Packet Switching

COM1337/3501

Textbook: Computer Networks: A Systems Approach,
L. Peterson, B. Davie, Morgan Kaufmann

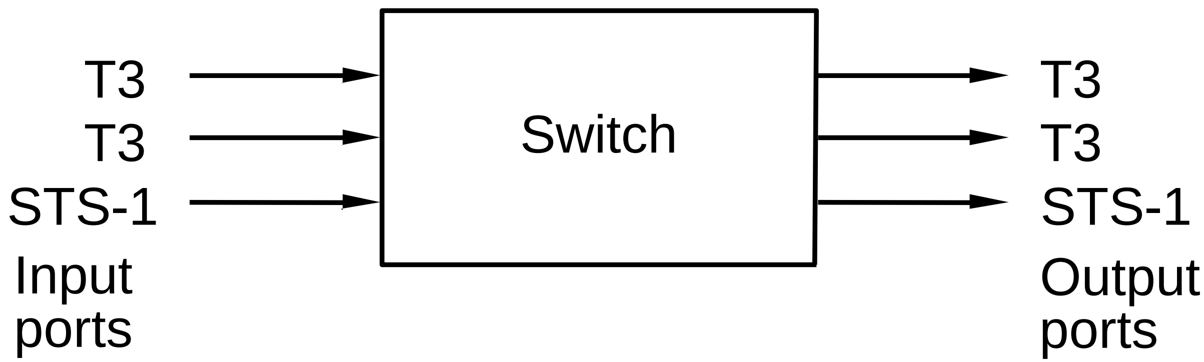
Chapter 3.

Outline

- Packet switching paradigms
- Bridges and extended LANs
- Cell switching
- Switching hardware

Scalable Networks

- Switch
  - forwards packets from input port to output port
  - port selected based on address in packet header



- Advantages
  - cover large geographic area (tolerate latency)
  - support large numbers of hosts (scalable bandwidth)

