examundo

Examen de práctica CCNA en español

50 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/ccna/

Fundamentos de redes

1. Un ingeniero de redes asignó 192.168.20.0/26 a la VLAN 10 y 192.168.20.64/27 a la VLAN 20, ambas del bloque 192.168.20.0/24. ¿Qué subred disponible ofrece exactamente 2 direcciones de host utilizables para un enlace WAN punto a punto y tiene la dirección de red más baja?

A network engineer has allocated 192.168.20.0/26 to VLAN 10 and 192.168.20.64/27 to VLAN 20 from the 192.168.20.0/24 block. Which available subnet provides exactly 2 usable host addresses for a point-to-point WAN link and has the lowest network address?

A. 192.168.20.96/30
B. 192.168.20.128/30
C. 192.168.20.92/30
D. 192.168.20.96/29

---

2. La ventana de congestión de un emisor TCP es de 32 KB y el receptor anuncia una ventana de 24 KB. El emisor tiene 10 KB de datos en tránsito sin confirmar. ¿Cuántos datos adicionales puede transmitir el emisor antes de esperar un acuse de recibo (acknowledgment)?

A TCP sender's congestion window is 32 KB, and the receiver advertises a window size of 24 KB. The sender has 10 KB of unacknowledged data in flight. How much additional data can the sender transmit before waiting for an acknowledgment?

A. 32 KB
B. 22 KB
C. 24 KB
D. 14 KB

---

3. La dirección MAC de un dispositivo de red aparece como 00-1A-2B-3C-4D-5E. ¿Qué parte representa el OUI (Organizationally Unique Identifier)?

A network device's MAC address is shown as 00-1A-2B-3C-4D-5E. What portion represents the Organizationally Unique Identifier (OUI)?

A. 00-1A
B. 3C-4D-5E
C. 2B-3C-4D-5E
D. 00-1A-2B

---

4. Un switch tiene 24 puertos. Los puertos 1-8 están en la VLAN 10, los puertos 9-16 en la VLAN 20 y los puertos 17-24 en la VLAN 30. Todos son puertos de acceso. ¿Cuántos dominios de colisión y cuántos dominios de broadcast hay en este switch?

A switch has 24 ports. Ports 1-8 are in VLAN 10, ports 9-16 are in VLAN 20, and ports 17-24 are in VLAN 30. All ports are access ports. How many collision domains and broadcast domains exist on this switch?

A. 3 dominios de colisión, 3 dominios de broadcast
B. 24 dominios de colisión, 1 dominio de broadcast
C. 24 dominios de colisión, 3 dominios de broadcast
D. 1 dominio de colisión, 3 dominios de broadcast

---

5. Un técnico elige el cable para una conexión 10GBASE-T entre un servidor y un switch separados por 75 metros. El entorno tiene interferencia electromagnética (EMI) moderada por luces fluorescentes. ¿Qué tipo de cable cumple la especificación MÍNIMA?

A technician is selecting cable for a 10GBASE-T connection between a server and switch 75 meters apart. The environment has moderate EMI from fluorescent lighting. Which cable type meets the MINIMUM specification?

A. Cat 6 STP
B. Cat 5e UTP
C. Cat 6A UTP
D. Cat 6 UTP

---

6. Un administrador de red resume las rutas 172.16.32.0/20, 172.16.48.0/20, 172.16.64.0/20 y 172.16.80.0/20. ¿Cuál es la ruta resumida (summary route) única más pequeña que incluye las cuatro redes?

A network administrator is summarizing routes for 172.16.32.0/20, 172.16.48.0/20, 172.16.64.0/20, and 172.16.80.0/20. What is the smallest single summary route that includes all four networks?

A. 172.16.32.0/18
B. 172.16.0.0/17
C. 172.16.32.0/19
D. 172.16.0.0/16

---

7. Un switch tiene 24 puertos y 8 dispositivos conectados. ¿Cuántos dominios de colisión y dominios de broadcast activos hay? (Supón la configuración por defecto, sin VLAN)

A switch has 24 ports with 8 devices connected. How many active collision domains and broadcast domains exist? (Assume default configuration with no VLANs)

A. 8 dominios de colisión, 1 dominio de broadcast
B. 1 dominio de colisión, 8 dominios de broadcast
C. 24 dominios de colisión, 1 dominio de broadcast
D. 1 dominio de colisión, 1 dominio de broadcast

---

8. Un administrador revisa documentación de direccionamiento IP de 1995 y encuentra una red marcada como "Clase B, 172.16.0.0/16". En redes modernas sin clases (CIDR), ¿por qué la etiqueta "Clase B" resulta engañosa en la práctica?

An administrator is reviewing IP addressing documentation from 1995 and finds a network labeled as "Class B, 172.16.0.0/16." In modern classless networking (CIDR), what makes the "Class B" designation misleading for operational purposes?

A. Las redes de Clase B ya no se pueden enrutar en Internet
B. CIDR exige que todas las redes de Clase B usen máscaras de subred de longitud variable
C. La máscara /16 se puede aplicar a cualquier rango de IP, sin importar los límites históricos de las clases
D. 172.16.0.0/16 es un rango privado y, por lo tanto, no tiene clases por definición

---

9. ¿Cuál es el equivalente decimal del número binario 11001000?

What is the decimal equivalent of the binary number 11001000?

A. 224
B. 208
C. 200
D. 192

---

10. ¿Cuál es la distancia máxima de transmisión de Ethernet 1000BASE-T sobre cable UTP Cat 5e?

What is the maximum transmission distance for 1000BASE-T Ethernet over Cat 5e UTP cable?

A. 185 metros
B. 2 kilómetros
C. 500 metros
D. 100 metros

Conectividad IP

11. Un router recibe tres rutas a 192.168.0.0: 192.168.0.0/22 por OSPF, 192.168.0.0/24 por EIGRP y 192.168.0.0/16 por una ruta estática. Llega un paquete con destino 192.168.0.50. ¿Qué ruta se usa?

A router receives three routes to 192.168.0.0: 192.168.0.0/22 via OSPF, 192.168.0.0/24 via EIGRP, and 192.168.0.0/16 via static route. A packet destined for 192.168.0.50 arrives. Which route is used?

A. La ruta OSPF /22, porque OSPF tiene una AD menor que EIGRP y es más específica que la estática
B. La ruta EIGRP /24, porque tiene la coincidencia de prefijo más larga (la más específica)
C. La ruta estática /16, porque las rutas estáticas tienen la AD más baja y siempre ganan
D. El router balancea la carga entre las tres rutas para maximizar el uso de los enlaces

---

12. ¿Qué estado de un router HSRP indica que está reenviando tráfico en nombre de la dirección IP virtual?

Which HSRP router state indicates that a router is forwarding traffic on behalf of the virtual IP address?

