DEPI

NTER-BRANCH CONNECTIVITY PROJECT

Presented by: Mohamed Goda
Merna Maged
Amr Ahmed

OVERVIEW

01

Project Overview

02

Network Design

03

Key Protocols and Technologies

04

Challenges and Solutions

05

Conclusion

PROJECT OVERVIEW

OBJECTIVE

The aim of this project is to design and implement a secure, scalable network infrastructure connecting two company branches. The network will ensure seamless communication, resource sharing, and high availability between both locations.

TECHNOLOGIES

- Routing: OSPF
- Switching: VTP , STP , EtherChannel ,secuirty
- Security: VPN ,ACLs
- NAT: Network Address Translation
- Management: Syslog Server,
- WLAN: Wireless LAN support
- DHCP server

NETWORK DESIGN OVERVIEW

Topology Components:

01 Routers:

- Two routers (left and right) with tunnel interfaces for VPN connectivity.
- NAT configuration

02 Distribution Switches:

- Serve as the central switches in each branch, connecting to both routers and access switches.
- Configured with EtherChannel for redundancy and link aggregation.

03 Access Switches:

- Connected to distribution switches via EtherChannel for high availability.
- VLANs configured on the access switches:
  - VLAN 10 (IT) for PCs.
  - VLAN 20 (Sales) for other devices like phones.

04 End Devices:

- PCs and phones connected to access switches and segmented by VLANs.

05 Servers:

- Syslog server for logging network events and TFTP server for device configuration backups.

06 Wireless Access Points (WAPs):

- Extending network coverage wirelessly
- Enabling mobile device connectivity via WLAN (Wireless LAN)

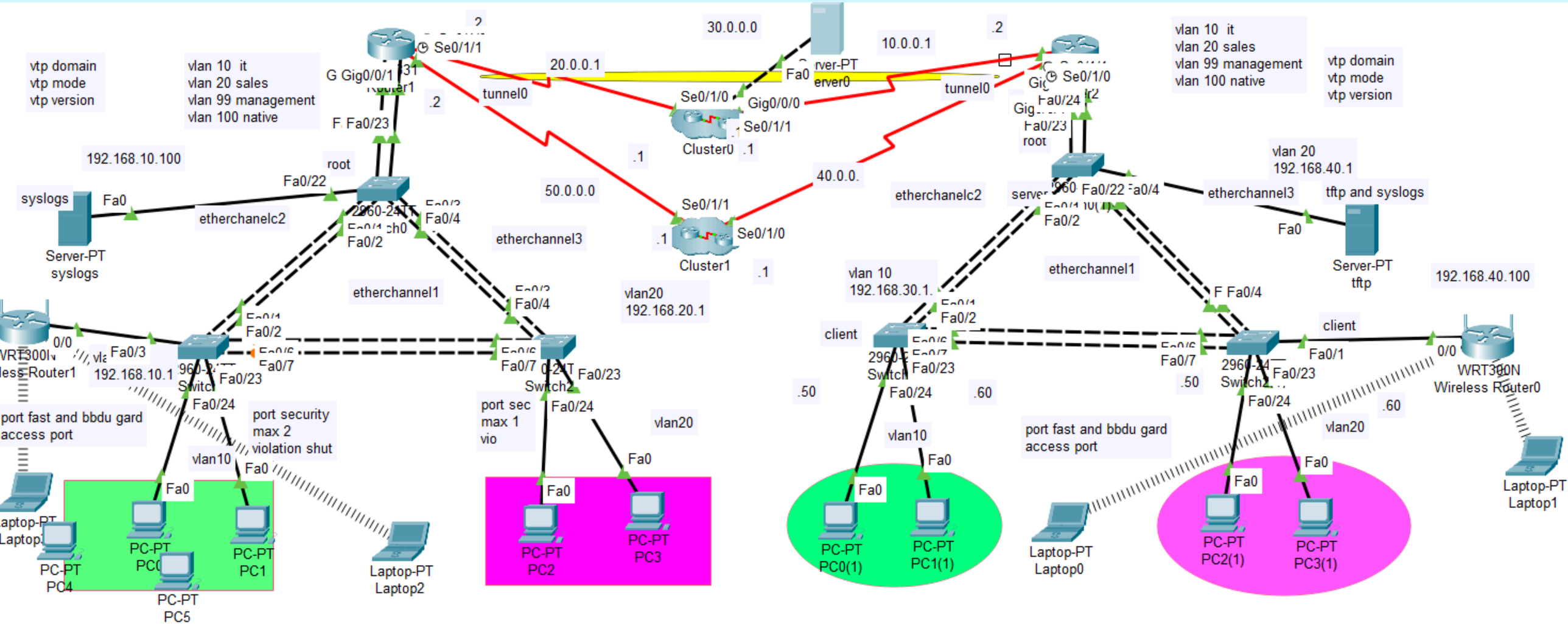
NETWORK DESIGN OVERVIEW

Redundancy and Link Aggregation:

- EtherChannel links between distribution and access switches for high availability and increased bandwidth.
- Spanning Tree Protocol (STP) prevents network loops, but EtherChannel minimizes STP complexity by grouping links.
- PortFast and BPDU Guard on end-device ports improve network startup time and security.

