Subnetting Table

subnet mask	CIDR	subnets	*hosts	Max. VLANs
255.255.255.0	/24	1	254	1
255.255.255.128	/25	2	126	2
255.255.255.192	/26	4	62	4
255.255.255.224	/27	8	30	8
255.255.255.240	/28	16	14	16
255.255.255.248	/29	32	6	32
255.255.255.252	/30	64	2	64

*number of host IP addresses available for interfaces does not include unassignable network and broadcast address.

Binary to Decimal Conversion

0	0	0	0	0	0	0	0	= 0
1	1	1	1	1	1	1	1	= 255
128	**64**	**32**	**16**	**8**	**4**	**2**	**1**	bit value
8	7	6	5	4	3	2	1	bit position

Network Cabling Types

Cable Type	Examples
straight-through	host to switch, switch to router
rollover	console port only
crossover	switch to switch, router to router
serial	WAN, DSL, router to telco

TCP/IP Model

Layer	PDU	Protocol	Device	Addr
application	data	HTTP	host	URL
transport	segment	TCP/UDP	firewall	socket
network	packet	IP	L3 switch, router	IP
data link	frame	Ethernet	L2 switch	MAC
physical	bits	Ethernet	cabling	none

SMF vs MMF Fiber Cabling

Single-mode Fiber	Multi-mode Fiber
laser light source	LED light source
single light path	multiple light paths
longer distance	shorter distance
campus backbone	building LAN

Application Ports

Protocol	Port	Purpose
FTP	TCP 21	file transfer, authentication
SSH	TCP 22	virtual terminal line access
Telnet	TCP 23	virtual terminal line access
DNS	*UDP 53	host name resolution
TFTP	UDP 69	file transfer, config device
HTTP	TCP 80	unencrypted web page
NTP	UDP 123	time synchronization
SNMP	UDP 161	monitoring devices
IMAP	TCP 143	email client agent
SMTP	TCP 25	email server to server
HTTPS	TCP 443	SSL encrypted web page
SFTP	TCP 22	encrypted file transfer
DHCP	UDP 67	dynamic host addressing

*DNS supports UDP and TCP

TCP	UDP
transport layer	transport layer
connection-oriented	connectionless
flow control	no flow control
loss recovery	packet discard
slower	faster
guaranteed delivery	best effort
retransmission	no retransmission
HTTP, Telnet, SSH	DHCP, SNMP, voice, video

Network Architecture

Topology	Characteristics
PAN	workspace, single user, private, bluetooth
LAN	single building, VLANs, fastest, private
WLAN	single building, wireless, slowest, private
CAN	connect multiple buildings, fast, private
MAN	connect multiple campuses, fast, private
WAN	connect all locations, slower, private, public

IP Address Classes

Class	IP Address Range	Default Mask
A	1.0.0.0 - 127.255.255.255	255.0.0.0
B	128.0.0.0 - 191.255.255.255	255.255.0.0
C	192.0.0.0 - 223.255.255.255	255.255.255.0
D	224.0.0.0 - 239.255.255.255	multicast
E	240.0.0.0 - 255.255.255.255	reserved

RFC 1918 Private Addressing

IPv4 Address Range	Subnet Mask	CIDR
10.0.0.0 - 10.255.255.255	255.0.0.0	/8
172.16.0.0 - 172.31.255.255	255.240.0.0	/12
192.168.0.0 - 192.168.255.255	255.255.0.0	/16

IPv6 Addressing (128 bits)

Address	Description
link-local	auto-configure, local subnet, prefix **FE80::/10**
global	public internet routable address
unique local	private globally unique, not internet routable, prefix **FD00::/8**
multicast	prefix **FF00::/8** (send to group members)

IPv6 Address Compression Rules

- IPv6 address hexadecimal digits (0-9, A-F)
- eliminate leading zeroes only in any 16 bit group
- replace string of zero groups with double colon once

Device Link Lights

- **no light** = port shutdown or no remote connection
- flashing green = normal operation
- solid green = link with no activity, no data sent
- solid orange or amber = hardware or configuration error, disabled, no data sent
- flashing orange or amber = configuration mismatch error, data is sent

Wireless Security Protocols

Protocol	Description
WEP	original RC4 encryption with static key
WPA	WEP key with stronger TKIP encryption
WPA2	current standard with AES encryption
WPA3	protected management frames (PMF)

*WPA2 (enterprise), WPA2-PSK (personal / home)

Cloud Models

- Public = least security, managed, low performance
- Private = on-premises, security, high performance
- Hybrid = cloud and on-premises connectivity
- Community = shared model, secure, cost-effective
- SaaS = Google, public application, less secure
- PaaS = developer software, private, high security
- IaaS = AWS VPC, private, high security

Client Addressing: Initial Connection to Server

- source MAC address = client network adapter
- destination MAC address = default gateway
- source IP address = client
- destination IP address = server

Port Type	Description
console	management interface, configuration
Ethernet	LAN interface, Ethernet, data
Serial	WAN interface, data
USB	management interface, configuration
SFP	transceiver, fiber to copper
PoE	Power over Ethernet enabled

Network Tables

- DHCP = configure dynamic host addressing
- DNS = resolve hostname to an IP address for routing
- ARP = learn MAC address of network server
- MAC address = destination MAC address and switch port
- IP routing = forward packet to next hop neighbor IP address
- host routing table = loopback route, default route, local route

Switches vs Routers

L2 Switch	L3 Switch	Router
frame forwarding	frame forwarding packet forwarding	packet forwarding path selection
MAC address table	MAC address table routing table ARP table	routing table ARP table
access edge	traffic aggregation	WAN
broadcast propagation	both options	no broadcast propagation
L2 segmentation	L2 / L3 segments	L3 segmentation

Cisco IOS Show Commands

show running-config

display the current running configuration script on Cisco devices.

show version

display the following operational information on a device.

