Secure And Stablished Network For University

prepared by:
Abdelrahman Khaled Mohamed
Abdulrahman Zakaria Hussein
Ahmed Mohammed Omar
Sara Mostafa Ahmed Helal
Mohammed Reda Abdelhaleem
Sara Ali Ghaly
Supervisor:
Engineer: Amr Reda

Table of Contents

1. Introduction

1.1 Document Control :

- **Document Title:** University Network Analysis Project Documentation

1.2 Document Purpose :

- **The purpose of this document is to outline the objectives, scope, and methodology of the University Network Analysis Project. It serves as a guide for all stakeholders involved, providing a clear framework for the project's execution. Additionally, this document aims to ensure effective communication among team members and facilitate the systematic collection and analysis of packet traces, ultimately contributing to enhanced network performance and security within the university.**

Technical Solution Overview

1.3 Details of the solution

1.3.1 Overview & Purpose of the project

The project aims to implement a state-of-the-art wired infrastructure that leverages the latest technological elements to enhance the university's network capabilities. By utilizing advanced hardware and software solutions, the project seeks to improve network performance, reliability, and security, thereby supporting the academic and administrative needs of the institution effectively.

1.4 Solution Components

I. **Network Solution:**

a. **Core switches**

*Model**:** 4 x Multilayer Switch 3650
* **Purpose:** These switches will serve as the backbone of the network, providing high-speed connectivity and efficient data routing across various segments of the university network.

b. **Servers Aggregator Switches & :**

Model:
10 x Switch 2960.

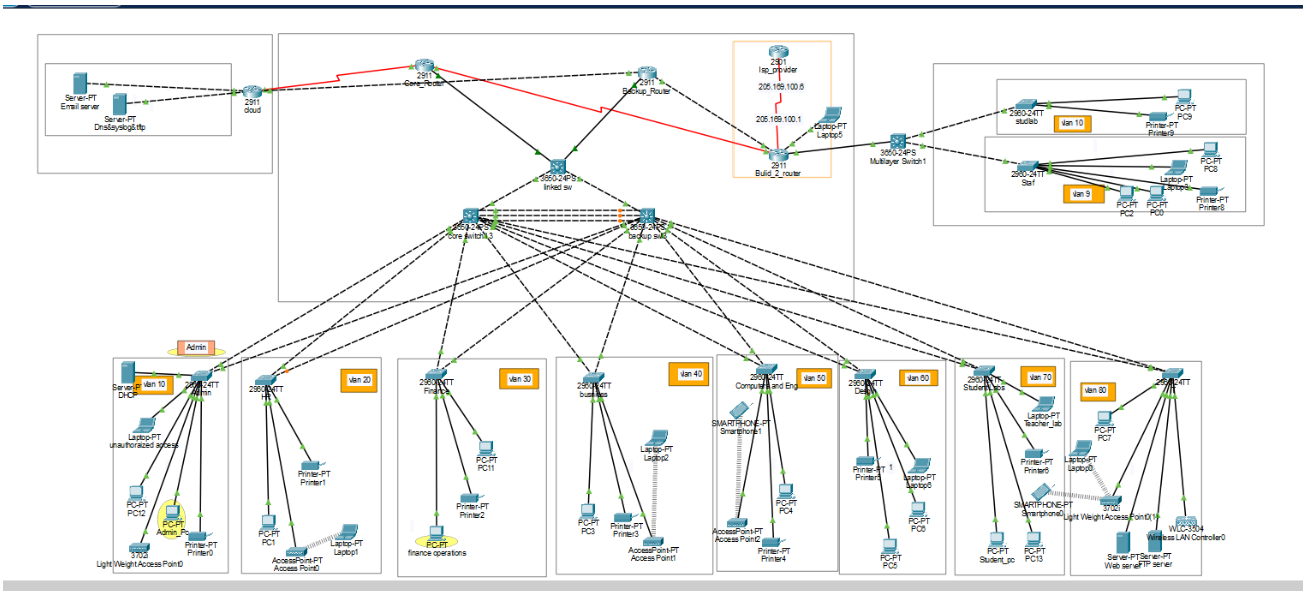
Purpose: These switches will aggregate traffic from server racks, ensuring robust connectivity
and optimal load balancing for both fiber and UTP connections..

c. **Routers:**

Model: 4 x Cisco Catalyst 2911 & 1x Cisco Catalyst 2901

2. Network Architecture

2.1 PhysicalTopology:



3. Naming Convention and IP scheme

3.1 Naming Convention

We will use a standard naming convention to name all network infrastructure equipment. This facilitates device identification and management during the day-to-day administration activities as well as problem troubleshooting.

According to network Infrastructure naming convention, we are going to use the following naming schema for our network devices:

Hostname	IP address
email 1	169.254.0.1
Admin_Pc	192.168.1.6
Printer0	192.168.1.8
sara	192.168.2.2
Laptop1	192.168.2.4
Printer1	192.168.2.3
finance operations	192.168.3.4
Printer2	192.168.3.2
PC11	192.168.3.3
Laptop11	192.168.4.4
Printer3	192.168.4.2
afna	192.168.4.3
PC4	192.168.5.2
Printer4	192.168.5.3
PC5	192.168.6.3
Printer5	192.168.6.2
Teacher_lab	192.168.7.4
Printer6	192.168.7.5
PC13	192.168.7.2
PC7	192.168.8.3
Web server	192.168.8.2
FTP server	192.168.8.4
PC2	192.168.9.4
PC0	192.168.9.2
Laptop3	192.168.9.5
Printer8	192.168.9.3
PC8	192.168.9.6
Printer9	192.168.10.2
PC9	192.168.10.3
ssh	192.168.207.2
Dns&syslog&tftp	20.0.0.6

