examundo

Тест CCNA на русском

Вопросов с ответами: 50. Гиды и переводы сделала и проверила программа. Человек их пока не проверял.

Обновлено 25 ноября 2026 г. · examundo.tech/ru/ccna/

Основы сетей

1. Сетевой инженер выделил из блока 192.168.20.0/24 подсеть 192.168.20.0/26 для VLAN 10 и подсеть 192.168.20.64/27 для VLAN 20. Какая из свободных подсетей даёт ровно 2 доступных адреса хостов для двухточечного WAN-канала и имеет наименьший адрес сети?

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. Окно перегрузки (congestion window) TCP-отправителя равно 32 KB, а получатель объявляет размер окна 24 KB. У отправителя 10 KB отправленных данных ещё не подтверждены. Сколько ещё данных отправитель может передать, не дожидаясь подтверждения?

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. MAC-адрес сетевого устройства записан как 00-1A-2B-3C-4D-5E. Какая часть является идентификатором организации (Organizationally Unique Identifier, OUI)?

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. В коммутаторе 24 порта. Порты 1-8 входят в VLAN 10, порты 9-16 в VLAN 20, порты 17-24 в VLAN 30. Все порты работают в режиме access. Сколько в этом коммутаторе доменов коллизий (collision domains) и широковещательных доменов (broadcast domains)?

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 домена коллизий, 3 широковещательных домена
B. 24 домена коллизий, 1 широковещательный домен
C. 24 домена коллизий, 3 широковещательных домена
D. 1 домен коллизий, 3 широковещательных домена

---

5. Техник выбирает кабель для соединения 10GBASE-T между сервером и коммутатором на расстоянии 75 метров. В помещении умеренные электромагнитные помехи (EMI) от люминесцентных ламп. Какой тип кабеля соответствует МИНИМАЛЬНОМУ требованию?

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. Сетевой администратор суммирует маршруты (route summarization) для сетей 172.16.32.0/20, 172.16.48.0/20, 172.16.64.0/20 и 172.16.80.0/20. Какой наименьший единый суммарный маршрут включает все четыре сети?

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. В коммутаторе 24 порта, подключено 8 устройств. Сколько активных доменов коллизий и широковещательных доменов существует? (Считайте, что конфигурация по умолчанию, без 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 доменов коллизий, 1 широковещательный домен
B. 1 домен коллизий, 8 широковещательных доменов
C. 24 домена коллизий, 1 широковещательный домен
D. 1 домен коллизий, 1 широковещательный домен

---

8. Администратор просматривает документацию по IP-адресации от 1995 года и находит сеть с пометкой «Class B, 172.16.0.0/16». Почему при современной бесклассовой адресации (CIDR) обозначение «Class B» на практике вводит в заблуждение?

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. Сети класса B больше не маршрутизируются в интернете
B. CIDR требует, чтобы все сети класса B использовали маски переменной длины
C. Маску /16 можно применять к любому диапазону IP-адресов независимо от исторических границ классов
D. 172.16.0.0/16 относится к диапазону частных адресов, поэтому он бесклассовый по определению

---

9. Чему равно в десятичной системе двоичное число 11001000?

What is the decimal equivalent of the binary number 11001000?

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

---

10. Каково максимальное расстояние передачи для Ethernet 1000BASE-T по кабелю Cat 5e UTP?

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

A. 185 метров
B. 2 километра
C. 500 метров
D. 100 метров

IP-связность и маршрутизация

11. Маршрутизатор получил три маршрута к 192.168.0.0: 192.168.0.0/22 по OSPF, 192.168.0.0/24 по EIGRP и статический маршрут 192.168.0.0/16. Приходит пакет для адреса 192.168.0.50. Какой маршрут будет использован?

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. Маршрут OSPF /22, потому что у OSPF AD ниже, чем у EIGRP, а сам маршрут конкретнее статического
B. Маршрут EIGRP /24, потому что у него самое длинное совпадение префикса (самый конкретный)
C. Статический маршрут /16, потому что у статических маршрутов самое низкое значение AD и они всегда побеждают
D. Маршрутизатор распределяет нагрузку между всеми тремя маршрутами для максимального использования каналов

---

12. Какое состояние маршрутизатора HSRP означает, что он пересылает трафик от имени виртуального IP-адреса?

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. Какая последовательность команд включает процесс OSPF 1 для интерфейсов ровно в подсети 10.1.1.0/24 и относит их к области 0 с помощью команды network в режиме конфигурации маршрутизатора?

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

---

14. Для чего нужен плавающий статический маршрут (floating static route)?

What is the purpose of a floating static route?

A. Для балансировки нагрузки между несколькими путями с равной стоимостью

B. Для автоматической редистрибуции между протоколами маршрутизации

C. Чтобы иметь резервный маршрут, который используется только при отказе основного

D. Чтобы задать маршрут по умолчанию в интернет

---

15. Два маршрутизатора OSPF в одном сегменте Ethernet настроены так: R1 (приоритет 100, RID 10.1.1.1) и R2 (приоритет 100, RID 192.168.1.1). Оба загружаются одновременно. Какой маршрутизатор станет 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. Ни один, потому что равный приоритет создаёт взаимную блокировку

B. R1, потому что у него меньший Router ID

C. R2, потому что 192.168.1.1 относится к частным IP-адресам

D. R2, потому что у него больший Router ID

---

16. Маршрутизатор узнал о сети 172.20.0.0/16 из трёх источников: OSPF, EIGRP и статического маршрута. Какой маршрут он внесёт в таблицу маршрутизации?

