Computer Networks

-Data link layer-

College of Information Science and Engineering
Ritsumeikan University

RITSUMEIKAN UNIVERSITY

W4 short test (1)

- Explain the main idea behind NAT!
  - Assign each home or business a single IP for traffic, but within the customer network, every computer gets a unique IP. Before the packet exists the customer network and goes to the ISP, the address is translated by the Network Address Translation box from an internal IP to the shared public IP. When it's applicable (e.g., TCP or UDP connection), the source port is replaced by an index into the NAT box's translation table, containing the original IP address and the original source port.
- What are the advantages of IPv6 compared to IPv4?
  - Longer addresses means more possible addresses, simplified header so faster to process packets for routers, better support for options and easier to skip over them.
- What is the hop limit field in the IPv6 header, and what does it mean?
  - Basically the time to live, that means the maximum number of hops between routers the packet can travel before discarded.

W4 short test (2)

- What is the main use case of the Internet Control Message Protocol?
  - Used by routers to send operational information and error messages to other addresses.
- Why do we need the Address Resolution Protocol?
  - Network Interface Cards do not understand Internet addresses, but have a physical machine address. ARP is used to identify these data link layer addresses associated with an IP address, to be able to communicate between hosts within/between networks.
- After the DHCP server receives an IP address request, it reserves an IP address and sends a message to the client. Which message is this?
  - DHCP OFFER
- Inside its own network, an organization can use its own algorithm for internal routing. However, when routing between independently operated networks, the same *exterior gateway* protocol must be used.

W4 short test (3)

- Which units are exchanged by which layers?
  - Segment - Transport layer, Packet - Network layer, Frame - Data link layer
- Which socket primitive would be used to release a connection?
  - CLOSE

W6 recap (1)

- The transport service is implemented by a transport protocol
- There are socket primitives that can be used to transfer data over a connection using TCP
- The three-way handshake used by TCP involves one peer checking with the other that the connection request is indeed current with a realiable way to release connections
- UDP is a connectionless protocol without flow or congestion control that is useful for many client-server situations (e.g., DNS, multimedia, broadcasting)

W6 recap (2)

- The connection-oriented TCP service is obtained by both the sender and the receiver creating endpoints called sockets
- Sockets have socket addresses including the IP address of the host and a number local to the host called a port
  - common ports
- The TCP header includes source port and destination port, sequence number, acknowledgment number, TCP header length, eight 1-bit fields, window size, checksum, urgent pointer, options, and data
- Establishing a TCP connection involves multiple connection states and managing the TCP window for the receiver's buffer
- TCP plays the main role in controlling congestion and ensuring reliable transport using a congestion window and algorithms like slow-start

Agenda

- Data link design
- Framing
- Error Detection and Correction
- Protocol examples
- Summary

