examundo

Examen de práctica CompTIA Network+ en español

70 preguntas con respuestas. Las guías y las traducciones las hizo y las revisó un software. Ninguna persona las ha revisado todavía.

Actualizado el 25 de noviembre de 2026 · examundo.tech/es/comptia-network-plus/

Conceptos de redes

1. Los servidores raíz de DNS y muchos nodos de borde de CDN responden en la misma dirección IP desde muchos lugares del mundo, y la solicitud de cada cliente se enruta automáticamente a la instancia más cercana (en topología de red) que comparte esa dirección. ¿Qué esquema de direccionamiento permite este comportamiento?

DNS root servers and many CDN edge nodes are reachable at the same IP address from many physical locations worldwide, and each client's request is automatically routed to the topologically nearest instance sharing that address. Which addressing scheme enables this behavior?

A. Anycast
B. Broadcast
C. Unicast
D. Multicast

---

2. En el diseño de una red de centro de datos (data center), ¿con qué término de flujo de tráfico se clasifica el tráfico entre un cliente en internet y un servidor web alojado dentro del centro de datos?

In a data center network design, traffic that flows between a client on the internet and a web server hosted inside the data center is classified using which traffic flow term?

A. Tráfico solo de entrada (ingress-only)
B. Tráfico norte-sur (north-south)
C. Tráfico este-oeste (east-west)
D. Tráfico intra-VLAN

---

3. En una arquitectura spine-leaf de centro de datos, ¿qué tipo de flujo de tráfico describe la comunicación entre dos servidores conectados a distintos switches leaf dentro del mismo centro de datos?

In a spine-leaf data center architecture, which type of traffic flow describes communication between two servers connected to different leaf switches within the same data center?

A. Tráfico norte-sur (north-south)
B. Tráfico de entrada (ingress)
C. Tráfico de administración fuera de banda (out-of-band)
D. Tráfico este-oeste (east-west)

---

4. ¿Qué servicio de red asigna automáticamente direcciones IP, máscaras de subred, puertas de enlace predeterminadas y direcciones de servidores DNS a los equipos que se unen a una red?

Which network service automatically assigns IP addresses, subnet masks, default gateways, and DNS server addresses to hosts joining a network?

A. ARP
B. DHCP
C. NTP
D. DNS

---

5. Un sitio de comercio electrónico tiene respuestas lentas en las horas de más compras porque un solo servidor web no puede atender todas las solicitudes. ¿Qué dispositivo se debe implementar para repartir las solicitudes de los clientes entre varios servidores web?

An e-commerce site experiences slow response times during peak shopping hours because a single web server cannot handle all incoming requests. Which device should be implemented to distribute client requests across multiple web servers?

A. Switch de capa 2
B. Balanceador de carga
C. Firewall
D. Servidor proxy

---

6. La plataforma de comercio electrónico de una tienda crea automáticamente más instancias de cómputo en minutos cuando sube el tráfico en el Black Friday, y las elimina automáticamente cuando el tráfico vuelve a lo normal. ¿Qué característica de la nube describe esto?

A retail company's e-commerce platform automatically provisions additional compute instances within minutes as customer traffic spikes on Black Friday, then automatically de-provisions those instances once traffic returns to baseline. Which cloud characteristic does this describe?

A. Multiinquilino (multitenancy)
B. Alta disponibilidad (high availability)
C. Elasticidad (elasticity)
D. Escalabilidad (scalability)

---

7. ¿Qué servicio de red se encarga de convertir nombres de dominio legibles, como www.example.com, en direcciones IP?

Which network service is responsible for resolving human-readable domain names, such as www.example.com, into IP addresses?

A. DNS
B. NTP
C. DHCP
D. SNMP

---

8. Un ingeniero de redes relaciona protocolos de aplicación con el modelo OSI para una auditoría de seguridad. Según el modelo OSI definido por CompTIA, ¿en qué capa se realiza principalmente el cifrado y descifrado de TLS?

A network engineer is mapping application protocols to the OSI model for a security audit. According to the CompTIA-defined OSI model, at which layer does TLS encryption and decryption primarily occur?

A. Capa de sesión (capa 5)
B. Capa de presentación (capa 6)
C. Capa de transporte (capa 4)
D. Capa de aplicación (capa 7)

---

9. Un técnico configura una regla de firewall para permitir las consultas normales de resolución de nombres DNS de los clientes que salen de la red. ¿Qué combinación de protocolo y puerto se debe permitir?

A technician is configuring a firewall rule to permit standard client DNS name resolution queries leaving the network. Which protocol and port combination should be allowed?

A. TCP puerto 43
B. UDP puerto 53
C. TCP puerto 53
D. UDP puerto 67

---

10. Una empresa instala un sistema de VoIP que necesita baja latencia y tolera una pequeña pérdida de paquetes sin retransmisión. ¿Qué característica hace que UDP sea la MEJOR opción para esta aplicación frente a TCP?

A company is deploying a VoIP system that requires low latency and can tolerate minor packet loss without needing retransmission. Which characteristic makes UDP the BEST choice for this application over TCP?

A. UDP usa ventanas (windowing) para controlar el flujo de segmentos
B. UDP necesita mantener el estado de una conexión persistente por sesión
C. UDP hace un saludo de tres vías (three-way handshake) para garantizar el orden de entrega
D. UDP no tiene confirmaciones ni retransmisiones que agreguen sobrecarga

---

11. Un técnico captura tráfico y ve que un switch reenvía una trama basándose solo en la dirección de hardware de destino que contiene. ¿En qué capa OSI toma el switch esta decisión de reenvío?

A technician captures traffic and observes a switch forwarding a frame based solely on the destination hardware address contained within it. At which OSI layer is the switch performing this forwarding decision?

A. Capa 2 - Enlace de datos
B. Capa 4 - Transporte
C. Capa 3 - Red
D. Capa 7 - Aplicación

---

12. Un equipo de seguridad quiere instalar un dispositivo que no solo vigile el tráfico de red en busca de firmas de ataques conocidos, sino que además descarte automáticamente los paquetes maliciosos antes de que lleguen a la red interna. ¿Qué dispositivo debe implementar?

A security team wants to deploy an appliance that not only monitors network traffic for known attack signatures but also automatically drops malicious packets before they reach the internal network. Which appliance should the team implement?

A. Switch de capa 2
B. Sistema de detección de intrusiones (IDS)
C. Servidor proxy
D. Sistema de prevención de intrusiones (IPS)

---

13. Un técnico revisa la configuración IPv6 de la interfaz de un router y encuentra la dirección fd12:3456:789a:1::1/64. ¿Qué tipo de dirección IPv6 es?

A technician examines the IPv6 configuration on a router interface and finds the address fd12:3456:789a:1::1/64. Which type of IPv6 address is this?

A. Dirección unicast global
B. Dirección multicast
C. Dirección local única (unique local address)
D. Dirección de enlace local (link-local)

---

14. ¿Qué dispositivo de red reenvía paquetes de datos entre redes IP distintas según la dirección IP de destino?

Which network appliance forwards data packets between different IP networks based on the destination IP address?

A. Hub
B. Router
C. Puente (bridge)
D. Switch

Implementación de redes

15. Una oficina pequeña tiene una sola dirección IP pública de su proveedor, pero necesita que 15 equipos internos accedan a internet al mismo tiempo. ¿Qué tecnología del router de borde lo hace posible?

A small office has only one public IP address from its ISP but needs 15 internal devices to access the internet simultaneously. Which technology on the edge router makes this possible?

A. Solo una puerta de enlace de nivel de aplicación (application-level gateway)
B. NAT dinámico con un grupo uno a uno
C. NAT estático
D. Traducción de direcciones por puerto (PAT)

16. Un administrador debe dividir en subredes la red 192.168.10.0/24 para 6 enlaces WAN punto a punto separados, y cada enlace necesita solo 2 direcciones de host utilizables. ¿Qué máscara de subred aprovecha MEJOR el espacio de direcciones en cada enlace?

A network administrator must subnet the 192.168.10.0/24 network to support 6 separate point-to-point WAN links, with each link requiring only 2 usable host addresses. Which subnet mask provides the MOST efficient use of address space for each link?

A. 255.255.255.192 (/26)
B. 255.255.255.252 (/30)
C. 255.255.255.240 (/28)
D. 255.255.255.248 (/29)

17. Un técnico de un centro de datos debe tender una conexión de fibra entre dos edificios separados por 5 kilómetros, con 10 Gigabit Ethernet. ¿Qué tipo de medio se debe elegir?

A data center technician must run a fiber connection between two buildings 5 kilometers apart, supporting 10 Gigabit Ethernet. Which media type should be selected?

A. Fibra multimodo OM3
B. Fibra multimodo OM4
C. Cobre Cat6a con convertidor de medios de fibra
D. Fibra monomodo OS2

18. Un router aprende una ruta a 10.20.30.0/24 por OSPF y por EIGRP. Los dos protocolos anuncian el mismo largo de prefijo. ¿Qué ruta instalará el router en su tabla de enrutamiento?

A router learns a route to 10.20.30.0/24 via both OSPF and EIGRP. Both protocols advertise the same prefix length. Which route will the router install in its routing table?