A. Standby
B. Listen
C. Speak
D. Active

---

13. ¿Qué secuencia de comandos habilita el proceso OSPF 1 en las interfaces que están exactamente en la subred 10.1.1.0/24 y las asigna al área 0, usando una instrucción network en el modo de configuración del router?

Which command sequence enables OSPF process 1 for interfaces in exactly the 10.1.1.0/24 subnet and assigns them to area 0 using a network statement in router configuration mode?

A. interface GigabitEthernet0/0, luego ip ospf 1 area 0
B. router ospf 1, luego network 10.1.1.1 255.255.255.0 area 0
C. ip routing ospf 1 area 0
D. router ospf 1, luego network 10.1.1.0 0.0.0.255 area 0

---

14. ¿Cuál es el propósito de una ruta estática flotante (floating static route)?

What is the purpose of a floating static route?

A. Balancear la carga del tráfico entre varias rutas de igual costo
B. Redistribuir automáticamente entre protocolos de enrutamiento
C. Dar una ruta de respaldo que solo se usa si falla la ruta principal
D. Dar una ruta predeterminada hacia Internet

---

15. Dos routers OSPF en el mismo segmento Ethernet tienen esta configuración: R1 (prioridad 100, RID 10.1.1.1) y R2 (prioridad 100, RID 192.168.1.1). Si ambos arrancan al mismo tiempo, ¿qué router será el DR?

Two OSPF routers on the same Ethernet segment have the following configurations: R1 (priority 100, RID 10.1.1.1) and R2 (priority 100, RID 192.168.1.1). Assuming both routers boot simultaneously, which router will become the DR?

A. Ninguno, porque la prioridad igual causa un bloqueo mutuo (deadlock)

B. R1, porque tiene el Router ID más bajo

C. R2, porque 192.168.1.1 es una dirección IP privada

D. R2, porque tiene el Router ID más alto

---

16. Un router aprendió la misma red de destino 172.20.0.0/16 por tres fuentes de enrutamiento: OSPF, EIGRP y una ruta estática. ¿Qué ruta instalará el router en su tabla de enrutamiento?

A router has learned the same destination network 172.20.0.0/16 via three routing sources: OSPF, EIGRP, and a static route. Which route will the router install in its routing table?

A. La ruta EIGRP

B. Las tres rutas, para balancear la carga

C. La ruta estática

D. La ruta OSPF

---

17. Un router OSPF en el área 10 recibe del ABR una LSA Tipo 3 que anuncia la red 172.20.0.0/16. Más tarde recibe de un ASBR una LSA Tipo 5 que anuncia la misma red 172.20.0.0/16. Ambas LSA tienen métricas válidas. ¿Qué ruta se instala?

An OSPF router in area 10 receives a Type 3 LSA from the ABR advertising network 172.20.0.0/16. The router later receives a Type 5 LSA from an ASBR advertising the same network 172.20.0.0/16. Both LSAs have valid metrics. Which route is installed?

A. La ruta entre áreas de la LSA Tipo 3, porque las rutas intra-área e inter-área se prefieren sobre las externas

B. Ninguna ruta se instala; OSPF no puede tener el mismo prefijo anunciado como inter-área y como externo

C. Se instalan ambas rutas con multipath de igual costo (ECMP) si sus costos totales son iguales

D. La ruta externa de la LSA Tipo 5, porque las LSA Tipo 5 tienen más precedencia que las Tipo 3 en la LSDB

---

18. ¿Cuál es el tipo de red OSPF predeterminado en las interfaces Ethernet?

Which OSPF network type is the default on Ethernet interfaces?

A. Non-broadcast

B. Point-to-point

C. Broadcast

D. Point-to-multipoint

---

19. Un router OSPF en una red broadcast tiene la prioridad de su interfaz en 0. El router forma correctamente una adyacencia con el DR. ¿A qué estado OSPF llega este router con el DR?

An OSPF router on a broadcast network has its interface priority set to 0. The router successfully forms an adjacency with the DR. What OSPF state does this router reach with the DR?

A. Estado INIT, porque se intercambian paquetes hello pero no se confirma comunicación bidireccional

B. Estado EXSTART, porque comienza el intercambio de DBD pero no puede completarse sin ser elegible para DR

C. Estado FULL, porque la prioridad 0 solo impide la elección de DR/BDR, no la formación de la adyacencia

D. Estado 2-WAY, porque los routers con prioridad 0 no pueden formar adyacencias FULL en redes broadcast

---

20. Tres routers OSPF en el mismo segmento Ethernet tienen esta configuración: R1 (prioridad 100, RID 1.1.1.1), R2 (prioridad 100, RID 2.2.2.2) y R3 (prioridad 100, RID 3.3.3.3). Todos arrancan al mismo tiempo. ¿Qué afirmación es correcta cuando se forman las adyacencias?

Three OSPF routers on the same Ethernet segment have the following configurations: R1 (priority 100, RID 1.1.1.1), R2 (priority 100, RID 2.2.2.2), R3 (priority 100, RID 3.3.3.3). All routers boot simultaneously. Which statement is correct after adjacencies form?

A. R1 es DR, R2 es BDR y R3 es DROTHER
B. El router con la dirección MAC más alta es el DR
C. R2 es DR porque tiene el Router ID intermedio
D. R3 es DR, R2 es BDR y R1 es DROTHER

Acceso a la red

21. ¿Qué estado de puerto de Rapid PVST+ (IEEE 802.1w) reúne de forma más directa los estados blocking, listening y disabled del Spanning Tree Protocol heredado 802.1D?

Which Rapid PVST+ (IEEE 802.1w) port state most directly consolidates the blocking, listening, and disabled port states used in legacy 802.1D Spanning Tree Protocol?

A. Learning
B. Blocking
C. Discarding
D. Forwarding

22. ¿Qué protocolo ofrece negociación dinámica de EtherChannel y es un estándar IEEE?

Which protocol provides dynamic EtherChannel negotiation and is an IEEE standard?

A. VTP
B. PAgP
C. CDP
D. LACP

23. Un administrador de red necesita verificar las asignaciones de VLAN en un switch Cisco. ¿Qué comando muestra una tabla concisa, centrada en las VLAN, con ID de VLAN, nombres, estado y puertos de acceso asignados?

A network administrator needs to verify VLAN assignments on a Cisco switch. Which command displays a concise VLAN-centric table containing VLAN IDs, names, status, and assigned access ports?

A. show vlan brief
B. show interfaces status
C. show ip interface brief
D. show running-config

24. ¿Cuál es la función de un puerto designado (Designated Port) en el Spanning Tree Protocol?

What is the role of a Designated Port in Spanning Tree Protocol?

