CompTIA Network+ Zertifizierungsprüfung – Ziele

PRÜFUNGSNUMMER: N10-009

Über die Prüfung

Durch die CompTIA Network+ Zertifizierungsprüfung wird zertifiziert, dass der erfolgreiche Teilnehmer über die folgenden erforderlichen Kenntnisse und Fähigkeiten verfügt:

- Netzwerkkonnektivität durch den Einsatz kabelgebundener und Wireless-Geräte herstellen.
- Nutzung und Pflege der Netzwerkdokumentation erklären.
- Allgemeine Netzwerkdienste konfigurieren.
- Grundlegende Konzepte für Rechenzentren, Clouds und Virtual Networking erklären.
- Aktivitäten im Netzwerk überwachen sowie Performance- und Verfügbarkeitsprobleme beheben.
- Techniken zur Härtung der Netzwerksicherheit implementieren.
- Netzwerk-Infrastruktur verwalten, konfigurieren und Fehler beheben.

PRÜFUNGSENTWICKLUNG

Die CompTIA Prüfungen ergeben sich aus Sachverständigen-Workshops und den Ergebnissen von branchenweiten Umfragen zu den von IT-Fachleuten geforderten Kenntnissen und Fertigkeiten.

CompTIA-RICHTLINIE ZUR NUTZUNG GENEHMIGTER MATERIALIEN

Die Verwendung von Inhalten, die von nicht autorisierten Schulungs-Websites von Drittanbietern (auch als „Braindumps“ bezeichnet) bereitgestellt werden, werden von CompTIA Certifications, LLC nicht genehmigt, befürwortet oder gebilligt. Personen, die solche Materialien zur Vorbereitung auf eine CompTIA-Prüfung nutzen, wird die Zertifizierung entzogen, und sie werden gemäß der CompTIA-Teilnehmervereinbarung von künftigen Prüfungen suspendiert. In dem Bemühen, die Prüfungsrichtlinien von CompTIA in Bezug auf die Verwendung nicht zugelassener Studienmaterialien klarer zu kommunizieren, verweist CompTIA alle Bewerber auf die CompTIA-Richtlinien zur Zertifizierungsprüfung. Bitte überprüfen Sie alle CompTIA-Richtlinien, bevor Sie mit dem Lernen für eine CompTIA-Prüfung beginnen. Die Bewerber müssen die CompTIA-Bewerber-Vereinbarung einhalten. Wenn ein Bewerber sich fragt, ob Lernmaterialien (bzw. „Merkzettel“) als nicht autorisiert betrachtet werden, sollte er sich zur Prüfung an CompTIA unter examsecurity@comptia.org wenden.

BITTE BEACHTEN

Die nachfolgend aufgeführten Beispiele sind keine vollständigen und endgültigen Listen. Andere Beispiele von Technologien, Prozessen oder Aufgaben, die sich auf die einzelnen Schulungsziele beziehen, können ebenfalls in die Prüfung aufgenommen werden, selbst wenn sie in diesem Dokument nicht aufgeführt sind. CompTIA überarbeitet den Inhalt der Prüfungen und aktualisiert Prüfungsfragen laufend, damit die Prüfungen auf dem neuesten Stand sind und die Sicherheit der Fragen gewahrt wird. Bei Bedarf veröffentlichen wir aktualisierte Prüfungen auf der Grundlage bestehender Prüfungsziele. Sie können sicher sein, dass alle zugehörigen Vorbereitungsmaterialien weiterhin gültig sind.

PRÜFUNGSDETAILS

Erforderliche Prüfung	N10-009
Anzahl der Fragen	Maximal 90
Fragentypen	Mehrfachauswahl und simulationsbasiert
Dauer der Prüfung	90 Minuten
Empfohlene Vorkenntnisse	Mindestens 9–12 Monate Erfahrung im Bereich IT-Netzwerke

PRÜFUNGSZIELE (WISSENSGEBIETE)

In der nachfolgenden Tabelle finden Sie die prüfungsrelevanten Wissensgebiete und deren Umfang in der Prüfung.

