examundo

CCNA 연습 문제

정답 포함 50문제. 가이드와 번역은 소프트웨어가 만들고 검토했어요. 아직 사람이 확인하지는 않았어요.

2026년 11월 25일 업데이트 · examundo.tech/ko/ccna/

네트워크 기초

1. 네트워크 엔지니어가 192.168.20.0/24 블록에서 VLAN 10에 192.168.20.0/26을, VLAN 20에 192.168.20.64/27을 할당했습니다. 아직 할당되지 않은 서브넷 중 점대점(point-to-point) WAN 링크용으로 쓸 수 있는 호스트 주소(usable host address)가 정확히 2개이고 네트워크 주소가 가장 낮은 것은 무엇입니까?

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 송신자의 혼잡 윈도우(congestion window)는 32 KB이고, 수신자가 알려 준 윈도우 크기(advertised window)는 24 KB입니다. 송신자에게는 아직 확인 응답을 받지 못한 데이터 10 KB가 전송 중입니다. 송신자는 확인 응답을 기다리기 전에 추가로 얼마를 보낼 수 있습니까?

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. 네트워크 장치의 MAC 주소가 00-1A-2B-3C-4D-5E로 표시됩니다. 이 중 OUI(Organizationally Unique Identifier)에 해당하는 부분은 어디입니까?

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. 스위치에 포트가 24개 있습니다. 1~8번 포트는 VLAN 10, 9~16번 포트는 VLAN 20, 17~24번 포트는 VLAN 30에 속하며, 모든 포트는 access 포트입니다. 이 스위치에는 충돌 도메인(collision domain)과 브로드캐스트 도메인(broadcast domain)이 각각 몇 개 있습니까?

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. 충돌 도메인 3개, 브로드캐스트 도메인 3개
B. 충돌 도메인 24개, 브로드캐스트 도메인 1개
C. 충돌 도메인 24개, 브로드캐스트 도메인 3개
D. 충돌 도메인 1개, 브로드캐스트 도메인 3개

---

5. 기술자가 **75**미터 떨어진 서버와 스위치 사이의 **10GBASE-T** 연결에 쓸 케이블을 고르고 있습니다. 이 환경에는 형광등에서 나오는 중간 정도의 전자파 간섭**(EMI)**이 있습니다. 최소 사양**(MINIMUM specification)**을 충족하는 케이블은 무엇입니까**?**

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. 네트워크 관리자가 **172.16.32.0/20, 172.16.48.0/20, 172.16.64.0/20, 172.16.80.0/20** 경로를 요약하려고 합니다. 네 네트워크를 모두 포함하는 가장 작은 단일 요약 경로**(summary route)**는 무엇입니까**?**

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. 스위치에 포트가 **24**개 있고 장치 **8**대가 연결되어 있습니다. 활성 충돌 도메인과 브로드캐스트 도메인은 각각 몇 개입니까**? (**기본 설정이며 **VLAN**은 없다고 가정합니다**.)**

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. 충돌 도메인 8개, 브로드캐스트 도메인 1개
B. 충돌 도메인 1개, 브로드캐스트 도메인 8개
C. 충돌 도메인 24개, 브로드캐스트 도메인 1개
D. 충돌 도메인 1개, 브로드캐스트 도메인 1개

---

8. 관리자가 **1995**년의 **IP** 주소 문서를 검토하다가 **"Class B, 172.16.0.0/16"**이라고 표시된 네트워크를 발견했습니다. 현대의 **classless** 네트워킹**(CIDR)**에서 운영상 **"Class B"**라는 표기가 오해를 부르는 이유는 무엇입니까**?**

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. Class B 네트워크는 더 이상 인터넷에서 라우팅되지 않는다
B. CIDR은 모든 Class B 네트워크가 가변 길이 서브넷 마스크를 쓰도록 요구한다
C. /16 마스크는 과거의 클래스 경계와 상관없이 어떤 IP 범위에도 적용할 수 있다
D. 172.16.0.0/16은 사설 주소 범위이므로 정의상 classless이다

---

9. 이진수 **11001000**의 십진수 값은 무엇입니까**?**

What is the decimal equivalent of the binary number 11001000?

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

---

10. Cat 5e UTP 케이블에서 **1000BASE-T** 이더넷의 최대 전송 거리는 얼마입니까**?**

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

A. 185미터
B. 2킬로미터
C. 500미터
D. 100미터

IP 연결

11. 라우터가 192.168.0.0에 대해 세 가지 경로를 학습했습니다. OSPF로 192.168.0.0/22, EIGRP로 192.168.0.0/24, 정적(static) 경로로 192.168.0.0/16입니다. 목적지가 192.168.0.50인 패킷이 도착했습니다. 어떤 경로가 사용됩니까?

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. OSPF /22 경로. OSPF가 EIGRP보다 AD가 낮고 static보다 구체적이기 때문이다

B. EIGRP /24 경로. 가장 긴 프리픽스 일치(가장 구체적)이기 때문이다

C. static /16 경로. static 경로는 AD가 가장 낮아 항상 이기기 때문이다

D. 라우터가 링크 사용률을 높이려고 세 경로에 로드 밸런싱한다

---

12. 라우터가 가상 IP 주소(virtual IP address)를 맡아 트래픽을 전달하고 있음을 나타내는 HSRP 라우터 상태는 무엇입니까?

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. 라우터 설정 모드에서 network 명령문을 사용하여, 정확히 10.1.1.0/24 서브넷의 인터페이스에 OSPF 프로세스 1을 활성화하고 area 0에 할당하는 명령 순서는 무엇입니까?

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, 그다음 ip ospf 1 area 0

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

C. ip routing ospf 1 area 0

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

---

14. 플로팅 정적 경로(floating static route)의 목적은 무엇입니까?

What is the purpose of a floating static route?

A. 동일 비용의 여러 경로로 트래픽을 로드 밸런싱하기 위해

B. 라우팅 프로토콜 사이에서 자동으로 재분배하기 위해

C. 주 경로(primary route)에 장애가 생겼을 때만 사용되는 백업 경로를 제공하기 위해

D. 인터넷으로 가는 기본 경로(default route)를 제공하기 위해

---

15. 같은 이더넷 세그먼트에 있는 두 OSPF 라우터의 설정이 R1(priority 100, RID 10.1.1.1), R2(priority 100, RID 192.168.1.1)입니다. 두 라우터가 동시에 부팅한다고 가정할 때 DR이 되는 라우터는 무엇입니까?

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. 어느 쪽도 되지 않는다. 우선순위가 같으면 교착 상태가 되기 때문이다

B. R1. Router ID가 더 낮기 때문이다

C. R2. 192.168.1.1이 사설 IP 주소이기 때문이다

D. R2. Router ID가 더 높기 때문이다

---

16. 라우터가 목적지 네트워크 172.20.0.0/16을 OSPF, EIGRP, static 경로의 세 가지 소스로 학습했습니다. 라우터는 어떤 경로를 라우팅 테이블에 설치합니까?

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 경로

B. 세 경로 모두(로드 밸런싱)

C. static 경로

D. OSPF 경로

---

17. area 10의 OSPF 라우터가 ABR로부터 네트워크 172.20.0.0/16을 알리는 Type 3 LSA를 받았습니다. 이후 ASBR로부터 같은 네트워크 172.20.0.0/16을 알리는 Type 5 LSA도 받았습니다. 두 LSA 모두 유효한 metric을 가지고 있습니다. 어떤 경로가 설치됩니까?

