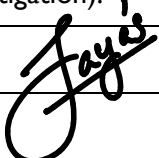


Canterbury Institute of Management (CIM)

ASSESSMENT COVER SHEET



1. Personal Details			
Student ID	Given Name(s)	Surname	Email Address
I. CIM12137	Ayesh Chathuranga	Jayasekara	cim12137@ciom.edu.au
Campus	Darwin Campus		
Course Title and Code	MBIS404 Networks and Communications		
Assessment Title	Assesment Task - Week 8		
Due Date & Time	24/11/2024		
Course Lecturer/Tutor Name: Sharad Neupane		Assessment Word Count (if applicable): 848	
2. Student Declaration			
<p>By signing and submitting this coversheet, I/we declare that:</p> <ul style="list-style-type: none"> ✓ This assessment submission is my/our own work unless otherwise acknowledged (including the use of generative AI tools) and is in accordance with the Institute's Academic Integrity and Honesty Policy available on the website. ✓ No part of this assessment has been submitted previously for advanced standing or academic credit in this or any other course. ✓ I/we certify that we have not given a copy or have shown a copy of this assessment item to another student enrolled in the course, other than members of this group. ✓ I/we are aware that the Lecturer/Tutor of this assessment may, for the purpose of assessing this assessment task communicate a copy of this assessment task to a plagiarism checking service to detect possible breaches of academic integrity, for example, plagiarism, recycling, cheating, contract cheating, or unauthorised use of generative AI (which may then retain a copy of the item on its database for the purpose of future investigation). 			
Signature:			Date: 23/11/24

Designing & Implementing a simple network

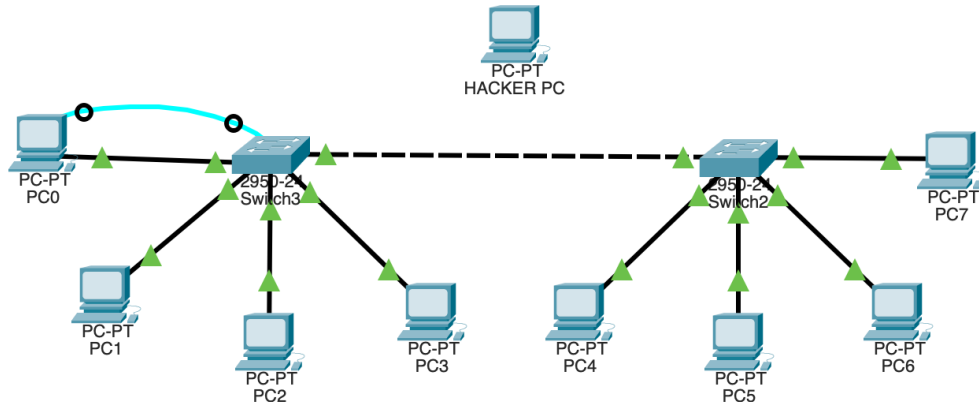


Figure 1: Network Overview

Following steps are followed when creating this network.

1. Select 2 switches and connect them on Fa0/1 on each switch which will be used as the trunk
2. Set hostnames for switches
3. Create 2 VLANs
4. Assign 2 end devices to each VLAN at each switch
5. Assign DHCP policy to assign IP addresses for each host
6. Configure port security to allow only known mac address for each port
7. Validate the configuration

Since configuring two switches involves identical commands being issued, configuration of one switch is demonstrated in this report.

There are two main configurations of Cisco devices: the startup-config and the running-config. The startup-config is the configuration that is loaded when the Cisco device is booted; it is located in the NVRAM. The running-config is the current configuration running on the router, located in the RAM.

