# CompTIA Network+ Cheat Sheet

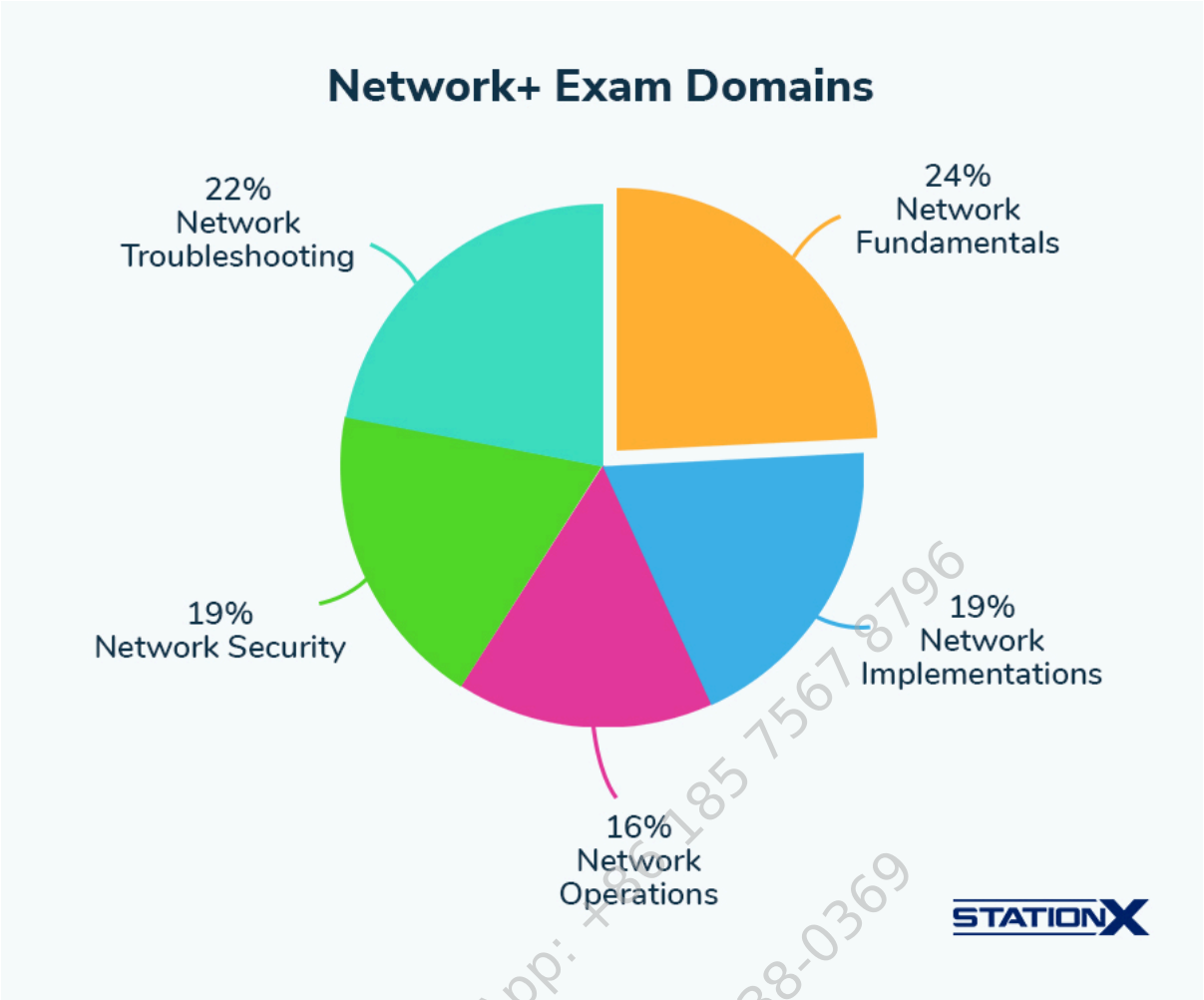

STATIONX
THE CYBER SECURITY COMPANY

## About CompTIA Network+

The CompTIA Network+ exam tests your fundamental skills in essential computer networking functions.

You'll need to answer at most 90 questions in this 90-minute examination and complete a survey after it ends. The passing score is 720 on a scale of 100–900.

