رواد مصر الرقمية

وزارة الاتصالات
وتكنولوجيا المعلومات

Implementing a Secure Multi-Branch Office Network

DEPI Graduation Project

Cisco Cybersecurity Engineer
(ONL2_ISS5_S2)

Supervised By:

Eng. Amr Adel

Team Members

Ahmed Mohamed Gharib

1- Firewall Security Policies & Zones.

2- DMZ Servers & Services.

3- Security Implementation.

Abdul Rahman Mohammed

1- Aggregation Core Zone.

2- Security Implementation

3- Firewall Inside Policies.

Hassan Mohamed Abdelnaby

1- Branches Overview.

2- DMZ Servers in each Branch.

3- Connectivity Between Branches.

Mohamed Samy El Hamzawy

1- Edge Routers & VPN.

2- ISP With Autonomous Number.

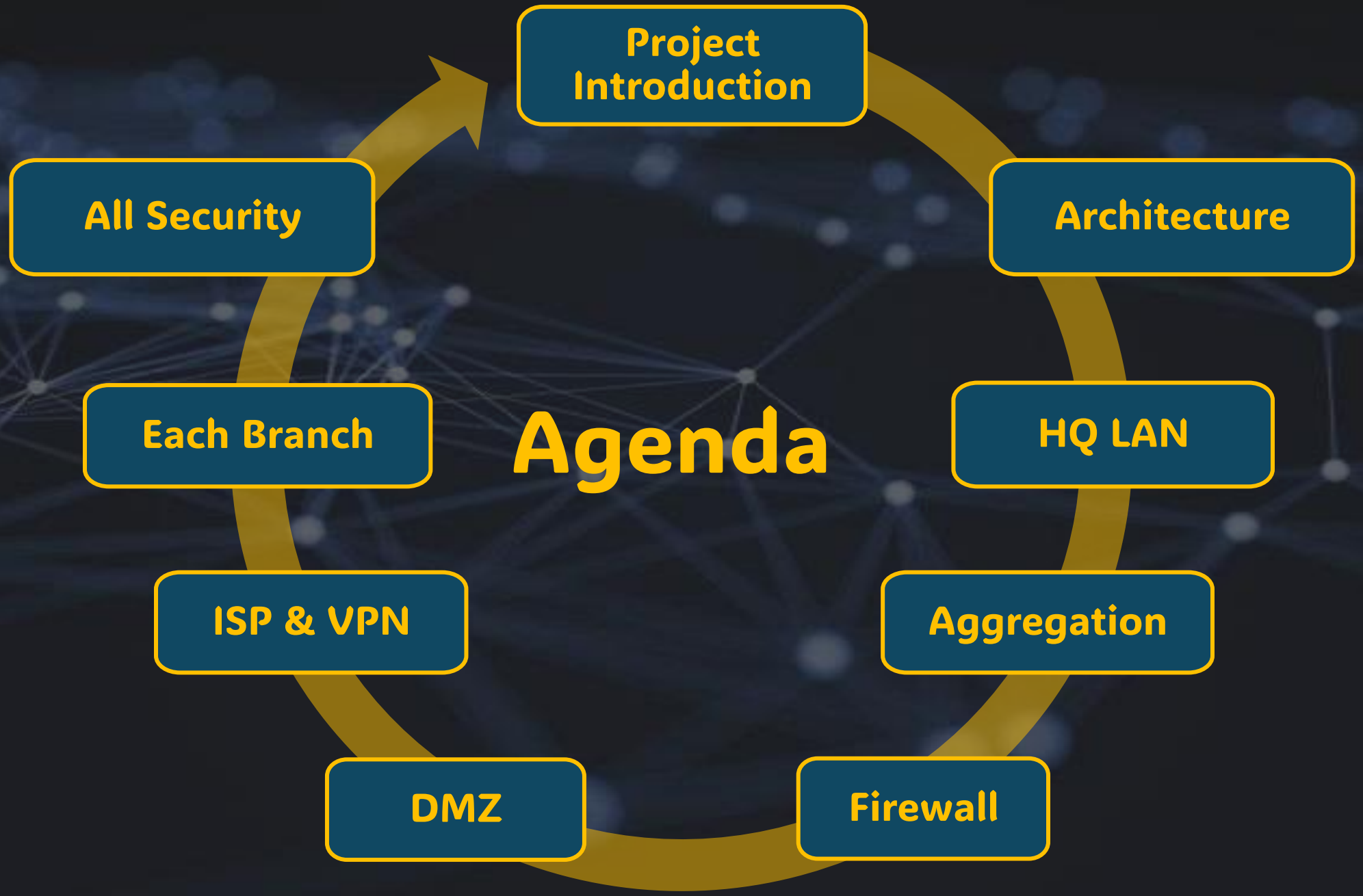
3- Routing & Interface Security.

Muhammed Mustafa Gomaa

1- Network Architecture Design.

2- Headquarters Internal Network.

3- Access Layer Security.


Agenda
Project Introduction
Architecture
HQ LAN
Aggregation
Firewall
DMZ
ISP & VPN
Each Branch
All Security

Project Introduction

Scenario → Requirements → Before → After the Project

Scenario

A **Company** With A Main Office And Three Branch Offices.

Each Office Requires Reliable Connectivity, Secure Communication, And Internet Access.

The **Company** Also Needs Secure And Protection Against Cyber Threats.

Requirements

Network
Segmentation For
Different Departments

Secure
Site-to-site VPNs.

Robust
Security Measures.

Before the Project

Inefficient Communication

With outdated systems, causing delays.

Lack of Network Security

Lacked segmentation and security protocols, making it vulnerable.

Limited Scalability

Due to reliance on third-party providers.

High Operational Costs

With limited flexibility due to leased line connections.

After the Project

Enhanced Security

Advanced security with VLAN segmentation, IPsec VPN, and ACLs, BPDU Guard, DHCP Snooping, Port Security, CDP and DAI.

Improved Efficiency

Improved efficiency with faster and more reliable communication.

Scalable Architecture:

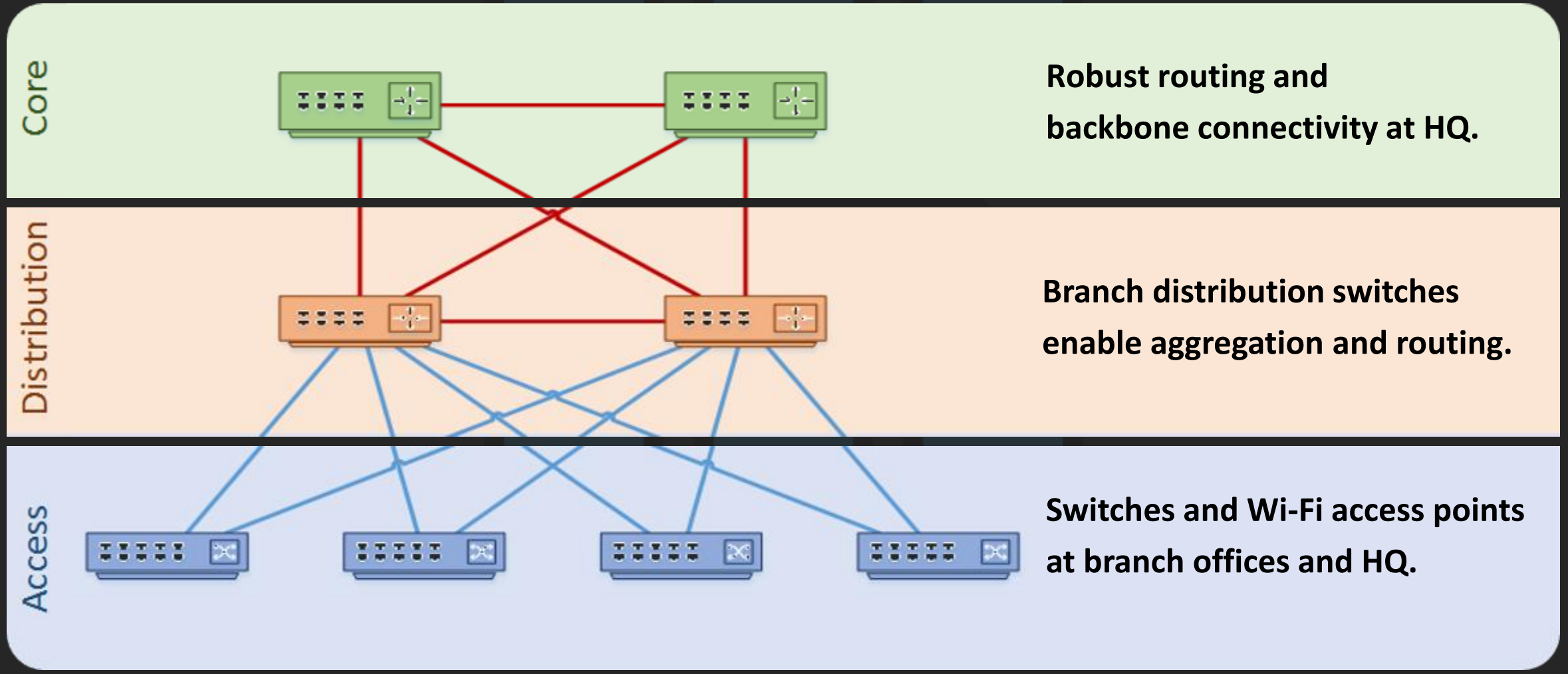
Scalable and flexible architecture allowing easy integration of new branches.

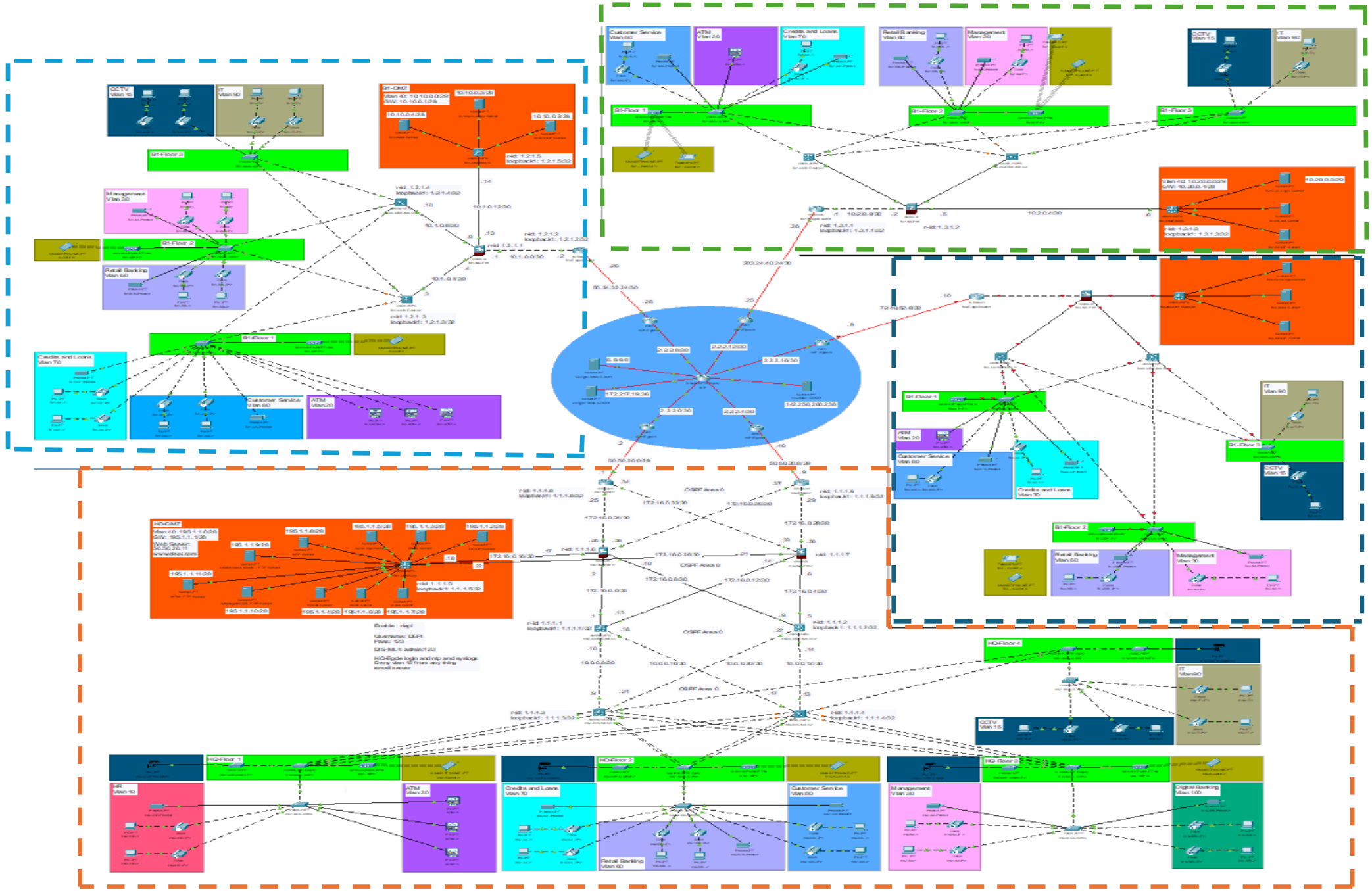
Centralized Management

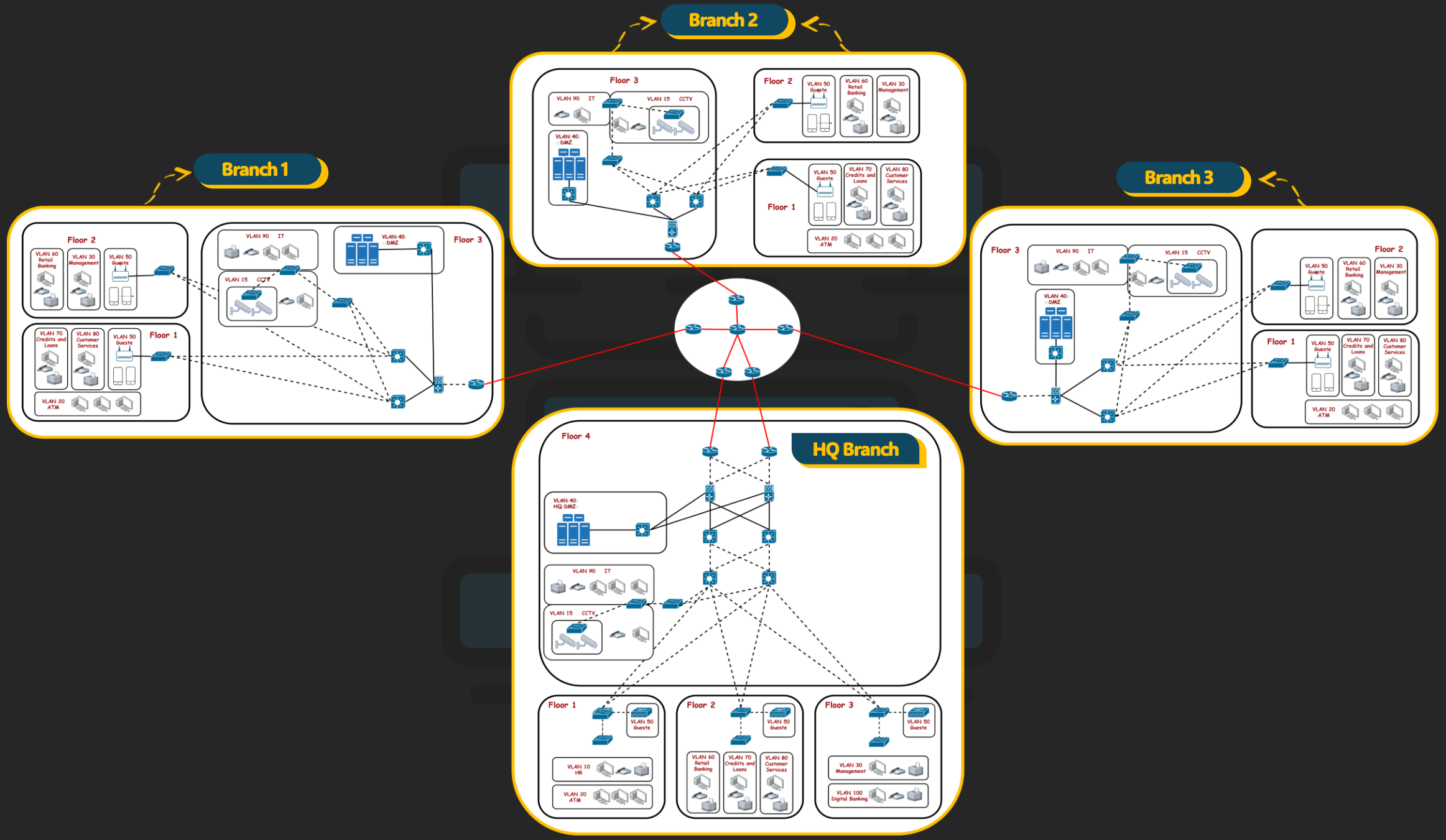
Centralized management using OSPF for routing and DHCP for IP address management.

