1.Physical(Addressing by multiplexing)//Communication resource ---- bandwidth //How to share the channel --- multiplexing
2.Data Link (Addressing by MAC address)//Data transmission across a link ----- flow/error control//Interconnecting links ----- switch/bridge LAN //Interface between layer 1-2 ------ MAC **3.Network (Addressing by IP)**//Interconnecting multiple LAN -- multi-protocol gateway //Routing / switching -circuit/packet/virtual circuit
4.Transport (Addressing by IP+port)//End-to-end channels ----connection/connectionless/(un)reliable **5.Application**

The communication **channel** is the physical medium that is used to send the signal from the transmitter to the receiver. Whatever the physical medium used for transmission of the information, the essential feature is that the transmitted signal is corrupted in a random manner by a variety of possible mechanisms, --Wireline/Fibre-optic/Wireless/Storage/Electromagnetic/UnderWater acoustic channels.

The width of the frequency range transmitted without being strongly attenuated is called the bandwidth.
The bandwidth is a physical property of the transmission medium.depends on the construction, thickness, and length of a wire or fiber.

The amount of thermal noise present is measured by the ratio of the signal power to the noise power, called the **SNR**(Signal-to-Noise Ratio),S/N.

maximum number of bits/sec =Blog2(1+S/N)

Multiplexing is a method by which multiple analog message signals or digital data streams are combined into one signal over a shared medium. aim is to share an expensive resource.

Multiplexing technologies: SDMA :Space division multiple access TDMA : Time FDMA : Frequency CDMA : Code

Circuit switching: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 duration of the communication session. The circuit functions as if the nodes were physically connected as with an electrical circuit.

Packet switching groups all transmitted data–regardless of content, type, or structure – into suitably sized blocks, called packets. features delivery of variable-bit-rate data streams (sequences of packets) over a shared network.

1.Packet switching allows more users to use network!
2.great for burst data – Greater efficiency in terms of resource sharing – simpler, no call setup
3.excessive congestion: packet delay and loss – protocols needed for reliable data transfer, congestion control

Virtual-Circuit Packet Switching:Hybrid of circuit switching and packet switching.pre-established path (=virtual circuit) .Packets from different virtual circuits may be interleaved.

Link layer services----------Framing、Flow control、 Error detection and correction、Inter-connection of links

Framing: break the bit stream into discrete frames 1.Character count 2.Flag bytes with byte stuffing 3.Starting and ending flags, with bit stuffing 4.Physical layer coding violations

Flow control A fast sender and slow receiver problem. Solutions-1.Feed-back based flow control - 2.Rate-based flow control

Error detection and correction---Error detecting code and error correcting code
d--errors caused by signal attenuation, noise. --receiver detects presence of errors: signals sender for retransmission or drops frame
c--receiver identifies and corrects bit error(s) without resorting to retransmission

Forward error correction (FEC) or channel coding is a technique used for controlling errors in data transmission over unreliable or noisy communication channels. The central idea is the sender encodes their message in a redundant way by using an error-correcting code (ECC).//The redundancy allows the receiver to detect a limited number of errors that may occur anywhere in the message, and often to correct these errors without retransmission.//FEC gives the receiver the ability to correct errors without needing a reverse channel to request retransmission of data, but at the cost of a fixed, higher forward channel bandwidth.

Inter-connection of links 1.Switches 2.Hubs 3.Bridges

Sub-layer structure of data link layer----------Media access control (MAC)、Logic link control (LLC)

Media access control (MAC)
//The media access control (MAC) data communication protocol sub-layer, also known as the medium access control, is a sublayer of the data link layer specified in the seven-layer OSI model (layer 2). //It provides addressing and channel access control mechanisms that make it possible for several terminals or network nodes to communicate within a multiple access network that incorporates a shared medium

Logic link control (LLC)//Multiplexing protocols transmitted over the MAC layer (when transmitting) and decoding them (when receiving).//Providing node-to-node flow and error control

