i341

Networks and Distributed Applications

Local Area Network Overview

Definition of a LAN:

Local Area Networks are high speed (Million Bits per second), privately owned, geographically limited to a building or campus (generally < 2 Km), intelligent only devices on shared media.

A LAN is designed to serve a part of an organization located in the same area (floor or building), the entire building, or a campus facility where multiple buildings are located within 2 Km of each other.

The LAN includes the media, software to manage the network, hardware to provide file and software storage and limited data processing and traffic on the LAN. The purpose of a LAN is to interconnect a group of laptops, printers, PCs, workstations and other *intelligent* devices to support resource and information sharing.

LAN Applications

- Laptops LANs
  - Low cost
  - Limited data rate
- Back end networks
  - Interconnecting large systems (servers and large storage devices)
    - High data rate ***(10/100/1000/10000 Mb)***
    - High speed interfaces
    - Distributed access
    - Limited distance ***(building. campus)***
    - No longer limited number of devices ***(large LAN switches)***

LAN Applications

- High speed office networks
- Storage Area networks
- Factory/Manufacturing networks
- Backbone LANs
  - Interconnect local LANs

Protocol Architecture

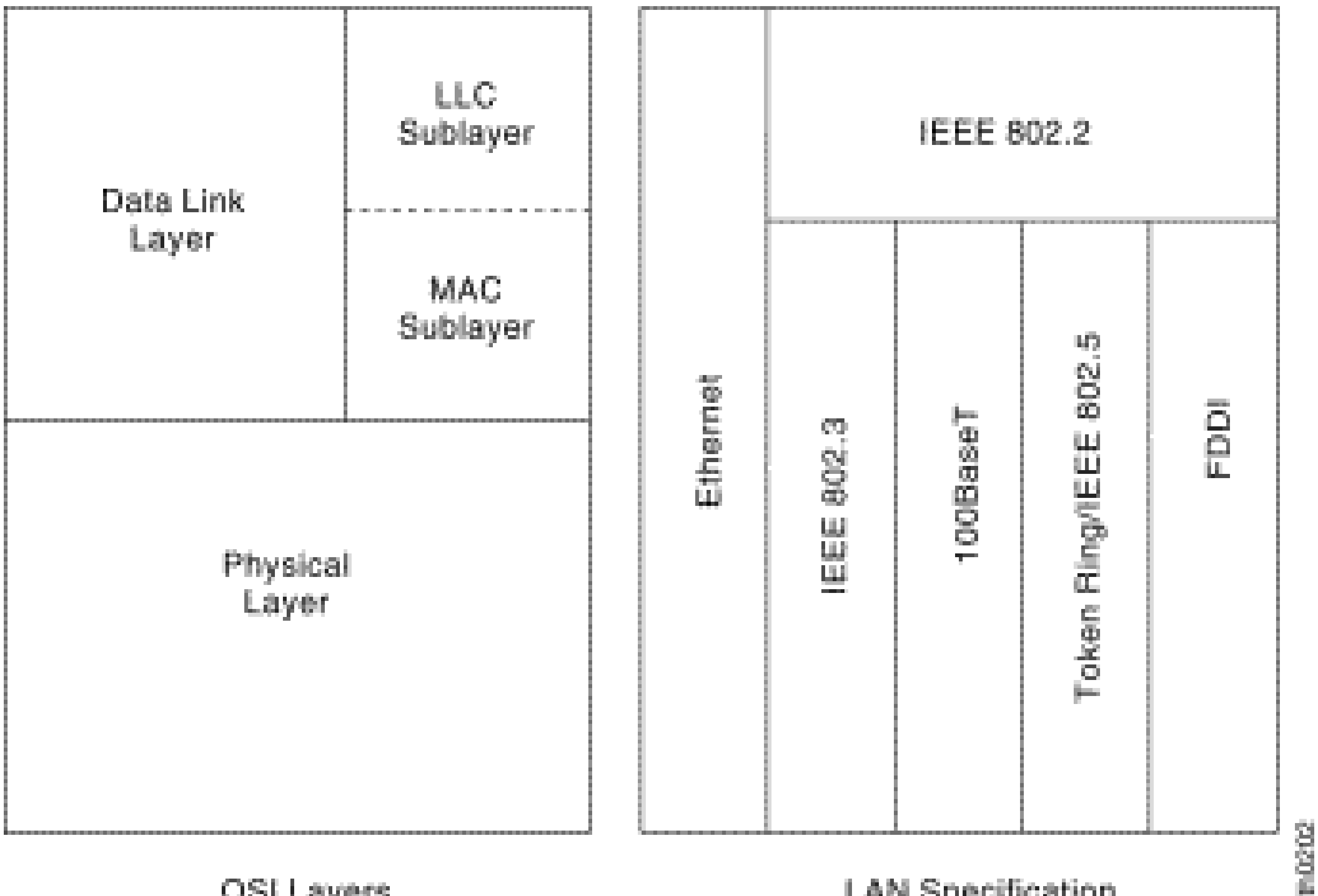
- Lower layers of OSI model
- IEEE 802 reference model
- Physical
- Media access control (MAC)
- Logical link control (LLC)

