7 Layer Protocol

1. Physical Layer: **(physical transmitting of data in bits - mechanical/electrical transmission)**This layer deals with the physical connection between devices. The physical layer is concerned with transmitting raw bits over a communication channel. The design issues have to do with making sure that when one side sends a 1 bit it is received by the other side as a 1 bit, not as a 0 bit. It defines the hardware specifications, such as cables, connectors, and signaling, required for transmitting raw data bits over a physical medium. It ensures that data can be transmitted and received reliably over the network infrastructure.

2. Data Link Layer: **(Framing and acknowledgement, flow control, collision resolving)** The data link layer is responsible for node-to-node communication, ensuring that data packets are delivered error-free over the physical layer. It handles tasks such as framing, error detection, and flow control. It also manages access to the physical medium, resolving issues like collisions in shared networks. Ethernet and Wi-Fi are examples of protocols that operate at this layer.

   Flow Control : Another issue that arises in the data link layer (and most of the higher layers as well) is how to keep a fast transmitter from drowning a slow receiver in data. Some traffic regulation mechanism may be needed to let the transmitter know when the receiver can accept more data.

3. Network Layer: (**routing and forwarding of data packets from the source to the destination across multiple networks.)** It is responsible for logical addressing, such as IP addresses, and determining the best path for data to travel through the network. Routing protocols like IP (Internet Protocol) operate at this layer.

   When a packet has to travel from one network to another to get to its destination, many problems can arise. The addressing used by the second network may be different from that used by the first one. The second one may not accept the packet at all because it is too large. The protocols may differ, and so on. It is up to the network layer to overcome all these problems to allow heterogeneous networks to be interconnected. In broadcast networks, the routing problem is simple, so the network layer is often thin or even nonexistent.

4. Transport Layer: **(segmentation, reassembly of data)** The transport layer ensures end-to-end communication between the source and destination devices. It provides mechanisms for segmentation, reassembly. TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) are common transport layer protocols.

5. The Session Layer: The session layer allows users on different machines to establish sessions between them. Sessions offer various services, including dialogue control **(keeping track of whose turn it is to transmit)**, token management **(preventing two parties from attempting the same critical operation simultaneously)**, and synchronization **(checkpointing long transmissions to allow them to pick up from where they left off in the event of a crash and subsequent recovery).**

6. Presentation Layer: The presentation layer is responsible for data translation, encryption, and compression. It ensures that data exchanged between applications is in a format that the recipient can

understand. **It handles tasks such as data encryption, character encoding, and data compression, thereby ensuring interoperability between different systems.**

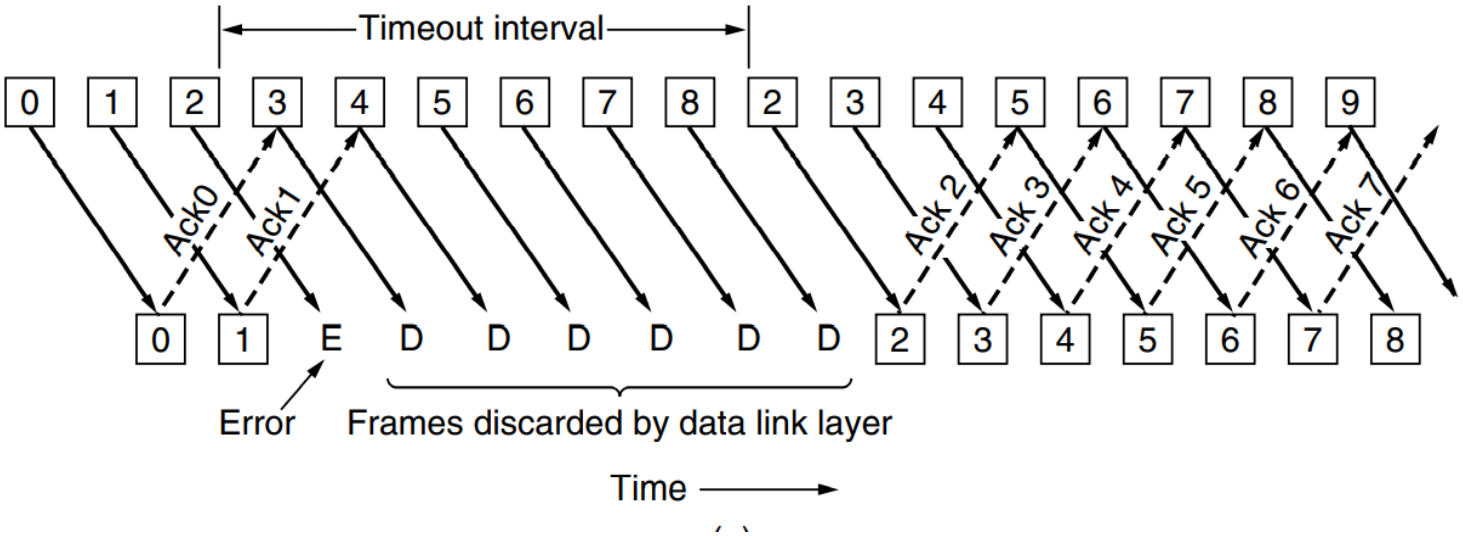
7. Application Layer: The application layer **enables communication between end-user applications and the network.** It provides interfaces for applications to access network services such as email, web browsing, file transfer, and remote login. Protocols like HTTP, FTP, SMTP, and DNS operate at this layer.

