NOTRE DAME UNIVERSITY
BANGLADESH

Computer Networks Project Report

Course Code: CSE-3204
Course Title: Computer Networks Lab
Project Title: Failover Network Using Redundant Paths
Batch : CSE (19+20)

Submitted by:

Sazzad Jelani	**ID: 0692220005101003**
Nafisa Tabassum	**ID: 0692220005101008**
Sadia Islam Mim	**ID: 0692220005101010**
Istiak Alam (CSE 20)	**ID: 0692230005101005**

Submission Date: June 20, 2025

Submitted to:

Dr. Fernaz Narin Nur
Adjunct Professor,
Notre Dame University Bangladesh

Contents

Failover Networks Using Redundant paths

Introduction

In modern enterprise and institutional environments, network availability is critical for ensuring smooth and uninterrupted communication across departments and with centralized systems. As organizations increasingly rely on digital communication and services, the demand for networks that can tolerate device or path failures without disrupting connectivity has become paramount.

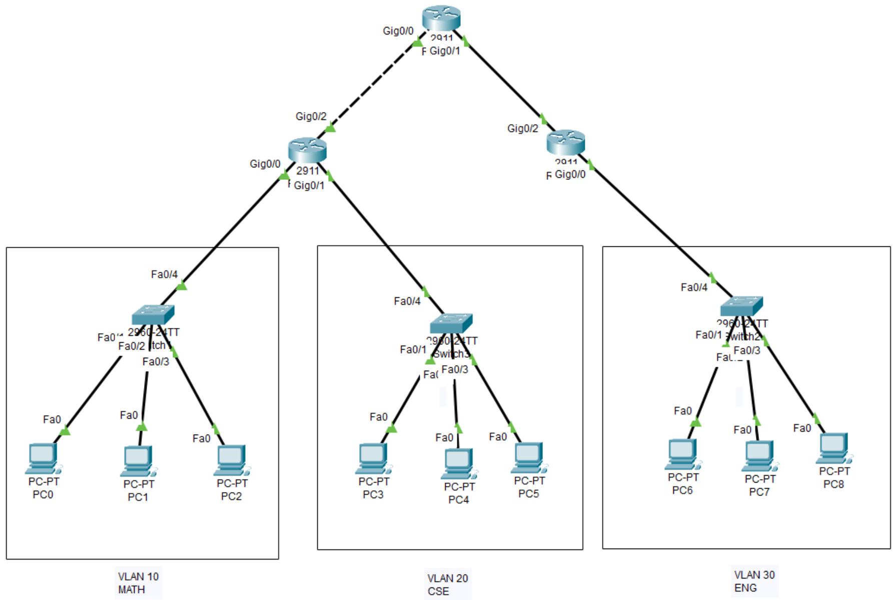
This project focuses on the design and simulation of a failover network using redundant paths in Cisco Packet Tracer. Through a comparative analysis of a basic static-routing topology versus an HSRP-enabled design, we demonstrate the importance of designing networks that remain operational even in the face of individual component failures.

Network Topology Overview

The network is designed to simulate a multi-departmental campus. The topology consists of three main sections representing departments, each with its own switch and set of PCs. These switches are configured with separate VLANs:

- VLAN 10 (Math Department)
- VLAN 20 (CSE Department)
- VLAN 30 (ENG Department)

In the initial topology, each departmental switch was connected to a single router. VLAN 10 and VLAN 20 were served solely by the left router, and VLAN 30 on the right router. These routers communicated with a central core router, which provided inter-VLAN routing. LAN where each department is logically separated using VLANs, yet all can communicate across the same network.