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 inter-area 경로. intra-area와 inter-area 경로가 external 경로보다 우선하기 때문이다

B. 어느 경로도 설치되지 않는다. OSPF는 같은 프리픽스를 inter-area와 external로 동시에 광고할 수 없기 때문이다

C. 총 비용이 같으면 두 경로 모두 ECMP(equal-cost multipath)로 설치된다

D. Type 5 external 경로. LSDB에서 Type 5 LSA가 Type 3 LSA보다 우선순위가 높기 때문이다

---

18. 이더넷 인터페이스에서 기본 OSPF 네트워크 유형(network type)은 무엇입니까?

Which OSPF network type is the default on Ethernet interfaces?

A. Non-broadcast

B. Point-to-point

C. Broadcast

D. Point-to-multipoint

---

19. 브로드캐스트 네트워크의 OSPF 라우터에 인터페이스 priority가 0으로 설정되어 있습니다. 이 라우터는 DR과 인접 관계를 성공적으로 맺었습니다. 이 라우터는 DR과 어떤 OSPF 상태에 도달합니까?

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 상태. hello 패킷은 교환하지만 양방향 통신이 확인되지 않았기 때문이다

B. EXSTART 상태. DBD 교환이 시작되지만 DR 자격이 없으면 완료될 수 없기 때문이다

C. FULL 상태. priority 0은 DR/BDR 선출만 막을 뿐 인접 관계 형성은 막지 않기 때문이다

D. 2-WAY 상태. priority가 0인 라우터는 브로드캐스트 네트워크에서 FULL 인접 관계를 만들 수 없기 때문이다

---

20. 같은 이더넷 세그먼트에 있는 세 OSPF 라우터의 설정이 R1(priority 100, RID 1.1.1.1), R2(priority 100, RID 2.2.2.2), R3(priority 100, RID 3.3.3.3)입니다. 모든 라우터가 동시에 부팅합니다. 인접 관계가 형성된 후 올바른 설명은 무엇입니까?

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. R1이 DR, R2가 BDR, R3은 DROTHER가 된다

B. MAC 주소가 가장 높은 라우터가 DR이 된다

C. R2가 DR이 된다. Router ID가 중간값이기 때문이다

D. R3이 DR, R2가 BDR, R1은 DROTHER가 된다

네트워크 액세스

21. 레거시 802.1D Spanning Tree Protocol의 blocking, listening, disabled 포트 상태를 가장 직접적으로(most directly) 하나로 합친 Rapid PVST+(IEEE 802.1w) 포트 상태는 무엇입니까?

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. 동적 EtherChannel 협상을 제공하며 IEEE 표준인 프로토콜은 무엇입니까?

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

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

---

23. 네트워크 관리자가 Cisco 스위치의 VLAN 할당을 확인하려고 합니다. VLAN ID, 이름, 상태, 할당된 access 포트를 VLAN 중심의 간결한 표로 보여 주는 명령은 무엇입니까?

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. Spanning Tree Protocol에서 Designated Port(지정 포트)의 역할은 무엇입니까?

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

A. BPDU만 수신한다
B. 루프를 막으려고 트래픽을 차단한다
C. 루트 브리지에 직접 연결된다
D. 네트워크 세그먼트에서 트래픽을 전달한다

---

25. Rapid PVST+에서 한 스위치의 포트 두 개가 같은 공유 이더넷 세그먼트에 연결되어 있고, 그 세그먼트의 designated 포트는 둘 중 하나만 될 수 있습니다. 같은 스위치에서 designated 포트가 되지 못한 두 번째 포트에는 어떤 역할이 할당됩니까?

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. Cisco 스위치에서 IEEE 802.1Q 트렁크가 기본 native VLAN 태깅 동작을 사용합니다. native VLAN에 속하는 일반 데이터 프레임은 어떻게 전송됩니까?

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. VLAN 태그 대신 MPLS 레이블을 붙여서
B. Layer 3 IP 패킷으로만
C. 802.1Q VLAN 태그 2개를 붙여서
D. 802.1Q VLAN 태그 없이

---

27. 엔지니어가 VLAN 20의 STP 루트 브리지가 어느 스위치인지 확인해야 합니다. 이 정보를 제공하는 명령은 무엇입니까?

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. 동작하려면 무선 LAN 컨트롤러(WLC)가 필요한 무선 액세스 포인트(AP) 모드는 무엇입니까?

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

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

---

29. 수렴(convergence) 시간을 최소화하려면 최종 사용자 장치에 연결된 포트에 어떤 STP 기능을 활성화해야 합니까?

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. STP에서 루트 브리지를 선출할 때 가장 우선하는 기준은 무엇입니까?

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

A. 가장 낮은 MAC 주소
B. 가장 낮은 브리지 priority
C. 가장 높은 브리지 priority
D. 가장 빠른 포트 속도

보안 기초

31. 무선 네트워크에 비밀번호 기반 개인용(personal) 인증이 필요하고 모든 클라이언트가 WPA3를 지원합니다. 수동적인 오프라인 비밀번호 추측 공격에 가장 강한 보호를 제공하는 보안 프로토콜은 무엇입니까?

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. SAE를 사용하는 WPA3-Personal
B. 128비트 키의 WEP
C. AES-CCMP를 사용하는 WPA2-Enterprise
D. TKIP를 사용하는 WPA2-Personal

---

32. 네트워크가 라우터 인터페이스에 inbound로 적용한 extended ACL 110을 사용합니다. 첫 번째 ACE는 'access-list 110 deny tcp any any eq 23'입니다. 이 ACE는 어떤 트래픽을 차단합니까?

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. 모든 출발지에서 모든 목적지로 가는 SSH 트래픽
B. 모든 출발지에서 모든 목적지로 가는 모든 TCP 트래픽
C. 모든 출발지에서 모든 목적지로 가는 Telnet 트래픽
D. 라우터 인터페이스로 향하는 Telnet 트래픽만

---

33. 회사가 인터넷을 통해 두 사이트를 VPN으로 연결해야 합니다. 이 연결은 멀티캐스트 트래픽과 여러 프로토콜(IPv4, IPv6, IPX)을 지원해야 합니다. 가장 적합한(MOST appropriate) VPN 기술은 무엇입니까?

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. IPsec tunnel mode만 사용

---

34. 네트워크 보안에서 AAA는 무엇의 약자입니까?

What does AAA stand for in network security?

A. Access, Authentication, and Administration
B. Authentication, Accounting, and Auditing
C. Authentication, Authorization, and Accounting
D. Authorization, Access, and Auditing

---

35. 관리자가 192.168.10.0/24 네트워크에서 10.1.1.100의 서버로 가는 IP 트래픽을 차단해야 합니다. 다른 목적지로 가는 트래픽에 미치는 영향을 최소화하려면 standard ACL을 어느 라우터 인터페이스에 적용해야 합니까?

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. 서버가 연결된 스위치 포트
B. 출발지(192.168.10.0/24)에 가장 가까운 라우터 인터페이스
C. 중간에 있는 모든 라우터 인터페이스
D. 목적지(10.1.1.100)에 가장 가까운 라우터 인터페이스

---

36. 기술자가 라우터의 running configuration에서 'enable secret 5 1mERr$hx5rVt7rPNoS4wqbXKX7m0'를 봤습니다. 이 enable secret 비밀번호에는 어떤 종류의 암호화가 쓰였습니까?

