

VIETNAM NATIONAL UNIVERSITY - HO CHI MINH CITY
HO CHI MINH CITY UNIVERSITY OF TECHNOLOGY
FACULTY OF COMPUTER SCIENCE AND ENGINEERING



Computer Networks(CO3094) - CC04 - Group 11

ASSIGNMENT 2

NETWORK DESIGN AND SIMULATION FOR A CRITICAL LARGE COMPANY

Lecturer: Diep Thanh Dang.
Students: Tran Hoang Phuc - 2252647
Huynh Dao Dong Quan - 2053367
Vo Hoang Phuc - 2252650

HO CHI MINH CITY, NOVEMBER 2024

Contents

1	Topic introduction	3
2	Network structures for buildings	4
2.1	Analyze the network system requirements of Headquarters and Branches	4
2.2	Checklist to be surveyed at the installation locations	5
2.3	Network structure and Wireless environment	6
3	List of minimum equipment, IP plan, and wiring diagram	7
3.1	List of recommended equipment and typical specifications	7
3.2	Schematic physical setup of the network	12
3.2.1	Headquarter in Ho Chi Minh city	12
3.2.2	Branches in Ha Noi and Da Nang	13
3.3	WAN connection diagram between Headquarters and Branches	14
4	Calculate the required throughput, and expected bandwidth from ISP, then suggest the configuration for the company network	16
4.1	Calculate the required throughput, and expected bandwidth from ISP	16
4.1.1	Required throughput	16
4.1.2	Expected bandwidth	18
4.2	Suggestion to the configuration for the company network	18
4.2.1	Router	18
4.2.2	Switch	19
4.2.3	Access Point	20
5	Design the network map using Packet Tracer or GNS3 simulation software	21
6	Test the system with popular tools such as ping, and traceroute	23
6.1	Connect between PCs in the same VLAN	23
6.2	Connect PCs between VLANs	24



6.3	Connect PCs between Headquarters and branches	25
6.4	Connect to servers in the DMZ	26
6.5	No connections from Customers’ devices to PCs on the LAN	27
6.6	Connect to the Internet to a Web server	28
7	Re-evaluation	29
7.1	Reliability	29
7.2	Ease of upgrade	29
7.3	Diverse support software safety	29
7.4	Network security	29
7.5	Remaining problems	29
7.6	Development orientation	30
8	References	30

1 Topic introduction

The main goal of this assignment is to develop and model an extensive computer network for BB Bank, a significant financial organization. The objective is to establish a network infrastructure that can efficiently support the business's activities throughout its two branch locations in Da Nang and Ha Noi as well as its headquarters in Ho Chi Minh City.

The network design's primary needs are complex. In addition to 30 workstations, 3 servers, and 5 or more networking devices at each Branch, the network must accommodate 120 workstations, 5 servers, and 12 networking devices at the Headquarters via a combination of wired and wireless access. Over a wide area network (WAN), secure, high-availability communication between the headquarters and branch locations is crucial. Implementing strong security measures like firewalls and IPS/IDS and offering dependable internet connection are also essential. Furthermore, during the following five years, the network must be built to handle a 20% increase in users, network traffic, and branch extensions. Following industry best practices for network topology, security, and scalability will be crucial during the design phase.

The report will provide the suggested network design, equipment list, IP addressing strategy, and cabling diagram in order to meet these needs. Future development plans, security issues, and performance analysis will also be discussed. Cisco Packet Tracer will be used to simulate and evaluate the design, with connectivity, dependability, and security serving as the main evaluation factors.

By the end of this assignment, a robust and scalable network solution will be presented to support BB Bank's critical operations across its Headquarters and Branch locations.

2 Network structures for buildings

2.1 Analyze the network system requirements of Headquarters and Branches

For the Headquarters

- The headquarters building consists of 7 floors, where the 1st floor is designated for the IT room and the Cabling Central Local.
- The installation scale is medium, including: 120 workstations, 5 servers, 12 or more network devices.
- Ensure the use of modern technology for both wired and wireless connections: Wired connections use GPON cable technology, Network infrastructure requires 1GbE/10GbE connectivity.
- The system is organized by VLAN, with each floor assigned a different VLAN, ensuring: Security, Authentication, Access rights. Internal machines can access each other's data, but machines outside the network cannot.
- For Internet connectivity:
 - The central network connects to the external Internet using an ADSL line.
 - Two Leased Lines are used for WAN connectivity.
- The company uses a combination of Licensed and Open-Source Software, including: Office applications, Client-server applications, Databases, and more.
- A surveillance camera system is installed.
- The BB bank has a growth rate of 20% per year in terms of increasing the number of employees, devices, etc.

For the Branches

- The building comprises two floors, with the first floor equipped with an Information Technology Room and an Cabling Central Local.
- The installation scale is relatively small, including 30 workstations, 3 servers, and at least 5 networking devices.
- Both branches are connected to the headquarters via a WAN link, utilizing either SD-WAN or MPLS, depending on the cost-benefit analysis.
- Available WAN options are analyzed based on cost, with the advantages and disadvantages of each option documented for consideration.

2.2 Checklist to be surveyed at the installation locations

Physical condition

- Measure physical area of rooms, environmental conditions, and temperature
- Check the space availability for setting up the IT room and Cabling Central Local.
- Evaluate the power supply and cooling systems in the buildin

Network Infrastructure

- Check routers, switches, patch panels, cabling, and wireless APs.
- Check out the number of workstations, servers, and networking devices that will be installed.
- Plan for the VLAN structure for different departments.
- Assess the feasibility of setting up leased lines for WAN connection and xDSL for Internet access.
- Ensure WAN link setup (SD-WAN, MPLS, VPN) and bandwidth adequacy.

Security and Availability

- Configure firewall, IPS/IDS, VPN, ACLs, and physical security.
- Plan for the installation of security devices such as firewall, IPS/IDS, and phishing detection.

Surveillance system

- Check out the number of surveillance camera used.
- Plan for physical installation of a surveillance camera system.

Cost Analysis

- Calculate how much the suggested network infrastructure will cost to implement, taking into account the price of hardware, software.

Training and Handover

- Train staff and provide documentation for network management.

2.3 Network structure and Wireless environment

In this assignment, we design the BBbank network based on a hierarchical network topology (extended star topology). An extended star network topology includes an additional networking device that is directly connected to the central networking device. It seems like a mesh of switches which are interconnected to the network and once central networking device which controls the network. There are 3 layers in a hierarchical network topology: Core Layer (Core Routers), Distribution Layer (Layer 3 Switches) and Access Layer (Layer 2 Switches and end devices). Hierarchical networks offer a wide range of benefits, such as enhanced performance, reliability, and scalability, better security, easier management and design, and improved cost-efficiency. Also at distribution layer, we implement Redundancy as mentioned above. Redundancy is used to improve high availability and system robustness because in case 1 of 2 layer 3 switches has a problem, the system is not crashed and still works with the other layer 3 switch. This assignment requires us to use 2 leased-line to connect from the main site to 2 auxiliary sites but we use in total 4 leased-line (2 for each connection to each auxiliary site) for load balancing. Dataflow at the router of main site will be high at peak hours so we have to ensure there will not be data congestion happening here between Sites. With these connections, we use Serial-DCE cables. Access Control List (ACL) is applied on Layer 3 switches to prevent customer's devices (devices using Wireless connection) from communicating to host devices of BBbank. Therefore, customer's devices like Laptops or phones using WiFi can communicate to every other devices in case they use WiFi also. They can not connect to BBbank's PCs.

Firewall ASA is installed at the main site to ensure the security for the system and ACL is also configured here to decide whether to accept or drop packets from Internet. This Firewall separates the system into 3 partitions: DMZ Zone, Outside and Inside. Actually, there is one more partition, which is ServerFarm (place important server here) but we place this zone inside the IT block and we consider it as INSIDE ZONE. Connection from BBbank to Internet is transmitted over ADSL line provided by the ISP through 2 DSL modems.

