Data Link Layer Switching

Savera Tanwir
Data Link Layer Switching

- Switching
- Bridges from 802.x to 802.y
- Local Internetworking
- Spanning Tree Bridges
- Remote Bridges
- Repeaters, Hubs, Bridges, Switches, Routers, Gateways
- Virtual LANs
Data Link Layer Switching

Multiple LANs connected by a backbone to handle a total load higher than the capacity of a single LAN.
Bridges from 802.x to 802.y

Operation of a LAN bridge from 802.11 to 802.3.
Bridging Problems from 802.x to 802.y

1. Frame translation
2. Different Data Rates
3. Different Maximum Frame lengths
4. Security issues
   - 802.11 & 802.16 support encryption, 802.3 doesn’t
5. QoS
   - 802.11 & 802.16 support QoS, 802.3 doesn’t
Bridges from 802.x to 802.y (2)

The IEEE 802 frame formats. The drawing is not to scale.
Local Internetworking

A configuration with four LANs and two bridges.
Filtering/Forwarding/Flooding

- If the destination device is on the same segment as the frame, the bridge will not send the frame onto other segments
  - This process is known as filtering
- If the destination device is on a different segment, the bridge forwards the frame to the appropriate segment
  - This process is known as forwarding
- If the destination address is unknown to the bridge, the bridge forwards the frame to all segments except the one on which it was received
  - This process is known as flooding
Spanning Tree Protocol

- A good network design should include spare (redundant) links to provide an alternate path if one fails.
- Problem: A *broadcast storm* caused by broadcast packets looping between switches would reduce available CPU resources and bandwidth.
Spanning Tree Protocol

- STP is used in switched networks to prevent loops
  - Has been standardized by IEEE 802.1D

- Protocol Operation
  - Elect a root bridge
    - Each switch has a MAC address and a configurable priority number; both of these numbers make up the Bridge Identification (BID) – Lowest BID wins
  - Find least cost paths to root bridge (measured as sum of all traversed port costs)
  - Disable links that are not part of those paths
Spanning Tree Basics

A ‘Tree-Like’ Loop-Free Topology Is Established

A Switch Is Elected as Root

Loop-Free Connectivity
Spanning Tree Bridges

(a) Interconnected LANs. (b) A spanning tree covering the LANs. The dotted lines are not part of the spanning tree.
Remote Bridges

Remote bridges can be used to interconnect distant LANs.
Switch

- Data Link Layer device
  - Examines frame header and *selectively* forwards frame based on MAC destination address
  - When frame is to be forwarded on segment, uses CSMA/CD to access segment
- Transparent
  - Hosts are unaware of presence of switches
- Plug-and-Play, Self-learning
  - Switches do not need to be configured
Repeaters, Hubs, Bridges, Switches, Routers and Gateways

<table>
<thead>
<tr>
<th>Layer</th>
<th>Device</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application layer</td>
<td>Application gateway</td>
</tr>
<tr>
<td>Transport layer</td>
<td>Transport gateway</td>
</tr>
<tr>
<td>Network layer</td>
<td>Router</td>
</tr>
<tr>
<td>Data link layer</td>
<td>Bridge, switch</td>
</tr>
<tr>
<td>Physical layer</td>
<td>Repeater, hub</td>
</tr>
</tbody>
</table>

(a) Which device is in which layer.
(b) Frames, packets, and headers.
Repeaters, Hubs, Bridges, Switches, Routers and Gateways

(2)

(a) A hub. (b) A bridge. (c) a switch.
How does one determine onto which LAN segment to forward frame?

Looks like a routing problem...
Backward Learning

- Every switch has a *switch table*
- Entry in switch table:
  - (MAC Address, Interface, Time Stamp)
  - Stale entries in table are dropped (after a few minutes)
- Switch *learns* which hosts can be reached through which interfaces
  - When a frame is received, switch “learns” location of sender: incoming LAN segment
  - Records sender/location pair in switch table
Filtering/Forwarding/Flooding

When switch receives a frame:

index switch table using MAC dest address
if entry found for destination
    then{
        if dest on segment from which frame arrived
            then drop the frame
        else forward the frame on interface indicated
    }
else flood
   forward on all but the interface on which the frame arrived
Switch example

Suppose C sends frame to D

- Switch receives frame from C
  - Notes in switch table that C is on interface 1
  - because D is not in table, switch forwards frame into interfaces 2 and 3

- Frame received by D

<table>
<thead>
<tr>
<th>address</th>
<th>interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>1</td>
</tr>
<tr>
<td>B</td>
<td>1</td>
</tr>
<tr>
<td>E</td>
<td>2</td>
</tr>
<tr>
<td>G</td>
<td>3</td>
</tr>
</tbody>
</table>
Switch example

Suppose D replies back with frame to C.

- Switch receives frame from D
  - notes in switch table that D is on interface 2
  - because C is in table, switch forwards frame only to interface 1
- Frame received by C
Switch: Traffic Isolation

- Switch installation breaks subnet into LAN segments
- Switch *filters* packets:
  - Same-LAN-segment frames not usually forwarded onto other LAN segments
  - Segments become separate *collision domains*
Switches: Dedicated Access

- Switch with many interfaces
- Hosts have direct connection to switch
- No collisions; Full-duplex

Switching: A-to-A’ and B-to-B’ simultaneously, no collisions
Switch Forwarding methods

1. **Store-and-Forward**
2. **Cut-through Switching**
   - Switch starts forwarding a frame before the whole frame has been received (As soon as the destination address is processed)
   - Produces a slight reduction in over-all latency
3. **Fragment Free Switching**
   - Switch starts forwarding a frame when enough bytes have been received from the source to detect a collision (e.g., 64 Bytes)
4. **Adaptive Switching**
   - Automatically switching between the other three modes

