DEPI FINAL PROJECT

Building and Securing a Small Network project

TEEM MEMBERS:

Eyad Osama Kamal
Ahmed Mohammed Ali
Shehab Yasser
Zeyad Mahmoud Salah
Mohammed Ibrahim Gomaa

UNDER SUPERVISION:

ENG.HASSNAA ELWAN

KEY FEATURES

1. **Network Design and Configuration**

   Eyad | Mohammed | Shehab

2. **VLANs and Inter-VLAN Routing**

   Mohammed | Eyad | Shehab

3. **Network Security Implementation**

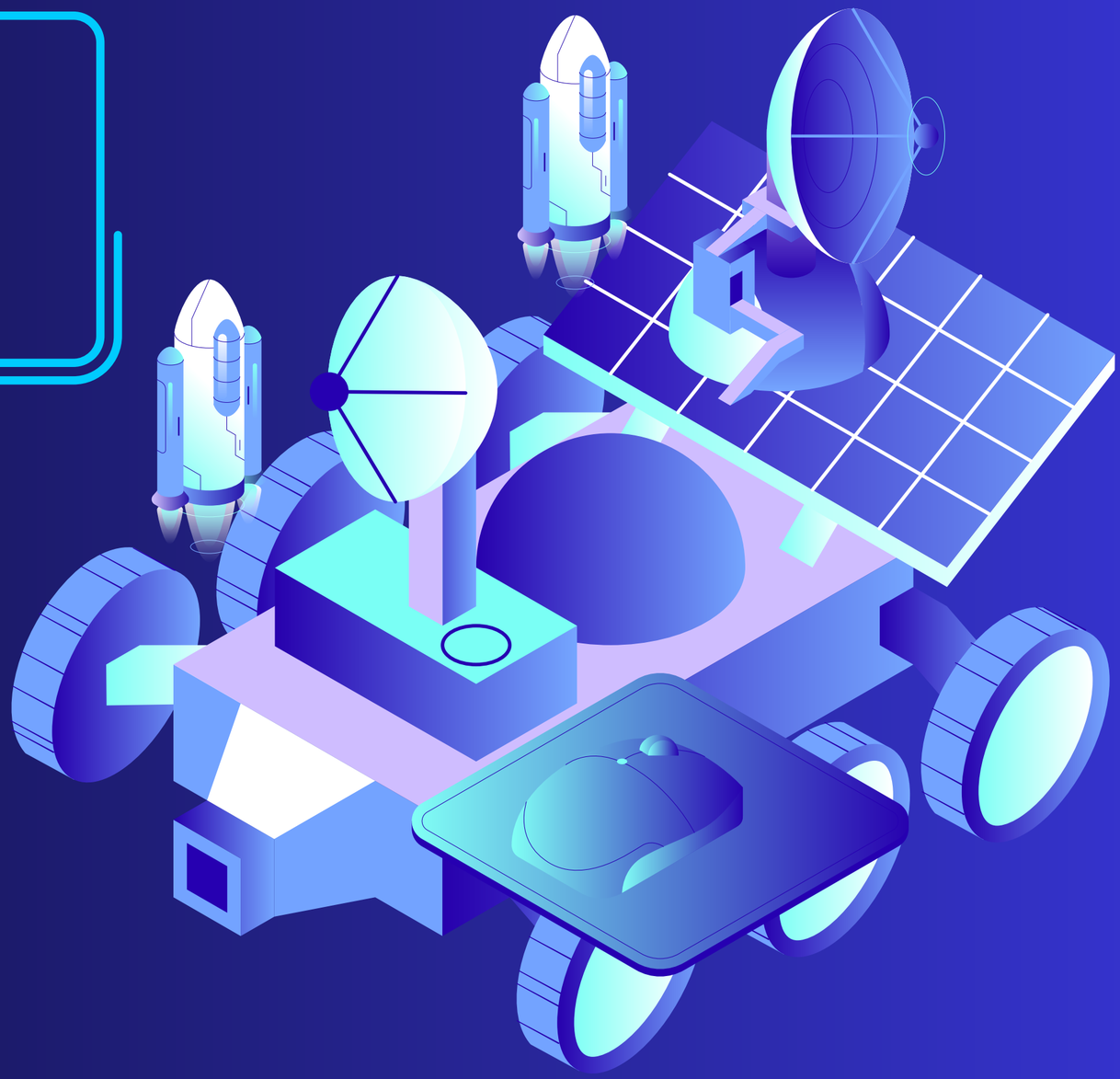
   Ahmed | Zeyad

4. **Final Testing and Reporting**

   Shehab | Zeyad | Mohammed | Eyad | Ahmed

1-NETWORK DESIGN AND CONFIGURATION

For a small network project, configuring switches and routers is fundamental to ensure proper communication between devices and secure network operation.



NETWORK SUBNETTING

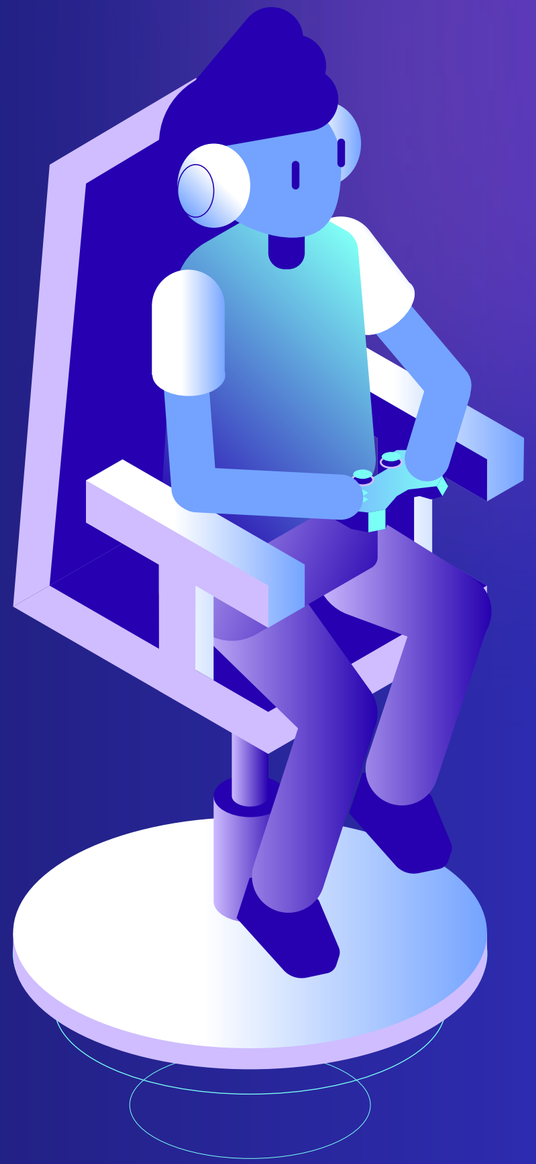
- Base network: 192.168.10.0
- No. of subnets= 3
- No. of subnets= 2^n
- 2^n=3==→ n=2
- Class C= 255.255.255.0→11111111. 11111111. 11111111.00000000
- After borrowing 2 bits
- New binary= 11111111. 11111111. 11111111.1100000
- New subnet mask: 255.255.255.192
- Block size= 64

