Key concepts:

1. Computer Network – built primarily from general purpose programmable hardware, and they aren't optimized for a particular application. So its generality is key in its composition.
    a. Unlike other networks, it lacks specificity.
    b. Taking over single use networks. For example, can stream tv shows instead of watching them on television via television signals. Can make phone calls via computer networks.
2. Scale – a system that is designed to support growth to an arbitrarily large size is said to scale.
3. Link – a network can consist of two or more computers directly connected by some physical medium. By physical medium, some examples are coaxial cable or an optical fiber. We call such a physical medium a link.
4. Nodes – the computers connected in a network by a physical link.
5. Point-to-point – links that are limited to a pair of nodes.
6. Multiple access – when more than two nodes share a single physical link. Wireless links, such as those provided by cellular networks and Wi-Fi networks, are examples of multiple access connectivity. It is often the case that multiple access links are limited in size, in terms of both the geographical distance they can cover and the number of nodes they can connect.
7. Switched network – nodes that are attached to at least two links and run software that forwards data received on one link out to another. When organized in a systematic way, these forwarding nodes form a switched network.
    a. Circuit Switched – is a method of implementing a telecommunications network in which two network nodes establish a dedicated communications channel (circuit) through the network before the nodes may communicate. The circuit guarantees the full bandwidth of the channel and remains connected for the entire duration of the communication session. Example: telephone system
    b. Packet Switched – computer networks are this type of switched network. Focus of this course. It's the grouping of data into packets that are transmitted over a digital network.
8. Packet, message – Blocks of data. Nodes in packet switched network send discrete blocks of data to each other. Those blocks are called packets, or messages.
9. Store-and-forward – routing strategy used in a packet switched network. Strategy typically used by a packet switched network. Each node in a store-and-forward network first receives a complete packet over some link, stores the packet in its internal memory, and then forwards the complete packet to the next node.
10. Cloud – any type of network, whether it is a single point-to-point link, a multiple access link, or a switched network.
11. Switches – nodes in the cloud that implement the network, their primary function is to store and forward packets.
12. Internetwork – a second way in which a set of computers can be indirectly connected. A set of independent networks (known as clouds) are interconnected. We adopt the Internet's convention of referring to a generic internetwork of networks as a lower i internet, and the currently operational TCP/IP Internet as the capital I Internet.
13. Router/gateway – node that is connected to two or more networks.
14. Host-to-host connectivity – a set of hosts are directly or indirectly connected to each other and each node is able to say which of the other nodes on the network it wants to communicate with.

15. Address – it's assigned to each node. Allows a node to indicate which other node it wants to communicate with. An address is a byte string that identifies a node; that is, the network can use a node's address to distinguish it from the other nodes connected to the network.
16. Routing – when a source node wants the network to deliver a message to a certain destination node, it specifies the address of the destination node. If the sending and receiving nodes are not directly connected, then the switches and routers of the network use this address decide how to forward the message toward the destination. The process of determining systematically how to forward messages toward the destination node based on its address is called routing.
17. Unicast – the source node wants to send a message to a single destination node.
18. Broadcast – the source node wants to send a message to all the nodes on the network.
19. Multicast – the source node wants to send a message to some subset of the other nodes, but not all of them.
20. Multiplexing – means that a system resource is shared among multiple users. At an intuitive level, multiplexing is similar to timesharing a computer system, where a single physical processor is shared (multiplexed) among multiple jobs. Each of those jobs believes it has its own private processor. Data being sent by multiple users can be multiplexed over the physical links that make up the network.
21. De-multiplexing – separating out the flow of data back to a switch.
22. Synchronous Time Division Multiplexing (STDM) – a method for multiplexing multiple flows onto one physical link. Divides time into equal sized quanta and, in a round-robin fashion, gives each flow a chance to send its data over the physical link. In other words, during time quantum 1, data from S1 to R1 is transmitted; during time quantum 2, data from S2 to R2 is transmitted; in quantum 3, S3 sends data to R3. And then this process repeats in a round-robin fashion.
23. Frequency Division Multiplexing (FDM) – transmits each flow over the physical link at a different frequency, similar to how signals for different TV stations are transmitted over different frequencies over the airwaves or coaxial cable TV ink.
24. Limitations of STDM and FDM:
    a. If one of the flows does not have any data to send, its share of the physical link (its time quantum or its frequency) remains idle. Even if one of the other flows has data to transmit.
    b. Works best when the maximum number of flows is fixed and known ahead of time. However, this is not practical.
25. Statistical Multiplexing – Similar to STDM in that the physical link is shared over time – first data from one flow is transmitted over the physical link, then data from another flow is transmitted, and so on. However, unlike STDM, data is transmitted from each flow on demand instead of waiting for a predetermined time slot. It's this avoidance of idle time that gives this packet switching approach its efficiency.

Example of a burst error:

We would like to transmit the following bit sequence:

1 1 0 0 0 1 0 1 1

However, the following bit sequence is received instead:

0 1 0 1 0 1 0 0 1

The number of bit errors (as we can see underlined) is, in this case, 3. The bit error rate (BER) is 3 divided by 9 (because there are 9 bits total). This results in a BER of 0.3333 or 33.3%.

Because there are more than one bit error, it is a burst error.

Network designers need to consider three classes of failures:

1. Bit and burst errors – single bit error (bit error) or multiple bit errors (burst error) within the packet.
2. Complete packet loss – a packet is completely lost on the network. This is typically due to congestion. Challenging in determining whether a packet is lost or merely late.
3. Failure at the node or link level – a physical link is cut or a computer it is connected to crashes. Could also be due to misconfiguration of the network device. Challenging in determining whether a computer has failed or if it's just slow.

Protocol defines two different interfaces:

1. Service interface – defines the operations that local objects can perform on the protocol. For example, a request/reply protocol would support operations by which an application can send and receive messages. With the HTTP protocol, that could support an operation to fetch a page of hypertext (e.g. web page) from a remote server.
2. Peer-to-peer interface (also known as peer interface) – defines the form and meaning of messages exchanged between protocol peers to implement the communication service. For example, with the HTTP protocol, the protocol specification defines in detail how a GET command is formatted, what arguments it should take, and how the web server should respond when it receives the command.

OSI 7 layer model:

Start from the bottom up:

1. Physical Layer – handles the transmission of raw bits over a communication link. Run on the node.
2. Data Link Layer – collects a stream of bits and aggregates them into a frame. Network adapters and device drivers running in the node's operating system typically implement the data link layer. Which means that frames, not bits, actually get delivered to the hosts. Run on the node.
3. Network Layer – handles the routing among the nodes within a packet switched network. It's at this layer, the unit of data exchanged among the nodes is known as a packet, instead of a frame (although they're the same thing). Run on the node.

4. Transport Layer – implements the process to process channel. Here, the unit of data exchanged is called a message. Run on the end host, not on the intermediate nodes. Provides services such as reliability, flow control, and multiplexing.
5. Session Layer – provides a namespace that is used to tie together the potentially different transport streams that are part of a single application. For example, it might manage the audio streams and video streams that are being combined in a teleconferencing application.
6. Presentation Layer – manages the format of the data being exchanged between peers. For example, whether an integer is 16, 32, or 64 bits long, how a video stream is formatted, etc.
7. Application Layer – implements the application level protocols, such as HTTP and FTP. HTTP is what enables web browsers to request web pages from web servers.