BAHRIA UNIVERSITY, Karachi Campus

Department of Software Engineering

REPORT

Course Title: **Course Code**:

Course Instructor: **Class**: BSE- (A/B/C)

Lab Instructor: Engr. Asma Shaheen **Name:** _____

PROJECT TITLE:

GROUP MEMBERS LIST:

S.NO	Enrollment	Name	Email
1	02-131222-085	Syed Ahnaf Raza	syahra2014@gmail.com
2	02-131222-062	Memoona Iqbal	memoonaiqbal3710@gmail.com
3	02-131222-47	Seemab Asghar	seemabasghar64@gmail.com
4	02-131222-0	Izaan Abdullah	Izaanabdullah90@gmail.com

SUBMISSION DATE: _____

Contents

ABSTRACT

The **Smart Disaster Response Network** project aims to address the challenges of disaster management by providing a secure, reliable, and efficient communication network for emergency services. In disaster scenarios, effective communication is crucial for coordinating response efforts and ensuring the safety of affected individuals. This network, modeled using **Cisco Packet Tracer**, integrates multiple technologies to create a cohesive infrastructure that supports communication between emergency departments such as **fire stations**, **police stations**, **hospitals**, and the **Emergency Operations Center (EOC)**.

The proposed solution features centralized routing through the **EOC switch**, with **VLAN segmentation** for network isolation, and **Quality of Service (QoS)** for traffic prioritization, ensuring that critical communication data is prioritized during emergencies. To enhance network security, **Access Control Lists (ACLs)** and **Port Security** are implemented to prevent unauthorized access, ensuring that only authorized devices can connect to the network. **IoT devices**, such as **weather sensors**, **CCTV cameras**, and **sirens**, are integrated to provide real-time disaster monitoring and response, further improving the network's overall efficiency.

The **EIGRP** protocol is used for dynamic routing, ensuring fast convergence of routing information across the network. Additionally, **Syslog** and **SNMP** monitoring are employed for centralized event logging and network performance monitoring, respectively. The use of **port security** prevents unauthorized devices from accessing critical network resources, securing the system during emergency operations.

This network design ensures that disaster response teams can communicate effectively, prioritize vital data, and secure network access during times of crisis. The project also explores the potential for future improvements, such as the implementation of **IPSec VPNs** for secure inter-department communication and the expansion of IoT capabilities to automate alerts and response actions.

By leveraging Cisco technologies, this project demonstrates how advanced network configurations can provide reliable communication systems in disaster response scenarios, supporting faster, coordinated action when lives are on the line.

1. Introduction

1.1 Introduction

This project implements a **Smart Disaster Response Network** designed to ensure effective communication between emergency services such as fire stations, police stations, hospitals, and the Emergency Operations Center (EOC). Using **Cisco Packet Tracer**, the network is modeled with real-world functionalities like IoT integration, VLAN segmentation, QoS, ACLs, Port Security, and Syslog for monitoring.

1.2 Problem Statement

Disasters often cause communication breakdowns, delaying coordination between emergency teams. The lack of a centralized, reliable, and secure communication backbone can hinder response efforts and exacerbate the crisis. Unauthorized devices accessing the network during emergencies can also pose significant security risks.

1.3 Proposed Solution

The network is designed with the following features to ensure efficient and secure communication:

- **Centralized routing via the EOC switch**, ensuring all communication between departments (police, fire stations, hospitals) goes through the EOC.
- **IoT integration** for real-time disaster monitoring and response.
- **Secure communication** using ACLs.
- **Port Security** to restrict unauthorized device connections and ensure network integrity.
- **Traffic prioritization via QoS** to handle emergency data.

