

SCHOOL NETWORK DESIGN AND IMPLEMENTATION

A CASE STUDY REPORT

Submitted by

GAGAN CHETHAN (RA2211003011335)

ASHUTOSH SINGH (RA2211003011334)

SHLOK BALSARA (RA2211003011333)

HEMANJALI POTHALA(RA2211003011330)

for the course

21CSC302J – COMPUTER NETWORKS

in partial fulfillment of the requirements for the degree of

BACHELOR OF TECHNOLOGY



DEPARTMENT OF COMPUTING TECHNOLOGIES

SCHOOL OF COMPUTING

FACULTY OF ENGINEERING AND TECHNOLOGY

SRM INSTITUTE OF SCIENCE AND TECHNOLOGY

KATTANKULATHUR - 603 203.



**SRM INSTITUTE OF SCIENCE AND TECHNOLOGY
KATTANKULATHUR – 603 203**

BONAFIDE CERTIFICATE

Certified that Computer Network A Case Study Report titled “**SCHOOL NETWORK DESIGN**” is the bonafide work of “**GAGAN CHETHAN**” [RA2211003011335], “**ASHUTOSH SINGH**” [RA2211003011334], “**SHLOK BALSARA**” [RA2211003011333], “**HEMANJALI POTHALA**”[RA2211003011330], who carried out the case study under my supervision. Certified further, that to the best of my knowledge the work reported herein does not form any other work .

SIGNATURE

Dr.A.JEYASEKAR

Course Faculty

Associate Professor

Department of Computing Technologies

Date : 12/11/2024

ABSTRACT

The design and implementation of a school network using Cisco Packet Tracer aim to provide a scalable, secure, and efficient network infrastructure to support modern educational needs. The network is designed to interconnect various campus areas, including administrative offices, classrooms, computer labs, libraries, and common areas, while ensuring seamless internet access and secure internal communication. The architecture includes hierarchical layers, incorporating core, distribution, and access layers to improve manageability, redundancy, and performance.

The core layer comprises high-performance routers to facilitate traffic routing between different network segments. The distribution layer consists of layer-3 switches that aggregate connections from various subnets and apply security policies, including VLANs, to segment traffic by departments or user groups, such as faculty, students, and administration. The access layer includes layer-2 switches connecting endpoint devices like desktops, laptops, printers, and IP phones, allowing flexible user access across the campus.

For enhanced network security, firewall configurations, ACLs, and VLANs are implemented to restrict unauthorized access and control data flow across different segments. Additionally, a DHCP server is set up to assign IP addresses dynamically, simplifying device management. DNS servers provide hostname-to-IP address resolution to streamline network communication. Other essential services like NAT (Network Address Translation) and PAT (Port Address Translation) facilitate secure internet access, while QoS (Quality of Service) prioritizes essential traffic for applications like VoIP and video conferencing.

Wireless access points (APs) are strategically placed for coverage across campus, providing secure Wi-Fi access for mobile devices. Network monitoring and management tools are configured to ensure real-time tracking, troubleshooting, and maintenance. Overall, the Cisco Packet Tracer design offers a reliable, secure, and future-ready network for a school environment, capable of supporting high-bandwidth applications, e-learning platforms, and collaborative educational technologies.

Table of Contents

| | |
|---------------------------------|----|
| Abstract | 2 |
| 1. Introduction | 4 |
| 2. Network Design..... | 5 |
| 3. Routing Configuration..... | 9 |
| 4. Testing and Validation | 10 |
| 5. Results | 12 |
| 6. Conclusion..... | 12 |
| 7. Reference | 13 |
| 8. Appendices | 13 |

TABLE OF FIGURES

| | |
|---|----|
| FIGURE 1: TOPOLOGY OF FULL NETWORK..... | 5 |
| FIGURE 2: TRACEROUTE SUCCESSFULL..... | 11 |
| FIGURE 3: DHCP IP ALLOCATION | 11 |
| FIGURE 4: PERFORMANCE MEASURE THROUGH PING TIME | 12 |

