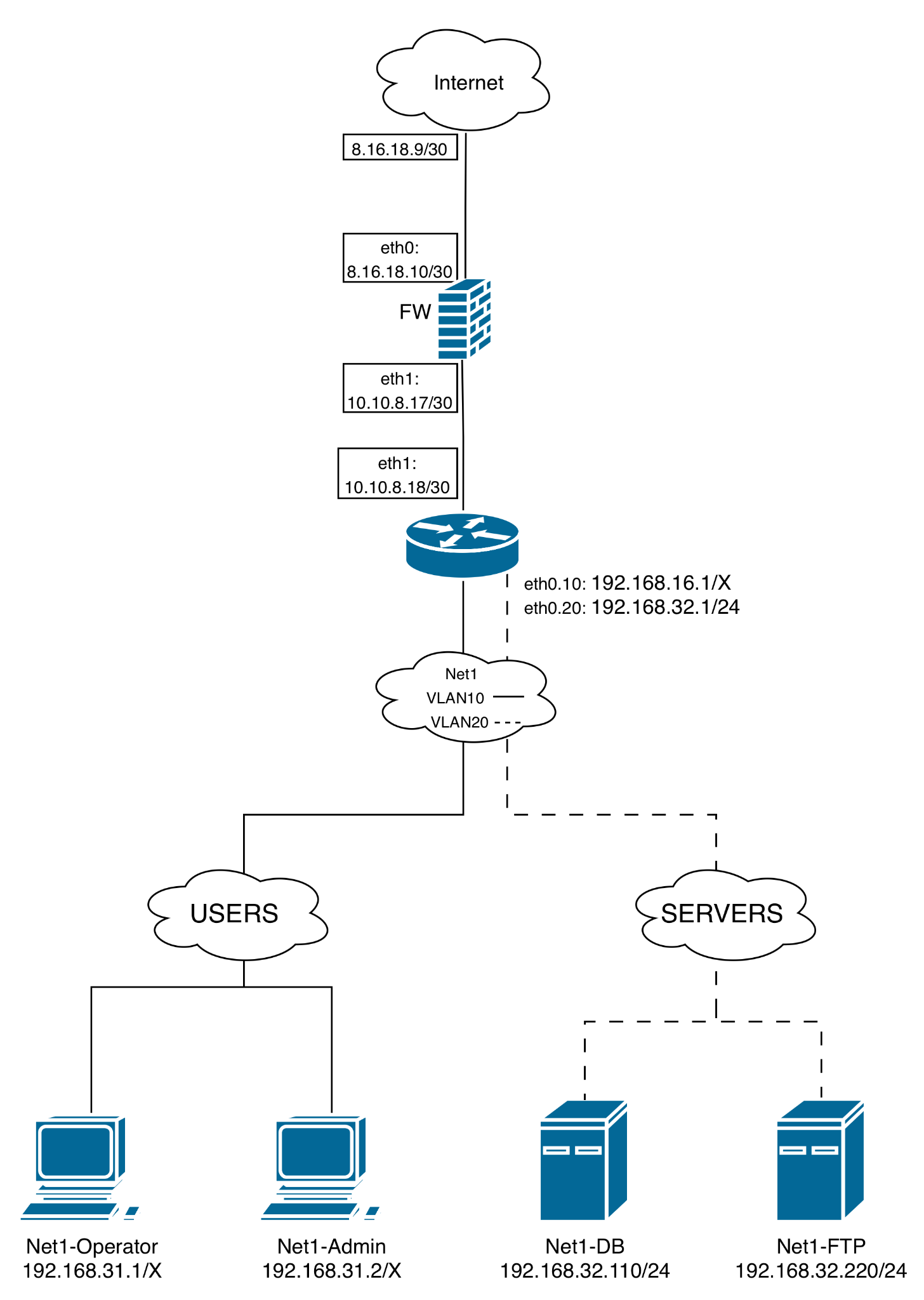
# 11 класс

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



1. Какая максимальная длина префикса сети, которую можно задать для подсети USERS (VLAN10) чтобы все её узлы оставались в одной подсети? В ответ запишите только число (например, 24). Число попыток ввода: 1 раз.

