Final Assignment

Ashim Pradhan

Ethical hacking and CyberSecurity, Softwarica College

STW360CT: Advanced Network Management and Design

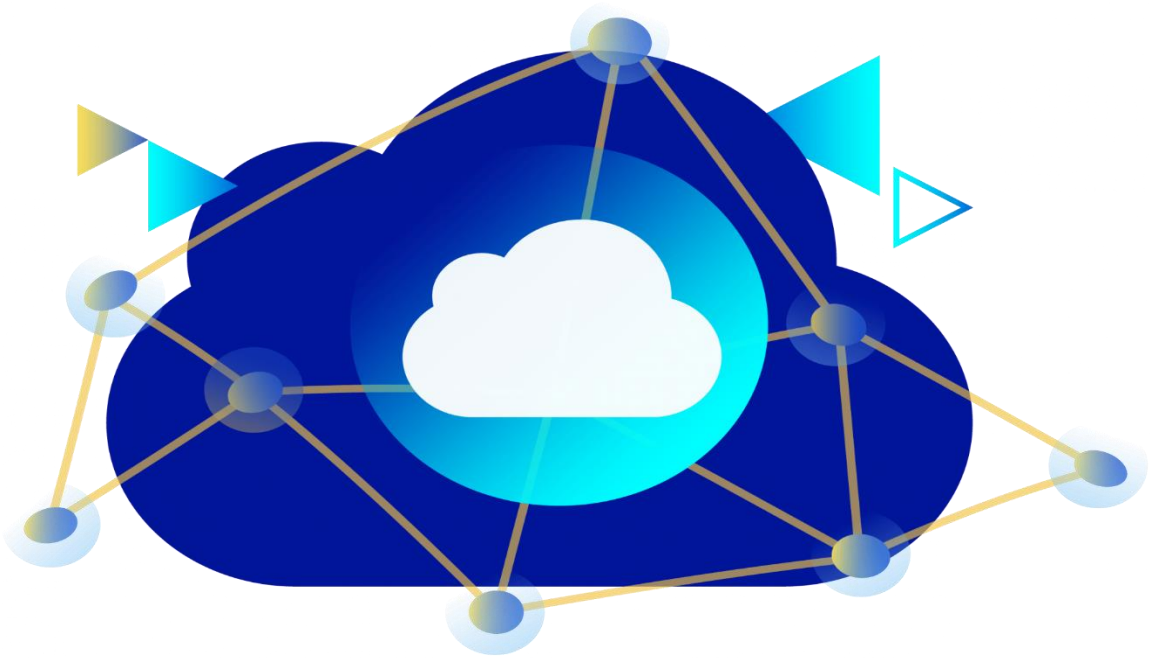
Manoj Tamang

Date: 27/07/2022

Contents

Introduction

This is the detailed report of the network architecture done by the company named Networks hat which is based in Kathmandu, Nepal. The company is worth 2.5 billion dollars and is one of the leading companies in the telecommunications industry. The networking is done with the end-to-end security on the system with both l2 as well as l3 security used. This company has been designing networks based on Campus design network architecture. Which consists of different layers such as the access layer which is the closest to the end user and which allows the user to get their request to further network reachable. Then comes the distribution layer which distributes the route all over the network and then there is the core layer which consists of the route to the edge router and the whole network. Then finally the edge route paves the path for the request to the outer world known as the internet.

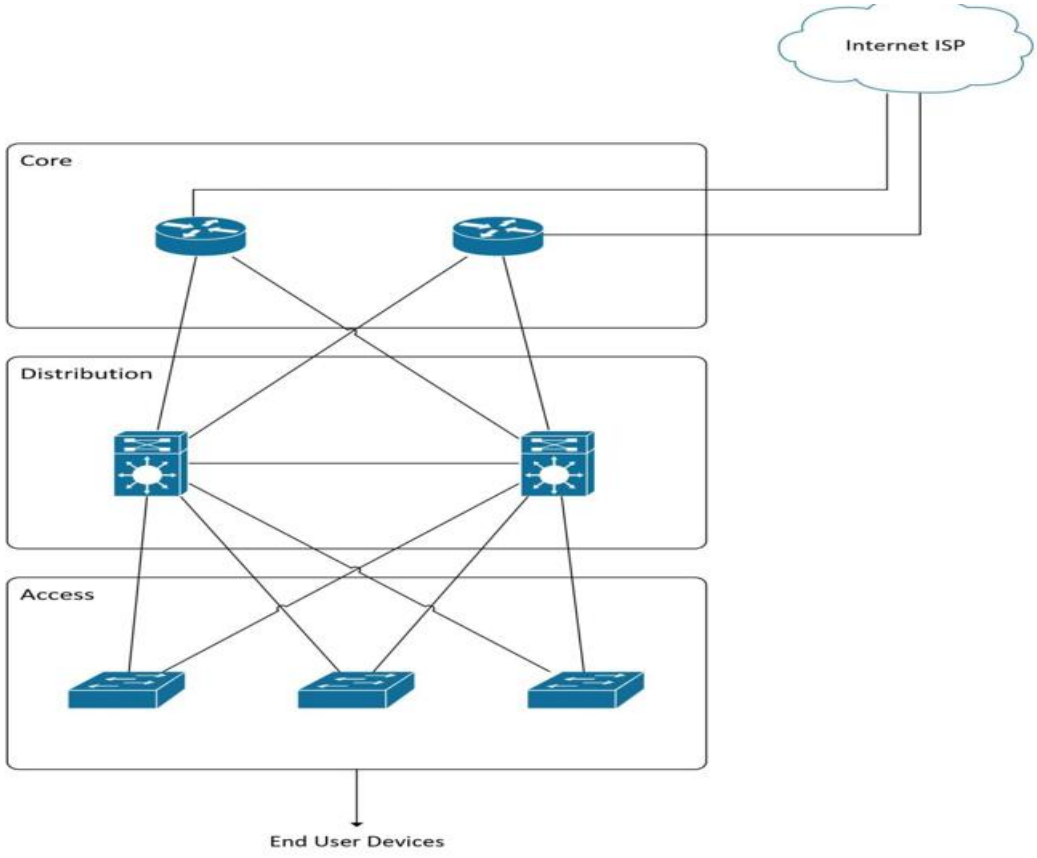


The network is designed in a full redundant way such that even if there is any failure on one device of the system it will not harm any of their services. Different services are used so that the system can heal even after any failure the system, alert if any malicious activity has been detected as well as monitor the devices. The effective use of layer 3 devices, such as multilayer switches, routers and layer 2 switches, Wireless controllers and access points, as well as routing and security protocols. Additionally, the network will be expandable if the business grows in the future. The VPN connection between the company's branches is another crucial procedure. Additionally, the system can be accessed remotely from the branches. Management of the different services on the network is done using the different types of servers such as DHCP, DNS, TFTP etc.

