Федеральное государственное автономное
образовательное учреждение
высшего образования
«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Институт космических и информационных технологий
Кафедра вычислительной техники

УТВЕРЖДАЮ
Заведующий кафедрой ВТ

_____ О.В. Непомнящий
подпись инициалы, фамилия
«_____» _____ 2021 г.

МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ

Метод управления маршрутизацией на основе политик
09.04.01 Информатика и вычислительная техника
09.04.01.05 Сети ЭВМ и телекоммуникации

Научный руководитель _____ доцент, канд. физ.-мат. наук К.В. Коршун
подпись, дата должность, ученая степень инициалы, фамилия

Выпускник _____ И.А. Дрокин
подпись, дата инициалы, фамилия

Рецензент _____ Генеральный директор ООО "Интертакс" М.В. Алексеев
подпись, дата должность, ученая степень инициалы, фамилия

Нормоконтролер _____ К.В. Коршун
подпись, дата инициалы, фамилия

Красноярск 2021

Федеральное государственное автономное
образовательное учреждение
высшего образования
«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Институт космических и информационных технологий
Кафедра вычислительной техники

УТВЕРЖДАЮ
Заведующий кафедрой ВТ

_____ О.В. Непомнящий
подпись инициалы, фамилия
«_____» _____ 2021 г.

ЗАДАНИЕ
НА ВЫПУСКНУЮ КВАЛИФИКАЦИОННУЮ РАБОТУ
в форме магистерской диссертации

Студенту Дрокину Ивану Александровичу
фамилия имя отчество

Группа КИ19-01-5М Направление (специальность) 09.04.01
номер код

«Информатика и вычислительная техника»
наименование

Тема выпускной квалификационной работы Метод управления маршрутизацией на основе политик

Утверждена приказом по университету № 19020/с от 11.06.2019

Руководитель ВКР К.В. Коршун, канд. физ.-мат. наук, доцент кафедры ВТ
инициалы, фамилия, должность, ученое звание и место работы

Исходные данные для ВКР: задание на магистерскую диссертацию

Перечень разделов ВКР: 1 Процесс маршрутизации пакета данных, обзор современных технологий, выявление проблемы и постановка цели исследования. 2 Проектирование метода. 3. Описание реализации метода.

Перечень графического материала: презентация доклада выступления

Руководитель ВКР _____ К.В. Коршун
подпись инициалы и фамилия

Задание принял к исполнению _____ И.А. Дрокин
подпись, инициалы и фамилия студента

«___» _____2021г.

РЕФЕРАТ

Выпускная квалификационная работа по теме «Метод управления маршрутизацией на основе политик» содержит 67 страниц текстового документа, 2 таблицы, 10 иллюстраций, 20 использованных источников.

ПРОТОКОЛ, МАРШРУТИЗАЦИЯ, RIP, EIGRP, OSPF, BGP, ADDRESS-FAMILY, JITTER, BANDWIDTH, THROUGHPUT, IP SLA, EEM, OER, PBR, SDN, ОПТИМИЗАЦИЯ, ИССЛЕДОВАНИЕ, QUAGGA, ISP, IPTABLES.

Цель работы - выполнить проектирование метода, позволяющего автоматизировать основные функции технологии Policy Base Routing (PBR). Это позволит расширить возможность управления маршрутизацией трафика. Для достижения поставленной цели, были сформулированы следующие задачи:

- Провести анализ предметной области, выявить плюсы и минусы существующих протоколов и технологий, маршрутизации;
- Сформировать набор функций технологии PBR, подлежащих автоматизации;
- Выполнить анализ возможных вариантов распространения маршрутной информации;
- Выполнить проектирование метода;
- Описать прототип схемы реализации разработанного метода.

Проведено исследование предметной области, выявлены недостатки и ограничения существующих технологий и протоколов. Рассмотрены инструменты оптимизации маршрутизации. Были выявлены проблемы маршрутизации трафика, которые могут возникать в сетях передачи данных. Было выполнено проектирование метода, автоматизирующего основные функции технологии PBR. Было выполнено описание алгоритма реализации разработанного метода с использованием тестовой сети, построенной на виртуальных машинах под управлением операционной системы Linux Ubuntu, с применением программного обеспечения Quagga, выполняющего задачу маршрутизации и передачу маршрутной информации.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Современные крупные распределенные корпоративные сети могут представлять из себя сложные иерархические конструкции, включающие сотни узлов, в которых выполняется обработка служебного и пользовательского трафика. Передача данных от источника к пункту назначения, представляет собой движение сегментированной единицы данных, пакета, по рассчитанному маршруту. При этом пакет проходит через некоторое число сетевых узлов, соединенных каналами связи. Суммарное время движения пакета, зависит от его скорости, на которую оказывают влияние полоса пропускания канала связи и величина загрузки коммутационного узла. Чем сильнее загружен канал связи и чем меньше свободных ресурсов, таких как оперативная память и мощность процессора, тем в целом медленнее работают приложения на этой сети. Поэтому процесс маршрутизации, то есть, построение оптимального маршрута движения пакета от источника к пункту назначения, играет большую роль для стабильной работы приложений в корпоративной сети.

Цель работы - выполнить проектирование метода, позволяющего автоматизировать основные функции технологии Policy Base Routing (PBR). Это позволит расширить возможность управления маршрутизацией трафика. Для достижения поставленной цели, были сформулированы следующие задачи:

- Провести анализ предметной области, выявить плюсы и минусы существующих протоколов и технологий, маршрутизации;
- Сформировать набор функций технологии PBR, подлежащих автоматизации;
- Выполнить анализ возможных вариантов распространения маршрутной информации;
- Выполнить проектирование метода;
- Описать прототип схемы реализации разработанного метода.

Автоматизация функций технологии PBR даст возможность маршрутизаторам в пределах корпоративной сети передачи данных, автоматически строить и изменять политики влияющие на выбор лучшего маршрута, таким образом самостоятельно вносить коррективы в таблицу маршрутизации. Технология PBR (Policy Base Routing), позволяет использовать механизм политик влияющих на выбор маршрута. Ее минусом является плохая масштабируемость, в следствии того, что все настройки выполняются в ручную администратором, а также отсутствие гибкого реагирования на возникающие изменения в сети. Поэтому было принято решение разработать метод использующий принцип действия PBR, в котором большая часть настроек выполняется в автоматическом режиме.

