CIS 315

Communication and Network Fundamentals

Technical Report for Final Project

Design Network for college

Team members

Shahed Alharbi	2240000201
Aisha Alhuzaym	2240002568
Heba Askar	2240006064
Raghad alqahtani	2240001622
Alya Shehab	2240002062
Zainab Hamada	2240003018

Instructor: Fatimah Alqadheeb

Table of contents:

Introduction

In today's interconnected world, effective communication and seamless information exchange are critical for organizations, especially educational institutions. This project focuses on designing a robust and efficient network system for a college, catering to the diverse needs of students, faculty, and administrative staff. The primary objective is to create a scalable, secure, and well-structured network that ensures optimized performance and supports future growth.

The network design assigns a dedicated router to each department within the college, ensuring localized control and efficient resource allocation. Within each department, the network is divided into four key sections: the head of department's office, faculty offices, classrooms, and laboratories, all interconnected using switches. This hierarchical approach enhances network reliability, performance, and manageability.

Using Cisco Packet Tracer as the primary simulation tool, this project explores innovative networking techniques to implement a cost-effective and practical solution. The report documents the planning, design, implementation, testing, and evaluation processes, addressing challenges encountered and their solutions.

This initiative not only highlights the importance of well-designed networks in academic institutions but also serves as a guide for implementing similar solutions, demonstrating the potential for scalable and efficient smart systems in educational settings.

Network Design

1.Network topology:

The above network was an out-expression of different hybrid topologies where they were based on wired and wireless connections. The hybrid topology provides flexible provisions for addressing diverse requirements of the departments. Devices were connected inside the network through switches that support VLANs capable of traffic isolation within each department. In this case, the focus was on efficiently routing traffic between VLANs and interconnecting subnets with routers.

2.Devices in the Network:

- Routers:

Devices like the 2811 and 1841 routers were utilized as core devices to route data traffic among departments (VLANs) and connect them to the internet.

- They support dynamic routing protocols like OSPF and EIGRP for streamlining traffic flow.

- Switches:

2960 and 2950 switches are used for connecting endpoint devices on each department.

The VLANs help with traffic isolation for both security and performance.

- Endpoint Devices:

Desktop computers (PC-PT) are used by students, employees, and administrative staff to carry out day-to-day tasks.

This addressed departments that were in need of mobility and flexibility.

Printers installed in each of the departments to enable printing.

- IoT Devices:

IoT devices like the Motion Detector and Temperature Monitor are installed for automation and monitoring of specified operations.

The devices were connected on a separate wireless network with WRT300N Access Points to increase security and network segmentation.

- IP Phones:

This will connect with departmental switches for internal and external communications.

3.Design Considerations:

- Security:
Traffic is treated with isolation through VLANs, which will minimize risk and guarantee data confidentiality.

- IoT Devices on Separate Networks:
To mitigate different cyber threats and restrict access to sensitive data, the IoT devices were designated on their own network.

- Efficiency:

Switches with Quality of Service (QoS) promote the use of expedited transport for priority traffic like voice (VoIP) and other critical data.

- Scalability and Flexibility:

The design is meant to allow the inclusion of new devices and/or departments to take place without major reconfiguration.

- Wireless Coverage:

Access points would be strategically placed to ensure that the IoT devices receive coverage and robust wireless connectivity where needed.

4. VLAN Allocation by Departments: The primary division of the network is into 6 VLANs designated to individual departments to have organized and efficient traffic. They are:

1. VLAN 10 - Computer Science Department:

- Desktop computers for students and teachers are installed in the CS department.

- Printer and peripheral devices usually connect to serve students of the CS department.

- Wired connections are mainly favored as they are highly stable and enhance performance.

2. VLAN 20 - Kindergarten Department:

- Workstations connected to lessons and activity management in an educational environment.

- Printer connected to produce the necessary educational materials.

- Options to connect IoT devices such as smartboards and child monitors.

3. VLAN 30 - Scientific Department:

- Hosting laboratories fitted with high-performance computers for scientific calculations and simulations.

- Inclusion of more advanced peripherals such as 3D printers and measuring devices.

- High bandwidth is required to accommodate highly resource-intensive applications.

4. VLAN 40 - English Department:

- It contains computers to be used for language instruction for both teachers and students.

- Printers to produce educational materials.

- IP phone units for internal communications to connect other departments.

