mputer Networks

Hasan Cam

Computer Engineering Department
King Fahd University of Petroleum & Minerals
cam@ccse.kfupm.edu.sa

December 1997

Topics Covered in this Session

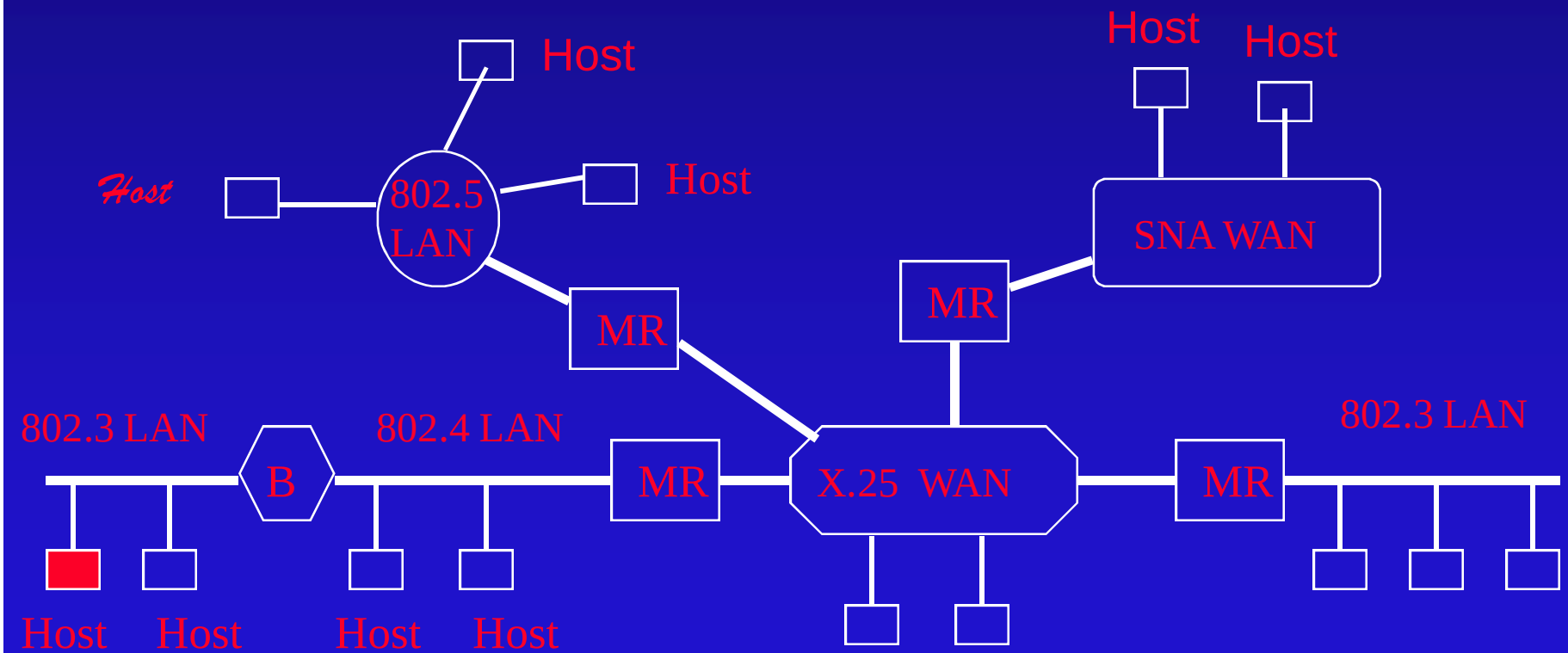
- Interconnection of Networks
- Transport Layer

