Campus Network Configuration

Name: Shaugato Paroi

Email: 103523487@student.swin.edu.au

# 1. Introduction

This document outlines the Campus Network Configuration configuration, implementation, and testing of the switched network for the International Travel Agency. The primary objective was to design and deploy a robust, scalable, and secure network that meets the specified requirements, including VLAN segmentation, Layer 3 routing, EtherChannel setup, HSRP redundancy, and security features such as DHCP snooping and port security.

# 2. Network Topology

The network topology consists of two distribution layer switches (DLS1 and DLS2) and two access layer switches (ALS1 and ALS2). The network is designed to support various VLANs, trunk links, and Layer 3 interfaces. The following are the gateway addresses configured for the VLANs in the network:  
  
A diagram of a network

Description automatically generated

## 2.1. Gateway Addresses

* **VLAN 10 (Staff)**: 172.16.10.1/24
* **VLAN 20 (Students)**: 172.16.20.1/24
* **VLAN 100 (Management)**: 172.16.100.1/24
* **VLAN 110 (Voice)**: 172.16.110.1/24

The distribution switches (DLS1 and DLS2) are configured to provide redundancy and high availability using HSRP for the VLANs.

# 3. Configuration Details

## 3.1. Layer 3 EtherChannel Configuration

The connection between DLS1 and DLS2 was configured as a Layer 3 EtherChannel using LACP, ensuring redundancy and load balancing between the distribution switches.

* **DLS1**:
  + IP Address: 172.16.200.1/30
* **DLS2**:
  + IP Address: 172.16.200.2/30

## 3.2. Trunk Links & EtherChannel Configuration

EtherChannels were configured for the trunk links between the switches to ensure efficient use of bandwidth and provide fault tolerance.

* **Port-channels on interfaces G1/0/1, G1/0/2, Fa0/1, Fa0/2**: Configured using PAgP.
* **Port-channels on interfaces G1/0/3, G1/0/4, Fa0/3, Fa0/4**: Configured statically.

All inter-switch links were statically set as 802.1q trunks with VLAN 800 set as the native VLAN to prevent any VLAN tagging issues.

## 3.3. VTP Configuration

The switches were configured to use VTP version 3 within the VTP domain "CISCO." All switches were set to VTP transparent mode to allow local VLAN configuration while preventing the propagation of VLAN information.

## 3.4. VLAN Configuration

The following VLANs were created on each switch, aligning with the organization's network segmentation strategy:

* **VLAN 10**: Staff
* **VLAN 20**: Students
* **VLAN 100**: Management
* **VLAN 110**: Voice
* **VLAN 800**: Native
* **VLAN 999**: Parking (for unused interfaces)

## 3.5. Access Port Configuration

Specific interfaces were configured as access ports for different VLANs:

* **DLS1**: Gi1/0/7 configured for VLAN 100.
* **ALS1**:
  + Fa0/7-12: Configured for VLAN 20.
  + Fa0/13-24: Configured for VLAN 10.
* **ALS2**:
  + Fa0/7-12: Configured for VLAN 10.
  + Fa0/13-24: Configured for VLAN 20.

Unused interfaces were placed in the Parking VLAN (VLAN 999), set to access mode, and shut down to enhance security.

## 3.6. Spanning-Tree Protocol (STP) Configuration

The Spanning-Tree Protocol was configured to optimize network redundancy and prevent loops.

* **MST Instance 1**: For VLAN 10 and VLAN 20, DLS1 was configured as the primary root bridge, and DLS2 as the secondary.
* **MST Instance 2**: For VLAN 100 and VLAN 110, DLS2 was configured as the primary root bridge, and DLS1 as the secondary.

## 3.7. Switch Virtual Interface (SVI) Configuration

SVIs were configured to provide Layer 3 routing between VLANs and to facilitate management:

* **Management VLAN 100 SVI Addresses**:
  + DLS1: 172.16.100.2
  + DLS2: 172.16.100.3
  + ALS1: 172.16.100.101
  + ALS2: 172.16.100.102
* **SVIs for VLANs 10, 20, and 110**:
  + DLS1: 172.16.x.2
  + DLS2: 172.16.x.3

## 3.8. Layer 3 Interface Configuration

Layer 3 interfaces were configured on the distribution switches to handle inter-VLAN routing:

* **DLS1 G1/0/11**: 192.168.0.2/30
* **DLS2 G1/0/12**: 192.168.1.2/30

## 3.9. HSRP Configuration

Hot Standby Router Protocol (HSRP) version 2 was configured to provide gateway redundancy for the VLANs:

* **DLS1**:
  + Active for VLANs 10 and 20.
* **DLS2**:
  + Active for VLANs 100 and 110.
* The **pre-empt** option was enabled on both switches, along with interface tracking for the links to the GATEWAY router.

