Chapter 5
Data Link Layer

A note on the use of these ppt slides:

We're making these slides freely available to all (faculty, students, readers). They're in powerpoint form so you can add, modify, and delete slides (including this one) and slide content to suit your needs. They obviously represent a *lot* of work on our part. In return for use, we only ask the following:
- If you use these slides (e.g., in a class) in substantially unaltered form, that you mention their source (after all, we'd like people to use our book!)
- If you post any slides in substantially unaltered form on a www site, that you note that they are adapted from (or perhaps identical to) our slides, and note our copyright of this material.

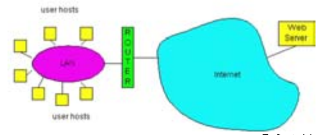
Thanks and enjoy! JFK/KWR

Computer Networking: A Top Down Approach Featuring the Internet,
2nd edition.
Jim Kurose, Keith Ross
Addison-Wesley, July 2002.

LAN technologies

Data link layer so far:
- services, error detection/correction, multiple access

Next: LAN technologies
- addressing
- Ethernet
- hubs, bridges, switches
- 802.11
- PPP
- ATM



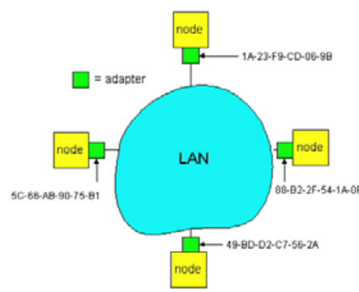
LAN Addresses and ARP

32-bit IP address:
- *network-layer* address
- used to get datagram to destination IP network (recall IP network definition)

LAN (or MAC or physical or Ethernet) address:
- used to get datagram from one interface to another physically-connected interface (same network)
- 48 bit MAC address (for most LANs) burned in the adapter ROM

LAN Addresses and ARP

Each adapter on LAN has unique LAN address

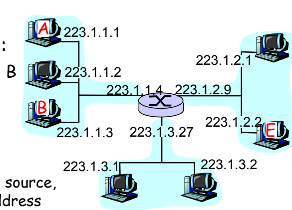


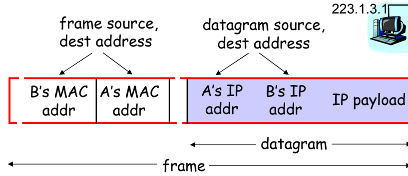
LAN Address (more)

- MAC address allocation administered by IEEE
- manufacturer buys portion of MAC address space (to assure uniqueness)
- Analogy:
  - (a) MAC address: like Social Security Number
  - (b) IP address: like postal address
- MAC flat address => portability
  - can move LAN card from one LAN to another
- IP hierarchical address NOT portable
  - depends on IP network to which node is attached

Recall earlier routing discussion

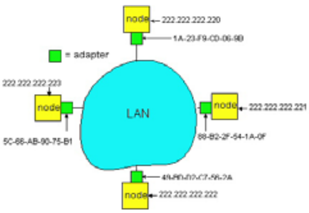
Starting at A, given IP datagram addressed to B:
- look up net. address of B, find B on same net. as A
- link layer send datagram to B inside link-layer frame





ARP: Address Resolution Protocol

Question: how to determine MAC address of B knowing B's IP address?



- Each IP node (Host, Router) on LAN has ARP table
- ARP Table: IP/MAC address mappings for some LAN nodes
  - < IP address; MAC address; TTL>
  - TTL (Time To Live): time after which address mapping will be forgotten (typically 20 min)

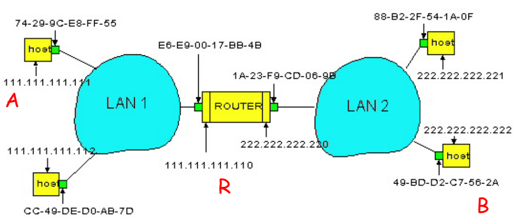
ARP protocol

- A wants to send datagram to B, and A knows B's IP address.
- Suppose B's MAC address is not in A's ARP table.
- A broadcasts ARP query packet, containing B's IP address
  - all machines on LAN receive ARP query
- B receives ARP packet, replies to A with its (B's) MAC address
  - frame sent to A's MAC address (unicast)
- A caches (saves) IP-to-MAC address pair in its ARP table until information becomes old (times out)
  - soft state: information that times out (goes away) unless refreshed
- ARP is "plug-and-play":
  - nodes create their ARP tables without intervention from net administrator