1. Introduction

1.1 Background

In today's educational landscape, a robust and reliable network infrastructure is essential to support digital learning, administrative tasks, and seamless communication. Schools increasingly rely on internet-based tools, cloud resources, and e-learning platforms, making network connectivity crucial for both students and staff. A well-designed network allows for efficient data sharing, secure access to resources, and real-time collaboration. Cisco Packet Tracer provides a powerful simulation environment for designing, testing, and visualizing network setups, making it ideal for creating and refining a school network model. By incorporating VLANs, firewalls, wireless access points, and various network protocols, this project aims to build a secure, scalable network tailored to the unique needs of a school environment.

1.2 Objectives

A well-designed network is crucial for modern schools, enabling efficient communication, resource sharing, and secure access to online learning platforms. This school network design project, built using Cisco Packet Tracer, aims to create a secure, scalable, and high-performance network infrastructure tailored to the needs of students, teachers, and administrative staff. The network layout follows a hierarchical structure, with core, distribution, and access layers to enhance manageability and reliability. Security is prioritized through VLANs, firewalls, and access control lists (ACLs), safeguarding sensitive data and controlling access across different campus segments. Services like DHCP and DNS streamline device management and network communication, while NAT and PAT enable secure internet access. Wireless access points provide campus-wide Wi-Fi connectivity for mobile users, and QoS policies optimize traffic flow to support bandwidth-intensive applications, such as video conferencing and VoIP. By incorporating redundancy and monitoring tools, this network is designed for minimal downtime and real-time performance tracking, ensuring a robust, adaptable environment that supports the growing demands of digital education.

2. Network Design

2.1 Topology

The network topology for this school design follows a hierarchical model, divided into core, distribution, and access layers. The core layer consists of high-performance routers for fast inter-segment data transfer. The distribution layer uses layer-3 switches to aggregate traffic, apply VLANs, and enforce security policies. At the access layer, layer-2 switches connect endpoint devices like computers, printers, and IP phones. Wireless access points are strategically placed for campus-wide Wi-Fi coverage. This topology ensures efficient traffic flow, scalability, and ease of management, while supporting secure and reliable communication across all school areas.

