access-list 102 permit ip 172.16.0.0 0.0.0.255 any
EDGE(config)#
```

ACL for VPN

A separate ACL has been configured for VPN access. VPN sends and encrypted traffic from the headquarters to the branch Kansas. The IP addresses of each department which was denied the access to the private network of branch has been given permit to access the branch's private network through VPN. VPN allows the connection of branch and headquarters through tunneling ([Supernetting Tutorial: - Supernetting Explained With Examples, n.d.](#)).

Figure 32

ACL for VPN on Headquarters EDGE

```
EDGE#sh run | sec access
access-list 101 permit ip 172.16.0.0 0.0.0.255 192.168.3.0 0.0.0.255
```

Network Address Translation (NAT)

IPv4 address conservation is one of the main justifications for adopting NAT. Due to the limited number of IPv4 addresses still available, NAT enables numerous devices connected to a private network to share a single public IP address. Here, Port address translation is used for natting purpose. ACL 102 has been used for nat.

Figure 33

NAT configuration in EDGE

```
interface FastEthernet0/0
ip address 20.0.0.2 255.0.0.0
ip nat inside
duplex auto
speed auto
!
interface FastEthernet0/1
ip address 30.0.0.2 255.0.0.0
ip nat inside
duplex auto
speed auto
!
interface FastEthernet1/0
ip address 50.0.0.1 255.0.0.0
ip nat outside
duplex auto
speed auto
!
interface FastEthernet1/1
ip address 40.0.0.1 255.0.0.0
ip nat outside
duplex auto
speed auto
```

ip nat inside source list 102 interface FastEthernet1/0 overload

Virtual Private Network (VPN)

Remote network connections can be made privately and securely using virtual private networks (VPNs). Each department in the headquarters can privately access resources as if they were on-site of branch and vice versa, and encrypt data traffic to ensure secrecy. By hiding IP addresses and avoiding geo-restrictions, VPNs preserve the users' privacy while boosting the security of public Wi-Fi networks. They are utilized for site-to-site connectivity and secure remote work all of which guarantee encrypted data transmission and reduce potential hazards. VPNs are flexible technologies that support online anonymity, safeguard private data, and enable secure communication over many networks and places.

Figure 34

VPN in headquarter

```
EDGE(config)#do sh run | sec crypto
crypto isakmp policy 10
  encr 3des
  hash md5
  authentication pre-share
  group 5
crypto isakmp key AARYA address 170.10.0.2
crypto ipsec transform-set DAHAL esp-3des esp-md5-hmac
crypto map CISCO 20 ipsec-isakmp
  set peer 170.10.0.2
  set transform-set DAHAL
  match address 101
EDGE(config)#
```

A specific ISAKMP policy (policy 10) is defined, specifying encryption (3DES), hash algorithm (MD5), authentication method (pre-shared key), and a group (Group 5) for key exchange. A pre-shared key "AARYA" is associated with the remote device at IP address 170.10.0.2 of branch's EGDE router. An IPsec transform-set named "DAHAL" is created, defining encryption (3DES) and integrity (MD5) algorithms for data protection. A crypto map named "CISCO" is configured with entry 20, which specifies the remote peer (IP address 170.10.0.2), the transform-set "DAHAL" for securing data, and an access control list (ACL)

defined as access list 101 for traffic matching. Similarly, VPN is also configured in Kansas branch that is shown below.

Figure 35

VPN for Kansas

```
Kansas-EDGE(config)#do sh run | sec crypto
crypto isakmp policy 10
  encr 3des
  hash md5
  authentication pre-share
  group 5
crypto isakmp key AARYA address 40.0.0.1
crypto isakmp key AARYA address 50.0.0.1
crypto ipsec transform-set DAHAL esp-3des esp-md5-hmac
crypto map CISCO 20 ipsec-isakmp
  set peer 50.0.0.1
  set peer 40.0.0.1
  set transform-set DAHAL
  match address 101
crypto map CISCO
Kansas-EDGE(config)#
```

Two pre-shared keys "AARYA" are associated with the headquarters at IP addresses 40.0.0.1 and 50.0.0.1 and remote peers have been configured to the same IP addresses i.e., IP addresses 40.0.0.1 and 50.0.0.1.

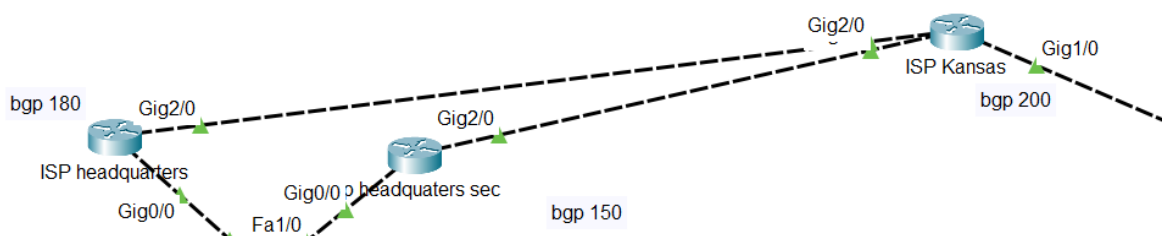
This way VPN is configured in both Headquarters and Kansas branch providing a secure encrypted traffic flow between them. ([What Is a Virtual Private Network \(VPN\)?, n.d.](#))

ISP

Two ISPs for headquarters have been used to provide redundancy for the network in-case of network failures through one ISP. The ISPs of headquarters have been connected to the edge router and BGP protocol is used to connect all three of them. Static default has also been configured in the EDGE to provide a default gateway for routes. ACL configuration has allowed only wanted traffic to access the ISP and NAT is also done for the departments to access the single public IP address used in each ISP.

Figure 36

ISPs



Assigned Networks in ISPs

Figure 37

IP addresses assigned in ISPs

```

ISP-Primary(config)#do sh ip int brief | ex una
Interface          IP-Address      OK? Method Status  Protocol
GigabitEthernet0/0  40.0.0.2        YES manual up      up
GigabitEthernet2/0  60.0.0.1        YES manual up      up
Loopback0          1.1.1.1         YES manual up      up
ISP-Primary(config)#

ISP-Secondary(config)#do sh ip int brief | ex una
Interface          IP-Address      OK? Method Status  Protocol
GigabitEthernet0/0  50.0.0.2        YES manual up      up
GigabitEthernet2/0  70.0.0.1        YES manual up      up
Loopback0          2.2.2.2         YES manual up      up
ISP-Secondary(config)#
  
```

IP addresses 40.0.0.2 and 50.0.0.2 are connected to edge while the network 60.0.0.1 and 70.0.0.1 are connected to the ISP of Kansas. Furthermore, a loopback address of 1.1.1.1 and 2.2.2.2 has also been added to stimulate the internet access to each department.

Figure 38*ISP of Kansas branch*

```
ISP-Kansas(config)#do sh ip int brief | ex una
Interface                IP-Address      OK? Method Status  Protocol
GigabitEthernet0/0       70.0.0.2        YES manual up      up
GigabitEthernet1/0       170.10.0.1      YES manual up      up
GigabitEthernet2/0       60.0.0.2        YES manual up      up
ISP-Kansas(config)#
```

The IP addresses 60 and 70 connects the two ISP of headquarters while 170.10.0.1 is the public IP for Kansas branch.

BGP**Figure 39***BGP in Headquarters ISPs*

```
ISP-Primary(config)#do sh ip bgp
BGP table version is 36, local router ID is 1.1.1.1
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
*> 40.0.0.0/8	0.0.0.0	0	0	32768	i
*	40.0.0.1	0	0	0	100 i
*	40.0.0.1	0	0	0	100 i
*	60.0.0.2	0	0	0	200 150 100 i
*> 50.0.0.0/8	40.0.0.1	0	0	0	100 i
*	60.0.0.2	0	0	0	200 150 i
*> 60.0.0.0/8	0.0.0.0	0	0	32768	i
*	40.0.0.1	0	0	0	100 150 200 i
*	60.0.0.2	0	0	0	200 i
*> 70.0.0.0/8	60.0.0.2	0	0	0	200 i
*	40.0.0.1	0	0	0	100 150 i
*> 170.10.0.0/16	60.0.0.2	0	0	0	200 i
*	40.0.0.1	0	0	0	100 150 200 i

```
ISP-Secondary#sh ip bgp
BGP table version is 34, local router ID is 2.2.2.2
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
* 40.0.0.0/8	70.0.0.2	0	0	0	200 180 i
*> 50.0.0.0/8	50.0.0.1	0	0	0	100 i
*> 50.0.0.0/8	0.0.0.0	0	0	32768	i
*	70.0.0.2	0	0	0	200 180 100 i
*	50.0.0.1	0	0	0	100 i
*> 60.0.0.0/8	70.0.0.2	0	0	0	200 i
*	50.0.0.1	0	0	0	100 180 i
*> 70.0.0.0/8	0.0.0.0	0	0	32768	i
*	70.0.0.2	0	0	0	200 i
*	50.0.0.1	0	0	0	100 180 200 i
*> 170.10.0.0/16	70.0.0.2	0	0	0	200 i
*	50.0.0.1	0	0	0	100 180 200 i

Figure 40*BGP neighbors of headquarters ISP-primary*

