Network Project

Design and establish an organizational network model

Yair Mor

Table Of Contents

Requirements

Design and Implement an Organizational Network Model

I was required to design and configure an organizational network model based on Cisco infrastructure according to the following requirements:

Physical Topology

1. The network will consist of three branches: a main branch and two secondary branches.
2. Each branch will have one router. (Bonus: In the main branch, two routers can be configured in high availability (HA) mode).
3. All routers will connect to an L3 switch simulating an ISP. Each router will connect to a routed port on this switch.
4. The main branch will include one (or two) access switches and two distribution switches.
5. Each secondary branch will have a single access switch connected directly to the router.
6. Each access switch will connect to one PC.
7. The network design should adhere to the above guidelines. Unspecified elements (e.g., port numbering or the number of links between switches) may be determined at my discretion.

Requirements

Logical Topology:

1. The WAN topology will be Hub-and-Spoke: Establish a GRE over IPsec tunnel between each secondary branch and the main branch.
2. Routing between branches will utilize Single Area OSPF.
3. No routing protocol will be enabled on the L3 switch representing the internet.
4. Each branch network will be divided into two VLANs: one for the IT department.
5. Per-VLAN Spanning Tree (PVST) with optimal load balancing.
6. Configure device access through SSH.
7. The network model will include LACP.
8. Each PC will receive an IP address via DHCP.
9. Where instructions are open to interpretation, I will implement as I see fit (e.g., while DHCP IP assignment is required for each endpoint, the device responsible for IP distribution has not been specified).

Security

1. Access to network device management interfaces will be restricted to the IT department only.
2. Apply the security tools and best practices covered in the course.
3. Configure each feature according to its best practices and secure configurations as taught (e.g., disabling all unused interfaces).

Automation

Present an automation tool for configuration and/or verification of at least one feature on the router

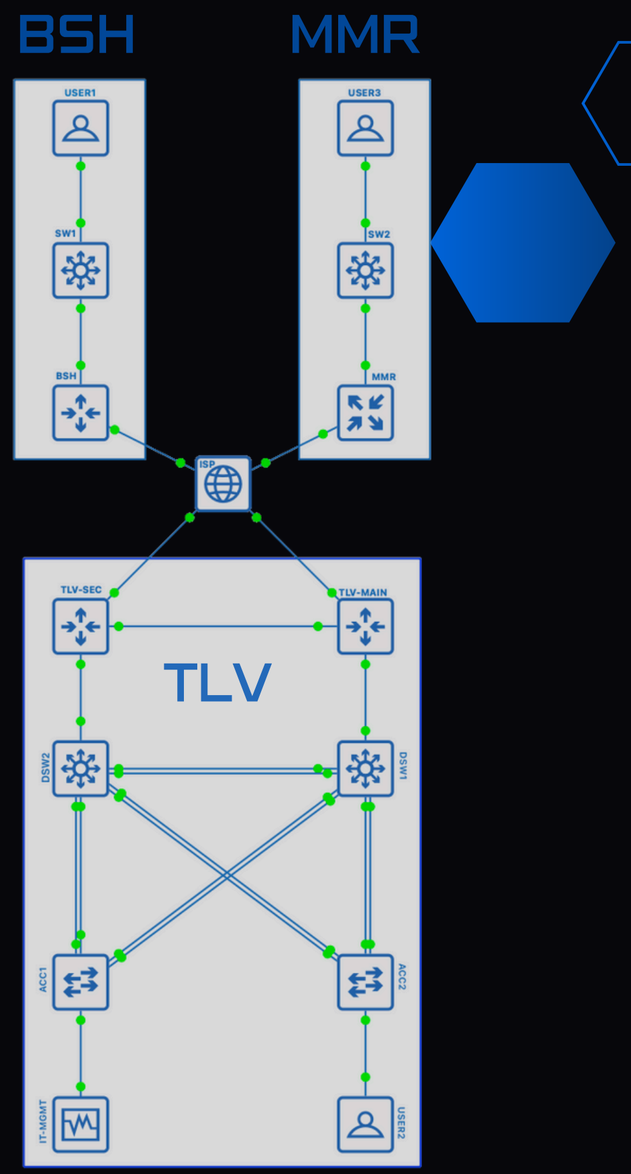
The Topology

The company's network consists of three interconnected networks across different cities, linked through a central switch simulating an ISP.
The main network uses a three-layer architecture (Access, DSW, Core) with high redundancy.
The other two networks are smaller.