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 해시(type 8)
B. MD5 해시(type 5)
C. Scrypt 해시(type 9)
D. 단순 Vigenère 암호(type 7)

---

37. 회사는 Cisco 라우터와 스위치에 접속하는 모든 네트워크 관리자에 대해 중앙 집중식 인증, 전체 명령 accounting, 명령별 authorization을 요구합니다. 이 요구 사항에 가장 적합한(BEST) AAA 프로토콜은 무엇입니까?

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. 로컬 인증

---

38. extended ACL에 'access-list 101 permit tcp any any established' 명령문 하나만 있습니다. 203.0.113.50에서 198.51.100.10의 443번 포트로 가는, SYN 플래그만 설정된 TCP 패킷이 ACL 101이 inbound로 적용된 인터페이스에 도착합니다. 이 패킷은 어떻게 됩니까?

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. TCP 연결을 맺는 과정의 일부이므로 허용된다
B. SYN 플래그만으로는 'established' 키워드와 일치하지 않으므로 거부된다
C. TCP 상태 테이블에 해당 항목이 있을 때만 허용된다
D. extended ACL은 TCP 포트 443을 허용할 수 없으므로 거부된다

---

39. 회사는 중앙 집중식 인증, 전체 명령 accounting, 전체 인증 payload 암호화를 요구합니다. 이 요구 사항을 가장 잘 충족하는(BEST) AAA 프로토콜은 무엇입니까?

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. 로컬 데이터베이스 인증
D. TACACS+

---

40. extended ACL에서 호스트 192.168.5.45의 트래픽만 허용해야 합니다. 올바른 와일드카드 마스크(wildcard mask)는 무엇입니까?

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

자동화와 프로그래밍

41. 네트워크 설계자가 SDN(Software-Defined Networking) 솔루션을 설계하고 있습니다. SDN 컨트롤러가 프로그래밍한 규칙에 따라 패킷 전달 동작을 실행하는 plane은 무엇입니까?

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. Management plane
B. Application plane
C. Data plane
D. Control plane

---

42. REST API가 인터페이스 조회에 대해 다음 JSON 응답을 반환합니다. {"status": "up", "speed": "1000", "duplex": "full"} Python 스크립트가 speed 값으로 수학 계산을 하려다 TypeError가 발생합니다. 문제는 무엇입니까?

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. JSON에 필수 "unit" 필드가 없다
B. API가 잘못된 JSON 구문을 반환했다
C. speed 값이 정수가 아니라 문자열이다
D. Python의 JSON 라이브러리가 중첩 객체를 지원하지 않는다

---

43. 회사가 기존 3계층(three-tier) 캠퍼스 네트워크에서 Cisco SD-Access 패브릭으로 이전합니다. 가장 중요한(PRIMARY) 아키텍처 변화는 무엇입니까?

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

A. 무선 전용 접속 덕분에 물리적 케이블링 요구가 50% 줄어든다
B. 기존 VLAN 대신 VXLAN 오버레이로 세그멘테이션한다
C. 라우팅 프로토콜이 꺼지고 모든 전달 결정을 스위치가 내린다
D. 정책 적용을 위해 모든 트래픽이 인터넷을 경유한다

---

44. 네트워크 프로그래머빌리티(network programmability)에서 YANG 데이터 모델의 목적은 무엇입니까?

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

A. YANG은 큰 설정 파일을 압축해 더 빨리 전송하게 한다
B. YANG은 설정 및 운영 데이터의 구조와 제약 조건을 정의한다
C. YANG은 API 전송 중 설정 데이터를 암호화한다
D. YANG은 CLI 명령을 그래픽 워크플로로 대체한다

---

45. 엔지니어가 REST API로 Cisco 스위치에 새 VLAN을 만들려고 하는데 409 Conflict 상태 코드를 받았습니다. VLAN ID는 유효하고 허용 범위 안에 있습니다. 가장 가능성이 높은(MOST likely) 원인은 무엇입니까?

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. 스위치가 다른 설정 변경을 처리하는 중이다
B. 요청 payload에 잘못된 JSON 구문이 있다
C. 해당 ID의 VLAN이 이미 스위치에 있다
D. API 자격 증명에 충분한 권한이 없다

---

46. 다음 설정 조각이 올바르게 파싱되지 못하게 하는 JSON 구문 오류는 무엇입니까?
{"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 값은 큰따옴표 대신 작은따옴표를 써야 한다
B. vlan 값은 문자열로 따옴표에 넣어야 한다
C. 이 JSON은 구문상 올바르다
D. 배열은 대괄호 대신 소괄호를 써야 한다

---

47. 엔지니어가 ncclient 라이브러리를 쓰는 Python 스크립트로 NETCONF를 통해 설정을 푸시합니다. 스크립트는 연결에 성공하지만 edit-config 작업이 "missing-element" 오류로 실패합니다. XML payload는 형식이 올바릅니다. 가장 가능성이 높은(MOST likely) 원인은 무엇입니까?

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 모델이 필수 요소를 요구하는데 payload에 없다
B. XML의 namespace 선언이 잘못되었다
C. 장치가 writable-running capability를 지원하지 않는다
D. 대상 datastore가 다른 세션에 의해 잠겨 있다

---

48. 어떤 API가 설정 변경을 허용하기 전에 인증을 요구합니다. 일정 시간이 지나면 만료되는 토큰 기반 접근을 제공해 자격 증명 노출 위험을 줄이는 인증 방식은 무엇입니까?

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 community string
B. bearer 토큰을 쓰는 OAuth 2.0
C. Base64 인코딩을 쓰는 Basic 인증
D. SSH 공개 키 인증

---

49. Cisco 장치에 대한 REST API 호출이 다음 JSON을 반환합니다.
{"status": "success", "vlan_id": 100, "vlan_name": "Engineering", "active": true}

"active" 키의 데이터 타입은 무엇입니까?

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

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

A. Boolean
B. Object
C. String
D. Integer

---

50. 네트워크 자동화 스크립트가 VLAN을 삭제하는 REST API 요청을 보냈고 서버가 HTTP 상태 코드 204로 응답했습니다. 이것은 무엇을 나타냅니까?

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. 장치에서 VLAN을 찾을 수 없었다
B. 서버에서 내부 오류가 발생했다
C. 인증 실패로 요청이 거부되었다
D. 요청이 성공했고 반환되는 내용은 없다

정답

1. A VLSM에서는 서브넷이 겹치지 않게 할당해야 하며, 연속 할당은 필수가 아닙니다. /26은 .0부터 .63까지, /27은 .64부터 .95까지 사용하므로 처음으로 비어 있는 주소는 192.168.20.96입니다. /30은 전체 주소 4개, 사용 가능한 호스트 2개(2^2 - 2)입니다. 192.168.20.96/30은 .96부터 .99까지이고 경계도 맞습니다. .92/30은 /27 블록과 겹치고, .96/29는 호스트가 6개이며, .128/30은 가장 낮은 주소가 아닙니다.

2. D TCP의 유효 윈도우(effective window)는 혼잡 윈도우(32 KB)와 수신자 윈도우(24 KB) 중 작은 값인 24 KB입니다. 확인 응답을 받지 못한 데이터는 최대 24 KB까지 가능합니다. 이미 10 KB가 전송 중이므로 24 - 10 = 14 KB를 더 보낼 수 있습니다. 22 KB는 혼잡 윈도우에서 뺀 잘못된 값(32 - 10)이고, 24 KB는 전송 중인 데이터를 무시했으며, 32 KB는 수신자 제한을 무시했습니다.