```
ISP-Primary(config)#do sh ip bgp ne
BGP neighbor is 40.0.0.1, remote AS 100, external link
  BGP version 4, remote router ID 50.0.0.1
  BGP state = Established, up for 01:27:40
  Last read 01:27:40, last write 01:27:40, hold time is 180, keepalive interval is 60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received(new)
    Address family IPv4 Unicast: advertised and received
  Message statistics:
    InQ depth is 0
    OutQ depth is 0

BGP neighbor is 60.0.0.2, remote AS 200, external link
  BGP version 4, remote router ID 170.10.0.1
  BGP state = Established, up for 00:25:40
  Last read 00:25:40, last write 00:25:40, hold time is 180, keepalive interval is 60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received(new)
    Address family IPv4 Unicast: advertised and received
  Message statistics:
    InQ depth is 0
    OutQ depth is 0
```

Figure 41*BGP neighbors of headquarters ISP-Secondary*

```
ISP-Secondary#sh ip bgp ne
BGP neighbor is 50.0.0.1, remote AS 100, external link
  BGP version 4, remote router ID 50.0.0.1
  BGP state = Established, up for 00:27:18
  Last read 00:27:18, last write 00:27:18, hold time is 180, keepalive interval is 60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received(new)
    Address family IPv4 Unicast: advertised and received
  Message statistics:
    InQ depth is 0
    OutQ depth is 0

BGP neighbor is 70.0.0.2, remote AS 200, external link
  BGP version 4, remote router ID 170.10.0.1
  BGP state = Established, up for 00:27:18
  Last read 00:27:18, last write 00:27:18, hold time is 180, keepalive interval is 60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received(new)
    Address family IPv4 Unicast: advertised and received
  Message statistics:
    InQ depth is 0
    OutQ depth is 0
```

Figure 42*BGP neighbors of Kansas Branch*

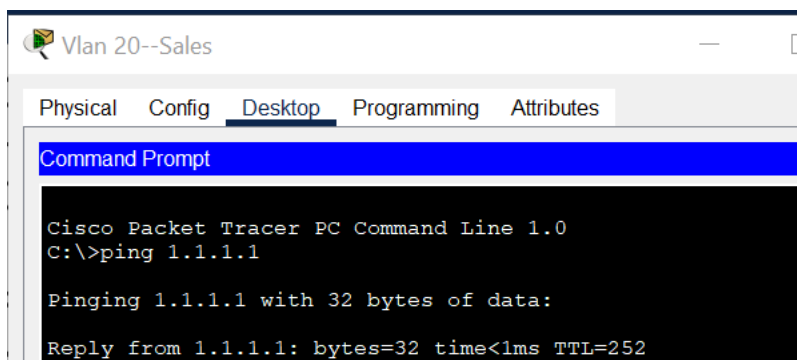
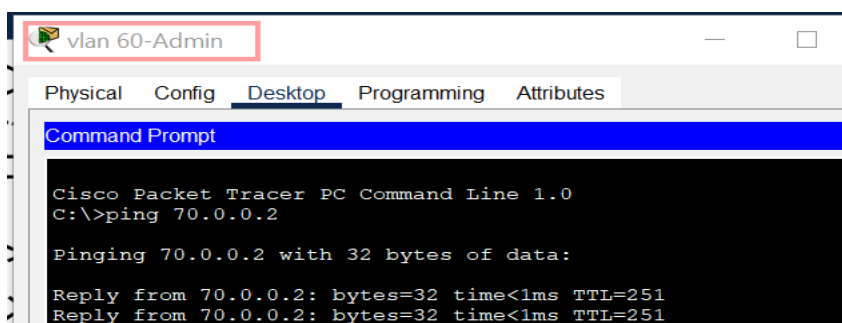
```

Local host: 70.0.0.2, Local port: 179
Foreign host: 70.0.0.1, Foreign port: 1029
Connection tableid (VRF): 0

BGP neighbor is 60.0.0.1, remote AS 180, external link
  BGP version 4, remote router ID 1.1.1.1
  BGP state = Established, up for 00:32:38
  Last read 00:32:38, last write 00:32:38, hold time is 180, keepalive interval is 60
seconds
  Neighbor capabilities:
    Route refresh: advertised and received(new)
    Address family IPv4 Unicast: advertised and received

BGP neighbor is 170.10.0.2, remote AS 250, external link
  BGP version 4, remote router ID 192.168.1.1
  BGP state = Established, up for 01:34:38
  Last read 01:34:38, last write 01:34:38, hold time is 180, keepalive interval is 60
seconds

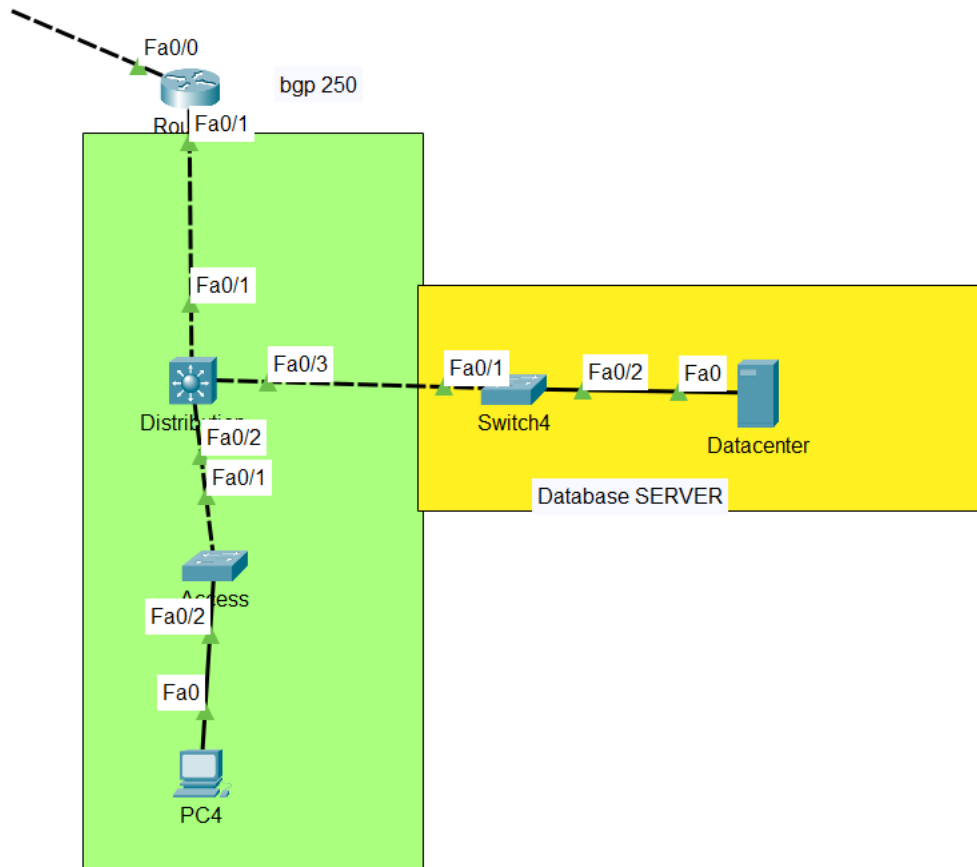
```

Figure 43*ICMP Echo Request to ISP of headquarters***Figure 44***ICMP Echo Request to ISP of Kansas*

Kansas Branch

Figure 45

Kansas Branch



A separate Kansas branch apart from headquarters has also been added to the network design where an EDGE, collapsed core and distribution and access layer has been configured. Furthermore, a datacenter has also been added according to the network design requirement. A layer 2 switch is configured for access layer where access links and trunk links has been established to carry vlan information to the edge router. In the distribution layer, a layer 2 switch has been added to server as an access layer of the data center as well. ACL as NAT well as VPN have been configured in the branch to provide a secure network traffic flow.

Assigned Networks in Kansas branch

```
kansas-distribution#sh ip int brief | ex una
Interface          IP-Address      OK? Method Status      Protocol
FastEthernet0/1    192.168.1.2     YES manual up          up
FastEthernet0/2    192.168.3.1     YES manual up          up
FastEthernet0/3    192.168.2.1     YES manual up          up
kansas-distribution#

KANSAS CONFIGURATION COMMANDS, ONE PER LINE, END WITH ENTER.
Kansas-EDGE(config)#do sh ip int brief | ex una
Interface          IP-Address      OK? Method Status      Protocol
FastEthernet0/0    170.10.0.2      YES manual up          up
FastEthernet0/1    192.168.1.1     YES manual up          up
Kansas-EDGE(config)#
```

Network assigned in the distribution of Kansas branch are 192.168.1.0/24 towards egde router, 192.168.2.0/24 towards data center and 192.168.3.0/24 towards access layer.

Network assigned in the EGDE router of Kansas branch are 170.10.0.2/16 towards ISP while 192.168.1.0/24 towards distribution/core switch.

Routing Protocol

OSPF

OSPF 20 area 0 has been configured in the distribution layer and private interface EGDE of the branch where the following network have been routed.

Figure 46

OSPF configuration and routes

```
kansas-distribution#sh run | sec ospf
router ospf 20
 log-adjacency-changes
 network 192.168.1.0 0.0.0.255 area 0
 network 192.168.2.0 0.0.0.255 area 0
 network 192.168.3.0 0.0.0.255 area 0

kansas-distribution#sh ip route ospf
O*E2 0.0.0.0/0 [110/1] via 192.168.1.1, 03:31:03, FastEthernet0/1
.
.
.

