IT DOJO

EXAM STUDY GUIDE

# Network+

## COMPTIA NETWORK+ (N10-009)

A domain-by-domain field guide to CompTIA Network+ — the vendor-neutral foundation for every networking and security career. Aligned to the current N10-009 objectives. DoD 8140/8570 approved.

5 Domains • Ports, subnetting & tables • Mnemonics & exam tips

Trusted IT & Cybersecurity Training Since 2003 • Virginia Beach, VA

**ABOUT THIS GUIDE** — This is an exam-preparation aid built around the official, publicly available exam objectives. It is designed to reinforce and condense your study — not to replace hands-on experience, official courseware, or a complete study plan. Certification exams are updated periodically, so always confirm the current objectives with the certifying body before you test. We work hard to keep this accurate but make no warranty that it is complete or error-free, and IT Dojo is not affiliated with the certification bodies named. Use it as one tool among several on your way to passing.

# Network+ at a Glance

Network+ validates the core skills to design, implement, operate, secure, and troubleshoot wired and wireless networks. It is broad and hands-on, and includes performance-based questions (PBQs) that drop you into a realistic scenario.

**EXAM CODE**
**N10-009** (V9)

**QUESTIONS**
**Max 90** (MC + PBQs)

**LENGTH**
**90 minutes**

**PASSING SCORE**
**720** (scale 100–900)

**RECOMMENDED**
**CompTIA A+ & 9–12 mo** experience

**RENEWAL**
**Valid 3 years** (CEUs)

## DOMAINS & EXAM WEIGHTING

| # | Domain | Weight | Relative |
|---|---|---|---|
| 1 | Networking Concepts | **23%** | |
| 2 | Network Implementation | **20%** | |
| 3 | Network Operations | **19%** | |
| 4 | Network Security | **14%** | |
| 5 | Network Troubleshooting | **24%** | |

**HOW TO USE THIS GUIDE**

Each section below gives the core ideas you must know, a short list of high-yield terms, an exam tip, and a self-check against the official outline. Use it as a primer and a final-week refresher — not as your only resource.

# 1 Networking Concepts

OSI model, appliances, protocols, addressing, and cloud

23%

## CORE CONCEPTS

- The **OSI model** has seven layers (Application down to Physical). Know what lives at each layer, how data is **encapsulated** on the way down and de-encapsulated on the way up, and which device or protocol maps to which layer. This framework underlies the entire exam.
- **Networking appliances & functions** — routers (L3), switches (L2), firewalls, IDS/IPS, load balancers, proxies, NGFWs, and wireless access points. Know what each does and where it sits in the traffic path.
- **Ports & protocols** — the transport choice of **TCP** (reliable, connection-oriented) vs. **UDP** (fast, connectionless), plus the well-known ports the exam expects on sight (see the cram sheet).
- **IPv4 addressing & subnetting** — classful ranges, private ranges (RFC 1918), **APIPA** (169.254.x.x), CIDR notation, and the ability to subnet quickly. **IPv6** adds 128-bit addressing, SLAAC, and address types (link-local, global unicast).
- **Traffic types** — unicast (one-to-one), multicast (one-to-many subscribers), anycast (nearest of many), and broadcast (all on the segment).
- **Cloud concepts** — service models (IaaS, PaaS, SaaS), deployment models, NFV, VPCs, network security groups, and the scalability and elasticity that make cloud networking different from on-prem.

## OSI MODEL (LAYER 7 → 1)

| Layer | Examples | Device |
|---|---|---|
| **7 Application** | HTTP, DNS, SMTP, SNMP | — |
| **6 Presentation** | TLS, SSL, JPEG, ASCII | — |
| **5 Session** | RPC, NetBIOS | — |
| **4 Transport** | TCP, UDP | — |
| **3 Network** | IP, ICMP, IPSec | Router |
| **2 Data Link** | Ethernet, ARP, MAC, switches | Switch |
| **1 Physical** | Cables, bits, signaling | Hub, repeater |

### HIGH-YIELD TERMS

OSI layers, encapsulation, TCP vs. UDP, well-known ports, RFC 1918, APIPA, CIDR, SLAAC, unicast/multicast/anycast/broadcast, VPC, NFV.

**EXAM TIP**

The **OSI model is the single most-tested concept** on Network+. Be able to place any protocol, device, or PDU at its correct layer instantly — many questions hinge on it.