(Carthern et al., [2021](#))

1. SETTING HOSTNAME FOR SWITCH

1 Setting *hostname* for switch

A hostname makes identification easier when the network complexity is evolving.

```
1 enable
2 conf t
3 hostname CIM12137-SW-1
4
```

Listing 1: Setting up hostname for switch

2 Creating two VLANs for each department

VLANs helps to logically separate the locale area networks to help achieve better security and management options. In this example two VLANs are created for Department A & B VLAN 10 & VLAN 20 assigned respectively.

```
1 enable
2 conf t
3 vlan 10
4 name Department_A
5 exit
6 vlan 20
7 name Department_B
8 exit
9
```

Listing 2: Creating two VLANs

Allocating switch ports to respective VLAN clients

This example has two clients per VLAN on each switch.

1. Department A - VLAN 10 - Fa0/2-3
2. Department B - VLAN 20 - Fa0/4-5

```
1 interface range fastethernet0/2 - 3
2 switchport mode access
3 switchport access vlan 10
4 exit
5 interface range fastethernet0/4 - 5
6 switchport mode access
7 switchport access vlan 20
8 exit
9
```

Listing 3: Assigning ports to VLANs

3. COMMUNICATION BETWEEN SWITCHES - TRUNK

3 Communication between switches - Trunk

In order for two switches to communicate a trunk port must be assigned so that traffic is carried from one switch to the other using this port. It must be noted that, if single trunk is used, it becomes a single point-of-failure resulting in total collapse of network. And due to increased loads usually fastest ports are chosen as trunk port, however in this example regular port was used for brevity.

```
1 interface fastethernet0/1
2 switchport mode trunk
3 switchport trunk allowed vlan 10,20
4 exit
5
```

Listing 4: Assigning trunk port for both VLANs

4 Assigning IPV4 ranges for each department

Each end device connecting to this network must have a IP address in order to communicate with each other. In this network DHCP protocol is configured for each VLAN.

1. Department A - VLAN 10–192.168.10.1/24
2. Department B - VLAN 20–192.168.20.1/24

```
1 interface vlan 10
2 ip address 192.168.10.1 255.255.255.0
3 no shutdown
4 exit
5 interface vlan 20
6 ip address 192.168.20.1 255.255.255.0
7 no shutdown
8 exit
9
```

Listing 5: Assigning IP ranges for both VLANs

5 Configuring DHCP Protocol

Dynamic Host Configuration Protocol defines algorithms to automatically allocate IP address to host devices avoiding collisions.

6. CONFIGURING SWITCH PORT SECURITY

```
1 ip dhcp excluded-address 192.168.10.1 192.168.10.10
2 ip dhcp excluded-address 192.168.20.1 192.168.20.10
3
```

Listing 6: Defining IP Pools for DHCP usage

Once the pools are defined, these pools must be allocated for each VLAN respectively.

```
1 ip dhcp pool VLAN10
2 network 192.168.10.0 255.255.255.0
3 default-router 192.168.10.1
4 exit
5 ip dhcp pool VLAN20
6 network 192.168.20.0 255.255.255.0
7 default-router 192.168.20.1
8 exit
9
```

Listing 7: Defining IP Pools for DHCP usage

At this point, all the connected end devices will be assigned IP addresses in their respective ranges depending on the VLAN. The communication link between hosts are successfully established as a result. (*See later sections for screen captures*).

6 Configuring switch port security

It is important that we make sure only known hosts are admitted in to the network. To limit unauthorized access, we can configure the switch to cross-check host MAC (*Media Access Control*) address is whitelisted. Here is a sample for securing one port.

```
1 interface fastethernet0/2
2 switchport mode access
3 switchport port-security
4 switchport port-security maximum 1
5 switchport port-security mac-address 00AA.BBCC.DDEE
6 switchport port-security violation shutdown
7 exit
8
```

Listing 8: Secure switch ports

Note: The MAC address of a host can be cloned by anyone. Therefore, restricting by MAC address may not be sufficient to prevent unauthorized access to a network in some use cases.