Mudium Acces protocols----------CSMA/CSMA/CD/Wirless LAN protocols---CSMA/CA

CMSA:1-persistent 、Nonpersistent、P-persistent CSMA(Carrier sense multiple access protocols**)** 定义：Protocols in which stations listen for a carrier (i.e., a transmission) and act accordingly are called carrier sense protocols.
1-p:When the sender (station) is ready to transmit data, it checks if the physical medium is busy. //If so, it senses the medium continually until it becomes idle, and then it transmits a piece of data (a frame).// In case of a collision, the sender waits for a random period of time and attempts to transmit again. //1-persistent CSMA is used in CSMA/CD systems including Ethernet.

collisions can still occur:propagation delay means two nodes may not hear each other’s transmission

collision:entire packet transmission time wasted **note:** role of distance & propagation delay in determining collision probability

n-p:A conscious attempt is made to be less greedy than in the previous one.//Before sending, a station senses the channel.
//If no one else is sending, the station begins doing so itself. //However, if the channel is already in use, the station does not continually sense it for the purpose of seizing it immediately upon detecting the end of the previous transmission. //Instead, it waits a random period of time and then repeats the algorithm. //Consequently, this algorithm leads to better channel utilization but longer delays than 1-persistent CSMA. Why? (a trade-off between collision rate and delay)
p-p: It applies to slotted channels //When a station becomes ready to send, it senses the channel. //If it is idle, it transmits with a probability p. With a probability q = 1 - p, it defers until the next slot. //If that slot is also idle, it either transmits or defers again, with probabilities p and q. //This process is repeated until either the frame has been transmitted or another station has begun transmitting.
//In the latter case, the unlucky station acts as if there had been a collision (i.e., it waits a random time and starts again). //If the station initially senses the channel busy, it waits until the next slot and applies the above algorithm.
CMSA/CD(CSMA with collision detection): If two stations sense the channel to be idle and begin transmitting simultaneously, they will both detect the collision almost immediately. Quickly terminating damaged frames saves time and bandwidth. is widely used on LANs in the MAC sublayer.

CSMA/CD can be in one of three states: contention, transmission, or idle.

Main procedure Is my frame ready for transmission? If yes, it goes on to the next point.//Is medium idle? If not, wait until it becomes ready//Start transmitting.//Did a collision occur? If so, go to collision detected procedure.//Reset retransmission counters and end frame transmission.

Collision detected procedure//Continue transmission until minimum packet time is reached to ensure that all receivers detect the collision.//Increment retransmission counter.//Was the maximum number of transmission attempts reached? If so, abort transmission.//Calculate and wait random backoff period based on number of collisions.//Re-enter main procedure at stage 1.

When a collision can be detected?//Propagation time along the cable *2//This will affect the frame size/ bit rate of Ethernet

How to detect a collision?//The sender keeps listening to the link//If it reads back something different from what it sent, then…//Special coding scheme is needed //Difficult for wireless link ->CSMA/CA

CSMA/CD with a single channel is inherently a half-duplex system. It is impossible for a station to transmit and receive frames at the same time

Wireless LAN protocols: The “hidden station problem” and “exposed station problem” of wireless LAN

CSMA/CA differs from CSMA/CD due to the nature of the medium, the radio frequency spectrum.

Collisions cannot be detected while occurring at the sending node, thus it is vital for CSMA/CA or another access method to be implemented. //One of the problems of wireless data communications is that it is not possible to listen while sending, therefore collision detection is not possible. //Another reason is the hidden terminal problem

Basic idea of CSMA/CA(CSMA with collision avoidance): the sender stimulates the receiver to output a short frame so that nearby stations will detect this transmission and avoid transmitting for a duration of the upcomming data frame

Collision avoidance is used to improve CSMA performance by not allowing wireless transmission of a node if another node is transmitting, thus reducing the probability of collision due to the use of a random truncated binary exponential backoff time.
– How to transmit frames to destination node • Switching by destination MAC address
– How to expand the network to connect different LANs • Connectivity between networks with different protocols
– What’s new in a network with a complex topology and how to solve the problem • Efficiency and reliability

Bridges :1.Connect multiple LANs in the data link layer 2. Bridges examine the data link layer address to do routing 3. They can transport any kind of packets to connect LANs with different protocols
Motivations of connecting multiple LANs
– Co-existance of multiple LANs in one organization, which involve to ask for a inter- connection
– Geographically distributed users ask for a inter-connection of LANs structure instead of a single LAN
– Split a logically single LAN into separate LANs to accommodate the load
– Geographical limitation forbids the single LAN plan, for example a long round-trip delay
– Reliability: inserting inter-connecting devices to prevent error spreading in the network
– Security: Inserting bridges at various places and being careful not to forward sensitive traffic can help