3 List of minimum equipment, IP plan, and wiring diagram

3.1 List of recommended equipment and typical specifications

Router

The Cisco Router 2901, part of the 2900 Series ISR, is a modular router designed for small to medium-sized businesses, offering up to 75 Mbps throughput with two onboard Gigabit Ethernet ports and four EHWIC slots for flexibility. It supports advanced services like VPN, firewall, intrusion prevention, and voice/video capabilities with optional DSPs. With expandable memory (up to 2 GB DRAM and 8 GB Flash), IPv6 support, and Cisco EnergyWise for power management, it is ideal for branch offices needing reliable, secure, and scalable networking. Configuration is done via Cisco IOS, supporting routing protocols, NAT, QoS, and more.



Figure 1: Cisco Router 2901

Price: 18.000.000 VND

Switch

The Cisco Catalyst 2960-24TT is a reliable Layer 2 managed switch designed for small to medium-sized networks, offering 24 Fast Ethernet ports (10/100 Mbps) for device connectivity and 2 Gigabit Ethernet uplink ports (10/100/1000 Mbps) for high-speed uplinks. It supports VLANs, STP, QoS, and advanced security features like port security and 802.1X authentication, making it suitable for network segmentation and traffic prioritization. Managed via Cisco IOS, SNMP, or a web interface, it includes Cisco EnergyWise for energy efficiency and is ideal for businesses needing a cost-effective solution for connecting multiple devices in a secure and scalable manner.



Figure 2: Cisco Catalyst 2960-24TT

Price: 7.000.000 VND

Multilayer switch

The Cisco WS-C3650-24PS is a member of the Cisco Catalyst 3650 Series, designed for enterprise-grade networks. It features 24 Gigabit Ethernet ports with PoE+ (Power over Ethernet Plus) support, allowing it to power devices such as IP phones, cameras, and wireless access points directly through Ethernet cables. The switch supports stackable configurations, enabling scalability and ease of management for growing networks. It is equipped with Cisco's Unified Access Data Plane (UADP) ASIC for enhanced performance and supports Layer 2 and Layer 3 switching capabilities. Additionally, it includes advanced features like Cisco IOS software, quality of service (QoS), and robust security options, making it suitable for high-performance and secure enterprise environments.



Figure 3: Cisco WS-C3650-24PS

Price: 40.000.000 VND

DSL Modem

The D-Link DSL-2740B is a wireless ADSL2+ modem router designed for home and small office use, supporting download speeds up to 24 Mbps and upload speeds up to 1 Mbps. It offers wireless connectivity with speeds up to 300 Mbps using IEEE 802.11b/g/n standards, along with four Ethernet LAN ports for wired connections. The device includes security features such as WPA/WPA2 encryption, SPI firewall, and QoS for prioritizing traffic, making it ideal for users who need reliable internet access with a mix of wired and wireless connections.



Figure 4: DSL-2740B Modem

Price: 1.500.000 VND

Access Point

The Cisco 3702I-C-K9 is a high-performance indoor wireless access point designed for enterprise environments, part of Cisco's Aironet 3700 series. It supports the 802.11ac Wi-Fi standard, offering dual-band operation (2.4 GHz and 5 GHz) with speeds up to 1.7 Gbps, making it suitable for high-density environments. The model features MIMO (Multiple Input, Multiple Output) technology for enhanced wireless capacity, improved coverage, and better signal strength. It is equipped with advanced security features, including WPA2 encryption, and integrates seamlessly with Cisco's wireless controllers for centralized management. The 3702I-C-K9 is designed to support a wide range of applications, from offices to schools, providing reliable and scalable wireless connectivity.



Figure 5: Cisco 3702I-C-K9

Price: 15.000.000 VND

Firewall

The ASA5506-SEC-BUN-K9 is a Cisco security appliance designed for small to medium-sized networks. It offers advanced firewall protection, VPN support, and threat defense, including features like intrusion prevention, URL filtering, and malware protection. This model comes with a security bundle, providing essential services such as stateful inspection and remote access VPNs. It's commonly used in environments where reliable, scalable security solutions are required, and supports cloud-managed features for flexible deployment.



Figure 6: Cisco ASA 5506

Price: 20.000.000 VND

Surveillance camera

A high-resolution fisheye network camera with a 12 MP panoramic view, the Hikvision DS-2CD63C5G0-IVS is perfect for indoor places that need 360-degree coverage, such retail establishments or bank lobbies. With its single-sensor design, it removes blind areas and offers a variety of display modes, such as regional, panoramic, and fisheye perspectives. For proactive security, the camera has cognitive analytics like line crossing and intrusion detection. It is a flexible solution for wide-area interior surveillance because of its inconspicuous form factor, effective H.265+ compression, and strong performance in a range of lighting conditions.



Figure 7: Hikvision DS-2CD63C5G0

Price: 17.000.000 VND

3.2 Schematic physical setup of the network

3.2.1 Headquarter in Ho Chi Minh city

Headquarter 1st floor

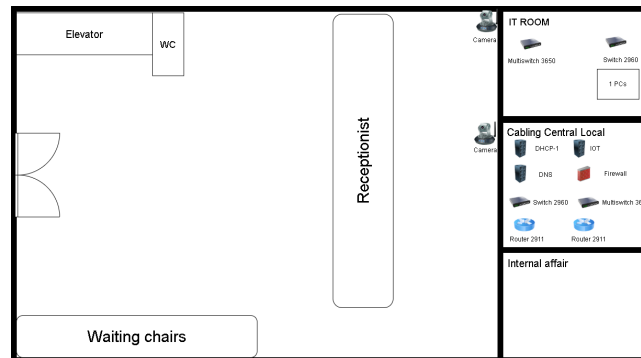


Figure 8: 1st Floor of Headquarter

First floor of the Bank is mainly use for customer service. It includes an IT room containing key network devices such as a multiswitch (3650), a switch (2960), and a PC. Adjacent to the IT room is the cabling central local area, which houses additional devices like a DHCP server, IoT devices, DNS server, firewall, switches, and routers (2911). Surveillance cameras are strategically placed for security, one near the entrance and another near the IT room. The floor also features functional areas such as a reception desk, a waiting area with chairs, and facilities like an elevator and a restroom (WC). The internal affairs section is located nearby, ensuring operational accessibility.

Headquarter 2nd-7th floor

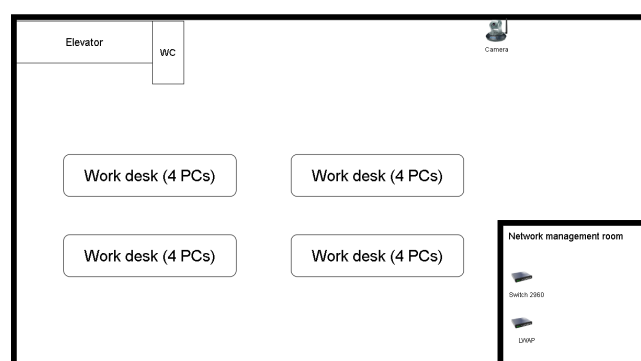


Figure 9: 2nd - 7th Floor of Headquarter

The 2nd - 7th floors are used for staffs. It includes four work desks, each equipped with four PCs, arranged symmetrically across the workspace. Surveillance is provided by

a strategically placed camera. A dedicated network management room houses key devices, including a Switch 2960 and a Lightweight Wireless Access Point (LWAP), ensuring proper connectivity and network control for the floor. Facilities like an elevator and restroom (WC) are present for convenience, maintaining functionality and accessibility.