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. Маршрут EIGRP

B. Все три маршрута для балансировки нагрузки

C. Статический маршрут

D. Маршрут OSPF

---

17. Маршрутизатор OSPF в области 10 получает от ABR LSA типа 3 с сетью 172.20.0.0/16. Позже он получает от ASBR LSA типа 5 с той же сетью 172.20.0.0/16. Метрики обоих LSA допустимы. Какой маршрут будет установлен?

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. Межобластной маршрут из LSA типа 3, потому что внутриобластные и межобластные маршруты предпочтительнее внешних

B. Ни один: в OSPF один и тот же префикс не может объявляться и как межобластной, и как внешний

C. Оба маршрута с балансировкой нагрузки (ECMP), если их полные стоимости равны

D. Внешний маршрут из LSA типа 5, потому что у LSA типа 5 в LSDB приоритет выше, чем у типа 3

---

18. Какой тип сети OSPF используется по умолчанию на интерфейсах Ethernet?

Which OSPF network type is the default on Ethernet interfaces?

A. Non-broadcast

B. Point-to-point

C. Broadcast

D. Point-to-multipoint

---

19. Интерфейс маршрутизатора OSPF в широковещательной сети имеет приоритет 0. Маршрутизатор успешно устанавливает соседство с DR. В какое состояние OSPF он переходит по отношению к DR?

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

A. Состояние INIT, потому что обмен hello-пакетами идёт, но двусторонняя связь не подтверждена

B. Состояние EXSTART, потому что обмен DBD начинается, но не может завершиться без права быть DR

C. Состояние FULL, потому что приоритет 0 запрещает только роль DR/BDR, а не установление соседства

D. Состояние 2-WAY, потому что маршрутизаторы с приоритетом 0 не могут установить соседство FULL в широковещательных сетях

---

20. Три маршрутизатора OSPF в одном сегменте Ethernet настроены так: R1 (приоритет 100, RID 1.1.1.1), R2 (приоритет 100, RID 2.2.2.2), R3 (приоритет 100, RID 3.3.3.3). Все загружаются одновременно. Какое утверждение верно после образования соседств?

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 становится DR, R2 становится BDR, R3 остаётся DROTHER

B. DR становится маршрутизатор с наибольшим MAC-адресом

C. R2 становится DR, потому что у него средний router ID

D. R3 становится DR, R2 становится BDR, R1 остаётся DROTHER

Доступ к сети

21. Какое состояние порта Rapid PVST+ (IEEE 802.1w) напрямую объединяет состояния blocking, listening и disabled из классического протокола связующего дерева 802.1D (Spanning Tree Protocol)?

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. Какой протокол обеспечивает динамическое согласование EtherChannel и является стандартом IEEE?

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

A. VTP

B. PAgP

C. CDP

D. LACP

23. Сетевому администратору нужно проверить назначение VLAN на коммутаторе Cisco. Какая команда выводит краткую таблицу по VLAN с идентификаторами, именами, состоянием и назначенными портами доступа (access)?

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. Какова роль назначенного порта (Designated Port) в протоколе связующего дерева (Spanning Tree Protocol, STP)?

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

A. Только получает BPDU
B. Блокирует трафик, чтобы предотвратить петли
C. Подключён напрямую к корневому мосту
D. Пересылает трафик в сегменте сети

---

25. В Rapid PVST+ два порта коммутатора подключены к одному общему сегменту Ethernet, и только один из них может стать назначенным портом этого сегмента. Какая роль назначается второму, неназначенному порту того же коммутатора?

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. На коммутаторе Cisco на транке IEEE 802.1Q действует поведение по умолчанию для native VLAN. Как транк передаёт обычные кадры данных из native VLAN?

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. С меткой MPLS вместо тега VLAN
B. Только как IP-пакеты уровня 3
C. С двумя тегами VLAN 802.1Q
D. Без тега VLAN 802.1Q

---

27. Инженеру нужно узнать, какой коммутатор является корневым мостом STP для VLAN 20. Какая команда даёт эту информацию?

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. Какой режим точки доступа Wi-Fi требует для работы контроллер беспроводной сети (wireless LAN controller, WLC)?

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

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

---

29. Какую функцию STP нужно включить на портах, подключённых к устройствам пользователей, чтобы сократить время сходимости?

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. Какой критерий имеет высший приоритет при выборе корневого моста в STP?

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

A. Наименьший MAC-адрес
B. Наименьший приоритет моста
C. Наибольший приоритет моста
D. Наибольшая скорость порта

Основы безопасности

31. Для беспроводной сети нужна аутентификация по паролю в режиме Personal, и все клиенты поддерживают WPA3. Какой протокол безопасности даёт самую сильную защиту от пассивного офлайн-подбора пароля?

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

A. WPA3-Personal с SAE
B. WEP с 128-битными ключами
C. WPA2-Enterprise с AES-CCMP
D. WPA2-Personal с TKIP

32. В сети применяется расширенный ACL 110 на входе интерфейса маршрутизатора. Первая запись: «access-list 110 deny tcp any any eq 23». Какой трафик блокирует эта запись?

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. Трафик SSH от любого источника к любому получателю
B. Весь трафик TCP от любого источника к любому получателю
C. Трафик Telnet от любого источника к любому получателю
D. Трафик Telnet только к интерфейсу самого маршрутизатора

33. Компании нужно соединить две площадки через интернет с помощью VPN. Соединение должно поддерживать многоадресный трафик (multicast) и несколько протоколов (IPv4, IPv6, IPX). Какая технология VPN подходит БОЛЬШЕ ВСЕГО?

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. Только IPsec в туннельном режиме

34. Как расшифровывается AAA в сетевой безопасности?

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. Администратору нужно заблокировать IP-трафик из сети 192.168.10.0/24 к серверу 10.1.1.100. На каком интерфейсе маршрутизатора следует разместить стандартный ACL, чтобы как можно меньше затронуть трафик к другим получателям?

