Lecture 8: LAN Protocols

CS 5516
Computer Architecture
Networks

VA Tech

Prof. Roy M. Wnek
Point-to-Point Protocol (PPP)

- Two communications protocols for sending Internet Protocol (IP) datagrams over serial point-to-point lines
  - Both were defined by the Internet Engineering Task Force (IETF)
  - Both provide router-to-router, host-to-router, and host-to-host connections
  - Both can be used over synchronous and asynchronous lines
  - Both set up and monitor router sessions and frame the data

- Most ISPs provide SLIP or PPP services
  - Users connect their computers to the host via modems over dialup or leased (dedicated) lines
  - These protocols carry IP frames as their data

- Serial Line Interface Protocol (SLIP) is the earlier protocol
  - Can only carry IP frames as data
Point-to-Point Protocol (PPP) is used more often because it supports a variety of protocols:
- Can encapsulate different Network-layer protocols such as IP, IPX, AppleTalk, DECnet, OSI/CLNP, and MAC-layer bridging.
- Allows a computer’s serial port to transmit datagrams (data packets) in the same way as a network adapter by encapsulating the datagrams into the serial transmissions.

PPP assigns an IP address automatically:
- Remote computers can connect into the network at any point.
- SLIP does not provide the automatic IP addressing scheme.

PPP can also connect remote local area networks (LANs) to form an internetwork:
- No speed limitations within the protocol; speeds are determined by the connecting equipment and communication lines.
- But, PPP is relatively slow, used only for internetwork connections with light traffic.
PPP Frame

- **Delimiters**: Mark the beginning and ending of the frame
- **Address**: Holds the destination address
- **Control**: Holds the sequence number to ensure proper handling
- **Protocol**: Identifies whether the frame contains IP, IPX, AppleTalk, or other
- **Information**: Contains the data, which can vary in length
- **Frame Check Sequence**: Calculates a checksum used for error checking

Higher Layers

<table>
<thead>
<tr>
<th>Network Layer</th>
<th>Network Control Protocol (NCP)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Link Layer</td>
<td>Link Control Protocol (LCP)</td>
</tr>
<tr>
<td>Physical Layer</td>
<td>HDLC</td>
</tr>
<tr>
<td></td>
<td>EIA-232E, EIA-422, EIA-423, CCITT(ITU) V.24, CCITT(ITU) V.35</td>
</tr>
</tbody>
</table>
### PPP Protocol Stack

**Physical Layer**
- Defines serial transmission over asynchronous and synchronous lines
- E.g. EIA-232, EIA-422, CCITT V.21 and V35.

**Data Link Layer**
- Based on the High-level Data-Link Control (HDLC) frame structure
- The Link Control Protocol (LCP) establishes and manages the link
- Specifies encapsulation methods and packet sizes, and checks to ensure links are functioning properly
- LCP packets are used to setup, maintain, and terminate connections

**Network Layer**
- There are a set of Network Control Protocols (NCP), each with its own control procedures
- The Internet Protocol Control was the original NCP, others include Open Systems Interconnection (OSI), DECnet, Internetwork Packet Exchange (IPX), and Banyan VINES

**Many products include PPP support**
- Routers such as Cisco and Synoptics
- Some products offer additional features
  - automatic recovery from a failed link
  - load-balancing traffic by using multiple links
  - Internetwork filtering
Data Link Sublayers

OSI Reference Model SubLayers

IEEE 802.x

802.3 CSMA-CD
802.5 Token Ring
802.11 Wireless LAN

Service Access Points (SAPs)

10Base2 Ethernet
LLC AND MAC SUBLAYER PROTOCOLS

- Data link control layer of the OSI model
  - Upper sublayer = Logical Link Control (LLC)
  - Lower sublayer = Media Access Control (MAC)

- MAC layer
  - Manages when communications can occur across the physical medium
  - Defines frame assembling and disassembling
  - Performs error detection via CRC checksum
  - Provides addresses that specify a physical connection to the LAN (NIC address ROM)

- LLC layer
  - Interfaces with the network layer through Service Access Points (SAPs)
  - Defined by the EEE 802.2 standard