3.2.2 Branches in Ha Noi and Da Nang

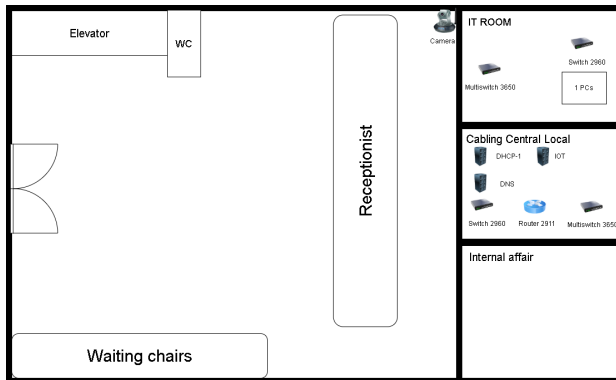


Figure 10: 1st Floor of Branch

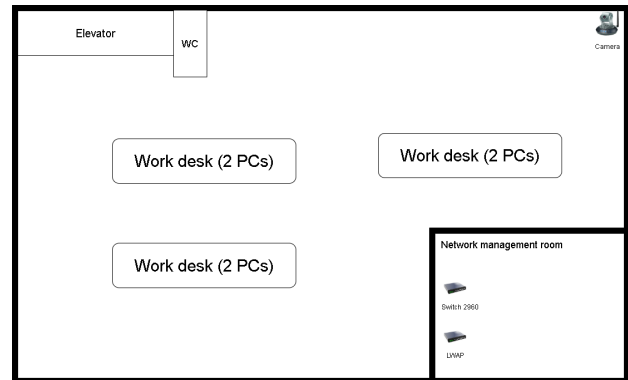


Figure 11: 2nd Floor of Branch

3.3 WAN connection diagram between Headquarters and Branches

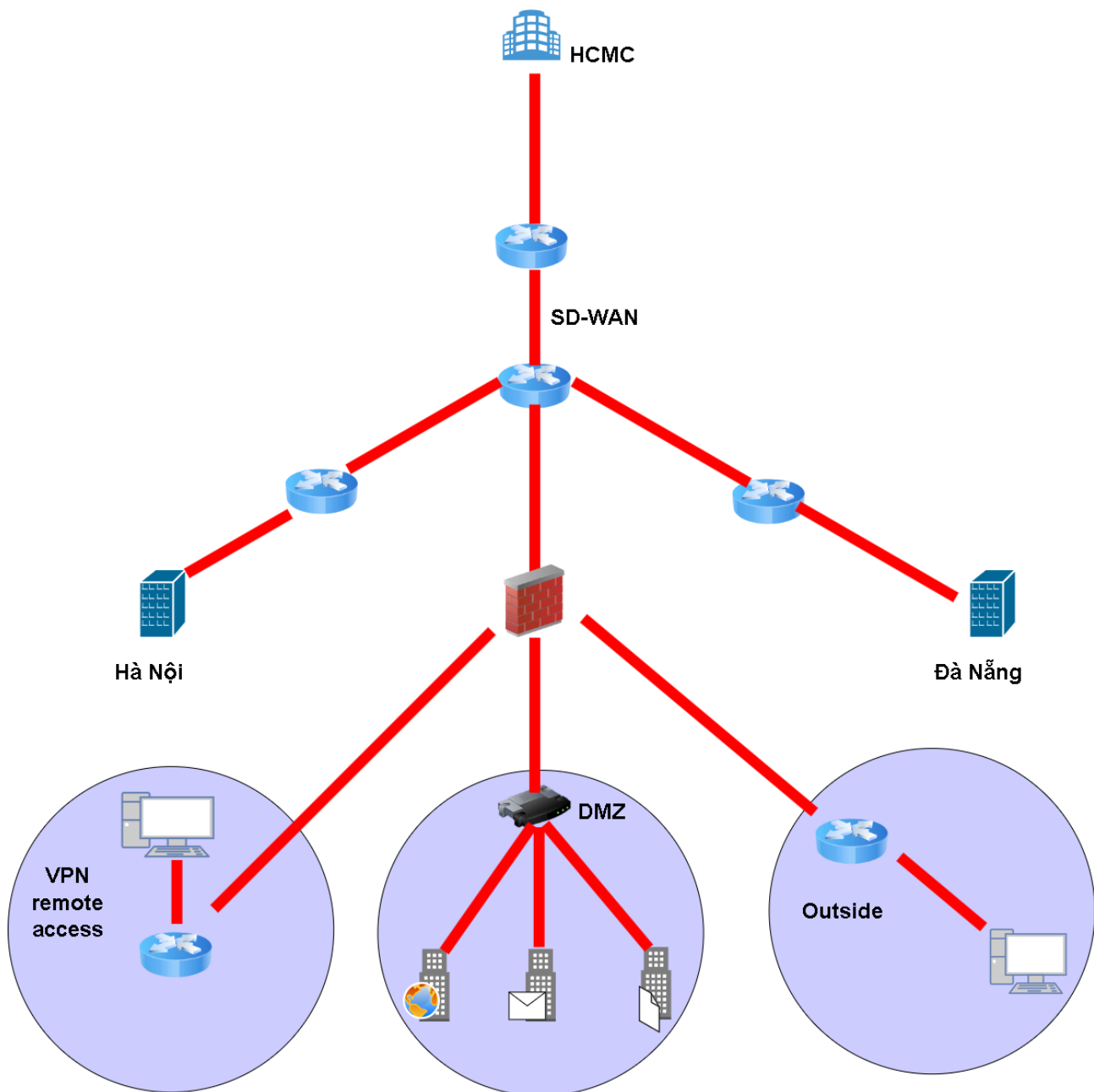


Figure 12: WAN connection diagram

This WAN connection diagram depicts a network infrastructure connecting multiple geographic locations, including HCMC (headquarter), Hanoi, and Da Nang, through routers for seamless communication. The network incorporates a firewall to enhance security and a DMZ (Demilitarized Zone) to host public-facing services like web and mail servers, as well as other critical systems. It also includes a VPN remote access feature, enabling secure connectivity for remote users to the central network. External connections to the internet are routed through an



"Outside" network, likely representing public or external users accessing services hosted within the DMZ. The setup ensures secure and efficient communication across distributed sites and external users.

IP Plan

HEADQUARTER				
Type	Network and Subnet Mask	Valid IP Address Range	Default Gateway	Broadcast Address
WLAN	192.168.100.0/24	192.168.100.2 to 192.168.100.253	192.168.100.1	192.168.100.254
VLAN Floor 1	192.168.1.0/24	192.168.1.2 to 192.168.1.253	192.168.1.1	192.168.1.254
VLAN Floor 2	192.168.2.0/24	192.168.2.2 to 192.168.2.253	192.168.2.1	192.168.2.254
VLAN Floor 3	192.168.3.0/24	192.168.3.2 to 192.168.3.253	192.168.3.1	192.168.3.254
VLAN Floor 4	192.168.4.0/24	192.168.4.2 to 192.168.4.253	192.168.4.1	192.168.4.254
VLAN Floor 5	192.168.5.0/24	192.168.5.2 to 192.168.5.253	192.168.5.1	192.168.5.254
VLAN Floor 6	192.168.6.0/24	192.168.6.2 to 192.168.6.253	192.168.6.1	192.168.6.254
DMZ	20.20.20.76/30	192.168.13.2 to 192.168.13.253	192.168.13.1	192.168.13.254
Security Camera	192.168.200.0/24	192.168.200.2 to 192.168.200.253	192.168.200.1	192.168.200.254
IT Floor	192.168.11.0/24	192.168.11.2 to 192.168.11.253	192.168.11.1	192.168.11.254
Server in IT Floor	192.168.12.0/24	192.168.12.2 to 192.168.12.254	192.168.12.2	192.168.12.254
HA NOI				
Server	192.168.15.0/24	192.168.15.2 to 192.168.15.253	192.168.15.1	192.168.15.254
Room	192.168.14.0/24	192.168.14.2 to 192.168.14.253	192.168.14.2	192.168.14.254
WLAN	192.168.102.0/24	192.168.102.2 to 192.168.102.253	192.168.102.1	192.168.102.254
SecurityCamera	192.168.203.0/24	192.168.203.2 to 192.168.203.253	192.168.203.2	192.168.203.254
DA NANG				
Server	192.168.17.0/24	192.168.17.2 to 192.168.17.253	192.168.17.1	192.168.17.254
Room	192.168.16.0/24	192.168.14.2 to 192.168.14.253	192.168.16.2	192.168.16.254
WLAN	192.168.103.0/24	192.168.102.2 to 192.168.102.253	192.168.103.1	192.168.103.254
SecurityCamera	192.168.204.0/24	192.168.204.2 to 192.168.204.253	192.168.204.2	192.168.204.25

Table 1: IP Plan table

4 Calculate the required throughput, and expected bandwidth from ISP, then suggest the configuration for the company network

4.1 Calculate the required throughput, and expected bandwidth from ISP

Data Streams and Workload of the System:

The data streams and workload of the system (approximately 80% during peak hours from 9 AM to 11 AM and from 3 PM to 4 PM) can be allocated to the Headquarters and the Branch as follows:

- Servers for software updates, web access, and database access, etc. The estimated total download traffic is about 1000 MB per day, and the total upload traffic is about 2000 MB per day.
- Workstations used for web browsing, document downloads, and customer transactions, etc. The estimated total download traffic is about 500 MB per day, and the total upload traffic is about 100 MB per day.
- WiFi-connected customer devices for downloading are about 500 MB per day.

