Graduation Project

Multi-Branch Bank Infrastructure with server integration

Cisco Network Administrator (ONL1_ISS2_S1e) - 2604

Made by

Abdelhameed Mohamed Elkhadrgy

Youssef Hany Feyala

Mahmoud Ahmed Zaki Hassan

Mohamed Rashed Rashed

Youssef Fathy Mohamed Youssef

Supervised by

Eng. Amr Reda

Table of Content

1. Introduction

1.1 Document Control

Document Information

Document Title : Multi-Branch Bank Infrastructure with server integration
Document Owner : Packet Masters

1.2 Document Purpose

The primary objective of this project is to build a robust and scalable network infrastructure capable of supporting various operational and business functions across multiple locations. The network aims to:

- Centralize the management of the network, allowing efficient administration of branches and resources.
- Implement VLANs for department-based segmentation, providing logical isolation and optimizing resource allocation.
- Secure communication between branches via VPN tunnels with encryption, ensuring the confidentiality and integrity of transmitted data.
- Ensure redundancy at critical points in the network to enhance reliability and minimize downtime.
- Provide secure, scalable wireless access for mobile users in the branches.
- Enable effective communication between central and remote branches, with efficient routing and switching configurations.

1.3 Key Features

 VLAN Segmentation: The network design divides departments into separate VLANs to optimize performance, secure communications, and manage resources efficiently. Each department (e.g., Retail Banking, IT, HR, etc.) has its own VLAN.
 VPN (GRE): A secure VPN tunnel (using GRE) connects the remote branch (Branch 1) to the central branch, allowing encrypted communication across the public network. This ensures data security and integrity when transmitting sensitive information between branches.
 Redundancy: Redundant connections between critical network components (core switches, distribution switches, access switches, and routers) ensure high availability and minimize the risk of network failures.
 Wireless LAN: The implementation of a Wireless LAN Controller (WLC) ensures that wireless devices in the central branch can securely and efficiently connect to the network, with centralized management of wireless access points.

 Centralized Servers: Critical network services such as DNS, DHCP, FTP, and Syslog servers are centralized in the central branch to facilitate easy management and maintenance. These servers also support the remote branches to ensure unified network services.

2. Technical Solution Overview

2.1 Details of the solution

This project implements a scalable and secure multi-branch network infrastructure with centralized management, utilizing VLANs for departmental segmentation, (GRE) for inter-branch communication, and redundancy through EtherChannel and HSRP to ensure high availability. Centralized services, such as DNS, DHCP, and Syslog, support seamless operations across both the central and remote branches. A Wireless LAN Controller (WLC) manages secure wireless access, while access control lists (ACLs) . The design is highly flexible and can easily scale to support future growth and additional branches, ensuring both reliability and efficient management.

2.2 Solution Components

I. Network Solution:

a. Core switches

4 x Cisco 3560 Series Layer 3 Switches.

b. Servers:

DHCP Server: Provides dynamic IP addressing to devices across VLANs.
DNS Server: Resolves hostnames to IP addresses.
FTP Server: Handles file transfers between devices on the network.
Syslog Server: Collects and stores logs from network devices for centralized monitoring and troubleshooting.
Email Server: Manages email communication for the organization.

c. Layer 2 Access Switches:

6 x Cisco 2960 Series Layer 2 Switches: Deployed at both the central and remote branches to connect end devices like PCs, printers, and access points. These switches handle VLAN assignments and port security.

d. Routers:

2 x Cisco 2811 Routers: These routers are used to connect the central branch with remote branches through VPN tunnels. They also participate in routing traffic between branches and the internet.

