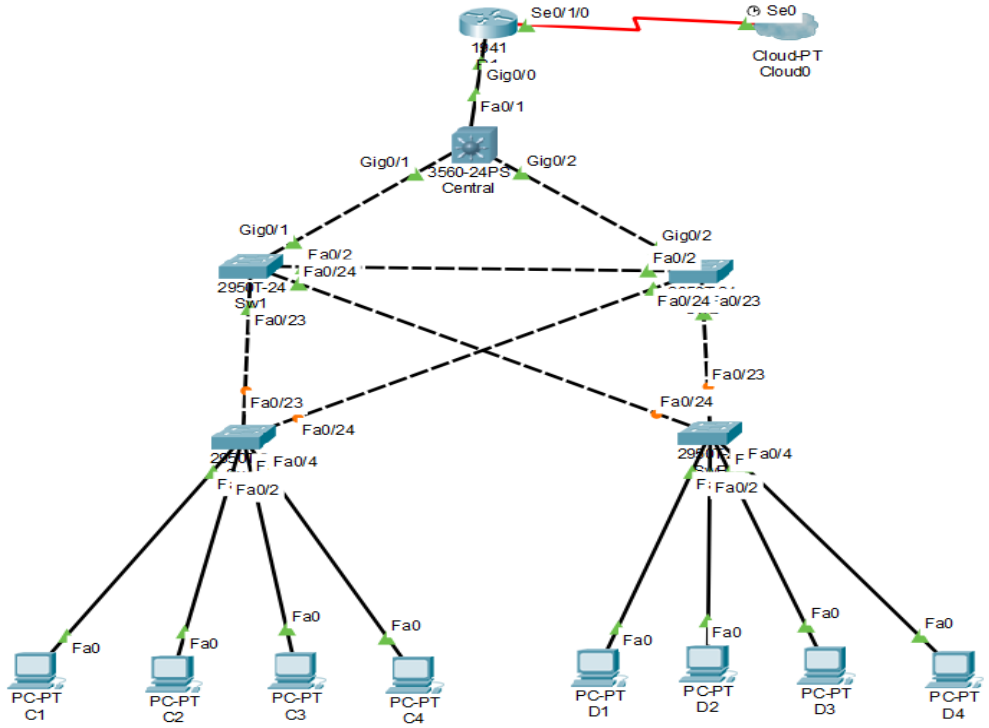
Security In Computing Practical's

Practical 7: Layer 2 Security

Topology:



Addressing Table:

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	gig0/0	192.168.1.1	255.255.255.0	N/A
	Se0/1/0	209.165.200.1	255.255.255.0	N/A
C1	NIC	10.1.1.10	255.255.255.0	10.1.1.1
C2	NIC	10.1.1.11	255.255.255.0	10.1.1.1
C3	NIC	10.1.1.12	255.255.255.0	10.1.1.1
C4	NIC	10.1.1.13	255.255.255.0	10.1.1.1
D1	NIC	10.1.1.114	255.255.255.0	10.1.1.1
D2	NIC	10.1.1.15	255.255.255.0	10.1.1.1
D3	NIC	10.1.1.16	255.255.255.0	10.1.1.1
D4	NIC	10.1.1.17	255.255.255.0	10.1.1.1

Objectives:

- Assign the Central switch as the root bridge.
- Secure spanning-tree parameters to prevent STP manipulation attacks.
- Enable port security to prevent CAM table overflow attacks.

Security In Computing Practical's

Part 1: Configure Switch / Router

Step 1: Configure secret

Execute command on all switches and router

R1/SW(config) # enable secret enpa55

Step 2: Configure console password

Execute command on all switches and router

R1/SW(config)# line console 0

R1/SW(config-line)# password conpa55

R1/SW(config-line)# login

Step 3: Configure SSH login

Execute command on all switches and router

R1/SW(config)# ip domain-name ccnasecurity.com

R1/SW(config)# username admin secret adminpa55

R1/SW(config)# line vty 0 4

R1/SW(config-line)# login local

R1/SW(config-line)# crypto key generate rsa

How many bits in the modulus [512]: 1024

Part 2: Configure Root Bridge

Step 1: Determine the current root bridge.

Central# show spanning-tree

SW1# show spanning-tree

Step 2: Assign Central as the primary root bridge.

Central(config)# spanning-tree vlan 1 root primary

Central# show spanning-tree

Step 3: Assign SW-1 as a secondary root bridge.

SW1(config)# spanning-tree vlan 1 root secondary

SW1# show spanning-tree

Part 3: Protect Against STP Attacks

Step 1: Enable PortFast on all access ports.

SWA/B(config)# int range fa0/1 - 4

SWA/B(config-if-range)# spanning-tree portfast

Step 2: Enable BPDU guard on all access ports.

SWA/B(config)# int range fa0/1 - 4

SWA/B(config-if-range)# spanning-tree bpduguard enable

Step 3: Enable root guard.

SW-1/2(config)# int range fa0/23 - 24

SW-1/2(config-if-range)# spanning-tree guard root

Part 4: Configure Port Security and Disable Unused Ports

Step 1: Configure basic port security on all ports connected to host devices.

SW-A/B(config)# int range fa0/1 - 22

SW-A/B(config-if-range)# switchport mode access

SW-A/B(config-if-range)# switchport port-security

SW-A/B(config-if-range)# switchport port-security maximum 2

SW-A/B(config-if-range)# switchport port-security violation shutdown

SW-A/B(config-if-range)# switchport port-security mac-address sticky

Security In Computing Practical's

Step 2: Verify port security.

SW-A/B# show port-security int fa0/1

Step 3: Disable unused ports.

SW-A/B(config)# int range fa0/5 - 22

SW-A/B(config-if-range)# shutdown

Step 4: Verify Connectivity

Ping C1->C2 (Successful)

Ping C1->D1 (Successful)

Step 5: Verify port security.

SW-A/B# show port-security int fa0/1