Computer Networking

Basics:

- **Network**: A computer network is a digital telecommunications network for sharing resources between nodes, which are computing devices that use a common telecommunications technology
- **Node**: A computing device.
- **Bus network**: All the devices are connected on one single long cable.
- **Client**: A client is a piece of computer hardware or software that accesses a service available by a server
- **Server**: A server is a computer program or device that provides functionality for other programs or devices called clients
- **Protocol**: A set of rules used in communication between clients

Network Devices:

- **Repeater**: A repeater is an electronic device that receives a signal and retransmits it.
- **Hub**: A hub is essentially a multi-port repeater. Wireless Access Point is essentially a hub in the air.
    - Active Hub: These are the hubs that have their own power supply and can clean, boost, and relay the signal along with the network. It serves both as a repeater as well as a wiring center.
    - Passive Hub: These are the hubs that collect wiring from nodes and power supply from the active hub. They are generally used to relay signals with cleaning or boosting them.
    - Intelligent Hub: It works like active hubs and includes remote management capabilities. They also provide flexible data rates to network devices. It also enables an administrator to monitor the traffic passing through the hub and to configure each port in the hub.
- **Bridge**: A bridge is a repeater with add on the functionality of filtering content by reading mac addresses of source and destination. It was mostly used to interconnect two LANs.
    - Transparent Bridge: These are the bridges in which the stations are completely unaware of the bridge's existence.
    - Source Routing Bridge: In these bridges, routing operation is performed by the source station and the frame specifies the route to follow.
- **Switch**: A switch reads each frame and has the intelligence to transmit data to the port it is destined for based on MAC addresses.
- **Router**: A router is a device like a switch that routes data packets based on their IP addresses. The router is mainly a Network Layer device.
- **Wireless Access Point**: A wireless access point is a networking device that allows wireless-capable devices to connect to a wired network.
- **Wireless LAN Controller**: A WLAN controller is used to manage large scale deployments of light weight and normal wireless access points.
- **Firewall**: A firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules.
- **IDS**: It's a software system that warns if there is an intrusion. They just get copies of packets that are analyzed.
- **IPS**: It's a software system can alert you if there may be a problem and block the same. They stay inline of the network and detect and block intrusions.
- **Email Security Appliance**: The Email Security Appliance is an email security gateway product. It is designed to detect and block a wide variety of email-borne threats, such as malware, spam, and phishing attempts.
- **Load Balancer**: A load balancer is a device that acts as a reverse proxy and distributes network or application traffic across several servers.

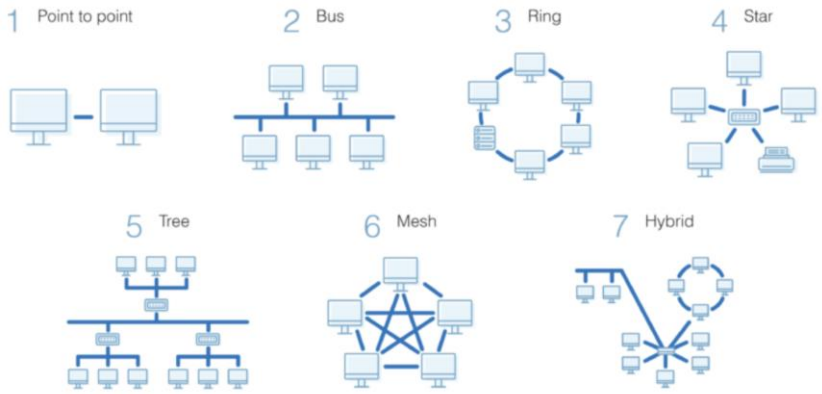
Types of Networks based on Area:

- WAN: A Wide Area Network is a telecommunications network that extends over a large geographical area for the primary purpose of computer networking.

