CompTIA Network+

N10-009

Complete Cheat Sheet & Study Guide

All 5 Domains • Key Ports & Protocols • Subnetting • Acronyms

KTaylorTech · ktaylortech.com

Study Guide Contents

■ *Exam: 90 min | Up to 90 questions | Maximum score 900 | Passing score 720*

DOMAIN 1 — Networking Concepts — 23% of exam

1.1 OSI Model (Must Memorize)

Layer	Name	PDU	Key Protocols / Devices	Mnemonic
7	Application	Data	HTTP, HTTPS, DNS, SMTP, FTP, SNMP	All
6	Presentation	Data	SSL/TLS, JPEG, MPEG, ASCII	People
5	Session	Data	NetBIOS, RPC, PPTP	Seem
4	Transport	Segment	TCP, UDP	To
3	Network	Packet	IP, ICMP, OSPF, BGP, Router	Need
2	Data Link	Frame	Ethernet, MAC, ARP, Switch, NIC	Data
1	Physical	Bit	Cables, Hubs, Repeaters, Wi-Fi radio	Processing

■ *Memory: 'All People Seem To Need Data Processing' (Layer 7→1) or reverse: 'Please Do Not Throw Sausage Pizza Away'*

1.2 TCP vs UDP

Feature	TCP	UDP
Connection	Connection-oriented (3-way handshake)	Connectionless
Reliability	Guaranteed delivery, retransmission	Best-effort, no retransmission
Speed	Slower (overhead)	Faster (low overhead)
Use Cases	HTTP/S, FTP, SSH, SMTP, Telnet	DNS, DHCP, VoIP, TFTP, SNMP, streaming
Header Size	20–60 bytes	8 bytes

1.3 IPv4 Addressing & Subnetting Cheat Sheet

Class	Range	Default Mask	CIDR	Hosts/Network
A	1–126.x.x.x	255.0.0.0	/8	16,777,214
B	128–191.x.x.x	255.255.0.0	/16	65,534
C	192–223.x.x.x	255.255.255.0	/24	254
D	224–239.x.x.x	Multicast	—	N/A
E	240–255.x.x.x	Experimental	—	N/A

CIDR / Subnet Quick Reference

CIDR	Subnet Mask	Hosts	Subnets from /24
/24	255.255.255.0	254	1
/25	255.255.255.128	126	2
/26	255.255.255.192	62	4
/27	255.255.255.224	30	8
/28	255.255.255.240	14	16
/29	255.255.255.248	6	32
/30	255.255.255.252	2	64

- Private ranges: 10.x.x.x | 172.16–31.x.x | 192.168.x.x
- APIPA: 169.254.x.x — assigned when DHCP fails
- Loopback: 127.0.0.1 (::1 for IPv6)

1.4 IPv6 Essentials

- 128-bit address, written in 8 groups of 4 hex digits: 2001:0db8:85a3::8a2e:0370:7334

- :: = consecutive all-zero groups (used once only)
- Link-local: fe80::/10 | Multicast: ff00::/8 | Loopback: ::1
- Global Unicast: 2000::/3 | Unique Local: fc00::/7
- No broadcast — replaced by multicast & anycast
- NDP (Neighbor Discovery Protocol) replaces ARP
- Transition: Dual Stack, Tunneling (6to4, Teredo), NAT64

1.5 Network Topologies

Topology	Description	Pro / Con
Star	All nodes connect to central switch/hub	Easy to manage / single point of failure at hub
Bus	Single cable backbone	Simple, cheap / hard to troubleshoot, legacy
Ring	Each node connects to two others	Predictable performance / one break = outage
Mesh	Every node connects to every other	Redundant / expensive, complex
Hybrid	Combination of topologies	Flexible / complex design

