CompTIA Network+ CERTIFICATION Plus Series

Objetivos do Exame de Certificação CompTIA Network+

NÚMERO DO EXAME: N10-009

CompTIA

Sobre o exame

O exame de certificação CompTIA Network+ certificará que o candidato aprovado tem o conhecimento e as habilidades necessárias para:

- Estabelecer conectividade de rede ao implantar dispositivos com e sem fio.
- Explicar o propósito da documentação e manter a documentação da rede.
- Configurar serviços de rede comuns.
- Explicar os conceitos básicos de data center, nuvem e rede virtual.
- Monitorar a atividade da rede e solucionar problemas de desempenho e de disponibilidade.
- Implementar técnicas de hardening de segurança de rede.
- Gerenciar, configurar e solucionar problemas de infraestrutura de rede.

ELABORAÇÃO DO EXAME

O resultado dos exames CompTIA é proveniente de workshops especializados e focados no assunto e pesquisas abrangentes em toda a indústria quanto às habilidades e conhecimentos exigidos de um profissional de TI.

POLÍTICA DE USO AUTORIZADO DE MATERIAIS DA COMPTIA

A CompTIA Certifications, LLC não está afiliada a, nem autoriza, endossa ou admite o uso de qualquer conteúdo fornecido por sites de treinamento externos não autorizados (também conhecidos como “brain dumps”). Os candidatos que usarem esses materiais como preparação para qualquer exame da CompTIA terão suas certificações anuladas e serão suspensos de futuros testes de acordo com o Contrato do Candidato CompTIA. Com o intuito de comunicar com maior clareza as políticas dos exames CompTIA referentes ao uso de materiais de estudo não autorizados, a CompTIA encaminha todos os candidatos à certificação para as Políticas do Exame de Certificação da CompTIA. Leia todas as políticas da CompTIA antes de iniciar o processo de estudo para qualquer exame CompTIA. Os candidatos serão obrigados a respeitar o Contrato do Candidato CompTIA. Se um candidato não tiver certeza se determinado material de estudo é considerado não autorizado (conhecido como “brain dump”), deverá entrar em contato com a CompTIA pelo e-mail examsecurity@comptia.org para confirmação.

OBSERVAÇÃO

As listas de exemplos fornecidas em formato de marcadores não são listas abrangentes. Outros exemplos de tecnologias, processos ou tarefas pertinentes a cada objetivo podem ser incluídos no exame, embora não estejam listados ou cobertos neste documento de objetivos. A CompTIA revisa constantemente o conteúdo de seus exames e atualiza as perguntas para assegurar que sejam atuais, e que a segurança das perguntas estejam protegidas. Quando necessário, publicaremos exames atualizados baseados nos objetivos do exame existentes. Lembre-se que todos os materiais de preparação dos exames ainda serão válidos.

DETALHES DO TESTE

Exame exigido	N10-009
Número de perguntas	No máximo 90
Tipos de perguntas	Múltipla escolha e baseadas em desempenho
Duração do teste	90 minutos
Experiência recomendada	Mínimo de 9 a 12 meses de experiência na área de redes de TI

OBJETIVOS DO EXAME (DOMÍNIOS)

A tabela abaixo lista os domínios avaliados por este exame e o peso que cada um representa.

DOMÍNIO		PORCENTAGEM DO EXAME
1.0	Conceitos de rede	23%
2.0	Implementação de redes	20%
3.0	Operações de redes	19%
4.0	Segurança de rede	14%
5.0	Resolução de problemas de rede	24%
Total		**100%**

1.0 Conceitos de rede

1.1 Explicar os conceitos relacionados ao modelo de referência Open Systems Interconnection (OSI).

- Camada 1 - Física
- Camada 2 - Enlace de dados
- Camada 3 - Rede
- Camada 4 - Transporte
- Camada 5 - Sessão
- Camada 6 - Apresentação
- Camada 7 - Aplicaçã

1.2 Comparar e contrastar dispositivos de rede, aplicativos e funções.

- **Dispositivos físicos e virtuais**
  - Roteador
  - Switch
  - Firewall
  - Sistema de detecção de intrusão (IDS)/sistema de prevenção de intrusão (IPS)
  - Balanceador de carga
  - Proxy
  - Armazenamento conectado à rede (NAS)
  - Rede de área de armazenamento (SAN)
  - Sem fio
    - Ponto de acesso (AP)
    - Controlador
- **Aplicações**
  - Rede de entrega de conteúdo (CDN)
- **Funções**
  - Rede privada virtual (VPN)
  - Qualidade de serviço (QoS)
  - Tempo de vida (TTL)

