CCNA2v7 Case Study

1. **Group Number \_15 = n**

# Topology

1. Icon

   Description automatically generated
2. A blue and white flag

   Description automatically generated with medium confidence

**Rn**

**Other students networks**

**Tutor**

**G0/1**

**G0/0**

1. A blue and white flag

   Description automatically generated with medium confidenceA blue and white flag

   Description automatically generated with medium confidence

**S2n**

**S1n15151**

1. Icon

   Description automatically generated

**PCB**

1. Icon

   Description automatically generated

**PCA**

LAN IPv4 address 30.15.0.0 /16

1. LAN IPv6 address 2001:7A21:15ad:: /48
2. External IPv4 address 183.19.1.15/24
3. External IPv6 address 2002:6000::15/48

# Assessment Objectives and marking scheme (Total 50 marks)

*See the marking schedule at the back for guidance.*

Part 1: Design an Addressing Scheme

Part 2: Initialize, Reload and Configure Basic Device Settings

Part 3: Configure Network Infrastructure Settings (VLANs, Trunking, Etherchannel) (10 marks)

Part 4: Configure Switch Security (10 marks)

Part 5: Configure Host Support and DHCP (10 marks)

Part 6: Configure Static Routes (5 marks)

Part 7: Test and Verify IPv4 and IPv6 End-to-End Connectivity

Part 8: Documentation All sections complete - Detailed written descriptions and justifications of all sections - Testing strategy reflection - Troubleshooting reflection - Command journal (15 marks)

Part 9: Clean Up

Marks can be deducted for parts 1 and 2 for poor IP address design or incorrect basic device configuration. The tutor will also ask questions so marks can be deducted if your understanding of each sections in not demonstrated

# Scenario

In this Case Study you will configure the devices in a small network. You must configure a router, switch and PCs to support both IPv4 and IPv6 connectivity for supported hosts. Your router and switch must also be managed securely. You will configure inter-VLAN routing, DHCP, Etherchannel, and port-security.

# Required Resources

* 1 Routers
* 2 Switches
* 2 PCs
* Console cables to configure the Cisco IOS devices via the console ports
* Ethernet cables as shown in the topology

# Instructions

## Design an Addressing Scheme

You will design both an IPv4 and an IPv6 addressing scheme to apply IPv4 and IPv6 addresses to all network interfaces in the topology. This is known as Dual Stacking.

### Design an IPv4 and IPv6 addressing scheme using VLSM.

* Subnet the LAN network into appropriately sized subnetworks. All routers, switches and hosts will have both IPv4 and IPv6 addresses. Design and fill in the blanks in the table below.

| Subnetwork | Number of Host Addresses Required | Ipv4 and IPv6 Network Address | Subnet Mask |
| --- | --- | --- | --- |
| Administration VLAN 5 | 553 | IPv4 Network Address: 30.15.0.1/22  Hosts: 1022  Range: 30.15.0.1 - 30.15.3.254  Broadcast: 30.15.3.255  IPv6 Network: 2001:7A21:15ad:0000::/64 | IPv4 Subnet Mask: 255.255.252.0  IPv6 Subnet Mask: /64 |
| Developers VLAN 10 | 96 | IPv4 Network Address: 30.15.4.1/25  Hosts: 126  Range: 30.15.4.1 - 30.15.4.126  Broadcast: 30.15.4.127  IPv6 Network: 2001:7A21:15ad:0001::/64 | IPv4 Subnet Mask: 255.255.255.128  IPv6 Subnet Mask: /64 |
| Infrastructure VLAN 15 | 25 | IPv4 Network Address: 30.15.4.129/27  Hosts: 30  Range: 30.15.4.129 - 30.15.4.158  Broadcast: 30.15.4.159  IPv6 Network: 2001:7A21:15ad:0002::/64 | IPv4 Subnet Mask: 255.255.255.224  IPv6 Subnet Mask: /64 |
| External Link R1 G0/0/0 | 2 | IPv4 Network Address: 30.15.4.161/30  Hosts: 2  Range: 30.15.4.161 - 30.15.4.162  Broadcast: 30.15.4.163  IPv6 Network: 2001:7A21:15ad:0003::/64 | IPv4 Subnet Mask: 255.255.255.252  IPv6 Subnet Mask: /64 |
| ISP Router Lo0  (represents an address on the internet) | N/A | External IPv4 address 183.19.1.15/24  External IPv6 address 2002:6000::15/48 |  |

### Assign IP Networks to VLANs

| VLAN | VLAN Name | Devices | IPv4 Network Address | IPv6 Network Address |
| --- | --- | --- | --- | --- |
| 5 | Administration | PC1  PC2  PC3 | 30.15.0.2 255.255.252.0  30.15.0.3 255.255.252.0  30.15.0.4 255.255.252.0 | 2001:7A21:15ad:0000::1/64  2001:7A21:15ad:0000::2/64  2001:7A21:15ad:0000::3/64 |
| 10 | Developers | PC4  PC5  PC6 | 30.15.4.2 255.255.255.128  30.15.4.3 255.255.255.128  30.15.4.4 255.255.255.128 | 2001:7A21:15ad:0001::1/64  2001:7A21:15ad:0001::2/64  2001:7A21:15ad:0001::3/64 |
| 15 | Infrastructure | PC7  PC8  PC9 | 30.15.4.130 255.255.255.224  30.15.4.131 255.255.255.224  30.15.4.132 255.255.255.224 | 2001:7A21:15ad:0002::1/64  2001:7A21:15ad:0002::2/64  2001:7A21:15ad:0002::3/64 |
| 20 | Secure\_Down | All unused switch ports | N/A | N/A |
| 92 | Native |  |  |  |

