

Guia de preparação CCNA

Tudo o que a prova cobra, organizado por domínio: conceitos-chave, comparações que confundem, pegadinhas reais, gatilhos do enunciado, questões comentadas e um plano para chegar pronto ao exame.

5 capítulos por domínio	**32** questões comentadas	**82%** nota de corte
6 provas completas no curso		

ANTES DE COMEÇAR

Como usar este guia

Este guia foi feito para ser estudado junto com as 6 provas completas do curso CCNA: o guia explica o que cai e onde estão as armadilhas; as provas treinam o ritmo e mostram o que você ainda não domina.

Quando	O que fazer
Semana 1	Faça o teste diagnóstico (página seguinte) e leia os capítulos 1 e 2. No fim da semana, faça a Prova 1 do curso no tempo do exame.
Semana 2	Leia os demais capítulos, começando pelos domínios em que você errou mais no diagnóstico. Faça as provas 2 e 3.
Semana 3	Releia os alertas de pegadinha e as tabelas de comparação. Faça as provas 4 e 5 e revise cada erro pela explicação.
Semana 4	Estude a folha de cola, faça a Prova 6 e refaça as provas abaixo de 80%. Agende o exame quando estiver acima de 80% em todas (a nota de corte é 82%).

Mapa do exame

Cada prova do curso tem 60 questões e 120 minutos, no formato do exame. Referência de aprovação: 82%.

Domínio (capítulo)	Peso	Neste guia
1. 1.0 Infraestrutura e Conectividade de Rede	25%	18 conceitos · 14 pegadinhas
2. 2.0 Switching e Acesso à Rede	25%	18 conceitos · 14 pegadinhas
3. 3.0 Roteamento IP	20%	18 conceitos · 14 pegadinhas
4. 4.0 Serviços de Rede e Segurança	20%	18 conceitos · 14 pegadinhas
5. 5.0 IA e Operações e Gerenciamento de Rede	10%	18 conceitos · 14 pegadinhas

Como ler os capítulos: os **tópicos-chave** são o que mais cai; a **tabela de memorização** separa o que a prova costuma confundir; os **alertas de prova** mostram as armadilhas das alternativas erradas; os **gatilhos** ligam palavras do enunciado à resposta; e o **checklist** diz se você está pronto para o domínio.

Estude um pouco todo dia, de graça

Instagram @strecht.simulados

Um post de prova por dia: questão comentada, pegadinhas e o "não confunda" de cada certificação.

Seguir no Instagram →

YouTube Strecht Simulados

Shorts diários com pegadinhas de prova e, aos sábados, um simulado comentado.

Inscrever-se no canal →

DIAGNÓSTICO

Você já sabe isso?

Responda às 12 questões sem consultar nada. As respostas, com a explicação e o capítulo para revisar, estão no fim do guia. Comece o estudo pelos capítulos em que errou.

D1 · 1.0 Infraestrutura e Conectividade de Rede

Um provedor entregou à empresa o prefixo IPv6 2001:DB8:AB00::/56, e cada VLAN receberá um /64. Quantas sub-redes /64 o prefixo permite criar?

A. 65.536 sub-redes
B. 256 sub-redes
C. 64 sub-redes
D. 16 sub-redes

D2 · 1.0 Infraestrutura e Conectividade de Rede

Um projetista precisa endereçar uma VLAN que terá 50 estações, usando a menor sub-rede possível para economizar endereços. Qual prefixo atende ao requisito?

A. /26, com 62 hosts
B. /27, com 30 hosts
C. /28, com 14 hosts
D. /25, com 126 hosts

D3 · 1.0 Infraestrutura e Conectividade de Rede

Um computador acessa só colegas da mesma sub-rede. Saída de ipconfig /all: IPv4 Address 10.5.5.20; Subnet Mask 255.255.255.0; Default Gateway 10.5.5.255; DHCP Enabled: No. O roteador da rede usa 10.5.5.1. Qual é o erro?

A. O DHCP desativado impede o acesso a outras redes
B. O gateway foi configurado com o broadcast da sub-rede
C. O endereço 10.5.5.20 está fora da sub-rede 10.5.5.0/24
D. A máscara deveria ser 255.255.0.0 para alcançar outras redes

D4 · 2.0 Switching e Acesso à Rede

No switch multicamada SW1, o administrador criou a interface vlan 30 com IP 10.30.0.1/24 e no shutdown, mas show ip interface brief mostra Vlan30 com status down e protocolo down. O comando show vlan brief não lista a VLAN 30. Qual ação faz a SVI subir?

A. Aplicar no switchport na interface vlan 30
B. Configurar ip default-gateway no switch SW1
C. Criar a VLAN 30 e ter uma porta ativa nessa VLAN
D. Executar o comando ip routing no modo global

D5 · 2.0 Switching e Acesso à Rede

Por política, a porta Gi1/0/30 de um switch PoE, ligada a um appliance com fonte própria, deve funcionar só para dados e jamais fornecer energia, mesmo que o equipamento seja trocado. Qual comando atende?

A. no switchport
B. power inline never
C. power inline static
D. power inline auto

D6 · 2.0 Switching e Acesso à Rede

Por política de segurança, as portas trunk entre os switches do núcleo devem ficar fixas em trunk e não devem enviar quadros DTP, para não negociar com dispositivos indevidos. Qual comando de interface completa essa configuração após switchport mode trunk?

A. switchport trunk native vlan 1
B. switchport nonegotiate
C. switchport port-security
D. switchport mode dynamic auto

D7 · 3.0 Roteamento IP

No R1 convivem duas entradas: uma aprendida do OSPF para 10.80.0.0/16, com AD 110, via 10.0.0.2, e uma estática para 10.80.9.0/24, configurada com AD 200, via 172.30.0.1. Um servidor em 10.80.9.50 recebe tráfego vindo do R1. Qual vizinho entrega esse tráfego?

A. 172.30.0.1, pela entrada /24
B. 10.0.0.2, pela métrica menor
C. 10.0.0.2, pela AD menor do OSPF
D. Os dois vizinhos, alternando

D8 · 3.0 Roteamento IP

O analista da filial executa show standby no roteador R2 para saber qual equipamento é o gateway ativo da VLAN 10 e obtém a saída: Vlan10 - Group 10; State is Standby; Virtual IP address is 10.10.10.1; Active router is 10.10.10.3, priority 110; Standby router is local; Priority 100 (default 100). Com base nessa saída, qual afirmação está correta?

A. O R2 é standby; 10.10.10.3 encaminha pelo IP virtual
B. O R2 tem prioridade maior e assumirá ao habilitar preempt
C. Os hosts devem usar 10.10.10.3 como gateway padrão
D. O R2 encaminha o tráfego enviado ao IP virtual da VLAN 10

D9 · 3.0 Roteamento IP

Configuração do R1: ip route 0.0.0.0 0.0.0.0 203.0.113.1 e ip route 0.0.0.0 0.0.0.0 198.51.100.1 10. Em show ip route aparece apenas S* 0.0.0.0/0 [1/0] via 203.0.113.1. O que acontece se o enlace com o provedor 203.0.113.1 cair e o próximo salto ficar inalcançável?

A. O R1 fica sem rota default até o enlace principal voltar
B. As duas defaults passam a ser usadas em balanceamento
C. O R1 envia o tráfego em broadcast para os dois provedores
D. A default via 198.51.100.1, com AD 10, entra na tabela

D10 · 4.0 Serviços de Rede e Segurança

Com RA guard aplicado com device-role host nas portas de acesso, as estações deixaram de receber RAs, inclusive os do roteador legítimo ligado ao uplink Gi1/0/48. Como corrigir mantendo a proteção?

A. Aplicar no Gi1/0/48 uma política com device-role router
B. Aplicar device-role host também no uplink Gi1/0/48
C. Remover o RA guard de todas as portas do switch
D. Habilitar DHCP snooping trust no uplink Gi1/0/48

D11 · 4.0 Serviços de Rede e Segurança

Ao estudar a VPN IPsec entre a matriz e uma filial, o analista quer entender o papel do IKE. Qual descrição está correta?

A. O IKE cifra cada pacote de dados do túnel
B. O IKE substitui o ESP no transporte dos dados do túnel
C. O IKE distribui rotas entre as LANs da VPN
D. O IKE autentica os pares e negocia SAs e chaves

D12 · 4.0 Serviços de Rede e Segurança

Para bloquear Telnet a um servidor, o administrador aplicou na entrada da interface da LAN a ACL a seguir, que tem uma única linha: access-list 101 deny tcp any host 10.1.50.10 eq 23. Logo depois, todos os usuários da LAN perderam acesso a todas as redes. Qual é a causa?

A. ACLs estendidas precisam usar a faixa de 1 a 99
B. Falta uma linha permit; o deny implícito descarta o resto
C. A porta 23 bloqueia também o tráfego web dos usuários
D. A ACL estendida deveria ser aplicada na saída da interface

01

CAPÍTULO 1 · 25% DA PROVA

1.0 Infraestrutura e Conectividade de Rede

Aqui eu preciso fazer conta de sub-rede IPv4 de cabeça (rede, broadcast, hosts, VLSM), dominar IPv6 (abreviação, tipos de endereço, EUI-64 modificado, /64 na LAN e /127 entre roteadores), ler contadores de interface e problemas de cabo e fibra, entender Wi-Fi (bandas, canais, segurança, interferência), virtualização e o DHCPv4 do IOS XE como cliente, servidor e relay. A prova traz endereço com prefixo para calcular, saídas de ipconfig /all, show interfaces e show ip dhcp para interpretar e cenários de cliente Windows, macOS e Linux. Onde mais erro: blocos maiores que /24 (onde .255 e .0 podem ser hosts), esquecer de inverter o 7º bit no EUI-64 e confundir os sintomas de duplex incompatível (late collisions), cabo ruim (CRC) e congestionamento (output drops).

Neste capítulo
18 tópicos-chave · 14 pegadinhas · 8 macetes · 14 gatilhos · 4 questões comentadas

Tópicos-chave

Rede e broadcast pelo tamanho do bloco

Cada prefixo define um bloco: /26 = 64, /27 = 32, /28 = 16, /29 = 8. O endereço de rede é o maior múltiplo do bloco menor ou igual ao valor do host; o broadcast é o último endereço do bloco. Ex.: 192.168.5.77/29 está em .72 a .79; 172.16.45.70/26 está em .64 a .127.

Hosts e quantidade de sub-redes

Hosts utilizáveis = 2^(bits de host) - 2: /27 = 30, /28 = 14, /26 = 62. Sub-redes = 2^(bits emprestados): /24 em /28 = 16, /22 em /26 = 16. Para 50 hosts, o menor que atende é /26 (62); /25 funciona mas desperdiça.

Blocos maiores que /24

Na /23 o incremento é 2 no terceiro octeto (192.168.10.0 a 192.168.11.255, 510 hosts) e na /21 é 8 (10.0.8.0 a 10.0.15.255). Nesses blocos, endereços terminados em .255 ou .0 no meio da faixa são hosts válidos; o último utilizável da 192.168.10.0/23 é 192.168.11.254.

VLSM

Aloque primeiro as maiores sub-redes, cada uma alinhada ao seu tamanho. Para 120, 60 e 25 hosts em 192.168.50.0/24: .0/25, .128/26 e .192/27, sobrando .224/27. Sub-redes sobrepostas ou pequenas demais derrubam a alternativa.

Faixas especiais de IPv4

Privados (RFC 1918): 10.0.0.0/8, 172.16.0.0/12 (172.16 a 172.31) e 192.168.0.0/16. 100.64.0.0/10 é o espaço compartilhado de provedor (RFC 6598, NAT de operadora), 169.254.0.0/16 é link-local de autoconfiguração e 192.0.2.0/24, 198.51.100.0/24 e 203.0.113.0/24 são de documentação.

/31 em IPv4 e /127 em IPv6

Em enlaces ponto a ponto, a RFC 3021 permite /31, sem endereços de rede e broadcast, gastando metade do /30. No IPv6, a RFC 6164 recomenda /127 entre roteadores, evitando o ping-pong; em LAN com hosts o padrão continua /64.

Abreviação de IPv6

Remova só os zeros à esquerda de cada grupo de 16 bits e troque uma única sequência de grupos zerados por ::. Zeros à direita nunca saem: 00A0 vira A0, e não A. 2001:0DB8:0000:0000:0000:00A0:0000:0001 vira 2001:DB8::A0:0:1.

Tipos de endereço IPv6

Link-local FE80::/10 (gerado automaticamente, bastando ipv6 enable; não roteado; usado como próximo salto), global unicast 2000::/3, local único FC00::/7 (na prática FD00::/8, para uso interno estável), multicast FF00::/8 e documentação 2001:DB8::/32. O solicited-node é FF02::1:FF seguido dos 24 bits finais do unicast e substitui o broadcast do ARP.

EUI-64 modificado

O roteador divide o MAC ao meio, insere FFFE entre o 3º e o 4º bytes e inverte o 7º bit do primeiro byte (02 vira 00, 00 vira 02). MAC 0050.56A1.2B3C com 2001:DB8:ACAD:10::/64 gera 2001:DB8:ACAD:10:250:56FF:FEA1:2B3C. O prefixo é manual; só o ID de interface vem do MAC.

SLAAC e Router Advertisement

No SLAAC o host junta o prefixo do RA a um ID de 64 bits, por isso a LAN precisa de /64 (um /80 quebra a autoconfiguração). O roteador IOS XE só envia RAs com ipv6 unicast-routing ativo. ipv6 address autoconfig faz a interface do roteador agir como cliente SLAAC; ipv6 address dhcp usa DHCPv6.

DHCPv4: DORA e relay

Discover (cliente, broadcast), Offer (servidor), Request (cliente) e Ack (servidor), sobre UDP 67 no servidor e 68 no cliente. Broadcast não atravessa roteador: ip helper-address na interface do lado dos clientes converte em unicast e preenche o giaddr, que o servidor usa para escolher o pool e para devolver a resposta.

Servidor DHCP no IOS XE

No pool: network (sub-rede e máscara), default-router (gateway), dns-server e lease (padrão de um dia; lease dias horas minutos ou infinite). Endereços fixos ficam fora com ip dhcp excluded-address, no modo global. Diagnóstico: show ip dhcp pool (alugados x total), binding (Client-ID 01 + MAC) e conflict (IP já em uso detectado por ping e ARP gratuito).

Contadores de erro de interface

CRC/FCS e input errors apontam cabo, porta, NIC ou duplex. Runts são quadros menores que 64 bytes com CRC inválido; giants passam de 1518 bytes com FCS inválido. Late collisions aparecem no lado half-duplex de um duplex incompatível. Output drops sem CRC indicam congestionamento na saída, não falha física.

Duplex e autonegociação

Fixar velocidade desliga toda a autonegociação da porta, inclusive a do duplex. Se um lado está fixo e o outro em auto, o lado em auto detecta a velocidade pelo sinal mas não o duplex e assume half-duplex: o enlace sobe com erros e lentidão. A correção é configurar as duas pontas iguais.

Cabeamento de cobre e fibra

Par trançado Ethernet, inclusive 1000BASE-T, vai até 100 m. Sem auto-MDIX, equipamentos diferentes usam cabo direto e iguais (switch-switch) usam cruzado; com auto-MDIX em pelo menos um lado, qualquer cabo funciona. Óticas: SX para multimodo (centenas de metros), LX/LH até 10 km em monomodo e 550 m em multimodo, EX até 40 km em monomodo.

Bandas e canais Wi-Fi

2,4 GHz alcança mais e atravessa melhor obstáculos, mas nos EUA só tem três canais sem sobreposição (1, 6 e 11). 5 GHz tem mais de 20 canais de 20 MHz e células menores; canais DFS mudam sozinhos ao detectar radar. Wi-Fi 5 = 802.11ac, Wi-Fi 6 = 802.11ax, 6E acrescenta 6 GHz, Wi-Fi 7 = 802.11be. Canais mais largos reduzem o número de canais para reúso.

Segurança Wi-Fi

WPA3-Personal usa SAE no lugar da PSK do WPA2 e resiste a ataque de dicionário; o WPA3 exige PMF (802.11w), o que pode barrar clientes antigos (use modo misto WPA2/WPA3 na transição). Credencial por usuário pede modo Enterprise com 802.1X e RADIUS. WEP e WPA/TKIP são inseguros.

Hipervisor, VM e contêiner

O hipervisor virtualiza o hardware e reparte CPU, memória, disco e rede entre VMs isoladas, cada uma com seu SO (Windows e Linux no mesmo host). O motor de contêineres virtualiza o SO: contêineres compartilham o kernel do host, são leves e sobem em segundos. Cada vNIC tem MAC próprio e se liga ao switch virtual do host, por isso a porta física mostra vários MACs.

Macetes para memorizar

Tamanho dos blocos

/25=128, /26=64, /27=32, /28=16, /29=8, /30=4: rede é o múltiplo do bloco, broadcast é o próximo múltiplo menos 1.

EUI-64

Parte o MAC, enfia FFFE no meio, vira o 7º bit (02 vira 00, 00 vira 02).

DHCP DORA

D e R saem do cliente, O e A saem do servidor; cliente sem IP grita em broadcast.

