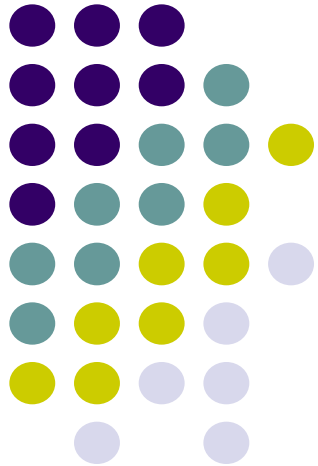
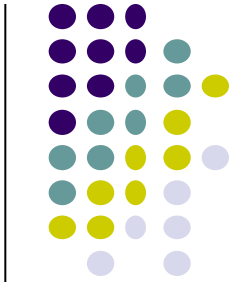
Packets, Frames and Error Detection

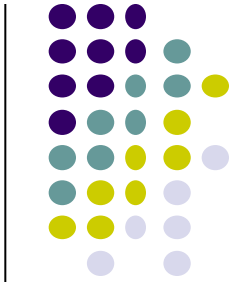


The Concept of Packets



- Most computer networks do not transfer data as an arbitrary string of continuous bits, instead the network system divides data into small blocks called *packets,* that it sends individually.
- Computer networks are often called *packet networks* or *packet switching networks* because they use packet technology.

Two Facts Motivate the Use of Packets



- 1- A sender and receiver need to coordinate transmission to ensure that data arrives correctly.
- 2- Helps ensure fairness: Because communication circuits and the associated modem hardware are expensive, multiple computers often share underlying connections and hardware. To ensure that all computers receive fair, prompt access to a shared communication facility, network system cannot allow one computer to deny access to others.

Packets and Time Division Multiplexing

- A network that permits many sources to take turns accesing a shared communication resource is providing a form of TDM.

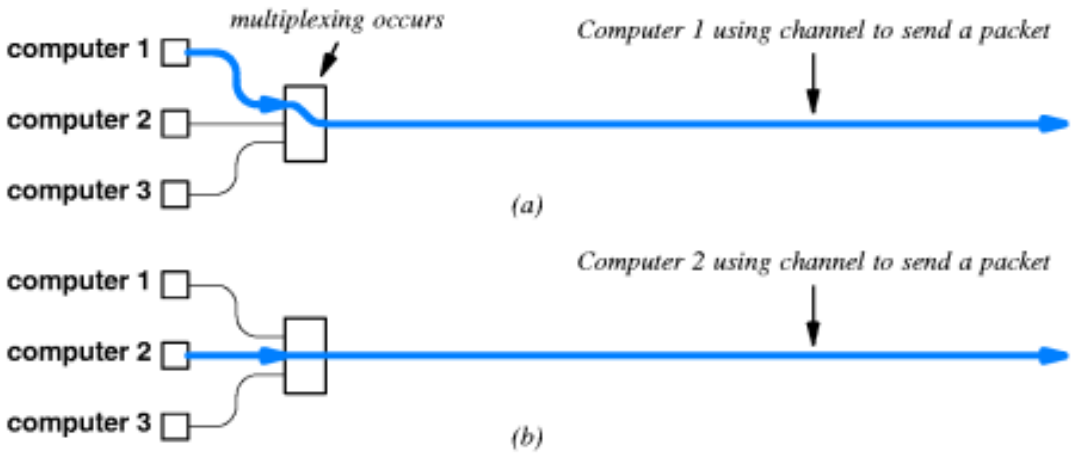
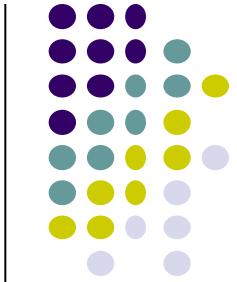
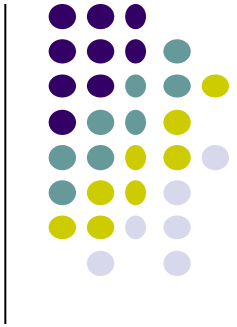


Figure 7.2 Illustration of multiplexing with packets. The sources take turns using the shared communication channel. (a) Computer *1* uses the resource to send a packet, and then (b) computer *2* uses the resource to send a packet.

