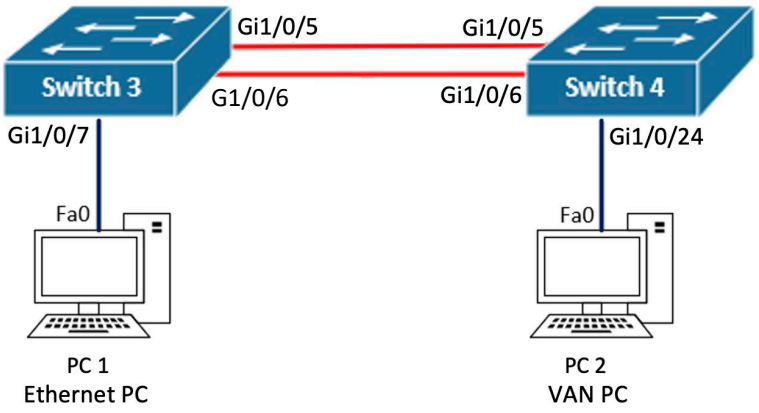
Lab SU-3a – VLANs, Remote Access and Switch Security

Topology Diagram, Addressing Table and VLAN Table



Device Name	IP address	Subnet Mask
Switch3	192.168.99.3	255.255.255.0
Switch4	192.168.99.4	255.255.255.0
PC1	192.168.1.3	255.255.255.0
PC2	192.168.1.4	255.255.255.0

VLAN ID	VLAN Name
10	Users
99	Management

Modifications to Network Drawing

If you are working via remote access, the PCs in the diagram are just for reference and will not be connected to your lab topology.

If you are working on-campus, you will connect the PCs to test intra-vlan communication in Part 3.

Objectives

Configure multiple VLANs to create multiple virtual switches.

Configure remote access to the switch.

Implementing security best practices on a switch.

Required Resources

Personal Computer

Terminal application

2 Cisco Catalyst 3650 switches

2 Test PCs (when working on-campus)

Background

Introduction to VLANs

VLAN technology allows network administrators to **virtually divide a switch into multiple, isolated layer 2 domains**. Essentially, by creating multiple VLANs we are creating multiple virtual switches within the same physical switch. After a VLAN is created, one or more physical switchports can be assigned to the VLAN. All end-devices connected to ports assigned to the same VLAN are thus connected to the same virtual switch. Devices connected to the same VLAN can communicate with each other without the aid of a layer 3 routing device, as long as they are allocated IP addresses in the same Network. On Cisco switches, by default, all switchports are assigned to the default VLAN, i.e. VLAN 1.

Interface Vlan

An **Interface Vlan** is a logical interface on the switch that is assigned to a particular VLAN. We can allocate an IP address and subnet mask to these type of interfaces (as opposed to layer 2 switchport interfaces). A device connected to a switchport assigned to the VLAN can communicate with the respective interface Vlan without the aid of a routing device, again, as long as the IP allocated to the device and the IP allocated to the interface Vlan are in the same network. This is why in Lab SU-2a, computers connected to the default VLAN 1 were able to ping the management IP that you configured on the switches' interface Vlan1.

Management VLAN

In order to connect to a switch using remote access services such as Telnet or SSH, the switch must be previously configured with a **management IP** address. In this and future labs, you will be required to configure a management VLAN on all switches and allocate the management IP to the corresponding interface Vlan. By default, the management VLAN in Cisco switches is VLAN 1, and you would have noticed that **interface Vlan1** exists by default on the switches. However, you will learn that it is a security best practice to not use VLAN 1 as the management VLAN and this interface should be disabled.

Following best practices, network administrators should designate a **dedicated management VLAN**, configure it on all switches and configure the corresponding interface VLAN on each switch with their allocated **management IP.** For example, if VLAN 99 is the management VLAN, VLAN 99 must be configured on all switches in the topology and interface Vlan99 on each switch will be allocated the management IP.

On Layer 2 switches we only use Vlan interfaces for management purposes. This means that you will **only configure one interface Vlan** in the switches for the purpose of allocating the management IP. Please note that, in TNE10006/TNE60006 skills assessments, configuring more than one interface Vlan is considered a major error and results in an automatic fail.