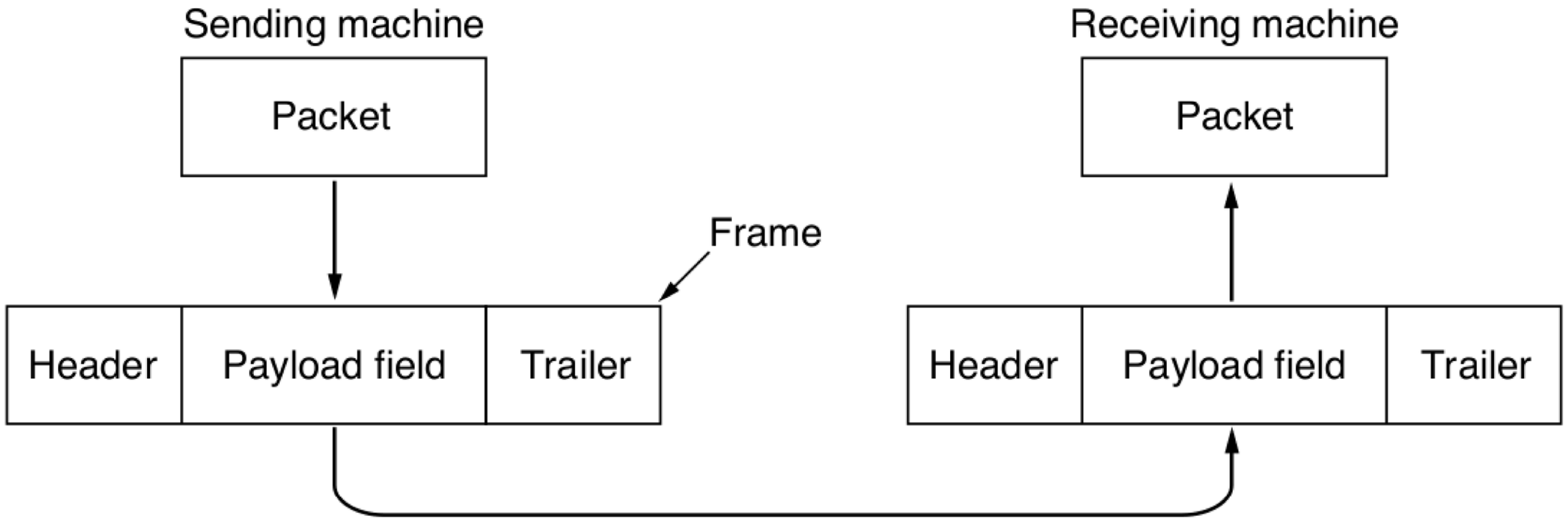
Data link layer functions

- The data link layer uses the services of the physical layer below it to send and receive bits over communication channels
- Communication channels make errors occasionally, maybe data lost
- Finite data rate with a nonzero propagation delay between the time a bit is sent and it is received

1. Provide a well-defined service interface to the network layer
2. Framing sequences of bytes as self-contained segments
3. Detecting and correcting transmission errors
4. Regulating the flow of data

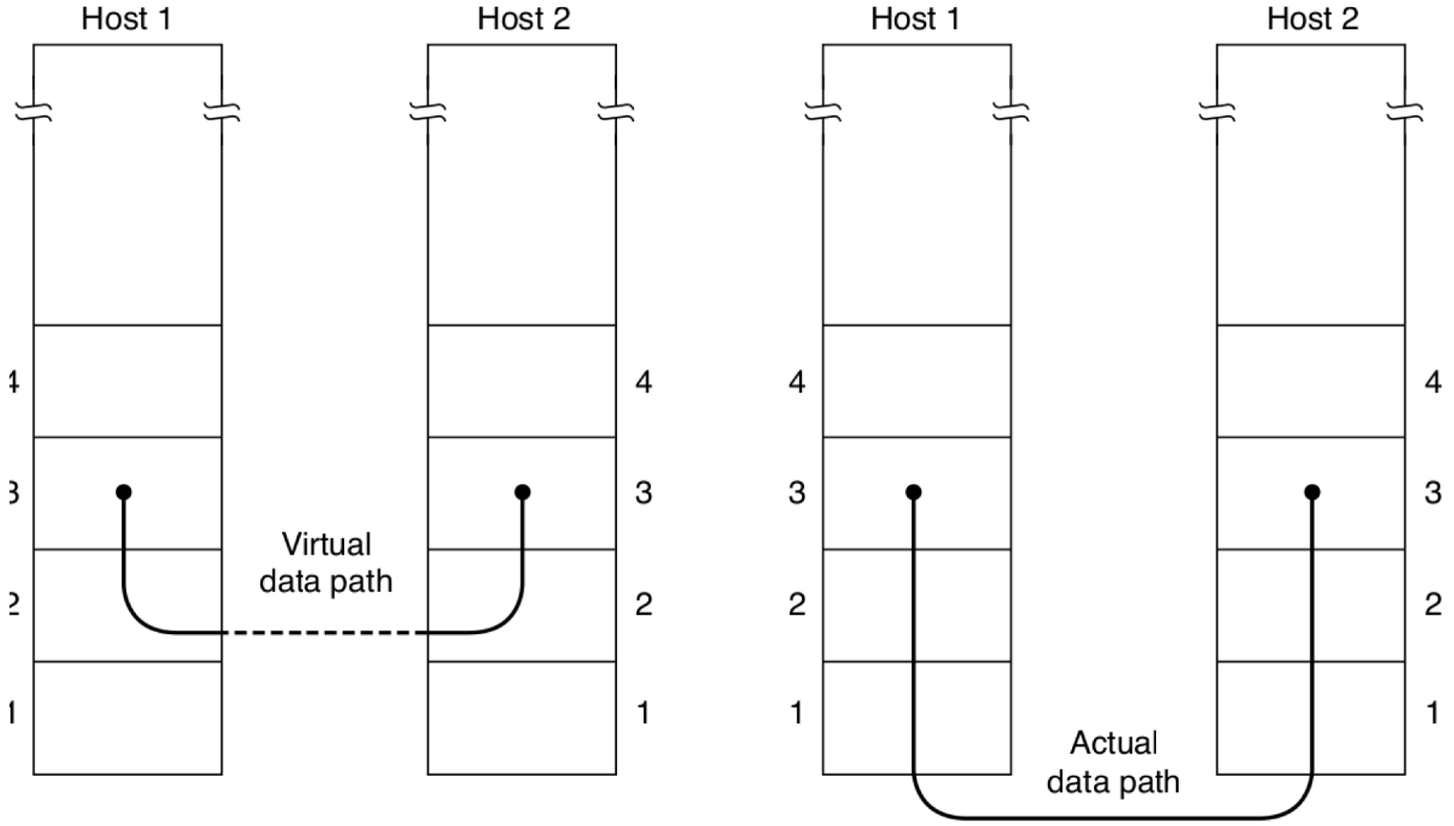
- The data link layer takes the packets it gets from the network layer and encapsulates them info **frames** for transmission

