Министерство образования Республики Беларусь
Учреждение образования
«Белорусский государственный университет
информатики и радиоэлектроники»

Факультет компьютерного проектирования

Кафедра проектирования информационно-компьютерных сетей

СОВРЕМЕННЫЕ СЕТЕВЫЕ ТЕХНОЛОГИИ

Рекомендовано УМО по образованию в области информатики и радиоэлектроники в качестве учебно-методического пособия для специальности 1-40 01 01 «Программное обеспечение информационных технологий»

Минск БГУИР 2020

УДК 004.738(076)
ББК 32.971.35я73
С56

А в т о р ы:

В. А. Леванцевич, К. А. Сурков, Д. А. Сурков, С. А. Медведев

Р е ц е н з е н т ы:

кафедра цифровых систем и технологий государственного учреждения образования «Институт бизнеса Белорусского государственного университета» (протокол №14 от 18.06.2018);

заведующий кафедрой информационных систем и технологий учреждения образования «Белорусский государственный технологический университет» кандидат технических наук, доцент В. В. Смелов

Современные сетевые технологии : учеб.-метод. пособие / С56 В. А. Леванцевич [и др.]. – Минск : БГУИР, 2020. – 120 с. : ил.
ISBN 978-985-543-548-9.

Изложены базовые принципы организации и функционирования компьютерных сетей, а также рассмотрены сетевые технологии, используемые в современных сетях.

УДК 004.738(076)
ББК 32.971.35я73

ISBN 978-985-543-548-9

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Компьютерные сети являются неотъемлемой частью современных информационных технологий. Значительная часть разрабатываемого и уже эксплуатируемого программного обеспечения, в том числе веб-базирующиеся информационные системы, распределенные вычисления и другие перспективные направления, так или иначе связаны с работой в сетях.

Современные сети непрерывно совершенствуются для удовлетворения потребностей пользователей. Изначально сети передачи данных ограничивались символьно-ориентированным обменом информацией между подключенными компьютерными системами. Традиционные телефонные, радио- и телевизионные сети были реализованы отдельно от сетей передачи данных. В прошлом каждый из этих сервисов использовал отдельные сетевые ресурсы с различными каналами связи и различными технологиями для передачи определенного сигнала связи. Каждый сервис имел собственный набор правил и стандартов.

Развитие технологий позволило объединить эти разные типы сетей в единую сетевую платформу. В отличие от выделенных сетей, единая сетевая платформа может передавать голос, потоковое видео, текст и графические изображения между множеством различных типов устройств по одному и тому же каналу связи и структуре сети. Эта платформа предоставляет доступ к широкому диапазону альтернативных и новых способов коммуникации, которые позволяют сотрудникам взаимодействовать друг с другом напрямую практически мгновенно.

Активное развитие «интернета вещей» и цифровизация деятельности человека обусловили необходимость разработки новых сетевых технологий и протоколов для повышения производительности и безопасности сетей.

В учебно-методическом пособии наряду с базовыми принципами организации и функционирования компьютерных сетей рассмотрены сетевые технологии, используемые в современных сетях, а также практические навыки их использования.

Большинство практических примеров выполнено с использованием межсетевой операционной системы Cisco IOS в среде моделирования Cisco Packet Tracer.

ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

1 МОДЕЛЬ ВЗАИМОДЕЙСТВИЯ ОТКРЫТЫХ СИСТЕМ

Вычислительной сетью называют систему обработки данных, состоящую из следующих компонентов:

– оконечных устройств;

– промежуточных сетевых устройств;

– каналов передачи данных;

– программного обеспечения (служб).

К оконечным устройствам можно отнести:

– компьютеры (рабочие станции, ноутбуки, файловые серверы, веб-серверы), сетевые принтеры;

– телефоны VoIP;

– системы дистанционного присутствия TelePresence;

– камеры видеонаблюдения;

– портативные мобильные устройства (смартфоны, планшетные ПК, КПК, беспроводные считыватели кредитных и дебетовых карт и сканеры штрих-кодов и многие другие устройства).

К промежуточным сетевым устройствам относятся:

– устройства сетевого доступа (модемы, концентраторы (HUB), коммутаторы (Switch) и точки беспроводного доступа);

– устройства сетевого взаимодействия (маршрутизаторы);

– устройства системы сетевой безопасности (межсетевые экраны).

В настоящее время используются три вида среды передачи: медный кабель, оптическое волокно, беспроводная сеть.

Общее представление сети предложено на рисунке 1.

Рисунок 1 – Общее представление сети

Для упорядочения работы сетевой инфраструктуры были созданы различные международные, национальные и корпоративные организации по стандартизации. Среди них можно выделить:

– Международную организацию по стандартизации;

– Общество Интернета;

– Институт инженеров по электротехнике и электронике (**IEEE**).

Международная организация по стандартизации (International Organization for Standardization, ISO) разработала модель сетевого взаимодействия открытых систем.

Общество Интернета (Internet Society, ISOC) способствует развитию открытых стандартов и протоколов для технической инфраструктуры Интернета, в том числе осуществляет надзор за Советом по архитектуре Интернета (Internet Architecture Board, IAB). IAB отвечает за общее руководство и разработку интернет-стандартов. IAB обеспечивает надзор за архитектурой протоколов и процедур, используемых Интернетом.

Организация IAB состоит из 13 членов, включая инженерную группу по развитию Интернета (Internet Engineering Task Force, IETF) и исследовательскую группу по развитию интернет-технологий (Internet Research Task Force, IRTF).

IETF разрабатывает, обновляет и поддерживает технологии Интернета и TCP/IP. Она также выпускает документы для разработки новых и обновления существующих протоколов, известные как «рабочие предложения» (Request for Comments, RFC), где приводится описание разработанных протоколов.

IRTF проводит долгосрочные исследования, связанные с сетью Интернет, а также с протоколами, архитектурой, приложениями и технологиями TCP/IP.

Международная некоммерческая ассоциация специалистов в области радиоэлектроники и электротехники (Institute of Electrical and Electronics Engineers, IEEE) создает и поддерживает стандарты в различных отраслях, в том числе в электроэнергетике, здравоохранении, телекоммуникациях и сетевых технологиях. Для сетевых техгологий в рамках этой организации создано семейство стандартов IEEE 802, которое отвечает за канальный и физический уровни различных сетевых технологий.

Корпорация по управлению доменными именами и IP-адресами (Internet Corporation for Assigned Names and Numbers, ICANN) – некоммерческая организация в США, координирующая действия по выделению IP-адресов, управлению доменными именами, используемыми в службах системы доменных имен, а также номерами портов, применяемых протоколами TCP и UDP. ICANN создает правила и несет общую ответственность за выполнение данных задач.

Администрация адресного пространства Интернет (Internet Assigned Numbers Authority, IANA) – отдел ICANN, отвечающий за надзор и управление распределением IP-адресов, доменными именами и идентификаторами протоколов для ICANN.

Структура ICANN представлена на рисунке 2.

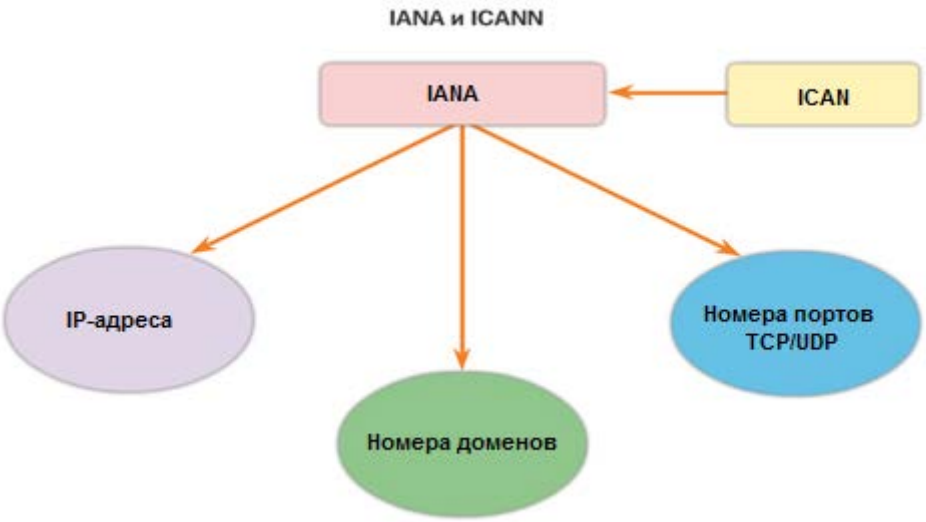


Рисунок 2 – Структура ICANN

С целью создания сетевых стандартов для обеспечения совместимости сетевой инфраструктуры от разных поставщиков в 1983 году ISO была предложена **Модель взаимодействия открытых систем** (Open System Interconnection, OSI).

Модель дает возможность эффективно разбить сложную задачу на части и описать принципы их работы (рисунок 3).

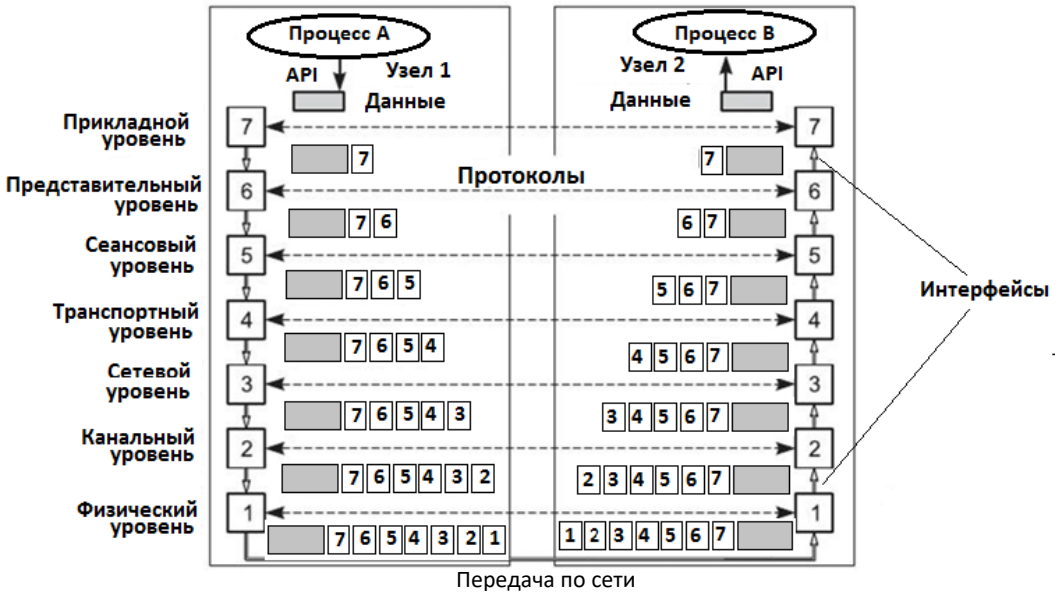


Рисунок 3 – Модель взаимодействия открытых систем

Каждый уровень добавляет к пакету данных свой заголовок, который понятен соответствующему уровню другого узла.

Набор протоколов, необходимый для организации взаимодействия по сети, называется *стеком протоколов.*

Основная идея модели OSI заключалась в том, чтобы этот набор протоколов можно было использовать для разработки международной сети, которая бы не зависела от конкретных запатентованных систем.

Прикладной уровень – набор разнообразных протоколов, с помощью которых приложения получают доступ к сети.

Представительный уровень – представление данных, передаваемых приложением, работающем на одном узле в форме, понятной приложению, работающему на другом узле (узлах).

Основные функции представительного уровня:

– форматирование данных;

– сжатие и распаковка;

– шифрование.

Сеансовый уровень обеспечивает создание сеанса связи (циклов операций, выполняемых без перерыва) между приложениями.

Основные функции сеансового уровня:

– установление и завершение сеанса;

– синхронизация работы сеансовых соединений (позволяют вставлять контрольные точки в длинные передачи, чтобы в случае отказа можно было вернуться назад к последней контрольной точке, вместо того чтобы начинать все сначала);

– извещение приложений процессов об исключительных ситуациях.

Транспортный уровень – доставка данных между конкретными приложениями, функционирующими на разных узлах.

Основные функции транспортного уровня:

– сегментирование (разбиение на сегменты, дейтаграммы) потоков данных, поступающих от приложений на узле отправления, и их повторная компоновка (сборка) в потоки данных приложений на узле назначения. Размер пакетов определяется кадрами канального уровня;

– передача данных с разной степенью надежности между прикладными программами, функционирующими на разных компьютерах.

Сетевой уровень – передача данных между узлами, находящимися в разных сетях (а также и в рамках одной сети), в том числе в сетях с различной сетевой технологией Ethernet, Token Ring, ATM, PPP.

Основные функции сетевого уровня:

– адресация сетей и узлов с помощью логических адресов (IP-адресов);

– упаковка сегментов (дейтаграмм) транспортного уровня в блоки данных сетевого уровня (IP-пакеты) при передаче или распаковка и передача конкретному протоколу транспортного уровня при приеме;

– определение оптимального маршрута и маршрутизация IP-пакетов по разнородной сети.

Канальный уровень – передача данных между узлами одной сети с одинаковой сетевой технологией.

Основные функции канального уровня:

– адресация узлов сети с помощью аппаратных адресов (MAC-адресов);

– упаковка пакета сетевого уровня в блок данных (кадр) канального уровня при передаче или распаковка кадра и передача данных соответствующему протоколу сетевого уровня;

– определение доступности физической среды передачи;

– передача или прием кадра;

– формирование контрольной суммы, коррекция ошибок.

Физический уровень – побитовая передача данных по физической среде передачи.

Физический уровень определяет следующие параметры:

– характеристики физических сред передачи данных (полоса пропускания, помехозащищенность, волновое сопротивление и др.);

– характеристики электрических сигналов (требования к фронтам импульсов, уровням напряжения или тока передаваемого сигнала);

– тип кодирования;

– скорость передачи сигналов;

– типы разъемов и назначение каждого контакта.

Модель OSI представляет расширенный список возможностей и сервисов, которые могут происходить на каждом уровне. Кроме того, она описывает взаимодействие каждого уровня с уровнями, расположенными рядом. Классическая модель OSI послужила основой, на которой были созданы другие модели сетевого взаимодействия.

Протокольная модель сетевого взаимодействия TCP/IP была создана в начале 70-х годов и нередко называется моделью сети Интернет. Такая модель определяет четыре уровня, необходимые для успешного взаимодействия. На рисунке приведено соответствие уровней двух моделей (рисунок 4).

Рисунок 4 – Стек протоколов TCP/IP

Теоретически одно сообщение, например, музыкальное видео или сообщение электронной почты, может быть отправлено по сети от источника к месту назначения как один непрерывный поток битов. Если бы такие сообщения действительно передавались, это означало бы, что другие приложения и устройства в это время не смогли бы отправлять и получать сообщения в той же сети. Большие потоки данных приводили бы к существенным задержкам. Кроме того, если какое-либо из звеньев инфраструктуры сети отказало во время передачи данных, то целое сообщение было бы утрачено и его необходимо было передавать повторно в полном объеме, поэтому передаваемые данные разделяют на более мелкие и управляемые части для передачи по сети. Такое разделение потока данных на более мелкие части называется *сегментацией*.

Сегментация сообщения предоставляет два основных преимущества:

– путем отправки небольших отдельных частей данных от источника к получателю в сети можно поддерживать множество различных чередующихся обменов сообщениями. Такой процесс называется *мультиплексированием*;

– сегментация повышает надежность сетевого взаимодействия.

Отдельные части каждого сообщения необязательно следуют по одному и тому же пути по сети от источника к получателю. Если определенный путь будет переполнен трафиком или сетевое оборудование выйдет из строя, отдельные части сообщения могут быть отправлены к месту назначения по другому пути. Если какую-либо часть сообщения не удается доставить к месту назначения, необходимо будет повторно передать только отсутствующие компоненты.

Недостаток использования сегментации и мультиплексирования для передачи сообщений через сеть – уровень сложности, которая добавляется ко всему процессу передачи. В качестве примера рассмотрим процесс передачи письма из 100 страниц, при этом каждый конверт вмещает только одну страницу. Процесс написания адресов, маркировка, получение и открытие всех 100 конвертов отнимает много времени у отправителя и получателя.

Различные типы устройств в сети участвуют в обеспечении надежной доставки всех частей сообщения в место назначения.

По мере того как данные приложений передаются по стеку протоколов на пути к передаче по сетевой среде, различные протоколы добавляют в них информацию на каждом из уровней. Обычно это называется процессом *инкапсуляции*.

Формы, которые принимают пакеты данных на каждом из уровней, называются протокольными блоками данных (Protocol Data Unit, PDU). В ходе инкапсуляции каждый последующий уровень инкапсулирует PDU, полученный от вышестоящего уровня в соответствии с используемым протоколом. На каждом уровне PDU получает другое название для отражения новых функций. На рисунке 5 представлены названия PDU различных уровней стека протоколов TCP/IP.

Можно выделить следующие PDU:

– *Данные* – общий термин для обозначения PDU прикладного уровня;

– *Сегмент* – PDU транспортного уровня;

– *Пакет* – PDU сетевого уровня;

– *Кадр* – PDU уровня канала данных;

– *Биты* – PDU физического уровня, используемые при физической передаче данных по среде передачи.

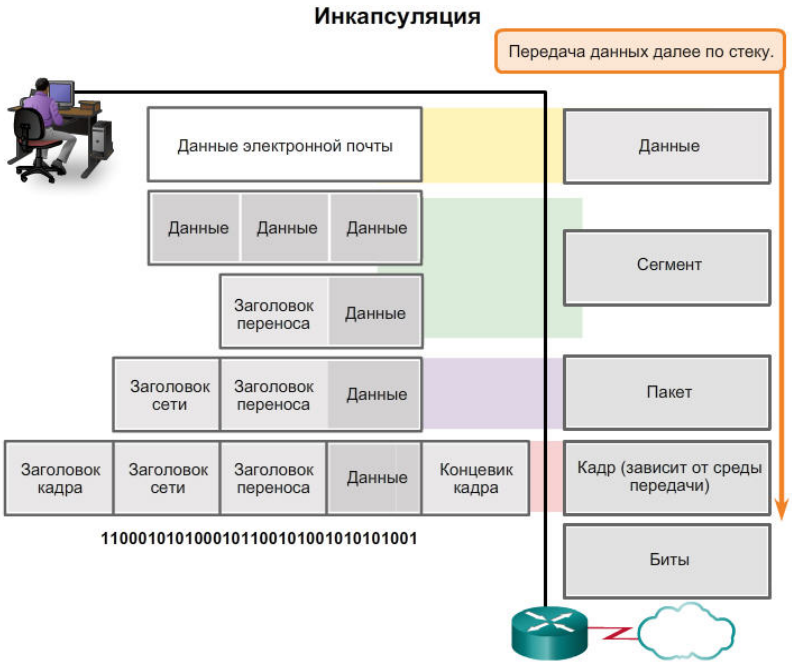


Рисунок 5 – Название блоков данных на различных уровнях

Адреса, используемые в сетевых технологиях:

– *составное символьное имя* – 4-216-filesrv.poit.bsuir.by;

– *цифровое логическое имя* IP – адрес 191.168.33.2;

– *аппаратный адрес сетевого интерфейса* (MAC-адрес) – 0081005e24a8;

– *порт-адрес* (номер), присваиваемый сетевому приложению, работающему на узле (в диапазоне 0–65 535).

2 ПРОТОКОЛ IPV4

Можно выделить следующие основные функции сетевого уровня:

– адресация узлов сетей с помощью логических адресов – IP-адресов;

– упаковка (инкапсуляция) сегментов данных, поступающих с транспортного уровня в IP-пакеты (подсоединение IP-заголовка);

– выбор оптимального маршрута продвижения IP-пакетов и направление пакетов по этому маршруту (маршрутизация пакетов);

– фрагментация пакетов в зависимости от используемой технологии канального уровня;

– распаковка (декапсуляция) пакетов.

Типичные протоколы сетевого уровня:

– IP-протокол версии 4 (IPv4);

– IP-протокол версии 6 (IPv6).

Протокол IPv4 был разработан как протокол с низкой нагрузкой. Его можно охарактеризовать как протокол без установления соединения (отсутствует предварительное согласование соединения), с негарантированной доставкой (отсутствие подтверждения о принятии пакета) и независимостью от среды передачи канального и физического уровней.

Он обеспечивает минимальные функции, которые необходимы для доставки пакета от узла источника к узлу назначения по взаимосвязанной системе сетей. Этот протокол не предназначен для мониторинга и управления потоком пакетов. При необходимости эти функции выполняют другие протоколы на других уровнях.

Канальный уровень OSI должен принять IP-пакет и подготовить его для передачи в коммуникационной среде. Пересылка пакетов IP не ограничивается какой-либо конкретной средой передачи данных.

Существует одна важная характеристика канального уровня, которая учитывается на сетевом уровне, – максимальный размер передаваемого блока данных **(**Maximum Transmission Unit, MTU) канального уровня.

Канальный уровень передает значение MTU на сетевой уровень. Затем сетевой уровень определяет размер IP-пакетов.

Промежуточное устройство (*как правило, это маршрутизатор*) должно разделить пакет при его пересылке из одной среды передачи данных в среду с меньшим максимальным размером передаваемого блока данных (MTU). Этот процесс называется *фрагментацией*.

Каждый IP-пакет снабжается заголовком, формат которого приведен на рисунке 6.

Рисунок 6 – Формат заголовка Ipv4-пакета

Назначение полей заголовка:

– **Версия** указывает версию протокола IP (версия IPv4-0100 или IPv6-0110);

– **Длина заголовка IP**-пакета указывает значение длины заголовка, измеренное в 32-битовых словах (обычно пять слов);

– **Дифференцированные сервисы** задают приоритетность пакета и вид критерия выбора маршрута;

– **Общая длина** указывает общую длину пакета с учетом заголовка и поля данных и составляет 65 535 байтов. При передаче по сетям различного типа длина пакета выбирается с учетом максимальной длины пакета протокола канального уровня, несущего IP-пакеты;

– **Идентификация, Флаг, Смещение** используются при фрагментации пакетов;

– **Срок жизни** задается источником передачи пакета и является счетчиком количества маршрутизаторов, через которые прошел пакет. По истечении времени жизни пакет аннулируется. Позволяет удалить зацикленные пакеты в случае неправильной настройки сети;

– **Протокол** указывает, какому протоколу верхнего (транспортного) уровня надо передать данные пакета. Обычно используются значения ICMP (1), TCP (6) и UDP (17);

– **Контрольная сумма** рассчитывается по всему заголовку;

– **Адрес источника** и **Адрес назначения** имеют одинаковые длину (32 бита) и структуру;

– **Параметры** являются необязательным полем и используются только при отладке сети. Это поле состоит из нескольких подполей. В этих подполях можно указывать точный маршрут прохождения маршрутизаторов, маршрутизаторы, помещать данные системы безопасности, а также временные отметки;

– В **Заполнение** (**Резерв**) может быть добавлено несколько байт для выравнивания заголовка пакета по 32-битной границе.

Каждое устройство в сети должно быть уникально представлено с помощью адреса. В IPv4-сетях этот адрес представлен в виде 32-битного двоичного числа. Эти адреса входят в состав заголовка IP-пакета.

IP-адрес состоит из двух логических частей:

– номера подсети (ID подсети) – сетевая часть;

– номера узла (ID хоста) в этой подсети – узловая часть.

Чтобы записать номер подсети, в поле номера узла в IP-адресе ставят нули. Чтобы записать номер узла, в поле номера подсети ставят нули.

Пример – **192.168.10.0** – номер сети; **0.0.0.10** – номер узла.

Для определения сетевой и узловой частей в IP-адресе используют отдельный 32-битный шаблон – **маску подсети** (рисунок 7).

Большинству людей сложно понять и запомнить строку из 32 бит, поэтому вместо двоичной системы для представления IPv4-адресов используется десятичный формат с разделительными точками. При этом каждый байт (октет) имеет значения в виде десятичного числа от 0 до 255.

Рисунок 7 – Структура IPv4-адреса

В маске подсети биты, определяющие номер сети, установлены в единицы (1), а биты, определяющие номер хоста, – в нули (0).

Адрес сети получается путем поразрядного логического умножения разрядов IP-адреса и маски (рисунок 8).

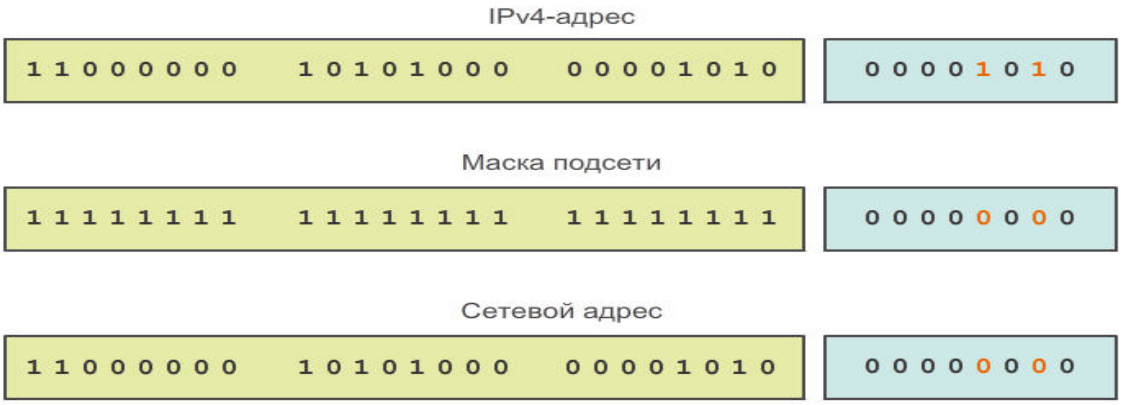


Рисунок 8 – Побитовая операция И

Длина префикса – это еще один способ представления маски подсети. Длина префикса означает количество бит, установленных на единицу (1) в маске подсети. Она обозначается наклонной чертой вправо (/), после которой идет набор единиц. Например, если маска подсети 255.255.255.0, то в двоичной версии маски подсети количество непрерывно следующих единиц справа налево равно 24, поэтому длина префикса составляет 24 бита или /24. Для нашего примера эта запись имеет вид 192.168.10.0/24. Префикс и маска подсети – это разные способы представления сетевой части адреса.

В IPv4-сети узлы могут обмениваться данными одним из следующих трех способов:

1 *Одноадресная передача* – процедура отправки пакета с одного узла на отдельный узел.

2 *Многоадресная передача* (*групповая*) – процедура отправки пакета с одного узла на группу выбранных узлов (могут находиться в различных сетях).

Узлы с индивидуальным адресом могут подписаться на групповую рассылку. Многоадресная передача сокращает трафик, позволяя узлу отправлять один пакет выбранной группе узлов, которые являются частью подписной группы мультивещания. Чтобы достичь множества целевых узлов с помощью одноадресной связи, узел-источник должен отправлять отдельный пакет на каждый адрес. В случае с многоадресной рассылкой узел-источник может отправлять один пакет, который достигает нескольких тысяч узлов назначения. Многоадресная передача включает в себя: широковещательную передачу видео и аудио, обмен данными протоколов маршрутизации, распространение программного обеспечения, удаленные игры и т. д.

З *Широковещательная передача.* Выделяют ограниченную и направленную (прямую) широковещательную передачи.

В ограниченной широковещательной передаче (limited broadcast) все разряды IP-адреса назначения равны единице – 255.255.255.255. Пакет отправляется всем узлам сети, в которой находится источник пакета. Ограниченная широковещательная передача ограничивается зоной действия данной, конкретной сети. Маршрутизаторы не пропускают пакеты с широковещательными адресами.

При направленной широковещательной передаче все единицы присутствуют только в узловой части. Она направляется всем узлам сети назначения. Направленный широковещательный адрес в сеть назначения 172.16.4.0 с маской 255.255.255.0 имеет вид 172.16.4.255.

В диапазоне адресов каждой сети IPv4 существуют три типа адресов:

– сетевой адрес;

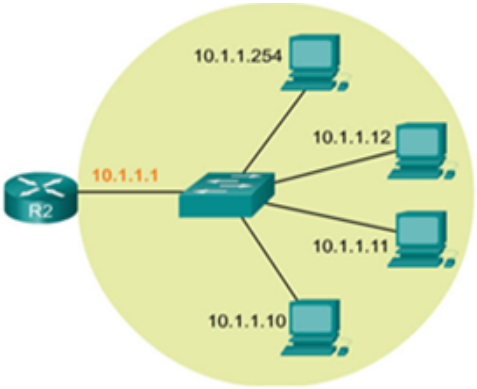
– индивидуальный адрес;

– широковещательный адрес.

По числу разрядов, отводимых для узловой части, можно определить общее количество узлов по правилу: если количество бит, отведенное под номер узла, равно N, то общее количество узлов равно

$$2^N - 2.$$

Два адреса узла вычитаются потому, что адреса со всеми разрядами, равными нулям или единицам, являются особыми (отводятся для обозначения адреса сети и широковещательного адреса). Как видно на рисунке 9, сетевой адрес равен 10.1.1.0/24, широковещательный адрес – 10.1.1.255/24 и диапазон индивидуальных адресов составляет от 10.1.1.1/24 до 10.1.1.254/24. На примере адрес 10.1.1.1 назначен интерфейсу маршрутизатора.



Сеть – 10.1.1.0; маска – 255.255.255.0;
сетевой адрес – 10.1.1.0;
широковещательный адрес – 10.1.1.255;
адрес первого узла – 10.1.1.1;
адрес последнего узла – 10.1.1.254.

Рисунок 9 – Типы адресов сети

Хотя большая часть узловых IPv4-адресов являются публичными, т. е. предназначенными для использования в сетях, доступных через Интернет, существуют блоки адресов, которые используются в сетях, требующих ограниченного доступа в Интернет. Эти адреса называются *частными адресами*.

Блоки частных адресов включают в себя адреса:

– 10.0.0.0–10.255.255.255 (10.0.0.0/8);

– 172.16.0.0–172.31.255.255 (172.16.0.0/12);

– 192.168.0.0–192.168.255.255 (192.168.0.0/16).

Частные адреса определены в документе RFC 1918 и используются в технологии сетевой трансляции адресов (Network Address Translation, NAT). Узлы, которые не требуют доступа в сеть Интернет, могут использовать частные адреса. Однако в рамках частной сети узлы по-прежнему должны иметь индивидуальные IP-адреса.

Узлы в различных сетях могут использовать одни и те же частные адреса. Пакеты, использующие эти адреса в качестве источника или назначения, не должны появляться в публичном интернет-доступе. Маршрутизатор или устройство межсетевого экрана, находящиеся по периметру этих частных сетей, должны блокировать или преобразовывать эти адреса.

В документе RFC 6598 IANA администрация адресного пространства Интернет зарезервировала другую группу адресов, которая называется *общим адресным пространством*. Так же как и в пространстве частных адресов RFC 1918, адреса общего адресного пространства не доступны глобально. Эти адреса предназначены только для использования в сетях операторов связи. Блок общих адресов – 100.64.0.0/10.

Публичные адреса. Подавляющее большинство адресов в диапазоне узлов одноадресной IPv4-рассылки являются публичными адресами. Эти адреса предназначены для использования в узлах с открытым доступом из Интернета. В диапазоне этих блоков IPv4-адресов также существуют адреса, предназначенные для особых целей. Некоторые адреса невозможно назначить узлам. Например, как было указано выше, в каждой сети *первый и последний*

адреса не могут быть назначены узлам – это сетевой и широковещательный адреса соответственно.

Логический интерфейс loopback. Loopback – особый адрес, который используют узлы, чтобы направлять трафик самим себе. Адрес обратной связи позволяет создавать ускоренный метод взаимодействия для приложений и сервисов TCP/IP, которые работают на одном и том же устройстве. С использованием loopback-адреса вместо назначенного IPv4-адреса узла два сервиса на одном узле могут обойти нижние уровни стека протоколов TCP/IP. Для проверки настройки TCP/IP на локальном узле можно послать эхо-запрос на loopback-адрес.

Хотя чаще используется только адрес 127.0.0.1, резервируются адреса с 127.0.0.0 до 127.255.255.255. Любой адрес из этого блока даст обратную связь с локальным узлом. Ни один адрес из этого блока не должен появляться в какой-либо сети.

Локальные адреса каналов. В качестве локальных адресов канала используются IPv4-адреса в блоке адресов от 169.254.0.0 до 169.254.255.255 (169.254.0.0 /16). Они используются в небольшой сети клиентом DCHP (входит в состав ОС) для самостоятельной конфигурации адресов в случае, если ни один DHCP-сервер не доступен. Коммуникация с помощью локальных IPv4-адресов подходит только для обмена данными с другими устройствами, находящимися в одной сети (канале).

Локальные адреса не могут использоваться за пределами локальной сети. Однако многие приложения типа клиент – сервер и одноранговые приложения будут работать надлежащим образом с локальными IPv4-адресами в рамках одной подсети.

Адреса TEST-NET. Блок адресов от 192.0.2.0 до 192.0.2.255 (192.0.2.0/24) зарезервирован для учебных целей. Эти адреса часто используются в сочетании с такими доменными именами, как example.com или example.net в серии документов, имеющих статус стандартов (RFC), в документации поставщиков и протоколов. Адреса из этого блока не должны появляться в сети Интернет.

Экспериментальные адреса. Адреса в блоке от 240.0.0.0 до 255.255.255.254 зарезервированы для использования в будущем. В настоящее время эти адреса могут использоваться только в исследовательских или экспериментальных целях, но не могут использоваться в IPv4-сети.

Как показано на рисунке 10, изначально существовало пять классов IP-адресов. При этом для каждого класса была определена фиксированная маска.

Блок адресов класса A разработан для поддержки очень крупных сетей, содержащих более чем 16 млн адресов узлов. Для обозначения сетевого адреса IPv4-адреса класса A использовали фиксированный префикс /8 с первым октетом. Остальные три октета использовались для адресов узлов.

Адресное пространство класса B разработано для поддержки потребностей небольших и крупных сетей, содержащих приблизительно

65 000 узлов. IP-адрес класса B использовал два старших октета для обозначения сетевого адреса.

Адресное пространство класса C было доступно чаще всех остальных классов адресов. Это адресное пространство предназначено для предоставления адресов небольшим сетям с максимальным количеством узлов не более 254.

Класс	Первые биты	Наименьший номер сети	Наибольший номер сети	Количество сетей	Максимальное число узлов в сети
A	0	1.0.0.0	127.0.0.0	128	$2^{24} - 2 = 16777214$
B	10	128.0.0.0	191.255.0.0	16384	$2^{16} - 2 = 65534$
C	110	192.0.0.0	223.255.255.0	2097152	$2^{8} - 2 = 254$
D	1110	224.0.0.0	239.255.255.255	Групповой адрес	
E	11110	240.0.0.0	247.255.255.255	Зарезервирован	

Рисунок 10 – Классы адресов

Классовое распределение адресного пространства часто приводило к потере множества адресов, что отрицательным образом сказалось на количестве доступных IPv4-адресов. Например, компании, в сети которой находится 260 узлов, необходимы адреса класса B с 65 534 адресами, при этом 65 284 адреса остаются неиспользуемыми. В настоящее время классовые адреса используются внутри частных сетей.

Бесклассовые адреса. В 1993 году организация IETF (Инженерная группа по развитию Интернета) для оптимизации выделения Ipv4-адресов создала новый стандарт, который позволил операторам связи вместо адресов класса A, B или C с помощью введенной метрики – маски подсети – назначать адреса в любых битовых границах адреса. Этот стандарт получил официальное название – бесклассовая междоменная маршрутизация (Classless Inter Domain Routing, CIDR).

Как показано на рисунке 11, администрация адресного пространства сети Интернет IANA регулирует назначение IPv4- и IPv6-адресов через своих региональных интернет-регистраторов (RIR):

– AfriNIC (Африканский сетевой информационный центр) – Африканский регион;

– APNIC (Азиатско-Тихоокеанский сетевой информационный центр) – Азиатско-Тихоокеанский регион;

– ARIN (Американский реестр интернет-адресов) – Североамериканский регион;

– LACNIC (Латиноамериканский и Карибский сетевой информационный центр) – Латинская Америка и некоторые острова Карибского моря;

– RIPE NCC (Координационный центр европейской континентальной сети) – Европа, Ближний Восток и Азия.

Рисунок 11 – Региональные интернет-регистраторы

В свою очередь региональные интернет-регистраторы отвечают за выделение IP-адресов локальным интернет-регистраторам (LIR) или интернет-провайдерам (ISP). Большинство компаний или организаций получают блоки IPv4-адресов от интернет-провайдеров.

Недостатки протокола IPv4:

– нехватка IP-адресов. IPv4 может предложить лишь 4,3 млрд уникальных публичных IP-адресов;

– NAT, CIDR и VLSM были разработаны в качестве обходных путей и помогли продлить жизнь IPv4;

– отсутствие сквозных соединений. Преобразование сетевых адресов (NAT) представляет проблему при использовании технологий, для которых необходимы сквозные соединения программами. NAT увеличивает нагрузку на шлюзы и замедляет процесс передачи пакетов;

– расширение таблицы интернет-маршрутизации. Дробление адресного пространства на небольшие блоки (для экономии адресов) ведет к росту количества сетей и росту таблиц маршрутизации, что является дополнительной нагрузкой на маршрутизаторы.

3 ПРОТОКОЛ IPV6

В начале 90-х годов специалисты инженерной группы по развитию сети Интернет (IETF) подняли вопрос о недостатках протокола IPv4 и начали поиски альтернативных решений. Результатом поисков стала разработка протокола IP версии 6 (IPv6). IPv6 помогает преодолеть ограничения протокола IPv4 и значительно расширяет доступные возможности протокола IPv4.