Key Configurations

- I Set up VLANs for Employees, IT/Management,
  plus a Native VLAN and a Security VLAN for restricted ports.
- I Established connectivity between networks using tunnels and OSPF for dynamic routing,
  with routers connected through Loopback interfaces for stability.

by using This topology I ensured reliable communication, scalability, and strong security.



ISP			
INTERFACE	IP ADDRESS	SUBMASK	CONNECTED TO
e0/0	64.100.0.1	255.255.255.252	BSH
e1/1	64.100.0.5	255.255.255.252	TLV-Main
e2/2	64.100.0.9	255.255.255.252	TLV-Second
e3/3	64.100.0.13	255.255.255.252	MMR

TLV-Main				
INTERFACE	IP ADDRESS	SUBMASK	Connect to	VIP
e0/0	64.100.0.6	255.255.255.252	ISP	
e0/1			DSW1	
e0/1.10	10.11.10.1	255.255.255.0	VLAN 10	10.11.10.7
e0/1.20	10.11.20.1	255.255.255.0	VLAN 20	10.11.20.7
e0/1.99	10.11.99.1	255.255.255.0	VLAN 99	
e0/2	10.11.1.1	255.255.255.252	TLV-SEC	
Ton1	172.16.1.2	255.255.255.252	BSH	
Ton3	172.16.3.2	255.255.255.252	MMR	
Lo	10.16.23.1	255.255.255.255		
e0/3, e1/0-3, e2/0-3			Shotdown	

TLV-Second				
INTERFACE	IP ADDRESS	SUBMASK	Connected to	VIP
e0/0	64.100.0.10	255.255.255.252	ISP	
e0/1			DSW2	
e0/1.10	10.11.10.2	255.255.255.0	VLAN 10	10.11.10.7
e0/1.20	10.11.20.2	255.255.255.0	VLAN 20	10.11.20.7
e0/1.99	10.11.99.2	255.255.255.0	VLAN 99	
e0/2	10.11.1.2	255.255.255.252	TLV-Main	
Ton2	172.16.2.2	255.255.255.252	BSH	
Ton4	172.16.4.2	255.255.255.252	MMR	
Lo	10.16.33.1	255.255.255.255		
e0/3, e1/0-3, e2/0-3			Shotdown	

DSW1					
Interface	EtherChannel	Mode / Ip address	Native	Vlans	Connected to
e0/0	x	Trunk	v	10, 20	TLV-Main
e1/0-1	Po1 LACP [Activel	Trunk	v	10, 20	DSW2
e2/0-1	Po2	Trunk	v	10, 20	ACC1
e3/0-1	Po4	Trunk	v	20	ACC2
e0/1-3,e1-3/2-3		Access		Block	shutdown
SVI20		10.11.20.3			

DSW2					
Interface	EtherChannel	Mode / Ip address	Native	Vlans	Connected to
e0/0	x	Trunk	v	10,20	TLV-Main
e1/0-1	Po1	Trunk	v	10,20	DSW1
e2/0-1	Po3	Trunk	v	20	ACC2
e3/0-1	Po5	Trunk	v	10,20	ACC1
e0/1-3,e1-3/2-3		Access		Block	shutdown
SVI20		10.11.20.4			

ACC1					
Interface	EtherChannel	Mode / Ip address	Native	Vlans	Connected to
e2/0-1	Po2	Trunk	v	All	DSW1
e3/0-1	Po5	Trunk	v	All	DSW2
e0/0	x	Access passive		10	IT-PC
e0-1/1-3,e2-3/2-3		Access		Block	shutdown
SVI20		10.11.20.6			