Новый метод получил название iPBR (Intellectual Policy Based Routing). Был сформирован список задач автоматизации:

- Наблюдать за состоянием каналов связи между маршрутизаторами, каналов с провайдерами. Возможность отслеживать изменения топологии и принимать нужные меры, повысит гибкость работы технологии.
- Распространять маршрутную информацию между маршрутизаторами, чтобы каждый обладал актуальными данными. Необходимое условие для получения состояния сходимости сети.
- Автоматически создавать правила политик, а в случае изменения топологии сети иметь возможность внести поправки. Это расширит возможности управления сетевым трафиком.

Была разработана структура и основные принципы функционирования iPBR. Введены и описаны сущности, позволяющие объяснить работу метода:

- Введен необходимый минимум служебных сообщений. Для обмена маршрутной информацией, на основе которой выполняется построения карты политик, используется сообщение UPDATE, сформирована структура сообщения.
- Назначены таймеры для решения задач управления и контроля.
- Описана операция установки соседских отношений.

- Обмен служебной информацией для автоматического распространения по всей сети данных для построения карт политик.
- Проверка состояний каналов связи и механизм реагирования в случае выхода канала из строя.
- Описан порядок шагов по настройки iPBR.
- Выполнен пример настройки со схемой и файлами конфигурации маршрутизаторов.

Для построения модели работы метода, можно использовать схему собранную на виртуальных машинах под управление операционной системы Linux Ubuntu. Для реализации алгоритма распространения маршрутной информации подойдет расширенный пакет программ маршрутизации Quagga.

1 Процесс маршрутизации пакета данных, обзор современных технологий, выявление проблемы и постановка цели исследования

В этой работе речь пойдет о маршрутизации в корпоративных сетях. О ее роли в процессе продвижения трафика, о том, что процессом маршрутизации можно управлять, о важности выбора оптимального маршрута обеспечивающего перемещение пакетов без потерь и на высокой скорости. Для примера будут рассмотрены традиционные протоколы маршрутизации и современные технологии управления передачей данных. Поэтому стоит начать с определения некоторых понятий.

1.1 Корпоративная сеть передачи данных, ее структура и свойства.

Корпоративная сеть передачи данных (СПД) - это телекоммуникационная сеть, принадлежащая и управляемая единой организацией в соответствии с правилами этой организации, объединяющая в общее информационное пространство все структурные подразделения, предназначенная для выполнения производственных функций компании [1].

Схема корпоративной СПД зависит от общей организационной структуры компании. Наибольшее распространение имеют два типа дизайна сети, по принципу функциональной структуры или географической структуры. Сеть передачи данных, может быть разделена на три основных уровня организации.

1) Уровень ядра (Core layer). Главной задачей является обработка потоков данных, с целью передачи в нужный сегмент корпоративной сети. В ядре используются высокоскоростные коммутаторы и маршрутизаторы с целью уменьшения задержек при передаче потоков данных. Для повышения надежности применяются схемы резервирования оборудования. Главная задача этого уровня максимально быстрое перемещение трафика между подключенными к ядру сегментами сети.

2) Уровень распределения (Distribution layer). Распределение потоков данных внутри сегмента сети и передача части потока данных в уровень ядра для дальнейшей обработки.

3) Уровень доступа (Access layer). Точка входа в сеть конечных пользователей. Главная задача оборудования уровня доступа состоит в обеспечении возможности надежного подключения к сети пользователей и обеспечение необходимых мер безопасности.

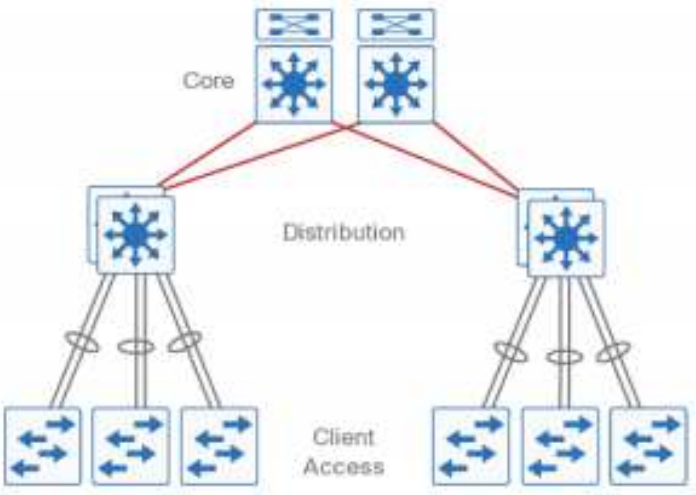

Рисунок 1. — Топология сети

В большом количестве компаний основные потоки данных передаются от филиалов в центральное подразделение, где располагаются корпоративные базы данных и сетевые сервисы. Наиболее удачной топологией сети для отображения подобных потоков трафика является топология "звезда", в которой могут присутствовать резервные связи для повышения отказоустойчивости [2].

Корпоративную СПД характеризуют следующие свойства:

Высокая производительность. Трафик между сетевыми узлами должен ходить без потерь и с минимальными задержками. За это отвечает архитектура сети, ширина каналов связи и мощность применяемого сетевого оборудования.

Надежность и отказоустойчивость. Нужно обеспечить непрерывную связь между общими ресурсами и пользователями. Для этого применяется принцип избыточности, структура сети имеет резервные каналы и оборудование.

Безопасность. Защита данных от несанкционированного доступа. Нужно применять при настройки сетевого оборудования современные протоколы безопасности.

Масштабируемость. Возможность без труда добавлять новые сетевые узлы, при этом производительность сети остается прежней. Правильно разработанный дизайн топологии сети позволит без значительных трудозатрат в перспективе управлять и развивать сеть.

Гибкость и управляемость. С ростом сети сложность ее управления увеличивается. Модульный принцип деления сети на однотипные сегменты упрощает ее развитие, управление, поиск и устранение неисправностей.

Компьютерная сеть представляет собой сложную и дорогую систему, решающую ответственные задачи и обслуживающую большое количество пользователей. Поэтому очень важно, чтобы сеть не просто работала, но работала качественно [3].

1.2 Компьютерный трафик и характеристики канала связи.

Трафик при передачи между сетевыми узлами, идет по каналам связи. Технологически каналы разделяются на проводные (или кабельные) и беспроводные. В современных телекоммуникационных системах информация передается с помощью электрического тока или напряжения, радиосигналов или световых сигналов - все эти физические процессы являются колебаниями электромагнитного поля различной частоты.