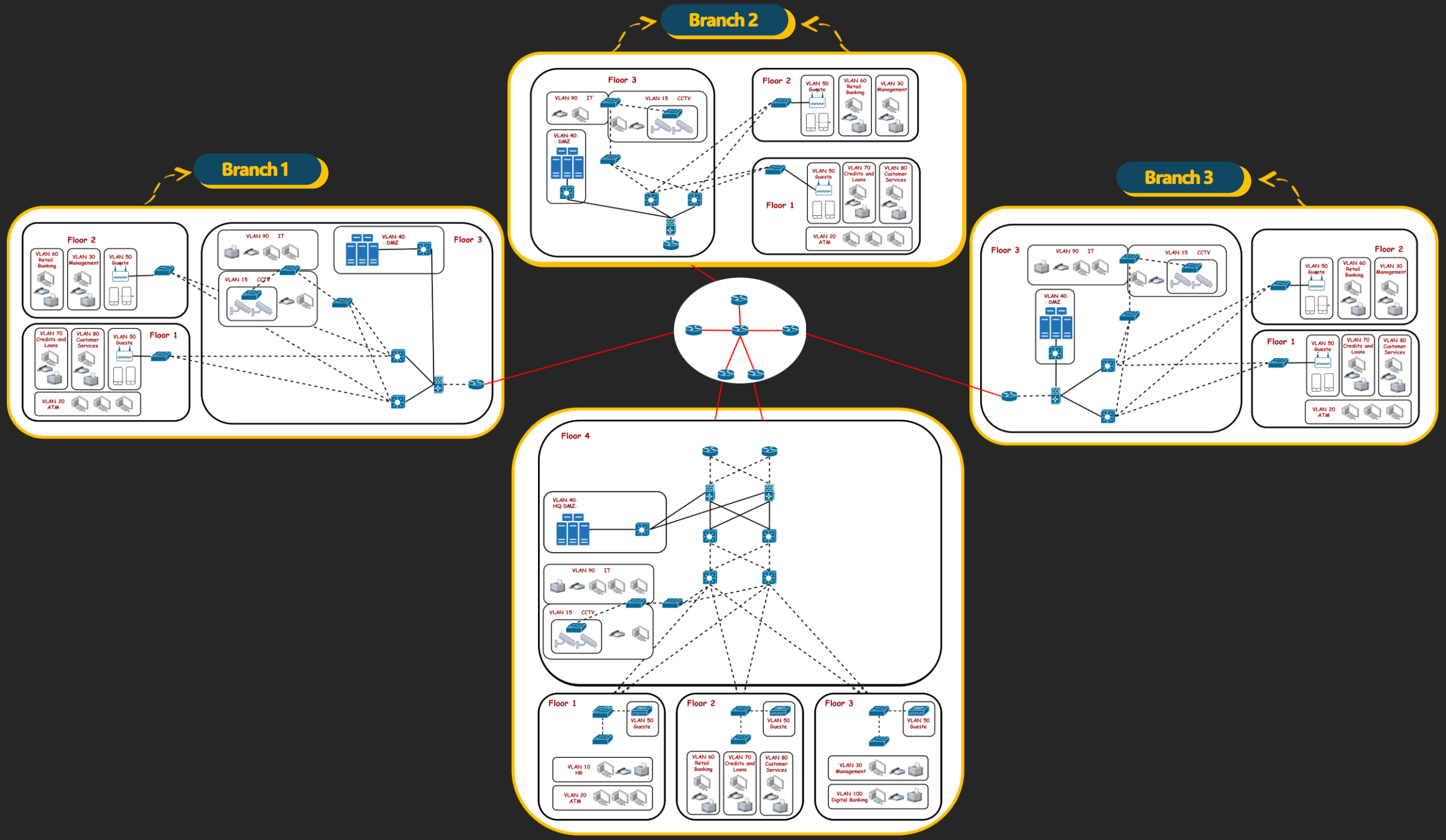
Network Architecture

High-Level Network Design:
Hierarchical Architecture



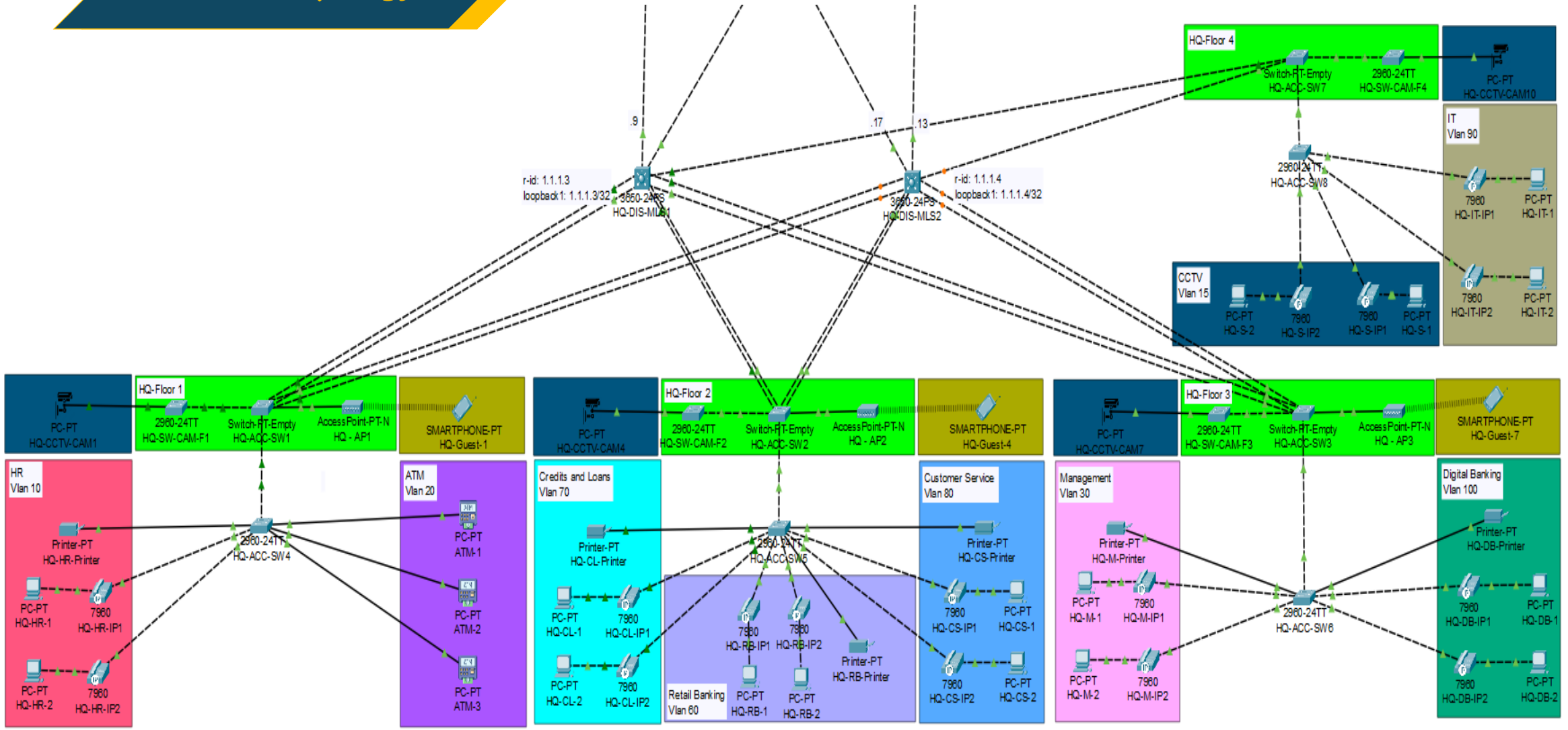

BI-Floor 1
BI-Floor 2
BI-Floor 3
BI-DMZ
Customer Service Vlan 60
ATM Vlan 20
Credits and Loans Vlan 70
Retail Banking Vlan 60
Management Vlan 30
CCTV Vlan 15
IT Vlan 90
HQ-DMZ
HQ-Floor 1
HQ-Floor 2
HQ-Floor 3
HQ-Floor 4
HR Vlan 10
Digital Banking Vlan 100
OSPF Area 0


Branch 2
Floor 3
VLAN 90 IT
VLAN 15 CCTV
VLAN 40 DMZ
Floor 2
VLAN 50 Gueste
VLAN 60 Retail Banking
VLAN 30 Management
Floor 1
VLAN 50 Gueste
VLAN 70 Credits and Loans
VLAN 80 Customer Services
VLAN 20 ATM
Branch 1
Floor 2
VLAN 60 Retail Banking
VLAN 30 Management
VLAN 50 Gueste
Floor 1
VLAN 70 Credits and Loans
VLAN 80 Customer Services
VLAN 50 Gueste
VLAN 20 ATM
VLAN 90 IT
VLAN 15 CCTV
VLAN 40 DMZ
Floor 3
Branch 3
Floor 3
VLAN 90 IT
VLAN 15 CCTV
VLAN 40 DMZ
Floor 2
VLAN 50 Gueste
VLAN 60 Retail Banking
VLAN 30 Management
Floor 1
VLAN 50 Gueste
VLAN 70 Credits and Loans
VLAN 80 Customer Services
VLAN 20 ATM
HQ Branch
Floor 4
VLAN 40 HQ DMZ
VLAN 90 IT
VLAN 15 CCTV
Floor 1
VLAN 50 Gueste
VLAN 10 HR
VLAN 20 ATM
Floor 2
VLAN 50 Gueste
VLAN 60 Retail Banking
VLAN 70 Credits and Loans
VLAN 80 Customer Services
Floor 3
VLAN 50 Gueste
VLAN 30 Management
VLAN 100 Digital Banking

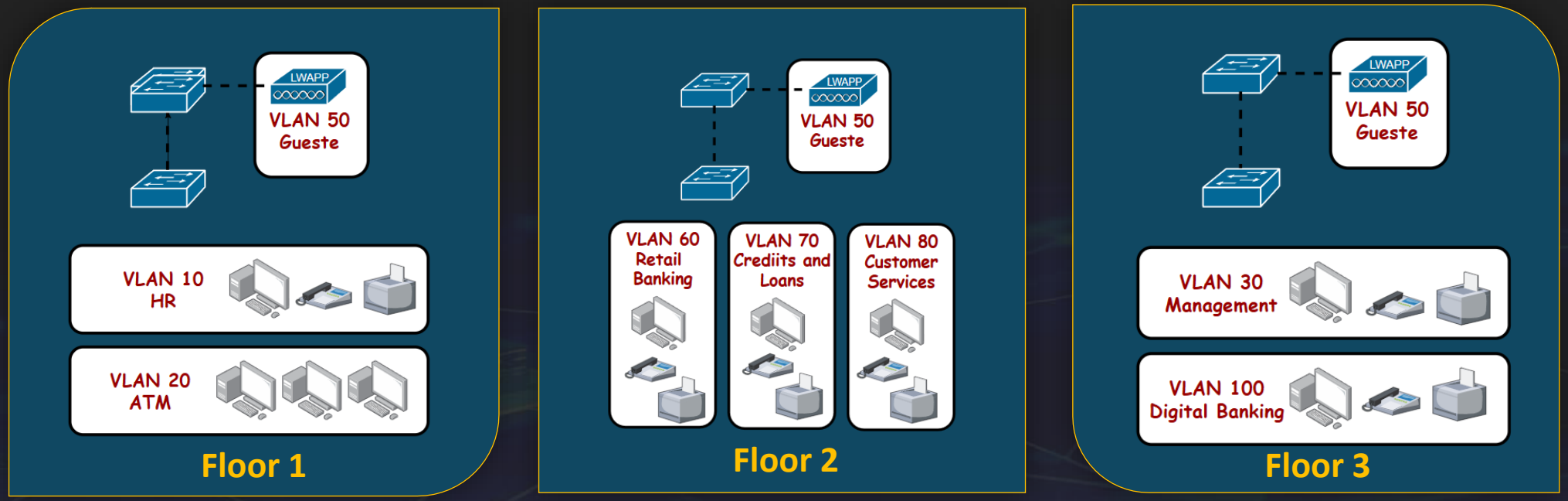

Branch 2
Floor 3
VLAN 90 IT
VLAN 15 CCTV
VLAN 40 DMZ
Floor 2
VLAN 50 Gueste
VLAN 60 Retail Banking
VLAN 30 Management
Floor 1
VLAN 50 Gueste
VLAN 70 Credits and Loans
VLAN 80 Customer Services
VLAN 20 ATM
Branch 1
Floor 2
VLAN 60 Retail Banking
VLAN 30 Management
VLAN 50 Gueste
Floor 1
VLAN 70 Credits and Loans
VLAN 80 Customer Services
VLAN 50 Gueste
VLAN 20 ATM
VLAN 90 IT
VLAN 15 CCTV
VLAN 40 DMZ
Floor 3
Branch 3
Floor 3
VLAN 90 IT
VLAN 15 CCTV
VLAN 40 DMZ
Floor 2
VLAN 50 Gueste
VLAN 60 Retail Banking
VLAN 30 Management
Floor 1
VLAN 50 Gueste
VLAN 70 Credits and Loans
VLAN 80 Customer Services
VLAN 20 ATM
Floor 4
VLAN 40 HQ DMZ
VLAN 90 IT
VLAN 15 CCTV
Floor 1
VLAN 50 Gueste
VLAN 10 HR
VLAN 20 ATM
Floor 2
VLAN 50 Gueste
VLAN 60 Retail Banking
VLAN 70 Credits and Loans
VLAN 80 Customer Services
Floor 3
VLAN 50 Gueste
VLAN 30 Management
VLAN 100 Digital Banking

HQ LAN

Network Topology

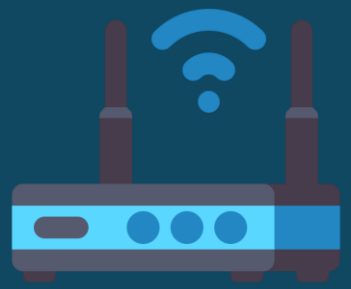


Architecture & VLANs



End Devices

PCs



WAPs

IP Phones

CCTV

ATMs

IP Phones

Voice VLAN

Prioritizes bandwidth to ensure high-quality voice calls.

Quality of Service (QoS)

Manages network traffic to minimize latency and jitter.