Network Design

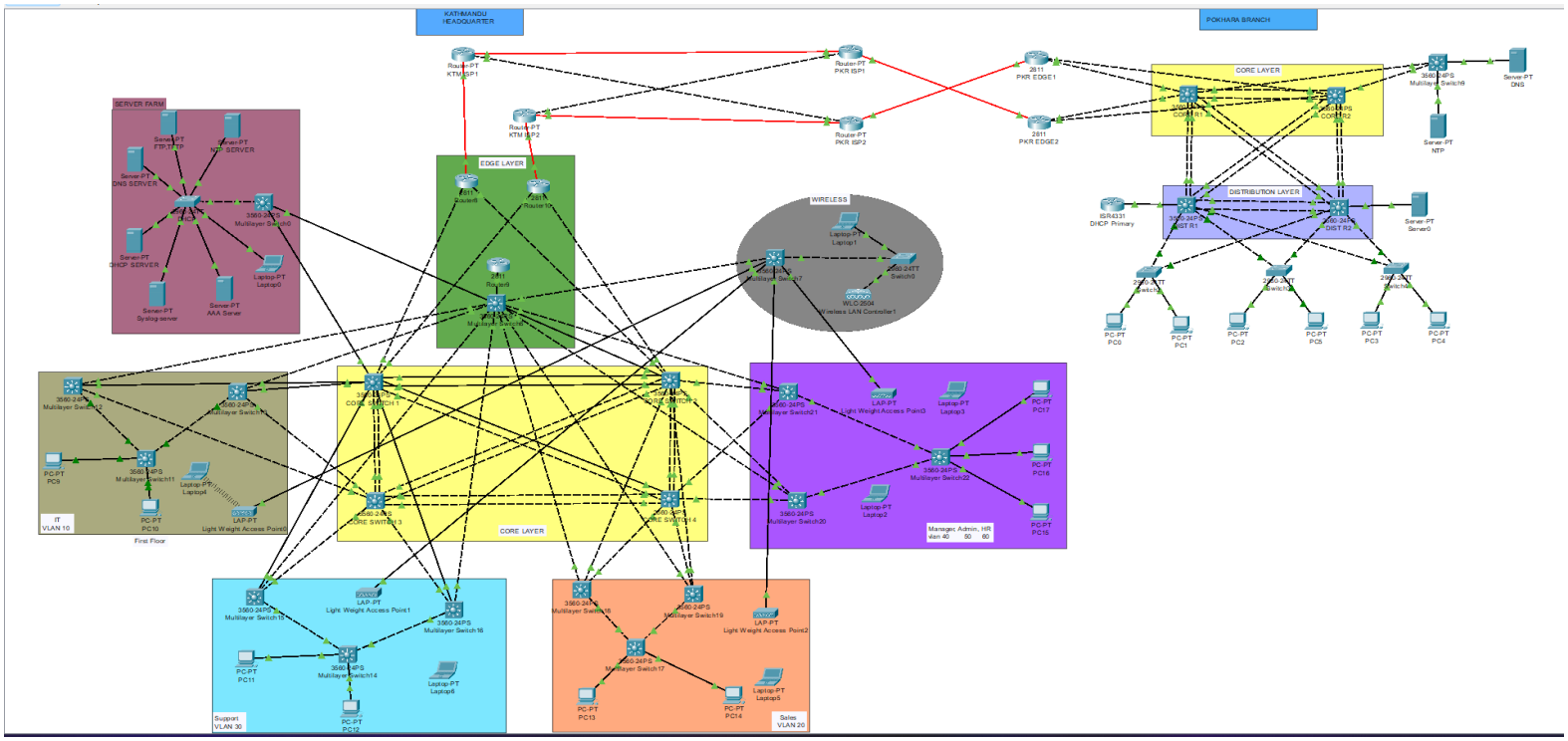
The design of the network is done using Campus Design network architecture, this networking is done for the enterprise which is located in a single geographical region. This hierarchical design consists of three different layers in it.

- Core layer: This is the central part of the network every packet from within the network travel from here to different sites. This part of the network must have higher resilience so that if any failure event on the network occurs then it must recover quickly and run smoothly for the betterment of the network services.
- Distribution Layer: This layer implements different policies to run the services on the network such as QoS, load balancing etc. This acts as the border between the access layer and the core layer in the network.
- Access layer: This provides the way to access the whole network to the end user and enjoy the network services available.

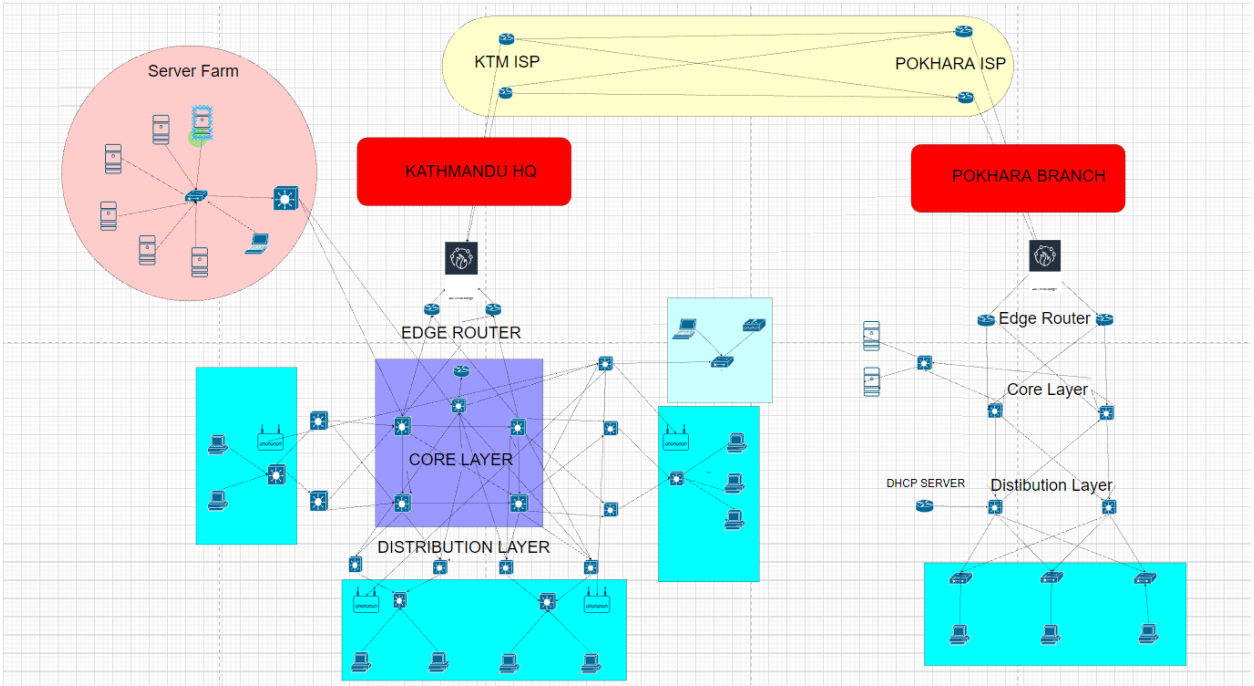


The above pictures show us the structural image of the campus network design usually used on the network.

PHYSICAL LAYOUT



LOGICAL LAYOUT



Assigning IP Addresses

The organized and preplanned way of assigning the IP addresses is the key part for the network designer. As IP addresses are limited resources, so it must be preserved and used wisely to avoid any wastage of the IP. Different departments are given as the requirement to have in the network which needs to be fulfilled. So to avoid the wastage of the IP on the network the subnetting of the IP address is done. The subnetting is done throughout the network and not only in the case of the department.