3.2 IP Addressing Scheme

The following is the IP schema that will be implemented at building Infrastructure:

VLAN Number	VLAN Name	Subnet	Default gateway
Vlan 10	Admin	255.255.255.0	192.168.2.1
Vlan 20	HR	255.255.255.0	192.168.2.1
Vlan 30	Finance	255.255.255.0	192.168.3.1

Vlan 40	busniess	255.255.255.0	192.168.4.1
Vlan 50	Computers and Eng	255.255.255.0	192.168.5.1
Vlan 60	Desgin	255.255.255.0	192.168.6.1
Vlan 70	Student Labs	255.255.255.0	192.168.7.1
Vlan 80	IT	255.255.255.0	192.168.8.1
Vlan 90	staf	255.255.255.0	192.168.9.1
Vlan 100	studlab	255.255.255.0	192.168.10.1

Table 1 - IP VLAN Scheme

4. Port Mapping

Device	Port	Peer Device
Core_Router	Gig0/0	linked sw
Core_Router	Serial0/2/1	Bulid_2_router
Core_Router	Serial0/2/0	cloud
cloud	Gig0/0	Dns&syslog&tftp
Backup_Router	Gig0/2	cloud
Backup_Router	Gig0/1	Bulid_2_router
Backup_Router	Gig0/0	linked sw
Bulid_2_router	Serial0/2/1	Isp_provider
Bulid_2_router	Gig0/0	Multilayer Switch1
Multilayer Switch	Gig1/0/3	studlab
Multilayer Switch	Gig1/0/2	Staf
studlab	F0/2	PC9
studlab	F0/3	Printer9
Staf	F0/2	Pc8
Staf	F0/4	Laptop3
Staf	F0/6	PC2
Staf	F0/5	Pc0
Staf	F0/3	Printer8
linked sw	Gig1/0/2	Ml3sw_Core
linked sw	Gig1/0/3	Ml3SW_Backup
Ml3sw_Core	Gig1/0/2	Admin
Ml3sw_Core	Gig1/0/3	HR
Ml3sw_Core	Gig1/0/4	Finance
Ml3sw_Core	Gig1/0/5	busniess
Ml3sw_Core	Gig1/0/6	Computers and Eng
Ml3sw_Core	Gig1/0/7	Desgin
Ml3sw_Core	Gig1/0/8	Student Labs
Ml3sw_Core	Gig1/0/9	IT
Ml3SW_Backup	Gig1/0/2	Admin
Ml3SW_Backup	Gig1/0/3	HR
Ml3SW_Backup	Gig1/0/4	Finance
Ml3SW_Backup	Gig1/0/5	busniess

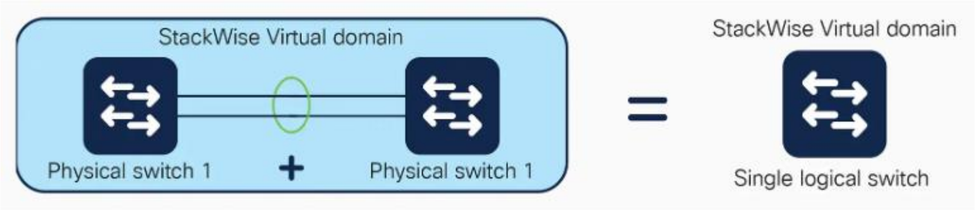
Ml3SW_Backup	Gig1/0/6	Computers and Eng
Ml3SW_Backup	Gig1/0/7	Desgin
Ml3SW_Backup	Gig1/0/8	Student Labs
Ml3SW_Backup	Gig1/0/9	IT
Admin	F0/6	DHCP
Admin	F0/7	email 1
Admin	F0/2	Admin_Pc
Admin	F0/3	Printer0
Admin	F0/8	Light Weight Access Point0
Admin	F0/4	unauthoraized access
HR	F0/6	Laptop20
HR	F0/4	Laptop18
HR	F0/3	Printer1
HR	F0/7	Access Point0
HR	F0/2	sara
Finance	F0/4	Pc11
Finance	F0/3	finance operations
Finance	F0/2	Printer2
busniess	F0/6	Laptop11
busniess	F0/4	Access Point1
busniess	F0/3	Printer3
busniess	F0/2	afna
Computers	F0/2	PC4
Computers	F0/4	Access Point2
Computers	F0/3	Printer4
Desgin	F0/4	Laptop6
Desgin	F0/6	PC6
Desgin	F0/2	Pc5
Desgin	F0/3	Printer5
Student Labs	F0/4	Teacher_lab
Student Labs	F0/3	Printer6
Student Labs	F0/5	PC13
Student Labs	F0/2	Student_pc
IT	F0/6	Wireless LAN Controller0
IT	F0/7	Light Weight Access Point0(1)

