**Chapter 6**

**6.1 Communication Links and Networks:**

**Explanation of Different Types of Communication Links:**

- **Physical (Wired) Links:** This category encompasses conventional mediums like copper wires and advanced technologies like fiber optic cables. Copper wires, in use since the 1800s, were initially adapted from the telephone network for data transmission. Fiber optic cables, using light signals through glass cables, enable high-speed digital communication, forming the backbone of internet infrastructure.

- **Last Mile Technologies:** The "last mile" denotes the final part of telecommunication networks delivering services to end-users. Technologies such as fiber optic cables (for high demand areas) and Digital Subscriber Line (DSL) over copper wires provide fast internet access. Asymmetric DSL (ADSL) offers faster downloads than uploads, aligning with typical user behavior.

- **Cable Television Services:** Cable TV networks, designed for one-way communication from central offices to subscribers, provide fast downloads but slower uploads. This setup suits home users consuming data for streaming and downloads but may not be ideal for businesses requiring symmetrical upload and download speeds.

- **Wireless Communication Links:** Wireless technologies include geosynchronous, geostationary, medium earth orbit (MEO), and low earth orbit (LEO) satellites. Mobile phone networks are also essential for wireless data transmission. Project Loon uses helium balloons for internet access in remote areas, while Starlink aims to deploy a network of satellites globally.

**Importance of Understanding Data Usage Patterns:**

Understanding a company's data usage patterns is pivotal for choosing appropriate internet connection technologies. Businesses assess factors like data volume, upload/download speeds, costs, and security. For example, businesses mainly receiving data might benefit from cable television services. In contrast, entities sending out data, like web pages or software downloads, may require technologies with symmetrical upload/download speeds, such as fiber optics. Selection involves evaluating cost, installation ease, speed, contract terms, and security, ensuring alignment with business requirements.

**6.2 Communication Links and Devices:**

**Overview of Communication Links:**

- **Modems:** Modems are devices converting digital signals into tones for transmission over analog mediums like phone lines. While traditional modems are rare, they played a significant role in early internet connections.

- **Wireless Communication:** Wireless options include geosynchronous, geostationary, MEO, and LEO satellites. Mobile networks provide data connectivity, with options like LTE and 5G supporting high-speed wireless internet access.

- **Emerging Technologies:** Project Loon utilizes balloons for internet access in remote areas, while Starlink plans a global satellite network. These technologies expand internet access to underserved regions.

- **Duplex Modes:** Communication links can be simplex (one-way), full-duplex (two-way simultaneous), or half-duplex (alternating one-way communication). Understanding these modes is crucial for efficient data transmission.

**Importance of Communication Understanding:**

Comprehending various communication links and devices is vital for businesses and individuals. It enables informed choices regarding internet connectivity, ensuring seamless data transmission for different purposes. Businesses must assess their specific needs, considering factors like speed, reliability, and coverage, to select the most suitable communication technologies.

**6.3 Local Area Networks (LANs):**

*Wired LANs:*

* **Ethernet Technology:** Ethernet, a dominant wired LAN technology, operates over cables and connectors. Devices on an Ethernet network follow a protocol to avoid collisions during data transmission. Ethernet speeds have evolved over the years, with 100 Gbit Ethernet being the state of the art in 2019. Ethernet devices are backward compatible, allowing devices built for older standards to participate in newer networks.
* **Wi-Fi Networks:** Wi-Fi, using routers to send and receive radio signals, is the prevalent technology for wireless LANs. Wi-Fi versions are identified by numbers and supported by the international 802.11 standard. Wi-Fi 6, set to replace Wi-Fi 5, offers significantly faster data transfer speeds. Wi-Fi networks are backward compatible, allowing devices with different Wi-Fi versions to communicate at the fastest supported speed.
* **Wi-Fi Privacy and Security:** Wi-Fi networks pose security risks, making encryption crucial to protect data transmissions. Public Wi-Fi usage requires extra precautions, such as verifying network connections and avoiding automatic network selection to prevent unauthorized access.

