Computer Networks (UE18CS301)

Unit 5

Aronya Baksy

November 2020

1 Link Layer

- Nodes that implement link-layer are connected together by links. The link layer manages the transmission of link-layer frames across these links.
- The link layer is implemented in hardware in the **Network Interface Card** (NIC), also called the network adapter.
- The NIC consists of a controller that takes care of multiple access protocols, setting error detection bits at the receiver side, and checking the validity of these bits at the sender side.
- In the 90s, NICs were separate cards that would plug into the computer's PCI bus, but now they are integrated into the host's motherboard (LAN on Motherboard configuration).

1.1 Services provided by Link Layer

- **Framing**: Encapsulation of network-layer datagrams into link-layer frames.
- **Link Access**: **Multiple Access Control** or MAC protocols are used when multiple senders share the same broadcast link while sending.
- **Reliable Delivery**: A guarantee to move all link layer frames across the link without errors. This is implemented using ACKs and responses similar to RDT in Transport Layer. For unreliable links like wireless, the goal is correcting the error locally instead of resorting to end-to-end transmission of the data again.
- **Error Detection and Correction**: Using more sophisticated techniques than those in the transport and network layers, errors can not only be corrected or detected.

2 Error Detection and Correction Techniques

2.1 Parity Checking

- In a one-dimensional parity checking scheme, the parity scheme is set to either even or odd.
- If even parity is being used, then the extra parity bit is set such that total number of 1s in the new data (original data + parity bit) is even.
- If even parity is being used, then the extra parity bit is set such that total number of 1s in the new data (original data + parity bit) is odd.
- If an even number of bit errors occur in an even parity scheme, then they would be undetected.
- If it is assumed that each bit is independent of all others in being wrong, then a single bit is enough, but in real world situations, bit errors occur in bursts. In such cases, single parity bit leads to upto 50% of errors being undetected.

2.2 Two dimensional Parity Checking

- Split the data string into i pieces of j bits each. These are arranged in a rectangular matrix form (with i rows and j columns).
- For each row and for each column, the parity bits are computed. One additional parity bit is computed for the last row and column of parity bits. The $i + j + 1$ parity bits are attached to the data.
- At the other end, the parities are once again checked. All the columns and rows must have the same parity (even or odd as specified). If there is a parity error in row i and column j, then that bit is in error and it can be corrected.

2.3 Checksumming

- The data is divided into 16 bit words, added, and the 1's complement of the sum is called the checksum.
- This simple technique is implemented in software at the transport layer.
- Checksumming leads to low packet overheads but leads to less probability of error detection than CRC (Cyclic Redundancy Checking).

2.4 Cyclic Redundancy Checking

- The generator is a string of $r + 1$ bits (where r is the number of error checking bits desired).
- The data string is multiplied with 2^r (ie. shifted to the left by r places). Then this data is divided by the generator string in modulo 2. (division in modulo 2 replaces subtraction with XOR).
- The r bit remainder of this division is added at the end of the data string (the original one, not shifted) and transmitted.
- At the sender side, this received data string is divided by the same generator. If the remainder of this division is 0 then no errors have occurred in transmission. In case of a non-zero remainder, an error is detected and the sender is requested to send the data again.

3 Multiple Access Protocols

- There are 2 main types of links: **point-to-point** links and **broadcast** links.
- In a P2P link, there is one sender and one receiver at either end of the link. Protocols such as PPP (Point to Point Protocol) and HLDC (High Level Data link Control protocol) are used for P2P links.
- In a broadcast link, all the nodes are connected to the same channel. All frames that are sent out by a sender are broadcast to all the nodes on the link, meaning that all nodes on the channel receive a copy of that frame.
- Ethernet and WLAN are examples of broadcast links.
- **Multiple Access Protocols** are used by nodes on a broadcast channel to regulate their communications.
- **Collisions** occur when multiple nodes transmit over the network at the same time. This means that all nodes on the network receive these 2 frames at the same time, and this data cannot be made sense of.
- Collisions lead to wastage of bandwidth over the channel, and large number of nodes transmitting at once lead to large wastage of channel bandwidth.
- The ideal Multiple Access Protocol has the following properties, assuming the link capacity R and M nodes on the channel.

  - When only one node is transmitting it uses the full throughput of the channel, ie. R.
  - If all M nodes are transmitting over the channel at once then average throughput of all nodes should be R/M.
  - Protocol should be decentralized, with no single point of failure.
  - Simple and inexpensive to implement.

- The types of Multiple Access Protocols are :
  - **Channel Partitioning or Channelization**: Divide the channel into M slots by Time or Frequency. Each node has exclusive access to its channel. (eg: TDMA, FDMA, CDMA (Code Division Multiple Access))
  - **Random Access Protocols**: Every node uses full link capacity R. If collision occurs then that node will retransmit after waiting for a random time interval, and repeat this retransmission until the frame gets through. (eg: ALOHA, slotted ALOHA, CSMA, CSMA/CD, CSMA/CA)
  - **Taking-Turns Protocols or Controlled Access Protocols**: Round robin protocols that give each node an equal opportunity to use channel, or proportional access based on amount of data that needs to be sent (eg: Reservation, Polling, Token Passing).

