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

COMPUTER NETWORK - CO3094

ASSIGNMENT 2 REPORT

Advisor: NGUYỄN PHƯƠNG DUY
Class: CC02
Group: 4
Students: Nguyễn Duy Thành - 1952456
Nguyễn Hoàng Ân - 2152406
Trần Trường Giang - 2152534
Trịnh Hoàng Duy - 2152473

9th April 2024

Contents

1 Introduction

In response to the dynamic growth and expansion plans of BB Bank, CCC (Computer & Construction Concept) has been entrusted with the pivotal task of designing a robust computer network infrastructure for the bank's Headquarters in Ho Chi Minh City and its two Branches in Da Nang and Ha Noi. This report outlines the comprehensive approach undertaken by CCC to address the unique IT requirements of BB Bank and ensure seamless connectivity, enhanced security, and future scalability.

1.1 Headquarters Network Structure

The Headquarters building, spanning seven floors, sets the stage for a state-of-the-art IT infrastructure. Equipped with an IT room and Cabling Central Local on the first floor, the network is designed to accommodate a medium-scale operation featuring 120 workstations, 5 servers, and 12 networking devices. Leveraging cutting-edge technologies, the network incorporates both wired and wireless connections, fiber cabling (GPON), and GigaEthernet 1GbE/10GbE. To enhance organizational efficiency, the network is structured using VLANs to segregate different departments.
Connectivity between the Headquarters and the Branches is established through leased lines for WAN connections, potentially employing SD-WAN and MPLS technologies. Internet access is facilitated by 2 xDSL lines with a load-balancing mechanism. Emphasizing the paramount importance of security, the network integrates firewall, IPS/IDS, and phishing detection mechanisms. Moreover, the report proposes a VPN configuration for site-to-site communication and teleworkers connecting to the Company LAN.

1.2 Branches Network Structure

The Branches, located in Da Nang and Ha Noi, each spanning two floors, are equipped with IT rooms and Cabling Central Local on the first floor. With a smaller scale of operations featuring 30 workstations, 3 servers, and 5 or more networking devices, the design focuses on optimizing resources while ensuring seamless connectivity with the Headquarters.

1.3 WAN Connectivity and Cost Analysis

The report delves into critical decision-making regarding WAN connectivity options between the Headquarters and Branches, evaluating technologies such as SD-WAN, MPLS, and others based on cost-effectiveness. A thorough cost-benefit analysis is provided, outlining options and dissecting the advantages and disadvantages of the selected solution.

1.4 Dataflows and Workload Analysis

Understanding the nature of BB Bank's operations, the report presents a detailed analysis of dataflows and workload distribution during peak hours. With a focus on servers handling software updates, web access, and database activities, as well as individual workstations and WiFi-connected devices, the report estimates daily download and upload requirements, forming the basis for network optimization.

1.5 Scalability and Future Growth

Recognizing the dynamic nature of the banking industry, the report anticipates a 20% growth rate in the BB Bank's network over the next five years. Proactive measures are proposed to accommodate this expansion, including considerations for increased users, network load, and potential branch extensions.
In conclusion, this report encapsulates CCC's strategic approach in designing a sophisticated computer network for BB Bank, aligning with its operational needs, security imperatives, and future growth aspirations. The proposed solutions aim to create a resilient, high-performance network that will serve as a technological backbone for BB Bank's continued success.

2 Network Structure Design

2.1 Network Topology and Hardware Requirements

Headquarters (Ho Chi Minh City):

- Floors: 7
- First Floor:
  - IT Room and Cabling Central Local
- Servers: 5
- Networking Devices: 14s (consider additional security-specific devices)
- Connectivity:
  - Wired and wireless connections
  - Fiber cabling (GPON)
  - GigaEthernet 1GbE/10GbE
- VLAN Structure: Organize the network according to departments
- WAN Connection: Leased lines for interconnecting branches (SD-WAN, MPLS), 2 xDSL for Internet access with load balancing
- Security: Firewall, IPS/IDS, phishing detection
- Software: Mix of licensed and open-source software
- High Availability: Implement redundancy and failover mechanisms

Each branch: Da Nang and Ha Noi

- Floors: 2
- First Floor:
  - IT Room and Cabling Central Local
- Servers: 3
- Networking Devices: 5 (consider additional devices)

- Connectivity: Interconnect with Headquarters using selected WAN technology
- Security: Implement firewall and basic security measures
- Software: Use standard office applications and required banking software

2.2 VPN Configuration

Site-to-Site VPN:

- Use IPSec for secure communication between Headquarters and Branches.

Teleworker VPN:

- Implement SSL VPN for remote employees connecting to the Company LAN securely.

2.3 WAN Connection Technology

Options:

- SD-WAN: Cost-effective, efficient use of multiple connections.
- MPLS: Reliable and secure, but may be more expensive.

Cost Analysis:

- Compare initial setup costs and recurring expenses.
- Consider long-term scalability and ease of management.

Advantages and Disadvantages:

2.3.0.1 SD-WAN:

- Advantages: Cost-effective, flexible, easy to manage.
- Disadvantages: May have lower security compared to MPLS.

2.3.0.2 MPLS:

- Advantages: High security, reliable, suitable for critical applications.
- Disadvantages: Higher cost, potential for longer implementation.

2.4 Network System Requirements and Scalability

- Growth Rate: Plan for a 20
- Traffic Analysis: Peak hours, dataflow, and workload considerations.
- Network Load Balancing: Implement load balancers at critical points for optimal performance.
- Device Configuration: Choose devices based on high-load areas.

2.5 Network Structure and Aesthetics

- Building Architecture: Design network structure considering aesthetics.
- Wireless Environment: Ensure secure wireless access points (WAPs).
- Network Security Standards: Implement standard security protocols (firewalls, DMZ).
- Server Farm: Centralize servers in a secure server farm.
- Partitioning: Set up partitions for network servers and devices (e.g., DMZ for external-facing services).

2.6 Checklist for Installation Locations

- Verify the availability of power outlets.
- Confirm physical security measures.
- Check for cable pathways and accessibility.
- Validate network coverage for wireless environments.

3 Technical Requirements

3.1 List of Minimum Equipment

Headquarters:

- Switches:
  - Quantity: 2 x 48-port GigaEthernet switches for workstations
  - Quantity: 1 x 24-port GigaEthernet switch for servers
  - Quantity: 1 x 12-port GigaEthernet switch for networking devices
- Routers:
  - Quantity: 1 x Router with SD-WAN capabilities or MPLS support
  - Quantity: 1 x Firewall/Security Appliance
- Access Points:
  - Quantity: Sufficient wireless access points for complete coverage
- Servers:
  - Quantity: 5 x Servers with recommended specifications
- Cabling:
  - Quantity: Sufficient Cat6 cables for workstations, servers, and networking devices
  - Quantity: Fiber optic cables for GPON connections
- Security Devices:

  - Quantity: 1 x Intrusion Prevention System (IPS)
  - Quantity: 1 x Phishing Detection Appliance
- Teleworker VPN:
  - Quantity: Licenses for SSL VPN connections

Branches:

- Switches:
  - Quantity: 1 x 24-port GigaEthernet switch for workstations
  - Quantity: 1 x 12-port GigaEthernet switch for servers and networking devices
- Router/Firewall:
  - Quantity: 1 x Router/Firewall for basic security
- Access Points:
  - Quantity: Sufficient wireless access points for complete coverage
- Servers:
  - Quantity: 3 x Servers with recommended specifications
- Cabling:
  - Quantity: Sufficient Cat6 cables for workstations, servers, and networking devices

3.2 Subnet Size

The subnet mask we have employed is 255.255.255.0, yielding a capacity for hosts represented by 2^8, which is equivalent to 256. This allocation proves sufficient to meet the numerical demands for workstation.

3.3 IP Plan

Headquarters:

- VLAN10: First Floor: IT room, Receptionist - 192.168.2.0/24
- VLAN20: Second Floor: Offices - 192.168.3.0/24
- VLAN30: Third Floor: First Floor: Offices - 192.168.4.0/24
- VLAN40: Fourth Floor: Offices - 192.168.5.0/24
- VLAN50: Fifth Floor: Offices - 192.168.6.0/24
- VLAN60: Sixth Floor: Offices - 192.168.7.0/24
- VLAN70: Seventh Floor: Chairman - 192.168.8.0/24

Branch in Ha Noi

- VLAN10: First Floor: - 192.170.1.0/24
- VLAN20: Second Floor - 192.170.2.0/24

Branch in Da Nang

- VLAN10: First Floor: - 192.169.1.0/24
- VLAN20: Second Floor - 192.169.2.0/24

3.4 Wiring Diagram (Cabling)

Headquarters:

- IT Room: Centralized patch panels for workstations, servers, and networking devices
- Cabling Central Local: Distribution of cables to respective floors and departments
- Fiber Cabling: GPON connections for high-speed data transfer

Branches:

- IT Room: Patch panels for workstations, servers, and networking devices
- Cabling Central Local: Distribution of cables within the building

3.5 Recommended Equipment and Specifications

- Switches:
  - Model: Cisco Catalyst 2960X Series
  - Specifications: 48-port GigaEthernet, Layer 2/Layer 3 capabilities
- Router/Firewall:
  - Model: Cisco ISR 4000 Series
  - Specifications: SD-WAN capable, or MPLS support, integrated firewall
- Access Points:
  - Model: Cisco Aironet 2800 Series
  - Specifications: Dual-band, high-performance wireless access points
- Servers:
  - Model: Dell PowerEdge R640
  - Specifications: Dual processors, ample RAM and storage
- Cabling:
  - Type: Cat6 for Ethernet, Fiber optic for GPON
  - Specifications: Compliant with industry standards

- Security Devices:
  - IPS: Cisco Firepower Next-Generation IPS
  - Phishing Detection: Cisco Email Security Appliance
- VPN Solution:
  - Model: Cisco AnyConnect for SSL VPN

3.6 WAN Connection Diagram (Using SD-WAN, MPLS, and OSPF Routing)

- SD-WAN Configuration:
  - Utilize multiple ISP connections for redundancy and load balancing.
  - Implement SD-WAN controllers for intelligent routing and traffic optimization.
- MPLS Configuration:
  - Establish MPLS connections between Headquarters and Branches for secure and reliable communication.
  - Implement OSPF routing protocol for dynamic route management within the MPLS network.
- Connection Redundancy:
  - Ensure fail-over mechanisms for both SD-WAN and MPLS connections.
- Firewall Configuration:
  - Implement firewall rules to control traffic between Headquarters and Branches.