Packets and frames



Services to the Network layer (1)

- The main service of the link layer is transferring data from the network layer on the source machine to the network layer on the destination machine



Services to the Network layer (2)

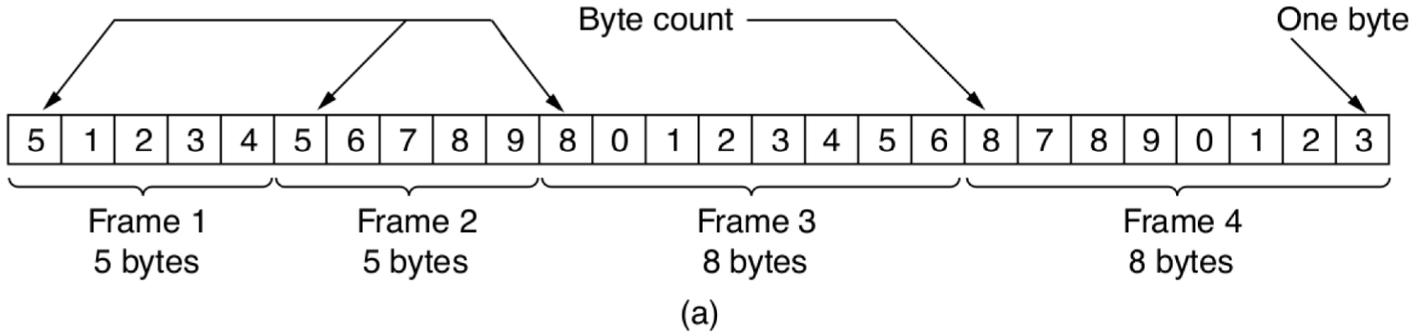
- Actual services vary from protocol to protocol
- Three main types of possible services
- Unacknowledged connectionless service, such as Ethernet
  - appropriate when error rate is low so recovery is left to higher layers
  - real-time traffic where late data is worse than bad data (e.g., video)
- Acknowledged connectionless service, such as WiFi
  - still no logical connections, but frames are sent individually acknowledged
  - good over unreliable channels
- Acknowledged connection-oriented service, such as satellite channel
  - source and destination machines establish a connection before any data are transferred
  - the data link layer guarantees that each frame is received in the right order
  - good for long, unreliable links