К улучшениям, которые предлагает протокол IPv6, относятся следующие:

1 *Расширенное адресное пространство*. В отличие от протокола IPv4, использующего 32 бита, IPv6-адреса используют 128-битную иерархическую адресацию, адресное пространство протокола IP версии 6 поддерживает 340 282 366 920 938 463 463 374 607 431 768 211 456 или 340 ундециллионов адресов, что примерно равно количеству песчинок на Земле.

2 *Улучшенная обработка пакетов*. Структура заголовка IPv6 была упрощена благодаря уменьшению количества полей. Это повышает обработку пакетов промежуточными маршрутизаторами, а также предоставляет поддержку расширений и дополнительных параметров, обеспечивая повышенную масштабируемость и долговечность.

3 *Отсутствие необходимости в использовании NAT*. Благодаря большому количеству общедоступных IPv6-адресов трансляция сетевых адресов (NAT) не требуется. Клиентские узлы, от самых крупных предприятий до жилых домов, могут получить общедоступный сетевой IPv6-адрес. Это позволяет устранить некоторые проблемы, связанные с преобразованием сетевых адресов, которые возникают при работе приложений, требующих наличия сквозного подключения.

4 *Интегрированная безопасность*. Протокол IPv6 изначально обладает средствами для аутентификации и обеспечения конфиденциальности. При использовании протокола IPv4 для этого требовалось реализовать дополнительные функции.

Одним из основных конструктивных улучшений протокола IPv6 по сравнению с IPv4 является упрощенный заголовок IPv6.

Заголовок IPv4 состоит из 20 октетов (до 60 байт, если используется поле **Параметры**) и 12 основных полей заголовка, не учитывая поля **Параметры** и **Заполнитель**.

Заголовок IPv6 состоит из 40 октетов (главным образом из-за длины адресов IPv6 источника и назначения) и 8 полей заголовков (3 основных поля заголовков IPv4 и 5 дополнительных полей).

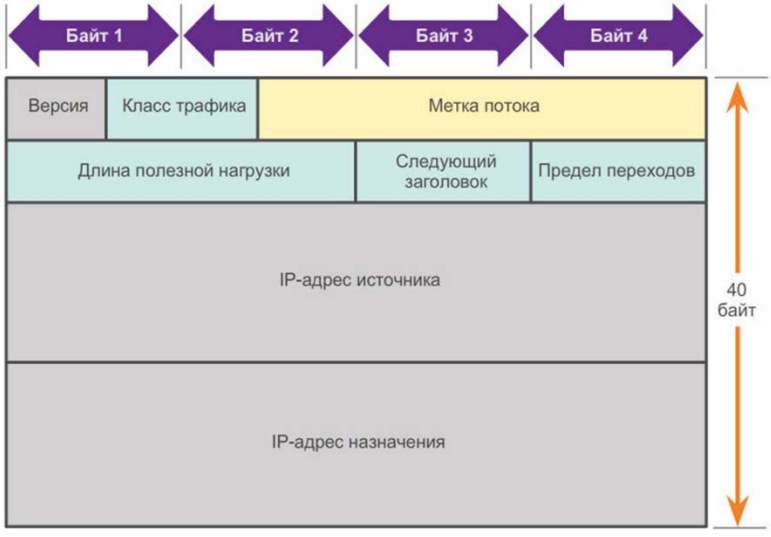


Рисунок 12 – Заголовок IPv6-пакета

В заголовке пакета IPv6 используются следующие поля:

1 Поля **Версия**, **Класс трафика**, **Длина полезной нагрузки**, **Предел перехода**, **Адрес источника**, **Адрес назначения** по своему функциональному назначению аналогичны соответствующим полям заголовка пакета IPv4.

2 **Метка потока** присваивается пакетам узлом-отправителем путем генерации псевдослучайного 20-битного числа. Позволяет значительно упростить процедуру маршрутизации однородного потока пакетов. При получении первого пакета с меткой потока маршрутизатор запоминает результаты обработки заголовков пакета (основного и дополнительных) в локальном кэше. Последующие пакеты с той же комбинацией **Адреса источника** и **Метки потока** обрабатываются с учетом информации кэша без детального анализа всех полей заголовка.

3 **Следующий заголовок** – 8-битное поле, соответствующее полю **Протокол** в заголовке IPv4. Оно указывает тип полезной нагрузки данных, которые переносит пакет, что позволяет сетевому уровню пересылать данные на соответствующий протокол более высокого уровня. Это поле также используется в тех случаях, когда в пакет IPv6 добавляются дополнительные заголовки расширений, приведенные на рисунке 13.

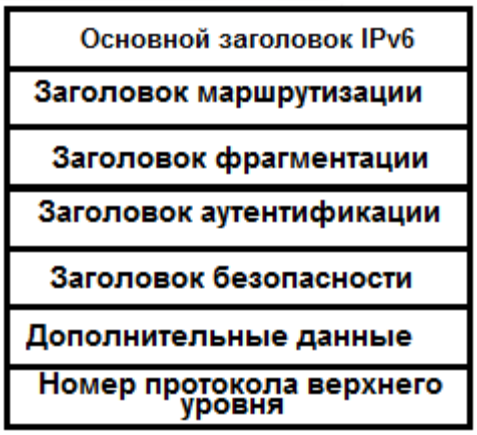


Рисунок 13 – Дополнительные заголовки

Длина IPv6-адресов составляет 128 бит, записанных в виде строки шестнадцатеричных значений. Каждые четыре бита представлены одной шестнадцатеричной цифрой, причем общее количество шестнадцатеричных значений равно 32. Четыре шестнадцатеричных значения формируют хекстет. Хекстеты отделяются друг от друга двоеточием. IPv6-адреса не чувствительны к регистру, их можно записывать как строчными, так и прописными буквами.

Для упрощения записи длинных IPv6-адресов существует два правила:

– пропуск всех ведущих нулей (0) в каждом хекстете;

– двойное двоеточие (::) может заменить любую непрерывную последовательность нулевых хекстетов. Двойное двоеточие (::) может использоваться в адресе только один раз. Пример применения правил приведен на рисунке 14.

Предпочтительно	FE80:0000:0000:0000:0123:4567:89AB:CDEF
Без ведущих нулей	FE80: 0: 0: 0: 123:4567:89AB:CDEF
Сжатый	FE80::123:4567:89AB:CDEF

Рисунок 14 – Форматы записи IPv6-адреса

Существуют три типа IPv6-адресов:

– *индивидуальный* (*unicast*) служит для IPv6-адресации интерфейса на устройстве;

– *групповой* (*multicast*) используется для отправки IPv6-пакетов по нескольким адресам назначения. В отличие от протокола IPv4 IPv6 не использует адрес широковещательной рассылки;

– *произвольный* (*anicast*) – любой индивидуальный IPv6-адрес, который может быть назначен нескольким устройствам. Пакет, отправляемый на адрес произвольной рассылки, направляется к ближайшему устройству с этим адресом.

Так как протокол IPv6 не использует маски, то для обозначения сетевой части адреса используется длина префикса.

Диапазон длины префикса может составлять от 0 до 128. Традиционная длина IPv6-префикса для локальных и других типов сетей – /64. Это означает, что длина префикса, или сетевая часть адреса, составляет 64 бита, а оставшиеся 64 бита остаются для идентификатора интерфейса (узловой части) адреса.

На рисунке 15 показаны шесть типов индивидуальных IPv6-адресов.

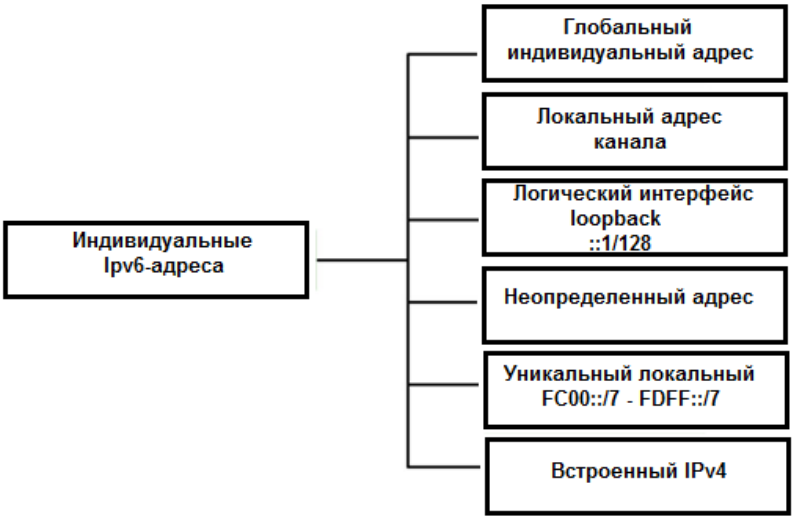


Рисунок 15 – Индивидуальные Ipv6-адреса

Глобальный индивидуальный адрес аналогичен публичному IPv4-адресу. Является уникальным по всему миру. Это маршрутизируемый адрес в Интернете, выделяется IANA и может назначаться статически и динамически: **2001:0DB8:0000:1111:0000:0000:0000:0200/64.**

Глобальный индивидуальный адрес состоит из трех частей: префикс глобальной маршрутизации, равный 48 бит; идентификатор подсети, равный 16 бит; идентификатор интерфейса, равный 64 бита.

На рисунке 16 изображен формат префикса глобальной маршрутизации – это сетевая часть адреса, назначаемая интернет-провайдером организации или клиенту, если у них есть необходимость создания подсетей. Если подсети не создаются, то может выделяться сетевой адрес с префиксом 64 бита. Адресов столько, что каждому жителю планеты может быть назначен глобальный префикс.

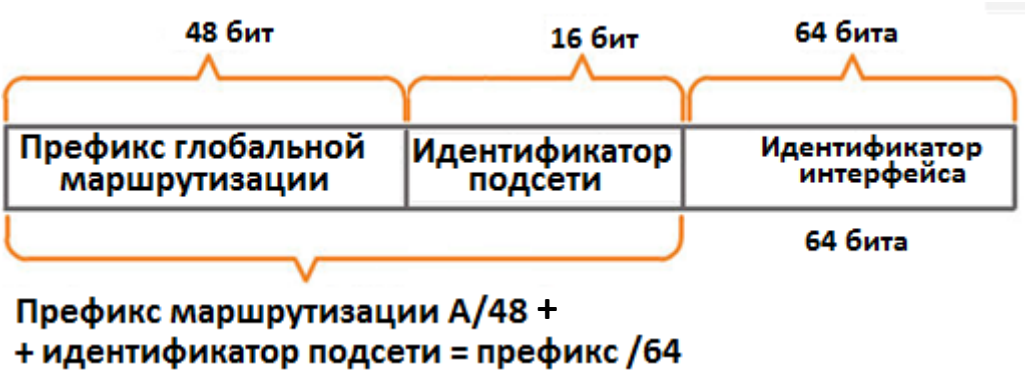


Рисунок 16 – Префикс глобальной маршрутизации

На рисунке 17 приведены отдельные поля глобального индивидуального адреса, которые закреплены за соответствующими организациями.

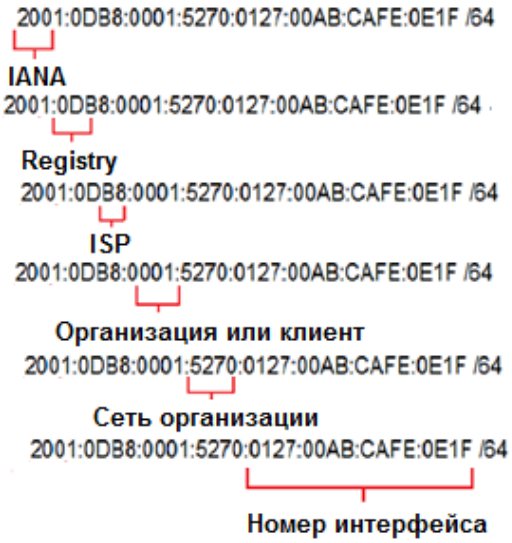


Рисунок 17 – Структура IPv6-адреса

Локальные адреса канала (*локальный канальный адрес*) используются для обмена данными с другими устройствами в пределах одной подсети. Первый хекстет локального канального адреса Ipv6 занимает 10 бит и имеет вид FE80::/10. Аналогичен локальному адресу канала Ipv4 (169.254.0.0–169.254.255.255). Ограничен одной подсетью и уникален в рамках одной подсети. Маршрутизаторы не смогут пересылать пакеты, имея локальный адрес канала источника или назначения. Автоматически назначается активному сетевому интерфейсу операционной системой узла и может использоваться для пересылки между узлами. Локальный адрес канала, назначенный маршрутизатору-шлюзу подсети, может быть использован узлами в качестве адреса шлюза по умолчанию.

Логический интерфейс loopback. Loopback-адрес используется узлом для отправки пакета самому себе и не может быть назначен физическому интерфейсу. Как и на loopback-адрес IPv4, для проверки настроек TCP/IP на локальном узле можно послать эхо-запрос на loopback-адрес IPv6. Loopback-адрес IPv6 состоит из нулей, за исключением последнего бита, который выглядит как ::1/128 или просто ::1 в сжатом формате.

Неопределенный адрес состоит из нулей и в сжатом формате представлен как ::/128 или просто :: . Он не может быть назначен интерфейсу и используется только в качестве адреса источника, когда устройству еще не назначен постоянный IPv6-адрес.

Уникальные локальные IPv6-адреса имеют некоторые общие особенности с частными адресами для IPv4. Первый хекстет адреса имеет значение от FC00::/7 до FDFF::/7. Уникальные локальные адреса используются для локальной адресации в пределах узла или между ограниченным количеством узлов. Эти адреса не маршрутизируются глобально.

Встроенный IPv4 адрес – специальные адреса, которые необходимы для перехода с протокола IPv4 на IPv6.

Групповые IPv6-адреса имеют префикс FFXX::/8. Групповые адреса могут быть только адресами назначения, а не адресами источника.

Существуют два типа групповых IPv6-адресов:

– назначенный групповой адрес;

– групповой адрес запрошенного узла.

Назначенные групповые адреса зарезервированы для заданных групп устройств. Назначенный групповой адрес – это один адрес, используемый для осуществления связи с группой устройств.

Существуют две распространенные группы назначенных групповых IPv6-адресов:

– *группа мультивещания для всех узлов* **FF02::1**. Это группа мультивещания, к которой подключены все устройства под управлением протокола IPv6. Пакет, отправленный этой группе, получается и обрабатывается всеми IPv6-интерфейсами в канале или сети. Эта группа адресов работает так же, как широковещательный адрес в протоколе IPv4;

– *группа мультивещания для всех маршрутизаторов* **FF02::2**. Это группа мультивещания, к которой подключены все IPv6-маршрутизаторы. Маршрутизатор становится частью этой группы, когда переходит под управление протоколом IPv6 (в Cisco IOS с помощью команды глобальной конфигурации ipv6 unicast-routing). Пакет, отправленный этой группе, получается и обрабатывается всеми IPv6-маршрутизаторами в канале или сети.

В отличие от назначаемой многоадресной рассылки, которая направляется всем узлам сети, групповые адреса запрашиваемого узла передаются не всем узлам, а отдельной группе узлов (принимают пакет не все).

Групповой адрес запрашиваемого узла состоит из двух частей:

– *групповой префикс* FF02:0:0:0:0:1:FF00::/104: – первые 104 бита группового адреса запрашиваемого узла;

– *младшие 24 бита узловой части индивидуального адреса* – эти биты копируются из крайних правых 24 бит глобального индивидуального адреса или локального адреса канала устройства, как показано на рисунке 18.

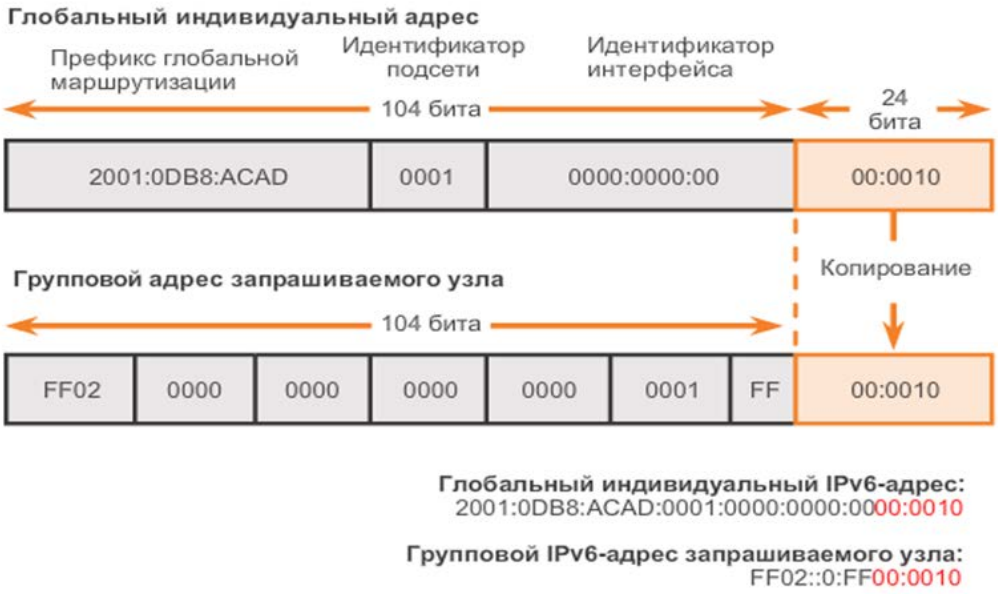


Рисунок 18 – Запрашиваемый групповой адрес

Групповые адреса используются в протоколе поиска соседей (Neighbor Discovery Protocol, NDP). Этот протокол является расширением протокола ICMPV6 и используется в работе протоколов автоматического назначения Ipv6-адресов, а также для нахождения MAC-адреса узла по его Ipv6-адресу (аналог протокола ARP в IPv4) и определения конфликта адресов.

Точно неизвестно, когда будет осуществлен переход на протокол IPv6: в ближайшем будущем протоколы IPv4 и IPv6 будут существовать совместно. Полный переход может занять многие годы. Специалисты IETF создали различные протоколы и инструменты, которые позволяют сетевым администраторам постепенно переводить свои сети на протокол IPv6.

Методы перехода можно разделить на три категории:

1 **Двойной стек.** Как показано на рисунке 19, двойной стек позволяет протоколам IPv4 и IPv6 сосуществовать в одной сети. Устройства с двойным стеком одновременно работают с протокольными стеками IPv4 и IPv6.

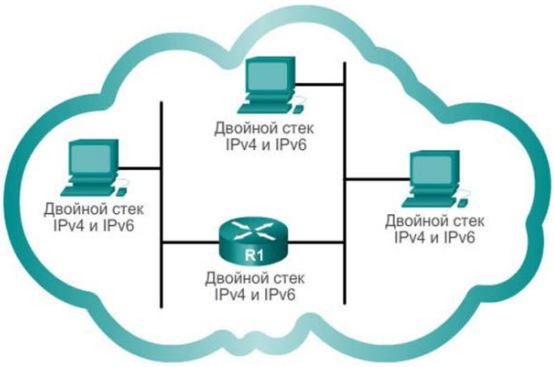


Рисунок 19 – Двойной стек протоколов

2 **Туннелирование**. Как показано на рисунке 20, туннелирование – это способ транспортировки IPv6-пакетов через IPv4-сеть. IPv6-пакет инкапсулируется внутри IPv4-пакета, как и другие типы данных.

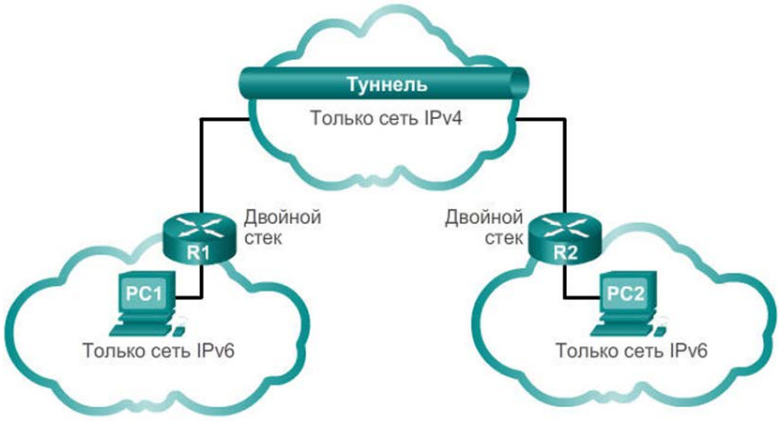


Рисунок 20 – Туннель для IPv6

3 **Преобразование**. Как показано на рисунке 21, преобразование сетевых адресов 64 (NAT64) позволяет устройствам под управлением IPv6 обмениваться данными с устройствами под управлением IPv4 с помощью метода преобразования, похожего на метод преобразования из NAT для IPv4. IPv6-пакет преобразовывается в пакет IPv4-пакет, и наоборот.

Рисунок 21 – NAT 64

4 ДИНАМИЧЕСКОЕ НАЗНАЧЕНИЕ IP-АДРЕСОВ

Способы назначения Ipv4- и IPv6-адресов во многом схожи, но у них есть определенные отличия.

IP-адреса назначаются вручную (статически) или автоматически с помощью протокола DHCPv4 или DHCPv6. Статическое назначение удобно для небольших сетей с постоянным количеством узлов. Для больших сетей используется автоматическое распределение адресов. Сервер назначает узлу следующие основные параметры:

– IP-адрес;

– маска подсети (IPv4) или длина префикса (IPv6);

– адрес шлюза по умолчанию;

– адрес DNS-сервера;

– время аренды.

DHCPv4 использует три метода присвоения адреса:

1 **Распределение вручную** – администратор вручную присваивает MAC-адресу клиента предварительно выделенный IPv4-адрес, который с помощью протокола DHCPv4 назначается устройству.

2 **Фиксированное распределение** – DHCPv4 автоматически присваивает устройству постоянный статический IPv4-адрес, выбирая его из пула доступных адресов. Аренда отсутствует.

3 **Динамическое распределение** – DHCPv4 динамически выдает в аренду IPv4-адрес из пула адресов на ограниченный период времени по выбору DHCP сервера или до тех пор, пока клиенту нужен адрес. Это наиболее распространенный метод. Срок аренды обычно составляет от 1–24 ч до недели или более. По истечении срока аренды клиент должен запросить другой адрес, хотя в большинстве случаев клиенту повторно назначается тот же адрес. Благодаря этому механизму «переехавшие» или отключившиеся клиенты не занимают адреса, в которых они больше не нуждаются. По истечении срока аренды сервер DHCP возвращает адрес в пул, из которого адрес может быть повторно получен при необходимости.

DHCPv4 работает по модели клиент – сервер. Сообщения DHCPv4 инкапсулируются в пакеты транспортного протокола UDP: номер порта клиента – 68, номер порта сервера – 67. Последовательность работы протокола DHCP приведена на рисунке 22.

Рисунок 22 – Работа протокола DHCP

При первоначальной аренде адреса начинается четырехэтапный процесс получения адреса в аренду. Клиент начинает процесс с сообщения DHCPDISCOVER со своего MAC-адреса с целью обнаружения доступных DHCPv4-серверов. Поскольку клиент не может знать, к какой подсети он относится, сообщение DHCPDISCOVER представляет собой широковещательную рассылку сетевого уровня (IPv4-адрес назначения 255.255.255.255. адреса источника неопределенный IPv4-адрес 0.0.0.0.) и канального уровня (MAC-адреса назначения FFFFFFFFFFFF, MAC-адресом источника является MAC-адрес узла, отправившего сообщение DHCPDISCOVER).

Сообщение DHCPDISCOVER находит в сети DHCPv4-серверы. Когда сервер DHCPv4 получает сообщение DHCPDISCOVER, он резервирует доступные IPv4-адреса для выдачи в аренду клиенту. Сервер также создает запись ARP, состоящую из MAC-адреса запрашивающего клиента и выданного клиенту IPv4-адреса. DHCPv4-сервер посылает сообщение привязки DHCPOFFER запрашивающему клиенту. Адресом источника одноадресной рассылки сообщения DHCPOFFER является MAC-адрес сервера, адресом назначения – MAC-адрес клиента.

Клиент, получив от сервера сообщение DHCPOFFER, отправляет в ответ сообщение DHCPREQUEST. Это сообщение используется как для первоначальной аренды адреса, так и для ее продления. Когда сообщение используется при первоначальной аренде, DHCPREQUEST служит уведомлением о принятии предложенных сервером параметров и косвенным отклонением для всех других серверов, которые также могли предоставить клиенту свои параметры.

В корпоративных сетях часто используется несколько DHCPv4-серверов. Сообщение DHCPREQUEST отправляется в форме широковещательной рассылки с целью информирования данного DHCPv4-сервера и других DHCPv4-серверов о том, что предложение было принято.

При получении сообщения DHCPREQUEST сервер проверяет, не используется ли выдаваемый в аренду IP-адрес с помощью отправки эхо-запроса по протоколу ICMP на этот адрес. После этого сервер создает новую запись ARP для клиентской аренды и отвечает сообщением одноадресной рассылки DHCPACK. Сообщение DHCPACK является копией сообщения DHCPOFFER, за исключением изменения в поле типа сообщения. При получении сообщения DHCPACK клиент загружает информацию о конфигурации и выполняет ARP-проверку присвоенного адреса. Если ARP-ответа нет, значит, IPv4-адрес доступен, и клиент начинает использовать его в качестве собственного адреса.

Когда аренда заканчивается, клиент посылает сообщение DHCPREQUEST непосредственно DHCPv4-серверу, который первоначально предложил IPv4-адрес. Если сообщение DHCPACK не получено за определенный период времени, клиент отправляет другое сообщение DHCPREQUEST широковещательной рассылкой, чтобы другой DHCPv4-сервер мог продлить срок аренды.

При получении сообщения DHCPREQUEST сервер подтверждает информацию об аренде ответным сообщением DHCPACK.

Как и в случае с IPv4-адресами, глобальные индивидуальные IPv6-адреса можно настроить вручную или динамически.

При этом существует три способа, автоматического назначения Ipv6-адресов:

– автоматическая настройка адреса без отслеживания состояния (SLAAC);

– протокол динамической конфигурации сетевого узла DHCPv6 (с отслеживанием состояния);

– комбинированный: SLAAC и DHCPv6 вместе (называется DHCPv6 без отслеживания состояния).

Автоматическая настройка адреса без отслеживания состояния (Stateless Address Autoconfiguration, SLAAC) – это способ получения устройством глобального IPv6-адреса одноадресной рассылки без использования DHCPv6-сервера. Этот способ называется «без отслеживания состояния» потому, что с настроенного на роутере сервера SLAAC клиенту пересылаются только префикс сети (номер сети), длина префикса и адрес шлюза по умолчанию, а узловая часть Ipv6-адреса назначается узлом самостоятельно. Таким образом, полный Ipv6-адрес не сохраняется на SLAAC-сервере. SLAAC не пересылает адрес DNS-сервера.

Как показано на рисунке 23, в основе работы SLAAC лежит протокол поиска соседа NDP, являющийся расширением протокола ICMPv6. SLAAC использует ICMPv6-сообщения **RS** (Router Solicitation) «Запрос к маршрутизатору» (отправляются на групповой адрес **FF02::2**), которое содержит запрос на получение IPv6-адреса, и сообщение **RA** (Router Advertisement) «Ответ/объявление маршрутизатора» (отправляется на групповой адрес **FF02::1**).

Сообщение RA содержит параметры настройки интерфейса: префикс сети, длину префикса и Ipv6-адрес шлюза и др.

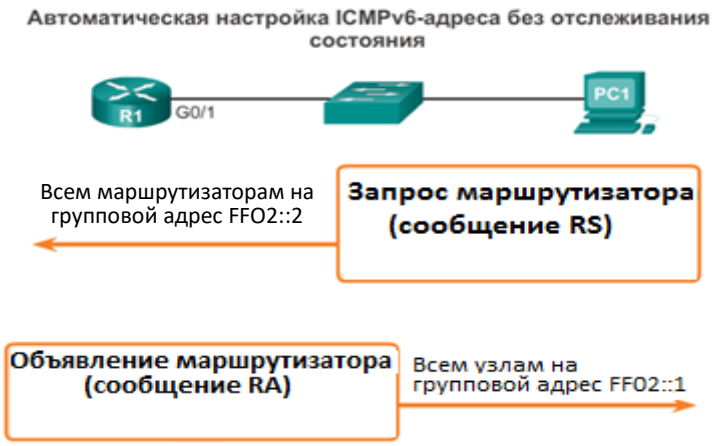


Рисунок 23 – Работа протокола SLAAC

Следует отметить, что сообщения RA с параметрами настройки адреса оправляются каждые 200 с. Если узел хочет получить параметры настройки адреса раньше, то он посылает сообщение RS.

При использовании SLAAC узловая часть формируется самим узлом двумя способами:

– с помощью расширенного уникального идентификатора EUI-64 (Extended Unique Identifier), используя свой 48-битный MAC-адрес;

– с помощью 64-битного случайного числа, сгенерированного операционной системой узла (более безопасный метод).

Как показано на рисунке 24, механизм EUI-64 использует 48-битный MAC-адрес Ethernet и выполняет вставку 16 бит в средней части 46-битного MAC-адреса с целью создания 64-битного идентификатора интерфейса.

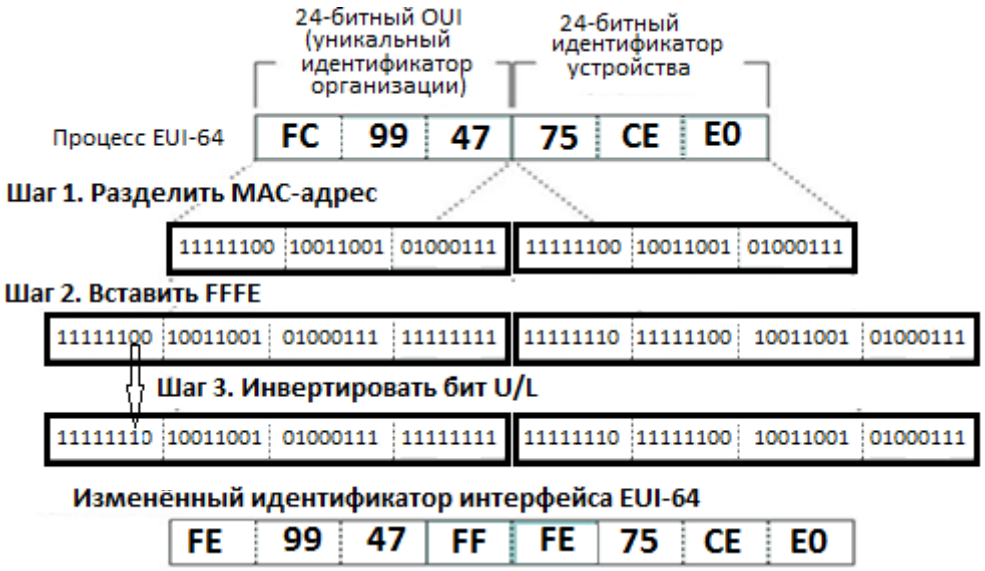


Рисунок 24 – Расширенный уникальный идентификатор

ICMPv6-сообщения RA содержат два флага, которые задают узлу один из трех вариантов получения Ipv6-адреса: SLAAC, DHCPv6 и SLAAC+DHCPv6; однако операционная система узла может игнорировать сообщение RA и использовать только DHCPv6-сервер. Состояние флагов сообщения RA задается специальными командами на маршрутизаторе.

При задании режима только DHCPv6, как показано на рисунке 25, узел в ответ на сообщение RS, получает RA-сообщение и начинает обращаться к DHCPv6-серверу для получения параметров настройки интерфейса: Ipv6-адрес, длина префикса, адрес шлюза и адрес DNS-сервера.

Протокол DHCPv6 использует в качестве транспорта протокол UDP и порты: 546 – сервер, 547 – клиент. Клиент передает сообщение DHCPv6 SOLICIT на зарезервированный IPv6-адрес многоадресной рассылки локального канала FF02::2.

Один или несколько серверов DHCPv6 отвечают клиенту сообщением ADVERTISE. Клиент отвечает серверу DHCPv6 одним из двух сообщений: REQUEST, если это режим SLAAC+DHCPv6 (запрос только адреса DNS-сервера), или INFORMATION-REQUEST, если это режим DHCPv6 (запрос всех параметров). Сервер отправляет клиенту DHCPv6 сообщение REPLY, содержащее запрашиваемую в сообщении REQUEST или INFORMATION-REQUEST информацию.

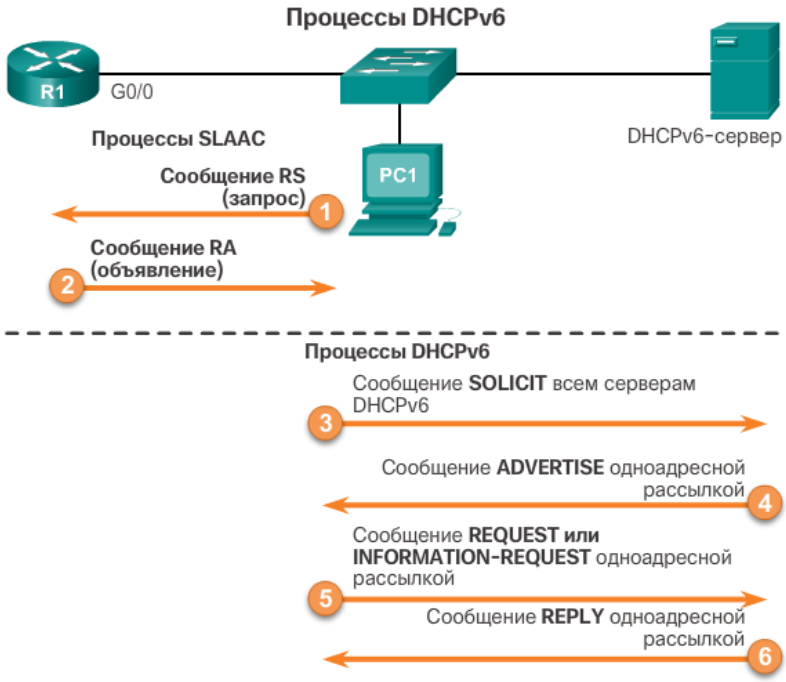


Рисунок 25 – Схема работы протокола DHCPV6

В режиме SLAAC+DHCPv6 узел получает основные параметры (префикс, длину префикса) с сервера SLAAC, формирует узловую часть самостоятельно, а для получения адреса DNS-сервера делает запрос на сервер DCPPv6 (рисунок 26).

Рисунок 26 – Схема работы протоколов SLAAC и DHCPv6

Так как работа протокола DHCP основана на широковещательных рассылках, то зона действия DHCP-сервера ограничивается одной сетью, так как маршрутизаторы не пропускают широковещательные пакеты. Для того чтобы DHCP-сервер в одной сети мог раздавать адреса в другой сети, находящейся за роутером, на роутере необходимо настроить ретрансляцию DHCP (рисунок 27).

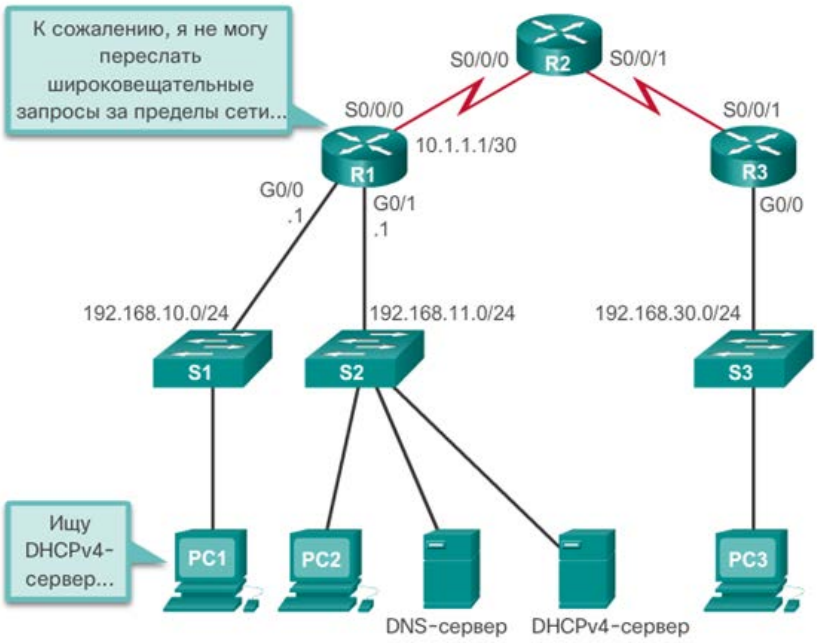


Рисунок 27 – Ретрансляция DHCP

Так на рисунке 27 узел PC1 сети 192.168.10.0/24 сможет получить адрес с DHCP-сервера сети 192.168.11.0/24 в том случае, если на R1 будет настроена ретрасляция широковещательных DHCP-запросов. В Cisco IOS это можно сделать следующими командами:

```
R1(config) # interface g0/0
R1(config) # ip helper-address 192.168.10.1/24
```

5 МАРШРУТИЗАЦИЯ ПАКЕТОВ

Для передачи информации межу сетями используются специальные устройства, которые называются маршрутизаторами. Основные функции маршрутизаторов:

– связывание сетей (в том числе с различной технологией канального уровня);

– определение оптимального маршрута для передачи пакетов;

– пересылка пакетов к пункту назначения;

– фрагментация пакетов.

Кроме основных функций, маршрутизатор может выполнять дополнительные функции, например, функции DHCP-сервера, осуществлять фильтрацию пакетов исходя из настроенных списков доступа и т. д.

Маршрутизатор представляет собой специализированный компьютер с процессором и памятью. Типы памяти маршрутизатора приведены на рисунке 28.