IT	F0/3	Web server
IT	F0/4	FTP server

5. Network Design Notes & Configurations

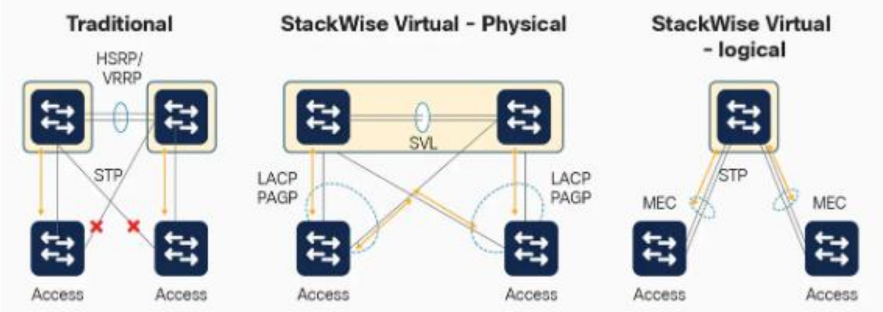
5.1 Stack-Wise Virtual Technology

Cisco Catalyst Stack-Wise Virtual technology allows the clustering of two physical switches together into a single logical entity. The two switches operate as one; they share the same configuration and forwarding state. This technology allows for enhancements in all areas of network design, including high availability, scalability, management, and maintenance.



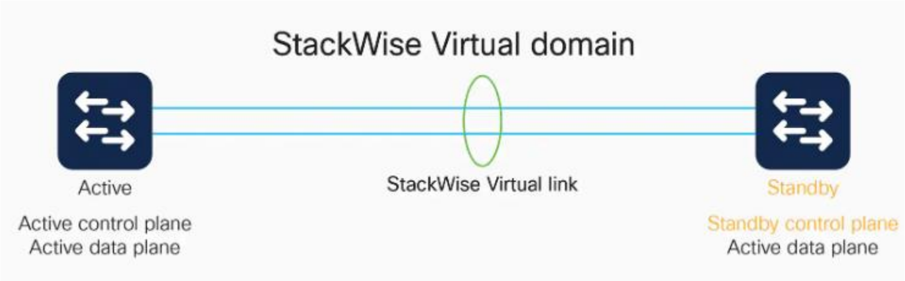
Key business benefits of the SVL include the following:

- Reduced risk associated with a looped topology.
- Non-stop business communication through the use of a redundant chassis with SSO-enabled supervisors.
- Better return on existing investments via increased bandwidth from access layer.
- Reduced configuration errors and elimination of First Hop Redundancy Protocols (FHRP), such as Hot Standby Routing Protocol (HSRP), GLBP and VRRP.
- Simplified management of a single configuration and fewer operational failure points



Within a StackWise Virtual domain, one device is designated as the SV active switch, and the other is designated as the SV standby switch (Figure 3). All control plane functions are centrally managed by the SV active switch, including:

- Management (Simple Network Management Protocol [SNMP], Telnet, Secure Shell [SSH] Protocol, etc.).
- Layer 2 protocols (Bridge Protocol Data Units [BPDUs], Protocol Data Units [PDUs], Link Aggregation Control Protocol [LACP], etc.).
- Layer 3 protocols (routing protocols, etc.).Software data path



```
Building configuration...

Current configuration : 2426 bytes
!
version 16.3.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Ml3sw_Core
!
!
enable password 7 0822455D0A16
!
!
!
!
!
!
no ip cef
no ipv6 cef
!
!
!
!
!
!
!
!
!
!
!
!
no ip domain-lookup
!
!
spanning-tree mode rapid-pvst
!
```

```
!
!
!
!
!
interface Port-channel1
!
interface GigabitEthernet1/0/1
switchport mode trunk
!
interface GigabitEthernet1/0/2
switchport access vlan 10
switchport mode access
spanning-tree portfast
!
interface GigabitEthernet1/0/3
switchport access vlan 20
switchport mode access
spanning-tree portfast
!
interface GigabitEthernet1/0/4
switchport access vlan 30
switchport mode access
spanning-tree portfast
ip access-group 100 in
!
interface GigabitEthernet1/0/5
switchport access vlan 40
switchport mode access
spanning-tree portfast
!
interface GigabitEthernet1/0/6
switchport access vlan 50
switchport mode access
spanning-tree portfast
!
interface GigabitEthernet1/0/7
switchport access vlan 60
switchport mode access
spanning-tree portfast
!
interface GigabitEthernet1/0/8
switchport access vlan 70
switchport mode access
spanning-tree portfast
!
interface GigabitEthernet1/0/9
switchport access vlan 80
switchport mode access
spanning-tree portfast
!
interface GigabitEthernet1/0/10
no switchport
ip address 192.168.205.1 255.255.255.0
duplex auto
speed auto
!
interface GigabitEthernet1/0/11
```

```
!
interface GigabitEthernet1/0/12
!
interface GigabitEthernet1/0/13
!
interface GigabitEthernet1/0/14
!
interface GigabitEthernet1/0/15
!
interface GigabitEthernet1/0/16
!
interface GigabitEthernet1/0/17
!
interface GigabitEthernet1/0/18
!
interface GigabitEthernet1/0/19
!
interface GigabitEthernet1/0/20
!
interface GigabitEthernet1/0/21
channel-group 1 mode passive
!
interface GigabitEthernet1/0/22
channel-group 1 mode passive
!
interface GigabitEthernet1/0/23
channel-group 1 mode passive
!
interface GigabitEthernet1/0/24
switchport mode trunk
!
interface GigabitEthernet1/1/1
!
interface GigabitEthernet1/1/2
!
interface GigabitEthernet1/1/3
!
interface GigabitEthernet1/1/4
!
interface Vlan1
no ip address
shutdown
!
interface Vlan30
mac-address 00e0.f7b5.2001
no ip address
ip access-group 100 in
!
ip classless
!
ip flow-export version 9
!
!
!
banner motd ^CNO Unauthorized Access!!^C
!
!
!
```

```
!
line con 0
password 7 0822455D0A16
login
!
line aux 0
!
line vty 0 4
login
!
!
!
!
End
++++++++++++++++++++++++++++++++++++++++++++
Building configuration...

Current configuration : 2153 bytes
!
version 16.3.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Ml3SW_Backup
!
!
enable password 7 0822455D0A16
!
!
!
!
!
!
no ip cef
no ipv6 cef
!
!
!
!
!
!
!
!
!
!
!
!
no ip domain-lookup
!
!
spanning-tree mode rapid-pvst
!
!
!
!
!
!
```

```
interface Port-channel1
!
interface GigabitEthernet1/0/1
 switchport mode trunk
!
interface GigabitEthernet1/0/2
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/3
 switchport access vlan 20
 switchport mode access
!
interface GigabitEthernet1/0/4
 switchport access vlan 30
 switchport mode access
 ip access-group 100 in
!
interface GigabitEthernet1/0/5
 switchport access vlan 40
 switchport mode access
!
interface GigabitEthernet1/0/6
 switchport access vlan 50
 switchport mode access
!
interface GigabitEthernet1/0/7
 switchport access vlan 60
 switchport mode access
!
interface GigabitEthernet1/0/8
 switchport access vlan 70
 switchport mode access
!
interface GigabitEthernet1/0/9
 switchport access vlan 80
 switchport mode access
!
interface GigabitEthernet1/0/10
!
interface GigabitEthernet1/0/11
!
interface GigabitEthernet1/0/12
!
interface GigabitEthernet1/0/13
!
interface GigabitEthernet1/0/14
!
interface GigabitEthernet1/0/15
!
interface GigabitEthernet1/0/16
!
interface GigabitEthernet1/0/17
!
interface GigabitEthernet1/0/18
!
interface GigabitEthernet1/0/19
!
```

```
interface GigabitEthernet1/0/20
!
interface GigabitEthernet1/0/21
 channel-group 1 mode active
!
interface GigabitEthernet1/0/22
 channel-group 1 mode active
!
interface GigabitEthernet1/0/23
 channel-group 1 mode active
!
interface GigabitEthernet1/0/24
 switchport mode trunk
!
interface GigabitEthernet1/1/1
!
interface GigabitEthernet1/1/2
!
interface GigabitEthernet1/1/3
!
interface GigabitEthernet1/1/4
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan30
 mac-address 00e0.a3a8.4201
 no ip address
 ip access-group 100 in
!
ip classless
!
ip flow-export version 9
!
!
!
banner motd ^CNO Unauthorized Access!!^C
!
!
!
!
line con 0
 password 7 0822455D0A16
 login
!
line aux 0
!
line vty 0 4
 login
!
!
!
!
end
```