WAN Connectivity:

- VPN Tunnel between routers (via Tunnel0) ensures secure communication between branches.
- NAT configuration on routers for external network (internet) access.


vtp domain
vtp mode
vtp version
vlan 10 it
vlan 20 sales
vlan 99 management
vlan 100 native
30.0.0.0
20.0.0.1
10.0.0.1
tunnel0
Se0/1/1
Se0/1/0
Gig0/0/0
Fa0
Cluster0
Cluster1
.1
.2
50.0.0.0
40.0.0.
192.168.10.100
root
Fa0/22
Fa0/23
Fa0/24
Fa0/2
Fa0/4
syslogs
Server-PT
etherchanelc2
etherchannel3
etherchannel1
vlan 20
192.168.40.1
tftp and syslogs
tftp
vlan 10
192.168.30.1.
vlan20
192.168.20.1
192.168.40.100
client
Fa0/1
Fa0/3
Fa0/7
0/0
WRT300N
Wireless Router0
192.168.10.1
port fast and bbdu gard
access port
port security
max 2
violation shut
port sec
max 1
vio
vlan10
vlan20
.50
.60
Laptop-PT
Laptop0
Laptop1
Laptop2
PC-PT
PC0
PC1
PC2
PC3
PC4
PC5
PC0(1)
PC1(1)
PC2(1)
PC3(1)

NETWORK PROTOCOLS

This project will employ Cisco networking devices and technologies, focusing on routing, switching, and security protocols

OSPF

- OSPF (Open Shortest Path First):Purpose: Dynamic routing protocol used to share routing information between routers.
- Usage in the Network:
  - Facilitates communication between routers and ensures efficient routing.
  - Ensures optimal path selection between the two branches.

VTP

- Purpose: Simplifies management of VLANs across multiple switches by synchronizing VLAN information.
- Usage in the Network:

Ensures consistent VLAN configurations on all switches.

Reduces manual configuration errors by centralizing VLAN information.

STP

- Purpose: Prevents loops in a Layer 2 network by blocking redundant paths.
- Usage in the Network:
  - Ensures a loop-free network topology while providing backup paths if a link fails.
  - Used in tandem with EtherChannel to optimize path selection and redundancy.

ETHERCHANNEL

- Purpose: Bundles multiple physical links into a single logical link for increased bandwidth and redundancy.
- Usage in the Network:
  - Implemented between distribution and access switches.
  - Provides load balancing and redundancy, allowing for automatic failover in case one link goes down.

VPN

- Purpose: Securely connects the two branches over the internet.

- Usage in the Network:
  - VPN Tunnel (Tunnel0) ensures encrypted communication between the two branches.
  - Protects sensitive data while traveling between locations.

NAT

- Purpose: Translates private IP addresses to public IP addresses for devices accessing the internet.
- Usage in the Network:
  - Configured on the routers to allow internal devices to access external networks .
  - Ensures that internal network addresses remain hidden from the public

DHCP

- Purpose: Automatically assigns IP addresses and network configuration settings to devices.

- Usage in the Network:
  - Simplifies IP address management, ensuring dynamic and efficient allocation of addresses in both wired and wireless networks.

HSRP

- Purpose: Provides network redundancy by allowing multiple routers to share a virtual IP address, ensuring continuous availability in case the primary router fails.
- Usage in the Network:
  - Ensures high availability and automatic failover in case the active router becomes unavailable.

SYSLOG

- Purpose: Collects and logs network events for monitoring and troubleshooting.
- Usage in the Network:
  - Centralized logging server (Syslog) used to record important events from routers and switches.
  - Helps in monitoring network health and diagnosing issues.

FTP server

- Purpose: Provides a platform for file sharing and configuration backups between network devices.
- Usage in the Network:
  - TFTP and configuration file backups.
  - Can also be used for upgrading firmware and software on devic

CHALLENGES AND SOLUTIONS

Network Scalability

- Challenge: Ensuring the network can accommodate future growth without significant redesign.

- Solution:
  - Implementing a hierarchical network design that separates layers (core, distribution, access).
  - Using VLANs and EtherChannel to optimize bandwidth and allow for easy expansion.

Security Concerns

- Challenge: Protecting sensitive data during transmission between branches.

- Solution:
  - Implementing VPN for secure communication between sites.
  - Configuring access control lists (ACLs) on routers to restrict unauthorized access.
  - configure switches security

CHALLENGES AND SOLUTIONS

Network Performance

- Challenge : Ensuring optimal performance during peak usage times.
- Solution:
  - Regular monitoring of network performance using Syslog and other tools.
  - Adjusting configurations and allocating resources based on traffic analysis.

Redundancy and Reliability

- Challenge: Ensuring continuous network availability and minimizing downtime.
- Solution:
  - Device Redundancy: Deploy multiple routers and switches; use HSRP for failover.
  - Link Redundancy: Implement EtherChannel and STP for loop prevention and failover.
  - backup ISPs

CONCLUSION

the network design project successfully established a robust and scalable infrastructure connecting two company branches, leveraging Cisco technologies to facilitate seamless communication and resource sharing. Through the implementation of routing protocols such as OSPF, VPNs for secure connectivity, and redundancy measures, the network demonstrated high availability and performance with minimal latency and packet loss. The thorough testing and validation processes highlighted the effectiveness of the design .

DEPI

Thank's For Watching