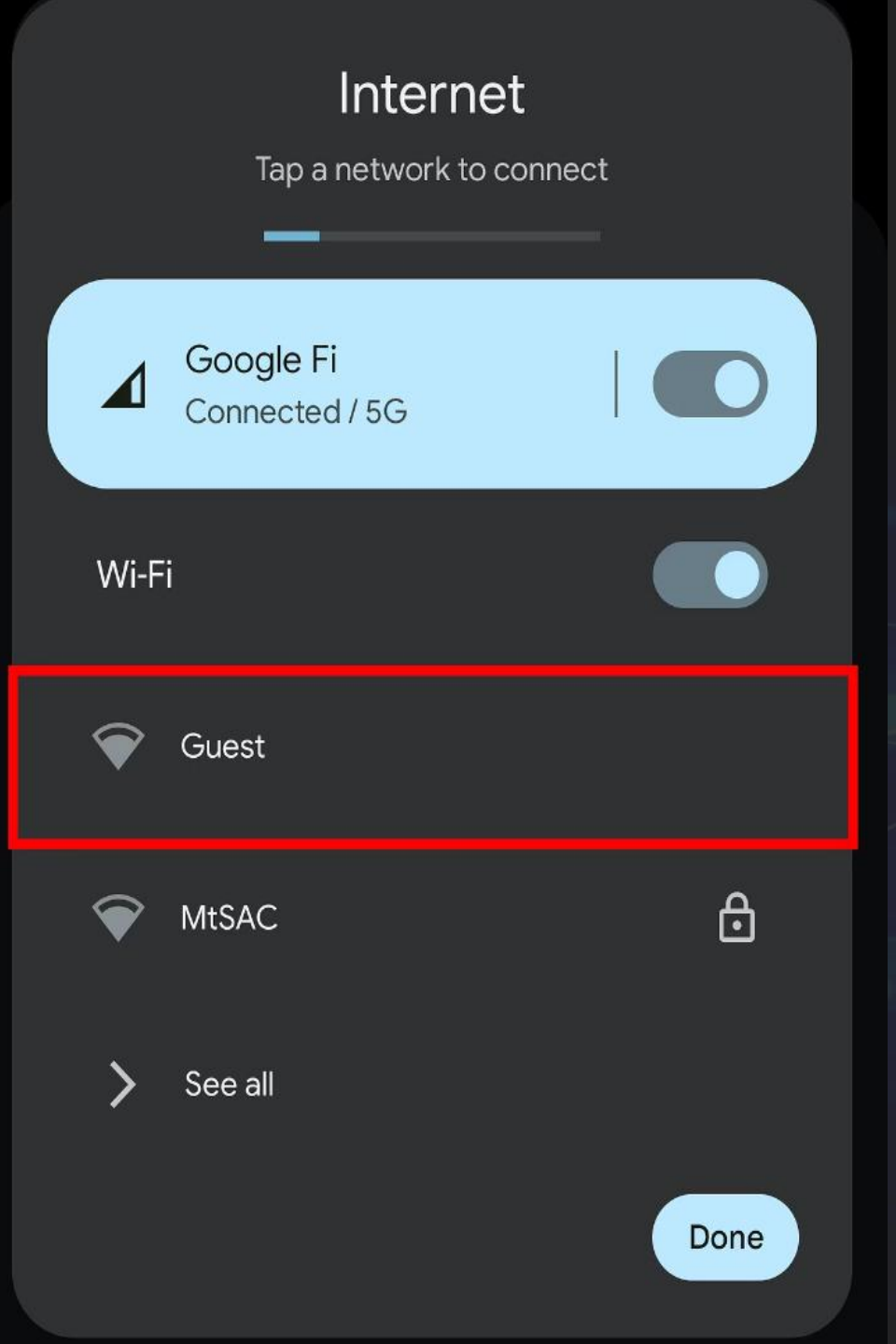
CCTV Cameras & ATMs

CCTV VLAN

Restricted access ensuring secure connection to recording servers.

ATM VLAN

Encrypted communications for PCI compliance and transaction safety.



Wireless (Guest-Only Access)

Network Isolation

Secures guest access separately from internal resources.

Captive Portal

Authentication gateway with terms of service acceptance.

Bandwidth Control

Limits guest bandwidth to prevent network abuse.


Security at the Access Layer

Security at the Access Layer

DHCP Snooping

Blocks rogue DHCP servers from assigning IP addresses.

Port Security

Blocks rogue DHCP servers from assigning IP addresses.

Dynamic ARP Inspection (DAI)

Prevents ARP spoofing and man-in-the-middle attacks.

CDP

Reduce CDP risks.

BPDU Guard

Stops unauthorized switches that create loops in the network.

DHCP Snooping

1

Unauthorized Blocking

Blocks rogue DHCP servers from issuing IP addresses.

2

Binding Table

Keeps track of legitimate IP address allocations.

BPDU Guard & Port Security

BPDU Guard

Prevents STP manipulation and network loops on edge ports.

Port Security

Restricts MAC address access with violation controls.

CDP (Cisco Discovery Protocol)

Understanding and Mitigating CDP Risks

Default CDP enablement exposes network topology to potential attackers.

Cisco Discovery Protocol shares device information at Layer 2.

Exposed information aids attackers in reconnaissance and targeted network attacks.

CDP (Cisco Discovery Protocol)

CDP Mitigation Strategies

Disable CDP

Stop device broadcasts using 'no cdp run' and 'no cdp enable' commands.

CDP Authentication

Encrypt and authenticate CDP messages to prevent spoofing and man-in-the-middle attacks.

CDP Monitoring

Use monitoring tools to detect abnormal CDP traffic and misconfigurations.

Access Control

Implement Role-Based Access Control to restrict device access and minimize attack surfaces.

DAI (Dynamic ARP Inspection):

Mitigating ARP Spoofing

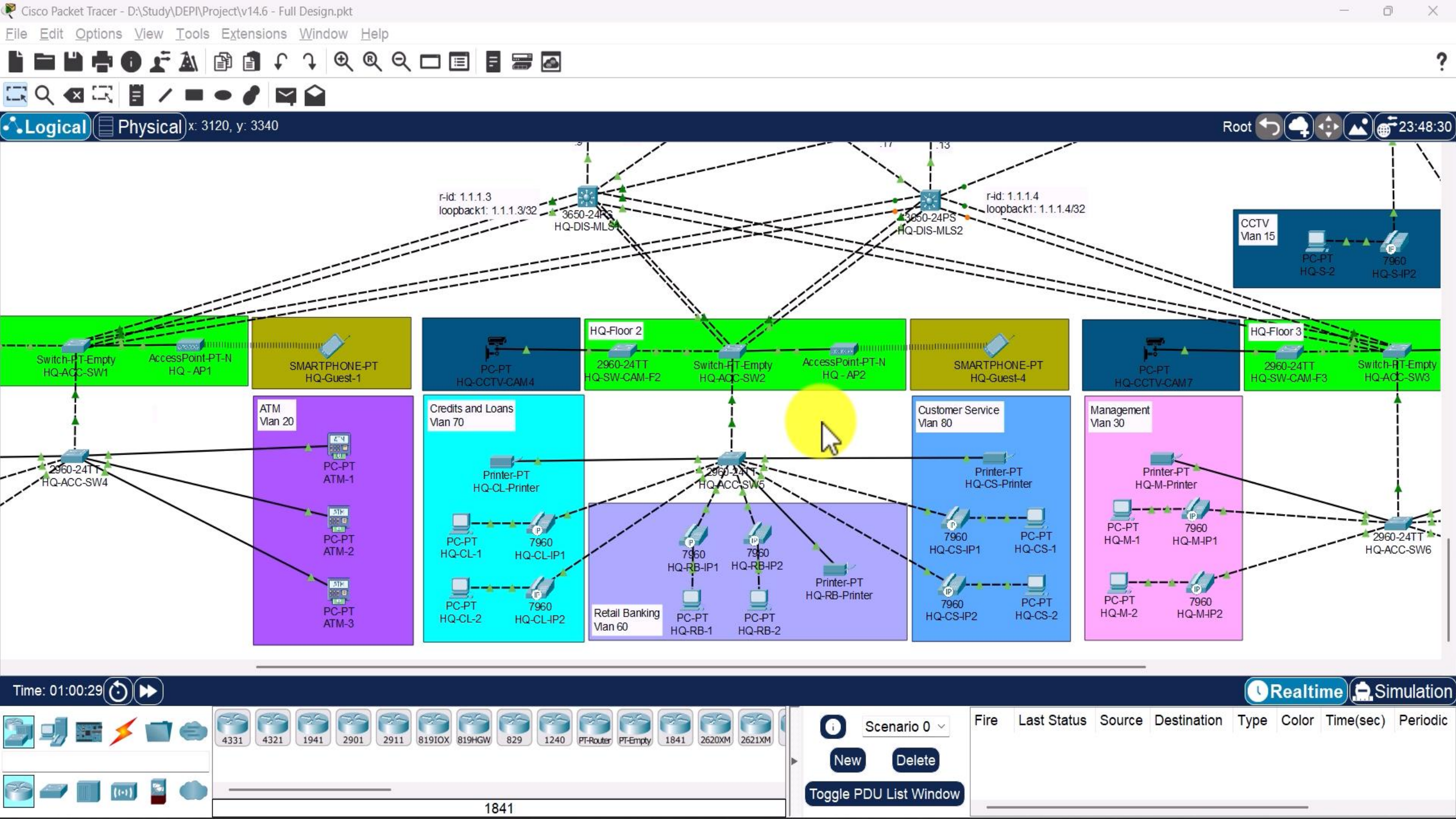
Packet Validation

Verifies ARP packets to block malicious attacks.

Binding Database

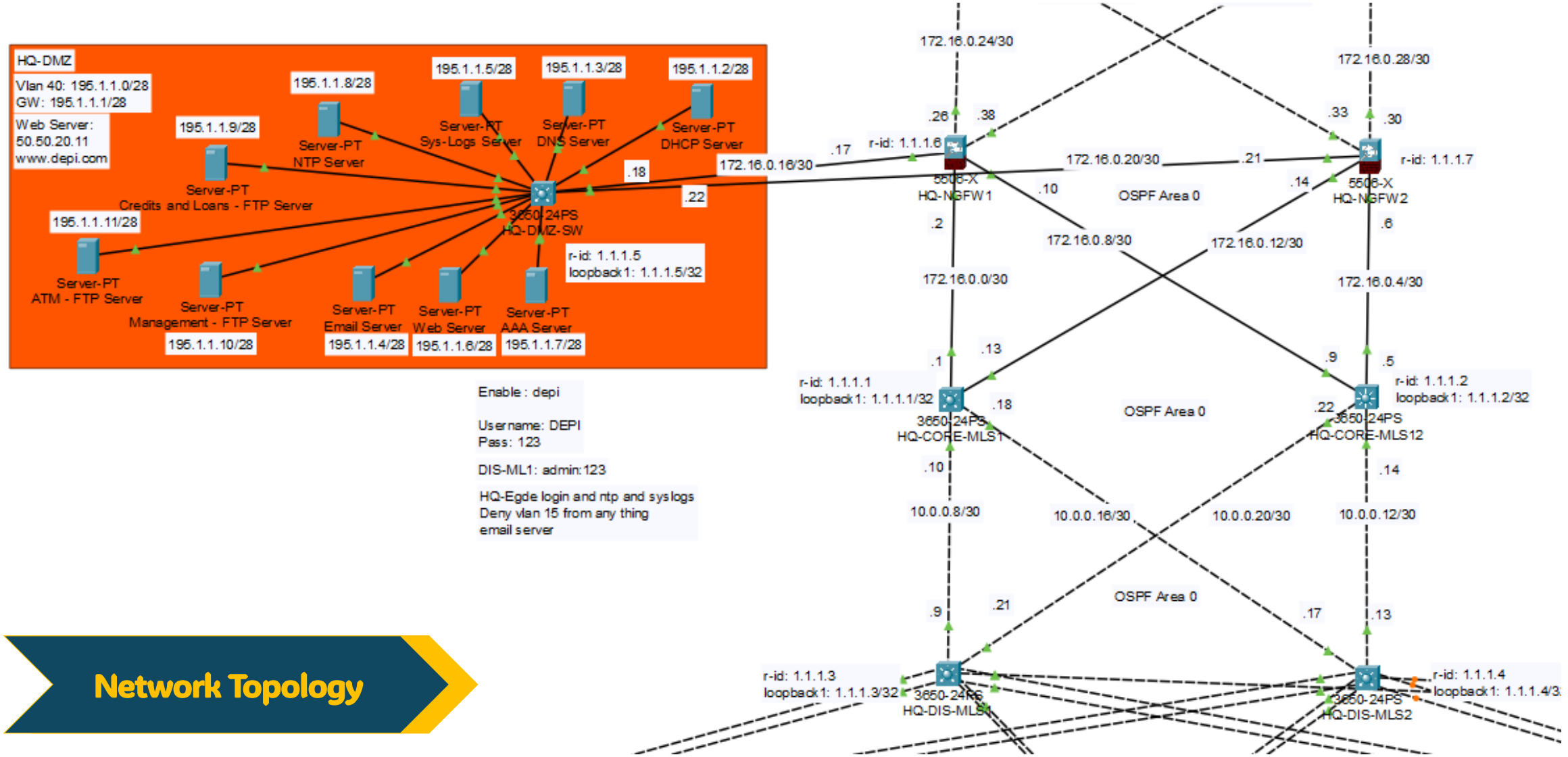
Relies on DHCP snooping data for precise ARP verification.

Explanatory video


Cisco Packet Tracer - D:\Study\DEPI\Project\v14.6 - Full Design.pkt
File Edit Options View Tools Extensions Window Help
Logical Physical x: 3120, y: 3340
Root 23:48:30
r-id: 1.1.1.3
loopback1: 1.1.1.3/32
3650-24PS
HQ-DIS-MLS1
r-id: 1.1.1.4
loopback1: 1.1.1.4/32
3650-24PS
HQ-DIS-MLS2
CCTV
Vlan 15
PC-PT
HQ-S-2
7960
HQ-S-IP2
Switch-PT-Empty
HQ-ACC-SW1
AccessPoint-PT-N
HQ - AP1
SMARTPHONE-PT
HQ-Guest-1
PC-PT
HQ-CCTV-CAM4
HQ-Floor 2
2960-24TT
HQ-SW-CAM-F2
Switch-PT-Empty
HQ-ACC-SW2
AccessPoint-PT-N
HQ - AP2
SMARTPHONE-PT
HQ-Guest-4
PC-PT
HQ-CCTV-CAM7
HQ-Floor 3
2960-24TT
HQ-SW-CAM-F3
Switch-PT-Empty
HQ-ACC-SW3
ATM
Vlan 20
PC-PT
ATM-1
PC-PT
ATM-2
PC-PT
ATM-3
Credits and Loans
Vlan 70
Printer-PT
HQ-CL-Printer
PC-PT
HQ-CL-1
7960
HQ-CL-IP1
PC-PT
HQ-CL-2
7960
HQ-CL-IP2
2960-24TT
HQ-ACC-SW4
2960-24TT
HQ-ACC-SW5
Retail Banking
Vlan 60
7960
HQ-RB-IP1
7960
HQ-RB-IP2
PC-PT
HQ-RB-1
PC-PT
HQ-RB-2
Printer-PT
HQ-RB-Printer
Customer Service
Vlan 80
Printer-PT
HQ-CS-Printer
7960
HQ-CS-IP1
PC-PT
HQ-CS-1
7960
HQ-CS-IP2
PC-PT
HQ-CS-2
Management
Vlan 30
Printer-PT
HQ-M-Printer
PC-PT
HQ-M-1
7960
HQ-M-IP1
PC-PT
HQ-M-2
7960
HQ-M-IP2
2960-24TT
HQ-ACC-SW6
Time: 01:00:29
Realtime
Simulation
4331
4321
1941
2901
2911
819IOX
819HGW
829
1240
PT-Router
PT-Empty
1841
2620XM
2621XM
1841
Scenario 0
New
Delete
Toggle PDU List Window
Fire
Last Status
Source
Destination
Type
Color
Time(sec)
Periodic

Aggregation

Topology → HSRP → Load Balance



Network Topology

HSRP Redundancy Overview

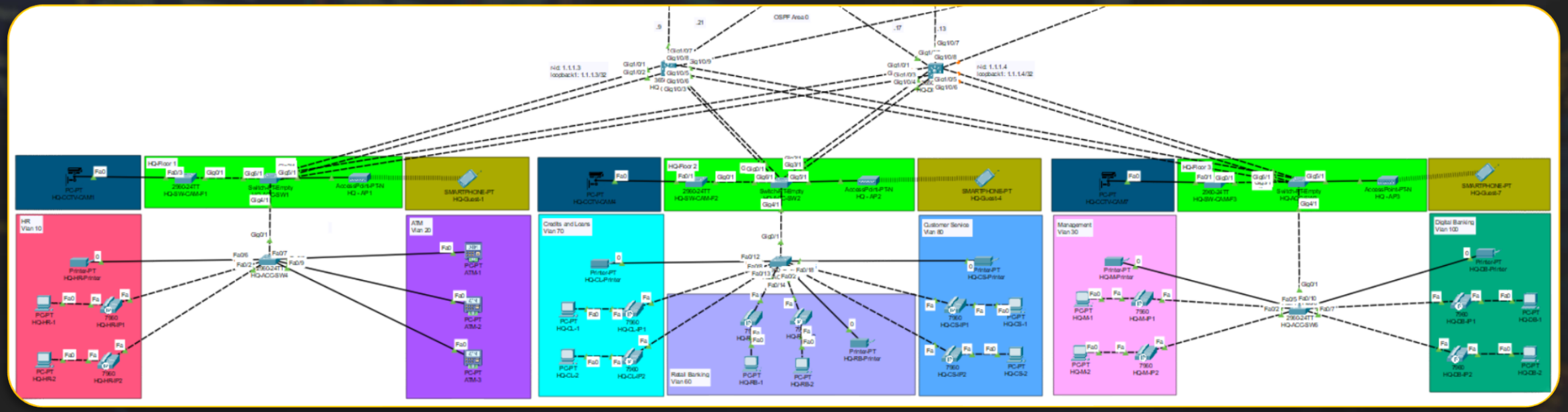
Gateway Availability

HSRP ensures continuous gateway access for critical VLANs, maintaining network reliability.