A. Recibe solo BPDU
B. Bloquea el tráfico para evitar bucles
C. Se conecta directamente al puente raíz (root bridge)
D. Reenvía el tráfico en un segmento de red

25. En Rapid PVST+, un switch tiene dos puertos conectados al mismo segmento Ethernet compartido, y solo uno de ellos puede ser el puerto designado de ese segmento. ¿Qué rol se asigna al segundo puerto, el no designado, de ese mismo switch?

In Rapid PVST+, a switch has two ports connected to the same shared Ethernet segment, and only one of the two can become the designated port for that segment. What role is assigned to the second, non-designated port on that same switch?

A. Puerto edge (Edge port)
B. Puerto alternativo (Alternate port)
C. Puerto de respaldo (Backup port)
D. Puerto raíz (Root port)

---

26. En un switch Cisco, un trunk IEEE 802.1Q usa el comportamiento predeterminado de etiquetado de la VLAN nativa. ¿Cómo transmite las tramas de datos ordinarias de la VLAN nativa?

On a Cisco switch, an IEEE 802.1Q trunk uses the default native-VLAN tagging behavior. How does it transmit ordinary data frames belonging to the native VLAN?

A. Con una etiqueta MPLS en lugar de una etiqueta de VLAN
B. Solo como paquetes IP de capa 3
C. Con dos etiquetas de VLAN 802.1Q
D. Sin etiqueta de VLAN 802.1Q

---

27. Un ingeniero necesita verificar qué switch es el puente raíz (root bridge) de STP para la VLAN 20. ¿Qué comando da esa información?

An engineer needs to verify which switch is the STP root bridge for VLAN 20. Which command provides this information?

A. show interfaces trunk
B. show vlan brief
C. show spanning-tree vlan 20
D. show spanning-tree summary

---

28. ¿Qué modo de punto de acceso inalámbrico (access point, AP) requiere un controlador de LAN inalámbrica para funcionar?

Which wireless access point mode requires a wireless LAN controller for operation?

A. Lightweight
B. Bridge
C. Mesh
D. Autonomous

---

29. ¿Qué función de STP se debe habilitar en los puertos conectados a dispositivos de usuario final para minimizar el tiempo de convergencia?

Which STP feature should be enabled on ports connected to end-user devices to minimize convergence time?

A. PortFast
B. BPDU Guard
C. BackboneFast
D. UplinkFast

---

30. En STP, ¿qué criterio tiene la prioridad más alta al elegir el puente raíz (root bridge)?

In STP, which criterion has the highest priority when electing the root bridge?

A. Dirección MAC más baja
B. Prioridad de puente más baja
C. Prioridad de puente más alta
D. Velocidad de puerto más rápida

Fundamentos de seguridad

31. Una red inalámbrica requiere autenticación personal con contraseña y todos los clientes admiten WPA3. ¿Qué protocolo de seguridad ofrece la mayor protección contra ataques pasivos de adivinación de contraseñas sin conexión (offline)?

A wireless network requires password-based personal authentication, and all clients support WPA3. Which security protocol provides the strongest protection against passive offline password-guessing attacks?

A. WPA3-Personal con SAE
B. WEP con claves de 128 bits
C. WPA2-Enterprise con AES-CCMP
D. WPA2-Personal con TKIP

---

32. Una red usa la ACL extendida 110 aplicada de entrada (inbound) en la interfaz de un router. La primera entrada (ACE) es 'access-list 110 deny tcp any any eq 23'. ¿Qué tráfico bloqueará esta ACE?

A network uses extended ACL 110 applied inbound on a router interface. The first ACE is 'access-list 110 deny tcp any any eq 23'. What traffic will this ACE block?

A. Tráfico SSH desde cualquier origen hacia cualquier destino
B. Todo el tráfico TCP desde cualquier origen hacia cualquier destino
C. Tráfico Telnet desde cualquier origen hacia cualquier destino
D. Tráfico Telnet dirigido solo a la interfaz del router

---

33. Una empresa necesita conectar dos sedes por Internet con una VPN. La conexión debe admitir tráfico multicast y varios protocolos (IPv4, IPv6, IPX). ¿Qué tecnología VPN es la MÁS adecuada?

A company needs to connect two sites over the internet with a VPN. The connection must support multicast traffic and multiple protocols (IPv4, IPv6, IPX). Which VPN technology is MOST appropriate?

A. SSL VPN
B. PPTP
C. GRE sobre IPsec
D. Solo IPsec en modo túnel

---

34. ¿Qué significa AAA en seguridad de redes?

What does AAA stand for in network security?

A. Access, Authentication, and Administration (Acceso, Autenticación y Administración)
B. Authentication, Accounting, and Auditing (Autenticación, Contabilización y Auditoría)
C. Authentication, Authorization, and Accounting (Autenticación, Autorización y Contabilización)
D. Authorization, Access, and Auditing (Autorización, Acceso y Auditoría)

---

35. Un administrador necesita bloquear el tráfico IP de la red 192.168.10.0/24 hacia un servidor en 10.1.1.100. ¿En qué interfaz del router se debe colocar una ACL estándar para minimizar su efecto en el tráfico hacia otros destinos?

An administrator needs to block IP traffic from the 192.168.10.0/24 network toward a server at 10.1.1.100. On which router interface should a standard ACL be placed to minimize its impact on traffic to other destinations?

A. En el puerto del switch del servidor
B. En la interfaz del router más cercana al origen (192.168.10.0/24)
C. En todas las interfaces intermedias del router
D. En la interfaz del router más cercana al destino (10.1.1.100)

---

36. Un técnico revisa la configuración en ejecución de un router y ve 'enable secret 5 1mERr$hx5rVt7rPNoS4wqbXKX7m0'. ¿Qué tipo de protección se usa para esta contraseña enable secret?

A technician examines a router's running configuration and sees 'enable secret 5 1mERr$hx5rVt7rPNoS4wqbXKX7m0'. What type of encryption is used for this enable secret password?

A. Hash SHA-256 (tipo 8)
B. Hash MD5 (tipo 5)
C. Hash Scrypt (tipo 9)
D. Cifrado Vigenère simple (tipo 7)

---

37. Una empresa requiere autenticación centralizada con contabilización (accounting) completa de comandos y autorización por comando para todos los administradores que acceden a routers y switches Cisco. ¿Qué protocolo AAA es el MÁS adecuado para este requisito?

A company requires centralized authentication with full command accounting and per-command authorization for all network administrators accessing Cisco routers and switches. Which AAA protocol is BEST suited for this requirement?

A. TACACS+
B. RADIUS
C. Kerberos
D. Autenticación local

---

38. Una ACL extendida contiene solo la instrucción 'access-list 101 permit tcp any any established'. Un paquete TCP con solo el indicador (flag) SYN activado, desde 203.0.113.50 y con destino 198.51.100.10 puerto 443, llega a la interfaz donde la ACL 101 se aplica de entrada. ¿Qué pasa con este paquete?

