JANUARY 16, 2023

Softwarica College of IT and E-commerce

Coventry University

NISCHAL KC
NETWORKING
Manoj tamang

Table of Contents

Table of figures

Table of tables

INTRODUCTION

This report includes the task of planning, putting into place, managing, and monitoring an organization's WAN and local networks. This implies that the job is to create documentation, administer, maintain, and enhance the organization's systems as much as feasible. By giving priority to four key areas—security, redundancy, quality, and quick adoption of high-security protocols—the project will be suited for the enterprises. The network will be secure, dependable, and set up using firewall tools like Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) etc.

Network design architecture

Several layers of architecture are developed as distinct network designs, each of which has a specific objective. Different layers have different specific rules that manage and support the network system. The layers are divide into t3 tires. I.e. core layer, distribution layer (DIST) and access layer (SW).

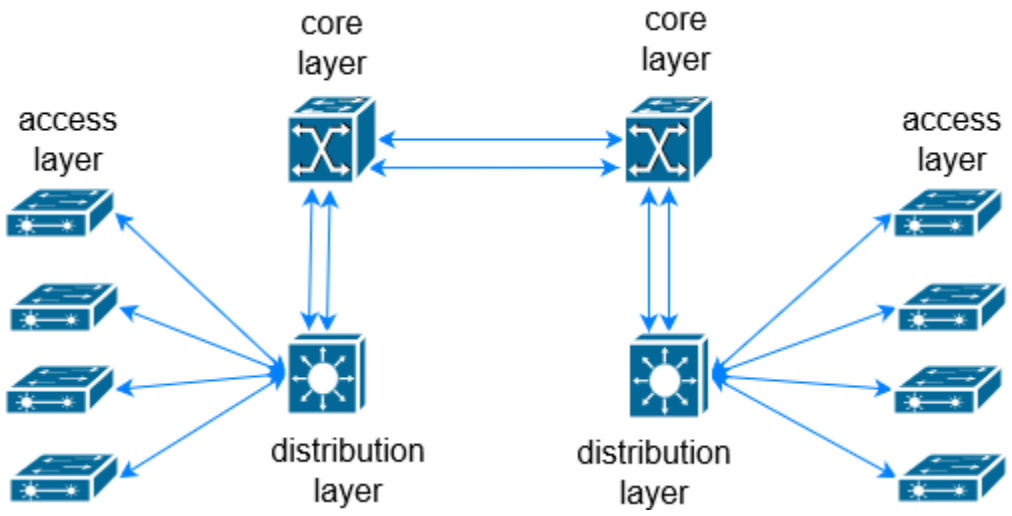


Figure 1 ; network architecture

This kind of network structure is beneficial to smaller network system as it cannot be expanded too much larger networks. This network design consist of only 3 layers which effects network versatility and compatibility with different services and devices. Architecture has been built using a modular system that provides redundancy, efficiency, stability, and simplicity of management.

Project objective

The ultimate objective of this task is to build, configure, and improvise the network of network-solution;

- Secure access into internet and off-site branches.
- Increase in capacity of network.
- Decrease low-latency for customer mobility.
- Identify the main points of failure in the current network and offer solutions to fix them.
- Centralization of network location for better control and establishment.
- Using an access point to aid with wireless device management and a wireless controller to monitor the AP.
- Configuring the network with least privilege, user-oriented access and secure environment.
- Backup route for every network for secure data connection.
- Maintain remote connection between main network administrators to branch with web protocols.

Logical diagram

The logical structure of the network is separated which is demonstrated in diagram given below;

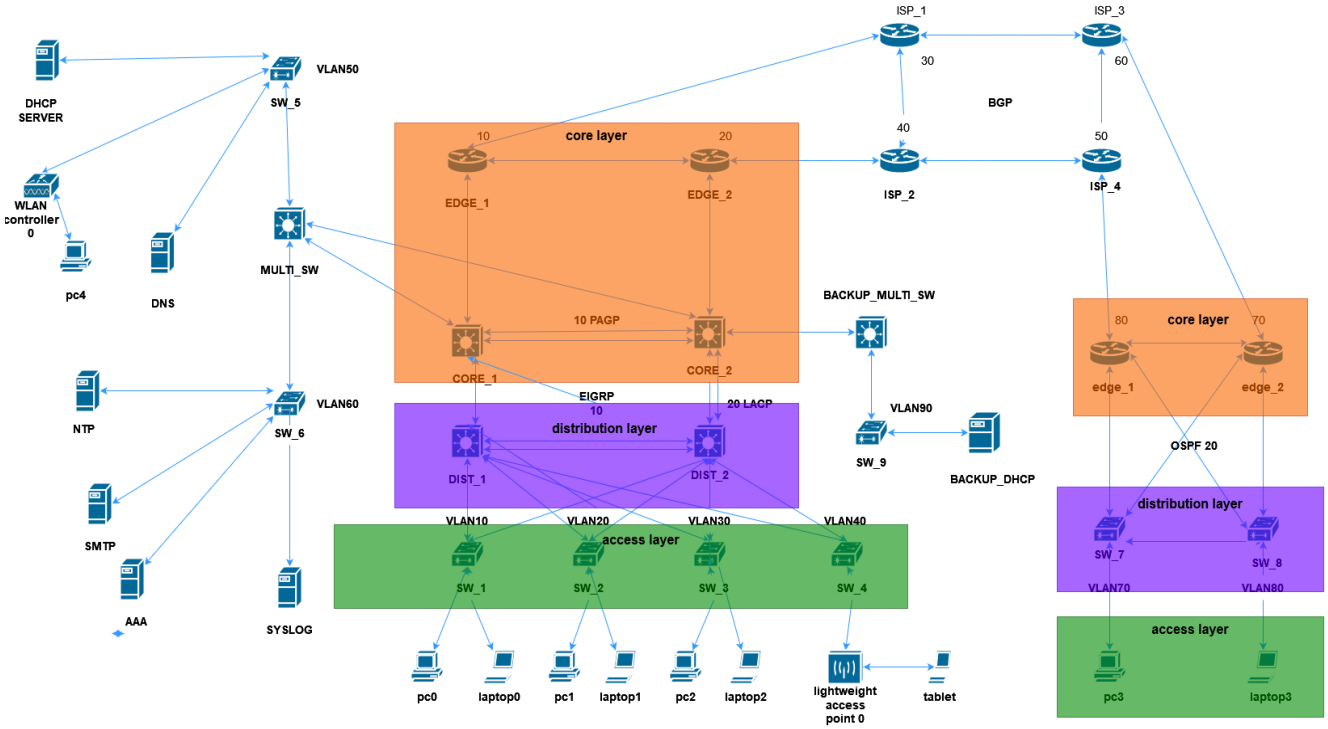


Figure 2 ; logical diagram

Physical architecture

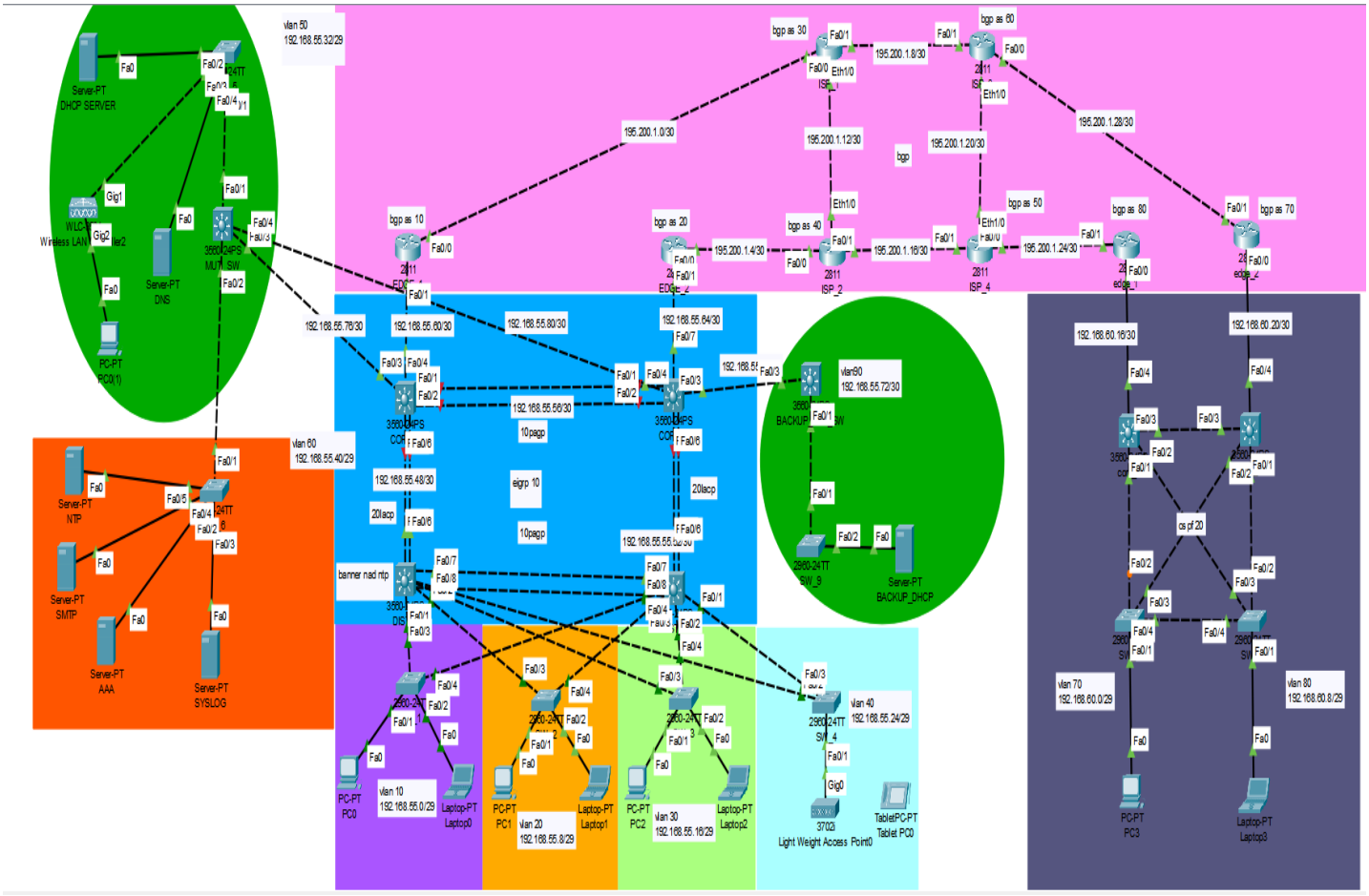


Figure 3 ; physical architecture

Vlan allocation plan

Due to the university networks extensive broadcasts area. Switches cause traffic overflow on the network, which compromises both performance and security. So, the first step in improving a LAN's security and reliability is to deploy "VLAN." The business establishes more VLANs as needed, including those for wireless APs & servers in addition to VLANs for each department. This network makes use of the VLAN encapsulation standard 802.1Q.

Department	VLAN ID	NO. of Hosts
Marketing	10	6
Sales	20	6
Support	30	6
Wireless APs	40	6
Server-1	50	6
Server-2	60	6
Branch – IT	70	6
Branch – sales & management	80	6
Backup – server	90	2

Table 1 ; VLAN allocation

Switches virtual interfaces (SVI)

These VPNs have specific logical interfaces which is regularly operated for constructing gateways.

VLAN SVIs	Gateway 1 (primary)	Gateway 2 (secondary)
Marketing (10)	192.168.55.1	192.168.55.2

Sales (20)	192.168.55.9	192.168.55.10
Support (30)	192.168.55.17	192.168.55.18
Wireless Aps (40)	192.168.55.25	192.168.55.26
Server-1 (50)	192.168.55.33	-
Server-2 (60)	192.168.55.41	-
Branch – IT (70)	192.168.60.1	192.168.60.2
Branch – sales & management (80)	192.168.60.9	192.168.60.10
Backup – server (90)	192.168.55.73	-

Table 2 ; switches virtual interfaces

IP determining plan

The complete determination of required IPs are allocated for the network-solution network.

IP determination in Kathmandu

This section contains the required IP determination of network in the Kathmandu network.