ACC2					
Interface	EtherChannel	Mode / Ip address	Native	Vlans	Connected to
e2/0-1	Po3	Trunk	v	20	DSW2
e3/0-1	Po4	Trunk	v	20	DSW1
e0/0	x	Access		10	USER
e0-1/1-3,e2-3/2-3		Access		Block	shutdown
SVI20		10.11.20.5			

Routing Table: Main (TLV)

Routing Table: Branch

BSH			
INTERFACE	IP ADDRESS	SUBMASK	Connected to
e0/0	64.100.0.2	255.255.255.252	ISP
e0/1			SW1
e0/1.10	10.10.10.1	255.255.255.0	VLAN 10
e0/1.20	10.10.20.1	255.255.255.0	VLAN 20
e0/1.99	10.10.99.1	255.255.255.0	VLAN 99
Ton1	172.16.1.1	255.255.255.252	TLV-Main
Ton2	172.16.2.1	255.255.255.252	TLV-SEC
Lo	10.16.13.1	255.255.255.255	
e0/3, e1/0-3, e2/0-3			Shotdown

MMR			
INTERFACE	IP ADDRESS	SUBMASK	Connected to
e0/0	64.100.0.14	255.255.255.252	ISP
e0/1			SW2
e0/1.10	10.12.10.1	255.255.255.0	VLAN 10
e0/1.20	10.12.20.1	255.255.255.0	VLAN 20
e0/1.99	10.12.99.1	255.255.255.0	VLAN 99
Ton3	172.16.3.1	255.255.255.252	TLV-MAIN
Ton4	172.16.4.2	255.255.255.252	TLV-SEC
Lo	10.16.43.1	255.255.255.255	
e0/3, e1/0-3, e2/0-3			Shotdown

SW1					
Interface	EtherChannel	Mode / Ip address	Native	Vlans	Connected to
e0/1		Trunk	99	All	BSH
e0/0		Access		10	USER
e0/2-3, e1/0-1, e2/0-1,e3/0-1				Block	Shutdown
SVI20		10.10.20.2			

SW2					
Interface	EtherChannel	Mode / Ip address	Native	Vlans	Connected to
e0/1		Trunk	99	ALL	MMR
e0/0		Access		10	USER3
e0/2-3, e1/0-1, e2/0-1,e3/0-1				Block	Shutdown
SVI20		10.12.20.2			

IPsec over GRE

Connections between networks over the internet:

- GRE: Creates a virtual tunnel that allows for the transfer of different types of traffic (including multicast and broadcast) but does not provide encryption or security.

- IPsec: Secures the traffic by encrypting and authenticating it, ensuring that data is transmitted securely.

In my implementation of GRE within IPsec, I created a secure and flexible tunnel that connected the branch offices in the organizational network. I mainly used this method in a Hub-and-Spoke model, where each branch is securely connected to the central office, ensuring an efficient and secure connection across all parts of the organization.

```
TLV-Main#sh int tun 1
Tunnel1 is up, line protocol is up
  Hardware is Tunnel
  Description: #TLV-MAIN TO BSH tunnel 1#
  Internet address is 172.16.1.1/30
  MTU 17874 bytes, BW 4000 Kbit/sec, DLY 50000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel linestate evaluation up
  Tunnel source 10.16.23.1 (Loopback0), destination 10.16.13.1
   Tunnel Subblocks:
      src-track:
         Tunnel1 source tracking subblock associated with Loopback0
          Set of tunnels with source Loopback0, 2 members (includes iterators),
on interface <OK>
  Tunnel protocol/transport GRE/IP
    Key disabled, sequencing disabled
    Checksumming of packets disabled
  Tunnel TTL 255, Fast tunneling enabled
  Tunnel transport MTU 1434 bytes
  Tunnel transmit bandwidth 8000 (kbps)
  Tunnel receive bandwidth 8000 (kbps)
  Tunnel protection via IPSec (profile "GRE-PROFILE0")
  Last input 00:00:04, output never, output hang never
  Last clearing of "show interface" counters 00:04:12
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     40 packets input, 4740 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     39 packets output, 4536 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 unknown protocol drops
     0 output buffer failures, 0 output buffers swapped out
```

```
BSH#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
10.16.13.1      10.16.33.1      QM_IDLE           1011 ACTIVE
10.16.13.1      10.16.23.1      QM_IDLE           1012 ACTIVE
```