**MEMORY AID**

OSI Layer 1→7: "**Please Do Not Throw Sausage Pizza Away**" (Physical, Data Link, Network, Transport, Session, Presentation, Application). Router = L3, Switch = L2, Hub = L1.

**OUTLINE COVERAGE — SELF-CHECK**

- ☐ OSI reference model
- ☐ Networking appliances & functions
- ☐ Cloud concepts & connectivity
- ☐ Ports, protocols & traffic types
- ☐ IPv4 & IPv6 addressing
- ☐ Network topologies & environments

# 2 Network Implementation

Routing, switching, wireless, and physical installations

20%

## CORE CONCEPTS

- **Routing technologies** — static vs. dynamic routing, the routing table, and the dynamic protocols **OSPF** (link-state), **EIGRP** (Cisco hybrid), and **BGP** (the routing protocol of the internet). Add **NAT/PAT** and first-hop redundancy (FHRP).
- **Switching technologies** — **VLANs** and 802.1Q trunking, Spanning Tree Protocol (STP) to prevent loops, port security, link aggregation (LACP), the MAC address table, jumbo frames, and Power over Ethernet (PoE).
- **Wireless standards** — the 802.11 family (a/b/g/n/ac, and ax / **Wi-Fi 6**), the 2.4, 5, and 6 GHz bands, channel planning to avoid overlap, SSIDs, and antenna types.
- **Physical cabling** — copper categories (Cat 5e, 6, 6a, 7, 8) and their speed/distance limits, fiber (single-mode vs. multimode), connectors (RJ45, LC, SC, ST), and transceivers (SFP, SFP+, QSFP).
- Match the medium to the requirement: distance, speed, and interference all drive the choice between copper and fiber, and between one cable category and another.

## WI-FI (802.11) STANDARDS

| Standard | Band | Max Speed |
|---|---|---|
| **a** | 5 GHz | 54 Mbps |
| **b** | 2.4 GHz | 11 Mbps |
| **g** | 2.4 GHz | 54 Mbps |
| **n (Wi-Fi 4)** | 2.4 / 5 GHz | 600 Mbps |
| **ac (Wi-Fi 5)** | 5 GHz | ~3.5 Gbps |
| **ax (Wi-Fi 6/6E)** | 2.4 / 5 / 6 GHz | ~9.6 Gbps |

### HIGH-YIELD TERMS

static/dynamic routing, OSPF/EIGRP/BGP, NAT/PAT, FHRP, VLAN, 802.1Q, STP, LACP, PoE, 802.11ax (Wi-Fi 6), single-mode vs. multimode fiber, SFP.

### EXAM TIP

Memorize **copper cable categories and their max speeds/distances** and the **802.11 standards with their bands and speeds** — both are reliable points and appear in PBQs.

**MEMORY AID**

**OSPF** = open standard link-state; **EIGRP** = Cisco; **BGP** = between autonomous systems (the internet). Copper Ethernet maxes at **100 meters**; need more, go fiber.

**OUTLINE COVERAGE — SELF-CHECK**

- [ ] Routing technologies & concepts
- [ ] Switching technologies & features
- [ ] Wireless standards & deployment
- [ ] Physical cabling & connectors
- [ ] Network appliance installation

# 3 Network Operations

Documentation, availability, monitoring, and management

19%

## CORE CONCEPTS

- **Documentation** — physical and logical network diagrams, rack diagrams, IP address management (IPAM), an IP/asset schema, and agreements such as SLAs and MOUs. Good documentation is what makes troubleshooting fast.
- **Disaster recovery & availability** — the recovery metrics **RTO** and **RPO**, reliability metrics **MTTR** and **MTBF**, recovery sites (hot/warm/cold), backups, and redundancy designs (active-active vs. active-passive).
- **High availability** is built from redundancy — load balancing, NIC teaming, clustering, and first-hop redundancy — so that a single failure does not take the service down.
- **Network monitoring** — **SNMP** for device polling and traps, **syslog** for centralized logs, flow data (NetFlow), SIEM correlation, and the performance baselines you compare against to spot anomalies.
- **Network management & access** — in-band vs. out-of-band management, jump boxes/hosts, console access, and secure remote management over VPN.