- LAN: A Local Area Network is a computer network that interconnects computers within a limited area such as a residence, school and so on
- MAN: Metropolitan Area Network
- Wireless Local Area Network (WLAN)
- Campus Area Network (CAN)
- Storage Area Network (SAN)
- Passive Optical Local Area Network (POLAN)
- Enterprise Private Network (EPN)
- Virtual Private Network (VPN)
- Personal Area Network (PAN)

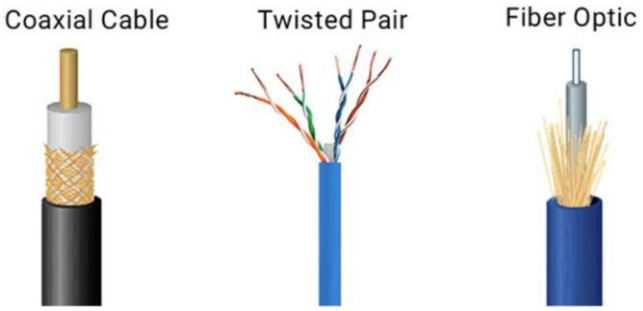
Types of Networks based on Topology:

- Mesh Topology
- Ring Topology
- Bus Topology
- Star Topology
- Hybrid Topology
- Point to Point Topology



Cable Types:

- **Coaxial Cabling**: Coaxial cable has an inner conductor that runs down the middle of the cable. This type of cabling comes in two types, thinnet and thicknet. Max Transmission Speed of 10 Mbps
- **Twisted-pair Cabling**: Has four pair of wires. It comes in two versions, UTP (Unshielded Twisted-Pair) and STP (Shielded Twisted-Pair). Uses 8P8C/RJ45 Connector
- **Fiber-optic Cabling**: Uses optical fibers to transmit data in the form of light signals. There are two types of fiber-optic cables - Single-mode fiber (SMF) and Multi-mode fiber (MMF). Uses ST/SC Connectors



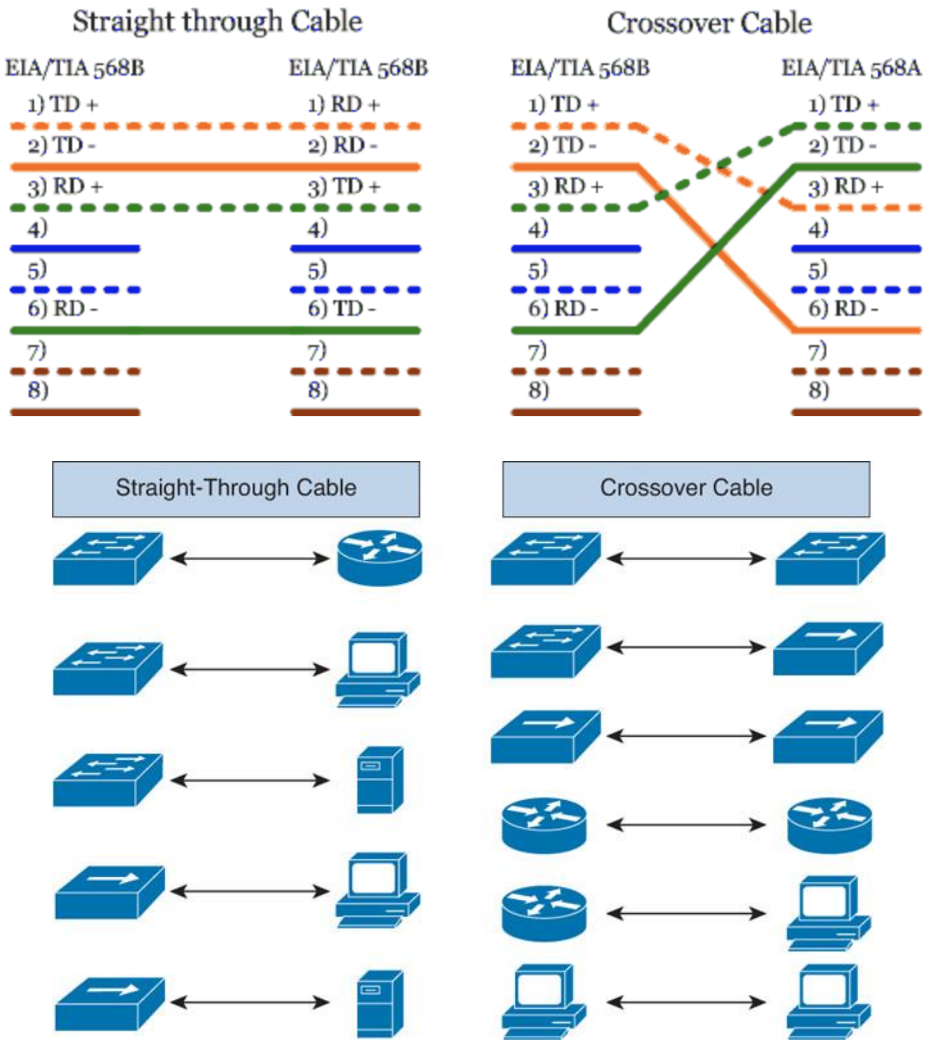
Ethernet Standards:

- **10Base-T** (IEEE 802.3): 10 Mbps with category 3 unshielded twisted pair (UTP) wiring, up to 100 meters long.

