examundo

Simulado CCNA 200-301 em português

50 questões com respostas. Os guias e as traduções foram feitos e revisados por software. Ainda não foram revisados por nenhuma pessoa.

Atualizado em 25 de novembro de 2026 · examundo.tech/pt/ccna/

Fundamentos de rede

1. Um engenheiro de rede alocou 192.168.20.0/26 para a VLAN 10 e 192.168.20.64/27 para a VLAN 20, a partir do bloco 192.168.20.0/24. Qual sub-rede disponível oferece exatamente 2 endereços de host utilizáveis para um enlace WAN ponto a ponto e tem o menor endereço de rede?

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. A janela de congestionamento (congestion window) de um emissor TCP é de 32 KB, e o receptor anuncia uma janela de 24 KB. O emissor tem 10 KB de dados enviados e ainda não confirmados. Quantos dados adicionais o emissor pode transmitir antes de esperar uma confirmação (ACK)?

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. O endereço MAC de um dispositivo de rede aparece como 00-1A-2B-3C-4D-5E. Qual parte representa o 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. Um switch tem 24 portas. As portas 1-8 estão na VLAN 10, as portas 9-16 na VLAN 20 e as portas 17-24 na VLAN 30. Todas as portas são portas de acesso (access ports). Quantos domínios de colisão e domínios de broadcast existem nesse 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 domínios de colisão, 3 domínios de broadcast
B. 24 domínios de colisão, 1 domínio de broadcast
C. 24 domínios de colisão, 3 domínios de broadcast
D. 1 domínio de colisão, 3 domínios de broadcast

---

5. Um técnico está escolhendo o cabo para uma conexão 10GBASE-T entre um servidor e um switch a 75 metros de distância. O ambiente tem EMI moderada causada por lâmpadas fluorescentes. Qual tipo de cabo atende à especificação 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. Um administrador de rede está sumarizando as rotas 172.16.32.0/20, 172.16.48.0/20, 172.16.64.0/20 e 172.16.80.0/20. Qual é a menor rota de sumarização única que inclui as quatro 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. Um switch tem 24 portas, com 8 dispositivos conectados. Quantos domínios de colisão e domínios de broadcast ativos existem? (Considere a configuração padrão, sem VLANs.)

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 domínios de colisão, 1 domínio de broadcast
B. 1 domínio de colisão, 8 domínios de broadcast
C. 24 domínios de colisão, 1 domínio de broadcast
D. 1 domínio de colisão, 1 domínio de broadcast

---

8. Um administrador está revisando a documentação de endereçamento IP de 1995 e encontra uma rede descrita como "Classe B, 172.16.0.0/16". Em redes modernas sem classes (CIDR), por que a designação "Classe B" é enganosa do ponto de vista operacional?

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. As redes Classe B não são mais roteáveis na Internet
B. O CIDR exige que todas as redes Classe B usem máscaras de sub-rede de tamanho variável (VLSM)
C. A máscara /16 pode ser aplicada a qualquer faixa de IP, independentemente dos antigos limites de classe
D. 172.16.0.0/16 é uma faixa de endereços privados e, por isso, é sem classes por definição

---

9. Qual é o equivalente decimal do número binário 11001000?

What is the decimal equivalent of the binary number 11001000?

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

---

10. Qual é a distância máxima de transmissão do Ethernet 1000BASE-T em cabo Cat 5e UTP?

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

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

Conectividade IP

11. Um roteador recebe três rotas para 192.168.0.0: 192.168.0.0/22 via OSPF, 192.168.0.0/24 via EIGRP e 192.168.0.0/16 via rota estática. Chega um pacote destinado a 192.168.0.50. Qual rota é usada?

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. A rota OSPF /22, porque o OSPF tem AD menor que o EIGRP e a rota é mais específica que a estática
B. A rota EIGRP /24, porque tem a correspondência de prefixo mais longa (a mais específica)
C. A rota estática /16, porque as rotas estáticas têm a menor AD e sempre vencem
D. O roteador faz balanceamento de carga entre as três rotas para maximizar o uso dos enlaces

12. Qual estado do HSRP indica que o roteador está encaminhando tráfego em nome do endereço 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. Qual sequência de comandos habilita o processo OSPF 1 nas interfaces da sub-rede 10.1.1.0/24 (e somente nela) e as coloca na área 0, usando um comando network no modo de configuração do roteador?

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, depois ip ospf 1 area 0
B. router ospf 1, depois network 10.1.1.1 255.255.255.0 area 0
C. ip routing ospf 1 area 0
D. router ospf 1, depois network 10.1.1.0 0.0.0.255 area 0

14. Qual é a finalidade de uma rota estática flutuante (floating static route)?

What is the purpose of a floating static route?

A. Balancear a carga do tráfego entre vários caminhos de mesmo custo
B. Redistribuir automaticamente entre protocolos de roteamento
C. Fornecer uma rota de backup que só é usada se a rota principal falhar
D. Fornecer uma rota padrão para a Internet

15. Dois roteadores OSPF no mesmo segmento Ethernet têm estas configurações: R1 (prioridade 100, RID 10.1.1.1) e R2 (prioridade 100, RID 192.168.1.1). Supondo que os dois iniciem ao mesmo tempo, qual roteador se torna o 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. Nenhum, porque prioridades iguais causam um impasse

B. R1, porque tem o Router ID menor

C. R2, porque 192.168.1.1 é um endereço IP privado

D. R2, porque tem o Router ID maior

---

16. Um roteador aprendeu a mesma rede de destino 172.20.0.0/16 por três origens de roteamento: OSPF, EIGRP e uma rota estática. Qual rota o roteador instalará na tabela de roteamento?

