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

Факультет инфокоммуникаций

Кафедра защиты информации

Е. С. Белоусова

МАРШРУТИЗАЦИЯ В IPV4- И IPV6-СЕТЯХ. ЛАБОРАТОРНЫЙ ПРАКТИКУМ

Рекомендовано УМО по образованию в области информатики и радиоэлектроники в качестве учебно-методического пособия для специальности 1-98 01 02 «Защита информации в телекоммуникациях»

Минск БГУИР 2022

УДК 004.71(076.5)
ББК 32.971.3я73
Б43

Р е ц е н з е н т ы:

кафедра телекоммуникационных систем
учреждения образования «Белорусская государственная академия связи»
(протокол № 5 от 23.12.2020);

ведущий научный сотрудник
научно-исследовательской лаборатории факультета связи и АСУ
учреждения образования «Военная академия Республики Беларусь»
кандидат технических наук, доцент А. В. Хижняк

Белоусова, Е. С.

Б43 Маршрутизация в IPv4- и IPv6-сетях. Лабораторный практикум учеб.-метод. пособие / Е. С. Белоусова. – Минск : БГУИР, 2022. – 102 с. : ил.
ISBN 978-985-543-639-4.

Состоит из восьми лабораторных работ, содержащих краткие теоретические сведения, описание хода выполнения лабораторного задания, вопросы для самоконтроля, ответы на которые оцениваются программной экспертной системой.
Предназначено для студентов, изучающих дисциплину «Компьютерные сети».

УДК 004.71(076.5)
ББК 32.971.3я73

ISBN 978-985-543-639-4

СОДЕРЖАНИЕ

ЛАБОРАТОРНАЯ РАБОТА № 1 ЛОКАЛЬНЫЕ СЕТИ С IP-ВИДЕОНАБЛЮДЕНИЕМ 5
1.1 Теоретическая часть 5
1.2 Лабораторное задание 14
1.3 Содержание отчета 17
1.4 Контрольные вопросы и задания 17
ЛАБОРАТОРНАЯ РАБОТА № 2 СТАТИЧЕСКАЯ МАРШРУТИЗАЦИЯ 18
2.1 Теоретическая часть 18
2.2 Лабораторное задание 27
2.3 Содержание отчета 29
2.4 Контрольные вопросы и задания 30
ЛАБОРАТОРНАЯ РАБОТА № 3 ДИСТАНЦИОННО-ВЕКТОРНЫЕ ПРОТОКОЛЫ МАРШРУТИЗАЦИИ 31
3.1 Теоретическая часть 31
3.2 Лабораторное задание 37
3.3 Содержание отчета 38
3.4 Контрольные вопросы и задания 38
ЛАБОРАТОРНАЯ РАБОТА № 4 ПРОТОКОЛ МАРШРУТИЗАЦИИ ПО СОСТОЯНИЮ КАНАЛА 39
4.1 Теоретическая часть 39
4.2 Лабораторное задание 53
4.3 Содержание отчета 56
4.4 Контрольные вопросы и задания 56
ЛАБОРАТОРНАЯ РАБОТА № 5 МАРШРУТИЗАЦИЯ В СЕТЯХ IPV6 57
5.1 Теоретическая часть 57
5.2 Лабораторное задание 68
5.3 Содержание отчета 69
5.4 Контрольные вопросы и задания 69
ЛАБОРАТОРНАЯ РАБОТА № 6 ПРОТОКОЛЫ МАРШРУТИЗАЦИИ RIPNG И EIGRP 70
6.1. Теоретическая часть 70
6.2 Лабораторное задание 75
6.3 Содержание отчета 76
6.4 Контрольные вопросы и задания 76
ЛАБОРАТОРНАЯ РАБОТА № 7 ПРОТОКОЛ IPV6-МАРШРУТИЗАЦИИ OSPFV3 77
7.1 Теоретическая часть 77
7.2 Лабораторное задание 83
7.3 Содержание отчета 85
7.4 Контрольные вопросы и задания 85

ЛАБОРАТОРНАЯ РАБОТА № 8 АГРЕГАЦИЯ МАРШРУТОВ 86
8.1 Теоретическая часть..... 86
8.2 Лабораторное задание 90
8.3 Содержание отчета..... 99
8.4 Контрольные вопросы и задания 99
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ 100

ЛАБОРАТОРНАЯ РАБОТА № 1
ЛОКАЛЬНЫЕ СЕТИ С IP-ВИДЕОНАБЛЮДЕНИЕМ

Цель: изучить устройство IP-видеокамеры, структуру системы видеонаблюдения, особенности ее построения; овладеть навыками конфигурирования локальных сетей с IP-видеонаблюдением.

1.1 Теоретическая часть

Использование современных цифровых систем видеонаблюдения позволяет получить значительный экономический эффект при обеспечении безопасности территориально распределенных объектов за счет автоматизации передачи изображений по компьютерной сети.

Структурно система видеонаблюдения состоит из [1]:

- IP-камеры – устройства, формирующего видеоизображение;
- транспортной сети, распределяющей и передающей сигналы на устройства сети;
- центрального оборудования, записывающего, управляющего и воспроизводящего видеоизображение.

IP-камера состоит из следующих частей: объектива, фильтра, CDD-матрицы (ПЗС-матрицы), устройства видеозахвата, блока сжатия (компрессии) изображения, интегрированного IP-сервера, управляющего процессора, оперативной памяти, флеш-памяти, интерфейса сетевого подключения, порта вывода видео- и аудиоданных, блока входов и выходов различных сигналов (рисунок 1.1).

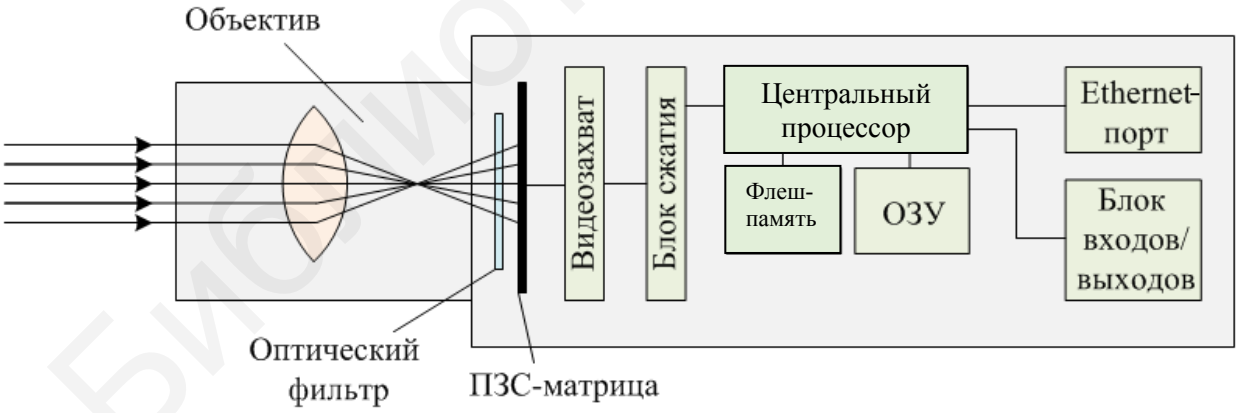


Рисунок 1.1 – Устройство IP-камеры видеонаблюдения

В роли принимающего световые колебания устройства выступает **CDD-матрица** – пластина, состоящая из светочувствительных ячеек. Именно от их количества зависит качество передаваемого изображения, разрешение IP-камеры. CDD-матрица преобразует свет, попадающий на нее, в электрический сигнал.

Устройство видеозахвата преобразует аналоговый электрический сигнал, поступающий от матрицы, в цифровой. Это происходит в три этапа: считывание и дискретизация, квантование и усиление и непосредственно кодирование.

Блок компрессии производит сжатие кодированного сигнала в один из форматов для последующей передачи по сети. Этот процесс может происходить одновременно аппаратно и программно, что обходится дешевле, но не так эффективно.

Процессор выводит оцифрованный и сжатый видеосигнал и контролирует работу интегрированного сервера и других управляющих программ. Передача изображения происходит через Ethernet порт.

Флеш-память позволяет хранить пользовательские настройки управляющих программ, может использоваться для резервного сохранения и дополнительной буферизации видео.

ОЗУ временно сохраняет данные, генерирующиеся при выполнении различных функций, заложенных в программу управления камерой.

Транспортная сеть состоит из пассивных и активных элементов. К пассивным элементам относятся кабельные линии связи, а к активным – коммутаторы. В транспортных сетях систем IP-видеонаблюдения используются кабельные линии двух видов: на основе UTP-кабеля категории 5 или 6 (витой пары) и на основе оптоволокна. Кабель UTP подходит для небольших расстояний, не более 90 м. Волоконно-оптический кабель применяют на больших расстояниях между коммутаторами или там, где по каким-либо причинам нельзя использовать кабель UTP [1].

Видеокамеры могут подключаться к различным сетям несколькими способами, в зависимости от стандартов передачи данных.

Подключение 100Ethernet происходит с помощью разъема RJ45 с использованием витой пары категорий 4, 5, 5e. Этот способ наиболее распространен в настоящее время из-за низкой стоимости и подходит для сетей, в которых используется не более 10–15 камер.

При построении сетей GigabitEthernet используется кабель 6 и 6A категорий. Кроме передачи данных с большого количества камер, возможна передача и другой информации этим способом.

Оптимальной представляется реализация транспортной сети по принципам отказоустойчивой иерархической модели, состоящей из трех уровней [1]:

- уровня доступа (access layer);
- уровня распределения (distribution layer);
- уровня ядра (core layer).

Основная задача уровня доступа – предоставляя порты, обеспечивать доступ к сети конечным устройствам и пользователям. Коммутаторы уровня доступа должны осуществлять контроль доступа к сети (Network Access Control, NAC),

управление качеством обслуживания (QoS), поддерживать отслеживание сетевого трафика IGMP (IGMP snooping) и разделение трафика по виртуальным локальным сетям (VLAN). Коммутаторы, используемые в системах IP-видеонаблюдения, должны иметь функцию PoE (Power over Ethernet), позволяющую запитывать IP-камеры по сигнальному кабелю, и порты SFP (Small Form-factor Pluggable) для подключения других коммутаторов по оптическим интерфейсам [1].

Стандарт IEEE 802.3af-2003 PoE регламентирует напряжение питания мощностью до 15,4 Вт по витым парам для каждого устройства. С учетом возможных потерь в кабеле, максимальная длина которого может достигать 100 м, мощность уменьшается приблизительно до 13 Вт. В более поздней редакции стандарта, IEEE 802.3at-2009, известной также как PoE+, мощность порта была повышена до 25,5 Вт [74].

Достаточно ли мощности порта коммутатора для работы видеокамеры, можно определить, оценив соответствие спецификаций производителя сетевого оборудования и потребляемой мощности. Последний показатель указан в технических характерисках камеры.

Уровень распределения отвечает за связь между уровнями доступа и ядра, осуществляет выполнение различных политик безопасности и управления сетью. Коммутаторы уровня распределения должны иметь возможность агрегировать каналы для увеличения пропускной способности и надежности сети, распределять нагрузку между параллельными каналами и перераспределять трафик в случае выхода канала из строя, а также маршрутизировать трафик на третьем уровне.

Ядро представляет собой выделенную магистраль. Оно должно обеспечивать высокую производительность и отказоустойчивость сети, распределяя трафик между ее сегментами [1].

В больших распределенных системах для уменьшения коллизий, ограничения и регулирования трафика прибегают к сегментированию сетей с помощью VLAN. Отдельные сегменты сети выделяются по функциональному принципу и строятся как самостоятельные блоки.

Функциональный блок, отвечающий за запись и хранение видеопотоков (рисунок 1.2), реализуется таким образом, чтобы IP-камеры и сетевой регистратор (Network Video Recorder, NVR) располагались в одном VLAN-сегменте и как можно ближе друг к другу. Это позволяет локализовать трафик видео высокого разрешения. Оптимален вариант, когда весь трафик проходит через один коммутатор. При расчете данного блока нужно учесть сумму максимального битрейта от всех камер и убедиться, что коммутатор и сетевой регистратор смогут его обработать. В случае удаленного расположения сетевого регистратора, когда трафик проходит через несколько коммутаторов, необходимо также убедиться в достаточной ширине канала до NVR.

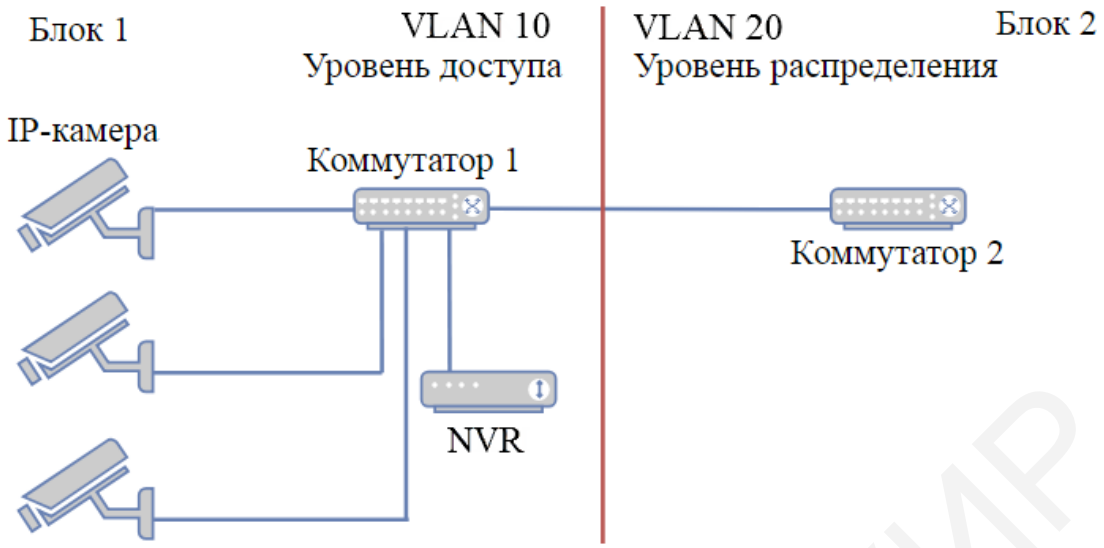


Рисунок 1.2 – Система IP-видеонаблюдения с возможностью записи и хранения видеопотоков

Функциональный блок на рисунке 1.3 отвечает за декодирование и вывод видеопотоков на мониторы операторов, а также за настройку и управление всеми компонентами системы IP-видеонаблюдения через автоматизированное рабочее место.

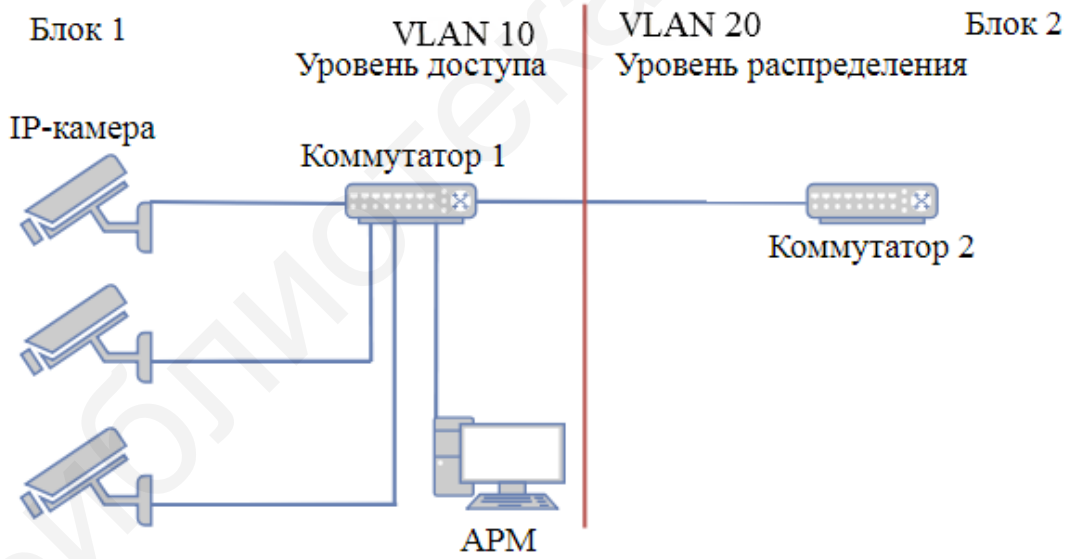


Рисунок 1.3 – Система IP-видеонаблюдения с возможностями настройки и управления компонентами

Через интерфейс АРМ администратор настраивает систему, осуществляет удаленное управление камерами, выбирает те, изображение с которых будет выводиться на мониторы, посылает запросы на просмотр видеоархива.

Блок, представленный на рисунке 1.4, отвечает за связь между первыми двумя функциональными блоками, обеспечивая маршрутизацию, логическую адресацию, инкапсуляцию и другие функции третьего уровня сети. В этот блок

входит сервер управления системой, который осуществляет администрирование всех ее компонентов. Он отслеживает присутствие устройств в сети, обеспечивает аутентификацию устройств и пользователей, раздает IP-адреса, поддерживает связь и синхронизацию между устройствами в сети, а также содержит базу всех настроек системы [1].

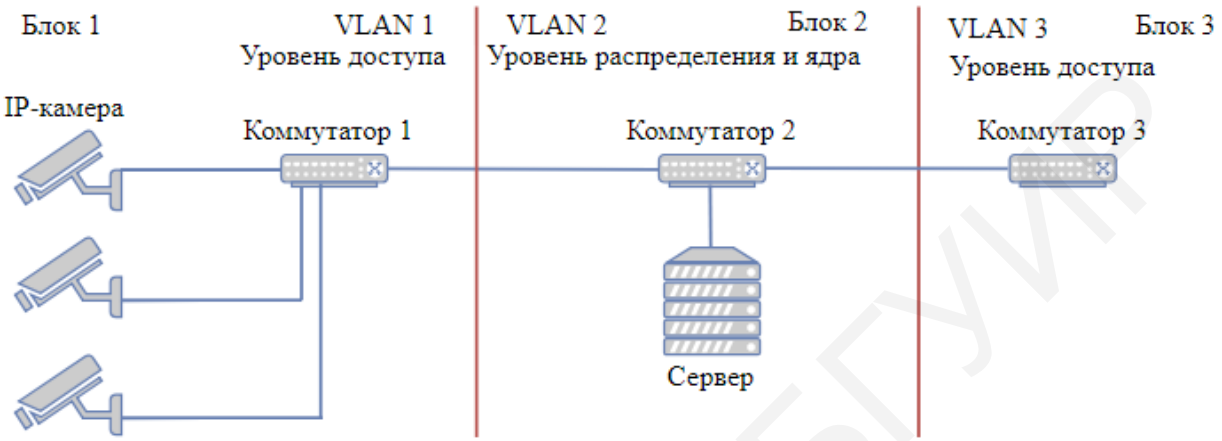


Рисунок 1.4 – Система IP-видеонаблюдения с функцией маршрутизации

В роли клиента может выступать любой компьютер, подключенный к сети и получающий потоки данных с видеосерверов, декомпрессирующий видеоизображение и выводящий его на монитор [3]. В настоящее время широкое распространение начали получать IP-камеры, представляющие собой видеосервер, интегрированный с видеокамерой. В зависимости от функциональных возможностей IP-камеры клиент может получать потоки данных как напрямую (посредством протокола семейства IP), так и через специальный видеосервер.

Основные критерии оценки качества распределенной системы цифрового видеонаблюдения – величина временной задержки между каким-либо событием, произошедшим перед видеокамерой, и моментом его отображения на экране клиента, а также количество кадров в секунду. Оба параметра зависят от пропускной способности сети и производительности сервера и клиента. Следует подчеркнуть: процессы компрессии/декомпрессии видео играют значительную роль, поэтому, если в глобальных сетях важна пропускная способность канала, то в локальных сетях слабым звеном зачастую становятся ограниченные вычислительные мощности отдельных компьютеров.

В системах видеонаблюдения общего пользования (рисунок 1.5) в качестве клиента может быть использован любой компьютер, поэтому вследствие ограниченности возможностей отдельных моделей реальная скорость вывода видео на экран может снижаться до 4 кадров/с при возможных 25 кадрах/с. В

этом случае нет смысла передавать клиенту кадры, которые он не в состоянии обработать: требуется механизм прореживания кадров на уровне сервера.

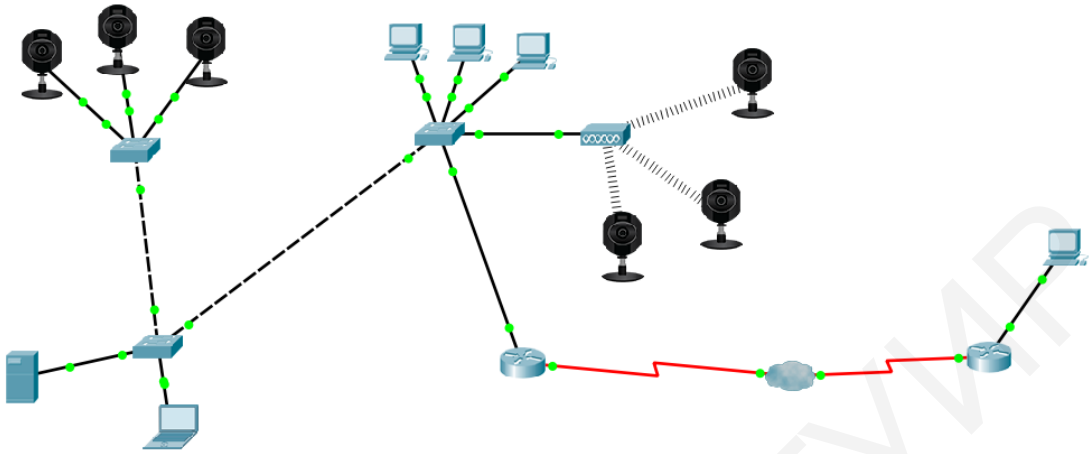


Рисунок 1.5 – Территориально распределенная многопользовательская система видеонаблюдения

Ethernet-коммутаторы способны отчасти решить проблемы коллизий, однако при высокой нагрузке на каждый порт неизбежно накопление очередей в буферах коммутаторов и серверов, а значит, задержки и потери даже в пределах локальной сети. Размер одного компрессированного видеокадра обычно составляет несколько килобайт, и при передаче по сети происходит его разбиение на несколько пакетов. Потеря одного пакета, представляющего кусочек компрессированного кадра, приведет к искажению реальной картинки: она необязательно будет повреждена целиком (существуют механизмы восстановления растрового изображения из компрессированного), однако потери качества восстановленного изображения окажутся в процентном соотношении больше, чем потери данных в компрессированном изображении. В случае если клиент успевает обрабатывать изображение с камеры со скоростью 25 кадров/с, можно просто отбросить «битый» кадр, однако на скорости 4 кадра/с его потеря будет весьма заметна. Следовательно, при низких скоростях вывода видео на экран необходимо предусмотреть механизм повторной посылки потерянных кадров.

Стандартные методы передачи видеопотоков по компьютерным сетям основываются на использовании протокола UDP, позволяющего организовывать одновременную передачу данных множеству клиентов (multicast), занимающего меньшую – по сравнению с протоколом TCP – часть пропускной способности, но не гарантирующего качество доставки и правильность порядка передачи данных. Порядок передачи данных реализуется на уровне приложения за счет буферизации входящего трафика и его пересортировки. Потерянные пакеты обычно не пересылают-

ся; вместо этого используются алгоритмы восстановления потерянной информации и механизмы регуляции скорости передачи данных.

По сравнению с UDP протокол TCP/IP обеспечивает регулирование скорости передачи данных в зависимости от загруженности канала связи, правильный порядок и повторную посылку потерянных данных. Основным аргументом в пользу UDP выступает возможность организации многоадресной рассылки видео множеству клиентов.

Для того чтобы оценить важность этой функции, рассмотрим основные случаи построения распределенной системы видеонаблюдения [3]:

- один клиент получает видеопотоки с одного сервера;
- несколько клиентов получают одинаковые видеопотоки с одного сервера;
- несколько клиентов получают разные видеопотоки с одного сервера;
- несколько клиентов получают разные видеопотоки с разных серверов.

Использование многоадресной рассылки с точки зрения уменьшения сетевого трафика выгодно только во втором случае, который по структуре соответствует принципам организации видеоконференций. В системах видеонаблюдения общего пользования наиболее распространены третий и четвертый варианты, поскольку выборки камер (из множества других, подключенных к серверу) для просмотра на компьютерах-клиентах делаются в зависимости от желания пользователей и чаще всего распределяются не по территориальному, а по тематическому признаку. Следовательно, в общем случае видеопотоки, адресованные различным клиентам, не будут совпадать друг с другом как по содержанию, так и по скорости.

При готовности к обработке нового видеокадра клиент отправляет запрос серверу, который в ответ посылает один кадр и переходит в состояние ожидания. Этот простой механизм хорошо работает на низких скоростях, что делает его удобным для камер. Однако он не в состоянии эффективно использовать вычислительные ресурсы клиента на высоких скоростях: неизбежен простой процесса декомпрессии во время ожидания нового кадра. Это приводит к большой задержке между реальным событием и его отображением, а также к снижению скорости вывода на экран.

Избежать простоя процесса декомпрессии можно следующим образом: так как используется протокол TCP/IP, то время окончания приема кадра клиентом примерно совпадает с моментом окончания передачи этого кадра на сервере. При этом после передачи предыдущего кадра сервер должен начать передачу нового. В этом случае клиент уже не посылает запрос на получение кадра, а вместо этого единожды «подписывается» на получение потока кадров. Чтобы пояснить, как происходит регуляция скорости в этом случае, рассмотрим одну из особенностей работы протокола TCP/IP (рисунок 1.6).

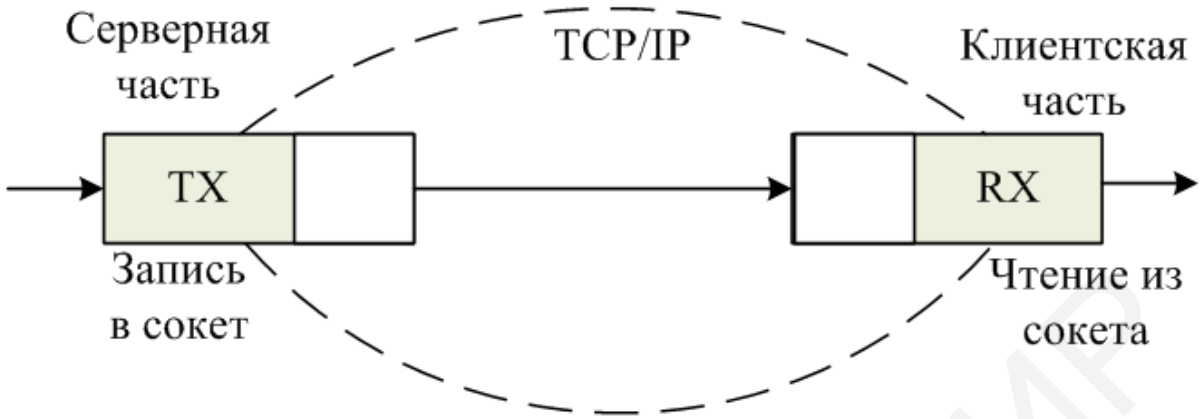


Рисунок 1.6 – Передача данных от сервера клиенту (TX и RX – буферы передачи и чтения соответственно)

С точки зрения программной реализации видеосервера процесс передачи данных по сети выглядит как запись этих данных в соответствующий сокет (дескриптор соединения) [3]. При этом данные помещаются в буфер передачи, расположенный на сервере, и, далее, средствами протокола, в буфер приема, находящийся на клиенте. Клиент получает данные в процессе чтения из буфера приема, и если он будет считывать информацию медленнее, чем сервер будет записывать данные в свой буфер передачи, то буфер приема заполнится, далее заполнится буфер передачи, и попытка записи в него новых данных будет приводить к ошибке.

Таким образом, уменьшение скорости чтения клиентом из буфера чтения приводит к уменьшению скорости передачи новых кадров сервером и наоборот, увеличение скорости чтения ведет к увеличению скорости передачи. Основная трудность при реализации этого метода заключается в ограничении скорости чтения из буфера клиента.

Рассмотрим упрощенную схему архитектуры программы-клиента (рисунок 1.7).

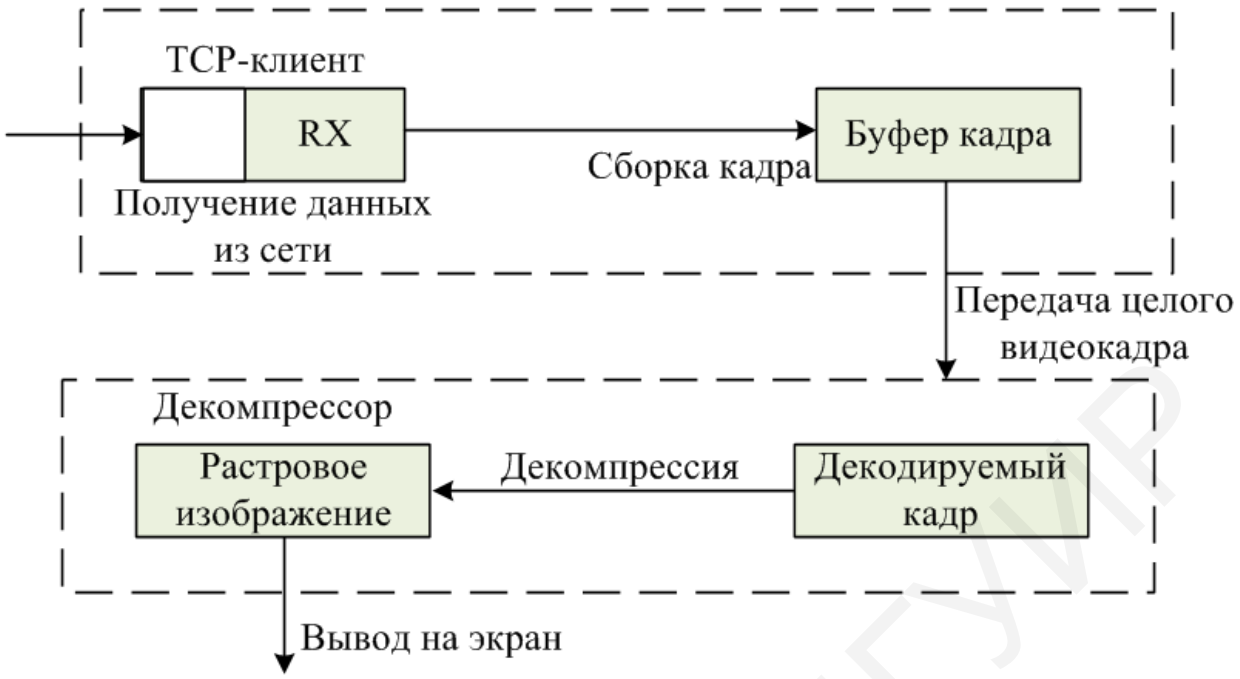


Рисунок 1.7 – Просмотр видео с одной камеры

Для обработки видео с одной камеры запускается два потока, выполняющихся параллельно, – TCP-клиент и декомпрессор. TCP-клиент читает данные из буфера, группирует их в кадры и передает декомпрессору. Декомпрессор осуществляет декомпрессию кадров и вывод их на экран. Для обработки видео с двух и более камер запускается по одному потоку декомпрессии на каждую из камер и общий поток чтения данных из всех сокетов соединений. Когда какой-либо поток декомпрессии не успевает обрабатывать все поставляемые ему кадры, поток чтения должен приостановить чтение из соответствующего сокета. Чтение можно остановить после получения какой-то части следующего кадра или после полного завершения приема кадра, передаваемого декомпрессору. В первом случае при возобновлении чтения придется вычитать остатки возможно уже устаревшего кадра (это может произойти при высокой скорости захвата кадров на сервере и низкой скорости обработки кадров клиентом). Во втором случае кадр, полученный после возобновления чтения, также будет устаревшим, поскольку сервер по окончании передачи одного кадра автоматически начнет отправку следующего. В обоих случаях будет возникать задержка между событием и его отображением. Кроме того, вследствие неравномерности распределения вычислительных ресурсов компьютера-клиента между процессами, при высокой нагрузке на процессор скорость обработки кадров декомпрессором меняется в широких пределах, что приводит к «рывкам» выводимого на экран видеопотока.

IP-видеокамеры используют в своей работе множество сетевых протоколов, необходимых как для передачи видеопотока по сети, так и для дистанционного управления камерой. Кроме выше перечисленных используются протоколы DHCP, DNS, NTP, ICMP, SMPT, FTP, HTTP и др.

При включенных службах динамической адресации возможно устанавливать большое число камер без выделения для них отдельных IP-адресов в пределах пула локальной вычислительной сети. При этом с помощью переадресации портов на маршрутизаторе можно обеспечить доступ к видеопотоку каждой камеры.

RTP (Real-time Transport Protocol) – протокол для передачи данных в реальном времени с контролем последовательности пакетов и синхронизации данных. Данный протокол хорошо подходит для видео- и аудиоданных, передаваемых по сети.

RTSP (Real Time Streaming Protocol) – протокол, предназначенный для управления данными мультимедиаустройств, например, IP-камер, с возможностью передачи команд «старт», «запись», «стоп» и т. п.

RTCP (Real-Time Transport Control Protocol) – протокол передачи управляющих пакетов в реальном времени, работающий совместно с RTP, обеспечивающий обратную связь и контроль качества передачи данных.

IGMP (Internet Group Management Protocol) – протокол, позволяющий организовывать сетевые устройства в группы при помощи маршрутизатора, например, для передачи данных от видеосервера к многочисленным клиентам, принимающим видеотрансляцию.

1.2 Лабораторное задание

Лабораторная работа выполняется на основе настроек, произведенных в лабораторной работе № 8 предыдущего семестра [26]. До начала выполнения необходимо открыть сохраненный файл с именем **Lab8.pkt**, полученный в лабораторной работе № 8, и проверить правильность соединений. По результатам выполнения данной лабораторной работы все устройства должны иметь доступ к серверу, на котором должны отображаться статусы всех IoT-устройств и условия их работы. Доступ к серверу должен осуществляться посредством DNS.

В данной лабораторной работе необходимо организовать ограничение доступа, исходя из следующих заданий.

