Cheat sheet of computer networks

Network Topologies:

Name	Description
Bus Topology	A bus topology, also called a line topology, is a type of network topology in which all network devices are connected through a central RJ-45 network cable or coaxial cable.
Ring Topology	A ring topology is a type of network topology in which each device is connected to two other devices on either side using RJ-45 or coaxial cables.
Star Topology	A star topology is a network topology in which each element of the network is physically connected to a central node such as a router, hub, or switch. In a star topology, hubs act as servers, and connecting nodes act as clients.
Mesh Topology	In a mesh topology, each node is connected to at least one other node and often to multiple nodes. Each node can send and receive messages from other nodes.
Tree Topology	A tree topology is a hybrid network topology in which star networks are interconnected by bus networks. Tree networks are hierarchical and each node can have any number of child nodes.
Hybrid Topology	A hybrid topology is a type of network topology that uses two or more different network topologies. These topologies can include mixed bus topologies, mesh topologies, ring topologies, star topologies, and tree topologies.

Types of Network:

Network Type	Description
PAN	Personal Network is a network consisting of only a small number of devices owned by an individual.
LAN	A local area network is a network that covers a small area (for example, a company's network).
WAN	A wide Area Network is a network that includes many devices and covers a large area. Usually collectively owned.
MAN	MAN stands for Metropolitan Area Network. It is a computer network that connects a findnumber of LANs to form a larger network so that the computer resources can be shared.

TCP/IP Model and OSI Model:

TCP/IP	OSI Model	Protocols
Application Layer	Application Layer	DNS, DHCP, FTP, HTTPS, IMAP, LDAP, NTP,POP3, RTP, RTSP, SSH, SIP, SMTP, SNMP, Telnet, TFTP
	Presentation Layer	JPEG, MIDI, MPEG, PICT, TIFF
	Session Layer	NetBIOS, NFS, PAP, SCP, SQL, ZIP
Transport Layer	Transport Layer	TCP, UDP
Internet Layer	Network Layer	ICMP, IGMP, IPsec, IPv4, IPv6, IPX, RIP
Link Layer	Data Link Layer	ARP, ATM, CDP, FDDI, Frame Relay, HDLC, MPLS, PPP, STP, Token Ring
	Physical Layer	Bluetooth, Ethernet, DSL, ISDN, 802.11 Wi-Fi

Computer Network Protocols:

Network Protocol	Description	Port number of protocol
Ethernet	A family of protocols that specify how devices on the same network segment format and transmit data.	44818, 2222
Wi-Fi or WLAN	A family of protocols that deal with wireless transmission.	–
TCP	Splits data into packets (reassembles later). Error checking is also included, as the acknowledgment is expected to be sent within a specified timeframe.	22
UDP	User Datagram Protocol	4096-65535
IP	Every device has an IP address. Packets are “addressed” to ensure they reach the correct user.	–
HTTP	Used to access web pages from a web server.	80
HTTP’S	uses encryption to protect data.	443
FTP	File Transfer Protocol: Handles file uploads and downloads, transferring data and programs.	21
SMTP	SMTP server has a database of user email addresses. Internet Message Access Protocol: Handles incoming mail.	587
IMAP	Internet Message Access Protocol: Process incoming mail.	993
ARP	ARP finds a host’s hardware address (also known as MAC (Media	–

Network Protocol	Description	Port number of protocol
	Access Control) address) based on its known IP address.	
DNS	DNS is the host name for the IP address translation service. DNS is a distributed database implemented on a hierarchy of name servers. It is an application layer protocol for messaging between clients and servers.	53
FTPS	FTPS is known as FTP SSL which refers to File Transfer Protocol (FTP) over Secure Sockets Layer (SSL) which is more secure from FTP. FTPS also called as File Transfer Protocol Secure.	21
POP3	POP3 is a simple protocol that only allows downloading messages from your Inbox to your local computer.	110
SIP	Session Initiation Protocol was designed by IETF and is described in RFC 3261. It's the protocol of application layer that describes the way to found out Internet telephone calls, video conferences and other multimedia connections, manage them and terminate them.	5060,5061
SMB	The SMB protocol was developed by Microsoft for direct file sharing over local networks.	139
SNMP	SNMP is an application layer protocol that uses UDP port numbers 161/162. SNMP is also used to monitor networks, detect network errors, and sometimes configure remote devices.	161
SSH	SSH (Secure Shell) is the permissions used by the SSH protocol. That is, a cryptographic network protocol used to send encrypted data over a network.	22
VNC	VNC stands for Virtual Network Communication.	5900
RPC	Remote Procedure Call (RPC) is a powerful technique for building distributed client-server based applications. It is based on extending traditional calls to local procedures so that the called procedure does not have to be in the same address space as the calling procedure.	1024 to 5000
NFS	NFS uses file handles to uniquely identify the file or directory on which the current operation is being performed. Internet Control Message Protocol (ICMP) to provide error control. Used for reporting errors and administrative queries.	2049
ICMP	Internet Control Message Protocol(ICMP) to provide an error control. It is used for reporting errors and management queries.	–
BOOTP	Bootstrap Protocol (BOOTP) is a network protocol used by network management to assign IP addresses to each member of that network	67