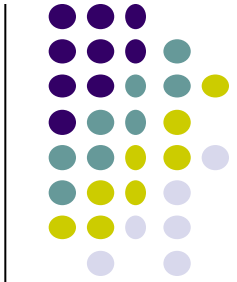


- Dividing data into small packets ensures that all sources receive prompt service because it prohibits one source from gaining exclusive access for an arbitrary long time.

Packets and Hardware Frames

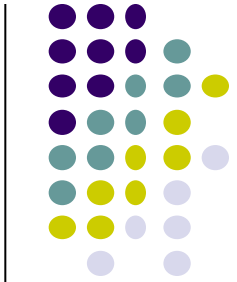


- Although the term *packet* refers to general concepts of a small block of data, there is no universal agreement on the exact format of a packet.
- Each hardware technology defines the details of packets that can be transferred on that hardware, and specifies how individual bits of the packet are transmitted. The term of *frame* is used to denote the definition of a packet used with a specific type of a network.
- A *frame* is data that is transmitted between network points as a unit complete with addressing and necessary protocol control information. A frame is usually transmitted serial bit by bit and contains a header field and a trailer field that "frame" the data. (Some control frames contain no data.)



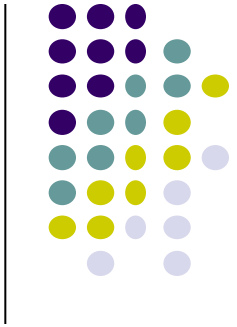
- If the data characters being carried in a frame do not include all possible values, the network system can choose two unused values and use them to mark the beginning and end of each frame.
- The sender transmits *soh* followed by the characters of data followed by *eot*.

Figure 7.3 An example frame that uses character *soh* to mark the beginning of the frame and *eot* to mark the end. The format is simple and unambiguous a receiver can tell when the entire frame has arrived, even if there are delays between characters.



- The chief disadvantage of the example framing sheme is overhead.
- The chief advantage of sending a character at the beginning and end of a frame becomes clear when one considers large delays and computers that crash.

Byte Stuffing



- To distinguish between data being sent and control information such as frame delimiters, network systems arrange for the sending side to change the data slightly before it sent, and then arrange for the receiving side to restore the original data.
- Because network systems usually insert extra bits or bytes to change data for transmission, the technique is known as *data stuffing*. The terms byte stuffing and character stuffing refer to data stuffing used with character-oriented hardware, and bit stuffing, which is more common, refers to data stuffing used with bit-oriented hardware.

Character In Data	Characters Sent
soh	esc x
eot	esc y
esc	esc z

An example of byte stuffing. For each occurrence of a character listed in the left column in the data, the sender transmits the two characters in the right column.

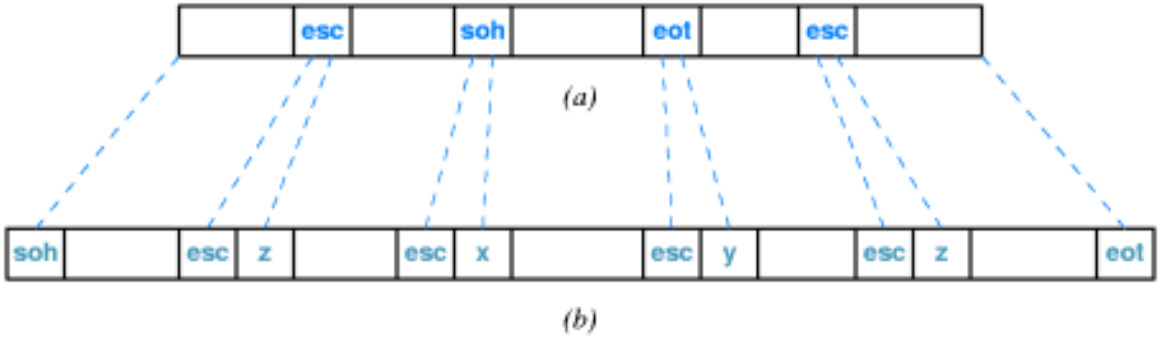
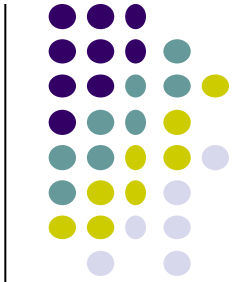


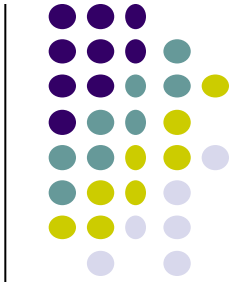
Figure 7.5 Illustration of byte stuffing, where (a) is an example of data that includes characters such as *soh*, and (b) is the frame after byte stuffing. The dashed lines show the locations in the original data where characters have been replaced or new characters added.

