CCNA2v7 Case Study

1. **Group Number \_\_\_17\_\_\_\_ = 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**

**S1n**

1. Icon

   Description automatically generated

**PCB**

1. Icon

   Description automatically generated

**PCA**

1. LAN IPv4 address 30.**17**.0.0 /16
2. LAN IPv6 address 2001:7A21:**17**ad:: /48
3. External IPv4 address 183.19.1.17 /24
4. External IPv6 address 2002:6000::17/48

# 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 STATELESS (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 |
| --- | --- | --- | --- |
| Developers VLAN | 96 | 30.17.4.0  2001:7A21:**17**ad:40::1 /64 | /25 255.255.255.128 |
| Infrastructure VLAN | 25 | 30.17.4.128  2001:7A21:**17**ad:30::1 /64 | /27 255.255.255.224 |
| Administration VLAN | 553 | 30.17.0.0  2001:7A21:**17**ad:20::1 /64 | /22 255.255.252.0 |
| External Link Rn G0/1 | 2 | 183.19.1.17  2002:6000::**17**  Fe80::**17** | 255.255.255.0  /48  /64 |
| ISP Router Lo0  (represents an address on the internet) | N/A | 183.19.1.1 /24 2002:6000::1/48 | N/A |
|  |  |  |  |

### Assign IP Networks to VLANs

| VLAN | VLAN Name | Devices | IPv4 Network Address | IPv6 Network Address |
| --- | --- | --- | --- | --- |
| 40 | Developers | PCA | 30.17.4.0 | 2001:7A21:**17**ad:40::1 /64 |
| 30 | Infrastructure | PCB | 30.17.4.128 | 2001:7A21:**17**ad:30::1 /64 |
| 20 | Administration | PCC | 30.17.0.0 | 2001:7A21:**17**ad:20::1 /64 |
| 10 | Secure\_Down | All unused switch ports | N/A | N/A |
| 92 | Native | nil |  |  |
| 100 | External | 2 | 183.19.1.17 | 2002:6000::17/48 |

### 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 |
| --- | --- | --- |
| PCA dev  Fe0/0 | 30.17.4.5 255.255.255.128 | 30.17.4.126 |
|  | 2001:7A21:17AD:40:230:F2FF:FE56:D4BC |  |
|  | FE80::230:F2FF:FE56:D4BC |  |
| PCB infrastructure Fe0/0 | 30.17.4.135 255.255.255.224 | 30.17.4.158 |
|  | 2001:7A21:17AD:30:290:21FF:FE2A:7C92 |  |
|  | FE80::290:21FF:FE2A:7C92 |  |
| PCC Admin Fe0/0 | 30.17.0.3 255.255.252.0 | 30.17.3.254 |
| 2001:7A21:17AD:20:230:A3FF:FE64:E1A4 |  |
|  | FE80::230:A3FF:FE64:E1A4 |  |
| Switch  Vlan20  Vlan30  Vlan40 | 30.17.0.1 /22 2001:7A21:17AD:20::1/64  30.17.4.129 /272001:7A21:17AD:30::1/64  30.17.4.1 /25 2001:7A21:17AD:30::1/64 |  |
| Switch 2  Vlan20  Vlan30  Vlan40 | 30.17.0.2 /22 2001:7A21:17AD:30::2/64  30.17.4.130 /27 2001:7A21:17AD:30::2/64  30.17.4.2 /25 2001:7A21:17AD:30::2/64 |  |
| Router1 g0/0 to switch  G0/0.20  G0/0.30  G0/0.40  G0/1 to internet | 30.17.3.254 /22 2001:7A21:17AD:20::1/64 FE80::20  30.17.4.158 /27 2001:7A21:17AD:30::1/64 FE80::30  30.17.4.128 /25 2001:7A21:17AD:40::1/64 FE80::40  192.168.1.1 /16 2002:1000::1/48 |  |
|  |  |  |
|  |  |
| Router2 |  |  |
| 0/0/0 | 192.168.2.1/16 2002:2000::1/48 |  |
| 0/01 | 183.19.1.1/24 |  |
| PC External | 183.19.1.17/24 2002:6000::17/48 | 183.19.1.1 |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |
|  |  |  |
|  |  |  |
|  |  |
|  |  |  |
|  |  |
|  |  |
|  |  |  |
|  |  |  |
|  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
| PC-B NIC |  |  |