LAN Architecture

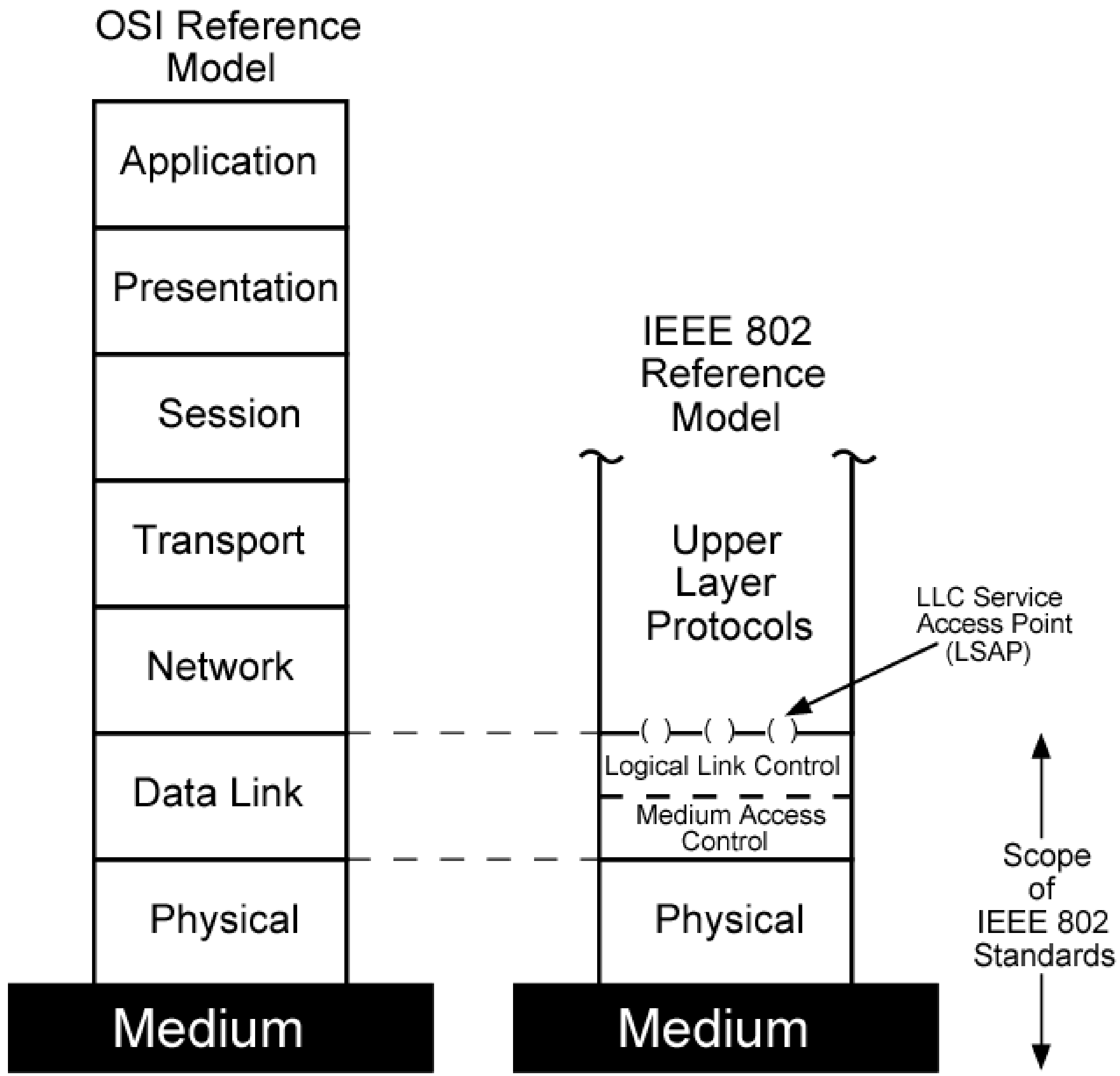
- Topologies
- Layout
- Medium access control
- Transmission medium

LAN Protocols and the OSI Reference Model

LAN protocols function at the lowest two layers of the OSI reference model, between the physical layer and the data link layer. The following illustration shows how several LAN protocols map to the OSI reference model:



IEEE 802 v OSI



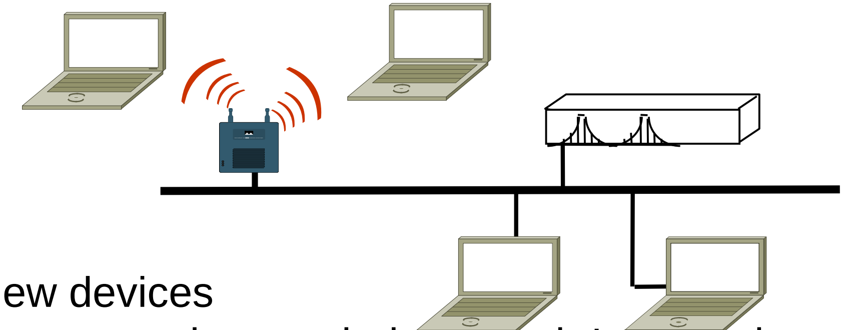
LAN Topologies

- **Bus**
- **Ring**
- **Star**

LAN Topologies:

The topology of a network concerns both the physical configuration of the cabling used to interconnect devices, and the logical manner in which systems view the structure of the communications network. The three principle network topologies utilized in LAN environments are star, bus and ring.

Bus - simply devices tapping into a single cable. Example : Baseband (Thicknet) Ethernet



Bus advantages:

Easy to tap and add new devices

Single cable vs. pt to pt connection to a hub for each LAN device

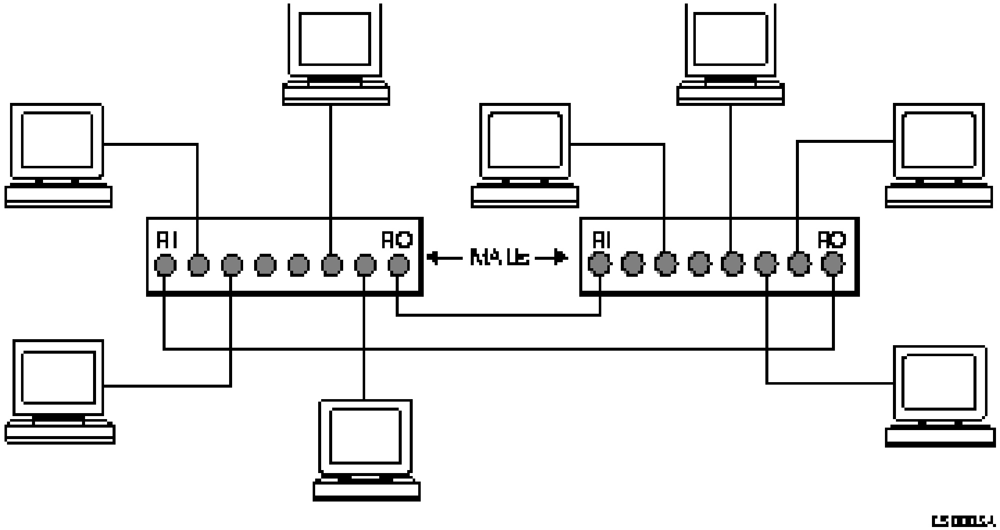
***Bus disadvantages*:**

Difficult to troubleshoot

If tap too deep, impedance can adversely affect/corrupt cable (entire LAN).