1.3 Resumir conceitos de nuvem e opções de conectividade.

- **Virtualização de funções de rede (NFV)**
- **Nuvem privada virtual (VPC)**
- **Grupos de segurança de rede**
- **Listas de segurança de rede**
- **Gateways de nuvem**
  - Gateway de internet
  - Gateway de Conversão de endereço de rede (NAT)
- **Opções de conectividade em nuvem**
  - VPN
  - Conexão direta
- **Modelos de implantação**
  - Público
  - Privado
  - Híbrido
- **Modelos de serviço**
  - Software como Serviço (SaaS)
  - Infraestrutura como Serviço (IaaS)
  - Plataforma como Serviço (PaaS)
- **Escalabilidade**
- **Elasticidade**
- **Multilocatário**

1.4 Explicar portas de rede, protocolos, serviços e tipos de tráfego comuns.

Protocolos	Portas
Protocolo de transferência de arquivo (FTP)	20/21
Protocolo de transferência segura de arquivo (SFTP)	22
Secure Shell (SSH)	22
Telnet	23
Protocolo de transferência de correio simples (SMTP)	25
Sistema de nomes de domínio (DNS)	53
Protocolo de configuração de host dinâmico (DHCP)	67/68
Protocolo de transferência de arquivo trivial (TFTP)	69
Protocolo de transferência de hipertexto (HTTP)	80
Protocolo de tempo de rede (NTP)	123
Protocolo de gerenciamento de rede simples (SNMP)	161/162
Protocolo de acesso do diretório leve (LDAP)	389
Protocolo de transferência de hipertexto seguro (HTTPS)	443
Bloco de mensagens do servidor (SMB)	445
Syslog	514
Protocolo de transferência de correio simples seguro (SMTPS)	587
Protocolo de acesso do diretório leve sobre SSL (LDAPS)	636
Servidor de linguagem de consulta estruturada (SQL)	1433
Protocolo de área de trabalho remota (RDP)	3389
Protocolo de iniciação de sessão (SIP)	5060/5061

- Tipos de Protocolo da Internet (IP)
  - Protocolo de mensagem de controle de internet (ICMP)
  - Protocolo de controle de transmissão (TCP)
  - Protocolo de datagrama de usuário (UDP)
  - Encapsulamento de roteamento genérico (GRE)
  - Segurança de protocolo de internet (IPSec)
    - Cabeçalho de autenticação (AH)
    - Carga útil de segurança encapsulada (ESP)
    - Troca de chaves via Internet (IKE)
- Tipos de tráfego
  - Unicast
  - Multicast
  - Anycast
  - Broadcast

1.5 Comparar e contrastar meios de transmissão e transceptores.

- Sem fio
  - Padrões 802.11
  - Celular
  - Satélite
- Com fio
  - Padrões 802.3
  - Fibra modo único vs. multimodo
  - Cabo de Cobre de conexão direta (DAC)
    - Cabo biaxial
  - Cabo coaxial
  - Velocidades do cabo
  - Cabo plenum vs. cabo não plenum
- Transceptores
  - Protocolo
    - Ethernet
    - Canal de fibra (FC)
  - Form factors
    - Small form-factor pluggable (SFP)
    - Quad small form-factor pluggable (QSFP)
- Tipos de conector
  - Subscriber connector (SC)
  - Local connector (LC)
  - Straight tip (ST)
  - Multi-fiber push on (MPO)
  - RJ11
  - RJ45
  - Conector tipo F
  - Bayonet Neill–Concelman (BNC)

1.6 Comparar e contrastar topologias, arquiteturas e tipos de rede.

- Malha
- Híbrido
- Estrela/hub e spoke
- Spine-leaf
- Ponto a ponto
- Modelo hierárquico de três camadas
  - Núcleo
  - Distribuição
  - Acesso
- Núcleo colapsado
- Fluxos de tráfego
  - Norte-Sul
  - Leste-Oeste

1.7 Considerando determinado cenário, usar o endereçamento de rede IPv4 apropriado.

- Pública vs. privada
  - Endereçamento IP privado automático (APIPA)
  - RFC1918
  - Loopback/localhost
- Sub-rede
  - Máscara de sub-rede de comprimento variável (VLSM)
  - Classless Inter-domain Routing (CIDR)
- Classes de endereço IPv4
  - Classe A
  - Classe B
  - Classe C
  - Classe D
  - Classe E

