Оглавление

Лаб 4

Как сигнал проходит по сети

Сценарий:

- На **Router 0** настроены интерфейсы, маршрут до соседней сети, и маршрут по умолчанию, ведущий на магистральный роутер **Router2**.
- **Router1** настроен аналогично с маршрутом по умолчанию на тот же магистральный роутер.
- Магистральный роутер связывает локальные сети через сеть 192.168.1.x (с маской /30, что обеспечивает два адреса для роутеров и один broadcast).
- Протокол ICMP (ping) используется для проверки связи между хостами, шлюзами и магистральными роутерами.

---

1. Протоколы канального уровня

- **Какие протоколы канального уровня используются в данной схеме?**
  - В локальных сетях используется **Ethernet** (IEEE 802.3), который работает с MAC-адресами.
  - На магистральных маршрутизаторах может использоваться **HDLC** или **PPP** для связи точка-точка.
- **Что такое кадр в Ethernet и что в нём содержится?**
  - Кадр — это единица данных канального уровня. Он включает:
    1. Заголовок (MAC-адреса источника и назначения, тип протокола).
    2. Полезную нагрузку (пакет сетевого уровня, обычно IP).
    3. Конец кадра (CRC для проверки ошибок).
- **Как канальный уровень взаимодействует с физическим?**
  - Канальный уровень организует передачу данных через физический уровень, формируя кадры и управляя доступом к среде передачи.

---

2. WAN

- **Какие технологии используются для WAN?**
  - В лабораторной работе используется статическая маршрутизация и связь через сеть 192.168.1.x. Реальные WAN-сети могут использовать технологии VPN, MPLS, Frame Relay или point-to-point соединения через PPP.
- **Зачем нужна сеть с маской /30?**
  - Маска /30 позволяет создать сеть с двумя узлами (адреса для двух маршрутизаторов) и одним broadcast-адресом. Это экономит IP-адреса.
- **Почему WAN сложнее, чем LAN?**
  - WAN охватывает большие расстояния, использует разные провайдеры и требует сложных протоколов маршрутизации (OSPF, BGP) для масштабируемости.

---

3. Статическая маршрутизация

- **В чём отличие статической маршрутизации от динамической?**
  - В статической маршрутизации маршруты задаются вручную администратором.
  - В динамической (OSPF, RIP, EIGRP) маршруты автоматически адаптируются к изменениям сети.
- **Как настроить статический маршрут?**
  - Пример команды для Cisco:
  - `Router(config)# ip route 192.168.2.0 255.255.255.0 192.168.1.1`
    - 192.168.2.0 — сеть назначения.
    - 255.255.255.0 — маска сети.
    - 192.168.1.1 — адрес следующего маршрутизатора.
- **Что такое маршрут по умолчанию?**
  - Маршрут для всех пакетов, для которых нет явного маршрута в таблице. Например:
  - `Router(config)# ip route 0.0.0.0 0.0.0.0 192.168.1.2`
- **Зачем нужны плавающие маршруты?**
  - Для резервирования. У плавающего маршрута выше административное расстояние, и он активируется только при отказе основного маршрута.

---

4. Сложные вопросы

- **Что произойдёт, если один из маршрутов перестанет работать?**
  - Если настроен плавающий маршрут, трафик автоматически перейдёт на резервный маршрут.
  - Если плавающий маршрут не настроен, связь с этой сетью будет потеряна.
- **Какие возможны ошибки при настройке статической маршрутизации?**
  - Неправильно указан next_hop.
  - Несовпадение маски сети.
  - Отсутствие возвратных маршрутов.
- **Как проверить маршруты?**
  - Команда `show ip route` покажет текущую таблицу маршрутизации.
  - Для проверки связи:
  - `ping 192.168.x.x`
  - `traceroute 192.168.x.x`
- **Какие проблемы может вызвать ручная настройка маршрутов?**
  - Человеческий фактор: забытые или ошибочные маршруты.
  - Низкая масштабируемость: сложно поддерживать в больших сетях.