Основными характеристиками физических каналов, связанными с передачей трафика являются:

Предложенная нагрузка - это поток данных, поступающий от пользователя на вход сети. Предложенную нагрузку можно характеризовать скоростью поступления данных в сеть в Мбит/сек.

Скорость передачи данных (throughput) - это фактическая скорость потока данных, прошедшего через сеть. Эта скорость может быть меньше, чем скорость предложенной нагрузки, так как данные в сети могут искажаться или теряться.

Емкость канала связи (capacity), называемая также пропускной способностью, представляет собой максимально возможную скорость передачи информации по каналу. Зависит от внутренних параметров канала (характерных для среды передачи), внешних параметров - уровня помех, а также принятого способа кодирования данных.

Полоса пропускания (bandwidth) - термин используется как синоним термина емкость канала связи, и является более распространенным, чем емкость.

Трафик компьютерных сетей, это трафик генерируемый приложениями, с которыми работает пользователь. Практически всегда, он является пульсирующим, периоды интенсивного обмена данными чередуются с продолжительными паузами. Например, когда вы загружаете из Интернета очередную страницу, скорость трафика резко возрастает, а после окончания загрузки падает практически до нуля.

Наличие буферной памяти в сетевых коммутаторах и маршрутизаторах, позволяет эффективно использовать пропускную способность каналов при передаче пульсирующего трафика, но при переполнении буфера, приводит к задержкам в доставке пакетов и потерям, что для трафика реального времени является серьезным недостатком.

Случайный характер процесса образования очередей приводит к случайным задержкам, при этом задержки отдельных пакетов могут быть значительными, в десятки раз превосходя среднюю величину задержек. Неравномерность задержек изменяет относительное положение пакетов в выходном потоке, а это может катастрофически сказаться на качестве работы некоторых приложений, например при передачи голоса. Пакеты могут теряться в сети или же приходить в узел назначения с искаженными данными, что равносильно потере пакета. Пакеты также могут дублироваться по разным причинам, например из-за ошибочных повторных передач пакета, предпринятых протоколом, в котором таким образом обеспечивается надежный обмен данными. Чем больше потерь и искажений пакетов происходит в сети, тем ниже скорость информационного потока.

Для оценки производительности сети используются различные характеристики задержек и потерь пакетов:

Односторонняя задержка пакетов (One-Way Delay Metric, OWD). Определяется как интервал времени между моментом помещения в исходящую линию связи первого бита пакета узлом-отправителем и моментом приема последнего бита пакета с входящей линии связи узла-получателя.

Вариация задержки пакета, которую также называют джиттером (jitter). Определяется стандартом как разность односторонних задержек для пары пакетов определенного типа, полученных на интервале измерений T.

Время реакции сети. Определяется как интервал времени между отправкой запроса пользователя к какой-либо сетевой службе и получением ответа на этот запрос.

Время оборота пакета (Round Trip Time, RTT). Определяется как интервал времени между отправкой первого бита пакета определенного типа узлом-отправителем узлу-получателю и получением последнего бита этого пакета узлом-отправителем после того, как пакет был получен узлом получателем и отправлен обратно.

Доля потерянных пакетов. Равная отношению количества потерянных пакетов к общему количеству переданных пакетов

Из-за последовательного характера передачи данных различными элементами сети, общая пропускная способность любого составного пути в сети, будет равна минимальной из пропускных способностей составляющих элементов маршрута. Для повышения пропускной способности составного пути, необходимо в первую очередь обратить внимание на самые медленные элементы, называемые узкими местами [3].

1.3 Маршрутизация, ее роль и назначение.

Маршрутизация – это процесс, при котором осуществляется передача пакетов маршрутизируемого протокола, при помощи протокола маршрутизации, от логического отправителя логическому получателю.

Маршрутизация является функцией третьего уровня модели OSI. Она основана на иерархической схеме, которая позволяет группировать отдельные адреса и работать с группами как с единым целым до тех пор, пока не потребуется установить индивидуальный адрес для окончательной доставки данных.

Маршрутизируемый протокол – это любой сетевой протокол, адрес сетевого уровня которого предоставляет достаточное количество информации для доставки пакета от одного сетевого узла другому на основе используемой схемы адресации.

Маршрутизирующий протокол (протокол маршрутизации) – это протокол, который поддерживает маршрутизируемые протоколы и предоставляет механизмы обмена маршрутной информацией.

Основным устройством, отвечающим за осуществления процесса маршрутизации, является маршрутизатор. Выполняет две ключевые функции: маршрутизация – поддержание таблицы маршрутизации, на основе обмена информацией об изменениях в топологии сети с другими маршрутизаторами; коммутация – перенаправление пакетов с входного интерфейса маршрутизатора на выходной интерфейс в зависимости от таблицы маршрутизации.

Все маршрутизаторы должны иметь локальные таблицы маршрутизации. Они используются при передаче информации, для определения наилучшего пути от источника к пункту назначения. Таблица маршрутизации содержит следующие записи: механизм, по которому был получен маршрут; мети или подсети назначения; административное расстояние; метрика маршрута; адрес интерфейса маршрутизатора расположенного на расстоянии одной пересылки через которого доступна сеть получатель; время присутствия маршрута в таблице; выходной интерфейс маршрутизатора, через который доступна сеть получатель.

Для выбора маршрутов полученных от разных протоколов маршрутизации используется концепция административного расстояния (AD). Малые значения величины административного расстояния предпочтительнее.

Каждый протокол маршрутизации, для определения лучшего маршрута к некоторой сети назначения использует значение метрики, предпочтительным

будет меньшее значение. Метрики могут быть вычислены на основе одной или нескольких характеристик. Наиболее часто в алгоритмах маршрутизации используются следующие параметры: ширина полосы пропускания, представляет собой средство оценки объема информации, который может быть передан по каналу связи; задержка – промежуток времени, необходимый для перемещения пакета по каждому из каналов связи от отправителя к получателю. Задержка зависит от пропускной способности промежуточных каналов, размера очередей в портах маршрутизаторов, загрузки сети и физического расстояния; загрузка – средняя загруженность канала связи в единицу времени; надежность – относительное количество ошибок на канале связи; количество переходов – количество маршрутизаторов, которые должен пройти пакет, прежде чем он достигнет пункта назначения; стоимость – значение назначенное администратором.

К пункту назначения может существовать множество путей, и все они могут отображаться в таблице маршрутизации. Многие протоколы маршрутизации поддерживают механизм балансировки нагрузки, при котором в таблицу маршрутизации могут быть записаны несколько возможных маршрутов к узлу получателю, и передача трафика будет осуществляться по каждому из маршрутов.