1.8 Resumir os casos de uso em evolução para ambientes de rede modernos.

- **Rede definida por software (SDN) e Rede de longa distância definida por software (SD-WAN)**
  - Aplicação Consciente
  - Provisionamento de toque zero
  - Transporte Agnóstico
  - Gerenciamento central de políticas
- **Rede de área local extensível virtual (VXLAN)**
  - Interconexão de data center (DCI)
  - Encapsulamento de camada 2
- **Arquitetura de confiança zero (ZTA)**
  - Autenticação baseada em políticas
  - Autorização
  - Acesso com privilégio mínimo
- **Borda segura de acesso seguro (SASE)/Borda de serviço de segurança (SSE)**
- **Infraestrutura como código (IaC)**
  - Automação
    - Playbooks/modelos/tarefas reutilizáveis
    - Desvio de configuração/conformidade
    - Upgrades
    - Inventários dinâmicos
  - Controle de origem
    - Controle de versões
    - Repositório central
    - Identificação de conflitos
    - Ramificação
- **Endereço IPv6**
  - Mitigação de esgotamento de endereços
  - Requisitos de compatibilidade
    - Tunelamento
    - Pilha dupla
    - NAT64

2.0 Implementação de rede

2.1 Explicar as características das tecnologias de roteamento.

- Roteamento estático
- Roteamento dinâmico
  - Border Gateway Protocol (BGP)
  - Enhanced Interior Gateway Routing Protocol (EIGRP)
  - Open Shortest Path First (OSPF)
- Seleção de rota
  - Distância administrativa
  - Comprimento do prefixo
  - Métrica
- Conversão de endereço
  - NAT
  - Conversão de endereço de porta (PAT)
- First Hop Redundancy Protocol (FHRP)
- IP Virtual (VIP)
- Subinterfaces

2.2 Considerando determinado cenário, configurar tecnologias e recursos de comutação.

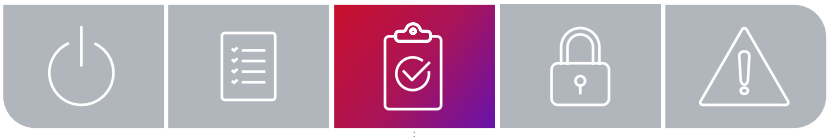
- Rede de área local virtual (VLAN)
  - Banco de dados VLAN
  - Interface do switch virtual (SVI)
- Configuração de interface
  - VLAN nativa
  - VLAN de voz
  - Marcação 802.1Q
  - Agregação de links
  - Velocidade
  - Duplex
- Spanning tree
- Unidade máxima de transmissão (MTU)
  - Quadros jumbo

2.3 Considerando determinado cenário, selecionar e configurar dispositivos e tecnologias sem fio.

- Canais
  - Largura do canal
  - Canais não sobrepostos
  - Impactos regulatórios
    - 802.11h
- Opções de frequência
  - 2.4 GHz
  - 5 GHz
  - 6 GHz
  - Direcionamento de banda
- Identificador de conjunto de serviços (SSID)
  - Identificador de conjunto de serviços básicos (BSSID)
  - Identificador de conjunto de serviços estendidos (ESSID)
- Tipos de rede
  - Redes mesh
  - Ad hoc
  - Ponto a ponto
  - Infraestrutura
- Criptografia
  - Acesso protegido Wi-Fi 2 (WPA2)
  - WPA3
- Redes de convidados
  - Portais cativos
- Autenticação
  - Chave pré-compartilhada (PSK) vs. empresarial
- Antenas
  - Omnidirecional vs. direcional
- Autonomous vs. lightweight access point

2.4 Explicar fatores importantes das instalações físicas.

- **Implicações importantes de instalação**
  - Locais
    - Quadro de distribuição intermediário (IDF)
    - Quadro de distribuição principal (MDF)
  - Tamanho do rack
  - Entrada/saída no lado da porta
  - Cabeamento
    - Painel de conexões
    - Painel de distribuição de fibra
  - Fechaduras
- **Alimentação**
  - Fonte de energia ininterrupta (UPS)
  - Unidade de distribuição de energia (PDU)
  - Carga de energia
  - Tensão
- **Fatores ambientais**
  - Umidade
  - Supressão de incêndio
  - Temperatura



