Toms Documentations

Part 1: Identify Network Details

- **IP Schemes**

10.40.0.0/16	NW Addr	Broadcast	Subnet	VLAN ID - Desc
10.40.200.0	10.40.200.0	10.40.200.255	255.255.255.0	2 – VOIP
10.40.0.0/23	10.40.0.0	10.40.1.255	255.255.254.0	10 - STAFF
10.40.2.0/24	10.40.2.0	10.40.2.255	255.255.255.0	20 – Management
10.40.254.0/24	10.40.254.0	10.40.254.255	255.255.255.0	99 – NWK Admin
10.40.0.0/16	N/A	N/A	N/A	100 - Native
10.40.253.0/24	10.40.253.0	10.40.253.255	255.255.255.0	N/A - External Network for services

- **Network VLANs**

VLAN ID	Subnet Mask / Network IDs
2	10.40.200.0/24
10	10.40.0.0/23
20	10.40.2.0/24
99	10.40.254.0/24
100	Native

- **DHCP scheme**

Network Address	Subnet Mask	Gateway	Range	DNS
10.40.0.0	255.255.254.0	10.40.0.1	10.40.0.2 - 10.40.1.254	10.40.254.2
10.40.2.0	255.255.255.0	10.40.2.1	10.40.2.2 - 10.40.2.254	10.40.254.2
10.40.200.0	255.255.255.0	10.40.200.1	10.40.200.10-240	N/A

- **VOIP scheme**

  VLAN 200 assigned to VOIP Voice with DHCP - See Observation

- **Routing scheme**

Destination IP	Subnet Mask	Gateway	Interface
0.0.0.0	0.0.0.0	10.40.0.1	G0/1.10
0.0.0.0	0.0.0.0	10.40.2.1	G0/1.20
10.40.254.0	255.255.255.0	10.40.0.1,10.4.2.1	Any inside NAT

- **OSPF**

Neighbor ID	Priority	Address	Interface
10.0.0.1	Area 0	172.40.1.1	Loopback 1
10.0.0.2	Area 0	172.40.1.2	Loopback 1

- **BGP**

Network	Next Hop	Advertising
BGP 40	BGP30, BGP10	4.4.4.4/30

- **Tunnel scheme**

Interface	IP Address	Protocol
Router 3, Tunnel1	34.34.34.2/30	GRE + IPSEC
Router 3, Tunnel2	14.14.14.1/30	GRE + IPSEC

- **End Hosts IPs**

Hosts	IP Address	Roles
Proxmox	10.40.254.3	VM Hypervisor
PiHole DNS	10.40.254.2	DNS
Windows 10	10.40.254.167	Syslog, SNMP, Netflow
Windows Server	10.40.254.166	Domain, Sites + Replication

- **ACLs**

Allow/Deny	To	From	Protocol/Stack
allow	10.4.0.254.2/32	10.40.0.0/22	UDP/TCP, Port 53, DNS
deny	10.40.254.0/24	10.40.0.0/22	Any, any

- **Backup**
  - **Every night at 23:00 backup each Proxmox VM/instance to remote site and locally**
  - **First sunday of every month backup Proxmox VM/instance to remote site and locally**