Internetworking

- Users want to share resources of other networks
- **Internetworking**: the interconnection of distinct networks for providing communication and effective sharing of resources among devices
  - » cables and physical interfaces (physical connectivity)
  - » protocols, management and applications needed to support user (interworking)

raction of Different Networks

1. LAN-to-LAN 2. LAN-to-WAN 3. WAN-to-WAN
4. LAN-to-WAN-to-LAN



B: Bridge MR: Multi-protocol router

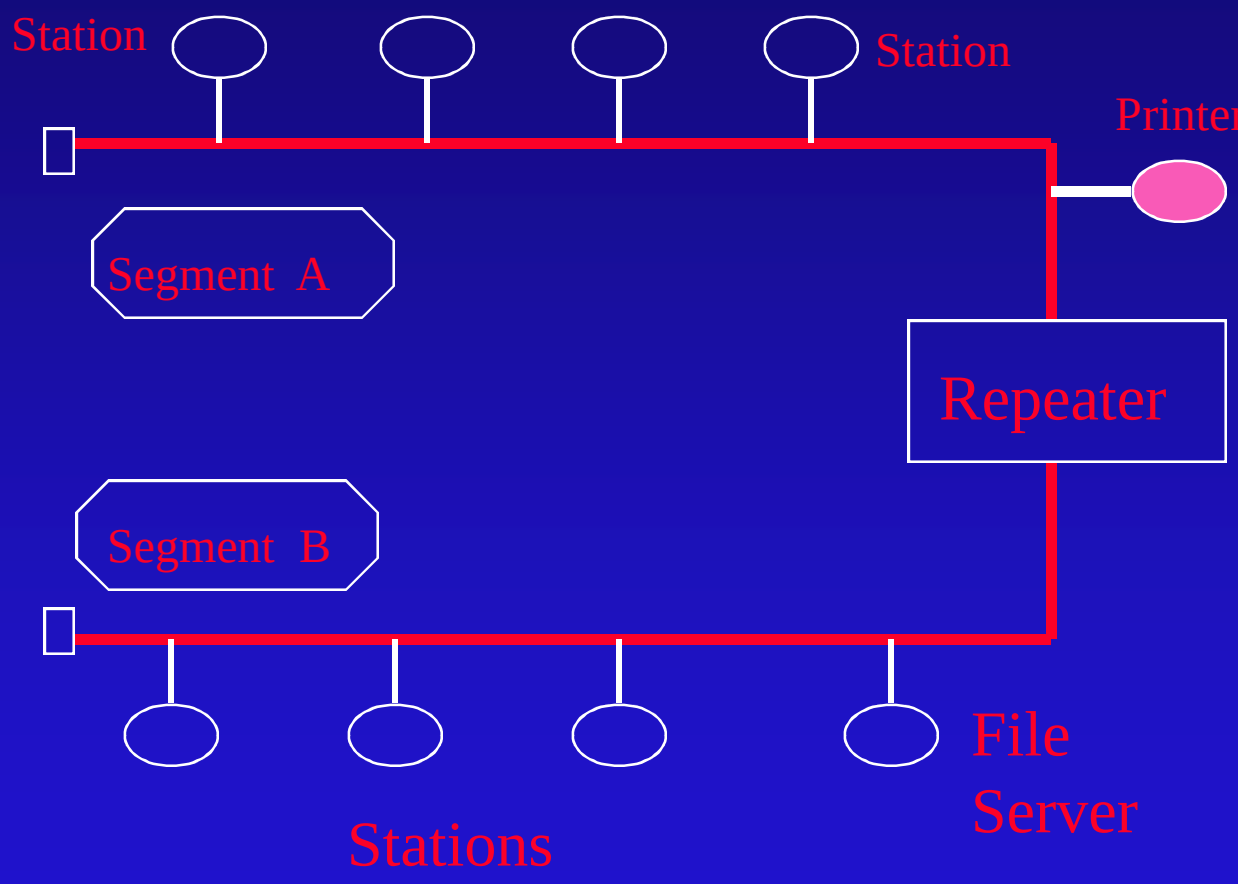
Relays

- Devices that interconnect LANs are known as relays and operate at one layer of OSI model
- There are four common types of relays
  - » **Repeater**: at physical layer (bits)
  - » **Bridge**: at data-link layer (frames)
  - » **Router**: at network layer (packets)
  - » **Gateways**: at transport and higher layers (protocols)