Canais 2,4 GHz

Um, seis, onze: os únicos que não se pisam.

Gerações Wi-Fi

ac = 5, ax = 6, 6E = 6 + banda de 6 GHz, be = 7.

Cabo sem auto-MDIX

Diferentes se ligam direto; iguais se cruzam.

Sinal e SNR

dBm mais perto de zero é mais forte; SNR = sinal menos ruído (-70 com ruído -92 dá 22 dB).

Fibra

SX fica no multimodo; LX/LH vai Longe no monomodo (10 km).

Tabela de memorização: não confunda

Quando é...	...e quando é
2,4 GHz Cobertura maior e melhor penetração em paredes e prateleiras; sofre com micro-ondas, Bluetooth e telefones sem fio; só 1, 6 e 11 sem sobreposição nos EUA.	**5 GHz** Muitos canais para reúso em alta densidade, ao custo de células menores; canais DFS podem mudar ao detectar radar.
Máquina virtual (hipervisor) Cada carga precisa de SO completo e próprio, inclusive SOs diferentes no mesmo host, com isolamento por hardware virtualizado.	**Contêiner (motor de contêineres)** Empacotar aplicação e bibliotecas, leve e portátil, subindo dezenas de instâncias em segundos sobre o kernel do host.

WPA2/WPA3-Personal Senha compartilhada por todos (no WPA3 protegida pelo SAE); trocar a senha afeta todos os usuários.	**WPA2/WPA3-Enterprise (802.1X)** Credencial individual validada em servidor RADIUS; revoga quem saiu sem mexer nos demais.
Late collisions, runts e erros com enlace up Duplex incompatível (um lado half): alinhe as duas pontas, de preferência em auto.	**CRC crescendo com duplex igual nas duas pontas** Problema físico no ponto (cabo ou conector): teste e troque o cabeamento.
Interferência cocanal APs vizinhos no mesmo canal (ex.: ambos no 6) disputando o meio como um hub.	**Interferência de canal adjacente** APs em canais que se sobrepõem (ex.: 1 e 3), gerando erros e retransmissões; use só 1, 6 e 11.
1000BASE-SX Fibra multimodo em distâncias de centenas de metros.	**1000BASE-LX/LH** Fibra monomodo até 10 km (ou multimodo até 550 m), como entre prédios a 2 km.
ipconfig /flushdns Registro DNS mudou e o cliente Windows ainda usa o IP antigo em cache.	**ipconfig /release e /renew** Cliente pegou endereço da VLAN ou pool errado e precisa de nova concessão DHCP.

Números que caem

Item	Valor
Limite do par trançado Ethernet (inclui 1000BASE-T)	**100 m**
1000BASE-LX/LH	**até 10 km em monomodo; até 550 m em multimodo**
1000BASE-EX	**até 40 km em monomodo**
Runts / giants	**menores que 64 bytes / maiores que 1518 bytes, com CRC/FCS inválido**
Canais sem sobreposição em 2,4 GHz (EUA)	**1, 6 e 11**
Canais de 20 MHz em 5 GHz	**mais de 20**
Banda de 6 GHz com canais de 320 MHz	**apenas três canais nos 1200 MHz**
SNR recomendada (Cisco Meraki)	**dados 20 dB; voz 25 dB**
Lease padrão do DHCP no IOS XE	**1 dia**
Portas do DHCPv4	**UDP 67 (servidor) e UDP 68 (cliente)**
Sub-redes /64 em um /56 e em um /48	**256 e 65.536**
Limite de saltos do tracert do Windows	**30**

Alertas de prova (pegadinhas)

⚠ **Alerta de prova:** Achar que 172.32.0.5 ou 100.64.1.1 são privados por parecerem com faixas internas.
Como não cair: 172.16.0.0/12 vai só até 172.31.255.255; 100.64.0.0/10 é espaço compartilhado de provedor (RFC 6598), não RFC 1918.

⚠ **Alerta de prova:** Descartar 192.168.10.255 como host na 192.168.10.0/23 por terminar em .255.
Como não cair: Em blocos maiores que /24, o broadcast é só o último endereço do bloco (192.168.11.255); .255 no meio é host válido.

⚠ **Alerta de prova:** No EUI-64, copiar o primeiro byte do MAC sem mexer ou colocar FFFE no fim.
Como não cair: FFFE entra entre o 3º e o 4º bytes e o 7º bit é invertido: 00 vira 02 e 02 vira 00.

⚠ **Alerta de prova:** Abreviar 00A0 para A ou usar :: duas vezes.
Como não cair: Só zeros à esquerda saem (00A0 = A0) e o :: aparece uma única vez.

⚠ **Alerta de prova:** Responder 172.16.45.255 como broadcast de 172.16.45.70/26, raciocinando como /24.
Como não cair: /26 tem blocos de 64: .70 está em .64 a .127, então o broadcast é .127.

⚠ **Alerta de prova:** No VLSM, dar /27 para um setor de 60 hosts ou /26 para 120.
Como não cair: /27 tem 30 hosts e /26 tem 62: confira 2^n - 2 antes de alocar e comece pelo maior.

⚠ **Alerta de prova:** Ver late collisions com enlace up e culpar cabo cruzado ou velocidade diferente.
Como não cair: Pinagem errada impede o enlace e velocidade diferente normalmente nem sobe; late collisions no lado half indicam duplex incompatível.

⚠ **Alerta de prova:** Ver output drops no uplink e mandar trocar o cabo.
Como não cair: Cabo ruim gera CRC e erros de entrada; output drops com CRC zerado é congestionamento (mais banda, como EtherChannel).

⚠ **Alerta de prova:** Acreditar que o lado em auto copia o full-duplex do lado fixado.
Como não cair: Sem negociação do outro lado, o lado em auto detecta só a velocidade e cai para half-duplex.

⚠ **Alerta de prova:** Culpar radar por problemas em 2,4 GHz ou micro-ondas por mudança de canal em 5 GHz.
Como não cair: Radar afeta canais DFS de 5 GHz; micro-ondas, Bluetooth e telefones sem fio interferem em 2,4 GHz.

⚠ **Alerta de prova:** Chamar APs nos canais 1 e 3 de interferência cocanal.
Como não cair: Cocanal é mesmo canal; canais diferentes que se sobrepõem geram interferência de canal adjacente.

⚠ **Alerta de prova:** Escolher WPA3-Personal para dar credencial própria a cada funcionário.
Como não cair: Personal continua com senha compartilhada; credencial individual é Enterprise com 802.1X e RADIUS.

⚠ **Alerta de prova:** Colocar ip helper-address na interface voltada ao datacenter ou usar ip address dhcp para atender os clientes.
Como não cair: O relay vai na interface (ou subinterface) que recebe o broadcast dos clientes; ip address dhcp torna o roteador cliente DHCP.

⚠ **Alerta de prova:** Usar ipconfig /renew ou /registerdns para resolver nome apontando para IP antigo.
Como não cair: Cache de nomes no Windows se limpa com ipconfig /flushdns; /renew trata da concessão DHCP.

Como cai na prova

📝 **Como cai:** Um endereço com prefixo (ex.: 10.20.30.140/28) e pede rede, broadcast, último host ou quantidade de hosts.
Como resolver: Ache o octeto interessante, o tamanho do bloco (16 na /28), o maior múltiplo menor ou igual ao valor (128) e o fim do bloco (143). Hosts = 2^n - 2.

📝 **Como cai:** Saída de ipconfig /all ou ip route com um campo errado e sintoma de alcance parcial.
Como resolver: Confira se o gateway é host válido dentro da sub-rede do cliente (nunca broadcast nem fora da máscara), se há 169.254, se a máscara bate com a dos vizinhos e se existe default.

📝 **Como cai:** Contadores de show interfaces (CRC, runts, late collisions, output drops) com o histórico de configuração das pontas.
Como resolver: Primeiro veja duplex e velocidade das duas pontas; se diferentes, é duplex. Se iguais e há CRC, é cabo. Se só output drops, é congestionamento.

📝 **Como cai:** Cenário de Wi-Fi descrevendo local, banda e sintoma (galpão, refeitório, aeroporto, auditório).
Como resolver: Associe sintoma à causa: alcance e obstáculos = banda; horário de micro-ondas = 2,4 GHz; troca de canal = DFS; lentidão com sinal forte = cocanal; erros com canais 1 e 3 = adjacente.

📝 **Como cai:** MAC e prefixo /64 com eui-64 pedindo o endereço formado, ou endereço longo pedindo a forma abreviada.
Como resolver: Para EUI-64: divida o MAC, insira FFFE, inverta o 7º bit, junte ao prefixo. Para abreviar: tire zeros à esquerda e use :: uma vez no maior bloco de zeros.

📝 **Como cai:** Clientes sem endereço com servidor DHCP remoto ou pool local no roteador.
Como resolver: Servidor remoto: helper-address na interface dos clientes e rota de volta ao giaddr. Pool local: network, default-router, excluded-address e se o pool não esgotou.

Gatilhos do enunciado

Se o enunciado trouxer...	Pense em
Cliente com 169.254.x.x e gateway em branco	**Nenhuma resposta do servidor DHCP: verifique enlace, VLAN da porta, relay e servidor.**
Ping por IP funciona, por nome dá 'não encontrado'	**DNS: teste com nslookup no cliente.**
Late collisions no lado half-duplex	**Duplex incompatível entre as pontas.**
Output drops no uplink em horário de backup, CRC zerado	**Congestionamento de saída, sem falha física.**
CRC em qualquer computador ligado ao mesmo ponto, duplex igual	**Cabo ou conector danificado no ponto.**
AP em 5 GHz perto de aeroporto muda de canal sozinho	**DFS detectou radar.**
Wi-Fi lento no refeitório no horário do almoço em 2,4 GHz	**Interferência dos fornos de micro-ondas.**
Notebook vê o SSID com sinal forte e não conecta após mudança de segurança	**Tipo de segurança do perfil salvo difere do exigido pelo SSID.**
Clientes antigos com WPA2 não conectam após ligar WPA3	**PMF (802.11w) obrigatório no WPA3.**
Vários MACs numa porta com um único servidor e uma NIC	**vNICs das VMs passando pelo switch virtual do host.**

Discover chega ao servidor com giaddr, mas a Offer nunca volta	**Servidor DHCP sem rota de volta para a sub-rede do giaddr.**
Clientes novos sem IP e os antigos funcionando; pool todo alugado	**Pool DHCP esgotado: ampliar sub-rede, reduzir lease ou limpar concessões.**
Notebooks não formam endereço por SLAAC nem recebem gateway IPv6	**Falta ipv6 unicast-routing no roteador (ou prefixo da LAN não é /64).**
Linux alcança só a própria sub-rede; ip route sem linha default	**ip route add default via IP-do-roteador.**

🎯 **Se você lembrar de só uma coisa deste capítulo...**

- Gateway tem de ser host válido na mesma sub-rede do cliente: nunca o broadcast, nunca fora da máscara.
- EUI-64: FFFE no meio e 7º bit invertido; SLAAC só funciona com /64 e com ipv6 unicast-routing no roteador.
- Late collisions = duplex; CRC com duplex certo = cabo; output drops sem CRC = congestionamento.
- helper-address vai na interface dos clientes; o servidor escolhe o pool pelo giaddr e precisa de rota de volta.
- 2,4 GHz: 1, 6 e 11, mais alcance e interferência de micro-ondas; 5 GHz: mais canais, menos alcance, DFS.

Essenciais para a prova (checklist)

☐ Sei achar rede, broadcast e faixa de hosts de /21 a /29 em menos de um minuto.

☐ Sei montar VLSM do maior para o menor sem sobreposição.

☐ Sei classificar 10/8, 172.16/12, 192.168/16, 100.64/10, 169.254/16 e os blocos de documentação.

☐ Sei abreviar IPv6 e formar endereço EUI-64 com a inversão do 7º bit.

☐ Sei distinguir link-local, global, ULA, multicast e solicited-node.

☐ Sei diagnosticar duplex, cabo e congestionamento pelos contadores de interface.

☐ Sei escolher ótica e fibra (SX, LX/LH, EX) pela distância.

☐ Sei explicar bandas, canais, DFS, interferência e WPA3 (SAE e PMF) x Enterprise (802.1X).

☐ Sei configurar pool DHCP, excluded-address, relay e ler binding, conflict e pool no IOS XE.

☐ Sei os comandos de cliente: ipconfig /all, /release, /renew, /flushdns, arp -a, nslookup, ip address, ip route, nmcli device status e /etc/resolv.conf.

Questões de revisão do capítulo

R1.1 · 1.0 Infraestrutura e Conectividade de Rede

Uma câmera de segurança no estacionamento fica a 140 metros do rack, e o técnico quer ligá-la com um único lance de cabo Cat 6 até a porta 1000BASE-T do switch. Qual é o problema dessa proposta?

A. Funciona só se a porta estiver em half-duplex
B. Precisa de auto-MDIX para alcançar 140 metros
C. Passa do limite de 100 m do par trançado
D. Exige cabo cruzado acima de 100 metros

R1.2 · 1.0 Infraestrutura e Conectividade de Rede

Ao comparar propostas de APs, um gestor vê os termos Wi-Fi 6 e Wi-Fi 7 e pede a correspondência com os padrões IEEE. Qual associação está correta?

A. Wi-Fi 6 é 802.11ac e Wi-Fi 7 é 802.11ax
B. Wi-Fi 6 é 802.11ax e Wi-Fi 7 é 802.11be
C. Wi-Fi 6 é 802.11n e Wi-Fi 7 é 802.11ac
D. Wi-Fi 6 é 802.11be e Wi-Fi 7 é 802.11ax

R1.3 · 1.0 Infraestrutura e Conectividade de Rede

Uma regra de firewall será escrita para a sub-rede /29 em que está o leitor de crachás 192.168.5.77. Qual é o endereço de rede dessa sub-rede?

A. 192.168.5.80/29
B. 192.168.5.72/29
C. 192.168.5.64/29
D. 192.168.5.76/29

R1.4 · 1.0 Infraestrutura e Conectividade de Rede

Um técnico habilitou IPv6 em uma interface de roteador apenas com o comando ipv6 enable, sem configurar endereço global. Em show ipv6 interface, aparece um endereço já configurado. A qual tipo e prefixo esse endereço pertence?

A. Multicast, no prefixo FF00::/8
B. Local único, no prefixo FC00::/7
C. Global unicast, no prefixo 2000::/3
D. Link-local, no prefixo FE80::/10

Respostas comentadas

R1.1. C) Passa do limite de 100 m do par trançado

Por quê: O par trançado Ethernet (incluindo 1000BASE-T) tem limite de 100 m por enlace. Distâncias maiores pedem fibra óptica ou um switch intermediário.

✗ A) Incorreta. O modo duplex não estende o alcance do cobre.
✗ B) Incorreta. O auto-MDIX ajusta pares, mas não aumenta a distância suportada.
✗ D) Incorreta. O tipo de cabo (direto ou cruzado) não muda o alcance máximo.

> **Dica de prova:** Cobre Ethernet: até 100 m.

R1.2. B) Wi-Fi 6 é 802.11ax e Wi-Fi 7 é 802.11be

Por quê: A Wi-Fi Alliance numerou as gerações: 802.11ac = Wi-Fi 5, 802.11ax = Wi-Fi 6 (6E na banda de 6 GHz) e 802.11be = Wi-Fi 7.

✗ A) Incorreta. O 802.11ac corresponde ao Wi-Fi 5.
✗ C) Incorreta. O 802.11n é anterior ao 802.11ac.
✗ D) Incorreta. A associação está invertida.

> **Dica de prova:** ax = Wi-Fi 6; be = Wi-Fi 7.

R1.3. B) 192.168.5.72/29

Por quê: Na /29 o incremento é 8: 64, 72, 80... O maior múltiplo de 8 menor ou igual a 77 é 72; o bloco vai de .72 (rede) a .79 (broadcast).

✗ A) Incorreta. 192.168.5.80/29 começa depois do endereço do leitor.
✗ C) Incorreta. 192.168.5.64/29 vai de .64 a .71.
✗ D) Incorreta. 76 não é múltiplo de 8, então não é início de bloco /29.

> **Dica de prova:** /29 = blocos de 8.

R1.4. D) Link-local, no prefixo FE80::/10

Por quê: O link-local é obrigatório em interfaces IPv6 e é usado na vizinhança, por exemplo como próximo salto de protocolos de roteamento. Ele não é roteado para fora do enlace.

✗ A) Incorreta. A interface entra em grupos multicast, mas o endereço unicast gerado é o link-local.
✗ B) Incorreta. ULAs precisam ser configurados; não surgem só com ipv6 enable.
✗ C) Incorreta. O endereço global depende de configuração manual, SLAAC ou DHCPv6.

> **Dica de prova:** Endereço automático da interface IPv6: link-local FE80::/10.