4.1.1 Required throughput

Headquarters

Servers (Total Data per Day):

$$\text{Download:} = \frac{1000 \times 5}{24 \times 3600} = 0.058 \text{ MB/s}$$

$$\text{Upload:} = \frac{2000 \times 5}{24 \times 3600} = 0.12 \text{ MB/s}$$

Workstations (Total Data per Day):

$$\text{Download:} = \frac{120 \times 500}{24 \times 3600} = 0.69 \text{ MB/s}$$

$$\text{Upload:} = \frac{120 \times 100}{24 \times 3600} = 0.14 \text{ MB/s}$$

Wi-Fi-Connected Devices (Customer Access):

$$\text{Download:} = \frac{500}{24 \times 3600} = 0.005 \text{ MB/s}$$

BB Branch

Servers (Total Data per Day):

$$\text{Download:} = \frac{1000 \times 3}{24 \times 3600} = 0.035 \text{ MB/s}$$

$$\text{Upload:} = \frac{2000 \times 3}{24 \times 3600} = 0.07 \text{ MB/s}$$

Workstations (Total Data per Day):

$$\text{Download:} = \frac{30 \times 500}{24 \times 3600} = 0.17 \text{ MB/s}$$

$$\text{Upload:} = \frac{30 \times 100}{24 \times 3600} = 0.034 \text{ MB/s}$$

Wi-Fi-Connected Devices (Customer Access):

$$\text{Download:} = \frac{500}{24 \times 3600} = 0.005 \text{ MB/s}$$

Total Required Throughput for Peak Hours

Headquarters

$$\text{Download:} = \frac{(1000 \times 5 + 500 \times 120) \times 0.8}{3 \times 3600} = 4.81 \text{ MB/s}$$

$$\text{Upload:} = \frac{(2000 \times 5 + 100 \times 120) \times 0.8}{3 \times 3600} = 1.63 \text{ MB/s}$$

BB Branch

$$\text{Download:} = \frac{(1000 \times 3 + 500 \times 30) \times 0.8}{3 \times 3600} = 1.33 \text{ MB/s}$$

$$\text{Upload:} = \frac{(2000 \times 3 + 100 \times 30) \times 0.8}{3 \times 3600} = 0.67 \text{ MB/s}$$

4.1.2 Expected bandwidth

The required bandwidth in Mbps can be calculated by dividing the required throughput in MB/hour by the number of seconds in an hour (3600 seconds), and then converting from megabytes to megabits (1 byte = 8 bits).

Headquarters Bandwidth:

$$\text{Total:} = (0.058 + 0.12) \text{ MB/s} \times 8 = 1.424 \text{ Mbps}$$

$$\text{Peak Hours:} = (4.81 + 1.63) \text{ MB/s} \times 8 = 51.52 \text{ Mbps}$$

BB Branch Bandwidth:

$$\text{Total:} = (0.035 + 0.07 + 0.17 + 0.034 + 0.005) \text{ MB/s} \times 8 = 2.512 \text{ Mbps}$$

$$\text{Peak Hours:} = (4.81 + 1.63 + 1.33 + 0.67) \text{ MB/s} \times 8 = 67.52 \text{ Mbps}$$

4.2 Suggestion to the configuration for the company network

4.2.1 Router

- **DSL (Digital Subscriber Line):** A broadband network technology that operates over telephone lines. In router configurations, DSL is typically used to simulate or implement the connection between an edge router and an Internet Service Provider (ISP). This ensures a stable Internet connection with appropriate speed for data transmission and communication between the headquarters and branch offices. DSL configuration often includes settings such as PPPoE (Point-to-Point Protocol over Ethernet) for login and authentication with the ISP.
- **SD-WAN (Software-defined Wide Area Network):** sits on top of the transport layer (like MPLS or internet broadband) and provides centralized control, dynamic path selection, and application-aware routing. It's the intelligent traffic management system that decides which "highway" (MPLS, internet, etc.) to use for different types of data.
- **IPsec (Internet Protocol Security):** A suite of security protocols designed to protect communication over IP networks. It is frequently used in site-to-site VPNs to encrypt

and authenticate transmitted data.

- **VPN Site-to-Site:** A secure connection between networks at different geographic locations over a public network, such as the Internet, using IPsec to encrypt data transmission between sites.
- **VPN Remote Access:** Enables remote users to securely connect to a company's internal network, often utilizing IPsec or SSL VPN for encryption and secure access.
- **Serial Interfaces:** Serial interfaces (e.g., Se0/0/0, Se0/0/1) are commonly used for WAN connections between different locations.
- **GigabitEthernet Interfaces:** GigabitEthernet interfaces (e.g., Gi0/0, Gi0/1) are employed for high-speed internal LAN connections or for linking to other network devices, such as switches or routers.
- **FastEthernet Interfaces:** FastEthernet interfaces are used for lower-speed LAN connections or to connect end devices such as desktop computers or servers.
- **NAT (Network Address Translation):** A mechanism to translate internal IP addresses into public IP addresses for Internet access, typically configured on edge routers (in the OUTSIDE zone).
- **Firewall Rules:** Firewall rules are applied on routers or other security devices to regulate inbound and outbound traffic, particularly for DMZ zones and external connections.
- **ACLs (Access Control Lists):** Used to control traffic flow and can be applied for VPN configuration or other security policies.

4.2.2 Switch

- **VLANs (Virtual Local Area Networks):** The internal network in the headquarters and branches is divided into three VLANs to simplify management and avoid complex configurations.
- **Inter-VLAN Routing:** A multilayer switch is employed to enable communication between VLANs. Typically, each VLAN is assigned an IP address on a sub-interface or an SVI (Switched Virtual Interface) on the multilayer switch. IP routing is activated to allow traffic switching between these VLANs.
- **IP Routing:** On the multilayer switch, IP routing is configured (using the `ip routing` command) to enable the switch to function as a router, routing traffic between the connected networks.
- **DTP (Dynamic Trunking Protocol):** DTP can be used to automatically negotiate trunking configurations between switches. Trunking is essential for enabling communication between different VLANs over a single physical link.

- **DHCP (Dynamic Host Configuration Protocol):** DHCP is commonly implemented on a server or router to automatically assign IP addresses to devices within the network.
- **Access Control Lists (ACLs):** ACLs can be applied on the multilayer switch to control access to the network or between VLANs.
- **QoS (Quality of Service):** In environments with CCTV webcams, QoS can be configured to ensure sufficient bandwidth for video surveillance traffic. This is especially critical to maintain video quality during network congestion.

4.2.3 Access Point

LWAP (Lightweight Access Point) is a type of wireless access point that operates in conjunction with a Wireless LAN Controller (WLC) to provide wireless connectivity in a network. LWAPs are designed to simplify the management and deployment of wireless networks, particularly in enterprise environments.