3.1 Carrier Sense Multiple Access (CSMA)

- **Carrier Sensing** (Listen before speaking) is the act of one interface listening to the channel, waiting for no transmissions on the network.
- If the channel is free for a short amount of time, then the interface can transmit the frames over the channel.
- Only Carrier Sensing is not an effective MAC protocol, as collisions can still occur due to propagation delays between one host and all the others on the channel.
- Due to these delays, the other host can think the channel to be empty and start transmitting, despite one host already transmitting. This leads to collisions.

3.2 CSMA/CD (CSMA with Collision Detection)

- The CSMA/CD protocol can be summarized from the point of a node on the network as follows:
  1. The node prepares a link-layer frame.
  2. It listens to the channel for any energy signatures that indicate that it is busy.
  3. If the channel is free, the node begins to transmit data into the channel.
  4. During this transmission, if any energy signals are detected then the ongoing transmission is aborted.
  5. After aborting, the node waits for a random time interval before going back to step 2.
- The delay between an aborted transmission and the next attempt at transmission is made random as if all nodes waited for the same delay, then collisions would occur forever.
- The delay is chosen using an algorithm called **exponential backoff**. If a node has already experienced n collisions, then it chooses a value from the set $\{0, 1, 2, ..., 2^n - 1\}$ at random.
- For Ethernet, the node waits $K \times 512$ bit times (bit time = time needed to transmit a single bit into the channel).

4 MAC Address and ARP Protocol

4.1 MAC Address

- MAC address is the hardware address of an interface on a network.
- It is a 48-bit number, written as 6 groups of 2 hex digits each, separated by a hyphen.
- Each hardware manufacturer is allocated one block of 2^{24} MAC addresses, and all MAC addresses across the world are unique.
- Normally, a destination host checks the MAC address of the link layer frame. If it matches with its own MAC address then it is decapsulated, else it is discarded.
- However in the case of a broadcast message which is to be sent to all the interfaces on that LAN, a special broadcast MAC address `FF-FF-FF-FF-FF-FF` is used.

4.2 Address Resolution Protocol

- This is used by hosts to know the MAC address of interfaces on the same LAN, given the IP Address of that interface.
- The ARP table is stored in the memory of each host and router in the LAN. It contains a mapping between IP Address and MAC address of interfaces.
- In case the MAC address is not found for a given IP Address, then an ARP packet containing the destination MAC address as `FF-FF-FF-FF-FF-FF` is first encapsulated into a link-layer frame and sent to all the interfaces in that subnet.
- Each interface inspects the ARP packet and checks if its IP Address matches the destination that is specified in the ARP packet. In case of a match, then that interface sends an ARP response to the original sender.
- The sender updates its ARP table and IP datagrams can now be encapsulated in link-layer frames and sent to that host.
- ARP is a plug-and-play protocol.

5 Ethernet

- Ethernet is the most widely used LAN protocol in the internet. The reasons for its popularity are:
  - Early adoption leading to large number of trained experts in the use of Ethernet technology.
  - Simpler to implement and cheaper than other LAN protocols like Token Ring, FDDI and ATM.
  - Continuous updates to Ethernet for higher speeds, switched Ethernet was a major revolution introduced in the 1990s.
  - More common and cheap hardware equipment (switches and adapters) for Ethernet than other protocols.
- The Ethernet frame has the following fields:
  1. **Preamble**: 8 byte preamble consists of 7 bytes of 10101010 and one byte of 10101011. The first 7 bytes allow the receiver to wake up and synchronize its clock with that of the receiver, and the last 2 bits of the 8th byte allow the receiver to know that the data part is starting now.
  2. **Destination and Source MAC Address**: MAC addresses of source and destination adaptors, each 6 bytes long.
  3. **Type**: 2 byte type field allows Ethernet to multiplex to various network layer protocols (not only IP). (eg: ARP has a type field of `0x0806`)

4. **Data**: (46 to 1500 bytes), if the data is less than 46 bytes then the network layer data is stuffed with some data. The network layer's length field is used to isolate the data from the stuffing.
5. **CRC**: 4-byte Cyclic Redundancy Checking code.