Single Area OSPF

I chose to use SINGLE AREA OSPF because it is a dynamic protocol that is easy to manage and suitable for small to medium networks. It allows for managing neighbor relationships between remote networks. OSPF creates a complete map of the network, calculates the shortest path, and performs updates only when there are changes in the network structure. The result is a stable and fast network with quick convergence, without the need for a complex hierarchical structure.

```
Gateway of last resort is 64.100.0.5 to network 0.0.0.0

      10.0.0.0/8 is variably subnetted, 14 subnets, 3 masks
O        10.10.10.0/24 [110/35] via 172.16.1.2, 00:34:16, Tunnel1
O        10.10.20.0/24 [110/35] via 172.16.1.2, 00:34:16, Tunnel1
O        10.12.10.0/24 [110/35] via 172.16.3.1, 00:34:16, Tunnel3
O        10.12.20.0/24 [110/35] via 172.16.3.1, 00:34:16, Tunnel3
      172.16.0.0/16 is variably subnetted, 6 subnets, 2 masks
O        172.16.2.0/30 [110/35] via 10.11.20.2, 00:32:36, Ethernet0/1.20
                       [110/35] via 10.11.10.2, 00:03:55, Ethernet0/1.10
O        172.16.4.0/30 [110/35] via 10.11.20.2, 00:32:36, Ethernet0/1.20
                       [110/35] via 10.11.10.2, 00:03:55, Ethernet0/1.10
```

```
TLV-Main#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
2.2.2.2           1   FULL/DR         00:00:38    10.11.20.2      Ethernet0/1.20
2.2.2.2           1   FULL/DR         00:00:38    10.11.10.2      Ethernet0/1.10
4.4.4.4           0   FULL/  -        00:00:38    172.16.3.1      Tunnel3
3.3.3.3           0   FULL/  -        00:00:38    172.16.1.2      Tunnel1
TLV-Main#show ip route ospf
```

Router on a Stick

Router on a Stick is a network configuration that allows for simple inter-VLAN routing without the need for multiple routers. Here are the key points:

- Single Interface: A single physical interface on the router connects to a switch and is configured as a trunk link.
- Subinterfaces: The router's interface is divided into multiple subinterfaces, each assigned to a specific VLAN with its own IP address.
- Inter-VLAN Routing: This configuration allows devices in different VLANs to communicate through the router.

```
TLV-Main#show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
Ethernet0/0                64.100.0.6      YES NVRAM  up                    up
Ethernet0/1                unassigned      YES NVRAM  up                    up
Ethernet0/1.10             10.11.10.1      YES NVRAM  up                    up
Ethernet0/1.20             10.11.20.1      YES NVRAM  up                    up
Ethernet0/1.99             10.11.99.1      YES NVRAM  up                    up
```

Per VLAN Spanning Tree (PVST)

I chose to use Per VLAN Spanning Tree (PVST) in my project because it effectively prevents traffic loops and ensures stable connectivity between network devices.

Key Features:

- Loop Prevention: PVST determines which links are active and which are blocked, ensuring smooth network operation.
- 802.1D Utilization: It uses the Spanning Tree Protocol 802.1D for efficient traffic management.
- VLAN-Based Management: PVST operates a separate Spanning Tree for each VLAN, allowing flexibility in traffic management.
- Distributed Decision-Making: It recalculates the topology in case of a link failure, maintaining network stability.

```
DSW2#show spanning-tree  vlan 10 | begin Interface
Interface            Role Sts Cost      Prio.Nbr Type
-------------------- ---- --- --------- -------- -----
Et0/0                Desg FWD 100       128.1    P2p
Po1                  Desg FWD 56        128.65   P2p
Po3                  Desg FWD 56        128.66   P2p

DSW2#show spanning-tree  vlan 20 | begin Interface
Interface            Role Sts Cost      Prio.Nbr Type
-------------------- ---- --- --------- -------- -----
Et0/0                Desg FWD 100       128.1    P2p
Po1                  Root FWD 56        128.65   P2p
Po3                  Desg FWD 56        128.66   P2p
Po5                  Desg FWD 56        128.67   P2p
```