1.6 WAN Concepts

- MPLS – Multi-Protocol Label Switching: label-based routing, reliable, used by ISPs
- SD-WAN – Software-Defined WAN: centralized policy control over WAN links
- Metro Ethernet – Ethernet-based WAN across a metro area
- DSL – uses existing phone lines; ADSL = asymmetric (download > upload)
- Cable – coax-based broadband; shared bandwidth
- Fiber (FTTH/FTTP) – highest speed, lowest latency
- Satellite – high latency (~600ms), good for remote areas
- Cellular – LTE/5G for mobile WAN; 5G NR: sub-6GHz & mmWave

DOMAIN 2 — Network Implementation — 20% of exam

2.1 Ethernet Standards

Standard	Speed	Cable	Max Distance
10BASE-T	10 Mbps	Cat3 UTP	100 m
100BASE-TX	100 Mbps	Cat5 UTP	100 m
1000BASE-T	1 Gbps	Cat5e UTP	100 m
1000BASE-SX	1 Gbps	Multi-mode fiber	550 m
1000BASE-LX	1 Gbps	Single-mode fiber	5 km
10GBASE-T	10 Gbps	Cat6a UTP	100 m
10GBASE-SR	10 Gbps	Multi-mode fiber	300 m
10GBASE-LR	10 Gbps	Single-mode fiber	10 km
40GBASE-SR4	40 Gbps	Multi-mode fiber	150 m
100GBASE-LR4	100 Gbps	Single-mode fiber	10 km

2.2 Cable Types

Type	Connector	Notes
Cat5	RJ-45	100 Mbps, 100m, legacy
Cat5e	RJ-45	1 Gbps, 100m, most common for GbE
Cat6	RJ-45	10 Gbps up to 55m; 1 Gbps to 100m
Cat6a	RJ-45	10 Gbps to 100m; augmented
Cat7	GG45/TERA	10 Gbps, shielded, 100m
Cat8	RJ-45	25/40 Gbps, data centers, 30m
Single-mode fiber	LC/SC	Long dist, laser source, yellow jacket
Multi-mode fiber	LC/SC	Short dist, LED/VCSEL, orange/aqua
Coax (RG-6)	F-type	Cable TV/broadband
Twinax (DAC)	SFP+	Short-range 10G in data centers

- T568A wiring order: G-w, G, O-w, Bl, Bl-w, O, Br-w, Br
- T568B wiring order: O-w, O, G-w, Bl, Bl-w, G, Br-w, Br (most common in US)
- Crossover cable: T568A one end, T568B other — connects like devices

2.3 Wireless (802.11)

Standard	Band	Max Speed	Range (approx)	Notes
802.11a	5 GHz	54 Mbps	~35 m indoor	Legacy, OFDM
802.11b	2.4 GHz	11 Mbps	~35 m	Legacy, DSSS
802.11g	2.4 GHz	54 Mbps	~38 m	OFDM, backward compat
802.11n	2.4/5 GHz	600 Mbps	~70 m	MIMO, Wi-Fi 4
802.11ac	5 GHz	3.5 Gbps	~35 m	MU-MIMO, Wi-Fi 5
802.11ax	2.4/5/6 GHz	9.6 Gbps	~35 m	OFDMA, Wi-Fi 6/6E
802.11be	2.4/5/6 GHz	46 Gbps	—	Wi-Fi 7 (EHT)

- 2.4 GHz: non-overlapping channels 1, 6, 11 | 5 GHz: many non-overlapping channels
- Security: WPA3 (current best) > WPA2-AES > WPA2-TKIP > WPA > WEP (broken)
- WPA2 modes: Personal (PSK) / Enterprise (802.1X + RADIUS)

• Antenna types: omnidirectional (equal all directions) vs. directional (Yagi, dish)

2.4 Routing Protocols

Protocol	Type	Algorithm	AD	Key Facts
RIP	Distance Vector	Bellman-Ford	120	Hop count ≤15; slow convergence
OSPF	Link State	Dijkstra (SPF)	110	Uses areas; no hop limit; fast
EIGRP	Hybrid	DUAL	90	Cisco proprietary (mostly); bandwidth+delay metric
BGP	Path Vector	Best path policy	20	Internet routing protocol (EGP); autonomous systems
IS-IS	Link State	Dijkstra	115	ISP backbones; similar to OSPF
Static	Manual	N/A	1	Admin-configured; no overhead

