Internetworking

Raj Jain

Raj Jain is now at
Washington University in Saint Louis
Jain@cse.wustl.edu
http://www.cse.wustl.edu/~jain/

Overview

- Internetworking terms and services
- Bridges vs routers
- How bridges work?
- Spanning Tree and source routing
- Internet Protocol (IP): Services, Header, Address format
- Other Router-level protocols: ARP, ICMP, EGP, OSPF
**Internetworking Terms**

- **End-system**: Host
- **Network**: Provides data transfer between end-systems
- **Internet**: A collection of networks
- **Subnetwork**: Each component of an internet
- **Intermediate System**: Connects two subnetworks
- **Port**: Application processes in the host

```
Subnet 1  Intermediate System  Subnet 2
```

**Internetworking Services**

- Connects two or more subnets
- May provide accounting and status information
- Accomodate subnets with
  - Different addressing schemes
  - Different maximum packet sizes
  - Different network access mechanisms
  - Different timeouts
  - May provide error recovery
  - Different routing techniques
  - Different user access control
  - Connectionless and connection-oriented subnets
Bridge vs Router

- Bridge: Connects or more identical LANs. Operates at layer 2 of the OSI model.
- Router: Connects two or more LANs that may or may not be identical. Operates at layer 3 of the OSI model.

Bridge: Functions

- Monitor all frames on LAN A
- Pickup those frames that are for stations on the other side
- Retransmit the frames on the other side
- Knows or learns about which stations are on various sides
- Makes no modification to content of the frames
  - May change headers.
- Provides storage for frames to be forwarded
- Improves reliability (less nodes per LAN)
- Improves performance (more bandwidth per node)
- Security (Can keeps different traffic from entering a LAN)
- May provide flow and congestion control
Data Encapsulation by Bridges

(a) Architecture

(b) Operation

Figure 11.5. Connection of two LANs by a bridge.

Half-Bridges for Point-to-point links

(a) Architecture

(b) Operation

Raj Jain
The Ohio State University
1. Fixed Routing

Path Determination By Bridges

![Diagram of LAN and bridges connecting stations](image)

Fig 11.10
2. Spanning Tree

Spanning Tree: Terminology

- **Bridge Identifier**: MAC address plus a priority level
- **Port identifier**: For each port of a bridge
- **Path cost**: Cost transmitting through a port
- **Root Bridge**: The bridge with the lowest identifier
- **Root port**: The port with the minimum cost to the root bridge
- **Root path cost**: Cost of the path to the root bridge
- **Designated bridge**: One per LAN. The bridge that provides minimum cost path from the LAN to the root bridge.
- **Designated Port**: The port of the designated bridge that connects the bridge to the LAN
Spanning Tree Algorithm

- All bridges multicast to “All bridges”
  - My ID
  - Root ID
  - My cost to root
- The bridges use the information received to update their info using Dijkstra’s algorithm and rebroadcast
- Initially all bridges consider themselves to be the root but eventually converge to one root as they find out the lowest Bridge ID.
- On each LAN, the bridge with minimum cost to the root becomes the Designated bridge
- All ports of all non-designated bridges are blocked.

3. Source Routing

- The frame header contains the complete route:
  LAN 1 - Bridge B1 - LAN 3 - Bridge B3 - LAN 2 - Dest
- Bridges are simple, end systems do the routing
- Four types of destination addressing:
  - Null: Destination on the same LAN
  - Nonbroadcast: Includes a route to destination
  - All-route Broadcast: Flooded. Bridges record route in the frame.
  - Single-route Broadcast: Once and only once on each LAN. Spanning tree used for broadcast
Route Discovery

- Manually on small internets
- Route server
- Dynamic route discovery
  - Transmit “All-route request frame” to destination
    The destination sends back “nonbroadcast response” on each frame. Source knows all routes to the destination. Selects one.
  - Transmit “single-route request frame” to destination
    The destination responds with one “All-routes response.” The source receives many responses and discovers all routes.

Internet Protocol (IP)

- IP deals with only with host addresses
- Services:
  - Send: User to IP
  - Deliver: IP to User
  - Error (optional): IP to User
- IP Header

<table>
<thead>
<tr>
<th>Version</th>
<th>IHL</th>
<th>Type of service</th>
<th>Total length</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
IP Header

- Version (4 bits)
- Internet header length (4 bits): in 32-bit words. Min header is 5 words or 20 bytes.
- Type of service (8 bits): Reliability, precedence, delay, and throughput
- Total length (16 bits): header+data in bytes
- Identifier (16 bits): Helps uniquely identify the datagram during its life for a given source, destination address
- Flags (3 bits): More flag - used for fragmentation
  No-fragmentation
  Reserved
- Fragment offset (13 bits): In units of 8 bytes
- Time to live (8 bits): Specified in router hops
- Protocol (8 bits): Next level protocol to receive the data
- Header checksum (16 bits): 1’s complement sum of all 16-bit words in the header
- Source Address (32 bits)
- Destination Address (32 bits)
- Options (variable): Security, source route, record route, stream id (used for voice) for reserved resources, timestamp recording
- Padding (variable): Makes header length a multiple of 4
- Data (variable): Data + header < 65,535 bytes
### IP vs ISO CLNP (Continued)

<table>
<thead>
<tr>
<th>Function</th>
<th>IP</th>
<th>ISO CLNP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Options</td>
<td>Security</td>
<td>Security</td>
</tr>
<tr>
<td></td>
<td>Precedence bits in TOS</td>
<td>Priority</td>
</tr>
<tr>
<td></td>
<td>Stricter source route</td>
<td>Complete source route</td>
</tr>
<tr>
<td></td>
<td>Loose source route</td>
<td>Partial source route</td>
</tr>
<tr>
<td></td>
<td>Record route</td>
<td>Record route</td>
</tr>
<tr>
<td></td>
<td>Padding</td>
<td>Padding</td>
</tr>
<tr>
<td></td>
<td>Timestamp</td>
<td>Not present</td>
</tr>
</tbody>
</table>

Ref: Piscitello and Chapin, p 384.

### Address Resolution Protocol (ARP)

- **Problem:** Given an IP address find the MAC address
- **Solution:** Address resolution protocol
- **The host broadcasts a request:**
  “What is the MAC address of 127.123.115.08?”
- **The host whose IP address is 127.123.115.08 replies back:**
  “The MAC address for 127.123.115.08 is 8A-5F-3C-23-45-56”
- **A router may act as a proxy for many IP addresses**
Internet Control Message Protocol (ICMP)

- Required companion to IP.
  Provides feedback from the network.
  - Destination unreachable
  - Time exceeded
  - Parameter problem
  - Source quench
  - Redirect
  - Echo reply
  - Timestamp
  - Timestamp reply
  - Information Request
  - Information reply

Autonomous Systems

- An internet connected by homogeneous routers under the administrative control of a single entity
Other Router-level Protocols

- Interior Router Protocol (IRP): Used for passing routing information among routers internal to an autonomous system
- Exterior Router Protocol (ERP): Used for passing routing information among routers between autonomous systems
- Open Shortest Path First (OSPF): Interior routing protocol. Provides least-cost path routes using a fully user configurable routing metric (any fn of delay, data rate, dollar cost, etc.) Link costs flooded (Link-state routing)
- Exterior Gateway Protocol (EGP): Periodic hellos and responses with cost to other networks

Summary

- Subnetwork, IS, ES
- Bridges and routers
- Spanning tree, source routing, route discovery
- IP: Address, header
- ARP, ICMP, EGP, OSPF