02

CAPÍTULO 2 · 25% DA PROVA

2.0 Switching e Acesso à Rede

Aqui eu preciso dominar a ligação entre switches e roteadores (portas L2 e L3, trunks 802.1Q, SVIs, router-on-a-stick, EtherChannel com LACP), a porta certa para cada dispositivo de borda (estação, impressora, telefone IP, AP, host virtualizado, appliance), a validação de documentação com CDP e LLDP, o Rapid PVST+ completo e o diagnóstico com show, ping, ping estendido, traceroute, logs e captura de pacotes. A prova é cheia de saídas de show spanning-tree, show interfaces trunk, show etherchannel summary e show ip interface brief. Onde mais erro: allowed vlan sem add, as combinações de DTP e LACP que não sobem, a diferença entre BPDU guard, root guard e loop guard e os temporizadores padrão de CDP e LLDP.

Neste capítulo

18 tópicos-chave · 14 pegadinhas · 7 macetes · 14 gatilhos · 4 questões comentadas

Tópicos-chave

Lista de VLANs permitidas no trunk

switchport trunk allowed vlan sem modificador substitui a lista inteira; add, remove e except alteram a lista atual. Esquecer o add derruba as VLANs que já passavam. VLAN ausente da lista allowed em show interfaces trunk não atravessa o enlace.

VLAN nativa

Quadros sem tag no trunk pertencem à nativa de cada lado; nativas diferentes geram %CDP-4-NATIVE_VLAN_MISMATCH e vazamento entre VLANs. No roteador, a subinterface da nativa usa encapsulation dot1Q X native.

DTP e modo operacional

dynamic desirable inicia a negociação e dynamic auto só responde: auto com auto fica em acesso. switchport nonegotiate desliga o envio de DTP em portas fixas. Em show interfaces switchport, Administrative Mode é o configurado e Operational Mode é o resultado.

SVI e autostate

A SVI fica up/up quando a VLAN existe, há pelo menos uma porta ativa transportando a VLAN e não há shutdown. Sem a VLAN criada ou sem porta ativa nela, o protocolo fica down: se a VLAN não aparece em show vlan brief (down/down), crie-a; se a VLAN existe e a SVI mostra up/down, falta porta ativa (acesso ou allowed no trunk). ip routing é o que permite rotear entre SVIs, mas não altera o estado delas.

Porta roteada x switchport

no switchport transforma a porta física de um switch multicamada em L3 (sem VLAN nem STP), ideal para enlace dedicado com firewall ou roteador. switchport sem parâmetros devolve a porta à camada 2. Em switch só L2, a gerência de outras redes usa ip default-gateway.

Router-on-a-stick

O roteador usa uma subinterface por VLAN (Gi0/0/0.10 com encapsulation dot1Q 10 e IP de gateway) e a porta do switch voltada a ele é trunk. Roteador não aceita switchport; SVI é solução de switch multicamada.

EtherChannel com LACP

LACP (IEEE, entre fabricantes): active inicia, passive responde; forma canal com active-active ou active-passive. PAgP (Cisco) usa desirable/auto; on dispensa negociação. Membros precisam de configuração idêntica e o mesmo channel-group; o divergente fica suspenso e a mudança deve ser feita na interface Port-channel.

Flags de show etherchannel summary

P agregado, D down, s suspenso, I stand-alone, S camada 2, R camada 3, U em uso. Po1(SU) com um membro (P) e outro (D) continua operando só com o membro agregado; passive dos dois lados mostra portas (I) e canal (SD).

VLAN de voz

Telefone com PC atrás: switchport access vlan (dados, sem tag) + switchport voice vlan (voz, com tag 802.1Q). O telefone descobre a VLAN de voz pelo CDP (ou LLDP-MED para outros fabricantes). Uma porta de acesso tem uma só VLAN de acesso.

PoE

power inline auto (padrão) detecta e alimenta, never transforma a porta em só dados e static reserva potência fixa. O switch só alimenta se houver orçamento: em show power inline, Admin auto com Oper off e Remaining perto de zero significa potência esgotada.

Porta de AP: modo local x FlexConnect

AP em modo local leva o tráfego dos clientes em CAPWAP até o controlador Catalyst 9800: a porta é de acesso na VLAN de gerência do AP. AP FlexConnect com comutação local coloca cada SSID na VLAN da filial: a porta é trunk com a VLAN de gerência do AP como nativa.

Host virtualizado e dispositivo final

Host com VMs em várias VLANs: trunk 802.1Q só com as VLANs das VMs e spanning-tree portfast trunk. Impressora, desktop e IoT: porta de acesso na VLAN adequada com PortFast; IoT isolado em VLAN própria. Appliance com dois enlaces LACP: channel-group N mode active.

CDP e LLDP

Ambos descobrem só vizinhos diretos na camada 2. No Catalyst 9300 o CDP vem ligado (60 s de envio, 180 s de holdtime) e o LLDP desligado até lldp run (30 s e 120 s). Local Intrfce/Local Intf é a porta local; Port ID é a porta do vizinho; detail mostra IP de gerência, plataforma e versão. Por interface: no cdp enable e no lldp transmit/receive.

Bridge ID e root bridge

Bridge ID = prioridade + extended system ID (número da VLAN) + MAC; vence o menor, e no empate de prioridade o menor MAC. A prioridade vai de 0 a 61440 em múltiplos de 4096, padrão 32768 (exibida 32778 na VLAN 10). root primary define 24576 (ou menos que a raiz atual) e root secondary 28672.

Root port e designated port

Root port é a de menor custo acumulado até a raiz, não a de menos saltos; empates: menor bridge ID do remetente e depois menor ID de porta do remetente. Cada segmento tem uma designated port (menor custo até a raiz); na raiz todas são designadas. Para mudar a root port localmente, ajuste o custo da porta.

Estados e papéis do RSTP

Estados: discarding, learning e forwarding (blocking e listening são do 802.1D). Papéis: root, designated, alternate (caminho reserva por outra ponte) e backup (redundância no mesmo segmento pela própria ponte). Transição rápida só em portas edge e enlaces ponto a ponto full-duplex, via proposal/agreement; half-duplex é tratado como compartilhado. Rapid PVST+ é o modo padrão do Catalyst 9300.

PortFast, BPDU guard e BPDU filter

spanning-tree portfast default ativa PortFast nas portas não trunk e bpduguard default coloca em err-disabled a porta PortFast que receber BPDU; a volta é shutdown/no shutdown ou errdisable recovery configurado. bpdufilter default, ao receber BPDU, tira o PortFast da porta; aplicado na interface equivale a desligar o STP nela.

Root guard e loop guard

Root guard vai nas portas designadas do núcleo/distribuição voltadas para baixo: BPDU superior leva a porta a root-inconsistent, que se recupera sozinha. Loop guard protege portas root e alternate: se os BPDUs param (fibra unidirecional), a porta vai para loop-inconsistent em vez de encaminhar.

Macetes para memorizar

DTP e LACP

Auto é tímido e passive é calado: dois tímidos ou dois calados nunca começam a conversa.

Prioridades do STP

24 manda, 28 espera, 32 é padrão; tudo em passos de 4096 até 61440.

Temporizadores de descoberta

CDP 60/180; LLDP 30/120 (o LLDP envia na metade do intervalo do CDP).

Os três guards

BPDU guard derruba (err-disabled); root guard barra o BPDU melhor (root-inconsistent); loop guard sente falta do BPDU (loop-inconsistent).

Caracteres do ping do IOS

! chegou, . sumiu, U alguém avisou que não dá.

show etherchannel summary

P está no Pacote, D está Down, s está suspenso, I está Isolado.

Porta de telefone com PC

Access leva o PC sem tag; voice leva a voz com tag.

Tabela de memorização: não confunda

Quando é...	...e quando é
BPDU guard Porta de usuário/PortFast onde nunca deve aparecer switch: qualquer BPDU coloca a porta em err-disabled.	**Root guard** Porta designada do núcleo voltada aos acessos: BPDU superior leva a root-inconsistent, que volta sozinho.
Root guard Reage a BPDU superior chegando por onde a raiz não pode ficar.	**Loop guard** Reage à ausência de BPDUs em porta root ou alternate (enlace unidirecional), indo para loop-inconsistent.
LACP (active/passive) Padrão IEEE, entre fabricantes ou com firewalls e appliances.	**PAgP (desirable/auto)** Proprietário da Cisco; não negocia com LACP.
CDP Vizinhos Cisco; ligado por padrão no Catalyst 9300; 60 s / 180 s.	**LLDP** Padrão IEEE 802.1AB para vizinhos de qualquer fabricante; desligado por padrão (lldp run); 30 s / 120 s.
AP em modo local Tráfego vai em CAPWAP ao controlador: porta de acesso na VLAN de gerência do AP.	**AP FlexConnect com comutação local** SSIDs saem nas VLANs da filial: trunk com nativa = VLAN de gerência do AP.

SVI Gateway de uma VLAN com muitos hosts em várias portas.	**Porta roteada (no switchport)** Enlace L3 dedicado a um único vizinho (firewall, roteador), sem VLAN nem STP.
traceroute do IOS Usa sondas UDP; um firewall que bloqueia UDP alto mostra só asteriscos.	**tracert do Windows** Usa ICMP Echo; passa onde ICMP é permitido. Ambos usam TTL e Time Exceeded.

Números que caem

Item	Valor
Prioridade STP padrão	**32768**
root primary / root secondary	**24576 / 28672**
Faixa de prioridade STP	**0 a 61440, em múltiplos de 4096**
CDP: envio / holdtime	**60 s / 180 s**
LLDP no Catalyst 9300: envio / holdtime	**30 s / 120 s (desabilitado globalmente por padrão)**
Ping padrão do IOS	**5 pacotes de 100 bytes, timeout de 2 s**
Traceroute do IOS	**até 30 saltos por padrão**
Forward delay do STP clássico	**15 s**

Alertas de prova (pegadinhas)

⚠ **Alerta de prova:** Usar switchport trunk allowed vlan 30 para acrescentar a VLAN 30.
Como não cair: Sem add a lista é substituída e o trunk passa a levar só a VLAN 30; use allowed vlan add 30.

⚠ **Alerta de prova:** Usar root secondary ou priority 61440 para garantir que o switch seja a raiz.
Como não cair: Ser raiz é root primary (24576); secondary (28672) é reserva; 61440 é a pior prioridade possível.

⚠ **Alerta de prova:** Achar que dynamic auto nos dois lados forma trunk.
Como não cair: auto só responde; é preciso desirable ou trunk em pelo menos um lado. auto + auto = acesso.

⚠ **Alerta de prova:** Configurar passive nos dois lados ou desirable para negociar com LACP.
Como não cair: passive + passive não forma canal; desirable e auto são PAgP. Um lado precisa de active.

⚠ **Alerta de prova:** Esperar que a porta em err-disabled por BPDU guard volte sozinha em 30 segundos.
Como não cair: Só volta com shutdown/no shutdown ou errdisable recovery configurado; corrija a causa antes.

⚠ **Alerta de prova:** Dizer que root guard coloca a porta em err-disabled.
Como não cair: err-disabled é do BPDU guard; root guard usa root-inconsistent e loop guard usa loop-inconsistent.

⚠ **Alerta de prova:** Escolher bpdufilter para derrubar a porta quando aparecer um switch.
Como não cair: BPDU filter não desativa a porta e pode esconder loops; a proteção é bpduguard.

⚠ **Alerta de prova:** Aplicar no switchport na SVI ou ip routing para subir uma SVI down.
Como não cair: SVI sobe com VLAN criada e porta ativa nela; no switchport é para porta física e ip routing só roteia.

⚠ **Alerta de prova:** Usar ip routing em switch L2 para ser gerenciado de outras redes.
Como não cair: Switch só L2 precisa de ip default-gateway para o tráfego de gerência dele.

⚠ **Alerta de prova:** Marcar 10 s e 40 s ou 60 s e 180 s como padrão do LLDP.
Como não cair: 10/40 são hello/dead do OSPF; 60/180 são do CDP. LLDP no Catalyst 9300: 30 s e 120 s.

⚠ **Alerta de prova:** Usar no cdp run para esconder o CDP só na interface do provedor, ou no lldp run para tirar LLDP de uma porta.
Como não cair: Os comandos globais desligam no equipamento inteiro; por porta use no cdp enable ou no lldp transmit e no lldp receive.

⚠ **Alerta de prova:** Escolher como root port o enlace direto de 100 Mb/s por ter menos saltos.
Como não cair: Vale o menor custo acumulado; dois enlaces de 1 Gb/s custam menos que um de 100 Mb/s.

⚠ **Alerta de prova:** Ler U.U.U no ping como tempo esgotado.
Como não cair: ! é resposta, . é tempo esgotado e U é destino inalcançável devolvido por um roteador (os pontos intercalados vêm do limite de taxa de ICMP).

⚠ **Alerta de prova:** Interpretar Gi1/0/2(D) em show etherchannel summary como porta suspensa.
Como não cair: D é down; suspensa é s minúsculo e isolada é I.

Como cai na prova

📝 **Como cai:** Saída de show spanning-tree vlan X com Root ID, Bridge ID, papéis (Root, Desg, Altn, Back) e estados.
Como resolver: Compare Root ID com Bridge ID para saber se é a raiz, subtraia o número da VLAN da prioridade para achar o valor configurado e leia papel + estado de cada porta.

📝 **Como cai:** Saída de show interfaces trunk, show interfaces switchport ou show etherchannel summary com VLAN que não passa ou canal parcial.
Como resolver: Procure a lista allowed, a nativa e os modos administrativo x operacional; no EtherChannel leia as flags de cada membro e o protocolo.

📝 **Como cai:** Dispositivo de borda descrito (impressora, telefone + PC, AP local ou FlexConnect, servidor com VMs, firewall) e pergunta pela configuração da porta.
Como resolver: Pergunte quantas VLANs chegam com tag: uma só sem tag = acesso (+ PortFast); dados + voz = access + voice; várias = trunk; dois enlaces com appliance = LACP active.

📝 **Como cai:** Saída de show ip interface brief ou show interfaces status com estados misturados.
Como resolver: administratively down = shutdown; down/down = físico; up/down = protocolo/camada 2; notconnect = sem enlace; err-disabled = desligada por erro.

📝 **Como cai:** Resultado de ping ou traceroute (U.U.U, * * *, saltos alternando, encapsulation failed) pedindo a conclusão.
Como resolver: Traduza os símbolos, localize o último salto que respondeu e lembre que o ping do roteador usa como origem a interface de saída, salvo no ping estendido.

Gatilhos do enunciado

Se o enunciado trouxer...	Pense em
Root ID igual ao Bridge ID / This bridge is the root	**O switch local é a root bridge da VLAN.**
Prioridade exibida 32778 ou 24586 sem ninguém configurar o valor quebrado	**Extended system ID: prioridade + número da VLAN.**
Estações demoram cerca de 30 s para encaminhar e falham no DHCP ao ligar	**Falta spanning-tree portfast nas portas de estação.**
Papel Altn com estado BLK	**Porta alternate: caminho reserva até a raiz, descartando.**
%CDP-4-NATIVE_VLAN_MISMATCH	**Igualar a VLAN nativa nas duas pontas do trunk.**

SVI down/down e VLAN fora de show vlan brief; ou SVI up/down	**Criar a VLAN; ou colocar porta ativa na VLAN (acesso ou allowed no trunk).**
SVIs up/up e hosts usando-as como gateway, mas VLANs não se falam	**Falta ip routing no switch multicamada.**
Discover repetido sem Offer e servidor DHCP em outra sub-rede	**ip helper-address na interface de gateway da VLAN.**
debug com encapsulation failed para destino na mesma sub-rede	**ARP não resolveu o MAC do destino.**
Traceroute alternando 10.0.12.2 e 10.0.12.1 até o limite	**Loop de roteamento entre os dois roteadores.**
show power inline com Admin auto, Oper off e Remaining 0.5 W	**Orçamento PoE do switch esgotado.**
Vizinho de outro fabricante ou telefones de outra marca não aparecem	**LLDP: habilitar com lldp run (desligado por padrão no Catalyst 9300).**
Porta para em err-disabled depois que o usuário liga um switch	**BPDU guard: remover o switch e fazer shutdown/no shutdown.**
Ping do roteador ao servidor ok, mas usuários da LAN não alcançam	**Ping estendido com origem na interface da LAN para testar a rota de volta.**

🎯 **Se você lembrar de só uma coisa deste capítulo...**

- allowed vlan sem add substitui a lista; mudança de EtherChannel se faz na interface Port-channel.
- auto + auto (DTP) e passive + passive (LACP) não formam nada.
- BPDU guard = err-disabled; root guard = root-inconsistent; loop guard = loop-inconsistent.
- SVI up exige VLAN criada + porta ativa nela; rotear entre SVIs exige ip routing.
- Catalyst 9300 de fábrica: CDP ligado, LLDP desligado, Rapid PVST+ como modo de STP.

Essenciais para a prova (checklist)

☐ Sei configurar trunk com allowed vlan add/remove/except e nativa igual nas pontas.

☐ Sei o resultado de cada combinação DTP e LACP e as flags de show etherchannel summary.

☐ Sei quando usar SVI, porta roteada, router-on-a-stick e ip default-gateway.

☐ Sei configurar a porta para estação, impressora, telefone com PC, AP local, AP FlexConnect, host virtualizado e firewall.

☐ Sei usar e ler CDP e LLDP (Local Intf x Port ID, detail, padrões e comandos por porta).

☐ Sei eleger root bridge, root port e designated port e ajustar prioridade e custo.

