examundo

CCNA 模拟考试（中文题库）

50 题，附答案。指南和译文由软件制作并核对，目前还没有人工审阅。

更新日期：2026 年 11 月 25 日 · examundo.tech/zh/ccna/

网络基础

1. 网络工程师从 192.168.20.0/24 地址块中，已把 192.168.20.0/26 分给 VLAN 10，把 192.168.20.64/27 分给 VLAN 20。下面哪个可用子网恰好提供 2 个可用主机地址，适合点对点 WAN 链路，并且网络地址最小？

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

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

---

2. TCP 发送方的拥塞窗口（congestion window）是 32 KB，接收方通告的窗口大小是 24 KB。发送方已有 10 KB 数据发出但未被确认。在等待确认之前，发送方还能再发送多少数据？

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

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

---

3. 某网络设备的 MAC 地址显示为 00-1A-2B-3C-4D-5E。哪一部分是组织唯一标识符（OUI，Organizationally Unique Identifier）？

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

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

---

4. 一台交换机有 24 个端口。端口 1-8 属于 VLAN 10，端口 9-16 属于 VLAN 20，端口 17-24 属于 VLAN 30。所有端口都是接入端口（access port）。这台交换机上有多少个冲突域和广播域？

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

A. 3 个冲突域，3 个广播域
B. 24 个冲突域，1 个广播域
C. 24 个冲突域，3 个广播域
D. 1 个冲突域，3 个广播域

---

5. 技术人员要为服务器和交换机之间相距 75 米的 10GBASE-T 连接选线缆。环境中日光灯带来中等程度的 EMI（电磁干扰）。哪种线缆满足最低规格要求?

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

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

---

6. 网络管理员要汇总 172.16.32.0/20、172.16.48.0/20、172.16.64.0/20 和 172.16.80.0/20 这四条路由。能包含这四个网络的最小单条汇总路由是什么?

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

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

---

7. 一台交换机有 24 个端口，连接了 8 台设备。活动的冲突域和广播域各有多少个？（假设默认配置，没有 VLAN）

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

A. 8 个冲突域，1 个广播域
B. 1 个冲突域，8 个广播域
C. 24 个冲突域，1 个广播域
D. 1 个冲突域，1 个广播域

---

8. 管理员在查看 1995 年的 IP 地址文档时，发现一个网络标注为“Class B，172.16.0.0/16”（B 类）。在现代的无类别网络（classless networking，CIDR）中，“B 类”这个说法为什么会在实际运维中造成误导?

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

A. B 类网络已经不能在互联网上路由
B. CIDR 要求所有 B 类网络都使用可变长子网掩码
C. /16 掩码可以用于任何 IP 范围，不受历史上的地址类别边界限制
D. 172.16.0.0/16 是私有地址范围，所以按定义就是无类别的

---

9. 二进制数 11001000 的十进制值是多少?

What is the decimal equivalent of the binary number 11001000?

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

---

10. 1000BASE-T 以太网在 Cat 5e UTP 线缆上的最大传输距离是多少?

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

A. 185 米
B. 2 公里
C. 500 米
D. 100 米

IP 连接

11. 一台路由器收到去往 192.168.0.0 的三条路由：通过 OSPF 学到的 192.168.0.0/22，通过 EIGRP 学到的 192.168.0.0/24，以及静态路由 192.168.0.0/16。一个目的地址为 192.168.0.50 的数据包到达。会使用哪条路由?

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

A. 使用 OSPF 的 /22 路由，因为 OSPF 的 AD 比 EIGRP 低，而且比静态路由更具体

B. 使用 EIGRP 的 /24 路由，因为它的前缀匹配最长（最具体）

C. 使用静态 /16 路由，因为静态路由的 AD 最低，总是优先

D. 路由器在三条路由之间负载均衡，以充分利用链路

---

12. HSRP 路由器处于哪个状态，说明它正在代表虚拟 IP 地址转发流量?

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

A. Standby

B. Listen

C. Speak

D. Active

---

13. 哪一组命令可以在路由器配置模式下，用 network 语句为恰好位于 10.1.1.0/24 子网的接口启用 OSPF 进程 1，并把它们划入区域 0?

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

A. interface GigabitEthernet0/0，然后 ip ospf 1 area 0

B. router ospf 1，然后 network 10.1.1.1 255.255.255.0 area 0

C. ip routing ospf 1 area 0

D. router ospf 1，然后 network 10.1.1.0 0.0.0.255 area 0

---

14. 浮动静态路由（floating static route）的作用是什么?

What is the purpose of a floating static route?

A. 在多条等价路径之间做负载均衡

B. 在路由协议之间自动重分发路由

C. 提供备份路由，只在主路由失效时才使用

D. 提供通往互联网的默认路由

---

15. 同一以太网段上的两台 OSPF 路由器配置如下：R1（优先级 100，RID 10.1.1.1）和 R2（优先级 100，RID 192.168.1.1）。假设两台路由器同时启动，哪台会成为 DR?

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

A. 都不会，因为优先级相同会造成死锁

B. R1，因为它的 Router ID 较小

C. R2，因为 192.168.1.1 是私有 IP 地址

D. R2，因为它的 Router ID 较大

---

16. 一台路由器通过三种途径学到同一个目的网络 172.20.0.0/16：OSPF、EIGRP 和静态路由。路由器会把哪条路由装入路由表?

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

A. EIGRP 路由

B. 三条路由都装入，用于负载均衡

C. 静态路由

D. OSPF 路由

---

17. 区域 10 中的一台 OSPF 路由器从 ABR 收到一条 Type 3 LSA，通告网络 172.20.0.0/16。之后它又从 ASBR 收到一条 Type 5 LSA，通告同一个网络 172.20.0.0/16。两条 LSA 的度量值都有效。会装入哪条路由?

