Jinnah University for Women
Department of Computer Science and Software Engineering
Batch: BSSE 2022
Computer Networks - CSS 3071

Theory Assignment

Question # 1

Task Details:

You have been appointed as a Network System Administrator by the SoftTech company in Sydney to allocate public IP Version 4 (IPv4) address into 3 different locations, "2 remote offices (Melbourne and Adelaide) and also one main office in Sydney". The major task is to allocate the unreserved public IPv4 addresses to different offices.

Requirements:

Your network design needs 4 subnets:

- Subnet A (Sydney): It requires 63 IP addresses (60 for PCs and 2 for servers (Windows, Fax), and 1 for router interface).
- Subnet B (Melbourne): It requires 53 IP addresses (50 for PCs and 2 for servers (DNS, Database), and 1 for router interface).
- Subnet C (Adelaide): It requires 43 IP addresses (40 for PCs and 2 for servers (Linux, Application).
- Subnet D (Between two routers): It requires just 2 IP addresses.

You need to use routers and switches to make a connection among devices and also between networks. Each office has its applications, but some applications require inter-department data transfer. All workstations need internet access, company intranet access, and also access to a wireless network. You need to come with a design report and send it to your technical manager.

Report: The report must contain the following sections:

- **Introduction:**

Critical analysis of networking requirements.

- **Local Area Network (LAN):**

Design and description of Local Area Network for all subnet which must include:

- Network topology; Discuss the reasons for choosing the particular network topology.
- LAN design connections to the servers, connection to other subnets, and also the internet.

- IP addresses: Find all network and host addresses including subnet masks according to the requirements by using the private address with your choice.

- **Hardware:**

Provide a complete description of all interconnecting devices (switches, routers, hubs, and access points) and wiring used to build the network. Justify your choice.

- **Conclusion:**

A comprehensive summary of the work done and recommendations.

Network Design Report

1. Introduction:

SoftTech's network infrastructure needs to accommodate three offices in Sydney, Melbourne, and Adelaide, each with its specific requirements. The primary challenge is to allocate IPv4 addresses efficiently while ensuring seamless connectivity, security, and scalability. This report presents a comprehensive network design solution to meet these requirements.

2. Local Area Network (LAN):

a) Network Topology:

The chosen network topology is a hierarchical design with a core, distribution, and access layer. Each office will have its access layer switches connected to distribution switches, which in turn connect to the core switch. This design ensures efficient traffic flow and easy scalability.

b) LAN Design Connections:

- **Sydney Office (Subnet A):**

- Connection to servers (Windows, Fax): Directly connected to access layer switch.

- Connection to other subnets: Through the distribution switch and the core switch.

- Internet access: Provided through the core switch's connection to the internet gateway.

- **Melbourne Office (Subnet B) and Adelaide Office (Subnet C):**

- Similar setup as Sydney office with connections to respective servers, other subnets, and internet access through the core switch.

- **Inter-Department Data Transfer:**

- Achieved through VLANs (Virtual Local Area Networks) configured on switches, allowing secure communication between departments.

- **Wireless Network Access**:

- Provided through access points connected to the access layer switches in each office.

c) IP Addresses:

Using private addresses from the range 192.168.0.0/16, the subnetting for each office is as follows:

- **Subnet A (Sydney):**

- Network Address: 192.168.1.0
- Subnet Mask: 255.255.255.192
- Host Range: 192.168.1.1 to 192.168.1.62
- Router Interface: 192.168.1.63

- **Subnet B (Melbourne):**

- Network Address: 192.168.2.0
- Subnet Mask: 255.255.255.192
- Host Range: 192.168.2.1 to 192.168.2.62
- Router Interface: 192.168.2.63

- **Subnet C (Adelaide):**

- Network Address: 192.168.3.0
- Subnet Mask: 255.255.255.192
- Host Range: 192.168.3.1 to 192.168.3.62
- Router Interface: 192.168.3.63

- **Subnet D (Between two routers):**

- Network Address: 192.168.4.0
- Subnet Mask: 255.255.255.252

- Host Range: 192.168.4.1 to 192.168.4.2

3. Hardware:

- Switches: Cisco Catalyst 2960X Series for access and distribution layers, Cisco Catalyst 3850 Series for the core layer.
- Routers: Cisco ISR 4000 Series routers for interconnecting subnets and providing internet access.
- Access Points: Cisco Aironet 2800 Series for wireless connectivity.
- Wiring: Cat6 Ethernet cables for reliable and high-speed connections.

Justification:

- Cisco devices are chosen for their reliability, scalability, and robust security features.
- The chosen wiring ensures Gigabit Ethernet connectivity, meeting the bandwidth requirements for modern applications.
- VLANs are used for segmentation and security, allowing for efficient management of network resources.

