Chapter 2 Internetworking

Topics covered:
Basic terminology. Principles of internetworking. Types of internetworking devices. Repeaters, hubs, bridges, routers, switches and gateways. Transparent and source-routing bridges. Multilayer switches. VLANs. Routing strategies. Addressing.

2.1 Terminology

Internetworking stands for connectivity and communication between two or more networks.

- Internetwork (internet): a collection of communication networks interconnected by bridges, switches and/or routers.

- Intranet: a corporate internet that provides key Internet applications. It is usually isolated and self-contained within an organization.

- End System (ES):

- Intermediate System (IS):

2.2 Principles of Internetworking

2.2.1 Requirements for Internetworking

The overall requirements for an internetworking facility are:

1. Provide a link between networks. At minimum, a physical and link control connection is needed.
2. Provide for the routing and delivery of data between processes on different networks.
3. Provide an accounting service that keeps track of the use of the various networks and routers and maintains status information.
4. Provide the services just listed without requiring modifications to the networking architecture of constituent networks. This means accommodating the following differences:

    - Different addressing schemes

    - Different maximum packet size

    - Different network access mechanisms

    - Different timeouts

    - Different error recovery services

- Different status reporting
- Different routing techniques
- Different user access control
- Connection-oriented vs. connectionless

It may be desirable for an internetwork service not to depend on the characteristics of individual networks.

By fulfilling these requirements, two important problems in interconnecting networks can be addressed:

-

-

2.2.2 Motivation for Internetworking

- Sharing of computer resources across a number of communications networks
- The use of multiple networks allows for network isolation when needed. This is critical to network performance as failure is contained within one network. Also, a network can be shielded from intrusion (Security).
- Contain the amount of traffic sent between the networks (e.g., Routing domains)
- Network Management that provides centralized support and troubleshooting capabilities in an internetwork.

2.2.3 Components of an Internetwork

- Campus Network: locally connected users in a building or group of buildings. It generally uses LAN technologies.
- Wide Area Networks (WANs): distant campuses connected together usually through connection providers such as a telephone company.
- Remote connections:

2.2.4 Routing domains

A routing domain is an administrative entity. Its goal is to establish boundaries for the dissemination of routing information.

2.3 Internetworking Devices

Devices that interconnect LANs are known as relays and operate at one layer of the OSI model.

There are 5 common types of relays:

-
-
-
-
-

2.3.1 Repeaters (Hubs)

- Overcomes restrictions caused by single segment usage such as number of users, cable length.
- Amplifies or regenerates weak signals.
- Extends cable length.
- Connects LANs of similar type.
- Provides simple connection between adjacent LANs at the expense of increased network congestion.

2.3.2 Bridges

The bridge was designed for interconnection of LANs that use identical protocols at the MAC layer. However, there are bridges capable of mapping between different MAC protocols (e.g., Ethernet and Token Ring).

A bridge main function is forwarding frames from one network to another. A bridge does the following:

Characteristics of bridges

- Interconnects two or more LANs (either similar or dissimilar) at the MAC level.
- Capable of deciding whether or not to forward a 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.

Reasons for using bridges

- Reliability: fault is limited to the network where it happened.
- Performance: intra-network traffic stays within one network.
- Security: Types of traffic with different security needs are kept on physically separate media.
- Geography: LANs may need to be on separate locations.

Design aspects of a bridge

- It should make no modification to the content or format of the frames it receives.
- It must contain addressing and routing/forwarding intelligence.
- It may connect more than 2 LANs

Bridges have to make a routing decision

- S1 transmits a frame on LAN-A intended for S5. B1 and B2 will read the frame. Each one must make a decision of whether or not to retransmit the frame to other LANs. This continues until the frame reaches LAN-E where it is received by S5.

- The routing decision may not always be a simple one. If we add bridge B7 between LAN-A and LAN-E.

- B7 may fail.