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. На порту коммутатора, к которому подключён сервер

B. На интерфейсе маршрутизатора, ближайшем к источнику (192.168.10.0/24)

C. На всех промежуточных интерфейсах маршрутизаторов

D. На интерфейсе маршрутизатора, ближайшем к получателю (10.1.1.100)

---

36. Техник просматривает текущую конфигурацию маршрутизатора и видит строку «enable secret 5 1mERr$hx5rVt7rPNoS4wqbXKX7m0». Какой тип защиты используется для этого пароля enable secret?

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

A. Хеш SHA-256 (тип 8)

B. Хеш MD5 (тип 5)

C. Хеш scrypt (тип 9)

D. Простой шифр Виженера (тип 7)

---

37. Компании нужна централизованная аутентификация с полным учётом команд и авторизацией каждой команды для всех сетевых администраторов, работающих с маршрутизаторами и коммутаторами Cisco. Какой протокол AAA подходит ЛУЧШЕ ВСЕГО?

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. Локальная аутентификация

---

38. Расширенный ACL состоит только из одной записи «access-list 101 permit tcp any any established». Пакет TCP только с флагом SYN от 203.0.113.50 к 198.51.100.10, порт 443, приходит на интерфейс, где ACL 101 применён на входе. Что произойдёт с пакетом?

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. Пакет будет разрешён, потому что он участвует в установлении соединения TCP

B. Пакет будет отклонён, потому что один флаг SYN не соответствует ключевому слову established

C. Пакет будет разрешён, только если в таблице состояний TCP есть соответствующая запись

D. Пакет будет отклонён, потому что расширенные ACL не могут разрешать порт TCP 443

---

39. Компании нужна централизованная аутентификация с полным учётом команд и возможностью шифровать всё содержимое пакета аутентификации. Какой протокол AAA подходит ЛУЧШЕ ВСЕГО?

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. Аутентификация по локальной базе данных

D. TACACS+

---

40. В расширенном ACL нужно разрешить трафик только от хоста 192.168.5.45. Какая обратная маска (wildcard mask) правильная?

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

Автоматизация и программируемость

41. Сетевой архитектор проектирует решение на основе программно-определяемых сетей (Software-Defined Networking, SDN). Какая плоскость выполняет пересылку пакетов по правилам, заданным контроллером SDN?

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

A. Плоскость администрирования (management plane)
B. Плоскость приложений (application plane)
C. Плоскость данных (data plane)
D. Плоскость управления (control plane)

---

42. REST API возвращает на запрос об интерфейсе такой ответ JSON: {"status": "up", "speed": "1000", "duplex": "full"}. Скрипт на Python пытается выполнить математическую операцию со значением speed и получает TypeError. В чём проблема?

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. В JSON нет обязательного поля "unit"
B. API вернул недопустимый синтаксис JSON
C. Значение speed записано как строка, а не как целое число
D. Библиотека JSON в Python не поддерживает вложенные объекты

---

43. Компания переходит с традиционной трёхуровневой кампусной сети на фабрику Cisco SD-Access. Каково ГЛАВНОЕ архитектурное изменение?

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

A. Потребность в физических кабелях снижается на 50%, потому что доступ только беспроводной
B. Для сегментации вместо традиционных VLAN используются наложенные сети VXLAN
C. Протоколы маршрутизации отключены, и все решения о пересылке принимают коммутаторы
D. Весь трафик маршрутизируется через интернет для применения политик

---

44. Для чего нужна модель данных YANG в программируемых сетях?

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

A. YANG сжимает большие файлы конфигурации для быстрой передачи
B. YANG определяет структуру и ограничения данных конфигурации и рабочего состояния
C. YANG шифрует данные конфигурации при передаче через API
D. YANG заменяет команды CLI графическими рабочими процессами

---

45. Инженер получает код состояния 409 Conflict при попытке создать новую VLAN через REST API на коммутаторе Cisco. Идентификатор VLAN допустим и входит в разрешённый диапазон. Какая причина НАИБОЛЕЕ вероятна?

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. Коммутатор сейчас обрабатывает другое изменение конфигурации

B. Тело запроса содержит недопустимый синтаксис JSON

C. VLAN с таким идентификатором уже существует на коммутаторе

D. У учётных данных API недостаточно прав

---

46. Какая синтаксическая ошибка JSON помешала бы правильному разбору этого фрагмента конфигурации?
{"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. Значение hostname должно быть в одинарных кавычках, а не в двойных

B. Значение vlan должно быть в кавычках как строка

C. Этот JSON синтаксически корректен

D. Для массива нужны круглые скобки вместо квадратных

---

47. Инженер пишет скрипт на Python с библиотекой ncclient для отправки конфигураций по NETCONF. Скрипт успешно подключается, но операция edit-config завершается ошибкой «missing-element». XML-данные синтаксически корректны. Какая причина НАИБОЛЕЕ вероятна?

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. Модель YANG требует обязательный элемент, которого нет в отправленных данных

B. Объявление пространства имён (namespace) в XML неверно

C. Устройство не поддерживает возможность writable-running

D. Целевое хранилище (datastore) заблокировано другим сеансом

---

48. API требует аутентификации перед изменением конфигурации. Какой метод аутентификации даёт доступ по токену с ограниченным сроком действия и тем самым снижает риск раскрытия учётных данных?

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. Строки сообщества SNMP (community strings)

B. OAuth 2.0 с токенами bearer

C. Базовая аутентификация (Basic) с кодированием Base64

D. Аутентификация SSH по открытому ключу

---

49. REST API устройства Cisco возвращает такой JSON:
{"status": "success", "vlan_id": 100, "vlan_name": "Engineering", "active": true}

Какой тип данных у значения ключа "active"?

