Week6: Network Access Layer

NOS_Lecture_slides_WK06.pdf

Overview of Network Access Layer

The Network Access Layer (Layer 2) handles direct communication between network devices and is responsible for reliable data delivery between adjacent nodes.

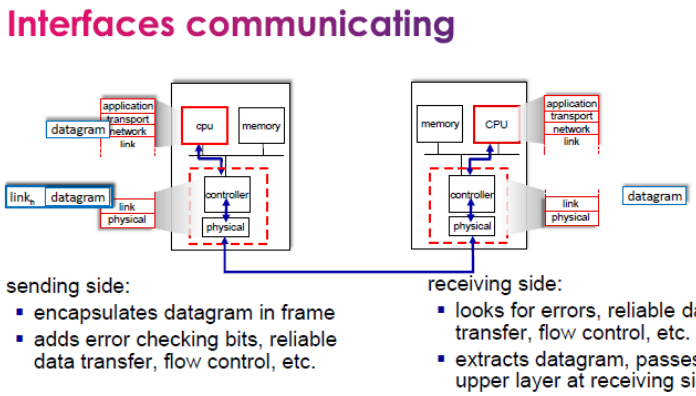
Link Layer Fundamentals

- Key Components:
  - Nodes: Both hosts and routers function as network nodes
  - Communication Channels: Connect adjacent nodes via wired or wireless connections
  - Frames: Layer-2 packets that encapsulate datagrams

Link Layer Services in Detail

- **Framing and Link Access:**
  - Encapsulates datagrams into frames
  - Manages channel access
  - Handles MAC addressing
- **Data Delivery Services:**
  - Ensures reliable delivery between adjacent nodes
  - Implements flow control mechanisms
  - Provides error detection and correction

- Supports half-duplex and full-duplex transmission



Implementation Details

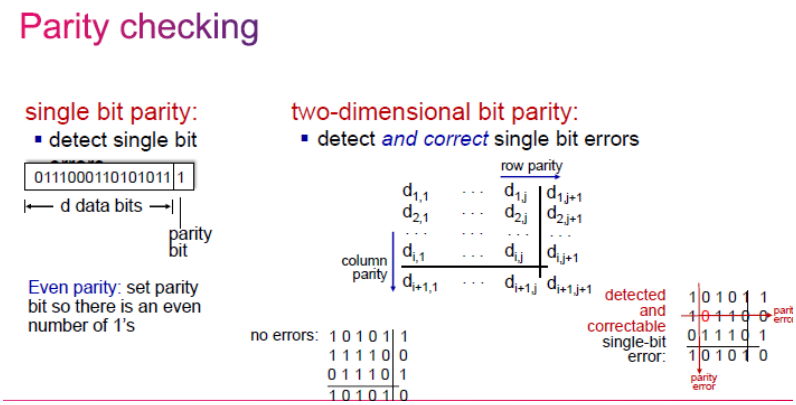
Link layer is implemented in:

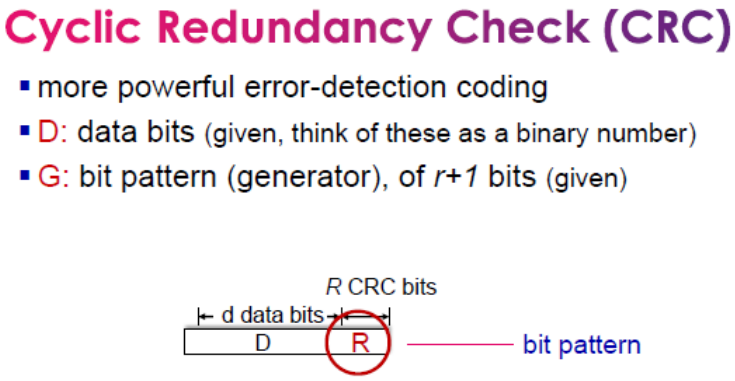
- Network Interface Cards (NIC)
- Host system software
- Hardware components
- Firmware

Error Detection and Correction

- **Key Methods:**
  - EDC (Error Detection and Correction bits)
  - Internet Checksum for segment verification
  - Cyclic Redundancy Check (CRC) for enhanced error detection
  - D: data protected by error checking

  Error detection not 100% reliable. Protocol may rarely miss some error.





Internet checksum is to detect errors (i.e., flipped bits) in transmitted segment

- sender
  - treat contents of UDP segment → including header field and ip addresses as 16bit int sequence
  - checksum addition of segement content
  - checksum value put into UDP checksum field
- reciever
  - compute checksum of received segment
  - check if computed checksum equals checksum field value: equal means no error & not equal means error detected

Multiple Access Protocols

- **Channel Types:**

    - Point-to-point connections
    - Broadcast shared medium
- **MAC Protocol Categories:**
    - Channel Partitioning (TDMA, FDMA)
    - Random Access (ALOHA, CSMA variants)
    - Taking Turns protocols

Channel Partitioning Protocols

- **TDMA (Time Division Multiple Access):**
    - Round-based channel access
    - Fixed-length time slots
    - Potential for idle slots
- **FDMA (Frequency Division Multiple Access):**
    - Divided frequency bands
    - Fixed frequency assignments
    - Possibility of idle frequency bands

Random Access Protocols

- **Characteristics:**
    - Potential for packet collisions
    - Includes ALOHA and CSMA variants
    - Implements collision detection and avoidance mechanisms

  These protocols form the foundation of modern network access methods, each suited for different network environments and requirements.

