CompTIA Network+ Zertifizierungsprüfung Prüfungsziele

PRÜFUNGSNUMMER: N10-008

CompTIA

Über die Prüfung

Die Bewerber werden aufgefordert, dieses Dokument zur Vorbereitung auf die CompTIA Network+ (N10-008) Zertifizierungsprüfung zu verwenden. Durch die CompTIA Network+ Zertifizierungsprüfung wird bestätigt, dass der erfolgreiche Teilnehmer über die folgenden erforderlichen Kenntnisse und Fähigkeiten verfügt:

- **Netzwerkkonnektivität durch den Einsatz kabelgebundener und kabelloser Geräte herstellen**
- **Netzwerkdokumentation verstehen und pflegen**
- **Zweck von Netzwerkdiensten verstehen**
- **Grundlegende Konzepte für Rechenzentren, Clouds und virtuelle Netzwerke verstehen**
- **Netzwerkaktivität überwachen, Leistungs- und Verfügbarkeitsprobleme erkennen**
- **Maßnahmen zur Erhöhung der Netzwerksicherheit anwenden**
- **Netzwerkinfrastruktur verwalten, konfigurieren und Fehler suchen**

Dieser Nachweis entspricht 9 bis 12 Monaten Praxiserfahrung in einer Position als Junior-Netzwerkadministrator/Netzwerk-Support-Techniker. Diese inhaltlichen Beispiele dienen der Verdeutlichung der Prüfungsziele und sind nicht als umfassende Auflistung aller Inhalte dieser Prüfung zu verstehen.

PRÜFUNGSAKKREDITIERUNG

Die Prüfung CompTIA Network+ (N10-008) ist vom US-Normungsinstitut ANSI für die Einhaltung der ISO-Norm 17024 akkreditiert und unterliegt somit regelmäßigen Prüfungen und Aktualisierungen der Prüfungsziele.

PRÜFUNGSENTWICKLUNG

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

CompTIA-RICHTLINIE ZUR NUTZUNG GENEHMIGTER MATERIALIEN

CompTIA Certifications, LLC genehmigt, befürwortet und billigt nicht die Verwendung von Inhalten, die von nicht autorisierten Schulungswebsites von Drittanbietern (auch „Braindumps“ genannt) bereitgestellt werden. 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. Zur klareren Kommunikation der Prüfungsrichtlinien von CompTIA zur Nutzung von ungenehmigten Studienmaterialien verweist CompTIA alle Zertifizierungsteilnehmer auf die **Zertifizierungsprüfungsrichtlinie von CompTIA**. Lesen Sie alle CompTIA-Richtlinien, bevor Sie mit dem Studium zur Vorbereitung auf eine der CompTIA-Prüfungen beginnen. Die Kandidaten müssen die **CompTIA Bewerber-Vereinbarung** einhalten. Wenn ein Teilnehmer eine Frage dazu hat, ob Studienmaterialien als ungenehmigt (Braindumps) angesehen werden, sollte er CompTIA unter **examsecurity@comptia.org** kontaktieren.

BEACHTEN SIE

Die aufgeführten Beispiele in Stichpunkten sind keine vollständigen 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 ihrer Prüfungen und aktualisiert die Prüfungsfragen ständig, damit ihre Prüfungen auf dem neuesten Stand sind und die Sicherheit der Fragen gewahrt wird. Bei Bedarf veröffentlichen wir aktualisierte Prüfungen auf Grundlage bestehender Prüfungsziele. Sie können sicher sein, dass alle zugehörigen Vorbereitungsmaterialien weiterhin gültig sind.

PRÜFUNGSDETAILS

Erforderliche Prüfung	N10-008
Anzahl der Fragen	Maximal 90
Arten der Fragen	Multiple-Choice und leistungsbasierte Simulationen
Dauer der Prüfung	90 Minuten
Empfohlene Vorerfahrung	• CompTIA A+ Zertifizierung oder entsprechende Kenntnisse • Mind. 9 bis 12 Monate Praxiserfahrung in einer Position als Junior-Netzwerkadministrator/ Netzwerk-Support-Techniker
Notwendige Punktzahl:	720 (auf einer Skala von 100–900)

PRÜFUNGSZIELE (GEBIETE)

In der nachfolgenden Tabelle finden Sie die prüfungsrelevanten Wissensgebiete und den Umfang, in dem diese in der Prüfung enthalten sind.

WISSENSGEBIET	PROZENTUALER ANTEIL AN DER PRÜFUNG
1.0 Netzwerkgrundlagen	24 %
2.0 Netzwerkimplementierung	19 %
3.0 Netzwerkbetrieb	16 %
4.0 Netzwerksicherheit	19 %
5.0 Netzwerkproblembehebung	22 %
Insgesamt	**100 %**

1.0 Netzwerkgrundlagen

1.1 Schichten des OSI-Modells und Kapselungskonzepts vergleichen und gegenüberstellen

- **OSI-Modell**
  - Schicht 1 – Bitübertragungsschicht
  - Schicht 2 – Sicherungsschicht
  - Schicht 3 – Vermittlungsschicht
  - Schicht 4 – Transportschicht
  - Schicht 5 – Sitzungsschicht
  - Schicht 6 – Darstellungsschicht
  - Schicht 7 – Anwendungsschicht
- **Datenkapselung und Entkapselung im OSI-Modell-Kontext**
  - Ethernet-Header
  - Internet-Protocol-(IP-) Header
  - Transmission-Control-Protocol-(TCP-)/ User-Datagram-Protocol-(UDP-) Header
  - TCP-Flags
  - Payload
  - Maximum Transmission Unit (MTU)

