COMP702 Scaling Networks Case

Name: Raine Roberts	ID:
Module: Network Security COMP702	Semester: 2

Company and Scenario Description

The company in focus is **RaineCorp**, a mid-sized technology firm specializing in IT consulting and software development.

The organization has 200 employees distributed across three departments: STAFF, CORPORATE and IT. The company operates from their first office in Hamilton City and has a secondary site operating in Tauranga City. The network must ensure high availability, scalability, and security while catering to inter-department communication and external client services.

RaineCorp requires a robust network that supports efficient data flow, segregates department traffic for security, and ensures high-speed internet access for employees. Scalability is critical as the company anticipates growth, business continuity and high availability are essential.

Network Design Justification

IP Addressing Scheme and VLAN Design

An IP addressing scheme utilizing **VLSM (Variable Length Subnet Masking)** has been implemented for efficient allocation. Based on the provided configurations:

- **VLAN 10 - STAFF**: 192.168.10.1/24
- **VLAN 20 - CORPORATE**: 192.168.20.1/24
- **VLAN 30 - IT**: 192.168.30.1/24
- **VLAN 99 - NATIVE**: For management and trunking purposes.
- **VLAN 199 - ADMIN_DOWN**: Reserved and unused ports.

Each VLAN aligns with departmental boundaries to ensure traffic isolation and enhance security. VLAN configurations are consistent across sites (Hamilton and Tauranga).

Network Devices and Loopback Interfaces

Core routers and Layer 3 switches have been configured with loopback interfaces to serve as OSPF router IDs and for management purposes. Each device has a unique loopback address to streamline network operations and troubleshooting.
Examples:

- **TGA_1_Loopback**: 5.5.5.5
- **HAM_1_Loopback**: 3.3.3.3

Detailed Network Diagram

A comprehensive network topology diagram is included, showcasing:

- Core routers, Layer 3 switches, and end devices.
- VLANs mapped to respective switches and ports.
- Trunk links between switches and routers.
- Redundant connections for high availability.