-

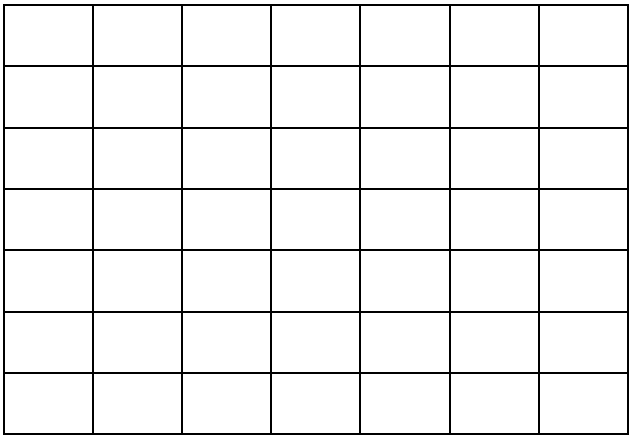
Many routing strategies are used in bridges:

- Fixed routing
- Spanning tree routing (Transparent bridges)
- Source routing

2.3.2.1 Fixed routing

- A route is selected for each source-destination pair of LANs. If more are available, the one with the least number of hops is selected.

- A central routing matrix is created. It shows the identity of the first bridge on the route.



Advantages:

- Simplicity
- Minimal processing requirements

Disadvantages:

- Bridges can be dynamically added and failures may occur, so tables must change.

2.3.2.2 Spanning Tree Routing (Transparent bridges)

Transparent bridge characteristics:

- It is intended to interconnect LANs that satisfy any of the MAC standards without end stations being aware of its existence (i.e., transparent)

- The routing mechanism is the spanning tree algorithm

The bridge must map the content of the incoming frame into an outbound frame that conforms to the frame format for the outbound LAN.

2.3.2.2.1 Frame Forwarding

A bridge maintains a filtering database. This information can be preloaded into the bridge (i.e., static routing).

2.3.2.2.2 Address Learning

The filtering database can be learned.

2.3.2.2.3 Spanning Tree Algorithm

Address learning is effective with a tree topology (i.e., no closed loop)

- **B1 and B2 know where S2 is:**

1.
2.
3.
4.
5.
6.
7.

- **B1 and B2 do not know of S2 yet:**

1.
2.
3.
4.
5.

In graph theory: for any connected graph, consisting of nodes and edges connecting pairs of nodes, there is a spanning tree of edges that maintains the connectivity of the graph but contains no closed loops.

Algorithm:

- Each bridge is assigned a unique id
- A special group MAC address is used to send a frame to all bridges
- Each port of a bridge has a unique "port id"
- Each port of a bridge has an associated cost

The spanning tree is constructed as follows:

1. Determine the root bridge (RB) that is the bridge with the lowest id.
2. Determine the root port (R) on all other bridges. This is the port used for the first hop on the minimum cost path to the root bridge. The lower port number is selected if more than one port exists.
   - The root path cost (rpc) is the cost of the path to the root bridge with minimum cost.

3. Determine the designated port (D) on each LAN. This is the port with the minimum rpc. If more bridges have the same rpc, the one with the highest priority is chosen as designated bridge (i.e., lowest-numbered bridge identifier).

   - The designated bridge is the bridge that provides the minimum cost path to the root bridge.