==========

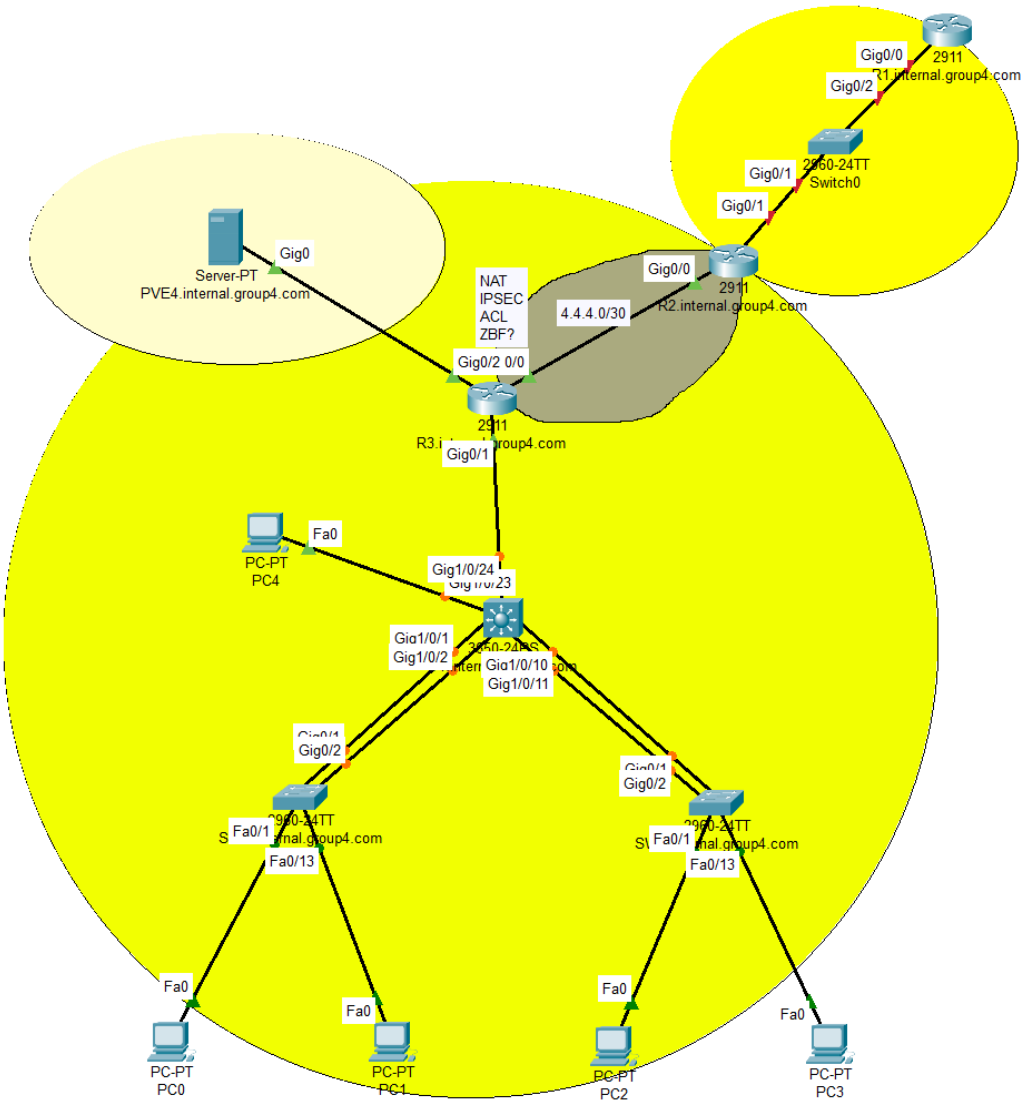
Part 2: Network Design and Diagram

- **Graphs**

- **ISP design**

    - External BGP (eBGP) Configuration :
        - R1 has an eBGP configuration with a neighbor at IP address 34.34.34.1 and a different ASN 30. This suggests that R1 is also peering with an external BGP router, representing a connection to an ISP or another external network.
    - Internal BGP (iBGP) Configuration:
        - In both routers, there's a BGP configuration with the same autonomous system number (ASN) 40, indicating that these routers are part of the same BGP autonomous system.
        - The BGP neighbors are configured using the loopback addresses of the other router (i.e., R1 has R2's loopback as a neighbor and vice versa). This iBGP peering allows for the exchange of routing information between R1 and R2.
        - The update-source Loopback1 command ensures that BGP updates are sourced from the loopback interface, which aids in maintaining a stable BGP session even if there are changes in the network topology.
    - Loopback Interfaces:
        - Both R1 and R2 have loopback interfaces configured with IP addresses 172.40.1.1 and 172.40.1.2 respectively. Loopback interfaces are software interfaces, so they remain up and operational as long as the router is functioning, making them reliable endpoints for iBGP peering.
    - IP OSPF Configuration:
        - Both R1 and R2 are configured with OSPF to manage routing within their autonomous system. This OSPF configuration includes associating the loopback and GigabitEthernet interfaces with OSPF Area 0.

