Computer network：a system that connects two or more computing devices for transmitting and sharing information

Gateway：a network node used in telecommunications that connects two networks with different transmission protocols together.

Circuit switch: Before a communication starts, a dedicated path must be established between the sender and the receiver

Packet Switch: No identified path is identified before, the sender only needs to know the receiver’s address

Protocol: a set of rules outlining how connected devices communicate across a network to exchange information easily and safely

Interfaces: the point of interconnection between a computer and a private or public network. A network interface could be a physical network interface card (NIC) or a logical interface (API, bridge, tunnel, virtual)

Network applications：a software program which operates over a network and allows communication and data sharing between multiple devices and users

Subnet mask：splits the IP address into the host and network addresses(IP & subnet mask = IP network)

Media Access Control (MAC) header : The data fields added at the beginning of a network packet in order to turn it into a frame to be transmitted

Network Address Translation (NAT): a way to map multiple private addresses inside a local network to a public IP address before transferring the information onto the internet

Performance：Latency = Propagation + transmit + queue、Propagation = distance/speed of light、Transmit = size/bandwidth、One bit transmission => propagation is important、Large bytes transmission => bandwidth is important

Web API：is designed to help other applications (mobile apps, other websites) to interact with Webserver

The JavaScript Object Notation (JSON) is widely used for interacting with WebAPI

Real-Time Transport Protocol (RTP)：specifies the coding schemes and media types of an application

Session Initiation Protocol (SIP)：SIP is an application layer protocol that bears a certain resemblance to HTTP, being based on a similar request/response model.

Peer-to-peer：a distributed application architecture that partitions tasks or workloads between peers

BitTorrnet：a communication protocol for peer-to peer file sharing, which enables users to distribute data and electronic files over the Internet in a decentralized manner

Presentation Formatting：Transform application data into a form that is suitable for transmission over a network and vice versa(encoding-decoding)

Tag：additional information included in a message—beyond the concrete representation of the base types—that helps the receiver decode the message

Stubs(Encoding)：• Definition: the piece of code that implements encoding • Stubs is invented to support Remote Procedure Call (RPC) protocol • On the server side, the stub converts the message back into a set of variables that can be used as arguments to call the remote procedure

Presentation formatting example：

* Abstract Syntax Notation One (ASN.1)：is an ISO standard that defines, among other things, a representation for data sent over a network. The representation-specific part of ASN.1 is called the Basic Encoding Rules (BER). One of the claims to fame of ASN.1 BER is that it is used by the Internet standard Simple Network Management Protocol (SNMP).
* Network Data Representation (NDR)：is the data-encoding standard used in the Distributed Computing Environment. Unlike XDR and ASN.1, NDR uses receiver-makes-right. It does this by inserting an architecture tag at the front of each message; individual data items are untagged. NDR uses a compiler to generate stubs. This compiler takes a description of a program written in the Interface Definition Language (IDL) and generates the necessary stubs. IDL looks pretty much like C, and so essentially supports the C type system.
* Markup Languages(XML)：XML syntax looks much like HTML. XML syntax provides for a nested structure of tag/value pairs. A XML format can be both processed by programs and read by humans. Parsers can be used across different XML-based languages

Compression：

* Huffman codes：if you know the relative probability that each symbol will occur in the data, then you can assign a different number of bits to each possible symbol in a way that minimizes the number of bits it takes to encode a given block of data.
* Run length Encoding：The idea is to replace consecutive occurrences of a given symbol with only one copy of the symbol, plus a count of how many times that symbol occurs—hence the name “run length.” For example, the string AAABCCCC would be encoded as A3B1C4.
* Differential Pulse Code Modulation (DPCM)：The idea here is to first output a reference symbol and then, for each symbol in the data, to output the difference between that symbol and the reference symbol. For example, using symbol A as the reference symbol, the string AAABBCDDDD would be encoded as A0001123333 since A is the same as the reference symbol, B has a difference of 1 from the reference symbol, and so on.
* Dictionary based Methods：The Unix compress and gzip commands use variants of the LZ algorithm. The idea of a dictionary-based compression algorithm is to build a dictionary (table) of variable length strings (think of them as common phrases) that you expect to find in the data, and then to replace each of these strings when it appears in the data with the corresponding index to the dictionary.
* Joint Photographic Experts Group(JPEG)：DCT->Quantization->Encoding
* Moving Picture Experts Group(MPEG)：a moving picture (i.e., video) is simply a succession of still images—also called frames or pictures—displayed at some video rate. Each of these frames can be compressed using the same DCT-based technique used in JPEG.
* Graphical Interchange Format (GIF)：Rather than sending those 24 bits per pixel, however, GIF first reduces 24-bit color images to 8-bit color images. This is done by identifying the colors used in the picture, of which there will typically be considerably fewer than 224, and then picking the 256 colors that most closely approximate the colors used in the picture.
* Portable Network Graphics(PNG)：Portable Network Graphics is a raster-graphics file format that supports lossless data compression. PNG is an improved, non-patented replacement for GIF. PNG is designed the format for transferring images on the Internet, not for professional-quality print graphics. PNG often has a transparent background