Switching

Packet Switching: Packet-switching networks place a tight upper limit on the size of packets. This ensures that no user can monopolize any transmission line for very long (e.g., many milliseconds), so that packet-switched networks can handle interactive traffic. It also reduces delay since the first packet of a long message can be forwarded before the second one has fully arrived

Q: does it broadcast? What is the use of small packets?

Go Back N and Automatic Repeat



1. Sender Window: The sender maintains a window of packets that it has sent but not yet received acknowledgment for. The size of this window is limited to N, hence the name "Go-Back-N."
2. Sending Packets: The sender sends multiple packets in sequence without waiting for individual acknowledgments. It continues sending until the window is filled.
3. Receiver Acknowledgment: The receiver acknowledges the receipt of packets by sending an acknowledgment (ACK) back to the sender. The ACK typically contains the sequence number of the next expected packet.
4. Timeout: If the sender does not receive an ACK for a packet within a certain timeout period, it assumes that the packet or one or more subsequent packets are lost and retransmits all unacknowledged packets in the window.
5. Go-Back-N Behavior: Upon a timeout, the sender "goes back" to retransmit the earliest unacknowledged packet and all subsequent packets in the window.
6. Duplicate Packets Handling: When the receiver receives a duplicate packet (due to retransmission), it discards the duplicate but still sends an acknowledgment for the last correctly received packet.

r+1 bit G(x) or r degree

00001……100000

If N is the frame length of T(x), then K = 1,...,N

[T(x) + E(X)] / G(x)

Single bit errors => x^i	G(x) has 2 or more terms
Two isolated single bit errors => x^i + x^j , i>j	G(x) % x != 0 and (x^K+ 1) % G(x) !=0
Odd number of errors	X+1 is a factor of G(x)
Burst errors of length <= r	r degree G(x) and G(x) has the final bit as 1

If the burst length is $r + 1$, the remainder of the division by $G(x)$ will be zero if and only if the burst is identical to $G(x)$. By definition of a burst, the first and last bits must be 1, so whether it matches depends on the $r - 1$ intermediate bits. If all combinations are regarded as equally likely, the probability of such an incorrect frame being accepted as valid is $½^{r-1}$.

It can also be shown that when an error burst longer than $r + 1$ bits occurs or when several shorter bursts occur, the probability of a bad frame getting through unnoticed is $½^{r}$, assuming that all bit patterns are equally likely.

