**«Сетевые технологии»**

1. **Модель OSI как средство описания технологий передачи данных. Адресация и описание данных.**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Уровень** | **Описание** | **PDU**  **(Protocol Data Unit)** | **Адресация** | **Протоколы** |
| **Прикладной**  Application | Обеспечивает взаимодействие пользователей с сетевыми сервисами через интерфейсы | Сообщение  (текст, файлы или другие типы данных) | Нет адресации | HTTP, FTP, SMTP, DNS, DHCP, Telnet, SSH, SNMP, POP3, IMAP |
| **Представления**  Presentation | Преобразует данные в унифицированный формат для передачи между различными операционными системами и устройствами, понятный приложениям | Представление | SSL/TLS, MIME, ASCII, EBCDIC, JPEG, MPEG |
| **Сеансовый**  Session | Управляет соединениями (сессиями) между двумя устройствами (приложениями) | Сессия | SIP, RPC, NetBIOS |
| **Транспортный**  Transport | Отвечает за передачу данных в сегментах (между приложениями), контролируя их целостность и корректность | Сегмент или датаграмма | портовые номера для идентификации приложений на устройствах | TCP, UDP, SCTP |
| **Сетевой**  Network | Управляет маршрутизацией данных, обеспечивая их доставку между различными сетями. Логическая адресация | Пакет | IP-адрес | IP (IPv4, IPv6), ICMP, IGMP, OSPF, EIGRP, BGP |
| **Канальный**  Data Link | Проверяет целостность данных и отвечает за передачу данных между устройствами по локальной сети | Кадры | MAC-адрес | Ethernet, Wi-Fi (IEEE 802.11), PPP, HDLC, ARP, RARP |
| **Физический**  Physical | Отвечает за физическую передачу данных через проводники или радиоволны | Биты | Нет адресации | Ethernet, Wi-Fi, Bluetooth,  PPP, HDLC |

PDU — это ключевая концепция в сетевой коммуникации, которая позволяет структурировать данные для их эффективной передачи и обработки на разных уровнях модели OSI. Каждый уровень добавляет свою служебную информацию, чтобы обеспечить корректную передачу данных от источника к получателю.

1. **Второй уровень модели OSI. Функционал и задачи.**

**Канальный уровень**

**[ DATA LINK L2 ]**

Этот уровень обеспечивает надёжную передачу данных, контролирует доступ к физической среде передачи данных и исправляет ошибки, которые могут возникнуть на физическом уровне.

Отвечает за передачу данных между устройствами в пределах одной сети (локальной сети, LAN).

|  |  |  |
| --- | --- | --- |
| **Функции** | **Реализация** | **Описание** |
| **Фрагментация и сборка данных** | Фрагментация | Данные, полученные с сетевого уровня, разбиваются на более мелкие блоки, называемые кадрами (frames) |
| Сборка | На принимающей стороне кадры собираются обратно в исходные данные |
| **Адресация** | MAC-адреса | Канальный уровень использует MAC-адреса для идентификации устройств в пределах локальной сети |
| **Контроль доступа к среде** | Методы доступа | Определяет, как устройства получают доступ к общей среде передачи данных |
| **Обнаружение и исправление ошибок** | Контрольная сумма CRC  (Cyclic Redundancy Check) | В заголовке фрейма содержится контрольная сумма, которая позволяет обнаружить ошибки в передаче данных |
| Исправление ошибок | В некоторых протоколах канального уровня (например, в протоколе HDLC) возможно исправление ошибок без повторной передачи данных |
| **Управление потоком** | Контроль потока | Определяет, какой узел имеет право передавать данные в текущий момент времени. Отвечает за то, чтобы передающее устройство не перегружало принимающее устройство данными, которые оно не успевает обработать |
| **Организация фреймов (кадров)** | Структура фрейма  (кадра) | Кадр состоит из заголовка (header), данных (payload) и хвоста (trailer). Заголовок содержит информацию о MAC-адресах источника и назначения, тип протокола вышестоящего уровня (например, IP), а хвост содержит контрольную сумму |

1. **Структура кадра Ethernet**

**Ethernet**

Кадр Ethernet — это единица передачи данных на канальном уровне модели OSI. Он используется для передачи данных между устройствами в локальной сети (LAN). Структура кадра Ethernet может варьироваться в зависимости от стандарта, но основные элементы остаются неизменными.

Включает в себя информацию о MAC-адресах источника и назначения, тип протокола вышестоящего уровня, данные и контрольную сумму для обнаружения ошибок.

|  |  |  |  |
| --- | --- | --- | --- |
| **Элемент** | | **Длина**  **(в байтах)** | **Назначение** |
| **Преамбула** | Preamble | **7** | Используется для синхронизации времени приема-передачи между передатчиком и приёмником. Оборудование парсит кадр, достаёт MAC-адреса и служебную информацию. |
| **Начало кадра** | Start Frame Delimiter, SFD | **1** | Обозначает начало кадра |
| **MAC-адрес назначения** | Destination MAC Address | **6** | Указывает MAC-адрес устройства-получателя. Может быть уникальным адресом (unicast), групповым адресом (multicast) или широковещательным адресом (broadcast) |
| **MAC-адрес источника** | Source MAC Address | **6** | Указывает MAC-адрес устройства-отправителя |
| **Тип/Длина** | EtherType/  Length | **2** | Указывает тип протокола вышестоящего уровня (например, IPv4, IPv6, ARP) или длину кадра. Если значение меньше 1500, то это длина кадра; если больше или равно 1536, то это тип протокола |
| **Данные** | Payload | **46-1500** | Содержит данные, передаваемые вышестоящим уровнем (например, пакет IP) |
| **Заполнитель** | Padding | **0-46** | Добавляется, если размер данных меньше минимального значения (46 байт), чтобы обеспечить минимальную длину кадра |
| **Контрольная сумма** | Frame Check Sequence, FCS | **4** | Содержит контрольную сумму (CRC), используемую для обнаружения ошибок в кадре. Принимающее устройство вычисляет CRC для принятого кадра и сравнивает его с FCS, чтобы определить, были ли ошибки при передаче |

1. **Третий уровень модели OSI. Функционал и задачи**

**Сетевой уровень**

**[ NETWORK L3 ]**

Этот уровень обеспечивает передачу пакетов через сеть, независимо от того, какие физические и канальные технологии используются.

Отвечает за маршрутизацию данных между различными сетями и управление передачей данных по пути от источника к назначению.

|  |  |  |
| --- | --- | --- |
| **Функции** | **Реализация** | **Описание** |
| **Фрагментация и сборка данных** | Фрагментация | Если пакет данных слишком большой для передачи через определённый сегмент сети, сетевой уровень может разделить его на более мелкие фрагменты (пакеты) |
| Сборка | На принимающей стороне пакеты собираются обратно в исходные данные |
| **Логическая адресация** | IP-адреса | Сетевой уровень использует IP-адреса (Internet Protocol Address) для идентификации устройств в сети |
| Подсети | IP-адреса могут быть разделены на подсети, что позволяет более эффективно управлять сетевыми ресурсами |
| **Маршрутизация** | Определение пути | Определяет оптимальный путь для передачи данных от источника к получателю через сеть. Это может включать в себя прохождение через несколько маршрутизаторов |
| Таблицы маршрутизации | Маршрутизаторы используют таблицы маршрутизации, чтобы определить, куда передавать пакеты данных |
| **Обнаружение и исправление ошибок** | Контроль ошибок | Сетевой уровень может использовать различные механизмы для обнаружения ошибок в передаче данных, хотя исправление ошибок обычно выполняется на более низких уровнях |
| Исправление ошибок | В некоторых протоколах канального уровня (например, в протоколе HDLC) возможно исправление ошибок без повторной передачи данных |
| **Управление потоком** | Контроль потока | Отвечает за то, чтобы передающее устройство не перегружало принимающее устройство данными, которые оно не успевает обработать. |
| **Логическое разделение сетей** | Виртуальные сети (VLAN) | Сетевой уровень может поддерживать виртуальные локальные сети, которые логически разделяют физическую сеть на несколько сегментов |

1. **Структура пакета IP**

**IPv4-пакет**

Пакет IP (Internet Protocol Packet) — это единица передачи данных на сетевом уровне модели OSI. Он используется для передачи данных между устройствами в сети, независимо от того, находятся ли они в одной локальной сети или в разных сетях.

