MODULE IV

Link Layer & Physical Layer

Lecture Notes

Aparna S Balan

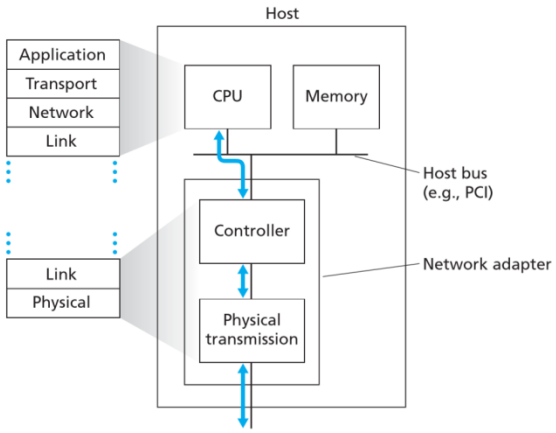
2021

VIDYA ACADEMY OF SCEINCE AND TECHNOLOGY

Introduction to the Link Layer

The basic service of any link layer is to move a datagram from one node to an adjacent node over a single communication link. Possible services that can be offered by a link-layer protocol include

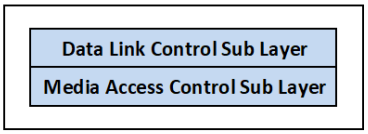
- **Framing**: All link-layer protocols encapsulate each network-layer datagram within a link-layer frame before transmission over the link. A frame consists of a data field, in which the network-layer datagram is inserted, and a number of header fields.
- **Link access**: A medium access control (MAC) protocol specifies the rules by which a frame is transmitted onto the link. The MAC protocol serves to coordinate the frame transmissions of the many nodes
- **Reliable delivery**: A link-layer protocol guarantees to move each network-layer datagram across the link without error. A link-layer reliable delivery service can be achieved with acknowledgments and retransmissions.
- **Error detection and correction**: Many link-layer protocols provide a mechanism to detect such bit errors. This is done by having the transmitting node include error-detection bits in the frame, and having the receiving node perform an error check.



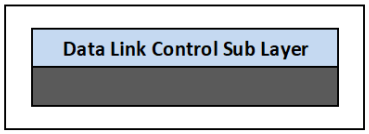
The link layer is implemented in a **network adapter**, also known as a **network interface card (NIC)**. The link-layer controller is the heart of the network adapter, which is a single, special-purpose chip that implements many of the link-layer services like framing, link access, error detection, and so on. Much of a link-layer controller's functionality is implemented in hardware. A part of the link layer is implemented in software that runs on the host's CPU. The software components of the link layer implement higher-level link-layer functionality such as assembling link-layer addressing information and activating the controller hardware. On the receiving side, link-layer software responds to controller interrupts, handling error conditions and passing a datagram up to the network layer. Thus, the link layer is a combination of hardware and software.

There are two different types of link-layer channels: broadcast channels and point-to-point communication link. **Broadcast channels** connect multiple hosts in wireless LANs, satellite networks, and hybrid fiber-coaxial cable (HFC) access networks. Here medium access protocol is needed to coordinate frame transmission. **Point-to-point communication link** connects two

routers connected by a long-distance link, or a user's office computer and the nearby Ethernet switch. Access to a point-to-point link is coordinated by Point-to-Point Protocol (PPP).



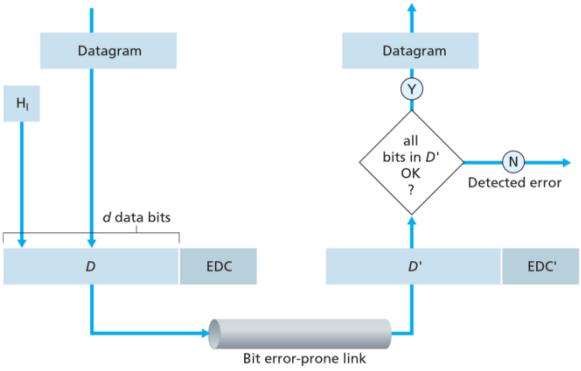
Data link layer of broadcat link



Data link layer of poin-to-point link

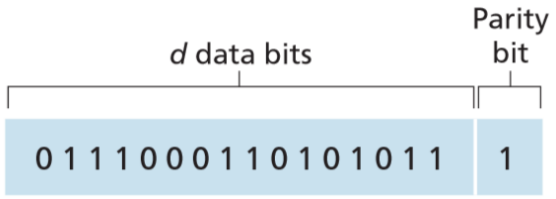
Data-Link layer is divided into two sub-layers: data link control (DLC) and media access control (MAC). These sub-layers deal with all the issues common to both point-to-point links and broadcast links.

Error Detection (Parity, Checksum and CRC)

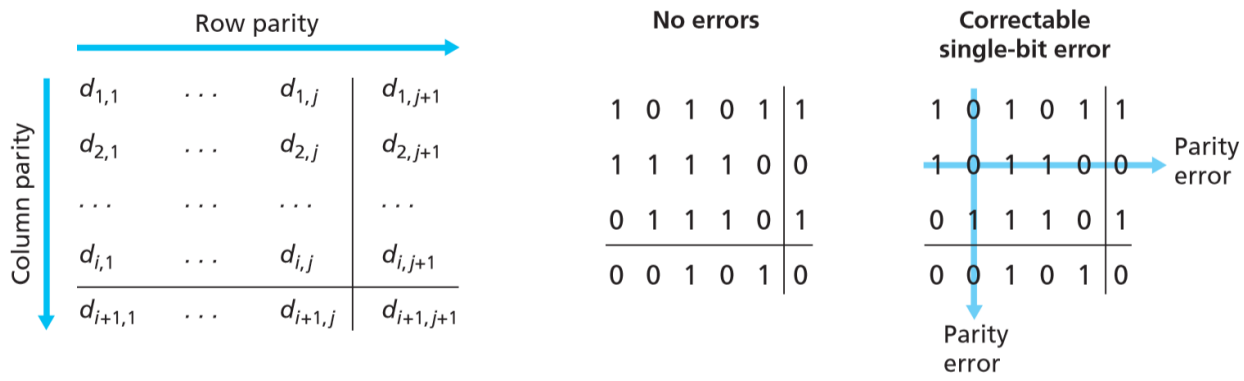


At the sending node, data, D, to be protected against bit errors is augmented with error-detection and -correction bits (EDC). Both D and EDC are sent to the receiving node in a link-level frame. At the receiving node, a sequence of bits, D and EDC is received. The D and EDC may differ from the original D and EDC as a result of in-transit bit flips. The receiver's challenge is to determine whether or not D is the same as the original D, given that it has only received D and EDC. Error-detection and correction techniques allow the receiver to sometimes detect that bit errors have occurred.

Parity Checks



The simplest form of error detection is the use of a **single parity bit**. Suppose that the information to be sent, D, has d bits. In an **even parity** scheme, the sender simply includes one additional bit and chooses its value such that the total number of 1s in the d+1 bits is even. For **odd parity** schemes, the parity bit value is chosen such that there is an odd number of 1s. The *receiver* needs only to count the number of 1s in the received d+1 bits. If an odd number of 1 valued bits are found with an even parity scheme, the receiver knows that at least one bit error has occurred. Single parity bits are not sufficient to find burst errors.