NETWORK SUBNETTING

- 1st Subnet:
- Network ID: 192.168.10.0
- Broadcast ID: 192.168.10.63
- Host range: 192.168.10.1-192.168.10.62

- 2nd subnet:
- Network ID: 192.168.10.64
- Broadcast ID: 192.168.10.127
- Host range: 192.168.10.65-192.168.10.126

- 3rd subnets:
- Network ID: 192.168.10.128
- Broadcast ID:192.168.10.191
- Host range: 192.168.10.129/192.168.10.62



BASIC CONFIGURATION TO A SWITCH

We started with the Basic configuration of the switch. We followed the following step:

1. Assign a Hostname:

we used the following commands:
Switch> enable (To enter privileged exec mode)
Switch# configure terminal (To enter global configuration mode)
Switch(config)# hostname S1 (Assign a hostname to the switch)

2. Secure Access (Passwords):

Set up passwords for user access and privilege levels. After that, we encrypted the passwords

S1(config)# enable secret class
S1 (config)# line vty 0 15
S1 (config-line)# password cisco
S1 (config-line)# login
S1 (config-line)# exit
S1 (config)# service password-encryption

3. Set Up a Default Gateway:

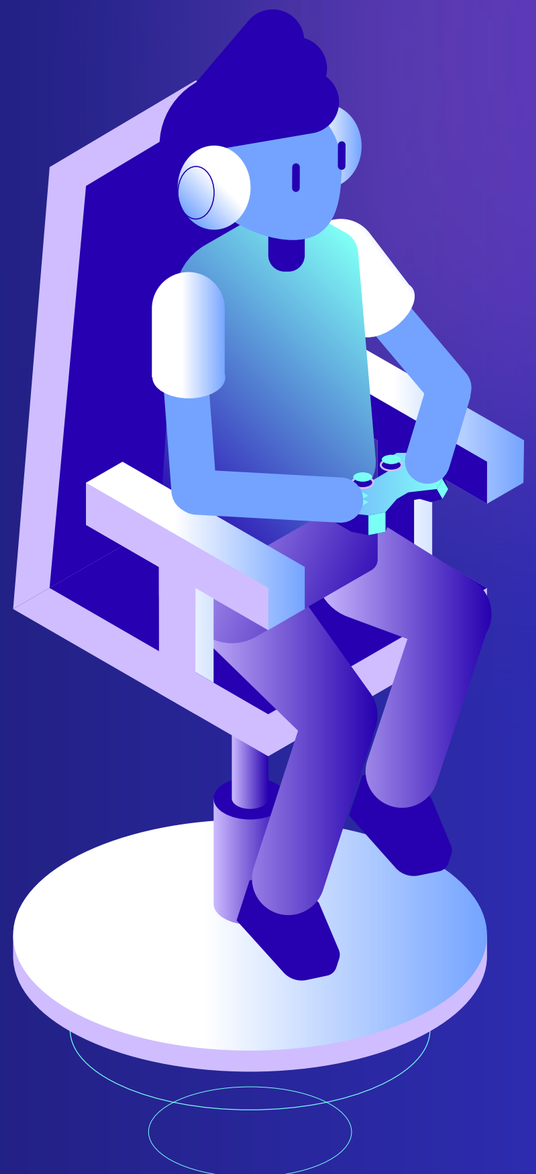
The switch needs a default gateway to communicate outside the local network.
S1(config)# ip default-gateway 192.168.0.1

4. Create VLANs:

VLAN segmentation is required for traffic separation. We divided the network into 3 VLANs, VLAN 30 for admins, VLAN 20 for sales, and VLAN 10 for guests.
S1(config)# vlan 10
S1(config-vlan)# name Guest
S1(config)# vlan 20
S1(config-vlan)# name Sales
S1(config)# vlan 30
S1(config-vlan)# name Admin

5. Assign Ports to VLANs and Configure them to operate in access mode and assign them to VLAN:

```
S1(config)# interface range fastethernet 0/1 - 3
S1(config-if-range)# switchport mode access
S1(config-if-range)# switchport access vlan 30
S1(config-if-range)# exit
S1(config)# interface range fastethernet 0/5 - 8
S1(config-if-range)# switchport mode access
S1(config-if-range)# switchport access vlan 20
S1(config-if-range)# exit
S1(config)# interface range fastethernet 0/9 - 12
S1(config-if-range)# switchport mode access
S1(config-if-range)# switchport access vlan 10
S1(config-if-range)# exit
```



6. Save Configuration from RAM to NVRAM:

```
Switch# copy running-config startup-config
```

BASIC CONFIGURATION OF A ROUTER

Then we did the basic configuration for the router.