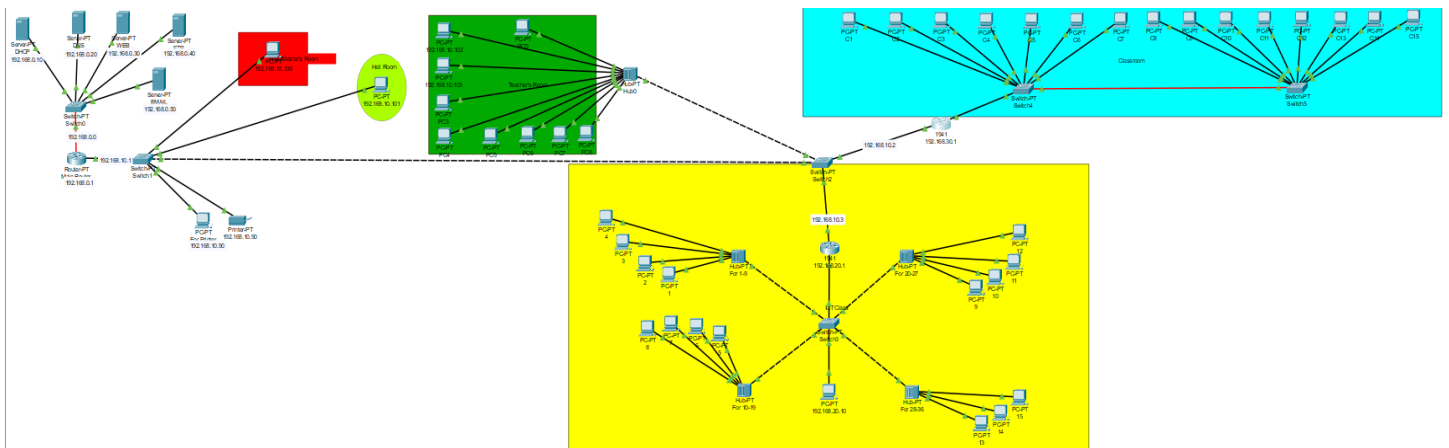


Figure 1: Topology of full network

2.2 Components

The network design for the project incorporates the following devices:

1. Routers (3):

- router for stream connectivity.
- Positioned at the core, distribution and access layer for redundancy.
- Connect to ISPs for internet connectivity.
- Configured with RIP, public IP addresses from ISPs.

2. Switches (6):

- Deployed at the core, distributed and access layers to provide redundancy and efficient routing.
- Configured for both switching and routing functionalities.
- Assigned IP addresses to enable routing.
- Connect individual departments to the all layers.
- Facilitate communication within respective areas.

3. End-User Devices (PCs):

- Deployed at the access layers and given IP.
- Connected to distribution layer switches for various departmental access.

4. Cisco Access Points (APs):

- Positioned at the access layer to provide wireless connectivity.
- Ensure wireless network availability in each layers of rooms.

5. DHCP Servers (1):

- Located in the server room.
- Dynamically allocate IP addresses to end-user devices.

6. Server Room Devices (Servers, etc.):

- DNS server, WEB server etc.
- Devices in the server room are allocated static IP addresses.
- These devices may include servers, storage units, and networking equipment.

7. Hub- PT(4):

- Uses for connect all networking devices
- Simulates the network set up
- Use Mac Addresses to reduce traffic

These devices collectively form a structured and well-organized network architecture, integrating redundancy, efficient routing, and secure communication to meet the specific requirements of the trading floor support center's operations.

2.3 IP Addressing Scheme

The IP address scheme for this school network design follows a structured approach, with different subnets assigned to various departments or functional areas. Each major segment—such as administration, classrooms, labs, and common areas—receives its own subnet, simplifying management and improving security. Using Class C private IP ranges (e.g., 192.168.x.x), each subnet is allocated a specific range to accommodate the number of devices per area while minimizing IP waste. DHCP servers are configured to dynamically assign IP addresses within each subnet, ensuring efficient IP management and easier device connections. VLANs are also implemented alongside the IP scheme to segregate traffic for different user groups, enhancing both performance and security across the network.

Teacher Room

| Device | Interface | IP Addresses | Subnet Mask | Gateway |
|--------|-----------|----------------|---------------|--------------|
| PC1 | Fa0/0 | 192.168.10.102 | 255.255.255.0 | 192.168.10.1 |
| PC2 | Fa0/0 | 192.168.10.103 | 255.255.255.0 | 192.168.10.1 |
| PC3 | Fa0/0 | 192.168.10.34 | 255.255.255.0 | 192.168.10.1 |
| PC4 | Fa0/0 | 192.168.10.35 | 255.255.255.0 | 192.168.10.1 |
| PC5 | Fa0/0 | 192.168.10.25 | 255.255.255.0 | 192.168.10.1 |
| PC6 | Fa0/0 | 192.168.10.33 | 255.255.255.0 | 192.168.10.1 |
| PC7 | Fa0/0 | 192.168.10.26 | 255.255.255.0 | 192.168.10.1 |
| PC8 | Fa0/0 | 192.168.10.30 | 255.255.255.0 | 192.168.10.1 |
| PC9 | Fa0/0 | 192.168.10.20 | 255.255.255.0 | 192.168.10.1 |