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

A. Type 3 的区域间路由，因为区域内和区域间路由优先于外部路由

B. 两条都不装入，因为 OSPF 不允许同一个前缀同时作为区域间路由和外部路由被通告

C. 如果总开销相同，两条都装入，做等价多路径

D. Type 5 的外部路由，因为在 LSDB 中 Type 5 LSA 的优先级高于 Type 3 LSA

---

18. 以太网接口上，OSPF 默认的网络类型是哪一种?

Which OSPF network type is the default on Ethernet interfaces?

A. Non-broadcast

B. Point-to-point

C. Broadcast

D. Point-to-multipoint

---

19. 广播网络上的一台 OSPF 路由器，接口优先级设为 0。这台路由器成功与 DR 建立了邻接关系。它与 DR 之间会达到什么 OSPF 状态?

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

A. INIT 状态，因为已交换 Hello 包，但没有确认双向通信

B. EXSTART 状态，因为 DBD 交换已开始，但没有 DR 资格就无法完成

C. FULL 状态，因为优先级 0 只是阻止参加 DR/BDR 选举，不阻止建立邻接

D. 2-WAY 状态，因为优先级为 0 的路由器在广播网络上无法形成 FULL 邻接

---

20. 同一以太网段上的三台 OSPF 路由器配置如下：R1（优先级 100，RID 1.1.1.1）、R2（优先级 100，RID 2.2.2.2）、R3（优先级 100，RID 3.3.3.3）。所有路由器同时启动。邻接关系建立后，下面哪个说法正确?

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

A. R1 成为 DR，R2 成为 BDR，R3 是 DROTHER

B. MAC 地址最大的路由器成为 DR

C. R2 成为 DR，因为它的 Router ID 居中

D. R3 成为 DR，R2 成为 BDR，R1 是 DROTHER

网络接入

21. 在 Rapid PVST+（IEEE 802.1w）中，哪个端口状态最直接地合并了传统 802.1D 生成树协议中的 blocking、listening 和 disabled 状态?

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

A. Learning

B. Blocking

C. Discarding

D. Forwarding

---

22. 哪个协议提供动态 EtherChannel 协商，并且是 IEEE 标准?

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

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

---

23. 网络管理员需要核对 Cisco 交换机上的 VLAN 分配情况。哪条命令会以简洁的、以 VLAN 为中心的表格，显示 VLAN ID、名称、状态和分配的接入端口?

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

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

---

24. 指定端口（Designated Port）在生成树协议（STP）中的作用是什么?

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

A. 只接收 BPDU
B. 阻塞流量以防止环路
C. 直接连接到根桥
D. 在网段上转发流量

---

25. 在 Rapid PVST+ 中，一台交换机有两个端口连接到同一个共享以太网段，而且只有其中一个能成为该网段的指定端口。同一台交换机上另一个非指定端口会被分配什么角色?

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

A. Edge port
B. Alternate port
C. Backup port
D. Root port

---

26. 在 Cisco 交换机上，IEEE 802.1Q 中继链路使用默认的本征 VLAN（native VLAN）标记行为。属于本征 VLAN 的普通数据帧是如何传输的?

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

A. 用 MPLS 标签代替 VLAN 标记
B. 只作为三层 IP 数据包
C. 带有两个 802.1Q VLAN 标记
D. 不带 802.1Q VLAN 标记

---

27. 工程师需要确认哪台交换机是 VLAN 20 的 STP 根桥。哪条命令能提供这个信息?

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

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

---

28. 哪种无线接入点（AP）模式必须有无线局域网控制器（WLC）才能工作?

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

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

---

29. 连接终端用户设备的端口上，应启用哪个 STP 功能来最大限度缩短收敛时间?

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

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

---

30. 在 STP 中，选举根桥（root bridge）时，最先比较哪个条件?

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

A. MAC 地址最小
B. 网桥优先级最小
C. 网桥优先级最大
D. 端口速率最快

安全基础

31. 某无线网络需要基于密码的个人认证，并且所有客户端都支持 WPA3。哪种安全协议对被动离线猜密码攻击的防护最强?

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

A. 使用 SAE 的 WPA3-Personal
B. 使用 128 位密钥的 WEP
C. 使用 AES-CCMP 的 WPA2-Enterprise
D. 使用 TKIP 的 WPA2-Personal

---

32. 某网络在路由器接口的入方向应用了扩展 ACL 110。第一条 ACE 是 'access-list 110 deny tcp any any eq 23'。这条 ACE 会阻止什么流量?

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

A. 从任何源到任何目的地的 SSH 流量
B. 从任何源到任何目的地的所有 TCP 流量
C. 从任何源到任何目的地的 Telnet 流量
D. 仅限发往路由器接口的 Telnet 流量

---

33. 某公司需要通过互联网用 VPN 连接两个站点。这条连接必须支持组播流量和多种协议（IPv4、IPv6、IPX）。哪种 VPN 技术最合适?

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

A. SSL VPN
B. PPTP
C. GRE over IPsec
D. 仅 IPsec 隧道模式

---

34. 在网络安全中，AAA 代表什么?

What does AAA stand for in network security?

A. Access, Authentication, and Administration（访问、认证、管理）
B. Authentication, Accounting, and Auditing（认证、记账、审计）
C. Authentication, Authorization, and Accounting（认证、授权、记账）
D. Authorization, Access, and Auditing（授权、访问、审计）

---

35. 管理员需要阻止来自 192.168.10.0/24 网络、发往服务器 10.1.1.100 的 IP 流量。为了尽量减少对去往其他目的地的流量的影响，标准 ACL 应放在哪个路由器接口上?

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

A. 服务器所连的交换机端口
B. 最靠近源（192.168.10.0/24）的路由器接口
C. 所有中间路由器的接口
D. 最靠近目的地（10.1.1.100）的路由器接口

---

36. 技术人员查看路由器的运行配置，看到 'enable secret 5 1mERr$hx5rVt7rPNoS4wqbXKX7m0'。这个 enable secret 密码用的是哪种加密类型?