- **100Base-TX** (IEEE 802.3u): known as Fast Ethernet, uses category 5, 5E, or 6 UTP wiring, up to 100 meters long.
- **100Base-FX** (IEEE 802.3u): a version of Fast Ethernet that uses multi-mode optical fiber. Up to 412 meters long.
- **1000Base-CX** (IEEE 802.3z): uses copper twisted-pair cabling. Up to 25 meters long.
- **1000Base-T** (IEEE 802.3ab): Gigabit Ethernet that uses Category 5 UTP wiring. Up to 100 meters long.
- **1000Base-SX** (IEEE 802.3z): 1 Gigabit Ethernet running over multimode fiber-optic cable.
- **1000Base-LX** (IEEE 802.3z): 1 Gigabit Ethernet running over single-mode fiber.
- **10GBase-T** (802.3.an): 10 Gbps connections over category 5e, 6, and 7 UTP cables.

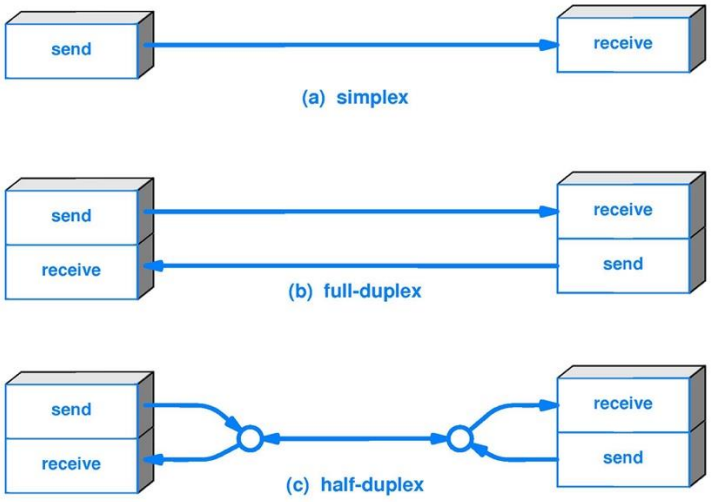
Ethernet Cable Forms:

- **Straight-through Cable:** On a straight through cable, the wired pins match. Straight through cable use one wiring standard: both ends use T568A wiring standard or both ends use T568B wiring standard.
- **Crossover Cable:** Crossover cable uses two different wiring standards: one end uses the T568A wiring standard, and the other end uses the T568B wiring standard. Pin1->Pin3 and Pin2->Pin6



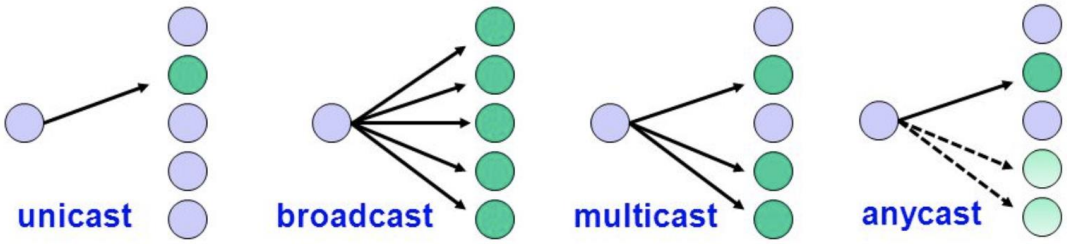
Data flow Types:

- **Simplex Mode:** Communication is unidirectional.
- **Half-Duplex Mode:** Each station can both transmit and receive, but not at the same time.
- **Full-Duplex Mode:** Both stations can transmit and receive simultaneously.



