Network Management

Khaula Molapo

Week 1

20240001

1

Network management is the process of monitoring, controlling, and maintaining computer networks to ensure they operate efficiently. In a corporate LAN (Local Area Network), network management is used to connect employees' computers, printers, and servers while keeping the network secure and fast.

Network administrators use tools to track network performance, detect problems, and prevent downtime. They can monitor traffic, manage bandwidth, and configure devices like switches and routers. Security is also important, so administrators set up firewalls, access controls, and VPNs to protect sensitive data.

Effective network management helps companies avoid interruptions, improve communication, and maintain reliable connections for employees. It also allows IT teams to plan for future growth by upgrading network components and optimizing performance. Without proper network management, a corporate network can experience slow performance, security risks, and data loss, which could impact the company's productivity and reputation.

2

Nagios is a popular network management tool used to monitor computer networks, servers, and devices. Its purpose is to detect and alert administrators about network problems before they become serious.

Key features include real-time monitoring, automated alerts, and performance reporting. Nagios can track uptime, bandwidth usage, and the status of devices and services. It also provides notifications via email or SMS if a network issue occurs.

The role of Nagios in network management is to ensure the network runs smoothly, prevent downtime, and help administrators troubleshoot problems quickly. By providing clear insights, Nagios helps maintain reliable and secure network operations in organizations of all sizes.

3

Using Cisco Packet Tracer, I designed a simple corporate network with two switches, four computers, and a router. I configured IP addresses for each device, set up a default gateway, and tested connectivity using ping commands.

I also set up monitoring to check the status of each device and the network connections. Packet Tracer allowed me to simulate network traffic, view packet flow, and identify potential issues.

This practice helped me understand how network devices work together and how configuration affects communication. Monitoring is important because it ensures all devices are functioning correctly and helps prevent downtime. It also prepares me for managing real networks in professional environments.

4

The FCAPS framework is used in network management to organize key functions:

- Fault Management: Detects, logs, and resolves network problems to maintain smooth operations.

- Configuration Management: Tracks network devices, settings, and changes to ensure consistency.

- Accounting Management: Monitors bandwidth usage and resource consumption for cost and capacity planning.

- Performance Management: Measures network speed, traffic, and uptime to optimize efficiency.

- Security Management: Controls access, protects data, and prevents unauthorized activities.

Using FCAPS ensures all aspects of network management are covered. Each component supports network operations by improving reliability, performance, and security, making network management systematic and effective.