PART III

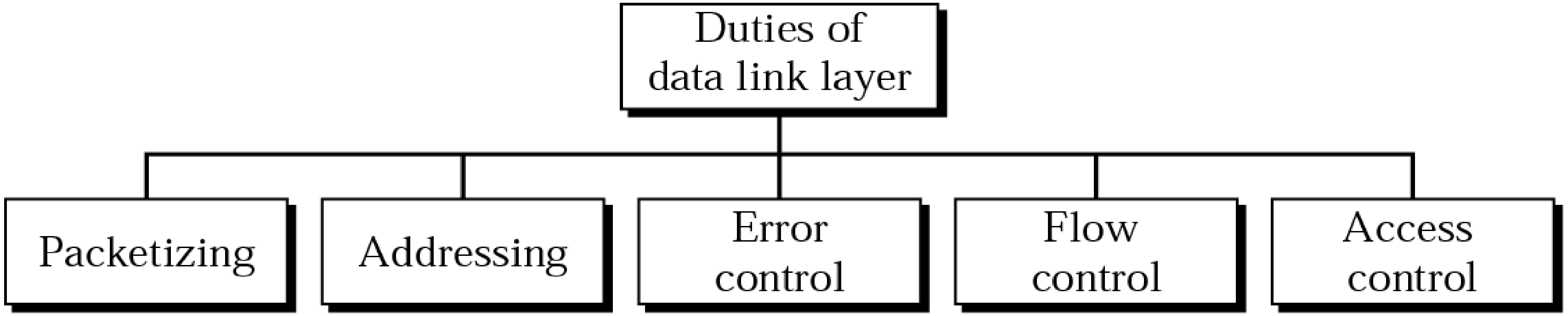
Data Link Layer

Data Link Layer

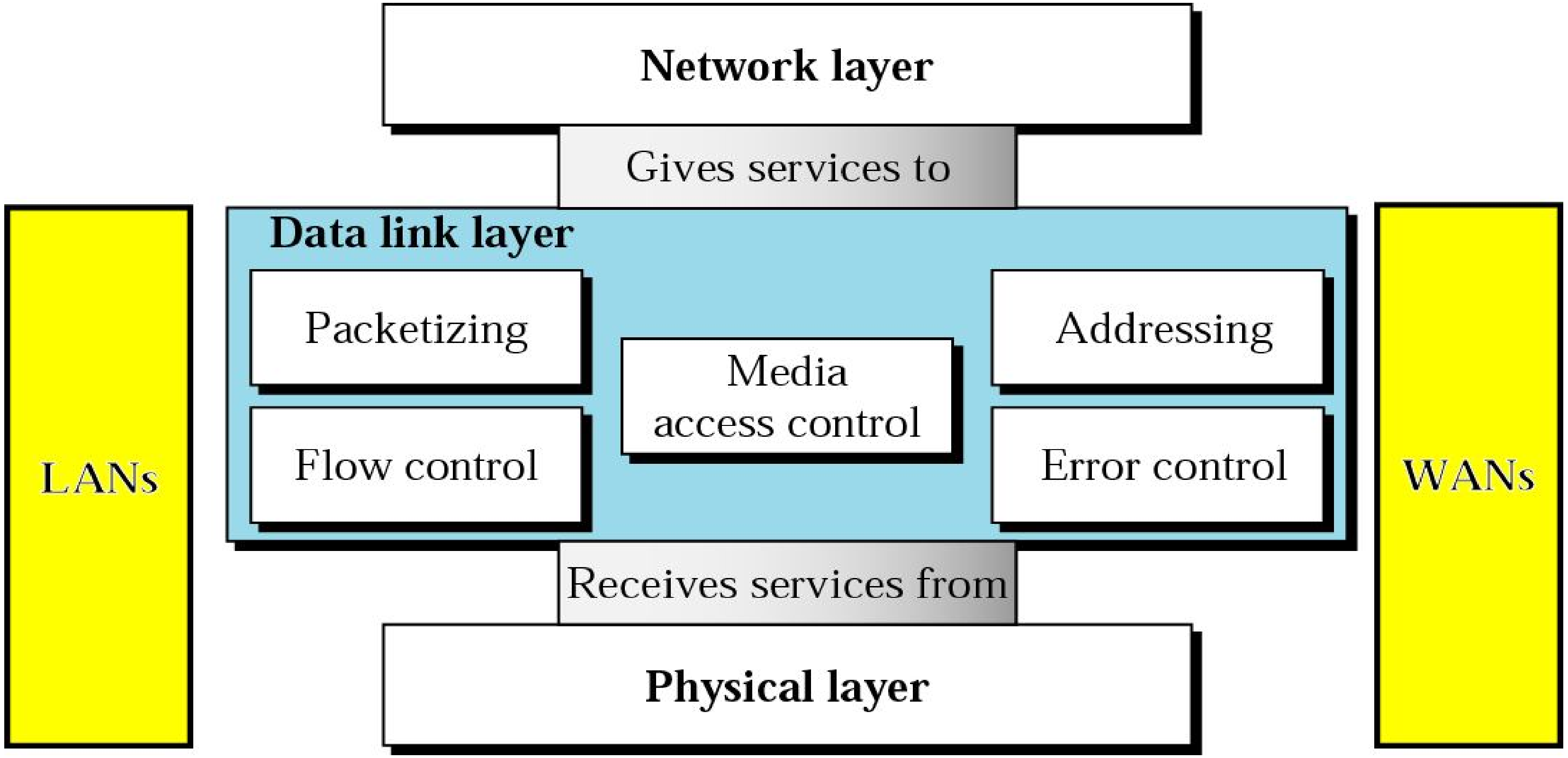
The data link layer transfers blocks of data between two nodes in a network. It is concerned with creating and transmitting frames that contain these blocks of data.