Transmission Errors



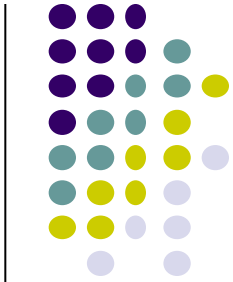
- A small change in the electrical signal can cause the receiver to misinterpret one or more bits of the data. In fact, interference can completely destroy a signal, meaning that although the sender transmits, the receiver doesnot detect that any data has arrived.
- The problems of lost, changed, or spuriously appearing bits account for much of the complexity needed in computer networks called *transmission errors.*

Parity Bits and Parity Checking



- To detect errors, network systems usually send a small amount of additional information with the data. A sender computes the value of the additional information from the data, and a receiver performs the same computation to verify that the packet was transmitted without error.
- Two forms of parity: Even and odd.

Detecting Errors with Checksums

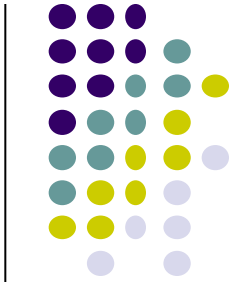


- Many computer network systems send a *checksum* along with each packet to help the receiver detect errors.
- To compute a checksum, the sender treats the data as a sequence of binary integers and computes their sum.

H	e	l	l	o		w	o	r	l	d	.
48	65	6C	6C	6F	20	77	6F	72	6C	64	2E

4865 + 6C6C + 6F20 + 776F + 726C + 642E + carry = 71FC

Figure 7.6 An example 16-bit checksum computation for a string of 12 ASCII characters. Characters are grouped into 16-bit quantities, added together using 16-bit arithmetic, and the carry bits are added to the result.

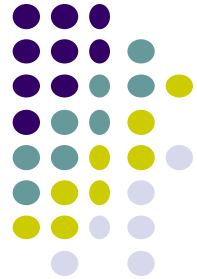


- The chief advantages arise from the size and ease of computation.
- Checksums have disadvantage of not detecting all common errors.

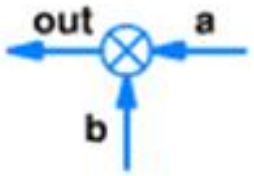
Data Item In Binary	Checksum Value	Data Item In Binary	Checksum Value
0001	1	0011	3
0010	2	0000	0
0011	3	0001	1
0001	1	0011	3
totals	7		7

Figure 7.7 Illustration of how a checksum can fail to detect transmission errors. Reversing the value of the second bit in each data item produces the same checksum.

Detecting Errors with Cyclic Redundancy Checks



- CRC techniques can detect more errors than a checksum.
- Hardware that calculates a CRC uses two simple components: a *shift register* and an *exclusive or (xor)* unit.



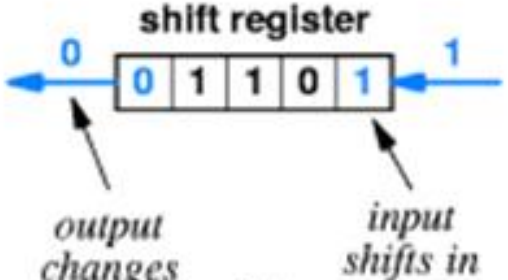
(a)

a	b	out
0	0	0
0	1	1
1	0	1
1	1	0

(b)

(a) A diagram of hardware that computes an *exclusive or*, and (b) the output value for each of the four combinations of input values. Such hardware units are used to calculate a CRC.

