CPSC 317 COMPUTER NETWORKING

Module 7: Link Layer – Day 1 – Introduction, Error Detection

1

LEARNING GOALS

Link Layer

- Explain the purpose of the link layer, and the four types of services the link layer provides
- Know the general structure of link layer "frames"
- Understand link layer addressing: MAC addresses
- Explain why the link layer may use "error correction"
- Know three techniques for error detection: parity (1D and 2D), checksum, CRC
- Understand the basic types of media (point-to-point, broadcast) and what is meant by "access control"
- Know the basic differences between a switch and a router

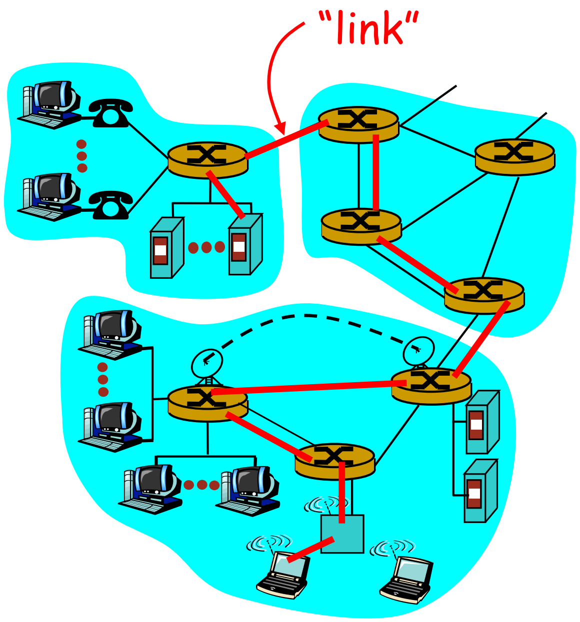
READING

- Reading: 6.1, 6.2

LINK LAYER: INTRODUCTION

Some terminology:

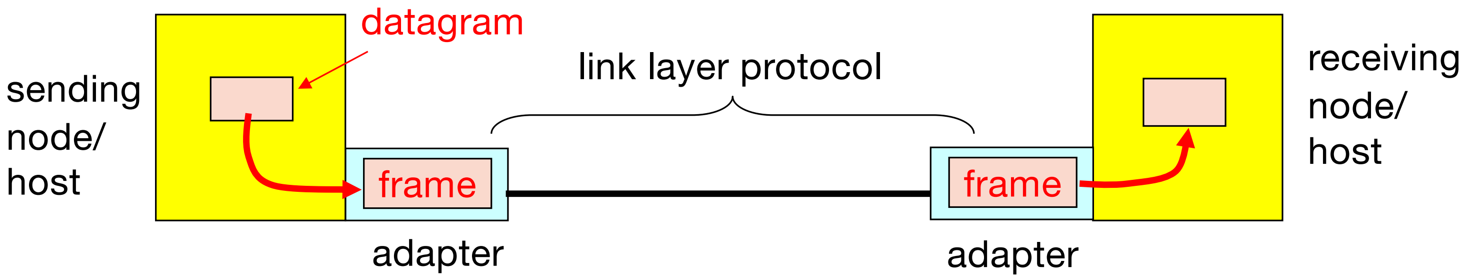
- hosts and routers are **nodes**
- communication channels that connect adjacent nodes along communication path are **links**
  - wired links
  - wireless links
  - LANs
- link layer packet is a **frame,** encapsulates datagram (network layer packet)



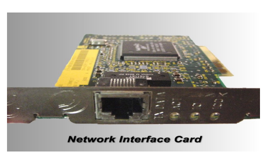
The **link layer** has responsibility of transferring a datagram from one node to an adjacent node over a link (physical medium)

PHYSICAL PIECES

ADAPTORS COMMUNICATING



- link layer implemented in "adapter", aka Network Interface Card (NIC)
  - Ethernet card, 802.11 card
  - Often built-in