5 Design the network map using Packet Tracer or GNS3 simulation software

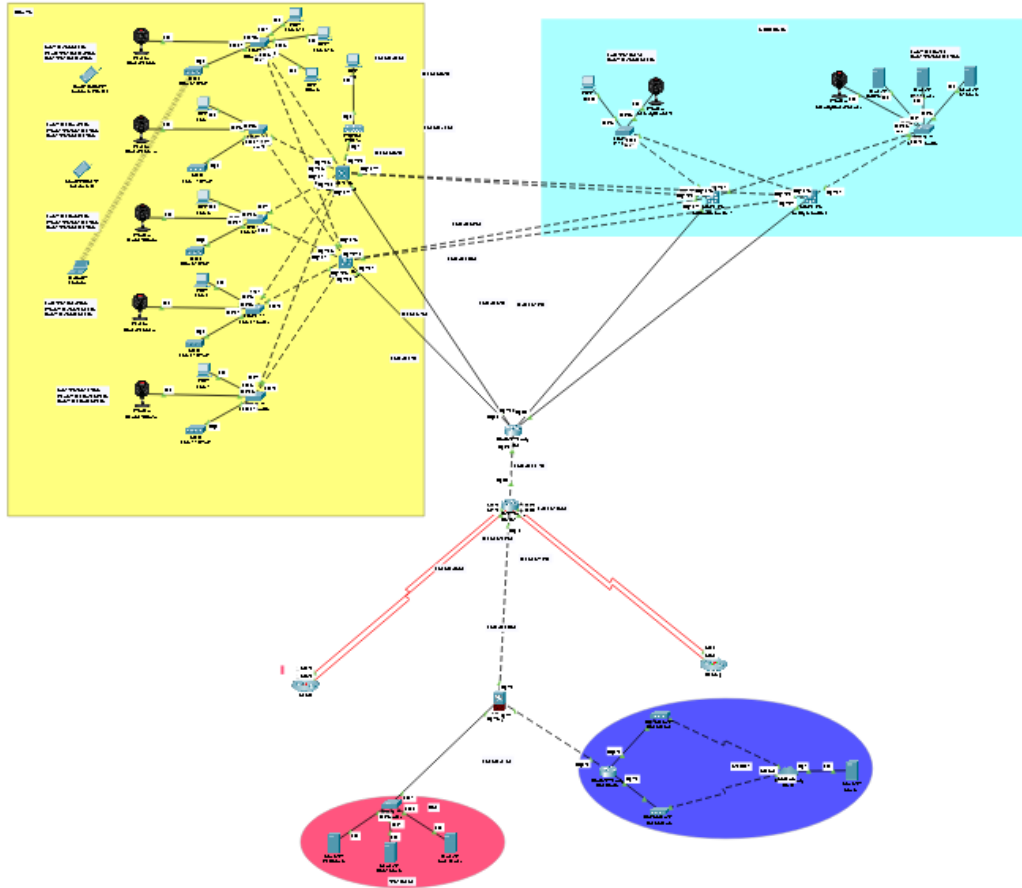


Figure 13: Entire system

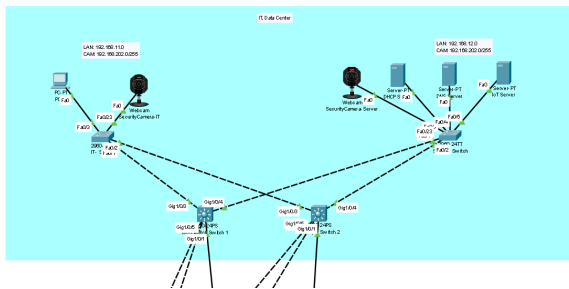


Figure 14: IT center

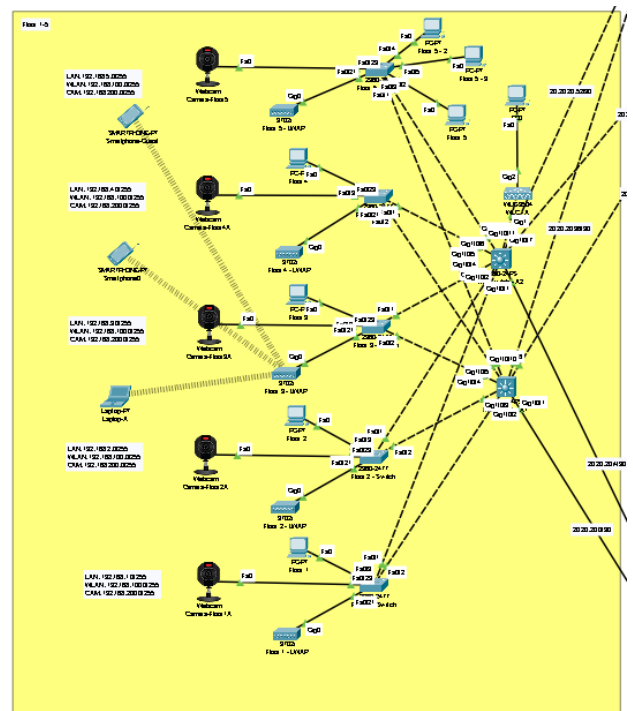


Figure 15: Headquarter

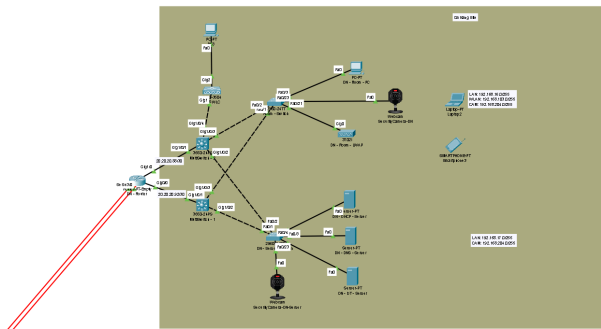


Figure 16: Da Nang Branch

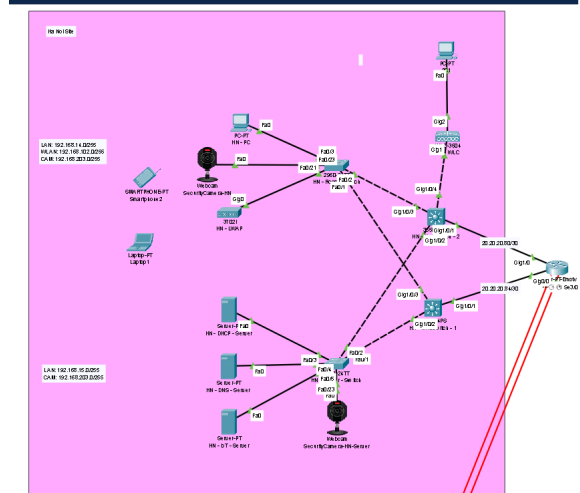


Figure 17: Ha Noi Branch

6 Test the system with popular tools such as ping, and traceroute

6.1 Connect between PCs in the same VLAN

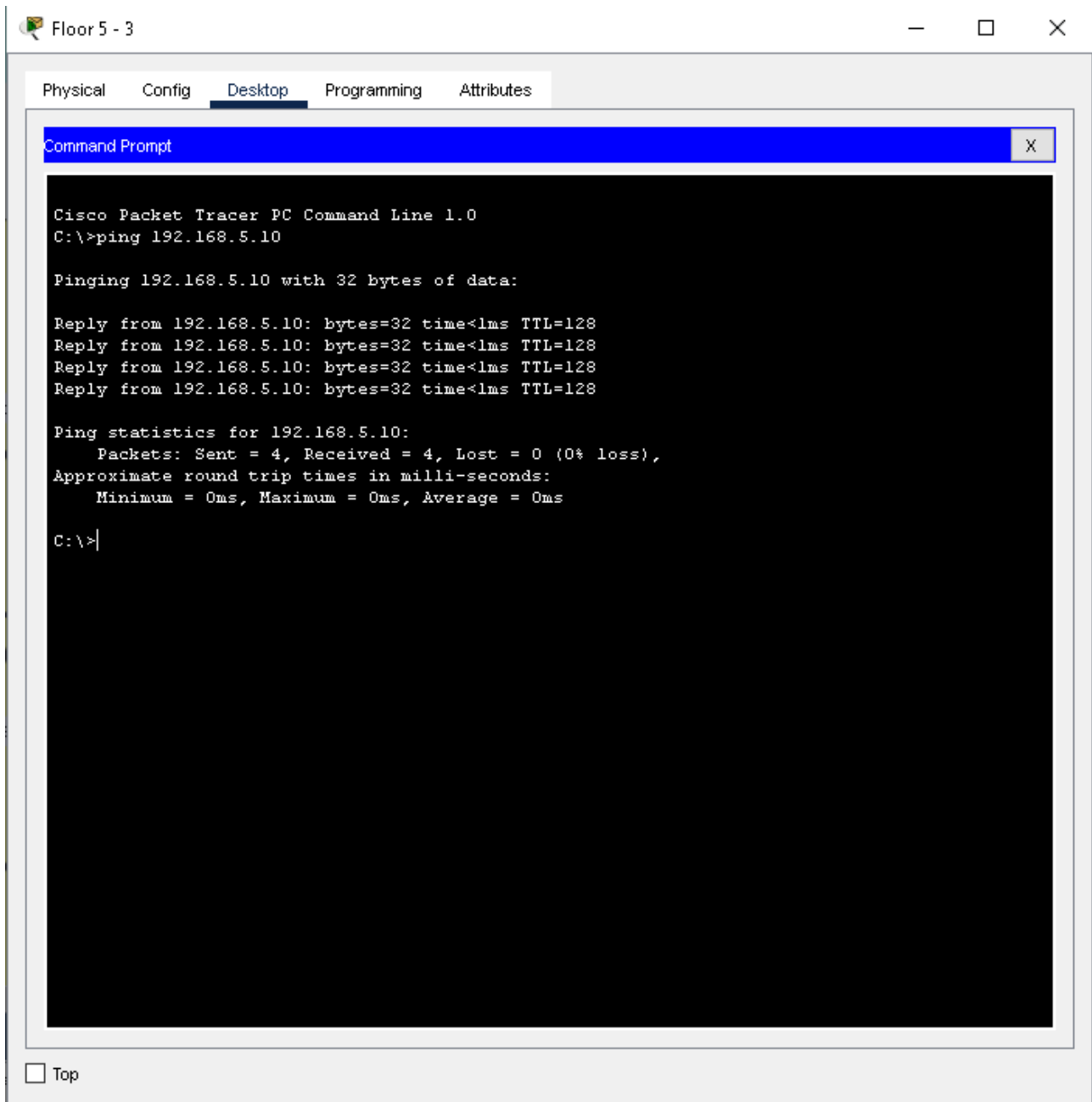


Figure 18: Test PC in same VLAN

6.2 Connect PCs between VLANs

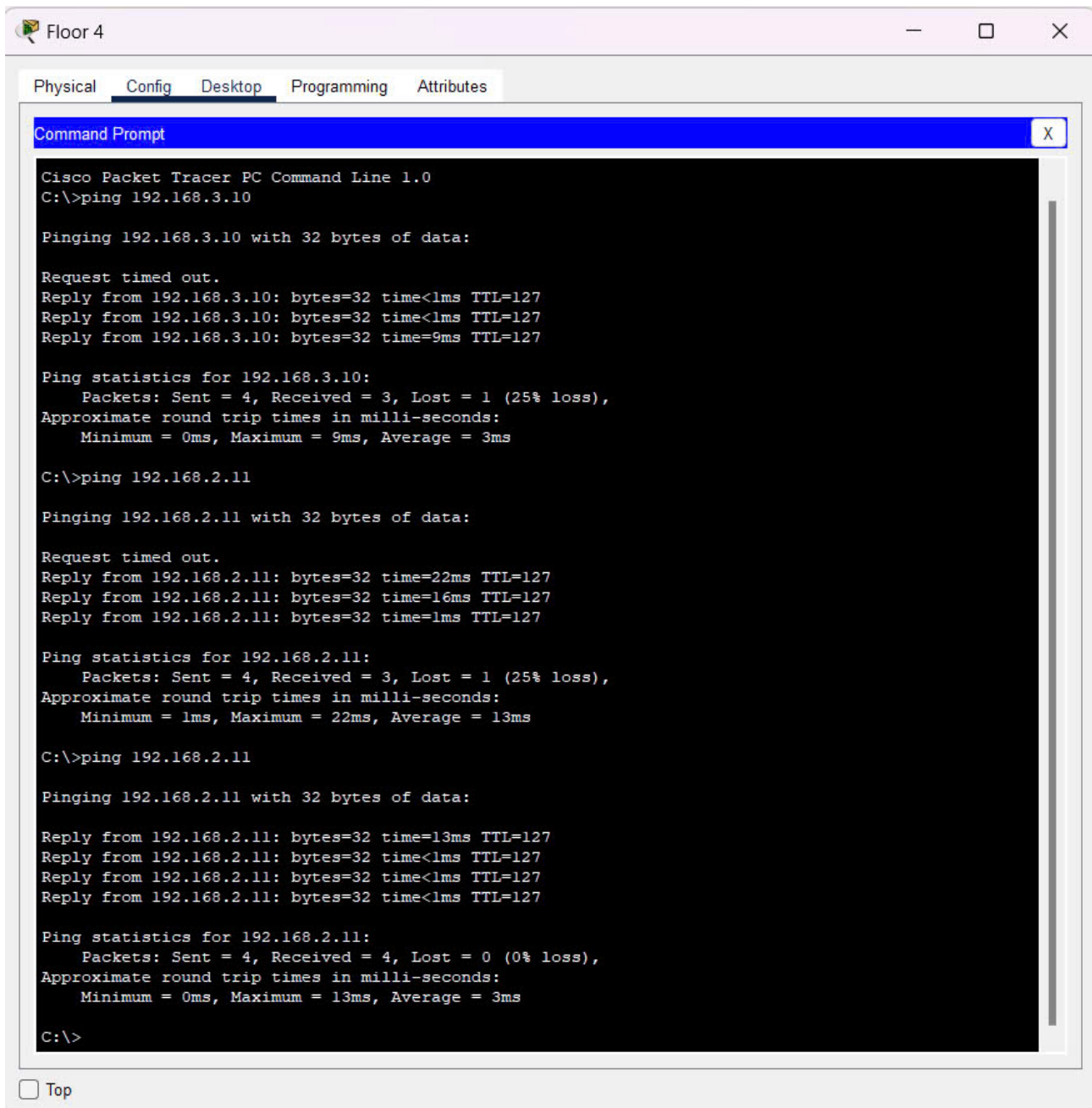
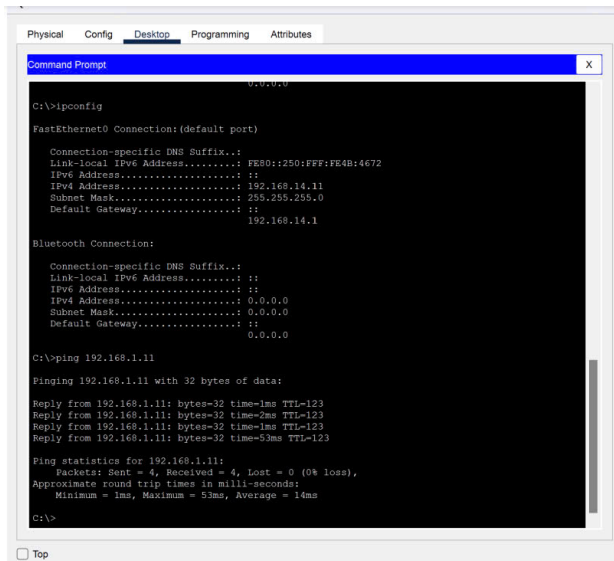


Figure 19: Test PC between VLANs

6.3 Connect PCs between Headquarters and branches



```

C:\>ipconfig

FastEthernet0 Connection: (default port)

    Connection-specific DNS Suffix...: FE80::250:5EFF:FE4B:4672