- **LAN design**
    - **Logical**



==========

Part 3: Devices and Configuration

Device: Router 1			
Port	**IP Address**	**Subnet**	**Security Mode**
Gigabit-0/0	10.0.0.1	255.255.255.0	N/A
Loopback1	172.40.1.1	255.255.255.0	N/A

```
!--------------------------------------------
! This is the config for Router 1
! with the connection for bgp
! and loopbacks
! Copy everything in box and paste into CLI with Shift + Insert
!--------------------------------------------

!Initial configuration configuring hostname domain username and passwords

conf t
hostname R1
ip domain-name internal.tom.com
!used for SSH and DNS
ip name-server 10.40.253.99
!DNS Server ip address
ip domain lookup
!enable DNS lookups
!set username and passwords
username tom password cisco123
enable password cisco123

!---------

!create loopback1

interface Loopback1
ip address 172.40.1.1 255.255.255.0
ip ospf 1 area 0

!---------

!create g0/0
!to R2
interface GigabitEthernet0/0
ip address 10.0.0.1 255.255.255.0
ip ospf 1 area 0
```

```
!---------

!create ospf routing

router ospf 1
router-id 10.0.0.1

!---------

router bgp 40
bgp log-neighbor-changes
neighbor 172.40.1.2 remote-as 40
neighbor 172.40.1.2 description ibgp with r2
neighbor 172.40.1.2 update-source Loopback1
neighbor 34.34.34.1 remote-as 30
network 34.34.34.0 mask 255.255.255.252
distance bgp 200 200 200
```

Device: Router 2

Port	IP Address	Subnet	Security Mode
Gigabit-0/0	10.0.0.2	255.255.255.0	N/A
Gigabit-0/1	4.4.4.1	255.255.255.252	N/A
Loopback1	172.40.1.2	255.255.255.0	N/A

```
!-------------------------------------------
! This is the config for Router 2
! with the connection for bgp
! and loopbacks
! Copy everything with Control+A and paste into CLI
!-------------------------------------------

!initial configuration configuring hostname domain username and passwords

conf t
hostname R2
ip domain-name internal.tom.com
```

```
!used for SSH and DNS
ip name-server 10.40.253.99
!DNS Server ip addr
ip domain lookup
!enable DNS lookups
!set username and passwords
username tom password cisco123
enable password cisco123

!---------

!create loopback1

interface Loopback1
ip address 172.40.1.2 255.255.255.0
ip ospf 1 area 0

!---------

!create g0/0

!to R1
interface GigabitEthernet0/0
ip address 10.0.0.2 255.255.255.0
ip ospf 1 area 0
no shut

!---------

!create g0/1 to internal router

interface g0/1
ip addr 4.4.4.1 255.255.255.252
no shutdown

!create ospf routing

router ospf 1
router-id 10.0.0.2

!---------

router bgp 40
bgp log-neighbor-changes
neighbor 172.40.1.1 remote-as 40
neighbor 172.40.1.1 description ibgp with r2
neighbor 172.40.1.1 update-source Loopback1
distance bgp 200 200 200
```