An extended ACL consists only of the statement 'access-list 101 permit tcp any any established'. A TCP packet with only the SYN flag set, from 203.0.113.50 destined for 198.51.100.10 port 443, arrives at the interface where ACL 101 is applied inbound. What is the fate of this packet?

A. Se permite, porque es parte del establecimiento de una conexión TCP
B. Se deniega, porque el indicador SYN solo no coincide con la palabra clave 'established'
C. Se permite solo si existe una entrada correspondiente en la tabla de estados TCP
D. Se deniega, porque las ACL extendidas no pueden permitir el puerto TCP 443

---

39. Una empresa requiere autenticación centralizada con contabilización (accounting) completa de comandos y la capacidad de cifrar todo el contenido de la autenticación. ¿Qué protocolo AAA cumple MEJOR estos requisitos?

A company requires centralized authentication with full command accounting and the ability to encrypt the entire authentication payload. Which AAA protocol BEST meets these requirements?

A. RADIUS
B. Kerberos
C. Autenticación con base de datos local
D. TACACS+

---

40. Una ACL extendida debe permitir tráfico solo del host 192.168.5.45. ¿Cuál es la máscara wildcard correcta?

An extended ACL needs to permit traffic from host 192.168.5.45 only. What is the correct wildcard mask?

A. 0.0.0.0
B. 0.0.0.255
C. 255.255.255.255
D. 255.255.255.0

Automatización y programabilidad

41. Un arquitecto de redes diseña una solución de redes definidas por software (SDN). ¿Qué plano es responsable de ejecutar las acciones de reenvío de paquetes según las reglas programadas por el controlador SDN?

A network architect is designing a Software-Defined Networking solution. Which plane is responsible for executing packet-forwarding actions based on rules programmed by the SDN controller?

A. Plano de administración (management plane)
B. Plano de aplicación (application plane)
C. Plano de datos (data plane)
D. Plano de control (control plane)

---

42. Una API REST devuelve esta respuesta JSON para una consulta de interfaz: {"status": "up", "speed": "1000", "duplex": "full"}. Un script de Python intenta hacer un cálculo matemático con el valor de speed y genera un TypeError. ¿Cuál es el problema?

A REST API returns the following JSON response for an interface query: {"status": "up", "speed": "1000", "duplex": "full"}. A Python script attempts to perform a mathematical calculation using the speed value and raises a TypeError. What is the issue?

A. Al JSON le falta el campo obligatorio "unit"
B. La API devolvió una sintaxis JSON inválida
C. El valor de speed es una cadena de texto, no un entero
D. La biblioteca JSON de Python no admite objetos anidados

---

43. Una empresa migra de una red de campus tradicional de tres capas a una fabric Cisco SD-Access. ¿Cuál es el cambio arquitectónico PRINCIPAL?

A company migrates from a traditional three-tier campus network to a Cisco SD-Access fabric. What is the PRIMARY architectural change?

A. Los requisitos de cableado físico se reducen un 50% porque el acceso es solo inalámbrico
B. La red usa superposiciones VXLAN para la segmentación en lugar de VLAN tradicionales
C. Los protocolos de enrutamiento se desactivan y los switches toman todas las decisiones de reenvío
D. Todo el tráfico se enruta por Internet para aplicar las políticas

---

44. ¿Cuál es el propósito de un modelo de datos YANG en la programabilidad de redes?

What is the purpose of a YANG data model in network programmability?

A. YANG comprime archivos de configuración grandes para transferirlos más rápido
B. YANG define la estructura y las restricciones de los datos de configuración y operación
C. YANG cifra los datos de configuración durante la transmisión por API
D. YANG reemplaza los comandos CLI con flujos de trabajo gráficos

---

45. Un ingeniero recibe un código de estado 409 Conflict al intentar crear una VLAN nueva mediante la API REST de un switch Cisco. El ID de la VLAN es válido y está dentro del rango permitido. ¿Cuál es la causa MÁS probable?

An engineer receives a 409 Conflict status code when attempting to create a new VLAN via REST API on a Cisco switch. The VLAN ID is valid and within the allowed range. What is the MOST likely cause?

A. El switch está procesando otro cambio de configuración
B. La carga útil (payload) de la solicitud tiene una sintaxis JSON inválida
C. Ya existe una VLAN con ese ID en el switch
D. Las credenciales de la API no tienen privilegios suficientes

---

46. ¿Qué error de sintaxis JSON impediría analizar correctamente este fragmento de configuración? {"hostname": "SW1", "vlan": 10, "ports": ["Gi0/1", "Gi0/2"], "enabled": true}

Which JSON syntax error would prevent this configuration snippet from being parsed correctly?
{"hostname": "SW1", "vlan": 10, "ports": ["Gi0/1", "Gi0/2"], "enabled": true}

A. El valor de hostname debería usar comillas simples en lugar de comillas dobles
B. El valor de vlan debería ir entre comillas como cadena de texto
C. Este JSON es sintácticamente correcto
D. El arreglo debería usar paréntesis en lugar de corchetes

---

47. Un ingeniero escribe un script de Python con la biblioteca ncclient para enviar configuraciones por NETCONF. El script se conecta bien, pero la operación edit-config falla con el error "missing-element". El XML está bien formado. ¿Cuál es la causa MÁS probable?

An engineer writes a Python script using the ncclient library to push configurations via NETCONF. The script connects successfully but the edit-config operation fails with "missing-element" error. The XML payload is well-formed. What is the MOST likely cause?

A. El modelo YANG exige un elemento obligatorio que no se incluyó en la carga útil
B. La declaración del espacio de nombres (namespace) en el XML es incorrecta
C. El dispositivo no admite la capacidad writable-running
D. Otra sesión bloqueó el datastore de destino

---

48. Una API exige autenticación antes de permitir cambios de configuración. ¿Qué método de autenticación ofrece acceso basado en tokens que expiran tras un período fijo, lo que reduce el riesgo de exponer las credenciales?

An API requires authentication before allowing configuration changes. Which authentication method provides token-based access that expires after a set period, reducing the risk of credential exposure?

A. Cadenas de comunidad SNMP
B. OAuth 2.0 con tokens bearer
C. Autenticación básica con codificación Base64
D. Autenticación SSH con clave pública

---

49. Una llamada a una API REST de un dispositivo Cisco devuelve este JSON: {"status": "success", "vlan_id": 100, "vlan_name": "Engineering", "active": true}

¿Cuál es el tipo de dato de la clave "active"?

A REST API call to a Cisco device returns the following JSON:
{"status": "success", "vlan_id": 100, "vlan_name": "Engineering", "active": true}

What is the data type of the "active" key?