Repeater

- overcomes restrictions caused by single segment usage such as number of users, cable length
- amplifies or regenerates weak signals (copy bits)
- extends cable length
- can connect LANs of a similar type but which use different media (e.g., connect a 10BASE5 (coax) and 10BASEF (fiber))
- provides simple connection between adjacent LANs at the expense of increased network congestion

Repeaters for a Multi-segment LAN



Bridge

- interconnects two or more LANs (either similar or dissimilar) at the MAC level
- capable of deciding whether or not to forward frame
- creates an extended network and keeps local traffic off
- can make minor changes to frame header
- does not inspect or modify the network layer packets inside frames

Router

- provides a more intelligent service
  - » makes a decision as to the best way to deliver a packet from source to destination
  - » may fragment packets to meet packet size requirements of LANs
  - » are slower than bridges
- permits translation between different address domains such as addresses of IEEE 802 LAN and X.25

Gateway

- connect end-systems whose host protocols have varying degrees of difference
- Transport gateways make a connection between two networks at the transport layer.
- Application gateways connect two parts of an application in the application layer. For instance, sending email between two machines using different mail formats

Routers versus Bridges

- Addressing
  - » Routers are explicitly addressed. (Every router on the Internet has an IP address).
  - » Bridges are not addressed: stations are unaware of their existence.
- Availability
  - » Routers can handle failures in links, stations, and other routers
  - » Bridges use only source and destination address. The MAC layer does not guarantee delivery of frames

Routers versus Bridges (cont.)

- Message Size
  - » Routers can perform fragmentation on packets and thus handle different packet sizes.
  - » Bridges cannot do fragmentation and should not forward a frame which is too big for the next LAN.
- Forwarding
  - » Routers forward a message to a specific destination.
  - » Bridges forward a message to an outgoing network.
- Priority
  - » Routers can treat packets according to priorities
  - » Bridges treat all packets equally.

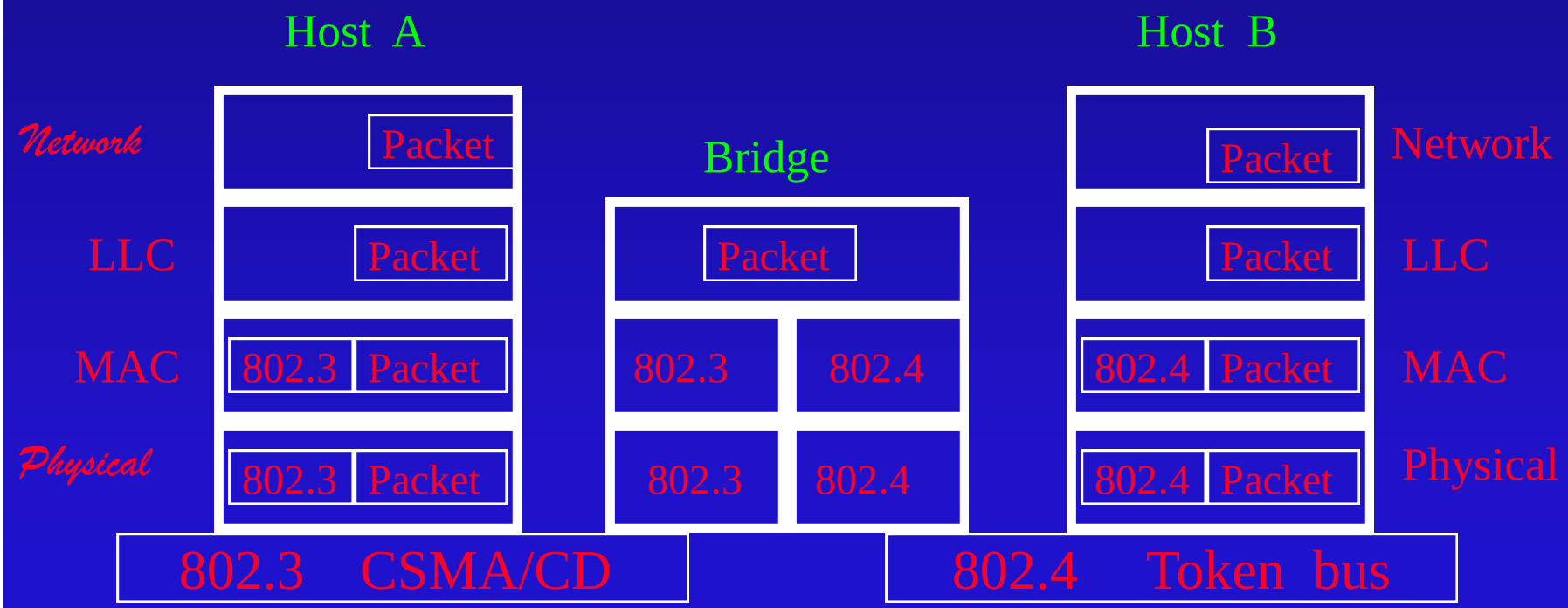
Routers versus Bridges (cont.)

