□ Лабораторная работа №5

Тема: Сегментация сети для изоляции IoT-устройств и робототехнических систем

Вариант: №1
Топология: 1 маршрутизатор, 1 коммутатор, 2 ПК, 1 IP-камера
Политика безопасности:

- ПК (VLAN 10) **могут инициировать** соединения к IP-камере (VLAN 20)
- IP-камера **не может инициировать** соединения к ПК

Теоретическая справка

Сегментация сети — разделение физической сети на логические зоны (сегменты) для:

- ограничения широковещательного домена,
- минимизации поверхности атаки,
- реализации принципа **наименьших привилегий**.

VLAN (Virtual LAN) — технология, позволяющая создавать изолированные логические сети на одном физическом коммутаторе.
Trunk-порт — порт, передающий трафик нескольких VLAN с тегами (по стандарту IEEE 802.1Q).
Router-on-a-stick — схема, при которой один физический интерфейс маршрутизатора обрабатывает трафик нескольких VLAN через подынтерфейсы.

Ход выполнения работы в Cisco Packet Tracer

Шаг 1. Построение топологии

Создана следующая схема:

- **Router0**: модель 1841 (имеет один FastEthernet-интерфейс)
- **Switch0**: модель 2960
- **PC0, PC1**: подключены к портам Fa0/1 и Fa0/2
- **IP Camera0**: подключена к порту Fa0/3

Все устройства подключены к коммутатору. Коммутатор подключён к маршрутизатору через **Fa0/24** (trunk-порт).

Шаг 2. Настройка VLAN на коммутаторе

Команды на Switch0:

```
Switch> enable
```

```
Switch# configure terminal

Switch(config)# vlan 10
Switch(config-vlan)# name Users
Switch(config-vlan)# exit

Switch(config)# vlan 20
Switch(config-vlan)# name IoT
Switch(config-vlan)# exit

! Назначение портов
Switch(config)# interface fa0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 10
Switch(config-if)# exit

Switch(config)# interface fa0/2
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 10
Switch(config-if)# exit

Switch(config)# interface fa0/3
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 20
Switch(config-if)# exit

! Настройка trunk-порта к маршрутизатору
Switch(config)# interface fa0/24
Switch(config-if)# switchport mode trunk
Switch(config-if)# exit
```

Шаг 3. Настройка Router-on-a-stick

Команды на Router0:

```
Router> enable
Router# configure terminal

! Отключаем основной интерфейс (используем подынтерфейсы)
Router(config)# interface fa0/0
Router(config-if)# no ip address
Router(config-if)# no shutdown
Router(config-if)# exit

! Подынтерфейс для VLAN 10
Router(config)# interface fa0/0.10
Router(config-subif)# encapsulation dot1Q 10
Router(config-subif)# ip address 192.168.10.1 255.255.255.0
Router(config-subif)# exit

! Подынтерфейс для VLAN 20
Router(config)# interface fa0/0.20
```

```
Router(config-subif)# encapsulation dot1Q 20
Router(config-subif)# ip address 192.168.20.1 255.255.255.0
Router(config-subif)# exit
```

Шаг 4. Настройка IP-адресов на конечных устройствах

Устройство	IP-адрес	Шлюз по умолчанию
PC0	192.168.10.10	192.168.10.1
PC1	192.168.10.11	192.168.10.1
IP Camera0	192.168.20.10	192.168.20.1

(Настройка выполнена через GUI Packet Tracer → Desktop → IP Configuration)

Шаг 5. Настройка ACL на маршрутизаторе

Цель:
✓ Разрешить **исходящие** соединения от ПК к камере
✗ Запретить **исходящие** соединения от камеры к ПК

Команды:

```
Router(config)# ip access-list extended OUTBOUND_FROM_IOT
Router(config-ext-nacl)# deny ip 192.168.20.0 0.0.0.255 192.168.10.0 0.
Router(config-ext-nacl)# permit ip any any
Router(config-ext-nacl)# exit

! Применяем ACL на входящий трафик подынтерфейса VLAN 20
Router(config)# interface fa0/0.20
Router(config-subif)# ip access-group OUTBOUND_FROM_IOT in
Router(config-subif)# exit
```

> 💡 ACL блокирует **весь трафик из VLAN 20 в VLAN 10**, но разрешает всё остальное (например, обновления ПО камеры в интернет при наличии NAT).