A. La ruta OSPF, porque tiene una métrica menor
B. La ruta EIGRP, porque tiene una distancia administrativa menor
C. Las dos rutas, instaladas como multipath de igual costo (ECMP)
D. La ruta con más saltos, para tener redundancia

19. Un técnico quiere comprobar que la pila TCP/IP de una estación de trabajo funciona bien antes de revisar la conexión física de la red. ¿A qué dirección IP se debe hacer ping para probar la interfaz de bucle local (loopback)?

A technician wants to verify that a workstation's TCP/IP stack is functioning correctly before troubleshooting the physical network connection. Which IP address should be pinged to test the local loopback interface?

A. 10.0.0.1
B. 255.255.255.255
C. 127.0.0.1
D. 0.0.0.0

---

20. ¿Cuál de las siguientes direcciones IPv6 NO es válida por una compresión de ceros incorrecta?

Which of the following IPv6 addresses is INVALID due to improper zero compression?

A. 2001:0db8:0000:0000:0000:ff00:0042:8329
B. 2001:db8::ff00:42:8329
C. fe80::1
D. 2001:db8::1234::5678

---

21. Un router necesita una sola ruta resumida para anunciar cuatro redes: 172.16.4.0/24, 172.16.5.0/24, 172.16.6.0/24 y 172.16.7.0/24. ¿Qué ruta resumida representa correctamente las cuatro redes sin incluir direcciones adicionales?

A router needs a single summary route to advertise four networks: 172.16.4.0/24, 172.16.5.0/24, 172.16.6.0/24, and 172.16.7.0/24. Which summary route correctly represents all four networks with no additional address space included?

A. 172.16.0.0/21
B. 172.16.4.0/21
C. 172.16.4.0/22
D. 172.16.4.0/23

---

22. Un técnico ejecuta ipconfig en una estación Windows y ve una dirección IPv6 que empieza con fe80::. ¿Qué indica esta dirección sobre la interfaz?

A technician runs ipconfig on a Windows workstation and observes an IPv6 address beginning with fe80::. What does this address indicate about the interface?

A. Es una dirección multicast usada para comunicación en grupo
B. Es una dirección unicast global enrutable en internet
C. Es una dirección de enlace local (link-local), válida solo en la subred local y no enrutable
D. Es una dirección local única (unique local) pensada para enrutamiento interno privado

---

23. Un centro de datos actualiza su cableado para admitir conexiones 10GBASE-T a la distancia completa del estándar, 100 metros. ¿Qué categoría de cable se debe instalar?

A data center is upgrading its cabling to support 10GBASE-T connections at the full standard distance of 100 meters. Which cable category should be installed?

A. Cat 6
B. Cat 5e
C. Cat 3
D. Cat 6a

---

24. Un técnico instala un punto de acceso inalámbrico que consume 25.5 W medidos en el dispositivo alimentado. ¿Qué estándar PoE es el MÍNIMO necesario para cubrir este consumo?

A technician is installing a wireless access point that draws 25.5 W of power measured at the powered device. Which PoE standard is the MINIMUM required to meet this power requirement?

A. IEEE 802.3at (PoE+)
B. IEEE 802.3bt Tipo 3
C. IEEE 802.3af (PoE)
D. Un inyector PoE pasivo genérico de 24 V

---

25. Un técnico instala tres puntos de acceso de 2.4 GHz en zonas de cobertura contiguas y debe reducir al mínimo la interferencia de canal compartido (co-channel) entre ellos. ¿Qué conjunto de canales debe elegir?

A technician is deploying three 2.4 GHz access points in adjacent coverage areas and must minimize co-channel interference between them. Which set of channels should be selected?

A. Canales 1, 5, 9
B. Canales 1, 4, 8
C. Canales 2, 7, 11
D. Canales 1, 6, 11

---

26. Un ingeniero inalámbrico quiere maximizar el rendimiento total de una red 802.11ac de 5 GHz en una oficina densa con muchos puntos de acceso (AP) que se traslapan. ¿Qué estrategia de ancho de canal es la MÁS adecuada?

A wireless engineer wants to maximize aggregate throughput on a 5 GHz 802.11ac network deployed across a dense office with many overlapping access points. Which channel width strategy is MOST appropriate?

A. No configurar el ancho de canal y confiar solo en la dirección de banda (band steering)
B. Usar un ancho de canal de 20 MHz para reducir la interferencia de canal compartido, con menos velocidad por AP
C. Usar un ancho de canal de 80 MHz en todos los AP para maximizar el rendimiento teórico
D. Usar un ancho de canal de 160 MHz para no tener que planificar los canales

---

27. Un ingeniero de redes revisa la configuración IPv6 de una estación de trabajo y encuentra la dirección fe80::a1b2:c3d4:e5f6:7890. ¿Qué tipo de dirección es?

A network engineer reviews IPv6 configuration on a workstation and finds the address fe80::a1b2:c3d4:e5f6:7890. What type of address is this?

A. Dirección de enlace local (link-local)
B. Dirección multicast
C. Dirección unicast global
D. Dirección local única (unique local)

---

28. Un técnico repasa el modelo OSI para resolver un problema de enrutamiento. ¿Qué capa se encarga del direccionamiento lógico y de determinar el mejor camino para que los datos viajen entre redes?

A technician is reviewing the OSI model to troubleshoot a routing issue. Which layer is responsible for logical addressing and determining the best path for data to travel across networks?

A. Enlace de datos (Data Link)
B. Física (Physical)
C. Red (Network)
D. Transporte (Transport)

Operaciones de red

29. Un técnico instala un switch de 1 Gbps y espera que las transferencias de archivos entre dos servidores lleguen cerca de 1000 Mbps. La velocidad medida es solo de 650 Mbps. ¿Qué término describe MEJOR el valor de 650 Mbps?

A technician installs a 1 Gbps switch and expects file transfers between two servers to reach close to 1000 Mbps. The actual measured transfer speed is only 650 Mbps. Which term BEST describes the 650 Mbps value?

A. Ancho de banda (bandwidth)
B. Rendimiento (throughput)
C. Atenuación (attenuation)
D. Sobrecarga (overhead)

---

30. La hoja de datos de un fabricante indica que un switch tiene una vida operativa esperada de 100,000 horas entre fallas. ¿Qué métrica representa este valor?

A vendor datasheet lists a switch's expected operational lifespan between failures as 100,000 hours. Which metric does this value represent?

A. MTBF
B. Tiempo de actividad del SLA (SLA uptime)
C. Jitter
D. MTTR

---

31. Un técnico ejecuta un ping continuo y ve que 15 de 100 paquetes enviados nunca recibieron respuesta. ¿Qué métrica mide esto?

A technician runs a continuous ping test and observes that 15 out of 100 packets sent never received a reply. Which metric does this measure?

A. Jitter
B. Latencia (latency)
C. Uso del ancho de banda (bandwidth utilization)
D. Pérdida de paquetes (packet loss)

---

32. El plan de recuperación ante desastres de una empresa fija un objetivo de punto de recuperación (RPO) de 4 horas para la base de datos de su tienda en línea. ¿Qué calendario de copias de seguridad cumple este requisito con el menor uso de almacenamiento?

A company's disaster recovery plan specifies a recovery point objective (RPO) of 4 hours for its e-commerce database. Which backup schedule satisfies this requirement while minimizing storage overhead?

A. Copia completa una vez por semana
B. Copias diferenciales una vez al día
C. Copias incrementales cada 4 horas
D. Copia completa una vez cada noche

---

33. Un ingeniero de redes necesita visibilidad del tráfico en un switch de núcleo de 100 Gbps de alto rendimiento sin agregar mucha carga de CPU al plano de control del switch. ¿Qué tecnología de monitoreo de flujos es la MÁS adecuada?

A network engineer needs traffic visibility on a high-throughput 100 Gbps core switch without adding significant CPU overhead to the switch's control plane. Which flow monitoring technology is MOST appropriate?

A. SNMP polling, porque agrega los contadores de interfaz en detalle por flujo
B. NetFlow v9, porque exporta un registro de flujo completo por cada paquete que pasa por la interfaz
C. sFlow, porque usa muestreo estadístico de paquetes procesado por un colector externo
D. Captura completa de paquetes con SPAN, porque garantiza el menor uso de CPU del switch

---

34. Un servidor de archivos crítico tuvo 26 minutos de caída no planificada en un mes de 30 días. Según los niveles estándar de disponibilidad, ¿a qué nivel se ajusta MÁS el tiempo de actividad real del servidor?

A critical file server experienced 26 minutes of unplanned downtime during a 30-day month. Based on the standard availability tiers, which rating does the server's actual uptime MOST closely satisfy?

A. Cinco nueves (99.999%)
B. Cuatro nueves (99.99%)
C. Dos nueves (99%)
D. Tres nueves (99.9%)

---

35. Antes de aplicar un cambio en una regla del firewall durante una ventana de mantenimiento programada, un técnico documenta los detalles del cambio, el impacto esperado y un procedimiento de reversión para que lo apruebe la gerencia. ¿Qué documento está creando?

Before implementing a firewall rule change during a scheduled maintenance window, a technician documents the change details, expected impact, and a rollback procedure for management approval. Which document is being created?