Departments	Network Address	Broadcast Address	Host address Range	Prefix	Subnet mask
Marketing	192.168.55.0	192.168.55.7	192.168.55.1-192.168.55.6	/29	255.255.255.248
Sales	192.168.55.8	192.168.55.15	192.168.55.9-192.168.55.14	/29	/29
Support	192.168.55.16	192.168.55.23	192.168.55.17-192.168.55.22	/29	255.255.255.248

Wireless APs	192.168.55.24	192.168.55.31	192.168.55.25-192.168.55.30	/29	255.255.255.248
Server-1	192.168.55.32	192.168.55.39	192.168.55.33-192.168.55.38	/29	255.255.255.248
Server-2	192.168.55.40	192.168.55.47	192.168.55.41-192.168.55.46	/29	255.255.255.248
DIST_1 – CORE 1	192.168.55.48	192.168.55.51	192.168.55.49-192.168.55.50	/30	255.255.255.252
DIST_2 – CORE 2	192.168.55.52	192.168.55.55	192.168.55.53-192.168.55.54	/30	255.255.255.252
CORE_1 – CORE_2	192.168.55.56	192.168.55.59	192.168.55.57-192.168.55.58	/30	255.255.255.252
CORE_1 – EDGE_1	192.168.55.60	192.168.55.63	192.168.55.61-192.168.55.62	/30	255.255.255.252
CORE_2 – EDGE_2	192.168.55.64	192.168.55.67	192.168.55.65-192.168.55.66	/30	255.255.255.252
CORE_2 – BACKUP_MUL_SW	192.168.55.68	192.168.55.71	192.168.55.69-192.168.55.70	/30	255.255.255.252
Backup-server	192.168.55.72	192.168.55.75	192.168.55.73-192.168.55.74	/30	255.255.255.252
CORE_1 – MUTI_SW	192.168.55.76	192.168.55.79	192.168.55.77-192.168.55.78	/30	255.255.255.252
C0RE_2 – MUTI_SW	192.168.55.80	192.168.55.83	192.168.55.81-192.168.55.82	/30	255.255.255.252

Table 3 ; IP Determination in Kathmandu server

IP determination in Dharan

This section contains the IP determination for dhading network.

Departments	Network Address	Broadcast Address	Host address Range	Prefix	Subnet mask
Branch – IT	192.168.60.0	192.168.60.7	192.168.60.1-192.168.60.6	/29	255.255.255.248
Branch – sales /management	192.168.60.8	192.168.60.15	192.168.60.9-192.168.60.14	/29	255.255.255.248
core_1 – edge_1	192.168.60.16	192.168.60.19	192.168.60.17-192.168.60.18	/30	255.255.255.252
core_2 – edge_2	192.168.60.21	192.168.60.22	192.168.60.21-192.168.60.22	/30	255.255.255.252

Table 4 ; IP Determination in Dharan server

IP determination in public ISP

Departments	Network Address	Broadcast Address	Host address Range	Prefix	Subnet mask
EDGE_1 – ISP_1	195.200.1.0	195.200.1.3	195.200.1.1-195.200.1.2	/30	255.255.255.252
EDGE_2 – ISP_2	195.200.1.4	195.200.1.7	195.200.1.5-195.200.1.6	/30	255.255.255.252
ISP_1 – ISP_3	195.200.1.8	195.200.1.11	195.200.1.9-195.200.1.10	/30	255.255.255.252
ISP_1 – ISP_2	195.200.1.12	195.200.1.15	195.200.1.13-195.200.1.14	/30	255.255.255.252

ISP_4 – ISP_2	195.200.1.16	195.200.1.19	195.200.1.17-195.200.1.18	/30	255.255.255.252
ISP_3 – ISP_4	195.200.1.20	195.200.1.23	195.200.1.21-195.200.1.22	/30	255.255.255.252
edge_1 – ISP_4	195.200.1.24	195.200.1.27	195.200.1.25-195.200.1.26	/30	255.255.255.252
edge_2 – ISP_3	195.200.1.28	195.200.1.31	195.200.1.29-195.200.1.30	/30	255.255.255.252

Table 5 ; IP Determination in Public ISPs

Module description

Network-solutions demonstrate the hierarchy model. According to this concept, networks should be built in "bits or modules" to ensure that the architecture is readily available, upgradable, and manageable.

This is particularly crucial for connecting to specialized data centers, which are frequently distant from an organization's primary headquarters and require more complicated network architectures. The following is a list of the implemented devices:

1. 2811 Router
2. Multi-Layer switch layer 3 3560 24PS
3. Switch layer 2
4. 2960 4TT router
5. Computers
6. Laptops
7. Mobile devices
8. Server
9. Light weight access
10. WLC-3504

Access layer

The user connectivity layer is referred to in this manner. The layer's primary goal is to give end users safe connections over various channels, such as Ethernet, WI-Fi, or other media. Additionally, it provides packets to the top layer. Security measures like "port-security" have also been added to this layer. Access links connect layer 2 switches to end devices, whereas 802.1Q is used to connect the distribution layer to the trunk.

Distribution layer

Distribution layer is connected to the access layer through which packet are forwarded & filtered according to the chosen strategies by a layer at a time. In this level of the network, pieces are separated with redundant cables for high-speed transmission. The two layers access and core are to be inter-connected to this layer. Regulations related to LANs are implemented in this section of layer. All VLAN gateways are created at this layer. Layer 3 switches are used in this layer, and they are linked through Layer 2 switches L2 and L3 links which are both available in this particular layer.

Core layer

This section of layer is considered to be the backbone of network. This layer is responsible for all the traffic of the foreign network (public networks of ISP). Core layer connects all remote office, company floors etc. to the internet.

The distribution layer and the access layer are directly connected to this layer. This layer is also connected to the server-1, server-2 and backup server for operating. OSPF 10 and EIGRP 20 routing protocols are used in this layer

EDGE ROUTER (network-solutions)

EDGE routers which are concluded in this category maintains nating of inside and outside network. This router connects the local network of network-solutions to the internet. Edge router is the communication bridge of internal network to internet.

Router (ISP)

Total of 4 router are connected in this networks, all of this consist of public network as assigned. The routing protocol between these routers is BGP routing protocol. Two medium for transmission are made each connected to the respective router EDGE_1 and EDGE_2. Even if one medium is disturbed another route is automatically operated.

Edge router (branch)

This router is similar to that of network-solution EDGE-ROUTER this also connects the internal network of dhading branch network to the internet (ISP). But in this network EIGRP 20 routing protocol is used and is connected to ISP_5 and ISP_6.

Services and protocols

Port security

When the frame is passed through a switch port, switches get MAC addresses. Users can create static MAC addresses, restrict the amount of MAC addresses that can be learnt for a port, and impose sanctions for such port when it is used by an unauthorized access by employing port security.

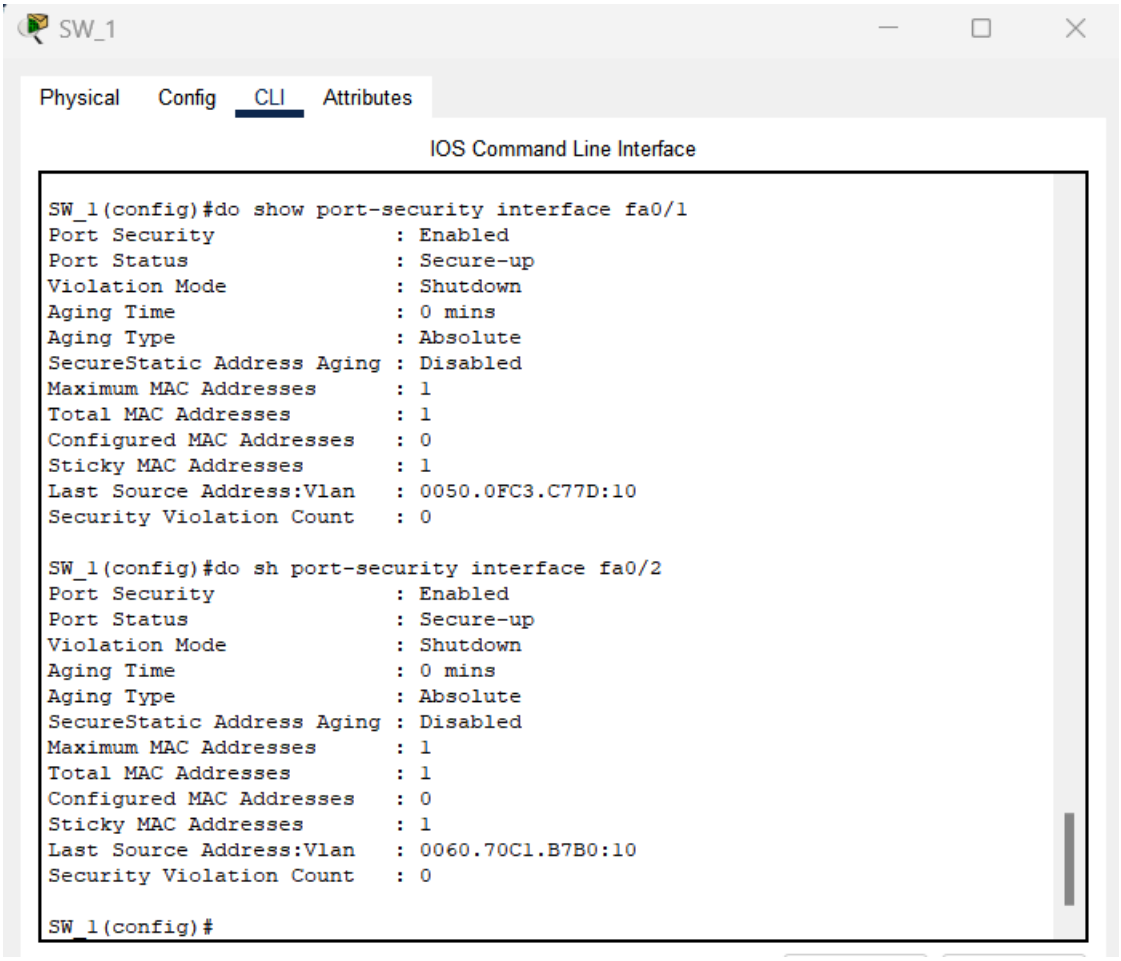


Figure 4 ; configuration of Port-security

Port fast & Spanning-tree-protocol

Configuration of Spanning Tree Protocol takes place in layer-2 switches. Reliable connections are added to a LAN to increase system availability. But unless some action is done, such as taking certain links down, these duplicate linkages may cause the frames to repeat in the networks indefinitely. Spanning Tree Protocol (STP) is used to address the issue of frame looping.