Internetworking----------
How network can be interconnected: //Concatenated virtual circuits //Connectionless internetworking //Tunneling //Internetwork routing//Fragmentation
Interconnecting devices: Hub, switch, router

Network layer in reality----------
IP address and related issues : An Internet Protocol address (IP address) is a numerical label assigned to each device (e.g., computer, printer) participating in a computer network that uses the Internet Protocol for communication.//An IP address serves two principal functions: host or network interface identification and location addressing.
Routing table using CIDR:Routers need a routing table including all the networks 1.Storage 2.Routing algorithm complexity
//Allocate the remaining IP in variable-sized blocks, without regard to classes//Build a lookup table with entries (IP_address, subnet mask, outgoing line)//Incoming packets are checked to find the entry by its IP
Addressing mapping between IP/MAC addresses: ARP, RARP, BOOTP, DHCP
ICMP (Internet Control Message Protocol) **ARP** (Address Resolution Protocol) **RARP** (Reverse ARP) **BOOTP** (Bootstrap Protocol) **DHCP** (Dynamic Host Configuration Protocol)
ARP://Data link layer hardware does not understand IP address //A mapping between the MAC/physical address and the IP address is needed//To send information between two hosts
RARP://The Reverse Address Resolution Protocol (RARP) is an obsolete computer networking protocol used by a host computer to request its Internet Protocol (IPv4) address from an administrative host, when it has available its Link Layer or hardware address, such as a MAC address.//RARP requires one or more server hosts to maintain a database of mappings of Link Layer addresses to their respective protocol addresses. Media Access Control (MAC) addresses needed to be individually configured on the servers by an administrator. RARP was limited to serving only IP addresses.//Broadcast MAC address to the RARP server and get the correspondent IP address//The broadcast is sent to the destination address of all 1’s(broadcast in the local network), so it will not be forwarded by routers and therefore each network an RARP server is needed.
BOOTP://The Bootstrap Protocol, or BOOTP, is a network protocol used by a network client to obtain an IP address from a configuration server.//Different with the RARP, BOOTP use UDP to messages, which can be forwarded by routers.
//BOOTP is usually used during the bootstrap process when a computer is starting up. A BOOTP configuration server assigns an IP address to each client from a pool of addresses. //BOOTP uses the User Datagram Protocol (UDP) as a transport on IPv4 networks only.
//The BOOTP server requires manual configuration of tables mapping addresses. For a new host added to a network, its mapping item has to be added manually.
DHCP://The Dynamic Host Configuration Protocol (DHCP) is a network configuration protocol for hosts on Internet Protocol (IP) networks. Computers that are connected to IP networks must be configured before they can communicate with other hosts. The most essential information needed is an IP address, and a default route and routing

prefix. DHCP eliminates the manual task by a network administrator. It also provides a central database of devices that are connected to the network and eliminates duplicate resource assignments.//In addition to IP addresses, DHCP also provides other configuration information, particularly the IP addresses of local Domain Name Server (DNS), network boot servers, or other service hosts.
//DHCP is used for IPv4 as well as IPv6. In most systems, it has largely replaced RARP and BOOTP.
//Broadcasting based mechanism using DHCP relay agents.

