1.Понятие коммутация. Способы коммутации.

Термин.

Коммутация - это процесс объединения абонентов сети с помощью транзитных узлов, посредством разбиения информации на сообщения, которые передаются последовательно.

Коммутация — это процесс пересылки данных через сеть от источника к получателю через промежуточные узлы

Цель коммутации:

- доставка кадров конкретному получателю;
- уменьшение коллизий;
- повышение производительности сети.

Способы коммутации.

Существует три основных способа:

1. Коммутация каналов

Перед началом передачи данных между конечными узлами устанавливается **выделенный физический канал**, который закрепляется

за ними на всё время сеанса связи. Канал монополизирован, даже если в паузах данные не передаются.

Плюсы:

- Гарантированная и постоянная пропускная способность.
- Предсказуемые задержки, данные приходят в том же порядке, в котором были отправлены.

Минусы:

- Неэффективное использование канала (простой в паузах).
- Длительное время установления соединения.
- Устойчивость к отказам низкая (при обрыве канала соединение рвётся).

2. Коммутация сообщений

Данные передаются **целиком, как единое логическое сообщение**. Каждый промежуточный узел (шлюз) принимает всё сообщение целиком, сохраняет его в своей памяти, проверяет на ошибки, а затем выбирает следующий узел и пересылает его дальше.

Плюсы:

- Более эффективное использование каналов, чем при коммутации каналов.
- Возможность управления приоритетами сообщений.
- Не требуется предварительное установление соединения.

Минусы:

- Требует больших буферов на промежуточных узлах для хранения целых сообщений.

- Большие задержки, так как передача на следующий узел начинается только после приёма ВСЕГО сообщения.
- Не подходит для интерактивного трафика (голос, видео).

3. Коммутация пакетов

Это основа современных компьютерных сетей, включая Интернет. Передаваемые данные разбиваются отправителем на небольшие фрагменты — **пакеты**. Каждый пакет снабжается заголовком с адресом назначения и служебной информацией. Пакеты независимо друг от друга путешествуют по сети, причём **маршруты разных пакетов одного сообщения могут быть разными**. На принимающей стороне пакеты собираются в исходное сообщение.

Плюсы:

- Максимально эффективное использование пропускной способности сети (канал не простаивает).
- Устойчивость к отказам: при повреждении одного маршрута пакеты могут пойти другим путём.
- Высокая скорость передачи (пакеты обрабатываются "на лету", не дожидаясь всего сообщения).

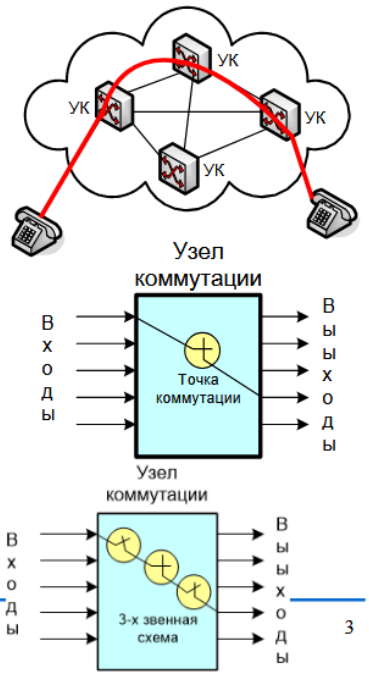
Минусы:

- Задержки (latency) и вариация задержек (jitter) из-за возможных очередей в узлах.
- Необходимость сборки пакетов и контроля порядка их следования.
- Возможны потери пакетов при перегрузке сети.

2.Основные принципы коммутации. Методы коммутации.

2.1. Общие принципы коммутации

- ***Коммутация*** – процесс соединения пользователей в сети через узлы коммутации (УК).
- ***Узел коммутации*** – сетевой узел, осуществляющий коммутацию входов и выходов узла для реализации соединений в сети.
- ***Точка коммутации*** – место (время) соединения входа и выхода (или промежуточной линии – при многозвенной коммутации).
- ***Многозвенная коммутация*** – вход и выход узла коммутации соединяются через несколько точек коммутации.



Метод	Суть
1. Коммутация каналов	Сначала **устанавливается физическое соединение** (канал), которое занято всё время сеанса.
2. Коммутация сообщений	Данные передаются **целиком** (файл, письмо). Каждый узел принимает, сохраняет и только потом пересылает дальше.
3. Коммутация пакетов (ГЛАВНЫЙ метод для сетей)	Данные **разбиваются на пакеты.** Пакеты идут независимо, могут разными путями, собираются в конце.

[3.Классификация коммутаторов. Характеристики коммутаторов.]

Классификация коммутаторов

1. По уровню модели OSI

- Неуправляемые:
  - Работают «из коробки», настройка не требуется.
- Управляемые:
  - Имеют интерфейс управления (CLI, Web, SNMP) для тонкой настройки.
  - Поддерживают продвинутые протоколы (VLAN, STP, QoS, агрегация каналов).

2. По роли в сети

- Фиксированные: Имеют фиксированное количество портов (8, 24, 48). Самый распространённый тип.
- Модульные: «Шасси» со слотами, куда вставляются модули с портами. Высокая гибкость и отказоустойчивость. Для ядра сети.
- Стек-коммутаторы: Несколько физических коммутаторов соединяются высокоскоростными шинами и работают как одно логическое устройство с единой точкой управления.