1.2 Merkmale von Netzwerktopologien und Netzwerktypen erläutern

- **Netz**
- **Stern/Hub-and-Spoke**
- **Bus**
- **Ring**
- **Hybrid**
- **Netzwerktypen und -merkmale**
  - Peer-to-Peer
  - Client-Server
  - Local area network (LAN)
  - Metropolitan area network (MAN)
  - Wide area network (WAN)
  - Wireless local area network (WLAN)
  - Personal area network (PAN)
  - Campus area network (CAN)
  - Storage area network (SAN)
  - Software-defined wide area network (SDWAN)
  - Multiprotocol label switching (MPLS)
  - Multipoint generic routing encapsulation (mGRE)
- **Servicebezogener Zugangspunkt**
  - Signalübergabepunkt
  - Smartjack
- **Virtuelle Netzwerkkonzepte**
  - vSwitch
  - Virtual network interface card (vNIC)
  - Network function virtualization (NFV)
  - Hypervisor
- **Anbieter-Verbindungen**
  - Satellit
  - Digital subscriber line (DSL)
  - Kabel
  - Standleitung
  - Metro-optical

1.3 Typen von Kabeln und Steckern zusammenfassen und erläutern, welcher Typ sich für eine bestimmte Lösung eignet

- **Kupfer**
  - Twisted Pair
    - Cat 5
    - Cat 5e
    - Cat 6
    - Cat 6a
    - Cat 7
    - Cat 8
  - Koaxial/RG-6
  - Twinaxial
  - Abschlussstandards
    - TIA/EIA-568A
    - TIA/EIA-568B
- **Glasfaser**
  - Single-Mode
  - Multi-Mode
- **Steckertypen**
  - Local connector (LC), Straight tip (ST), Subscriber connector (SC), Mechanical transfer (MT), Registered jack (RJ)
    - Angled physical contact (APC)
    - Ultra-physical contact (UPC)
  - RJ11
  - RJ45
  - Stecker Typ F
  - Sendeempfänger/Medienkonverter
  - Sendeempfängertyp
    - Small form-factor pluggable (SFP)
    - Enhanced form-factor pluggable (SFP+)
    - Quad small form-factor pluggable (QSFP)
    - Enhanced quad small form-factor pluggable (QSFP+)
- **Kabelmanagement**
  - Patchfeld/Steckfeld
  - Glasfaser-Patchfeld/Steckfeld
  - Klemmleiste
    - 66
    - 110
    - Krone
    - Bix
- **Ethernet-Standards**
  - Kupfer
    - 10BASE-T
    - 100BASE-TX
    - 1000BASE-T
    - 10GBASE-T
    - 40GBASE-T
  - Glasfaser
    - 100BASE-FX
    - 100BASE-SX
    - 1000BASE-SX
    - 1000BASE-LX
    - 10GBASE-SR
    - 10GBASE-LR
    - Coarse wavelength division multiplexing (CWDM)
    - Dense wavelength division multiplexing (DWDM)
    - Bidirectional wavelength division multiplexing (WDM)

1.4 Anhand eines gegebenen Szenarios ein Subnetz konfigurieren und die geeigneten IP-Adressierungsschemata anwenden

- **Öffentliche vs. private Adressen**
  - RFC1918
  - Network address translation (NAT)
  - Port address translation (PAT)
- **IPv4 oder IPv6**
  - Automatic Private IP Addressing (APIPA)
  - Extended unique identifier (EUI-64)
  - Multicast
  - Unicast
  - Anycast
  - Broadcast
  - link local
  - Loopback
  - Standard-Gateway
- **IPv4-Subnetze**
  - Classless (Subnetzmaske in variabler Länge)
  - Classfull
    - A
    - B
    - C
    - D
    - E
  - Classless-Inter-Domain-Routing-(CIDR-) Notation
- **IPv6-Konzepte**
  - Tunneling
  - Dual Stack
  - Kurzschreibweise
  - Router advertisement
  - Stateless address autoconfiguration (SLAAC)
- **Virtual IP (VIP)**
- **Subinterfaces**

1.5 Gängige Ports und Protokolle, deren Anwendung und verschlüsselte Alternativen erläutern

Protokolle	Ports
File Transfer Protocol (FTP)	20/21
Secure Shell (SSH)	22
Secure File Transfer Protocol (SFTP)	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
Post Office Protocol v3 (POP3)	110
Network Time Protocol (NTP)	123
Internet Message Access Protocol (IMAP)	143
Simple Network Management Protocol (SNMP)	161/162
Lightweight Directory Access Protocol (LDAP)	389
Hypertext Transfer Protocol Secure (HTTPS) [Secure Sockets Layer (SSL)]	443
HTTPS [Transport Layer Security (TLS)]	443
Server Message Block (SMB)	445
Syslog	514
SMTP TLS	587
Lightweight Directory Access Protocol (over SSL) (LDAPS)	636
IMAP over SSL	993
POP3 over SSL	995
Structured Query Language (SQL) Server	1433
SQLnet	1521
MySQL	3306
Remote Desktop Protocol (RDP)	3389
Session Initiation Protocol (SIP)	5060/5061
IP-Protokollarten	
- Internet Control Message Protocol (ICMP)	
- TCP	
- UDP	
- Generic Routing Encapsulation (GRE)	
- Internet Protocol Security (IPSec)	
- Authentication Header (AH)/Encapsulating Security Payload (ESP)	
Verbindungslos vs. verbindungsorientiert	

1.6 Verwendung und Zweck von Netzwerkdiensten erläutern

- **DHCP**
  - Bereich
  - Ausschlussbereiche
  - Reservierung
  - Dynamische Zuweisung
  - Statische Zuweisung
  - Lease-Time
  - Bereichsoptionen
  - Verfügbare Leases
  - DHCP-Relay
  - IP-Helper/UDP-Forwarding
- **DNS**
  - Datensatzarten
    - Adresse (A vs. AAAA)
    - Canonical name (CNAME)
    - Mail exchange (MX)
    - Start of authority (SOA)
    - Pointer (PTR)
    - Text (TXT)
    - Service (SRV)
    - Name server (NS)
  - Global hierarchy
    - Root DNS servers
  - Intern vs. extern
  - Zonenübertragungen
  - Authoritative Name server
  - Time to live (TTL)
  - DNS-Caching
  - Reverse-DNS/Reverse-Lookup/ Forward-Lookup
  - Rekursiv-Lookup/Iterativ-Lookup
- **NTP**
  - Stratum
  - Clients
  - Server

