**LAB JOURNAL**

<https://smartrack.swinburne.edu.au>

|  |  |  |
| --- | --- | --- |
| **Device Label** | **Type** | **Model** |
| Switch 1 (S1) | Layer 2 Switch | Catalyst 2960 |
| Switch 2 (S1) | Layer 2 Switch | Catalyst 2960 |
| Switch 3 (S3) | Layer 3 Switch | Catalyst 3650 |
| Switch 4 (S4) | Layer 3 Switch | Catalyst 3650 |
| Router 1 (R1) | Router | ISR 4321 |
| Router 2 (R2) | Router | ISR 4321 |
| Router 3 (R3) | Router | ISR 4321 |
| Router 4 (R4) | Router | ISR 4321 |

* Display the Interface Status on Switch 1 : Switch# **show ip interface brief**
* On the command line interface of PC1 to display the ARP table information: **arp -a**
* to empty the content of the ARP table: **arp -d**
* When entering commands at the CLI, the **<tab>** key and “**?”** help you auto-complete commands and display the CLI help.
* **User Mode** – signified by a **“>”** after the device name. This mode has minimal privileges, you will not be able to change configuration settings and you will only be able to view the status of a subset of parameters and some configuration settings.
* **Administrator Mode** – signified by a **“#”** after the device name. Also called “enable mode” or “privileged execution mode”. In this mode you will be able to examine the status of the full set of parameters and all configuration settings.
* **Configuration Mode** – signified by a **“(config)#”** after the device name. In this mode you will be able to change the device configuration.
* Other than these three primary modes, a number of sub-configuration modes exist. For example, if you are configuring a network interface the prompt will be followed by **“(config-if)#”**.
* You can transition from User Mode to Administrator Mode by entering the command **“enable”**
* Logout from User Mode by entering **“exit”**
* Transition from Administrator Mode to User Mode by entering **“exit”**
* Transition from Administrator Mode to Configuration Mode by entering “configure terminal”
* Transition from Configuration Mode to Administrator Mode by entering **“exit”**
* Transition from a Sub-configuration Mode to Configuration Mode by entering **“exit”**
* Transition from Configuration or Sub-configuration Modes to Administrator Mode by entering **“end”**
* To set the switch name, you need to use the **hostname** command in Configuration mode. Enter the following commands at Switch3 CLI:

Switch>ena

Switch#conf t

Switch(config)#hostname Switch3

Switch3(config)#end

Switch3#

* To configure the MOTD we use the **banner motd** from the Configuration mode. Enter the following commands at Switch3 CLI:

Switch3#conf t

Switch3(config)#banner motd + \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\*\* This is Week 2 \*\*

\*\* of Semester 2 \*\*

\*\* at Swinburne \*\*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* +

Switch3(config)#end

Switch3#

* the running configuration or **running-config**) and the startup configuration or **startup-config:** Use the **show running-config** and **show startup-config** command at the CLI of your switches
* On Switch3, save the running configuration to the startup configuration and then reload the switch. To do this, you must be on Administrator Mode and use the copy running-config startup-config command:

Switch3#**copy running-config startup-config**

Switch3#**reload**

* Now, reload Switch4 without saving the running configuration to the startup configuration. The switch will prompt you so save the configuration, enter “no” and then hit enter to confirm.

Switch4#**reload**

System configuration has been modified. Save? [yes/no]:no

Proceed with reload? [confirm]

* **User Mode Password** – must be entered before you can login to the device in User Mode via console
* **Administrator Mode Password** – must be entered after typing “**enable**” before entering Administrator Mode
* **Line VTY Password** – must to be entered when telneting to the device before you login in User Mode
* By default, these passwords are not set.
* To set the **User Mode Password** to **“ccna”** on Switch3, enter the following commands:

Switch3#**conf t**

Switch3(config)#**line console 0**

Switch3(config-line)#**password ccna**

Switch3(config-line)#**login**

Switch3(config-line)#**end**

Switch3#**exit**

* To set the **Administrator Mode Password** to **“cisco”** on Switch3, enter the following commands:

Switch3#**conf t**

Switch3(config)#**enable secret cisco**

* When using the keyword secret, the encrypted password will be display when you use the **show run** command.
* To delete the Administrator Mode Password, you can use the following commands:

Switch3#**conf t**

Switch3(config)#**no enable secret**

* Disable Switch4 GigabitEthernet interface 1/0/1 by using the following commands:

Switch4#**conf t**

Switch4(config)# **interface gigabitEthernet 1/0/1**

Switch4(config-if)#**shutdown**

Switch4(config-if)#**end**

* Disable Switch4 GigabitEthernet interfaces 1/0/2 through to GigabitEthernet interface 1/0/4 using the following commands:

Switch4#**conf t**

Switch4(config)# **interface range gigabitEthernet 1/0/2 - 4**

Switch4(config-if)#**shutdown**

Switch4(config-if)#**end**

* Use the **show ip interface brief** command to validate the interface status on Switch4
* To re-enable Switch4 GigabitEthernet interface 1/0/1 use following commands:

Switch4#**conf t**

Switch4(config)# **interface gigabitEthernet 1/0/1**

Switch4(config-if)#**no shutdown**

* Configure Swtich3 management **IP address** and **Subnet Mask.** To do this, use the following commands:

Switch3(config)**interface vlan1**

Switch3(config-if)#**ip address 192.168.1.3 255.255.255.0**

Switch3config-if)#**no shutdown**

Switch3config-if)#**end**

* Use the **ping** command on the switches and PCs to validate your answers. For example, if you want to send a ping request from Switch3 to Switch4, use the following command from Administrator or User Mode:

Switch3#**ping 192.168.1.4**

* Delete the startup configuration on Switch3 using the command below. You must hit Enter to confirm.

Switch3#**write erase**

Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]

[OK]

* Delete the vlan database on Switch3 using the command below. You must hit Enter to confirm.

Switch#**delete vlan.dat**

Delete filename [vlan.dat]?

* Connect to the CLI at your switches and use the **#show vlan brief** command to view the default VLAN database information.
* 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**

* 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**

* Use the no switchport access vlan command to remove the VLAN 10 assignment to G1/0/24.

S3(config)# **interface g1/0/24**

S3(config-if)# **no switchport access vlan**

S3(config-if)# **end**

* To remove a single VLAN, we can use the **no vlan** command followed by the VLAN ID.
* Enable Telnet access on Switch 3

Switch3(config)#**line vty 0 15**

Switch3(config-line)#**password ccna**

Switch3(config-line)#**login**

* Configure VLAN trunking on Switch3

Switch3(config)#**interface range gigabitEthernet 1/0/5 – 6**

Switch3(config-if-range)#**switchport mode trunk**

* Test Telnet access to Switch3 from Swtich4

Switch4#**telnet 192.168.99.3**

* Disable Telnet services

Switch3(config)#**line vty 0 15**

Switch3(config-line)#**transport input none**

Switch3(config-line)#**no login**

Switch3(config-line)#**end**

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

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

* Generate the SSH certificate

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

* Configure a local user account

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

* Enable SSH services

Switch3(config)#**line vty 0 15**

Switch3(config-line)#**transport input ssh**

Switch3(config-line)#**login local**

Switch3(config-line)#**end**

* Use the **show ip ssh command** to validate the SSH server has been enabled
* Test SSH access to Switch3 from Switch4

Switch4#**ssh -l labuser 192.168.99.3**

* Modify the default connection timeout and authentication retries values

Switch3(config)#**ip ssh time-out 60**

Switch3(config)#**ip ssh authentication-retries 4**

* 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**

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

* The default DTP mode of a 2960 switch port is dynamic auto. This allows the interface to convert the link to a trunk if the neighbouring interface is set to trunk or dynamic desirable mode.

Set Gi1/0/5 on S3 to negotiate trunk mode.

S3(config)# **interface g1/0/5**

S3(config-if)# **switchport mode dynamic desirable**

* Issue the **show interfaces trunk** command to view trunked interfaces. Notice that the mode on S3 is set to desirable, and the mode on S4 is set to auto.

S3# **show interfaces trunk**

* Change the switchport mode on interface Gi1/0/5 to force trunking. Make sure to do this on both switches.

S3(config)# **interface g1/0/5**

S3(config-if)# **switchport mode trunk**

* Issue the **show flash:** command to determine if a **vlan.dat** file exists in flash.

S3# **show flash:**

Directory of flash:/

* Issue the **show flash** command to verify that the vlan.dat file has been deleted.

S3# **show flash**

* The commands to assign a default gateway on the switch are:

S3(config)# **ip default-gateway a.b.c.d**

* Configure Ethernet Interface settings for R1. Configuring an interface on the router is similar to configuring an interface on a switch. Unlike the switch, IP addresses are configured on the actual interfaces rather than the virtual interfaces. The other primary difference to the switch is that the router interfaces are always shutdown by default and have to be enabled.

Configure Gi0/0/0 on the Router.