    Link-local IPv6 Address . . . . .: FE80::250:5EFF:FE4B:4672
    IPv6 Address . . . . .: ::
    IPv4 Address . . . . .: 192.168.14.11
    Subnet Mask . . . . .: 255.255.255.0
    Default Gateway . . . . .: ::

Bluetooth Connection:

    Connection-specific DNS Suffix...: FE80::250:5EFF:FE4B:4672
    Link-local IPv6 Address . . . . .: FE80::250:5EFF:FE4B:4672
    IPv6 Address . . . . .: ::
    IPv4 Address . . . . .: 0.0.0.0
    Subnet Mask . . . . .: 0.0.0.0
    Default Gateway . . . . .: ::
    0.0.0.0

C:\>ping 192.168.1.11

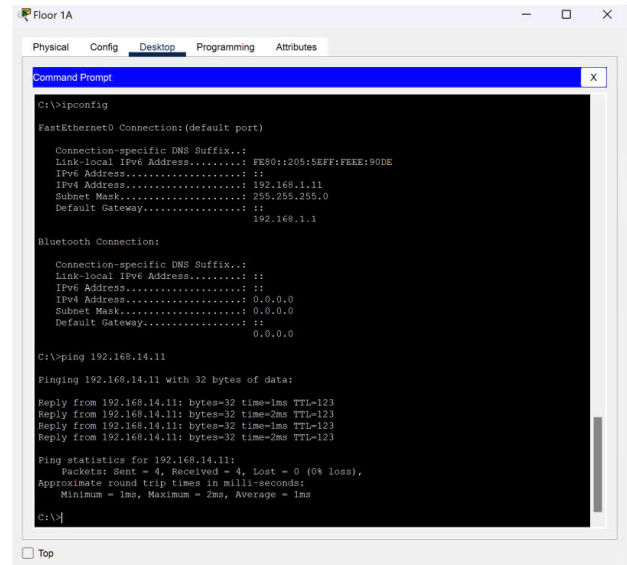
Pinging 192.168.1.11 with 32 bytes of data:

Reply from 192.168.1.11: bytes=32 time=1ms TTL=123
Reply from 192.168.1.11: bytes=32 time=2ms TTL=123
Reply from 192.168.1.11: bytes=32 time=1ms TTL=123
Reply from 192.168.1.11: bytes=32 time=53ms TTL=123

Ping statistics for 192.168.1.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 53ms, Average = 14ms

C:\>
  