- The data link layer responsibilities include:
  - creating frames of data
  - determining where a frame starts and ends
  - physical addressing at the link level of sender and receiver
  - providing flow control to keep one node from overwhelming the other node
  - detecting transmission errors
  - providing access control to determine who has control of the link at any one time
- Devices that operate on this layer: Switches and Bridges

Data link layer duties



Position of the data-link layer



IEEE 802 Data Link sub layers

- The IEEE refined the standards and divided the Data Link layer into two sublayers: the LLC and the MAC sub layer.

- **LLC sublayer**

  LLC is short for Logical Link Control. The Logical Link Control is the upper sublayer of the Data Link layer.

  LLC masks the underlying network technology by hiding their differences hence providing a single interface to the network layer.

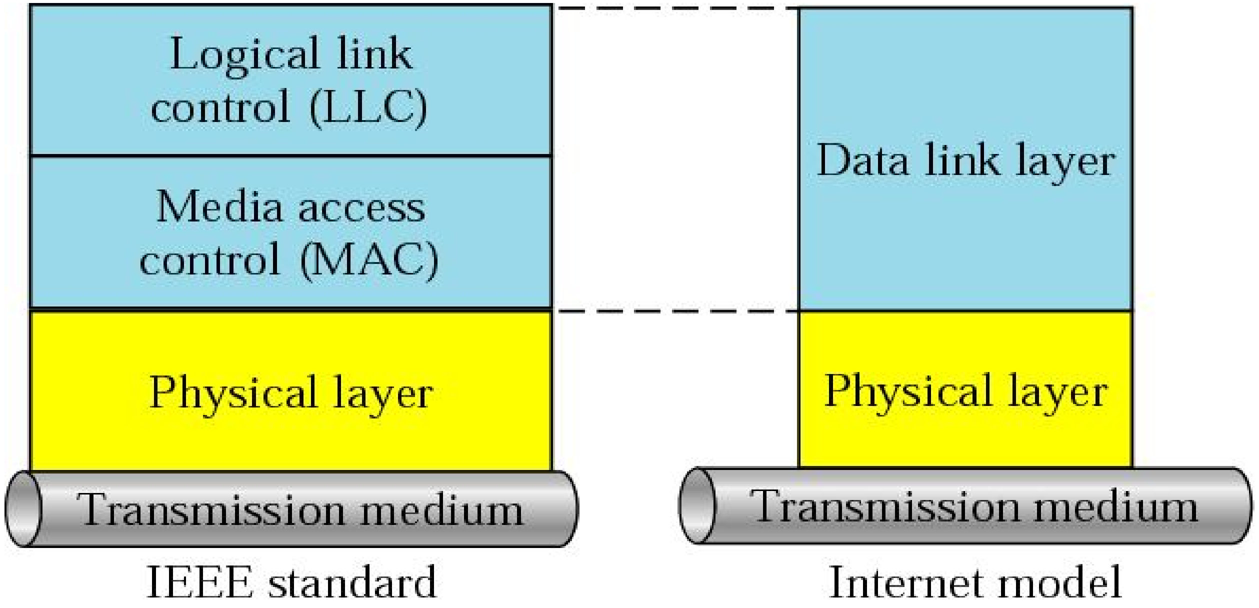
  - The LLC sublayer uses Source Service Access Points (SSAPs) and Destination Service Access Points (DSAPs) to help the lower layers communicate to the Network layer protocols acting as an intermediate between the different network protocols (IPX, TCP/IP, etc.) and the different network types (Ethernet, Token Ring, etc.)
  - This layer is also responsible for frames sequencing and acknowledgements.
  - The LLC sublayer is defined in the IEEE standard 802.2.

- **MAC sublayer**

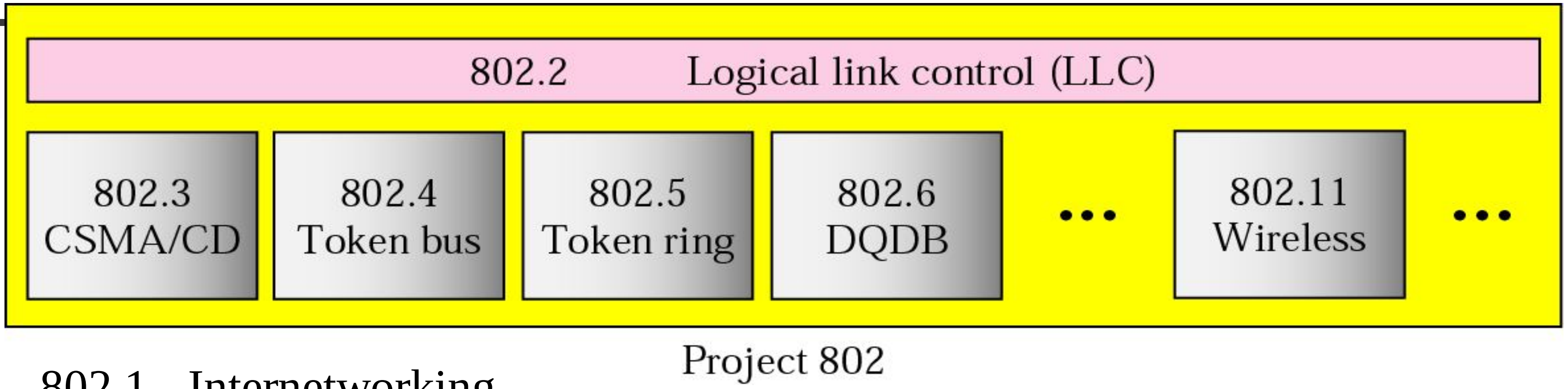
  The Media Access Control layer takes care of physical addressing and allows upper layers access to the physical media, handles frame addressing, error checking.