3.0 Operações de redes

3.1 Explicar o propósito dos processos e procedimentos organizacionais.

- **Documentação**
  - Diagramas físicos vs. lógicos
  - Diagrama de rack
  - Mapas e diagramas de cabos
  - Diagramas de rede
    - Camada 1
    - Camada 2
    - Camada 3
  - Inventário de ativos
    - Hardware
    - Software
    - Licenciamento
    - Suporte a garantia
  - Gerenciamento de endereço IP (IPAM)
  - Contrato de nível de serviço (SLA)
  - Wireless survey/heat map
- **Gerenciamento do ciclo de vida**
  - Fim da vida útil (EOL)
  - Fim do suporte (EOS)
  - Gerenciamento de software
    - Patches e correções de bugs
    - Sistema operacional (OS)
    - Firmware
  - Descomissionamento
- **Gestão de mudanças**
  - Acompanhamento do processo de solicitação/solicitação de serviço
- **Gerenciamento de configurações**
  - Configuração de produção
  - Configuração de backup
  - Baseline/golden configuration

3.2 Considerando determinado cenário, usar tecnologias de monitoramento de rede.

- **Métodos**
  - SNMP
    - Traps
    - Management information base (MIB)
    - Versões
      - v2c
      - v3
    - Community strings
    - Autenticação
  - Flow data
  - Captura de pacote
  - Métricas de baseline
    - Alerta/notificação de anomalia
  - Agregação de log
    - Coletor Syslog
    - Gerenciamento de eventos e informações de segurança (SIEM)
  - Integração da Interface de programação de aplicativos (API)
  - Espelhamento de portas
- **Soluções**
  - Descoberta de rede
    - Ad hoc
    - Programado
  - Análise de tráfego
  - Monitoramento de desempenho
  - Monitoramento de disponibilidade
  - Monitoramento de configuração

3.3 Explicar os conceitos de recuperação de desastres (DR).

- **Métricas de DR**
  - Objetivo de ponto de recuperação (RPO)
  - Objetivo de tempo de recuperação (RTO)
  - Tempo médio de reparo (MTTR)
  - Tempo médio entre falhas (MTBF)
- **Sites de DR**
  - Cold site
  - Warm site
  - Hot site
- **Abordagens de alta disponibilidade**
  - Ativo-ativo
  - Ativo-passivo
- **Testes**
  - Teste de mesa
  - Testes de validação

3.4 Considerando determinado cenário, implementar serviços de rede IPv4 e IPv6.

- **Endereçamento dinâmico**
  - DHCP
    - Reservas
    - Escopo
    - Tempo de concessão
    - Opções
    - Relé / Auxiliar de IP
    - Exclusões
  - Configuração automática de endereço sem estado (SLAAC)
- **Resolução de nomes**
  - DNS
    - Extensões de segurança de nomes de domínio (DNSSEC)
    - DNS sobre HTTPS (DoH) e DNS sobre TLS (DoT)
    - Tipos de registros
      - Endereço (A)
      - AAAA
      - Nome canônico (CNAME)
      - Servidor de mensagens (MX)
      - Texto (TXT)
      - Nameserver (NS)
      - Ponteiro (PTR)
    - Tipos de zona
      - Encaminhamento
      - Reverso
    - Autoritativo vs. não autoritativo
    - Primário vs. secundário
    - Recursivo
  - Arquivo de hosts
- **Protocolos de tempo**
  - NTP
  - Protocolo de tempo de precisão (PTP)
  - Segurança de tempo de rede (NTS)

3.5 Comparar e contrastar os métodos de acesso e gerenciamento de rede.

- **VPN site a site**
- **VPN de cliente para site**
  - Sem cliente
  - Túnel dividido vs. túnel completo
- **Métodos de conexão**
  - SSH
  - Interface gráfica do usuário (GUI)
  - API
  - Console
- **Jump box/host**
- **Gerenciamento in-band vs. out-of-band**

4.0 Segurança de rede

4.1 Explicar a importância dos conceitos básicos de segurança de rede.

- Segurança lógica
  - Criptografia
    - Dados em trânsito
    - Dados em repouso
  - Certificados
    - Infraestrutura de chave pública (PKI)
    - Autoassinado
  - Gerenciamento de identidade e acesso (IAM)
    - Autenticação
      - Autenticação multifator (MFA)
      - Logon único (SSO)
      - Serviço de usuário discado de autenticação remota (RADIUS)
      - LDAP
      - Linguagem de marcação de asserção de segurança (SAML)
      - sistema de controle de acesso do controlador de acesso de terminal (TACACS+)
      - Autenticação baseada em tempo
    - Autorização
      - Privilégio mínimo
      - Controle de acesso baseado em função
  - Delimitação geográfica

