Lecture 24

- Section 5.6
  - The Internet Control Message Protocol (ICMP)
- Sections 6.1 and 6.2
  - Introduction to the data link layer and its services
  - Error detection and correct @ data link layer

Chapter 5: Network Layer

5. 1 Introduction

5.2 Routing algorithms

5.2.1 link-state routing algorithm

5.2.2 distance vector routing

5.3 Intra-Autonomous System (AS) routing: OSPF

5.4 Routing among Autonomous Systems (ISPs)

5.6 The Internet Message Control Protocol (ICMP)

ICMP: Internet Control Message Protocol

- used by hosts & routers to communicate network-level information
  - error reporting: unreachable host, network, port, protocol
  - echo request/reply (used by ping)
- network-layer "above" IP:
  - ICMP msgs carried in IP datagrams
- ICMP message: type, code plus first 8 bytes of IP datagram causing error

Type	Code	description
0	0	echo reply (ping)
3	0	dest. network unreachable
3	1	dest host unreachable
3	2	dest protocol unreachable
3	3	dest port unreachable
3	6	dest network unknown
3	7	dest host unknown
4	0	source quench (congestion control - not used)
8	0	echo request (ping)
9	0	route advertisement
10	0	router discovery
11	0	TTL expired
12	0	bad IP header

Traceroute and ICMP

- Source sends series of UDP segments to dest
  - first has TTL =1
  - second has TTL=2, etc.
  - unlikely port number
- When nth datagram arrives to nth router:
  - router discards datagram
  - and sends to source an ICMP message (type 11, code 0)
  - ICMP message includes name of router & IP address
- when ICMP message arrives, source calculates RTT
- traceroute does this 3 times

Stopping criterion

- UDP segment eventually arrives at destination host
- destination returns ICMP "port unreachable" packet (type 3, code 3)
- when source gets this ICMP, stops.

What have we covered in Chapter 5?

- Principles behind network control plane:
  - traditional routing algorithms
- instantiation, implementation in the Internet:
  - OSPF, DV (RIP), BGP
  - Internet Control Message Protocol: ICMP

Chapter 6: The Data Link Layer & LANs

Chapter objectives:

- understand principles behind data link layer services:
  - error detection, correction
  - sharing a broadcast channel: multiple access
  - link layer addressing
  - reliable data transfer: *done (uses ARQ, which is the same technique presented in Chapter 3)*
- instantiation and implementation of various link layer technologies