1. Реализовать систему видеонаблюдения:

1.1. Добавить и подключить видеокамеры, количество и тип соединения которых указаны в таблице 1.1.

Таблица 1.1 – Количество проводных и беспроводных камер

Вторая цифра шифра	Количество камер	
	с проводным соединением	с беспроводным соединением
1	5	6
2	4	7
3	8	3
4	6	5
5	7	4
6	8	3
7	9	2
8	8	3
9	5	6
0	2	9

1.2. Осуществить автоматическое присвоение IP-адресов камерам. Все видеокамеры должны находиться в отдельном VLAN. Реализовать отображение данных с видеокамер на сервере и возможность подключения к серверу для просмотра видеопотока с других устройств из других сетей (см. рисунок 1.5). Результат отразить в отчете.

1.3. Добавить в сеть не менее четырех детекторов движения и сирен (Siren). Реализовать функцию записи при срабатывании детектора движения и включения сирены. При отключении детектора движения сигнал оповещения и запись должны быть остановлены. Для каждой камеры должен быть назначен отдельный детектор движения. Результат отразить в отчете.

2. Организовать ограничения доступа:

2.1. Добавить в проект следующие объекты: дверь (Door), сирена (Siren), считыватель RFID (RFID Reader), две карты RFID (RFID Card). В программном коде одной из карт поменять параметр CARD_ID на шифр студента.

2.2. На сервере реализовать следующие условия:

- открытие двери при правильном идентификаторе карты RFID, находящемся в диапазоне от шифра –10 до шифра +10;
- если идентификация не осуществляется, дверь должна быть закрыта;
- не открывать дверь при неверном идентификаторе карты: при обнаружении неверной карты включить сирену.

2.3. Результаты работы системы ограничения доступа представить в отчете.

3. Реализовать систему пожарной безопасности:

3.1. Добавить в проект не менее четырех датчиков пожарной безопасности (Fire Monitor), четырех пожарных спринклеров (Fire Sprinkler) и четырех сирен (Siren). С каждым датчиком должен быть связан один спринклер и сирена.

Осуществить настройку на сервере, реализующую условия включения сирены и спринклера при срабатывании определенного датчика. Для подключения спринклеров добавить MCU-PT из раздела «Components»→«Boards», осуществить подключение спринклеров с помощью кабеля IoT. Осуществить настройку блока микроконтроллера MCU-PT в соответствии с рисунком 1.7.

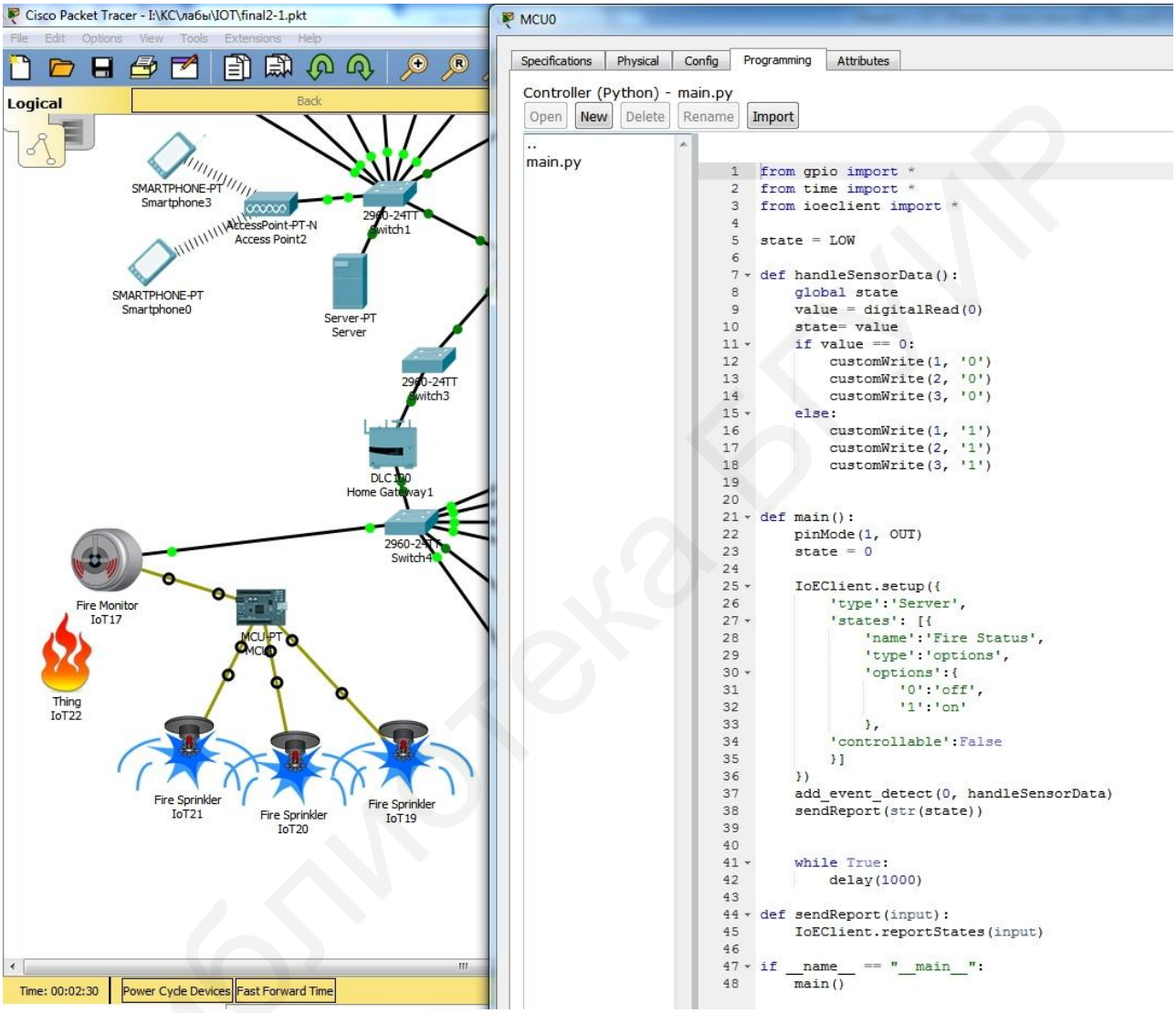


Рисунок 1.7 – Настройка блока микроконтроллера MCU-PT для системы пожарной безопасности

3.2. Для проверки правильности работы системы добавить объект Thing из раздела «Components»→«Boards». Изменить программный код данного объекта в соответствии с рисунком 1.8. Данный объект должен реализовать в окружающее пространство инфракрасное излучение, соответствующее температуре 900 °С. При расположение данного объекта вблизи датчика должен сработать соответствующий спринклер и сирена.

Результаты работы зафиксировать в отчете. Сохранить файл под именем **Lab1.pkt.**

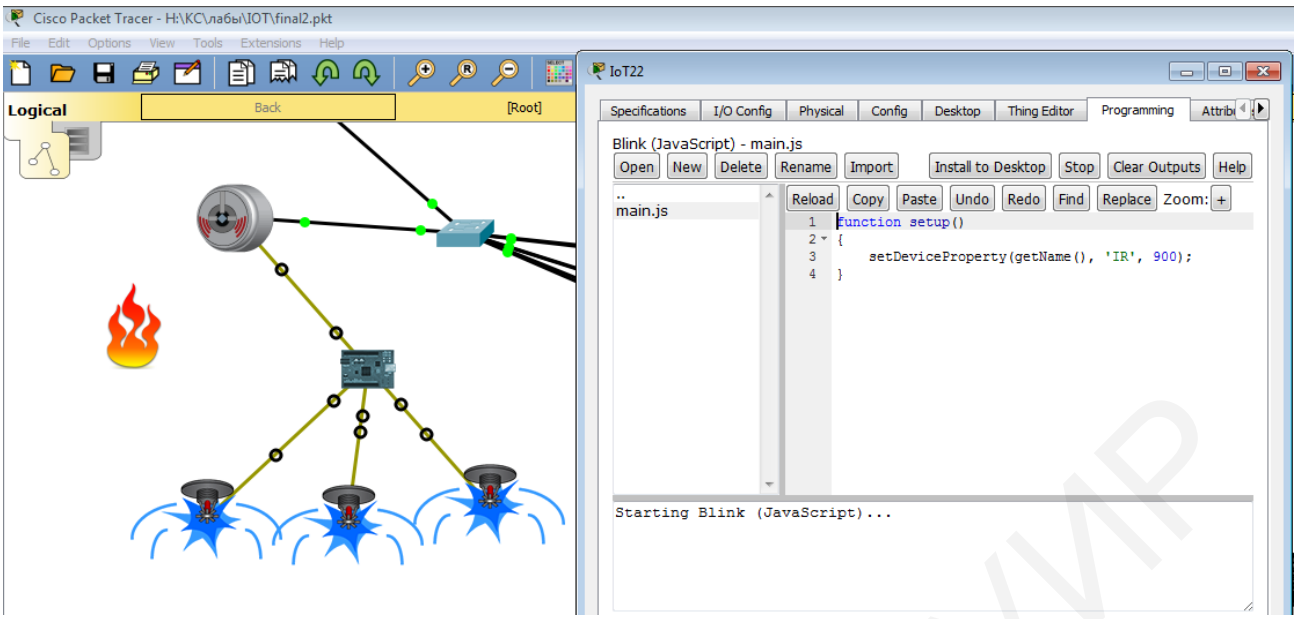


Рисунок 1.8 – Пример проверки правильности работы системы пожарной безопасности

1.3 Содержание отчета

1. Цель работы, исходные данные из таблицы 1.1.
2. Результаты произведенных настроек (см. пункты 1–2 задания 1, пункт 3 задания 2, пункт 2 задания 3 подраздела 1.2).
3. Вывод по работе.
4. Ответы на контрольные вопросы.

1.4 Контрольные вопросы и задания

1. Объяснить устройство IP-камеры и принцип ее работы.
2. Представить подробное описание уровней транспортной сети системы видеонаблюдения и пояснить их отличия.
3. В чем заключатся функции PoE? Какие стандарты PoE существуют?
4. Пояснить принципы использования VLAN для систем видеонаблюдения.
5. Перечислить особенности работы системы IP-видеонаблюдения с возможностью записи и хранения видеопотоков и управлением компонентами.
6. Объяснить назначение системы IP-видеонаблюдения с функцией маршрутизации.
7. Перечислить основные проблемы и пути их решения в распределенной системе цифрового видеонаблюдения.
8. В чем заключается назначение и описание сетевых протоколов, необходимых для передачи видеопотока по сети и дистанционного управления IP-камерой?

ЛАБОРАТОРНАЯ РАБОТА № 2
СТАТИЧЕСКАЯ МАРШРУТИЗАЦИЯ

Цель: изучить виды механизмов коммутации и статических маршрутов; научиться понимать содержание таблиц маршрутизации; овладеть навыками настройки статической маршрутизации.

2.1 Теоретическая часть

Одной из важных задач маршрутизатора является доставка пакетов в разные сети [4]. Пунктом назначения для IP-пакета может быть веб-сервер, расположенный в другой стране, или сервер электронной почты в локальной сети. Маршрутизатор использует таблицу маршрутизации, чтобы найти оптимальный путь для пересылки пакетов и обеспечить их своевременную доставку. Эффективность передачи данных между сетями в значительной степени зависит от возможности маршрутизаторов пересылать пакеты по наиболее оптимальному пути.

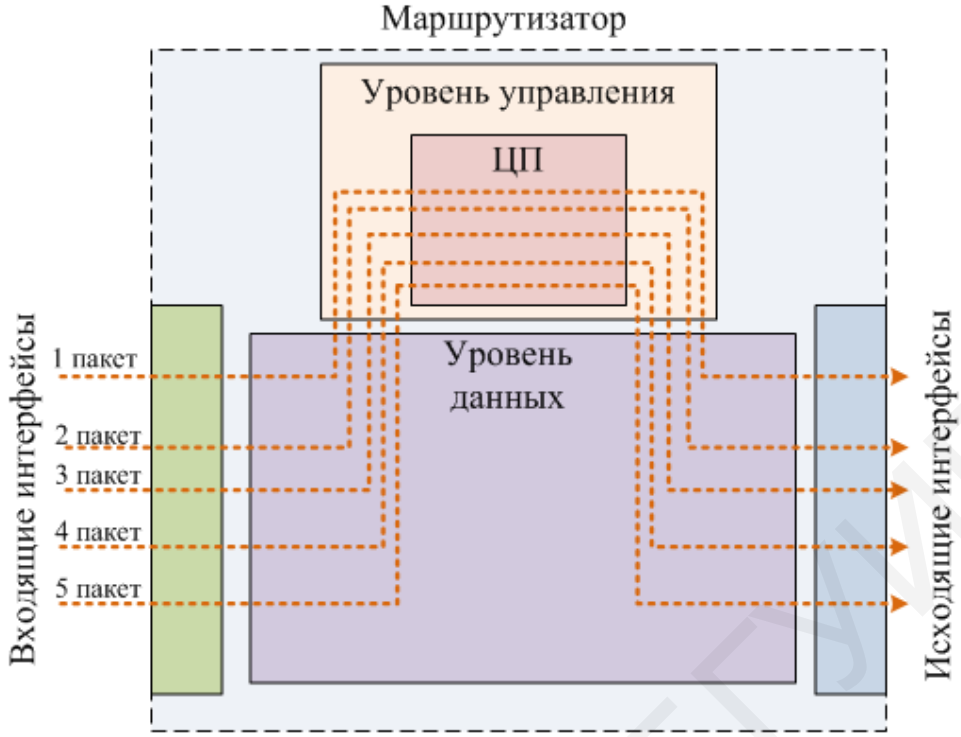
Когда узел отправляет пакет устройству в другой IP-сети, этот пакет пересылается на шлюз по умолчанию, поскольку узел не может напрямую взаимодействовать с устройствами, расположенными вне локальной сети. Этот шлюз часто используется для подключения локальной сети к Интернету.

Маршрутизаторы поддерживают три механизма пересылки пакетов:

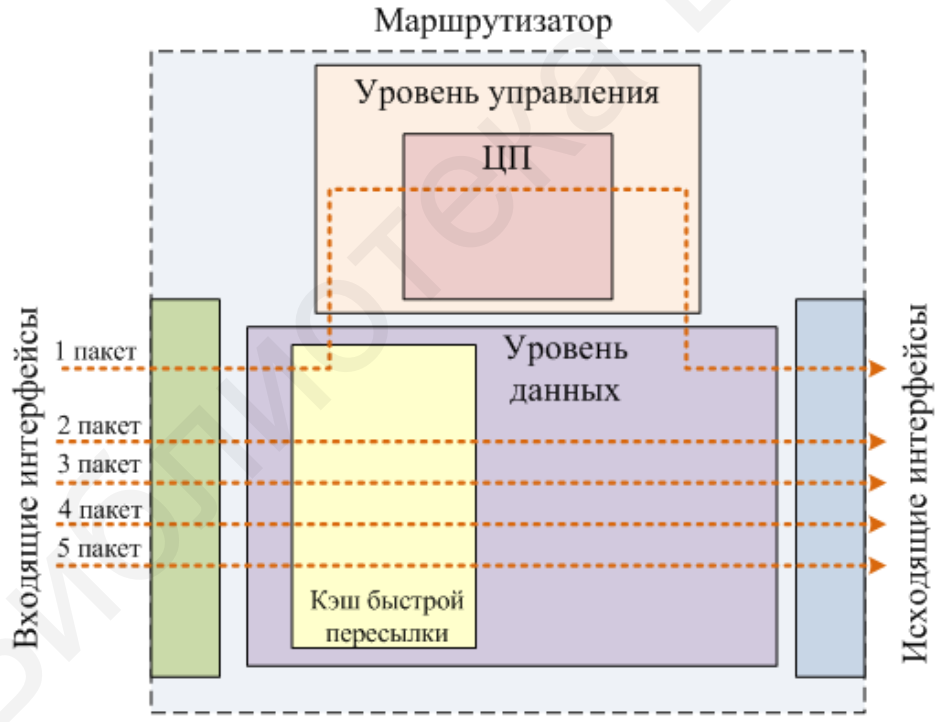
- программная коммутация;
- быстрая коммутация;
- Cisco Express Forwarding.

Программная коммутация заключается в том, что когда пакет прибывает на интерфейс, он пересылается на уровень управления, где центральный процессор маршрутизатора (ЦП) сопоставляет адрес назначения с записью в таблице маршрутизации, а затем определяет выходной интерфейс и пересылает пакет (рисунок 2.1, а). Маршрутизатор совершает такие действия с каждым пакетом, даже если целый поток пакетов предназначен для одного адреса назначения. Механизм программной коммутации работает очень медленно и редко реализуется в современных сетях.

Быстрая коммутация – самый распространенный механизм пересылки пакетов, который использует кэш быстрой коммутации для хранения информации о следующих переходах [4]. Когда пакет прибывает на интерфейс, он пересылается на уровень управления, где ЦП ищет совпадение в кэше быстрой коммутации (рисунок 2.1, б). Если совпадение не найдено, пакет проходит программную коммутацию и пересылается на выходной интерфейс. Информация о трафике также хранится в кэше быстрой коммутации. Если на интерфейс прибывает другой пакет, адресованный тому же назначению, то информация о следующем переходе повторно используется из кэш-памяти без вмешательства ЦП.



а – программная коммутация



б – быстрая коммутация

Рисунок 2.1 – Механизм пересылки пакетов

Cisco Express Forwarding (CEF) – способ пересылки пакетов, предпочтительный для Cisco IOS [4]. Как и быстрая коммутация, CEF создает 24-портовую

базу данных переадресации (Forwarding Information Base, FIB) и таблицу смежности (Adjacency Table). Однако записи таблицы инициированы не пакетами, как при быстрой коммутации, а изменениями – например, в сетевой топологии. Таким образом, по завершении сходимости сети в базе данных FIB и таблице смежности оказывается вся информация, необходимая маршрутизатору при пересылке пакета (рисунок 2.2). FIB содержит предварительно вычисленные маршруты и информацию о следующих переходах для маршрутизаторов, в том числе информацию об интерфейсе.

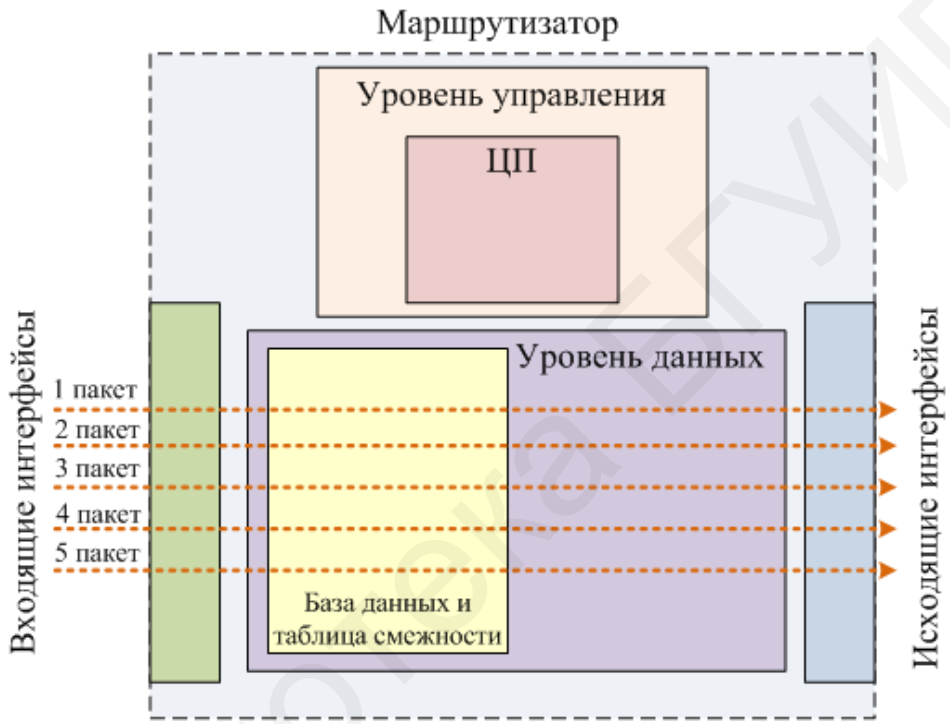


Рисунок 2.2 – Механизм Cisco Express Forwarding

Маршрутизаторы поддерживают локальные и глобальные сети и могут обеспечивать соединение между разными типами сетей. Таким образом, они совместимы с множеством типов интерфейсов. Один из таких интерфейсов – **логический интерфейс внутри маршрутизатора (loopback)**. Он не назначается физическому порту (поэтому его нельзя подключить к другому устройству) и считается программным интерфейсом, который автоматически переводится в состояние UP во время работы маршрутизатора.

Применение интерфейса loopback может быть целесообразным при тестировании и управлении устройством Cisco IOS, поскольку он обеспечивает доступность хотя бы одного интерфейса. Его можно использовать, например, для тестирования внутренних процессов маршрутизации путем имитации сетей за пределами маршрутизатора.

Кроме того, IPv4-адрес, назначенный loopback-интерфейсу, может быть необходим для маршрутизаторов, в которых используется IPv4-адрес интерфейса в целях идентификации. Включение интерфейса и назначение loopback-адресов выполняется с помощью простого набора команд [4]:

```
Router(config)# interface loopback number
Router(config-if)# ip address ip-address subnet-mask
Router(config-if)# exit
```

На маршрутизаторе можно активировать несколько интерфейсов loopback. IPv4-адрес для каждого интерфейса должен быть уникальным и не должен быть задействован другим интерфейсом.

Таблица маршрутизации представляет собой файл данных в ОЗУ, используемый для хранения информации о сетях с прямым подключением и об удаленных сетях. Она содержит ассоциации с сетями или следующими переходами: с помощью этих ассоциаций маршрутизатор узнает о том, на какой маршрутизатор, представляющий собой следующий переход на пути до пункта назначения, необходимо отправить пакет. Также ассоциация со следующим переходом может быть исходящим интерфейсом для следующего назначения.

Таблица маршрутизации хранит следующую информацию:

- маршруты с прямым подключением – это маршруты, поступающие из активных интерфейсов маршрутизатора. Маршрутизаторы добавляют маршрут с прямым подключением, когда интерфейс настроен с IP-адресом и активирован;

- удаленные маршруты – это удаленные сети, подключенные к другим маршрутизаторам. Маршруты к этим сетям могут быть настроены статически либо динамически с использованием протоколов динамической маршрутизации.

В таблице маршрутизации (рисунок 2.3) присутствуют следующие виды записей:

- интерфейсы локального маршрута – добавляются, когда интерфейс настроен и активен;

- интерфейсы с прямым подключением – добавляются в таблицу маршрутизации, когда интерфейс настроен и активен;

- статические маршруты – добавляются, когда маршрут настроен вручную и активен выходной интерфейс;

- динамические маршруты – добавляются, когда определены сети и реализуются протоколы маршрутизации, которые получают информацию о сетях динамически (EIGRP или OSPF).

```
Router#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, E - EGP
       i - IS-IS, 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

Gateway of last resort is not set

     172.20.0.0/16 is variably subnetted, 8 subnets, 2 masks
D       172.20.0.0/30 [90/5376] via 172.20.0.5, 00:10:51, GigabitEthernet0/2/0
C       172.20.0.4/30 is directly connected, GigabitEthernet0/2/0
L       172.20.0.6/32 is directly connected, GigabitEthernet0/2/0
C       172.20.0.8/30 is directly connected, GigabitEthernet0/0
L       172.20.0.10/32 is directly connected, GigabitEthernet0/0
C       172.20.0.12/30 is directly connected, GigabitEthernet0/3/0
L       172.20.0.14/32 is directly connected, GigabitEthernet0/3/0
D       172.20.0.16/30 [90/5376] via 172.20.0.13, 00:10:41, GigabitEthernet0/3/0
D    192.168.7.0/24 [90/28416] via 172.20.0.5, 00:10:51, GigabitEthernet0/2/0
D    192.168.8.0/24 [90/28416] via 172.20.0.5, 00:10:51, GigabitEthernet0/2/0
D    192.168.9.0/24 [90/28416] via 172.20.0.5, 00:10:51, GigabitEthernet0/2/0
```

Рисунок 2.3 – Пример таблицы маршрутизации

Источники записей таблицы маршрутизации идентифицируются с помощью кода. Код определяет, каким образом был получен маршрут.

К примерам распространенных кодов относятся [4, 5]:

- код **L** указывает адрес, назначенный интерфейсу маршрутизатора: данный код позволяет маршрутизатору быстро определить, что полученный пакет предназначен для интерфейса, а не для пересылки;

- код **C** определяет сеть с прямым подключением;

- код **S** определяет статический маршрут, созданный для достижения конкретной сети;

- код **D** определяет сеть, динамически полученную от другого маршрутизатора с помощью протокола EIGRP;

- код **R** определяет, что данные о маршруте получены динамически от другого маршрутизатора посредством протокола маршрутизации RIP;

- код **O** определяет сеть, динамически полученную от другого маршрутизатора с помощью протокола маршрутизатора OSPF.

Записи таблицы маршрутизации содержат следующие сведения (рисунок 2.4):

- источник маршрута – определение способа получения маршрута;

- сеть назначения – определение адреса удаленной сети;

- административное расстояние – определение надежности источника маршрута: наименьшее значение указывает на предпочтительный источник маршрута;

- метрика – определение значения, присвоенного для достижения удаленной сети: наименьшее значение указывает на предпочтительный маршрут;

- следующий переход – определение IPv4-адреса следующего маршрутизатора, на который следует переслать пакет;

- временная метка маршрута – определение количества времени, прошедшего с тех пор, как был получен маршрут [6];

- исходящий интерфейс – определение выходного интерфейса для отправки пакета к конечному пункту назначения.

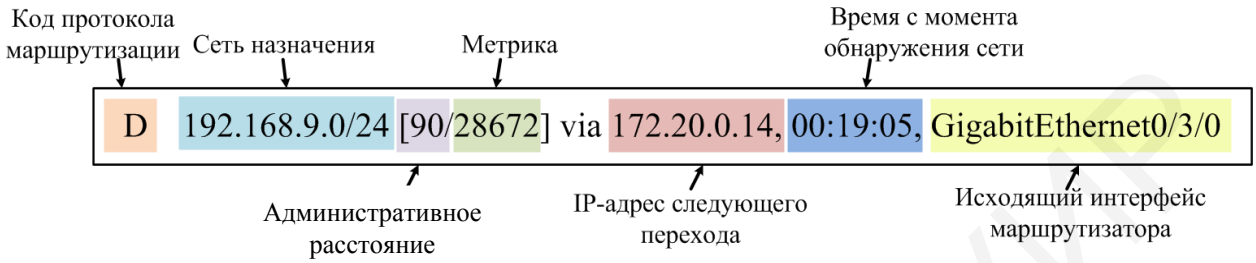


Рисунок 2.4 – Содержание таблицы маршрутизации

Новый маршрутизатор, в котором не настроены интерфейсы, имеет пустую таблицу маршрутизации. Перед тем как состояние интерфейса будет изменено на рабочее и будет добавлено в таблицу маршрутизации IPv4, интерфейс должен:

- получить допустимый IPv4-адрес;

- быть активирован с помощью команды `no shutdown`;

- получить несущий сигнал от другого устройства (маршрутизатора, коммутатора, узла и т. д.).

Когда интерфейс находится в рабочем состоянии, его сеть добавляется в таблицу маршрутизации в качестве сети с прямым подключением.

Корректно настроенный активный интерфейс с прямым подключением фактически создает две записи в таблице маршрутизации (рисунок 2.5). Записи содержат следующие сведения [5]:

- источник маршрута – определение способа получения маршрута;

- сеть назначения – адрес удаленной сети;

- исходящий интерфейс – определение выходного интерфейса для пересылки пакетов к сети назначения.

Интерфейсы прямого подключения имеют два кода источника маршрута:

- код **C** определяет сеть с прямым подключением;

- код **L** определяет IPv4-адрес, назначенный интерфейсу маршрутизатора.

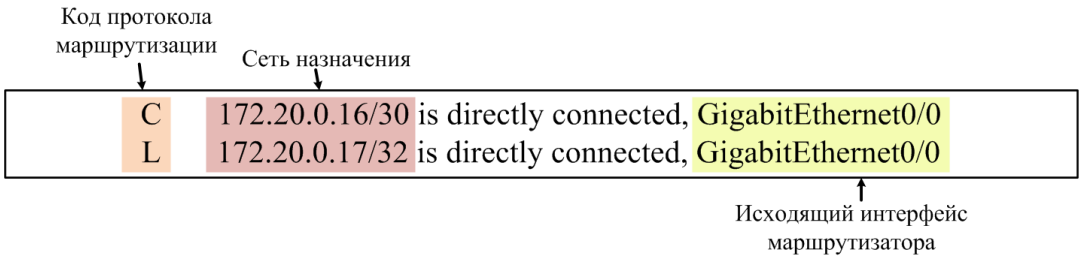


Рисунок 2.5 – Пример таблицы маршрутизации с интерфейсами прямого подключения

После того как интерфейсы с прямым подключением настроены и добавлены в таблицу маршрутизации, реализуется статическая или динамическая маршрутизация.

Статическая маршрутизация настраивается вручную и определяет точный маршрут между двумя сетевыми устройствами. Статические маршруты не обновляются автоматически, и при изменениях в сетевой топологии их нужно повторно настраивать вручную. К преимуществам использования статических маршрутов относятся высокий уровень безопасности и эффективность расходования ресурсов. Статические маршруты используют более узкую полосу пропускания, чем протоколы динамической маршрутизации; для расчета и связи маршрутов циклы ЦП не используются. В таблице маршрутизации представлены два распространенных типа статических маршрутов:

- статические маршруты в удаленную (конкретную) сеть;
- статические маршруты по умолчанию.

Статические маршруты настраиваются с помощью команды глобальной конфигурации `ip route`. Чаще всего используется следующий синтаксис команды [4]:

```
ip route network-address subnet-mask {ip-address| exit-intf}
```

Для настройки статической маршрутизации обязательно указываются следующие параметры:

- `network-address` – адрес удаленной сети назначения, который необходимо добавить в таблицу маршрутизации;
- `subnet-mask` – маска подсети или просто маска удаленной сети, которую необходимо добавить в таблицу маршрутизации;
- `ip-address` – IP-адрес подключаемого маршрутизатора, который используется для пересылки пакетов в удаленную сеть назначения;
- `exit-intf` – исходящий интерфейс, который используется для передачи пакета на следующий переход [5].

С помощью команды `show ip route` можно проверить правильность таблицы маршрутизации. Статический маршрут определяется в таблице маршрутизации посредством кода **S**.

На рисунке 2.6 представлен пример сети. Если маршрутизация в данной сети не настроена, то у каждого маршрутизатора в таблице есть данные только о ближайших подключенных к нему сетях. Например, маршрутизатор Router3 на рисунке 2.6 имеет информацию о сетях 172.20.0.16/30 и 172.20.0.12/30, которые в таблице маршрутизации помечены кодом **C** (сети с прямым подключением). Код **L** указывает адрес, назначенный интерфейсу маршрутизатора. Данные в другие сети он передать не сможет, поэтому необходимо настроить маршрутизацию.

Для передачи данных в удаленные сети маршрутизатор должен располагать информацией о следующем переходе (следующем маршрутизаторе, пересылающем данные далее), который можно определить с помощью IP-адреса или выходного интерфейса, а также обоих параметров сразу. В зависимости от того, как указано место назначения, создается один из трех возможных типов маршрута [6]:

- маршрут следующего перехода – указывается только IP-адрес следующего перехода;
- напрямую подключенный статический маршрут – указывается только выходной интерфейс маршрутизатора;
- полностью заданный статический маршрут – указывается IP-адрес следующего перехода и выходной интерфейс.

Для маршрутизатора Router3 (рисунок 2.6) маршруты следующего перехода задаются следующим образом:

```
ip route 192.168.200.0 255.255.255.0 172.20.0.18
```

При настройке статического маршрута также можно использовать выходной интерфейс для настройки адреса следующего перехода:

```
ip route 192.168.200.0 255.255.255.0 GigabitEthernet 0/0
```

Полностью заданный статический маршрут может быть настроен следующим образом:

```
ip route 192.168.200.0 255.255.255.0 GigabitEthernet 0/0 172.20.0.18
```

Статический маршрут по умолчанию – это маршрут, которому соответствуют все пакеты [5]. Вместо хранения всех маршрутов ко всем сетям в таблице маршрутизации маршрутизатор может хранить один маршрут по умолчанию, представляющий любую сеть, отсутствующую в таблице маршрутизации.