7. MISCELLANEOUS - LOGIN BANNER

7 Miscellaneous - Login Banner

A banner can be displayed at each login to inform and warn users of potential consequences of unauthorized access.

```
1  # banner motd #
2  You are accessing a restricted switch.
3  Do NOT proceed further if you are not certain of what you
4  are doing.
5  #
```

Listing 9: Setting up a login banner message

8 Miscellaneous - Management IP Address

The VLAN1 is usually kept for management purposes.

```
1  interface vlan 1
2  ip address 192.168.10.101 255.255.255.0
3  no shutdown
4  exit
5  ip default-gateway 192.168.10.1
6  exit
7
```

Listing 10: Assigning management IP for VLAN

9. CONFIGURATION VALIDATION

9 Configuration Validation

9.1 Department A - Connectivity between hosts

This department has the following hosts with IP addresses associated as below.

1. PC0 - 192.168.10.12/24
2. PC1 - 192.168.10.11/24
3. PC4 - 192.168.10.13/24
4. PC5 - 192.168.10.14/24

The connectivity can be tested using the **ping** command. In this example connectivity is tested from PC0 to the other PCs on the same VLAN.

```
C:\>ping 192.168.10.11

Pinging 192.168.10.11 with 32 bytes of data:

Reply from 192.168.10.11: bytes=32 time<1ms TTL=128
Reply from 192.168.10.11: bytes=32 time<1ms TTL=128
Reply from 192.168.10.11: bytes=32 time<1ms TTL=128
Reply from 192.168.10.11: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.10.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.10.13

Pinging 192.168.10.13 with 32 bytes of data:

Reply from 192.168.10.13: bytes=32 time<1ms TTL=128
Reply from 192.168.10.13: bytes=32 time<1ms TTL=128
Reply from 192.168.10.13: bytes=32 time<1ms TTL=128
Reply from 192.168.10.13: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.10.13:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.10.14

Pinging 192.168.10.14 with 32 bytes of data:

Reply from 192.168.10.14: bytes=32 time=1ms TTL=128
Reply from 192.168.10.14: bytes=32 time=1ms TTL=128
Reply from 192.168.10.14: bytes=32 time<1ms TTL=128
Reply from 192.168.10.14: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.10.14:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Figure 2: Ping Command Sample Originating from PC0

9. CONFIGURATION VALIDATION

9.2 Department B - Connectivity between hosts

This department has the following hosts with IP addresses associated as below.

1. PC2 - 192.168.20.11/24
2. PC3 - 192.168.20.12/24
3. PC6 - 192.168.20.14/24
4. PC7 - 192.168.20.13/24

The connectivity can be tested using the **ping** command. In this example connectivity is tested from PC2 to the other PCs on the same VLAN.

```
C:\>ping 192.168.20.12

Pinging 192.168.20.12 with 32 bytes of data:

Reply from 192.168.20.12: bytes=32 time=13ms TTL=128
Reply from 192.168.20.12: bytes=32 time<1ms TTL=128
Reply from 192.168.20.12: bytes=32 time<1ms TTL=128
Reply from 192.168.20.12: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.20.12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 13ms, Average = 3ms

C:\>ping 192.168.20.14

Pinging 192.168.20.14 with 32 bytes of data:

Reply from 192.168.20.14: bytes=32 time<1ms TTL=128
Reply from 192.168.20.14: bytes=32 time<1ms TTL=128
Reply from 192.168.20.14: bytes=32 time<1ms TTL=128
Reply from 192.168.20.14: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.20.14:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.20.13

Pinging 192.168.20.13 with 32 bytes of data:

Reply from 192.168.20.13: bytes=32 time<1ms TTL=128
Reply from 192.168.20.13: bytes=32 time<1ms TTL=128
Reply from 192.168.20.13: bytes=32 time<1ms TTL=128
Reply from 192.168.20.13: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.20.13:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Figure 3: Ping Command Sample Originating from PC2

Note: This connectivity proves that the trunk is functional and hosts are able to talk to each other over the trunk.