SVL Configuration

5.2 Layer 2 technologies

- Spanning Tree is configured in order to protect against physical and logical misconfigurations and a possibility to erroneously create L2 loops. Spanning tree is used in RPVST+ mode.
- Spanning tree root is configured to be on the core with priority 0 for all Vlans.
- Dot1q will be the protocol used for trunking for all uplinks.
- VLANs carried over the trunking link between the core and the switches.

- Hosts & Server ports on edges are configured as spanning tree port fast to exclude them from the spanning tree protocol decreasing the time these ports take to be up. Unless it is configured as trunk and these ports are explicitly configured as trunk.
- All switches must be managed in a secure a manner by using SSH, authentication mechanism and set privilege levels for different users if needed.
- SNMP V2 is used to manage the switches using different read and read/write community strings.
- BPDU filter will be applied globally on all switches to protect the network from miss connection of switches to the network, which could lead to network loops.

5.2.1 VTP and Vlan Configuration

VTP is a Layer 2 messaging protocol that allows managing, the addition, deletion, and renaming of VLANs on a network-wide basis. In the current setup it is recommended that all Catalysts are in VTP transparent mode. In other words we don’t want those switches to listen to VTP updates and share VLAN database between them. Such approach requires more configuration work, because all VLANs should be configured on every switch. This will avoid simple but critical VLAN configuration mistakes being propagated via VTP.

5.2.1.1 VTP Configuration

```
#show vtp status
VTP Version capable : 1 to 2
VTP version running : 1
VTP Domain Name :
VTP Pruning Mode : Disabled
VTP Traps Generation : Disabled
Device ID : 0001.64E5.61E0
Configuration last modified by 0.0.0.0 at ٣-١-٩٣ ٠٠:٠٠:٠٠
Local updater ID is 0.0.0.0 (no valid interface found)

Feature VLAN :
--------------
VTP Operating Mode : Server
Maximum VLANs supported locally : 1005
Number of existing VLANs : 13
Configuration Revision : 120
MD5 digest : 0x43 0x98 0x3C 0xDB 0x2E 0x26 0x79 0x9D
0x9F 0x2D 0x36 0xB0 0x0D 0x0D 0x93 0x82
```

VTP Configuration

- VTP mode will be configured as transparent on all switches to avoid network outages due to miss-configured switches being added to the network or user miss-configuration that could be propagated to the entire network.