WISSENSGEBIET		PROZENTUALER ANTEIL AN DER PRÜFUNG
1.0	Netzwerkkonzepte	23 %
2.0	Netzwerkimplementierung	20 %
3.0	Netzwerkbetrieb	19 %
4.0	Netzwerksicherheit	14 %
5.0	Netzwerkfehlerbehebung	24 %
Insgesamt		**100 %**

1.0 Netzwerkkonzepte

1.1 Konzepte im Zusammenhang mit dem OSI-Referenzmodell (Open Systems Interconnection) erklären.

- Schicht 1 – Bitübertragungsschicht
- Schicht 2 – Datenverbindungsschicht
- Schicht 3 – Vermittlungsschicht
- Schicht 4 – Transportschicht
- Schicht 5 – Sitzungsschicht
- Schicht 6 – Darstellungsschicht
- Schicht 7 – Anwendungsschicht

1.2 Netzwerkgeräte, Anwendungen und Funktionen vergleichen und gegenüberstellen.

- Physische und virtuelle Geräte
  - Router
  - Switch
  - Firewall
  - Intrusion Detection System (IDS)/ Intrusion Prevention System (IPS)
  - Load Balancer
  - Proxy
  - Network Attached Storage (NAS)
  - Storage Area Network (SAN)
  - Wireless
    - Access Point (AP)
    - Controller
- Anwendungen
  - Content Delivery Network (CDN)
- Funktionen
  - Virtual Private Network (VPN)
  - Quality of Service (QoS)
  - Time to live (TTL)

1.3 Cloud-Konzepte und Konnektivitätsoptionen zusammenfassen.

- Network Functions Virtualization (NFV)
- Virtual Private Cloud (VPC)
- Netzwerk-Sicherheitsgruppen
- Netzwerk-Sicherheitslisten
- Cloud-Gateways
  - Internet-Gateway
  - Network-Address-Translation (NAT)-Gateway
- Cloud-Konnektivitätsoptionen
  - VPN
  - Direkte Verbindung
- Bereitstellungsmodelle
  - Öffentlich
  - Privat
  - Hybrid
- Service-Modelle
  - Software-as-a-Service (SaaS)
  - Infrastructure-as-a-Service (IaaS)
  - Platform-as-a-Service (PaaS)
- Skalierbarkeit
- Anpassbarkeit
- Mandantenfähige Systeme / Software-Instanzen

1.4 Gängige Netzwerk-Ports, Protokolle, Dienste und Traffic-Typen erklären.

Protokolle	Ports
File Transfer Protocol (FTP)	20/21
Secure File Transfer Protocol (SFTP)	22
Secure Shell (SSH)	22
Telnet	23
Simple Mail Transfer Protocol (SMTP)	25
Domain Name System (DNS)	53
Dynamic Host Configuration Protocol (DHCP)	67/68
Trivial File Transfer Protocol (TFTP)	69
Hypertext Transfer Protocol (HTTP)	80
Network Time Protocol (NTP)	123
Simple Network Management Protocol (SNMP)	161/162
Lightweight Directory Access Protocol (LDAP)	389
Hypertext Transfer Protocol Secure (HTTPS)	443
Server Message Block (SMB)	445
Syslog	514
Simple Mail Transfer Protocol Secure (SMTPS)	587
Lightweight Directory Access Protocol over SSL (LDAPS)	636
Structured Query Language (SQL) Server	1433
Remote Desktop Protocol (RDP)	3389
Session Initiation Protocol (SIP)	5060/5061

- Internet-Protocol-(IP)-Typen
  - Internet Control Message Protocol (ICMP)
  - Transmission Control Protocol (TCP)
  - User Datagram Protocol (UDP)
  - Generic Routing Encapsulation (GRE)
  - Internet Protocol Security (IPSec)
    - Authentication Header (AH)
    - Encapsulating Security Payload (ESP)
    - Internet Key Exchange (IKE)
- Traffic-Typen
  - Unicast
  - Multicast
  - Anycast
  - Broadcast

1.5 Übertragungsmedien und Transceiver vergleichen und gegenüberstellen.