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

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

A. Boolean (логический)
B. Object (объект)
C. String (строка)
D. Integer (целое число)

---

50. Скрипт сетевой автоматизации отправляет запрос REST API на удаление VLAN, и сервер отвечает кодом состояния HTTP 204. Что это означает?

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. VLAN не найдена на устройстве
B. На сервере произошла внутренняя ошибка
C. Запрос отклонён из-за сбоя аутентификации
D. Запрос выполнен успешно, содержимое не возвращается

Правильный ответ

1. A При VLSM подсети выделяют без пересечений, а идти подряд они не обязаны. /26 занимает адреса с 192.168.20.0 по .63, /27 с .64 по .95, так что первый свободный адрес .96. В подсети /30 всего 4 адреса, из них 2 для хостов (2^2 - 2 = 2), и 192.168.20.96/30 выровнена по границе /30. Подсеть 192.168.20.92/30 пересекается с /27, 192.168.20.96/29 даёт 6 хостов, а 192.168.20.128/30 свободна, но её адрес не наименьший.

2. D Эффективное окно TCP равно меньшему из окна перегрузки (32 KB) и окна получателя (24 KB), то есть 24 KB. Столько неподтверждённых данных может быть в пути. Если 10 KB уже в пути, можно отправить ещё 24 - 10 = 14 KB. Ответ 22 KB получается, если вычесть 10 из окна перегрузки, 24 KB не учитывает уже отправленное, а 32 KB игнорирует лимит получателя.

3. D OUI занимает первые 24 бита (первые 3 октета) 48-битного MAC-адреса. Его присваивает IEEE, и он указывает на производителя, в этом примере 00-1A-2B. Остальные 3 октета (3C-4D-5E) производитель назначает сам, они определяют конкретный сетевой интерфейс. В варианте 00-1A только 16 бит, а 2B-3C-4D-5E захватывает и OUI, и часть устройства.

4. C Каждый порт коммутатора образует отдельный домен коллизий, поэтому их 24: коммутатор делит сеть на микросегменты. Каждая VLAN образует отдельный широковещательный домен, значит 3 VLAN дают 3 домена. Вариант с одним широковещательным доменом не учитывает VLAN, вариант с 3 доменами коллизий путает их с VLAN, а один домен коллизий был бы у концентратора (hub), не у коммутатора.

5. C Cat 6A UTP подходит для 10GBASE-T на расстояние до 100 метров. Cat 6 обычно рассчитан на 10GBASE-T только примерно до 55 метров, в зависимости от условий монтажа, а нужно 75. Cat 5e для 10GBASE-T на 75 метров не предназначен. Экранирование Cat 6 STP лучше защищает от помех, но само по себе не гарантирует, что канал Cat 6 выдержит 10GBASE-T на 75 метрах. У Cat 6A лучше характеристики перекрёстных наводок (crosstalk), поэтому он работает на все 100 метров.

6. B Сети занимают диапазон с 172.16.32.0 по 172.16.95.255. В третьем октете у 32 и 95 совпадает только первый бит, поэтому общий префикс равен 17 битам. Маршрут 172.16.0.0/17 покрывает адреса с 172.16.0.0 по 172.16.127.255, включая лишние: точно описать эти четыре сети одним префиксом нельзя. 172.16.32.0/19 охватывает только две первые сети, 172.16.32.0/18 не лежит на границе сети /18, а в /16 лишних адресов ещё больше.

7. A Коммутатор создаёт отдельный домен коллизий на каждый активный порт: 8 устройств дают 8 доменов. Коллизий между портами нет благодаря буферизации и полному дуплексу (full-duplex). Все порты в одной VLAN по умолчанию входят в один широковещательный домен, поэтому широковещательный кадр с любого порта доходит до всех остальных. Вариант с 24 доменами считает все порты, а не только активные. Один домен коллизий и один широковещательный домен бывают у концентратора (hub).

8. C CIDR (Classless Inter-Domain Routing) отменил жёсткое деление на классы A, B и C. Маску /16 можно применить к любой сети, например к 10.0.0.0/16 или 192.168.0.0/16, а маршрутизаторам важна только длина префикса. Многие публичные адреса лежат в бывшем диапазоне класса B (с 128.0.0.0 по 191.255.255.255) и маршрутизируются. Частные адреса (RFC 1918) с CIDR не связаны, а VLSM служит для деления на подсети и не является требованием CIDR.

9. C Переводим 11001000 в десятичную систему: (1×128) + (1×64) + (0×32) + (0×16) + (1×8) + (0×4) + (0×2) + (0×1) = 128 + 64 + 8 = 200. Число 192 записывается как 11000000, 208 как 11010000, 224 как 11100000. Такой перевод нужен для работы с масками подсетей и IP-адресами.

10. D Максимальная длина кабеля для 1000BASE-T (Gigabit Ethernet) по Cat 5e или Cat 6 UTP составляет 100 метров (328 футов) по стандарту IEEE 802.3ab: до 90 метров горизонтального кабеля и 10 метров патч-кордов. Предел 185 метров был у тонкого коаксиала 10BASE2, а 500 метров у толстого коаксиала 10BASE5. Одномодовый 1000BASE-LX работает до 5 километров, а не до 2. На меди дальше 100 метров мешают затухание сигнала и сбои синхронизации.

11. B В маршрутизации Cisco самое длинное совпадение префикса (longest prefix match) ВСЕГДА важнее административной дистанции (administrative distance, AD). Адрес 192.168.0.50 входит во все три префикса, но /24 самый конкретный, поэтому используется маршрут EIGRP, хотя его AD (90) выше, чем у статического (1). AD сравнивается, только когда длина префикса у маршрутов ОДИНАКОВАЯ. Статический /16 самый общий, он проигрывает. Балансировка нагрузки между разными длинами префиксов не применяется.