The above figure shows a two-dimensional generalization of the single-bit parity scheme. Here, the d bits in D are divided into i rows and j columns. A parity value is computed for each row and for each column. The resulting i + j + 1 parity bits comprise the link-layer frame's error-detection bits. Suppose that a single bit error occurs in the original d bits of information. With this two-dimensional parity scheme, the parity of both the column and the row containing the flipped bit will be in error. The receiver can thus not only detect the fact that a single bit error has occurred, but can use the column and row indices of the column and row with parity errors to actually identify the bit that was corrupted and correct that error. In the above figure, the 1-valued bit in position (2,2) is corrupted and switched to a 0—an error that is both detectable and correctable at the receiver.

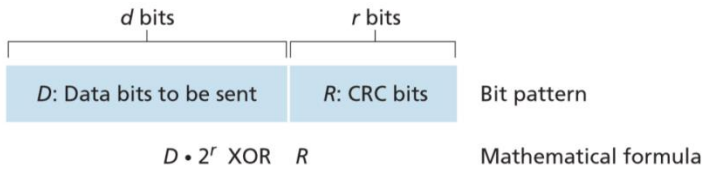
The ability of the receiver to both detect and correct errors is known as **forward error correction (FEC)**. These techniques are commonly used in audio storage and playback devices such as audio CDs. FEC techniques have the advantage that it can decrease the number of sender retransmissions required.

Checksum Methods

In checksum techniques, the d bits of data are treated as a sequence of k-bit integers. One simple checksum method is to simply sum these k-bit integers and use the resulting sum as the error-detection bits. In **internet checksum**, bytes of data are treated as 16-bit integers and summed. The 1s complement of this sum then forms the Internet checksum that is carried in the segment header. The receiver checks the checksum by taking the 1s complement of the sum of the received data and checking whether the result is all 1 bits. If any of the bits are 0, an error is indicated.

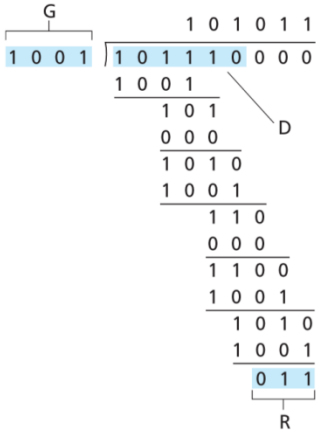
Cyclic Redundancy Check (CRC)

Cyclic redundancy check (CRC) codes are also known as **polynomial codes**, since it is possible to view the bit string to be sent as a polynomial whose coefficients are the 0 and 1 values in the bit string, with operations on the bit string interpreted as polynomial arithmetic.



Consider the d-bit piece of data, D, that the sending node wants to send to the receiving node. The sender and receiver must first agree on an r + 1 bit pattern, known as a **generator**, which will be denoted as G. The most significant (leftmost) bit of G must be a 1. For a given piece of data, D, the sender will choose r additional bits, R, and append them to D such that the resulting d + r bit pattern is exactly divisible by G using modulo-2 arithmetic. The receiver divides the d + r received bits by G. If the remainder is nonzero, the receiver knows that an error has occurred; otherwise the data is accepted as being correct. All CRC calculations are done in modulo-2 arithmetic without carries in addition or borrows in subtraction. The R is computed as

$$R = \text{remainder}\frac{D \cdot 2^r}{G}$$

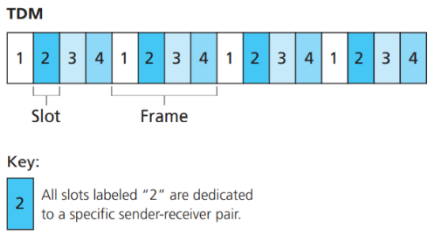


Multiple access protocols

A broadcast link, can have multiple sending and receiving nodes all connected to the same, single, shared broadcast channel. Multiple access protocols are needed in a wide variety of network settings, including both wired and wireless access networks, and satellite networks. Because all nodes are capable of transmitting frames, more than two nodes can transmit frames at the same time. When this happens, all of the nodes receive multiple frames at the same time; that is, the transmitted frames collide at all of the receivers. When there is a collision, none of the receiving nodes can make any sense of any of the frames that were transmitted. All the frames involved in the collision are lost, and the broadcast channel is wasted during the collision interval. Coordination of the broadcast channel is the responsibility of the **multiple access protocol**. Multiple access protocol can be categorised into: **channel partitioning protocols, random access protocols, and taking-turns protocols**.

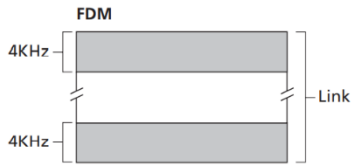
In multiple access protocol, when there is a collision, each node involved in the collision repeatedly retransmits its frame until its frame gets through without a collision. But when a node experiences a collision, it doesn't necessarily retransmit the frame right away. Instead, it waits a random delay before retransmitting the frame. Each node involved in a collision chooses independent random delays.

Channel Partitioning Protocols



Time-division multiplexing (TDM), frequency-division multiplexing (FDM) and code division multiple access (CDMA) are three techniques that can be used to partition a broadcast channel's bandwidth among all nodes sharing that channel. Assume that channel supports N nodes and that the transmission rate of the channel is R bps.

TDM divides time into time frames and further divides each time frame into N time slots. Each time slot is then assigned to one of the N nodes. Whenever a node has a packet to send, it transmits the packet's bits during its assigned time slot in the revolving TDM frame. TDM eliminates collisions and is perfectly fair: Each node gets a dedicated transmission rate of R/N bps during each frame time. Major drawbacks are: First, a node is limited to an average rate of R/N bps even when it is the only node with packets to send. A second drawback is that a node must always wait for its turn in the transmission sequence—again, even when it is the only node with a frame to send.



FDM divides the R bps channel into different frequencies (each with a bandwidth of R/N) and assigns each frequency to one of the N nodes. FDM creates N smaller channels of R/N bps out of the single, larger R bps channel. Drawback is a node is limited to a bandwidth of R/N, even when it is the only node with packets to send.

While TDM and FDM assign time slots and frequencies, respectively, to the nodes, **CDMA** assigns a different code to each node. Each node then uses its unique code to encode the data bits it sends. If the codes are chosen carefully, CDMA networks have the wonderful property that different nodes can transmit simultaneously and yet have their respective receivers correctly receive a sender's encoded data bits in spite of interfering transmissions by other nodes.