- Segurança física
  - Câmera
  - Bloqueios

- Tecnologias Deception
  - Honeypot
  - Honeynet

- Terminologia de segurança comum
  - Risco
  - Vulnerabilidade
  - Exploração
  - Ameaça
  - Confidencialidade, integridade e disponibilidade (CIA)

- Auditorias e conformidade regulatória
  - Localidade dos dados
  - Padrão de Segurança de Dados da Payment Card Industry (PCI DSS)
  - Regulamento Geral de Proteção de Dados (GDPR)

- Aplicação de segmentação de rede
  - Internet das Coisas (IoT) e Internet das Coisas Industrial (IIoT)
  - Controle de supervisão e aquisição de dados (SCADA), Sistema de controle industrial (ICS), Tecnologia operacional (OT)
  - Visitante
  - Traga seu próprio aparelho (BYOD)

4.2 Resumir vários tipos de ataques e respectivos impactos na rede.

- Negação de serviço (DoS)/Negação de serviço distribuído (DDoS)
- Salto de VLAN
- Inundação de Controle de acesso de mídia (MAC flooding)
- Envenenamento de Protocolo de resolução de endereço (ARP poisoning)
- Falsificação de ARP
- Envenenamento de DNS
- Falsificação de DNS
- Dispositivos e serviços não autorizados
  - DHCP
  - AP

- Evil twin
- Ataque on-path

- Engenharia social
  - Phishing
  - Dumpster diving
  - Shoulder surfing
  - Tailgating

- Malware

4.3 Considerando determinado cenário, aplicar recursos de segurança de rede, técnicas de defesa e soluções.

- Hardening de dispositivo
  - Desabilitar portas e serviços não utilizados
  - Alterar senhas padrão
- Controle de acesso de rede (NAC)
  - Segurança de porta
  - 802.1X
  - Filtro de MAC
- Gerenciamento de chaves
- Regras de segurança
  - Lista de controle de acesso (ACL)
  - Filtragem do Localizador uniforme de recursos (URL)
  - Filtro de conteúdo
- Zonas
  - Confiável vs. não confiável
  - Sub-rede filtrada

5.0 Resolução de problemas de rede

5.1 Explicar a metodologia de resolução de problemas.

- **Identificar o problema**
  - Reunir informações
  - Fazer perguntas aos usuários
  - Identificar os sintomas
  - Determinar se algo mudou
  - Replicar o problema, se possível
  - Abordar vários problemas individualmente
- **Estabelecer uma teoria de causa provável**
  - Questionar o óbvio
  - Considerar várias abordagens
    - Modelo OSI de cima para baixo/de baixo para cima
    - Dividir e conquistar
- **Testar a teoria para determinar a causa**
  - Se a teoria for confirmada, determinar as próximas etapas para resolver o problema
  - Se a teoria não for confirmada, estabelecer uma nova teoria ou encaminhá-la para superiores
- **Estabelecer um plano de ação para resolver o problema e identificar possíveis efeitos**
- **Implementar a solução ou encaminhá-la para superiores conforme necessário**
- **Verificar a funcionalidade completa do sistema e implementar medidas preventivas, se aplicável**
- **Documentar constatações, ações, resultados e lições aprendidas ao longo do processo**

5.2 Considerando determinado cenário, solucionar problemas comuns de cabeamento e de interface física.

- **Problemas de cabo**
  - Cabo incorreto
    - Modo único vs. multimodo
    - Categoria 5/6/7/8
    - Par trançado blindado (STP) vs. par trançado não blindado (UTP)
  - Degradação de sinal
    - Crosstalk
    - Interferência
    - Atenuação
  - Terminação inadequada
  - Transmissor (TX)/ Receptor (RX) transposto
- **Problemas de interface**
  - Aumento de contadores de interface
    - Verificação cíclica de redundância (CRC)
    - Runts
    - Giants
    - Drops
  - Port status
    - Error disabled
    - Administratively down
    - Suspended
- **Problemas de hardware**
  - Power over Ethernet (PoE)
    - Orçamento de energia excedido
    - Padrão incorreto
  - Transceptores
    - Incompatibilidade
    - Intensidade do sinal