3. D OUI는 48비트 MAC 주소의 앞 24비트(앞 3옥텟)이며 IEEE가 제조사를 구분하려고 할당합니다. 따라서 00-1A-2B가 정답입니다. 나머지 3옥텟(3C-4D-5E)은 제조사가 할당하며 각 인터페이스를 구분합니다. 00-1A는 16비트뿐이고, 2B-3C-4D-5E는 OUI와 장치 부분이 섞여 있습니다. 이 구조를 알면 장애를 처리할 때 제조사를 확인할 수 있습니다.

4. C 스위치는 마이크로세그멘테이션(microsegmentation)을 하므로 포트마다 충돌 도메인이 하나씩 생겨 모두 24개입니다. VLAN마다 브로드캐스트 도메인이 따로 생기므로 VLAN 3개는 브로드캐스트 도메인 3개입니다. 브로드캐스트 도메인 1개라는 보기는 VLAN 분리를 무시했고, 충돌 도메인 3개라는 보기는 충돌 도메인이 VLAN과 같다고 잘못 가정했습니다. 충돌 도메인 1개라는 보기는 스위치를 허브와 혼동했습니다.

5. C Cat 6A UTP는 10GBASE-T를 최대 100미터까지 지원하는 표준 케이블링 요건을 충족합니다. 누화(crosstalk) 특성이 개선되어 100미터 전 구간이 가능하고, 제대로 설치하면 이 환경에도 적합합니다. Cat 6은 설치 조건에 따라 대체로 55미터까지만 지원하므로 75미터에 못 미칩니다. Cat 5e는 75미터 10GBASE-T용으로 규정되지 않았습니다. Cat 6 STP는 EMI 차폐는 더 좋지만, 차폐만으로 75미터에서 10GBASE-T 채널 성능이 보장되지는 않습니다.

6. B 네 네트워크의 전체 범위는 172.16.32.0부터 172.16.95.255까지입니다. 세 번째 옥텟 32와 95는 첫 비트만 같으므로 공통 프리픽스는 17비트이고, 가장 작은 요약은 172.16.0.0/17(172.16.0.0~172.16.127.255)입니다. 이 요약은 필요 이상의 주소도 포함합니다. 네 네트워크를 정확히 요약하려면 172.16.32.0/19와 172.16.64.0/19가 필요합니다. 172.16.32.0/19만 쓰면 앞의 두 네트워크만 포함하고, 172.16.32.0/18은 올바른 /18 경계가 아니고, /16은 /17보다 더 넓습니다.

7. A 스위치는 활성 포트마다 충돌 도메인을 하나씩 만듭니다. 장치 8대가 연결되어 있으므로 충돌 도메인은 8개이고, 버퍼링과 full-duplex 덕분에 포트 사이에 충돌이 생기지 않습니다. 같은 VLAN의 모든 포트는 기본적으로 브로드캐스트 도메인 1개를 공유합니다. 충돌 도메인 24개는 연결되지 않은 포트까지 센 값이고, 충돌 도메인 1개와 브로드캐스트 도메인 1개는 허브의 특성입니다.

8. C CIDR(Classless Inter-Domain Routing)은 RFC 791에서 도입된 Class A/B/C의 엄격한 구조를 없앴습니다. CIDR에서는 첫 옥텟 값과 상관없이 어떤 네트워크에도 /16 마스크를 쓸 수 있습니다(예: 10.0.0.0/16). "Class B"는 옛 표기일 뿐이고, 라우터는 프리픽스 길이(/16)만 봅니다. 옛 Class B 범위에는 지금도 쓰이는 공인 IP가 많으므로 라우팅되지 않는다는 보기는 틀렸습니다. 사설 주소(RFC 1918)는 CIDR과 별개이고, VLSM은 서브네팅 기법이지 CIDR의 요구 사항이 아닙니다.

9. C 11001000을 변환하면 (1×128) + (1×64) + (0×32) + (0×16) + (1×8) + (0×4) + (0×2) + (0×1) = 128 + 64 + 8 = 200입니다. 서브넷 마스크와 IP 주소를 이해하는 데 꼭 필요한 기술입니다. 192는 11000000, 208은 11010000, 224는 11100000입니다. 자주 쓰는 옥텟 값(128, 192, 224, 240, 248, 252, 254, 255)은 바로 변환할 수 있어야 서브네팅 계산이 쉽습니다.

10. D IEEE 802.3ab에 따르면 Cat 5e 또는 Cat 6 UTP 케이블에서 1000BASE-T(기가비트 이더넷)의 최대 케이블 길이는 100미터(328피트)입니다. 수평 케이블 최대 90미터에 패치 케이블 10미터를 더한 길이입니다. 185미터는 10BASE2 얇은 동축 케이블의 한계이고, 500미터는 10BASE5 굵은 동축 케이블의 한계입니다. 2킬로미터는 1000BASE-LX의 표준 단일 모드(single-mode) 거리도 아니며, 그 거리는 5킬로미터입니다. 구리선에서 100미터를 넘으면 감쇠와 타이밍 문제로 성능이 떨어집니다.

11. B Cisco 라우팅에서는 항상 가장 긴 프리픽스 일치(longest prefix match)가 administrative distance(AD)보다 우선합니다. 192.168.0.50은 세 프리픽스에 모두 속하지만 /24가 가장 구체적이므로, static 경로의 AD(1)보다 EIGRP의 AD(90)가 높아도 EIGRP 경로가 사용됩니다. AD는 프리픽스 길이가 같은 경로끼리만 비교합니다. /16 static은 가장 덜 구체적이라 집니다. 프리픽스 길이가 다르면 로드 밸런싱도 하지 않습니다.

12. D Active 상태는 HSRP 라우터가 현재 가상 IP 주소로 가는 패킷을 전달하고 해당 주소에 대한 ARP 요청에 응답한다는 뜻입니다. HSRP 그룹마다 한 번에 하나의 라우터만 Active가 될 수 있습니다. Standby는 백업 상태로, Active 라우터를 감시하다가 장애가 나면 역할을 넘겨받습니다. Listen은 HSRP 광고를 받지만 Active도 Standby도 아닌 상태입니다. Speak은 Active와 Standby를 정하려고 우선순위를 교환하는 중간 상태입니다.

13. D 정답은 'router ospf 1, 그다음 network 10.1.1.0 0.0.0.255 area 0'입니다. 전통적인 방법은 OSPF 프로세스 아래에서 와일드카드 마스크와 함께 network 명령을 쓰는 것입니다. 이 명령은 정확히 10.1.1.0/24 범위의 인터페이스를 area 0에 넣습니다. 'ip ospf 1 area 0'은 올바른 인터페이스 수준 설정이지만 문제가 요구한 router 설정 모드 방식이 아닙니다. 255.255.255.0을 와일드카드 마스크로 쓴 보기는 서브넷과 정확히 일치하지 않고, 'ip routing ospf'는 잘못된 구문입니다.

