SECP1513: Technology Information System

Mind Map Chapter 6

Semester 1 2024/2025

1st December 2024

Faculty of Computing

Prepared by:

Muhammad Thaqif bin Abdul Aziz	SX231702ECJHF04
Aqilah binti Mohamad Kasim	SX231764ECRHF04
Muhammad Munzir bin Mohamed Dauzkaply Nor	SX240286ECRHS04

Network & Communication

Trends in Networking

Emerging Technologies
- Current trends in networking include advancements in 5G and Wi-Fi 6, which offer faster speeds, lower latency, and higher capacity.
- These technologies are transforming how users connect to the Internet and interact with devices, enabling more efficient communication.
- The adoption of these technologies is crucial for supporting the growing demand for high-speed connectivity.

Artificial Intelligence and Machine Learning
- AI and machine learning are increasingly being integrated into networking, providing predictive analytics and self-operating networks.
- These technologies enhance network management by automating routine tasks and improving decision-making processes.
- The use of AI can lead to more efficient resource allocation and proactive threat detection.

Cloud Computing and Remote Work
- Cloud computing is revolutionizing how organizations operate, enhancing remote work efficiency and enabling multi-cloud strategies.
- It allows for flexible resource management and collaboration, making it easier for teams to work together regardless of location.
- The shift to cloud-based solutions is driving innovation and transforming traditional IT infrastructures.

Internet of Things (IoT)
- The Internet of Things (IoT) connects a vast array of devices, facilitating automation and data exchange across various applications.
- IoT technologies are enhancing efficiency in industries such as manufacturing, healthcare, and smart homes.
- As IoT continues to grow, it presents new challenges and opportunities for network security and management.

DevOps and Digital Transformation
- DevOps practices promote collaboration between IT and software development teams, streamlining processes and enhancing productivity.
- Digital transformation involves automating manual processes and integrating technology into all aspects of business operations.
- These trends are reshaping organizational structures and workflows, driving innovation and efficiency in the digital age.

Data Security Challenges
- Ensuring data security is a paramount concern for organizations, as cyber threats continue to evolve and become more sophisticated.
- Effective data security strategies involve managing access, monitoring network activity, and implementing robust security measures.
- Organizations must prioritize data integrity and protection to maintain trust and safeguard sensitive information.

Careers in IT

Network Administrator Role
- Network administrators are responsible for managing LANs and WANs, ensuring security and optimal performance.
- They play a critical role in maintaining network infrastructure, troubleshooting issues, and implementing security measures.
- This position requires a combination of technical skills and practical experience in network management.

Required Skills and Qualifications
- A degree in Computer Science (CS) or Information Technology (IT) is typically required for network administrator roles.
- Practical experience through internships or previous positions is highly valued, as it enhances problem-solving abilities and technical knowledge.
- Continuous learning and staying updated with emerging technologies are essential for success in this field.

Salary Expectations
- The salary for network administrators ranges from $47,000 to $64,000 annually, depending on experience, location, and organizational size.
- Factors such as certifications and specialized skills can also influence earning potential in this career path.
- The demand for skilled network administrators continues to grow, reflecting the increasing reliance on technology in various sectors.

Network Security

Importance of Network Security
- Network security is critical for protecting data and resources from unauthorized access and cyber threats.
- It encompasses various measures and technologies designed to safeguard networks and ensure data integrity.
- A robust security framework is essential for maintaining trust and reliability in digital communications.

Security Measures
- Key security measures include firewalls, proxy servers, Virtual Private Networks (VPNs), and Intrusion Detection Systems (IDS).
- Firewalls act as barriers between trusted and untrusted networks, controlling incoming and outgoing traffic.
- Proxy servers provide an additional layer of security by acting as intermediaries for requests from clients seeking resources from other servers.

VPNs and Remote Connections
- VPNs enable secure remote connections, allowing users to access private networks over public channels.
- They encrypt data transmitted over the Internet, ensuring confidentiality and protection from eavesdropping.
- VPNs are essential for remote work, providing employees with secure access to organizational resources.