1.7 Grundlegende Netzwerkarchitektur im Unternehmen und im Rechenzentrum erläutern

- **Dreistufig**
  - Core
  - Verteilungs-/Aggregationsschicht
  - Zugang/Edge
- **Software-definiertes Netzwerk**
  - Anwendungsschicht
  - Kontrollebene
  - Infrastrukturebene
  - Verwaltungsebene
- **Spine-and-Leaf**
  - Software-definiertes Netzwerk
  - Top-of-Rack-Switching
  - Backbone
- **Datenverkehrsfluss**
  - Nord-Süd
  - Ost-West
- **Niederlassung vs. Rechenzentrum vor Ort vs. Colocation**
- **Speichernetzwerke**
  - Verbindungstypen
    - Fibre Channel over Ethernet (FCoE)
    - Fibre Channel
    - Internet Small Computer Systems Interface (iSCSI)

1.8 Cloud-Konzepte und Konnektivitätsoptionen zusammenfassen

- **Bereitstellungsmodelle**
  - Öffentlich
  - Privat
  - Hybrid
  - Community
- **Service-Modelle**
  - Software-as-a-Service (SaaS)
  - Infrastructure-as-a-Service (IaaS)
  - Platform-as-a-Service (PaaS)
  - Desktop-as-a-Service (DaaS)
- **Infrastructure-as-Code**
  - Automatisierung/Orchestrierung
- **Konnektivitätsoptionen**
  - Virtual private network (VPN)
  - Private Direktverbindung zum Cloud-Anbieter
- **Mandanten-/Instanzierungsfähigkeit**
- **Anpassbarkeit**
- **Skalierbarkeit**
- **Sicherheitsimplikationen**

2.0 Netzwerkimplementierungen

2.1 Verschiedene Komponenten, ihre Funktionen und ihre geeignete Anordnung im Netzwerk vergleichen und gegenüberstellen

- **Netzwerkkomponenten**
  - Layer-2-Switch
  - Layer-3-Switch
  - Router
  - Hub
  - Access Point
  - Bridge
  - Drahtloser WLAN-Controller
  - Loadbalancer
  - Proxyserver
  - Kabelmodem
  - DSL-Modem
  - Repeater
  - Voice-Gateway
  - Medienkonverter
  - Intrusion-Prevention-System (IPS)/ Intrusion-Detection-System (IDS)
  - Firewall
  - VPN Endpunkt
- **Vernetzte Komponenten**
  - Voice-over-Internet-Protocol-(VoIP-)Telefon
  - Drucker
  - Zugangskontrollsystem
  - Kameras
  - Heizungs-, Lüftungs- und Klimatechniksensoren
  - Internet der Dinge (IoT)
    - Kühlschrank
    - Intelligente Lautsprecher
    - Intelligente Thermostate
    - Intelligente Türklingeln
  - Industrial control systems/ supervisory control and data acquisition (SCADA)

2.2 Routing-Technologien und Konzepte für die Bandbreitenverwaltung vergleichen und gegenüberstellen

- **Routing**
  - Dynamisches Routing
    - Protokolle [Routing Internet Protocol (RIP), Open Shortest Path First (OSPF), Enhanced Interior Gateway Routing Protocol (EIGRP), Border Gateway Protocol (BGP)]
    - Link-State vs. Distanz-vektor vs. Hybrid
  - Statisches Routing
  - Standardroute
  - Administrative Distanz
  - Extern vs. Intern
  - Time-to-Live (Gültigkeitsdauer)
- **Bandbreitenverwaltung**
  - Traffic-Shaping
  - Quality of service (QoS)

2.3 Anhand eines gegebenen Szenarios allgemeine Ethernet-Switching-Funktionen konfigurieren und bereitstellen

- Data virtual local area network (VLAN)
- Voice VLAN
- Portkonfigurationen
  - Port-Tagging/802.1Q
  - Port-Aggregation
    - Link Aggregation Control Protocol (LACP)
  - Duplex
  - Geschwindigkeit
  - Flow Control
  - Portspiegelung
  - Portsicherheit
  - Jumbo-Frames
  - Auto-medium-dependent Interface Crossover (MDI-X)
- Media-access-control-(MAC-) Adresstabellen
- Power over Ethernet (PoE)/ Power over Ethernet plus (PoE+)
- Spanning-Tree-Protokoll
- Carrier-sense multiple access with collision detection (CSMA/CD)
- **Address-Resolution-Protokoll (ARP)**
- **Neighbor-Discovery-Protokoll**

2.4 Anhand eines vorgegebenen Szenarios geeignete WLAN-Standards und -Technologien installieren und konfigurieren

- **802.11-Standards**
  - a
  - b
  - g
  - n (WiFi 4)
  - ac (WiFi 5)
  - ax (WiFi 6)
- **Frequenzen und Frequenzbereich**
  - 2,4 GHz
  - 5 GHz
- **Kanäle**
  - Regulatorische Auswirkungen
- **Kanalbündelung (Channel Bonding)**
- **Service Set Identifier (SSID)**
  - Basic Service Set
  - Extended Service Set
  - Independent Basic Service Set (Ad-hoc)
  - Roaming
- **Antennentypen**
  - Omnidirektional
  - Richtantenne
- **Verschlüsselungsstandards**
  - WiFi Protected Access (WPA)/ WPA2 Personal [Advanced Encryption Standard (AES)/ Temporal Key Integrity Protocol (TKIP)]
  - WPA/WPA2 Enterprise (AES/TKIP)
- **Mobilfunktechnologien**
  - Code-division Multiple Access (CDMA)
  - Global System for Mobile Communications (GSM)
  - Long-Term Evolution (LTE)
  - 3G, 4G, 5G
- **Multiple Input, Multiple Output (MIMO) und Multi-User MIMO (MU-MIMO)**