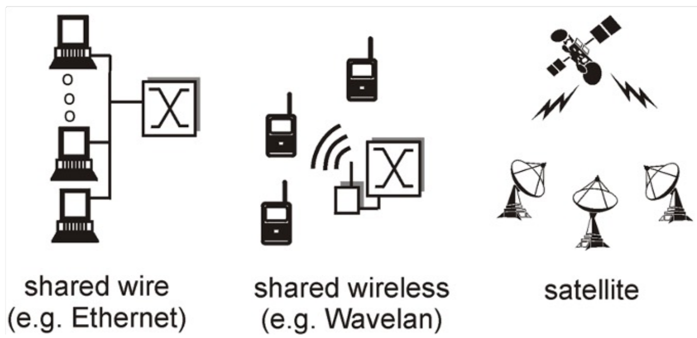


- one adapter on each side
- adapter is semi-autonomous
- link & physical layers

MULTIPLE ACCESS LINKS AND PROTOCOLS

Two types of "links":

- point-to-point
  - PPP for dial-up access
  - point-to-point link between two routers
- broadcast (shared wire or medium)
  - traditional Ethernet
  - upstream fiber, coax, or Hybrid Fiber Coax
  - 802.11 wireless LAN



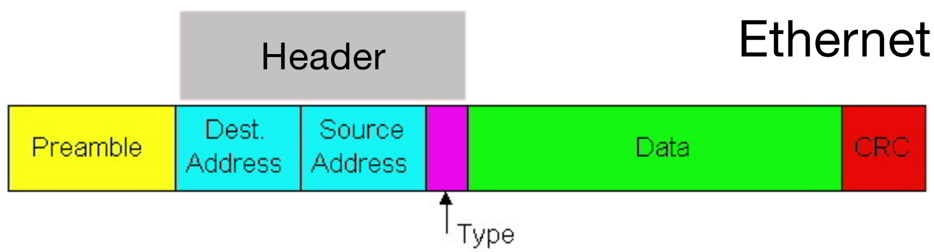
LINK LAYER SERVICES

- Framing (or packetizing):
  - encapsulate datagram into frame, adding header, trailer
  - media access control "MAC" addresses used to identify source, dest
    - different from IP addresses!
  - broadcast medium (to whom, from whom)
- Link Access:
  - MAC protocol (media access control)
  - with half duplex, multiple nodes on a link can transmit, but not at the same time

LINK LAYER SERVICES (MORE)

- Reliable delivery (retransmission):
  - seldom used on low bit error links (fiber, twisted pair)
  - more often used on wireless links: high error rates
    - Q: Why link-level reliability when IP has no reliability?
- Error Detection and Correction:
  - errors caused by signal attenuation, noise
  - receiver detects presence of errors and drops frame
  - receiver identifies *and corrects* bit error(s)

LINK LAYER FRAME (802.XXX)



- Ethernet header: 14 bytes
  - Dest and Source MAC addresses: 6 bytes each
  - EtherType: 2 bytes
- Minimum transmission frame size: 64 bytes
- Ethernet payload (data): 46-1500 bytes

MAC ADDRESS

- 48 bits --- 6 bytes
- Given in hexadecimal
- Locally administered
- **88-B2-2F-54-1A-0F**

- Broadcast address:
  - FF-FF-FF-FF-FF-FF

MAC VERSUS IP

- 32-bit (or 128-bit) IP address:
  - Used to get datagram to destination IP subnet
  - Must be unique in the world
- 48-bit MAC (or LAN or physical or Ethernet) address:
  - Used to get frame from one interface to another physically-connected interface (same network)
  - MAC address (for most LANs) burned in the adapter ROM
  - Generally unique in the world, but must be unique in the network

CLICKER QUESTION

If we used MAC addresses rather than IPv4 addresses for the network layer, how big would the forwarding tables in routers need to be?