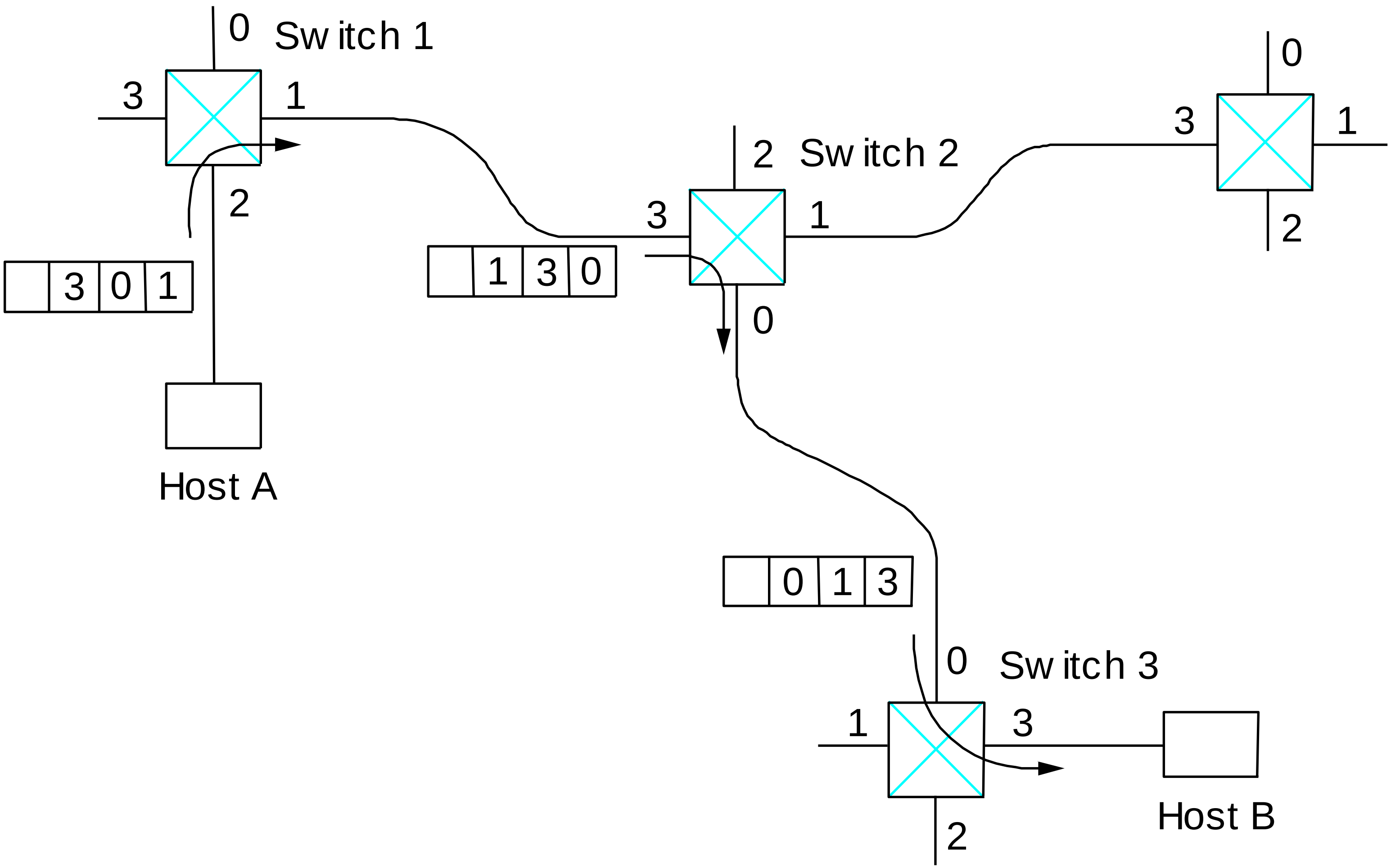
Packet Switching Paradigms

- Virtual circuit switching (routing)
- Datagram switching (routing)
- Source routing

Source Routing

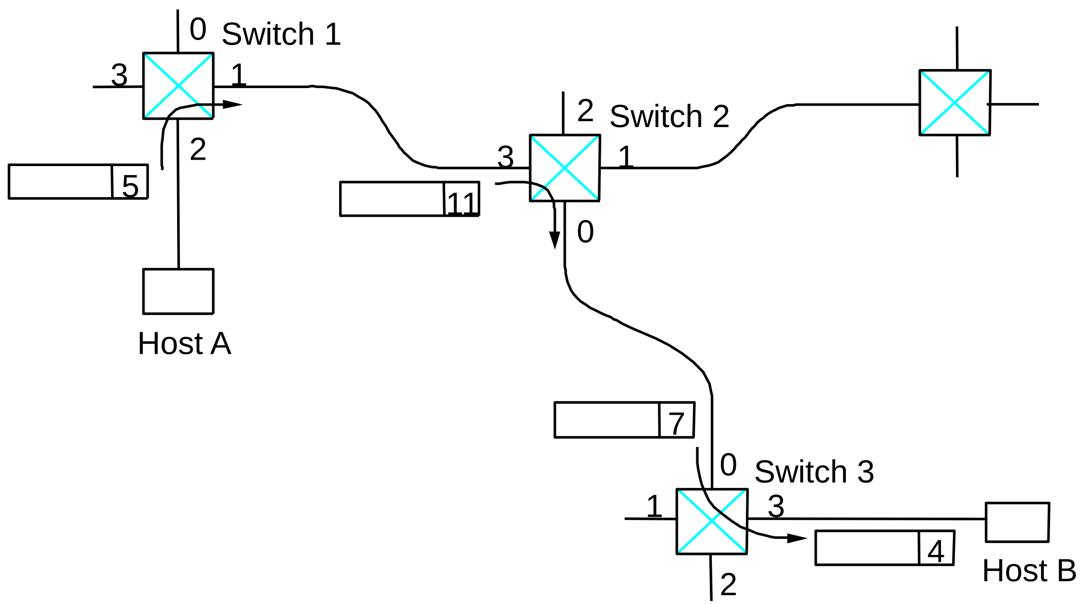
- The information to route the packet is provided by the source host and included in the packet
- Example of implementing source routing:
  - Assign a number to each switch output port
  - Include the list of output ports that the packet has to go through
  - The list is rotated by the intermediate switches before forwarding
- Disadvantage:
  - Packet initiators need to have a sufficient information about the network topology
  - The header has a variable length

Source Routing



Virtual Circuit (VC) Switching

- Explicit connection setup (and tear-down) phase
- Subsequent packets follow same circuit (path)
- Sometimes called *connection-oriented* model