3.0 Netzwerkbetrieb

3.1 Anhand eines gegebenen Szenarios die geeigneten Statistiken und Sensoren zur Gewährleistung der Verfügbarkeit des Netzwerks verwenden

- **Leistungsmetriken/-sensoren**
  - Gerät/Gehäuse
    - Temperatur
    - Central-Processing-Unit-(CPU-) Nutzung
    - Speicher
  - Netzwerk-Metriken
    - Bandbreite
    - Latenz
    - Jitter
- **SNMP**
  - Traps
  - Object identifiers (OIDs)
  - Management Information Bases (MIBs)
- **Protokolle (Logs) von Netzwerkgeräten**
  - Einsehen der Protokolle
    - Datenverkehrsprotokolle
    - Audit logs
    - Syslog
  - Stufen der Protokollierung/ Schweregrade
- **Schnittstellenstatistik/-status**
  - Link-Status (oben/unten)
  - Geschwindigkeit/Duplex
  - Datenverkehr senden/empfangen
  - Cyclic redundancy checks, CRCs (zyklische Redundanzprüfungen)
  - Protokollpaket und Bytezahl
- **Schnittstellenfehler oder -warnungen**
  - CRC-Fehler
  - Giant-Pakete
  - Runt-Pakete
  - Kapselungsfehler
- **Umweltfaktoren und -sensoren**
  - Temperatur
  - Feuchtigkeit
  - Elektrik
  - Überschwemmung
- **Basis**
- **NetFlow-Daten**
- **Betriebszeit/Ausfallzeit**

3.2 Zweck der organisatorischen Dokumente und Richtlinien erläutern

- **Pläne und Verfahren**
  - Change-Management
  - Plan für die Reaktion auf einen Sicherheitsvorfall
  - Desaster Recovery
  - Betriebskontinuitätsplan
  - Systemlebenszyklus
  - Standardbetriebsverfahren
- **Härtung und Sicherheitsrichtlinien**
  - Passwortrichtlinie
  - Nutzungsrichtlinie
  - Bring-Your-Own-Device-(BYOD-) Richtlinie
  - Remote-Access-Richtlinie
  - Onboarding- und Offboarding-Richtlinie
  - Sicherheitsrichtlinie
  - Schutz vor Datenverlust
- **Allgemeine Dokumentation**
  - Physisches Netzwerkdiagramm
    - Grundriss
    - Rack-Diagramm
    - Intermediate-Distribution-Frame (IDF)-/Main-Distribution-Frame (MDF)-Dokumentation
  - Logisches Netzwerkdiagramm
  - Schaltplan
  - Bericht zur Standortprüfung
  - Audit- und Bewertungsbericht
  - Grundlegende Konfigurationen
- **Allgemeine Vereinbarungen**
  - Geheimhaltungsvereinbarung (NDA)
  - Dienstleistungsvereinbarung (SLA)
  - Absichtserklärung (Memorandum of Understanding – MOU)

3.3 Konzepte für Hochverfügbarkeit und Notfallwiederherstellung (Desaster Recovery) erläutern; beste Lösung zusammenfassen

- **Lastverteilung**
- **Multipathing**
- **Network interface card (NIC) teaming**
- **Redundante Hardware/Cluster**
  - Switches
  - Router
  - Firewalls
- **Support von Einrichtungen und Infrastruktur**
  - Unterbrechungsfreie Stromversorgung (USV)
  - Power distribution units (PDUs)
  - Generator
  - HLK (Heizung, Lüftung, Klima)
  - Brandschutzeinrichtung
- **Konzepte zu Redundanz und Hochverfügbarkeit (HV)**
  - Cold Site
  - Warm Site
  - Hot Site
  - Cloud-Site
  - Active/Active vs. Active/Passive
    - Multiple Internet Service Providers (ISPs)/ verschiedene Pfade
    - Virtual Router Redundancy Protocol (VRRP)/First Hop Redundancy Protocol (FHRP)
  - Mean-Time-to-Repair (MTTR)
  - Mean-Time-between-Failure (MTBF)
  - Recovery-Time-Objective (RTO)
  - Recovery-Point-Objective (RPO)
- **Sicherung und Wiederherstellung von Netzwerkkomponenten**
  - Zustand
  - Konfiguration

4.0 Netzwerksicherheit

4.1 Allgemeine Sicherheitskonzepte erläutern

- **Confidentiality, integrity, availability, CIA (Vertraulichkeit, Integrität, Verfügbarkeit)**
- **Bedrohungen**
  - Intern
  - Extern
- **Schwachstellen**
  - Common Vulnerabilities and Exposures, CVE (häufige Sicherheitsrisiken und Sicherheitslücken)
  - Zero-Day
- **Missbräuche**
- **Prinzip der geringsten Rechte**
- **Rollenbasierter Zugriff**
- **Zero Trust**
- **Defense-in-Depth**
  - Durchsetzung der Netzsegmentierung
  - Perimeternetz [bisher bekannt als Demilitarized Zone, DMZ (entmilitarisierte Zone)]
  - Aufgabentrennung
  - Netzzugangskontrolle
  - Honeypot
- **Authentifizierungsmethoden**
  - Multifaktor
  - Terminal Access Controller Access-Control System Plus (TACACS+)
  - Single-Sign-On (SSO)
  - Remote Authentication Dial-In User Service (RADIUS)
  - LDAP
  - Kerberos
  - Lokale Authentifizierung
  - 802.1X
  - Extensible Authentication Protocol (EAP)
- **Risikomanagement**
  - Bewertungen des Sicherheitsrisikos
    - Bedrohungsanalyse
    - Sicherheitsrisikobewertung
    - Penetrationstests
    - Posture-Beurteilung
  - Bewertungen von Unternehmensrisiken
    - Prozessbewertung
    - Bewertung der Lieferanten
- **Security information and event management (SIEM)**