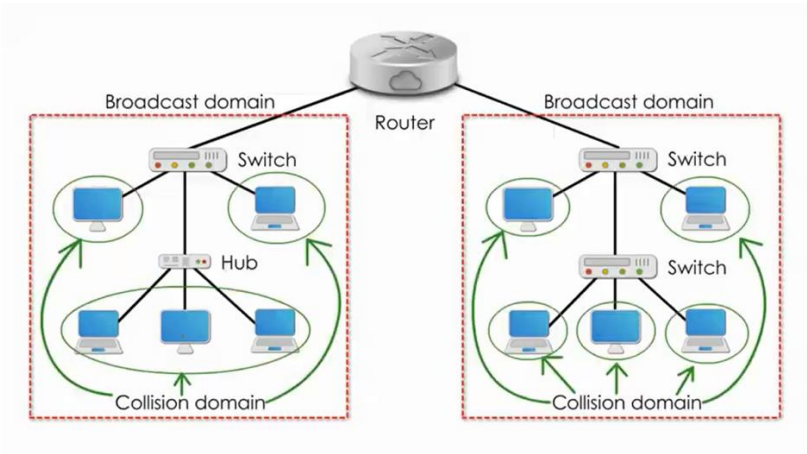
Communication Types:

- **Unicast:** Communication from one point to another point
- **Broadcast:** Communication from one point to all other points
- **Multicast:** Communication from one/more points to a set of other points
- **Anycast:** It is a network addressing and routing methodology in which a single destination IP address is shared by nodes in multiple locations.



Network Domain:

- **Broadcast Domain:** A broadcast domain is a logical division of a computer network, in which all nodes can reach each other by broadcast at the data link layer.
- **Collision Domain:** A collision domain is a network segment connected by a shared medium where simultaneous data transmissions collide with one another.



54321 Rule:

5 - the number of network segments
4 - the number of repeaters needed to join the segments into one collision domain
3 - the number of network segments that have active (transmitting) devices attached
2 - the number of segments that do not have active devices attached
1 - the number of collision domains

Types of Layered Models: Layers and Protocol Data Units (PDUs):

OSI Model:

1. Physical Layer (Bits)
2. Datalink Layer (Frame)
3. Network Layer (Packet)
4. Transport Layer (Segment)
5. Session Layer (Data)
6. Presentation Layer (Data)
7. Application Layer (Data)

TCP/IP Model (4):

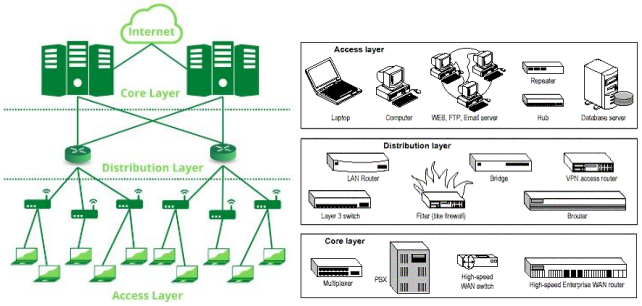
1. Physical Layer (Frame): Physical Addresses (MAC)
2. Network Layer (Packet): IP Addresses (IP)
3. Transport Layer (Segment): Port Addresses (Ports)
4. Application Layer (Data): Specific Addresses (Data)

TCP/IP Model (5 – In use by CCNA):

1. Physical Layer (Bits)
2. Datalink Layer (Frame): Physical Address (MAC)
3. Network Layer (Packet): IP Addresses (IP)
4. Transport Layer (Segment): Port Addresses (Ports)
5. Application Layer (Data): Specific Addresses (Data)

Cisco 3-Layer Model:

1. Core Layer: This layer is considered the backbone of the network and includes the high-end switches and high-speed cables such as fiber cables. This layer of the network does not route traffic at the LAN. In addition, no packet manipulation is done by devices in this layer. Rather, this layer is concerned with speed and ensures reliable delivery of packets
2. Distribution Layer: This layer includes LAN-based routers and layer 3 switches. This layer ensures that packets are properly routed between subnets and VLANs in your enterprise. This layer is also called the Workgroup layer.
3. Access Layer: This layer includes hubs and switches. This layer is also called the desktop layer because it focuses on connecting client nodes, such as workstations to the network. This layer ensures that packets are delivered to end user computers.