14. C 플로팅 정적 경로는 주 경로보다 administrative distance가 높게(예: 기본값 1 대신 5) 설정되어 있어서, 주 경로를 쓸 수 없을 때만 라우팅 테이블에 들어갑니다. 평소에는 OSPF(AD 110) 같은 동적 라우팅 프로토콜 경로를 우선하게 하거나 dial-on-demand 백업 링크에 자주 씁니다. 로드 밸런싱은 동일 비용 경로가 있어야 가능하고, 프로토콜 사이의 재분배는 별개의 과정입니다. 인터넷을 가리킬 수는 있지만 그것이 본래 목적은 아니며, 핵심은 높은 AD로 만드는 백업 전용 동작입니다.

15. D OSPF 우선순위가 같으면(둘 다 100) 가장 높은 Router ID가 우선합니다. OSPF는 Router ID를 숫자로 비교하는데 192.168.1.1이 10.1.1.1보다 크므로 R2가 DR이 됩니다. 192.168.1.1이 사설 주소라는 사실은 관계없고, OSPF는 모든 32비트 RID를 똑같이 취급합니다. 우선순위가 같아도 교착 상태가 되지 않고 다음 기준으로 넘어갑니다. AD처럼 낮은 값이 이긴다고 생각하기 쉽지만, DR 선출에서는 priority가 높은 쪽, 그다음 RID가 높은 쪽이 이깁니다.

16. C Cisco 라우터는 소스가 다른 경로 중에서 administrative distance(AD)로 하나를 고릅니다. static은 AD 1(가장 신뢰), EIGRP는 90, OSPF는 110입니다. AD가 가장 낮은 경로가 선택되므로 static 경로가 이깁니다. OSPF는 static과 EIGRP보다 우선순위가 낮습니다. 로드 밸런싱은 AD와 metric이 모두 같은 경로가 여러 개일 때만 가능한데 여기서는 해당하지 않습니다. AD는 metric보다 먼저 비교합니다.

17. A OSPF의 경로 우선순위는 intra-area(Type 1/2) > inter-area(Type 3) > external Type 1(Type 5 E1) > external Type 2(Type 5 E2) 순서입니다. 같은 프리픽스를 광고해도 우선순위가 더 높은 Type 3 inter-area 경로가 이깁니다. Type 5 LSA의 우선순위가 높은 것이 아니며 external 경로는 항상 가장 낮습니다. ECMP는 같은 유형이고 비용이 같을 때만 적용됩니다. OSPF는 겹치는 광고를 받을 수 있고, 우선순위 규칙으로 선택합니다.

18. C 이더넷 같은 다중 접속(multi-access) 매체에서 OSPF의 기본 네트워크 유형은 Broadcast입니다. 이 모드에서는 인접 관계와 LSA flooding을 줄이려고 DR과 BDR을 선출합니다. Point-to-point는 serial 링크의 기본값이며 DR/BDR을 선출하지 않습니다. Non-broadcast는 Frame Relay hub-and-spoke 같은 NBMA에 쓰며 neighbor를 수동으로 설정해야 합니다. Point-to-multipoint도 NBMA용이지만 각 링크를 point-to-point처럼 다뤄 DR/BDR이 없습니다. 네트워크 유형이 다르면 인접 관계가 안 맺어지거나 라우팅 문제가 생길 수 있지만, 항상 인접 관계가 막히는 것은 아닙니다.

19. C priority가 0인 OSPF 라우터도 DR 및 BDR과 FULL 상태에 도달합니다. priority 0은 DR이나 BDR이 될 자격이 없고 선출에 참여하지 않는다는 뜻입니다. 브로드캐스트 네트워크에서는 모든 라우터가 DR, BDR과 LSDB 전체를 교환해 FULL 인접 관계를 맺고, 다른 DROTHER와는 2-WAY까지만 갑니다. priority는 선출 자격에만 영향을 줍니다. EXSTART와 INIT은 FULL 전의 중간 상태입니다.

20. D 모든 라우터의 OSPF priority가 같으면(100) Router ID가 기준이 됩니다. OSPF는 가장 높은 Router ID를 DR로, 두 번째로 높은 것을 BDR로 선출합니다. 따라서 R3(3.3.3.3)이 DR, R2(2.2.2.2)가 BDR, R1(1.1.1.1)이 DROTHER입니다. R1이 DR이라는 보기는 낮은 RID가 이긴다고 거꾸로 생각했고, '중간 RID' 규칙은 존재하지 않습니다. MAC 주소는 OSPF의 DR 선출과 관계없습니다.

21. C Rapid PVST+는 802.1D의 다섯 가지 포트 상태를 discarding, learning, forwarding의 세 가지로 줄였습니다. 레거시 blocking, listening, disabled 상태는 모두 포트가 프레임을 전달하지도 MAC 주소를 학습하지도 않으므로 discarding 하나로 합쳐졌습니다. Learning은 레거시 learning 상태와 같고 바뀌지 않았습니다. Forwarding도 레거시 forwarding 상태와 같습니다. Blocking은 RSTP에서 별도의 상태 이름으로 쓰지 않고 listening, disabled와 함께 discarding에 흡수되었습니다.

22. D LACP(Link Aggregation Control Protocol)는 IEEE 802.3ad에 정의된 업계 표준 프로토콜로, EtherChannel 벤들을 동적으로 협상합니다. 벤더 중립이라 다른 벤더의 스위치끼리도 동작합니다. PAgP(Port Aggregation Protocol)는 Cisco 전용(proprietary)이라 Cisco 장비끼리만 동작합니다. VTP(VLAN Trunking Protocol)는 VLAN 데이터베이스 동기화용이고, CDP(Cisco Discovery Protocol)는 neighbor 탐색용이라 둘 다 링크를 묶지 않습니다.

23. A 'show vlan brief'는 VLAN ID, 이름, 상태, 할당된 access 포트를 VLAN 중심의 간결한 표로 보여 줍니다. 'show interfaces status'는 포트 속도, duplex, VLAN을 포트 중심으로 보여 주므로 VLAN 이름과 VLAN 상태가 있는 VLAN 중심 표가 아닙니다. 'show running-config'는 모든 설정을 보여 주지만 VLAN 할당을 찾으려면 직접 읽어야 합니다. 'show ip interface brief'는 라우팅 인터페이스와 SVI의 Layer 3 IP 정보를 보여 주고 Layer 2 VLAN 소속은 보여 주지 않습니다.

24. D STP의 Designated Port는 연결된 네트워크 세그먼트(충돌 도메인)의 트래픽을 루트 브리지 쪽으로 전달하는 포트입니다. 세그먼트마다 하나씩 있으며, 그 세그먼트에서 루트 브리지까지 경로 비용이 가장 낮은 포트입니다. 루트가 아닌 스위치에서 루트 브리지 쪽으로 연결된 포트는 Designated Port가 아니라 Root Port입니다. 루프를 막으려고 트래픽을 차단하는 포트는 Blocking(RSTP에서는 Alternate/Backup) 상태입니다. 모든 포트가 BPDU를 받지만 designated 포트는 트래픽도 전달하며 Forwarding 상태입니다.

25. C RSTP의 backup 포트 역할은 한 스위치의 포트 두 개 이상이 같은 공유 세그먼트(보통 허브)에 연결되어 하나만 designated가 될 수 있을 때를 위한 것입니다. 밀려난 포트가 backup 포트가 되어 같은 스위치의 designated 포트를 대신할 수 있게 합니다. alternate 포트는 다른 스위치나 세그먼트를 통해 루트 브리지로 가는 백업 경로이며 root 포트에 대응하는 discarding 상태 포트입니다. Root port는 루트로 가는 최적 경로를 뜻하고, Edge port는 PortFast 방식의 종단 호스트 링크라 이중화 역할과 관계가 없습니다.