4 Technical Configuration

4.1 Headquarters Wired Network

The system load and capacity parameters (concentrated around 80% during peak hours from 9 AM to 11 AM and 3 PM to 4 PM) are applicable to both the Headquarters and Branches.

- 5 servers with a total download and upload capacity of 1000MB/day. Peak-hour concentration for 3 hours, with 80% focus during the day.
  - Peak-hour Bandwidth: Bandwidth $= \frac{5\times100\times0.8\times8}{3\times3600} = 2.96$ (Mbps)
  - Peak-hour Throughput: Throughput $= \frac{5\times1000\times8}{3\times3600} = 1.93$ (Mbps)
- 200 workstations with a total download and upload capacity of 500MB/day. Peak-hour concentration for 3 hours, with 80% focus during the day.
  - Peak-hour Bandwidth: Bandwidth $= \frac{200\times500\times0.8\times8}{3\times3600} = 59.3$ (Mbps)
  - Peak-hour Throughput: Throughput $= \frac{200\times500\times8}{3\times3600} = 27.8$ (Mbps)

4.2 Headquarters Wireless Network

- The WiFi-connected laptop is intended for customers to access approximately 1000MB per day. The total peak-hour usage time is 3 hours, with 80% of the day's activities concentrated during peak hours. Assuming there are about 100 regular access sessions within this timeframe:
  - Peak-hour Bandwidth: Bandwidth $= \frac{100 \times 1000 \times 0.8 \times 8}{3 \times 3600} = 59.3$ (Mbps)
  - Peak-hour Throughput: Throughput $= \frac{100 \times 1000 \times 8}{3 \times 3600} = 27.8$ (Mbps)

4.3 Branch Wired Network

- 3 servers with a combined download and upload capacity of 1000MB per day. The total peak-hour usage time is 3 hours, with 80% of the day's activities concentrated during peak hours.
  - Peak-hour Bandwidth: Bandwidth $= \frac{3 \times 1000 \times 0.8 \times 8}{3 \times 3600} = 1.78$ (Mbps)
  - Peak-hour Throughput: Throughput $= \frac{3 \times 1000 \times 8}{3 \times 3600} = 0.83$ (Mbps)
- 100 workstations with a total download and upload capacity of 500MB per day. The total peak-hour usage time is 3 hours, with 80% of the day's activities concentrated during peak hours.
  - Peak-hour Bandwidth: Bandwidth $= \frac{100 \times 500 \times 0.8 \times 8}{3 \times 3600} = 29.6$ (Mbps)
  - Peak-hour Throughput: Throughput $= \frac{100 \times 500 \times 8}{3 \times 3600} = 13.9$ (Mbps)

4.4 Branch Wireless Network

- The Wi-Fi-connected laptop is designed for customer usage, allowing access to approximately 1000MB per day. The total peak-hour usage time is 3 hours, with 80% of the day's activities concentrated during peak hours. Assuming there are about 50 regular access sessions throughout the day:
  - Peak-hour Bandwidth: Bandwidth $= \frac{50 \times 1000 \times 0.8 \times 8}{3 \times 3600} = 29.6$ (Mbps)
  - Peak-hour Throughput: Throughput $= \frac{50 \times 1000 \times 8}{3 \times 3600} = 13.9$ (Mbps)

4.5 Safety Parameters

- The computer network system of the company is projected to experience a growth rate of 20%. Therefore, the minimum bandwidth required for the system to operate smoothly is
  - Bandwidth $= 2.96 + 59.3 + 59.3 + 2 \times (1.78 + 29.6 + 29.6) = 243.52$ (Mbps)
  - Predicted 20% growth: Bandwidth $\times 1.2 = 292.224 \approx 292$ (Mbps)
- The computer network system of the company is projected to experience a growth rate of 20%. Therefore, the minimum throughput required for the system to operate smoothly is
  - Throughput $= 1.39 + 27.8 + 27.8 + 2 \times (0.83 + 13.9 + 13.9) = 114.25$ (Mbps)
  - Predicted 20% growth: Throughput $\times 1.2 = 127.1 \approx 137$ (Mbps)

5 Network Map Design

5.1 Headquarters

The connection in the Headquarters is internal VLANs, distributed by a multilayer switch `MS_0`. We also use a Cisco ASA `ASA0` (Adaptive Security Appliance) as a firewall between different VLANs within the building.

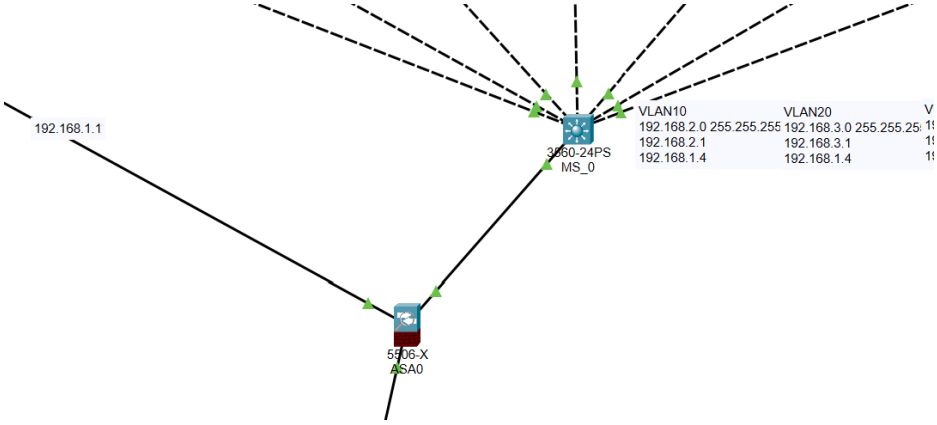

Figure 1: Connection in Headquarters

The first floor is designated for hosting servers, housing a Web server, FTP server, Mail server, and DNS server all interconnected through a server switch (SW1). Additionally, a switch is set up to link to the multilayer switch, with two network devices connected to this switch.

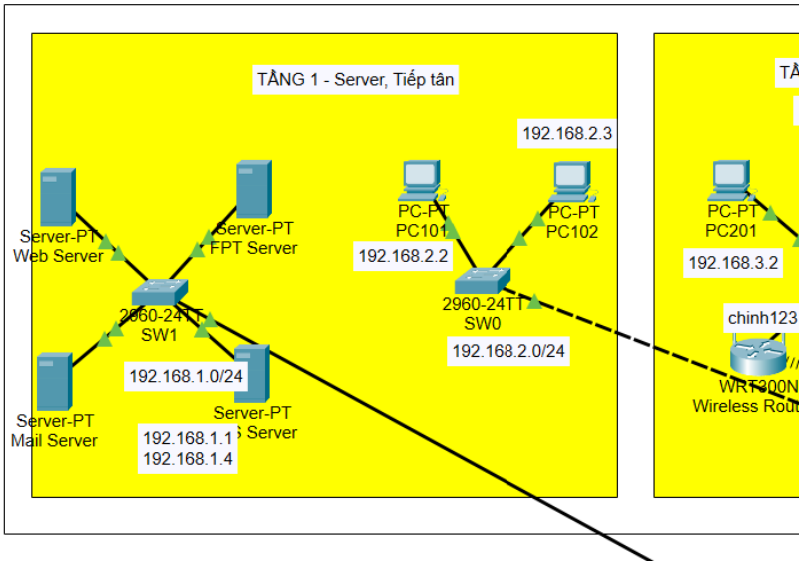

Figure 2: Headquarters - 1st floor

All six remaining floors are equipped with a switch and two network devices each. In addition,

the second floor provides a wireless router for wireless connections. The chairman's office on the seventh floor is equipped with a server SV4 to maximize bandwidth and connection speed.