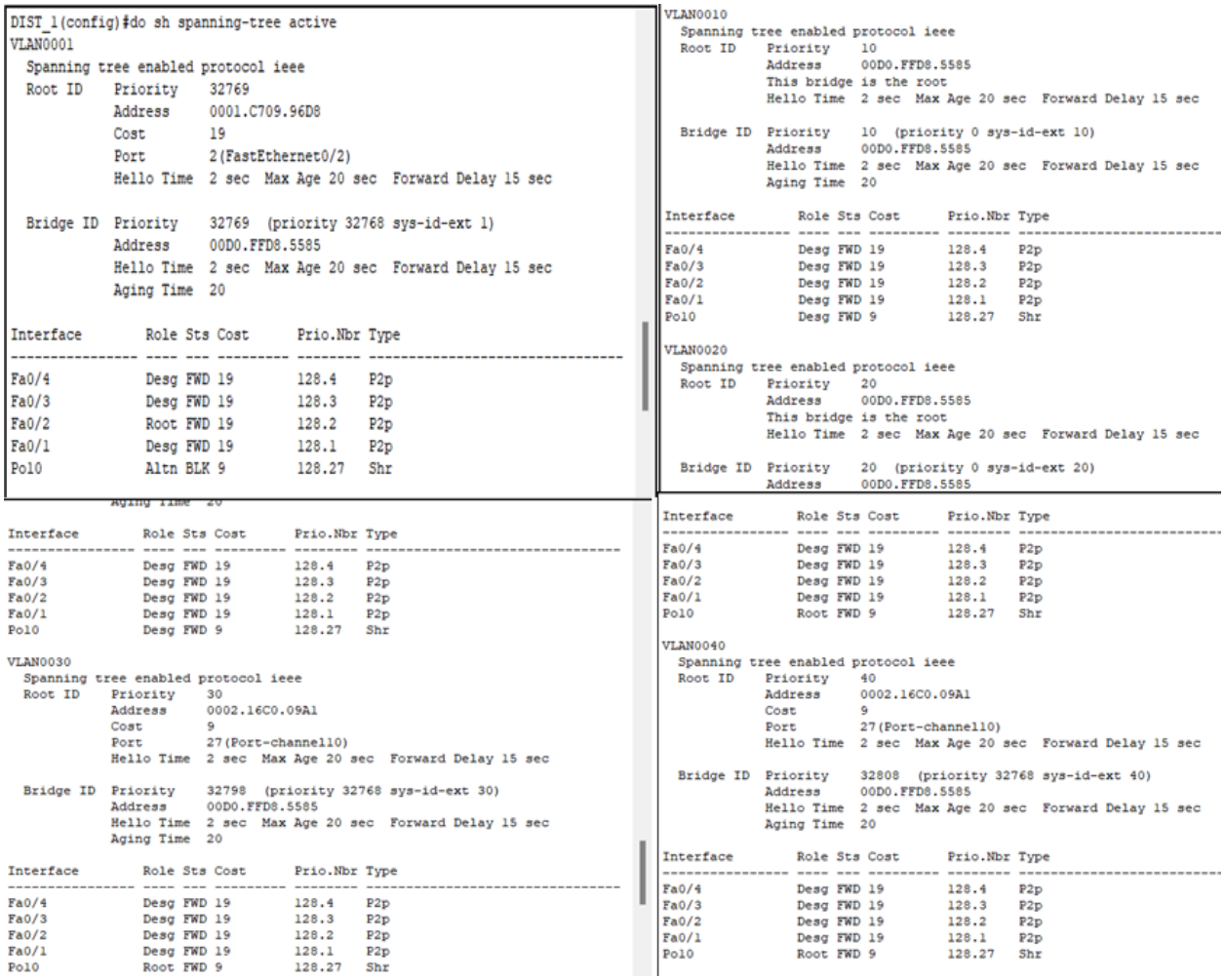


Figure 5 ; spanning-tree protocols on all VPNs

DHCP snooping

DHCP snooping verifies and filters DHCP communications. This protocol prevent DHCP from automatically assigning IP to foreign users. Additionally, this connects the database and stores data on untrusted devices with leased IP addresses. The DORA procedure is followed by DHCP snooping.

```
SW_2(config-if)#do sh ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN
Interface
------------------  ---------------  ----------  -------------  ----
----------------
00:02:16:E8:80:87   192.168.55.12    0           dhcp-snooping  20
FastEthernet0/1
00:01:96:88:B8:5A   192.168.55.14    0           dhcp-snooping  20
FastEthernet0/2
Total number of bindings: 2
SW_2(config-if)#
```

Figure 6 ; DHCP snooping in vlan 20

Access Control List (ACL)

ACLs consist tables that direct the access rights for addresses for internet services. Network interfaces, operating systems like Linux and Windows NT, and Windows Active Directory all provide ACL support. Access control lists are primarily used to protect corporate assets both internally and outside. ACLs may enhance a company's network's performance and manageability in addition to its security. In this Edge_2 router the access is not restricted for any of the addresses and access is to given any IP address of any subnet masks.

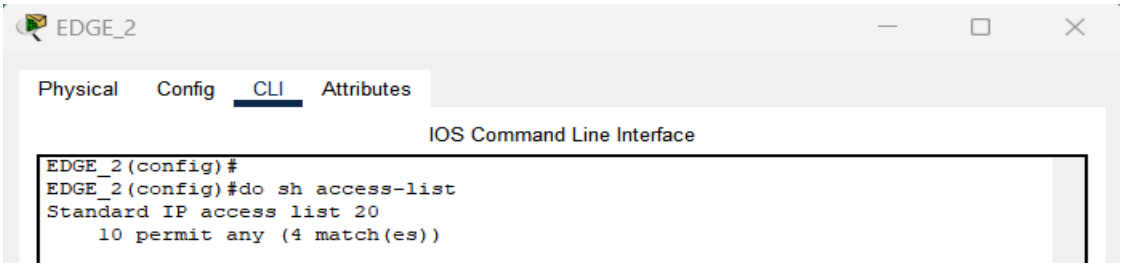


Figure 7 ; configuration of Access-list

FHRP – (First Hop redundancy Protocol)

The process of using backup devices and links is known as redundancy. When 2 devices are inter-connected using a singular link type. And if the link fails the whole systems connection fails as a result another backup link are addressed which acts as backup link. Redundant links are supplementary connections. In certain terms, a duplicate connection serves as a fallback in case the primary link fails. Similar to a backup device, a redundant technology is utilized in case the primary device fails. Redundancy is the use of backup hardware and connections. This is a standby protocol which comes in play if and only if the primary link goes down.

HSRP – (Hot stand by routing protocol)

A Cisco-exclusive redundancy mechanism called the Hot Standby Router Protocol (HSRP) is used to offer redundancy for a network's default gateway. In the case of a router or link failure, HSRP offers automatic failover. In this routing protocol bunches of secondary gateway IP is assigned for multiple VLANs as shown in the figure below (0., 2022)

```
Username: nischal
Password:

DIST_1>
DIST_1>en
Password:
Password:
DIST_1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
DIST_1(config)#
DIST_1(config)#
DIST_1(config)#do sh standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
Vl10        10   110 P Standby  192.168.55.2    local           192.168.55.3
Vl20        20   110 P Standby  192.168.55.10   local           192.168.55.11
Vl30        30   110 P Standby  192.168.55.18   local           192.168.55.19
Vl40        40   110 P Standby  192.168.55.26   local           192.168.55.27
DIST_1(config)#
```

Figure 8 ; HSRP on all Vlan 10, 20, 30 and 40

Ether-Channel LACP and PAGP

In multiple enterprises, there are only single link through which all the traffic are advanced. Due to which user get experience high latency and slow availability of internet. So to overcome such hurdles a port link aggregation technology is used called Ether-channel. It also goes by the name Link Aggregation. It offers fast, fault-tolerant connections and also constantly operated in backbone networks. This uses two protocol called LACP and PAGP. Both of these protocol are cisco proprietary and both of them is used in "network-solution's" network. (stone, 2020)

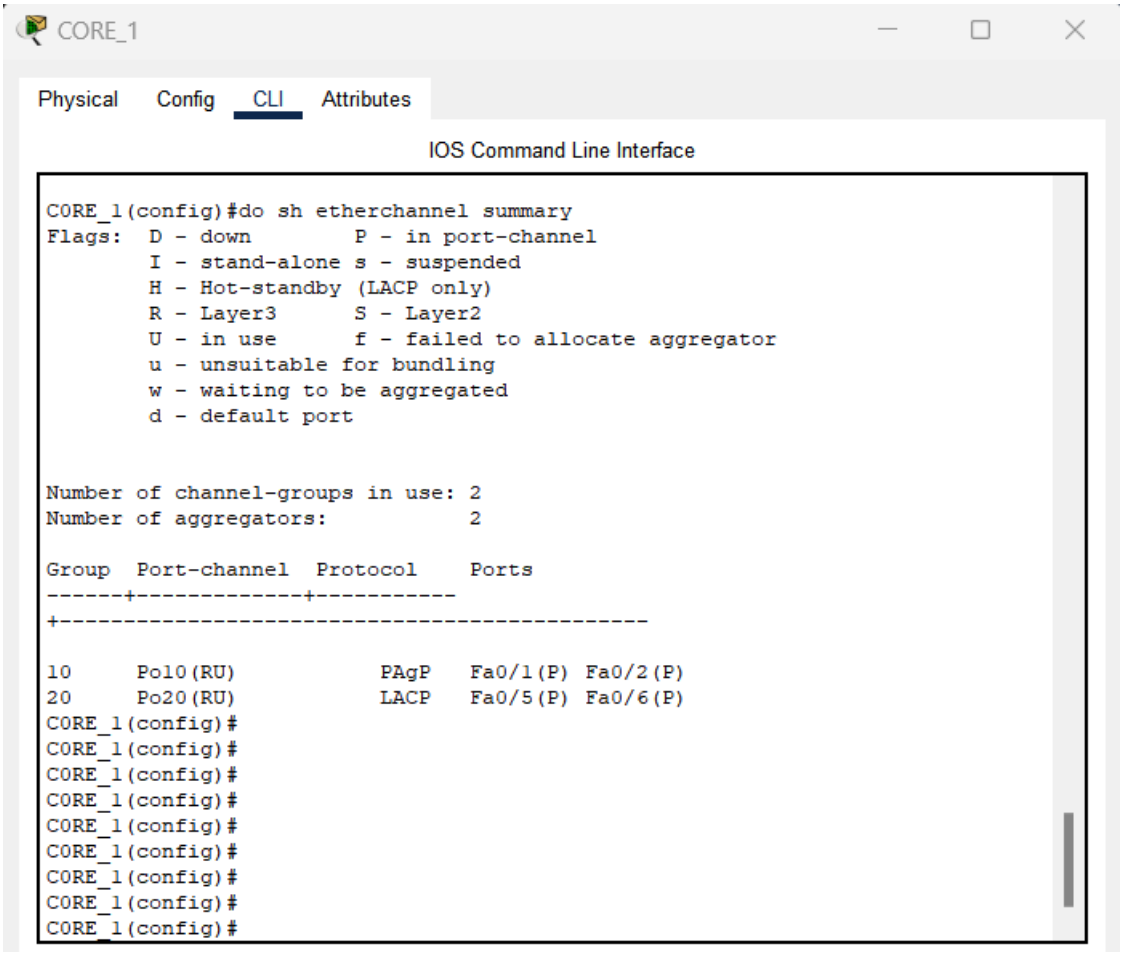


Figure 9 ; Ether-channel summary

LACP (Link aggregation protocol) and PAgP (Port aggregation protocol)

The Port Aggregation Protocol (PAgP) of Cisco is an Ether Channel technology.

In this sort of data/traffic load balancing, Cisco Ethernet switch ports are logically aggregated.

Up to eight physical lines can be combined into one virtual link using a PAgP EtherChannel.

An EtherChannel is created using the IEEE standard known as Link Aggregation Control Protocol, which was first introduced in 802.3ad. The Cisco PAgP and this protocol are essentially identical. You may set your interface in a variety of modes.

Routing protocols

The routing protocols configured in network-solution in Kathmandu and branch of dhading with ISPs are listed below:

BGP (Border gateway protocol)

Border Gateway Protocol (BGP) is a gateway protocol which allows internet to interchange routing information between autonomous systems (AS). In this network BGP is configured in external ISP network unique autonomous system (AS) has been implemented to the internet.

As number is give 10, 20, 30, 40, 50, 60, 70 and 80 to EDGE_1, EDGE_2, and ISP 1, 2, 3, 4 and 5 respectively.

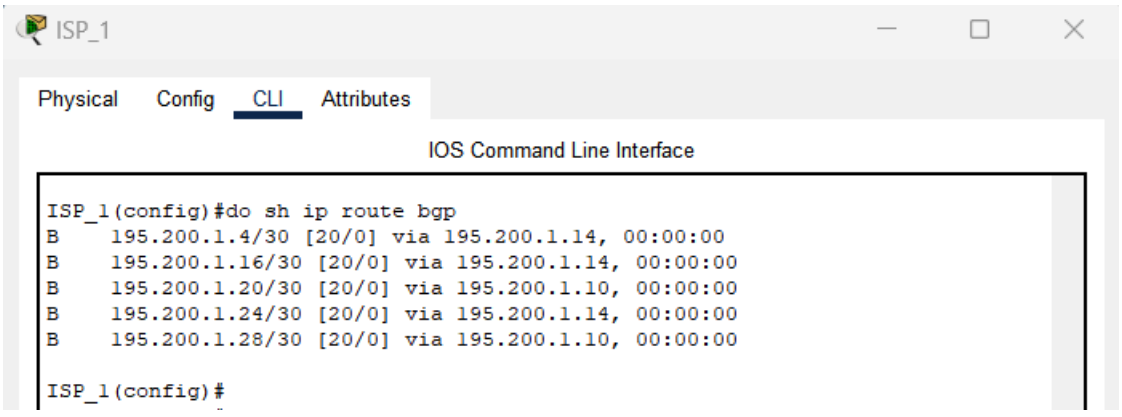


Figure 10 ; routing protocol BGP configuration

OSPF – (Open short path first)

The OSPF is a link-state routing system that selects the most advantageous route to the intended destination network using three tables.