### Assign IP Addresses to device interfaces.

* Assign IPv4 and IPv6 GUA and IPv6 Link-local addresses from the appropriate subnet to routers switches and host device interfaces. Fill in the blanks in the table below.

**Addressing Table**

| Device / Interface | IP Address / Prefix | Default Gateway if applicable |
| --- | --- | --- |
| Interface VLAN 5 | ip address 30.15.0.1 255.255.252.0 | ip helper-address 30.15.0.1 |
| S | ipv6 address FE80::5 link-local |  |
| ipv6 address 2001:7A21:15AD::1/64 |  |
| Interface VLAN 10 | ip address 30.15.4.1 255.255.255.128 | ip helper-address 30.15.4.1 |
|  | ipv6 address FE80::5 link-local |  |
| ipv6 address 2001:7A21:15AD:1::/64 |  |
| Interface VLAN 15 | ip address 30.15.4.129 255.255.255.224 | ip helper-address 30.15.4.129 |
|  | ipv6 address FE80::5 link-local |  |
| ipv6 address 2001:7A21:15AD:2::/64 |  |
| Interface VLAN 20 | None |  |
| None |  |
| None |  |
| Native VLAN 92 | None |  |
|  | None |  |
| None |  |

**Record interface names and IPv4 and IPv6 addresses on your diagram.**

## Initialize, Reload and Configure Basic Device Settings

### Initialize and reload router and switch.

* Erase the startup configurations and VLANs from the router and switch and reload the devices.
* After the switch is reloaded, configure the SDM template to support IPv6 as needed, and reload the switch again.

### Configure your Devices

Configuration tasks for the three routers include the following:

* Disable DNS lookup
* Hostname
* Domain name
* Encrypted

| Task | Specification where required |
| --- | --- |
| Disable DNS lookup | No ip domain-lookup |
| Router name | R1-15 |
| Domain name | example.com |
| Encrypted privileged EXEC password | router123 |
| Console access password | cisco123 |
| Set the minimum length for passwords | Set min length to 8 |
| Create an administrative user in the local database | User: admin  Password: admin123 |
| Set login on VTY lines to use local database | Line vty 0 4  Login local |
| Set VTY lines to accept SSH connections only | Line vty 0 4  Transport input ssh |
| Encrypt the clear text passwords | Service password-encryption |
| Configure an MOTD Banner | Welcome to example.com, Unauthorized access is prohibited. |
| Enable IPv6 Routing | Ipv6 unicast-routing |
| Configure all Interfaces, router sub-interfaces and Switch SVIs | VLAN’s created on switches 1-4 and assigned seperate IP Addresses.  Default Gateway on switches 1-4 set to External Link.  Router sub interfaces have been set on router for ip helper configuration for the vlans. |
| SSH access | hostname  RouterName  ip domain-name example.com  crypto key generate rsa  2048 username admin privilege 15 secret AdminPassword123  line vty 0 4  transport input ssh  login local  ip ssh version 2 |
| Switch default gateways to appropriate router sub-interface | interface Vlan5  ip address 30.15.0.3 255.255.252.0  ipv6 address 2001:7A21:15AD::3/64  ip helper-address 30.15.0.1  !  interface Vlan10  ip address 30.15.4.3 255.255.255.128  ipv6 address 2001:7A21:15AD:1::3/64  ip helper-address 30.15.4.1  !  interface Vlan15  ip address 30.15.4.131 255.255.255.224  ipv6 address 2001:7A21:15AD:3::2/64  ip helper-address 30.15.4.129  !  ip default-gateway 30.15.4.161 |

## Configure Network Infrastructure Settings (VLANs, Trunking, EtherChannel)

| Task | **Specification details and justify your design and choices** |
| --- | --- |
| Create VLANs | Created VLAN 5 Administration, VLAN 10 Developers, VLAN 15 Infrastructure, VLAN 20 Unused-Port and assign VLAN 92 as new Native |
| Secure all unused interfaces | S1,2,3:  FastEthernet0/10-24  GigabitEthernet0/1-2  Administratively Down  Hard coded as Access Port  Moved to VLAN 20 SECURE\_DOWN  S4:  FastEthernet0/1-3  FastEthernet0/10-24  GigabitEthernet0/2  Administratively Doen  Hard coded as Access Port  Moved to VLAN 20 SECURE\_DOWN |
| Create 802.1Q trunk links | All Switches FastEthernet0/4-9 |
| Configure Inter-vlan routing | FastEthernet0/1 Vlan 5  FastEthernet0/2 Vlan 10  FastEthernet0/3 Vlan 15 |
| Create a Layer 2 EtherChannel with two ports on each switch | All Switches Group/Channel 1 FastEthernet0/4-5  All Switches Group/Channel 2 FastEthernet0/6-7  All Switches Group/Channel 3 FastEthernet0/8-9 |
| Configure Access ports | S1, S2, S3 FastEthernet0/1-3 |