26. D native VLAN의 데이터 프레임은 기본적으로 태그 없이(untagged) 전송되므로 정답은 "802.1Q VLAN 태그 없이"입니다. "태그 2개"는 기본 native VLAN 동작이 아닙니다. MPLS 레이블은 일반 802.1Q 트렁크 전달과 관계가 없습니다. 트렁크는 이더넷 프레임을 전달하므로 "Layer 3 IP 패킷으로만"도 틀렸습니다.

27. C 'show spanning-tree vlan 20'은 루트 브리지 ID, 로컬 브리지 priority, 포트 역할과 상태를 포함한 VLAN 20의 STP 토폴로지를 보여 줍니다. 로컬 스위치가 루트인지, 아니면 루트의 브리지 ID가 무엇인지 분명히 알 수 있습니다. 'show vlan brief'는 VLAN 할당만 보여 주고 STP 역할은 보여 주지 않습니다. 'show interfaces trunk'는 트렁킹 상태와 허용 VLAN을 보여 줍니다. 'show spanning-tree summary'는 요약 정보만 보여 주며 VLAN 20의 루트 브리지를 알려 주지 않습니다.

28. A Lightweight AP(LAP)는 설정, 관리, 제어를 무선 LAN 컨트롤러(WLC)에 의존합니다. 컨트롤러와는 CAPWAP(Control and Provisioning of Wireless Access Points) 프로토콜로 통신하며, AP 자체의 설정과 펌웨어는 최소한입니다. Autonomous AP는 각 AP에 전체 설정이 있는 독립 장비라 컨트롤러가 필요 없습니다. Mesh는 AP끼리 무선으로 연결하는 배치 방식이라 lightweight(WLC 필요)일 수도 autonomous일 수도 있습니다. Bridge 모드는 유선 네트워크 두 개를 무선으로 연결하며 컨트롤러가 꼭 필요하지는 않습니다.

29. A PortFast는 링크가 올라오면 access 포트를 바로 Forwarding 상태로 전환해 30초의 Listening과 Learning 지연을 건너뜁니다. 루프를 만들지 않는 최종 사용자 장치(PC, 프린터 등)에는 안전합니다. UplinkFast와 BackboneFast는 업링크 장애와 간접 링크 장애를 위한 레거시 STP 최적화 기능이며 최종 사용자 포트용이 아닙니다. BPDU Guard는 PortFast 포트가 BPDU를 받으면(스위치가 잘못 연결된 경우) 포트를 비활성화하는 보안 기능이며 수렴 시간을 줄이지는 않고 PortFast와 함께 보호용으로 씁니다.

30. B STP의 루트 브리지는 가장 낮은 브리지 ID로 선출하며, 브리지 ID는 브리지 priority와 MAC 주소를 합친 값입니다. 브리지 priority를 먼저 비교하고 값이 가장 낮은 스위치가 루트 브리지가 됩니다. priority가 같으면 가장 낮은 MAC 주소로 결정합니다. priority는 낮은 값이 이기므로 '가장 높은 priority'는 틀렸습니다. '가장 낮은 MAC 주소'는 priority가 같을 때만 쓰는 기준입니다. 포트 속도는 루트 브리지 선출에 쓰이지 않고 포트 비용 계산에만 영향을 줍니다.

31. A "SAE를 사용하는 WPA3-Personal"은 WPA2-Personal의 PSK 인증 대신 SAE(Simultaneous Authentication of Equals)를 써서 forward secrecy와 수동적 오프라인 사전 공격에 대한 보호를 제공합니다. SAE 인증 후에도 4-way handshake로 트래픽 키를 만듭니다. 문제에서 클라이언트가 WPA3를 지원한다고 명시했습니다. WPA2-Enterprise는 개인용이 아닌 기업용 인증을 씁니다. TKIP는 2012년에 폐기된 전환용 프로토콜로 암호학적으로 약합니다. WEP는 키 길이와 관계없이 몇 분 안에 뚫릴 수 있습니다.

32. C 포트 23은 Telnet의 well-known 포트이므로 'eq 23'은 Telnet 세션과 일치합니다. 출발지와 목적지가 모두 'any'이므로 주소와 관계없이 Telnet 트래픽과 일치합니다. SSH는 22번 포트를 쓰므로 일치하지 않습니다. ACE는 tcp의 'eq 23'만 지정하므로 HTTP(80)나 HTTPS(443) 같은 다른 TCP 포트는 이 항목과 일치하지 않습니다. 그래서 정답은 "모든 출발지에서 모든 목적지로 가는 Telnet 트래픽"입니다. inbound 인터페이스 ACL은 통과 트래픽과 라우터 자신에게 오는 트래픽을 모두 필터링할 수 있습니다.

33. C GRE(Generic Routing Encapsulation) over IPsec은 멀티캐스트와 여러 프로토콜을 터널링하는 GRE의 장점에 IPsec의 암호화와 인증을 더한 방식입니다. GRE는 프로토콜에 독립적이어서 라우팅 프로토콜(OSPF, EIGRP), 멀티캐스트, IPv6를 지원합니다. IPsec tunnel mode만으로는 유니캐스트 IP 트래픽만 지원하고 멀티캐스트나 IP가 아닌 프로토콜은 안 됩니다. SSL VPN은 원격 접속 클라이언트용이며 site-to-site용이 아니고 멀티캐스트도 지원하지 않습니다. PPTP는 안전하지 않은 구식 프로토콜이며 현대적인 암호화 표준이 없습니다.

34. C AAA는 Authentication(사용자 신원 확인), Authorization(신원에 따른 권한 부여), Accounting(사용자 활동과 자원 사용 기록)의 약자입니다. Cisco 네트워크 보안의 기본 틀이며 TACACS+와 RADIUS 같은 프로토콜로 구현합니다. 'Access, Authentication, and Administration'은 authentication과 access control을 혼동하고 AAA에 없는 administration을 넣었습니다. 'Authorization, Access, and Auditing'은 accounting 대신 auditing을 넣었습니다. 'Authentication, Accounting, and Auditing'은 핵심인 authorization이 빠졌습니다.

35. D standard ACL은 출발지 IP 주소만으로 필터링하고 목적지 포트나 프로토콜은 구분하지 못합니다. 같은 출발지 네트워크에서 다른 목적지로 가는 정상 트래픽까지 막지 않으려면 standard ACL을 목적지에 가능한 한 가깝게 적용해야 합니다. 그래서 "목적지(10.1.1.100)에 가장 가까운 라우터 인터페이스"가 정답입니다. 출발지 가까이에 두면 192.168.10.0/24에서 다른 곳으로 가는 트래픽도 막힙니다. 모든 중간 인터페이스에 적용하면 자원을 낭비합니다. 일부 스위치는 포트 ACL을 지원하지만 문제는 라우터 인터페이스를 묻습니다. 규칙은 standard ACL은 목적지 근처, extended ACL은 출발지 근처입니다.

36. B '5'는 MD5 해시를 뜻합니다. 'enable secret'은 항상 해시를 쓰므로(되돌릴 수 있는 암호화가 아님) 'enable password'보다 안전합니다. Type 5는 MD5(구식이지만 여전히 흔함)입니다. Type 7은 'service password-encryption'이 line 비밀번호에 쓰는 약한 Vigenère 암호라 쉽게 복원됩니다. Type 8은 PBKDF2-SHA256, type 9는 scrypt로 둘 다 더 강한 최신 알고리즘입니다. enable secret 뒤의 숫자가 해시 알고리즘을 나타내고, 긴 문자열이 해시된 비밀번호입니다.