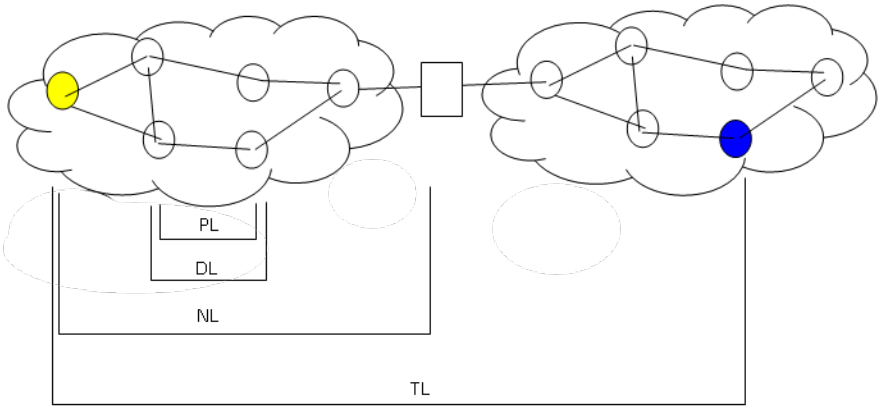
1

Link Layer

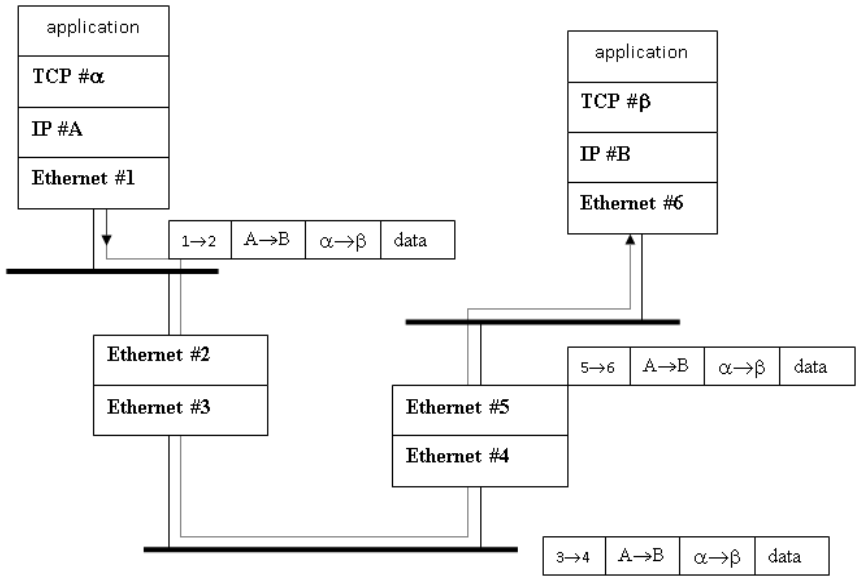
6.1 Introduction and services

2

Scope of layers operation



3

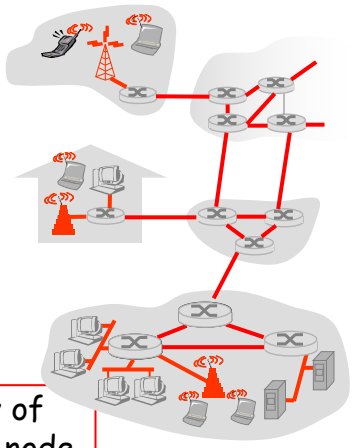


4

Link Layer (layer 2): Introduction

Terminology:

- hosts and routers are nodes
- communication channels that connect adjacent nodes along communication path are links
  - wired links
  - wireless links
  - LANs
- layer-2 packet is a frame, encapsulates a layer 3 packet



data-link layer has responsibility of transferring datagram from one node to *physically adjacent* node over a link

5

Link layer: context

- different links can be implemented using different technologies
  - e.g, first link is twisted pair, intermediate links are fiber, last link is wireless
- different links can use different data link layer protocols
  - e.g., Ethernet on first link, frame relay on intermediate links, 802.11 on last link
- each link protocol provides different services
  - e.g., may or may not provide rdt over link

6

Link Layer Services

- *framing, addressing, link access:*
  - encapsulate datagram into frame, adding header, trailer
  - "MAC" addresses used in frame headers to identify source, dest on the same subnet
    - different from IP address!
  - channel access if shared medium
- *reliable delivery between adjacent nodes*
  - we learned how to do this already (chapter 3)!
  - seldom used on low bit-error link (fiber, some twisted pair)
  - wireless links: high error rates
    - Q: why both link-level and end-end reliability?

7

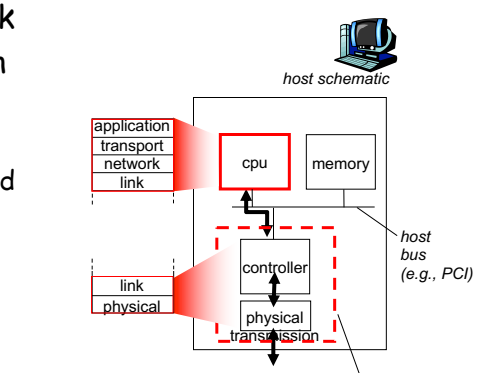
Link Layer Services (more)

- *error detection*:
  - errors caused by signal attenuation, noise.
  - receiver detects presence of errors:
    - signals sender for retransmission; or drops frame
- error correction:
  - by using ARQ protocols; or
  - receiver identifies *and corrects* bit error(s) without resorting to retransmission
- *link layer flow control:*
  - pacing between adjacent sending and receiving nodes
- *half-duplex and full-duplex*
  - with half duplex, nodes at both ends of link can transmit, but not at same time

8

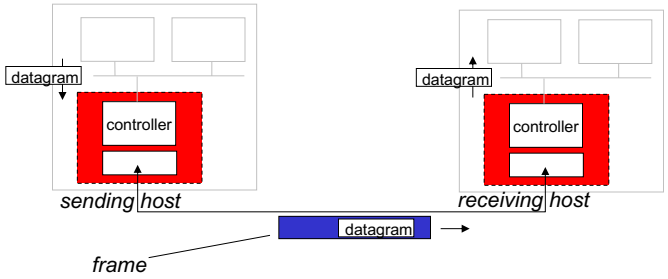
Where is the link layer implemented?