1……1

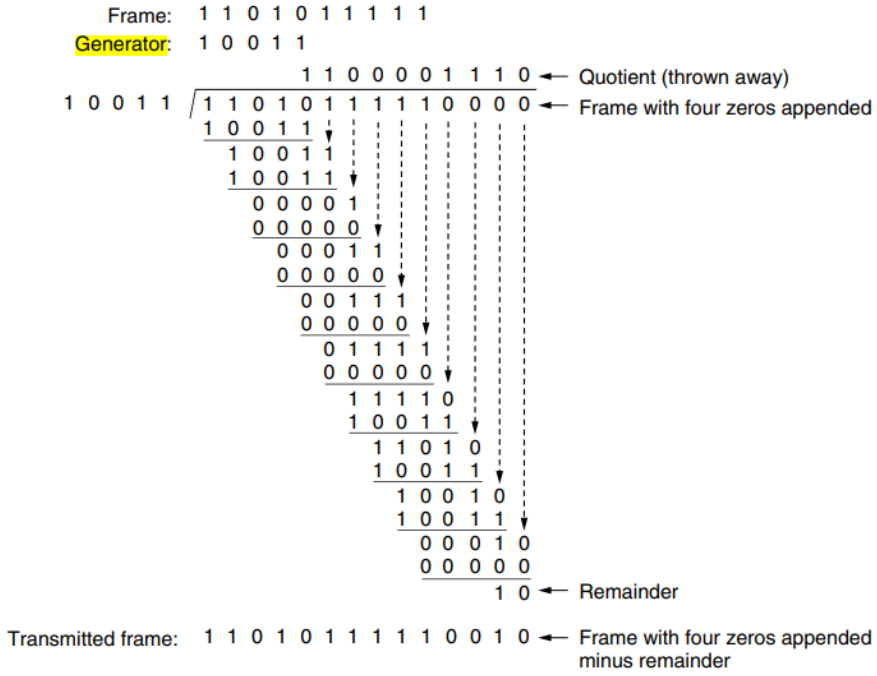


Figure 3-9. Example calculation of the CRC.

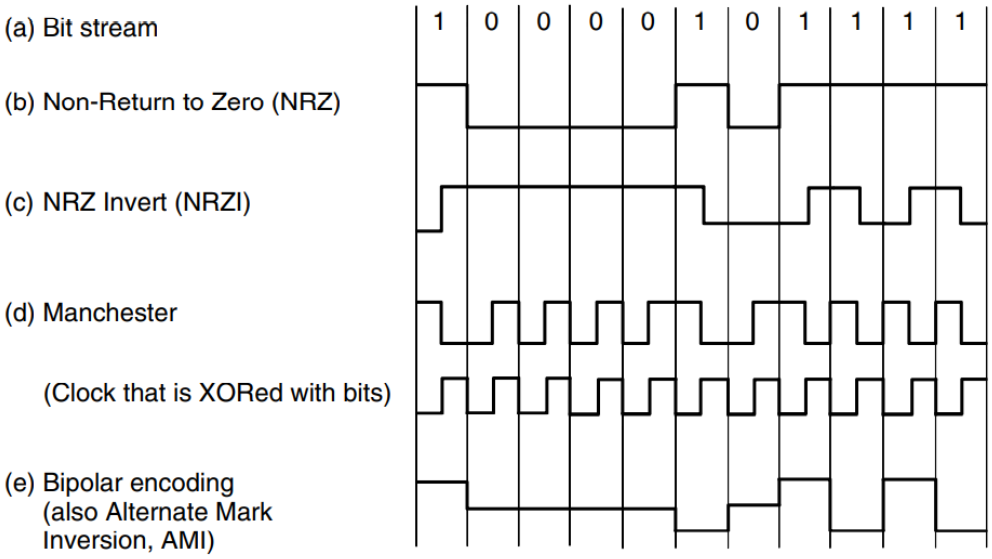
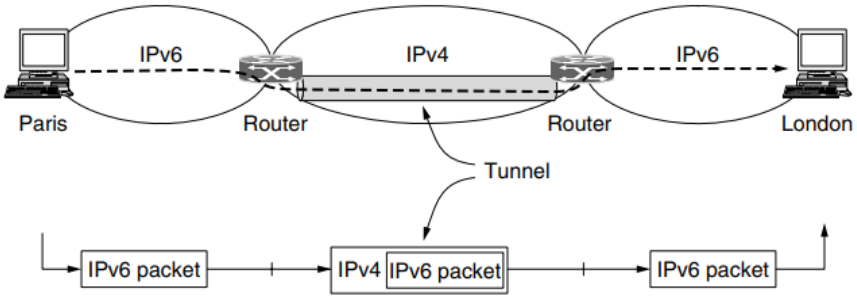


Figure 2-20. Line codes: (a) Bits, (b) NRZ, (c) NRZI, (d) Manchester, (e) Bipolar or AMI.

4. **Multiplicative Inverse (except for 0):**
   - For every nonzero element a in $\mathbb{Z}/P\mathbb{Z}$, its multiplicative inverse a^{-1} exists because of the property of modular arithmetic that ensures that if a and P are coprime, then there exists an integer b such that $a \times b \equiv 1 \mod P$. Since P is prime, every integer a in the range 1 to $P - 1$ is coprime with P, and hence, has a multiplicative inverse.

Tunneling



Three way handshake