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. A rota EIGRP

B. As três rotas, para balanceamento de carga

C. A rota estática

D. A rota OSPF

---

17. Um roteador OSPF na área 10 recebe uma LSA Tipo 3 do ABR anunciando a rede 172.20.0.0/16. Depois, recebe uma LSA Tipo 5 de um ASBR anunciando a mesma rede 172.20.0.0/16. Ambas as LSAs têm métricas válidas. Qual rota é instalada?

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. A rota interárea Tipo 3, porque as rotas intra-área e interárea são preferidas às externas

B. Nenhuma das rotas é instalada; o OSPF não pode ter o mesmo prefixo anunciado como interárea e como externo

C. As duas rotas são instaladas com ECMP (equal-cost multipath), se os custos totais forem iguais

D. A rota externa Tipo 5, porque as LSAs Tipo 5 têm precedência maior que as Tipo 3 no LSDB

---

18. Qual é o tipo de rede OSPF padrão em 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. Um roteador OSPF em uma rede broadcast tem a prioridade da interface definida como 0. O roteador forma com sucesso uma adjacência com o DR. Que estado OSPF esse roteador atinge com o 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 os pacotes hello são trocados, mas a comunicação bidirecional não é confirmada

B. Estado EXSTART, porque a troca de DBD começa, mas não pode terminar sem elegibilidade para DR

C. Estado FULL, porque a prioridade 0 só impede a eleição para DR/BDR, não a formação da adjacência

D. Estado 2-WAY, porque roteadores com prioridade 0 não conseguem formar adjacências FULL em redes broadcast

---

20. Três roteadores OSPF no mesmo segmento Ethernet têm estas configurações: R1 (prioridade 100, RID 1.1.1.1), R2 (prioridade 100, RID 2.2.2.2), R3 (prioridade 100, RID 3.3.3.3). Todos iniciam ao mesmo tempo. Qual afirmação está correta depois que as adjacências se formam?

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 vira DR, R2 vira BDR, R3 é DROTHER
B. O roteador com o maior endereço MAC vira DR
C. R2 vira DR porque tem o Router ID mediano
D. R3 vira DR, R2 vira BDR, R1 é DROTHER

Acesso à rede

21. Qual estado de porta do Rapid PVST+ (IEEE 802.1w) reúne mais diretamente os estados blocking, listening e disabled usados no Spanning Tree Protocol 802.1D antigo?

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. Qual protocolo oferece negociação dinâmica de EtherChannel e é um padrão IEEE?

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

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

23. Um administrador de rede precisa verificar as atribuições de VLAN em um switch Cisco. Qual comando mostra uma tabela concisa, organizada por VLAN, com IDs, nomes, status e portas de acesso atribuídas?

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. Qual é a função de uma Designated Port (porta designada) no Spanning Tree Protocol?

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

A. Receber apenas BPDUs
B. Bloquear o tráfego para evitar loops
C. Conectar-se diretamente à root bridge
D. Encaminhar tráfego em um segmento de rede

25. No Rapid PVST+, um switch tem duas portas conectadas ao mesmo segmento Ethernet compartilhado, e só uma das duas pode se tornar a porta designada desse segmento. Qual função é atribuída à segunda porta, a não designada, no mesmo 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. Edge port
B. Alternate port
C. Backup port
D. Root port

---

26. Em um switch Cisco, um trunk IEEE 802.1Q usa o comportamento padrão de tagging da VLAN nativa (native VLAN). Como ele transmite os quadros de dados comuns pertencentes à 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. Com um rótulo MPLS no lugar de uma tag de VLAN
B. Somente como pacotes IP de camada 3
C. Com duas tags de VLAN 802.1Q
D. Sem tag de VLAN 802.1Q

---

27. Um engenheiro precisa verificar qual switch é a root bridge do STP para a VLAN 20. Qual comando fornece essa informação?

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. Qual modo de ponto de acesso sem fio exige um controlador de LAN sem fio (WLC) para funcionar?

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

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

---

29. Qual recurso do STP deve ser habilitado em portas conectadas a dispositivos de usuário final para minimizar o tempo de convergência?

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. No STP, qual critério tem a maior prioridade na eleição da root bridge?

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

A. Menor endereço MAC
B. Menor prioridade de bridge
C. Maior prioridade de bridge
D. Maior velocidade de porta

Fundamentos de segurança

31. Uma rede sem fio exige autenticação pessoal por senha, e todos os clientes oferecem suporte a WPA3. Qual protocolo de segurança dá a maior proteção contra ataques passivos de adivinhação de senha 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 com SAE
B. WEP com chaves de 128 bits
C. WPA2-Enterprise com AES-CCMP
D. WPA2-Personal com TKIP

---

32. Uma rede usa a ACL estendida 110 aplicada na entrada (inbound) de uma interface de roteador. A primeira ACE é 'access-list 110 deny tcp any any eq 23'. Que tráfego essa ACE vai bloquear?

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. Tráfego SSH de qualquer origem para qualquer destino
B. Todo o tráfego TCP de qualquer origem para qualquer destino
C. Tráfego Telnet de qualquer origem para qualquer destino
D. Tráfego Telnet destinado apenas à interface do roteador

---

33. Uma empresa precisa conectar dois sites pela internet com uma VPN. A conexão deve dar suporte a tráfego multicast e a vários protocolos (IPv4, IPv6, IPX). Qual tecnologia de VPN é a MAIS adequada?

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. Somente IPsec em modo túnel

---

34. O que significa AAA em segurança de redes?

What does AAA stand for in network security?