- Wireless
  - 802.11-Standards
  - Mobilfunk
  - Satellit
- Kabelgebunden
  - 802.3-Standards
  - Single-mode vs. Multimode-Glasfaser
  - Direct Attach Copper (DAC)-Kabel
    - Twinaxial-Kabel
  - Koaxialkabel
  - Kabel-Geschwindigkeiten
  - Plenum vs. Nicht-Plenum-Kabel
- Transceiver
  - Protokoll
    - Ethernet
    - Fibre Channel (FC)
  - Formfaktoren
    - Small form-factor pluggable (SFP)
    - Quad small form-factor pluggable (QSFP)
- Steckertypen
  - Subscriber Connector (SC)
  - Local Connector (LC)
  - Straight Tip (ST)
  - Multi-fiber push on (MPO)
  - Registered jack (RJ)11
  - RJ45
  - F-type
  - Bayonet Neill-Concelman (BNC)

1.6 Netzwerk-Topologien, -Architekturen und -Typen vergleichen und gegenüberstellen.

- Mesh
- Hybrid
- Star / Hub-and-Spoke
- Spine and leaf
- Punkt-zu-Punkt
- Dreistufiges hierarchisches Modell
  - Core
  - Distribution
  - Access
- Collapsed Core
- Traffic-Flows
  - Nord-Süd
  - Ost-West

1.7 In einem gegebenen Szenario eine geeignete IPv4-Netzwerk-Adressierung verwenden.

- Öffentliche vs. private Adressen
  - Automatic Private IP Addressing (APIPA)
  - RFC1918
  - Loopback/Localhost
- Subnetze
  - Variable Length Subnet Mask (VLSM)
  - Classless Inter-domain Routing (CIDR)
- IPv4-Adressklassen
  - Klasse A
  - Klasse B
  - Klasse C
  - Klasse D
  - Klasse E

1.8 Aufkommende Anwendungsfälle für moderne Netzwerkumgebungen zusammenfassen.

- Software-Defined Network (SDN) Und Software-Defined Wide Area Network (SD-WAN)
  - Anwendungsbewusst
  - Zero-Touch-Bereitstellung
  - Transportagnostisch
  - Zentrales Richtlinienmanagement
- Virtual Extensible Local Area Network (VXLAN)
  - Datacenter interconnect (DCI)
  - Schicht-2-Verkapselung
- Zero trust architecture (ZTA)
  - Richtlinienbasierte Authentifizierung
  - Autorisierung
  - Prinzip der geringsten Zugangsrechte
- Secure Access Secure Edge (SASE)/ Security Service Edge (SSE)
- Infrastructure as Code (IaC)
  - Automatisierung
    - Playbooks/Vorlagen/ wiederverwendbare Aufgaben
    - Konfigurationsabweichung/ Compliance
    - Upgrades
    - Dynamic Inventories
  - Quellenkontrolle
    - Versionskontrolle
    - Zentrales Repository
    - Identifizierung von Konflikten
    - Abzweigungen / Branching
- IPv6-Adressierung
  - Abmilderung der Adresserschöpfung
  - Kompatibilitätsanforderungen
    - Tunneling
    - Dual Stack
    - NAT64

2.0 Netzwerkimplementierung

2.1 Die Merkmale von Routing-Technologien erklären.

- Statisches Routing
- Dynamisches Routing
  - Border Gateway Protocol (BGP)
  - Enhanced Interior Gateway Routing Protocol (EIGRP)
  - Open Shortest Path First (OSPF)
- Routenauswahl
  - Administrative Distanz
  - Präfixlänge
  - Metrik
- Address Translation
  - NAT
  - Port address translation (PAT)
- First Hop Redundancy Protocol (FHRP)
- Virtual IP (VIP)
- Sub-Interfaces

2.2 In einem gegebenen Szenario Switching-Technologien und -Funktionen konfigurieren.

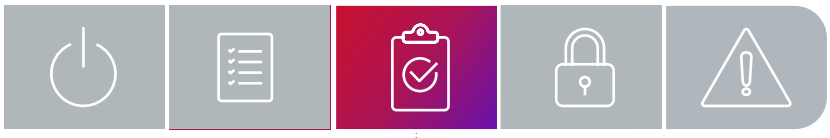
- Virtual Local Area Network (VLAN)
  - VLAN-Datenbank
  - Switch Virtual Interface (SVI)
- Interface-Konfiguration
  - Natives VLAN
  - Voice VLAN
  - 802.1Q-Tagging
  - Link-Aggregation
  - Geschwindigkeit
  - Duplex
- Spanning Tree
- Maximum Transmission Unit (MTU)
  - Jumbo-Frames

