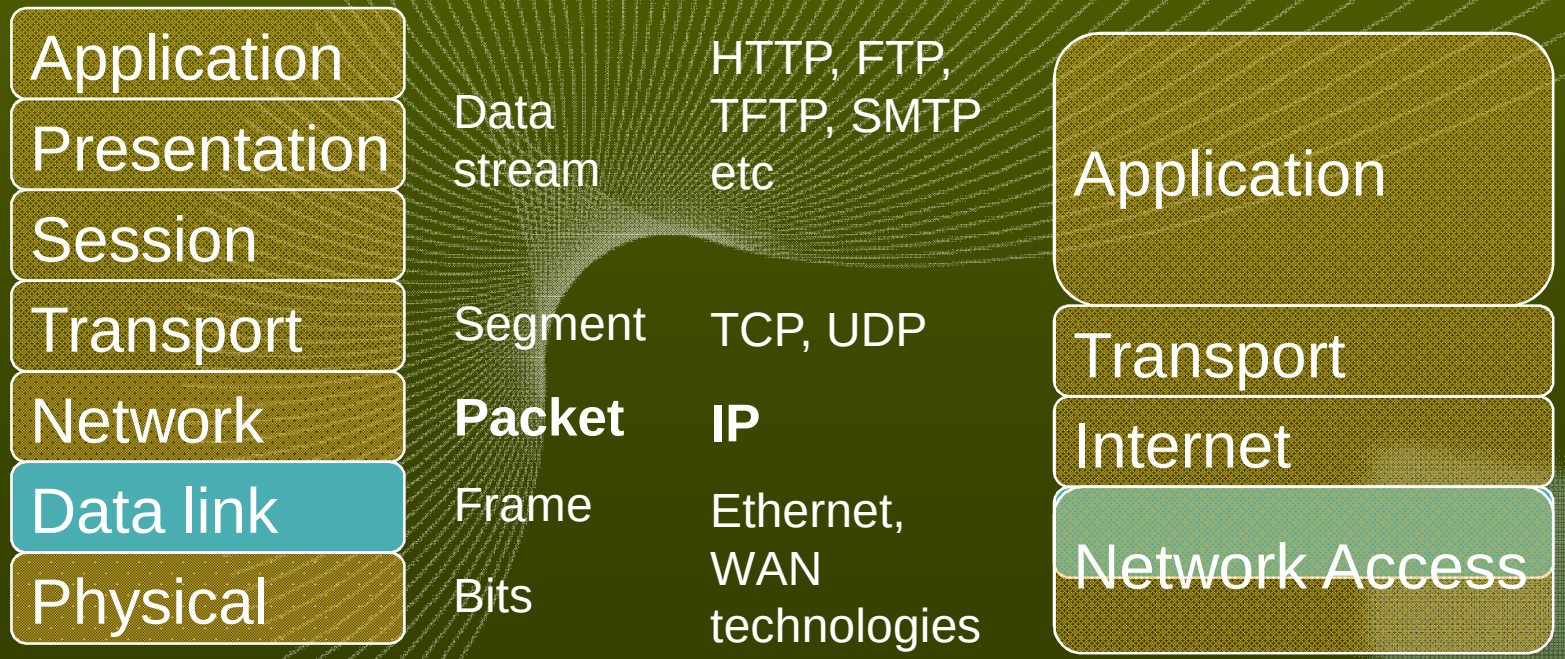
INSTITUT TEKNOLOGI TELKOM

OSI data link layer

OSI data link layer

- **OSI model layer 2**
- **TCP / IP model part of Network Access layer**



Data link layer topics

- Data Link layer protocols
- Preparing data for transmission
- Media access control methods
- Logical network topologies
- Encapsulating packets into frames
- Layer 2 frame structure and header and trailer fields