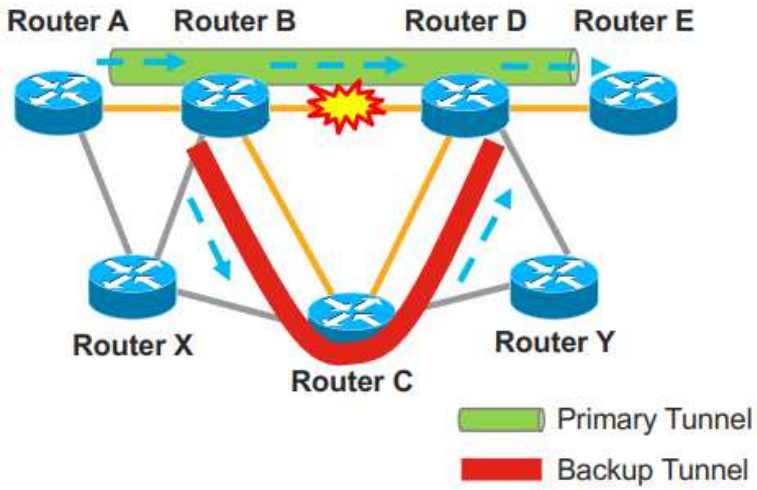

Рисунок 2. — Резервирование маршрута

Одной из основных задач маршрутизаторов является построение таблицы маршрутизации на основе данных полученных от протоколов маршрутизации и настройках введенных вручную. Выбор маршрута для занесения в таблицу маршрутизации должен основываться на следующих критериях:

1) Доступность IP адреса перехода. Процесс маршрутизации заключается в последовательной передачи трафика от отправителя к получателю. Маршрутизатор должен знать IP адрес следующего маршрутизатора в цепочки передачи трафика.

2) Метрика маршрута. Если переход возможен, то протокол маршрутизации выбирает наилучший возможный маршрут передачи. Критерием выбора маршрута является минимальная метрика маршрута.

3) Префикс. Маршрутизатор рассматривает длину префикса (маска подсети), если имеется несколько маршрутов до сети получателя, но с разными прификсами, то в таблицу маршрутизации заносятся все маршруты. В качестве маршрута по которому будет отправлен трафик, выбирается маршрут с наибольшим совпадением префикса сети, это действует принцип наибольшего совпадения маршрута.

4) Административное расстояние маршрута. Если маршрутизатор имеет более одного маршрута до получателя, критерием выбора для занесения в таблицу маршрутизации является минимальное административное расстояние.

После создания таблицы маршрутизации маршрутизатор должен поддерживать ее точное соответствие реальной топологии сети. Поддержка таблиц маршрутизации осуществляется либо администратором сети вручную, либо с помощью динамических протоколов маршрутизации. Точность отображения маршрутов в таблице, является ключевым фактором для обеспечения пересылки данных к получателю.

1.4 Протоколы маршрутизации внутреннего шлюза и их алгоритмы.

К ним относятся любой протокол маршрутизации, используемый исключительно внутри автономной системы. Каждый IGP протокол

представляет один домен маршрутизации внутри AS. При использовании протоколов динамической маршрутизации, администратор сети конфигурирует выбранный протокол на каждом маршрутизаторе в сети. После этого маршрутизаторы начинают обмен информацией об известных им сетях и их состояний. Причем маршрутизаторы обмениваются информацией только с теми маршрутизаторами, где запущен тот же протокол динамической маршрутизации. Когда происходит изменение топологии сети, информация об этих изменениях автоматически распространяется по всем маршрутизаторам, и каждый маршрутизатор вносит необходимые изменения в свою таблицу маршрутизации.

Для распространения информации о сетях между маршрутизаторами, протокол маршрутизации определяет набор правил: каким образом распространяются обновления маршрутов; какая информация содержится в обновлениях; как часто рассылаются обновления; каким образом выполняется поиск получателей обновлений.

Протоколы маршрутизации на основе дистанционно-векторного алгоритма (пример RIP).

Между соседними маршрутизаторами происходит периодическая пересылка копий таблиц маршрутизации друг друга. Маршрутизатор получив от соседа таблицу маршрутизации, добавляет значение вектора расстояния, количества переходов, это увеличивает результирующий вектор расстояния. Этот алгоритм не предоставляет маршрутизаторам точную топологию всей сети, поскольку каждому маршрутизатору известны только соседние с ним маршрутизаторы.

Применение дистанционно-векторной маршрутизации накладывает жесткие ограничения по диаметру сети передачи данных. Это максимальное расстояние измеряется числом пересылок от отправителя к получателю.

Сходимость достигается, когда все маршрутизаторы внутри домена маршрутизации имеют согласованную информацию о доступных маршрутах.

Дистанционно-векторные протоколы отличаются медленной сходимостью, и поэтому подвержены возникновению петель маршрутизации.

Время, которое требуется, для того чтобы все маршрутизаторы обработали обновление маршрутной информации и обновили свои таблицы маршрутизации, называется временем сходимости. Данные маршрутизаторами не будут передаваться до тех пор, пока все таблицы маршрутизации не будут полностью обновлены.

Протоколы маршрутизации на основе учета состояния канала (пример OSPF).

Маршрутизаторы обмениваются сообщениями о состоянии канала (LSA). Эти объявления представляют собой небольшие пакеты, которые содержат информацию об известных маршрутизатору каналах связи;

База данных топологии (Topological Database). Эта база данных содержит информацию, полученную в сообщениях LSA;

Алгоритм выбора кратчайшего пути (Shortest Path First – SPF). Алгоритм осуществляет вычисления над базой данных топологии сети, результатом чего является построение связующего дерева протокола SPF. При получении каждого пакета LSA, содержащего изменения состояний каналов, алгоритм SPF заново вычисляет наилучшие маршруты и обновляет таблицу маршрутизации [10].

Время сходимости протоколов маршрутизации с учетом состояния каналов связи значительно меньше, чем у дистанционно-векторных протоколов маршрутизации. Это связано с тем, что каждый маршрутизатор в домене маршрутизации имеет информацию о реальной топологии сети и может самостоятельно производить пересчет маршрутов к сетям получателям при получении пакетов LSA с изменениями топологии сети.

Протоколы маршрутизации гибридного типа (пример EIGRP).

Объединяет в себе черты как дистанционно-векторных, так и протоколов с учетом состояния каналов связи.