## Configure Switch security

| Task | Specification details and justify your design choices |
| --- | --- |
| Configure four different types of access port-security on access ports. Decide on the violation action and justify your decisions | Access port FastEthernet 0/1 Between PC1 and S1.  switchport port-security  switchport port-security maximum 1  Switchport port-security mac-address sticky  switchport port-security violation shutdown  switchport port-security aging time 2  Switchport port-security aging type inactivity |
| Secure all unused interfaces | All unused interfaces moved to VLAN20 Secure\_Down VLAN and administratively shut down and turned into access ports. |
| Configure DHCP snooping and limit the rate on appropriate ports | FastEthernet 0/1-3  Ip dhcp snooping  ip dhcp snooping limit rate 10 |
| Configure Dynamic ARP Inspection (DAI) on switches | ip arp inspection vlan 5, 10, 15 |
| Configure BPDUguard and PortFast on relevant ports | FastEthernet 0/1-3  spanning-tree bpduguard enable  spanning-tree portfast |

## Configure Host Support

### Configure Router to be a DHCP server

Configuration Tasks for AK\_Router and HN\_Router include the following

| Task | Specification details and justify your design choices |
| --- | --- |
| Create a default routes for IPv4 and IPv6 that direct traffic to external network | Default Gateway for network is ip address 30.15.4.161 255.255.255.252 on port gigabit 0/0/1. Traffic comes into this network and if is sent out of serial port 0/1/0 to ip address 183.19.1.15 which is the ISP. |
| Create separate IPv4 and IPv6 (O flag) DHCP pools for Developers and Infrastructure VLANs. Specify the default router gateway address for each. Exclude appropriate addresses | !  !  ip dhcp excluded-address 30.15.4.161  ip dhcp excluded-address 30.15.4.1 30.15.4.10  ip dhcp excluded-address 30.15.0.1 30.15.0.10  ip dhcp excluded-address 30.15.4.129 30.15.4.134  !  ip dhcp pool Administration  network 30.15.0.0 255.255.252.0  default-router 30.15.0.1  dns-server 8.8.8.8  ip dhcp pool Developers  network 30.15.4.0 255.255.255.128  default-router 30.15.4.1  dns-server 8.8.8.8  ip dhcp pool Infrastructure  network 30.15.4.128 255.255.255.224  default-router 30.15.4.129  dns-server 8.8.8.8  !  !  !  ip cef  ipv6 unicast-routing  !  no ipv6 cef  !  ipv6 dhcp pool Administration  address prefix 2001:7A21:15ad::/64 lifetime 172800 86400  dns-server 2001:4860:4860::8888  domain-name example.com  !  ipv6 dhcp pool Developers  address prefix 2001:7A21:15ad:0001::/64 lifetime 172800 86400  dns-server 2001:4860:4860::8888  domain-name example.com  !  ipv6 dhcp pool Infrastructure  address prefix 2001:7A21:15ad:0002::/64 lifetime 172800 86400  dns-server 2001:4860:4860::8888  domain-name example.com  !  ! |
| Verify and record Host device dynamic IP address parameters learned from DHCP | R1-15#show ip dhcp binding  IP address Client-ID/ Lease expiration Type  Hardware address  30.15.0.17 0002.171A.7CEE -- Automatic  30.15.0.21 0001.631A.01AB -- Automatic  30.15.0.14 0005.5E3D.87EE -- Automatic  30.15.4.11 00D0.D3C4.211B -- Automatic  30.15.4.12 0001.9728.5688 -- Automatic  30.15.4.14 0040.0BBA.5C3A -- Automatic  30.15.4.135 00D0.5801.E787 -- Automatic  30.15.4.137 00D0.BAC3.EAE0 -- Automatic  30.15.4.139 0050.0F13.92E6 -- Automatic  As the DHCPv6 server is SLAAC with Stateless, there is no device logging the ipv6 addresses, as the host devices use a combination of their own physical address and the routers IPv6 address. |

## Configure Static Routes

### Configure static routes to External networks.

* + - 1. Configure IPv4 Fully specified static routes and floating static routes to another students LAN. Use an administrative distance of **60** for the backup route
      2. Configure IPv6 next hop static routes and floating static routes to a third students LAN. Use an administrative distance of **60** for the backup route

Describe and justify your static route configurations:

|  |
| --- |
| Static route is configured to the ISP Router from the Network Router, the route is configured so that all packets sent with a destination IPv4 or IPv6 address not in the network range of the network is sent out of the static route towards the ISP router in an attempt to find the packet destination. |

## Test and Verify End-to-End Connectivity

Use the ping command to test IPv4 and IPv6 connectivity between all network devices. Paste a screenshot of your ping results into this document for verification.