Kansas-EDGE(config)#do sh ip route ospf
O 192.168.2.0 [110/2] via 192.168.1.2, 03:32:27, FastEthernet0/1
O 192.168.3.0 [110/2] via 192.168.1.2, 03:32:27, FastEthernet0/1
```

Static Default

```
ip route 0.0.0.0 0.0.0.0 170.10.0.1
!
```

Static default has been configured in EDGE route to allow the flow to private network to the public ISP since it acts as a default gateway between them.

BGP

BGP has also been configured in the EDGE router towards public interface since it provides traffic optimization and scalability also allowing the network to make optimal use of multiple ISP connections and ensuring reliable connectivity with the network.

Figure 47

BGP networks and Neighbors

```
Kansas-EDGE(config)#do sh ip bgp
BGP table version is 29, local router ID is 192.168.1.1
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
*> 40.0.0.0/8             170.10.0.1              0      0      0 200 180 i
*> 50.0.0.0/8             170.10.0.1              0      0      0 200 150 i
*> 60.0.0.0/8             170.10.0.1              0      0      0 200 i
*> 70.0.0.0/8             170.10.0.1              0      0      0 200 i
*> 170.10.0.0/16          0.0.0.0                 0      0 32768 i
*                          170.10.0.1              0      0      0 200 i
```

```
Kansas-EDGE(config)#do sh ip bgp ne
BGP neighbor is 170.10.0.1, remote AS 200, external link
  BGP version 4, remote router ID 170.10.0.1
  BGP state = Established, up for 00:08:06
  Last read 00:08:06, last write 00:08:06, hold time is 180, keepalive
interval is 60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received(new)
    Address family IPv4 Unicast: advertised and received
  Message statistics:
    InQ depth is 0
    OutQ depth is 0
```

BGP is also configured in the ISP of Kansas branch where the network assigned is 170.10.0.0/16 with the remote AS 200. Routes of all ISP is distributed in BGP routing protocol.

ACL for Kansas Branch

Figure 48

ACL for Kansas

```

Kansas-EDGE(config)#do sh run | sec access
access-list 101 permit ip 192.168.3.0 0.0.0.255 172.16.0.0 0.0.0.255
access-list 110 deny ip 192.168.3.0 0.0.0.255 172.16.0.0 0.0.0.255
access-list 110 permit ip 192.168.3.0 0.0.0.255 any

```

In the Kansas branch, Extended Access control policies has been made which permits and denies the access to other network as per need. The access list 110 is configured for NAT while ACL 101 is specifically configured for VPN. In access list 110, the private network has permit access to any other network except for private network of headquarter. Meanwhile, ACL for VPN has been made in such a way that only private network of Kansas branch i.e., 192.168.3.0/24 has access to private network of headquarter for each VLAN i.e., 172.16.0.0/24. Supernetting for ACL has also been done in Kansas branch for easier configuration.

PAT for Kansas Branch

Figure 49

PAT for Kansas ([What Is the Role of NAT and PAT in Making Internet Routing More Efficient](#))

```

Kansas-EDGE#sh run | sec nat
ip nat outside
ip nat inside
default-information originate
ip nat inside source list 110 interface FastEthernet0/0 overload

```

The private interface of EDGE is set as 'ip nat inside' while the public interface is set as 'ip nat outside'. "default-information originate," is also done since it advertises a default route (0.0.0.0/0) into the routing domain and PAT is done using the access list 110 where policies of permit and deny has been set for the private network of the branch. This allows many private network to use a single public network.

VPN

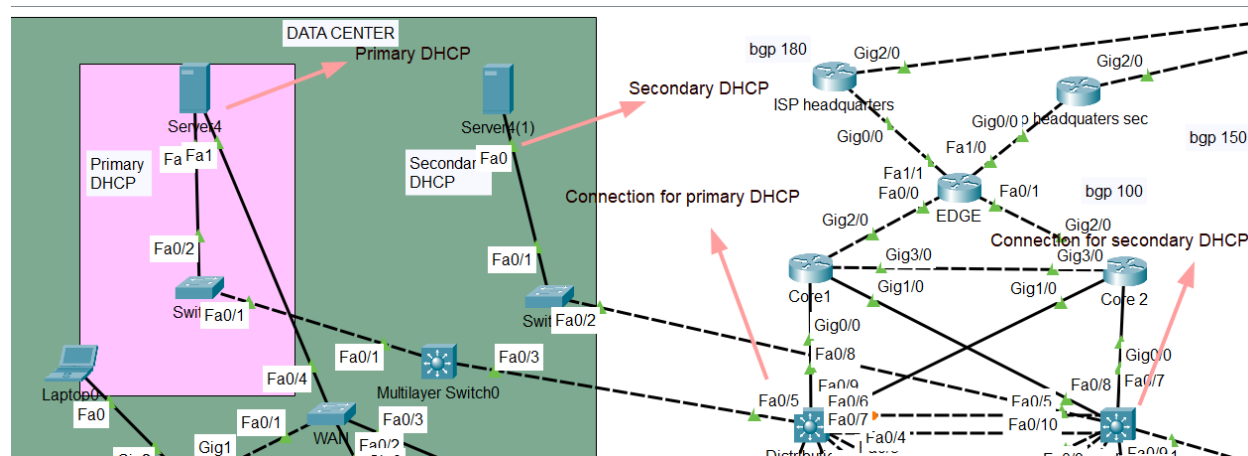
Configurations for [VPN](#) has been shown above.

Services Configuration

DHCP

Figure 50

DHCP Servers



A network mechanism called Dynamic Host Configuration mechanism (DHCP) is used to randomly allocate IP addresses within a network. By automatically assigning and handling IP addresses as devices link to the network, it streamlines the IP address management process.

In this network there are 8 separate departments getting IP addresses through DHCP, of the network 172.16.0.0/24 where VLSM has also been done to reduce the wastage of IPv4 address. Two DHCP servers have been configured for redundancy and scalability which is each joined to primary distribution and secondary distribution switches. OSPF routing protocol has been enabled between the server and multilayer switch so that the IP address for VLAN can route towards the access layer. DHCP ensures that each department's PC receive a unique IP address from the available address pool. Meanwhile, PC requests for IP address through DORA process. Additionally, the use of virtual IP addresses for each department has been set which is also the default get way for them so that PCs always has an access point in case of link failures ([What Is DHCP \(Dynamic Host Configuration Protocol\)?, 2023](#)).

Figure 51*DHCP configurations*

Interface: FastEthernet0 Service: ☒ On ☐ Off

Pool Name: marketing

Default Gateway: 172.16.0.62

DNS Server: 0.0.0.0

Start IP Address: 172.16.0.16

Subnet Mask: 255.255.255.192

Maximum Number of Users: 35

TFTP Server: 0.0.0.0

WLC Address: 0.0.0.0

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
serverPool	100.0.0.1	0.0.0.0	100.0.0.100	255.0.0.0	512	0.0.0.0	100.0.0.5
IT	172.16.0.238	0.0.0.0	172.16.0.227	255.255.255.240	7	0.0.0.0	0.0.0.0
HR	172.16.0.222	0.0.0.0	172.16.0.211	255.255.255.240	7	0.0.0.0	0.0.0.0
admin	172.16.0.206	0.0.0.0	172.16.0.195	255.255.255.240	8	0.0.0.0	0.0.0.0
system admin	172.16.0.190	0.0.0.0	172.16.0.179	255.255.255.240	8	0.0.0.0	0.0.0.0
management	172.16.0.174	0.0.0.0	172.16.0.163	255.255.255.240	10	0.0.0.0	0.0.0.0
front support	172.16.0.158	0.0.0.0	172.16.0.131	255.255.255.224	20	0.0.0.0	0.0.0.0
sales	172.16.0.126	0.0.0.0	172.16.0.67	255.255.255.192	30	0.0.0.0	0.0.0.0
marketing	172.16.0.62	0.0.0.0	172.16.0.3	255.255.255.192	35	0.0.0.0	0.0.0.0