A. Procedimiento operativo estándar (SOP)
B. Solicitud de cambio (change request)
C. Acuerdo de nivel de servicio (SLA)
D. Informe de línea base (baseline)

---

36. Un equipo de redes planea actualizar el firmware de todos los switches de núcleo durante una ventana de mantenimiento programada. ¿Qué documento se debe completar y aprobar ANTES de hacer el cambio, y detalla el procedimiento de reversión si la actualización falla?

A network team is planning a firmware upgrade on all core switches during a scheduled maintenance window. Which document should be completed and approved BEFORE the change is implemented, detailing the rollback procedure if the upgrade fails?

A. Un acuerdo de confidencialidad (NDA)
B. Un acuerdo de nivel de servicio (SLA)
C. Una solicitud de cambio (change management)
D. Un memorando de entendimiento (MOU)

---

37. Un ingeniero de redes necesita identificar los equipos y aplicaciones que más ancho de banda consumen en un enlace WAN, sin capturar el contenido completo de los paquetes de cada sesión. ¿Qué tecnología da MEJOR esta visibilidad?

A network engineer needs to identify the top bandwidth-consuming hosts and applications across a WAN link without capturing full packet payloads for every session. Which technology BEST provides this visibility?

A. SNMP polling
B. NetFlow
C. Agregación de syslog
D. Captura de paquetes con Wireshark

---

38. El disco duro de un servidor Linux falla, y el sistema operativo se cae y queda totalmente inutilizable hasta que se reinicia a mano. ¿En qué nivel de severidad de syslog de RFC 5424 se registraría con MÁS probabilidad este evento?

A Linux server's hard drive fails, causing the operating system to crash and become completely unusable until it is manually restarted. Under which RFC 5424 syslog severity level would this event MOST likely be logged?

A. Informativo (Informational, severidad 6)
B. Crítico (Critical, severidad 2)
C. Emergencia (Emergency, severidad 0)
D. Advertencia (Warning, severidad 4)

---

39. Durante una llamada VoIP, los usuarios dicen que el audio se entrecorta porque los paquetes de voz llegan en tiempos irregulares. ¿Qué métrica de rendimiento describe este problema?

During a VoIP call, users report choppy audio caused by inconsistent arrival times of voice packets. Which performance metric describes this issue?

A. Ancho de banda (bandwidth)
B. Pérdida de paquetes (packet loss)
C. Jitter
D. Latencia (latency)

---

40. Un acuerdo de nivel de servicio (SLA) garantiza 99.99% de disponibilidad para un circuito WAN en un mes de 30 días. ¿Cuánto tiempo total de caída se permite aproximadamente con este SLA?

A service level agreement guarantees 99.99% uptime for a WAN circuit over a 30-day month. Approximately how much total downtime is permitted under this SLA?

A. Unos 43 minutos
B. Unas 7.2 horas
C. Unas 72 horas
D. Unos 4.3 minutos

---

41. Un ingeniero sénior debe actualizar el firmware de doce switches de producción en una ventana de mantenimiento programada y necesita un documento con los comandos exactos paso a paso, las salidas esperadas y el procedimiento de reversión para esta tarea específica. ¿Qué documento debe crear?

A senior engineer must upgrade firmware on twelve production switches during a scheduled maintenance window and needs a document that lists the exact step-by-step commands, expected outputs, and rollback procedure for this specific task. Which document should be created?

A. Procedimiento operativo estándar (SOP)
B. Acuerdo de nivel de servicio (SLA)
C. Método de procedimiento (MOP, method of procedure)
D. Memorando de entendimiento (MOU)

---

42. Los usuarios de una llamada VoIP dicen que el audio se corta y que hay retrasos variables entre palabras, aunque el tiempo promedio de ida y vuelta medido con ping es de solo 20 ms. ¿Qué métrica es MÁS probable que cause este síntoma?

Users on a VoIP call report audio that cuts in and out with variable delay between words, even though the average round-trip time measured by ping is only 20 ms. Which metric is MOST likely responsible for the reported symptom?

A. Rendimiento (throughput), la velocidad de transferencia lograda
B. Jitter, la variación en el retraso de llegada de los paquetes
C. Ancho de banda (bandwidth), la capacidad máxima teórica del enlace
D. Latencia (latency), el retraso fijo de transmisión en un sentido

---

Resolución de problemas de red

43. La computadora de escritorio de un usuario no llega a la red, y el técnico nota que la luz de enlace (link light) de la tarjeta de red está apagada. ¿En qué capa del modelo OSI debe EMPEZAR la solución de problemas?

A user's desktop cannot reach the network, and the technician notices the link light on the NIC is not illuminated at all. At which layer of the OSI model should troubleshooting BEGIN?

A. Capa de red (capa 3)
B. Capa física (capa 1)
C. Capa de aplicación (capa 7)
D. Capa de transporte (capa 4)

---

44. Poco después de agregar un switch nuevo a la red sin STP activado, usuarios de varias VLAN reportan que pierden toda la conectividad, y el uso de CPU de los switches sube casi al 100% en toda la red. ¿Qué condición es MÁS probable?

Shortly after a new switch is added to the network without STP enabled, users across multiple VLANs report a complete loss of connectivity, and switch CPU utilization spikes to nearly 100% network-wide. Which condition is MOST likely occurring?

A. Agotamiento del servidor DHCP
B. Un ataque de envenenamiento de la caché ARP
C. Un punto de acceso no autorizado (rogue) que realiza un ataque de desautenticación
D. Una tormenta de difusión (broadcast storm) causada por un bucle de conmutación de capa 2

---

45. Un técnico de redes nota que un servidor conectado a un puerto de switch tiene muchas colisiones tardías (late collisions) junto con una mezcla de tramas runt y errores CRC, pero ningún otro equipo del mismo switch reporta problemas. ¿Cuál es la causa MÁS probable?

A network technician notices that a server connected to a switch port is experiencing a high number of late collisions along with a mix of runts and CRC errors, but no other devices on the same switch report issues. Which of the following is the MOST likely cause?

A. Alcance de DHCP agotado en la subred local
B. Asignación incorrecta de VLAN en el puerto del switch
C. Desajuste de dúplex entre la NIC del servidor y el switch
D. Un cable Ethernet defectuoso que supera el límite de 100 metros

---

46. Un técnico mide la pérdida de señal en un tendido largo de cable Ethernet de cobre y ve que la pérdida en decibeles supera el estándar TIA/EIA-568 para la categoría del cable, aunque la longitud está dentro del límite de 100 metros. ¿Qué término describe esta condición?

A technician measures signal loss on a long copper Ethernet run and finds the decibel loss exceeds the TIA/EIA-568 standard for the cable category, even though the cable length is within the 100-meter limit. Which term describes this condition?

A. Latencia (latency)
B. Atenuación (attenuation)
C. Diafonía (crosstalk)
D. Jitter

---

47. Un técnico quiere comprobar rápidamente la conectividad básica de capa 3 entre una estación de trabajo y un servidor remoto. ¿Qué utilidad de línea de comandos es la MÁS adecuada como PRIMERA herramienta?

A technician wants to quickly verify basic Layer 3 connectivity between a workstation and a remote server. Which command-line utility is the MOST appropriate FIRST tool to use?

A. ping
B. netstat
C. nslookup
D. tracert

---

48. Dos estaciones de trabajo de la misma VLAN pierden la conectividad de forma intermitente, y cada vez coincide con una advertencia de "conflicto de dirección IP" en el registro de eventos local. Un técnico confirma que ambas usan direcciones IP estáticas asignadas a mano. ¿Cuál es la causa raíz MÁS probable?

Two workstations on the same VLAN intermittently lose network connectivity, and each occurrence coincides with an 'IP address conflict' warning in the local event log. A technician confirms both machines use manually assigned static IP addressing. What is the MOST likely root cause?

A. Dos equipos del segmento tienen asignada manualmente la misma dirección IP

B. Una máquina virtual clonada produjo una dirección MAC duplicada en el segmento

C. El alcance de DHCP se traslapa con el rango usado para direcciones estáticas

D. Un equipo malicioso del segmento realiza un ataque de suplantación ARP (ARP spoofing)

---

49. Siguiendo la metodología de solución de problemas de CompTIA, un técnico reunió información y estableció una teoría de la causa probable de una falla de red. Según la metodología, ¿qué debe hacer el técnico A CONTINUACIÓN, antes de aplicar una solución?

Following the CompTIA troubleshooting methodology, a technician has gathered information and established a theory of probable cause for a network outage. According to the methodology, what should the technician do NEXT, before implementing a solution?

A. Probar la teoría para determinar la causa

B. Documentar los hallazgos, las acciones y los resultados

C. Establecer un plan de acción para resolver el problema

D. Verificar que todo el sistema funcione

---

50. Después de poner los conectores a un cable de conexión (patch cable) Cat 6 nuevo, un técnico quiere confirmar que los pares de hilos están conectados en el orden correcto en ambos extremos. ¿Qué herramienta es la MÁS adecuada?

After terminating a new Cat 6 patch cable, a technician wants to confirm the individual wire pairs are terminated in the correct order at both ends. Which tool is MOST appropriate for this task?