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

A. SHA-256 哈希（类型 8）
B. MD5 哈希（类型 5）
C. Scrypt 哈希（类型 9）
D. 简单的维吉尼亚密码（类型 7）

---

37. 某公司要求对所有访问 Cisco 路由器和交换机的网络管理员，实行集中认证、完整的命令记账（accounting）和逐条命令授权。哪种 AAA 协议最适合这个需求?

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

A. TACACS+
B. RADIUS
C. Kerberos
D. 本地认证

---

38. 某个扩展 ACL 只有一条语句 'access-list 101 permit tcp any any established'。一个只设置了 SYN 标志的 TCP 数据包，源为 203.0.113.50，目的为 198.51.100.10 的 443 端口，到达了入方向应用 ACL 101 的接口。这个数据包会怎样处理?

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

A. 被允许，因为它是建立 TCP 连接的一部分
B. 被拒绝，因为只有 SYN 标志不匹配 established 关键字
C. 只有在 TCP 状态表中有对应条目时才被允许
D. 被拒绝，因为扩展 ACL 不能允许 TCP 443 端口

---

39. 某公司要求集中认证、完整的命令记账（accounting），并且能加密整个认证数据载荷。哪种 AAA 协议最符合这些要求?

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

A. RADIUS
B. Kerberos
C. 本地数据库认证
D. TACACS+

---

40. 扩展 ACL 需要只允许来自主机 192.168.5.45 的流量。正确的通配符掩码是什么?

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

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

自动化与可编程性

41. 网络架构师正在设计软件定义网络（SDN）方案。哪个平面负责根据 SDN 控制器下发的规则，执行数据包转发操作?

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

A. 管理平面
B. 应用平面
C. 数据平面
D. 控制平面

---

42. 某 REST API 对接口查询返回如下 JSON：{"status": "up", "speed": "1000", "duplex": "full"}。Python 脚本用 speed 的值做数学运算时，引发了 TypeError。问题出在哪里?

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

A. JSON 缺少必需的 "unit" 字段
B. API 返回的 JSON 语法无效
C. speed 的值是字符串，不是整数
D. Python 的 JSON 库不支持嵌套对象

---

43. 某公司从传统的三级架构（three-tier）园区网迁移到 Cisco SD-Access 交换矩阵（fabric）。最主要的架构变化是什么?

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

A. 由于只用无线接入，物理布线需求减少 50%
B. 网络用 VXLAN 叠加网络做分段，取代传统 VLAN
C. 路由协议被禁用，所有转发决策都由交换机做出
D. 所有流量都经过互联网进行策略执行

---

44. 在网络可编程性中，YANG 数据模型的作用是什么?

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

A. YANG 压缩大型配置文件，以加快传输
B. YANG 定义配置数据和运行状态数据的结构与约束
C. YANG 在 API 传输过程中加密配置数据
D. YANG 用图形化工作流取代 CLI 命令

---

45. 工程师通过 REST API 在 Cisco 交换机上创建新 VLAN 时，收到 409 Conflict 状态码。VLAN ID 有效，在允许的范围内。最可能的原因是什么?

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

A. 交换机正在处理另一项配置更改
B. 请求载荷中的 JSON 语法无效
C. 交换机上已经存在该 ID 的 VLAN
D. API 凭据的权限不足

---

46. 下面这段配置片段中，哪个 JSON 语法错误会导致它无法被正确解析?
{"hostname": "SW1", "vlan": 10, "ports": ["Gi0/1", "Gi0/2"], "enabled": true}

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

A. hostname 的值应该用单引号，而不是双引号
B. vlan 的值应该用引号括起来，作为字符串
C. 这段 JSON 语法是正确的
D. 数组应该用圆括号，而不是方括号

---

47. 工程师写了一个使用 ncclient 库的 Python 脚本，通过 NETCONF 推送配置。脚本连接成功，但 edit-config 操作失败，报 "missing-element" 错误。XML 载荷的格式是正确的。最可能的原因是什么？

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

A. YANG 模型要求一个必填元素，但载荷中没有包含
B. XML 中的命名空间声明不正确
C. 设备不支持 writable-running 能力
D. 目标数据存储被另一个会话锁定

---

48. 某 API 要求先认证才能更改配置。哪种认证方式提供基于令牌的访问，令牌在一段时间后过期，从而降低凭据泄露的风险？

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

A. SNMP 团体字符串
B. 使用 bearer 令牌的 OAuth 2.0
C. 使用 Base64 编码的基本认证
D. SSH 公钥认证

---

49. 对 Cisco 设备的某次 REST API 调用返回如下 JSON：
{"status": "success", "vlan_id": 100, "vlan_name": "Engineering", "active": true}

键 "active" 的数据类型是什么？

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

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

A. 布尔值（Boolean）
B. 对象（Object）
C. 字符串（String）
D. 整数（Integer）

---

50. 网络自动化脚本发送 REST API 请求来删除一个 VLAN，服务器返回 HTTP 状态码 204。这说明什么？

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

A. 设备上找不到该 VLAN
B. 服务器遇到内部错误
C. 请求因认证失败而被拒绝
D. 请求成功，并且没有返回内容

正确答案

1. A VLSM（可变长子网掩码）要求子网互不重叠，但不要求连续分配。/26 占用 192.168.20.0 到 .63，/27 占用 .64 到 .95，所以第一个空闲地址是 192.168.20.96。/30 共 4 个地址，恰好 2 个可用主机（2^2 - 2 = 2）。192.168.20.96/30 覆盖 .96 到 .99，边界正确，地址也最小。192.168.20.92/30 与已分配的 /27 重叠。192.168.20.96/29 有 6 个可用主机。192.168.20.128/30 也是 2 个主机，但网络地址不是最小。

2. D TCP 的有效窗口取拥塞窗口（32 KB）和接收方通告窗口（24 KB）中较小的一个，也就是 24 KB。发送方最多可以有 24 KB 未确认的数据在途。已有 10 KB 未确认，所以还能再发 24 - 10 = 14 KB。22 KB 是错用拥塞窗口来减（32 - 10）。24 KB 没有扣掉在途数据。32 KB 只看了拥塞窗口，忽略了接收方的限制。

