CompTIA.

Network+

CompTIA Network+ es la certificación principal para validar tus conocimientos sobre herramientas y conceptos esenciales de redes. Serás evaluado en tus habilidades de conectividad de red, documentación, configuración de servicios, centros de datos, nube, redes virtuales, monitoreo, resolución de problemas y fortalecimiento de la seguridad. Esta certificación te prepara para trabajos en soporte técnico, operaciones de red y administración de sistemas.

Objetivos del curso Network+ (V9)

Conceptos de redes (23%)

- **Capas del modelo OSI:** física, enlace de datos, red, transporte, sesión, presentación, aplicación.
- **Dispositivos de red:** enrutadores, conmutadores, cortafuegos, IDS/IPS, equilibradores de carga, proxies, NAS, SAN y dispositivos inalámbricos.
- **Conceptos de nube:** NFV, VPC, grupos de seguridad de red, puertas de enlace de nube, modelos de implementación (público, privado, híbrido), modelos de servicio (SaaS, IaaS, PaaS).
- **Puertos y protocolos:** FTP, SFTP, SSH, Telnet, SMTP, DNS, DHCP, HTTP, HTTPS, SNMP, LDAP, RDP, SIP.
- Tipos de tráfico: unidifusión, multidifusión, anycast, difusión.
- Medios de transmisión: inalámbricos (802.11, celular, satélite), cableados (fibra, coaxial, DAC).
- Transceptores y conectores: se, LC, ST, MPO, RJ11, RJ45, tipo F, BNC.
- **Topologías de red:** malla, híbrida, estrella/hub y radio, espina y hoja, punto a punto, de tres niveles, y núcleo colapsado.
- **Direccionamiento IPv4:** público vs. privado, APIPA, RFC1918, loopback, subnetting (VLSM, CIDR), y clases de direcciones (A, B, C, D, E).

Implementación de redes (20%)

- Tecnologías de enrutamiento: enrutamiento estático y dinámico (BGP, EIGRP, OSPF), selección de rutas, NAT, PAT, FHRP, VIP y subinterfaces.
- Tecnologías de conmutación: VLANs, configuración de interfaces, árbol de expansión, MTU y tramas jumbo.
- Dispositivos inalámbricos: canales, opciones de frecuencia, SSID, tipos de redes, cifrado, redes de invitados, autenticación, antenas y puntos de acceso.
- Instalaciones físicas: implicaciones de instalación, consideraciones de energía y factores ambientales.

Operaciones de red (19%)

- Documentación: diagramas físicos vs. lógicos, diagramas de racks, mapas de cables, diagramas de red, inventario de activos, IPAM, SLA y encuestas inalámbricas.
- Gestión del ciclo de vida: EOL, EOS, gestión de software y desmantelamiento.
- Gestión de cambios: seguimiento del proceso de solicitudes.
- Gestión de configuraciones: producción, respaldo, configuraciones base.
- Monitoreo de red: SNMP, datos de flujo, captura de paquetes, métricas base, agregación de registros, integración de API y duplicación de puertos.
- Recuperación ante desastres: RPO, RTO, MTTR, MTBF, sitios fríos/templados/calientes, activo-activo/pasivo y pruebas.
- Servicios de red: DHCP, SLAAC, DNS, NTP, PTP y NTS.
- Acceso y gestión: VPNs, SSH, GUI, API y consola.

Seguridad de la red (14%)

- Seguridad lógica: encriptación (datos en tránsito/descanso), PKI, 1AM, MFA, SSO, RADIUS, LDAP, SAML, TACACS+, autenticación basada en el tiempo, autorización, privilegios mínimos, control de acceso basado en roles y geofencing.
- Seguridad física: cámaras y cerraduras.
- Tecnologías de engaño: honeypot y honeynet.
- Términos de seguridad: riesgo, vulnerabilidad, explotación, amenaza y triada CIA.
- Auditorías y cumplimiento: localización de datos, PCI DSS y GDPR.
- Segmentación de la red: IoT, IIoT, SCADA, ICS, OT, invitados y BYOD.
- Tipos de ataques: DoS/DDoS, salto de VLAN, inundación de MAC, envenenamiento/suplantación de ARP, envenenamiento/suplantación de DNS, dispositivos/servicios maliciosos, gemelo malvado, ataque en el camino y ingeniería social (phishing, búsqueda en la basura, observación por encima del hombro, acceso no autorizado).
- Características de seguridad y defensa: endurecimiento de dispositivos, NAC, gestión de claves, ACL, filtrado de contenido/URL, zonas de confianza vs. no confianza y subred protegida.

Solución de problemas de red (24%)

- Metodología de resolución de problemas: identificar el problema, establecer una teoría, realizar pruebas, planificar e implementar una solución, verificar la funcionalidad y documentar hallazgos.
- Problemas de cableado e interfaces físicas: problemas de cables (tipo incorrecto, degradación de señal, terminación incorrecta, TX/RX transpuestos), problemas de interfaces (aumento de contadores, estado del puerto) y problemas de hardware (PoE, incompatibilidad de transceptores, fuerza de señal).
- Problemas de servicios de red: problemas de conmutación (STP, asignación de VLAN, ACLs), problemas de enrutamiento (tabla de enrutamiento y rutas predeterminadas), agotamiento de pool de direcciones y puerta de enlace/IP/máscara de subred incorrectos.
- Problemas de rendimiento: congestión, latencia, pérdida de paquetes e interferencia inalámbrica.
- Herramientas y protocolos: analizadores de protocolos, herramientas de línea de comandos, probadores de cables y analizadores de Wi-Fi.

Habilidades adquiridas

- Desplegar dispositivos cableados e inalámbricos, cubriendo direccionamiento IP, puertos, protocolos y arquitectura de red para el despliegue de redes.
- Comprender los procesos y procedimientos de documentación, ciclo de vida, gestión de cambios y configuración.
- Dominar la virtualización, los modelos de servicios en la nube, la elasticidad y
- Vigilar las redes para garantizar alta disponibilidad y resolver problemas de conectividad para mantener el rendimiento de la red.
- Establecer redes seguras y mitigar vulnerabilidades para fortalecer la seguridad.
- Diagnosticar y resolver problemas de red utilizando las herramientas adecuadas para una resolución efectiva.