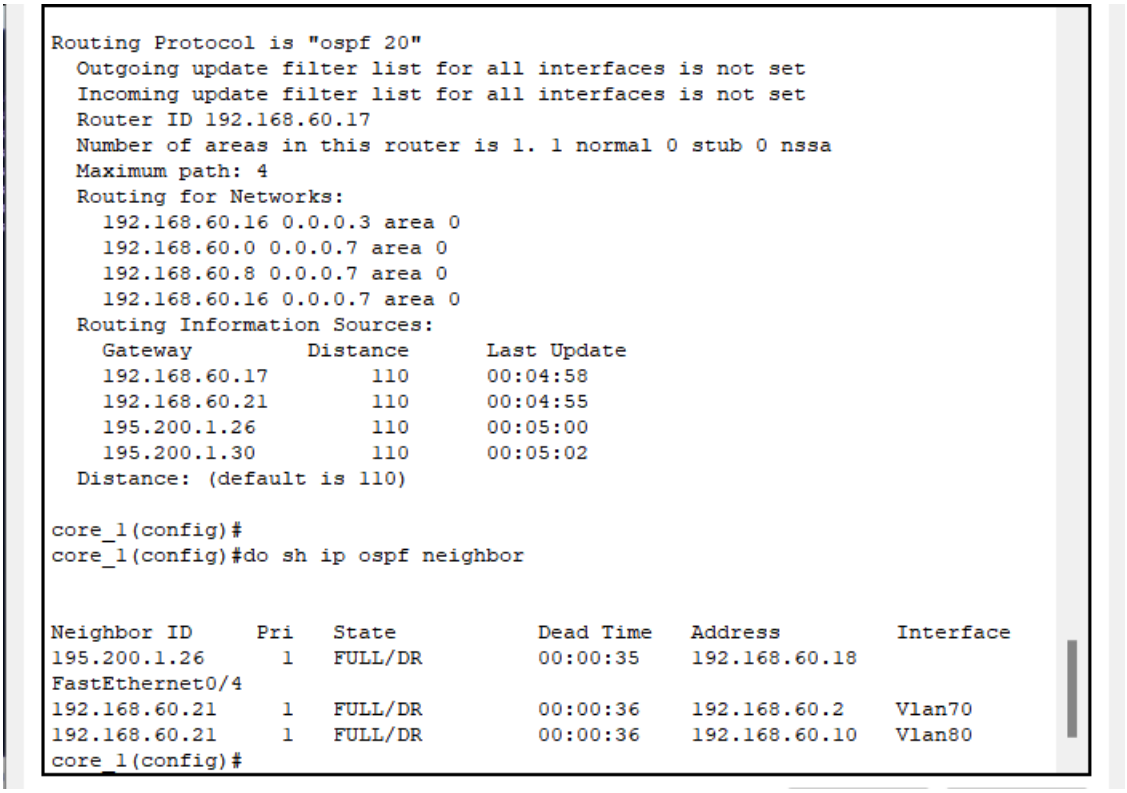
• The first table includes information on neighbors who are closely related to one another.

• The whole network topology is handled by the second table.

• Data about the actual path is kept in the third table.

The server room router employs the OSPF routing protocol.

This is loop-free and can quickly update the whole network system with routing information.



```
Routing Protocol is "ospf 20"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 192.168.60.17
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    192.168.60.16 0.0.0.3 area 0
    192.168.60.0 0.0.0.7 area 0
    192.168.60.8 0.0.0.7 area 0
    192.168.60.16 0.0.0.7 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    192.168.60.17         110      00:04:58
    192.168.60.21         110      00:04:55
    195.200.1.26          110      00:05:00
    195.200.1.30          110      00:05:02
  Distance: (default is 110)

core_1(config)#
core_1(config)#do sh ip ospf neighbor


Neighbor ID     Pri   State           Dead Time   Address         Interface
195.200.1.26      1   FULL/DR         00:00:35    192.168.60.18
FastEthernet0/4
192.168.60.21     1   FULL/DR         00:00:36    192.168.60.2    Vlan70
192.168.60.21     1   FULL/DR         00:00:36    192.168.60.10   Vlan80
core_1(config)#
```

Figure 11 ; routing protocol OSPF configuration

EIGRP - (Enhanced Interior Gateway Routing Protocol)

EIGRP is a hybrid routing protocol that compares pathways from both the link-state protocol and the distance vector protocol in order to discover the quickest route to a given location.

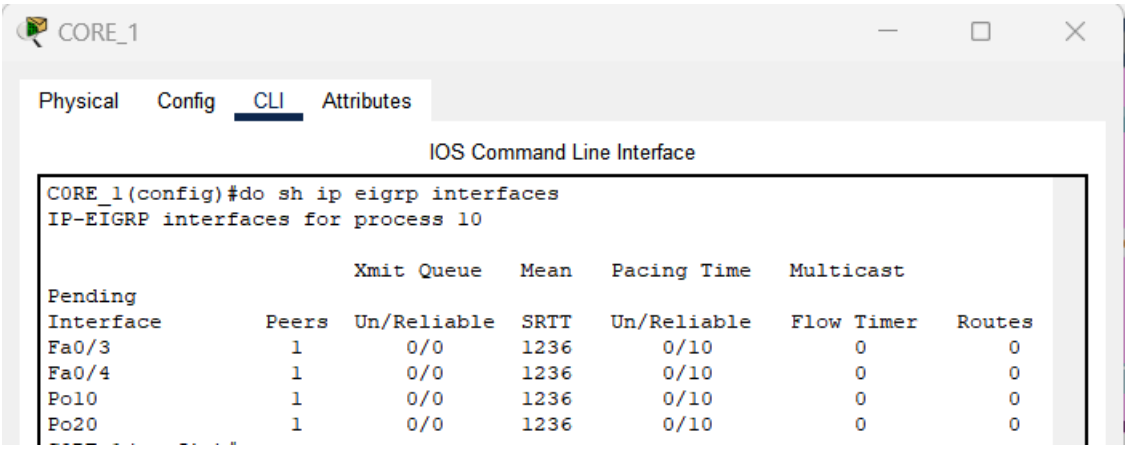


Figure 12 ; EIGRP interfaces

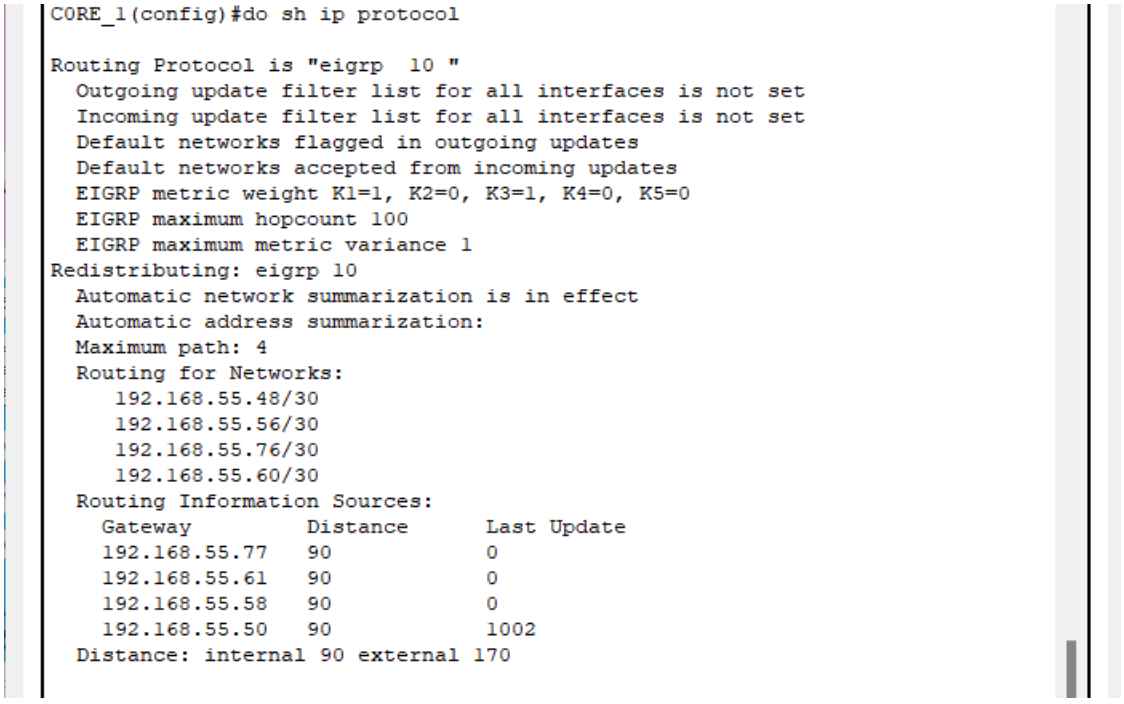


Figure 13 ; EIGRP information in edge router

User-exec

This is used for the configuration of security in all switches and routers. This enables a login authentication for entering terminal. Username and password is required to be able to perform any kind of commands.

Figure 14 ; User exec

Wireless LAN Controller

In multiple huge corporation each and every devices are not cabled and new and modern technologies are advanced to wireless connection. Devices like mobile phones, tablet and laptops preferably support Wi-Fi connections. Thus to maintain Wireless network. WLAN, with LAN controller and light weight access point is configured. The topology of WLAN is accessed to the all end users and wireless devices.

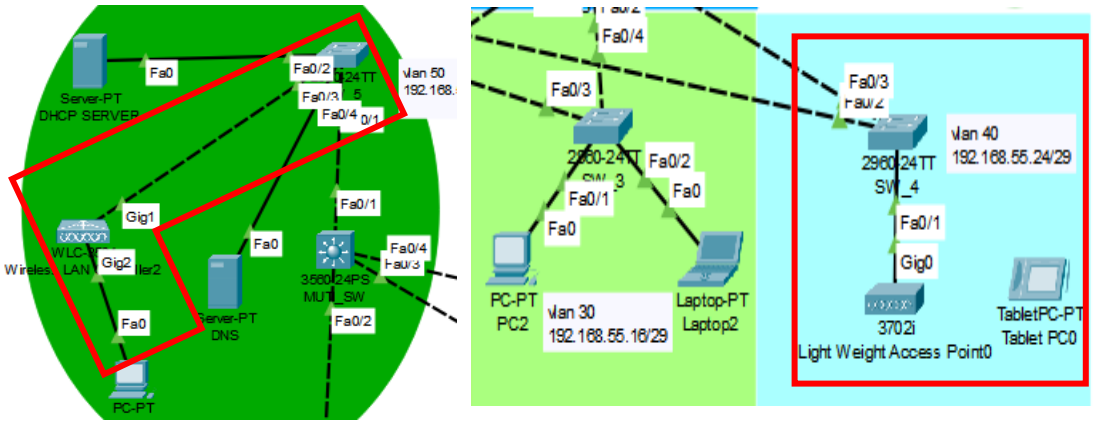


Figure 15 ; wireless configuration i. WLAN ii.wireless APs

The access point is directly linked to a vlan switch (AP). Where the trunk native command has been applied and a WLC has been installed in the data center to monitor those AP. The AP was dynamically allocated by the data center's DHCP server. One SSID is set up as seen in the diagram.

This is cisco wireless LAN controller. A user interface is created with username Nischal and password accordingly.

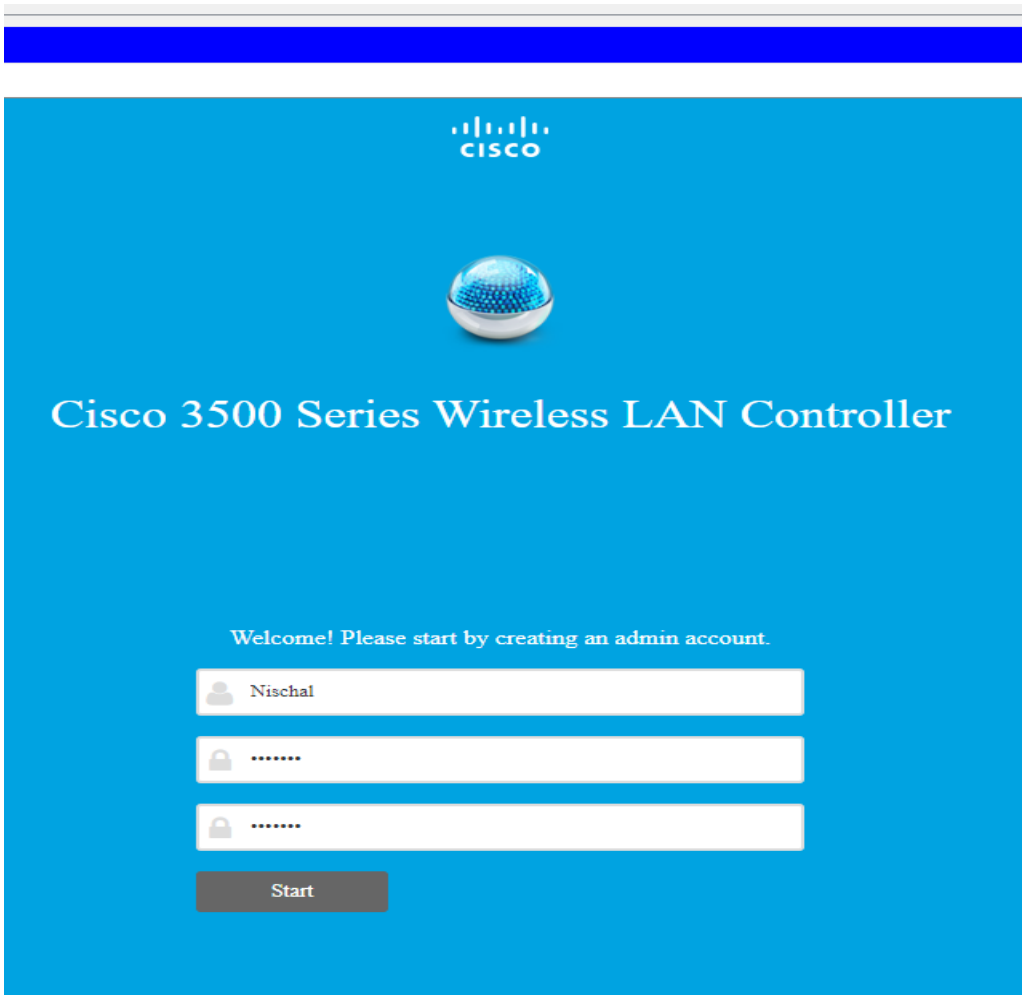


Figure 16 ; Login page for WLAN configuration

Setting up controller and creating the wireless network with configuration.

