NT200 CompTIA Network+

Kurzbeschreibung:

In diesem Kurs **NT200 CompTIA Network+** lernen Sie die grundlegenden Prinzipien der Installation, Konfiguration und Fehlerbehebung von Netzwerktechnologien sowie Sicherheitsmaßnahmen um Netzwerke vor Bedrohungen zu schützen und Sicherheitslücken zu minimieren.

Kurssprache: Wahlweise Deutsch oder Englisch
Kursunterlagen: Englisch
Prüfungssprache: Englisch

Zielgruppe:

Der Kurs **NT200 CompTIA Network+** richtet sich an Spezialisten fur den technischen Support, Spezialisten fur Netzwerkbetrieb, Systemadministratoren.

Voraussetzungen:

Um den Kursinhalten und dem Lerntempo des Kurses **NT200 CompTIA Network+** gut folgen zu können, sind folgende Voraussetzungen zu erfüllen:

- mindestens 9-12 Monate praktische Netzwerkerfahrung empfohlen

Sonstiges:

Dauer: 5 Tage

Preis: 2490 Euro plus Mwst.

Ziele:

- Einrichten von Netzwerkkonnektivität durch den Einsatz von kabelgebundenen und drahtlosen Geräten.
- Erläutern des Zwecks der Dokumentation und Führen der Netzwerkdokumentation.
- Allgemeine Netzwerkdienste zu konfigurieren.
- Erläuterung grundlegender Konzepte für Rechenzentren, Clouds und virtuelle Netzwerke.
- Überwachen von Netzwerkaktivitäten und Beheben von Leistungs- und Verfügbarkeitsproblemen.
- Härtungstechniken für die Netzwerksicherheit implementieren.
- Verwalten, Konfigurieren und Beheben von Fehlern in der Netzwerkinfrastruktur

Die CompTIA Network+ Zertifizierungsprüfung besteht aus maximal 90 Fragen, die in 90 Minuten beantwortet werden müssen. Sie brauchen ein Ergebnis von mindestens 720 Punkten (auf einer Skala von 100-900), um die Prüfung zu bestehen.

Die Prüfung können Sie in einem Pearson VUE Testzentrum oder online ablegen.

Inhalte/Agenda:

- **Networking concepts – Netzwerkgrundlagen (23%)**
  - **OSI-Schichtenmodell:** physikalisch, Data Link, Netzwerk, Transport, Sitzung, Darstellung, Anwendung
  - **Netzwerkkomponenten:** Router, Switches, Firewalls, IDS/IPS, Load Balancer, Proxys, NAS, SAN, drahtlose Geräte
  - **Cloud-Konzepte:** NFV, VPC, Network Security Groups, Cloud-Gateways; Bereitstellungsmodelle (öffentlich, privat, hybrid); Servicemodelle (SaaS, IaaS, PaaS)
  - **Ports und Protokolle:** FTP, SFTP, SSH, Telnet, SMTP, DNS, DHCP, HTTP, HTTPS, SNMP, LDAP, RDP, SIP
  - **Übertragungstypen:** Unicast, Multicast, Anycast, Broadcast
  - **Netzwerktopologien:** Mesh, Hybrid, Stern-/Hub-Spoke, Spine-Leaf, Punkt-zu-Punkt, Drei-Schichten-Architektur, Collapsed Core
  - **IPv4-Adressierung:** öffentliche vs. private Adressen, APIPA, RFC 1918, Loopback, Subnetting (VLSM, CIDR), Klassen A–E
- **Network implementation – Netzwerkinfrastruktur implementieren (20%)**
  - **Routing-Technologien:** statisches und dynamisches Routing (BGP, EIGRP, OSPF), Routenauswahl, NAT, PAT, FHRP, virtuelle IPs, Subinterfaces
  - **Switching:** VLANs, Interface-Konfiguration, Spanning Tree Protocol, MTU, Jumbo Frames
  - **Drahtlose Netzwerke:** Kanäle, Frequenzen, SSID, Netzwerktypen, Verschlüsselung, Gastnetzwerke, Authentifizierung, Antennentypen, Access Points
  - **Physische Installation:** Rack-Montage, Stromversorgung, Umgebungsbedingungen
- **Network operations – Netzwerkbetrieb (19%)**
  - **Dokumentation:** physische/logische Netzpläne, Rackschemata, Kabelmanagement, Asset-Inventar, IP-Adressmanagement, SLAs, WLAN-Site-Surveys
  - **Lifecycle-Management:** EOL/EOS-Planung, Software- und Geräteverwaltung
  - **Change-Management:** Änderungsanträge, Genehmigungen und Dokumentation
  - **Konfigurationsmanagement:** Produktivsysteme, Konfigurations-Backups, Standardkonfigurationen
  - **Netzwerküberwachung:** SNMP, Flow-Analyse, Paketmitschnitt, Baselines, Log-Zusammenführung, API-Integration, Port-Mirroring
  - **Notfallwiederherstellung:** RPO, RTO, MTTR, MTBF, Cold/Warm/Hot Sites, Active-Active/Passive-Strategien, Testszenarien
  - **Netzwerkdienste:** DHCP, SLAAC, DNS, NTP, PTP, NTS
  - **Zugriff und Verwaltung:** VPNs, SSH, grafische Oberflächen, API-Zugriffe, Konsolenzugriff
- **Network security – Netzwerksicherheit (14%)**
  - **Logische Sicherheitsmaßnahmen:** Verschlüsselung (in Transit/at Rest), PKI, IAM, MFA, SSO, RADIUS, LDAP, SAML, TACACS+, zeitbasierte Authentifizierung, Least Privilege, rollenbasierte Zugriffskontrolle, Geofencing
  - **Physische Sicherheitsmaßnahmen:** Videoüberwachung, Zugangskontrollen
  - **Täuschungstechniken:** Honeypots, Honeynets
  - **Sicherheitsgrundlagen:** Risiko, Schwachstelle, Exploit, Bedrohung, Vertraulichkeit–Integrität–Verfügbarkeit (CIA-Triade)
  - **Audits & Compliance:** Datenlokalität, PCI DSS, DSGVO
  - **Netzwerksegmentierung:** IoT, IIoT, SCADA, ICS, OT, Gastnetzwerke, BYOD-Umgebungen
  - **Angriffsarten:** DoS/DDoS, VLAN-Hopping, MAC-Flooding, ARP-Spoofing, DNS-Spoofing, Rogue Devices, Evil Twin, Man-in-the-Middle, Social Engineering (Phishing, Dumpster Diving, Shoulder Surfing, Tailgating)
  - **Sicherheitsfunktionen:** Hardening, NAC, Schlüsselverwaltung, Access Control Lists (ACL), URL-Filterung, Inhaltsfilter, Sicherheitszonen (trusted/untrusted), DMZ/Sicherheitszonen
- **Network troubleshooting – Netzwerkprobleme beheben (24%)**
  - **Fehlersuchmethodik:** Problemidentifikation, Hypothese, Tests, Lösung planen und umsetzen, Ergebnisse prüfen und dokumentieren
  - **Verkabelung & Schnittstellen:** falsche Kabeltypen, Signalverlust, fehlerhafte Terminierung, vertauschte TX/RX, Portstatus, Interface Counter, Probleme mit PoE oder Transceivern
  - **Netzwerkdienstprobleme:** VLAN-Fehler, Spanning Tree, Routing-Tabellen, Subnetzmasken, Gateway-Konfigurationen, Adresspools
  - **Performanceprobleme:** Überlastung, Latenz, Paketverlust, Interferenzen im WLAN
  - **Diagnose-Tools:** Protokollanalysatoren, CLI-Tools (z. B. ping, traceroute, ipconfig), Kabelfehlertester, WLAN-Analysetools