☐ Sei os estados e papéis do RSTP e quando a transição é rápida.

- ☐ Sei aplicar PortFast, BPDU guard, root guard e loop guard no lugar certo e o efeito de cada um.
- ☐ Sei interpretar ping, ping estendido (source, size, df-bit, repeat), traceroute, show logging e monitor capture.

Questões de revisão do capítulo

R2.1 · 2.0 Switching e Acesso à Rede

Clientes da VLAN 70 não recebem endereço. Uma captura na porta de um cliente mostra a saída: DHCP Discover de 0.0.0.0 para 255.255.255.255 repetido a cada poucos segundos e nenhuma Offer. O servidor DHCP fica em outra sub-rede, atrás do gateway da VLAN 70. O que provavelmente falta?

A. spanning-tree portfast na porta do servidor DHCP
B. ip helper-address na interface de gateway da VLAN 70
C. ip dhcp snooping trust na porta do próprio cliente
D. ip default-gateway configurado no switch de acesso

R2.2 · 2.0 Switching e Acesso à Rede

Um servidor diz que não recebe pacotes de um cliente ligado à porta Gi1/0/1 do switch. O técnico quer capturar no próprio Catalyst 9300 o tráfego que entra nessa porta, para confirmar se os pacotes chegam. Qual recurso ele deve usar?

A. debug ip packet com a ACL do servidor aplicada
B. show interfaces Gi1/0/1 counters
C. show mac address-table dynamic interface Gi1/0/1
D. Embedded Packet Capture (monitor capture)

R2.3 · 2.0 Switching e Acesso à Rede

Um trunk entre dois switches transporta hoje apenas as VLANs 10 e 20. A nova VLAN 30 precisa passar pelo trunk sem interromper as VLANs atuais. Qual comando de interface deve ser usado nas duas pontas?

A. switchport trunk allowed vlan 30
B. switchport trunk native vlan 30
C. switchport trunk allowed vlan add 30
D. switchport trunk allowed vlan except 30

R2.4 · 2.0 Switching e Acesso à Rede

Um switch de distribuição precisa ser a root bridge da VLAN 10 e continuar sendo, mesmo que outro switch seja adicionado com a prioridade padrão. Qual comando, no modo de configuração global desse switch, atende ao requisito da forma recomendada?

A. spanning-tree vlan 10 root secondary
B. spanning-tree vlan 10 root primary
C. spanning-tree vlan 10 cost 1
D. spanning-tree vlan 10 priority 61440

Respostas comentadas

R2.1. B) ip helper-address na interface de gateway da VLAN 70

Por quê: Uma captura com Discover sem Offer indica que o pedido não alcança o servidor (ou a resposta não volta). Com servidor em outra sub-rede, configure o relay na interface L3 da VLAN.

✗ A) Incorreta. PortFast acelera a porta, mas o problema é o encaminhamento entre sub-redes.
✗ C) Incorreta. A porta do cliente não deve ser confiável; isso não faz o Discover chegar ao servidor.
✗ D) Incorreta. O gateway do switch L2 só serve ao tráfego de gerência dele.

> **Dica de prova:** Discover sem Offer e servidor remoto: falta relay (helper-address).

R2.2. D) Embedded Packet Capture (monitor capture)

Por quê: No Catalyst 9300, a captura de pacotes é feita com monitor capture, definindo a interface e a direção (in, out ou both), e o resultado pode ser exibido ou exportado.

✗ A) Incorreta. debug ip packet trata tráfego processado pela CPU e pode sobrecarregar o equipamento.
✗ B) Incorreta. Contadores mostram volumes, sem detalhar os pacotes.
✗ C) Incorreta. A tabela MAC mostra endereços aprendidos, não o conteúdo dos pacotes.

> **Dica de prova:** Ver os pacotes no próprio switch: monitor capture (EPC).

R2.3. C) switchport trunk allowed vlan add 30

Por quê: switchport trunk allowed vlan sem modificador substitui a lista; add, remove e except alteram a lista existente. Esquecer o add é causa comum de queda de VLANs no trunk.

✗ A) Incorreta. Sem add, a lista é substituída e o trunk passaria a levar só a VLAN 30.
✗ B) Incorreta. Muda a VLAN nativa, que não é o objetivo.
✗ D) Incorreta. except permitiria todas as VLANs menos a 30, o oposto do pedido.

> **Dica de prova:** Acrescentar VLAN no trunk: allowed vlan add.

R2.4. B) spanning-tree vlan 10 root primary

Por quê: root primary altera a prioridade do switch na VLAN para 24576 ou para um valor menor que o da raiz atual, sempre em múltiplos de 4096. A prioridade padrão é 32768.

✗ A) Incorreta. root secondary define 28672, preparando o switch para assumir só se a raiz principal falhar.

✗ C) Incorreta. O custo afeta a escolha de portas, não a eleição da root bridge.

✗ D) Incorreta. 61440 é a maior prioridade possível, o que torna o switch o pior candidato a raiz.

> **Dica de prova:** Ser raiz: root primary (24576); reserva: root secondary (28672).

03

CAPÍTULO 3 · 20% DA PROVA

3.0 Roteamento IP

Aqui eu preciso ler a tabela de roteamento e dizer para onde vai o pacote, configurar e diagnosticar rotas estáticas IPv4 e IPv6 (default, rede, host e flutuante), configurar OSPFv2 e OSPFv3 em área única (vizinhança, ponto a ponto, eleição de DR/BDR, router ID) e interpretar o estado de HSRP e VRRP. A prova traz trechos de show ip route, show ip ospf neighbor/interface e show standby/vrrp e pede o próximo salto, a causa ou o comando. Onde mais erro: deixar a distância administrativa passar na frente do prefixo mais longo, escolher AD errada para a flutuante, esquecer a interface quando o próximo salto IPv6 é link-local e confundir os padrões de preempção do HSRP e do VRRP.

Neste capítulo

18 tópicos-chave · 14 pegadinhas · 7 macetes · 14 gatilhos · 4 questões comentadas

Tópicos-chave

Ordem de escolha da rota

Primeiro o prefixo mais longo que contém o destino; para o mesmo prefixo, a menor distância administrativa entre fontes; dentro do mesmo protocolo, a menor métrica, e custos iguais geram balanceamento. Prefixos diferentes convivem na tabela e nunca são balanceados entre si.

Distâncias administrativas padrão

Conectada 0, estática 1, eBGP 20, OSPF 110, IS-IS 115, RIP 120, iBGP 200; 255 significa fonte não confiável e a rota nunca é instalada. Métricas de protocolos diferentes não são comparadas: entre fontes, decide a AD.

Leitura de uma entrada da tabela

Código (C conectada, L local /32, S estática, O OSPF, S* candidata a default), prefixo, [AD/métrica], via próximo salto, idade da rota e interface de saída. Em O 10.20.0.0/16 [110/20] via 10.1.1.2, 00:12:44, Gi0/1, 110 é a AD e 20 o custo. Cada interface ativa com IPv4 instala a C da sub-rede (AD 0, que nenhuma estática vence) e a L /32 do próprio endereço.

Rota default e gateway of last resort

ip route 0.0.0.0 0.0.0.0 próximo-salto (IPv6: ipv6 route ::/0 próximo-salto) casa com qualquer destino e só é usada sem rota mais longa. Aparece como S* e na linha Gateway of last resort. Sem rota e sem default, o pacote é descartado e pode voltar ICMP inalcançável.

Rota de host

Máscara 255.255.255.255 (/32) no IPv4 e /128 no IPv6: é o prefixo mais longo possível e sempre vence a rota de rede que contém o endereço. Com máscara /24 a entrada vira rota de rede.

Estática flutuante

Reserva com AD maior que a da rota principal e menor que 255; atrás do OSPF precisa passar de 110 (ex.: 130). Ela fica na configuração mas só aparece na tabela quando a principal some. AD menor que 110 (ex.: 90, 100 ou 5) faz a estática vencer sempre.

Estática por interface, por próximo salto e recursiva

Só com interface de saída aparece como S ... is directly connected e, em Ethernet, depende de proxy ARP; a forma totalmente especificada é ip route rede máscara interface próximo-salto. Próximo salto remoto é resolvido recursivamente pela tabela. Estática some da tabela (mas fica na config) quando o próximo salto fica inalcançável.

Estáticas IPv6

Exigem ipv6 unicast-routing e a sintaxe ipv6 route prefixo/tamanho próximo-salto. Com próximo salto link-local (FE80::), informe também a interface de saída, pois o link-local se repete em vários enlaces. Cuidado com prefixo digitado: 2001:DB8:3:: e 2001:DB8:30:: são redes diferentes.

Sumarização em rota estática

Quatro /24 contíguas começando em múltiplo de 4 no terceiro octeto cabem numa /22 (255.255.252.0): 10.20.0.0 a 10.20.3.0 ou 172.16.8.0 a 172.16.11.0. /21 incluiria redes extras e /24 cobre só a primeira.

Router ID do OSPF

Número de 32 bits escolhido nesta ordem: comando router-id, maior IP de loopback ativa, maior IP de interface física ativa. Loopback ou router-id dão estabilidade. Deve ser único no domínio; no IOS XE 17.13.1a ou posterior a troca vale na hora (antes exigia clear ip ospf process ou recarga).

Requisitos de vizinhança OSPF

Precisam coincidir: área, hello e dead, sub-rede e máscara (em broadcast) e autenticação; para chegar a FULL, MTU compatível. Custo e prioridade podem ser diferentes e o router ID tem de ser diferente. MTU diferente prende em EXSTART/EXCHANGE.

Eleição de DR e BDR

Em redes broadcast vence a maior prioridade de interface (0 a 255, padrão 1) e, no empate, o maior router ID; prioridade 0 tira o roteador da disputa. A eleição não é preemptiva: um roteador novo com prioridade maior não toma o lugar do DR ativo. Entre DROTHERs o estado normal é 2WAY; FULL só com DR e BDR.

OSPF point-to-point

ip ospf network point-to-point em enlace Ethernet com dois roteadores elimina a eleição de DR/BDR e leva os vizinhos direto a FULL; os dois lados devem usar o mesmo tipo. Temporizadores continuam 10/40 e o custo continua pela largura de banda.

Custo OSPF e reference bandwidth

Custo = referência / largura de banda, com referência padrão de 100 Mb/s; por isso 1 Gb/s e 10 Gb/s ficam com custo 1. Ajuste auto-cost reference-bandwidth com o mesmo valor em todos os roteadores.

Comandos de OSPFv2

network endereço wildcard area X (no modo router) ou ip ospf 1 area 0 na interface. passive-interface anuncia a rede sem enviar hellos (LAN só com hosts, F/C 0/0). default-information originate injeta a default no OSPF, vista como externa (O*E2).

OSPFv3

Exige ipv6 unicast-routing e ipv6 ospf processo area área em cada interface, sem comando network. Router ID continua de 32 bits: sem IPv4, configure router-id. Vizinhos e próximos saltos aparecem em link-local (FE80::) com a interface de saída.

HSRP

Hosts usam o IP virtual como gateway; o Active responde ao ARP com o MAC virtual e encaminha, o Standby monitora e assume. Padrões: hello 3 s, hold 10 s, prioridade 100 e preempção desabilitada. standby track reduz a prioridade (decremento padrão 10) quando o uplink cai. HSRPv2: hellos para 224.0.0.102, TLV e obrigatório para IPv6.

VRRP

O Master encaminha o tráfego do IP virtual e os Backups aguardam. A preempção vem habilitada por padrão. O dono do endereço virtual (IP real igual ao virtual) tem prioridade 255 e é sempre Master quando ativo.

Macetes para memorizar

Decisão de rota

Prefixo, depois AD, depois métrica: o maior prefixo é o chefe.

Tabela de AD

0 conectada, 1 estática, 20 eBGP, 110 OSPF, 115 IS-IS, 120 RIP, 200 iBGP.

Router ID

Manual, depois loopback maior, depois física maior.

Vizinhança OSPF

Área, hello/dead e máscara iguais; MTU igual para FULL; RID sempre diferente.

Preempção dos FHRP

HSRP Hesita (sem preempt), VRRP Volta (preempt ligado).

MAC virtual

ac é HSRPv1, 9f é HSRPv2, 5e é VRRP.

Temporizadores

HSRP 3/10, OSPF Ethernet 10/40, NBMA 30/120.

Tabela de memorização: não confunda

Quando é...	...e quando é
Prefixo mais longo Destinos cobertos por prefixos diferentes: a /25 vence a /24 e a /16, mesmo com AD maior.	**Distância administrativa** Mesmo prefixo vindo de fontes diferentes: conectada 0 > estática 1 > OSPF 110.
HSRP Active/Standby, prioridade 100, sem preempção por padrão, MAC 0000.0c07.acXX (v1) ou 0000.0c9f.fXXX (v2).	**VRRP** Master/Backup, preempção habilitada por padrão, owner com prioridade 255, MAC 0000.5e00.01XX.
Estática sem AD (ou AD menor que 110) Deve substituir a rota OSPF imediatamente.	**Estática flutuante (AD entre 111 e 254)** Deve ser reserva e só entrar quando a rota OSPF sumir.
OSPF broadcast Segmento multiacesso com vários roteadores: elege DR e BDR, DROTHERs ficam em 2WAY.	**OSPF point-to-point** Enlace Ethernet só com dois roteadores: sem DR/BDR e adjacência direto em FULL.
OSPFv2 IPv4: network com wildcard ou ip ospf 1 area 0 na interface.	**OSPFv3** IPv6: ipv6 unicast-routing + ipv6 ospf 1 area 0 na interface; router-id manual sem IPv4; próximos saltos link-local.
ip ospf priority 0 Roteador nunca deve ser DR/BDR, mas continua enviando hellos e formando vizinhança.	**passive-interface** LAN só de hosts: continua anunciada sem enviar hellos nem formar vizinhança.

Próximo salto IPv6 global ipv6 route ::/0 2001:DB8:FFFF::1 basta (pode ser recursiva).	**Próximo salto IPv6 link-local** ipv6 route ::/0 GigabitEthernet0/0/0 FE80::1: a interface é obrigatória.

Números que caem

Item	Valor
AD conectada / estática / eBGP / OSPF / IS-IS / RIP / iBGP	**0 / 1 / 20 / 110 / 115 / 120 / 200**
AD que nunca é instalada	**255**
OSPF em Ethernet: prioridade, hello, dead	**1, 10 s, 40 s**
Temporizadores OSPF em NBMA	**30 s / 120 s**
Faixa de prioridade OSPF	**0 a 255**
Reference bandwidth padrão do OSPF	**100 Mb/s**
HSRP: hello, hold, prioridade	**3 s, 10 s, 100 (preempção desabilitada)**
Decremento padrão do standby track	**10**
Prioridade do owner no VRRP	**255**
Multicast dos hellos do HSRPv2	**224.0.0.102**
Tamanho do router ID (OSPFv2 e OSPFv3)	**32 bits**

Alertas de prova (pegadinhas)

⚠ **Alerta de prova:** Escolher a rota de menor AD mesmo quando outra tem prefixo mais longo.
Como não cair: AD só desempata o mesmo prefixo; a /24 estática com AD 200 vence a /16 do OSPF para destinos dentro dela.

⚠ **Alerta de prova:** Criar a flutuante atrás do OSPF com AD 90 ou 100.
Como não cair: Qualquer AD menor que 110 vence o OSPF o tempo todo; use valor acima de 110 e abaixo de 255.

⚠ **Alerta de prova:** Usar AD 255 para deixar a rota bem guardada como reserva.
Como não cair: AD 255 nunca é instalada, nem como reserva.

⚠ **Alerta de prova:** Fazer exceção para um servidor com ip route 10.9.9.50 255.255.255.0.
Como não cair: Com /24 a entrada vale para a rede inteira; rota de host usa 255.255.255.255 (ou /128 no IPv6).

⚠ **Alerta de prova:** Configurar ip default-gateway no roteador ou rota com máscara 255.255.255.255 como default.
Como não cair: ip default-gateway é para equipamento sem roteamento IP; default é 0.0.0.0 0.0.0.0.

⚠ **Alerta de prova:** Usar ::/128 ou FE80::/10 como rota default IPv6.
Como não cair: ::/128 é o endereço não especificado e FE80::/10 é link-local; default é ::/0.

⚠ **Alerta de prova:** Criar ipv6 route ::/0 FE80::1 sem a interface.
Como não cair: Link-local se repete em todo enlace; informe interface de saída e endereço.

⚠ **Alerta de prova:** Ler [110/20] como custo 110 e AD 20, ou como 20 saltos.
Como não cair: É sempre [AD/métrica], e a métrica do OSPF é custo, não saltos.

⚠ **Alerta de prova:** Dar o DR ao menor router ID ou achar que um roteador novo com prioridade 200 vira DR na hora.
Como não cair: Vence o maior router ID no empate, e a eleição não é preemptiva.

⚠ **Alerta de prova:** Tratar 2WAY/DROTHER como falha ou culpar MTU por ele.
Como não cair: 2WAY entre DROTHERs é normal; MTU prende em EXSTART/EXCHANGE.