5.2.1.2 Vlan Configuration

- VLANs will be statically assigned to DC Switches.
- The Vlans would be created as per table 1.

```
 Ml3sw_Core#show vlan

VLAN Name Status Ports
---- -------------------------------- --------- -------------------------------
1 default active Po1, Gig1/0/11, Gig1/0/12, Gig1/0/13
Gig1/0/14, Gig1/0/15, Gig1/0/16, Gig1/0/17
Gig1/0/18, Gig1/0/19, Gig1/0/20, Gig1/0/21
Gig1/0/22, Gig1/0/23, Gig1/0/24, Gig1/1/1
Gig1/1/2, Gig1/1/3, Gig1/1/4
10 VLAN0010 active Gig1/0/2
20 VLAN0020 active Gig1/0/3
30 VLAN0030 active Gig1/0/4
40 VLAN0040 active Gig1/0/5
50 VLAN0050 active Gig1/0/6
60 VLAN0060 active Gig1/0/7
70 VLAN0070 active Gig1/0/8
80 VLAN0080 active Gig1/0/9
1002 fddi-default active
1003 token-ring-default active
1004 fddinet-default active
1005 trnet-default active

VLAN Type SAID MTU Parent RingNo BridgeNo Stp BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1 enet 100001 1500 - - - - - 0 0
10 enet 100010 1500 - - - - - 0 0
20 enet 100020 1500 - - - - - 0 0
30 enet 100030 1500 - - - - - 0 0
40 enet 100040 1500 - - - - - 0 0
50 enet 100050 1500 - - - - - 0 0
60 enet 100060 1500 - - - - - 0 0
70 enet 100070 1500 - - - - - 0 0
80 enet 100080 1500 - - - - - 0 0
1002 fddi 101002 1500 - - - - - 0 0
1003 tr 101003 1500 - - - - - 0 0
1004 fdnet 101004 1500 - - - ieee - 0 0
1005 trnet 101005 1500 - - - ibm - 0 0

VLAN Type SAID MTU Parent RingNo BridgeNo Stp BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------

Remote SPAN VLANs
------------------------------------------------------------------------------

Primary Secondary Type Ports
------- --------- ----------------- ------------------------------------------
```

5.2.2 Spanning-tree

STP is a Layer 2 link-management protocol that provides path redundancy while preventing undesirable loops in the network. For a Layer 2 Ethernet network to function properly, only one active path can exist between any two stations. STP operation is transparent to end stations, which cannot detect whether they are connected to a single LAN segment or a switched LAN of multiple segments.

When you create fault-tolerant internetworks, you must have a loop-free path between all nodes in a network. The STP algorithm calculates the best loop-free path throughout a switched Layer 2 network. Layer 2 LAN ports send and receive STP frames at regular intervals. Network devices do not forward these frames, but use the frames to construct a loop-free path.

5.2.2.1 Spanning-tree Configuration

Spanning Tree is configured in order to protect against physical and logical misconfigurations and a possibility to erroneously create L2 loops. Spanning tree is used in RPVST+ mode.

We recommend to not enable Bpdu filter to avoid any loop.

```
Ml3sw_Core#show spanning-tree
VLAN0001
Spanning tree enabled protocol rstp
Root ID Priority 32769
Address 00D0.BC53.3AC7
```

```
Cost 4
Port 1(GigabitEthernet1/0/1)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)
Address 00E0.F7B5.2086
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 20

Interface Role Sts Cost Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Gi1/0/1 Root FWD 4 128.1 P2p
Po1 Altn BLK 3 128.29 Shr

VLAN0010
Spanning tree enabled protocol rstp
Root ID Priority 32778
Address 0001.9621.8E07
Cost 19
Port 2(GigabitEthernet1/0/2)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32778 (priority 32768 sys-id-ext 10)
Address 00E0.F7B5.2086
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 20

Interface Role Sts Cost Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Gi1/0/1 Desg FWD 4 128.1 P2p
Gi1/0/2 Root FWD 19 128.2 P2p

VLAN0020
Spanning tree enabled protocol rstp
Root ID Priority 32788
Address 00D0.BC53.3AC7
Cost 4
Port 1(GigabitEthernet1/0/1)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32788 (priority 32768 sys-id-ext 20)
Address 00E0.F7B5.2086
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 20

Interface Role Sts Cost Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Gi1/0/1 Root FWD 4 128.1 P2p
Gi1/0/3 Desg FWD 19 128.3 P2p

VLAN0030
Spanning tree enabled protocol rstp
Root ID Priority 32798
Address 00D0.58CE.C069
Cost 19
Port 4(GigabitEthernet1/0/4)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
```

```
Bridge ID Priority 32798 (priority 32768 sys-id-ext 30)
Address 00E0.F7B5.2086
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 20

Interface Role Sts Cost Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Gi1/0/1 Desg FWD 4 128.1 P2p
Gi1/0/4 Root FWD 19 128.4 P2p

VLAN0040
Spanning tree enabled protocol rstp
Root ID Priority 32808
Address 0001.6438.C977
Cost 19
Port 5(GigabitEthernet1/0/5)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32808 (priority 32768 sys-id-ext 40)
Address 00E0.F7B5.2086
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 20

Interface Role Sts Cost Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Gi1/0/1 Desg FWD 4 128.1 P2p
Gi1/0/5 Root FWD 19 128.5 P2p

VLAN0050
Spanning tree enabled protocol rstp
Root ID Priority 32818
Address 0002.1602.47B9
Cost 19
Port 6(GigabitEthernet1/0/6)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32818 (priority 32768 sys-id-ext 50)
Address 00E0.F7B5.2086
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 20

Interface Role Sts Cost Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Gi1/0/1 Desg FWD 4 128.1 P2p
Gi1/0/6 Root FWD 19 128.6 P2p

VLAN0060
Spanning tree enabled protocol rstp
Root ID Priority 32828
Address 0000.0C33.7A38
Cost 19
Port 7(GigabitEthernet1/0/7)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32828 (priority 32768 sys-id-ext 60)
Address 00E0.F7B5.2086
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 20
```

```
Interface Role Sts Cost Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Gi1/0/1 Desg FWD 4 128.1 P2p
Gi1/0/7 Root FWD 19 128.7 P2p

VLAN0070
Spanning tree enabled protocol rstp
Root ID Priority 32838
Address 000D.BD12.16E4
Cost 19
Port 8(GigabitEthernet1/0/8)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32838 (priority 32768 sys-id-ext 70)
Address 00E0.F7B5.2086
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 20

Interface Role Sts Cost Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Gi1/0/1 Desg FWD 4 128.1 P2p
Gi1/0/8 Root FWD 19 128.8 P2p

VLAN0080
Spanning tree enabled protocol rstp
Root ID Priority 32848
Address 0090.2B33.550C
Cost 19
Port 9(GigabitEthernet1/0/9)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32848 (priority 32768 sys-id-ext 80)
Address 00E0.F7B5.2086
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 20

Interface Role Sts Cost Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Gi1/0/1 Desg FWD 4 128.1 P2p
Gi1/0/9 Root FWD 19 128.9 P2p
```

