VLAN Trunking & Security Implementation in Cisco Packet Tracer

Overview:

This document outlines the implementation of VLAN trunking and port security between two switches to enable inter-switch communication and segment network traffic securely. The design focuses on connecting three departments: HR, Sales, and IT, using VLANs with enhanced security practices to prevent unauthorized access.

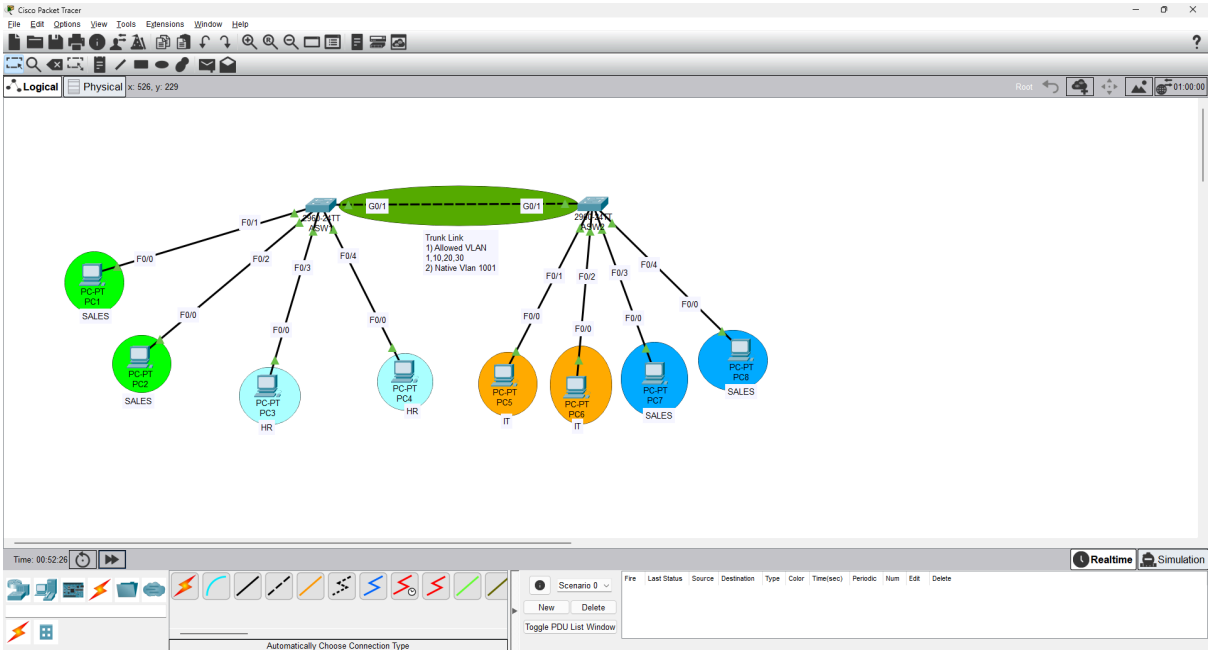
Why Do We Need a Trunk on Switches?

By default, VLANs are isolated within a single switch, meaning devices in different VLANs cannot communicate unless explicitly configured.

- A trunk link is required to allow multiple VLANs to pass traffic between switches over a single physical connection.
- Without a trunk, each VLAN would need a separate cable between switches, which is inefficient and impractical.
- Trunking enables scalability and network optimization, allowing seamless communication while preventing unnecessary broadcast traffic.

🌐 **Network Topology**

- Devices:Two Cisco 2960 switches, connected via Gigabit Ethernet trunk link.
- A total of 8 PCs were connected, with 4 on each switch.
- VLAN Assignments
- VLAN 10 → HR Department
- VLAN 20 → Sales Department
- VLAN 30 → IT Department



⚖️ Purpose of Trunking

Trunking allows VLAN traffic from multiple VLANs to be carried over a single physical link between switches, enabling communication across switches for devices on the same VLAN.

🛠️ Configuration Summary

```
# Enable trunking
interface Gig0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport trunk native vlan 1001
 switchport trunk allowed vlan 10,20,30

# Disable DTP to prevent trunk negotiation attacks
 switchport nonegotiate

# Configure access ports
interface range FastEthernet0/2 - 0/5
 switchport mode access
 switchport access vlan 10   # Example for HR
```

```
interface range FastEthernet0/6 - 0/7
 switchport mode access
 switchport access vlan 20   # Example for Sales

# Disable unused ports
interface range FastEthernet0/8 - 0/24
 shutdown
```

```
ASW1#show vlan  brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                Gig0/2
10   VLAN0010                         active    Fa0/1, Fa0/2
20   VLAN0020                         active    Fa0/3, Fa0/4
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
ASW1#
```

```
ASW2#show vlan  brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                Gig0/2
10   Sales                            active    Fa0/3, Fa0/4
20   Hr                               active
30   IT                               active    Fa0/1, Fa0/2
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
ASW2#
```

```
ASW1#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Gig0/1      on           802.1q         trunking      1001

Port        Vlans allowed on trunk
Gig0/1      1,10,20,30

Port        Vlans allowed and active in management domain
Gig0/1      1,10,20

Port        Vlans in spanning tree forwarding state and not pruned
Gig0/1      1,10,20

ASW1#
```

```
ASW2#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Gig0/1      on           802.1q         trunking      1001

Port        Vlans allowed on trunk
Gig0/1      1,10,20,30

Port        Vlans allowed and active in management domain
Gig0/1      1,10,20,30

Port        Vlans in spanning tree forwarding state and not pruned
Gig0/1      1,10,20,30

ASW2#
ASW2#
```

```
ASW1#show int g0/1 switchport
Name: Gig0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1001 (Inactive)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: 1,10,20,30
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
```

⚡ Security Measures Implemented

- Set native VLAN to an **unused VLAN (1001)** to prevent VLAN hopping attacks.
- Used **"switchport nonegotiate"** to disable Dynamic Trunking Protocol (DTP).
- Defined **allowed VLANs** on the trunk to restrict unnecessary VLAN traffic.
- Disabled **unused switch ports** to eliminate attack surfaces.

✅ Verification & Troubleshooting

Show VLAN status
show vlan brief

Show trunk port configuration
show interfaces trunk

Verify native VLAN
show interfaces Gig0/1 switchport

🚀 Conclusion

This VLAN trunking implementation optimizes network communication, reduces cabling complexity, and improves security. By setting up VLANs and trunks correctly, this lab demonstrates best practices in network segmentation and inter-switch connectivity, essential for enterprise environments.

In this lab, I successfully configured VLAN trunking and implemented security measures using Cisco 2960 switches in Packet Tracer. By segmenting departments through VLAN assignments and establishing a secure trunk link, I ensured efficient data transmission while minimizing security risks.