**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 | hostname R1 |
| Domain name | ip domain-name thomas.com |
| Encrypted privileged EXEC password | Enable secret cisco |
| Console access password | Line console 0, password cisco, login |
| Set the minimum length for passwords | security password min-length 5 |
| Create an administrative user in the local database | Username Thomas privilege 15 secret cisco |
| Set login on VTY lines to use local database | Login local |
| Set VTY lines to accept SSH connections only | Transport input ssh |
| Encrypt the clear text passwords | Service password-encryption |
| Configure an MOTD Banner | Banner motd “Welcome to Thomas.com” |
| Enable IPv6 Routing | Ipv6 unicast routing |
| Configure all Interfaces, router sub-interfaces and Switch SVIs | Line console 0, password 7 cisco |
| SSH access | Hostname, ip domain-name Thomas.com crypto key generate rsa 512 |
| Switch default gateways to appropriate router sub-interface | Ip default-gateway 30.17.1.1 |
|  |  |

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

| Task | **Specification details and justify your design and choices** |
| --- | --- |
| Create VLANs | Created 3 vlans using VLSM, starting with /22 the largest, 1022 hosts, enough for 553 hosts with 469 leftover. Then /25 with a space of 126 hosts for 96 devices with 30 leftover. And /27 with 30 hosts for 25 devices with 5 leftover. Note that I did subnet for another subnet with /30, for 2 devices, but I don’t see how that is needed. |
| Secure all unused interfaces | Any port that doesn’t have a device connected to it which is 3,4 and 6-23 are manually shut off to prevent unapproved devices being connected |
| Create 802.1Q trunk links | Our switches have two trunk links, to allow all vlan traffic between them. |
| Configure Inter-vlan routing | On our switch g0/0 interface we have added 3 sub interfaces 0.20, 0.30 and 0.40 to act as a default gateway for each of our vlans. Traffic passing between vlans will have to go to the router first to enter the vlan. |
| Create a Layer 2 EtherChannel with two ports on each switch | Our switches are joined by an EtherChannel, with fe0/0 and fe0/1, for redundancy and loadbalancing. It would have been nice to have a gigabit etherchannel but you cant combine a fastethernet and a gigabit port in an etherchannel. One of our two gigabit ports on S1 is being used for the router unfortunely so this cant be done. |
| Configure Access ports | All ports not connected to another switch 3-24 are hardcoded access ports. Ports connected to a device are allocated a vlan |

## 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 | All of our access ports have port security enabled, with a maximum of 3 mac-addresses allowed to send data to the port, any more would be above the expected amount for the network. We have a sticky mac-address that meants that only the first one mac-address to send data to the port will be allowed to send data. However aging will remove this sticked mac-adddress after 10 days. I was not able to pick the type of aging, could have been a packet tracer thing. Whenever a device breaks one of these rules the port will block data from that unauthorized device, until the authorized device comes back. I could of made it disable the port completely but as there is a lot of testing in this environment that would be a huge pain. |
| Secure all unused interfaces | All interfaces not being used are administratively shutdown to prevent anyone plugging in any unauthorized devices that could cause hard to the network. |
| Configure DHCP snooping and limit the rate on appropriate ports | DHCP snooping has been enabled to prevent the switch from listing to DHCP offers from fake DHCP clients, this means enabling it on all access ports and setting trust on the fe0/1-2 trunk ports and gigabit0/1 port that’s connect to the router/dhcp server. I’m currently running into an error that prevents dynamic dhcp on a client on fe/0/24, only by trusting that port, will it work. I have also limited the rate of allowed dhcp requests to 5 |
| Configure Dynamic ARP Inspection (DAI) on switches | I have enabled ARP inspection to prevent attackers from spoofing the mac address of trusted devices. It will check arp requests to make sure it is coming from a trusted device and is not invalid or gratuitous. It is inspecting the source mac address on all vlans, I have set my trust links to be trusted sources of arp requests |
| Configure BPDUguard and PortFast on relevant ports | On all access ports I have enabled BPDU guard to prevent an attacker from inserting a switch into the network. Switches gain control with BPDU messages, so if this is coming from one of my access ports, then it knows it is a switch and will error disable the port to stop the attack. I have set this as default on all portfast ports. |