Active-Passive Setup

Reliable failover mechanisms prevent network service disruption by switching to standby devices.

HSRP Configuration Details



HSRP Peers

HQ-DIS-MLS1 and HQ-DIS-MLS2 serve as redundant gateways to maintain continuous network availability.

VLAN Assignments

VLANs 10–50 run on MLS1

VLANs 60–100 run on MLS2

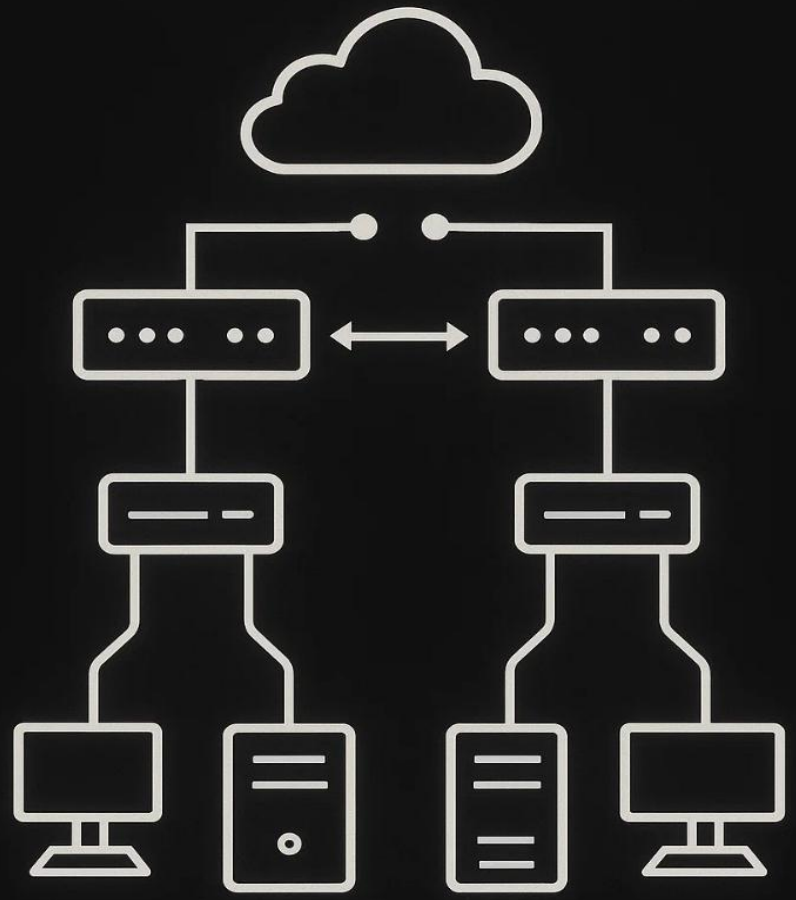
Effectively balancing load between peers.

Benefits of HSRP Redundancy

No delay
Instant failover during network issues.

Reliable
Network keeps working if something fails.

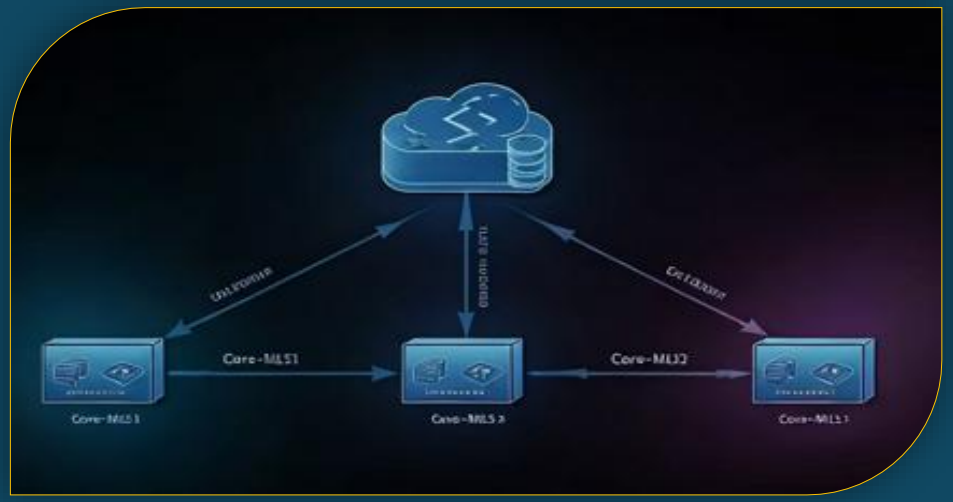
Less downtime
Systems stay online more consistently.



Load Balancing Strategy

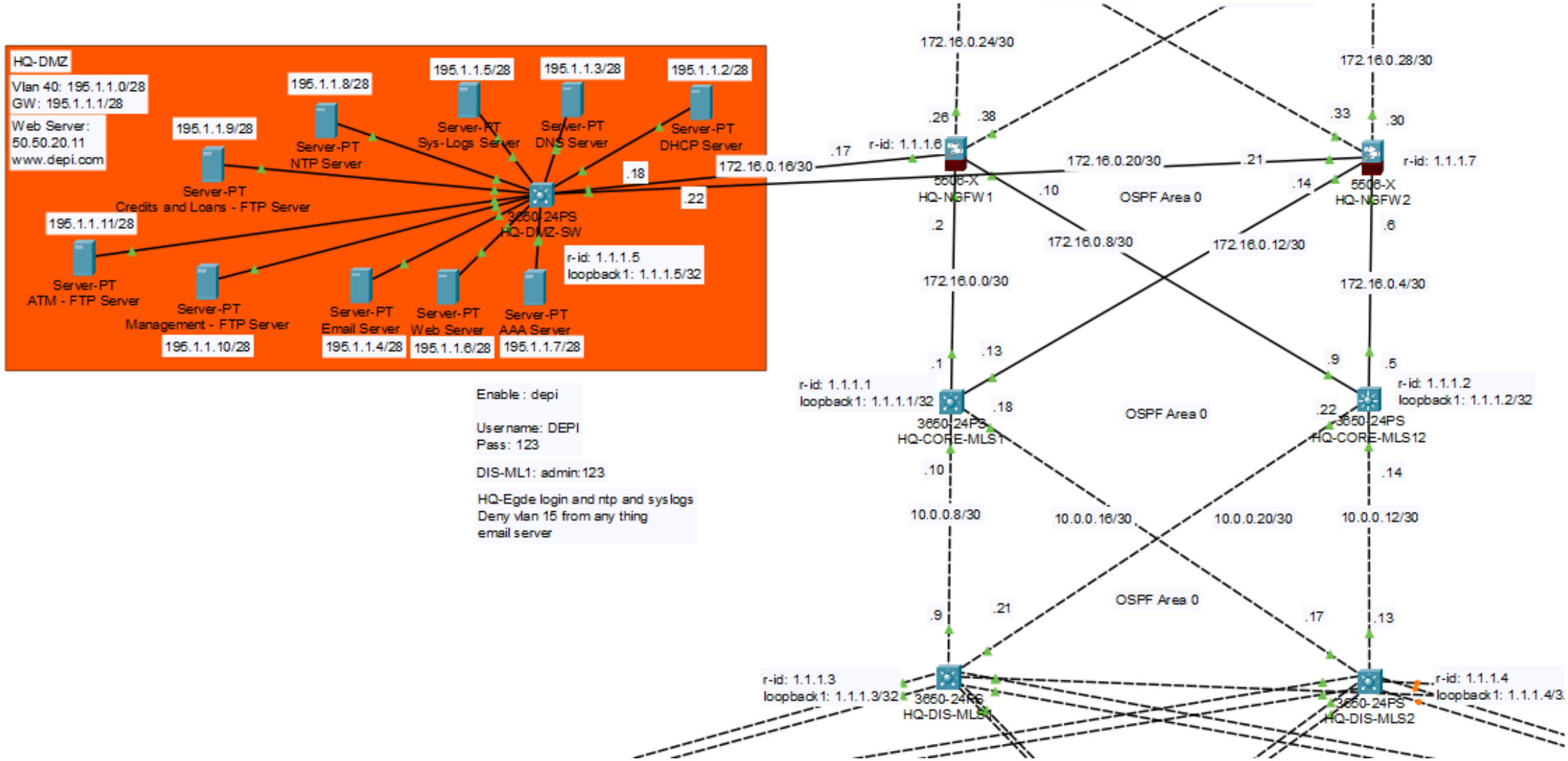
Traffic Distribution

Evenly divides outbound traffic
to prevent bottlenecks.

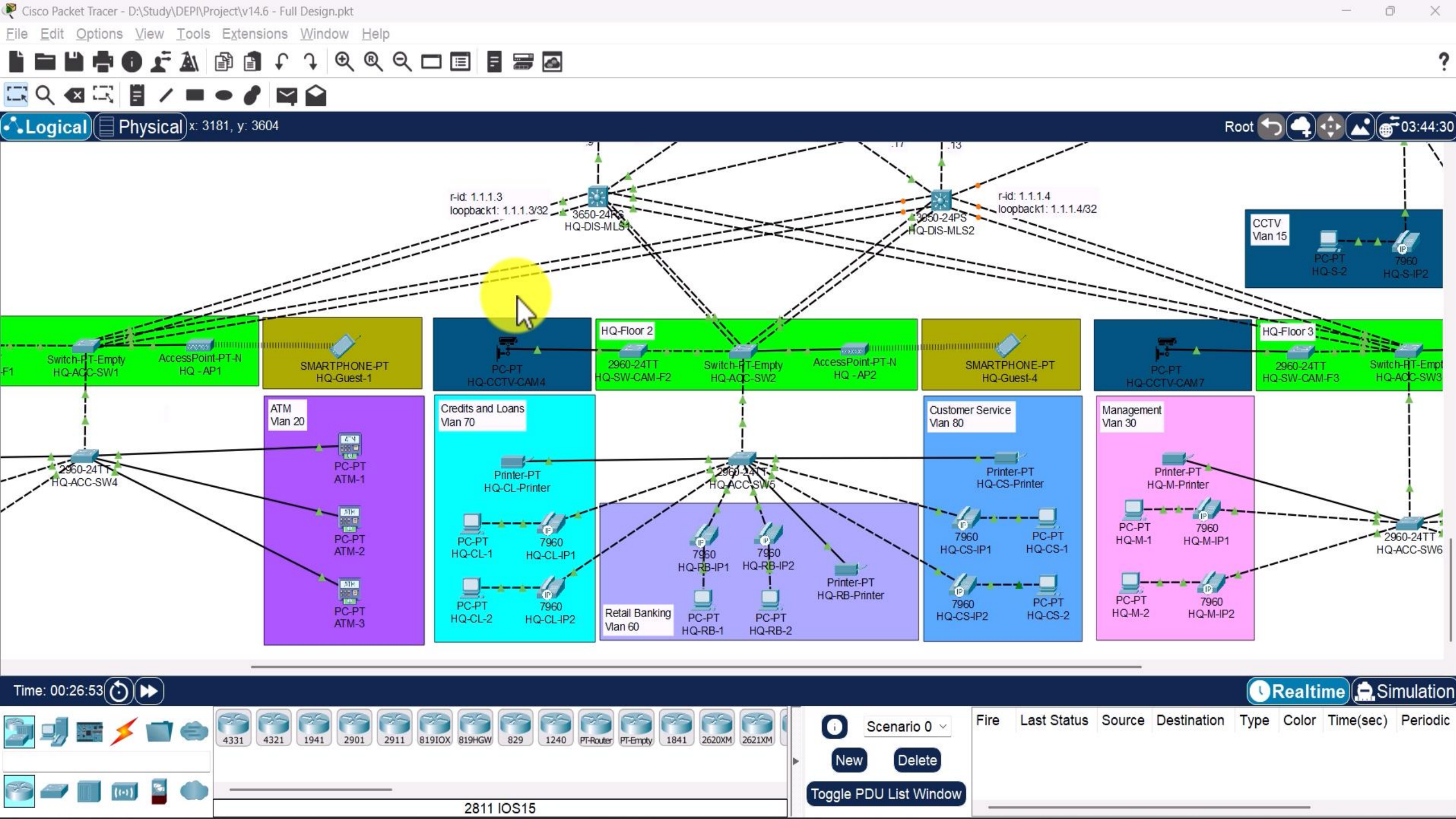


Authorized Traffic Only

MLS1 defaults to Core-MLS1
MLS2 defaults to Core-MLS2.