- Analogy: phone call

- Each switch maintains a VC table

Virtual Circuit Switching

- Connection Setup approaches:
  - Permanent Virtual Circuits (PVC): manually setup/removed by network administrators
  - Switched Virtual Circuits (SVC): dynamically setup through signaling over some control channels
- Connection state => VC table
  - incoming interface, VC Identifier (VCI), outgoing interface, outgoing VCI
- SVC:
  - The setup message is forwarded over the network
  - New entries are created in the VC table and destination switches choose incoming VCI
  - When the setup message reaches the destination, connection

Virtual Circuits

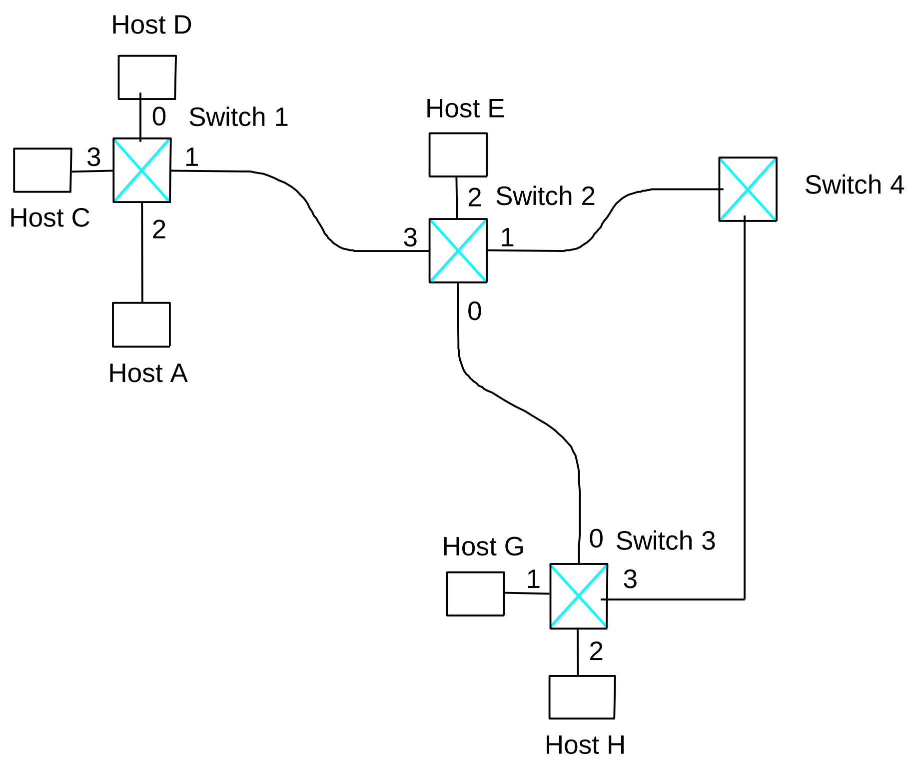
- Examples of Virtual Circuit Technology:
  - Frame Relay, X.25, Asynchronous Transfer Mode (ATM)
- Frame Relay was popular for creating virtual private networks (VPNs) using PVC.
- ATM is a more complex technology that provides mechanisms for supporting quality of service

Datagram Switching

- No connection setup phase
- Each packet forwarded independently
- Sometimes called *connectionless* model

- Analogy: postal system

- Each switch maintains a forwarding (routing) table



Virtual Circuit Model

- **Setup**: Typically wait full RTT for connection setup before sending first data packet.

- **Header**: While the connection request contains the full destination address, each data packet contains only a small identifier, making the per-packet header overhead small.

- **Quality of Service (QoS)**:
  – Connection setup allows resource reservation
  – If a switch or a link in a connection fails, the connection is broken and a new one needs to be established.