3. По уровню коммутации

- Коммутаторы 2-го уровня (L2 Switch): Основной тип. Работают с MAC-адресами и кадрами Ethernet. Не «видят» IP-адреса.
- Коммутаторы 3-го уровня (L3 Switch): По сути, гибрид коммутатора и маршрутизатора. Могут коммутировать кадры на L2, но также маршрутизировать пакеты между подсетями на L3 (по IP-адресам). Ключевое для крупных сетей.
- Коммутаторы 4-го уровня и выше (L4+/Application-aware): Могут принимать решения на основе информации из транспортного и

прикладного уровней (порты TCP/UDP, содержимое). Для балансировки нагрузки и безопасности.

4. По способу коммутации

- С промежуточным хранением (Store-and-Forward):
  - Принимает весь кадр → проверяет CRC на ошибки → затем пересылает.
- Сквозной (Cut-Through):
  - Начинает передачу, как только считал MAC-адрес назначения (первые 6 байт).
- Бесфрагментный (Fragment-Free, Modified Cut-Through):
  - Принимает первые 64 байта (мин. размер кадра), проверяет на коллизии → затем передаёт.
  - Компромисс между скоростью и контролем ошибок.

Характеристики коммутаторов:

- Скорость портов и общая пропускная способность - (Fast Ethernet,Gigabit Ethernet)
- Таблица MAC-адресов - Количество MAC-адресов
- Размер кадров - Поддержка увеличенных кадров
- поддержка протоколов (STP, VLAN, QoS,RSTP/MSTP)

4. Принципы работы коммутатора.

Алгоритм:

1. Получение кадра
2. Анализ Source MAC → запись в таблицу
3. Анализ Destination MAC
4. Передача или flood (для broadcast и unknown unicast)

5. Очистка устаревших записей

5. Методы построения таблиц коммутации. Режимы работы коммутаторов. Просмотр и настройка таблиц MAC-адресов.

Методы построения таблиц:

1. Статическая настройка - Администратор вручную добавляет записи

2. Динамическое прослушивание - IGMP Snooping, DHCP Snooping**.**

Режимы работы коммутаторов:

Режимы работы коммутаторов:

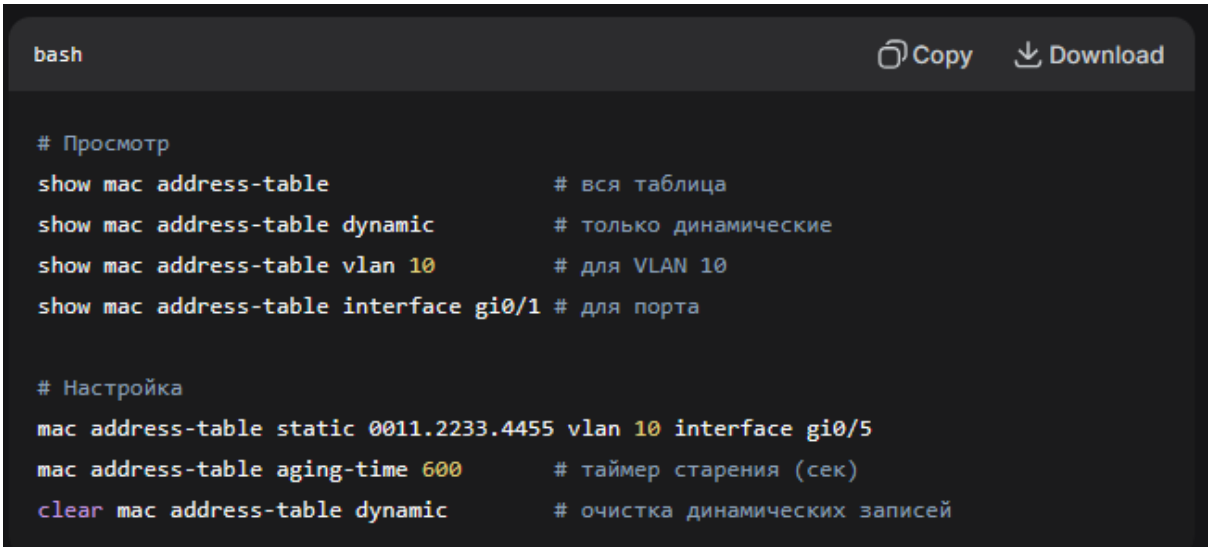
По способу коммутации кадров:

Режим	Принцип	Задержка	Контроль ошибок
Store-and-Forward	Принять весь кадр → проверить CRC → передать	Максимальная	Да (отбрасывает ошибочные)
Cut-Through	Прочитать адрес получателя (6 байт) → начать передачу	Минимальная	Нет (передаёт с ошибками)
Fragment-Free	Принять 64 байта → проверить → передать	Средняя	Частичный (от коллизий)

По буферизации:

- **Port-based** — у каждого порта свой буфер
- **Shared Memory** — общий буфер для всех портов (эффективнее)

Просмотр и настройка таблиц MAC-адресов.



6. Базовые настройки коммутатора.

- Имя устройства
- Настройка IP-адресации
- Настройка портов
- Настройка VLAN
- шлюз по умолчанию
- защита доступа(добавление пароля)
- Безопасность портов (Port Security, SSH вместо Telnet)
- отключение неиспользуемых портов.

7. Основные принципы проектирования коммутируемых сетей. Иерархическая трехуровневая модель построения сети.