A. Access, Authentication, and Administration (acesso, autenticação e administração)
B. Authentication, Accounting, and Auditing (autenticação, contabilização e auditoria)
C. Authentication, Authorization, and Accounting (autenticação, autorização e contabilização)
D. Authorization, Access, and Auditing (autorização, acesso e auditoria)

---

35. Um administrador precisa bloquear o tráfego IP da rede 192.168.10.0/24 para um servidor em 10.1.1.100. Em qual interface de roteador uma ACL padrão (standard ACL) deve ser colocada para minimizar o impacto no tráfego para outros 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. Na porta do switch onde o servidor está conectado
B. Na interface de roteador mais próxima da origem (192.168.10.0/24)
C. Em todas as interfaces de roteadores intermediários
D. Na interface de roteador mais próxima do destino (10.1.1.100)

---

36. Um técnico examina a configuração em execução de um roteador e vê 'enable secret 5 1mERr$hx5rVt7rPNoS4wqbXKX7m0'. Que tipo de proteção é usado nessa senha 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. Cifra de Vigenère simples (tipo 7)

---

37. Uma empresa exige autenticação centralizada, com contabilização completa de comandos e autorização por comando para todos os administradores de rede que acessam roteadores e switches Cisco. Qual protocolo AAA é o MAIS adequado para esse 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. Autenticação local

---

38. Uma ACL estendida tem apenas a instrução 'access-list 101 permit tcp any any established'. Chega um pacote TCP com somente a flag SYN, de 203.0.113.50 para 198.51.100.10 porta 443, na interface onde a ACL 101 está aplicada na entrada (inbound). O que acontece com esse pacote?

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. O pacote é permitido, porque faz parte do estabelecimento de uma conexão TCP
B. O pacote é negado, porque a flag SYN sozinha não casa com a palavra-chave 'established'
C. O pacote é permitido somente se existir uma entrada correspondente na tabela de estados TCP
D. O pacote é negado, porque ACLs estendidas não podem permitir a porta TCP 443

---

39. Uma empresa exige autenticação centralizada, com contabilização completa de comandos e a capacidade de criptografar todo o conteúdo da autenticação. Qual protocolo AAA atende MELHOR a esses 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. Autenticação por banco de dados local
D. TACACS+

---

40. Uma ACL estendida precisa permitir tráfego somente do host 192.168.5.45. Qual é a máscara curinga (wildcard mask) correta?

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

Automação e programabilidade

41. Um arquiteto de rede está projetando uma solução de rede definida por software (SDN). Qual plano é responsável por executar as ações de encaminhamento de pacotes com base em regras programadas pelo 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 gerenciamento (management plane)
B. Plano de aplicação (application plane)
C. Plano de dados (data plane)
D. Plano de controle (control plane)

---

42. Uma API REST retorna a seguinte resposta JSON para uma consulta de interface: {"status": "up", "speed": "1000", "duplex": "full"}. Um script Python tenta fazer um cálculo matemático com o valor de speed e gera um TypeError. Qual é o 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. Falta o campo obrigatório "unit" no JSON
B. A API retornou uma sintaxe JSON inválida
C. O valor de speed é uma string, não um inteiro
D. A biblioteca JSON do Python não aceita objetos aninhados

---

43. Uma empresa migra de uma rede de campus tradicional em três camadas para uma malha (fabric) Cisco SD-Access. Qual é a mudança arquitetural PRINCIPAL?

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

A. Os requisitos de cabeamento físico caem 50% porque o acesso passa a ser só sem fio
B. A rede usa overlays VXLAN para segmentação, em vez de VLANs tradicionais
C. Os protocolos de roteamento são desativados e todas as decisões de encaminhamento são tomadas pelos switches
D. Todo o tráfego é roteado pela internet para aplicar as políticas

---

44. Qual é a finalidade de um modelo de dados YANG na programabilidade de redes?

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

A. O YANG compacta arquivos de configuração grandes para transferi-los mais rápido
B. O YANG define a estrutura e as restrições dos dados de configuração e operacionais
C. O YANG criptografa os dados de configuração durante a transmissão pela API
D. O YANG substitui os comandos CLI por fluxos de trabalho gráficos

---

45. Um engenheiro recebe o código de status 409 Conflict ao tentar criar uma nova VLAN por uma API REST em um switch Cisco. O ID da VLAN é válido e está dentro da faixa permitida. Qual é a causa MAIS provável?

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. O switch está processando outra alteração de configuração
B. O corpo da requisição (payload) contém sintaxe JSON inválida
C. Já existe uma VLAN com esse ID no switch
D. As credenciais da API não têm privilégios suficientes

---

46. Qual erro de sintaxe JSON impediria que este trecho de configuração fosse interpretado corretamente?

{"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. O valor de hostname deveria usar aspas simples em vez de aspas duplas

B. O valor de vlan deveria estar entre aspas, como string

C. Este JSON está sintaticamente correto

D. O array deveria usar parênteses em vez de colchetes

---

47. Um engenheiro escreve um script Python com a biblioteca ncclient para enviar configurações por NETCONF. O script conecta com sucesso, mas a operação edit-config falha com o erro "missing-element". O payload XML está bem formado. Qual é a causa MAIS provável?

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. O modelo YANG exige um elemento obrigatório que não foi incluído no payload

B. A declaração de namespace no XML está incorreta

C. O dispositivo não oferece suporte à capability writable-running

D. O datastore de destino está bloqueado por outra sessão

---

48. Uma API exige autenticação antes de permitir alterações de configuração. Qual método de autenticação oferece acesso baseado em token que expira após um período definido, reduzindo o risco de exposição de credenciais?

