Announcements

- Reading Chapters 15
  - problems:
- Midterm #2
  - was returned (see end of notes for grade info)

copyright 1996 Jeffrey K. Hollingsworth

Monitoring

- Record (log) significant events
  - attempts to login to the system
  - changes to selected files or directories
- Possible to compromise the log
  - the user or software breaking in could delete all or part of the logs
  - could record logs to non-erasable storage
    - have a line printer attached to the machine
    - use WORM drives

copyright 1996 Jeffrey K. Hollingsworth

Encryption: protecting info from being read

- Given a message m
  - use a key k, and function E_k to compute $E_k(m)$
  - store or send only $E_k(m)$
  - use a second second key k and function $D_{k'}$ such that
    - $D_{k'}(E_k(m)) = m$
  - E_k and $D_{k'}$ need not be kept a secrete
- If k=k' it's called private key encryption
  - need to keep k secret
  - example DES
- if k != k', it's called public key encryption
  - need only keep one of them secret
  - if k' is secret, anyone can send a private message
  - if k is secret, it is possible to "sign" a message
  - still need a way to authenticate k or k' for a user
  - example RSA

copyright 1996 Jeffrey K. Hollingsworth

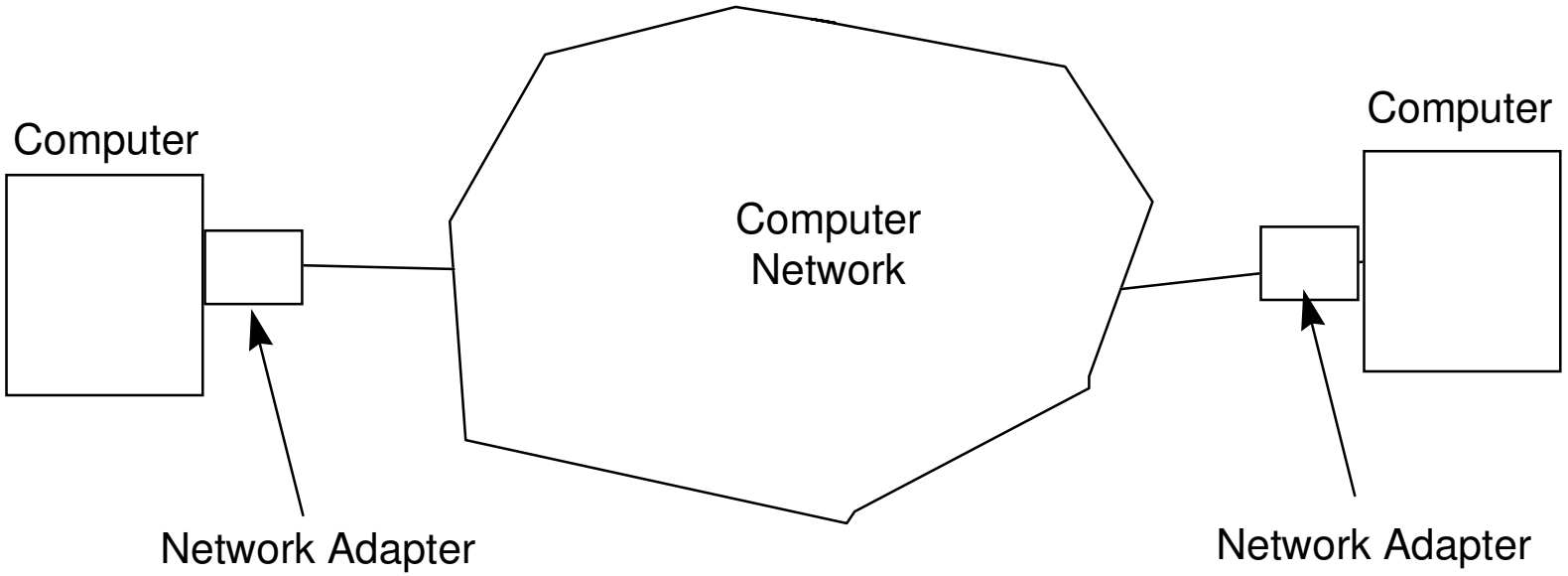
Networks are divided into layers

- ISO - seven layer reference model
  - Application (end application)
    - firewalls work at this layer
  - Presentation (encryption or compression)
  - Session (end-to-end connections)
  - Transport (splitting data into packets)
  - Network (routing packets)
    - routers work at this later
  - Link (moves frames and detects errors)
    - bridges at this layer
  - Physical (EE type stuff)
- TCP/IP - three layer model
  - link, network, transport/session/presentation

copyright 1996 Jeffrey K. Hollingsworth

Networks

- Communication channels between semi-autonomous computers
- Attached to host system by an adapter



copyright 1996 Jeffrey K. Hollingsworth

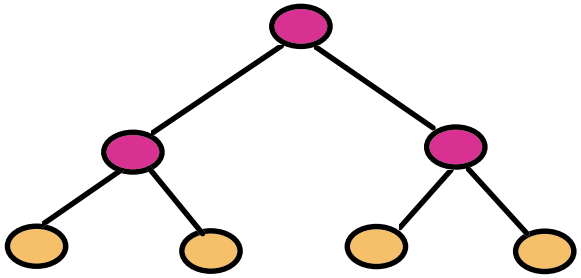
Networks

- Topology
  - Fully connected - link between all sites
  - Partially connected
    - links between subset of sites
    - can be an arbitrary graph
  - Hierarchical networks
    - network topology looks like a tree
    - internal nodes route messages between different subtrees
    - if an internal node fails, children can not communicate with each other
    - star network - hierarchical network with single internal node

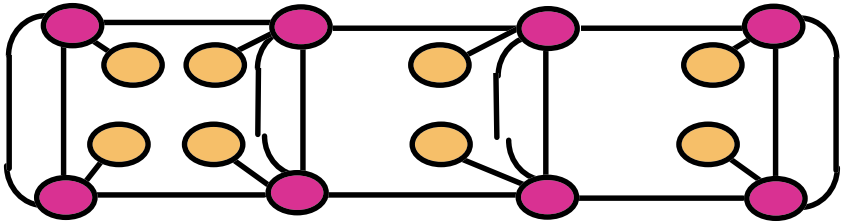
copyright 1996 Jeffrey K. Hollingsworth

Network Topologies

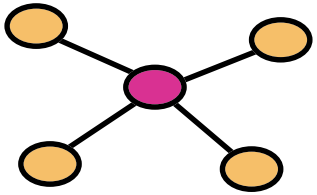
- Tree (TMC CM-5)



- Mesh
  - 2-d Intel Parago
  - 3-d Cray T3E



- Star (Ethernet 10Base-, physical only)



copyright 1996 Jeffrey K. Hollingsworth

Midterm #2

- Solutions are on the class web page
- Overall results
  - average 60
  - min 22
  - max 94
  - standard deviation 17
- Per Problem results:

	1	2	3	4	5	6
Avg	11	6	14	9	5	14
Min	2	0	0	0	0	4
Max	14	9	23	15	15	20

copyright 1996 Jeffrey K. Hollingsworth