⚠ **Alerta de prova:** Colocar preempt no roteador que já é ativo para o outro retomar, ou achar que o VRRP precisa de vrrp preempt.
Como não cair: No HSRP o preempt vai no roteador de maior prioridade que quer retomar; no VRRP a preempção já vem ligada.

⚠ **Alerta de prova:** Ler o MAC 0000.5e00.0103 como VRRP grupo 103.
Como não cair: O prefixo é 0000.5e00.01; só os dois últimos dígitos (03) são o VRID.

⚠ **Alerta de prova:** Marcar 3 s e 10 s como hello/dead do OSPF ou 30/120 como padrão em Ethernet.
Como não cair: 3/10 são hello/hold do HSRP; 30/120 é NBMA; OSPF em Ethernet usa 10/40.

⚠ **Alerta de prova:** Usar network com prefixo IPv6 no OSPFv3 ou ip ospf 1 area 0 para IPv6.
Como não cair: OSPFv3 é habilitado com ipv6 ospf 1 area 0 na interface; ip ospf é OSPFv2.

Como cai na prova

📝 **Como cai:** Trecho de show ip route ou show ipv6 route e um destino; pergunta por qual próximo salto ou interface o pacote sai.
Como resolver: Liste as entradas que contêm o destino, fique com a de prefixo mais longo e só então use AD e métrica; sem nenhuma, vá para a default ou descarte.

📝 **Como cai:** Rota principal aprendida por OSPF e pedido de rota reserva ou de exceção para um host.
Como resolver: Reserva: mesma rede com AD acima de 110. Exceção: rota /32 (ou /128). Confira máscara e sintaxe antes de olhar o próximo salto.

📝 **Como cai:** Dois roteadores sem vizinhança OSPF com saídas de show ip ospf interface.
Como resolver: Compare área, hello/dead, máscara, tipo de rede e MTU; ignore custo, prioridade e router ID (que só precisa ser diferente).

📝 **Como cai:** Segmento com vários roteadores e prioridades/router IDs; pede DR e BDR ou avalia estados em show ip ospf neighbor.
Como resolver: Maior prioridade, empate pelo maior router ID, prioridade 0 fora, sem preempção; DROTHER-DROTHER = 2WAY normal.

📝 **Como cai:** Saída de show standby ou show vrrp brief e pergunta sobre quem encaminha ou o que acontece quando o ativo volta.
Como resolver: Quem encaminha é o Active/Master; para retomar, o roteador que volta precisa de prioridade maior e preempt (no VRRP já vem ligado; owner 255 sempre Master).

Gatilhos do enunciado

Se o enunciado trouxer...	Pense em
Várias rotas contendo o destino com prefixos diferentes	**Prefixo mais longo vence; AD e métrica não entram.**
Mesmo prefixo por estática e OSPF	**Menor AD: estática 1 vence OSPF 110, salvo AD configurada maior.**
Rota de reserva usada só se a principal sumir	**Estática flutuante com AD maior que a da principal.**
S 10.30.0.0/16 is directly connected sem rede conectada	**Estática configurada só com interface de saída.**
Dois próximos saltos com a mesma métrica para o mesmo prefixo	**Balanceamento por caminhos de custo igual.**
Vizinho preso em EXSTART/EXCHANGE	**MTU diferente nas interfaces.**

Sem adjacência com área, hello/dead ou máscara diferentes	**Igualar o parâmetro divergente nos dois lados.**
1 Gb/s e 10 Gb/s com custo 1	**auto-cost reference-bandwidth igual em todos os roteadores.**
Roteador só com IPv6 não inicia o OSPFv3	**Configurar router-id de 32 bits.**
Roteadores internos não aprendem a default do roteador de borda	**default-information originate no processo OSPF.**
Ativo antigo volta com prioridade maior e não retoma no HSRP	**Falta standby X preempt nele.**
Standby deve assumir quando cai o uplink do ativo	**standby track da interface com decrement + preempt no outro.**
MAC do gateway 0000.0c07.acXX, 0000.0c9f.fXXX ou 0000.5e00.01XX	**HSRPv1, HSRPv2 ou VRRP, com o grupo nos dígitos finais.**
Ping de ida ok mas sem resposta; roteador remoto perdeu uma rota	**Falta a rota de volta: conectividade exige rotas nos dois sentidos.**

🎯 **Se você lembrar de só uma coisa deste capítulo...**

- Prefixo mais longo primeiro; AD só desempata o mesmo prefixo; métrica só dentro do mesmo protocolo.
- Flutuante atrás do OSPF: AD acima de 110 e abaixo de 255; ela só aparece na tabela quando a principal some.
- Próximo salto IPv6 link-local exige a interface de saída na rota estática.
- EXSTART/EXCHANGE = MTU; 2WAY entre DROTHERs = normal; DR não é preemptivo.
- HSRP sem preempt por padrão; VRRP com preempt por padrão.

Essenciais para a prova (checklist)

- ☐ Sei escolher a rota de qualquer destino numa tabela IPv4 ou IPv6.
- ☐ Sei ler código, [AD/métrica], via, idade e interface de uma entrada.
- ☐ Sei configurar default, rota de rede, rota de host e flutuante em IPv4 e IPv6.
- ☐ Sei resumir quatro /24 contíguas numa /22.
- ☐ Sei os critérios do router ID e por que usar loopback ou router-id.
- ☐ Sei listar o que precisa coincidir para a vizinhança OSPF e o sintoma de cada falha.
- ☐ Sei eleger DR/BDR e explicar o efeito de priority 0, point-to-point e passive-interface.
- ☐ Sei habilitar OSPFv3 por interface e explicar o próximo salto em link-local.
- ☐ Sei interpretar show standby e show vrrp brief, preempt, track e MACs virtuais.

Questões de revisão do capítulo

R3.1 · 3.0 Roteamento IP

Um roteador novo, só com endereços IPv6 e nenhum IPv4 configurado, não inicia o processo ipv6 router ospf 1 do OSPFv3. Qual é a correção necessária?

A. Configurar um endereço link-local manual na loopback
B. Habilitar ip routing além de ipv6 unicast-routing
C. Configurar router-id 1.1.1.1 no processo do OSPFv3
D. Usar o comando network com o prefixo IPv6 da LAN

R3.2 · 3.0 Roteamento IP

Na VLAN de servidores há três roteadores OSPF. O roteador R3 tem pouca CPU e a equipe quer garantir que ele nunca seja eleito DR nem BDR nesse segmento, sem mexer nos outros. O que configurar na interface do R3?

A. ip ospf priority 255
B. ip ospf priority 0
C. ip ospf cost 0
D. ip ospf network broadcast

R3.3 · 3.0 Roteamento IP

O roteador de uma pequena filial tem apenas a LAN e um enlace com o provedor, cujo próximo salto é 203.0.113.1. Não há protocolo de roteamento. Qual comando dá à filial acesso a todas as redes externas?

A. ip route 0.0.0.0 0.0.0.0 203.0.113.1 255
B. ip default-gateway 203.0.113.1
C. ip route 0.0.0.0 255.255.255.255 203.0.113.1
D. ip route 0.0.0.0 0.0.0.0 203.0.113.1

R3.4 · 3.0 Roteamento IP

R1 e R2 compartilham a sub-rede 10.0.12.0/30, mas não formam adjacência OSPF. A saída de show ip ospf interface Gi0/0 mostra no R1: Internet Address 10.0.12.1/30, Area 0; no R2: Internet Address 10.0.12.2/30, Area 1. Temporizadores e MTU estão iguais. Qual é a correção?

A. Configurar ip ospf priority 0 no R2
B. Mudar a máscara das duas interfaces para /24
C. Trocar o tipo de rede para point-to-point
D. Colocar as duas interfaces na mesma área

Respostas comentadas

R3.1. C) Configurar router-id 1.1.1.1 no processo do OSPFv3

Por quê: No OSPFv3, router ID, área e IDs de LSA permanecem com 32 bits. Em roteadores sem IPv4, defina o router ID com o comando router-id.

✗ A) Incorreta. Link-local manual não fornece o router ID de 32 bits.
✗ B) Incorreta. ip routing trata do IPv4 e não fornece router ID.
✗ D) Incorreta. O OSPFv3 é habilitado por interface, não com network.

> **Dica de prova:** OSPFv3 sem IPv4: configure router-id manualmente.

R3.2. B) ip ospf priority 0

Por quê: A prioridade OSPF vai de 0 a 255 (padrão 1). O maior valor vence a eleição; 0 tira o roteador da disputa.

✗ A) Incorreta. 255 é a maior prioridade e aumentaria a chance de o R3 ser DR.
✗ C) Incorreta. O custo afeta a escolha de caminhos e não a eleição.
✗ D) Incorreta. broadcast é o tipo padrão em Ethernet e mantém a eleição.

> **Dica de prova:** Nunca DR/BDR: ip ospf priority 0.

R3.3. D) ip route 0.0.0.0 0.0.0.0 203.0.113.1

Por quê: Em roteadores stub, uma única rota default estática aponta para o provedor. O prefixo 0.0.0.0/0 casa com qualquer destino e só é usado na falta de rota mais longa.

✗ A) Incorreta. Com distância administrativa 255 a rota nunca é instalada.
✗ B) Incorreta. ip default-gateway só é usado quando o roteamento IP está desabilitado, como em switches de camada 2.
✗ C) Incorreta. A máscara 255.255.255.255 cria uma rota de host para 0.0.0.0, e não uma default.

> **Dica de prova:** Stub com um provedor: ip route 0.0.0.0 0.0.0.0 próximo-salto.

R3.4. D) Colocar as duas interfaces na mesma área

Por quê: O ID de área faz parte do hello. Em um mesmo enlace, as interfaces devem estar na mesma área para que os roteadores formem adjacência.

✗ A) Incorreta. Prioridade afeta só a eleição de DR/BDR.
✗ B) Incorreta. As máscaras já coincidem; o problema é a área.
✗ C) Incorreta. O tipo de rede não resolve a diferença de área.

> **Dica de prova:** Sem adjacência e áreas diferentes no enlace: alinhe a área.

04

CAPÍTULO 4 · 20% DA PROVA

4.0 Serviços de Rede e Segurança

Aqui eu preciso configurar acesso administrativo seguro (usuários locais com secret, SSH, AAA com TACACS+ e RADIUS), transferir arquivos com SCP e SFTP, configurar NAT e PAT no IOS XE, diagnosticar registros DNS, descrever VPNs IPsec, escrever e posicionar ACLs IPv4 e aplicar a segurança de camada 2 (DHCP snooping, DAI, storm control, RA guard e port security). A prova cobra muito comando exato, a ordem dos argumentos e a interface/direção certas. Onde mais erro: os termos inside local x inside global, a ordem da lista de métodos AAA, onde aplicar ACL padrão x estendida, o deny implícito e a diferença entre os modos de violação do port security.

Neste capítulo

18 tópicos-chave · 14 pegadinhas · 8 macetes · 14 gatilhos · 4 questões comentadas

Tópicos-chave

Credenciais locais

Use username ... secret e enable secret, que gravam hash forte (tipos 8 ou 9); password fica em texto claro e o service password-encryption gera tipo 7, reversível. Com as duas linhas, enable secret prevalece. privilege 15 leva o usuário direto ao EXEC privilegiado; o nível 1 é o EXEC de usuário.

SSH nas linhas vty

Pré-requisitos: hostname, ip domain name, crypto key generate rsa e username ... secret. Nas vty: login local e transport input ssh. Para limitar quem abre SSH, aplique ACL padrão com access-class N in em line vty.

AAA e lista de métodos

Tudo começa com aaa new-model. A lista (ex.: aaa authentication login default group tacacs+ local) é consultada na ordem escrita; o próximo método só é usado se o anterior retornar erro (servidor inacessível), nunca quando a senha é rejeitada. A conta local é a reserva para indisponibilidade.

Definição de servidores AAA

radius server NOME com address ipv4 IP auth-port 1812 acct-port 1813 e key; tacacs server NOME com address ipv4 e key. aaa group server tacacs+ GRUPO com server name agrupa servidores já definidos para a lista de métodos.

TACACS+ x RADIUS

TACACS+: TCP 49, corpo inteiro protegido e funções de AAA separadas, permitindo autorizar e contabilizar comando por comando. RADIUS: UDP 1812/1813, só a senha ocultada no Access-Request e autenticação com autorização combinadas no Access-Accept.

SCP e SFTP

SCP e SFTP usam SSH e cifram; TFTP não autentica nem cifra e FTP autentica sem cifrar. No copy o primeiro argumento é a origem e o segundo o destino (copy running-config scp://usuario@servidor/arquivo). Como servidor SCP o roteador precisa de SSH, chaves RSA, autenticação e autorização (AAA) e ip scp server enable.

Termos do NAT

Inside/outside dizem de que lado está o host; local/global, de que ponto de vista o endereço é visto. Inside local é o IP privado real do host interno e inside global o endereço traduzido; outside local e outside global iguais indicam destino não traduzido.

NAT estático, dinâmico e PAT

Estático: ip nat inside source static local global, um para um permanente (servidor publicado); com tcp local porta global porta publica só uma porta. Dinâmico sem overload: um IP do pool por host ativo. PAT: ip nat inside source list ACL interface X overload (ou pool ... overload), diferenciando sessões pela porta no inside global.

Diagnóstico de NAT

Interfaces precisam de ip nat inside (LAN) e ip nat outside (provedor); a ACL do NAT tem de casar com a rede interna. show ip nat statistics resume traduções e interfaces inside/outside; show ip nat translations detalha cada entrada; clear ip nat translation * remove as dinâmicas.

Registros DNS

A (nome para IPv4), AAAA (nome para IPv6), CNAME (apelido para outro nome, que precisa ter A/AAAA), MX (servidor de e-mail do domínio, menor preferência primeiro), NS (servidores autoritativos e delegação de subdomínio) e PTR (reverso, em in-addr.arpa com octetos invertidos). Após mudar registro, o cliente pode precisar esperar o TTL ou limpar o cache.

IPsec: AH, ESP e IKE

AH (protocolo IP 51) dá integridade e autenticação sem confidencialidade e não atravessa NAT; ESP (protocolo IP 50) cifra e também dá integridade. O IKE (IKEv2 em UDP 500, e UDP 4500 com NAT) autentica os pares e negocia SAs e chaves; quem protege os dados é o ESP.

Modos e tipos de VPN

Modo túnel encapsula o pacote IP original inteiro com novo cabeçalho entre gateways (usual em site a site); modo transporte protege a carga mantendo o cabeçalho original, entre os hosts finais. Site a site liga redes inteiras pelos roteadores; acesso remoto liga o notebook do usuário à rede.

Lógica das ACLs

Avaliação de cima para baixo: a primeira correspondência vence, por isso o específico vem antes do genérico. Toda ACL termina com deny implícito, então uma ACL de bloqueio pontual precisa de um permit no fim. ACL só filtra depois de aplicada a interface ou linha.

Numeração, wildcard e atalhos

Padrão: 1 a 99 e 1300 a 1999; estendida: 100 a 199 e 2000 a 2699. Wildcard = 255.255.255.255 menos a máscara (/28 = 0.0.0.15). host X = X 0.0.0.0; any = 0.0.0.0 255.255.255.255. Estendida: protocolo, origem, destino e eq porta (SSH TCP 22, Telnet TCP 23, HTTPS TCP 443).

Posicionamento e edição de ACLs

Estendida perto da origem; padrão (só olha a origem) perto do destino. in é o que entra no roteador pela interface; out, o que sai. Em ip access-list extended NOME, use número de sequência para inserir (15 permit ...) ou remover (no 20); remark documenta, log registra correspondências e echo-reply libera só respostas de ping.

DHCP snooping e DAI

Snooping exige ip dhcp snooping global + ip dhcp snooping vlan X; uplinks para o servidor legítimo ficam trust e portas de usuário untrusted, onde OFFER/ACK são descartados; ip dhcp snooping limit rate limita inundação (sem limite por padrão). O DAI usa os bindings do snooping para descartar ARPs inválidos em portas untrusted; uplinks entre switches que inspecionam ficam trust.

Storm control e RA guard

storm-control broadcast level 20 limita o broadcast recebido na porta (também multicast e unicast, em percentual, bps ou pps); por padrão descarta o excesso, com action trap ou action shutdown. RA guard (RFC 6105): política com device-role host nas portas de usuário descarta RAs; device-role router na porta do roteador legítimo, aplicada com ipv6 nd raguard attach-policy.

Port security

Modos de violação: protect (descarta em silêncio), restrict (descarta e registra em syslog e contador) e shutdown (padrão, err-disabled, mostrado como Secure-shutdown). mac-address sticky aprende o MAC e o grava na running-config, sobrevivendo ao reinício se salvo. Reativação: remover a causa e shutdown/no shutdown ou errdisable recovery.

Macetes para memorizar

💡 TACACS+ x RADIUS

TACACS+ é TCP, Tudo cifrado e Tarefas separadas; RADIUS é UDP 1812/1813 e esconde só a senha.

💡 Termos do NAT

Inside/outside = onde mora o host; local/global = de onde você olha.

💡 IPsec

ESP Esconde (cifra); AH só Autentica; IKE só negocia.

💡 Posição da ACL

Estendida perto da origem, padrão perto do destino (Estendida Embarca cedo, Padrão Para no fim).