Department	Network	Subnet Mask	Usable Host
IT	192.168.149.0	255.255.255.128	192.168.149.1-126
Sales	192.168.149.128	255.255.255.192	192.168.149.129-190
Support	192.168.149.192	255.255.255.224	192.168.149.193-222
Management	192.168.149.224	255.255.255.240	192.168.149.225-138
Admin	192.168.149.240	255.255.255.240	192.168.149.141-154
HR	192.168.150.0	255.255.255.248	192.168.150.1-6

In the network, two types of IP are used private and public. The private IP is used inside the enterprise network as they are available for free. So these IPs are generally used inside the network as a different company can same private IP. While the public IP is of value and costs some amount of money. And these tips are unique and are always one in number throughout the world.

VLAN Allocation

VLANs are created to create the logical boundaries between the network and allow us to split the broadcast of the network devices. So if we command interface to access one VLAN it means we have created a new broadcast for it and is separated from the default broadcast of the device. The command for VLAN allocation is given below


```
Switch(config)#vlan 20
Switch(config-vlan)#name IT
Switch(config-vlan)#exit
Switch(config)#int f0/1
Switch(config-if)#swi
Switch(config-if)#switchport acc
Switch(config-if)#switchport access vlan 20
Switch(config-if)#swi
Switch(config-if)#switchport mod
Switch(config-if)#switchport mode tr
Switch(config-if)#switchport mode trunk
```

Ctrl+F6 to exit CLI focus

Now below is the VLAN created in the network with the network assigned to it.

VLAN No.	VLAN Name	Department
10	IT	IT
20	Sales	Sales
30	Support	Support
40	Management	Management
50	Admin	Admin
60	HR	HR

Layer Two Protocol Used

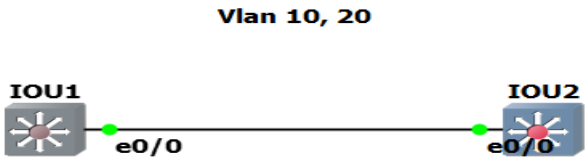
Different kinds of protocols are used in networking for the proper connections between the two network devices and to transmit the data from one device to other. The protocol is used both on layer 2 as well as layer 3 and also in the upper layer as well. Some of the layer 2 protocols used in the network topology is as follows:

VTP Protocol

This protocol is used in both the distribution and the access layer. The vtp is used wisely on those layers as the major need of the VLAN creation is in the access layer so if any VLAN is created here must be written to the distribution layer to make the gateway for the VLANs. So for this, the switches in both the layer are kept in the same domain and with the same password but with the different modes enabled on it. The access layer switches are turned from server to mode and the distribution switches are turned to client mode. As there is no need to create any VLAN in the distribution other than in the access layer. So by this protocol, the VLAN created on the access layer is written to the distribution switches.

Trunking

The trunking protocol is done on layer two of the OSI model. In this network, topology trunking is almost done on all the access layer switches. This is done here to allow all the traffic coming from different VLANs to travel from that path simultaneously. This is done here as there is more than one VLAN on the same switch so to transmit signals we only need to create trunk ports instead of adding other cables to the switch.



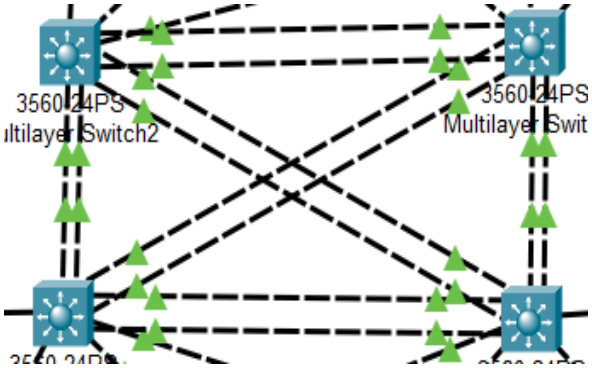

```
IOU1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
IOU1(config)#vlan 10
IOU1(config-vlan)#exit
IOU1(config)#vlan 20
IOU1(config-vlan)#exit
IOU1(config)#int e0/0
IOU1(config-if)#swi
IOU1(config-if)#switchport tr
IOU1(config-if)#switchport trunk
% Incomplete command.

IOU1(config-if)#switchport trunk enca
IOU1(config-if)#switchport trunk encapsulation do
IOU1(config-if)#switchport trunk encapsulation dot1q
IOU1(config-if)#swi
IOU1(config-if)#switchport mode
IOU1(config-if)#switchport mode tr
IOU1(config-if)#switchport mode trunk
IOU1(config-if)#
```

Spanning Tree Protocol

As in this network, topology redundancy has been made so that the network is not disturbed by a single change on the network device. So in case of device failure, the redundant ways can be referred to flow the data in that way. So while creating this in switches different loops can be formed to avoid the port being blocked automatically. So to bring back that blocked interface to up stp is used which allows user to make one switch root bridge for 1 VLAN and other for other remaining VLAN. This means the VLAN packet from 1 transfers from another way while other Vlans packets flow from an alternative way.

Etherchannel

There has been the use of different redundant ways in the network design which will allow much-needed redundancy in the time of need. This has been used between two multilayer switches which use two cables to connect. This is simply used in the core layer of the network which holds the whole pressure of data transmission. The same IP addresses are given to two of the interface so that both interfaces can act like one interface on the device.




```
D_SW1#sh etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate
aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


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

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

10     Po10(RU)           LACP   Fa0/1(P) Fa0/7(P)
12     Po12(RU)           LACP   Fa0/8(P) Fa0/9(P)
D_SW1#
```

This EtherChannel is done to avoid the blockage of the interface due to stp. So that all the interfaces could transfer the data between the source and destination.

CDP protocol

This protocol is simply used on the devices to monitor the devices connected. All the devices are configured with CDP protocol as the cables are connected to the switch routers. They are connected in such a way that it is very hard to notice which one is connected to which specific device. So to monitor those devices in such cases CDP protocol has been used.

```
CNTL/Z.
DSW1(config)#cdp run
DSW1(config)#do sh cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B -
Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r -
Repeater, P - Phone
Device ID    Local Intrfce   Holdtme    Capability
Platform    Port ID
Switch       Fas 0/4          132
3560        Fas 0/1
Core1        Fas 0/2          132
3560        Fas 0/1
SW1          Fas 0/1          137
3560        Fas 0/3
Core3        Fas 0/3          132
3560        Fas 0/1
DSW1(config)#
```

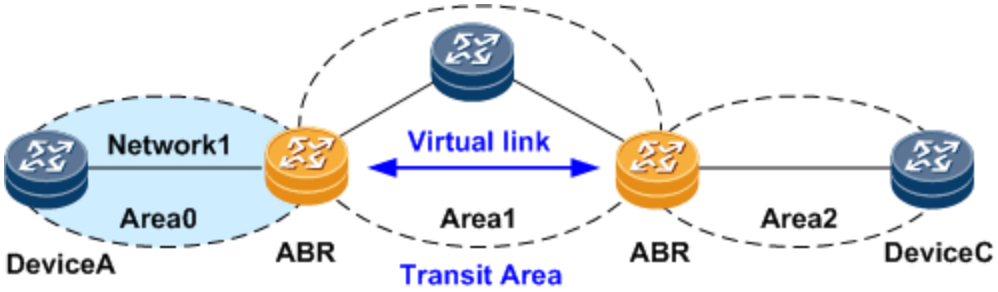
Layer three protocol Used

Different protocols have also been used on the layer three devices on the network to establish the communication between the devices. Some of the protocols which have been used in this network topology are the OSPF routing protocol, hsrp etc.