Random Access Protocols

In a random-access protocol, a transmitting node always transmits at the full rate of the channel i.e. R bps. When there is a collision, each node involved in the collision repeatedly retransmits its frame until its frame gets through without a collision. But when a node experiences a collision, it doesn't necessarily retransmit the frame right away. Instead, it waits a random delay before retransmitting the frame. Each node involved in a collision chooses

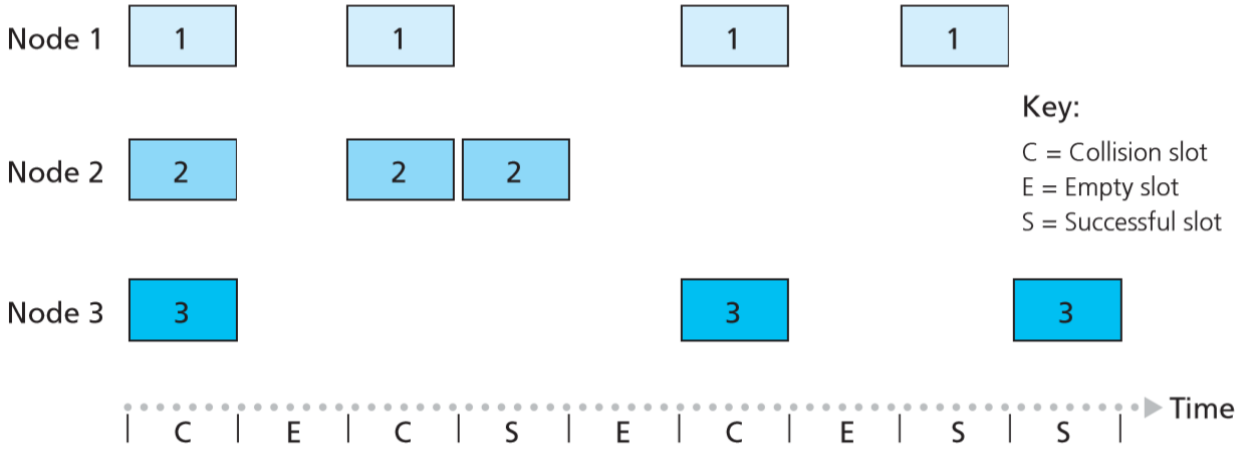
independent random delays. Following are some of the common random-access protocols: **Slotted ALOHA, Aloha (Pure Aloha) and Carrier Sense Multiple Access (CSMA)**.

Slotted ALOHA

One of the simplest random-access protocol is slotted ALOHA protocol. Here all frames consist of exactly L bits. Time is divided into slots of size L/R seconds. Nodes start to transmit frames only at the beginnings of slots. The nodes are synchronized so that each node knows when the slots begin. If two or more frames collide in a slot, then all the nodes detect the collision event before the slot ends.

When the node has a fresh frame to send, it waits until the beginning of the next slot and transmits the entire frame in the slot. If there isn't a collision, the node has successfully transmitted its frame and thus need not consider retransmitting the frame. If there is a collision, the node detects the collision before the end of the slot. The node retransmits its frame in each subsequent slot with probability p (a number between 0 and 1) until the frame is transmitted without a collision.

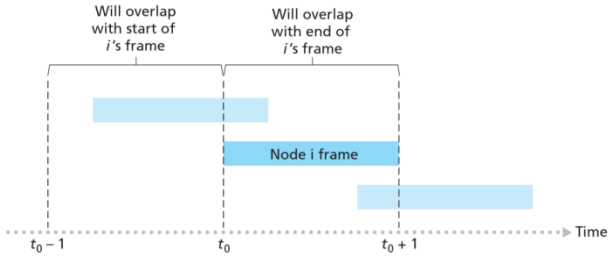
Slotted ALOHA allows a node to transmit continuously at the full rate, R, when that node is the only active node. Slotted ALOHA is also highly decentralized, because each node detects collisions and independently decides when to retransmit. Slotted ALOHA is also an extremely simple protocol.



In slotted aloha when there are multiple active nodes, a certain fraction of the slots will have collisions and will therefore be "wasted." After collision another fraction of the slots will be empty because all active nodes refrain from transmitting as a result of the probabilistic transmission policy. The only "unwasted" slots will be those in which exactly one node transmits. A slot in which exactly one node transmits is said to be a successful slot. When there are N active nodes, the efficiency of slotted ALOHA is $Np(1 - p)^{N-1}$.

Aloha (Pure Aloha)

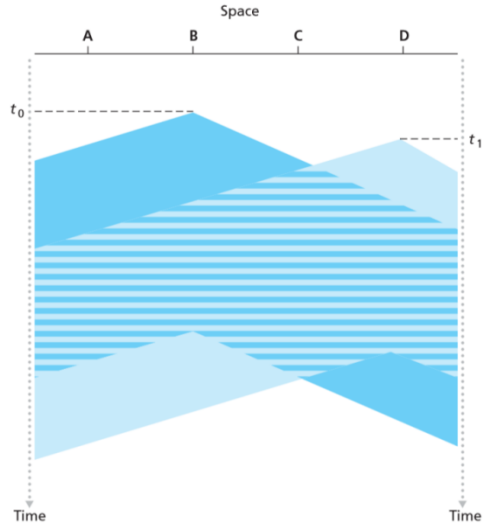
In pure ALOHA, when a frame first arrives, the node immediately transmits the frame in its entirety into the broadcast channel. If a transmitted frame experiences a collision with one or more other transmissions, the node will then immediately retransmit the frame with probability p. Otherwise, the node waits for a frame transmission time. After this wait, it then transmits the frame with probability p, or waits for another frame time with probability 1 – p.



Suppose this frame begins transmission at time t_0. In order for this frame to be successfully transmitted, no other nodes can begin their transmission in the interval of time $[t_0 - 1, t_0]$. The probability that all other nodes do not begin a transmission in this interval is also $(1 - p)^{N-1}$. Thus, the probability that a given node has a successful transmission is $p(1 - p)2^{(N-1)}$, exactly half that of slotted ALOHA.

Carrier Sense Multiple Access (CSMA)

In this a node listens to the channel before transmitting. If a frame from another node is currently being transmitted into the channel, a node then waits until it detects no transmissions for a short amount of time and then begins transmission. This property is called **carrier sensing**. A transmitting node listens to the channel while it is transmitting. If it detects that another node is transmitting an interfering frame, it stops transmitting and waits a random amount of time before repeating the sense-and-transmit-when-idle cycle. This is called **collision detection**.

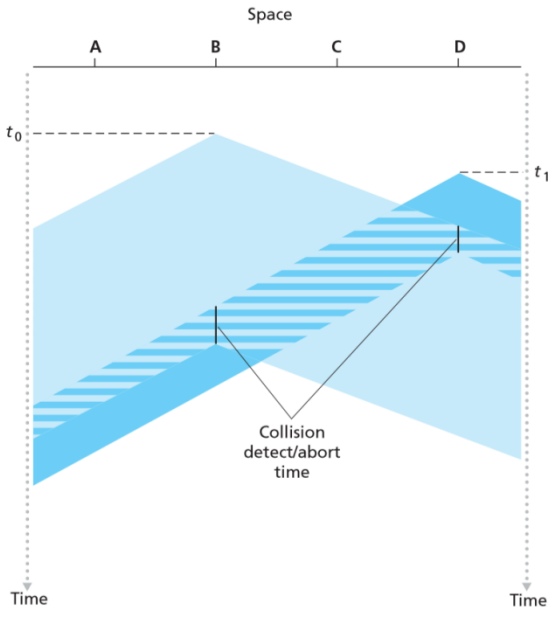


This figure shows a space-time diagram of four nodes (A, B, C, D) attached to a linear broadcast bus. The horizontal axis shows the position of each node in space; the vertical axis represents time. At time t_0, node B senses the channel is idle, as no other nodes are currently transmitting. Node B thus begins transmitting, with its bits propagating in both directions along the broadcast medium. The downward propagation of B's bits, with increasing time indicates that a nonzero amount of time is needed for B's bits actually to propagate along the broadcast medium. At time t_1 ($t_1 > t_0$), node D has a frame to send. Although node B is currently transmitting at time t_1, the bits being transmitted by B have yet to reach D, and thus D senses the channel idle at t_1. In accordance

with the CSMA protocol, D thus begins transmitting its frame. A short time later, B's transmission begins to interfere with D's transmission at D, which results in collision.