```

Figure 20: Test connection from branch to headquarter



```

C:\>ipconfig

FastEthernet0 Connection: (default port)

    Connection-specific DNS Suffix...: FE80::205:5EFF:FE4E:90DE
    Link-local IPv6 Address . . . . .: FE80::205:5EFF:FE4E:90DE
    IPv6 Address . . . . .: ::
    IPv4 Address . . . . .: 192.168.1.11
    Subnet Mask . . . . .: 255.255.255.0
    Default Gateway . . . . .: ::
    192.168.1.1

Bluetooth Connection:

    Connection-specific DNS Suffix...: FE80::205:5EFF:FE4E:90DE
    Link-local IPv6 Address . . . . .: FE80::205:5EFF:FE4E:90DE
    IPv6 Address . . . . .: ::
    IPv4 Address . . . . .: 0.0.0.0
    Subnet Mask . . . . .: 0.0.0.0
    Default Gateway . . . . .: ::
    0.0.0.0

C:\>ping 192.168.14.11

Pinging 192.168.14.11 with 32 bytes of data:

Reply from 192.168.14.11: bytes=32 time=1ms TTL=123
Reply from 192.168.14.11: bytes=32 time=2ms TTL=123
Reply from 192.168.14.11: bytes=32 time=1ms TTL=123
Reply from 192.168.14.11: bytes=32 time=2ms TTL=123

Ping statistics for 192.168.14.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\>
  