The following Spanning-tree features are enabled:

- In order to protect Spanning Tree from any misconfigurations STP PortFast BPDU guard is used. The STP PortFast BPDU guard enhancement allows network designers to enforce the STP domain borders and keep the active topology predictable. The devices behind the ports that have STP PortFast enabled are not able to influence the STP topology. At the reception of BPDUs from PortFast enabled port, the BPDU guard operation disables the port. The BPDU guard transitions the port into errdisable state
- Uplinkfast is enabled on the switches for fast convergence from indirect link failures.

- Spanning tree root is configured to be on the core switch with priority 0 for all Vlans.

5.2.3 Err-disable recovery

If the configuration shows a port to be enabled, but software on the switch detects an error situation on the port, the software shuts down that port. In other words, the port is automatically disabled by the switch operating system software because of an error condition that is encountered on the port.

When a port is error disabled, it is effectively shut down and no traffic is sent or received on that port. The port LED is set to the color orange.

In network err-disable recovery will be disabled.

```
errdisable recovery cause
```

5.2.4 L2 Port configuration

5.2.4.1 Access Port Configuration

```
interface Port-channel1
!
interface GigabitEthernet1/0/1
switchport mode trunk
!
interface GigabitEthernet1/0/2
switchport access vlan 10
switchport mode access
spanning-tree portfast
!
interface GigabitEthernet1/0/3
switchport access vlan 20
switchport mode access
spanning-tree portfast
!
interface GigabitEthernet1/0/4
switchport access vlan 30
switchport mode access
spanning-tree portfast
ip access-group 100 in
!
interface GigabitEthernet1/0/5
switchport access vlan 40
switchport mode access
spanning-tree portfast
!
interface GigabitEthernet1/0/6
switchport access vlan 50
switchport mode access
spanning-tree portfast
!
interface GigabitEthernet1/0/7
switchport access vlan 60
switchport mode access
spanning-tree portfast
!
interface GigabitEthernet1/0/8
switchport access vlan 70
switchport mode access
spanning-tree portfast
!
interface GigabitEthernet1/0/9
switchport access vlan 80
switchport mode access
spanning-tree portfast
!
interface GigabitEthernet1/0/10
no switchport
ip address 192.168.205.1 255.255.255.0
duplex auto
speed auto
!
interface GigabitEthernet1/0/11
!
interface GigabitEthernet1/0/12
!
interface GigabitEthernet1/0/13
!
interface GigabitEthernet1/0/14
!
interface GigabitEthernet1/0/15
!
interface GigabitEthernet1/0/16
!
interface GigabitEthernet1/0/17
!
interface GigabitEthernet1/0/18
!
interface GigabitEthernet1/0/19
!
interface GigabitEthernet1/0/20
!
interface GigabitEthernet1/0/21
channel-group 1 mode passive
!
interface GigabitEthernet1/0/22
channel-group 1 mode passive
!
interface GigabitEthernet1/0/23
channel-group 1 mode passive
!
interface GigabitEthernet1/0/24
switchport mode trunk
!
interface GigabitEthernet1/1/1
!
```

```
interface GigabitEthernet1/1/2
!
interface GigabitEthernet1/1/3
!
interface GigabitEthernet1/1/4
!
interface Vlan1
no ip address
shutdown
!
 description ***** To-ISA ****
 switchport
 switchport mode access
 switchport access vlan 4
 storm-control broadcast level 10.00
 storm-control multicast level 10.00
 spanning-tree portfast edge
 spanning-tree bpdufilter enable
 spanning-tree bpduguard enable
```

Access Port Configuration

- Portfast feature is enabled on all user and server ports to allow stable and fast L2 and spanning-tree convergence.
- Ports that are connected to the hosts are put in switchport access mode and are assigned to their corresponding Vlan using switchport commands.

5.2.4.2 Trunk port configuration

All uplink 10 gig Ethernet ports of the edge switches and the corresponding ports on the core are configured as dot1Q trunks.