Структура пакета IP включает в себя заголовок и полезную нагрузку.

|  |  |  |  |
| --- | --- | --- | --- |
| **Элемент** | | **Длина**  **(в битах)** | **Назначение** |
| **Версия** | Version | **4** | Указывает версию IP-протокола (например, IPv4 или IPv6). Для IPv4 это значение равно 4 |
| **Длина заголовка** | Internet Header Length, IHL | **4** | Указывает длину заголовка в 32-битных словах. Минимальное значение — 5 (20 байт), максимальное — 15 (60 байт). Если заголовок содержит опции, его длина может увеличиваться, что позволяет включать дополнительные параметры. |
| **Тип обслуживания** | Type of Service, TOS | **8** | Используется для указания требований к качеству обслуживания (QoS). Включает в себя приоритет, задержку, пропускную способность и надёжность.  Например, пакеты с высоким приоритетом могут быть обработаны быстрее, чем пакеты с низким приоритетом. Это особенно важно для приложений, требующих низкой задержки, таких как VoIP или видеоконференции. |
| **Общая длина** | Total Length | **16** | Указывает общую длину пакета, включая заголовок и данные, в байтах. Максимальный размер пакета — 65535 байт.  Если пакет превышает максимальную длину, он может быть фрагментирован на несколько частей, каждая из которых будет передана отдельно. |
| **Идентификатор** | Identification | **16** | Используется для идентификации фрагментов пакета. Помогает принимающей стороне собрать фрагментированный пакет. Это поле также помогает отслеживать пакеты и выявлять возможные проблемы с доставкой. |
| **Флаги** | Flags | **3** | Управляет фрагментацией пакета. Первый бит не используется, второй бит (DF — Don't Fragment) указывает, разрешена ли фрагментация, третий бит (MF — More Fragments) указывает, есть ли еще фрагменты пакета. Флаги играют важную роль в управлении фрагментацией пакетов. Если фрагментация запрещена, пакет будет отброшен, если его размер превышает максимальный размер фрейма сети. |
| **Смещение фрагмента** | Fragment Offset | **13** | Указывает позицию фрагмента в исходном пакете. Используется для правильного сборки фрагментированного пакета |
| **Время жизни** | Time to Live, TTL | **8** | Указывает максимальное количество хопов (hops), которые может пройти пакет до того, как будет уничтожен. Используется для предотвращения зацикливания пакетов. Когда TTL достигает 0, пакет удаляется |
| **Протокол** | Protocol | **8** | Указывает протокол вышестоящего уровня (например, TCP, UDP, ICMP).  Например, значение 6 указывает на TCP, а значение 17 — на UDP |
| **Контрольная сумма заголовка** | Header Checksum | **16** | Используется для обнаружения ошибок в заголовке пакета. Принимающее устройство вычисляет контрольную сумму и сравнивает её с этим значением. Если контрольная сумма не совпадает, пакет считается повреждённым и удаляется |
| **IP-адрес источника** | Source IP Address | **32** | Указывает IP-адрес устройства-отправителя |
| **IP-адрес назначения** | Destination IP Address | **32** | Указывает IP-адрес устройства-получателя |
| **Параметры** | Options | **До 40 байт** | **Необязательный**. Используется для различных параметров, таких как запись маршрута, временные метки и т.д.  Например, опции могут использоваться для указания предпочтительных маршрутов или записи времени прохождения пакета через различные узлы сети. |
| **Заполнитель** | Padding | **До 4 байт** | Добавляется для выравнивания заголовка до 32-битного слова |
| **Данные** | Payload | **До 65535 байт** | Содержит данные, передаваемые вышестоящим уровнем (например, сегмент TCP или датаграмма UDP) |

1. **MAC-адрес. Структура, назначение**

**MAC-адрес**

MAC-адрес (Media Access Control Address) — уникальный физический адрес сетевого устройства, используемый на канальном уровне модели OSI для идентификации устройства в локальной сети.

**Структура MAC-адреса**

|  |  |  |
| --- | --- | --- |
| **Компонент** | **Описание** | **Пример** |
| **OUI**  (Organizationally Unique Identifier) | Первые 24 бита. Назначаются производителю сетевого устройства IEEE. | 00:1A:2B |
| **Уникальный идентификатор устройства** | Последние 24 бита. Присваиваются производителем для уникальной идентификации устройства. | 4C:5D:6E |
| **Итоговый MAC-адрес** | Состоит из OUI и уникального идентификатора. Общая длина — 48 бит. | 00:1A:2B:4C:5D:6E |

**Типы MAC-адресов**

|  |  |  |
| --- | --- | --- |
| **Тип адреса** | **Описание** | **Пример** |
| **Уникальный**  (Unicast) | Указывает на конкретное устройство в сети. Используется для одноадресной передачи данных. | 00:1A:2B:4C:5D:6E |
| **Широковещательный**  (Broadcast) | Отправляет данные всем устройствам в сети. Представляет собой адрес из всех единиц | FF:FF:FF:FF:FF:FF |
| **Групповой**  (Multicast) | Используется для передачи данных группе устройств. | 01:00:5E:00:00:FB |

**MAC-адрес**

**Назначение MAC-адреса**

|  |  |
| --- | --- |
| **Функция** | **Описание** |
| **Идентификация устройства** | Уникально идентифицирует устройство в локальной сети (LAN). |
| **Адресация на канальном уровне** | Используется для передачи данных между устройствами в пределах одной сети. |
| **Маршрутизация кадров** | Определяет источник и получателя данных в Ethernet-кадрах. |
| **Работа протоколов** | Необходим для работы сетевых протоколов, таких как Ethernet, Wi-Fi. |

**Преимущества и недостатки MAC-адресов**

|  |  |
| --- | --- |
| **Преимущества** | **Недостатки** |
| Гарантированная уникальность адреса | Ограниченная длина (48 бит) может привести к повторениям в будущем. |
| Работают на низком уровне модели OSI | MAC-адреса не маршрутизируются за пределами локальной сети. |
| Удобство в локальной адресации | Сложность ручного управления в крупных сетях. |

1. **IPv4 адрес. Структура, назначение**

**IPv4-адрес**

IPv4-адрес — это 32-битный числовой идентификатор устройства в сети, используемый на сетевом уровне модели OSI для взаимодействия между устройствами.

**Назначение IPv4-адреса**

|  |  |
| --- | --- |
| **Функция** | **Описание** |
| **Идентификация устройства** | Уникально определяет устройство в сети (локальной или глобальной). |
| **Маршрутизация пакетов** | Указывает источник и пункт назначения данных в сети. |
| **Обеспечение логической адресации** | Отделяет физическую топологию сети от логической. |
| **Подключение к Интернету** | Является основой для взаимодействия устройств в глобальной сети Интернет. |

**Структура IPv4-адреса**

|  |  |  |
| --- | --- | --- |
| **Компонент** | **Описание** | **Пример** |
| **Сеть**  (Network) | Часть адреса, определяющая принадлежность устройства к конкретной сети. | 192.168.0.0 |
| **Устройство**  (Host) | Часть адреса, уникально идентифицирующая устройство в пределах сети. | .1 (в адресе 192.168.0.1) |
| **Длина** | IPv4-адрес состоит из 32 бит (4 октета по 8 бит). | 11000000.10101000.00000000.00000001 |
| **Пример полного адреса** | IPv4 записывается в виде десятичного представления, разделённого точками. | 192.168.0.1 |

**IPv4-адрес**

**Классы IPv4-адресов**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Класс** | **Диапазон сети** | **Количество сетей** | **Количество хостов в сети** | **Назначение** |
| **A** | 0.0.0.0 – 127.255.255.255 | 128 | ~16 миллионов | Для крупных сетей. |
| **B** | 128.0.0.0 – 191.255.255.255 | 16 384 | ~65 тысяч | Для средних сетей. |
| **C** | 192.0.0.0 – 223.255.255.255 | 2 миллиона | ~254 | Для небольших сетей. |
| **D** | 224.0.0.0 – 239.255.255.255 | - | - | Для мультимастинговых адресов. |
| **E** | 240.0.0.0 – 255.255.255.255 | - | - | Резервные (исследования). |

**Типы IPv4-адресов**

|  |  |  |  |
| --- | --- | --- | --- |
| **Тип адреса** | | **Описание** | **Пример** |
| **Публичный** | Public | Адреса, используемые для взаимодействия устройств в Интернете. | 8.8.8.8 |
| **Частный** | Private | Адреса для локальных сетей, не маршрутизируются в Интернет. | 192.168.0.1 |
| **Автоматический** | APIPA | Назначаются автоматически при отсутствии DHCP-сервера. | 169.254.0.1 |
| **Широковещательный** | Broadcast | Используются для передачи данных всем устройствам в сети. | 192.168.1.255 |
| **Мультимастинг** | Multicast | Применяются для передачи данных группе устройств. | 224.0.0.1 |
| **Резервный** | Loopback | Для тестирования сетевого стека на локальном устройстве. | 127.0.0.1 |

**IPv4-адрес**

**Преимущества и недостатки IPv4**

|  |  |
| --- | --- |
| **Преимущества** | **Недостатки** |
| Простота настройки и поддержки | Ограниченное количество адресов |
| Широкая совместимость | Отсутствие встроенной безопасности |
| Эффективная маршрутизация в малых сетях | Устаревание (переход на IPv6) |

1. **Маска подсети. Структура, назначение**

**Маска подсети**

Маска подсети — это 32-битное число, используемое для разделения IP-адреса на части: сеть и хост.