Network Protocol	Description	Port number of protocol
	in order to join other network devices through a main server.	
DHCP	Dynamic Host Configuration Protocol (DHCP) is an application layer protocol. DHCP is based on a client-server model, based on discoveries, offers, requests, and ACKs.	68
NAT	Network Address Translation (NAT) is the process of translating one or more local IP addresses into one or more global IP addresses, or vice versa, in order to provide Internet access to local hosts.	5351
PPP	Point-to-Point Protocol (PPP) is basically an asymmetric protocol suite for various connections or links without framing. H. Raw bit pipe. PPP also expects other protocols to establish connections, authenticate users, and carry network layer data as well.	1994
RIP	Routing Information Protocol (RIP) is a dynamic routing protocol that uses hop count as a routing metric to find the best path between source and destination networks.	520
OSPF	Open Shortest Path First (OSPF) is a link-state routing protocol used to find the best path between a source and destination router using its own shortest path first).	89
EIGRP	Enhanced Interior Gateway Routing Protocol (EIGRP) is a dynamic routing protocol used to find the best path and deliver packets between any two Layer 3 devices.	88
BGP	Border Gateway Protocol (BGP) is a protocol used to exchange Internet routing information and is used between ISPs in different ASes.	179
STP	Spanning Tree Protocol (STP) is used to create a loop-free network by monitoring the network, tracking all connections, and shutting down the least redundant connections.	0 to 255
RARP	RARP, stand for Reverse Address Resolution Protocol, is a computer network-based protocol used by client computers to request IP addresses from a gateway server’s Address Resolution Protocol table or cache.	–
LAPD	The D-channel LAPD or Link Access Protocol is basically the Layer 2 protocol normally required for the ISDN D-channel. It is derived from the LAPB (Link Access Protocol Balanced) protocol.	–
IPsec	IP Security (IPSec) is a standard suite of Internet Engineering Task Force (IETF) protocols between two communication points on IP networks to provide data authentication, integrity, and	4500

Network Protocol	Description	Port number of protocol
	confidentiality. It also defines encrypted, decrypted, and authenticated packets.	
ASCII	ASCII (American Standard Code for Information Interchange) is the standard character encoding used in telecommunications. The ASCII representation "ask-ee" is strictly a 7-bit code based on the English alphabet. ASCII codes are used to represent alphanumeric data.	9500
EBCDIC	EBCDIC (Extended Binary Encoded Decimal Interchange Code) (pronounced "ehb-suh-dik" or "ehb-kuh-dik") is an alphanumeric binary code developed by IBM to run large-scale computer systems .	–
X.25 PAD	X.25 is an International Telecommunication Union Telecommunication Standardization Sector (ITU-T) protocol standard simply for Wide Area Network (WAN) communications that basically describes how the connections among user devices and network devices are established and maintained.	–
HDLC	High-Level Data Link Control (HDLC) commonly uses the term "frame" to denote units or logs of units of data that are frequently transmitted or transmitted from one station to another, express. Each frame on the link must start and end with a flag sequence field (F).	–
SLIP	SLIP stands for Serial Line Internet Protocol. It is a TCP/IP implementation which was described under RFC 1055 (Request for Comments).	
LAP	Link Access Procedure (LAP) is basically considered as an ITU family of Data Link Layer (DLL) protocols that are subsets of High-Level Data Link Control (HDLC). LAP is particularly derived from IBM's System Development Life Cycle (SDLC).	–
NCP	Network Control Protocol (NCP) is a set of protocols that are part of Point-to-Point Protocol (PPP).	524
Mobile IP	Mobile IP is a communication protocol (created by extending the Internet Protocol, IP) that allows a user to move from one network to another using the same her IP address.	434
VOIP	Voice over Internet Protocol (VoIP), is a technology that allowing you to make voice calls over a broadband Internet connection instead of an analog (regular) phone line. Some VoIP services allow you to call people using the same service, but others may allow you to call anyone.	5060
LDAP	Lightweight Directory Access Protocol (LDAP) is an internet protocol works on TCP/IP, used to access information from directories. LDAP protocol is basically used to access an active	389