All port channels are recommended to be LACP.

```
Core switch
*************
Interface range TenGigaEthernet1/1/1-2
 switchport mode trunk
 channel-group 1 mode active
 !
```

Trunk Port Configuration

5.3 Layer 3 Technologies

5.3.1 Interface VLANs

The core switch will be layer 3 termination for not all VLANs, Server VLANs will be terminated on FW.

```
Ml3sw_Core#sh interface vlan 30
```

```
Vlan30 is up, line protocol is up
Hardware is CPU Interface, address is 00e0.f7b5.2001 (bia 00e0.f7b5.2001)
MTU 1500 bytes, BW 100000 Kbit, DLY 1000000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
ARP type: ARPA, ARP Timeout 04:00:00
Last input 21:40:21, output never, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
1682 packets input, 530955 bytes, 0 no buffer
Received 0 broadcasts (0 IP multicast)
0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
563859 packets output, 0 bytes, 0 underruns
0 output errors, 23 interface resets
0 output buffer failures, 0 output buffers swapped out
*********************************************
 Ml3sw_Core#sh interface vlan1
Vlan1 is administratively down, line protocol is down
Hardware is CPU Interface, address is 00e0.f7b5.2086 (bia 00e0.f7b5.2086)
MTU 1500 bytes, BW 100000 Kbit, DLY 1000000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
ARP type: ARPA, ARP Timeout 04:00:00
Last input 21:40:21, output never, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
1682 packets input, 530955 bytes, 0 no buffer
Received 0 broadcasts (0 IP multicast)
0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
563859 packets output, 0 bytes, 0 underruns
0 output errors, 23 interface resets
0 output buffer failures, 0 output buffers swapped out
```

5.4 Wan Configuration

In this section we are going to discuss the HQ WAN Router Setup.

- Router will be connected to an OOB & FW Management switch to Fortigate.

- Router will be connected to WAN Links & Microwave.
- Internet link to be hosted directly on the Fortigate FW for better network security
- Router will act as the Voice GW and the WAN RTR

5.5 Management Technologies

5.5.1 AAA & Network Devices Access

This point discuss method will be used for securing access to network devices through usernames, passwords, controlling access line parameters, controlling remote access protocols, and affecting privileges of users and commands.

SSH will be the only enabled remote access control protocol to secure the management traffic

```
service password-encryption
!
hostname Router_Core
!
!
```

```
!
enable password 7 0822455D0A16
username admin password 7 082048430017544045
username admin15 privilege 15 secret 5 $1$mERr$4vA4HFsBWaKMIyHAaPqub.
!
!
license udi pid CISCO2911/K9 sn FTX1524I6GZ-
banner motd ^CNO Unauthorized Access!!^C
!
!
!
!
line con 0
password 7 0822455D0A16
login
!
line aux 0
!
line vty 0 4
login local
transport input ssh
!
!
ntp authentication-key 1 md5 0822455D0A16 7
ntp trusted-key 1
ntp server 20.0.0.6 key 1
!
```

Local Users and SSH Configuration

```
service password-encryption
!
username admin privilege 15 secret Cisco_123
!
 aaa new-model
!
aaa authentication login CONS local
aaa authorization exec default local
line con 0
password 7 0822455D0A16
login
!
line aux 0
!
line vty 0 4
login local
transport input ssh
```