E. Wireless LAN Controller (WLC):

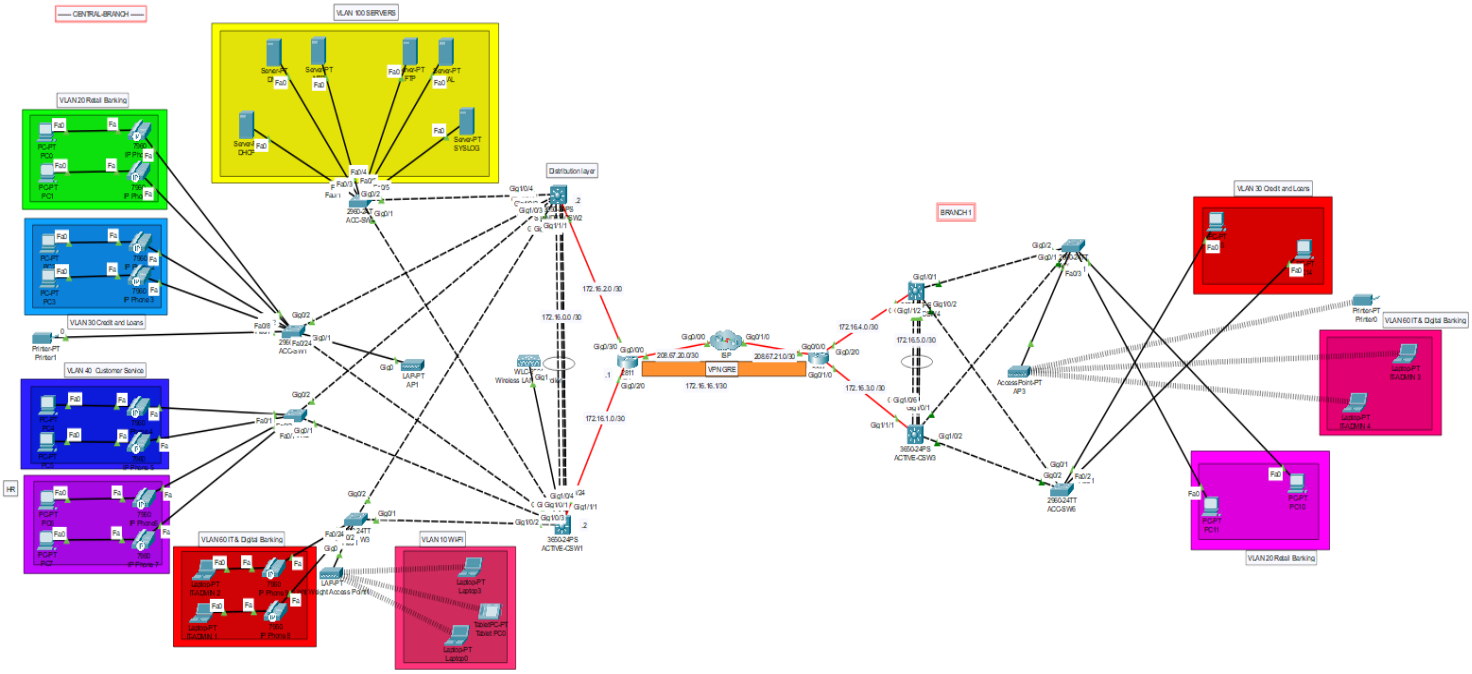
Cisco WLC 5508: This controller manages wireless access points across the central branch, ensuring centralized control of wireless traffic and security.

F. APs:

2 x Cisco Light weight AP
1 x standalone AP

3. Network Architecture

Physical Topology



4. Naming Convention and IP scheme

4.1 Naming Convention

We will use a standard naming convention to name all network infrastructure equipment. This facilitates device identification and management during the day-to-day administration activities as well as problem troubleshooting.

According to network Infrastructure naming convention, we are going to use the following naming schema for our network devices:

Hostname	IP address
R1	172.16.1.1 /30
ACTIVE-CSW1	192.168.99.254
STANDBY-CSW2	192.168.99.254
ACC-SW1	192.168.99.10
ACC-SW2	192.168.99.11
ACC-SW3	192.168.99.12
R2	172.16.3.2
ACTIVE-CSW3	10.0.99.254
STANDBY-CSW4	10.0.99.254
ACC-SW1.	10.0.99.10
ACC-SW2.	10.0.99.11
Wireless LAN Controller	192.168.99.3
DHCP server	192.168.100.50
DNS server	192.168.100.5
NTP server	192.168.100.20
FTP server	192.168.100.15
EMAIL server	192.168.100.25
SYSLOG server	192.168.100.10

4.2 IP Addressing Scheme

The following is the IP schema that will be implemented at building Infrastructure:

VLAN Number	VLAN Name	Subnet	Default gateway
Central branch			

5	Voice	192.168.5.0 /24	192.168.5.254
10	WI-FI	192.168.10.0 /24	192.168.10.254
20	Retail Banking	192.168.20.0 /24	192.168.20.254
30	Credit and Loans	192.168.30.0 /24	192.168. 30.254
40	Customer Service	192.168. 40.0/24	192.168. 40.254
50	HR	192.168.50.0 /24	192.168.50.254
60	IT & Digital Banking	192.168.60.0 /24	192.168.60.254
99	Management	192.168.99.0 /24	192.168.99.254
100	Servers	192.168.100.0/24	192.168.100.254
Branch 1			
20	Retail Banking	10.0.20.0/24	10.0.20.254
30	Credit and Loans	10.0.30.0/24	10.0.30.254
60	IT & Digital Banking	10.0.60.0/24	10.0.60.254
99	Management	10.0.99.0/24	10.0.99.254

Table 1 - IP VLAN Scheme

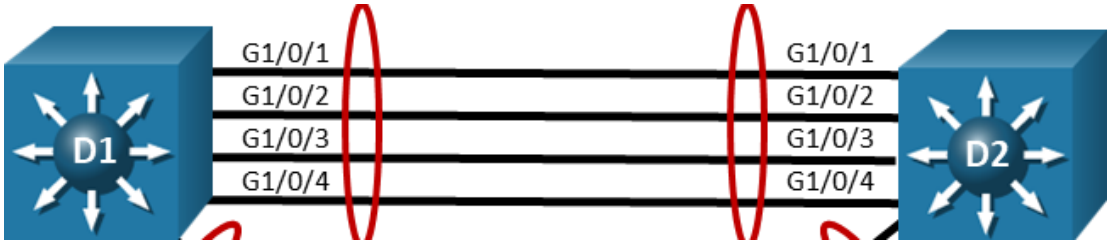
5. Port Mapping

Device	Port	Peer Device
R1	Gig0/0/0	ISP
R1	Gig0/2/0	ACTIVE-CSW1
R1	Gig0/3/0	STANDBY-CSW2
ACTIVE-CSW1	Gig1/0/24	WLC
ACTIVE-CSW1	Gig1/0/1	ACC-SW1
ACTIVE-CSW1	Gig1/0/2	ACC-SW2
ACTIVE-CSW1	Gig1/0/3	ACC-SW3
ACTIVE-CSW1	Gig1/0/4	ACC-SW4
ACTIVE-CSW1	Port-CH 1	STANDBY-CSW2
ACTIVE-CSW1	Gig1/1/1	R1
STANDBY-CSW2	Gig1/0/1	ACC-SW1
STANDBY-CSW2	Gig1/0/2	ACC-SW2
STANDBY-CSW2	Gig1/0/3	ACC-SW3
STANDBY-CSW2	Gig1/0/4	ACC-SW4
STANDBY-CSW2	Port-CH 1	ACTIVE-CSW1
STANDBY-CSW2	Gig1/1/1	R1
ACC-SW1	Gig0/1	ACTIVE-CSW1
ACC-SW1	Gig0/2	STANDBY-CSW2
ACC-SW1	F0/24	AP1
ACC-SW2	Gig0/1	ACTIVE-CSW1
ACC-SW2	Gig0/2	STANDBY-CSW2
ACC-SW3	Gig0/1	ACTIVE-CSW1
ACC-SW3	Gig0/2	STANDBY-CSW2
ACC-SW3	F0/24	AP2
ACC-SW4	Gig0/1	ACTIVE-CSW1
ACC-SW4	Gig0/2	STANDBY-CSW2
R2	Gig0/0/0	ISP
R2	Gig0/1/0	ACTIVE-CSW3
R2	Gig0/2/0	STANDBY-CSW4
ACTIVE-CSW**3**	Gig1/1/1	R1
ACTIVE-CSW**3**	Gig1/0/1	ACC-SW5
ACTIVE-CSW**3**	Gig0/2/0	ACC-SW6
ACTIVE-CSW**3**	Port-CH 1	STANDBY-CSW4
ACC-SW**5**	Gig0/1	ACTIVE-CSW3
ACC-SW**5**	Gig0/2	STANDBY-CSW4
ACC-SW**5**	F0/24	AP3
ACC-SW**6**	Gig0/1	ACTIVE-CSW3
ACC-SW**6**	Gig0/2	STANDBY-CSW4