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. Community strings do SNMP

B. OAuth 2.0 com bearer tokens

C. Autenticação Basic com codificação Base64

D. Autenticação SSH por chave pública

---

49. Uma chamada de API REST a um dispositivo Cisco retorna o seguinte JSON:

{"status": "success", "vlan_id": 100, "vlan_name": "Engineering", "active": true}

Qual é o tipo de dado da chave "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. Boolean

B. Object

C. String

D. Integer

---

50. Um script de automação de rede envia uma requisição de API REST para excluir uma VLAN, e o servidor responde com o código de status HTTP 204. O que isso indica?

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. A VLAN não foi encontrada no dispositivo

B. O servidor encontrou um erro interno

C. A requisição foi rejeitada por falha de autenticação

D. A requisição teve sucesso e nenhum conteúdo é retornado

Resposta correta

1. A Com VLSM, as sub-redes não podem se sobrepor, mas não precisam ser contíguas. A /26 ocupa de .0 a .63 e a /27 ocupa de .64 a .95, então o primeiro endereço livre é .96. Uma /30 tem 4 endereços e exatamente 2 utilizáveis. A 192.168.20.96/30 cobre de .96 a .99 e é o menor endereço disponível. A .92/30 se sobrepõe à /27, a .96/29 dá 6 hosts e a .128/30 não é a menor.

2. D A janela efetiva do TCP é o menor valor entre a janela de congestionamento (32 KB) e a janela anunciada pelo receptor (24 KB), ou seja, 24 KB. Como já há 10 KB sem confirmação, o emissor pode enviar mais 24 - 10 = 14 KB. 22 KB subtrai da janela de congestionamento (32 - 10). 24 KB ignora os dados em trânsito. 32 KB ignora o limite do receptor.

3. D 00-1A-2B está correto porque o OUI são os primeiros 24 bits (3 primeiros octetos) de um endereço MAC de 48 bits, atribuídos pelo IEEE para identificar o fabricante. Os 3 octetos restantes (3C-4D-5E) são definidos pelo fabricante e identificam a interface. 00-1A tem só 16 bits. 2B-3C-4D-5E mistura o OUI com a parte do dispositivo.

4. C Cada porta do switch forma um domínio de colisão (collision domain) separado, então são 24. Cada VLAN forma um domínio de broadcast (broadcast domain) separado, então 3 VLANs dão 3 domínios de broadcast. "24 domínios de colisão, 1 domínio de broadcast" ignora as VLANs. "3 e 3" supõe que as VLANs definem os domínios de colisão. "1 e 3" confunde o switch com um hub.

5. C O Cat 6A UTP atende ao padrão de cabeamento 10GBASE-T para distâncias de até 100 metros. O Cat 6 é geralmente especificado para 10GBASE-T até 55 metros, conforme a instalação, menos que os 75 exigidos. O Cat 5e não é especificado para 10GBASE-T nessa distância. A blindagem do Cat 6 STP melhora a proteção contra EMI, mas não garante o desempenho exigido a 75 metros. Bem instalado, o Cat 6A UTP serve para esse ambiente.

6. B 172.16.0.0/17 é a menor sumarização única que cobre as quatro redes. O intervalo vai de 172.16.32.0 a 172.16.95.255. Os valores 32 e 95 no terceiro octeto só compartilham o primeiro bit, o que dá um prefixo comum de 17 bits. Essa rota cobre também endereços extras, de 172.16.0.0 a 172.16.127.255. A /19 cobre só duas redes, a 172.16.32.0/18 não é um limite válido e a /16 inclui endereços demais.

7. A "8 domínios de colisão, 1 domínio de broadcast" está correto. O switch cria um domínio de colisão para cada porta ativa (8 dispositivos, 8 domínios), e o full-duplex evita colisões. Todas as portas na mesma VLAN dividem um único domínio de broadcast, e um broadcast chega a todas as outras portas. "1 e 8" inverte os conceitos. "24 e 1" conta também as portas inativas. "1 e 1" descreve um hub.

8. C O CIDR (Classless Inter-Domain Routing) acabou com a estrutura rígida de classes A/B/C. Com o CIDR, uma máscara /16 pode ser aplicada a qualquer rede, seja qual for o primeiro octeto. O rótulo "Classe B" é só histórico: os roteadores olham apenas o comprimento do prefixo (/16). A ideia de que não são roteáveis é falsa, pois muitos IPs públicos ainda estão em faixas da antiga Classe B. Ser endereço privado (RFC 1918) não depende do CIDR, e o VLSM é uma técnica, não uma exigência.

9. C Convertendo 11001000 de binário para decimal: (1×128) + (1×64) + (0×32) + (0×16) + (1×8) + (0×4) + (0×2) + (0×1) = 128 + 64 + 8 = 200. 192 seria 11000000, 208 seria 11010000 e 224 seria 11100000. Saber converter rápido os valores comuns de octeto (128, 192, 224, 240, 248, 252, 254, 255) ajuda muito nos cálculos de sub-redes.

10. D O comprimento máximo do cabo para 1000BASE-T (Gigabit Ethernet) em Cat 5e ou Cat 6 UTP é de 100 metros, conforme o padrão IEEE 802.3ab. Isso inclui até 90 metros de cabeamento horizontal mais 10 metros de patch cords. 185 metros era o limite do 10BASE2 e 500 metros era o limite do 10BASE5, ambos em cabo coaxial. 2 quilômetros não é o alcance padrão do 1000BASE-LX em fibra monomodo, que chega a 5 quilômetros.

11. B A correspondência de prefixo mais longa (longest prefix match) SEMPRE vem antes da distância administrativa (AD) na decisão de roteamento. O IP 192.168.0.50 está nos três prefixos, mas a /24 é a mais específica, então a rota EIGRP é usada, mesmo com AD 90 contra AD 1 da estática. A AD só é comparada quando os prefixos têm o MESMO tamanho. A /16 é a menos específica e perde. Não há balanceamento entre prefixos diferentes.

