Cisco Switching Mini Project Documentation

Project Overview

This mini network project demonstrates advanced switching concepts using Cisco Packet Tracer. The implementation includes four switches configured with:

- Basic security and management settings
- EtherChannel for link aggregation
- VTP for centralized VLAN management
- VLAN segmentation with pruning
- Port security mechanisms

Network Topology

The topology consists of four switches:

- SW1 (VTP Server)
- SW2 (VTP Client)
- SW3 (VTP Client)
- SW4 (VTP Client)
- SW5 (VTP Client)
- SW6 (VTP Client)
- SW7 (VTP Client)
- SW8 (VTP Client)

Connection Specifications:

Connection	Channel-group	Protocol	Interfaces
Sw1 Sw3	1	LACP	(fa0/1-2) (fa0/1-2)
Sw2 Sw3	2	PAGP	(fa0/1-2) (fa0/3-4)
Sw3 Sw6	3	PAGP	(fa0/1-2) (fa0/7-8)
Sw3 Sw5	4	LACP	(fa0/1-2) (fa0/5-6)
Sw6 Sw4	5	PAGP	(fa0/1-2) (fa0/3-4)
Sw5 Sw4	6	LAGP	(fa0/3-4) (fa0/3-4)
Sw4 Sw8	2	PAGP	(fa0/1-2) (fa0/7-8)
Sw4 Sw7	1	LAGP	(fa0/1-2) (fa0/5-6)

PC Port Assignments:

VLAN	Name	Port range
10	HR	192.168.1.10-27/24
20	ICT	
30	FIN	

Configuration Summary

1. Basic Switch Configurations

Applied to all switches:

- Unique hostname (for each switch)
- Security banner warning against unauthorized access
- Privileged EXEC password: cisco
- Console access:
    - Password: cisco
    - Logging synchronous
    - 2-minute timeout
- VTY (remote) access:
    - Password: cisco
    - Logging synchronous

    - 2-minute timeout
- Password encryption enabled
- IP domain lookup disabled
- Configurations saved to NVRAM

2. EtherChannel Implementation

Configured using mixed protocols:

- **LACP** & **PAGP**
- All port-channels configured as trunks

3. VTP Configuration

- Domain: cisco.com
- Version: 2
- Password: cisco
- Modes:
    - SW1: Server
    - SW2-SW8: Clients

4. VLAN Configuration

Created on VTP Server (SW1) and propagated to clients:

1. VLAN 10: HR
2. VLAN 20: ICT
3. VLAN 30: FIN

Access ports are assigned on switches according to the port ranges specified in the topology.

5. VLAN Pruning

- Implemented on SW1
- VLAN 20 blocked on Port-Channel 1

6. Port Security

Applied to all access ports (Fa0/6-24):

- Maximum 2 MAC addresses per port
- Sticky MAC address learning
- Violation mode: Shutdown
- Verification using show port-security

Testing and Verification

Connectivity Tests

1. Intra-VLAN communication:
    - PCs in same VLAN can ping each other
    - PCs in different VLANs cannot communicate
2. VLAN 20 Isolation:
    - After pruning, VLAN 20 devices cannot communicate across switches
    - Other VLANs maintain connectivity

Checkpoint	Command	Expected outcome
Etherchannel status	Show etherchannel	All ports in Su state
VTP configuration	Show vtp status	Consistent domain/version across switches
VLAN propagation	Show vlan	All VLANs are present on all switches
Port security	Show port-security	Correct the violation mode and Mac limits