  Note: Further topics to be covered include LAN addressing, ARP, Ethernet, switches, and VLANs.

  Error Detection, correction

Multiple Access Protocols

Lans → adressing, ARP → ethernet → switches → VLANS

ALOHA Protocol

ALOHA was one of the first random access protocols, developed at the University of Hawaii.

- **Pure ALOHA:**
  - Nodes transmit frames immediately when ready
  - If collision occurs, nodes wait random time before retransmitting
  - Efficiency is around 18%
- **Slotted ALOHA:**
  - Time divided into discrete slots
  - Nodes can only begin transmission at start of slots
  - Improved efficiency up to 37%

CSMA (Carrier Sense Multiple Access)

CSMA improves upon ALOHA by listening to the channel before transmitting.

- **1. CSMA/CD (Collision Detection):**
  - Used in traditional Ethernet
  - Listens while transmitting to detect collisions
  - Aborts transmission if collision detected
  - Uses binary exponential backoff for retransmission
- **2. CSMA/CA (Collision Avoidance):**
  - Used in wireless networks (WiFi)
  - Implements RTS/CTS (Request to Send/Clear to Send) mechanism
  - Uses random backoff before transmission
  - Better suited for wireless where collision detection is difficult

- **3. Persistent CSMA variants:**
  - 1-persistent: Transmit immediately when channel becomes idle
  - Non-persistent: Wait random time if channel is busy
  - p-persistent: Transmit with probability p when channel becomes idle

Access protocols

two types of links → point to point & broadcast shared wire or medium

Single shared broadcast channel

two or more simultaneous transmisions by nodes interference.

LANs

MAC (Media Access Control) addresses are 48-bit hardware addresses that uniquely identify each network interface card (NIC). They are:

- Permanent: Assigned by manufacturer during production
- Globally unique: No two devices share the same MAC address
- Hexadecimal format: Written as six pairs of hexadecimal digits (e.g., 00:1A:2B:3C:4D:5E)

ARP (Address Resolution Protocol) is crucial for mapping IP addresses to MAC addresses:

- **ARP Table Structure:**
  - Contains IP-to-MAC address mappings
  - Includes TTL (Time-To-Live) values for entries
  - Dynamically updated through ARP requests/replies

ARP Process:

- **1. ARP Request:**
  - Node broadcasts: "Who has IP address x.x.x.x?"
  - Request contains sender's MAC and IP addresses

- **2. ARP Reply:**
  - Target node responds with its MAC address
  - Reply is unicast directly to requester
- **3. ARP Cache Management:**
  - Entries timeout to maintain accuracy
  - Can be updated by gratuitous ARP
  - Supports both static and dynamic entries

LAN (Local Area Network) Addressing:

- **Hierarchical Structure:**
  - IP addresses for logical addressing (Layer 3)
  - MAC addresses for physical addressing (Layer 2)
  - Both required for complete packet delivery
- **Key Features:**
  - Supports broadcast and multicast communication
  - Enables plug-and-play device connectivity
  - Facilitates local network segmentation

Ethernet

Ethernet is the dominant wired LAN technology, providing high-speed data transmission and reliable network connectivity.

Traditional Ethernet

- **Bus Topology:**
  - All nodes connected to a single cable (bus)
  - Signal travels entire length of cable
  - Terminated at both ends to prevent signal reflection
  - Vulnerable to single point of failure

Modern Ethernet

- **Star Topology:**
  - Nodes connect to central switch
  - More reliable than bus topology
  - Easier to troubleshoot and maintain
  - Supports full-duplex communication

Ethernet Switches

- **Key Features:**
  - Layer 2 device that forwards frames based on MAC addresses
  - Maintains MAC address table (switching table)
  - Supports multiple simultaneous transmissions
  - Provides dedicated bandwidth to each port
- **Switch Operation:**
  - Learning: Records source MAC addresses
  - Forwarding: Sends frames to specific ports
  - Flooding: Broadcasts unknown destination frames
  - Filtering: Prevents unnecessary frame forwarding

Subnetting

Subnetting divides a large network into smaller, more manageable segments.

- **Benefits of Subnetting:**
  - Improved network performance through traffic isolation
  - Enhanced security with better access control
  - More efficient use of IP address space
  - Simplified network management and troubleshooting
- **Subnet Components:**

- Network portion of IP address
- Subnet mask determines network boundaries
- Host portion for device addressing
- Default gateway for inter-subnet communication

Modern Ethernet networks typically combine switching technology with proper subnetting to create efficient, scalable, and manageable network infrastructures.