Class Room

| Device | Interface | IP Addresses | Subnet Mask | Gateway |
|--------|-----------|----------------|---------------|--------------|
| PC1 | Fa0/0 | 192.168.30.102 | 255.255.255.0 | 192.168.30.1 |
| PC2 | Fa0/0 | 192.168.30.105 | 255.255.255.0 | 192.168.30.1 |
| PC3 | Fa0/0 | 192.168.30.113 | 255.255.255.0 | 192.168.30.1 |
| PC4 | Fa0/0 | 192.168.30.117 | 255.255.255.0 | 192.168.30.1 |
| PC5 | Fa0/0 | 192.168.30.106 | 255.255.255.0 | 192.168.30.1 |
| PC6 | Fa0/0 | 192.168.30.112 | 255.255.255.0 | 192.168.30.1 |
| PC7 | Fa0/0 | 192.168.30.100 | 255.255.255.0 | 192.168.30.1 |
| PC8 | Fa0/0 | 192.168.30.115 | 255.255.255.0 | 192.168.30.1 |
| PC9 | Fa0/0 | 192.168.30.117 | 255.255.255.0 | 192.168.30.1 |
| PC10 | Fa0/0 | 192.168.30.101 | 255.255.255.0 | 192.168.30.1 |
| PC11 | Fa0/0 | 192.168.30.141 | 255.255.255.0 | 192.168.30.1 |
| PC12 | Fa0/0 | 192.168.30.119 | 255.255.255.0 | 192.168.30.1 |
| PC13 | Fa0/0 | 192.168.30.103 | 255.255.255.0 | 192.168.30.1 |
| PC14 | Fa0/0 | 192.168.30.118 | 255.255.255.0 | 192.168.30.1 |
| PC15 | Fa0/0 | 192.168.30.104 | 255.255.255.0 | 192.168.30.1 |

Lab Room

| Devices | Interface | IPAddresses | Subnet Mask | Gateway |
|---------|-----------|----------------|---------------|--------------|
| PC1 | Fa0/0 | 192.168.20.143 | 255.255.255.0 | 192.168.20.1 |
| PC2 | Fa0/0 | 192.168.20.138 | 255.255.255.0 | 192.168.20.1 |
| PC3 | Fa0/0 | 192.168.20.134 | 255.255.255.0 | 192.168.20.1 |
| PC4 | Fa0/0 | 192.168.20.150 | 255.255.255.0 | 192.168.20.1 |
| PC5 | Fa0/0 | 192.168.20.155 | 255.255.255.0 | 192.168.20.1 |
| PC6 | Fa0/0 | 192.168.20.148 | 255.255.255.0 | 192.168.20.1 |
| PC7 | Fa0/0 | 192.168.20.154 | 255.255.255.0 | 192.168.20.1 |
| PC8 | Fa0/0 | 192.168.20.103 | 255.255.255.0 | 192.168.20.1 |
| PC9 | Fa0/0 | 192.168.20.103 | 255.255.255.0 | 192.168.20.1 |
| PC10 | Fa0/0 | 192.168.20.135 | 255.255.255.0 | 192.168.20.1 |
| PC11 | Fa0/0 | 192.168.20.139 | 255.255.255.0 | 192.168.20.1 |
| PC12 | Fa0/0 | 192.168.20.122 | 255.255.255.0 | 192.168.20.1 |
| PC13 | Fa0/0 | 192.168.20.118 | 255.255.255.0 | 192.168.20.1 |
| PC14 | Fa0/0 | 192.168.20.115 | 255.255.255.0 | 192.168.20.1 |
| PC15 | Fa0/0 | 192.168.20.142 | 255.255.255.0 | 192.168.20.1 |
| PC16 | Fa0/0 | 192.168.20.10 | 255.255.255.0 | 192.168.20.1 |