---

5. "Починить схему"

- **Какие шаги нужно предпринять?**
  1. Проверить IP-адреса и маски на всех интерфейсах (`show ip interface brief`).
  2. Убедиться в правильности таблиц маршрутизации (`show ip route`).
  3. Использовать `ping` и `traceroute` для проверки связи.

4. Настроить возвратные маршруты на магистральных маршрутизаторах.

---

1. Принцип работы протоколов канального уровня

- **Ethernet: как кадры доставляются в пределах одной сети?**
  - Ethernet формирует кадры, включающие MAC-адреса отправителя и получателя. В пределах локальной сети коммутаторы читают MAC-адрес назначения из кадра и пересылают его только на соответствующий порт. Если адрес неизвестен, кадр отправляется на все порты (broadcast).
  - Протокол используется для передачи данных внутри одной физической или логической локальной сети.
- **PPP: его роль в обеспечении связи точка-точка?**
  - PPP (Point-to-Point Protocol) обеспечивает соединение между двумя узлами. Он инкапсулирует сетевые протоколы, проверяет подлинность (CHAP, PAP), сжимает данные и управляет соединением. Используется для WAN-сетей и модемных соединений.

---

2. Почему выбрана подсеть /30 для магистральных роутеров?

- Подсеть с маской **/30 (255.255.255.252)** создаёт сеть из четырёх адресов:
  - Один адрес для маршрутизатора A.
  - Один адрес для маршрутизатора B.
  - Один адрес для broadcast.
  - Один сетевой адрес.
- Это минимально необходимое количество адресов для связи точка-точка, что экономит IP-пространство.

---

3. Как настроить статическую маршрутизацию?

- **Пример команды на маршрутизаторе Cisco:**
- `Router(config)# ip route 192.168.2.0 255.255.255.0 192.168.1.1`
  - **192.168.2.0** — сеть назначения.
  - **255.255.255.0** — маска сети.
  - **192.168.1.1** — адрес следующего узла (next_hop) или интерфейс выхода.
- **Объяснение:**
  - Этот маршрут отправляет весь трафик, предназначенный для сети 192.168.2.0/24, через роутер с адресом 192.168.1.1.
- **Добавление маршрута по умолчанию:**
- `Router(config)# ip route 0.0.0.0 0.0.0.0 192.168.1.2`
  - Отправляет весь трафик, не указанный в таблице маршрутизации, через магистральный роутер.

---

4. Как организована отказоустойчивость?

- За счёт **плавающих маршрутов**:
  - Используются маршруты с большим административным расстоянием (AD).
  - Например:
  - `Router(config)# ip route 192.168.3.0 255.255.255.0 192.168.1.2 10`
    - **10** — административное расстояние. Маршрут активируется, если основной маршрут недоступен.

---

5. Что будет, если один маршрут "упадёт"?

- Если основной маршрут становится недоступен, маршрутизатор переключается на плавающий маршрут с более высоким AD.
- Это обеспечивает непрерывность связи, особенно в критичных сетях.

---

6. Какие проблемы могут быть в схеме?

- **Отсутствие маршрутов в обе стороны.**
  - Пример: если на одном маршрутизаторе есть маршрут до другой сети, но обратный маршрут не настроен, связь не будет работать.
- **Неправильная настройка маски сети.**
  - Ошибки в маске могут привести к тому, что пакеты будут отправляться не в ту сеть.
- **Неправильный IP-адрес next_hop.**
  - Если адрес следующего узла указан неправильно, пакеты не достигнут цели.
- **Отсутствие маршрута по умолчанию.**
  - Если маршрут для "неизвестных" сетей не настроен, маршрутизатор будет сбрасывать такие пакеты.

5я лаба

Описание сети

В лабораторной рассматривается динамическая маршрутизация с настройкой следующих протоколов:

1. **RIP**:
   - Используется для сетей с маской **/24**.
   - Настроены loopback-интерфейсы для тестирования.
   - Основное поведение: маршруты автоматически добавляются в таблицу маршрутизации с периодическим обновлением.
   - При отказе линка маршрутизация перестраивается через альтернативные пути.
2. **OSPF**:
   - Настроен на сетях с той же маской **/24**.