2. Design

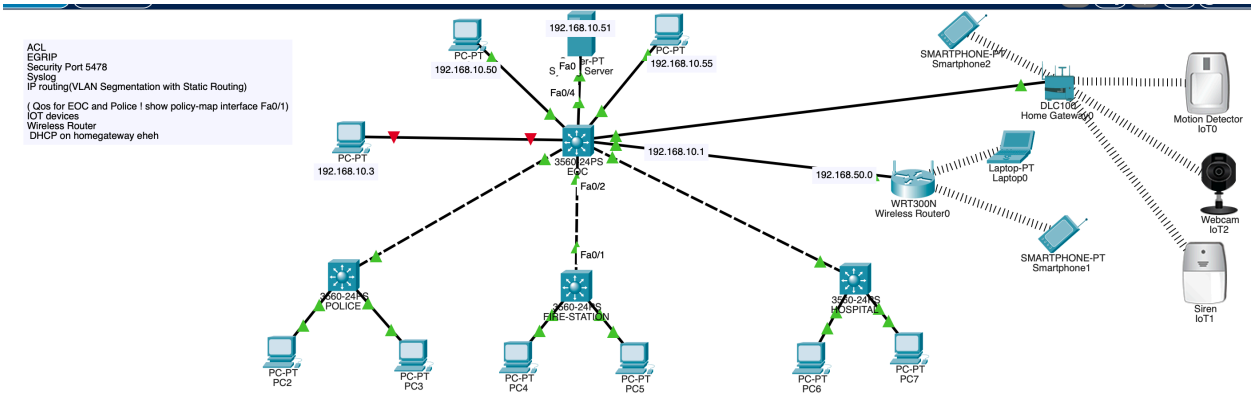
2.1 Workflow Diagram

The network workflow begins with:

- **Emergency Detection:** IoT devices (e.g., weather sensors, CCTV cameras) detect and send data to the EOC.
- **Data Processing:** EOC processes data and shares updates with police, fire, and hospitals.
- **Communication:** Departments interact with the EOC but cannot directly communicate with each other.
- **Monitoring:** Syslog servers log events, and SNMP traps provide alerts.
- **Port Security:** Prevents unauthorized devices from accessing the network during emergencies.

2.2 User Interfaces (Packet Tracer, Physical View)

- **Physical View:** Displays the physical setup, including 4 Layer 3 switches, IoT devices, and wireless router and a homegateway.



- **Logical View:** Showcases VLAN segmentation, routing tables, and secured port configurations.

PC	VLAN	IP Address	Gateway
EOC PC 1	VLAN 10	192.168.10.10	192.168.10.1
EOC PC 2	VLAN 10	192.168.10.11	192.168.10.1
Police PC 1	VLAN 20	192.168.20.10	192.168.20.1
Police PC 2	VLAN 20	192.168.20.11	192.168.20.1
Hospital PC 1	VLAN 30	192.168.30.10	192.168.30.1
Hospital PC 2	VLAN 30	192.168.30.11	192.168.30.1
Fire Station PC 1	VLAN 40	192.168.40.10	192.168.40.1
Fire Station PC 2	VLAN 40	192.168.40.11	192.168.40.1

ACls:-

Source VLAN	Destination VLAN	Action
EOC (10)	Police (20)	Allow
EOC (10)	Hospital (30)	Allow
EOC (10)	Fire Station (40)	Allow
Police (20)	Hospital (30)	Deny
Police (20)	Fire Station (40)	Deny
Hospital (30)	Police (20)	Deny
Hospital (30)	Fire Station (40)	Deny

QoS configuration for **FastEthernet0/1** based on the output of show policy-map interface FastEthernet0/1:

Class-map	Match Criteria	Packets Matched	Bytes Matched	Offered Rate (5 mins)	Drop Rate (5 mins)	Queueing Type	Bandwidth (%)	Bandwidth (kbps)	Burst (Bytes)	Drops
Critical-Traffic	access-group 105	10	280	0 bps	0 bps	Strict Priority	50%	50000	1250000	0
class-default	any	3660	285483	156 bps	0 bps	Default Queueing	N/A	N/A	N/A	N/A

1. **Critical-Traffic Class:**
   - **Match Criteria:** Traffic matching access list 105.
   - **Queueing:** Strict priority queuing, meaning that this traffic will be processed first and will not be queued behind other types of traffic.
   - **Bandwidth Allocation:** 50% of the available bandwidth (50,000 kbps) and a burst allowance of 1,250,000 bytes.
   - **Matched Traffic:** 10 packets and 280 bytes have matched this class, with zero drops so far.
2. **Class-default:**
   - **Match Criteria:** Matches any traffic that does not match the Critical-Traffic class.
   - **Offered Rate:** The 5-minute offered rate is 156 bps, with no drops observed.
   - **Queueing:** Default queueing behavior, which uses weighted fair queuing (WFQ) or a similar default mechanism.
3. show port-security command: This table summarizes the port security status of the specified ports on the switch.