Routing to another LAN

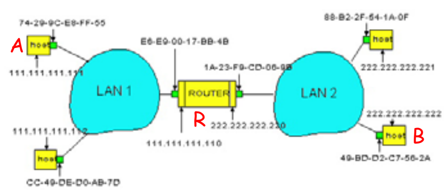
walkthrough: send datagram from A to B via R

assume A know's B IP address



Two ARP tables in router R, one for each IP network (LAN)

- A creates datagram with source A, destination B
- A uses ARP to get R's MAC address for 111.111.111.110
- A creates link-layer frame with R's MAC address as dest, frame contains A-to-B IP datagram
- A's data link layer sends frame
- R's data link layer receives frame
- R removes IP datagram from Ethernet frame, sees its destined to B
- R uses ARP to get B's physical layer address
- R creates frame containing A-to-B IP datagram sends to B



Chapter 5 outline

- 5.1 Introduction and services
- 5.2 Error detection and correction
- 5.3Multiple access protocols
- 5.4 LAN addresses and ARP
- 5.5 Ethernet
- 5.6 Hubs, bridges, and switches
- 5.7 Wireless links and LANs
- 5.8 PPP
- 5.9 ATM
- 5.10 Frame Relay

IEEE 802.11 Wireless LAN

- 802.11b
  - 2.4-5 GHz unlicensed radio spectrum
  - up to 11 Mbps
  - widely deployed, using base stations
- 802.11a
  - 5-6 GHz range
  - up to 54 Mbps
- 802.11g
  - 2.4-5 GHz range
  - up to 54 Mbps
- All use CSMA/CA for multiple access
- All have base-station and ad-hoc network versions

Base station approch

Wireless host communicates with a base station

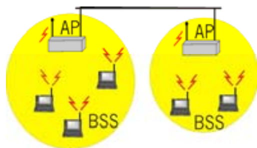
base station = access point (AP)

Basic Service Set (BSS) (a.k.a. "cell") contains:

wireless hosts

access point (AP): base station

BSS's combined to form distribution system (DS)



Ad Hoc Network approach

No AP (i.e., base station)

wireless hosts communicate with each other

to get packet from wireless host A to B may need to route through wireless hosts X,Y,Z

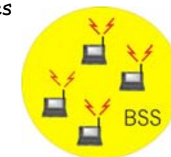
Applications:

"laptop" meeting in conference room, car

interconnection of "personal" devices

battlefield

IETF MANET
(Mobile Ad hoc Networks)
working group



IEEE 802.11: multiple access

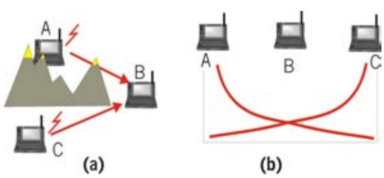
Collision if 2 or more nodes transmit at same time

CSMA makes sense:

get all the bandwidth if you're the only one transmitting

shouldn't cause a collision if you sense another transmission

Collision detection doesn't work: hidden terminal problem



IEEE 802.11 MAC Protocol: CSMA/CA

802.11 CSMA: sender

- if sense channel idle for **DISF** sec.

then transmit entire frame (no collision detection)

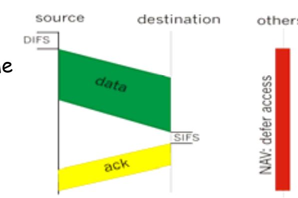
-if sense channel busy then binary backoff

802.11 CSMA receiver

- if received OK

return ACK after **SIFS**

(ACK is needed due to hidden terminal problem)



Collision avoidance mechanisms

Problem:

two nodes, hidden from each other, transmit complete frames to base station

wasted bandwidth for long duration !