The latest CompTIA Security+ exam code is N10-008, available from September 2021 to sometime in 2024. The exam objectives (domains) are as follows:




CompTIA Network+ Exam Domains



## Domains

This Net+ cheat sheet arranges concepts according to our Total Seminars Network+ course subtopics. Diagrams put concepts into a visual form and tables compartmentalize information. Here's a key to finding items by domain:

| Hashtag (Remember to type the # symbol) | Domain (N10-008) |
|---|---|
| #nf | Networking Fundamentals |
| #ni | Network Implementations |
| #no | Network Operations |
| #ns | Network Security |
| #nt | Network Troubleshooting |

## Network Models

This section lays the foundation for all other Network+ sections.

| Domain | Concept | Elaboration |
|---|---|---|
| #nf | OSI model | Open Systems Interconnect:<br>1. Physical<br>2. Data Link<br>3. Network<br>4. Transport<br>5. Session<br>6. Presentation<br>7. Application<br><br>Memory aid: **Please Do Not Throw Sausage Pizza Away** |
| #nf | Unicast/Broadcast | One/All network devices receive data |
| #nf #ni | DHCP | Dynamic Host Configuration Protocol |

## Cabling and Topology

Be careful: it's easy to provide incorrect answers to exam questions related to the different fiber connector types.

| Domain | Concept | Elaboration |
|---|---|---|
| #nf | Network topology | • Mesh<br>• Star (hub-and-spoke)<br>• Bus<br>• Ring<br>• Hybrid |
| #nf | TIA/EIA-568A | 1. White/green<br>2. Green<br>3. White/orange<br>4. Blue<br>5. White/blue<br>6. Orange<br>7. White/brown<br>8. Brown |
| #nf | TIA/EIA-568B | Swap "green" and "orange" in TIA/EIA-568A |
| #nf | Coaxial | F-type, BNC |
| #nf | Twinaxial/twinax | Has two inner conductors instead of one as in coaxial |
| #nf | Twisted pair | RJ-45, RJ-11 |
| #nf | STP/UTP | Shielded/Unshielded twisted pair |

| | | |
|---|---|---|
| #nf | Fiber optic | SC, ST, LC, FC, MT-RJ |
| #nt | Plenum-rated | Fire-resistant cable; compare with riser-rated, non-plenum rated, and PVC |
| #nf | Multimode/Single-mode | Cables carry LED/laser signals |
| #nf | UTP category | Define speed and length of cables:<br>• Cat 3<br>• Cat 5<br>• Cat 5e<br>• Cat 6/6a<br>• Cat 7<br>• Cat 8 |

## Ethernet Basics

Recognizing the Ethernet naming syntax (10Base5, 100Base5, 1000Base5, 10Broad5, 10BaseT, etc.) is crucial to the Network+ exam.

| Domain | Concept | Elaboration |
|---|---|---|
| #ni #nt | (Auto-)MDI-X | (Automatic) medium dependent interface crossover |
| #ni #nt | Uplink port | Enable connection between two switches using a straight-through cable |
| #ni #nt | CSMA/CD | Carrier sense multiple access with collision detection |



## Ethernet Standards

Familiarize yourself with 1000Base and 10GBase types (names, distances, node numbers, cable types, etc.).

| Domain | Concept | Elaboration |
|---|---|---|
| #nf | 1000BaseT | Maximum cable length: 100m; max speed: 1,000 Mbps (1 Gbps) |
| #nf | Half-duplex | For one-way communication |
| #nf | Full-duplex | For simultaneous two-way traffic |
| #nf | GBIC | Gigabit interface converter |
| #nf | SFP, SFP+ | Small form-factor pluggable |
| #nf | QSFP | Quad small form-factor pluggable |

| | | |
|---|---|---|
| #ni #nt | Switching/Bridging loop | Two or more data link layer paths between two endpoints |
| #ni #nt | Layer 2 attack | Attacks on OSI model layer 2 (data link) |
| #ni #nt | Flood guard | Block malicious traffic from entering a network |

