Design a Multi-Site Network for a Complex Corporate Building System Background

Final Project Computer Network

Table Of Contents

1. Introduction

This document presents a detailed proposal for the design and implementation of a network infrastructure for CMC Holding, meeting the requirements of connection, performance, security and expansion ability for three operating locations of the company in Hà Nội and Đà Nẵng. The objective is to build a stable, safe and effective network, supporting the business and development of the company.

2. Overview of CMC Holding and the requirements

CMC Holdings is a mid-size company with about 600 employees, working in 3 locations:

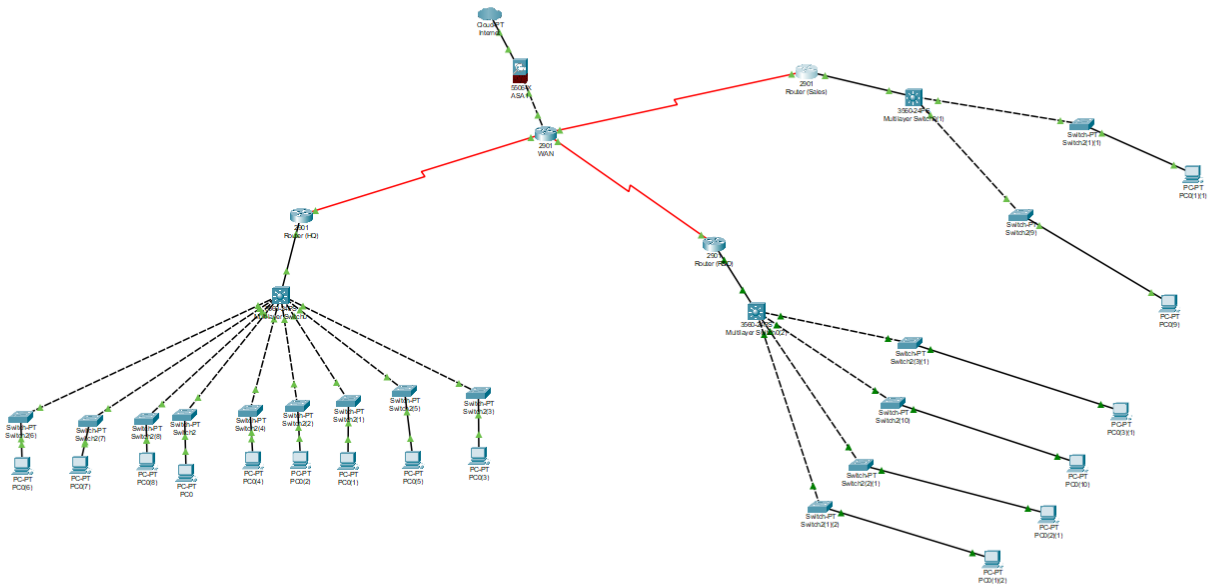
- **Headquarters (HQ)**: 10 floors, Hà Nội. There are about 300 employees working here.
- **R&D Office**: 5 floors, Đà Nẵng. There are about 200 employees working here
- **Sales Office**: 3 floors, Hà Nội (about 3 km from HQ): There are 100 employees working here.

The requirements:

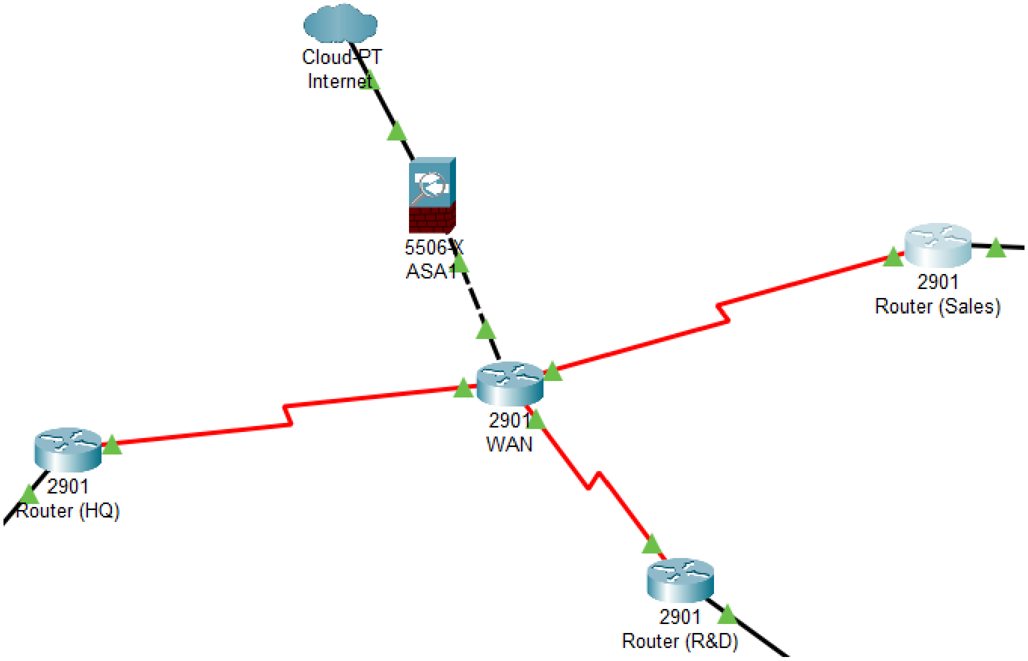
- Access the Internet at high speed and stability for all employees.
- Connect locally efficiently between all departments and locations.
- High availability of all Internet services.
- Security data and system.
- Available for expanding in the future.
- Support both IPv4 and IPv6.

3. Network Architecture

3.1 Logical Network Topology Diagrams



Overall WAN Topology:

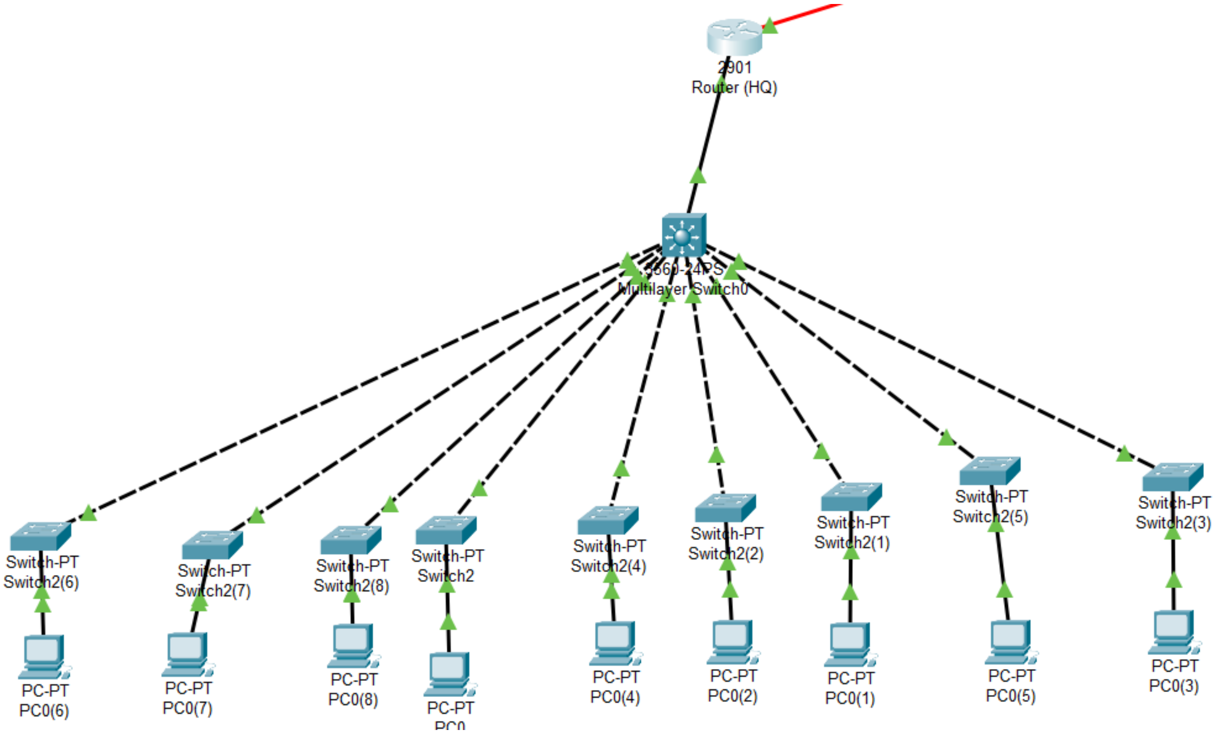


- The Wan will interconnect the three company sites securely and efficiently, primarily leveraging public internet infrastructure.
- **Model**: Star Topology.