12. D O estado Active indica que o roteador HSRP está encaminhando pacotes para o IP virtual e respondendo às requisições ARP desse IP. Só um roteador por grupo HSRP pode estar Active. Standby é o estado de reserva: o roteador monitora o Active e assume se ele falhar. Em Listen, o roteador recebe os anúncios HSRP, mas não é Active nem Standby. Speak é um estado de transição na eleição, em que os roteadores trocam prioridades.

13. D A sequência correta é 'router ospf 1, depois network 10.1.1.0 0.0.0.255 area 0'. O método tradicional usa o comando `network` no processo OSPF com uma máscara curinga (wildcard mask). Ele casa com as interfaces da faixa 10.1.1.0/24 e as coloca na área 0. A opção com `ip ospf 1 area 0` é válida na interface, mas não usa o modo do roteador. A opção com 255.255.255.0 usa uma máscara normal como se fosse curinga. 'ip routing ospf 1 area 0' tem sintaxe inválida.

14. C Uma rota estática flutuante tem distância administrativa (AD) maior que a da rota principal (por exemplo, AD 5 em vez do padrão 1). Por isso, ela só entra na tabela de roteamento quando a rota principal não está disponível. Também serve para preferir um protocolo dinâmico (como OSPF, AD 110) no uso normal. Ela não faz balanceamento de carga nem redistribuição. Pode apontar para a Internet, mas o que a define é a AD elevada, que cria o comportamento de backup.

15. D Quando as prioridades OSPF são iguais (as duas são 100), o desempate é o maior Router ID (RID). O OSPF compara os RIDs numericamente: 192.168.1.1 é maior que 10.1.1.1, então o R2 vira DR. Ser um endereço privado não importa. Prioridades iguais não causam impasse, o OSPF só passa ao próximo critério. Na eleição do DR vencem a maior prioridade e depois o maior RID, ao contrário da AD, em que o menor vence.

16. C Os roteadores Cisco usam a distância administrativa (AD) para escolher entre rotas de origens diferentes. A rota estática tem AD 1 (a mais confiável), o EIGRP tem AD 90 e o OSPF tem AD 110. O roteador escolhe a rota com a menor AD, então a estática vence. O balanceamento de carga só ocorre com rotas de mesma AD e mesma métrica, o que não é o caso. A AD é avaliada antes da métrica.

17. A A ordem de preferência do OSPF é: intra-área (Tipo 1/2), interárea (Tipo 3), externa E1 (Tipo 5) e externa E2 (Tipo 5). Mesmo com o mesmo prefixo, a rota interárea Tipo 3 vence por estar mais acima nessa ordem. As LSAs Tipo 5 NÃO têm precedência maior, pois as rotas externas são sempre as menos preferidas. O ECMP só vale para rotas do MESMO tipo e de mesmo custo. O OSPF aceita anúncios sobrepostos e aplica essas regras.

18. C Broadcast é o tipo de rede OSPF padrão em Ethernet e em outras mídias de acesso múltiplo. Nesse modo, o OSPF elege um DR (Designated Router) e um BDR (Backup Designated Router) para reduzir as adjacências e o flooding de LSAs. Point-to-point é o padrão em enlaces seriais e não elege DR/BDR. Non-broadcast é usado em redes NBMA, como Frame Relay, e exige vizinhos configurados manualmente. Point-to-multipoint também é para NBMA, mas trata cada enlace como ponto a ponto, sem DR/BDR.

19. C Um roteador com prioridade OSPF 0 chega ao estado FULL com o DR e com o BDR. Prioridade 0 só significa que ele não pode ser DR nem BDR e não participa da eleição. Em redes broadcast, TODOS os roteadores formam adjacência FULL com o DR e o BDR e trocam o LSDB completo. Com os outros DROTHERs, ficam apenas em 2-WAY. EXSTART e INIT são estados de transição antes do FULL.

20. D Com prioridades iguais (100), o desempate é o Router ID. O OSPF elege o MAIOR Router ID como DR e o segundo maior como BDR. Assim, R3 (3.3.3.3) é DR, R2 (2.2.2.2) é BDR e R1 (1.1.1.1) é DROTHER. A opção com R1 como DR inverte a lógica, pois o menor RID não vence. Não existe regra do RID mediano. O endereço MAC não importa na eleição do DR.

21. C O Rapid PVST+ simplifica os cinco estados de porta do 802.1D em três: discarding, learning e forwarding. O estado discarding assume as funções dos antigos blocking, listening e disabled, pois nos três casos a porta não encaminha quadros nem aprende endereços MAC. Learning corresponde ao antigo learning e não muda. Forwarding também corresponde ao antigo forwarding. Blocking não é usado como estado separado no RSTP, pois foi incorporado ao discarding.

22. D O LACP (Link Aggregation Control Protocol), definido no IEEE 802.3ad, é o protocolo padrão do mercado para negociar EtherChannels dinamicamente. Ele é neutro quanto ao fabricante e funciona entre switches de marcas diferentes. O PAgP (Port Aggregation Protocol) é proprietário da Cisco e só funciona entre equipamentos Cisco. O VTP (VLAN Trunking Protocol) sincroniza o banco de dados de VLANs, não agrega enlaces. O CDP (Cisco Discovery Protocol) descobre vizinhos, não forma EtherChannel.

23. A 'show vlan brief' lista IDs de VLAN, nomes, status e portas de acesso atribuídas em uma tabela concisa, organizada por VLAN. 'show interfaces status' mostra velocidade, duplex e VLAN por porta, mas não traz nomes nem status das VLANs. 'show running-config' mostra toda a configuração e exige procurar as VLANs no texto. 'show ip interface brief' mostra informações de IP em interfaces roteadas e SVIs, não a associação às VLANs na camada 2.