2.3 In einem gegebenen Szenario Wireless-Geräte und -Technologien auswählen und konfigurieren.

- Kanäle
  - Kanalbreite
  - Nicht überlappende Kanäle
  - Regulatorische Auswirkungen
    - 802.11h
- Frequenzoptionen
  - 2,4 GHz
  - 5 GHz
  - 6 GHz
  - Bandsteuerung
- Service Set Identifier (SSID)
  - Basic Service Set Identifier (BSSID)
  - Extended Service Set Identifier (ESSID)
- Netzwerktypen
  - Mesh-Netzwerke
  - Ad hoc
  - Punkt zu Punkt
  - Infrastruktur
- Verschlüsselung
  - Wi-Fi Protected Access 2 (WPA2)
  - WPA3
- Gastnetzwerke
  - Captive-Portale
- Authentifizierung
  - Pre-shared key (PSK) vs. Enterprise
- Antennen
  - Omnidirektional vs. direktional
- Autonomer vs. lightweight Access Point

2.4 Wichtige Faktoren physischer Installationen erklären.

- **Wichtige Faktoren für die Installation**
  - Standorte
    - Intermediate Distribution Frame (IDF)
    - Main Distribution Frame (MDF)
  - Rack-Größe
  - Auslass/Einlass auf der Port-Seite
  - Verkabelung
    - Patchfeld
    - Glasfaser-Patchfeld/Steckfeld
  - Abschließbar
- **Stromversorgung**
  - Unterbrechungsfreie Stromversorgung (USV)
  - Power Distribution Unit (PDU)
  - Leistungsaufnahme
  - Spannung
- **Umweltfaktoren**
  - Feuchtigkeit
  - Brandschutzeinrichtung
  - Temperatur



3.0 Netzwerkbetrieb

3.1 Den Zweck organisatorischer Prozesse und Verfahren erläutern.

- **Dokumentation**
  - Physikalische vs. logische Diagramme
  - Rack-Diagramme
  - Kabelpläne und Diagramme
  - Netzwerkdiagramme
    - Schicht 1
    - Schicht 2
    - Schicht 3
  - Asset-Bestand
    - Hardware
    - Software
    - Lizensierung
    - Garantie-Support
  - IP Address Management (IPAM)
  - Service-Level-Agreement (SLA)
  - Wireless-Vermessung/Heatmap
- **Lebenszyklusmanagement**
  - End-of-life (EOL)
  - End-of-support (EOS)
  - Software-Verwaltung
    - Patches und Bug Fixes
    - Betriebssystem (OS)
    - Firmware
  - Außerbetriebnahme
- **Change-Management**
  - Prozessverfolgung/ Serviceanfrage
- **Konfigurationsmanagement**
  - Produktionskonfiguration
  - Backup-Konfiguration
  - Baseline-/goldene Konfiguration

3.2 In einem gegebenen Szenario Netzwerk-Überwachungstechnologien einsetzen.

- **Methoden**
  - SNMP
    - Traps
    - Management Information Base (MIB)
    - Versionen
      - v2c
      - v3
    - Community-Strings
    - Authentifizierung
  - Flow-Daten
  - Paketerfassung
  - Baseline-Kennzahlen
    - Alarmierung/ Benachrichtigung bei Anomalien
  - Protokoll-Aggregation
    - Syslog-Collector
    - Security information and Event Management (SIEM)
  - Application Programming Interface (API)-integration
  - Portspiegelung
- **Lösungen**
  - Netzwerkerkennung
    - Ad hoc
    - Geplant
  - Traffic-Analyse
  - Leistungsüberwachung
  - Verfügbarkeitsüberwachung
  - Konfigurationsüberwachung

3.3 Konzepte der Notfallwiederherstellung (Disaster Recovery – DR) erklären.

- DR-Kennzahlen
  - Recovery-Point-Objective (RPO)
  - Recovery-Time-Objective (RTO)
  - Mean-Time-to-Repair (MTTR)
  - Mean-Time-between-Failure (MTBF)
- DR-Sites
  - Cold Site
  - Warm Site
  - Hot Site
- Ansätze für hohe Verfügbarkeit
  - Aktiv-aktiv
  - Aktiv-passiv
- Tests
  - Tabletop-Übungen
  - Validierungstests

