5.3.8: Reliable Network

Network Architecture

Networks must help a wide scope of applications and services, just as they work over a wide range of cables and devices, making up the physical infrastructure. In this specific situation, the term network architecture alludes to the technologies that help the foundation and the programmed services and rules, or protocols, that move data over the network.

As networks advance, there are four fundamental qualities that the underlying architectures need to deliver to meet users' needs:

- Fault Tolerance
- Scalability
- Quality of Service (QoS)
- Security

Fault Tolerance

The Internet is expected to be consistently accessible to many clients who depend on it. This requires a network architecture that is designed to tolerate flaws. A fault-tolerant network restrains the effect of failure, with the goal that the least number of devices are impacted. It is additionally designed to permit speedy recuperation when such a failure happens. These networks rely upon various ways between the source and destination of a message. If a path fails, the messages can be instantly sent over an alternate link. Having numerous ways to reach a destination is known as redundancy.

One way dependable networks give repetition is by executing a packet-switched network. Packet switching parts traffic into packets that are steered over a shared network.

Definition: Packet Switching

Packet switching is the process of breaking down data into small blocks called packets that are sent independently over a shared network. Each packet contains addressing information that allows it to be routed to the proper destination, where the packets are reassembled into the original data.

For example, a solitary message, an email, or a video stream, is broken into multiple message blocks, called packets. Every packet has a record of the addressing information for the source and destination of the message. Packet are routed independently and reassembled at the destination. This allows for efficient use of shared networks.

Scalability

A scalable network can grow rapidly to help new users and applications without affecting the service's performance being conveyed to existing users.

Another network can be effortlessly added to a current network. Furthermore, networks are versatile because the designers observe acknowledged protocols and standards. This permits software and hardware vendors to improve items and administrations without stressing over structuring another arrangement of rules for working inside the network.

Quality of Service

Ensuring quality of service (QoS) is becoming increasingly important in modern networks. With new applications, such as live video and voice transmissions, users expect a higher standard of service delivery. No one likes to watch a video that keeps pausing or buffering. As data, voice, and video content continue to merge onto the same network, QoS is an essential tool to manage congestion and ensure reliable delivery of content to all users.

Congestion happens when the interest for bandwidth surpasses the amount that is accessible. Network bandwidth is estimated in the number of bits transmitted in a solitary second or bits per second (bps). When synchronous correspondences have endeavored over the network, the interest for network bandwidth can surpass its accessibility, causing a network congestion.

When traffic volume is more than what can be shipped over the network, devices queue or hold the packets in memory until assets become accessible to transmit them.

With a QoS strategy, the router can deal with data and voice traffic progression, offering priority to voice communications if the network encounters congestion.

Security

Vital individual and business resources are the network infrastructure, services, and data on network-attached devices.

Two kinds of network security worries must be addressed: network infrastructure and information security.

Ensuring the physical security of devices providing network connectivity and preventing unauthorized access to management software.

Information security ensures the protection of data transmitted over networks and stored on attached devices. To accomplish the objectives of network security, there are three essential requirements:

- Confidentiality: Data secrecy implies that the planned and approved recipients can access and read information.
- Integrity: Data honesty affirms that the data has not been adjusted in transmission, from root to goal.
- Availability- Data accessibility implies confirmation of timely and solid access to information services for approved users.

We will delve deeper into the three requirements in a subsequent chapter.