12. D В состоянии Active маршрутизатор HSRP пересылает пакеты для виртуального IP-адреса и отвечает на ARP-запросы к нему. В группе HSRP только один маршрутизатор может быть Active. Standby находится в резерве: он следит за Active и берёт работу на себя при его отказе. В состоянии Listen маршрутизатор получает сообщения HSRP, но не является ни Active, ни Standby. Speak бывает во время выборов, когда маршрутизаторы обмениваются приоритетами.

13. D Команду network вводят в процессе OSPF с обратной маской (wildcard mask). Запись network 10.1.1.0 0.0.0.255 area 0 выбирает интерфейсы ровно из диапазона 10.1.1.0/24 и помещает их в область 0. Настройка на интерфейсе (ip ospf 1 area 0) допустима, но в условии нужен режим конфигурации маршрутизатора. В варианте с 255.255.255.0 это число читается как обратная маска и даёт не ту подсеть, а синтаксис ip routing ospf 1 area 0 недопустим.

14. C У плавающего статического маршрута административная дистанция (administrative distance, AD) выше, чем у основного (например, 5 вместо 1), поэтому он попадает в таблицу маршрутизации только при недоступности основного. Так делают резервные каналы или отдают предпочтение динамическому протоколу (например, OSPF с AD 110). Для балансировки нужны маршруты с равной стоимостью, а редистрибуция настраивается отдельно. Такой маршрут может вести в интернет, но его суть в резерве.

15. D Если приоритеты OSPF равны (оба 100), решает наибольший Router ID. OSPF сравнивает их как числа: 192.168.1.1 больше, чем 10.1.1.1, поэтому DR становится R2. Частный адрес или нет, не важно: для OSPF все 32-битные RID одинаковы. Равный приоритет не блокирует выборы, просто применяется следующий критерий. Не путайте с AD, где лучше меньшее значение: в выборах DR побеждает больший приоритет, затем больший RID.

16. C Маршрутизаторы Cisco выбирают между маршрутами из разных источников по административной дистанции (AD). У статического маршрута AD равна 1 (самое высокое доверие), у EIGRP 90, у OSPF 110. Выбирается маршрут с наименьшей AD, поэтому побеждает статический. Балансировка нагрузки возможна, только если у маршрутов одинаковые AD и метрика, а здесь они разные. AD проверяется раньше метрики.

17. A OSPF предпочитает маршруты в таком порядке: внутриобластные (intra-area, типы 1 и 2), межобластные (inter-area, тип 3), внешние E1 (тип 5), внешние E2 (тип 5). Оба LSA объявляют один префикс, поэтому побеждает межобластной маршрут из типа 3. У LSA типа 5 приоритет НЕ выше: внешние маршруты идут последними. ECMP работает только для маршрутов ОДНОГО типа с равной стоимостью. Один префикс МОЖЕТ объявляться разными LSA, тогда маршрутизатор применяет эти правила.

18. C В Ethernet и других сетях с множественным доступом OSPF по умолчанию использует тип Broadcast и выбирает назначенный маршрутизатор (Designated Router, DR) и резервный (Backup Designated Router, BDR), чтобы сократить число соседств и рассылку LSA. Point-to-point стоит по умолчанию на последовательных каналах, без DR и BDR. Non-broadcast нужен в сетях NBMA (например, Frame Relay), соседей там задают вручную. Point-to-multipoint тоже для NBMA, но без DR и BDR.

19. C Маршрутизатор с приоритетом OSPF 0 достигает состояния FULL с DR и BDR. Приоритет 0 лишь не даёт ему стать DR или BDR, в выборах он не участвует. В широковещательной сети ВСЕ маршрутизаторы устанавливают соседство FULL с DR и BDR (обмениваются полными базами LSDB), а между собой остальные (DROTHER) остаются в 2-WAY. INIT и EXSTART служат промежуточными состояниями перед FULL.

20. D Если приоритеты OSPF равны (100), решает router ID. DR становится маршрутизатор с НАИБОЛЬШИМ router ID, BDR со вторым по величине. Значит, DR будет R3 (3.3.3.3), BDR будет R2 (2.2.2.2), а R1 (1.1.1.1) останется DROTHER. Наименьший RID здесь не побеждает, хотя в других протоколах меньшее значение бывает лучше. Правила «среднего router ID» не существует, а MAC-адреса в выборах DR не участвуют.

21. C Rapid PVST+ сокращает пять состояний 802.1D до трёх: discarding, learning и forwarding. Состояние discarding заменяет прежние blocking, listening и disabled, потому что в этих трёх состояниях порт не пересылает кадры и не изучает MAC-адреса. Learning соответствует прежнему состоянию learning и не изменилось. Forwarding тоже соответствует прежнему forwarding. Отдельного состояния blocking в RSTP нет, оно вошло в discarding.

22. D LACP (Link Aggregation Control Protocol), описанный в IEEE 802.3ad, это отраслевой стандарт для динамического согласования EtherChannel. Он не привязан к производителю и работает между коммутаторами разных вендоров. PAgP (Port Aggregation Protocol) принадлежит Cisco и работает только между устройствами Cisco. VTP (VLAN Trunking Protocol) синхронизирует базу VLAN, а не объединяет каналы. CDP (Cisco Discovery Protocol) нужен для обнаружения соседей.