(a)

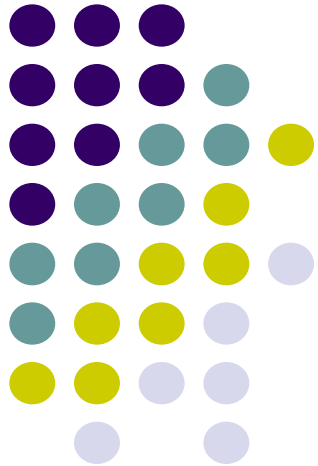


(b)

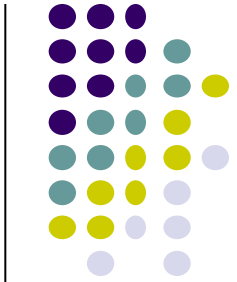
A shift register (a) before and (b) after a shift operation. During a shift, each bit moves left one position, and the output becomes equal to the leftmost bit.

Figure 7.11 A modification of the frame format from Figure 7.3 that includes a *16*-bit CRC.

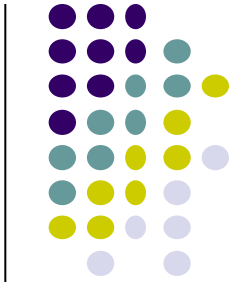
Hardware Addressing and Frame Type Identification



Specifying a Recipient

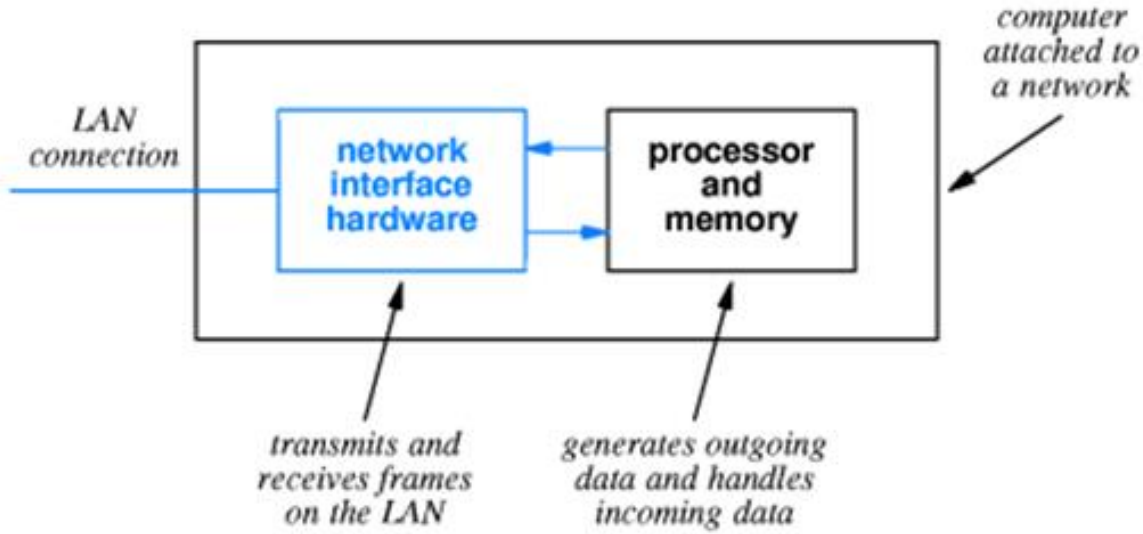


- How can two computers communicate directly across a shared medium in which all attached stations receive a copy of all signals?
  - Most LAN technologies use an addressing sheme to provide direct communication.
  - Each station on the LAN is assigned a unique numeric value called a *physical address*, *hardware address* or *media access address (MAC address)*.
- Each frame transmitted across a shared LAN includes two addresses - specifies the intended recipient and specifies the sender.



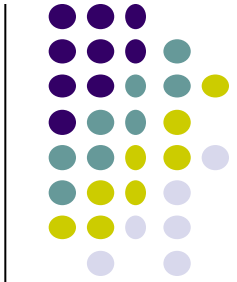
- Each frame begins with a fixed *header* that contains space for the two addresses. Locations in the header reserved for addresses a known generically as *fields*.
- The network interface hardware is designed to examine address fields in framesthat pass across the network and to accept only those frames in which the destination matches the station address.

- Because a network interface operates without using a station's CPU, a frame can be transferred across a shared LAN from one computer to another without interfering with processing on the computers.

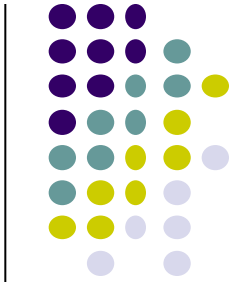


Organization of the hardware in a computer attached to a LAN. Because it is powerful and independent, the network interface hardware does not use the CPU when transmitting or receiving bits of a frame.