Math Review:

- Binary:
  - IPv4 addresses use Binary.
  - 2 possible values per bit (Base 2): 0,1
  - Total number of outcomes for a given number: 2^n (For example, for 8 bits: $2^8 = 256$)
  - To represent 255 in Binary

Base	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Binary Bit	1	1	1	1	1	1	1	1
Decimal	128	64	32	16	8	4	2	1

128+64+32+16+8+4+2+1 = 255

- IPv4 has 32 bits – 4 octets. 232 = 429,49,67,296 IP addresses

- Hexadecimal:
  - MAC addresses use Hexadecimal.
  - 16 possible values per bit (Base 16): 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F
  - Converting from Decimal to Hexadecimal (Ex: 224->E0):

    224 in Binary: 1110 0000 (Divide into 4 bits each)

    $1110_2 = 14_{10} = E_{16}$

    $0000_2 = 0_{10} = 0_{16}$

    Result: E0

IPv4 Addressing:

- Internet Protocol v4 is a connectionless network layer protocol. Each packet is treated independently in this protocol which allows the packets to take different paths as needed.
- An IPv4 address is a layer 3 logical address assigned by an administrator. It is used to identify specific devices on a network and must be unique in internet.
- Private IP addresses are NATted to public address when traffic is sent onto internet.
- Format of IP address:
  - 32 bits 4 octets of 8 bits (1byte) each
  - Network Address Portion (Network ID)
    - Identifies a specific network.
    - Routers look at destination of IP address and match to network address.
  - Host portion (Host ID):
    - Identifies a specific endpoint on a network.
- Address Classes to accommodate different sizes of network and aid in classifying networks:

Class A – Unicast	0.0.0.0 to 127.255.255.255	8 network bits, 24 host bits
Class B – Unicast	128.0.0.0 to 191.255.255.255	16 network bits, 16 host bits
Class C – Unicast	192.0.0.0 to 223.255.255.255	24 network bits, 8 host bits
Class D – Multicast	224.0.0.0 to 240.255.255.255	
Class E – Reserved for future	241.0.0.0 to 255.255.255.255	

- Exceptions, Reservations and Special addresses:
  - 0.0.0.0/8 - Default network
  - 127.0.0.0/8 – Local Loopback address.
  - 224.0.0.X – Link local multicasts, generally used by routing tables.
  - 224.0.0.5-224.0.0.6 - OSPF
  - Directed Broadcast address: Fill 1s in the entire host portion of the address.
  - Local Broadcast address: Fill 1s in all 32 bits. Generally used for DHCP address
  - 10.0.0.0/8 – Private IP address range (not routable on internet)
  - 172.16.0.0/12 – Private IP address range (not routable on internet)
  - 192.168.0.0/16 – Private IP address range (not routable on internet)
  - 169.254.0.0/16 – Non-routable Link Local Addresses (Automatic Private IP Addressing)
- Subnet Masks:
  - Used to determine network and host portion of a given IP address through AND operation.
  - Is the device remote (route through default gateway) or local (ARP)?
  - Class A: 255.0.0.0
  - Class B: 255.255.0.0
  - Class C: 255.255.255.0
  - Discontinuous subnet masks not supported:

    11110000.11111111.00000110.11000000 (240.244.3.191)

- Only contiguous subnet masks are supported.
  11111111.11110000.00000000.00000000 (255.240.0.0)
- Classless Inter Domain Routing (CIDR):
  - Replaces classful IP addressing with variable length subnet mask (VLSM)
  - CIDR notation /X where X denotes number of 1's present in binary form of a subnet mask.
  - Reduces wastage of big number of addresses.
  - Ex: /11 = 255.224.0.0

- Subnetting:
  - Work the following for a given IP address: Network address, First IP address, Last IP address, Broadcast address.
  - Binary method to work an IP address:
    - Subnet address: Fill the host portion with binary 0s.
    - Broadcast address: Fill the host portion with binary 1s.
    - First host: Fill the host portion with binary 0s and set the last bit to 1.
    - Last host: Fill the host portion with binary 1s and set the last bit to 0.
    - Ex: 172.16.35.123/20:
      Subnet: **172.16.0010 0000.0000 0000** = 172.16.32.0
      1st Host: **172.16.0010 0000.0000 0001** = 172.16.32.1
      Last Host: **172.16.0010 1111.1111 1110** = 172.16.47.254
      Broadcast: **172.16.0010 1111.1111 1111** = 172.16.47.255
  - Number of hosts in a network: $2^h - 2$ (h = number of bits in host portion)
  - Number of networks: 2^n (n = number of bits in network portion)
  - Number of subnets: 2^n (n = number of bits in variating network octet)

