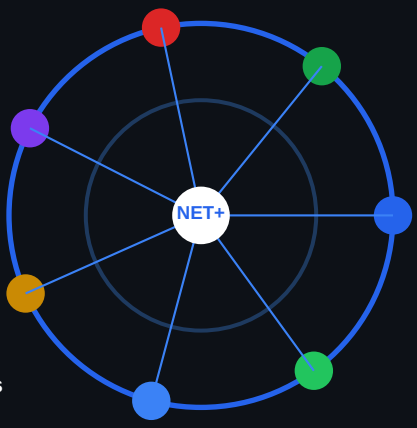
CompTIA Network+

N10-008 / N10-009

EXAM CHEATSHEET



25 Pages | 50+ Diagrams | Quick-Ref Tables | Exam Tips | Memory Aids

OSI Model

Please Do Not Throw Sausage Pizza Away All People Seem To Need Data Processing

SENDER
Encap

RECEIVER
Decap

7	APPLICATION	PDU: Data	HTTP FTP SMTP DNS
6	PRESENTATION	PDU: Data	SSL TLS JPEG MPEG
5	SESSION	PDU: Data	NetBIOS RPC NFS
4	TRANSPORT	PDU: Segment	TCP UDP Segments
3	NETWORK	PDU: Packet	IP ICMP OSPF Packets
2	DATA LINK	PDU: Frame	MAC Ethernet Frames
1	PHYSICAL	PDU: Bit	Cables Hubs Bits

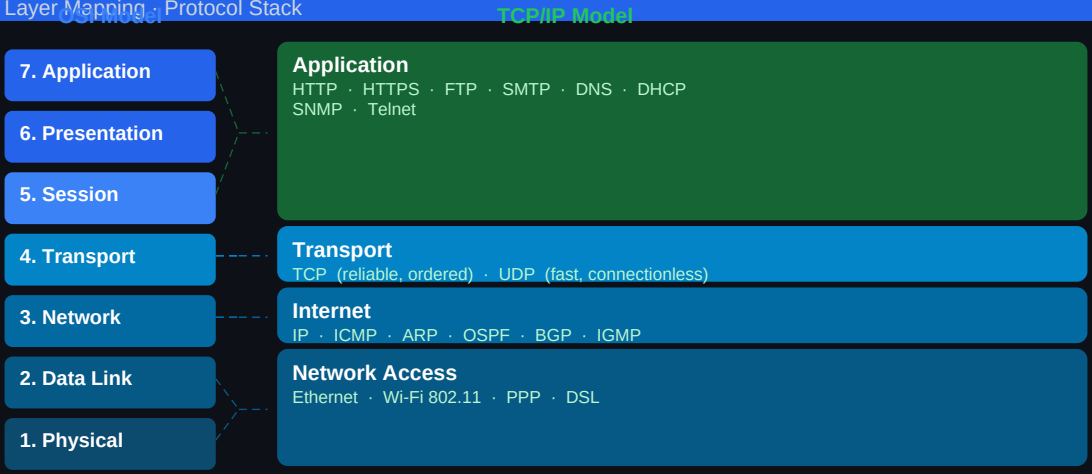
Layer	Device	Address	Key Protocol
7 App	Proxy/FW	Data	HTTP SMTP FTP
4 Trans	FW/LB	Port#	TCP UDP
3 Net	Router	IP Addr	IP ICMP BGP
2 Data	Switch	MAC Addr	Ethernet ARP
1 Phys	Hub/Rep	Signal	802.3 DSL

■ EXAM TIP

CompTIA loves to ask which OSI layer a device or protocol operates at. Routers = Layer 3, Switches = Layer 2, Hubs = Layer 1. SSL/TLS = Layer 6. Sockets = Layer 5.

TCP/IP Model vs OSI

Layer Mapping · Protocol Stack



Feature	TCP	UDP
Connection	Connection-oriented	Connectionless
Reliability	Guaranteed delivery	Best effort
Order	Ordered packets	No ordering
Speed	Slower (overhead)	Faster
Use Case	HTTP, FTP, Email	DNS, VoIP, Video

■ EXAM TIP

TCP/IP has 4 layers; OSI has 7. Top 3 OSI layers (App/Pres/Sess) = TCP/IP Application layer. Know this mapping cold — it appears on nearly every exam.

Ports & Protocols

Well-Known Ports 0–1023 · Common Services

Port	Service	Proto	Use
20	FTP Data	TCP	File Transfer
21	FTP Control	TCP	File Transfer
22	SSH / SCP	TCP	Secure Shell
23	Telnet	TCP	Unsecure Remote
25	SMTP	TCP	Send Email
53	DNS	TCP/UDP	Name Resolution
67	DHCP Server	UDP	IP Assignment
68	DHCP Client	UDP	IP Assignment
69	TFTP	UDP	Trivial FTP
80	HTTP	TCP	Web Traffic
110	POP3	TCP	Receive Email
119	NNTP	TCP	Newsgroups
123	NTP	UDP	Time Sync
143	IMAP	TCP	Email Retrieval

Port	Service	Proto	Use
161	SNMP	UDP	Network Mgmt
162	SNMP Trap	UDP	SNMP Alerts
389	LDAP	TCP	Directory Svc
443	HTTPS	TCP	Secure Web
445	SMB	TCP	File Sharing
500	IKE/IPsec	UDP	VPN Key Exch
514	Syslog	UDP	Log Messages
587	SMTP TLS	TCP	Secure Email
636	LDAPS	TCP	Secure LDAP
993	IMAPS	TCP	Secure IMAP
995	POP3S	TCP	Secure POP3
1433	MSSQL	TCP	SQL Server
1723	PPTP	TCP	VPN Tunnel
3389	RDP	TCP	Remote Desktop

PORT RANGES

0–1023 Well-Known (System) **1024–49151** Registered (Apps) **49152–65535** Dynamic / Ephemeral

■ EXAM TIP

Memorize: SSH=22, DNS=53, HTTP=80, HTTPS=443, RDP=3389, SMTP=25, SNMP=161. Know TCP vs UDP — DNS uses BOTH (UDP for queries, TCP for zone transfers >512 bytes).