## Installing a Physical Network

Remember the following concepts in structured cabling:

| Domain | Concept | Elaboration |
|---|---|---|
| #nf | 66-punchdown | Typically used in non-VoIP telephone systems |
| #nf | 110-punchdown | For copper-wired networks |
| #nf | Fiber distribution panel | For fiber-optic networks |
| #nt | Wiremap | Simple test to confirm each wire terminates correctly |
| #nt | TDR | Time domain reflectometer |
| #nt | OTDR | Optical TDR |
| #nt | NEXT | Near-end crosstalk |
| #nt | FEXT | Far-end crosstalk |
| #nf #ns #no | MDF | Main distribution frame |
| #nf #ns #no | IDF | Intermediate distribution frame |
| #nf #ns | U (unit) | Standard height for rack components; 19-inch wide and a multiple of 1¾-inch tall |
| #nf #ns | Demarc | Separate the telecom company's property from your responsibility |



## TCP/IP Basics

Review additional information on IPv4 on your own.

| Domain | Concept | Elaboration |
|---|---|---|
| #nf #ni | Internet Protocol (IP) | IPv4 and IPv6 |
| #nf #ni | Transmission Control Protocol (TCP) | Connection-oriented |

| | | |
|---|---|---|
| #nf #ni | User Datagram Protocol (UDP) | Connectionless |
| #nf #ni | IPv4 address | 32-bit number, consisting of four decimals from 0 to 255 separated by period (.), e.g., 192.168.1.1 |
| #nf #ni | IPv4 loopback | 127.0.0.1 |
| #nf #ni | APIPA/link-local | 169.254.x.x |
| #nf #ni | Classless Inter-Domain Routing (CIDR) | CIDR IPv4 addresses have a prefix; e.g., "/24" in "10.150.23.58/24" denotes a 255.255.255.0 subnet mask. |

## Routing

Review router-related abbreviations below.

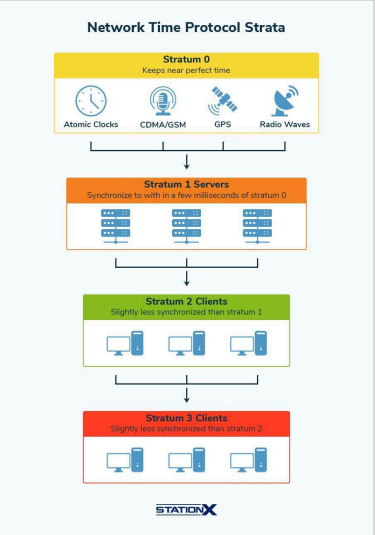
| Domain | Concept | Elaboration |
|---|---|---|
| #nf #ni | BGP | Border Gateway Protocol |
| #ni | OSPF | Open Shortest Path First |
| #ni | RIP | Routing Information Protocol |
| #nf #ni | MTU | Maximum transmission unit |
| #nf #ni | IGP/EGP | Interior/Exterior Gateway Protocol |
| #nf | NAT | Network Address Translation |
| #nf | PAT | Port Address Translation |