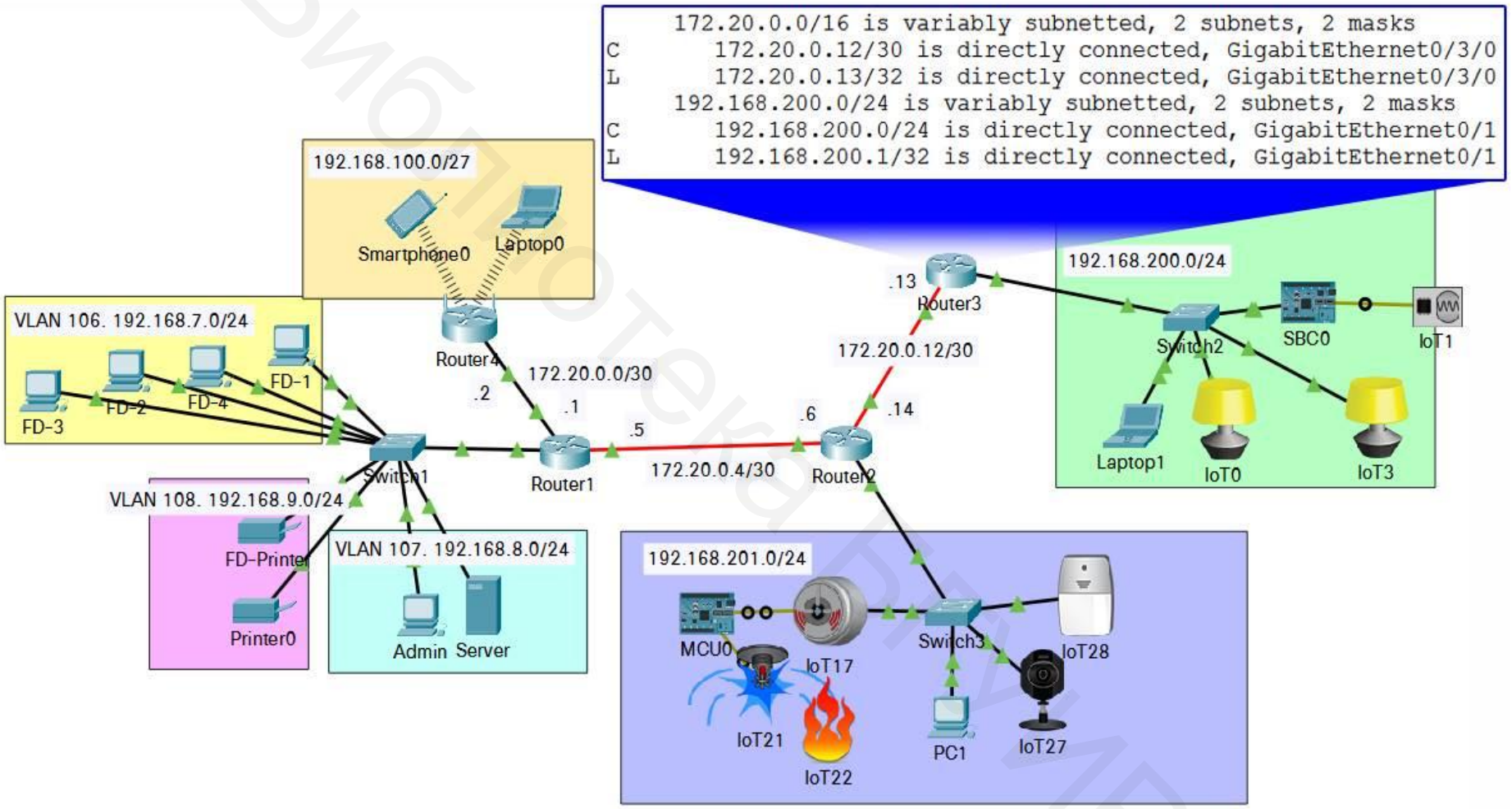


Рисунок 2.6 – Пример сети до настройки маршрутизации

Для того чтобы настроить статический IPv4-маршрут по умолчанию, используется команда глобальной конфигурации:

```
ip route 0.0.0.0 0.0.0.0 {exit-intf | next-hop-ip}
```

Например, маршрутизатор Router3 имеет доступ ко всем сетям только через интерфейс маршрутизатора Router2 (см. рисунок 2.6). Поэтому можно настроить маршрут по умолчанию следующим образом:

```
ip route 0.0.0.0 0.0.0.0 GigabitEthernet 0/0
```

или

```
ip route 0.0.0.0 0.0.0.0 172.20.0.14
```

На рисунке 2.6 маршрутизаторы соединены между собой оптоволоконным кабелем. Для обеспечения такого соединения в маршрутизаторе должен присутствовать слот SFP, в который монтируется оптический разъем 1000BASE-LX/LH SFP, обеспечивающий подключение оптоволоконного кабеля (рисунок 2.7).

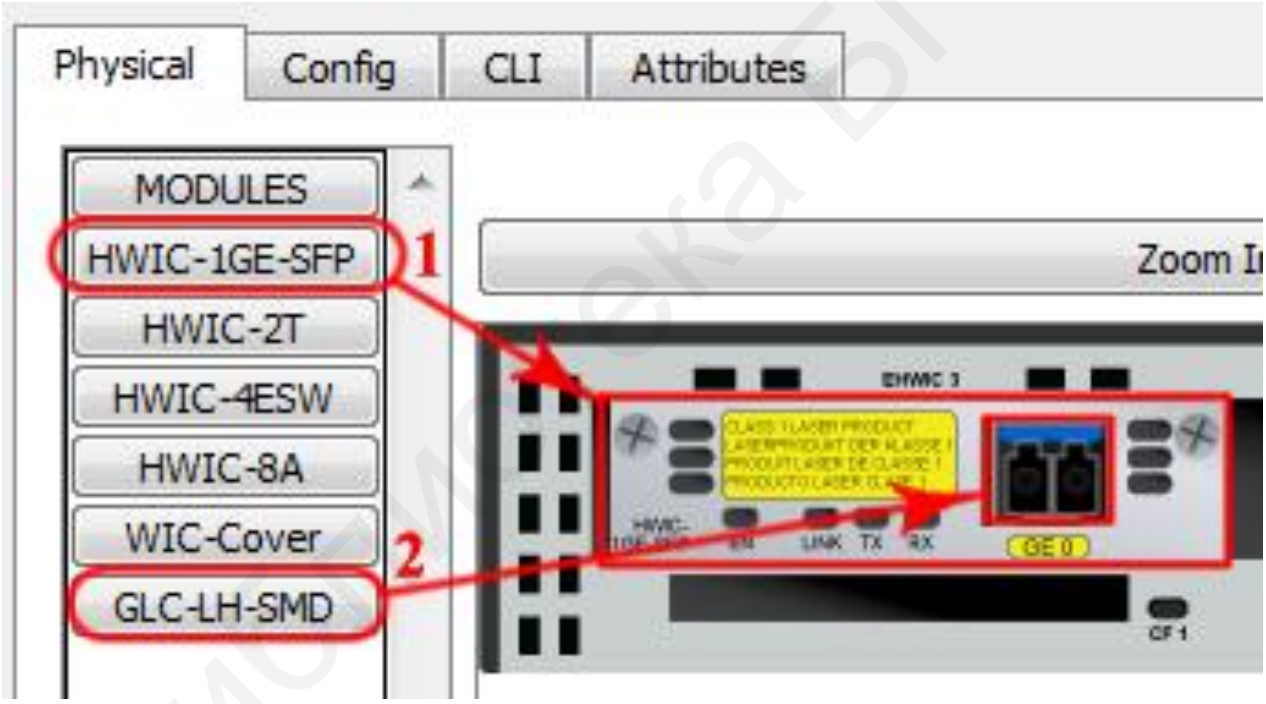


Рисунок 2.7 – Размещение слота SFP и разъема 1000BASE-LX/LH SFP в маршрутизаторе

2.2 Лабораторное задание

Лабораторная работа выполняется на основе настроек, произведенных в лабораторной работе № 1. До начала выполнения необходимо открыть сохраненный файл с именем **Lab1.pkt**, полученный в лабораторной работе № 1, и проверить правильность соединений.

Смоделированную сеть необходимо разделить на следующие подсети: подсеть с VLAN, подсеть с беспроводным маршрутизатором, подсеть с IoT-устройствами из лабораторной работы № 8 предыдущего семестра [26], подсеть

с устройствами для ограничения доступа из лабораторной работы № 1 (см. рисунок 2.6). Редактирование IP-адресации локальных сетей не требуется. В сети должно быть четыре маршрутизатора, один из которых беспроводной. Маршрутизаторы должны быть соединены оптоволоконным кабелем, как показано на рисунке 2.8.

В данной лабораторной работе необходимо настроить статическую маршрутизацию, исходя из следующих заданий.

1. Настроить IP-адресацию интерфейсов маршрутизаторов. В таблице 2.1 выбрать IP-адреса для интерфейсов маршрутизаторов в соответствии с третьей цифрой шифра. Маска для новых подсетей – 255.255.255.252. На рисунке 2.8 представлен пример подключения подсетей. Сохранить файл Cisco Packet Tracer под именем **Lab2.pkt**.

Таблица 2.1 – Исходные данные для настройки IP-адресации

Цифра шифра	IP-адреса интерфейсов сети		
	№ 1	№ 2	№ 3
0	172.18.116.129, 172.18.116.130	172.18.116.133, 172.18.116.134	172.18.116.137, 172.18.116.138
1	172.22.178.193, 172.22.178.194	172.22.178.197, 172.22.178.198	172.22.178.201, 172.22.178.202
2	172.18.26.129, 172.18.26.130	172.18.26.133, 172.18.26.134	172.18.26.137, 172.18.26.138
3	172.15.115.225, 172.15.115.226	172.15.115.229, 172.15.115.230	172.15.115.233, 172.15.115.234
4	172.28.20.225, 172.28.20.226	172.28.20.229, 172.28.20.230	172.28.20.233, 172.28.20.234
5	172.24.2.129, 172.24.2.130	172.24.2.133, 172.24.2.134	172.24.2.137, 172.24.2.138
6	172.30.72.161, 172.30.72.162	172.30.72.165, 172.30.72.166	172.30.72.169, 172.30.72.170
7	172.16.46.193, 172.16.46.194	172.16.46.197, 172.16.46.198	172.16.46.201, 172.16.46.202
8	172.19.14.129, 172.19.14.130	172.19.14.133, 172.19.14.134	172.19.14.137, 172.19.14.138
9	172.13.102.129, 172.13.102.130	172.13.102.133, 172.13.102.134	172.13.102.137, 172.13.102.138

2. Настроить статическую маршрутизацию на всех маршрутизаторах, используя только маршруты следующего перехода или напрямую подключенные статические маршруты. Для этого осуществить настройку всех маршрутизаторов в файле **Lab2.pkt** и сохранить его под именем **Lab2-1.pkt**. Проверить правильность работы сети. Все устройства IoT и ограничения доступа должны отправлять на сервер данные о своем состоянии. Устройства из VLAN должны

отвечать на ICMP-пакеты. Результаты выполнения команды `show ip route` на каждом маршрутизаторе представить в отчете.

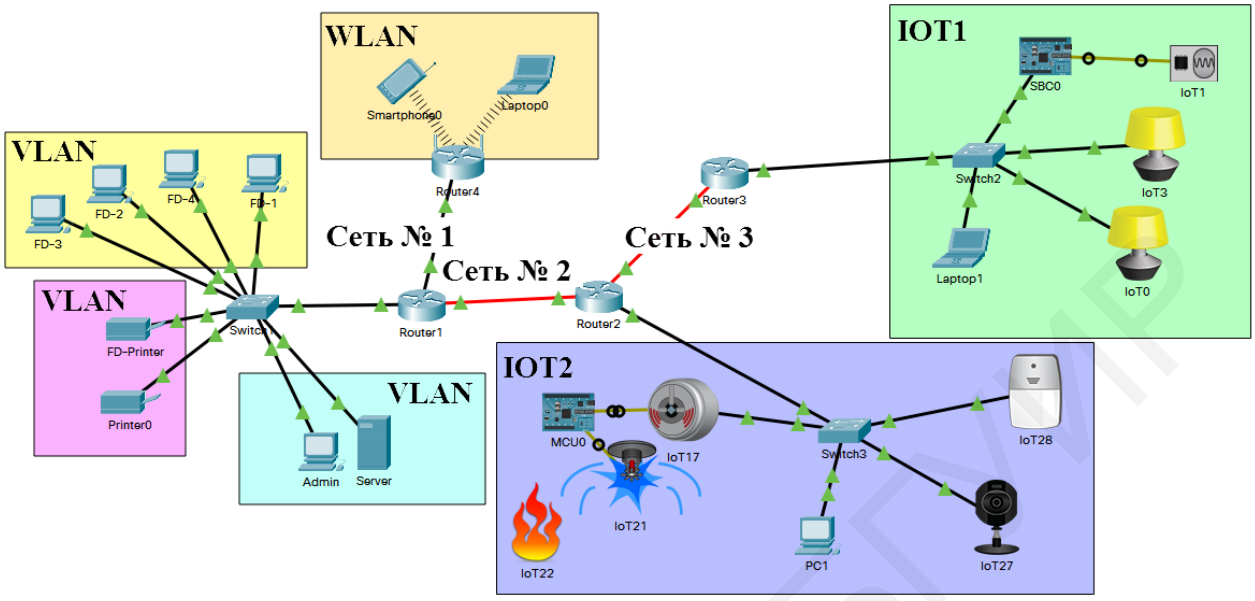


Рисунок 2.8 – Пример моделирования сети в Cisco Packet Tracer

3. Настроить статическую маршрутизацию на всех маршрутизаторах, используя статические маршруты по умолчанию, где это возможно. Для этого осуществить настройки в файле **Lab2.pkt** и сохранить его под именем **Lab2-2.pkt**. Проверить правильность работы сети. Все устройства IoT должны отправлять на сервер данные о своем состоянии, пользователи всех устройств сети должны получать доступ к информации на сервере. Результаты проверки представить в отчете.

4. По результатам выполнения данной лабораторной работы все устройства во всех файлах должны получать доступ к серверу, на котором должны отображаться статусы всех IoT-устройств и условия, заданные для их работы. Доступ к серверу должен осуществляться посредством DNS.

2.3 Содержание отчета

1. Цель работы, исходные данные из таблицы 2.1.
2. Результаты произведенных настроек (см. задания 2–3 подраздела 2.2), изображение смоделированной сети.
3. Вывод по работе.
4. Ответы на контрольные вопросы.

2.4 Контрольные вопросы и задания

1. Перечислить виды и отличия механизмов пересылки пакетов.
2. В чем заключается назначение логического интерфейса и как осуществляется его настройка на маршрутизаторе?
3. В чем заключается назначение таблицы маршрутизации? Перечислить виды записей в таблице маршрутизации.
4. Описать коды таблицы маршрутизации.
5. Что такое интерфейсы прямого подключения?
6. Привести типы статических маршрутов и примеры их настройки.

ЛАБОРАТОРНАЯ РАБОТА № 3
ДИСТАНЦИОННО-ВЕКТОРНЫЕ ПРОТОКОЛЫ МАРШРУТИЗАЦИИ

Цель: изучить назначения, принцип действия протоколов динамической маршрутизации RIPv1, RIPv2, EIGRP; овладеть навыками настройки данных протоколов на маршрутизаторах.

3.1 Теоретическая часть

Протоколы динамической маршрутизации позволяют маршрутизаторам динамически обмениваться данными об удаленных сетях и автоматически добавлять эти данные в собственные таблицы маршрутизации [7].

Основным преимуществом протоколов динамической маршрутизации является то, что они обеспечивают обмен данными между маршрутизаторами в случаях изменений в топологии. Подобный обмен позволяет маршрутизаторам автоматически получать информацию о новых сетях, а также находить альтернативные пути в случае сбоя канала к текущей сети.

По сравнению со статической маршрутизацией протоколы динамической маршрутизации требуют меньшего вмешательства со стороны администратора. Тем не менее к издержкам их использования можно отнести тот факт, что часть ресурсов маршрутизатора выделяется для работы протокола (включая время ЦП и полосу пропускания сетевого канала). Несмотря на преимущества динамической маршрутизации, статическая маршрутизация по-прежнему находит применение. В отдельных случаях рекомендуется использовать именно статическую маршрутизацию, в то время как в других предпочтительней выбрать динамическую маршрутизацию. Для сетей среднего уровня можно настроить как статическую, так и динамическую маршрутизацию [8].

Все протоколы маршрутизации разработаны для получения данных об удаленных сетях и быстрой адаптации к любым изменениям в топологии [4]. Метод, используемый для выполнения этих задач, зависит от выбранного алгоритма и эксплуатационных характеристик протокола.

В целом работу протокола динамической маршрутизации можно описать следующим образом:

1. Маршрутизатор отправляет и принимает сообщения маршрутизации на свои интерфейсы.

2. Маршрутизатор предоставляет общий доступ к сообщениям маршрутизации и данным о маршрутах для других маршрутизаторов, использующих тот же протокол маршрутизации.

3. Маршрутизаторы осуществляют обмен данными маршрутизации для получения информации об удаленных сетях.

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

В момент включения питания у маршрутизатора нет данных о топологии сети. Кроме того, у него нет сведений о наличии устройств на другом конце каналов. Маршрутизатору доступна лишь информация из его собственного файла конфигурации, сохраненного в энергонезависимом ОЗУ (NVRAM). После успешной загрузки маршрутизатор применяет сохраненную конфигурацию. Если IP-адресация настроена верно, первоначально маршрутизатор выполняет обнаружение напрямую подключенных сетей. После начальной загрузки и обнаружения источников маршрутов выполняется обновление таблицы маршрутизации с добавлением всех напрямую подключенных сетей и интерфейсов, на которых размещены эти сети.

После настройки протокола маршрутизации маршрутизатор начинает обмен данными о корректировке маршрутов для получения информации обо всех удаленных маршрутах.

Маршрутизатор отправляет пакет обновления из всех включенных на нем интерфейсов, содержащий данные таблицы маршрутизации, в которой имеется информация о напрямую подключенных сетях.

В то же время маршрутизатор принимает и обрабатывает аналогичные пакеты обновлений от других подключенных маршрутизаторов. После получения обновления маршрутизатор проверяет пакет на наличие данных о новых сетях и добавляет все сети, не прописанные в таблице маршрутизации.

На этапе обмена данными у маршрутизаторов есть информация о собственных напрямую подключенных сетях, а также о подключенных сетях соседних устройств. Маршрутизаторы реагируют на изменения в топологии независимо друг от друга, этот процесс называют сходимостью. Продолжая процесс сходимости, маршрутизаторы выполняют обмен периодическими обновлениями. Каждый из маршрутизаторов еще раз проверяет обновления на предмет наличия новых данных. Сходимость сети считается достигнутой, когда все маршрутизаторы получили полные и точные данные обо всей сети. Время сходимости – время, требуемое маршрутизатору для обмена данными, расчета оптимальных путей и обновления таблиц маршрутизации. Сеть не является полностью рабочей до момента достижения полной сходимости. Сходимость подразумевает как совместную, так и самостоятельную работу устройств. Маршрутизаторы обмениваются данными друг с другом, однако они должны самостоятельно определять влияние изменений в топологии на собственные маршруты. К свойствам сходимости относятся скорость распространения данных маршрутизации и расчет оптимальных путей. Скорость распространения соотносится со временем, необходимым для отправки информации о маршрутизации от маршрутизаторов внутри сети. Протоколы маршрутизации можно оценивать по скорости сходимости: чем быстрее выполняется сходимость, тем более эффективным является протокол маршрутизации.

Дистанционно-векторные протоколы осуществляют обмен обновлениями с соседними устройствами [4]. Некоторые дистанционно-векторные протоколы регулярно отправляют обновления. Например, протокол RIP делает это каждые 30 секунд и продолжает отправлять обновления даже в том случае, если топология сети не изменялась. Протокол RIPv1 осуществляет доступ ко всем соседним устройствам посредством отправки обновлений на IPv4-адрес всех узлов в сети 255.255.255.255. Широковещательная рассылка регулярных обновлений не является эффективной, поскольку они занимают полосу пропускания и потребляют ресурсы ЦП сетевого устройства, а каждое сетевое устройство должно обработать сообщение широковещательной рассылки. В свою очередь, протоколы RIPv2 и EIGRP используют групповые адреса, поэтому обновления получают только те соседние устройства, которым они требуются. Протокол EIGRP также может отправлять одноадресные сообщения только тому соседнему устройству, которое в этом «заинтересовано». Кроме того, протокол EIGRP отправляет обновление при необходимости, а не регулярно.

Алгоритм, используемый для протоколов маршрутизации, определяет следующие процессы:

- механизм отправки и получения данных маршрутизации;
- механизм расчета оптимальных путей и добавления маршрутов в таблицу маршрутизации;
- механизм обнаружения и реагирования на изменения в топологии.

Различные протоколы маршрутизации используют различные алгоритмы для установки маршрутов в таблицу маршрутизации, отправки обновлений соседним устройствам и принятия решений об определении пути. Протокол RIP использует алгоритм Беллмана – Форда. Протоколы IGRP и EIGRP используют алгоритм DUAL.

Протокол RIPv1 обладает следующими ключевыми характеристиками:

- широковещательная рассылка обновлений маршрутизации (255.255.255.255) выполняется каждые 30 секунд;
- в качестве метрики для выбора пути служит число переходов;
- число переходов, превышающее 15, считается слишком удаленным; маршрутизатор 15-го перехода не передает обновление на следующий маршрутизатор.

Для включения протокола RIP используется команда `router rip`. Она напрямую не запускает работу протокола RIP, но с ее помощью осуществляется переход в режим конфигурации маршрутизатора, где выполняется настройка параметров маршрутизации.

Для отключения и удаления протокола RIP используется команда глобальной конфигурации `no router rip`. Данная команда останавливает работу протокола RIP и удаляет все его существующие настройки.

При переходе в режим конфигурации RIP маршрутизатор получает указание о запуске RIP. При этом маршрутизатору необходимо сообщить, какие локальные интерфейсы он должен использовать для обмена данными с другими маршрутизаторами, а также какие локально подключенные сети он должен объявить для них.

Для включения маршрутизации RIP используется команда режима конфигурации маршрутизатора `network сетевой_адрес`, в которой указывается сетевой адрес для каждой напрямую подключенной сети. Данная команда выполняет следующие действия:

- включает протокол RIP на всех интерфейсах, которые относятся к конкретной сети; связанные интерфейсы теперь могут и отправлять, и получать пакеты обновлений протокола RIP;

- объявляет указанную сеть в обновлениях маршрутизации RIP, отправляемых другим маршрутизаторам каждые 30 секунд.

Команда `show ip protocols` отображает текущие настройки протокола маршрутизации IPv4 [4]. На рисунке 3.1 представлен результат ввода команды `show ip protocols`.

```
Router1#show ip protocols                                              1
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 22 seconds               2
Invalid after 180 seconds, hold down 180, flushed after 240
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Redistributing: rip
Default version control: send version 1, receive 1
  Interface              Send  Recv  Triggered RIP  Key-chain
  GigabitEthernet0/1.8   1     1                                       3
  GigabitEthernet0/1.7   1     1
  GigabitEthernet0/1.9   1     1
  GigabitEthernet0/0     1     1
  GigabitEthernet0/1/0   1     1
Automatic network summarization is not in effect                       4
Maximum path: 4
Routing for Networks:
          172.20.0.0
          192.168.7.0                                                  5
          192.168.8.0
          192.168.9.0
          192.168.100.0
Passive Interface(s):
Routing Information Sources:
          Gateway         Distance      Last Update                    6
          172.20.0.6           120      00:00:27
Distance: (default is 120)
```

Рисунок 3.1 – Результат выполнения команды `show ip protocols`

Выходные данные, получаемые в результате выполнения команды `show ip protocols` для сети (см. рисунок 2.6), включают [4]:

- информацию о том, что маршрутизация RIP настроена и запущена на маршрутизаторе Router1;

- значения различных таймеров (например, следующее обновление маршрутизации отправляется маршрутизатором Router1 через 22 секунды);

- текущую настроенную версию протокола RIPv1;

- информацию о том, что маршрутизатор в настоящее время не выполняет объединение в пределах классовой сети;

- информацию о сетях, которые объявляются маршрутизатором Router1, т. е. сетях, которые маршрутизатор включил в обновления протокола RIP;

- информацию о соседних устройствах RIP вместе с IP-адресом их следующего перехода и значением административной дистанции, которое маршрутизатор использует для отправки обновлений соседним устройствам, а также при получении обновлений от них.

С помощью команды `show ip route` можно проверить добавление маршрутов RIP в таблицу маршрутизации.

Для включения RIPv2 используется команда режима конфигурации маршрутизатора протокола RIP `version 2`.

Протоколы RIPv1 и RIPv2 по умолчанию автоматически суммируют сети в пределах основной сети. После отключения функции автоматического объединения с помощью команды `no auto-summary` протокол RIPv2 прекращает объединение сетей по их классовой адресации на пограничных маршрутизаторах. Теперь протокол RIPv2 включает все подсети и соответствующие маски в свои обновления маршрутизации [4].

Обновления протокола RIP по умолчанию пересылаются из всех интерфейсов, поддерживающих RIP. Однако отправку обновлений необходимо выполнять только из интерфейсов, подключенных к другим маршрутизаторам с поддержкой RIP. Отправка ненужных обновлений в сеть LAN имеет следующие последствия:

- необоснованное расходование полосы пропускания;

- неэффективное потребление ресурсов;

- риски для информационной безопасности.

С помощью команды конфигурации маршрутизатора `passive-interface` можно запретить передачу обновлений маршрутизации через интерфейс маршрутизации, но при этом разрешить объявление сети для других маршрутизаторов. Команда прекращает отправку обновлений из указанного интерфейса. Тем не менее сеть, к которой относится указанный интерфейс, по-прежнему объявляется в обновлениях маршрутизации, которые отправляются из других интерфейсов [4].

Протокол EIGRP обеспечивает повышенную эффективность, сокращает объем обновлений маршрутизации и поддерживает безопасный обмен сообщениями. Протокол не отправляет регулярные обновления: распространению подлежат только изменения в таблице маршрутизации, что позволяет снизить нагрузку на сеть, связанную с работой протокола. Связанные обновления по событию указывают на то, что протокол EIGRP отправляет обновления только тем соседним устройствам, которым они требуются. Такие обновления используют меньший размер полосы пропускания, что особенно важно в больших сетях с множеством маршрутов [6].

Данный протокол поддерживает механизм keepalive (Hello), который предусматривает регулярную отправку и прием небольших сообщений-приветствий для поддержания отношений смежности с соседними маршрутизаторами. В отличие от регулярных обновлений, механизм keepalive обеспечивает низкое потребление ресурсов сети.

Также производится обработка и сохранение всех маршрутов, принятых от соседних устройств (не только оптимальных путей), в таблице топологии. Алгоритм DUAL может выполнять вставку резервных маршрутов в таблицу топологии EIGRP.

В большинстве случаев протокол EIGRP является протоколом внутренней маршрутизации с самой быстрой, практически мгновенной сходимостью, поскольку он обрабатывает альтернативные маршруты. В случае сбоя основного маршрута маршрутизатор может использовать указанный альтернативный маршрут: переключение на него выполняется немедленно и не требует взаимодействия с другими маршрутизаторами.

Протокол EIGRP использует протоколозависимые модули (PDM), т. е. он является единственным протоколом с поддержкой не только IPv4 и IPv6, но и других протоколов.

Для установления отношений соседства протокол EIGRP использует пакеты hello, которые по умолчанию отправляются каждые 5 секунд (hello-интервал). В случае если маршрутизатор не присылает hello-сообщение в течении hold time (по умолчанию 15 секунд, 3 hello-интервала), то он считается недоступным.

Каждый процесс EIGRP обслуживает три таблицы:

- таблицу соседей (neighbor table), в которой содержится информация о других ближайших маршрутизаторах, непосредственно подключенных к текущему и участвующих в обмене маршрутами. Информация о данной таблице может быть получена по команде `show ip eigrp neighbors`;

- таблицу топологии сети (topology table), в которой содержится информация о маршрутах, полученная от соседей (`show ip eigrp topology`);

- таблицу маршрутизации (routing table), на основе которой маршрутизатор принимает решения о перенаправлении пакетов (`show ip route`).

Настройка EIGRP состоит из трех шагов:

- включения протокола глобальной командой `router eigrp AS`. AS – номер автономной системы, который должен быть одинаковым у всех маршрутизаторов;

- указания сетей, относящихся к маршрутизатору, с помощью команды `network сетевой_адрес`;

- отключения функции автоматического объединения командой `no auto-summary`.

3.2 Лабораторное задание

Лабораторная работа выполняется на основе настроек, произведенных в задании 1 лабораторной работы № 2. До начала выполнения необходимо открыть сохраненный файл с именем **Lab2.pkt**, полученный в лабораторной работе № 2, и проверить настройки IP-адресации маршрутизаторов: маршрутизация не должна быть настроена. По результатам выполнения данной лабораторной работы все устройства должны иметь доступ к серверу, на котором должны отображаться статусы всех IoT-устройств и условия их работы. Доступ к серверу должен осуществляться посредством DNS.

В данной лабораторной работе необходимо настроить динамическую маршрутизацию, исходя из следующих заданий.

1. Настроить протокол динамической маршрутизации RIP версии 1. Отключить функции автоматического объединения маршрутов, запретить передачу обновлений маршрутизации через интерфейс маршрутизатора, подключенного к локальным сетям. Проверить результат настройки и представить в отчете результаты выполнения команд `show ip protocols` и `show ip route` для каждого маршрутизатора. Сохранить текущую конфигурацию всех маршрутизаторов. Сохранить файл под именем **Lab3-1.pkt.**

2. Осуществить наблюдение процесса сходимости сети с маршрутизацией по протоколу RIPv1. Отключить все маршрутизаторы. Перейти в режим симуляции времени, настроить фильтры только на пакеты RIP-протокола и включить все маршрутизаторы. Определить суммарное время сходимости сети.

3. Настроить протокол динамической маршрутизации RIP версии 2. Проверить результат настройки и представить в отчете результаты выполнения команд `show ip protocols` и `show ip route` для каждого маршрутизатора. Сохранить текущую конфигурацию всех маршрутизаторов. Сохранить файл под именем **Lab3-2.pkt.**

4. Осуществить наблюдение процесса сходимости сети с маршрутизацией по протоколу RIPv2. Отключить все маршрутизаторы. Перейти в режим симуляции времени, настроить фильтры только на пакеты RIP-протокола и вклю-

чить все маршрутизаторы. Определить суммарное время сходимости сети. В выводе произвести сравнение работы протокола RIPv1 и протокола RIPv2.

5. Открыть сохраненный файл **Lab2.pkt** и проверить настройки IP-адресации маршрутизаторов: маршрутизация не должна быть настроена. Настроить протокол динамической маршрутизации EIGRP. Номер автономной системы должен быть равен шифру студента. Отключить функцию автоматического объединения маршрутов, запретить передачу обновлений маршрутизации через интерфейс маршрутизатора, подключенного к локальным сетям. Проверить результат настройки и представить в отчете результаты выполнения команд `show ip eigrp neighbors`, `show ip eigrp topology`, `show ip protocols` и `show ip route` для каждого маршрутизатора. Сохранить текущую конфигурацию всех маршрутизаторов. Сохранить файл под именем **Lab3-3.pkt.**

6. Осуществить наблюдение процесса сходимости сети с маршрутизацией по протоколу EIGRP. Отключить все маршрутизаторы. Перейти в режим симуляции времени, настроить фильтры только на пакеты EIGRP-протокола и включить все маршрутизаторы. Определить суммарное время сходимости сети. В выводе произвести сравнение работы протоколов EIGRP, RIPv1 и RIPv2.

3.3 Содержание отчета

1. Цель работы.
2. Результаты произведенных настроек (см. задания 1–6 подраздела 3.2), изображение смоделированной в данной работе сети.
3. Вывод по работе.
4. Ответы на контрольные вопросы.

3.4 Контрольные вопросы и задания

1. Произвести сравнение динамической и статической маршрутизации.
2. Описать механизм работы динамической маршрутизации.
3. Что такое сходимость сети?
4. Перечислить дистанционно-векторные протоколы.
5. В чем заключается отличие протоколов RIPv1 и RIPv2.
6. Представить пример конфигурации протокола RIP на маршрутизаторе.
7. Перечислить отличительные черты протокола EIGRP.
8. Представить пример конфигурации протокола EIGRP на маршрутизаторе.

ЛАБОРАТОРНАЯ РАБОТА № 4
ПРОТОКОЛ МАРШРУТИЗАЦИИ ПО СОСТОЯНИЮ КАНАЛА

Цель: изучить алгоритм поиска кратчайшего пути, механизм передачи данных при настройке маршрутизации по состоянию канала; овладеть навыками настройки протокола OSPF на маршрутизаторах.

4.1 Теоретическая часть

Протоколы маршрутизации по состоянию канала считаются более сложными, чем дистанционно-векторные протоколы [4], т. к. для вычисления оптимального пути они используют алгоритм маршрутизации кратчайшего пути (SPF, Shortest Path First, или алгоритм Эдсгера Дейкстры). Данный алгоритм использует метрики расстояния, или стоимости, необходимые для вычисления кратчайшего пути. Стоимость пути до соседних маршрутизаторов может быть задана автоматически или определена вручную. Чаще всего она обратно пропорциональна пропускной способности канала связи [9]. Для определения совокупной стоимости маршрута алгоритм использует суммированную стоимость всех путей от источника до места назначения.

Алгоритм поиска кратчайшего пути создает дерево кратчайших путей SPF путем размещения каждого маршрутизатора в корне и расчета кратчайших путей к каждому из узлов. После этого дерево используется для расчета оптимальных маршрутов. Протокол OSPF вносит оптимальные маршруты в базу данных пересылки, которая применяется для создания таблицы маршрутизации [4].

К протоколам маршрутизации IPv4 по состоянию канала относятся следующие протоколы:

- алгоритм кратчайшего пути (OSPFv2);
- протокол маршрутизации промежуточных систем (IS-IS).

Протокол OSPF использует стоимость в качестве метрики. Путь с более низкой стоимостью считается более оптимальным по сравнению с путем с более высокой стоимостью. Стоимость интерфейса (S) обратно пропорциональна его пропускной способности (P_{int}):

$$S=\frac{P}{P_{int}}, \qquad (4.1)$$

где P – заданная пропускная способность.

Высокая пропускная способность указывает на низкую стоимость. Высокие нагрузка и значения задержки по времени указывают на высокую стоимость. Следовательно, канал связи Ethernet со скоростью 10 Мбит/с имеет более высокую стоимость, чем канал связи Ethernet со скоростью 100 Мбит/с. OSPF использует эталонную пропускную способность со значением 100 Мбит/с для всех каналов, скорость которых равна или выше скорости FastEthernet-

соединения. Таким образом, значение стоимости, назначенное для интерфейса FastEthernet с пропускной способностью 100 Мбит/с, будет равно 1.

Протокол OSPF создает три базы данных, каждая из которых содержит следующие таблицы (таблица 4.1) [10].

Таблица 4.1 – Базы данных и таблицы, создаваемые протоколом OSPF

База данных	Таблица	Команда для просмотра таблицы
База данных смежности	Таблица соседних устройств	`show ip ospf neighbor`
База данных состояний каналов (LSDB)	Таблица топологии	`show ip ospf database`
База данных пересылки	Таблица маршрутизации	`show ip route`

База данных смежности содержит список всех соседних маршрутизаторов, с которыми установлен двусторонний обмен данными. Для каждого маршрутизатора существует уникальная таблица [10].

База данных состояний каналов (Link State DataBase, LSDB) представляет топологию сети и содержит данные обо всех маршрутизаторах в сети. Все маршрутизаторы в области используют идентичные базы данных.

База данных пересылки содержит данные о маршрутах, созданных при запуске алгоритма в базе данных состояний каналов. Каждый маршрутизатор использует уникальную таблицу маршрутизации, которая содержит данные о способе и месте отправки пакетов на другие маршрутизаторы.