```

interface Vlan10
mac-address 0006.2ae4.1101
ip address 172.16.0.2 255.255.255.192
ip helper-address 15.0.0.1
ip helper-address 16.0.0.1
standby 10 ip 172.16.0.62
standby 10 preempt
!
interface Vlan20
mac-address 0006.2ae4.1102
ip address 172.16.0.66 255.255.255.192
ip helper-address 15.0.0.1
ip helper-address 16.0.0.1
standby 10 ip 172.16.0.126
standby 10 preempt
!
interface Vlan30
mac-address 0006.2ae4.1103
ip address 172.16.0.130 255.255.255.224
ip helper-address 15.0.0.1
ip helper-address 16.0.0.1
standby 10 ip 172.16.0.158
standby 10 preempt
.

```

In the distribution layer, IP helper address of the primary and secondary DHCP server has been configured respectively inside each SVI interface. When a department initiates the DHCP DORA process and sends out a DHCP Discover message as a broadcast, the IP helper address is responsible for relaying this broadcast request to the DHCP servers, according to their placement during configuration.

Figure 52*DHCP for WLC*

SERVICES

- HTTP
- DHCP**
- DHCPv6
- TFTP
- DNS
- SYSLOG
- AAA
- NTP
- EMAIL
- FTP
- IoT
- VM Management
- Radius EAP

DHCP

Interface: **FastEthernet1** Service: ☒ On ☐ Off

Pool Name: serverPool

Default Gateway: 100.0.0.1

DNS Server: 0.0.0.0

Start IP Address: 100.0.0.100

Subnet Mask: 255.0.0.0

Maximum Number of Users: 512

TFTP Server: 0.0.0.0

WLC Address: 100.0.0.5

Buttons: Add, Save, Remove

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
serverPool	100.0.0.1	0.0.0.0	100.0.0.100	255.0.0.0	512	0.0.0.0	100.0.0.5

Additionally, DHCP server is also providing IP addresses to accesspoints and laptops for WLC configuration which is requested through DORA process.

Figure 53*IP address through DHCP in departments*

Vlan 10--Marketing

Physical Config **Desktop** Programming Attributes

IP Configuration

Interface: FastEthernet0

IP Configuration: ☒ DHCP ☐ Static

IPv4 Address: 172.16.0.3

Subnet Mask: 255.255.255.192

Default Gateway: 172.16.0.62

DNS Server: 0.0.0.0

IPv6 Configuration

Light Weight Access Point0

Physical **Config** Attributes

GLOBAL

Settings

WLC

INTERFACE

GigabitEthernet0

Dot11Radio0

GigabitEthernet0

Port Status: ☒ On

Bandwidth: ☐ 1000 Mbps ☒ 100 Mbps ☐ 10 Mbps

Duplex: ☐ Half Duplex ☒ Full Duplex

MAC Address: 0060.705E.3101

IP Configuration

☒ DHCP ☐ Static

IPv4 Address: 100.0.0.105

Subnet Mask: 255.0.0.0

URL: <https://100.0.0.5/frameWireless.html>

MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

All APs

Current Filter: [Change Filter] [Clear Filter]

Number of APs: 2

AP Name	IP Address(Ipv4/Ipv6)	AP Model	AP MAC	AP Up Time	Admin Status	Op St
Light_Weight_Access_Point0	100.0.0.105	AIR-CAP3702I-A-K9	00:60:70:5E:31:01	0 d, 8 h 19 m 15 s	Enabled	RE
Light_Weight_Access_Point1	100.0.0.104	AIR-CAP3702I-A-K9	00:E0:8F:24:32:01	0 d, 8 h 19 m 14 s	Enabled	RE

WLAN ID Type Profile Name WLAN SSID Admin Status Security Policies

2 WLAN NetworkHats wireless Enabled [WPA2][Auth(PSK)] Remove

Two APs has been added here

Initially, the browser in the laptop has been opened and an authentication for WLC has been set. Then, the two Aps of IP addresses 100.0.0.104 and 100.0.0.105 were added and profile name has been set to NetworkHats. The wireless network SSID is set to 'wireless' and password has been configured. After the APs has been successfully added, they provided a wireless internet access which was connected to two different laptops.

Figure 56

Wireless connection in laptop

Laptop1

Physical Config Desktop Programming Attributes

GLOBAL Settings Algorithm Settings INTERFACE Wireless0 Bluetooth

Wireless0

Port Status: ☒ On

Bandwidth: 300 Mbps

MAC Address: 0006.2AB2.B698

SSID: wireless

Authentication:

- ☐ Disabled
- ☐ WPA-PSK
- ☐ WPA
- ☐ 802.1X
- ☐ WEP
- ☒ WPA2-PSK
- ☐ WPA2

Method:

WEK Key: []

PSK Pass Phrase: wireless

User ID: []

Password: []

Encryption Type: MD5

User Name: []

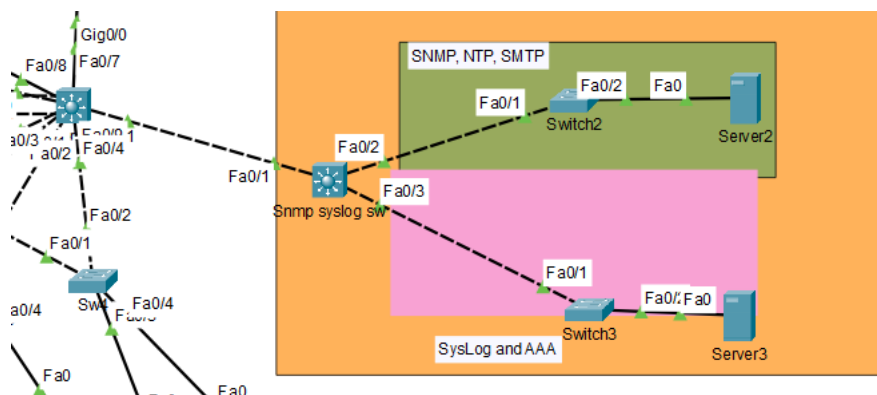
Password: []

IP Configuration:

- ☒ DHCP
- ☐ Static

IPv4 Address: 100.0.0.103

Subnet Mask: 255.0.0.0

Figure 57*Server configurations***AAA**

A system for network security called AAA (Authentication, Authorization, and Accounting) controls user access and activity. Configuring AAA entails creating rules to authenticate user identities (Authentication), decide what actions are allowed (Authorization), and record interactions for auditing (Accounting). Authorization determines what users can do, while Accounting records user actions. Authentication verifies user credentials, such as passwords ([What Is AAA?, n.d.](#)).

Figure 58*AAA configuration*

The screenshot shows the 'Services' tab in a network management system. The 'AAA' service is selected in the left sidebar. The main configuration area is titled 'AAA' and includes the following sections:

- Service:** A radio button is selected for 'On'. The 'Radius Port' is set to 1645.
- Network Configuration:**
 - Client Name: (empty)
 - Client IP: (empty)
 - Secret: (empty)
 - Server Type: Radius
- Table:** A table with columns: Client Name, Client IP, Server Type, and Key. It contains one entry:

Client Name	Client IP	Server Type	Key
1 core1	13.0.0.1	Radius	cisco
- User Setup:**
 - Username: (empty)
 - Password: (empty)
- Table:** A table with columns: Username and Password. It contains one entry:

Username	Password
1 kali	kali

```

core1(config)#do sh run | sec aaa
aaa new-model
aaa authentication login default group radius
aaa authentication enable default group radius
aaa authorization exec default group radius

```

Here, AAA has been configured in core1 router. SSH is authenticated and authorized by this.

SSH

A secure network protocol called SSH (Secure Shell) allows for encrypted communication and remote device access. It guarantees user authentication, data confidentiality, and security from tampering. SSH is frequently used for file transfers, secure remote management, and running commands on distant devices. It offers a secure means of interconnecting and managing systems over dubious networks.

Figure 59

SSH configuration and login

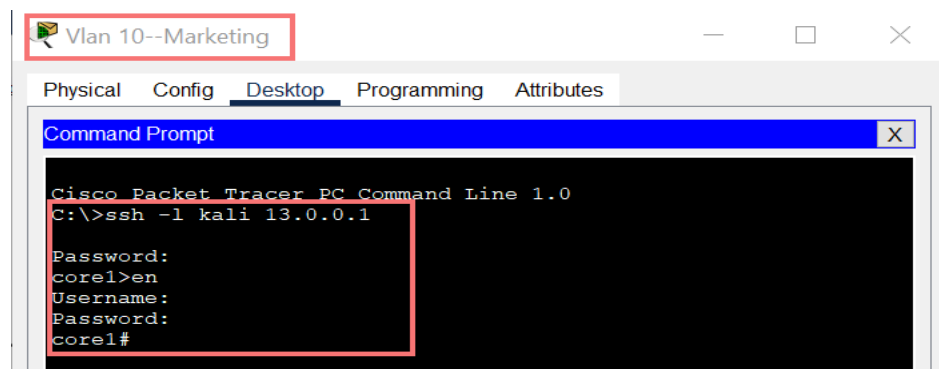
```

core1(config)#do sh run | sec line vty
line vty 0 4
transport input ssh
core1(config)#do sh run | sec domain
ip domain-name cisco.com

core1(config)#crypto key gen rsa
% You already have RSA keys defined named core1.cisco.com .
% Do you really want to replace them? [yes/no]: yes
The name for the keys will be: core1.cisco.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]