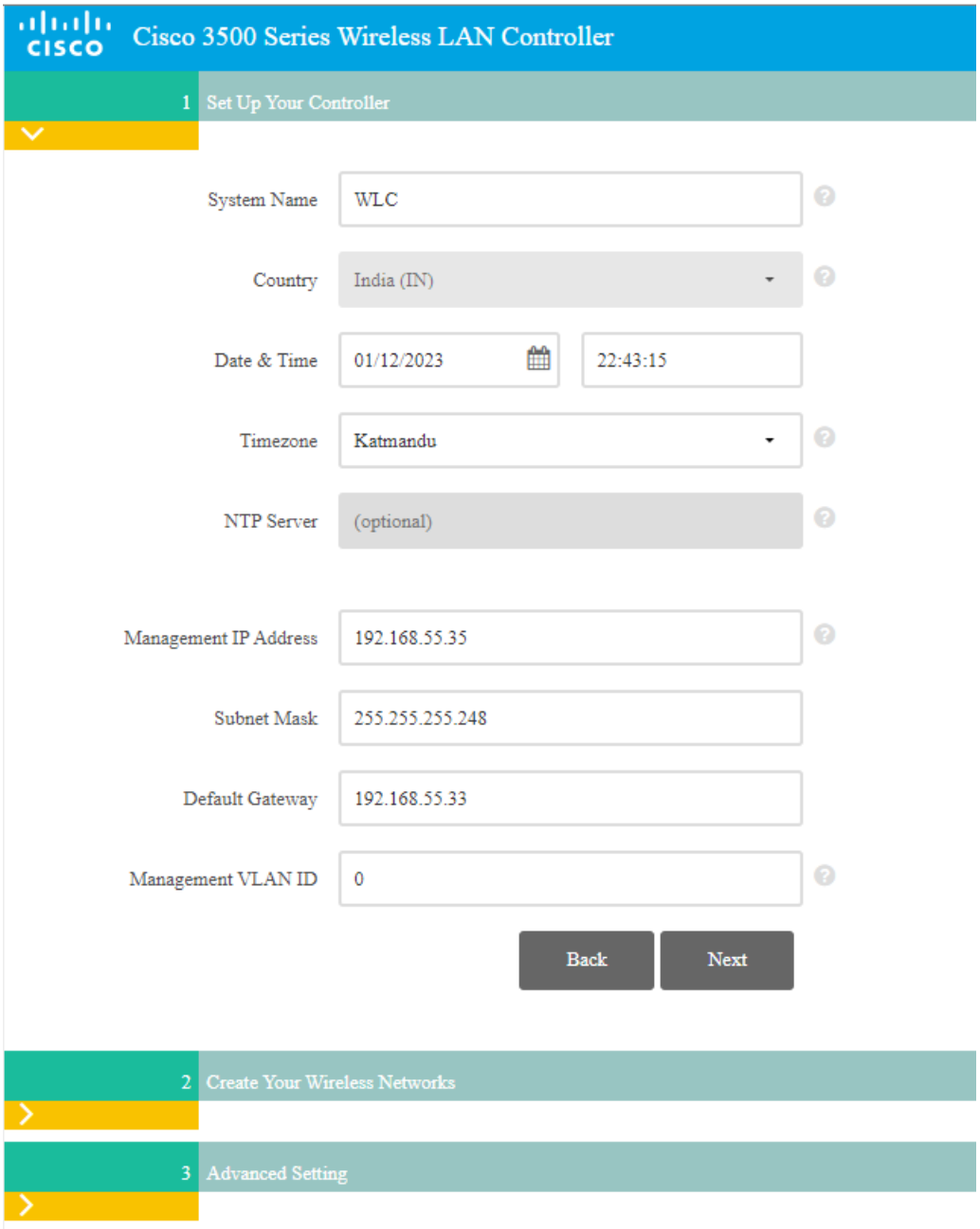


Figure 17 ; wireless LAN controller

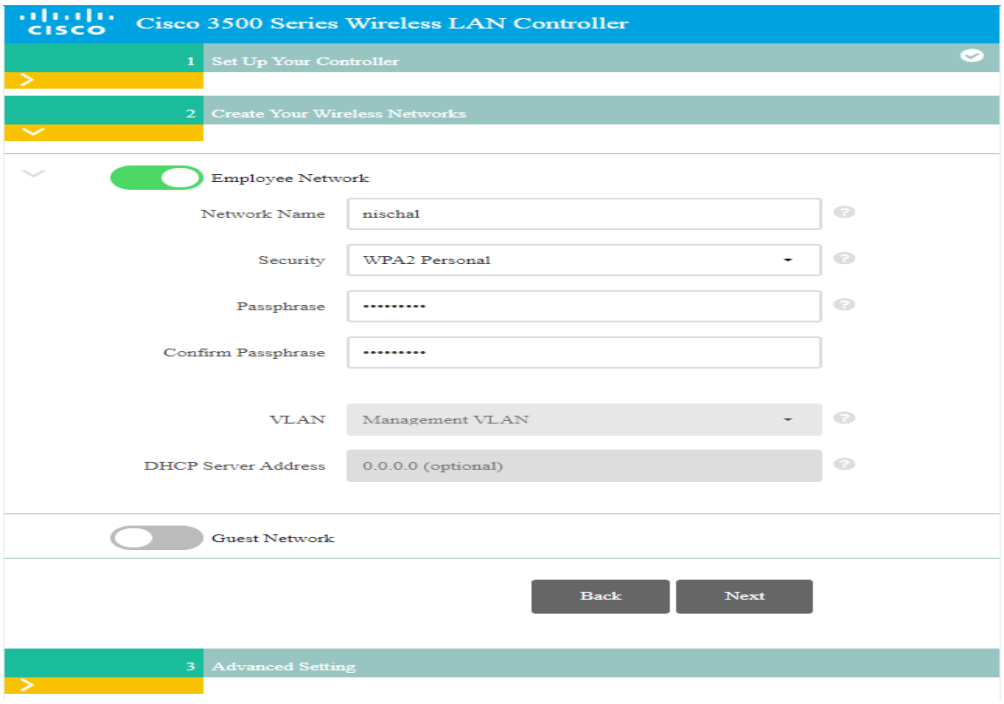


Figure 18 ; wireless LAN controller

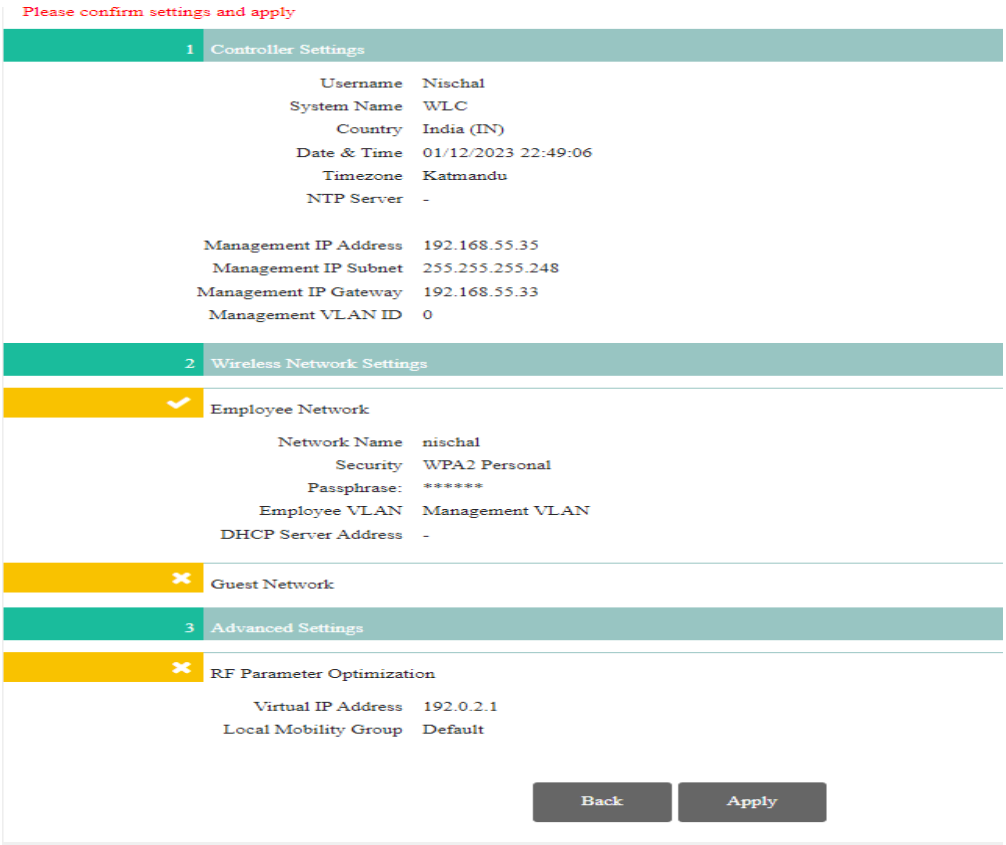


Figure 19 ; wireless LAN controller

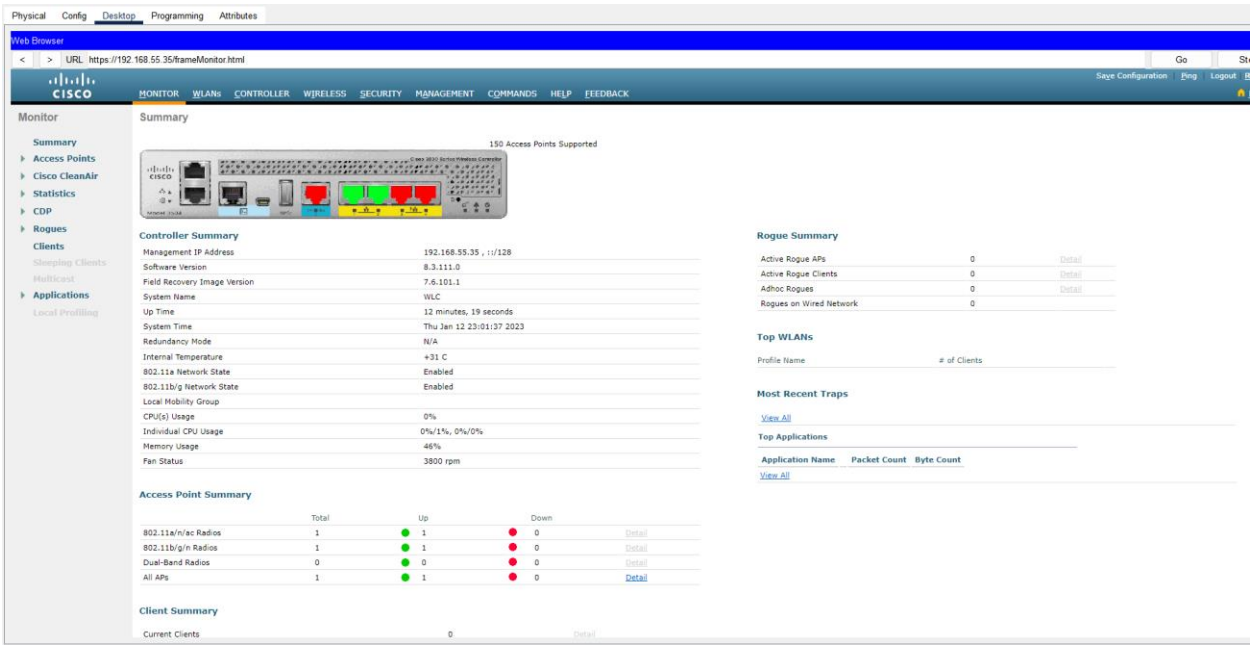


Figure 20 ; wireless LAN controller

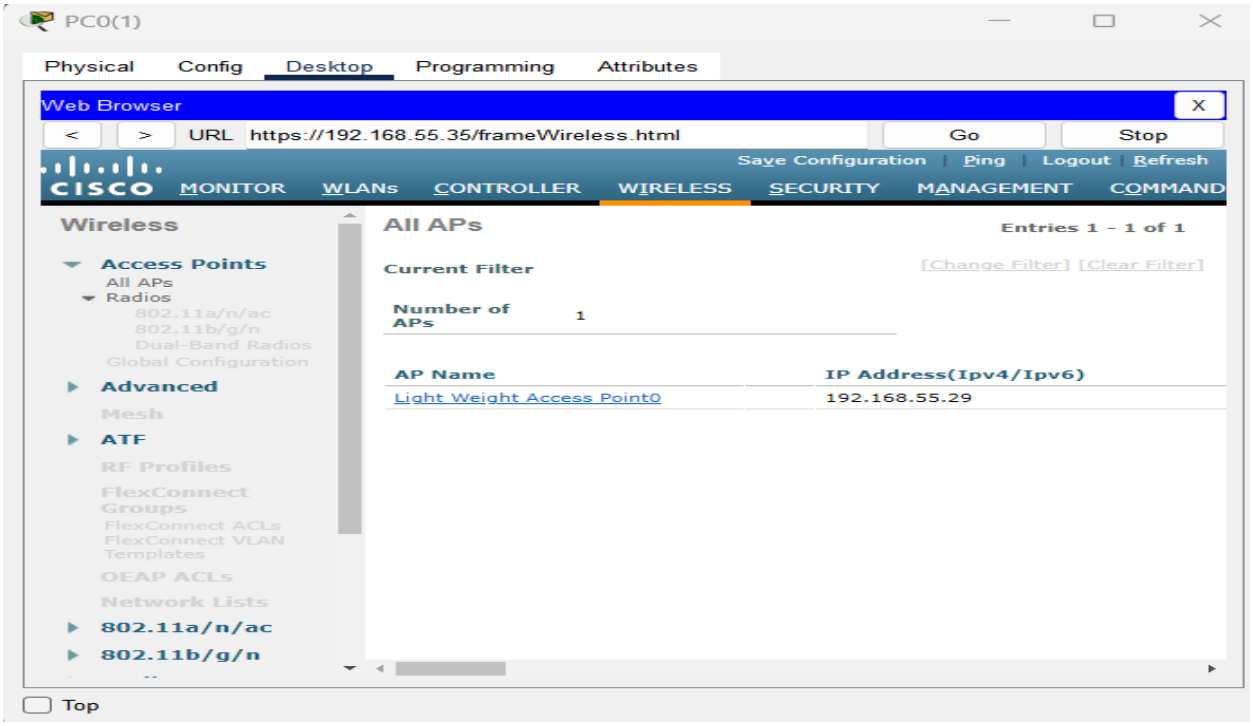


Figure 21 ; wireless LAN controller

Network Address Translation (NAT)

During the process of packet transferring the device uses public addressing method so that it is aware of the client and can reply appropriately. Before sending data, numerous local addresses are transformed into public address in nating. The Edge router has the NAT configured.

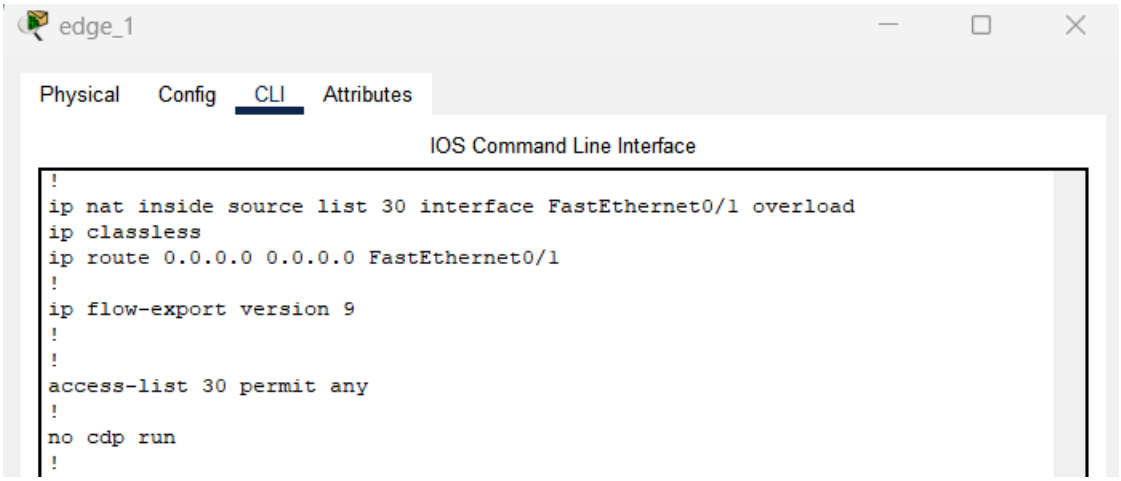


Figure 22 ; NATING on router EDGE_1

Firewall

When attackers infiltrate with miscellaneous network traffic, firewalls guard your computer or network from outside cyberattacks. Furthermore, it act as a protection form