Протокол OSPF осуществляет обмен сообщениями для передачи данных маршрутизации, используя для этого пять типов пакетов, к которым относятся [4]:

- пакет приветствия (hello) – тип 0x01;
- пакет описания базы данных (пакеты дескрипторов базы данных, DataBase Descriptors, DBD) – тип 0x02;
- пакет запроса состояния канала (Link State Request, LSR) – тип 0x03;
- пакет обновления состояния канала (Link State Update, LSU) – тип 0x04;
- пакет подтверждения состояния канала (Link State Acknowledgment, LSAck) – тип 0x05.

Пакет обновления состояния канала (LSU) используется для отправки ответа на пакеты запроса состояния канала (LSR) и объявления новых данных. Пакеты обновления состояния канала (LSU) содержат один или несколько различных типов сообщений – объявлений состояния канала (Link State Advertisement, LSA), – которые в свою очередь содержат информацию о маршруте для сетей назначения (таблица 4.2). При получении LSU маршрутизатор

отправляет LSAck для подтверждения приема LSU. Поле данных LSAck является пустым.

Таблица 4.2 – Типы пакетов LSA

Тип пакета LSA	Описание
1	Пакеты LSA маршрутизатора
2	Пакеты LSA сети
3, 4	Суммарные пакеты LSA
5	Пакеты LSA внешней автономной системы
6	Пакеты LSA многоадресной рассылки в среде OSPF
7	Определяются для не полностью тупиковых зон (Not-So-Stubby Area, NSSA)

Маршрутизаторы, использующие протокол OSPF, выполняют указанные ниже действия для достижения состояния сходимости [4].

1. Установление отношений смежности с соседними устройствами. Маршрутизатор отправляет пакеты приветствия (hello) из всех интерфейсов для определения всех соседних устройств в пределах этих каналов. При наличии соседнего устройства маршрутизатор пытается установить с ним отношения смежности. Когда два маршрутизатора определяют, что они являются соседями, они переходят в состояние смежности. Два смежных соседних устройства продолжают обмениваться hello-пакетами, которые выполняют функцию keepalive-проверки в целях мониторинга состояния соседнего устройства. Если с определенного момента маршрутизатор не получает hello-пакеты от соседнего устройства, такое соседнее устройство считается недоступным, и отношения смежности нарушаются.

2. Обмен объявлениями о состоянии канала. После установления отношений смежности маршрутизаторы выполняют обмен объявлениями о состоянии канала (LSA). LSA содержат состояние и стоимость каждого подключенного напрямую канала. Маршрутизаторы отправляют LSA смежным устройствам. При получении LSA смежные устройства мгновенно отправляют свои LSA напрямую подключенным соседям: данный процесс продолжается до тех пор, пока все маршрутизаторы области не получат все LSA. Помимо данных о состоянии канала, в пакет состояния канала также включаются порядковые номера и сведения о времени создания, что позволяет управлять процессом лавинной рассылки. Эти данные используются каждым из маршрутизаторов для определения, был ли пакет состояния канала от другого маршрутизатора получен ранее или пакет содержит более свежие данные, чем те, что уже добавлены в базу.

3. Создание таблицы топологии. После получения объявлений о состоянии канала (LSA) маршрутизаторы создают базу данных топологии на основе

полученных пакетов. В ней в конечном итоге собирается вся информация о топологии сети.

4. Выполнение алгоритма поиска кратчайшего пути SPF. После указанных выше действий маршрутизаторы выполняют алгоритм поиска кратчайшего пути, который создает дерево кратчайших путей SPF.

Протокол OSPF проходит несколько этапов и состояний в процессе достижения сходимости [4]. Они представлены в таблице 4.3.

Таблица 4.3 – Описание состояний в процессе сходимости

Этап	Состояние	Описание
Установление смежности	DOWN	Не получено ни одного пакета приветствия. Маршрутизатор отправляет пакеты приветствия
	INIT	Пакеты приветствия принимаются от соседних устройств. Они содержат идентификатор отправляющего маршрутизатора
	2WAY	Выбор выделенного маршрутизатора (DR) и резервного выделенного маршрутизатора (BDR)
Синхронизация баз данных	EXSTART	Согласование отношений ведущего и ведомого устройств и порядкового номера пакета DBD. Ведущее устройство инициирует обмен пакетами DBD
	EXCHANGE	Маршрутизаторы выполняют обмен пакетами DBD. Если требуется дополнительная информация, выполняется переход в состояние Loading. В ином случае выполняется переход в состояние Full
	LOADING	Пакеты LSR и LSU используются для получения дополнительных данных маршрутизации. Маршруты обрабатываются посредством алгоритма поиска кратчайшего пути
FULL		Состояние сходимости достигнуто

Оптимальные маршруты вносятся в таблицу маршрутизации из дерева кратчайших путей SPF. Решения по маршрутизации принимаются на основе записей в таблице маршрутизации.

Для обеспечения большей эффективности и масштабируемости протокол, OSPFv2 поддерживает иерархическую маршрутизацию с разделением на области. Под **областью OSPF** определяют группу маршрутизаторов, использующих одинаковые данные о состоянии канала в своих базах состояний. Таким образом, протокол OSPFv2 можно реализовать для одной или нескольких областей.

В случае одной области все маршрутизаторы находятся в единой области, называемой магистральной, или нулевой (область 0). При использовании протокола для нескольких областей все области должны быть подключены к магистральной. Маршрутизаторы, с помощью которых осуществляется соединение между областями, называются пограничными маршрутизаторами (ABR).

В OSPFv2 для нескольких областей протокол может разделять одну большую автономную систему (AS) на более мелкие области в целях обеспечения иерархической маршрутизации. При использовании иерархической маршрутизации выполняется маршрутизация между областями (межобластная маршрутизация), но многие из операций, потребляющих ресурсы процессора, например, повторный расчет базы данных, выполняются в пределах одной области.

При наличии слишком большого числа маршрутизаторов в одной области базы данных состояний канала имеют слишком большой размер, и нагрузка на ЦП, таким образом, увеличивается. Поэтому распределение маршрутизаторов по областям разделяет потенциально большие базы данных на базы меньшего размера, тем самым обеспечивая возможность более эффективного управления.

Сообщения протокола OSPFv2 содержат следующие данные (рисунок 4.1):

- заголовок кадра канала данных Ethernet, который определяет групповой MAC-адрес назначения (0100.5E00.0005 или 0100.5E00.0006);

- заголовок IP-пакета, который определяет значение 89 в поле протокола IPv4, указывающее, что этот пакет является пакетом OSPF; он также определяет один из двух групповых адресов OSPF (224.0.0.5 или 224.0.0.6);

- заголовок пакета OSPFv2, который определяет тип пакета OSPFv2, идентификатор маршрутизатора и идентификатор области;

- данные в зависимости от типа пакета OSPFv2.

К наиболее важным полям пакета OSPF относятся:

- тип пакета;

- идентификатор маршрутизатора – IPv4-адрес исходного маршрутизатора;

- идентификатор области, в которой создан пакет;

- маска подсети, связанная с исходящим интерфейсом;

- интервал приветствия (HelloInterval) – интервал (в секундах), по истечении которого маршрутизатором отправляется следующий пакет приветствия. В сетях с множественным доступом по умолчанию задан 10-секундный интервал приветствия. В соседних маршрутизаторах должен использоваться один и тот же таймер, иначе отношения смежности не установятся;

- приоритет маршрутизатора, который используется при выборе DR/BDR. По умолчанию для всех маршрутизаторов OSPFv2 задан приоритет 1, однако его можно изменить вручную, выбрав значение в диапазоне от 0 до 255: чем выше это значение, тем больше вероятность того, что маршрутизатор будет использоваться как выделенный маршрутизатор (DR) на этом канале;

- интервал простоя (RouterDeadInterval) – интервал ожидания маршрутизатором сигнала от соседнего устройства в секундах, по истечении которого соседний маршрутизатор объявляется недействующим. Как правило, значение интервала простоя равно четырехкратному значению интервала приветствия,

т. е. 40 секундам. В соседних маршрутизаторах должен использоваться один и тот же таймер, иначе отношения смежности не установятся;

- идентификатор выделенного маршрутизатора (DR);
- идентификатор резервного выделенного маршрутизатора (BDR);
- идентификаторы всех смежных маршрутизаторов.

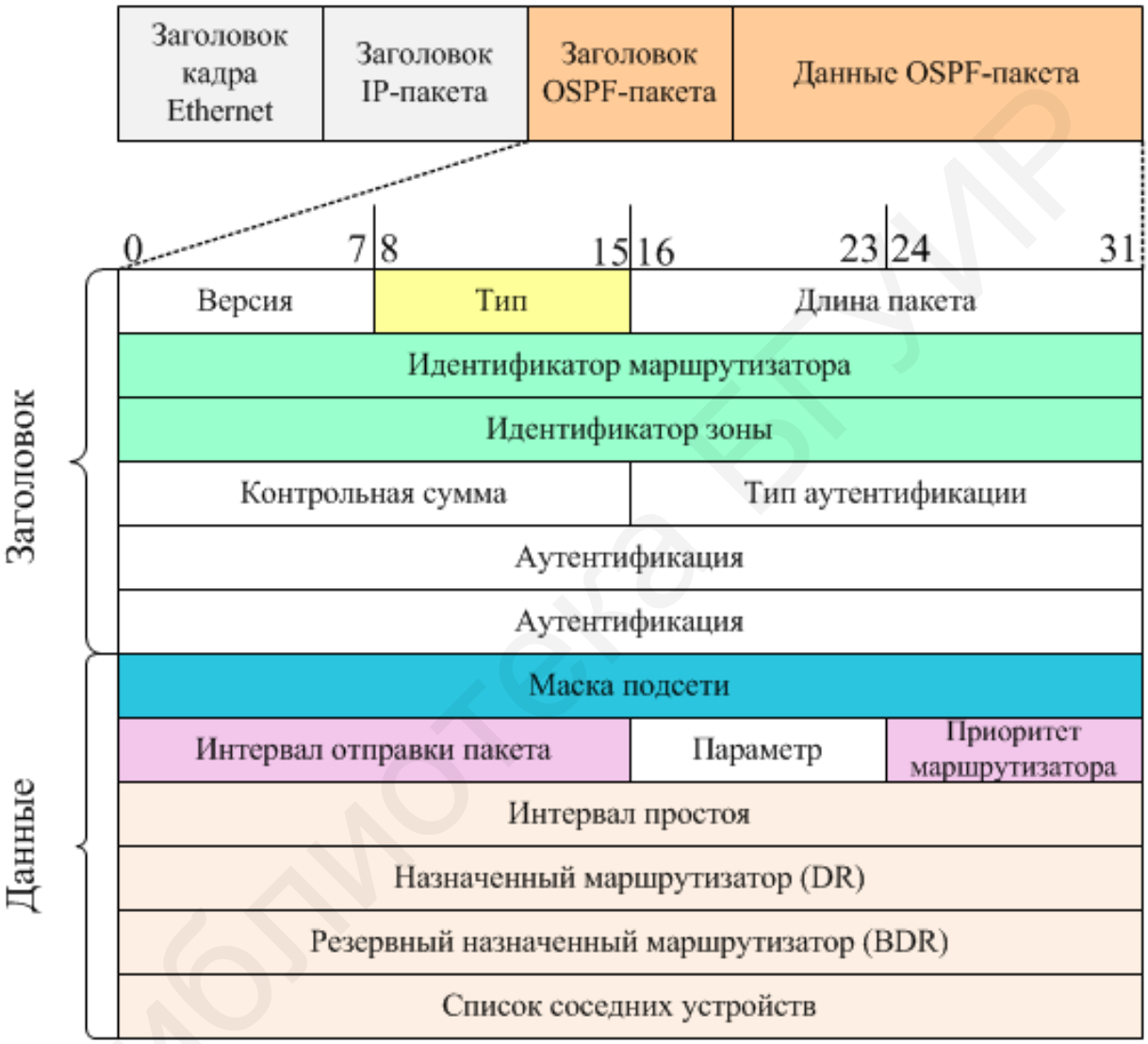


Рисунок 4.1 – Содержимое пакета приветствия OSPF

Выделенный маршрутизатор (designated router, DR) управляет процессом рассылки LSA в сети. Каждый маршрутизатор устанавливает отношения соседства с DR. Сведения об изменениях в сети отправляется DR-маршрутизатором, обнаружившим это изменение, а DR отвечает за то, чтобы эта информация была отправлена остальным маршрутизаторам сети [11].

Каждый маршрутизатор сети устанавливает отношения соседства не только с DR, но и с **резервным выделенным маршрутизатором (backup**

designated router, BDR). DR и BDR также устанавливают отношения соседства между собой. При выходе из строя DR, BDR становится DR и выполняет все его функции.

Протокол OSPFv2 включается с помощью команды режима глобальной конфигурации `router ospf process-id`. Значение `process-id` представляет собой число в диапазоне от 1 до 65535. `Process-id` имеет локальное значение, т. е. оно не обязательно должно быть идентичным значениям на соседних маршрутизаторах OSPF для установления отношений смежности между этими устройствами.

Для определения интерфейсов для OSPFv2 используется команда `network-address wildcard-mask area area-id`.

При настройке OSPFv2 для одной области на всех маршрутизаторах необходимо настроить команду `network` с одинаковым значением `area-id`. Несмотря на то что можно использовать любой идентификатор области, для OSPF одной области рекомендуется использовать идентификатор 0. Такое условное обозначение упрощает включение поддержки OSPFv2 для нескольких областей в случае изменений сети в будущем.

OSPFv2 является бесклассовым протоколом, следовательно, для работы с ним всегда требуется шаблонная маска или, как ее еще называют, wildcard-маска. При определении интерфейсов, участвующих в процессе маршрутизации, шаблонная маска, как правило, представляет собой обратную величину маски подсети, настроенной для этого интерфейса. Шаблонная маска – это строка из 32-х двоичных цифр, используемая маршрутизатором для определения битов адреса, которые будут рассматриваться на предмет совпадения. В маске подсети двоичное значение 1 равно совпадению, а двоичное значение 0 не является совпадением. В отношении шаблонной маски верно обратное. **Бит 0 шаблонной маски** совпадает с соответствующим значением бита в адресе. **Бит 1 шаблонной маски** игнорирует соответствующее значение бита в адресе. Простейший способ рассчитать шаблонную маску – вычесть маску подсети из 255.255.255.255 (рисунок 4.2) [4].

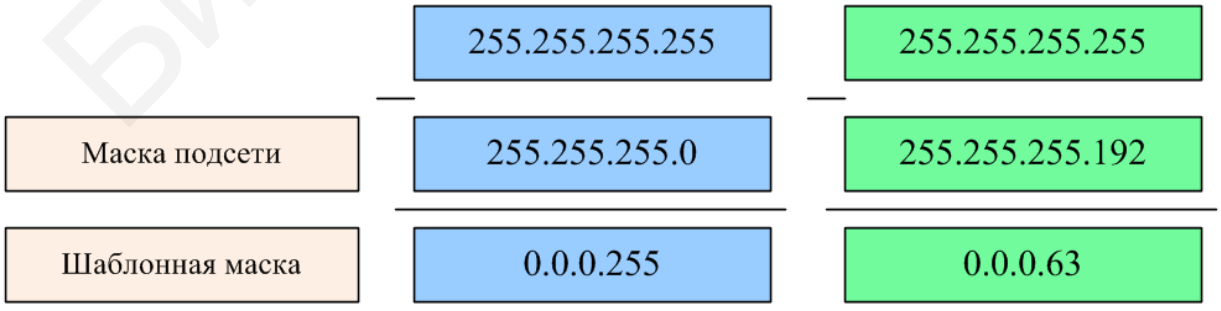


Рисунок 4.2 – Пример вычисления шаблонной маски для масок 255.255.255.0 и 255.255.255.192

В качестве примера рассмотрим сеть, представленную на рисунке 4.3, для которой был выделен адрес 172.20.0.0/24, разделенный на 17 подсетей, как показано в таблице 4.4. Также в данной таблице рассчитана шаблонная маска для каждой сети. Все это существенно облегчает процесс настройки на каждом устройстве.

Для машрутизатора Router1 (рисунок 4.3) настройка протокола OSPFv2 осуществлялась следующим образом:

```
Router1(config)#route ospf 1
Router1(config-router)#network 172.20.0.0 0.0.0.7 area 1
Router1(config-router)#network 172.20.0.16 0.0.0.7 area 1
Router1(config-router)#network 172.20.0.8 0.0.0.7 area 1
Router1(config-router)#network 172.20.0.40 0.0.0.7 area 1
Router1(config-router)#network 172.20.0.60 0.0.0.3 area 1
Router1(config-router)#network 172.20.0.92 0.0.0.3 area 1
Router1(config-router)#network 172.20.0.64 0.0.0.3 area 1
```

Для остальных маршрутизаторов настройка осуществлялась аналогичным образом.

Идентификатор маршрутизатора используется для уникальной идентификации маршрутизатора в домене маршрутизации OSPF и настраивается напрямую посредством команды режима глобальной конфигурации OSPFv2 `router-id rid`. Значение `rid` является любым 32-битным значением, выраженным как IPv4-адрес. В сети выбор маршрутизатора DR осуществляется непосредственно в процессе организации сети OSPFv2. При активации каналов OSPF устройство маршрутизации, для которого настроен наивысший приоритет, назначается маршрутизатором DR. В случае если приоритет не настроен или он одинаков, маршрутизатором DR выбирается маршрутизатор с самым высоким значением идентификатора. Устройство маршрутизации со следующим значением идентификатора выбирается в качестве маршрутизатора BDR.

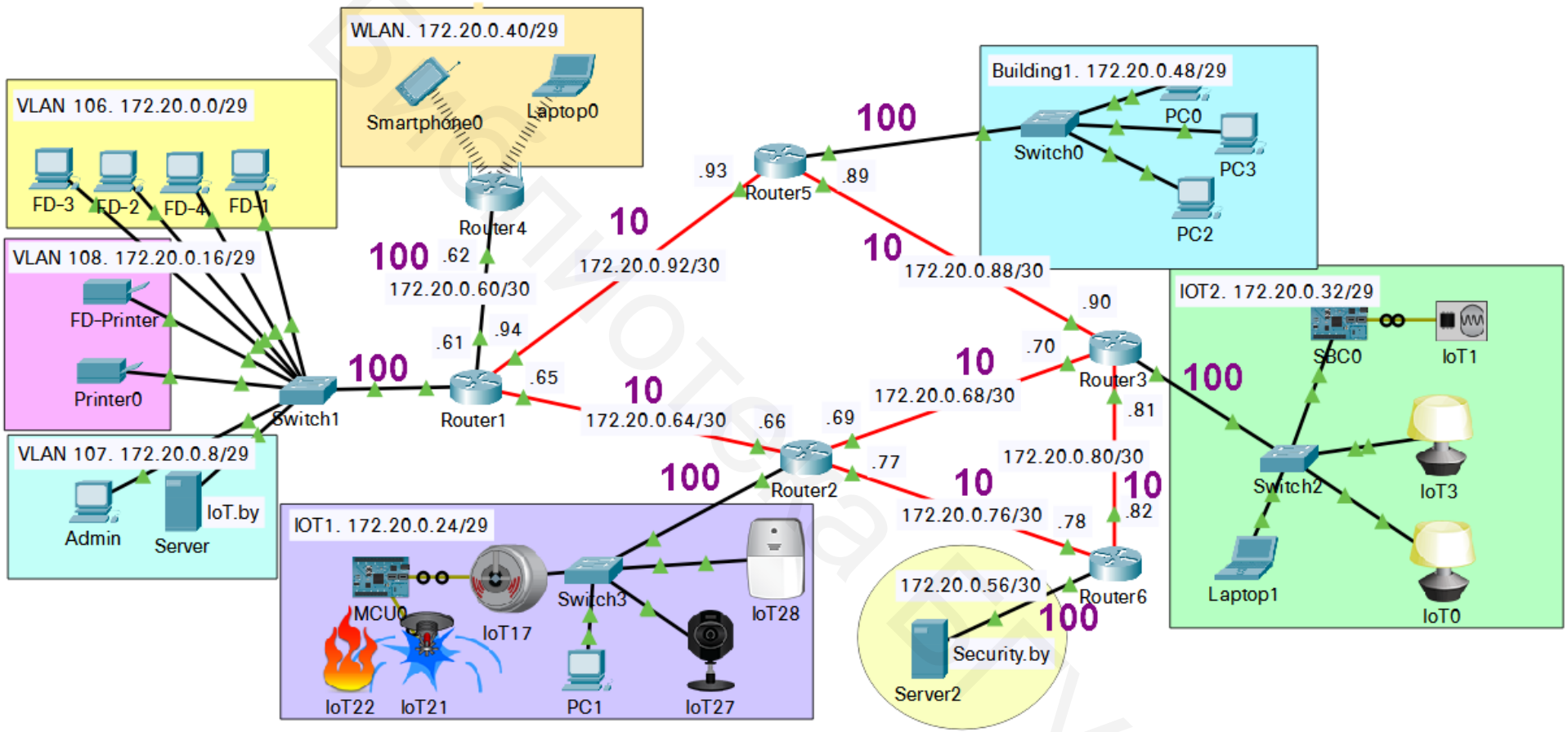


Рисунок 4.3 – Пример сети с маршрутизацией по состоянию канала

Идентификатор может быть получен одним из следующих способов:

- на основе наивысшего активного IP-адреса любого из физических интерфейсов маршрутизатора;

- на основе наивысшего IP-адреса любого из loopback-адресов маршрутизатора;

- на основе IP-адреса, установленного с помощью команды OSPF `router-id`.

Изначально на маршрутизаторах не настроены идентификаторы или loopback-интерфейсы, и идентификатор каждого маршрутизатора определяется наивысшим IP-адресом любого активного интерфейса. Данный метод не рекомендуется использовать, т. к. в этом случае администратору сложнее различать маршрутизаторы.

Таблица 4.4 – Разделение сети 172.20.0.0/24 на подсети

Название подсети	IP-адрес подсети	Диапазон адресов	Шаблонная маска
VLAN 106	172.20.0.0/29	172.20.0.1–172.20.0.6	0.0.0.7
VLAN 107	172.20.0.8/29	172.20.0.9–172.20.0.14	0.0.0.7
VLAN 108	172.20.0.16/29	172.20.0.17–172.20.0.22	0.0.0.7
Сеть IOT1	172.20.0.24/29	172.20.0.25–172.20.0.30	0.0.0.7
Сеть IOT2	172.20.0.32/29	172.20.0.33–172.20.0.38	0.0.0.7
WLAN	172.20.0.40/29	172.20.0.41–172.20.0.46	0.0.0.7
Сеть Building1	172.20.0.48/29	172.20.0.49–172.20.0.54	0.0.0.7
Server	172.20.0.56/30	172.20.0.57–172.20.0.58	0.0.0.3
Router1–Router4	172.20.0.60/30	172.20.0.61–172.20.0.62	0.0.0.3
Router1–Router2	172.20.0.64/30	172.20.0.65–172.20.0.66	0.0.0.3
Router2–Router3	172.20.0.68/30	172.20.0.69–172.20.0.70	0.0.0.3
Router2–Router6	172.20.0.76/30	172.20.0.77–172.20.0.78	0.0.0.3
Router3–Router6	172.20.0.80/30	172.20.0.81–172.20.0.82	0.0.0.3
Router3–Router5	172.20.0.88/30	172.20.0.89–172.20.0.90	0.0.0.3
Router5–Router1	172.20.0.92/30	172.20.0.93–172.20.0.94	0.0.0.3

Идентификатор маршрутизатора выглядит как IP-адрес, однако его маршрутизация невозможна, и, следовательно, он не включается в таблицу маршрутизации, если только процессом маршрутизации OSPF не выбран интерфейс (физический или логический loopback), который надлежащим образом определен командой `network`.

Для настройки идентификатора маршрутизатора Router1 (см. рисунок 4.3) с использованием loopback-адреса используются следующие команды:

```
Router1(config)#interface loopback 0
Router1(config-if)#ip address 1.1.1.1 255.255.255.255
```

После ввода команд для присвоения идентификатора маршрутизатору на основе значения loopback-адреса необходимо осуществить перезагрузку, выполнив команду `reload`. Аналогично настраиваются loopback-адреса на других маршрутизаторах. После перезагрузки всех маршрутизаторов с помощью команды `show ip protocols` можно узнать идентификатор маршрутизатора.

Еще один способ настройки идентификатора – команда `router-id`. Для маршрутизатора Router1 она реализуется следующим образом:

```
Router1(config)#router ospf 1
Router1(config-router)#router-id 11.11.11.11
Router1#clear ip ospf process
```

Для того чтобы изменения вступили в силу, необходимо либо перезагрузить маршрутизатор, либо использовать команду `clear ip ospf process` для удаления данных процесса маршрутизации OPSF. Аналогичным способом осуществляется настройка на других маршрутизаторах.

Команда `passive-interface` используется для блокировки передачи сообщений маршрутизации из определенного интерфейса. Тем не менее сеть, к которой относится указанный интерфейс, по-прежнему объявляется в сообщениях маршрутизации и отправляется из других интерфейсов.

Для уменьшения загруженности сети отправка обновлений маршрутизации из интерфейсов, не подключенных к другим маршрутизаторам, на маршрутизаторе Router1 блокируется следующим образом:

```
Router1(config)#route ospf 1
Router1(config-router)#passive-interface GigabitEthernet 1/0
Router1(config-router)#passive-interface GigabitEthernet 0/0
```

Проверить настройки интерфейса можно с помощью команды `show ip ospf interface GigabitEthernet 0/0` (рисунок 4.4).

```
Router1#sh ip ospf interface GigabitEthernet 0/0

GigabitEthernet0/0 is up, line protocol is up
  Internet address is 172.20.0.61/30, Area 1
  Process ID 1, Router ID 11.11.11.11, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State WAITING, Priority 1
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    No Hellos (Passive interface)
  Index 4/4, flood queue length 0
  Next 0x0(0)/0x0(0)
```

Рисунок 4.4 – Результат настройки пассивности интерфейса GigabitEthernet 0/0

Заданная пропускная способность по умолчанию для OSPF равна скорости FastEthernet (100 Мбит/с), однако скорость каналов в большинстве современных устройств сетевой инфраструктуры превышает 100 Мбит/с. Вследствие этого интерфейсы FastEthernet, GigabitEthernet и 10GigabitEthernet имеют одинаковую стоимость. Поэтому для правильного использования сетей со скоростью канала более 100 Мбит/с для заданной пропускной способности необходимо установить большее значение. С помощью команды `show interfaces GigabitEthernet 0/1/0` на маршрутизаторе Router1 можно узнать пропускную способность (рисунок 4.5).

```
Router1#show interfaces GigabitEthernet 0/1/0
GigabitEthernet0/1/0 is up, line protocol is up (connected)
  Hardware is CN Gigabit Ethernet, address is 0050.0fb5.9d50 (bia
0050.0fb5.9d50)
  Internet address is 172.20.0.65/30
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
```

Рисунок 4.5 – Пропускная способность интерфейса GigabitEthernet 0/1/0

По формуле (4.1) мы можем рассчитать стоимость интерфейса GigabitEthernet 0/1/0 (S):

$$S=\frac{100\ 000\ 000}{1\ 000\ 000\ 000}=0{,}1\approx 1. \qquad (4.2)$$

Значение стоимости выражается целым числом, ввиду этого полученное значение округляется до целого значения. При помощи команды `show ip ospf interface GigabitEthernet 0/1/0` мы можем удостовериться, что стоимость действительно равна 1 (рисунок 4.6).

```
Router1#show ip ospf interface GigabitEthernet 0/1/0

GigabitEthernet0/1/0 is up, line protocol is up
  Internet address is 172.20.0.65/30, Area 1
  Process ID 1, Router ID 11.11.11.11, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router (ID) 22.22.22.22, Interface address 172.20.0.66
```

Рисунок 4.6 – Стоимость интерфейса GigabitEthernet 0/1/0

Необходимо отметить, что в таблице маршрутизации Router1 метрика до сети 172.20.0.56 равна 3, т. к. маршрут к данной сети проходит через интерфейсы маршрутизаторов Router2 и Router3 (рисунок 4.3), пропускная способность которых такая же, а значит, равна и стоимость. Суммарная стоимость маршрута равна 3 (рисунок 4.7).

```
Router1#show ip route ospf
     172.20.0.0/16 is variably subnetted, 20 subnets, 3 masks
O       172.20.0.48 [110/2] via 172.20.0.93, 00:01:45, GigabitEthernet0/0/0
O       172.20.0.56 [110/3] via 172.20.0.66, 00:01:45, GigabitEthernet0/1/0
O       172.20.0.68 [110/2] via 172.20.0.66, 00:01:45, GigabitEthernet0/1/0
O       172.20.0.72 [110/2] via 172.20.0.66, 00:01:45, GigabitEthernet0/1/0
O       172.20.0.76 [110/2] via 172.20.0.66, 00:01:45, GigabitEthernet0/1/0
O       172.20.0.80 [110/3] via 172.20.0.66, 00:01:45, GigabitEthernet0/1/0
                    [110/3] via 172.20.0.93, 00:01:45, GigabitEthernet0/0/0
O       172.20.0.84 [110/3] via 172.20.0.66, 00:01:45, GigabitEthernet0/1/0
                    [110/3] via 172.20.0.93, 00:01:45, GigabitEthernet0/0/0
O       172.20.0.88 [110/2] via 172.20.0.93, 00:01:45, GigabitEthernet0/0/0
```

Рисунок 4.7 – Стоимость маршрута от Router1 к сети 172.20.0.56/30

Для настройки эталонной пропускной способности используется команда конфигурации маршрутизатора `auto-cost reference-bandwidth Mb/s`. Эту команду необходимо настроить на всех маршрутизаторах. Изменение эталонной пропускной способности фактически не изменяет ширину полосы пропускания канала и влияет только на расчеты при определении метрики. Для настройки других значений используются следующие команды:

- для GigabitEthernet – `auto-cost reference-bandwidth 1000`;
- для 10GigabitEthernet – `auto-cost reference-bandwidth 10000`.

Для возврата к значению заданной пропускной способности по умолчанию используется команда `auto-cost reference-bandwidth 100`.

При изменении параметра заданной пропускной способности по умолчанию с помощью команды `auto-cost reference-bandwidth 10000` на маршрутизаторе Router1 стоимость интерфейсов 1 Гбит/с будет равна 10. Для введения изменений необходимо на всех маршрутизаторах изменить параметр заданной пропускной способности по умолчанию. В этом случае стоимость маршрута до сети 172.20.0.56 будет равна 120 (рисунок 4.8). Если устройство,

подключенное к интерфейсу GigabitEthernet 0/0 маршрутизатора Router6, не поддерживает скорость GigabitEthernet, то стоимость будет отличаться от отображаемых выходных данных. Например, для скорости FastEthernet (100 Мбит/с) стоимость будет равна 100. На рисунке 4.3 отмечены стоимости интерфейсов. Стоимость маршрута от Router1 до сети 172.20.0.56 равна 120.

```
Router1#show ip route ospf
     172.20.0.0/16 is variably subnetted, 20 subnets, 3 masks
O       172.20.0.48 [110/110] via 172.20.0.93, 00:00:32, GigabitEthernet0/0/0
O       172.20.0.56 [110/120] via 172.20.0.66, 00:00:32, GigabitEthernet0/1/0
O       172.20.0.68 [110/20] via 172.20.0.66, 00:00:32, GigabitEthernet0/1/0
O       172.20.0.72 [110/110] via 172.20.0.66, 00:00:32, GigabitEthernet0/1/0
O       172.20.0.76 [110/20] via 172.20.0.66, 00:00:32, GigabitEthernet0/1/0
O       172.20.0.80 [110/30] via 172.20.0.66, 00:00:32, GigabitEthernet0/1/0
                    [110/30] via 172.20.0.93, 00:00:32, GigabitEthernet0/0/0
O       172.20.0.84 [110/120] via 172.20.0.66, 00:00:32, GigabitEthernet0/1/0
                    [110/120] via 172.20.0.93, 00:00:32, GigabitEthernet0/0/0
O       172.20.0.88 [110/20] via 172.20.0.93, 00:00:32, GigabitEthernet0/0/0
```

Рисунок 4.8 – Стоимость маршрута от Router1 к сети 172.20.0.56/30

В большинстве интерфейсов метрика пропускной способности имеет значение по умолчанию. В случае если реальная скорость отличается, для правильного расчета стоимости маршрута в OSPF параметр пропускной способности нужно изменить, чтобы он был равен фактической скорости. Для этого используется команда `bandwidth`. Команда изменяет метрику пропускной способности, используемой алгоритмом OSPF для расчета стоимости маршрутизации, но не изменяет фактическую пропускную способность (скорость) канала. Например, для маршрутизатора Router1 (см. рисунок 4.3) изменить пропускную способность интерфейса GigabitEthernet 0/1/0 с 1 Гбит/с на 512 Мбит/с можно с помощью команды `bandwidth 512000`. После сохранения конфигурации и перезагрузки маршрутизатора таблица маршрутизации перестраивается (сравните с рисунком 4.7), все маршруты строятся через интерфейс GigabitEthernet 0/0/0, т. к. его пропускная способность составляет 1 Гбит/с (рисунок 4.9).

```
Router1#show ip route ospf
     172.20.0.0/16 is variably subnetted, 20 subnets, 3 masks
O       172.20.0.48 [110/2] via 172.20.0.93, 00:00:14, GigabitEthernet0/0/0
O       172.20.0.56 [110/4] via 172.20.0.93, 00:00:14, GigabitEthernet0/0/0
O       172.20.0.68 [110/5] via 172.20.0.93, 00:00:14, GigabitEthernet0/0/0
O       172.20.0.72 [110/5] via 172.20.0.93, 00:00:14, GigabitEthernet0/0/0
O       172.20.0.76 [110/4] via 172.20.0.93, 00:00:14, GigabitEthernet0/0/0
O       172.20.0.80 [110/3] via 172.20.0.93, 00:00:14, GigabitEthernet0/0/0
```

Рисунок 4.9 – Изменение таблицы маршрутизации в результате уменьшения пропускной способности интерфейса GigabitEthernet 0/1/0

Возможна ручная настройка значения стоимости при использовании команды конфигурации интерфейса `ip ospf cost`. Преимущество настройки

стоимости в сравнении с настройкой пропускной способности интерфейса заключается в том, что маршрутизатору не требуется рассчитывать метрику. И, напротив, если настраивается пропускная способность интерфейса, маршрутизатор должен рассчитывать стоимость OSPFv2 с учетом пропускной способности. Команду `ip ospf cost` рекомендуется использовать в неоднородных средах, где маршрутизаторы разных производителей могут использовать для расчета значений стоимости OSPFv2 метрику, отличную от значения пропускной способности.