3. D 00-1A-2B 是正确答案。OUI 是 48 位 MAC 地址的前 24 位（前 3 个字节），由 IEEE 分配，用来标识厂商。其余 3 个字节（3C-4D-5E）由厂商分配，用来区分具体的网卡。3C-4D-5E 是设备专属部分，不是 OUI。00-1A 只有 16 位。2B-3C-4D-5E 同时跨了 OUI 和设备部分。

4. C 交换机的每个端口都是一个独立的冲突域（collision domain），共 24 个，因为交换机用微分段，端口之间不会发生冲突。每个 VLAN 是一个独立的广播域（broadcast domain），3 个 VLAN 就是 3 个广播域。选项“24 个冲突域，1 个广播域”忽略了 VLAN 的分隔。“3 个冲突域”错把冲突域和 VLAN 对应起来。“1 个冲突域”把交换机当成了集线器。

5. C Cat 6A UTP 满足 10GBASE-T 标准，距离最长可达 100 米。Cat 6 用于 10GBASE-T 时，一般只到约 55 米，视安装条件而定，达不到 75 米。标准没有规定 Cat 5e 可用于这条 75 米的 10GBASE-T 链路，虽然它可以支持其他高于 1 Gbps 的以太网速率。Cat 6 STP 的抗 EMI 能力比 Cat 6 UTP 好，但屏蔽本身不能保证 Cat 6 在 75 米处达到 10GBASE-T 的要求。Cat 6A 的串扰性能更好，可以支持完整的 100 米。

6. B 172.16.0.0/17 是能覆盖这四个网络的最小单条汇总路由。它们合起来的地址范围是 172.16.32.0 到 172.16.95.255。第三个字节的 32 和 95 只有第一位相同，所以公共前缀总共是 17 位。这条汇总覆盖 172.16.0.0 到 172.16.127.255，会多包含一些地址。没有任何单个 CIDR 前缀能刚好覆盖这四个网络，精确汇总需要 172.16.32.0/19 加 172.16.64.0/19。172.16.32.0/19 只覆盖前两个网络。172.16.32.0/18 不是有效的 /18 网络边界。172.16.0.0/16 比 /17 多包含更多不需要的地址。

7. A 8 个冲突域，1 个广播域是正确答案。交换机为每个活动端口创建一个独立的冲突域（8 台设备就是 8 个冲突域），通过缓冲和全双工消除端口之间的冲突。但默认情况下，同一个 VLAN 里的所有端口共用一个广播域，任何端口发出的广播都会到达其他所有端口。“1 个冲突域，8 个广播域”把概念弄反了。“24 个冲突域”把所有端口都算上了，而不是只算活动的。“1 个冲突域，1 个广播域”描述的是集线器，不是交换机。

8. C CIDR（Classless Inter-Domain Routing，无类别域间路由）取消了固定的 A/B/C 类结构。在 CIDR 下，/16 掩码可以用在任何网络上（例如 10.0.0.0/16、192.168.0.0/16），与第一个字节的数值无关。“B 类”只是历史遗留的叫法，路由器实际只看前缀长度（/16），不看地址类别。关于不能路由的说法是错的，很多公网 IP 仍然落在历史上的 B 类范围（128.0.0.0 到 191.255.255.255）内。私有地址（RFC 1918）与 CIDR 无关。VLSM 是一种子网划分技术，不是 CIDR 的要求。

9. C 把 11001000 从二进制换算成十进制：(1×128) + (1×64) + (0×32) + (0×16) + (1×8) + (0×4) + (0×2) + (0×1) = 128 + 64 + 8 = 200。这个换算技巧对理解子网掩码和 IP 地址很重要。192 的二进制是 11000000，208 是 11010000，224 是 11100000。能快速换算常见的字节值（128、192、224、240、248、252、254、255）对子网计算很有帮助。

10. D 按 IEEE 802.3ab 标准，1000BASE-T（千兆以太网）在 Cat 5e 或 Cat 6 UTP 上的最大线缆长度是 100 米（328 英尺），其中包括最多 90 米的水平布线和 10 米的跳线。185 米是 10BASE2 细同轴电缆以太网的限制。500 米是 10BASE5 粗同轴电缆的限制。2 公里不是 1000BASE-LX 的标准单模传输距离，它支持 5 公里。铜缆超过 100 米后，信号衰减和时序问题会降低性能。

11. B 在 Cisco 路由决策中，最长前缀匹配永远优先于管理距离（AD，administrative distance）。192.168.0.50 同时落在这三个前缀内，但 /24 最具体（前缀最长），所以使用 EIGRP 路由，即使它的 AD（90）比静态路由的 AD（1）高。只有前缀长度相同时才比较 AD。/16 静态路由最不具体，所以落选。/22 的 OSPF 路由比 /16 具体，但不如 /24。不同前缀长度的路由之间不会做负载均衡。

12. D Active 状态表示这台 HSRP 路由器当前正在为虚拟 IP 地址转发数据包，并响应针对它的 ARP 请求。每个 HSRP 组同一时间只能有一台路由器处于 Active。Standby 是备用状态，路由器监视 Active 路由器，在它故障时接管。Listen 状态下路由器能收到 HSRP 通告，但既不是 Active 也不是 Standby。Speak 是选举过程中的过渡状态，路由器互相交换优先级信息来决定 Active 和 Standby 角色。

13. D 正确的命令是 router ospf 1，然后 network 10.1.1.0 0.0.0.255 area 0。传统的启用方式是在 OSPF 进程下用 network 命令加通配符掩码（wildcard mask）。network 10.1.1.0 0.0.0.255 area 0 匹配恰好位于 10.1.1.0/24 范围内的接口，并把它们放进区域 0。“interface GigabitEthernet0/0，然后 ip ospf 1 area 0”是有效的接口级配置，但不符合题目要求的路由器配置模式方式。“network 10.1.1.1 255.255.255.0 area 0”把 255.255.255.0 当成了通配符掩码，不能精确匹配该子网。“ip routing ospf 1 area 0”语法无效。