Для определения наилучших маршрутов используют векторы расстояния с более точными метриками.

Обновление баз данных маршрутизации происходит только при изменении топологии сети.

Обладают быстрой сходимостью.

Используют значительно меньшие объемы оперативной памяти и вычислительные ресурсы маршрутизаторов.

1.5 Технологии расширяющие возможности традиционной маршрутизации.

1.5.1 IP SLA и Embedded Event Manager (EEM)

Технология Cisco IOS IP SLA (Service Level Agreements), расшифровывается как, соглашения об уровне обслуживания. С ее помощью можно организовать мониторинг состояния сети и контролировать уровень качественных характеристик сети. Эта технология позволяет:

- Сформировать нужный тест, задать ему необходимые параметры;
- Запустить тест на выполнение;
- Можно вывести результаты теста с помощью командной строки;
- Результаты тестов сохраняются и доступ к ним можно получить по протоколу SNMP;
- Можно настроить отправку SNMP trap и syslog сообщений, информирующих о неудовлетворительных и удовлетворительных результатах тестов;
- Можно сконфигурировать маршрутизатор Cisco, так чтобы он принимал решения о маршрутизации на основе результатов тестов.

Применяя эту технологию, мы получим дополнительную возможность, повысить качество работы СПД. Можно привести примером, следующую ситуацию, когда трафик передается от филиала в центральное подразделение, по основному каналу. В качестве протокола маршрутизации выступает

протокол OSPF. Тогда в стандартной ситуации перевод трафика на резервный канал произойдет, только если соседство на основном канале будет разорвано. Но если вдруг на основном канале появились ошибки, приводящие к потери пакетов, это может быть связано с ухудшением физического состояния кабеля или транспортного оборудования. Небольшие потери есть, но при этом OSPF соседи опрашивают друг друга, и трафик не переходи на качественный резервный канал, а некоторые приложения уже не могут стабильно работать с таким уровнем качества. В такой ситуации, настроенный мониторинг IP SLA, может зафиксировать ухудшение качества на основном канале, а с помощью механизма обработки событий автоматически внести изменения в таблицу маршрутизации, и временно перевести трафик на стабильный резервный канал.

EEM (Embedded Event Manager) – встроенный в Cisco IOS обработчик событий, позиционируется как средство самодиагностики и устранения проблем самим маршрутизатором. События могут быть самыми разными от высокой загрузки CPU и памяти, отключения интерфейса до высокой температуры в корпусе маршрутизатора. Наличие IP SLA тестов расширяет возможности EEM, так как тесты могут дать маршрутизатору представление не только о том, что происходит непосредственно с ним, но и в сети.

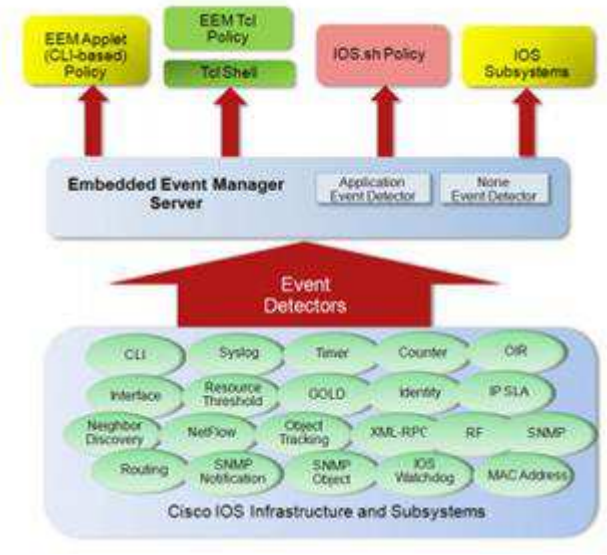

Рисунок 3. — Архитектура EEM

Результаты тестов записываются в SNMP переменные и могут генерироваться syslog сообщения, EEM же, в свою очередь спроектирован так, что может реагировать именно на такие события. Случилось событие, тогда запускается подготовленный для этого случая сценарий, выполняется какое-то действие. В итоге, применение этих технологий позволяет в некоторых ситуациях минимизировать время простоя сети и повысить стабильность функционирования [4].

1.5.2 Policy Base Routing (PBR).

PBR - маршрутизация на основе политик. Эта технология реализует механизм пересылки пакетов данных, основанный на политике, которая представляет набор правил, сформированный администратором сети. С ее помощью можно получить более гибкий механизм для обработки пакетов на маршрутизаторах, который будет дополнять существующий механизм, работающий по правилам классических протоколов маршрутизации.

В стандартном случае, когда пакет приходит на маршрутизатор, в него нужно заглянуть и на основе поля "адрес назначения", принять решение, в какой интерфейс отправить пакет далее по маршруту, согласно данным таблицы маршрутизации. Механизм PBR позволяет администраторам сети определить свои правила, по которым будет осуществляться маршрутизация пакетов [5].

Примеры задач, которые PBR может решить: Маршрутизировать трафик по любому признаку, который можно указать в ACL (IP отправителя и получателя, порты TCP/UDP); Маршрутизировать VoIP трафик через один канал, а весь остальной, через другой; Маршрутизировать трафик пользователей VLAN 10 через один канал, а пользователей VLAN 20 через другой; Маршрутизировать трафик, который генерирует маршрутизатор, по определенному пути.

PBR перехватывает пакеты до стандартной маршрутизации и отправляет пакеты согласно логики настроенных правил. Если для группы пакетов в PBR,

не указано как их маршрутизировать, то они будут отправлены по стандартным правилам маршрутизации.

Основной объект с помощью которого настраивается PBR это Route-map (карта маршрутов), она состоит из списка правил. В каждом правиле Route-map два компонента: match - описывает трафик, который должен маршрутизироваться механизмом PBR; set - инструкция, куда перенаправить трафик, отфильтрованный с помощью правил match.

У каждого правила Route-map есть порядковый номер. Когда пакеты проходят сквозь интерфейс, к которому применена PBR, пакеты проверяются по порядку по правилам. Если пакет совпал с описанием в match, то он маршрутизируется по правилу set. Если пакет не совпал с описанием в match, правила проверяются дальше. Если ни в одном правиле совпадения не найдено, то пакет будет маршрутизироваться по стандартной таблице маршрутизации.

Если PBR используется для распределения трафика между различными каналами (например ISP), то трафик нужно не просто отправлять на определенный next-hop, но и проверять, работоспособен ли канал, через который отправляется трафик. Для проверки работоспособности используется комбинация IP SLA и Track [6].

