Broadcast в сети

Broadcast (широковещательная передача) — это тип передачи данных, при котором пакет отправляется всем устройствам в одной сети. В сетях Ethernet широковещательный пакет имеет MAC-адрес получателя FF:FF:FF:FF:FF:FF, что означает, что он принимается всеми устройствами в сети.

Особенности Broadcast-трафика:

- Используется для обнаружения устройств, например, протоколами ARP (Address Resolution Protocol) и DHCP (Dynamic Host Configuration Protocol).
- Распространяется во всех устройствах одной VLAN, но не выходит за ее пределы.
- Чрезмерное количество Broadcast-пакетов может вызывать нагрузку на сеть, снижая производительность (Broadcast Storm).

Как VLAN помогают бороться с Broadcast-трафиком?

VLAN делят сеть на отдельные широковещательные домены, ограничивая распространение Broadcast-пакетов. Это уменьшает нагрузку на сеть и повышает безопасность, так как устройства в одной VLAN не видят трафик из другой VLAN без маршрутизации.

Trunk-порт в сети

Trunk-порт — это порт на коммутаторе, который передает трафик сразу нескольких VLAN. В отличие от Access-порта, который принадлежит только одной VLAN, Trunk использует тегирование кадров для различения VLAN.

Как работает Trunk-порт?

- Передача данных идет с добавлением тегов VLAN по стандарту IEEE 802.1Q.
- Кадры, идущие от Trunk-порта, содержат дополнительный заголовок, указывающий, к какой VLAN относится пакет.
- Trunk-порты применяются для соединения коммутаторов или подключения устройств, поддерживающих несколько VLAN, например, маршрутизаторов.

VLAN (Virtual Local Area Network)

VLAN (виртуальная локальная сеть) — это логически выделенный сегмент в сети, работающий как отдельная подсеть. VLAN позволяют разделить одну физическую сеть на несколько виртуальных, повышая безопасность, управляемость и эффективность сети.

1. Зачем нужны VLAN?

Без VLAN все устройства в сети находятся в одном широковещательном домене, что приводит к увеличению трафика, снижению безопасности и усложнению управления сетью. Использование VLAN позволяет разделить устройства на логические группы, уменьшить широковещательный трафик, повысить безопасность и упростить администрирование.

2. Принцип работы VLAN

Каждая VLAN функционирует как отдельная логическая сеть. Устройства внутри одной VLAN могут обмениваться данными напрямую, а устройства в разных VLAN требуют маршрутизации.

При передаче пакетов они могут быть **нетегированными (Untagged)** — обычные Ethernet-кадры, или **тегированными (Tagged)** — с заголовком VLAN (IEEE 802.1Q), содержащим номер VLAN.

Коммутаторы используют два основных типа портов:

- **Access-порт** принадлежит только одной VLAN и передает нетегированные кадры.
- **Trunk-порт** передает трафик нескольких VLAN с тегами 802.1Q.

3. Протоколы VLAN

Для работы VLAN используется стандарт **IEEE 802.1Q**, который добавляет к кадрам тег с номером VLAN. Устаревший протокол **ISL (Inter-Switch Link)**, разработанный Cisco, встречается только на старых устройствах этой компании.

4. Взаимодействие VLAN

Поскольку VLAN создают отдельные широковещательные домены, для обмена данными между VLAN требуется маршрутизация. Это можно сделать двумя способами:

1. **Через маршрутизатор** (Router-on-a-Stick) — используется один физический интерфейс с подинтерфейсами для каждой VLAN.
2. **Через коммутатор уровня 3** — создаются виртуальные интерфейсы SVI, выполняющие маршрутизацию внутри коммутатора.

5. Настройка VLAN

Создание и назначение VLAN на Cisco-коммутаторе

bash

```
Switch(config)# vlan 10
Switch(config-vlan)# name ACCOUNTING
Switch(config)# vlan 20
Switch(config-vlan)# name IT

Switch(config)# interface FastEthernet 0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 10

Switch(config)# interface FastEthernet 0/2
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 20
```

Настройка Trunk-порта

bash

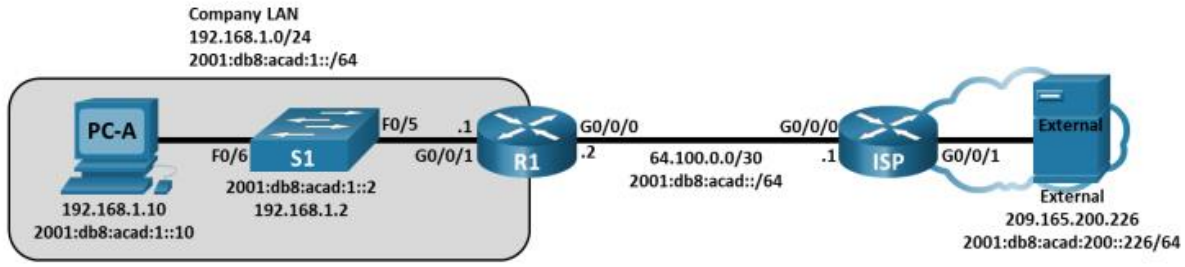
```
Switch(config)# interface FastEthernet 0/24
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan 10,20
```

6. Достоинства и недостатки VLAN

Использование VLAN повышает безопасность, уменьшает широковещательный трафик и делает сеть более управляемой. Однако неправильная настройка может привести к потерям связи, а маршрутизация между VLAN требует дополнительного оборудования.