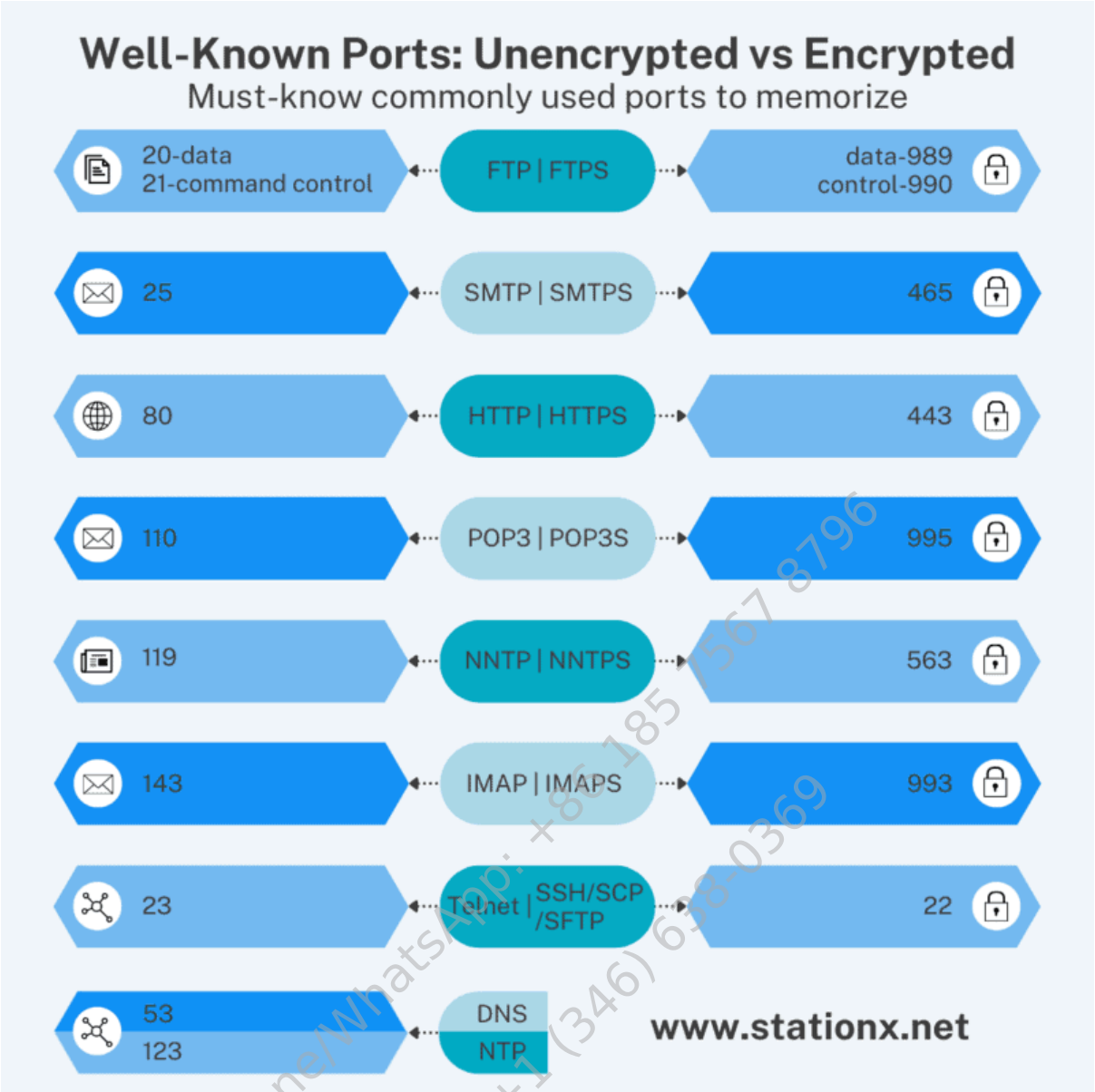


## TCP/IP Applications

Remember to check out our Common Ports Cheat Sheet.

| Domain | Concept | Elaboration |
|---|---|---|
| #nf | NTP | Network Time Protocol |

| | | |
|---|---|---|
| | |  |
| #nf | SNTP | Simple Network Time Protocol |
| #nt | IGMP | Internet Group Management Protocol |
| #nf #nt | IPAM | IP Address Management |
| #nt | Networking troubleshooting tools | Windows: tracert<br>Linux:<br>• traceroute<br>• ifconfig<br>• pathping<br>• netstat |






## Network Naming

Network administrators cannot skip this section.

| Domain | Concept | Elaboration |
|---|---|---|
| #nf | DNS | Domain Name System |
| #nf | SOA | Start of authority |
| #nf | A/AAAA | DNS record for IPv4/IPv6 |
| #nf | CNAME | Canonical name or alias |
| #nf | MX | Mail exchange |
| #nf | PTR | Pointer record |

## Securing TCP/IP

Review key network security acronyms here.

| Domain | Concept | Elaboration |
|---|---|---|
| #ns | RADIUS | For authentication, authorization, and accounting |
| #ns | TACACS+ | For access control |
| #ns | Kerberos | For authentication and authorization on wired networks |
| #ns | EAP | Extensible Authentication Protocol |
| #ns | PEAP | Protected Extensible Authentication Protocol |
| #nt | PKI | Public Key Infrastructure |
| #ns | SAML | Security Assertion Markup Language |

## Switch Features

The definition for VLAN (virtual local area network) is in the section Integrating Networked Devices.