Secure Port	Max Secure Addr (Count)	Current Addr (Count)	Security Violation (Count)	Security Action
Fa0/4	1	1	0	Shutdown
Fa0/5	1	1	1	Shutdown
Fa0/7	1	1	0	Shutdown
Fa0/8	1	1	1	Shutdown

EIGRP Configuration Overview

Aspect	Details
EIGRP Process	router eigrp 1
Networks Configured	- 192.168.10.0/24 - 192.168.1.0/30 - 192.168.30.0/24 - 192.168.2.0/30 - 192.168.40.0/24 - 192.168.3.0/30
Auto-Summary	Disabled (no auto-summary)

EIGRP Neighbors

Neighbor IP	Interface	Hold Time (sec)	Uptime	SRTT (ms)	RTO (ms)	Queue (Cnt)	Sequence #
192.168.2.2	Fa0/2	11	01:00:30	40	1000	0	64
192.168.1.2	Fa0/1	14	01:00:29	40	1000	0	66
192.168.3.2	Fa0/3	13	01:00:29	40	1000	0	63

EIGRP Topology Table

Network	Successors	FD (Feasible Distance)	Next Hop	Interface
192.168.1.0/30	1	28160	Connected	Fa0/1
192.168.2.0/30	1	28160	Connected	Fa0/2
192.168.3.0/30	1	28160	Connected	Fa0/3
192.168.10.0/24	1	25625600	Connected	Vlan10
192.168.20.0/24	1	25628160	192.168.1.2	Fa0/1
192.168.30.0/24	1	25628160	192.168.2.2	Fa0/2
192.168.40.0/24	1	25628160	192.168.3.2	Fa0/3

EIGRP Routing Table

Network	Next Hop	Metric (FD)	Interface
192.168.3.0/30	192.168.3.2	25628160	Fa0/3
192.168.20.0/24	192.168.1.2	25628160	Fa0/1
192.168.30.0/24	192.168.2.2	25628160	Fa0/2
192.168.40.0/24	192.168.3.2	25628160	Fa0/3

- **Networks**: Six networks are advertised by the EIGRP process.
- **Neighbors**: Three neighbors are established on FastEthernet interfaces (Fa0/1, Fa0/2, Fa0/3).
- **Topology**: Displays the topology and reachable networks with their corresponding next-hop IPs and interfaces.
- **Routing Table**: Displays the EIGRP-learned routes with the next-hop IP and the interface they will exit.

ACLs:-

ACL Name	Entry	Action	Source IP	Source Wildcard	Destination IP	Destination Wildcard	Matches
100	10	Permit	192.168.10.0	0.0.0.255	192.168.20.0	0.0.0.255	12
100	20	Permit	192.168.10.0	0.0.0.255	192.168.30.0	0.0.0.255	21
100	30	Permit	192.168.10.0	0.0.0.255	192.168.40.0	0.0.0.255	5
100	40	Deny	Any	N/A	Host 255.255.255.255	N/A	2
105	10	Permit	192.168.10.0	0.0.0.255	Any	N/A	N/A

This table summarizes the ACL entries, the action (permit or deny), the source and destination IP ranges, the wildcard mask, and the number of matches for each entry.