5. VLAN 50 - Public Relations Department:

- Desktops and laptops meant for running campaigns and public communication.

- Printers are used to produce reports and promotional materials.

- Media organizations communicate through the use of IP phone systems.

6. VLAN 60 - Administration Department:

- It comprises machines used by administrative staff and managers for sensitive tasks.

- Network operations shall have a secure integration to hold sensitive information.

- It is segmented from other departments so that confidentiality is achieved.

5. Suggestions to Improve Performance:

- Network security would be strengthened by applying 802.1X protocols for access control.
- Get in the habit of regularly backing up administrative information to protect against data catastrophe.
- Replace existing switches and routers with faster ones to facilitate future expansion.

Implementaion step-by-step:

Tool	Count	Ip
Router	10	192.168.30.0/24
Switch	16	192.168.20.0/24
Pc	30	192.168.10.0/24
Lab	12	192.168.50.0/24
Printer	8	192.168.70.0/24

: Step 1 Adding Devices to the Workspace:

1: Open Packet Tracer and create a new workspace.

2: Add 10 Routers.

3: Click on the "Routers" section and drag 10 routers to the workspace.

4: Add 16 Switches.

5: Click on the "Switches" section and drag 16 switches to the workspace.

6: Add 30 Computers and 10 Laptops.

7: Click on the "End Devices" section and add 30 computers and

10 laptops and 8 printer to the workspace.

Step 2: :Physical Connections

Connecting Routers to Switches./ 1
the "Copper Straight-Through" cable to connect each router/ 2
to Use at least one switch .Make sure to use different interfaces on the routers to connect them to the switches.
3/ For example: Router0(FastEthernet/0) to Switch0(FastEthernet0/1).
Connecting Switches to Each Other/ 4
Interconnect switches with "Copper Crossover" cables to/ 5
ensure that all switches are part of the same network or VLAN.
Connecting Computers and Laptops to Switches/ 6
Use the "Copper Straight-Through" cable to connect computers and laptops to switches./7
Each switch should connect to multiple devices .

Step 3: :Configuring Routers

1: Basic Configuration:
2: Click on each router to open the configuration window and go to the CLI tab.

3: Use the following commands for basic setup

```
Router> enable
Router# configure terminal
Router(config)# hostname RouterX (Replace X with the router number)
Router(config)# interface fastEthernet 0/0
Router(config-if)# ip address 192.168.30.0/24 255.255.255.0 (Use unique subnet for each router)
Router(config-if)# no shutdown
Router(config-if)# exit
Router(config)# ip route 0.0.0.0 0.0.0.0 192.168.30.0/24 (Use the next-hop IP address for routing
Router(config)# end
```

Configuring Switches : Step4:

1: Basic Switch Configuration

Click on each switch ,go to the CLI tab ,2: and use the following commands:

```
Switch> enable
Switch# configure terminal
Switch(config)# hostname SwitchX (Replace X with the switch number)
Switch(config)# interface vlan 1
Switch(config-if)# ip address 192.168.X.2 255.255.255.0 (Use the corresponding subnet of the connected router)
Switch(config-if)# no shutdown
    Switch(config-if)# end
```

Configuring Computers and Laptops: Step5:

1: IP Address Configuration:

2:Click on each computer and laptop, go to the Desktop tab, and then click On IP Configuration.

3:Assign IP addresses and subnet masks manually.Make sure each device has a unique IP within the respective routers subne.

4: Example:

5: Computer0 :192.168.10.0/24 ,Subnet Mask :255.255.255.0

6: Laptop0 :192.168.20.0/24 ,Subnet Mask :255.255.255.0

Step 6: :Testing the Network

1: Ping Test:

2: Use the Command Prompt on each computer and laptop to ping other devices in the network to ensure connectivity.

3: Example :ping 1192.168.50.0/24 (Pinging the default gateway).

Step 7 :Advanced Configuration (Optional)

1: VLAN Configuration on Switches (for more advanced setups).

2: You can create VLANs to segment network traffic.

```
Switch(config)# vlan 10
Switch(config-vlan)# name Sales
Switch(config-vlan)# exit
Switch(config)# interface fastEthernet 0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 10
Switch(config-if)# end
```

Testing and Troubleshooting

During the network testing phase, various devices were evaluated to ensure proper functionality and connectivity. Below is a summary of the testing steps, issues encountered, and their resolutions for each device: a Personal Computer (PC), Laptop, Phones, Printers, Switches, and Routers. The devices were connected using either cables or the virtual Wi-Fi within the program.