Server Room

| Servers | Interface | IP Adresses | Subnet Mask | Gateway |
|---------|-----------|---------------|---------------|-------------|
| DHCP | Fa0/0 | 192.168.10.10 | 255.255.255.0 | 192.168.0.1 |
| DNS | Fa0/0 | 192.168.10.20 | 255.255.255.0 | 192.168.0.1 |
| WEB | Fa0/0 | 192.168.10.30 | 255.255.255.0 | 192.168.0.1 |
| FTP | Fa0/0 | 192.168.10.40 | 255.255.255.0 | 192.168.0.1 |
| EMAIL | Fa0/0 | 192.168.10.50 | 255.255.255.0 | 192.168.0.1 |

Printer Room

| Devices | Interface | IP Addresses | Subnet Mask | Gateway |
|---------|-----------|---------------|---------------|--------------|
| PC | Fa0/0 | 192.168.10.90 | 255.255.255.0 | 192.168.10.1 |
| PRINTER | Fa0/0 | 192.168.10.91 | 255.255.255.0 | 192.168.10.1 |

Head Master ROOM

| Devices | Interface | IP Addresses | Subnet Mask | Gateway |
|---------|-----------|----------------|---------------|--------------|
| PC | Fa0/0 | 192.168.10.100 | 255.255.255.0 | 192.168.10.1 |

Hall Room

| Devices | Interface | IP Addresses | Subnet Mask | Gateway |
|---------|-----------|----------------|---------------|--------------|
| PC | Fa0/0 | 192.168.10.101 | 255.255.255.0 | 192.168.10.1 |

3 Routing Configuration

3.1 Ruter Configure

Router configuration involves setting up the basic parameters and interfaces for a network device to ensure proper communication. The first step is to set the router's hostname for identification, typically using the ``hostname`` command. Next, an interface (e.g., GigabitEthernet0/0) is configured with an IP address and subnet mask to define the network segment it will communicate with. The ``ip address`` command assigns the desired IP address and subnet mask to the interface. Finally, the ``no shutdown`` command is used to enable the interface, bringing it up and making it active for network operations. This basic configuration allows the router to start routing traffic between networks.

| Devices | Interface | IP Addresses | Subnet Mask |
|---------|--------------------|--------------|---------------|
| R1 | FastEthernet0/0 | 192.168.10.1 | 255.255.255.0 |
| R1 | FastEthernet4/0 | 192.168.0.1 | 255.255.255.0 |
| R2 | GigabitEthernet0/0 | 192.168.10.2 | 255.255.255.0 |
| R2 | GigabitEthernet0/1 | 192.168.30.1 | 255.255.255.0 |
| R3 | GigabitEthernet0/0 | 192.168.20.1 | 255.255.255.0 |
| R3 | GigabitEthernet0/1 | 192.168.10.3 | 255.255.255.0 |

3.2 RIP Configure

To configure RIP (Routing Information Protocol) in a router, you begin by enabling the RIP routing protocol with the command `router rip`. Next, use the `version 2` command to specify RIP version 2, which supports classless routing. Then, add the networks that you want to advertise using the `network` command, specifying the network addresses. Finally, `no auto-summary` can be used to disable automatic summarization of routes. This basic configuration allows the router to start exchanging routing information using RIP.

| Device | Known Networks | Subnet Mask |
|--------|----------------|---------------|
| R1 | 192.168.0.0 | 255.255.255.0 |
| R1 | 192.168.10.0 | 255.255.255.0 |
| R2 | 192.168.10.0 | 255.255.255.0 |
| R2 | 192.168.30.0 | 255.255.255.0 |
| R3 | 192.168.10.0 | 255.255.255.0 |
| R3 | 192.168.20.0 | 255.255.255.0 |

4. Testing and Validation

Packet Tracer was utilized to simulate and test the designed network. Packet Tracer is a network simulation tool that provides a virtual environment for designing, configuring, and testing network scenarios.

Network Topology Design: The network topology, including routers, switches, PCs, servers, and other devices, was designed within Packet Tracer based on the specified requirements.