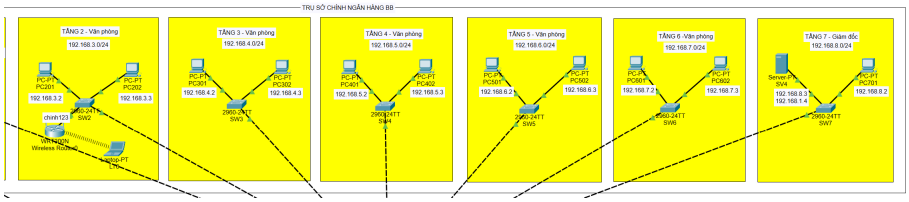

Figure 3: Headquarters - Other floors

5.2 Branch

Granted that 2 branches has the same structure, we will only take the branch Hanoi into illustration.
The first floor is designated for hosting servers, housing a Web server, FTP server, and DNS server all interconnected through a server switch SW1. Additionally, an other switch SW2 is geared for 2 network devices: NT_T1_PC1 and NT_T1_PC2

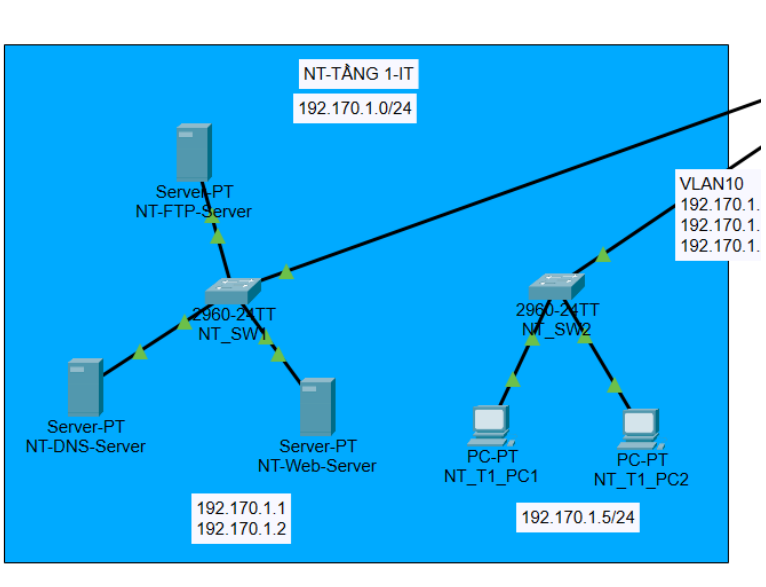

Figure 4: Branch - 1st floor

The second floor is set up with switch SW3 for 2 network devices: NT_T2_PC1 and NT_T2_PC2. In addition, the second floor provides a wireless router for wireless connections.

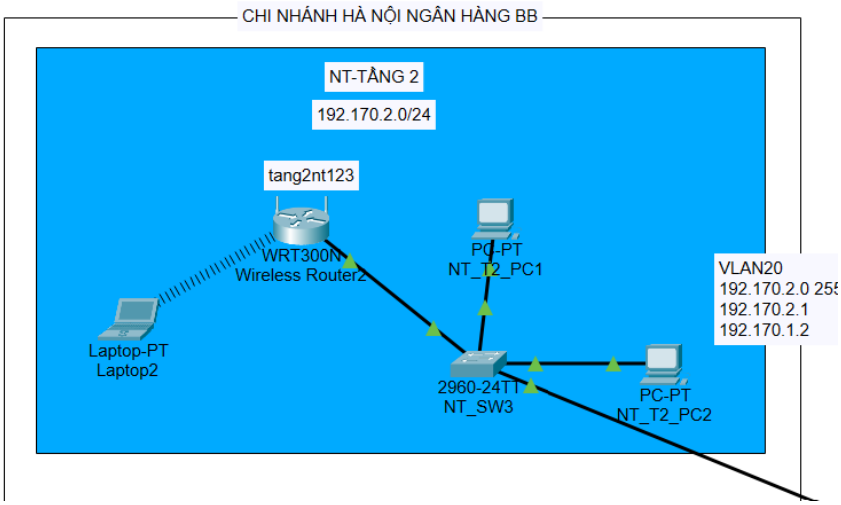

Figure 5: Branch - 2nd floor

5.3 Internet Connection

To establish robust connections between branches and headquarters, a comprehensive infrastructure has been implemented. For each branch or headquarters, a sophisticated setup features two Cisco GigE High Speed WICs `1941` and a Cisco ISR4321/K9 Router `ISR4321`, ensuring reliable and high-speed interconnectivity. Enhancing the internal network within each branch, we've incorporated two essential components, the multilayer switches `MS1` and `MS2`, providing advanced network management capabilities.
Furthermore, to facilitate seamless access to the Internet, a dedicated DSL modem router `DSL Modem0` has been integrated into the network architecture. This modem is complemented by the presence of a server, `Server0`, strategically positioned to optimize bandwidth utilization and enhance overall connection speed.