tcp：Reliable,Connection oriented,Byte-stream service,three-way handshake, Connection oriented transport layer,ack, SequenceNum(sequence number for the first byte of data carried in that segment.), flow control(preventing senders from overrunning the capacity of the receivers), congestion control(preventing too much data from being injected into the network, thereby causing switches or links to become overloaded), Wraparound(Reusing of sequence numbers), Silly Window Syndrome(occurs when the sending application program creates data slowly, the receiving application program consumes data slowly), Nagle’s Algorithm(If there is data to send but the window is open less than MSS, then we may want to wait some amount of time before sending the available data. We also introduce a timer and to transmit when the timer expires), Karn/Partridge Algorithm(Do not sample RTT when retransmitting,Double timeout after each retransmission)

UDP：data loss doesn’t affect,Multiplayer Online Games, VoIP, and Video Live Streaming,Fast but non-guaranteed transfer. “best effort”

Switching：

switching and forwarding-receive incoming packets on one of its links and to transmit them on some other link. Two common approaches:datagram(packet contains enough information to enable any switch to decide how to get it to destination) or Connectionless approach、Virtual circuit or Connection-oriented approach. Have forwarding table(map destination to port)

VC：set up a virtual connection from the source host to the destination host and then send the data. And establish “VC table” in each switch. VC contains virtual circuit identifier (VCI), If a packet arrives on the designated incoming interface and that packet contains the designated VCI value in its header, then the packet should be sent out the specified outgoing interface with the specified outgoing VCI value first having been placed in its header. Characteristics(Since host A has to wait for the connection request to reach the far side of the network and return before it can send its first data packet, there is at least one RTT of delay before data is sent • While the connection request contains the full address for host B (which might be quite large, being a global identifier on the network), each data packet contains only a small identifier, which is only unique on one link.)

Layer 2 Switching-Switching is done at Layer 2 (Data link layer).No built-in security features. Do not offer any QoS services to enable effective packet switching (best effort).

Layer 3 Switching-Switching is done at Layer 3 (Network layer) --- Routing features. Have built-in security features, such as access control lists. support QoS capability offered that can prioritize different types of network traffic

Bridge: Frames potentially loop through the extended LAN forever => spanning tree(Only the root bridge is still generating configuration messages.). But not scale.

Internetwork: An arbitrary collection of networks interconnected to provide some sort of host-host to packet delivery service.

Packet Delivery Model:Connectionless model for data delivery. Best-effort delivery (unreliable service)

MTU (Maximum Transmission Unit):Ethernet (1500 bytes), FDDI (4500 bytes) => split data to fragmentations => receiver reassemble

Classless Inter-Domain Routing (CIDR):use Variable Length Subnet Masking(VLSM) to split.(給予需求的address數即可), aggregate routes=> Excessive storage requirement at the routers.

IP Forwarding Revisited: It is also possible to have prefixes in the forwarding tables that overlap(use longest match)

Address Translation Protocol (ARP):A table of IP to physical address. Broadcast request if IP address not in table. target machine responds with its physical address. table entries are discarded if not refreshed(correctness)

Dynamic Host Configuration Protocol (DHCP): DHCP server is responsible for providing configuration information to hosts and maintains a pool of available addresses

Internet Control Message Protocol (ICMP): Defines a collection of error messages that are sent back to the source host whenever a router or host is unable to process an IP datagram successfully

Routing Information Protocol (RIP): a typical distance-vector routing protocol(Similar to build road sign direction)

Open Shortest Path First (OSPF): Link-State Interior Gateway Protocol used to distribute routing information within a single Autonomous System.(Dijkstra algorithm)

Autonomous system (AS): A collection of networks under the same administrative authority and share a common routing strategy

NRZ:Both the sending and decoding process is driven by a clock. Every clock cycle, the sender transmits a bit and the receiver recovers a bit. The sender and receiver have to be precisely synchronized.