Она определяет, какая часть IP-адреса относится к сети, а какая — к устройствам в этой сети.

**Назначение маски подсети**

|  |  |
| --- | --- |
| **Функция** | **Описание** |
| **Определение границ сети** | Указывает, какая часть IP-адреса относится к сети, а какая — к хостам. |
| **Маршрутизация пакетов** | Позволяет устройствам и маршрутизаторам правильно передавать пакеты внутри и между сетями. |
| **Оптимизация адресного пространства** | Помогает разделить сеть на более мелкие подсети для рационального использования адресов. |
| **Поддержка безопасности** | Разделяет сеть на сегменты, снижая риск несанкционированного доступа. |

**Структура маски подсети**

|  |  |  |
| --- | --- | --- |
| **Компонент** | **Описание** | **Пример** |
| Часть для сети | Биты, установленные в "1", определяют сеть. | 255.255.255.0 (24 бита для сети) |
| Часть для хостов | Биты, установленные в "0", указывают диапазон возможных адресов хостов. | .0 (8 бит для хостов) |
| Полная длина | Маска состоит из 32 бит, как и IP-адрес. | 11111111.11111111.11111111.00000000 |

1. **Способ задания IP-адреса. DHCP – назначение и принцип работы**

**Способ задания IP-адреса. DHCP**

IP-адрес может быть назначен устройству вручную (статически) или автоматически с помощью протокола DHCP

(Dynamic Host Configuration Protocol).

**Способы задания IP-адреса**

|  |  |  |
| --- | --- | --- |
| **Способ** | **Описание** | **Пример использования** |
| **Статический** | IP-адрес задается вручную администратором. Не меняется без прямого вмешательства. | Важные серверы, сетевые устройства (например, маршрутизаторы). |
| **Динамический** | IP-адрес выделяется автоматически сервером DHCP на ограниченное время (аренда). | Рабочие станции, ноутбуки, смартфоны в локальной сети. |
| **APIPA**  (автоконфигурация) | Устройство назначает себе адрес автоматически из диапазона 169.254.x.x, если DHCP недоступен. | Автоматическая настройка в случае сбоя DHCP. |

**Назначение DHCP**

|  |  |
| --- | --- |
| **Функция DHCP** | **Описание** |
| **Автоматическое распределение IP** | Назначает уникальный IP-адрес каждому устройству в сети. |
| **Снижение ошибок настройки** | Исключает человеческие ошибки при ручной настройке. |
| **Упрощение управления сетью** | Позволяет централизованно управлять параметрами сети, такими как маска подсети, шлюз, DNS. |
| **Временное использование IP-адресов** | Выделяет IP-адреса на ограниченное время, возвращая их в пул после окончания аренды. |

**DHCP**

**Принцип работы DHCP**

|  |  |  |  |
| --- | --- | --- | --- |
| **Этап работы** | | **Описание** | **Результат** |
| **1** | **Обнаружение**  (Discovery) | **Клиент отправляет широковещательный запрос в сеть для поиска DHCP-сервера**  На этом этапе сервер проверяет, в сети ли устройство. Технически этот процесс выглядит как отправка отдельного запроса на универсальный адрес 255.255.255.255. | Сообщение DHCPDISCOVER |
| **2** | **Предложение**  (Offer) | **DHCP-сервер предлагает IP-адрес и параметры конфигурации**  Сервер, работающий по протоколу DHCP, подбирает предложения с возможными подключениями и отправляет их на устройство по его уникальному MAC-адресу. По итогу для подключения выбирается только один вариант (чаще всего именно последний доступный вариант присоединения к сети) | Сообщение DHCPOFFER |
| **3** | **Запрос**  (Request) | **Клиент принимает предложение и запрашивает подтверждение**  Запрос включает в себя MAC-адрес клиента и IP, который отправил сервер на предыдущем этапе. | Сообщение DHCPREQUEST |
| **4** | **Подтверждение**  (Acknowledge) | **Сервер подтверждает запрос, и клиент получает параметры конфигурации**  Сервер отправляет по MAC-адресу клиента сообщения с данными параметров, с помощью которых устройство будет авторизовано в сети. | Сообщение DHCPACK |



1. **Шлюз и маршрут по умолчанию. Назначение, способы задания**

**Шлюз и маршрут по умолчанию**

Шлюз — это устройство (или программное обеспечение), которое служит связующим звеном между двумя сетями, обеспечивая передачу данных между ними. В большинстве случаев шлюз работает на сетевом уровне модели OSI.

|  |  |
| --- | --- |
| **Функция шлюза** | **Описание** |
| **Перенаправление трафика** | Шлюз перенаправляет пакеты данных между сетями, в том числе между локальной сетью и внешними сетями (например, Интернетом) |
| **Сетевой переход** | Работает как точка соединения между сетями с разными адресациями (например, между IPv4 и IPv6). |
| **Маршрутизация** | Определяет на основе маршрутов, какой путь должен пройти пакет, чтобы добраться до назначения. |
| **Обеспечение безопасности** | Может фильтровать трафик и выполнять функции межсетевого экрана (например, проверка пакетов и блокировка нежелательного трафика). |

**Маршрут по умолчанию**

Маршрут по умолчанию — это маршрут, который используется устройством, если для адреса назначения не найден более конкретный маршрут в таблице маршрутизации.

|  |  |
| --- | --- |
| **Функция маршрута по умолчанию** | **Описание** |
| **Указание "последней инстанции"** | Когда не найден подходящий маршрут для пакета, он отправляется по маршруту по умолчанию. |
| **Подключение к внешним сетям** | Обычно маршрутизатор использует маршрут по умолчанию для отправки пакетов в Интернет. |
| **Упрощение настройки сети** | Использование маршрута по умолчанию позволяет упростить конфигурацию, особенно в малых и средних сетях. |

**Шлюз и маршрут по умолчанию**

**Назначение маршрута по умолчанию**

|  |  |
| --- | --- |
| **Назначение** | **Описание** |
| **Интернет-подключение** | Используется для маршрутизации пакетов, которые не принадлежат локальной сети (например, для доступа в Интернет). |
| **Отправка трафика в другие сети** | Указывает путь для пакетов, адреса назначения которых не находятся в текущей сети или подсети. |
| **Оптимизация маршрутизации** | Упрощает таблицы маршрутизации, заменяя множественные записи на одну запись маршрута по умолчанию. |

**Способы задания шлюза и маршрута по умолчанию**

|  |  |  |
| --- | --- | --- |
| **Элемент** | **Описание** | **Пример** |
| **Шлюз по умолчанию**  (default gateway) | Указывается в конфигурации устройства (например, компьютера или маршрутизатора), чтобы направлять трафик в другие сети | На маршрутизаторе:  ip route 0.0.0.0 0.0.0.0 192.168.1.1 |
| **Маршрут по умолчанию** | Добавляется в таблицу маршрутизации и используется, если более конкретный маршрут отсутствует | На сервере:  route add default gw 192.168.0.1 |

1. **Коммутатор. Служебные таблицы и их назначение**

**Коммутатор**

Коммутатор (Switch) — это сетевое устройство, предназначенное для соединения устройств в одной локальной сети (LAN) и передачи данных между ними на канальном уровне модели OSI.