- Multiple MAC protocols can exist under the same LLC

- A Network User Interface (NUI)
  - Provides a single MAC address to the same Ethernet LAN
  - Supports terminal and workstation on separate LLC addresses
Logical Link Control (LLC) Sublayer

- **LLC protocols**
  - For peer to peer communications between end users
  - Over multipoint bus and ring topologies.
  - All stations are common to the transmission medium, with no intermediate switching

- **Major modes of service**
  - Class 1 (Unacknowledged Connectionless) requires both the sending and receiving station address to be contained in each packet; most commonly used mode
    - Provide no acknowledgments, flow control, or error control
    - Relies on higher level protocols to perform these functions
  - Class 2 (Connection oriented) Provides acknowledgments, flow control, and error recovery via info frames
  - Class 3 (Acknowledged Connectionless) acknowledges each individual frame
Media Access Control (MAC) Sublayer

- **MAC sublayer**
  - Manages and controls communications across the physical media
  - Manages the frame assembling and disassembling
  - Performs error detection and addressing functions

- **Four most common MAC layers include:**
  - 802.3 CSMA/CD Ethernet
  - 802.4 Token Bus
  - 802.5 Token Ring
  - 802.6 Metropolitan Area Networks (MANs)

- **MAC layer bridge protocol**
  - 802.1d bridge (Spanning Tree)
  - Designed to interface any 802 LAN with any other 802 LAN

- **A LAN node has a single MAC address**
  - But can simultaneously handles several data exchanges (logical connections) originating from different upper layer protocols
  - Each connection identified by a SAP
Protocol Data Units (PDUs)

- The LLC sublayer adds a header to user data forming a PDU
  - The information field can be variable in size
  - Header contains both destination and source Service Access Points (SAPs) addresses and a Control field
    - Port for a network hardware device or application for network software
    - E.g. specifies a memory buffer into which NIC places the frame data

- The MAC sublayer adds a header and a checksum trailer to the LLC PDU
  - For transmission across the MAC layer and physical medium
    - Unique MAC addresses identify physical station points on the network
    - Each station reads this MAC address to determine if the call should be passed to one of the LLC entities
    - Each NUI has its own SAP and address
IEEE LAN Standards Committees

- 802.1 Internetworking
- 802.2 Logical Link Control
- 802.3 CSMA/CD local area networks
- 802.4 Token Bus local area networks
- 802.5 Token Ring local area networks
- 802.6 Metropolitan Area Networks
- 802.7 Broadband Technical Advisory Group
- 802.8 Fiber Optic Technical Advisory Group
- 802.9 Integrated voice and data networks
- 802.10 Network security
- 802.11 Wireless networks
- 802.12 Demand Priority Access local area networks

• Specifies Higher Layers & Management Interface (HILI)
• Focus on bridging protocols e.g. 802.1d = Spanning Tree
History of Ethernet

- In 1971, the University of Hawaii, ALOHANET, a radio system, was the first Multiple Access network.

- In 1976, carrier sense was introduced.

- In the late 1970s, 2.94 Mbps Ethernet was implemented at the Xerox Palo Alto Research Center.
  - over 100 personal workstations on a 1-km cable.

- In 1980, a consortium of DEC, Intel, and Xerox (DIX) build a 10 Mbps Ethernet.
  - Published the first Ethernet specifications.
  - The basis for the IEEE standard 802.3.
  - This standard used a MAC protocol called CSMA/CD within a standard Ethernet frame, across a common physical medium bus with channel attached MAC addressed stations.
History of Ethernet 2

- First Ethernet products appeared in 1981
- Fast Ethernet (100 Mbps) IEEE 802.3u approved: 1995
- Gigabit Ethernet (1Gbps) IEEE 802.3z approved: 1998