Format of a Phsical Address

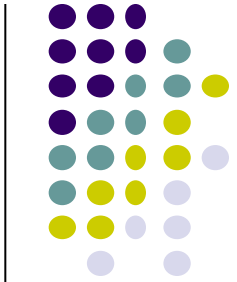


- The various address forms can be grouped into three broad categories:
  1. Static Addressing: Relies on the hardware manufacturer to assign a unique phsical address to each network interface.
  2. Configurable Addressing: Provides a mechanism that a customer can use to set a phsical address.
  3. Dynamic Addressing: Provides a mechanism that automatically assigns a phsical address to a station when the station first boots.



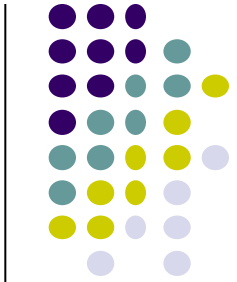
- The chief advantages of static addressing are ease of use and permanence, because a computer's adddress does not change each time the computer is rebooted.
- Dynamic addressing has two advantages:
  - it eliminates the need for hardware manufacturers to coordinate in assigning address,
  - it allows each address to be smaller.
- Configurable address provide a compromise between static and dynamic shemes; it is permanent because computer's address remains the same across reboots and it does not need to be large because the address is unique only on a given network.

Broadcasting



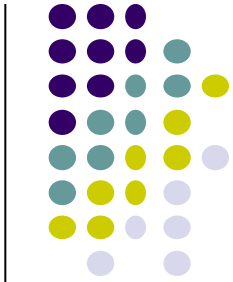
- Originally applied to radio and television transmissions, refers to transmissions that are available to a large audiance.
- When an application broadcasts data, it makes a copy of the data available to all other computers on the network.
- Broadcasts has many uses. For example; finding the printers on the network.

Multicasting



- How can computers on a shared LAN take advantage of the broadcast capability without wasting CPU resources on other computers?
- *Multicasting* is a restricted form of broadcasting.

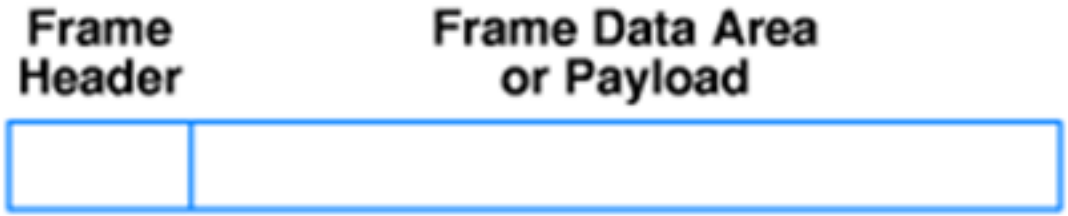
Identifying Packet Contents



- Explicit Frame Type: The bits of a frame used to identifiy the contents are called the *frame type field*, and the frame is called *self-identifying*.
- Implicit Frame Type: The frame carries only data. The sender and receiver must must agree on the contents of a frame or agree to use part of the data portion of a frame as a type field.

Frame Headers and Frame Format

- Each LAN technology defines a frame format.



The general format of a frame sent across a LAN. The header contains information such as the addresses of the sender and the recipient.

Example Frame Format

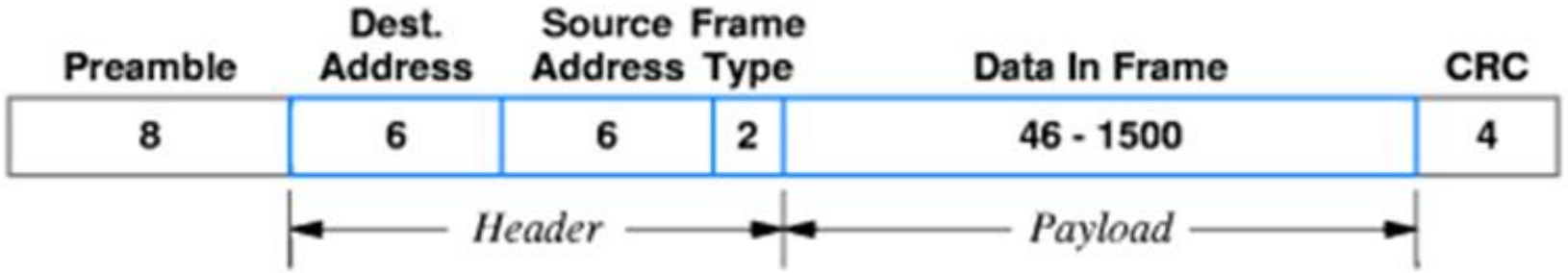
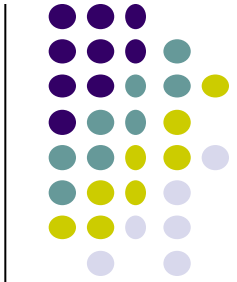