Коммутатор принимает решения о передаче пакетов на основе информации о MAC-адресах, которые он сохраняет в своих служебных таблицах.

**Основные служебные таблицы коммутатора**

|  |  |  |
| --- | --- | --- |
| **Тип таблицы** | **Описание** | **Назначение** |
| **Таблица MAC-адресов** (MAC Table) | Содержит записи о MAC-адресах устройств, подключённых к портам коммутатора. Каждая запись ассоциирует MAC-адрес с конкретным портом устройства. | Используется для определения, на какой порт коммутатора следует отправить кадр на основе его MAC-адреса. |
| **Таблица ARP**  (ARP Table) | Таблица, которая хранит отображение между IP-адресами и MAC-адресами в сети. Хотя коммутатор сам по себе не использует ARP, она может быть полезна для функций с маршрутизацией. | Позволяет устройствам, работающим на сетевом уровне, разрешать IP-адреса в MAC-адреса, что важно для межсетевых коммуникаций. |
| **Таблица VLAN**  (VLAN Table) | Таблица, содержащая информацию о VLAN (виртуальных локальных сетях) и их соответствующих портах. | Используется для разделения трафика между различными VLAN, если на коммутаторе настроена поддержка VLAN. |
| **Таблица маршрутизации** (Routing Table) | Используется в коммутаторах, которые поддерживают маршрутизацию между различными подсетями (Layer 3 switch). | Определяет на основе маршрутов, какой порт должен быть использован для отправки пакетов в другие подсети или сети. |

**Коммутатор. Служебные таблицы**

Таблица MAC-адресов, также известная как таблица адресации или таблица коммутации, является основным элементом, который помогает коммутатору принимать решение о том, на какой порт отправить кадр.

|  |  |  |  |
| --- | --- | --- | --- |
| **Принцип работы таблицы MAC-адресов:**   1. Когда коммутатор получает кадр, он проверяет MAC-адрес назначения в таблице.   2.Если адрес найден, кадр отправляется на соответствующий порт.  Если адрес не найден, кадр отправляется на все порты (широковещательная рассылка), кроме порта, с которого он пришёл.  3. Запись о MAC-адресе добавляется в таблицу, если источник ещё не зарегистрирован |  | **Поле** | **Описание** |
| **MAC-адрес** | Уникальный физический адрес устройства (например, сетевой карты). |
| **Порт** | Номер порта коммутатора, на который подключено устройство с данным MAC-адресом. |
| **Время последнего обновления** | Время, прошедшее с последнего обновления записи о MAC-адресе. |

Коммутаторы поддерживают создание виртуальных локальных сетей (VLAN), что позволяет разделять одну физическую сеть на несколько логических. Каждому VLAN соответствует определённый набор портов.

|  |  |  |  |
| --- | --- | --- | --- |
| **Принцип работы таблицы VLAN:**   1. Каждый порт коммутатора может быть привязан к конкретному VLAN. 2. Когда устройство отправляет кадр, коммутатор проверяет, к какому VLAN он принадлежит, и перенаправляет его только в рамках этого VLAN. |  | **Поле** | **Описание** |
| **VLAN ID** | Уникальный идентификатор VLAN (например, VLAN 10, VLAN 20) |
| **Порты** | Список портов, которые принадлежат конкретному VLAN |
| **Тип VLAN** | Указывает тип VLAN (например, данные или голосовой) |

**Коммутатор. Служебные таблицы**

В современных коммутаторах с поддержкой маршрутизации (Layer 3 switch) может быть также таблица маршрутизации, которая используется для передачи пакетов между различными подсетями.

|  |  |  |  |
| --- | --- | --- | --- |
| **Принцип работы таблицы маршрутизации:**   1. Когда коммутатор получает IP-пакет, он ищет соответствующий маршрут в таблице маршрутизации. 2. Пакет перенаправляется на соответствующий интерфейс в зависимости от маршрута. |  | **Поле** | **Описание** |
| **Сетевой адрес** | Адрес сети назначения, с которой необходимо связаться |
| **Маска подсети** | Маска подсети для указания диапазона адресов в сети |
| **Шлюз** | IP-адрес маршрутизатора, через который нужно направить пакет |
|  |  | **Интерфейс** | Локальный интерфейс коммутатора, через который должен быть направлен пакет |

ARP-таблица (Address Resolution Protocol) — это таблица, которая хранит информацию о соответствии IP-адресов и MAC-адресов в локальной сети. Она необходима для того, чтобы устройство могло определить MAC-адрес, соответствующий известному IP-адресу, прежде чем отправить кадр в сеть.

|  |  |  |  |
| --- | --- | --- | --- |
| **Принцип работы ARP-таблицы:**   1. Когда устройство хочет отправить данные на другое устройство в той же локальной сети, оно сначала проверяет свою ARP-таблицу. Если запись отсутствует, устройство отправляет широковещательный ARP-запрос. 2. Если запись отсутствует, устройство отправляет широковещательный ARP-запрос. Целевое устройство отвечает с своим MAC-адресом, и запросившее устройство добавляет запись в свою ARP-таблицу. 3. Если устройство снова отправляет данные на тот же IP-адрес, оно может использовать существующую запись в ARP-таблице, если она еще не устарела |  | **Поле** | **Описание** |
| **IP-адрес** | IP-адрес устройства, с которым нужно установить соединение |
| **MAC-адрес** | MAC-адрес устройства, соответствующий данному IP-адресу |
| **Тип записи** | Указывает, является ли запись статической (вручную заданной) или динамической (полученной через ARP) |
|  | **Время жизни (TTL)** | Время, в течение которого запись остается актуальной, после чего она удаляется |

**Маршрутизатор. Таблица маршрутизации**

**Маршрутизатор**

Маршрутизатор — это сетевое устройство, которое используется для соединения различных сетей, например, локальной сети с глобальной (Интернетом), и для передачи пакетов данных между ними. Он работает на сетевом уровне модели OSI и использует информацию из таблицы маршрутизации для определения наилучшего пути для каждого пакета.

Таблица маршрутизации — это структура данных, хранящая информацию о путях, которые маршрутизатор использует для доставки пакетов в различные сети.

Она включает записи (маршруты) с адресами назначения, масками подсетей, шлюзами, и интерфейсами маршрутизатора.

**Типы маршрутов в таблице маршрутизации**

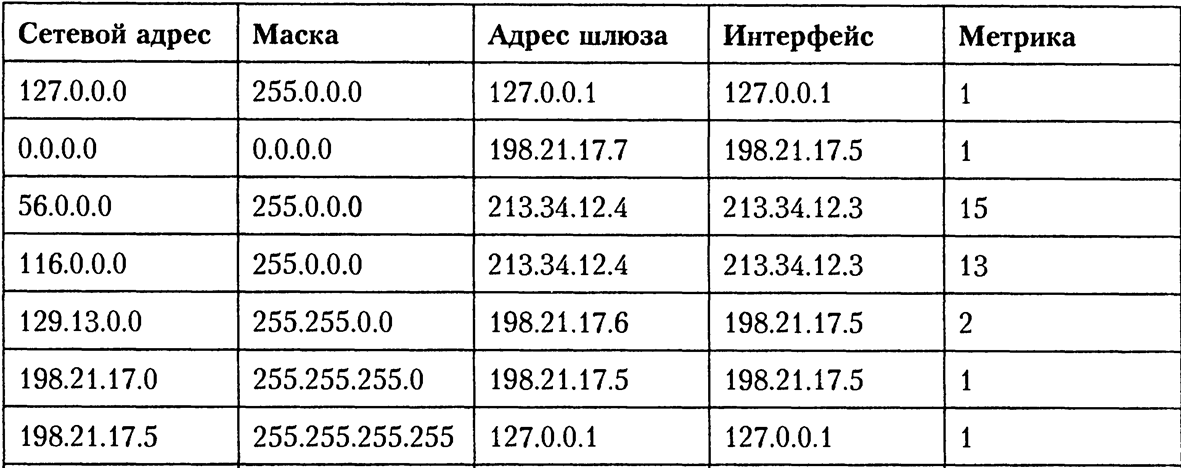
|  |  |
| --- | --- |
| **Тип маршрута** | **Описание** |
| **Статический маршрут**  (Static Route) | Маршрут, добавленный вручную администратором, обычно используется для фиксированных соединений, например, для VPN или маршрута по умолчанию. |
| **Динамический маршрут**  (Dynamic Route) | Маршрут, добавленный автоматически с помощью протоколов динамической маршрутизации (например, OSPF, RIP, BGP). Маршрут может изменяться в зависимости от состояния сети. |
| **Маршрут по умолчанию**  (Default Route) | Маршрут, который используется для передачи пакетов, если нет более конкретного маршрута в таблице. Обычно указывает на шлюз по умолчанию, который направляет трафик во внешние сети, такие как Интернет. |
| **Маршрут внутренней сети**  (Local Route) | Маршрут, который используется для направлений, относящихся непосредственно к самому маршрутизатору, например, для маршрутов, определяющих локальные адреса. |