OSPF Routing Protocol

This routing protocol has been used overall in all the private networks i.e on the enterprise network both in headquarters and branch. This Routing protocol has been used to connect different areas on the network. Where the core layer of the network is named area 0 and the other layer on the network is connected to this backbone of the network. Through which the route of the different areas is shared throughout the network.

And the concept of the virtual link is also used in some cases where the other non-backbone area are not directly connected to the backbone areas. For this to happen the router between Area 0 and the non-backbone area is virtually linked by which the ABR router shares its route with the non-backbone area router. With this, the end user from the non-backbone area can still access the network without being attached to the backbone area.



Eigrp Protocol

This protocol is used in the public ISP area where it is used to share the route between the isp with the partnership of BGP protocol. The EIGRP neighborship between the ISP router and the public side of the edge router of the company is done. While creating the neighbourship between the routers we have been taking good care of their autonomous system number and the network which is being directly connected. This routing protocol is used only in the public area only for the help of EBGP protocol which is configured on all public routers.

```
Router#sh run | Sec eigrp
router eigrp 10
 network 67.45.40.0 0.0.0.7
 network 200.150.0.4 0.0.0.3
 network 67.45.40.8 0.0.0.3
 no auto-summary
Router#sh ip eigrp nei
Router#sh ip eigrp neighbors
IP-EIGRP neighbors for process 10
H   Address         Interface       Hold Uptime    SRTT
RTO   Q   Seq
                                    (sec)          (ms)
Cnt  Num
0   67.45.40.10     Fa5/0           10   01:18:56  40
1000  0   16
1   200.150.0.6     Fa0/0           14   01:18:56  40
1000  0   13
2   67.45.40.1      Fa4/0           11   01:18:56  40
1000  0   15

Router#
```

Border Gateway Protocol

This protocol is used on the internet site as it is reliable to carry a huge amount of route information. Among internal and external BGP, external BGP is used as the different autonomous system numbers used in the topology. This protocol has been used so that there is no loss of packet if there is any change in the path of the route. So, it will insist to the user that there is no loss on the packet sent over the ISP if there is any failure on any of the network devices.

```
Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ
OutQ Up/Down  State/PfxRcd
67.45.40.10     4   105     108      81        36    0
0 00:16:24        4
67.45.40.1      4   100      82      81        36    0
0 00:16:24        4
200.150.0.6     4   106     104      82        36    0
0 00:16:25        4

Router#sh run | sec bgp
router bgp 102
 bgp log-neighbor-changes
 no synchronization
 neighbor 67.45.40.10 remote-as 105
 neighbor 67.45.40.1 remote-as 100
 neighbor 200.150.0.6 remote-as 106
 network 67.45.40.0 mask 255.255.255.248
 network 200.150.0.4 mask 255.255.255.252
 network 67.45.40.8 mask 255.255.255.252
Router#
```

HSRP Protocol

This protocol is used on the distribution layer where there is more than one gateway for the end user VLAN. So by using this protocol one is setting one of the gateway switches as the main or active gateway while the other remains the standby switch. By using this protocol some kind of load balancing on the data packet that travels from the end user to the network is done. At one time, one VLAN uses one of the gateways as its active gateway while at the same time another VLAN uses it as a standby gateway and directs its packet from the other gateway. In this protocol one of the switch's priorities is set higher than the another to indicate that it is the active gateway.

Network Services

Different types of services are made available on the network for the users to enjoy while they are connected to it. These services will allow the user to access the server which is being dedicated to network services. While accessing these services users can surf the internet, store their data in the servers, and get the IP automatically after getting connected to the network. Some of the services that are commonly used on the network are DHCP, DNS, TFTP, NAT, VPN etc.

DHCP Service

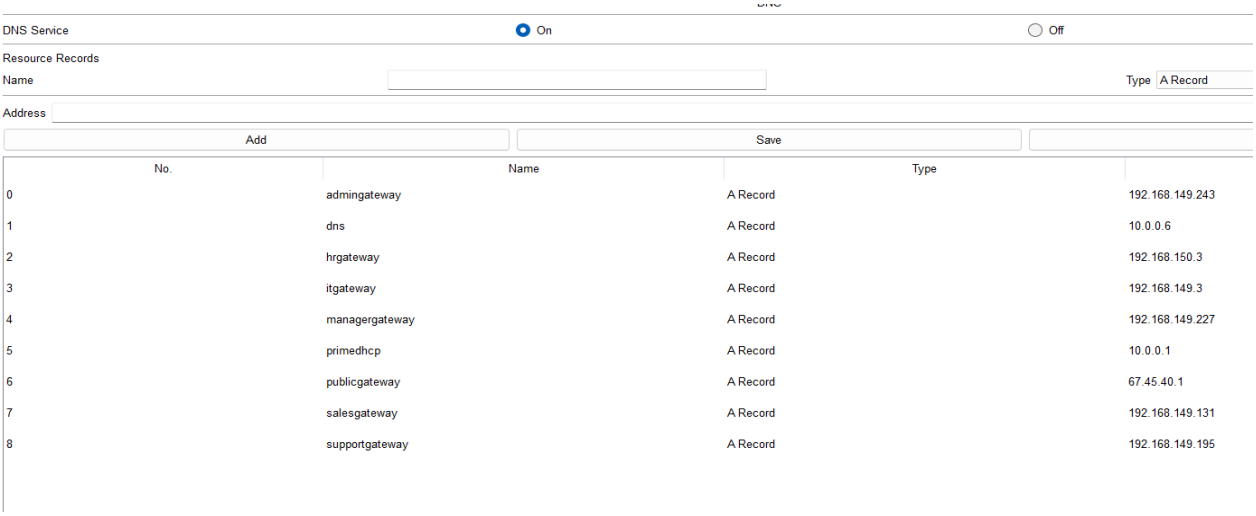
There are overall two DHCP servers which have been dedicated to assigning the IP to the user according to the block provided by the network administrator. This service minimizes the risk of IP duplication on the network which might cause the tragic in the network. The primary DHCP is established on the distribution layer for assigning IP addresses faster to the end user. While the secondary server is set up on the core layer so that in case of any failure on the primary DHCP it will take over. And the services on the entire network carry on with the failure of one device on the network.

Add | Save

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User
Sales	192.168.149.131	10.0.0.6	192.168.149.132	255.255.255.192	50
Support	192.168.149.195	10.0.0.6	192.168.149.196	255.255.255.224	20
Management	192.168.149.227	10.0.0.6	192.168.149.228	255.255.255.240	8
Admin	192.168.149.243	10.0.0.6	192.168.149.244	255.255.255.240	5
HR	192.168.150.3	10.0.0.6	192.168.150.4	255.255.255.248	3
IT	192.168.149.3	10.0.0.6	192.168.149.4	255.255.255.128	80
serverPool	0.0.0.0	0.0.0.0	10.0.0.0	255.255.255.252	3

DNS Service

DNS service is provided so that the user doesn't have to remember the IP address. Instead, they need to remember the domain name to access the much easier device. As people, it is hard for one to remember the IP which is four octets long while domain names such as fb.com, and www.ashim.com can be a lot easier for the user to remain. So to make the user remember the name of the device the DNS service remembers its IP and converts the domain name written by the user.