Solution:

small reservation packets

nodes track reservation interval with internal "network allocation vector" (NAV)

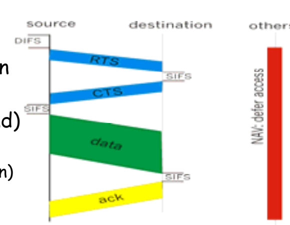
Collision Avoidance: RTS-CTS exchange

sender transmits short RTS (request to send) packet: indicates duration of transmission

receiver replies with short CTS (clear to send) packet

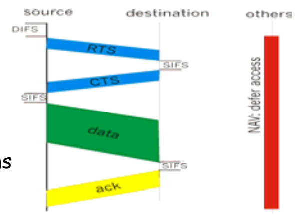
notifying (possibly hidden) nodes

hidden nodes will not transmit for specified duration: NAV



Collision Avoidance: RTS-CTS exchange

- RTS and CTS short:
  - collisions less likely, of shorter duration
  - end result similar to collision detection
- IEEE 802.11 allows:
  - CSMA
  - CSMA/CA: reservations
  - polling from AP



Chapter 5 outline

- 5.1 Introduction and services
- 5.2 Error detection and correction
- 5.3Multiple access protocols
- 5.4 LAN addresses and ARP
- 5.5 Ethernet
- 5.6 Hubs, bridges, and switches
- 5.7 Wireless links and LANs
- 5.8 PPP
- 5.9 ATM
- 5.10 Frame Relay

Point to Point Data Link Control

- one sender, one receiver, one link: easier than broadcast link:
  - no Media Access Control
  - no need for explicit MAC addressing
  - e.g., dialup link, ISDN line
- popular point-to-point DLC protocols:
  - PPP (point-to-point protocol)
  - HDLC: High level data link control (Data link used to be considered "high layer" in protocol stack!

PPP Design Requirements [RFC 1557]

- packet framing: encapsulation of network-layer datagram in data link frame
  - carry network layer data of any network layer protocol (not just IP) *at same time*
  - ability to demultiplex upwards
- bit transparency: must carry any bit pattern in the data field
- error detection (no correction)
- connection liveness: detect, signal link failure to network layer
- network layer address negotiation: endpoint can learn/configure each other's network address

PPP non-requirements

- no error correction/recovery
- no flow control
- out of order delivery OK
- no need to support multipoint links (e.g., polling)

Error recovery, flow control, data re-ordering all relegated to higher layers!

PPP Data Frame

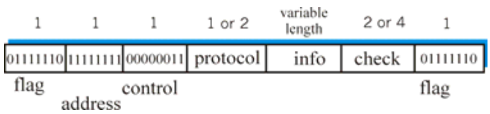
- Flag: delimiter (framing)
- Address: does nothing (only one option)
- Control: does nothing; in the future possible multiple control fields
- Protocol: upper layer protocol to which frame delivered (eg, PPP-LCP, IP, IPCP, etc)

1	1	1	1 or 2	variable length	2 or 4	1
01111110	11111111	00000011	protocol	info	check	01111110
flag	address	control				flag

PPP Data Frame

info: upper layer data being carried

check: cyclic redundancy check for error detection



Byte Stuffing

"data transparency" requirement: data field must be allowed to include flag pattern <01111110>

Q: is received <01111110> data or flag?

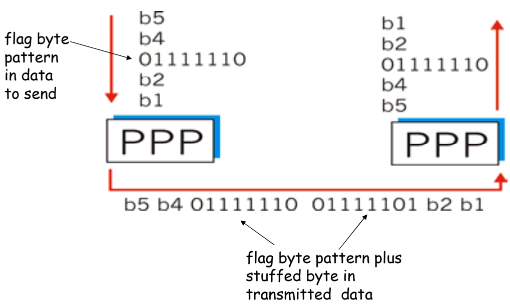
Sender: adds ("stuffs") extra < 01111110> byte after each < 01111110> *data* byte

Receiver:

two 01111110 bytes in a row: discard first byte, continue data reception

single 01111110: flag byte

Byte Stuffing



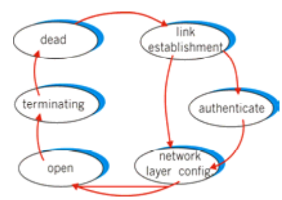
PPP Data Control Protocol

Before exchanging network-layer data, data link peers must

configure PPP link (max. frame length, authentication)

learn/configure network layer information

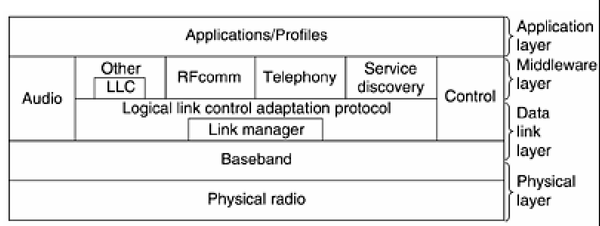
for IP: carry IP Control Protocol (IPCP) msgs (protocol field: 8021) to configure/learn IP address