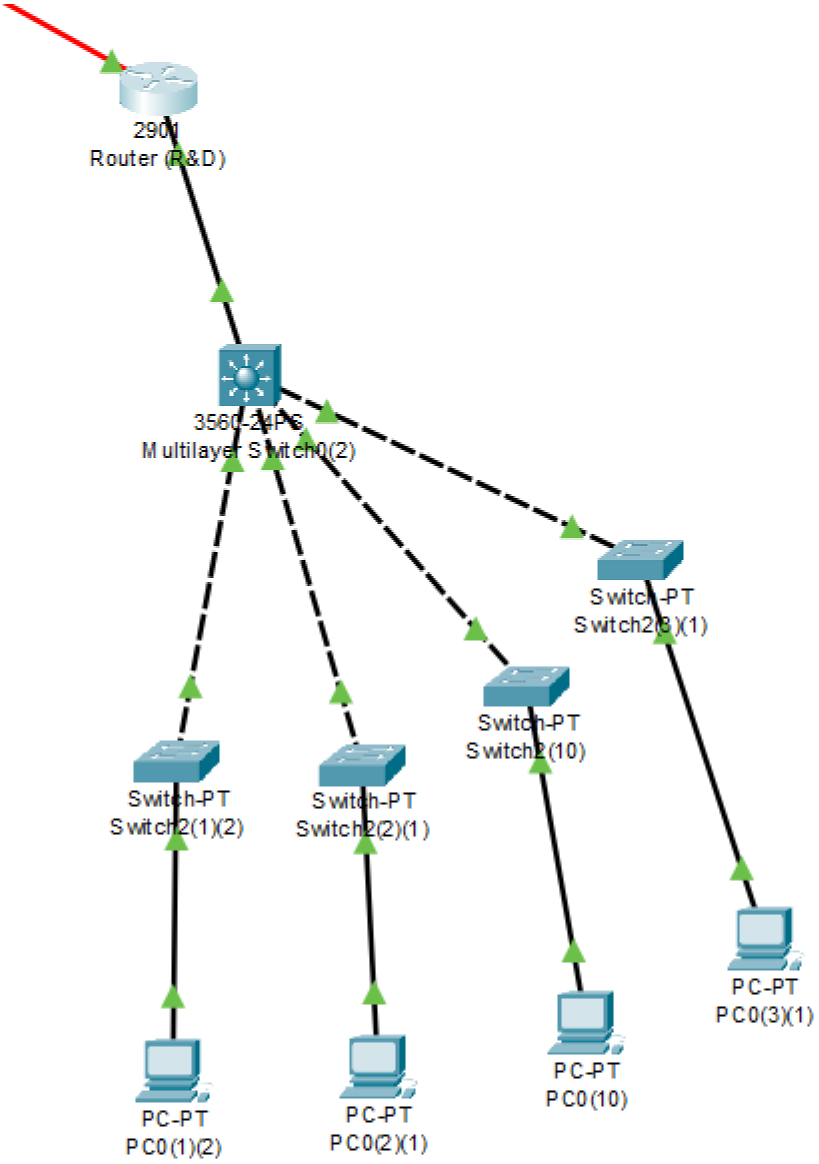
- **Central Internet connection point**: ASA firewall devices act as the main secure port connected to the Internet.
- **Central WAN router**: ASA firewall connects to a router (WAN), this router is active like a distribution point connecting WAN to branches.
- **Connect site**: From the central router (WAN), there are separate connections to each router of the site: router of HQ, router of R&D offices and router of sales offices.