| Domain | Concept | Elaboration |
|---|---|---|
| #ni | VTP | VLAN Trunking Protocol |
| #ni #ns #nt | STP | Spanning Tree Protocol |
| #ni #ns #nt | BPDU | Bridge protocol data unit |
| #ni #no | LACP | Link Aggregation Control Protocol |
| #ni | QoS | Quality of service |
| #ni | IDS | Intrusion detection system |
| #ni | IPS | Intrusion prevention system |

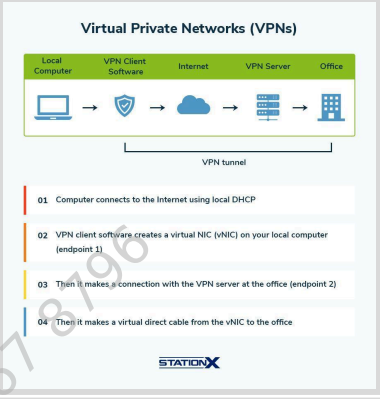
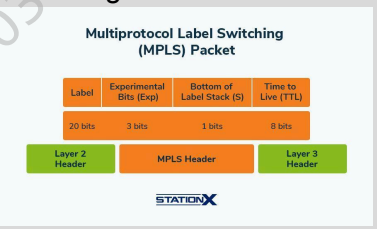
## IPv6

Here are IPv6 concepts for quick learning:

| Domain | Concept | Elaboration |
|---|---|---|
| #nf #ni | NDP | Neighbor Discovery Protocol |
| #nf #ni | IPv6 address | 128-bit hexadecimal number, e.g., 2001:7120:0000:8001:0000:0000:0000:1F10 |
| #nf #ni | IPv6 loopback | ::1 (unicast) |
| #nf | VLSM | Variable-length subnet mask |

# WAN Connectivity

Review additional information on WAN construction by yourself.

| Domain | Concept | Elaboration |
|---|---|---|
| #nf #ns | VPN | Virtual Private Network   |
| #nf | WDM/BWDM | Bidirectional wavelength division multiplexing |
| #nf | DWDM | Dense wavelength division multiplexing |
| #nf | MPLS | Multiprotocol Label Switching   |
| #ni | GSM | Global System for Mobile Communications |
| #ni | TDMA | Time-division multiple access |
| #ni | EDGE | Enhanced Data rates for GSM Evolution |
| #ni | CDMA | Code-division multiple access |
| #nf #ns | ICA | Independent Computing Architecture (Citrix) |
| #nf #ns | TightVNC | Tight Virtual Network Computing |
| #nf #ns | RDP | Microsoft Remote Desktop Protocol |
| #nf #ns | PPTP | Point-to-Point Tunneling Protocol |
| #nf #ns | L2TP/IPsec | Layer 2 Tunneling Protocol over IPsec |
| #nf #ns | EAP | Encapsulating Security Payload |

| | | |
|---|---|---|
| #nf #ns | GRE | Generic Routing Encapsulation |

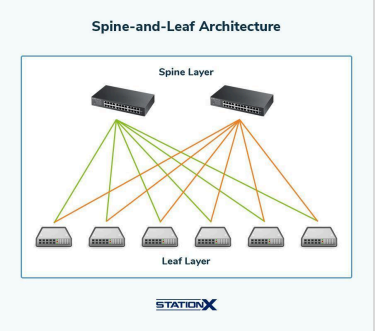
## Wireless Networking

The ubiquity of mobile devices makes mastering wireless networking a necessity.

| Domain | Concept | Elaboration |
|---|---|---|
| #ni | SSID | Service Set Identifier |
| #ni | BSSID/ESSID | Basic/Extended Service Set Identifier |
| #ni | CSMA/CA | Carrier-sense multiple access with collision avoidance |
| #ni | DSSS | Direct-sequence spread-spectrum |
| #ni | OFDM | Orthogonal frequency-driven multiplexing |
| #ni | Wireless Ethernet versions | • 802.11a<br>• 802.11b<br>• 802.11g<br>• (802.11i)<br>• 802.11n<br>• 802.11ac<br>• 802.11ax |
| #ni | PoE | Power over Ethernet<br>• PoE injector<br>• PoE+ 802.3af. 15.4 watts<br>• PoE+ 802.3at, 30 watts |
| #ni #nt | Wireless antennae | • Omni<br>• Dipole<br>• Patch<br>• Directional/Yagi<br>• Directional/Parabolic<br>• SMA (SubMiniature version A) connector<br>Gain measured in dBi |
| #ni | WPA2 | Wi-Fi Protected Access version 2, encryption: CCMP-AES |
| #nt | APIPA | Automatic Private IP Addressing |
| #ns | Evil twin | Fake Wi-Fi access point to trick people into choosing it over the genuine one |

