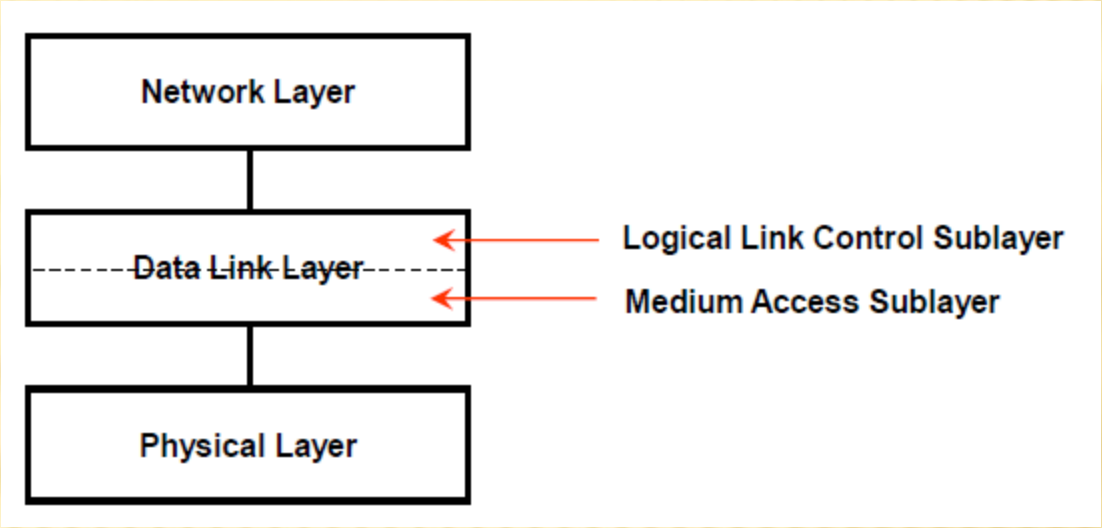
BROADBAND AND HIGH SPEED

Network Control / Management Protocols in High Speed Networks

TOPICS TO BE COVERED

Topic	No of Weeks	Contact Hours
Introduction to Broadband Networks Characteristics of High-Speed Networks	1	4
Switching Crossbar Switches Multistage Interconnection Networks (MINs) Omega Networks Delta Networks ATM Switches The Batcher-Banyan Switches High Performance Switches	2	8
Network Control/Management Protocols in High Speed Networks Medium-Access Control Protocols Routing Protocols Flow Control/Congestion Control Error Control	1	4

AN OVERVIEW OF MAC AND LLC LAYERS



- IEEE 802 standard defines:
  - Physical layer protocol
  - Data link layer protocol
    - Medium Access (MAC) Sublayer
    - Logical Link Control (LLC) Sublayer

- **Physical layer** includes topology and transmission medium
- **The data link layer** provides the functional and procedural means to transfer data between network entities and provide the means to detect and correct errors that may occur in the physical layer.
  - **The LLC sublayer** is primarily concerned with:
    - Multiplexing protocols transmitted over the MAC layer (when transmitting) and decoding them (when receiving).
    - Providing node-to-node flow and error control
  - **The MAC sublayer** enable two stations (or nodes) using a shared communication resource to establish, maintain and terminate a connection. determines who is allowed to access the media at any one time (e.g. CSMA/CD)..
    - Examples: Satellite, Ethernet, Cellular
    - The MAC sublayer is only used in broadcast or shared channel networks
    - Medium access (MAC) sublayer is **not important on point-to-point links**

MAC – MAIN TASKS

- **What is expected from Medium Access Protocols:**
  - Main task is to **minimize collisions** in order to **utilize the bandwidth** by:
    - Determining **when** a station can use the link (medium)
    - **what** a station should do when the link is **busy**
    - **what** the station should do when it is involved in **collision**
- **The methods used for Medium Access Control are:**

  - Carrier-sense multiple-access with collision detection (CSMA/CD) for bus topologies
  - Control token or Token Passing for bus and ring topologies

MAC CLASSIFICATIONS

- A *medium-access control* (*MAC*) protocol is a set of procedures used for providing access to the network users with sharing of communication resources.
- MACs are classified according to how the users access the network resource.
- *Four classes are identified:*
  - *Contention access protocols: ALOHA, CSMA, and CSMA/CD.*
  - *Demand assignment access protocols: Token ring and token bus.*
  - *Fixed allocation access protocols: TDMA, FDMA, WDMA, CDMA.*
  - *Adaptive assignment access protocols: CSMA/CD, +TDMA.*

MAC PERFORMANCE

- **Several factors affect the performance of medium access protocols in high-speed networks:**
  - The propagation delay (T_p) *is large compared with the transmission delay* (T_x).
  - The need for simple protocols.
  - Support of multimedia traffic service.

MEDIUM-ACCESS CONTROL PROTOCOLS

- **Several factors** affect the performance of medium access protocols in high-speed networks:
  - The propagation delay (T_p) is large compared with the transmission delay (T_x).
  - The need of simple protocols.
  - Support of multimedia traffic service.