■ *AD = Administrative Distance. Lower AD = more trusted. Connected interface = 0, Static = 1*

2.5 VLANs & Switching

• VLAN – logical segmentation of a switch; same VLAN = same broadcast domain
• Access port – carries traffic for ONE VLAN (connects end devices)
• Trunk port – carries multiple VLANs using 802.1Q tagging (connects switches/routers)
• Native VLAN – untagged traffic on a trunk (default VLAN 1; best practice: change it)
• Inter-VLAN routing: Router-on-a-stick (subinterfaces) OR Layer 3 switch (SVIs)
• STP (802.1D) – prevents loops; elects Root Bridge (lowest Bridge ID)
• RSTP (802.1w) – rapid STP; faster convergence (~1s vs 30–50s)
• Port roles: Root, Designated, Alternate (RSTP)/Blocked (STP), Disabled
• LACP (802.3ad) – Link Aggregation; bundles multiple physical links into one logical link

DOMAIN 3 – Network Operations — 19% of exam

3.1 Network Services

Service	Port(s)	Function
DHCP	67 (server) / 68 (client) UDP	Dynamic IP address assignment; DORA process
DNS	53 UDP/TCP	Hostname-to-IP resolution; hierarchy: root→TLD→authoritative
NTP	123 UDP	Time synchronization; Stratum 0=atomic clock
SNMP	161 UDP (agent) / 162 (trap)	Network device monitoring; v3 = encrypted+auth
Syslog	514 UDP	Centralized logging; severity 0(emerg)–7(debug)
TFTP	69 UDP	Trivial FTP; firmware transfer, no auth

3.2 DNS Record Types

Record	Purpose
A	IPv4 address mapping
AAAA	IPv6 address mapping
CNAME	Alias to another hostname
MX	Mail exchange server
PTR	Reverse lookup (IP → hostname)
NS	Name server for a domain
SOA	Start of authority; primary NS, serial, refresh info
TXT	Text strings; used for SPF, DKIM, DMARC
SRV	Service location (e.g., SIP, XMPP)

3.3 High Availability & Disaster Recovery

- MTTR – Mean Time To Repair: avg time to restore a failed component
- MTBF – Mean Time Between Failures: avg time between failures
- RTO – Recovery Time Objective: max tolerable downtime
- RPO – Recovery Point Objective: max tolerable data loss (time)

Availability %	Downtime/Year	Downtime/Month	Tier
99%	3.65 days	7.3 hours	—
99.9%	8.76 hours	43.8 min	3-nines
99.99%	52.6 minutes	4.38 min	4-nines
99.999%	5.26 minutes	26.3 sec	5-nines

- Load balancing methods: Round-robin, Least connections, IP hash, Weighted
- NIC Teaming (bonding): Active-Active or Active-Passive failover
- FHRP: HSRP (Cisco), VRRP (open standard), GLBP — virtual gateway IPs

3.4 Network Monitoring & Management

- SNMP Versions: v1 (community string, insecure) | v2c (bulk queries) | v3 (auth + encryption)
- NetFlow/sFlow – traffic analysis; tracks flows between IP pairs
- RMON – Remote Monitoring; SNMP extension for LAN traffic stats
- Bandwidth monitoring: SNMP polling, NetFlow, packet capture (Wireshark)
- Baseline – documented normal performance; needed to identify anomalies
- Syslog severity levels: 0=Emergency, 1=Alert, 2=Critical, 3=Error, 4=Warning, 5=Notice, 6=Info, 7=Debug

3.5 Documentation & Change Management

- Physical diagram – shows physical location of devices and cables

- Logical diagram – shows IP addressing, VLANs, routing, protocols
- Network baseline – performance metrics during normal operation
- Change management: Request → Impact Assessment → Approval → Implementation → Verification → Documentation
- IPAM – IP Address Management; tracks IP allocation
- Cable management: patch panels, labeling, color-coding, documentation