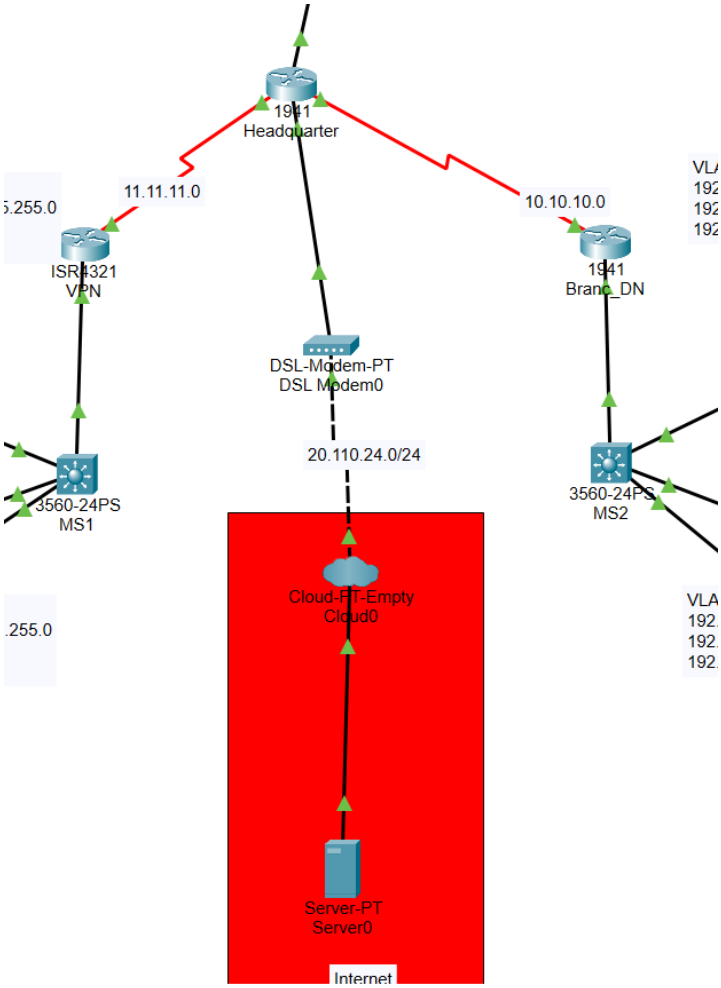

Figure 6: Internet Connection

6 Functional Testing

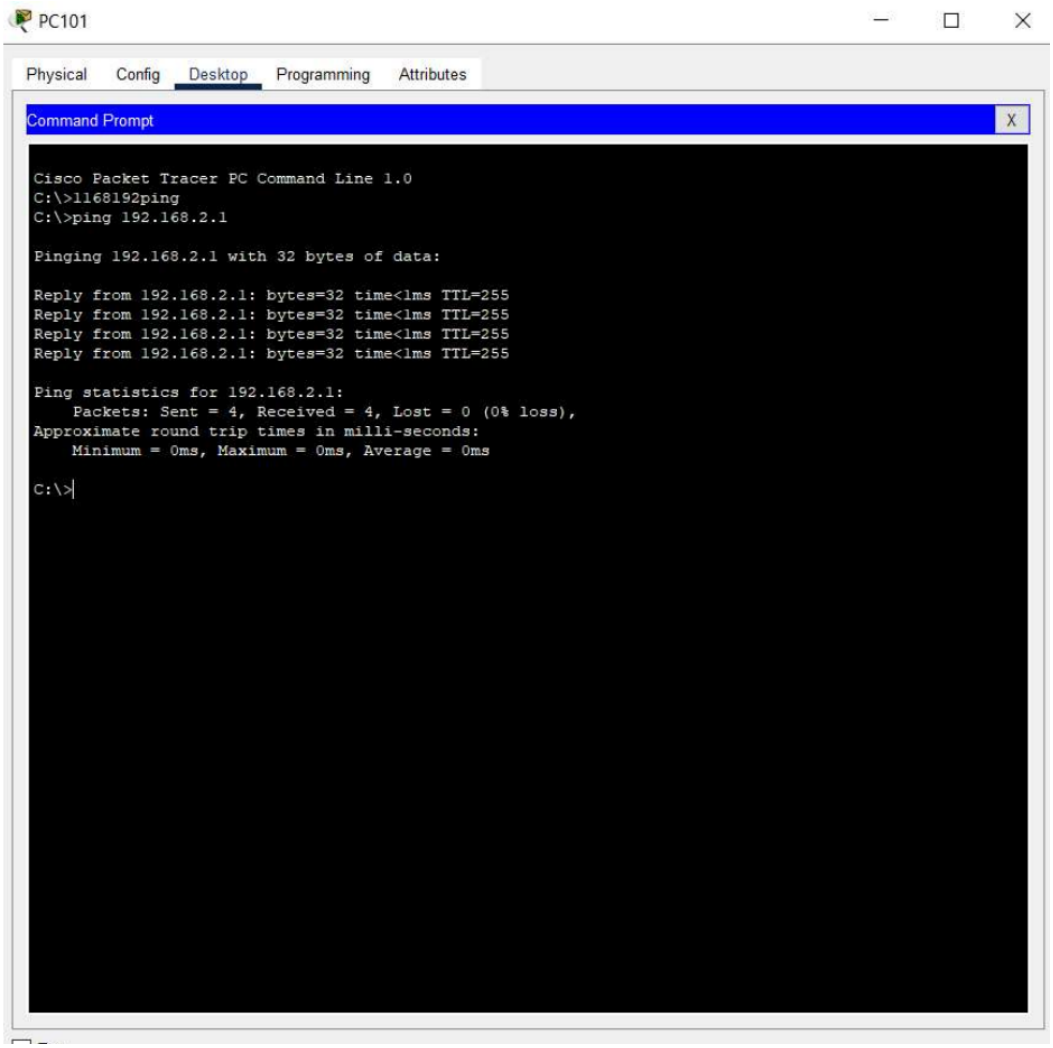

Figure 7: Ping within the VLAN internally

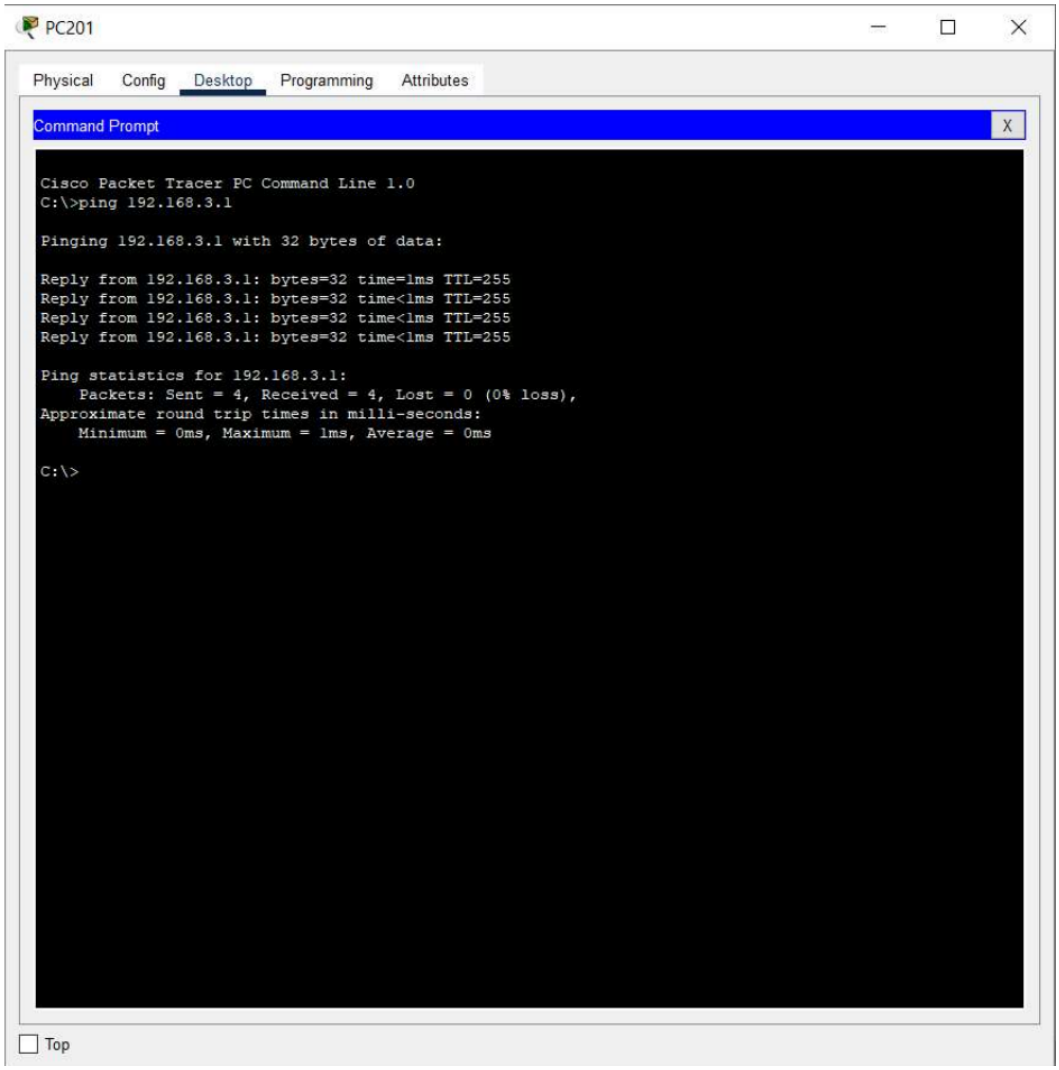

Figure 8: Ping within the VLAN internally

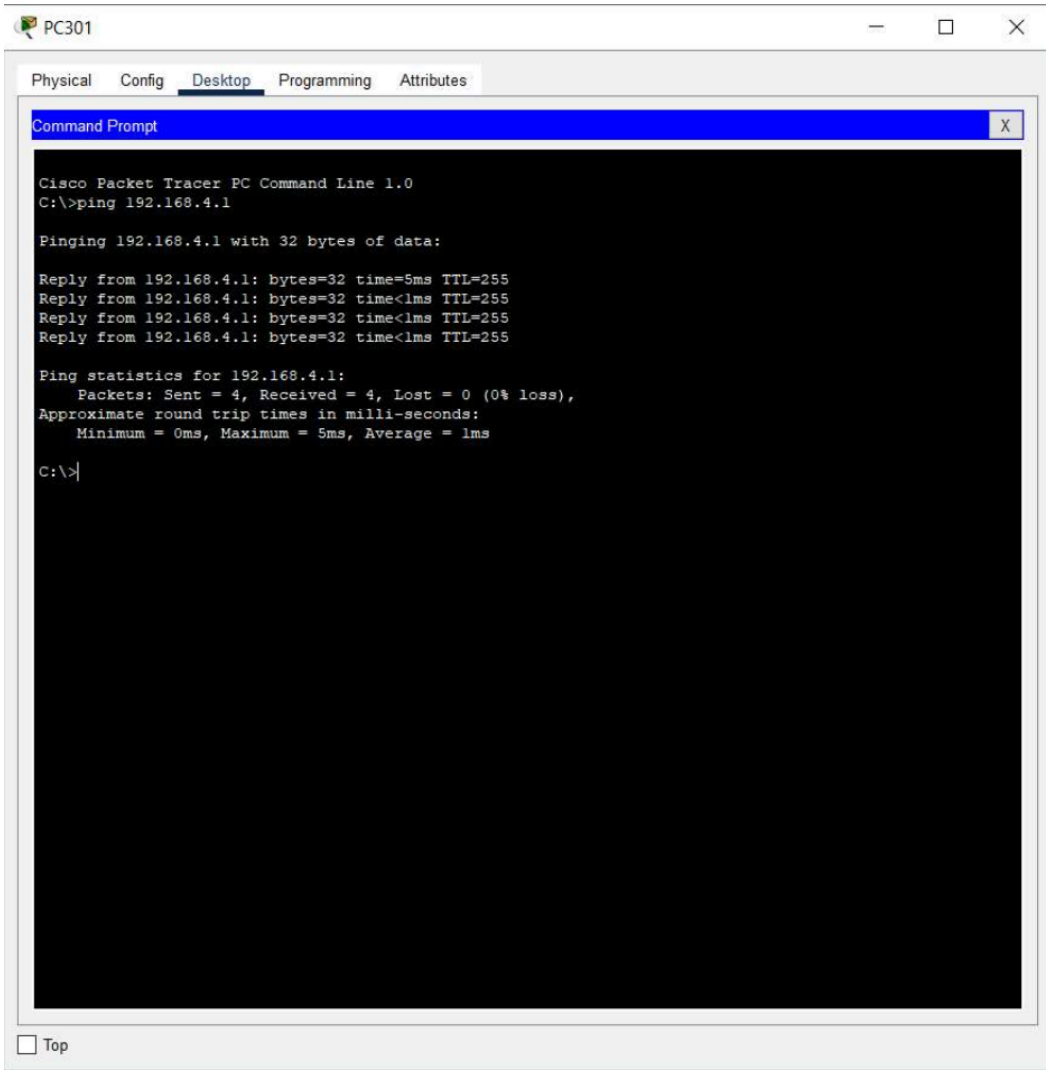

Figure 9: Ping within the VLAN internally

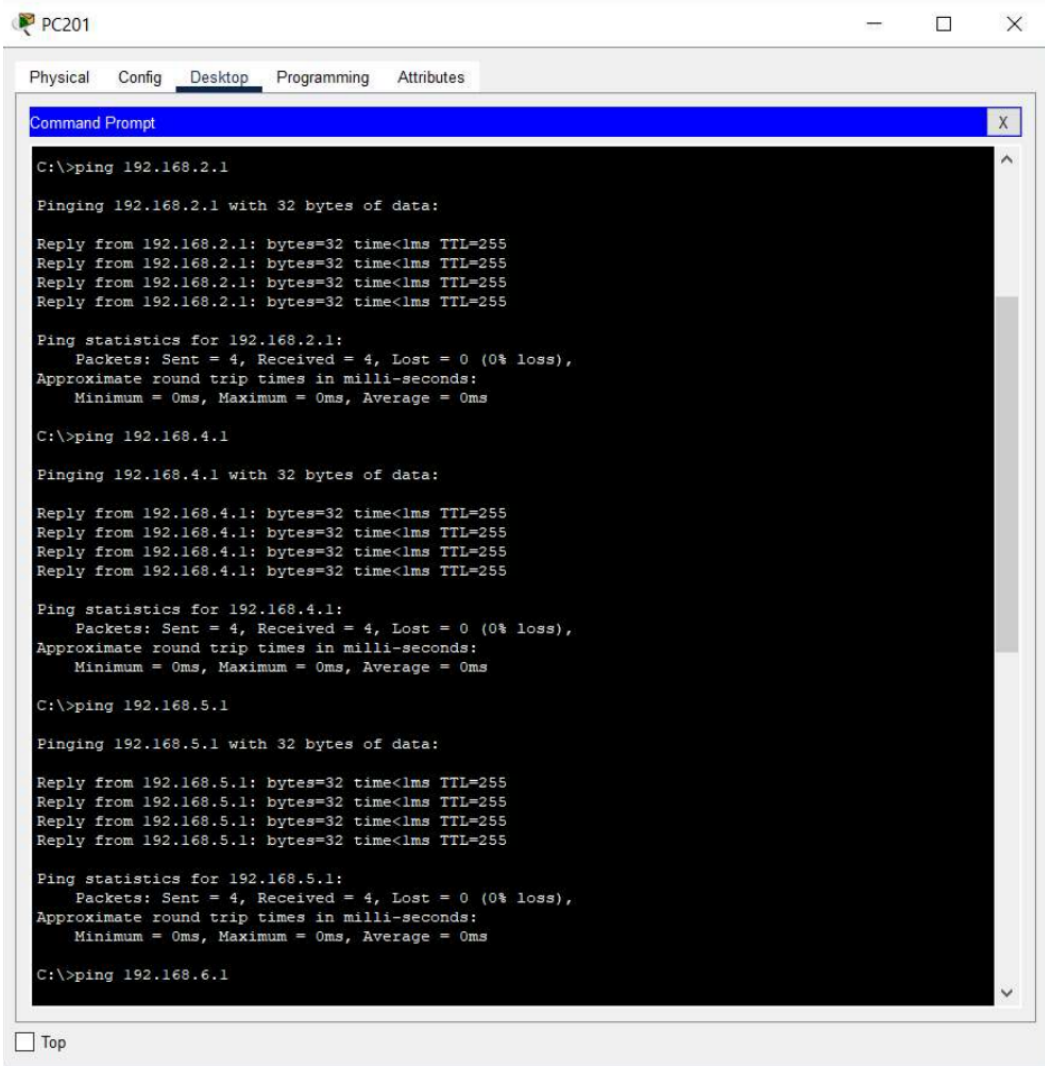

Figure 10: Ping between VLANs

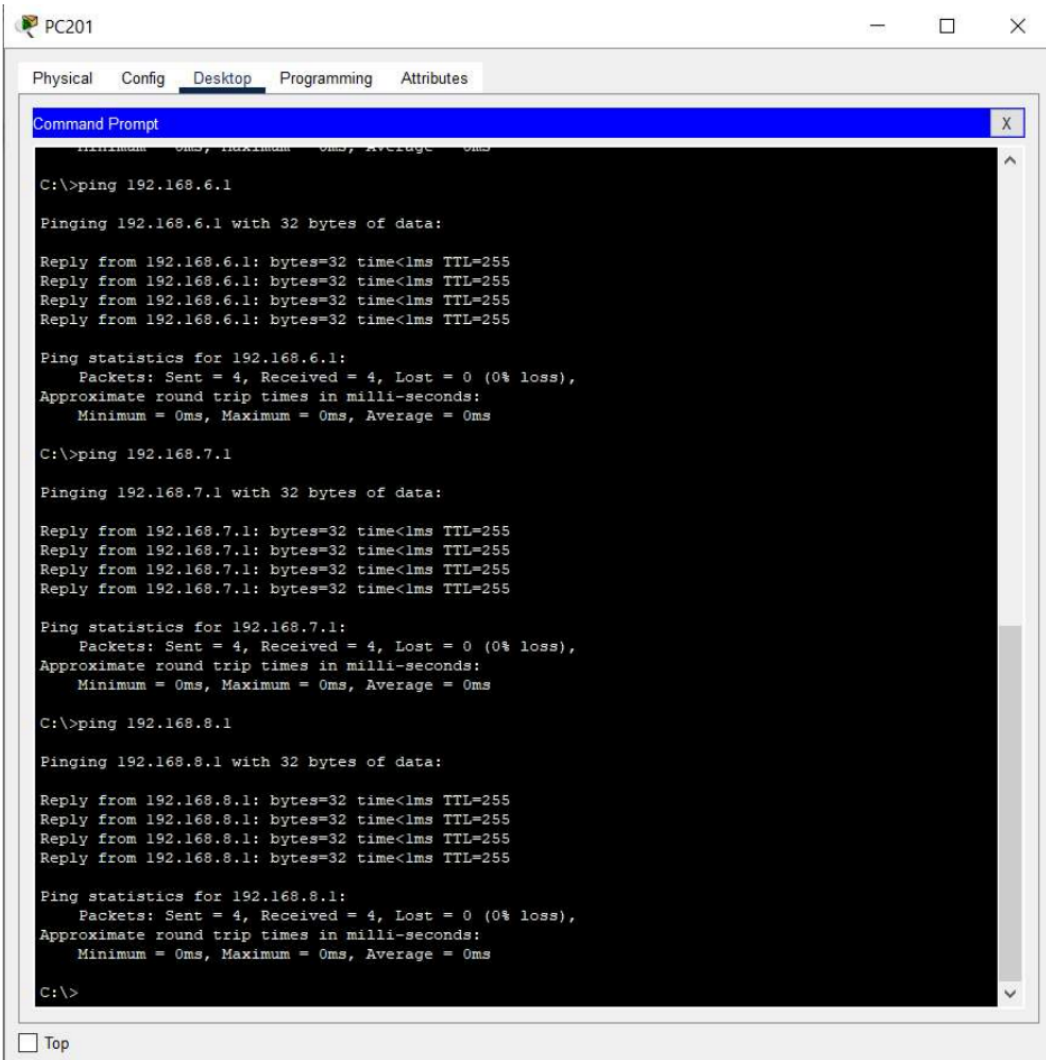

Figure 11: Ping between VLANs

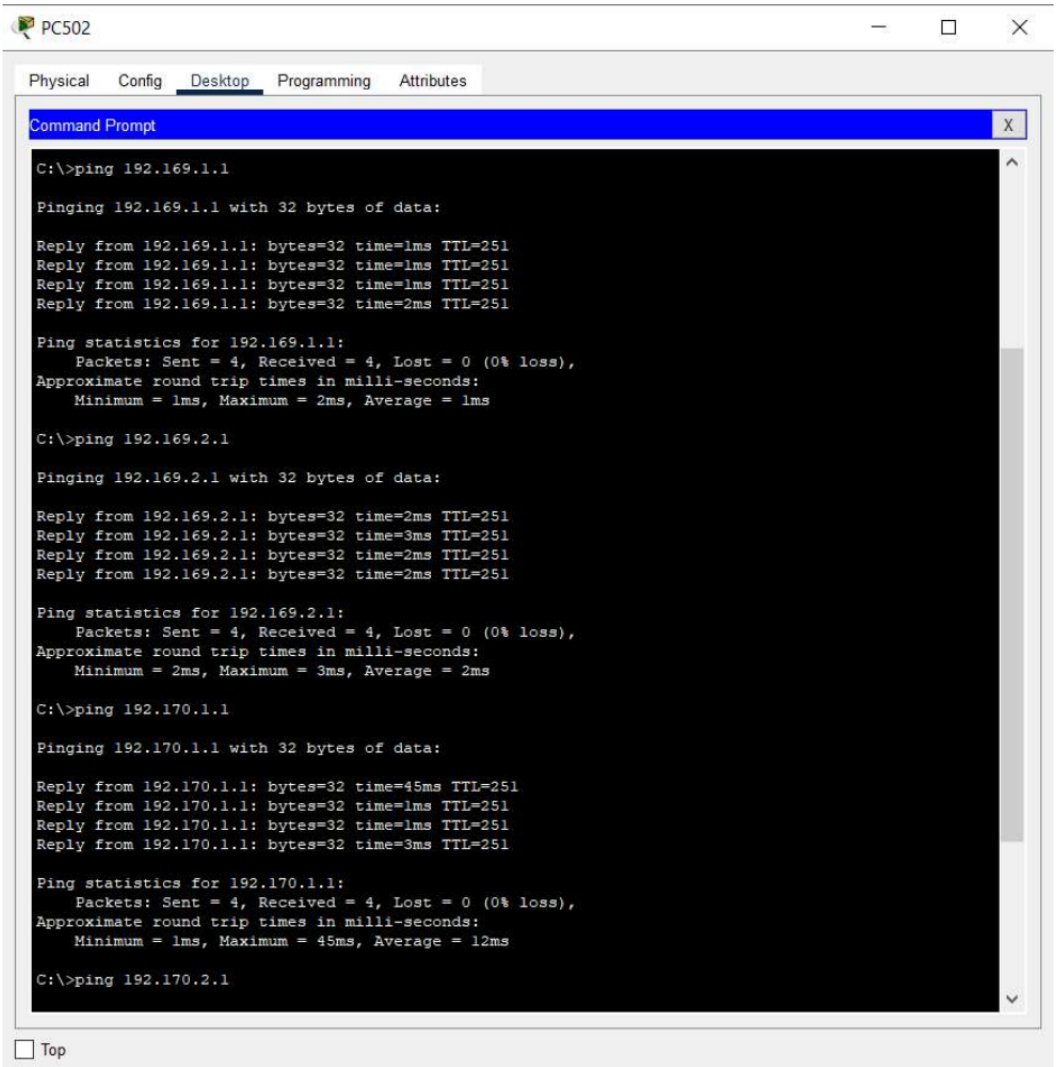

Figure 12: Ping to Branch Ha Noi

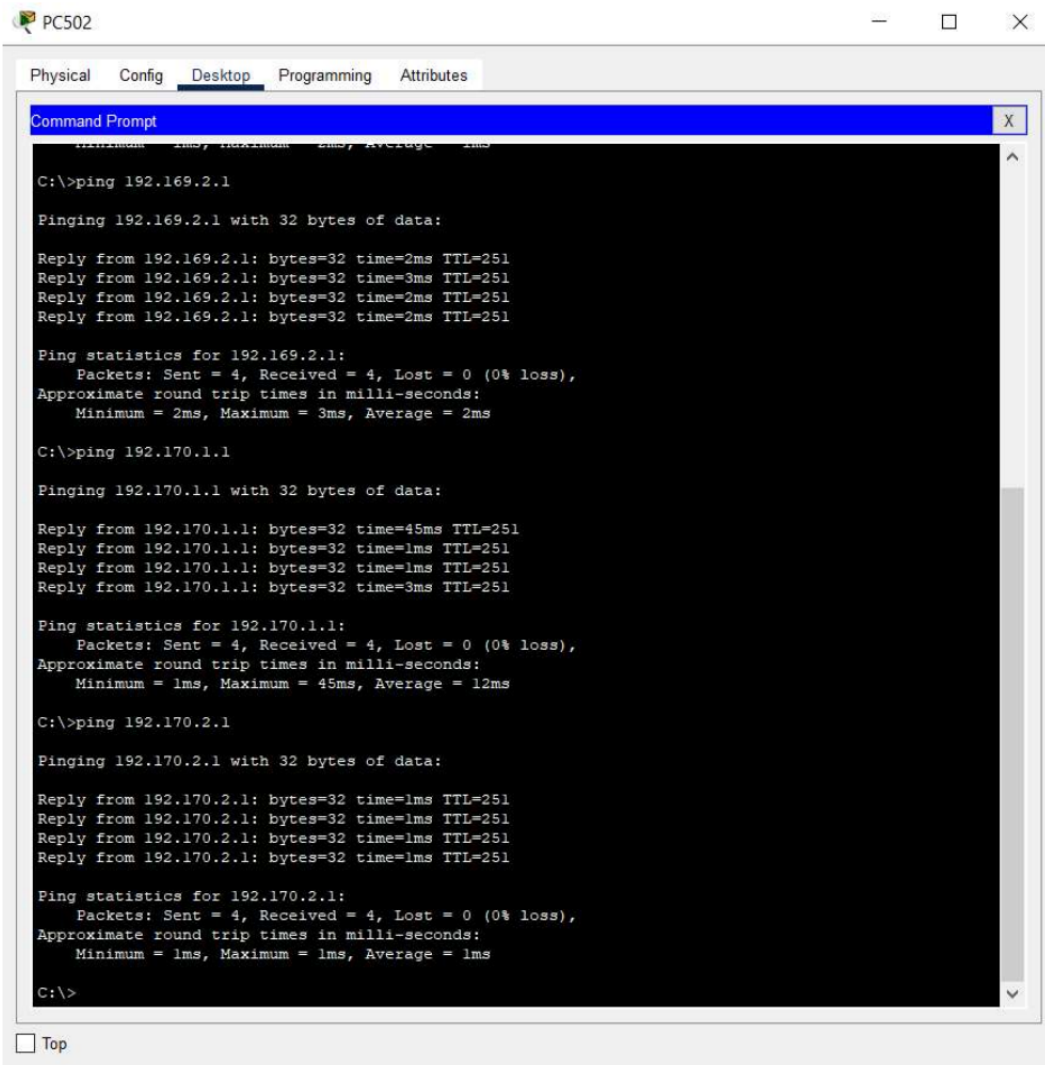

Figure 13: Ping to branch Da Nang

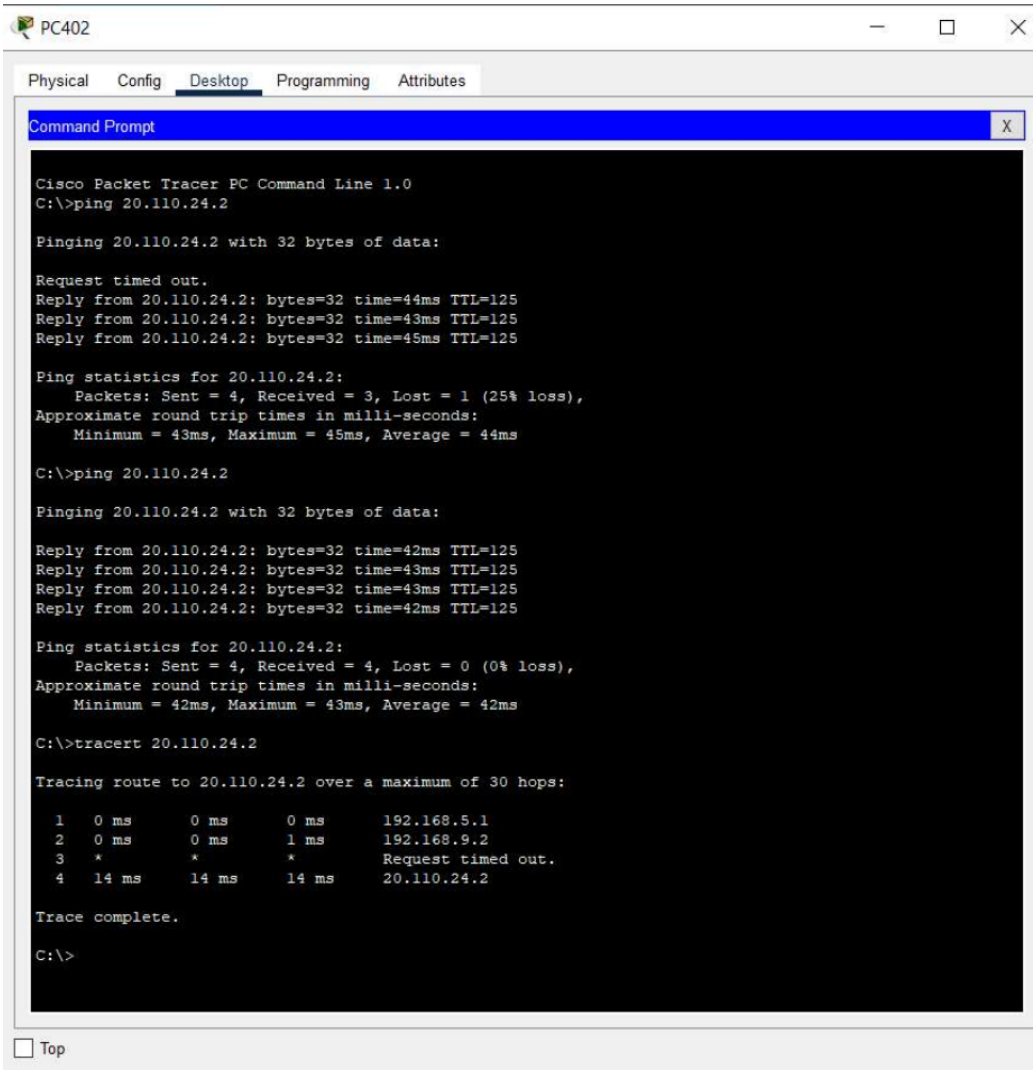

Figure 14: Ping to Internet

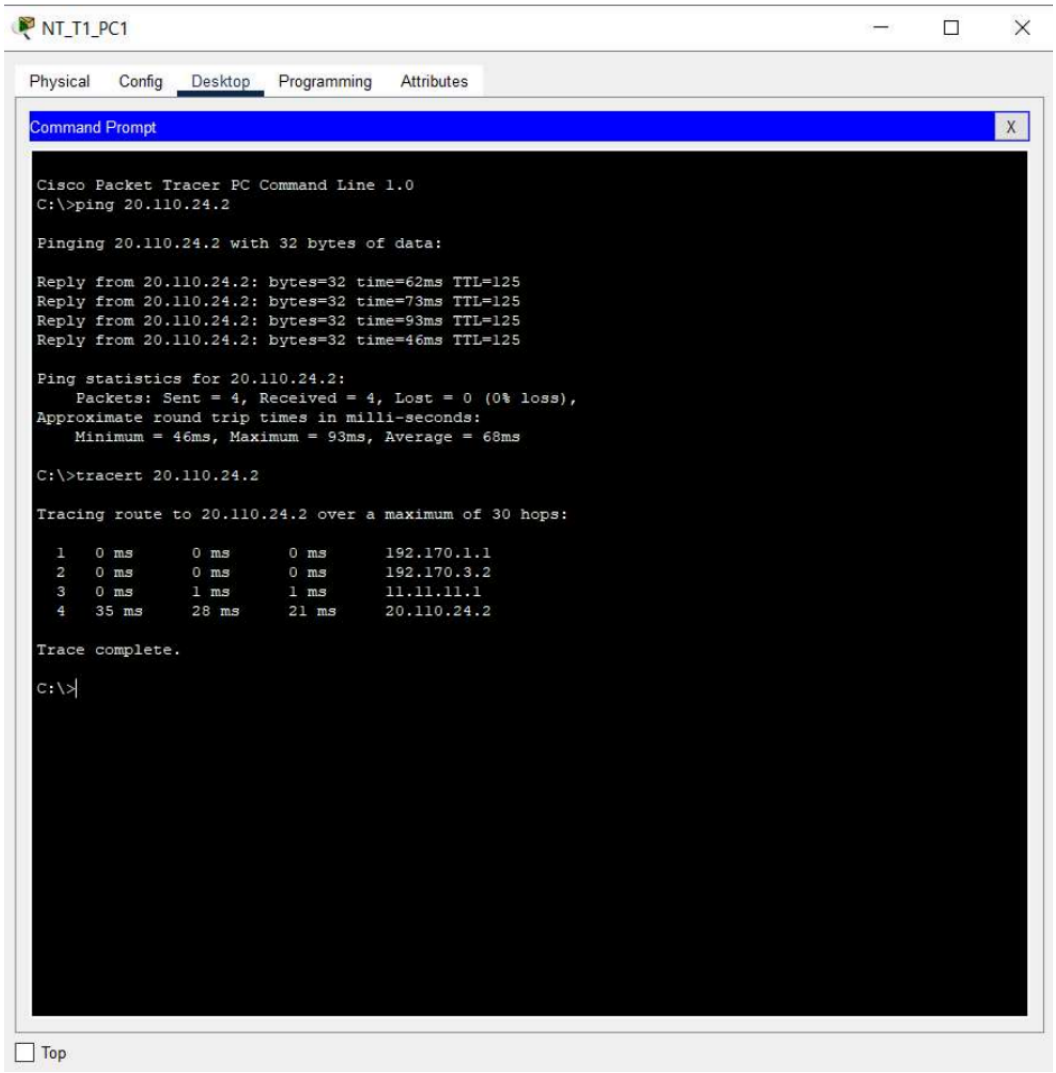

Figure 15: Ping to Internet

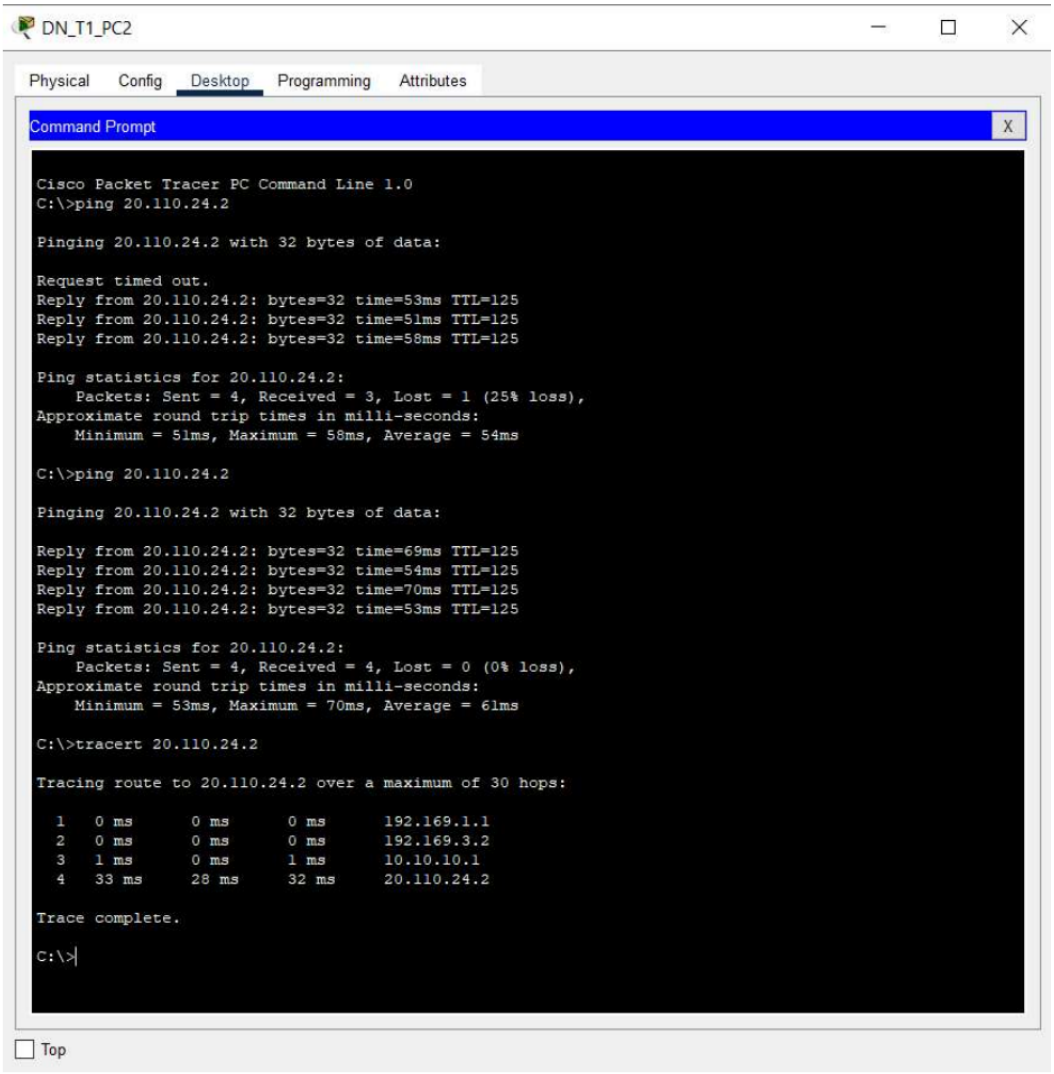

Figure 16: Ping to Internet

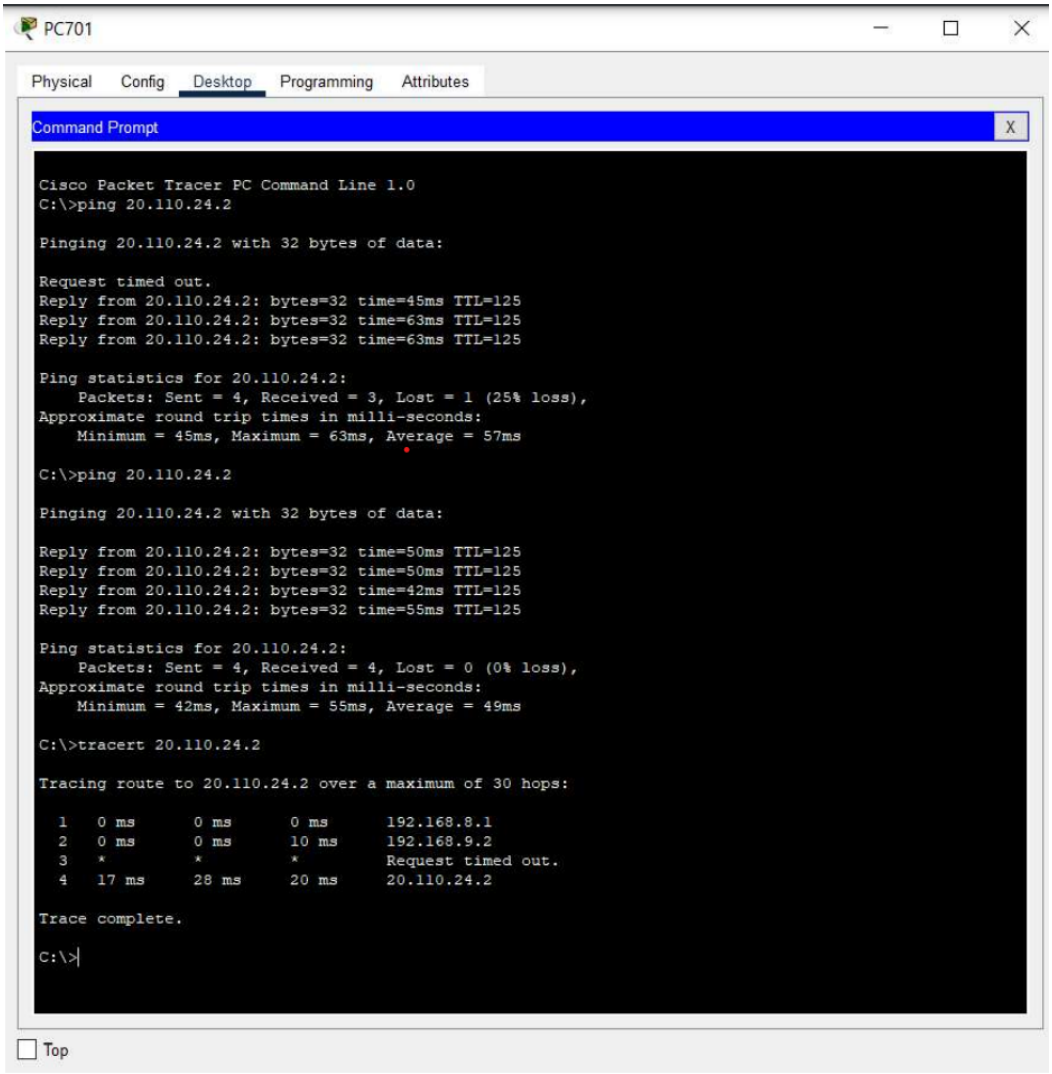