Ответ: 20

**Пояснение:**

В подсети USERS (VLAN10) используются адреса:

* Net1-Operator: 192.168.31.1/X
* Net1-Admin: 192.168.31.2/X
* Шлюз VLAN10 (роутер): 192.168.16.1/X (eth0.10)

Нужно выбрать максимально длинный префикс (самую “узкую” сеть), при котором все эти адреса остаются хостами и находятся в одной подсети.

Проверяем, что будет при разных префиксах.

**/20 (255.255.240.0)**

Шаг подсетей по 3-му октету: 0–15, 16–31, 32–47, …

Адреса:

* 192.168.16.1 попадает в диапазон 16–31 в сети 192.168.16.0/20
* 192.168.31.1 и 192.168.31.2 тоже в диапазоне 16–31. Та же сеть 192.168.16.0/20  
  Все адреса — хосты, все в одной подсети. Следовательно, /20 подходит.

**/21 (255.255.248.0)**

Шаг по 3-му октету: 0–7, 8–15, 16–23, 24–31, 32–39, …

Тогда:

* 192.168.16.1 в сети 192.168.16.0/21 (диапазон 16–23)
* 192.168.31.1 и 192.168.31.2 в сети 192.168.24.0/21 (диапазон 24–31)  
  Адреса оказываются в разных подсетях. Следовательно, /21 не подходит.

Так как /21 уже не подходит, а /20 ещё подходит, то **максимальная** **длина** префикса — **20**.

1. Какое правило iptables нужно добавить на FW для SNAT/MASQUERADE трафика из внутренних VLAN в Интернет?

iptables -t <ПАРАМЕТР1> -A <ПАРАМЕТР2> -s 192.168.0.0/16 -o <ПАРАМЕТР3> -j MASQUERADE

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!

ФЛАГ: nat\_POSTROUTING\_eth0

**Пояснение:**

* -t nat — используется таблица NAT, потому что требуется подмена адресов (а не фильтрация). SNAT/MASQUERADE всегда делается в таблице nat.
* -A POSTROUTING — цепочка POSTROUTING обрабатывает пакеты после того, как ядро выбрало маршрут, но до фактической отправки. Это правильное место для SNAT/MASQUERADE, т.к. уже известно, через какой интерфейс пакет уходит “наружу”.
* -s 192.168.0.0/16 — правило применяется ко всей внутренней адресации VLAN (все 192.168.x.x), чтобы любой хост из внутренних VLAN при выходе в Интернет был “замаскирован”.
* -o eth0 — ограничиваем NAT только трафиком, который уходит во внешнюю сеть/Интернет через внешний интерфейс FW. По схеме внешний интерфейс FW — eth0.
* -j MASQUERADE — выполняет SNAT “автоматически”: подставляет в качестве исходного адреса текущий адрес внешнего интерфейса (eth0). Это типичный выбор для выхода в Интернет, особенно если внешний IP может быть динамическим.

Результат: любой трафик из внутренних 192.168.0.0/16, уходящий через eth0, будет иметь исходный адрес FW (eth0), и ответы из Интернета вернутся на FW, который по таблице NAT отправит их обратно внутреннему хосту.

1. Какой адрес сети используется на линке между FW и маршрутизатором?

10.10.8.16

10.10.8.17

10.10.8.18

10.10.8.19

10.10.0.0

Флаг: 1

\*Строка с верным ответом тоже принималась

**Пояснение:**

На линке адреса **10.10.8.17/30** (FW) и **10.10.8.18/30** (маршрутизатор). Для префикса **/30** размер блока 4 адреса, диапазон **10.10.8.16–10.10.8.19**, где:

* адрес сети: **10.10.8.16**
* хосты: 10.10.8.17, 10.10.8.18
* broadcast: 10.10.8.19