14. C 浮动静态路由的管理距离（AD）比主路由高（例如 AD 为 5，而不是默认的 1），所以只有在主路由不可用时才会进入路由表。它常用于拨号按需备份链路，或者让动态路由协议（如 AD 为 110 的 OSPF）在正常情况下优先于这条静态路由。浮动静态路由不做负载均衡，负载均衡需要等价路由。它也不在协议之间重分发路由，重分发是另一个单独的过程。浮动静态路由可以指向互联网，但那不是它的核心用途，关键在于提高的 AD 让它只作备份。

15. D OSPF 优先级相同时（都是 100），决胜条件是 Router ID 最大者胜出。OSPF 按数值比较 Router ID：192.168.1.1 大于 10.1.1.1，所以 R2 成为 DR。192.168.1.1 是私有地址这一点无关紧要，OSPF 对所有 32 位 RID 一视同仁。选 RID 较小者是错的，OSPF 选的是最大的。优先级相同不会造成死锁，OSPF 只是进入下一个决胜条件。很多人以为数值小的优先（像管理距离那样），但 DR 选举看的是优先级高，再看 RID 大。

16. C Cisco 路由器用管理距离（AD）在不同来源的路由之间做选择。静态路由的 AD 是 1（最可信），EIGRP 是 90，OSPF 是 110。路由器选择 AD 最低的路由，所以静态路由胜出。OSPF 的 AD 为 110，比静态和 EIGRP 都差。EIGRP 的 AD 为 90，比 OSPF 好，但比静态路由差。只有多条路由的 AD 和度量值都相同时才会负载均衡，这里不是这种情况。AD 的比较先于度量值。

17. A OSPF 的路由优先顺序是：区域内（Type 1/2）> 区域间（Type 3）> 外部 Type 1（Type 5 E1）> 外部 Type 2（Type 5 E2）。两条 LSA 虽然通告同一个前缀，但 Type 3 的区域间路由在优先顺序中更高，所以胜出。Type 5 LSA 的优先级并不更高，外部路由始终是最不优先的。ECMP 只适用于类型相同且开销相等的路由，这里类型不同。OSPF 允许重叠的通告，路由器按优先规则决定用哪条。

18. C Broadcast 是以太网等多路访问介质上 OSPF 的默认网络类型。在这种模式下，OSPF 会选举指定路由器（DR）和备份指定路由器（BDR），以减少邻接关系和 LSA 泛洪。Point-to-point 是串行链路上的默认类型，不选举 DR/BDR。Non-broadcast 用于 NBMA 网络（如 Frame Relay 的中心辐射结构），需要手动配置邻居。Point-to-multipoint 也用于 NBMA，但把每条链路当作点对点处理，不选 DR/BDR。网络类型不一致可能阻止邻接建立或引起路由问题，但并不一定总会阻止邻接形成。

19. C 优先级为 0 的 OSPF 路由器与 DR 和 BDR 之间可以达到 FULL 状态。优先级 0 表示这台路由器没有资格成为 DR 或 BDR，不会参加选举。但在广播网络上，所有路由器都会与 DR 和 BDR 形成 FULL 邻接（交换完整的 LSDB），而与其他 DROTHER 之间只停在 2-WAY 状态。优先级设置不会阻止 FULL 邻接的形成，只影响选举资格。EXSTART 和 INIT 是到达 FULL 之前的过渡状态。

20. D 所有路由器的 OSPF 优先级相同（100）时，用 Router ID 决胜。OSPF 选 RID 最大的为 DR，第二大的为 BDR。R3（3.3.3.3）成为 DR，R2（2.2.2.2）成为 BDR，R1（1.1.1.1）是 DROTHER。“R1 成为 DR”把逻辑弄反了，RID 小的不会胜出。“R2 因为 RID 居中成为 DR”编造了一条不存在的“中间值”规则。“MAC 地址最大”是把 OSPF 与旧式网桥混淆了，MAC 地址与 OSPF 的 DR 选举无关。

21. C Rapid PVST+ 把 802.1D 原来的五种端口状态简化为三种：discarding、learning 和 forwarding。Discarding 状态吸收了传统的 blocking、listening 和 disabled 三种状态的功能，因为这三种状态下端口都不转发帧，也不学习 MAC 地址。选项 Learning 与传统的 learning 状态直接对应，没有变化。Forwarding 也直接对应传统的 forwarding 状态。Blocking 在 RSTP 中不再作为独立的状态名称使用，它与 listening 和 disabled 一起并入了 discarding。

22. D LACP（Link Aggregation Control Protocol，链路聚合控制协议）定义在 IEEE 802.3ad 中，是动态协商 EtherChannel 捆绑的行业标准协议。它不依赖特定厂商，可以在不同厂商的交换机之间使用。PAgP（Port Aggregation Protocol）是 Cisco 私有协议，只能在 Cisco 设备之间使用。VTP（VLAN Trunking Protocol）用于同步 VLAN 数据库，不用于链路聚合。CDP（Cisco Discovery Protocol）用于发现邻居，不用于把链路捆绑成 EtherChannel。

23. A show vlan brief 以简洁的、以 VLAN 为中心的表格列出 VLAN ID、名称、状态和分配的接入端口。show interfaces status 以端口为中心，显示端口速率、双工和 VLAN，但没有题目要求的包含 VLAN 名称和状态的 VLAN 表格。show running-config 显示全部配置命令，VLAN 分配要自己从里面找。show ip interface brief 显示路由接口和 SVI 的三层 IP 信息，不显示二层 VLAN 成员关系。

