Objetivos del examen de certificación CompTIA Network+

NÚMERO DE EXAMEN: N10-009

Acerca del examen

El examen de certificación CompTIA Network+ certificará que el candidato aprobado tenga los conocimientos y las habilidades requeridas para:

- Establecer conectividad de red al implementar dispositivos alámbricos e inalámbricos.
- Explicar el objetivo de la documentación y mantener la documentación de red.
- Configurar servicios comunes de red.
- Explicar conceptos básicos de centros de datos, nube y redes virtuales.
- Monitorear la actividad de red y resolver problemas de desempeño y disponibilidad.
- Implementar técnicas de fortalecimiento (hardening) de seguridad de red.
- Administrar, configurar y resolver problemas de infraestructura de red.

DESARROLLO DEL EXAMEN

Los exámenes de CompTIA son resultado de talleres de expertos del área temática y resultados de encuestas de toda la industria con respecto a las habilidades y conocimientos necesarios para un profesional de TI.

POLÍTICA DE USO DE MATERIALES AUTORIZADOS COMPTIA

CompTIA Certifications, LLC no está afiliado y no autoriza, aprueba o tolera la utilización de cualquier contenido proporcionado por otros sitios de capacitación no autorizados (conocidos como "brain dumps"). A las personas que utilicen este tipo de materiales en la preparación de cualquier examen CompTIA se les anularán los certificados y será suspendida la realización de futuras pruebas en concordancia con el Acuerdo para Candidatos de CompTIA. En un esfuerzo por comunicar de manera más clara las políticas de exámenes de CompTIA en relación con el uso de materiales de estudio autorizados, CompTIA dirige a todos los candidatos de certificación a las Políticas de Examen de Certificación CompTIA. Revise todas las políticas CompTIA antes de comenzar el proceso de estudio para cualquier examen CompTIA. Se les pedirá a los candidatos que respeten el Acuerdo para Candidatos de CompTIA. Si un candidato tiene una pregunta acerca de qué materiales de estudio se consideran no autorizados (conocidos como “brain dumps”), él/ella deberá comunicarse con CompTIA al correo electrónico examsecurity@comptia.org para confirmar.

RECUERDE

Las listas de ejemplos proporcionadas en formato con viñetas no son listas completas. Otros ejemplos de tecnologías, procesos o tareas relativas a cada objetivo también pueden ser incluidos en el examen, aunque no estén enumerados o cubiertos en este documento de objetivos. CompTIA revisa constantemente el contenido de nuestros exámenes y actualiza las preguntas de las pruebas para asegurar que nuestros exámenes sean actuales y la seguridad de las preguntas esté protegida. Cuando sea necesario, publicaremos exámenes actualizados, basados en objetivos de examen existentes. Sepa que todos los materiales relacionados de preparación para el examen serán válidos.

DETALLES DE LA PRUEBA

Examen requerido	N10-009
Número de preguntas	90 como máximo
Tipos de preguntas	Selección múltiple y basadas en la ejecución
Tiempo de la prueba	90 minutos
Experiencia recomendada	Un mínimo de 9–12 meses de experiencia en el área de redes de TI

OBJETIVOS DEL EXAMEN (DOMINIOS)

La siguiente tabla enumera los dominios medidos en este examen y el grado en el que están representados.

DOMINIO		PORCENTAJE DEL EXAMEN
1.0	Conceptos de redes	23%
2.0	Implementación de red	20%
3.0	Operaciones de red	19%
4.0	Seguridad de red	14%
5.0	Resolución de problemas de red	24%
Total	**100%**	

1.0 Conceptos de redes

1.1 Explicar conceptos relacionados con el modelo de referencia sobre Interconexión de Sistemas Abiertos (OSI).

- Capa 1 - Física
- Capa 2 - Enlace de datos
- Capa 3 - Red
- Capa 4 - Transporte
- Capa 5 - Sesión
- Capa 6 - Presentación
- Capa 7 - Aplicación

1.2 Comparar y contrastar dispositivos, aplicaciones y funciones de redes.

- **Dispositivos físicos y virtuales**
  - Enrutador
  - Conmutador
  - Firewall
  - Sistema de Detección de Intrusión (IDS)/sistema de prevención de intrusión (IPS)
  - Balanceador de carga
  - Proxy
  - Almacenamiento adjunto en red (NAS)
  - Red de área de almacenamiento (SAN)
  - Inalámbrica
    - Punto de acceso (AP)
    - Controlador
- **Aplicaciones**
  - Red de entrega de contenido (CDN)
- **Funciones**
  - Red privada virtual (VPN)
  - Calidad de servicio (QoS)
  - Tiempo de vida (TTL)