Typically Network Contention is CSMA/CD

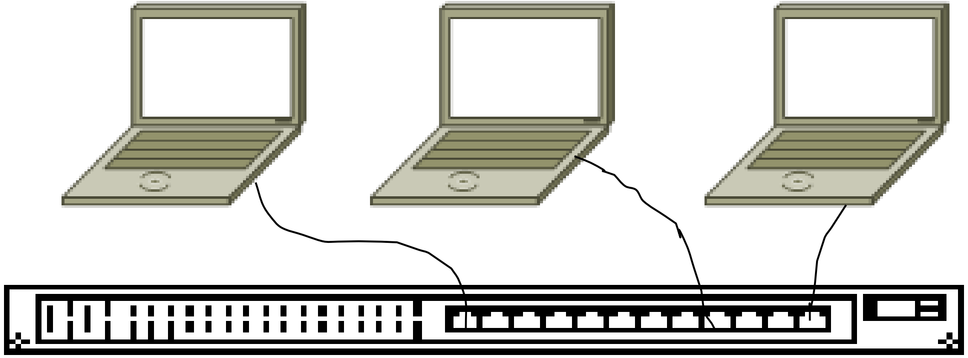
Ring Topology (Token Ring)



Stations on a Token Ring network attach to the network using a multistation access unit (MAU). Although the **Token Ring is logically a ring**, it is physically a star, with devices radiating from each MAU.

MAUs connect a limited number of devices, typically two, four, or eight. You can extend the Token Ring by connecting the Ring Out (RO) port of one MAU to the Ring In (RI) port of the next as illustrated below. You must complete the ring by connecting all RI and RO ports.

Star Topology



LAN Hub/Switch

A star topology is a LAN architecture in which the endpoints on a network are connected to a common central hub, or switch, by dedicated links. Logical bus and ring topologies are often implemented physically in a star.

***Star advantages*:**

Centralized control
Network Management Visibility
Easier to troubleshoot since each device a pt to pt connection.

***Star disadvantages*:**

Expensive investment in cable (since everything point to point).
Single Point of failure

802.3 Layers – Physical Layer

- Encoding/decoding **(Manchester Encoding)**
- Preamble generation/removal
- Bit transmission/reception
- Transmission medium **(copper, fiber, RF)**

LAN Media-Access Methods

LAN protocols typically use one of two methods to access the physical network medium: *carrier sense multiple access collision detect* (CSMA/CD) and *token passing*.

In the CSMA/CD media-access scheme, network devices contend for use of the physical network medium. CSMA/CD is therefore sometimes called *contention access*. Examples of LANs that use the CSMA/CD media-access scheme are Ethernet/IEEE 802.3 networks, including 100BaseT/1000BaseT.

In the token-passing media-access scheme, network devices access the physical medium based on possession of a token. Examples of LANs that use the token-passing media-access scheme are Token Ring/IEEE 802.5 and FDDI.

LAN Access Control Techniques:

CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance):

With CSMA/CA, a station wishing to transmit, listens to the medium and;

If the medium is idle, transmit

If the medium is busy, wait an amount of time (drawn from a probability distribution - the retransmission delay) and listen to the medium again (step 1).

If there is a collision (determined by a lack of acknowledgment), wait a random time and repeat step 1.

CSMA/CA is used by Wireless LANSs (802.11) and LocalTalk (AppleTalk) devices.

CSMA/CA Disadvantage: If two devices were to actually transmit at the same moment (given the propagation delay and distance of a larger LAN, this is a distinct possibility) If two frames were to collide, the medium remains unusable for the duration of transmission of both damaged frames. For large frames, the amount of wasted bandwidth can be considerable.

LAN Access Control Techniques:

CSMA/CD (Carrier Sense Multiple Access with Collision Detection):
With CSMA/CD, a station wishing to transmit, listens to the medium, if the medium is idle transmits. CSMA/CD differs from CSMA/CA in that it also listens while sending. If a collision is detected during transmission, a jamming signal is transmitted (by the closest device to the collision), to let all stations on the LAN know that a collision has occurred. After hearing the jamming signal, the devices (whose frames collided), wait for a random period (a random integer generated by the Network Interface/Adapter card) before attempting to transmit again. Now the amount of wasted bandwidth is reduced to the time it takes to detect a collision.

CSMA/CD is used by Ethernet and 802.3 attached devices.

CSMA/CD Disadvantage: On heavily utilized networks, being a probabilistic access method (instead of deterministic), it is possible that someone may never get access to the medium (network).

LAN Access Control Techniques:

Token Passing: With Token Passing, there is a small frame called a Token, which travels through the network. A station wishing to transmit must wait until it detects a token passing by. The station (wishing to transmit), then marks the token busy (by changing one bit in the token). This transforms the token to a Start of Frame delimiter and adds any field required to construct a valid token ring frame. The station then appends to the token ring frame any data frames it has to send to someone else on the network. When the transmitting station has either used up the allotted time slot, or finished transmission, the transmitting station inserts a new token on the network. Other stations can now wait to the token if they have anything to send, or it could return to the station (if nobody else on the network required it) to finish transmitting, if it has not.

Token Passing is utilized on BOTH ring and bus networks, IEEE 802.5 is Token Ring, and IEEE 802.4 is Token Bus. Examples of Token Bus are GM's MAP (Manufacturing Automated Protocol) and ARCnet. Token Passing is a deterministic access method. Each station is treated fairly and guaranteed access to the medium (network).

Token Passing Disadvantages: Addition overhead of the token maintenance, to recover from situations such as lost or duplicate tokens.