Основные принципы проектирования коммутируемых сетей

1. Иерархичность

- **Разделение на уровни** (доступ, распределение, ядро)
- Каждый уровень решает свои задачи
- Упрощает проектирование, масштабирование, поиск проблем

2. Модульность

- Сеть делится на **функциональные блоки**
- Каждый блок можно проектировать и модернизировать отдельно
- Примеры блоков: офисный сегмент, серверная, WAN-подключение

3. Отказоустойчивость

- **Избыточность** на всех уровнях
- Дублирование критичных элементов
- Быстрое восстановление при сбоях (STP, EtherChannel)

4. Масштабируемость

- Возможность **легкого расширения**
- Добавление новых пользователей без перестройки сети
- Резерв производительности на 3-5 лет

5. Безопасность

- **Сегментация** сети (VLAN)
- Контроль доступа между сегментами
- Защита от broadcast storms

6. Производительность

- **Согласование пропускной способности** между уровнями
- Предотвращение узких мест (bottleneck)
- Качество обслуживания (QoS) для приоритетного трафика

Иерархическая трехуровневая модель

Уровень 1: Доступ (Access Layer)

```
Назначение:
- Подключение конечных устройств (ПК, телефоны, принтеры)
- Контроль доступа к сети

Оборудование:
- Неуправляемые/управляемые коммутаторы
- Точки доступа Wi-Fi

Функции:
• Port Security (безопасность портов)
• VLAN assignment (назначение VLAN)
• STP на портах (PortFast)
• PoE для IP-телефонов/камер
• Basic QoS marking
```

Уровень 2: Распределение (Distribution Layer)

```
Назначение:
- Агрегация трафика от коммутаторов доступа
- Граница между сетями (маршрутизация)

Оборудование:
- Мощные L3 коммутаторы
- Маршрутизаторы

Функции:
• Маршрутизация между VLAN
• Фильтрация трафика (ACL)
• Агрегация каналов (EtherChannel)
• Контроль широковещательных доменов
• Advanced QoS
• Redundancy (HSRP, VRRP)
```

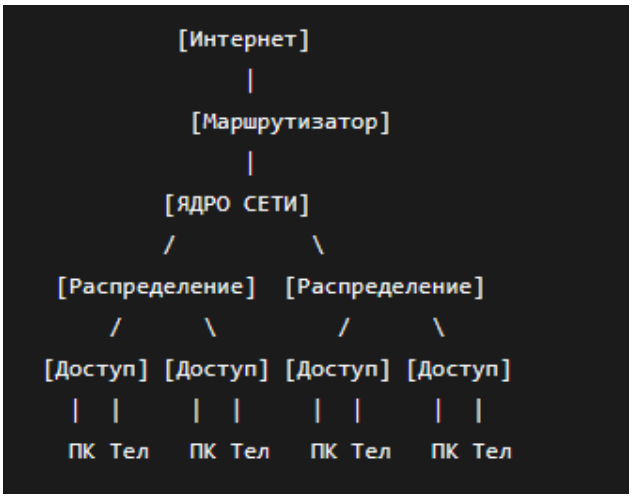
Уровень 3: Ядро (Core Layer)

```
Назначение:
- Высокоскоростная транспортировка трафика
- Соединение распределительных блоков

Оборудование:
- Высокопроизводительные L3 коммутаторы
- Скорость портов 10/40/100 Гбит/с

Функции:
• Максимальная скорость и надежность
• Минимальная задержка (low latency)
• Отказоустойчивость (без STP, только маршрутизация)
• Быстрая конвергенция при сбоях
```

Пример сети по модели:



Преимущества трехуровневой модели:

1. Простота проектирования — каждый уровень имеет четкие задачи
2. Легкость масштабирования — можно добавлять блоки доступа
3. Упрощение поиска неисправностей — проблемы локализуются по уровням
4. Предсказуемая производительность — пропускная способность планируется
5. Снижение стоимости — оборудование подбирается под задачи уровня

8. Безопасность в коммутируемых сетях. Принципы обеспечения безопасности коммутируемой сети.

1. MAC-атаки:

    MAC flooding — переполнение таблицы MAC-адресов

    MAC spoofing — подмена MAC-адреса

2. VLAN-атаки:

    VLAN hopping — несанкционированный доступ к другому VLAN

    Double tagging — двойная VLAN-разметка

3. Атаки на протоколы:

    STP атаки — захват root bridge

    DHCP spoofing — подмена DHCP-сервера

    ARP spoofing — подмена ARP-таблиц

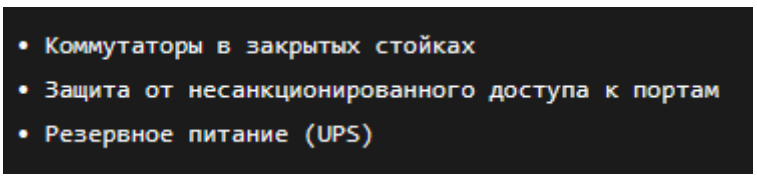
4. Несанкционированный доступ:

    Подключение к свободным портам

    Доступ к управлению коммутатором

Принципы обеспечения безопасности

Принцип 1: Физическая защита



Принцип 2: Сегментация сети - разделение сети на VLAN

Принцип 3: Контроль доступа к портам

Принцип 4: Защита от VLAN-атак

Настройка транковых портов: Защита от DTP (Dynamic Trunking Protocol)

Принцип 5: Безопасность управления - Настройка SSH вместо Telnet

Принцип 6: Защита от ARP/DHCP атак - DHCP Snooping и Dynamic ARP Inspection (DAI)

Принцип 7: Защита STP - BPDU Guard & Root Guard

Принцип 8: ACL (Access Control Lists) - Фильтрация между VLAN

9. Port Security. Режимы Port Security.

Port Security — технология контроля доступа к порту коммутатора по MAC-адресам. (**Фиксирует**, какие устройства могут подключаться к порту.)