Figure 17: Ping from DMZ

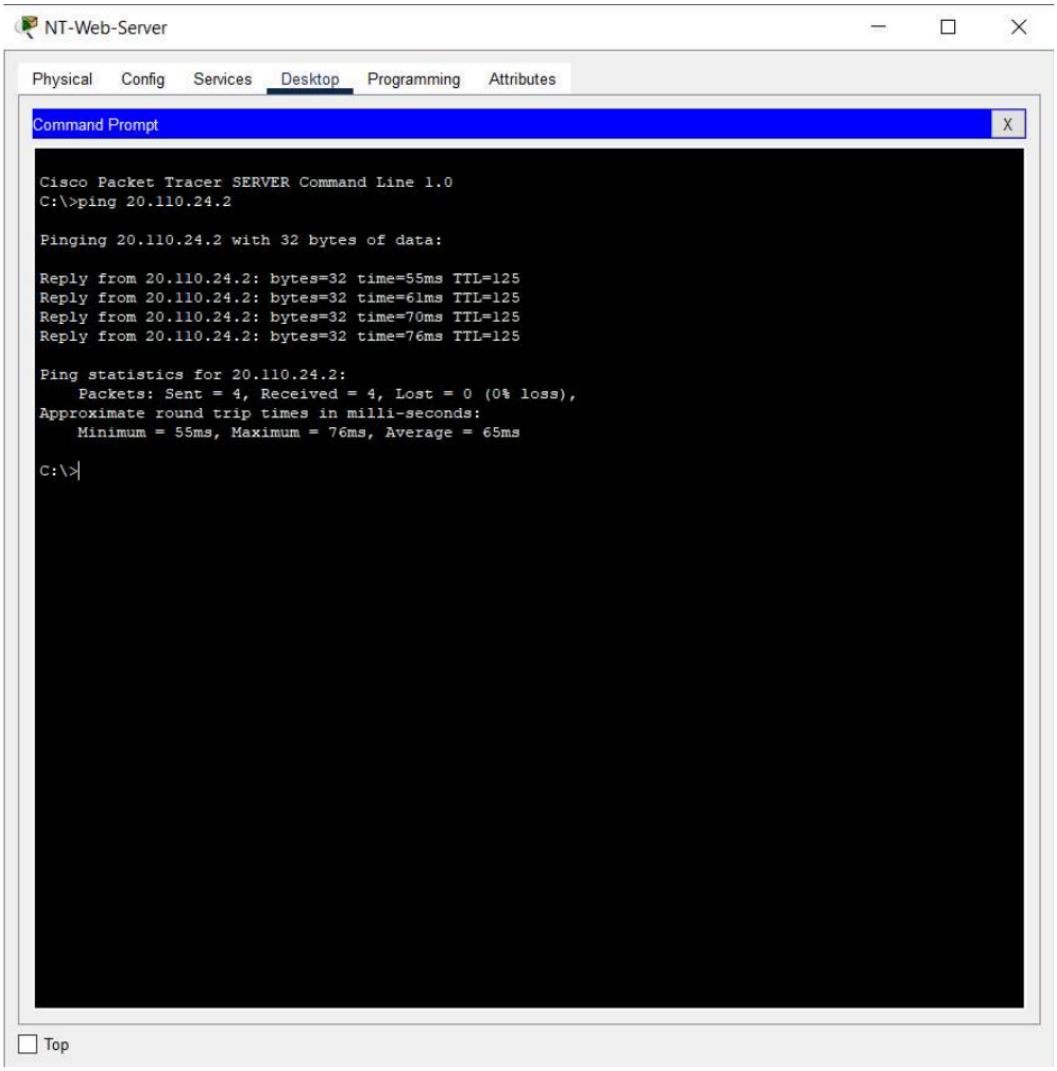

Figure 18: Ping from Web server

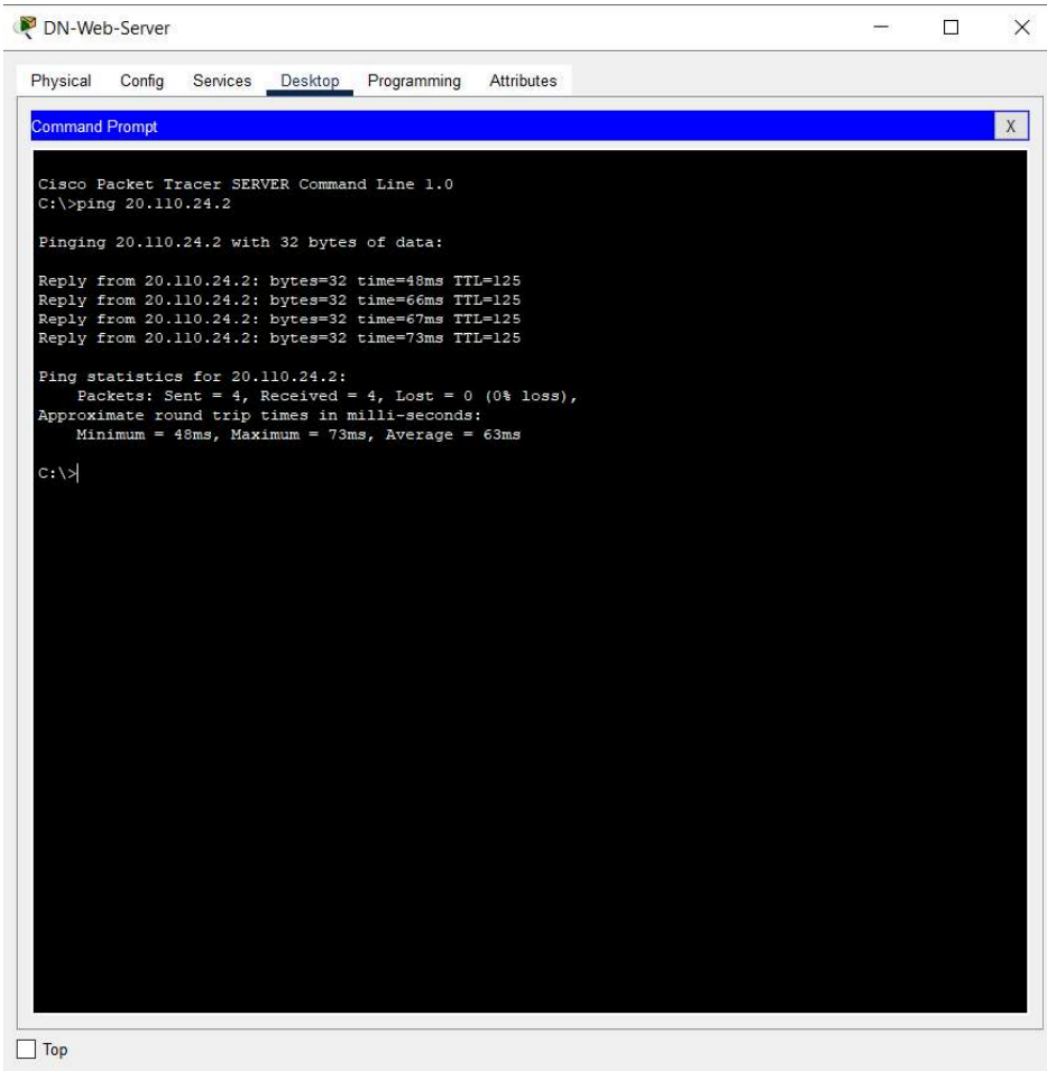

Figure 19: Ping from Web server

7 Reevaluation and Development Orientation

7.1 Reliability

Strengths

- **Redundancy:** Leased lines and xDSL provide backups for WAN connectivity.
- **Security solutions:** Firewalls, IPS/IDS, and VPNs offer protection against threats.
- **Scalable infrastructure:** Cat 6A cabling and modular network components allow for future expansion.

Weaknesses:

- **Single point of failure:** Core router failure could disrupt network operations.
- **Power outages:** Consider backup power solutions for critical systems.
- **Software updates:** Careful planning and testing required to avoid disruptions.

7.2 Ease of Upgrade

Strengths:

- **Open-source software:** OpenWRT or FreeBSD offer flexibility and customization.
