Chapter 2

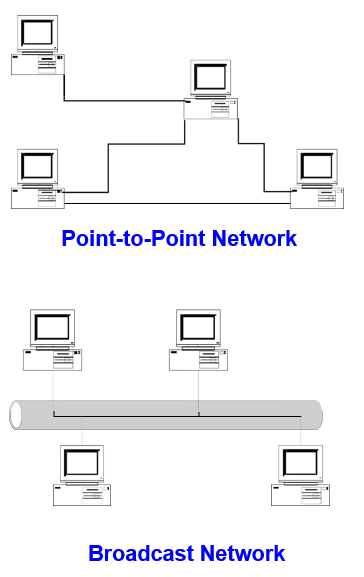
**Data Link Layer**

Main tasks:

* Transfer network layer data from one machine to another machine via a data link
* Convert the data between raw bit stream of the physical layer and groups of bits -> bytes -> frames
* Perform flow control between sender and receiver
* Error detection and correction
* Sliding Window Protocols

**Types of Networks**

* Point-to-point network
  + Each link connects two end po ints: hosts or any network devices
  + Usually for long distance connections
* Broadcast Network
  + A number of stations share a common transmission medium
  + Usually for local networks



**Possible Services**

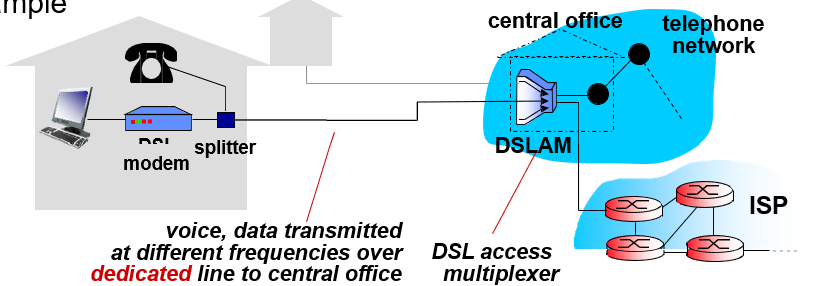
* Unacknowledged connectionless service
  + Frame is sent with no connection / error recovery
  + Ethernet
* Acknowledged connectionless service
  + Frame is sent with retransmissions if needed
  + 802.11
* Acknowledged connection-oriented service
  + Connection is set up; rarely done

**Multiple Access**

* Network Topology
  + Point-to-Point> N(N-1)/2 links to connect N nodes
  + Broadcast -> The shared medium forms a single domain
* Medium Access Control (MAC) Protocols
  + Rules to share a medium
  + Carrier Sense Multiple Access/Collision Detection (CSMA/CD)
  + Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA)

**Point-To-Point protocol**

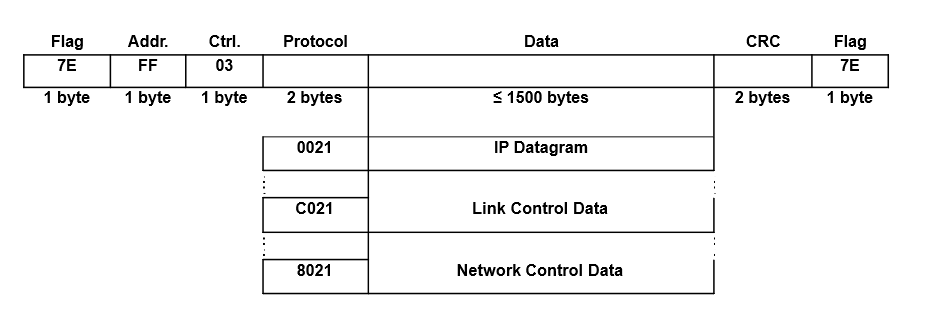
* Data link protocol
* Main purpose of PPP is **encapsulation** and **transmission** of IP datagrams, or other network layer protocol data, over a serial link
* Currently, PPP is used by most dial-up Internet access
* Everything is connected via DSLAM



**PPP Encapsulation**

PPP frame format

* Flag: mark the beginning and ending of a frame
* Protocol: used to multiplex different protocol data
* No addressing, only two end hosts



**Point-to-Point Protocol**

PPP consists of two types of control protocols:

* Link Control Protocol (LCP)
  + Responsible for agreeing on PPP encapsulation options, packet size limits, and detecting common mis-configuration errors over the data link
  + Optional features to provide peer authentication, detect link status
* Network Control Protocol (NCP)
  + PPP supports a family of NCPs and treat each network protocol like an interface
  + IP Control Protocol, used for configure the link to transmit IP datagrams

**Local Area Networks**

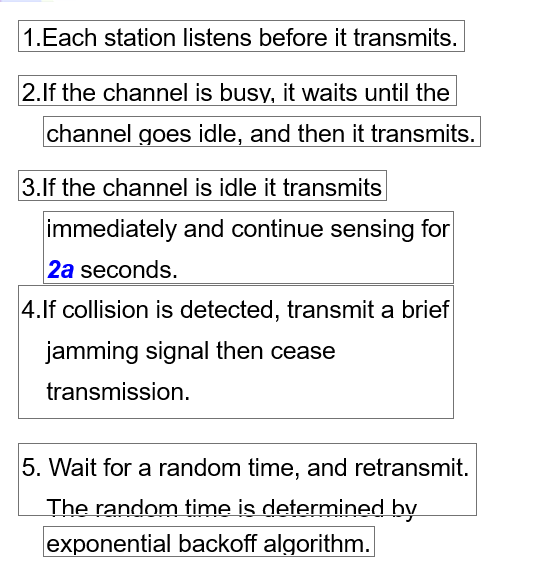
* LANs typically connect computers within a building or a campus
* Many LANs are broadcast networks
* **Bus** and **Ring** are two typical LAN topologies used in early days
* The protocol that determines who can transmit on a broadcast channel is called the Medium Access Control (MAC) protocol

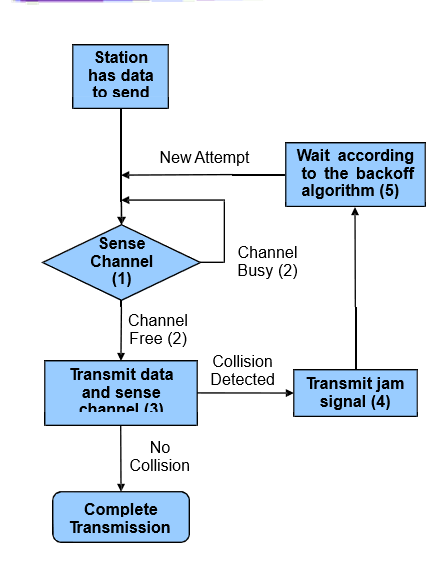


* In order to ensure that only one station transmit at a time on a shared communications channel, the MAC protocol determines who can transmit on a broadcast channel
* The MAC protocol is implemented in the MAC sublayer which is the lower sublayer of the data link layer
* The higher portion of the data link layer if the Logical Link Control (LLC)
* The LLC provides the different services to the network layer
  + Unacknowledged connectionless service
  + Acknowledged connectionless service
  + Connection-oriented service
  + Framing
  + Error Control
  + Addressing

**Media Access Control**

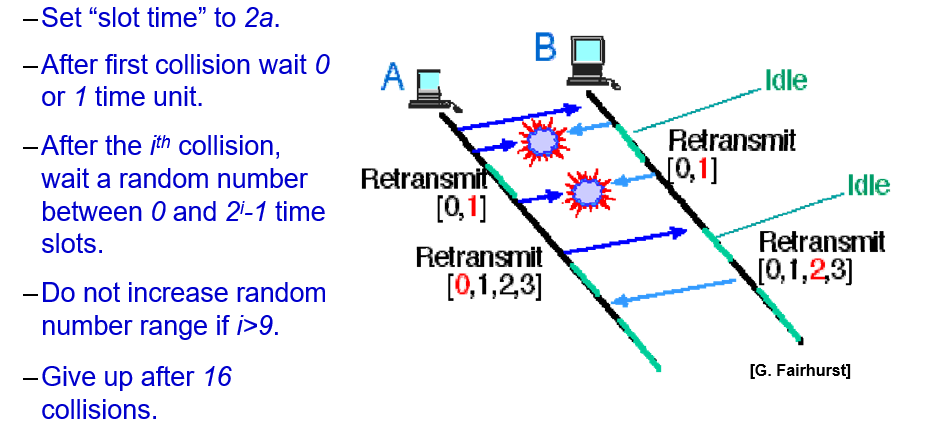
* MAC algorithms are used to resolve collisions and share the medium in a broadcast network