## RECOVERY SITE TYPES

| Site | Whats Ready | Speed | Cost |
|---|---|---|---|
| **Cold** | Space & power only | Slowest | Lowest |
| **Warm** | Some hardware; restore data | Moderate | Medium |
| **Hot** | Fully equipped, near-real-time data | Fastest | Highest |

### HIGH-YIELD TERMS

logical/physical diagrams, IPAM, SLA/MOU, RTO/RPO, MTTR/MTBF, hot/warm/cold sites, active-active vs. active-passive, SNMP, syslog, NetFlow, baseline, out-of-band.

### EXAM TIP

Do not confuse the four-letter metrics. **RTO/RPO** are about recovery objectives; **MTTR/MTBF** are about reliability. They show up together specifically to trip you up.

### MEMORY AID

**RTO** = how fast you must **recover**; **RPO** = how much **data** you can lose. **MTBF** = time **Between** failures (reliability); **MTTR** = time **To Repair**.

**OUTLINE COVERAGE — SELF-CHECK**

- [ ] Network documentation
- [ ] Disaster recovery & business continuity
- [ ] High availability & redundancy
- [ ] Network monitoring & logging
- [ ] Network management & access methods

# 4 Network Security

Concepts, attacks, hardening, and remote access

14%

## CORE CONCEPTS

- **Security concepts** — the CIA triad applied to networks, defense in depth, **zero trust**, least privilege, role-based access, and identity controls (MFA, RADIUS, TACACS+, 802.1X). Physical security and geofencing also appear.
- **Common attacks** — DoS/DDoS, **VLAN hopping**, **ARP spoofing/poisoning**, **DNS poisoning**, on-path (MITM), rogue access points and evil twins, MAC flooding, and social engineering. Learn the indicator that gives each one away.
- **Network hardening** — disable unused ports and services, change default credentials, apply **port security**, **802.1X**, **DHCP snooping**, and **dynamic ARP inspection**, and filter with ACLs. Small hardening steps close the most common holes.
- **Remote access** — site-to-site vs. client-to-site VPNs, **IPSec** (with AH and ESP), and SSL/TLS VPNs. Know when each is appropriate.
- Match the **mitigation to the attack**: DHCP snooping stops rogue DHCP servers, dynamic ARP inspection stops ARP poisoning, and port security stops MAC flooding.

## COMMON NETWORK ATTACKS

| Attack | Best Mitigation |
|---|---|
| **ARP poisoning** | Dynamic ARP Inspection (DAI). |
| **Rogue DHCP** | DHCP snooping. |
| **MAC flooding** | Port security. |
| **VLAN hopping** | Disable DTP; change native VLAN. |
| **Evil twin / rogue AP** | Wireless IPS; 802.1X; WPA3. |
| **DDoS** | Rate limiting; upstream filtering. |

**HIGH-YIELD TERMS**

zero trust, least privilege, 802.1X, RADIUS/TACACS+, DDoS, VLAN hopping, ARP poisoning, DNS poisoning, evil twin, DHCP snooping, dynamic ARP inspection, IPSec.

**EXAM TIP**

The exam loves **attack-to-mitigation mapping**. When you see ARP poisoning, think dynamic ARP inspection; rogue DHCP, think DHCP snooping; MAC flooding, think port security.

**MEMORY AID**

**DHCP snooping** stops rogue **DHCP**; **D**ynamic **A**RP **I**nspection stops **ARP** poisoning; **port security** stops **MAC flooding**. **RADIUS** encrypts only the password; **TACACS+** encrypts the whole payload.

**OUTLINE COVERAGE — SELF-CHECK**

- [ ] Security concepts & zero trust
- [ ] Common attack types & indicators
- [ ] Network hardening techniques
- [ ] Remote access & VPNs
- [ ] Physical & logical access control

# 5 Network Troubleshooting

Methodology, cabling, tools, and common issues

24%

## CORE CONCEPTS

- CompTIA's **seven-step troubleshooting methodology** is examinable in order: identify the problem, establish a theory of probable cause, test the theory, establish a plan of action, implement the solution, verify full system functionality, and document findings. Expect questions on what step comes next.
- **Cabling issues** — attenuation, crosstalk, EMI, incorrect pinout, transmit/receive (TX/RX) reversed, bad or dirty connectors, and exceeding distance limits. Many "network down" scenarios are physical-layer problems.
- **Hardware tools** — cable tester, tone generator and probe (toner), wire map tester, OTDR and light meter for fiber, multimeter, and spectrum analyzer for wireless interference.
- **Software tools & commands** — `ping`, `traceroute/tracert`, `nslookup/dig`, `ipconfig/ifconfig/ip`, `netstat`, `arp`, `nmap`, and protocol analyzers like Wireshark/tcpdump. Know what each one reveals.
- **Common issues** — IP address conflicts, wrong default gateway or subnet mask, DNS failures, DHCP exhaustion, duplex/speed mismatch, and wireless problems (interference, channel overlap, weak signal).