1. Assign a Hostname:
Router> enable
Router# configure terminal
Router(config)# hostname R1

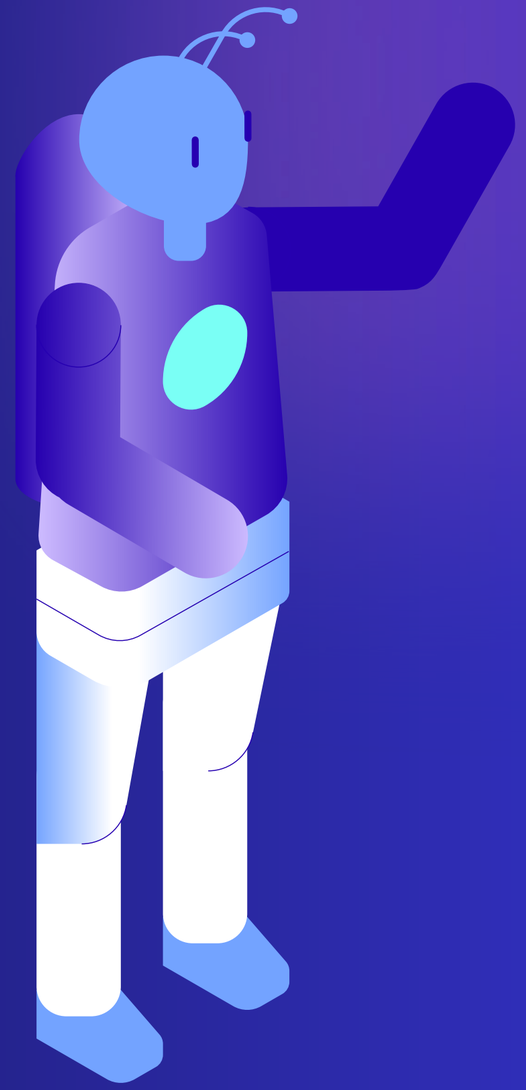
2. Configure Interfaces:
Assign IP addresses to interfaces connected to the LAN. We divided 3 virtual interfaces as sub interfaces in one physical interface. This is the inter-vlan method using router-on-stick.

3. Secure the Router (Basic Security):
Passwords for User and Privileged Access. After that, we encrypted the passwords.

```
R1 (config)# enable secret class
R1 (config)# line vty 0 15
R1 (config-line)# password cisco
R1(config-line)# login
R1(config-line)# exit
R1(config)# service password-encryption
```

4. Save Configuration from RAM to NVRAM:

```
R1# copy running-config startup-config
```



VERIFICATION AND TESTING

Verification and testing
Then we did verification and testing for the switch and router.

Conclusion

The basic switch and router configurations outlined above establish a functional and secure small network. By following these steps, a network administrator can ensure proper device communication, network segmentation, and secure access for both internal and external traffic.

2-VLANS AND INTER-VLAN ROUTING

Overview

This report details the troubleshooting steps taken during the implementation of VLANs and Inter-VLAN routing in a small network project. The network includes three VLANs configured using Cisco devices, and Inter-VLAN routing is implemented using a (router-on-a-stick) configuration.

The primary issues encountered included VLAN misconfiguration, routing failures between VLANs, and incorrect trunking between switches and routers. The following sections describe the problems faced, their causes, and the steps taken to resolve each issue.

NETWORK SETUP

VLAN 10: IP range 192.168.10.0/26, Subnet Mask 255.255.255.192, Interface: Fastethernet 0/0.10

VLAN 20: IP range 192.168.10.64/26, Subnet Mask 255.255.255.192, Interface: Fastethernet 0/0.20

VLAN 30: IP range 192.168.10.128/26, Subnet Mask 255.255.255.192, Interface: Fastethernet 0/0.30

ISSUES ENCOUNTERED AND TROUBLESHOOTING STEPS

Issue 1: Hosts in Different VLANs Cannot Communicate (Inter-VLAN Routing Failure)

Symptoms: Devices in different VLANs were unable to communicate with each other. For example, hosts in VLAN 10 could not ping hosts in VLAN 20.

Cause: The issue was due to an incorrect configuration of the subinterfaces on the router responsible for Inter-VLAN routing. The subinterfaces were missing the correct VLAN tags (dot1Q encapsulation).

Troubleshooting Steps:

1. Checked the configuration of the subinterfaces on the router using the command:

    Router# show running-config interface Fastethernet 0/0

2. Found that the `encapsulation dot1Q` command was missing on some subinterfaces.

3. Reconfigured the subinterfaces to include the correct VLAN encapsulation:

    Router(config)# interface Fastethernet 0/0.10
    Router(config-subif)# encapsulation dot1Q 10
    Router(config-subif)# ip address 192.168.10.1 255.255.255.192

```
Router(config)# interface Fastethernet 0/0.20
   Router(config-subif)# encapsulation dot1Q 20
   Router(config-subif)# ip address 192.168.10.65 255.255.255.192

Router(config)# interface Fastethernet 0/0.30
   Router(config-subif)# encapsulation dot1Q 30
   Router(config-subif)# ip address 192.168.10.129 255.255.255.192
```

Result: After correcting the configuration, communication between VLANs was successful, and devices in VLAN 10 could communicate with devices in VLAN 20 and VLAN 30.

HOSTS IN THE SAME VLAN CANNOT COMMUNICATE

Symptoms: Hosts within the same VLAN were unable to communicate with each other. For example, two hosts in VLAN 20 could not ping each other.

Cause: The switch ports were not correctly assigned to the proper VLANs.

Troubleshooting Steps:

1. Verified the VLAN configuration on the switch using1
   Switch# show vlan brief

2. Discovered that some interfaces (e.g., `FastEthernet 0/1` and `FastEthernet 0/2`) were not assigned to the correct VLAN (VLAN 20)

3. Corrected the VLAN assignment using the following commands:

```
Switch(config)# interface range FastEthernet 0/5 - 8
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 20
```

Result: Once the switch ports were assigned to the correct VLAN, the hosts within VLAN 20 were able to communicate with each other without issues.

VLAN TRUNKING ISSUES BETWEEN SWITCH AND ROUTER

Symptoms: The router was not receiving traffic from certain VLANs, and devices in these VLANs could not communicate with the router.

Cause: The trunk link between the switch and the router was not configured correctly. The `trunk` configuration was missing on the switch port connecting to the router.

Troubleshooting Steps:

1. Verified the trunking configuration on the switch with the following command:

Switch# show interfaces trunk

2. Found that the interface connecting to the router was not in trunking mode.
3. Configured the trunk link on the switch using:

```
Switch(config)# interface FastEthernet 0/4
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan 10,20,30
```

Result: After configuring the trunk port, traffic from all VLANs started to flow correctly to the router, and Inter-VLAN communication was restored.

Lessons Learned

1. Correct VLAN tagging on subinterfaces: It's essential to ensure that each subinterface on the router has the correct encapsulation for the VLAN it serves. Missing this can prevent inter-VLAN routing.

2.Proper VLAN assignment on switches: Ports must be correctly assigned to the appropriate VLAN. Mismatches can lead to hosts within the same VLAN not being able to communicate.