Overall LAN Topology (HQ, R&D and Sale office)

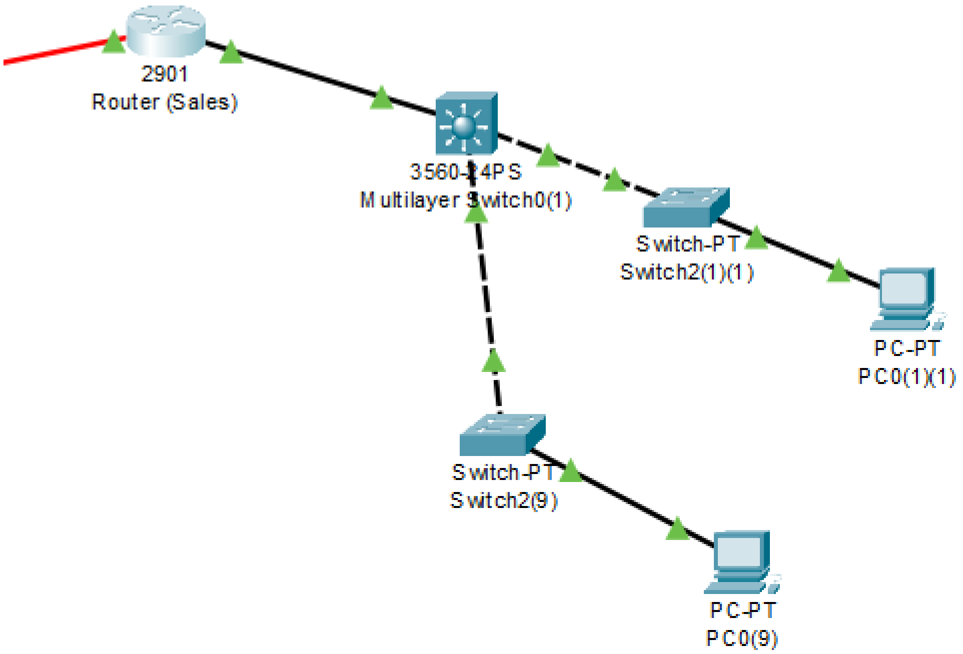
- **HQ LAN topology**



- **R&D office LAN topology**



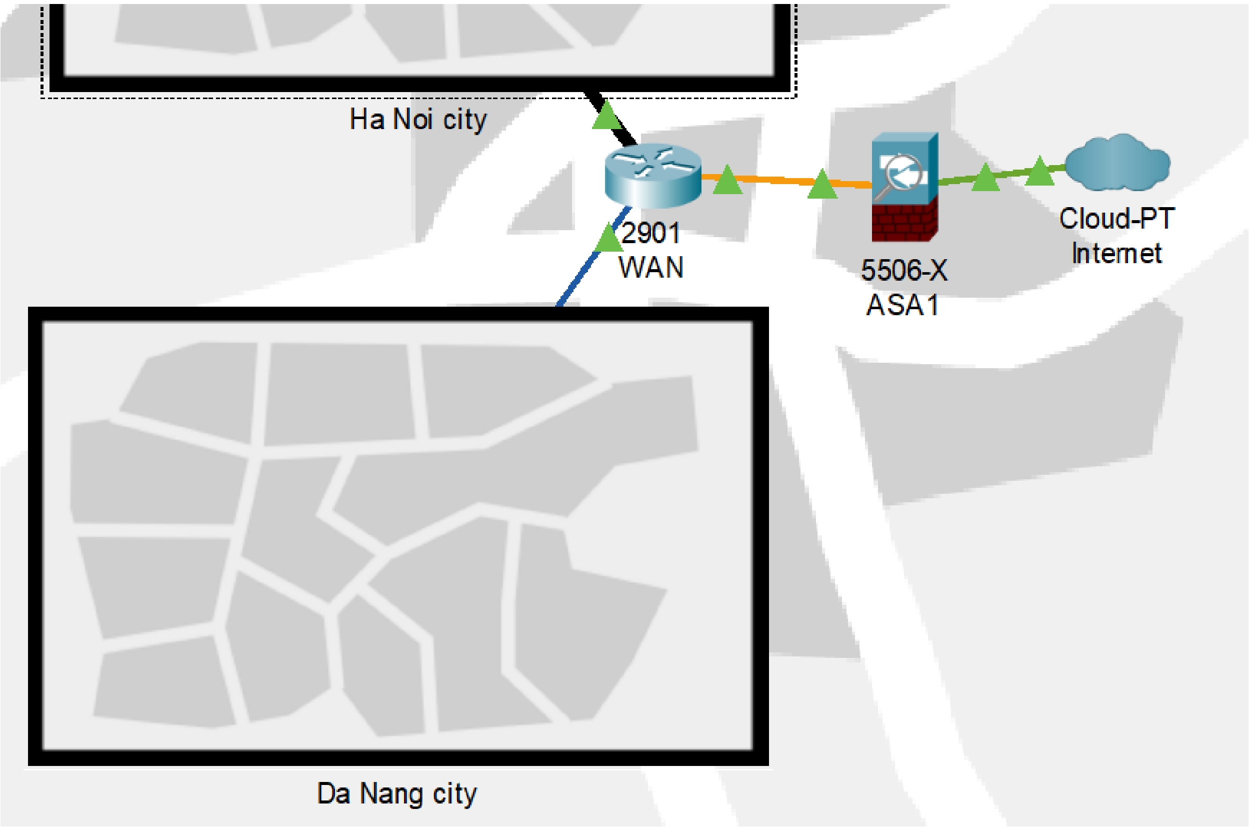
- **Sales office LAN topology**



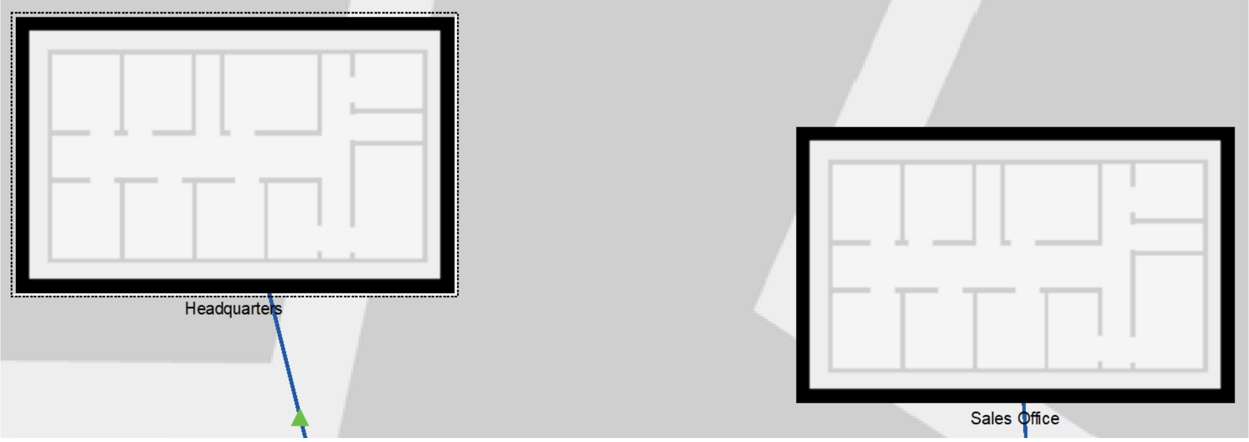
- **Model**: Two-Tier LAN architecture, including Core/Distribution and Access.
  - **Site router**: Router of HQ, R&D and Sales office connects to the WAN central, acts as an output/entrance gate for all devices in local.
  - **Core/Distribution (Collapsed)**: Router connects to Multilayer Switch. This switch is like a central LAN, performing high-speed switches and routing between internal VLANs.
  - **Access layer**: Multiple access switches connect to the multiplayer switch. These Access switch provides a direct network connection for terminals such as computers (PCs), printers and Wireless Access Points (WAPS).

3.2 Physical Network Topology Diagram

Overall:



In Hà Nội city (HQ and Sales office):



3.3 Subnetting Strategy

3.3.1 IPv4 Address Allocation (Using VLSM)

Use the address range 10.0.0.0.0.0/8. Each location will be granted a large block, then split with VLSM for VLANs/departments.

Each floor can be granted one /22 or /23 blocks, then split by VLANs. General VLANs (servers, management, ...): are granted separate subnets.

- HQ (300 employees, 10 floors): Issued 10.10.0.0/16 (65,534 addresses)
- R&D Office (200 employees, 5 floors): Issued 10.20.0.0/17 (32,766 addresses)
- Sales Office (100 employees, 3 floors): Issued 10.30.0.0/18 (16,382 addresses)

3.3.2 IPV6 Address Allocation

Using a Global Unicast Address (Gua) prostitute is assumed by ISP, for example: “2001:db8:cmc::/48”.