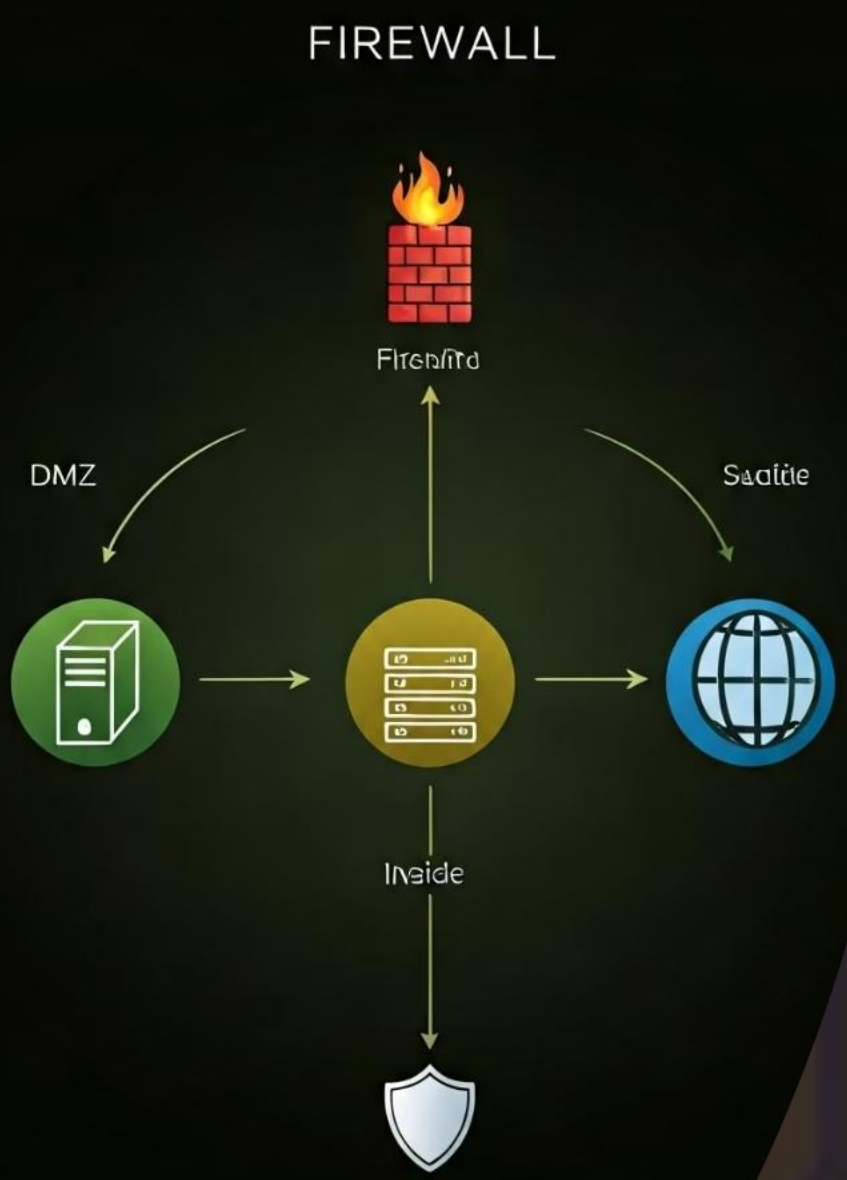

HQ-DMZ
Vlan 40: 195.1.1.0/28
GW: 195.1.1.1/28
Web Server:
50.50.20.11
www.depi.com
195.1.1.8/28
195.1.1.5/28
195.1.1.3/28
195.1.1.2/28
195.1.1.9/28
Server-PT
NTP Server
Server-PT
Sys-Logs Server
Server-PT
DNS Server
Server-PT
DHCP Server
Server-PT
Credits and Loans - FTP Server
195.1.1.11/28
3650-24PS
HQ-DMZ-SW
r-id: 1.1.1.5
loopback1: 1.1.1.5/32
Server-PT
ATM - FTP Server
Server-PT
Management - FTP Server
195.1.1.10/28
Server-PT
Email Server
195.1.1.4/28
Server-PT
Web Server
195.1.1.6/28
Server-PT
AAA Server
195.1.1.7/28
172.16.0.16/30
.17
.18
.22
Enable : depi
Username: DEPI
Pass: 123
DIS-ML1: admin:123
HQ-Egde login and ntp and syslogs
Deny vlan 15 from any thing
email server
172.16.0.24/30
172.16.0.28/30
.26
.38
.33
.30
r-id: 1.1.1.6
r-id: 1.1.1.7
172.16.0.20/30
.21
5506-X
HQ-NGFW1
.10
OSPF Area 0
.14
5506-X
HQ-NGFW2
.2
.6
172.16.0.8/30
172.16.0.12/30
172.16.0.0/30
172.16.0.4/30
.1
.13
.9
.5
r-id: 1.1.1.1
loopback1: 1.1.1.1/32
.18
OSPF Area 0
.22
r-id: 1.1.1.2
loopback1: 1.1.1.2/32
3650-24PS
HQ-CORE-MLS1
3650-24PS
HQ-CORE-MLS12
.10
.14
10.0.0.8/30
10.0.0.16/30
10.0.0.20/30
10.0.0.12/30
OSPF Area 0
.9
.21
.17
.13
r-id: 1.1.1.3
loopback1: 1.1.1.3/32
3650-24PS
HQ-DIS-MLS1
r-id: 1.1.1.4
loopback1: 1.1.1.4/3
3650-24PS
HQ-DIS-MLS2

Explanatory video


Cisco Packet Tracer - D:\Study\DEPI\Project\v14.6 - Full Design.pkt
File Edit Options View Tools Extensions Window Help
Logical Physical x: 3181, y: 3604
Root 03:44:30
r-id: 1.1.1.3
loopback1: 1.1.1.3/32
3650-24PS
HQ-DIS-MLS1
r-id: 1.1.1.4
loopback1: 1.1.1.4/32
3650-24PS
HQ-DIS-MLS2
CCTV
Vlan 15
PC-PT
HQ-S-2
7960
HQ-S-IP2
Switch-PT-Empty
HQ-ACC-SW1
AccessPoint-PT-N
HQ -AP1
SMARTPHONE-PT
HQ-Guest-1
PC-PT
HQ-CCTV-CAM4
HQ-Floor 2
2960-24TT
HQ-SW-CAM-F2
Switch-PT-Empty
HQ-ACC-SW2
AccessPoint-PT-N
HQ -AP2
SMARTPHONE-PT
HQ-Guest-4
PC-PT
HQ-CCTV-CAM7
HQ-Floor 3
2960-24TT
HQ-SW-CAM-F3
Switch-PT-Empt
HQ-ACC-SW3
ATM
Vlan 20
PC-PT
ATM-1
PC-PT
ATM-2
PC-PT
ATM-3
Credits and Loans
Vlan 70
Printer-PT
HQ-CL-Printer
PC-PT
HQ-CL-1
7960
HQ-CL-IP1
PC-PT
HQ-CL-2
7960
HQ-CL-IP2
2960-24TT
HQ-ACC-SW4
2960-24TT
HQ-ACC-SW5
7960
HQ-RB-IP1
7960
HQ-RB-IP2
Printer-PT
HQ-RB-Printer
Retail Banking
Vlan 60
PC-PT
HQ-RB-1
PC-PT
HQ-RB-2
Customer Service
Vlan 80
Printer-PT
HQ-CS-Printer
7960
HQ-CS-IP1
PC-PT
HQ-CS-1
7960
HQ-CS-IP2
PC-PT
HQ-CS-2
Management
Vlan 30
Printer-PT
HQ-M-Printer
PC-PT
HQ-M-1
7960
HQ-M-IP1
PC-PT
HQ-M-2
7960
HQ-M-IP2
2960-24TT
HQ-ACC-SW6
Time: 00:26:53
Realtime
Simulation
4331
4321
1941
2901
2911
819IOX
819HGW
829
1240
PT-Router
PT-Empty
1841
2620XM
2621XM
2811 IOS15
Scenario 0
New
Delete
Toggle PDU List Window
Fire
Last Status
Source
Destination
Type
Color
Time(sec)
Periodic

Firewall

- Zoning
- Polices
- Least-Privilege
- DMZ to Inside
- DMZ Isolation
- Internet Access
- OSPF Routing



Firewall Zoning and Proxy ARP

Three Firewall Zones

DMZ, Inside, and Outside segregate network traffic for security.

Proxy ARP Enabled

Enhances security by controlling address resolution within zones.

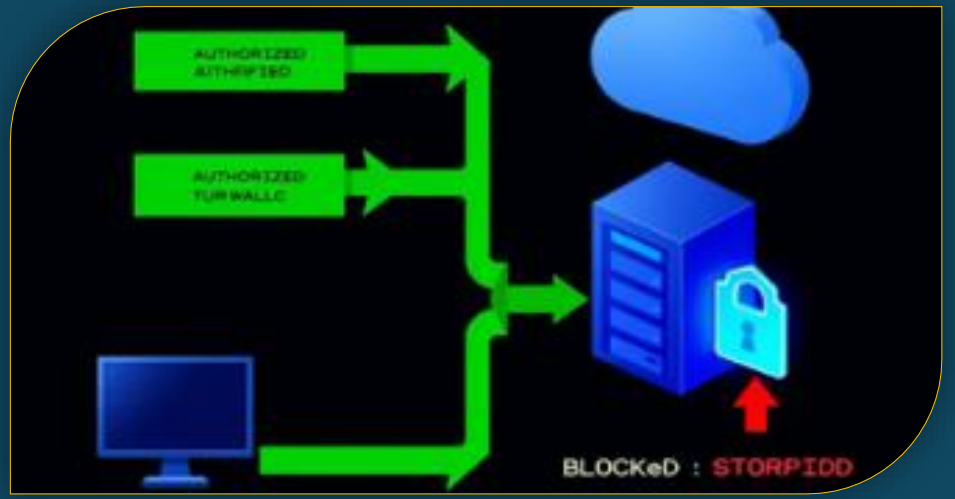
Branch-specific Firewalls

Each branch operates its own firewall for tailored protection.

Firewall Security Polices

Access Control

Strict rules govern traffic moving among DMZ, Inside, and Outside zones.



Authorized Traffic Only

Only essential services and approved directions are allowed per security requirements.

VLAN Access Policies

CCTV/ATM VLAN

Fully isolated network with no internet access, limited to local access for maintenance only.

Guest VLAN

Provides full internet access while blocking internal resources, with bandwidth capped at 10 Mbps per device.

Employee VLAN

Internet access based on job role, blocking YouTube and social media with enforced content filtering and app control.

Controlling DMZ to Inside Network Traffic

DMZ to Inside Link

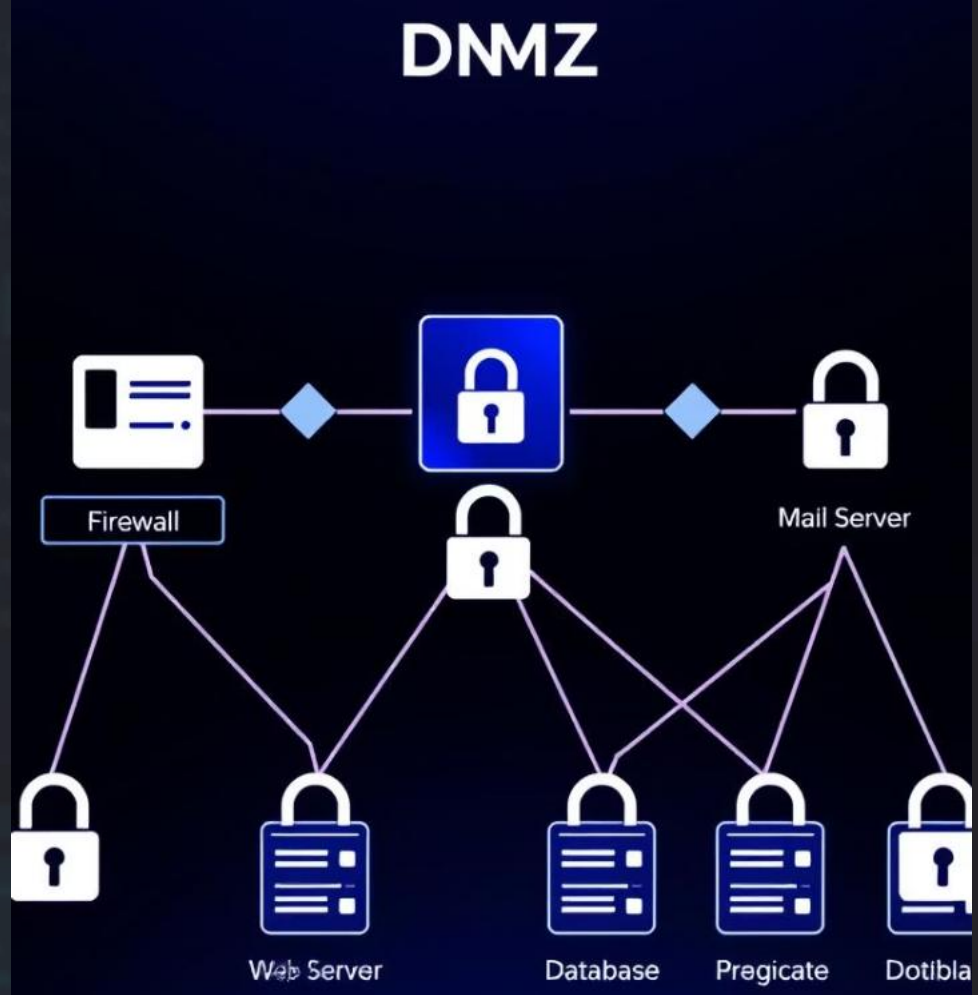
Firewall tightly controls data moving into the internal network.

Enhanced Security

Prevents lateral movement and unauthorized access within the network.

Controlled Access

Only approved traffic flows between DMZ and Inside zones.



Isolation Between DMZ and Outside Network

1

DMZ to Outside

The firewall restricts traffic flows to safeguard internal resources.

2

Secure Isolation

Effectively keeps external threats away from both internal and DMZ segments.

3

External Resource Control

Manages secure access to and from external services.

Routing and Internet Access

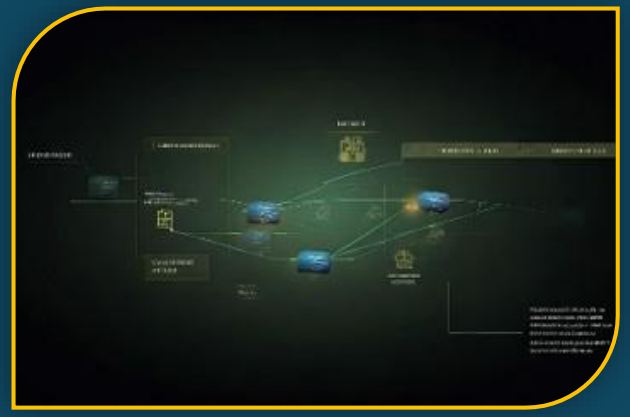
Default Route Propagation

Firewall shares default route with the Edge Router to direct internet traffic efficiently.

Ensures Seamless Connectivity

Maintains consistent and secure access to internet resources across the network.

Integrating OSPF Routing



OSPF Configuration

Enables dynamic routing between the LAN and Edge Router.

Secure Internet Access

Firewall manages routes securely for outbound connectivity.

Improved Efficiency

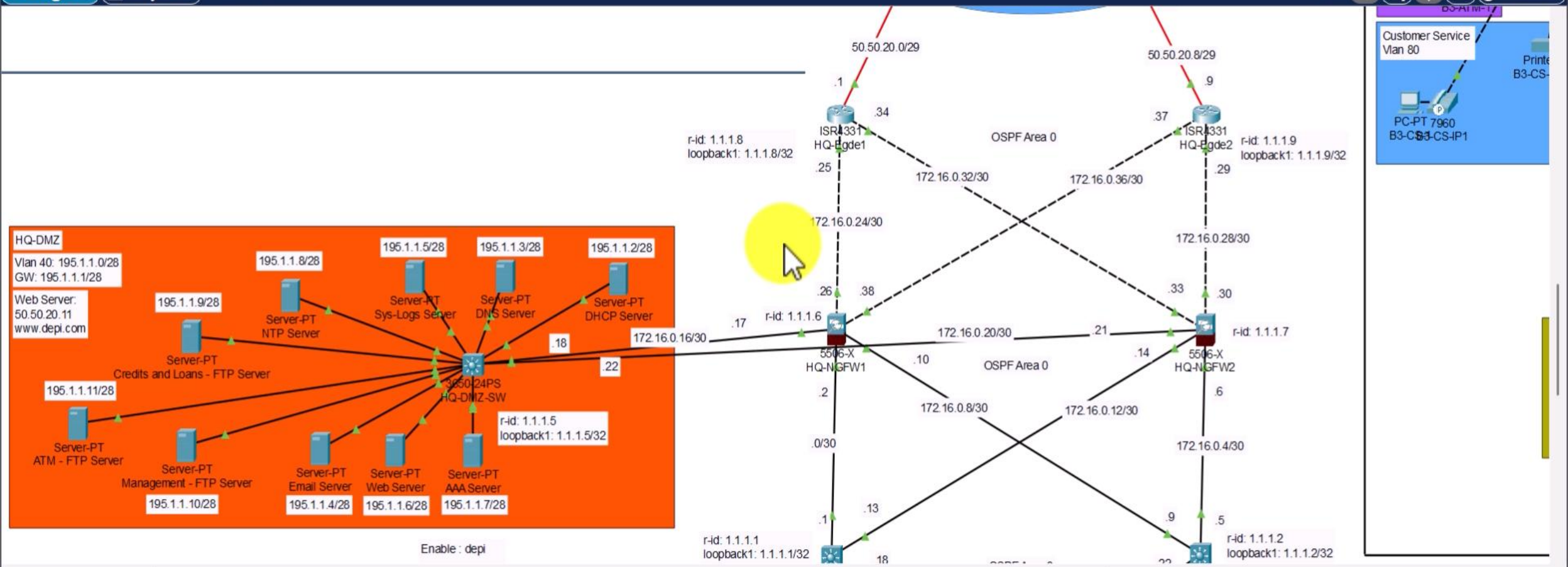
Dynamic routes adapt to network changes and maintain connectivity.