# Virtualization and Cloud Computing

This section covers virtual machines and key ideas in cloud computing.

| Domain | Concept | Elaboration |
|---|---|---|
| #nf | Cloud | Considerations:<br>• Scalability<br>• Elasticity<br>• Multitenancy<br>• Security implications<br>• Principle of least privilege<br><br>Types:<br>• Public<br>• Private<br>• Community<br>• Hybrid |
| #nf | Hypervisor Type 1 | Bare or native metal |
| #nf | Hypervisor Type 2 | App-like VM on the operating system |
| #nf | IaaS | Infrastructure as a Service |
| #nf | PaaS | Platform as a Service |
| #nf | SaaS | Software as a Service |
| #nf | DaaS | Desktop as a Service |
| #nf | VDI | Virtual desktop infrastructure |
| #nf | IaC | Infrastructure as Code |
| #nf | vSwitch | Virtual switch |
| #nf | VPC | Virtual private cloud |
| #nf | NFV | Network function virtualization |
| #nf | SDN | Software-defined networking<br><br>  |



# Data Centers

The prevalence of cloud computing makes learning about data centers a necessity.

| Domain | Concept | Elaboration |
|---|---|---|
| #nf | FCoE | Fibre Channel over Ethernet |
| #nf | FC | Fibre Channel |
| #nf | HBA | Host bus adaptor |
| #no | FHRP | First Hop Redundancy Protocol |
| #no | VRRP | Virtual Router Redundancy Protocol |
| #no | HSRP | Hot Standby Router Protocol |
| #no | UPS | Uninterruptible power supply |
| #no | HVAC | Heating, ventilation, and air conditioning |
| #no | PDU | Power distribution unit |

## Integrating Networked Devices

Know the differences between every type of “area network.”

| Domain | Concept | Elaboration |
|---|---|---|
| #ni #ns | IoT | Internet of Things |
| #nf #ni | VoIP | Voice over IP |
| #ni | ICS | Industrial control systems |
| #ni | SCADA | Supervisory control and data acquisition system |
| #nf #ni | LAN | Local area network |
| #nf | WLAN | Wireless local area network |
| #ni | VLAN | Virtual LAN; split one broadcast domain into two |
| #nf | CAN | Campus area network |
| #nf | WAN | Wide area network |
| #nf | SD-WAN | Software-defined wide area network |
| #nf | MAN | Metropolitan area network |
| #nf | PAN | Personal area network |
| #nf | SAN | Storage area network |



## Network Operations

Network operations cover the actions needed to protect a network and its associated organization. Two main risks are security and business.

| Domain | Concept | Elaboration |
|---|---|---|
| #no #ns | NDA | Nondisclosure Agreement |
| #no #ns | MOU | Memorandum of Understanding |
| #no #ns #nf | MSA | Multi-Source Agreement |

| | | |
|---|---|---|
| #no #ns | SLA | Service Level Agreement |
| #no #ns | BYOD | Bring Your Own Device |
| #no #ns | SOW | Statement of Work |
| #ns | Incident response | • Forensics<br>• First responder<br>• Secure the area<br>• Document the scene<br>• Collect evidence<br>• Chain of custody<br>• Forensics report<br>• Legal hold<br>• Electronic discovery (e-discovery) |
| #no | RPO | Recovery point objective |
| #no | RTO | Recovery time objective |
| #no | MTTR | Mean time to repair |
| #no | MTTF | Mean time to failure |
| #no | MTBF | Mean time between failures |
| #no | BCP | Business continuity plan |
| #no #nt | AUP | Acceptable use policy |
| #no #nt | MDM | Mobile Device Manager |
| #no #nt | COBO | Corporate-owned, business only |
| #no #nt | COPE | Corporate-owned, personally enabled |
| #no #nt | CYOD | Choose your own device |