## 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 | I have created a |
| Create separate IPv4 and IPv6 DHCP pools for Developers and Infrastructure VLANs. Specify the default router gateway address for each. Exclude appropriate addresses | I have an ipv4 dhcp server working, with a pool for each vlan. Each pool has a default gateway at the last host address in the vlans subnet. Vlan 20 has 30.17.3.254, 30 has 30.17.4.158, 40 has 30.17.4.126. The DHCP server does work, however me and Raine have an issue with ip dhcp snooping blocking dhcp requests on the access ports. It only works when we trust the access port, which should only be done for trunk ports or ports to dhcp servers. I also have a ipv6 dhcp server, with pools in each of the subinterfaces on the router. Ge0/0.20 has 2001:7A21:17AD:20::1/64, 30 has 2001:7A21:17AD:30::1/64 and 40 has 2001:7A21:17AD:40::1/64. They all have the O flag meaning they are stateless dhcp servers, meaning the server provides some information but the client makes its own gua address. |
| Verify and record Host device dynamic IP address parameters learned from DHCP | Network address and subnet  30.17.0.0 255.255.252.0  Default-router: 30.17.x.x for each subnet  Dns-server: 30.17.x.x  Domain-name: Thomas.com |
|  |  |

## 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:

|  |
| --- |
| Because there is no third LAN, I have one default static route from R1 to R2. I have set a directly connected static route for ipv4. Traffic for 183.19.0.0 255.255.0.0 goes to GE0/0/1. I was not able to set a ip address for a fully specified route, this might be a packet tracer thing, or something to do with the ip addressing I have set up as I put the ip addresses for between the two routers as 192.168.1.1/16 and 192.168.2.1/16. I did subnet for two external addresses in /30 but didn’t not use them and it works currently to ping from a client in our network to 183.19.1.17.  As for ipv6 I have tried to create a static route but nothing will be sent outside of the network, I can ping from between the routers but R1 will not send anything if it is past 183.19.1.1. It is currently as 0::/0 so it should forward everything no matter what but I cant figure why it wont send packets. |

## 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:

|  |
| --- |
| I’m going to go into a terminal on every device, and ping every ipv4 and ipv6 address in the list generated above. If the device has multiple ips for vlans or subinterfaces I will pick one at random to prevent too many things to ping. |

| From | To | Protocol | IP Address | Test Results |
| --- | --- | --- | --- | --- |
|  | PCB | Ipv4 | 30.17.4.135 | Success |
|  |  | Ipv6 | 2001:7A21:17AD:30:290:21FF:FE2A:7C92 | Success |
|  | PCC | Ipv4 | 30.17.0.3 | Success |
|  |  | Ipv6 | 2001:7A21:17AD:20:230:A3FF:FE64:E1A4 | Success |
|  | S1 | Ipv4 | 30.17.0.1 | Success |
| PCA |  | Ipv6 | 2001:7A21:17AD:40::3 | Success |
|  | S2 | Ipv4 | 30.17.4.130 | Success |
|  |  | Ipv6 | 2001:7A21:17AD:20::2 | Fail |
|  | R1 | Ipv4 | 30.17.4.126 | Success |
|  |  | Ipv6 | 2001:7A21:17AD:40::1 | Success |
|  | External | Ipv4 | 183.19.1.17 | Success |
|  |  | Ipv6 | 2002:6000::17 | Fail |
|  |  |  |  |  |
|  |  |  |  |  |
|  | PCA | Ipv4 | 30.17.4.5 | Success |
| S1 |  | Ipv6 | 2001:7A21:17AD:40:230:F2FF:FE56:D4BC | Success |
|  | PCB | Ipv4 | 30.17.4.135 | Success |
|  |  | ipv6 | 2001:7A21:17AD:30:290:21FF:FE2A:7C92 | fail |
|  | PCC | Ipv4  Ipv6 | 30.17.0.3  2001:7A21:17AD:20:230:A3FF:FE64:E1A4 | Success  Success |
|  | S2 | Ipv4  Ipv6 | 30.17.4.130  2001:7A21:17AD:20::2 | Success  Fail |
|  | R1 | Ipv4  Ipv6 | 30.17.0.1  2001:7A21:17AD::1 | Success  Fail |
|  | External | Ipv4  Ipv6 | 183.19.1.17  2002:6000::17 | Fail  Fail |
|  | PCA | Ipv4 | 30.17.4.5 | Success |
|  |  | Ipv6 | 2001:7A21:17AD:40:230:F2FF:FE56:D4BC | Success |
|  | PCB | Ipv4 | 30.17.4.135 | Success |
|  |  | Ipv6 | 2001:7A21:17AD:30:290:21FF:FE2A:7C92 | Success |
|  | PCC | Ipv4 | 30.17.0.3 | Success |
| R1 |  | Ipv6 | 2001:7A21:17AD:20:230:A3FF:FE64:E1A4 | Success |
|  | S1 | Ipv4 | 30.17.0.1 | Success |
|  |  | Ipv6 | 2001:7A21:17AD:40::3 | Fail |
|  | S2 | Ipv4 | 30.17.4.130 | Success |
|  |  | Ipv6 | 2001:7A21:17AD:20::2 | Fail |
|  | External | Ipv4 | 183.19.1.17 | Success |
|  |  | Ipv6 | 2002:6000::17 | Fail |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  | PCA | Ipv4 | 30.17.4.5 | Success |
|  |  | Ipv6 | 2001:7A21:17AD:40:230:F2FF:FE56:D4BC | Fail |
|  | PCB | Ipv4 | 30.17.4.135 | Success |
|  |  | Ipv6 | 2001:7A21:17AD:30:290:21FF:FE2A:7C92 | Fail |
| External | PCC | Ipv4 | 30.17.0.3 | Successs |
|  |  | Ipv6 | 2001:7A21:17AD:20:230:A3FF:FE64:E1A4 | Fail |
|  | S1 | Ipv4 | 30.17.0.1 | Fail |
|  |  | Ipv6 | 2001:7A21:17AD:40::3 | Fail |
|  | S2 | Ipv4 | 30.17.4.2 | Fail |
|  |  | Ipv6 | 2001:7A21:17AD:40::3 | Fail |
|  | R1 | Ipv4 | 30.17.4.126 | Success |
|  |  | Ipv6 | 2001:7A21:17AD::1 | Fail |