Device: Router 3			
Port	**IP Address**	**Subnet**	**Security Mode**
Gigabit-0/0	4.4.4.2	255.255.255.252	N/A
Gigabit-0/1	4.4.4.1	255.255.255.0	N/A
Gigabit-0/1.2	10.40.200.0	255.255.255.0	Virtual
Gigabit-0/1.10	10.40.0.0	255.255.254.0	Virtual
Gigabit-0/1.20	10.40.2.0	255.255.255.0	Virtual
Gigabit-0/1.99	10.40.254.0	255.255.255.0	Virtual
Gigabit-0/1.100	Native	Native	Virtual
Gigabit-0/2	10.40.253.0	255.255.255.0	N/A

```
!--------------------------------------------
! This is the config for Router 3
! with the connection for each VLAN inside
! plus the proxmox server
! Copy everything with Control+A and paste into CLI
!--------------------------------------------

!initial configuration configuring hostname domain username and passwords

conf t
hostname R3
ip domain-name internal.tom.com
!used for SSH and DNS
ip name-server 10.40.254.99
!DNS Server ip addr
ip domain lookup
!enable DNS lookups
!set username and passwords
username tom password cisco123
enable password cisco123


!create nat + access-list for NAT
```

```
access-list 101 permit ip any any

ip nat inside source list 101 interface g0/0 overload

!creating sub interfaces for each VLAN and setting G0/2 to bridge group 99 + local OSPF ------- Please check the cables are correct physically

!create server network so ospf does not complain
interface g0/2
ip addr 10.40.253.1 255.255.255.0
ip nat inside
no shutdown
!--------

!create g0/0 to R2
int g0/0
ip addr 4.4.4.2 255.255.255.252
ip nat outside
no shutdown
!--------

!create OSPF process
router ospf 1
router-id 10.40.254.3
!--------

!set server network into ospf
interface g0/2
ip ospf 1 area 1
!--------

!set main int up
interface g0/1
no shutdown
!--------

!vlan 2 VOIP
interface g0/1.2
encapsulation dot1q 2
!no shutdown
ip address 10.40.200.1 255.255.255.0
ip nat inside
no shutdown
!--------

!vlan 10 STAFF
interface g0/1.10
encapsulation dot1q 10
ip address 10.40.0.1 255.255.254.0
ip ospf 1 area 1
```

```
ip nat inside
no shutdown
!--------

!vlan 20 MANAGEMENT
interface g0/1.20
ip address 10.40.2.1 255.255.255.0
ip ospf 1 area 1
encapsulation dot1q 20
ip nat inside
no shutdown
!--------

!vlan 99 NETMGN
interface g0/1.99
encapsulation dot1q 99
ip address 10.40.254.3 255.255.255.0
ip nat inside
no shutdown
!--------

int g0/1.100
encapsulation dot1q 100 native
no shutdown



!create dhcp pools for each ip addr range

ip dhcp pool VLAN10
network 10.40.0.0 255.255.254.0
default-router 10.40.0.1
dns-server 10.40.253.2 !---------------- Change depending on real world and PT

ip dhcp pool VLAN20
network 10.40.2.0 255.255.255.0
default-router 10.40.2.1
dns-server 10.40.253.2 !---------------- Change depending on real world and PT

ip dhcp pool VOIP
network 10.40.200.0 255.255.255.0
default-router 10.40.200.1
dns-server 10.40.253.2 !---------------- Change depending on real world and PT

ip dhcp excluded-address 10.40.2.1 10.40.0.1 10.40.200.1


!set SSH --------------------------

!domain-name set at start
```

```
crypto key generate rsa modulus 1024
!or
!crypto key generate rsa


line vty 0 4
transport input ssh
login local


!create tunnel to AS30

interface tunnel 3
ip add 172.40.30.1 255.255.255.252
tunnel destination 3.3.3.2
tunnel source 4.4.4.2
ip mtu 1400
ip tcp adjust-mss 1360

exit

!setup radius
aaa new-model
aaa authentication login vty-lines group radius
aaa authorization exec default group radius local
aaa accounting exec default start-stop group radius
radius server radius
address ipv4 10.40.254.167 auth-port 1812 acct-port 1813
key tom
```