1.3 Resumir los conceptos de nube y las opciones de conectividad.

- **Virtualización de funciones de red (NFV)**
- **Nube privada virtual (VPC)**
- **Grupos de seguridad de red**
- **Listas de seguridad de red**
- **Puertas de enlace a nube**
  - Puerta de enlace a Internet
  - Puerta de enlace de traducción de dirección de red (NAT)
- **Opciones de conectividad de nube**
  - VPN
  - Corriente continua
- **Modelos de implementación**
  - Público
  - Privado
  - Híbrido
- **Service models**
  - Software como Servicio (SaaS)
  - Infraestructura como Servicio (IaaS)
  - Plataforma como Servicio (PaaS)
- **Escalabilidad**
- **Elasticidad**
- **Multitenancy**

1.4 Explicar los puertos, protocolos, servicios y tipos de tráfico en red comunes.

Protocolos	Puertos
Protocolo de Transferencia de Archivos (FTP)	20/21
Protocolo Seguro de Transferencia de Archivos (SFTP)	22
Shell seguro (SSH)	22
Telnet	23
Protocolo de Transferencia de Correo Simple (SMTP)	25
Sistema de nombres de dominio (DNS)	53
Protocolo de Configuración Dinámica de Host (DHCP)	67/68
Protocolo de Transferencia de Archivos Trivial (TFTP)	69
Protocolo de Transferencia de Hipertexto (HTTP)	80
Protocolo de Tiempo de Red (NTP)	123
Protocolo de Administración de Red Simple (SNMP)	161/162
Protocolo ligero de acceso a directorio (LDAP)	389
Protocolo de Transferencia Segura de Hipertexto (HTTPS)	443
Bloque de Mensajes de Servidor (SMB)	445
Syslog	514
Protocolo de Transferencia Segura de Correo Simple (SMTPS)	587
Protocolo ligero de acceso a directorio por SSL (LDAPS)	636
Lenguaje de consulta estructurada (SQL)	1433
Protocolo de Escritorio Remoto (RDP)	3389
Protocolo de Inicio de Sesión (SIP)	5060/5061

- Tipos de Protocolo de Internet (IP)
  - Protocolo de mensajes de control de internet (ICMP)
  - Protocolo de Control de Transmisión (TCP)
  - Protocolo de Datagrama del Usuario (UDP)
  - Encapsulación de Enrutamiento Genérico (GRE)
  - Seguridad del Protocolo de Internet (IPSec)
    - Encabezado de Autenticación (AH)
    - Carga útil de seguridad encapsulada (ESP)
    - Intercambio de Clave en Internet (IKE)
- Tipos de tráfico
  - Unicast
  - Multicast
  - Anycast
  - Broadcast

1.5 Comparar y contrastar los medios de transmisión y transceivers.

- Inalámbrica
  - Estándares 802.11
  - Celular
  - Satelital
- Cableado
  - Estándares 802.3
  - Fibra de modo simple vs. multimodal
  - Cable de cobre de conexión directa (DAC)
    - Cable Twinaxial
  - Cable coaxial
  - Velocidades del cable
  - Cable pleno vs. no pleno
- Transceivers
  - Protocolo
    - Ethernet
    - Canal de fibra (FC)
  - Factores de forma
    - Pequeño Factor de Forma Enchufable (SFP)
    - Pequeño Factor de Forma Enchufable Cuádruple (QSFP)
- Tipos de conector
  - Conector de suscriptor (SC)
  - Conector Local (LC)
  - Punta recta (ST)
  - Push on multifibra (MPO)
  - Conector registrado (RJ)11
  - RJ45
  - Tipo F
  - Bayonet Neill–Concelman (BNC)

1.6 Comparar y contrastar las topologías, arquitecturas y tipos de red.

- Malla
- Híbrido
- Star/hub and spoke
- Spine and leaf
- Punto a punto
- Modelo jerárquico de tres niveles
  - Core
  - Distribución
  - Acceso
- Core colapsado
- Flujos de tráfico
  - Norte-sur
  - Este-oeste

1.7 Dado un escenario, utilizar las direcciones adecuadas de una red Ipv4.

- Pública vs. privada
  - Dirección IP privada automática (APIPA)
  - RFC1918
  - Loopback/localhost
- Subred
  - Máscara de subred de longitud variable (VLSM)
  - Enrutamiento interdominio sin clase (CIDR)
- Clases de dirección IPv4
  - Clase A
  - Clase B
  - Clase C
  - Clase D
  - Clase E