Note: you cannot delete interface Vlan1, however, if not using VLAN 1 as the management VLAN, interface Vlan1 should be disabled (administratively down)

Remote Access

As explained in previous labs, when we remote access a device in the lab, we are really remote accessing the SmartRack server, which in turns connects physically to the console port of the device. In this scenario, the switch is being accessed via a console connection (not remote access).

In a production network, you would want to be able to remote access network devices using Telnet or SSH terminal services. These services allow you to establish an IP connection to a remote system, and then use your local keyboard and display to manage the device. In this scenario, a network administrator does not

have to connect to the console port of the device for management, as long as the device is configured with IP settings and connected to the network.

Telnet and SSH are both terminal services we can use for remote access. However, SSH, as opposed to Telnet, encrypts the messages being exchanged between the switch (or router) and the terminal application in the network administrator's computer. It is a security best practice to use SSH instead of Telnet in a production network, as plain text messages exchanged during a Telnet session can potentially be intercepted, thus disclosing sensitive information (such as passwords, or configuration commands) to unauthorized parties.

Switch Security Best Practices

There are a range of common attacks targeting switches to gain either unauthorized access to the network, or to obtain network traffic meant for other devices. There are a number of basic security practices that network administrators must adhere to in order mitigate these attack

Remove management from VLAN1

As mentioned before, it is a security best practice to not use the default VLAN 1 as the management VLAN. In a switch, all ports are enabled by default, and all ports belong to VLAN 1 by default. If we leave the switch management on VLAN 1, anyone with physical access to the switch can connect a laptop/PC to a VLAN 1 switchport, potentially gaining management access to network devices or intercepting management traffic with sensitive information. In this scenario the attacker would also be able to launch a denial of service attack in the management network, rendering network administrators unable to manage the network.

Disable unused ports

You will learn that switches learn which devices are connected to which ports by observing the source MAC address of incoming frames; this is how switches build their MAC address tables and then make forwarding decisions based on said tables. A common attack targeting switches, is to attempt to overflow the MAC address table with incorrect information, by connecting a laptop/PC to an unused switchport and sending lots of packets with fake source MAC addresses. Through these types of attacks, the table reaches its maximum size, leaving no space for legitimate MAC address information. In this scenario, if a frame arrives the switch with a destination MAC address for which the switch does not have a mapped destination port, the frame will be flooded out all switchports (except the port the frame was received on). This is what we call **MAC flooding attacks**.

Another common attack is what we call **MAC address spoofing**. An attacker that manages to connect a laptop/PC to an unused port, can send frames with a modified source MAC address to pose as a legitimate host. Through this attack, the switch will assume that said host is connected to a certain port, when in reality is the attacker computer connected to it. In this scenario, traffic that is intended for the legitimate host, potentially containing sensitive information, will be received by the attacker.

Both these type of MAC attacks can be mitigated by disabling unused ports, reducing the chances of an attacker connecting a rogue end device to the switch.

Configure Switchport Port-Security

Typically, wall network outlets that connect end devices to switches are placed in semi-public spaces (office space, lobby, etc.). Therefore, even if we disable unused ports, it is still feasible for an attacker to disconnect a legitimate device and connect a rogue device to a wall outlet that connects an active port in the switch. Also, if a legitimate device is compromised, i.e. hacked, the attacker can launch an attack from said device. Therefore, disabling unused ports is not always enough to mitigate attacks targeting a switch.

Cisco switches offer a feature called **switchport port-security** through which we can control the MAC address learning behavior of the switch. Using port-security, the network administrator can control how many MAC addresses are learned on a particular port, which MAC addressees can be learned on a port. and the violation action to be taken if there is a breach of port-security settings.

Part 1: Build the Network

In Part 1, you will use skills learned in previous labs to build the network topology for this lab.

Step 1: Physical Topology

Use the skills learned in Lab SU-1a to perform the following tasks:

- Connect to SmartRack Web Interface
- Reserve a networking Kit in your allocated room
- Power on **Switch 3** and **Switch 4**
- Leave all other devices powered off
- Use the **show ip interface brief** to validate the physical connections

Note: the existing switch inter-connections should match the Topology Diagram above.