    - Используется для более крупной сети (другой организации), обеспечивая быстрое восстановление маршрутов при отказах.
    - Реализована маршрутизация для loopback и других интерфейсов.
3. **BGP**:
    - На пограничном маршрутизаторе R9 настроено перераспределение маршрутов между протоколами RIP и OSPF.
    - BGP, как правило, используется для межорганизационного взаимодействия и анонсирования маршрутов.
4. **Redistribution**:
    - Для объединения двух организаций настроено перераспределение маршрутов (route redistribution) на R9, чтобы маршруты RIP могли быть видимы в OSPF и наоборот.

---

1. Динамическая маршрутизация

- **Что это такое?**
    - Динамическая маршрутизация автоматически обновляет маршруты в таблице маршрутизации с помощью протоколов (RIP, OSPF, BGP).
    - Протоколы используют различные алгоритмы для выбора лучшего маршрута и их актуализации.
- **Преимущества:**
    - Автоматизация управления маршрутами.
    - Быстрое восстановление при отказе сети.
    - Масштабируемость в крупных сетях.
- **Недостатки:**
    - Занимает больше ресурсов процессора и памяти маршрутизаторов.
    - Требует настройки и мониторинга.

---

2. RIP

- **Принципы работы:**
    - Использует алгоритм Bellman-Ford.
    - Обновляет маршруты каждые 30 секунд.
    - Максимальная длина маршрута: 15 хопов.
    - Пример команды настройки:
    - `Router(config)# router rip`
    - `Router(config-router)# network 192.168.0.0`
- **Плюсы:**
    - Простота настройки.
- **Минусы:**
    - Ограничение по хопам (15).
    - Медленное сходимость.

---

3. OSPF

- **Принципы работы:**
    - Использует алгоритм Dijkstra.

    - Делит сеть на области (Areas).
    - Рассылает только изменения маршрутов, а не всю таблицу.
    - Пример команды настройки:
    - `Router(config)# router ospf 1`
    - `Router(config-router)# network 192.168.1.0 0.0.0.255 area 0`
- **Плюсы:**
    - Быстрая сходимость.
    - Подходит для больших сетей.
- **Минусы:**
    - Сложнее настройки по сравнению с RIP.

---

4. BGP

- **Принципы работы:**
    - Используется для междоменной маршрутизации.
    - Обменивается маршрутами между автономными системами (AS).
    - Пример команды настройки:
    - `Router(config)# router bgp 65001`
    - `Router(config-router)# neighbor 192.168.1.2 remote-as 65002`
- **Особенности:**
    - Поддерживает миллионы маршрутов.
    - Использует политику маршрутизации (prefixed-based).

---

5. Отказоустойчивость (FHRP)

- **Что это такое?**
    - Протоколы семейства FHRP (First Hop Redundancy Protocol) обеспечивают отказоустойчивость для шлюзов.
    - Примеры: HSRP, VRRP, GLBP.
- **Как работает?**
    - Шлюзы объединяются в группу, и один из них становится активным.
    - Если активный шлюз выходит из строя, другой из группы автоматически становится активным.
- **Пример настройки HSRP:**
- `Router(config-if)# standby 1 ip 192.168.1.254`
- `Router(config-if)# standby 1 priority 110`
- `Router(config-if)# standby 1 preempt`

6я лаба

Подробное описание сети

Лабораторная работа посвящена настройке **ACL** (Access Control Lists) и **NAT** (Network Address Translation), включает пять схем:

1. **Стандартный ACL:**
    - Настроены три хоста и маршрутизатор.
    - ACL блокирует доступ определённому IP-адресу (например, 10.10.1.3).

    - Применяется на входящем интерфейсе маршрутизатора.
2. **Расширенный ACL:**
    - Схема дополнена сервером (например, FTP).
    - Расширенный ACL фильтрует трафик по IP-адресу, порту и протоколу (например, TCP для порта 21).
3. **Статический NAT:**
    - Один внутренний IP-адрес сопоставляется одному внешнему.
    - Используется для предоставления доступа к серверу из внешней сети.
4. **Динамический NAT:**
    - Несколько внутренних адресов используют пул внешних адресов.
    - Пул адресов указывается на маршрутизаторе.
5. **PAT (Port Address Translation):**
    - Несколько внутренних адресов используют один внешний IP, различаясь портами.
    - Это экономит IP-адреса.