- Each site will be granted one /56 prefix from /48:
  - HQ: “2001:db8:cmc:0100::/56”
  - R&D Office: “2001:db8:cmc:0200::/56”
  - Sales Office: “2001:db8:cmc:0300::/56”
- In each site, each VLAN will be granted one /64 subnet from /56 Prefix of that site. For example, at HQ (2001:db8:cmc:0100::/56):
  - HR VLAN: “2001:db8:cmc:0101::/64”
  - Marketing VLAN: “2001:db8:cmc:0102::/64”
  - Dev VLAN: “2001:db8:cmc:0103::/64”
  - ….
- Link-Local address (fe80::/10) will be automatically used for communication on the same link.
- Unique Local Addresses (ULA) (fc00::/7) can be used for internal services without access from the Internet if necessary, for example: “fd00:cmc::/48”.

4. VPN and WAN Connectivity

4.1 Site-to-Site VPN

Solution: Use IPSEC/IKEV2 for Site-to-Site VPN connection between site (HQ, R&D, Sales) to Asa Firewall or Router (WAN) center. IPSec provides powerful and authentic encryption.

Redundant VPN Tunnels:

- Each site (HQ, R&D, Sales) should have an internet connection from two different ISPs (if possible) to connect to Asa Firewall/Router (WAN) central.
- Establish two Tunnel VPN in parallel from each site to the center, each tunnel through a different ISP.
- Use Dynamic Routing Protocols (for example, BGP or OSPF via Green/IPSEC Tunnels) or IP SLA on central Router and Router sites to automatically switch (Failover).

4.2 Remote Access VPN

Solution: SSL VPN (e.g. Cisco anyconnect on ASA, OpenVPN) allows employees to work from the solution: SSL VPN (for example, Cisco anyconnect on ASA, OpenVPN) allows remote workers to work safely connected to the company through the central Asa Firewall).

Advantages of SSL VPN: Easy to use, surpassing most user firewalls.

Authentication: Use two factors authentication (Two -Factor Authentication (2FA). Integrated with Active Directory/LDAP.

Decentralization: Applying detailed access policies.

Equipment: Asa Firewall of the center will act as VPN Concentrator.

5. Security and management

5.1 Firewall and Access Control Policies

Firewall location: ASA Firewall is the main control point.

- **Internal Segmentation**: Use the Firewall feature of Multilayer Switches at each site or ACLS on the site Routers to control the flow between important VLANs. Consider Internal Segmentation Firewalls (ISFW) if higher security requirements between key VLANs.

Access control policies (ACLs):

- Least privilege of ACLs is default deny
- Apply ACLs in ASA Firewall, Routers and Multiplayer Switches.
- Use Role-Based Access Control (RBAC).
- Regularly review and update ACLS.

5.2 Network Monitoring and Logging Solutions

Network Monitoring:

- Tools: Using Network Monitoring System (NMS) solutions such as Prtg Network Monitor, Zabbix, Nagios, Solarwinds Orion.
- Protocol: SNMP, NetFlow / sFlow / IPFIX.
- Monitoring parameters: equipment status, bandwidth, latency, error ratio, CPU/Memory, VPN Tunnels status.
- Alerting: Automatic warning settings.

Logging Solutions:

- Syslog Server: Deploying centralized Syslog Server (for example: Graylog, Elk Stack).
- Log content: Login event, configuration change, error, security event, Firewall.
- Storage and analysis: Safety log storage, analysis for abnormal detection.

6. Expansion Recommendations

Module design: Classification network architecture and Topo shaped to easily add new sites or expand resources in existing sites.

Bandwidth provisioning: Select WAN transmission line capable of upgrading.

IP address: IPv4 and IPV6 address plan with backup.

Wireless: WLC design has the ability to manage additional APS.

Cloud Integration: Ensure safe and effective connection to Cloud.

Software-Defined Networking (SDN): Consider deploying SDN in the future.

Security Posture Enhancement: Deploying Siem, EDR.

7. Conclusion

Proposing this network design (updating the network architecture according to the new diagram) to provide CMC Holdings with a modern, safe, effective and expandable network infrastructure. The successful implementation requires detailed planning, suitable equipment selection, careful configuration and professional operation management.

The next steps include:

1. Discuss in more detail about the specific requirements of each department.
2. Actual survey at locations.
3. Select specific equipment and services suppliers.
4. Detailed implementation planning.