No.	Name	Type	
0	admingateway	A Record	192.168.149.243
1	dns	A Record	10.0.0.6
2	hrgateway	A Record	192.168.150.3
3	itgateway	A Record	192.168.149.3
4	managergateway	A Record	192.168.149.227
5	primedhcp	A Record	10.0.0.1
6	publicgateway	A Record	67.45.40.1
7	salesgateway	A Record	192.168.149.131
8	supportgateway	A Record	192.168.149.195

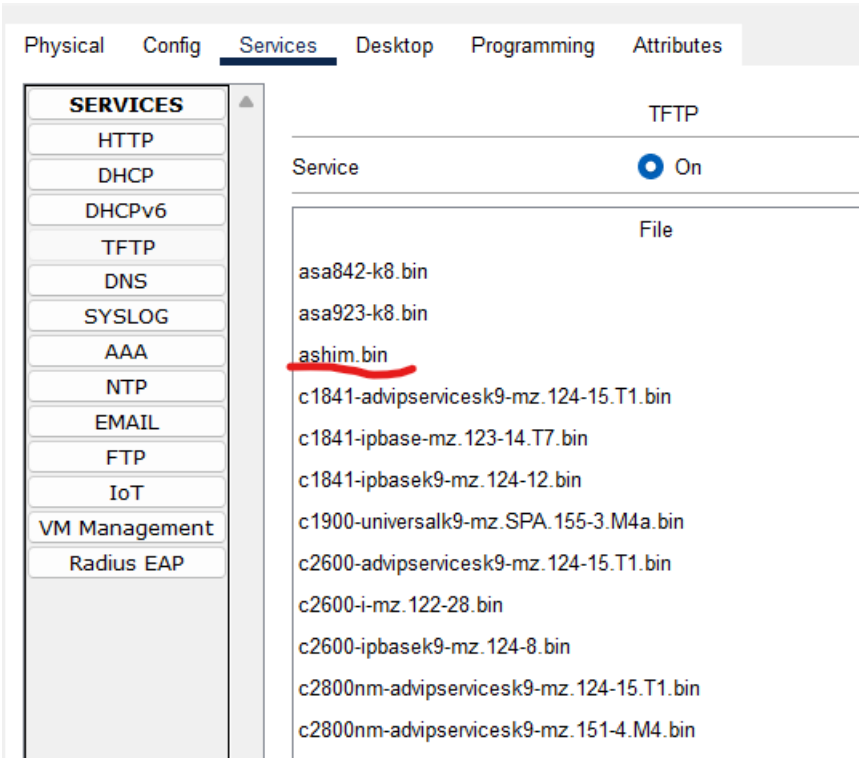
TFTP

The file from the remote server can be accessed and uploaded to the server easily with the use of TFTP. The updated version of the IOS file for the devices can be downloaded by one user and uploaded to the server. Then the other user can download this file from the server which will be must faster and easier for a user to do. Downloading the bigger iso file from the internet takes a much longer time than downloading from this server which is within the network. This means this server is also meant for sharing the file between the user of the employee. And most importantly it is meant to preserve the resource, time of the user etc.

```
DSW1#copy flash: t
DSW1#copy flash: tftp:
Source filename []? c3560-advipservicesk9-mz.
122-37.SE1.bin
Address or name of remote host []? 10.0.0.10
Destination filename [c3560-advipservicesk9-mz.
122-37.SE1.bin]? ashim.bin

Writing c3560-advipservicesk9-mz.
122-37.SE1.bin....!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!
[OK - 8662192 bytes]

8662192 bytes copied in 4.123 secs (17525 bytes/sec)
DSW1#
```

Ctrl+F6 to exit CLI focus

Copy Paste



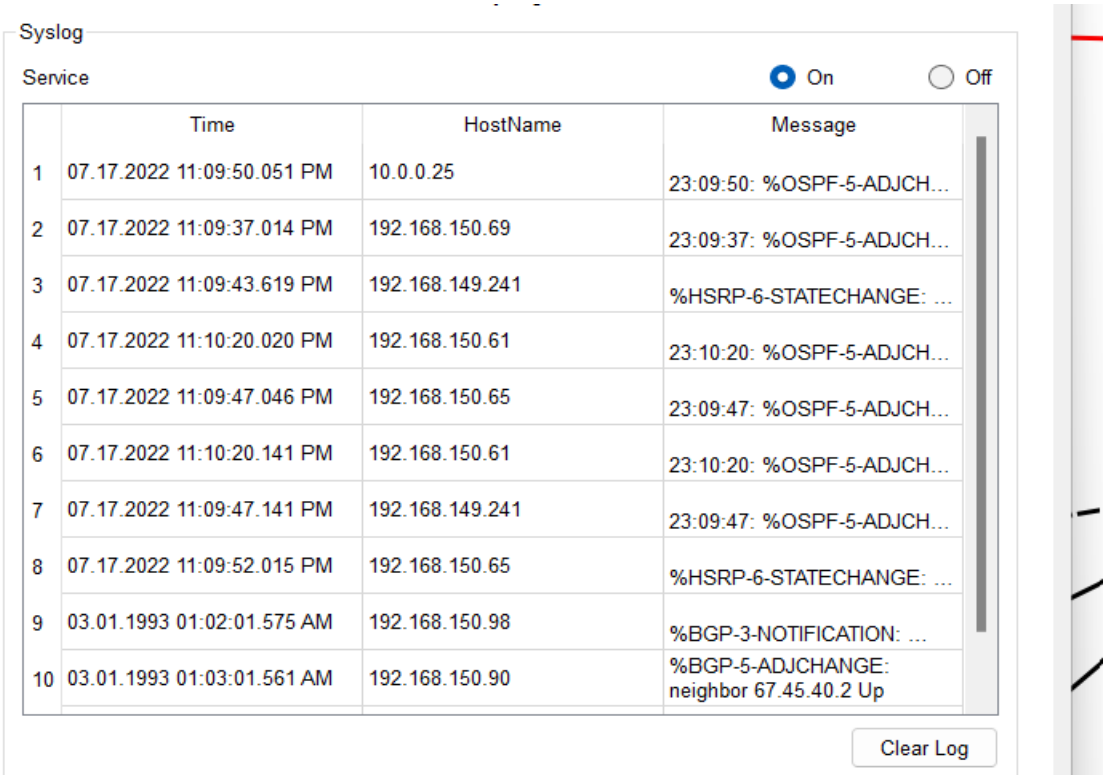
NTP

The server is meant to maintain the time synchronization within the network. The time synchronization on the network with the NTP server maintains this synchronization with every packet switched on the network.

```
Switch#sh ntp status
Clock is synchronized, stratum 2, reference is 10.0.0.18
nominal freq is 250.0000 Hz, actual freq is 249.9990 Hz,
precision is 2**24
reference time is E656330D.0000004F (22:54:5.079 UTC Sun
Jul 17 2022)
clock offset is 0.00 msec, root delay is 0.00  msec
root dispersion is 16.45 msec, peer dispersion is 0.11
msec.
loopfilter state is 'CTRL' (Normal Controlled Loop),
drift is - 0.000001193 s/s system poll interval is 4,
last update was 11 sec ago.
Switch#
```