(13.3.2)Тестирование сетевого подключения

1.1 Топология



1.2 Таблица адресации

Устройство	Интерфейс	IP-адрес / Префикс	Шлюз по умолчанию
R1	G0/0/0	64.100.0.2 /30	N/A
R1	G0/0/0	2001:db8:acad::2 /64	N/A
R1	G0/0/1	192.168.1.1 /24	N/A
ISP	G0/0/0	64.100.0.1 /30	N/A
ISP	G0/0/1	209.165.200.225 /27	N/A
S1	VLAN 1	192.168.1.2 /24	192.168.1.1
PC-A	NIC	192.168.1.10 /24	192.168.1.1
External	NIC	209.165.200.226 /27	209.165.200.225

1.3 Задачи

Часть 1: Использование команды для базового тестирования сети

1. **Проверка доступности устройств**

Используйте команду для отправки запросов к различным устройствам в сети.

2. **Анализ задержек и потерь пакетов**

Проверьте среднее время отклика и процент потерь.
Определите возможные узкие места в сети. Для этого подготовьте таблицу анализа

Часть 2: Использование команд для тестирования сети

1. **Определение маршрутов прохождения пакетов**

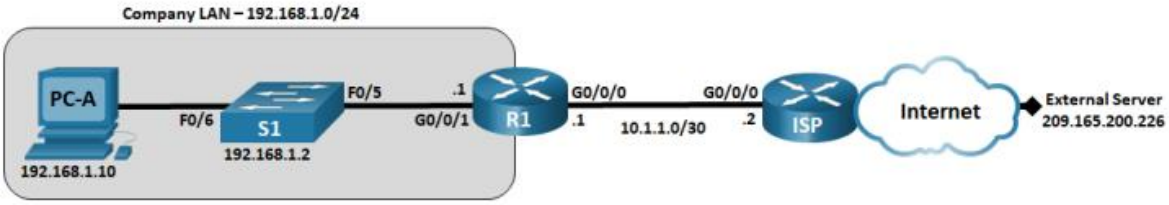
   Используйте команды для отображения маршрута прохождения пакетов. Определите возможные точки задержек и узлы отказа.

2. **Проверка конфигурации маршрутизации**

   Используйте команды для диагностики маршрутов.
   Убедитесь, что IP-адреса настроены правильно.

(17.4.6) Устранение проблем с подключением

2.1 Топология



2.2 Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1	G0/0/0/1	192.168.1.1	255.255.255.0	N/A
R1	G0/0/0	10.1.1.1	255.255.255.252	N/A
ISP	G0/0/0	10.1.1.2	255.255.255.252	N/A
ISP	Lo0	209.165.200.226	255.255.255.255	N/A
S1	VLAN 1	192.168.1.2	255.255.255.0	192.168.1.1
PC-A	NIC	192.168.1.10	255.255.255.0	192.168.1.1

2.3 Задачи

Часть 1: Определение проблемы

1. **Анализ сети с помощью команд диагностики**
   Используйте команды для выявления проблем.
   Определите узлы с высокой задержкой или потерей пакетов.

Часть 2: Внесение изменений в сеть

1. **Настройка маршрутов и IP-адресов**
   Проверьте таблицы маршрутизации и скорректируйте при необходимости.
   Убедитесь, что все устройства используют правильные шлюзы.
2. **Проверка доступности внешнего сервера**
   Используйте `ping` и `traceroute` для проверки связи с `209.165.200.226`.

Часть 3: Проверка работоспособности сети

1. **Проверка связи между узлами**
   Убедитесь, что PC-A, S1 и R1 могут доступны друг друга.
2. **Тестирование стабильности сети**
   Проверьте стабильность соединения в течение нескольких минут.

Часть 4: Документирование исправлений

Задокументируйте все найденные ошибки.

Используйте команды для сохранения конфигурации.

Когда вы вводите URL (например, http://www.cisco.com) в браузере, система доменных имен (DNS) преобразует доменное имя (www.cisco.com) в IP-адрес, чтобы компьютер мог найти нужный сервер. В этой лабораторной работе мы наблюдаем за этим процессом и используем команду `nslookup` для получения дополнительной информации о DNS.

(15.4.8) Наблюдение за преобразованием URL в IP-адрес

1. Откройте командную строку Windows.
2. Выполните команду `ping www.icann.org`.
    a. DNS переведет www.icann.org в IP-адрес и выполнит проверку соединения.
    b. Если отображается IPv6-адрес, можно использовать команду `ping -4 www.icann.org`, чтобы получить IPv4-адрес.
3. Запишите IP-адрес www.icann.org.
4. Введите полученный IP-адрес в браузер (например, https://192.0.32.7).
5. Повторите эти шаги для www.cisco.com и сравните результаты.

Часть 2: Использование nslookup для анализа DNS-запроса веб-сайта

1. В командной строке выполните команду `nslookup`.
2. Введите `www.cisco.com`.
3. Сравните результаты с `ping www.cisco.com`.
4. Введите команду `nslookup 172.230.155.162` (замените на свой IP). Узнайте, к какому домену привязан этот IP.
5. Выполните `nslookup www.google.com` и запишите полученные IP-адреса.

Часть 3: Использование nslookup для анализа почтовых серверов

1. В `nslookup` введите команду `set type=mx`.
2. Введите `cisco.com`.
3. Определите, какой сервер будет использоваться первым.
4. Введите команду `ipconfig /all` и запишите используемые DNS-серверы.