Explanatory video

Cisco Packet Tracer - D:\Study\DEPI\Project\v16.2 - Full Design.pkt

File Edit Options View Tools Extensions Window Help

Logical Physical x: 1631, y: 2640 Root 03:28:30



Time: 00:35:47 Realtime Simulation

4331 4321 1941 2901 2911 819IOX 819HGW 829 1240 PT-Router PT-Empty 1841 2620XM 2621XM

829

Scenario 0

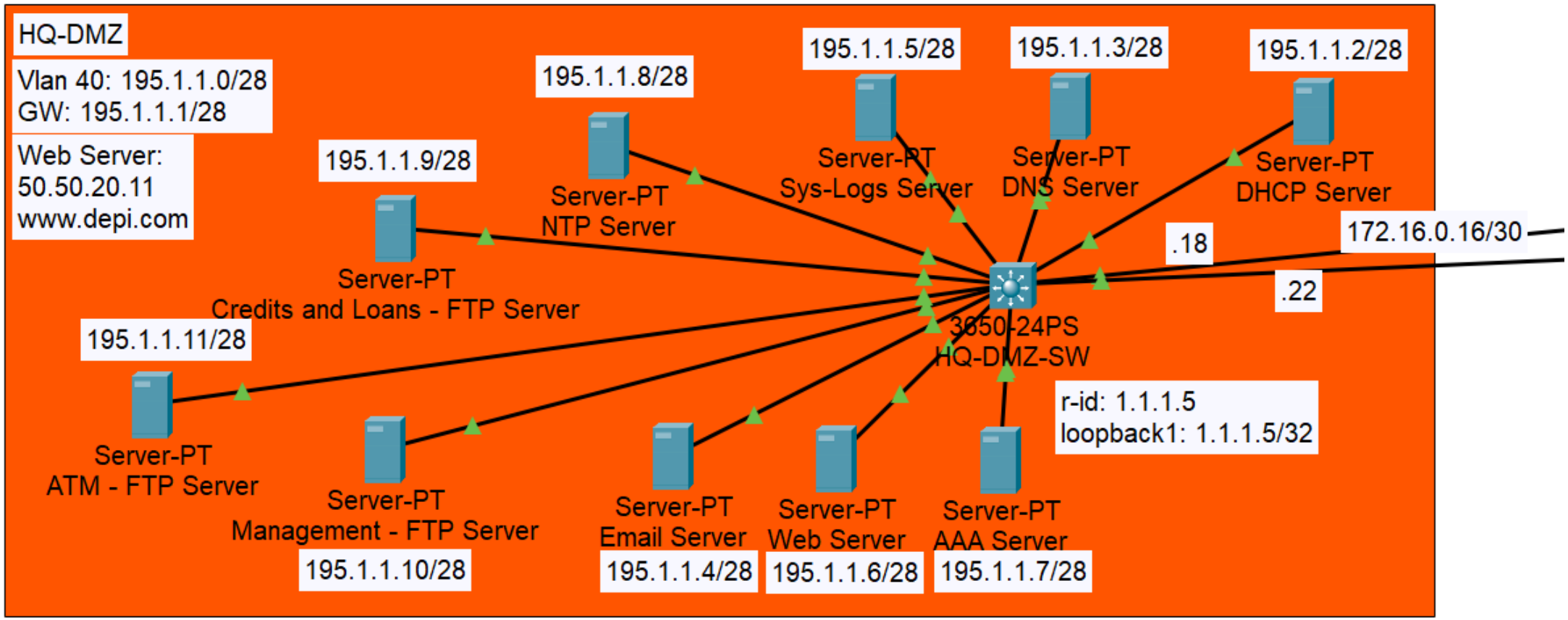
New Delete

Toggle PDU List Window

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic


DMZ
Demilitarized Zone

Network Topology



Servers In the DMZ

Web Server

Hosts corporate websites, securely handling web traffic within the DMZ.

Email Server

Manages and filters all inbound and outbound company emails.

DHCP Server

Dynamically assigns IP addresses to devices in the network.

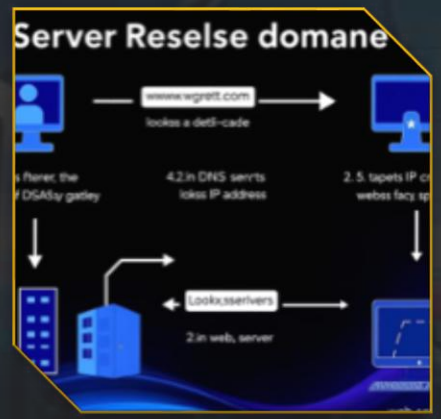
NTP Server

Ensures accurate timestamps by synchronizing device time.

Servers In the DMZ

DNS Server

Provides domain name resolution and IP leasing for DMZ clients.

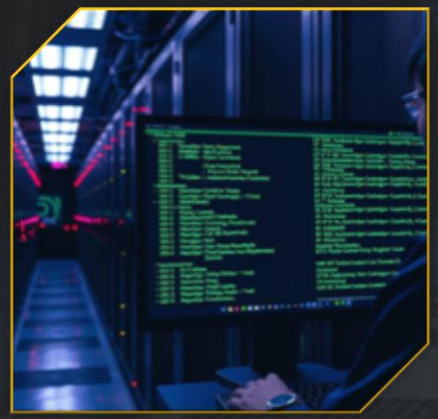


AAA Server

Handles authentication, time sync, and centralized logging functions.

Sys-logs Server

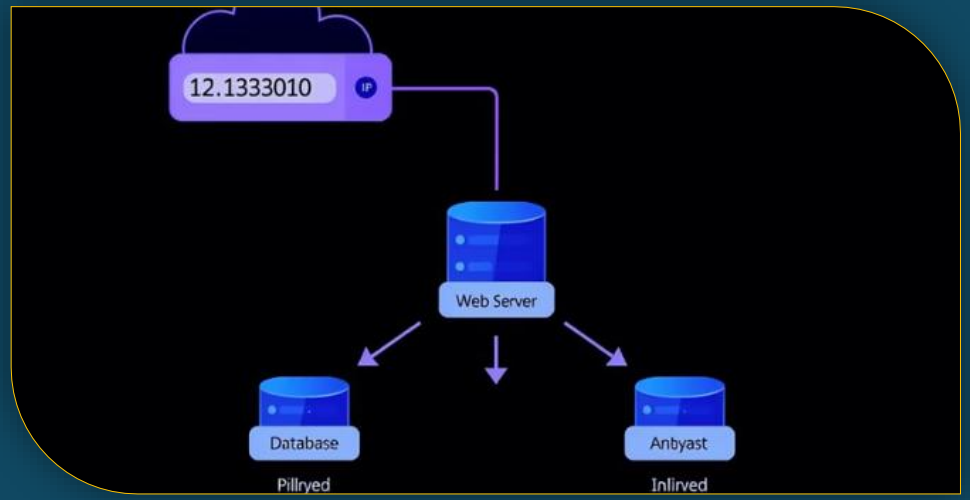
Collects system logs for monitoring security and operations.



FTP Server

Facilitates secure file transfers within the network.

Static NAT



Public-Private IP Mapping

Public IP **50.50.20.3** is mapped to internal DMZ server **195.1.1.6**.

External Access Enabled

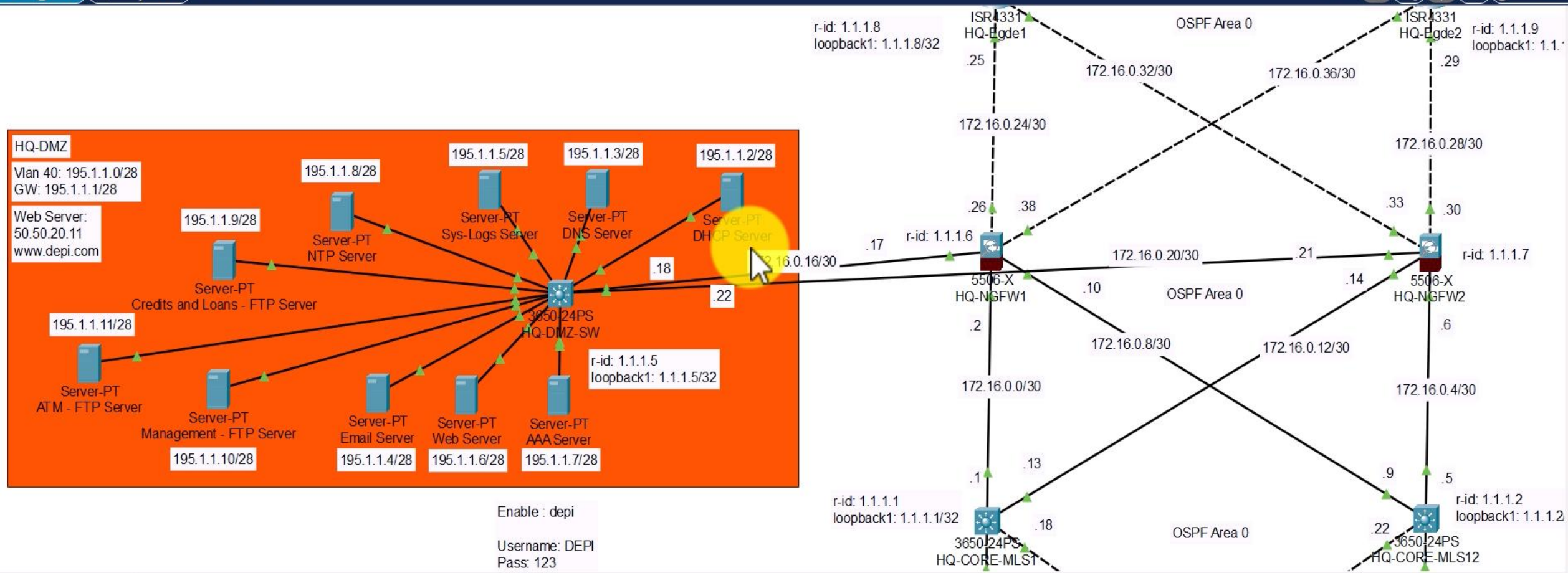
Clients outside the network securely reach the DMZ server.

Explanatory video

Cisco Packet Tracer - D:\Study\DEPI\Project\v14.7 - Full Design.pkt

File Edit Options View Tools Extensions Window Help

Logical Physical x: 1387, y: 2481 Root 13:35:00



Enable : depi

Username: DEPI
Pass: 123

Time: 00:19:07 Realtime Simulation

PC Laptop Server Meraki Server Network Controller Printer IP Phone VoIP Device Phone TV Tablet Smart Phone Generic Wireless Generic Wired

Fiber

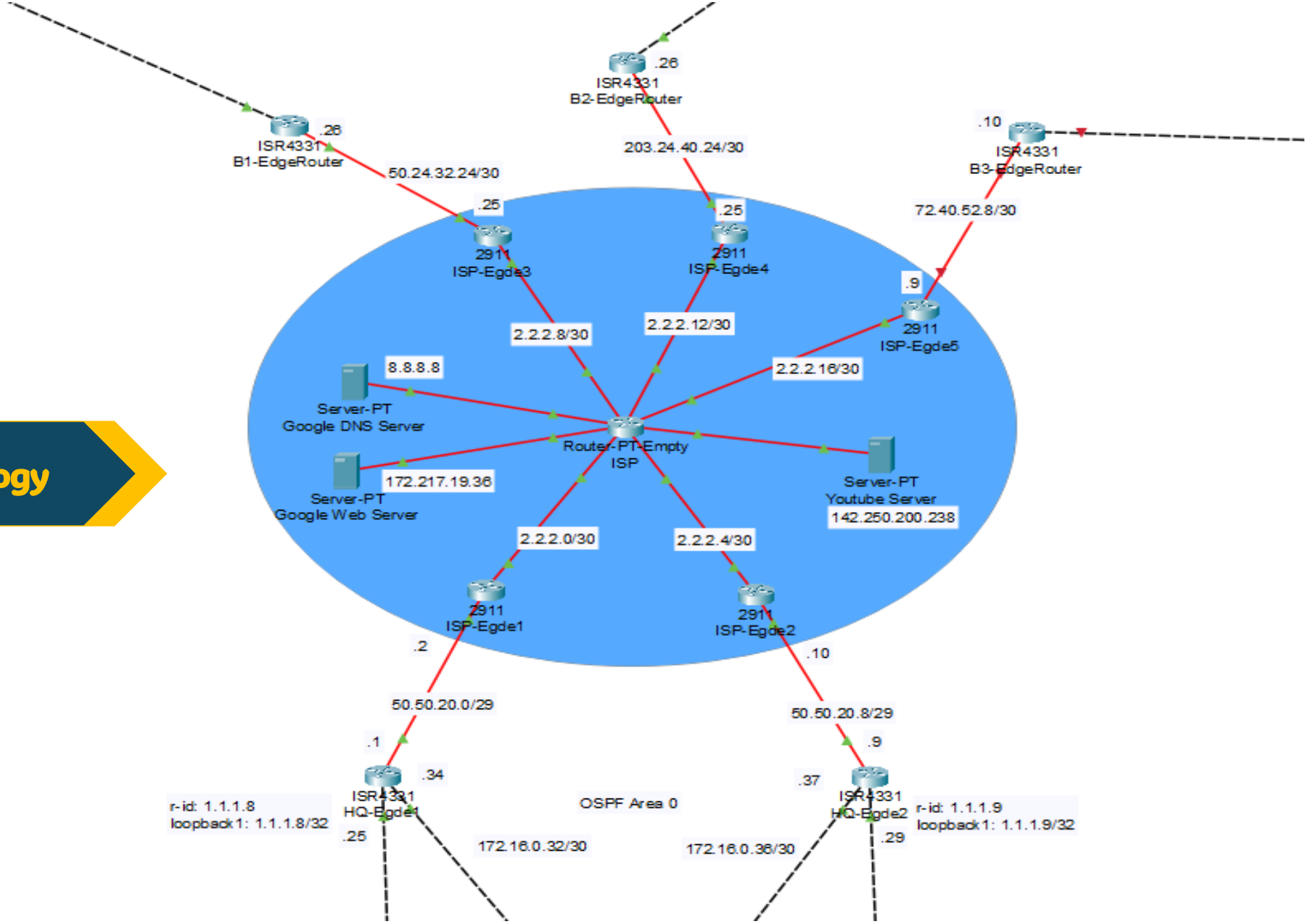
Scenario 0 New Delete Toggle PDU List Window

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic

ISP & VPN

Topology → Connection → OSPF → Security → IPSec

Network Topology



ISP Network Connections

Branch Connectivity

Each branch is linked through the ISP with a fixed gateway.

Reliable Network

ISP infrastructure ensures seamless communication across branches.