A. Booleano (Boolean)
B. Objeto (Object)
C. Cadena de texto (String)
D. Entero (Integer)

---

50. Un script de automatización de red envía una solicitud a una API REST para eliminar una VLAN, y el servidor responde con el código de estado HTTP 204. ¿Qué indica esto?

A network automation script sends a REST API request to delete a VLAN, and the server responds with HTTP status code 204. What does this indicate?

A. La VLAN no se encontró en el dispositivo
B. El servidor tuvo un error interno
C. La solicitud se rechazó por un fallo de autenticación
D. La solicitud tuvo éxito y no se devuelve contenido

Respuesta correcta

1. A VLSM (máscaras de longitud variable) exige subredes que no se solapen. El /26 ocupa de .0 a .63 y el /27 de .64 a .95, así que la primera dirección libre es .96. Un /30 tiene 4 direcciones y exactamente 2 de host (2^2 - 2 = 2). 192.168.20.96/30 cubre de .96 a .99. 192.168.20.92/30 se solapa con el /27. El /29 da 6 hosts. 192.168.20.128/30 sirve, pero no es la dirección más baja.

2. D La ventana efectiva de TCP es el mínimo entre la ventana de congestión (32 KB) y la ventana anunciada por el receptor (24 KB), es decir, 24 KB. Como ya hay 10 KB sin confirmar, el emisor puede enviar 24 - 10 = 14 KB más. 22 KB resta de la ventana de congestión (32 - 10). 24 KB ignora los datos en tránsito. 32 KB usa solo la ventana de congestión e ignora el límite del receptor.

3. D El OUI son los primeros 24 bits (los 3 primeros octetos) de la dirección MAC de 48 bits, y el IEEE lo asigna para identificar al fabricante. Aquí 00-1A-2B identifica al fabricante. Los otros 3 octetos (3C-4D-5E) los asigna el fabricante e identifican la interfaz. 00-1A tiene solo 16 bits. 2B-3C-4D-5E mezcla el OUI con la parte del dispositivo.

4. C Cada puerto de un switch forma su propio dominio de colisión (collision domain), así que hay 24 (microsegmentación). Cada VLAN forma un dominio de broadcast (broadcast domain) aparte, así que 3 VLAN dan 3. Decir 1 dominio de broadcast ignora las VLAN. Decir 3 dominios de colisión supone que siguen a las VLAN. Decir 1 dominio de colisión confunde el switch con un hub.

5. C Cat 6A UTP cumple el estándar de cableado 10GBASE-T hasta 100 metros. Cat 6 normalmente se especifica para 10GBASE-T hasta 55 metros, según la instalación, y aquí se necesitan 75. Cat 5e no está especificado para 10GBASE-T a esa distancia. El blindaje de Cat 6 STP ayuda con la EMI, pero no garantiza el rendimiento de 10GBASE-T a 75 metros.

6. B 172.16.0.0/17 es el resumen único más pequeño que cubre las cuatro redes. Su rango va de 172.16.32.0 a 172.16.95.255. Los valores 32 y 95 del tercer octeto solo comparten el primer bit, lo que da un prefijo común de 17 bits. Ese resumen incluye direcciones de más. 172.16.32.0/19 cubre solo las dos primeras redes. 172.16.32.0/18 no es un límite de red /18 válido. El /16 incluye aún más direcciones sobrantes.

7. A Un switch crea un dominio de colisión (collision domain) por cada puerto activo: 8 dispositivos son 8 dominios, porque el almacenamiento en búfer y el full-duplex eliminan las colisiones. Por defecto todos los puertos están en la misma VLAN y comparten un solo dominio de broadcast (broadcast domain). Contar 24 dominios cuenta puertos inactivos. 1 dominio de colisión y 1 de broadcast describe un hub, no un switch.

8. C CIDR (Classless Inter-Domain Routing) eliminó la estructura rígida de clases A, B y C. Con CIDR, una máscara /16 se puede aplicar a cualquier red (por ejemplo 10.0.0.0/16), sin importar el primer octeto. La etiqueta "Clase B" es un resto histórico: los routers solo miran la longitud del prefijo. Muchas IP públicas siguen en rangos de Clase B, ser privada (RFC 1918) no depende de CIDR, y CIDR no exige usar VLSM.

9. C Al convertir 11001000 a decimal: 128 + 64 + 8 = 200, porque los bits en 1 son los de valor 128, 64 y 8. 192 sería 11000000, 208 sería 11010000 y 224 sería 11100000. Convertir rápido los valores comunes de un octeto (128, 192, 224, 240, 248, 252, 254, 255) es clave para calcular subredes.

10. D La longitud máxima de cable para 1000BASE-T (Gigabit Ethernet) sobre UTP Cat 5e o Cat 6 es de 100 metros (328 pies), según IEEE 802.3ab. Incluye hasta 90 metros de cableado horizontal y 10 metros de cables de conexión (patch cables). 185 metros era el límite del coaxial delgado 10BASE2 y 500 metros el del coaxial grueso 10BASE5. 2 kilómetros no corresponde al alcance de 1000BASE-LX, que llega a 5 km.

11. B La coincidencia de prefijo más largo (longest prefix match) SIEMPRE se aplica antes que la distancia administrativa (AD). 192.168.0.50 entra en los tres prefijos, pero el /24 es el más específico, así que se usa la ruta EIGRP, aunque su AD (90) sea mayor que la de la estática (1). El /22 es más específico que el /16, pero menos que el /24. La AD solo se compara entre rutas con el MISMO prefijo. El balanceo de carga no aplica entre prefijos distintos.

12. D El estado Active indica que el router HSRP reenvía los paquetes de la IP virtual y responde a las solicitudes ARP de esa IP. Solo un router por grupo HSRP puede estar Active a la vez. Standby es el respaldo: vigila al router Active y toma su lugar si falla. En Listen el router recibe anuncios HSRP, pero no es Active ni Standby. Speak es un estado de transición durante la elección, en el que se intercambian prioridades.

13. D La secuencia correcta es 'router ospf 1' y luego 'network 10.1.1.0 0.0.0.255 area 0'. El método tradicional usa el comando network dentro del proceso OSPF con una máscara wildcard. La configuración en la interfaz (ip ospf 1 area 0) es válida, pero no es el método pedido en modo router. 255.255.255.0 se interpretaría como wildcard y no coincidiría exactamente con la subred. 'ip routing ospf 1 area 0' no es sintaxis válida.

14. C Una ruta estática flotante tiene una distancia administrativa (AD) mayor que la ruta principal (por ejemplo AD 5 en lugar de 1), así que solo entra en la tabla de enrutamiento cuando la principal no está disponible. Se usa para enlaces de respaldo o para preferir un protocolo dinámico (como OSPF, AD 110). No balancea carga (eso requiere rutas de igual costo) ni redistribuye rutas. Podría apuntar a Internet, pero lo que la define es ser un respaldo.