A. About the same size as they are when using IPv4 addresses

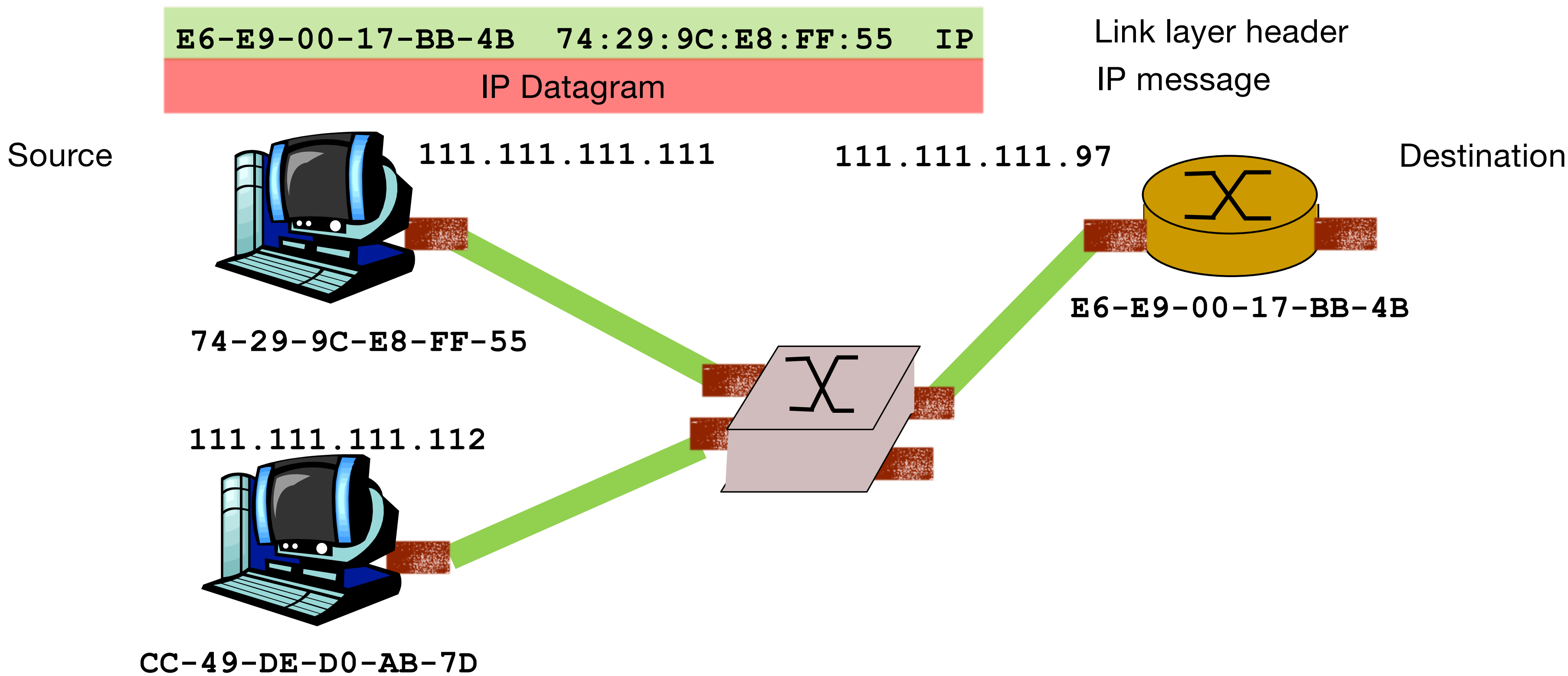
B. Much larger than they are when using IPv4 addresses

C. Much smaller than they are when using IPv4 addresses

MAC ADDRESS ASSIGNMENT

- MAC address allocation administered by IEEE
- Manufacturer buys portion of MAC address space (to assure uniqueness)
- Analogy:
  - MAC address: like Social Insurance Number
    - never changes, only has local meaning
  - IP address: like postal address
    - changes when you move, has global meaning
- MAC flat address is portable
  - can move LAN card from one LAN to another
- IP hierarchical (network/host) address is not portable
  - depends on IP subnet to which node is attached