1.8 Resumir casos de uso en evolución para entornos de red modernos.

- **Red definida por software (SDN) y red de área ampliada definida por software (SD-WAN)**
  - Detección de aplicación
  - Aprovisionamiento sin contacto
  - Sin transporte
  - Administración central de la política
- **Red de Área Local extensible virtual (VXLAN)**
  - Interconexión de centro de datos (DCI)
  - Encapsulación de capa 2
- **Arquitectura de Confianza cero (ZTA)**
  - Autenticación basada en políticas
  - Autorización
  - Acceso de mínimo privilegio
- **Secure Access Secure Edge (SASE)/ Security Service Edge (SSE)**
- **Infraestructura como código (IaC)**
  - Automatización
    - Tareas reutilizables de Playbooks/plantillas/
    - Desfase/cumplimiento de configuración
    - Actualizaciones
    - Inventarios dinámicos
  - Control de fuente
    - Control de versiones
    - Repositorio central
    - Identificación de conflictos
    - Branching
- **Dirección IPv6**
  - Mitigación de agotamiento de direcciones
  - Requisitos de compatibilidad
  - Tunelización
  - Dual stack
  - NAT64

2.0 Implementaciones de red

2.1 Explicar las características de las tecnologías de enrutamiento.

- Enrutamiento estático
- Enrutamiento dinámico
  - Protocolo de Enrutamiento de Frontera (BGP)
  - Protocolo de Enrutamiento de Gateway Interior Mejorado (EIGRP)
  - Ruta Abierta Más Corta Primero (OSPF)
- Selección de ruta
  - Distancia administrativa
  - Longitud del prefijo
  - Métrica
- Traducción de dirección
  - NAT
  - Traducción de Dirección de Puerto (PAT)
- First Hop Redundancy Protocol (FHRP)
- IP virtual (VIP)
- Subinterfaces

2.2 Dado un escenario, configurar tecnologías y características de conmutación.

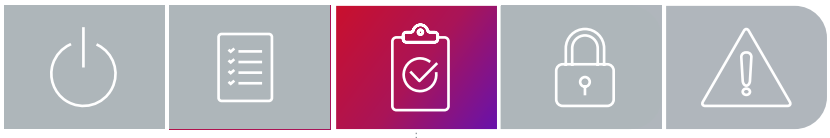
- Red de Área Local Virtual (VLAN)
  - Base de datos VLAN
  - Interfaz de conmutador virtual (SVI)
- Configuración de interfaz
  - VLAN nativa
  - VLAN de voz
  - Etiquetado de 802.1Q
  - Agregación de enlaces
  - Velocidad
  - Dúplex
- Árbol de expansión
- Unidad Máxima de Transmisión (MTU)
  - Jumbo frames

2.3 Dado un escenario, seleccionar y configurar dispositivos y tecnologías inalámbricas.

- Canales
  - Ancho del canal
  - Canales no superpuestos
  - Impactos regulatorios
    - 802.11 h
- Opciones de frecuencia
  - 2.4GHz
  - 5GHz
  - 6GHz
  - Band steering
- Identificador de Conjunto de Servicios (SSID)
  - Identificador de Conjunto de Servicios Básicos (BSSID)
  - Identificador Extendido de Conjunto de Servicios (ESSID)
- Tipos de red
  - Redes de mallas
  - Ad hoc
  - Punto a punto
  - Infraestructura
- Cifrado
  - Acceso Protegido Wi-Fi 2 (WPA2)
  - WPA3
- Redes de invitados
  - Portales cautivos
- Autenticación
  - Clave previamente compartida (PSK) vs. empresarial
- Antenas
  - Omnidireccional vs. direccional
- Punto de acceso autónomo vs. liviano

2.4 Explicar factores importantes de las instalaciones físicas.

- **Importantes implicaciones de la instalación**
  - Ubicaciones
    - Repartidor Intermedio (IDF)
    - Repartidor Principal (MDF)
  - Tamaño de gabinete
  - Escape/admisión lateral
  - Cableado
    - Patch panel
    - Panel de distribución de fibra
  - Bloqueable
- **Energía**
  - Fuente de alimentación ininterrumpida (UPS)
  - Unidad de distribución de energía (PDU)
  - Carga de energía
  - Voltaje
- **Factores ambientales**
  - Humedad
  - Supresión de incendios
  - Temperatura