23. A Команда show vlan brief показывает краткую таблицу по VLAN: идентификаторы, имена, состояние и назначенные порты доступа. show interfaces status выводит скорость, дуплекс и VLAN по портам, но без имён и состояния VLAN. В show running-config видны все команды конфигурации, и VLAN придётся искать среди них. show ip interface brief показывает данные уровня 3 для маршрутизируемых интерфейсов и SVI, а не принадлежность к VLAN на уровне 2.

24. D Назначенный порт (Designated Port) пересылает трафик своего сегмента сети (домена коллизий) в сторону корневого моста. В каждом сегменте он один: порт с наименьшей стоимостью пути до корневого моста. Порт некорневого коммутатора, ведущий к корневому мосту, называется корневым (Root Port). Порты, которые блокируют трафик от петель, находятся в состоянии Blocking (Alternate или Backup в RSTP). BPDU получают все порты, но назначенный ещё и пересылает трафик в состоянии Forwarding.

25. C Роль backup port в RSTP нужна именно для случая, когда два или больше портов одного коммутатора подключены к одному общему сегменту (обычно через концентратор). Назначенным может быть только один, второй становится backup и резервирует его на том же коммутаторе. Alternate port даёт запасной путь к корневому мосту через другой коммутатор или сегмент. Root port описывает лучший путь к корню, а edge port подключает конечный хост, как PortFast, и с резервированием не связан.

26. D По умолчанию кадры данных native VLAN идут по транку 802.1Q без тега (untagged). Два тега 802.1Q не относятся к поведению native VLAN по умолчанию. Метка MPLS не связана с обычной пересылкой по транку 802.1Q. Вариант «Только как IP-пакеты уровня 3» неверен, потому что транк пересылает кадры Ethernet.

27. C Команда show spanning-tree vlan 20 показывает топологию STP для VLAN 20: идентификатор корневого моста, приоритет локального моста, роли и состояния портов. Она прямо показывает, является ли локальный коммутатор корневым, или выводит ID корня. show vlan brief перечисляет назначения VLAN, но не роли STP. show interfaces trunk показывает состояние транка и разрешённые VLAN. show spanning-tree summary выводит лишь общие сведения и не определяет корневой мост для VLAN 20.

28. A Точки доступа lightweight (LAP) зависят от контроллера WLC: он отвечает за их настройку, управление и логику. Связь с ним идёт по протоколу CAPWAP (Control and Provisioning of Wireless Access Points). Точки autonomous настраивают по отдельности, контроллер им не нужен. В топологии mesh точки соединяются друг с другом по радио и могут быть как lightweight (с WLC), так и autonomous. Режим bridge соединяет по радио две проводные сети и сам по себе контроллера не требует.

29. A PortFast сразу переводит порт доступа в состояние Forwarding при появлении линка и пропускает задержку Listening и Learning в 30 секунд. Это безопасно для ПК и принтеров, которые не создают петель. UplinkFast и BackboneFast относятся к старым оптимизациям STP для отказов аплинков и непрямых отказов, не для портов пользователей. BPDU Guard отключает порт с PortFast, если на него пришёл BPDU (по ошибке подключён коммутатор), но сходимость не ускоряет.

30. B Корневой мост в STP выбирается по наименьшему идентификатору моста (bridge ID), который состоит из приоритета моста и MAC-адреса. Сначала сравнивается приоритет, и корневым становится коммутатор с наименьшим значением. При равенстве приоритетов решает наименьший MAC-адрес. Наибольший приоритет не подходит, потому что побеждают меньшие значения. Скорость порта на выбор корня не влияет, хотя она влияет на стоимость порта.

31. A WPA3-Personal использует метод Simultaneous Authentication of Equals (SAE) вместо PSK из WPA2-Personal. Он даёт прямую секретность (forward secrecy) и защиту от пассивных офлайн-атак по словарю. Ключи трафика после SAE по-прежнему создаёт четырёхэтапное рукопожатие (four-way handshake). В WPA2-Enterprise аутентификация корпоративная, а нужен Personal. TKIP в WPA2-Personal слабее и признан устаревшим в 2012 году. WEP взламывают за минуты при любой длине ключа.

32. C Порт 23 принадлежит Telnet, поэтому условие eq 23 отбирает сеансы Telnet. Источник и получатель указаны как any, значит адреса не важны. SSH использует порт 22, и эта запись его не затрагивает. Другие порты TCP, например HTTP (80) и HTTPS (443), тоже не подходят под условие. ACL на входе интерфейса фильтрует и транзитный трафик, и трафик к самому маршрутизатору. Доступ к маршрутизатору ограничивают ещё политики плоскости управления (control plane) и access-class на линиях VTY.

33. C GRE (Generic Routing Encapsulation) поверх IPsec сочетает способность GRE туннелировать multicast и разные протоколы с шифрованием и аутентификацией IPsec. GRE поддерживает протоколы маршрутизации (OSPF, EIGRP), multicast и IPv6. IPsec в туннельном режиме сам по себе передаёт только одноадресный IP-трафик. SSL VPN нужен для удалённого доступа клиентов, а не для связи площадок. PPTP устарел и небезопасен.

34. C AAA означает Authentication (аутентификация, проверка личности), Authorization (авторизация, выдача прав по личности) и Accounting (учёт действий и использования ресурсов). Эта модель реализуется протоколами TACACS+ и RADIUS. В остальных вариантах есть лишние понятия (administration, auditing, access) или нет authorization, а именно она определяет, что разрешено аутентифицированному пользователю.

35. D Стандартный ACL фильтрует только по IP-адресу источника, а не по порту назначения или протоколу. Поэтому его ставят как можно ближе к получателю: иначе он заблокирует трафик из 192.168.10.0/24 и к другим получателям. ACL на всех промежуточных интерфейсах только тратит ресурсы. Некоторые коммутаторы поддерживают ACL на портах (port ACL), но вопрос об интерфейсе маршрутизатора. Правило: стандартные ACL ближе к получателю, расширенные ближе к источнику.