Network Protocol	Description	Port number of protocol
	directory.	
GRE	GRE or Generic Routing Encapsulation is a tunneling protocol developed by Cisco. It encapsulates IP packets i.e. deliverable inner packets into outer packets.	47
AH	The HTTP headers Authorization header is a request type header that used to contains the credentials information to authenticate a user through a server. If the server responds with 401 Unauthorized and the WWW-Authenticate header not usually.	51
ESP	Encapsulation security payload, also abbreviated as ESP plays a very important role in network security. ESP or Encapsulation security payload is an individual protocol in IPSec.	500
NNTP	Network News Transfer Protocol (NNTP) is the underlying protocol of UseNet, which is a worldwide discussion system which contains posts or articles which are known as news.	119
RPC-DCOM	DCOM- Distributed Component Object Model– helps remote object via running on a protocol known as the Object Remote Procedure Call (ORPC).	–
IRC	Internet Relay Chat (IRC) is an Internet application that was developed by Jakko Oikarinen in Finland. Chat is the most convenient immediate way to communicate with others via Internet.	6667

IEEE Standards:

Standards	Description
IEEE 802	LAN/MAN
IEEE 802.1	LAN/MAN Bridging and management
IEEE 802.1s	Multiple spanning tree
IEEE 802.1 w	Rapid reconfiguration of spanning tree
IEEE 802.1x	Port-based network access control
IEEE 802.2	Logical Link Control (LLC)
IEEE 802.3	CSMA/CD access method (Ethernet)
IEEE 802.3ae	10 Gigabit Ethernet
IEEE 802.4	Token passing bus access method and Physical layer specifications
IEEE 802.5	Token Ring access method and Physical layer specifications
IEEE 802.6	Distributed Queue Dual Bus (DQDB) access method and Physical layer specifications (MAN)
IEEE 802.7	Broadband LAN

Standards	Description
IEEE 802.8	Fiber Optic
IEEE 802.9	Isochronous LANs (standard withdrawn)
IEEE 802.10	Interoperable LAN/MAN Security
IEEE 802.11	Wireless LAN MAC and Physical layer specifications
IEEE 802.11a	Wireless with speed upto 54 Mbps
IEEE 802.11b	Wireless with speed upto 11 Mbps
IEEE 802.11g	Wireless with speed upto 54 Mbps
IEEE 802.11n	Wireless with speed upto 600 Mbps
IEEE 802.12	Demand-priority access method, physical layer and repeater specifications
IEEE 802.13	Not used
IEEE 802.14	Cable modems (proposed standard was withdrawn)
IEEE 802.15	Wireless Personal Area Network (WPAN)
IEEE 802.16	Wireless Metropolitan Area Network (Wireless MAN)
IEEE 802.17	Resilient Packet Ring (RPR) Access

Networking Devices:

Device	Description
Client	Any device, such as a workstation, laptop, tablet, or smartphone, that is used to access a network.
Server	Provides resources to network users, including email, web pages, or files.
Hub	A Layer 1 device that does not perform any inspection of traffic. A hub simply receives traffic in a port and repeats that traffic out of all the other ports.
Switch	A Layer 2 device that makes its forwarding decisions based on the destination Media Access Control (MAC) address. A switch learns which devices reside off which ports by examining the source MAC address. The switch then forwards traffic only to the appropriate port, and not to all the other ports.
Router	A Layer 3 device that makes forwarding decisions based on Internet Protocol (IP) addressing. Based on the routing table, the router intelligently forwards the traffic out of the appropriate interface.
Multilayer switch	Can operate at both Layer 2 and Layer 3. Also called a Layer 3 switch, a multilayer switch is a high-performance device that can switch traffic within the LAN and forward packets between subnets.
Media	Media can be copper cabling, fiber-optic cabling, or radio waves. Media varies in its cost, bandwidth capacity, and distance limitation.
Analog modem	Modem is short for modulator/demodulator. An analog modem converts the digital signals generated by a computer into analog signals that can travel over conventional