4.2 Лабораторное задание

Лабораторная работа выполняется на основе настроек, произведенных в задании 1 лабораторной работы № 2. До начала выполнения необходимо открыть сохраненный файл с именем **Lab2.pkt**, полученный в лабораторной работе № 2, и проверить настройки IP-адресации маршрутизаторов: маршрутизация не должна быть настроена. В существующую сеть добавить сеть Building1, содержащую три компьютера, сеть с сервером Security.by и два маршрутизатора. Соединение сетей осуществить, как показано на рисунке 4.10. На сервере Security.by должны отображаться статусы устройств, добавленных в лабораторной работе № 1. По результатам выполнения данной лабораторной работы все устройства любой из подсети должны иметь доступ к серверам, на которых должны отображаться статусы всех IoT-устройств и условия их работы. Доступ к серверам должен осуществляться посредством DNS.

В данной лабораторной работе необходимо настроить маршрутизации по состоянию канала, исходя из следующих заданий.

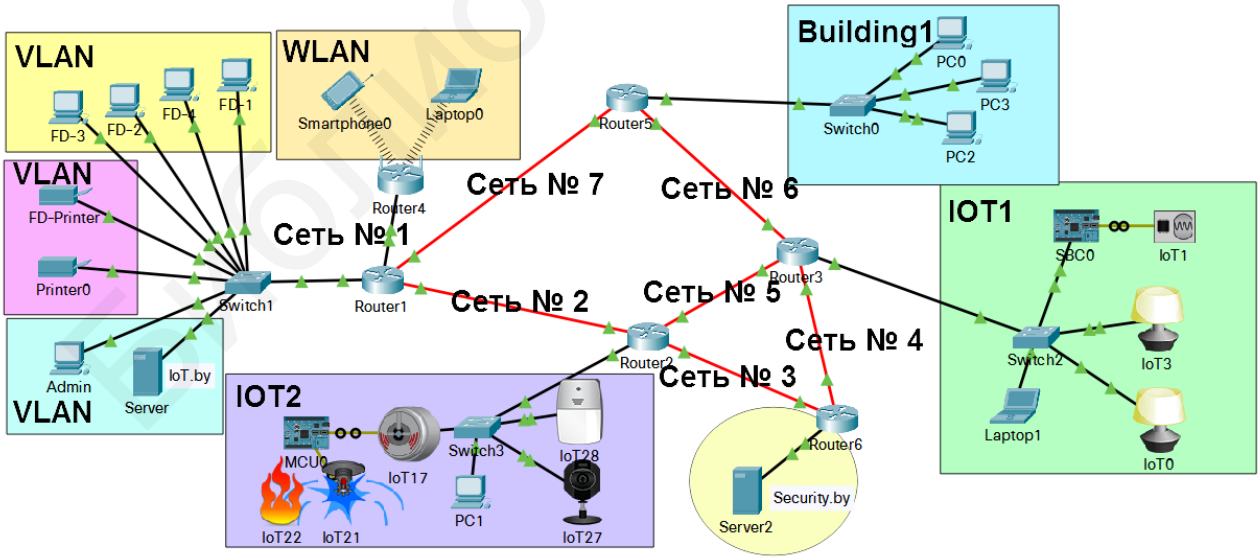


Рисунок 4.10 – Пример моделирования сети в Cisco Packet Tracer

1. Настроить бесклассовую IP-адресацию. Из таблицы 4.5 в соответствии с третьей цифрой шифра выбрать IP-адрес сети, осуществить разделение на

подсети с использованием VLSM и заполнить таблицу 4.6. Осуществить настройку всех устройств в сети. Сохранить файл под именем **Lab4.pkt**.

Таблица 4.5 – Исходные данные для настройки маршрутизации по состоянию канала

Вторая цифра шифра	IP-адрес сети	Значение process-id	Router-id	Пропускная способность по умолчанию, Мбит/с	Пропускная способ-ность интерфейса, Кбит/с
0	172.16.0.0/20	10	10.10.10.10	3000	512
1	172.17.0.0/21	20	20.20.20.20	10000	256
2	172.18.0.0/22	30	30.30.30.30	6000	128
3	172.19.0.0/23	40	40.40.40.40	50000	512
4	172.21.0.0/22	50	15.15.15.15	4000	256
5	172.22.0.0/23	60	25.25.25.25	20000	128
6	172.23.0.0/24	70	35.35.35.35	100000	512
7	172.24.0.0/24	80	45.45.45.45	2000000	256
8	172.30.0.0/21	90	13.13.13.13	1000000	128
9	172.31.0.0/20	12	18.18.18.18	200000	512

Таблица 4.6 – Результаты разделения заданной сети на подсети

Номер подсети	IP-адрес подсети	Диапазон адресов	Шаблонная маска
VLAN			
VLAN			
VLAN			
WLAN			
Сеть Building1			
Сервер Security.by			
Router1–Router4			
Router1–Router2			
Router2–Router3			
Router2–Router6			

Номер подсети	IP-адрес подсети	Диапазон адресов	Шаблонная маска
Router3–Router6			
Router3–Router5			
Router5–Router1			

2. Настроить протокол OSPFv2 на всех маршрутизаторах с указанием process-id в соответствии с исходными данными из таблицы 4.5. Настроить пассивные интерфейсы на каждом маршрутизаторе. Определить DR- и BDR-маршрутизаторы, внести данные в таблицу 4.7. Представить в отчете результаты выполнения команды `show ip protocols` для DR-маршрутизатора. Сохранить файл под именем **Lab4-2.pkt**.

3. Настроить loopback-интерфейсы. Осуществить настройку loopback-интерфейсов на каждом маршрутизаторе в соответствии со следующими IP-адресами:

- Router1: 1.1.1.1/32;
- Router2: 2.2.2.2/32;
- Router3: 3.3.3.3/32;
- Router4: 4.4.4.4/32;
- Router5: 5.5.5.5/32.

Данные внести в таблицу 4.7. Сохранить файл под именем **Lab4-3.pkt.**

4. Настроить идентификаторы маршрутизаторов в соответствии с исходными данными из таблицы 4.5. Для каждого последующего маршрутизатора значение каждого октета увеличивать на 1. Данные внести в таблицу 4.7. Сохранить файл под именем **Lab4-4.pkt**.

Таблица 4.7 – Определение DR- и BDR-маршрутизаторов

Имя маршрутизатора	До настройки идентификаторов маршрутизаторов		Настройка loopback		Настройка идентификаторов маршрутизаторов		Passive-interface
	Router ID	DR/ BDR	Router ID	DR/ BDR	Router ID	DR/ BDR	
Router1							
Router2							
Router3							
Router4							
Router5							

5. Проанализировать таблицу маршрутизации. В отчете представить изображение смоделированной сети с обозначением стоимости каждого маршрута (см. рисунок 4.3) и таблицу маршрутизации маршрутизатора Router1. Сохранить файл под именем **Lab4-5.pkt**.

6. В соответствии с исходными данными из таблицы 4.5 изменить пропускную способность на каждом маршрутизаторе. В отчете представить изображение смоделированной сети с обозначением стоимости каждого маршрута (см. рисунок 4.3) и таблицу маршрутизации выделенного маршрутизатора. Сохранить файл под именем **Lab4-6.pkt**.

7. Изменить пропускную способность на маршрутизаторе Router3 для любого интерфейса в соответствии с исходными данными из таблицы 4.5. В отчете представить изображение смоделированной сети с обозначением стоимости каждого маршрута (см. рисунок 4.3) и таблицу маршрутизации маршрутизатора Router3. Сохранить файл под именем **Lab4-7.pkt**.

8. Изменить пропускную способность на маршрутизаторе Router2 для любого интерфейса в соответствии с исходными данными из таблицы 4.5. В отчете представить изображение смоделированной сети с обозначением стоимости каждого маршрута (см. рисунок 4.3) и таблицу маршрутизации маршрутизатора Router2. Сохранить файл под именем **Lab4-8.pkt**.

4.3 Содержание отчета

1. Цель работы, исходные данные из таблицы 4.5.
2. Результаты произведенных настроек (заполненные таблицы 4.6, 4.7, см. задания 2, 5–8 подраздела 4.2), изображения смоделированной в данной работе сети со стоимостью маршрутов.
3. Вывод по работе.
4. Ответы на контрольные вопросы.

4.4 Контрольные вопросы и задания

1. Объяснить алгоритм поиска кратчайшего пути.
2. Что такое протокол OSPFv2, как происходит определение стоимости маршрутов?
3. Описать базы данных протокола OSPF.
4. Перечислить типы сообщений протокола OSPFv2.
5. Перечислить действия маршрутизаторов, использующих протокол OSPFv2.
6. Перечислить состояния маршрутизатора, использующего протокол OSPFv2, в процессе сходимости.
7. Описать содержание сообщения протокола OSPFv2.
8. Чем отличается выделенный маршрутизатор от резервного?
9. Перечислить принципы настройки протокола OSPFv2 на маршрутизаторе.

ЛАБОРАТОРНАЯ РАБОТА № 5
МАРШРУТИЗАЦИЯ В СЕТЯХ IPV6

Цель: изучить принципы настройки IPv6-адресации, особенности конфигурации DHCP- и DNS-серверов в IPv6-сетях; овладеть навыками настройки IPv6-адресации, DHCP и статической маршрутизации для IPv6-сетей.

5.1 Теоретическая часть

С ростом популярности Интернета появилась проблема ограниченного адресного пространства IPv4-адресации. Сокращение адресного пространства протокола IPv4 стало причиной перехода к использованию IPv6. Теоретическое максимальное количество IPv4-адресов составляет $4{,}3 \cdot 10^9$. В протоколе IPv6 адресное пространство составляет 128 бит, что достаточно для генерации $340 \cdot 10^{36}$ адресов.

Настройка IPv6-адресации похожа на настройку IPv4. Большинство команд конфигурации и проверки IPv6 в Cisco IOS идентичны своим аналогам IPv4. Во многих случаях единственным отличием между ними является использование в командах `ipv6` вместо `ip`.

Для настройки интерфейса IPv6 необходимо выполнить следующие действия.

1. Настроить IPv6-адрес и длину префикса с помощью команды конфигурации интерфейса `ipv6 address ipv6-address/prefix-length`.

2. Активировать интерфейс с помощью команды `no shutdown`.

Интерфейс может сгенерировать собственный локальный IPv6-адрес с помощью команды конфигурации интерфейса `ipv6 enable`.

В отличие от IPv4 интерфейсы с IPv6 обычно используют несколько IPv6-адресов [4]. Устройство IPv6 должно иметь как минимум локальный и глобальный индивидуальный IPv6-адреса. Кроме того, в рамках IPv6 интерфейс может иметь несколько глобальных индивидуальных IPv6-адресов для одной подсети. Для создания глобального индивидуального IPv6-адреса можно использовать команду `ipv6 address ipv6-address /prefix-length eui-64`, которая реализует процесс EUI-64.

Команда `ipv6 address ipv6-address /prefix-length link-local` настраивает статический локальный адрес канала на интерфейсе, который используется вместо автоматически настроенного локального адреса канала, когда глобальный индивидуальный IPv6-адрес назначается интерфейсу или включается с помощью команды `ipv6 enable`. Команда интерфейса `ipv6 enable` используется для автоматического создания локального IPv6-адреса канала вне зависимости от того, был ли назначен глобальный индивидуальный адрес.

Например, для сети представленной на рисунке 5.1, выделен IPv6-адрес 2001:DB8:ACAD::/64. Известно, что для разделения на подсети необходимо

изменить шестнадцатеричное значение в четвертом гекстете. Таким образом, можно получить подсети с адресами от 2001:0DB8:ACAD:0000::/64 до 2001:0DB8:ACAD:FFFF::/64. Для удобства настройки интерфейсов в таблице 5.1 и на рисунке 5.1 представлена IPv6-адресация каждого интерфейса маршрутизатора.

Таблица 5.1 – IPv6-адресация интерфейсов маршрутизаторов

Имя устройства или сети	Имя интерфейса	Глобальный адрес	Локальный адрес
Router1	GigabitEthernet 0/0/0	2001:DB8:ACAD:3::1/64	FE80::1
	GigabitEthernet 0/1/0	2001:DB8:ACAD:1::1/64	
	GigabitEthernet 0/1.6	2001:DB8:ACAD:106::1/64	
	GigabitEthernet 0/1.7	2001:DB8:ACAD:107::1/64	
	GigabitEthernet 0/1.8	2001:DB8:ACAD:108::1/64	
Router2	GigabitEthernet 0/2/0	2001:DB8:ACAD:1::2/64	FE80::2
	GigabitEthernet 0/3/0	2001:DB8:ACAD:2::1/64	
	GigabitEthernet 0/0	2001:DB8:ACAD:300::1/64	
Router3	GigabitEthernet 0/1/0	2001:DB8:ACAD:3::2/64	FE80::3
	GigabitEthernet 0/3/0	2001:DB8:ACAD:2::2/64	
	GigabitEthernet 0/0	2001:DB8:ACAD:200::1/64	

Например, для настройки интерфейса GigabitEthernet 0/0/0 маршрутизатора Router1 используются следующие команды:

```
Router1(config)#interface gigabitEthernet 0/0/0
Router1(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64
Router1(config-if)#ipv6 address FE80::1 link-local
Router1(config-if)#exit
```

Аналогичным образом настраиваются остальные интерфейсы на всех маршрутизаторах. Маршрутизатор Router1 подключен к VLAN. Для настройки IPv6 необходимо на каждом sub-интерфейсе удалить IPV4-адрес командой `no ip address` и осуществить настройку IPv6-адреса, как показано выше.

IPv6-адресация на устройствах может быть настроена как ручным способом, так и автоматически. Устройства могут получить глобальный индивидуальный IPv6-адрес посредством автоконфигурации без сохранения состояния адреса (SLAAC) или при помощи DHCPv6.

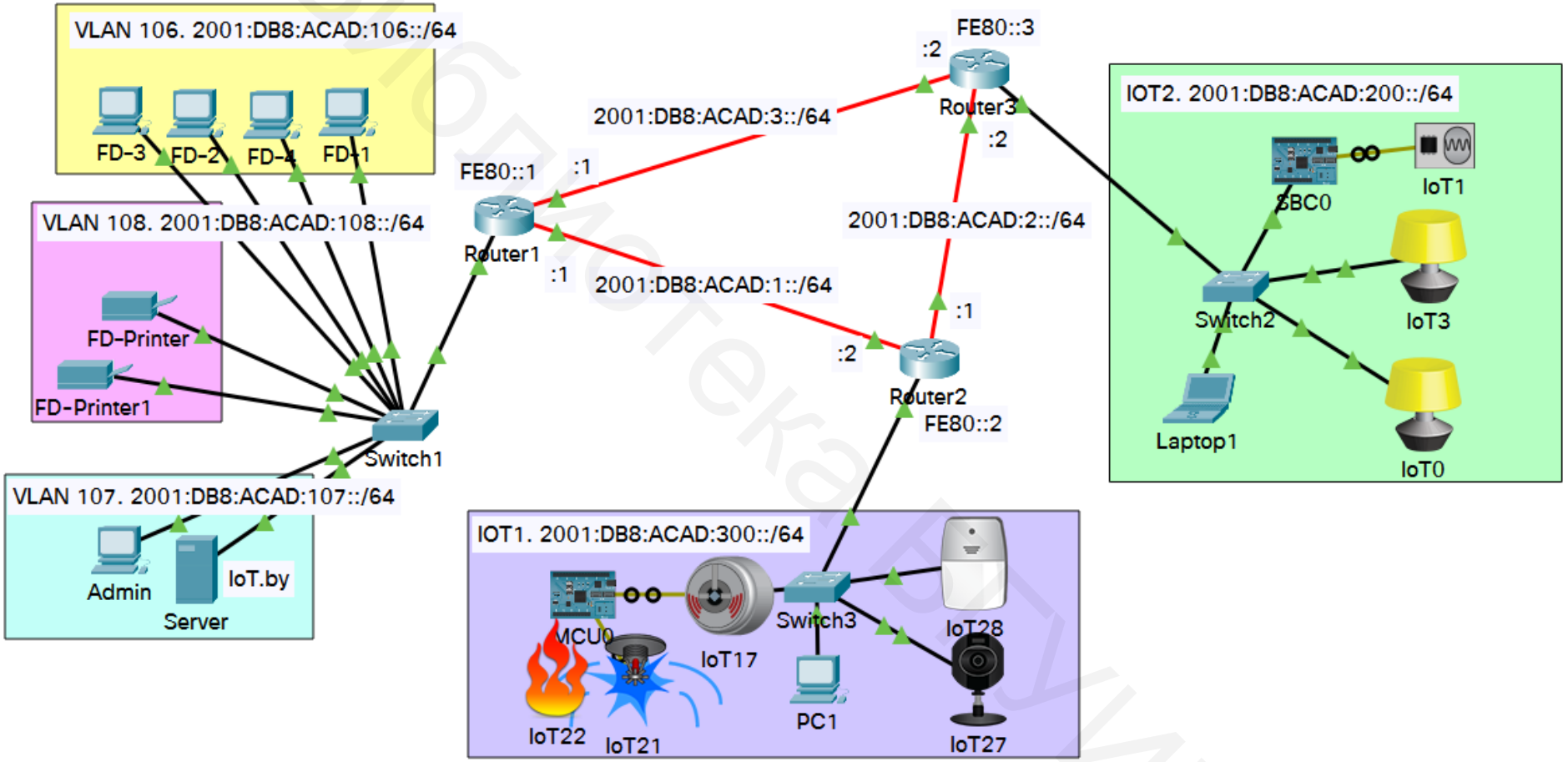


Рисунок 5.1 – Пример смоделированной сети с IPv6-адресацией

SLAAC (Stateless Address Autoconfiguration) – способ получения устройством префикса, длины префикса и адреса шлюза по умолчанию от маршрутизатора IPv6 без помощи DHCPv6-сервера. При использовании SLAAC для получения необходимой информации устройства полагаются на сообщения «Объявления маршрутизатора ICMPv6» [6].

IPv6-маршрутизаторы периодически передают сообщения «Объявления маршрутизатора ICMPv6» всем устройствам в сети под управлением IPv6. По умолчанию маршрутизаторы Cisco отправляют такие сообщения каждые 200 секунд на адрес групповой передачи всем IPv6-узлам. IPv6-устройству, находящемуся в сети, не нужно ждать этих периодических сообщений. Устройство может отправить сообщение «Запрос маршрутизатора ICMPv6», который использует адрес групповой передачи всем IPv6-узлам. Когда маршрутизатор IPv6 получает такое сообщение, он сразу же отправляет в ответ объявление маршрутизатора.

IPv6-маршрутизация не включена по умолчанию. Чтобы маршрутизатор работал как IPv6-маршрутизатор, необходимо использовать команду глобальной конфигурации `ipv6 unicast-routing`.

Сообщение «Объявления маршрутизатора ICMPv6» содержит префикс, длину префикса и другие сведения IPv6-устройства. Кроме того, такое сообщение указывает IPv6-устройству один из следующих способов получения информации по адресации.

- **SLAAC.** Устройство должно использовать префикс, длину префикса и шлюз по умолчанию, которые содержатся в сообщении «Объявления маршрутизатора». Другая информация недоступна с DHCPv6-сервера.

- **SLAAC и DHCPv6.** Устройство должно использовать префикс, длину префикса и шлюз по умолчанию, которые содержатся в сообщении «Объявления маршрутизатора». На DHCPv6-сервере доступна и другая информация, например, адрес DNS-сервера. Устройство получит эти дополнительные данные в процессе поиска и запросов к DHCPv6-серверу. Этот процесс называется «DHCPv6 без запоминания состояний», поскольку DHCPv6-серверы не выделяют и не отслеживают какие-либо назначения IPv6-адресов, а предоставляют дополнительную информацию, например, об адресе DNS-сервера.

- **DHCPv6.** Устройство не должно использовать данные из сообщения «Объявления маршрутизатора» для получения информации об адресации. Вместо этого устройство использует обычные процессы поиска и запросов к DHCPv6-серверам для получения всей информации об адресации, включающей в себя индивидуальный адрес IPv6, длину префикса, адрес шлюза по умолчанию и адреса DNS-серверов. В этом случае DHCPv6-сервер работает как DHCP-сервер, который фиксирует данные аналогично DHCP-серверу для IPv4.

DHCPv6-сервер выделяет и отслеживает IPv6-адреса, чтобы не назначать один и тот же IPv6-адрес для нескольких устройств.

В основе SLAAC лежит протокол ICMPv6. Он аналогичен ICMPv4, но при этом имеет дополнительные функциональные возможности и демонстрирует большую устойчивость к ошибкам. SLAAC использует ICMPv6-сообщения запроса маршрутизатора и объявления маршрутизатора, чтобы предоставлять информацию об адресации и другую информацию о конфигурации, обычно предоставляемую DHCP-сервером.

Сообщение запроса маршрутизатора (RS) отправляются, если клиент настроен на получение информации об адресации автоматически с использованием SLAAC, т. е. он посылает на маршрутизатор сообщение RS. Сообщение RS отправляется на IPv6-адрес многоадресной рассылки FF02::2, который поддерживают все маршрутизаторы.

Сообщение объявления маршрутизатора (RA) используется для предоставления информации об адресации. Маршрутизатор отправляет сообщения RA клиентам, настроенным на получение IPv6-адресов автоматически. Сообщение RA содержит префикс и длину префикса локального сегмента. Эта информация используется клиентом для создания собственного глобального индивидуального IPv6-адреса. Маршрутизатор передает сообщение RA периодически или в ответ на сообщение RS. По умолчанию маршрутизаторы Cisco отправляют сообщения RA каждые 200 секунд. Сообщения RA всегда отправляются на общий для всех узлов IPv6-адрес многоадресной рассылки FF02::1.

Как видно из термина, SLAAC не отслеживает состояние адреса: служба сообщает о том, что ни один из серверов не поддерживает информацию о сетевом адресе. В отличие от сервера DHCP сервер SLAAC не знает, какие IPv6-адреса используются, а какие доступны.

На рисунке 5.2 устройство PC1 настроено на автоматическое получение настроек IPv6-адресации. С момента загрузки PC1 не получил сообщений RA, поэтому он отправляет сообщение RS на адрес многоадресной рассылки, который поддерживают все маршрутизаторы, чтобы проинформировать локальный IPv6-маршрутизатор о необходимости получения сообщения RA.

Далее маршрутизатор принимает сообщение RS и отправляет в ответ сообщение RA, в него включены префикс и длина префикса сети. Сообщение отправляется на общий для всех узлов IPv6-адрес многоадресной рассылки FF02::1 с адресом канала маршрутизатора типа link-local в качестве IPv6-адреса источника.

Устройство PC1 получает сообщение RA, содержащее префикс и длину префикса для локальной сети и использует его для создания собственного глобального индивидуального IPv6-адреса. Теперь устройство PC1 имеет 64-разрядный префикс сети, но требует 64-битный идентификатор интерфейса (IPv6 Interface Identifier, IID) для создания глобального индивидуального адреса.

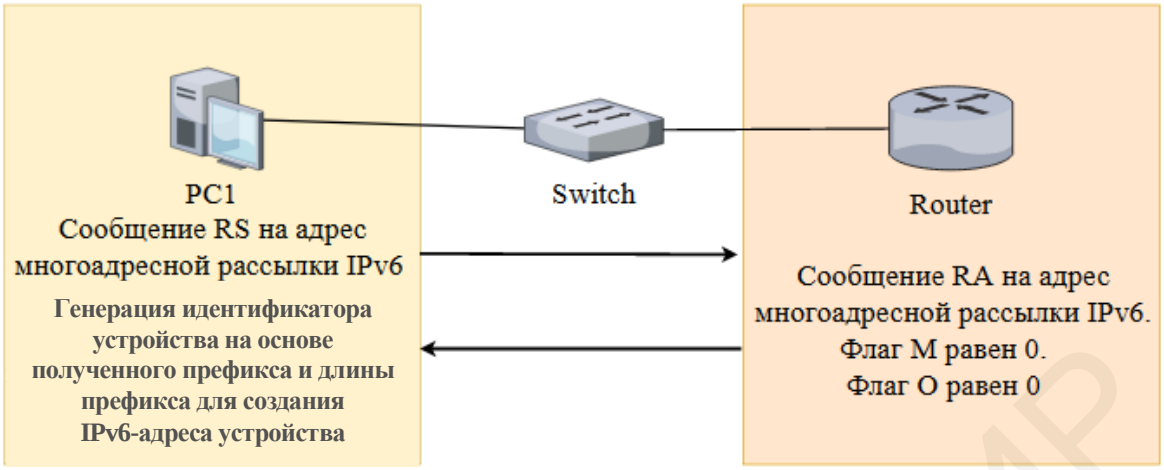


Рисунок 5.2 – Принцип работы SLACC

Существует два способа создания устройством PC1 собственного уникального IID: EUI-64 и генерация случайным образом.

Поскольку SLAAC – это процесс без отслеживания состояния, перед использованием устройством PC1 вновь созданного IPv6-адреса необходимо проверить его уникальность. PC1 посылает по протоколу ICMPv6 сообщение запроса поиска соседа с собственным адресом в качестве IPv6-адреса назначения. Если другие устройства не отвечают сообщением запроса поиска соседа, значит, адрес является уникальным и может быть использован. Если сообщение запроса поиска соседей получено, значит, адрес не уникален и операционная система должна установить новый идентификатор интерфейса для использования. Этот процесс является частью процесса обнаружения соседних устройств ICMPv6 и известен как обнаружение адресов-дубликатов (Duplicate Address Detection, DAD).

Настроен ли клиент на автоматическое получение информации об IPv6-адресации с использованием SLAAC, DHCPv6 или сочетанием обоих вариантов, зависит от настроек, содержащихся в сообщении RA. ICMPv6-сообщения RA содержат два флага, указывающих, какой из вариантов должен быть использован клиентом. Этими флагами являются флаг управляемой конфигурации адресов (M) и флаг другой конфигурации (O). Сообщения RA настраиваются на отдельном интерфейсе маршрутизатора. Для повторной активации режима SLAAC на интерфейсе, на котором мог быть установлен другой вариант работы, флаги M и O необходимо сбросить до их первоначального значения, равного 0 (см. рисунок 5.2). Для этого применяются команды режима конфигурации интерфейса `no ipv6 nd managed-config-flag` и `no ipv6 nd other-config-flag`.

DHCPV6 совместно с SLAAC. Для DHCPv6 без отслеживания состояния значение флага O установлено равным 1, а значение флага M остается со значением по умолчанию, равным 0. Значение флага O, равное 1, используется для информирования клиента о том, что на DHCPv6-сервере без отслеживания со-

стояния доступна дополнительная информация о конфигурации (рисунок 5.3). Для того чтобы изменить сообщение RA, отправляемое на интерфейс маршрутизатора для указания использования DHCPv6 без отслеживания состояния, используется команда `ipv6 nd other-config-flag`.

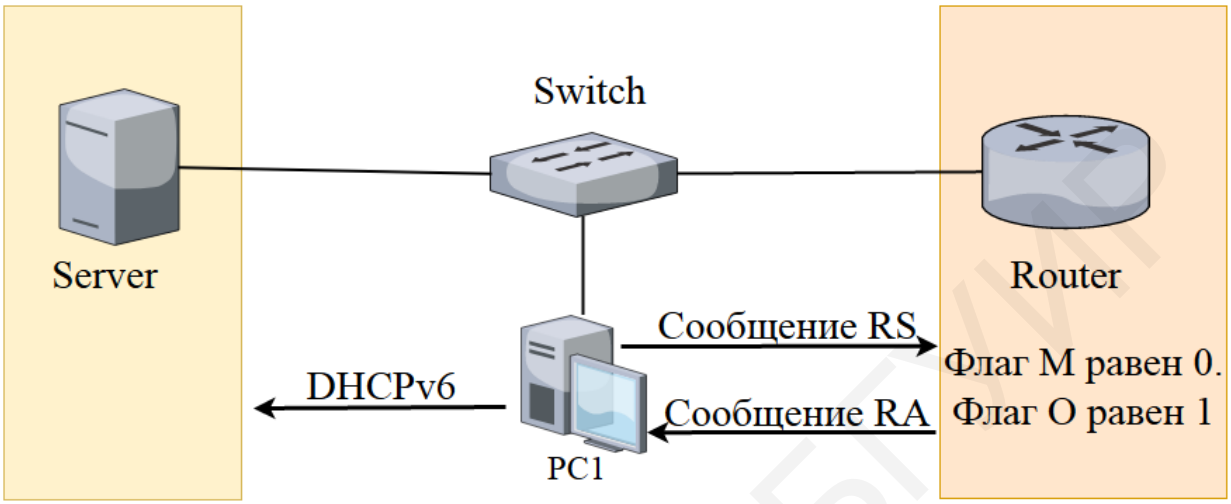


Рисунок 5.3 – Принцип работы SLACC с DHCPv6
без отслеживания состояния канала

Протокол DHCPv6 с отслеживанием состояния (только DHCPv6). Флаг M указывает, используется ли DHCPv6 с отслеживанием состояния. Флаг O не используется. Для того чтобы изменить значение флага M с 0 на 1 для объявления DHCPv6 с отслеживанием состояния (рисунок 5.4), применяется команда `ipv6 nd managed-config-flag`.

В случае если в сообщении RA указан вариант работы DHCPv6 (с отслеживанием состояния или без), инициируется работа DHCPv6. Сообщения протокола DHCPv6 посылаются через протокол UDP. Сообщения DHCPv6 от сервера к клиенту используют UDP порт назначения 546. Клиент отправляет сообщения на сервер DHCPv6 через UDP порт назначения 547. Клиенту необходимо определить местоположение сервера DHCPv6, для этого он передает сообщение DHCPv6 **SOLICIT** на зарезервированный IPv6-адрес многоадресной рассылки FF02::1:2, используемый всеми DHCPv6 серверами. Данный адрес многоадресной рассылки действует в рамках канала link-local – это означает, что маршрутизаторы не направляют сообщения в другие сети.

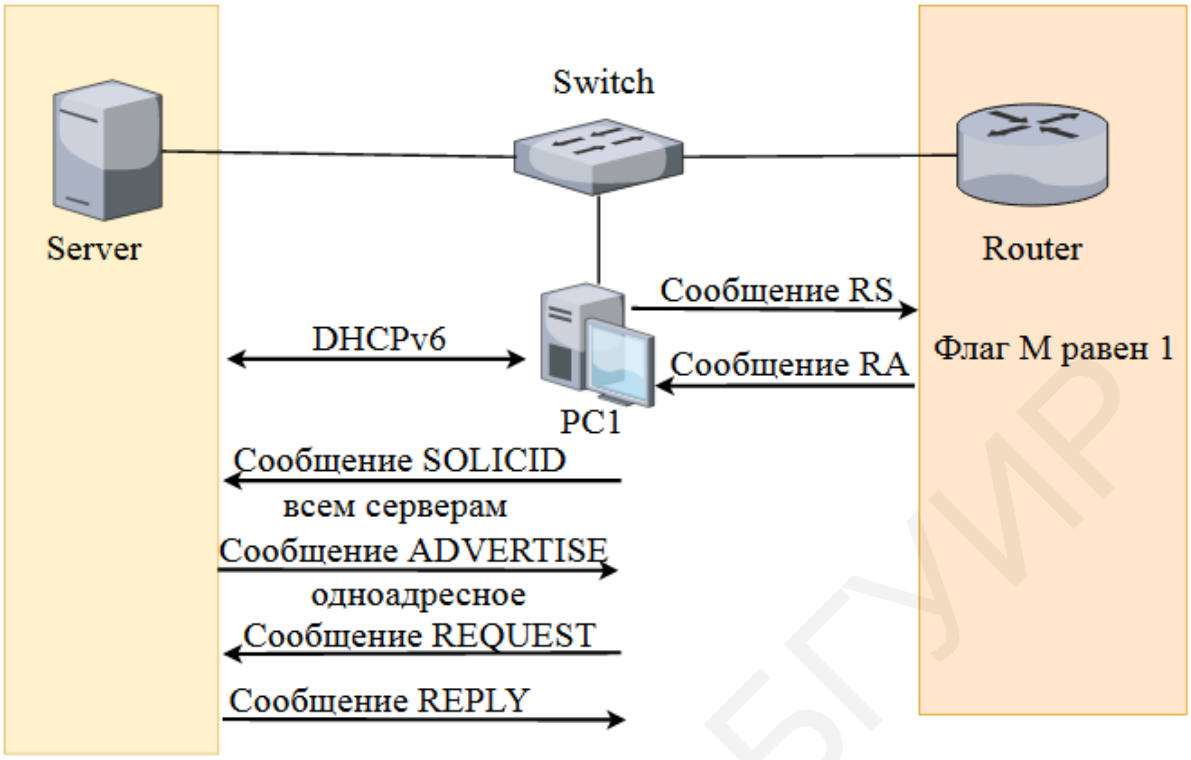


Рисунок 5.4 – Принцип работы DHCPv6 с отслеживанием состояния

Один или несколько серверов DHCPv6 отвечают DHCPv6-сообщением **ADVERTISE**. Сообщение **ADVERTISE** сообщает DHCPv6-клиенту, что сервер доступен для предоставления службы DHCPv6.

Клиент отвечает серверу DHCPv6 сообщением **REQUEST** или **INFORMATION-REQUEST**, в зависимости от того, является ли DHCPv6-сервер сервером с отслеживанием состояния или без него.

В случае DHCPv6 без отслеживания состояния клиент отправляет DHCPv6 сообщение **INFORMATION-REQUEST** серверу DHCPv6, запрашивая только параметры конфигурации, например, адрес DNS-сервера. Клиент создает собственный IPv6-адрес при помощи префикса из сообщения RA и самогенерируемого идентификатора интерфейса (см. рисунок 5.4).

В случае использования DHCPv6-клиента с отслеживанием состояния клиент отправляет DHCPv6 сообщение **REQUEST** серверу для получения от него IPv6-адреса и всех остальных параметров конфигурации.

Маршрутизатор может ретранслировать запрос к DHCP-серверу, если тот находится в другой сети. Для этого используются команда `ipv6 dhcp relay destination (address)` в настройках интерфейса, однако в некоторых версиях Cisco Packet Tracer данная команда недоступна.