**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** |
| IPv6 default route doesn’t work | No solution found, I have tried all sorts of static configurations like ipv6 on the ports. Not even the most basic 0::/0 will forward data. After consulting tutor, R1 has been configured correctly, and R2 shouldn’t have an ipv6 default route to R1 |
| DHCP messages would get blocked by the switch. | The DHCP snooping on the switch was blocking messages from getting to the router. This was because the switch was added option 82 information to dhcp packets, which the router was discarding as a security measure. This can be fixed with the “ip dhcp relay information trust-all command” which makes the router trust packets with option 82 information. |
| DHCP messages from S2 to S1 were not being forwarded. | Same as the issue before, S1 was discarding packets sent by S2 that had option 82 added. The command “ip dhcp snooping information option allow-untrusted” ensures they get forwarded. This still didn’t allow them to get the dhcp messages as the etherchannel between S1 and S2 did not have dhcp snooping trust applied to it. This is a fault of packet tracer not applying this. After deleting the etherchannel, they were able to get the dhcp messages. |
|  |  |

## Command Journal

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

|  |  |
| --- | --- |
| enable | Enter privilege exec mode to access commands to edit the switch settings |
| config t | Enter global configuration mode to access commands to edit the console settings |
| line console 0  interface vlan 1  interface f0/1 | Enter line configuration mode to change settings like ip or passwords. |
| line console 0  password cisco  login | Set a password to secure user exec mode, the first mode on the switch when you log in |
| config t  enable secret cisco | Set a password to secure privileged exec mode, the mode entered with enable |
| config t  line vty 0 15  password cisco  login | Set a password to secure vty line access, for remote access from ssh or telnet |
| config t  service password-encryption | Encrypt passwords from plain-text |
| show running-config | Displays all current configuration settings on the switch |
| hostname karam\_switch | Set the name of the device to karam\_switch> |
| config t  banner motd #message here# | Set a banner to be displayed when a user is attempting to log into the switch |
| config t  no ip domain-lookup | Prevents the switch from looking for a dns server if you type a command wrong |
| erase startup-config | Delete the currently saved settings to be run when the switch is rebooted |
| copy running-config startup-config | Save the current settings to be run when the switch is rebooted |
| reload | Reboot the switch |
| ping 10.1.10.10 | ping ip address |
| traceroute 10.1.10.10 | trace the hops a frame goes through from the ip address back to the switch |
| show ip route | Display the routing table |
| show ip arp | Display the arp table |
| show version | Displays the ios version and table name |
| show cdp neighbors detail | Display information about switches connected to your switch |
| show ip interface brief | Display status information for all the ports on the device |
| show interfaces (vlan1 or port) | Display status information for a certain port |
| config t  interface vlan 1 10.1.10.110 255.255.255.0  no shutdown | Set the ipv4 and subnet mask for the whole device  No shutdown sets the vlan1 to enabled, will be in administratively down mode if this isn’t done |
| ip default-gateway 192.168.1.1 | Set the default gateway for the switch to use |
| show mac address-table | Displays all saved macs and ips, and the port they are routed to on the switch. |
| clear mac address-table dynamic | Delete all macs and ips saved on the switch |
| show sdm prefer |  |
| sdm prefer dual-ipv4-and-ipv6 default | Configures the switch to use both ipv4 and ipv6 addresses |
| ipv6 address 2001:acad:n:n::63/64 | Assign a GUA ipv6 address |
| ipv6 unicast-routing | Enables the router to route/forward ipv6 packets |
| Interface gigabitethernet 0/0 | Enter the interface for a gigabitethernet port |
| Ipv6 address fe80::200 link-local | Assign an ipv6 link local address |
| **security passwords min-length 8** | Set a minimum acceptable password length with the security passwords min-length command. |
| **login block-for 120 attempts 3 within 60** | Deter brute-force password guessing attacks with the **login block-for *#* attempts *#* within *#*** command |
| Exec-timeout 5 30 | Disable an inactive privileged EXEC mode access after a specified amount of time with the **exec-timeout** command. |
| Transport input ssh/telnet | Enable vty inbound ssh/telnet sessions |
| ip-domain name | Configure the IP domain name of the network by using the global configuration mode command |
| **crypto key generate rsa general-keys modulus #** | Generate a key for ssh encryption # is size of bits in the key. 360-2048 Recommended is 1024 |