Configuration Implementation: Using the designed topology, configurations were implemented on routers, switches, and other network devices according to the provided guidelines. Cisco Packet Tracer allows users to configure devices with a user-friendly interface similar to actual Cisco devices.

Traffic Simulation: Packet Tracer allows the simulation of network traffic and communication between devices. This involves generating traffic, testing connectivity, and ensuring that data flows as expected.

Verification of Redundancy and Failover: The hierarchical design with redundancy at every layer, including multiple routers, multilayer switches, and ISP connections, was tested to verify failover mechanisms and ensure network resilience.

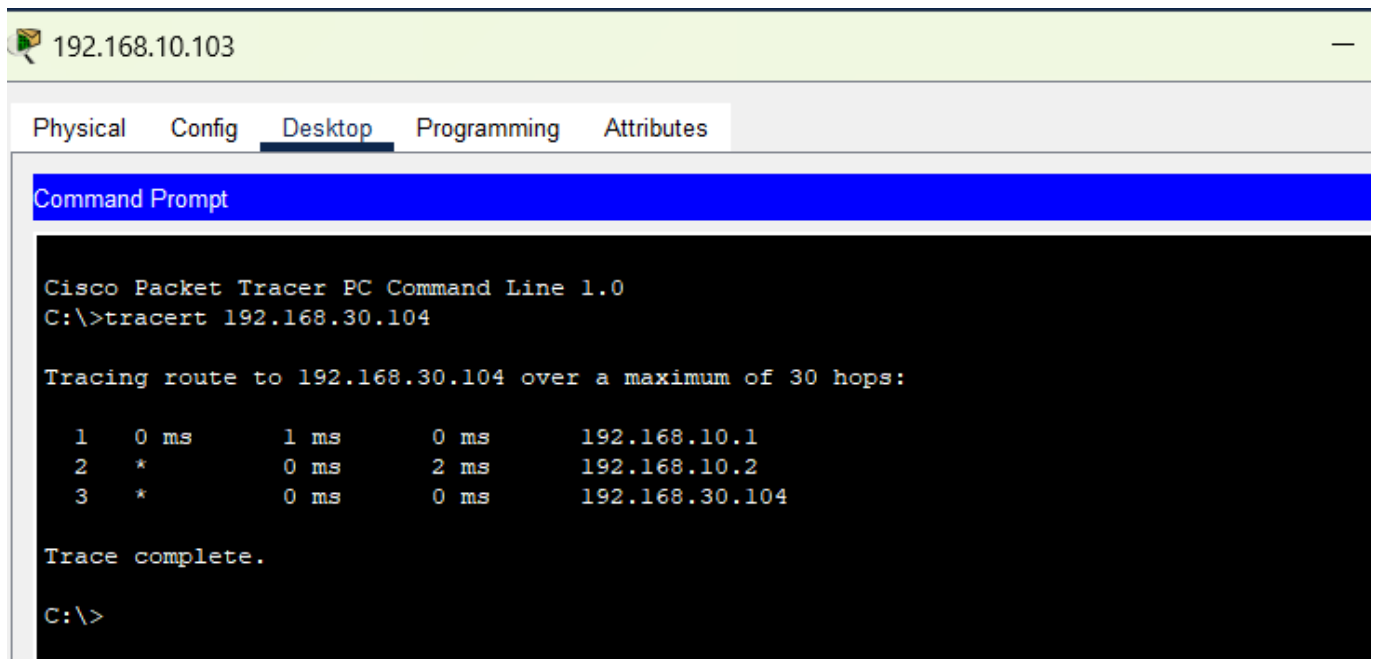


Figure 2: Tracing command

DHCP and IP Address Allocation: Dynamic Host Configuration Protocol (DHCP) functionality and IP address allocation were tested to ensure that devices received the correct IP addresses dynamically and that devices in the server room had static IP assignments.