Device: Distribution 1			
Port/Interface	**IP Address/VLAN**	**Subnet**	**Security Mode**
Port-channel-1	Trunk	N/A	N/A
Port-channel-2	Trunk	N/A	N/A
VLAN 99	10.40.254.11	255.255.255.0	N/A
!----------			

```
! This is the config for Distrib 1
! with the connection for each VLAN inside
! plus the proxmox server
! Copy everything with Control+A and paste into CLI
!-------------------------------------------

!initial configuration configuring hostname domain username and passwords

conf t
hostname D1
ip domain-name internal.tom.com
!used for SSH and DNS
ip name-server 10.40.253.99
!DNS Server ip addr
ip domain lookup
!enable DNS lookups
!set username and passwords
username tom password cisco123
enable password cisco123

!---------

!create VLAN 2 VOIP

vlan 2
name VOIP

!create VLAN 10 STAFF

vlan 10
name STAFF
!--------

!create VLAN 20 Managment

vlan 20
name MANAGEMENT
!--------

!create VLAN 99 Network Management

vlan 99
name NETMGN
!--------

!create VLAN 100

vlan 100
name tnative
!--------
```

```
!exit from vlan configs
exit
!--------

!set vlan 99 ip addr ---------- change between configs - currently D1
interface vlan 99
ip address 10.40.254.11 255.255.255.0

!create port channel 1 - g1/0/1-2 to trunk and port channel 1 to sw1

interface port-channel 1
switchport trunk allowed vlan 2-99
switchport trunk native vlan 100
switchport trunk encapsulation dot1q
switchport mode trunk
exit
interface range g1/0/1-2
switchport trunk allowed vlan 2-99
switchport trunk native vlan 100
switchport trunk encapsulation dot1q
switchport mode trunk
no shutdown
channel-group 1 mode active

!using lacp - set to passive so layer 3 switch can enable lacp


!create port channel 2 - g1/0/13-14 to trunk and port channel 2 to sw2

interface port-channel 2
switchport trunk allowed vlan 2-99
switchport trunk native vlan 100
switchport trunk encapsulation dot1q
switchport mode trunk
exit
interface range g1/0/13-14
switchport trunk allowed vlan 2-99
switchport trunk native vlan 100
switchport trunk encapsulation dot1q
switchport mode trunk
no shutdown
channel-group 2 mode active

!using lacp - set to passive so layer 3 switch can enable lacp

interface g1/0/24
switchport trunk allowed vlan 2-99
switchport trunk native vlan 100
switchport trunk encapsulation dot1q
```

```
switchport mode trunk
no shutdown


int g1/0/12
switchport mode access
switchport access vlan 2
no shut
exit

!setup radius
aaa new-model
aaa authentication login vty-lines group radius
aaa authorization exec default group radius local
aaa accounting exec default start-stop group radius
radius server radius
address ipv4 10.40.254.167 auth-port 1812 acct-port 1813
key tom
```

Device: Switch 1			
Port/Interface	**IP Address/VLAN**	**Subnet**	**Security Mode**
Fast Eth 0/13-24	VLAN20	N/A	switchport port-security maximum 3
Fast Eth 0/1-12	VLAN10	N/A	switchport port-security maximum 3
Port-channel-1	Trunk	N/A	N/A

```
!Configuring hostname and DNS lookup for each device - change here when required between configs

conf t
hostname SW1
ip domain-name internal.tom.com
!used for SSH and DNS
ip name-server 10.40.253.99
!DNS Server ip addr
ip domain lookup
!enable DNS lookups
logging 10.40.253.167
logging on
```

```
username tom password cisco123

enable password cisco123

!create VLAN 2 VOIP

vlan 2
name VOIP

!create VLAN 10 STAFF

vlan 10
name STAFF
!--------

!create VLAN 20 Managment

vlan 20
name MANAGEMENT
!--------

!create VLAN 99 Network Management

vlan 99
name NETMGN
!--------

!create VLAN 100

vlan 100
name tnative
!--------

!exit from vlan configs
exit
!--------

!set ports to vlan 10

int range fa0/1-12
switchport access vlan 10
switchport port-security maximum 3
exit
!--------

!set ports to vlan 20

int range fa0/13-24
switchport access vlan 20
switchport port-security maximum 3
```

```
!--------

!set vlan 99 ip addr ---------- change between configs - currently SW1

interface vlan 99
ip address 10.40.254.21 255.255.255.0

!--------

!exit from vlans
exit
!--------

!create port channel 1 - g0/1-2 to trunk and port channel 1  ---------- change between configs - currently SW1

interface port-channel 1
exit
interface range g0/1-2
switchport trunk allowed vlan 2-99
switchport trunk native vlan 100
!switchport trunk encapsulation dot1q
channel-group 1 mode passive

!using lacp - set to passive so layer 3 switch can enable lacp

!--------

!set SSH

!domain-name set at start

crypto key generate rsa modulus 1024
!or
!crypto key generate rsa
line vty 0 4
transport input ssh
login local
exit

!setup radius
aaa new-model
aaa authentication login vty-lines group radius
aaa authorization exec default group radius local
aaa accounting exec default start-stop group radius
radius server radius
address ipv4 10.40.254.167 auth-port 1812 acct-port 1813
key tom
```