При включении питания операционная система маршрутизатора загружается из флеш-памяти в ОЗУ, а текущие настройки сохраняются в NVRAM. Сетевым интерфейсам маршрутизатора присваивается IP-адрес и маска подсети (префикс и длина префикса для IPV6).

Память	Энергозависимая/ энергонезависимая	Хранилища
ОЗУ	Энергозависимая	• Текущая версия IOS • Файл текущей конфигурации • Таблица маршрутизации и таблица ARP • Буфер пакетов
ПЗУ	Энергонезависимая	• Указания по начальной загрузке • Базовое программное обеспечение для диагностики • Версия IOS с ограниченными возможностями
Энергонезависимое ОЗУ (NVRAM)	Энергонезависимая	• Файл загрузочной конфигурации
Флеш-память	Энергонезависимая	• IOS • Прочие системные файлы

Рисунок 28 – Память маршрутизатора

Маршрутизатор выполняет три основных шага:

– деинкапсуляцию пакета третьго уровня путем удаления заголовка и концевика кадра канального уровня;

– поиск оптимального пути в таблице маршрутизации в соответствии с IP-адресом места назначения;

– если маршрутизатор находит путь до места назначения, он инкапсулирует пакет третьего уровня в новый кадр канального уровня и пересылает кадр из выходного интерфейса.

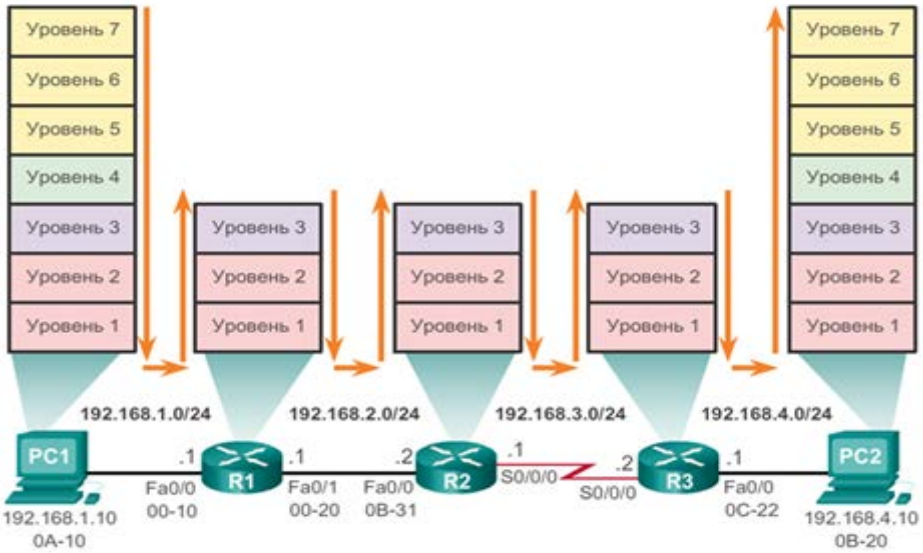


Рисунок 29 – Процесс пересылки пакетов

Маршрутизаторы оборудованы несколькими интерфейсами, каждый из которых предназначен для отдельной IP-сети. Маршрутизатор отвечает за выбор маршрута между сетями на основании **данных таблицы маршрутизации**.

Таблица маршрутизации содержит информацию о следующих типах путей:

– *маршрутах к сетям с прямым подключением* (непосредственно подключенным к интерфейсам маршрутизатора). Если IP-адрес назначения пакета принадлежит узлу в сети с прямым подключением, подключенной к одному из интерфейсов маршрутизатора, то этот пакет пересылается напрямую узлу назначения. Это означает, что IP-адрес назначения пакета – это узловой адрес в той же подсети, что и интерфейс маршрутизатора;

– *маршрутах к удаленным сетям.* Если IP-адрес назначения пакета принадлежит удаленной сети, то отправить пакет в удаленные сети можно только с помощью пересылки на другой маршрутизатор;

– *маршрутах по умолчанию.* Если IP-адрес назначения пакета не принадлежит подключенной или удаленной сети, маршрутизатору нужно определить, доступен ли «шлюз последней надежды». «Шлюз последней надежды» задается, когда на маршрутизаторе настроен маршрут по умолчанию. При наличии маршрута по умолчанию пакет пересылается на «шлюз последней надежды». Если маршрутизатор не располагает маршрутом по умолчанию, то пакет отбрасывается. В этом случае маршрутизатор отправляет на IP-адрес источника пакета ICMP-сообщение о недоступности узла.

Маршруты в таблице маршрутизации могут задаваться двумя способами:

– вручную администратором сети – такие маршруты называются статическими маршрутами;

– динамически с помощью протоколов маршрутизации – динамические маршруты.

Определение оптимального маршрута подразумевает оценку нескольких путей в одну и ту же сеть назначения и выбор оптимального или кратчайшего пути для прохождения этого маршрута. Когда существует несколько путей до одной сети, каждый путь использует различный выходной интерфейс маршрутизатора для достижения сети.

Протокол маршрутизации выбирает наилучший путь исходя из значения метрик, используемых для определения расстояния до сети. Метрика – это числовое значение, характеризующее «стоимость» маршрута (количество переходов, пропускную способность, качество обслуживания). Наиболее оптимальным путем к сети является путь с наименьшей метрикой.

Протоколы динамической маршрутизации обычно используют собственные правила и метрики для построения и обновления таблиц маршрутизации. Алгоритм маршрутизации генерирует метрики для каждого пути через сеть. Метрики могут основываться на одной или нескольких характеристиках пути. Некоторые протоколы маршрутизации выбирают маршрут на основе нескольких метрик, объединяя их в одну метрику.

Далее приведем примеры динамических протоколов и используемых ими метрик:

– протокол RIP (Routing Information Protocol) – количество переходов;

– протокол OSPF (Open Shortest Path First) – основанная на суммарной полосе пропускания каналов от источника до места назначения;

– протокол EIGRP (Enhanced Interior Gateway Routing Protocol усовершенствованный протокол внутренней маршрутизации между шлюзами) – пропускная способность, задержка, нагрузка и надежность.

Что происходит, когда в таблице маршрутизации содержатся два или более путей с одинаковыми протоколами маршрутизации и одинаковыми метриками?

Если маршрутизатор располагает двумя или более путями к пункту назначения с метриками равной стоимости, он отправляет пакеты по обоим путям. Это называется распределением нагрузки в соответствии с равной стоимостью.

При правильной конфигурации распределение нагрузки может повысить эффективность и производительность сети.

Если на маршрутизаторе с помощью различных протоколов маршрутизации, основанных на различных метриках, построено несколько маршрутов к одной и той же сети, то какой маршрут предпочтительней?

Для сравнительной оценки маршрутов, построенных с помощью различных протоколов маршрутизации в операционной системе Cisco IOS, используется понятие «административное расстояние» (AD). Административное расстояние представляет «надежность» маршрута: чем меньше его значение, тем более надежным является источник маршрута. На рисунке 30 приведены различные протоколы маршрутизации и соответствующие им значения AD.

Источник маршрута	Административное расстояние
Прямой	0
Статическая	1
Суммарный маршрут EIGRP	5
Внешний BGP	20
Внутренний EIGRP	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
Внешний EIGRP	170
Внутренний BGP	200

Рисунок 30 – Административная дистанция

Таким образом, метрика используется для выбора оптимального маршрута при использовании одного вида протоколов маршрутизации, а административная дистанция – для выбора маршрута при использовании различных типов протоколов маршрутизации.

В целом работу протокола динамической маршрутизации можно описать следующим образом:

1 Маршрутизатор определяет и заносит в таблицу маршрутизации информацию о напрямую подключенных сетях.

2 Маршрутизатор отправляет и принимает сообщения протоколов маршрутизации на свои интерфейсы.

3 Маршрутизаторы осуществляют обмен данными маршрутизации о напрямую подключенных сетях с соседями для получения информации об удаленных сетях, которые не являются смежными (два маршрутизатора соединены друг с другом общей смежной сетью).

4 При обнаружении маршрутизатором изменений в топологии протокол маршрутизации может объявить это изменение для других маршрутизаторов.

Существуют различные протоколы маршрутизации (рисунок 31). Для классификации протоколов динамической маршрутизации необходимо определить понятие автономной системы (AS).

Автономная система, или домен маршрутизации, – это группа IP-сетей и маршрутизаторов, управляемых одним или несколькими операторами и имеющих единую политику маршрутизации. Например, сеть интернет-провайдера или сеть компании. Так, региональный интернет-регистратор RIPE присвоил номер автономной системы AS6697 локальному интернет-регистратору(LIR) Белпак (Белтелеком).

Исходя из наличия автономных систем протоколы динамической маршрутизации можно разделить на две большие группы:

– **протоколы внутренней маршрутизации**, используемые для маршрутизации внутри автономной системы. Данный тип маршрутизации также называют внутренней маршрутизацией автономной системы. Компании, организации и даже операторы связи используют протоколы внутренней

маршрутизации в своих внутренних сетях. К протоколам внутренней маршрутизации относятся протоколы RIP, EIGRP, OSPF и IS-IS;

– **протоколы внешней маршрутизации**, используемые для маршрутизации между автономными системами. Маршрутизацию данного типа также называют внешней маршрутизацией автономной системы. Взаимодействие между сетями операторов связи и крупных компаний может осуществляться посредством протокола внешней маршрутизации. На данный момент протокол граничного шлюза (Border Gateway Protocol, BGP) представляет собой единственный практически выполнимый и официальный протокол маршрутизации, используемый в сети Интернет.

Рисунок 31 – Классификация протоколов динамической маршрутизации

Протоколы внутренней маршрутизации:

– **RIPv1 (устаревший)** – дистанционно-векторный классовый протокол внутренней маршрутизации;

– **IGRP (устаревший)** – дистанционно-векторный классовый протокол внутренней маршрутизации, разработанный компанией Cisco (не используется после выхода IOS 12.2 и более поздних версий);

– **RIPv2** – дистанционно-векторный бесклассовый протокол внутренней маршрутизации;

– **EIGRP** – дистанционно-векторный бесклассовый протокол внутренней маршрутизации, разработанный компанией Cisco;

– **OSPF** – бесклассовый протокол внутренней маршрутизации (по состоянию канала);

– **IS-IS** – бесклассовый протокол внутренней маршрутизации (по состоянию канала).

К протоколам внешней маршрутизации можно отнести протокол **BGP** – бесклассовый протокол внешней маршрутизации (по вектору маршрута).

На рисунке 32 приведен пример применения различных протоколов маршрутизации.

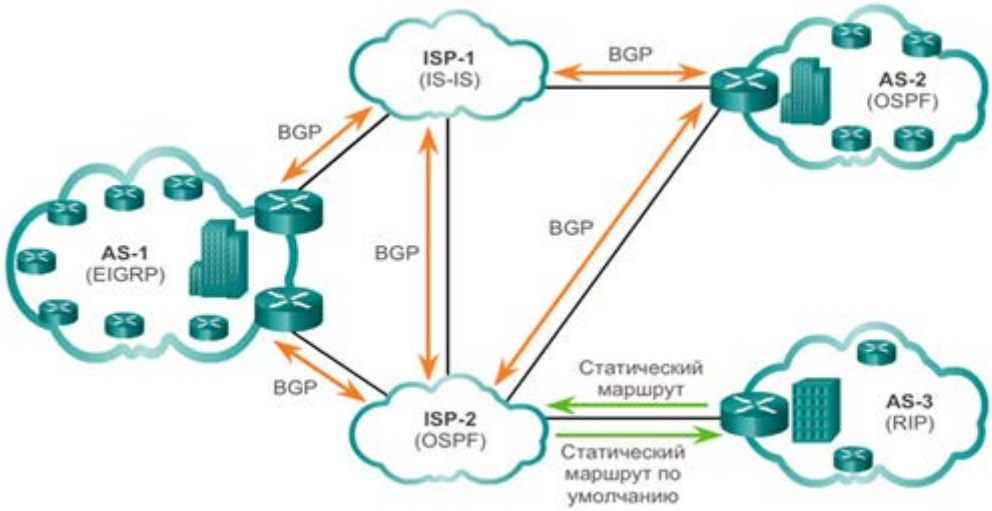


Рисунок 32 – Протоколы внутренней и внешней маршрутизации

Главное различие между классовыми и бесклассовыми протоколами маршрутизации заключается в том, что классовые протоколы маршрутизации не отправляют данные о маске подсети в обновлениях маршрутизации. Бесклассовые протоколы маршрутизации включают в обновления маршрутизации данные о маске подсети.

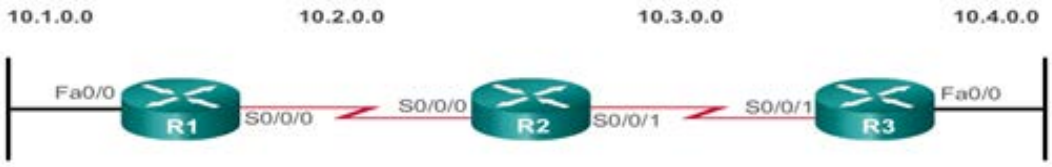
Название протокола определяется двумя параметрами, которые используются при его работе. Дистанция (**расстояние**) определяет удаленность сети назначения; основывается на таких метриках, как число переходов, стоимость, полоса пропускания, значение задержки и т. д. **Вектор** определяет направление маршрутизатора следующего перехода или выходного интерфейса маршрута для доступа к адресу назначения.

Рассмотрим принцип работы дистанционно-векторного протокола RIP. На первом этапе маршрутизатор выполняет обнаружение подключенных сетей напрямую, после чего осуществляет обмен этой информацией с соседними устройствами. Протокол RIP отправляет обновление всем соседним устройствам каждые 30 с и продолжает отправлять обновления даже в том случае, если топология сети не изменялась. К соседним устройствам относятся маршрутизаторы, которые совместно используют канал и работают на базе одного протокола маршрутизации.

Маршрутизатору известны только сетевые адреса собственных интерфейсов и адреса удаленных сетей, доступ к которым он может осуществлять через соседние устройства. После получения обновления маршрутизатор проверяет пакет на наличие данных о новых сетях. Он добавляет все сети, не прописанные в таблице маршрутизации. Маршрутизаторы, использующие дистанционно-векторную маршрутизацию, не

имеют данных о полной топологии сети, например, о пропускной способности каналов, задержках и т. д., а имеют информацию только о количестве переходов (маршрутизаторов) до сети назначения.

На рисунке 33 показан окончательный вариант содержимого таблиц маршрутизации, заполненных по протоколу RIP.



Сеть	Интерфейс	Переход
10.1.0.0	Fa0/0	0
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/0	1
10.4.0.0	S0/0/0	2

Сеть	Интерфейс	Переход
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/1	0
10.1.0.0	S0/0/0	1
10.4.0.0	S0/0/1	1

Сеть	Интерфейс	Переход
10.3.0.0	S0/0/1	0
10.4.0.0	Fa0/0	0
10.2.0.0	S0/0/1	1
10.1.0.0	S0/0/1	2

Рисунок 33 – Таблица маршрутизации протокола RIP

После построения таблиц маршрутизации оптимальный маршрут выбирается исходя из количества переходов по алгоритму Беллмана – Форда.

Недостатки протокола RIPv1:

– учитывается только количество переходов, но не пропускная способность каналов;

– максимальное количество переходов – 15;

– административная дистанция – 120;

– медленное обнаружение отказов.

На основе протокола RIPv1 был разработан усовершенствованный протокол RIPv2.

Следует отметить, что из-за своих ограничений протоколы RIP используются редко. Наибольшее распространение получили протоколы динамической маршрутизации по состоянию канала, например, OSPF.

Основные характеристики протоколов внутренней маршрутизации:

1 **Скорость сходимости** определяет скорость обмена данными маршрутизации и представляет собой время, в течение которого все маршрутизаторы в данной топологии сети будут иметь полностью заполненные таблицы маршрутизации. Чем выше скорость сходимости, тем предпочтительней протокол.

2 **Масштабируемость** определяет максимально возможный размер сети с учетом используемого протокола маршрутизации. Чем больше размер сети, тем больше возможностей для масштабирования должно быть предусмотрено протоколом маршрутизации.

3 **Классовые или бесклассовые протоколы (использование VLSM)**: классовые протоколы маршрутизации не включают маску подсети в обновления и не поддерживают использование VLSM. Бесклассовые протоколы маршрутизации включают в обновления маску подсети, поддерживают использование VLSM и обеспечивают более качественное объединение маршрутов.

4 **Потребление ресурсов** включает такие требования протокола маршрутизации, как объем памяти (ОЗУ), потребление ресурсов ЦП и полосы пропускания канала. Чем выше требования к ресурсам, тем более мощное аппаратное обеспечение требуется для поддержки работы протокола маршрутизации (помимо процессов пересылки пакетов).

5 **Реализация и обслуживание** – характеристика, описывающая уровень знаний, требуемый сетевому администратору для реализации и обслуживания сети на базе развернутого протокола.

Сравнительная характеристика внутренних протоколов маршрутизации приведена на рисунке 34.

	Дистанционно-векторный				Состояние канала	
	RIPv1	RIPv2	IGRP	EIGRP	OSPF	IS-IS
Скорость сходимости	Медленная	Медленная	Медленная	Быстрая	Быстрая	Быстрая
Масштабируемость-Размер сети	Ограниченная	Ограниченная	Ограниченная	Широкая	Широкая	Широкая
Использование VLSM	Нет	Да	Нет	Да	Да	Да
Потребление ресурсов	Низкое	Низкое	Низкое	Среднее	Высокое	Высокое
Реализация и обслуживание	Простое	Простое	Простое	Сложное	Сложное	Сложное

Рисунок 34 – Сравнительный анализ протоколов динамической маршрутизации

6 СЕТЕВАЯ ТРАНСЛЯЦИЯ АДРЕСОВ

Количества публичных IPv4-адресов недостаточно, чтобы назначить уникальные адреса всем устройствам, подключенным к сети Интернет. Количество подключенных устройств «интернета вещей» в 2030 году достигнет 125 млрд, тогда как количество возможных Ipv4-адресов составляет около 4,3 млрд. Без использования NAT адресное пространство IPv4 было бы исчерпано задолго до наступления 2000 года, поэтому большинство сетей в настоящее время строится по следующему принципу: клиенту выделяется один или несколько «белых» публичных адресов.

При передаче трафика внутри сети используются частные адреса. При необходимости отправки трафика из внутренней сети с частными адресами во внешнюю сеть (или получения трафика из другой сети) частный адрес преобразуется в уникальный публичный адрес с помощью службы сетевой трансляции адресов – NAT.

Несмотря на свои преимущества, NAT имеет ряд ограничений, которые будут рассмотрены далее. Решением проблемы исчерпания пространства IPv4-адресов и ограничений NAT является окончательный переход на IPv6, однако такой переход сопряжен со значительными финансовыми и временными затратами.

Как показано на рисунке 35, в большинстве случаев сети реализуются с использованием частных IPv4-адресов в соответствии с RFC 1918.

Рисунок 35 – Преобразование NAT

Кроме экономии адресов, NAT обеспечивает повышение степени конфиденциальности и безопасности сети – это объясняется тем, что данный механизм скрывает внутренние IPv4-адреса от внешних сетей.

Для маршрутизатора с поддержкой NAT можно настроить один или несколько действующих публичных IPv4-адресов. Эти публичные адреса известны как пул адресов NAT. Когда внутреннее устройство отправляет трафик за пределы сети, маршрутизатор с поддержкой NAT преобразует внутренний IPv4-адрес устройства в публичный адрес из пула NAT.

Маршрутизатор NAT обычно работает на границе тупиковой сети. Тупиковая сеть – это сеть, использующая единственное соединение с соседней сетью, один входящий маршрут и один исходящий маршрут. В примере, показанном на рисунке 36, R2 является пограничным маршрутизатором. С точки зрения интернет-провайдера маршрутизатор R2 создает тупиковую сеть.

Рисунок 36 – Тупиковая сеть

Когда устройству в тупиковой сети требуется соединение с устройством вне его сети, пакет пересылается пограничному маршрутизатору. Пограничный маршрутизатор выполняет процесс NAT, преобразуя внутренний частный адрес устройства в публичный адрес.

В Cisco IOS для технологии NAT используется четыре типа адресов:

– внутренний локальный адрес;

– внутренний глобальный адрес;

– внешний локальный адрес;

– внешний глобальный адрес.

При этом внутренний адрес – это адрес устройства, преобразуемый механизмом NAT, внешний – это адрес устройства назначения, локальный – это любой адрес, появляющийся во внутренней сети, глобальный адрес – это любой адрес, появляющийся во внешней сети.

На рисунке 37 показано, как адресуется трафик, отправленный внутренним компьютером внешнему веб-серверу через маршрутизатор с поддержкой NAT.

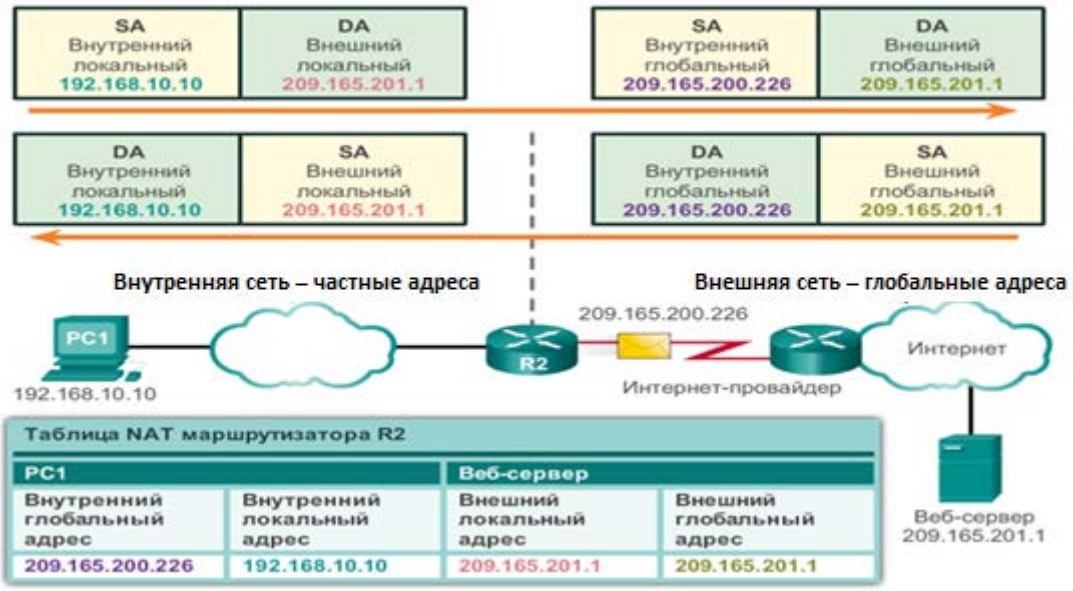


Рисунок 37 – Принцип работы NAT

Также на рисунке 37 показано, как первоначально адресуется и преобразуется обратный трафик: PC1 с частным адресом 192.168.10.10 хочет подключиться к внешнему веб-серверу с публичным адресом 209.165.201.1.

PC1 посылает пакет, адресованный веб-серверу. Пакет пересылается маршрутизатору R2, на котором настроена поддержка технологии NAT.

Маршрутизатор R2 преобразует внутренний локальный адрес 192.168.10.10 во внутренний глобальный адрес 209.165.200.226 и добавляет это сопоставление локального и глобального адресов в таблицу NAT. R2 отправляет по назначению пакет с преобразованным адресом источника.

Веб-сервер отвечает пакетом, адресованным внутреннему глобальному адресу PC1 (209.165.200.226).

R2 получает пакет с адресом назначения 209.165.200.226. R2 проверяет таблицу NAT и находит запись для этого сопоставления. R2 использует эту информацию и преобразует внутренний глобальный адрес (209.165.200.226) во внутренний локальный адрес (192.168.10.10), после чего пакет пересылается PC1.

Существуют три механизма преобразования сетевых адресов:

1 **Статическое преобразование** сетевых адресов (статический NAT) – это взаимно однозначное соответствие между локальным и глобальным адресами.

2 **Динамическое преобразование** сетевых адресов (динамический NAT) – это сопоставление адресов по схеме «многие ко многим» между локальными и глобальными адресами.

3 Преобразование адресов портов (PAT) – это сопоставление адресов по схеме «многие к одному» между локальными и глобальным адресами. Данный метод также называется перегрузкой (NAT с перегрузкой).

Статический NAT использует сопоставление локальных и глобальных адресов по схеме «один в один». Эти соответствия задаются администратором сети и остаются неизменными (рисунок 38).

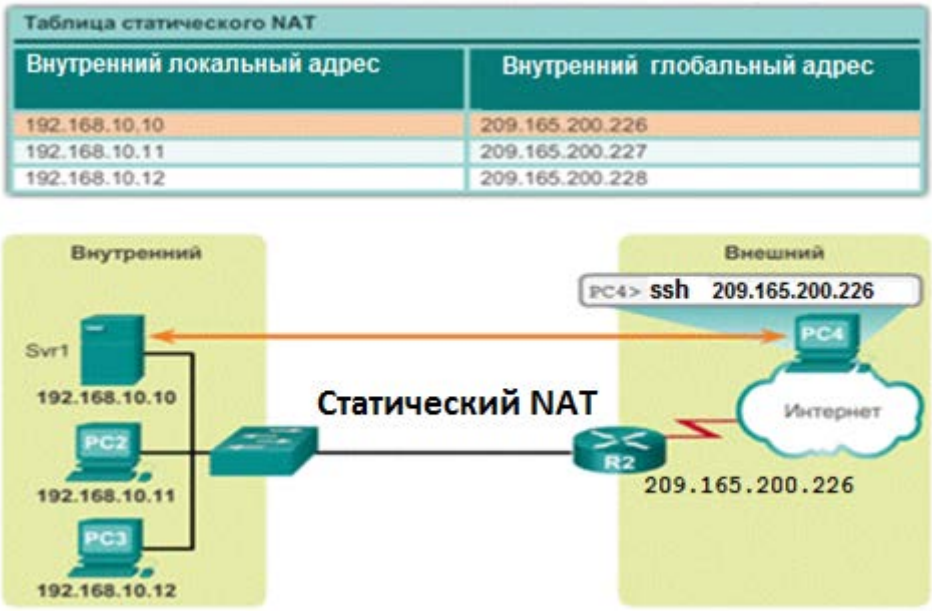


Рисунок 38 – Статический NAT

Для маршрутизатора R2 настроены статические соответствия для внутренних локальных адресов Svr1, PC2 и PC3. Когда эти устройства отправляют трафик в Интернет, их внутренние локальные адреса преобразуются в заданные внутренние глобальные адреса.

Метод статического преобразования сетевых адресов особенно полезен для веб-серверов или устройств, которые должны иметь постоянный адрес,

доступный из Интернета, например, для веб-сервера компании. При этом сервер располагается за маршрутизатором, на котором можно настроить различные политики безопасности, защищающие сервер от атак из внешней сети.

Статический NAT также подходит для устройств, которые должны быть доступны для удаленного управления авторизованными пользователями из внешней сети, но при этом оставаться закрытыми для общего доступа через Интернет. Например, сетевой администратор может с PC4 подключиться с помощью SSH к внутреннему глобальному адресу Svr1 (209.165.200.226). Маршрутизатор R2 преобразует этот внутренний глобальный адрес во внутренний локальный адрес и подключает сеанс администратора к Svr1.

Для статического NAT требуется достаточное количество публичных адресов, доступных для общего количества одновременных сеансов пользователей внутренней сети.

Метод динамического преобразования сетевых адресов (динамический NAT) использует пул публичных адресов, которые присваиваются в порядке живой очереди, и работает по схеме «многие к многим». Когда внутреннее устройство запрашивает доступ к внешней сети, динамический NAT присваивает доступный публичный IPv4-адрес из пула (рисунок 39).

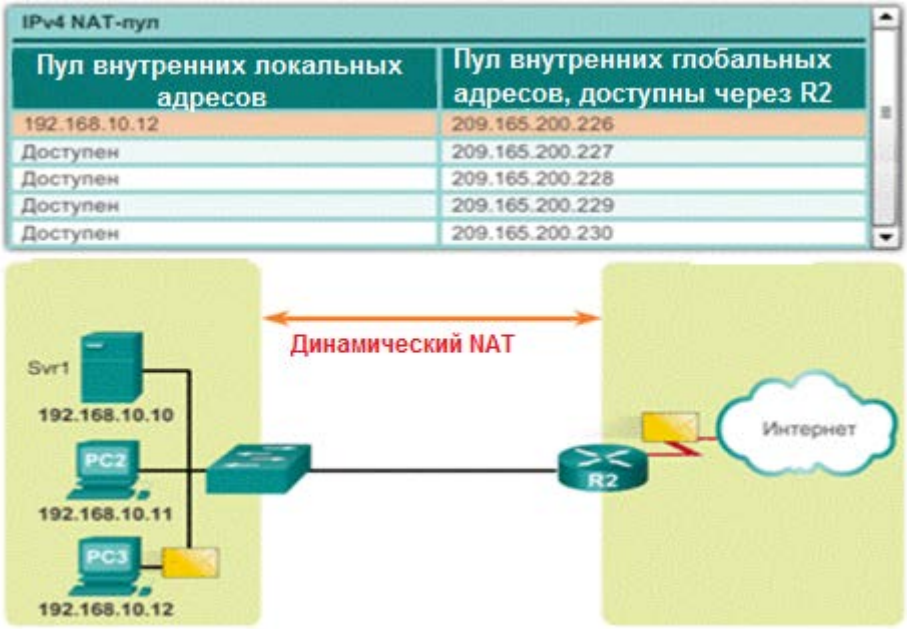


Рисунок 39 – Динамический NAT

На рисунке 38 PC3 получает доступ к Интернету, используя первый доступный адрес из пула динамического NAT. Другие адреса по-прежнему доступны для использования. Аналогично статическому NAT для динамического NAT требуется достаточное количество публичных адресов, способное обеспечить общее количество одновременных сеансов пользователей. При отсутствии свободных глобальных адресов в пуле доступ узлу во внешнюю сеть невозможен.

Преобразование адресов портов (PAT), также называемое NAT с перегрузкой, сопоставляет множество частных IPv4-адресов одному или нескольким публичным IPv4-адресам. NAT с перегрузкой – это наиболее распространенный метод преобразования сетевых адресов.

В данном методе один (или несколько) глобальных адресов сопоставляются группе пар значений: частному IP-адресу источника и порту источника протокола транспортного уровня TCP или UDP.

Преобразование PAT пытается сохранить оригинальный порт источника. В том случае, если оригинальный порт источника уже используется, PAT назначает первый доступный номер порта, начиная с начала соответствующей группы портов – 0-511, 512-1023 или 1024-65535. Если доступных портов больше нет, а в пуле адресов есть несколько внешних адресов, PAT переходит к следующему адресу, пытаясь выделить оригинальный порт источника. Данный процесс продолжается до тех пор, пока не исчерпаются как доступные порты, так и внешние IP-адреса (рисунок 40).

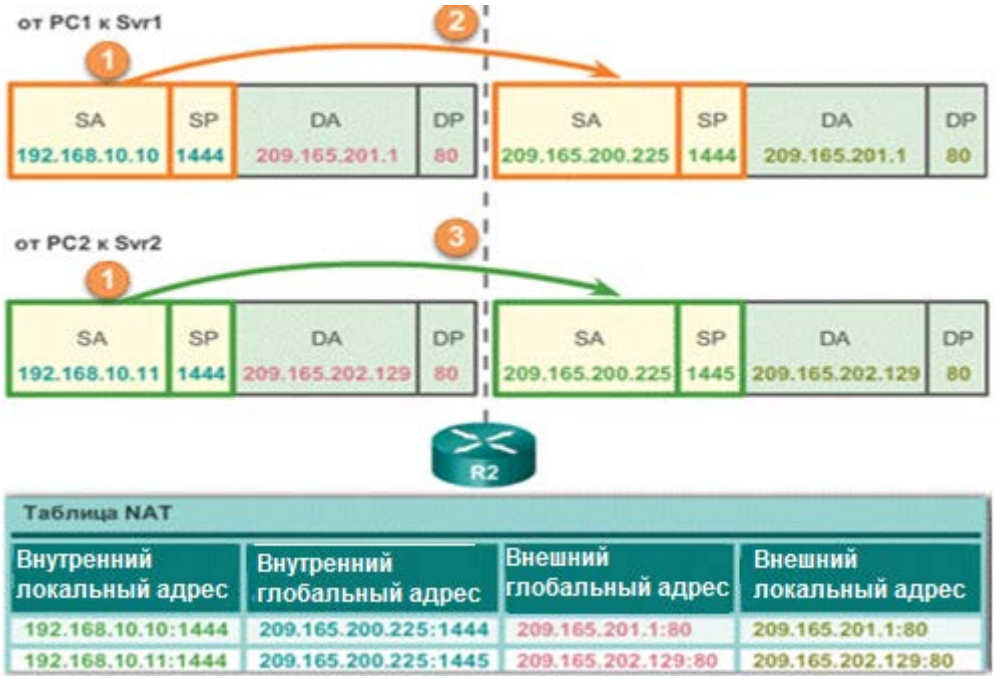


Рисунок 40 – Принцип работы NAT с перегрузкой

Так, на рисунке 40 маршрутизатор R2 обрабатывает каждый пакет, поступающий из внутренней сети. Он использует номер порта (в рассматриваемом примере номера портов совпадают – 1444) для идентификации устройства, с которого поступил пакет. Адрес источника (SA) – это внутренний локальный адрес с добавленным номером порта TCP/IP. Адрес назначения (DA) – это внешний локальный адрес с добавленным номером порта службы. В данном примере порт службы равен 80: соответствует протоколу HTTP.

Так как номера портов источников совпадают (что бывает редко), маршрутизатор увеличивает номер порта на единицу (1445), заменяет внутренний локальный адрес на внутренний глобальный адрес и записывает это сопоставление в таблицу NAT.

PAT гарантирует, что устройства будут использовать разные номера портов TCP для каждого сеанса взаимодействия с сервером в Интернете. При возвращении ответа от сервера номер порта источника, который становится номером порта назначения при обратной передаче, определяет, какому устройству маршрутизатор перешлет соответствующие пакеты.

NAT обеспечивает множество преимуществ, в том числе следующие:

– NAT сохраняет официально зарегистрированную схему адресации, разрешая частное использование внутренних сетей. NAT экономит адреса благодаря мультиплексированию приложений на уровне портов. При использовании NAT с перегрузкой внутренние узлы могут использовать для всех внешних взаимодействий один публичный IPv4-адрес. При этом типе конфигурации для поддержки множества внутренних узлов требуется очень небольшое количество внешних адресов;

– NAT повышает гибкость подключений к публичной сети. Для обеспечения надежных подключений к публичной сети можно создать множественные пулы, резервные пулы и пулы распределения нагрузки;

– NAT обеспечивает согласованность схем внутренней сетевой адресации. Если в сети не используются частные IPv4-адреса и NAT, изменение схемы публичных IPv4-адресов потребует изменения адресов всех узлов существующей сети. Затраты на изменение адресации узлов могут оказаться существенными. NAT позволяет сохранить существующую схему частных IPv4-адресов, одновременно поддерживая простой переход на новую схему публичной адресации. Это означает, что организация может сменить интернет-провайдера, не меняя настроек своих внутренних клиентов;

– NAT обеспечивает безопасность сети. Поскольку частные сети не объявляют ни свои адреса, ни внутреннюю топологию, они остаются в достаточной степени защищенными при использовании NAT для получения управляемого внешнего доступа. Тем не менее, NAT не заменяет межсетевые экраны.

Преобразование сетевых адресов (NAT) имеет ряд недостатков. Тот факт, что узлы в Интернете взаимодействуют непосредственно с устройством, поддерживающим NAT, а не с фактическим узлом частной сети, создает ряд проблем.

Один из недостатков использования NAT связан с производительностью сети, особенно это касается протоколов реального времени, таких как VoIP. NAT увеличивает задержки коммутации, поскольку преобразование каждого IPv4-адреса в заголовках пакетов требует времени. Коммутация первого пакета является программным процессом – этот пакет всегда проходит более медленным путем. Маршрутизатор должен анализировать каждый пакет, чтобы решить, требуется ли его преобразование. Маршрутизатор должен изменить

заголовок IPv4 и по возможности изменить заголовок TCP или UDP. При каждом преобразовании должна быть пересчитана контрольная сумма заголовка IPv4, а также контрольная сумма TCP или UDP. Если в кэше есть соответствующая запись, остальные пакеты проходят по пути с быстрой коммутацией. В противном случае они тоже задерживаются.

Другим недостатком использования NAT является потеря сквозной адресации. Многие интернет-протоколы и приложения зависят от сквозной адресации от источника до узла назначения. Некоторые приложения не совместимы с NAT. Например, некоторые приложения безопасности, такие как электронные подписи, не работают с NAT, поскольку IPv4-адрес источника изменяется, прежде чем пакет успевает достигнуть узла назначения.

Кроме того, утрачивается возможность трассировки сквозного соединения IPv4. Очень сильно усложняется трассировка пакетов, подвергающихся многочисленным изменениям адреса пакета при прохождении нескольких участков NAT, что, в свою очередь, затрудняет устранение неполадок.

Использование NAT также усложняет протоколы туннелирования, такие как IPSec, так как NAT изменяет значения в заголовках, что мешает проверкам целостности, выполняемым протоколом IPSec и другими протоколами туннелирования. Кроме того, протокол IPSec является протоколом сетевого уровня и не использует порты, что затрудняет его работу через PAT.