Принцип работы:

1. **Изучение MAC-адресов** на порту
2. **Сравнение** с разрешенным списком
3. **Действие при нарушении** (заранее настроенное)

Позволяет:

- ограничить число MAC;

- зафиксировать MAC за портом.

Режимы:

- protect; **«Защищать»**
    - **Лишние MAC-адреса блокируются**
    - **Порт остается включенным**
    - **Нет уведомлений в логах**
- restrict; **«Ограничивать»**
    - **Лишние MAC блокируются**
    - **Порт работает**
    - **Отправляет SNMP-траппы и логи**
    - **Счетчик нарушений увеличивается**
- shutdown (самый строгий). **«Отключать»**
    - **Порт сразу отключается** (err-disable state)
    - **Требует ручного включения** (shutdown/no shutdown)
    - **SNMP-траппы и логи отправляются**

10. Общая настройка безопасности

- BPDU Guard — защита STP;
- DHCP Snooping — защита от rogue DHCP;
- DAI — защита ARP;
- Storm Control — защита от broadcast storm.

11. Настройка Port Security

Основные параметры:

- maximum;

- violation mode;
- sticky MAC.

Типичное применение: порты доступа пользователей.

10. Настройка параметров безопасности коммутатора.

1. Базовые меры безопасности

- Пароли: сложные, разные для console/vty/enable
- Шифрование паролей в конфигурации
- SSH вместо Telnet, отключение неиспользуемых сервисов (HTTP, CDP)

2. Безопасность портов (Port Security)

- Ограничить количество MAC-адресов на порту (обычно 1-3)
- Режимы при нарушении: Restrict/Shutdown
- Sticky MAC: автоматическое запоминание устройств
- На всех пользовательских портах

3. VLAN безопасность

- Отдельный VLAN для управления (Management VLAN)
- Native VLAN ≠ 1 (поменять на неиспользуемый)
- Explicit VLAN listing на транках
- DTP отключить (nonegotiate)

4. Защита протоколов

- DHCP Snooping: защита от подмены DHCP-сервера
- DAI (ARP Inspection): защита от ARP-спуфинга
- STP защита: BPDU Guard на access-портах, Root Guard на uplink
- Storm Control: ограничение broadcast/multicast штормов

5. Контроль доступа (ACL)

- Фильтрация между VLAN (если нужна изоляция)
- Ограничение доступа к управлению (только с определенных IP)
- Логирование нарушений

6. Мониторинг и логирование

- Настройка syslog на внешний сервер
- SNMPv3 для мониторинга (аутентификация + шифрование)
- Таймстемпы в логах

7. Обязательный минимум на каждый порт:

- 1. Port Security (max 2 MAC, violation restrict)
- 2. PortFast + BPDU Guard
- 3. Назначение VLAN
- 4. Описание порта
- 5. Отключение ненужных протоколов (CDP)

11. Настройка Port Security.

1. Включить Port Security на порту:

```
interface gi0/1
 switchport port-security
```

2. Задать лимит MAC-адресов:

```
switchport port-security maximum 2    # максимум 2 устройства
```

3. Выбрать действие при нарушении:

```
switchport port-security violation restrict   # блокировать, но порт работает
# ИЛИ
switchport port-security violation shutdown   # отключить порт полностью
```

4. Способ определения MAC:

```
switchport port-security mac-address sticky   # САМЫЙ ЧАСТЫЙ
```

Коммутатор сам запомнит первые 2 устройства и сохранит их в конфиг.

Быстрая настройка для всех портов:

```
interface range gi0/1-24
 switchport port-security
 switchport port-security maximum 2
 switchport port-security violation restrict
 switchport port-security mac-address sticky
 spanning-tree portfast
```

Важно:

1. Работает только на access-портах
2. Sticky — самый удобный метод

3. Restrict — порт работает, администратор видит нарушение
4. Shutdown — максимальная защита, но требует ручного восстановления

12. Настройка виртуальных локальных сетей на коммутаторах.

Виртуальная локальная сеть — логическое разделение физической сети на изолированные сегменты.

1. Создать VLAN:

```
vlan 10
 name Sales        # имя для VLAN 10
vlan 20
 name Accounting   # VLAN 20
```

2. Назначить порты в VLAN:

```
interface gi0/1
 switchport mode access      # режим доступа (для устройств)
 switchport access vlan 10   # добавить порт в VLAN 10
```

3. Настроить транк между коммутаторами:

```
interface gi0/24
 switchport mode trunk                 # режим транка
 switchport trunk allowed vlan 10,20     # какие VLAN пропускать
```

Быстрая настройка для группы портов:

```
interface range gi0/1-10
 switchport mode access
 switchport access vlan 10
```

Важно:

1. Access порт — для конечных устройств (ПК, телефоны)
2. Trunk порт — для связи между коммутаторами
3. VLAN 1 — по умолчанию, лучше использовать другие
4. Native VLAN — должен совпадать на обоих концах транка

13. Виртуальные локальные сети VLAN. Способы организации VLAN. Виды VLAN.

Виртуальные локальные сети VLAN

Логическое разделение одной физической сети на несколько изолированных широковещательных доменов.