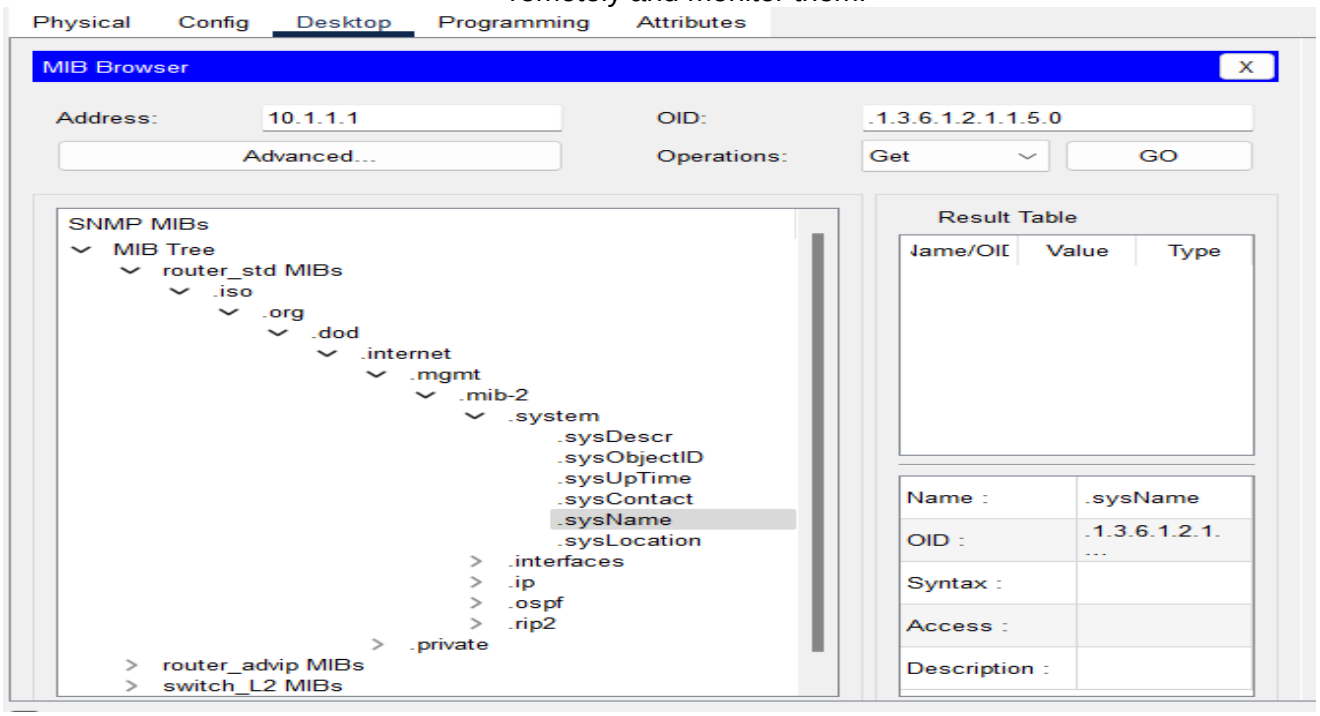
SYSLOG

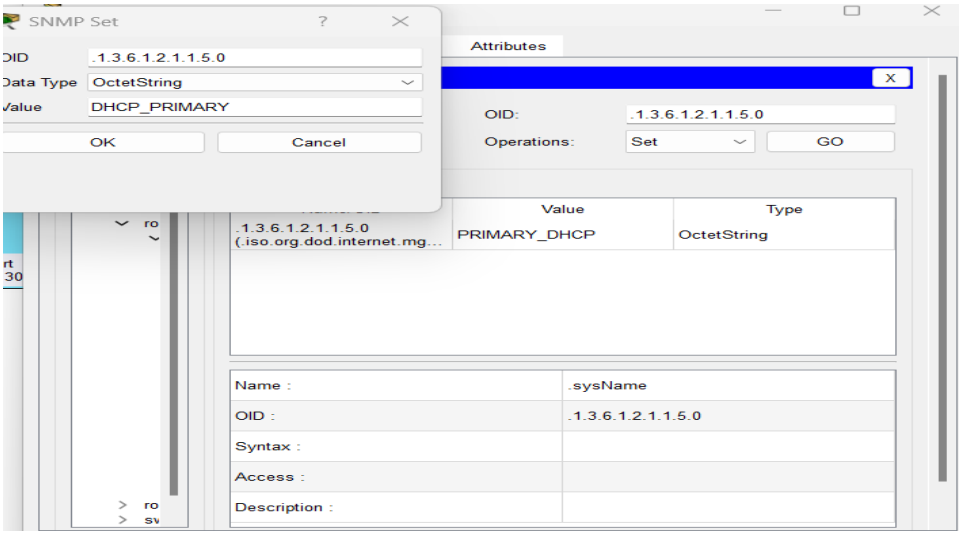
Syslog is used to monitor every event that takes place on the network. It makes it easier to communicate with the server. The Syslog agent is maintained on the network to send messages to the server for the other network devices on the network. The server maintains the log file for the whole network devices on the network. And after collecting these whole messages from the network it creates the overall view of what is going on, on the network. And helps one to know the important events that took place on the network.



SNMP

This protocol is used to monitor the devices on the network, manage the network devices and sometimes configure them remotely. It eases the task of manually monitoring the devices one by one which would be hectic work to do. So instead we can use this protocol to access them remotely and monitor them.



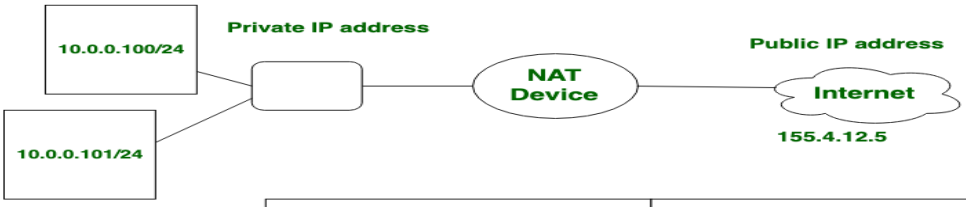


Wireless Services

The wireless device is also connected to the network with the help of an access point. This point acts as the access layer for the wireless devices through which all the wireless devices transmit their packet to each other. The whole access points are managed and monitored by a single wireless controller. And the IP to these access points is assigned directly by the DHCP server. And all the devices connecting to this access point get their IP as well from the DHCP server. The authenticity to the access point is done by WLC which means when the end user tries to connect to those access points. They are needed to provide a valid SSID of the access point and the password for that SSID.

Internet Access

One of the major services needed for one company to keep on running is internet service. Which is needed for the company for the day to day. Without any access to the internet, the company would be secluded and would not get a good future and would be very hard for them to progress. Getting access to the internet which works on public IP addresses is a tough task for the network engineer to do. As we know public addresses are needed to be bought with money and are not free as private addresses. So to translate these private addresses to public addresses using NAT. There are different types of natting in this network design the PAT is used to do the natting. PAT uses the port to translate private addresses to public addresses. For example, the addresses are converted in the below table:

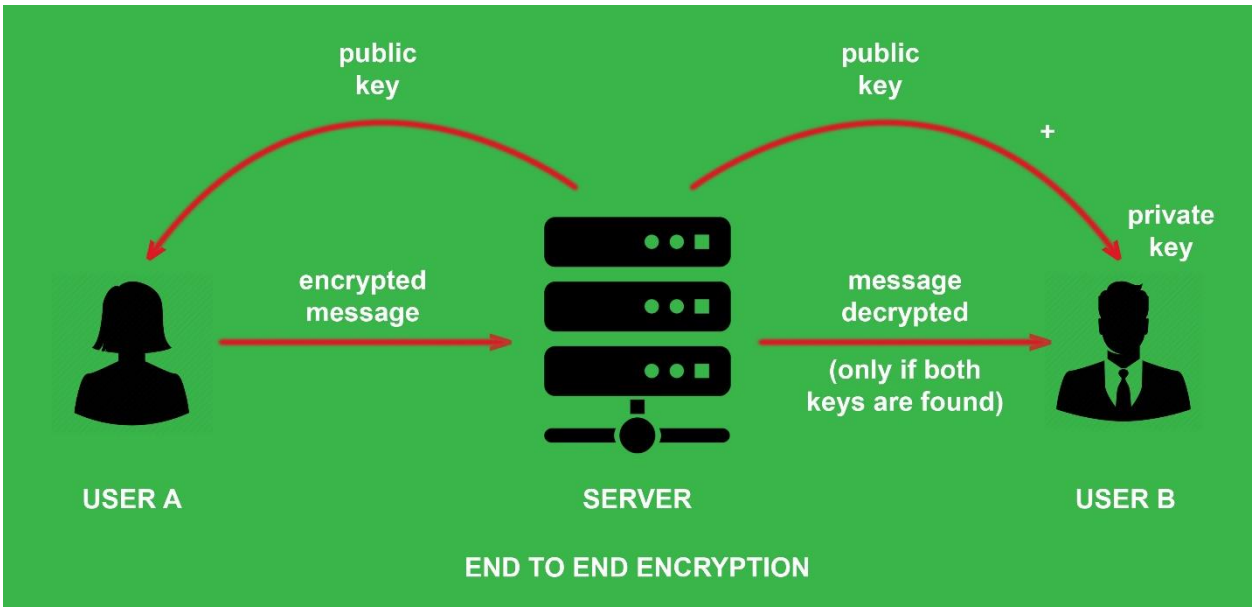


private ip address : Port	public ip address : Port
10.0.0.100:1055	155.4.12.1:1055
10.0.0.101:1056	155.4.12.1:1056

PAT

VPN Service

To get the remote service for the headquarters, admin and skilled individuals to the branches of the company mostly the VPN service is used. To access them remotely in this network site-to-site VPN has been used. With this service, one can ssh to the remote machines on the branches and access them remotely with all encrypted packets. The end-to-end encryption method is done using crypto isakmp and IPsec policy. This means every packet sent from one branch to another is end-to-end encrypted and even if an intruder tries to intercept the packet would not be able to understand any of the packets sent through.



With this VPN service, the server can be shared from the headquarters to the branches which means it would make economically good for the company which shares the server worth some thousand cash. Vpn is done on the edge router which acts as the gateway for the user packet to other branches and only allows the user to access the remote host and not by any other network inside the network. And the wireless devices on the network cannot access the remote network using a VPN service.

Remote Access

The remote access to the different network devices on the remote branch is the crucial part. To manage remote devices remote access is done using different methods such as telnet and SSH. But in this network topology ssh is used instead of telnet as it is much more secure than it. SSH is preferred here as the packet transmission is done with end to end encryption method. And passwords are shared using the sha hash algorithm.

Network Security

When the network is set up the most and foremost need of the network is to be a safe workspace to conduct some business. So to make the network safe different policies or rules, devices and services are used. Different methods are there to keep the network safe but the pre-plan would be the best option for one to create a secure network. Different sets of rules should be maintained on the network by the user to be safe from different kinds of attacks.

ACL List

These lists are created on the layer three devices or on the edge routing devices which sets a required amount of rules for the user on the network. This list determines whether the packet coming from the outside network is trustable or not. The trusted as well as untrusted networks can be mentioned here to allow or avoid the packet from that network respectively. This list is mostly used when the packets are leaving the home network and are going to leave for the branches through the outside world. And it looks for the top of the IP header where it is written what is the source of the packet and what is the destination of the packet. So this information is read and checked with the ACL list created on the network and if the source IP or destination IP is not trusted or not valid the packet is dropped. And are restricted to enter the network.

```
access-list 101 permit ip 192.168.0.0 0.0.255.255
172.16.0.0 0.0.255.255
access-list 102 permit ip 192.168.0.0 0.0.255.255
67.45.40.0 0.0.0.255
access-list 102 permit ip 192.168.0.0 0.0.255.255
202.54.0.0 0.0.255.255
access-list 102 permit ip 192.168.0.0 0.0.255.255
200.150.0.0 0.0.0.255
access-list 102 permit ip 192.168.0.0 0.0.255.255
43.250.48.0 0.0.0.255
access-list 102 permit ip 192.168.0.0 0.0.255.255
103.116.48.0 0.0.0.255
access-list 103 permit ip 10.1.2.0 0.0.0.255 67.45.40.0
0.0.0.255
access-list 103 permit ip 10.1.2.0 0.0.0.255 202.54.0.0
0.0.255.255
access-list 103 permit ip 10.1.2.0 0.0.0.255 200.150.0.0
0.0.0.255
access-list 103 permit ip 10.1.2.0 0.0.0.255 43.250.48.0
0.0.0.255
access-list 103 permit ip 10.1.2.0 0.0.0.255
103.116.48.0 0.0.0.255
Router#
```

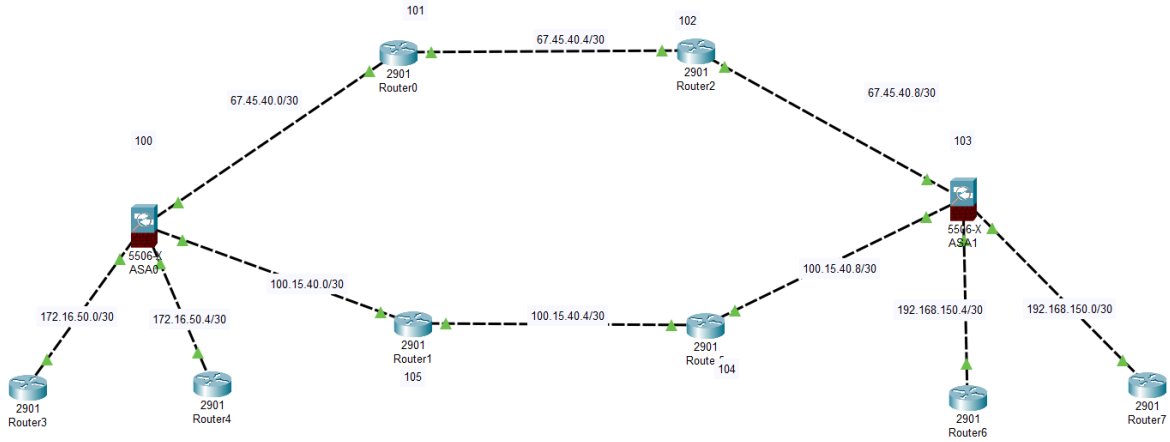
The above figure shows us the use of the extended ACL list which are range above 99 and takes rules on pair with the source and the destination network. While there are other types of ACL lists named standard which only takes the individual network whether to permit or deny. This list is usually used in the specified period.

AAA Server

AAA server is mainly used for security purposes. In the network, it is used to create certain rules to access any of the network devices. To access the console of the network devices the user must validate that he is the trusted one with passing the authentication. While on the remote accessing part they need to apply the password which has been set on this server earlier by the network administrator of the network. And also accounts for the date and time of the authentication used. This authentication simply adds up to the security of the network as the non-authorized user cannot access any of the network devices on the system. This directly maintains the authenticity of the network.