💡 Faixas de ACL numerada

Padrão 1-99 e 1300-1999; estendida 100-199 e 2000-2699.

💡 Port security

Protect protege calado, Restrict reclama no log, Shutdown derruba (padrão).

💡 Registros DNS

A = IPv4, AAAA = IPv6, CNAME = apelido, MX = Mail, NS = quem manda na zona, PTR = Pra trás (reverso).

💡 Portas de serviços

SSH 22, Telnet 23, HTTPS 443, TACACS+ 49, RADIUS 1812/1813, IKE 500/4500.

Tabela de memorização: não confunda

Quando é...	...e quando é
TACACS+ Administração de dispositivos com autorização e registro comando por comando; TCP 49 e corpo todo protegido.	**RADIUS** Autenticação com UDP 1812/1813, autenticação e autorização juntas e só a senha ocultada (como no 802.1X do Wi-Fi).

AH Só integridade e autenticação, sem cifrar e sem atravessar NAT (protocolo IP 51).	**ESP** Precisa cifrar os dados ou passar por NAT encapsulado em UDP (protocolo IP 50).
Modo túnel VPN entre gateways (site a site): novo cabeçalho IP externo envolvendo o pacote inteiro.	**Modo transporte** Proteção entre os próprios hosts finais, mantendo o cabeçalho original.
ACL padrão Filtra só pela origem; aplicar perto do destino para não bloquear outros tráfegos.	**ACL estendida** Filtra protocolo, origem, destino e porta; aplicar perto da origem para descartar cedo.
access-class em line vty Restringir quem abre SSH/Telnet para o próprio equipamento.	**ip access-group em interface** Filtrar tráfego que atravessa a interface, na direção in ou out.
NAT estático Servidor interno publicado sempre no mesmo IP global (ou só uma porta, com tcp local porta global porta).	**PAT (overload)** Muitos hosts internos navegando com um ou poucos IPs públicos.
DHCP snooping Bloquear servidor DHCP falso e inundação de DHCP em portas untrusted.	**Dynamic ARP Inspection** Bloquear ARP falso (envenenamento do gateway), usando os bindings do snooping.

Números que caem

Item	Valor
TACACS+	**TCP 49**
RADIUS	**UDP 1812 (autenticação) e 1813 (accounting)**
IKE / IKE com NAT	**UDP 500 / UDP 4500**
ESP / AH	**protocolo IP 50 / protocolo IP 51**
ACL IP padrão numerada	**1 a 99 e 1300 a 1999**
ACL IP estendida numerada	**100 a 199 e 2000 a 2699**
Portas em ACL	**SSH TCP 22, Telnet TCP 23, HTTP TCP 80, HTTPS TCP 443**
Níveis de privilégio	**0 a 15 (1 = EXEC de usuário, 15 = EXEC privilegiado)**
Hash do secret	**tipos 8 ou 9 (tipo 7 é reversível)**

Alertas de prova (pegadinhas)

⚠ **Alerta de prova:** Achar que, com group radius local, errar a senha no RADIUS faz o switch tentar a conta local.
Como não cair: O próximo método só entra se o anterior retornar erro (servidor fora); rejeição de senha encerra a tentativa.

⚠ **Alerta de prova:** Escrever aaa authentication login default local group tacacs+ para usar o local só como reserva.
Como não cair: A ordem escrita é a ordem de consulta: o servidor vem primeiro e local por último.

⚠ **Alerta de prova:** Resolver senha em texto claro com service password-encryption ou senha mais longa.
Como não cair: Tipo 7 é reversível; recrie com username ... secret.

⚠ **Alerta de prova:** Atribuir ao RADIUS TCP 49, corpo todo cifrado ou AAA separados.
Como não cair: Essas são características do TACACS+; RADIUS é UDP 1812/1813 com só a senha protegida.

⚠ **Alerta de prova:** Usar copy flash: scp://... quando a ideia é trazer a imagem para a flash.
Como não cair: copy origem destino: para trazer é copy scp://usuario@servidor/arquivo flash:.

⚠ **Alerta de prova:** Usar ip nat outside source ou inside destination para a LAN navegar.
Como não cair: Saída de hosts internos é ip nat inside source list ... overload.

⚠ **Alerta de prova:** Esquecer overload no pool de dois IPs para 300 usuários.
Como não cair: Sem overload cada usuário ocupa um IP e só dois navegam ao mesmo tempo.

⚠ **Alerta de prova:** Chamar o IP privado do host de inside global ou o IP público de outside local.
Como não cair: Host interno: inside local (privado real) e inside global (traduzido).

⚠ **Alerta de prova:** Usar CNAME ou MX para resolução reversa e PTR para apelido.
Como não cair: Reverso é PTR em in-addr.arpa; apelido é CNAME; e-mail é MX; delegação é NS; IPv6 é AAAA.

⚠ **Alerta de prova:** Dizer que o AH cifra a carga ou que o IKE cifra os pacotes de dados.
Como não cair: Só o ESP cifra; o IKE negocia SAs e chaves.

⚠ **Alerta de prova:** Aplicar a ACL padrão na entrada da interface dos usuários.
Como não cair: ACL padrão perto da origem bloqueia tudo daquela origem, inclusive internet; coloque perto do destino.

⚠ **Alerta de prova:** Acrescentar a nova linha permit sem número numa ACL que termina com deny ip any any.
Como não cair: Sem número a entrada vai para o fim, depois do deny, e nunca casa; use número de sequência menor.

⚠ **Alerta de prova:** Marcar as portas dos usuários como trust no DHCP snooping ou no DAI.
Como não cair: Trust só nos uplinks para o servidor legítimo ou para switches que inspecionam; usuários ficam untrusted.

⚠ **Alerta de prova:** Escolher protect ou sticky para descartar e registrar sem derrubar a porta.
Como não cair: protect não registra; sticky é aprendizado de MAC; o modo que descarta e registra é restrict.

Como cai na prova

📝 **Como cai:** Bloco de configuração (AAA, SSH, servidor RADIUS/TACACS+) com um comando faltando ou errado.
Como resolver: Siga a ordem lógica: aaa new-model, servidores, grupo, lista de métodos; para SSH: hostname, domínio, RSA, usuário secret, login local e transport input ssh. Desconfie de comando no modo errado.

📝 **Como cai:** Saída de show ip nat translations ou cenário de navegação/publicação de servidor.
Como resolver: Identifique inside local x inside global; escolha estático para servidor fixo, tcp com porta para publicar um serviço e list + overload para muitos hosts. Confira inside/outside e a ACL.

📝 **Como cai:** ACL (ou saída de show access-lists) com comportamento inesperado.
Como resolver: Percorra de cima para baixo até a primeira correspondência, lembre do deny implícito, confira wildcard, protocolo/porta, interface e direção.

📝 **Como cai:** Sintoma de acesso por nome (site, e-mail, reverso, subdomínio, IPv6).
Como resolver: Mapeie a necessidade ao registro: A/AAAA, CNAME, MX, PTR ou NS.

📝 **Como cai:** Ataque ou falha de camada 2 (DHCP falso, ARP falso, tempestade, RA falso, switch na mesa).
Como resolver: Associe: servidor DHCP falso = snooping; ARP = DAI; broadcast = storm control; RA = RA guard; MACs a mais = port security. Confira trust no uplink e untrusted nos usuários.

📝 **Como cai:** Descrição de VPN IPsec pedindo protocolo, modo ou portas.
Como resolver: Cifrar = ESP; só autenticar = AH; negociar = IKE (UDP 500, 4500 com NAT); gateways = túnel; usuário com notebook = acesso remoto.

Gatilhos do enunciado

Se o enunciado trouxer...	Pense em
Comando aaa authentication não é aceito	**Falta aaa new-model.**
Autorizar e registrar cada comando dos administradores	**TACACS+.**
Backups de configuração não podem trafegar em claro e exigem autenticação	**SCP ou SFTP no lugar de TFTP/FTP.**
Muitos hosts e um único IP público na interface do provedor	**ip nat inside source list ACL interface X overload.**
Quinto usuário não navega com pool de quatro IPs	**NAT dinâmico sem overload (um IP por host).**
PAT configurado e nada é traduzido	**Marcação inside/outside e ACL do NAT casando com a rede interna.**
Nome aponta para servidor antigo no nslookup	**Atualizar o registro A (e esperar TTL ou limpar cache).**
Parceiros recusam e-mail porque o IP não volta o nome	**Registro PTR em in-addr.arpa.**
VPN com um dos lados atrás de NAT	**Liberar UDP 500 e UDP 4500; usar ESP (AH não passa por NAT).**
Após uma ACL de um deny, todos perdem acesso a tudo	**Deny implícito: falta permit no fim.**
Host que devia ser bloqueado continua acessando	**Permit genérico antes do deny específico: reordenar por número de sequência.**
Clientes sem IP logo após ligar DHCP snooping	**ip dhcp snooping trust no uplink do servidor legítimo.**
Respostas ARP falsas dizendo ser o gateway	**Dynamic ARP Inspection com DHCP snooping.**
Port Status: Secure-shutdown com contador de violação 1	**MAC excedente no port security; retirar o excesso e shutdown/no shutdown.**

🎯 Se você lembrar de só uma coisa deste capítulo...

- Lista AAA: método seguinte só com erro do anterior, nunca com senha rejeitada.
- Toda ACL tem deny implícito e para na primeira correspondência; padrão perto do destino, estendida perto da origem.
- PAT = inside source list ... overload; inside local é o IP privado real, inside global o traduzido.
- Só o ESP cifra; AH não atravessa NAT; IKE negocia em UDP 500/4500.
- Trust só nos uplinks (snooping e DAI); port security padrão é shutdown e restrict é o que registra sem derrubar.

Essenciais para a prova (checklist)

- ☐ Sei criar usuários com secret e privilege, preparar SSH e restringir vty com access-class.
- ☐ Sei montar aaa new-model, servidores RADIUS/TACACS+, grupos e listas de métodos na ordem correta.
- ☐ Sei diferenciar TACACS+ e RADIUS em portas, criptografia e separação de AAA.
- ☐ Sei escrever copy com SCP/SFTP nos dois sentidos e habilitar o roteador como servidor SCP.
- ☐ Sei configurar NAT estático, NAT de porta, NAT dinâmico e PAT e ler show ip nat translations/statistics.
- ☐ Sei escolher A, AAAA, CNAME, MX, NS e PTR para cada problema de nome.
- ☐ Sei explicar AH, ESP, IKE, modo túnel x transporte e site a site x acesso remoto.
- ☐ Sei escrever, posicionar, editar por sequência e documentar ACLs padrão e estendidas.
- ☐ Sei configurar DHCP snooping, DAI, storm control, RA guard e port security e seus estados.

Questões de revisão do capítulo

R4.1 · 4.0 Serviços de Rede e Segurança

Uma filial usa 192.168.10.0/24 na LAN e recebeu um único endereço público, configurado pelo provedor na interface GigabitEthernet0/0/1 do roteador IOS XE. As interfaces já estão marcadas como inside e outside, e a ACL 1 permite a rede interna. Qual comando permite que todos os hosts naveguem ao mesmo tempo usando esse único endereço?

A. ip nat inside destination list 1 interface GigabitEthernet0/0/1
B. ip nat outside source list 1 interface GigabitEthernet0/0/1 overload
C. ip nat inside source static 192.168.10.1 interface GigabitEthernet0/0/1
D. ip nat inside source list 1 interface GigabitEthernet0/0/1 overload

R4.2 · 4.0 Serviços de Rede e Segurança

O switch precisa enviar o arquivo de configuração salvo na flash para um servidor SFTP, usando um usuário do servidor. Qual comando, executado no switch, faz essa cópia segura?

A. copy sftp://usuario@10.0.0.50/config.txt flash:
B. copy running-config ftp://10.0.0.50/config.txt
C. copy flash:config.txt sftp://usuario@10.0.0.50/config.txt
D. copy flash:config.txt tftp://10.0.0.50/config.txt

R4.3 · 4.0 Serviços de Rede e Segurança

Um usuário ligou um roteador doméstico com IPv6 em uma porta de acesso e as estações da VLAN passaram a receber anúncios de roteador (RA) falsos. Qual configuração bloqueia RAs vindos das portas de usuários?

A. DHCP snooping com trust nas portas dos usuários
B. Política RA guard com device-role router nas portas
C. Política RA guard com device-role host nas portas
D. Dynamic ARP Inspection nas portas dos usuários

R4.4 · 4.0 Serviços de Rede e Segurança

O site intranet.empresa.com.br foi migrado do servidor 10.1.1.10 para 10.1.2.20. Usuários ainda chegam ao servidor antigo. Saída de nslookup intranet.empresa.com.br no cliente: Server dns1.empresa.com.br; Address 10.1.1.10. Qual é a correção?

A. Criar um registro MX apontando para 10.1.2.20 no DNS
B. Atualizar o registro A do nome para 10.1.2.20
C. Trocar o gateway padrão dos clientes
D. Criar um registro PTR para o nome intranet

Respostas comentadas

R4.1. D) ip nat inside source list 1 interface GigabitEthernet0/0/1 overload

Por quê: PAT, também chamado de NAT overload, permite que muitos endereços internos compartilhem um endereço global, usando números de porta para separar as sessões.

✗ A) Incorreta. inside destination trata de endereços de destino e não cria tradução de origem para os hosts navegarem.

✗ B) Incorreta. A tradução outside source altera endereços de origem de pacotes vindos de fora, o que não resolve a saída dos hosts internos.

✗ C) Incorreta. A tradução estática mapeia um único host interno, e não toda a rede.

> **Dica de prova:** Muitos hosts, um IP público: inside source list ... interface ... overload.

R4.2. C) copy flash:config.txt sftp://usuario@10.0.0.50/config.txt

Por quê: No IOS XE, o equipamento pode ser cliente SFTP: copy origem sftp://usuario@servidor/arquivo. SFTP e SCP usam SSH; TFTP e FTP não cifram.

✗ A) Incorreta. Copia do servidor para a flash, o sentido inverso.
✗ B) Incorreta. FTP não cifra a transferência.
✗ D) Incorreta. TFTP não cifra nem autentica.

> **Dica de prova:** Enviar arquivo com segurança: copy ... sftp://.

R4.3. C) Política RA guard com device-role host nas portas

Por quê: O RA guard (RFC 6105) cria uma política com o papel do dispositivo; ipv6 nd raguard attach-policy aplica a política às interfaces. Em portas de host, RAs são descartados.

✗ A) Incorreta. DHCP snooping trata de DHCPv4 e as portas de usuários não devem ser trust.
✗ B) Incorreta. device-role router permite RAs; seria usado só na porta do roteador legítimo.
✗ D) Incorreta. O DAI valida ARP do IPv4, não anúncios de roteador IPv6.

> **Dica de prova:** RA falso vindo de usuários: RA guard device-role host.

R4.4. B) Atualizar o registro A do nome para 10.1.2.20

Por quê: O registro A associa o nome ao IPv4. Após atualizá-lo, os clientes podem precisar esperar o TTL ou limpar o cache local (ipconfig /flushdns no Windows).

✗ A) Incorreta. MX é para e-mail.
✗ C) Incorreta. O problema é a resolução do nome, não o roteamento.
✗ D) Incorreta. PTR é para resolução reversa.

> **Dica de prova:** Nome aponta para IP antigo: atualize o registro A.

05

CAPÍTULO 5 · 10% DA PROVA

5.0 IA e Operações e Gerenciamento de Rede

Aqui eu preciso entender o papel da IA agêntica nas operações (planejar, agir com ferramentas, humano no circuito), escolher o melhor prompt para uma IA generativa considerando persona, instruções, contexto, formato de saída e classificação de dados, diferenciar as abordagens de gerenciamento (dispositivo, controlador, nuvem, automação e infraestrutura como código), conhecer SNMP, Ansible e o formato das mensagens de syslog. O peso é menor (10%) e o domínio cobra conceito direto e interpretação de mensagem de log. Onde mais erro: confundir ios_command com ios_config, trap com inform, a ordem dos campos de %FACILIDADE-SEVERIDADE-MNEMÔNICO e o sentido do logging trap (de 0 até o nível informado).

Neste capítulo

18 tópicos-chave · 14 pegadinhas · 7 macetes · 14 gatilhos · 4 questões comentadas

Tópicos-chave

IA agêntica

Opera em ciclo: decompõe um objetivo amplo em subtarefas, age por meio de ferramentas e APIs e ajusta o plano com o retorno do ambiente, sem um humano orquestrando cada passo. A IA generativa tradicional entrega uma resposta por prompt, e scripts fixos são a automação antiga sem raciocínio.

AgenticOps x AIOps

Segundo a Cisco, AgenticOps é um modelo operacional em que agentes raciocinam, diagnosticam e agem rapidamente, com humanos no circuito para validar, aprovar ou interromper. A AIOps tradicional gera mais alertas e painéis para a equipe analisar depois.

Humano no circuito

Mudanças com risco de indisponibilidade sugeridas por um agente só são aplicadas após aprovação humana. A confiança declarada pelo modelo não substitui a revisão, e registrar depois não evita o impacto.