4.2 Häufige Angriffsarten miteinander vergleichen und gegenüberstellen

- **Technologiebasiert**
  - Denial-of-service (DoS)/Distributed Denial-of-Service (DDoS)
    - Botnet/Befehl und Steuerung
  - On-Path-Attack (früher bekannt als Man-in-the-Middle-Angriff)
  - DNS-Poisoning
  - VLAN-Hopping
  - ARP-Spoofing
  - Rogue-DHCP
  - Rogue-Access-Point (AP)
  - Evil Twin
  - Ransomware
  - Passwortangriffe
    - Brute-Force
    - Wörterbuch
  - MAC-Spoofing
  - IP-Spoofing
  - De-Authentifizierung
  - Malware
- **Mensch und Umwelt**
  - Social Engineering
    - Phishing
    - Tailgating
    - Piggybacking
    - Shoulder-Surfing

4.3 Anhand eines gegebenen Szenarios Netzwerk-Härtungstechniken anwenden

- **Best Practices**
  - Sicheres SNMP
  - Router Advertisement (RA) Guard
  - Portsicherheit
  - Dynamische ARP-Prüfung
  - Überwachung der Kontrollebene (Control plane policing)
  - Private VLANs
  - Nicht benötigte Switchports deaktivieren
  - Nicht benötigte Netzwerkdienste deaktivieren
  - Standardkennwörter ändern
  - Kennwortkomplexität/-länge
  - DHCP-Snooping aktivieren
  - Standard-VLAN ändern
  - Patch- und Firmware-Verwaltung
  - Zugriffskontrollliste
  - Rollenbasierter Zugriff
  - Firewall-Regeln
    - Explizite Ablehnung
    - Implizite Ablehnung
- **Drahtlose Sicherheit**
  - MAC-Filter
  - Antennenplatzierung
  - Sendeleistung
  - Isolierung des Funk-Clients
  - Isolierung des Gastnetzwerks
  - Vorinstallierte Schlüssel
  - EAP
  - Geofencing
  - Captive Portal
- **Überlegungen zum IoT-Zugang**

4.4 Fernzugriffsmethoden und Konsequenzen für die Sicherheit vergleichen und gegenüberstellen

- **Site-to-Site-VPN**
- **Client-to-Site-VPN**
  - VPN ohne Client
  - Split-Tunnel vs. vollständiger Tunnel
- **Remote-Desktop-Verbindung**
- **Remote-Desktop-Gateway**
- **SSH**
- **Virtual Network Computing (VNC)**
- **Virtueller Desktop**
- **Überlegungen zur Authentifizierung und Autorisierung**
- **In-Band- vs. Out-of-Band-Verwaltung**

4.5 Bedeutung physischer Sicherheitsmaßnahmen erläutern

- **Erkennungsmethoden**
  - Kamera
  - Bewegungserkennung
  - Asset-Tags
  - Manipulationserkennung
- **Präventionsmethoden**
  - Mitarbeiterschulung
  - Hardware für die Zugangskontrolle
    - Ausweisleser
    - Biometrie
  - Abschließbare Regale
  - Abschließbare Schränke
  - Zutrittssteuerung des Vorraums (früher bekannt als „Man-Trap“)
  - Intelligente Schließfächer
- **Anlagenentsorgung**
  - Rückstellung auf die Werkseinstellungen/Löschen der Konfiguration
  - Geräte für die Entsorgung säubern

5.0 Netzwerkfehlerbehebung

5.1 Methoden zur Netzwerkfehlersuche erläutern

- **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 prüfen, 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 Problem melden
- **Aktionsplan zur Lösung des Problems aufstellen und mögliche Auswirkungen bestimmen**
- **Die Lösung umsetzen oder das Problem gegebenenfalls melden**
- **Vollständige Systemfunktionalität prüfen und gegebenenfalls präventive Maßnahmen ergreifen**
- **Ergebnisse, Aktionen, Ergebnisse und gelernte Lektionen dokumentieren**

5.2 Anhand eines gegebenen Szenarios häufige Konnektivitätsprobleme mit Kabeln lösen und die geeigneten Werkzeuge auswählen

- **Spezifikationen und Einschränkungen**
  - Durchsatz
  - Geschwindigkeit
  - Entfernung
- **Überlegungen zu den Kabeln**
  - Abgeschirmte und nicht abgeschirmte
  - Kabelkanal und Steigleitungen
- **Nutzung der Kabel**
  - Rollover-Kabel/Konsolenkabel
  - Crossover-Kabel
  - Power-over-Ethernet
- **Allgemeine Probleme**
  - Abschwächung
  - Interferenz
  - Verlust in Dezibel (dB)
  - Falsche Pinbelegung
  - Falsche Anschlüsse
  - Offen/Kurzschluss
  - Statusanzeigen licht-emittierende Dioden (LEDs)
  - Falsche Empfänger
  - Duplexing-Probleme
  - Senden und Empfangen (TX/RX) vertauscht
  - Verschmutzte optische Kabel
- **Gängige Werkzeuge**
  - Kabel-Crimpzange
  - LSA-Auflegewerkzeug
  - Kabelsuch- und Testgerät
  - Loopback-Adapter
  - Optisches Zeitbereichsre-flektometer (OTDR)
  - Multimeter
  - Kabeltester
  - Verkabelungsplan
  - Network Tap/Abhören/Mitschneiden
  - Schmelzspleißen
  - Spektrumanalysatoren
  - Scheren/Schneidgeräte
  - Abisolierzange
  - Faser-Belichtungsmesser