**Маршрутизатор**

**Основные поля таблицы маршрутизации**

|  |  |
| --- | --- |
| **Поле таблицы** | **Описание** |
| **Сетевой адрес**  (Destination Network) | Адрес назначения, для которого определяется маршрут. Это может быть IP-адрес сети или диапазон. |
| **Маска подсети**  (Subnet Mask) | Маска подсети, которая используется для определения, какие адреса сети принадлежат текущему маршруту. |
| **Шлюз**  (Gateway) | IP-адрес следующего устройства (обычно это маршрутизатор), через которое пакеты должны быть направлены, чтобы попасть в целевую сеть. |
| **Интерфейс**  (Interface) | Локальный интерфейс маршрутизатора, через который пакет будет передан. Это может быть физический интерфейс  (например, Ethernet) или виртуальный (например, VPN). |
| **Метрика**  (Metric) | Числовое значение, которое обозначает «стоимость» маршрута. Чем меньше метрика, тем предпочтительнее маршрут. |
| **Тип маршрута**  (Route Type) | Указывает, как был добавлен маршрут в таблицу: вручную (статический маршрут) или автоматически (динамический маршрут). |

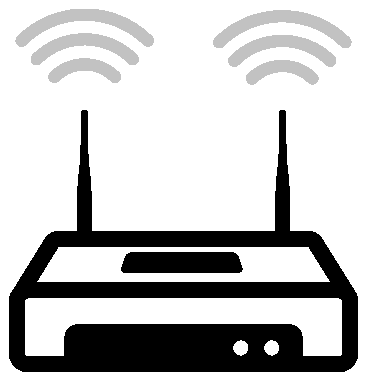
**Пример таблицы маршрутизации**



**Маршрутизатор. Принцип работы**

**Принцип работы маршрутизатора и таблицы маршрутизации**

|  |  |  |
| --- | --- | --- |
| **Этап работы** | | **Описание** |
| **1** | **Получение пакета** | Когда маршрутизатор получает пакет, он сначала проверяет его IP-адрес назначения |
| **2** | **Поиск в таблице маршрутизации** | Маршрутизатор ищет подходящий маршрут в таблице маршрутизации для указанного адреса назначения |
| **3** | **Передача пакета** | Если маршрут найден, пакет передается на соответствующий интерфейс маршрутизатора с указанием шлюза для дальнейшей маршрутизации |
| **4** | **Маршрут по умолчанию** | Если для адреса назначения не найден конкретный маршрут, используется маршрут по умолчанию, если он настроен |



**13. Классическая трехуровневая архитектура корпоративных сетей. Компоненты и назначение**

**Трехуровневая архитектура сетей**

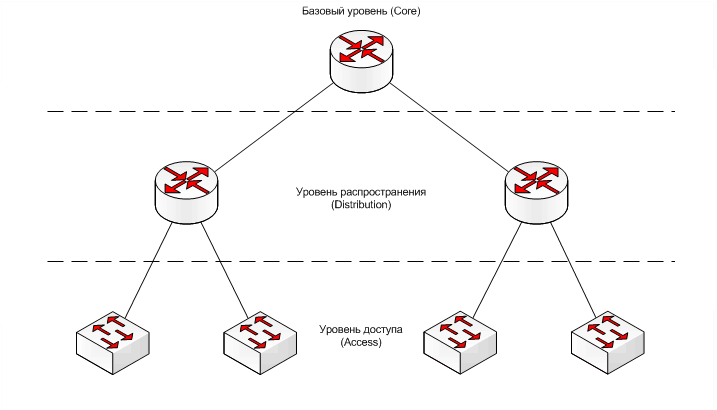
Классическая трехуровневая архитектура корпоративных сетей — это модель построения сети, которая делит её на три уровня: ядро, агрегация/дистрибуция и доступ.

Этот подход упрощает управление сетью, повышает её производительность, надёжность и масштабируемость.

|  |  |  |  |
| --- | --- | --- | --- |
| **Уровень** | **Назначение** | **Характеристики** | **Примеры** |
| **Ядро**  (Core Layer) | **Высокоскоростная передача данных между различными сегментами сети** | Высокая производительность и пропускная способность | * Передача данных между дата-центром и офисами. * Объединение филиалов через магистраль. |
| Центральный магистральный слой, обеспечивающий соединение всех частей сети | Отказоустойчивость за счёт резервирования |
| Минимизация задержек при передаче данных | Минимальная обработка данных  (только пересылка пакетов) |
| **Агрегация/**  **Дистрибуция**  (Distribution Layer) | **Связующее звено между уровнем доступа и ядром** | Поддержка функций маршрутизации и коммутации | * Фильтрация трафика. * Обеспечение подключения VLAN к ядру. * Разграничение зон сети по функциям (например, офисные и серверные) |
| Обеспечение управления трафиком и применение политик безопасности | Применение политик контроля доступа (ACL),  QoS (качество обслуживания) |
| Агрегация данных с уровня доступа | Увеличение надёжности с использованием протоколов отказоустойчивости (например, резервирование шлюзов) |
| **Доступ**  (Access Layer) | **Реализация базовых функций безопасности и управления доступом** | Поддержка VLAN для сегментации сети | * Подключение рабочих станций. * Управление доступом пользователей к сетевым ресурсам. * Организация точек доступа Wi-Fi |
| Подключение конечных устройств (ПК, ноутбуков, принтеров, IP-телефонов и т.д.) к сети | Возможность подключения по проводным (Ethernet) и беспроводным (Wi-Fi) интерфейсам.  Часто включает технологии PoE (Power over Ethernet) для питания устройств |

**Трехуровневая архитектура сетей**

|  |  |
| --- | --- |
| **Преимущество** | **Описание** |
| **Масштабируемость** | Уровень ядра поддерживает высокоскоростное объединение распределенных сетей, что позволяет легко добавлять новые сегменты |
| **Простота управления** | Чёткое разделение уровней делает управление и диагностику более простыми |
| **Гибкость** | Легко реализовать политику безопасности и приоритизацию трафика на уровне распределения |
| **Отказоустойчивость** | Возможность построения резервных маршрутов (например, через протоколы STP или HSRP) |
| **Оптимизация производительности** | Быстрая передача трафика через ядро и оптимальное использование ресурсов |