AAA Configuration

5.5.2 EIGRP

EIGRP (Enhanced Interior Gateway Routing Protocol) is a Cisco proprietary routing protocol that uses a distance vector routing algorithm, enhanced with features of link-state protocols. It is designed for efficiency, scalability, and rapid convergence in large networks.

```
Router_Core#show ip eigrp topology
IP-EIGRP Topology Table for AS 5/ID(192.168.207.1)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
r - Reply status

P 10.10.10.0/30, 1 successors, FD is 2169856
via Connected, Serial0/2/1
P 10.10.10.4/30, 1 successors, FD is 2169856
via Connected, Serial0/2/0
P 20.0.0.4/30, 7 successors, FD is 30976
via 192.168.4.50 (30976/5376), GigabitEthernet0/0.40
via 192.168.3.50 (30976/5376), GigabitEthernet0/0.30
via 192.168.5.50 (30976/5376), GigabitEthernet0/0.50
via 192.168.8.50 (30976/5376), GigabitEthernet0/0.80
via 192.168.2.50 (30976/5376), GigabitEthernet0/0.20
via 192.168.1.50 (30976/5376), GigabitEthernet0/0.10
via 192.168.6.50 (30976/5376), GigabitEthernet0/0.60
via 10.10.10.6 (2172416/5120), Serial0/2/0
via 10.10.10.2 (2172928/5632), Serial0/2/1
P 66.0.0.0/30, 7 successors, FD is 28416
via 192.168.4.50 (28416/2816), GigabitEthernet0/0.40
via 192.168.3.50 (28416/2816), GigabitEthernet0/0.30
via 192.168.5.50 (28416/2816), GigabitEthernet0/0.50
via 192.168.8.50 (28416/2816), GigabitEthernet0/0.80
via 192.168.2.50 (28416/2816), GigabitEthernet0/0.20
via 192.168.1.50 (28416/2816), GigabitEthernet0/0.10
via 192.168.6.50 (28416/2816), GigabitEthernet0/0.60
via 10.10.10.2 (2170112/2816), Serial0/2/1
via 10.10.10.6 (2170368/3072), Serial0/2/0
P 66.0.0.4/30, 7 successors, FD is 28416
via 192.168.4.50 (28416/2816), GigabitEthernet0/0.40
via 192.168.3.50 (28416/2816), GigabitEthernet0/0.30
via 192.168.5.50 (28416/2816), GigabitEthernet0/0.50
via 192.168.8.50 (28416/2816), GigabitEthernet0/0.80
via 192.168.2.50 (28416/2816), GigabitEthernet0/0.20
via 192.168.1.50 (28416/2816), GigabitEthernet0/0.10
via 192.168.6.50 (28416/2816), GigabitEthernet0/0.60
via 10.10.10.6 (2170112/2816), Serial0/2/0
via 10.10.10.2 (2170368/3072), Serial0/2/1
P 192.168.1.0/24, 1 successors, FD is 28160
via Connected, GigabitEthernet0/0.10
P 192.168.2.0/24, 1 successors, FD is 28160
via Connected, GigabitEthernet0/0.20
P 192.168.3.0/24, 1 successors, FD is 28160
via Connected, GigabitEthernet0/0.30
P 192.168.4.0/24, 1 successors, FD is 28160
via Connected, GigabitEthernet0/0.40
P 192.168.5.0/24, 1 successors, FD is 28160
via Connected, GigabitEthernet0/0.50
P 192.168.6.0/24, 1 successors, FD is 28160
via Connected, GigabitEthernet0/0.60
P 192.168.7.0/24, 1 successors, FD is 28160
via Connected, GigabitEthernet0/0.70
P 192.168.8.0/24, 1 successors, FD is 28160
via Connected, GigabitEthernet0/0.80
P 192.168.9.0/24, 7 successors, FD is 30976
via 192.168.4.50 (30976/28416), GigabitEthernet0/0.40
via 192.168.3.50 (30976/28416), GigabitEthernet0/0.30
via 192.168.5.50 (30976/28416), GigabitEthernet0/0.50
via 192.168.8.50 (30976/28416), GigabitEthernet0/0.80
via 192.168.2.50 (30976/28416), GigabitEthernet0/0.20
via 192.168.1.50 (30976/28416), GigabitEthernet0/0.10
via 192.168.6.50 (30976/28416), GigabitEthernet0/0.60
via 10.10.10.2 (2172416/28160), Serial0/2/1
via 10.10.10.6 (2172928/28672), Serial0/2/0
P 192.168.10.0/24, 7 successors, FD is 30976
via 192.168.4.50 (30976/28416), GigabitEthernet0/0.40
via 192.168.3.50 (30976/28416), GigabitEthernet0/0.30
via 192.168.5.50 (30976/28416), GigabitEthernet0/0.50
via 192.168.8.50 (30976/28416), GigabitEthernet0/0.80
via 192.168.2.50 (30976/28416), GigabitEthernet0/0.20
via 192.168.1.50 (30976/28416), GigabitEthernet0/0.10
via 192.168.6.50 (30976/28416), GigabitEthernet0/0.60
via 10.10.10.2 (2172416/28160), Serial0/2/1
via 10.10.10.6 (2172928/28672), Serial0/2/0
```

SNMP Configuration

5.5.3 Disable unneeded services

Disable Services that may be Involve Security risks as Bootp server, pad service, http server, https server and finger service.

```
service timestamps debug datetime msec local show
service timestamps debug datetime msec local time
service timestamps log datetime msec local  show
service timestamps log datetime msec local  time
logging buffered 32768 debugging
service tcp-keepalives-in
service tcp-keepalives-out
no service tcp-small-servers
no service udp-small-servers
no logging console
no ip http access-class
no service finger
no service pad
no ip domain-lookup
no ip http server
no ip https server
```

Disable Unneeded Services

5.5.4 Banner

Banner message used to display a security warning for any one try to access network devices.

```
************************************************************************
banner motd ^CNO Unauthorized Access!!^C
************************************************************************
```

Banner Configuration

5.5.5 NTP and time

It is often extremely useful to be able to accurately pinpoint when a particular event occurred. You may want to compare network event messages from various routers on your network for fault isolation, troubleshooting, and security purposes. This is impossible if their clocks are not set to a common source. In fact, the problem is even worse than merely setting the clocks to a single common standard because some clocks run a little bit fast and others run a little bit slow. So they need to be continuously adjusted and synchronized.

Network Time Protocol (NTP) is a standard for protocol which we can use to achieve the previous requirements.

```
Router_Core#show running-config | include ntp
ntp authentication-key 1 md5 0822455D0A16 7
ntp trusted-key 1
ntp server 20.0.0.6 key 1
```

NTP Configuration

5.5.6 Logging

Logging is critical for fault notification, network forensics, and security auditing. Cisco equipment handles log messages in following ways:

- By default, the router sends all log messages to its console port. Only users that are physically connected to the router console port may view these messages, though. This is called console logging.
- Terminal logging is similar to console logging, but it displays log messages to the router’s VTY lines instead. This type of logging is not enabled by default, so if you want to use it, you need to need activate it for each required line.
- Buffered logging creates a circular buffer within the router’s RAM for storing log messages. This circular buffer has a fixed size to ensure that the log will not deplete valuable system memory. The router accomplishes this by deleting old messages from the buffer as new messages are added.
- The router can use syslog to forward log messages to external syslog servers for centralized storage. This type of logging is not enabled by default.

```
line con 0
password 7 0822455D0A16
login
!
line aux 0
!
line vty 0 4
login local
transport input ssh
!
```

Logging Configuration