CAMPUS NETWORK TRAFFIC VISUALIZATION

Submitted to

**CISCO**



**PROJECT REPORT**

Submitted by

Sanidhya Tyagi



**Department of CSE-AIML/AIDS**

**Lakshmi Narain College of Technology, Bhopal (M.P.) Session 2024-25**

# LAKSHMI NARAIN COLLEGE OF TECHNOLOGY, BHOPAL

**DEPARTMENT OF CSE-AIML/AIDS**



**CERTIFICATE**

This is to certify that the work embodied in this project work entitled **”Project Title”** has been satisfactorily completed by the **Student Name 1** (Roll No.)**.** It is a bonafide piece of work, carried out under the guidance in **Department of CSE-AIML/AIDS**, **Lakshmi Narain College of Technology, Bhopal** for the partial fulfillment of the **Bachelor of Technology** during the academic year 2023-2024.

Guide Name Designation **(GUIDE)**

Approved By

**Dr. Tripti Saxena**

**Professor & Head Department of CSE-AIML/AIDS**

**INDEX**

|  |  |  |
| --- | --- | --- |
| **S.NO.** | **TOPICS** | **PAGES** |
| **1.** | Description | 1-2 |
| **2.** | Literature Survey | 10-12 |
| **3.** | Mini objective & scope of project | 2-3 |
| **4.** | Problem Analysis and requirement specification | 8-10 |
| **5.** | Detailed Design(Modeling and ERD/DFD) | 10-12 |
| **6.** | Hardware/Software platform environment | 2-3 |
| **7.** | Snapshots of Input & Output | 5-6 |
| **8.** | Coding | 10-20 |
| **9.** | Project limitation and Future scope | 2-3 |
|  | References | 2-3 |
|  | Total Approx. 20-40 Pages | |

## CHAPTER 1

**DESCRIPTION**

The network is designed to simulate a multi-department organizational infrastructure with packet sniffers placed at strategic points for **packet flow investigation** and **network monitoring**.

**1. Department 1**

* **Devices:**
  + PC-PT (10.1.1.1) – Host machine initiating requests
  + PC-PT (10.1.1.2) – Secondary workstation
  + Switch0 – Cisco 2960-24TT switch connecting PCs to the core router
  + Sniffer1 – Captures packets between Host PC and Switch
* **Function:** This department handles local user traffic that gets aggregated by Switch0 and sent towards the main router.

**2. Department 2**

* **Devices:**
  + PC-PT (11.1.1.1) and PC-PT (11.1.1.2)
  + Switch1 – Cisco 2960-24TT switch
  + Sniffer2 – Captures packets between Switch1 and Router1
* **Function:** Provides workstation access for users, forwarding traffic to the main router through monitored links.

**3. Web Department**

* **Devices:**
  + PC-PT (12.1.1.1) and PC-PT (12.1.1.2)
  + Switch2 – Cisco 2960-24TT switch
  + Sniffer3 – Monitors communication between Web Department PCs and servers
* **Function:** Hosts internal web-related operations and connects directly to external web and DNS servers.

**4. Core Network & Routers**

* **Router1 (2911)** – IPs: 10.1.1.3 (Dept 1), 11.1.1.3 (Dept 2), 14.1.1.1 (Core link)
* **Router3 (2911)** – IPs: 14.1.2.1 (Core link), 12.1.1.3 (Web Department)
* **Sniffer0** – Positioned between Router1 and Router3 to capture **inter-router traffic**.
* **Purpose:** Handles routing between internal departments and external servers.

**5. Server Segment**

* **Servers:**
  + Web Server (12.1.1.4) – Handles HTTP/HTTPS requests
  + DNS Server (12.1.1.5) – Resolves domain names to IP addresses
* **Connection:** Linked to Web Department via Router3 and monitored by Sniffer3.
* **Function:** Responds to internal and external network requests.

## CHAPTER 2

**SCOPE**

This project focuses on **analyzing and monitoring packet transmission** within a multi-department network using network sniffers strategically placed between critical nodes. It covers:

1. **End-to-End Packet Flow Tracking**
   * Monitoring how a user’s request travels from a host PC to the web server and back.
   * Visualizing the complete route via switches, routers, and the server infrastructure.
2. **Network Traffic Analysis Using Sniffers**
   * **Sniffer0**: Captures packets between inter-network routers to analyze routing behavior.
   * **Sniffer1**: Captures packets between the host PC and its switch for local LAN traffic analysis.
   * **Sniffer2**: Captures packets between departmental switches and routers for departmental traffic analysis.
   * **Sniffer3**: Captures packets between the Web Department switch and the server for application-level analysis.
3. **Layer-Wise Investigation**
   * **Layer 1 (Physical)**: Observing cable and port connectivity issues.
   * **Layer 2 (Data Link)**: Checking MAC address resolution and switch forwarding.
   * **Layer 3 (Network)**: Analyzing IP routing and inter-network communication.
4. **Performance Measurement**
   * Identify latency points across departments.
   * Measure packet loss, retransmissions, and bottlenecks in communication.
5. **Security Monitoring**
   * Detect unauthorized packet injection or suspicious traffic patterns.
   * Validate that packets are reaching only the intended destinations.
6. **Educational & Research Purpose**
   * Demonstrates practical network troubleshooting methods.
   * Useful for training in network monitoring and packet-level analysis in enterprise setups.