ACL 100:

- **Entry 10**:
  - **Action**: **Permit**
  - **Source**: 192.168.10.0/24 (any IP in this range)
  - **Destination**: 192.168.20.0/24 (any IP in this range)
  - **Matches**: 12
    This entry allows traffic from the **192.168.10.0/24** network to the **192.168.20.0/24** network.
- **Entry 20**:
  - **Action**: **Permit**
  - **Source**: 192.168.10.0/24
  - **Destination**: 192.168.30.0/24
  - **Matches**: 21
    This entry permits traffic from the **192.168.10.0/24** network to the **192.168.30.0/24** network.
  -
- **Entry 30**:
  - **Action**: **Permit**
  - **Source**: 192.168.10.0/24
  - **Destination**: 192.168.40.0/24
  - **Matches**: 5
    This entry permits traffic from the **192.168.10.0/24** network to the **192.168.40.0/24** network.
- **Entry 40**:
  - **Action**: **Deny**
  - **Source**: Any IP
  - **Destination**: 255.255.255.255 (broadcast address)
  - **Matches**: 2
    This entry denies any traffic destined for the **broadcast address (255.255.255.255)**, which is typically used for broadcast messages.

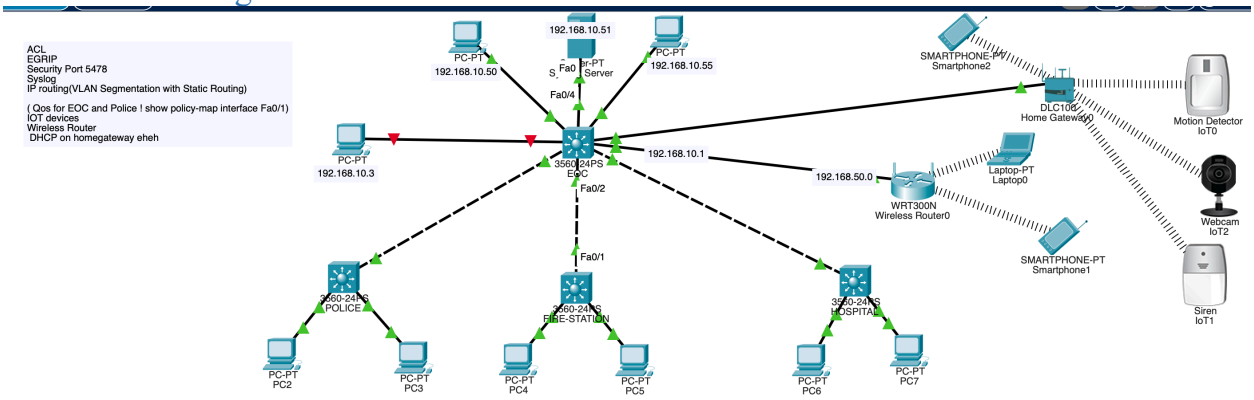
ACL 105:

- **Entry 10**:
  - **Action**: **Permit**
  - **Source**: 192.168.10.0/24
  - **Destination**: Any IP address
    This entry allows all traffic from the **192.168.10.0/24** network to any destination. This is generally used to allow unrestricted traffic from a specific source network.

Summary of what this ACL configuration does:

- **ACL 100** defines rules that permit communication between different networks (192.168.10.0/24 to 192.168.20.0/24, 192.168.30.0/24, and 192.168.40.0/24), while also denying traffic directed to the broadcast address **255.255.255.255**.
- **ACL 105** is more general, permitting any traffic from **192.168.10.0/24** to anywhere (not restricted to specific destination IPs).

2.3 Network Diagram



The network includes:

- **EOC Switch:** Core switch connecting all departments.
- **Police, Fire, and Hospital Switches:** Layer 3 switches connected via trunk links to the EOC.
- **IoT Devices:** Weather sensors and CCTV cameras connected to the EOC.
- **Wireless Router:** Enables mobile devices to connect with the EOC.
- **Secure Ports:** All access ports implement Port Security to restrict unauthorized connections.

3. Methodology

3.1 Technologies Used

3.1.1 Networking Devices

- **4 x Cisco Layer 3 Switches (3560).**
- **1 x Wireless Router. 1 x Homegateway.**
- **Mobile Devices**
- **IoT Devices** (Weather sensors, CCTV cameras, Sirens).