Device: Switch 1			
Port/Interface	**IP Address/VLAN**	**Subnet**	**Security Mode**
Fast Eth 0/13-24	VLAN20	N/A	switchport port-security maximum 3
Fast Eth 0/1-12	VLAN10	N/A	switchport port-security maximum 3
Port-channel-1	Trunk	N/A	N/A

```
!Configuring hostname and DNS lookup for each device - change here when required between configs

conf t
hostname SW2
ip domain-name internal.tom.com
!used for SSH and DNS
ip name-server 10.40.253.99
!DNS Server ip addr
ip domain lookup
!enable DNS lookups
logging 10.40.253.167
logging on

username tom password cisco123

enable password cisco123

!create VLAN 2 VOIP

vlan 2
name VOIP

!create VLAN 10 STAFF

vlan 10
name STAFF
!--------

!create VLAN 20 Managment

vlan 20
name MANAGEMENT
!--------
```

```
!create VLAN 99 Network Management

vlan 99
name NETMGN
!--------

!create VLAN 100

vlan 100
name tnative
!--------

!exit from vlan configs
exit
!--------

!set ports to vlan 10

int range fa0/1-12
switchport access vlan 10
switchport port-security maximum 3
exit
!--------

!set ports to vlan 20

int range fa0/13-24
switchport access vlan 20
switchport port-security maximum 3
!--------

!set vlan 99 ip addr ---------- change between configs - currently SW2

interface vlan 99
ip address 10.40.254.22 255.255.255.0

!--------

!exit from vlans
exit
!--------

!create port channel 1 - g0/1-2 to trunk and port channel 1  ---------- change between configs - currently SW1

interface port-channel 1
exit
interface range g0/1-2
switchport trunk allowed vlan 2-99
switchport trunk native vlan 100
```

```
!switchport trunk encapsulation dot1q
channel-group 1 mode passive

!using lacp - set to passive so layer 3 switch can enable lacp

!--------

!set SSH

!domain-name set at start

crypto key generate rsa modulus 1024
!or
!crypto key generate rsa
line vty 0 4
transport input ssh
login local
exit

!setup radius
aaa new-model
aaa authentication login vty-lines group radius
aaa authorization exec default group radius local
aaa accounting exec default start-stop group radius
radius server radius
address ipv4 10.40.254.167 auth-port 1812 acct-port 1813
key tom
```

==========

Part 4: Security Policy

- **Risk assessment**

Threat	Vulnerability	Control	Likelihood	Impact	Risk
Unauthorized access	Weakness Password	Using strong password/ authentication control	Moderate	Major	High
Hardware Failure	Overheated Malfunction cable Old equipement	Set a proper airflow Keep maintenance all cable and devices	Moderate	Severe	Very High

Human Error	Wrong configuration Wrong setup physical devices	Provide a manual sheet and work instruction	Moderate	Minor/Significant	Medium
Malware	Infected by attachment, email or files	Keep system/devices updated, Use a security software to prevent and alert when found a suspicious files	Moderate	Major	High
Natural Disaster	Flood, fire, lightning, earthquake	Use DR/BCP plan	Rare	Severe	Medium
Network Failure	Route leaks/ route hijacks, route instability/ DDos/ Compromised	Create loopback Use Wireshark Always backup configuration files	Likely	Minor/Significant	Medium/High

- **Risk Mitigation Strategies**

Before starting a risk mitigation strategy, an Information Technology team should conduct a risk assessment on the project before implementation. This will ensure potential gaps in the project are identified and security controls can be put in place.

Some components that are implemented in the design have potential risks that will require some mitigation to be put into place; below will include some of these main components:

OSPF

One issue that OSPF routing protocols have is that they can be easily compromised. This is especially dangerous as the compromises usually go undetected. The integrity of the project's routing domain depends on the security of the least secure router in the domain. By using a single router in the OSPF section of the network, the control of the whole network can be compromised.

The solution to the above is using a tool to monitor routers joining the OSPF neighboring such as LogRhythm or WireShark which showcases visibility of risks, threats and operational issues that might have gone undetected otherwise.