24. D STP 中的指定端口负责在所连接的网段（冲突域）上朝根桥方向转发流量。每个网段有一个指定端口，也就是该网段上到根桥路径开销最低的端口。根端口（Root Port）是非根交换机上朝根桥方向的端口，不是指定端口。为防止环路而阻塞流量的端口处于 Blocking 状态（RSTP 中是 Alternate 或 Backup），不是指定端口。所有端口都能接收 BPDU，但指定端口还会转发流量，处于 Forwarding 状态。

25. C RSTP 专门为这种情况定义了 backup port（备份端口）角色：同一台交换机的两个或多个端口连到同一个共享网段（通常经过集线器），只有一个能成为指定端口，落选的端口就成为备份端口，为同一台交换机上的指定端口提供冗余。这与 alternate port 不同，alternate port 是通过另一台交换机或另一个网段提供到根桥的备用路径，是根端口对应的 discarding 状态端口。Root port 不对，它描述的是朝根桥的最佳路径，不是本地备份。Edge port 也不对，它指的是类似 PortFast 的连接终端主机的链路，与冗余角色无关。

26. D “不带 802.1Q VLAN 标记”是正确答案，因为默认情况下，本征 VLAN 的数据帧以不加标记（untagged）的方式传输。“带有两个 802.1Q 标记”并不是默认本征 VLAN 的行为。“用 MPLS 标签代替 VLAN 标记”与普通的 802.1Q 中继转发无关。“只作为三层 IP 数据包”是错的，因为中继链路转发的是以太网帧。

27. C show spanning-tree vlan 20 显示 VLAN 20 的 STP 拓扑，包括根桥 ID、本地网桥优先级以及端口角色和状态。它会明确指出本地交换机是不是根，或者显示根的网桥 ID。show vlan brief 列出 VLAN 分配，但不显示 STP 角色。show interfaces trunk 显示中继状态和允许的 VLAN，不显示 STP 拓扑。show spanning-tree summary 显示的是生成树的摘要信息，不能指出 VLAN 20 的根桥。

28. A Lightweight（轻量级）AP 依赖无线局域网控制器（WLC）完成配置、管理和控制，并使用 CAPWAP（Control and Provisioning of Wireless Access Points）协议与控制器通信。AP 本身只有极少的配置和固件。Autonomous（自治）AP 是独立设备，每台 AP 自带完整配置，不需要控制器。Mesh 是一种部署拓扑，AP 之间通过无线相连，但 Mesh AP 既可以是轻量级的（需要 WLC），也可以是自治的。Bridge 模式用来无线连接两个有线网络，本身并不要求控制器。

29. A PortFast 让接入端口在链路启动后立即进入 Forwarding 状态，跳过 30 秒的 Listening 和 Learning 延迟。这对不会形成环路的终端设备（电脑、打印机）是安全的。UplinkFast 和 BackboneFast 是传统的 STP 优化功能，针对上行链路和间接链路故障，不用于终端用户端口。BPDU Guard 是安全功能，PortFast 端口一旦收到 BPDU（说明误接了交换机）就会被关闭，它并不缩短收敛时间，而是与 PortFast 配合起保护作用。

30. B STP 选举根桥依据的是最小的网桥 ID，它由网桥优先级和 MAC 地址组成。先比较网桥优先级，优先级值最小的交换机成为根桥。如果优先级相同，再用最小的 MAC 地址决胜。“网桥优先级最大”是错的，因为值小的获胜。MAC 地址最小只在优先级相同时才用来决胜。端口速率不影响根桥选举，不过它会影响端口开销的计算。

31. A 使用 SAE 的 WPA3-Personal 用对等实体同时验证（SAE，Simultaneous Authentication of Equals）取代了 WPA2-Personal 的 PSK 认证，提供前向保密，并能防御被动离线字典攻击。SAE 认证之后，WPA3-Personal 仍用四次握手来建立流量密钥。题干已明确客户端都支持 WPA3。WPA2-Enterprise 使用的是企业认证，不是题目要求的个人认证。使用 TKIP 的 WPA2-Personal 加密较弱，TKIP 是过渡协议，2012 年被弃用，存在已知漏洞。WEP 已被 FMS、KoreK、PTW 等攻击彻底攻破，无论密钥多长，几分钟就能破解。

32. C 端口 23 是 Telnet 的知名端口号，所以 eq 23 匹配 Telnet 会话。这条 ACE 的源和目的都是 any，所以不管来源或目的地址是什么，只要是 Telnet 流量就会匹配。SSH 用的是端口 22，不是 23，不会被匹配。这条 ACE 指定的是 tcp 加 eq 23，其他 TCP 端口（如 80 的 HTTP 和 443 的 HTTPS）不会匹配这一条。入方向的接口 ACL 既能过滤转发的流量，也能过滤发往路由器本身的流量；控制平面策略和 VTY 的 access-class 配置也能限制发往路由器的流量。

33. C GRE over IPsec 既有 GRE（Generic Routing Encapsulation，通用路由封装）承载组播和多种协议的能力，又有 IPsec 的加密和认证。GRE 与协议无关，支持路由协议（OSPF、EIGRP）、组播和 IPv6，IPsec 则提供安全性。单独的 IPsec 隧道模式只支持单播 IP 流量，不支持组播和非 IP 协议。SSL VPN 用于远程访问客户端，不用于站点到站点，也不支持组播和路由协议。PPTP 已被弃用，不安全，缺乏现代加密标准。GRE 加 IPsec 是 Cisco 在需要动态路由或组播的站点到站点 VPN 中的标准方案。

34. C AAA 代表认证（Authentication，验证用户身份）、授权（Authorization，根据身份授予权限）和记账（Accounting，记录用户活动和资源使用）。这套框架是 Cisco 网络安全的基础，通过 TACACS+ 和 RADIUS 等协议实现。“Access, Authentication, and Administration”把认证和访问控制混为一谈，还加入了不属于 AAA 的管理。“Authorization, Access, and Auditing”调换了顺序，并用审计取代了记账，审计是相关但不同的概念。“Authentication, Accounting, and Auditing”漏掉了授权，而授权正是决定已认证用户能做什么的关键一步。