15. D Si las prioridades OSPF son iguales (ambas 100), el desempate es el Router ID (RID) más alto. 192.168.1.1 es mayor que 10.1.1.1, así que R2 es el DR. Que 192.168.1.1 sea privada no importa: OSPF trata igual a todos los RID de 32 bits. La prioridad igual no causa un bloqueo mutuo: OSPF pasa al siguiente criterio. En la elección del DR gana la prioridad más alta y luego el RID más alto.

16. C Los routers Cisco usan la distancia administrativa (AD) para elegir entre rutas de distintas fuentes. La estática tiene AD 1 (la más confiable), EIGRP tiene AD 90 y OSPF tiene AD 110. Se elige la ruta con la AD más baja, así que gana la estática. El balanceo de carga solo ocurre con rutas de igual AD y métrica, lo que aquí no pasa. La AD se evalúa antes que la métrica.

17. A El orden de preferencia de OSPF es: intra-área (Tipo 1/2), inter-área (Tipo 3), externa E1 y externa E2 (Tipo 5). Aunque ambas LSA anuncien el mismo prefijo, gana la ruta inter-área Tipo 3, porque está más arriba en esa jerarquía. Las LSA Tipo 5 NO tienen más precedencia: las rutas externas son las menos preferidas. ECMP solo aplica a rutas del MISMO tipo y costo igual. OSPF SÍ puede recibir anuncios solapados.

18. C Broadcast es el tipo de red OSPF predeterminado en Ethernet y otros medios de acceso múltiple. OSPF elige un DR (Designated Router) y un BDR (Backup Designated Router) para reducir adyacencias e inundación de LSA. Point-to-point es el predeterminado en enlaces seriales y no elige DR/BDR. Non-broadcast se usa en redes NBMA y exige configurar vecinos a mano. Point-to-multipoint también es para NBMA, pero trata cada enlace como punto a punto, sin DR/BDR.

19. C Un router con prioridad OSPF 0 llega al estado FULL con el DR y el BDR. La prioridad 0 solo lo hace inelegible para ser DR o BDR, pero no impide la adyacencia. En redes broadcast, TODOS los routers forman adyacencias FULL con el DR y el BDR (intercambian la LSDB completa) y solo 2-WAY con los demás DROTHER. INIT y EXSTART son estados de transición previos a FULL.

20. D Con prioridades iguales (100), el desempate es el Router ID. OSPF elige el RID MÁS ALTO como DR y el segundo más alto como BDR. R3 (3.3.3.3) es DR, R2 (2.2.2.2) es BDR y R1 (1.1.1.1) es DROTHER. Elegir el RID más bajo invierte la lógica. No existe una regla del RID intermedio. Las direcciones MAC no intervienen en la elección del DR de OSPF.

21. C Rapid PVST+ reduce los cinco estados originales de 802.1D a tres: discarding, learning y forwarding. El estado discarding absorbe las funciones de los antiguos blocking, listening y disabled, porque en los tres casos el puerto no reenvía tramas ni aprende direcciones MAC. Learning y Forwarding equivalen directamente a sus estados heredados. Blocking ya no existe como nombre de estado en RSTP.

22. D LACP (Link Aggregation Control Protocol), definido en IEEE 802.3ad, es el protocolo estándar para negociar dinámicamente grupos EtherChannel. Es neutral respecto al fabricante y funciona entre switches de distintas marcas. PAgP (Port Aggregation Protocol) es propietario de Cisco. VTP (VLAN Trunking Protocol) sincroniza la base de datos de VLAN, no agrega enlaces. CDP (Cisco Discovery Protocol) descubre vecinos, no forma EtherChannel.

23. A 'show vlan brief' muestra en una tabla concisa los ID de VLAN, nombres, estado y puertos de acceso asignados. 'show interfaces status' muestra velocidad, dúplex y VLAN por puerto, pero no la tabla centrada en las VLAN. 'show running-config' muestra toda la configuración y hay que buscar las VLAN a mano. 'show ip interface brief' muestra información de capa 3 de interfaces enrutadas y SVI, no la pertenencia a VLAN de capa 2.

24. D Un puerto designado en STP reenvía el tráfico de su segmento hacia el puente raíz (root bridge). Cada segmento tiene un puerto designado: el de menor costo de ruta hacia el puente raíz. El puerto raíz (Root Port) es el que conecta a un switch no raíz hacia el puente raíz. Los puertos que bloquean para evitar bucles están en estado Blocking (o Alternate/Backup en RSTP). Todos los puertos reciben BPDU, pero los designados además reenvían tráfico.

25. C El puerto de respaldo (backup port) de RSTP existe para cuando un mismo switch tiene dos o más puertos en el mismo segmento compartido (normalmente por un hub) y solo uno puede ser designado. El puerto que pierde queda como respaldo del designado en ese mismo switch. El puerto alternativo da una ruta de respaldo hacia el puente raíz (root bridge) por otro switch u otro segmento. El puerto raíz es la mejor ruta hacia la raíz. El puerto edge conecta a un equipo final.

26. D Las tramas de datos de la VLAN nativa se transmiten sin etiqueta (untagged) por defecto, así que la respuesta es "sin etiqueta de VLAN 802.1Q". Dos etiquetas 802.1Q no describen el comportamiento predeterminado de la VLAN nativa. Una etiqueta MPLS no tiene relación con el reenvío normal en un trunk 802.1Q. Un trunk reenvía tramas Ethernet, no solo paquetes IP de capa 3.

27. C 'show spanning-tree vlan 20' muestra la topología STP de la VLAN 20: el ID del puente raíz, la prioridad del switch local y los roles y estados de los puertos. Indica si el switch local es la raíz o muestra el ID de la raíz. 'show vlan brief' lista las VLAN, no los roles STP. 'show interfaces trunk' muestra el estado de los trunks y las VLAN permitidas. 'show spanning-tree summary' da un resumen, no identifica la raíz de la VLAN 20.

28. A Los AP lightweight (LAP) dependen de un controlador de LAN inalámbrica (WLC) para su configuración, administración e inteligencia, y se comunican con él mediante CAPWAP. El AP casi no guarda configuración. Los AP autonomous son independientes y no necesitan controlador. Mesh es una topología en la que los AP se conectan entre sí por radio, y pueden ser lightweight o autonomous. El modo bridge conecta dos redes cableadas de forma inalámbrica y no exige controlador.

29. A PortFast pasa un puerto de acceso al estado Forwarding en cuanto el enlace sube, sin esperar los 30 segundos de Listening y Learning. Es seguro en equipos finales (PC, impresoras), que no crean bucles. UplinkFast y BackboneFast son optimizaciones heredadas para fallas de enlaces de subida e indirectos, no para puertos de usuario. BPDU Guard es una función de seguridad que desactiva un puerto PortFast si recibe una BPDU, pero no reduce la convergencia.