Connecting to Networking Devices:

- Connectors used: Serial Cable or RJ45 or USB.
- Protocols used: Telnet, SSH, GUI
- Review Cisco common CLI command reference

IPv4 Subnetting

packetlife.net

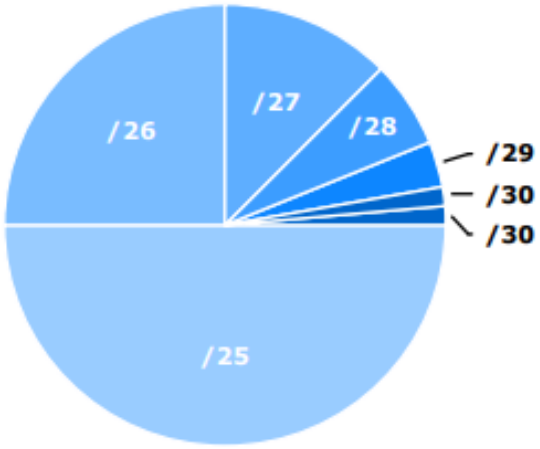
Subnets

CIDR	Subnet Mask	Addresses	Wildcard
/32	255.255.255.255	1	0.0.0.0
/31	255.255.255.254	2	0.0.0.1
/30	255.255.255.252	4	0.0.0.3
/29	255.255.255.248	8	0.0.0.7
/28	255.255.255.240	16	0.0.0.15
/27	255.255.255.224	32	0.0.0.31
/26	255.255.255.192	64	0.0.0.63
/25	255.255.255.128	128	0.0.0.127
/24	255.255.255.0	256	0.0.0.255
/23	255.255.254.0	512	0.0.1.255
/22	255.255.252.0	1,024	0.0.3.255
/21	255.255.248.0	2,048	0.0.7.255
/20	255.255.240.0	4,096	0.0.15.255
/19	255.255.224.0	8,192	0.0.31.255
/18	255.255.192.0	16,384	0.0.63.255
/17	255.255.128.0	32,768	0.0.127.255
/16	255.255.0.0	65,536	0.0.255.255
/15	255.254.0.0	131,072	0.1.255.255
/14	255.252.0.0	262,144	0.3.255.255
/13	255.248.0.0	524,288	0.7.255.255
/12	255.240.0.0	1,048,576	0.15.255.255
/11	255.224.0.0	2,097,152	0.31.255.255
/10	255.192.0.0	4,194,304	0.63.255.255
/9	255.128.0.0	8,388,608	0.127.255.255
/8	255.0.0.0	16,777,216	0.255.255.255
/7	254.0.0.0	33,554,432	1.255.255.255
/6	252.0.0.0	67,108,864	3.255.255.255
/5	248.0.0.0	134,217,728	7.255.255.255
/4	240.0.0.0	268,435,456	15.255.255.255
/3	224.0.0.0	536,870,912	31.255.255.255
/2	192.0.0.0	1,073,741,824	63.255.255.255
/1	128.0.0.0	2,147,483,648	127.255.255.255
/0	0.0.0.0	4,294,967,296	255.255.255.255

Decimal to Binary

Subnet Mask		Wildcard	
255	1111 1111	0	0000 0000
254	1111 1110	1	0000 0001
252	1111 1100	3	0000 0011
248	1111 1000	7	0000 0111
240	1111 0000	15	0000 1111
224	1110 0000	31	0001 1111
192	1100 0000	63	0011 1111
128	1000 0000	127	0111 1111
0	0000 0000	255	1111 1111

Subnet Proportion



Classful Ranges

A	0.0.0.0 – 127.255.255.255
B	128.0.0.0 - 191.255.255.255
C	192.0.0.0 - 223.255.255.255
D	224.0.0.0 - 239.255.255.255
E	240.0.0.0 - 255.255.255.255