4. Ports which are neither (R) nor (D) are Blocking (B).

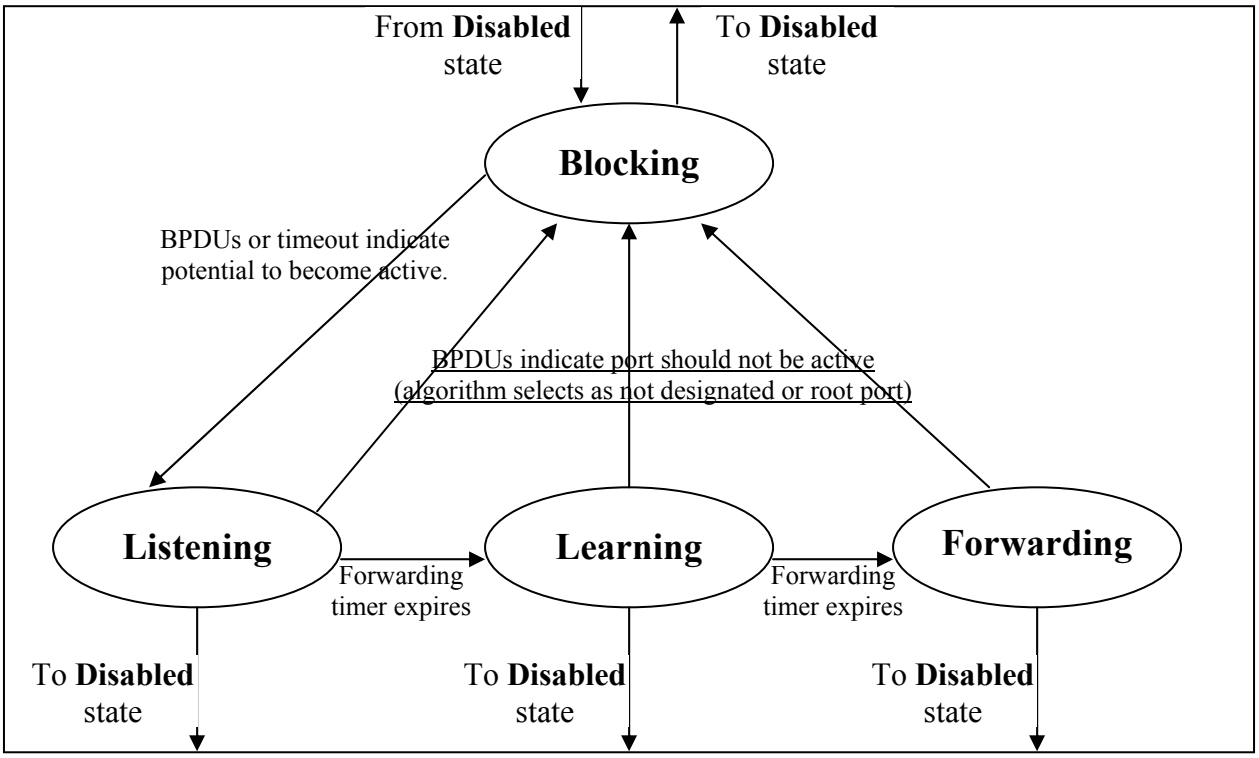
BPDUs (Bridge Protocol Data Units) are used to exchange information between bridges.

- BPDUs are sent by all the bridges each claiming to be the root bridge. B1 is elected as the root bridge.

- All other bridges determine the root port (R) and root path cost (rpc).

- Example: On LAN-5: B3, B4 and B5 send BPDUs claiming to be the designated bridge. B4 and B5 have the lowest RPC. B4 has a higher priority. B4 becomes the designated bridge (D).

2.3.2.2.4 Spanning Tree State Transition Diagram for a bridge port



The following is a table summarizing the actions taken by a bridge in each state.

	Receive BPDUs	**Transmit BPDUs**	**Learn addresses**	**Forward data frames**
Disabled				
Blocking				
Listening				
Learning				
Forwarding				

2.3.2.3 Source Routing Bridges

- Developed by IEEE 802.5 committee

The sending station determines the route to be followed by a frame and includes routing information with this frame.

Each frame includes the type of routing desired:

- Null: no routing desired.
- Nonbroadcast: the frame includes a single route using LANs and bridges.
- All-routes broadcast: the frame will reach each LAN (and the destination station) by all possible routes.

  To avoid looping:

- Single-route broadcast: the frame will appear once on each LAN. The frame is forwarded to bridges on the spanning tree with source node as root. The destination receives one copy.

Route discovery and selection:

There are three options:

- Manually load information into each station.
    - Problem:

- Stations in the same LAN exchange routing information.
    - Problem:

- Dynamic route discovery procedure by stations

Two approaches are possible:

1.
    - Source station transmits an all-routes request to destination.
    - Destination sends back a nonbroadcast response on each discovered route.
    - Source uses one of these to send subsequent frames.

        - Problem:

2.
    - Source station transmits a single-route request.
    - Destination responds with an all-routes response.
    - Source chooses one for subsequent transmissions.

2.3.2.4 Spanning Tree vs. Source Routing

Characteristics	Transparent bridging	Source route bridging
Transparency		
Topology knowledge		
Frame format		
Frame forwarding		
Bridge mode		
Data Link operation		
Link utilization		
Configuration (LAN numbering, bridge numbering, spanning tree, etc)		
Performance		
Routing		

2.3.2.5 Source Routing Transparent (SRT) Bridges

A key problem is that both (transparent and source routing bridges) are incompatible. To allow the interconnections of LANs using a mixture of transparent and source routing bridges, a new standard was developed by the IEEE 802.5 committee, and that is the Source Routing Transparent (SRT) technique.