36. B Цифра 5 означает хеш MD5. Команда enable secret всегда использует необратимое хеширование, поэтому она надёжнее, чем enable password. MD5 (тип 5) устарел, но всё ещё встречается. Тип 7 обозначает слабый шифр Виженера, который команда service password-encryption применяет к паролям линий, его легко расшифровать. Тип 8 означает PBKDF2-SHA256, тип 9 означает scrypt, оба сильнее. Длинная строка в конце содержит хеш пароля.

37. A TACACS+ разделяет аутентификацию, авторизацию и учёт и шифрует всё содержимое пакета, а не только пароль. Главное: он поддерживает авторизацию каждой команды, то есть определяет, какие команды может выполнять каждый пользователь. RADIUS объединяет аутентификацию и авторизацию и работает в основном по UDP, он лучше подходит для контроля доступа к сети. Локальная аутентификация не централизована, а Kerberos не даёт авторизации и учёта команд.

38. B Слову established в ACL Cisco соответствуют пакеты TCP с флагом ACK или RST. У чистого SYN (первого пакета рукопожатия TCP) этих флагов НЕТ, поэтому запись не срабатывает, и неявный запрет (implicit deny) в конце ACL отбрасывает пакет. Так established пропускает ответный трафик, но блокирует новые входящие соединения. ACL Cisco IOS не хранят состояние (stateless): таблица состояний TCP есть у межсетевых экранов вроде ASA, а здесь проверяются только флаги каждого пакета.

39. D TACACS+ шифрует всё содержимое пакета, а не только пароль, и разделяет аутентификацию, авторизацию и учёт, поэтому даёт детальный учёт команд. RADIUS шифрует только поле пароля и объединяет аутентификацию с авторизацией. Локальная база не централизована: на каждом устройстве свои пользователи. Kerberos служит для единого входа (single sign-on), и на уровне CCNA его для AAA на устройствах Cisco обычно не применяют. TACACS+ использует TCP 49, RADIUS использует UDP 1812 и 1813.

40. A Обратная маска 0.0.0.0 задаёт точное совпадение с одним хостом: 0 значит «бит должен совпасть», 1 значит «не важно». То же самое даёт запись host 192.168.5.45. Маска 255.255.255.255 означает any и подходит ко всем адресам. 0.0.0.255 требует совпадения первых трёх октетов и допускает любое значение в четвёртом (подсеть /24). 255.255.255.0 действует наоборот и здесь не годится. Запомните: где в маске подсети единицы, в обратной маске нули.

41. C Плоскость данных (data plane, или forwarding plane) пересылает пакеты по таблицам потоков и политикам, которые установил контроллер SDN. В традиционной сети решения о маршрутах принимает плоскость управления (control plane) устройства, а в SDN эта логика собрана в контроллере. Плоскость администрирования (management plane) отвечает за настройку и мониторинг. В плоскости приложений (application plane) работают программы, которые обращаются к контроллеру через northbound API.

42. C Значение "1000" взято в кавычки, поэтому в JSON оно считается строкой. json.loads() в Python сохраняет этот тип, и арифметика, например speed + 2, вызывает TypeError. Исправление: int(data['speed']). Отсутствие поля "unit" не вызвало бы TypeError, а при обращении к нему была бы ошибка KeyError. Синтаксис JSON корректен, и вложенные объекты библиотека json поддерживает. REST API часто отдают числа строками, поэтому перед вычислениями преобразуйте типы.

43. B SD-Access строит логические сегменты (Virtual Networks, VN) с помощью туннелей VXLAN (Virtual Extensible LAN) поверх физической IP-сети (underlay). Они заменяют сегментацию на VLAN и дают масштабируемую микросегментацию по политикам. В underlay по-прежнему работают протоколы маршрутизации (обычно IS-IS или OSPF). Трафик остаётся внутри фабрики, отправлять его через интернет не нужно. Доступ бывает и проводным, и беспроводным, так что кабели остаются.

44. B YANG (Yet Another Next Generation) задаёт схему данных конфигурации и рабочего состояния: какие данные есть, их типы, допустимые диапазоны, обязательные и необязательные поля и связи. По моделям YANG протоколы NETCONF и RESTCONF обмениваются проверенными данными. Сам YANG не шифрует: защиту даёт транспорт (SSH для NETCONF, HTTPS для RESTCONF). Графического интерфейса у этого текстового языка нет. Данные он не сжимает, их представление зависит от формата (XML, JSON).

45. C Код HTTP 409 Conflict означает конфликт состояния ресурса: здесь пытаются создать VLAN, которая уже есть. При нехватке прав сервер вернул бы 401 Unauthorized или 403 Forbidden, при неверном синтаксисе JSON 400 Bad Request. Одновременные изменения конфигурации в некоторых системах тоже дают конфликт, но по соглашениям REST код 409 указывает именно на попытку создать дубликат. Не путайте его с 423 Locked (ресурс временно недоступен).

46. C Этот JSON синтаксически правилен. В JSON строки и ключи берутся в двойные кавычки, а не в одинарные, поэтому hostname записан верно. Значение vlan записано как число (10) без кавычек: JSON различает строки (в кавычках) и числа (без кавычек). Массивы в JSON записываются в квадратных скобках [ ], а не в круглых. Логическое значение (boolean) true написано правильно: строчными буквами и без кавычек. Частых ошибок (одинарные кавычки, пропущенные или лишние запятые, непарные скобки) здесь нет.