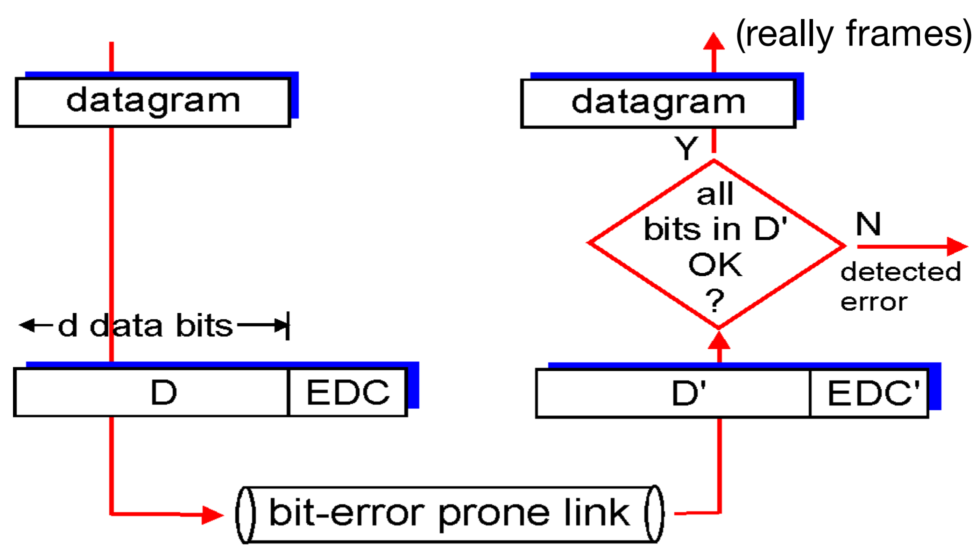
SENDING AN IP DATAGRAM



ERROR DETECTION AND CORRECTION

ERROR DETECTION

- EDC = Error Detection and Correction bits (redundancy)
- D = Data protected by error checking, may include header fields
- Error detection not 100% reliable!
  - protocol may miss some errors, but rarely
  - larger EDC field yields better detection and correction



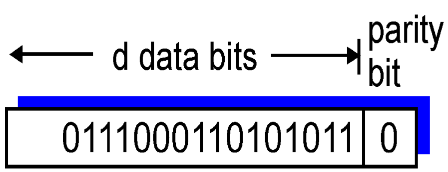
SINGLE BIT PARITY

1 0 0 1 0 0 1 0 0 0 1 0 0 0 1 0 0 0 1 1 parity ?

1

Even parity: add on a parity bit to make the parity even

Detect single bit errors



CLICKER QUESTION

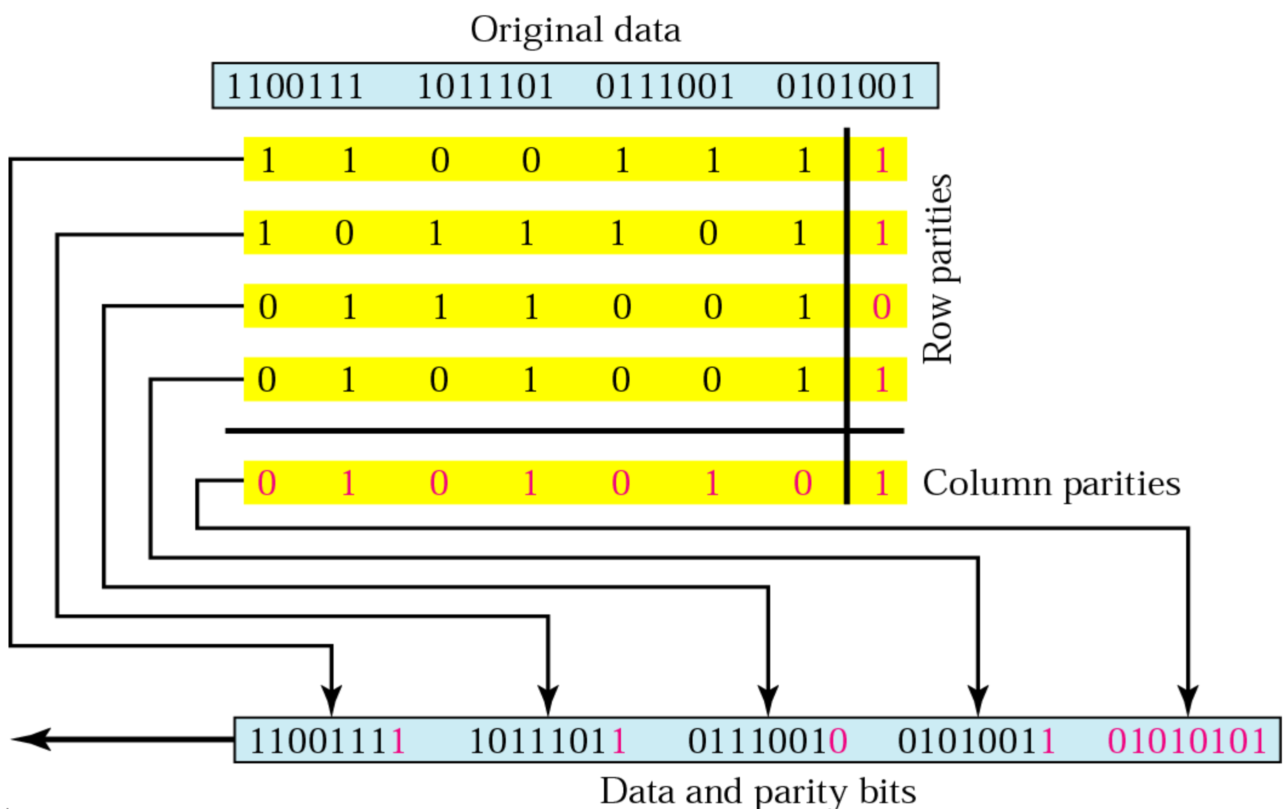
Will a single parity bit be able to detect when two bits have been erroneously changed?