Describe your Testing strategy:

|  |
| --- |
| Testing will be conducted using 1 Switch, 1 Router, 1 Host Device, 1 External Router and 1 External Host, each device will ping a different set of devices then the other to make sure all devices are pinged and connectivity is established.    Functional Testing  Connectivity Tests: Use tools like ping, traceroute, and SSH to verify basic connectivity between devices.  Configuration Verification: Ensure that all configurations (IP addresses, VLANs, routing protocols) are correctly set up.  Service Availability: Test if DHCP IPv4 and DHCP Stateless IPv6 is available.  Fault Tolerance and Redundancy Testing  Link Failures: Simulate link failures to verify the network’s ability to reroute traffic.  Device Failures: Simulate device failures to ensure high availability configurations (e.g., rerouting, load balancing) are effective.  Security Testing  Access Control: Verify that ACLs, firewall rules, and other security measures are properly configured. |

| From | To | Protocol | IP Address | Test Results |
| --- | --- | --- | --- | --- |
| PC1 | PC2 | IPv4 | 30.15.0.14 | Success |
|  |  | IPv6 | 2001:7A21:15AD:0:202:17FF:FE1A:7CEE | Success |
|  | PC3 | IPV4 | 30.15.0.11 | Success |
|  |  | IPv6 | 2001:7A21:15AD:0:201:63FF:FE1A:1AB | Success |
|  | S1-15 | IPV4 | 30.15.0.3 255.255.252.0 (VLAN 5) | Success |
|  |  | IPV6 | 2001:7A21:15AD::3/64 (VLAN 5) | Success |
|  | S2-15 | IPV4 | 30.15.0.4 255.255.252.0 (VLAN 5) | Success |
|  |  | IPV6 | 2001:7A21:15AD::4/64 (VLAN 5) | Success |
|  | ISP Router | IPV4 | 183.19.1.15 255.255.255.0 | Success |
|  |  | IPV6 | 2002:6000::15/48 | Success |
|  | R1-15 | IPV4 | 30.15.4.161 255.255.255.252 | Success |
|  |  | IPV6 | 2001:7A21:15AD:3::/64 | Success |
|  | PC-10 External | IPV4 | 192.168.0.10 | Success |
|  |  | IPV6 | 2001:6000::20 | Success |
| S1-15 | PC-1 | IPV4 | 30.15.0.16 | Success |
|  |  | IPV6 | 2001:7A21:15AD:0:205:5EFF:FE3D:87EE | Success |
|  | PC-4 | IPV4 | 30.15.4.17 | Success |
|  |  | IPV6 | 2001:7A21:15AD:1:201:97FF:FE28:5688 | Success |
|  | S3-15 | IPV4 | 30.15.0.5 255.255.252.0 (VLAN5) | Success |
|  |  | IPV6 | 2001:7A21:15AD::5/64 (VLAN5) | Success |
|  | S4-15 | IPV4 | 30.15.0.2 255.255.252.0 | Success |
|  |  | IPV6 | 2001:7A21:15AD::2/64 | Success |
|  | ISP Router | IPV4 | 183.19.1.15 255.255.255.0 | Success |
|  |  | IPV6 | 2002:6000::15/48 | Success |
|  | R1-15 | IPV4 | 30.15.4.161 255.255.255.252 | Success |
|  |  | IPV6 | 2001:7A21:15AD:3::/64 | Success |
| R1-15 | PC-5 | IPV4 | 30.15.4.11 | Success |
|  |  | IPV6 | 30.15.4.11 2001:7A21:15AD:1:240:BFF:FEBA:5C3A | Success |
|  | PC-6 | IPV4 | 30.15.4.14 | Success |
|  |  | IPV6 | 2001:7A21:15AD:1:2D0:D3FF:FEC4:211B | Success |
|  | S1-15 | IPV4 | 30.15.0.3 255.255.252.0 (VLAN 5) | Success |
|  |  | IPV6 | 2001:7A21:15AD::3/64 (VLAN 5) | Success |
|  | S2-15 | IPV4 | 30.15.0.4 255.255.252.0 (VLAN 5) | Success |
|  |  | IPV6 | 2001:7A21:15AD::4/64 (VLAN 5) | Success |
|  | ISP Router | IPV4 | 183.19.1.15 255.255.255.0 | Success |
|  |  | IPV6 | 2002:6000::15/48 | Success |
|  | PC 10 – External | IPV4 | 192.168.0.10 | Success |
|  |  | IPV6 | 2001:6000::20 | Success |
| PC 10 - External | PC-7 | IPV4 | 30.15.4.139 | Success |
|  |  | IPV6 | 2001:7A21:15AD:2:2D0:BAFF:FEC3:EAE0 | Success |
|  | PC-8 | IPV4 | 30.15.4.135 | Success |
|  |  | IPV6 | 2001:7A21:15AD:2:2D0:58FF:FE01:E787 | Success |
|  | S1-15 | IPV4 | 30.15.0.3 255.255.252.0 (VLAN 5) | Success |
|  |  | IPV6 | 2001:7A21:15AD::3/64 (VLAN 5) | Success |
|  | S2-15 | IPV4 | 30.15.0.4 255.255.252.0 (VLAN 5) | Success |
|  |  | IPV6 | 2001:7A21:15AD::4/64 (VLAN 5) | Success |
|  | R1-15 | IPV4 | 30.15.4.161 255.255.255.252 | Success |
|  |  | IPV6 | 2001:7A21:15AD:3::/64 | Success |
|  | ISP Router | IPV4 | 183.19.1.15 255.255.255.0 | Success |
|  |  | IPV6 | 2002:6000::15/48 | Success |
| ISP Router Lo0 | PC-10 External | IPV4 | 192.168.0.10 | Success |
|  |  | IPV6 | 2001:6000::20 | Success |
|  | R1-15 | IPV4 | 30.15.4.161 255.255.255.252 | Success |
|  |  | IPV6 | 2001:7A21:15AD:3::/64 | Success |
|  | S1-15 | IPV4 | 30.15.0.3 255.255.252.0 (VLAN 5) | Success |
|  |  | IPV6 | 2001:7A21:15AD::3/64 (VLAN 5) | Success |
|  | S2-15 | IPV4 | 30.15.0.4 255.255.252.0 (VLAN 5) | Success |
|  |  | IPV6 | 2001:7A21:15AD::4/64 (VLAN 5) | Success |
|  | PC-1 | IPV4 | 30.15.0.16 | Success |
|  |  | IPV6 | 2001:7A21:15AD:0:205:5EFF:FE3D:87EE | Success |
|  | PC-2 | IPV4 | 30.15.0.14 | Success |
|  |  | IPV6 | 2001:7A21:15AD:0:202:17FF:FE1A:7CEE | Success |