Использование динамических NAT и PAT не позволяет пользователям из внешней сети первыми подключиться к устройствам за NAT, используя протоколы TCP и UDP. Для доступа к устройствам за NAT необходимо на маршрутизаторах, на которых настроен NAT, включить функцию «проброса портов». Еще один способ прохода через NAT – это использование посредника. Сначала узлы за NAT, которым надо связаться напрямую, сообщают узлу-посреднику свои параметры настройки NAT (номера портов и IP-адреса), потом каждый узел за NAT получает параметры настройки NAT-узла, с которым он хочет установить связь, и после этого узлы начинают общаться через NAT напрямую. Такие технологии носят название UDP hole punching. По такой схеме работают программы Skype, Teamviewer. Еще одна технология прохода через NAT – технология NAT Traversal. Эту технологию использует протокол организации защищенного VPN туннеля IPSec. Суть ее состоит в том, что сформированный пакет протокола IPSec перед отправкой запаковывается в UDP-пакет – в результате в пакете появляются порты, и тогда такой пакет может пройти через NAT, на котором настроен проброс портов.

NAT для IPv6 используется в совсем другом контексте, нежели NAT для IPv4. Разнообразные варианты NAT для IPv6 используются с целью предоставления прозрачного доступа между сетями, в которых используется только протокол IPv6, и сетями, в которых используется только протокол IPv4. NAT для IPv6 не применяется для преобразования частных IPv6-адресов в глобальные IPv6-адреса.

В идеале IPv6 должен по возможности использоваться в исходном формате. Это означает, что устройства IPv6 взаимодействуют друг с другом по сетям IPv6. IETF разработала несколько методов перехода от IPv4 к IPv6, включая использование двойного стека, туннелирование и преобразование.

Двойной стек применяется, когда устройства используют протоколы, связанные как с IPv4, так и с IPv6. Туннелирование для IPV6 – это процесс инкапсуляции пакетов IPv6 в пакеты IPv4. Данный метод позволяет передавать пакет IPv6 по сети, в которой используется только протокол IPv4.

NAT для IPv6 следует использовать не как долгосрочную стратегию, а как временный механизм, помогающий перейти с IPv4 на IPv6. Со временем появилось несколько типов NAT для IPv6, включая NAT-PT (Network Address Translation-Protocol Translation, преобразование сетевых адресов – преобразование протоколов). IETF признала технологию NAT-PT устаревшей и порекомендовала использовать ее замену – NAT64.

7 ВИРТУАЛЬНЫЕ ЛОКАЛЬНЫЕ СЕТИ

Так как технологии виртуальных локальных сетей относятся к технологиям канального уровня, то для понимания логики работы таких сетей необходимо рассмотреть, каким образом работают устройства канального уровня: мосты и коммутаторы. Так как первые сети технологии Ethernet строились по топологии «общая шина» на повторителях (HUB), то количество коллизий в таких сетях было пропорционально количеству компьютеров. Это обстоятельство резко снижало производительность таких сетей.

С появлением технологии Fast Ethernet появились специальные устройства: сначала мосты, а затем коммутаторы, которые позволили разделять (сегментировать) один общий домен коллизий на отдельные сегменты. В результате коллизии, возникающие в одном сегменте, не влияли на коллизии в другом сегменте. На рисунке 41 изображена схема работы моста.

В исходном состоянии мост не знает, компьютеры с какими MAC-адресами подключены к каждому из его портов. В этом случае мост просто передает любой захваченный и буферизованный кадр на все свои порты, за исключением того, от которого этот кадр получен (передается широковещательный кадр).

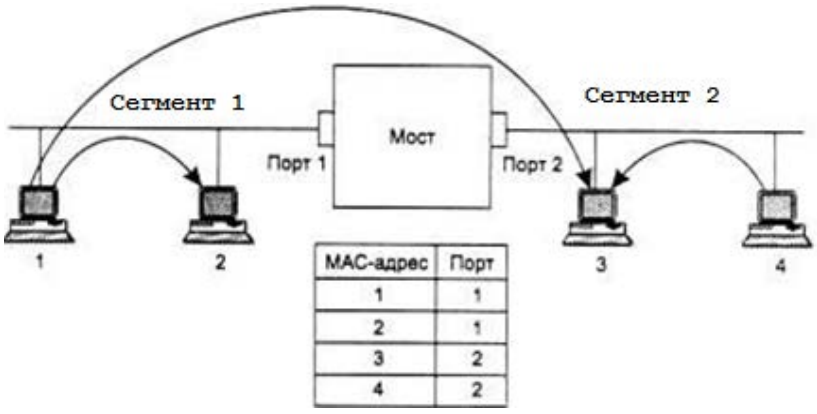


Рисунок 41 – Схема работы моста

Одновременно с передачей кадра на все порты мост изучает адрес источника кадра и делает запись о его принадлежности в своей адресной таблице, которую также называют таблицей фильтрации или маршрутизации. Например, получив на свой порт 1 кадр от компьютера 1, мост делает первую запись в своей адресной таблице: MAC-адрес 1 – порт 1. Если все четыре компьютера данной сети проявляют активность и посылают друг другу кадры, то скоро мост построит полную адресную таблицу сети, состоящую из четырех записей – по одной записи на узел.

После того как мост прошел этап обучения, он может работать более рационально. При получении кадра, направленного, например, от компьютера 1 компьютеру 3, он просматривает адресную таблицу на предмет совпадения ее адресов с адресом назначения 3. Поскольку такая запись есть, то мост проверяет, находятся ли компьютеры с адресами источника (в нашем случае – это адрес 1) и адресом назначения (адрес 3) в одном сегменте. Так как в нашем примере они находятся в разных сегментах, то мост выполняет операцию ***продвижения*** **(forwarding)** кадра – передает кадр на другой порт, предварительно получив доступ к другому сегменту.

Если бы оказалось, что компьютеры принадлежат одному сегменту, то кадр просто был бы удален из буфера, и работа с ним на этом бы закончилась. Такая операция называется ***фильтрацией*** **(filtering).**

Если же адрес назначения неизвестен, то мост передает кадр на все свои порты, кроме порта – источника кадра, как и на начальной стадии процесса обучения.

Процесс обучения моста никогда не заканчивается. Мост постоянно следит за адресами источника буферизуемых кадров, чтобы быть в состоянии автоматически приспосабливаться к изменениям, происходящим в сети, – перемещениям компьютеров из одного сегмента сети в другой, появлению новых компьютеров.

Для связи значительного количества сетей несколько мостов стали конструктивно объединять в одно устройство – коммутатор. Таким образом, коммутатор – это набор мостов. Одновременно устанавливает несколько соединений между разными парами портов (*микросегментация*) (рисунок 42).

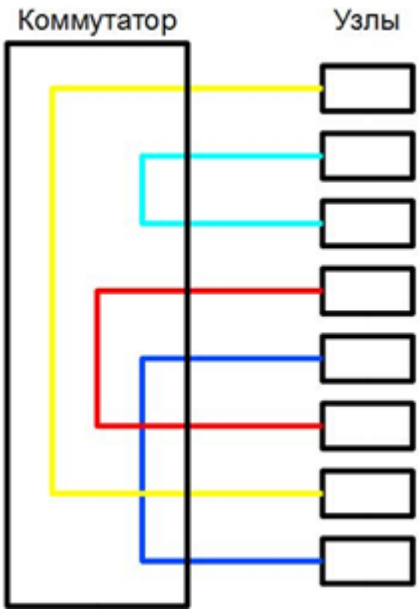
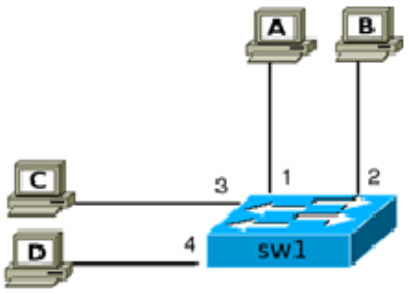


Рисунок 42 – Структурная схема коммутатора

Каждый порт коммутатора – отдельный домен коллизий, т. е. доменов коллизий столько, сколько портов, так как одновременная передача может возникнуть только между отдельным портом и компьютером, подключенным к этому порту.

При дуплексной передаче коллизии отсутствуют, так как тракты приема и передачи разделены.

Так же как и мост, коммутатор строит аналогичную таблицу коммутации (рисунок 43).



Порт коммутатора	MAC-адрес хоста
1	A
2	B
3	C
4	D

Рисунок 43 – Таблица коммутации коммутатора

На рисунке 44 изображены три режима работы коммутаторов:

– с промежуточным хранением (буферизацией (Store and Forward). Коммутатор помещает весь кадр в буфер, проверяет его на отсутствие ошибок, выбирает порт коммутации и после этого посылает в него кадр;

– «на лету» (on-the-fly) или сквозной (cut-through). Коммутатор считывает в кадре только адрес назначения и после выполняет коммутацию. Этот режим уменьшает задержки при передаче, но в нем нет метода обнаружения ошибок;

– исключение фрагментов. Этот режим является модифицированной формой сквозного режима. В нем передача осуществляется после фильтрации фрагментов коллизий, к которым относится подавляющее число ошибочных пакетов. Коммутатор в этом режиме ждет окончания проверки, не является ли полученный пакет коллизионным фрагментом, и только после этого передает его.

Рисунок 44 – Способы обработки кадров коммутатором

В зависимости от количества уровней модели OSI выделяют:

– **коммутаторы второго уровня**, которые коммутируют кадры на основе анализа MAC-адресов канального уровня модели OSI;

– **коммутаторы третьего уровня**, которые осуществляют коммутацию и фильтрацию на основе адресов канального (уровень 2) и сетевого (уровень 3) уровней модели OSI.

Производительность сети является важным фактором эффективности работы организации. Одной из технологий повышения производительности сети является разделение крупных широковещательных доменов на более мелкие. Маршрутизаторы устроены таким образом, что блокируют широковещательный трафик на интерфейсе. При этом маршрутизаторы обычно имеют ограниченное количество интерфейсов LAN. Основная роль маршрутизатора заключается в передаче информации между сетями, а не в предоставлении оконечным устройствам доступа к сети.

Поэтому для уменьшения размера широковещательных доменов была разработана технология разделения сети на отдельные широковещательные домены с помощью устройств второго уровня, которая получила название виртуальные локальные сети (Virtual Local Area Network, VLAN). Несмотря на то, что сети VLAN в основном используются в коммутируемых локальных

сетях, современные реализации VLAN способны функционировать также в муниципальных (MAN) и глобальных (WAN) сетях.

Сети VLAN обеспечивают гибкость сегментации и организации. Сети VLAN позволяют сгруппировать устройства внутри локальной сети. Сети VLAN основываются не на физических, а на логических подключениях.

Сети VLAN позволяют администратору производить сегментацию по функциям, проектным группам или областям применения вне зависимости от физического расположения пользователя или устройства. Устройства в пределах сети VLAN работают таким образом, будто находятся в собственной независимой сети, даже если делят одну общую инфраструктуру с другими VLAN. Любой порт коммутатора может принадлежать сети VLAN. Одноадресные, широковещательные и многоадресные пакеты пересылаются и рассылаются только к конечным станциям в пределах той сети VLAN, которая является источником этих пакетов. Каждая сеть VLAN на рисунке 45 считается отдельной логической сетью, и пакеты, адресованные станциям, не принадлежащим данной сети VLAN, должны пересылаться через устройство, поддерживающее маршрутизацию.

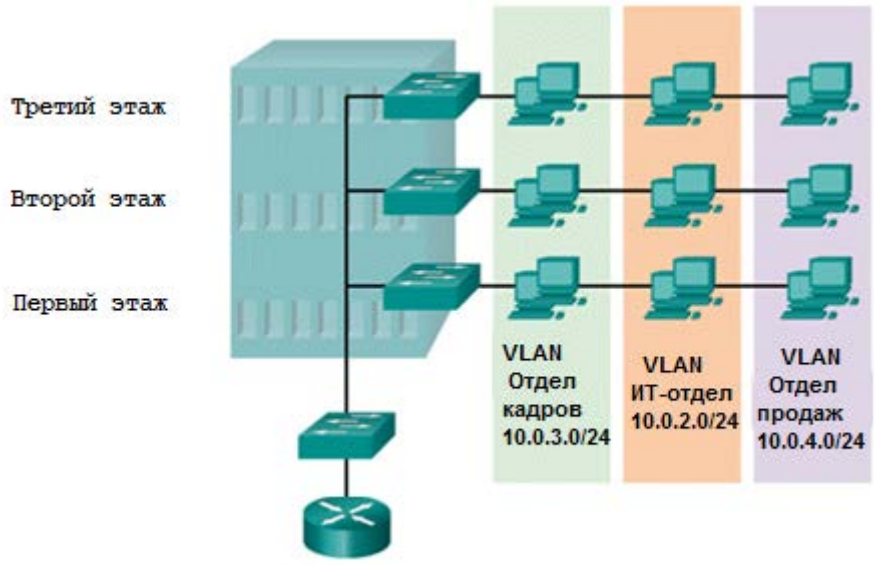


Рисунок 45 – Пример организации сети VLAN

Сеть VLAN создает логический широковещательный домен, который может охватывать несколько физических сегментов LAN. Разделяя крупные широковещательные домены на более мелкие сети, VLAN повышают производительность сети. Если устройство в одной сети VLAN передает широковещательный кадр Ethernet, то этот кадр получают все устройства в рамках этой VLAN; устройства же в других сетях VLAN этот кадр не получают.

Сети VLAN позволяют реализовывать политику обеспечения доступа и безопасности, учитывая интересы различных групп пользователей. Каждый

порт коммутатора может быть назначен только одной сети VLAN (за исключением порта, подключенного к IP-телефону или другому коммутатору).

Таким образом, к основным преимуществам использования VLAN относятся:

1 Безопасность. Группы, обладающие уязвимыми данными, отделены от остальной части сети, благодаря чему снижается вероятность утечки конфиденциальной информации.

2 Повышение производительности. Разделение однородных сетей второго уровня на несколько логических рабочих групп (широковещательных доменов) уменьшает количество лишнего сетевого трафика и повышает производительность.

3 Уменьшенные широковещательные домены. Разделение сети на сети VLAN уменьшает количество устройств в широковещательном домене.

4 Упрощение администрирования сети. Сети VLAN упрощают управление сетью, поскольку пользователи с аналогичными требованиями к сети используют одну и ту же сеть VLAN. При введении в эксплуатацию нового коммутатора на назначенных портах реализуются все правила и процедуры, уже примененные в этой конкретной VLAN. Также IT-специалистам легче определять функцию сети VLAN, назначая ей соответствующее имя.

5 Упрощенное управление проектами. Сети VLAN объединяют пользователей и сетевые устройства для соответствия деловым или географическим требованиям сети. Управление проектом и работа на прикладном уровне упрощены благодаря использованию разделения функций. Каждая VLAN в коммутируемой сети относится к какой-либо IP-сети, таким образом, в проекте сети VLAN нужно учитывать реализацию иерархической системы сетевой адресации. Иерархическая адресация подразумевает упорядоченное назначение номеров IP-сети сетям VLAN с учетом работы сети в целом.

В коммутаторах могут быть реализованы следующие типы VLAN:

– на основе портов;
– на основе стандарта IEEE 802.1Q;
– на основе MAC-адресов;
– на основе стандарта IEEE 802.1ad (Q-in-Q VLAN);
– на основе портов и протоколов IEEE 802.1v.

На рисунке 46 приведен пример организации сети на основе портов. В этом случае определенные порты разных коммутаторов включаются в соответствующие VLAN. Если в одну VLAN включены порты разных коммутаторов, то необходимо создать отдельное соединение для каждой VLAN.

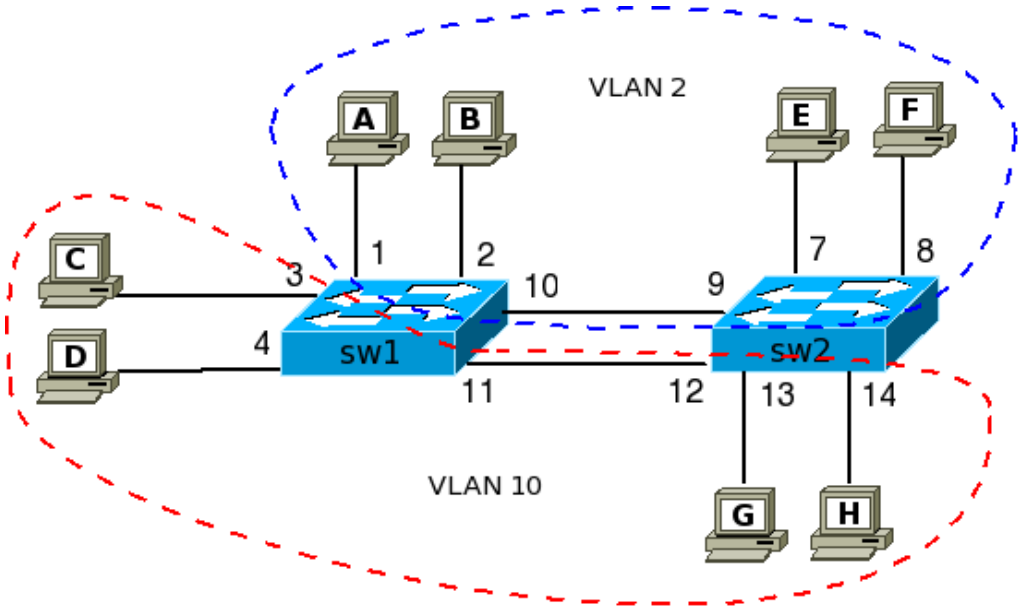


Рисунок 46 – Пример организации VLAN на основе портов

Когда количество VLAN возрастает, то для каждого VLAN необходимо добавлять связь между коммутаторами, для того чтобы объединить хосты в каждой VLAN. Это является недостатком такого подхода.

Для исключения этого недостатка используется метод построения сети VLAN на основе стандарта IEEE 802.1Q и транкового канала, который показан на рисунке 47.

В этом случае на каждом коммутаторе соответствующий порт переводится в транковый режим – транковый порт. В нашем примере это порты 21 и 22 соответствующих коммутаторов. Между двумя транковыми портами образуется транковый канал типа «точка – точка», через который проходят кадры из разных VLAN. Транки виртуальных сетей обеспечивают распространение всего трафика VLAN между коммутаторами так, чтобы устройства, находящиеся в одной сети VLAN, но подключенные к разным коммутаторам, могли обмениваться данными без вмешательства маршрутизатора.

Транк виртуальных сетей не принадлежит какой-либо определенной сети VLAN, а, скорее, является «кабельным каналом» передачи многих VLAN между коммутаторами и маршрутизаторами. Транк может также использоваться между сетевым устройством и сервером или другим устройством, оснащенным соответствующим сетевым адаптером с поддержкой 802.1Q.

Как показано на рисунке 47, для того чтобы направлять кадры из транкового канала в соответствующую VLAN, в кадр канального уровня добавляется специальный тег, изображенный на рисунке 48, где находится номер соответствующей VLAN.

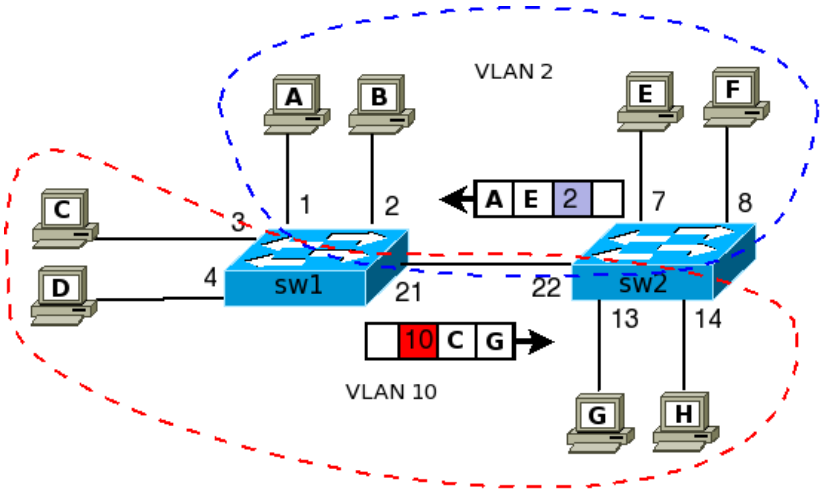


Рисунок 47 – Пример сети VLAN на основе стандарта IEEE 802.1Q

Обновленный кадр становится маркированным. После попадания в соответствующую VLAN тег отбрасывается, и кадр опять становится немаркированным.

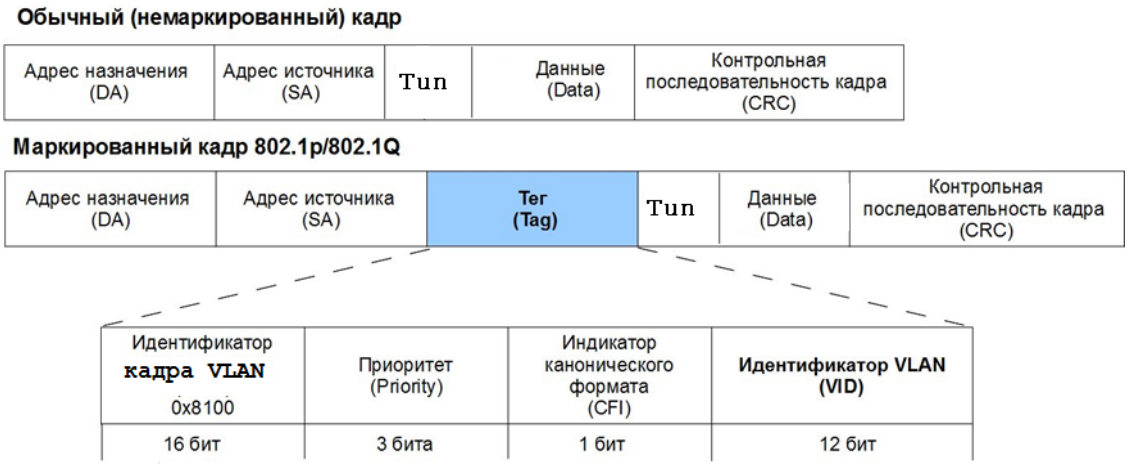


Рисунок 48 – Формат кадра IEEE 802.1Q

Выделят различные типы VLAN:

1 *Виртуальная локальная сеть для данных* – это сеть VLAN, которая настроена специально для передачи трафика, генерируемого пользователем. Сеть VLAN, передающая голосовой трафик или трафик управления, не является сетью VLAN для передачи данных. Рекомендуется отделять голосовой и управляющий трафики от трафика данных. VLAN для передачи данных иногда называют пользовательской сетью VLAN. Сети VLAN для данных используются для разделения сети на группы пользователей или устройств.

2 *VLAN по умолчанию*. Все порты коммутатора становятся частью VLAN по умолчанию после первоначальной загрузки коммутатора. Порты коммутатора, находящиеся в сети VLAN по умолчанию, являются частью одного широковещательного домена. Благодаря этому любое устройство, подключенное к любому порту коммутатора, может обмениваться данными с

другими устройствами на других портах коммутатора. Сетью VLAN по умолчанию для коммутаторов Cisco установлена VLAN 1.

3 *Native VLAN* – это понятие в стандарте 802.1Q, которое обозначает VLAN на коммутаторе, где все кадры идут без тега (т. е. трафик передается нетегированным). В CISCO по умолчанию Native VLAN – это VLAN 1. Номер Native VLAN можно поменять. Если коммутатор получает нетегированные кадры на транковом порту, он автоматически пересылает их к Native VLAN.

Рекомендуется настроить native VLAN как неиспользуемую VLAN, отличающуюся от сети VLAN 1 и других VLAN.

4 *Управляющая VLAN – это любая сеть VLAN, настроенная для доступа к функциям управления коммутатора. Сеть VLAN 1 по умолчанию является управляющей VLAN.* Для создания управляющей VLAN на коммутаторе необходимо создать виртуальный интерфейс SVI (Switch Virtual Interface) для данной VLAN, *назначаются IP-адрес и маска подсети, благодаря чему коммутатором можно управлять через протоколы HTTP, Telnet, SSH или SNMP. Поскольку в исходной настройке коммутатора Cisco VLAN 1 является сетью VLAN по умолчанию, VLAN 1 не следует использовать в качестве управляющей VLAN*. Все порты назначены сети VLAN 1 по умолчанию. Таким образом, сети Native VLAN и управляющая VLAN совпадают. Подобная настройка считается угрозой безопасности.

5 VLAN для передачи голоса. Для поддержки передачи голоса по IP (VoIP) требуется отдельная сеть VLAN. Для VoIP-трафика требуются:

– гарантированная полоса пропускания для обеспечения высокого качества голосовой передачи;

– приоритет передачи перед другими типами сетевого трафика;

– возможность маршрутизации в обход перегруженных участков;

– задержка менее 150 мс по всей сети.

Для того чтобы соответствовать этим требованиям, вся сеть должна быть специально спроектирована для поддержки VoIP.

8 ВИРТУАЛЬНЫЕ ЧАСТНЫЕ СЕТИ

Глобальные сети WAN (Wide Area Network) используются для организации связи между корпоративной сетью предприятия и локальными сетями удаленных филиалов, а также для подключения удаленных работников к корпоративной сети. Без глобальных сетей сети LAN оставались бы группой изолированных сетей. Сети LAN обеспечивают достаточную скорость и экономическую эффективность при передаче данных в пределах относительно небольших географических областей. Однако по мере того, как организации расширяются, для решения бизнес-задач требуется обмен информацией между территориально разнесенными площадками. Ниже приведены некоторые примеры использования глобальных сетей:

– персоналу в офисах региональных отделений или филиалов организации необходимо взаимодействовать с центральным офисом и обмениваться с ним данными;

– предприятиям требуется обмен информацией с организациями клиентов. Например, производители программного обеспечения регулярно обмениваются информацией о продукте и рекламными материалами с дистрибьюторами, продающими их продукцию конечным пользователям;

– сотрудники, путешествующие по делам предприятия, часто нуждаются в доступе к информации, хранящейся в корпоративных сетях.

Соединить филиалы, находящиеся на больших расстояниях, с помощью собственных линий связи и оборудования, как правило, нереально из-за слишком высокой стоимости. Поэтому глобальная сеть обычно принадлежит оператору связи. Организация должна вносить плату за предоставляемые оператором связи услуги по подключению к удаленным узлам. К WAN-провайдерам относятся такие операторы связи, как владельцы телефонной сети, кабельные компании или операторы спутниковой связи и сотовой связи. Операторы связи предоставляют каналы для подключения удаленных узлов с целью передачи данных.

На рисунке 49 приведена классификация способов организации доступа к глобальной сети. Приведенные технологии имеют общее название – технологии «последней мили». Последняя миля – это канал, соединяющий конечное клиентское оборудование с узлом доступа провайдера. Как видно, соединить удаленные филиалы или подключить удаленных пользователей (т. е. организовать глобальную сеть) можно двумя способами: с помощью технологий частных глобальных сетей либо с помощью технологий общедоступных сетей.

При использовании частных глобальных сетей интернет-провайдеры предлагают аренду: постоянные выделенные линии (каналы) «точка – точка» либо коммутируемые соединения, которые в свою очередь делятся на соединения коммутации каналов, например, ТСОП (телефонная сеть общего пользования) или ISDN и соединения с коммутацией пакетов, такие как Ethernet, ATM и Frame Relay. Эти сети называются частными, потому что по ним передается информация только конкретной организации, с которой заключен договор на аренду. Другая организация не имеет возможности передавать данные по этой сети. Провайдер обеспечивает определенный уровень безопасности.

При использовании технологий общедоступных сетей данные передаются через открытую сеть Интернет. Интернет-провайдер предлагает широкополосный доступ, основанный на технологиях DSL, а также на беспроводных технологиях. При этом по одним и тем же линиям и оборудованию могут передаваться данные различных пользователей. Поэтому в этом случае стоит проблема защиты передаваемой информации.

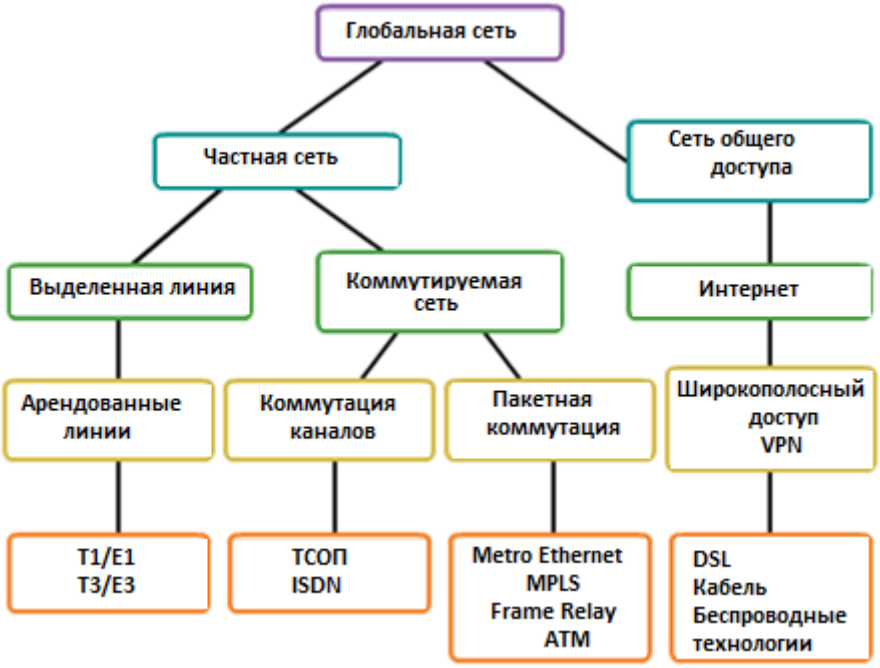


Рисунок 49 – Способы доступа к глобальной сети

Технологии частных глобальных сетей

Выделенные линии. Арендованные линии существуют с начала 50-х годов прошлого века, и по этой причине для них используются разные названия, такие, как арендуемый кабель, выделенная линия, последовательный канал, последовательная линия, канал «точка – точка» или каналы T1/E1 и T3/E3.

Термин «арендованная линия» подчеркивает тот факт, что организация ежемесячно платит интернет-провайдеру за использование линии. Арендованные линии доступны в различных модификациях. Как правило, их стоимость зависит от требуемой пропускной способности и расстояния между подключаемыми точками (рисунок 50).

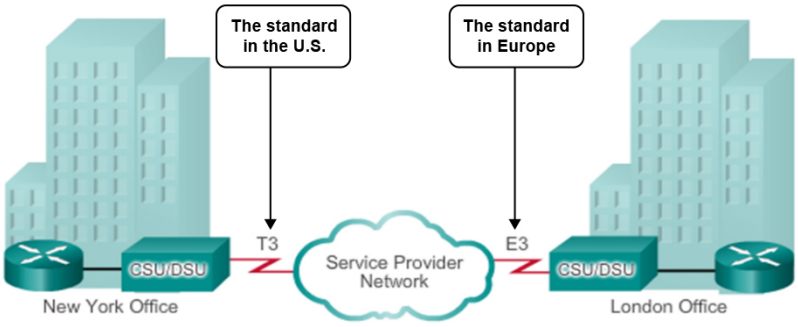


Рисунок 50 – Выделенные линии

В Северной Америке интернет-провайдеры используют систему Т-каналов для определения возможности передачи цифровых сигналов по последовательным каналам в медных кабельных линиях, тогда как в Европе используют систему Е-каналов, как показано на рисунке 49. Канал T1,

например, поддерживает скорость 1,544 Мбит/с, канал E1 – 2,048 Мбит/с, Т3 –43,7 Мбит/с, а E3 – 34,368 Мбит/с.

Преимущества арендованных линий:

– простота. Установка и техническое обслуживание каналов связи типа «точка – точка» требуют минимального опыта;

– качество. Если каналы связи типа «точка – точка» обладают требуемой пропускной способностью, они обычно обеспечивают высокое качество обслуживания. Выделенная пропускная способность избавляет от задержек и искажений при передаче данных между оконечными точками;

– доступность. Постоянная доступность является существенной для некоторых приложений, например, для электронной торговли. Каналы связи типа «точка – точка» обеспечивают постоянную выделенную линию, требуемую для VoIP или передачи видео по протоколу IP.

Недостатки арендованных линий:

– стоимость. Как правило, каналы «точка – точка» характеризуются самой высокой стоимостью доступа к сети WAN. Стоимость решений с использованием арендованных линий может стать значительной при их использовании для подключения множества площадок, находящихся на больших расстояниях. Кроме того, для каждой конечной точки необходим интерфейс на маршрутизаторе, что увеличивает стоимость оборудования;

– ограниченная гибкость. Трафик WAN изменчив, а арендованные линии обладают фиксированной пропускной способностью, поэтому пропускной способности линии часто бывает недостаточно. Для внесения каких-либо изменений в арендованную линию требуется, как правило, посещение объекта персоналом интернет-провайдера, чтобы настроить пропускную способность.

Коммутируемый доступ (Dial-Up). Устаревшая технология, основанная на использовании аналогового модема и обычной телефонной линии. Физические характеристики модема и аналоговой линии не позволяют получить скорость передачи сигнала выше 56 кбит/с.

К преимуществам модема и аналоговых линий относятся простота, доступность и низкая стоимость внедрения. Недостатками являются низкие скорости передачи данных и относительно длительное время установления соединения. С видео и голосовым трафиком из-за настолько низких скоростей передачи данных нормально работать оказывается невозможным.

Цифровая сеть с интеграцией служб (Integrated Services Digital Network, ISDN) является технологией коммутации каналов, которая позволяет местной телефонной линии сети передавать цифровые сигналы, что приводит к повышению пропускной способности коммутируемых подключений.

ISDN, кроме передачи аналоговых сигналов, передает также мультиплексированные цифровые сигналы с разделением по времени, что позволяет передавать по подканалам одного канала связи два или несколько сигналов, или битовых потоков. Кажется, что сигналы передаются одновременно, но физически они поступают в канал по очереди.

ISDN превращает местную телефонную линию в цифровую.

Главные особенности использования ISDN – это более высокая скорость передачи информации по сравнению с Dial-Up доступом, возможность передачи различного типа трафика (телевидение, телефония и т. д.). Скорость передачи данных составляет 64 кбит/с при использовании одного и 128 кбит/с, при использовании двух каналов связи. Популярность технологии снизилась из-за наличия варианта подключения к сети Интернет с использованием высокоскоростного канала DSL и других широкополосных технологий.

Технология второго уровня для множественного доступа (Frame Relay) – используется для соединения между собой локальных сетей предприятия. При этой технологии один интерфейс маршрутизатора можно использовать для подключения к нескольким филиалам. Frame Relay используется для передачи как голосового трафика, так и трафика со скоростью передачи данных до 4Мбит/с, причем некоторые провайдеры предлагают даже более высокие скорости. Требует дорогого дополнительного оборудования передачи/приема.

Технология асинхронного режима передачи (ATM) способна обеспечить передачу голоса, видео и данных по частным сетям и сетям общего доступа. Она создана на основе ячеистой, а не кадровой архитектуры. Ячейки ATM всегда имеют фиксированную длину 53 байт. Ячейка ATM содержит 5-байтовый заголовок, за которым следуют 48 байт полезной нагрузки ATM. Небольшие ячейки фиксированной длины удобны для переноса голосового и видео трафика, поскольку этот тип трафика зависит от задержек. В этом случае при передаче видео и голосового трафика нет необходимости в ожидании передачи более крупных пакетов данных.

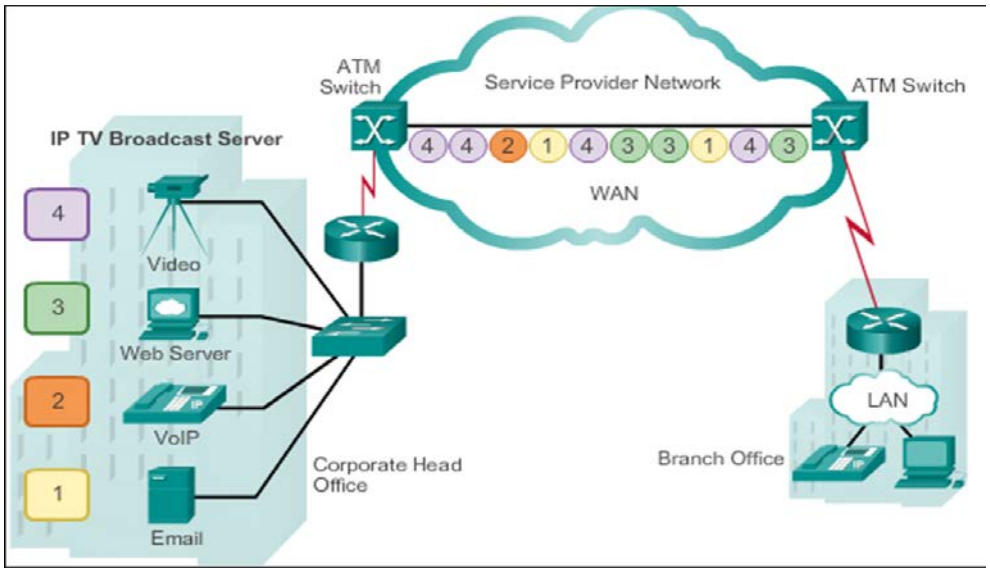


Рисунок 51 – Пример использования технологии ATM

53-байтовая ячейка ATM менее экономна, чем кадры и пакеты большего размера в Frame Relay. К тому же в ячейке ATM на каждые 48 байт полезной нагрузки приходится 5 байт служебной информации. Если в ячейке переносятся сегментированные пакеты сетевого уровня, то заголовок увеличивается, так как

коммутатору ATM необходимо повторно собирать пакеты в месте назначения. Для передачи аналогичного объема данных сетевого уровня пропускная способность типичного канала ATM должна быть, по крайней мере, на 20 % больше, чем у Frame Relay. Имеет значительную стоимость оборудования.

