ADVENTIST UNIVERSITY
OF CENTRAL AFRICA

NAME: Joseph MUTANGANA

STUDENT ID: 29061

COURSE NAME: Computer Networks

INSTRUCTOR NAME: Joshua IRADUKUNDA

ASSIGNMENT TITLE: Assignment#1

DATE: Oct-12-2025

STP/RSTP & PORT SECURITY CONFIGURATION LAB

IN CISCO PACKET TRACER

HANDS-ON LAB

Prepared by: Joseph MUTANGANA

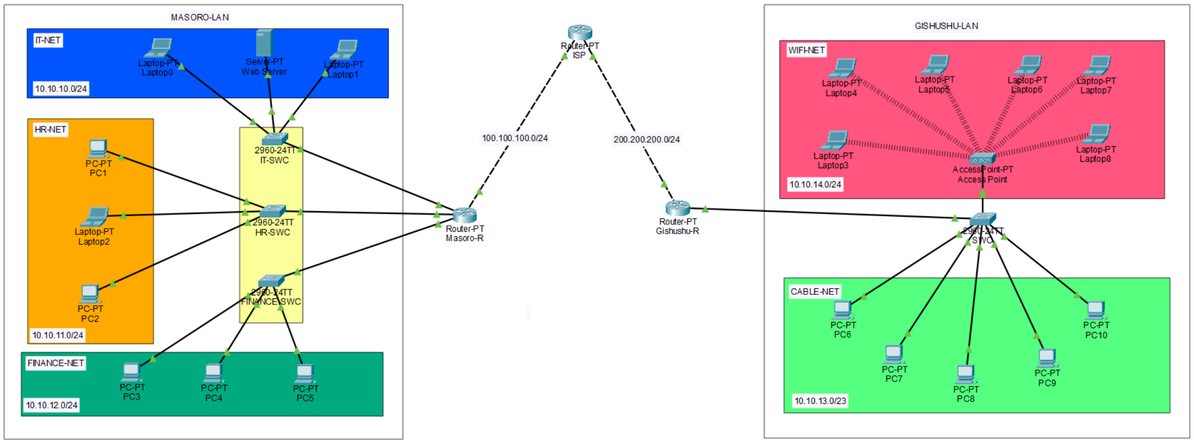
Table of Contents

1. Introduction

In modern networks, security and loop prevention are critical for maintaining reliable and safe communication between devices. Two essential concepts in network design are Port Security and Spanning Tree Protocol (STP) / Rapid Spanning Tree Protocol (RSTP).

Port Security is a feature on switches that controls access to a switch port based on MAC addresses. It prevents unauthorized devices from connecting to the network, reducing the risk of attacks and misconfigurations. Administrators can limit the number of devices per port, specify allowed MAC addresses, and define the action when a violation occurs (e.g., shutdown the port, restrict access, or just log it).

2. Network Topology Design



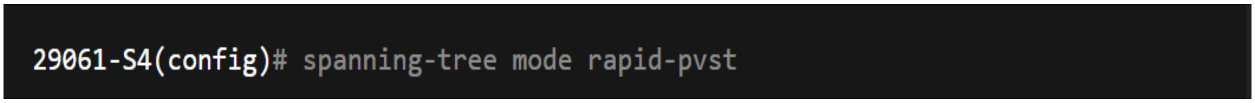
Routers: Used to make connect network and Acts as DHCP server

Switch: Connects multiple end devices

End Devices (Server, PCs/Laptops): Clients used in topology

3. STP/RSTP

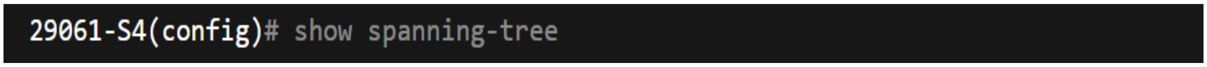
Use the following command



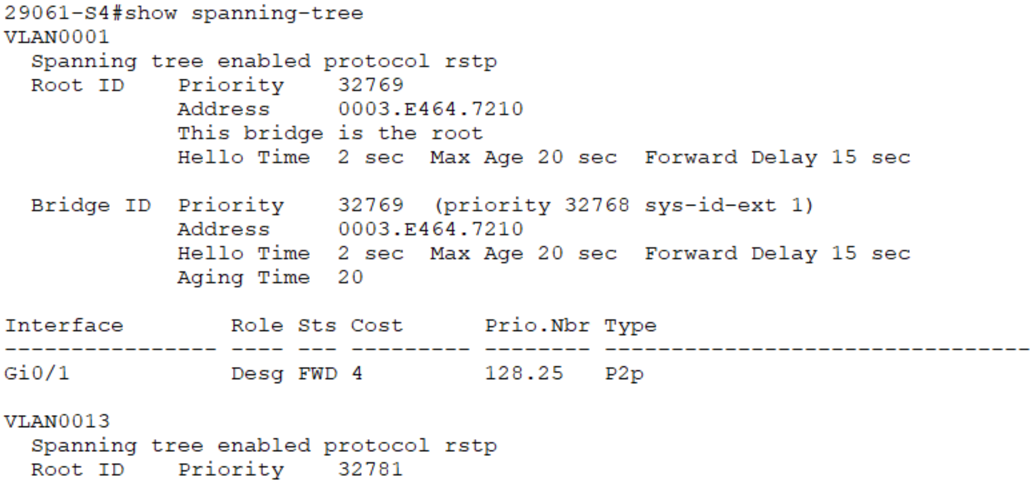
```
29061-S4(config)# spanning-tree mode rapid-pvst
```