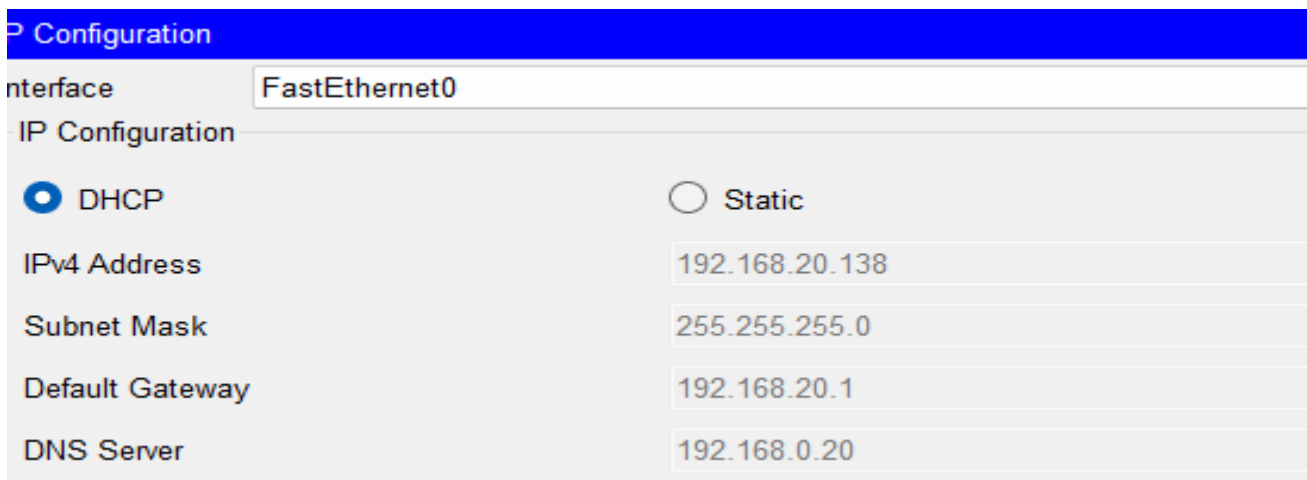
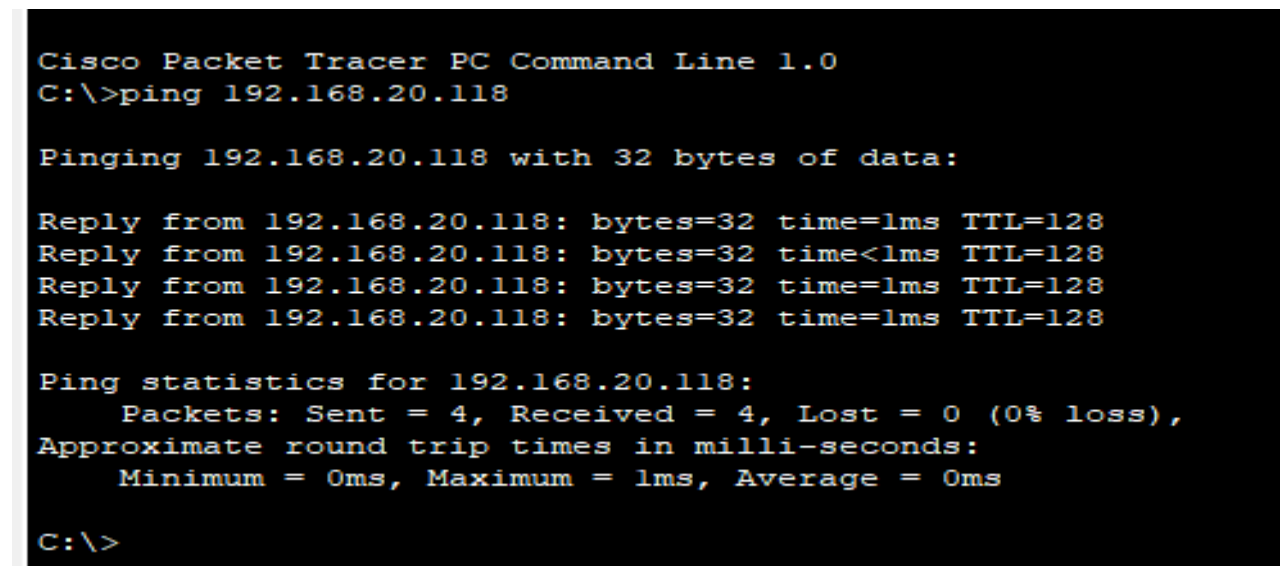