Elements of transport layer protocols----------

Addressing://Host + port //TSAP (Transport service access point)/ NSAP (Network service access point)
Basic scenario for a transport connection:(3 way handshake)1.A server process on host 2 attaches itself to a TSAP, waiting for an incoming call//2.A client application process on host 1 sends a CONNECT request to the TSAP //3.The server process responds and the connection is established //4.A client-server service is carried out by the connection //5.The connection is released
Relase:there are two styles of terminating a connection: asymmetric release and symmetric release. Asymmetric release is the way the telephone system works: when one party hangs up, the connection is broken. Symmetric release treats the connection as two sep
arate unidirectional connections and requires each one to be released separately.
UDP&TCP:1. Connection differences:TCP is connection oriented.UDP is connectionless, that is, there is no need to establish a connection before sending data.//2. Security differences:TCP provides reliable service. The data transmitted through TCP connection is error free, no loss, no repetition, and arrives in order.UDP does its best to deliver, i.e. reliable delivery is not guaranteed.//3. The difference of transmission efficiency:TCP transmission efficiency is relatively low.UDP transmission efficiency is high, suitable for high-speed transmission and real-time communication or broadcast communication.//4. Differences in the number of connected objects:TCP connections can only be point-to-point, one-to-one.UDP supports one-to-one, one to many, many to one and many to many interactive communication.**TCP** - transmission control protocol, which provides connection oriented and reliable byte flow services. Before the client and server exchange data, a TCP connection must be established between the two parties before data can be transmitted. TCP provides overtime retransmission, discarding duplicate data, checking data, traffic control and other functions, ensuring that data can be transferred from one end to the other.**UDP** - user datagram protocol, which is a simple transport layer protocol for datagram. UDP does not provide reliability. It only sends the datagram that the application passes to the IP layer, but it can not guarantee that they can reach the destination. Because UDP does not need to establish a connection between the client and the server before transmitting the datagram, and there is no mechanism such as overtime retransmission, the transmission speed is very fast.**Application**: TCP protocol is adopted in transport layer for HTTP protocol. After entering IP address in browser, it establishes connection with server. TCP protocol is adopted, which is a connection oriented and reliable byte flow service.
UDP is the best choice when emphasis is placed on transmission performance rather than transmission integrity, such as audio, multimedia applications, and video conferencing. In addition, Tencent QQ is also used UDP protocol.
DNS (the Domain Name System)//The Domain Name System (DNS) is a hierarchical distributed naming system for computers, services, or any resource connected to the Internet or a private network. It associates various information with domain names assigned to each of the participating entities.//A Domain Name Service translates queries for domain names (which are meaningful to humans) into IP addresses for the purpose of locating computer services and devices worldwide.

Motivations://The Domain Name System makes it possible to assign domain names to groups of Internet resources and users in a meaningful way, independent of each entity's physical location. //Because of this, World Wide Web (WWW) hyperlinks and Internet contact information can remain consistent and constant even if the current Internet routing arrangements change or the participant uses a mobile device. //Internet domain names are easier to remember than IP addresses //Users take advantage of this when they recite meaningful Uniform Resource Locators (URLs) and e-mail addresses without having to know how the computer actually locates them.
How it works: //The Domain Name System distributes the responsibility of assigning domain names and mapping those names to IP addresses by designating authoritative name servers for each domain. //Authoritative name servers are assigned to be responsible for their particular domains, and in turn can assign other authoritative name servers for their sub-domains. //This mechanism has made the DNS distributed and fault tolerant and has helped avoid the need for a single central register to be continually consulted and updated.
WWWArchitecture overview//Client-server structure//The client side: Browsers //The server side: Web pages
access: System architecture and communication show infomation: Brower/helper/plug-in find:Search engine
Work flow http://www.itu.org/home/index.html 协议：http DNS：www.itu.org/home 路径名：index.html
//The browser determines the URL//The browser asks DNS for the IP address of www.itu.org//DNS replies with the IP 156.106.192.32 //The browser makes a TCP connection to port 80 on 156.106.192.32//It sends over a request asking for the file /home/index.html
//The www.itu.gov server sends back the file /home/index.html//The TCP connection is released
//The browser displays the text of the received file//The browser fetches and displays all images in the file

Symmetric cryptography methods

-**Substitution ciphers--**The letters of plaintext are replaced by other letters or by numbers or symbols.1 If the plaintext is viewed as a sequence of bits, then substitution involves replacing plaintext bit patterns with ciphertext bit patterns.
-**Transposition ciphers**
-**Rotor machine**//Multiple stages of encryption can produce an algorithm that is significantly more difficult to cryptanalyze. This is as true of substitution ciphers as it is of transposition ciphers.//The machine consists of a set of independently rotating cylinders through which electrical pulses can flow. Each cylinder has 26 input pins and 26 output pins, with internal wiring that connects each input pin to a unique output pin.//The significance of the rotor machine today is that it points the way to the most widely used cipher ever: the Data Encryption Standard (DES).
-**Steganography** The methods of steganography conceal the existence of the message, whereas the methods of cryptography render the message unintelligible to outsiders by various transformations o f the text.//1.Character marking//2.Invisible ink//3.Pin punctures
-**One time pads** Using a random key that is as long as the message, so that the key need not be repeated. In addition, the key is to be used to encrypt and decrypt a single message, and then is discarded. Each new message requires a new key of the same length as the new message.Such a scheme, known as a one-time pad, is unbreakable.
-**Key sharing in quantum cryptography**