*Other Wireless LAN Types:*

* **Bluetooth:** Bluetooth technology facilitates wireless communication between devices in close proximity, such as phones, keyboards, and printers. Devices connect through a simple pairing process.
* **Radio Frequency ID (RFID):** RFID transfers information from tags to readers and finds applications in product tracking, inventory management, passports, animal identification, and more. RFID tags can be active, passive, or battery-assisted passive, each with specific use cases.
* **Near Field Communication (NFC):** NFC, a form of RFID, requires devices to be very close, ensuring secure communication. Applications include contactless payments, social networking, and Bluetooth pairing setup.
* **ZigBee:** ZigBee supports wireless control and monitoring in various fields, including industrial control, home automation, and medical data collection. ZigBee networks utilize mesh topology and offer strong security features.
* **Personal Area Networks (PANs):** PANs involve devices carried by an individual, like phones connecting with watches. PAN technologies include Bluetooth, various wireless protocols, and wired connections like USB. Body Area Networks (BANs) monitor vital signs and fall under the PAN category.

*Importance of Understanding Wireless Protocols:*

While specific technical details may change, understanding different wireless protocols and their applications is essential. Businesses should be prepared to ask relevant questions when selecting a network type for specific applications, ensuring the system's success and security.

**6.4 Wide Area Networks and the Internet:**

*Wide Area Networks (WANs):*

* **Definition:** WANs cover large geographic areas, often spanning countries or continents. They utilize communication links and include switching nodes to control message routing.
* **Switching Nodes:**
  + **Repeaters:** Amplify signals for longer travel but lack intelligence for message routing.
  + **Bridges:** Connect links and pass messages only if addressed to a device on the other side, reducing traffic.
  + **Switches:** Connect multiple links, acting as bridges between every pair of links.
  + **Routers:** Determine the final destination of a message and select a suitable route to reach it.
  + **Gateways:** Serve as access points between different networks, commonly used between organizational networks and the Internet.
* **Importance:** While technical details differ, understanding the role of appropriate devices in a network is crucial for effective communication.

*The Internet:*

* **Evolution:** Originating from a U.S. military project in 1969, the Internet has grown globally, connecting people, organizations, and even the International Space Station.
* **Funding and Growth:** Internet usage is mostly free for users, funded indirectly through taxes and budgets. This model has led to rapid growth and the establishment of new businesses.
* **Internet Backbone:** Operated by telecommunications firms, the Internet backbone employs various technologies, primarily fiber optics, and is expected to evolve with technological advancements and demand.
* **Significance:** Understanding the workings of the Internet is vital for businesses. Staying informed about its evolution helps anticipate changes, ensuring seamless connectivity and cost-effective solutions.

*Packet Switching:*

* **Concept:** Messages are divided into packets of about 1,500 bytes, numbered, and sent individually. Upon arrival, packets are reassembled by number, forming the complete message.
* **Analogy:** Similar to mailing a book like Moby-Dick on 10,000 postcards, each taking different routes and arriving out of order. Reassembly is possible once all postcards are received.
* **Benefits:**
  + Efficient Network Sharing: Allows computers to share networks efficiently.
  + Fault Tolerance: Bypasses broken links and balances load on different links.
  + Reliable Connections: Creates reliable connections from imperfect physical links, enhancing data transfer reliability.

*Alternative Switching Methods:*

1. **Circuit Switching:** Maintains a communication path for a conversation, even if there's no ongoing transmission.
2. **Message Switching:** Sends an entire message as a unit and makes the communication path available for other messages afterward. Messages in a conversation may take different paths.

Understanding these concepts is fundamental for businesses, enabling effective utilization of network resources and ensuring seamless communication.

**6.5 INTERNET APPLICATIONS**

**The World Wide Web:**

The World Wide Web, introduced in 1991, transformed how information is accessed and shared. Its fundamental concepts include Uniform Resource Locators (URLs), hyperlinks, and discovery through search engines. Websites are identified by domain names and structured with pages and folders. Internet Protocol (IP) addresses, represented as four 8-bit numbers, identify devices on the Internet. The domain name system (DNS) maps human-readable domain names to IP addresses.

Where you fit in: Understanding the fundamentals of the web is essential for business professionals, as websites play a crucial role in corporate presence and communication strategies.