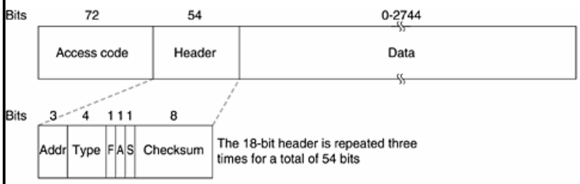
A word about Bluetooth

- Low-power, small radius, wireless networking technology
  - 10-100 meters
- omnidirectional
  - not line-of-sight infared
- Interconnects gadgets
- 2.4-2.5 GHz unlicensed radio band
- up to 721 kbps
- Interference from wireless LANs, digital cordless phones, microwave ovens:
  - frequency hopping helps
- MAC protocol supports:
  - error correction
  - ARQ
- Each node has a 12-bit address

BlueTooth Architecture



A Typicall BlueTooth Data Frame



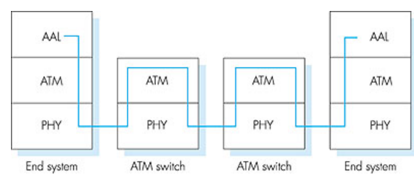
Chapter 5 outline

5.1 Introduction and services
5.2 Error detection and correction
5.3Multiple access protocols
5.4 LAN addresses and ARP
5.5 Ethernet
5.6 Hubs, bridges, and switches
5.7 Wireless links and LANs
5.8 PPP
5.9 ATM
5.10 Frame Relay

Asynchronous Transfer Mode: ATM

- **1990's/00 standard for high-speed** (155Mbps to 622 Mbps and higher) *Broadband Integrated Service Digital Network* architecture
- Goal: *integrated, end-end transport of carry voice, video, data*
  - meeting timing/QoS requirements of voice, video (versus Internet best-effort model)
  - "next generation" telephony: technical roots in telephone world
  - packet-switching (fixed length packets, called "cells") using virtual circuits

ATM architecture

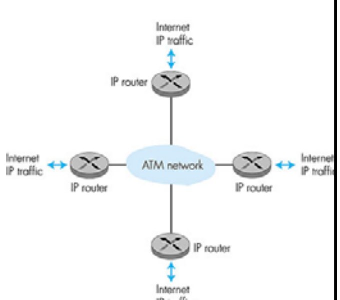


- adaptation layer: only at edge of ATM network
  - data segmentation/reassembly
  - roughly analagous to Internet transport layer
- ATM layer: "network" layer
  - cell switching, routing
- physical layer

ATM: network or link layer?

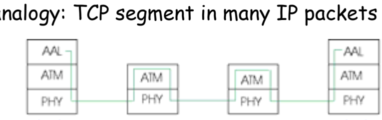
Vision: end-to-end transport: "ATM from desktop to desktop"
- ATM *is* a network technology

Reality: used to connect IP backbone routers
- "IP over ATM"
- ATM as switched link layer, connecting IP routers



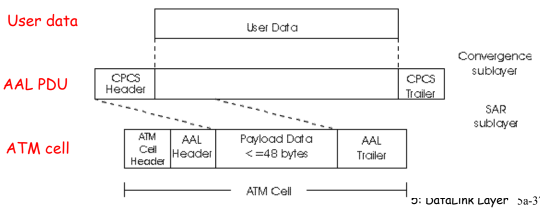
ATM Adaptation Layer (AAL)

- ATM **Adaptation Layer** (AAL): "adapts" upper layers (IP or native ATM applications) to ATM layer below
- AAL present **only in end systems**, not in switches
- AAL layer segment (header/trailer fields, data) fragmented across multiple ATM cells
  - analogy: TCP segment in many IP packets



ATM Adaptation Layer (AAL) [more]

Different versions of AAL layers, depending on ATM service class:
- AAL1: for CBR (Constant Bit Rate) services, e.g. circuit emulation
- AAL2: for VBR (Variable Bit Rate) services, e.g., MPEG video
- AAL5: for data (eg, IP datagrams)