core1(config)#
*Aug 11 1:34:33.269: %SSH-5-ENABLED: SSH 1.99 has been enabled

```

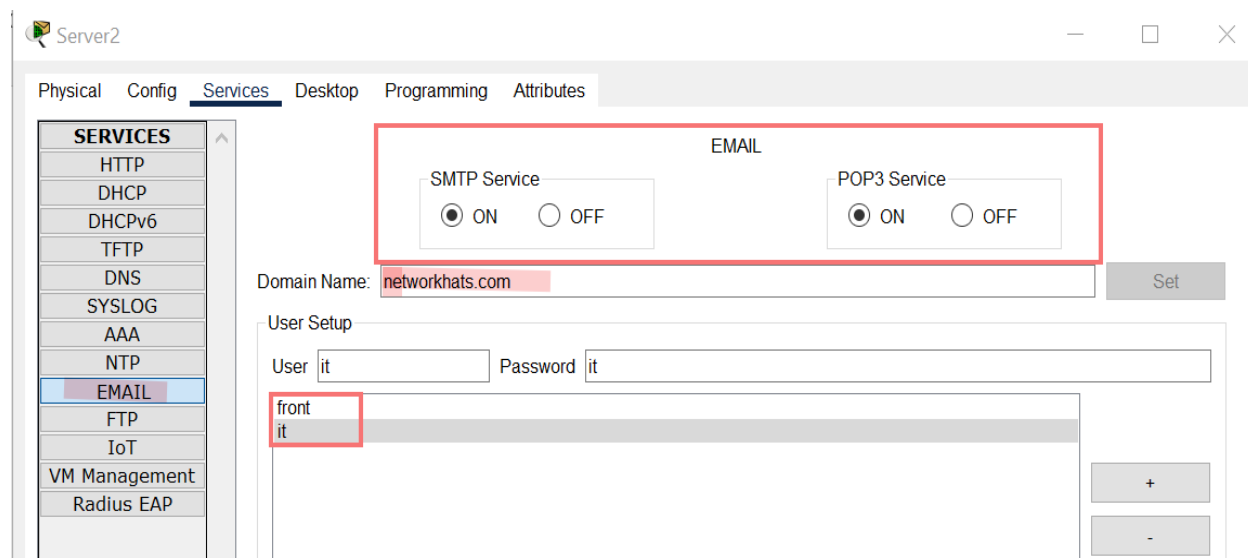


SMTP and POP3

It is possible to transmit and route outgoing email messages from departments to servers or between branches using the SMTP (Simple Mail Transfer Protocol) protocol. Post Office Protocol version 3 (POP3) is in charge of transferring incoming email messages from a server to departments, allowing for the downloading of messages for offline access. While POP3 concentrates on message retrieval and offline storage, SMTP prioritizes email transmission efficiency which make up the core of email communication ([Hosting, n.d.](#)).

Figure 60

SMTP configuration in server



Here the domain name has been set to networkhats.com and two user front and it has been created.

Figure 61*SMTP configuration in clients*

Vlan 30--FrontSupport

Physical Config **Desktop** Programming Attributes

Configure Mail

User Information

Your Name: front

Email Address: front@networkhats.com

Server Information

Incoming Mail Server: 160.12.1.1 *← IP address of the server*

Outgoing Mail Server: 160.12.1.1

Logon Information

User Name: front *← User name and password configured in the server*

Password: ••••

vlan 80-IT

Physical Config **Desktop** Programming Attributes

Configure Mail

User Information

Your Name: it

Email Address: it@networkhats.com

Server Information

Incoming Mail Server: 160.12.1.1

Outgoing Mail Server: 160.12.1.1

Logon Information

User Name: it

Password: ••

Save Remove

The mail address must be configured in such a way that the domain name must match and the mail server must have the IP address of the server and user name and password must match.

Figure 62*Email from front support and reply*

MAIL BROWSER

Mails

Compose Reply Receive Delete Configure Mail

	From	Subject	Received
1	front@networkhats.com	Hello	Fri Aug 11 2023 02:02:54

Hello
 front@networkhats.com
 Sent : Fri Aug 11 2023 02:02:54
 Hello this is front support

Sending mail to front@networkhats.com , with subject : RE: Hello .. Mail Server: 160.12.1.1
 Send Success.

Figure 63*Reply from IT*

Vlan 30--FrontSupport

Physical Config **Desktop** Programming Attributes

MAIL BROWSER

Mails

Compose Reply Receive Delete Configure Mail

	From	Subject	Received
1	it@networkhats.com	RE: Hello	Fri Aug 11 2023 02:07:32
2	it@networkhats.com	test	Mon Aug 7 2023 15:37:33

RE: Hello
it@networkhats.com
Sent : Fri Aug 11 2023 02:07:32

Hello this is IT

Subject : Hello
From : front@networkhats.com
Sent : Fri Aug 11 2023 02:02:54

Hello this is front support

Receiving mail from POP3 Server 160.12.1.1
Receive Mail Success.

SNMP

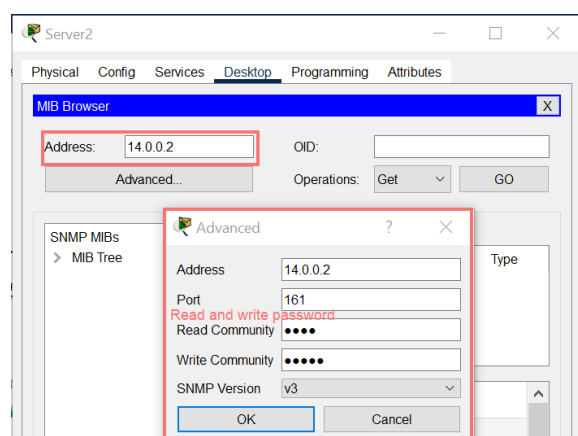
The Simple Network Management Protocol (SNMP) is a vital tool for managing and keeping track of network systems and devices. It enables network administrators to get useful data regarding the functionality of devices, traffic patterns, and resource usage. Furthermore, SNMP offers a uniform framework for remote setup and management of network devices, to change settings, upgrade firmware, and carry out activities remotely.

SNMP has been configured in the server and core1 router as well as primary distribution switch which provides all the network information about them in the server.

Figure 64

SNMP Configuration in distribution

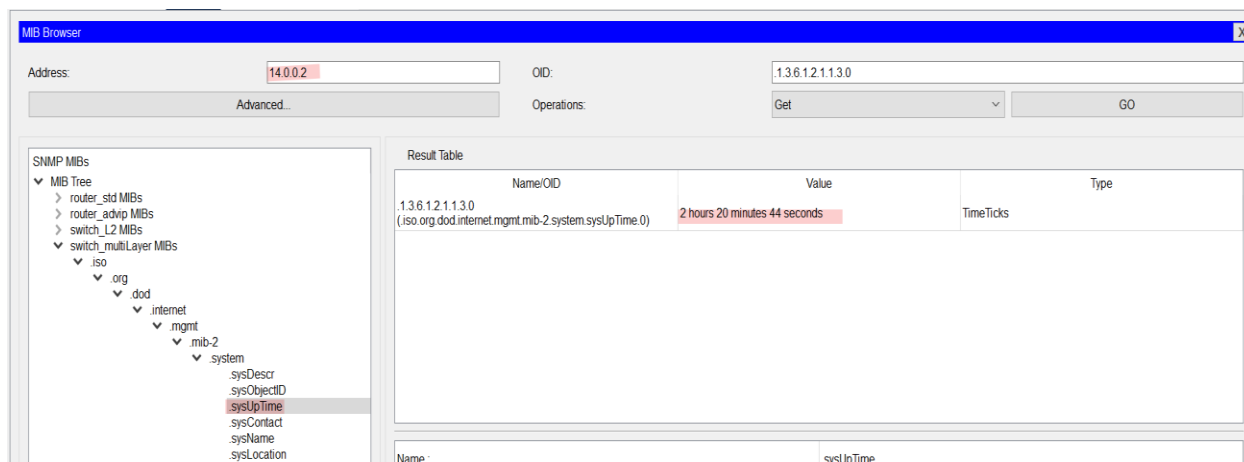
```
PrimaryDistribution(config)#do sh run | sec snmp
snmp-server community read RO
snmp-server community write RW
PrimaryDistribution(config)#do sh ip int brief | ex una
Interface      IP-Address      OK? Method Status
Protocol
FastEthernet0/5    111.10.0.1      YES manual up
FastEthernet0/8    11.0.0.2        YES manual up
FastEthernet0/9    14.0.0.2        YES manual up
Vlan10           172.16.0.1      YES manual up
Vlan20           172.16.0.65     YES manual up
Vlan30           172.16.0.129    YES manual up
Vlan40           172.16.0.161    YES manual up
Vlan50           172.16.0.177    YES manual up
Vlan60           172.16.0.193    YES manual up
Vlan70           172.16.0.209    YES manual up
Vlan80           172.16.0.225    YES manual up
PrimaryDistribution(config)#
```



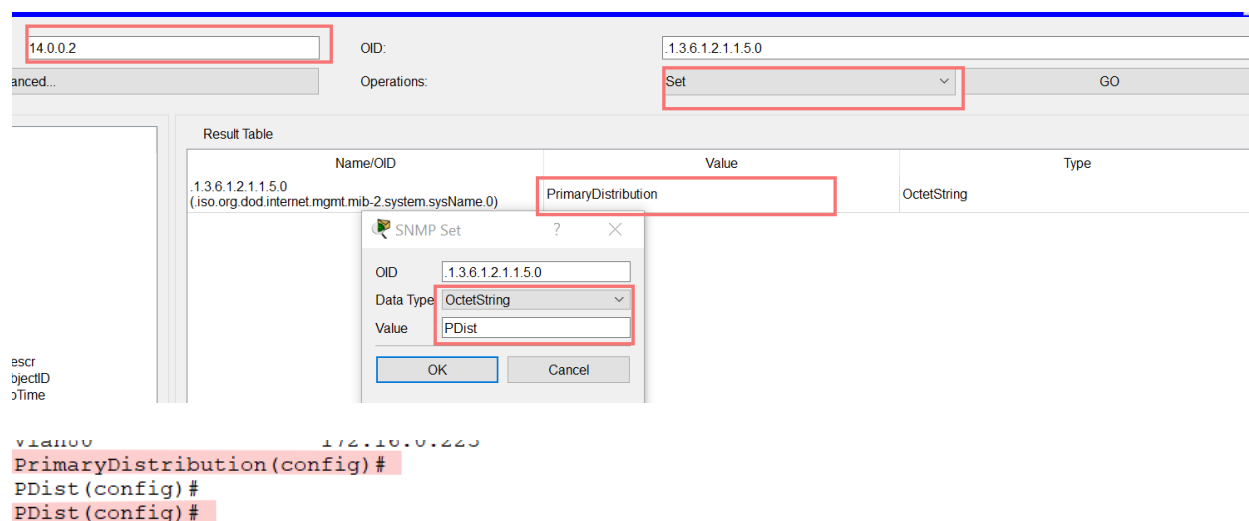
Inside the MIB browser of the server, the IP address of switch is logged in and ‘read’ and ‘write’ password is inserted which then shows all the configurations in the switch.

Figure 65

Showing running time of the Switch

**Figure 66**

Changing the name of switch



Here, the name of PrimaryDistribution is changed to PDist through snmp set operation.

This shows the remote setup and management function of SNMP for network devices ([Simple Network Management Protocol \(SNMP\) - GeeksforGeeks, 2018](#)).

NTP

Network devices can synchronize their clocks with a very precise time source using the commonly used Network Time Protocol (NTP) protocol. NTP makes ensuring that devices on a network keep accurate and consistent time, which is necessary for a number of tasks like data synchronization, authentication, and logging.

Figure 67

NTP configuration