EXAMPLES OF MAC PROTOCOLS

1. Slotted Ring:

- A stream of *fixed-size slots* are circulated around the ring.
- A *slot* can either be *empty* or *full*.
- When a station is ready to transmit a packet, it performs the following: with the arrival of the first empty slot, the station sets the *full/empty flag* of that slot to *full* and places a data packet on that slot.
- The source *releases* the slot as it rotate back around the ring.
- In case of the receiver does not receive the packet, the sender can be informed by the *status* of slot rotated back.

EXAMPLES OF MAC PROTOCOLS

2. Token Ring:

- Point-to-Point cables between consecutive stations.
- A token circulates around the ring when it is idle.
- A station which wants to transmit changes the token to a *header* by inverting the last bit, and starts transmission immediately.
- As bits traveled around the ring come back, they are removed by the sender.
- After the last bit has returned, the sender generates the token.

EXAMPLES OF MAC PROTOCOLS

3. Carrier Sense Multiple Access (CSMA):

- Listen to the channel before sending. If idle, send; else wait.
- Variations: *1-persistent*, *non-persistent*, *p-persistent*.
- It is possible that the channel is sensed idle while it is actually busy due to the propagation delay.
- Ethernet protocol – *CSMA/CD*. Stop as soon as a collision is detected.

ROUTING PROTOCOLS

- **Routing** is to select the **best set of links to transfer message between a source and a destination**.
- Routing protocols can be classified as follows:
  - *Centralized* or *distributed control:*
    - In *centralized control*, the route is decided by a central controller;
    - In *distributed control*, the route is decided individually.
  - *Deterministic* or *adaptive control*:
    - In *deterministic control*, the routing path is determined upon the sending of a message;
    - In *adaptive control*, the routing path should be determined as the message is routed through the network.
  - *Frequency of routing decision:*
    - The route is updated at the duration of a packet, a burst, or a call.

ROUTING PROTOCOLS

- Routing protocols in the high-speed networks may be characterized by:
  - *Call-based routing , deterministic,* with *distributed control* is appropriate.
  - Adopting a ***regular topology*** to simplify the decision of establishing a route and to reduce the memory space of the routing of the routing tables.
  - Minimizing the processing related to routing by moving the processing from *within the network* to the *edge of the network*.

EXAMPLE OF ROUTING PROTOCOLS

- *Routing schemes* in high-speed networks:
  - Asynchronous transfer mode (ATM) network routing-
  - Deflection routing
  - Source routing
  - Lightwave network routing

EXAMPLE OF ROUTING PROTOCOLS

1. Asynchronous Transfer Mode (ATM) Network Routing:

- ATM routing is basically *virtual-circuit routing* enhanced with *virtual paths*.
- In virtual-path routing, the basic principle is to group a bundle of connections with the same source and destination to form a single *virtual path*.
- The nodes need only to identify the *virtual path identity (VPI)*.
- The *virtual-circuit* is an appropriate alternative in high-speed multimedia networks because of its excellent packet delay performance achieved by little processing.

EXAMPLE OF ROUTING PROTOCOLS

2. Deflection Routing:

- When the packets arrive, each is routed to the desired outgoing link if no conflict occur; if there is a conflict, some of the competing packets are selected and routed in the remaining outgoing links.
- It is *adaptive routing*, the route assigned to a packet may be adapted to the changes of network load or network failure.
- It is proposed for *optical packet switched* networks.

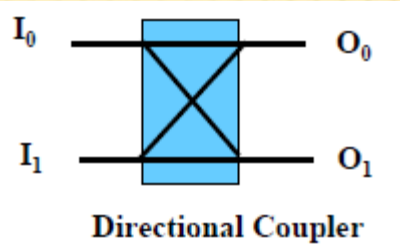
- Deflection routing suffers from:
  - Additional delay for deflected packets.
  - Potential congestion due to deflected packets will stay in the network longer.
  - Overhead due to resequencing of out-of-order packets.
- The problems of packet deflection can be alleviated by implementing a priority scheme. Priority may based on:
  - Distance to destination.
  - Number of previous deflections.

3. Source Routing:

- The processing related to routing to be moved from *within the network* to the *edge of the network*.
- **The header of a packet contains a routing control field which is divided into *n* subfields, with i^{th} subfield indicating the outgoing link label of the i^{th} transit node along the packet's path.**
- In *source routing*, route information can be carried in the packet instead of being stored in the intermediate nodes.
- The basic requirements to implement this scheme are:
  - A low error-rate channel to guarantee the error-free reception of the routing label.
  - High network bandwidth to accommodate the overhead.

4. Lightwave Network Routing:

- A signal on a link actually consists of a set of wavelengths.
- The *directional couplers* are used as switches.



- The directional coupler cannot switch the different wavelengths independently. All wavelengths on the same incoming link must be directed to the same outgoing link.