6. Network Design Notes & Configurations

6.1 Port-Aggeration

In this project, we implemented Layer 3 port aggregation using EtherChannel with a static configuration approach. Instead of relying on dynamic negotiation protocols like LACP (Link Aggregation Control Protocol), we manually configured the EtherChannel on the involved Layer 3 switches. This static method provides control over the aggregation, ensuring a reliable connection between the core and distribution layers, increasing bandwidth, and providing redundancy. The static EtherChannel configuration allows for seamless traffic flow across multiple links and ensures that, in case of a link failure, traffic will automatically switch to the remaining active links without requiring complex negotiation protocols.




```
interface GigabitEthernet1/0/10
 no switchport
 no ip address
 channel-group 1 mode on
 duplex auto
 speed auto
!
interface GigabitEthernet1/0/11
 no switchport
 no ip address
 channel-group 1 mode on
 duplex auto
 speed auto
!
interface GigabitEthernet1/0/12
 no switchport
 no ip address
 channel-group 1 mode on
 duplex auto
 speed auto
!
interface GigabitEthernet1/0/13
 no switchport
 no ip address
 channel-group 1 mode on
 duplex auto
interface Port-channel1
 no switchport
 ip address 172.16.0.1 255.255.255.252
```

Etherchannel configration

6.2 Layer 2 technologies

- Spanning Tree is configured in order to protect against physical and logical misconfigurations and a possibility to erroneously create L2 loops. Spanning tree is used in RPVST mode.
- VLANs carried over the trunking link between the core and the switches.

- Hosts & Server ports on edges are configured as spanning tree port fast to exclude them from the spanning tree protocol decreasing the time these ports take to be up. Unless it is configured as trunk and these ports are explicitly configured as trunk.
- All switches must be managed in a secure a manner by using SSH, authentication mechanism and set privilege levels for different users if needed.
- BPDU Guard is a security feature we used to protect the network from loops by preventing unauthorized devices from sending Bridge Protocol Data Units (BPDUs). It was enabled on access ports with PortFast. If a BPDU is received on these ports, BPDU Guard automatically shuts down the port, preventing potential misconfigurations or loops from affecting network stability. This ensures that only trusted devices participate in the Spanning Tree Protocol (Rapid PVST)

6.2.1 VTP and Vlan Configuration

VTP is a Layer 2 messaging protocol that allows managing, the addition, deletion, and renaming of VLANs on a network-wide basis. In the current setup it is recommended that all Catalysts are in VTP transparent mode. In other words we don't want those switches to listen to VTP updates and share VLAN database between them. Such approach requires more configuration work, because all VLANs should be configured on every switch. This will avoid simple but critical VLAN configuration mistakes being propagated via VTP.

6.2.1.1 VTP Configuration

```
vtp domain DEPI
vtp mode server
```

VTP Configuration

- VTP mode will be configured as server\client.

6.2.1.2 Vlan Configuration

- VLANs will be statically assigned to DC Switches.
- The Vlans would be created as per table 1.

```
vlan <>
 name XXX
```

6.2.2 Spanning-tree

STP is a Layer 2 link-management protocol that provides path redundancy while preventing undesirable loops in the network. For a Layer 2 Ethernet network to function properly, only one active path can exist between any two stations. STP operation is transparent to end stations, which cannot detect whether they are connected to a single LAN segment or a switched LAN of multiple segments.

When you create fault-tolerant internetworks, you must have a loop-free path between all nodes in a network. The STP algorithm calculates the best loop-free path throughout a switched Layer 2 network. Layer 2 LAN ports send and receive STP frames at regular intervals. Network devices do not forward these frames, but use the frames to construct a loop-free path.