35. D 标准 ACL 只能按源 IP 地址过滤，不能按目的端口或协议过滤。最佳做法是把标准 ACL 放在尽可能靠近目的地的位置，这样不会误挡同一个源网络发往其他目的地的合法流量。所以应选“最靠近目的地（10.1.1.100）的路由器接口”。放在最靠近源的位置，会把 192.168.10.0/24 发往其他目的地的流量也一起挡掉。放在所有中间接口会浪费资源。有些交换机支持端口 ACL，但题目问的是路由器接口。这符合 ACL 放置规则：标准 ACL 靠近目的地，扩展 ACL 靠近源。

36. B “5”表示 MD5 哈希。enable secret 始终使用哈希（不可逆），所以比 enable password 更安全。类型 5 是 MD5（较旧，但仍然常见）。类型 7 是弱的维吉尼亚密码，由 service password-encryption 用于线路密码，很容易还原。类型 8 是 PBKDF2-SHA256，类型 9 是 scrypt，这两种都是更强的现代算法。enable secret 后面的数字表示哈希算法，后面的长字符串是密码的哈希值。MD5 在新部署中已不推荐，但在旧配置中仍很常见。

37. A TACACS+ 是正确答案，因为它把认证、授权和记账分成各自独立的过程，并且加密整个数据载荷，而不只是密码。关键在于 TACACS+ 支持逐条命令授权，可以精细控制每个用户能执行哪些命令。RADIUS 把认证和授权合在一起，主要用 UDP，更适合网络接入控制，而不是设备管理。本地认证无法在多台设备上集中管理。Kerberos 是基于票据的认证协议，无法提供题目要求的逐条命令授权加命令记账的组合。

38. B Cisco ACL 中的 established 关键字匹配设置了 ACK 或 RST 标志的 TCP 数据包，不匹配只有 SYN 标志的数据包。纯 SYN 包（TCP 握手的第一个包）没有设置 ACK 或 RST，所以不匹配这条语句。ACL 末尾有隐含拒绝（implicit deny），所以这个 SYN 包会被丢弃。这是重要的安全概念：established 关键字允许返回流量（ACK 响应、RST 复位），但会阻止新的入站连接请求（只有 SYN 的包）。Cisco IOS 的 ACL 是无状态的，没有 TCP 状态表（那是 ASA 等有状态防火墙的功能）。established 的判断只根据每个数据包的 TCP 标志。

39. D TACACS+ 加密整个数据载荷（不只是密码），并把认证、授权和记账分成独立的功能，因此能提供精细到命令级别的记账。RADIUS 只加密数据包中的密码字段，不加密整个载荷，而且把认证和授权合在一起，所以不太适合详细的命令记账。本地数据库认证没有集中化，每台设备各自维护独立的用户库。Kerberos 是单点登录协议，在 CCNA 级别的部署中通常不用于 Cisco 设备的 AAA。TACACS+ 使用 TCP 端口 49，RADIUS 使用 UDP 1812 和 1813。

40. A 通配符掩码 0.0.0.0 表示精确匹配单个主机，所有位都必须完全一致（0 表示必须匹配，1 表示不关心）。这等同于 ACL 语法中的 host 192.168.5.45。通配符 255.255.255.255 表示 any（所有位都不关心），会匹配所有地址。0.0.0.255 匹配前三个字节，第四个字节可以是任何值（相当于 /24 子网）。255.255.255.0 与需要的正好相反，对这个目的无效。记住：通配符掩码是子网掩码的反码，子网掩码用 1 的地方，通配符用 0。

41. C 数据平面（Data plane，也叫转发平面）负责根据 SDN 控制器下发的流表和策略执行转发操作。传统网络中由控制平面做路由决策，而在 SDN 中这套逻辑集中在控制器里，设备本地的数据平面只按控制器编好的规则转发数据包。管理平面负责设备配置和监控。应用平面包含通过北向 API 与控制器交互的应用，但数据包转发发生在数据平面。

42. C “speed 的值是字符串，不是整数”是正确答案，因为 "1000" 带有引号，在 JSON 中就是字符串。Python 的 json.loads() 会保留这个类型，所以做 speed + 2 之类的算术运算会引发 TypeError。解决办法是 int(data['speed'])。缺少 "unit" 字段不会引发 TypeError，访问它时最多是 KeyError，否则只是缺少元数据。这个 JSON 语法有效（可以解析）。Python 的 json 库完全支持嵌套对象。这是调用 API 时典型的数据类型陷阱：REST API 常把数字作为字符串返回。计算之前一定要先验证并转换类型。

43. B SD-Access 在物理 IP 底层网络（underlay）之上，用 VXLAN（Virtual Extensible LAN）叠加隧道创建逻辑网络分段（虚拟网络，VN），取代传统基于 VLAN 的分段，实现可扩展的、基于策略的微分段。底层网络仍然运行路由协议（通常是 IS-IS 或 OSPF），为交换矩阵节点之间提供 IP 可达性。流量仍留在交换矩阵内部的本地网络，不需要经过互联网（那会带来延迟和安全风险）。SD-Access 同时支持有线和无线终端，并没有强制只用无线，有线终端、上行链路和 AP 的布线仍然需要。

44. B YANG（Yet Another Next Generation）是一种数据建模语言，定义配置数据和运行状态数据的结构。它规定有哪些数据、数据类型、有效范围、哪些字段必填或可选，以及它们之间的关系。NETCONF 和 RESTCONF 等协议使用 YANG 模型，确保控制器与设备之间的数据交换一致且经过验证。YANG 本身不做加密，安全由传输协议负责（NETCONF 用 SSH，RESTCONF 用 HTTPS）。YANG 不提供图形界面，它是基于文本的建模语言。YANG 也不压缩数据，它只定义结构，数据表示的效率由编码格式（XML、JSON）决定。