Illustration of the frame format used with Ethernet. The number in each field gives the size of the field measured in 8-bit octets.

Value	Meaning
0000-05DC	Reserved for use with IEEE LLC/SNAP
0800	Internet IP Version 4
0805	CCITT X.25
0900	Ungermann-Bass Corporation network debugger
0BAD	Banyan Systems Corporation VINES
1000-100F	Berkeley UNIX Trailer encapsulation
6004	Digital Equipment Corporation LAT
6559	Frame Relay
8005	Hewlett Packard Corporation network probe
8008	AT&T Corporation
8014	Silicon Graphics Corporation network games
8035	Internet Reverse ARP
8038	Digital Equipment Corporation LANBridge
805C	Stanford University V Kernel
809B	Apple Computer Corporation AppleTalk
80C4-80C5	Banyan Systems Corporation
80D5	IBM Corporation SNA
80FF-8103	Wellfleet Communications
8137-8138	Novell Corporation IPX
818D	Motorola Corporation
FFFF	Reserved

Examples of frame types used with Ethernet (type values are given in hexadecimal). The table lists only a few examples; many other types have been assigned.

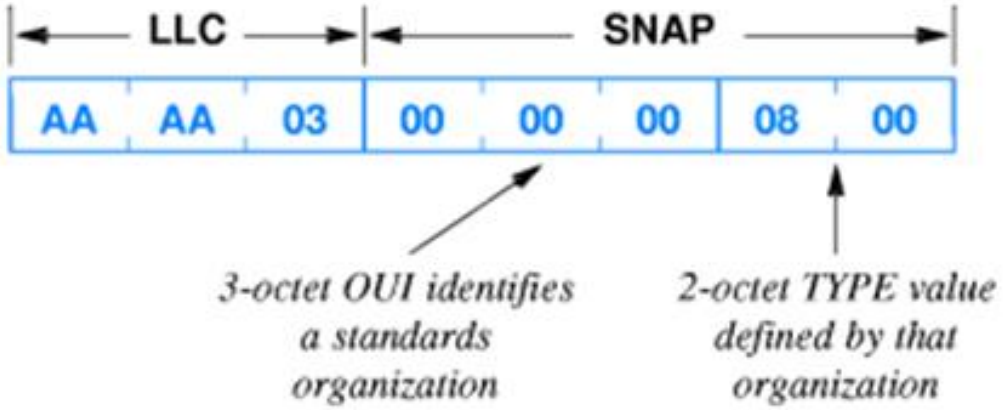
Using Networks that do not have Self-Identifying Frames



- How can computers connected to such networks know the type of data in each frame?
- Two possible approaches:
  - Before any data is sent, the sender and receiver agree to use a single format for data.
  - Before any data is sent, the sender and receiver agree to use the first few octets of data field to store type information.

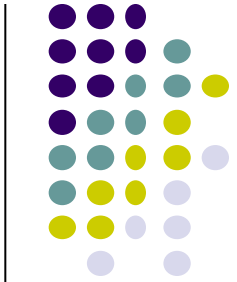
Illustration of how type information can be included in a frame's data area if the frame header does not include a type field.

- To ensure that all software agrees on values used to specify types, standards organizations have defined the meaning of each value.
- IEEE LLC/SNAP header is widely accepted.



An example of the 8-octet IEEE LLC/SNAP header, which is used to specify the type of data. The SNAP portion specifies an organization and a type defined by that organization.

Network Analyzers



- A network analyzer or network monitor is a device used to determine how well a network system is performing.