IP Addressing

IPv4 Structure · Classes · Public vs Private

IPv4 Address Structure (32 bits = 4 octets)

192	168	10	5
Octet 1	Octet 2	Octet 3	Octet 4

IPv4 Address Classes (Legacy)

A	1–126	255.0.0.0	/8	16M hosts	Gov / ISP
B	128–191	255.255.0.0	/16	65534 hosts	Universities
C	192–223	255.255.255.0	/24	254 hosts	Small nets
D	224–239	—	—	Multicast	OSPF, video
E	240–255	—	—	Reserved	Research

Private IP Ranges (RFC 1918)

10.0.0.0/8	(Class A)	10.0.0.0 – 10.255.255.255	16 million hosts
172.16.0.0/12	(Class B)	172.16.0.0 – 172.31.255.255	1 million hosts
192.168.0.0/16	(Class C)	192.168.0.0 – 192.168.255.255	65,534 hosts

Special Addresses

127.0.0.1	Loopback	0.0.0.0	Default route / a	255.255.255.255	Limited broadca	169.254.x.x	APIPA

■ EXAM TIP

127.x.x.x = loopback. 169.254.x.x = APIPA (auto-assigned when DHCP fails). Class D = multicast. Know private ranges — 10.x, 172.16-31.x, 192.168.x — these CANNOT route on the public internet.

Subnetting Essentials

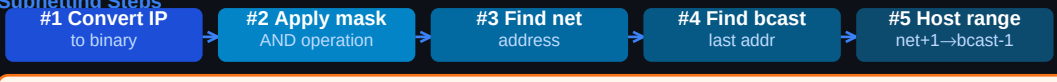
CIDR · Subnet Masks · Quick Tricks

CIDR	Subnet Mask	Hosts	Subnets(C)	Wildcard
/8	255.0.0.0	16,777,214	1	0.255.255.255
/16	255.255.0.0	65,534	256	0.0.255.255
/24	255.255.255.0	254	65536	0.0.0.255
/25	255.255.255.128	126	2	0.0.0.127
/26	255.255.255.192	62	4	0.0.0.63
/27	255.255.255.224	30	8	0.0.0.31
/28	255.255.255.240	14	16	0.0.0.15
/29	255.255.255.248	6	32	0.0.0.7
/30	255.255.255.252	2	64	0.0.0.3
/31	255.255.255.254	0(p2p link)	128	0.0.0.1
/32	255.255.255.255	1 host	256	0.0.0.0

Powers of 2: 2^1=1 2^2=4 2^3=8 2^4=16 2^5=32 2^6=64 2^7=128 2^8=256

Hosts = 2^(32-prefix) - 2

Subnetting Steps



■ EXAM TIP

Magic number trick: 256 - subnet mask octet = block size. E.g., /26 → 256-192=64. Subnets: 0,64,128,192. Remember: hosts = 2^host_bits - 2 (subtract network + broadcast).

IPv6

128-bit Address · Types · Compression Rules

IPv6 Address: 128 bits = 8 groups of 16-bit hex

2001	0DB8	85A3	0000	0000	8A2E	0370	7334
g1	g2	g3	g4	g5	g6	g7	g8

Network Prefix /64 — Interface ID /64

Compression Rules

Rule 1:	Leading zeros omitted	0DB8 → DB8 | 0001 → 1
Rule 2:	Consecutive zero groups → ::	0000:0000:0000 → ::
Rule 3:	:: used ONCE only	2001::1 (not 2001::::1)
Loopback:	::1 (= 0:0:0:0:0:0:0:1)	Like 127.0.0.1 in IPv4

IPv6 Address Types

Unicast — One-to-one
Global (2000::/3), Link-local (FE80::/10), Unique-local (FC00::/7)

Multicast — One-to-many
FF00::/8 (replaces broadcast)

Anycast — One-to-nearest
Routed to nearest interface

Feature	IPv4	IPv6
Size	32-bit	128-bit
Format	Decimal dotted	Hex colon
Addresses	~4.3 billion	340 undecillion
Broadcast	Yes	No (multicast)
NAT needed	Yes	No
Header	Variable	Fixed 40B

■ EXAM TIP

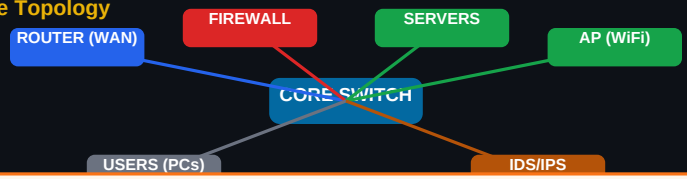
FE80::/10 = Link-local (automatic, non-routable). FF00::/8 = Multicast. ::1 = Loopback. IPv6 has no broadcast — uses multicast instead. EUI-64 generates interface ID from MAC address.

Network Devices

Routers · Switches · Firewalls · APs · More

HUB	Layer 1	Physical	Broadcasts all traffic to all ports. Collision domain. Legacy.	DEPRECATED
SWITCH	Layer 2	Data Link	Forwards by MAC. Builds MAC table. Creates collision domains per port.	COMMON
ROUTER	Layer 3	Network	Routes by IP. Connects networks. Default gateway. Breaks broadcast.	CORE
FIREWALL	Layer 3-7	Multiple	Filters traffic by rules. Stateful/stateless. Next-gen (NGFW).	CRITICAL
AP	Layer 2	Wireless	Wireless access point. Connects Wi-Fi devices to wired network.	NETWORK
MODEM	Layer 1	Physical	Modulates/demodulates signal. DSL, cable. Connects to ISP.	EDGE
IDS/IPS	Layer 3-7	Multiple	IDS=detects/alerts. IPS=detects+blocks. Inline vs passive.	SECURITY
PROXY	Layer 7	App	Intermediary. Forward/reverse proxy. Caches. Hides clients.	APP LAYER

Common Enterprise Topology



■ EXAM TIP

Key distinction: Hub (Layer 1) broadcasts; Switch (Layer 2) uses MAC table; Router (Layer 3) uses IP. IDS=passive monitor, IPS=active block. Multilayer switch = switch + routing.