## TROUBLESHOOTING COMMAND-LINE TOOLS

| Tool | What It Tells You |
|---|---|
| **ping** | Basic reachability and round-trip latency. |
| **traceroute / tracert** | The hop-by-hop path to a destination. |
| **nslookup / dig** | DNS name-to-IP resolution. |
| **ipconfig / ip** | Local interface, IP, gateway, DNS config. |
| **netstat** | Active connections and listening ports. |
| **arp** | MAC-to-IP mappings in the local cache. |

### HIGH-YIELD TERMS

7-step methodology, attenuation, crosstalk, EMI, TX/RX reversed, OTDR, toner probe, ping, traceroute, nslookup, netstat, duplex mismatch, channel overlap.

### EXAM TIP

This is the **largest domain (24%)** and the most PBQ-heavy. Know the **seven steps in order** and what each command-line tool outputs — both are guaranteed points.

**MEMORY AID**

Troubleshooting steps: "**I Tend To Plan In Very Detailed**" — Identify, Theory, Test, Plan, Implement, Verify, Document. `ping` tests reachability; `traceroute` shows the path; `nslookup` tests DNS.

**OUTLINE COVERAGE — SELF-CHECK**

- [ ] Apply the troubleshooting methodology
- [ ] Troubleshoot cabling & physical issues
- [ ] Use hardware & software tools
- [ ] Troubleshoot common network issues
- [ ] Troubleshoot wireless issues

# Acronym & Term Quick-Reference

Network+ is acronym-dense. These appear across multiple domains — know them on sight.

**OSI** — Open Systems Interconnection (7-layer model)

**TCP/UDP** — Transmission Control / User Datagram Protocol

**VLAN** — Virtual Local Area Network

**STP** — Spanning Tree Protocol

**LACP** — Link Aggregation Control Protocol

**PoE** — Power over Ethernet

**NAT/PAT** — Network / Port Address Translation

**OSPF** — Open Shortest Path First

**BGP** — Border Gateway Protocol

**EIGRP** — Enhanced Interior Gateway Routing Protocol

**APIPA** — Automatic Private IP Addressing (169.254.x.x)

**CIDR** — Classless Inter-Domain Routing

**SLAAC** — Stateless Address Autoconfiguration

**SNMP** — Simple Network Management Protocol

**SDN** — Software-Defined Networking

**SSID** — Service Set Identifier

**RADIUS** — Remote Authentication Dial-In User Service

**802.1X** — Port-based network access control

**DAI** — Dynamic ARP Inspection

**VPN** — Virtual Private Network

**IPSec** — Internet Protocol Security

**RTO/RPO** — Recovery Time / Point Objective

**MTTR/MTBF** — Mean Time To Repair / Between Failures

**OTDR** — Optical Time-Domain Reflectometer

## SUGGESTED STUDY PLAN

| Timeframe | Focus |
|---|---|
| **Week 1** | Domain 1 (Networking Concepts, 23%) — master the OSI model, ports, and addressing; start subnetting drills. |
| **Week 2** | Domain 2 (Implementation) — routing, switching, VLANs, wireless standards, and cabling. |
| **Week 3** | Domain 3 (Operations) — documentation, availability metrics, and monitoring. |
| **Week 4** | Domain 4 (Security) — attacks, hardening, and VPNs; drill attack-to-mitigation mapping. |
| **Weeks 5–6** | Domain 5 (Troubleshooting, 24%) — memorize the seven steps and every tool; practice PBQs, then take full-length exams. |

**EXAM-DAY STRATEGY**

Network+ rewards **methodical thinking**. On troubleshooting questions, apply the seven-step method and pick the answer that matches the **current** step. On PBQs, read the whole scenario first. When two answers look right, choose the one that fixes the root cause with the least disruption, and flag hard items to revisit — every question counts the same.

# Rote-Fact Reference

The pure-memorization facts this exam expects you to know cold. Drill these until recall is automatic.