<table>
<thead>
<tr>
<th>Ethernet Type</th>
<th>Media Type</th>
<th>Distance</th>
</tr>
</thead>
<tbody>
<tr>
<td>10Base5</td>
<td>Thick Cable Ethernet</td>
<td>500 meter bus</td>
</tr>
<tr>
<td>10Base2</td>
<td>Thin Cable Ethernet</td>
<td>185 meter bus</td>
</tr>
<tr>
<td>1Base5</td>
<td>Twisted pair StarLAN</td>
<td>500 meter diam. star</td>
</tr>
<tr>
<td>10BaseT</td>
<td>Twisted pair Ethernet</td>
<td>100 meter diam. star</td>
</tr>
<tr>
<td>100BaseT</td>
<td>Twisted pair FastEthernet</td>
<td>100 meter diam. star</td>
</tr>
<tr>
<td>100BaseF</td>
<td>Fiber Optic FastEthernet</td>
<td>2 km diam. star</td>
</tr>
</tbody>
</table>
802.3 CSMA/CD (Ethernet)

- Specific Ethernet data link functions:
  - Encapsulation and de-encapsulation of user data
  - Media access management (such as physical layer and buffer management)
  - Collision detection and handling
  - Data encoding and decoding
  - Channel access to the LAN medium

- 10BaseT CSMA/CD allows rates theoretically at 10 Mbps
  - Increasingly inefficient under heavier traffic loads
  - Actual throughput may only be 3.5 Mbps

- Best effort delivery
  - No complete guarantee of successful sending a message
Protocol Data Units (PDUs)

- IEEE 802.3 CSMA/CD MAC PDU
  - Maximum size of the frame is 1500 bytes

- Preamble field
  - Provides synchronization.
  - It is the "carrier" that is detected by other nodes, which stops them from transmitting

- Start of Frame Delimiter (SFD)

- Destination and source address
  - Provide the MAC layer destination and source address
  - Addresses are created by combining 24 bit number from the NIC manufacturer with a 24 bit unique address to form a 48 bit MAC address

- The length of the data field in bytes

- The data field is the LLC PDU

- The pad adds filler bytes to achieve a minimum frame length

- Frame check is a standard CRC
• States of the Ethernet
  – Idle
  – Transmission
  – Collision

• Key features of the CSMA/CD
  – Listening to the channel
  – Transmitting only if an “idle” channel is detected
  – Listen while transmitting during the collision window
  – Waiting a random amount of time if it is busy
CSMA/CD

- All versions of Ethernet gain access to the shared media using the "first-come-first-served" CSMA/CD method.

- When a station wishes to transmit a packet, it must first listen to see if anyone else is transmitting:
  - Based on detection of exiting traffic (carrier sense).

- If there is some activity, the station will have to wait until it is complete then defer an extra 9.6 microseconds before continuing:
  - This extra gap ensures all stations can distinguish the end of one packet from the beginning of the next.

- If no cable activity is sensed, transmission begins:
  - After starting a transmission, the station continues to listen.
  - There is a possibility that remote stations, further down the cable, will have sensed the "quiet" and started their own transmissions.
  - Collisions would then result.
• Collisions arise because of the cable propagation delay
  – This delay means that two stations at the extreme of the cable are "out of touch" for some amount of time
    • 25.6 μs in a maximum sized network (with repeater) of 2500 meters
  – Like with each other-like a distant star that have exploded thousands of years ago, but the light hasn't reached us yet.

• Collisions then occur when two separated stations start transmitting without having detected one another

• When collisions occur and are detected
  – all transmitting stations immediately cease sending
  – To ensure that all stations are aware of the conflict, the sensing stations will all transmit a short "jamming" burst (128 bits) and then wait before attempting to transmit
    • This extra transmit time ensures that all stations recognize that a collision has occurred
CSMA/CD 3

- Collisions due to cable propagation delay will only occur near the beginning of each packet.

- This "collision window" lasts for first 51.2 microseconds of a transmission:
  - If a station at one end of a maximum sized network started a transmission 25.6 µsec after a station 2500 meters away, it would sense a collision almost immediately.
  - However, the first station wouldn't detect the collision until an extra 25.6 µsec has had elapsed.
  - By this time, it would have been transmitting for 51.2 microseconds.
When a collision is sensed, all stations must stop transmitting and then wait
  - Eventually they will try again, and by this time, some additional stations might need to transmit and collisions could reoccur
  - In fact, on each succeeding attempt, there might be a greater chance of collision as more and more stations get desperate