Технология Ethernet была разработана в качестве технологии доступа в сетях LAN. Однако в то время ее использование в качестве технологии доступа в глобальных сетях не имело смысла, поскольку максимальная поддерживаемая длина кабеля не превышала одного километра. Но новые стандарты Ethernet с использованием оптоволоконных кабелей сделали Ethernet оптимальным вариантом доступа к глобальной сети. Стандарт IEEE 1000BASE-LX, например, поддерживает оптоволоконные кабели длиной 5 км, а стандарт IEEE 1000BASE-ZX – кабели длиной до 100 км и более.

В настоящее время интернет-провайдеры предлагают сервис WAN на основе Ethernet с подключением по оптоволоконным кабелям. Сервис WAN на основе Ethernet может выступать под разными названиями, включая такие, как Metropolitan Ethernet (METROE), Ethernet over MPLS (EoMPLS) и Virtual Private LAN Service (VPLS).

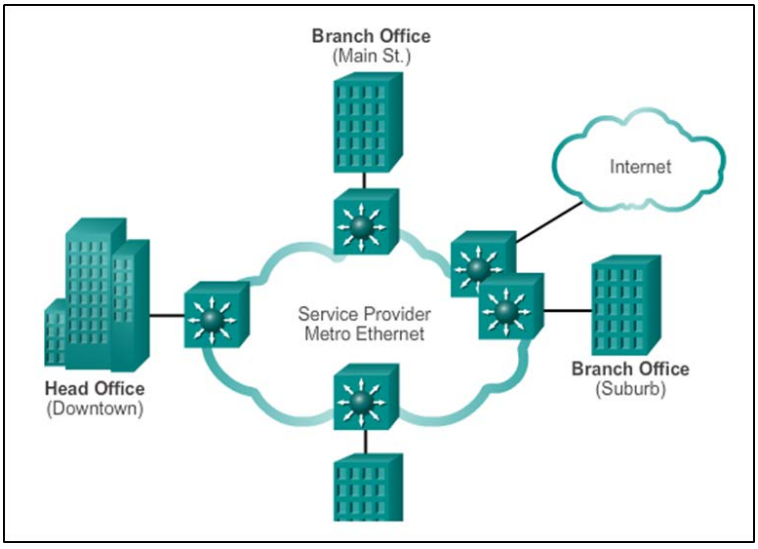


Рисунок 52 – Пример использования технологии Ethernet
в глобальных сетях

Преимущества технолгии Ethernet для организации глобальных сетей:

– *снижение затрат и объема администрирования*. WAN на основе Ethernet обеспечивает создание коммутируемой сети второго уровня с высокой пропускной способностью, способной управлять передачей данных, голоса и видео в рамках одной и той же инфраструктуры. Эта особенность позволяет повысить пропускную способность и устраняет потребность в дорогостоящих преобразованиях, необходимых для использования других технологий глобальной сети. Данная технология позволяет предприятиям экономично соединить друг с другом многочисленные узлы, находящиеся в пределах крупного города, и подключить их к сети Интернет;

– *простота интеграции с существующими сетями*. WAN на основе Ethernet легко подключить к существующим сетям LAN на основе Ethernet без больших затрат финансов и времени;

– *повышение производительности бизнеса*. Применение технологии WAN на основе Ethernet позволяет использовать приложения IP, повышающие производительность, которые сложно внедрить в сетях Frame Relay, например, связь по IP, VoIP и потоковое и широковещательное видео.

Популярность подключений с использованием технологии WAN на основе Ethernet выросла, и в настоящее время они практически вытеснили WAN на основе Frame Relay и ATM.

Технологии общедоступных глобальных сетей

Технология DSL (Digital Subscriber Line) – семейство цифровых абонентских линий, предназначенных для организации доступа по аналоговой телефонной сети, используя кабельный модем.

Эта технология (ADSL, VDSL, HDSL, ISDL, SDSL, SHDSL, RADSL под общим названием xDSL) обеспечивает высокоскоростное соединение до 50 Мбит/с (фактическая скорость до 2 Мбит/с) на расстояние до 5,46 км.

Преимущество технологий xDSL – возможность значительно увеличить скорость передачи данных по телефонным проводам без модернизации абонентской телефонной линии. Пользователь получает доступ в сеть Интернет с сохранением обычной работы телефонной связи.

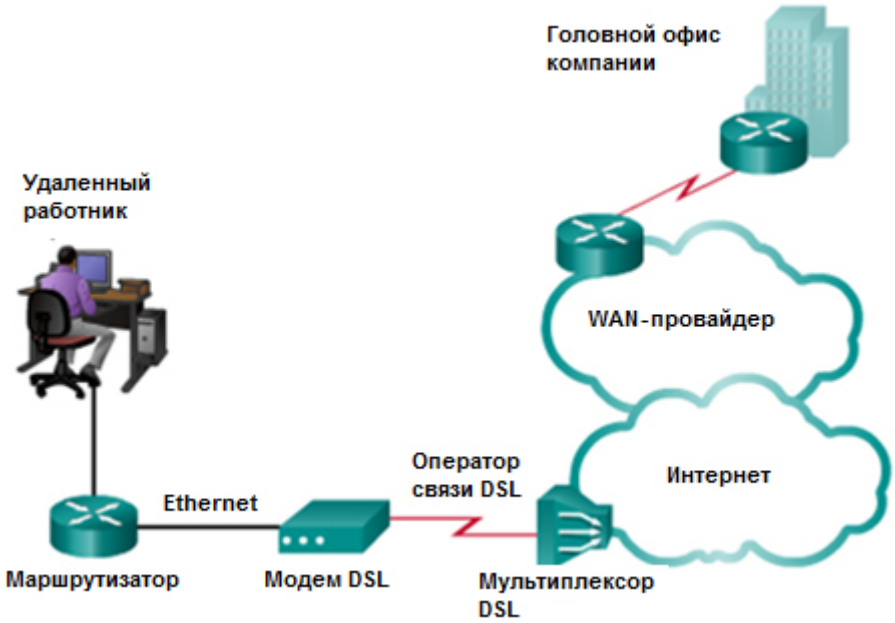


Рисунок 53 – Пример использования технологии DSL

Модем DSL преобразует сигнал Ethernet, поступающий от устройства пользователя, в сигнал DSL, который передается центральному офису.

С помощью мультиплексора доступа цифровых абонентских линий DSALM, установленного у провайдера, несколько абонентских линий DSL

мультиплексируются в единый высокоскоростной канал. Для достижения высоких скоростей передачи данных в современных технологиях DSL применяются сложные методы кодирования и модуляции.

Технология Data Over Cable Service Interface Specifications (DOCSIS) – стандарт передачи данных по коаксиальному (телевизионному) кабелю. Этот стандарт предусматривает передачу данных абоненту по сети кабельного телевидения с максимальной скоростью до 42 Мбит/с и получение данных от абонента со скоростью до 10,24 Мбит/с.

Коаксиальные кабели широко используются в городах для подключения к телевизионному вещанию. Доступ к сети предоставляют многие операторы кабельного телевидения. В этом случае предоставляется более высокая пропускная способность, чем при использовании телефонной местной линии.

Кабельные модемы обеспечивают постоянное подключение и простоту установки. Абонент подключает компьютер или маршрутизатор LAN к кабельному модему, который преобразует цифровые сигналы в аналоговые, используемые для передачи данных по сети кабельного телевидения. Все местные абоненты совместно используют пропускную способность кабельного соединения. По мере увеличения числа пользователей, пользующихся этой услугой, доступная пропускная способность может оказаться ниже ожидаемого показателя.

В беспроводных технологиях для отправки и приема данных используются нелицензированные полосы радиочастот. Нелицензированные полосы доступны всем, кто использует устройство, имеющее беспроводный маршрутизатор и поддерживающее беспроводную технологию.

Можно выделить следующие технологии беспроводного широкополосного доступа:

Технология Wi-Fi. Подробно рассматривается в разделе беспроводные сети.

Технология WiMAX. Технология WiMAX предлагает высокоскоростной широкополосный сервис с беспроводным доступом и обеспечивает охват, сравнимый с охватом сети мобильной телефонной связи и не идущий ни в какое сравнение с охватом, предоставляемым посредством точек доступа технологии Wi-Fi. Сеть WiMAX функционирует подобно сети Wi-Fi, но на более высоких скоростях, на больших расстояниях и для большего числа пользователей. Она использует сеть вышек WiMAX, подобных вышкам сети мобильной телефонной связи. Для получения доступа к сети WiMAX абонентам требуется подписаться на услуги интернет-провайдера, чья вышка WiMAX находится в пределах 30 км от местоположения абонента. Также им требуются определенный тип приемника WiMAX и специальный код шифрования, чтобы получить доступ к базовой станции.

Доступ через сотовую связь. Используются технологии 3G, 4G, 5G.

Спутниковый доступ. Обычно используется там, где недоступен доступ по каналу DSL или кабельной линии. Кабельная линия и канал DSL имеют более высокие скорости загрузки, но спутниковые системы приблизительно в

10 раз быстрее, чем аналоговый модем. Для получения доступа к спутниковым интернет-сервисам абонентам требуется спутниковая антенна, два модема (восходящий и нисходящий канал) и коаксиальные кабели, соединяющие антенну и модем.

Для соединения удаленных сетей или пользователей через другую общедоступную сеть (например, Интернет) используется технология *виртуальных частных сетей* **(**Virtual Private Network, VPN). VPN – обобщенное название технологий, позволяющих обеспечить одно или несколько сетевых соединений (логическую сеть) *поверх другой сети*. При этом между связываемыми сетями в общедоступной сети создается туннель.

Суть туннелирования состоит в том, чтобы «упаковать» передаваемую порцию данных вместе со служебными полями в новый «конверт» и передать его, обеспечив по возможности, конфиденциальность и целостность всей инфрмации. В процессе инкапсуляции (туннелирования) принимают участие следующие типы протоколов:

– транспортируемый протокол;

– несущий протокол;

– протокол инкапсуляции.

Протокол транзитной сети является *несущим*, а протокол объединяемых сетей – *транспортируемым*. Пакеты транспортируемого протокола помещаются в поле данных пакетов *несущего* протокола с помощью протокола инкапсуляции. «Пакеты-пассажиры» не обрабатываются при транспортировке по транзитной сети. Инкапсуляцию выполняет пограничное устройство (маршрутизатор или шлюз), которое находится на границе между исходной и транзитной сетями. Извлечение пакетов *транспортируемого* протокола из несущих пакетов выполняет второе пограничное устройство, расположенное на границе между транзитной сетью и сетью назначения. Пограничные устройства указывают в несущих пакетах свои адреса, а не адреса узлов в сети назначения.

Таким образом, общий порядок инкапсуляции в случае использования site-to-site VPN следующий: пользователь отправляет обычный пакет, пакет доходит до устройства, на котором настроен туннель, устройство заворачивает этот пакет в поле data протокола инкапсуляции, который, в свою очередь, заворачивается в поле data несущего протокола. Это позволяет использовать независимую адресацию внутри туннеля и снаружи туннеля. При этом в несущем протоколе используется одна адресация (например, публичные IP-адреса), а в транспортируемом протоколе могут использоваться частные адреса связываемых сетей, что не мешает маршрутизации пакета через Интернет (так как маршрутизация осуществляется для внешнего, несущего протокола).

Когда целевое устройство получает такой пакет, оно разворачивает его, отбрасывая из него заголовок протокола инкапсуляции, а потом заголовок транспортируемого протокола, после чего данные передаются получателю. На рисунке 54 приведена классификация различных типов VPN.

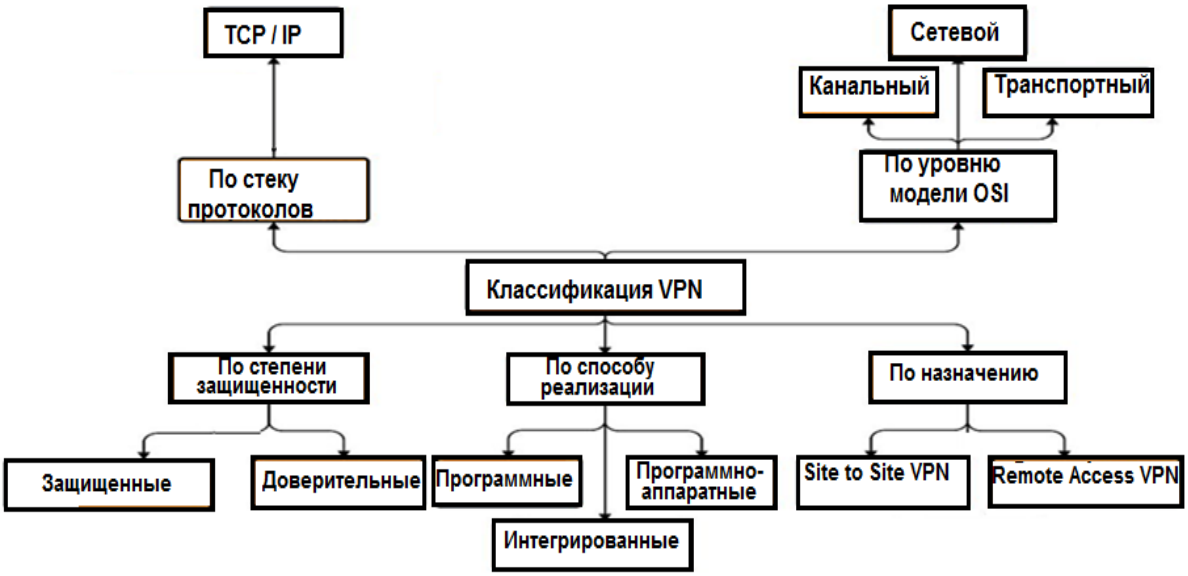


Рисунок 54 – Классификация VPN

Классификация методов:

1 *По степени защищенности используемой среды*:

а) защищенные – наиболее распространенный вариант виртуальных частных сетей, с помощью которого можно создать надежную и защищенную сеть на основе ненадежной, как правило, Интернета. Примером защищенных VPN являются: IPSec, OpenVPN и PPTP;

б) доверительные и незащищенные используются в случаях, когда передающую среду можно считать надежной и необходимо решить лишь задачу создания туннелей. Примерами подобных решений VPN являются: Multi-protocol label switching (MPLS) и L2TP (Layer 2 Tunnelling Protocol) (точнее эти протоколы перекладывают задачу обеспечения безопасности на другие протоколы, например, L2TP, как правило, используется в паре с IPSec). Среди незащищенных протоколов можно выделить протокол GRE (Generic Routing Encapsulation).

2 *По способу реализации*:

а) в виде специального программно-аппаратного устройства, например, маршрутизатора. Такая реализация обеспечивает высокую производительность и, как правило, высокую степень защищенности;

б) в виде программного решения. Используется персональный компьютер со специальным программным обеспечением, обеспечивающим функциональность VPN;

в) интегрированное решение. Кроме организации VPN, дополнительно решаются также задачи фильтрации сетевого трафика, организации сетевого экрана и обеспечения качества обслуживания и т. д.

3 *По назначению*:

а) **Site-to-Site VPN**. Используют для объединения в единую защищенную сеть нескольких распределенных филиалов одной организации,

обменивающихся данными по открытым каналам связи. Как показано на рисунке 55, с двух сторон соединения имеются VPN-шлюзы (VPN-серверы);

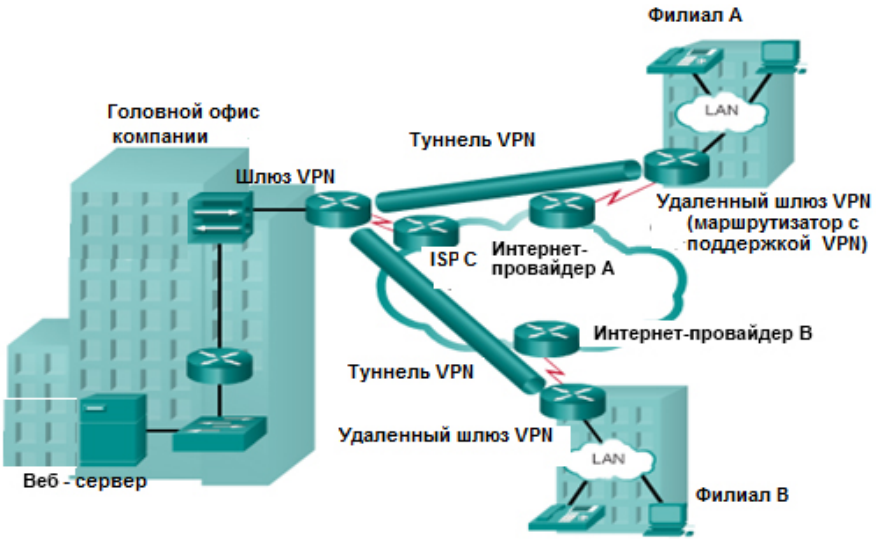


Рисунок 55 – Схема организации Site-to-Site VPN

б) **Remote Access VPN** используют для создания защищенного канала между сегментом корпоративной сети (центральным офисом или филиалом) и одиночным пользователем.

На рисунке 56 для доступа к VPN-серверу офиса на удаленных узлах должны работать VPN-клиенты, а в головном офисе должен быть установлен VPN-сервер. Пользователь, работая удаленно, подключается к корпоративным ресурсам с домашнего компьютера, корпоративного ноутбука, смартфона.

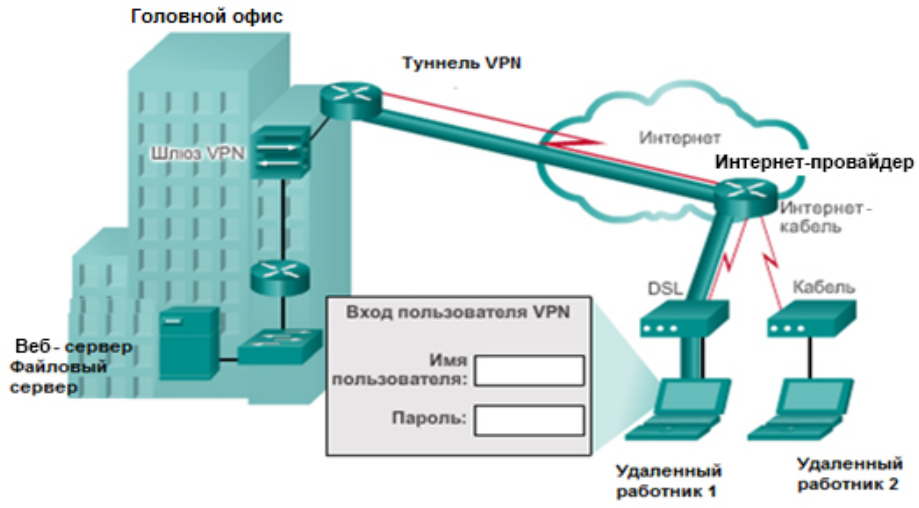


Рисунок 56 – Схема организации Remote Access VPN

4 *По типу стека протоколов*. На сегодняшний день самым распространенным стеком является стек TCP/IP.

В зависимости от уровня сетевой модели ISO/OSI VPN-туннель может быть организован на канальном (PPP, PPTP, L2TP, PPPoE, MPLS), сетевом

(GRE, IPSec), транспортном и представительном (SSL VPN) уровнях. Часто в организации туннеля может быть одновременно задействовано несколько уровней.

Типы технологий VPN

Наиболее популярными типами технологий VPN в настоящее время являются PPTP, L2TP, IPsec, SSL VPN (наиболее популярная реализация OpenVPN).

1 PPTP (Point-to-Point Tunneling Protocol) – туннельный протокол типа «точка – точка», позволяющий устанавливать защищенное соединение за счет создания специального туннеля в незащищенной сети. Был разработан компанией Microsoft и включен в операционную систему. PPTP расширяет возможности PPP-протокола, расположенного на канальном уровне. PPTP позволяет инкапсулировать пакеты PPP в пакеты протокола Internet Protocol (IP) и передавать их по сетям IP (в том числе и по сети Интернет).

PPTP обеспечивает безопасную передачу данных от удаленного клиента к VPN-серверу предприятия путем создания в сети TCP/IP частной виртуальной сети типа Remote Access VPN. PPTP может также использоваться для организации туннеля между двумя локальными сетями типа Site-to-Site VPN.

PPTP работает, устанавливая обычную PPP-сессию с противоположной стороной с помощью протокола GRE. Второе соединение на TCP порту 1723 используется для инициации и управления GRE-соединением. Для защиты данных PPTP-трафика может быть использован протокол MPPE (Microsoft Point-to-Point Encryption), для аутентификации – MSCHAPv2 и EAP-TLS.

На рисунке 57 представлена схема работы протокола PPTP.

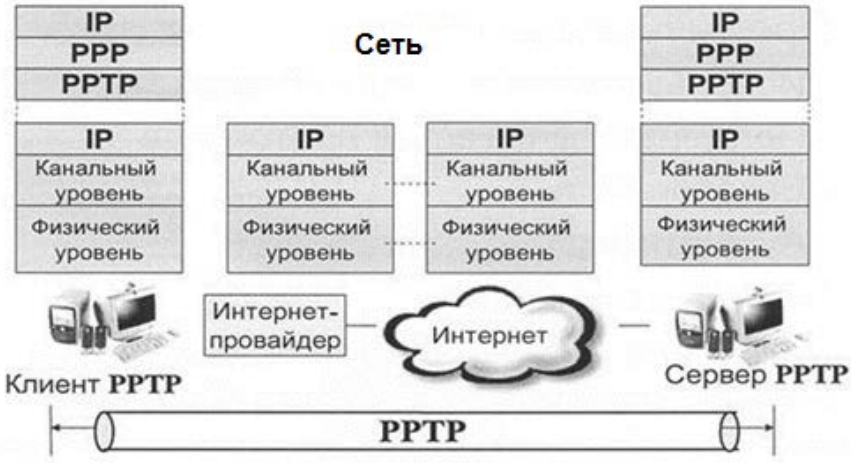


Рисунок 57 – Схема работы протокола PPTP

На рисунке 58 приведена структура пакета протокола. Исходный IP-пакет запаковывается в пакет протокола PPP, который в свою очередь запаковывается в туннельный протокол GRE, после чего сформированный пакет повторно запаковывается в IP-пакет (добавляется заголовок доставки).

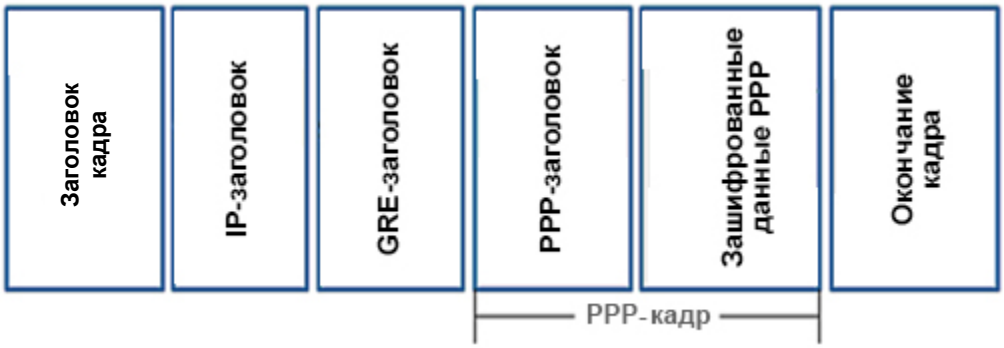


Рисунок 58 – Кадр протокола PPTP

GRE не работает с NAT, поэтому PPTP для работы с NAT необходим дополнительный модуль PPTP NAT helper.

2 L2TP (Layer 2 Tunnelling Protocol) включает в себя протоколы Layer 2 Forwarding (L2F) от компании Cisco и Point-to-Point Tunneling Protocol (PPTP) от Microsoft. В VPN-сетях позволяет создавать туннели с необходимыми приоритетами доступа, однако из-за отсутствия механизмов шифрования и аутентификации является небезопасным протоколом и используется совместно с шифрующим протоколом IPSec (IP-security). Структура кадра протокола приведена на рисунке 59.

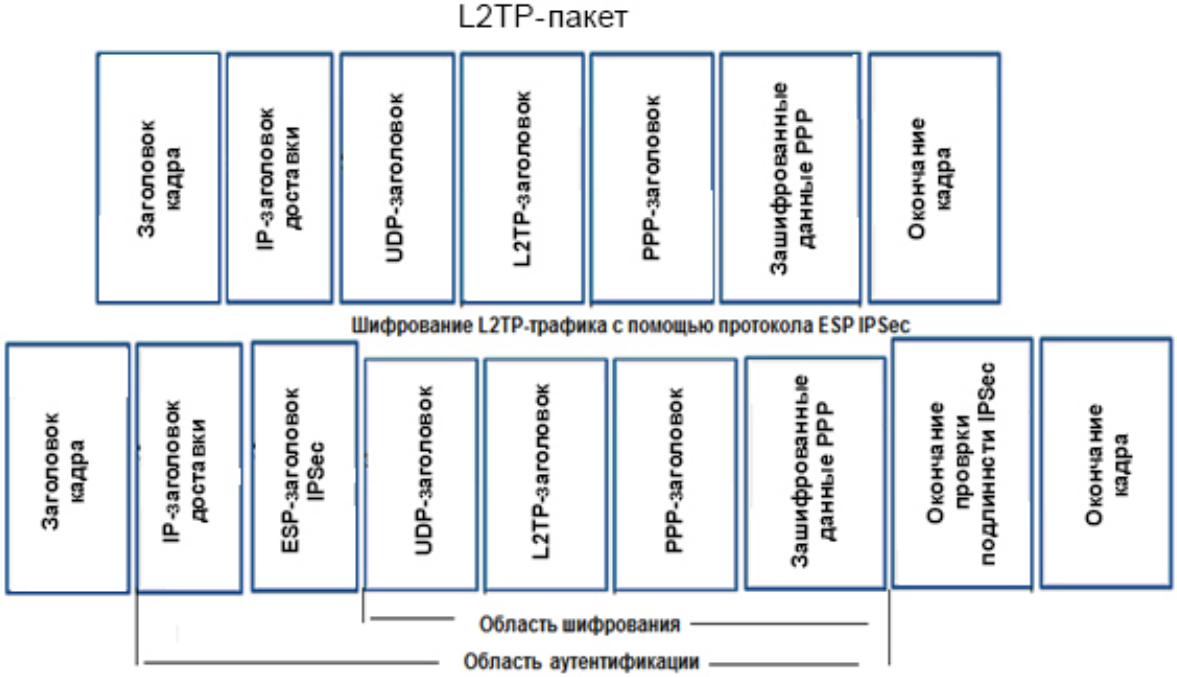


Рисунок 59 – Структура кадра протокола L2TP /IPSec

Главным плюсом L2TP перед PPTP считается работа через NAT. Это достигается тем, что на заключительном этапе L2TP-пакет помещается в UDP-пакет, в заголовке которого имеются порты, что позволяет при переходе через NAT настроить проброс портов. L2TP пропускает данные и управляется

через один порт UDP (User Datagram Protocol), а протокол PPTP отправляет пользовательскую информацию через GRE-туннель, а управляющую – через TCP-соединение. Кроме того, в случае использования дополнительного, стороннего протокола IPSec, L2TP является более надежным в плане шифрования. Встроен во все современные операционные системы.

Преимущества L2TP протокола перед PPTP:

– не блокируется брандмауэрами, работает через NAT;
– обеспечивает более стабильное соединение;
– легче в настройке и работе;
– безопаснее в случае использования дополнительных протоколов.

3 Протокол IPSec (IP Security) – *стандарт*, который определяет способ настройки сети VPN в защищенном режиме с помощью протокола IP. IPSec не жестко связан с конкретными методами шифрования и аутентификации, алгоритмами обеспечения безопасности или технологией обмена ключами – возможно включение новых алгоритмов.

Механизм IPSec решает следующие задачи:

– аутентификацию пользователей или компьютеров при инициализации защищенного канала;
– шифрование и аутентификацию данных, передаваемых между конечными точками защищенного канала;
– автоматическое снабжение конечных точек канала секретными ключами, необходимыми для работы протоколов аутентификации и шифрования данных.

IPSec включает в себя три протокола, каждый со своими функциями:

1) ESP (Encapsulating Security Payload) – безопасная инкапсуляция полезной нагрузки) занимается непосредственно шифрованием данных, а также может обеспечивать аутентификацию источника и проверку целостности данных;

2) AH (Authentication Header – заголовок аутентификации) отвечает за аутентификацию источника и обеспечивает целостность путем проверки того, что ни один бит в защищаемой части пакета не был изменен во время передачи, и последующую проверку подлинности передаваемых данных.

Однако использование AH может вызвать проблемы при прохождении пакета через NAT-устройство. Так как протокол AH выполняет проверку целостности всего пакета, включая заголовок доставки, а при переходе через NAT меняется IP-адрес в этом заголовке, то на приемной стороне контрольная сумма такого пакета не будет соответствовать контрольной первоначально рассчитанной контрольной сумме в пакете. Также стоит отметить, что AH разрабатывался только для обеспечения аутентификации и проверки целостности. Он не гарантирует конфиденциальность путем шифрования содержимого пакета;

3) IKE (Internet Key Exchange protocol – протокол обмена ключами) – протокол, используемый для первичной настройки соединения, взаимной аутентификации конечными узлами друг друга и обмена секретными ключами.

Используется для формирования безопасного вспомогательного канала между двумя узлами, называемого IKE SECURITY ASSOCIATION (IKE SA);

4) SA (Security Association) представляет собой набор параметров защищенного соединения (например, алгоритм шифрования, хеш-функцию ключ шифрования), который может использоваться обеими сторонами соединения. У каждого соединения есть ассоциированный с ним SA. SA создаются парами, так как каждая SA – это однонаправленное соединение, а данные необходимо передавать в двух направлениях. Полученные пары SA хранятся на каждом узле.

Так как каждый узел способен устанавливать несколько туннелей с другими узлами, каждый SA имеет уникальный номер, позволяющий определить, к какому узлу он относится. Этот номер называется SPI (Security Parameter Index) или индекс параметра безопасности.

SA храняться в базе данных (БД) **SAD** (Security Association Database).

Каждый узел IPSec также имеет вторую БД – **SPD** (Security Policy Database), содержащую настроенную политики безопасности узла. SPD служит для соотнесения приходящих IP-пакетов с правилами обработки для них. Большинство VPN-решений разрешают создание нескольких политик с комбинациями подходящих алгоритмов для каждого узла, с которым нужно установить соединение.

Работа протокола IKE выполняется в две фазы.

Первая фаза IKE может проходить в одном из двух режимов.

Основной режим состоит из трех двусторонних обменов между отправителем и получателем:

– во время первого обмена согласуются алгоритмы и хеш-функции, которые будут использоваться для защиты IKE соединения, посредством сопоставления IKE SA каждого узла;

– используя алгоритм Диффи – Хеллмана, стороны обмениваются общим секретным ключом. Также узлы проверяют идентификацию друг друга путем передачи и подтверждения последовательности псевдослучайных чисел;

– проверяется идентичность противоположной стороны.

В результате выполнения основного режима создается безопасный вспомогательный туннель для последующего ISAKMP – обмена (этот протокол определяет порядок действий для аутентификации соединения узлов, создания и управления SA, генерации ключей.

Агрессивный режим. Этот режим обходится меньшим числом обменов и, соответственно, числом пакетов. В первом сообщении помещается практически вся нужная для установления IKE SA информация: открытый ключ Диффи-Хеллмана, идентификатор пакета. Получатель посылает в ответ всю информацию, необходимую для завершения обмена. Первому узлу требуется только подтвердить соединение.

С точки зрения безопасности агрессивный режим слабее, так как участники начинают обмениваться информацией до установления безопасного канала, поэтому возможен несанкционированный перехват данных. Однако

этот режим быстрее, чем основной. По стандарту IKE любая реализация обязана поддерживать основной режим, а агрессивный режим желательно поддерживать.

На второй фазе уже доверяющие друг другу участники через вспомогательный туннель договариваются о том, как строить основной туннель для данных. Согласуется общая политика IPSec, стороны получают общие секретные ключи для алгоритмов протоколов IPSec (AH или ESP), устанавливаются IPSec SA.

После установки основного туннеля вспомогательный ISAKMP-туннель остается работоспособным и используется для обновления SA основного. Дело в том, что ключи, выбираемые для шифрования информации в IPSec-туннеле, имеют некоторое «время жизни» (может выражаться как в количестве байт проходящих через туннель, так и в секундах – что первое достигнет порогового значения), по истечение которого должны быть заменены. По умолчанию lifetime IPSec SA составляет 4 608 000 Кбайт/3600 с.

Участники, получив основной шифрованный туннель с параметрами, которые их всех устраивают, направляют туда потоки данных, подлежащие шифрованию. Периодически, в соответствии с настроенным lifetime, обновляются ключи шифрования для основного туннеля: участники вновь связываются по ISAKMP-туннелю, проходят вторую фазу и устанавливают новые SA.

В работе протоколов IPSec можно выделить пять этапов.

Первый этап начинается с создания на каждом узле, поддерживающем стандарт IPSec, политики безопасности. На этом этапе определяется, какой трафик подлежит шифрованию, какие функции и алгоритмы могут быть использованы.

Второй этап является первой фазой IKE. Его цель – организовать безопасный канал между сторонами для второй фазы IKE. На втором этапе выполняются:

– аутентификация и защита идентификационной информации узлов;

– проверка соответствий политик IKE SA-узлов для безопасного обмена ключами;

– обмен ключами по алгоритму Диффи – Хеллмана, в результате которого у каждого узла будет общий секретный ключ;

– создание безопасного канала для второй фазы IKE.

Третий этап является второй фазой IKE. Его задачей является создание IPSec-туннеля. На третьем этапе выполняются следующие функции:

– согласуются параметры IPSec SA по защищаемому IKE SA-каналу, созданному в первой фазе IKE;

– устанавливается IPStc SA;

– периодически осуществляется пересмотр ipsec sa, чтобы убедиться в ее безопасности;

– (опционально) выполняется дополнительный обмен Диффи – Хеллмана.

На четвертом этапе, после создания IPSec SA, начинается обмен информацией между узлами через IPSec-туннель, используются протоколы и параметры, установленные в SA.

На пятом этапе прекращают действовать текущие IPSec SA. Это происходит при их удалении или по истечении времени жизни, значение которого содержится в SAD на каждом узле. Если требуется продолжить передачу, запускается вторая фаза IKE (если требуется, то и первая фаза), и далее создаются новые IPSec SA.

На рисунке 60 приведен стек протоколов, используемых стандарте IPSec.

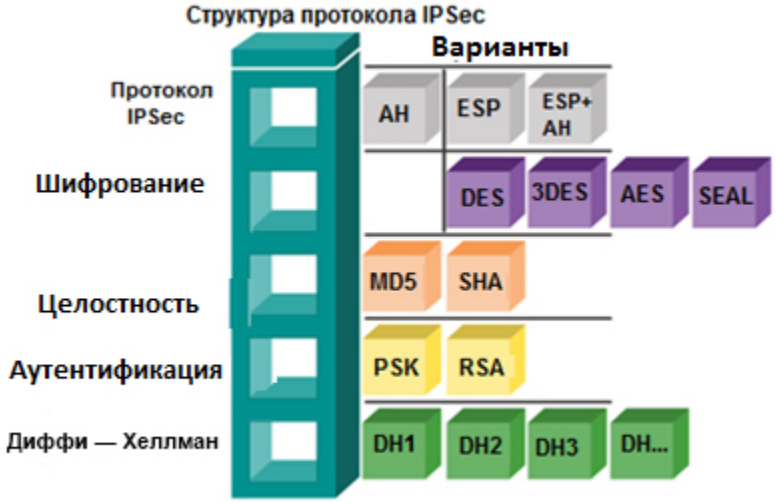


Рисунок 60 – Стек протоколов IPSec

Протоколы AH и ESP могут работать в двух режимах – **в транспортном режиме и режиме туннелирования** (рисунок 61). При работе в транспортном режиме IPSec работает только с информацией транспортного уровня, т. е. шифруется только поле данных пакета, содержащего протоколы TCP/UDP (заголовок IP-пакета не изменяется (не шифруется)). Транспортный режим, как правило, используется для установления соединения между хостами.

В режиме туннелирования шифруется весь IP-пакет, включая заголовок сетевого уровня. Для того чтобы его можно было передать по сети, он помещается в другой IP-пакет. По существу, это защищенный IP-туннель. Туннельный режим может использоваться для подключения удаленных компьютеров к виртуальной частной сети (схема подключения «хост – сеть») или для организации безопасной передачи данных через открытые каналы связи (например, сеть Интернет) между шлюзами для объединения разных частей виртуальной частной сети (схема подключения «сеть – сеть»).

Режимы IPSec не являются взаимоисключающими. На одном и том же узле некоторые SA могут использовать транспортный режим, а другие – туннельный.

На фазе аутентификации вычисляется контрольная сумма ICV (Integrity Check Value) пакета. При этом предполагается, что оба узла знают секретный ключ, который позволяет получателю вычислить ICV и сравнить с результатом, присланным отправителем. Если сравнение ICV прошло успешно, считается, что отправитель пакета аутентифицирован.

Рисунок 61 – Туннельный и транспортный режимы работы протокола AH

Для туннельного режима AH при выполнении расчета в контрольную сумму ICV включаются следующие компоненты:

– все поля внешнего заголовка IP, за исключением некоторых полей в заголовке IP, которые могут быть изменены при передаче. Эти поля, значения которых для расчета ICV равняются нулю, могут быть частью службы (Type of Service, TOS), флагами, смещением фрагмента, временем жизни (TTL), а также заголовком контрольной суммы;

– все поля AH;

– исходный IP-пакет.