- **Personal Computer (PC):** The connectivity between the PC and other devices was tested using the "ping" command to verify that the PC could communicate with other devices on the network.
- **Laptop:** The laptop was connected to the same network, and connectivity with other devices like the printer, PC, and phone was tested using "ping" and "traceroute" commands.
- **Phones:** Smartphones were simulated within the network. Connectivity was tested by sending data packets to ensure they functioned properly within the network.
- **Printer:** The printer's ability to receive data from other devices on the network was tested using the "ping" command to ensure accessibility.
- **Switch:** The switch was used to connect all devices within the local network. It was verified that the switch was functioning correctly, and connectivity between connected devices was tested.
- **Router:** The router, which connects the internal network to external networks or the internet, was tested for connectivity between internal and external networks using commands like "ping."

2. Troubleshooting

During the testing process, several issues were encountered, which were resolved as follows:

- **Connectivity Issues Between Devices:** Some devices were unable to communicate with others. The IP address settings were checked to ensure that all devices were on the same network range. Adjustments were made where necessary.
- **Ping Test Failures:** Some devices failed to send or receive data packets correctly. Firewall settings on the router and switch were checked to ensure they weren't blocking communication between devices.
- **Internet Access Issues:** When testing connectivity to the internet, some devices couldn't access external networks. The router's settings were verified to ensure proper internet connectivity.

3. Results

Connectivity between all devices was successfully tested using Packet Tracer. All issues encountered during testing, including connectivity issues and IP settings adjustments, were resolved.

As a result, it was confirmed that the network operates efficiently, and all devices are correctly connected.

Results:

Outcomes:

1- Network Setup: The LAN network was configured using a star topology where all devices are connected to central switches. Routers are used for Internet access, and the wireless network is spread via multiple access points

2- Successful Device Communication: All devices in the network were able to communicate without packet loss or timeouts, indicating the correct configuration of IP addressing, routing, and DNS settings.

3- Throughput: Data transfer rates across the network varied depending on the segment:
   - Wired Connections: Maximum throughput of 1 Gbps (gigabit Ethernet)
   - Wireless Connections: Maximum throughput of 300 Mbps on Wi-Fi 5 and up to 1.2 Gbps on Wi-Fi 6 devices

4- Latency: Ping tests showed low latency across the network. The average round-trip time (RTT) between devices was approximately 10ms for wired connections and 20ms for wireless connections.

5- Packet Loss: Minimal packet loss was observed (less than 1% on wireless links, negligible on wired links), which is typical in a well-configured network.

Performance Analysis:

1- Network Congestion: No significant network congestion was detected during the simulation. However, the Wi-Fi performance decreased slightly in high-density areas like the library, which can be mitigated by adding more access points.

2- Error Rates: No transmission errors were found in the wired network. In the wireless network, a small percentage of packet retries occurred in areas with high interference or high device density.

3- Security Tests: Security protocols were tested by attempting unauthorized access. The firewall and access control lists (ACLs) successfully blocked any unauthorized attempts.

Data collected:

Device 1	Device 2	Packet loss(%)	Latency (ms)	Throughput (Mbps)
PC1	Router	0%	10	1000
Router	Switch	0%	5	1000
Switch	PC2	0%	8	1000
Laptop (Wi-Fi)	Router	1%	20	300
Wi-Fi device	Access point	0.5%	25	400

Conclusion

environment which merges wired and wireless forms of technologies. The network consisted of different components which included routers, PCs, and phones, the system was able to cater for diverse user requirements as it was complete.

The findings demonstrated efficient interactive communication and incorporation of various network components .However ,during configuration and troubleshooting ,challenges were of minor significance ,Test procedures managed to fix such issues.

Recommendations :

Scalability: Develop the network further so as to incorporate more devices and users in view of the fact that the university will escalate in the future.

Security Enhancements :Include in the network additional features like VLANs ,firewalls and intrusion detection to enhance and secure the data in the network.

Performance Optimization :There should be load balancing and quality of service (QoS) configuration management to manage resources effectively.

Future Applications :Investigate incorporating IoT smart technologies for example controlling lighting and environmental conditions automatically.

This project gave a good understanding of the network design and simulation processes allowing ways for expansion and application in the practical world