A CSMA/CD system, therefore, needs some form of orderly retry procedures for use after collisions
  - Ethernet uses the Truncated Binary Exponential Back-off Algorithm
  - Implemented within the controller chip on the NIC

Truncated Binary Exponential Back-off Algorithm
1. When any packet collision is detected, the transmitting stations continue transmit an extra 16 bytes of Ones (the jamming signal) and will then cease to transmit
2. The stations involved will wait (back off) a random length of time before trying again
   - The random wait tries to prevent all the retries occurring at once and is determined as follows:
3. The retransmit delay after a collision was designed to be multiples of this 51.2 µsec collision window time
   - On the first retry, each station will randomly decide either to send immediately (after the 9.6 µsec gap) or wait one collision window (51.2 µsec) and then send
   - With luck, only two stations were involved, and will pick different times so no collision will occur
   - However, there is a good chance (50% if two stations are involved) that they will wait the same delay and then collide again.

4. The number of successive collisions is recorded by each station. Before transmitting a third time (second retry), a random delay of 0, 1, 2, or 3 windows will be waited
   - Now there is only a 25% chance of any two stations waiting the same delay.

5. Should a third retry be necessary, the time delay will randomly be 0-7 window times (0-358.4 µsec), then 0-15, 0-31, 0-63 . . .
   - The last six retries will stay in the 0-1023 range until the maximum of 15 retries is reached.

6. If 16 collisions (15 retries) in a row are detected, the transmitter gives up, and higher levels of software must decide what to do

   - Once a successful transmission is made, all stations set their collision counters back to zero in preparation for the next packet
Thick Cable Ethernet-10base5

- Originally the Attachment Unit Interface (AUI) was an external transceiver (transmitter and receiver) mounted directly on the central cable
- A 15-wire drop cable leads to the adapter card inside the computer
- The transceiver performs the actual tasks of transmitting, receiving, and checking for collisions
- A maximum of 100 stations can be placed on any one cable segment
Thick Cable Ethernet-10base5

- Transceivers clamps directly on cable
  - Makes electrical connection with a "vampire tap" which "bites" into the shield and center conductor

- Stations have to be spaced a minimum of 2.5 meters apart
  - This spacing was selected to minimize the accumulation of multiple cable reflections off the taps, which would cause transmission errors

- Each cable segment can be no longer than 500 meters
Thin Cable Ethernet-10Base2

• The separate components of the original DIX physical arrangement were too elaborate for widespread use
  – A variation, introduced by 3Com moved the transceiver onto the controller board
  – Replaced the Ethernet cable with a lower cost, more flexible thin cable, RG-58
  – Replaced separate taps and type-N connectors are with BNC and T connectors right at the back of the PC

• Individual stations can now be connected as close as 0.5 meters.

• A segment reduced to 185 meters with only 30 stations
  – Length restriction is due partly to slightly higher cable loss and partly to slightly lower signal velocity on the thinner cable

![Diagram of 50-ohm Termination and 0.2” Diameter 50-ohm Coaxial Cable]
StarLAN-1 Base5

- A once major variation on Ethernet developed by AT&T used a much lower data rate of 1 megabits/sec
  - Allowed use of standard telephone wiring
  - Attractive choice for those with existing wiring

- Up to ten stations could be "daisy chained" per arm and then connected into a central wiring concentrator
  - By reducing the daisy-chain to four stations per arm, the overall radius could reach 250 meters

- 1 Mbit/sec StarLAN replaced with a fully Ethernet-compatible 10 Mbits/sec StarLAN
Twisted Pair Ethernet-10BaseT

- Most common variation of Ethernet used a central concentrator with a dedicated cable of unshielded twisted pair (UTP) running to each station
  - Physical star topology
  - The data rate of 10 megabits/sec

- The standard length of any one arm of the star is a maximum to 100 meters
  - Can be exceeded in most cases, at a cost to performance

- This Ethernet variation was developed as a market reaction to IBM's Token Ring
  - Ease of wiring
  - Network maintenance
Twisted Pair Ethernet-10BaseT

- Continuous testing of network connectivity cable is inherent in this design
  - Panel lights at the concentrator indicate normal or abnormal operation
  - A connection that fails or misbehaves can be automatically terminated via software, without disturbing other stations