30. B La elección del puente raíz se basa en el ID de puente (bridge priority) (bridge ID) más bajo, que combina la prioridad del puente y la dirección MAC. Primero se evalúa la prioridad y gana el switch con el valor más bajo. Si hay empate, desempata la dirección MAC más baja. El valor de prioridad más alto pierde, porque gana el más bajo. La velocidad del puerto no cuenta en la elección, aunque sí afecta el costo de los puertos.

31. A WPA3-Personal con SAE (Simultaneous Authentication of Equals) reemplaza la autenticación PSK de WPA2-Personal y ofrece secreto hacia adelante (forward secrecy) y protección contra ataques de diccionario offline pasivos. WPA2-Enterprise usa autenticación empresarial, no la personal que se pide. TKIP es más débil y quedó obsoleto en 2012. WEP se rompe en minutos con ataques como FMS, KoreK y PTW, sin importar la longitud de la clave.

32. C El puerto 23 es el puerto conocido de Telnet, así que 'eq 23' coincide con sesiones Telnet. Con origen 'any' y destino 'any', coincide con el tráfico Telnet de cualquier origen a cualquier destino. SSH usa el puerto 22, por lo que no coincide. La ACE solo aplica a TCP puerto 23, no a otros puertos como HTTP (80) o HTTPS (443). Una ACL de entrada puede filtrar tráfico en tránsito y tráfico dirigido al propio router.

33. C GRE (Generic Routing Encapsulation) sobre IPsec combina la capacidad de GRE de transportar multicast y varios protocolos con el cifrado y la autenticación de IPsec. GRE no depende del protocolo y admite protocolos de enrutamiento (OSPF, EIGRP), multicast e IPv6. IPsec en modo túnel solo admite tráfico IP unicast. SSL VPN es para clientes de acceso remoto, no sitio a sitio. PPTP está obsoleto y es inseguro.

34. C AAA significa Authentication (verificar la identidad del usuario), Authorization (dar permisos según esa identidad) y Accounting (registrar la actividad y el uso de recursos). Se implementa con protocolos como TACACS+ y RADIUS. Las otras opciones cambian los términos: agregan administración o acceso, que no forman parte de AAA, o reemplazan accounting por auditing. La que omite authorization quita el paso que define qué puede hacer un usuario autenticado.

35. D Las ACL estándar solo filtran por dirección IP de origen, no por puerto ni protocolo. Se colocan lo más cerca posible del destino, para no bloquear tráfico legítimo de esa red hacia otros destinos. Si se colocara cerca del origen, se bloquearía todo lo que sale de 192.168.10.0/24. Ponerla en todas las interfaces intermedias desperdicia recursos. El puerto del switch no es una interfaz de router. Regla: estándar cerca del destino, extendida cerca del origen.

36. B El '5' indica un hash MD5. 'enable secret' siempre usa hash (no es reversible), por eso es más seguro que 'enable password'. El tipo 7 es un cifrado Vigenère débil que usa 'service password-encryption' y se revierte fácilmente. El tipo 8 es PBKDF2-SHA256 y el tipo 9 es scrypt, ambos más fuertes. MD5 está en desuso para instalaciones nuevas, pero sigue siendo común en configuraciones antiguas.

37. A TACACS+ separa autenticación, autorización y contabilización, y cifra todo el contenido del paquete, no solo las contraseñas. Admite autorización por comando: controla qué comandos ejecuta cada usuario. RADIUS combina autenticación y autorización y usa principalmente UDP, por lo que sirve más para dar acceso a la red. La autenticación local no es centralizada. Kerberos usa tickets y no ofrece esa autorización y registro por comando.

38. B La palabra clave 'established' coincide con paquetes TCP que tienen el indicador ACK o RST. NO coincide con un paquete que solo tiene SYN, como el primero del handshake de TCP. Como la ACL termina con un deny implícito, el paquete se descarta. Así se permite el tráfico de respuesta, pero se bloquean los intentos nuevos de conexión entrantes. Las ACL de Cisco IOS no guardan estado: no hay tabla de estados TCP (eso es de firewalls con estado, como ASA).

39. D TACACS+ cifra todo el contenido del paquete (no solo la contraseña) y separa autenticación, autorización y contabilización, lo que permite un registro detallado por comando. RADIUS solo cifra el campo de la contraseña y combina autenticación con autorización, por eso sirve menos para registrar comandos. La base de datos local no es centralizada: cada dispositivo tiene sus propios usuarios. Kerberos no se usa comúnmente para AAA en dispositivos Cisco.

40. A Una máscara wildcard 0.0.0.0 indica una coincidencia exacta con un solo host: todos los bits deben coincidir (0 = debe coincidir, 1 = no importa). Equivale a 'host 192.168.5.45' en la sintaxis de ACL. 255.255.255.255 significa 'any': todos los bits no importan. 0.0.0.255 coincide con los tres primeros octetos y acepta cualquier valor en el cuarto (una subred /24). 255.255.255.0 es lo contrario de lo que se necesita. La wildcard es la inversa de la máscara de subred.

41. C El plano de datos (data plane o forwarding plane) ejecuta las acciones de reenvío según las tablas de flujo y las políticas que instala el controlador SDN. En SDN la lógica del plano de control se centraliza en el controlador y el dispositivo solo reenvía. El plano de administración configura y monitorea. El de aplicación contiene las aplicaciones que hablan con el controlador por APIs northbound.

42. C El valor de speed es una cadena (string) porque "1000" está entre comillas en el JSON. json.loads() de Python conserva ese tipo, así que una operación como speed + 2 genera un TypeError. Se corrige con int(data['speed']). La falta de un campo "unit" no causaría TypeError (sería un KeyError al acceder a él). El JSON es sintácticamente válido, y la biblioteca de Python sí admite objetos anidados. Conviene validar y convertir tipos antes de calcular.

43. B SD-Access usa túneles overlay VXLAN (Virtual Extensible LAN) para crear segmentos lógicos (Virtual Networks) sobre un underlay IP físico, y reemplaza la segmentación basada en VLAN con microsegmentación por políticas. El underlay sigue usando protocolos de enrutamiento (normalmente IS-IS u OSPF). El tráfico se queda dentro de la fabric, sin pasar por Internet. SD-Access admite equipos cableados e inalámbricos, y el cableado sigue siendo necesario.