Breaking up the bit stream

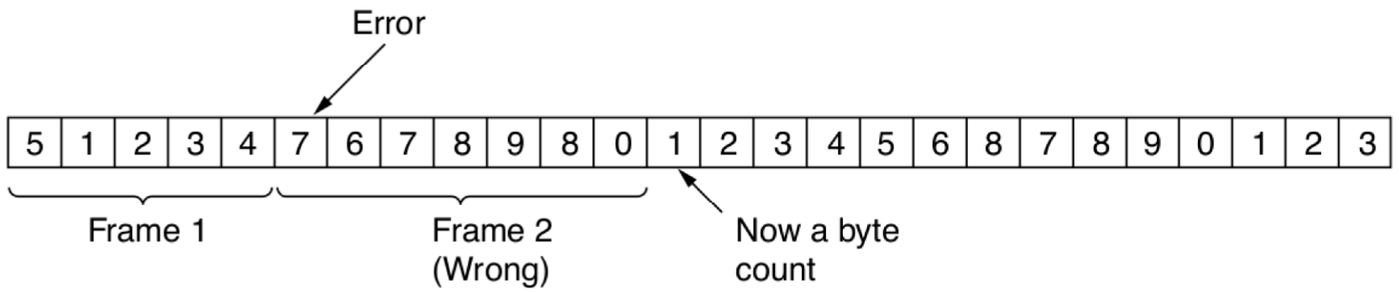
- To provide a service to the network layer, the link layer must use the service provided to it by the physical layer
  - if the channel is noisy (e.g., wireless), it will add some redundancy to its signals to reduce the bit error rate
  - however, the bit stream received by the data link layer is not guaranteed to be error-free (e.g., bits with different values, different number of bits, etc.)
- Breaking up the bit stream into discrete frame while making it easy for the receiver to find the start of new frames (and using little channel bandwidth)
  - byte count
  - flag bytes with byte stuffing
  - flag bytes with bit stuffing
  - physical layer invalid characters

Using just byte count

- Uses a field in the header to specify the number of bytes in the frame
- When the data link layer at the destination sees the byte count, it knows how many bytes follow (and where is the end of the frame)
- Transmission errors can happen: unable to locate the correct start of the next frame (even if the destination knows it is incorrect), so rarely used as it is