- Dedicated connectivity uses two pairs of unshielded, twisted wires (EIA Category 3 or above)
  - a transmit pair and a receive pair
  - The two wires of each pair are twisted independent of each other to reduce crosstalk and maintain a balanced state
  - Lower grade telephone cabling may work for short distances with performance risk
History of Token Ring

- Developed by IBM development labs in Zurich, Switzerland, in the late 1960s
- In 1985, IBM chose 4Mbps Token Ring as its LAN protocol
- First products appearing in 1986
  - Wiring concentrator (Multistation Access Unit),
  - Cabling with type 3 telephone
  - Various applications (NetBIOS Emulation, 3270 Emulation, APPC/PC)
- IEEE has adopted Token Ring as IEEE Standard 802.5
  - 802.5 MAC Token Passing Protocol working on the IEEE 802.2 Logical Link Control sublayer
- Later, IEEE 802.4 defined a Token Bus standard
  - A token passing MAC protocol for operating on a bus topology
- In 1988, the 16 Mbit/s standard was introduced.
  - Response to Ethernet's speed advantage
802.5 Token Ring

- Most often implemented as a Physical star topology with a hub and forming a Logical Ring

- Token are data packets with multiple fields
  - Token moves counter-clockwise around ring
  - Token status is marked “Free” or “Busy”

- Any station may seize a free token
  - Modify its status
  - Load data into token
  - Send token to the destination station

- If the token is busy (the token contains data destined for a different station)
  - Non-addressee station regenerates it and passes it on to the next station without modification

- Only one station on the ring can transmit data over the common medium at a given time
Token Ring

• Multistation Access Units (MAUs) used as Token Ring hubs
  – Automatically bypass non-operational spokes
  – May be passive or active (integral repeater)

• Token Ring types
  – Type 1: Shielded Twisted Pair
    • Up to 260 notes
  – Type 3: Unshielded Twisted Pair (Category 3,4,5 UTP)
    • Up to 72 nodes
### Token Ring 2

- One of Token Ring's features is its ability to monitor the "health" of each network adapter and its associated cable
  - Will cut stations out of the ring should a failure occur
  - Of great benefit in larger networks, when troubleshooting can take longer to locate a fault

- Under uniformly high traffic loading, the Token Ring protocol is much more bandwidth efficient than other LAN protocols
  - Because there are fewer idle tokens
  - Opposed to Ethernet, where heavy load causes many collisions
  - Un-even traffic loading may cause "starvation"

- Tokens may be assigned priorities for specific stations on the ring
Token Ring 3

- Logical ring of wire is within the **MAU**
  - Four-wire “lobe cables” extend the incoming and the outgoing signal to the stations
  - Relay contacts bridge the four wires of each lobe cable whenever a station is off or not connected
  - When a machine is turned on, the bypass relay opens, causing the circumference of the ring to extend through the lobe cabling (in effect inserting the station into the ring)

- The "ring" follows the twisted pair through the MAU, the lobe cables, and the stations
1. Free token

2. Token with C destination

3. Token passed through node D on to node C

4. Token received by node C and new free token passed to B
Token Ring PDU

- The maximum frame size using the 4 Mbps medium is 4,000 bytes, for the 16 Mbps medium it is 17,800 bytes.

- When an empty token is sent, only three characters are needed:
  - Start Delimiter (SD)
  - Access Control (AC)
  - End Delimiter (ED)

- When a node takes possession of the token, it converts the token to a data carrying frame, adding several fields.