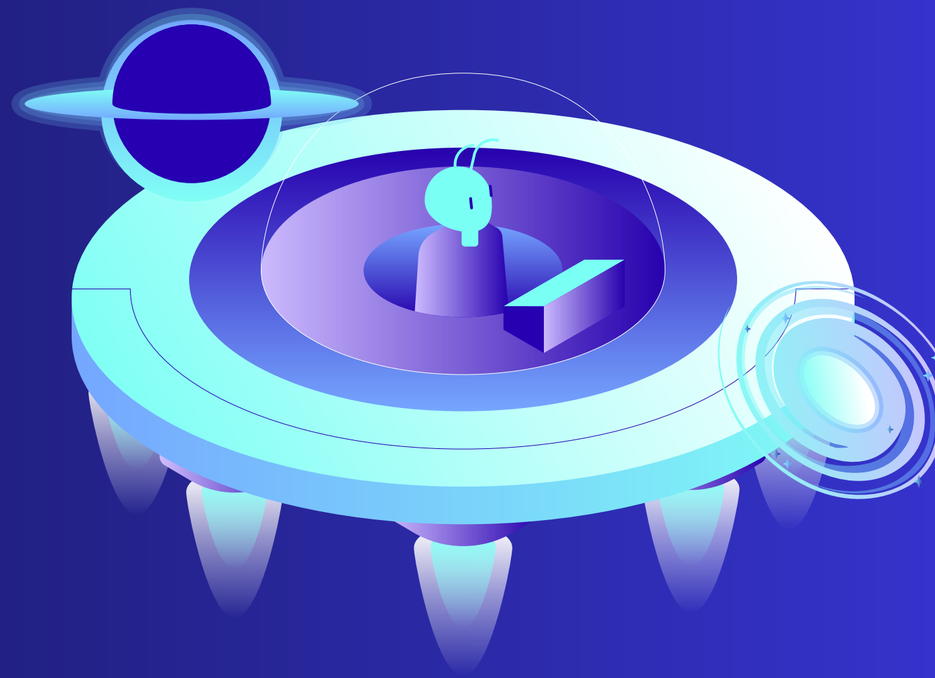
3. Trunk configuration: Trunk ports between the switch and router must be properly configured to carry traffic for all VLANs. Without trunking, VLAN traffic cannot be passed to the router for Inter-VLAN routing.

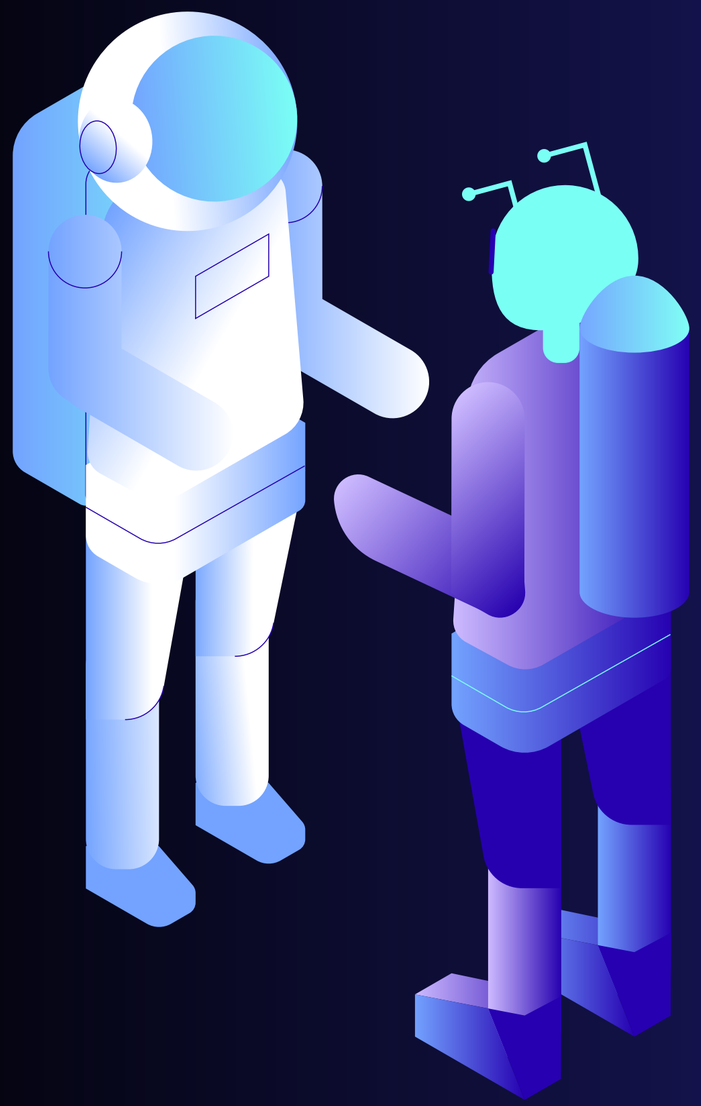
Conclusion

Through systematic troubleshooting of the VLAN and Inter-VLAN routing issues, we were able to identify and resolve the main problems: incorrect VLAN encapsulation on the router's subinterfaces, improper VLAN assignment on switch ports, and missing trunk configuration. After these fixes, the VLANs and Inter-VLAN routing functioned as expected.

3-NETWORK SECURITY IMPLEMENTATION

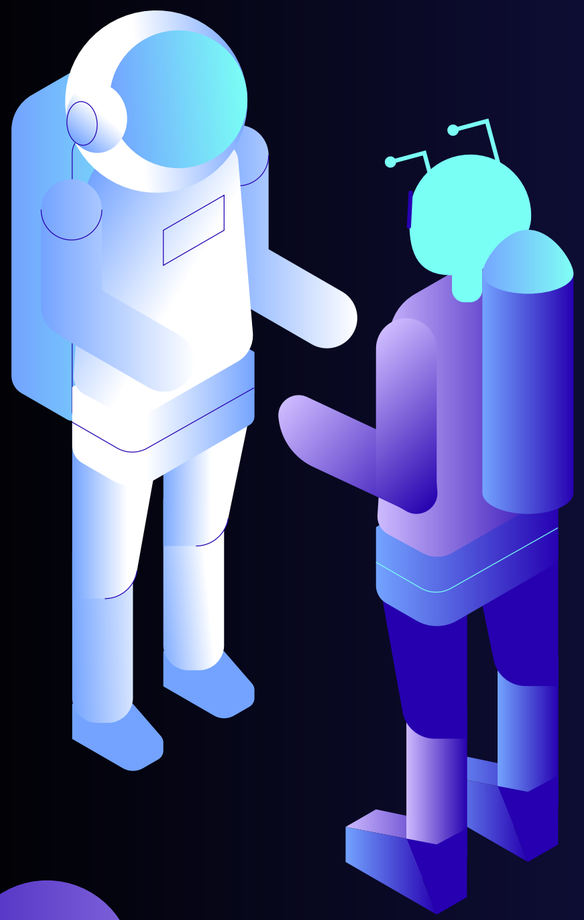
For a small network project, configuring switches and routers is fundamental to ensure proper communication between devices and secure network operation.