Step 2: Configure General Switch Settings

Use the skills learned in Lab SU-2a to perform the following tasks on Switch3 and Switch4

- Validate that your switches booted with default settings (i.e. startup-config not present)
- Configure the switch **hostnames** as per the Topology Diagram
- Configure a **banner MOTD** including your student ID

Note: always use the **show startup-config** and **show vlan brief** commands as soon as your devices have booted up at the beginning of your practice, to validate that there are no previous configuration settings. If a startup-config file and/or custom VLANs exist, you should remove them using the **write erase** and **delete vlan.dat** commands a reload the switch.

You are also advised to use the **no ip domain-lookup** command. This command will stop the system from attempting to translate erroneous entries (i.e. when you mistype a configuration command) into an IP address. When an input is not recognized as a configuration command, the switch assumes that it's a hostname instead and it will attempt to translate it to an IP address. In a production network, where a DNS server is present, this is a useful. However, in a lab environment, this will just result in the switch running multiple failed translation attempts while you wait for this process to be over to be able to continue.

Part 2: Configuring VLANs

In Part 2, you will learn how to configure multiple VLANs to create multiple virtual switches.

Step 1: Observe the Default VLAN Configuration

Connect to the CLI at your switches and use the **show vlan brief** command to view the default VLAN database information. This command, as any other show command, should be used from the Administrator (enable) Mode:

```
Switch#show vlan brief
```

How many VLANs are there in a Cisco Switch by default? 5

What is default VLAN membership of interfaces Gi1/0/1 – 24? They all belong to VLAN 1

Note: the term "membership" refers to the VLAN assignment for the ports. When we assign a switchport to a VLAN, we say that we are configuring the VLAN membership.

Step 2: Configure User VLANs

In the previous step you would have observed that Cisco switches have five VLANs configured by default; VLAN 1 (the default VLAN) and VLANs 1002 – 1005. Typically, we don't use these existing VLANs to connect end devices to the switch.

Instead, in a company network, we configure custom **User VLANs**, as many as needed to meet the company's organisational requirements. For example, we might want to have HR staff connected to a VLAN, while having Admin staff connected to a different VLAN and the Engineering department to a third VLAN. This is one of the ways in which VLANs are useful, we can divide our network to match the organisational workgroups, allowing us to configure different service levels to each virtual network, as well as controlling the traffic that can be exchanged between the different groups.

To configure a VLAN on a switch, you use the **vlan** command followed by the VLAN ID. This will take you into the VLAN configuration mode, where you can configure a human language name for the VLAN. The VLAN name has no operational purpose, however, it helps network administrators identify the purpose of the VLAN.

a) Configure user VLAN 10 on Switch3 using the following commands:

```
Switch3#config t
Switch3(config)#vlan 10
Switch3(config-vlan)#name Users
Switch3(config-vlan)#end
```

b) Use the **show vlan brief** command to validate the changes to the VLAN configuration. You should now see all the pre-existing VLANs and **VLAN 10** with name **Users**

c) Use the same set of commands to configure VLAN 10 on Switch4.

Step 3: Configure VLAN Membership

The next step after configuring a User VLAN, is to assign switchports to the VLAN. In the previous step, you would have observed that all switchports are by default allocated to VLAN 1 still, and there were no ports allocated to VLAN 10.

To assign a port to a VLAN, we first need to set the port as an access port using the **switchport mode access command.** An access port is a port that will send and receive traffic for a single VLAN. You will later learn that there is a different switchport mode that will allow a port to send and receive traffic for multiple VLANs. Switchports that connect to end-devices in User VLANs should always be configured as access ports. After setting the port to access mode, we use the **switchport access vlan** command to specify the VLAN ID we want the port to belong to; if no VLAN ID is specified, the port will remain in VLAN 1.

a) Use the following configuration commands to allocate ports G1/0/10 – 14 to VLAN 10

```
Switch3#config t
Switch3(config)#interface range gigabitEthernet 1/0/10 - 14
Switch3(config-if-range)#description Users VLAN
Switch3(config-if-range)#switchport mode access
Switch3(config-if-range)#switchport access vlan 10
```

The **description** command is used to label the port. This label has no operational purpose; however, it helps administrators identify to which VLAN an interface belongs to.

b) Use the **show vlan brief** command to validate the changes to VLAN 10 membership.

c) Use the same set of commands to allocate interface Gi1/0/13 to VLAN 10 on Switch 4

Step 4: Connectivity Scenarios

Consider the following hypothetical scenario and answer the questions. For this, remember that the links interconnecting the switches belong to the default VLAN 1, therefore, only VLAN 1 traffic can be carried across the switches.