Firewall

This networking device is used to manage as well as monitor the incoming and outgoing network traffic on the network. The device acts according to the rules and policies are given by the user. They set rules first for the device to allow traffic from the trusted sites or users and act as a barrier for the traffic which is marked as intrusted. They work on the principle of outside and inside of the network. The inside of the network means the interface facing toward the internal network and the outside means the interface facing outwards to the internet.



Port-Security

The port security is done on the network to secure the network from unknown devices sending packets to the network. We can apply this to the access layer to avoid unknown devices to connect to it. We can limit the devices connected to the access devices by setting the limit of the mac address of the device as one. This means when the computer is attached to the access layer the switch learns the mac id of that device and if any other device is connected to that switch it does not allow connection to it. The violation rules can be set if any violation is done in this by connecting an unknown device to the switch then it restricts the packet coming from that device.

BPDU Guard

The BPDU guard is used on all the unused interfaces of the access layer switches to avoid attacks related to stp. This type of guard is simply used to protect the switching network. This is done so that in case of any unknown devices connected to those interfaces could not harm the network.

DHCP SNOOPING

This is the protocol used on the layer two switches to not let any untrusted dhcp to access the network. This protocol protects the network from any untrusted user who connects to the network and wants to become the DHCP server and allocate the IP to the user.

```
DHCP snooping trust/rate is configured on the following
Interfaces:

Interface                  Trusted    Allow option
Rate limit (pps)
-----------------------    -------    ------------
----------------
FastEthernet0/4            yes        yes
unlimited
  Custom circuit-ids:
FastEthernet0/3            yes        yes
unlimited
  Custom circuit-ids:
SW2#
```

Important Topics screenshot

Standby brief

```
DSW8#sh standby br
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
Vl40        40   100 P Standby  192.168.149.226 local           192.168.149.227
Vl50        50   110 P Active   local           192.168.149.242 192.168.149.243
Vl60        60   100 P Standby  192.168.150.2   local           192.168.150.3
DSW8#
```

OSPF Route

```
Core2#sh ip route ospf
     1.0.0.0/32 is subnetted, 1 subnets
O       1.1.1.1 [110/2] via 192.168.150.85,
4294967276:4294967246:4294967245, Port-channel15
     2.0.0.0/32 is subnetted, 1 subnets
O       2.2.2.2 [110/2] via 192.168.150.169,
4294967276:4294967246:4294967245, Port-channel12
     3.0.0.0/32 is subnetted, 1 subnets
O       3.3.3.3 [110/2] via 192.168.150.77,
4294967276:4294967246:4294967245, Port-channel13
     10.0.0.0/30 is subnetted, 7 subnets
O       10.0.0.0 [110/2] via 192.168.150.109,
4294967276:4294967246:4294967280, FastEthernet0/9
O       10.0.0.4 [110/2] via 192.168.150.109,
4294967276:4294967246:4294967280, FastEthernet0/9
O       10.0.0.8 [110/2] via 192.168.150.109,
4294967276:4294967246:4294967280, FastEthernet0/9
O       10.0.0.12 [110/2] via 192.168.150.109,
4294967276:4294967246:4294967280, FastEthernet0/9
O       10.0.0.16 [110/2] via 192.168.150.109,
4294967276:4294967246:4294967280, FastEthernet0/9
O       10.0.0.20 [110/2] via 192.168.150.109,
4294967276:4294967246:4294967280, FastEthernet0/9
```

IP DHCP POOL

```
DHCP_PRIMARY>
DHCP_PRIMARY>en
DHCP_PRIMARY#sh run | Sec pool
ip dhcp pool IT
 network 192.168.149.0 255.255.255.128
 default-router 192.168.149.3
 dns-server 10.0.0.6
ip dhcp pool Sales
 network 192.168.149.128 255.255.255.192
 default-router 192.168.149.131
 dns-server 10.0.0.6
ip dhcp pool Support
 network 192.168.149.192 255.255.255.224
 default-router 192.168.149.195
 dns-server 10.0.0.6
ip dhcp pool Management
 network 192.168.149.224 255.255.255.240
 default-router 192.168.149.227
 dns-server 10.0.0.6
ip dhcp pool Admin
 network 192.168.149.240 255.255.255.240
 default-router 192.168.149.243
 dns-server 10.0.0.6
ip dhcp pool HR
 network 192.168.150.0 255.255.255.248
 default-router 192.168.150.3
 dns-server 10.0.0.6
ip dhcp pool WLC
 network 10.0.0.24 255.255.255.252
 default-router 10.0.0.25
 dns-server 10.0.0.6
ip dhcp pool wifi
 network 10.1.2.0 255.255.255.0
 default-router 10.1.2.1
 dns-server 10.0.0.6
ip dhcp pool Admin_one
```

IP Excluded Address

```
% Incomplete command.
DHCP_PRIMARY#sh run | sec excluded
ip dhcp excluded-address 192.168.149.1 192.168.149.3
ip dhcp excluded-address 192.168.149.193 192.168.149.195
ip dhcp excluded-address 192.168.149.129 192.168.149.131
ip dhcp excluded-address 192.168.149.225 192.168.149.227
ip dhcp excluded-address 192.168.149.241 192.168.149.243
ip dhcp excluded-address 192.168.150.1 192.168.150.3
ip dhcp excluded-address 10.1.2.3
ip dhcp excluded-address 192.168.149.250
DHCP_PRIMARY#
```

NAT

```
Router>en
Router#sh run | sec nat
 ip nat inside
 ip nat inside
 ip nat outside
 default-information originate
ip nat inside source list 102 interface FastEthernet1/0
overload
ip nat inside source list 103 interface FastEthernet1/0
overload
Router#
```

Ctrl+F6 to exit CLI focus Copy Paste

VPN

```
Router#sh run | Sec crypto
crypto isakmp policy 10
 authentication pre-share
 group 5
crypto isakmp key branch_hq address 103.116.48.1
crypto ipsec transform-set VPN esp-aes esp-sha-hmac
crypto map name 10 ipsec-isakmp
 set peer 103.116.48.1
 set transform-set VPN
 match address 101
 crypto map name
Router#
```

Ctrl+F6 to exit CLI focus Copy

BGP Route

```
Router#sh ip route bgp
B    43.250.48.0 [20/0] via 200.150.0.6, 00:00:00
B    103.116.48.0 [20/0] via 67.45.40.10, 00:00:00
B    200.150.0.0 [20/0] via 67.45.40.10, 00:00:00
B    202.54.0.0/29 [20/0] via 67.45.40.10, 00:00:00
B    202.54.0.8/30 [20/0] via 200.150.0.6, 00:00:00

Router#
```

Conclusion

Hence the proper security devices and maintaining proper rules can make a network safe from any malicious activity. Though the user is prohibited from accessing some of the sites which are in return for their good as well as for the company. As the technology keeps on growing and is unstoppable so the network needs to be more scalable and more smooth in any kind of situation. So while planning for the network one must keep in mind the scalability of the network and healing strength of the network. And faster the data packet transmission between the network devices on the network better it is for the users.

Recommendation

The network devices on the network must be monitored and managed properly. The ACL list on the firewall must be properly maintained and timely updated as per the requirement of the network. And the password of the different protocols must be changed timely and should keep a stronger password so that no authentication problems occur.