- Token Bus PDU is similar.
802.4 Token Bus

- Least commonly used 802 protocol
- Forms a logical ring around a physically linear bus
- Each node knows its own address and the address of the preceding node
- Tokens are passed in logical ring by descending address
- Tokens contain the address of the next station
- Stations can use the bus only for a limited amount of time
Token Bus Routine

<table>
<thead>
<tr>
<th>Token status</th>
<th>Addressee</th>
<th>Next Node</th>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Free</td>
<td>nil</td>
<td>A</td>
</tr>
<tr>
<td>2</td>
<td>Busy</td>
<td>E</td>
<td>A</td>
</tr>
<tr>
<td>3</td>
<td>Free</td>
<td>nil</td>
<td>D</td>
</tr>
<tr>
<td>4</td>
<td>Free</td>
<td>nil</td>
<td>E</td>
</tr>
<tr>
<td>5</td>
<td>Free</td>
<td>nil</td>
<td>C</td>
</tr>
<tr>
<td>6</td>
<td>Busy</td>
<td>E</td>
<td>C</td>
</tr>
</tbody>
</table>
Fiber Data Distribution Interface (FDDI)

- LAN and MAN standard defined by ANSI and CBEMA as X3T12
  - Also recognized as an ISO standard

- Token Ring is the basis for FDDI
  - Similar protocol logic except
    - Free token seizing
    - Relapse of token after transmission

- Physical star topology with hub and forming a Logical Ring

- Requires a master station
  - Listens for the presence of a good token
  - If a good token is not heard after a specified time, it regenerates ones

- 100 Mbps maximum data rate
  - Actual throughput much lower

- Physical media-dependent
  - Single or multi-mode fiber
  - Copper Data Distribution Interface (CDDI) with STP or UTP
• FDDI Station Management layer (SMT) encompasses OSI Physical and Data Link/MAC layers

• FDDI protocol structure make it ideal as a LAN backbone
FDDI Ring

• Dual counter-rotating rings
  – Primary ring
  – Secondary ring

• Two types of nodes
  – *Class A* or *Primary Stations* are attached to both rings
  – *Class B* or *Secondary Stations* are attached to the Primary ring

• Dual-attached stations use an internal by-pass switch to automatically “self heal” the network
  – Both physical ports share a single MAC Layer and MAC addresses
FDDI Applications

- Link high-performance desktop machines in a workgroup

- High speed backbone to link routers & concentrators
  - MAN and WAN applications

- FDDI standard for max distance between end-stations and concentrators
  - 100m with Cat. 5 UTP
  - 2 km with multi-mode fiber
  - 60km with single-mode fiber

- Total size
  - 500 dual attached nodes
  - Total circumference of 200 km for dual-attached fiber rings
FDDI Self Healing

- Dual-attached FDDI nodes may bypass breaks in the network lines
- Automatically causes a “ring wrap” (loop back)
  - Traffic is diverted to the secondary ring
  - The point of failure is removed from the network
- FDDI nodes may connect to multiple hubs
Redundancy in FDDI Connections

- FDDI to dual-attached concentrators for server access

- FDDI connecting router to dual-attached concentrators for server access
FDDI Operations

• A node with traffic to send may seize a free token
  – Takes original token off the ring
  – Transmits full frame with destination address

• A new token is released onto the ring
  – Even though the destination station has not received the full frame
  *Major difference from Token Ring*
  – Allows high speed transmissions can be without waiting for the transmitting station to clear the original token

• Addressee only reads the frame & copies the message

• Non-addressees read the frame & do nothing

• Original frame eventually returns to the transmitting node
  – Transmitting node purges frame from the ring
FDDI Token Passing Routine

1. A absorbs the token

2. A transmits frame to C & appends new token (D ignores frame)

3. C reads in frame & frame continues back to A (D has chance to transmit if it has traffic to send)

4. A takes the frame off the network (C has a chance to transmit if it has traffic to send)
Merits of a FDDI LAN

- Advantages of FDDI LANs
  - Accommodate large numbers of users on a single LAN segment
  - More stations than other LAN protocols
  - 100 Mbps shared bandwidth
  - Large geographic area coverage
  - High reliability through self healing
  - Fiber immune to electro-magnetic interference
  - Direct efficient attachment for hosts
  - Built in network management (SMT)
  - Support for multimedia services on LAN
  - Economics of Dual Access Stations

- Disadvantages of FDDI LANs
  - More expensive to install with fiber
  - Lower performance with copper
FDDI PDU

• Protocol Data Units (PDUs) similar to those used in Token Ring

• FDDI fields are labeled in symbols which represent four bits

• The information field (data packet) ranges from 128 to 4500 bytes

• The address fields conform to the Token Ring standard

• The maximum frame length is 9000 bytes