Carrier Sense Multiple Access with Collision Detection (CSMA/CD)

IN CSMA/CD when a node performs collision detection, it ceases transmission as soon as it detects a collision. The nodes abort their transmission a short time after detecting a collision. If two nodes transmitted frames at the same time and then both waited the same fixed amount of time, they'd continue colliding forever. An interval that is short when the number of colliding nodes is small, and long when the number of colliding nodes is large is a suitable choice.



The adapter in a node, obtains a datagram from the network layer, prepares a link-layer frame, and puts the frame adapter buffer. If the adapter senses that the channel is idle, it starts to transmit the frame. If the adapter senses that the channel is busy, it waits until it senses no signal energy and then starts to transmit the frame. While transmitting, the adapter monitors for the presence of signal energy coming from other adapters using the broadcast channel. If the adapter transmits the entire frame without detecting signal energy from other adapters, the adapter is finished with the frame. If, on the other hand, the adapter detects signal energy from other adapters while transmitting, it aborts the transmission. After aborting, the adapter waits a random amount of time and does the retransmission.

Taking-Turns Protocols

There are dozens of taking-turns protocols, and each one of these protocols has many variations. Two important taking turns protocols are polling protocol and token-passing protocol.

The **polling protocol** requires one of the nodes to be designated as a master node. The master node polls each of the nodes in a round-robin fashion. The master node first sends a message to node 1, saying that it (node 1) can transmit up to some maximum number of frames. After node 1 transmits some frames, the master node tells node 2 it can transmit up to the maximum number of frames. The master node can determine when a node has finished sending its frames by observing the lack of a signal on the channel. The procedure continues in this manner, with the master node polling each of the nodes in a cyclic manner.

The polling protocol eliminates the collisions and empty slots. It is efficient than random access protocols. The first drawback of polling protocol is that the protocol introduces a polling delay. The second drawback is that if the master node fails, the entire channel becomes inoperative.

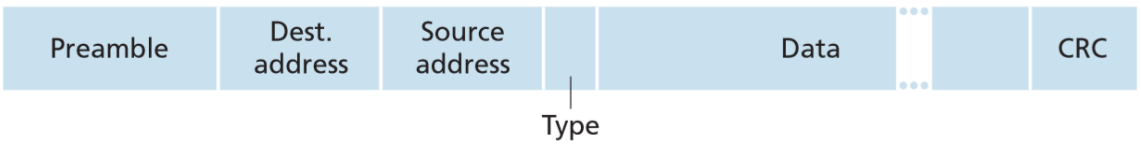
The second taking-turns protocol is the **token-passing protocol**. In this protocol there is no master node. A small, special-purpose frame known as a token is exchanged among the nodes in some fixed order. When a node receives a token, it holds onto the token only if it has some frames to transmit; otherwise, it immediately forwards the token to the next node. If a node does have frames to transmit when it receives the token, it sends up to a maximum number of frames and then forwards the token to the next node.

Advantages of token passing are decentralized nature and high efficiency. The main drawback is that the failure of one node can crash the entire channel. Another one is if a node accidentally neglects to release the token, then some recovery procedure must be invoked to get the token back in circulation.

IEEE 802.3 Ethernet

The original Ethernet LAN was invented in the mid-1970s by Bob Metcalfe and David Boggs. It was the first widely deployed high-speed LAN. Token ring, FDDI, and ATM were more complex and expensive than Ethernet. Ethernet is the most prevalent wired LAN technology. Ethernet can be installed using a hub-based star topology . A **hub** is a physical-layer device that acts on individual bits rather than frames. When a bit, representing a zero or a one, arrives from one interface, the hub simply re-creates the bit, boosts its energy strength, and transmits the bit onto all the other interfaces. Bu in future the hub was replaced by switch which resulted in a switch-based star topology.

In ethernet, a sending adapter encapsulates the IP datagram within an Ethernet frame and passes the frame to the physical layer. The receiving adapter receives the frame from the physical layer, extracts the IP datagram, and passes the IP datagram to the network layer.



- **Data field (46 to 1,500 bytes):** This field carries the IP datagram. The maximum transmission unit (MTU) of Ethernet is 1,500 bytes. This means that if the IP datagram exceeds 1,500 bytes, then the host has to fragment the datagram. The minimum size of

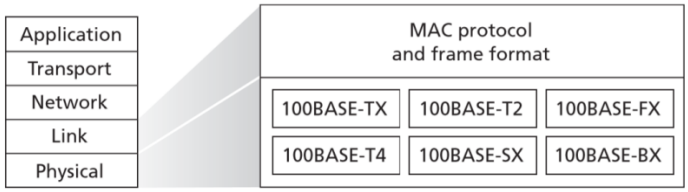
the data field is 46 bytes. This means that if the IP datagram is less than 46 bytes, the data field has to be "stuffed" to fill it out to 46 bytes.

- **Destination address (6 bytes):** This field contains the MAC address of the destination adapter. If the adapter receives a frame with any other MAC address, it discards the frame.
- **Source address (6 bytes):** .This field contains the MAC address of the adapter that transmits the frame onto the LAN.
- **Type field (2 bytes):** The type field permits Ethernet to multiplex network-layer protocols. A given host may support multiple network-layer protocols using different protocols for different applications. The type number of the upper layer protocol is given here.
- **Cyclic redundancy check (CRC) (4 bytes):** The purpose of the CRC field is to allow the receiving adapter to detect bit errors in the frame.
- **Preamble (8 bytes):** Each of the first 7 bytes of the preamble has a value of 10101010; the last byte is 10101011. The first 7 bytes of the preamble serve to "wake up" the receiving adapters and to synchronize their clocks to that of the sender's clock. The last 2 bits of the eighth byte of the preamble alert the adapter that the "important data" is about to come.

All of the Ethernet technologies provide **connectionless service** to the network layer. Frames are send from one adapter to another without handshaking. Ethernet technologies provide an **unreliable service** to the network layer. When an adapter receives a frame from another adapter, it runs the frame through a CRC check, but neither sends an acknowledgment when a frame passes the CRC check nor sends a negative acknowledgment when a frame fails the CRC check. When a frame fails the CRC check, the adapter simply discards the frame.