4. Conclusion:

The proposed network design effectively meets SoftTech's requirements for IP address allocation, inter-office connectivity, internet access, and wireless network support. The hierarchical topology, along with VLAN segmentation, ensures efficient traffic flow, scalability, and security. Implementing Cisco devices and Cat6 wiring guarantees a robust and high-performance network infrastructure. Additional security measures like firewalls and intrusion detection/prevention systems can further enhance network security. Overall, this design provides a solid foundation for SoftTech's network operations and future growth.

Question # 2

Write down the summary of the following research paper:

> Fiţigău and G. Toderean, "Network performance evaluation for RIP, OSPF and EIGRP routing protocols," *Proceedings of the International Conference on ELECTRONICS, COMPUTERS and ARTIFICIAL INTELLIGENCE - ECAI-2013*, Pitesti, 2013, pp. 1-4, doi: 10.1109/ECAI.2013.6636217.

Also, provide answers to the following questions referring to the above article

- The author defined three different types of routing protocols; Link-state routing protocol, Distance Vector routing protocol, and Hybrid routing protocol compare them, and explain the mechanism of updating routes?
- Identify Cisco proprietary control protocols and define the advantages of these protocols?
- Author created a simulated network environment to perform their experiments, Identify which simulator is used in their experiments and compare this simulator with packet tracer?
- The authors have used OSPF, RIP, and EIGRP protocols for the experiments. Explain the results of performance evaluation of these protocols.
- Which protocol has better results for the video transferring process and how?

Summary:

The paper investigates the performance of three routing protocols—RIP, OSPF, and EIGRP—within a network layer. It examines their effectiveness in routing packets for various applications such as video, HTTP, and voice. The study also includes analysis of network behavior during link failure/recovery using a controller between nodes. Additionally, the paper evaluates the protocols based on metrics like delay, FTP, email, HTTP, VoIP, and video conferencing through simulated network models.

In summary, the research emphasizes the crucial role of routing protocols in modern networks and compares the performance of RIP, OSPF, EIGRP, and IGRP. It concludes that EIGRP performs best for delay, email, and FTP, while OSPF and RIP are more suitable for real-time applications. The study underscores the significance of efficient routing protocols in managing user traffic in communication networks.

Answers of given questions:

1. **Types of Routing Protocols and Mechanism of Updating Routes:**
    - **Link-State Routing Protocol**: In this approach, each router maintains a detailed map of the entire network. When changes occur (such as link failures or additions), routers exchange link-state advertisements (LSAs) to update their maps. The **Dijkstra algorithm** is commonly used to compute the shortest path.
    - **Distance Vector Routing Protocol**: Routers periodically exchange routing tables containing distance metrics (e.g., hop count) to reach various destinations. The **Bellman-Ford algorithm** is often employed for route computation.

- **Hybrid Routing Protocol**: Combines features of both link-state and distance vector protocols. Examples include **EIGRP**, which uses a metric based on bandwidth and delay, and **OSPF**, which uses LSAs for topology updates.

2. **Cisco Proprietary Control Protocols and Their Advantages:**
   - **Cisco's EIGRP (Enhanced Interior Gateway Routing Protocol)**: A proprietary protocol with several advantages:
     - **Fast Convergence**: EIGRP quickly adapts to network changes, minimizing downtime.
     - **Bandwidth Optimization**: EIGRP uses bandwidth and delay metrics for route selection.
     - **Loop Prevention**: It employs the **Diffusing Update Algorithm (DUAL)** to prevent routing loops.
   - **Cisco's OSPF (Open Shortest Path First)**: Although not proprietary, OSPF is widely used in Cisco networks. Its advantages include:
     - **Scalability**: OSPF supports large networks efficiently.
     - **Fast Convergence**: It reacts swiftly to topology changes.
     - **Hierarchical Design**: OSPF organizes networks into areas for better management.
3. **Simulated Network Environment and Comparison with Packet Tracer:**
   - The authors created a simulated network environment for their experiments. Comparing this simulator with **Cisco Packet Tracer**:
     - **Packet Tracer**: Developed by Cisco, it is a network simulation tool primarily used for educational purposes. It allows users to design, configure, and troubleshoot networks.
     - The unnamed simulator used in the study may have different features or limitations compared to Packet Tracer.
4. **Performance Evaluation Results for OSPF, RIP, and EIGRP:**
   - The paper does not provide detailed results, but it evaluates the network performance of these protocols concerning video, HTTP, and voice applications.
   - For specific performance metrics (such as latency, throughput, or convergence time), further analysis would be needed.
5. **Best Protocol for Video Transfer:**
   - **OSPF** is often preferred for video streaming due to its scalability, fast convergence, and efficient use of network resources.