  - This layer controls and communicates directly with the physical network media through the network interface card. It converts the frames into bits to pass them on to the Physical layer who puts them on the wire (and vice versa)

LLC and MAC sublayers



IEEE standards for LANs



802.1 - Internetworking
802.2 - Logical Link Control *
802.3 - Ethernet or CSMA/CD*
802.4 - Token-Bus LAN *
802.5 - Token Ring LAN *
802.6 - Metropolitan Area Network (MAN)
802.7 - Broadband Technical Advisory Group
802.8 - Fiber-Optic Technical Advisory Group
802.9 - Integrated Voice/Data Networks
802.10 - Network Security
802.11 - Wireless Networks
802.12 - Demand Priority Access LAN, 100 Base VG-AnyLAN
802.13 – Not assigned
802.14 - Cable modem
802.15 - Bluetooth
802.16 - Wireless MAN (Broadband WMANs)

Data Link layer addresses

- BIAs (Burned-in Address), physical address and most commonly referred to as MAC address. This is a fixed address programmed into a NIC or a router interface.
  - 00-10-E3-42-A8-BC is an example of a MAC address.
  - The first 6 hexadecimal digits (3 bytes) **OUI – Organizational Unique Identifier** specify the vendor/manufacturer of the NIC,
  - the other 6 digits (3 bytes) define the host.

- The layer 2 broadcast address is
  - FF-FF-FF-FF-FF-FF.

NIC Manufacture code

- 00 00 03 SMC Standard Microsystems Corp.
- 00 00 0C CISCO Cisco
- 00 00 1B NOVELL Novell / Eagle
- 00 40 B4 3COM 3COM
- 00 AA 00 INTEL Intel
- 10 00 5A IBM IBM

MAC address types

- UNICAST – identify a single destination
- BROADCAST – identify all the computers link in the network
- MULTICAST – identify group of computers (it is not often use)
- Network Load Balancing NLB Unicast vs. Multicast
- http://msmvps.com/blogs/clusterhelp/archive/2005/08/07/61965.aspx

Network Load Balancing (NLB) Clustering

- **Unicast** - Each NLB cluster node replaces its real (hard coded) MAC address with a new one (generated by the NLB software) and each node in the NLB cluster uses the same (virtual) MAC. Because of this virtual MAC being used by multiple computers, a switch is not able to learn the port for the virtual NLB cluster MAC and is forced to send the packets destined for the NLB MAC to all ports of a switch to make sure packets get to the right destination.

- So, basically, the way NLB traffic is handled is kind of like this:
  - 1. An inbound packet for IP address w.x.y.z (NLB Virtual IP) arrives
    2. The ARP request is generated and is sent across all ports of the switch since there is no mapping at this point
    3. All of the NLB cluster nodes respond with the same MAC
    4. The switch sends the traffic to all ports because it is not able to tell which is the proper port and this leads to switch flooding

- If an NLB cluster node is using unicast, NLB isn't able to tell each node apart as they all have the same MAC. Since each NLB cluster node has the same MAC, communication between NLB cluster nodes is not possible unless each NLB cluster node has an additional NIC with a unique MAC.

Network Load Balancing (NLB) Clustering

- **Multicast** - NLB adds a layer 2 MAC address to the NIC of each node. Each NLB cluster node basically has two MAC addresses, its real one and its NLB generated address. With multicast, you can create static entries in the switch so that it sends the packets only to members of the NLB cluster. Mapping the address to the ports being used by the NLB cluster stops all ports from being flooded. Only the mapped ports will receive the packets for the NLB cluster instead of all ports in the switch. If you don't create the static entries, it will cause switch flooding just like in unicast.

- **Flooding Solutions**:
  1. Hook all NLB devices to a hub and then connect it to a port on the switch. Since all NLB nodes with the same MAC come through the same port, there is no switch port flooding.
  2. Configure a VLAN for all NLB cluster nodes to contain all NLB cluster traffic to just the VLAN and not run it over the entire switch.
  3. Use multicast and configure static mapping for the NLB cluster nodes in the switch so it only floods the mapped ports instead of the entire switch.
  4. Use port mirroring so that all ports involved in the NLB cluster mirror each other.