## 3.10. EIGRP Configuration

EIGRP was configured with the following settings to ensure efficient routing within the network:

* **Autonomous System (AS)**: 100
* **Automatic Summarization**: Disabled to allow for precise control of routing advertisements.
* **Default Route**: Configured to propagate into EIGRP.

## 3.11. PortFast, BPDUguard, and UDLD Protection Configuration

These features were enabled to enhance the network's resilience against certain types of Layer 2 issues:

* **PortFast**: Enabled on all access ports to reduce the time it takes for interfaces to enter the forwarding state.
* **BPDUguard**: Enabled on all access ports to prevent the acceptance of BPDUs on those ports.
* **UDLD Protection**: Configured on all switchport interfaces to place ports into an error-disabled state if a unidirectional link is detected.

## 3.12. DHCP Snooping and Port Security Configuration

Security measures were implemented to safeguard the network against DHCP attacks and unauthorized access:

* **DHCP Snooping**:
  + Trusted on trunk ports of ALS1 and ALS2.
  + User access ports were limited to 15 DHCP requests per second.
  + DLS1 and DLS2 were configured to trust DHCP information.
* **Port Security**:
  + **ALS1 Fa0/13-24**: Configured to allow only three MAC addresses per port, with the port being shut down on a violation.
  + **ALS2 Fa0/18**: Configured to only allow MAC address 1234.1234.1234, entering protected mode on a violation.

## 3.13. VLAN 150 (Server Farm) Configuration

A Server Farm was added to the network, with VLAN 150 allocated for this purpose. VLAN 151 (Isolated) and VLAN 152 (Community) were configured for specific servers.

* **DLS2**:
  + VLAN 150: Primary HSRP.
  + VLAN 151: Isolated VLAN, assigned to interfaces Gi1/0/15-17.
  + VLAN 152: Community VLAN, assigned to interfaces Gi1/0/18-20.
* **DLS1**: Configured as the standby for VLAN 150 HSRP.

**3.14. Access Control Lists (ACLs) and VLAN Access Control Lists (VACLs)**

ACLs and VACLs were configured to enforce security policies within the network:

* **ACL**: Configured to separate student (VLAN 20) and staff (VLAN 10) networks.
* **VACL**: Configured on ALS1 Fa0/9 to block the temporary staff member from accessing the rest of the Staff VLAN while still allowing access to other network resources.

**3.15. SSH and NTP Configuration**

SSH and NTP were configured to allow secure management and time synchronization across the network:

* **SSH on GATEWAY**:
  + Domain name: sshremote.lab
  + Username: Admin
  + Password: sshuser
  + SSH access tested and verified using PuTTY.
* **NTP Configuration**:
  + DLS1 was set as the NTP server.
  + DLS2, ALS1, and ALS2 were synchronized with the NTP server via the Management VLAN.

# 4. Verification and Testing

## 4.1. Connectivity Tests

Ping tests were conducted between all SVIs, verifying that inter-VLAN routing and Layer 3 interfaces were operational. Successful pings confirmed that all configured IP addresses were reachable.

## 4.2. HSRP Functionality Tests

Failover scenarios were tested by shutting down active interfaces on DLS1 and DLS2, ensuring that the standby switch took over as expected without any loss of connectivity.

## 4.3. Security Feature Verification

The functionality of PortFast, BPDUguard, and UDLD protection was tested by simulating network events. All features responded as expected, providing additional layers of security and protection.

## 4.4. ACL and VACL Testing

The ACL and VACL configurations were tested to ensure that traffic was being correctly filtered according to the policies defined. The temporary staff member on ALS1 Fa0/9 was restricted as intended.

## 4.5. SSH and NTP Testing

SSH access to the GATEWAY was tested and confirmed to be secure. The correct time synchronization was verified across DLS1, DLS2, ALS1, and ALS2.

# 5. Conclusion

The network configuration for the International Travel Agency was successfully implemented and thoroughly tested. All network elements, including redundancy features, security protocols, and routing configurations, were verified to be fully functional and in line with the provided specifications. The network is now ready for deployment, with all objectives achieved as per the case study requirements.