- in each and every host that connects to network
- link layer implemented in "adaptor" (aka *network interface card* NIC)
  - Ethernet card, 802.11 card (built in, USB, or PCMCI card) implements link, physical layer
- attaches into host's system buses
- combination of hardware software, firmware



9

Adaptors Communicating



- sending side:
  - encapsulates datagram in frame
  - adds error checking bits, rdt, flow control, etc.
  - uses an access protocol to send protocol on medium
- receiving side
  - looks for errors, rdt, flow control, etc
  - extracts datagram, passes to upper layer at receiving side

10

Link Layer

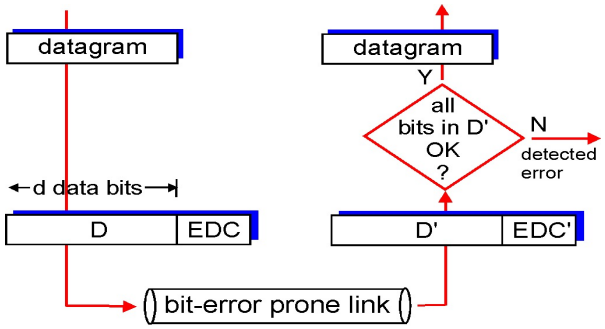
6.1 Introduction and services

6.2 Error detection and correction

11

Error Detection

D = Data protected by error checking, may include header fields
EDC= Error Detection and Correction bits (redundancy)



Error detection not 100% reliable!

- protocol may miss some errors, but rarely
- larger EDC field yields better detection and correction

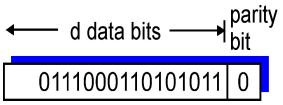
12

Parity Checking

Single Bit Parity:

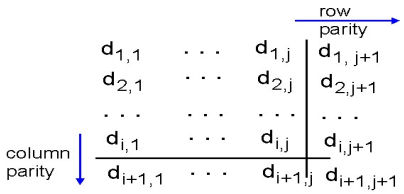
Parity bit = XNOR of all data bits (odd parity) – even parity can be used

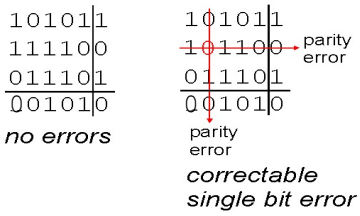
Detect single bit errors



Two Dimensional Bit Parity:

Detect *and correct* single bit errors





13

Internet checksum (review)

Goal: detect "errors" (e.g., flipped bits) in transmitted packet (note: used at transport layer *only*)

Sender:

- treat segment contents as sequence of 16-bit integers
- checksum: addition (1's complement sum) of segment contents
- sender puts checksum value into segment checksum field

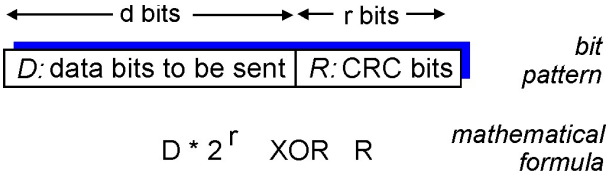
Receiver:

- compute checksum of received segment
- check if computed checksum equals checksum field value:
  - NO - error detected
  - YES - no error detected. *But maybe errors nonetheless?*

14

Checksumming: Cyclic Redundancy Check

- view data bits, D, as a binary number
- choose r+1 bit pattern (generator), G
- goal: choose r CRC bits, R, such that
  - <D,R> exactly divisible by G (modulo 2)
  - receiver knows G, divides <D,R> by G. If non-zero remainder: error detected!
  - can detect all burst errors less than r+1 bits
- widely used in practice (Ethernet, 802.11 WiFi, ATM)



15

CRC Example

Want:

$D \cdot 2^r$ XOR R = nG

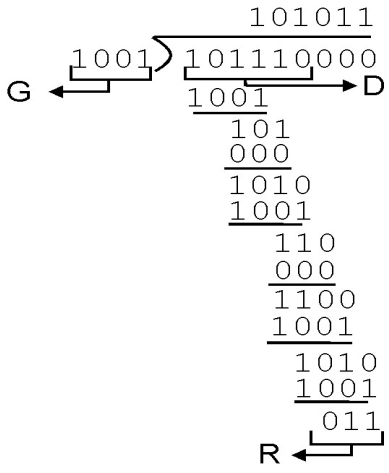
equivalently:

$D \cdot 2^r$ = nG XOR R

equivalently:

if we divide $D \cdot 2^r$ by G, want remainder R

$$R = \text{remainder}\left[\frac{D \cdot 2^r}{G}\right]$$



16