malwares linking to a device or its network through the internet. Firewalls can be set up to permit relevant and essential data through while blocking data from specific places (i.e., computer network addresses), programs, or ports. (For further detail, see Understanding Denial-of-Service Attacks.)

A firewall is configured in another network different form the network-solution. Two inside and outside network are as shown in the diagram. (Greene, 2018)

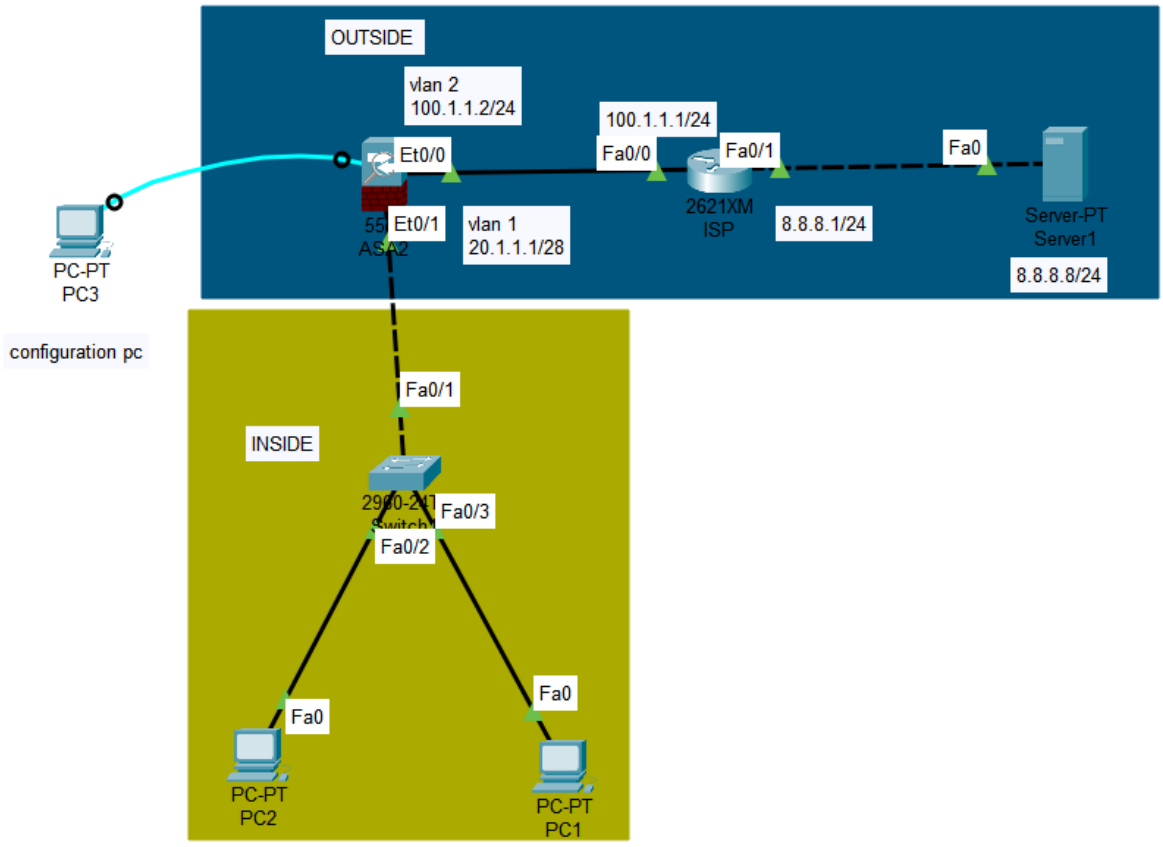


Figure 23 ; FIREWALL configuration with different network

Server and services

DHCP - (Dynamic Host Configuration Protocol)

In DHCP, a connection is established by exchanging most of eight DHCP messages between client and server, also called DORA. While DNS assists in gaining access to internet resources by translating hostnames into IP, non-operating ports are blocked by DHCP and devices get their IP through dhcp. The setting up and testing of DHCP. (Gilbert, 2023)