44. B YANG es un lenguaje de modelado de datos que define el esquema de los datos de configuración y de estado operativo: qué datos existen, sus tipos, rangos válidos, campos obligatorios u opcionales y sus relaciones. NETCONF y RESTCONF usan modelos YANG para intercambiar datos validados entre controladores y dispositivos. YANG no cifra (lo hacen SSH y HTTPS), no ofrece interfaz gráfica y no comprime datos. La eficiencia depende del formato de codificación (XML, JSON).

45. C HTTP 409 Conflict indica un conflicto con el estado del recurso: aquí, intentar crear una VLAN que ya existe. Es el uso clásico del 409. La falta de privilegios devolvería 401 Unauthorized o 403 Forbidden. Un JSON inválido generaría 400 Bad Request. Los cambios simultáneos pueden causar conflictos en algunos sistemas, pero en REST el 409 apunta a un intento de crear un recurso duplicado. Es común confundir el 409 con el 423 Locked.

46. C Este JSON es válido. JSON exige comillas dobles (no simples) en claves y cadenas, así que el hostname está bien. El valor de vlan es un número (10) y se escribe sin comillas: JSON distingue cadenas (con comillas) de números (sin comillas). Los arreglos (arrays) llevan corchetes [ ], no paréntesis. El booleano 'true' va en minúsculas y sin comillas. Los errores comunes son comillas simples, comas faltantes o sobrantes y corchetes sin cerrar, y aquí no hay ninguno.

47. A "missing-element" indica una violación de una restricción del modelo YANG: falta en el XML una hoja (leaf) o un contenedor obligatorio definido en el modelo. Es una falla de validación del esquema. Si faltara la capacidad writable-running, el error sería "operation-not-supported". Un namespace incorrecto daría "unknown-namespace" o errores de análisis. Un datastore bloqueado devuelve "in-use" o "resource-denied".

48. B OAuth 2.0 usa tokens bearer con tiempo limitado, que se emiten tras la autenticación inicial y expiran solos. Así, un token robado sirve poco tiempo. La aplicación envía el token, no las credenciales. La autenticación básica envía usuario y contraseña en cada solicitud, y Base64 no es cifrado. La clave pública SSH es fuerte para la CLI, pero no suele usarse en APIs REST sobre HTTP y no expira sola. Las cadenas SNMP son secretos en texto plano que no expiran.

49. A El tipo es booleano porque true (en minúsculas y sin comillas) es un literal booleano de JSON. Los valores booleanos se escriben true o false, sin comillas. Una cadena iría entre comillas, como "Engineering". Un entero es un número sin comillas, como 100. Un objeto es una estructura anidada entre llaves. Conocer los tipos de dato de JSON es esencial para leer bien las respuestas de una API en scripts de automatización.

50. D HTTP 204 No Content indica que la solicitud se procesó con éxito y no hay cuerpo de respuesta. Es típico de las operaciones DELETE, donde basta con confirmar la eliminación. Si no se encontrara la VLAN, el servidor devolvería 404 Not Found. Los fallos de autenticación devuelven 401 Unauthorized o 403 Forbidden. Los errores internos devuelven 500. Los códigos 2xx indican éxito, 4xx errores del cliente y 5xx errores del servidor.

Palabras clave en inglés

subnet	subred	Parte de una red IP más grande, definida por su máscara.
VLSM (variable-length subnet mask)	máscara de subred de longitud variable	Dividir una red en subredes de distinto tamaño.
usable host addresses	direcciones de host utilizables	Direcciones de la subred que puedes asignar a equipos.
summary route	ruta resumida	Una sola ruta que representa varias redes.
collision domain	dominio de colisión	Zona donde las tramas pueden chocar; una por puerto de switch.
broadcast domain	dominio de broadcast o de difusión	Equipos que reciben el mismo broadcast; uno por VLAN.
OUI (Organizationally Unique Identifier)	identificador del fabricante	Primeros 24 bits de una dirección MAC.
congestion window	ventana de congestión	Límite que TCP pone a los datos enviados sin confirmar.
acknowledgment (ACK)	acuse de recibo	Mensaje que avisa que los datos llegaron.
routing table	tabla de enrutamiento	Lista de redes y caminos que usa el router.
longest prefix match	coincidencia del prefijo más largo	Regla por la que gana la ruta más específica.
administrative distance (AD)	distancia administrativa	Confianza en la fuente de una ruta; gana el valor más bajo.
static route	ruta estática	Ruta que el administrador configura a mano.
floating static route	ruta estática flotante	Ruta de respaldo con distancia administrativa más alta.
neighbor adjacency	adyacencia entre vecinos	Relación entre dos routers OSPF para compartir su información.
router ID (RID)	identificador del router	Número de 32 bits que identifica a cada router OSPF.
designated router (DR)	router designado	Router OSPF elegido para reducir adyacencias en una red broadcast.
tiebreaker	criterio de desempate	Lo que decide cuando dos valores son iguales.
first-hop redundancy	redundancia de primer salto	Puerta de enlace de respaldo para los equipos; HSRP la ofrece.
preempt	retomar el papel activo	Opción HSRP para que el router de mayor prioridad tome el control.

access port	puerto de acceso	Puerto de switch asignado a una VLAN para un equipo final.
trunk	enlace troncal	Enlace que lleva el tráfico de varias VLAN.
native VLAN	VLAN nativa	VLAN que cruza el troncal sin etiqueta por defecto.
untagged frame	trama sin etiqueta	Trama que no lleva la marca 802.1Q de VLAN.
root bridge	puente raíz	Switch de referencia de STP, con el bridge ID más bajo.
designated port	puerto designado	Puerto STP que reenvía tráfico en su segmento.
alternate port	puerto alternativo	Puerto RSTP de respaldo hacia el puente raíz por otro camino.
convergence	convergencia	Proceso en que la red se estabiliza después de un cambio.
link aggregation	agregación de enlaces	Unir varios enlaces físicos en uno lógico, como EtherChannel.
wireless LAN controller (WLC)	controlador de red inalámbrica	Equipo que administra los puntos de acceso lightweight.
access control list (ACL)	lista de control de acceso	Reglas que permiten o bloquean tráfico en orden.
wildcard mask	máscara wildcard o comodín	Máscara inversa: 0 debe coincidir, 1 no importa.
implicit deny	denegación implícita	Regla invisible al final de una ACL que bloquea lo demás.
inbound / outbound	entrante / saliente	Sentido del tráfico respecto a la interfaz.
accounting	contabilización, registro de actividad	Parte de AAA que guarda lo que hizo cada usuario.
payload	carga útil	Datos que transporta un paquete o una solicitud.
site-to-site VPN	VPN de sitio a sitio	Túnel seguro que conecta dos sedes por Internet.
data plane	plano de datos	Parte que reenvía los paquetes.
control plane	plano de control	Parte que decide los caminos; en SDN vive en el controlador.
status code	código de estado	Número HTTP que indica el resultado de una solicitud.

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/ccna/