Ethernet Standards

Speeds · Cabling · IEEE 802.3 Evolution

Standard	Speed	Cable	Range	Era	Notes
10BASE-T	10 Mbps	Cat 3	100m	1990s	Half duplex, legacy
100BASE-TX	100 Mbps	Cat 5	100m	Fast E	Full duplex
1000BASE-T	1 Gbps	Cat 5e/6	100m	GigE	Most common today
10GBASE-T	10 Gbps	Cat 6a/7	100m	10GigE	Data centers
40GBASE-SR4	40 Gbps	MMF	150m	40GigE	Backbone/DC
100GBASE-LR4	100 Gbps	SMF	10km	100GigE	Long haul / DC
1000BASE-SX	1 Gbps	MMF	550m	Fiber	Short wavelength
1000BASE-LX	1 Gbps	SMF	5km	Fiber	Long wavelength

Ethernet Naming Convention Decoder

1000 BASE - T

- 1000 — Speed in Mbps
- BASE — Baseband signal
- T — Medium: T=Twisted,

Duplex Modes

HALF DUPLEX — Send OR receive, not both. CSMA/CD collision detection.

FULL DUPLEX — Send AND receive simultaneously. Switches support this.

AUTO-MDIX — Auto crossover detection. Eliminates need for crossover cable.

■ EXAM TIP

Naming: [Speed][BASE][Medium]. T=copper twisted pair, SX=short fiber, LX=long fiber. Cat 5e supports GigE. Cat 6a supports 10GigE. Auto-MDIX eliminates crossover cables in modern equipment.

Cabling & Connectors

Fiber · Copper · STP/UTP · Connectors

Category	Speed	Max Length	Use Case
Cat 3	10 Mbps	100m	VoIP, legacy Ethernet
Cat 5	100 Mbps	100m	Fast Ethernet (legacy)
Cat 5e	1 Gbps	100m	Gigabit (most common)
Cat 6	1 Gbps / 10G	55m/100m	10GigE short runs
Cat 6a	10 Gbps	100m	10GigE full distance
Cat 7	10 Gbps	100m	Shielded, data centers
Cat 8	25-40 Gbps	30m	Data center only

Cable Types

UTP — **Unshielded Twisted Pair**
Most common, easy to install, susceptible to EMI

STP — **Shielded Twisted Pair**
Shield reduces interference. Industrial environments.

Coax — **Coaxial Cable**
Central conductor + shield. Cable TV, legacy networks.

Plenum — **Fire-rated cable**
Low-smoke PVC. Required in air-handling spaces.

SMF — **Single-Mode Fiber**
Core: 9 µm core · Max: 40km+ · Std: OS1/OS2

MMF — **Multi-Mode Fiber**
Core: 50/62.5 µm · Max: 550m · Std: OM1-OM5

Common Connectors

- **RJ-45** Ethernet copper · 8P8C, most common
- **RJ-11** Phone/DSL · 6P2C or 6P4C
- **LC** Fiber (small) · SFP modules, DC
- **SC** Fiber (push-pull) · Square connector
- **ST** Fiber (bayonet) · Twist-lock
- **MTP/MPO** Multi-fiber · 12/24 strand bundle
- **F-type** Coaxial · Cable TV/satellite

■ EXAM TIP

SMF (yellow) = long distance. MMF (orange/aqua) = short runs. RJ-45 = Ethernet. Plenum cable required in air ducts (fire safety). Cat 6a = 10GigE at 100m. STP used in EMI-heavy environments.

Wireless Networking

802.11 Standards · Frequencies · Security

Standard	Band	Max Speed	Range	Year	Tech	Wi-Fi Ver
802.11a	5 GHz	54 Mbps	35m	1999	OFDM	Legacy 5GH
802.11b	2.4 GHz	11 Mbps	38m	1999	DSSS	Legacy 2.4
802.11g	2.4 GHz	54 Mbps	38m	2003	OFDM	Widely used
802.11n	2.4/5 GHz	600 Mbps	70m	2009	MIMO	Wi-Fi 4
802.11ac	5 GHz	3.5 Gbps	35m	2014	MU-MIMO	Wi-Fi 5
802.11ax	2.4/5/6GHz	9.6 Gbps	30m+	2021	OFDMA	Wi-Fi 6
802.11be	2.4/5/6GHz	46 Gbps	30m+	2024	EHT	Wi-Fi 7

Frequency Bands Comparison

2.4 GHz
Better range,
more interference
14 channels (US: 1-11)
Non-overlapping: 1,6,11

5 GHz
Faster speed,
less interference
45 channels available
20/40/80/160 MHz width

6 GHz
Wi-Fi 6E only,
best performance
59 channels
320 MHz width possible

Wireless Security Protocols

Protocol	Full Name	Encryption	Status	Key Length
WEP	Wired Equivalent Privacy	RC4	BROKEN — do not use	64/128-bit
WPA	Wi-Fi Protected Access	TKIP	Deprecated, weak	128-bit
WPA2	WPA Version 2	AES/CCMP	Current standard	128-bit
WPA3	WPA Version 3	GCMP-256	Best, latest	256-bit

■ EXAM TIP

Non-overlapping 2.4GHz channels: 1, 6, 11. WEP=BROKEN. WPA2-AES=current minimum. Wi-Fi 5=802.11ac. Wi-Fi 6=802.11ax. 5GHz = faster but shorter range. SSID = network name.