LAN Access Control Techniques:

Token Passing: ***Media Access Control***

Devices on a Token Ring network get access to the media through token passing. Token and data pass to each station on the ring, as follows:

1. ***The token passes around the ring until a device needs to transmit data (claims token).***

2. ***The device that wants to transmit takes the token and appends on a frame header (making it a frame).***

3. ***Each device passes the frame to the next device, until the frame reaches its destination.***

4. ***As the frame passes to the intended recipient, the recipient sets certain bits in the frame to indicate that it received the frame.***

5. ***The original sender of the frame strips the frame data off the ring and issues a new token***

MAC Frame Format

- *MAC layer receives data from LLC layer*
- *MAC control*
- *Destination MAC address*
- *Source MAC address*
- *LLC*
- *CRC*
- *MAC layer detects errors and discards frames*
- *LLC optionally retransmits unsuccessful frames*

Ethernet MAC Address Frame Formats:

Preamble	Destination Address	Source Address	Type Field	Data	CRC-32

Ethernet (DIX) V2.0 Frame:

Preamble: Ethernet uses an 8 octet preamble & no starting delimiter, actual bit pattern being the same as the 802.3 format.
Type Field: The type field identifies the upper layer protocol carried within the frame. Vendors (manufacturers) are assigned 2 Octet type fields for each major protocol they register with Xerox.

Preamble	SD	Destination Address	Source Address	Length Field	Data	PAD	CRC-32

IEEE 802.3 Frame :

Preamble: 7 Octets used for bit synchronization (Alt 1s and 0s)
SD (Start Delimiter): 1 octet used for character synchronization
Destination Add: 6 octets (MAC Address)
Source Add: 6 octets (MAC Address)
Length: 2 octets used to indicated length of data field. * (Valid Range 3 - 1500 Bytes)
PAD (0 to 46 octets) Required
CRC - Cyclic Redundancy Check: standard Frame Check Sequence to validate integrity of the Ethernet frame.

Basic Ethernet Frame Format

The **IEEE 802.3** standard defines a basic data frame format that is required for all MAC implementations, plus several additional optional formats that are used to extend the protocol's basic capability. The basic data frame format contains:

• **Preamble (PRE)—Consists of 7 bytes. The PRE is an alternating pattern of ones and zeros that tells** receiving stations that a frame is coming, and that provides a means to synchronize the frame-reception portions of receiving physical layers with the incoming bit stream.

• **Start-of-frame delimiter (SOF)—Consists of 1 byte. The SOF is an alternating pattern of ones and** zeros, ending with two consecutive 1-bits indicating that the next bit is the left-most bit in the left-most byte of the destination address.

• **Destination address (DA)—Consists of 6 bytes. The DA (MAC add) field identifies which station(s) should** receive the frame.

• **Source addresses (SA)—Consists of 6 bytes. The SA (MAC add) field identifies the sending station.**

• **Length/Type—Consists of 2 bytes. This field indicates either the number of MAC-client data bytes** that are contained in the data field of the frame, or the frame type ID if the frame is assembled using an optional format. If the Length/Type field value is less than or equal to 1500, the number of LLC bytes in the Data field is equal to the Length/Type field value. If the Length/Type field value is greater than 1536, the frame is an optional type frame, and the Length/Type field value identifies the particular type of frame being sent or received.

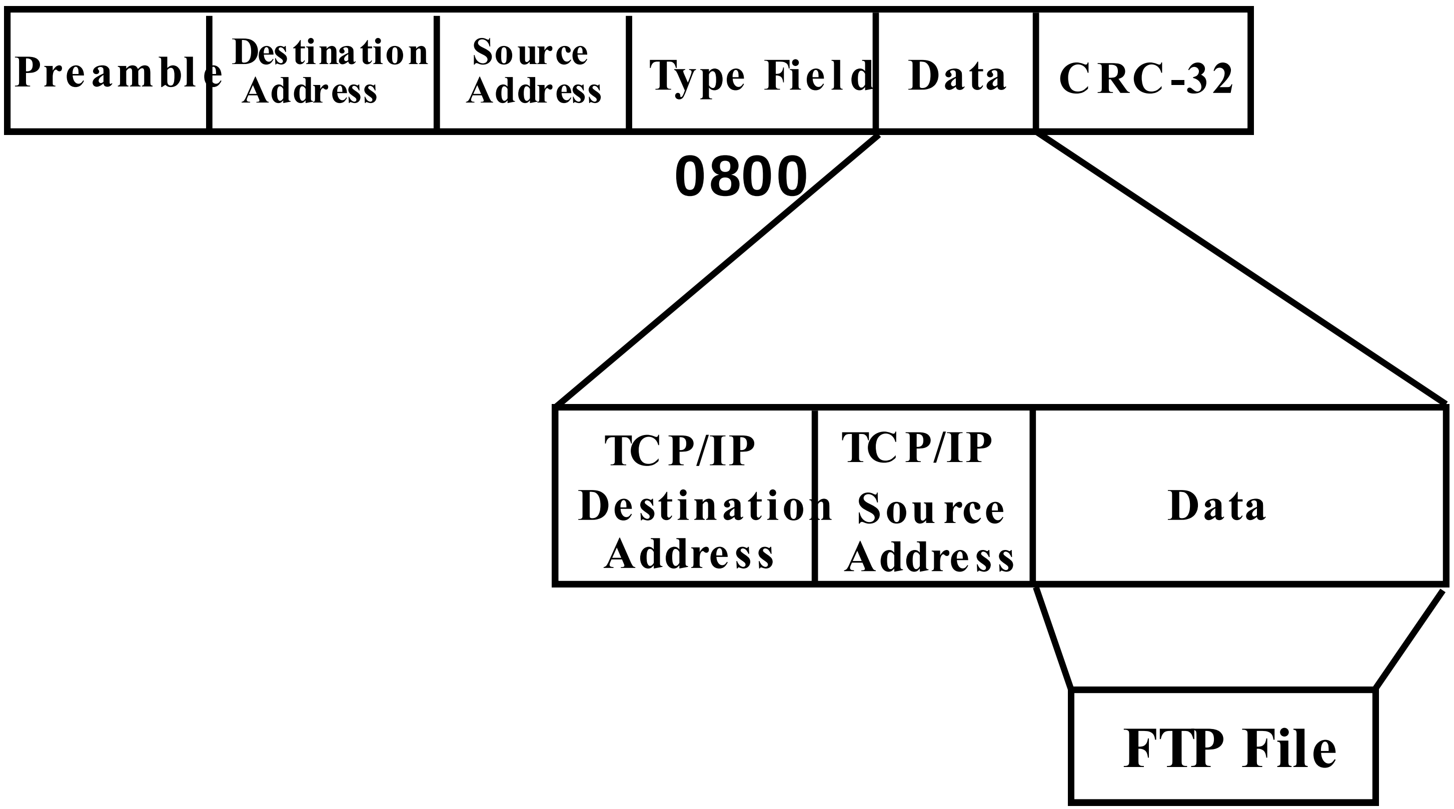
• **Data—Is a sequence of *n bytes of any value, where n is less than or equal to 1500. If the length of*** the Data field is less than 46, the Data field must be extended by adding a filler (a pad) sufficient to bring the Data field length to 46 bytes.