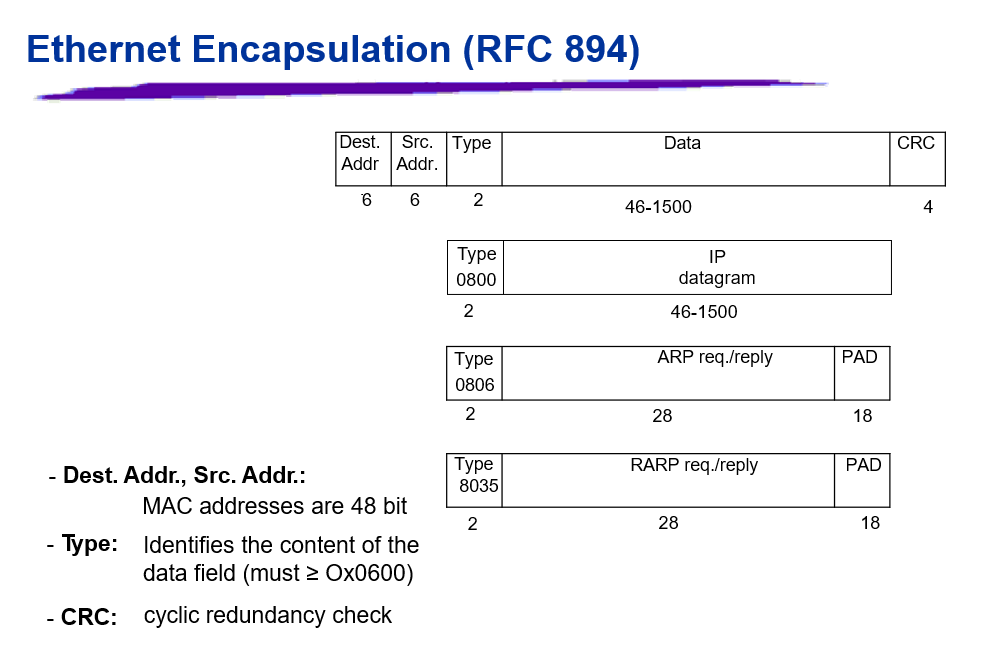


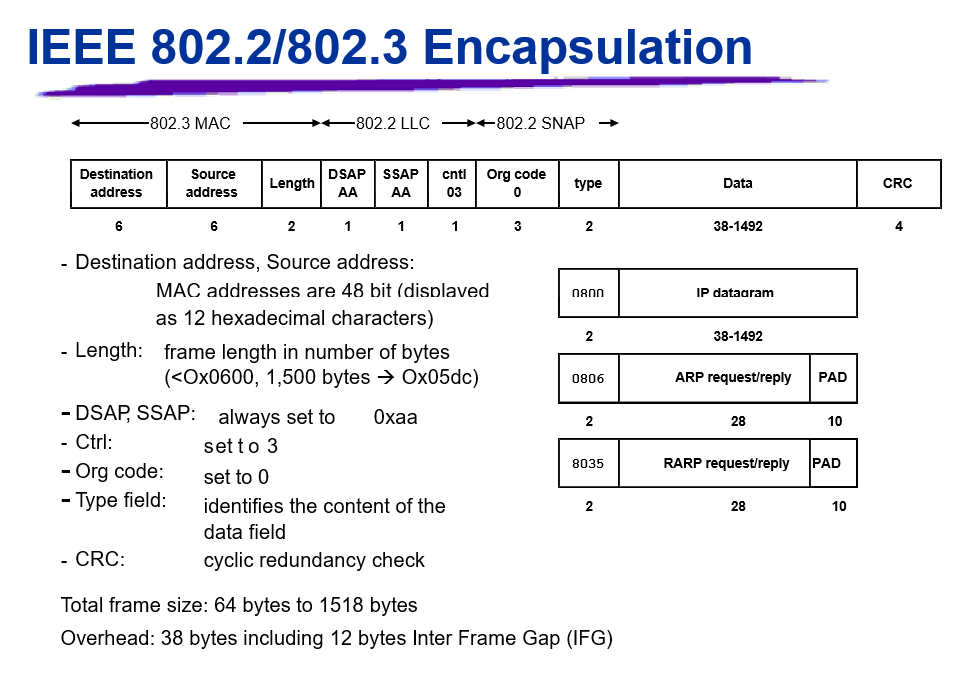


**Exponential Backoff Algorithm**

* If a station is involved in a collision, it waits a random amount of time before attempting a retransmission
* The random time is determined by the following algorithm