Ethernet comes in many different flavours such as 10BASE-T, 10BASE-2, 100BASE-T, 1000BASE-LX, and 10GBASE-T. The first part of the acronym refers to the speed of the standard: 10 (10 Megabit per second), 100 (100 Megabit), 1000 (Gigabit), or 10G (10 Gigabit). BASE refers to baseband Ethernet, meaning that the physical media only carries Ethernet traffic. The final part of the acronym refers to the physical media itself; Ethernet is carried over a variety of physical media including coaxial cable, copper wire, and fiber. Generally, a T refers to twisted-pair copper wires.

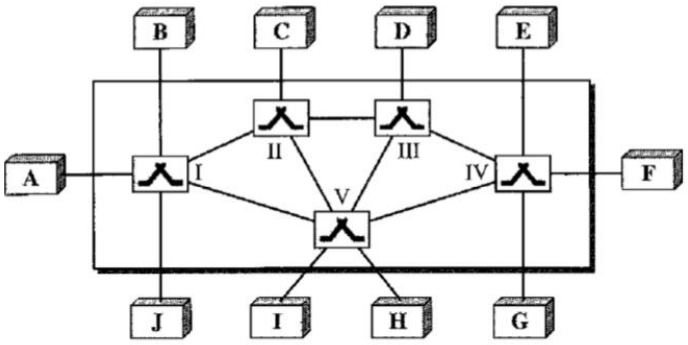
An Ethernet was initially developed as a segment of coaxial cable. The early 10BASE-2 and 10BASE-5 standards specify 10 Mbps Ethernet over two types of coaxial cable, each limited in length to 500 meters. Long distance can be covered by **repeaters**. Repeater is a device that receives a signal on the input side, and regenerates the signal on the output side.



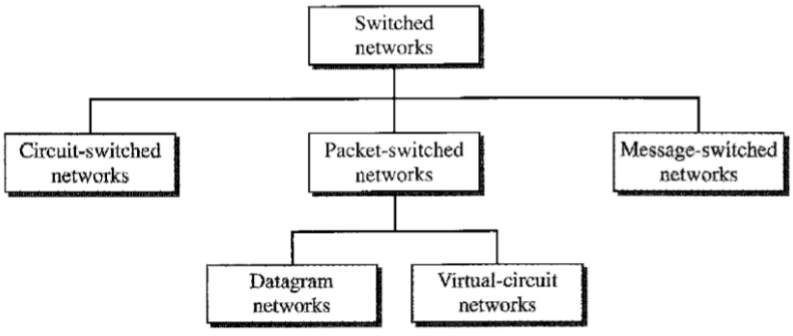
100 Mbps Ethernet standards implementation is given here, which has a common link layer and different physical layers. 100 Mbps Ethernet is limited to a 100 meter distance over twisted pair, and to several kilometers over fiber.

Gigabit Ethernet is an extension to the highly successful 10 Mbps and 100 Mbps Ethernet standards. It offering a raw data rate of 1,000 Mbps. It uses the standard Ethernet frame format and is backward compatible with 10BASE-T and 100BASE-T technologies. It allows for point-to-point links as well as shared broadcast channels. It uses CSMA/CD for shared broadcast channels. It allows for full-duplex operation at 1,000 Mbps in both directions for point-to-point channels.

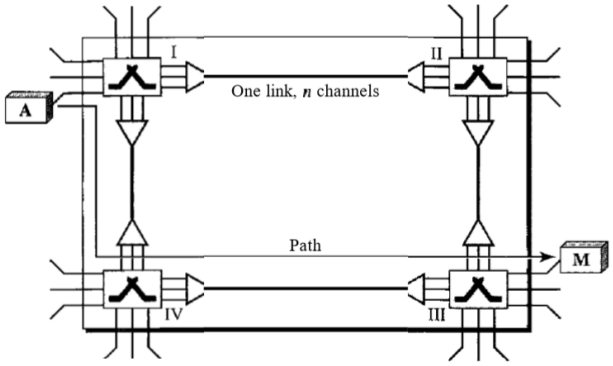
Switching and bridging



A switched network consists of a series of interlinked nodes, called switches. **Switches** are devices capable of creating temporary connections between two or more devices linked to the switch. In a switched network, some of these nodes are connected to the end systems. Others are used only for routing. The end systems are labelled A, B, C, D, and so on, and the switches are labelled I, II, III, IV, and V. Each switch is connected to multiple links.

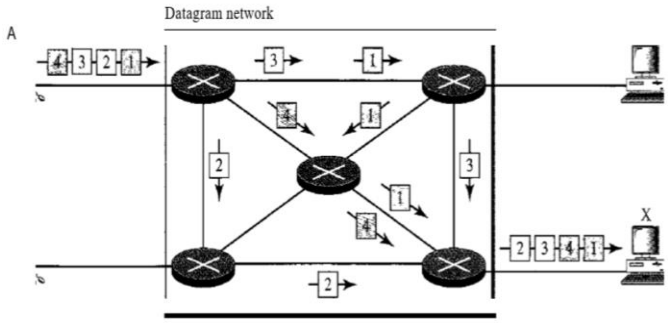


Traditionally, three methods of switching have been important: circuit switching, packet switching, and message switching. Networks can be categorised into three: circuit-switched networks, packet-switched networks, and message-switched. Packet-switched networks can further be divided into two subcategories- virtual-circuit networks and datagram networks.



A **circuit-switched network** is made of a set of switches connected by physical links, in which each link is divided into n channels. In circuit switching, the resources need to be reserved during the setup phase; the resources remain dedicated for the entire duration of data transfer phase until the teardown phase. In the given circuit-switched network, four switches and four links are shown. Each link is divided into n (n is 3) channels by using FDM or TDM. When end system A needs to communicate with end system M, system A needs to request a connection to M that must be accepted by all switches as well as by M itself. This is called the **setup phase**; a circuit (channel) is reserved on each link, and the combination of circuits or channels defines the dedicated path. After the dedicated path made of connected circuits (channels) is established, **data transfer** can take place. After all data have been transferred, the circuits are **teardown**.

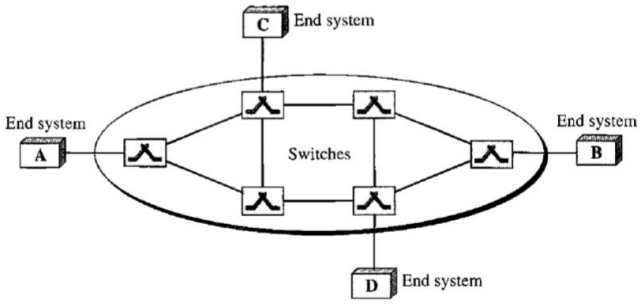
In a **packet-switched network**, there is no resource reservation; resources are allocated on demand. The allocation is done on a first-come, first-served basis. When a switch receives a packet, no matter what is the source or destination, the packet must wait if there are other packets being processed. In a datagram network, each packet is treated independently of all others. Even if a packet is part of a multi-packet transmission, the network treats it as though it existed alone. Packets in this approach are referred to as datagrams. **Datagram switching** is normally done at the network layer.