1.5.3 Optimized Edge Routing (OER).

Традиционная маршрутизация не в состоянии учитывать текущее состояние сети с точки зрения производительности. Чтобы это изменить, была разработана технология Optimized Edge Routing (OER), ее новое название — Performance Routing (PfR). В OER выделяются классы трафика (например приложения или подсети). Производительность (комплексное понятие, может включать в себя задержку, пропускную способность, потери и т.п.) каждого класса периодически измеряется и сравнивается с установленными правилами (политиками). По результатам этих сравнений OER выбирает лучший выход из сети для данного класса трафика.

OER может измерять время отклика и доступность каналов в сторону провайдеров, с внешних интерфейсов своих граничных маршрутизаторов (Border Routers). Изменения производительности этих каналов на BR определяются по-префиксно. Если производительность падает ниже заданного значения, то маршрутизация изменяется для повышения производительности. Обычная маршрутизация не в состоянии решить такую задачу, а OER может автоматически определить проблемное состояние и переправить трафик через другой выходной канал.

Механизм OER состоит из пяти шагов:

1) OER Profile Phase. Выбираем какой именно трафик мы будем оптимизировать с точки зрения производительности, поскольку в RIB может быть много всяких маршрутов. Выбор производится с помощью комбинации двух способов. С помощью изучения (learning) потоков трафика, протекающих через устройство, выбираются потоки с наименьшей задержкой или с наивысшей пропускной способностью. В дополнение к (learning) или вместо него, можно сконфигурировать класс трафика вручную.

2) OER Measure Phase. Определившись с классами трафика, нужно определить метрики, характеризующие производительность для каждого из этих классов. Для этого есть два механизма: активный мониторинг и пассивный мониторинг, их можно использовать и оба сразу. Пассивный мониторинг - измерение метрик производительности потока трафика во время его прохождения через устройство. Работает не для всех классов трафика и не для всех устройств и не для всех версий IOS. Активный мониторинг фактически состоит в генерации искусственного трафика для эмуляции активности данного класса. Можно использовать и оба типа мониторинга сразу. Пассивный может обнаруживать выход производительности класса трафика из допустимых границ, а активный — для поиска альтернативного пути, если таковой имеется.

3) OER Apply Policy Phase. После сбора метрик производительности для данного класса, OER сравнивает эти результаты с набором граничных значений для каждой метрики. Если какая-то метрика, а значит и политика, выходит за

граничные значения - происходит событие Out-of-Policy (OOP). Данные сравниваются двумя способами: либо как отклонение от среднего, либо как выход за границу. Возможно и то, и другое сразу. В OER существует два вида политик. Политики классов трафика (traffic class policies) - создаются для префиксов или для приложений. Политики линков (link policies) - создаются для выходов за границу сети. Оба типа политик определяют критерии для генерации события OOP. Политики применяются глобально (для всех классов трафика) или локально (только для некоторых классов). В случае множества политик, метрик производительности, способов назначения этих политик классам, существует механизм разрешения конфликтов между политиками. Это делается с помощью механизма приоритетов.

4) OER Control Phase. В этой фазе OER, еще ее называют «фаза усиления» (enforce phase), трафик контролируется для увеличения производительности. Способ этого контроля зависит от способа задания класса трафика. Если класс трафика задан только с использованием префикса - будет скорректирована информация о достижимости префикса. Если класс трафика задан приложением, т.е. префиксом и дополнительными условиями, OER уже не сможет использовать обычный протокол маршрутизации и здесь уже на помощь придет PBR.

5) OER Verify Phase. В этой фазе, если класс трафика вышел за границы, предусмотренные политикой (OOP), OER начинает вмешиваться с целью повлиять на трафик этого класса. После вмешательства OER удостоверяется, что оптимизируемый трафик использует тот (gateway), который нужен. Если после этого трафику лучше не стало, то OER отменит изменения и повторит перечисленные фазы сначала.

Компоненты сети под управлением OER:

OER Master Controller (MC). Маршрутизатор, координирующий работу OER по всей сети. Может выполнять только эту функцию, может так же быть пограничным роутером (BR). Master наблюдает за исходящим трафиком с помощью пассивного или активного мониторинга и применяет к этим потокам

имеющиеся политики для оптимизации маршрутизации, являясь по сути центром управления для всех (BR).

OER Border Router (BR). Граничный маршрутизатор с одним или несколькими линками к провайдерам. Именно на нем все изменения, принятые MC, внедряются в жизнь. BR тоже участвует в мониторинге, сообщая данные MC. BR может быть одновременно и MC.

OER-Managed Network Interfaces. То, чем управляет OER. Сеть под управлением OER должна иметь как минимум два исходящих интерфейса для трафика, текущего наружу. На каждом BR так же должен быть хотя бы один интерфейс, достижимый из внутренней сети, чтобы его можно было пометить как «internal» для пассивного мониторинга. И есть еще локальный интерфейс (local) для взаимодействия между MC и BR [7].

Очевидно что механизм работы этой технологии не прост. Но он является новой ступенью развития интеллектуальной маршрутизации. Он позволяет добавить автоматизацию в процесс управления передачей трафика, способствует увеличению надежности и отказоустойчивости в сетях с избыточной топологией.

1.6 SDN, технология автоматизации процесса управления СПД.

Можно выделить следующие проблемы современных компьютерных сетей. Научно-технические проблемы - сегодня невозможно контролировать и надежно предвидеть поведение таких сложных объектов, как глобальные компьютерные сети. Экономические - сети дороги, сложны и требуют для своего обслуживания высококвалифицированных специалистов. Проблемы развития - в архитектуре современных сетей имеются существенные барьеры для экспериментирования и создания новых сервисов.

Ответом на кризис компьютерных сетей стало появление принципиально нового подхода к их построению - программно-конфигурируемые сети (SDN). В SDN уровни управления сетью и передачи данных, разделяются за счет

переноса функций управления (маршрутизаторами, коммутаторами и т. п.) в приложения, работающие на отдельном сервере (контроллере).