**Web 2.0:**

Web 2.0, also known as the Social Web, shifted the focus from content created by site owners to user-generated content. Social networking platforms like Facebook, YouTube, and Twitter exemplify this shift. Companies utilize social media for marketing, customer engagement, and feedback. User reviews and interactive features enhance websites' content and functionality.

Where you fit in: Businesses leverage Web 2.0 technologies for customer interaction and marketing. Your understanding of these platforms can contribute to effective online strategies.

**Streaming:**

Streaming technology allows real-time transmission of audio and video content over the Internet. Internet telephony (VoIP) enables cost-effective voice communication, while streaming video facilitates on-demand access to movies, tutorials, and live broadcasts. Teleconferencing solutions, including video calls and telepresence robots, facilitate virtual meetings, enhancing collaboration.

Where you fit in: Understanding streaming technologies is vital, as they are widely used for communication, entertainment, and business collaboration. Proficiency in these technologies can improve communication efficiency in the workplace.

**The Internet of Things (IoT):**

The IoT refers to interconnected devices equipped with sensors, actuators, and microprocessors, enabling them to communicate and perform tasks autonomously. IoT devices, such as smart home appliances and industrial machinery, collect and exchange data to enhance efficiency and automation. Sensors play a critical role in IoT systems, enabling data collection for analysis and decision-making.

Where you fit in: IoT technology is revolutionizing various industries. Familiarity with IoT concepts and applications is valuable, especially in sectors where automation and data-driven decisions are essential.

**Other Internet Applications:**

Apart from the web and IoT, the Internet hosts several other applications such as email, file transfer protocols (FTP), SSH (Secure Shell), UDP (User Datagram Protocol), and SNMP (Simple Network Management Protocol). These protocols facilitate different functionalities, including secure remote access, domain name resolution, and network device management.

Where you fit in: While these protocols operate behind the scenes, having a general awareness of their existence and functionalities can enhance your overall understanding of Internet technologies.

Understanding these diverse Internet applications is crucial for business professionals, as these technologies shape modern communication, collaboration, and information exchange in the digital age.

**6.6 NETWORK SECURITY**

**Access Control and Identity Authentication:**

Network security involves protecting information systems from unauthorized access. Access control concepts, discussed in Section 5.5, apply to networks. Your network identity determines your actions and the applications/resources you can access. Identity authentication methods include something you know, have, are, or do. Single sign-on (SSO) simplifies user access, emphasizing the importance of secure sign-on methods.

Where you fit in: Managers should ensure network security measures are well-funded and supported to protect sensitive information.

**Firewalls and Defense Against Attacks:**

Firewalls are essential in defending against unauthorized network penetration. They detect intrusion attempts and prevent unauthorized activities inside and outside the network. Attacks, similar to those on databases, involve impersonating authorized users, social engineering, and password theft. Denial of Service (DoS) attacks flood a network with requests, overwhelming it. Distributed DoS (DDoS) attacks, involving a network of infected systems (botnet), make defense challenging.

Where you fit in: As a manager, you should invest in user training to recognize phishing attacks, employ anti-malware software, and implement regular data backups.

**Phishing and Identity Theft:**

Phishing attacks deceive users into providing confidential information via fake websites. Attackers exploit human vulnerability, often using urgent language or mimicking legitimate organizations. Users should verify requests, avoid clicking suspicious links, and confirm the source's authenticity through alternative means. Identity theft, a consequence of attacks, occurs when personal information is stolen, leading to financial and emotional repercussions.

Where you fit in: Managers play a role in educating employees about phishing risks, emphasizing vigilance, and encouraging secure online practices.

**Privacy and IoT Security:**

Privacy concerns involve IP addresses, MAC addresses, and cookies. Users can control cookies, but IoT devices, connected to the Internet, pose security challenges. Managers should identify IoT devices, set security standards, integrate IoT into security policies, and engage top management. Cyber insurance can mitigate risks, and managers must ensure technical staff address IoT security effectively.

Where you fit in: Managers must oversee IoT security initiatives, ensuring technical staff actively implement measures to protect against emerging threats. Stay proactive to safeguard networks and sensitive information.