This figure shows how the datagram approach is used to deliver four packets from station A to station X. The switches in a datagram network are traditionally referred to as routers. All four packets (or datagrams) belong to the same message, but may travel different paths to reach their destination. This is so because the links may be involved in carrying packets from other sources and do not have the necessary bandwidth available to carry all the packets from A to X. Packets may also be lost or dropped because of a lack of resources. The datagram networks are sometimes referred to as connectionless networks.

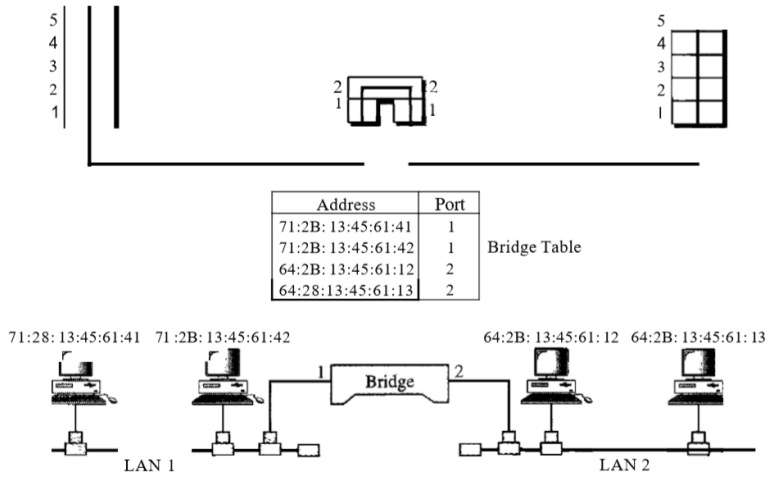
Each switch (or packet switch) has a **routing table** which is based on the destination address. The routing tables are dynamic and are updated periodically. The destination addresses

and the corresponding forwarding output ports are recorded in the tables. The destination address in the header of a packet in a datagram network remains the same during the entire journey of the packet.



A **virtual-circuit network** is a cross between a circuit-switched network and a datagram network. The network has switches that allow traffic from sources to destinations. A source or destination can be a computer, packet switch, bridge, or any other device that connects other networks. The identifier that is actually used for data transfer is called the virtual-circuit identifier. When a frame arrives at a switch, it has a VCI; when it leaves, it has a different VCl.

A **bridge** operates in both the physical and the data link layer. As a physical layer device, it regenerates the signal it receives. As a data link layer device, the bridge can check the physical (MAC) addresses (source and destination) contained in the frame. A bridge has filtering capability. It can check the destination address of a frame and decide if the frame should be forwarded or dropped. If the frame is to be forwarded, the decision must specify the port. A bridge has a table that maps addresses to ports. A bridge has a table used in filtering decisions.



In the figure two LANs are connected by a bridge. If a frame destined for the station 712B13456142 arrives at port 1, the bridge consults its table to find the departing port. According to its table, frames for 7l2B13456142 leave through port 1; therefore, there is no need for forwarding, and the frame is dropped. On the other hand, if a frame for 712B13456141 arrives at port 2, the departing port is port 1 and the frame is forwarded. A bridge does not change the physical (MAC) addresses in a frame.

A **transparent bridge** is a bridge in which the stations are completely unaware of the bridge's existence. If a bridge is added or deleted from the system, reconfiguration of the stations is unnecessary.

A two-layer switch is a bridge, a bridge with many ports and a design that allows better (faster) performance. A bridge with a few ports can connect a few LANs together. A bridge with many ports may be able to allocate a unique port to each station, with each station on its own independent entity

Signal Strength and Interference

Signal strength is the magnitude of an electric field at a reference point, which is located at a significant distance from the transmitting antenna. This is expressed in terms of the signal power of the receiver or the voltage per length received by the reference antenna

There are three basic ways to increase signal strength when receiving a signal: **amplification**, **antenna tuning**, and **antenna orientation**. Using an amplifier will amplify noise as well and may simply result in a louder version of the same noisy signal. The length of the antenna can be tuned to the frequency of interest. This can be done by adjusting the length of the antenna, or changing to an antenna tuned for the range you are interested in. Finally, using a directional antenna that is designed to focus the signal energy can increase the signal strength.

There are three basic types of interference: radio frequency interference (RFI), electrical interference and intermodulation. **Radio frequency interference (RFI)** is caused by radio and TV transmitters, communications equipment, cable television systems and other types of equipment that generate radio frequency energy as part of their operation. **Electrical interference** is caused by computers and digital equipment, heavy electrical equipment, lighting systems, faulty electrical devices, etc. **Intermodulation** is a type of interference caused by the internal combination of strong radio signals in wireless receivers.

Radio Frequency Interference is caused by radio frequency (RF) signals on or near the frequency of the affected wireless receiver. The interfering signals might have been transmitted intentionally or unintentionally as the result of some defect or undesired characteristic of the source. It is not necessary that the interfering signal be exactly on the same frequency as the wireless system to be troublesome. Strong RF signals that are near the wireless frequency can affect the operation of the wireless receiver, causing audio and reception problems. Many wireless microphone systems operate in the frequency bands used for TV broadcasting. TV transmitters are generally quite powerful and can interfere with wireless receivers at very considerable distances. Interference by AM radio stations is only a problem when the transmitter is close by.

Electrical interference is almost never intentional. The equipment causing electrical interference problems was not intended to be a source of RF energy. Often, the interference is

the result of a defect, failure or maintenance problem that can be readily corrected. Manufacturers are required to design and manufacture their products so that they do not cause harmful interference. There are three basic types of electrical interference: noise from electrical equipment, noise generated by electronic devices such as computers, and interference from natural sources such as lightning. All forms of electrical interference are relatively rare and account for only a small percentage of all wireless interference problems.

Intermodulation or "intermod" is a type of interference sometimes encountered in wireless microphone systems. Intermodulation differs from other forms of interference in that it is created in the wireless system itself, not directly by some external source. Interference due to intermodulation is caused by strong signals which are generally not near that of the wireless frequency. Instead, these strong signals overload some circuit in the wireless receiver, causing the circuit to internally generate harmonics of the strong signals. These harmonics then combine, or mix, in the receiver to create a new frequency that was not present at the receiver input. The newly-created frequency, called an "intermodulation product," then interferes with the wireless system in much the same way as other sources of interference. Other transmitters with frequency very near that of the wireless system may become the source of interference.

Data Encoding

Encoding is the process of converting the data or a given sequence of characters, symbols, alphabets etc., into a specified format, for the secured transmission of data. Data encoding is the process of using various patterns of voltage or current levels to represent **1s** and **0s** of the digital signals on the transmission link. The data encoding technique is divided into the following types, depending upon the type of data conversion: analog data to analog signals, analog data to digital signals, digital data to analog signals and digital data to digital signals.