47. A Ошибка «missing-element» говорит о нарушении модели YANG: в XML нет обязательного элемента (leaf или container), и проверка схемы не проходит. Без возможности writable-running ошибка была бы «operation-not-supported». Неверное пространство имён дало бы «unknown-namespace» или ошибку разбора. Заблокированное хранилище вернуло бы «in-use» или «resource-denied». Коды ошибок NETCONF указывают на разные причины, дело не всегда в синтаксисе или аутентификации.

48. B OAuth 2.0 использует токены bearer (bearer tokens) с ограниченным сроком действия. Их выдают после первичной аутентификации, и они сами истекают, поэтому украденный токен опасен недолго. С каждым запросом передаётся токен, а не учётные данные. Basic передаёт имя и пароль с каждым запросом, а Base64 их не шифрует. Ключи SSH подходят для CLI, обычно не применяются в REST API и сами не истекают. Строки сообщества SNMP передаются открытым текстом и срока действия не имеют.

49. A Значение true без кавычек и строчными буквами в JSON относится к типу Boolean и означает «истина». Логические значения пишутся как true или false без кавычек. Строки заключают в кавычки, как "Engineering". Целые числа пишут без кавычек, как 100. Объекты представляют собой вложенные структуры в фигурных скобках.

50. D HTTP 204 No Content означает, что запрос успешно обработан, а тела ответа нет. Это типично для операций DELETE, где достаточно подтверждения удаления без возврата данных. Если бы VLAN не нашлась, сервер вернул бы 404 Not Found. Сбои аутентификации возвращают 401 Unauthorized или 403 Forbidden. Внутренние ошибки сервера возвращают 500 Internal Server Error. Коды 2xx означают успех, 4xx ошибки клиента, 5xx ошибки сервера.

Ключевые английские слова

subnet mask	маска подсети	Показывает, какая часть IP-адреса относится к сети.
usable host addresses	адреса для узлов	Адреса подсети, которые можно назначить устройствам.
VLSM (variable-length subnet mask)	маски переменной длины	Деление сети на подсети разного размера.
summary route	суммарный маршрут	Один маршрут вместо нескольких соседних сетей.
collision domain	домен коллизий	Участок, где кадры могут столкнуться. У каждого порта коммутатора свой.
broadcast domain	широковещательный домен	Устройства, которые получают широковещательные кадры друг друга.
window size	размер окна TCP	Сколько данных можно отправить без подтверждения.
acknowledgment (ACK)	подтверждение	Сообщение о том, что данные получены.
routing table	таблица маршрутизации	Список сетей и путей, по которым маршрутизатор отправляет пакеты.
longest prefix match	самый длинный префикс	Правило: пакет идёт по самому точному подходящему маршруту.
administrative distance	административная дистанция	Степень доверия к источнику маршрута. Меньше значит лучше.
metric	метрика	Стоимость пути, по которой протокол сравнивает свои маршруты.

next hop	следующий переход	Адрес соседнего маршрутизатора, которому передают пакет.
static route	статический маршрут	Маршрут, который администратор прописал вручную.
floating static route	плавающий статический маршрут	Запасной маршрут с повышенной административной дистанцией.
default gateway	шлюз по умолчанию	Маршрутизатор, через который узел выходит в другие сети.
neighbor adjacency	соседство	Связь маршрутизаторов OSPF для обмена данными о сети.
designated router (DR)	назначенный маршрутизатор	Главный маршрутизатор OSPF в сегменте, с которым синхронизируются остальные.
first-hop redundancy protocol (FHRP)	протокол резервирования шлюза	Позволяет другому маршрутизатору заменить отказавший шлюз. Пример: HSRP.
preemption	перехват роли	Возврат активной роли маршрутизатору с более высоким приоритетом.
access port	порт доступа	Порт коммутатора для одной VLAN и конечного устройства.
trunk	транк, магистральный канал	Канал, по которому идут кадры нескольких VLAN.
native VLAN	нетегированная VLAN транка	VLAN, кадры которой по умолчанию идут по транку без тега.
spanning tree (STP)	протокол связующего дерева	Убирает петли между коммутаторами, отключая лишние пути.
root bridge	корневой мост	Главный коммутатор STP, от него строится дерево.
designated port	назначенный порт	Порт, который пересылает трафик своего сегмента в STP.
link aggregation	агрегирование каналов	Объединение нескольких физических линий в одну логическую, EtherChannel.
wireless LAN controller (WLC)	контроллер беспроводной сети	Устройство, которое централизованно управляет точками доступа.
access control list (ACL)	список контроля доступа	Строки правил, которые разрешают или запрещают трафик.
wildcard mask	обратная маска	Маска, где 0 требует совпадения бита, а 1 допускает любое значение.
implicit deny	неявный запрет	Невидимое последнее правило ACL: всё остальное запрещено.
inbound / outbound	на входе / на выходе	Направление трафика через интерфейс, к которому применён ACL.

accounting	учёт действий	Запись того, что делал пользователь. Третья A в AAA.
port security	защита порта	Ограничивает, какие MAC-адреса могут работать через порт коммутатора.
NAT (Network Address Translation)	трансляция адресов	Замена одних IP-адресов другими при проходе через маршрутизатор.
QoS (quality of service)	качество обслуживания	Приоритет для важного трафика, например для голоса.
data plane	плоскость данных	Часть устройства, которая пересылает пакеты.
control plane	плоскость управления	Часть, которая решает, куда направлять трафик.
management plane	плоскость администрирования	Часть для настройки устройства и наблюдения за ним.
payload	полезная нагрузка	Сами данные внутри пакета или запроса, без заголовков.

Сайт Examundo независим. Он не связан с организациями, которые проводят эти экзамены, и не одобрен ими. Вопросы оригинальные, они не взяты из настоящих экзаменов. examundo.tech/ru/ccna/