6.2.2.1 Spanning-tree Configuration

Spanning Tree is configured in order to protect against physical and logical misconfigurations and a possibility to erroneously create L2 loops. Spanning tree is used in RPVST+ mode.

```
spanning-tree mode rapid-pvst
spanning-tree extend system-id
```

6.2.3 L2 Port configuration

6.2.3.1 Access Port Configuration

```
interface FastEthernet0/1
 switchport access vlan 20
 switchport mode access
 switchport voice vlan 5
 switchport port-security
 switchport port-security maximum 3
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0005.5E6E.1BD7
 switchport port-security mac-address sticky 0060.2F43.2128
 spanning-tree portfast
 spanning-tree bpduguard enable
 mls qos trust cos
```

Access Port Configuration

- Portfast feature is enabled on all user and server ports to allow stable and fast L2 and spanning-tree convergence.
- Ports that are connected to the hosts are put in switchport access mode and are assigned to their corresponding Vlan using switchport commands.
- In this project, we configured Voice VLANs on access ports to prioritize voice traffic for devices like IP phones. A Voice VLAN allows both voice and data traffic to coexist on the same port, but separates them into different VLANs, ensuring that voice traffic receives higher priority for better call quality.

6.2.3.2 Trunk port configuration

In this project, we configured trunk ports to allow multiple VLANs to pass through a single physical link between switches. Trunk ports carry tagged traffic for all VLANs, including the management, data, and voice VLANs, ensuring that inter-VLAN communication can occur across different switches.

```
Core switch
Note : DTP had Negotiated Port Status
interface Vlan99
 mac-address 0050.0fb9.d408
 ip address 192.168.99.1 255.255.255.0
 ip helper-address 192.168.100.50
 ip access-group WLC out
 standby 1 ip 192.168.99.254
 standby 1 priority 150
 standby 1 preempt
```

Trunk Port Configuration

6.3 Voice over IP Technology

6.3.1 Telephone service on router 2811

We implemented a telephone service using IP telephony through the Voice VLAN. IP phones were connected to the network via access ports configured with both a Voice VLAN and a Data VLAN. This setup allows for the prioritization of voice traffic, ensuring high-quality phone calls with minimal latency. The IP phones communicate through a central VoIP server, providing features like call routing, voicemail, and internal communication for the organization's branches.

```
telephony-service
 max-ephones 10
 max-dn 10
 ip source-address 192.168.5.254 port 2000
 auto assign 1 to 11
ephone-dn 1
 number 1001
ephone 1
 device-security-mode none
 mac-address 00E0.F904.95C0
 type 7960
 button 1:1
 ip dhcp pool voice
 network 192.168.5.0 255.255.255.0
 default-router 192.168.5.254
 option 150 ip 3.3.3.3
```

6.4 Management Technologies

6.4.1 Network Devices Access

This point discuss method will be used for securing access to network devices through usernames, passwords, controlling access line parameters, controlling remote access protocols, and affecting privileges of users and commands.

SSH will be the only enabled remote access control protocol to secure the management traffic

```
ip domain-name bank.com
 crypto key generate rsa general-keys modulus 1024
 line vty 0 4
 login local
 transport input ssh
 line vty 5 15
 login local
 transport input ssh
```

Local Users and SSH Configuration

6.4.2 DHCP-Server using relay agent

We configured a DHCP relay agent to enable devices in different VLANs across the network to obtain IP addresses from a centralized DHCP server. Since VLANs are segmented and broadcast traffic is confined to each VLAN, devices in remote VLANs cannot directly communicate with the DHCP server located in a different VLAN..

```
 interface Vlan99
ip helper-address 192.168.100.50      #this is the ip of DHCP server we had configured#
```

DHCP-Relay Configuration

6.4.3 Centralized Mail Server

We implemented a mail server to handle internal and external email communication for the organization. The mail server is responsible for managing user accounts, sending and receiving emails, and ensuring secure email transmission across the network. It supports standard email protocols like SMTP (Simple Mail Transfer Protocol) for sending emails, and POP3 (Post Office Protocol) for retrieving emails.

6.4.4 FTP Server

We configured an FTP server to enable file sharing and management across the network, with different access privileges assigned based on employee positions. The FTP server allows secure file transfers within the organization, supporting various file-sharing needs for different departments.