Analog-to-analog conversion, or modulation, is the representation of analog information by an analog signal. In this process a characteristic of carrier wave is varied according to the instantaneous amplitude of the modulating signal. Analog to analog conversion can be done in three ways: amplitude modulation, frequency modulation and phase modulation. The modulation in which the amplitude of the carrier wave is varied according to the instantaneous amplitude of the modulating signal keeping phase and frequency as constant is called **amplitude modulation**. The modulation in which the frequency of the carrier wave is varied according to the instantaneous amplitude of the modulating signal keeping phase and amplitude as constant is called **frequency modulation**. The modulation in which the phase of the carrier wave is varied

according to the instantaneous amplitude of the modulating signal keeping amplitude and frequency as constant is called **phase modulation**.

In **analog to digital conversion** an analog signal is converted into a digital signal. The digital signal is represented with a binary code, which is a combination of bits 0 and 1. Codec is a device that performs this operation. **Pulse Code Modulation (PCM)** is the most common technique used to change an analog signal to digital data (digitization). The analog signal is sampled first. Then the sampled signal is quantized and these quantized values are encoded as streams of bits. **Delta modulation** is simpler modulation technique than PCM. It finds the change from the previous value.

Digital-to-analog conversion (DAC) is the process by which digital signals are converted to analog signals. A modem converts computer digital data to analog audio-frequency signals that can be transmitted over telephone lines. An analog signal is characterized by its amplitude, frequency, and phase. There are three kinds of digital-to-analog conversions: amplitude shift keying, frequency shift keying and phase shift keying. **Amplitude shift keying** is a technique in which carrier signal is analog and data to be modulated is digital. The amplitude of analog carrier signal is modified to reflect binary data. The binary signal when modulated gives a zero value when the binary data represents 0 while gives the carrier output when data is 1. The frequency and phase of the carrier signal remain constant. In **frequency shift keying** the frequency of analog carrier signal is modified to reflect binary data. The output of a frequency shift keying modulated wave is high in frequency for a binary high input and is low in frequency for a binary low input. The amplitude and phase of the carrier signal remain constant. In **phase shift keying** the phase of the analog carrier signal is modified to reflect binary data. The amplitude and frequency of the carrier signal remains constant.

Digital-to-digital encoding is the representation of digital information by a digital signal. When binary 1s and 0s generated by the computer are translated into a sequence of voltage pulses that can be propagated over a wire, this process is known as digital-to-digital encoding. Some of the techniques come under this category are: unipolar, polar and biphase. In **unipolar** scheme, all the signal levels are either above or below the axis. Non return to zero (NRZ) is a unipolar line coding scheme in which positive voltage defines bit 1 and the zero voltage defines bit 0. In **polar** schemes, the voltages are on the both sides of the axis. In **biphase**, the duration of the bit is divided into two halves. The voltage remains at one level during the first half and moves to the other level in the second half. The transition at the middle of the bit provides synchronization.

Ethernet Switches

The role of the switch is to receive incoming link-layer frames and forward them onto outgoing links. The switch itself is transparent to the hosts and routers in the subnet. Switch's output interfaces have buffers for storing frames. Switches are plug-and-play devices because they require no intervention from a network administrator or user. The administrator need not configure the switch tables at the time of installation or when a host is removed from one of the LAN segments. A switch interface can send and receive at the same time thus full-duplex device. Switch eliminates collision and it can support heterogeneous links.

Address	Interface	Time
62-FE-F7-11-89-A3	1	9:32
7C-BA-B2-B4-91-10	3	9:36
....	....	....

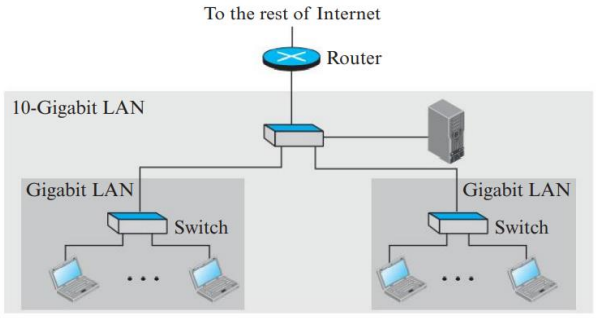
Switch performs filtering and forwarding functionalities. Filtering is the switch function that determines whether a frame should be forwarded to some interface or should just be dropped. Forwarding is the switch function that determines the interfaces to which a frame should be directed, and then moves the frame to those interfaces. Switch filtering and forwarding are done with a switch table. The switch table contains entries for some, but not necessarily all, of the hosts and routers on a LAN. An entry in the switch table contains (1) a MAC address, (2) the switch interface that leads toward that MAC address, and (3) the time at which the entry was placed in the table. Switches forward packets based on MAC addresses rather than on IP addresses.

When a frame with destination address DD-DD-DD-DD-DD-DD arrives at the switch on interface x. The switch indexes its table with the MAC address DD-DD-DD-DD-DD-DD. If there is no entry in the table for DD-DD-DD-DD-DD-DD, the switch forwards copies of the frame to the output buffers preceding all interfaces except for interface x. If there is an entry in the table with interface x, no need to forward the frame to any of the other interfaces, the switch performs the filtering function by discarding the frame. If there is an entry in the table, associating DD-DD-DD-DD-DD-DD with interface y≠x, the switch performs its forwarding function by putting the frame in an output buffer that precedes interface y.

The switching table is built automatically, dynamically, and autonomously. There for switch has self-learning capability. In the initial phase of this learning process, the switching table is empty. For each incoming frame received on an interface, the switch stores the MAC address in the frame's source address field, the interface from which the frame arrived and the current time in its table. The switch deletes an address in the table if no frames are received with that address as the source address after some period of time (aging time).

Routers

A router is a three-layer device; it operates in the physical, data-link, and network layers. As a physical-layer device, it regenerates the signal it receives. As a link-layer device, the router checks the physical addresses contained in the packet. Router is an internetworking device which connects independent networks to form an internetwork. It has a physical and logical (IP) address for each of its interfaces. It acts only on those packets in which the link-layer destination address matches the address of the interface at which the packet arrives. It also changes the link-layer address of the packet when it forwards the packet.



In this figure, an organization has two separate buildings with a Gigabit Ethernet LAN installed in each building. The organization uses switches in each LAN. The two LANs can be connected to form a larger LAN using 10-Gigabit Ethernet technology that speeds up the connection to the Ethernet and the connection to the organization server. A router then can connect the whole system to the Internet.

MAC Address

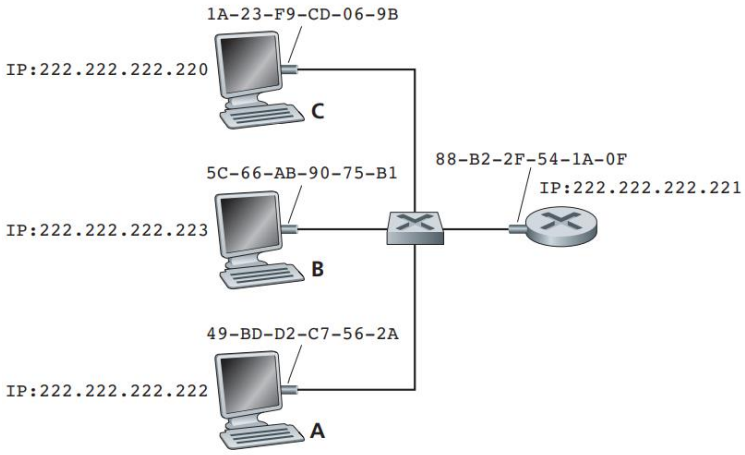
The adapters (network interfaces) of hosts and routers have link-layer (MAC) addresses. A host or router with multiple network interfaces will have multiple MAC addresses associated with it. A link-layer address is variously called a LAN address, a physical address, or a MAC address. The MAC address is 6 bytes long, expressed in hexadecimal notation, with each byte of the address expressed as a pair of hexadecimal numbers (e.g., 1A-23-F9-CD-06-9B). MCA addresses are unique. MAC address has a flat structure rather than a hierarchical structure loke IP address.