Device	Description
	phone lines.
Broadband modem	A digital modem used with high-speed DSL or cable Internet service. Both operate in a similar manner to the analog modem, but use higher broadband frequencies and transmission speeds.
Access point (AP)	A network device with a built-in antenna, transmitter, and adapter that provides a connection point between WLANs and a wired Ethernet LAN. APs usually have several wired RJ-45 ports to support LAN clients. Most small office or home office (SOHO) routers integrate an AP.

Cables in Networking Devices:

Ethernet Standards (IEEE)	Data Rate	Cable Fiber Type	Maximum Distance (IEEE)
Ethernet (10Base-FL)	10 Mbps	50m or 62.5um Multimode @ 850nm	2km
Fast Ethernet (100Base-FX)	100 Mbps	50m or 62.5um Multimode @ 1300nm	2km
Fast Ethernet (100Base-SX)	100 Mbps	50m or 62.5um Multimode @ 850nm	300m
Gigabit Ethernet (1000Base-SX)	1000 Mbps	50m Multimode @ 850nm	550m
Gigabit Ethernet (1000Base-SX)	1000 Mbps	62.5um Multimode @ 850nm	220m
Gigabit Ethernet (1000Base-LX)	1000 Mbps	50m or 62.5um Multimode @ 1300nm	550m
Gigabit Ethernet (1000Base-LX)	1000 Mbps	9um Singlemode @1310nm	5km
Gigabit Ethernet (1000Base-LH)	1000 Mbps	9um Singlemode @1550nm	70km

Types of Ethernet Networks:

Speed	Common Name	Informal IEEE Standard Name	Formal IEEE Standard Name	Cable Type, Maximum Length
10 Mbps	Ethernet	10BASE-T	802.3	Copper, 100 m
100 Mbps	Fast Ethernet	100BASE-T	802.3u	Copper, 100 m
1000 Mbps	Gigabit Ethernet	1000BASE-LX	802.3z	Fiber, 5000 m
1000 Mbps	Gigabit Ethernet	1000BASE-T	802.3ab	Copper, 100 m

Speed	Common Name	Informal IEEE Standard Name	Formal IEEE Standard Name	Cable Type, Maximum Length
10 Gbps	10 Gig Ethernet	10GBASE-T	802.3an	Copper, 100 m

Types of Network Connections:

Type	Description
Internet	A network of millions of interconnected and cooperatively connected computers is called the Internet. Internet includes people, resources and means of collaboration
Intranet	It is an internal private network built within an organization using Internet and World Wide Web standards and products that provides access to corporate information for the organization's employees.
Extranet	This is a type of network that allows external users to access an organization's intranet.

Transmission Meia:

- **Guided Media:**

Type of media	Description
Twisted Pair Cable	It is a superimposed winding of two separately insulated conductors. As a rule, several such pairs are grouped together in a protective cover. They are the most widely used transmission media.
Coaxial Cable	It has a PVC or Teflon insulating layer and an outer plastic sheath containing two parallel conductors, each with a separate conformal protective cover.
Optical Fiber Cable	It uses the concept of light reflection through a glass or plastic core. The core is surrounded by a less dense glass or plastic shell called the cladding. Used to transfer large amounts of data.
Stripline	Stripline is a transverse electromagnetic (TEM) transmission line medium invented by Robert M. Barrett at the Air Force Cambridge Research Center in the 1950s. Stripline is the earliest form of planar transmission line.
Microstripline	Conductive material is separated from the ground plane by a dielectric layer.