BGP

Potential security risks with BGP that can occur include, route leaks, which happens when a router advertises routes that are incorrect. Another risk could be route hijacks, whereby a router

advertises routes that are more attractive than legitimate ones. Lastly, route instability occurs when a router changes routes frequently or withdraws them without probable reason.

Some strategies for defending BGP in a network from hijacking include, using IP address prefix filtering which blocks inbound network traffic from networks that are controlled by malicious users. Another strategy could be to deploy BGP detection whereby operators can monitor the network latency, performance and failed packet deliveries to identify BGP hijack attempts.

VOIP

The most common security risks that are associated with VOIP in the network design could be DDoS attacks. This occurs when users overwhelm the server with unwanted data to use all available bandwidth. In the case with VOIP, this can mean the inability to make or receive calls and worse case, admin controls would no longer be available.

A possible solution from a potential DDoS attack on the VOIP component of the network design could be to use some basic measures such as changing the password of the admin controls regularly and closely monitoring the phone system. This will help to quickly identify and mitigate the potential consequences from this common risk.

Malware

Malware is seen as any malicious software that is able to run on the systems a part of the network design which causes harm and interrupts business continuity.

Some preventative measures that can be taken to lessen the likelihood of malware could be to filter and allow file types that are safe to receive, actively monitor the network traffic (packets, inbound and outbound), and using internet security gateways that can inspect certain protocols including some encrypted protocols.

Network Failure

If the network were to fail due to various reasons, this can leave the design vulnerable when it is regarding the security of the network. Network downtime can have negative consequences in regards to attacks (DDoS, Malware, Ransomware, etc.) as this allows opportunities to steal data and perform damaging acts.

To mitigate this, implement some redundancy and backup systems (backup power supplies, redundant network paths, failover mechanisms) which will help to minimize downtime which inturn will mitigate vulnerabilities and improve business continuity.

Natural Disaster

Natural disasters such as floods, fires, lightning, etc. can create opportunities for potential attacks to occur within the network. Like stated above, natural disasters can cause network downtime which allows unwanted users to access and perform malicious activities.

Similarly to the above, installing and implementing backup systems such as power supplies to the network will ensure that in the case of a network failure due to nature, the system can be operational, preventing gaps and opportunities to breach.

Hardware Failure

Hardware plays a vital role in the network's infrastructure as it is the backbone for all controls within the design. For example, if a server were to become inoperational, this will have drastic effects on business continuity and will provide risks towards data.

To ensure this can be mitigated, updating the hardware of the network will ensure that failure will be less likely. Outdated hardware is typically unable to contain the latest security measures, thus updating it will prevent network security risks. Keeping software updated on the hardware will ensure that the latest security measures are installed (if supported), allow hardware to perform faster, protect data and keep backdoors closed to unwanted users.

Unauthorized Access

Once an individual has gained unauthorized access to data or computer networks, they can cause numerous damages. They may steal data, files, destroy information or sabotage other systems that are critical to business continuity.

Some ways to prevent unauthorized access could be to use multi-factor authentication. This prevents unauthorized users from accessing the data as it requires an additional verification step. For example, using secret classes in Cisco related products (routers, switches). Another way to mitigate this risk is to monitor user activity. This can help to detect and prevent prohibited access and potential security breaches. There are tools in place such as Cisco Secure Network Analytics to create custom alerts to detect unauthorized access.

- Screenshots

Radius Server clients

```
client SW1 {
        ipaddr = 10.40.254.21
        secet = group4
        nastype = cisco
}
client SW2 {
        ipaddr = 10.40.254.22
        secret = group4
        nastype = cisco
}
client D1 {
        ipaddr = 10.40.254.11
        secret = group4
        nastype = cisco
}
client R3 {
        ipaddr = 10.40.254.3
        secret = gtroup4
        nastype = cisco
}
client R2 {
        ipaddr = 10.40.254.2
        secret = group4
        nastype = cisco
}
client R1 {
        ipaddr = 10.40.254.1
        secret = group4
        nastype = cisco
}
```

Login User

```
admin   Cleartext-Password := group4
        Cisco-AVPair = "shell:priv-lvl=15"
```