R1(config)# **int g0/0/0**

R1(config-if)# **description Connection to Switch2 – VLAN 20**

R1(config-if)# **ip address 192.168.20.1 255.255.255.0**

R1(config-if)# **no shutdown**

R1(config-if)# **exit**

R1(config)# **exit**

* The #**show ip route** command displays the current routing table. As we will not configure any advanced routing in this Unit, it will only display summary information about the directly connected networks.
* For example, you can test inter-vlan routing between VLAN 10 and VLAN 20, by pinging S3 in VLAN 10 sourcing the ping from the router interface connected to VLAN 20. To do this you use the command:

R1# **ping 192.168.10.11 source g0/0/0**

* Configure the **lo0** interface:

R1(config)# **interface lo0**

R1(config-if)# **description Loopback test interface**

R1(config-if)# **ip address 209.165.200.225 255.255.255.224**

R1(config-if)# **end**

* Enable the Gi0/0/1 interface:

R1(config)# **interface g0/0/1**

R1(config-if)# **no shutdown**

R1(config-if)# **end**

* Create a subinterface on R1 Gi0/0/1 for VLAN 99 using 99 as the sub-interface ID and assign an interface description.

R1(config)# **interface g0/0/1.99**

R1(config-subif)# **description Connection to management VLAN**

R1(config-subif)# **encapsulation dot1Q 99**

R1(config-subif)# **ip address 192.168.1.1 255.255.255.0**

R1(config-if)# **end**

* One way to help resolve where the error is occurring is to do a **tracert** from PC-A to S3.

C:\Users\User1> **tracert 192.168.1.11**

* In the spanning tree, ports are designated as a **root** port, a **designated** port, or an **alternate** port.

**Root Port:** A port that is activated and following it will direct traffic towards the root bridge

**Designated Port:** A port that is activated and following it will direct traffic away from the root bridge

**Alternate Port:** A redundant port that is currently not activated

* Issue the **show spanning-tree** command on all three switches. The Bridge ID Priority is calculated by adding the priority value and the extended system ID. The extended system ID is always the VLAN number. In the example below, all three switches have equal Bridge ID Priority values (32769 = 32768 + 1, where default priority = 32768, VLAN number = 1); therefore, the switch with the lowest MAC address becomes the root bridge (S2 in the example).

S1# **show spanning-tree**

* Change port cost. In addition to the blocked port, the only other active port on this switch is the port designated as the root port. Lower the cost of this root port by issuing the **spanning-tree cost** interface configuration mode command.

If **S1** is the root bridge in your topology, change the cost to **18**.

If **S3** or **S4** is the root bridge in your topology, change the cost to **3**.

S3(config)# **interface g1/0/2**

S3(config-if)# **spanning-tree cost 3**

* **Remove port cost changes.** a. Issue the **default spanning-tree cost** interface configuration mode command to remove the cost statement that you created earlier.

S1(config)# **interface g1/0/2**

S1(config-if)# **default spanning-tree cost**

* Configure switch S1 to be the primary root bridge for all existing VLANs.

S1(config)# **spanning-tree vlan 1,10,99 root primary**

* Configure switch S3 to be the secondary root bridge for all existing VLANs.

S3(config)# **spanning-tree vlan 1,10,99 root secondary**

* Change STP mode to PVST+ on S3

S3(config)#**spanning-tree mode pvst**

* To examine PVST+ convergence, you will create a Layer 2 topology change while using the **debug** command to monitor spanning-tree events.

Enter the **debug spanning-tree events** command in privileged EXEC mode on switch S4.

S4# **debug spanning-tree events**

Spanning Tree event debugging is on

* Configure S3 for Rapid PVST+.

S3(config)# **spanning-tree mode rapid-pvst**

* Verify configurations with the **show running-config | include spanning-tree mode** command. The example below is for switch S3, repeat for all three switches

S3# **show running-config | include spanning-tree mode**

spanning-tree mode rapid-pvst

* PortFast is a feature of spanning tree that transitions a port immediately to a forwarding state as soon as it is turned on. This is useful in connecting hosts so that they can start communicating on the VLAN instantly, rather than waiting on spanning tree. To prevent ports that are configured with PortFast from forwarding BPDUs, which could change the spanning tree topology, BPDU guard can be enabled. At the receipt of a BPDU, BPDU guard disables a port configured with PortFast.

Configure interface G1/0/7 on S3 with PortFast.

S3(config)# **interface G1/0/7**

S3(config-if)# **spanning-tree portfast**

Configure interface G1/0/7 on S3 with BPDU guard.

S3(config)# **interface G1/0/7**

S3(config-if)# **spanning-tree bpduguard enable**