Зачем нужно:

- Безопасность (изоляция отделов)
- Уменьшение broadcast-трафика
- Группировка по функциям (финансы, отдел продаж, гости)

3 способа организации VLAN

1. По портам (Port-based VLAN)

Самый распространенный

- VLAN назначается на физический порт коммутатора
- Все устройства на этом порту — в одном VLAN
- Просто, но негибко

2. По MAC-адресам (MAC-based VLAN)

- VLAN назначается по MAC-адресу устройства
- Устройство сохраняет VLAN при переподключении
- Гибко, но сложнее в управлении

3. По IP-адресам (Protocol-based VLAN)

- Разделение по протоколу (IP, IPX) или подсети
- Редко используется

Типы портов

Тип порта	Назначение	Пример
Access	Для конечных устройств	ПК, телефон, принтер
Trunk	Для связи коммутаторов	Кабель между свитчами
Hybrid	И access, и trunk (не Cisco)	—

14. Порядок настройки VLAN на коммутаторе.

Шаг 1: Создать VLAN

```
vlan 10
 name Sales          # дать имя VLAN
```

Шаг 2: Назначить порты в VLAN

```
interface gi0/1
 switchport mode access      # режим доступа
 switchport access vlan 10   # поместить порт в VLAN 10
```

Шаг 3: Настроить транковые порты

(если есть другие коммутаторы)

```
interface gi0/24
 switchport mode trunk                 # режим транка
 switchport trunk allowed vlan 10,20   # разрешить VLAN
```

Шаг 4: Настроить Management VLAN

```
interface vlan 99
 ip address 192.168.99.10 255.255.255.0
 no shutdown
```

Важные моменты:

1. Порядок важен: сначала создать VLAN, потом назначать порты
2. Access порты — для устройств, Trunk порты — для связи свитчей
3. VLAN 1 — не использовать для данных
4. Сохранять конфигурацию после настройки

15. Организация магистральных линий связи на коммутаторах с несколькими VLAN

Магистраль — один физический канал, передающий трафик нескольких VLAN между коммутаторами.

Настройка Trunk (шаги):

1. Включить режим trunk:

interface gi0/24

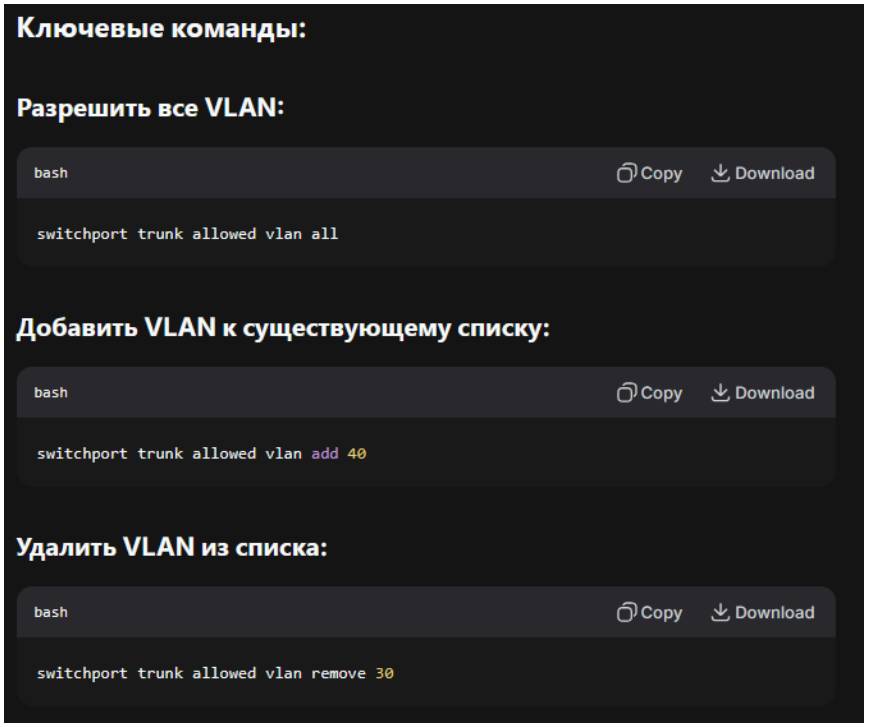
switchport mode trunk

2. Указать разрешенные VLAN:

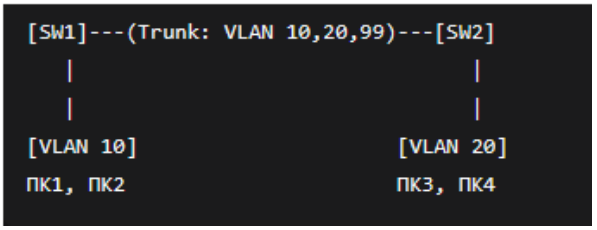
switchport trunk allowed vlan 10,20,30,99

3. Изменить Native VLAN (рекомендуется):

switchport trunk native vlan 999 # вместо VLAN 1



Пример сети с Trunk:



Настройка позволяет:
ПК1 (VLAN 10 на SW1) ↔ ПК2 (VLAN 10 на SW2) — общаются через trunk
При этом трафик VLAN 10 изолирован от VLAN 20

16. Организация маршрутизации трафика различных виртуальных сетей. Техника Router-on-a-stick (ROAS) для обеспечения IP маршрутизации между VLANами

Организация маршрутизации трафика между VLAN

A. Организация маршрутизации между VLAN

Проблема:

Устройства в разных VLAN не могут общаться напрямую, даже если подключены к одному коммутатору.

Требуется:

Маршрутизатор (или L3-коммутатор), который будет пересылать пакеты между VLAN.