```
SNMP_SYSLOG#sh clock
21:41:50.463 EST Thu Aug 10 2023
SNMP_SYSLOG#sh run | sec ntp
ntp server 160.12.1.1
ntp update-calendar
SNMP_SYSLOG#
```

The screenshot displays the NTP configuration page in a network device's configuration utility. The left sidebar lists various services, with NTP selected. The main panel shows the NTP service is turned on. Below this, there are fields for authentication, including a key and password, both set to '0'. A calendar for August 2023 is shown, with the 10th highlighted. The current time is displayed as 09:41:37PM.

Services List:

- HTTP
- DHCP
- DHCPv6
- TFTP
- DNS
- SYSLOG
- AAA
- NTP**
- EMAIL
- FTP
- IoT
- VM Management
- Radius EAP

NTP Configuration:

- Service: ☒ On ☐ Off
- Authentication: ☒ Enable ☐ Disable
- Key: 0 Password: 0

Calendar: August 2023

Sun	Mon	Tue	Wed	Thu	Fri	Sat
30	31	1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31	1	2

Current Time: 09:41:37PM

Syslog

Syslog is a widely used protocol for gathering and transmitting log messages generated by different network hardware, software, and systems. By enabling these messages to be routed to a centralized syslog server, where they may be kept, processed, and reviewed, it plays a significant part in centralized logging and monitoring. Syslog messages help with fixing issues, performance monitoring, and security analysis by offering details into the operational status, events, failures, and actions of network devices and applications ([What Is Syslog? / Sumo Logic](#), *n.d.*).

Syslog is set in a server with IP address 160.11.1.1 which is logged in the secondary distribution switch. The IP of switch 160.10.1.1 whose logs are displayed in the syslog server.

Figure 68

Syslog Configuration and logs

The figure illustrates the Syslog configuration and logs. It is divided into two main sections: a terminal window showing configuration commands and a Syslog service interface showing a list of log messages.

Terminal Window Configuration:

```

DistributionStandby(config)#do sh run | sec logging
logging 160.11.1.1
DistributionStandby(config)#do sh ip int brief | ex una

```

Interface IP Address Table:

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/7	12.0.0.2	YES	manual	up	up
FastEthernet0/8	13.0.0.2	YES	manual	up	up
FastEthernet0/9	160.10.1.1	YES	manual	up	up
FastEthernet0/10	16.0.0.2	YES	manual	up	up
Vlan10	172.16.0.2	YES	manual	up	up
Vlan20	172.16.0.66	YES	manual	up	up
Vlan30	172.16.0.130	YES	manual	up	up
Vlan40	172.16.0.162	YES	manual	up	up
Vlan50	172.16.0.178	YES	manual	up	up
Vlan60	172.16.0.194	YES	manual	up	up
Vlan70	172.16.0.210	YES	manual	up	up
Vlan80	172.16.0.226	YES	manual	up	up

Syslog Service Interface:

The Syslog service is configured with the following settings:

- Service: Syslog
- On/Off: ☒ On

The Syslog log table displays the following messages:

Service	Time	HostName	Message
1	-	172.16.0.193	16:25:52: %OSPF-5-ADJCHG: Proce...
2	-	160.10.1.1	16:25:53: %OSPF-5-ADJCHG: Proce...
3	-	172.16.0.161	16:25:53: %OSPF-5-ADJCHG: Proce...
4	-	160.10.1.1	16:25:58: %OSPF-5-ADJCHG: Proce...
5	-	172.16.0.177	16:25:58: %OSPF-5-ADJCHG: Proce...
6	-	160.10.1.1	%HSRP-6-STATECHANGE: Vlan10 G...
7	-	160.10.1.1	%HSRP-6-STATECHANGE: Vlan50 G...

Layer 2 security

Port security configurations has been shown above.

DHCP snooping

In order to protect against unauthorized or malicious DHCP activities, layer 2 network security feature DHCP snooping is used. It works by keeping track of and controlling DHCP messages sent and received between clients and servers. Messages can travel through trusted ports connected to reliable DHCP servers, while messages connecting to untrusted ports connected are checked. In addition to maintaining a binding database of IP and MAC addresses, DHCP snooping validates DHCP responses ([2021](#)).

Here, DHCP snooping is applied in the L2 switch connected to the DHCP server so that IP from any other server is not accessible by different departments. The interface connecting to the server is trusted which automatically distrust other interfaces providing an extra layer of security.

Figure 69

DHCP Snooping

```
DHCP-access-sw1(config)#do sh ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
1
Insertion of option 82 is enabled
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Interface          Trusted      Rate limit (pps)
-----
FastEthernet0/2    yes         unlimited
DHCP-access-sw1(config)#
DHCP-access-sw1(config)#
```

BPDU guard

A layer 2 network security feature called BPDU Guard is intended to stop accidental loops in Ethernet networks. In order to maintain a loop-free topology using the Spanning Tree Protocol (STP), switches exchange messages known as Bridge Protocol Data Units (BPDUs), which are monitored for on ports. A BPDU Guard-enabled port quickly stops the port after receiving a BPDU, successfully preventing the unintentional generation of network loops that can cause network instability and performance problems [PortFast and BPDU Guard. \(n.d.\)](#).

BPDU guard and port fast is configured and enabled in access layer switch of servers of Kansas branch and headquarters.

Figure 70

BPDU guard and port fast

```
Kansas-datacenter-access(config)#do sh spanning-tree summary
Switch is in rapid-pvst mode
Root bridge for: default
Extended system ID      is enabled
Portfast Default        is enabled
PortFast BPDU Guard Default is enabled
Portfast BPDU Filter Default is disabled
Loopguard Default       is disabled
EtherChannel misconfig guard is disabled
UplinkFast              is disabled
BackboneFast            is disabled
Configured Pathcost method used is short
```

Name	Blocking	Listening	Learning	Forwarding	STP Active
VLAN0001	0	0	0	2	2
1 vlans	0	0	0	2	2

```
Kansas-datacenter-access(config)#
Switch#sh spanning-tree summary
Switch is in pvst mode
Root bridge for: default
Extended system ID      is enabled
Portfast Default        is enabled
PortFast BPDU Guard Default is enabled
Portfast BPDU Filter Default is disabled
Loopguard Default       is disabled
EtherChannel misconfig guard is disabled
UplinkFast              is disabled
BackboneFast            is disabled
Configured Pathcost method used is short
```

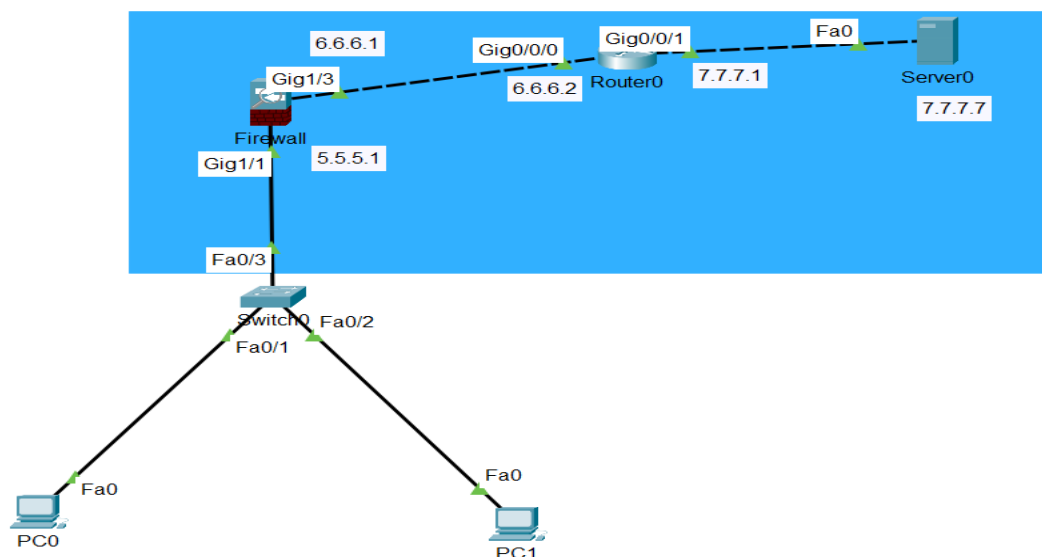
Name	Blocking	Listening	Learning	Forwarding	STP Active
VLAN0001	0	0	0	2	2
1 vlans	0	0	0	2	2

Firewall

A firewall acts as a protective barrier between trusted internal systems and external, potentially problematic networks like the internet, operating as a safeguarding tool within computer networks. Its main job is to control and monitor the movement of incoming and outgoing data traffic while complying to predetermined security regulations. By following these guidelines, firewalls improve network security by rejecting efforts of unauthorized access, fending off online threats, and preventing data breaches ([What Is a Firewall?, n.d.](#)).

Figure 71

Firewall setup



Firewall configuration

In the above shown network fire wall has been configured to provide IP address through DHCP to each PC. ICMP (ping) and TCP protocols are allowed inside the firewall. Furthermore, ACL, NAT and routing protocol has been separately configured.

IP address assigned inside firewall

In the interface g1/1 IP address of 5.5.5.1/8 and interface g1/3 has been assigned the address 6.6.6.1/24.

Figure 72

IP in firewall