Segurança de agentes

Agentes têm autoridade delegada: aplique privilégio mínimo, controle das ferramentas disponíveis, aprovação para ações de alto risco e registro das ações. Privilégio 15 em tudo, conta compartilhada ou logs desligados são as respostas erradas.

Validar a recomendação da IA

Agentes e assistentes podem errar (alucinação ou erro propagado). Confronte a sugestão com as saídas show antes de agir: no shutdown numa interface já up/up com vizinho OSPF em EXSTART deve ser rejeitado, e a investigação vai para a MTU.

Model Context Protocol (MCP)

Padroniza a integração do modelo com ferramentas e recursos (inventário, alarmes, tíquetes) no nível do protocolo, sem descrever cada ferramenta no texto de todo prompt, tornando a integração mais confiável.

Componentes do prompt

Persona (papel, tom e profundidade técnica), instruções claras com restrições (o que fazer e o que não fazer), contexto e dados do caso (saídas de comandos), formato de saída (tabela com colunas, só comandos) e classificação de dados. O melhor prompt combina tarefa específica, dados do caso e formato.

Classificação de dados no prompt

Antes de enviar a um assistente externo, remova ou mascare o que a política proíbe (senhas, chaves, IPs públicos, nomes internos). Pedir para apagar depois, mudar o formato do arquivo ou colar tudo para ficar mais preciso não resolve.

Abordagens de gerenciamento

Por dispositivo: CLI caixa a caixa, escala mal e favorece erros manuais. Por controlador: política definida uma vez num ponto central (ex.: Catalyst Center) e empurrada aos dispositivos. Em nuvem: painel web do fabricante e provisionamento remoto para centenas de sites sem TI local. Automação e IaC padronizam mudanças.

Northbound e southbound

Aplicações e automação falam com o controlador pela API northbound (ex.: Intent API REST do Catalyst Center, com HTTPS e JSON). O controlador fala com os dispositivos pelas interfaces southbound.

Infraestrutura como código

Configuração tratada como software: arquivos versionados em Git como fonte única da verdade, revisão antes de aplicar e aplicação automatizada. Declarativa descreve o estado final e a ferramenta converge para ele; imperativa executa a sequência de passos.

Componentes e operações do SNMP

O gerente (NMS) envia Get, GetBulk (grandes volumes) e Set (altera, ex.: sysContact); o agente no dispositivo responde com objetos da MIB local e envia notificações. Trap vai uma vez sem confirmação; Inform fica em memória até a resposta do gerente (mais confiável e mais custoso; o SNMPv1 não suporta).

Versões e segurança do SNMP

v1 e v2c usam comunidade em texto claro; community public RW é risco alto porque permite alterar a configuração. SNMPv3 tem noAuthNoPriv, authNoPriv (só autenticação) e authPriv (autenticação e criptografia). Se precisar de v2c: comunidade forte, RO e ACL.

Portas do SNMP

UDP 161 para consultas ao agente e UDP 162 para receptores de notificações (traps e informs). UDP 514 é do syslog.

Ansible

Sem agente: um nó de controle conecta por SSH (network_cli para IOS). O inventário (INI ou YAML) define hosts e grupos; o playbook é YAML com plays e tarefas. cisco.ios.ios_command executa comandos (show) e devolve a saída; cisco.ios.ios_config gerencia configuração com lines e parents.

Idempotência

Executar o mesmo playbook várias vezes dá o mesmo resultado: o ios_config compara com a running-config e só aplica o que difere, então a segunda execução informa que nada mudou. As linhas em lines devem estar escritas como aparecem na running-config.

Formato e severidades do syslog

seq no:timestamp: %FACILIDADE-SEVERIDADE-MNEMÔNICO: descrição. Em 000123: ... %SYS-5-CONFIG_I, 000123 é a sequência, SYS a facilidade, 5 a severidade e CONFIG_I o mnemônico. Níveis: 0 emergencies, 1 alerts, 2 critical, 3 errors, 4 warnings, 5 notifications, 6 informational, 7 debugging; menor número = mais grave.

Destinos de log e carimbo de tempo

Console, terminal (vty), buffer local (logging buffered, lido com show logging) e servidor syslog (logging host IP). logging trap N envia ao servidor as severidades de 0 até N; o padrão é informational (6). service timestamps log datetime msec põe data e hora com milissegundos; combine com NTP.

Macetes para memorizar

💡 Severidades do syslog

Do pior para o mais brando: 0 emergencies, 1 alerts, 2 critical, 3 errors, 4 warnings, 5 notifications, 6 informational, 7 debugging; número menor = mais grave.

💡 logging trap

Trap N é 'de zero até N': do mais grave até o limite.

Portas SNMP

161 pergunta, 162 avisa (um a mais para o aviso).

Operações SNMP

Get lê, Set muda, Trap grita uma vez, Inform grita até alguém responder.

Módulos Ansible

command coleta, config configura.

IA agêntica

Planeja, age, se adapta; e o humano aprova o que é arriscado.

Prompt bom

Quem (persona) + o quê (instrução e restrições) + com quais dados (mascarados) + como entregar (formato).

Tabela de memorização: não confunda

Quando é...	...e quando é
IA generativa tradicional Uma resposta de texto por prompt, com o humano orquestrando cada etapa.	**IA agêntica** Planeja subtarefas, usa ferramentas para agir e se adapta ao retorno.
cisco.ios.ios_command Coletar saída de show version, show ip interface brief, sem alterar nada.	**cisco.ios.ios_config** Garantir linhas de configuração (lines + parents), de forma idempotente.
Trap Notificação enviada uma vez, sem confirmação.	**Inform** Notificação reenviada até o gerente confirmar; não existe no SNMPv1.
Automação imperativa Scripts e playbooks que executam passo a passo os comandos.	**IaC declarativa** Arquivos versionados com o estado final desejado e ferramenta que converge para ele.
Gerenciamento por controlador Controlador on-premises (Catalyst Center, controlador sem fio) com visão consolidada do campus.	**Gerenciamento em nuvem** Muitas filiais sem TI local, instalação automática e painel web hospedado pelo fabricante.
Persona no prompt Quer rigor e linguagem de especialista (Aja como engenheiro de roteamento sênior).	**Formato de saída no prompt** Quer resposta pronta para uso (tabela com colunas porta, estado e erros; só comandos).
logging host Define para qual servidor syslog as mensagens vão.	**logging trap** Define até qual severidade é enviada ao servidor (0 até N).

Números que caem

Item	Valor
SNMP consultas / notificações	**UDP 161 / UDP 162**
Syslog	**UDP 514**
Severidades do syslog	**0 emergencies, 1 alerts, 2 critical, 3 errors, 4 warnings, 5 notifications, 6 informational, 7 debugging**
Nível padrão de logging trap para servidores syslog	**6 (informational)**
Níveis de segurança do SNMPv3	**noAuthNoPriv, authNoPriv, authPriv**

Alertas de prova (pegadinhas)

⚠ **Alerta de prova:** Permitir a mudança crítica porque o agente declarou confiança alta, ou deixar aplicar e registrar depois.
Como não cair: Ação de alto risco exige aprovação humana antes; confiança do modelo não substitui revisão.

⚠ **Alerta de prova:** Dar privilégio 15 em tudo ou usar a conta dos engenheiros para o agente.
Como não cair: Privilégio mínimo, ferramentas controladas e logs que identifiquem cada ação.

⚠ **Alerta de prova:** Aplicar a recomendação do agente porque ele identificou o alarme.
Como não cair: Se as saídas show contradizem a sugestão, rejeite e investigue a evidência.

⚠ **Alerta de prova:** Colar a configuração completa para a IA ser mais precisa e pedir para apagar depois.
Como não cair: Mascare senhas, chaves e dados restritos antes de enviar; depois não adianta.

⚠ **Alerta de prova:** Escolher a persona quando o objetivo é receber em formato de planilha.
Como não cair: Persona muda tom; quem garante o resultado utilizável é o formato de saída explícito.

⚠ **Alerta de prova:** Usar ios_command com configure terminal ou show running-config para mudar configuração.
Como não cair: ios_command coleta saída; mudança é ios_config com lines e parents.

⚠ **Alerta de prova:** Achar que o Ansible instala um agente leve ou usa SNMP com escrita.
Como não cair: Ansible é sem agente e usa SSH (CLI) a partir de um nó de controle.

⚠ **Alerta de prova:** Ler a segunda execução sem mudanças como falha de SSH.
Como não cair: Sem mudanças com sucesso é idempotência; falha apareceria como erro.

⚠ **Alerta de prova:** Achar que logging trap warnings envia só o nível 4 ou de 4 a 7.
Como não cair: Envia de 0 até 4 (igual ou mais grave); números maiores são menos graves.

⚠ **Alerta de prova:** Em %SYS-5-CONFIG_I, chamar 000123 de prioridade ou trocar facilidade e severidade.
Como não cair: 000123 é sequência; o texto é a facilidade e o número a severidade.

⚠ **Alerta de prova:** Confiar que SNMPv2c cifra a comunidade ou que RW é só leitura.
Como não cair: v1/v2c mandam a comunidade em claro e RW permite escrita; use SNMPv3 authPriv.

⚠ **Alerta de prova:** Liberar TCP 161/162, inverter as portas ou usar 514 para consultas.
Como não cair: SNMP é UDP: 161 consultas, 162 notificações; 514 é syslog.

⚠ **Alerta de prova:** Usar logging buffered ou logging console com IP, ou snmp-server host para mandar logs ao servidor.
Como não cair: Envio ao servidor syslog é logging host IP.

⚠ **Alerta de prova:** Usar ntp server para pôr milissegundos nas mensagens.
Como não cair: NTP sincroniza o relógio; o carimbo nas mensagens vem de service timestamps log datetime msec.

Como cai na prova

📝 **Como cai:** Lista de quatro prompts e pede o que melhor aplica persona, dados, instruções e formato.
Como resolver: Elimine os que pedem teoria, são vagos ou enviam dados sensíveis; fique com o que traz os dados do caso mascarados, tarefa específica, restrições e formato.

📝 **Como cai:** Cenário de agente de IA propondo ou executando uma ação.
Como resolver: Verifique risco e evidência: alto risco = aprovação humana; recomendação contradita pelas saídas show = rejeitar; acesso do agente = privilégio mínimo e logs.

📝 **Como cai:** Descrição de como uma empresa gerencia a rede e pede a classificação.
Como resolver: CLI caixa a caixa = dispositivo; ponto central on-premises = controlador; painel do fabricante para muitas filiais = nuvem; passos scriptados = imperativa; estado desejado versionado = IaC declarativa.

📝 **Como cai:** Mensagem de syslog do IOS pedindo facilidade, severidade ou o que é enviado com logging trap.
Como resolver: Quebre %FACILIDADE-SEVERIDADE-MNEMÔNICO, traduza o número pela tabela 0 a 7 e lembre que trap N envia de 0 até N.

📝 **Como cai:** Necessidade de automação com Ansible (coletar, configurar, onde definir hosts, por que não precisa de software no switch).
Como resolver: Coletar = ios_command; configurar = ios_config (lines, parents); hosts = inventário; playbook = YAML; sem agente, via SSH.

Gatilhos do enunciado

Se o enunciado trouxer...	Pense em
Agente vai acessar switches para coletar dados e propor correções	**Privilégio mínimo e registro das ações.**
Agente propõe mudança com risco de indisponibilidade	**Aprovação humana antes de aplicar.**
Agente precisa consultar inventário, alarmes e abrir tíquetes de forma padronizada	**Model Context Protocol (MCP).**
Divide objetivo em subtarefas e usa ferramentas	**Característica da IA agêntica.**
Política classifica senhas, chaves e IPs públicos como restritos	**Mascarar os dados antes de montar o prompt.**
Definir políticas uma vez e aplicar a centenas de switches e APs a partir de um ponto central	**Gerenciamento baseado em controlador.**
300 lojas sem TI com painel web do fabricante	**Gerenciamento em nuvem.**
Estado final em arquivos no Git, revisados e aplicados por ferramenta	**IaC declarativa.**
Aplicação conversa com o Catalyst Center por REST/JSON	**API northbound (Intent API).**
NMS perde alertas e quer reenvio até confirmação	**SNMP inform.**
Autenticação e criptografia no monitoramento SNMP	**SNMPv3 authPriv.**
Indicar quais roteadores o Ansible gerencia, agrupados por local	**Inventário do Ansible.**

Correlacionar logs com milissegundos	**service timestamps log datetime msec + NTP.**
Mensagem %LINEPROTO-5-UPDOWN ou %LINK-3-UPDOWN	**Facilidade-severidade-mnemônico: 5 notifications, 3 errors.**

🎯 **Se você lembrar de só uma coisa deste capítulo...**

- Ação de alto risco proposta por agente só com aprovação humana; recomendação de IA se confere com show antes de aplicar.
- Prompt: mascarar dados restritos antes de enviar; formato define resposta utilizável, persona define tom.
- ios_command coleta, ios_config configura (idempotente); Ansible é sem agente via SSH, inventário define hosts, playbook é YAML.
- SNMP: UDP 161/162, inform tem confirmação, v3 authPriv cifra; v2c manda comunidade em claro.
- Syslog: %FACILIDADE-SEVERIDADE-MNEMÔNICO, 0 é o mais grave, logging trap N envia 0 até N.

Essenciais para a prova (checklist)

☐ Sei diferenciar IA agêntica, IA generativa tradicional e scripts fixos, e AgenticOps de AIOps.

☐ Sei os controles para agentes: privilégio mínimo, aprovação humana, registro e validação das recomendações.

☐ Sei para que serve o MCP.

☐ Sei escolher o melhor prompt pelos componentes persona, instruções, dados classificados e formato.

☐ Sei classificar gerenciamento por dispositivo, controlador, nuvem, automação imperativa e IaC declarativa, e northbound x southbound.

☐ Sei gerente, agente, MIB, Get, GetBulk, Set, Trap, Inform, versões e portas do SNMP.

☐ Sei montar inventário e playbook Ansible e escolher ios_command ou ios_config.

☐ Sei decodificar uma mensagem de syslog e configurar logging host, trap, buffered e timestamps.

Questões de revisão do capítulo

R5.1 · 5.0 IA e Operações e Gerenciamento de Rede

Um playbook Ansible precisa coletar a saída de show version e show ip interface brief de vários roteadores IOS XE, sem alterar nenhuma configuração. Qual módulo é o indicado?

A. cisco.ios.ios_command
B. ansible.builtin.copy
C. cisco.ios.ios_facts_set
D. cisco.ios.ios_config

R5.2 · 5.0 IA e Operações e Gerenciamento de Rede

Uma empresa quer definir políticas de rede uma única vez e aplicá-las a centenas de switches e APs do campus a partir de um ponto central, com visão consolidada da rede, usando Catalyst Center e um controlador sem fio. Qual abordagem de gerenciamento é essa?

A. Baseada em dispositivo
B. Baseada em syslog central
C. Baseada em controlador
D. Baseada em console local

R5.3 · 5.0 IA e Operações e Gerenciamento de Rede

O switch tem logging host 10.0.0.99 e o administrador configurou logging trap warnings. Quais severidades passam a ser enviadas ao servidor syslog?

A. Da 0 (emergencies) até a 4 (warnings)
B. Somente a 4 (warnings)
C. Da 4 (warnings) até a 7 (debugging), as menos graves
D. Da 0 até a 6, pois esse é o padrão

R5.4 · 5.0 IA e Operações e Gerenciamento de Rede

Um engenheiro está montando a automação com Ansible e precisa indicar quais roteadores e switches serão gerenciados, agrupando-os por local, como filiais e matriz. Onde essa informação é definida?

A. No módulo cisco.ios.ios_command
B. No inventário do Ansible
C. No arquivo de log do Ansible
D. Na running-config de cada switch

Respostas comentadas

R5.1. A) cisco.ios.ios_command

Por quê: ios_command executa comandos (normalmente show) e retorna a saída, podendo aguardar condições com wait_for. Mudanças de configuração ficam com ios_config.

✗ B) Incorreta. O módulo copy copia arquivos para hosts gerenciados, não executa comandos na CLI do IOS.

✗ C) Incorreta. Esse módulo não existe na coleção cisco.ios.

✗ D) Incorreta. O ios_config gerencia linhas de configuração.

> **Dica de prova:** Coletar show via Ansible: ios_command.

R5.2. C) Baseada em controlador

Por quê: Na gestão por controlador, a configuração e a política são definidas centralmente e enviadas aos dispositivos por interfaces southbound; aplicações e operadores interagem pelo controlador.

✗ A) Incorreta. Na abordagem por dispositivo, cada equipamento é configurado individualmente.

✗ B) Incorreta. Syslog centraliza registros, mas não configura os dispositivos.

✗ D) Incorreta. O console local exige acesso físico a cada equipamento.

> **Dica de prova:** Ponto central que empurra política a muitos dispositivos: controlador.

R5.3. A) Da 0 (emergencies) até a 4 (warnings)

Por quê: logging trap define o limite: são enviadas as mensagens com severidade igual ou mais grave (número menor ou igual). O padrão para servidores syslog é informational.

✗ B) Incorreta. O filtro não seleciona um único nível; inclui os mais graves.

✗ C) Incorreta. Níveis de número maior são menos graves e ficam de fora.