## Protecting Networks

This is a vital section, especially if you intend to embark on a career in cyber security.

| Domain | Concept | Elaboration |
|---|---|---|
| #ns | CIA triad | Confidentiality, integrity, availability |
| #ns | Honeypot/honeynet | Individual/connected devices inviting attacks to capture information |
| #ns #nt | Rogue DHCP server | IP address is outside of the network ID |
| #ns | Screened subnet (demilitarized zone, DMZ) | Five components:<br>• External network<br>• External router<br>• Perimeter network<br>• Internal router<br>• Internal network |
| #ni #ns #nt | Man-in-the-middle (MITM)/on-path attack | Intercept a two-party conversation for one's advantage<br><br>Tools:<br>• Ettercap |

| | | |
|---|---|---|
| | | • Wireshark<br>• tcpdump |
| #ns | Spoofing | Digital misrepresentation<br>• MAC<br>• IP<br>• VLAN |
| #ni #ns | DTP | Cisco Dynamic Trunking Protocol |
| #ns | ITAD | IT asset disposal |
| #ns | DNS poisoning | Exploit known DNS vulnerabilities |
| #ns | URL hijacking/typosquatting | Target URL typos |
| #ns | Replay attack | Intercept data and replay later |
| #ns | Downgrade attack | Force a network channel to switch to an unprotected or less secure data transmission standard |
| #ns | Session hijacking | Seize control of a user's browsing session to gain access |
| #no #ns | Brute-force attack | Trying character combinations |
| #no #ns | Dictionary attack | Using lists of probable passwords |
| #ni #ns | VLAN hopping | Attacker can move from one VLAN to another |
| #ns | CVE | Common vulnerabilities and exposure: publicly disclosed list of security flaws |
| #ns | CNA | CVE Numbering Authority |
| #ns | Zero-day | Flaw discovered by third party sooner than vendor |
| #ni #ns | DAI | Cisco Dynamic ARP Inspection |
| #ni #ns | RA | Router Advertisement |
| #ni #ns | Control plane policing | Use QoS to stop Denial-of-Service attacks |
| #ni #nt #ns | Firewall | Filter for network traffic<br>- Hardware/software<br>- Stateful/stateless<br>- Network-based/host-based<br>- Context-/application-aware |
| #ni #nt | UTM | Unified threat management |
| #ni | ACL | Access control list |
| #ni | DPI | Deep-packet inspection |
| #ns | Virus | Run on a computer without the user's knowledge.<br><br>Examples: Boot Sector, Macro, Program, |

| | | |
|---|---|---|
| | | Polymorphic, Stealth, and Multipartite. |
| #ns | Worm | Replicate itself across a network |
| #ns | Trojan Horse | Perform useful functions superficially but runs malicious programs covertly |
| #ns | Spyware | Spy on a computer and record its activities.<br><br>Examples: keylogger and browser-hijacking adware |
| #ns | Rootkit | Gain administrator-level access to the system core undetected |
| #ns | Ransomware | Hold a computer hostage until the user pays |
| #ns | Adware | Unwanted software displaying advertisements |
| #ns | Remote Access Trojans (RATs) | Malware to remotely control an infected computer |
| #ns | Logic bomb | Start a malicious program upon fulfillment of certain logical conditions |
| #ns | Crypto-malware | Mine cryptocurrency that enriches perpetrators |
| #ns | Physical controls | • Deterrent:<br>  ○ Preventative<br>  ○ Detective<br>  ○ Corrective<br>• Recovery<br>• Compensating controls |