```
!
interface GigabitEthernet1/1
 nameif inside
 security-level 100
 ip address 5.5.5.1 255.0.0.0
!

interface GigabitEthernet1/3
 nameif outside
 security-level 0
 ip address 6.6.6.1 255.255.255.0
!
```

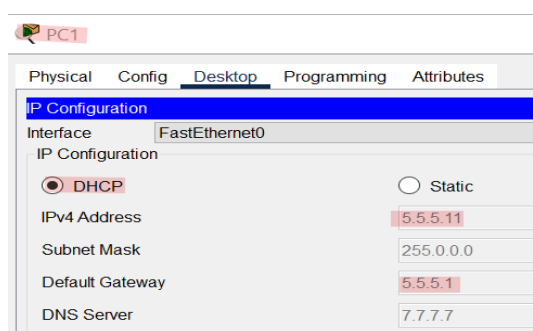
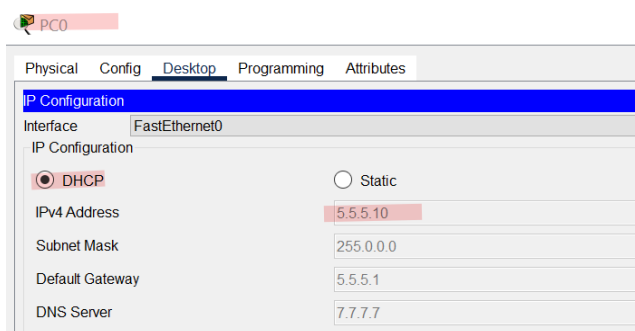
DHCP pool

DHCP address allocation is configured on the g1/1 interface to assign IP addresses to PCs. The DHCP pool is defined to allocate addresses from 5.5.5.10 to 5.5.5.50, with a DNS server address of 7.7.7.7. 'dhcpd enable inside' enables DHCP inside the inside interface, done with natting.

Figure 73

DHCP config in firewall

```
!
dhcpd address 5.5.5.10-5.5.5.50 inside
dhcpd dns 7.7.7.7 interface inside
dhcpd enable inside
!
```



ACL and Access groups

Extended policy of ACL named net is configured to permit any Transmission Control Protocol (TCP) traffic to pass unrestrictedly from any source IP address to any destination IP address. This rule permits various types of TCP-based communications, such as web browsing, email, file transfers, and more. Likewise, the second policy permits ICMP traffic, commonly known as "ping," to flow without hindrance from any source IP address to any destination IP address.

Figure 74

ACL and Access-group

```
access-list net extended permit tcp any any
access-list net extended permit icmp any any
!
!
access-group net out interface outside
access-group net in interface outside
!
```

Meanwhile, in the access-group, ACL applies the "net" ACL outbound on the outside interface. Outbound ACLs determines what types of outgoing traffic are permitted or denied based on source, destination, and protocols i.e., the traffic leaving the firewall and entering the external network. This helps prevent unauthorized or potentially harmful traffic from leaving your network and reaching the external environment.

Applying the "net" ACL inbound on the outside interface (access-group net in interface outside) involves regulating incoming traffic directed at your network from external sources. Inbound ACLs allow you to filter and control the types of traffic allowed to enter your network. By specifying permitted and denied traffic based on specific criteria, you can protect your internal network from potential threats and unauthorized access attempts originating from the outside.

NAT

```
object network aarya
  subnet 5.5.5.0 255.255.255.0
  nat (inside,outside) dynamic interface
,
```

When devices within the "aarya" subnet (5.5.5.0/24) send traffic from the internal network ("inside" interface) to external destinations ("outside" interface), the source IP address of the outgoing packets is automatically replaced with the IP address of the "outside" interface (6.6.6.1) before leaving the firewall. This helps conceal the internal IP addresses and presents a single external IP address (6.6.6.1) to the outside world, improving security and privacy while allowing internal devices to communicate with external resources.

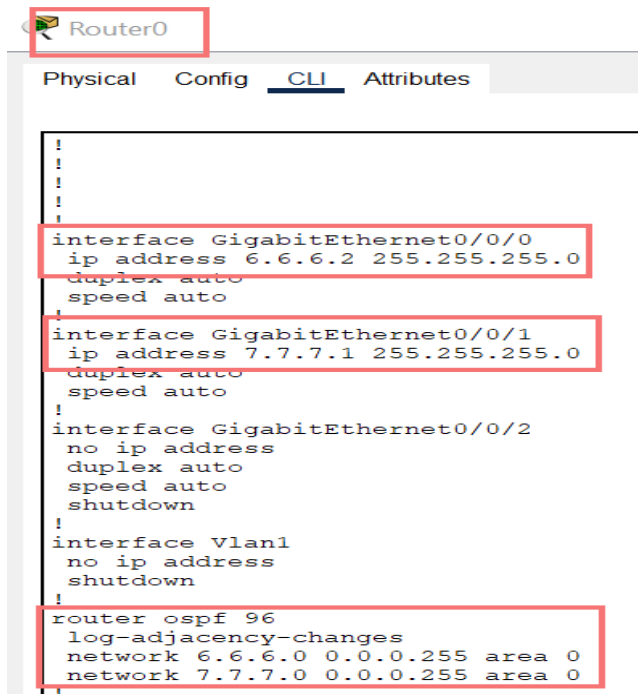
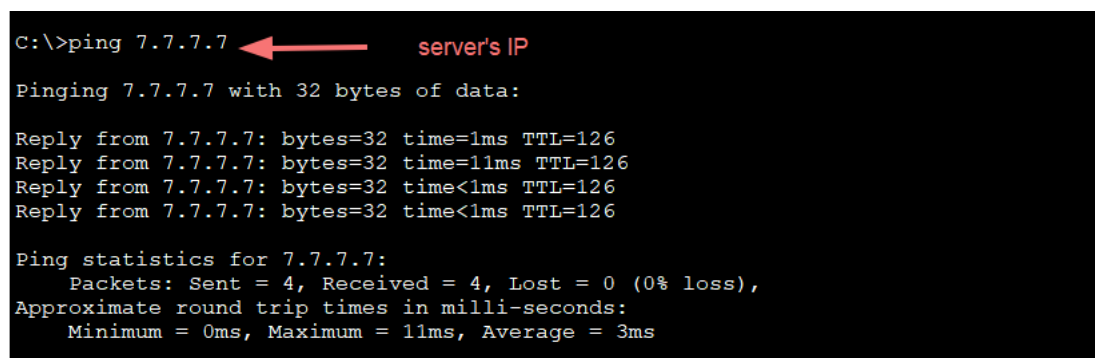
Static Default