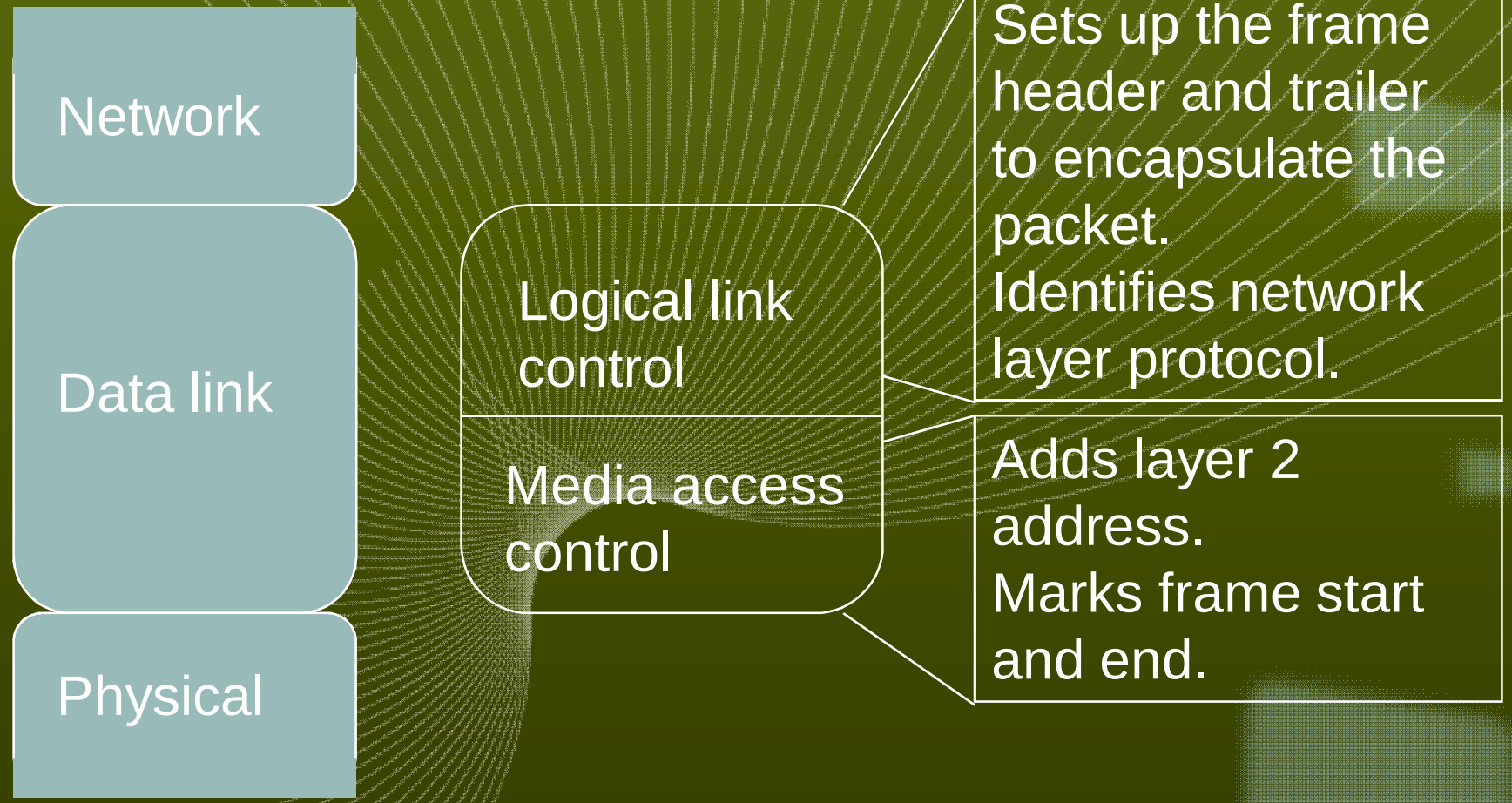
Functions of data link layer

- Encapsulates packets by adding a frame header and trailer including appropriate addressing.
- Controls access to the transmission medium.

Hops

- There may be a different layer 2 protocol in use on each hop of a journey.
- Different media, different types of link, different bandwidths, LAN/WAN affect the choice of protocol.
- Different protocols have different frames.
- The router removes the old frame and adds a new header and trailer for the next hop.

Sublayers


Network
Data link
Physical
Logical link control
Media access control
Sets up the frame header and trailer to encapsulate the packet.
Identifies network layer protocol.
Adds layer 2 address.
Marks frame start and end.