A. Probador de cable (probador de mapa de cableado, wire map tester)

B. Generador de tono y sonda (tone generator and probe)

C. Analizador de protocolos

D. OTDR

---

51. Un técnico revisa las estadísticas de interfaz de un switch y nota un aumento constante de errores CRC en un puerto conectado a la estación de un usuario. ¿Qué capa OSI es la causa raíz MÁS probable?

A technician reviewing interface statistics on a switch notices a steadily increasing count of CRC errors on a single port connected to a user's workstation. Which OSI layer is MOST likely the root cause of this issue?

A. Capa 2 - Enlace de datos

B. Capa 3 - Red

C. Capa 4 - Transporte

D. Capa 1 - Física

---

52. Según la metodología de solución de problemas de red de CompTIA, ¿qué paso debe hacer un técnico PRIMERO cuando un usuario reporta que su estación de trabajo no llega a internet?

According to the CompTIA network troubleshooting methodology, which step should a technician perform FIRST when responding to a user report that a workstation cannot reach the internet?

A. Establecer una teoría de la causa probable

B. Probar la teoría para determinar la causa

C. Establecer un plan de acción para resolver el problema

D. Identificar el problema

---

53. Un técnico decide empezar a resolver una queja de conectividad revisando primero el cableado y el estado de la tarjeta de red antes de ver la configuración de las aplicaciones. ¿Qué modelo de solución de problemas describe MEJOR este enfoque?

A technician chooses to begin troubleshooting a connectivity complaint by first checking cabling and NIC status before checking application settings. This approach is BEST described as which troubleshooting model?

A. Enfoque de sustitución (substitution)
B. Enfoque de abajo hacia arriba (bottom-up)
C. Enfoque de divide y vencerás (divide-and-conquer)
D. Enfoque de arriba hacia abajo (top-down)

---

54. En un traceroute a un servidor web remoto, los tiempos de ida y vuelta se mantienen por debajo de 5 ms en los primeros cuatro saltos, luego suben a más de 150 ms y se quedan altos en todos los saltos restantes, sin pérdida de paquetes en ningún salto. ¿Qué conclusión es la MÁS acertada?

During a traceroute to a remote web server, round-trip times remain under 5 ms for the first four hops, then jump to over 150 ms and stay consistently high for the remaining hops, with no packet loss reported at any hop. Which conclusion is MOST accurate?

A. Hay un enlace de larga distancia o congestionado entre el salto cuatro y el salto cinco
B. Hay un bucle de enrutamiento a partir del salto cinco
C. El servidor de destino es inalcanzable por una regla de firewall
D. El dispositivo del salto cinco está descartando paquetes y debe reemplazarse

---

55. Un técnico quiere ver los routers individuales por los que pasa un paquete en su camino a un equipo de destino. ¿Qué utilidad de línea de comandos debe usar?

A technician wants to view the individual routers a packet passes through on its way to a destination host. Which command-line utility should the technician use?

A. ipconfig
B. ping
C. netstat
D. tracert

---

56. Un técnico quiere verificar que los circuitos de transmisión y recepción de la tarjeta de red de una estación de trabajo funcionan bien, sin conectar la tarjeta a la red en uso. ¿Qué herramienta debe usar?

A technician wants to verify that a workstation's NIC transmit and receive circuits are functioning correctly without connecting the NIC to the live network. Which tool should be used?

A. Generador de tono y sonda (tone generator and probe)
B. Certificador de cable (cable certifier)
C. Conector de bucle (loopback plug)
D. Herramienta de impacto (punch-down tool)

Seguridad de redes

57. Una empresa aloja un servidor web público que debe seguir accesible desde internet, pero sin dar acceso directo a la LAN interna si el servidor se ve comprometido. ¿Qué diseño de red logra MEJOR este objetivo?

A company hosts a public-facing web server that must remain accessible from the internet while preventing direct access to the internal LAN if the server is compromised. Which network design BEST achieves this goal?

A. Poner el servidor web en la LAN interna, protegido por un firewall de host

B. Poner el servidor web en la misma VLAN que la red de administración

C. Configurar reenvío de puertos (port forwarding) directamente a la VLAN de la LAN interna

D. Poner el servidor web en una subred filtrada (screened subnet o DMZ) entre dos firewalls

---

58. Un técnico de redes va a retirar el acceso de administración remota heredado a un switch de núcleo, que hoy usa Telnet para configurar por línea de comandos (CLI). ¿Qué protocolo debe implementar para cifrar las sesiones de administración al switch?

A network technician is decommissioning legacy remote-management access to a core switch that currently relies on Telnet for CLI configuration. Which protocol should the technician implement to encrypt administrative sessions to the switch?

A. SNMPv2

B. FTP

C. HTTP

D. SSH

---

59. Varios usuarios reportan que, al escribir la URL correcta del portal bancario de la empresa, los redirigen a un sitio fraudulento que captura sus credenciales, aunque sus archivos hosts locales no fueron modificados. ¿Qué ataque lo causó con MÁS probabilidad?

Multiple users report that typing the correct URL for the company's banking portal redirects them to a fraudulent site that captures their credentials, even though their local hosts files are unmodified. Which attack MOST likely caused this?

A. ARP spoofing

B. Envenenamiento de la caché DNS (DNS cache poisoning)

C. Secuestro de sesión (session hijacking)

D. MAC spoofing

---

60. Un administrador de redes configura servicios AAA para administrar switches y routers, y necesita que todo el paquete de autenticación, no solo el campo de la contraseña, viaje cifrado entre el equipo de red y el servidor de autenticación. ¿Qué protocolo debe elegir?

A network administrator is configuring AAA services for switch and router management and requires that the entire authentication packet, not just the password field, be encrypted between the network device and the authentication server. Which protocol should the administrator select?

A. Kerberos

B. LDAPS

C. TACACS+

D. RADIUS

---

61. Varios usuarios de una red dicen que los redirigen a sitios web desconocidos, y la investigación muestra que un dispositivo no autorizado de la red entrega concesiones DHCP con una dirección de puerta de enlace predeterminada maliciosa. ¿Qué ataque describe este caso?

Several users on a network report being redirected to unfamiliar websites, and investigation reveals an unauthorized device on the network issuing DHCP leases with a malicious default gateway address. Which attack does this scenario describe?

A. Ataque Smurf (smurf attack)
B. Ataque de amplificación DNS (DNS amplification)
C. Ataque de servidor DHCP falso (rogue DHCP)
D. Inundación SYN (SYN flood)

---

62. Un atacante envía un correo muy personalizado al director financiero de una empresa, se hace pasar por el director ejecutivo (CEO) y pide con urgencia una transferencia bancaria no autorizada. ¿Qué tipo de ataque de ingeniería social describe esto?

An attacker sends a highly personalized email to a company's chief financial officer, impersonating the CEO and urgently requesting an unauthorized wire transfer. Which type of social engineering attack does this describe?

A. Pharming
B. Vishing
C. Tailgating
D. Whaling

---

63. Un atacante envía consultas DNS pequeñas a resolvedores DNS abiertos, con la IP de origen falsificada para que sea la de la víctima, y los resolvedores envían respuestas grandes a la víctima y saturan su ancho de banda. ¿Qué tipo de ataque se describe?

An attacker sends small DNS queries with a spoofed source IP address matching a victim's IP to open DNS resolvers, causing the resolvers to send large responses to the victim and overwhelm its available bandwidth. Which type of attack is described?

A. Ataque de amplificación DNS (DNS amplification)
B. Envenenamiento de la caché DNS (DNS cache poisoning)
C. Envenenamiento ARP (ARP poisoning)
D. Inundación SYN (SYN flood)

---

64. Un equipo de seguridad instala un servidor que imita una base de datos de producción, con credenciales falsas y archivos señuelo, en un segmento aislado de la red. ¿Cuál es el propósito PRINCIPAL de esta instalación?

A security team deploys a server that mimics a production database, complete with fake credentials and decoy files, on an isolated segment of the network. What is the PRIMARY purpose of this deployment?

A. Atraer a los atacantes lejos de los activos reales y estudiar sus tácticas
B. Cifrar datos sensibles en reposo con llaves de cifrado señuelo
C. Ofrecer una base de datos de respaldo por si falla el servidor de producción
D. Balancear las consultas a la base de datos entre varios servidores

---

65. Un administrador de redes necesita un protocolo AAA que cifre toda la carga útil del paquete (no solo la contraseña) y que separe autenticación, autorización y contabilidad (accounting) en procesos distintos, para un control detallado por comando en los equipos de red. ¿Qué protocolo debe elegir?

A network administrator needs an AAA protocol that encrypts the entire packet payload (not just the password) and separates authentication, authorization, and accounting into distinct processes for granular command-level control on network devices. Which protocol should be selected?

A. LDAP
B. Kerberos
C. RADIUS
D. TACACS+

---

66. Un administrador de redes configura un firewall para permitir el tráfico de regreso de las conexiones que se iniciaron desde dentro de la red, sin crear reglas de entrada explícitas para cada sesión. ¿Qué tecnología de firewall debe implementar?