**Troubleshooting Reflection**

Describe at least three errors that you came across during your configuration. Describe the solution and the methods and commands you used to find the solution. Your reflection needs to be detailed to demonstrate your understanding and critical thinking

|  |  |
| --- | --- |
| **Problems/Errors** | **Solution, method and commands used** |
| %SPANTREE-2-RECV\_PVID\_ERR: Received 802.1Q BPDU on non trunk FastEthernet0/8 VLAN1.  %SPANTREE-2-BLOCK\_PVID\_LOCAL: Blocking FastEthernet0/8 on VLAN0001. Inconsistent port type. | I had created EtherChannels before hard coding ports as Trunk. To fix the error, I had to make sure all ports were hard coded as Trunk so they were matching. Once finished I reloaded all the effected Switches which fixed the issue.  (config)# interface range FastEthernet 0/4 - 9  (config-if-range)# switchport mode trunk  (config-if-range)# switchport trunk allowed vlan all |
| No IPv6 Enabled on Switches | The command to assign an IPv6 address to a vlan was not working. After some searching on the internet, I found the below code to enable dual ipv4 and ipv6. When this code was run on each switch it fixed the issue.  (config)# sdm prefer dual-ipv4-and-ipv6 default |
| IPv4 Bad Mask | Received this error after incorrectly inputting an ipv4 network address instead of a host address, after incrementing network addresses by 1 this issue was resolved. |
| IP-4-DUPADDR: Duplicate address 30.15.4.1 on Vlan10, sourced by 0060.2F13.9B02 | Duplicate IP addresses error, recieved because I configured the vlan’s before the DHCP pools, and assigned the first ip address from the available to the vlans instead of the dhcp pool. The solution is to go back to each vlan and update the ip address to incriment by 1. |
| Dhcp snooping | DHCP Snooping seems to disable IPv4 DHCP requests unless access ports are trusted. Unsure of the solution to this or if it is a packet tracer bug. |