Verification:

Use the following command:



```
29061-S4(config)# show spanning-tree
```



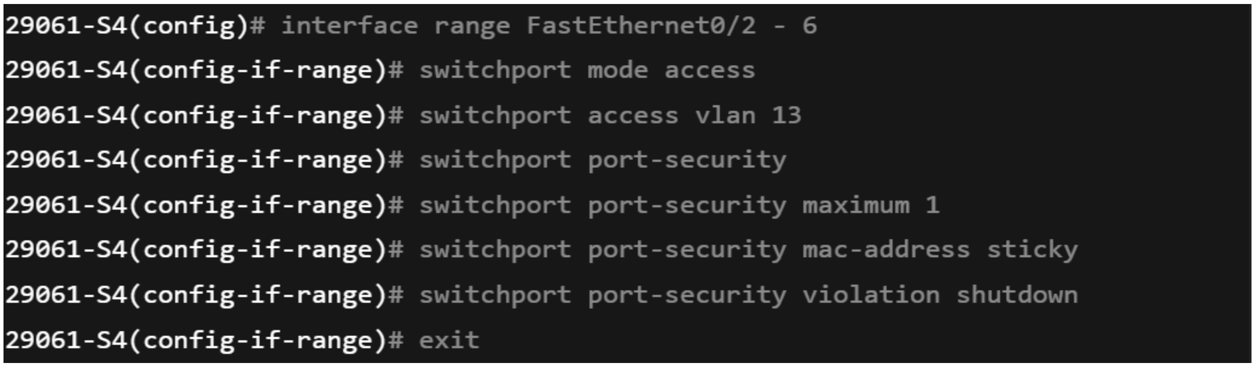
```
29061-S4#show spanning-tree
VLAN0001
  Spanning tree enabled protocol rstp
  Root ID    Priority    32769
             Address     0003.E464.7210
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     0003.E464.7210
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Gi0/1            Desg FWD 4         128.25   P2p

VLAN0013
  Spanning tree enabled protocol rstp
  Root ID    Priority    32781
```

3. Port Security Configuration



```
29061-S4(config)# interface range FastEthernet0/2 - 6
29061-S4(config-if-range)# switchport mode access
29061-S4(config-if-range)# switchport access vlan 13
29061-S4(config-if-range)# switchport port-security
29061-S4(config-if-range)# switchport port-security maximum 1
29061-S4(config-if-range)# switchport port-security mac-address sticky
29061-S4(config-if-range)# switchport port-security violation shutdown
29061-S4(config-if-range)# exit
```

Explanation of used commands

Interface range FastEthernet0/2 – 6: This allows to apply configure same configuration on more than one port.

switchport mode access: forces port to work as access port.

switchport access vlan 13: Assign the port to vlan 13.

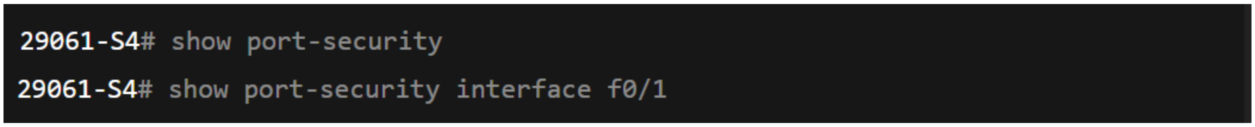
switchport port-security: Enables port security features on the port.

switchport port-security maximum 1: Limits each port to learn only one MAC addresss

switchport port-security violation shutdown: If violation occurs, the port goes into error.

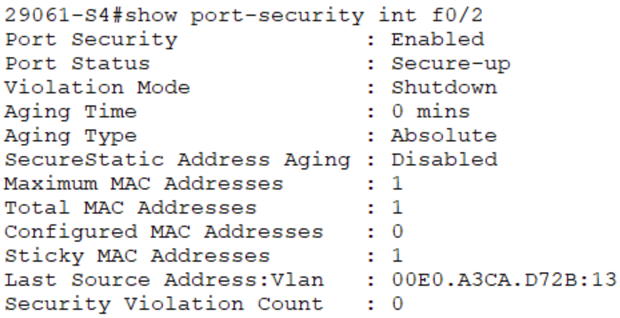
switchport port-security mac-address sticky: Allows switch to store first connected MAC address in the running configuration

Verification



```
29061-S4# show port-security
29061-S4# show port-security interface f0/1
```

show port-security interface f0/1: displays the security set to specific port



```
29061-S4#show port-security int f0/2
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : 00E0.A3CA.D72B:13
Security Violation Count   : 0
```

Summary:

1. Port Security:
    - Limits devices per switch port.
    - Prevents unauthorized access using MAC address filtering.
    - Offers violation actions: shutdown, restrict, or protect.
2. STP / RSTP:
    - Prevents loops in networks with redundant links.
    - STP has slower convergence; RSTP is faster.
    - Ensures continuous communication without broadcast storms.
3. Combined Benefit:
    - Protects the network from unauthorized devices.
    - Ensures reliable, loop-free network topology.
    - Enhances both security and network stability.

END.