5.1 Switches

- Switches are active link-layer devices that perform the link-layer functions of **forwarding** and **filtering**.
- Switches are transparent, meaning that hosts and routers are not aware of their presence.
- Filtering is the functionality wherein the switch decides whether to forward or simply drop a frame. It is done in the case that the switch receives a frame from one LAN segment addressed to an adaptor on the same LAN segment.
- Forwarding is the functionality wherein the frame is forwarded to the right interface in the switch after consulting the switch table.
- The switch table is a mapping between the MAC address of an adaptor and the interface number of the switch to which that adaptor is connected.
- Switch tables are built automatically, and hence switches are called **self-learning devices**.
- Initially switch table is empty. When the switch receives an incoming frame with source MAC address A on its interface x, it enters the record (A, x) in its switch table.
- Let the destination MAC of this frame be B. As there is no entry for B in the switch table, the switch forwards this frame to all the interfaces except the one where the frame entered into the switch.
- When some interface eventually responds to this forwarded frame, the switch learns the interface number corresponding to the MAC address B as well.

5.2 Properties of Link-Layer Switching

- **No Collisions**
- **Heterogenous Links**
- **Management**: Switches can disconnect malfunctioning adaptors, are resistant to physical layer disasters (cable cut etc.) and collect important diagnostic data that can be used to configure networks better (such as bandwidth usage and collision rates and traffic data).

6 Wireless Networks

- The IEEE 802.11 protocol is responsible for creating standards for wireless networks.
- The components of a wireless network are
  1. **Wireless Hosts**
  2. **Wireless Links**: Two main characteristics are coverage area and link rate.
  3. **Wireless Access Points**: Send and receive frames from hosts associated with it (ie. within its coverage area and used by host to send data between itself and the larger network). APs are connected to the larger internet via Ethernet links.
  4. Network Infrastructure
- Networks that use wireless access points (aka base stations) are said to be operating in **infrastructure mode**.

- Networks that are self regulating, do not need any base stations are said to operate in **ad-hoc mode**. In ad-hoc mode, the wireless hosts are themselves responsible for all network services provided to one another.
- Classification of wireless networks:
  1. **Single Hop, Infrastructure**: 802.11 wireless, 3G mobile networks.
  2. **Single Hop, infrastructure-less**: No single base station, but one of the nodes coordinates all transmissions (eg: Bluetooth, 802.11 networks in ad-hoc mode)
  3. **Multiple Hops, Infrastructure**: Base station is present that is wired to the larger network. However, some wireless nodes may have to relay their communication through other wireless nodes in order to communicate via the base station. (eg: Wireless sensor networks, wireless mesh networks).
  4. **Multiple Hop, infrastructure less**: Nodes may relay their messages across several other nodes till the destination node. Nodes can be mobile with changing connectivity. (eg: Mobile Ad-Hoc Networks, Vehicular Ad-Hoc networks)

6.1 Architecture of 802.11 LAN

- A **Basic Service Set** (BSS) consists of one wireless AP and the stations (hosts) that are associated with it.
- In an ad-hoc network a BSS does not have any APs.

6.1.1 Channels and Association

- Each AP is assigned an SSID (**Service Set Identifier**) by the network admin who installed it.
- Along with an SSID, a channel number between 1 and 11 (802.11 transmits between 2.4 and 2.485 GHz, this 85 MHz band is divided into 11 channels, but channels 1, 6, 11 are the only non-overlapping ones).
- A wireless LAN with an aggregate transmission rate of 33 Mbps can be created by installing three 802.11b APs at the same physical location, assigning channels 1, 6, and 11 to the APs, and interconnecting each of the APs with a switch.
- A **WiFi jungle** is an area wherein a wireless host receives a sufficiently strong signal from more than one AP.
- The 802.11 standard requires that APs send out **Beacon Frames** at a fixed interval, the host scans all 11 channels and seeks all the APs that are sending beacon frames.
- Thus the station learns about all the nearby APs and then selection is done either manually or automatically (if automatic, then one with the highest signal strength is typically chosen).
- The station sends out an *association request* frame, and the AP responds with an *association acknowledgement* frame, to confirm the association.
- After this, the station sends out a DHCP discovery message into the subnet of that AP to get its IP Address.

6.2 802.11 MAC Protocl: CSMA/CA

- The CSMA/CA protocol is as follows:
  1. If the channel is sensed idle, then the sender waits for one **DIFS (Distributed Inter-Frame Space)** unit of time before sending.
  2. Else the sender chooses a random backoff value (from binary exponential backoff) and counts down that value while the channel is idle (if channel is busy the counter is paused).
  3. The sender transmits the entire frame when the counter reaches to 0.

4. When the receiver receives a valid frame (one that passes the CRC check), it waits for one **SIFS (Short Inter-Frame Space)** unit of time before sending a **link-layer acknowledgement message**.
5. If the transmitting station does not receive an acknowledgment within a given amount of time, it assumes that an error has occurred and retransmits the frame, using the CSMA/CA protocol to access the channel.

- To handle the **hidden-terminal** problem (host H1 and H2 are inaccessible directly from each other as they lie outside each other's coverage area, but only via the AP they can reach one another), the system of RTS (Request-To-Send) and CTS (Clear-To-Send) and ACK messages are used. The CTS is broadcast to all the nodes so that they stop trannsmitting while the sender sends the data.