## CHAPTER 3

**PROBLEM ANALYSIS**

**1. Background**

Modern networks involve multiple interconnected departments, routers, switches, and servers. While data travels from a client machine (PC) to a destination server, it passes through several devices. Without proper monitoring, it becomes difficult to identify where delays, losses, or malicious activities occur.

**2. Problem Statement**

In complex departmental networks:

* **Packet tracking is difficult** without dedicated monitoring tools.
* **Fault isolation** becomes time-consuming when multiple routers and switches are involved.
* **Security breaches** (e.g., packet sniffing by attackers) can occur without detection.
* **Performance issues** like packet loss, congestion, or routing delays often go unnoticed until they impact users.

**3. Key Issues Identified**

1. **Lack of visibility** into packet flow between nodes.
2. **Unidentified bottlenecks** in communication between departments and the server.
3. **No real-time capture** of inter-router and inter-department traffic.
4. **Difficult to pinpoint faults** at Layer 1, Layer 2, or Layer 3 without a structured approach.
5. **Security gaps** due to unmonitored internal traffic.

**4. Need for a Solution**

To ensure **efficient, secure, and reliable communication**, it is necessary to:

* Deploy **network sniffers** at strategic points.
* Capture and analyse packets **between PCs, switches, and routers**.
* Track the **entire flow** from request initiation to server response.
* Identify **network performance issues** and **potential intrusions** quickly.

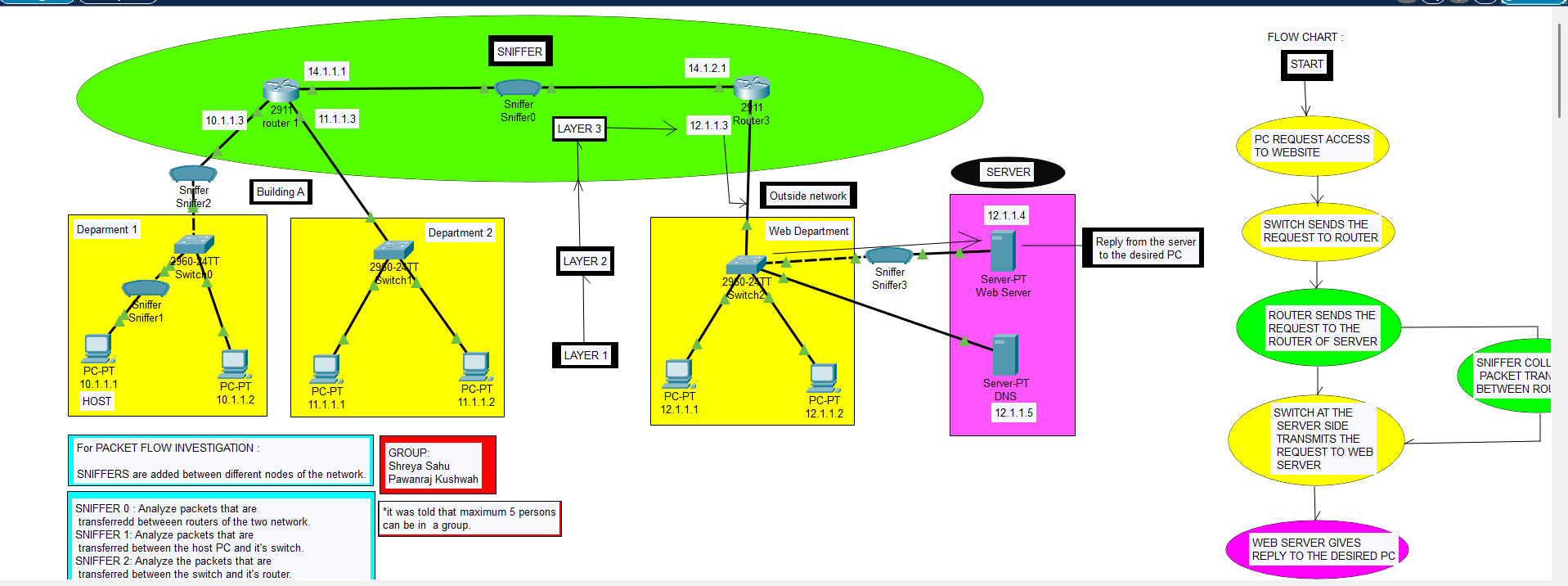
**5. Expected Outcome**

By implementing packet sniffers and structured monitoring:

* The **path of packets** will be clearly understood.
* **Performance metrics** (latency, loss, throughput) will be measurable.
* **Network troubleshooting time** will be reduced.
* **Security monitoring** will be enhanced.

## CHAPTER 4

**OUTPUTS**



## CHAPTER 4

**CONCLUSION**

The packet flow investigation successfully demonstrates how strategic placement of sniffers within a network can provide complete visibility into data transmission between various devices, including PCs, switches, routers, and servers. By capturing packets at multiple layers, the system enables precise identification of delays, bottlenecks, and anomalies in real time.

This approach not only improves **network troubleshooting efficiency** but also strengthens **security monitoring** by detecting suspicious traffic patterns early. The structured flow—from user request to server response—ensures a clear understanding of how data moves across the network, helping administrators make informed optimization decisions.

Ultimately, implementing such a monitoring mechanism leads to **faster fault isolation, better performance management, and enhanced overall reliability** of the network infrastructure.