A. Yes

B. No

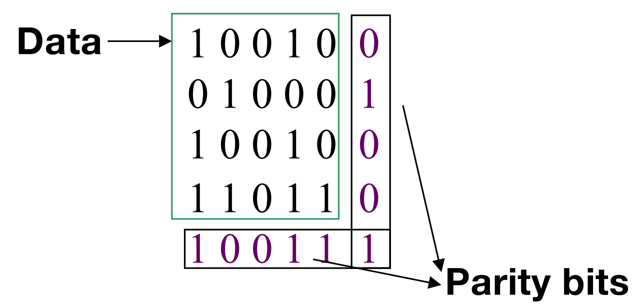
C. Sometimes

TWO DIMENSIONAL PARITY



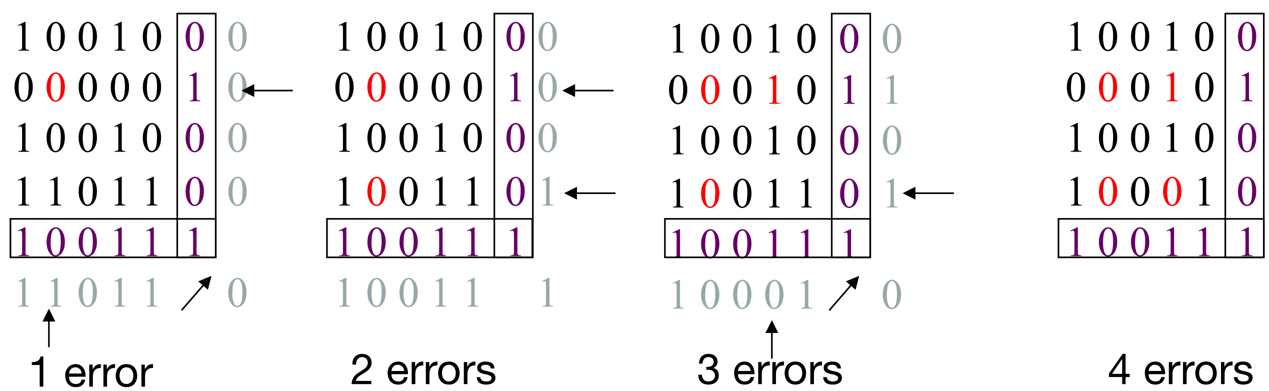
2-D EDC

1. Data blocks are organized into table
2. Last column: check bits for rows
3. Last row: check bits for columns
4. Can **detect** and **correct single** bit error



Can detect one, two, three errors,
But NOT all four errors.