3.4 In einem gegebenen Szenario IPv4- und IPv6-Netzwerkdienste implementieren.

- Dynamische Adressierung
  - DHCP
    - Reservierungen
    - Bereiche
    - Lease-Time
    - Optionen
    - Relay/IP Helper
    - Exklusionen
  - Stateless Address Autoconfiguration (SLAAC)
- Namensauflösung
  - DNS
    - Domain Name System Security Extensions (DNSSEC)
    - DNS over HTTPS (DoH) und DNS over TLS (DoT)
    - Eintragstypen
      - Adresse (A)
      - AAAA
      - Canonical Name (CNAME)
      - Mail Exchange (MX)
      - Text (TXT)
      - Nameserver (NS)
      - Pointer (PTR)
    - Zonen-Typen
      - Forward
      - Reverse
    - Autoritativ vs. nicht autoritativ
    - Primär vs. sekundär
    - Rekursiv
  - Hosts-Datei
- Zeitprotokolle
  - NTP
  - Precision Time Protocol (PTP)
  - Network Time Security (NTS)

3.5 Methoden des Netzwerkzugriffs und der Netzwerkverwaltung vergleichen und gegenüberstellen.

- Site-to-Site-VPN
- Client-to-Site-VPN
  - Ohne Client
  - Split Tunnel vs. Full Tunnel
- Verbindungsmethoden
  - SSH
  - Graphical User Interface (GUI)
  - API
  - Konsole
- Jump-Box/Host
- In-Band- vs. Out-of-Band-Verwaltung

4.0 Netzwerksicherheit

4.1 Die Bedeutung grundlegender Netzwerk-Sicherheitskonzepte erklären.

- **Logische Sicherheit**
  - Verschlüsselung
    - Daten im Transit
    - Verschlüsselung der ruhenden Daten / Data at rest
  - Zertifikate
    - Public Key Infrastructure (PKI)
    - Selbstsigniert
  - Identity and Access Management (IAM)
    - Authentifizierung
      - Multifaktor-Authentifizierung (MFA)
      - Single-Sign-On (SSO)
      - Remote Authentication Dial-In User Service (RADIUS)
      - LDAP
      - Security Assertion Markup Language (SAML)
      - Terminal Access Controller Access Control System Plus (TACACS+)
      - Zeitbasierte Authentifizierung
    - Autorisierung
      - Prinzip der geringsten Rechte
      - Regelbasierte Zugriffskontrolle
  - Geofencing
- **Physische Sicherheit**
  - Kamera
  - Schlösser
- **Täuschungstechnologien**
  - Honeypot
  - Honeynet
- **Allgemeine Sicherheitsterminologie**
  - Risiko
  - Schwachstelle
  - Exploit
  - Bedrohung
  - Die Triade „Confidentiality, Integrity, and Availability“ (CIA – Vertraulichkeit, Integrität und Verfügbarkeit)
- **Audits und Einhaltung von Vorschriften**
  - Datenstandort
  - Payment Card Industry Data Security Standards (PCI DSS)
  - Datenschutz-Grundverordnung (DSGVO)
- **Durchsetzung der Netzsegmentierung**
  - Internet of Things (IoT) und Industrial Internet of Things (IIoT)
  - Supervisory Control and Data Acquisition (SCADA), Industrial Control System (ICS), Operational Technology (OT)
  - Gast
  - Bring Your Own Device (BYOD)

4.2 Verschiedene Angriffstypen und ihre Auswirkungen auf das Netzwerk zusammenfassen.

- **Denial of Service (DoS)/Distributed Denial of Service (DDoS)**
- **VLAN-Hopping**
- **Media Access Control (MAC)-Flooding**
- **Address Resolution Protocol (ARP)-Poisoning**
- **ARP-Spoofing**
- **DNS-Poisoning**
- **DNS-Spoofing**
- **Betrügerische Geräte und Dienste**
  - DHCP
  - AP
- **Evil Twin**
- **On-Path-Angriff**
- **Social Engineering**
  - Phishing
  - Dumpster Diving
  - Shoulder Surfing
  - Tailgating
- **Malware**

4.3 In einem gegebenen Szenario Netzwerksicherheitsfunktionen, Sicherheitsmaßnahmen und Lösungen anwenden.

- **Geräte härten**
  - Ungenutzte Ports und Dienste deaktivieren
  - Standardpasswörter ändern
- **Network Access Control (NAC)**
  - Port-Sicherheit
  - 802.1X
  - MAC-Filter
- **Schlüssel-Verwaltung**
- **Sicherheitsregeln**
  - Access Control List (ACL)
  - Uniform-Resource-Locator(URL)-Filterung
  - Inhaltsfilterung
- **Zonen**
  - Vertrauenswürdig vs. nicht vertrauenswürdig
  - Sicherheitsüberwachtes Subnetz