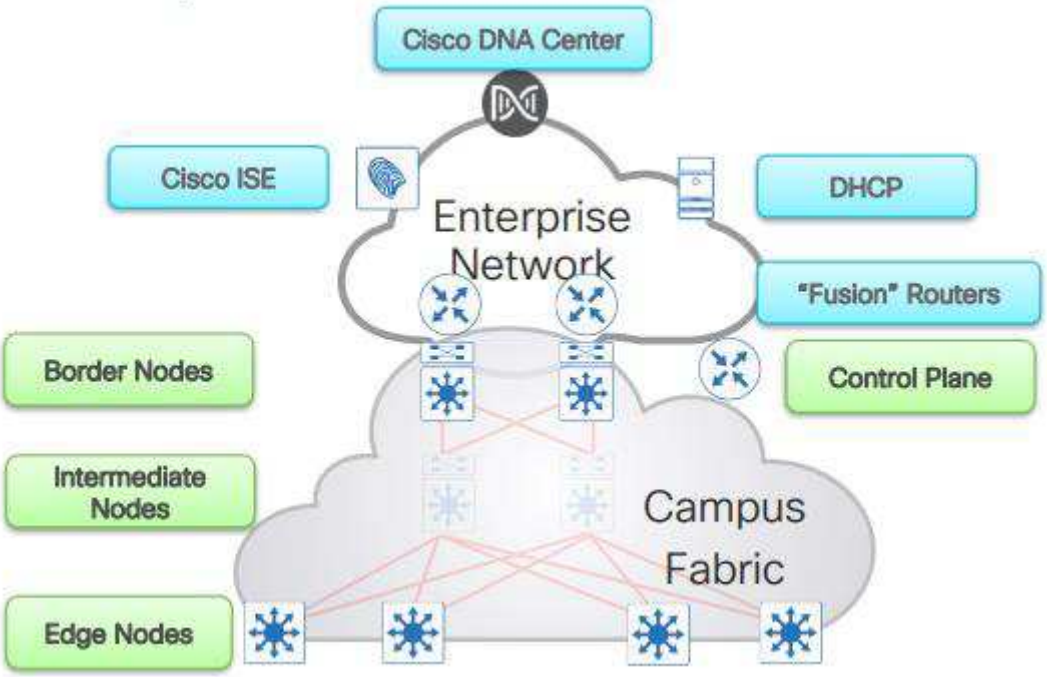

Рисунок 4. — Архитектура SDN

Основные идеи SDN: Разделение процессов передачи и управления данными; Единый, унифицированный, независящий от поставщика интерфейс между уровнем управления и уровнем передачи данных; Логически централизованное управление сетью, осуществляемое с помощью контроллера с установленной сетевой операционной системой и реализованными поверх сетевыми приложениями; Виртуализация физических ресурсов сети.

В архитектуре SDN можно выделить три уровня:

1) Инфраструктурный уровень, предоставляющий набор сетевых устройств (коммутаторов и каналов передачи данных);

2) Уровень управления, включающий в себя сетевую операционную систему, которая обеспечивает приложениям сетевые сервисы и программный интерфейс для управления сетевыми устройствами и сетью;

3) Уровень сетевых приложений для гибкого и эффективного управления сетью.

Наиболее перспективным и активно развивающимся стандартом для SDN является OpenFlow - открытый стандарт, в котором описываются требования, предъявляемые к коммутатору, поддерживающему протокол OpenFlow для удаленного управления.

Согласно спецификации стандарта OpenFlow, взаимодействие контроллера с коммутатором осуществляется посредством протокола OpenFlow - каждый коммутатор должен содержать одну или более таблиц потоков (flow tables), групповую таблицу (group table) и поддерживать канал (OpenFlow channel) для связи с удаленным контроллером - сервером. Спецификация не регламентирует архитектуру контроллера и API для его приложений. Каждая таблица потоков в коммутаторе содержит набор записей (flow entries) о потоках или правила. Каждая такая запись состоит из полей-признаков (match fields), счетчиков (counters) и набора инструкций (instructions).

Механизм работы коммутатора OpenFlow достаточно прост. Когда на коммутатор приходит пакет, в таблицах потоков, ищется правило, у которого поле признаков соответствует заголовку пакета. При наличии совпадения, над пакетом выполняются преобразования, определяемые набором инструкций, указанных в найденном правиле. Если нужного правила в таблице не обнаружено, то пакет инкапсулируется и отправляется контроллеру, который формирует соответствующее правило для пакетов данного типа и устанавливает его на коммутаторе, либо пакет может быть сброшен. Управление данными в OpenFlow осуществляется не на уровне отдельных пакетов, а на уровне их потоков. Правило в коммутаторе OpenFlow устанавливается с участием контроллера только для первого пакета, а затем все остальные пакеты потока его используют.

Логически-централизованное управление данными в сети предполагает вынесение всех функций управления сетью на отдельный физический сервер, называемый контроллером, который находится в ведении администратора сети. Контроллер может управлять как одним, так и несколькими OpenFlow-коммутаторами и содержит сетевую операционную систему (СОС),

предоставляющую сетевые сервисы по низкоуровневому управлению сетью, сегментами сети и состоянием сетевых элементов, а также приложения, осуществляющие высокоуровневое управление сетью и потоками данных. В каждом контроллере имеется хотя бы одно приложение, которое управляет коммутаторами, соединенными с этим контроллером, и формирует представление о топологии физической сети, находящейся под управлением контроллера, тем самым централизуя управление. Представление топологии сети включает в себя топологию коммутаторов, расположение пользователей и хостов и других элементов и сервисов сети. Представление также включает в себя привязку между именами и адресами, поэтому одной из важнейших задач, решаемых СОС, является постоянный мониторинг сети.

Одна из идей, активно развиваемая в рамках SDN,- это виртуализация сетей с целью более эффективного использования сетевых ресурсов. Под виртуализацией сети понимается изоляция сетевого трафика - группирование (мультиплексирование) нескольких потоков данных с различными характеристиками в рамках одной логической сети, которая может разделять единую физическую сеть с другими логическими сетями или сетевыми срезами (network slices). Каждый такой срез может использовать свою адресацию, свои алгоритмы маршрутизации, управления качеством сервисов и т.д.

Виртуализация сети позволяет: повысить эффективность распределения сетевых ресурсов и сбалансировать нагрузку на них; изолировать потоки разных пользователей и приложений в рамках одной физической сети; администраторам разных срезов использовать свои политики маршрутизации и правила управления потоками данных; проводить эксперименты в сети, используя реальную физическую сетевую инфраструктуру; использовать в каждом срезе только те сервисы, которые необходимы конкретным приложениям.