CONFIGURATION OF A ROUTER TO CREATE ACL

Are you ready to join us on this journey? Whether you're a developer, creator, investor, or simply curious about the potential of the Metaverse, there's a place for you in shaping the future of digital interaction.



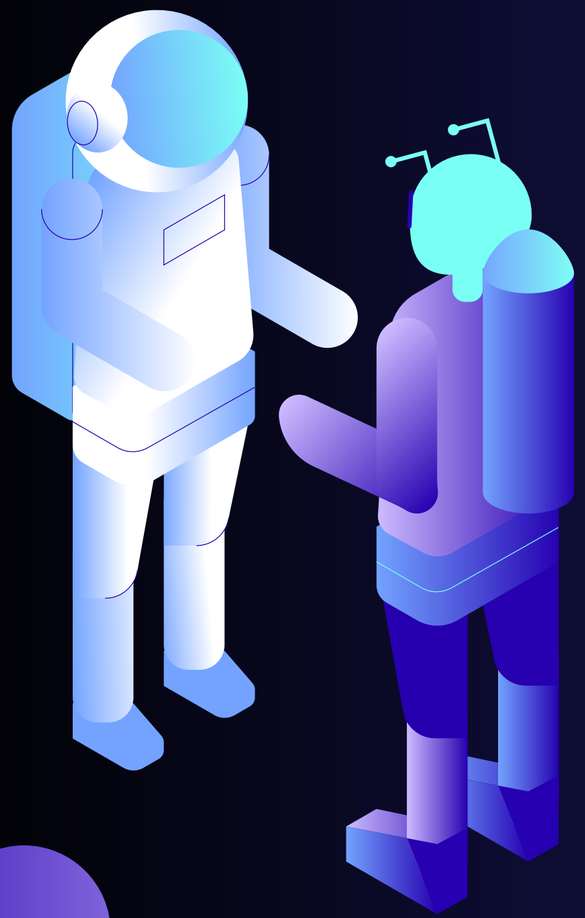
Then we did the configuration for the router.

1. Access the Configuration mode:
R1> enable
R1# configure terminal
2.create an ACL For a standard ACL:
R1 (config)# access-list 1 deny any

3. Apply the ACL to an Interface
After creating the ACL, you need to apply it to a specific interface:
R1 (config)# interface f0/0.10
R1 (config-subif)# ip access-group 1 in
R1 (config)# interface f0/0.20
R1 (config-subif)# ip access-group 1 in

in: Indicates that the ACL will be applied to incoming traffic.

"Any device from Interface f0/0.10 or f0/0.20 is not allowed to connect to the router. Only f0/0.30 devices are allowed to access"



4.create an extended ACL
R1(config)# access-list 100 permit tcp any any eq 80
R1(config)# access-list 100 permit tcp any any eq 443
R1(config)# access-list 100 deny ip any any

5. Apply the ACL to an Interface:
R1 (config)# interface f0/0.30
R1 (config-subif)# ip access-group 100 in

“The interface that is allowed to access the router can access through port 80, 443 only”

6. Save Configuration from RAM to NVRAM:
R1# copy running-config startup-config

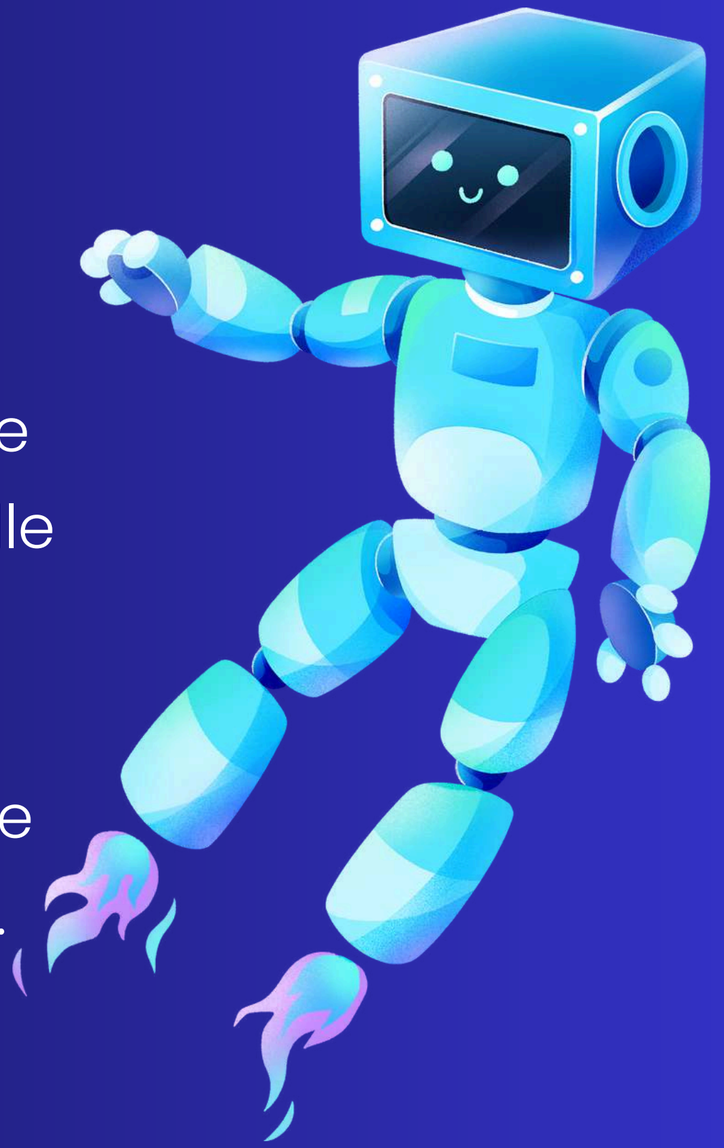
VERIFICATION AND TESTING

Then we did verification and testing for the router.
R1# show access-lists

Conclusion

Access Control Lists are essential tools for managing network security and controlling data flow in routers and switches. By defining who can access specific resources and what actions they can perform, ACLs help protect sensitive information and ensure that only authorized users can interact with network resources.