5.0 Netzwerkfehlerbehebung

5.1 Die Methodik der Fehlerbehebung erklären.

- **Das Problem identifizieren**
  - Informationen sammeln
  - Nutzer befragen
  - Symptome identifizieren
  - Mögliche Veränderungen feststellen
  - Wenn möglich, das Problem nachstellen
  - An mehrere Probleme einzeln herangehen
- **Eine Theorie über die wahrscheinliche Ursache erstellen**
  - Offensichtliches hinterfragen
  - Mehrere Herangehensweisen erwägen
    - Top-to-Bottom/Bottom-to-Top OSI-Modell
    - Teile und herrsche
- **Die Theorie testen, um die Ursache zu bestimmen**
  - Nach Bestätigung der Theorie die nächsten Schritte zur Problembehebung festlegen
  - Falls sich die Theorie nicht bestätigt, neue Theorie aufstellen oder eskalieren
- **Aktionsplan zur Lösung des Problems aufstellen und mögliche Auswirkungen bestimmen**
- **Die Lösung umsetzen oder das Problem gegebenenfalls melden**
- **Ggf. vollständige Systemfunktionalität prüfen und präventive Maßnahmen ergreifen**
- **Erkenntnisse, Aktionen, Ergebnisse und gelernte Lektionen während des gesamten Prozesses dokumentieren.**

5.2 In einem gegebenen Szenario gängige Probleme mit der Verkabelung und der physischen Schnittstelle beheben.

- **Kabelprobleme**
  - Falsches Kabel
    - Singlemodus vs. Multimodus
    - Kategorie 5/6/7/8
    - Shielded Twisted Pair (STP) vs. Unshielded Twisted air (UTP)
  - Degradation des Signals
    - Überlagerung
    - Interferenz
    - Abschwächung
  - Unsachgemäße Terminierung
  - Transmitter (TX)/Receiver (RX) vertauscht
- **Schnittstellenprobleme**
  - Erhöhen von Schnittstellenzählern
    - Cyclic Redundancy Check (CRC)
    - Runt-Pakete
    - Giant-Pakete
    - Drop-Pakete
  - Port-Status
    - Fehler deaktiviert
    - Administrativ deaktiviert
    - Ausgesetzt
- **Hardwareprobleme**
  - Power over Ethernet (PoE)
    - Leistungsbudget überschritten
    - Falscher Standard
  - Transceiver
    - Mismatch
    - Signalstärke

5.3 In einem gegebenen Szenario allgemeine Probleme mit Netzwerkdiensten beheben.

- **Switching-Probleme**
  - STP
    - Netzwerk-Loops
    - Auswahl der Root Bridge
    - Port-Rollen
    - Port-Status
  - Falsche VLAN-Zuweisung
  - ACLs
- **Routenauswahl**
  - Routing-Tabelle
  - Standardrouten
- **Erschöpfung des Adressvorrats**
- **Falscher Standard-Gateway**
- **Falsche IP-Adresse**
  - Doppelte IP-Adresse
- **Falsche Subnetzmaske**

5.4 In einem gegebenen Szenario gängige Performance-Probleme beheben.

- **Datenstau / Bottleneck**
- **Engpässe**
- **Bandbreite**
  - Durchsatzleistung
- **Latenz**
- **Paketverlust**
- **Jitter**
- **Wireless**
  - Interferenz
    - Kanalüberlappung
  - Verschlechterung oder Verlust des Signals
  - Unzureichende Funkabdeckung
  - Abgrenzungsprobleme der Kunden
  - Falsche Roaming-Konfiguration

5.5 In einem gegebenen Szenario das passende Tool oder Protokoll zur Lösung von Netzwerkfehlern anwenden.

- **Softwaretools**
  - Protokoll-Analysator
  - Kommandozeile
    - ping
    - traceroute/tracert
    - nslookup
    - tcpdump
    - dig
    - netstat
    - ip/ifconfig/ipconfig
    - arp
  - Nmap
  - Link Layer Discovery Protocol (LLDP)/Cisco Discovery Protocol (CDP)
  - Geschwindigkeitstester
- **Hardwaretools**
  - Toner
  - Kabeltester
  - Network TAP (Test Access Point)
  - Wi-Fi-Analysator
  - Visuelle Fehlersuche
- **Grundlegende Befehle für Netzwerkgeräte**
  - MAC-Adresstabelle anzeigen
  - Route anzeigen
  - Schnittstelle anzeigen
  - Konfiguration anzeigen
  - ARP anzeigen
  - VLAN anzeigen
  - Leistung zeigen