```

Figure 21: Test connection from headquarter to branch

6.4 Connect to servers in the DMZ

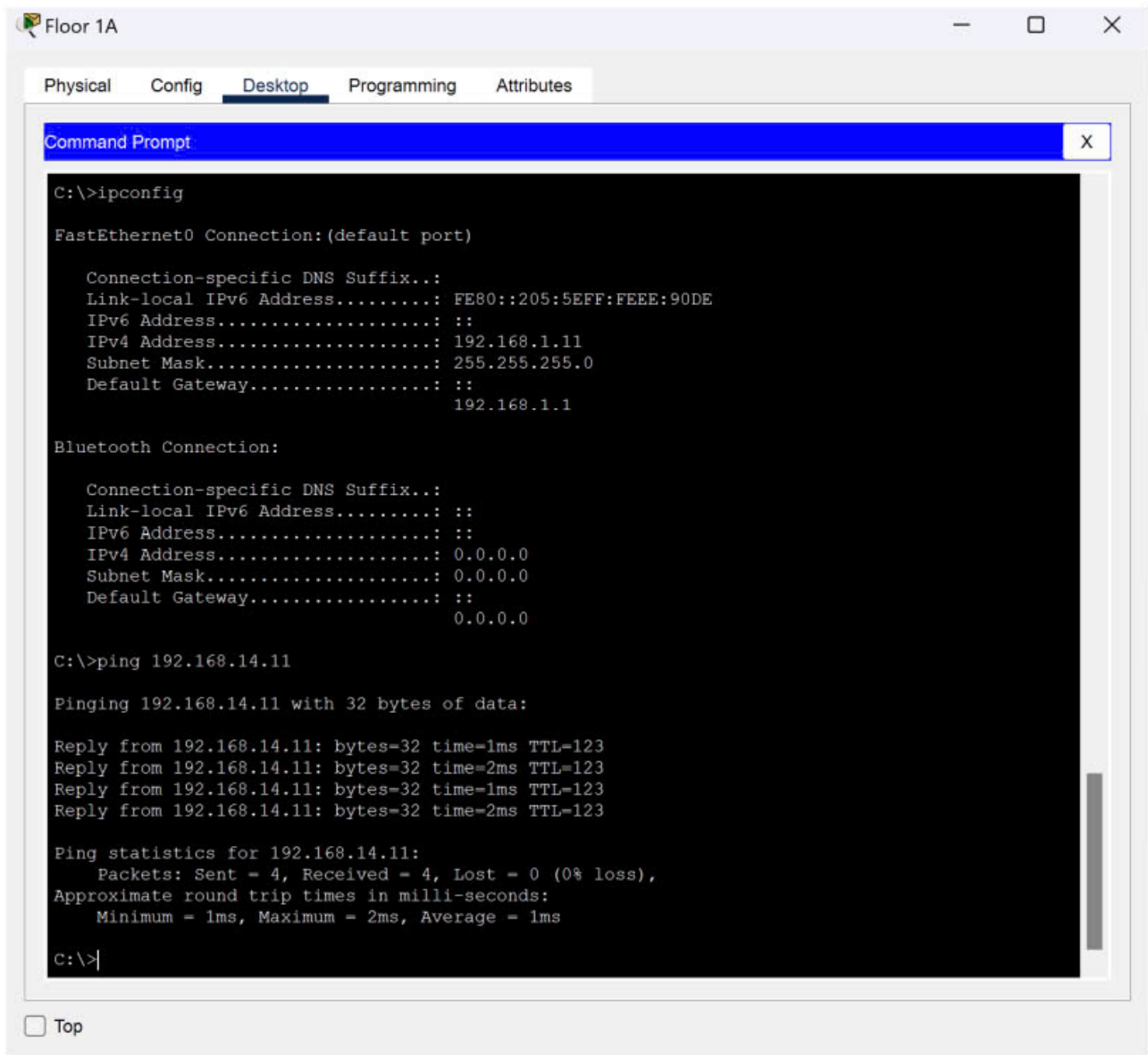


Figure 22: Test connection to server in DMZ

6.5 No connections from Customers' devices to PCs on the LAN

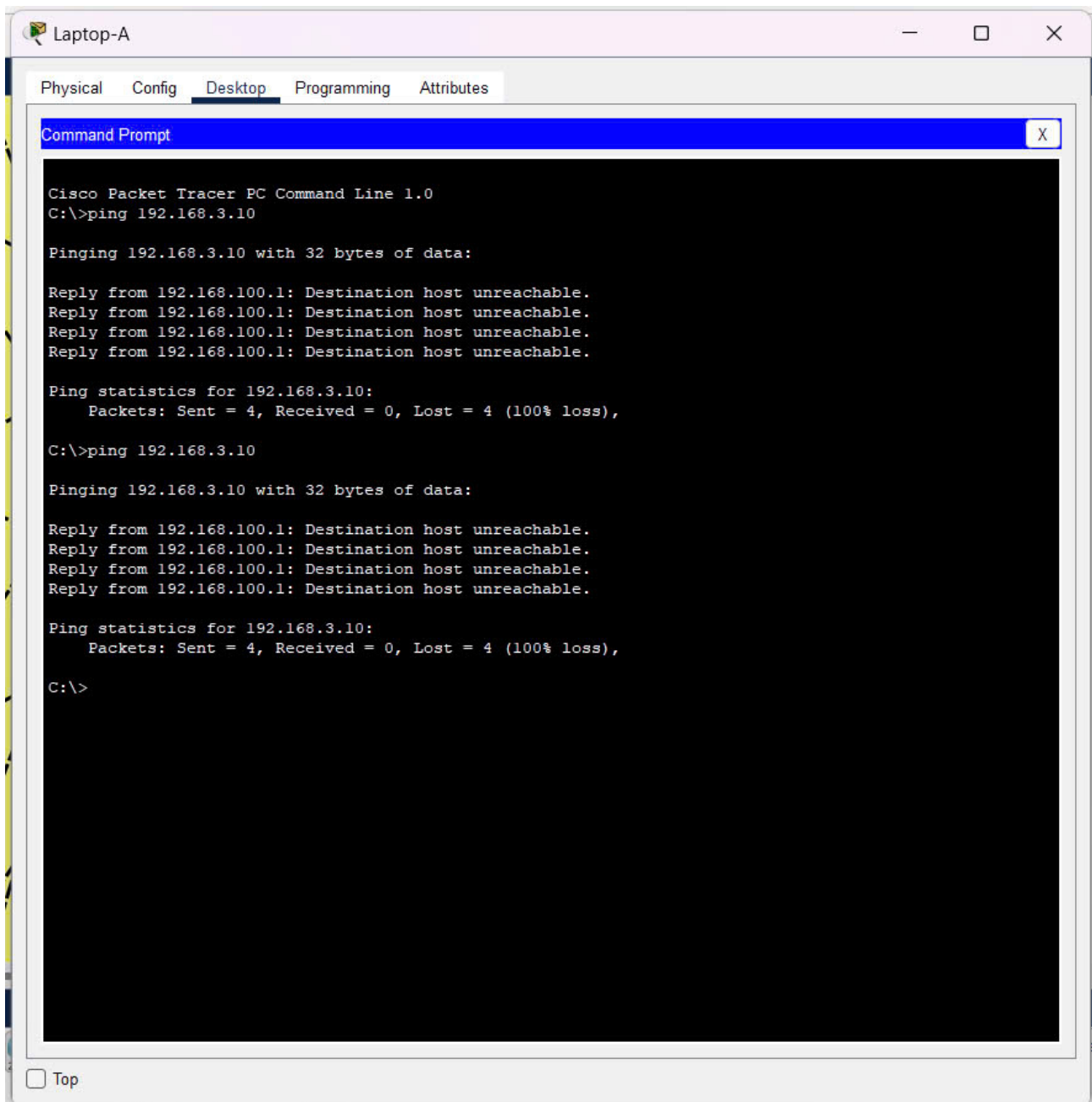


Figure 23: Test customer connection to VLAN

6.6 Connect to the Internet to a Web server

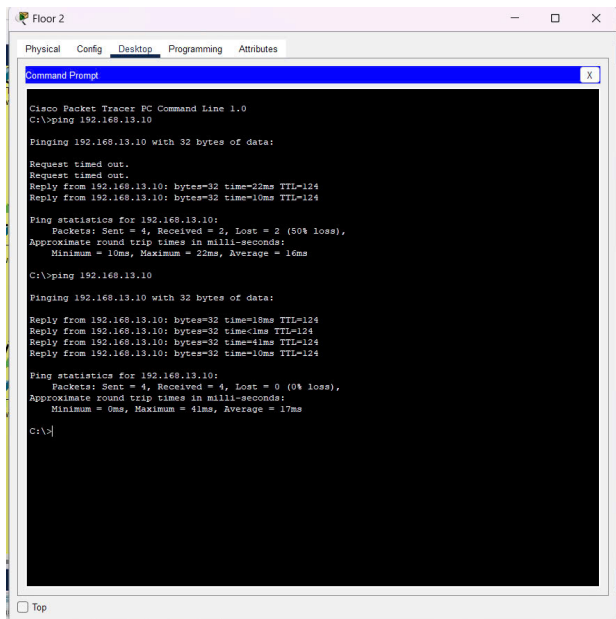


Figure 24: Test connection to Web server

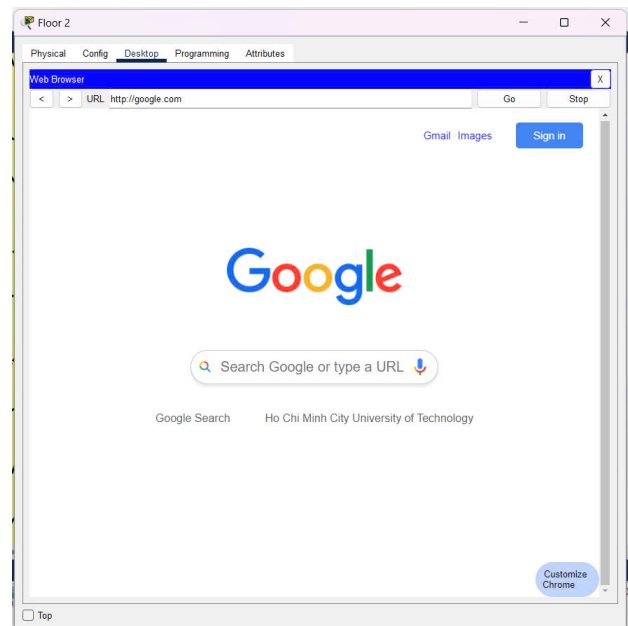


Figure 25: Web server google.com

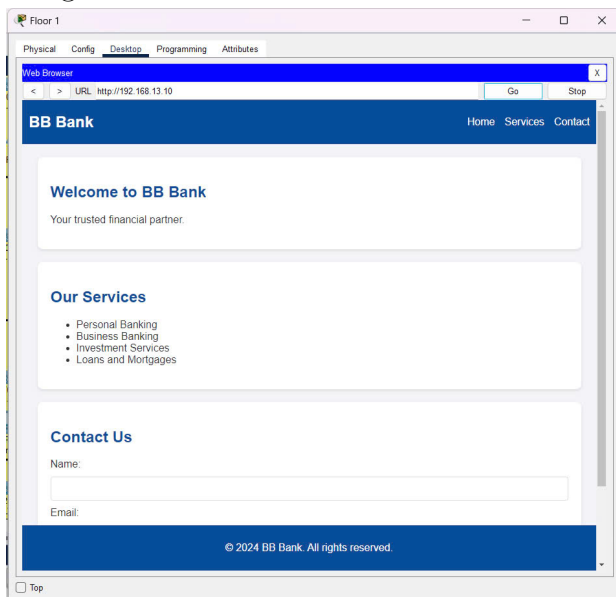


Figure 26: Test Web server

7 Re-evaluation

7.1 Reliability

- Evaluate the system's fault tolerance by simulating network failures (e.g., server downtime, router failure).
- Ensure that load-balancing mechanisms effectively distribute traffic to prevent single points of failure.

7.2 Ease of upgrade

- The modular design of WAN routers allows straightforward hardware and software upgrades. The DMZ ensures services are isolated for minimal disruption during upgrades.
- Adding modular upgrades (e.g., adding new VLANs, servers, or auxiliary sites) is supportive
- Developing IPSEC VPN for site-to-site work and teleworker to work from home.

7.3 Diverse support software safety

- The system can support both licensed and open-source software (HIS, RIS-PACS, CRM, etc.) seamlessly
- Interoperability between client-server and database systems across the main and auxiliary sites is reliable

7.4 Network security

- The firewalls, ACL provide a protective barrier between internal systems and external threats.
- The DMZ is completely isolated

7.5 Remaining problems

- Currently, the firewall configuration is at a basic level, allowing traffic from the internal network to connect externally and managing access to areas such as the DMZ. However, it is necessary to implement more detailed security policies to ensure stricter control over the flow of data between security zones.

- The cost taken of the whole system is high. It should be perfectly balanced along with the performance.

7.6 Development orientation

- Configure additional security layers for the firewall, including traffic filtering and advanced monitoring, to safeguard the system against both external and internal threats.
- Implement IDS(Intrusion Detection System) which effectively detect illegal access of malicious activities or policy violations, a crucial method for maintaining network security and protecting sensitive data from cyber-attacks.
- Expand wireless networks at the headquarters and branch offices using the WPA3 security protocol to ensure the safety of mobile users and IoT devices.
- Continue refining IP address allocation using subnetting to ensure efficient management and network stability as the device count increases..

8 References

1. J. F. Kurose and K. W. Ross, *Computer Networking: A Top-Down Approach*, 7th ed., Pearson, 2017.
2. Basic Firewall Configuration in Cisco Packet Tracer. <https://www.geeksforgeeks.org/basic-firewall-configuration-in-cisco-packet-tracer/>.
3. YouTube Video: Enterprise Networking Projects/ Cisco Packet Tracer Projects Series. <https://www.youtube.com/playlist?list=PLvUOx2WG6R7PMM8UhMWevH75QzGyXOv4g>
4. How to configure wireless network in packet tracer. <https://www.computernetworkingnotes.com/ccna-study-guide/how-to-configure-wireless-network-in-packet-tracer.html>.
5. Related questions and good answers in <https://community.cisco.com/>