ROUTER-ON-STICK



Introduction

Router-on-a-Stick is a network configuration technique that enables a single physical router interface to handle multiple VLANs (Virtual Local Area Networks) using sub interfaces. This method is commonly used in network environments to allow inter-VLAN communication while minimizing the number of physical interfaces required.

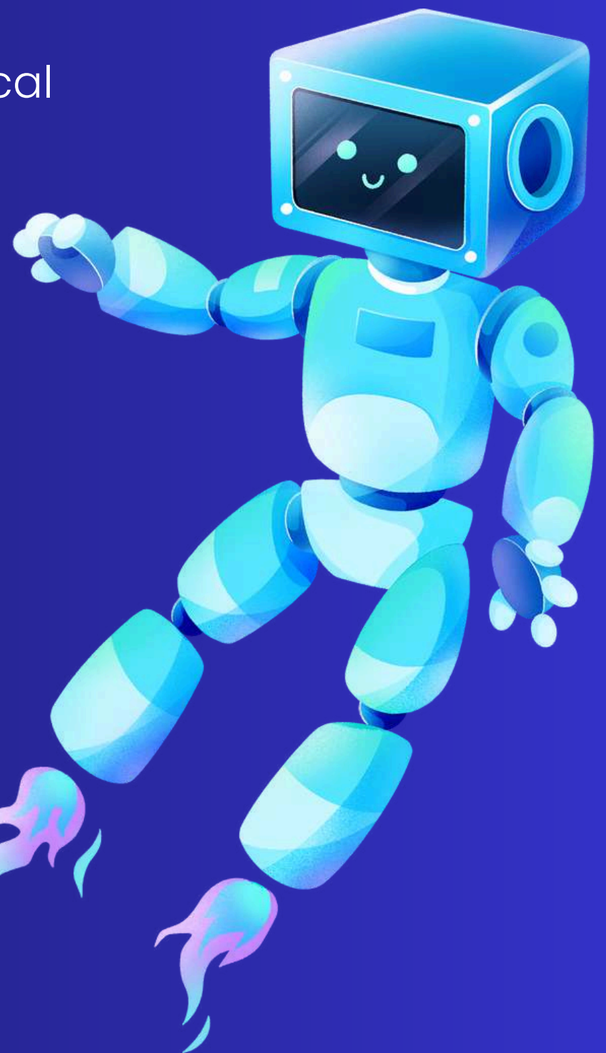
Purpose of Router-on-a-Stick

- Efficient VLAN Management: Allows routing between VLANs using a single physical interface.
- Cost-effective: Reduces the need for multiple physical interfaces or separate routers.
- Centralized Routing: Provides a central point of control for managing VLAN communication.

Network Topology

In a typical Router-on-a-Stick setup, the following components are involved:

1. Router: Configured with sub interfaces for each VLAN.
2. Switch: Configured with multiple VLANs and connected to the router via a trunk port.
3. End Devices: PCs or other devices connected to the switch ports assigned to specific VLANs.



Configuration Details:

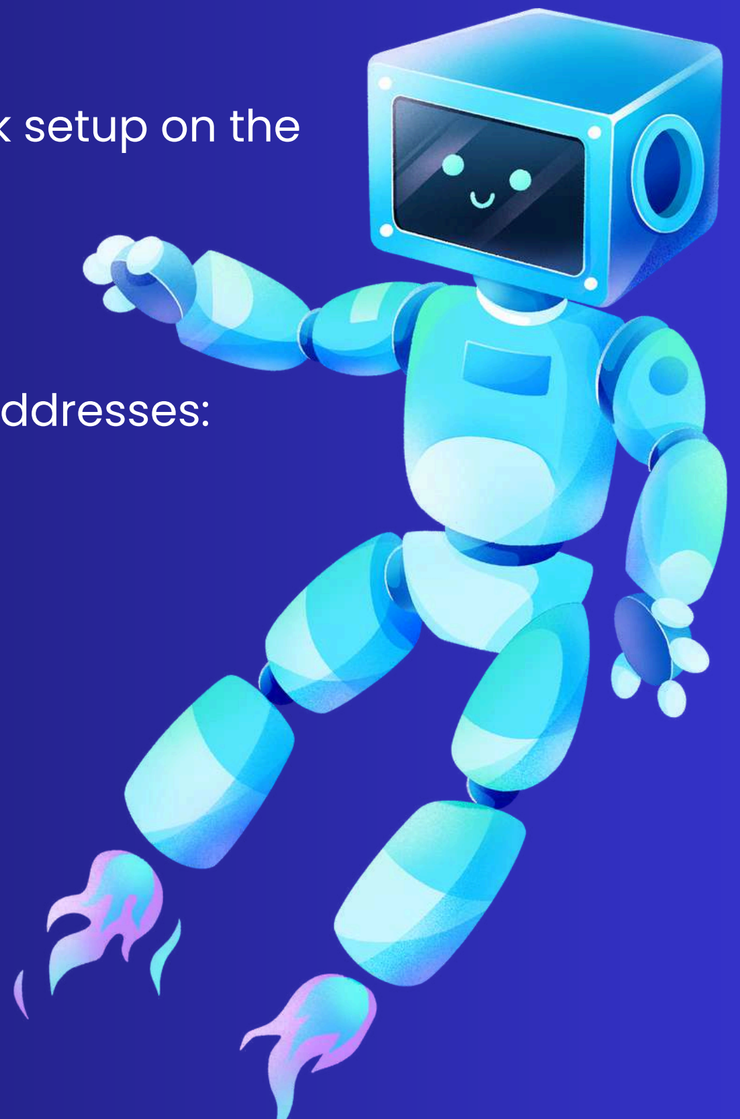
1.Router Configuration

2.The following configuration assumes a Cisco router with a Router-on-a-Stick setup on the interface FastEthernet0/0