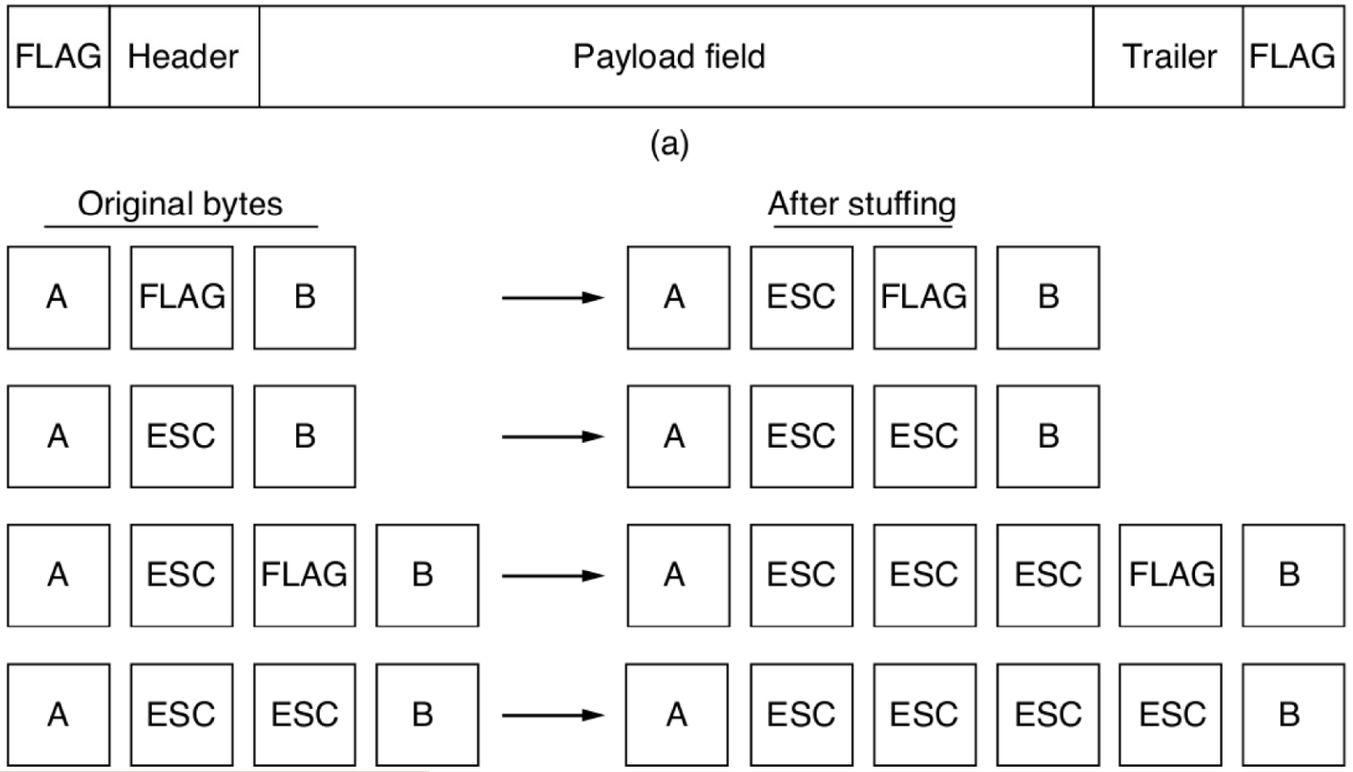
(a)



(b)