## Command Journal

You may use the following template or another one that is approved by the tutor

|  |  |  |
| --- | --- | --- |
| **Command(s)** | **Example of Practice** | **Function / Description** |
| User mode:    Switch> | Press ***enter*** at the console page to enter user mode. | User mode: this is for viewing the state of the router and no modifications can be made here. Some pings |
| Privileged mode:    Switch# | Type ***enable*** while in user mode:    Switch> enable  Switch# | Type enable and receive the privileged exec mode. This mode allows configuration changes to be made. |
| Exit privileged mode: | Type ***disable*** while in privileged mode:    Switch# disable  Switch> | This is used to return to user mode without taking them to the console page, as with the commands **end** and **exit.** |
| Exit | Type ***exit*** while in any sub configuration mode: | Using this command will take you back to a previous configuration mode. |
| End | Type ***end* or *ctrl + z*** while in any sub configuration mode: | Using this command will take you straight back to privileged mode from and sub configuration mode. |
| Global Configuration mode:    Switch(config)# | Type ***configure*** ***terminal***while in privileged mode:    Switch# configure terminal  Switch(config)# | Used to access configuration options on the device. Typing **configure** will prompt the user to select which component to configure, terminal, memory or network.    If we type *configure terminal*, we can configure the switch directly. |
| Line Configuration mode:    Switch(config-line)# | Type ***line (management line type) (line number) (ending line number)*** while in configuration mode:    Switch(config)# line console 0  Switch(config-line)# | Used to access and modify the operation of a terminal line.    Line configuration commands always begin with line followed by the management type and the line number. |
| Interface Configuration mode:    Switch(config-if)# | Type ***interface (interface-id)*** while in configuration mode:    Switch(config)# interface vlan 1  Switch(config-if)# | Interface configuration modes modify how the interface operates, used to configure switch ports and router interfaces. |
| Hostname | Type ***hostname (new name)*** while in configuration mode:    Switch(config)# hostname S\_3  S\_3(config)# | Used to change the hostname of the switch or other cisco device. |
| No hostname | Type **no hostname**while in global configuration mode:    S\_3(config)# no hostname  Switch(config)# | Removes set hostname and returns hostname to factory default. |
| Banner motd | Type ***banner motd #(message)#*** in configuration mode:    Switch(config)# banner motd #  Message Of The Day# | This command displays a message to any user who wants to access the switch.    # is known as a delimiting character, it can be set to any character, but must start and end with that set character. |
| Clock set | Type ***clock set (hour:minute:second month day year)*** while in privileged mode:    Switch# clock set 2:33:01 August 26 2022 | Changes the current time stored on the switch. |
| Set privileged mode password:    Password: cisco | Type ***enable password (password)*** while in line configuration (console) mode:  Switch(config)# line console 0  Switch(config-line)# password cisco  Switch(config-line)# login  Switch(config-line)# end | This enables a password for privileged mode. Adding the command **login** in a new line enables password checking at login.    Console authentication requires both **password** and **login** commands to work.  **end** command takes the user back to configuration mode and updates the consoles running configuration. |
| Set secret password:    Password: \*\*\*\*\* | Type ***enable secret password (password)*** while in configuration mode:    Switch(config)# enable secret cisco  Switch(config)# end | This establishes a secret password for privileged mode also, but it will be displayed as ciphertext in the configuration file. |
| Set vty password:    Password: cisco | Type ***password (password)*** while in line configuration mode:    Switch(config)# line vty 0 15  Switch(config-line)# password cisco  Switch(config-line)# login  Switch(config-line)# end | This establishes a password to all vty lines. When a user wants to access through telnet or secure shell. You can set different passwords for different lines by changing which lines you connect to, for example line vty 0 5 will change the passwords for lines 0 – 5. |
| Encrypt plaintext passwords:    Password: 081909ASD09823AS | Type ***service password-encryption*** while in configuration mode:    Switch(config)# service password-encryption  Switch(config)# end | This encrypts all plaintext passwords that have been set on the device. When we use **show running-config** we will now see that all passwords have been encrypted. |
| Establish user:    Username: raine  Password: cisco | Type **username (username) password (password)** while in configuration mode:    Switch(config)#username raine password cisco  Switch(config)#line vty 0 4  Switch(config-line)#login local  Switch(config-line)#end | This establishes a username-based authentication system for the cisco device. By typing **login local** while in line configuration mode, we can enable password checking at login. The **end** command takes the user back to configuration mode and updates the consoles running configuration. |
| Disable ip domain look up: | Type ***no ip domain-lookup*** while in configuration mode:    Switch(config)# no ip domain-lookup | This disables DNS look up, this saves time if an incorrect command has been input during a prompt. |
| Reload | Type ***reload*** while in privileged mode:    Switch# reload  Proceed with reload? [confirm] *enter* | Reloads the system. Useful to test configuration changes, and reset changes if configurations have not been saved. |
| Erase start up configuration | Type ***erase startup-config*** in privileged mode:    Switch# erase startup-config | Erases all configurations to the cisco device. After this command is performed, the user must perform a **reload**. |
| Save changes made during configuration to startup-config: | Type ***copy running-config startup-config*** in privileged mode:    Switch(config)# copy running-config startup-config | This copies changes made to the running configuration, to the start-up configuration file. All changes made will now be the same every time a user connects to the cisco device. |
| Change ip address of cisco device: | Type ***ip address (IP) (Default Gateway)*** in interface configuration:    Switch(config)# interface vlan 1  Switch(config-if)# ip address 192.168.1.3 255.255.255.0  Switch(config-if)# no shutdown | Change interface to vlan 1, by default all switch ports are part of vlan 1. Now we can change the address by assigning an IP and default-gateway IP. Typing the **no shutdown** command brings up the interface. |
| No shutdown | Type ***no shutdown*** in interface configuration:    Switch(config)# interface vlan 1  Switch(config-if)# ip address 192.168.1.3 255.255.255.0  Switch(config-if)# no shutdown | The command no shutdown enables an interface, making it available to communicate with. For example, typing **no shutdown** in vlan1 interface after setting an IP Address enables that address in the switch. |
| Shutdown | Type ***shutdown*** in interface configuration:    Switch(config)# interface vlan 1  Switch(config-if)# shutdown | This command disables an interface, stopping communication with it. For example, in the above we have set our IP, by using the command **shutdown** in the vlan1 interface it will disable that address for the switch. |
| Show ip route | Type ***show ip route*** in privileged mode:    Router# show ip route | This command shows the different route sources. **L:** Directly connected local interface IP address. **C:** Directly connected network. **S:** Static route was manually configured by an administrator. **O:** OSPF. **D:** EIGRP. |
| Enable IPv6 routing | Type **ipv6 unicast-routing** in global configuration mode: | This command allows enables IPv6 on the cisco device, must be configured on switch and router to connect the two. |