Основные способы:

1. Через отдельные физические порты роутера

- Каждый VLAN → отдельный кабель → отдельный порт роутера
- Неэффективно: много кабелей, много портов

2. Router-on-a-Stick (ROAS)

- Один физический порт роутера → транк → коммутатор
- На одном порту создаются подинтерфейсы для каждого VLAN
- Оптимально для малых сетей

3. L3-коммутатор

- Коммутатор сам маршрутизирует между VLAN
- SVL (Switched Virtual Interfaces) — виртуальные интерфейсы VLAN
- Лучшее решение для средних/крупных сетей

Техника Router-on-a-Stick (ROAS)

Один физический порт маршрутизатора обслуживает несколько VLAN через подинтерфейсы с тегированием 802.1Q.

Топология

```
[PC1 в VLAN 10]---[Switch]---(Trunk)---[Router]---(Trunk)---[Switch]---[PC2 в VLAN 20]
```

Как работает ROAS:

1. PC1 (VLAN 10, IP 192.168.10.5) хочет отправить пакет PC2 (VLAN 20, IP 192.168.20.10)
2. Коммутатор добавляет тег VLAN 10 и отправляет на роутер через транк
3. Маршрутизатор принимает пакет на gi0/0.10
4. Роутер смотрит таблицу маршрутизации и решает отправить через gi0/0.20
5. Роутер отправляет пакет с тегом VLAN 20 через транк
6. Коммутатор получает пакет, удаляет тег и отправляет PC2

Преимущества ROAS:

- Экономия портов на маршрутизаторе
- Простота настройки
- Низкая стоимость (не нужен L3-коммутатор)

Недостатки:

- Пропускная способность ограничена одним каналом
- Высокая нагрузка на процессор роутера
- Не подходит для высоконагруженных сетей

17. Автоматизация настройки VLAN на коммутаторе. Протокол VTP и GVRP (MVRP).

Автоматизация настройки VLAN. VTP и GVRP/MVRP

18. Обеспечение отказоустойчивости в коммутируемых сетях. Протоколы семейства STP

Отказоустойчивость — способность сети продолжать работу при выходе из строя отдельных компонентов (кабелей, портов, коммутаторов).

Основные принципы:

1. Избыточность — дублирование критичных элементов

2. Автоматическое восстановление — без вмешательства администратора
3. Минимальное время простоя — быстрая конвергенция

Типы избыточности:

- Физическая: Дублирование кабелей, коммутаторов, источников питания
- Логическая: Протоколы для автоматического переключения на резервный путь

Проблема петель (loops) и её решение

Проблема:

При создании избыточных соединений образуются петли, которые вызывают:

1. Broadcast-шторм — бесконечная циркуляция широковещательных кадров
2. Множественные копии unicast-кадров
3. Нестабильность таблиц MAC-адресов
4. Полный отказ сети

Решение:

Протоколы семейства STP (Spanning Tree Protocol) автоматически блокируют избыточные пути, создавая древовидную топологию без петель.

Протоколы семейства STP

1. STP (Spanning Tree Protocol) — IEEE 802.1D

Первая версия, классический протокол.

Принцип работы:

- Выбор Root Bridge (корневого коммутатора)
- Расчет путей до Root Bridge
- Блокировка избыточных портов
- Активация заблокированных портов при аварии

Недостатки:

- Медленная конвергенция (30-50 секунд)
- Нет различения портов к пользователям и коммутаторам

---

2. RSTP (Rapid Spanning Tree Protocol) — IEEE 802.1w

Ускоренная версия STP.

Улучшения:

- Конвергенция за 1-3 секунды вместо 30-50
- Новые типы портов:
  - Designated/Alternate/Backup (вместо Blocking/Listening/Learning)
- Быстрое переключение при авариях
- Обратная совместимость с STP

---

3. MSTP (Multiple Spanning Tree Protocol) — IEEE 802.1s

Поддержка нескольких независимых деревьев.

Преимущества:

- Несколько VLAN → несколько деревьев STP
- Балансировка нагрузки — разные VLAN идут разными путями
- Эффективнее чем один STP для всех VLAN

---

4. PVST+ (Per-VLAN Spanning Tree) — проприетарный Cisco

Отдельное STP дерево для каждого VLAN.

Особенности:

- Только для оборудования Cisco
- Максимальная гибкость
- Высокая нагрузка на коммутаторы (много инстансов STP)

19. Технологии повышения надежности и производительности в коммутируемых сетях. Сравнение протоколов STP, RSTP, MSTP

1. Технологии надежности

- STP/RSTP/MSTP — защита от петель
- EtherChannel (LACP) — объединение каналов (пропускная способность + отказоустойчивость)

- StackWise/VSS — объединение коммутаторов в стек

2. Сравнение STP, RSTP, MSTP

Параметр	STP (802.1D)	RSTP (802.1w)	MSTP (802.1s)
Конвергенция	30-50 сек	**1-3 сек**	**1-3 сек**
Деревья	1 для всех VLAN	1 для всех VLAN	**Несколько** (по группам VLAN)
Балансировка	Нет	Нет	**Да** (разные VLAN — разные пути)
Порты	5 состояний	3 состояния	3 состояния
Применение	Устарел	Средние сети	Крупные сети с VLAN

Выбор:

- RSTP — для большинства сетей
- MSTP — если нужна балансировка нагрузки между каналами

20. Методы разрешения петель коммутации. Протоколы STP. RSTP. PVST.