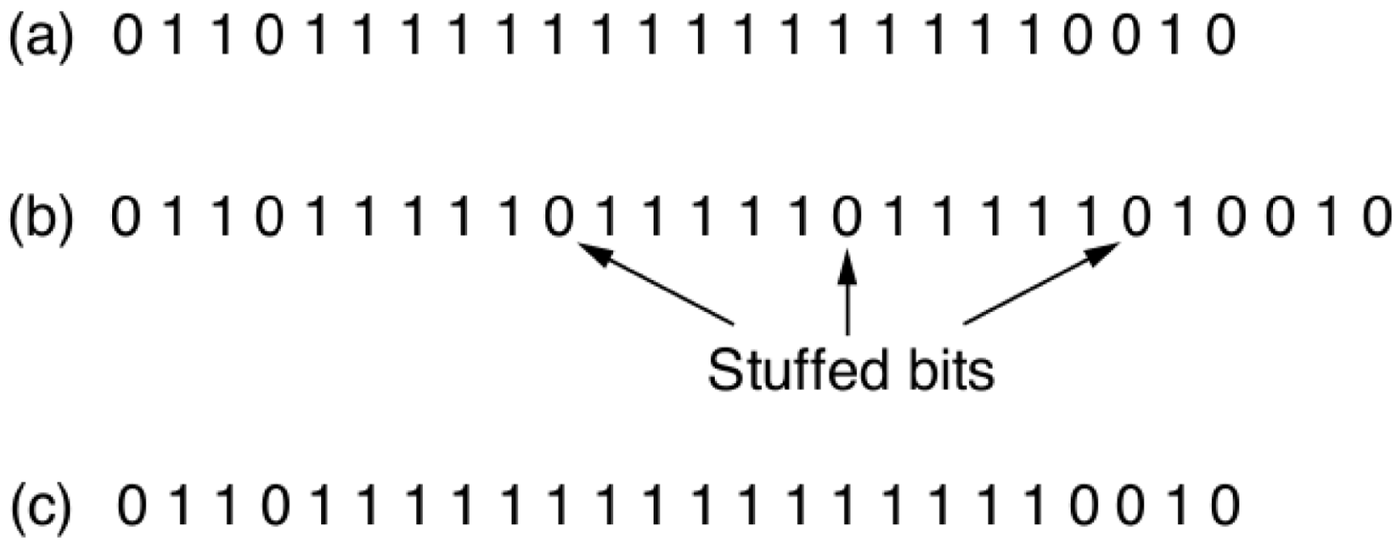
Byte stuffing

- Have each frame start and end with special bytes, called a **flag byte**
- Have the sender's data link layer insert a special escape byte just before "accidental" flag bytes: **byte stuffing**
- Basis of the **PPP** (Point-to-Point Protocol) that carries packets over the Internet



Bit stuffing and Invalid characters

- Here, frames contain an arbitrary number of bits made up of units of any size
- Each frame begins and ends with a special bit pattern, a flag byte
- Ensures a minimum density of transitions that help the physical layer maintain synchronization, basis for the **HDLC** (High-level Data Link Control) protocol



- Some reserved signals (invalid characters/"code violations") can be used to indicate the start and end of frames

Error control and Flow control

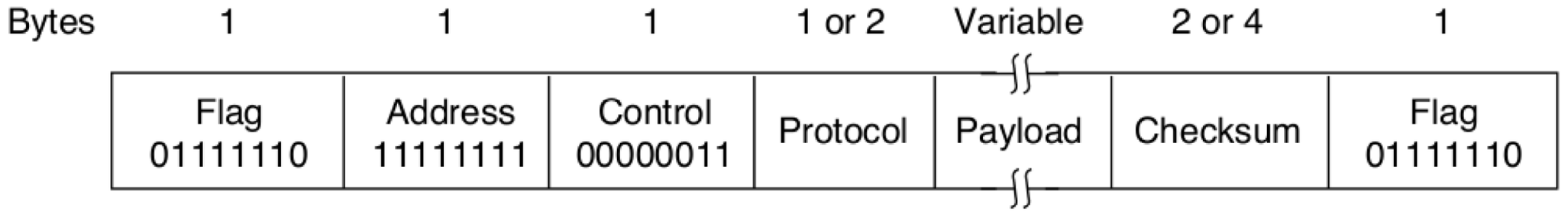
- Error control is mainly about ensuring all frames are eventually delivered
  - to the network layer at the destination, in the proper order
- Ensures reliable, connection-oriented service
- Requires acknowledgement frames and timers
- Flow control is needed when a sender wants to transmit frames faster than the receiver can accept them
  - feedback-based flow control: receiver sends back information to the sender giving it permission to send more data or receiver tells the sender how the receiver is doing
  - rate-based flow control: protocol has a built-in mechanism that limits the rate at which senders may transmit data, no feedback from the receiver is necessary