AAL5 - Simple And Efficient AL (SEAL)

AAL5: **low overhead** AAL used to carry IP datagrams
- 4 byte cyclic redundancy check
- PAD ensures payload multiple of 48bytes
- large AAL5 data unit to be fragmented into 48-byte ATM cells

CPCS-PDU payload	PAD	Length	CRC
0-65535	0-47	2	4

ATM Layer

Service: transport cells across ATM network
- analagous to IP network layer
- very different services than IP network layer

Network Architecture	Service Model	Guarantees ? Bandwidth	Loss	Order	Timing	Congestion feedback
Internet	best effort	none	no	no	no	no (inferred via loss)
ATM	CBR	constant rate	yes	yes	yes	no congestion
ATM	VBR	guaranteed rate	yes	yes	yes	no congestion
ATM	ABR	guaranteed minimum	no	yes	no	yes
ATM	UBR	none	no	yes	no	no

ATM Layer: Virtual Circuits

VC transport: cells carried on VC from source to dest
- call setup, teardown for each call *before* data can flow
- each packet carries VC identifier (not destination ID)
- *every* switch on source-dest path maintain "state" for each passing connection
- link,switch resources (bandwidth, buffers) may be *allocated* to VC: to get circuit-like perf.

Permanent VCs (PVCs)
- long lasting connections
- typically: "permanent" route between to IP routers

Switched VCs (SVC):
- dynamically set up on per-call basis

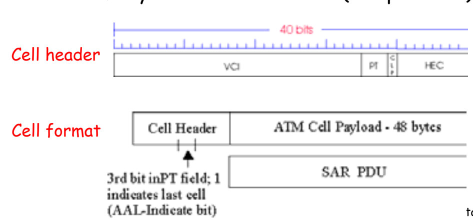
ATM VCs

Advantages of ATM VC approach:
- QoS performance guarantee for connection mapped to VC (bandwidth, delay, delay jitter)

Drawbacks of ATM VC approach:
- Inefficient support of datagram traffic
- one PVC between each source/dest pair) does not scale (N*2 connections needed)
- SVC introduces call setup latency, processing overhead for short lived connections

ATM Layer: ATM cell

- 5-byte ATM cell header
- 48-byte payload
  - Why?: small payload -> short cell-creation delay for digitized voice
  - halfway between 32 and 64 (compromise!)



ATM cell header

VCI: virtual channel ID

- will *change* from link to link thru net

PT: Payload type (e.g. RM cell versus data cell)

CLP: Cell Loss Priority bit

- CLP = 1 implies low priority cell, can be discarded if congestion

HEC: Header Error Checksum

- cyclic redundancy check

ATM Physical Layer (more)

Two pieces (sublayers) of physical layer:

- Transmission Convergence Sublayer (TCS): adapts ATM layer above to PMD sublayer below
- Physical Medium Dependent: depends on physical medium being used

TCS Functions:

- Header **checksum** generation: 8 bits CRC
- Cell **delineation**
- With "unstructured" PMD sublayer, transmission of **idle cells** when no data cells to send

ATM Physical Layer

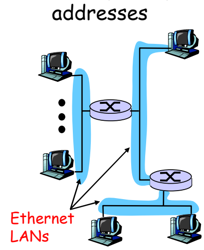
Physical Medium Dependent (PMD) sublayer

- **SONET/SDH:** transmission frame structure (like a container carrying bits);
  - bit synchronization;
  - bandwidth partitions (TDM);
  - several speeds: OC3 = 155.52 Mbps; OC12 = 622.08 Mbps; OC48 = 2.45 Gbps, OC192 = 9.6 Gbps
- **TI/T3:** transmission frame structure (old telephone hierarchy): 1.5 Mbps/ 45 Mbps
- **unstructured:** just cells (busy/idle)

IP-Over-ATM

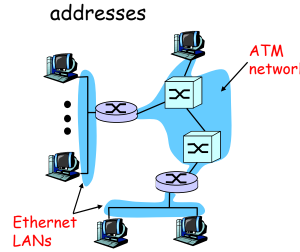
Classic IP only

- 3 "networks" (e.g., LAN segments)
- MAC (802.3) and IP addresses



IP over ATM

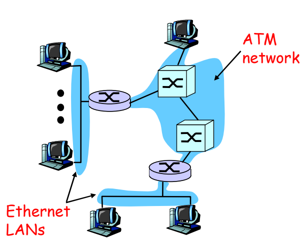
- replace "network" (e.g., LAN segment) with ATM network
- ATM addresses, IP addresses