3.1.2 Protocols

- **EIGRP (Enhanced Interior Gateway Routing Protocol):**
  - Provides dynamic routing between switches and routers.
  - Ensures fast convergence and efficient routing of disaster data.
  - **Commands to Configure EIGRP:**

```
enable
configure terminal
router eigrp 1
network 192.168.10.0 0.0.0.255
network 192.168.20.0 0.0.0.255
network 192.168.30.0 0.0.0.255
network 192.168.40.0 0.0.0.255
end
```

- **ACLs (Access Control Lists):**
  - Restricts communication between departments to ensure security and proper segregation.
  - **Commands to Configure ACLs:**

```
access-list 100 deny ip 192.168.20.0 0.0.0.255 192.168.40.0 0.0.0.255
access-list 100 permit ip any any
interface vlan 10
ip access-group 100 in
```

- **QoS (Quality of Service):**
  - Prioritizes emergency traffic from IoT devices and EOC systems to ensure critical data gets delivered without delays.
  - **Commands to Configure QoS:**

```
enable
configure terminal
class-map match-all Emergency_Traffic
match access-group 100
policy-map Priority
class Emergency_Traffic
priority 1000
```

```
interface FastEthernet0/1
service-policy output Priority
```

- **Port Security:**
  - Prevents unauthorized access at the port level using sticky MAC addressing.
  - **Commands for Port Security:** See Section 3.4 below.

3.1.3 Configuration Tools

- **Cisco Packet Tracer:** Used to model, simulate, and test the Smart Disaster Response Network.
  - **Features Used:**
    - Device Placement: Adding routers, switches, and IoT devices.
    - CLI Configuration: Setting up VLANs, EIGRP, ACLs, Port Security, and QoS, DHCP.
    - Simulations: Verifying data flow, security violations, and real-time traffic.

3.1.4 Additional Concepts

- **Syslog:**
  - Centralized logging of network events for troubleshooting and monitoring.
  - **Commands to Configure Syslog:**

```
enable
configure terminal
logging 192.168.10.11
logging trap warnings
exit
```

- **DHCP:**
  - Assigns IP addresses to IoT devices via the Home Gateway in the EOC.
  - **Commands to Configure DHCP:**

```
enable
configure terminal
ip dhcp pool IoT_Devices
network 192.168.30.0 255.255.255.0
default-router 192.168.30.1
dns-server 8.8.8.8
exit
```

- **Sticky MAC Addressing:**
  - Dynamically learns and binds MAC addresses to ports to prevent unauthorized devices.
  - **Commands:** See Section 3.4 below.

3.1.4.1 Port Security Implementation

- **Configuration on Access Ports:**
  - Limits ports to a single authorized device using sticky MAC addressing.
  - Shuts down ports on violation to prevent unauthorized access.
- **Commands:**

```
interface FastEthernet0/5
switchport mode access
switchport port-security
switchport port-security maximum 1
switchport port-security mac-address sticky
switchport port-security violation shutdown
```

- **Verification:**

```
show port-security interface fastethernet 0/5
```

- **Recovery:**

```
interface FastEthernet0/5
shutdown
no shutdown
```

3.2. Network Communication Methodology

In the **Smart Disaster Response Network**, communication is structured to ensure that the right information is sent to the right places at the right time, with high levels of security and traffic prioritization. The methodology follows a logical flow designed to prioritize critical communications while limiting access to sensitive resources. Here's an overview of how communication happens within the network:

1. Communication Flow

- **Emergency Operations Center (EOC)**: The core of the network, all communication between the fire stations, police stations, hospitals, and other emergency entities flows through the **EOC Switch**. This ensures centralized control and monitoring of all emergency responses. The **EOC** processes real-time data from IoT devices (e.g., weather sensors, CCTV cameras, and sirens) and sends relevant updates to the appropriate departments.
- **Departments (Fire Stations, Police Stations, Hospitals)**: These departments can communicate only with the **EOC** and not directly with each other. This segmentation is critical for maintaining order and security, preventing cross-communication that may not be needed or could interfere with emergency operations. By routing all inter-department communication through the **EOC**, the network ensures that no unauthorized communication occurs between departments.
- **IoT Devices**: **IoT devices** (e.g., weather sensors, CCTV cameras, sirens) are integrated into the network and send data directly to the **EOC**. These devices are part of a larger monitoring system that ensures the EOC is kept up-to-date with real-time disaster information. The IoT devices do not communicate directly with other departments, maintaining their role as passive data sources.