Scenario: five PCs, configured with the specified IP addresses, are connected to the network as follows:

- PC1 with IP 192.168.1.3/24 connects to Gi1/0/7 on Switch3
- PC2 with IP 192.168.1.4/24 connects to Gi1/0/24 on Switch4
- PC3 with IP 192.168.10.10/24 connects to Gi1/0/10 on Switch3
- PC4 with IP 192.168.10.11/24 connects to Gi1/0/11 on Switch3
- PC5 with IP 192.168.10.7/24 connects to Gi1/0/13 on Switch 4

Note: you are not required to connect test PCs to the switches to run ping tests and answer the questions, instead you must use your networking knowledge to predict an outcome.

a) Will PC1 and PC2 be able to ping each other? Yes? No? Why? _____
Yes because they are from the same VLAN

b) Will PC1 and PC3 be able to ping each other? Yes? No? Why? _____
No because they are from different VLAN

c) Will PC3 and PC4 be able to ping each other? Yes? No? Why? _____
Yes because they are from the same VLAN and share a switch

d) Will PC3 and PC5 be able to ping each other? Yes? No? Why? _____
No because the default VLAN occuping the switches is VLAN 1 where they are VLAN 10

To remove a single VLAN, we can use the **no vlan** command followed by the VLAN ID. To remove all VLANs on the switch, we can delete the **vlan.dat** file. When configuring VLANs on the switch, the VLAN related settings are saved to the **vlan.dat** file instead of the **running-config**. To delete this file, we use the **delete vlan.dat** command from the Administrator Mode, this will cause all VLAN settings to be removed after the next reload.

Note: you are advised to check the VLAN database on your switches at the beginning of every practice using the **show vlan brief** command. If VLANs other than the default VLANs exist, delete the **vlan.dat** and reload the switch.

Part 3: Testing Intra-VLAN communication (On-Campus)

In Part 3, you will use the test computers in the ATC labs to test communication between two computers in the same VLAN. Only complete Part 3 if you are working on-campus.

Step 1: Start, Connect and Configure the Ethernet PC

A Virtual PC is a virtual computer managed by the primary operating system on a physical PC. Within the Virtual PC, you can run a unique copy of any operating system you'd like, and it will not interfere with the primary PC. The primary PCs in the ATC labs are restricted in what students can do configuration-wise, whereas in the Virtual PCs you have full access to all aspects of the computer configuration.

On the PCs in the ATC lab, you can run up to two Virtual PCs, configure them with specified IP settings and connect them to your networking devices for testing purposes. These virtual PCs are named based on how they connect to the networking equipment:

- The **Ethernet PC** uses a secondary network card installed in the computer. You will find there is an Ethernet cable connected to this secondary card. This cable extends from your desk to a patch panel in networking enclosure, and from there we can extend this connection to the switch or router we want to connect the Ethernet PC to.
- The **VAN PC** uses a Virtual Area Network connection. Physically, this connection shares the same network card as the physical PC. However, this card is partitioned to establish one connection to the Swinburne network, and another connection to the VAN infrastructure within the lab.

In this step we will start, configure and connect the **Ethernet PC (PC1)** to your network.

1. Ask your instructor for assistance to extend the Ethernet connection, from your desk to port **Gi1/0/7** on **Switch 3**.
2. Start the **Virtual Machine Launcher** application via the start menu on your PC.
3. From the **Virtual Machine Launcher**, within the **Cisco** menu, launch the **PC with Ethernet** virtual PC
4. In the Virtual PC, go to Control Panel → **Network Connections** (this might vary depending on the Windows OS version). A new dialog window will open.
5. Right-click the network card (most likely called Local Area Network or LAN) and select **Properties.** A new dialog window will open.
6. Select **Internet Protocol (TCP/IP)** and click on **Properties.** A new dialog window will open.
7. Select the **Use the following IP address** radio button and configure PC1 **IP address** and **Subnet Mask** as per the Addressing Table on page 1.
8. Close all dialog windows (IP settings will not take effect until you do so)
9. Launch a DOS command line: Start Menu → Programs → Accessories → **Command Prompt**
10. At the prompt, type **ipconfig** to check the computer network configuration, make sure that the IP address and subnet mask matches the Addressing Table specifications.