5.3 Considerando determinado cenário, solucionar problemas comuns com serviços de rede.

- **Problemas de comutação**
  - STP
    - Loops de rede
    - Root bridge selection
    - Funções das portas
    - Estados das portas
  - Atribuição de VLAN incorreta
  - ACLs
- **Seleção de rota**
  - Tabela de roteamento
  - Rotas padrão
- **Esgotamento do pool de endereços**
- **Gateway padrão incorreto**
- **Endereço IP incorreto**
  - Endereço IP duplicado
- **Máscara de sub-rede incorreta**

5.4 Considerando determinado cenário, solucionar problemas comuns de desempenho.

- **Congestionamento/contenção**
- **Gargalos**
- **Largura de banda**
  - Capacidade de transferência
- **Latência**
- **Perda de pacotes**
- **Jitter**
- **Wireless**
  - Interferência
    - Sobreposição de canal
  - Degradação ou perda de sinal
  - Cobertura sem fio insuficiente
  - Problemas de desassociação de cliente
  - Configuração incorreta de roaming

5.5 Considerando determinado cenário, usar a ferramenta ou protocolo apropriado para resolver problemas de rede.

- **Ferramentas de software**
  - Analisador de protocolo
  - Linha de comando
    - ping
    - traceroute/tracert
    - nslookup
    - tcpdump
    - dig
    - netstat
    - ip/ifconfig/ipconfig
    - arp
  - Nmap
  - Protocolo de descoberta de camada de link (LLDP)/Protocolo de descoberta Cisco (CDP)
  - Testador de velocidade
- **Ferramentas de hardware**
  - Toner
  - Testador de cabos
  - Taps
  - Analisador de Wi-Fi
  - Localizador visual de falhas
- **Comandos básicos do dispositivo de rede**
  - show mac-address-table
  - show route
  - show interface
  - show config
  - show arp
  - show vlan
  - show power

Lista de acrônimos CompTIA Network+ N10-009

Veja abaixo uma lista de acrônimos que aparecem no exame CompTIA Network+ N10-009. Os candidatos são incentivados a rever a lista completa e a obter conhecimentos de todos os acrônimos listados como parte de um programa de preparação abrangente para o exame.

ACRÔNIMO	ESCRITO POR EXTENSO
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
ESSID	Extended Service Set Identifier

ACRÔNIMO	ESCRITO POR EXTENSO
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

ACRÔNIMO	ESCRITO POR EXTENSO
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

ACRÔNIMO	ESCRITO POR EXTENSO
UDP	User Datagram Protocol
UPS	Uninterruptible Power Supply
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

Lista de hardware e software propostos para CompTIA Network+

A CompTIA incluiu esta lista de exemplos de hardware e software para ajudar os candidatos a se prepararem para o exame Network+. Esta lista também pode ser útil para as empresas de treinamento que pretendam criar um componente laboratorial para sua oferta de treinamento. As listas com marcadores abaixo de cada tópico são listas de exemplo e não são exaustivas.

EQUIPAMENTO

- Painéis de conexões ópticas e de cobre
- Switch de camada 3/switch gerenciado/switch PoE
- Roteador
- Firewall
- Ponto de acesso sem fio
- Notebooks básicos compatíveis com virtualização
- Telefone de voz sobre IP (VoIP)

HARDWARE SOBRESSALENTE

- Placa de interface de rede (NIC)
- Fontes de energia
- SFPs
- Ponto de acesso sem fio
- UPS
- Injetor PoE

PEÇAS SOBRESSALENTES

- Cabos de conexão
  - Fibra
  - Cobre
- Antenas
- Adaptadores Bluetooth/sem fio
- Cabos de console [Barramento universal serial (USB) para adaptador serial RS-232]
- NIC/ USB NIC adicional

FERRAMENTAS

- Testador de cabos
- Gerador de tons
- Medidor de potência óptica
- Testador PoE

SOFTWARE

- Analisador de protocolo/captura de pacotes
- Software de emulação de terminal
- Sistemas operacionais Linux/Windows
- Firewall de software
- Software IDS/IPS
- Mapeador de rede
- Software de hipervisor
- Laboratorio em nuvem IaaS/Contas de demonstracao
- Ambiente de rede virtual
- Analisador de Wi-Fi
- Analisador de espectro
- Ferramentas de monitoramento de rede
- Analisador de dados de fluxo
- Servidor TFTP
- Várias versões de firmware

OUTROS

- Exemplo de documentação de rede
- Logs de amostra
- Cabos com defeito
- Diagramas de rede na nuvem
- Exemplo de configuração playbook/runbook

CompTIA