A network administrator is configuring a firewall to allow return traffic for connections that originated from inside the network without creating explicit inbound rules for each session. Which firewall technology should the administrator implement?

A. Inspección con estado (stateful inspection)
B. Solo lista de control de acceso (ACL)
C. Filtrado de contenido basado en proxy
D. Filtrado de paquetes sin estado (stateless)

---

67. Una organización rediseña la arquitectura de su red con base en el modelo de seguridad de confianza cero (zero trust). ¿Qué principio refleja MEJOR este enfoque?

An organization is redesigning its network architecture around the zero trust security model. Which principle BEST reflects this approach?

A. La confianza se otorga automáticamente según la ubicación en la red, como pertenecer a una VLAN interna
B. Los firewalls perimetrales son el único punto de control de todo el tráfico
C. Toda solicitud de acceso se autentica y se autoriza, sin importar dónde esté quien la hace
D. Los usuarios que se autentican una vez al iniciar sesión mantienen la confianza durante toda la sesión

---

68. Un equipo de seguridad quiere una solución que vigile el tráfico de red en busca de patrones maliciosos y genere alertas, pero que no tome ninguna acción directa para bloquear el tráfico. ¿Qué dispositivo cumple MEJOR este requisito?

A security team wants a solution that monitors network traffic for malicious patterns and generates alerts but does not take direct action to block traffic. Which device BEST meets this requirement?

A. Sistema de detección de intrusiones (IDS)
B. Firewall de nueva generación (NGFW)
C. Equipo de gestión unificada de amenazas (UTM)
D. Sistema de prevención de intrusiones (IPS)

---

69. Un empleado remoto se conecta a la VPN de la empresa, y todo su tráfico de internet, incluida la navegación personal, pasa por la red corporativa. ¿Qué configuración de VPN se usa?

A remote employee connects to the corporate VPN, and all of the employee's internet traffic, including personal web browsing, is routed through the corporate network. Which VPN configuration is in use?

A. Túnel sin cliente (clientless)
B. Túnel completo (full tunnel)
C. Túnel dividido (split tunnel)
D. Túnel sitio a sitio (site-to-site)

---

70. Un técnico necesita administrar de forma remota la interfaz de línea de comandos de un servidor Linux con una conexión cifrada. ¿Qué protocolo debe usar EN LUGAR de Telnet?

A technician needs to remotely administer a Linux server's command-line interface over an encrypted connection. Which protocol should the technician use INSTEAD of Telnet?

A. SSH
B. TFTP
C. SNMP
D. SMTP

Respuesta correcta

1. A Anycast asigna la misma dirección IP a varios servidores en lugares distintos, y el enrutamiento lleva a cada cliente a la instancia más cercana o de mejor rendimiento. Así funcionan los servidores raíz de DNS y las CDN. Multicast entrega un flujo a un grupo de suscriptores. Unicast es de uno a uno. Broadcast llega a todos los equipos de un segmento local y no cruza internet.

2. B El tráfico norte-sur (north-south) cruza el perímetro del centro de datos, como un cliente de internet que llega a un servidor web. El tráfico este-oeste (east-west) va de servidor a servidor dentro del centro de datos. "Ingress-only" no es una clasificación reconocida. El tráfico intra-VLAN es entre equipos de la misma VLAN.

3. D El tráfico este-oeste (east-west) se queda dentro del centro de datos y va de un servidor a otro, aquí de un switch leaf a otro pasando por la capa spine. Es el patrón más común en entornos virtualizados. El norte-sur entra o sale hacia clientes externos. El tráfico fuera de banda es una red aparte para administrar equipos. Ingress solo indica entrada.

4. B DHCP (Dynamic Host Configuration Protocol) presta direcciones IP junto con la máscara de subred, la puerta de enlace y los servidores DNS, sin configuración manual. DNS convierte nombres en direcciones IP, pero no asigna direcciones. ARP relaciona una IP con una MAC en el segmento local. NTP sincroniza la hora.

5. B Un balanceador de carga (load balancer) reparte las solicitudes entre un grupo de servidores con algoritmos como round robin o menos conexiones, y mejora el rendimiento y la disponibilidad. Un proxy reenvía o guarda en caché las solicitudes; un proxy inverso también puede balancear, pero la respuesta más directa es el balanceador. El firewall aplica políticas de seguridad. El switch de capa 2 solo reenvía tramas.

6. C La elasticidad (elasticity) es la capacidad de la nube de aumentar y reducir recursos de forma automática y casi en tiempo real según la demanda, y liberarlos cuando ya no hacen falta. La escalabilidad (scalability) es más amplia: agregar capacidad de forma planificada, a menudo en un solo sentido. Multiinquilino es compartir la infraestructura entre clientes. Alta disponibilidad es redundancia contra caídas.

7. A DNS (Domain Name System) traduce nombres como www.example.com en las direcciones IP numéricas que usan los routers y los equipos. DHCP asigna la configuración IP (dirección, máscara y puerta de enlace). NTP sincroniza los relojes. SNMP sirve para monitorear y administrar dispositivos de red.

8. B CompTIA ubica el cifrado, el descifrado y el formato de los datos, como TLS/SSL, en la capa 6 (presentación), aunque en la práctica TLS funciona entre transporte y aplicación. Es una trampa clásica del examen. La capa de sesión abre y cierra sesiones. Transporte segmenta y entrega (TCP/UDP). HTTP está en la capa de aplicación; TLS lo envuelve.

9. B Las consultas DNS normales de un cliente usan UDP puerto 53, porque son intercambios pequeños de una solicitud y una respuesta, y UDP tiene poca sobrecarga. TCP puerto 53 se usa en transferencias de zona y también admite consultas DNS, por ejemplo cuando una respuesta UDP llega truncada. El puerto TCP 43 es de WHOIS. El puerto UDP 67 lo usan los servidores DHCP.

10. D UDP no tiene conexión: no hace saludo inicial, confirmaciones ni retransmisiones. Eso reduce la latencia a cambio de no garantizar la entrega, y es lo ideal para voz y video en tiempo real, donde un paquete reenviado llega demasiado tarde. El saludo de tres vías, las ventanas y el estado de conexión son mecanismos de TCP.

11. A Un switch reenvía tramas según la dirección MAC de destino del encabezado de enlace de datos, así que la respuesta es la capa 2. La capa 3 usa direcciones IP; los routers y los switches multicapa pueden reenviar en esa capa. La capa 4 usa puertos, como firewalls y balanceadores. La capa 7 revisa el contenido, no la MAC.

12. D Un IPS se coloca en línea con el tráfico, compara los paquetes con firmas y reglas de comportamiento, y puede descartar o bloquear tráfico malicioso en tiempo real. Un IDS hace el mismo análisis, pero fuera de banda (out-of-band) y solo genera alertas. Un proxy filtra solicitudes de aplicación, pero no está hecho para bloquear intrusiones por firmas. Un switch de capa 2 no inspecciona.

13. C Las direcciones del rango fc00::/7, que en la práctica empiezan con fd00::/8, son direcciones locales únicas (unique local address, ULA). Son privadas, parecidas al espacio RFC 1918: se enrutan dentro de un sitio, pero no en internet. Las de enlace local usan fe80::/10. Las unicast globales empiezan con 2000::/3. Las multicast usan ff00::/8.

14. B Un router trabaja en la capa 3 y reenvía paquetes entre redes IP distintas: mira la dirección IP de destino y consulta su tabla de enrutamiento para elegir la mejor ruta. Un switch reenvía tramas dentro de un mismo dominio de difusión de capa 2 según la MAC. Un hub repite la señal a todos los puertos. Un puente (bridge) divide una red de capa 2 en dominios de colisión menores, pero no enruta.

15. D PAT, también llamado NAT overload, asigna muchas direcciones privadas a una sola IP pública y distingue cada sesión por su número de puerto de origen, así que muchos equipos comparten una dirección. El NAT estático es una relación fija uno a uno. El NAT dinámico con grupo uno a uno necesita una IP pública por cada equipo activo y se agotaría. Una puerta de enlace de aplicación no traduce direcciones para varios equipos.

16. B La máscara 255.255.255.252 (/30) da 4 direcciones en total (2^2) y deja exactamente 2 utilizables después de reservar la de red y la de difusión (broadcast), justo lo que necesita un enlace con dos equipos. Una /29 desperdicia 4 direcciones, una /28 desperdicia 12 y una /26 desperdicia 60. De las máscaras listadas, la /30 desperdicia menos. Los enlaces punto a punto que admiten /31 pueden usar un bloque aún menor.

17. D La fibra monomodo OS2 tiene un núcleo mucho más fino y usa láser, así que alcanza 10 km o más a 10 Gigabit Ethernet sin dispersión modal importante. Es la única opción viable para 5 km. La multimodo OM3 llega a unos 300 m con 10GbE y la OM4 a unos 400 a 550 m. El cobre Cat6a se limita a 100 m, con o sin convertidor.

18. B Cuando varios protocolos anuncian el mismo destino, el router decide por distancia administrativa (administrative distance, AD) y no compara métricas de protocolos distintos. La AD interna predeterminada de EIGRP es 90, menor que la de OSPF (110), así que gana EIGRP. Las métricas solo desempatan dentro del mismo protocolo. ECMP aplica con rutas del mismo protocolo. El número de saltos no cuenta aquí.