Standards

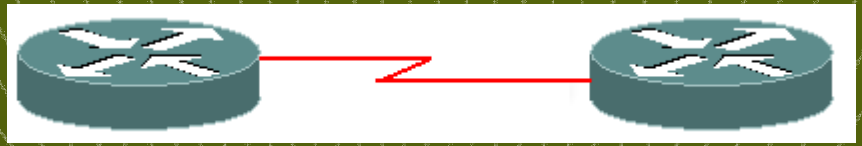
Institute of Electrical and Electronics Engineers

- **IEEE 802.2 Logical link control**
- **IEEE 802.3 Ethernet**
- **IEEE 802.5 Token ring**
- **IEEE 802.11 Wi-fi**

International Telecommunication Union (ITU)

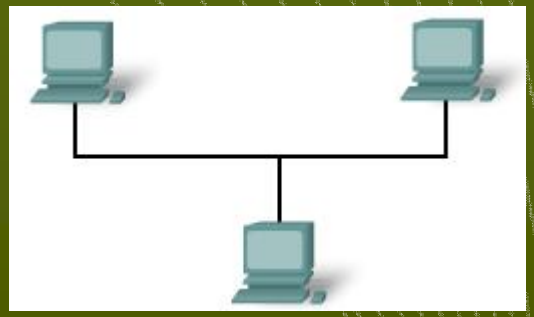
- **Various WAN standards: HDLC, ISDN, Frame relay**

Point to point link

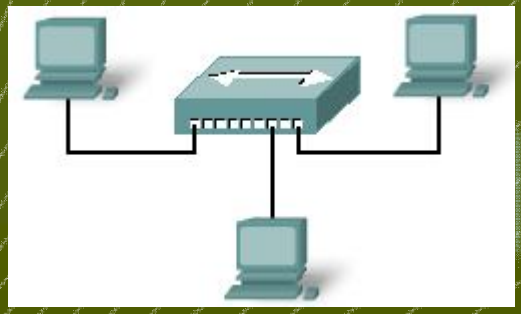


- Only two devices on the network
- Full duplex: both can send at the same time, no problem with media access
- Half duplex: data can only travel one way at a time so one device can send at a time. Simple media access control.

Shared medium



Physical bus

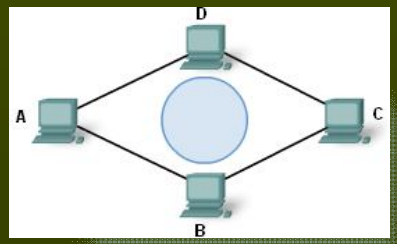


Star with hub

- Needs media access control.
- If there is no control there will be many collisions and the frames will be destroyed.

Controlled media access

- Predictable, deterministic.
- Each device is given a time when it may send, and it most not send at any other time.
- High overhead.
- No collisions.
- Token passing – each host in turn gets the token and is allowed to send.
- E.g. token ring, FDDI



Contention based media access

- Non-deterministic, first come first served.
- Each device “listens” and sends when the medium seems to be clear.
- Low overhead.
- Collisions occur.
- Need a way of re-sending lost frames.
- Becomes inefficient on large networks.
- E.g. traditional Ethernet.

Variation on contention based

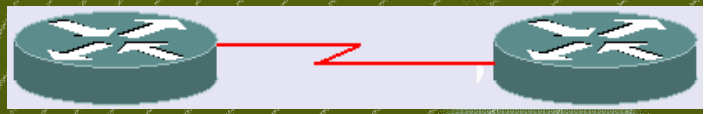
- Traditional Ethernet uses CSMA/CD (collision detection): collisions are allowed and detected, frames sent again.
- Wi-fi uses CSMA/CA (collision avoidance): when the medium is clear, host sends signal to say it is about to use the medium. It then sends.

Different environments

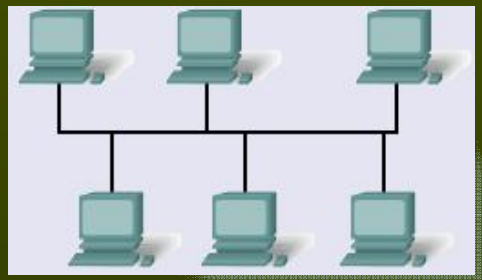
- **Fragile environment e.g. satellite link**
  - frames are likely to be lost – need large overhead of control mechanisms to make sure data arrives.
- **Protected environment e.g. modern LAN – frames not often lost – do not need such elaborate control mechanisms**
- **Therefore need different layer 2 protocols**

Addressing needs

- Point to point link – only one possible destination. Minimal addressing.