Network Topologies

Star · Mesh · Bus · Ring · Hybrid

STAR

Most common. Central switch/hub. Single point of failure at center.

MESH

Every node connects to every other. High redundancy. Expensive.

BUS

Single cable backbone. Easy/cheap. Legacy (coax). Collision domain.

RING

Each node connects to two others. Token passing. SONET/FDDI.

HYBRID

Combination. Star-bus, star-ring. Most real networks.

POINT-TO-POINT

Direct link between two nodes. WAN links, leased lines.

Topology	Pros	Cons	Used Where
Star	Easy troubleshoot	Switch = SPOF	LAN networks
Mesh	High redundancy	Expensive	WAN/Internet
Bus	Simple/cheap	Collisions	Legacy coax
Ring	Equal access	Break = fail	SONET/FDDI
Hybrid	Flexible	Complex	Enterprise

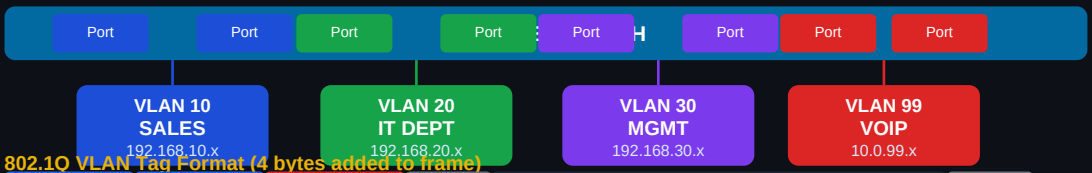
■ EXAM TIP

Star = most common LAN. Full mesh = n*(n-1)/2 connections. Ring = token passing, SONET. Hybrid = what real networks use. Bus = legacy, avoid. Know which has SPOFs (star=switch, bus=cable).

VLANs & Trunking

Segmentation · 802.1Q · Inter-VLAN Routing

VLAN Segmentation Diagram



802.1Q VLAN Tag Format (4 bytes added to frame)

Concept	Description
Access Port	Belongs to 1 VLAN. Connects end devices. Untagged traffic.
Trunk Port	Carries multiple VLANs. Tagged 802.1Q. Connects switches.
Native VLAN	Untagged traffic on trunk. Default VLAN 1 (change for security!).
VLAN 1	Default VLAN. All ports default. DO NOT use for production.
Inter-VLAN	Router-on-a-stick (sub-interfaces) or Layer 3 switch (SVIs).
Voice VLAN	Separate VLAN for VoIP. QoS prioritization. Cisco: voice vlan.
Management VLAN	Admin access VLAN. Change from VLAN 1 for security.

■ EXAM TIP

VLAN IDs range 1-4094 (12 bits). Native VLAN carries untagged traffic — change from VLAN 1! Inter-VLAN routing needs Layer 3. Trunk ports use 802.1Q tagging between switches.

Network Monitoring

SNMP · Syslog · NetFlow · Performance

SNMP — Simple Network Management Protocol (UDP 161/162)

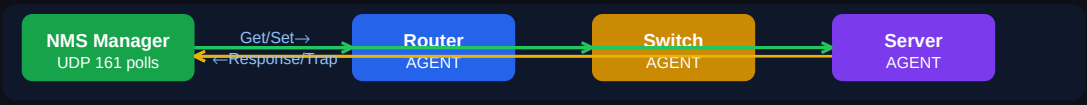
MANAGER NMS — Network Mgmt Station. Polls agents for data. Sends commands.

AGENT Runs on network devices. Reports to manager. Collects MIB data.

MIB Management Info Base. Database of variables. OID-based.

TRAP Agent-to-Manager alert. UDP 162. Async notification.

v1: Clear text, community string | v2c: Bulk queries | v3: Auth+Encryption (USE THIS)



Syslog — System Logging (UDP 514 / TCP 514/601)

0	1	2	3	4	5	6	7
Emergency	Alert	Critical	Error	Warning	Notice	Info	Debug
System u	Immediat	Critical	Error co	Warning	Normal b	Informat	Debug me

Mnemonic: Every Awesome Cat Does Will Notice Intoxicated Dogs (0=Emergency → 7=Debug)

NetFlow & Traffic Analysis

NetFlow
Cisco standard. Captures flow metadata. Src/Dst IP, port, protocol, bytes.

sFlow
Sampled flow. Industry standard. Packet sampling. Scalable for high speed.

IPFIX
IETF standard based on NetFlow v9. Flexible template-based.

Packet Capture
Wireshark/tcpdump. Full payload capture. Deep inspection. High storage.

Metric	Description	Good Range	Bad Sign
Latency	Round-trip delay	<50ms LAN	>100ms
Jitter	Latency variation	<30ms VoIP	>50ms
Packet Loss	Dropped packets	<0.1%	>1%
Bandwidth	Available capacity	70% util	>80%
Throughput	Actual data rate	~bandwidth	<<bandwidth

■ EXAM TIP

SNMP v3 = only secure version (authentication + encryption). Syslog 0=Emergency (worst). NetFlow = metadata only (not full packets). Wireshark captures full packets for deep inspection.

High Availability & Redundancy

Load Balancing · Failover · FHRP

HA Key Metrics — Availability Nines

99%	99.9%	99.99%	99.999%	99.9999%
1 Nine	2 Nines	3 Nines	4 Nines	5 Nines
87.6 hrs/yr	8.76 hrs/yr	52.56 min/yr	5.26 min/yr	31.5 sec/yr
7.3 hrs/mo	43.8 min/mo	4.4 min/mo	26.3 sec/mo	2.6 sec/mo

Load Balancing

First Hop Redundancy Protocols (FHRP)

HSRP — **Hot Standby Router Protocol**
Cisco proprietary — Active/Standby. Virtual IP/MAC.