CompTIA Network+ N10-009 Abkürzungsliste

Es folgt eine Liste von Abkürzungen, die in den CompTIA Network+ N10-009-Prüfungen vorkommen. Teilnehmer sind aufgefordert, die komplette Liste durchzugehen und sich Arbeitskenntnisse aller aufgeführten Akronyme als Teil des umfassenden Prüfungsvorbereitungsprogramms zu erwerben.

ABKÜRZUNG	BEDEUTUNG
A	Address
ACL	Access Control List
AH	Authentication Header
AP	Access Point
API	Application Programming Interface
APIPA	Automatic Private Internet Protocol Addressing
ARP	Address Resolution Protocol
AUP	Acceptable Use Policy
BGP	Border Gateway Protocol
BNC	Bayonet Neill–Concelman
BSSID	Basic Service Set Identifier
BYOD	Bring Your Own Device
CAM	Content-addressable Memory
CDN	Content Delivery Network
CDP	Cisco Discovery Protocol
CIA	Confidentiality, Integrity, and Availability
CIDR	Classless Inter-domain Routing
CLI	Command-line Interface
CNAME	Canonical Name
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
DAC	Direct Attach Copper
DAS	Direct-attached Storage
DCI	Data Center Interconnect
DDoS	Distributed Denial-of-service
DHCP	Dynamic Host Configuration Protocol
DLP	Data Loss Prevention
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
DoH	DNS over Hypertext Transfer Protocol Secure
DoS	Denial-of-service
DoT	DNS over Transport Layer Security
DR	Disaster Recovery
EAPoL	Extensible Authentication Protocol over LAN
EIGRP	Enhanced Interior Gateway Routing Protocol
EOL	End-of-life
EOS	End-of-support

ABKÜRZUNG	BEDEUTUNG
ESP	Encapsulating Security Payload
ESSID	Extended Service Set Identifier
EULA	End User License Agreement
FC	Fibre Channel
FHRP	First Hop Redundancy Protocol
FTP	File Transfer Protocol
GDPR	General Data Protection Regulation
GRE	Generic Routing Encapsulation
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IaaS	Infrastructure as a Service
IaC	Infrastructure as Code
IAM	Identity and Access Management
ICMP	Internet Control Message Protocol
ICS	Industrial Control System
IDF	Intermediate Distribution Frame
IDS	Intrusion Detection System
IoT	Internet of Things
IIoT	Industrial Internet of Things
IKE	Internet Key Exchange
IP	Internet Protocol
IPAM	Internet Protocol Address Management
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security
IS-IS	Intermediate System to Intermediate System
LACP	Link Aggregation Control Protocol
LAN	Local Area Network
LC	Local Connector
LDAP	Lightweight Directory Access Protocol
LDAPS	Lightweight Directory Access Protocol over SSL
LLDP	Link Layer Discovery Protocol
MAC	Media Access Control
MDF	Main Distribution Frame
MDIX	Medium Dependent Interface Crossover
MFA	Multifactor Authentication
MIB	Management Information Base
MPO	Multifiber Push On
MTBF	Mean Time Between Failure
MTTR	Mean Time To Repair
MTU	Maximum Transmission Unit
MX	Mail Exchange
NAC	Network Access Control
NAS	Network-attached Storage
NAT	Network Address Translation
NFV	Network Functions Virtualization
NIC	Network Interface Cards
NS	Name Server
NTP	Network Time Protocol
NTS	Network Time Security
OS	Operating System
OSPF	Open Shortest Path First
OSI	Open Systems Interconnection
OT	Operational Technology
PaaS	Platform as a Service