Step 2: Start, Connect and Configure the VAN PC

In this step we will start, configure and connect the **VAN PC (PC2)** as per the Topology Diagram and Addressing Table.

1. From the **Virtual Machine Launcher**, within the **Cisco** menu, launch the **PC with VAN** virtual PC
2. On the **Virtual Machine Launcher**, click the **Virtual Networks** tab. You should see a list of all the devices you have booked.

   Note: If this list is empty is because you have started the Virtual Machine Launcher before you booked the devices. In this case, you will have to exit and re-start the Virtual Machine Launcher.
3. From the list of devices, select **Switch 4**. This will establish a connection from your VAN PC to port **Gi1/0/24** on **Switch 4**.
4. Follow the steps learned on Part 3, Step 2 to **configure PC2 IP settings** on the VAN PC.

Step 3: Test your Network

Use **ping** and **arp** command prompt tools to test connectivity between your two virtual PCs and observe their ARP tables.

a) Can PC1 communicate with PC2? Professor said skip

b) What is the MAC address of PC1? _____

c) What is the MAC address of PC2? _____

Part 4: Configuring Switch Management and Remote Access

In Part 4, you will learn how to configure the management IP of the switch on a dedicated management VLAN and enable Telnet and SSH services for remote access.

Step 1: Remove Management from VLAN 1

In Lab SU-2a you allocated the management IP of the switches to the default management Interface Vlan. You also observed how, in that scenario, the PCs connected to switchports with default settings were able to ping the management IP of the switches. This is because, by default, the default management interface (interface Vlan1) and all physical ports belong to the same VLAN, i.e. VLAN 1.

In a production scenario, network administrators should follow best practices to ensure the management VLAN is protected from unauthorised access. This includes moving the switch management to a dedicated VLAN by following these steps:

- Disable Interface Vlan1
- Create a dedicated Management VLAN
- Configure an interface Vlan in the dedicated Management VLAN
- Allocate the management IP to the management interface Vlan

Also, we should not allocate access ports to the management VLAN. This ensures that end-devices will not connect to the management VLAN directly through the switch, and that all traffic from end-devices into the management VLAN must be routed through a layer 3 device where we can enforce access control.

Note: this unit does not cover access control, however, note that this can be done by configuring Access Control Lists (ACLs) on routers, specifying which IP addresses can communicate with other IP addresses.

a) Disable Interface Vlan1

```
Switch3#config t
Switch3(config)#interface Vlan 1
Switch3(config-if)#shutdown
Switch3(config-if)#exit
```

b) Create management VLAN 99

```
Switch3(config)#vlan 99
Switch3(config-vlan)#name Management
Switch3(config-vlan)#exit
```

c) Create management Interface Vlan 99 and allocate the management IP

```
Switch3(config)#interface vlan 99
Switch3(config-if)#description Management
Switch3(config-if)#ip address 192.168.99.3 255.255.255.0
Switch3(config-if)#exit
```

d) Use the **show vlan brief** command to validate management **VLAN 99** has been configured and that no access ports are allocated to it.

e) Use the **show ip interface brief** command to validate that management **interface Vlan99** has been configured and allocated the right management IP address.

f) Repeat the above configuration steps on Switch 4 to configure the management VLAN and management IP address as per the Addressing Table above.

g) From Switch3 ping Switch4. Is this ping successful. Yes? No? Why?

No because the VLAN 99 doesn't posess the ports that connects the switches together

h) If on-campus, ping from PC1 to Switch 3. Is this ping successful. Yes? No? Why?

