Premier University, Department of CSE
6th Semester, Assignment, Fall 2024
Course Title: Computer Networks, Course Code: CSE 367
Course Outcome: CO3 Total Marks: 10

Problem Statement:

You are the network architect for MetroRail Transit Authority (MTA), which operates an extensive railway network across five major metropolitan cities:

- Dhaka (Main Branch) – Central Operations Hub
- Chittagong (City Branch) – South Maintenance Hub
- Sylhet (City Branch) – South-West Control Center
- Rajshahi (City Branch) – Disaster Recovery & Data Redundancy Center
- Khulna (City Branch) – East Expansion & Future Network Scaling

The transit authority plans to upgrade its network infrastructure to support an intelligent railway system that ensures secure, efficient, and high-speed connectivity between stations, control centers, and maintenance hubs. The system will leverage IPv6 adoption, VLAN segmentation, and SD-WAN for secure interconnectivity.

Your task is to design a scalable, secure, and resilient network architecture for this international railway system while ensuring optimal data flow, passenger service reliability, and security against cyber threats.

Network Design Requirements:

1. **IPv4 Addressing Scheme:**
   - Each railway station should be assigned a unique IPv4 subnet for better scalability.
   - The central operations hub in Dhaka will manage over 10 railway stations, each requiring IPv4 allocation for IoT sensors, surveillance cameras, ticketing systems, and passenger Wi-Fi.
   - All other regional hubs should also maintain separate IPv4 subnets for their allocated stations and maintenance facilities.
2. **Network Segmentation & VLANs:**
   - **Use VLANs to separate network traffic for:**
     - Operational Traffic (Train control, scheduling, real-time train tracking)
     - Security & Surveillance (CCTV, alarm systems)
     - Passenger Services (Public Wi-Fi, ticketing kiosks)
   - **Implement inter-VLAN routing for necessary communication while enforcing security policies.**
3. **SD-WAN Implementation:**
   - Each hub must connect to other hubs using SD-WAN to optimize traffic flow.
   - Implement QoS (Quality of Service) to prioritize real-time train control data over passenger Wi-Fi.
   - SD-WAN must support failover mechanisms in case a regional hub loses connectivity.
4. **Security Policies & Firewall Rules:**
   - Restrict external access to core railway operations.
   - Whitelist only specific traffic between hubs (e.g., control data from Dhaka

to Chittagong).
- Implement Zero Trust Security, ensuring authentication before any inter-region communication.

5. Redundancy & Failover Mechanism:

- Deploy backup links for critical railway communication in case of network failures.
- Set up a disaster recovery site in Rajshahi to handle data backup and system failover.

6. Traffic Control & Filtering:

- Limit passenger Wi-Fi speeds to prevent excessive congestion.
- Monitor and block unauthorized access to sensitive railway databases.
- Filter traffic from external networks to prevent cyber threats.

Deliverables:

1. IPv4 Addressing Plan:

- Provide a structured IPv4 subnet breakdown for each regional hub and railway station.
- Explain how the addressing scheme ensures scalability, efficiency, and security.

2. Network Diagram:

- **High-level design of the intelligent railway network, showing:**
  - Interconnectivity between hubs and stations
  - SD-WAN architecture for secure routing
  - Firewalls and access control policies

3. SD-WAN Configuration Plan:

- Define traffic prioritization policies for operational data vs. passenger services.
- Specify how automatic failover mechanisms work during network failures.

4. Security & Firewall Configuration:

- Implement firewall policies to restrict access to railway control systems.
- Define Zero Trust authentication rules for cross-hub communication.

5. Justifications & Scalability Considerations:

- Explain how the design scales as new railway stations are added.
- Discuss potential challenges in cybersecurity, bandwidth management, and redundancy.

Key Considerations:

• **Security:** Protect critical train control systems from external threats.
• **Scalability:** Ensure the network can grow as more cities join the MetroRail system.
• **Reliability:** Implement redundant links and disaster recovery to ensure 24/7 operations.
• **Efficiency:** Optimize bandwidth usage to balance passenger services and railway control data.