VRRP — **Virtual Router Redundancy**
Open standard (RFC3768) — Master/Backup. Industry standard.

GLBP — **Gateway Load Balancing**
Cisco proprietary — Active load balancing across gateways.

Active/Passive	Primary handles traffic. Standby takes over on failure. No load sharing.
Active/Active	Both handle traffic simultaneously. Load sharing. Both must sync state.
NIC Teaming	Multiple NICs bonded together. Redundancy + bandwidth aggregation.
Spanning Tree	STP/RSTP prevents loops. Blocks redundant paths. Elects root bridge.
Port Channel	LACP/PAgP — bundles multiple links into one logical link. IEEE 802.3ad.

■ EXAM TIP

HSRP = Cisco only. VRRP = open standard. 'Five nines' (99.999%) = ~5.26 min downtime/year. Active/Active = load sharing. LACP (802.3ad) bundles links. STP prevents Layer 2 loops.

Cloud Networking

IaaS · PaaS · SaaS · Deployment Models

Cloud Service Models

SaaS — **Software as a Service** — You manage: Nothing!
Gmail, Office 365, Salesforce, Zoom

PaaS — **Platform as a Service** — You manage: App + Data
AWS Elastic Beanstalk, Heroku, Azure App

IaaS — **Infrastructure as a Service** — You manage: OS up
AWS EC2, Azure VMs, GCP Compute Engine

On-Prem — **On-Premises** — You manage: Everything
Your own data center

Cloud Deployment Models

Public Cloud	Private Cloud	Hybrid Cloud
Shared infra. Provider owned. AWS/Azure/GCP. Scalable, cost-effective.	Dedicated infra. On-prem or hosted. Higher security, more control.	Mix of public + private. Data sovereignty. Burst to public as needed.

Cloud Networking Concepts

VPC	**Virtual Private Cloud**	Isolated network within public cloud
SDN	**Software-Defined Networking**	Separate control/data plane. Centralized mgmt.
NFV	**Network Function Virtualization**	Virtual routers, firewalls, LBs.
CDN	**Content Delivery Network**	Edge caching. Reduces latency.
Direct Connect	**Dedicated WAN link**	AWS Direct Connect / Azure ExpressRoute
VPN Gateway	**Site-to-Site VPN**	Encrypted tunnel to cloud VPC
Elastic IP	**Static cloud IP**	Assigned to instances. Portable.
Subnet	**Cloud subnet**	Public (has IGW) vs Private (no internet).

■ EXAM TIP

IaaS=you manage OS up. PaaS=you manage app+data. SaaS=you manage nothing. SDN separates control plane from data plane. VPC = isolated cloud network. Elasticity = scale up/down automatically.

Documentation & Policies

Network Diagrams · SOPs · Change Mgmt

Essential Network Documentation

Physical Diagram	Shows actual physical layout — cables, racks, rooms, patch pan	Required
Logical Diagram	Shows IP addressing, VLANs, routing, services. Layer 3 view.	Required
Network Baseline	Normal performance metrics. Bandwidth, latency. Used for compa	Required
Asset Inventory	Hardware/software list. Make, model, serial, location, warrant	Required
IP Address Mgmt	IPAM system. Who has what IP. Prevents conflicts. Subnet track	Required
SOPs	Standard Operating Procedures. Step-by-step instructions for t	Required
Change Log	All changes recorded. Who, what, when, why, rollback plan.	Required
MOU/SLA	SLA = uptime guarantees. MOU = mutual understanding of service	Legal

Change Management Process

Acronym	Full Name	Description
AUP	Acceptable Use Policy	Rules for proper use of network resources
SLA	Service Level Agreement	Uptime guarantees, response times, penalties
NDA	Non-Disclosure Agreement	Confidentiality of sensitive network info
DRP	Disaster Recovery Plan	Steps to restore after major outage/disaster
BCP	Business Continuity Plan	Keep business running during disruption
MOU	Memo of Understanding	Inter-org service agreements
ISP SLA	Internet SLA	Guaranteed bandwidth, uptime, support response

■ EXAM TIP

Always document BEFORE and AFTER changes. Baseline = normal reference. SLA defines uptime guarantees (99.9% etc). Change windows minimize user impact. Rollback plan = mandatory in change requests.

Network Threats & Attacks

DoS · MITM · Spoofing · Social Engineering

Attack Categories & Types

DoS — **Denial of Service**
Flood target with traffic/requests. Make service unavailable.
UDP Flood | ICMP Flood | SYN Flood

DDoS — **Distributed DoS**
Coordinated from many sources (botnet). Amplified DoS.
Application layer | Protocol | Volumetric

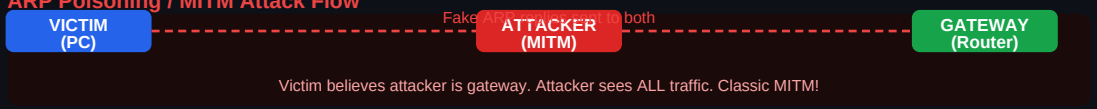
MITM — **Man-in-the-Middle**
Intercepts communication between two parties. Eavesdrop or modify.
SSL Stripping | DNS Spoofing | ARP Poisoning

Spoofing — **Identity Falsification**
Impersonating another host/user. IP, MAC, Email spoofing.
MAC Spoofing | ARP Spoofing | IP Spoofing

Phishing — **Social Engineering**
Deceptive emails/sites to steal credentials. Pretexting.
Vishing | Whaling | Spear Phishing

Ransomware — **Malware**
Encrypts victim data. Demands payment. Spreads via phishing.
RaaS | Locker | Crypto-ransomware

ARP Poisoning / MITM Attack Flow



Victim believes attacker is gateway. Attacker sees ALL traffic. Classic MITM!