Развёрнутые ответы на вопросы

1. ACL

- **Что такое ACL?**
    - ACL — это списки правил, применяемых к интерфейсам маршрутизаторов или коммутаторов для фильтрации трафика.
    - Основные действия: `permit` (разрешить) и `deny` (запретить).
    - Применение: контроль доступа, безопасность сети, разграничение трафика.
- **Пример стандартного ACL:**
- `access-list 1 deny 10.10.1.3`
- `access-list 1 permit any`
- `interface g0/0`
- `ip access-group 1 in`
    - Блокирует доступ от IP 10.10.1.3 на входе интерфейса g0/0.
- **Пример расширенного ACL:**
- `access-list 101 permit tcp any host 192.168.1.100 eq 21`
- `access-list 101 deny ip any any`
- `interface g0/0`
- `ip access-group 101 in`
    - Разрешает доступ к FTP-серверу (192.168.1.100:21) и блокирует остальной трафик.

---

2. NAT

- **Что такое NAT?**
    - NAT преобразует IP-адреса из частной сети в публичные и обратно.
    - Типы NAT:
        1. **Статический NAT:** прямое соответствие внутреннего и внешнего адреса.
        2. **Динамический NAT:** внутренние адреса используют пул внешних адресов.

3. **PAT:** несколько внутренних адресов используют один внешний с разными портами.

- **Пример статического NAT:**
- `ip nat inside source static 192.168.1.10 203.0.113.10`
- `interface g0/0`
- `ip nat inside`
- `interface g0/1`
- `ip nat outside`
    - Внутренний сервер с IP 192.168.1.10 доступен по внешнему адресу 203.0.113.10.
- **Пример динамического NAT:**
- `ip nat pool MYPOOL 203.0.113.20 203.0.113.30 netmask 255.255.255.0`
- `access-list 10 permit 192.168.1.0 0.0.0.255`
- `ip nat inside source list 10 pool MYPOOL`
- **Пример PAT:**
- `ip nat inside source list 10 interface g0/1 overload`

---

3. Port Forwarding

- **Что это такое?**
    - Это тип статического NAT, перенаправляющий трафик на внутренние серверы через определённые порты.
    - Используется для предоставления доступа к web- и FTP-серверам.
- **Пример настройки для FTP-сервера:**
- `ip nat inside source static tcp 192.168.1.100 21 203.0.113.10 21`

---

4. Уязвимости NAT и ACL

- **Уязвимости NAT:**
    - Невозможность отслеживать внутренние подключения при неправильной настройке.
    - Отсутствие шифрования — NAT не обеспечивает конфиденциальности.
- **Уязвимости ACL:**
    - Возможность обхода правил из-за ошибок настройки.
    - Ограниченность стандартных ACL, недостаточная гибкость фильтрации.

---

5. Защита сети

- **DHCP Snooping:**
    - Предотвращает атаки DHCP Spoofing.
    - Пример настройки:
    - `Switch(config)# ip dhcp snooping`
    - `Switch(config)# ip dhcp snooping vlan 10`
    - `Switch(config-if)# ip dhcp snooping trust`
- **IP Source Guard:**
    - Блокирует трафик от IP-адресов, не связанных с их MAC-адресами.
    - Пример настройки:
    - `Switch(config-if)# ip verify source`
- **Контроль ACL и NAT:**

- Постоянный мониторинг логов и тестирование конфигурации.
- Минимизация числа открытых портов и использование шифрования.

---

6. Настройка web и FTP через NAT

- Настройка web-сервера:
- `ip nat inside source static tcp 192.168.1.100 80 203.0.113.10 80`
- Настройка FTP-сервера:
- `ip nat inside source static tcp 192.168.1.101 21 203.0.113.10 21`

Эти настройки обеспечат доступ к внутренним серверам через NAT с внешнего адреса 203.0.113.10.