## Network Monitoring

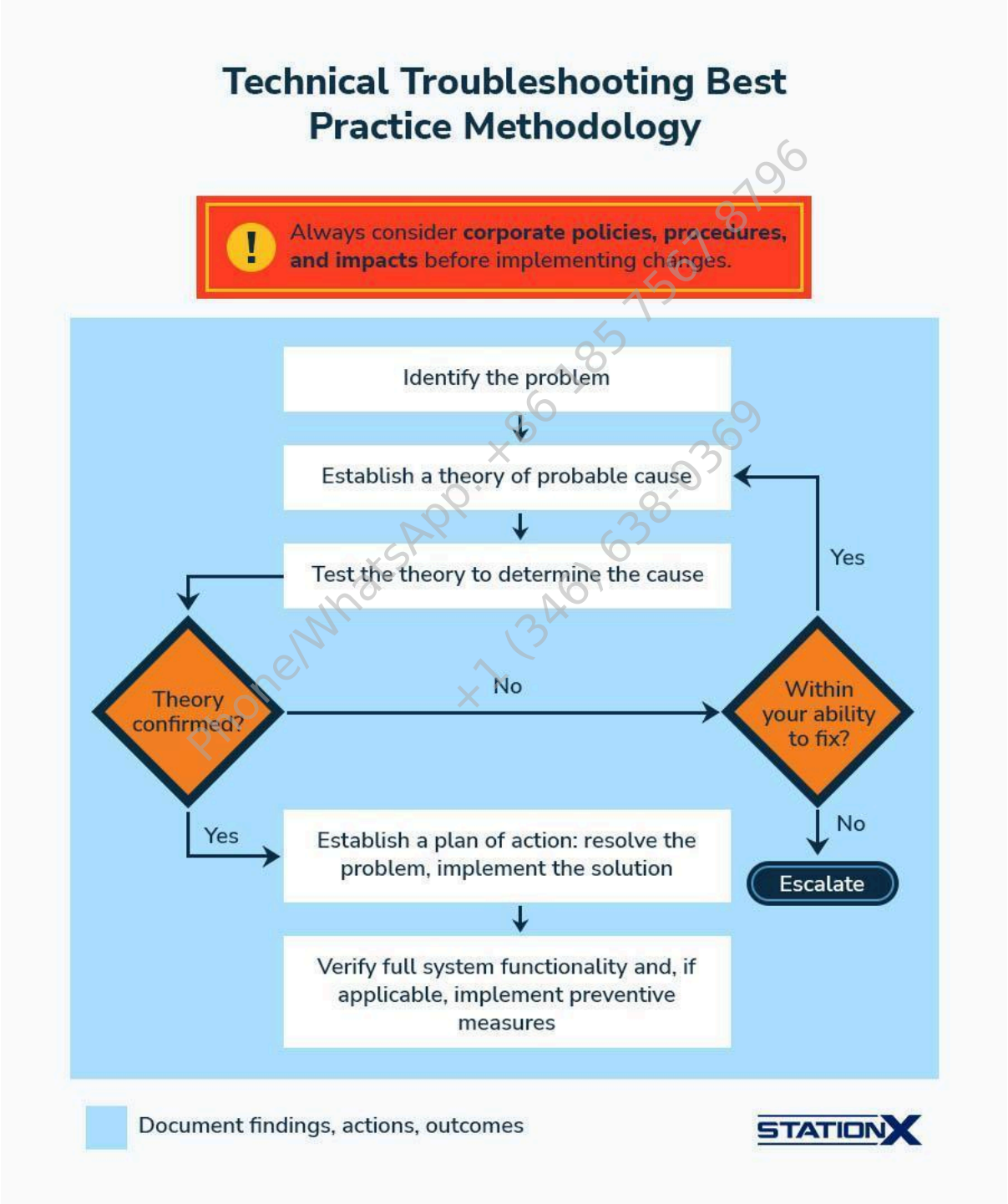
Monitoring a network helps nip problems in the bud.

| Domain | Concept | Elaboration |
|---|---|---|
| #ns | SIEM | Security Information and Event Management |
| #nf #no #ns | SNMP | Simple Network Management Protocol |
| #nf #no #ns | NMS | Network management system/station |
| #no | Event Viewer, Syslog | Tools to display logs |

# Network Troubleshooting

Apply the six technical troubleshooting steps (same as A+) to networking problems.

| Domain | Concept | Elaboration |
|---|---|---|
| #nt | Additional considerations on the “establish theory” step | - Top-to-bottom/bottom-to-top<br>- OSI model<br>- Divide and conquer |



Technical Troubleshooting Best Practice Methodology (borrowed from our A+ Cheat Sheet)

## Conclusion

We hope this quick review Network+ cheat sheet helps your learning or career journey. Check out our other articles on networking, strictly exam-related test taking tips, and Network+ accelerated certification training programs, which include supplemental sample tests and chapter-end test questions. No matter where you go next, we wish you all the best.