Методы разрешения

- Ручное проектирование без избыточности (ненадежно)
- Алгоритмы коммутации с проверкой петель (неэффективно)
- Протоколы STP (основное решение)

Протоколы STP семейства

STP (Spanning Tree Protocol) - 802.1D

- 1 дерево для всей сети
- Блокирует избыточные порты
- Медленный: конвергенция 30-50 сек
- Состояния портов: Blocking → Listening → Learning → Forwarding

RSTP (Rapid STP) - 802.1w

- Быстрый: конвергенция 1-3 сек
- 3 состояния: Discarding, Learning, Forwarding
- Типы портов: Root, Designated, Alternate, Backup
- Обратная совместимость со STP

PVST/PVST+ (Per-VLAN Spanning Tree) - Cisco

- Отдельное дерево для каждого VLAN
- Балансировка нагрузки возможна
- Только для оборудования Cisco
- Большая нагрузка на CPU

21.Принципы работы STP. Типы и состояние портов. Алгоритм покрывающего дерева.

Автоматически отключает избыточные пути в сети, создавая **беспетельное дерево** (spanning tree).

2. Типы портов в STP

По роли в дереве:

- **Root Port (RP)** — порт с лучшим путем к Root Bridge (на всех НЕ-root коммутаторах)
- **Designated Port (DP)** — порт, который передает трафик в сегмент (один на сегмент)
- **Non-Designated Port (NDP)** — заблокированный порт (Alternate/Backup)
- **Disabled Port** — выключен администратором

По состоянию (состояния STP):

1. **Blocking** — не передает данные, слушает BPDU (20 сек)
2. **Listening** — готовится передавать, не учит MAC (15 сек)
3. **Learning** — учит MAC-адреса, не передает данные (15 сек)
4. **Forwarding** — нормальная работа (передает данные)
5. **Disabled** — выключен

3. Алгоритм покрывающего дерева (шаги)

Шаг 1: Выбор Root Bridge

1. **Сравнивается Priority** (по умолчанию 32768, можно изменить)
2. **При равенстве** — сравнивается MAC-адрес (меньший выигрывает)
3. **Root Bridge** становится "центром" сети

Шаг 2: Выбор Root Port на каждом коммутаторе

Выбирается **один порт** с лучшим путем к Root Bridge:

1. **Lowest Root Path Cost** — наименьшая стоимость пути
2. **Lowest Sender Bridge ID** — если стоимость одинакова
3. **Lowest Sender Port ID** — если Bridge ID одинаков

Шаг 3: Выбор Designated Port в каждом сегменте

В каждом сегменте (участке между устройствами):

- Выбирается **один порт**, который будет передавать трафик
- Если коммутатор ближе к Root Bridge — его порт становится Designated

Шаг 4: Блокировка оставшихся портов

Все не-Root и не-Designated порты переходят в **Blocking** состояние.

22. Протокол ERPS. Назначение, описания алгоритма работы.

Ethernet Ring Protection Switching — протокол защиты колец Ethernet.

Цель: Быстрое восстановление связи в кольцевых топологиях при обрывах (конвергенция < 50 мс).

Применение: Metro-Ethernet, транспортные сети, промышленные сети (где нужно быстрое восстановление).

2. Принцип работы

Основная идея:

- Сеть строится в виде **кольца** (физически)
- Один порт в кольце **блокируется** для предотвращения петель
- При обрыве — заблокированный порт **мгновенно открывается**

Компоненты:

- **RPL (Ring Protection Link)** — защитное звено (заблокированный порт)
- **RPL Owner** — узел, который блокирует RPL
- **RPL Neighbor** — соседний узел к RPL Owner

---

3. Алгоритм работы (шаги)

Шаг 1: Инициализация кольца

1. Все узлы в кольце обмениваются **R-APS (Ring APS) сообщениями**
2. **RPL Owner** блокирует свой RPL-порт (предотвращает петлю)

3. Кольцо работает как **линия** (логически)

Шаг 2: Нормальная работа

- **RPL Owner** периодически отправляет **NR (No Request)** сообщения
- Все узлы знают, что кольцо целое
- Данные идут по активному пути, RPL-порт заблокирован

Шаг 3: Обрыв обнаружен

1. Узлы по обе стороны обрыва **перестают получать R-APS сообщения**
2. Они отправляют **SF (Signal Fail)** сообщения в кольцо
3. Сообщения распространяются в обе стороны

Шаг 4: Восстановление

1. **RPL Owner** получает SF сообщение
2. **Немедленно разблокирует** RPL-порт (менее 50 мс)
3. Данные идут через ранее заблокированный порт
4. Кольцо снова работает (но теперь с обрывом в другом месте)

Шаг 5: Устранение обрыва

1. Связь восстановлена физически
2. Узлы рядом с бывшим обрывом отправляют **NR сообщения**
3. **RPL Owner** получает NR, снова блокирует RPL-порт
4. Возврат к нормальному состоянию (с защитой на случай следующего обрыва)

23. Настройка протокола ERPS.

1. Подготовка

- Топология — **кольцо** (физически)
- Выбрать **RPL Owner** (один узел)
- Выбрать **RPL порт** (будет заблокирован в нормальном состоянии)

24. Технология Etherchannel. Протоколы агрегации LACP и PAgP.

EtherChannel - Объединение нескольких физических каналов в один логический для:

- Увеличения пропускной способности (сумма скоростей)
- Резервирования (при отказе одного канала — остальные работают)
- Балансировки нагрузки (трафик распределяется по каналам)

Результат: 2, 4, 8 портов → 1 логический канал.