24. D No STP, uma Designated Port encaminha o tráfego do seu segmento de rede (domínio de colisão) em direção à root bridge. Cada segmento tem uma porta designada, a que tem o caminho de menor custo até a root bridge. A Root Port é a porta de um switch não raiz que aponta para a root bridge. As portas que bloqueiam tráfego estão no estado Blocking (ou Alternate/Backup no RSTP). Todas as portas recebem BPDUs, mas as designadas também encaminham tráfego, no estado Forwarding.

25. C O RSTP define a função backup port para o caso em que um único switch tem duas ou mais portas no mesmo segmento compartilhado (em geral por um hub) e só uma pode ser designada. A porta que perde vira backup port e dá redundância à porta designada no mesmo switch. A alternate port é diferente: ela dá um caminho de reserva até a root bridge por outro switch ou segmento. A root port é o melhor caminho até a raiz. A edge port é um enlace no estilo PortFast para um host final.

26. D "Sem tag de VLAN 802.1Q" está correto, porque os quadros de dados da VLAN nativa são enviados sem tag por padrão. "Com duas tags de VLAN 802.1Q" não descreve o comportamento padrão da VLAN nativa. "Com um rótulo MPLS no lugar de uma tag de VLAN" não tem relação com o encaminhamento comum em trunks 802.1Q. "Somente como pacotes IP de camada 3" está errado, pois o trunk encaminha quadros Ethernet.

27. C 'show spanning-tree vlan 20' mostra a topologia STP da VLAN 20, incluindo o ID da root bridge, a prioridade do switch local e as funções e estados das portas. Ele indica se o switch local é a raiz ou mostra o ID da raiz. 'show vlan brief' lista as VLANs, mas não as funções do STP. 'show interfaces trunk' mostra o status dos trunks e as VLANs permitidas. 'show spanning-tree summary' mostra um resumo, sem identificar a raiz da VLAN 20.

28. A Os pontos de acesso lightweight (LAPs) dependem de um controlador de LAN sem fio (WLC) para configuração e gerenciamento. Eles usam o protocolo CAPWAP (Control and Provisioning of Wireless Access Points) para falar com o controlador. Os APs autônomos (autonomous) são independentes e não precisam de controlador. Mesh é uma topologia, e os APs mesh podem ser lightweight ou autônomos. O modo bridge liga duas redes cabeadas sem fio e não exige controlador.

29. A O PortFast leva uma porta de acesso direto ao estado Forwarding quando o enlace sobe, sem os 30 segundos de atraso dos estados Listening e Learning. É seguro para dispositivos finais (PCs, impressoras), que não criam loops. UplinkFast e BackboneFast são recursos antigos para falhas de uplink e de enlaces indiretos, não para portas de usuário. O BPDU Guard é de segurança: desativa uma porta PortFast que recebe um BPDU, mas não reduz a convergência e é usado junto com o PortFast.

30. B A eleição da root bridge no STP se baseia no menor bridge ID, que combina a prioridade de bridge (bridge priority) e o endereço MAC. A prioridade é avaliada primeiro, e o switch com o menor valor vira a root bridge. Se houver empate, o menor endereço MAC desempata. "Maior prioridade de bridge" está errado, pois valores menores vencem. A velocidade da porta não entra na eleição, embora afete o cálculo do custo das portas.

31. A "WPA3-Personal com SAE" usa o SAE (Simultaneous Authentication of Equals) no lugar do PSK do WPA2-Personal. Isso dá sigilo futuro (forward secrecy) e protege contra ataques passivos de dicionário offline. O enunciado diz que os clientes aceitam WPA3. O WPA2-Enterprise usa autenticação corporativa, não a pessoal pedida. O WPA2-Personal com TKIP é mais fraco, e o TKIP foi descontinuado em 2012. O WEP está quebrado e pode ser invadido em minutos, qualquer que seja o tamanho da chave.

32. C A porta 23 é a porta conhecida do Telnet, então 'eq 23' casa com sessões Telnet. A ACE usa origem 'any' e destino 'any', ou seja, casa com Telnet de qualquer origem para qualquer destino. O SSH usa a porta 22 e não é afetado. A ACE só trata TCP na porta 23, então HTTP (80) e HTTPS (443) não casam. Uma ACL de entrada na interface filtra tráfego em trânsito e tráfego para o próprio roteador.

33. C GRE (Generic Routing Encapsulation) sobre IPsec (GRE over IPsec) une a capacidade do GRE de transportar multicast e vários protocolos com a criptografia e a autenticação do IPsec. O GRE aceita protocolos de roteamento (OSPF, EIGRP), multicast e IPv6. O IPsec em modo túnel sozinho só aceita IP unicast. A SSL VPN é para acesso remoto de clientes, não site a site. O PPTP é obsoleto e inseguro. GRE com IPsec é a solução Cisco padrão para VPN site a site com roteamento dinâmico ou multicast.

34. C AAA significa Authentication (autenticação: verificar a identidade do usuário), Authorization (autorização: dar permissões conforme a identidade) e Accounting (contabilização: registrar atividades e uso de recursos). É a base da segurança de rede Cisco e é implementado com protocolos como TACACS+ e RADIUS. As outras opções trocam termos: confundem autenticação com controle de acesso, trocam accounting por auditing ou omitem a autorização.

35. D As ACLs padrão filtram apenas pelo endereço IP de origem, não por destino, porta ou protocolo. A boa prática é colocá-las o mais perto possível do destino, para não bloquear o tráfego legítimo da mesma origem para outros lugares. Perto da origem, ela bloquearia também esse tráfego. Em todas as interfaces, gasta recursos à toa. Alguns switches aceitam ACL na porta, mas a pergunta pede uma interface de roteador. Regra: ACL padrão perto do destino, ACL estendida perto da origem.