- Error Rate
  - » Network layers have error-checking algorithms that examines each received packet. Erroneous packets are discarded.
  - » The MAC layer provides a very low undetected bit error rate by means of the frame check sequence (FCS) incorporated into a frame. A bridge should discard frames havingan incorrect FCS.
- Security
  - » Both bridges and routers provide the ability to put ñsecurity wallsò around specific stations.
  - » Routers generally provide greater security than bridges because
    - ï they can be addressed directly and
    - ï they use additional data for implementing security.

Overall Routers provide:

- improved reliability since alternative paths can be used
- improved bandwidth utilization because the best path is chosen
- fragmantation on packets
- enhanced security
- better error rate because error check can be done on entire packet

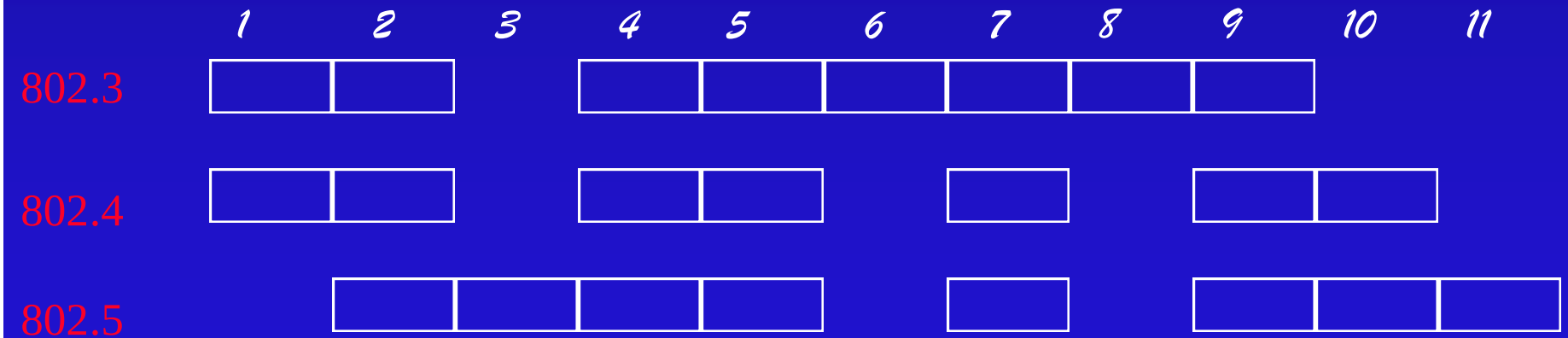
tion of a LAN bridge from 802.3 to 802.4