**14. Двухуровневая архитектура корпоративных сетей. Компоненты и назначение**

**Двухуровневая архитектура сетей**

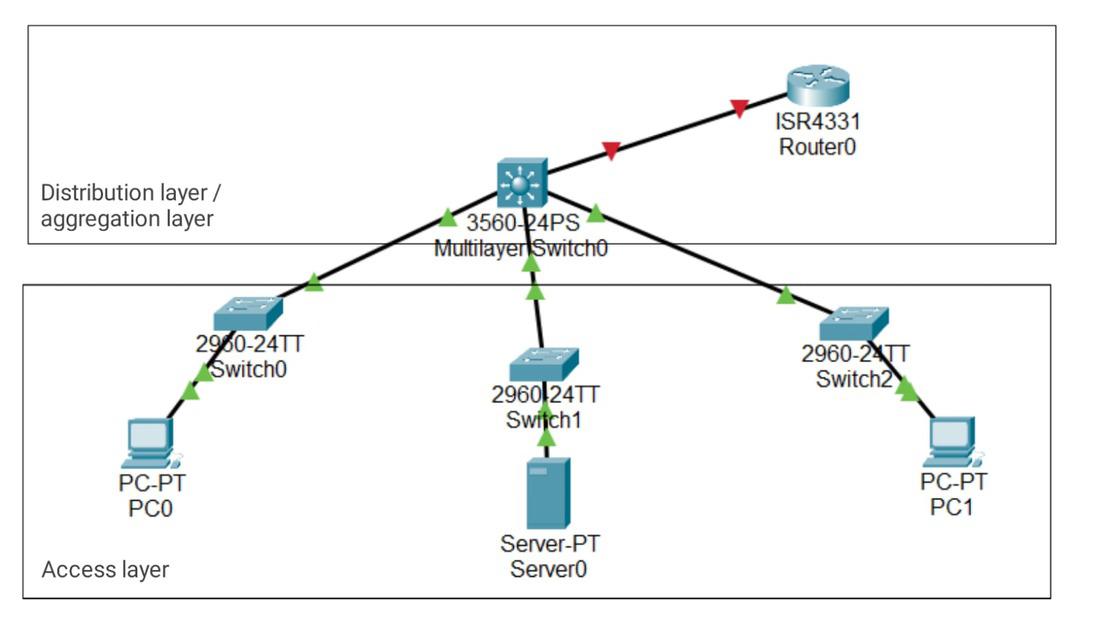
Двухуровневая архитектура корпоративных сетей — это упрощённый подход к построению сетевой инфраструктуры, в котором выделяются только два уровня: агрегация (дистрибуция) и доступ. Она часто применяется в небольших и средних сетях, где нет необходимости в отдельном уровне ядра.

|  |  |  |  |
| --- | --- | --- | --- |
| **Уровень** | **Назначение** | **Характеристики** | **Примеры** |
| **Агрегация/**  **Дистрибуция**  (Distribution Layer) | **Часто объединяет функции уровня ядра в классической архитектуре** | | * Организация межсетевой маршрутизации между VLAN * Балансировка трафика и повышение отказоустойчивости * Применение политик безопасности и фильтрации |
| **Централизованное управление трафиком** | Маршрутизация между сегментами сети (например, VLAN) |
| Выполнение функций маршрутизации и фильтрации | Применение политик контроля доступа (ACL),  QoS (качество обслуживания) |
| Агрегация данных с уровня доступа | Увеличение надёжности с использованием протоколов отказоустойчивости (например, резервирование шлюзов) |
| **Доступ**  (Access Layer) | **Реализация базовых функций безопасности и управления доступом** | Поддержка VLAN для сегментации сети | * Подключение рабочих станций * Управление доступом пользователей к сетевым ресурсам * Организация точек доступа Wi-Fi |
| Подключение конечных устройств (ПК, ноутбуков, принтеров, IP-телефонов и т.д.) к сети | Управление портами для подключения пользователей.  Часто включает технологии PoE (Power over Ethernet) для питания устройств |

**Двухуровневая архитектура сетей**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Основные принципы** | **Описание** | **Преимущества** | **Недостатки** | **Применение** |
| **Объединение функций ядра и агрегации** | Уменьшается количество уровней, что упрощает настройку и администрирование | **Простота** | **Ограничение пропускной способности**  Нет выделенного магистрального уровня | * Небольшие офисы: Один или два коммутатора выполняют функции агрегации и доступа * Отделения компаний: Двухуровневая сеть подключается к магистральной сети организации * Учебные заведения: Простая инфраструктура для обеспечения подключения студентов и преподавателей |
| **Упрощение управления** | Меньшее кол-во устройств и уровней делает сеть проще в обслуживании | **Меньшая отказоустойчивость**  Из-за меньшего количества резервных путей увеличивается риск сбоев |
| **Экономия** | Меньшее кол-во оборудования снижает затраты | **Экономичность** | **Ограниченная масштабируемость**  При увеличении количества устройств или пользователей производительность может снижаться |
| **Масштабируемость** | Подходит для небольших сетей и может быть расширена при росте компании.  Не требуется высокая пропускная способность | **Универсальность** |

**Двухуровневая архитектура сетей**



**15. Инкапсуляция 802.1q. Типы интерфейсов, их назначение**

**802.1q**

802.1Q — это стандарт для инкапсуляции данных в сетях с использованием VLAN.

Он позволяет разделять одну физическую сеть на несколько логически изолированных сетей, обеспечивая передачу трафика различных VLAN через один физический канал. В каждый Ethernet-кадр добавляется тег VLAN, который содержит идентификатор VLAN (VLAN ID).

|  |  |  |
| --- | --- | --- |
| **Тип интерфейса** | **Назначение** | **Характеристики** |
| **Access** | Подключение конечных устройств  (компьютеров, принтеров, IP-телефонов) | * Кадры, передаваемые через Access-интерфейс, не имеют тегов * При получении кадра с тегом интерфейс его отбрасывает |
| Работа только с одной VLAN, без тегов в кадрах |
| **Trunk** | Передача трафика нескольких VLAN между коммутаторами, маршрутизаторами или серверами | * Все кадры передаются с тегами, кроме VLAN по умолчанию (native VLAN) * Поддерживает несколько VLAN |
| Тегирование 802.1Q для идентификации VLAN |
| **Native VLAN** | VLAN по умолчанию для кадров, передаваемых без тегов по Trunk-интерфейсу | * любой трафик, отправленный без тега, будет автоматически ассоциирован с Native VLAN |
| Использование для совместимости с устройствами, которые не поддерживают тегирование |

**16. ARP-шторм в современных сетях. Методы борьбы**

**ARP-шторм**

ARP-шторм — это ситуация, при которой сеть подвергается перегрузке из-за большого количества ARP-запросов. Он может быть вызван неправильной настройкой сетевого оборудования, программными ошибками или злоумышленными действиями (например, атаками).

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Причины** | |  | **Последствия** | |  | **Методы борьбы** | |
| **Замкнутые петли в сети** | При отсутствии защитных механизмов, широковещательные запросы могут бесконечно циркулировать, создавая петли |  | **Перегрузка сети** | Увеличивается объем трафика, связанный с обработкой широковещательных запросов |  | **Протоколы предотвращения петель в сети STP**  **(Spanning Tree Protocol)** | Динамически отключается избыточные пути сохраняя только один активный путь в каждом сегменте |
| **Избыточная генерация ARP-запросов** | Устройства, работающие некорректно, могут генерировать слишком много запросов |  | **Снижение производительности оборудования** | Коммутаторы и маршрутизаторы начинают терять пакеты, что снижает производительность |  | **Storm Control** | Ограничивает уровень широковещательного, многоадресного и одноадресного трафика на порту коммутатора |
| **ARP-атаки** | Злоумышленник может намеренно инициировать массовые ARP-запросы для создания шторма |  | **Остановка сети** | Высокий уровень трафика приводит к блокировке обмена данными |  | **Разделение сети на VLAN** | Сегментация сети на VLAN уменьшает влияние широковещательных запросов, поскольку они остаются внутри соответствующего VLAN |
| **Большие широковещательные домены** | (В больших сетях широкий охват одного широковещательного домена усиливает эффект лавинообразного распространения ARP-запросов |  |  |  |  | **Dynamic ARP Inspection** | DAI проверяет достоверность ARP-пакетов, используя базу данных DHCP Snooping, и отбрасывает недостоверные пакеты |
|  |  |  |  |  |  | **Контроль широковещательного трафика на уровне маршрутизаторов и коммутаторов** | Уменьшение размера широковещательного трафика, Оптимизация ARP-таблиц путём увеличения времени жизни записей, Использование современных протоколов |

**17. Протокол STP. Назначение и принцип работы**

**STP**

STP (Spanning Tree Protocol) — это сетевой протокол канального уровня модели OSI, разработанный для предотвращения возникновения петель в топологии Ethernet. Петли могут приводить к широковещательным штормам, перегрузке сети и некорректной работе устройств.

BPDU (Bridge Protocol Data Unit) — специальные пакеты, используемые STP для обмена информацией между коммутаторами.

STP использует два типа BPDU.

Configuration BPDU - передаёт информацию о состоянии сети и стоимости путей.