3.0 Operaciones de redes

3.1 Explicar el objetivo de los procesos y procedimientos organizacionales.

- **Documentación**
  - Diagramas físicos vs. lógicos
  - Diagramas de rack
  - Mapas y diagramas de cables
  - Diagramas de red
    - Capa 1
    - Capa 2
    - Capa 3
  - Inventario de activos
    - Hardware
    - Software
    - Licencias
    - Soporte de garantía
  - Administración de direcciones IP (IPAM)
  - Acuerdo de Nivel de Servicio (SLA)
  - Encuesta inalámbrica/ mapa de calor
- **Administración de ciclo de vida**
  - End-of-life (EOL)
  - Fin del soporte (EOS)
  - Administración de software
    - Parches y corrección de errores
    - Sistema operativo (OS)
    - Firmware
  - Dar de baja
- **Administración de cambios**
  - Seguimiento de proceso de solicitud/solicitud de servicio
- **Administración de la configuración**
  - Configuración de producción
  - Configuración de copia de seguridad
  - Configuración de línea de base/superior

3.2 Dado un escenario, utilizar las tecnologías de monitoreo de red.

- **Métodos**
  - SNMP
    - Trampas
    - Base de Información de Administración (MIB)
    - Versiones
      - v2c
      - v3
    - Cadenas de comunidad
    - Autenticación
  - Datos de flujo
  - Captura de paquetes
  - Métrica de línea de base
    - Notificación/alerta de anomalía
  - Agregación de bitácoras
    - Recolector de bitácoras
    - Información de seguridad y administración de eventos (SIEM)
  - Integración de interfaz de programación de aplicación (API)
  - Replicación de puerto
- **Soluciones**
  - Descubrimiento de red
    - Ad hoc
    - Programado
  - Análisis de tráfico
  - Monitoreo de desempeño
  - Monitoreo de disponibilidad
  - Monitoreo de configuración

3.3 Explicar los conceptos de recuperación de desastres (DR).

- **Métrica de DR**
  - Punto objetivo de recuperación (RPO)
  - Tiempo objetivo de recuperación (RTO)
  - Tiempo medio de reparación (MTTR)
  - Tiempo medio entre fallos (MTBF)
- **Sitios de DR**
  - Cold site
  - Warm site
  - Hot site
- **Enfoques de alta disponibilidad**
  - Activo-activo
  - Activo/pasivo
- **Prueba**
  - Ejercicio de simulación
  - Pruebas de validación

3.4 Dado un escenario, implementar servicios de red IPv4 y IPv6.

- **Enrutamiento dinámico**
  - DHCP
    - Reservaciones
    - Alcance
    - Tiempo de asignación
    - Opciones
    - Transmisión/IP helper
    - Exclusiones
  - Configuración automática de direcciones sin estado (SLAAC)
- **Resolución de nombres**
  - DNS
    - Extensiones de seguridad de nombre de dominio (DNSSEC)
    - DNS por HTTPS (DoH) y DNS por TLS (DoT)
    - Tipos de registro
      - Dirección (A)
      - AAAA
      - Nombre Canónico (CNAME)
      - Intercambiador de Correo (MX)
      - Texto (TXT)
      - Nameserver (NS)
      - Puntero (PTR)
    - Tipos de zona
      - Adelante
      - Hacia atrás
    - Autoritativo vs. no autoritativo
    - Primario vs. secundario
    - Recursivo
  - Archivo Hosts
- **Protocolos de hora**
  - NTP
  - Protocolo de precisión de hora (PTP)
  - Seguridad de hora de red (NTS)

3.5 Comparar y contrastar el acceso de red y los métodos de administración.

- **VPN de sitio a sitio**
- **VPN de cliente a sitio**
  - Sin cliente
  - Túnel dividido vs. túnel completo
- **Métodos de conexión**
  - SSH
  - Interfaz gráfica del usuario (GUI)
  - API
  - Consola
- **Jump box/host**
- **Administración de banda vs. fuera de banda**

4.0 Seguridad de red

4.1 Explicar la importancia de los conceptos básicos de seguridad de red.

- **Seguridad lógica**
  - Cifrado
    - Datos en tránsito
    - Datos en reposo
  - Certificados
    - Infraestructura de Clave Pública (PKI)
    - Auto-firmado
  - Administración de identidad y acceso (IAM)
    - Autenticación
      - Autenticación de multifactores (MFA)
      - Inicio de sesión único (SSO)
      - Servicio de autenticación remota de usuario por acceso telefónico (RADIUS)
      - LDAP
      - Lenguaje de marcado de aserción de seguridad (SAML)
      - Controlador de acceso a terminal Sistema de control de acceso Plus (TACACS+)
      - Autenticación basada en el tiempo
    - Autorización
      - Menor privilegio
      - Control de acceso basado en roles
  - Geofencing
- **Seguridad física**
  - Cámara
  - Cerraduras