Problem Statement

- <u>Analyzing the Problem</u>

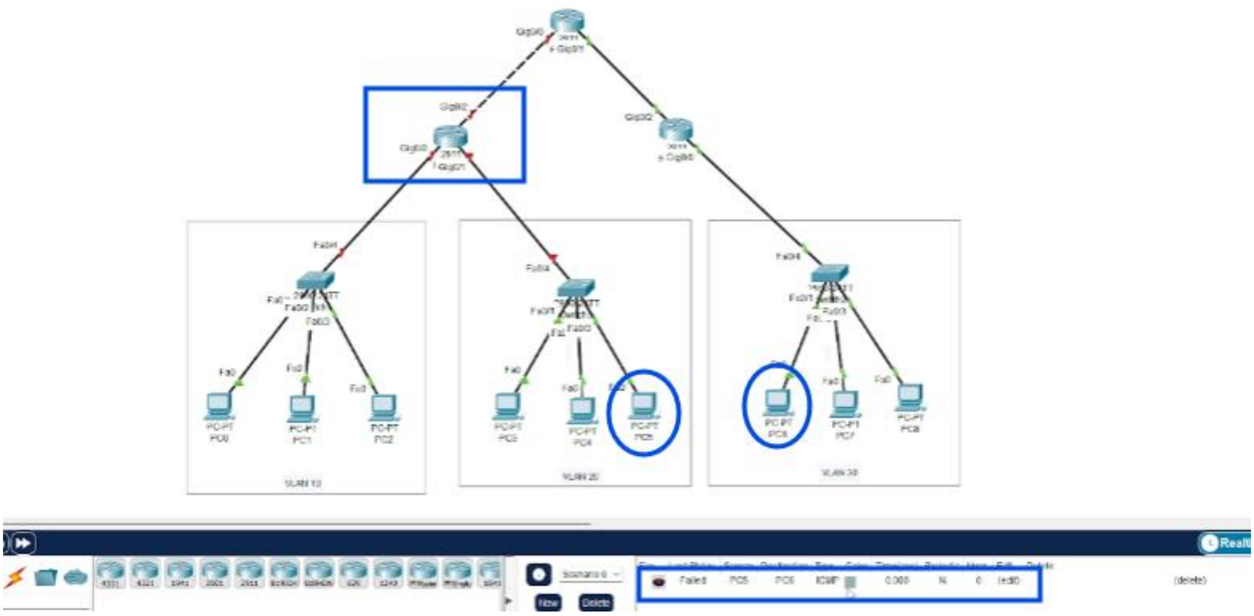
Although this setup allows inter-VLAN communication, it lacks redundancy. So if any router failed, the department it served internet will become isolated. If either of these routers failed or a cable was disconnected, all devices connected to its respective switch lost inter-VLAN connectivity and access to other departments. Only devices on same VLAN will be able to communicate with other. This created a critical vulnerability, no failover path was available.

Additionally, the design lacked dynamic fault tolerance. Even though static routing was applied, the system had no mechanism to elect an alternate routing path dynamically in case of failure. Thus, manual intervention was required, making the system unreliable for real-time communications.

If the LEFT Router Fails:

- VLAN 10 and VLAN 20 PCs use the left router as their default gateway.
- These PCs will lose their gateway (cannot reach any other VLANs or the internet).
- VLAN 30 PC (which uses the right router) can still reach the network it belongs to and any remote VLAN if routing exists via the right router.

Switches only forward within VLANs. Routers handle inter-VLAN routing. The router-to-router cable doesn't act as a failover path unless the routing configuration explicitly uses it to forward traffic between VLANs.Thus, the purpose of the proposed design **is continuity of communication among departments even if router associated with one or multiple VLAN crashes**.



- Objective

Certain requirements which are not fulfilled by the current topology:

This network setup ensures:

- To implement a topology where each department (VLAN) has physical connections to more than one router.
- Fault-tolerant routing using HSRP virtual IP addressing.
- Logical separation via VLANs.
- Backup network availability for failed network.
- To reduce downtime and manual recovery steps by automating failover using redundant links.

Proposed Solution and Design Approach

In the improved topology, HSRP is implemented using two routers—an active and a standby. Each switch is now connected to both routers via trunk links, and a multilayer switch is used as the core device. This switch provides high-speed routing and simplifies the centralization of the network. The ISP or external connection is simulated via the core router's upper link.

To overcome the lacings of the original topology, we adopted a revised architecture as shown below (with HSRP and a multilayer switch).

Features	Without HSRP	With HSRP
Redundancy	No	Yes, with failover via HSRP
VLAN Trunking	No	Yes
Multilayer Switching	No	Yes
Central Router Access Reliability	Partial (unreachable if router fails)	Full (available via active or standby router)
Automatic Failover	No	Yes
Centralized Gateway Addressing	No	Yes (via HSRP Virtual IP)

Background Study

- Redundant Path

A redundant path refers to the availability of multiple, alternative routes for data to travel between two points, ensuring that if one path fails, data can still be transmitted via another path. This mechanism enhances network reliability and availability by preventing disruptions caused by failures or congestion in the primary data path.