EtherChannel

I implemented a Channel Group in my project using Cisco networking to combine multiple physical ports into a single logical interface, known as EtherChannel. This setup increases overall bandwidth and provides redundancy by allowing all grouped ports to function as a single aggregated link. Within the network, routers and switches recognize this group as one logical port, which simplifies management and improves performance. This approach significantly enhanced the efficiency and reliability of the network.

```
DSW1#show etherchannel summary | begin Group
Group  Port-channel  Protocol    Ports
------+-------------+-----------+--------------------
1      Po1(SU)         LACP      Et1/0(P)    Et1/1(P)
2      Po2(SU)         LACP      Et2/0(P)    Et2/1(P)
4      Po4(SU)         LACP      Et3/0(P)    Et3/1(P)
```

```
DSW2#show etherchannel summary | begin Group
Group  Port-channel  Protocol    Ports
------+-------------+-----------+--------------------
1      Po1(SU)         LACP      Et1/0(P)    Et1/1(P)
3      Po3(SU)         LACP      Et2/0(P)    Et2/1(P)
5      Po5(SU)         LACP      Et3/0(P)    Et3/1(P)
```

LACP (Link Aggregation Control Protocol)

LACP, a standardized protocol (IEEE 802.3ad), facilitates the dynamic creation of EtherChannels. It automatically manages port grouping to ensure that if one port fails, the remaining ports continue to function seamlessly as an aggregated link, maintaining network stability and load balancing.

DHCP

DHCP (Dynamic Host Configuration Protocol) is a protocol that automatically allocates IP addresses and associated information to devices on a network, simplifying the configuration process and reducing errors.

I set up DHCP on both routers at the main branch. Each router has a different address range, and I also reserved a specific range of addresses for the devices I want to configure separately.

```
Pool USER :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 1
 Pending event                  : none
 1 subnet is currently in the pool :
 Current index        IP address range                    Leased addresses
 10.11.10.13          10.11.10.1      - 10.11.10.254      1

Pool IT-MGMT :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 1
 Pending event                  : none
 1 subnet is currently in the pool :
 Current index        IP address range                    Leased addresses
 10.11.20.12          10.11.20.1      - 10.11.20.254      1
```

```
TLV-Main#show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address          Client-ID/                Lease expiration        Type
                    Hardware address/
                    User name
10.11.10.12         0063.6973.636f.2d61.      Sep 29 2024 09:37 PM    Automatic
                    6162.622e.6363.3030.
                    2e30.6230.302d.4574.
                    302f.30
10.11.20.11         0063.6973.636f.2d61.      Sep 29 2024 06:56 PM    Automatic
                    6162.622e.6363.3030.
                    2e30.6330.302d.4574.
                    302f.30
```

HSRP (Hot Standby Router Protocol)

HSRP is a protocol that provides redundancy by designating one router as active and another as standby within a group, allowing them to operate as a single virtual router. If the active router fails, the standby router takes over seamlessly to ensure continuous network connectivity. I implemented HSRP in my project to enhance redundancy and maintain network availability in case of a router failure.

```
TLV-Main#show standby
Ethernet0/1.10 - Group 10
  State is Active
    2 state changes, last state change 15:11:32
  Virtual IP address is 10.11.10.7
  Active virtual MAC address is 0000.0c07.ac0a
    Local virtual MAC address is 0000.0c07.ac0a (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 2.688 secs
  Authentication MD5, key-string
  Preemption enabled
  Active router is local
  Standby router is 10.11.10.2, priority 100 (expires in 9.872 sec)
  Priority 110 (configured 110)
    Track object 10 state Up decrement 20
  Group name is "hsrp-Et0/1.10-10" (default)
Ethernet0/1.20 - Group 20
  State is Active
    2 state changes, last state change 15:11:31
  Virtual IP address is 10.11.20.7
  Active virtual MAC address is 0000.0c07.ac14
    Local virtual MAC address is 0000.0c07.ac14 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 2.144 secs
  Authentication MD5, key-string
  Preemption enabled
  Active router is local
  Standby router is 10.11.20.2, priority 100 (expires in 9.856 sec)
  Priority 110 (configured 110)
    Track object 10 state Up decrement 20
    Track object 20 (unknown)
  Group name is "hsrp-Et0/1.20-20" (default)
```

