9 класс

На изображении представлена схема сети. На основе этой схемы ответьте на вопросы.

Изображение выглядит как текст, снимок экрана, диаграмма, Шрифт

Содержимое, созданное искусственным интеллектом, может быть неверным.

1. Какая комбинация аргументов позволяет задать маршрут по-умолчанию на SRV для реализации доступа к глобальной сети? Введите в поле ответа номер варианта (число 1, 2, 3, 4 или 5)! Ограничение попыток ввода: 1 раз!

1. route add 0.0.0.0 mask 0.0.0.0 via eth1

2. route add 0.0.0.0 mask 0.0.0.0 via 176.11.254.10

3. route add default gw 172.16.20.1

4. route add default gw 176.11.254.10

5. route add default gw 176.11.254.10/33

Флаг: 3

\*Строка с верным ответом тоже принималась

**Пояснение:**

В контексте IPv4-маршрутизации маршрут по умолчанию (0.0.0.0/0) на хосте задаёт следующий хоп (next-hop), на который направляются пакеты, не подпадающие под более специфические записи таблицы маршрутизации. Требование к next-hop: он должен быть непосредственно достижимым по канальному уровню через один из локальных интерфейсов хоста, то есть принадлежать той же IP-подсети, что и данный интерфейс, чтобы хост мог разрешить его MAC-адрес (ARP) и сформировать кадр.

**Разбор вариантов:**

1. route add 0.0.0.0 mask 0.0.0.0 via eth1 — некорректно по синтаксису/семантике: параметр via в данном виде не задаёт next-hop; для шлюза требуется IP-адрес (gw <ip>), а привязка к интерфейсу выполняется отдельно.

2. route add 0.0.0.0 mask 0.0.0.0 via 176.11.254.10 — next-hop не является непосредственно достижимым из подсети 172.16.20.0/X; адрес 176.11.254.10 относится к внешнему сегменту FW (провайдерскому), поэтому SRV не сможет выполнить ARP к этому адресу.

3. На схеме интерфейс SRV имеет адрес 172.16.20.10/X (eth1), а ближайший маршрутизирующий узел (FW) в этом же L2/L3-сегменте — 172.16.20.1/X. Следовательно, корректная настройка default route на SRV — указание 172.16.20.1 в качестве шлюза по умолчанию.

4. route add default gw 176.11.254.10 — аналогично (2): недостижимый next-hop для SRV.

5. route add default gw 176.11.254.10/33 — некорректный формат (шлюз не задаётся с префиксом) и невозможная маска /33 для IPv4.

Итог: правильный вариант — 3.

1. Какая максимальная длина префикса сети, которую можно задать для подсети FW-SRV, чтобы все её узлы оставались в одной подсети? В ответ запишите только число (например, 24). Число попыток ввода: 1 раз!

Ответ: 28

**Пояснение:**

На линке FW-SRV используются адреса:

* FW eth1: 172.16.20.1/X
* SRV eth1: 172.16.20.10/X

Нужно выбрать максимально длинный префикс (то есть самую “узкую” сеть), при котором оба адреса остаются в одной подсети.

Проверяем, в какие подсети попадают эти адреса при разных префиксах:

/29 (255.255.255.248)

Шаг подсетей по последнему октету: 0–7, 8–15, 16–23, …

172.16.20.1 попадает в 172.16.20.0–7

172.16.20.10 попадает в 172.16.20.8–15

Они в разных подсетях ⇒ /29 слишком длинный, не подходит.

/28 (255.255.255.240)

Шаг: 0–15, 16–31, 32–47, …

172.16.20.1 в подсети 172.16.20.0–15

172.16.20.10 в пподсети 172.16.20.0–15

Они в одной подсети. Следовательно, /28 подходит.

Так как /29 уже не подходит, а /28 подходит, то максимальная длина префикса — 28.

1. SRV нужно настроить таким образом, чтобы весь HTTPS трафик автоматически перенаправлялся на прокси-сервер, который функционирует на 444 порту. Какая комбинация аргументов позволяет это выполнить? Выберете пропущенные параметры и объедините их в ответ (флаг) в следующем виде, через разделитель “\_”:  
   ПАРАМЕТР1\_ПАРАМЕТР2\_ПАРАМЕТР3

Например:   
Если ПАРАМЕТР1 = SEND, ПАРАМЕТР2 = ++tuda, ПАРАМЕТР3 = 2026 то итоговый флаг будет SEND\_++tuda\_2026  
Ответы представленные в другом виде или с ошибкой хотя бы в одном символе приняты к ответу не будут. Число попыток ввода: 2 раза!

iptables -t nat -A PREROUTING -p tcp ПАРАМЕТР1 ПАРАМЕТР2 -j ПАРАМЕТР3 --to-port 444

Флаг: --dport\_443\_REDIRECT

**Пояснение:**

-t nat — правило добавляется в таблицу NAT, потому что требуется изменить адресацию/порт назначения пакета (это не фильтрация, а преобразование).

-A PREROUTING — цепочка PREROUTING срабатывает сразу при поступлении пакета, до маршрутизации. Это нужно, чтобы перехватить HTTPS-запросы “на входе” и успеть изменить их до принятия решения, куда их дальше отправлять.

-p tcp — HTTPS работает поверх TCP.

--dport 443 — выбираем пакеты, у которых порт назначения 443 (стандартный порт HTTPS).

-j REDIRECT --to-port 444 — цель REDIRECT перенаправляет трафик на локальный порт на этой же машине (SRV). Параметр --to-port 444 задаёт новый порт назначения — 444, где слушает прокси.