2. Протоколы агрегации

1. LACP (Link Aggregation Control Protocol)

- Стандарт IEEE (802.3ad/802.1AX)
- Работает между любыми вендорами
- Режимы: Active (инициатор) / Passive (отвечает)

2. PAgP (Port Aggregation Protocol)

- Только Cisco
- Режимы: Desirable (инициатор) / Auto (ждёт)

25.Сравнение протоколов агрегации LACP и PAgP.

Общая цель: Оба протокола служат для автоматического объединения нескольких физических каналов связи (Ethernet-линков) в один логический канал (Link Aggregation Group / Port-Channel). Это повышает пропускную способность, обеспечивает отказоустойчивость и балансировку нагрузки.

Критерий	PAgP (Port Aggregation Protocol)	LACP (Link Aggregation Control Protocol)
Производитель / Стандарт	Проприетарный протокол Cisco.	Открытый стандарт (**IEEE 802.3ad**, теперь **802.1AX**).
Совместимость	Работает только между устройствами Cisco.	Мультивендорный, работает между оборудованием любых производителей.
Режимы работы	• **Auto** (пассивно ждет PAgP-пакеты) • **Desirable** (активно инициирует согласование) • **On** (ручное создание, без протокола)	• **Active** (активно отправляет LACP-пакеты) • **Passive** (пассивно ждет LACP-пакеты) • **On** (ручное создание, без протокола)
Идентификатор группы	Использует 8-битный **PGID** (Port Group Identifier).	Использует 16-битный **Aggregator ID**.
Гибкость	Менее гибкий в настройке параметров агрегации.	Более гибкий, поддерживает «частичную» агрегацию (например, до 16 портов в группе, из которых активно до 8).
Распространенность	Используется в чисто Cisco-средах.	**Де-факто индустриальный стандарт**. Используется повсеместно.

26.*Технология VRF.

VRF — это технология, позволяющая создать несколько независимых виртуальных таблиц маршрутизации и экземпляров FIB (Forwarding Information Base) на одном физическом маршрутизаторе или L3-коммутаторе.

Основная идея: Аналогична VLAN на канальном уровне, но для сетевого уровня (L3). Каждый VRF изолирует трафик и маршрутную информацию, как если бы это были отдельные физические устройства.

Ключевые аспекты:

1. Изоляция: Маршруты, интерфейсы и трафик в одном VRF полностью отделены от другого. У них могут быть перекрывающиеся IP-адреса (например, сеть 10.0.0.0/24 может существовать в VRF_A и VRF_B одновременно).
2. Компоненты VRF:

- Отдельная таблица маршрутизации (VRF table).
- Отдельная CEF/FIB таблица.
- Набор интерфейсов, привязанных к VRF (физических, сабинтерфейсов, логических).

3. Применение:
   - Организация услуг для разных клиентов (Multi-VRF / VPN) на оборудовании провайдера без смешивания их трафика.
   - Сегментация корпоративной сети (например, отдельные VRF для производства, офиса, гостевого доступа).
   - Лабораторные стенды и тестирование на реальном оборудовании.
   - Основа для технологий MPLS L3VPN, где VRF используются на граничных устройствах провайдера (PE-маршрутизаторах).

Принцип работы: Когда интерфейс назначается VRF, все пакеты, пришедшие на него, обрабатываются в контексте таблицы маршрутизации этого VRF. Маршрутизатор принимает решение о пересылке, основываясь только на информации из этого VRF.

27.*Протокол VRRP для решения проблемы с отказом основного шлюза.

Проблема: В стандартной Ethernet-сети при отказе маршрутизатора, являющегося шлюзом по умолчанию для хостов, вся связь с другими сетями прерывается, пока шлюз не будет восстановлен вручительно или не изменена настройка на хостах.

Решение — VRRP (Virtual Router Redundancy Protocol):
Это протокол избыточности шлюза, позволяющий создать виртуальный маршрутизатор (Virtual IP, VIP), который будет общим шлюзом для хостов в сети. В группу VRRP входят несколько физических устройств.

Принцип работы:

1. Группа VRRP: Несколько маршрутизаторов образуют группу (обычно одна и та же VLAN/подсеть).
2. Вирутальный IP (VIP) и MAC: Группе назначается виртуальный IP-адрес (который и прописывается у хостов как шлюз) и виртуальный MAC-адрес (формат 00-00-5E-00-01-XX, где XX — номер группы VRRP).
3. Роли в группе:
   - Мастер (Master): Один маршрутизатор, который отвечает за转发 трафика, адресованного на VIP. Он отправляет

периодические сообщения (ADVERTISEMENT) для подтверждения своей работоспособности.
    - Резервный/Бэкап (Backup): Один или несколько маршрутизаторов, которые отслеживают состояние Мастера. Если сообщения от Мастера перестают приходить, резервный маршрутизатор с наивысшим приоритетом становится Мастером и берет на себя обслуживание VIP.
4. Приоритет (Priority): Определяет, кто станет Мастером (по умолчанию 100). Чем выше приоритет (до 255), тем выше шанс стать Мастером.
5. Преимущества:
    - Прозрачность для конечных устройств: Хосты всегда используют один и тот же VIP в качестве шлюза.
    - Автоматическое переключение (Failover): Время восстановления обычно 1-3 секунды.
    - Балансировка нагрузки: Можно настроить разные группы VRRP, где разные физические маршрутизаторы будут Мастерами для разных подсетей.

Аналоги: HSRP (Cisco proprietary) и GLBP (Cisco, с балансировкой нагрузки). Открытым стандартом, аналогичным VRRPv2, является HSRP, а VRRPv3 поддерживает IPv6.