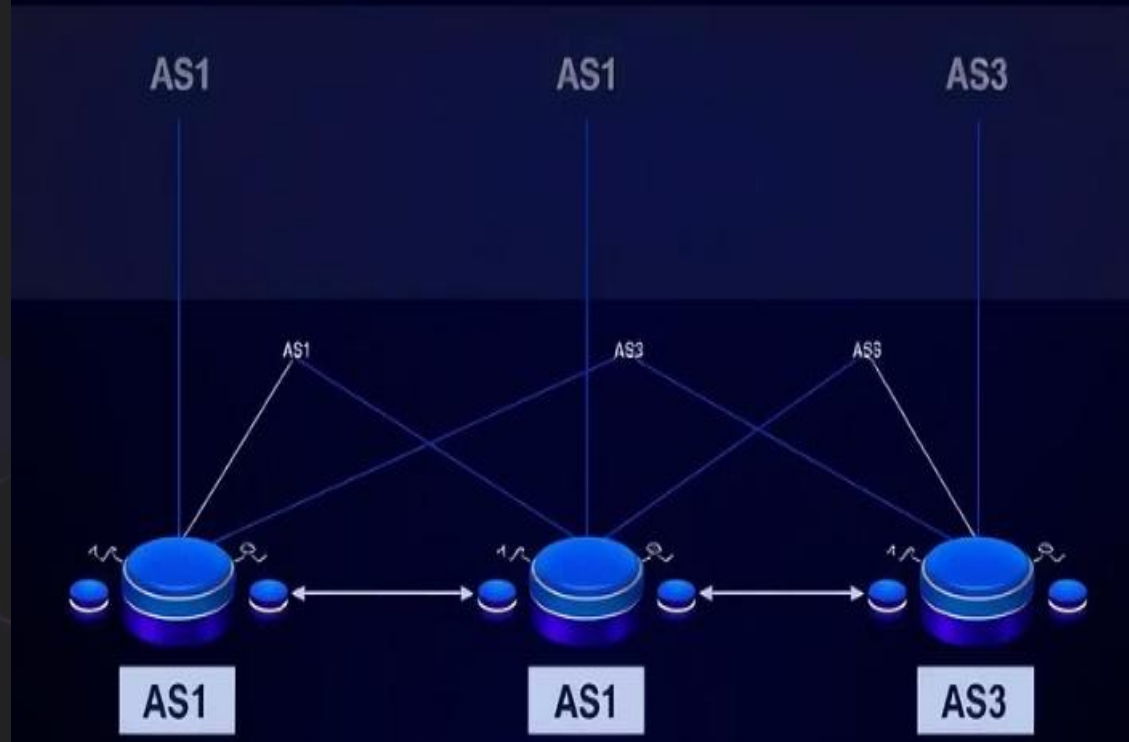
OSPF Routing Enabled

Autonomous System

OSPF runs within the ISP’s autonomous system controlling the routing

Efficient Data Flow

Routing protocols optimize data transmission across the ISP network



OSPF Security Features

OSPF Authentication

Secures routing updates, blocking unauthorized routers from joining.

Passive Interface

Blocks harmful clients by disabling routing updates on specified interfaces.

VPN Setup with IPSec

Branch-to-HQ Security

Branches connect securely only to the main HQ.

Restricted Communication

Branches cannot communicate directly with each other.

Data Encryption

Critical data and shared servers are encrypted for safety.

IPSec VPN Data Protection

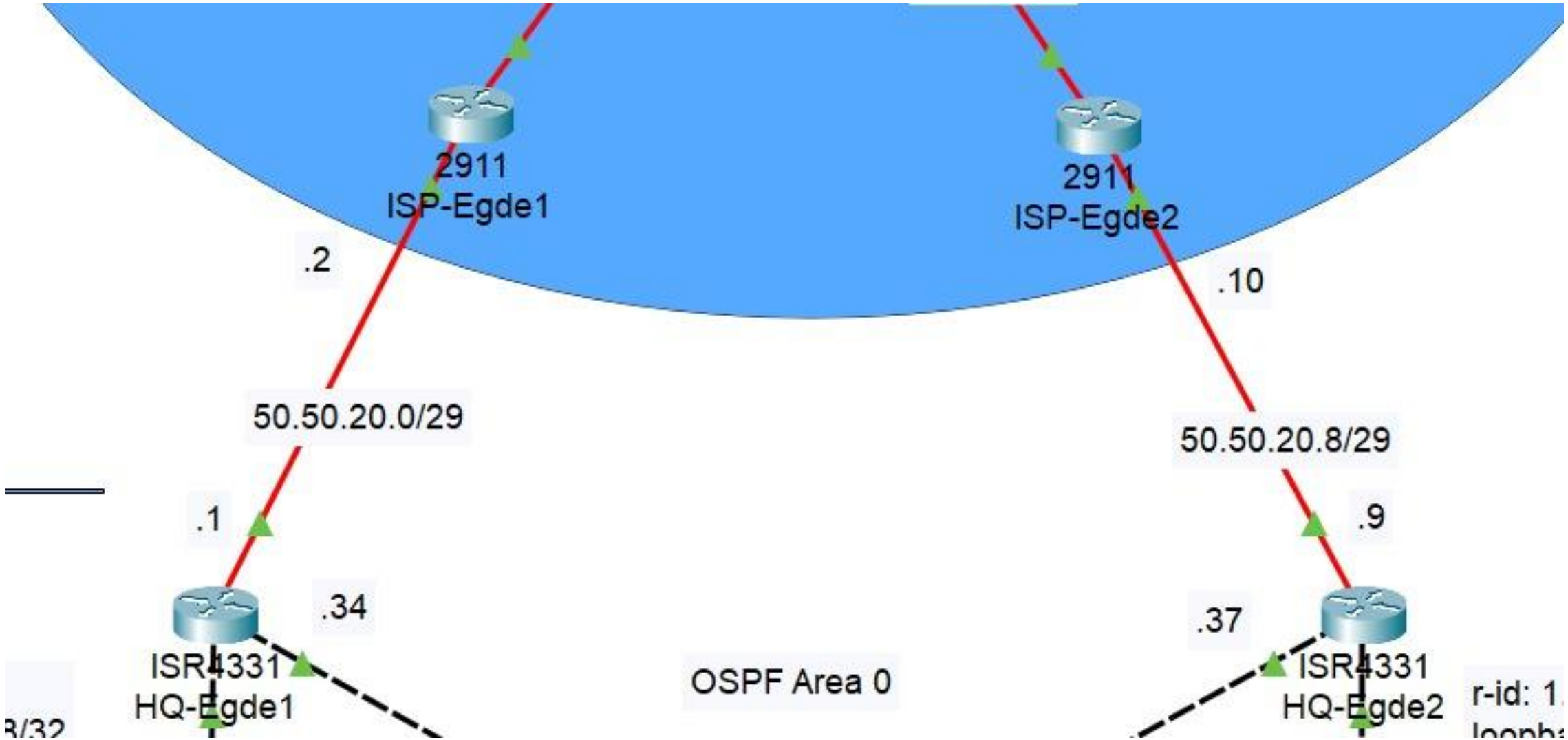
Secure Communication

Ensuring safe data exchange between HQ and branch offices

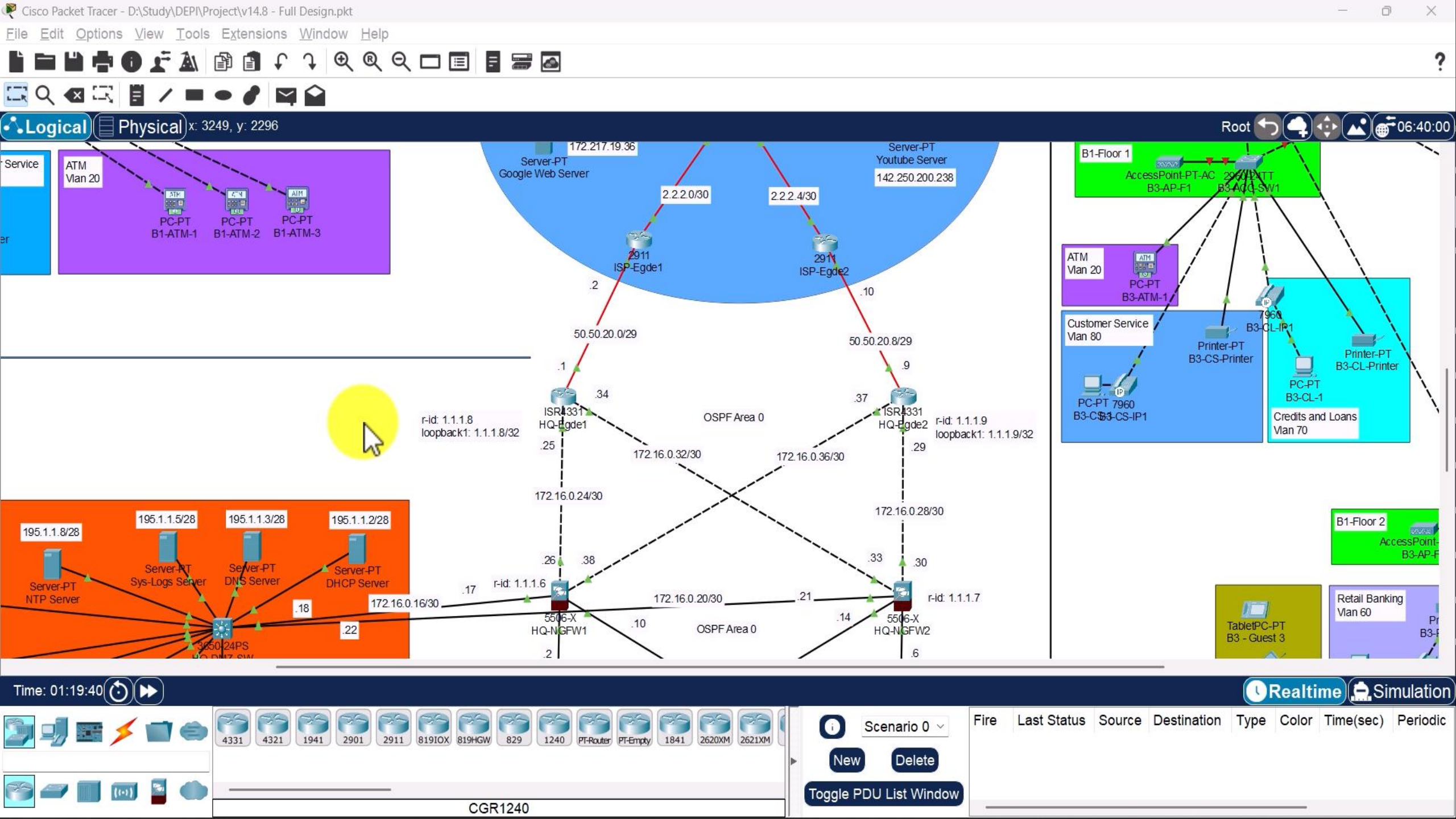
Data Encryption

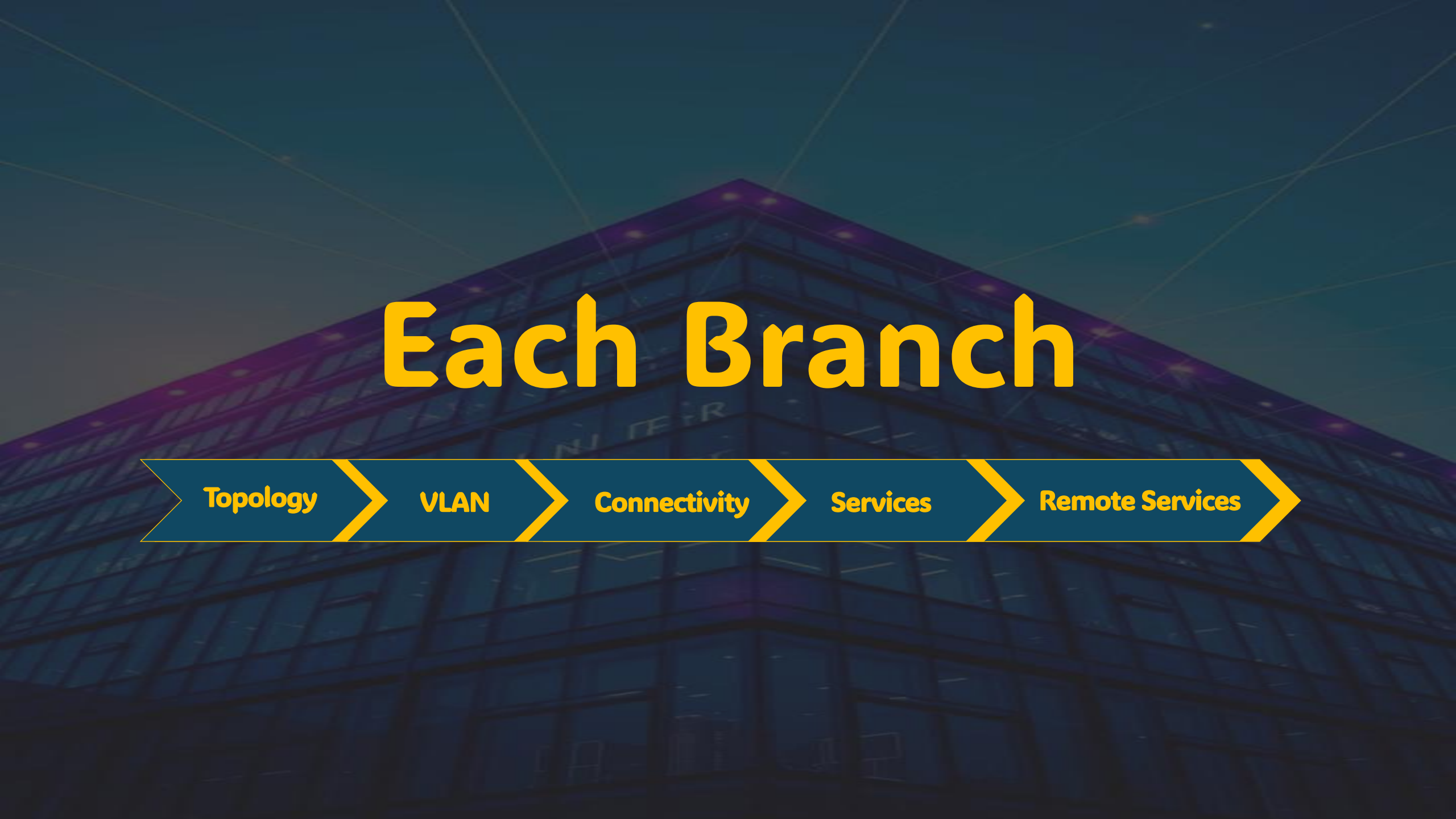
Protecting confidentiality and integrity of network data