When an adapter wants to send a frame to some destination adapter, the sending adapter inserts the destination adapter's MAC address into the frame and then sends the frame into the LAN. An adapter may receive a frame that isn't addressed to it. Thus, when an adapter receives a frame, it will check to see whether the destination MAC address in the frame matches its own MAC address. If there is a match, the adapter extracts the enclosed datagram and passes the datagram up the protocol stack. If there isn't a match, the adapter discards the frame, without

passing the network-layer datagram up. Thus, the destination only will be interrupted when the frame is received.

If a sending adapter wants all the other adapters on the LAN to receive and process the frame it is about to send, the sending adapter inserts a special MAC broadcast address (FF-FF-FF-FF-FF-FF) into the destination address field of the frame.

Address Resolution Protocol (ARP)

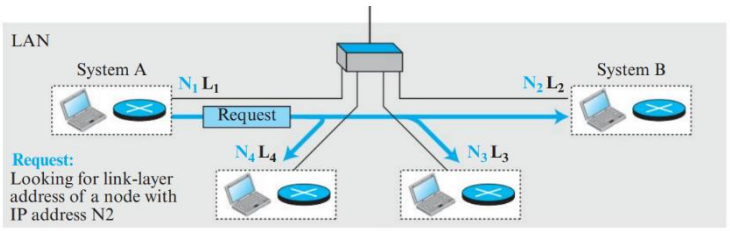


Address Resolution Protocol (ARP) translates between network-layer addresses (IP addresses) and link-layer addresses (MAC addresses). In this example, each host and router have a single IP address and single MAC address. Assume that whenever a switch receives a frame on one interface, it forwards the frame on all of its other interfaces. The host with IP address 222.222.222.220 wants to send an IP datagram to host 222.222.222.222. The sending host 222.222.222.220 provides its ARP module the IP address 222.222.222.222, and the ARP module returns the corresponding MAC address 49-BD-D2-C7-56-2A.

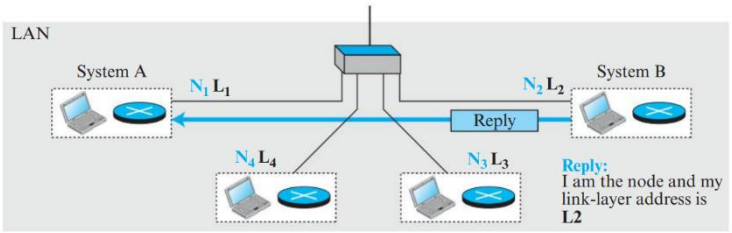
Each host and router has an ARP table in its memory, which contains mappings of IP addresses to MAC addresses. This is how the ARP table in host 222.222.222.220 might look like. The ARP table also contains a time-to-live (TTL) value, which indicates when each mapping will be deleted from the table. A typical expiration time for an entry is 20 minutes from when an entry is placed in an ARP table.

IP Address	MAC Address	TTL
222.222.222.221	88-B2-2F-54-1A-0F	13:45:00
222.222.222.223	5C-66-AB-90-75-B1	13:52:00

The sending host needs to obtain the MAC address of the destination given the IP address. If the MAC address of the destination is available in the ARP table of the sender, it is easy. If the corresponding entry is not in the ARP table, the address is resolved used ARP protocol.

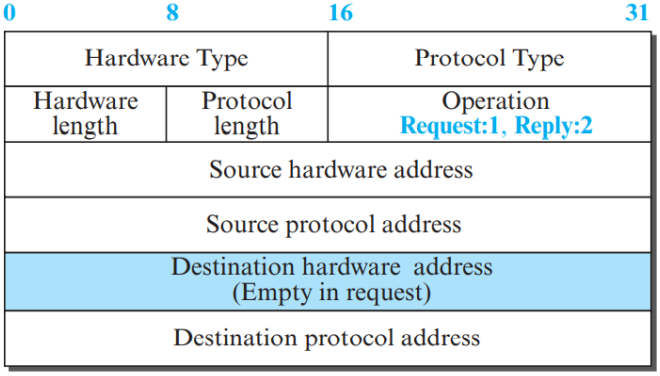


a. ARP request is broadcast

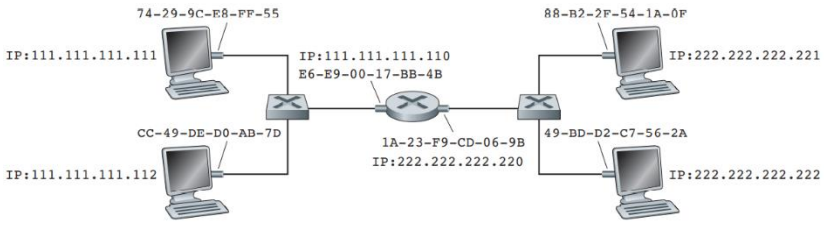


b. ARP reply is unicast

When a host or a router needs to find the link-layer address of another host or router in its network, whose entry is not available in host's ARP table, it sends an ARP request packet. The packet includes the link-layer and IP addresses of the sender and the IP address of the receiver. Because the sender does not know the link-layer address of the receiver, the query is broadcast over the link using the link-layer broadcast address. Every host or router on the network receives and processes the ARP request packet, but only the intended recipient recognizes its IP address and sends back an ARP response packet. The response packet contains the recipient's IP and link-layer addresses. The packet is unicast directly to the node that sent the request packet.



The hardware type field defines the type of the link-layer protocol; Ethernet is given the type 1. The protocol type field defines the network-layer protocol. The source hardware and source protocol addresses are variable-length fields defining the link-layer and network-layer addresses of the sender. The destination hardware address and destination protocol address fields define the receiver link-layer and network-layer addresses. An ARP packet is encapsulated directly into a data-link frame.



This network has two subnets. Subnet 1 have addresses of the form 111.111.111.xxx and all of the interfaces connected to Subnet 2 have addresses of the form 222.222.222.xxx. Suppose that host 111.111.111.111 wants to send an IP datagram to a host 222.222.222.222, which is in another network. The sending host passes the datagram to its adapter, along with the MAC address of the first hope router, i.e., E6-E9-00-17-BB-4B. The router now has to determine the correct interface on which the datagram is to be forwarded. It

can be done using the ARP table or with address resolution mechanism. This way the datagram reaches the destination.