```
:
route outside 0.0.0.0 0.0.0.0 6.6.6.2 1
,
```

route outside 0.0.0.0 0.0.0.0 6.6.6.2 1 sets a default route for all traffic to go to the next hop IP address 6.6.6.2.

Router configuration

IP addresses assigned in the router are 6.6.6.2/24 and 7.7.7.1/24 towards firewall and server respectively. Furthermore, OSPF has also been configured which is routing the above mentioned networks.

Figure 75*Configuration in router***ICMP echo request****Figure 76***Ping from PC to server*

The secure flow of traffic through firewall is configured and ping request was successful from PC to server.

Software-Defined Networking (SDN)

Software-Defined Networking (SDN) is a networking approach that separates the control plane from the data plane in network devices. In traditional networks, these planes are tightly integrated within devices like switches and routers. In SDN, the control plane, responsible for making decisions about how data is routed, is centralized in a software controller. This controller communicates with network devices to direct data flow and manage network policies. The data plane, on the other hand, focuses solely on forwarding data based on instructions received from the controller. This separation allows for dynamic and programmable control of the network, enabling rapid adjustments to changing traffic patterns and network requirements ([Raza, 2021](#)).

Network Virtualization

Network virtualization is a technology that abstracts and separates the physical network infrastructure from the services it provides. It allows multiple virtual networks to coexist on the same physical network hardware. Each virtual network operates as if it has its own isolated set of network resources, including virtual switches, routers, and even its own addressing scheme. This abstraction is achieved through software-based techniques, enabling efficient utilization of physical resources and improved isolation between different virtual networks.

This is like making building seem to have more rooms than it actually does by creating virtual floors that only certain departments can access, and they can rearrange their rooms and furniture however they want. In the world of networking, it is like we're creating virtual spaces that act like separate networks, even though they're using the same physical network equipment. This makes sure that each virtual networks can't see or interfere with each other.

Cloud computing

Cloud computing is a paradigm that involves delivering various computing services – such as computing power, storage, and applications – over the internet. These services are provided by remote servers hosted in data centers, which are accessed by users and organizations through a network connection. Cloud computing is categorized into three main models: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). Each model offers different levels of control and management for users. The underlying network infrastructure of cloud computing relies on data centers interconnected with high-speed networks, enabling rapid provisioning and scalability of resources based on demand.

Visualize cloud computing as the act of renting a toolbox rather than possessing and storing all tools within your home. Ordinarily, when a specific tool is required for a project, it would be purchased, allocated storage space, and maintained. Yet, in the realm of cloud computing, a metaphorical enchanted toolbox materializes at your disposal whenever tools are needed. All tools are securely housed within a designated workshop (data center) situated remotely, accessible through an internet connection.

Impact on traditional three tier network

The integration of Software-Defined Networking (SDN), network virtualization, and cloud computing significantly impacts the traditional three-tier network architecture. SDN introduces centralized control and programmability, allowing dynamic traffic management across tiers. Network virtualization abstracts physical resources, enabling multiple virtual networks on the same infrastructure, enhancing isolation and scalability. Cloud computing shifts certain functions to external servers, potentially altering the distribution of tiers. These technologies collectively lead to a more adaptable, efficient, and scalable network architecture.

Risk Assessment and management

Effective risk management involves discovering, analyzing, and ranking possible dangers and risks to the company's operations, assets, and goals through regular risk assessments. These evaluations are essential for preserving a proactive approach to risk reduction and guaranteeing the organization's resilience in the face of changing difficulties. The risk management plan must be updated as part of a continuous improvement process to address new risks and threats. This entails several crucial actions.

Regular risk assessments assist in identifying new or evolving hazards that may emerge as a result of technical improvements, legislative changes, market upheavals, or other external causes. It's possible that the initial risk management plan did not take these new risks into account.

Once emerging risks have been discovered, they must be thoroughly analyzed in order to comprehend their possible impact and possibility. Organizations can effectively allocate resources and set priorities thanks to this analysis.

Updated risk mitigation methods should be included in the risk management plan to handle the recently discovered risks and it should specify who is responsible for managing and keeping track of the increasing risks. To guarantee the success of the revised risk management plan, regular review and monitoring are also very essential.

Enhancing Network Security: Comprehensive Policies and Procedures

To guarantee the security and integrity of the network infrastructure, complete security rules and procedures must be developed and put into place for the networking module. These policies that are made provide precise instructions for upholding a safe and resilient network environment and has encompassed every aspect of network architecture, setup, and operations.

Security in Network Architecture

- The network architecture should be precisely defined, along with segmentation, VLANs, and DMZ design.
- Set up security perimeters and zones to keep sensitive information and crucial components separate.
- Establish rules for where to put firewalls, intrusion detection/prevention systems, and other security hardware.
- Put in place secure remote access techniques like VPNs and two-factor authentication (2FA).

Security via Configuration

- Consider it mandatory to use strong, complex passwords and to update them frequently.
- To prevent unauthorized access, use role-based access control (RBAC).
- Access control lists (ACLs) can be set up to restrict communication between various network segments.
- To stop unauthorized devices from connecting to network ports, enable port security.
- Use Dynamic ARP Inspection and DHCP snooping to reduce address spoofing attacks.
- To hide internal IP addresses from outside networks, use network address translation (NAT).

Administrative Security

- Update and patch network hardware and software often to fix known vulnerabilities.
- Use logging and monitoring techniques to identify security incidents and take appropriate action.
- Set up incident response processes to deal with security breaches and prevent harm.
- To find potential weakness, conduct frequent security audits and vulnerability assessments.
- To stop unauthorized changes, provide protocols for secure configuration management and change control.
- Inform and acquaint users and network administrators with security best practices and guidelines.

Adherence to Policy

- The aforementioned rules and procedures should be followed.
- A procedure for periodic policy evaluation must be established and revised to account for emerging threats and technologies.
- Ongoing oversight, audits, and accountability methods must be utilized to enforce policy adherence.
- Penalties for non-compliance will be fined to guarantee that defined security criteria are followed.

Conclusion

In summary, the documentation presented here shows a detailed plan for a strong and secure three-tier network that adequately showcases expertise in network and security consulting. The architecture offers both efficient communication and robust data protection by seamlessly combining VLANs, OSPF and BGP routing, NATing, VPN, and a variety of necessary security measures. The addition of Layer 2 security safeguards and a distinct firewall configuration further demonstrate the company's dedication to all-encompassing defence. Clarifying the impact of SDN on the three-tier network architecture and creating risk management strategies and policies demonstrate the company's commitment to keeping up with cutting-edge technology while upholding high security standards. The company's reputation as an industry leader is embodied by its comprehensive approach to network design and security.

References

Can Anyone Please Explain L3 SVI Configuration ,What Is SVI and Where - Cisco Community. <https://community.cisco.com/t5/switching/can-anyone-please-explain-l3-svi-configuration-what-is-svi-and/td-p/4508180>

EtherChannel in Computer Network - GeeksforGeeks. (2018, May 3). GeeksforGeeks. <https://www.geeksforgeeks.org/etherchannel-in-computer-network/>

Hosting, S. W. (n.d.). What Are Email Protocols - POP3, SMTP and IMAP - SiteGround Tutorials. SiteGround Knowledge Resources. <https://world.siteground.com/tutorials/email/protocols-pop3-smtp-imap/>

J. (2021, August 30). What is DHCP Snooping? - Explanation and Configuration - Study CCNA. Study CCNA. <https://study-ccna.com/dhcp-snooping/>

PortFast and BPDU Guard. (n.d.). PortFast and BPDU Guard. https://www.arubanetworks.com/techdocs/ArubaOS_64_Web_Help/Content/ArubaFrameStyles/Branch%20Office/PortFast%20and%20BPDU%20Guard.htm

Raza, D. (2021, September 11). Software Defined Networks(SDN). Medium. https://medium.com/@danish_raza/software-defined-networks-sdn-7b5e3c25ba97

Simple Network Management Protocol (SNMP) - GeeksforGeeks. (2018, July 17). GeeksforGeeks. <https://www.geeksforgeeks.org/simple-network-management-protocol-snmp/>

ComputerNetworkingNotes. <https://www.computernetworkingnotes.com/ccna-study-guide/supernetting-tutorial-supernetting-explained-with-examples.html>

Switchport Port Security Explained With Examples. (n.d.). ComputerNetworkingNotes. <https://www.computernetworkingnotes.com/ccna-study-guide/switchport-port-security-explained-with-examples.html>

Types of Routing Protocols - The Ultimate Guide (The Essentials!). Comparitech.

<https://www.comparitech.com/net-admin/routing-protocol-types-guide/>

U. (2019, November 2). Default static route. Study CCNA. <https://study-ccna.com/default-static-route>

Understand the Hot Standby Router Protocol Features and Functionality. (2022, August 5). Cisco. <https://www.cisco.com/c/en/us/support/docs/ip/hot-standby-router-protocol-hsrp/9234-hsrpguidetoc.html>

Understand VLAN Trunk Protocol (VTP). (2022, December 13). Cisco. <https://www.cisco.com/c/en/us/support/docs/lan-switching/vtp/10558-21.html>

What Is a Firewall? (n.d.). Cisco. <https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html>

What Is a Virtual Private Network (VPN)? (n.d.). Cisco. <https://www.cisco.com/c/en/us/products/security/vpn-endpoint-security-clients/what-is-vpn.html>

What Is a WLAN Controller? (WLC). (n.d.). Cisco. <https://www.cisco.com/c/en/us/products/wireless/wireless-lan-controller/what-is-wlan-controller.html>

What Is AAA? (n.d.). What Is AAA? https://www.arubanetworks.com/techdocs/ClearPass/6.7/Aruba_DeployGd_HTML/Content/802.1X%20Authentication/About_AAA.htm

What is DHCP (Dynamic Host Configuration Protocol)? (2023, January 1). Networking. <https://www.techtarget.com/searchnetworking/definition/DHCP>

What is syslog? | Sumo Logic. (n.d.). Sumo Logic. <https://www.sumologic.com/syslog/>

What is the role of NAT and PAT in making internet routing more efficient. (n.d.). What Is the Role of NAT and PAT in Making Internet Routing More Efficient.

<https://www.tutorialspoint.com/what-is-the-role-of-nat-and-pat-in-making-internet-routing-more-efficient>