✗ D) Incorreta. O padrão é informational (6), mas aqui foi alterado para warnings (4).

> **Dica de prova:** logging trap N: envia de 0 até N.

R5.4. B) No inventário do Ansible

Por quê: No Ansible, o inventário (INI ou YAML) define hosts e grupos; os playbooks escolhem em quais grupos as tarefas serão executadas.

✗ A) Incorreta. O módulo executa comandos, mas não define os hosts gerenciados.

✗ C) Incorreta. Logs registram execuções, não os alvos.

✗ D) Incorreta. Os dispositivos não precisam de configuração do Ansible.

> **Dica de prova:** Quem o Ansible gerencia: inventário.

DIA DA PROVA

Estratégia de prova

O 200-301 CCNA v2.0 é uma prova de 120 minutos com questões de múltipla escolha, múltipla resposta e tarefas práticas, e a Cisco não divulga a quantidade de questões nem a nota de corte. Os pesos são 25% Infraestrutura e Conectividade, 25% Switching e Acesso, 20% Roteamento IP, 20% Serviços e Segurança e 10% IA e Operações. Espere muitas questões com saída de comando (show, ping, traceroute, ipconfig, syslog) ou trecho de configuração pedindo a conclusão, a causa ou o comando que falta. As alternativas erradas costumam ser comandos reais usados no modo errado, no lugar errado ou do protocolo vizinho (CDP x LLDP, LACP x PAgP, HSRP x VRRP, TACACS+ x RADIUS). O v2.0 também pode exigir avaliar saídas e recomendações de IA agêntica e assistentes digitais de rede.

Como responder

✓ Distribua o estudo pelos pesos: os domínios 1.0 e 2.0 somam metade da prova e trazem muita conta de sub-rede e leitura de show.

✓ Diante de uma saída de comando, ache o campo decisivo antes de ler as alternativas (Root ID x Bridge ID, [AD/métrica], flags P/D/s/I, Status/Protocol, inside local/global).

✓ Em comando de configuração, confira o modo em que ele vive (global, interface, pool DHCP, line vty, router ospf): alternativas erradas costumam trazer comando real no modo errado.

✓ Em questões de Escolha DUAS, julgue cada afirmação sozinha como verdadeira ou falsa; não procure pares que pareçam combinar.

✓ Em roteamento, aplique sempre a ordem prefixo mais longo, depois AD, depois métrica, mesmo que a alternativa destaque uma AD menor.

✓ Memorize os padrões de fábrica cobrados (CDP ligado e LLDP desligado no Catalyst 9300, Rapid PVST+, HSRP sem preempt, VRRP com preempt, lease de 1 dia, logging trap informational): muitas questões dependem deles.

✓ Em recomendação de IA ou agente, compare a sugestão com a evidência das saídas e prefira a alternativa com validação e aprovação humana.

✓ Treine com a meta de 82% nos simulados de 60 questões, cerca de 2 minutos por questão, e reserve tempo para as tarefas práticas.

Erros que derrubam candidatos

✗ Errar conta de sub-rede em blocos maiores que /24 ou esquecer de inverter o 7º bit no EUI-64.

✗ Usar switchport trunk allowed vlan sem add e confundir os resultados de DTP auto/auto e LACP passive/passive.

✗ Trocar BPDU guard (err-disabled), root guard (root-inconsistent) e loop guard (loop-inconsistent).

✗ Deixar a distância administrativa vencer o prefixo mais longo ou dar AD menor que 110 à estática flutuante.

✗ Inverter inside local e inside global, esquecer o overload ou a marcação inside/outside no NAT.

✗ Esquecer o deny implícito e a regra da primeira correspondência nas ACLs, ou aplicar ACL padrão perto da origem.

✗ Achar que a lista AAA cai para o método local quando a senha é rejeitada pelo servidor.

Na semana da prova

- ☐ Confirme a versão agendada: o v2.0 vale a partir de 03/02/2027 e o v1.1 pode ser feito até 02/02/2027.
- ☐ A página do exame lista os idiomas inglês e japonês: revise os nomes em inglês dos comandos, estados e saídas (root-inconsistent, err-disabled, EXSTART, Secure-shutdown).
- ☐ Refaça as provas completas cronometradas e revise cada erro pela explicação das alternativas, anotando o detalhe que separou a certa da errada.
- ☐ Revise as tabelas de números: blocos de sub-rede, AD, temporizadores (CDP, LLDP, OSPF, HSRP), prioridades STP, portas (SNMP, RADIUS, TACACS+, IKE) e severidades do syslog.
- ☐ Na véspera, releia só os quadros lembrar e as pegadinhas de cada domínio e durma bem.

REVISÃO FINAL

Folha de cola

Leia na véspera e na manhã da prova: os gatilhos e as pegadinhas mais importantes de cada domínio.

1. 1.0 Infraestrutura e Conectividade de Rede

‣ Cliente com 169.254.x.x e gateway em branco → **Nenhuma resposta do servidor DHCP: verifique enlace, VLAN da porta, relay e servidor.**

‣ Ping por IP funciona, por nome dá 'não encontrado' → **DNS: teste com nslookup no cliente.**

‣ Late collisions no lado half-duplex → **Duplex incompatível entre as pontas.**

‣ Output drops no uplink em horário de backup, CRC zerado → **Congestionamento de saída, sem falha física.**

‣ CRC em qualquer computador ligado ao mesmo ponto, duplex igual → **Cabo ou conector danificado no ponto.**

⚠ 172.16.0.0/12 vai só até 172.31.255.255; 100.64.0.0/10 é espaço compartilhado de provedor (RFC 6598), não RFC 1918.

⚠ Em blocos maiores que /24, o broadcast é só o último endereço do bloco (192.168.11.255); .255 no meio é host válido.

⚠ FFFE entra entre o 3º e o 4º bytes e o 7º bit é invertido: 00 vira 02 e 02 vira 00.

2. 2.0 Switching e Acesso à Rede

‣ Root ID igual ao Bridge ID / This bridge is the root → **O switch local é a root bridge da VLAN.**

‣ Prioridade exibida 32778 ou 24586 sem ninguém configurar o valor quebrado → **Extended system ID: prioridade + número da VLAN.**

‣ Estações demoram cerca de 30 s para encaminhar e falham no DHCP ao ligar → **Falta spanning-tree portfast nas portas de estação.**

‣ Papel Altn com estado BLK → **Porta alternate: caminho reserva até a raiz, descartando.**

‣ %CDP-4-NATIVE_VLAN_MISMATCH → **Igualar a VLAN nativa nas duas pontas do trunk.**

⚠ Sem add a lista é substituída e o trunk passa a levar só a VLAN 30; use allowed vlan add 30.

⚠ Ser raiz é root primary (24576); secondary (28672) é reserva; 61440 é a pior prioridade possível.

⚠ auto só responde; é preciso desirable ou trunk em pelo menos um lado. auto + auto = acesso.

3. 3.0 Roteamento IP

‣ Várias rotas contendo o destino com prefixos diferentes → **Prefixo mais longo vence; AD e métrica não entram.**

‣ Mesmo prefixo por estática e OSPF → **Menor AD: estática 1 vence OSPF 110, salvo AD configurada maior.**

‣ Rota de reserva usada só se a principal sumir → **Estática flutuante com AD maior que a da principal.**

‣ S 10.30.0.0/16 is directly connected sem rede conectada → **Estática configurada só com interface de saída.**

‣ Dois próximos saltos com a mesma métrica para o mesmo prefixo → **Balanceamento por caminhos de custo igual.**

⚠ AD só desempata o mesmo prefixo; a /24 estática com AD 200 vence a /16 do OSPF para destinos dentro dela.

⚠ Qualquer AD menor que 110 vence o OSPF o tempo todo; use valor acima de 110 e abaixo de 255.

⚠ AD 255 nunca é instalada, nem como reserva.

4. 4.0 Serviços de Rede e Segurança

‣ Comando aaa authentication não é aceito → **Falta aaa new-model.**

‣ Autorizar e registrar cada comando dos administradores → **TACACS+.**

‣ Backups de configuração não podem trafegar em claro e exigem autenticação → **SCP ou SFTP no lugar de TFTP/FTP.**

‣ Muitos hosts e um único IP público na interface do provedor → **ip nat inside source list ACL interface X overload.**

‣ Quinto usuário não navega com pool de quatro IPs → **NAT dinâmico sem overload (um IP por host).**

⚠ O próximo método só entra se o anterior retornar erro (servidor fora); rejeição de senha encerra a tentativa.

⚠ A ordem escrita é a ordem de consulta: o servidor vem primeiro e local por último.

⚠ Tipo 7 é reversível; recrie com username ... secret.

5. 5.0 IA e Operações e Gerenciamento de Rede

‣ Agente vai acessar switches para coletar dados e propor correções → **Privilégio mínimo e registro das ações.**

‣ Agente propõe mudança com risco de indisponibilidade → **Aprovação humana antes de aplicar.**

‣ Agente precisa consultar inventário, alarmes e abrir tíquetes de forma padronizada → **Model Context Protocol (MCP).**

‣ Divide objetivo em subtarefas e usa ferramentas → **Característica da IA agêntica.**

‣ Política classifica senhas, chaves e IPs públicos como restritos → **Mascarar os dados antes de montar o prompt.**

⚠ Ação de alto risco exige aprovação humana antes; confiança do modelo não substitui revisão.

⚠ Privilégio mínimo, ferramentas controladas e logs que identifiquem cada ação.

⚠ Se as saídas show contradizem a sugestão, rejeite e investigue a evidência.

GABARITO

Respostas do diagnóstico

D1. B) 256 sub-redes → revise o capítulo 1

Por quê: Número de sub-redes = 2^(diferença de prefixos). /56 para /64 dá 256; /48 para /64 daria 65.536.

✗ A) Incorreta. 65.536 sub-redes /64 caberiam em um /48.

✗ C) Incorreta. 64 sub-redes exigiriam 6 bits.

✗ D) Incorreta. 16 sub-redes corresponderiam a um /60.

> **Dica de prova:** /56 em /64: 256 sub-redes.

D2. A) /26, com 62 hosts → revise o capítulo 1

Por quê: Procure o menor n com 2^n - 2 maior ou igual ao número de hosts: 2^6 - 2 = 62 atende 50, logo sobram 6 bits de host (32 - 6 = /26).

✗ B) Incorreta. Uma /27 oferece 30 hosts, insuficiente.

✗ C) Incorreta. Uma /28 oferece 14 hosts, insuficiente.

✗ D) Incorreta. Uma /25 oferece 126 hosts; funciona, mas desperdiça endereços.

> **Dica de prova:** 50 hosts: 6 bits de host, /26.

D3. B) O gateway foi configurado com o broadcast da sub-rede → revise o capítulo 1

Por quê: O gateway precisa ser um endereço de host válido, na mesma sub-rede, pertencente ao roteador. Broadcast ou endereço de rede nunca servem como gateway.

✗ A) Incorreta. Configuração manual funciona se os parâmetros estiverem corretos.

✗ C) Incorreta. 10.5.5.20 pertence a 10.5.5.0/24.

✗ D) Incorreta. Ampliar a máscara não corrige o gateway inválido.

> **Dica de prova:** Gateway = IP do roteador, nunca o broadcast.

D4. C) Criar a VLAN 30 e ter uma porta ativa nessa VLAN → revise o capítulo 2

Por quê: O estado de linha da SVI (autostate) depende das portas da VLAN: sem VLAN criada ou sem porta ativa nela, a SVI permanece down/down.

✗ A) Incorreta. no switchport é aplicado a portas físicas, não a SVIs.

✗ B) Incorreta. O gateway padrão de um switch L2 não altera o estado de uma SVI.

✗ D) Incorreta. ip routing habilita roteamento entre interfaces, mas não sobe uma SVI cuja VLAN não existe.

> **Dica de prova:** SVI down/down: VLAN existe? Há porta ativa na VLAN?

D5. B) power inline never → revise o capítulo 2

Por quê: power inline never transforma a porta em porta só de dados; auto (padrão) detecta e alimenta; static reserva potência fixa.

✗ A) Incorreta. Converte a porta em camada 3, sem tratar do PoE.
✗ C) Incorreta. static reserva potência e alimenta o dispositivo.
✗ D) Incorreta. auto detecta e alimenta dispositivos PoE.

> **Dica de prova:** Porta PoE só para dados: power inline never.

D6. B) switchport nonegotiate → revise o capítulo 2

Por quê: O DTP negocia trunks automaticamente. Em portas com modo fixo, switchport nonegotiate desativa o envio de quadros DTP, reduzindo riscos de negociação indevida.

✗ A) Incorreta. Define a VLAN nativa, sem desativar o DTP.
✗ C) Incorreta. Port security limita MACs e não controla o DTP.
✗ D) Incorreta. Coloca a porta em negociação passiva, o oposto do pedido.

> **Dica de prova:** Trunk fixo sem DTP: switchport nonegotiate.

D7. A) 172.30.0.1, pela entrada /24 → revise o capítulo 3

Por quê: Mesmo com AD 200, a estática para 10.80.9.0/24 é instalada (o prefixo é diferente da /16) e vence para destinos dentro dela.

✗ B) Incorreta. Métricas de fontes diferentes não são comparadas.
✗ C) Incorreta. A AD só desempata rotas para o mesmo prefixo.
✗ D) Incorreta. Prefixos diferentes não são balanceados entre si.

> **Dica de prova:** AD não vence prefixo mais longo.

D8. A) O R2 é standby; 10.10.10.3 encaminha pelo IP virtual → revise o capítulo 3

Por quê: No HSRP, o roteador ativo responde pelo IP e MAC virtuais; o standby monitora os hellos e assume se o ativo falhar. Os hosts apontam o gateway para o IP virtual.

✗ B) Incorreta. O R2 tem prioridade 100, menor que a do ativo (110).
✗ C) Incorreta. Os hosts usam o IP virtual 10.10.10.1 como gateway, para ter redundância.
✗ D) Incorreta. Quem encaminha o tráfego do IP virtual é o roteador ativo, não o standby.

> **Dica de prova:** HSRP: hosts usam o IP virtual; quem encaminha é o Active.

D9. D) A default via 198.51.100.1, com AD 10, entra na tabela → revise o capítulo 3

Por quê: Duas rotas default com distâncias diferentes formam principal e reserva. Enquanto a principal (AD menor) for válida, a reserva fica fora da tabela.

✗ A) Incorreta. A rota de reserva existe justamente para esse caso.
✗ B) Incorreta. Com ADs diferentes não há balanceamento; com a principal ausente, só a reserva fica.
✗ C) Incorreta. Roteadores não fazem broadcast de tráfego unicast.

> **Dica de prova:** Default reserva: mesma rota com AD maior.

D10. A) Aplicar no Gi1/0/48 uma política com device-role router → revise o capítulo 4

Por quê: No RA guard, cada porta recebe a política adequada: host nas portas de usuários (RAs descartados) e router nas portas com roteadores legítimos.

✗ B) Incorreta. device-role host no uplink bloquearia os RAs legítimos.
✗ C) Incorreta. Remover tudo eliminaria a proteção contra RAs falsos.
✗ D) Incorreta. DHCP snooping não trata RAs do IPv6.

> **Dica de prova:** RA guard: host nos usuários, router no uplink do roteador.

D11. D) O IKE autentica os pares e negocia SAs e chaves → revise o capítulo 4

Por quê: O IKEv2 (UDP 500/4500) negocia as SAs; o ESP usa essas SAs para cifrar e autenticar o tráfego. As SAs expiram e são renovadas periodicamente.

✗ A) Incorreta. Quem protege os pacotes de dados é o ESP (ou o AH).
✗ B) Incorreta. O IKE não transporta os dados do túnel.
✗ C) Incorreta. Roteamento não é função do IKE.

> **Dica de prova:** IKE negocia; ESP protege os dados.

D12. B) Falta uma linha permit; o deny implícito descarta o resto → revise o capítulo 4

Por quê: Pacotes que não casam com nenhuma entrada são descartados pelo deny implícito. Uma ACL de bloqueio pontual precisa terminar com um permit, por exemplo permit ip any any.

✗ A) Incorreta. 1 a 99 são ACLs padrão; 100 a 199 são as estendidas numeradas.
✗ C) Incorreta. A entrada só casa com TCP 23; o tráfego web é descartado pelo deny implícito.
✗ D) Incorreta. A direção não explica a perda total; o problema é a ausência de permit.

> **Dica de prova:** Toda ACL tem deny implícito no fim: inclua o permit necessário.

Agora, treine no formato real

Faça as 6 provas completas do curso CCNA: 360 questões inéditas, tempo do exame, explicação de cada alternativa e link da documentação para revisar.

Ver as 6 provas completas e o cupom do mês →

Até o dia da prova, uma revisão por dia no seu feed

Instagram @strecht.simulados

Um post de prova por dia: questão comentada, pegadinhas e o “não confunda” de cada certificação.

Seguir no Instagram →

YouTube Strecht Simulados

Shorts diários com pegadinhas de prova e, aos sábados, um simulado comentado.

Inscrever-se no canal →

Material independente de preparação, sem afiliação ou endosso de Cisco. As questões são inéditas e não reproduzem a prova real.