FLOW CONTROL/CONGESTION CONTROL

- Flow control/congestion control is a **set of protocols for protecting the network from overload.**
- *Congestion control* has to do with making sure the subnet is able to carry the offered traffic. It is a global issue, involving the behavior all hosts and routers.
- *Flow control* relates to end-to-end traffic between a given sender and a given receiver. Its job to make sure that a fast sender cannot continuously transmit data faster than the receiver can absorb it.

OBJECTIVES

- The *objectives* of flow control/congestion control are:
  - To prevent throughput and delay degradation due to congestion.
  - To allocate network resources fairly among competing users.
  - To prevent deadlocks.

- The operation of flow control/congestion control takes place at various layers:
  - **Data link layer:** To control the flow between two neighboring nodes in the network **(Point-to-Point flow control)**.
  - **Network Layer:** To control external traffic to network **(Congestion Control).**
  - **Transport layer:** To control information delivery from the source to the destination **(End-to-end flow control)**.

- Flow control/congestion control protocols can be classified according to the following mechanisms:
  - *Window control* versus *rate control*
  - *Feedback control* versus *open-loop control*
  - *Preventive control* versus *reactive control*
  - *Packet-based control* versus *call-based control*

No.	Flow control/congestion control Protocol	Explanation
1.	***Window-based control***	The window tells the sender how many bytes can be sent. Example: The ″Window Size″ Field of the TCP header.
2.	***Rate-based control***	Sender may send at a rate based on the **contract** with the network. The sender may adjust the rate based on the status of the network. (Refer to Resource Management Cells (RM) of ATM networks).
3.	***Feedback control***	1. Monitor the system to detect when and where congestion occurs (e.g., Routers). 2. Pass the information (*feedback*) about congestion to the sources. 3. Sources adjust their operations to correct the problem.
4.	***Open-loop control***	It minimizes congestion in the first place, rather than letting it happen and reacting after fact. It includes when to accept new traffic and when to discard packets and which ones.
5.	***Call-based control***	Flow control/congestion control algorithms deal with the whole packets during the call, and not on the packet-by packet basis.

FLOW CONTROL/CONGESTION CONTROL

- In high-speed network, processing should be reduced as much as possible.
- In general, window-based, feedback, adaptive, and packet-based types of flow control/congestion control needs intensive processing plus numerous acknowledgement and are not as suitable for high-speed networks as are the **rate-based, open-loop, Preventive control, and call-based control.**

- To achieve efficiency, high speed networks contains the following components:
  - *Admission control*
  - *Traffic policing*
  - *Congestion control*

Admission Control:

- When a new call requests a connection, the network should first decide whether it can accept this call or not.
- The **factors that affect the acceptance of a call** may include:
  - *Availability of network resources*, i.e., network bandwidth.
  - *Traffic characteristics of the new call*, e.g., maximum transmission rate, maximum packet size, token bucket rate, and token bucket size.
  - *The desired service (Quality-of-Service)*, e.g., minimum delay noticed, maximum delay variation (jitter), loss probability, etc.

Traffic Policing:

- Once a connection has been set up, the traffic source needs to be monitored to ensure that it does not violate the traffic pattern claimed in the call admission phase.

- Traffic policing schemes can be distinguished by:
  - *The logical group to be policed:* Sets of virtual circuits, or all circuits at a network access point.
  - *The scheme to determine the violation of traffic source:* e.g., the leaky-bucket scheme.
  - *Action to be taken while violation is discovered:* **Packet discarding, packet marking, or call blocking.**

Congestion Control:

- Congestion control aims to:
  - Avoid congestion inside the network.
  - Preserve the end-to-end traffic smoothness.
  - Satisfy the QOS requirements.
- Congestion causes excessive number of dropped packets and excessive delay.
- Caused by temporary overload in system.
- Controlling congestion in high speed networks is difficult because:
  - Traditional feedback schemes are not effective.
  - Processing Bottleneck.
  - Bursty traffic.

ERROR CONTROL

- Error control protocols are designed for packet recovery due to packet errors or loss due to:
  - Errors in the communication.
  - Packet misrouting in the switches.
  - Packet dropping for congestion control.
  - Network failure.

- Error detection and retransmission can be exercised at:
  - Hop-by-hop level.
  - End-to-end level.

- Error control protocols can be implemented as follows:
  - *Forward error correction* or *feedback control*.
  - *Selective-repeat, retransmission* or *go-back-N retransmission*.

- Considerations in high-speed networks:
  - *Extremely low error rate:*
  - Errors are primarily due to packet discarding for congestion.
  - *Cheap bandwidth:* Large amount of redundancy may be used to enhance the error correcting capability.
  - *Long propagation delay:* Feedback control is inefficient due to the large delay of waiting for acknowledgement.

  - In high speed networks, a good error control protocol is a hybrid of *forward error control coding* which can recover most of the errors and *selective-repeat retransmission* of erroneous packets only if necessary.