DOMAIN 4 – Network Security — 14% of exam

4.1 Security Threats & Attack Types

Attack	Description
Phishing	Deceptive email/message to steal credentials; spear phishing = targeted
DoS / DDoS	Flood target with traffic; DDoS = distributed sources (botnet)
Man-in-the-Middle	Attacker intercepts communications (ARP spoofing, SSL stripping)
ARP Poisoning	Fake ARP replies map attacker MAC to legitimate IP
DNS Spoofing	Corrupt DNS cache to redirect to malicious IP
VLAN Hopping	Switch spoofing or double tagging to access other VLANs
Rogue DHCP/AP	Unauthorized DHCP server or access point on network
Evil Twin	Fake AP mimics legitimate SSID to capture credentials
Brute Force	Systematically try all password combinations
SQL Injection	Inject SQL into input fields to manipulate DB
XSS	Cross-site scripting; inject malicious scripts into web pages
Session Hijacking	Steal session token to impersonate authenticated user
Zero-Day	Exploit for unknown/unpatched vulnerability

4.2 Network Security Controls

- Firewall types: Packet filter | Stateful | Next-gen (NGFW) | WAF (web app)
- IDS – Intrusion Detection System: monitors and alerts (passive)
- IPS – Intrusion Prevention System: monitors and BLOCKS (inline, active)
- Signature-based: known threats | Anomaly-based: behavioral deviation
- DMZ – Demilitarized Zone: semi-trusted network hosting public-facing servers
- Honeypot – decoy system to attract/study attackers
- NAC – Network Access Control: verify device posture before granting access
- Port Security – limit MAC addresses per switch port; sticky MAC
- DHCP Snooping – blocks rogue DHCP servers; builds binding table
- Dynamic ARP Inspection (DAI) – validates ARP against DHCP snooping table
- 802.1X – port-based authentication; requires RADIUS server (EAP)

4.3 VPN Technologies

VPN Type	Protocol(s)	Notes
Site-to-Site	IPSec (ESP/AH)	Connects two networks; tunnel mode
Remote Access	SSL/TLS, IPSec	Client-to-network; split vs. full tunnel
PPTP	GRE + MPPE	Legacy, weak encryption — avoid
L2TP/IPSec	L2TP over IPSec	Common for remote access; dual encapsulation
OpenVPN	SSL/TLS	Open-source, flexible, port 1194 UDP
WireGuard	Custom (UDP)	Modern, fast, minimal attack surface
DMVPN	IPSec + mGRE	Dynamic multipoint VPN; Cisco; hub-and-spoke→mesh

- IPSec modes: Transport (payload only) | Tunnel (entire packet)
- IPSec protocols: AH (authentication, no encryption) | ESP (auth + encryption)
- IKE phases: Phase 1 = establish ISAKMP SA | Phase 2 = negotiate IPSec SA

4.4 Authentication & Access Control

- AAA: Authentication (who) | Authorization (what) | Accounting (when/what done)
- RADIUS – UDP 1812/1813; encrypts only password; used for network device auth

- TACACS+ – TCP 49; encrypts entire payload; Cisco; better for device management
- LDAP – TCP 389 (636 for LDAPS); queries directory services (AD)
- Kerberos – TCP/UDP 88; ticket-based; default auth in AD environments
- MFA – Multi-Factor Auth: Something you know + have + are
- Zero Trust – never trust, always verify; micro-segmentation; least privilege

DOMAIN 5 – Network Troubleshooting — 24% of exam

5.1 CompTIA Troubleshooting Methodology (MEMORIZE)

Step	Action
1	Identify the problem — gather info, question users, identify symptoms, duplicate if possible
2	Establish a theory of probable cause — consider obvious first (OSI bottom-up or top-down)
3	Test the theory — if confirmed, determine fix; if not, establish new theory or escalate
4	Establish a plan of action — identify steps to resolve, notify affected users
5	Implement the solution OR escalate — apply fix; verify system functionality
6	Verify full system functionality — confirm fix and check for side effects
7	Document findings — record problem, cause, resolution, and preventive measures