Как видно из рисунка 61, режим туннелирования AH защищает весь исходный IP-пакет за счет дополнительного внешнего заголовка доставки, который в режиме транспорта AH не используется:

В режиме **транспорта ESP** аутентифицирует не весь пакет, а обеспечивает защиту только полезных данных IP. Заголовок ESP в режиме транспорта ESP добавляется в IP-пакет сразу после заголовка IP, а окончание ESP (ESP Trailer), соответственно, добавляется после данных.

Режим транспорта ESP шифрует следующие части пакета:

– полезные данные IP;

– ESP Trailer.

Алгоритм шифрования, который использует режим шифрования цепочки блоков (Cipher Block Chaining, CBC), имеет незашифрованное поле между заголовком ESP и полезной нагрузкой. Это поле называется вектором инициализации IV (Initialization Vector) для расчета CBC, которое выполняется на получателе. Так как это поле используется для начала процесса

расшифровки, оно не может быть зашифрованным. Несмотря на то что у злоумышленника есть возможность просмотра IV, он никак не сможет расшифровать зашифрованную часть пакета без ключа шифрования. Для предотвращения изменения вектора инициализации злоумышленниками он охраняется контрольной суммой ICV.

В этом случае ICV выполняет следующие расчеты:

– все поля в заголовке ESP;

– полезные данные, включая открытый текст IV;

– все поля в ESP Trailer, за исключением поля данных проверки подлинности.

Туннельный режим ESP инкапсулирует весь исходный IP-пакет в заголовок нового IP, заголовок ESP и ESP Trailer. Для того чтобы указать, что в заголовке IP присутствует ESP, устанавливается идентификатор протокола IP 50, причем исходный заголовок IP и полезные данные остаются без изменений. Как и в случае с туннельным режимом AH, внешний IP-заголовок базируется на конфигурации туннеля IPSec. В случае использования туннельного режима ESP область аутентификации IP-пакета показывает, где была поставлена подпись, удостоверяющая его целостность и подлинность, а зашифрованная часть показывает, что информация является защищенной и конфиденциальной. Исходный заголовок помещается после заголовка ESP. После того как зашифрованная часть инкапсулируется в новый туннельный заголовок, который не зашифровывается, осуществляется передача IP-пакета. При отправке через общедоступную сеть такой пакет маршрутизируется на IP-адрес шлюза принимающей сети, а уже шлюз расшифровывает пакет и отбрасывает заголовок ESP с использованием исходного заголовка IP для последующей маршрутизации пакета на компьютер, находящийся во внутренней сети.

Как показано на рисунке 62, режим туннелирования ESP шифрует следующие части пакета:

– исходный IP-пакет;

– ESP Trailer.

Для туннельного режима ESP расчет ICV производится следующим образом:

– все поля в заголовке ESP;

– исходный IP-пакет, включая открытый текст IV;

– все поля заголовка ESP, за исключением поля данных проверки подлинности.

Протокол IPSec работает на сетевом уровне модели OSI, номера портов протоколов зашифрованы внутри пакета и недоступны, поэтому при переходе через NAT нельзя настроить проброс портов. Для решения этой проблемы IETF определила способ инкапсуляции ESP в UDP, получивший название NAT-T (NAT Traversal).

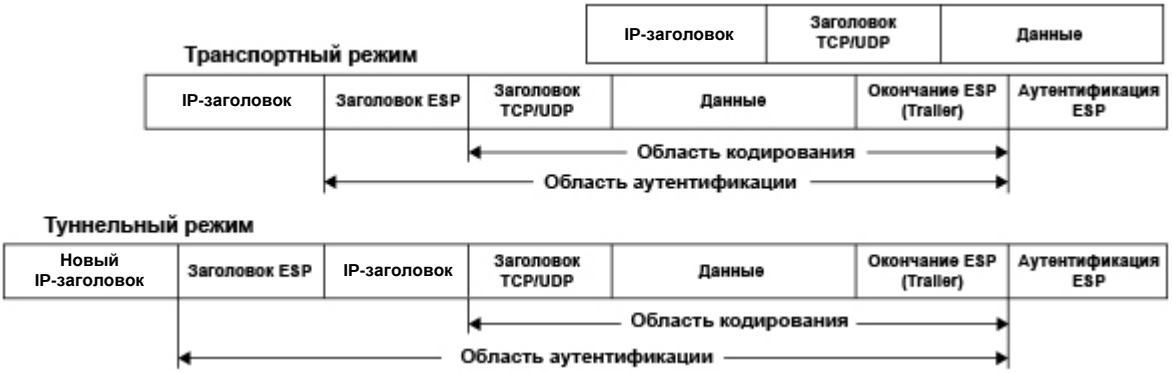


Рисунок 62 – Туннельный и транспортный режим протокола ESP

Протокол NAT Traversal поднимает пакеты IPSec вверх до транспортного уровня и инкапсулирует их в пакеты UDP, которые NAT корректно пересылает. Для этого NAT-T помещает дополнительный заголовок UDP перед пакетом IPSec, чтобы он во всей сети обрабатывался как обычный пакет UDP и хост получателя не проводил никаких проверок целостности. После поступления пакета по месту назначения заголовок UDP удаляется, и пакет данных продолжает свой дальнейший путь как инкапсулированный пакет IPSec. Таким образом, с помощью механизма NAT-T возможно установление связи между клиентами IPSec в защищенных сетях с общедоступными хостами IPSec через межсетевые экраны.

Следует отметить, что основные AH-, ESP-протоколы могут работать по схеме: только AH, только ESP и совместно AH и ESP.

Недостатки IPSec: во-первых, для неподготовленного пользователя он очень сложен в настройке, что может снизить уровень защиты в том случае, если настройки протокола сделаны неправильно; во-вторых, он гораздо требовательнее к вычислительным ресурсам. Этот недостаток может быть устранен при реализации IPSec на специализированных аппаратных устройствах (маршрутизаторах).

4 SSL (Secure Sockets Layer) и **TLS (Transport Layer Security) VPN**, как видно из названия, представляют целый класс решений, опирающихся на соответствующие протоколы SSL и TLS. Широкая распространенность этих протоколов способствовала их детальному изучению и последовательному выявлению все новых и новых уязвимостей как в архитектуре, так и в конкретных реализациях. Аббревиатура TLS (Transport Layer Security) появилась в качестве замены обозначения SSL (Secure Sockets Layer) после того, как протокол окончательно стал интернет-стандартом. Такая замена вызвана юридическими аспектами, так как спецификация SSL изначально принадлежала компании Netscape. И сейчас нередко названия SSL и TLS продолжают использовать в качестве синонимов, но каноническим именем является TLS, а протоколы семейства SSL окончательно устарели. SSL 3.0 был упразднен в июне 2015 года, актуальной на текущий момент является версия TLS 1.3.

Достоинством SSL/TLS VPN является то, что из-за широкого применения этих протоколов в сети Интернет они беспрепятственно пропускаются практически всеми публичными сетями. Недостаток – не слишком высокая производительность на практике и сложность в настройке, а также необходимость установки дополнительного ПО.

Протокол SSL/TLS находится на представительном уровне, как показано на рисунке 63.

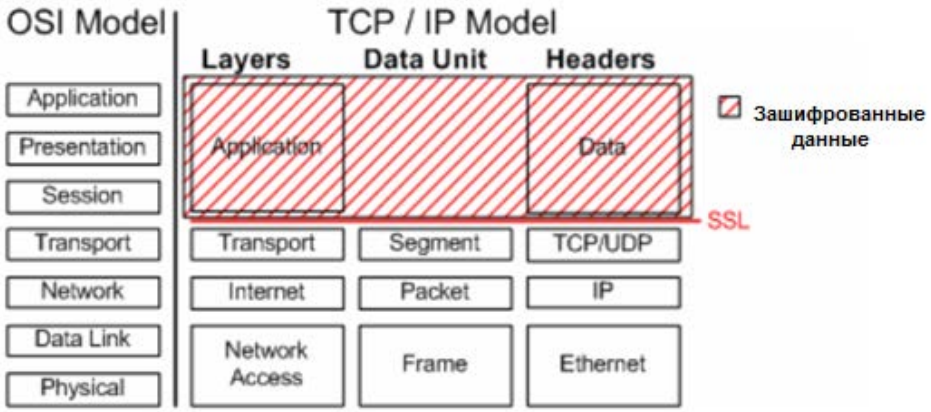


Рисунок 63 – Протокол SSL/TLS и OSI-модель

Популярными реализациями SSL/TLS VPN являются OpenVPN (SSL 3.0/TLS 1.3). OpenVPN в силу своей открытости имеет множество реализаций практически для всех платформ и к тому же на данный момент считается одним из надежных вариантов VPN.

ПО OpenVPN передает данные по сети с помощью протоколов UDP или TCP. Для OpenVPN можно выбрать произвольный порт, что позволяет преодолевать ограничения файервола, через который осуществляется доступ из локальной сети в Интернет (если такие ограничения установлены).

9 БЕСПРОВОДНЫЕ СЕТИ

В настоящее время беспроводные сети получают все большее распространение. При этом можно выделить следующие типы беспроводных сетей:

– беспроводная персональная сеть (WPAN – пикосети). Используемые технологии: Bluetooth, Wi-Fi Direct;

– беспроводные локальные сети LAN (WLAN). В сетях такого типа, как правило, используется технология Wi-Fi;

– глобальные сети (WWAN). В глобальных сетях используются технологии: WiMAX, сотовый беспроводной доступ 2G, 3G, 4G, 5G (тестируется), спутниковый беспроводной доступ.

Все беспроводные устройства работают в диапазоне радиоволн электромагнитного спектра. За регулирование выделения радиочастотного (РЧ) спектра отвечает Международный союз электросвязи. Для различных целей

предусмотрены частотные диапазоны, которые называют полосами. Некоторые полосы в электромагнитном спектре жестко регулируются и используются в таких областях, как контроль трафика и сети связи аварийно-спасательных служб. Другие полосы не подлежат лицензированию (например, промышленные, научные и медицинские частотные диапазоны, а также частотные диапазоны национальной информационной инфраструктуры).

Беспроводная связь осуществляется в диапазоне радиоволн (т. е. 3–300 ГГц) электромагнитного спектра.

Так, например, стандарт для беспроводных локальных сетей WLAN IEEE 802.11 выделяет три частоты работы в не лицензируемых диапазонах частот:

– 2,4 ГГц (УВЧ);

– 5 ГГц (СВЧ);

– 60 ГГц (КВЧ).

Локальные беспроводные сети, технология Wi-Fi. В 1999 году появились пионеры беспроводных технологий – 3Com, Aironet (ныне Cisco), Harris Semiconductor, Lucent, Nokia и Symbol Technologies основали альянс **Wireless Ethernet Compatibility Alliance (WECA)** и зарегистрировали свою новую технологию под маркой **Wi-Fi**. Альянс разрабатывает семейство стандартов Wi-Fi-сетей IEEE 802.11 и представляет собой промышленную группу, в которую входят все основные производители беспроводного оборудования Wi-Fi. Их задачей является тестирование и гарантия возможности совместной работы беспроводных сетевых устройств всех составляющих членство компаний, а также продвижение сетей 802.11 как всемирного стандарта для беспроводных сетей. На рисунке 64 приведены основные характеристики беспроводных сетей стандарта 802.11.

IEEE Standard	Maximum Speed	Frequency	Backwards Compatible
802.11	2 Mb/s	2.4 GHz	—
802.11a	54 Mb/s	5 GHz	—
802.11b	11 Mb/s	2.4 GHz	—
802.11g	54 Mb/s	2.4 GHz	802.11b
802.11n	600 Mb/s	2.4 GHz and 5 GHz	802.11a/b/g
802.11ac	1.3 Gb/s (1300 Mb/s)	5 GHz	802.11a/n
802.11ad	7 Gb/s (7000 Mb/s)	2.4 GHz, 5 GHz, and 60 GHz	802.11a/b/g/n/ac

Рисунок 64 – Стандарты беспроводных сетей

Рассмотрим беспроводные сети стандарта 802.11:

IEEE 802.11a. Разработан в 1999 году. Работает в менее загруженной частотной полосе 5 ГГц и обеспечивает скорость до 54 Мбит/с. Поскольку этот стандарт работает на более высоких частотах, он имеет меньшую зону покрытия и менее эффективен внутри зданий. Беспроводные устройства оснащены одной антенной для передачи и приема беспроводных сигналов. Устройства, работающие в соответствии с данным стандартом, несовместимы со стандартами 802.11b и 802.11g.

IEEE 802.11b. Разработан в 1999 году. Работает в частотной полосе 2,4 ГГц и обеспечивает скорость до 11 Мбит/с. Устройства, работающие в соответствии с этими стандартами, имеют больший диапазон и более высокую эффективность при использовании внутри зданий по сравнению с устройствами стандарта 802.11a. Беспроводные устройства оснащены одной антенной для передачи и приема беспроводных сигналов.

IEEE 802.11g. Разработан в 2003 году. Работает в частотной полосе 2,4 ГГц и обеспечивает скорость до 54 Мбит/с. Устройства, работающие в соответствии с этим стандартом, работают с той же радиочастотой и диапазоном, что и устройства со стандартом 802.11b, но имеют пропускную способность стандарта 802.11a. Беспроводные устройства оснащены одной антенной для передачи и приема беспроводных сигналов. Этот стандарт совместим со стандартом 802.11b. Однако при работе с клиентами стандарта 802.11b общая пропускная способность снижается.

IEEE 802.11n. Разработан в 2009 году. Работает в частотных полосах 2,4 и 5 ГГц, известен как двухполосное устройство. Стандартные скорости передачи данных – 150–600 Мбит/с; диапазон действия – до 70 м. Тем не менее, чтобы обеспечить более высокую скорость, точкам доступа и беспроводным клиентам требуются несколько антенн, использующих технологию многоканального входа — многоканального выхода (MIMO). Технология поддерживает до четырех антенн. Стандарт 802.11n поддерживает обратную совместимость с устройствами 802.11a/b/g.

IEEE 802.11ac (Wi-Fi 5). Разработан в 2013 году. Работает в частотной полосе 5 ГГц, обеспечивая скорость передачи данных в диапазоне от 450 Мбит/с до 1,3 Гбит/с (1300 Мбит/с). Данный стандарт использует технологию MIMO для повышения производительности обмена данными. Может поддерживаться до восьми антенн, при этом скорость возрастает до 6,77 Гбит/с. Стандарт 802.11ac поддерживает обратную совместимость с устройствами 802.11a/n, но поддержка смешанных сред ограничивает предполагаемую скорость передачи данных.

IEEE 802.11ad. Разработан в 2014 году. Этот стандарт также называют WiGig. Он использует решение для трехполосного Wi-Fi, в котором задействованы частотные полосы 2,4; 5; 60 ГГц. Стандарт теоретически обеспечивает скорость передачи данных до 7 Гбит/с. Тем не менее, полоса 60 ГГц – это технология, для работы которой требуется прямая видимость, следовательно, проходить сквозь стены сигнал не сможет. В роуминге устройства пользователей коммутируются на полосы 2,4 и 5 ГГц с более низкой частотой. Стандарт поддерживает обратную совместимость с существующими устройствами Wi-Fi.

Для создания беспроводной сети используются оконечные устройства, оснащенные беспроводными сетевыми адаптерами, и промежуточные устройства инфраструктуры (например, беспроводной маршрутизатор или точка беспроводного доступа).

Точки доступа могут быть автономными и управляемыми контроллером.

Автономные точки доступа представляют собой автономные устройства, настраиваемые с помощью графического интерфейса пользователя или интерфейса командной строки. Автономные точки доступа рекомендуется использовать в тех случаях, когда в наличии сети требуются не более двух точек доступа.

Точки доступа, управляемые контроллером, рекомендуется использовать в случаях, когда в сети требуется много точек доступа. По мере добавления дополнительных точек доступа настройка и управление каждой из них осуществляются контроллером WLAN автоматически (рисунок 65).

Рисунок 65 – Точки доступа, управляемые контроллером

Выделяют несколько видов топологий, используемых в беспроводных сетях.

1 **Режим прямого подключения (ad hoc)** показан на рисунке 66.

Для режима прямого подключения характерно: устройства соединены по беспроводной сети без промежуточных устройств; нет подключения к проводной сети; простота развертывания; к примерам этого режима можно отнести Bluetooth и Wi-Fi Direct.

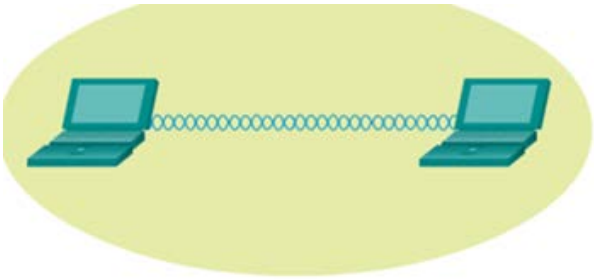


Рисунок 66 – Режим прямого подключения

2 **В инфраструктурном режиме** беспроводные клиенты соединены друг с другом посредством точки доступа. Точки доступа имеют порт Ethernet для подключения к сетевой инфраструктуре посредством кабеля.

Выделяют два структурных элемента топологии инфраструктурного режима: базовый набор сервисов (BSS) и расширенный набор сервисов (ESS).

BSS состоит из одной точки доступа, которая взаимодействует со всеми связанными беспроводными клиентами. На рисунке 67 показаны два набора BSS. Окружностями обозначена зона покрытия, в пределах которой беспроводные клиенты BSS могут поддерживать связь друг с другом. Эта зона называется зоной основного обслуживания (BSA). Если беспроводной клиент выходит из зоны основного обслуживания, он больше не может напрямую связываться с другими беспроводными устройствами в пределах зоны BSA. BSS является структурным элементом топологии, а BSA – фактической зоной покрытия (термины BSA и BSS зачастую используются как взаимозаменяемые).

В MAC-адресе второго уровня точки доступа используются для уникальной идентификации каждого набора BSS и называется идентификатором базового набора сервисов (BSSID). Таким образом, идентификатор BSSID является формальным именем BSS и всегда связан только с одной точкой доступа.

Когда один набор BSS обеспечивает недостаточное радиочастотное покрытие, то с помощью общей распределительной системы можно связать два или более наборов BSS, что образует расширенный набор сервисов (ESS). Как показано на рисунке 67, набор сервисов ESS представляет собой объединение двух или более наборов BSS, взаимосвязанных посредством кабельной распределительной системы. Теперь беспроводные клиенты в одной зоне BSA могут обмениваться данными с беспроводными клиентами в другой зоне BSA в пределах одного набора ESS. Перемещающиеся мобильные беспроводные клиенты в роуминге могут переходить из одной зоны BSA в другую (с тем же набором ESS) и без проблем выполнять подключение.

Прямоугольной областью обозначена зона покрытия, в пределах которой участники набора ESS могут осуществлять обмен данными. Эта область называется зоной расширенного обслуживания (ESA). ESA, как правило, содержит несколько наборов BSS в перекрывающихся и/или отдельных конфигурациях.

Каждый ESS определяется идентификатором SSID, а в ESS каждый BSS определяется идентификатором BSSID.

Каждая сеть представляется своим уникальным логическим адресом – network name. В стандарте 802.11 им служит SSID (Service Set Identifier). Одна сеть ESS имеет один SSID. На практике SSID используется для того, чтобы указать беспроводной станции адрес сети для подсоединения. Прежде чем связаться с определенной беспроводной сетью, станция должна иметь тот же SSID, что и AP.

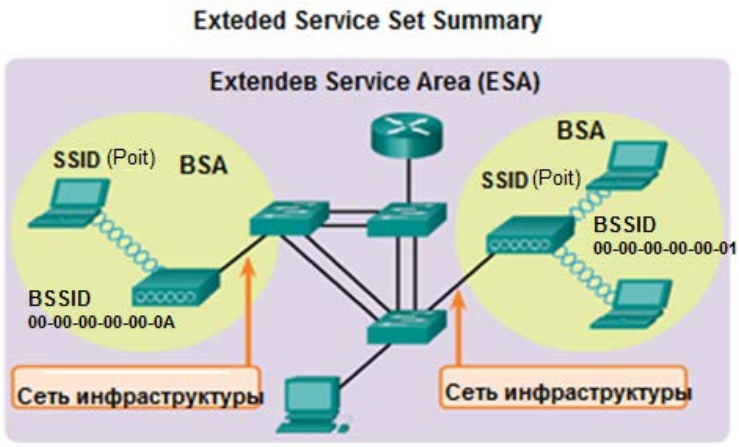


Рисунок 67 – Инфраструктурный режим

3 **В мостовом режиме** точки доступа соединяются только между собой, образуя мостовое соединение.

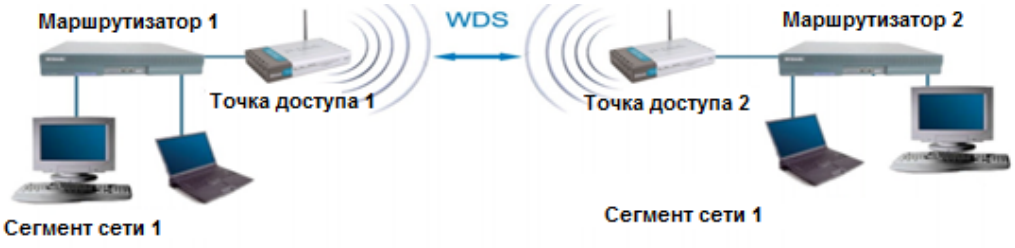


Рисунок 68 – Мостовой режим

4 **В режиме моста и точки доступа** организуется мостовая связь между точками доступа и одновременно подключаются клиентские компьютеры.

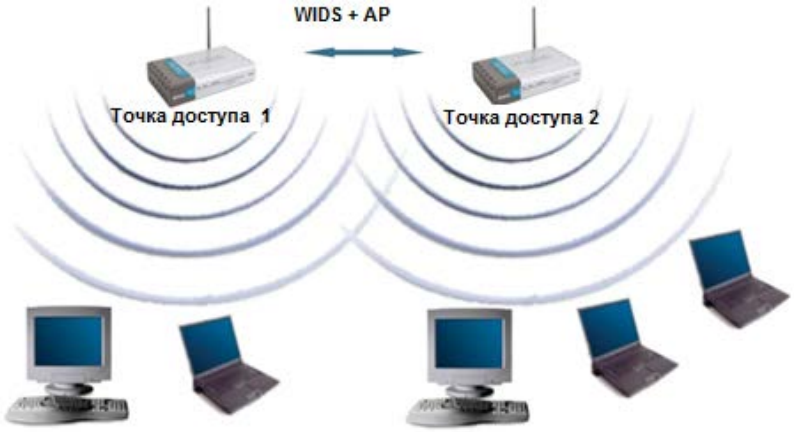


Рисунок 69 – Режим моста и точки доступа

Физический и канальный уровень модели OSI для беспроводных сетей отличаются от соответствующих уровней других технологий.

Физический уровень состоит из двух подуровней:

– PLCP (Physical Layer Convergence Protocol). Выполняет процедуру упаковки PDU уровня MAC во фрейм соответствующего метода передачи беспроводной сети. В настоящее время в сетях 802.11 используются следующие методы передачи: ортогональное частотное разделение сигналов (Orthogonal Frequency Division Multiplexing, OFDM), расширение спектра скачкообразной перестройкой частоты (Frequency Hopping Spread Spectrum, FHSS), прямое последовательное расширение спектра (Direct Sequence Spread Spectrum, DSSS);

– PMD (Physical Medium Dependent) – подуровень, зависящий от среды передачи. Осуществляет модуляцию потока байтов высокочастотными электромагнитными колебаниями. При этом используются различные методы модуляции: BPSK (Binary phase-shift keying) – бинарная фазовая модуляция, QPSK (Quadrature PSK) – квадратурная фазовая модуляция и QAM (Quadrature Amplitude Modulation) – квадратурная амплитудная модуляция.

Задача канального уровня – обеспечение доступа к среде передачи. На этом уровне используются метод CSMA/CA и его дополнение в виде метода MACA (Multiple Access with Collision Avoidance – множественного доступа с предотвращением коллизий).

Последовательность кадра узлом:

– прослушать среду;

– после окончания передачи кадра отсчитать интервал времени, равный межкадровому интервалу (может браться из кадра);

– если среда свободна, то отсчитать случайный интервал времени;

– если среда свободна, передать служебный кадр RTS – Request to Send (запрос на отправку);

– целевой узел, получив этот кадр, вырабатывает сигнал занятости среды CTS (Clear To Send – готовность к отправке). В этом кадре указывается, какое время среда будет занята. Все остальные узлы, получив этот сигнал, ждут указанное время;

– момент передачи кадра данных;

– после приема данных узел назначения отвечает сигналом ACK.

Существуют два режима контроля доступа к среде передачи:

1 DCF (Distributed Coordination Function) – распределенный режим контроля доступа к среде передачи. В этом режиме управление доступом к среде передачи выполняется по алгоритму CSMA/CA+ MACA. В таком режиме узлы работают без точки доступа.

2 PCF (Point Coordination Function) − централизованный режим контроля доступа PCF (Point Coordination Function). Точка доступа играет роль арбитра среды. Режимы DCF и PCF могут сосуществовать вместе (*режимы задаются точкой доступа путем изменения межкадрового растояния*).

Формат кадра канального уровня беспроводной сети приведен на рисунке 70.

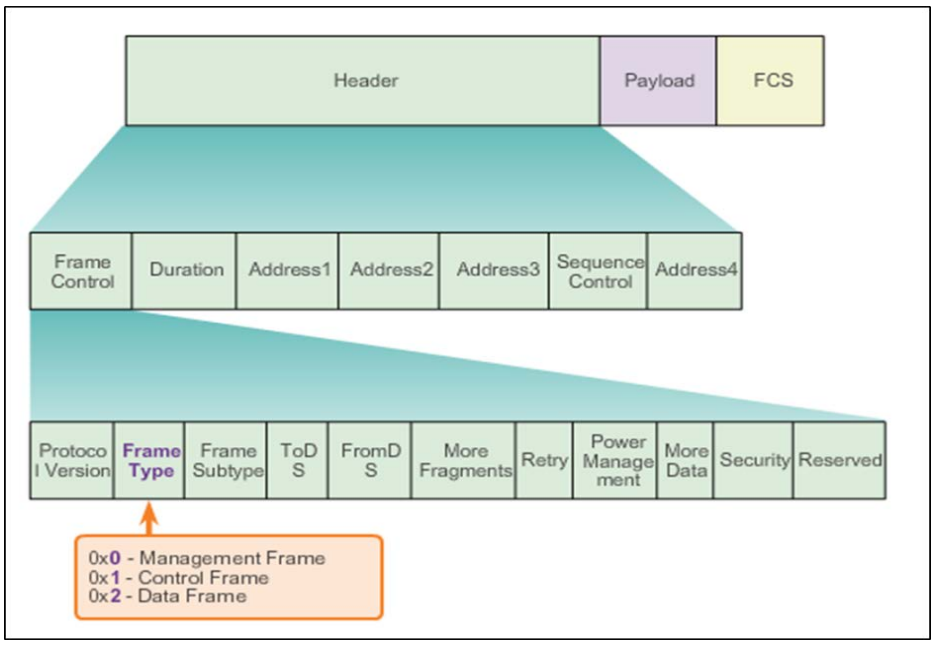


Рисунок 70 – Формат кадра беспроводной сети

Кадры беспроводной сети 802.11 содержат следующие поля:

– **Управление кадром (Frame Control).** Определяет тип кадра беспроводной сети и содержит подполя для версии протокола, типа кадра, типа адреса, настроек управления питанием и безопасности;

– **Продолжительность (Duration).** Как правило, используется для обозначения оставшегося времени, требуемого для приема следующего передаваемого кадра;

– **Адрес 1 (Address1).** Содержит MAC-адрес принимающего беспроводного устройства или точки доступа;

– **Адрес 2 (Address2).** Содержит MAC-адрес передающего беспроводного устройства или точки доступа;

– **Адрес 3 (Address3).** В отдельных случаях содержит MAC-адрес назначения, например, интерфейс маршрутизатора (шлюз по умолчанию), к которому подключена точка доступа;

– **Secuence Control (Управление последовательностью).** Содержит подполя для номера последовательности и номера фрагмента, служит для фрагментации кадра;

– **Адрес 4 (Address4).** Обычно отсутствует, поскольку используется только в режиме прямого соединения;

– Полезная информация (Payload). Содержит данные для передачи;

– **FCS**. Контрольная последовательность кадра, которая используется для контроля ошибок канального уровня.

Поле **Тип кадра** (**Frame Type**), которое входит в состав поля **Управление кадром**, задает следующие типы кадров беспроводной сети:

– кадр управления – используется в процессе обслуживания процесса обмена данными, например, при поиске, аутентификации и ассоциации с точкой доступа;

– контрольный кадр – кадры RTS, CTS, ACK и служебные кадры;

– кадр данных – используется для передачи данных.

Поле **Подтип кадра** (**Frame Subtype**) детализирует подтип кадра в одном из типов кадра.

Единица в поле **To DS** (**Distributed System**) означает, что кадр передается к проводной сети из беспроводной, а если единичное значение в поле **From DS**, то кадр передается из проводной в беспроводную сеть.

Поле **MF (More Fragments)** указывает, фрагментирован кадр или нет. Это поле совместно с полем **Управление последовательностью** служит для фрагментации кадров.

Поле **Retry** (повторить) – указывает, выполняется ли повторная передача кадра.

Бит **PM** устанавливается узлом (станцией) при передаче кадра к точке доступа и сообщает, в каком режиме находится станция: в активном или спящем. В спящем режиме узел не принимает и не передает данные и находится в режиме энергосбережения. В это время точка доступа записывает данные, приходящие к этому узлу в свой буфер. Спящая станция периодически «просыпается» и считывает эти данные с точки доступа. Бит MD устанавливается точкой доступа при передаче кадра к узлу, если у нее есть еще данные для узла. Эти два бита используются для режима энергосбережения узла.

Поле **Protection Frame** указывает, используется ли шифрование данных.

В поле **Order** принимаются кадры в том же порядке, как и отправляются, или не принимаются.

Канал беспроводной сети – это диапазон частот (относительно основной несущей частоты), на котором передаются данные канала.

Характеристики канала:

– скорость передачи данных (бит/с) – скорость, с которой могут передаваться данные;

− ширина полосы передаваемого сигнала, измеряется в герцах (Гц);

− средний уровень шума в канале связи или чаще соотношение сигнал/шум.

Все стандарты IEEE 802.11b/g/n работают на СВЧ-частотах спектра радиосигналов.

Стандарты IEEE 802.11b/g/n работают в частотном диапазоне 2,4–2,5 ГГц, стандарты 802.11a/n/ac – в диапазоне 5–5,9 ГГц, стандарты 802.11ad использует частоту 60 ГГц.

На рисунке 71 показано, что полоса 2,4 ГГц поделена на 13 (в Европе), 11 (в Северной Америке) каналов (несущих частот). Для стандарта 802.11b ширина одного канала составляет 22 МГц, при этом доступно три независимых канала: 1, 6, 11. Для стандартов 802.11g/n при ширине 20 Мгц доступны четыре непересекающихся канала: 1, 5, 11, 13. Каждый канал отделяется полосой 5 МГц. Чтобы устранить помехи, нужно использовать неперекрывающиеся каналы. В диапазоне 5 ГГц существует 23 непересекающихся канала.

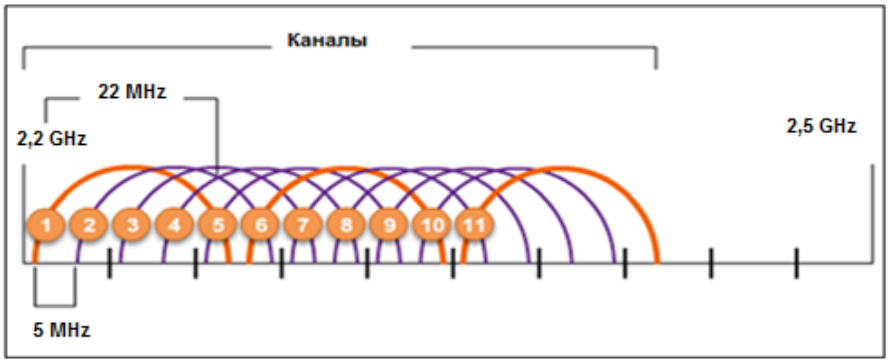


Рисунок 71 – Каналы беспроводной сети

Некоторые стандарты беспроводных сетей могут использовать соединение каналов, при котором два канала по 20 МГц объединяются в один канал 40 МГц. Соединение каналов увеличивает пропускную способность за счет использования для доставки данных одновременно двух каналов.

Большинство современных точек доступа могут автоматически регулировать каналы, чтобы обойти помехи.

Технология MIMO (Input Multiple Output, Multiple, многоканальный вход – выход) – метод кодирования потоков в пределах одного канала. Каждая передающая антенна передает отдельный пространственный поток (рисунок 72).

Принимающие антенны принимают все потоки, но каждая выбирает пространственный поток «своего» передатчика.

Общая скорость равна сумме скоростей пространственных потоков.

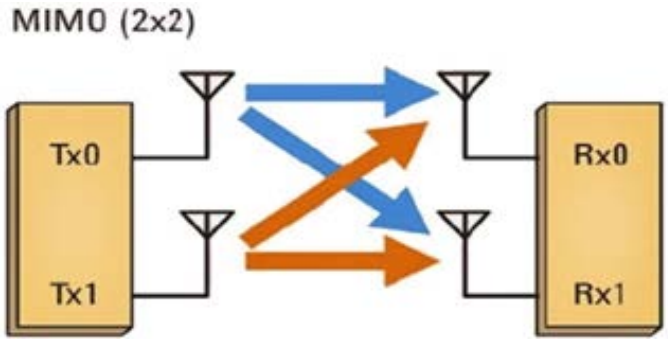


Рисунок 72 – Технология MIMO

Чтобы беспроводные устройства могли осуществлять обмен данными по сети, они должны с помощью кадров управления выполнить процесс, состоящий из трех этапов:

1) обнаружение новой точки беспроводного доступа;
2) аутентификация на точке доступа;
3) ассоциация с точкой доступа.

Для выполнения ассоциации беспроводной клиент и точка доступа должны согласовать особые параметры. Чтобы разрешить согласование, эти

параметры необходимо предварительно настроить на точке доступа, а затем – на клиенте.

К общим настраиваемым параметрам точки доступа можно отнести:

1) идентификатор SSID. Обычно длина имени составляет от 2 до 32 символов;

2) пароль (ключ);

3) сетевой режим (Network mode) – относится к стандартам сети WLAN 802.11a/b/g/n/ac/ad;

4) режим безопасности (Security mode) – этот термин относится к настройкам параметров безопасности (WEP, WPA или WPA2, WPA3);

5) настройки канала (Channel settings) – относится к частотным каналам, которые используются для передачи беспроводных данных.

Беспроводные устройства выполняют обнаружение точек доступа в двух режимах:

– пассивный (Passive mode) – режим, при котором точка доступа ищет клиента. Точка доступа открыто объявляет свою службу путем регулярной отправки кадров сигнала широковещательной рассылки, содержащих имя SSID, сведения о поддерживаемых стандартах и настройки безопасности;

– активный (Active mode) – режим, при котором клиент ищет точку доступа. Беспроводные клиенты должны знать имя SSID. Беспроводной клиент рассылает широковещателые кадры запроса поиска на несколько каналов. Запрос поиска содержит имя SSID и сведения о поддерживаемых стандартах. Активный режим может понадобиться в том случае, если для беспроводного маршрутизатора или точки доступа настроен запрет широковещательной рассылки кадров сигнала.

Стандарт 802.11 изначально разработан с учетом двух механизмов аутентификации:

– открытая аутентификация обеспечивает подключение к беспроводной сети для любого беспроводного устройства. Такой метод аутентификации следует использовать только в тех случаях, когда безопасность не имеет большого значения;

– аутентификация согласованного ключа – технология, подразумевающая использование ключа, предварительно согласованного с клиентом и точкой доступа.

Методы аутентификации, используемые в беспроводных сетях:

1 WEP (Wired Equivalent Privacy – безопасность, эквивалентная проводному соединению) – менее надежный метод по сравнению с WPA.

2 WPA (Wi-Fi Protecred Access), который бывает трех видов:

а) WPA2-Personal (-Personal Key или -PSK), предназначенный для небольших сетей;

б) WPA2-Enterprise. Для авторизации требуется сервер удаленной аутентификации пользователей – Radius;

в) WPA3.

Процесс ассоциации состоит из следующих этапов:

1 Беспроводной клиент пересылает кадр запроса ассоциации, который содержит его MAC-адрес.

2 Точка доступа отправляет в ответ отклик по ассоциации, содержащий BSSID-точки доступа, который является MAC-адресом точки доступа.

3 Точка доступа сопоставляет логический порт, известный как идентификатор ассоциации (AID), с беспроводным клиентом. Идентификатор AID равнозначен порту коммутатора и позволяет коммутатору инфраструктуры отслеживать кадры, отправляемые беспроводному клиенту для пересылки.

4 После ассоциации беспроводного клиента с точкой доступа трафик может передаваться между ними.

При планировании беспроводной сети надо рассчитать необходимое количество точек доступа в зависимости:

– от количества подключаемых клиентов. Одна точка доступа в среднем на 15 клиентов (с шифрованием) и одна точка доступа в среднем на 20 клиентов (без шифрования);

– уровня принимаемого сигнала в зоне покрытия. Для уверенного приема уровень сигнала в зоне покрытия точки доступа должен быть ослаблен не менее чем на – 70 дБ. Здесь необходимо учитывать план помещения, а также тип используемых материалов. Существуют программные средства, которые позволяют приблизительно рассчитать количество точек в зависимости от указанных параметров, например, программа Wi-Fi_Planner от компании D-Link;

– обеспечения требований по скорости.