5.3 Anhand eines gegebenen Szenarios die geeigneten Netzwerk-Softwaretools und Befehle anwenden

- **Softwaretools**
  - WiFi-Analysator
  - Protokollanalysator/ Paketaufzeichnung
  - Bandbreitengeschwindigkeitstester
  - Port-Scanner
  - iperf
  - NetFlow-Analyzer
  - Trivial-File-Transfer-Protokoll-(TFTP-) Server
  - Terminal-Emulationssoftware
  - IP-Scanner
- **Befehlszeilen-Tool**
  - ping
  - ipconfig/ifconfig/ip
  - nslookup/dig
  - traceroute/tracert
  - arp
  - netstat
  - hostname
  - route
  - telnet
  - tcpdump
  - nmap
- **Grundlegende Befehle für die Netzwerkplattformen**
  - show interface
  - show config
  - show route

5.4 Anhand eines gegebenen Szenarios häufig auftretende drahtlose Verbindungsprobleme beheben

- **Spezifikationen und Einschränkungen**
  - Durchsatz
  - Geschwindigkeit
  - Entfernung
  - Empfangene Signalstärke Anzeige (RSSI) Signalstärke
  - Effektive isotrope Strahlungsleistung (EIRP)/Leistungseinstellungen
- **Überlegungen**
  - Antennen
    - Platzierung
    - Typ
    - Polarisierung
  - Kanalauslastung
  - AP-Zuordnungszeit
  - Standortbeurteilung
- **Allgemeine Probleme**
  - Interferenz
    - Kanalüberlappung
  - Dämpfung des Antennenkabels/ Signalverlust
  - RF-Dämpfung/Signalverlust
  - Falsche SSID
  - Falscher Schlüssel
  - Konflikt mit dem Verschlüsselungsprotokoll
  - Unzureichende Funkabdeckung
  - Probleme mit dem Captive Portal
  - Abgrenzungsprobleme der Kunden

5.5 Anhand eines gegebenen Szenarios allgemeine Netzwerkprobleme beheben

- **Überlegungen**
  - Überprüfung der Gerätekonfiguration
  - Routing-Tabellen
  - Status der Schnittstelle
  - VLAN-Zuweisung
  - Auslastung des Netzwerkes
- **Allgemeine Probleme**
  - Kollisionen
  - Broadcast-Sturm
  - Doppelte MAC-Adressen
  - Doppelte IP-Adresse
  - Multicast-Flooding
  - Asymmetrisches Routing
  - Switching-Schleifen
  - Routing-Schleifen
  - Rogue-DHCP-Server
  - Ausschöpfung des DHCP-Spielraums
  - Probleme mit IP-Einstellungen
    - Falsches Gateway
    - Falsche Subnetzmaske
    - Falsche IP-Adresse
    - Falscher DNS
  - Fehlende Route
  - Niedrige Signalstärke bei optischen Verbindungen
  - Probleme mit dem Zertifikat
  - Hardware-Fehler
  - Host-basierte/Netzwerk-basierte Firewall-Einstellungen
  - Gesperrte Dienste, Ports oder Adressen
  - Falsches VLAN
  - DNS-Probleme
  - NTP-Probleme
  - BYOD-Probleme
  - Probleme mit lizenzierten Funktionen
  - Probleme mit der Netzwerkleistung

Network+ (N10-008) Akronym-Liste

Es folgt eine Liste von Abkürzungen, die in den CompTIA Network+ Prüfungen vorkommen. Teilnehmer sind aufgefordert, die komplette Liste durchzugehen und ausreichende praktische Kenntnisse aller aufgeführten Abkürzungen als Teil des umfassenden Prüfungsvorbereitungsprogramms zu erwerben.

ABKÜRZUNG	BEDEUTUNG
AAA	Authentication Authorization, Accounting and Auditing (Authentifizierung, Autorisierung, Abrechnung und Prüfung)
ACL	Access Control List (Zugriffskontrollliste)
AES	Advanced Encryption Standard (erweiterter Verschlüsselungsstandard)
AH	Authentication Header (Authentifizierungsheader)
AP	Access Point (Zugangspunkt)
APC	Angled physical contact (gewinkelte physische Kontaktanschlüsse)
APIPA	Automatic Private Internet Protocol Addressing (automatische private Internetprotokoll-Adressierung)
ARP	Address Resolution Protocol
AUP	Acceptable Use Policy (Nutzungsrichtlinie)
BGP	Border Gateway Protocol
BNC	British Naval Connector/Bayonet Niell-Concelman (britischer Marinestecker/ Bajonettverschluss nach Niell-Concelman)
BYOD	Bring Your Own Device
CAM	Content Addressable Memory (Tabelle) (Assoziativspeicher)
CAN	Campus Area Network (Campusnetzwerk)
CDMA	Code Division Multiple Access (Codemultiplexverfahren)
CIA	Confidentiality, Integrity, and Availability (Vertraulichkeit, Integrität und Verfügbarkeit)
CIDR	Classless Inter-Domain Routing (nicht klassiertes Routing zwischen Domains)
CLI	Command-Line Interface (Befehlszeilenschnittstelle)
CNAME	Canonical Name (kanonischer Name)
CPU	Central Processing Unit (zentrale Prozessoreinheit)
CRC	Cyclic Redundancy Checking (zyklische Redundanzprüfung)
CSMA/CA	Carrier-Sense Multiple Access with Collision Avoidance (Carrier-Sense-Mehrfachzugriff mit Kollisionsvermeidung)
CSMA/CD	Carrier-Sense Multiple Access with Collision Detection (Carrier-Sense-Mehrfachzugriff mit Kollisionserkennung)
CSU	Channel Service Unit
CVE	Common Vulnerabilities and Exposures (Häufige Sicherheitsrisiken und Sicherheitslücken)