5.2 Key CLI Tools

Command	OS	Purpose / Key Flags
ping	Win/Lin/Mac	ICMP echo test connectivity; -t (continuous Win), -c (count Lin)
traceroute/tracert	Lin/Win	Trace path hop-by-hop; -d (Win: no DNS lookup)
ipconfig /all	Windows	Show IP, MAC, gateway, DNS, DHCP server
ip addr / ifconfig	Lin/Mac	Show interface IP and MAC addresses
nslookup	Win/Lin	Query DNS records; type=MX/AAAA/PTR etc.
dig	Lin/Mac	Advanced DNS query; +short, +trace
netstat -an	Win/Lin	Show active connections and listening ports
ss -tuln	Linux	Modern replacement for netstat
arp -a	Win/Lin	Display ARP cache (IP↔MAC mappings)
route print	Windows	Display routing table
ip route	Linux	Display/manipulate routing table
nmap	Lin/Win	Port scanning, OS detection (-sV, -O, -p)
tcpdump	Lin/Mac	Packet capture on CLI; -i eth0 -n port 80
Wireshark	Win/Lin	GUI packet capture and analysis
pathping	Windows	Combines ping + tracert; shows packet loss per hop
mtr	Linux	Real-time combined traceroute + ping

5.3 Common Network Issues & Likely Causes

Symptom	Likely Cause(s)
No connectivity (single host)	Bad cable/NIC, wrong IP/mask/gateway, port disabled
No connectivity (all hosts)	Switch/router failure, upstream ISP issue, DNS failure
Slow network	Duplex mismatch, high utilization, broadcast storm, STP loop
Intermittent drops	Faulty cable/connector, interference (Wi-Fi), failing NIC
IP conflict	Duplicate static IP or rogue DHCP; check DHCP bindings
APIPA address (169.254.x.x)	DHCP server unreachable; check DHCP service and scope
DNS not resolving	Wrong DNS server, DNS service down, record mismatch

Symptom	Likely Cause(s)
High latency	WAN congestion, routing issue, QoS misconfiguration
Asymmetric routing	Multiple paths with different return routes; check route table
Wi-Fi poor signal	Distance, interference (channel overlap, microwaves), obstacles
Wi-Fi auth failure	Wrong passphrase, certificate issue, RADIUS failure
VLAN mismatch	Access port on wrong VLAN; trunk native VLAN mismatch
STP loop / broadcast storm	Disabled STP, misconfig, rogue switch

5.4 Cable Troubleshooting Tools

Tool	Use
Cable tester	Verifies continuity and wiring order (T568A/B)
TDR (Time Domain Reflectometer)	Locates cable faults by measuring signal reflection timing
OTDR	Fiber optic equivalent of TDR; finds breaks/splices in fiber
Toner probe (Fox/Hound)	Traces cable runs through walls; tone generator + probe
Light meter / OLTS	Measures fiber optic signal loss
Multimeter	Tests voltage, continuity; verifies PoE power
Visual fault locator	Visible laser light to locate fiber breaks
Spectrum analyzer	Detects Wi-Fi/RF interference sources