2. Communication Restrictions

- **Access Control Lists (ACLs)**: ACLs are used to restrict the communication between different departments.
    - For example, **ACL 100** permits communication between the **EOC** (192.168.10.0/24) and fire, police, and hospital networks (192.168.20.0/24, 192.168.30.0/24, 192.168.40.0/24), ensuring that each department can send and receive necessary emergency data from the EOC.
    - The **EOC** is the only entity that can communicate with all departments, while **police**, **fire**, and **hospital networks** are restricted from directly communicating with each other.
    - This control is achieved using the ACL's **permit** and **deny** actions that define which IP ranges can send traffic to other ranges.
- **Port Security**: Port Security mechanisms are implemented to prevent unauthorized devices from accessing the network during critical operations.
    - Ports are configured to accept only authorized devices with **sticky MAC addresses**. If an unauthorized device attempts to connect, the port is immediately shut down, preventing any potential security breaches.

- **Quality of Service (QoS)**: QoS is crucial for prioritizing emergency traffic. Using a **policy-map** that prioritizes **Critical-Traffic** (e.g., IoT data or alerts), the network ensures that emergency messages and data from the **EOC**are delivered without delay, even under heavy network load. **Critical-Traffic** is given strict priority, while non-essential traffic is handled in a default manner.

3. Network Segmentation and Isolation

- **VLAN Segmentation**: Different networks for police, fire stations, hospitals, and the **EOC** are segmented into separate **VLANs** to ensure that communication is organized and controlled. The VLANs are:
    - **VLAN 10**: EOC Network
    - **VLAN 20**: Police Station Network
    - **VLAN 30**: Fire Station Network
    - **VLAN 40**: Hospital Network
- These VLANs are separated using Layer 3 switches, which handle the routing between VLANs. This isolation prevents unauthorized or accidental communication between departments and ensures that only necessary data is exchanged.

4. Communication Protocols and Routing

- **EIGRP**: The **Enhanced Interior Gateway Routing Protocol (EIGRP)** is used for dynamic routing across the network. It ensures that all departments can communicate with the **EOC** efficiently, even if the network topology changes. Each department's router advertises its network to the **EOC's** router, which learns the best route for traffic to follow.
    - For example, the **EOC** router knows how to route packets from the **police network** (192.168.20.0/24) to the **fire station network** (192.168.30.0/24) or the **hospital network** (192.168.40.0/24) based on the EIGRP routing table.

5. Security and Monitoring

- **Syslog**: All network activities, including communication and access attempts, are logged to a centralized **Syslog**server. This allows the **EOC** or network administrators to monitor the network for any suspicious or unauthorized activities. Alerts are generated for any security violations, providing a real-time picture of the network's status.
- **SNMP Traps**: SNMP traps are configured to send alerts to network administrators in case of critical events like device failures, port security violations, or network outages.

Summary

The **Smart Disaster Response Network** ensures that communication is efficient, secure, and centralized. By using **EOC-based communication**, **ACLs**, **QoS**, and **Port Security**, the network prioritizes critical data and ensures that only authorized entities can communicate with each other.

4. Conclusions and Further Work

Conclusions:

The **Smart Disaster Response Network** provides a centralized, secure, and efficient communication system for handling emergencies. With features like QoS, IoT integration, ACLs, and Port Security, the network ensures priority for critical traffic, restricts unauthorized communication, and enhances security by preventing unauthorized access.

Further Work:

- Implement **IPSec VPNs** to enhance security for inter-department communication.
- Introduce redundancy with protocols like **HSRP** for gateway failover.
- Expand IoT capabilities to include advanced automation and alerting.
- Integrate **802.1X authentication** for enhanced port-level security.

5. References

1. Cisco Packet Tracer Documentation: Cisco NetAcad.
2. EIGRP Configuration Guide: Cisco.
3. Port Security Configuration Guide: Cisco.
4. ACLs and Access Control: Cisco Security.

Github Repo:-

https://github.com/syahra712/CCN-Semester-Project