

Lecture 2: Computer Networks Review (Part I)

Yuan Xue

Suppose you want to build a computer network. What technologies would serve as the underlying building blocks, what kind of software architecture would you design to integrate these building blocks into an effective communication service, and what would be the weaknesses in the design that may be exploited by attackers? Answering these questions is the overall goal of this lecture.

I. DIRECT LINK NETWORKS

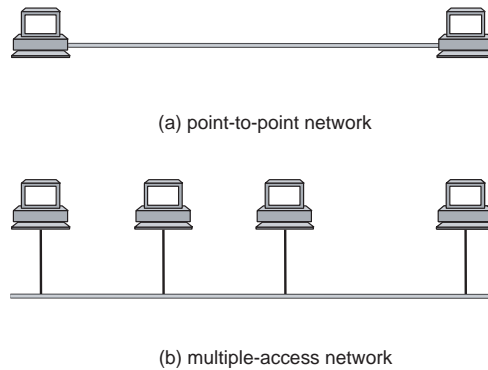


Fig. 1. Direct Link Network.

Starting from the simplest, we study the network in which all the hosts are directly connected by some physical medium (as shown in Fig. 1), such as a wire or a fiber. There are five additional problems that must be addressed before the hosts can successfully communicate with each other.

- *Encoding.* The first step to establish communication between two hosts is to turn binary data into the signals that the links are able to carry, and then to transform the signal back into the corresponding binary data at the receiving node. Let us ignore the details of modulation, and assume that we are working with two discrete signals: high and low. As shown in Fig. 2, different encoding mechanisms can encode bits into signals.

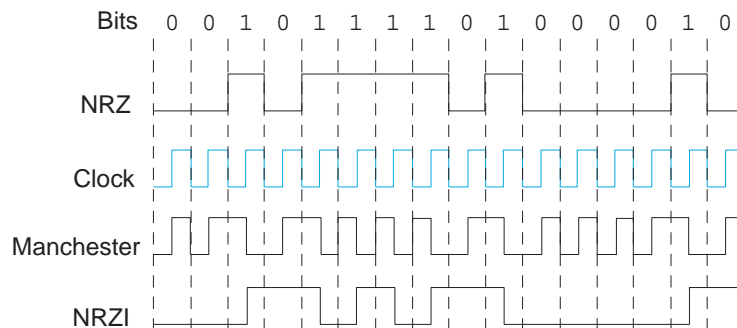


Fig. 2. Encoding Schemes.

- *Framing.* With encoding, we know how to transmit a sequence of bits over a point-to-point link. Framing then delineates the sequence of bits transmitted over the link into complete messages that

can be delivered. There are several approaches to address the framing problem, including the sentinel approach (e.g., PPP) and the byte-counting approach for byte-oriented protocols; and high-level data link control (HDLC) for bit-oriented protocols.

- *Error detection.* Bit errors can be introduced into frames due to electrical interference or thermal noise. Error detection detects transmission errors. Several commonly techniques for error detection include cyclic redundancy check (CRC) (e.g., Fig. 3 (a)), two-dimensional parity (e.g., Fig. 3 (b)), and Internet checksum. Some error codes can only detect the errors, some codes are strong enough to correct errors.

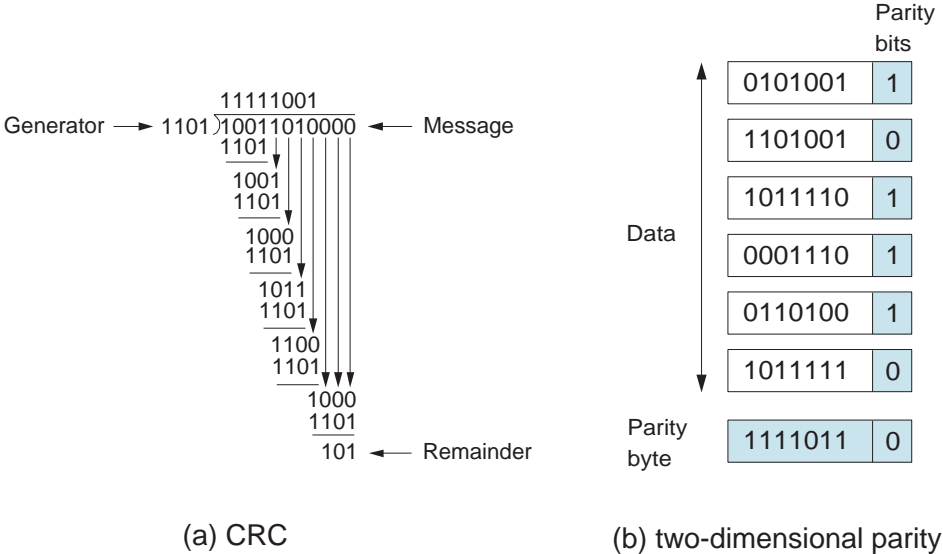


Fig. 3. Error Detection Schemes.

- *Reliability delivery.* When errors are detected, and can not be corrected, the corrupted frames must be discarded. Reliability delivery is sometimes implemented in point-to-point link network to recover from these lost frames.
- *Media access control.* When the link is shared by multiple hosts, their accesses to the link need mediation. Take Ethernet as an example. CSMA/CD (Carrier Sense Multiple Access / Collision Detection) is used to provide media access control. Essentially, participating hosts monitor the traffic on the link. If no transmission is taking place at the time, the particular host can transmit. If two hosts attempt to transmit simultaneously, this causes a collision, which is detected by all participating hosts. After a random time interval, the hosts that collided attempt to transmit again. If another collision occurs, the time intervals from which the random waiting time is selected are increased step by step. This is known as exponential back off.

Nearly all the networking functionalities described above are implemented in the network adaptor (as shown in Fig. 4): encoding, framing, error detection, and the media access control. In Ethernet, each adaptor has a unique Ethernet address, which is also the MAC address of the corresponding host. Each frame transmitted on an Ethernet is received by every adaptor connected to that Ethernet. Each adaptor recognizes those frames addressed to its own address, and passes only those frames to the host. An adaptor can also be programmed to run in *promiscuous* mode, in which case it delivers all received frames to the host.

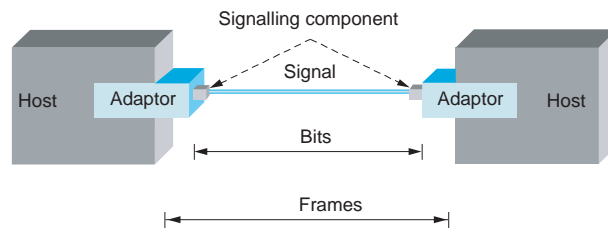


Fig. 4. Network Adaptor.

Even in such a simple direct link network, security threats still exist. Some examples include frequency jamming, eavesdropping (*e.g.*, packet sniffing), MAC address spoofing.