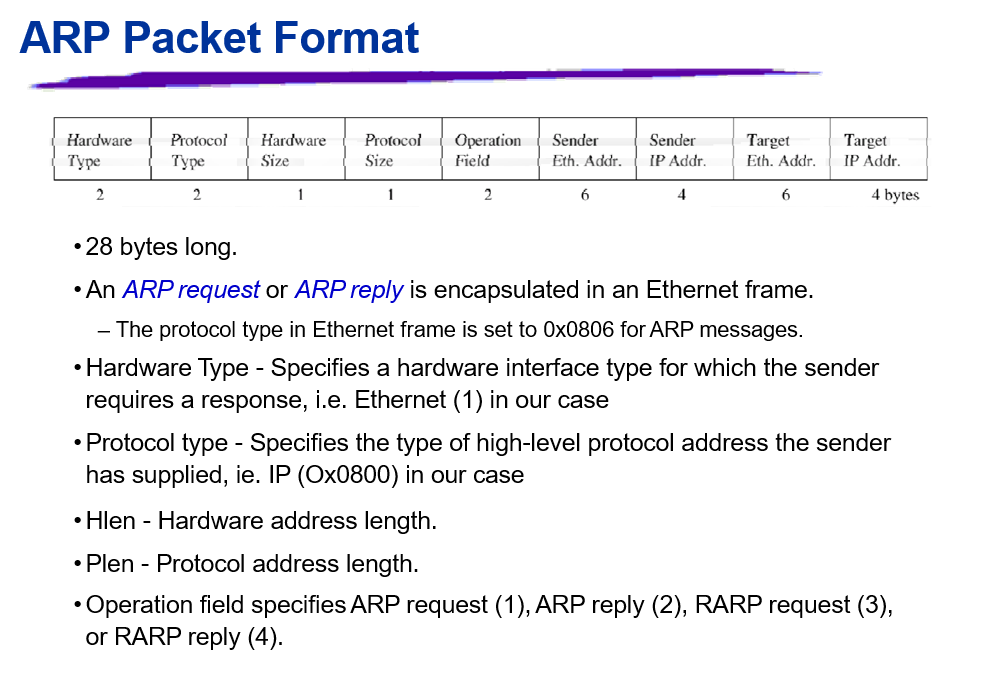


**Address Resolution Protocol**

* IP addresses are not recognizable in the interface layer where physical addresses (or MAC addresses) are used
* Different kinds of physical networks use different addressing schemes
* Address Resolution Protocol (ARP): maps an IP address to a MAC address per RFC 826
* Reverse Address Resolution Protocol (RARP): maps a MAC address to an IP address per RFC 903

**ARP Process**

* When a source host wants to send an IP packet to a destination, it first broadcasts an **ARP request** asking for the MAC address corresponding to a target IP address
* A target device will return an **ARP reply** with its MAC address
* All other networks receiving the ARP request will record the sender’s IP address and MAC address



* Ethernet destination: ff:ff:ff:ff:ff:ff (broadcast address)
* Target Ethernet Address: not set
* The ARP reply is sent by the node whose IP address matches the **target IP address** in the ARP request
  + It fills its MAC address into the **target Ethernet Address** field of the ARP request
  + It then swaps the two sender addresses (Ethernet and IP addresses) with the two target addresses, sets the op field to 2
  + The ARP reply is sent back to the source host only
* **All other nodes receiving the broadcast ARP request record the MAC and IP address of the sender**

**Arp Cache**

* Sending an ARP request/reply for each IP datagram is inefficient
* Each host maintains an **ARP cache** containing the recent resolved IP addresses
* A source host first checks its ARP cache for the destination MAC address
  + If entry is found, send out the IP packet within an Ethernet Frame
  + Otherwise, send an ARP request
* Elements of an entry in the ARP table
  + IP address
  + MAC address
  + Flags
* An entry expires after 20 minutes after it is created or referred to
* Manipulate the ARP table by the ARP command
  + -arp -a: Displays all entries in the ARP table
  + -arp -d: Deletes an entry in the ARP table
  + -arp -s: Inserts an entry into the ARP table