UNIT II

PHYSICAL LAYER AND DATA LINK LAYER

Applications: Ethernet in LAN/WAN setups, encoding in RFID readers

Ethernet in LAN/WAN Setups

Ethernet is a standard networking technology that provides wired connections in Local Area Networks (LANs) and Wide Area Networks (WANs).

- **Connectivity and Resource Sharing:** It allows devices (computers, printers, servers, RFID readers) within an office, campus, or factory to connect and share resources and information efficiently.
- **Internet Access:** Ethernet connects end-user devices to the internet via routers or switches, forming the physical layer of many TCP/IP networks.
- **Power over Ethernet (PoE):** A significant application is the use of a single Ethernet cable to provide both a data connection and electrical power to devices like security cameras, VoIP phones, and networked RFID readers, simplifying installation and reducing cabling costs.
- **Industrial Automation:** Ethernet is widely adopted in industrial settings for reliable, high-speed communication between various automation devices, including Programmable Logic Controllers (PLCs) and sensors.

Encoding in RFID Readers

Encoding refers to the process of writing specific, organized data onto an RFID tag's memory banks so that readers can identify and interact with it correctly.

- **Unique Identification:** The primary application is assigning a unique identifier (ID) to each physical item (assets, inventory, tools, people). This ID is then linked to detailed information in a database or software system.
- **Supply Chain Management:** In logistics and inventory tracking, specific encoding schemes and standards like the GS1 Tag Data Standard (TDS) or RAIN ISO numbering (EPC Class 1 Gen2V2) are used to ensure global compatibility and organization of product information, such as lot numbers, serial numbers, and manufacturing dates.

- **Access Control:** For door access systems, RFID cards or tags are encoded with unique identifiers that the reader verifies to grant or deny entry, often working in conjunction with a central control system.
- **Data Logging and Real-time Monitoring:** Data can be written to a tag as an item moves through different processes (e.g., in a manufacturing line), with readers at various points collecting this information in real time to monitor workflow and status.

Wi-Fi MAC in homes and airports, CRC in packet verification

A **Wi-Fi MAC address** is a unique hardware identifier used for local network communication and device management, while a **Cyclic Redundancy Check (CRC)** is an error-detection code used to verify the integrity of data packets during transmission.

Wi-Fi MAC Addresses in Homes and Airports

A Media Access Control (MAC) address is a unique, 48-bit physical address "burned into" a device's network interface card (NIC) by the manufacturer. It operates at the data link layer (Layer 2) of the OSI model and is used for communication within a local area network (LAN).

- **Local Identification:** MAC addresses ensure that data frames are delivered to the correct physical device on the same local network segment (e.g., within a home or a single area of an airport terminal). Network switches and access points use MAC address tables to learn which devices are connected to which ports and forward traffic efficiently.
- **Access Control (Filtering):** Network administrators, in both home and airport settings, can use MAC address filtering as a basic security measure to restrict network access to only approved devices. However, this is not a strong security measure on its own as MAC addresses can be easily "spoofed" (changed in software).
- **Network Management:** In home networks, the router might use a device's MAC address to assign a consistent IP address via the Dynamic Host Configuration Protocol (DHCP). In enterprise environments like airports, network teams use MAC addresses for inventory, monitoring, and troubleshooting to pinpoint the physical location of a device causing problems.
- **Privacy and Tracking:** Static MAC addresses can be used to track a device's movement across different physical locations, which has significant privacy implications in public spaces like airports. To counter this, modern operating systems use **MAC address randomization**, where

a device uses a random, locally administered MAC address when scanning for or connecting to public Wi-Fi networks.

CRC in Packet Verification

A Cyclic Redundancy Check (CRC) is an efficient mathematical method used to detect accidental errors or changes in digital data that may occur during transmission or storage due to noise or interference.

Mechanism: CRC works by treating a block of data as a binary polynomial.

- The sender calculates a short, fixed-length checksum (or Frame Check Sequence) based on a division of the data by a predetermined "generator polynomial" using modulo-2 arithmetic.
- This CRC checksum is appended to the data and transmitted as part of the data packet or frame.
- The receiver performs the same calculation on the received data. The expected result (remainder) should be zero.

Error Detection:

- If the calculated remainder at the receiver is **zero**, the data is assumed to be error-free and is accepted.
- If the remainder is **non-zero**, it means an error was detected during transmission, and the receiver can request that the sender retransmit the data.

- **Application:** CRC is a crucial component in many network protocols, including Wi-Fi and Ethernet frames, where a CRC-32 checksum is typically used to ensure high data integrity. It is effective at detecting common errors like single-bit and burst errors. CRC is only for error *detection*, not *correction*, and does not protect against intentional data tampering.

Fiber media in ISP backbones

Fiber optic media is the universal and primary choice for **Internet Service Provider (ISP) backbones** due to its unmatched high speed, massive bandwidth capacity, and signal integrity over long distances. It has largely replaced traditional copper cabling in this critical infrastructure role.

Role and Importance in ISP Backbones

The internet backbone is a core network of the largest and fastest interconnections that link major routers, data centers, and internet exchange points (IXPs) across cities, countries, and continents. Fiber media is the foundational pillar of this network, enabling global data exchange by:

- **Handling Enormous Data Volumes:** Fiber cables can carry vast amounts of data simultaneously (up to terabits per second) as pulses of light, which is essential for modern data demands like cloud computing and video streaming.
- **Ensuring Long-Distance Transmission:** Data transmitted through fiber experiences minimal signal loss (attenuation) compared to other media, allowing it to cover thousands of kilometers with fewer repeaters and ensuring data integrity across the globe.
- **Providing High Speed and Low Latency:** Data travels through fiber at speeds close to the speed of light, which minimizes latency (signal delay). This is crucial for real-time applications and smooth global internet traffic flow.
- **Offering Reliability and Immunity to Interference:** Because fiber uses light signals instead of electrical ones, it is immune to electromagnetic interference (EMI) and crosstalk. This results in highly stable and reliable connections, which is a critical requirement for a global network backbone.

Key Technologies and Components

ISPs and telecom companies use several technologies and components to leverage fiber media in their backbones:

- **Single-Mode Fiber (SMF):** This is the predominant type used in long-haul backbone networks. It has a small core and transmits a single beam of light from a laser, enabling very high data rates over long distances.
- **Wavelength-Division Multiplexing (WDM):** This technology allows multiple channels of information to be sent through a single fiber strand using different wavelengths (colors) of light, dramatically increasing the network's total capacity.

- **High-Performance Routers and Switches:** Powerful networking equipment is used at connection points to manage and direct the immense volume of data traffic efficiently across the network.
- **Internet Exchange Points (IXPs) and Points of Presence (PoPs):** These are the physical locations where different backbone networks and ISPs interconnect and exchange data, often in neutral, high-performance facilities.
- **Submarine Communications Cables:** Extensive networks of armored fiber optic cables laid on the ocean floor are used to connect different continents, forming the physical global internet infrastructure.