QUICK REFERENCE – Common Ports & Protocols

Port	Protocol	Transport	Notes
20	FTP Data	TCP	FTP active mode data transfer
21	FTP Control	TCP	FTP command channel
22	SSH / SFTP	TCP	Secure shell & file transfer
23	Telnet	TCP	Unencrypted remote access — legacy
25	SMTP	TCP	Email sending (server-to-server)
53	DNS	TCP/UDP	UDP for queries; TCP for zone transfers
67	DHCP Server	UDP	Server listens for client discovery
68	DHCP Client	UDP	Client receives IP offer
69	TFTP	UDP	Trivial FTP; no auth; firmware upgrades
80	HTTP	TCP	Unencrypted web traffic
88	Kerberos	TCP/UDP	AD authentication tickets
110	POP3	TCP	Email retrieval (downloads mail)
119	NNTP	TCP	Usenet news transfer
123	NTP	UDP	Network time synchronization
135	RPC/WMI	TCP	Windows RPC endpoint mapper
137-139	NetBIOS	TCP/UDP	Windows name resolution & file sharing
143	IMAP	TCP	Email retrieval (keeps mail on server)
161	SNMP	UDP	Network monitoring queries
162	SNMP Trap	UDP	Unsolicited SNMP notifications
179	BGP	TCP	Inter-AS internet routing
389	LDAP	TCP	Directory services queries
443	HTTPS	TCP	Encrypted web traffic (TLS)
445	SMB	TCP	Windows file sharing / AD
465	SMTPS	TCP	SMTP over SSL (legacy)
514	Syslog	UDP	Log forwarding to syslog server
587	SMTP Submit	TCP	Mail submission with auth (STARTTLS)
636	LDAPS	TCP	LDAP over SSL/TLS
993	IMAPS	TCP	IMAP over SSL/TLS
995	POP3S	TCP	POP3 over SSL/TLS
1194	OpenVPN	UDP	Open-source VPN
1433	MS SQL	TCP	Microsoft SQL Server
1521	Oracle DB	TCP	Oracle database listener
1701	L2TP	UDP	Layer 2 Tunneling Protocol
1723	PPTP	TCP	Point-to-Point Tunneling Protocol (legacy)
3306	MySQL	TCP	MySQL / MariaDB database
3389	RDP	TCP	Remote Desktop Protocol (Windows)
5060	SIP	TCP/UDP	VoIP signaling (unencrypted)

Port	Protocol	Transport	Notes
5061	SIPS	TCP	SIP over TLS
5900	VNC	TCP	Virtual Network Computing remote access
6514	Syslog TLS	TCP	Encrypted syslog
8080	HTTP Alt	TCP	Alternate HTTP / proxy
8443	HTTPS Alt	TCP	Alternate HTTPS

Encryption, Protocols & Standards Reference

Encryption Standards

Algorithm	Type	Key Length	Notes
AES	Symmetric	128/192/256-bit	Current standard; very fast; used in WPA2/3, IPSec
3DES	Symmetric	168-bit	Legacy triple-DES; being phased out
RSA	Asymmetric	1024–4096-bit	Key exchange and digital signatures; slow
ECC	Asymmetric	256-bit equiv	Smaller keys, same strength; used in TLS 1.3
DH / ECDH	Key exchange	—	Diffie-Hellman key exchange; forward secrecy
SHA-1	Hash	160-bit output	Deprecated; collision vulnerable
SHA-256	Hash	256-bit output	Current standard for integrity checking
MD5	Hash	128-bit output	Broken; don't use for security; only checksum
HMAC	MAC	Variable	Message auth using symmetric key + hash

PKI & Certificates

- PKI – Public Key Infrastructure: framework for issuing/managing digital certificates
- CA (Certificate Authority) – issues and signs certificates
- X.509 – standard format for digital certificates
- CSR – Certificate Signing Request; sent to CA to get a signed cert
- CRL – Certificate Revocation List; list of revoked certs (check periodically)
- OCSP – Online Certificate Status Protocol; real-time revocation check
- Self-signed cert – signed by issuer itself; not trusted by default in browsers
- Wildcard cert (*.domain.com) – covers all subdomains
- SAN cert – Subject Alternative Name; covers multiple specific domains

TLS/SSL Versions

Version	Status	Notes
SSL 2.0/3.0	Broken	Deprecated; POODLE/BEAST attacks
TLS 1.0	Deprecated	PCI DSS non-compliant since 2018
TLS 1.1	Deprecated	Disabled in most browsers
TLS 1.2	Current	Most widely deployed; supports AES-GCM, SHA-256
TLS 1.3	Current	Fastest; removed weak ciphers; mandatory PFS