36. B O '5' indica um hash MD5. O 'enable secret' sempre usa hash (não reversível), o que é mais seguro que o 'enable password'. O tipo 7 é uma cifra de Vigenère fraca usada pelo 'service password-encryption' e é fácil de reverter. O tipo 8 é PBKDF2-SHA256 e o tipo 9 é scrypt, ambos mais fortes. O número depois de 'enable secret' indica o algoritmo, e a cadeia longa é a senha em hash. O MD5 é obsoleto para novas instalações, mas ainda comum em configurações antigas.

37. A TACACS+ está correto porque separa autenticação, autorização e contabilização (accounting) em processos distintos e criptografa todo o conteúdo do pacote, não só a senha. Ele permite autorização por comando. O RADIUS junta autenticação e autorização e usa principalmente UDP, sendo mais indicado para controle de acesso à rede. A autenticação local não é centralizada. O Kerberos é baseado em tickets e não oferece autorização por comando com accounting.

38. B A palavra-chave 'established' casa com pacotes TCP que têm a flag ACK ou RST. Ela NÃO casa com um pacote só com SYN, que é o primeiro da conexão TCP. Como há um deny implícito no fim da ACL, o pacote SYN é descartado. Assim, a ACL deixa passar o tráfego de retorno, mas bloqueia novas conexões de entrada. As ACLs do Cisco IOS não guardam estado: não existe tabela de estados TCP, e a checagem é feita por pacote, só pelas flags.

39. D O TACACS+ criptografa todo o conteúdo do pacote, não só a senha, e separa autenticação, autorização e contabilização, o que permite contabilizar comandos em detalhe. O RADIUS criptografa só o campo da senha e junta autenticação e autorização, sendo menos indicado para contabilizar comandos. O banco de dados local não é centralizado, pois cada dispositivo tem seus usuários. O Kerberos é de login único e pouco comum para AAA em dispositivos Cisco no nível CCNA. O TACACS+ usa a porta TCP 49 e o RADIUS usa UDP 1812 e 1813.

40. A A máscara curinga 0.0.0.0 indica correspondência exata com um único host: todos os bits devem casar (0 = deve casar, 1 = não importa). Equivale a 'host 192.168.5.45' na sintaxe da ACL. 255.255.255.255 significa 'any' e casa com qualquer endereço. 0.0.0.255 casa os três primeiros octetos e aceita qualquer valor no quarto (uma /24). 255.255.255.0 é o inverso do necessário. Lembre: a máscara curinga é o inverso da máscara de sub-rede.

41. C O plano de dados (data plane) executa as ações de encaminhamento com base nas tabelas de fluxo e nas políticas instaladas pelo controlador SDN. Nas redes tradicionais, o plano de controle toma as decisões de roteamento, mas no SDN essa lógica fica centralizada no controlador. O plano de gerenciamento cuida da configuração e do monitoramento. O plano de aplicação reúne aplicações que falam com o controlador pelas APIs northbound, mas o encaminhamento ocorre no plano de dados.

42. C "O valor de speed é uma string, não um inteiro" está correto, pois "1000" está entre aspas e, portanto, é uma string em JSON. O json.loads() do Python mantém esse tipo, então uma conta como speed + 2 gera TypeError. A correção é int(data['speed']). A falta de "unit" não causa TypeError. A sintaxe JSON é válida. A biblioteca json do Python aceita objetos aninhados. As APIs REST muitas vezes devolvem números como string, então valide e converta o tipo antes de calcular.

43. B O SD-Access usa túneis overlay VXLAN (Virtual Extensible LAN) para criar segmentos lógicos (Virtual Networks, ou VNs) sobre um underlay IP físico. Isso substitui a segmentação por VLANs e permite microssegmentação escalável, guiada por políticas. O underlay ainda usa protocolos de roteamento (em geral IS-IS ou OSPF) para dar alcance IP entre os nós da malha. O tráfego fica na malha, sem passar pela internet. Há dispositivos com e sem fio, e o cabeamento continua necessário.

44. B O YANG (Yet Another Next Generation) é uma linguagem de modelagem de dados que define o esquema dos dados de configuração e de estado operacional: quais dados existem, seus tipos, faixas válidas, campos obrigatórios ou opcionais e relações. Protocolos como NETCONF e RESTCONF usam modelos YANG para trocar dados de forma consistente e validada. O YANG não criptografa: isso é feito pelo transporte (SSH no NETCONF, HTTPS no RESTCONF). Também não é uma interface gráfica e não compacta dados.

45. C O HTTP 409 Conflict indica um conflito com o estado do recurso. Aqui, a tentativa de criar uma VLAN que já existe, que é o uso clássico do 409. A falta de privilégios retornaria 401 Unauthorized ou 403 Forbidden. Um JSON inválido geraria 400 Bad Request. Alterações simultâneas de configuração podem gerar conflitos em alguns sistemas, mas o 409 nas convenções REST aponta para criação duplicada de recurso. Não confunda o 409 com o 423 Locked.

46. C Este JSON é sintaticamente válido. O JSON exige aspas duplas (não simples) em chaves e strings, então o hostname está correto. O valor de vlan é numérico (10), sem aspas: o JSON diferencia strings (com aspas) de números (sem aspas). Os arrays usam colchetes [ ], não parênteses. O booleano 'true' está em minúsculas e sem aspas. Erros comuns de JSON são aspas simples, vírgulas faltando, vírgulas sobrando e colchetes que não fecham, e nenhum aparece aqui.