To enforce security and proper access control, we implemented role-based permissions. Employees were grouped according to their roles, and access levels were assigned accordingly

```
ip ftp username cisco
ip ftp password cisco
```

FTP config on access SW

6.4.5 NTP and time

It is often extremely useful to be able to accurately pinpoint when a particular event occurred. You may want to compare network event messages from various routers on your network for fault isolation, troubleshooting, and security purposes. This is impossible if their clocks are not set to a common source. In fact, the problem is even worse than merely setting the clocks to a single common standard because some clocks run a little bit fast and others run a little bit slow. So they need to be continuously adjusted and synchronized.

Network Time Protocol (NTP) is a standard for protocol which we can use to achieve the previous requirements.

```
no service timestamps log datetime msec
service timestamps debug datetime msec
ntp server 192.168.100.20
clock time zone EG 2
```

NTP Configuration

6.4.6 SYSLOG Server

We implemented a Syslog server to centralize log management and enhance network monitoring and troubleshooting capabilities. The Syslog server collects and stores log messages generated by various network devices, including routers, switches, firewalls, and servers.

```
logging trap debugging
logging 192.168.100.10
```

Logging Configuration

6.4.7 WLC for Wireless Management

We Implemented Wireless LAN Controller (WLC) with WPA2 authentication and restricting access to the management VLAN (VLAN 99) for only the IT team via HTTPS is an important aspect of network security and management.

```
ip access-list extended WLC
 permit tcp 192.168.60.0 0.0.0.255 host 192.168.99.3 eq 443
 permit tcp 10.0.60.0 0.0.0.255 host 192.168.99.3 eq 443
 deny tcp any host 192.168.99.3 eq 443
 permit ip any any
int vlan 99
ip access-group WLC out
```

ACL Configuration

6.4.7.1 WPA2 Authentication

WPA2 (Wi-Fi Protected Access 2) is a widely used security protocol that encrypts wireless traffic, ensuring that data transmitted over the network is secure.

Pre-Shared Key (PSK): Suitable for smaller networks; uses a shared password.

6.5 Layer 2 Security

We implemented several Layer 2 security features to enhance the network's security posture. Port Security was configured to restrict the number of MAC addresses learned on switch ports, preventing unauthorized access and mitigating MAC flooding attacks. We also enabled BPDU Guard on access ports to protect against misconfigured or rogue switches that could introduce loops into the network by shutting down any port that receives a Bridge Protocol Data Unit (BPDU). To further secure the network, we implemented Dynamic ARP Inspection (DAI), which validates ARP packets against a DHCP snooping database to mitigate ARP spoofing attacks. Additionally, we configured IP DHCP Snooping to prevent unauthorized DHCP servers from assigning IP addresses, designating trusted ports for legitimate DHCP servers while marking all client-facing ports as untrusted. Together, these Layer 2 security measures significantly enhance the security and integrity of our network infrastructure, ensuring that only authorized devices can connect and that network disruptions are minimized.

```
ip arp inspection vlan 5,10,20,30,40,50,99,100
!
ip dhcp snooping vlan 5,10,20,30,40,50,99,100
interface GigabitEthernet0/1 #NOTICE THIS IS TRUNK PORT SO ITS TRUSTED#
 ip arp inspection trust
 ip dhcp snooping trust
 switchport mode trunk
interface Fastethernet 0/1    #NOTICE THIS IS AN ACCESS PORT#
```

```
switchport port-security
 switchport port-security maximum 3
 switchport port-security mac-address sticky
 spanning-tree portfast
 spanning-tree bpduguard enable
```

Layer 2 Security Configration

6.6 GRE Tunnel

we implemented Generic Routing Encapsulation (GRE) tunnels to establish connectivity between multiple branches. GRE is a tunneling protocol that encapsulates a wide variety of network layer protocols in a point-to-point connection, allowing us to create a virtual link between branch offices over the internet or other networks

```
BRANCH 1 ROUTER
interface Tunnel1
 ip address 172.16.16.1 255.255.255.252
 mtu 1476
 tunnel source GigabitEthernet0/0/0
 tunnel destination 208.67.21.2
BRANCH 2 ROUTER
 interface Tunnel1
 ip address 172.16.16.2 255.255.255.252
 mtu 1476
 tunnel source GigabitEthernet0/0/0
 tunnel destination 208.67.20.1
```