Bridges from 802.x to 802.y

- Any copying between different LANs requires reformatting, which takes CPU time, requires a new checksum calculation.
- Each LAN uses a different frame format

1. Preamble 2. Start delimiter 3.Access control 4. Frame control 5. Addresses of destination and source 6. Length 7. Data 8. Pad 9. Checksum 10. End delimiter 11. Frame status



The IEEE 802 frame formats

s from 802.x to 802.y (cont.)

- Interconnected LANs do not necessarily run at the same data rate; buffers are needed.
- LANs have a different maximum frame length. In IEEE 802, frames that are too large to be forwarded must be discarded.
- Problems encountered in building bridges are shown next.

802.3: mes, 10 Mbps
802.4: 8191-byte frames, 10 Mbps
802.5: 5000-byte frames, 4 Mbps

Destination LAN

Source LAN	802.3 (CSMA/CD)	802.4 (Token Bus)	802.5 (Token Ring)
802.3		1, 4	1, 2, 4, 8
802.4	1, 5, 8, 9,10	9	1,2,3,8,9,10
802.5	1,2,5,6,7,10	1,2,3,6,7	6,7

Ac

1. Reformat the frame and compute new checksum
2. Reverse the bit order
3. Copy the priority, meaninful or not
4. Generate a ficticious priority
5. Discard priority
6. Drain the ring
7. Set A and C bits
8. Worry about congestion (fast LAN to slow LAN)
9. Worry about token handoff ACK being delayed or impossible
10. Panic if frame is too long for destination LAN

Bridges can be characterized by

- Routing Tables
- Filtering
- Forwarding
- Learning Algorithm

Bridges (cont.)

- Routing table
  - » contains one entry per station of network to which bridge is connected
  - » is used to determine the network of destination station of a received packet
- Filtering
  - » is used by bridge to allow only those packets destined to the remote network
  - » packets are filtered with respect to their destination and multicast addresses

Bridges (cont.)

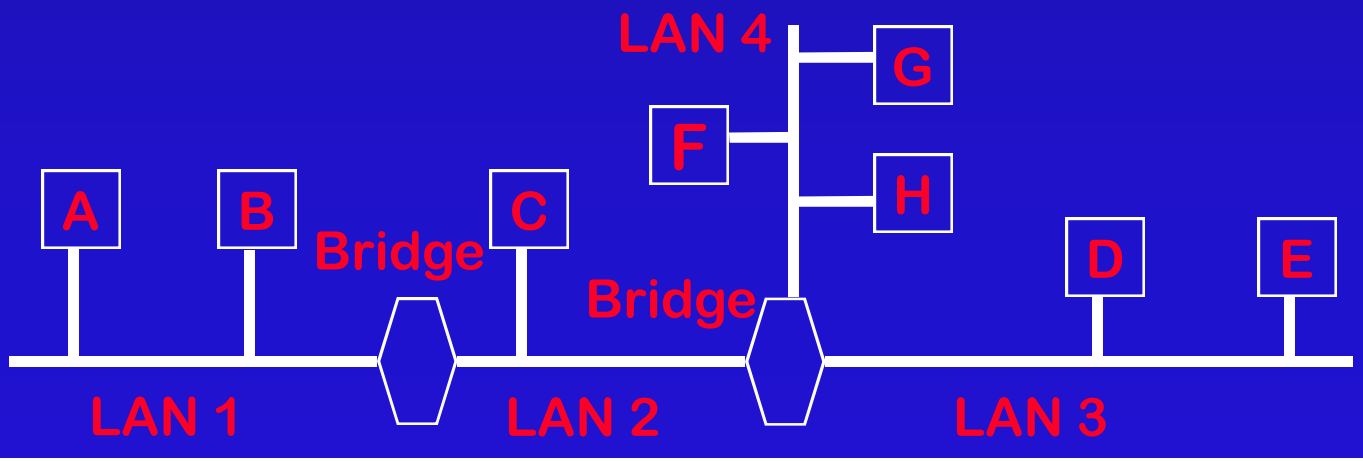
- Forwarding:
  the process of passing a packet from one network to another
- Learning:
  the process by which the bridge learns how to reach stations on the internetwork.