19. C 127.0.0.1 es la dirección de loopback estándar de IPv4, reservada en el bloque 127.0.0.0/8. Al hacerle ping se comprueba la pila TCP/IP local sin usar el hardware físico. 0.0.0.0 es una dirección no especificada o de ruta predeterminada. 255.255.255.255 es el broadcast limitado. 10.0.0.1 es una dirección privada RFC 1918 que puede tener cualquier equipo.

20. D Según RFC 5952, una dirección solo puede usar una vez '::', porque si se usa dos veces no se sabe cuántos grupos de ceros reemplaza cada una. La forma completa, la forma comprimida una sola vez y fe80::1 son válidas. '2001:db8::1234::5678' usa '::' dos veces, y ningún analizador IPv6 puede expandirla sin ambigüedad.

21. C Los valores 4 a 7 del tercer octeto en binario (00000100 a 00000111) comparten los primeros seis bits y solo cambian 2, así que el resumen es 172.16.4.0/22, un bloque de 4 redes /24 seguidas. La /23 solo cubre 2 redes (4 y 5). La 172.16.4.0/21 no es un prefijo válido, porque tiene bits de host activos. La 172.16.0.0/21 incluiría también de 172.16.0.0 a 172.16.3.0.

22. C El prefijo fe80::/10 está reservado para direcciones de enlace local (link-local). Se asignan solas a cada interfaz para hablar dentro del mismo enlace, por ejemplo en el descubrimiento de vecinos, y los routers nunca las reenvían fuera del segmento. Las unicast globales empiezan con 2000::/3 y se enrutan en internet. Las locales únicas usan fc00::/7. Las multicast empiezan con ff00::/8.

23. D El Cat 6a resiste mejor la diafonía entre cables vecinos (alien crosstalk) y admite 10 Gbps (10GBASE-T) en un canal completo de 100 m; existe en versión blindada y sin blindar. El Cat 6 normal llega a 10 Gbps solo hasta unos 37 a 55 m. El Cat 5e admite 1 Gbps y 2.5GBASE-T a 100 m, pero no está especificado para 10GBASE-T a distancia completa. El Cat 3 es obsoleto.

24. A IEEE 802.3at, o PoE+, entrega hasta 25.5 W en el dispositivo (30 W en el origen, por las pérdidas del cable), así que es el mínimo que cubre este consumo. IEEE 802.3af (PoE) llega a 12.95 W, que no alcanza. IEEE 802.3bt Tipo 3 da unos 51 W y serviría, pero sobra. Los inyectores pasivos de 24 V no están estandarizados y no garantizan compatibilidad con equipos 802.3.

25. D Los canales 1, 6 y 11 son el conjunto estándar sin traslape para tres puntos de acceso en 2.4 GHz con canales de 20 MHz. La señal 802.11b ocupa unos 22 MHz y 802.11g/n usa 20 MHz. Los canales 1, 5, 9 solo se separan por cuatro números y no son el conjunto estándar. En 2, 7, 11 los canales 7 y 11 quedan muy cerca. En 1, 4, 8 la separación es de 3 a 4 canales y hay interferencia entre canales adyacentes.

26. B En entornos densos, los canales más anchos gastan más del espectro limitado de 5 GHz, dejan menos canales sin traslape y aumentan la interferencia entre puntos de acceso. Los canales de 20 MHz bajan la velocidad máxima por punto, pero permiten reutilizar muchos más canales, y eso mejora la capacidad total. Usar 80 o 160 MHz en todos agotaría los canales. El band steering solo mueve clientes entre 2.4 y 5 GHz.

27. A Las direcciones del rango fe80::/10 son de enlace local (link-local): se asignan solas a cada interfaz IPv6, sirven solo en el segmento local y nunca se enrutan. Las locales únicas están en fc00::/7 y son de uso privado, parecido a RFC 1918. Las unicast globales empiezan con 2000::/3 y se enrutan en todo internet. Las multicast empiezan con ff00::/8 y van a grupos de equipos.

28. C La capa de red (capa 3) maneja el direccionamiento lógico (direcciones IP) y las decisiones de enrutamiento entre redes, por eso ahí trabajan los routers. La capa física (capa 1) trata bits y señales eléctricas. Enlace de datos (capa 2) usa direcciones MAC para entregar tramas locales. Transporte (capa 4) administra conexiones y segmentación (TCP/UDP), pero no elige caminos.

29. B El throughput es la velocidad real de datos transferidos con éxito en un enlace, casi siempre menor que el máximo teórico por la sobrecarga de protocolos, la contención y los límites del hardware. El ancho de banda (bandwidth) es la capacidad máxima del enlace (aquí 1 Gbps). La sobrecarga son los bits que no son datos (encabezados, ACK), una causa y no el valor medido. La atenuación es la pérdida de señal por distancia.

30. A El MTBF (Mean Time Between Failures, tiempo medio entre fallas) es una métrica de confiabilidad, casi siempre dada por el fabricante, que predice el tiempo medio de operación antes de una falla de hardware. El MTTR mide cuánto tarda una reparación. El uptime del SLA es un porcentaje de disponibilidad por contrato. El jitter es la variación en el tiempo de llegada de los paquetes.

31. D La pérdida de paquetes es el porcentaje de paquetes enviados que no llegan a su destino, aquí el 15 por ciento, y es un indicador clave de la calidad del enlace o de congestión. El jitter mide la variación de tiempo entre paquetes que sí llegan. La latencia mide el retraso de los paquetes que sí llegan. El uso del ancho de banda indica cuánta capacidad se consume.

32. C El RPO es la máxima pérdida de datos aceptable, medida en tiempo. Con copias incrementales cada 4 horas se pierden como máximo 4 horas de datos, y se usa mucho menos almacenamiento y tiempo de respaldo que con copias completas repetidas. Una copia completa semanal puede perder hasta una semana. Las diferenciales diarias y las completas nocturnas dejan hasta 24 horas expuestas.

33. C sFlow toma muestras de paquetes a una tasa definida (por ejemplo 1 de cada 2048) y envía muestras ligeras a un colector externo, así que la sobrecarga es baja incluso a 100 Gbps. NetFlow v9 exporta registros de flujo, no un registro por paquete, y sus recursos dependen de la implementación, el hardware y el muestreo. SNMP da totales por interfaz, sin detalle por flujo. SPAN duplica el tráfico y no garantiza el menor uso de CPU.

34. D Un mes de 30 días tiene 43,200 minutos. Con tres nueves (99.9%) se permiten unos 43.2 minutos de caída al mes, y los 26 minutos entran en ese límite. Con cuatro nueves (99.99%) solo se permiten unos 4.3 minutos, así que 26 minutos lo exceden. Dos nueves (99%) permiten unos 432 minutos, mucho más de lo necesario. Cinco nueves permiten solo unos 26 segundos.

35. B Una solicitud de cambio (change request) documenta de manera formal una modificación propuesta, su justificación, el impacto esperado y el plan de reversión, y se envía a aprobación en el proceso de gestión de cambios antes de aplicarla. El informe de línea base registra el rendimiento normal. El SLA define el nivel de servicio con un proveedor o cliente. El SOP describe tareas rutinarias repetibles.

36. C La solicitud de cambio es el documento formal que se revisa y aprueba en el proceso de gestión de cambios (change management). Indica el alcance, la evaluación de riesgos, la ventana de mantenimiento y, sobre todo, el plan de reversión para restablecer el servicio si el cambio falla. Un SLA define garantías de rendimiento. Un NDA trata de confidencialidad. Un MOU expresa una intención general, sin el detalle técnico de reversión.

37. B NetFlow exporta registros de flujo que resumen IP de origen y destino, puertos, protocolo y bytes. Sirve para encontrar a los equipos que más tráfico generan (top talkers) con poca sobrecarga, comparado con capturar paquetes completos. SNMP da métricas del dispositivo, como CPU o contadores de interfaz, no detalle por flujo. Syslog reúne mensajes de eventos. La captura completa es muy pesada para analizar toda una WAN de forma continua.

38. C RFC 5424 define la severidad 0 (Emergency) como "el sistema es inutilizable", que es lo que pasa cuando una caída deja todo el equipo fuera de servicio. Crítico (2) es para fallas graves que degradan el servicio, pero no siempre dejan el sistema inutilizable. Advertencia (4) es para condiciones no críticas que conviene vigilar. Informativo (6) son mensajes de rutina sin falla.

39. C El jitter es la variación del retraso entre paquetes sucesivos que llegan a su destino. Si es excesivo, el audio se entrecorta o se distorsiona en aplicaciones en tiempo real como VoIP. La latencia es el retraso total de un paquete, de ida o de ida y vuelta, no su variación. La pérdida de paquetes son los que nunca llegan y causa cortes. El ancho de banda es la capacidad máxima del enlace.

40. D El 99.99%, conocido como cuatro nueves, permite 0.01% de caída. Un mes de 30 días tiene 43,200 minutos, y el 0.01% es aproximadamente 4.32 minutos, es decir "unos 4.3 minutos". "Unos 43 minutos" corresponde a 99.9% (tres nueves) en el mismo período. "Unas 7.2 horas" es 99% (dos nueves) en un mes de 30 días, y "unas 72 horas" es una disponibilidad de 90%.