Для настройки маршрутизатора в качестве DHCPv6 сервера без отслеживания состояния необходимо совершить следующие действия:

1. Активировать маршрутизацию IPv6 с помощью команды `ipv6 unicast-routing`.

2. Настроить DHCPv6-пул командой `ipv6 dhcp pool (pool-name)`.

3. Настроить параметры пула командами `dns-server (адрес dns-сервера), domain-name (имя domain)`.

4. Настроить интерфейс с помощью команд

```
Router(config-)# interface (type number)
Router(config-if)# ipv6 dhcp server (pool name)
Router(config-if)# ipv6 nd other-config-flag.
```

5. Настроить префикс с помощью команды `ipv6 general-prefix (pool name) ipv6-prefix/prefix-length`.

6. Настроить пул локальных адресов командой `ipv6 local pool (pool name) ipv6-prefix/prefix prefix-length`.

Для маршрутизатора Router1 (см. рисунок 5.1) IPv6-маршрутизация активируется при помощи команды `ipv6 unicast-routing`.

Далее настраивается три пула DHCP, т. к. он подключен к трем VLAN. Например, для VLAN 106 DHCP настраивается следующим образом:

```
Router1(config)#ipv6 dhcp pool VLAN106
Router1(config-dhcpv6)#dns-server 2001:DB8:ACAD:107::100
Router1(config-dhcpv6)#domain-name VLAN106
```

Аналогичным образом настраивается DHCP для других VLAN. Сеть VLAN 106 подключается к sub-интерфейсу маршрутизатора Gigabit-Ethernet 0/1.6, в настройках которого должен быть указан DHCP:

```
Router1(config)#interface GigabitEthernet 0/1.6
Router1(config-subif)#ipv6 address dhcp 2001:DB8:ACAD:107::100/64
Router1(config-subif)#ipv6 nd other-config-flag
Router1(config-subif)#ipv6 dhcp server VLAN106
```

Настройка префикса и пула локальных адресов VLAN 106 для маршрутизатора Router1 (см. рисунок 5.1) осуществляется следующим образом:

```
Router1(config)#ipv6 general-prefix VLAN106 2001:DB8:ACAD:106::/64
Router1(config)#ipv6 local pool VLAN106 2001:DB8:ACAD:106::/40 64
```

Для получения IPv6-адреса необходимо в настройках IP-адреса удалить IPv4-адрес, выбрав режим Static, в конфигурации IPv6-адреса сначала выбрать DHCP, а затем Auto Config. В результате устройство должно получить IPv6-адреса шлюза по умолчанию и DNS-сервера и сконфигурировать свой собственный IPV6-адрес (рисунок 5.5).

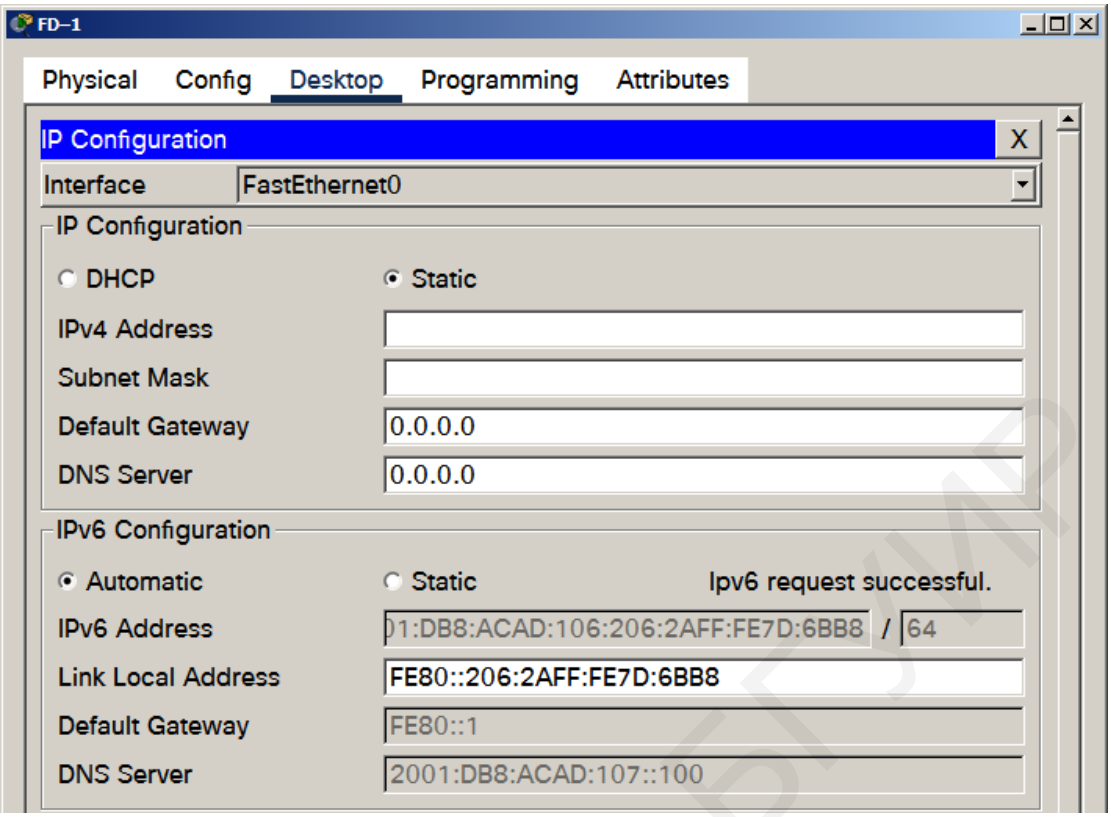


Рисунок 5.5 – Конфигурация IPv6-адреса на оконечном устройстве

Аналогичным образом осуществляется настройка IPv6-адреса на IoT-устройствах (рисунок 5.6). Для настройки доступа к серверу с IoT-устройства необходимо указать его адрес, а также имя и пароль пользователя. На DNS-сервере также необходимо удалить IPv4-адреса и назначить имена с IPv6-адресами (рисунок 5.7).

Статические маршруты для протокола IPv6 настраиваются с помощью команды глобальной конфигурации `ipv6 route`.

Следующий маршрутизатор для пересылки пакетов может быть определен с помощью IPv6-адреса, выходного интерфейса или обоих параметров сразу. В зависимости от того как указано место назначения, создается один из трех возможных типов маршрутов:

- статический маршрут IPv6 следующего перехода – указывается только IPv6-адрес следующего перехода (`ipv6-prefix/prefix-length`);

- напрямую подключенный статический маршрут IPv6 – указывается только выходной интерфейс маршрутизатора (`exit-intf`);

- полностью заданный статический маршрут IPv6 – указывается IPv6-адрес следующего перехода и выходной интерфейс (`ipv6-address | exit-intf`).

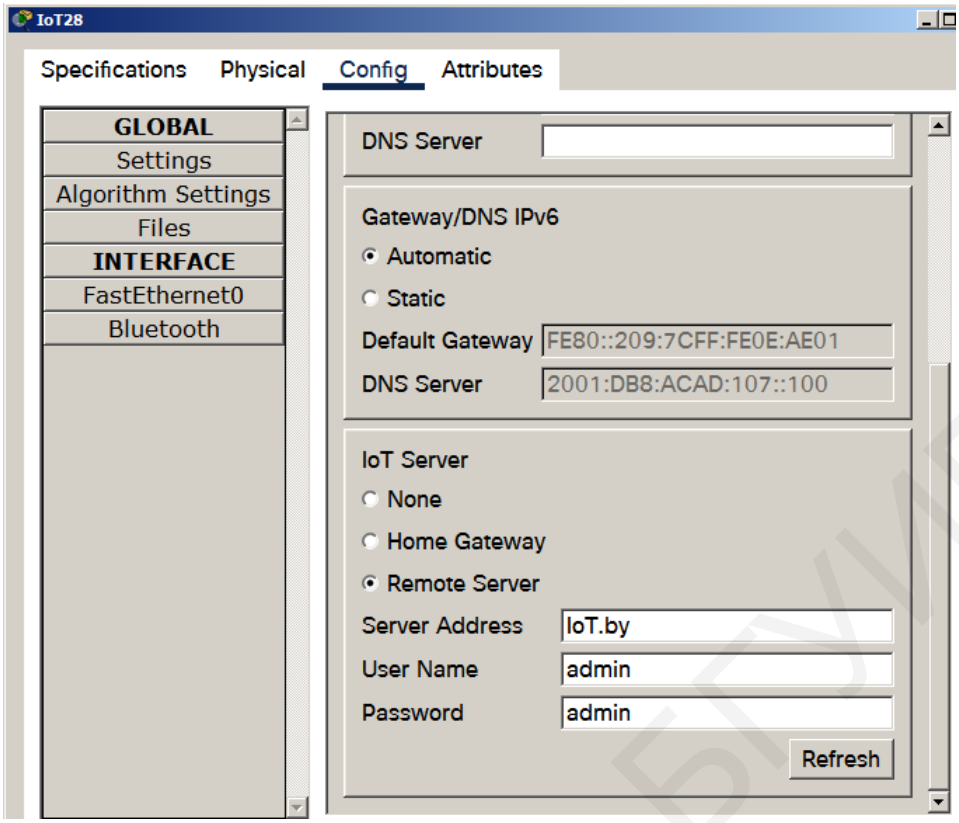


Рисунок 5.6 – Конфигурация IPv6-адреса на IoT-устройстве

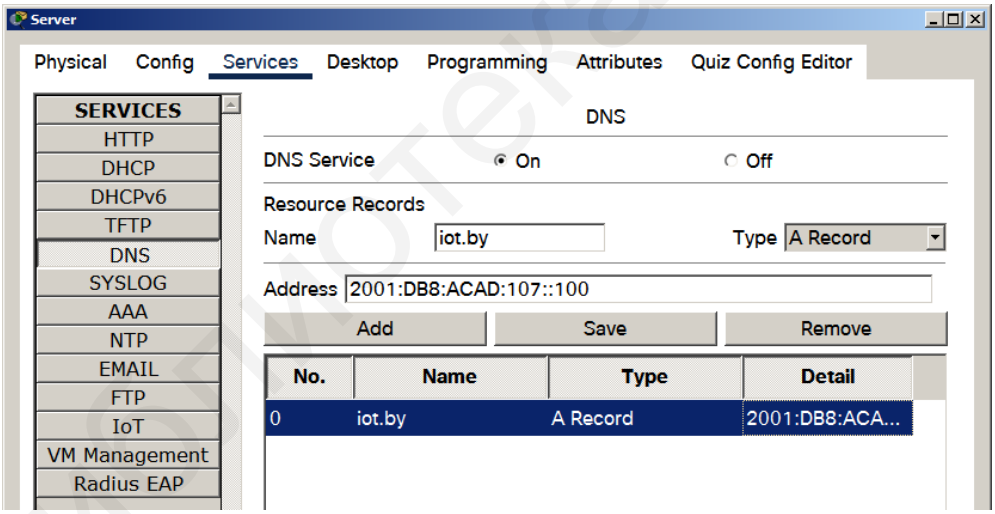


Рисунок 5.7 – Конфигурация DNS

Для маршрутизатора Router1 (см. рисунок 5.1) статический маршрут в сети IOT1, IOT2 и сеть между маршрутизатором Router2 и Router3 настраиваются следующим образом:

```
    Router1(config)# ipv6 route 2001:DB8:ACAD:300::/64
GigabitEthernet 0/1/0 FE80::2
    Router1(config)# ipv6 route 2001:DB8:ACAD:200::/64
GigabitEthernet 0/0/0 FE80::3
```

```
Router1(config)# ipv6 route 2001:DB8:ACAD:2::/64
GigabitEthernet 0/0/0 FE80::4
```

Команду `show ipv6 route` можно использовать для проверки того, что сети, использующие IPv6, и конкретные IPv6-адреса интерфейса были внесены в таблицу маршрутизации IPv6. Команда `show ipv6 route` отображает только сети, использующие IPv6, но не отображает сети, использующие IPv4. Команда `ping` для IPv6 идентична команде, используемой для IPv4, за исключением того, что в ней используется IPv6-адрес.

5.2 Лабораторное задание

Лабораторная работа выполняется на основе настроек, произведенных в задании 1 лабораторной работы № 2. До начала выполнения необходимо открыть сохраненный файл с именем **Lab2.pkt**, полученный в лабораторной работе № 2, и проверить настройки IP-адресации маршрутизаторов: маршрутизация не должна быть настроена. В смоделированной сети необходимо удалить сеть с беспроводным маршрутизатором. Все маршрутизаторы необходимо соединить друг с другом (см. рисунок 5.1). По результатам выполнения данной лабораторной работы все устройства любой из подсети должны иметь доступ к серверу, на котором должны отображаться статусы всех IoT-устройств и условия их работы. Доступ к серверу должен осуществляться посредством DNS.

В данной лабораторной работе необходимо настроить статическую маршрутизацию по протоколу IPv6, исходя из следующих заданий.

1. Настроить IPv6-адресацию. Взять IPv6-адрес в соответствии с третьей цифрой шифра из таблицы 5.2 и разбить его на подсети для смоделированной сети. Адрес каждой новой подсети увеличивать на единицу. Подписать IPv6-адреса каждой подсети, как показано на рисунке 5.1. Изображение смоделированной сети представить в отчете. Осуществить настройку всех интерфейсов маршрутизаторов.

Таблица 5.2 – IPv6-адреса для смоделированной сети

Третья цифра шифра	IPv6-адрес
0	2001:E50:5486::/48
1	2001:DD0:DD45::/48
2	2001:5:A519::/48
3	2001:50:F179::/48
4	2001:400:DD5E::/48
5	2001:5600:E8::/48
6	2001:900:9561::/48
7	2001:E200:AD00::/48
8	2001:AC00:109F::/48
9	2001:8000:78::/48

2. Настроить DHCPv6-сервер на каждом маршрутизаторе. Для всех устройств IPv6-адрес должен быть получен автоматически. Заполнить таблицу 5.3. В отчете представить результаты выполнения команды `show ipv6 dhcp pool`.

Таблица 5.3 – IPv6-адресация смоделированной сети

Имя устройства или сети	Имя интерфейса	Глобальный адрес	Локальный адрес

3. Настроить DNS. Удалить DNS по протоколу IPv4, добавить IPv6-адрес сервера в таблицу DNS. Результат настройки DNS-сервера представить в отчете. Настроить DNS на всех устройствах. Сохранить файл под именем **Lab5-1.pkt**.

4. Настроить статическую маршрутизацию IPv6 на всех маршрутизаторах. Построенные маршруты должны проходить максимум через два маршрутизатора. На всех устройствах удалить IPv4-адресацию. В результате настройки все устройства должны быть доступны устройствам из других сетей по протоколу IPv6. На сервере должны отображаться статусы всех устройств IoT. В отчете представить результат выполнения команды `show ipv6 route` на одном маршрутизаторе и отображение на сервере всех устройств IoT. Сохранить файл под именем **Lab5-2.pkt**.

5.3 Содержание отчета

1. Цель работы, исходные данные в соответствии с вариантом из таблицы 5.2.
2. Результаты произведенных настроек (см. задания 2–4 подраздела 5.2), заполненная таблица 5.3, изображение смоделированной сети.
3. Вывод по работе.
4. Ответы на контрольные вопросы.

5.4 Контрольные вопросы и задания

1. Произвести сравнение IPv6- и IPv4-протоколов.
2. Описать последовательность действий при настройке интерфейса по протоколу IPv6.
3. Какие существуют способы настройки автоматического получения IPv6-адреса оконечными устройствами?
4. В чем заключается назначение и принцип работы SLAAC?
5. Пояснить назначение ICMPv6-сообщений маршрутизатора.
6. Привести пример конфигурации SLACC с DHCPv6 без отслеживания состояния канала и объяснить принцип его работы.
7. Привести пример конфигурации DHCPv6 с отслеживанием состояния канала и объяснить принцип его работы
8. Перечислить типы статических маршрутов IPv6.

ЛАБОРАТОРНАЯ РАБОТА № 6
ПРОТОКОЛЫ МАРШРУТИЗАЦИИ RIPng и EIGRP

Цель: изучить принцип работы протоколов RIP и EIGRP и выделить отличительные черты данных протоколов для IPv4- и IPv6-сетей; овладеть навыками настройки протоколов RIPng и EIGRP на маршрутизаторах.

6.1. Теоретическая часть

RIPng (протокол RIP нового поколения) – это протокол маршрутизации на базе векторов расстояния для маршрутизации IPv6-адресов. RIPng основан на RIPv2 [7, 13]. В отличие от RIPv2 протокол RIPng активируется через интерфейс, а не в режиме конфигурации маршрутизатора, т. е. в протоколе RIPng недоступна команда `network сетевой_адрес`. Вместо нее используется команда `ipv6 router rip имя_домена`, затем на каждом интерфейсе используется команда `ipv6 rip имя_домена enable`. Для маршрутизатора Router1 на рисунке 6.1 протокол RIPng с доменным именем LAN1 активируется следующим образом:

```
Router1(config)#ipv6 router rip LAN1
Router1(config)#interface g0/0
Router1(config-if)#ipv6 rip LAN1 enable
```

Аналогично активируется протокол RIPng на всех остальных интерфейсах маршрутизатора.

Процедура передачи маршрута по умолчанию по сети в протоколе RIPng идентична аналогичной процедуре в протоколе RIPv2. Предположим, что у маршрутизатор Router5 соединен через интерфейс GigabitEthernet 0/0/0 с внешней интернет-сетью с адресом 2001:DB8:ACAD:AAAA::/64. Чтобы передать маршрут по умолчанию, маршрутизатор Router1 необходимо настроить следующим образом:

- с использованием статического маршрута по умолчанию с помощью команды глобальной конфигурации `ipv6 route ::/0 2001:DB8:ACAD:AAAA::1/64;`
- с использованием команды режима конфигурации интерфейса `ipv6 rip имя_домена default-information originate`.

Таким образом, маршрутизатору Router5 дается указание работать в режиме источника данных о маршруте по умолчанию и транслировать статический маршрут по умолчанию в обновлениях RIPng, отправляемых из настроенного интерфейса.

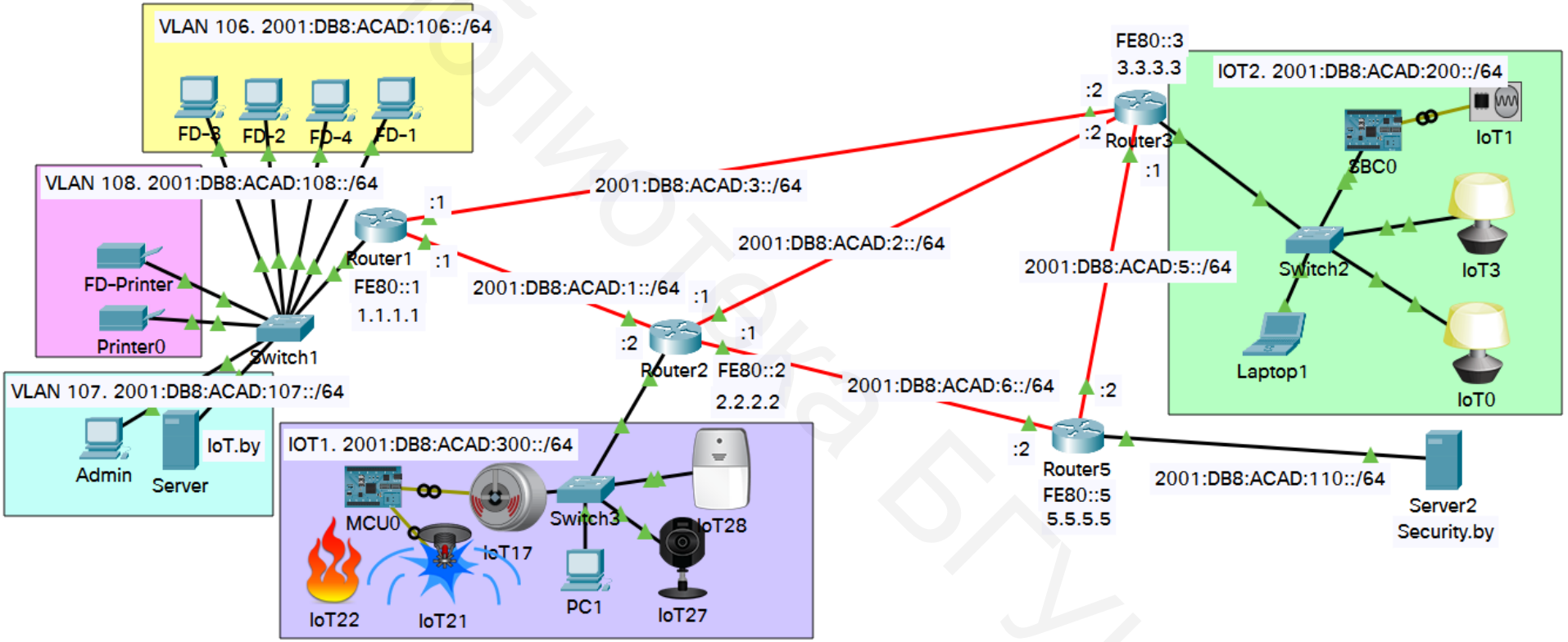


Рисунок 6.1 – Сеть с маршрутизацией по протоколу RIPng

Команда `show ipv6 protocols` позволяет просматривать информацию о том, что:

- маршрутизация RIPng настроена и запущена;
- интерфейсы настроены с использованием RIPng [7].

Команда `show ipv6 route` отображает маршруты, указанные в таблице маршрутизации.

Протокол EIGRP для IPv6 обменивается данными о маршрутах, чтобы заполнить таблицу маршрутизации IPv6 префиксами удаленных сетей. Протокол EIGRP для IPv4 выполняется на сетевом уровне IPv4, взаимодействуя с другими IPv4-узлами EIGRP и объявляя только маршруты IPv4. EIGRP для IPv6 выполняет те же функции, что и EIGRP для IPv4, но в качестве транспорта сетевого уровня использует IPv6, взаимодействуя с другими IPv6-узлами EIGRP и объявляя маршруты IPv6. EIGRP для IPv6 также использует алгоритм DUAL как механизм вычислений, гарантирующий построение путей без петель и резервных путей для всего домена маршрутизации.

Как и все протоколы маршрутизации IPv6 протокол EIGRP для IPv6 использует процессы, независимые от его аналога для IPv4. Процессы и операции являются точно такими же, как и для протокола маршрутизации IPv4, но они выполняются независимо. Каждый из протоколов, EIGRP для IPv4 и EIGRP для IPv6, использует отдельные таблицы соседних устройств EIGRP, таблицы топологии IP EIGRP и таблицы IP-маршрутизации.

Команды настройки и проверки EIGRP для IPv6 очень похожи на команды, используемые в EIGRP для IPv4.

Основные особенности протокола EIGRP для IPv4 и IPv6 заключаются в следующем:

- EIGRP для IPv4 объявляет сети IPv4, а EIGRP для IPv6 объявляет префиксы IPv6;
- протокол EIGRP для IPv4 и для IPv6, являясь протоколом маршрутизации на основе векторов расстояния, использует одни и те же административные дистанции;
- протокол EIGRP для IPv4 и для IPv6 использует одни и те же методы и процессы DUAL;
- протокол EIGRP для IPv4 и для IPv6 использует в своей составной метрике пропускную способность, задержку, надежность и загрузку;
- протокол EIGRP для IPv4 и для IPv6 использует надежный транспортный протокол (Reliable Transport Protocol, RTP), который отвечает за гарантированную доставку пакетов EIGRP всем соседним устройствам;
- протокол EIGRP для IPv4 и для IPv6 отправляет инкрементные обновления в случае изменения состояния места назначения;

- протокол EIGRP для IPv4 и для IPv6 использует простой механизм приветствий для получения сведений о соседних маршрутизаторах и создания отношений смежности;

- протокол EIGRP для IPv4 отправляет сообщения на адрес групповой рассылки 224.0.0.10, в качестве адреса источника в этих сообщениях используется IPv4-адрес исходящего интерфейса. EIGRP для IPv6 передает свои сообщения на адрес групповой рассылки FF02::A. В качестве источника сообщений EIGRP для IPv6 используется локальный IPv6-адрес канала выходного интерфейса;

- протокол EIGRP для IPv4 может использовать либо аутентификацию без шифрования, либо аутентификацию MD5. В EIGRP для IPv6 используется MD5;

- протокол EIGRP для IPv4 и для IPv6 использует 32-битное число для идентификатора маршрутизатора. Идентификатор маршрутизатора представлен в десятичном формате с разделительными точками и обычно называется IPv4-адресом. Если у маршрутизатора EIGRP для IPv6 не настроен IPv4-адрес, для настройки 32-битного идентификатора маршрутизатора необходимо использовать команду `eigrp router-id`. Процесс определения идентификатора маршрутизатора одинаков для обоих протоколов EIGRP, для IPv4 и для IPv6.

Маршрутизаторы, на которых работает такой протокол динамической маршрутизации, как EIGRP, обмениваются сообщениями с соседними устройствами, находящимися в той же подсети или подключенными к этому же каналу. Маршрутизаторам нужно обмениваться сообщениями протокола маршрутизации только со своими непосредственно подключенными соседями. Эти сообщения всегда отправляются с IP-адреса маршрутизатора-источника, выполняющего пересылку.

Локальный IPv6-адрес канала позволяет устройству обмениваться данными с другими устройствами, использующими IPv6, по одному и тому же каналу и только по этому каналу (подсети). Пакеты с link-local адресом источника или назначения не могут быть направлены за пределы того канала, в котором создан пакет.

Сообщения EIGRP для IPv6 отправляются с использованием следующих параметров:

- IPv6-адреса источника – локального IPv6-адреса канала выходного интерфейса;

- IPv6-адреса назначения – адреса групповой рассылки, IPv6-адреса FF02::A, который является адресом всех маршрутизаторов EIGRP в области действия локального канала. Если пакет может быть отправлен как пакет с индивидуальным адресом, он отправляется на локальный адрес канала соседнего маршрутизатора.

На рисунке 6.1 мы видим, что для каждого маршрутизатора настроены локальные и глобальные индивидуальные адреса IPv6. Как и для всех остальных протоколов маршрутизации, перед настройкой протокола EIGRP необхо-

дима команда режима глобальной конфигурации `ipv6 unicast-routing`, которая включает маршрутизацию IPv6.

Чтобы перейти в режим конфигурации EIGRP для IPv6, используется команда режима глобальной конфигурации `ipv6 router eigrp autonomous-system` [7]. Аналогично EIGRP для IPv4, значение `autonomous-system` (автономная система) должно быть одинаковым на всех маршрутизаторах. Для настройки идентификатора маршрутизатора применяется команда `eigrp router-id`. EIGRP для IPv6 использует 32-битное значение для идентификатора маршрутизатора. С целью получения этого значения протокол EIGRP для IPv6 использует тот же процесс, что и EIGRP для IPv4. Команда `eigrp router-id` имеет приоритет над всеми IPv4-адресами интерфейсов loopback и физических интерфейсов. Если у маршрутизатора EIGRP для IPv6 нет активных интерфейсов с IPv4-адресом, применяется команда `eigrp router-id`.

Идентификатор маршрутизатора должен быть 32-битным значением, уникальным в IP-домене маршрутизации EIGRP. В противном случае возможны конфликты маршрутизации.

По умолчанию процесс EIGRP для IPv6 находится в отключенном состоянии. Чтобы включить его, требуется команда `no shutdown`. Даже после включения EIGRP для IPv6 обмен обновлениями маршрутизации с соседними устройствами невозможен, пока на соответствующих интерфейсах не будет включен протокол EIGRP.

Маршрутизатору для создания отношений смежности с соседними устройствами требуется как команда `no shutdown`, так и идентификатор маршрутизатора. Чтобы включить EIGRP для IPv6 на интерфейсе, используется команда режима конфигурации интерфейса `ipv6 eigrp autonomous-system`.

Для маршрутизатора Router1 с идентификатором 1.1.1.1 (см. рисунок 6.1) настройка автономной системы 2 протокола EIGRP осуществляется следующим образом:

```
Router1(config)#ipv6 router eigrp 2
Router1(config-rtr)#eigrp router-id 1.1.1.1
Router1(config-rtr)#no shutdown
```

Для настройки протокола EIGRP на интерфейсе GigabitEthernet 0/0/0 используются следующие команды:

```
Router1(config)#interface GigabitEthernet 0/0/0
Router1(config-if)#ipv6 eigrp 2
```

В результате настройки дожно отобразиться сообщение

```
%DUAL-5-NBRCHANGE: IPv6-EIGRP 2: Neighbor FE80::2
(GigabitEthernet 0/0/0) is up: new adjacency
```

Это сообщение показывает, что маршрутизатор Router1 создал отношение смежности EIGRP-IPv6 с соседним устройством по локальному адресу канала FE80::2, т. е. с маршрутизатором Router2 (FE80::1).

Для настройки пассивного интерфейса с EIGRP для IPv6 используется команда `passive-interface`.

6.2 Лабораторное задание

Лабораторная работа выполняется на основе настроек, произведенных в задании 3 лабораторной работы № 5. До начала выполнения необходимо открыть сохраненный файл с именем **Lab5-1.pkt**, полученный в лабораторной работе № 5, и проверить настройки IPv6-адресации на всех устройствах: маршрутизация не должна быть настроена. В существующую сеть добавить маршрутизатор и сервер Security.by, на котором будет осуществляться мониторинг и контроль за устройствами из сети IOT1. Соединение сетей осуществить, как показано на рисунке 6.1. Привязать устройства из сети IOT1 к добавленному серверу. Сохранить файл под именем **Lab6-1.pkt.** По результатам выполнения данной лабораторной работы все устройства любой из подсетей должны иметь доступ к серверам, на которых должны отображаться статусы всех IoT-устройств и условия их работы. Доступ к серверам должен осуществляться посредством DNS.

В данной лабораторной работе необходимо настроить маршрутизации по протоколам RIPng и EIGRP, исходя из следующих заданий.

1. Настроить протокол динамической маршрутизации RIPng. Включить IPv6-маршрутизацию командой `ipv6 unicast-routing`. Включить маршрутизацию по протоколу RIPng, используя команду `ipv6 rip имя_домена enable`. Имя домена использовать в соответствии с исходными данными из таблицы 6.1.

Таблица 6.1 – Исходные данные для настройки маршрутизации по протоколу RIPng и EIGRP

Первая цифра шифра	Имя домена	Номер автономной системы	Router-id
0	LAN	120	10.10.10.10
1	NETWORK	14	20.20.20.20
2	RIPLAN	25	30.30.30.30
3	RIPng	63	40.40.40.40
4	CISCO	5	15.15.15.15
5	CISCORIP	90	25.25.25.25
6	ROUTE	30	35.35.35.35
7	TEST	25	45.45.45.45
8	RIPROUTE	2	13.13.13.13
9	RIP	45	18.18.18.18

2. Проверить результат настройки маршрутизации по протоколу RIPng и представить в отчете результаты выполнения команд `show ipv6 protocols` и `show ipv6 route` для любых двух маршрутизаторов. Сохранить текущую конфигурацию всех маршрутизаторов. Сохранить файл под именем **Lab6-2.pkt.**

3. Настроить протокол динамической маршрутизации EIGRP. Открыть файл **Lab6-1.pkt**. Проверить настройки IPv6-адресации на всех устройствах: маршрутизация не должна быть настроена. С помощью команды `ipv6 router eigrp номер_автономной_системы` осуществить настройку маршрутизации. Номер автономной системы установить в соответствии с исходными данными из таблицы 6.1. В соответствии с исходными данными из таблицы 6.1 настроить идентификаторы маршрутизаторов. Для каждого последующего маршрутизатора значение каждого октета увеличивать на 1. Настроить пассивные интерфейсы на каждом маршрутизаторе.

4. Проверить результат настройки маршрутизации по протоколу EIGRP и представить в отчете результаты выполнения команд `show ipv6 protocols`, `show ipv6 eigrp neighbors` и `show ipv6 route` для любых двух маршрутизаторов. Сохранить текущую конфигурацию всех маршрутизаторов. Сохранить файл под именем **Lab6-3.pkt.**

6.3 Содержание отчета

1. Цель работы, исходные данные в соответствии с вариантом из таблицы 6.1.
2. Результаты произведенных настроек (см. задания 2, 4 подраздела 6.2), изображение смоделированной сети.
3. Вывод по работе.
4. Ответы на контрольные вопросы.

6.4 Контрольные вопросы и задания

1. Произвести сравнение протокола RIP и RIPng. Представить пример конфигурации протокола RIPng.
2. Описать процесс передачи маршрута по умолчанию в сети, в которой настроена маршрутизация по протоклу RIPng.
3. Произвести сравнение протокола EIGRP для IPv4- и IPv6-сетей.
4. В чем заключается механизм обмена данными между маршрутизаторами по протоколу EIGRP?
5. Привести пример конфигурации протокола EIGRP на маршрутизаторе.

ЛАБОРАТОРНАЯ РАБОТА № 7
ПРОТОКОЛ IPV6-МАРШРУТИЗАЦИИ OSPFv3

Цель: изучить и проанализировать механизм работы протокола OSPFv3, сравнить с работой протокола OSPFv2; овладеть навыками настройки протокола OSPFv3.

7.1 Теоретическая часть

Протокол OSPFv3, так же как и OSPFv2, используется для обмена префиксами IPv6. Протокол OSPFv3 осуществляет обмен данными маршрутизации для заполнения таблицы маршрутизации IPv6 удаленными префиксами, как и при использовании OSPFv2 для IPv4. Благодаря функции семейств адресов протокол OSPFv3 обеспечивает поддержку как IPv4, так и IPv6.

Протокол OSPFv2 работает в сетях IPv4, осуществляет обмен данными с другими равноправными узлами OSPF IPv4 и объявляет только IPv4-маршруты.

Протокол OSPFv3 предоставляет те же возможности, что и протокол OSPFv2, но при этом использует IPv6 как транспорт на уровне сети, осуществляет обмен данными с равноправными узлами OSPFv3 и объявляет маршруты IPv6. Протокол OSPFv3 также использует алгоритм поиска кратчайшего пути SPF как инструмент определения оптимальных маршрутов посредством домена маршрутизации.