Figure 3: DHCP IP Allocation

5.Results and Evaluation

5.1 Performance Metrics

The `ping` command is used to test connectivity between devices on a network. You start by typing `ping` followed by the target IP address or hostname you want to test. The command sends ICMP Echo Request packets to the destination, and if reachable, it will receive ICMP Echo Replies. It helps diagnose network issues by confirming whether a device is responding on the network.

A screenshot of a Cisco Packet Tracer PC Command Line interface. The text is as follows:

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.20.118

Pinging 192.168.20.118 with 32 bytes of data:

Reply from 192.168.20.118: bytes=32 time=1ms TTL=128
Reply from 192.168.20.118: bytes=32 time<1ms TTL=128
Reply from 192.168.20.118: bytes=32 time=1ms TTL=128
Reply from 192.168.20.118: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.20.118:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

Figure4:Ping Command

6. Conclusion

6.1 Summary

The network diagram presented showcases a segmented structure with various subnetworks connected via routers and switches. Each section represents distinct areas, likely for specific purposes: servers, students, classrooms, and an administration network. Key devices include servers, PCs, routers, and multiple switches, indicating a hierarchical design. The color-coded areas, such as green, yellow, and blue, imply different network zones, perhaps signifying VLANs or subnetworks. Routers bridge these zones, allowing controlled inter-network communication. The network layout is optimized for scalability, with each segment accommodating multiple devices and sufficient redundancy to minimize single points of failure in which design network of school work well.

6.2 Lessons Learned

Throughout the project, several valuable lessons have been learned:

- **Redundancy is Key:** The inclusion of redundancy at various levels is crucial for maintaining network availability and minimizing downtime.
- **Effective Design:** Proper segmentation enhances security and facilitates organizational structure, simplifying network management.
- **Thorough Testing Matters:** Rigorous testing using simulation tools like Cisco Packet Tracer is essential to identify and rectify issues before deployment.
- **Scalability Considerations:** Designing the network with scalability in mind allows for future growth and expansion without significant overhauls.
- **Documentation is Essential:** Comprehensive documentation of configurations, IP addressing, and design decisions streamlines troubleshooting and future modifications.

7. References

Cisco Network Design for Schools: Key References

Here are some valuable resources to guide your Cisco network design for a school:

This Official Cisco Documentation

Cisco Service Ready Architecture for Schools:

comprehensive guide provides a detailed architectural overview, network foundation design, and security considerations for school networks. It's a must-read for understanding Cisco's recommended approach.

[Documentation Link](#)

8. Appendices

Abbreviations:

LAN: Local Area Network

WAN: Wide Area Network

DHCP: Dynamic Host Configuration Protocol

HTTP: Hypertext Transfer Protocol

HTTPS: Hypertext Transfer Protocol Secure

FTP: File Transfer Protocol

SMTP: Simple Mail Transfer Protocol

IMAP: Internet Message Access Protocol

ACL: Access Control List

QoS: Quality of Service

VRF: Virtual Routing and Forwarding

IS-IS: Intermediate System-to-Intermediate System

IPv4: Internet Protocol version 4

IPv6: Internet Protocol version 6

DHCPv6: Dynamic Host Configuration Protocol version 6

SLA: Service Level Agreement

DNS: Domain Name System