- **Unguided Media**:

Type of media	Description
Radio waves	These are easy to generate and can penetrate buildings. There is no need to align the transmit and receive antennas. Frequency Range: 3kHz – 1GHz AM radios, FM radios, and cordless phones use radio waves for transmission.
Microwaves	**Multiplexer types**: line-of-sight transmission. H. Transmitting and receiving antennas should be placed properly. The distance a signal travels is directly proportional to the height of the antenna. Frequency Range: 1GHz – 300GHz They are mainly used for mobile telephony and television distribution.
Infrared	Infrared is used for short distance communication. Obstacles cannot be penetrated. This prevents interference between systems. Frequency Range: 300GHz – 400THz It is used in TV remote controls, wireless mice, keyboards, printers, etc.

Types of Multiplexers:

Type	Description
Frequency Division Multiplexing (FDM)	The frequency spectrum is divided into logical channels and each user has exclusive access to his channel. It transmits signals in several different frequency ranges and multiple video channels over a single cable. Each signal is modulated onto a different carrier frequency and the carrier frequencies are separated by guard bands.
Time Division Multiplexing (TDM)	Each user gets full bandwidth for a short period of time on a regular basis. The entire channel is dedicated to her one user, but only for a short time.
Wavelength Division Multiplexing	This is the same as FDM but applied to fiber, with the difference that here the operating frequency is much higher, actually in the optical range. Due to its extremely high bandwidth, fiber optic has great potential.

Collision Detection:

Type	Description
Carrier Sense Multiple Access with Collision Detection (CSMA/CD)	In this method, after sending a frame, the station monitors the media to see if the transmission was successful. If successful, the transmission is terminated, otherwise the frame is retransmitted.
Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)	The basic idea behind CSMA/CA is that stations must be able to receive while transmitting in order to detect collisions from different stations. A collision in a wired network nearly doubles the energy of the received signal, allowing stations to detect a potential collision.
ALOHA	It was developed for wifi, but can also be used for shared media. Multiple stations can transmit data at the same time, which can lead to collisions and data corruption.

Network Layer Services:

Type	Description
Packetizing	The process of encapsulating data (also called payload) received from upper layers of the network into network layer packets at the source and decapsulating the payload from the network layer packets at the destination is called packetization.
Routing and Forwarding	These are two other services provided by the network layer. A network has many routes from a source to a destination. The network layer sets some strategies for finding the best possible route. This process is called routing.

Mode of Communication:

Types	Description
Simplex Mode	In simplex mode, communication is one-way, like one-way. Only one of the two devices on the link can transmit, the other can only receive. Simplex mode allows data to be sent in one direction using the full capacity of the channel.
Half-Duplex Mode	In half-duplex mode, each station can both transmit and receive, but not at the same time. When one device transmits, the other device can only receive and vice versa. Half-duplex mode is used when simultaneous communication in both directions is not required.
Full-Duplex Mode	In full-duplex mode, both stations can transmit and receive at the same time. In full-duplex mode, signals in one direction share the capacity of the link with signals in the other direction. This sharing can be done in two ways: • Either the link must contain two physically separate transmission paths, one for sending and the other for receiving. • Or the capacity is divided between signals traveling in both directions.

Classes in Computer Networking:

CLASS	LEADING BITS	NET ID BITS	HOST ID BITS	NO. OF NETWORKS	ADDRESSES PER NETWORK	START ADDRESS	END ADDRESS
CLASS A	0	8	24	27 (128)	24 2 (16,777,216)	0.0.0.0	127.255.255.255
CLASS B	10	16	16	14 2 (16,384)	16 2 (65,536)	128.0.0.0	191.255.255.255
CLASS C	110	24	8	21 2 (2,097,152)	8 2 (256)	192.0.0.0	223.255.255.255
CLASS D	1110	NOT DEFINED	NOT DEFINED	NOT DEFINED	NOT DEFINED	224.0.0.0	239.255.255.255
CLASS E	1111	NOT DEFINED	NOT DEFINED	NOT DEFINED	NOT DEFINED	240.0.0.0	255.255.255.255