- Multilayer Switch

A multilayer switch (Core) is used to handle both Layer 2 and Layer 3 switching. This enables VLAN interconnectivity and routing without relying entirely on external routers for inter-VLAN traffic. It also centralizes all routing paths toward the ISP router and the server.

- VLAN (Virtual LAN)

A VLAN, or Virtual LAN, is a logical grouping of network devices that behave as if they were connected to the same physical network, even if they are physically located on different segments.

- Trunk

Trunking is a method of carrying multiple VLANs over a single physical link, typically between network switches or between a switch and a router.

Routing Protocols

- STP (Spanning Tree Protocol)

STP is a network protocol used to prevent looping within a network topology. STP was created to avoid the problems that arise when computers exchange data on a local area network (LAN) that contains redundant paths. STP uses the spanning tree algorithm to prevent loops.

- HSRP (Hot Standby Router Protocol)

Even if physical connections are perfect, logical routing paths need to be configured which routes you set inside routers. Even sometimes physical connections are optional but internal configuration is important.

HSRP protocol enables a set of router interfaces to work together to present the appearance of a single virtual router or default gateway to the hosts on a LAN. The virtual router does not exist; it represents the common target for routers that are configured to provide backup to each other. In this protocol, one of the routers is selected to be the active router and another to be the standby router, which assumes control of the designated active router fail. HSRP uses trunk to see all VLANs, enabling failover.

- MHSRP(Multiple Hot Standby Router Protocol)

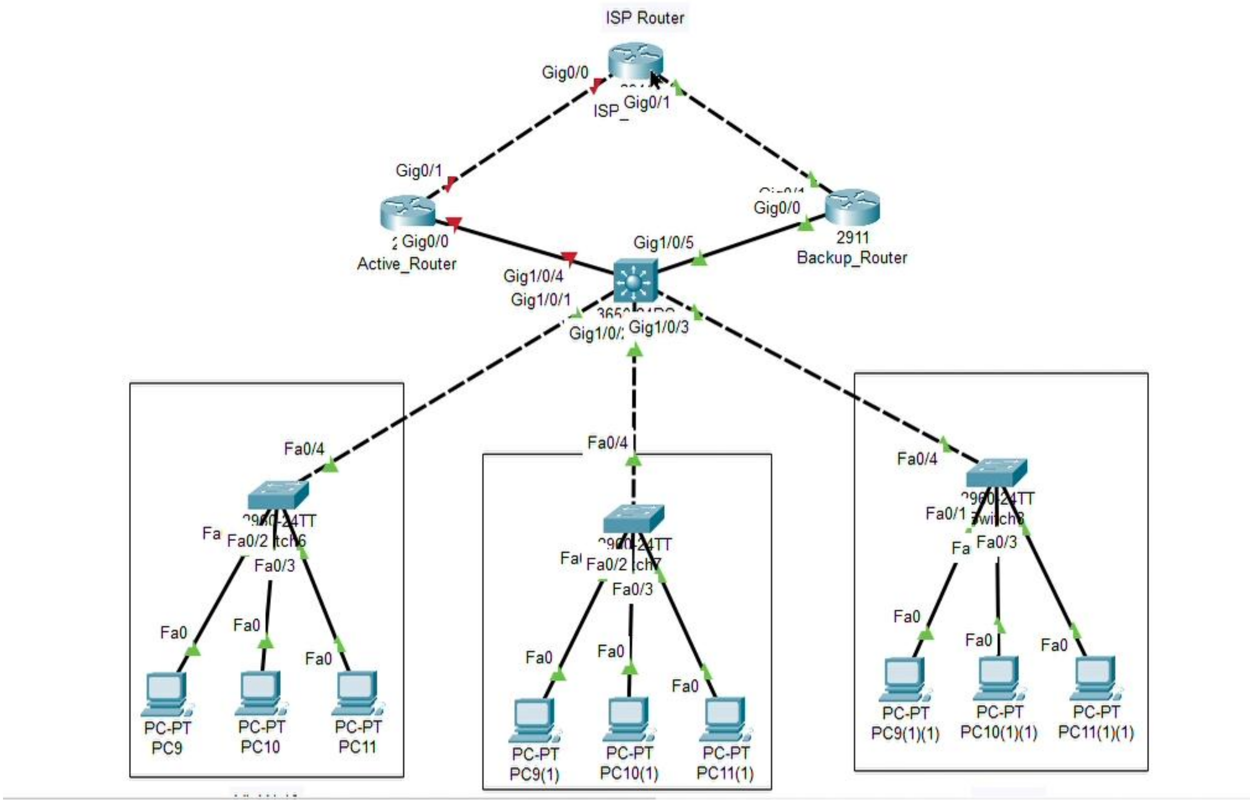
To support load balancing in addition to failover, Multiple HSRP (MHSRP) can be implemented. we can configure Multigroup HSRP between two routers. Let us consider in this topology VLAN 10 and VLAN 20 are group 1. VLAN 30 being the 2nd group. So for two groups of networks:

- Router 1 is Active for group 1.
- Router 2 is Active for group 2.

Each router is Standby (Backup) for the alternative groups. In HSRP the standby router listens but doesn’t forward traffic until the active router fails.

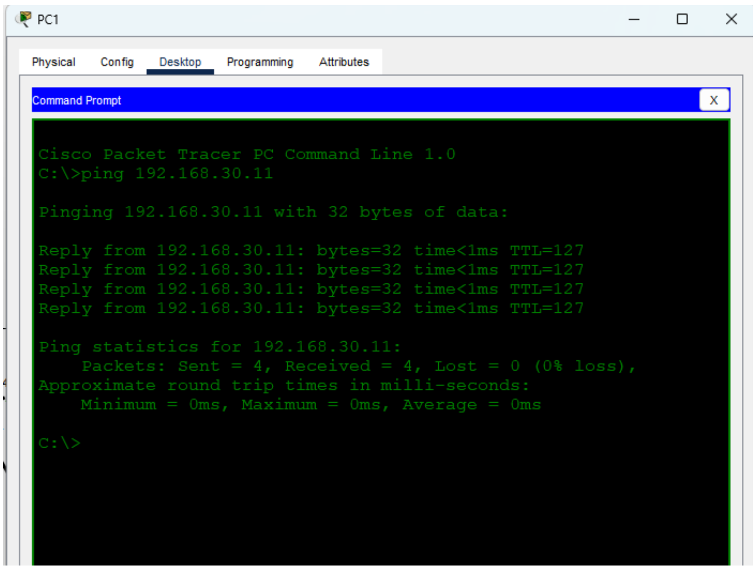
HSRP Configuration & Testing

Network Topology



Testing (ping status)

- After turning of the Active_Router, all the other devices still going through the network
  As an example: ping from PC1 to PC7 – ***ping 192.168.30.11***



Troubleshooting and Observations

- As for testing purpose, we tried multiple topologies for the following problem to solve where we were not able to solve the problem for wider network.
- Our aim was to establish a instant failover network. But for cisco simulation it takes almost 10-15 minutes to establish a new network. So, it will be a thing to observe if it happens in real situation also.

Future Work / Improvements

- Applying MHSRP as it seems like a better and efficient approach on HSRP protocol.
- Applying dynamic routing (like OSPF or EIGRP) instead of static so routers would automatically exchange routing information.
- As organizations grow, their networks become more complex. Working with multiple layers of distribution and access switches, supporting more VLANs, interdepartmental routers will be an room for improvement.
- Trying on more advanced redundancy protocols to explore and compare HSRP with:

VRRP (Virtual Router Redundancy Protocol): An open standard alternative to HSRP, offering similar redundancy with vendor interoperability.

GLBP (Gateway Load Balancing Protocol): A Cisco protocol that not only offers redundancy but also enables true load balancing between routers, enhancing performance and redundancy simultaneously.

References

- https://cciethebeginning.wordpress.com/2008/08/27/mhsrp-and-load-sharing/
- https://cciethebeginning.wordpress.com/2008/08/27/mhsrp-and-load-sharing/
- https://www.networkacademy.io/ccna/network-services/hot-standby-router-protocol-hsrp
- https://www.computernetworkingnotes.com/ccna-study-guide/hsrp-configuration-and-load-balancing-explained.htmlhttps://www.cisco.com/c/en/us/support/docs/ip/hot-standby-router-protocol-hsrp/9234-hsrpguidetoc.html#toc-hId--375142717