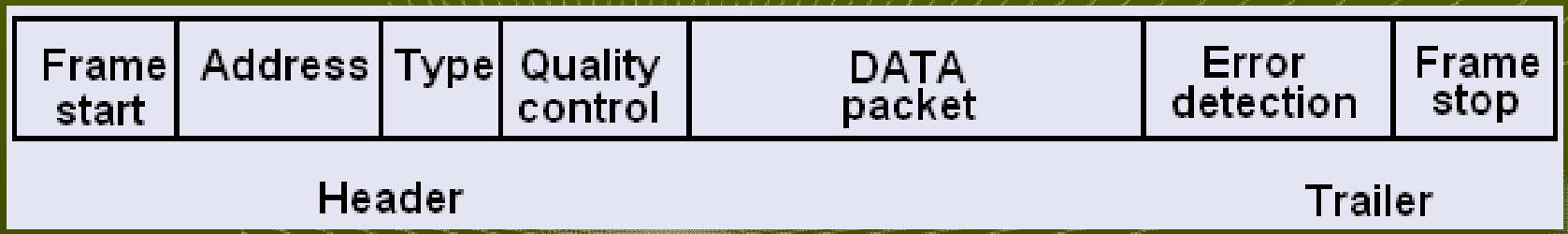


- Multi-access network – need full addressing system.
- Therefore need different layer 2 protocols.



Layer 2 frame format

- All protocols have the same general form but there are variations.



PPP frame

- **Point to point links. Minimal addressing. Control mechanisms.**

Flag	Address	Control	Protocol	Data	FCS
1 byte	1 byte	1 byte	2 bytes	variable	2 or 4 bytes

Start

Minimal address

Packet

Check and stop

Ethernet frame

- Multi-access links. Full addressing. No control field.
- Same for all Ethernet types/bandwidths.

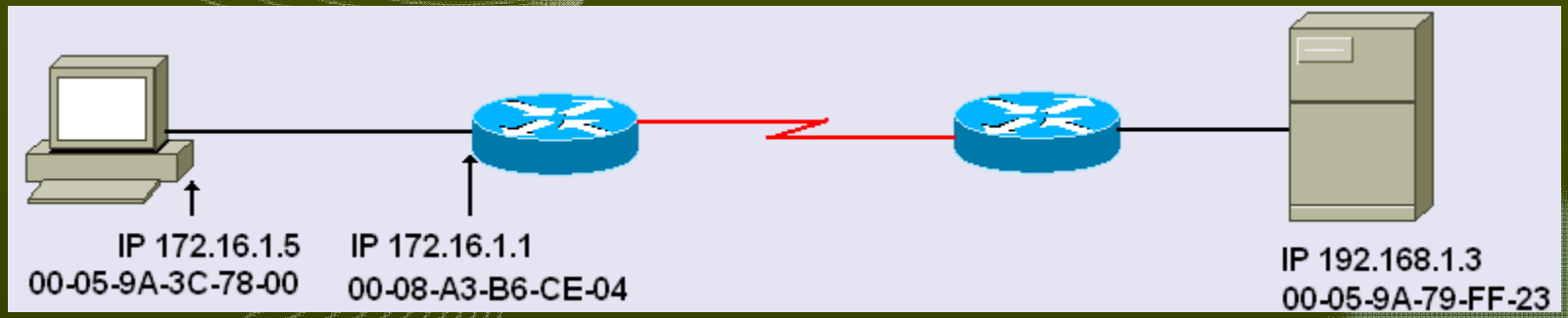
Preamble	Destination	Source	Type	Data	Frame Check Sequence
8 bytes	6 bytes	6 bytes	2 bytes	46 - 1500 bytes	4 bytes
Timing and start	Addresses 48 bits each		Layer 3 protocol	Packet	Check and stop

802.11 Wi-Fi

- LAN wireless protocol
- Fragile environment – lots of interference, risk of lost frames, contention.
- Every transmission needs to be acknowledged.
- No acknowledgement – re-send frame.
- Lots of control mechanisms in frame.

End to end

- PC sends packet to server
- Packet header has PC IP address and source and server IP address as destination.
- Frame header has PC MAC address as source and router MAC address as destination.



Within a LAN

- Hubs and switches link hosts