После определения количества точек доступа необходимо их правильно расположить, используя следующие общие правила:

1 Точки доступа следует размещать выше физических препятствий.

2 По возможности размещать точки доступа вертикально рядом с потолком в центре каждой зоны.

3 Размещать АР в тех местах, где будут находиться пользователи. (Например, конференц-залы, как правило, больше подходят для размещения точки доступа, чем коридор).

4 Следует учитывать наличие устройств, создающих электромагнитные помехи.

Для уменьшения взаимного влияния необходимо правильно выбрать каналы, на которых работают точки доступа. Как было сказано ранее, каналы не должны пересекаться. Существует целый ряд программных средств, которые позволяют оценить электромагнитную обстановку и корректно выбрать каналы и измерить уровень принимаемого сигнала в конкретном месте.

Для повышения производительности работы беспроводной сети следует наряду с диапазоном 2,4 ГГц использовать диапазон 5 ГГц.

ЛАБОРАТОРНЫЕ РАБОТЫ

ЛАБОРАТОРНАЯ РАБОТА №1

ПЛАНИРОВАНИЕ СЕТИ. РАЗБИЕНИЕ СЕТЕЙ НА ПОДСЕТИ

Цель работы:
– освоить методы планирования адресного пространства сети;
– научиться разбивать сети на подсети.

Порядок выполнения работы:
1 Изучить теоретическую часть лабораторной работы.
2 Разбить сеть на подсети с помощью масок фиксированной и переменной длины для заданной преподавателем топологи.
3 Защитить лабораторную работу.

Содержание работы
При планировании сети необходимо изучить требования к сети, определить ее основные части и при необходимости разделить сеть на требуемое количество подсетей.
Можно выделить следующие причины разделения сети на подсети:
– повышение производительности сети за счет уменьшения широковещательного трафика;
– упрощение администрирования сети;
– эффективное использование Ipv4-адресов.
Широковещательный пакет – это пакет, который поступает всем узлам данной сети. Область сети, в которой узлы «видят» широковещательные пакеты, называется широковещательным доменом.
Широковещательные пакеты возникают:
– при работе сетевых протоколов (например, DHCP, ARP и др.);
– неправильной настройке сети (петлевые соединения коммутаторов);
– неисправности сетевой карты;
– атаке на сеть.
Чем больше количество компьютеров сети, тем больше широковещательных пакетов. Иногда из-за неправильной работы сети может возникнуть широковещательный шторм. Широковещательный шторм – это лавинообразное увеличение широковещательных пакетов. При нормальном режиме работы количество широковещательных пакетов составляет не более 10 % от общего количества пакетов. Каждый компьютер широковещательного домена обязан обработать широковещательный IP-пакет, даже если он ему не предназначен. Наличие широковещательных пакетов снижает производительность сети.
Когда маршрутизатор получает широковещательную рассылку, он не пересылает ее на другие интерфейсы, поэтому, используя маршрутизаторы, мы можем разделить одну большую сеть на несколько меньших подсетей (широковещательных доменов). Широковещательные пакеты в одной подсети не будут поступать в другие сети, поэтому производительность сети повысится.

Наличие нескольких меньших подсетей упрощает администрирование сети. Сетевые администраторы могут группировать устройства и службы в подсети по их географическому местоположению (например, третий этаж здания), организационному подразделению (например, отдел продаж), по типу устройств (принтеры, серверы, глобальная сеть и т. п.) или по другому значимому для сети принципу.

Еще одно преимущество разбиения сетей на подсети – это эффективное использование IP-адресов сети. Например, можно выделить требуемое количество адресов, которое определяется количеством узлов.

План распределения адресов должен содержать информацию о требуемом размере подсети, количестве узлов и принципе назначения адресов узлам. Необходимо определить узлы, которым нужно выделить статические IP-адреса, и узлы, которые смогут получать сетевые адреса по протоколу DHCP.

Ipv4-адрес состоит из двух частей: номера сети и номера узла. Номер сети определяется количеством последовательных единиц в маске подсети. Как показано на рисунке 73, при записи номера сети в узловой части адреса записываются нули, например, в адресе 192.168.1.0/24 (с маской 255.255.255.0) в узловой части присутствуют нули.

Рисунок 73 – Разбиение сети на четыре подсети

После определения количества подсетей мы должны увеличить сетевую часть адреса (и соответственно маску подсети) на такое количество бит, которое достаточно для получения требуемого количества подсетей. На рисунке приведен пример разбиения базового сетевого адреса 192.168.1.0/24 на четыре подсети.

Диапазоны адресов распределены следующим образом:

1 Сеть 192.168.1.0/26;

а) сетевой адрес 192.168.1.0/26;

б) широковещательный 192.168.1.63/26;

в) адреса узлов 192.168.1.1–192.168.1.62/26.

2 Сеть 192.168.1.64/26:

а) сетевой адрес 192.168.1.64/26;

б) широковещательный 192.168.1.127/26;

в) адреса узлов 192.168.1.65–192.168.1.126/26.

3 Сеть 192.168.1.128/26:

а) сетевой адрес 192.168.1.128/26;

б) широковещательный 192.168.1.191/26;

в) адреса узлов 192.168.1.129–192.168.1.190/26.

4 Сеть 192.168.1.192/26:

а) сетевой адрес 192.168.1.192/26;

б) широковещательный 192.168.1.255/26;

в) адреса узлов 192.168.1.193–192.168.1.254/26.

Разбиение сети на подсети с одинаковым количеством узлов хорошо подходит для случая, когда в подсетях одинаковое количество узлов, что бывает крайне редко. Как правило, количество узлов разное, поэтому такое разбиение приводит к образованию «незадействованных адресов», что снижает эффективность разбиения.

Поэтому широко используется разбиение на подсети с помощью масок переменной длины VLSM (Variable Length Subnet Mask). При использовании VLSM на первом этапе выбирается сеть с максимальным количеством узлов, исходная маска увеличивается на определенное количество единиц, чтобы получить определенное количество узлов. Первый сетевой адрес с новой маской является новым адресом первой подсети.

Маска для второго полученного сетевого адреса увеличивается исходя из количества узлов следующей по размеру сети. Этот процесс может повторяться несколько раз и позволяет создавать подсети разных размеров исходя из необходимого количества узлов для каждой подсети. Для примера используем VLSM для разбиения изображенной на схеме топологии с исходным адресом 172.16.128.0/17 (рисунок 74).

При маске, равной 17, доступно 32 766 адресов, а для нашей топологии сумма всех требуемых адресов составляет 31512 адресов. Как видно из топологии, всего присутствует девять подсетей. На начальном этапе определяем сеть с самым большим количеством узлов – это сеть с 16 000 узлами. Для получения посети с таким количеством адресов увеличим маску на единицу (18) за счет сокращения бит в узловой части. Подсеть с такой маской обеспечивает 16 382 адреса.

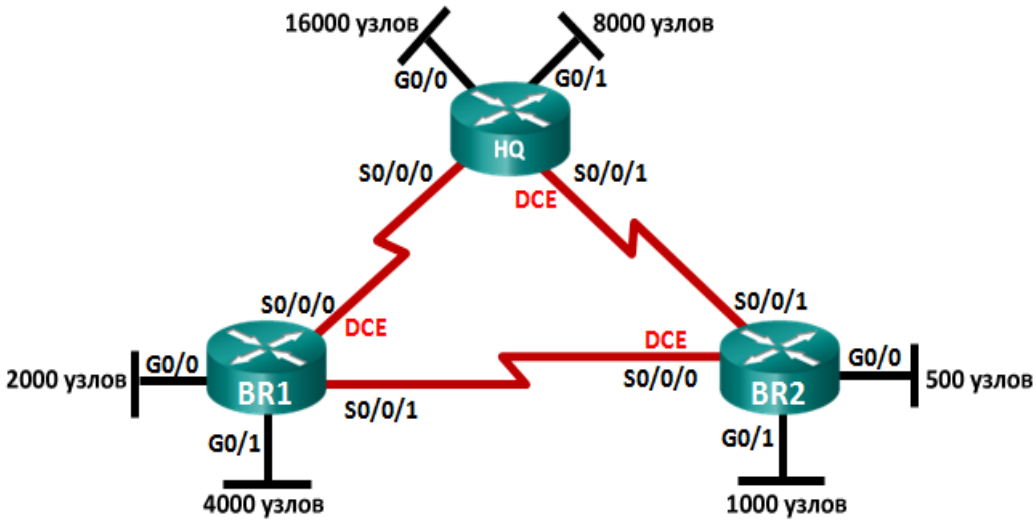


Рисунок 74 – Базовая топология для VLSM

При изменении значения заимствованного бита получим два адреса с новой маской: 172.16.128.0/18 и 172.16.192.0/18. Первый сетевой адрес будет выделен самой большой сети. Оставшийся адрес будет использован для дальнейшего разбиения для следующей по величине сети с 8000 узлами. Для адресации такого количества узлов необходимо опять увеличить маску на единицу, что позволит получить 8190 адресов. При этом опять получится два сетевых адреса: 172.16.192.0/19 и 172.16.192.224.0/19. Первый из адресов будет задействован для сети с 8000 узлами, а второй будет использован для получения сетевого адреса для следующей по величине сети с количеством узлов 4 000. При этом маска сети также будет увеличена на единицу, и получатся два следующих адреса: 172.16.224.0/20 и 172.16.240.0/20. Продолжая процесс разбиения, получим новые адреса, которые приведены на рисунке 75.

Описание подсети	Необходимое количество узлов	Сетевой адрес/CIDR	Адрес первого узла	Широковещательный адрес
HQ G0/0	16 000	172.16.128.0/18	172.16.128.1	172.16.191.255
HQ G0/1	8000	172.16.192.0/19	172.16.192.1	172.16.223.255
BR1 G0/1	4000	172.16.224.0/20	172.16.224.1	172.16.239.255
BR1 G0/0	2000	172.16.240.0/21	172.16.240.1	172.16.247.255
BR2 G0/1	1000	172.16.248.0/22	172.16.248.1	172.16.251.255
BR2 G0/0	500	172.16.252.0/23	172.16.252.1	172.16.253.255
HQ S0/0/0 – BR1 S0/0/1	2	172.16.254.0/30	172.16.254.1	172.16.254.3
HQ S0/0/1 – BR2 S0/0/1	2	172.16.254.4/30	172.16.254.5	172.16.254.7
BR1 S0/0/1 – BR2 S0/0/0	2	172.16.254.8/30	172.168.254.9	172.168.254.11

Рисунок 75 – Результаты разбиения с помощью VLSM

ЛАБОРАТОРНАЯ РАБОТА №2

СТАТИЧЕСКАЯ МАРШРУТИЗАЦИЯ

Цель работы:

– освоить навыки настройки статических маршрутов с помощью Cisco IOS в симуляторе Cisco Packet Tracer.

Порядок выполнения работы:

1 Изучить теоретическую часть лабораторной работы.

2 Настроить статические маршруты для заданной преподавателем топологии сети.

3 Защитить лабораторную работу.

Содержание работы

При пересылке пакетов из одной сети в другую маршрутизатор выбирает маршрут следования пакетов исходя из информации о маршрутах, находящихся в таблице маршрутизации. Эти записи могут добавляться в таблицу маршрутизации автоматически, с помощью динамических протоколов маршрутизации либо вручную администратором сети. В последнем случае такие маршруты называются статическими. В отличие от протокола динамической маршрутизации статические маршруты не обновляются автоматически, и при изменениях в сетевой топологии их необходимо повторно настраивать вручную.

Статическая маршрутизация имеет три основных назначения:

1 Обеспечение упрощенного обслуживания таблицы маршрутизации в небольших сетях, которые не планируется существенно расширять.

2 Маршрутизация к тупиковым сетям и от них. Тупиковая сеть представляет собой сеть, доступ к которой осуществляется через один маршрут, и маршрутизатор имеет только одно соседнее устройство.

3 Использование маршрута по умолчанию для представления пути к любой сети, не имеющего более точного совпадения с другим маршрутом в таблице маршрутизации.

На рисунке 76 представлен пример подключения к тупиковой сети и использования маршрута по умолчанию. Следует заметить, что у любой сети, подключенной к маршрутизатору R1, будет только один путь для доступа к другим сетям назначения (к сетям, подключенным к маршрутизатору R2, или к местам назначения за пределами маршрутизатора R2). Это означает, что сеть 172.16.3.0 является тупиковой, а маршрутизатор R1 – тупиковым маршрутизатором. Запуск динамического протокола маршрутизации между маршрутизаторами R2 и R1 был бы необоснованной тратой ресурсов.

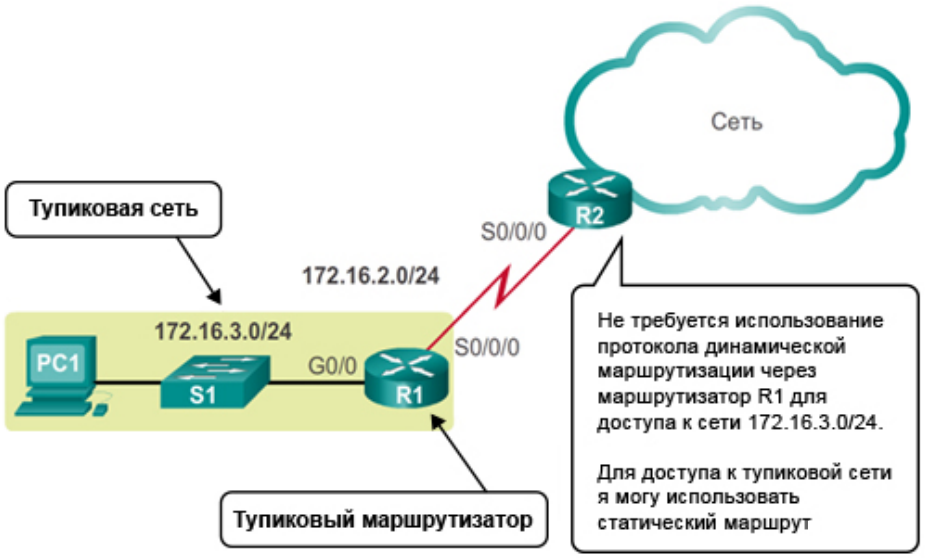


Рисунок 76 – Тупиковая сеть

Статические маршруты к удаленным сетям делятся:
– на стандартный статический маршрут;
– статический маршрут по умолчанию;
– суммарный статический маршрут:
– плавающий статический маршрут.

В операционной системе Cisco IOS для задания *стандартного статического* маршрута используется команда *ip route*. Синтаксис команды приведен на рисунке 77.

```
Router(config)# ip route network-address subnet-mask {ip-address|exit-intf}
```

Параметр	Описание
network address	Адрес удаленной сети назначения, который необходимо добавить в таблицу маршрутизации
subnet-mask	• Маска подсети удаленной сети назначения, которую необходимо добавить в таблицу маршрутизации. • Маску подсети можно изменить для объединения группы сетей
ip-address	• Как правило, называется IP-адресом маршрутизатора следующего перехода. • Обычно используется при подключении к среде широковещательного доступа (т. е. Ethernet). • Обычно создает рекурсивный поиск
exit-intf	• Использование исходящего интерфейса для передачи пакетов в сеть назначения. • Также упоминается как напрямую подключенный статический маршрут. • Обычно используется при подключении к сети в конфигурации «точка — точка»

Рисунок 77 – Синтаксис команды задания статического маршрута

В зависимости от того, как указан следующий адрес пересылки пакета, создается один из трех возможных типов маршрута (рисунок 78):

1 Маршрут следующего перехода – в команде *ip route* указывается только IP-адрес следующего перехода.

2 Напрямую подключенный статический маршрут – в команде *ip route* указывается только выходной интерфейс маршрутизатора.

3 Полностью заданный статический маршрут – в команде *ip route* указываются IP-адрес следующего перехода и выходной интерфейс.

На рисунке 77 последовательно приведены команды задания трех типов маршрутов. В настоящее время полностью заданный маршрут используется редко, так как требует несколько проходов по таблице маршрутизации, что замедляет процесс маршрутизации.

Напрямую подключенный маршрут используется, как правило, при соединении маршрутизаторов по последовательному интерфейсу типа «точка – точка».

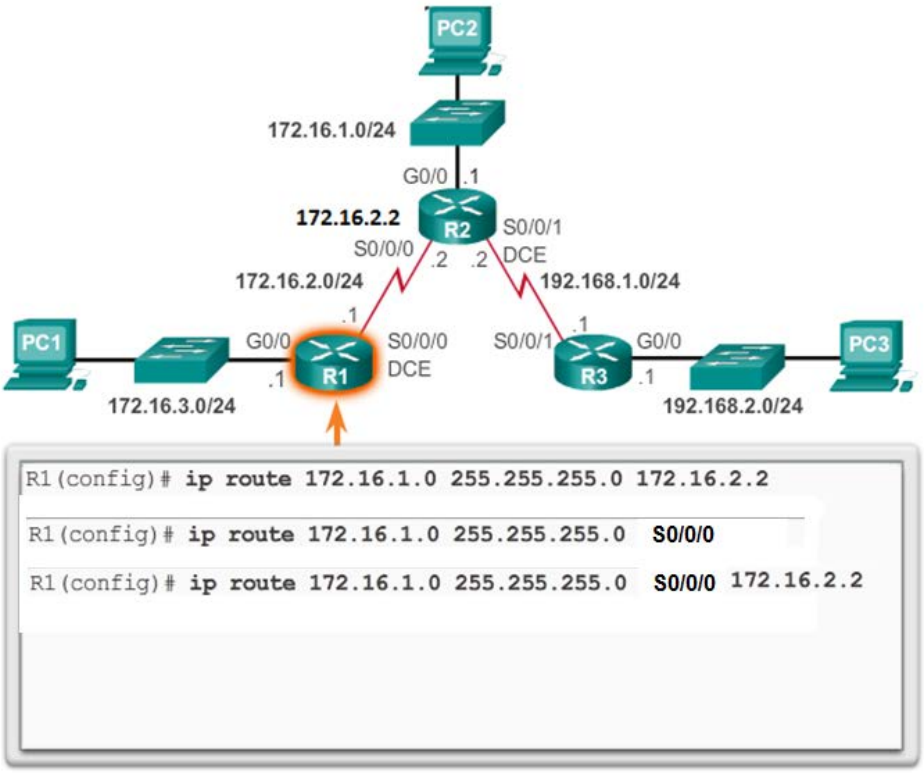


Рисунок 78 –Три типа статических маршрутов

Статический маршрут по умолчанию идентифицирует IP-адрес шлюза, на который маршрутизатор отправляет все IP-пакеты, для которых у него нет известного динамического или статического маршрута. Статический маршрут по умолчанию – это статический маршрут с IPv4-адресов назначения равным 0.0.0.0/0. При настройке статического маршрута по умолчанию задается «шлюз последней надежды».

Для уменьшения числа записей в таблице маршрутизации можно объединить несколько статических маршрутов в один статический маршрут (рисунок 79). Это возможно при следующих условиях:

– сети назначения являются смежными и могут быть объединены в один сетевой адрес;

– все статические маршруты используют один и тот же выходной интерфейс или один IP-адрес следующего перехода.

```
Router(config) #ip route 0.0.0.0 0.0.0.0 (ip-adress | intf)
```

Параметр	Описание
0.0.0.0	Соответствует любому адресу сети
0.0.0.0	Соответствует любой маске подсети
ip-address	• Как правило, называется IP-адресом маршрутизатора следующего перехода. • Обычно используется при подключении к среде широковещательного доступа (т. е. Ethernet). • Обычно создает рекурсивный поиск
exit-intf	• Использование исходящего интерфейса для передачи пакетов в сеть назначения. • Также упоминается как напрямую подключенный статический маршрут. • Обычно используется при подключении к сети в конфигурации «точка – точка»

Рисунок 79 – Синтаксис команды задания маршрута по умолчанию

На рисунке 80 суммарный маршрут рассчитывается путем сравнения двоичных эквивалентов адресов сетей. Результирующей будет та часть адресов, которая имеет общие двоичные значения. На рисунке одинаковыми значениями будут 22 бита адресов сетей, т. е. 172.16.0.0/22. Тогда на маршрутизаторе R3 на рисунке 81 можно отменить три отдельных статических маршрута и задать один суммарный маршрут.

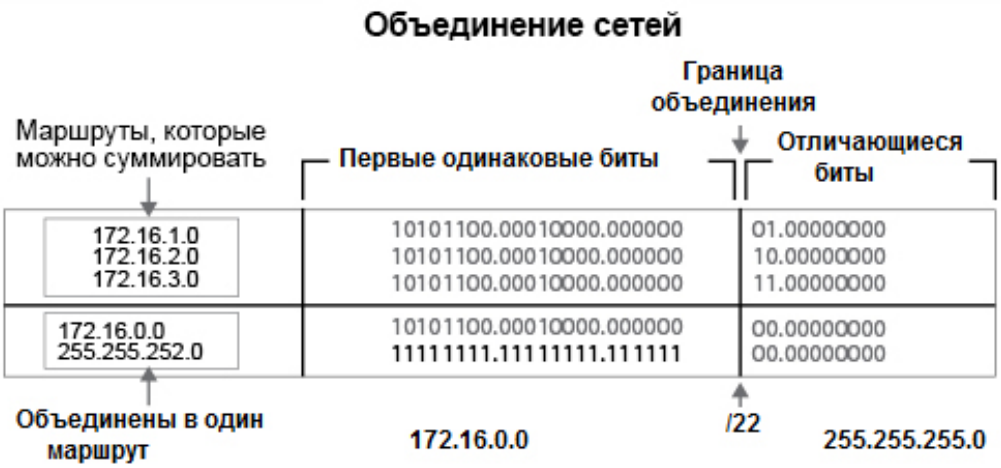


Рисунок 80 – Расчет суммарного маршрута

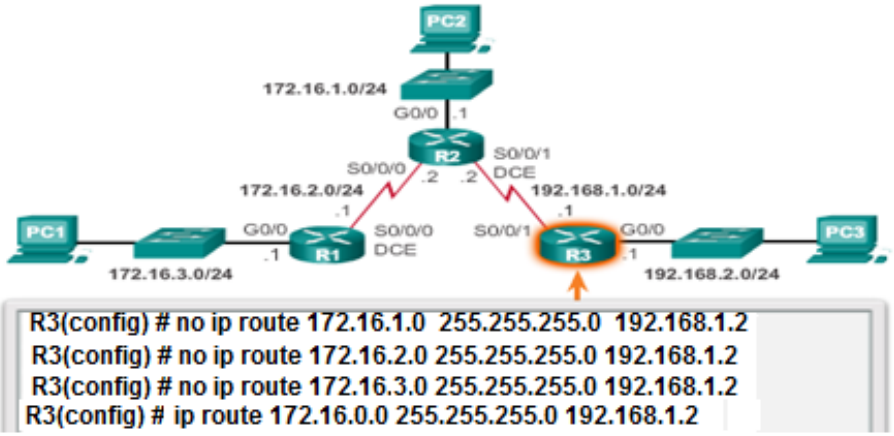


Рисунок 81 – Задание суммарного статического маршрута

Плавающие статические маршруты – это статические маршруты, используемые для предоставления резервного пути основному статическому маршруту или динамическому маршруту на случай сбоя в работе этих маршрутов.

Плавающий статический маршрут используется только тогда, когда основной маршрут недоступен.

Для задания плавающего маршрута создается статический маршрут с более низким приоритетом, чем основной маршрут.

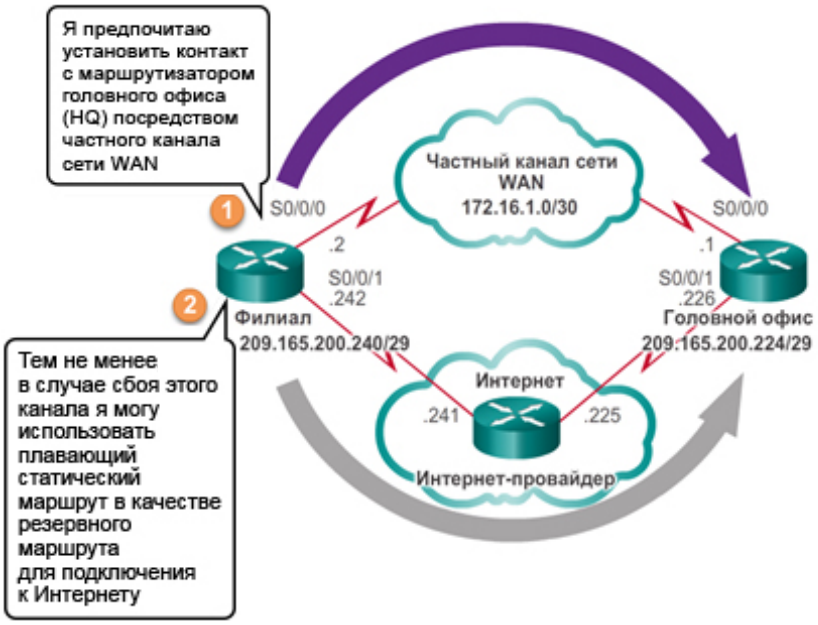


Рисунок 82 – Плавающий статический маршрут

Преимущества статической маршрутизации по сравнению с динамической маршрутизацией следующие:

– статические маршруты не объявляются по сети, таким образом, они более безопасны;

– статические маршруты не занимают трафика, так как не передаются по сети. Кроме того, для расчета и связи маршрутов не используются ресурсы ЦП;

– путь, используемый статическим маршрутом для отправки данных, известен.

У статической маршрутизации также имеются недостатки:

– исходная настройка и дальнейшее обслуживание требуют временных затрат;

– при настройке часто допускаются ошибки, особенно в больших сетях;

– для внесения изменений в данные маршрута требуется вмешательство администратора;

– недостаточные возможности масштабирования для растущих сетей (обслуживание при этом становится довольно трудоемким);

– для качественного внедрения требуется досконадьное знание всей сети.

Следует отметить, что статические маршруты могут существовать в таблице маршрутизации вместе с динамическими, при этом приоритет статических маршрутов выше.

Далее приведены примеры команд для настройки статических маршрутов для топологии сети, представленной на рисунке 83:

– R1(config)# ip route 192.168.204.0 255.255.255.0 192.168.202.2;

– R3(config)# ip route 192.168.201.0 255.255.255.0 192.168.203.1;

– R2(config)# ip route 192.168.201.0 255.255.255.0 192.168.202.1;

– R2(config)# ip route 192.168.204.0 255.255.255.0 192.168.203.2.

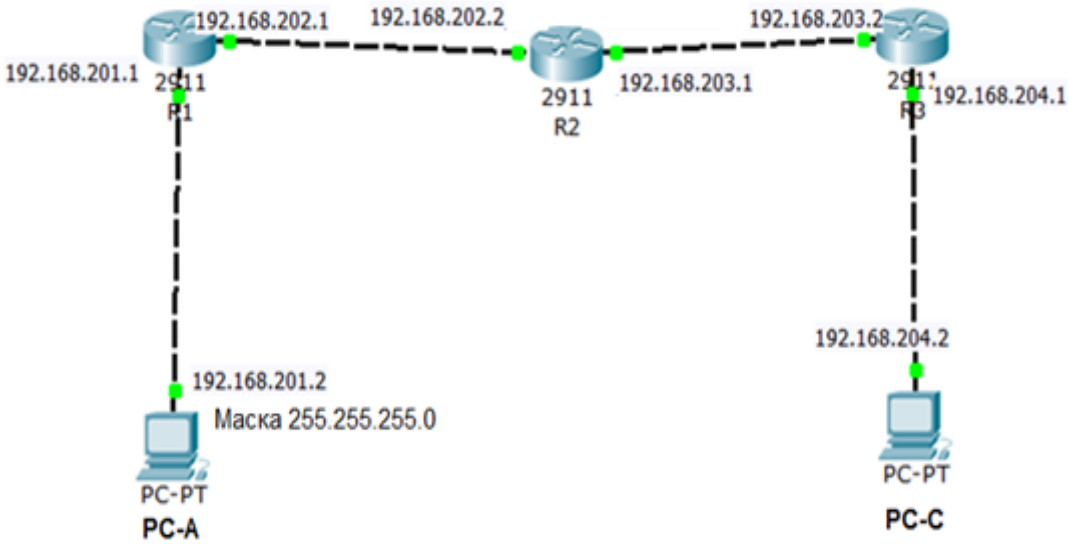


Рисунок 83 –Топология для задания статических маршрутов

ЛАБОРАТОРНАЯ РАБОТА №3

НАСТРОЙКА СЛУЖБЫ DHCP И СЕТЕВОЙ ТРАНСЛЯЦИИ АДРЕСОВ (NAT)

Цель работы:

– освоить навыки настройки службы DHCPv4 с помощью Cisco IOS в симуляторе Cisco Packet Tracer;

– освоить навыки настройки статического и динамического преобразования адресов с помощью Cisco IOS в симуляторе Cisco Packet Tracer.

Порядок выполнения работы:

1 Изучить теоретическую часть лабораторной работы.

2 Настроить службу DHCPv4 и службу статического и динамического преобразования адресов для заданной преподавателем топологии сети.

3 Защитить лабораторную работу.

Содержание работы

Перед выполнением данной работы необходимо ознакомиться с теоретическим материалом по указанным темам в соответствующих разделах данного учебно-методического пособия. На рисунке 84 приведены топология сети, для которой необходимо настроить службы DHCPv4 и NAT, а также таблица распределения адресов.

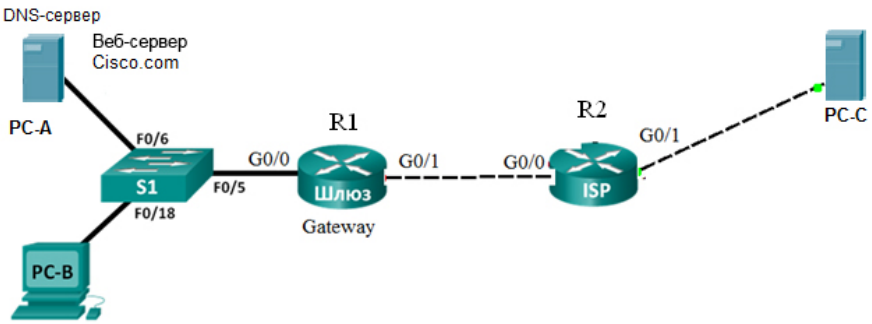


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
Шлюз	G0/0	192.168.1.1	255.255.255.0	N/A
	G0/1	209.165.201.18	255.255.255.252	N/A
ISP	G0/0	209.165.201.17	255.255.255.252	N/A
	G0/1	192.31.7.1	255.255.255.0	N/A
PC-A (смоделированный Веб- и DNS-сервер)	NIC	192.168.1.20	255.255.255.0	192.168.1.1
PC-B	NIC	DHCP	DHCP	DHCP
PC-C	NIC	192.31.7.2	255.255.255.0	192.31.7.1

Рисунок 84 – Базовая топология

Как видно из таблицы адресации, компьютеру PC-B адрес должен назначаться с помощью службы DHCPv4, развернутой на шлюзе Gateay. Остальным узлам назначаются статические адреса.

Для настройки DHCPv4-сервера на маршрутизаторе необходимо выполнить следующие основные настройки:

– включить поддержку DHCP (при необходимости);
– исключить адреса из пула;
– задать имя пула DHCP;
– задать диапазона(пула) адресов;
– задать шлюз по умолчанию;
– задать DNS-сервер;
– задать время аренды адреса (при необходимости).

В число исключенных адресов должны входить адреса, присвоенные маршрутизаторам, серверам, принтерам и другим устройствам, сконфигурированным вручную.

Следующая команда исключает из пула динамического выделения 20 адресов для статического назначения:

```
R1(config)# ip dhcp excluded-address 192.168.1.1 192.168.1.20
```

Команда **ip dhcp pool pool-name** создает пул с заданным именем и переводит маршрутизатор в режим конфигурации протокола DHCPv4:

```
R1(config)# ip dhcp pool R1G1
```

Следующая команда задает пул адресов. Как видно, всего в пуле 254 адреса, 20 первых из которых исключены из распределения:

```
R1(dhcp-config)# network 192.168.1.0  255.255.255.0
```

Следующие две команды задают IP-адрес шлюза по умолчанию и DNS-сервера:

```
R1(dhcp-config)# default-router 192.168.1.1
R1(dhcp-config)# dns-server 192.31.17.2
```

Командой **show ip dhcp binding** на маршрутизаторе R1 можно просмотреть список арендованных DHCP-адресов.

Если на PC-B в настройках протокола IP выбрать опцию **Получить адрес автоматически,** то данному компьютеру DHCP-сервером будет выделен IP-адрес.

Согласно сценарию данной лабораторной работы интернет-провайдер (ISP) выделил для компании пространство публичных IP-адресов 209.165.200.224/27. В результате компания получила 30 публичных IP-адресов. Адреса от 209.165.200.225 до 209.165.200.241 подлежат статическому распределению, а адреса от 209.165.200.242 до 209.165.200.254 – динамическому распределению.

Статический NAT использует сопоставление локальных и глобальных адресов по схеме «один к одному». Метод статического преобразования сетевых адресов особенно полезен для веб-серверов или устройств, которые

должны иметь постоянный адрес, доступный из Интернета для технического персонала компании.

Настроенная статическая привязка позволяет маршрутизатору осуществлять трансляцию адресов между частным внутренним адресом сервера 192.168.1.20 и публичным адресом 209.165.200.225. Благодаря этому пользователь может получить доступ к компьютеру PC-A через Интернет. Компьютер PC-A моделирует сервер или устройство с постоянным адресом, к которому можно получить доступ через Интернет.

Статическое преобразование выполняется командой

```
Gateway(config)# ip nat inside source static 192.168.1.20
209.165.200.225
```

Далее с помощью команд ip nat inside и ip nat outside выполняются внутренние и внешние интерфейсы к маршрутизатору NAT:

```
Gateway(config)# interface g0/0
Gateway(config-if)# ip nat inside
Gateway(config-if)# interface g0/1
Gateway(config-if)# ip nat outside
```

Отобразить таблицу статических преобразований NAT можно с помощью команды

show ip nat translations.

Для доступа из внешней сети к веб-серверу за NAT необходимо на маршрутизаторах настроить статические маршруты. На маршрутизаторе ISP в качестве сети назначения необходимо использовать публичный сетевой адрес **209.165.200.224**, выданный провайдером.

На маршрутизаторе Gateway можно использовать маршрут по умолчанию

```
ISP(config)# ip route 209.165.200.224  255.255.255.224  209.165.201.18
Gateway(config)# ip route 0.0.0.0  0.0.0.0  209.165.201.17
```

Для проверки работы NAT необходимо на сервере PC-A добавить службы HTTP- и DNS-серверов. В настройках DNS-сервера необходимо добавить запись соответствия символьного имени веб-сервера, например, Cisco.com, и его IP-адреса, который в случае использования статического NAT будет иметь значение **209.165.200.225.** На компьютере PC-C при настройке адресов IP-протокола в качестве IP-адреса DNS-сервера также необходимо указать адрес **209.165.200.225.** Схема считается работоспособной, если при наборе в браузере компьютера PC-C имени Cisco.com произойдет отображение встроенной страницы веб-сервера PC-A.

Во второй части работы необходимо, используя команды, настроить динамическое преобразование для других узлов частной сети из диапазона выделенных глобальных адресов **от 209.165.200.242 до 209.165.200.254.** Динамическое преобразование основано на принципе «несколько частных адресов к нескольким глобальным адресам».

На рисунке 85 приведена пошаговая настройка динамического NAT, а также список команд настройки динамического NAT для нашего примера:

```
Gateway(config)# access-list 1 permit 192.168.1.0 0.0.0.255
Gateway(config)# ip nat pool dynamic_NAT 209.165.200.242
209.165.200.254 netmask 255.255.255.224
Gateway(config)# #ip nat inside source list 1 pool
dynamic_NAT
Gateway(config)# interface g0/0
Gateway(config-if)# ip nat inside
Gateway(config-if)# interface g0/1
Gateway(config-if)# ip nat outside
```

Пошаговая настройка динамического NAT

Шаг 1	Задайте пул глобальных адресов, используемый для преобразования: `ip nat pool` *name start-ip end-ip* `{netmask` *netmask* `|` `prefix-length` *prefix-length}*
Шаг 2	Настройте стандартный список доступа, позволяющий адреса,которые должны быть преобразованы: `accesslist` *access-list-number* `permit` *source* [*source-wildcard*]
Шаг 3	Установите динамическое преобразование источника, задав список доступа и пул, определенные в предыдущих шагах: `ip nat inside source list` *access-list-number* `pool` *name*
Шаг 4	Задайте внутренний интерфейс: `interface` *type number* `ip nat inside`
Шаг 5	Задайте внешний интерфейс: `interface` *type number* `ip nat outside`

Рисунок 85 – Последовательность настройки динамического NAT

Для проверки динамического NAT на сервере PC-C в разделе службы включить поддержку служб HTTP и DNS. В базу службы DNS добавьте запись о ресурсах типа A: имени Cisco1.com соответствует адрес 192.31.17.2.

На компьютере PC-B в браузере необходимо набрать имя веб-страницы Cisco1.com. При правильной настройке сети отобразится внутренняя страница Cisco.

Отобразите и поясните назначение записей в таблице NAT.

Для настройки PAT-преобразования по схеме «много частных адресов – один публичный адрес» необходимо выполнить следующие команды:

```
Gateway(config)# access-list 1 permit 192.168.1.0. 0.0.0.255
Gateway(config)# ip nat inside source list 1 interface g0/1
overload
Gateway(config)# interface g0/1
Gateway(config)# ip nat inside
Gateway(config)# interface g0/0
Gateway(config)# ip nat outside
```

В данном примере в качестве публичного адреса используется адрес интерфейса g0/1 маршрутизатора Gateway 209.165.201.17.