47. A "missing-element" indica uma violação de restrição do modelo YANG: um leaf ou container obrigatório definido no modelo não está no payload XML. É uma falha de validação do esquema. Sem a capability writable-running, o erro seria "operation-not-supported". Um namespace errado geraria "unknown-namespace" ou erros de interpretação. Um datastore bloqueado retorna "in-use" ou "resource-denied". Cada código de erro do NETCONF aponta para um tipo de falha.

48. B O OAuth 2.0 usa bearer tokens com prazo de validade, emitidos após a autenticação inicial, o que limita o risco se um token vazar. Os aplicativos enviam o token, não as credenciais, em cada requisição. A autenticação Basic envia usuário e senha em toda requisição, e o Base64 não é criptografia. A chave pública SSH é forte para acesso por CLI, mas normalmente não é usada em APIs REST e não expira sozinha. As community strings do SNMP são segredos em texto puro, sem expiração nem token.

49. A Boolean está correto, pois true (em minúsculas e sem aspas) é um literal booleano do JSON, que representa verdadeiro ou falso. No JSON, os valores booleanos são escritos como true ou false, sem aspas. As strings ficam entre aspas, como "Engineering". Os inteiros são números sem aspas, como 100. Os objetos são estruturas aninhadas entre chaves. Entender os tipos de dados do JSON é essencial para ler as respostas de APIs em scripts de automação.

50. D O HTTP 204 No Content está correto: indica que a requisição foi processada com sucesso e que não há corpo na resposta. É típico de operações DELETE, em que basta confirmar a exclusão. Se a VLAN não existisse, o servidor retornaria 404 Not Found. Falhas de autenticação retornam 401 Unauthorized ou 403 Forbidden. Erros internos retornam 500 Internal Server Error. Os códigos 2xx indicam sucesso, os 4xx indicam erro do cliente e os 5xx indicam erro do servidor.

Palavras-chave em inglês

subnet	sub-rede	Parte menor de uma rede IP, com seu próprio prefixo.
subnet mask	máscara de sub-rede	Indica quais bits do endereço são da rede e quais do host.
wildcard mask	máscara curinga	Inverso da máscara: 0 exige bit igual, 1 aceita qualquer valor.
prefix length	tamanho do prefixo	Número de bits da rede, como /24.
usable host address	endereço de host utilizável	Endereço da sub-rede que pode ser dado a um dispositivo.
VLSM (variable-length subnet mask)	máscara de sub-rede de tamanho variável	Dividir uma rede em sub-redes de tamanhos diferentes.
summary route	rota sumarizada	Uma só rota que cobre várias redes.
longest prefix match	correspondência de prefixo mais longa	Regra que escolhe a rota mais específica para o destino.
administrative distance (AD)	distância administrativa	Confiança na fonte da rota; o menor valor vence.
routing table	tabela de roteamento	Lista de rotas que o roteador usa para encaminhar pacotes.
static route	rota estática	Rota configurada à mão pelo administrador.
floating static route	rota estática flutuante	Rota reserva que só entra se a principal falhar.
equal-cost load balancing	balanceamento de carga entre rotas de mesmo custo	Dividir o tráfego entre caminhos com o mesmo custo.
adjacency	adjacência	Relação entre roteadores OSPF que trocam informações de roteamento.
designated router (DR)	roteador designado	Roteador OSPF eleito no segmento para reduzir adjacências.
tiebreaker	critério de desempate	O que decide quando dois valores são iguais.
collision domain	domínio de colisão	Área onde quadros podem colidir; cada porta de switch separa uma.
broadcast domain	domínio de broadcast	Área que recebe o mesmo broadcast; cada VLAN forma uma.
congestion window	janela de congestionamento	Limite que o emissor TCP calcula conforme a rede.
unacknowledged data	dados sem confirmação	Dados enviados que o receptor ainda não confirmou.
shielded (STP) / unshielded (UTP)	blindado / sem blindagem	Tipos de cabo de par trançado, com ou sem proteção contra interferência.
access port	porta de acesso	Porta do switch que pertence a uma VLAN.

trunk	trunk (tronco)	Enlace que transporta várias VLANs entre equipamentos.
native VLAN	VLAN nativa	VLAN cujos quadros passam sem tag no trunk 802.1Q.
untagged frame	quadro sem tag	Quadro Ethernet sem a marca de VLAN 802.1Q.
root bridge	root bridge (bridge raiz)	Switch eleito como referência da árvore no Spanning Tree.
bridge priority	prioridade da bridge	Valor usado para eleger a raiz; o menor vence.
designated port	porta designada	Porta que encaminha o tráfego de um segmento no STP.
discarding	estado de descarte	Estado em que a porta não encaminha quadros nem aprende MAC.
link aggregation	agregação de enlaces	Juntar vários enlaces em um só, como no EtherChannel.
lightweight access point	ponto de acesso leve	Ponto de acesso que depende de um controlador WLC.
standard ACL	ACL padrão	Lista de acesso que filtra só pelo IP de origem.
extended ACL	ACL estendida	Lista que filtra por origem, destino, protocolo e porta.
inbound	de entrada	Tráfego que chega pela interface.
implicit deny	negação implícita	Regra não escrita no fim da ACL que bloqueia o resto.
accounting	contabilização	Parte do AAA que registra o que o usuário fez.
hash	hash	Resultado de um cálculo de mão única, usado para guardar senhas.
data plane	plano de dados	Parte da rede que encaminha os pacotes.
payload	carga útil (conteúdo)	Os dados dentro de um pacote ou de uma requisição.
status code	código de status	Número HTTP que diz se a requisição deu certo.

O Examundo é independente. Não é afiliado às entidades que fazem essas provas nem tem a aprovação delas. As questões são originais, não são da prova real. examundo.tech/pt/ccna/