A **network protocol** defines rules and conventions for communication between network devices. Network protocols include mechanisms for devices to identify and make connections with each other, as well as formatting rules that specify how data is packaged into messages sent and received. Some protocols also support message ​acknowledgment and data compression designed for reliable and/or high-performance network communication.

[**Processing delay**](https://en.wikipedia.org/wiki/Processing_delay) – time routers take to process the packet header. [**Queuing delay**](https://en.wikipedia.org/wiki/Queuing_delay)– time the packet spends in routing queues. [**Transmission delay**](https://en.wikipedia.org/wiki/Transmission_delay)– time it takes to push the packet's bits onto the link.: = message (bits)/rate (bps) [**Propagation delay**](https://en.wikipedia.org/wiki/Propagation_delay) **–** time for a signal to reach its destination: = distance /speed of flight in media How quickly a message travels over the wire.

**Packet Switching:** describes the type of network in which relatively small units of data called packets are routed through a network based on the destination address contained within each packet. Breaking communication down into packets allows the same data path to be shared among many users in the network. Breaking message into packets allows parallel transmission across all links, reducing end to end latency. It also prevents a link from being “hogged” for a long time by one message. Efficient use of expensive links: The links are assumed to be expensive and scarce. Packet switching allows many, bursty flows to share the same link efficiently. Resilience to failure of links &routers: Enables statistical multiplexing

|  |  |  |
| --- | --- | --- |
|  | **Round Trip Time (RTT**) is twice the one way dela. Measure of how long to signal and get a response.  **Framing** allows complete messages to be recovered at the far end of the link. | Message latency = how long does it take to send a message  **Latency** = Propagation + Transmit + Queue  Propagation Delay = Distance/Speed Of Light  Transmit Time = MessageSize/Bandwidth  Two strategies to correct errors: Detect and retransmit, or Automatic Repeat reQuest. (ARQ) Error correcting codes, or Forward Error Correction (FEC)  Advantages of Error Detection: Requires smaller number of bits/overhead. Requires less/simpler processing. Advantages of Error Correction Reduces number of retransmissions.  Error correction codes: Hamming codes  Error detection codes: Parity, Checksums, Cyclic redundancy codes  The Hamming distance tells us how much error can safely be tolerated. |
| Different devices switch different things  Physical layer: electrical signals (repeaters and hubs) Link layer: frames (bridges and switches)  Network layer: packets (routers)  **Physical Layer: Repeaters**  Distance limitation in local-area networks Electrical signal becomes weaker as it travels Imposes a limit on the length of a LAN Repeaters join LANs together Analog electronic device Continuously monitors electrical signals on each LAN Transmits an amplified copy | **Limitations of Repeaters and Hubs**  - One large collision domain  Every bit is sent everywhere So, aggregate throughput is limited E.g., three departments each get 10 Mbps independently … and then connect via a hub and must share 10 Mbps  - Cannot support multiple LAN technologies  Does not buffer or interpret frames So, can’t interconnect between different rates or formats E.g., 10 Mbps Ethernet and 100 Mbps Ethernet  - Limitations on maximum nodes and distances Does not circumvent the limitations of shared media E.g., still cannot go beyond 2500 meters on Ethernet | Link Layer: **Bridges** Connects two or more LANs at the link layer  Extracts destination address from the frame. Looks up the destination in a table.  Forwards the frame to the appropriate LAN segment. Each segment is its own collision domain  Link Layer: **Switches** Typically connects individual computers A switch is essentially the same as a bridge … though typically used to connect hosts, not LANs Like bridges, support concurrent communication Host A can talk to C, while B talks to D CSC |

**Self Learning:** Building the Table When a frame arrives Inspect the source MAC address Associate the address with the incoming interface Store the mapping in the switch table Use a time-to-live field to eventually forget the mapping CSC

|  |  |
| --- | --- |
| **Advantages of Switches/bridge Over Hubs/Repeaters**  Only forwards frames as needed Filters frames to avoid unnecessary load on segments Sends frames only to segments that need to see them  Extends the geographic span of the network Separate collision domains allow longer distances  Improves privacy by limiting scope of frames Hosts can “snoop” the traffic traversing their segment … but not all the rest of the traffic Applies carrier sense and collision detection Does not transmit when the link is busy Applies exponential back-off after a collision Joins segments using different technologies | **Disadvantages Over Hubs/Repeaters**  - Delay in forwarding frames Bridge/switch must receive and parse the frame … and perform a look-up to decide where to forward Storing and forwarding the packet introduces delay Solution: **cut-through** switching  - Need to learn where to forward frames Bridge/switch needs to construct a forwarding table Ideally, without intervention from network administrators Solution: self-learning  - Higher cost |
|  | **Switches vs. Routers**  Advantages of switches over routers  - Plug-and-play Fast filtering and forwarding of frames No pronunciation ambiguity Disadvantages of switches over routers  - Topology is restricted to a spanning tree  - Large networks require large ARP tables  - Broadcast storms can cause the network to collapse |