Additional Threats

Vishing	Voice phishing over phone. Impersonates bank/IT support.
Tailgating	Physically following authorized person through secure door.
Evil Twin	Rogue AP mimicking legitimate Wi-Fi. Captures credentials.
Rogue DHCP	Unauthorized DHCP server handing out wrong gateway = MITM.
DNS Poisoning	Corrupts DNS cache. Redirects to attacker-controlled server.
SQL Injection	Malicious SQL via input fields. Bypasses auth, dumps data.

■ EXAM TIP

DDoS = botnet distributed attack. ARP poisoning enables MITM. Rogue DHCP = set attacker as default gateway. Evil twin = fake AP. Always verify with: arp -a (check for duplicate MACs).

Security Devices & Layers

Firewalls · IDS/IPS · Proxy · Honeypot

Defense in Depth — Security Layers

Type	Description	Level
Packet Filter	Layer 3-4. Inspects headers only. IP/port/protocol rules. Fast	Basic
Stateful	Layer 4. Tracks connection state table. Allows established ses	Standard
Application FW	Layer 7 / NGFW. Deep packet inspection. App-aware. Content fil	Advanced
WAF	Web App Firewall. Protects HTTP/S. Blocks SQLi, XSS, OWASP Top	App-specific
NGFW	Next-Gen Firewall. IPS+DPI+SSL inspection+App ID+User ID.	Enterprise

IDS vs IPS Comparison

IDS — Intrusion Detection
- Passive — monitors only
- Sends ALERTS only
- Out-of-band (copy of traffic)
- Cannot block in real-time

IPS — Intrusion Prevention
- Active — inline, blocks traffic
- Drops malicious packets
- Adds latency (inline)
- Can cause false positives

DMZ	Demilitarized Zone	Screened subnet between two firewalls. Public servic
Proxy Server	Forward/Reverse Proxy	Caches content, hides clients, content filter.
Honeypot	Decoy System	Fake vulnerable system to lure attackers. Gather int
NAC	Network Access Control	Checks device posture before granting network access
SIEM	Security Info & Event Mgmt	Correlates logs. Centralized security monitoring.
DLP	Data Loss Prevention	Prevents sensitive data from leaving the network.

■ EXAM TIP

IDS = detect only (passive). IPS = detect + block (inline). NGFW includes IPS+DPI+App awareness. DMZ = public-facing servers. Honeypot = trap attackers. SIEM aggregates and correlates all logs.

Authentication & Access Control

MFA · RADIUS · TACACS+ · AAA · Zero Trust

AAA Framework

AUTHENTICATION	AUTHORIZATION	ACCOUNTING
Who are you?	**What can you do?**	**What did you do?**
username/password certificate MFA biometrics	ACLs roles privileges	session time commands run data transferred

RADIUS vs TACACS+

Feature	RADIUS	TACACS+
Developer	IETF Open Standard	Cisco Proprietary
Transport	UDP 1812/1813	TCP 49
Encryption	Password only	Full packet
Auth + Author	Combined	Separated
Accounting	Yes	Yes
Use Case	Wi-Fi, VPN, dial-up	Network device admin
Speed	Faster (UDP)	Reliable (TCP)

Multi-Factor Authentication (MFA) Factors

Something YOU KNOW	Something YOU HAVE	Something YOU ARE	Somewhere YOU ARE
Password PIN Security Q	Smart card Token Phone	Fingerprint Face Iris	GPS location IP range
Weakest alone	TOTP, HOTP, FIDO2 key	Biometrics	Context-aware

Access Control Models

DAC	**Discretionary Access Control**	Owner controls permissions. File system ACLs. Most flex
MAC	**Mandatory Access Control**	Labels/clearance levels. Government/military. Most rest
RBAC	**Role-Based Access Control**	Permissions by job role. Most common enterprise model.
ABAC	**Attribute-Based Access Control**	Rules based on attributes (user, env, resource).
Zero Trust	**Never Trust, Always Verify**	No implicit trust. Verify every request. ZTNA/BeyondCor

■ EXAM TIP

RADIUS = UDP, combines auth+authz. TACACS+ = TCP, separates all three AAA, encrypts full packet. MFA requires 2+ DIFFERENT factor types. RBAC = most common. Zero Trust = verify everything always.

Encryption & VPNs

IPsec · SSL/TLS · VPN Types · PKI

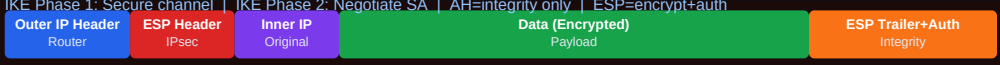
Algorithm	Type	Key Size	Notes
AES	Symmetric	128/192/256-bit	Fastest symmetric. Gold standard. AES-256 for high s
3DES	Symmetric	168-bit	Triple-DES. Legacy. Being phased out.
RSA	Asymmetric	1024-4096-bit	Public/private key. Key exchange + digital signature
ECC	Asymmetric	256-bit+	Elliptic curve. Smaller keys, same strength. Mobile/
DH/ECDH	Key Exchange	—	Diffie-Hellman. Securely exchange keys over public c
SHA-256	Hashing	256-bit	Message integrity. One-way. Used in TLS/digital sign
MD5	Hashing	128-bit	BROKEN for security. Use SHA-256+. File integrity on

VPN Types & Protocols

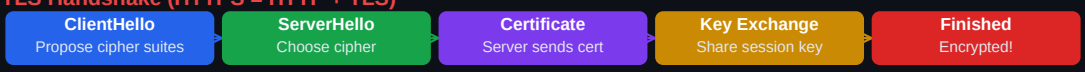
Site-to-Site	Connects two offices permanently. IPsec tunnels. Replaces MPLS.
Remote Access	Individual user connects to HQ. SSL VPN or IPsec client.
Client-to-Site	Same as remote access. Full tunnel vs split tunnel.
SSL/TLS VPN	Browser-based or client. TCP 443. Firewall-friendly. Easy.
IPsec VPN	Network layer. AH+ESP protocols. IKE key exchange.
Split Tunnel	Only corporate traffic through VPN. Rest goes direct internet.