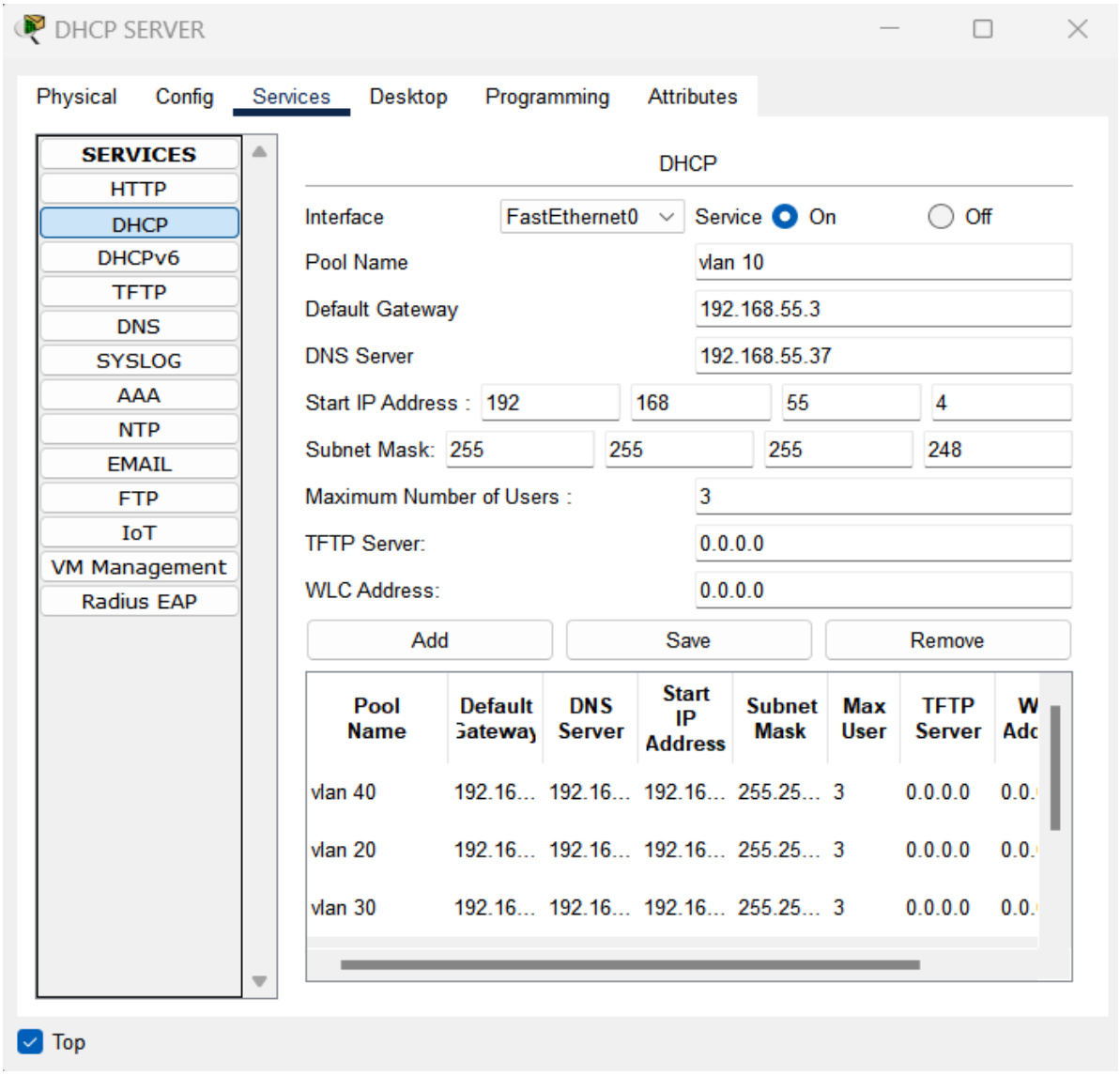


Figure 24 ; DHCP server configuration

DHCP client and relay

Discovery, offer, request, and acknowledgement are all part of DHCP, which is a client-server protocol. Server port 67 is used by the server, and client port 68 is used by the client. This protocol utilizes UDP services for client-server communication. Various IP addresses are available from a pool of addresses. The DHCP relay agent assists in transferring configuration data to the client's device as well as distributing DHCP packets between clients and servers. The DHCP client sends DHCP server signals using UDP protocol broadcasts. A DHCP client and relay verification:

```
interface Vlan10
 mac-address 00d0.ffd8.5501
 ip address 192.168.55.1 255.255.255.248
 ip helper-address 192.168.55.34
 ip helper-address 192.168.55.74
 standby 10 ip 192.168.55.3
 standby 10 priority 110
 standby 10 preempt
!
interface Vlan20
 mac-address 00d0.ffd8.5502
 ip address 192.168.55.9 255.255.255.248
 ip helper-address 192.168.55.34
 ip helper-address 192.168.55.74
 standby 20 ip 192.168.55.11
 standby 20 priority 110
 standby 20 preempt
!
interface Vlan30
 mac-address 00d0.ffd8.5503
 ip address 192.168.55.17 255.255.255.248
 ip helper-address 192.168.55.34
 ip helper-address 192.168.55.74
 standby 30 ip 192.168.55.19
 standby 30 priority 110
 standby 30 preempt
!
interface Vlan40
 mac-address 00d0.ffd8.5504
 ip address 192.168.55.25 255.255.255.248
 ip helper-address 192.168.55.34
 ip helper-address 192.168.55.74
 standby 40 ip 192.168.55.27
 standby 40 priority 110
 standby 40 preempt
!
```

Figure 25 ; DHCP client and relay

Domain Name Server (DNS)

It relates to the network-solution company's domain name server, which converts a domain name to an IP address. The name "instagram.com" has been set up in DNS as the official website of the network-solutions firm, where any future company-related updates would be made. Every department user has access to the DNS server, which has been assigned to the data center.

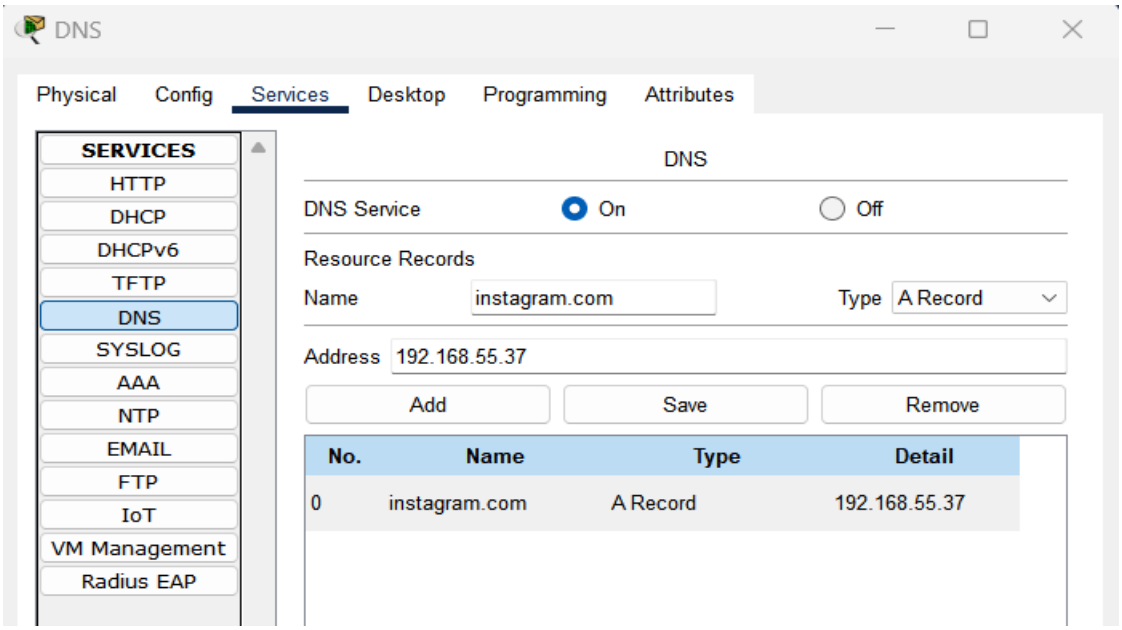


Figure 26 ; configuration of DNS server

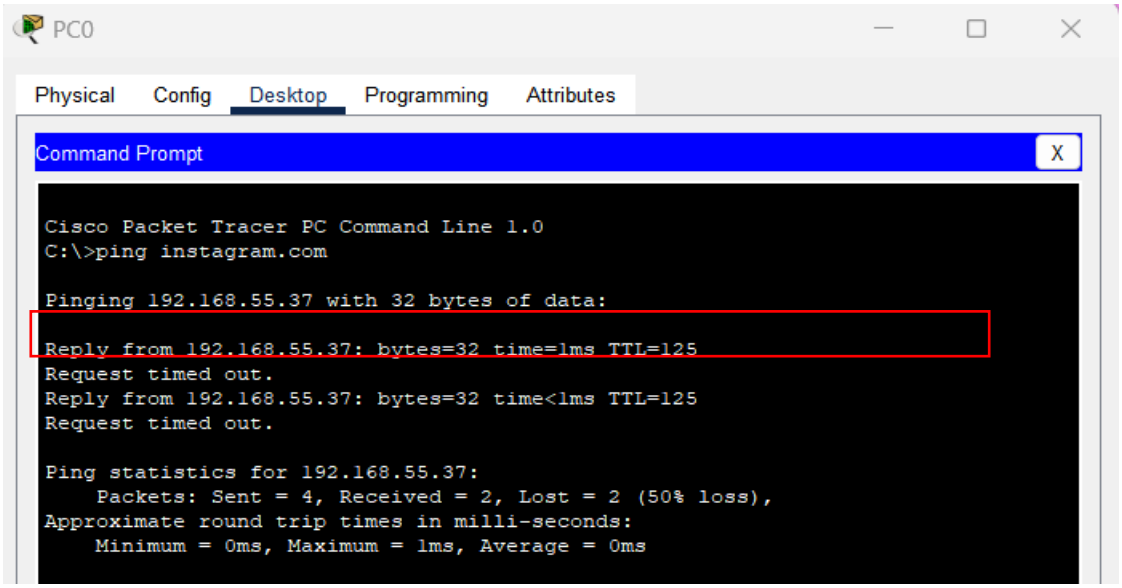


Figure 27 ; configuration of DNS server

SYSLOG server

All of the logging details are forwarded by SYSLOG server to one centralized place. The log information can be searched, managed, and archived from this location. Since the Syslog protocol is supported by many devices, you can use it to log a wide variety of events, including web server, router, etc.

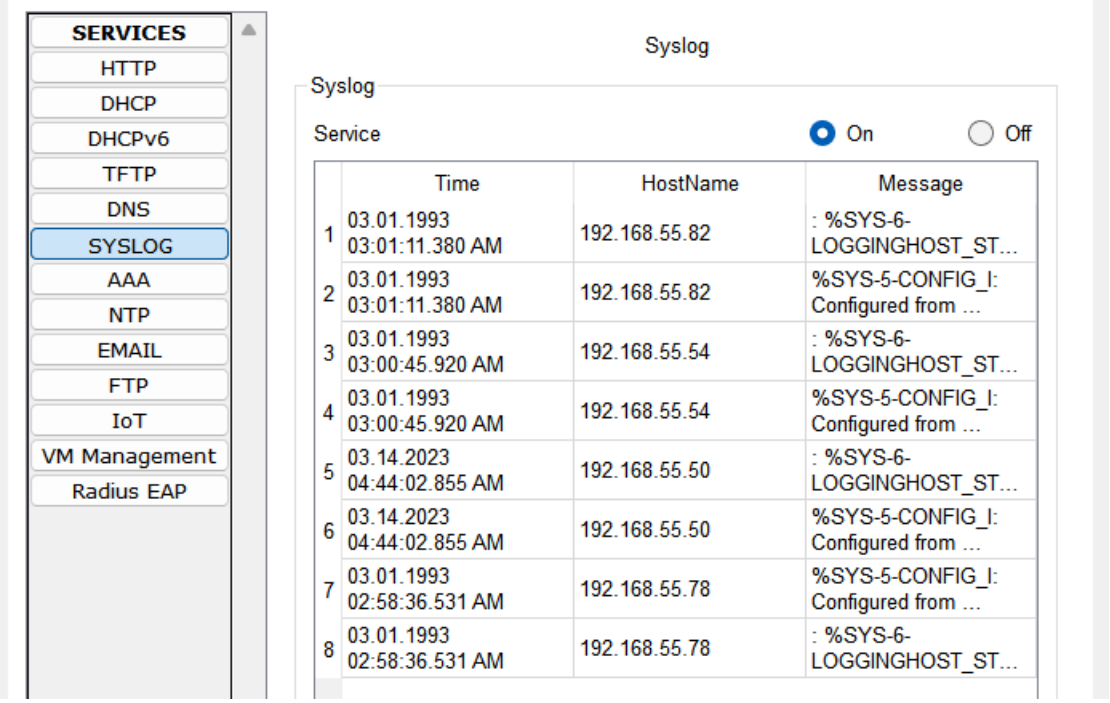


Figure 28 ; SYSLOG information in server

Figure 29 ; syslog implementation in EDGE_2 router

Network Time Protocol (NTP)

Hundreds of thousands of computers and other devices clocks are synchronized with the help pf NTP using internet services. It helps to organize the time by synchronizing time with the present. [(*Configuring NTP*, 2022)]

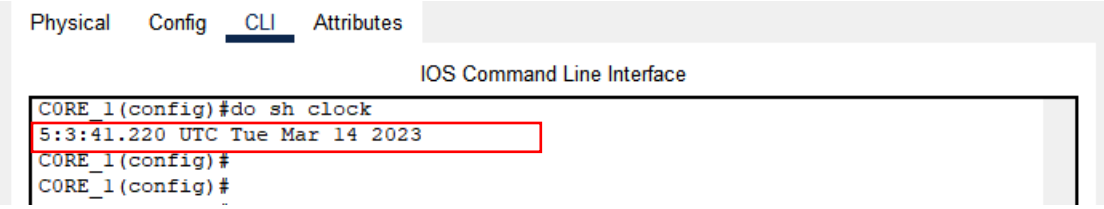


Figure 30 ; NTP configuration in DIST_1 layer

BANNER

A banners in Cisco connectivity is a message or picture that appears when a user connects to a router or switch, for example. Important information or cautions, including security guidelines or login instructions, might be shown in the banner. Additionally, a company's logo or other promotional materials can be shown on the banner.