Topology Change Notification (TCN) BPDU - сообщает об изменениях в топологии (например, при подключении нового устройства).

|  |  |  |  |
| --- | --- | --- | --- |
| **Основные задачи** | **Проблемы** | **Преимущества STP** | **Недостатки STP** |
| **Предотвращение появления циклов** передачи пакетов в сетях с избыточными связями | **Лавинообразное увеличение трафика**:  Циклы приводят к дублированию широковещательных пакетов, что вызывает перегрузку сети. | Защита от петель, даже в сложных топологиях. | Медленная сходимость в классической версии STP. |
| **Обеспечение доступности** альтернативных путей для повышения отказоустойчивости сети | **Неопределённость MAC-адресов**:  Коммутаторы начинают обновлять свои таблицы MAC-адресов из-за конфликтующих данных. | Повышение отказоустойчивости сети за счёт резервных путей. | Ограниченная масштабируемость в крупных сетях. |
| **Оптимизация трафика** за счёт выбора единственного активного пути между любыми двумя узлами | **Проблемы с доставкой пакетов**:  Пакеты могут зацикливаться, так и не достигнув пункта назначения. | Возможность автоматического восстановления после сбоя. | Возможность ложных срабатываний при некорректной настройке. |

**STP**

**Основные этапы работы**

|  |  |  |
| --- | --- | --- |
| **Этап работы** | | **Описание** |
| **1** | **Выбор корневого коммутатора**  (Root Bridge) | STP начинает с выбора корневого коммутатора.  Корневой коммутатор определяется по Bridge ID, который состоит из приоритета (по умолчанию 32768) и MAC-адреса |
| **2** | **Выбор Root Port**  на всех остальных коммутаторах | Root Port — это порт на коммутаторе, который обеспечивает минимальную стоимость пути до корневого коммутатора.  Стоимость пути определяется в зависимости от скорости интерфейсов  (чем выше скорость, тем ниже стоимость). |
| **3** | **Выбор Designated Port**  для каждого сегмента | Designated Port — это порт, который отвечает за пересылку трафика в сегменте.  Выбирается порт с наименьшей стоимостью пути до корневого коммутатора. |
| **4** | **Блокировка избыточных портов** | Все порты, не являющиеся Root или Designated, переводятся в состояние Blocking.  Это предотвращает прохождение трафика через заблокированные порты, исключая петли. |

**Состояние портов**

|  |  |
| --- | --- |
| **Состояние портов** | **Описание** |
| **Blocking** | Порт не участвует в передаче данных, только получает BPDU (Bridge Protocol Data Units).  Это состояние предотвращает петли. |
| **Listening** | Порт проверяет BPDU и участвует в выборе Root и Designated Ports. |
| **Learning** | Порт начинает изучать MAC-адреса из поступающего трафика, но ещё не передаёт данные. |
| **Forwarding** | Порт передаёт и принимает данные. |
| **Disabled** | Порт отключён вручную или из-за неисправности. |

**18. Статическая маршрутизация. Принцип работы**

**Статическая маршрутизация**

Статическая маршрутизация — это метод управления маршрутизацией данных в сети, при котором маршруты прописываются вручную администратором.

Она предполагает создание фиксированных путей для передачи пакетов от источника к получателю.

Не зависит от протоколов динамической маршрутизации. Требует ручной настройки и контроля.

|  |  |  |
| --- | --- | --- |
| **Преимущества** | **Недостатки** | **Описание** |
| Простота реализации | Трудоёмкость настройки | Легко настроить в малых и статичных сетях.При добавлении или изменении сетей необходимо вручную обновлять маршруты |
| Отсутствие нагрузки на процессор маршрутизатора | Неавтоматизированность | Нет необходимости вычислять маршруты или обмениваться маршрутной информацией.  Маршруты не меняются при сбое соединения. Требуется вмешательство администратора |
| Безопасность | Плохая масштабируемость | Администратор точно контролирует пути передачи данных, минимизируя возможность нежелательных маршрутов.В крупных сетях ручное управление становится неэффективным. |

**Принцип работы статической маршрутизации**

|  |  |  |
| --- | --- | --- |
| **Для каждого маршрута в сети администратор вручную прописывает:**  1. Адрес назначения (Destination Address): куда направляется трафик.  2. Маску подсети (Subnet Mask): для определения сети назначения.  3. Шлюз (Next Hop): IP-адрес или интерфейс, через который следует отправлять данные. |  | **При отправке пакета маршрутизатор:**  1. Сравнивает IP-адрес назначения с таблицей маршрутов.  2. Выбирает маршрут с наилучшим соответствием (по длине префикса или приоритету).  3. Направляет пакет на указанный интерфейс или следующий маршрутизатор. |

**19. Динамическая маршрутизация. Принцип работы на примере OSPF**

**Динамическая маршрутизация**

Динамическая маршрутизация — это метод настройки маршрутизаторов, при котором пути передачи данных (маршруты) определяются автоматически с помощью протоколов маршрутизации. Маршрутизаторы обмениваются информацией о топологии сети, обновляя таблицы маршрутов в режиме реального времени.

|  |  |  |
| --- | --- | --- |
| **Преимущества** | **Недостатки** | **Описание** |
| Масштабируемость | Сложность | Подходит для больших и сложных сетей. Более сложная настройка и управление по сравнению со статической маршрутизацией. |
| Автоматическое управление | Риск сбоев | Упрощает управление сетью и снижает нагрузку на администраторов. Возможность сбоев в работе протоколов маршрутизации, что может привести к потере маршрутов. |
| Производительность | Нагрузка на сеть | Оптимизация маршрутов и балансировка нагрузки. Обмен маршрутной информацией может создавать дополнительную нагрузку на сеть. |
| Отказоустойчивость | Автоматическое обнаружение отказов и поиск альтернативных путей. |

OSPF - это один из наиболее распространённых протоколов динамической маршрутизации, разработанный как стандарт для использования в IP-сетях.

|  |  |
| --- | --- |
| **Характеристика OSPF** | **Описание** |
| **Протокол внутридоменной маршрутизации** | Используется для маршрутизации внутри автономной системы (AS) |
| **Алгоритм SPF (Shortest Path First)** | Основан на алгоритме Дейкстры, который рассчитывает кратчайший путь |
| **Метрическая основа** | OSPF использует стоимость (cost) как основную метрику, основанную на пропускной способности интерфейса (чем выше скорость интерфейса, тем ниже его стоимость) |
| **Поддержка разделения сети на области (areas)** | Позволяет разбить сеть на области для уменьшения нагрузки на маршрутизаторы |

**Основные типы пакетов OSPF**

|  |  |
| --- | --- |
| **Тип пакета** | **Описание** |
| **Hello** | Обнаружение соседей и поддержание связи |
| **Database Description (DBD)** | Обмен информацией о содержимом баз данных |
| **Link State Request (LSR)** | Запрос недостающих данных у соседей |
| **Link State Update (LSU)** | Передача обновлений о состоянии связей |
| **Link State Acknowledgment (LSAck)** | Подтверждение получения обновлений |

**Принцип работы OSPF**

|  |  |  |
| --- | --- | --- |
| **Этап работы** | | **Описание** |
| **1** | **Выбор DR и BDR**  (Designated Router/  Backup Designated Router) | В каждой сети OSPF выбирает — основной маршрутизатор для обмена маршрутной информацией.  Также выбирается резервный маршрутизатор. |
| **2** | **Обмен маршрутной информацией** | После включения маршрутизаторы отправляют Hello-пакеты, чтобы обнаружить соседей.  Формируется список соседей.  После этого начинается обмен базами данных о топологии сети (LSDB — Link State Database) |
| **3** | **Расчёт кратчайших путей** | Используется алгоритм SPF для построения дерева кратчайших путей.  Таблица маршрутов обновляется на основе этого дерева |
| **4** | **Обновление маршрутов** | Если происходит изменение в сети (например, выход интерфейса из строя), маршрутизатор отправляет обновления (LSA — Link State Advertisement  Все маршрутизаторы пересчитывают маршруты |

**20. Протоколы семейства GHRP. Принцип работы на примере VRRP**

**VRRP (GHRP)**

Протоколы семейства GHRP (Gateway Redundancy Protocols) используются для обеспечения отказоустойчивости на уровне шлюзов в локальных сетях. Эти протоколы позволяют организовать резервирование маршрутизаторов или коммутаторов, выступающих в роли шлюза по умолчанию для устройств в сети.

**Основные протоколы семейства GHRP:**

* HSRP (Hot Standby Router Protocol) — проприетарный протокол Cisco.
* VRRP (Virtual Router Redundancy Protocol) — открытый стандарт.
* GLBP (Gateway Load Balancing Protocol) — проприетарный протокол Cisco с балансировкой нагрузки.