37. A TACACS+는 authentication, authorization, accounting을 별도 프로세스로 분리하고 비밀번호뿐 아니라 전체 payload를 암호화하므로 정답입니다. 특히 명령별 authorization을 지원해 사용자마다 실행할 수 있는 명령을 세밀하게 제어할 수 있습니다. RADIUS는 authentication과 authorization을 합치고 주로 UDP를 쓰므로 장비 관리보다 네트워크 접근 제어에 더 맞습니다. 로컬 인증은 여러 장비를 중앙에서 관리할 수 없습니다. Kerberos는 티켓 기반 인증 프로토콜이라 명령별 authorization과 명령 accounting을 함께 제공하지 못합니다.

38. B Cisco ACL의 'established' 키워드는 ACK 또는 RST 플래그가 설정된 TCP 패킷과 일치하며, SYN만 있는 패킷과는 일치하지 않습니다. TCP handshake의 첫 패킷인 순수 SYN은 ACK도 RST도 없으므로 이 명령문과 일치하지 않고, 끝의 암시적 거부(implicit deny)에 걸려 버려집니다. 'established'는 돌아오는 트래픽(ACK 응답, RST)은 허용하지만 새로운 inbound 연결 시도(SYN만)는 막습니다. Cisco IOS ACL은 stateless라 TCP 상태 테이블이 없으며(그것은 ASA 같은 stateful 방화벽의 기능), 패킷마다 TCP 플래그만 봅니다.

39. D TACACS+는 비밀번호만이 아니라 전체 payload를 암호화하고 authentication, authorization, accounting을 분리해서 명령 수준의 세밀한 accounting을 제공합니다. RADIUS는 패킷 안의 비밀번호 필드만 암호화하고 authentication과 authorization을 합치므로 상세한 명령 accounting에 덜 적합합니다. 로컬 데이터베이스 인증은 장비마다 사용자 DB를 따로 두어 중앙 집중이 안 됩니다. Kerberos는 single sign-on 프로토콜로 CCNA 수준의 Cisco 장비 AAA에는 흔히 쓰이지 않습니다. TACACS+는 TCP 49번 포트, RADIUS는 UDP 1812와 1813을 씁니다.

40. A 와일드카드 마스크 0.0.0.0은 단일 호스트와의 정확한 일치를 뜻합니다. 모든 비트가 정확히 같아야 하기 때문입니다(0 = 반드시 일치, 1 = 상관없음). ACL 구문의 'host 192.168.5.45'와 같습니다. 255.255.255.255는 모든 비트를 신경 쓰지 않으므로 'any'이며 모든 주소와 일치합니다. 0.0.0.255는 앞의 세 옥텟은 일치시키고 네 번째 옥텟은 무엇이든 허용하므로 /24 서브넷입니다. 255.255.255.0은 필요한 것의 반대이며 이 목적에는 맞지 않습니다. 와일드카드 마스크는 서브넷 마스크의 반대입니다.

41. C "Data plane"(forwarding plane)은 SDN 컨트롤러가 설치한 flow table과 정책에 따라 전달 동작을 실행합니다. 기존 네트워크에서는 control plane이 라우팅 결정을 내리지만, SDN에서는 이 로직이 컨트롤러에 집중되고 장치의 data plane은 컨트롤러가 프로그래밍한 규칙대로 패킷을 전달하기만 합니다. Management plane은 장치 설정과 모니터링을 담당합니다. Application plane은 northbound API로 컨트롤러와 상호작용하는 애플리케이션이며, 실제 패킷 전달은 data plane에서 일어납니다.

42. C "1000"이 따옴표로 묶여 있으므로 JSON에서 문자열(string)입니다. Python의 json.loads()는 이 타입을 그대로 유지하므로 speed + 2 같은 산술은 TypeError를 일으킵니다. int(data['speed'])로 변환하면 해결됩니다. "unit" 필드가 없어도 TypeError가 아니라 접근할 때 KeyError가 나거나 단지 메타데이터가 없을 뿐입니다. JSON 구문은 올바르고, Python의 json 라이브러리는 중첩 객체를 완전히 지원합니다. REST API는 일관성을 위해 숫자를 문자열로 반환하는 경우가 많으므로 계산 전에 타입을 확인하고 변환하세요.

43. B SD-Access는 물리적인 IP 언더레이 위에 VXLAN(Virtual Extensible LAN) 오버레이 터널로 논리적 네트워크 세그먼트(Virtual Network, VN)를 만들어, 기존 VLAN 기반 세그멘테이션을 대체하고 확장 가능한 정책 기반 마이크로 세그멘테이션을 가능하게 합니다. 언더레이는 패브릭 노드 사이의 IP 연결을 위해 여전히 라우팅 프로토콜(보통 IS-IS 또는 OSPF)을 씁니다. 트래픽은 패브릭 안에서 온프레미스로 유지되며 인터넷을 거칠 필요가 없습니다. SD-Access는 유선과 무선 단말을 모두 지원하므로 무선 전용이 필요하지 않고 케이블링도 여전히 필요합니다.

44. B YANG(Yet Another Next Generation)은 설정 및 운영 상태 데이터의 스키마를 정의하는 데이터 모델링 언어입니다. 어떤 데이터가 있는지, 타입, 유효 범위, 필수와 선택 필드, 관계를 정합니다. NETCONF와 RESTCONF 같은 프로토콜이 YANG 모델을 써서 컨트롤러와 장치 사이에 일관되고 검증된 데이터를 교환합니다. 암호화는 YANG이 하지 않고 전송 프로토콜(NETCONF는 SSH, RESTCONF는 HTTPS)이 담당합니다. YANG은 텍스트 기반 모델링 언어라 GUI를 제공하지 않고 데이터를 압축하지도 않습니다.

45. C HTTP 409 Conflict는 리소스 상태 충돌을 뜻하며, 여기서는 이미 있는 VLAN을 만들려 한 경우입니다. 409의 대표적인 사용 사례입니다. 권한이 부족하면 409가 아니라 401 Unauthorized나 403 Forbidden을 반환합니다. 잘못된 JSON 구문은 400 Bad Request가 됩니다. 동시에 설정을 바꾸면 충돌이 생기는 시스템도 있지만, REST 관례에서 409는 중복 리소스 생성 시도를 가리킵니다. 409를 일시적으로 쓸 수 없는 423 Locked와 혼동하거나, 모든 오류를 인증 문제로 생각하기 쉽습니다.

46. C 이 JSON은 구문상 올바릅니다. JSON은 문자열 키와 값에 작은따옴표가 아니라 큰따옴표를 요구하므로 hostname 형식은 맞습니다. vlan 값은 따옴표 없는 숫자(10)로 올바르게 표현되었고, JSON은 문자열(따옴표)과 숫자(따옴표 없음)를 구분합니다. 배열은 소괄호가 아니라 대괄호 [ ]를 써야 합니다. 불리언 true는 소문자에 따옴표가 없어 맞습니다. 흔한 오류는 작은따옴표 사용, 쉼표 누락, 마지막 쉼표, 괄호 불일치인데 여기에는 없습니다.