  Tecnologías de engaño
  - Honeypot
  - Honeynet
- **Terminología común de seguridad**
  - Riesgo
  - Vulnerabilidad
  - Explotaciones
  - Amenaza
  - Confidencialidad, integridad y disponibilidad (CIA)
- **Cumplimiento regulatorio y de auditorías**
  - Ubicación de datos
  - Estándares de seguridad de datos para la industria de tarjetas de pago (PCI DSS)
  - Reglamento General de Protección de Datos (GDPR)
- **Cumplimiento de segmentación de red**
  - Internet de las cosas (IoT) e Internet de las cosas industrial (IIoT)
  - Adquisición de datos y control de supervisión (SCADA), sistema de control industrial (ICS), tecnología operacional (OT)
  - Invitado
  - Trae Tu Propio Dispositivo (BYOD)

4.2 Resumir los diversos tipos de ataques y su impacto en la red.

- **Denegación de servicio (DoS)/ denegación de servicio distribuido (DDoS)**
- **Ensanchamiento de VLAN**
- **Desbordamiento de Media Access Control (MAC)**
- **Envenenamiento del Address Resolution Protocol (ARP)**
- **ARP spoofing**
- **Envenenamiento de DNS**
- **DNS spoofing**
- **Dispositivos y servicios malintencionados**
  - DHCP
  - AP
- **Evil twin**
- **Ataque en ruta**
- **Ingeniería social**
  - Phishing
  - Buscar en la basura
  - Fisgoneo
  - Infiltración
- **Malware**

4.3 Dado un escenario, aplicar características de seguridad de red, técnicas y soluciones de defensa.

- Protección de dispositivos
  - Deshabilitar puertos y servicios no usados
  - Cambiar contraseñas predeterminadas
- Control de acceso de red (NAC)
  - Seguridad de puertos
  - 802.1X
  - Filtrado MAC
- Administración de claves
- Reglas de seguridad
  - Lista de control de acceso (ACL)
  - Filtrado de Localizador uniforme de recursos (URL)
  - Filtrado de contenido
- Zonas
  - Confiables vs. no confiables
  - Subred analizada

5.0 Resolución de problemas de red

5.1 Explicar la metodología de resolución de problemas.

- Identificar el problema
  - Reunir información
  - Preguntar a los usuarios
  - Identificar síntomas
  - Determinar si algo ha cambiado
  - Replicar el problema, si es posible
  - Abordar múltiples problemas individualmente
- Establecer una teoría de la causa probable
  - Preguntarse por lo obvio
  - Considerar enfoques múltiples
    - Modelo OSI de arriba hacia abajo/de abajo hacia arriba
    - Dividir y conquistar
- Probar la teoría para determinar la causa
  - Una vez confirmada la teoría, determinar los próximos pasos para resolver el problema
  - Si la teoría no se confirma, reestablecer una nueva teoría o escalar
- Establecer un plan de acción para resolver el problema e identificar los efectos potenciales
- Implementar la solución o escalar, según sea necesario
- Verificar la funcionalidad completa del sistema e implementar medidas preventivas, si es aplicable
- Documentar conclusiones,acciones, resultados y lecciones aprendidas durante el proceso

5.2 Dado un escenario, solucionar problemas comunes con el cableado y problemas de interfaz física.

- Problemas de cables
  - Cable incorrecto
    - Modo simple vs. multimodo
    - Categoría 5/6/7/8
    - Par Trenzado con Blindaje (STP) vs. Par trenzado sin blindaje (UTP)
  - Degradación de la señal
    - Diafonía
    - Interferencia
    - Atenuación
  - Término inadecuado
  - Transmisor (TX)/ Receptor (RX) transpuesto
- Problemas de interfaz
  - Aumentando conteo de interfaz
    - Cyclic redundancy check (CRC)
    - Runts
    - Giants
    - Caídas
  - Estado de puerto
    - Error deshabilitado
    - Administrativamente caído
    - Suspendido
- Problemas de hardware
  - Alimentación sobre Ethernet (PoE)
    - Presupuesto de energía excedido
    - Estándar incorrecto
  - Transceiver
    - Error de coincidencia
    - Intensidad de la señal