ЛАБОРАТОРНАЯ РАБОТА №4

НАСТРОЙКА МАРШРУТИЗАЦИИ МЕЖДУ VLAN НА ОСНОВЕ СТАНДАРТА 802.1Q И ТРАНКОВОГО КАНАЛА

Цель работы:

– изучить принципы построения виртуальных локальных сетей;

– освоить навыки настройки виртуальных локальных сетей на коммутаторах Cisco.

Порядок выполнения работы:

1 Изучить теоретическую часть лабораторной работы.

2 Для заданного преподавателем варианта настроить виртуальную локальную сеть на основе стандарта IEEE 802.1Q и транковых каналов.

3 Защитить лабораторную работу.

Содержание работы

Существует технология, которая позволяет разделить один широковещательный домен на несколько более мелких доменов с помощью коммутаторов. Эта технология называется технологией виртуальных локальных сетей (Virtual Local Area Network, VLAN), где каждый домен представляет собой независимую изолированную сеть.

На рисунке 86 показаны отдельные подсети, в каждой из которых есть свой коммутатор. Сети объединяются между собой с помощью маршрутизатора. При этом на каждый коммутатор необходим отдельный вход маршрутизатора.

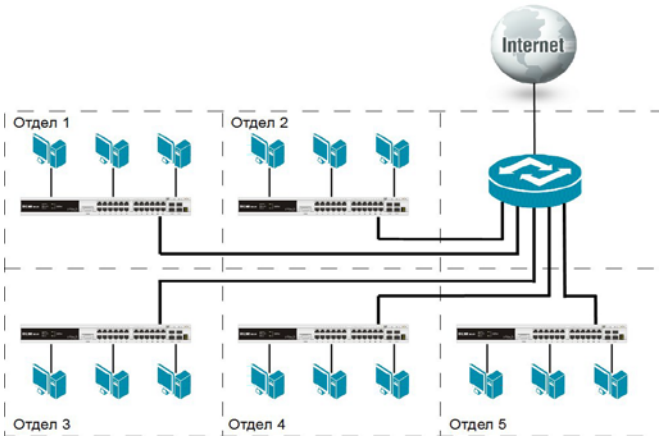


Рисунок 86 – Физическое разделение на подсети

На рисунке 87 показана та же сеть, разделенная на подсети с помощью технологии VLAN. Каждая подсеть представляет собой отдельную VLAN. Все VLAN объединяются с помощью одного порта маршрутизатора. Для этого на

маршрутизаторе настраиваются подынтерфейсы для каждой VLAN. Этот метод называют маршрутизацией между VLAN с использованием конфигурации router-on-a-stick. При использовании данного метода физический интерфейс маршрутизатора разделен на несколько подынтерфейсов, обеспечивающих логические пути ко всем подключенным сетям VLAN.

Кадры разных VLAN могут распространяться между коммутаторами и между роутером и коммутатором по одному общему физическому соединению, называемому транковым каналом (на рисунке выделены жирной линией T).

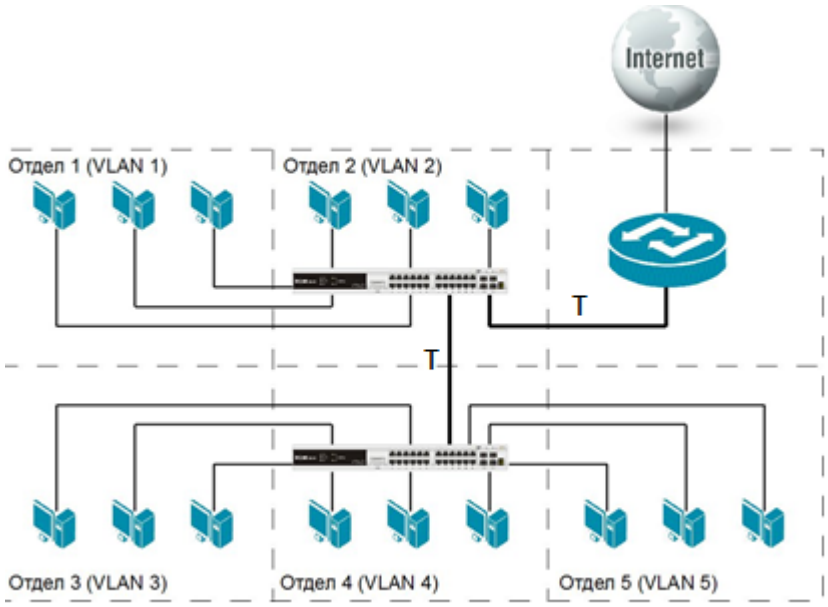


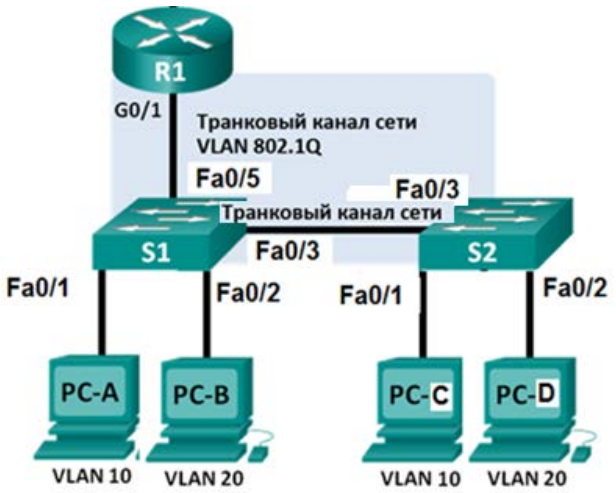
Рисунок 87 – Логическое разделение сети с помощью VLAN

В стандарте IEEE 802.1Q для идентификации пакетов, проходящих через транковый канал, в кадр канального уровня добавляется информация о номере VLAN. Эта информация добавляется в заголовок при передаче кадра в транковый канал и удаляется при приеме кадра из транкового канала.

В ходе выполнения лабораторной работы необходимо настроить две VLAN 10: **Студенты и Преподаватели**, а также настроить маршрутизацию между ними согласно базовой топологии, таблицы адресов и таблицы назначения портов коммутатора, приведенной на рисунке 88.

На коммутаторе S1 можно настроить имена сети VLAN, указанные в таблице назначения портов коммутатора с помощью команд:

```
S1(config)# vlan 10
S1(config-vlan)# name Students
S1(config-vlan)# vlan 20
S1(config-vlan)# name Faculty
```



а

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1	G0/1.1	192.168.1.1	255.255.255.0	N/A
	G0/1.10	192.168.10.1	255.255.255.0	N/A
	G0/1.20	192.168.20.1	255.255.255.0	N/A
	Lo0	209.165.200.225	255.255.255.224	N/A
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
S2	VLAN 1	192.168.1.12	255.255.255.0	192.168.1.1
PC-A	NIC	192.168.10.2	255.255.255.0	192.168.10.1
PC-B	NIC	192.168.20.2	255.255.255.0	192.168.20.1
PC-C	NIC	192.168.10.3	255.255.255.0	192.168.10.1
PC-D	NIC	192.168.20.3	255.255.255.0	192.168.20.1

б

Порты	Назначение	Сеть
S1 F0/3	Транковый канал 802.1Q	N/A
S2 F0/3	Транковый канал 802.1Q	N/A
S1 F0/5	Транковый канал 802.1Q	N/A
S1 F0/1, S2 F0/1	Сеть VLAN 10 — студенты	192.168.10.0/24
S1 F0/2, S2 F0/2	Сеть VLAN 20 — преподаватели	192.168.20.0/24

в

а – базовая топология; б – таблица адресов; в – таблица портов

Рисунок 88 – Базовая топология и параметры конфигурации

На следующем этапе на коммутаторе S1 необходимо настроить транковые каналы на интерфейсе, подключенном к маршрутизатору R1, и интерфейсе, подключенном к маршрутизатору R2:

```
S1(config)# interface fa0/5
S1(config-if)# switchport mode trunk
```

```
S1(config-if)# interface fa0/3
S1(config-if)# switchport mode trunk
```

Далее на коммутаторе S1 следует назначить порты доступа для компьютеров PC-A сети VLAN 10 и PC-B сети VLAN 20:

```
S1(config)# interface fa0/1
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 10
S1(config)# interface fa0/2
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 20
```

Ниже приведены команды настройки для коммутатора S2:

```
S2(config)# vlan 10
S2(config-vlan)# name Students
S2(config-vlan)# vlan 20
S2(config-vlan)# name Faculty
S2(config)# interface f0/3
S2(config-if)# switchport mode trunk
S2(config-if)# interface f0/1
S2(config-if)# switchport mode access
S2(config-if)# switchport access vlan 10
S1(config-if)# interface f0/2
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 20
```

После настройки коммутаторов необходимо настроить параметры маршрутизатора для соответствующих VLAN. Так, для VLAN 1, которая является виртуальной локальной сетью по умолчанию, создадим подынтерфейс на интерфейсе G0/1 маршрутизатора R1, где номер VLAN (в данном случае 1) – это идентификатор подынтерфейса:

```
R1(config)# interface g0/1.1
```

Настроим подынтерфейс для работы с VLAN 1:

```
R1(config-subif)# encapsulation dot1Q 1
```

Зададим IP-адрес для подынтерфейса из таблицы адресов:

```
R1(config-subif)# ip address 192.168.1.1 255.255.255.0
```

Аналогичным способом настроим подынтерфейсы для VLAN 10 и VLAN 20:

```
R1(config-subif)# interface g0/1.10
R1(config-subif)# encapsulation dot1Q 10
R1(config-subif)# ip address 192.168.10.1 255.255.255.0
R1(config-subif)# interface g0/1.20
R1(config-subif)# encapsulation dot1Q 20
```

```
R1(config-subif)# ip address 192.168.20.1 255.255.255.0
R1(config-subif)# exit
R1(config)# interface g0/1
R1(config-if)# no shutdown
```

Команды просмотра настроек коммутатора:

```
      S1# show interface trunk
S2# show vlan brief
S2# show  running-config
```

ЛАБОРАТОРНАЯ РАБОТА №5

НАСТРОЙКА VPN GRE-ТУННЕЛЯ ПО СХЕМЕ «ТОЧКА – ТОЧКА»

Цель работы:

– изучить принципы построения виртуальных частных сетей;

– освоить навыки настройки виртуальной частной сети на основе незащищенного GRE-туннеля.

Порядок выполнения работы:

1 Изучить теоретическую часть лабораторной работы.

2 Для заданного преподавателем варианта настроить виртуальную частную сеть типа site-to-site на основе GRE-протокола.

3 Защитить лабораторную работу.

Содержание работы

Универсальная инкапсуляция при маршрутизации (Generic Routing Encapsulation, GRE) – один из примеров незащищенного протокола создания туннелей для site-to-site VPN. GRE – это протокол туннелирования, разработанный компанией Cisco, позволяющий инкапсулировать пакеты протоколов различного типа внутри IP-туннелей. Благодаря этому создается виртуальный канал «точка – точка» между удаленными VPN-шлюзами поверх IP-сети.

Как видно из рисунка 89, формирование пакета для передачи по туннелю происходит следующим образом: к исходному IP-пакету с передаваемыми данными добавляется заголовок GRE-протокола, после этого формируется новый IP-пакет, в который добавляется IP-заголовок доставки пакета по туннелю.

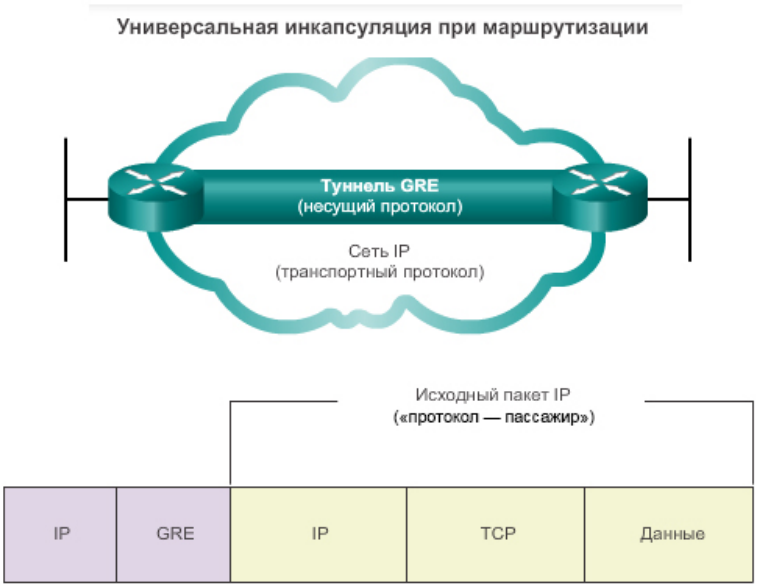


Рисунок 89 – Схема работы GRE-протокола

Формат GRE-заголовка приведен на рисунке 90.

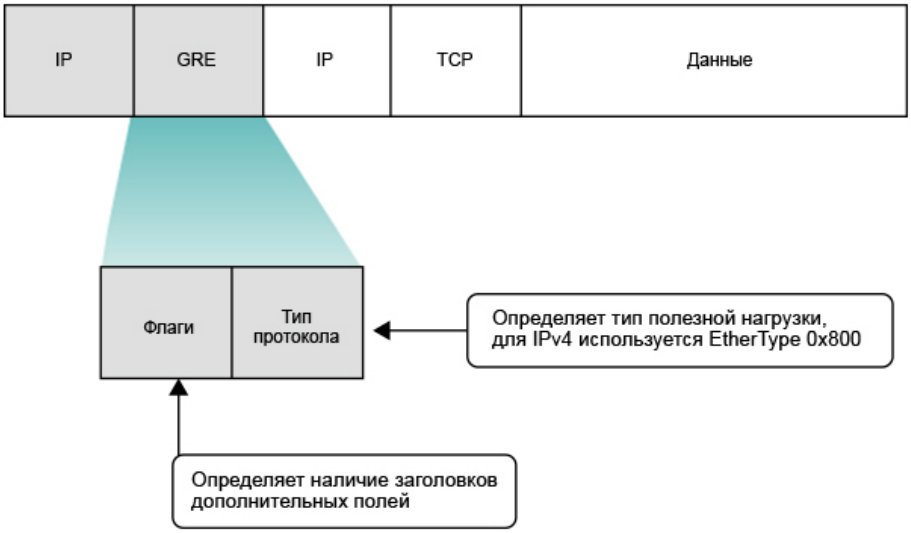


Рисунок 90 – Формат GRE-заголовка

Поле **Флаги** указывает на дополнительные поля, которые могут быть включены в GRE-заголовок.

Поле **Тип протокола** указывает на тип протокола инкапсулированного пакета, например, IPv4 (для этого протокола используется номер 0×800) или IPv6, Ipx и т. д.

Во внешнем заголовке IP в поле протокола используется значение 47, указывающее на то, что за ним будет следовать заголовок GRE.

Достоинством GRE-протокола является то, что в GRE-пакет может быть включен пакет любого протокола сетевого или канального уровня.

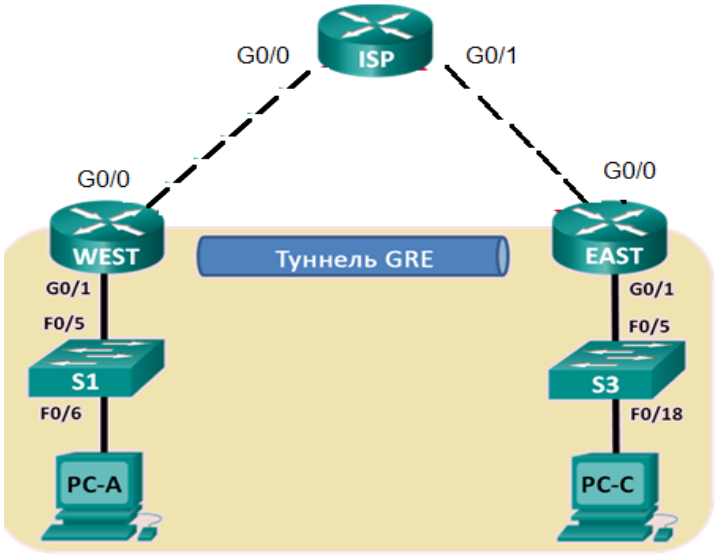
Недостатки протокола:

– создается незащищенный туннель;

– не работает через NAT;

– работает только в IP-сетях.

На рисунке 91 приведены базовая топология организации VPN-туннеля и таблица адресов.



а

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
WEST	G0/1	192.168.1.1	255.255.255.0	Недоступно
	G0/0	64.103.211.2	255.255.255.252	Недоступно
	Tunnel0	10.1.1.1	255.255.255.252	Недоступно
EAST	G0/1	192.168.2.1	255.255.255.0	Недоступно
	G0/0	209.165.122.2	255.255.255.252	Недоступно
	Tunnel0	10.1.1.2	255.255.255.252	Недоступно
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-C	NIC	192.168.2.3	255.255.255.0	192.168.2.1

б

а – базовая топология; б – таблица адресов

Рисунок 91 – Базовая топология и таблица адресов GRE-туннеля

В лабораторной работе необходимо настроить незашифрованный туннель GRE VPN «точка – точка» и убедиться, что сетевой трафик использует туннель. Также будет нужно настроить протокол маршрутизации RIP ver.2 внутри туннеля GRE VPN. Туннель GRE существует между маршрутизаторами WEST и EAST. Интернет-провайдер не знает о туннеле GRE. Для связи между маршрутизаторами WEST и EAST и интернет-провайдером применяются статические маршруты по умолчанию.

Для настройки маршрутов по умолчанию используем команды:

```
WEST(config)# ip route 0.0.0.0 0.0.0.0 64.103.211.1
EAST(config)# ip route 0.0.0.0 0.0.0.0 209.165.122.1
```

Последовательность команд для создания VPN-туннеля приведена на рисунке 92.

Команда	Описание
tunnel mode gre ip	Указывает, что режимом работы интерфейса туннеля является GRE по IP
tunnel source *ip_adress*	Указывает адрес источника туннеля
tunnel description *ip_adress*	Указывает адрес назначения туннеля
ip_adress *ip_adress mask*	Указывает IP-адрес интерфейса туннеля

Рисунок 92 – Команды настройки GRE-туннеля

Последовательность команд для настройки туннеля на маршрутизаторе WEST для базовой топологии имеет следующий вид:

```
WEST(config)# interface tunnel 0
WEST(config-if)# ip address 10.1.1.1 255.255.255.252
WEST(config-if)# tunnel source 64.103.211.2
WEST(config-if)# tunnel destination 209.165.122.2
```

Команды настройки туннеля на маршрутизаторе EAST аналогичны командам маршрутизатора WEST:

```
EAST(config)# interface tunnel 0
EAST(config-if)# ip address 10.1.1.2 255.255.255.252
EAST(config-if)# tunnel source 209.165.122.2
EAST(config-if)# tunnel destination 64.103.211.2
```

Для команды **tunnel source** в качестве источника можно использовать имя интерфейса или IP-адрес.

На следующем этапе необходимо настроить протокол маршрутизации RIPv2 таким образом, чтобы локальные сети (LAN) на маршрутизаторах WEST и EAST могли обмениваться данными с помощью туннеля GRE.

Для GRE-туннеля команда network протокола RIP будет включать сеть IP-туннеля, а не сеть, связанную с интерфейсом маршрутизатора. Следует помнить, что маршрутизатор ISP в этом процессе маршрутизации не участвует.

Настройка протокола динамической маршрутизации RIPv2 на маршрутизаторе WEST для сетей 192.168.1.0/24 и 10.1.1.0/30 имеет следующий вид:

```
WEST(config)# router rip
WEST(config-router)#version 2
WEST(config-router)# network 192.168.1.0
WEST(config-router)# network 10.1.1.0
WEST(config-router)# no auto-summary
```

Настройка протокола RIPv2 на маршрутизаторе EAST для сетей 192.168.2.0/24 и 10.1.1.0/30 происходит следующим образом:

```
EAST(config)# router rip
EAST(config-router)# version 2
```

```
EAST(config-router)# network 192.168.2.0
EAST(config-router)# network 10.1.1.0
EAST(config-router)# no auto-summary
```

На рисунке 93 приведен вид таблицы маршрутизации для маршрутизатора WEST.

```
WEST# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override


C        64.103.211.0/30 is directly connected, Serial0/0/0
L        64.103.211.2/32 is directly connected, Serial0/0/0

C        192.168.1.0/24 is directly connected, GigabitEthernet0/1
L        192.168.1.1/32 is directly connected, GigabitEthernet0/1
R        192.168.2.0/24 [110/1001] via 10.1.1.2, 00:00:07, Tunnel0
C        10.1.1.0/30 is directly connected, Tunnel0
L        10.1.1.1/32 is directly connected, Tunnel0
```

Рисунок 93 – Таблица маршрутизации для маршрутизатора WEST

Как видно, созданный туннель-маршрутизатор видит подключенную к нему сеть напрямую.

ЛАБОРАТОРНАЯ РАБОТА №6

РАБОТА С IPV6-АДРЕСАМИ

Цель работы:
– изучить типы и структуру Ipv6-адресов.

Порядок выполнения работы:

1 Изучить теорию по лабораторной работе.

2 Для заданного преподавателем варианта определить типы IPv6-адресов и отработать правила их сокращенной записи.

3 Защитить лабораторную работу.

Содержание работы

Поскольку пространство сетевых IPv4-адресов сокращается, а IPv6-адреса используются все чаще, сетевым специалистам необходимо понимать, как функционируют сети IPv4 и IPv6. Множество устройств и приложений уже поддерживают протокол IPv6.

Длина IPv6-адреса составляет 128 бит. Чаще всего он состоит из 32 шестнадцатеричных символов. Каждый шестнадцатеричный символ равен 4 битам ($4 \cdot 32 = 128$). Несокращенный IPv6-адрес узла имеет следующий вид:

2001:0DB8:0001:0000:0000:0000:0000:0001

Хекстет – это шестнадцатеричная IPv6-версия октета IPv4. Длина IPv6-адреса составляет восемь хекстетов с разделением точками.

Если читать IPv6-адрес слева направо, то первый (крайний слева) хекстет обозначает тип IPv6-адреса. Например, если в крайнем левом хекстете IPv6-адреса указаны одни нули, то это, скорее всего, адрес логического интерфейса (loopback):

0000:0000:0000:0000:0000:0000:0000:0001 = адрес логического интерфейса

::1 = сокращенный адрес логического интерфейса

Если первый хекстет IPv6-адреса выглядит как FE80, то такой адрес является локальным адресом канала:

FE80:0000:0000:0000:C5B7:CB51:3C00:D6CE = локальный адрес канала

На рисунке 94 показана зависимость значения первого хекстета от типа Ipv6-адреса.

Первый (крайний слева) хекстет	Тип IPv6-адреса
0000 — 00FF	Адрес логического интерфейса, любой адрес, неуказанный адрес или IPv4-совместимый адрес
2000 — 3FFF	Глобальный адрес одноадресной передачи (маршрутизируемый адрес в диапазоне адресов, которые в настоящий момент распределяются администрацией адресного пространства Интернет [IANA])
FE80 — FEBF	Локальный адрес канала (адрес одноадресной передачи, идентифицирующий главный компьютер в локальной сети)
FC00 — FCFF	Уникальный локальный адрес (такие адреса аналогичны частным адресам протокола IPv4)
FF00 — FFFF	Многоадресная рассылка

Рисунок 94 – Основные типы Ipv6-адресов

Существуют и другие типы IPv6-адресов, которые еще не нашли широкого применения или уже устарели, либо более не поддерживаются. Например, адреса anycast это новый тип IPv6-адресов, которые могут использоваться маршрутизаторами для распределения нагрузки и поиска альтернативных путей, если маршрутизатор становится недоступным. На адреса anycast должны реагировать только маршрутизаторы. В свою очередь уникальные локальные адреса теряют свою актуальность и постепенно вытесняются уникальными локальными адресами. В IPv6-сетях не используются широковещательные адреса, которые применяются в IPv4-сетях, – вместо них используются групповые адреса (таблица 1).

Таблица 1 – Различные типы Ipv6-адресов

IPv6-адрес	Ответ
2001:0DB8:1:ACAD::FE55:6789:B210	1. ____
::1	2. ____
FC00:22:A:2::CD4:23E4:76FA	3. ____
2033:DB8:1:1:22:A33D:259A:21FE	4. ____
FE80::3201:CC01:65B1	5. ____
FF00::	6. ____
FF00::DB7:4322:A231:67C	7. ____
FF02::2	8. ____

Варианты ответов:

а) адрес обратной связи;

б) глобальный адрес одноадресной передачи;

в) локальный адрес канала;

г) уникальный локальный адрес;

д) многоадресная рассылка.

Для закрепления знаний о типах адресов необходимо сопоставить IPv6-адрес, приведенный в таблице 1, с его типом. Следует отметить, что если операционная система сетевого устройства или компьютера поддерживает

протокол IPv6, то любому сетевому интерфейсу устройства автоматически назначается локальный канальный Ipv6-адрес.

Существуют два правила сокращенной записи Ipv6-адресов.

Правило 1 В IPv6-адресе гекстет, состоящий из четырех нулей, можно сократить до одного нуля:

2001:0404:0001:1000:**0000:0000**:0EF0:BC00

2001:0404:0001:1000:**0**:**0**:0EF0:BC00 (четыре нуля сокращены до одного)

Правило 2 В IPv6-адресе начальные нули в каждом гекстете можно опустить, в то время как конечные нули опускать нельзя:

2001:0404:0001:1000:0000:0000:0EF0:BC00

2001:404:1:1000:0:0:EF0:BC00 (опущены начальные нули)

Примеры правил сокращенной записи адресов представлены на рисунке 95.

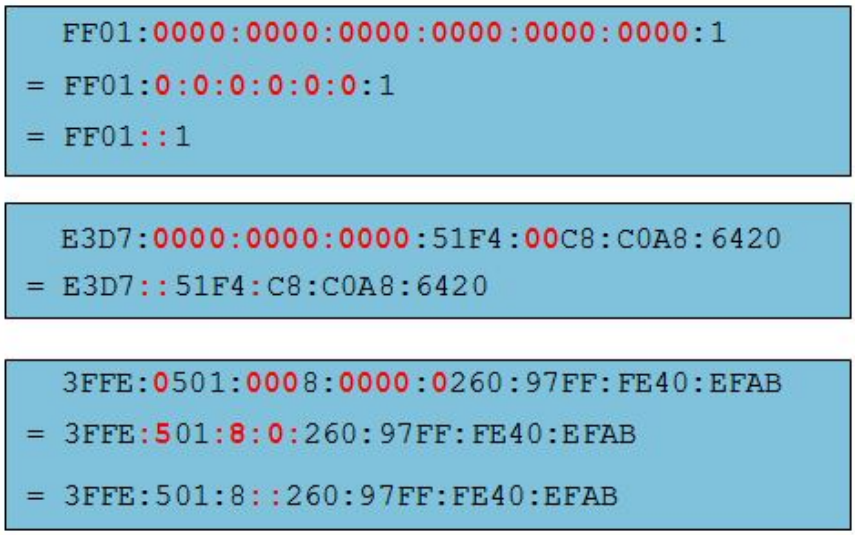


Рисунок 95 – Примеры сокращенной записи IPv6-адресов

IPv6-адрес представляет собой 128-битный адрес, состоящий из двух частей: сетевой части, которая определяется первыми 64 битами (или первыми четырьмя хекстетами), и узловой части, которая определяется последними 64 битами (или последними четырьмя хекстетами). Типичный глобальный адрес одноадресной передачи выглядит так:

сетевая часть: **2001:DB8:0001:ACAD:xxxx:xxxx:xxxx:xxxx**
узловая часть: **xxxx:xxxx:xxxx:xxxx:0000:0000:0000:0001**

В большинстве адресов одноадресной передачи (маршрутизируемых адресов) используется 64-битный сетевой префикс и 64-битный адрес узла. При этом длина сетевой части IPv6-адреса не ограничивается 64 битами, а обозначается косой чертой в конце адреса, после которой следует десятичное число, обозначающее длину.

Если сетевой префикс имеет вид /64, значит, длина сетевой части IPv6-адреса при чтении слева направо равна 64 битам. Оставшуюся длину IPv6-адреса составляет узловая часть (идентификатор интерфейса), представленная последними 64 битами. В некоторых случаях, например в адресах логического интерфейса, сетевой префикс может иметь вид /128, т. е. длину 128 бит. В этом случае для идентификатора интерфейса битов не остается, а значит, сеть ограничена одним узлом. Примеры адресов с различными префиксами приведены в таблице 2.

Таблица 2 – Примеры Ipv6-адресов с различными префиксами

Глобальный адрес одноадресной передачи	2001:DB8:0001:ACAD:0000:0000:0000:0001/64
Адрес логического интерфейса	::1/128
Адрес многоадресной рассылки	FF00::/8
Адрес для всех сетей	::/0 (аналогично адресу из четырех нулей в IPv4)
Локальный адрес канала	fe80::8d4f:4f4d:3237:95e2%14 (обратите внимание на то, что значение /14 в конце адреса представлено в виде символа процентов и десятичного числа 14.Этот адрес взят из результатов выполнения команды ipconfig /all в окне командной строки Windows)

Слева направо сетевая часть глобального IPv6-адреса одноадресной передачи имеет иерархическую структуру, из которой можно получить следующую информацию:

1 Глобальный номер маршрутизации IANA (первые три двоичных бита имеют фиксированное значение 001):

200::/12

2 Префикс регионального реестра Интернет (RIR) (биты с /12 до /23):

200**1:0D**::/23

Примечание – Шестнадцатеричный символ D в двоичной системе имеет вид 1101. Биты с 21 по 23 – это 110, а последний бит является частью префикса интернет-провайдера.

3 Префикс интернет-провайдера (биты до /32):

2001:0D**B8**::/32

4 Префикс организации или идентификатор агрегата уровня организации (SLA), присваиваемый клиенту интернет-провайдером (биты до /48):

2001:0DB8:**0001**::/48

5 Префикс подсети (присваивается клиентом; биты до /64):

2001:0DB8:0001:**ACAD**::/64

6 Идентификатор интерфейса (узел определяется последними 64 битами в адресе):

2001:DB8:0001:ACAD:**8D4F:4F4D:3237:95E2**/64

На приведенном ниже рисунке 96 показано, что IPv6-адрес можно разделить на четыре основные части:

– глобальный префикс маршрутизации – /32;

– идентификатор агрегата уровня организации (SLA) – /48;

– идентификатор подсети (LAN) – /64;

– идентификатор интерфейса (последние 64 бита).

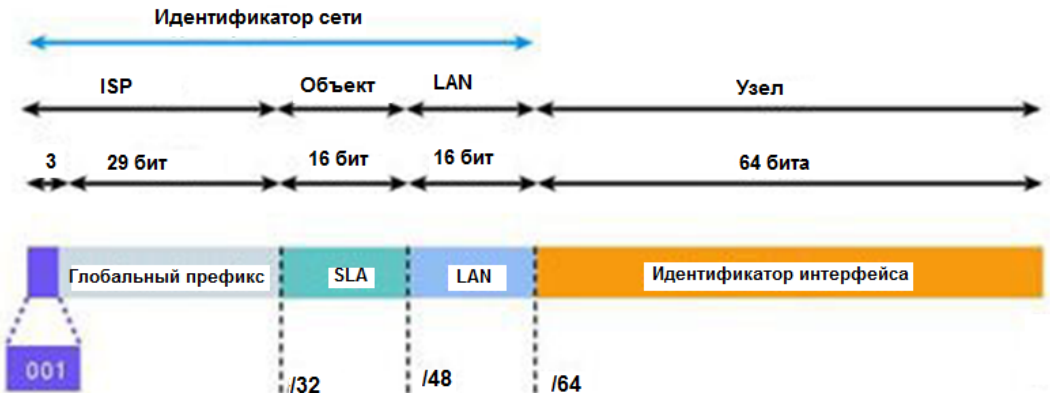
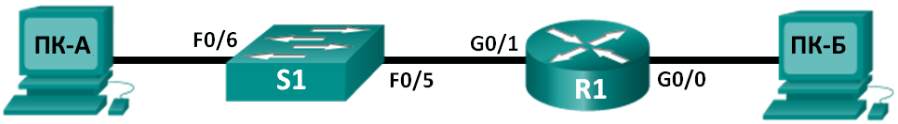


Рисунок 96 – Префиксы Ipv6-адресов

В качестве примера назначения Ipv-адресов рассмотрим топологию на рисунке 97.



Устройство	Интерфейс	IPv6-адрес	Длина префикса	Шлюз по умолчанию
R1	G0/0	2001:DB8:ACAD:A::1	64	Недоступно
	G0/1	2001:DB8:ACAD:1::1	64	Недоступно
S1	VLAN 1	2001:DB8:ACAD:1::B	64	Недоступно
ПК-А	Сетевой адаптер	2001:DB8:ACAD:1::3	64	FE80::1
ПК-Б	Сетевой адаптер	2001:DB8:ACAD:A::3	64	FE80::1

Рисунок 97 – Топология и таблица адресов IPv6-сети

Необходимо назначить адреса следующим образом: в левой части сети вручную назначаются статические адреса, а в правой – автоматически с помощью протокола SLAAC.

Вначале назначим глобальные IPv6-адреса одноадресной передачи из таблицы маршрутизации каждому из двух интернет-интерфейсов маршрутизатора R1:

```
R1(config)# interface g0/0
R1(config-if)# ipv6 address 2001:db8:acad:a::1/64
R1(config-if)# no shutdown
```

R1(config-if)# **interface g0/1**

R1(config-if)# **ipv6 address 2001:db8:acad:1::1/64**

R1(config-if)# **no shutdown**

Просмотрим назначенные адреса:

R1# **show ipv6 interface g0/0**

GigabitEthernet0/0 is up, line protocol is up

IPv6 is enabled, link-local address is FE80::D68C:B5FF:FECE:A0C0

No Virtual link-local address(es):

Global unicast address(es): 2001:DB8:ACAD:A::1, subnet is 2001:DB8:ACAD:A::/64

Joined group address(es):

FF02::1

FF02::1:FF00:1

FF02::1:FFCE:A0C0

Примечание – Выделенным цветом обозначен локальный канальный адрес, назначенный интерфейсу маршрутизатора автоматически.

Далее активируем IPv6-маршрутизацию на маршрутизаторе R1 с помощью команды IPv6 unicast-routing:

R1(config)# ipv6 unicast-routing

На ПК-В в настройках протокола Ipv6 выберем пункт. **Получить адрес автоматически.** В результате ПК-В получит сетевую часть Ipv6-адреса по протоколу SLAAC с интерфейса g0/0 маршрутизатора, а узловая часть добавится автоматически в виде случайно сгенерированного числа. При этом в качестве шлюза по умолчанию будет являться локальный канальный адрес интерфейса g0/0 маршрутизатора.

На ПК-А зададим статический Ipv6-адрес, как показано на рисунке 98.

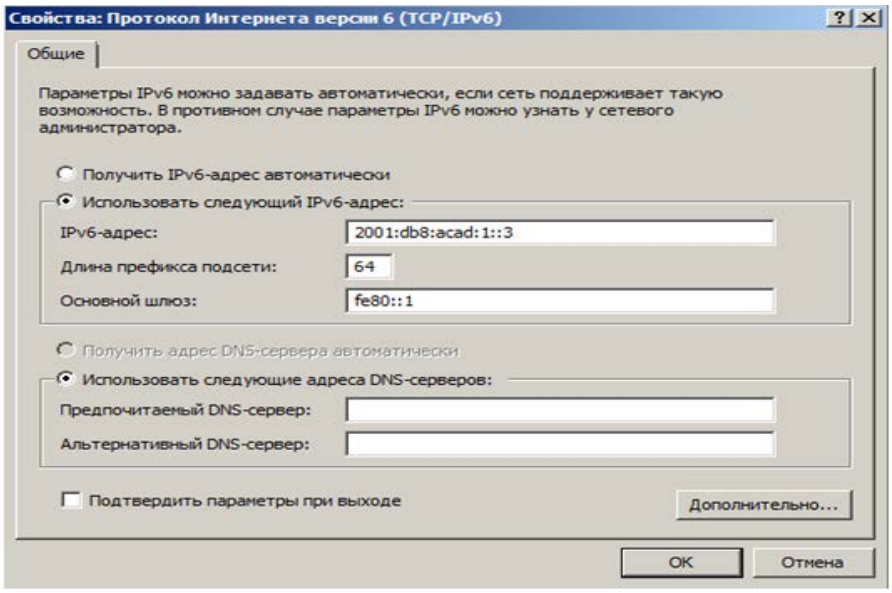


Рисунок 98 – Назначение статического адреса ПК-А

После этого можно проверить связь между компьютерами с помощью команды ping.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Таненбаум, Э. Компьютерные сети / Э. Таненбаум. – СПб. : Питер, 2019. – 960 с.

2 Олифер, В. Компьютерные сети: принципы, технологии, протоколы : учебник / В. Олифер, Н. Олифер. – СПб. : Питер, 2018. – 992 с.

3 Одом, У. Официальное руководство Cisco по подготовке к сертификационным экзаменам ccent/ccna icnd1 100-101 / У. Одом. – М. : Вильямс, 2017. – 912 с.

4 Одом, У. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCNA ICND2 200-105. Маршрутизация и коммутация / У. Одом. – М. : Вильямс, 2018. – 1008 с.

5 Куроуз, Д. Ф. Компьютерные сети. Нисходящий подход / Д. Ф. Куроуз, К. В. Росс. – М. : Эксмо, 2016. – 912 с.

6 Смелянский, Р. Л. Компьютерные сети. В 2 ч. Ч. 2 : Сети ЭВМ / Р. Л. Смелянский. – М. : Академия, 2011. – 240 с.