41. C Un MOP (method of procedure) es un documento de una tarea específica, paso a paso, con los comandos exactos, los resultados esperados y los pasos de reversión de un cambio planificado, como una actualización de firmware. Un SOP cubre procesos generales y recurrentes, no el guion detallado de un cambio único. Un SLA define garantías de servicio. Un MOU es un acuerdo no vinculante de intención entre partes.

42. B El jitter, la variación en el retraso de llegada, explica por qué los paquetes llegan con espacios desiguales aunque la latencia promedio de ida y vuelta sea baja (20 ms). Así superan lo que el búfer de jitter puede compensar y el audio se entrecorta. Una latencia promedio baja no descarta picos de retraso. El throughput afectaría la calidad en general. El ancho de banda es solo el techo teórico del enlace.

43. B Una luz de enlace apagada indica que no hay señal eléctrica ni óptica válida entre la tarjeta de red y el puerto del switch, un síntoma de la capa 1 (cable defectuoso, conector suelto, puerto deshabilitado o tarjeta dañada). Revisar direcciones IP (capa 3), puertos y sesiones (capa 4) o la aplicación (capa 7) es prematuro, porque sin conexión física ninguna funciona. Es el punto de partida de la solución de problemas de abajo hacia arriba.

44. D Una tormenta de difusión (broadcast storm) por un bucle de capa 2 puede ocurrir cuando un switch nuevo crea una ruta redundante sin protección de spanning tree: las tramas de difusión circulan sin fin y consumen ancho de banda y CPU en toda la red. El agotamiento de DHCP solo impediría que nuevos clientes obtengan dirección. La desautenticación afecta solo a clientes inalámbricos. El envenenamiento ARP ataca equipos concretos y no sube la CPU de todos.

45. C Las colisiones tardías con errores CRC y runts en un solo puerto apuntan a un desajuste de dúplex (duplex mismatch) entre la tarjeta de red (NIC) del servidor y el puerto: un lado en full duplex y el otro en half o con la autonegociación fallida. Eso causa colisiones que no deberían ocurrir en un enlace full duplex bien negociado. Una distancia excesiva también puede causarlas en half duplex, pero los síntomas juntos indican dúplex. Una VLAN mal asignada corta la conectividad, no daña tramas. DHCP agotado no genera errores de capa 1 o 2.

46. B La atenuación (attenuation) es la pérdida de potencia de la señal al viajar por el medio, y se mide en decibeles. Puede pasar del límite del estándar incluso dentro de 100 m por mala calidad del cable, conductores dañados, curvas demasiado cerradas o conectores deficientes. La latencia es el retraso de los datos, no una pérdida de potencia. El jitter es la variación de la latencia. La diafonía es interferencia entre pares cercanos, otro problema distinto.

47. A Ping envía solicitudes de eco ICMP y espera respuestas, y da una comprobación rápida de sí o no de la conectividad IP de extremo a extremo (capa 3). Tracert sirve más cuando ping falla y hay que ubicar en qué salto se pierde el tráfico. Netstat muestra el estado local de conexiones y puertos, no la conectividad remota. Nslookup prueba la resolución DNS, no la conectividad IP.

48. A El sistema operativo muestra el aviso de "conflicto de dirección IP" cuando un ARP gratuito revela que otro equipo ya responde por esa IP, lo más común cuando se asignan a mano direcciones estáticas duplicadas. Como ambos equipos son estáticos, un traslape de DHCP es menos directo, pues afectaría sobre todo a clientes con direcciones dinámicas. El ARP spoofing suele activar alertas de seguridad o de IDS. Una MAC duplicada causa inestabilidad (MAC flapping).

49. A La metodología de siete pasos va así: identificar el problema, establecer una teoría de la causa probable, probar la teoría, establecer un plan de acción, aplicar la solución, verificar que todo funcione y documentar. Después de formar la teoría, lo que sigue es probarla, porque actuar con una teoría sin confirmar puede hacer perder tiempo o causar cambios innecesarios. El plan de acción viene cuando se confirma la teoría. Verificar va después de aplicar la solución, y documentar es el último paso.

50. A Un probador de mapa de cableado (wire map tester) comprueba la continuidad pin a pin de ambos extremos de un cable UTP y muestra al instante errores de cableado, pares divididos (split pairs), cortos o pares invertidos. Un OTDR es para fibra óptica y mide la luz reflejada para hallar roturas o empalmes. Un analizador de protocolos captura y decodifica tráfico. El generador de tono y sonda sirve para localizar un cable entre muchos, no para verificar el orden de los pines.

51. D Los errores CRC indican tramas que llegaron dañadas, y la causa casi siempre está en la capa física: un cable dañado, un conector defectuoso o interferencia electromagnética cercana. Aunque la revisión CRC se hace en la capa de enlace de datos, la causa que hay que investigar es el medio físico. Los problemas de capa 2 suelen verse en la tabla de direcciones MAC o en las VLAN. La capa 3 trata de enrutamiento y la capa 4 de puertos y sesiones, y ninguna produce errores CRC.

52. D La metodología de siete pasos de CompTIA siempre empieza con "identificar el problema": reunir información, preguntar al usuario, identificar síntomas y ver si algo cambió. Saltarse este paso lleva a adivinar. "Establecer una teoría de la causa probable" es el paso dos y depende de lo reunido en el paso uno. "Probar la teoría" y "establecer un plan de acción" vienen todavía después.

53. B El enfoque de abajo hacia arriba (bottom-up) empieza en la capa física del modelo OSI y sube por enlace de datos, red, transporte y, al final, aplicación, como al revisar primero cableado y tarjeta de red. El de arriba hacia abajo (top-down) empieza en la capa de aplicación. Divide y vencerás empieza en una capa intermedia, como la 3, y sube o baja según el resultado. La sustitución cambia una pieza sospechosa por una buena y no sigue capas.

54. A Un aumento sostenido de la latencia sin pérdida de paquetes indica retraso de propagación o congestión en el enlace entre esos saltos, no una falla. La pérdida de paquetes, que no se reportó, sería la señal de un equipo que descarta. Un bucle de enrutamiento mostraría direcciones repetidas o saltos crecientes y mensajes de TTL excedido. Un destino bloqueado por firewall daría tiempos agotados o mensajes de destino inalcanzable, no respuestas exitosas con retraso alto.

55. D Tracert (traceroute en Linux y macOS) envía paquetes con valores TTL cada vez mayores y registra la dirección IP de cada router que responde, así traza el camino completo hasta el destino. Ping solo confirma la conectividad y el tiempo de ida y vuelta a un destino, sin mostrar los saltos intermedios. Ipconfig muestra la configuración IP del propio equipo. Netstat muestra conexiones activas y puertos en escucha de la máquina local.

56. C Un conector de bucle (loopback plug) conecta los pines de transmisión directamente a los de recepción, y así el software de diagnóstico de la tarjeta confirma que puede enviar y recibir señales sin una red activa. El generador de tono y sonda sirve para rastrear un cable por paredes o manojos. El certificador valida el desempeño eléctrico de un tendido, no la tarjeta. La herramienta de impacto (punch-down) fija los conductores en un panel o jack y no diagnostica.

57. D Una subred filtrada (screened subnet o DMZ) aísla los servidores de cara a internet detrás de un firewall externo, y un segundo firewall interno limita el tráfico de la DMZ hacia la LAN interna, así que un servidor comprometido no puede saltar directo hacia adentro. Un firewall de host en la LAN deja el servidor en el segmento de confianza. El reenvío directo elimina la segmentación. La VLAN de administración expone las interfaces de gestión a un equipo público.

58. D SSH cifra toda la sesión CLI, incluidas las credenciales, con algoritmos criptográficos fuertes, y es el reemplazo estándar de Telnet en equipos de red. SNMPv2 manda las cadenas de comunidad en texto claro y sirve para monitorear, no para la CLI. FTP no es para administrar equipos y también manda credenciales sin cifrar. HTTP también es texto claro y se usa para interfaces gráficas, no para línea de comandos.

59. B El envenenamiento de la caché DNS inserta un registro falso en la caché de un resolvedor, así que la URL correcta se resuelve a una IP del atacante aunque no se haya alterado nada en el equipo del cliente. El ARP spoofing actúa en la capa 2 dentro de una subred y no explica una redirección de la resolución de nombres. El MAC spoofing cambia la identidad de hardware, no registros DNS. El secuestro de sesión toma una sesión ya autenticada.

60. C TACACS+ cifra todo el cuerpo del paquete sobre TCP puerto 49 y separa autenticación, autorización y contabilidad (accounting) en procesos distintos, con autorización por comando, lo que da confidencialidad completa en sesiones de administración de equipos. RADIUS (UDP 1812/1813) solo cifra el campo de la contraseña en el Access-Request y deja el nombre de usuario y otros atributos en texto claro. Kerberos usa tickets para acceder a recursos. LDAPS cifra consultas al directorio.