## COMMON PORTS & PROTOCOLS

| Port | Protocol | Notes |
|---|---|---|
| **20 / 21** | FTP (data / control) | Unencrypted file transfer. |
| **22** | SSH / SCP / SFTP | Secure remote access & transfer. |
| **23** | Telnet | Remote access — unencrypted (insecure). |
| **25** | SMTP | Email sending. |
| **53** | DNS | Name resolution (TCP & UDP). |
| **67 / 68** | DHCP | Dynamic IP assignment. |
| **69** | TFTP | Trivial FTP (UDP). |
| **80** | HTTP | Web (unencrypted). |
| **88** | Kerberos | Authentication. |
| **110 / 995** | POP3 / POP3S | Email retrieval / over TLS. |
| **123** | NTP | Time synchronization. |
| **137–139** | NetBIOS | Legacy Windows networking. |
| **143 / 993** | IMAP / IMAPS | Email retrieval / over TLS. |
| **161 / 162** | SNMP | Network management / traps. |
| **389 / 636** | LDAP / LDAPS | Directory services / over TLS. |
| **443** | HTTPS | Web over TLS. |
| **445** | SMB | Windows file sharing. |
| **514** | Syslog | Log collection. |
| **3306** | MySQL | MySQL database. |
| **3389** | RDP | Remote Desktop. |

## CIDR / SUBNET QUICK REFERENCE

| CIDR | Subnet Mask | Usable Hosts |
|---|---|---|
| **/24** | 255.255.255.0 | 254 |
| **/25** | 255.255.255.128 | 126 |
| **/26** | 255.255.255.192 | 62 |
| **/27** | 255.255.255.224 | 30 |
| **/28** | 255.255.255.240 | 14 |
| **/29** | 255.255.255.248 | 6 |
| **/30** | 255.255.255.252 | 2 |

## PRIVATE (RFC 1918) & SPECIAL RANGES

| Range | Use |
|---|---|
| **10.0.0.0 – 10.255.255.255** | Private Class A (/8). |
| **172.16.0.0 – 172.31.255.255** | Private Class B (/12). |
| **192.168.0.0 – 192.168.255.255** | Private Class C (/16). |
| **169.254.0.0 / 16** | APIPA (no DHCP reached). |
| **127.0.0.1** | Loopback (localhost). |

## COPPER CABLE CATEGORIES

| Category | Max Speed | Max Distance |
|---|---|---|
| **Cat 5e** | 1 Gbps | 100 m |
| **Cat 6** | 1 Gbps (10G ≤ 55 m) | 100 m |
| **Cat 6a** | 10 Gbps | 100 m |
| **Cat 7** | 10 Gbps | 100 m |
| **Cat 8** | 25–40 Gbps | 30 m |

# Flashcards — Cover & Recall

Cover the right column, answer each prompt aloud, then check. Repeat over several days — retrieving the answer (not re-reading it) is what moves it into long-term memory.

| Prompt | Answer |
|---|---|
| **OSI layers, 7 down to 1** | Application, Presentation, Session, Transport, Network, Data Link, Physical. |
| **Router / switch / hub operate at which OSI layers?** | Router = L3, switch = L2, hub = L1. |
| **TCP vs. UDP** | TCP = reliable, connection-oriented; UDP = fast, connectionless. |
| **Ports: HTTP / HTTPS** | 80 / 443. |
| **Ports: SSH / Telnet / RDP** | 22 / 23 / 3389. |
| **Ports: DNS / DHCP** | 53 / 67–68. |
| **What is the APIPA range?** | 169.254.0.0/16 — assigned when no DHCP server is reachable. |
| **RFC 1918 private ranges** | 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16. |
| **Usable hosts in a /24, /27, /30** | 254, 30, 2. |
| **OSPF vs. BGP vs. EIGRP** | OSPF = open link-state; BGP = between autonomous systems (internet); EIGRP = Cisco. |
| **What does STP prevent?** | Switching loops in a Layer 2 network. |
| **802.1Q is for…** | VLAN tagging on trunk links. |
| **Max distance for copper Ethernet?** | 100 meters. |
| **Single-mode vs. multimode fiber** | Single-mode = long distance, laser; multimode = shorter distance, LED. |
| **Wi-Fi 6 standard name and bands** | 802.11ax; 2.4, 5, and 6 GHz. |
| **RTO vs. RPO** | RTO = time to recover; RPO = acceptable data loss. |
| **MTBF vs. MTTR** | MTBF = time between failures (reliability); MTTR = time to repair. |
| **Mitigation for ARP poisoning** | Dynamic ARP Inspection (DAI). |
| **Mitigation for rogue DHCP** | DHCP snooping. |
| **Mitigation for MAC flooding** | Port security. |

| | |
|---|---|
| **RADIUS vs. TACACS+** | RADIUS encrypts only the password; TACACS+ encrypts the whole payload (and separates AAA). |
| **The seven troubleshooting steps** | Identify, theory, test theory, plan, implement, verify, document. |
| **Which tool shows the hop-by-hop path?** | traceroute / tracert. |
| **Which command tests DNS resolution?** | nslookup / dig. |