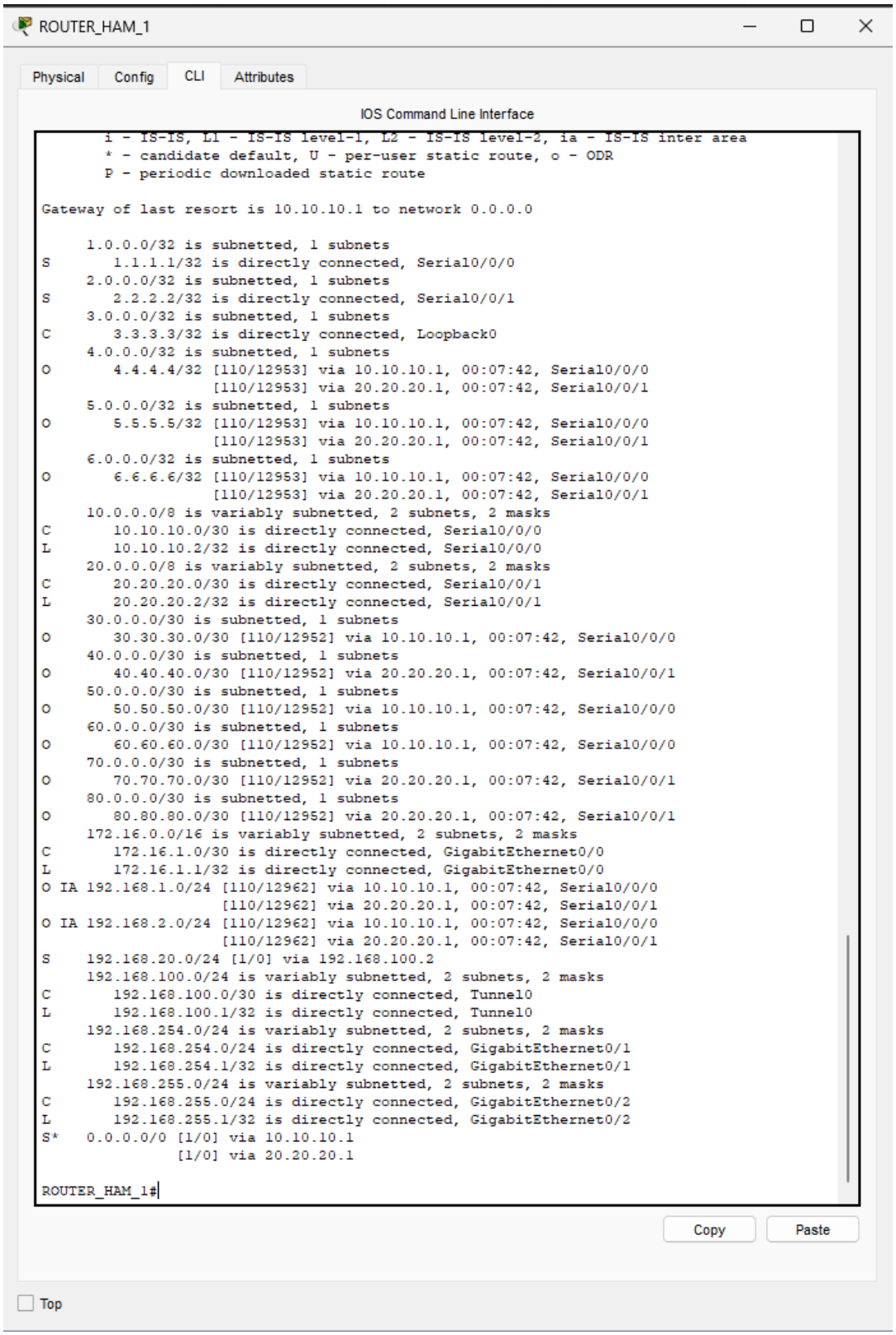
Physical Design Considerations

Physical devices are strategically located in the server room as pictured in the Packet Tracer file, the rooms must be equipped with proper cooling and UPS power backup and load balancing. Ethernet cables should be organized into patch panels for easy maintenance.

(Refer to the attached Packet Tracer file for details)

Screenshots ROUTER_HAM_1

Show ip route


ROUTER_HAM_1
Physical
Config
CLI
Attributes
IOS Command Line Interface
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route
Gateway of last resort is 10.10.10.1 to network 0.0.0.0
1.0.0.0/32 is subnetted, 1 subnets
S 1.1.1.1/32 is directly connected, Serial0/0/0
2.0.0.0/32 is subnetted, 1 subnets
S 2.2.2.2/32 is directly connected, Serial0/0/1
3.0.0.0/32 is subnetted, 1 subnets
C 3.3.3.3/32 is directly connected, Loopback0
4.0.0.0/32 is subnetted, 1 subnets
O 4.4.4.4/32 [110/12953] via 10.10.10.1, 00:07:42, Serial0/0/0
[110/12953] via 20.20.20.1, 00:07:42, Serial0/0/1
5.0.0.0/32 is subnetted, 1 subnets
O 5.5.5.5/32 [110/12953] via 10.10.10.1, 00:07:42, Serial0/0/0
[110/12953] via 20.20.20.1, 00:07:42, Serial0/0/1
6.0.0.0/32 is subnetted, 1 subnets
O 6.6.6.6/32 [110/12953] via 10.10.10.1, 00:07:42, Serial0/0/0
[110/12953] via 20.20.20.1, 00:07:42, Serial0/0/1
10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C 10.10.10.0/30 is directly connected, Serial0/0/0
L 10.10.10.2/32 is directly connected, Serial0/0/0
20.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C 20.20.20.0/30 is directly connected, Serial0/0/1
L 20.20.20.2/32 is directly connected, Serial0/0/1
30.0.0.0/30 is subnetted, 1 subnets
O 30.30.30.0/30 [110/12952] via 10.10.10.1, 00:07:42, Serial0/0/0
40.0.0.0/30 is subnetted, 1 subnets
O 40.40.40.0/30 [110/12952] via 20.20.20.1, 00:07:42, Serial0/0/1
50.0.0.0/30 is subnetted, 1 subnets
O 50.50.50.0/30 [110/12952] via 10.10.10.1, 00:07:42, Serial0/0/0
60.0.0.0/30 is subnetted, 1 subnets
O 60.60.60.0/30 [110/12952] via 10.10.10.1, 00:07:42, Serial0/0/0
70.0.0.0/30 is subnetted, 1 subnets
O 70.70.70.0/30 [110/12952] via 20.20.20.1, 00:07:42, Serial0/0/1
80.0.0.0/30 is subnetted, 1 subnets
O 80.80.80.0/30 [110/12952] via 20.20.20.1, 00:07:42, Serial0/0/1
172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C 172.16.1.0/30 is directly connected, GigabitEthernet0/0
L 172.16.1.1/32 is directly connected, GigabitEthernet0/0
O IA 192.168.1.0/24 [110/12962] via 10.10.10.1, 00:07:42, Serial0/0/0
[110/12962] via 20.20.20.1, 00:07:42, Serial0/0/1
O IA 192.168.2.0/24 [110/12962] via 10.10.10.1, 00:07:42, Serial0/0/0
[110/12962] via 20.20.20.1, 00:07:42, Serial0/0/1
S 192.168.20.0/24 [1/0] via 192.168.100.2
192.168.100.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.100.0/30 is directly connected, Tunnel0
L 192.168.100.1/32 is directly connected, Tunnel0
192.168.254.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.254.0/24 is directly connected, GigabitEthernet0/1
L 192.168.254.1/32 is directly connected, GigabitEthernet0/1
192.168.255.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.255.0/24 is directly connected, GigabitEthernet0/2
L 192.168.255.1/32 is directly connected, GigabitEthernet0/2
S* 0.0.0.0/0 [1/0] via 10.10.10.1
[1/0] via 20.20.20.1
ROUTER_HAM_1#
Copy
Paste
Top