**bandwidth-delay product** is the [product](https://en.wikipedia.org/wiki/Multiplication) of a data link's capacity (in [bits per second](https://en.wikipedia.org/wiki/Bit_rate)) and its [round-trip delay time](https://en.wikipedia.org/wiki/Round-trip_delay_time) . The result, an amount of data measured in bits (or [bytes](https://en.wikipedia.org/wiki/Byte)), is equivalent to the maximum amount of data on the network circuit at any given time, i.e., data that has been transmitted but not yet acknowledged.The product computed represents the amount of data the sender can send before it would be possible to receive a response.

|  |  |
| --- | --- |
| “Layering” is commonly used in computer networks, because: a) It forces all network software to be written in ANSI ‘C’. b) Encapsulation is the lowest overhead method to transmit data. c) It allows widespread code and implementation reuse. d) It keeps networks warm enabling them to run faster. | Characteristics of IP ·  CONNECTIONLESS: mis-sequencing , ·UNRELIABLE: may drop packets, BEST EFFORT: … but only if necessary, DATAGRAM: individually routed |
| TCP vs UDP  Bigger header  Data Doesn’t always get sent out immediat. Side effect of congestion control  Bigger overhead.: Retransmission of packets, acknowledgment.  UDP is message oriented. TCP is stream,-oriented. | Running out of IP addresses. Running out of capacity in the global routing tables Solutions Subnetting within an organization to subdivide the organization’s network ID. Classless Inter-Domain Routing **CIDR** is a new addressing scheme for the Internet which allows for more efficient allocation of IP addresses than the old Class A, B, and C address scheme. |

Media Access Control (**MAC**) address is a [binary number](https://www.lifewire.com/working-with-binary-and-hexadecimal-numbers-816247) used to uniquely identify computer [network adapters](https://www.lifewire.com/definition-of-adapter-817585). These numbers are embedded into the network hardware during the manufacturing process, or stored in firmware, and designed to not be modified.

**ARP** (Address Resolution Protocol) converts an [Internet Protocol (IP) address](https://www.lifewire.com/what-is-an-ip-address-2625920) to its corresponding physical network address. IP networks including those that run on [Ethernet](https://www.lifewire.com/what-is-ethernet-3426740) and [Wi-Fi](https://www.lifewire.com/what-is-wi-fi-2377430) require ARP in order to function.

**MAC** operates at Layer 2 of the [OSI model](https://www.lifewire.com/open-systems-interconnection-model-816290) while **IP** operates at [Layer 3](https://www.lifewire.com/layer-3-switch-817583). This allows MAC addressing to support other kinds of networks besides TCP/IP.

|  |  |  |
| --- | --- | --- |
|  |  |  |
| The other problem with IPv4 is network address translation (NAT) |  |  |
| **ICMP**: internet control message protocol used by hosts & routers to communicate network level information: error reporting: unreachable host, network, port, protocol echo request/reply (used by ping)  - network-layer “above” IP: ICMP msgs carried in IP datagrams - - -ICMP message: type, code plus first 8 bytes of IP datagram causing error Type |  |  |
|  |  | **Link layer. Which of the following are true?**  (a.) An Ethernet switch can interconnect a 10Mb/s Ethernet network and a 1Gb/s Ethernet.  (d.) 4B/5B is considered more efficient than Manchester encoding because more user data is transmitted in same amount of time.  (e.) The 802.11b wireless protocol incorporates a link-layer ACK not present in regular Ethernet.  **Which are true about network switches and routers?**  -.Ethernet switches learn the location of hosts on their network by observing the frames they process.  **Which are true about Ethernet protocols?**  The Ethernet spanning tree may take a longer path through a network than that which would be calculated by a link-state algorithm (assuming both have converged). |
| Which of the following statement(s) are TRUE? [1/1] (a) The Ethernet is a connectionless and reliable data link protocol (b) Ethernet switches, like IP routers, use a table to determine which output links to send a packet. |  |  |