# Exam Cram Sheet

Network+ distilled to the must-memorize essentials — your final-review sheet. If you can recall every line here from memory, you are ready.

### OSI (7→1)

- App, Presentation, Session, Transport,
- Network, Data Link, Physical
- Router L3, Switch L2, Hub L1

### PORTS: LOW

- 20/21 FTP, 22 SSH, 23 Telnet
- 25 SMTP, 53 DNS, 67/68 DHCP
- 69 TFTP, 80 HTTP, 88 Kerberos

### PORTS: HIGH

- 110 POP3, 143 IMAP, 161/162 SNMP
- 389 LDAP, 443 HTTPS, 445 SMB
- 514 Syslog, 636 LDAPS, 3389 RDP

### ADDRESSING

- Private: 10/8, 172.16/12, 192.168/16
- APIPA = 169.254.0.0/16
- Loopback = 127.0.0.1

### SUBNET HOSTS

- /24 = 254, /25 = 126, /26 = 62
- /27 = 30, /28 = 14, /29 = 6, /30 = 2
- Hosts = 2^(host bits) − 2

### ROUTING

- Static vs. dynamic
- OSPF = link-state (open)
- BGP = internet / between AS
- EIGRP = Cisco; NAT/PAT conserves IPs

### SWITCHING

- VLAN + 802.1Q trunking
- STP prevents loops
- LACP = link aggregation
- Port security, PoE

### WIRELESS

- a=5GHz, b/g=2.4GHz
- n = 2.4/5, ac = 5
- ax (Wi-Fi 6) = 2.4/5/6 GHz
- Use WPA3

### CABLING

- Cat 5e/6 = 1G, 6a = 10G
- Copper max 100 m
- SMF = long; MMF = short
- Fiber for distance / no EMI

### AVAILABILITY

- RTO = recover time; RPO = data loss
- MTBF = reliability; MTTR = repair
- Sites: cold/warm/hot
- Active-active vs. active-passive

### SECURITY MITIGATIONS

- ARP poisoning → DAI
- Rogue DHCP → DHCP snooping
- MAC flooding → port security
- VLAN hopping → disable DTP

### TROUBLESHOOTING

- 7 steps: Identify, Theory, Test,
- Plan, Implement, Verify, Document
- ping=reach, traceroute=path
- nslookup=DNS, netstat=connections

# Free & Community Study Resources

Free and community study resources for this exam, compiled to help you actually pass. These are independent, third-party resources — IT Dojo is not affiliated with them and cannot guarantee their availability or accuracy — but each is widely used and well regarded by candidates. Always cross-check against the current official exam objectives.

### FREE VIDEO TRAINING

Professor Messer N10-009 — The complete free Network+ video course, plus monthly study groups and weekly pop quizzes.

### OFFICIAL & FREE PRACTICE

CompTIA Exam Objectives — The official N10-009 blueprint and free sample questions — anchor all study to this.

ExamCompass — Free N10-009 practice tests and topic quizzes, no signup required.

### QUICK REFERENCE & COMMUNITY

StationX Cheat Sheet — Free quick reference: ports, OSI model, subnetting, and acronyms.

r/CompTIA — Active community with "how I passed" write-ups and study advice.

IT DOJO

## Ready to earn your Network+?

IT Dojo's instructor-led Network+ training delivers live expert instruction, hands-on labs, and subnetting and PBQ practice that prepare your team for the exam and the job. Employer-sponsored training for DoD, federal, and corporate clients.

**Course:** www.itdojo.com/comptia-training/network-fundamentals/

**Phone:** 757-216-3656 | **Email:** info@itdojo.com

**Hours:** Monday–Friday, 8:30 AM – 4:30 PM ET

4176 South Plaza Trail, Suite 207, Virginia Beach, VA 23452