Red bits are errors



CHECKSUMS

Goal: detect "errors" (e.g., flipped bits) in transmitted packet

Sender:

- Computes some function on the data
- Appends the checksum value to the data
- Sends the data and checksum

Receiver:

- Computes the same function on the received data
- Check if computed checksum equals received checksum value
  - NO - error detected
  - YES - no error detected
- Not all errors can be detected

INTERNET CHECKSUM

- Treat the data as a sequence of 16-bit integers
- Function: addition (1's complement sum, carry out added back in) of all these 16 bit integers
- Checksum is the 1's complement of the computed value (flip all the bits)
- Verifying is computing the same function over the data and checksum (correct if 0)

CYCLIC REDUNDANCY CHECK (CRC)

A BETTER WAY TO DETECT ERRORS

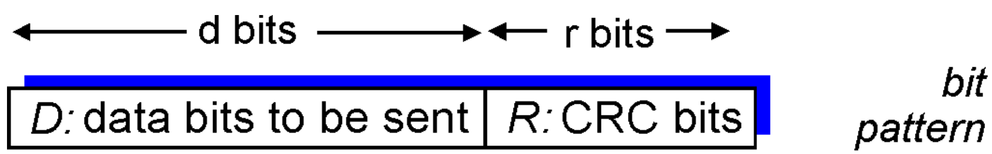
- Certain kinds of errors are observed frequently “in the wild”
  - Burst errors – a string of several bits in a row that are incorrect or all 0s or all 1s
- CRCs of length 32 can detect every burst error of length 33 or less and burst errors greater than 33 with probability 1-1/2^32 (99.99999997%)
- CRCs can’t correct errors

CYCLIC REDUNDANCY CHECK

- Parameterized by constants G and r
- r + 1 is the length of G (r = 8, 12, 16, 32)
- G is the generator (an arbitrary bit pattern, but some are better than others)
- The sender wants to send D
- The sender chooses r CRC bits, R, such that
  - <D,R> is exactly divisible by G (modulo 2)
- The receiver knows G, divides <D,R> by G. If the remainder is non-zero an error is detected!

CRC

- The computation of R and the division by G can be computed quickly in hardware
- Uses only XOR and shift



CRC Example (3-bit CRC)

Want:

$D \cdot 2^r \text{ XOR } R = nG$

$r = 3$ bits

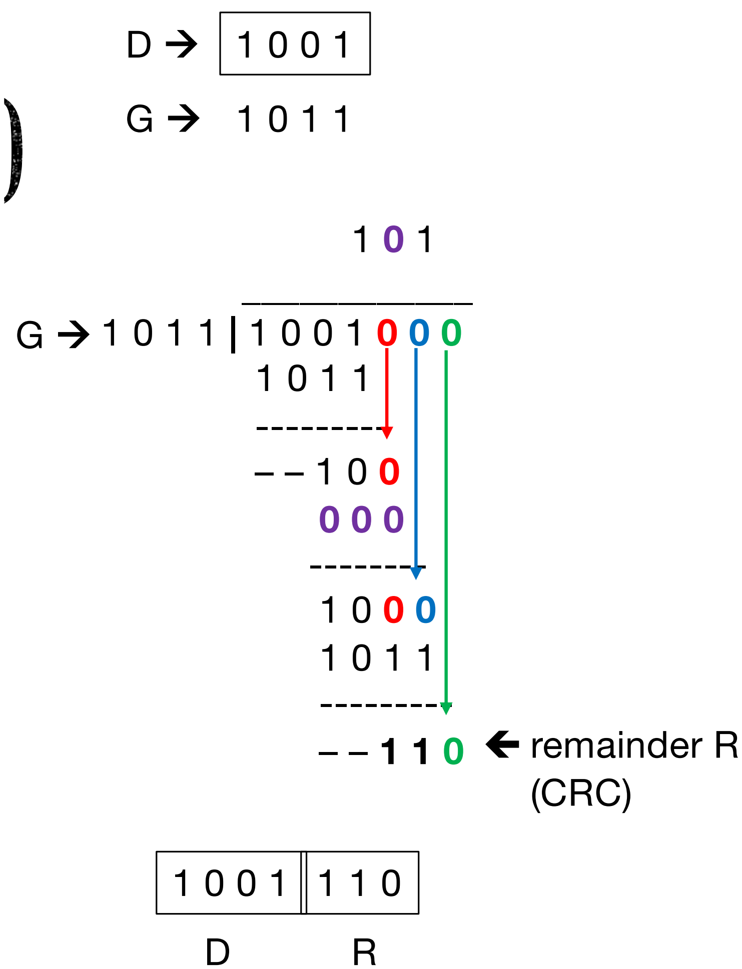
equivalently:

$D \cdot 2^r = nG \text{ XOR } R$

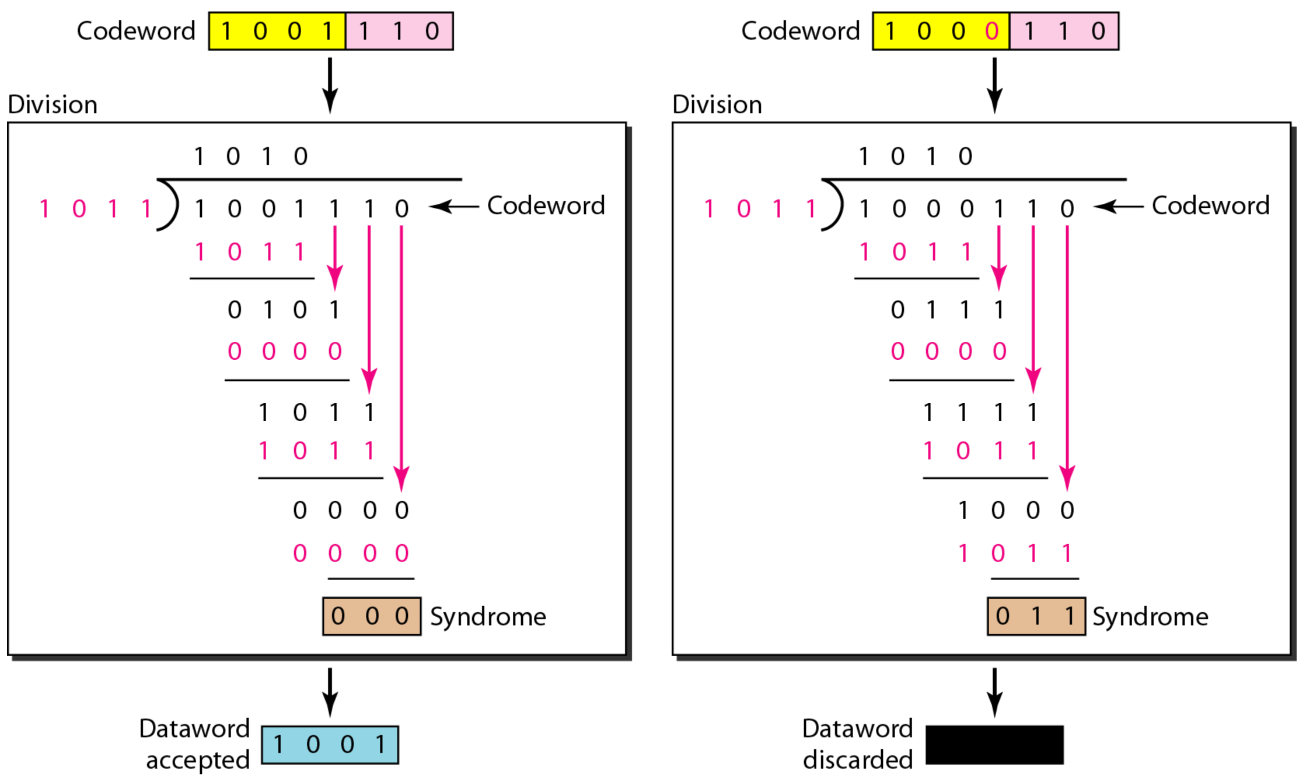
equivalently:

If we divide $D \cdot 2^r$ by G

we want remainder R



CRC VERIFICATION



INCLASS ACTIVITY

- ICA71