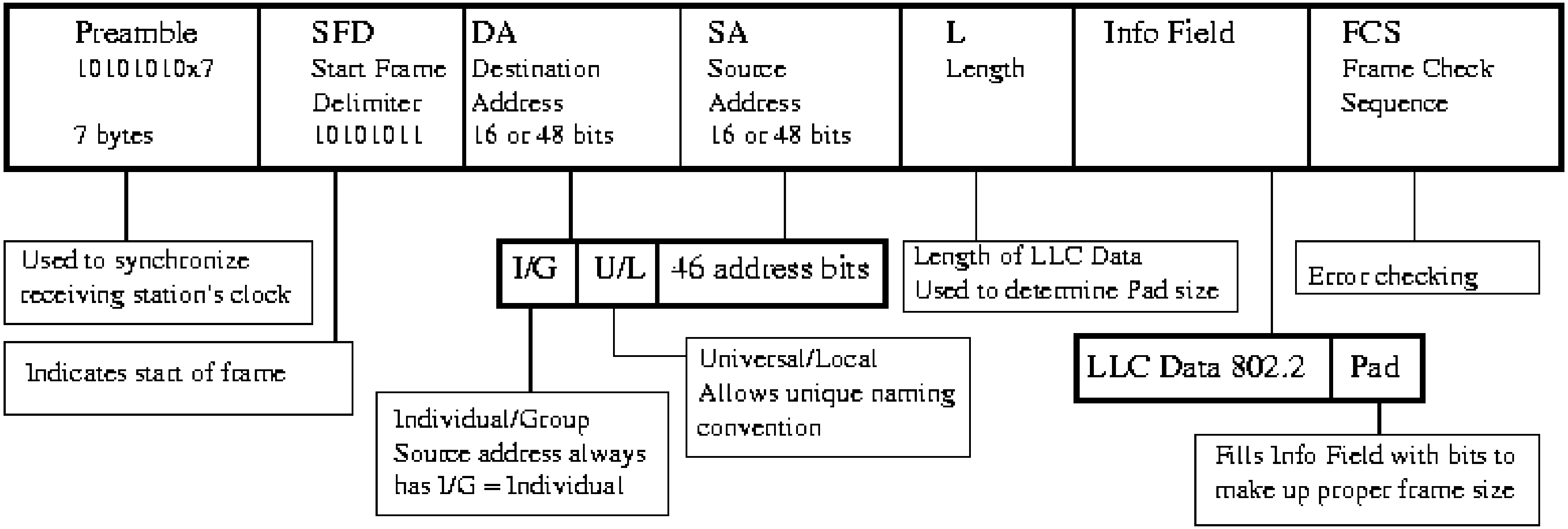
• **Frame check sequence (FCS)—*Consists of 4 bytes. This sequence contains a 32-bit cyclic*** redundancy check (CRC) value, which is created by the sending MAC and is recalculated by the receiving MAC to check for damaged frames. The FCS is generated over the DA, SA, Length/Type, and Data fields.

PDU (Protocol Data Unit)

The Data section of an Ethernet Packet may contain about anything in any format. Ethernet does not interpret the data section, except to look at the protocol type field or length. The data section must be a minimum length of 46 bytes, even if there is only 1 byte to send, and may be as large as 1500 bytes. Typically the data section would contain the protocol packet used by upper layer software such as TCP/IP, XNS, IPX, SNA, MOP, LAT....

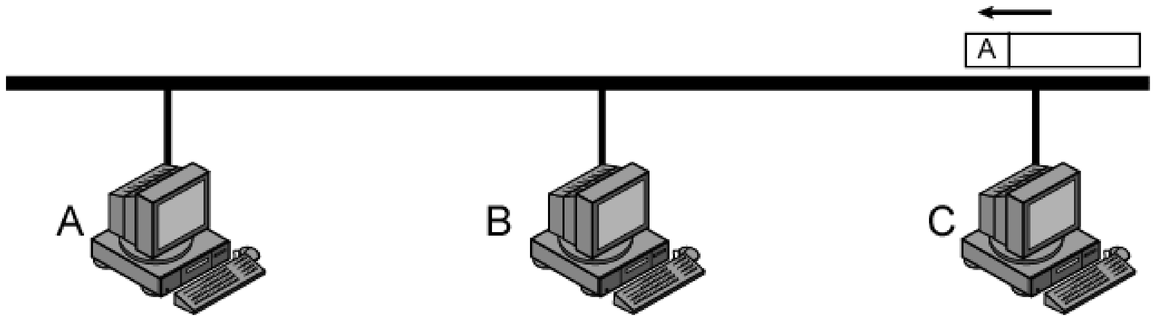
The following diagram illustrates a FTP request from an end user in a TCP/IP frame over an Ethernet network.