- **Modular hardware:** Components can be easily upgraded or replaced.
- **NMS:** Streamlines monitoring and management tasks.

Weaknesses:

- **MPLS technology:** Can be complex to configure and manage.
- **Custom configurations:** Time and expertise needed for maintaining unique setups.
- **Vendor lock-in:** Choosing proprietary hardware or software can limit future upgrade options.

7.3 Diverse Support Software

Strengths:

- **Open-source options:** Availability of free and open-source alternatives for various functions.
- **Vendor-neutral hardware:** Supports various software options for flexibility.
- **Modular design:** Allows for integration of specialized software tools as needed.

Weaknesses:

- **Compatibility issues:** Different software versions or platforms might not work together seamlessly.
- **Expertise required:** Managing diverse software requires skilled IT personnel.
- **Security vulnerabilities:** Keeping diverse software up-to-date can be challenging.

7.4 Safety and Network Security

Strengths:

- **Firewalls, IPS/IDS, and VPNs:** Protect against unauthorized access and malicious attacks.
- **Segmented network:** VLANs restrict traffic flow for improved security.
- **Regular backups and disaster recovery plans:** Minimize data loss and ensure business continuity.

Weaknesses:

- **Physical security:** Secure IT rooms and equipment to prevent physical tampering.
- **Phishing and social engineering:** User training and awareness programs are crucial.
- **Human error:** Implement access control and audit procedures to minimize accidental security breaches.

7.5 Remaining Problems

- **Integration of future technologies:** Consider how the network will adapt to emerging trends like IoT, cloud computing, and SD-WAN advancements.
- **Data storage and management:** Strategize for data growth and implement efficient backup and archiving solutions.
- **Talent acquisition and retention:** Invest in training and development for IT personnel to keep pace with evolving technologies.

7.6 Development Orientation in the Future

- **Embrace cloud-based solutions:** Consider cloud services for email, file storage, and disaster recovery for scalability and cost-effectiveness.
- **Automate network management:** Utilize automation tools for tasks like provisioning, configuration, and patching for improved efficiency.
- **Prioritize data analytics and security:** Leverage data analytics tools for network optimization and security monitoring for proactive threat detection and mitigation.
- **Stay informed about industry trends:** Continuously evaluate new technologies and adapt the network design accordingly to remain competitive.