SSH

SSH (Secure Shell) is a secure communication protocol designed to enable a secure connection between computers over an unsecured network. The protocol provides a secure connection for remote management of devices and systems, such as servers and routers.

Key Features of SSH:

- Data Security: SSH encrypts the data transmitted between the client and the server, helping to prevent eavesdropping by third parties.
- Authentication: Users can authenticate the identity of the server and the user using passwords or public/private keys, providing a higher level of security.
- Remote Management: Allows remote management of devices and systems, enabling access to Linux servers, routers, switches, and more, from anywhere with an internet connection.
- Support for Additional Protocols: SSH can also be used for file transfer via SFTP (SSH File Transfer Protocol) or SCP (Secure Copy Protocol).

```
TLV-Main#show running-config | include ssh
ip ssh time-out 6
ip ssh authentication-retries 2
ip ssh version 2
 transport input ssh
 transport output ssh
```

Switchport Security

To prevent unauthorized access, I used Switchport Security in the Restricted mode. In this mode, administrators can choose to set static MAC addresses, or alternatively, allow the switch to automatically learn dynamic addresses.

```
ACC2#show run | begin interface Ethernet0/0
interface Ethernet0/0
 switchport access vlan 10
 switchport mode access
 switchport port-security maximum 2
 switchport port-security violation restrict
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky aabb.cc00.0b00
 switchport port-security
```

Additionally, the "sticky" option lets the switch remember the MAC addresses of connected devices even after a reboot. However, while Switchport Security provides flexibility in managing network security, incorrect configuration can lead to blocking access for legitimate devices. Therefore, it is an essential tool for enhancing network security and stability.

CDP

CDP (Cisco Discovery Protocol) is a Cisco protocol that lets network devices share information with nearby devices, such as names, IP addresses, and software versions. It operates at Layer 2 and updates every 60 seconds to help with device discovery and troubleshooting.

However, for security reasons, I disabled CDP to prevent the device from sharing its information and reduce the risk of unauthorized access or attacks.

```
TLV-Main#show run
no cdp run
```

```
DSW2#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
ACC1.yairus.com  Eth 3/0           169              S I   Linux Uni Eth 3/0
ACC1.yairus.com  Eth 3/1           145              S I   Linux Uni Eth 3/1
DSW1.yairus.com  Eth 1/0           168              S I   Linux Uni Eth 1/0
DSW1.yairus.com  Eth 1/1           136              S I   Linux Uni Eth 1/1
ACC2.yairus.com  Eth 2/0           176              S I   Linux Uni Eth 2/0
ACC2.yairus.com  Eth 2/1           158              S I   Linux Uni Eth 2/1
TLV-Second.yairus.com
                 Eth 0/0           142              R B   Linux Uni Eth 0/1

Total cdp entries displayed : 7
```

DAI

I used Dynamic ARP Inspection (DAI) to protect the network from ARP spoofing attacks. By working with DHCP Snooping, DAI verifies ARP messages against a binding table of valid IP-to-MAC addresses.