Reserved Ranges

RFC 1918	10.0.0.0 - 10.255.255.255
Localhost	127.0.0.0 - 127.255.255.255
RFC 1918	172.16.0.0 - 172.31.255.255
RFC 1918	192.168.0.0 - 192.168.255.255

Terminology

CIDR
Classless interdomain routing was developed to provide more granularity than legacy classful addressing; CIDR notation is expressed as /XX

VLSM
Variable-length subnet masks are an arbitrary length between 0 and 32 bits; CIDR relies on VLSMs to define routes

TCP AND UDP PORT NUMBERS

ECHO	**7/TCP**		
ECHO	**7/UDP**		
FTP-DATA	**20/TCP**		**#FTP, DATA**
FTP	**21/TCP**		**#FTP, CONTROL**
SSH	**22/TCP**		**#SSH REMOTE LOGIN**
TELNET	**23/TCP**		
SMTP	**25/TCP**	**MAIL**	
TIME	37/TCP	TIMSERVER	
TIME	37/UDP	TIMSERVER	
RLP	39/UDP	RESOURCE	#RESOURCE LOCATION
NAMESERVER	42/TCP	NAME	#HOST NAME SERVER
NAMESERVER	42/UDP	NAME	#HOST NAME SERVER
NICNAME	43/TCP	WHOIS	
DNS	**53/TCP**		**#DOMAIN NAME SERVER**
DNS	**53/UDP**		**#DOMAIN NAME SERVER**
BOOTPS	**67/UDP**	**DHCPS**	**#BOOTSTRAP PROTOCOL**
BOOTPC	**68/UDP**	**DHCPC**	**#BOOTSTRAP PROTOCOL**
TFTP	**69/UDP**		**#TRIVIAL FILE TRANSFER**
HTTP	**80/TCP**	**WWW WWW-HTTP**	**#WORLD WIDE WEB**
KERBEROS	88/TCP	KRB5 KERBEROS-SEC	#KERBEROS
KERBEROS	88/UDP	KRB5 KERBEROS-SEC	#KERBEROS
RTELNET	107/TCP		#REMOTE TELNET SERVICE
POP2	109/TCP	POSTOFFICE	#POST OFFICE PROTOCOL
POP3	**110/TCP**		**#POST OFFICE PROTOCOL**
SQLSERV	118/TCP		#SQL SERVICES
NTP	**123/UDP**		**#NETWORK TIME PROTOCOL**
NETBIOS-NS	137/TCP	NBNAME	#NETBIOS NAME SERVICE
NETBIOS-NS	137/UDP	NBNAME	#NETBIOS NAME SERVICE
IMAP	**143/TCP**	**IMAP4**	**#INTERNET MESSAGE ACCESS PROTOCOL**
SQL-NET	150/TCP		
SQLSRV	156/TCP		
SNMP	**161/UDP**		**#SNMP**
SNMPTRAP	162/UDP	SNMP-TRAP	#SNMP TRAP
BGP	179/TCP		
IRC	**194/TCP**		**#INTERNET RELAY CHAT**
MFTP	349/TCP		
MFTP	349/UDP		
LDAP	**389/TCP**		
HTTPS	**443/TCP**	**MCOM**	**#HTTP OVER TLS/SSL**
HTTPS	**443/UDP**	**MCOM**	**#HTTP OVER TLS/SSL**
ISAKMP	**500/UDP**	**IKE**	**#INTERNET KEY EXCHANGE**
CMD	514/TCP	SHELL	
SYSLOG	514/UDP		
ROUTER	520/UDP	ROUTE ROUTED	
TIMED	525/UDP	TIMESERVER	
DHCPV6-CLIENT	546/TCP		#DHCPV6 CLIENT
DHCPV6-CLIENT	546/UDP		#DHCPV6 CLIENT
DHCPV6-SERVER	547/TCP		#DHCPV6 SERVER
DHCPV6-SERVER	547/UDP		#DHCPV6 SERVER
LDAPS	**636/TCP**	**SLDAP**	**#LDAP OVER TLS/SSL**
MSEXCH-ROUTING	691/TCP		#MS EXCHANGE ROUTING
MSEXCH-ROUTING	691/UDP		#MS EXCHANGE ROUTING
FTPS-DATA	989/TCP		#FTP DATA,OVER TLS/SSL
FTPS	990/TCP		#FTP CTRL OVER TLS/SSL
TELNETS	992/TCP		#TELNET OVER TLS/SSL
WINS	**1512/TCP**		**#WINDOWS NAME SERVICE**
WINS	**1512/UDP**		**#WINDOWS NAME SERVICE**
L2TP	**1701/UDP**		
H.323	**1718/TCP**		**#H.323 RAS (MULTICAST)**
H.323	**1719/TCP**		**#H.323 RAS (UNICAST)**
H.323	**1720/TCP**		**#H.323 CALL SIGNALLING**
PPTP	**1723/TCP**		**#POINT-TO-POINT**