Correction vs Detection

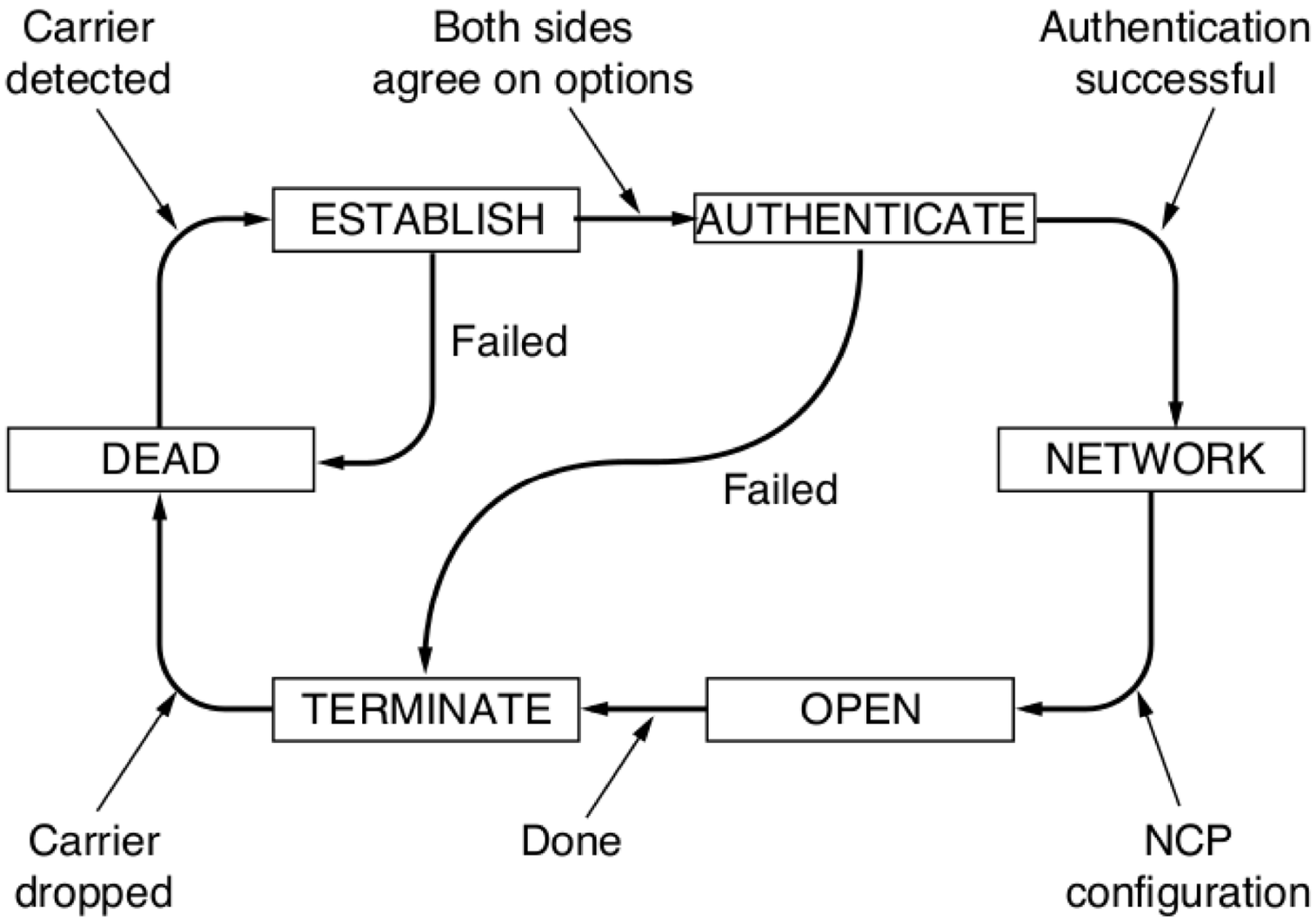
- Error-correcting codes, referred to as **FEC** (Forward Error Correction)
  - include enough redundant information to enable the receiver to deduce what the transmitted data must have been
  - e.g., **Hamming codes** where the source encodes the message by adding redundant bits for the detection of up to two immediate bit errors
- Error-detecting codes
  - include only enough redundancy to allow the receiver to deduce that an error has occurred (but not which error) and have it request a retransmission
  - e.g., an example of **checksum**, **parity bits**: adding an extra bit to indicate if the number of 1 bits is even or odd
- Key consideration is the type of errors likely to occur, e.g. over fiber the error rate is lower compared to wireless, so error detection and retransmission is more efficient than dealing with an occasional error and correcting it

Data link layer protocols (1)

- HLDC (High-level data link control): a bit-oriented protocol developed by ISO
- PPP (Point-to-point protocol): establishing a direct connection between two nodes without any host or any other networking device in between over many types of physical networks including serial cable, phone line, trunk line, cellular telephone, etc.