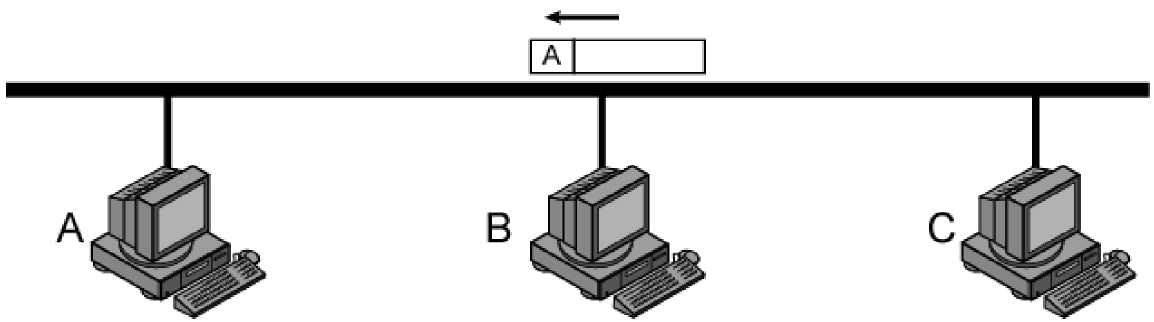


Min Size (octets)	Max Size (octets)	
Preamble	7	7
Start Frame Delimiter	1	1
Destination Address	6	6
Source Address	6	6
Length	2	2
Information Field	46	1500
Frame Check Sequence	4	4
TOTAL:	*72*	*1526 Octets*