IPsec VPN Tunnel (Encrypted Encapsulation)

IKE Phase 1: Secure channel | IKE Phase 2: Negotiate SA | AH=integrity only | ESP=encrypt+auth



TLS Handshake (HTTPS = HTTP + TLS)



■ EXAM TIP

AES-256 = strongest symmetric. RSA used for key exchange, not bulk data. IPsec uses ESP (encrypt) + AH (integrity). IKE Phase 1 = authenticate peers. TLS 1.3 = current standard. HTTPS = TLS on port 443.

Troubleshooting Methodology

CompTIA 7-Step Process · OSI Approach

CompTIA 7-Step Troubleshooting Methodology

1	**Identify the Problem** Gather info. User reports. Symptoms. When did it start? What changed?	Question: single or multiple users? Intermitt
2	**Establish Theory** Top-down or bottom-up. OSI model. Most probable cause first.	Approach: Physical first, then logical layers
3	**Test the Theory** Confirm or eliminate. Use diagnostic tools. Ping, tracert.	If wrong: re-establish new theory. If right:
4	**Establish Action Plan** Plan the fix. Identify effects. Schedule maintenance window.	Document before touching anything!
5	**Implement Solution** Apply the fix. Change one thing at a time. Follow plan.	If not solved: escalate or try new approach.
6	**Verify & Test** Confirm problem is resolved. Test from user perspective.	Check for side effects. Test related systems.
7	**Document Findings** Record: problem, cause, solution, prevention.	Update knowledge base. Lessons learned.

OSI-Based Troubleshooting Approaches

Bottom-Up	Top-Down	Divide & Conquer	Swap Component
Start at Layer 1 (Physical). Check cables, lights, connectors. Work up. Best for: Physical/connection problems	Start at Layer 7 (Application). Check apps, services, config. Work down. Best for: Application/service issues	Start at Layer 3 (Network). Can you ping? Work up or down. Best for: Connectivity issues	Replace suspected bad component. Swap cable, NIC, switch port. Best for: Hardware failures

■ EXAM TIP

Always document BEFORE making changes. Change one thing at a time. Step 2 establishes theory — not solution. Step 6 = verify from USER perspective. 'What changed recently?' is the most important question.

Common Network Issues

Symptoms · Causes · Solutions

	Causes:		Fix:	
No Connectivity Cannot reach any host	• Disconnected cable • NIC disabled	• Wrong VLAN • IP conflict	• Check link lights • ipconfig /all	• ping 127.0.0.1 • Check switch port
Slow Performance High latency, low throughput	• Bandwidth saturation • Duplex mismatch	• Bad cable/NIC • Interference	• Check utilization • iperf test	• Cable test • Wi-Fi analyzer
Intermittent Random drops/slowness	• Faulty hardware • Interference	• Overheating • MTU issues	• Replace cables • Check logs	• Monitor temp • ping -f (MTU test)
DNS Failure Cannot resolve names	• Wrong DNS server • DNS server down	• Split-horizon issue • Cache poisoned	• nslookup • ping by IP works?	• Check /etc/resolv.conf • ipconfig /flushdns
DHCP Issues No IP or wrong IP (169.254.x.x)	• DHCP server down • IP pool exhausted	• Rogue DHCP • DHCP relay missing	• ipconfig /renew • Check DHCP scope	• Review DHCP leases • Check relay agent
Wireless Issues Wi-Fi drops, slow, no connect	• Wrong SSID/password • Interference (2.4GHz)	• AP overloaded • Driver issue	• Check SSID/passphrase • Switch to 5GHz	• Add AP • Update drivers

Quick Symptom → Layer Map

Can't ping 127.0.0.1	→ TCP/IP stack broken	Fix: Reinstall TCP/IP
Can ping 127.0.0.1, not gateway	→ Layer 3 routing issue	Fix: Check IP/mask/GW
Can ping by IP, not by name	→ DNS failure	Fix: Check DNS server
Link light OFF	→ Layer 1 physical	Fix: Check cable/NIC
IP 169.254.x.x	→ DHCP failure (APIPA)	Fix: ipconfig /renew

■ EXAM TIP

169.254.x.x = APIPA — DHCP failed. Start with ping 127.0.0.1 to test TCP/IP stack. Can ping IP but not name? = DNS problem. Link light off = Layer 1 issue. Duplex mismatch = late collisions + slowness.

CLI Troubleshooting Tools

ping · tracert · ipconfig · netstat · nslookup

ping — Connectivity test. ICMP echo request/reply. Tests Layer 3.
ping 8.8.8.8 | ping -t (continuous) | ping -n 10 (10 packets)
`ping gateway = Layer 3` `ping 127.0.0.1 = local stack`

tracert (traceroute) — Maps path to destination. Shows each hop. TTL-based.
tracert 8.8.8.8 | traceroute (Linux/Mac)
`High RTT = bottleneck hop` `* * * = firewall blocking`

ipconfig (ifconfig) — Display/manage IP configuration. Windows essential.
ipconfig /all | ipconfig /release | ipconfig /renew | /flushdns
`/flushdns = clear cache` `/all = full details`

netstat — Network statistics. Active connections, ports, routing table.
netstat -an | netstat -rn (route table) | netstat -s (statistics
`-n = numeric IPs` `-a = all connections`

nslookup (dig) — DNS query tool. Resolve names, check DNS records.
nslookup google.com | nslookup -type=MX domain | dig @8.8.8.8 doma
`Check MX, A, CNAME, PTR` `Test specific DNS server`

arp — View/manage ARP cache. IP-to-MAC mappings.
arp -a (view all) | arp -d (delete entry) | arp -s (static entr
`Find rogue devices` `Duplicate MACs = ARP spoof`

route — View and modify routing table.
route print | route add | route delete | netstat -r
`Gateway = next hop` `Default route = 0.0.0.0`