45. C HTTP 409 Conflict 表示资源状态冲突，这里就是试图创建一个已经存在的 VLAN，这正是 409 的典型用法。权限不足会返回 401 Unauthorized 或 403 Forbidden，不是 409。JSON 语法无效会返回 400 Bad Request。虽然在某些系统中并发配置更改也可能引起冲突，但 REST 惯例中的 409 指向的是重复创建资源。很多人会把 409 与 423 Locked（资源暂时不可用）混淆，或者认为任何错误都与认证有关。

46. C 这段 JSON 语法有效。JSON 要求字符串的键和值使用双引号（不是单引号），所以 hostname 的写法是对的。vlan 的值 10 是数字类型，不加引号，这是正确的，JSON 用引号区分字符串，数字不加引号。JSON 中的数组必须用方括号 [ ]，不能用圆括号。布尔值 true 是小写且不加引号，写法正确。常见的 JSON 错误包括使用单引号、键值对之间缺少逗号、多余的结尾逗号或括号不匹配，这里都没有出现。

47. A "missing-element" 明确表示违反了 YANG 模型约束，也就是 YANG 模型中定义的必填叶节点或容器没有出现在 XML 载荷里。这是模式验证（schema validation）失败。如果缺少 writable-running 能力，错误会是 "operation-not-supported"，不是 "missing-element"。命名空间不对会产生 "unknown-namespace" 或解析错误。数据存储被锁定会返回 "in-use" 或 "resource-denied"。关键是要认识到 NETCONF 错误码对应特定的故障类型："missing-element" 是模式问题，"in-use" 是锁冲突，"invalid-value" 是违反约束。

48. B OAuth 2.0 使用有时限的 bearer 令牌，令牌在初次认证后签发，并会自动过期，这样即使令牌泄露，被利用的时间窗口也有限。应用在每次 API 请求中发送的是令牌，而不是凭据。基本认证（Basic authentication）每次请求都要传送用户名和密码，即使经过 Base64 编码也没有加密，而且要反复发送。SSH 公钥认证适合 CLI 访问，通常不用于基于 HTTP 的 REST API，而且密钥不会自动过期。SNMP 团体字符串是明文共享密钥，没有过期或令牌机制，被认为不适合现代 API 认证。

49. A 布尔值是正确答案，因为不带引号的小写 true 是 JSON 的布尔字面量，表示真或假。JSON 中布尔值写成 true 或 false，不加引号。字符串要用引号括起来，例如 "Engineering"。整数是不带引号的数字，例如 100。对象是用花括号括起来的嵌套结构。理解 JSON 数据类型，是在自动化脚本中正确解析 API 响应的基础。

50. D HTTP 204 No Content 是正确答案，表示请求已成功处理，并且没有响应正文。这在 DELETE 操作中很常见，只需确认已删除，不必返回数据。如果找不到该 VLAN，服务器会返回 404 Not Found。认证失败返回 401 Unauthorized 或 403 Forbidden。服务器内部错误返回 500 Internal Server Error。理解 HTTP 状态码对自动化脚本的错误处理很重要：2xx 表示成功，4xx 表示客户端错误，5xx 表示服务器错误。

英文关键词

subnet	子网	从一个大网络里划出来的小网络
subnet mask	子网掩码	标出地址里哪几位是网络部分
usable host address	可用主机地址	子网里能分配给设备的地址

summary route	汇总路由	用一条路由代表多个网络
prefix length	前缀长度	斜线后的数字，表示网络位有几位
broadcast domain	广播域	一个广播帧能到达的范围，每个 VLAN 一个
collision domain	冲突域	数据帧可能互相冲突的范围，交换机每个端口一个
acknowledgment (ACK)	确认	接收方告诉发送方数据已收到
congestion window	拥塞窗口	TCP 发送方按网络状况限制的发送量
routing table	路由表	路由器保存的去往各网络的路径
longest prefix match	最长前缀匹配	选前缀最长、最具体的那条路由
administrative distance	管理距离	路由来源的可信度，数值低的优先
metric	度量值	同一协议内比较路径好坏的数值
floating static route	浮动静态路由	主路由失效时才使用的备用静态路由
default gateway	默认网关	主机把外部流量先发给的路由器
adjacency	邻接关系	两台 OSPF 路由器之间建立的关系
Designated Router (DR)	指定路由器	广播网段上集中交换 OSPF 信息的路由器
Router ID	路由器 ID	OSPF 用来识别路由器的 32 位编号
wildcard mask	通配符掩码	0 表示必须匹配，1 表示不管
preempt	抢占	优先级更高的路由器夺回主用角色
failover	故障切换	主设备出故障时由备用设备接管
access port	接入端口	只属于一个 VLAN 的交换机端口
trunk	中继链路	同时承载多个 VLAN 的链路
native VLAN	本征 VLAN	中继上默认不打标签的 VLAN
root bridge	根桥	生成树的中心交换机，网桥 ID 最小
bridge priority	网桥优先级	选根桥时先比较的数值，低的赢
convergence	收敛	网络变化后重新达到稳定状态
EtherChannel	以太通道（链路聚合）	把多条物理链路合成一条逻辑链路
wireless LAN controller (WLC)	无线局域网控制器	集中管理轻量级接入点的设备
lightweight access point	轻量级接入点	要靠控制器才能工作的无线接入点
access control list (ACL)	访问控制列表	按顺序允许或拒绝流量的规则
implicit deny	隐含拒绝	ACL 末尾看不见的拒绝所有规则
inbound / outbound	入方向 / 出方向	流量进入接口，或离开接口
authentication	认证	确认用户是谁

authorization	授权	决定用户能做什么
accounting	记账	记录用户做过什么
data plane	数据平面	设备中实际转发数据包的部分
control plane	控制平面	决定流量走哪条路的部分
status code	状态码	服务器用来说明请求结果的数字
payload	载荷	消息里真正要传送的数据

Examundo 是独立网站，与主办这些考试的机构没有隶属关系，也未获其认可。题目均为原创，不是考试真题。 examundo.tech/zh/ccna/