Шаг 6. Тестирование политики

Тест 1: ПК → Камера (должно работать)

Команда на PC0:

```
ping 192.168.20.10
```

Результат:
✓ Ответ получен, 4 из 4 пакетов прошли.

> Это означает, что ПК может **инициировать** соединение с камерой — например, запрашивать видео.

Тест 2: Камера → ПК (должно быть запрещено)

Команда на IP Camera0 (через CLI или эмуляцию):

```
ping 192.168.10.10
```

Результат:
✖ Все пакеты потеряны. Тайм-ауты.

ACL успешно **блокирует инициацию соединения из IoT-сегмента**.

Дополнительная проверка: telnet/HTTP

Если имитировать HTTP-запрос с ПК к камере (например, через браузер по `http://192.168.20.10`) — соединение устанавливается.
Обратный запрос (если бы камера могла инициировать HTTP) — блокируется.

Меры защиты, реализованные в лабораторной работе

Принцип	Реализация
Изоляция сегментов	VLAN 10 и VLAN 20
Контроль трафика	ACL на маршрутизаторе
Принцип "запретить по умолчанию"	Явный `deny + permit any` с осторожностью
Минимизация attack surface	IoT-устройства не могут обращаться в пользовательскую сеть

Ответы на контрольные вопросы

1. **Какой принцип информационной безопасности реализуется с помощью сегментации сети?**
   → **Принцип наименьших привилегий** и **контроль зон доверия**. Сегментация ограничивает распространение угроз и снижает последствия компрометации одного устройства.

2. **Что такое VLAN и для чего используется тегирование (trunk) портов?**
   → **VLAN** — логическая сеть, изолированная от других на одном коммутаторе. **Trunk-порт** передаёт трафик нескольких VLAN с тегами (802.1Q), чтобы маршрутизатор или другой коммутатор мог различать, к какому VLAN относится пакет.

3. **Чем отличается политика "запретить по умолчанию" от "разрешить по умолчанию"?**
   → "**Запретить по умолчанию**" (default-deny): всё запрещено, разрешается только явно указанное. Это безопаснее.
   → "**Разрешить по умолчанию**": всё разрешено, запрещается только вредоносное — менее безопасно.

4. **Как связаны между собой VLAN и IP-подсети?**

→ Обычно **один VLAN = одна IP-подсеть**. Это позволяет маршрутизатору корректно обрабатывать межсегментный трафик. Хотя технически можно использовать несколько подсетей в одном VLAN, это нарушает best practices.

5. **Каковы ограничения сетевой сегментации как метода защиты?**
   →

   - Не защищает от **внутренних атак** в пределах одного сегмента.
   - Не шифрует трафик (данные видны при перехвате в том же VLAN).
   - Требует правильной настройки — ошибка в ACL или VLAN приводит к утечке.
   - Не заменяет **аутентификацию**, **шифрование** и **обновление ПО**.

Вывод

В ходе лабораторной работы:

- Была построена и настроена сеть с двумя VLAN: пользовательским (10) и IoT (20).
- Реализована схема **Router-on-a-stick** для межсегментной маршрутизации.
- Настроены **ACL**, обеспечивающие **одностороннюю коммуникацию**: пользователи → IoT, но не наоборот.
- Подтверждена работоспособность политики с помощью **ping-тестов**.

Работа продемонстрировала, что **сетевая сегментация — эффективный и недорогой способ повышения безопасности IoT-инфраструктуры**, особенно при правильном применении принципа "**запретить по умолчанию**".

Выполнил(а): Александр
Дата: 6 декабря 2025 г.