Configure Sub interfaces for VLAN

1.Create sub interfaces for each VLAN with appropriate encapsulation and IP addresses:

```
Router(config-subif)# interface GigabitEthernet0/0.10
Router(config-subif)# encapsulation dot1Q 10
Router(config-subif)# ip address 192.168.10.1 255.255.255.192
Router(config-subif)# interface GigabitEthernet0/0.20
Router(config-subif)# encapsulation dot1Q 20
Router(config-subif)# ip address 192.168.10.65 255.255.255.192
Router(config-subif)# interface GigabitEthernet0/0.30
Router(config-subif)# encapsulation dot1Q 30
Router(config-subif)# ip address 192.168.10.129 255.255.255.192
```



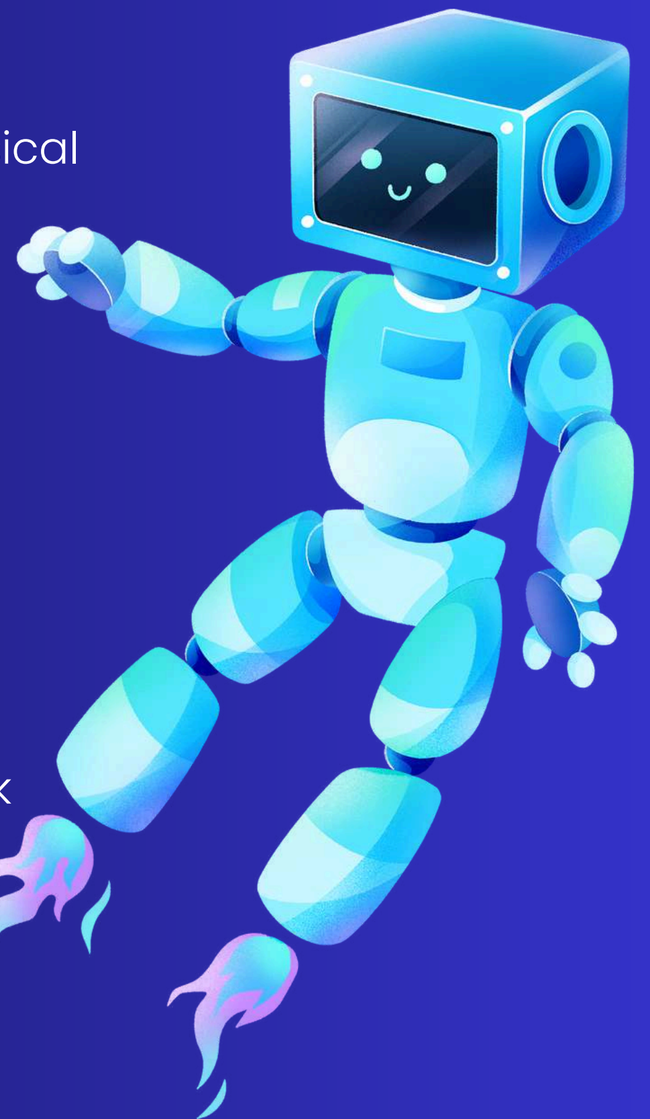
Purpose of Router-on-a-Stick

- Efficient VLAN Management: Allows routing between VLANs using a single physical interface.
- Cost-effective: Reduces the need for multiple physical interfaces or separate routers.
- Centralized Routing: Provides a central point of control for managing VLAN communication.

Network Topology

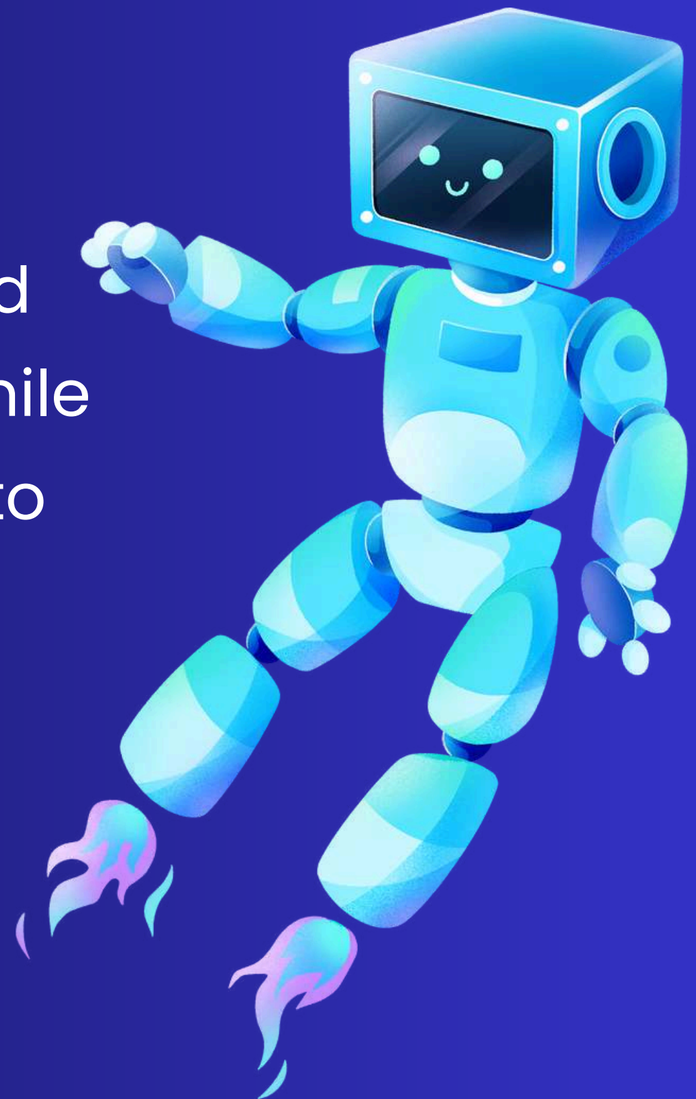
In a typical Router-on-a-Stick setup, the following components are involved:

1. Router: Configured with sub interfaces for each VLAN.
2. Switch: Configured with multiple VLANs and connected to the router via a trunk port.
3. End Devices: PCs or other devices connected to the switch ports assigned to specific VLANs.



Conclusion

The Router-on-a-Stick configuration is a powerful and efficient way to enable inter-VLAN communication while minimizing hardware costs. It is well-suited for small to medium-sized networks where VLAN segmentation is required.