No because VLAN 1 is down

Step 2: Enable Telnet Access

When connecting to a switch via remote access, we are connecting to a virtual terminal line in the switch called **line vty**. On Cisco switches, we can allow up to 16 concurrent remote access connections, that means the switch has 16 line vty virtual terminals. To enable Telnet access to the switch we should configure all 16 virtual terminals using the **password** and **login** commands, this automatically enables Telnet access to the switch as Telnet is the default terminal access service.

a) Enable Telnet access on Switch 3

```
Switch3(config)#line vty 0 15
Switch3(config-line)#password ccna
Switch3(config-line)#login
```

b) Enable Telnet access on Switch 4 following the same set of commands

To test Telnet access, we will establish a Telnet connection from Switch3 to Switch4 and vice versa, however, in the previous step you would have observed that Switch3 and Switch4 cannot communicate with each other. For Switch3 and Switch4 to be able to communicate with each other, we must configure the interfaces interconnecting the switches to carry traffic for the management VLAN 99. We will do this by configuring **VLAN trunking** on these interfaces. Please note that we will cover VLAN trunking in more detail in future lab practices.

c) Configure VLAN trunking on Switch3

```
Switch3(config)#interface range gigabitEthernet 1/0/5 - 6
Switch3(config-if-range)#switchport mode trunk
```

d) Configure VLAN trunking on Switch4

```
Switch4(config)#interface range gigabitEthernet 1/0/5 - 6
Switch4(config-if-range)#switchport mode trunk
```

e) Test Telnet access to Switch3 from Swtich4

5

```
Switch4#telnet 192.168.99.3
```

If the connection is successful, the switch will prompt for the password you have configured on the line vty before granting you access to the CLI execution mode.

Terminate the Telnet connection by typing **exit.** This will take you back to the CLI at Switch4.

f) Test Telnet access to Switch4 from Swtich3 following the same procedure described above.

Step 3: Enable SSH Access on Switch3

As mentioned in the Background section, it is a security best practice to use SSH service instead of Telnet. This is because messages exchanged during an SSH connection are encrypted. Only the two parties in the SSH session are able to read the messages using a pre-established decryption key. In this way, even if an attacker managed to gain access to the management network and intercept the messages exchanged during an SSH management session, said attacker will not be able to read the potentially sensitive information.

When requesting SSH access to a switch, the switch send the requesting client an electronic certificate to use for authentication and encryption purposes during the session. This certificate is generated based on the fully qualified domain of the switch (i.e. hostname and domain name). Also, SSH services require username and password authentication; local user accounts can be configured on the switch for authentication before granting access to the CLI via SSH.

In summary, in order to configure SSH remote access we should complete the following tasks on the switch:

- Disable Telnet services on the virtual terminals
- Configure a fully qualified domain name
- Generate an SSH certificate
- Configure a local user account
- Enable SSH services on the virtual terminals

Note: disabling Telnet is not required to enable SSH, however, it is considered best practice.

Follow the following configuration steps on Switch 3 to enable SSH access.

a) Disable Telnet services

```
Switch3(config)#line vty 0 15
Switch3(config-line)#transport input none
Switch3(config-line)#no login
Switch3(config-line)#end
```

These commands disable all remote access services and can also be used to disable SSH access if previously configured.

b) Configure a domain name (the hostname of the switch has already been configured)

```
Switch3(config)#ip domain-name ccna.lab
```

c) Generate the SSH certificate

```
Switch3(config)#crypto key generate rsa general-keys modulus 1024
```

This will generate a certificate signed with a 1024bit RSA key. If the hostname or domain name change, you should regenerate the certificate. The command **crypto key zeroize** is used to remove a previously generated certificate.

d) Configure a local user account

```
Switch3(config)#username labuser privilege 15 secret labpassword
```

A privilege level of 15 indicates administrator or enable mode access rights for the user. Lower levels can be used to create users with partial administrative privileges.

e) Enable SSH services

```
Switch3(config)#line vty 0 15
Switch3(config-line)#transport input ssh
Switch3(config-line)#login local
Switch3(config-line)#end
```

The command **login local** indicates the switch will be using the local user accounts for authentication.

f) Use the **show ip ssh command** to validate the SSH server has been enabled

What is the default SSH version? 1/0/0-1/0/9 and 1/0/15 - 1/0/24

What is the default session timeout? _____

How many authentication retries are allowed by default? _____

g) Test SSH access to Switch3 from Switch4

```
Switch4#ssh -l labuser 192.168.99.3
```

If the connection is successful, the switch will prompt you for the password you have configured for **labuser** before granting you access to the CLI.

To close the SSH connection type **exit.**

h) (Optional) Modify the default connection timeout and authentication retries values

```
Switch3(config)#ip ssh time-out 60
Switch3(config)#ip ssh authentication-retries 4
```

Part 5: Configuring Switch Security Best Practices

In Part 5, you will learn how to disable switchports and how to configure switchport port-security.