Transparent Bridges

- The first IEEE 802 bridge is a transparent bridge or spanning tree bridge.
- People wanted to have complete transparency: when a site with multiple LANs buys bridges designed to the IEEE standard, just plug connectors into bridges. So,
  - » no need for hardware/software changes,
  - » no setting of address switches,
  - » no downloading of routing tables or parameters
- A transparent bridge accepts every frame transmitted on all the LANs to which it is attached.

Transparent Bridges (cont.)

- decide whether to discard or forward incoming frames
- maintain large hash (routing) table, which lists each possible destination and indicates which output line (LAN) it belongs on.
  - » Initially, flooding algorithm is used.
  - » As time progresses, backward learning algorithm is used.
  - » All hash tables are initially empty.



Transparent Bridges (cont.)

- Topology can change dynamically. To handle it:
  - » the arrival time of each frame is also updated
  - » peridocically, a process in a bridge scans hash table
- There must be only one path of bridges and LANs between any two segments in the bridged LAN.
- have the advantage of being easy to install
- use only a subset of topology (the spanning tree)
- are chosen by the CSMA/CD and token bus people

Source Routing Bridges

- Token ring people chose the source routing bridge.
- Transmitter, or source, of frame in source routing specifies which route the frame is to follow; hence, the term source routing.
- Every machine in the internetwork knows, or can find, the best path to every other machine; discovery frame is used.
- Sender knows whether or not the destination is on its own LAN.
- set the high-order bit of destination address to 1 if frame is destined to another LAN

Source Routing Bridges (cont.)

- A route is a sequence of bridge #, LAN #, bridge #, LAN #, é .
- are interested in those frames with the high-order bit of destination address set to 1. For each such a frame, source routing bridge
  - » scans the route looking for the LAN # on which the frame arrived
  - » if this LAN # is followed by its own bridge #, then bridges forward frame onto the LAN whose number follows its bridge number in the route; otherwise, frame is discarded.

Comparison of Bridges

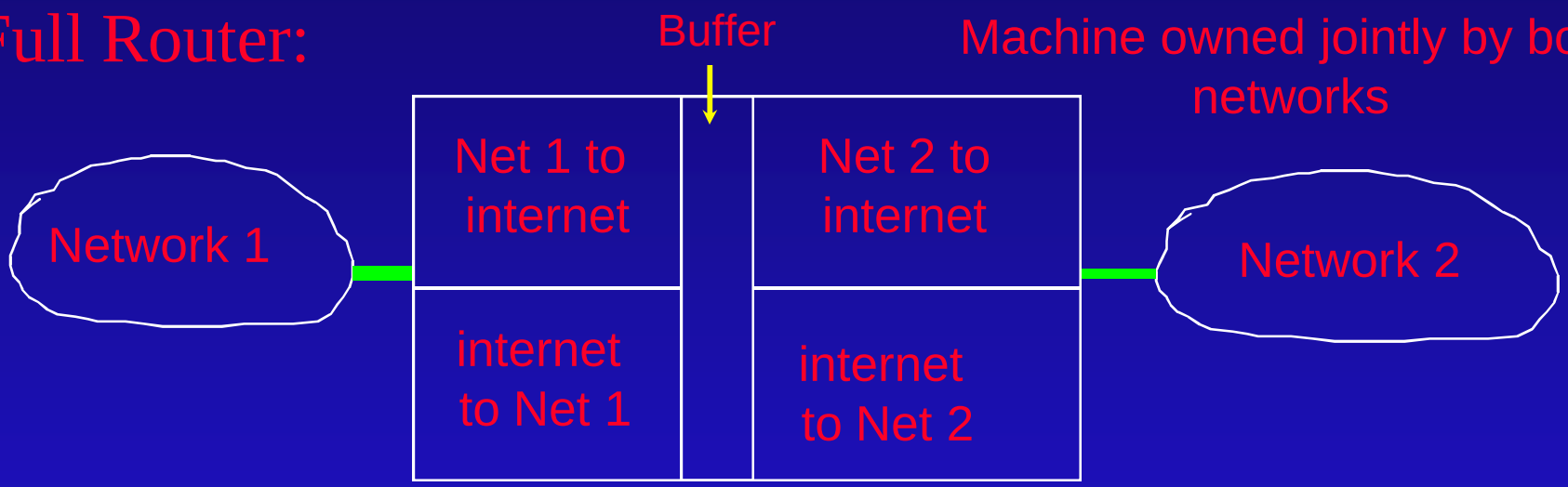
Issue	Transparent Bridge	Source Routing Bridge
Orientation	Connectionless	Connection-oriented
Transparency	Transparent to hosts	Not transparent
Configuration	Automatic	Manual
Routing	Suboptimal	Optimal
Locating Destinations	Backward learning	Discovery frames
Failures	Handled by bridges	Handled by hosts
Complexity	In the bridges	In the hosts