Как и все остальные протоколы маршрутизации IPv6, протокол OSPFv3 работает независимо от протоколов IPv4. По сути процессы и операции являются теми же, что и в протоколе маршрутизации IPv4, однако выполняются независимо. Протоколы OSPFv2 и OSPFv3 содержат отдельные таблицы смежности, таблицы топологии OSPF и таблицы IP-маршрутизации.

Настройка протокола OSPFv3 и команды проверки аналогичны используемым в протоколе OSPFv2.

Можно выделить следующие сходства между протоколами OSPFv2 и OSPFv3 [4]:

- состояние канала – протоколы OSPFv2 и OSPFv3 являются бесклассовыми протоколами маршрутизации по состоянию канала;
- алгоритм маршрутизации – протоколы OSPFv2 и OSPFv3 используют алгоритм поиска кратчайшего пути SPF для принятия решений по маршрутизации;
- метрика – в запросах для комментариев протоколов OSPFv2 и OSPFv3 метрики определены как стоимость отправки пакетов из интерфейса;
- области – в OSPFv3 используется такая же концепция разделения на несколько областей, как и в OSPFv2. Разделение на несколько областей позволяет минимизировать лавинную рассылку данных о состоянии канала и обеспечивает более высокий уровень стабильности в пределах домена OSPF;

- типы пакетов OSPF – как и OSPFv2, OSPFv3 использует также пять основных типов пакетов (Hello, DBD, LSR, LSU и LSAck);

- механизм обнаружения соседних устройств – система определения состояния соседних устройств включает список состояний и событий соседних устройств OSPF;

- процесс выбора маршрутизаторов DR/BDR – процесс выбора маршрутизаторов DR/BDR в OSPFv3 аналогичен процессу в OSPFv2;

- идентификатор маршрутизатора – протоколы OSPFv2 и OSPFv3 используют в качестве идентификатора маршрутизатора 32-битное значение, представленное в десятичном формате с разделением точкой.

Как правило, идентификатором маршрутизатора является IPv4-адрес. Для настройки идентификатора применяется команда OSPF `router-id`. При определении 32-битного идентификатора маршрутизатора в обоих протоколах используется один и тот же процесс. Предпочителен напрямую настроенный идентификатор маршрутизатора. В случае невозможности его использования идентификатором маршрутизатора назначается IPv4-адрес интерфейса loopback, имеющий самое высокое значение.

Изменения в протоколы OSPFv2 и OSPFv3 можно внести с помощью команды режима конфигурации маршрутизатора `auto-cost reference-bandwidth ref-bw`. Эта команда влияет только на ту метрику OSPF, в которой была настроена. Например, если данная команда выполнена для протокола OSPFv3, она не влияет на метрики маршрутизации OSPFv2.

Протоколы OSPFv2 и OSPFv3 используют механизм приветствия для получения данных о соседних маршрутизаторах и установления отношений смежности. Однако протокол OSPFv3 для установления отношений смежности с соседними маршрутизаторами не требует сопоставления подсетей: отношения смежности с соседними устройствами устанавливаются посредством адресов типа link-local, а не при помощи глобальных индивидуальных адресов.

Основными различиями протоколов OSPFv2 и OSPFv3 являются [4]:

- объявления – OSPFv2 объявляет маршруты IPv4, а OSPFv3 – маршруты для IPv6;

- исходный адрес – сообщения OSPFv2 поступают с IPv4-адреса выходного интерфейса, а сообщения OSPF в OSPFv3 поступают с адреса типа link-local выходного интерфейса;

- групповые адреса маршрутизатора OSPF – OSPFv2 использует адрес 224.0.0.5; а OSPFv3 – FF02::5;

- групповые адреса маршрутизатора DR/BDR – OSPFv2 использует адрес 224.0.0.6, а OSPFv3 – FF02::6;

- объявление сетей – OSPFv2 объявляет сети, используя команду конфигурации маршрутизатора `network`, а OSPFv3 – команду конфигурации интерфейса `ipv6 ospf process-id area area-id`;

- IP-маршрутизация – по умолчанию включена в IPv4, а в IPv6 должна быть настроена командой глобальной конфигурации `ipv6 unicast-routing`;

- аутентификация – OSPFv2 использует аутентификацию без шифрования или MD5, OSPFv3 использует аутентификацию IPsec.

На рисунке 7.1 представлена сеть, в которой на каждом маршрутизаторе настроен протокол маршрутизации OSPFv3. В качестве примера рассмотрим настройку на маршрутизаторе Router1.

Маршрутизация настраивается с помощью команды `ipv6 unicast-routing`. Далее, после настройки IPv6-адресации на необходимых интерфейсах используется команда режима глобальной конфигурации `ipv6 router ospf process-id` для перехода в режим конфигурации протокола OSPFv3. Как и в OSPFv2, значение `process-id` представляет собой число в диапазоне от 1 до 65535, которое задается администратором. В целях обеспечения согласованности все маршрутизаторы используют идентификатор процесса. Протоколу OSPFv3 требуется назначить 32-битный идентификатор маршрутизатора при помощи команд

```
Router1(config)#ipv6 unicast-routing
Router1(config)#ipv6 router ospf 7
Router1(config-rtr)#router-id 1.1.1.1
```

Протокол OSPFv3, как и OSPFv2, может использовать следующие типы адресов:

- напрямую заданный идентификатор маршрутизатора;

- настроенный IPv4-адрес логического интерфейса loopback, имеющий самое высокое значение;

- настроенный IPv4-адрес активного интерфейса, имеющий самое высокое значение [4].

При отсутствии источников IPv4-адреса маршрутизатор отображает сообщение консоли для настройки идентификатора маршрутизатора вручную.

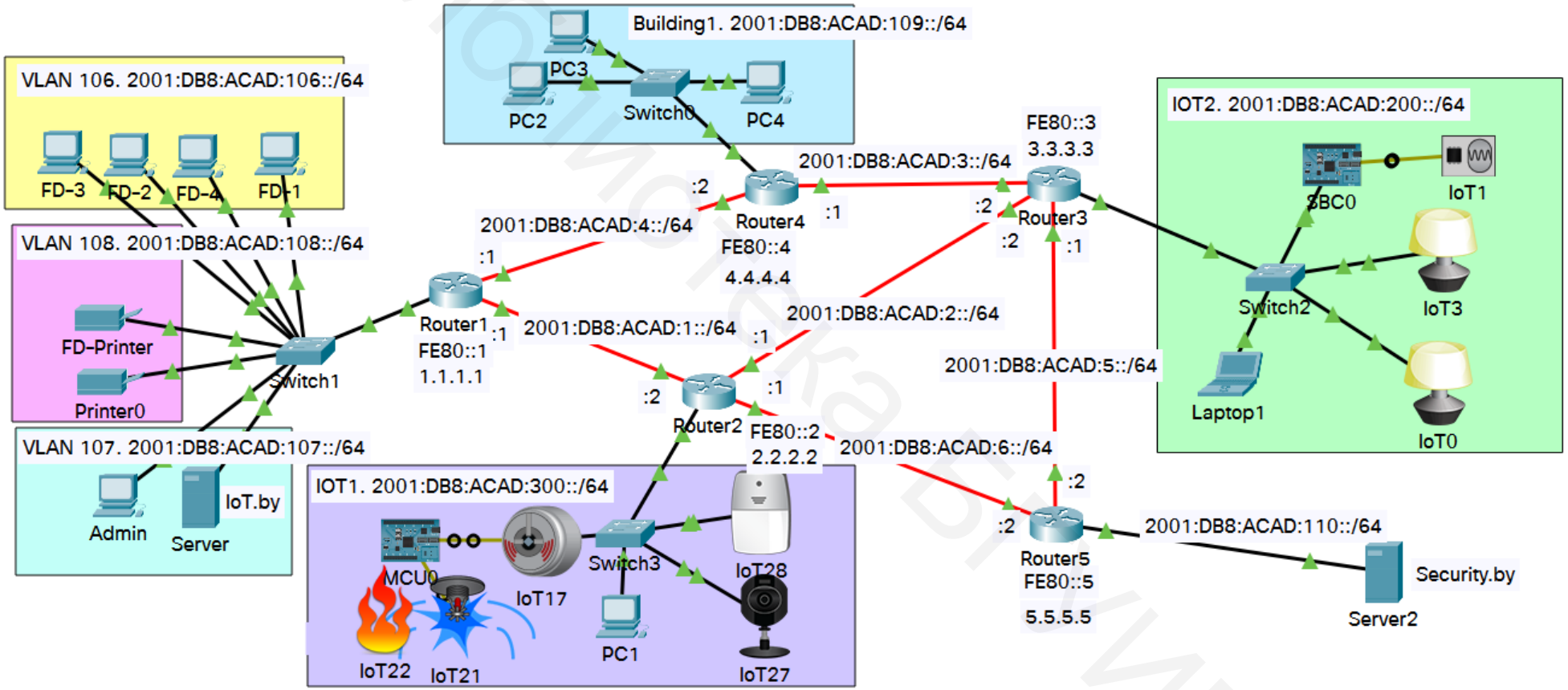


Рисунок 7.1 – Сеть с маршрутизацией по протоколу OSPFv3

Протоколы маршрутизации IPv6 включаются на интерфейсе, а не из режима конфигурации маршрутизатора, как в IPv4. Для включения OSPFv3 используется команда режима конфигурации интерфейса `ipv6 ospf process-id area area-id`. Значение `process-id` определяет заданный процесс маршрутизации и должно совпадать с идентификатором процесса, используемым для создания процесса маршрутизации в команде `ipv6 router ospf process-id`. Значение `area-id` представляет собой область, связанную с интерфейсом OSPFv3. Для интерфейса GigabitEthernet 0/1/0 маршрутизатора Router1 (см. рисунок 7.1) настройка OSPFv3 осуществляется следующим образом:

```
Router1(config)#interface GigabitEthernet 0/1/0
Router1(config-if)#ipv6 ospf 7 area 1
```

Значение `area-id` может быть любым. В качестве примера выбрано значение 1, поскольку область 1 не является магистральной областью. Аналогичным образом осуществляется настройка на всех остальных маршрутизаторах и их интерфейсах.

Маршрутизаторы, использующие протокол динамической маршрутизации (например, OSPF), осуществляют обмен сообщениями между соседними устройствами в пределах одной сети или канала. Им требуется только отправлять или принимать сообщения протокола маршрутизации от напрямую подключенных соседних устройств. В IPv4-сетях эти сообщения отправляются с IPv4-адреса источника, т. е. маршрутизатора, осуществляющего пересылку.

В сетях с IPv6 для этой цели идеально подходят IPv6-адреса типа link-local. Локальный IPv6-адрес канала позволяет устройству обмениваться данными с другими устройствами, использующими IPv6, по одному и тому же каналу (подсети). Пакеты с link-local адресом источника или назначения не могут быть направлены за пределы того канала, в котором создан пакет.

Сообщения OSPFv3 отправляются с использованием:

- IPv6-адреса источника – IPv6-адрес типа link-local выходного интерфейса;
- IPv6-адреса назначения – пакеты OSPFv3 могут отправляться на индивидуальный адрес с использованием IPv6-адреса типа link-local соседнего устройства;
- многоадресной рассылки – адрес FF02::5 является адресом маршрутизатора OSPF, а адрес FF02::6 – групповым адресом маршрутизатора DR/BDR.

Команда `passive-interface` в OSPFv3, как и в OSPFv2, запрещает отправку обновлений маршрутизации из определенного интерфейса маршрутизатора. Для маршрутизатора Router1 (см. рисунок 7.1) sub-интерфейсы настроены как пассивные следующим образом:

```
Router1(config)#ipv6 router ospf 7
Router1(config-rtr)#passive-interface GigabitEthernet 0/1.6
Router1(config-rtr)#passive-interface GigabitEthernet 0/1.7
Router1(config-rtr)#passive-interface GigabitEthernet 0/1.8
```

Как и в OSPFv2, в OSPFv3 возможно изменение значения заданной пропускной способности с помощью команды `auto-cost reference-bandwidth`, после выполнения которой появляется информационное сообщение консоли о том, что данную команду необходимо применить ко всем маршрутизаторам. Изменение метрик в таблице маршрутизации в результате изменения заданной пропускной способности происходит после удаления процесса маршрутизации OPSF с помощью команды привилегированного режима `clear ipv6 ospf process`. При этом протокол OSPFv3 на маршрутизаторе принудительно выполняет повторное установление отношений смежности с соседними устройствами.

Команда `show ipv6 protocols` позволяет быстро проверить критически важные данные конфигурации OSPFv3, включая идентификатор процесса OSPF, идентификатор маршрутизатора и интерфейсы, включенные для OSPFv3.

Команда `show ipv6 route ospf` предоставляет подробные данные о маршрутах OSPF в таблице маршрутизации.

Команда `show ipv6 ospf neighbor` используется для проверки установления маршрутизатором отношений смежности с соседними маршрутизаторами. Если идентификатор соседнего маршрутизатора не отображается или не показывает состояние FULL, это значит, что маршрутизаторы не установили отношения смежности OSPF.

Если два маршрутизатора не установили отношения смежности, обмен данными о состоянии канала не осуществляется. Неполное заполнение баз данных состояний каналов может привести к появлению ошибочных деревьев кратчайших путей SPF и таблиц маршрутизации. В этом случае маршруты к сетям назначения могут отсутствовать или не являться оптимальными путями.

Для каждого соседнего устройства команда `show ipv6 ospf neighbor` отображает следующие выходные данные (рисунок 7.2):

- Neighbor ID – идентификатор соседнего маршрутизатора;
- Pri, приоритет OSPF интерфейса – значение, используемое при выборе маршрутизаторов DR и BDR;
- State – состояние OSPF интерфейса;
- Dead Time – интервал времени, в течение которого маршрутизатор ожидает получения пакета приветствия от соседнего устройства прежде, чем объявит его недействующим. Данное значение сбрасывается при получении интерфейсом пакета приветствия;

- Interface ID – идентификатор интерфейса или идентификатор канала;

- Interface – интерфейс, на котором этот маршрутизатор установил отношения смежности с соседним устройством [4].

```
Router#show ipv6 ospf neighbor

Neighbor ID     Pri   State           Dead Time   Interface ID    Interface
4.4.4.4           1   FULL/DR         00:00:37    5               GigabitEthernet0/1/0
2.2.2.2           1   FULL/BDR        00:00:37    5               GigabitEthernet0/3/0
5.5.5.5           1   FULL/DR         00:00:37    4               GigabitEthernet0/2/0
```

Рисунок 7.2 – Пример таблицы смежности маршрутизатора

Состояние (State) FULL означает, что маршрутизатор и его соседнее устройство имеют идентичные базы данных состояний каналов OSPF. В сетях с множественным доступом состояние двух маршрутизаторов, состоящих в отношениях смежности, может отображаться как INIT, 2WAY, EXSTART и др. (см. таблицу 4.3).

7.2 Лабораторное задание

Лабораторная работа выполняется на основе настроек, произведенных в задании 3 лабораторной работы № 6. До начала выполнения необходимо открыть сохраненный файл с именем **Lab6-1.pkt**, полученный в лабораторной работе № 6, и проверить настройки IPv6-адресации на всех устройствах: маршрутизация не должна быть настроена. В существующую сеть добавить маршрутизатор и подключить к нему подсеть Building1, содержащую три компьютера. Соединение сетей осуществить в соответствии с рисунком 7.1. По результатам выполнения данной лабораторной работы все устройства любой из подсетей должны получать доступ к серверам, на которых должны отображаться статусы всех IoT-устройств и условия их работы. Доступ к серверам должен осуществляться посредством DNS.

В данной лабораторной работе необходимо настроить маршрутизацию по протоколу OSPFv3, исходя из следующих заданий.

1. Настроить бесклассовую IPv6-адресацию. На основе данных из таблицы 5.2 и разделения заданного IPv6-адреса выбрать IPv6-адреса для добавленной сети Building1, содержащей три компьютера и маршрутизатора. Дополнить таблицу 5.3 лабораторной работы № 5 и представить ее в отчете. Осуществить настройку всех устройств в сети. Сохранить файл под именем **Lab7.pkt.**

2. Настроить протокол OSPFv3 на всех маршрутизаторах с указанием process-id в соответствии с исходными данными из таблицы 7.1.

Таблица 7.1 – Исходные данные для настройки маршрутизации по состоянию канала

Первая цифра шифра	Значение process-id	Router-id	Пропускная способность по умолчанию, Мбит/с
0	10	10.10.10.10	3000
1	20	20.20.20.20	30000
2	30	30.30.30.30	5000
3	40	40.40.40.40	50000
4	50	15.15.15.15	8000
5	60	25.25.25.25	80000
6	70	35.35.35.35	100000
7	80	45.45.45.45	2000000
8	90	13.13.13.13	9000000
9	12	18.18.18.18	900000

3. Настроить идентификаторы маршрутизаторов в соответствии с исходными данными из таблицы 7.1. Для каждого последующего маршрутизатора значение каждого октета увеличивать на 1. Настроить пассивные интерфейсы на каждом маршрутизаторе. Определить DR- и BDR-маршрутизаторы, заполнить таблицу 7.2. Проверить доступность устройств из разных сетей. Представить в отчете результаты выполнения команд `show ipv6 protocols`, `show ipv6 ospf neighbor` и `show ipv6 route` для маршрутизатора Router1. Сохранить файл под именем **Lab7-1.pkt**.

Таблица 7.2 – Определение DR- и BDR-маршрутизаторов

Имя маршрутизатора	Настройка идентификаторов маршрутизаторов		Passive-interface
	Router ID	DR/BDR	

4. Изменить эталонную пропускную способность на каждом маршрутизаторе в соответствии с исходными данными из таблицы 7.1. В отчете представить изображение смоделированной сети с обозначением стоимости каждого маршрута (см. рисунок 7.1) и таблицу маршрутизации маршрутизатора Router1. Сохранить файл под именем **Lab7-2.pkt**.

7.3 Содержание отчета

1. Цель работы, исходные данные из таблицы 7.1.
2. Результаты произведенных настроек (см. задания 3–4 подраздела 7.2), заполненная таблица 7.2, изображение смоделированной сети.
3. Вывод по работе.
4. Ответы на контрольные вопросы.

7.4 Контрольные вопросы и задания

1. Назвать различия протоколов OSPFv2 и OSPFv3.
2. Назвать сходства между протоколами OSPFv2 и OSPFv3.
3. Описать процесс настройки маршрутизации по протоколу OSPFv3.
4. Какие данные передаются в сообщениях OSPFv3?
5. В чем заключается назначение таблицы смежности маршрутизатора? Описать ее структуру.

ЛАБОРАТОРНАЯ РАБОТА № 8
АГРЕГАЦИЯ МАРШРУТОВ

Цель: изучить принципы объединения маршрутов в IPv4- и IPv6-сетях; овладеть навыками конфигурации суммарных и плавающих статических маршрутов.

8.1 Теоретическая часть

Агрегация (объединение) маршрутов – это процесс объявления группы смежных адресов единым адресом с более короткой маской подсети. Такой тип объединения позволяет сократить количество записей в обновлениях маршрутов и в локальных таблицах маршрутизации. Также это позволяет сократить использование полосы пропускания в целях обновлений маршрутизации, что обеспечивает более быстрый поиск по таблице маршрутизации [4].

В IPv4- и IPv6-сетях выделяют следующие типы статических маршрутов:

- стандартный статический маршрут (рекомендуется использовать при подключении к определенной удаленной сети);
- статический маршрут по умолчанию;
- суммарный статический маршрут;
- плавающий статический маршрут.

Статические маршруты чаще всего используются для подключения к конкретной сети или предоставления «шлюза последней надежды» для тупиковой сети. Их также можно использовать для создания резервного маршрута на случай отказа основного маршрута.

На рисунке 8.1 на маршрутизаторе 1, подключенном к внешней сети, настроен статический маршрут для доступа к тупиковой сети, а на маршрутизаторе 2 настроен статический маршрут по умолчанию для отправки пакетов во внешнюю сеть.

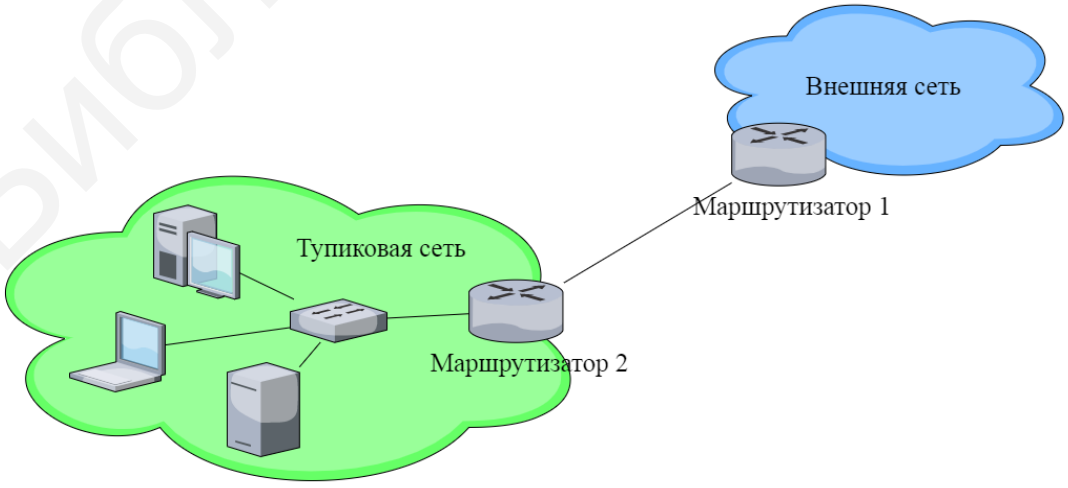


Рисунок 8.1 – Пример тупиковой сети

Тупиковая сеть (Stub Network) – изолированный участок локальной сети, в которой маршрутизаторы не имеют детальных маршрутов ко всем сетям, а используют маршрут по умолчанию [12].

Статические маршруты по умолчанию также могут использоваться в следующих случаях:

- при отсутствии других маршрутов в таблице маршрутизации, совпадающих с IP-адресом назначения пакета;
- при подключении пограничного маршрутизатора сети организации к сети интернет-провайдера.
- при подключении маршрутизатора только к одному маршрутизатору (тупиковый маршрутизатор).

Для уменьшения числа записей в таблице маршрутизации можно объединить несколько статических маршрутов в один статический маршрут, который называют суммарным. 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.

В соответствии с рисунком 8.2 маршрутизатору 1 требуется четыре отдельных статических маршрута для подключения к сетям в диапазоне от 172.20.0.0/16 до 172.23.0.0/16. Вместо этого можно настроить один суммарный статический маршрут, который будет обеспечивать подключение к ним.

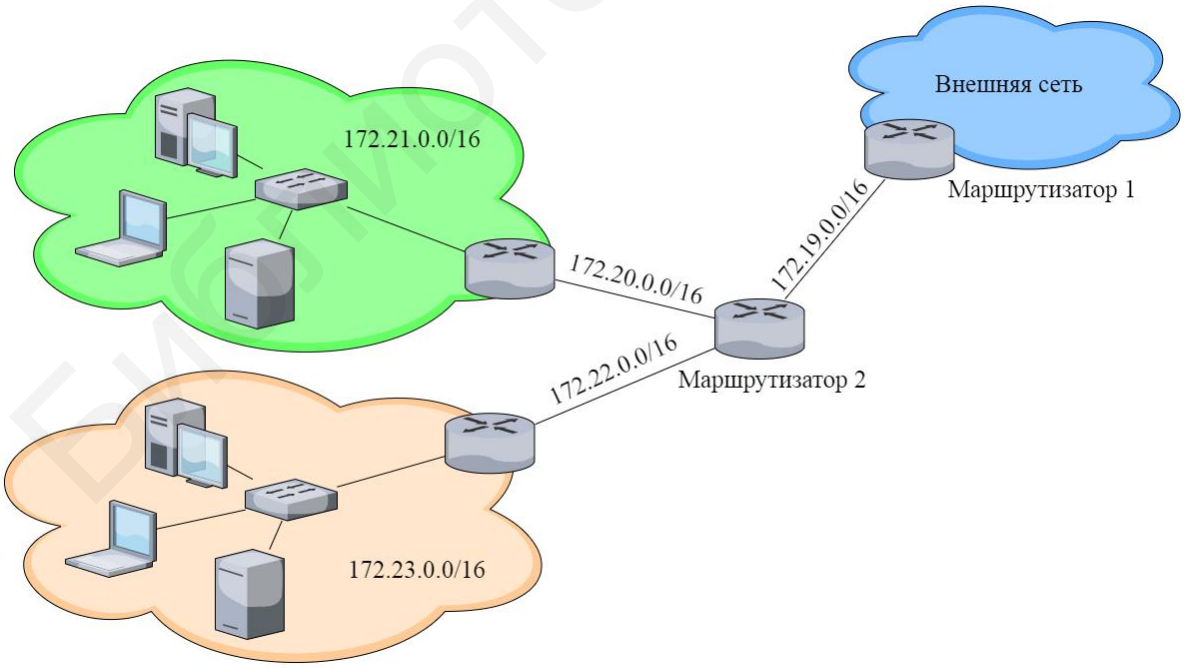


Рисунок 8.2 – Пример сети с суммарным статическим маршрутом

Для конфигурации суммарного статического маршрута на маршрутизаторе 1 необходимо использовать команду `ip route 172.20.0.0 255.252.0.0 172.19.0.2`.

Несколько статических IPv6-маршрутов можно объединить в один маршрут IPv6 в следующих случаях:

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

- все маршруты используют один выходной интерфейс или одинаковый IPv6-адрес следующего перехода.

На рисунке 8.3 маршрутизатор 1 содержит четыре статических маршрута IPv6, обеспечивающих доступ к сетям в диапазоне от 2001:DB8:ACAD:1::/64 до 2001:DB8:ACAD:4::/64.

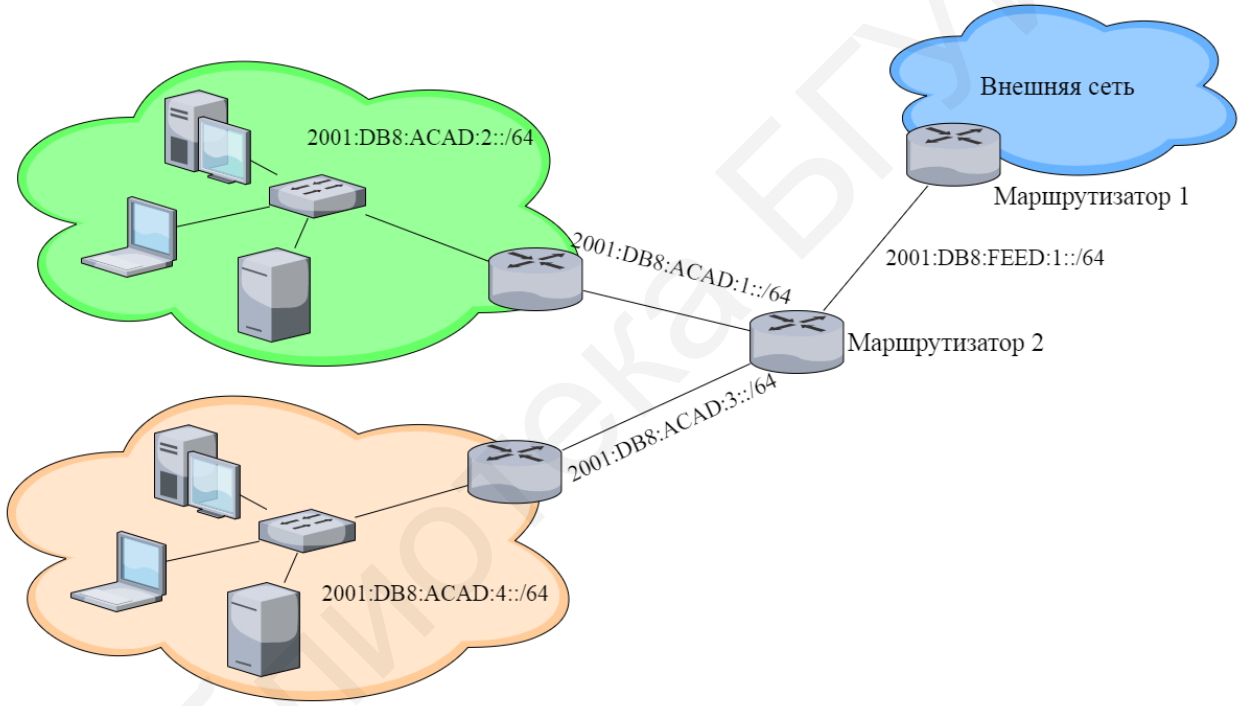


Рисунок 8.3 – Пример сети для объединения IPv6-маршрута

После определения суммарного маршрута следует заменить существующие маршруты одним суммарным маршрутом. Для начала необходимо удалить существующие статические маршруты и настроить новый суммарный статический IPv6-маршрут. Суммарный IPv6-маршрут на маршрутизаторе 1 (см. рисунок 8.3) может быть настроен с помощью команды `ipv6 route 2001:DB8:ACAD::/61 2001:DB8:FEED:1::2`.

Плавающие статические маршруты – это статические маршруты, используемые для предоставления резервного пути основному статическому или динамическому маршруту на случай сбоя в работе канала. Он используется только тогда, когда основной маршрут недоступен.

Для этой цели плавающий статический маршрут настраивается с более высоким значением административного расстояния, чем основной маршрут. Следует помнить, что административное расстояние указывает на надежность маршрута. При наличии нескольких путей к адресу назначения маршрутизатор выбирает путь с самым низким значением административного расстояния.

Предположим, что администратору необходимо создать резервный маршрут по протоколу EIGRP. При настройке плавающего статического маршрута необходимо использовать более высокое значение административного расстояния, чем для EIGRP. EIGRP имеет административное расстояние со значением 90. Если плавающий статический маршрут настроен с административным расстоянием 95, то динамический маршрут, установленный посредством EIGRP, имеет приоритет перед плавающим статическим маршрутом. Если маршрут, получаемый по EIGRP, недоступен, то вместо него используется плавающий статический маршрут.

На рисунке 8.4 маршрутизатор филиала 1 перенаправляет весь трафик на маршрутизатор филиала 2 через частную сеть.

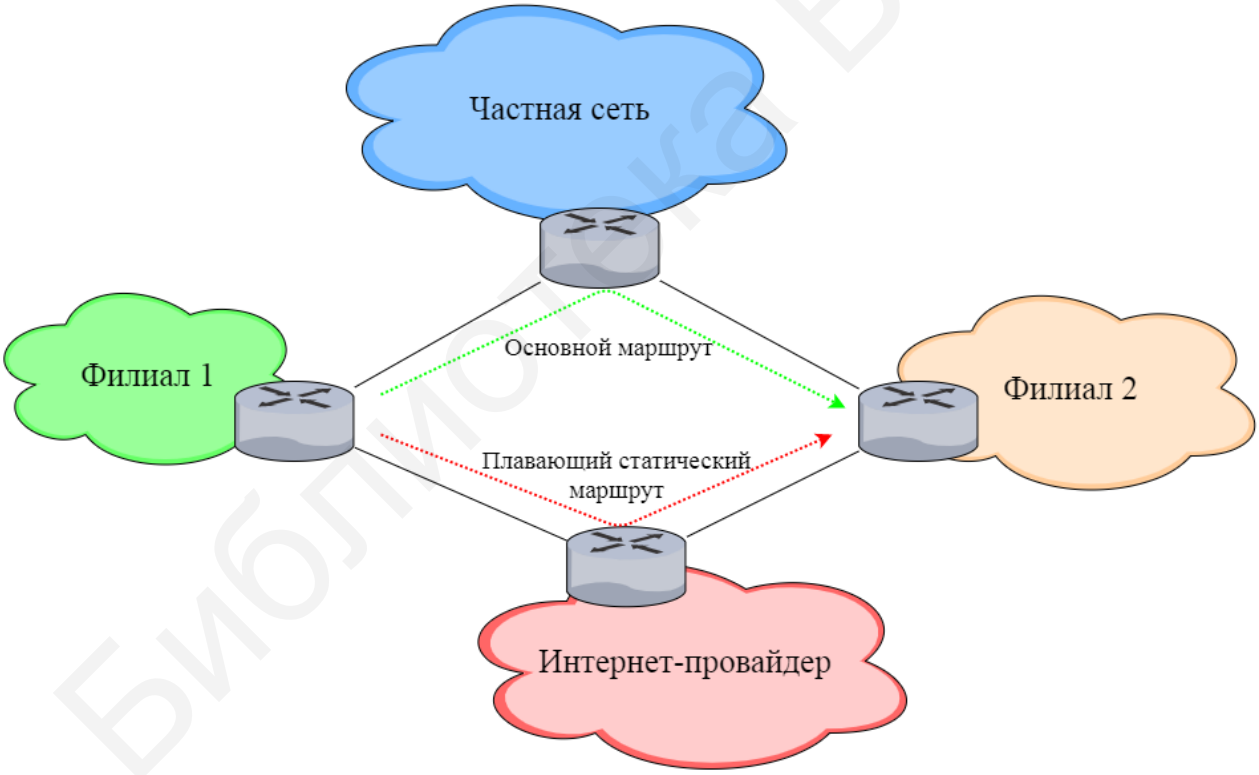


Рисунок 8.4 – Пример сети с плавающим статическим маршрутом

В этом примере маршрутизаторы осуществляют обмен данными о маршруте посредством протокола EIGRP. Плавающий статический маршрут с административным расстоянием, равным 91 или больше, можно настроить для использования в качестве резервного маршрута. При сбое канала связи через частную сеть и удалении маршрута EIGRP из таблицы маршрутизации маршру-

тизатор выбирает плавающий статический маршрут как оптимальный путь для доступа к сети филиала 2.

Статические маршруты IPv4 настраиваются с помощью команд глобальной конфигурации `ip route` и выставления значения административного расстояния. Если оно не задано, используется значение, по умолчанию равное 1.

На рисунке 8.5 представлен пример сети с настроенными статическими маршрутами, которые проходят от маршрутизатора Router1 к сетям 192.168.200.0/24 и 192.168.201.0/24 через маршрутизатор Router3.

Для конфигурации плавающего статического маршрута, который будет проходить через Router2 (рисунок 8.6) в случае неисправности маршрутизатора Router3, необходимо ввести команду `ip route 192.168.200.0 255.255.255.0 172.20.0.6 250` на маршрутизаторе Router1. В конце данной команды указывается административное расстояние, значение которого должно быть больше административного расстояния основного маршрута.