Network Topology

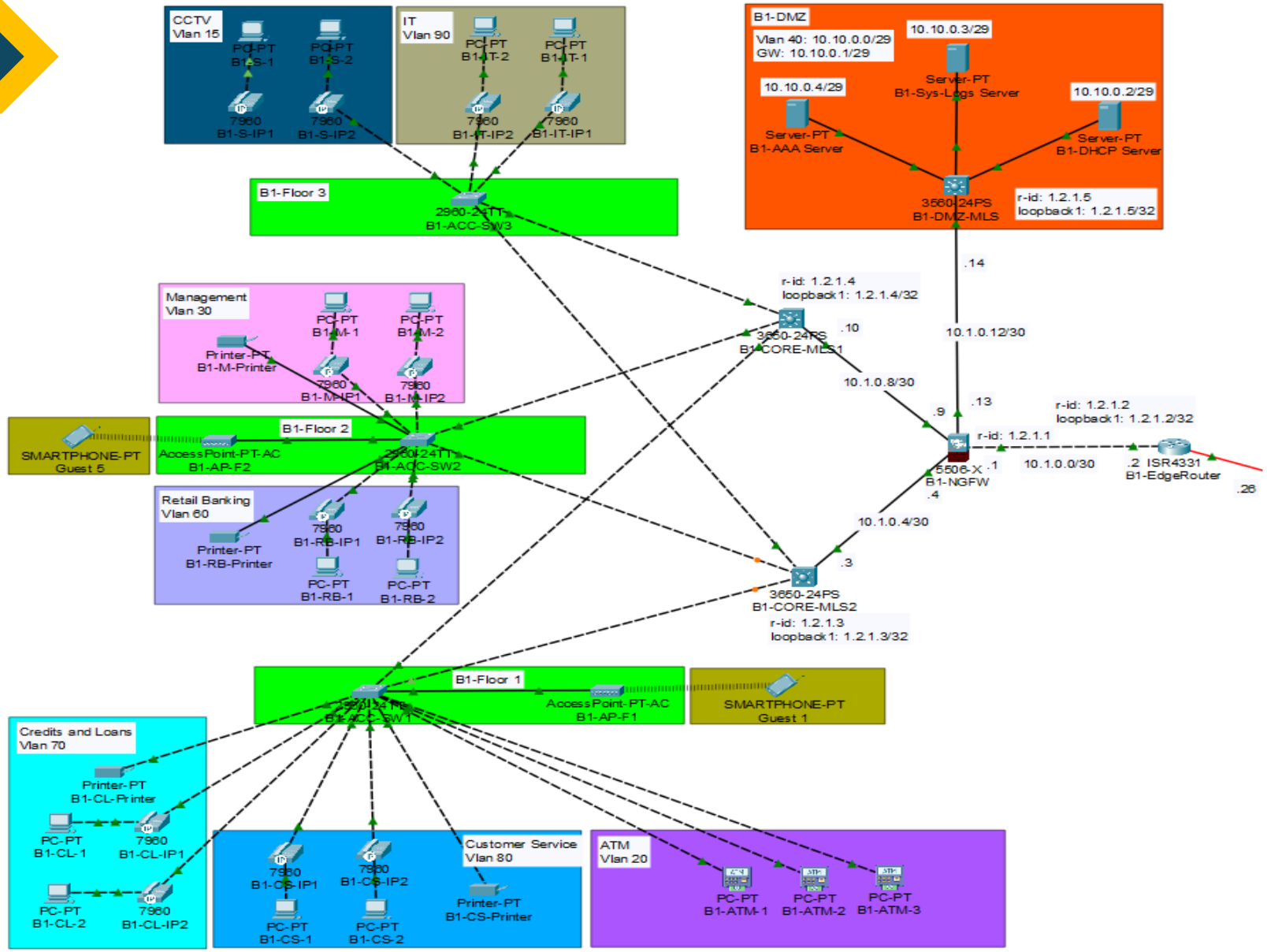


Explanatory video


Cisco Packet Tracer - D:\Study\DEPI\Project\v14.8 - Full Design.pkt
File Edit Options View Tools Extensions Window Help
Logical
Physical
x: 3249, y: 2296
Root
06:40:00
ATM Vlan 20
PC-PT B1-ATM-1
PC-PT B1-ATM-2
PC-PT B1-ATM-3
Server-PT Google Web Server
172.217.19.36
Server-PT Youtube Server
142.250.200.238
2.2.2.0/30
2.2.2.4/30
2911 ISP-Egde1
2911 ISP-Egde2
.2
.10
50.50.20.0/29
50.50.20.8/29
.1
.9
.34
.37
ISR4331 HQ-Egde1
ISR4331 HQ-Egde2
r-id: 1.1.1.8
loopback1: 1.1.1.8/32
r-id: 1.1.1.9
loopback1: 1.1.1.9/32
OSPF Area 0
.25
.29
172.16.0.32/30
172.16.0.36/30
172.16.0.24/30
172.16.0.28/30
195.1.1.8/28
195.1.1.5/28
195.1.1.3/28
195.1.1.2/28
Server-PT NTP Server
Server-PT Sys-Logs Server
Server-PT DNS Server
Server-PT DHCP Server
.26
.38
.33
.30
.17
.18
.22
172.16.0.16/30
r-id: 1.1.1.6
172.16.0.20/30
.21
.14
r-id: 1.1.1.7
5506-X HQ-NGFW1
5506-X HQ-NGFW2
.10
OSPF Area 0
.2
.6
B1-Floor 1
AccessPoint-PT-AC B3-AP-F1
2960-24TT B3-ACC-SW1
ATM Vlan 20
PC-PT B3-ATM-1
7960 B3-CL-IP1
Customer Service Vlan 80
Printer-PT B3-CS-Printer
Printer-PT B3-CL-Printer
PC-PT B3-CL-1
PC-PT 7960 B3-CS-IP1
Credits and Loans Vlan 70
B1-Floor 2
TabletPC-PT B3 - Guest 3
Retail Banking Vlan 60
Time: 01:19:40
Realtime
Simulation
4331
4321
1941
2901
2911
819IOX
819HGW
829
1240
PT-Router
PT-Empty
1841
2620XM
2621XM
CGR1240
Scenario 0
New
Delete
Toggle PDU List Window
Fire
Last Status
Source
Destination
Type
Color
Time(sec)
Periodic


Each Branch
Topology
VLAN
Connectivity
Services
Remote Services

Network Topology



VLAN Allocation Details

HR

CCTV

ATM

Voice

Guest

IT

Management

Customer Service

Retail Banking

Credits And Loans

Branch Connectivity

Site-to-Site VPN

Encrypted connections securely link branches to headquarters.

Redundancy

Backup ISP links ensure minimal downtime and high reliability.

Bandwidth Allocation

Priority bandwidth during peak times for critical applications like VoIP.

VLAN Allocation Details

VPN Tunnels

Sales laptops establish secure connections to headquarters through encrypted VPN tunnels.

Access Control List

Access Control Lists restrict guest networks from accessing sensitive financial servers.

Routing

OSPF protocol dynamically reroutes traffic to maintain connectivity after link failures.

Local Branch Services

DHCP Server

Automatically assigns IP addresses and network settings to devices, reducing manual errors.

AAA Server

Manages authentication protocols like RADIUS to strengthen user access and security.

Syslog Server

Collects and centralizes logs from all devices, simplifying troubleshooting and monitoring.

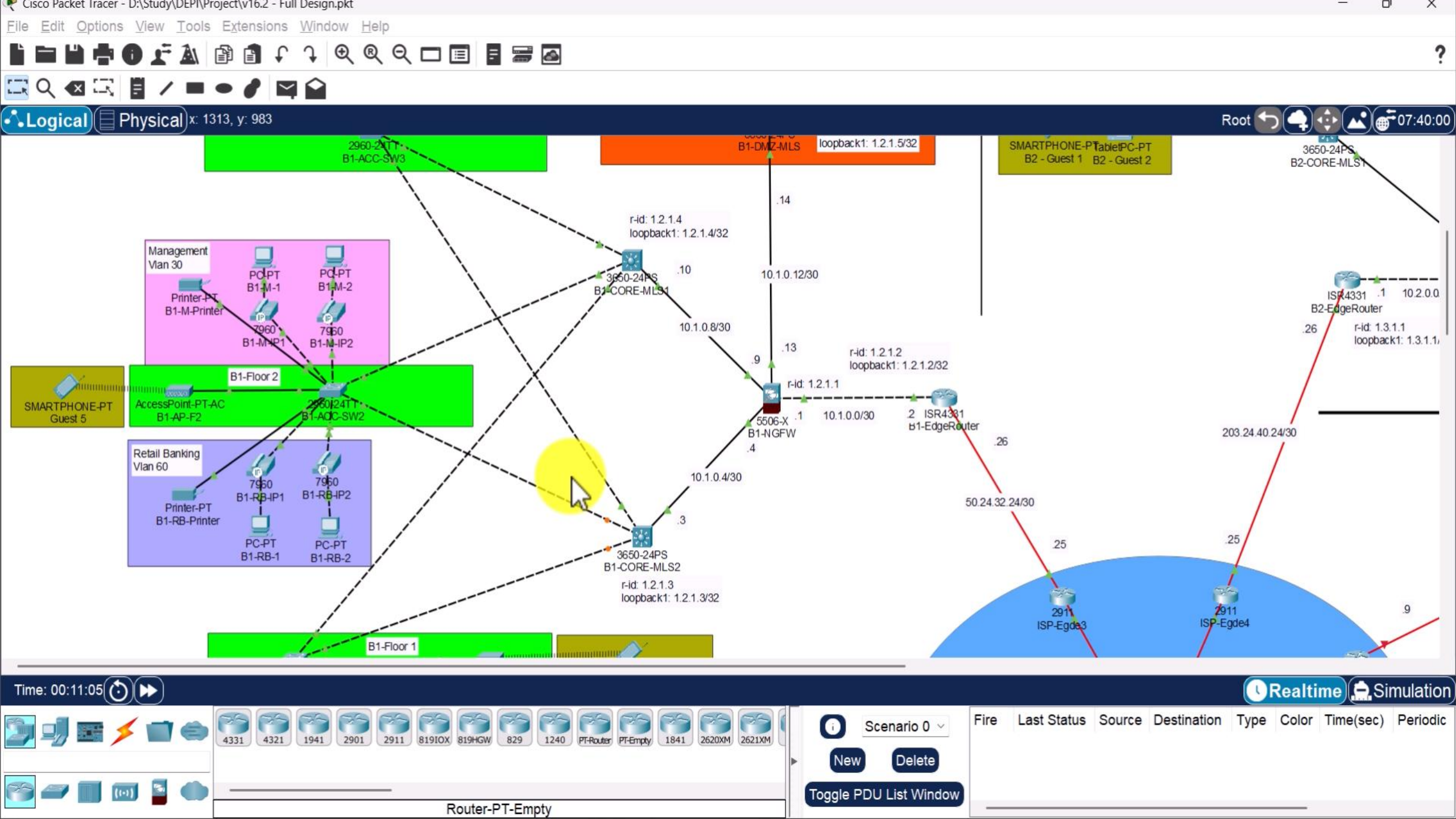
Remote Services from HQ

DNS (Domain Name Resolution)
Translates domain names to IP addresses, powered by centralized HQ servers.

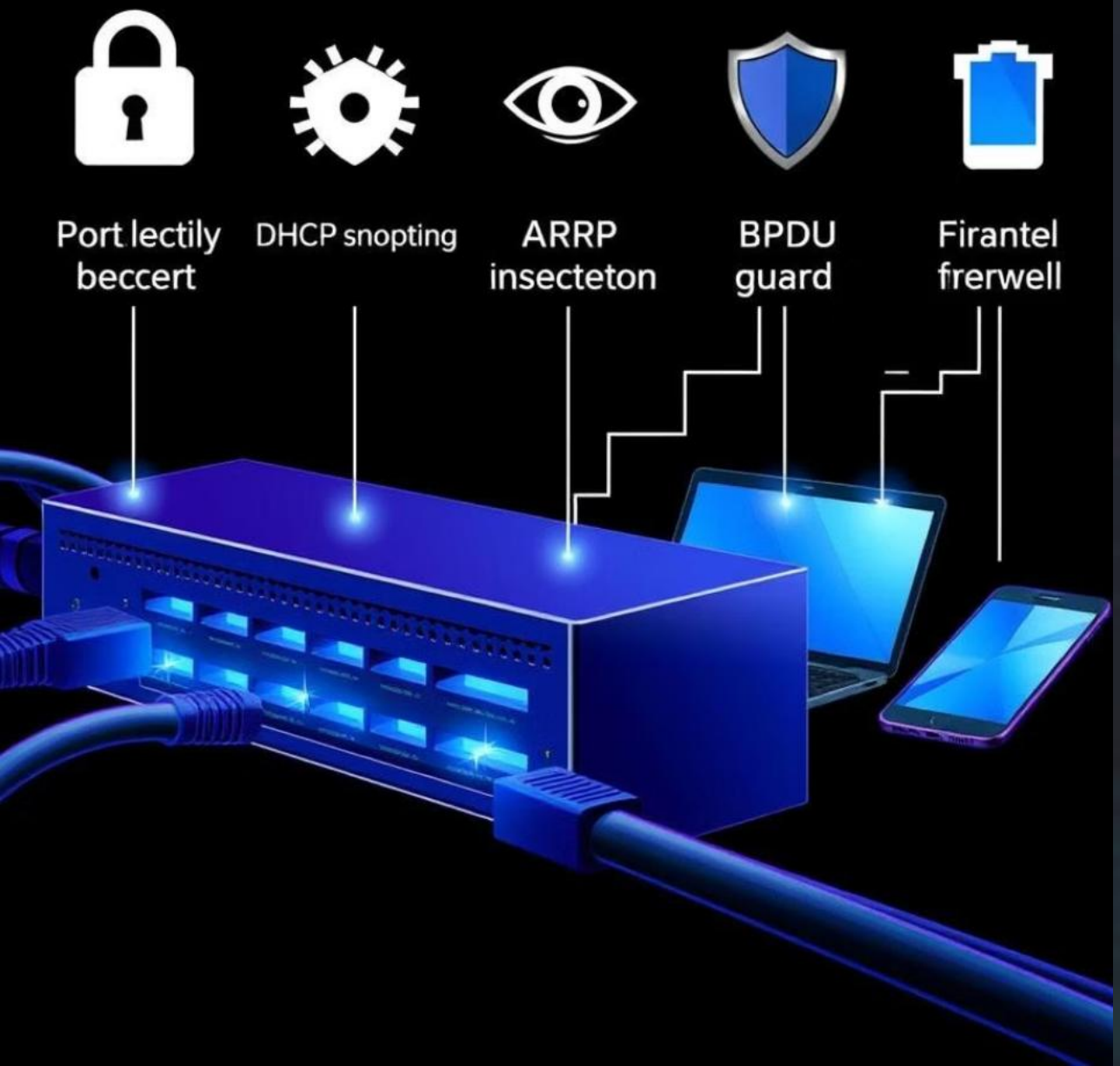
NTP (Network Time Protocol)
Synchronizes branch clocks for unified, accurate network time via HQ server.

FTP (File Transfer Protocol)
Secure centralized file sharing to enhance collaboration across branches.

Explanatory video


Cisco Packet Tracer - D:\Study\DEPI\Project\v16.2 - Full Design.pkt
File Edit Options View Tools Extensions Window Help
Logical
Physical
x: 1313, y: 983
Root
07:40:00
2960-24TT
B1-ACC-SW3
B1-DMZ-MLS
loopback1: 1.2.1.5/32
SMARTPHONE-PT
B2 - Guest 1
TabletPC-PT
B2 - Guest 2
3650-24PS
B2-CORE-MLS1
.14
r-id: 1.2.1.4
loopback1: 1.2.1.4/32
Management
Vlan 30
PC-PT
B1-M-1
PC-PT
B1-M-2
Printer-PT
B1-M-Printer
7960
B1-M-IP1
7960
B1-M-IP2
.10
3650-24PS
B1-CORE-MLS1
10.1.0.12/30
10.1.0.8/30
.9
.13
r-id: 1.2.1.2
loopback1: 1.2.1.2/32
r-id: 1.2.1.1
B1-Floor 2
SMARTPHONE-PT
Guest 5
AccessPoint-PT-AC
B1-AP-F2
2960-24TT
B1-ACC-SW2
5506-X
B1-NGFW
.1
10.1.0.0/30
.2
ISR4331
B1-EdgeRouter
.4
Retail Banking
Vlan 60
7960
B1-RB-IP1
7960
B1-RB-IP2
Printer-PT
B1-RB-Printer
PC-PT
B1-RB-1
PC-PT
B1-RB-2
10.1.0.4/30
.3
3650-24PS
B1-CORE-MLS2
r-id: 1.2.1.3
loopback1: 1.2.1.3/32
B1-Floor 1
ISR4331
B2-EdgeRouter
.1
10.2.0.0
.26
r-id: 1.3.1.1
loopback1: 1.3.1.1
203.24.40.24/30
.26
50.24.32.24/30
.25
.25
2911
ISP-Egde3
2911
ISP-Egde4
.9
Time: 00:11:05
Realtime
Simulation
4331
4321
1941
2901
2911
819IOX
819HGW
829
1240
PT-Router
PT-Empty
1841
2620XM
2621XM
Router-PT-Empty
Scenario 0
New
Delete
Toggle PDU List Window
Fire
Last Status
Source
Destination
Type
Color
Time(sec)
Periodic

All Project Security



Key Access Layer Security Measures

- Port Security
- Disable Unused Ports
- DHCP Snooping
- Dynamic ARP Inspection
- BPDU Guard
- Disable CDP

Distribution, Core, and Edge Security

Distribution & Core

- Access Control Lists (ACLs)
- OSPF (Authentication + Passive Interface)

Edge Router, DMZ & Firewall

- OSPF (Authentication Passive Interface)
- Firewall Policies
- Disable CDP VPN NAT


Thank You :)