ABKÜRZUNG	BEDEUTUNG
CWDM	Coarse Wave Division Multiplexing (grobes Wellenlängenmultiplexing)
Daas	Desktop-as-a-Service
dB	Dezibel
DDoS	Distributed Denial of Service (verteilte Denial-of-Service-Angriffe)
DHCP	Dynamic Host Configuration Protocol
DLP	Data Loss Prevention (Vermeidung von Datenverlust)
DNS	Domain Name System (Domänennamensystem)
DoS	Denial-of-Service (Dienstverweigerung)
DSL	Digital Subscriber Line (digitaler Teilnehmeranschluss)
DSU	Data Service Unit
DWDM	Dense Wavelength Division Multiplexing
EAP	Extensible Authentication Protocol
EIA	Electronic Industries Association (Verband der Elektronikindustrie)
EIGRP	Enhanced Interior Gateway Routing Protocol
EIRP	Effective Isotropic Radiated Power (effektive isotrope Strahlungsleistung)
ESP	Encapsulated Security Payload (gekapselte Sicherheitsnutzlast)
EUI	Extended Unique Identifier
FCoE	Fibre Channel over Ethernet
FHRP	First Hop Redundancy Protocol
FTP	File Transfer Protocol
GBIC	Gigabit Interface Converter
GRE	Generic Routing Encapsulation
GSM	Global System for Mobile Communications
HA	High Availability (Hochverfügbarkeit)
HDMI	High-Definition Multimedia Interface
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
HVAC/HLK	Heating, Ventilation and Air Conditioning (Heizungs-, Lüftungs- und Klimatechnik)
IaaS	Infrastructure as a Service
ICMP	Internet Control Message Protocol
ICS	Industrial Control System (industrielles Steuerungssystem)
IDF	Intermediate Distribution Frame (Zwischenverteiler)
IDS	Intrusion Detection System (Angriffserkennungssystem)

ABKÜRZUNG	BEDEUTUNG
IGMP	Internet Group Management Protocol
IMAP	Internet Message Access Protocol
IoT	Internet-of-Things (Internet der Dinge)
IP	Internet Protocol
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security (Internetprotokollsicherheit)
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
iSCSI	Internet Small Computer Systems Interface
ISP	Internet Service Provider (Internetdienstanbieter)
LACP	Link Aggregation Control Protocol
LAN	Local Area Network
LC	Local Connector (LC-Stecker)
LDAP	Lightweight Directory Access Protocol
LDAPS	Lightweight Directory Access Protocol (über SSL)
LED	Light-Emitting Diode (Leuchtdiode)
LTE	Long-Term Evolution (langfristige Entwicklung)
MAC	Media Access Control/Medium Access Control
MAN	Metropolitan Area Network
MDF	Main Distribution Frame (Hauptverteiler)
MDIX	Medium Dependent Interface Crossover (medienabhängige Schnittstellenübergänge)
mGRE	Multipoint Generic Routing Encapsulation (generische Mehrpunkt-Routing-Kapselung)
MIB	Management Information Base (Verwaltungsdatenbank)
MIMO	Multiple Input Multiple Output (Mehrfacheingabe Mehrfachausgabe)
MU-MIMO	Multiuser – Multiple Input Multiple Output (Mehrbenutzer – Mehrfacheingabe Mehrfachausgabe)
MOU	Memorandum of Understanding (Absichtserklärung)
MPLS	Multiprotocol Label Switching (Multiprotokoll-Etiketten-Vermittlung)
MTBF	Mean Time Between Failure (mittlere Zeit zwischen Ausfällen)
MT-RJ	Mechanical Transfer – Registered Jack (mechanischer Transfer – registrierter Wagenheber)
MTTR	Mean Time to Repair (mittlere Zeit bis zur Reparatur)
MTU	Maximum Transmission Unit
MX	Mail Exchange (E-Mail-Austausch)
NAC	Network Access Control (Netzwerk-Zugangskontrolle)
NAS	Network Attached Storage (Netzwerkverknüpfte Speicherung)
NAT	Network Address Translation (Netzwerk-Adressübersetzung)
NDA	Non-Disclosure Agreement (Vertraulichkeitsvereinbarung)

ABKÜRZUNG	BEDEUTUNG
NFV	Network Function Virtualization (Virtualisierung von Netzwerkfunktionen)
NGFW	Next-Generation Firewall
NIC	Network Interface Card (Netzwerkkarte)
NS	Name Server (Namenserver)
NTP	Network Time Protocol
OID	Object Identifier (Objektbezeichner)
OSI	Open Systems Interconnection (offene Systemzusammenschaltung)
OSPF	Open Shortest Path First (kürzesten Pfad zuerst öffnen)
OTDR	Optical Time Domain Reflectometer (optisches Zeitbereichsreflektometer)
PaaS	Platform-as-a-Service
PAN	Personal Area Network
PAT	Port Address Translation (Port-Adressübersetzung)
PDU	Power Distribution Unit (Stromverteilungseinheit)
PoE	Power over Ethernet (Strom über Ethernet-Kabel)
POP3	Post Office Protocol Version 3
PSK	Pre-Shared Key
PTR	Pointer Record (Zeigersatz)
QoS	Quality of Service (Dienstgüte)
QSFP	Quad Small Form-factor Pluggable
RA	Router Advertisements (Routerankündigungen)
RADIUS	Remote Authentication Dial-In User Service (Authentifizierungsdienst für sich einwählende Benutzer)
RAID	Redundant Array of Inexpensive (or Independent) Disks (Redundantes Array aus kostengünstigen (oder unabhängigen) Festplatten)
RDP	Remote Desktop Protocol
RF	Radio Frequency (Funkfrequenz)
RFC	Request for Comment (Bitte um Stellungnahme)
RG	Radio Guide (Normbezeichnung für Koaxialkabel)
RIP	Routing Internet Protocol
RJ	Registered Jack (genormte Buchse)
RPO	Recovery Point Objective
RSSI	Received Signal Strength Indication (Anzeige der empfangenen Signalstärke)
RTO	Recovery Time Objective (gewünschte Wiederherstellungsdauer)
RTSP	Real-Time Streaming Protocol
SaaS	Software-as-a-Service
SAN	Storage Area Network
SC	Standard Connector/Subscriber Connector (Standardstecker/Teilnehmerstecker)
SCADA	Supervisory Control and Data Acquisition
SDN	Software Defined Network
SDWAN	Software-Defined WAN (Software-definiertes WAN)
SFP	Small Form-factor Pluggable
SFTP	Secure File Transfer Protocol
SIEM	Security Information and Event Management
SIP	Session Initiation Protocol

