**CS221 L**

**Network and firewall management**

* **Inshaal Sheeraz 2023260**
* **Arham Khalid 2023128**
* **Ajwa Asghar 2023092**

**Introduction**

In today’s interconnected world, household networks host a variety of devices ranging from personal computers and smartphones to IoT-enabled appliances. Ensuring smooth communication and robust security among these devices is critical. This proposal outlines a Network and Firewall Management System that leverages a structured representation of household devices and data packets for efficient routing and security.

Objectives

* Device Management: Represent all household devices in a structured format with unique identification.
* Data Packet Management: Implement a linked list-based system for packet representation and processing.
* Firewall Functionality: Scan and validate data packets to ensure error-free and secure communication.
* Network Efficiency: Route valid data packets to their intended destination within the household network.

**System Design**

**1. Device Representation**

Household devices will be modeled as nodes in a graph. Each node will be a struct containing:

* MAC Address (e.g., 00:1A:2B:3C:4D:5E or similar patterns) A unique identifier for each device.
* Device Type: A string or enumerator specifying the type of device (e.g., Laptop, Smartphone, IoT\_Device).

**2. Network Representation**

The devices will form a graph where:

* Each device node is connected to other nodes representing communication paths.
* Edges between nodes indicate a possible direct communication link.

**3. Data Packet Representation**

Data packets will be modeled as nodes in a linked list. Each node will contain:

* **Packet ID**: A unique identifier for the data packet.
* **Source MAC Address**: The origin of the packet.
* **Destination MAC Address**: The intended recipient.
* **Data Payload**: The content of the packet.
* **Error Flag**: A boolean indicating if the packet contains errors.

**4. Firewall Functionality**

The firewall will process data packets before routing. The steps include:

* **Error Check**: If the errorFlag is set, the packet is discarded.
* **Destination Validation**: Ensure the destination MAC address is part of the household network.
* **Criteria Check**: Validate the packet against predefined security or content criteria.

**5. Routing Mechanism**

Valid packets will be routed using the graph representation of devices:

1. Identify the source and destination nodes in the graph.
2. Use a traversal algorithm (e.g., BFS or DFS) to find the shortest path for communication.
3. Deliver the packet to the destination node.

**Implementation Plan**

**Phase 1: System Design**

* Define the DeviceNode and DataPacket structs.
* Implement a graph structure to represent the network.

**Phase 2: Packet Processing**

* Develop the linked list-based data packet management.
* Write functions to scan packets for errors, validate destinations, and check criteria.

**Phase 3: Routing and Communication**

* Implement graph traversal for routing.
* Integrate the firewall and routing mechanisms.

**Phase 4: Testing and Deployment**

* Simulate a household network with multiple devices and packet exchanges.
* Test edge cases, including invalid packets and unreachable destinations.

**Benefits**

* **Security**: The firewall ensures only valid packets are routed, reducing the risk of attacks or data leaks.
* **Efficiency**: The graph-based network and linked list packet system offer structured and optimized communication.
* **Scalability**: The design can easily accommodate additional devices or network nodes.