IP-Over-ATM

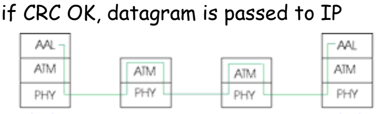
Issues:

- IP datagrams into ATM AAL5 PDUs
- from IP addresses to ATM addresses
  - just like IP addresses to 802.3 MAC addresses!



Datagram Journey in IP-over-ATM Network

- at Source Host:
  - IP layer maps between IP, ATM dest address (using ARP)
  - passes datagram to AAL5
  - AAL5 encapsulates data, segments cells, passes to ATM layer
- ATM network: moves cell along VC to destination
- at Destination Host:
  - AAL5 reassembles cells into original datagram
  - if CRC OK, datagram is passed to IP



Chapter 5 outline

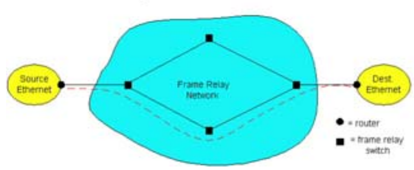
- 5.1 Introduction and services
- 5.2 Error detection and correction
- 5.3Multiple access protocols
- 5.4 LAN addresses and ARP
- 5.5 Ethernet
- 5.6 Hubs, bridges, and switches
- 5.7 Wireless links and LANs
- 5.8 PPP
- 5.9 ATM
- 5.10 Frame Relay

Frame Relay

Like ATM:
- wide area network technologies
- Virtual-circuit oriented
- origins in telephony world
- can be used to carry IP datagrams
  - can thus be viewed as link layers by IP protocol

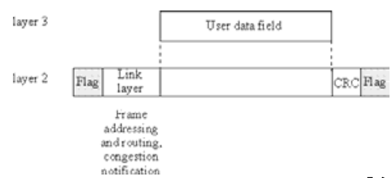
Frame Relay

- Designed in late '80s, widely deployed in the '90s
- Frame relay service:
  - no error control
  - end-to-end congestion control



Frame Relay (more)

- Designed to **interconnect** corporate customer LANs
  - typically permanent VC's: "**pipe**" carrying aggregate traffic between two routers
  - switched VC's: as in ATM
- corporate customer **leases** FR service from public Frame Relay network (eg, Sprint, ATT)



Frame Relay (more)

flags	address	data	CRC	flags

- Flag bits, 01111110, delimit frame
- address:
  - 10 bit VC ID field
  - 3 congestion control bits
    - FECN: forward explicit congestion notification (frame experienced congestion on path)
    - BECN: congestion on reverse path
    - DE: discard eligibility

Frame Relay -VC Rate Control

- Committed Information Rate (CIR)
  - defined, "guaranteed" for each VC
  - negotiated at VC set up time
  - customer pays based on CIR
- DE bit: Discard Eligibility bit
  - Edge FR switch measures traffic rate for each VC; marks DE bit
  - DE = 0: high priority, rate compliant frame; deliver at "all costs"
  - DE = 1: low priority, eligible for congestion discard

Frame Relay - CIR & Frame Marking

- **Access Rate**: rate **R** of the access link between **source router** (customer) and **edge FR switch** (provider); $64\text{Kbps} < \mathbf{R} < 1{,}544\text{Kbps}$
- Typically, **many VCs** (one per destination router) multiplexed on the same access trunk; each VC has own **CIR**
- Edge FR switch **measures** traffic rate for each VC; it **marks** (ie DE = 1) frames which **exceed** CIR (these may be later dropped)
- Internet's more recent differentiated service uses similar ideas

Chapter 5: Summary

- principles behind data link layer services:
  - error detection, correction
  - sharing a broadcast channel: multiple access
  - link layer addressing, ARP
- link layer technologies: Ethernet, hubs, bridges, switches,IEEE 802.11 LANs, PPP, ATM, Frame Relay
- journey down the protocol stack now *OVER!*
  - next stops: multimedia, security, network management