Frame Transmission on Bus LAN

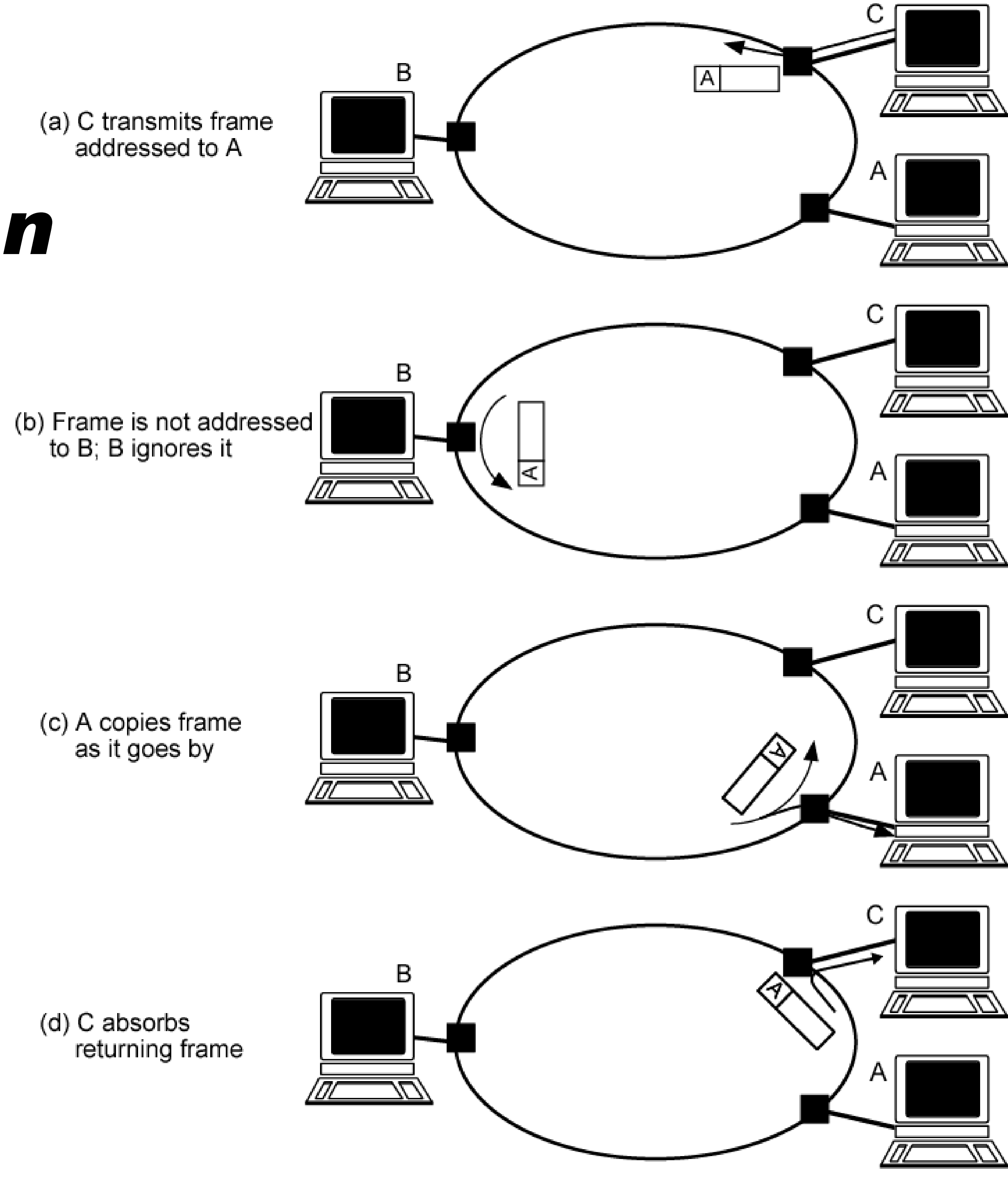


C transmits frame addressed to A



Frame is not addressed to B; B ignores it

Frame Transmission Ring LAN



Logical Link Control

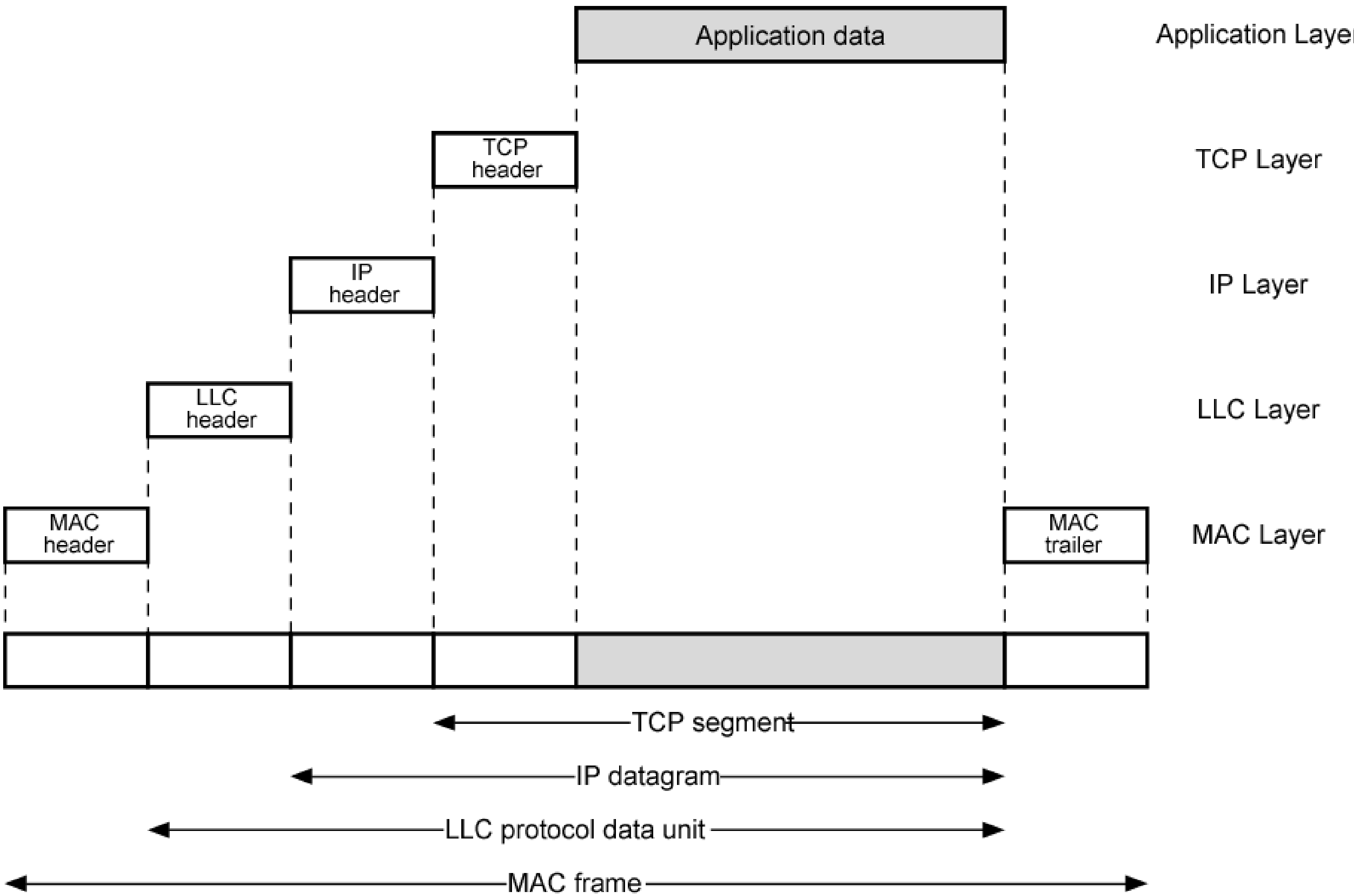
Interface to higher level protocols, Flow and error control

- Transmission of link level PDUs between two stations
- Must support multiaccess, shared medium
- Relieved of some link access details by MAC layer
- Addressing involves specifying source and destination LLC users
  - Referred to as service access points (SAP)
  - Typically higher level protocol

LLC Protocol

- Modeled after HDLC
- Asynchronous balanced mode to support connection mode LLC service (type 2 operation)
- Unnumbered information PDUs to support Acknowledged connectionless service (type 1)
- Multiplexing using LSAPs

LAN Protocols in Context



LAN Frame Types

LAN data transmissions fall into three classifications: ***unicast*, *multicast*, and *broadcast***. In each type of transmission, a single packet is sent to one or more nodes.

In a **unicast** transmission, a single packet is sent from the source to a destination on a network. First, the source node addresses the packet by using the address of the destination node. The package is then sent onto the network, and finally, the network passes the packet to its destination.

A **multicast** transmission consists of a single data packet that is copied and sent to a specific subset of nodes on the network. First, the source node addresses the packet by using a multicast address. The packet is then sent into the network, which makes copies of the packet and sends a copy to each node that is part of the multicast address.

A **broadcast** transmission consists of a single data packet that is copied and sent to all nodes on the network. In these types of transmissions, the source node addresses the packet by using the broadcast address. The packet is then sent into the network, which makes copies of the packet and sends a copy to every node on the network.

MAC Layer Protocols

MAC Layer Protocols

MAC Address Formats:

Ethernet DIX V2.0

Preamble	Destination Address	Source Address	Type Field	Data	CRC-32

Preamble: Ethernet uses an 8 octet preamble and no starting delimiter, the actual bit pattern being the same as the 802.3 format.

Type Field: The type field identifies the upper layer protocol carried within the frame. Vendors (manufacturers) are assigned 2 Octet type fields for each major protocol they register with Xerox.

Destination Add: 6 octets (MAC Address)

Source Add: 6 octets (MAC Address)

CRC - Cyclic Redundancy Check: standard Frame Check Sequence to validate integrity of the Ethernet frame

IEEE 802.3 Frame

Preamble	SD	Destination Address	Source Address	Length Field	Data	PAD	CRC-32

Preamble: 7 Octets used for bit synchronization (Alt 1s and 0s)