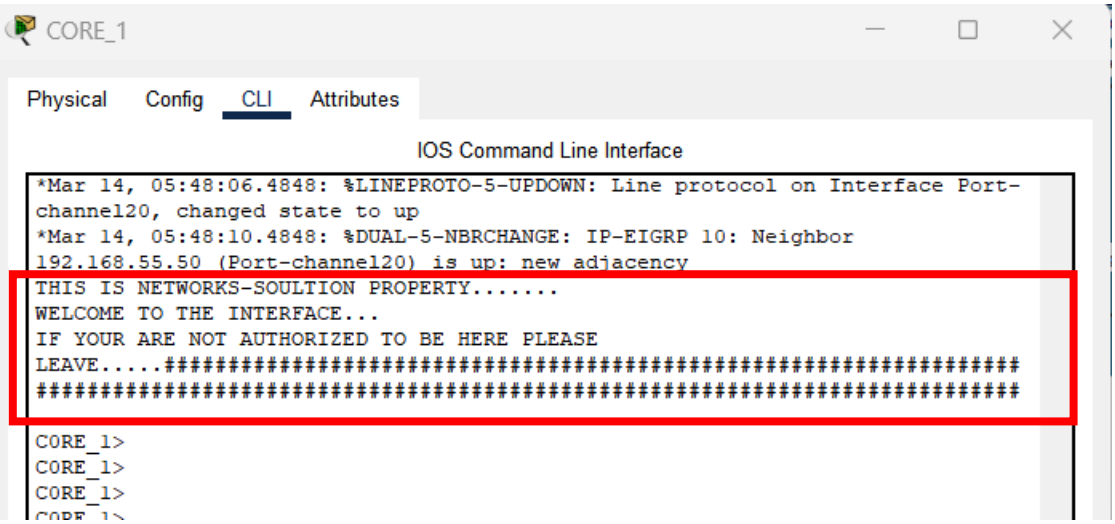


Figure 31 ; applying banner in router

AAA authentication server

In an IP-based network, authentication, authorization, and accounting systems are used to keep track of user behavior and control access to network resources. A dedicated server is often used for AAA. I have allowed AAA authentication in SW_2 of VLAN20. AAA server is configured and username and password is created accordingly. For greater security enabled password is added. (*What is AAA (Authentication, Authorization, and Accounting)?*, no date)

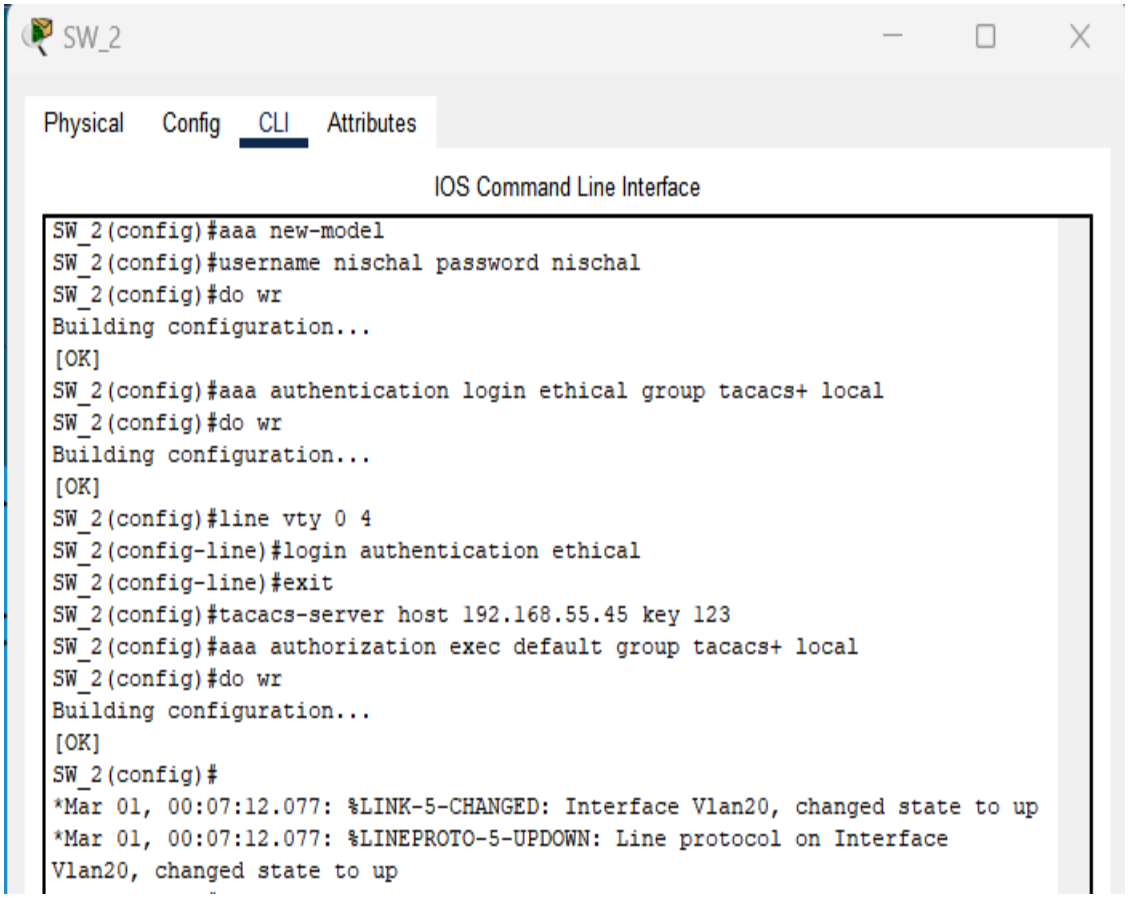


Figure 32 ; implementation of AAA authentication

```
C:\>telnet 192.168.55.12
Trying 192.168.55.12 ...Open


User Access Verification

Username: nischal
Password:
SW_2>
SW_2>
SW_2>do sh run
       ^
% Invalid input detected at '^' marker.

SW_2>en
Password:
SW_2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW_2(config)#do sh run
Building configuration...

Current configuration : 1699 bytes
!
version 15.0
service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname SW_2
!
enable password 123
!
```

Figure 33 ; telent for accessing the interface

Virtual Private Network (VPN)

Security and connectivity are enhanced by VPNs (Virtual Private Networks). Through these technologies, you can securely connect to a private network over a public network, like the internet. Data transferred over the network is protected by VPNs using encryption, making it harder for attackers and other such unwanted outsiders to interrupt and access the data. (v., 2017)

```
crypto isakmp policy 100
 encr 3des
 hash md5
 authentication pre-share
 group 5
!
crypto isakmp key nischal address 195.200.1.26
!
!
!
crypto ipsec transform-set nischal esp-3des esp-md5-hmac
!
crypto map nischal 10 ipsec-isakmp
 set peer 195.200.1.26
 set transform-set nischal
 match address 101
!
!
!
!
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface FastEthernet0/0
 ip address 195.200.1.5 255.255.255.252
 ip nat outside
 duplex auto
 speed auto
 crypto map nischal
!
```

Figure 34 ; vpn configuration on EDGE_2

```
crypto isakmp policy 100
 encr 3des
 hash md5
 authentication pre-share
 group 5
!
crypto isakmp key nischal address 195.200.1.5
!
!
!
crypto ipsec transform-set nischal esp-3des esp-md5-hmac
!
crypto map nischal 10 ipsec-isakmp
 set peer 195.200.1.5
 set transform-set nischal
 match address 102
!
!
!
!
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface FastEthernet0/0
 ip address 192.168.60.18 255.255.255.252
 ip nat inside
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 195.200.1.26 255.255.255.252
 ip nat outside
 duplex auto
 speed auto
 crypto map nischal
```

Figure 35 ; vpn configuration on edge_1

Network risk management

When it comes to network security, a company must take action that will aid in thwarting an intruder. A company must have a plan for monitoring, following up on, and mitigating security concerns. Notable study shows that hackers cause $445 billion in damages each year throughout the globe. Due to internet weaknesses, people try various techniques to get access to it, which results in the theft of information and money. Staff members granting access, stolen gadgets, and systems of other companies within the supply chain are the typical ways to gain access. (Kin Ly, no date)

The techniques used by criminals to engage in illicit activity are the same. "Risk equals Threat multiplied by Vulnerability" is a formula for calculating risk. The goal of network risk management is to categorize, evaluate, and manage risks for safeguarding business.

There are several ways to mitigate risk management in network security, including:

- **Firewall**

The primary function of a firewall is to block unauthorized access to a network while allowing authorized communications. There are several types of firewalls, including packet filtering firewalls, circuit-level gateways, application-level gateways (proxy firewalls), and stately inspection firewalls. Packet filtering firewalls operate at the network layer of the OSI model and use access control lists (ACLs) to filter traffic based on IP addresses, ports, and other network-layer information.

- **Backup system**

The changes might be made by an organization's employee or by Access and changes could be made by an outsider. An error occurs or a backdoor is created in the network as a result of these factors. Backups enable automatic backups of data, databases, applications, and operating systems. To mitigate such unauthorized or misconfiguration, it restores data immediately and also be used to recover files.

- **Missing patches**

Computer and security patch updates must be implemented on a regular basis in a company. Checking crucial files during periodic patch updates for unauthorized modifications will assist to reduce the chance of missing fixes. The policy of a company should serve as controlling IT and staff initiative to reduce risks. Cardholder data is sensitive, and employees must be aware of their duties to secure it.

- **Authentication**

A secure password is required, as is two-factor authentication. Configured passwords must be encrypted using various techniques and give the necessary authentication and characteristics. Monitoring password attempts and tracing IP addresses will aid in problem resolution.

It's crucial to remember that risk management is a continuous process, and that in order to maintain security measures up to date and effective against the changing threat landscape, they must be constantly monitored and reviewed.

Figure 36 ; network risk management

Implementation of risk management

- **Mapping of your network**

To manage your risk, you must first understand where it is. Identify the resources in the networks which may be attacked by cyber thieves first. This implies you'll have to describe your network, which may be challenging if it's a jumble of cloud computing, for example. You'll want to know which portions of your network hackers could wish to attack, which are most vulnerable, and which may not be safe at all.

- **Identification of network risk**

After you've discovered your network's weak points, you'll need to determine the threats that might damage your firm. You'll want to look at both external threats, such as assaults and breaches, and internal risks, such as improperly setup infrastructure and other faults that might let bad actors in. Part of evaluating risk is looking at present and emerging dangers – cyber thieves are frequently one point further of protection, therefore you should expect risks to evolve and commit to a risk monitoring strategy. You should also consider the hazards you've experienced in the past, since this will provide some information into the present risks. Previous assaults can also reveal how attackers entered company systems in the past.

- **Possible threats**

Once you've identified the hazards, it's important to prepare beforehand. What will your team's response be if your network is attacked? How fast will you be able to detect the attack? Having backup systems, such that compromised sections of the networks may be quickly replaced with other systems, or being able to quickly change credentials to shut out attackers, are two approaches to prepare for an attack. Having a strategy in place and making decisions ahead of time is an important aspect of risk mitigation - the Ponemon Institute found that planning for an attack is one of the greatest ways to lower the cost of one. The average time to control a breach is 279 days — in that time attacker can impels a lot of harm. However, if company has a strategy, you will be able to spot the breach and respond promptly.

Conclusion

The network is easy for using, efficient, and expandable. Long - term basis, there won't be a problem. However, the client must promptly upgrade their system to protect themselves against zero-day assaults. In order to prevent data modification or change, only authorized personnel should use the computers in the IT department. Each switch is linked to a different network using HSRP to strengthen and improve the network's accuracy. This implies that if one network is down due to a problem, another network will function as a backup to get you where you need to go. This made our client happier in the end.

.

Reference

0., O. (2022) *What is HSRP ? Explained with Examples*. Available at: https://www.orbit-computer-solutions.com/the-host-standdby-routing-protocol-hsrp-explained/.

Configuring NTP (2022). Available at: https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/6-x/system_management/configuration/guide/b_Cisco_Nexus_9000_Series_NX-OS_System_Management_Configuration_Guide/sm_3ntp.html.

Gilbert, B. (2023) *What Is DHCP – Overview of IP Address Assignment*. Available at: https://www.whatismyip.com/dhcp/.

Greene, L. (2018) *Fire Walls*. Available at: https://idighardware.com/2014/03/fire-walls/.

Kin Ly, B. (no date) *Why networking in risk management is failing (and a new model to try)*. Available at: https://www.riskleadershipnetwork.com/insights/why-networking-in-risk-management-is-failing-new-model-to-try.

stone, G. (2020) *ETHERCHANNEL: LACP, PAgP, AND STATIC PROTOCOLS*. Available at: https://www.sunsetlearning.com/etherchannel-lacp-pagp-static-protocols/.

v., V. (2017) *Cisco ASA Site to Site VPN Failover How-To*. Available at: https://techstat.net/cisco-asa-policy-based-redundant-site-site-vpn-failover/.

What is AAA (Authentication, Authorization, and Accounting)? (no date). Available at: https://www.tutorialspoint.com/what-is-aaa-authentication-authorization-and-accounting.