Router

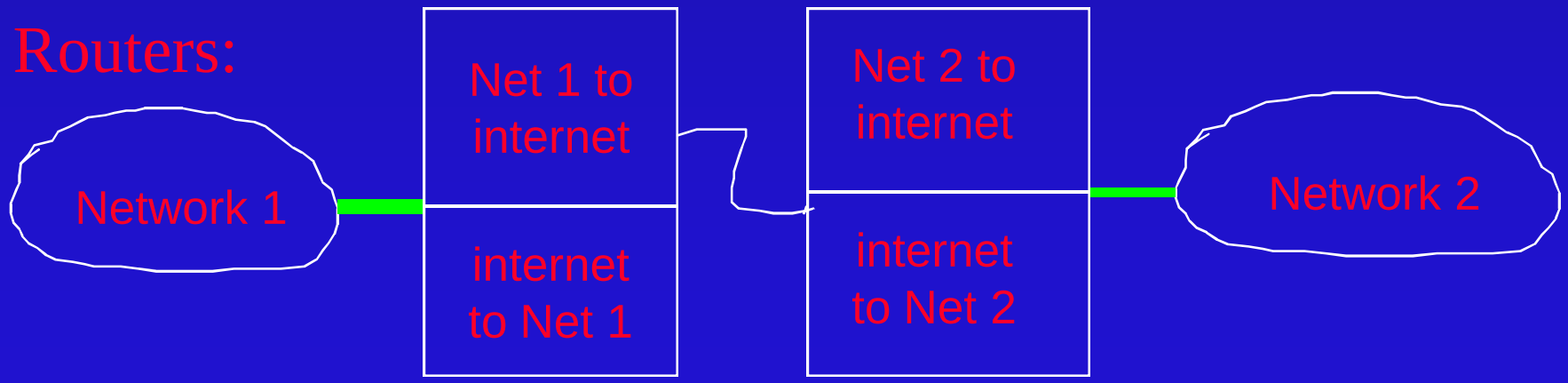
- connects dissimilar networks, provided that end-systems use a common network layer protocol, such as IP
- unlike bridge, router receive only those packets addressed to it by either a user machine or another router
- select the best route
- The question of who owns, operates, and maintains a router arises especially when two networks belong to independent organizations.

ull Router and Two Half-Routers

Full Router:



Two-Half Routers:



Disadvantages of Routers

Routers

- are protocol-dependent devices that must understand the protocol they are forwarding
- can require a considerable amount of initial configuration (installation is more complex than bridges)
- are relatively complex devices, and generally are more expensive than bridges

Advantages of Routers

Routers

- provide sophisticated routing, flow control, and traffic isolation
- are configurable, which allows network manager to make policy based on routing decisions
- allow active loops so that redundant paths are available

B-routers: Bridging Routers

- combine features of bridges and routers (i.e., combine capabilities of data-link and network layers)
- capable of establishing a bridge between two networks as well as routing some messages from the bridge networks to other networks
- are sometimes called smart hubs and are a combination of bridge/router hardware and software

Gateways

- connect two networks above the network layer of OSI model
- are capable of converting data frames and network protocols into the format needed by another network
- provide for translation services between different computer protocols

l r

- is the heart of the whole protocol hierarchy
- provides reliable, efficient, cost-effective data transport from source machine to destination
- makes use of the services provided by the network layer
- two types of transport service:
  - » connection-oriented
  - » connectionless
- Hardware and/or software within transport layer that does the work is called the transport entity

Why need transport layer?

- Network layer is part of communication subnet and is run by the carrier (at least for WANs)
- What happens if
  - » network layer offers connection-oriented service but is unreliable?
  - » network layer loses packets?
  - » routers crash from time to time?
- Users have no control over the subnet
- provides quality of service (QoS)
- real networks are not flawless
- isolates upper layers from technology, imperfections

nsport Layer QoS parameters

- Connection establishment delay: the time elapsing between a transport connection being requested and the confirmation received
- Connection establishment failure probability: the chance of a connection not being established within the maximum establishment delay time
- Throughput measures the number of bytes of user data transferred per second.
- Transit delay measures the time between a message sent by the transport layer on the source machine and its being received by the transport user on the destination machine.

nsport Layer QoS parameters (cont.)

- Residual error ratio measures the number of lost or garbled messages as a fraction of the total sent.
- Protection parameter allows transport user to specify interest against wiretappers.
- Priority parameter allows transport user to indicate the importance level of its connections.
- Resilience parameter gives the probability of transport layer itself spontaneously terminating a connection due to internal problems or congestion.

ble Transport Service Primitives

Primitive	TPDU sent	Meaning
LISTEN	(none)	Block until some process tries to connect
CONNECT	Connection request	Actively attempt to establish a connection
SEND	Data	Send information
RECEIVE	(none)	Block until a DATA TPDU arrives
DISCONNECT	Disconnection request	This side wants to release the connection

TPDU: Transport Protocol Data Unit

Transport Layer (cont.)

- To transport users, a connection is a reliable bit pipe.
- TCP (Transmission Control Protocol) is designed to provide a reliable end-to-end byte stream over an unreliable internetwork.
- The IP layer gives no guarantee that datagrams will be delivered properly.
- TCP service is obtained by having both sender and receiver create end points, called sockets

TCP Service

- is obtained by having sockets
- Each socket has a socket number (address) consisting of
  - » IP address of the host and
  - » a 16-bit number local to that host, called a port. (A port is the TCP name for a TSAP)
- Connection is established between a socket on the sending machine and a socket on the receiving machine.

t Primitives used in Berkeley UNIX for TCP

Primitive	Meaning
SOCKET	Create a new communication end point
BIND	Attach a local address to a socket
LISTEN	Announce willingness to accept connections; give queue size
ACCEPT	Block the caller until a connection attempt arrives
CONNECT	Actively attempt to establish a connection
SEND	Send some data over the connection
RECEIVE	Receive some data from the connection
CLOSE	Release the connection

nents of Transport Protocols

- Addressing: an application process wishes to connect a remote application process, its address must be specified.
  - In Internet, end points are (IP address, local port) pairs.
  - In ATM networks, they are AAL-SAPs.
- Establishing a connection
- Relasing a connection
- Flow Control
- Multiplexing
- Crash Recovery