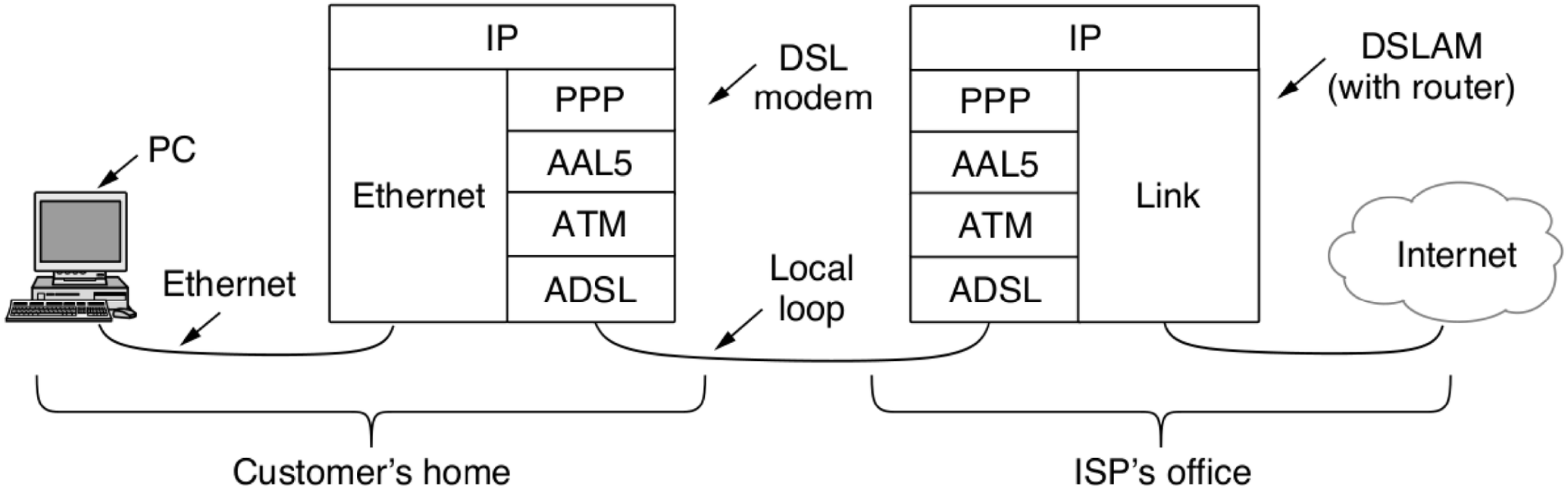


PPP state diagram



Data link layer protocols (2)

- Protocols in the **ADSL** (Asymetric Digital Subscriber Loop)



- In Ethernet: commonly used in LAN, MAN, WAN and not limited to the Data link layer

W7 summary (1)

- The data link layer uses the services of the physical layer below it to send and receive bits over communication channels
- Communication channels make errors occasionally, data may be lost
- The data link layer takes the packets it gets from the network layer and encapsulates them info frames for transmission
  1. Provide a well-defined service interface to the network layer
  2. Framing sequences of bytes as self-contained segments
  3. Detecting and correcting transmission errors
  4. Regulating the flow of data
- Three main types of possible services: unacknowledged, acknowledged connectionless, acknowledged connection-oriented
- To provide a service to the network layer, the link layer must use the service provided to it by the physical layer

W7 summary (2)

- Methods for breaking up the bit stream into discrete frames: byte count, flag bytes with byte stuffing or bit stuffing, and invalid characters
- Error control is mainly about ensuring all frames are eventually delivered to ensure a reliable service
- Flow control is about controlling the sending of transmission frames at a faster pace than they can be accepted
- FEC include enough redundant information to enable the receiver to deduce what the transmitted data must have been (e.g., Hamming codes)
- Error-detecting codes include only enough redundancy to allow the receiver to deduce that an error has occurred (but not which error) and have it request a retransmission (e.g., checksum, parity bits)
- PPP is about establishing a direct connection between two nodes without any host or any other networking device in between over many types of physical networks

W8 review test

- Similar style as the short tests
  - will be held on Manaba R+, so bring a device you wish to use to complete the test
  - students may use any material to complete the test
- Recheck previous short tests, and study the class handouts (slides) alongside with the textbook
  - there will be no questions related to material we did not cover (even if it is in the textbook)