61. C Un servidor DHCP falso (rogue DHCP server) es un servidor DHCP no autorizado que entrega concesiones con una puerta de enlace o un DNS malicioso, y así el atacante intercepta o redirige el tráfico de las víctimas. La amplificación DNS usa resolvedores abiertos para inundar a una víctima y no involucra DHCP. Un ataque Smurf inunda con respuestas ICMP falsificadas por difusión. Una inundación SYN agota la tabla de conexiones con saludos TCP incompletos.

62. D Whaling es un ataque de phishing dirigido a ejecutivos de alto valor, con pretextos personalizados y creíbles, como una solicitud de transferencia falsa de parte del "CEO". El vishing usa llamadas de voz, no correo. El tailgating es seguir físicamente a una persona autorizada por una puerta segura. El pharming redirige a sitios maliciosos con manipulación de DNS, no con un correo que suplanta a alguien.

63. A Es un ataque de amplificación (o reflexión) DNS: el atacante falsifica la IP de la víctima como origen de consultas pequeñas a resolvedores abiertos, que responden con mensajes mucho más grandes dirigidos a la víctima y consumen su ancho de banda, una técnica de denegación de servicio distribuida. El envenenamiento ARP actúa en tablas locales de capa 2. El envenenamiento de caché DNS redirige a sitios maliciosos. La inundación SYN agota el estado de conexiones.

64. A Describe un honeypot (señuelo): sirve para atraer y observar el comportamiento de los atacantes en un entorno aislado y vigilado, generar inteligencia de amenazas y desviar la atención de los sistemas reales de producción. No ofrece conmutación por falla, así que no es una base de respaldo. No reparte consultas, así que no es balanceo de carga. Guarda datos señuelo para que los encuentren, no administra llaves de datos legítimos en reposo.

65. D TACACS+ cifra todo el cuerpo del paquete sobre TCP y separa autenticación, autorización y contabilidad en procesos independientes, lo que permite autorizar por comando en routers y switches, un uso típico en entornos Cisco. RADIUS solo cifra el campo de la contraseña y junta autenticación y autorización en un paso, y por eso el control por comando es más difícil. Kerberos es para autenticación con tickets y SSO. LDAP es un protocolo de acceso a directorios, no un marco AAA.

66. A Los firewalls con inspección con estado (stateful) mantienen una tabla de estado de las conexiones establecidas (IP de origen y destino, puertos, números de secuencia) y permiten de forma automática el tráfico de regreso de conexiones iniciadas desde dentro, sin reglas de entrada espejo. El filtrado sin estado evalúa cada paquete por separado con reglas fijas y necesita reglas de entrada explícitas. El proxy termina las conexiones en la capa de aplicación. Una ACL sola es filtrado sin estado.

67. C Confianza cero (zero trust) funciona con "nunca confiar, siempre verificar": exige autenticar y autorizar de forma continua cada solicitud de recurso, esté quien la hace dentro o fuera del perímetro. Dar confianza por la VLAN es el modelo perimetral antiguo que zero trust reemplaza. Depender solo de un firewall perimetral contradice la microsegmentación y la verificación interna. Mantener la confianza toda la sesión va contra la verificación continua.

68. A Un IDS funciona de forma pasiva, casi siempre analiza una copia del tráfico desde un puerto SPAN o un tap, y genera alertas de actividad sospechosa, pero no puede descartar ni bloquear paquetes en tiempo real. Un IPS va en línea y puede bloquear o reiniciar sesiones maliciosas, más de lo que se pidió. Un firewall de nueva generación filtra en línea con reconocimiento de aplicaciones y puede bloquear. Un UTM reúne varias funciones activas, como antivirus e IPS.

69. B Una VPN de túnel completo (full tunnel) obliga a que todo el tráfico del equipo remoto, incluido el que va a internet, pase por la red corporativa, de modo que las políticas de seguridad y el monitoreo se aplican a cada paquete. El túnel dividido (split tunnel) solo manda por la VPN el tráfico a recursos corporativos y la navegación personal sale directa. El sitio a sitio conecta dos redes o puertas de enlace, no un equipo remoto. La VPN sin cliente da acceso por navegador a aplicaciones específicas.

70. A SSH (Secure Shell, TCP puerto 22) da acceso remoto cifrado por línea de comandos y reemplaza directamente a Telnet, que manda credenciales y datos de sesión en texto claro por el puerto TCP 23. SNMP sirve para monitorear y administrar equipos de red, no para acceder a una consola. SMTP envía correo. TFTP transfiere archivos sin autenticación ni cifrado, aún menos seguro que Telnet para este fin.

Palabras clave en inglés

OSI model	modelo OSI	Modelo de siete capas que describe cómo se comunican las redes.
presentation layer	capa de presentación (capa 6)	Capa OSI que se ocupa del formato y el cifrado de datos.
IP address	dirección IP	Dirección lógica que identifica a un dispositivo en una red.
MAC address	dirección MAC	Dirección física de una interfaz de red, usada en la capa 2.
subnet	subred	Parte de una red IP con su propio rango de direcciones.
subnet mask	máscara de subred	Indica qué parte de la dirección IP es de red y cuál de host.
default gateway	puerta de enlace predeterminada	Dispositivo que recibe el tráfico destinado a otras redes.
port number	número de puerto	Número que identifica un servicio o aplicación en un equipo.
TCP	protocolo de control de transmisión	Protocolo con conexión que confirma la entrega de los datos.
UDP	protocolo de datagramas de usuario	Protocolo sin conexión que no confirma la entrega de los datos.
unicast	unidifusión	Envío de un origen a un solo destino.
multicast	multidifusión	Envío de un origen a un grupo de destinos suscritos.
broadcast	difusión	Envío a todos los dispositivos de la red local.

anycast	anycast (difusión por proximidad)	Una dirección compartida por varios servidores; el enrutamiento elige el más cercano.
DNS	sistema de nombres de dominio	Servicio que convierte nombres de dominio en direcciones IP.
DHCP	protocolo de configuración dinámica de host	Asigna direcciones IP y otros datos de red de forma automática.
NAT	traducción de direcciones de red	Cambia direcciones IP entre redes, por ejemplo de privada a pública.
switch	conmutador (switch)	Conecta equipos en una red local y reenvía según direcciones MAC.
router	enrutador (router)	Conecta redes distintas y reenvía paquetes según direcciones IP.
routing table	tabla de enrutamiento	Lista de rutas que usa un router para reenviar paquetes.
VLAN	red de área local virtual	Red lógica separada dentro de los mismos switches físicos.
trunk port	puerto troncal	Puerto de switch que transporta tráfico de varias VLAN.
access point	punto de acceso	Equipo que conecta dispositivos inalámbricos con la red cableada.
SSID	identificador de conjunto de servicios	Nombre con el que aparece una red wifi.
twisted pair	par trenzado	Dos hilos trenzados entre sí para reducir la interferencia.
split pair	par dividido	Pines correctos, pero con hilos de pares trenzados equivocados.
open / short	circuito abierto / cortocircuito	Abierto: conductor interrumpido. Corto: dos conductores que se tocan.
crosstalk	diafonía	Señal de un par que interfiere con otro par cercano.
latency	latencia	Tiempo que tarda un dato en llegar a su destino.
packet loss	pérdida de paquetes	Paquetes que se envían, pero no llegan a su destino.
SNMP	protocolo simple de administración de red	Protocolo para monitorear y administrar equipos de red.
disaster recovery	recuperación ante desastres	Plan para restablecer sistemas y datos después de una falla grave.
firewall	cortafuegos	Permite o bloquea tráfico de red según reglas definidas.
access control list (ACL)	lista de control de acceso	Lista de reglas que permiten o niegan tráfico o acceso.

VPN	red privada virtual	Túnel protegido que conecta usuarios o redes a través de otra red.
ipconfig	comando ipconfig	Muestra la configuración IP de un equipo con Windows.
netstat	comando netstat	Muestra conexiones de red activas y puertos en escucha.
arp	comando arp	Muestra la tabla que relaciona direcciones IP con direcciones MAC.
nslookup / dig	comandos nslookup y dig	Consultan servidores DNS y muestran sus respuestas.
tracert / pathping	comandos tracert y pathping	Muestran los saltos hasta un destino; pathping también mide pérdida de paquetes.
load balancer	balanceador de carga	Reparte las solicitudes de los clientes entre varios servidores.
jitter	jitter (variación del retraso)	Variación del retraso entre paquetes; entrecorta voz y video.
throughput	rendimiento real	Velocidad real de datos transferidos, menor que el ancho de banda.
PoE	alimentación por Ethernet	Energía eléctrica enviada a un dispositivo por el mismo cable de red.
RPO	objetivo de punto de recuperación	Máxima pérdida de datos aceptable, medida en tiempo.
change request	solicitud de cambio	Documento aprobado antes de un cambio, con impacto y plan de reversión.
honeypot	honeypot (señuelo)	Sistema falso que atrae atacantes para observarlos.
zero trust	confianza cero	Modelo que verifica cada acceso, sin importar desde dónde se pida.

Examundo es independiente. No está afiliado con los organismos que hacen estos exámenes ni tiene su aprobación. Las preguntas son originales, no son del examen real. examundo.tech/es/comptia-network-plus/