Note: removing management from the default VLAN is also a security best practice. This has been completed in Part 4.

Step 1: Disable Unused Ports

In the Background section we discussed two types of switch attacks that can be carried out simply by connecting a laptop/PC to a switchport in the switch and sending frames with modified source MAC address. These types of attacks can be mitigated by disabling unused ports in the switch.

Ports that are not used for interconnecting to other network devices, or ports that do not belong to an existing user VLAN are considered unused ports. Refer to the network diagram to identify the ports used for interconnecting the switches, use the **show vlan brief command** to identify which ports are not assigned to a user VLAN and answer the following questions:

Which are the unused ports on Switch3? 1/0/1-1/0/4

Which are the unused ports on Switch4? _____

Note: Use the **shutdown** command to disable ports Gi1/0/1 – 4 on Switch3

```
Switch3(config)#interface range gigabitEthernet 1/0/1 - 4
Switch3(config)#shutdown
```

a) Disable all other unused ports on Switch3

b) Disable all unused ports on Switch4

c) Use the **sh ip interface brief** command to validate that all unused ports have been disabled on both switches

Step 2: Configure Switchport Port-security on Switch3

As discussed, limiting the number of MAC addresses that are allowed to connect to a switch will help mitigate certain type of switch attacks, especially on switchports that are accessible through a wall outlet in public spaces. The Cisco **port-security** feature can be used to accept a maximum number of MAC addresses associated with each port, manually programme which MAC addresses are allowed to connect to a port and set different actions to be taken when port-security policies are breached.

Refer to the table in the next page for the set of configuration commands used to configure port-security on an interface.

Note: port-security can only be configured on ports that have been configured to explicit access or trunk mode using the **switchport mode** command. Ports with default switchport mode will not accept port-security settings.

Note: the general **switchport port-security** command must always be used in order to enable port-security in the port. If you configure other port-security commands on the port but forget to include the **switchport port-security** command, port-security settings will not take effect.

Switchport port-security configuration commands.

`Switch(config-if)#switchport port-security`	Enable port security on the interface. Sets a default maximum of one MAC address on this port and action taken upon breach to shutdown
`Switch(config-if)#switchport port-security maximum N`	Configure the maximum MAC addresses allowed on this port to N
`Switch(config-if)#switchport port-security violation shutdown`	If the maximum MAC addresses is breached, this interface will be immediately disabled and the administrator is informed via SNMP
`Switch(config-if)#switchport port-security violation restrict`	If the maximum MAC addresses is breached, packets with unknown source addresses will be dropped by the switch and the administrator is informed via SNMP
`Switch(config-if)#switchport port-security violation protect`	Behaves like restrict mode except no notification is made to the administrator
`Switch(config-if)#switchport port-security mac-address sticky`	MAC addresses learnt are sticky. Once a MAC address is learnt on a port it is saved and can't be removed from the list of MAC addresses associated with this port. You can disable this by re-issuing this command with "no" at the start of the command.
`Switch(config-if)#switchport port-security mac-address xxxx.xxxx.xxxx`	Allocate a specific MAC address to the list of MAC addresses of this port. An address can be manually added if the mode is sticky or dynamic

Show commands to explore port-security related settings and current status:

`Switch#show mac address-table`	Display the current learnt MAC addresses and which ports they are associated with
`Switch#show port-security`	Display a summary of port security status for the switch
`Switch#show port-security interface <interfaceID>`	Display the port security status for the nominated interface. Includes the state of port security, the violation mode, and the maximum MAC addresses allowed on this port
`Switch#show port-security address`	Display which MAC addresses are attached to secure ports on the switch and the status of the secure port
`Switch#show interface <inerfaceID>`	Show detailed configuration and status information for the specified interface

a) Configure all VLAN 10 ports on Switch 3 with the following port-security settings:

- Maximum MAC address allowance: 3
- Violation action: shutdown (this is the default setting)
- Sticky MAC address learning

b) Configure VLAN 10 port on Switch 4 with the following port-security settings:

- Maximum MAC address allowance: 1
- Violation action: restrict
- Only allow MAC address: 0060.5cd2.9b05