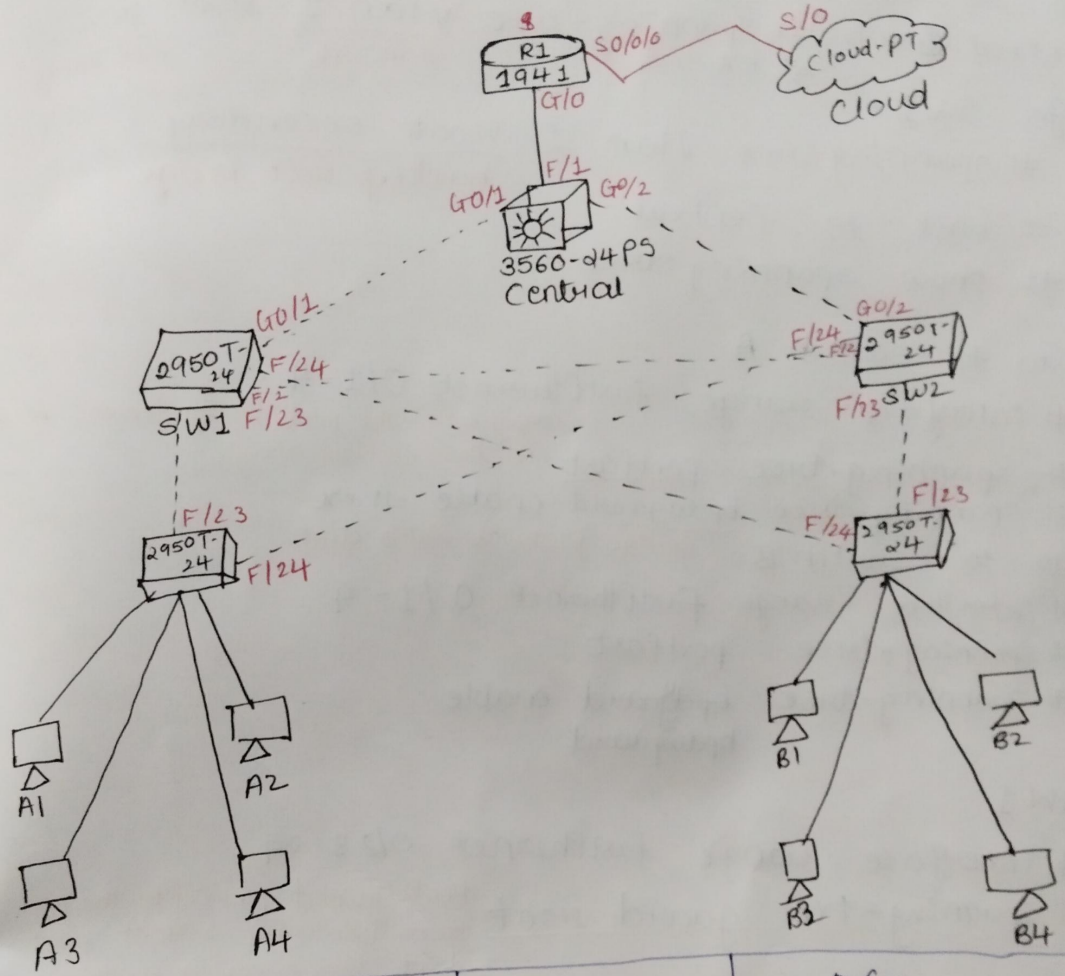
Practical 7

Layer 2 security



Device	IP	Subnet	DG
R1 S/0/0	201.10.10.1	255.255.255.0	
R1 G0/0	192.168.29.1	255.255.255.0	
PC A1	10.10.10.20	255.255.255.0	
B1	10.10.10.10	" "	

Secure the Router & switches with password & ssh
Set the Hostname & display name of all switches.

→ Go to central switch to make it a root bridge.
central (config)# spanning-tree vlan 1 root primary
ex
vlan id — root bridge

→ In SW1
#spanning-tree vlan 1 root secondary
backup root bridge

→ Go back to central
show spanning-tree

→ Go to switch A
interface range fastEthernet 0/1-4
configure the ports to go from 1 state to another immediately.
spanning-tree portfast
spanning-tree bpduguard enable # ex
Bridge Protocol Data Unit

→ Go to switch B
interface range fastEthernet 0/1-4
spanning-tree portfast
spanning-tree ~~bpdguard~~ enable
bpduguard

→ SW1
interface range fastEthernet 0/23-24
spanning-tree guard root
Root guard prevents the port from becoming a root port if it receives a superior BPDU.

→ SW2
interface range fastEthernet 0/23-24
spanning-tree guard root

→ SWA : (Repeat same for SWB)
interface range f 0/1-22
switchport mode access
access configuration for switchports
switchport port-security maximum (2)
max no. of mac addresses allowed.
enables port security mode that restricts no. of MAC add
switchport port-security violation shutdown
if violation is detected shutdown
switchport port-security mac-address sticky
Dynamically learn the mac-add of devices connected to a port and securing them

→ Go to SWA (Repeat for SWB)
#ex #ex #ex
login to SWA using password.
SWA# show port-security interface f 0/1
conf t
interface range fastEthernet 0/5 - 22
shutdown

Spanning tree protocol: A layer 2 network protocol.
select root bridge, root port
It is used to prevent looping within a n/w topology

Layer 2 switch operates at layer 2 of OSI i.e. Datalink
Layer 2 uses MAC address to determine where data goes. Switch has a table that has the details of which port is connected to which MAC address.

BPDU - Message exchanged ~~with~~ between switches participating in a spanning tree protocol. They are used for electing the root bridge, determine the best path to the root bridge, and prevent network loops by managing port states.

Bridge Protocol Data Unit