		TUNNELING PROTOCOL
RADIUS	**1812/UDP**	**#RADIUS AUTHENTICATION**
SSO	**2258/UDP**	**#SINGLE SIGN OUT**
RDP	**3389/TCP**	**#REMOTE DESKTOP PROTOCOL**
MSFW-CONTROL	3847/TCP	#MICROSOFT FIREWALL
SDP-PORTMAPPER	3935/TCP	#SDP PORT MAPPER PROTOCOL
SDP-PORTMAPPER	3935/UDP	#SDP PORT MAPPER PROTOCOL
IPSEC	**4500/TCP**	**#MICROSOFT IPSEC NAT-T**
IPSEC	**4500/UDP**	**#MICROSOFT IPSEC NAT-T**
SIP	**5060/UDP**	**#NON-ENCRYPTED TRAFFIC**
SIP	**5061/UDP**	**#SIP OVER TLS**
MS-LICENSING	5720/TCP	#MICROSOFT LICENSING
MS-LICENSING	5720/UDP	#MICROSOFT LICENSING
MAN	9535/TCP	#REMOTE MAN SERVER

IP PORT NUMBERS

IP	**0**	**IP**	**# INTERNET PROTOCOL**
ICMP	**1**	**ICMP**	**# INTERNET CONTROL MESSAGE PROTOCOL**
GGP	3	GGP	# GATEWAY-GATEWAY PROTOCOL
TCP	**6**	**TCP**	**# TRANSMISSION CONTROL PROTOCOL**
EGP	8	EGP	# EXTERIOR GATEWAY PROTOCOL
PUP	12	PUP	# PARC UNIVERSAL PACKET PROTOCOL
UDP	**17**	**UDP**	**# USER DATAGRAM PROTOCOL**
HMP	20	HMP	# HOST MONITORING PROTOCOL
XNS-IDP	22	XNS-IDP	# XEROX NS IDP
RDP	27	RDP	# "RELIABLE DATAGRAM" PROTOCOL
IPV6	**41**	**IPV6**	**# INTERNET PROTOCOL IPV6**
IPV6-ROUTE	43	IPV6-ROUTE	# ROUTING HEADER FOR IPV6
IPV6-FRAG	44	IPV6-FRAG	# FRAGMENT HEADER FOR IPV6
ESP	**50**	**ESP**	**# ENCAPSULATING SECURITY PAYLOAD**
AH	**51**	**AH**	**# AUTHENTICATION HEADER**
IPV6-ICMP	58	IPV6-ICMP	# ICMP FOR IPV6
IPV6-NONXT	59	IPV6-NONXT	# NO NEXT HEADER FOR IPV6
IPV6-OPTS	60	IPV6-OPTS	# DESTINATION OPTIONS FOR IPV6

Cisco Common CLI Reference

`enable`	Switch to enable mode from user mode
`configure terminal`	Switch to configure terminal mode from enable mode
`disable`	To go back to user mode
`erase startup-config`	Delete existing startup-config
`show version`	To see the version of the firmware installed
`hostname`	To change the hostname of the device
`copy run start`	Saving configuration to NVRAM
`wr`	Same function as copy run start
`show ip int br`	See interfaces on the router
`show cdp neighbors`	To view the neighbors connected
`debug ip packet`	To trace all packets
`un all`	Disable all debugging

`ip dhcp pool <name>`
`> network <cidr>`
`> default-router <GW>`
`> network <cidr>`
`> dns-server <8.8.8.8>`
	To create a new dhcp pool, its network and other parameters in it

`ip dhcp excluded <ipaddr>`	To exclude an ip address being assigned