9. CONFIGURATION VALIDATION

9.3 Simulated Unauthorized Access

In this simulation, Fa0/3 of CIM12137-SW-2 was configured to only allow PC5 MAC address. Once unauthorized access is detected the port was shut-down securely as indicated below.

```
CIM12137-SW-2#
%LINK-3-UPDOWN: Interface FastEthernet0/3, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to down

%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up

CIM12137-SW-2#
%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to administratively down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to down

CIM12137-SW-2#show port-security interface fa0/3
Port Security          : Enabled
Port Status            : Secure-shutdown
Violation Mode         : Shutdown
Aging Time             : 0 mins
Aging Type             : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses  : 1
Total MAC Addresses    : 1
Configured MAC Addresses : 1
Sticky MAC Addresses   : 0
Last Source Address:Vlan : 0001.C70D.6826:10
Security Violation Count : 1 <- See count
```

Figure 4: Security Log for fa0/3 port

And the resulting simulation shows broken connection.

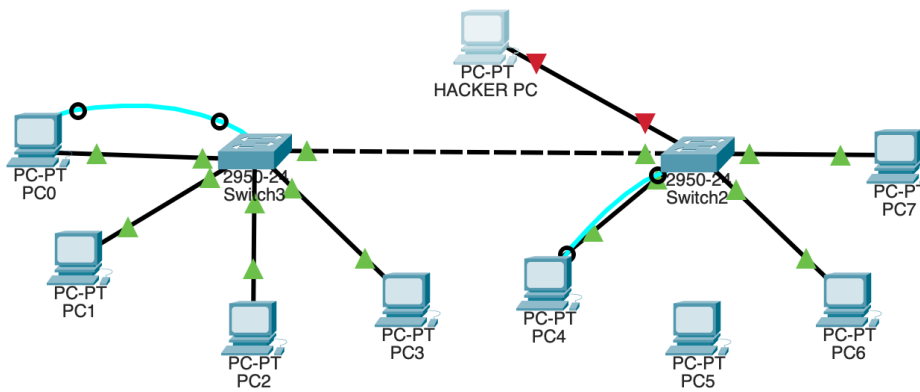
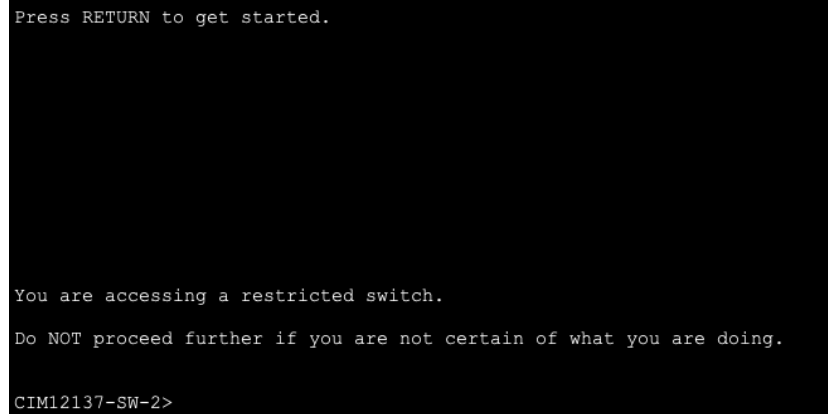


Figure 5: Simulation Overview after security breach

9. CONFIGURATION VALIDATION

9.4 Login Message

The login message will be shown each time a new user logs in to the console.



```
Press RETURN to get started.  
  
You are accessing a restricted switch.  
Do NOT proceed further if you are not certain of what you are doing.  
  
CIM12137-SW-2>
```

Figure 6: Login Message Displayed

Bibliography

Carthern, C., Wilson, W., & Rivera, N. (2021). *Cisco Networks [Second Edition]* [<https://www.perlego.com/book/4513826> (visited 2024-11-24)]. Apress.