This ensures only authorized devices communicate on the network, enhancing security and preventing unauthorized access.

```
ACC2#show ip dhcp sn
ACC2#show ip dhcp snooping
Switch DHCP snooping is enabled
Switch DHCP gleaning is disabled
DHCP snooping is configured on following VLANs:
10,20
DHCP snooping is operational on following VLANs:
10,20
```

block ports

I created a VLAN for blocked ports to enhance network security and prevent unauthorized access. When a blocked port is not assigned to an active VLAN, I ensured that no device could connect to the network through those ports. This reduced the risk of attacks such as data theft or network intrusion. Additionally, the VLANs allowed me to manage traffic more effectively, optimizing resource usage across the network.

```
DSW2# show vlan br

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active
10   User                             active
20   IT-MGMT                          active
88   Block                            active    Et0/1, Et0/2, Et0/3, Et1/2
                                                Et1/3, Et2/2, Et2/3, Et3/2
                                                Et3/3
99   Native                           active
```

BDPU Guard

I implemented BDPU Guard to enhance network security by preventing unauthorized switches from disrupting the network. This feature blocks ports when a BPDU is detected on ports intended for end devices, thereby safeguarding against potential loops and misconfigurations that rogue switches could introduce. Its integration is critical in environments that rely on Spanning Tree Protocol (STP), as it helps maintain the integrity of the network topology.

PortFast

I configured PortFast on ports connected to end devices to significantly reduce the time it takes for new devices to join the network. By allowing these ports to transition immediately to the "forwarding" state—bypassing the typical STP processing stages—PortFast facilitates quicker network access. This is especially advantageous in dynamic environments where devices are frequently connecting and disconnecting, ensuring a seamless experience while preserving the stability of the STP process.

```
ACC2#show spanning-tree detail

 VLAN0010 is executing the rstp compatible Spanning Tree protocol
  Bridge Identifier has priority 32768, sysid 10, address aabb.cc00.0700
  Configured hello time 2, max age 20, forward delay 15, transmit hold-count 6
  Current root has priority 4106, address aabb.cc00.0e00
  Root port is 65 (Port-channel3), cost of root path is 56
  Topology change flag not set, detected flag not set
  Number of topology changes 2 last change occurred 19:06:01 ago
          from Port-channel4
  Times:  hold 1, topology change 35, notification 2
          hello 2, max age 20, forward delay 15
  Timers: hello 0, topology change 0, notification 0, aging 300

 Port 1 (Ethernet0/0) of VLAN0010 is designated forwarding
    Port path cost 100, Port priority 128, Port Identifier 128.1.
    Designated root has priority 4106, address aabb.cc00.0e00
    Designated bridge has priority 32778, address aabb.cc00.0700
    Designated port id is 128.1, designated path cost 56
    Timers: message age 0, forward delay 0, hold 0
    Number of transitions to forwarding state: 10
    The port is in the portfast edge mode
    Link type is point-to-point by default
    Bpdu guard is enabled
    BPDU: sent 34192, received 0
```

Line VTY, Console & more

The use of Line VTY and Line Console allows me to manage access to devices both remotely and locally via SSH and TTY connections.

This is crucial for maintaining system security and efficient device management in the network, as it provides different access levels for users based on their needs.

```
TLV-Main#show run | include secret
enable secret 5 $1$TbVM$MTz1pUo8k7LqM4pmMLkJk/
username admin secret 5 $1$c8b.$g7l6qroBHx1pnq/d56IMU/
```

```
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 access-class IT_SSH in
 exec-timeout 6 0
 login local
 transport input ssh
 transport output ssh
```

Ansible Configuration

In this project, I used Ansible to simplify the device configuration process. The INI file contains the device's connection details, including SSH credentials and privilege escalation settings.

The YAML playbook loads a pre-prepared configuration file onto the device using Ansible's ios_config module, enabling easy and efficient configuration management while reducing human errors. Ansible streamlines the process, especially in environments with multiple devices.

```yaml
---
- name: Connect and run configuration file
  hosts: cisco_device
  gather_facts: no
  vars_prompt:
    - name: "config_file"
      prompt: "Enter the configuration file path"
      private: no

  tasks:
    - name: Load configuration from file
      cisco.ios.ios_config:
        src: "{{ config_file }}"
        save_when: changed
```