**VRRP**

VRRP — это стандартный протокол (описан в RFC 5798), используемый для обеспечения высокой доступности шлюза по умолчанию в сетях IPv(4/6).

|  |  |  |
| --- | --- | --- |
| **Преимущества** | **Недостатки** | **Описание** |
| Высокая отказоустойчивость | Нет балансировки нагрузки | Если основной маршрутизатор выходит из строя, резервный маршрутизатор автоматически принимает роль Master, обеспечивая бесперебойную работу сети.  VRRP не поддерживает распределение нагрузки между маршрутизаторами. Только один маршрутизатор в группе всегда будет являться активным |
| Минимальная задержка при переключении | Благодаря быстрому выбору нового Master маршрутизатора сеть продолжает работать с минимальными задержками. |
| Простота настройки | Ограниченная настройка | VRRP является стандартом, поддерживаемым многими производителями оборудования, и имеет простую конфигурацию.  VRRP предоставляет ограниченные возможности для настройки в сравнении с другими протоколами, такими как HSRP или GLBP |

**VRRP**

|  |  |  |  |
| --- | --- | --- | --- |
| **Этап работы** | | **Описание** | **Результат** |
| **1** | **Создание виртуального маршрутизатора** | Определяется виртуальный IP-адрес (используется как шлюз по умолчанию для клиентов) | Устройства в сети используют виртуальный IP как адрес шлюза |
| Генерируется виртуальный MAC-адрес |
| **2** | **Выбор Master маршрутизатора** | Устройства обмениваются VRRP-пакетами | Назначается основной маршрутизатор (Master) для управления трафиком |
| Выбирается маршрутизатор с наивысшим приоритетом |
| При равенстве приоритетов выбирается с наивысшим IP |
| **3** | **Работа Master маршрутизатора** | Master отправляет VRRP-пакеты по мультикасту 224.0.0.18 для уведомления резервных | Клиенты получают стабильный доступ к сети через Master |
| Обрабатывает весь трафик для виртуального IP-адреса |
| **4** | **Мониторинг состояния Master** | Backup маршрутизаторы слушают VRRP-пакеты | Сеть остается работоспособной даже при сбое Master |
| Если пакеты не приходят в течение времени Dead Interval (по умолчанию 3 сек), Backup переходит в Master |
| **5** | **Переключение при отказе** | Backup маршрутизатор с наивысшим приоритетом занимает роль Master | Автоматическое восстановление работы шлюза без вмешательства администратора |
| Начинает отправлять VRRP-пакеты и обрабатывать трафик |
| **6** | **Возвращение Master**  **(если настроено)** | Если прежний Master восстанавливается, он снова становится Master (если его приоритет выше текущего) | Восстановление изначальной структуры сети |

**21. NAT. Типы адресов. Назначение и принцип работы**

**NAT**

NAT (преобразование сетевых адресов) — это технология, позволяющая изменять IP-адреса в заголовках пакетов при их прохождении через маршрутизатор. Основное назначение NAT — экономия глобальных IPv4-адресов и обеспечение взаимодействия между локальными сетями и Интернетом.

|  |  |  |
| --- | --- | --- |
| **Тип Адреса** | **Описание** | **Пример** |
| **Внутренний**  (Private) | Используется в локальной сети. Не маршрутизируется в Интернете. | 192.168.0.1  10.0.0.1 |
| **Внешний**  (Public) | Адрес, видимый в Интернете. Обычно предоставляется провайдером. | 203.0.113.1 |
| **Локальный внутренний**  (Inside Local) | Адрес устройства в локальной сети до преобразования NAT. | 192.168.0.2 |
| **Глобальный внутренний**  (Inside Global) | Внешний адрес локального устройства после преобразования NAT. | 203.0.113.2 |
| **Локальный внешний**  (Outside Local) | Локальный адрес удалённого устройства, используемый в локальной сети. | 203.0.113.3 |
| **Глобальный внешний**  (Outside Global) | Реальный публичный адрес удалённого устройства. | 198.51.100.1 |

|  |  |
| --- | --- |
| **Преимущества** | **Недостатки** |
| Экономия IPv4-адресов | Усложняет трассировку пакетов (например, для отладки) |
| Повышение безопасности (скрытие внутренней топологии сети) | Проблемы с протоколами, зависящими от IP-адресов (например, IPsec) |
| Упрощение подключения локальных сетей к Интернету через один публичный адрес | Увеличение времени обработки пакетов из-за преобразований |

**NAT**

**Типы NAT**

|  |  |  |
| --- | --- | --- |
| **Тип NAT** | **Описание** | **Пример использования** |
| **Static NAT** | Устанавливает постоянное соответствие между внутренним и внешним IP-адресом. | Доступ к внутреннему серверу (например, веб-серверу) из Интернета. |
| **Dynamic NAT** | Внутренние адреса преобразуются в один из пула внешних адресов. | Временное соединение устройств с Интернетом, если у провайдера ограничен пул IP. |
| **PAT (NAT Overload)** | Использует один внешний IP-адрес для нескольких внутренних устройств. Порт добавляется для идентификации трафика. | Интернет-доступ для всех устройств в локальной сети через один публичный адрес. |

**Принцип работы NAT**

|  |  |  |
| --- | --- | --- |
| **Этап работы** | | **Описание** |
| **1** | **Инициация соединения** | Устройство в локальной сети отправляет пакет на удаленный хост в Интернет. |
| **2** | **Преобразование адреса** | Маршрутизатор заменяет исходный (локальный) IP-адрес на внешний (публичный). |
| **3** | **Создание записи в таблице NAT** | В таблице NAT создается запись для сопоставления локального адреса и порта с публичным адресом и портом |
| **4** | **Отправка пакета** | Преобразованный пакет пересылается на удаленный хост |
| **5** | **Возврат пакета** | Удаленный хост отвечает на внешний IP-адрес маршрутизатора |
| **6** | **Обратное преобразование** | Маршрутизатор заменяет внешний адрес на локальный, используя запись в таблице NAT |

**22. Агрегирование интерфейсов: Принцип работы и пример LACP**

**Агрегирование интерфейсов**

Агрегирование интерфейсов (Link Aggregation) — это технология, объединяющая несколько физических каналов в один логический для повышения пропускной способности и обеспечения отказоустойчивости.

**Основные характеристики агрегации интерфейсов**

|  |  |
| --- | --- |
| **Характеристика** | **Описание** |
| **Повышение пропускной способности** | Объединение нескольких физических каналов в один логический увеличивает общий доступный трафик |
| **Отказоустойчивость** | В случае выхода из строя одного из физических каналов соединение продолжает работать через другие |
| **Балансировка нагрузки** | Трафик распределяется между каналами в зависимости от настроек (MAC-адрес, IP, порт) |
| **Простота управления** | Объединённые каналы управляются как один интерфейс |

**LACP**

LACP (Link Aggregation Control Protocol) — это протокол, определённый в стандарте IEEE 802.3ad, который используется для автоматической конфигурации и управления агрегацией интерфейсов Ethernet. LACP позволяет динамически объединять несколько физических интерфейсов в один логический канал (агрегированный канал), обеспечивая балансировку нагрузки и отказоустойчивость.

|  |  |
| --- | --- |
| **Преимущества** | **Недостатки** |
| Автоматическая настройка и отказоустойчивость | Увеличивает сложность сети |
| Поддержка стандарта IEEE (межвендорная совместимость) | Возможны неравномерные нагрузки |
| Максимально использует доступные ресурсы | Требует дополнительной настройки и оборудования |

**Принцип работы LACP**

|  |  |  |
| --- | --- | --- |
| **Этап работы** | | **Описание** |
| **1** | **Определение физических интерфейсов** | Выбираются физические интерфейсы, которые будут участвовать в объединении |
| **2** | **Обмен LACP-пакетами** | Устройства обмениваются пакетами LACP для согласования настроек (активные и пассивные интерфейсы) |
| **3** | **Формирование агрегата** | Успешно согласованные интерфейсы объединяются в один логический канал |
| **4** | **Балансировка нагрузки** | Трафик распределяется между интерфейсами на основе настроек (например, хэширование по MAC-адресам) |
| **5** | **Возврат пакета** | Если один из каналов выходит из строя, трафик перенаправляется на оставшиеся рабочие интерфейсы |