47. A "missing-element"는 YANG 모델 제약 위반을 나타냅니다. YANG 모델에서 정의한 필수 leaf나 container가 XML payload에 없다는 뜻으로, 스키마 검증이 실패한 것입니다. writable-running capability가 없다면 "missing-element"가 아니라 "operation-not-supported" 오류가 납니다. namespace가 틀리면 "unknown-namespace"나 파싱 오류가 납니다. datastore가 잠겨 있으면 "in-use"나 "resource-denied"를 반환합니다. NETCONF 오류 코드는 "missing-element" = 스키마 문제, "in-use" = 잠금 충돌, "invalid-value" = 제약 위반처럼 구체적인 실패 유형에 대응합니다.

48. B OAuth 2.0은 최초 인증 후 발급되는 시간 제한이 있는 bearer 토큰을 쓰며 토큰은 자동으로 만료되므로, 토큰이 유출되어도 악용할 수 있는 시간이 짧습니다. 애플리케이션은 자격 증명이 아니라 토큰을 API 요청마다 보냅니다. Basic 인증은 요청마다 사용자 이름과 비밀번호를 보내며, Base64는 암호화가 아닙니다. SSH 공개 키 인증은 CLI 접근에는 강력하지만 보통 HTTP 기반 REST API에는 쓰지 않고 키가 자동 만료되지도 않습니다. SNMP community string은 만료나 토큰 방식이 없는 평문 공유 비밀이라 현대 API 인증에는 약합니다.

49. A 따옴표 없는 소문자 true는 참/거짓을 나타내는 JSON 불리언 리터럴이므로 Boolean이 정답입니다. JSON에서 불리언 값은 따옴표 없이 true 또는 false로 씁니다. 문자열은 "Engineering"처럼 따옴표로 묶습니다. 정수는 100처럼 따옴표 없는 숫자입니다. 객체는 중괄호로 묶인 중첩 구조입니다. 자동화 스크립트에서 API 응답을 올바르게 파싱하려면 JSON 데이터 타입을 이해해야 합니다.

50. D HTTP 204 No Content는 요청이 성공적으로 처리되었고 응답 본문이 없다는 뜻입니다. 삭제가 됐다는 확인만으로 충분해서 데이터를 돌려주지 않는 DELETE 작업에서 흔합니다. VLAN이 없었다면 404 Not Found를 반환합니다. 인증 실패는 401 Unauthorized나 403 Forbidden, 서버 내부 오류는 500 Internal Server Error입니다. 자동화 스크립트의 오류 처리를 위해 HTTP 상태 코드를 이해해야 하며, 2xx는 성공, 4xx는 클라이언트 오류, 5xx는 서버 오류를 뜻합니다.

핵심 영어 단어

subnet mask	서브넷 마스크	IP 주소에서 네트워크 부분과 호스트 부분을 나누는 값
VLSM	가변 길이 서브넷 마스크	서브넷마다 필요한 크기로 마스크 길이를 다르게 쓰는 방법
CIDR	클래스 없는 주소 지정	클래스 대신 프리픽스 길이로 네트워크를 나타내는 방식
usable host address	사용 가능한 호스트 주소	네트워크 주소와 브로드캐스트 주소를 뺀, 장비에 줄 수 있는 주소
route summarization	경로 요약	여러 네트워크를 더 짧은 프리픽스 하나로 묶어 알리는 것

collision domain	충돌 도메인	동시에 보낸 프레임이 서로 부딪칠 수 있는 범위
broadcast domain	브로드캐스트 도메인	브로드캐스트 프레임 하나가 도달하는 범위
OUI	제조사 식별자(OUI)	MAC 주소 앞 24비트로, IEEE가 제조사에 배정한 값
congestion window	혼잡 윈도우	네트워크 혼잡을 고려해 TCP 송신자가 정하는 전송량 한도
VLAN	가상 LAN	스위치 포트를 논리적으로 나눈 별도의 브로드캐스트 도메인
access port	액세스 포트	VLAN 하나에 속하며 보통 단말을 연결하는 스위치 포트
trunk	트렁크	여러 VLAN의 트래픽을 함께 실어 나르는 링크
native VLAN	네이티브 VLAN	802.1Q 트렁크에서 기본적으로 태그 없이 보내는 VLAN
EtherChannel	이더채널	물리 링크 여러 개를 논리 링크 하나로 묶는 기술
LACP	링크 집계 제어 프로토콜	EtherChannel을 협상하는 IEEE 표준 프로토콜
root bridge	루트 브리지	스패닝 트리의 기준이 되는, 브리지 ID가 가장 낮은 스위치
designated port	지정 포트	한 세그먼트에서 트래픽을 전달하도록 뽑힌 포트
discarding	디스카딩, 폐기 상태	프레임을 전달하지도 MAC 주소를 배우지도 않는 RSTP 포트 상태
convergence	수렴	변화 뒤에 네트워크가 다시 안정된 상태가 되는 과정
PortFast	포트패스트	단말 포트를 대기 없이 바로 전달 상태로 바꾸는 STP 기능
WLC	무선 LAN 컨트롤러	경량 AP의 설정과 관리를 중앙에서 맡는 장비
routing table	라우팅 테이블	라우터가 목적지별 경로를 저장해 둔 표
longest prefix match	최장 프리픽스 일치	목적지와 맞는 경로 중 프리픽스가 가장 긴 것을 고르는 규칙
administrative distance	관리 거리	경로를 알려 준 출처의 신뢰도로, 낮을수록 우선인 값
metric	메트릭	같은 프로토콜 안에서 경로의 좋고 나쁨을 비교하는 값
floating static route	플로팅 정적 경로	관리 거리를 높여 주 경로가 사라질 때만 쓰는 정적 경로
adjacency	인접 관계	OSPF 라우터들이 링크 상태 정보를 주고받는 이웃 관계
designated router (DR)	지정 라우터	브로드캐스트 네트워크에서 인접 관계와 LSA 전파를 줄이려고 뽑는 OSPF 라우터
router ID	라우터 ID	OSPF 라우터를 구분하는 32비트 값
wildcard mask	와일드카드 마스크	0은 일치, 1은 무시를 뜻하는 ACL과 OSPF용 마스크
preemption	선점	우선순위가 높은 라우터가 Active 역할을 다시 가져오는 동작
access control list (ACL)	접근 제어 목록	패킷을 허용하거나 거부하는 조건을 순서대로 적은 목록
implicit deny	암시적 거부	ACL 끝에 보이지 않게 있는 모두 거부 규칙
authentication, authorization, accounting (AAA)	인증, 권한 부여, 계정 관리	누구인지, 무엇을 할 수 있는지, 무엇을 했는지 관리하는 체계

TACACS+	장비 관리용 AAA 프로토콜	TCP 49번 포트로 명령어별 권한 부여와 기록을 지원하는 프로토콜
NAT	네트워크 주소 변환	패킷의 IP 주소를 다른 주소로 바꾸는 기능
control plane	제어 평면	경로를 계산하고 전달 방법을 결정하는 부분
data plane	데이터 평면	정해진 규칙대로 패킷을 실제로 전달하는 부분
overlay	오버레이	물리 네트워크 위에 터널로 만든 논리 네트워크
data model	데이터 모델	데이터의 구조, 자료형, 제약을 정의한 틀

Examundo는 독립 사이트입니다. 시험을 만드는 기관과 제휴 관계가 없으며 승인을 받지도 않았습니다. 문제는 자체 제작한 것이며 실제 시험 문제가 아닙니다.
examundo.tech/ko/ccna/