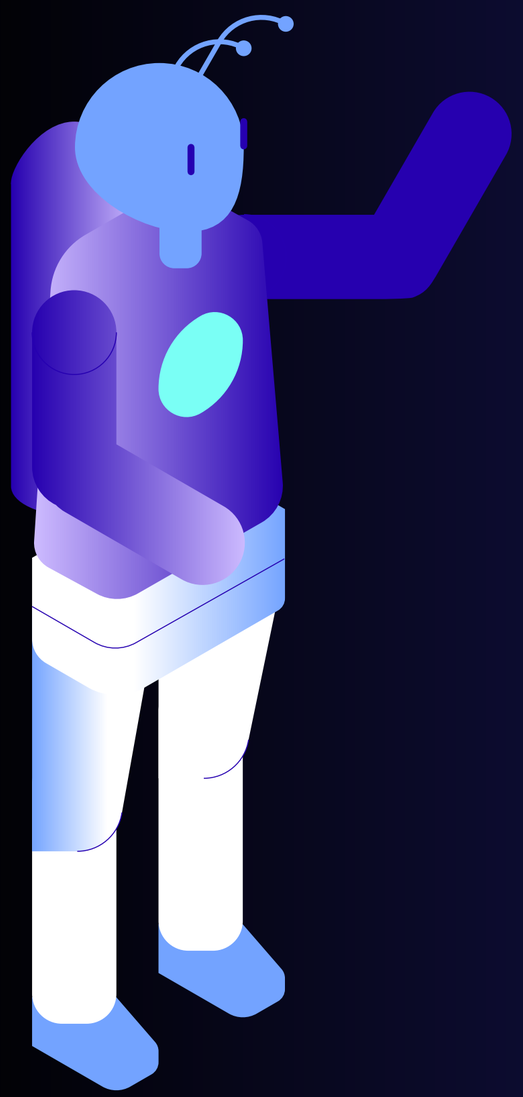
SEC

To configure network security for a basic topology where switches are connected to a router, and the router is connected to the Internet, you'll want to implement several key security measures. Here’s a list of configurations including port security, firewall rules, and other network security deliverables for both the switches and the router.

1. Switch Configuration (Port Security)

Basic Port Security:
Port security helps in controlling which devices can connect to switch ports. Here's an example of configuring port security for an interface on the switch.

```
Switch(config)# interface FastEthernet 0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 2   # Allow a max of 2 MAC addresses
Switch(config-if)# switchport port-security violation shutdown   # Shutdown the port if violation occurs
Switch(config-if)# switchport port-security mac-address sticky   # Learn MAC addresses dynamically and make them sticky
Switch(config-if)# end
```



Verify Port Security:

Switch# show port-security interface FastEthernet 0/1

Enable SSH for Secure Management:

```
Switch(config)# ip domain-name VLAN_S1.com
Switch(config)# crypto key generate rsa
Switch(config)# username admin privilege 15 secret cisco
Switch(config)# line vty 0 4
Switch(config-line)# transport input ssh
Switch(config-line)# login local
Switch(config-line)# exit
Switch(config)# ip ssh version 2
```

2. Router Configuration (Basic Security and Firewall)

Enable SSH on the Router (for Remote Management):

```
Router(config)# ip domain-name example.com
Router(config)# crypto key generate rsa
Router(config)# username admin privilege 15 secret cisco123
Router(config)# line vty 0 4
Router(config-line)# transport input ssh
Router(config-line)# login local
Router(config-line)# exit
Router(config)# ip ssh version 2
```

3. Deliverables for Packet Tracer Topology

1. IP Addressing: Ensure all devices (PCs, Switches, Router) have appropriate IP addresses for LAN and WAN connectivity.
2. Port Security: Configure port security on all switch interfaces that connect to end devices.
3. NAT: Implement NAT for LAN devices to access the Internet through the router.

4. Firewall Rules: Configure ACLs on the router to filter unwanted traffic and allow only necessary services (HTTP, HTTPS, SSH).

5. SSH Management: Set up SSH for secure management on both the switch and the router.

6. Verification: Ensure the configurations work by testing with `ping`, `traceroute`, and checking port security and NAT translations.

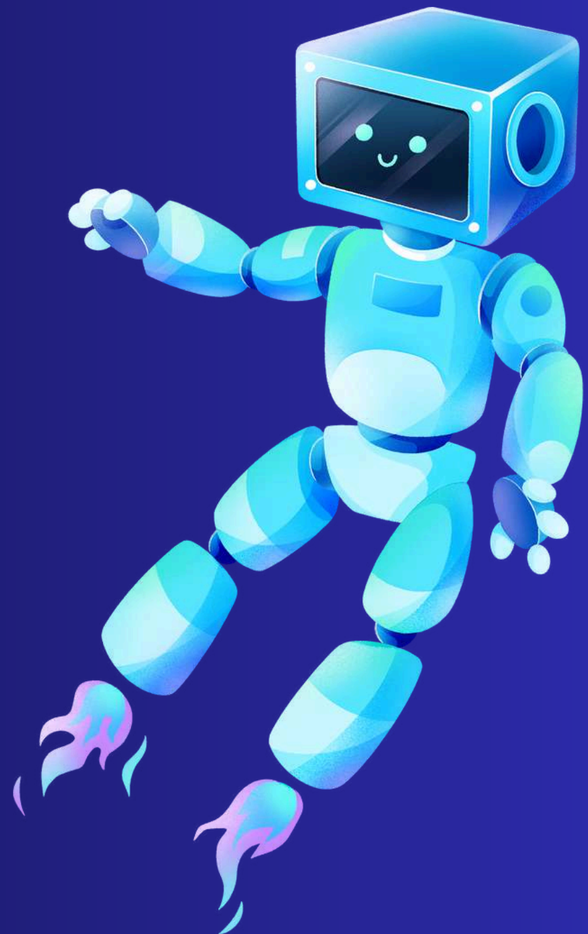
4. Verifications and Show Commands

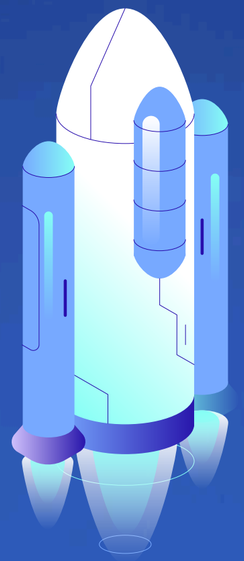
- Verify Port Security:
 Switch# show port-security

- Check NAT Translations:
 Router# show ip nat translations

- Check ACLs:
 Router# show access-lists

- Check interface status:
 Router# show ip interface brief





THANK YOU