- IOS version and hardware
- how long since restart (uptime)
- configuration register
- how system was started (flash etc)

show ip interface brief

display summary of interface operational status (up/up) and assigned IP address. (subnet mask is not shown)

show interfaces [interface]

display detailed operational and configuration settings for a single interface or all interfaces.

- operational status of interfaces
- IP address and subnet mask
- hardware MAC address
- Layer 2 Interface errors and data rate

show interface status

display switch port connected status, vlan, duplex, and speed setting of interface.

show cdp neighbors

display all directly connected devices and the following.

- Layer 2 operational connectivity
- neighbor hostname
- local and neighbor switch port connection
- neighbor device type and capability (router etc)

show ip route

display the routing table on a Cisco device with route, next hop address, and local exit interface.

show switch

display all switches assigned to a switch stack along with base MAC address, stack role, and current state.

show inventory

display product id (PID), version id (VID), and serial number (SN) of chassis and installed hardware.

show mac address-table

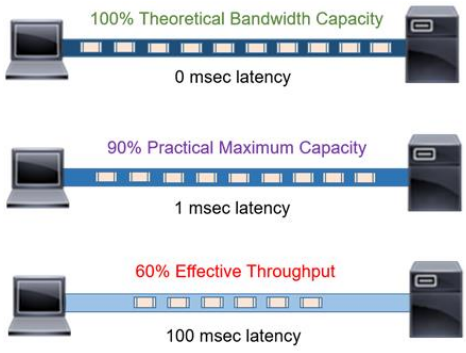
display the MAC address table entries on a switch with destination MAC address, associated port, and VLAN.

Cisco CLI Modes

- user exec mode >enable
- privileged exec (enable) mode #
- global configuration mode (config)#
- interface configuration mode (config-if)#
- help mode ?
- auto-complete keys = ALT-TAB

Network Performance

- network latency = delays from source/destination
- bandwidth = theoretical interface capacity
- throughput = data rate after network latency effects
- speed test = client to ISP, public, throughput
- Iperf = client to server, throughput



Cisco Security Privilege Levels (16)

- user level 0 = logout, enable, disable, exit, help
- user exec level 1 = limited read-only access
- privileged exec level 15 (default) = **unlimited access**

CIA Security Triad

- Confidentiality = access based on authorization
- Integrity = data is trustworthy and accurate
- Assurance = guarantee reliable access to data

Wireless Standards

Standard	Band (GHz)	Channels
802.11b	2.4	1,6,11 (non-overlapping)
802.11g	2.4	1,6,11 (non-overlapping)
802.11a	5	multiple channels
802.11n	2.4	1,6,11 (non-overlapping)
	5	multiple channels
802.11ac	5	multiple channels
802.11ax	2.4, 5	1,6,11 (non-overlapping) multiple (5 GHz)
	6	multiple channels

*all unlicenced frequency bands
*wireless interference = microwave, bluetooth

Host Commands

ping

measure RTT network latency between source and destination.

tracert

measure forwarding path of packets and per hop latency.

ipconfig /all (windows)

display host interface addressing to include IP address, subnet mask, MAC address, default gateway, and DNS server.

ifconfig (linux)

display host interface addressing to include IP address, subnet mask, MAC address, packets sent/received, and interface errors

arp -a

display host ARP table entries for IP address and MAC address.

netstat

display host connection table with TCP/UDP ports and associated socket addressing for applications.

route print

display host routing table with loopback route, local subnet route, and default route to default gateway.

nslookup

verify the DNS name server for a host is operational and DNS server is resolving hostname correctly.

netsh

command line interface program to display and modify the curent windows host configuration.

Wireless Service Set Identifier (SSID)

- Up to 32 character string
- case-sensitive naming
- access point association only (SSID=WLAN)
- auto-advertise in access point beacons (default)
- static wireless client configuration optional

Cyber Security

- threats = malware, phishing, ransomware
- social engineering + phishing = ransomware
- denial of service = flooding network with traffic
- vulnerability = firewall errors, default password
- spoofing = disguise computer with valid address
- MFA = multi-factor authentication

Protocol Quick Facts

- VLAN = Layer 2 broadcast domain
- router interface = Layer 3 broadcast domain
- ICMP = ping command / firewall filter issue
- subnet mask = network address portion
- default gateway = same subnet as VLAN/subnet
- NAT = translate private address to public address
- RDP = remote management of windows hosts
- Telnet = unencrypted virtual terminal line access
- SSH = encrypted virtual terminal line access
- RJ-45 connector = Ethernet cabling
- RJ-11 connector = telco / voice line
- LC / SC = fiber cabling connectors
- VPN = encrypted link for remote workers
- SSL = host to host encryption, web application
- UTP copper cabling signal loss = crosstalk, EMI
- physical layer: signaling, encoding, hardware
- data link layer: encapsulation, media access control
- network layer: logical addressing, path selection
- wireshark protocol capture file = .pcap
- interface same subnet required for connected links