Datagram Model

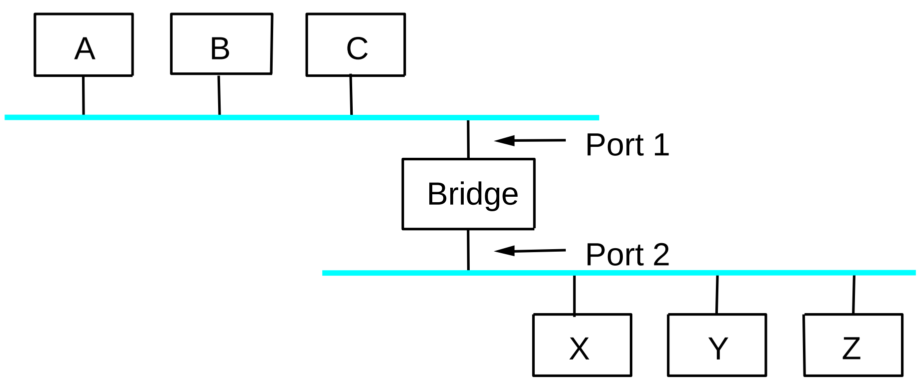
- **Setup**: There is no round trip time delay waiting for connection setup; a host can send data as soon as it is ready.
- **Header**: Since every packet must carry the full address of the destination, the overhead per packet is higher than for the connection-oriented model.
- **Quality of Service (QoS):**
  - Source host has no way of knowing if the network is capable of delivering a packet or if the destination host is even up.
  - Since packets are treated independently, it is possible to route around link and node failures.
  - Successive packets may follow different paths and be received out of order.

Outline

- Packet switching paradigms
- **Bridges and extended LANs**
- Cell switching
- Switching hardware

Bridges and Extended LANs

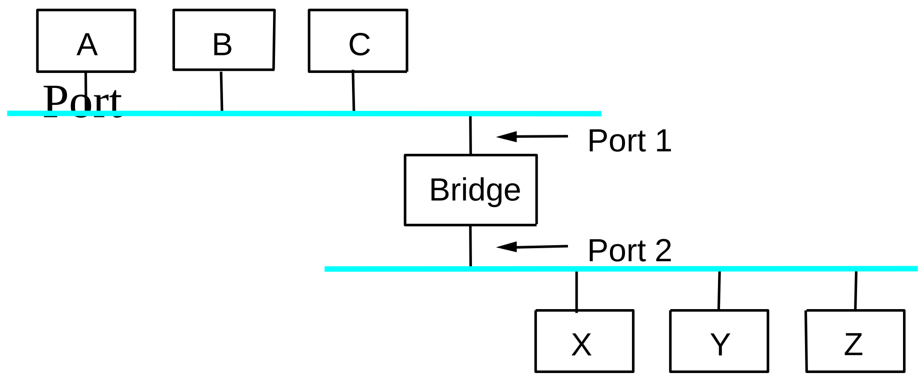
- LANs have physical limitations (e.g., 2500m)
- Connect two or more LANs with a *bridge*
  - accept and forward strategy
  - level 2 connection (does not add packet header)



- Ethernet Switch is a LAN Switch = Bridge

Learning Bridges

- Do not forward when unnecessary
- Maintain forwarding table

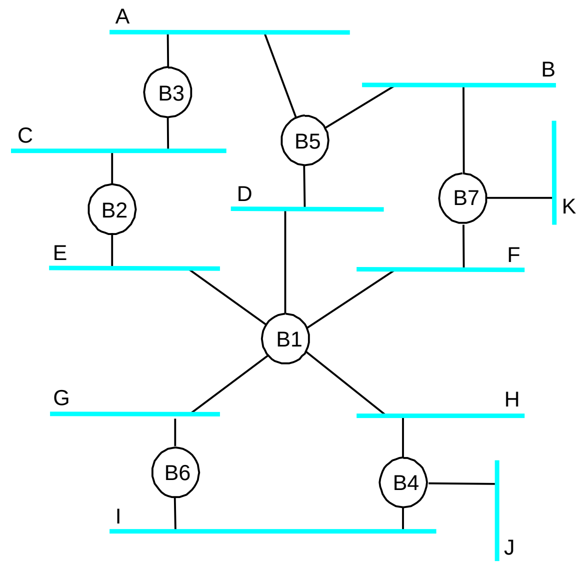


Host	Port
A	1
B	1
C	1
X	2
Y	2
Z	2

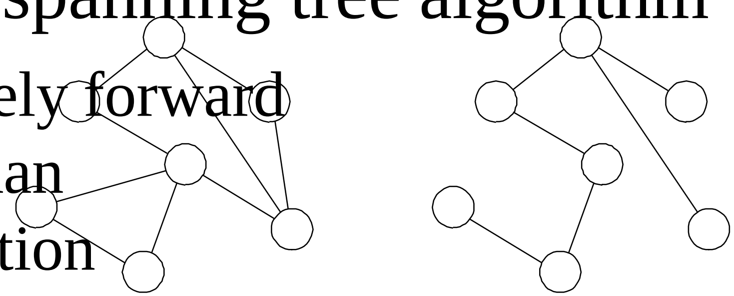
- Learn table entries based on source address
- Table is an optimization; need not be complete
- Always forward broadcast frames