| Login local | Use the login local line to authenticate vty line access. |
| Ip ssh version 2 | Uses version 2 of the ssh protocol. |
| Ip ssh authentication-retries 5 | Locks user out after # of wrong attempts |
| Ip ssh time-out 120 | Sets max wait time for a response from the client when trying to establish ssh connection |
| Show ip ports all | Shows all services running on ports |
| show control-plane host open-ports | Shows all services running on ports, for prior ios-xe versions. |
| Duplex | Enable full/half/auto duplux operation |
| speed | Configure traffic speed, 10/100/auto |
| Mdix auto | Enable use of straight and crossover cable |
| Ctrl + a | Go to start of line |
| Vlan <vlan id number> | Create a vlan |
| (config-vlan) name <name of vlan> | Name the vlan (optional) |
| Switchport access vlan <vlan id> | Assign vlan to a switch port |
| Show vlan | Shows all vlans and ports they are assigned to. |
| Switchport trunk allowed vlan <vlan id> | Allow traffic from these vlans through trunk links |
| Switchport mode access/trunk/dynamic | Set the type of port. |
| Show interfaces fastethernet 0/1 switchport | Verify port modes |
| Switchport trunk native vlan <vlan id> | Set the native vlan id |
| Show spanning tree | See root and bridge id priority, address and cost. |
| Spanning tree mode <type of mode> | PVST+/RAPID/RAPID-PVST+/MST |
| spanning-tree vlan <vlan-id> priority <0-61440> | Change the root bridge |
| Spanning-tree vlan <id> root primary |  |
| Spanning-tree vlan <id> root secondary |  |
| Spanning-tree portfast | Enable portfast on interface, add default for all interfaces |
| spanning-tree bpduguard enable | Turns on bpduguard on access ports, add default for all interfaces |
| (config-if-range) channel-group 1 mode ? | Set etherchannel mode, active/auto/desirable/on/passive |
| Channel-protocol <pagp or lacp> | Set the protocol for the different negotiation protocols |
| Show etherchannel summary | See set etherchannels and their status |
| Ip dhcp pool <name> | Create a dhcp pool |
| Network <network address> <subnet mast> | Set the networks ip from which to give ips |
| Default-router <ip of default gateway> | Set the default gateway to give |
| Dns-server <ip of dns server> | Set ip of dns server to give |
| Ip dhcp excluded-address <ip addresses to exclude> | Set ips that the dhcp server will not give out |
| Show ip dhcp binding | See the mac address and ips that are given out by the server |
| Show ip dhcp pool <name> | See a pools given, excluded and potential ip addresses |
| Domain-name <example.com> | Set the name of the domain pc will be in |
| Ipv6 nd other-config-flag | Set O flag on ipv6 dhcp server |
| Ipv6 dhcp server <name> | Set name of ipv6 server |
| Ipv6 dhcp pool <name> | Create and name ipv6 dhcp pool |
| Ipv6 nd managed-config-flag | Set M flag |
| Ipv6 nd prefix default no-autoconfig | For Stateful dhcp server |
| Show ipv6 dhcp pool |  |
| Show ipv6 dhcp binding |  |
| Standby <group number 0-4095> ip <shared/virtual ip> | Turn on HSRP on router |
| Show standby | Verify HSRP settings |
| Standby <group number> priority <0-255> | Set priority to become active/standby |
| Standby <group no> timers <hello time> <hold time> | Change HSRP timers |
| Standby <group no> preempt | Give router power to become the active router |
| Standby <group no> track <interface> <decrease amount> | Set the amount of priority to go down if interface goes down |
| Switchport port-security | Enable port security on ports, do first to turn on |
| Switchport port-security mac-address sticky | Allow data only from first mac address on port |
| Switchport port-security maximum <no> | First amount of mac addresses allowed to send data |
| Switchport port-security aging time <time> | How long until the list of stored mac addresses is cleared |
| Switchport port-security violation | What to do if the rules are broken |
| Protect/restrict | Will block data until right device is connected, protect will notify, restrict wont |
| Shutdown | Port will go into error disabled state when rule broken, has to be shutdown, no shutdown to get back up. Is default. |
| Show port-security interface | See security settings on an interface |
| Show port-security address | See stored mac address and remaining age. |
| Ip dhcp snooping | Enable dhcp snooping on all ports |
| Ip dhcp snooping trust | On trusted ports connected to router/dhcp server to enable tranmisison of dhcp packets |
| Ip dhcp snooping limit rate | Limit the amount of dhcp discovery messages that can be received per second |
| Ip arp inspection | Enables checking arp packets |
| Show ip route | Show routing table of router |
| ip route network-address subnet-mask { ip-address | exit-intf [ip-address]} [administrative distance] | Set a static route to route certain traffic to a certain interface/ip address |
| ipv6 route ipv6 prefix/prefix length { ipv6-address | exit-intf [ip-address]} [administrative distance] |  |
|  |  |