| View Gigabit interface | Type **interface G0/1** in global configuration mode: | This command allows the user to change into the gigabit interface and change its configuration. |
| Set link-local | Type **ipv6 address fe80::1 link-local** in interface configuration mode: | This command enables the user to set a link-local address, link local addresses are signified by the fe80 at the beginning of the address. |
| Ping | Type ***ping (ip address)*** in privileged mode:    Switch# ping 192.168.1.3 | This command attempts to pings an ip address that is connected to the network.  It also populates the arp table if the ping is successful. |
| Traceroute | Type ***traceroute (ip address)*** in privileged mode:    Switch# traceroute 192.168.1.4 | The **traceroute** command lets you to see the path a packet takes in order to get to a destination from a source, it shows the sequence of hops the packet has taken between the two devices. |
| Show arp | Type ***show arp*** in privileged mode:    Switch# show arp | Builds an ARP table that displays ip and mac addresses based off of devices that have communicated with the switch. |
| Clear arp | Type ***clear arp*** in privileged mode:    Switch# clear arp | Clears the current arp table, and removes cached ip and mac addresses. |
| Show mac address-table | Type ***show mac address-table*** in privileged mode:    Switch# show mac address-table | Builds a mac Address table that displays all cached mac addresses on the switch. |
| Clear mac address-table | Type ***clear mac address-table*** in privileged mode:    Switch# clear mac address-table | Clears the current mac address table and removes them from the cache. |
| Show cdp | Type ***show cdp*** in privileged mode:    Switch# show cdp | This command shows the global CDP information, if the switch is sending CDP packets, the hold time value, and if CDPv2 advertisements are enabled. |
| Show cdp neighbors (detail) | Type ***cdp neighbors detail*** in privileged mode:    Switch# show cdp neighbors detail | This command shows the CDP information of your neighbour’s switch, such as device ID, local interface, hold time, capability, platform, switch version and port ID. |
| Show version | Type ***show version*** in privileged mode:    Switch# show version | Displays information about the switch, like the model, switch version and IOS image. |
| Show running-config | Type **show running-config**in privileged mode:    Switch# show running-config | Displays information about the current running config of the switch, such as set passwords, banner messages, domain lookup, addresses and ports. |
| Show startup-config | Type **show startup-config** in privileged mode:    Switch# show startup-config | Similar to the above, but for the saved startup-config. |
| Show interface (interface) | Type **show interface (interface)** in privileged mode:    Switch# show interface vlan1 | Displays information about an interface, including a description of it, its ip address, |
| Nslookup | Type **nslookup** in command prompt | When the nslookup command is issued, the default DNS server configured for your host is displayed. |
| Show current SDM template | Type **show sdm prefer** in privileged mode. | Verify that SDM is using either the dual-ipv4-and-ipv6 template or the lanbase-routing  template. |
| Change SDM template | Type **sdm prefer dual-ipv4-and-ipv6 default** in configuration mode. | Assigns dual-ipv4-and-ipv6 template to the cisco device. |
| Default-gateway | Type **Ip default-gateway (default gateway)** in configuration mode. | Configures the ipv4 default gateway. |
| Unicast-routing | Type **unicast-routing** in global configuration mode. | Enables configuration of ipv6 for the cisco device. |
| Ipv6 Configuration | Type **ipv6 address (ipv6**) in interface configuration mode. | Assigns an Ipv6 address to the interface. |
| Ipv6 link-local configuration | Type **ipv6 address (ipv6 link-local address) link-local** in interface configuration mode. | Assigns an Ipv6 link-local address to the interface. |
| Transport input SSH/Telnet | Type **transport input ssh** in line configuration mode. | Configure the types of terminals that can access to the device, SSH or Telnet. |
| Logging synchronous | Type **logging synchronous** in line configuration mode. | Makes sure commands are not interrupted by line protocol logs. |
| Ip-domain name | Type **ip domain-name (domain-name).local** in configuration mode. | Set a domain name for your cisco device. |
| Crypto key | Type **crypto key generate rsa** in configuration mode. | Generates an RSA keypair, only usable once a domain name has been set. It then prompts the user to input a bit modulus amount. 2048 or above is standard and better encryption, but takes longer to calculate. |
| Ip SSH Version | Type **ip ssh version 2** in configuration mode. | Swaps the SSH connection version from the default (V.1) to the newer V.2 |
| Login local | Type **login local** in line configuration mode. | Searches the local database for usernames and passwords. |
| ip arp inspection vlan 5,10,15 | Type this command in configuration mode. | Enables ARP inspection on VLANs 5, 10, and 15 to mitigate ARP spoofing. |
| ip dhcp snooping vlan 5,10,15 | Type this command in configuration mode. | Enables DHCP snooping on VLANs 5, 10, and 15 to prevent rogue DHCP servers. |
| spanning-tree mode pvst | Type this command in configuration mode. | Sets the Spanning Tree Protocol (STP) mode to Per VLAN Spanning Tree (PVST). |
| switchport trunk native vlan 92 | Type this command in interface configuration mode. | Sets VLAN 92 as the native VLAN on trunk ports. |
| switchport mode trunk | Type this command in interface configuration mode. | Configures the interface as a trunk port. |
| switchport access vlan 5 | Type this command in interface configuration mode. | Sets VLAN 5 as the access VLAN. |
| ip dhcp snooping trust | Type this command in interface configuration mode. | Marks the port as trusted for DHCP snooping. |
| ip dhcp snooping limit rate 10 | Type this command in interface configuration mode. | Limits the rate of DHCP packets on the port to 10 packets per second. |
| switchport port-security | Type this command in interface configuration mode. | Enables port security on the port. |
| switchport port-security mac-address sticky | Type this command in interface configuration mode. | Dynamically learns and stores MAC addresses on the secure MAC address table. |
| switchport port-security mac-address <mac> | Type this command in interface configuration mode. | Specifies a specific MAC address for port security. |
| switchport port-security aging time 2 | Type this command in interface configuration mode. | Sets the aging time for secure MAC addresses to 2 minutes. |
| spanning-tree portfast | Type this command in interface configuration mode. | Enables PortFast to minimize STP convergence time on the port. |
| spanning-tree bpduguard enable | Type this command in interface configuration mode. | Enables BPDU guard to protect against accidental loops on the port. |
| ip helper-address 30.15.0.1 | Type this command in interface configuration mode. | Configures a DHCP relay agent address for VLAN 5. |
| ip default-gateway 30.15.4.161 | Type this command in global configuration mode. | Sets the default gateway IPv4 address for the switch. |
| ip dhcp excluded-address 30.15.4.161 | Type this command in global configuration mode. | Excludes the IP address 30.15.4.161 from DHCP pool allocation. |
| ip dhcp pool Administration | Type this command in global configuration mode. | Configures DHCP pool for VLAN 5 (Administration). |
| ip cef | Type this command in global configuration mode. | Enables Cisco Express Forwarding. |
| no ipv6 cef | Type this command in global configuration mode. | Disables Cisco Express Forwarding for IPv6. |
| ipv6 dhcp pool Administration | Type this command in global configuration mode. | Configures IPv6 DHCP pool for VLAN 5 (Administration). |
| ip classless | Type this command in global configuration mode. | Enables classless routing. |
| ip route 0.0.0.0 0.0.0.0 183.19.1.15 | Type this command in global configuration mode. | Configures a default route. |
|  |  |  |