Function	Windows	Linux/Mac
IP config	ipconfig /all	ifconfig / ip addr
Route table	route print	netstat -r / ip route
DNS lookup	nslookup	dig / host / nslookup
Trace route	tracert	traceroute
ARP table	arp -a	arp -n
Port scan	netstat -an	ss -tulnp / netstat -an
Packet cap	Wireshark/netsh	tcpdump -i eth0
DNS flush	ipconfig /flushdns	systemd-resolve --flush

■ EXAM TIP
ping -t = continuous Windows (Ctrl+C to stop). tracert shows * when ICMP blocked. ipconfig /flushdns clears DNS cache. netstat -an shows all listening ports. arp -a shows duplicate MACs = ARP spoofing!

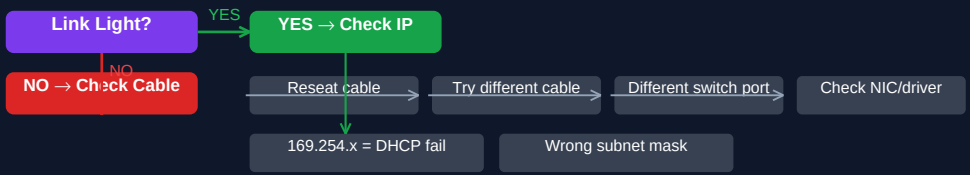
Hardware Troubleshooting

Cables · NICs · Switches · Wireless

Cable Testing & Diagnostics

Cable Tester	Checks wire map, continuity, shorts, miswires. Basic go/no-go.
TDR	Time-Domain Reflectometer. Locates cable breaks, kinks. Shows distan
OTDR	Optical TDR. Tests fiber optic cable. Finds breaks, bends, splices.
Loopback Plug	Tests NIC/port. Sends data out, receives back. Hardware test.
Toner Probe	Tone generator traces cable through walls. Identifies cable runs.
Multimeter	Tests voltage, resistance. Power, continuity of cable/connector.
Wi-Fi Analyzer	Shows SSID, channel, signal strength (dBm). Finds interference.

Hardware Symptom Diagnostic Flow



Switch/Port LED Indicators

GREEN solid	Link established, connected	Normal operation
GREEN blinking	Activity — data transmitting	Normal operation
AMBER/Orange	Speed 10/100 or fault	Check speed setting
No light	No link detected	Check cable/device
AMBER blinking	STP blocking or error	Spanning tree active

■ EXAM TIP

No link light = Layer 1 problem (cable/NIC/port). AMBER blinking on switch = STP blocking. TDR finds cable break distance. Always try a known-good cable first — simplest fix first!

Performance & Optimization

QoS · Bandwidth · Traffic Shaping · Acronym Ref

QoS — Quality of Service

Classification	Identify traffic type (voice, video, data, bulk)	DSCP, CoS, ACLs
Marking	Tag packets with priority value. DSCP in IP header.	EF, AF, BE, CS
Queuing	Prioritize queues. Low-latency for voice first.	LLQ, WFQ, CBWFQ
Policing	Drop or re-mark traffic exceeding rate. Hard limit.	Traffic contract
Shaping	Buffer excess traffic instead of dropping. Smooth out.	Token bucket
Congestion Mgmt	Manage overloaded interfaces. WRED drops early.	WRED, tail drop

DSCP Priority Values (6-bit in IP header)

EF (46)	AF41-43	AF31-33	CS0 (0)
Expedited Forwarding	Assured Forwarding	Assured Forwarding	Best Effort (BE)
VoIP, real-time	Video conferencing	Call signaling	Default traffic
Highest priority	High priority	Medium-high	Lowest priority

Essential Acronym Quick Reference

ACL	Access Control List	AP	Access Point	ARP	Address Resolution Protocol
BGP	Border Gateway Protocol	CIDR	Classless Inter-Domain Routing	DHCP	Dynamic Host Config Protocol
DMZ	Demilitarized Zone	DNS	Domain Name System	EIGRP	Enhanced Interior Gateway Routi
FQDN	Fully Qualified Domain Name	FTP	File Transfer Protocol	HTTPS	HTTP Secure
ICMP	Internet Control Message Protoco	IDS	Intrusion Detection System	IGP	Interior Gateway Protocol
IPS	Intrusion Prevention System	IPsec	IP Security	LACP	Link Aggregation Control Protocol
LDAP	Lightweight Directory Access Prot	MAC	Media Access Control	MPLS	Multiprotocol Label Switching
NAT	Network Address Translation	NIC	Network Interface Card	OSPF	Open Shortest Path First
PAT	Port Address Translation	PKI	Public Key Infrastructure	QoS	Quality of Service
RADIUS	Remote Auth Dial-In User Service	RIP	Routing Info Protocol	SDN	Software-Defined Networking
SLA	Service Level Agreement	SMTP	Simple Mail Transfer Protocol	SNMP	Simple Network Mgmt Protocol
SSH	Secure Shell	SSL	Secure Sockets Layer	STP	Spanning Tree Protocol
TACACS+	Terminal Access Ctrl Access Ctrl	TCP	Transmission Control Protocol	TLS	Transport Layer Security
UDP	User Datagram Protocol	VLAN	Virtual Local Area Network	VPN	Virtual Private Network
WAN	Wide Area Network				

■ EXAM TIP

VoIP needs QoS! Use LLQ to prioritize voice. DSCP EF = VoIP (highest). Bandwidth ≠ throughput — always measure actual throughput. 80% utilization = time to upgrade. Jitter >30ms = call quality issues.