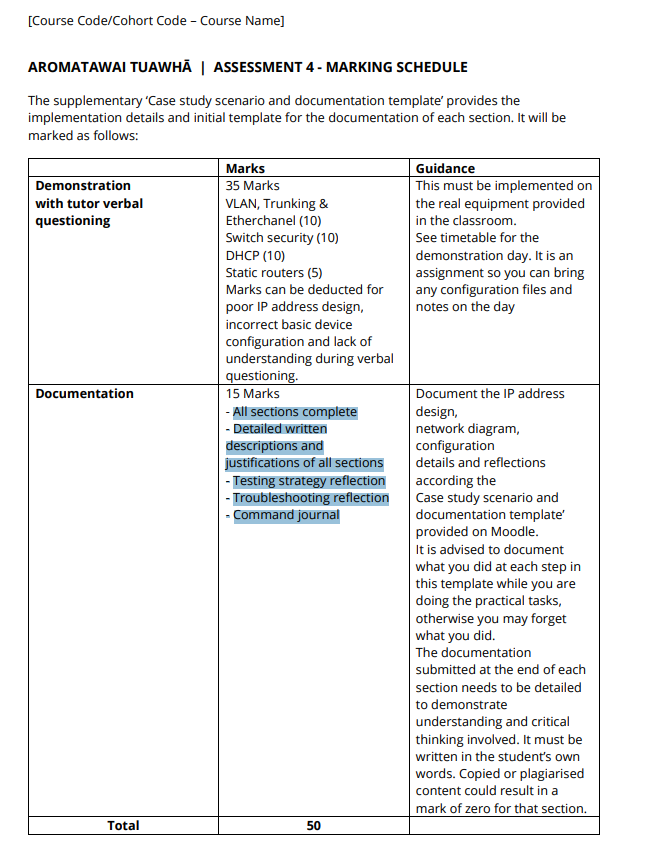
## Clean up

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