- Cut-through Switches fall back to Store-and-forward if the outgoing interface is busy at the time
- These forwarding methods are not controlled by the user and are configured only by the switch itself
Institutional network

to external network

router

switch

mail server

web server

IP subnet

hub

hub

hub
NIIT NETWORK ARCHITECTURE

Diagram of network architecture showing various devices and connections, with IP addresses and links labeled.
Switches vs. Routers

- Both store-and-forward devices
  - Routers: network layer devices (examine network layer headers)
  - Switches are link layer devices
- Routers maintain routing tables, implement routing algorithms
- Switches maintain switch tables, implement filtering, learning algorithms
Virtual LANs

- A way of creating independent logical LAN within a physical LAN

- Why?
  - Security
  - Load Balancing
  - Broadcast Control
  - Administrative Demarcation/Management Flexibility
One VLAN is one broadcast domain
Virtual LANs

Four physical LANs organized into two VLANs, gray and white
Virtual LANs

How?
- Reconfiguration of the LAN is done through software rather than by physically unplugging and moving devices or wires.
- Behave as if connected to the same wire - even though actually/physically connected to different segments of a LAN.
Assigning VLAN Memberships

- The four ways that are in use are:

  1. Port-based
     - A switch port is manually configured to be a member of a VLAN
     - This method only works if all machines on the port belong to the same VLAN
  2. MAC-based
     - VLAN membership is based on the MAC address of the workstation
     - The switch has a table listing of the MAC address of each machine, along with the VLAN to which it belongs
  3. Layer 3 Protocol-based
     - Every Layer 3 protocol or IP address is assigned a VLAN membership
     - Major disadvantage: Violates the independence of the layers, so an upgrade from IPv4 to IPv6, for example, will cause the switch to fail
  4. Authentication-based
     - Devices can be automatically placed into VLANs based on the authentication credentials of a user or device using the 802.1X protocol
Identifying VLANs

- How to identify VLAN color of a station?
  - Put a VLAN ID field (color field) in the frame header

Frame Tagging

- In 1998, IEEE 802.1Q changed the Ethernet header

Potential Problems

- Need we throw out several hundred million existing Ethernet cards?
- If not, who generates the new fields?
- What happens to frames that are already the maximum size?
Identifying VLANs

Solution
- VLAN fields are only actually used by the bridges and switches and not by the user machines
  - Thus, to use VLANs, the bridges or switches have to be VLAN and 802.1Q aware

Answers to potential problems
- No
- The 1st VLAN-aware bridge or switch to touch a frame adds VLAN tags and the last one down the road removes them
- 802.1Q just raised the limit of total frame size to 1522 Bytes
The IEEE 802.1Q Standard

Transition from legacy Ethernet to VLAN-aware Ethernet. The shaded symbols are VLAN aware. The empty ones are not.
The IEEE 802.1Q Frame Format

- **Priority**
  - 3-bit field used to store a priority level for the frame
  - Use of this field is defined in IEEE 802.1p

- **Canonical Format Indicator (CFI)**
  - 1-bit indicator that is always set to zero for Ethernet switches
  - Used for compatibility between Ethernet and Token Ring networks

- **VLAN ID**
  - 12-bit field specify the VLAN to which the frame belongs
  - A value of 0 means that the frame doesn't belong to any VLAN
  - A value of 1 is used with bridges
  - A value of 0xFFF is reserved
  - All other values may be used as VLAN identifiers, allowing up to 4093 VLANs

- Because inserting this header changes the frame, 802.1Q encapsulation forces a recalculation of the original checksum.
## Summary

<table>
<thead>
<tr>
<th>Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FDM</td>
<td>Dedicate a frequency band to each station</td>
</tr>
<tr>
<td>WDM</td>
<td>A dynamic FDM scheme for fiber</td>
</tr>
<tr>
<td>TDM</td>
<td>Dedicate a time slot to each station</td>
</tr>
<tr>
<td>Pure ALOHA</td>
<td>Unsynchronized transmission at any instant</td>
</tr>
<tr>
<td>Slotted ALOHA</td>
<td>Random transmission in well-defined time slots</td>
</tr>
<tr>
<td>1-persistent CSMA</td>
<td>Standard carrier sense multiple access</td>
</tr>
<tr>
<td>Nonpersistent CSMA</td>
<td>Random delay when channel is sensed busy</td>
</tr>
<tr>
<td>P-persistent CSMA</td>
<td>CSMA, but with a probability of p of persisting</td>
</tr>
<tr>
<td>CSMA/CD</td>
<td>CSMA, but abort on detecting a collision</td>
</tr>
<tr>
<td>Bit map</td>
<td>Round robin scheduling using a bit map</td>
</tr>
<tr>
<td>Binary countdown</td>
<td>Highest numbered ready station goes next</td>
</tr>
<tr>
<td>Tree walk</td>
<td>Reduced contention by selective enabling</td>
</tr>
<tr>
<td>MACA, MACAW</td>
<td>Wireless LAN protocols</td>
</tr>
<tr>
<td>Ethernet</td>
<td>CSMA/CD with binary exponential backoff</td>
</tr>
<tr>
<td>FHSS</td>
<td>Frequency hopping spread spectrum</td>
</tr>
<tr>
<td>DSSS</td>
<td>Direct sequence spread spectrum</td>
</tr>
<tr>
<td>CSMA/CA</td>
<td>Carrier sense multiple access with collision avoidance</td>
</tr>
</tbody>
</table>

Channel allocation methods and systems for a common channel.