Subnet Address or Subnet ID Using/16Prefix	1st Usable IP Address	Last usable IP Address	Broadcast Address
120.0.0.0/24	120.0.0.1	120.0.255.254	120.0.255.255
120.1.0.0/24	120.1.0.1	120.1.255.254	120.1.255.255
120.2.0.0/24	120.2.0.1	120.2.255.254	120.2.255.255
120.3.0.0/24	120.3.0.1	120.3.255.254	120.3.255.255
120.100.0.0/24	120.100.0.1	120.100.255.254	120.100.255.255
120.101.0.0/24	120.101.0.1	120.101.255.254	120.101.255.255
120.200.0.0/24	120.200.0.1	120.200.255.254	120.200.255.255
120.201.0.0/24	120.201.0.1	120.201.255.254	120.201.255.255
120.253.0.0/24	120.253.0.1	120.253.255.254	120.253.255.255
120.254.0.0/24	120.254.0.1	120.254.255.254	120.254.255.255

Subnet Address or Subnet ID Using/16Prefix	1st Usable IP Address	Last usable IP Address	Broadcast Address
120.255.0.0/24	120.255.0.1	120.255.255.254	120.255.255.255

Subnetting:

Private IP Address with Subnet Mask	Private IP Range	Private IP Range denoted in CIDR
10.0.0.0 255.0.0.0	10.0.0.0 to 10.255.255.255	10.0.0.0/8
172.16.0.0 255.240.0.0	172.16.0.0 to 172.31.255.255	172.16.0.0/12
192.168.0.0 255.255.0.0	192.168.0.0 to 192.168.255.255	192.168.0.0/16

CIDR	SUBNET MASK	WILDCARD MASK	# OF IP ADDRESSES	# OF USABLE IP ADDRESSES
/32	255.255.255.255	0.0.0.0	1	1
/31	255.255.255.254	0.0.0.1	2	2*
/30	255.255.255.252	0.0.0.3	4	2
/29	255.255.255.248	0.0.0.7	8	6
/28	255.255.255.240	0.0.0.15	16	14
/27	255.255.255.224	0.0.0.31	32	30
/26	255.255.255.192	0.0.0.63	64	62
/25	255.255.255.128	0.0.0.127	128	126
/24	255.255.255.0	0.0.0.255	256	254
/23	255.255.254.0	0.0.1.255	512	510
/22	255.255.252.0	0.0.3.255	1,024	1,022
/21	255.255.248.0	0.0.7.255	2,048	2,046
/20	255.255.240.0	0.0.15.255	4,096	4,094
/19	255.255.224.0	0.0.31.255	8,192	8,190
/18	255.255.192.0	0.0.63.255	16,384	16,382
/17	255.255.128.0	0.0.127.255	32,768	32,766
/16	255.255.0.0	0.0.255.255	65,536	65,534
/15	255.254.0.0	0.1.255.255	131,072	131,070
/14	255.252.0.0	0.3.255.255	262,144	262,142
/13	255.248.0.0	0.7.255.255	524,288	524,286
/12	255.240.0.0	0.15.255.255	1,048,576	1,048,574
/11	255.224.0.0	0.31.255.255	2,097,152	2,097,150
/10	255.192.0.0	0.63.255.255	4,194,304	4,194,302
/9	255.128.0.0	0.127.255.255	8,388,608	8,388,606
/8	255.0.0.0	0.255.255.255	16,777,216	16,777,214
/7	254.0.0.0	1.255.255.255	33,554,432	33,554,430
/6	252.0.0.0	3.255.255.255	67,108,864	67,108,862
/5	248.0.0.0	7.255.255.255	134,217,728	134,217,726
/4	240.0.0.0	15.255.255.255	268,435,456	268,435,454

CIDR	SUBNET MASK	WILDCARD MASK	# OF IP ADDRESSES	# OF USABLE IP ADDRESSES
/3	224.0.0.0	31.255.255.255	536,870,912	536,870,910
/2	192.0.0.0	63.255.255.255	1,073,741,824	1,073,741,822
/1	128.0.0.0	127.255.255.255	2,147,483,648	2,147,483,646
/0	0.0.0.0	255.255.255.255	4,294,967,296	4,294,967,294

Methods of Network Security:

Method	Description
Authentication	Verify a user’s identity, usually by asking them to enter a password or biometric identifier.
Encryption	Encrypt data with a key, that is, the same key is required to decrypt the data. This is how HTTPS works.
Firewalls	Protect the network from unauthorized access.
MAC Address Filtering	Allow devices to access or be prevented from accessing the network based on their physical address embedded in the device’s network adapter.

GeeksforGeeks

https://www.geeksforgeeks.org/computer-network-cheat-sheet/