Spanning Tree Algorithm

- Problem: loops

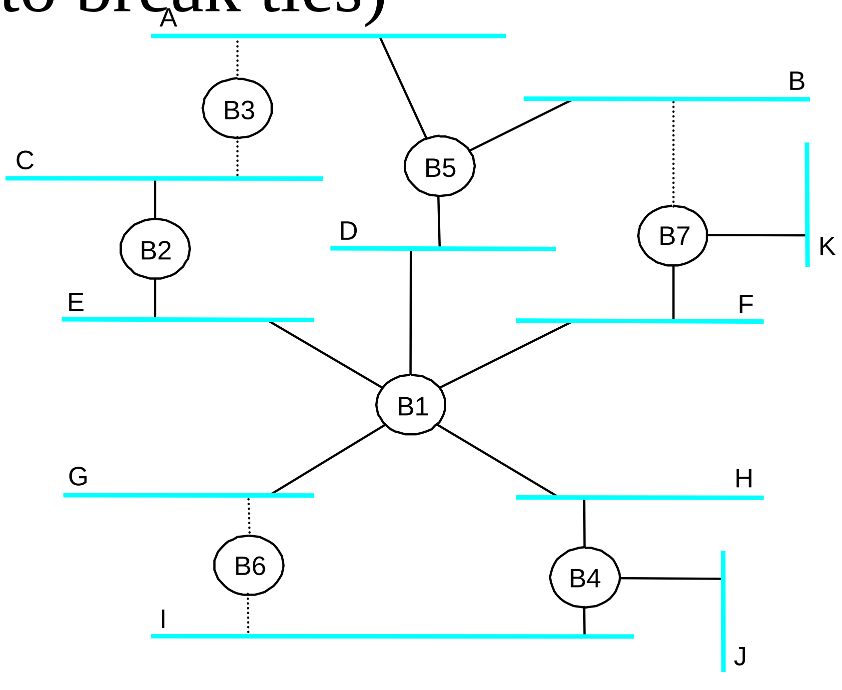


- Bridges run a distributed spanning tree algorithm
  - select which bridges actively forward
  - developed by Radia Perlman
  - now IEEE 802.1 specification



Algorithm Overview

- Each bridge has unique id (e.g., B1, B2, B3)
- Select bridge with smallest id as root
- Select bridge on each LAN closest to root as designated bridge (use id to break ties)
- Each bridge forwards frames over each LAN for which it is the designated bridge



Algorithm Details

- Bridges exchange configuration messages
  - id for bridge sending the message
  - id for what the sending bridge believes to be root bridge
  - distance (hops) from sending bridge to root bridge
- Each bridge records current best configuration message for each port
- Initially, each bridge believes it is the root

Algorithm Detail (cont)

- When learn not root, stop generating config messages
  - in steady state, only root generates configuration messages
- When learn not designated bridge, stop forwarding config messages
  - in steady state, only designated bridges forward config messages
- Root continues to periodically send config messages
- If any bridge does not receive config message after a period of time, it starts generating config messages claiming to be the root

Broadcast and Multicast

- Forward all broadcast/multicast frames
  - current practice
- Learn when no group members downstream
- Accomplished by having each member of group G send a frame to bridge multicast address with G in source field

Limitations of Bridges

- Do not scale
  - spanning tree algorithm does not scale
  - broadcast does not scale
- Do not accommodate heterogeneity
- Caution: beware of transparency
  - Bridged LANs do not always behave as single shared medium LAN: they drop packets when congested, higher latency

Virtual LANs (VLAN)

- VLANs are used to:
  - increase scalability: reduce broadcast messages
  - provide some basic security by separating LANs
- VLANs have an ID (color).
- Bridges insert the VLAN ID between the ethernet header and its payload
- Packets (unicast and multicast) are only forwarded to VLAN with the same ID as the source VLAN