Show ip ospf neighbors

```
Neighbor ID     Pri   State           Dead Time   Address         Interface
1.1.1.1           0   FULL/  -        00:00:37    10.10.10.1      Serial0/0/0
2.2.2.2           0   FULL/  -        00:00:30    20.20.20.1      Serial0/0/1
4.4.4.4          90   FULL/BDR        00:00:16    172.16.1.2      GigabitEthernet0/0
ROUTER_HAM_1#
```

Show vlan brief

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
ROUTER_HAM_1#
```

show ip nat statistics

```
ROUTER_HAM_1#show ip nat statistics
Total translations: 0 (0 static, 0 dynamic, 0 extended)
Outside Interfaces: Serial0/0/0 , Serial0/0/1
Inside Interfaces: GigabitEthernet0/1 , GigabitEthernet0/2
Hits: 0  Misses: 26
Expired translations: 0
Dynamic mappings:
ROUTER_HAM_1#
```

show lldp neighbors

```
ROUTER_HAM_1#show lldp neighbors
Capability codes:
    (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
    (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other
Device ID           Local Intf     Hold-time  Capability      Port ID
ROUTER_HAM_2        Gig0/0         120        R               Gig0/0
SWITCH_HAM_CORE_2   Gig0/2         120        R               Gig1/0/10
SWITCH_HAM_CORE_1   Gig0/1         120        R               Gig1/0/9

Total entries displayed: 3
ROUTER_HAM_1#
```

show ntp associations

```
ROUTER_HAM_1#show ntp associations

address         ref clock       st   when     poll    reach  delay          offset
disp
 ~192.168.30.252.INIT.          16   -        64      0      0.00           0.00
0.49
 * sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
ROUTER_HAM_1#
```

Screenshots CORE_HAM_1

Show ip route

```
SWITCH_HAM_CORE_1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 192.168.254.1 to network 0.0.0.0

C    192.168.10.0/24 is directly connected, Vlan10
C    192.168.20.0/24 is directly connected, Vlan20
C    192.168.30.0/24 is directly connected, Vlan30
C    192.168.254.0/24 is directly connected, Vlan2
S*   0.0.0.0/0 [1/0] via 192.168.254.1
               [1/0] via 192.168.254.2

SWITCH HAM CORE 1#
```

Show ip vlan brief

```
SWITCH_HAM_CORE_1#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active
2    OUTSIDE                          active    Gig1/0/9, Gig1/0/10
10   STAFF                            active
20   CORPORATE                        active
30   IT                               active
99   NATIVE                           active
199  ADMIN_DOWN                       active    Gig1/0/11, Gig1/0/12, Gig1/0/13,
Gig1/0/14
                                                Gig1/0/15, Gig1/0/16, Gig1/0/17,
Gig1/0/18
                                                Gig1/0/19, Gig1/0/20, Gig1/0/21,
Gig1/0/22
                                                Gig1/0/23, Gig1/0/24, Gig1/1/1, Gig1/1/2
                                                Gig1/1/3, Gig1/1/4
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
SWITCH HAM CORE 1#
```

Show lldp neighbors

```
SWITCH_HAM_CORE_1#show lldp neighbors
Capability codes:
    (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
    (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other
Device ID           Local Intf     Hold-time  Capability      Port ID
SWITCH_HAM_CORE_2   Po1            120        R               Gig1/0/2
ROUTER_HAM_2        Gig1/0/10      120        R               Gig0/2
SWITCH_HAM_CORE_2   Po1            120        R               Gig1/0/1
SWITCH_HAM_CORE_2   Po1            120        R               Gig1/0/4
SWITCH_HAM_DISTRIBUTION_2Gig1/0/8       120        R               Gig1/0/8
SWITCH_HAM_CORE_2   Po1            120        R               Gig1/0/3
SWITCH_HAM_DISTRIBUTION_1Po2            120        R               Gig1/0/6
SWITCH_HAM_DISTRIBUTION_1Po2            120        R               Gig1/0/7
ROUTER_HAM_1        Gig1/0/9       120        R               Gig0/1
SWITCH_HAM_CORE_2   Po1            120        R               Gig1/0/5

Total entries displayed: 10
SWITCH_HAM_CORE_1#
```

Show ntp associations

```
SWITCH_HAM_CORE_1#show ntp associations

address         ref clock       st   when     poll    reach  delay          offset
disp
 ~192.168.30.252.INIT.          16   -        64      0      0.00           0.00
0.49
 * sys.peer  # selected  + candidate  - outlyer  x falseticker  ~ configured
```

Problems and Issues

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

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	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.

	Switch(config)# end	
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:	The **traceroute** command lets you to see the path a packet takes in order to

	Switch# traceroute 192.168.1.4	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.