Необходимо отметить, что настроенный плавающий статический маршрут не отображается в таблице маршрутизации до тех пор, пока не начнет использоваться. После восстановления работы всей сети данные будут снова передаваться по основному маршруту.

Конфигурация плавающих статических маршрутов для IPv6-сетей осуществляется аналогично с помощью команды `ip route` и настройки значения административного расстояния.

8.2 Лабораторное задание

В данной лабораторной работе необходимо настроить суммарные и плавающие статические IPv4- и IPv6-маршруты на основе настроек, произведенных в заданиях лабораторных работ № 2, 4, 5 и 7, исходя из следующих заданий.

1. До начала выполнения необходимо открыть сохраненный файл с именем с именем **Lab4-2.pkt**, полученный в лабораторной работе № 4, и проверить настройки IP-адресации и маршрутизации OSPFv2. В данной сети должны находиться следующие подсети: подсети с VLAN, подсеть с беспроводным маршрутизатором, подсеть Building1, подсеть с серверами, подсеть с IoT-устройствами, подсеть с IP-видеонаблюдением. Соединение сетей должно быть осуществлено способом, показанным на рисунке 8.7. По результатам выполнения первой части лабораторной работы все устройства любой из подсетей должны получать доступ к серверам, на которых должны отображаться статусы всех IoT-устройств и условия их работы. Доступ к серверам должен осуществляться посредством DNS.

В данной части лабораторной работы необходимо настроить суммарный статический IPv4-маршрут, исходя из следующих заданий.

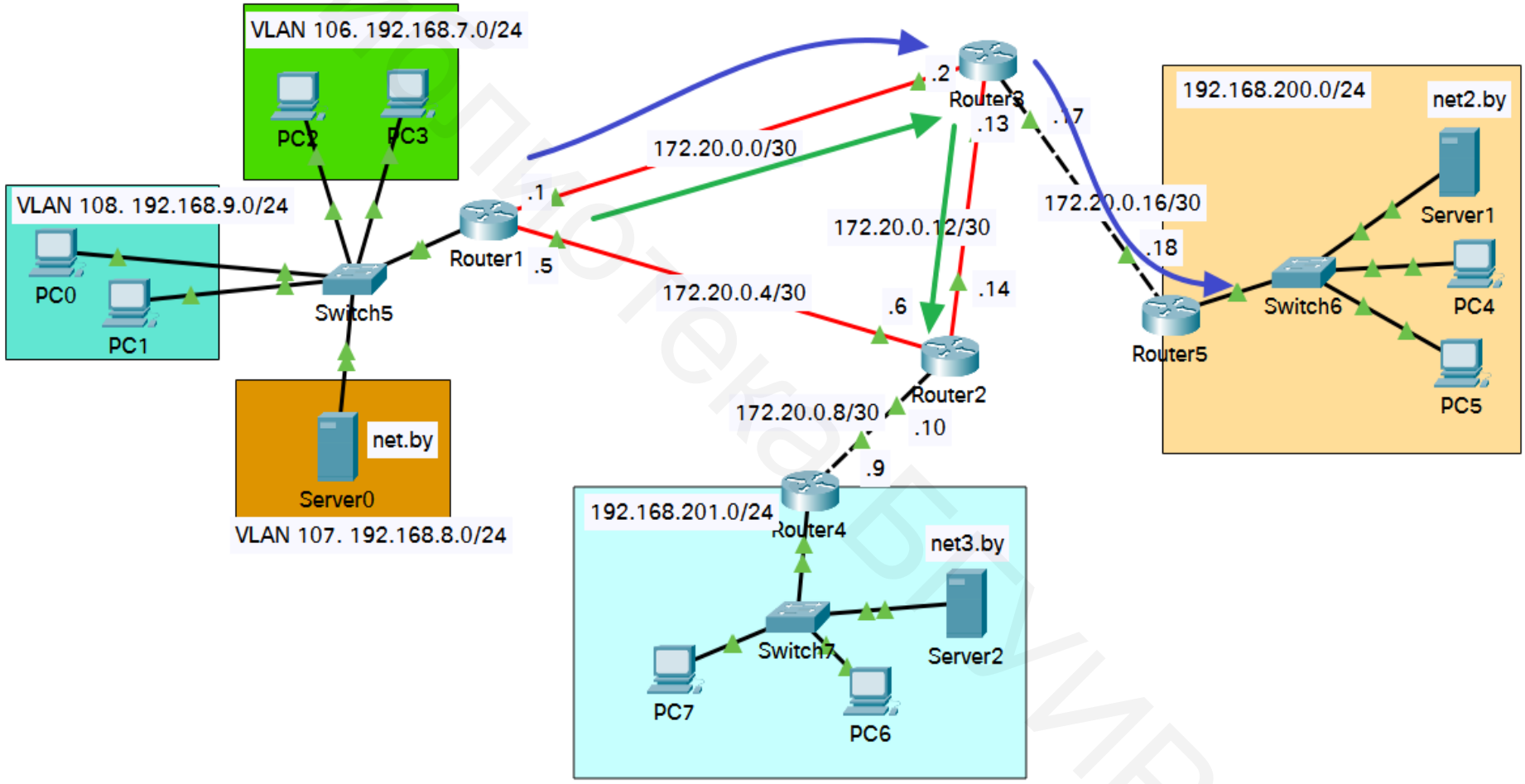


Рисунок 8.5 – Пример сети с настроенным статическим маршрутом

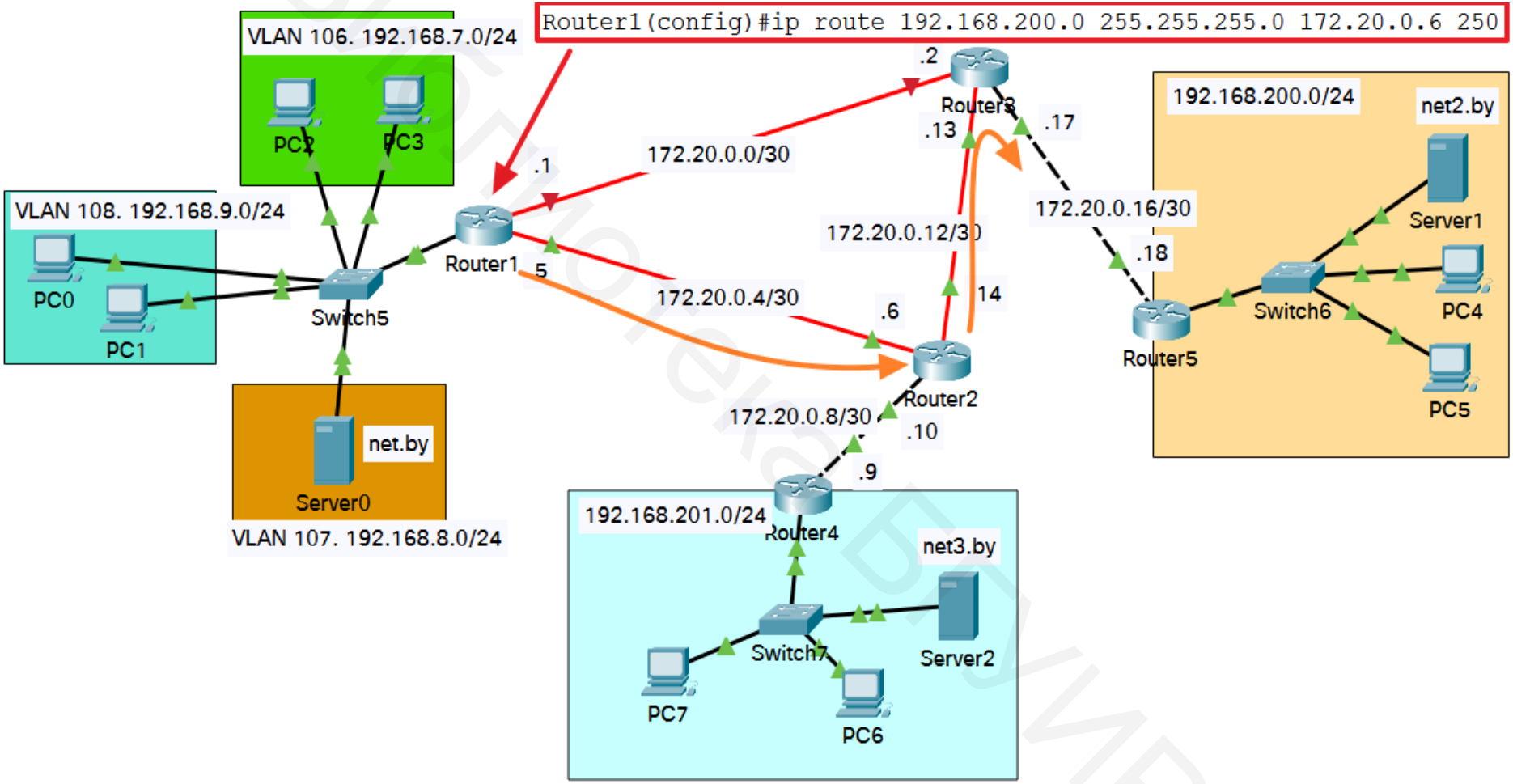


Рисунок 8.6 – Пример сети с настроенным плавающим статическим маршрутом

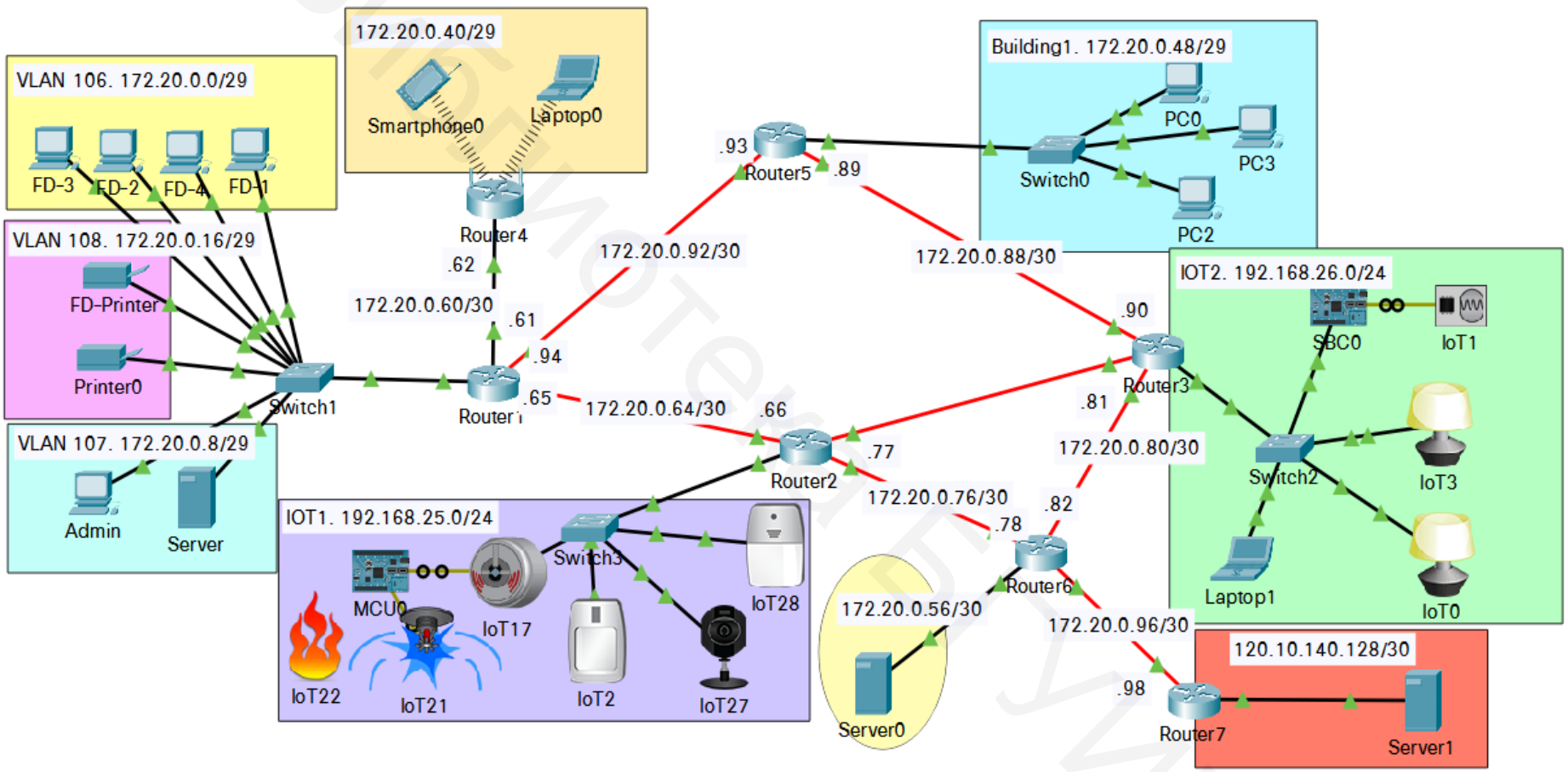


Рисунок 8.7 – Пример смоделированной сети в Cisco Packet Tracer

1.1. Добавить маршрутизатор, через который будет организовываться доступ во внешнюю сеть (маршрутизатор Router7 на рисунке 8.7). К данному маршрутизатору подключить сервер. Определить **реальный** публичный адрес сервера, исходя из данных в таблице 8.1.

Таблица 8.1 – Исходные данные для настройки внешней сети

Первая цифра шифра	Публичный IP-адрес для внешней сети	Доменное имя
0	46.216.181.40/29	bsuir.by
1	87.250.250.240/30	ya.ru
2	172.217.18.108/30	youtube.com
3	54.204.115.52/29	instagram.com
4	5.101.152.160/28	wiki.ru
5	23.22.39.112/28	nasa.gov
6	140.98.193.144/28	ieee.org
7	104.244.42.128/30	twitter.com
8	129.42.38.8/30	ibm.com
9	178.248.237.64/29	habr.com

1.2. Рассчитать и настроить суммарный IPv4-маршрут для добавленного маршрутизатора (маршрутизатор Router7 на рисунке 8.7), а на соседнем маршрутизаторе (маршрутизатор Router6 на рисунке 8.7) задать маршрут по умолчанию к новому маршрутизатору (маршрутизатор Router7 на рисунке 8.7).

Для рассылки статического маршрута по умолчанию внутри сети необходимо на соседнем маршрутизаторе (маршрутизатор Router6 на рисунке 8.7) в настройках OSPF ввести команду `default-information originate`. Представить в отчете результат расчета суммарного маршрута и конфигурацию маршрутов на новом и соседнем от него маршрутизаторе. В результате внешний сервер должен быть доступен с любого устройства в сети. Доступ ко всем серверам должен осуществляться по DNS. Сохранить файл под именем **Lab8-1.pkt**.

2. До начала выполнения необходимо открыть сохраненный файл с именем **Lab7-1.pkt**, полученный в лабораторной работе № 7, и проверить настройки IP-адресации и маршрутизации OSPFv3. В данной сети должны находиться следующие подсети: подсети с VLAN, подсеть Building1, подсеть с сервером, подсеть с IoT-устройствами, подсеть с IP-видеонаблюдением. Соединение сетей должно быть осуществлено способом, показанным на рисунке 8.8.

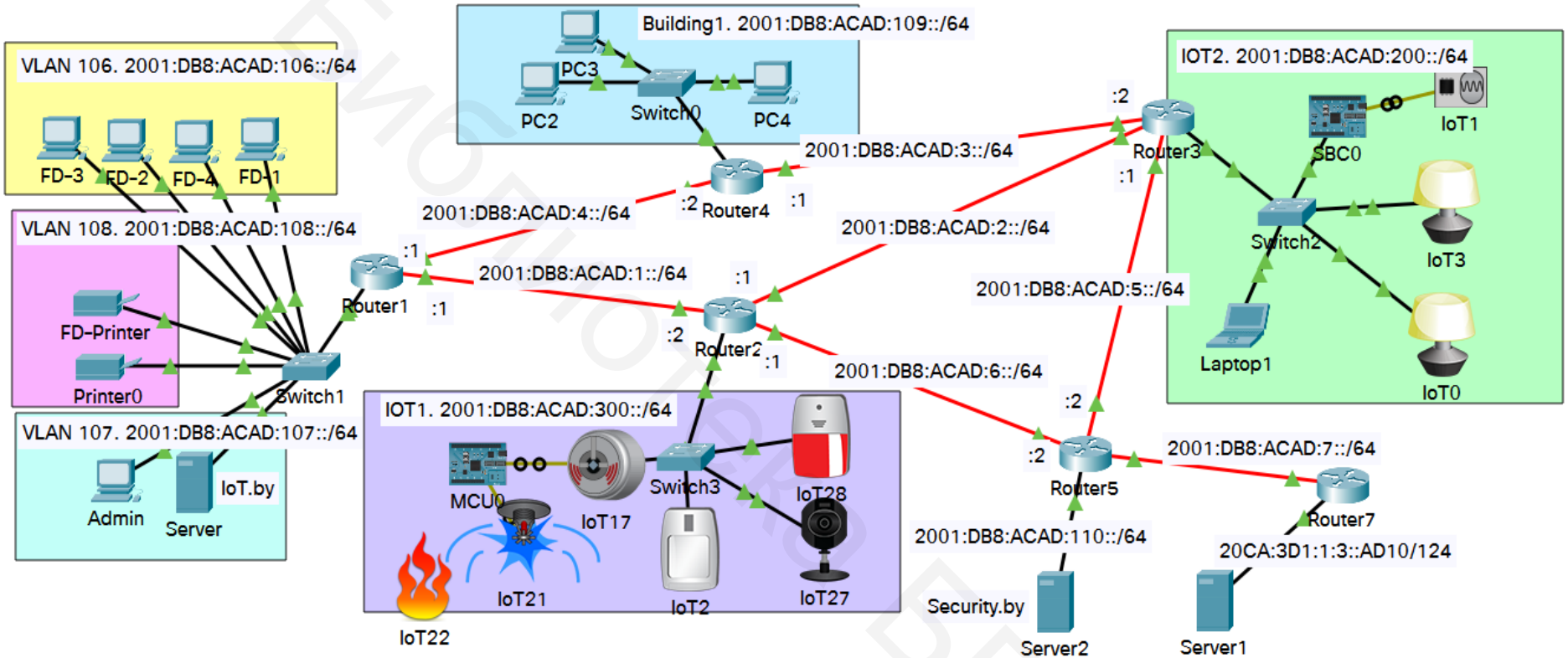


Рисунок 8.8 – Пример смоделированной сети в Cisco Packet Tracer

По результатам выполнения второй части лабораторной работы все устройства любой из подсетей должны получать доступ к серверам, на которых должны отображаться статусы всех IoT-устройств и условия их работы. Доступ к серверам должен осуществляться посредством DNS.

В данной части лабораторной работы необходимо настроить суммарный статический IPv6-маршрут, исходя из следующих заданий.

2.1. Добавить маршрутизатор, через который будет организовываться доступ во внешнюю сеть (маршрутизатор Router7 на рисунке 8.8). К данному маршрутизатору подключить сервер, IPv6-адрес которого указан в таблице 8.2.

Таблица 8.2 – Исходные данные для настройки внешней сети

Первая цифра шифра	Публичный IPv6-адрес сервера	Доменное имя
0	2a00:1450:4010:c0b::8a/120	google.com
1	2a02:6b8::2:242/92	ya.ru
2	2a00:1450:4010:c0d::be/120	youtube.com
3	2406:da00:ff00::3d5:7bf8/100	instagram.com
4	2001:420:1101:1::185/116	cisco.com
5	2600:1f18:1f:db01:11af:58af:ae11:f645/112	nasa.gov
6	2a00:1148:db00:0:b0b0::1/124	mail.ru
7	2a02:2208:1:1::89/120	byfly.by
8	2a0a:7d80::d/124	tut.by
9	2a02:26f0:f1:182::24c5/112	viber.com

2.2. Для добавленного маршрутизатора (маршрутизатор Router7 на рисунке 8.8) рассчитать и настроить суммарный маршрут, а на соседнем маршрутизаторе (маршрутизатор Router5 на рисунке 8.8) задать маршрут по умолчанию к новому маршрутизатору (маршрутизатор Router7 на рисунке 8.8). Для рассылки статического маршрута по умолчанию внутри сети необходимо на соседнем маршрутизаторе (маршрутизатор Router5 на рисунке 8.8) в настройках OSPF ввести команду `default-information originate`. Представить в отчете результат расчета суммарного маршрута и конфигурацию маршрутов на новом и соседнем от него маршрутизаторе. В результате внешний сервер должен быть доступен с любого устройства в сети. Доступ ко всем серверам должен осуществляться по DNS. Сохранить файл под именем **Lab8-2.pkt.**

3. До начала выполнения необходимо открыть сохраненный файл с именем **Lab2-1.pkt**, полученный в лабораторной работе № 2, и проверить настройки IP-адресации и статической маршрутизации. В данной сети должны находиться следующие подсети: подсети с VLAN, подсеть с беспроводным маршрутизатором, подсеть с IoT-устройствами, подсеть с IP-видеонаблюдением.

В данной части лабораторной работы необходимо настроить плавающий статический IPv4-маршрут, исходя из следующих заданий.

3.1. Организовать соединение маршрутизаторов по топологии «кольцо», как показано на рисунке 8.9. Удостовериться, что в исходном файле **Lab2-1.pkt** настроены статические маршруты. Настроить плавающие статические IPv4-маршруты на всех маршрутизаторах. Представить в отчете результаты настройки.

3.2. Отключить маршрутизатор, через который проходит основной маршрут, и удостовериться, что все устройства из любой подсети получают доступ к серверу, на котором отображаются статусы всех IoT-устройств и условия их работы. Доступ к серверу должен осуществляться посредством DNS. В отчете представить таблицу маршрутизации одного из маршрутизаторов с настроенными плавающими статическими маршрутами.

3.3. Восстановить работу отключенного в задании 3.2 маршрутизатора и представить в отчете таблицу маршрутизации, из которой видно, что основные маршруты активны. Сохранить файл под именем **Lab8-3.pkt**.

4. До начала выполнения необходимо открыть сохраненный файл с именем **Lab5-2.pkt**, полученный в лабораторной работе № 5, и проверить настройки IPv6-адресации и статической маршрутизации. В данной сети должны находиться следующие подсети: подсети с VLAN, подсеть с IoT-устройствами, подсеть с IP-видеонаблюдением.

В данной части лабораторной работы необходимо настроить плавающий статический IPv6-маршрут, исходя из следующих заданий.

4.1. Удостовериться, что в исходном файле **Lab5-2.pkt** настроены статические маршруты. Настроить плавающий статический маршрут на всех маршрутизаторах. Представить в отчете результаты настройки.

4.2. Отключить маршрутизатор, через который проходит основной маршрут, и удостовериться, что все устройства из любой подсети получают доступ к серверу, на котором отображаются статусы всех IoT-устройств и условия их работы. Доступ к серверу должен осуществляться посредством DNS. В отчете представить таблицу маршрутизации одного из маршрутизаторов с настроенными плавающими статическими маршрутами.

4.3. Восстановить работу отключенного в задании 4.2 маршрутизатора и представить в отчете таблицу маршрутизации, из которой видно, что основные маршруты активны. Сохранить файл под именем **Lab8-4.pkt**.

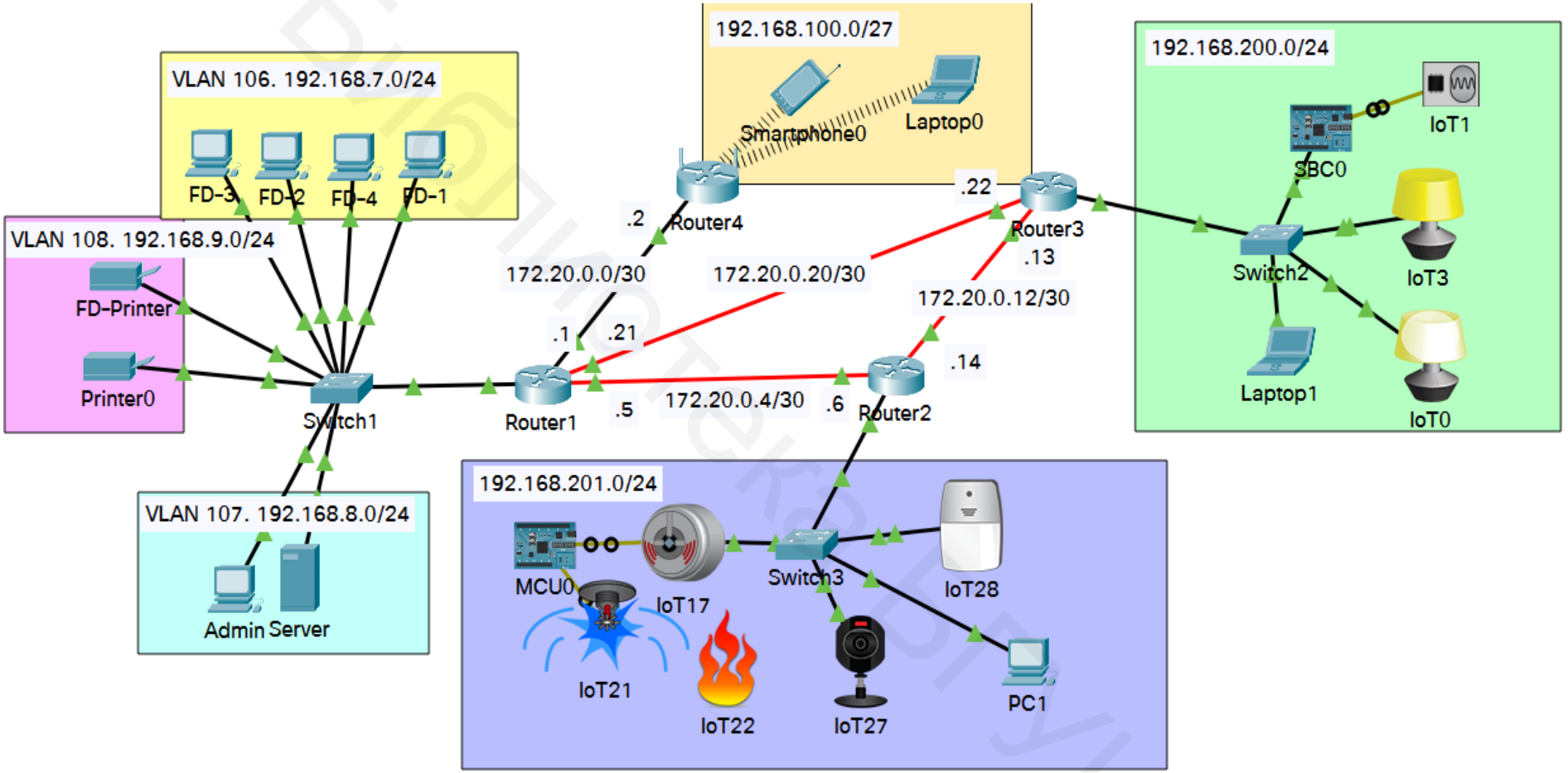


Рисунок 8.9 – Пример смоделированной сети в Cisco Packet Tracer

8.3 Содержание отчета

1. Цель работы, исходные данные из таблиц 8.1, 8.2.

2. Результаты произведенных настроек из (см. задания 1–4 подраздела 8.2), изображения смоделированных сетей.

3. Вывод по работе.

4. Ответы на контрольные вопросы.

8.4 Контрольные вопросы и задания

1. Объяснить назначение всех видов статических маршрутов.

2. Перечислить условия объединения статических IPv4- и IPv6-маршрутов.

3. Привести пример реализации конфигурации суммарных статических IPv4- и IPv6-маршрутов.

4. Объяснить назначение плавающих статических IPv4- и IPv6-маршрутов и представить пример их конфигурации.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Каменев, Д. С. Проектируем систему IP-видеонаблюдения [Электронный ресурс] / Д. С. Каменев. // ИКС. – Режим доступа: https://www.iksmedia.ru/articles/3754049-Proektiruem-sistemu-IPvideonablyude.html. – Дата доступа: 21.12.2021.

2. Чернобровцев, А. Д. Какие сети нужны для систем видеонаблюдения предприятий? [Электронный ресурс] / А. Д. Чернобровцев // Открытые системы. – Режим доступа: https://www.osp.ru/nets/2012/04/13017491. – Дата доступа: 23.12.2021.

3. Новиков, С. А. Передача данных видеонаблюдения по IP-сетям [Электронный ресурс] / С. А. Новиков // Открытые системы. СУБД. – Режим доступа: http://citforum.ru/ nets/digest/video/ – Дата доступа: 26.12.2021.

4. Яницкая, Т. С. Глобальные и территориальные инфокоммуникационные сети / Т. С. Яницкая, А. Б. Кузьмичев. – Тольятти : ПВГУС, 2016. – 256 с.

5. Инфокоммуникационные системы и сети. Практикум : учеб. пособие / И. Г. Карпов [и др.]. – Тамбов : ФГБОУ ВО «ТГТУ», 2016. – 236 с.

6. Материалы CISCO CCNA. Маршрутизация [Электронный ресурс] // Дневники Сетевого Инженера. – Режим доступа: https://arny.ru/education/ccna-rs/materialyi-cisco-ccna-chasti-1-i-2-kursa-marshrutizatsiya/. – Дата доступа: 27.12.2020.

7. Ловшук, А. П. Исследование способов обеспечения отказоустойчивой маршрутизации в сетях пакетной коммутации / А. П. Ловшук, Е. А. Шеленок // Ученые заметки ТОГУ. – 2016. – Т. 7, № 2. – С. 223–230.

8. Инфокоммуникационные сети: энциклопедия : в 2 т. / Т. 1 : Инфокоммуникационные сети: классификация, структура, архитектура, жизненный цикл, технологии / С. П. Воробьёв [и др.]. – СПб. : Наукоемкие технологии, 2019. – 739 с.

9. Таненбаум, Э. Компьютерные сети / Э. Таненбаум, Д. Уэзеролл. – СПб. : Питер, 2012. – 960 с.

10. Рубашенков, А. М. Протокол OSPF / А. М. Рубашенков, Д. А. Семёнов // Научный журнал. – 2018. – № 10 (33). – С. 20–21.

11. Бирюков, А. А. Безопасность протокола OSPF / А. А. Бирюков // Системный администратор. – 2012. – № 7–8.

12. Королькова А. В. Сетевые технологии. Лабораторные работы / А. В. Королькова, Д. С. Кулябов. – М. : РУДН, 2014. – 106 с.

13. Ловшук, А. П. Исследование способов обеспечения отказоустойчивой маршрутизации в сетях пакетной коммутации / А. П. Ловшук, Е. А. Шеленок // Ученые заметки ТОГУ. – 2016. – Т. 7, № 2. – С. 223–230.

14. Бабаян, Р. Г. Промышленное видеонаблюдение / Р. Г. Бабаян // Вестник науки. – 2019. – Т. 1, № 6 (15). – С. 35–37.

15. Ракчеев А. Ю. Настройка динамической маршрутизации OSPF / А. Ю. Ракчеев // Colloquium-journal. – 2020. – № 5 (57). – С. 106–110.

16. Васин, Н. Н. Основы сетевых технологий на базе коммутаторов и маршрутизаторов / Н. Н. Васин. – М. : Интернет-университет информационных технологий, 2011. – 270 с.

17. Королькова А. В. Сетевые технологии. Лабораторные работы / А. В. Королькова, Д. С. Кулябов. – М. : РУДН, 2014. – 106 с.

18. Телекоммуникационные системы и сети : в 3 т. : Т. 3 : Мультисервисные сети : учеб. пособие / В. В. Величко [и др.]. – Изд. 2-е. – М. : Горячая линия – Телеком, 2015. – 592 с.

19. Гребешков, А. Ю. Вычислительная техника, сети и телекоммуникации : учеб. пособие для вузов / А. Ю. Гребешков– М. : Горячая линия – Телеком, 2015. – 190 с.

20. Ганжа, В. А. Компьютерные сети. Введение : учеб.-метод. пособие / В. А. Ганжа, В. В. Шиманский. – Минск : БГУИР, 2015. – 155 с.

21. Лэммл, Т. CCNP. Маршрутизация: учеб. руководство / Т. Лэммл, Ш. Одом, К. Уоллес. – М. : Лори, 2015. – 485 с.

22. Амато, В. Основы организации сетей Cisco : в 2 т. : Т. 1. / В. Амато. – М. : Вильяме, 2002. – 512 с.

23. Елисеев, А. И. Технологии маршрутизации : учеб. пособие / А. И. Елисеев, Д. В. Поляков. – Тамбов : ФГБОУ ВО «ТГТУ», 2016. – 79 с.

24. Семенов, Ю. А. Протоколы и алгоритмы маршрутизации в Internet / Ю. А. Семенов // Алгоритмы телекоммуникационных сетей : в 3 ч. / М. : Национальный открытый университет «ИНТУИТ», 2016. – 1004 с.

25. Цветков, В. Ю. Протоколы внутренней маршрутизации: OSPF и EIGRP : учеб.-метод. пособие / В. Ю. Цветков, К. А. Волков. – Минск : БГУИР, 2017. – 72 с.

26. Белоусова, Е. С. Основы построения локальных сетей. Лабораторный практикум : учеб.-метод. пособие / Е. С. Белоусова. – Минск : БГУИР, 2020. – 103 с.

Св. план 2021, поз. 28

Учебное издание

Белоусова Елена Сергеевна

МАРШРУТИЗАЦИЯ В IPV4- И IPV6-СЕТЯХ. ЛАБОРАТОРНЫЙ ПРАКТИКУМ

УЧЕБНО-МЕТОДИЧЕСКОЕ ПОСОБИЕ

Редактор *С. Г. Девдера*
Корректор *Е. Н. Батурчик*
Компьютерная правка, оригинал-макет *О. И. Толкач*

Подписано в печать 14.04.2022. Формат 60×84 1/16. Бумага офсетная. Гарнитура «Таймс».
Отпечатано на ризографе. Усл. печ. л. 6,16. Уч.-изд. л. 6,0. Тираж 40 экз. Заказ 51.

Издатель и полиграфическое исполнение: учреждение образования
«Белорусский государственный университет информатики и радиоэлектроники».
Свидетельство о государственной регистрации издателя, изготовителя,
распространителя печатных изданий №1/238 от 24.03.2014,
№2/113 от 07.04.2014, №3/615 от 07.04.2014.
Ул. П. Бровки, 6, 220013, г. Минск