Public key cryptography----------
Motivation: //Conventionally all cryptographic systems have been based on the elementary tools of substitution and permutation//Public-key algorithms are based on mathematical functions rather than on substitution and permutation. //More important, public-key cryptography is asymmetric, involving the use of two separate keys, in contrast to symmetric encryption, which uses only one key. The use of two keys has profound consequences in the areas of confidentiality, key distribution, and authentication, as we shall see.
Public key cryptography:
Asymmetric algorithms rely on one key for encryption and a different but related key for decryption. These algorithms have the following important characteristic.
It is computationally infeasible to determine the decryption key given only knowledge of the cryptographic algorithm and the encryption key.
In addition, some algorithms, such as RSA, also exhibit the following characteristic.
Either of the two related keys can be used for encryption, with the other used for decryption.
Key component: A one-way function, which is one that maps a domain into a range such that every function value has a unique inverse, with the condition that the calculation of the function is easy, whereas the calculation of the inverse is infeasible

Security services

-**Data confidentiality**//Disclosure: Release of message contents to any person or process not possessing the appropriate cryptographic key.//Traffic analysis: Discovery of the pattern of traffic between parties. In a connection-oriented application, the frequency and duration of connections could be determined. In either a connection-oriented or connectionless environment, the number and length of messages between parties could be determined.
-**Data integrity:** //Message authentication is a mechanism or service used to verify the integrity of a message. Message authentication assures that data received are exactly as sent (i.e., contain no modification, insertion, deletion, or replay). In many cases, there is a requirement that the authentication mechanism assures that purported identity of the sender is valid.//When a hash function is used to provide message authentication, the hash function value is often referred to as a message digest.
-**Authentication:1.**Authentication is the technique by which a process verifies that its communication partner is who it is supposed to be and not an imposter.
2. --General model://Alice starts out by sending a message either to Bob or to a trusted KDC (Key distribution center).//Several other message exchanges follow in various direction, during which Trudy may intercept, modify or replay them in order to trick Alice and Bob//When the protocol has been completed so that both Alice and Bob are sure about the identifications of the counterparts, in most of the protocols , they will also have established a secret session key for use in the upcoming conversation.//The reason of introducing the session key is to reduce the amount of traffic using the user’ s secrete keys or public keys, so that to reduce the amount of ciphertext and intruder can obtain.
Basic concepts
1.Physical--Bandwidth, multiplexing, switching
2.Data link--FEC, flow control, MAC address, MAC protocols, switch/bridge, LAN, VLAN
3.Network--Routing algorithms, IP/CIDR, ICMP, NAT, routing table, routers, internetworking
4.Transport--Transport service primitives, TCP/UDP and their applications
5.Application-Web, DNS, Email
6.Security--Encryption, symmetric/asymmetric encryption, authentication, data integrity, confidentiality
What’ s the structure of communication systems?Hosts, links/channel, internetworking, information theory
How users can exchange information through the network?
Multiplexing, MAC, Addressing(MAC/IP), routing/switching, connection establishment
How to exchange information safely?FEC, flow control(data link/transport), routing, connection, security
What’ s the essential components of LANs?Framing, MAC, addressing, switching
How to send data across network?1.Transport->network->data link-> physical layer
How the protocols are implemented in this procedure?
--Internet / TCP/IP ----------
How to design a subnetwork?IP, CIDR, routers, routing table
What kind of devices/protocols/technologies will be involved in a campus network?
LAN (Ethernet/WLAN), MAC, IP, DNS, ARP, NAT, switch, bridge, router, routing, TCP/UDP, VLAN, VPN, security
How to access a web?
Protocols/hardwares involved in this procedure (access network, Ethernet/WLAN/MAC, routers/routing, IP, TCP, DNS, Web server
--Network security
How to protect data?Integrity, confidentiality, data authentication
How to identify users?Authentication
How to identify user/protect data? Digital signature
How to use symmetric/asymmetric encryption and other mechanisms to achieve network security