Intrusion Detection Systems
- IDS monitor network traffic for suspicious activity and potential threats, providing alerts for any detected anomalies.
- They play a crucial role in identifying and mitigating security breaches before they can cause significant damage.
- Effective IDS implementation enhances overall network security and helps organizations respond quickly to threats.

Communication Systems

Definition and Importance of Communication
- Communication refers to the process of sharing data between devices, which is essential for effective interaction and collaboration in technology.
- It involves various methods and technologies that facilitate the transfer of information across different platforms and devices.
- The efficiency of communication systems directly impacts productivity and connectivity in both personal and professional environments.

Connectivity in Networking
- Connectivity is the linking of computers, networks, and the Internet, enabling seamless data exchange and resource sharing.
- It encompasses various technologies and protocols that ensure devices can communicate effectively with one another.
- The evolution of connectivity has led to the development of more sophisticated and faster communication methods.

Wireless Revolution
- The wireless revolution has transformed how we access information, providing high mobility and anytime access to data.
- Wireless technologies have enabled users to connect to networks without physical cables, enhancing convenience and flexibility.
- This shift has facilitated the growth of mobile devices and applications, making information accessible on-the-go.

Elements of Communication Systems
- Key elements of communication systems include devices, connection interfaces, data specifications, and channels.
- Devices are the hardware components that facilitate communication, while connection interfaces determine how these devices interact.
- Data specifications ensure that the information being shared is formatted and transmitted correctly, while channels are the mediums through which data travels.

Types of Channels
- Channels can be categorized into physical and wireless types, each with distinct characteristics and applications.
- Physical channels include twisted pair cables, coaxial cables, and fiber-optic cables, which are used for wired connections.
- Wireless channels utilize radio waves, Bluetooth, Wi-Fi, and satellites to transmit data without physical connections.

Network Terminologies

Understanding Networks
- Networks are systems that connect computers to share data and resources, forming the backbone of modern communication.
- They enable collaboration, resource sharing, and efficient data management across various devices and locations.
- The structure and design of a network can significantly influence its performance and security.

Types of Networks
- Different types of networks exist, including Local Area Networks (LAN), Wide Area Networks (WAN), Personal Area Networks (PAN), and Metropolitan Area Networks (MAN).
- Each type serves specific purposes and scales, catering to different organizational needs and geographical coverage.
- Understanding these types is crucial for selecting the appropriate network solution for a given context.

Network Devices
- Key devices in a network include nodes, clients, servers, routers, and switches, each playing a vital role in data transmission and management.
- Nodes are endpoints in a network, while clients are devices that request services from servers.
- Routers direct data traffic between networks, and switches connect devices within a network, optimizing communication.

Network Protocols
- Protocols such as TCP/IP, HTTPS, DNS, and packetization govern how data is transmitted and received over networks.
- TCP/IP is the foundational protocol for the Internet, ensuring reliable communication between devices.
- HTTPS provides secure data transmission, while DNS translates domain names into IP addresses, facilitating easier navigation.

Network Topologies
- Network topologies describe the arrangement of different elements in a network, influencing its performance and reliability.
- Common topologies include bus (common cable), star (central switch), ring (circular link), tree (hierarchical), and mesh (multiple paths, wireless).
- Each topology has its advantages and disadvantages, affecting factors such as scalability, fault tolerance, and ease of installation.

Network Strategies
- Client/Server and Peer-to-Peer (P2P) are two primary network strategies, each with distinct characteristics.
- The Client/Server model centralizes service control, allowing for easier management and security.
- In contrast, P2P networks distribute authority among nodes, promoting direct communication and resource sharing.

Organizational Networks
- Intranets and extranets are types of organizational networks that facilitate internal and external communication.
- An intranet is a private network used within an organization, providing secure access to resources and information.
- An extranet extends limited access to external users, enabling collaboration with partners and clients while maintaining security.