Если требуется дополнительная помощь или пояснения — обращайся!

7я лаба

Описание сети

В лабораторной работе рассматривается настройка DHCP (Dynamic Host Configuration Protocol) на трёх типах конфигураций:

1. **Локальный DHCP-сервер:**
   - Отдельный сервер в локальной сети раздаёт IP-адреса устройствам.
   - Сеть использует маску **/24**.
   - Хосты настроены для автоматического получения IP через DHCP.
2. **Роутер как DHCP-сервер:**
   - DHCP-функции настроены непосредственно на маршрутизаторе для сети **192.168.1.0/24**.
   - Первые 10 адресов в диапазоне исключены из раздачи (зарезервированы).
3. **DHCP-Relay:**
   - Настроена сеть с несколькими VLAN (10, 11, 12) и маршрутизатором, выполняющим роль **Router-on-a-Stick**.
   - Используется DHCP-Relay для перенаправления запросов DHCP в другую сеть.

Ответы на вопросы

1. Что такое DHCP?

- DHCP (Dynamic Host Configuration Protocol) — это протокол, который автоматически раздаёт IP-адреса, маски подсети, шлюзы и другие параметры хостам в сети.
- Работает на основе модели клиент-сервер. Клиенты отправляют широковещательный запрос, сервер отвечает, предоставляя IP-адрес и параметры.
- **Основные этапы работы DHCP:**

1. **DISCOVER:** клиент отправляет широковещательный запрос.
2. **OFFER:** сервер предлагает свободный IP-адрес.
3. **REQUEST:** клиент запрашивает предложенный адрес.
4. **ACKNOWLEDGE:** сервер подтверждает выдачу IP-адреса.

---

2. Уязвимости DHCP

- **DHCP Spoofing:**
  - Злоумышленник запускает ложный DHCP-сервер, выдающий неправильные параметры, что может привести к перенаправлению трафика.
- **DHCP Starvation:**
  - Злоумышленник отправляет большое количество запросов DHCP, истощая пул IP-адресов сервера.
- **Незащищённость широковещательных запросов:**
  - Злоумышленники могут перехватить запросы DISCOVER и вмешаться в процесс.

---

3. Методы защиты

- **DHCP Snooping:**
  - Ограничивает DHCP-трафик только доверенными портами.
  - Недоверенные порты блокируют DHCP-сообщения от ложных серверов.
- `Switch(config)# ip dhcp snooping`
- `Switch(config)# ip dhcp snooping vlan 10`
- `Switch(config-if)# ip dhcp snooping trust`
- **IP Source Guard (Dynamic IP Lockdown):**
  - Блокирует трафик с IP-адресов, которые не соответствуют записям в таблице DHCP Snooping.
- `Switch(config-if)# ip verify source`
- **Периодический мониторинг и резервирование диапазонов:**
  - Контроль пула адресов для предотвращения атак DHCP Starvation.
  - Резервирование критичных адресов (например, шлюзов).

---

4. Пример настройки DHCP на маршрутизаторе

- **Настройка DHCP-сервера на маршрутизаторе:**
- `ip dhcp excluded-address 192.168.1.1 192.168.1.10`
- `ip dhcp pool MYPOOL`
- `  network 192.168.1.0 255.255.255.0`
- `  default-router 192.168.1.1`
- `  dns-server 8.8.8.8`
- **Настройка DHCP-Relay:**
- `interface vlan 10`
- `  ip address 192.168.10.1 255.255.255.0`
- `  ip helper-address 192.168.1.100`

---

5. DHCP Snooping и IP Source Guard

- **Что это такое?**
  - **DHCP Snooping:** предотвращает атаки DHCP, проверяя происхождение запросов.
  - **IP Source Guard:** проверяет трафик на соответствие разрешённым IP-адресам и MAC-адресам.
- **Настройка DHCP Snooping и IP Source Guard:**
- `Switch(config)# ip dhcp snooping`
- `Switch(config)# ip dhcp snooping vlan 10`
- `Switch(config-if)# ip dhcp snooping trust`
- `Switch(config-if)# ip verify source`