Cloud & Virtualization Concepts

Term	Definition
IaaS	Infrastructure as a Service — VMs, storage, networking (AWS EC2, Azure VMs)
PaaS	Platform as a Service — dev environment managed (Heroku, Azure App Service)
SaaS	Software as a Service — fully managed apps (Gmail, Office 365, Salesforce)
Public Cloud	Resources shared with other tenants; managed by provider
Private Cloud	Dedicated to one org; on-prem or hosted
Hybrid Cloud	Mix of on-prem + public cloud with integration
VPC	Virtual Private Cloud — isolated network segment in public cloud
SDN	Software-Defined Networking — separates control plane from data plane
NFV	Network Function Virtualization — run firewalls, routers as VMs
VXLAN	Virtual Extensible LAN — encapsulates L2 in UDP; scales to 16M segments

N10-009 Acronym Glossary

Acronym	Expansion
AAA	Authentication, Authorization, Accounting
ACL	Access Control List
AES	Advanced Encryption Standard
AH	Authentication Header (IPSec)
AP	Access Point
ARP	Address Resolution Protocol
AS	Autonomous System (BGP)
BGP	Border Gateway Protocol
BPDU	Bridge Protocol Data Unit
BYOD	Bring Your Own Device
CA	Certificate Authority
CIDR	Classless Inter-Domain Routing
CLI	Command-Line Interface
CSMA/CA	Carrier Sense Multiple Access/Collision Avoidance
CSMA/CD	Carrier Sense Multiple Access/Collision Detection
DAI	Dynamic ARP Inspection
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
DNS	Domain Name System
DORA	Discover, Offer, Request, Acknowledge
EAP	Extensible Authentication Protocol
EIGRP	Enhanced Interior Gateway Routing Protocol
ESP	Encapsulating Security Payload
FHRP	First Hop Redundancy Protocol
FTP	File Transfer Protocol
GRE	Generic Routing Encapsulation
GLBP	Gateway Load Balancing Protocol
HSRP	Hot Standby Router Protocol
HTTP	Hypertext Transfer Protocol
HTTPS	HTTP Secure
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IKE	Internet Key Exchange
IMAP	Internet Message Access Protocol
IPS	Intrusion Prevention System
IPSec	IP Security
IPAM	IP Address Management
IS-IS	Intermediate System to Intermediate System
LACP	Link Aggregation Control Protocol
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LLDP	Link Layer Discovery Protocol

Acronym	Expansion
MAC	Media Access Control
MAN	Metropolitan Area Network
MFA	Multi-Factor Authentication
MPLS	Multi-Protocol Label Switching
MTBF	Mean Time Between Failures
MTTR	Mean Time To Repair
MTU	Maximum Transmission Unit
MU-MIMO	Multi-User Multiple Input Multiple Output
NAC	Network Access Control
NAT	Network Address Translation
NDP	Neighbor Discovery Protocol
NIC	Network Interface Card
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
OCSP	Online Certificate Status Protocol
OFDM	Orthogonal Frequency Division Multiplexing
OFDMA	OFDM with Multiple Access (Wi-Fi 6)
OSPF	Open Shortest Path First
OTDR	Optical Time Domain Reflectometer
PAT	Port Address Translation (NAT overload)
PKI	Public Key Infrastructure
POP3	Post Office Protocol v3
PPP	Point-to-Point Protocol
PPTP	Point-to-Point Tunneling Protocol
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Service
RDP	Remote Desktop Protocol
RIP	Routing Information Protocol
RPO	Recovery Point Objective
RSTP	Rapid Spanning Tree Protocol
RTO	Recovery Time Objective
SAN	Storage Area Network / Subject Alt Name
SFTP	SSH File Transfer Protocol
SIP	Session Initiation Protocol
SMB	Server Message Block
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSL	Secure Sockets Layer
STP	Spanning Tree Protocol
TACACS+	Terminal Access Controller Access-Control System+
TDR	Time Domain Reflectometer

TLS	Transport Layer Security
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
VRRP	Virtual Router Redundancy Protocol
VXLAN	Virtual Extensible LAN
WAN	Wide Area Network
WPA	Wi-Fi Protected Access
WLAN	Wireless LAN

■ *Study tip: Go through acronyms daily using flashcards. Recognizing acronyms instantly saves time on exam day.*