SD (Start Delimiter): 1 octet used for character synchronization

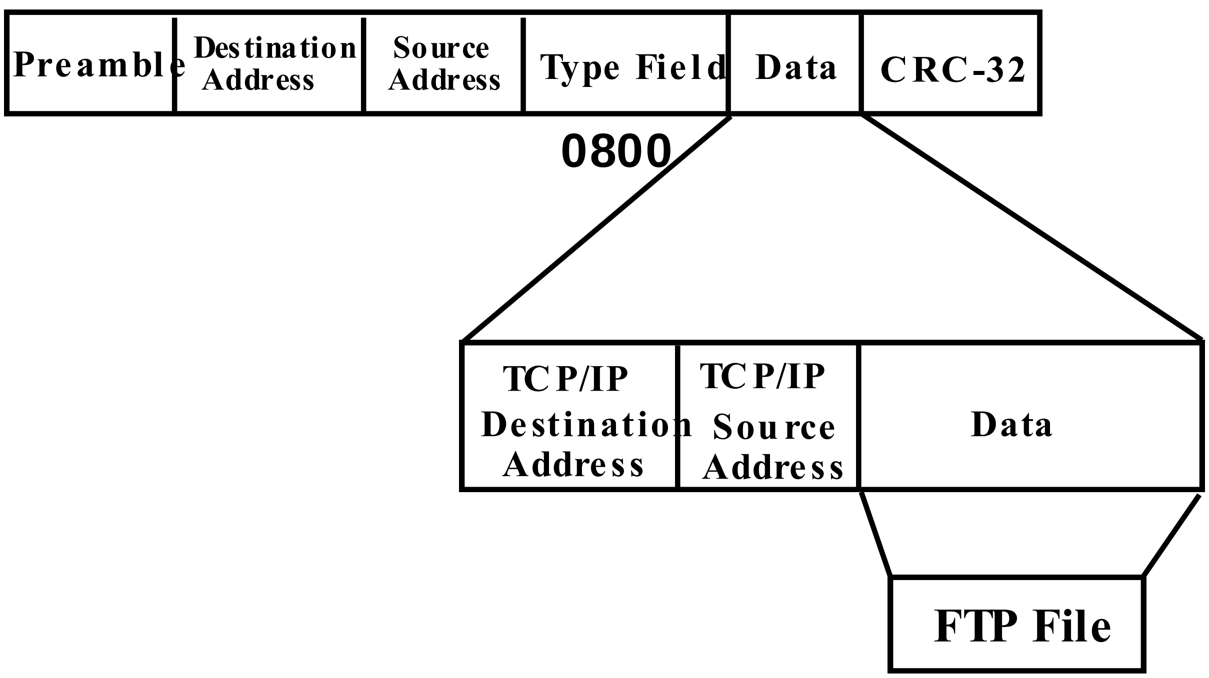
Length: 2 octets used to indicated length of data field. * (Valid Range 3 - 1500 Bytes)

PAD (0 to 46 octets) Required

MAC Layer Protocols

PDU (Protocol Data Unit)

The Data section of an Ethernet Packet may contain about anything in any format. Ethernet does not interpret the data section, except to look at the protocol type field or length. The data section must be a minimum length of 46 bytes, even if there is only 1 byte to send, and may be as large as 1500 bytes. Typically the data section would contain the protocol packet used by upper layer software such as TCP/IP, XNS, IPX, SNA, MOP, LAT....



MAC Layer Protocols

EtherNet (DIX) Ver 2 Type Fields:

Source: http://pax.cavebear.com/CaveBear/Ethernet/type.html

The 13th and 14th octets of an Ethernet or IEEE802.3 packet (after the preamble) consist of the"Ethernet Type" or "IEEE802.3 Length" field. The "Ethernet Type" values are managed by XEROX. Some assignments are public (see + below), others private. Current information includes: Xerox Public Ethernet Packet Type documentation(Xerox Courier Vol. 3 Issue 4 October 1988);
IEEE802.3 Std; NIC RFC1010; contributions from network managers and vendors.

Note	Hex	
@	0000-05DC	IEEE802.3 Length Field (0.:1500.)
+	0101-01FF	Experimental
	0200	Xerox PUP (conflicts w/ 802.3 Length Field range) (see 0A00)
	0201	Xerox PUP Address Translation (conflicts ...) (see 0A01)
	0400	Nixdorf (conflicts with 802.3 Length Field)
+*	0600	Xerox NS IDP
	0601	XNS Address Translation (3Mb only)
+*	0800	DOD Internet Protocol (IP)
+	0801	X.75 Internet
+	0802	NBS Internet
+	0803	ECMA Internet
+	0804	CHAOSnet
+	0805	X.25 Level 3
+*	0806	Address Resolution Protocol (ARP) (for IP and for CHAOS)
	0807	XNS Compatibility
	081C	Symbolics Private
+	0888-088A	Xyplex
	0900	Ungermann-Bass network debugger
	0A00	Xerox IEEE802.3 PUP
	0A01	Xerox IEEE802.3 PUP Address Translation
	0BAD	Banyan Systems
	0BAF	Banyon VINES Echo
	1000	Berkeley Trailer negotiation
	1001-100F	Berkeley Trailer encapsulation for IP

MAC Layer Protocols

Ethernet MulticastAddresses and uses

Ethernet Address	Type Field	Usage
Multicast Addresses:		
01-00-1D-00-00-00	-802-	Cabletron PC-OV PC discover (on demand)
01-00-1D-42-00-00	-802-	Cabletron PC-OV Bridge discover (on demand)
01-00-1D-52-00-00	-802-	Cabletron PC-OV MMAC discover (on demand)
01-00-5E-00-00-00 through 01-00-5E-7F-FF-FF	0800	DoD Internet Multicast (RFC-1112)
01-00-5E-80-00-00 through 01-00-5E-FF-FF-FF	????	DoD Internet reserved by IANA
01-00-81-00-00-02	????	Synoptics Network Management
01-80-C2-00-00-00	-802-	Spanning tree (for bridges)
01-80-C2-00-00-01 through 01-80-C2-00-00-0F	-802-	802.1 alternate Spanning multicast
01-80-C2-00-00-10	-802-	Bridge Management
01-80-C2-00-00-11	-802-	Load Server
01-80-C2-00-00-12	-802-	Loadable Device
01-80-C2-00-00-14	-802-	OSI Route level 1 (within area) IS hello?
01-80-C2-00-00-15	-802-	OSI Route level 2 (between area) IS hello?
01-80-C2-00-01-00	-802-	FDDI RMT Directed Beacon
01-80-C2-00-01-10	-802-	FDDI status report frame