ABKÜRZUNG	BEDEUTUNG
PAT	Port Address Translation
PCI DSS	Payment Card Industry Data Security Standards
PDU	Power Distribution Unit
PKI	Public Key Infrastructure
PoE	Power over Ethernet
PSK	Pre-shared Key
PTP	Precision Time Protocol
PTR	Pointer
QoS	Quality of Service
QSFP	Quad Small Form-factor Pluggable
RADIUS	Remote Authentication Dial-in User Service
RDP	Remote Desktop Protocol
RFID	Radio Frequency Identifier
RIP	Routing Information Protocol
RJ	Registered Jack
RPO	Recovery Point Objective
RSTP	Rapid Spanning Tree Protocol
RTO	Recovery Time Objective
RX	Receiver
SaaS	Software as a Service
SAML	Security Assertion Markup Language
SAN	Storage Area Network
SASE	Secure Access Service Edge
SC	Subscriber Connector
SCADA	Supervisory Control and Data Acquisition
SDN	Software-defined Network
SD-WAN	Software-defined Wide Area Network
SFP	Small Form-factor Pluggable
SFTP	Secure File Transfer Protocol
SIP	Session Initiation Protocol
SIEM	Security Information and Event Management
SLA	Service-level Agreement
SLAAC	Stateless Address Autoconfiguration
SMB	Server Message Block
SMTP	Simple Mail Transfer Protocol
SMTPS	Simple Mail Transfer Protocol Secure
SNMP	Simple Network Management Protocol
SOA	Start of Authority
SQL	Structured Query Language
SSE	Security Service Edge
SSH	Secure Shell
SSID	Service Set Identifier
SSL	Secure Socket Layer
SSO	Single Sign-on
ST	Straight Tip
STP	Shielded Twisted Pair
SVI	Switch Virtual Interface
TACAS+	Terminal Access Controller Access Control System Plus
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TTL	Time to Live
TX	Transmitter
TXT	Text
UDP	User Datagram Protocol
UPS	Uninterruptible Power Supply

ABKÜRZUNG	BEDEUTUNG
URL	Uniform Resource Locator
USB	Universal Serial Bus
UTM	Unified Threat Management
UTP	Unshielded Twisted Pair
VIP	Virtual IP
VLAN	Virtual Local Area Network
VLSM	Variable Length Subnet Mask
VoIP	Voice over IP
VPC	Virtual Private Cloud
VPN	Virtual Private Network
WAN	Wide Area Network
WPA	Wi-Fi Protected Access
WPS	Wi-Fi Protected Setup
VXLAN	Virtual Extensible LAN
ZTA	Zero Trust Architecture

CompTIA Network+ Vorgeschlagene Hardware-und Software-Liste

CompTIA führt hier einige Hardware- und Software-Beispiele auf, welche die Teilnehmer bei der Vorbereitung auf die Network+ Prüfung unterstützen sollen. Diese Liste ist möglicherweise auch für Schulungsfirmen von Nutzen, die ihrem Schulungsangebot eine praktische Komponente hinzufügen möchten. Die Aufzählungen unter den jeweiligen Themen haben nur Beispielcharakter und erheben keinen Anspruch auf Vollständigkeit.

Ausstattung

- Optische und Kupferpatchfelder
- Layer-3-Switch/Managed Switch/ PoE-Switch
- Router
- Firewall
- Wireless Access Point
- Einfache Laptops mit Virtualisierungs-Support
- Voice-over-IP(VoIP)-Telefon

Zusätzliche Hardware

- Netzwerkkarte (NIC)
- Netzteile
- SFPs
- Wireless Access Point
- USV
- PoE-Injektor

Ersatzteile

- Patchkabel
  - Glasfaser
  - Kupfer
- Antennen
- Bluetooth/Wireless-Adapter
- Konsolenkabel [Universal Serial Bus (USB) auf seriellen Adapter RS-232]
- Zusatz-NIC/-USB-NIC

Werkzeuge

- Kabeltester
- Kabelsuch- und Testgerät
- Optisches Leistungsmessgerät
- PoE-Tester

Software

- Protokollanalysator/ Paketaufzeichnung
- Terminalemulationssoftware
- Linux-/Windows-Betriebssysteme
- Software-Firewall
- Software-IDS/-IPS
- Netzwerkmapper
- Hypervisor-Software
- IaaS-Cloud-Lab-/Demo-Konten
- Virtuelle Netzwerkumgebung
- Wi-Fi-Analysator
- Spektrumanalysator
- Netzwerk-Überwachungstools
- Flow-Datenanalysator
- TFTP-Server
- Verschiedene Firmware-Versionen

Sonstiges

- Beispiel einer Netzwerkdokumentation
- Beispiel-Logs
- Defekte Kabel
- Cloud-Netzwerkdiagramme
- Beispielkonfiguration – Playbook/Runbook

CompTIA