Manchester: Doubles the rate at which the signal transitions are made on the link. Which means the receiver has half of the time to detect each pulse of the signal. The rate at which the signal changes is called the link’s baud rate. In Manchester the bit rate is half the baud rate

Framing: When node A wishes to transmit a frame to node B, it tells its adaptor to transmit a frame from the node’s memory. This results in a sequence of bits being sent over the link. The adaptor on node B then collects together the sequence of bits arriving on the link and deposits the corresponding frame in B’s memory. Recognizing exactly what set of bits constitute a frame—that is, determining where the frame begins and ends—is the central challenge faced by the adaptor. => PPP is common.

Error Detection: add redundant information to a frame that can be used to determine if errors have been introduced

* CRC (Cyclic Redundancy Check): Used in HDLC, DDCMP, CSMA/CD, Token Ring. uses Generator Polynomial which is available on both sender and receiver side
* Two Dimensional Parity (BISYNC): This results in an extra parity byte for the entire frame, in addition to a parity bit for each byte.
* Checksum(used in IP packet): The receiver performs the same calculation on the received data and compares the result with the received checksum

Reliable Transmission: using acknowledgements and timeouts to implement reliable delivery is sometimes called Automatic Repeat reQuest (ARQ). Use sequence number (When the sender retransmits frame 0, the receiver can determine that it is seeing a second copy of frame 0 rather than the first copy of frame 1 and therefore can ignore it (the receiver still acknowledges it, in case the first acknowledgement was lost)

Sliding Window Protocol’s solution:

* Negative Acknowledgement (NAK):Receiver sends NAK for frame 6 when frame 7 arrive (in the previous example). However this is unnecessary since sender’s timeout mechanism will be sufficient to catch the situation
* Additional Acknowledgement:Receiver sends additional ACK for frame 5 when frame 7 arrives. Sender uses duplicate ACK as a clue for frame loss
* Selective Acknowledgement:Receiver will acknowledge exactly those frames it has received, rather than the highest number frames. Receiver will acknowledge frames 7 and 8. Sender knows frame 6 is lost. Sender can keep the pipe full (additional complexity)

Ethernet:

1. Uses CSMA/CD technology. Use Manchester/other encoding schemes. Carrier Sense Multiple Access with Collision Detection. A set of nodes send and receive frames over a shared link. Carrier sense means that all nodes can distinguish between an idle and a busy link. Collision detection means that a node listens as it transmits and can therefore detect when a frame it is transmitting has collided with a frame transmitted by another node.
2. Multiple Ethernet segments can be joined together by repeaters. A repeater is a device that forwards digital signals.
3. Any signal placed on the Ethernet by a host is broadcast over the entire network
4. Each host on an Ethernet (in fact, every Ethernet host in the world) has a unique Ethernet Address. The address belongs to the adaptor, not the host.
5. ✓Idle: The adaptor transmits frames. • The upper bound of 1500 bytes in the message means that the adaptor can occupy the line for a fixed length of time. ✓ Busy: The adaptor waits for the line to go idle

✓Collision: Stop transmitting. After a random amount of time, it will sense the channel (if idle) before transmitting • It first makes sure to transmit (64-bit preamble + 32-bit jamming sequence = 96 bits) and then stops transmission • Each time the adaptor tries to transmit but fails, it doubles the amount of time it waits before trying again. • The strategy of doubling the delay interval between each retransmission attempt is known as Exponential Backoff

* Worse case
* So Ethernets work best under lightly loaded conditions and are easy to administer and maintain.

2. What is DNS? Please explain why DNS is designed at the hierarchy level. DNS is Domain Name System that translates domain names (e.g., www.example.com) into IP addresses (e.g., 192.168.1.1) Hierarchical design is to distribute authoritative functions for different regions (different countries) to reduce the matters of bottleneck requests, support load balance, security or simplify the process of finding the destination with the desired domain name by looking at the local DNS servers.

5. What are CDN and Caching? What do the services often use CDN and Caching at most? CDN (Content Delivery Network) is a network of geographically distributed servers or data centers that work together to deliver web content to users from the server that is physically closest to them. Caching is a technique to use temporary storage for frequently accessed data, such as web pages in a high-speed storage layer (cache) to reduce the need to fetch the data from the original source repeatedly. The services often use CDN and Caching: Web services (Facebook, Streaming Services, E-commerce, Search Engines, …)