ABKÜRZUNG	BEDEUTUNG
SLA	Service Level Agreement (Dienstleistungsvertrag)
SLAAC	Stateless Address Auto-Configuration (zustandslose Adress-Autokonfiguration)
SMB	Server Message Block (LAN-Manager- oder NetBIOS-Protokoll)
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SOA	Start of Authority (Zonenbeginn)
SOHO	Small Office / Home Office (Kleinbüro/Heimbüro)
SQL	Structured Query Language (strukturierte Abfragesprache)
SRV	Service Record (Diensteintrag)
SSD	Solid State Drive (Solid-State-Laufwerk)
SSH	Secure Shell
SSID	Service Set Identifier (Netzwerkname)
SSL	Secure Sockets Layer
SSO	Single Sign-On (einmaliges Anmelden)
ST	Straight Tip oder Snap Twist (ST-Stecker)
STP	Spanning Tree Protocol
SYSLOG	System Log (Systemprotokoll)
TACACS+	Terminal Access Controller Access Control System Plus (Terminal-Zugang Controller-Zugang Kontrollsystem Plus)
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TIA/EIA	Telecommunications Industry Association/ Electronic Industries Alliance (Verband der Telekommunikationsindustrie/ Verband der Elektrotechnik)
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TTL	Time to Live (Gültigkeitsdauer)
TX/RX	Transmit and Receive (Senden und Empfangen)
UDP	User Datagram Protocol
UPC	Ultra-Physical Contact (Ultra-physischer Kontakt)
URL	Uniform Resource Locator
USB	Universal Serial Bus
USV	Unterbrechungsfreie Stromversorgung
UTP	Unshielded Twisted Pair (nicht abgeschirmtes Kabel mit verdrillten Adernpaaren)
VIP	Virtual IP (virtuelle IP-Adresse)
VLAN	Virtual Local Area Network
VM	Virtual Machine (virtuelle Maschine)
VNC	Virtual Network Computing (virtuelles Netzwerk-Computing)
vNIC	virtual Network Interface Card (virtuelle Netzwerkschnittstellenkarte)
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
VRRP	Virtual Router Redundancy Protocol
WAN	Wide Area Network
WAP	Wireless Access Point (drahtloser Zugangspunkt)
WDM	Wavelength Division Multiplexing (Wellenlängenmultiplexing)
WLAN	Wireless Local Area Network
WPA	WiFi Protected Access (Verschlüsselungsart)

Network+ Hardware- und Software-Empfehlungen

CompTIA führt hier einige Hardware- und Software-Beispiele auf, die die Teilnehmer bei der Vorbereitung auf die Network+ Prüfung unterstützen sollen. Diese Liste kann auch für Schulungsunternehmen hilfreich sein, die eine Praxiskomponente für ihr Schulungsangebot erstellen möchten. Die Aufzählungen zu den einzelnen Themen sind Beispiellisten und nicht erschöpfend.

AUSSTATTUNG

- Optische und Kupferpatchfelder
- Klemmleisten
- Layer-2-Switch
- Layer-3-Switch
- PoE-Switch
- Router
- Firewall
- VPN Endpunkt
- Wireless Access Point
- Einfache Laptops mit Unterstützung von Virtualisierung
- Tablet/Mobiltelefon
- Medienkonverter
- VoIP-System (einschließlich eines Telefons)

ZUSÄTZLICHE HARDWARE

- NICs
- Netzteile
- GBICs
- SFPs
- Managed Switch
- Wireless Access Point
- USV
- PoE-Injektor

ERSATZTEILE

- Patchkabel
- RJ11-Stecker
- RJ45-Stecker, Modularbuchsen
- Unshielded-Twisted-Pair-Kabelrolle (nicht abgeschirmtes Kabel mit verdrillten Adernpaaren)
- Rolle mit Koaxialkabel
- F-Steckverbinder
- Glasfasersteckverbinder
- Antennen
- Bluetooth-/drahtlose Adapter
- Konsolenkabel (RS-232 an USB-Seriell-Adapter)

WERKZEUGE

- Telco-/Netzwerk-Crimpzange
- Kabeltester
- LSA-Auflegewerkzeug
- Abisolierzange
- Crimpzange für Koaxialkabel
- Seitenschneider
- Kabelsuch- und Testgerät
- Glasfaser-Werkzeugsatz
- Optisches Leistungsmessgerät

SOFTWARE

- Protokollanalysator/Paketaufzeichnung
- Terminalemulationssoftware
- Linux-/Windows-Betriebssystem
- Software-Firewall
- Software-IDS/-IPS
- Netzwerkmapper
- Hypervisor-Software
- Virtuelle Netzwerkumgebung
- WiFi-Analysator
- Spektrumanalysator
- Netzwerk-Überwachungstools
- DHCP-Service
- DNS-Service
- NetFlow-Analyzer
- TFTP-Server
- Firmware-Backups für Upgrades

SONSTIGES

- Beispiel einer Netzwerkdokumentation
- Beispiel-Logs
- Defekte Kabel
- Cloud-Netzwerkdiagramme

CompTIA