5.3 Dado un escenario, solucionar problemas comunes con servicios de red.

- **Problemas de conmutación**
  - STP
    - Bucles de red
    - Selección de Root bridge
    - Roles de puerto
    - Estados de puerto
  - Asignación de VLAN incorrecta
  - ACL
- **Selección de ruta**
  - Tabla de enrutamiento
  - Rutas predeterminadas
- **Agotamiento de conjunto de direcciones**
- **Puerta de enlace predeterminada incorrecta**
- **Dirección IP incorrecta**
  - Dirección IP duplicada
- **Máscara de subred incorrecta**

5.4 Dado un escenario, resolver problemas comunes de desempeño.

- **Congestión/contención**
- **Cuello de botella**
- **Ancho de banda**
  - Capacidad de rendimiento
- **Latencia**
- **Pérdida de paquetes**
- **Fluctuación**
- **Inalámbrica**
  - Interferencia
    - Superposición de canales
  - Degradación o pérdida de la señal
  - Cobertura inalámbrica insuficiente
  - Problemas de disociación de clientes
  - Mala configuración de roaming

5.5 Dado un escenario, usar la herramienta o protocolo apropiado para resolver los problemas de red.

- **Herramientas de software**
  - Analizador de protocolo
  - Línea de comando
    - ping
    - traceroute/tracert
    - nslookup
    - tcpdump
    - dig
    - netstat
    - ip/ifconfig/ipconfig
    - arp
  - Nmap
  - Protocolo de descubrimiento de capa en enlace (LLDP)/Protocolo de descubrimiento Cisco (CDP)
  - Tester de velocidad
- **Herramientas de hardware**
  - Tóner
  - Tester de cables
  - Taps
  - Analizador WiFi
  - Localizador visual de fallas
- **Comandos básicos de dispositivos de red**
  - show mac-address-table
  - show route
  - show interface
  - show config
  - show arp
  - show vlan
  - show power

Lista de siglas de CompTIA Network+ N10-009

A continuación, hay una lista de siglas que aparecen en el examen de CompTIA Network+ N10-009. Se insta a los candidatos a revisar la lista completa y alcanzar un conocimiento práctico de todas las siglas listadas, como parte de un programa completo de preparación para el examen.

SIGLAS	FRASE COMPLETA
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
ESP	Encapsulating Security Payload

SIGLAS	FRASE COMPLETA
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
PAT	Port Address Translation

SIGLAS	FRASE COMPLETA
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
URL	Uniform Resource Locator

SIGLAS	FRASE COMPLETA
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

Lista propuesta de hardware y software para CompTIA Network+

CompTIA ha incluido esta lista de muestra de hardware y software para asistir a los candidatos mientras se preparan para el examen de Network+. Esta lista también puede ser útil para capacitar a las empresas que desean crear un componente de laboratorio en su oferta de capacitación.
Las listas con viñetas debajo de cada tema son una lista de muestra y no completas.

EQUIPOS

- Patch panel óptico y de cobre
- Switch Capa 3/switch administrado/ switch PoE
- Enrutador
- Firewall
- Punto de acceso inalámbrico
- Computadoras portátiles básicas que admiten virtualización
- Teléfono de voz sobre IP (VoIP)

HARDWARE DE REPUESTO

- Tarjeta de Interfaz de red (NIC)
- Fuentes de energía
- SFP
- Punto de acceso inalámbrico
- UPS
- Inyector PoE

PARTES DE REPUESTO

- Cables de parches
  - Fibra
  - Cobre
- Antenas
- Adaptadores inalámbricos/Bluetooth
- Cables de consola [Bus serial universal (USB) para RS-232 adaptador serial]
- NIC/USB NIC adicional

HERRAMIENTAS

- Tester de cable
- Generador de tono
- Medidor de potencia óptica
- Tester PoE

SOFTWARE

- Analizador de protocolo/Captura de paquetes
- Software de emulación de terminal
- Sistemas operativos Linux/Windows
- Firewall de software
- Software IDS/IPS
- Mapeador de red
- Software hipervisor
- Cuentas de demostración/lab de nube IaaS
- Entorno virtual de red
- Analizador WiFi
- Analizador de espectro
- Herramientas de monitoreo de red
- Analizador de datos de flujo
- Servidor TFTP
- Diversas versiones de firmware

OTRA

- Documentación de red de muestra
- Registros de muestra
- Cables defectuosos
- Diagramas de red en la nube
- Playbook/runbook de configuración de muestra

CompTIA