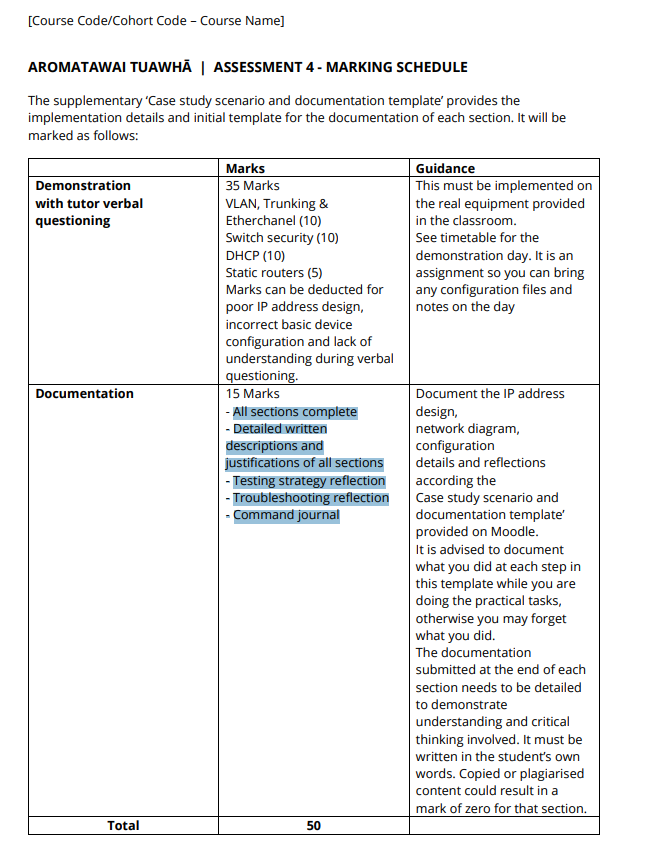
## Clean up

NOTE: DO NOT PROCEED WITH CLEANUP UNTIL YOUR INSTRUCTOR HAS CHECKED YOUR CASE STUDY IMPLEMENTATION AND HAS INFORMED YOU THAT YOU MAY BEGIN CLEAN UP.

Restore host computer network connectivity, and then turn off power to the host computers.

Before turning off power to the router and switch, remove the NVRAM configuration files and VLAN.dat file from both devices and reload all devices.

Disconnect and neatly put away all LAN cables.



End of document