Программные средства SDN позволяют администраторам добавлять новую функциональность к уже имеющейся сетевой архитектуре. На централизованном контроллере SDN системный администратор может

наблюдать всю сеть в едином представлении, за счет чего повышаются удобство управления, безопасность и упрощается выполнение ряда других задач. Программно-конфигурируемые сети открывают большие возможности для промышленности и бизнеса, позволяя решать задачи повышения пропускной способности каналов, упрощения управления сетью, перераспределения нагрузки, повышения масштабируемости сети [8].

1.7 Выводы, плюсы и минусы рассмотренных технологий.

Основными требованиями, предъявляемыми к корпоративной сети передачи данных, являются высокая скорость доступа к общим ресурсам и надежность работы, без перерывов 24 часа в день, 7 дней в неделю. Эти требования формируются запросами пользователей СПД, для возможности выполнять свои повседневные задачи. При этом нужно учитывать что СПД, как живой организм не находится в одном состоянии, а развивается, растет число сетевых узлов, добавляются новые сервисы. Этот рост, в итоге приводит к модернизации СПД, физической замене устаревших узлов и реорганизации логической структуры, переконфигурированию сетевых протоколов. Это сложные задачи для реализации, с учетом того, что структурные изменения нужно проводить на работающей сети, и перерывы связи должны быть минимальны. Этим я хочу подчеркнуть, что задачи логической конфигурации СПД, в частности настройка протоколов маршрутизации, для больших сетей, достаточно сложный процесс.

Наиболее популярными внутренними протоколами маршрутизации (IGP) являются, протокол EIGRP, разработанный компанией Cisco и протокол OSPF. Протокол EIGRP имеет смысл разворачивать на сети построенной исключительно на маршрутизаторах Cisco, при ограничение в 255 маршрутизаторов. Это два основных минуса, сужающие область применения протокола. А в целом протокол работает быстро, надежно и предоставляет механизм балансировки трафика. Протокол OSPF, поддерживается всеми основными производителями сетевого оборудования. Может успешно

применяться в огромных сетях, для увеличения стабильности работы имеет механизм сегментации общего домена на отдельные зоны. Но при сложной топологии сети с большим количеством узлов, потребует от маршрутизаторов для хранения и обработки данных, повышенного расхода ресурсов процессора и памяти. Особенно это актуально для маршрутизаторов формирующих магистраль (или зону 0).

Перечисленные классические протоколы, применяются повсеместно, и демонстрируют вполне успешные результаты в идеальных условиях. А вот в реальной жизни, топологии могут быть далеки от оптимальных. Для обеспечения отказоустойчивости нужно строить сеть с избыточной топологией, когда удаленный объект имеет несколько каналов связи. Хорошо если пропускная способность основного и резервного каналов одинакова и достаточно широка, но так бывает не всегда. Значит при переходе на резервный канал, быстрое движение трафика может быть ограничено узким каналом. И тут классический протокол маршрутизации уже не выручит. Это лишь один из примеров, когда реальная топология плохо реализуется классической маршрутизацией. В этом случае на помощь приходят дополнительные протоколы и технологии, такие как IP SLA, PBR, OER и др. Рассматривая каждый случай индивидуально, с их помощью можно внести в процесс управления движением трафика элемент автоматизации. Когда при возникновении прогнозируемого события, СПД самостоятельно принимает верное решение, выбирает лучший путь для маршрутизации трафика, без вмешательства администратора. Минусом такого подхода является требование высокой квалификации персонала выполняющего настройку СПД, отсюда возможно возникновение ошибок, причем ошибки могут проявить себя не сразу, а в процессе эксплуатации СПД, т.к человек не машина, и просчитать все шаги наперед не сможет.

Совершенно отличающийся подход, для решения проблемы автоматизации СПД, предлагает технология SDN. Тут процесс ручной конфигурации сетевого оборудования сведен к минимуму. Выделенный сервер

- контроллер, сетевая операционная система и специализированные управляющие приложения, автономно выполняют функции управления элементами сетевой инфраструктуры и потоками данных в сети. На мой взгляд, большую перспективу SDN может получить при строительстве новых СПД, так как перевод существующей рабочей СПД на концепцию SDN, процесс финансово очень затратный, трудоемкий и сложный, но возможный.

Рассмотрим рисунок №5, на нем представлена топология корпоративной СПД, имеющая два выхода в сеть Интернет. Основной канал строится через провайдера ISP-1, и резервный канал через провайдера ISP-2. Тут возможно два варианта использования этих каналов для передачи данных. Первый вариант, когда для работы задействован только один основной канал, резервный будет простаивать и вступит в работу в случае, когда на основном канале возникла авария на физическом уровне. Этот вариант решается с помощью традиционных протоколов маршрутизации. Во втором варианте, мы можем одновременно направлять трафик по обоим каналам. Это позволяет разделять сети, выбирать для них лучший маршрут, и в итоге организовать возможность управлять движением трафика. Для простой топологии эта задача решается с помощью традиционных протоколов маршрутизации и технологии PBR. Но если немного усложнить структуру СПД, рисунок №6, то решение по организации управления маршрутами тоже усложняется.

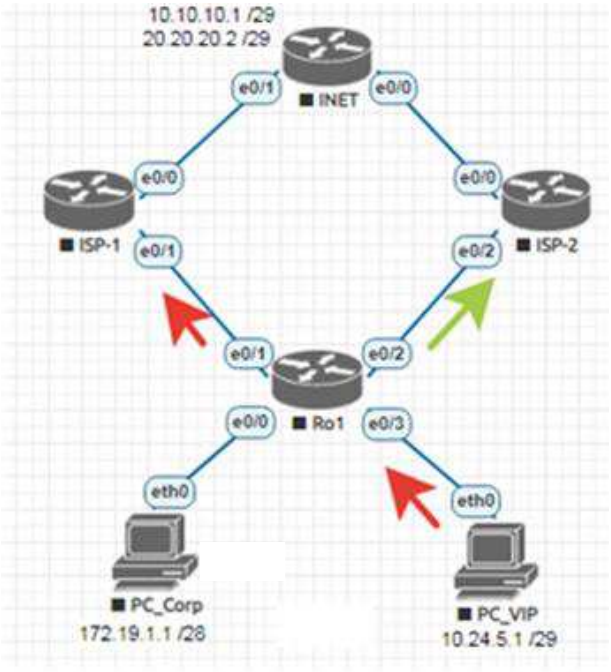

Рисунок 5. — Топология сети

Можно поставить задачу, организовать возможность управлять движением трафика, когда некоторые сети будут ходить через канал ISP-1, а другие через канал ISP-2. Пусть для пользователей VIP-1 и VIP-2 выход в интернет строится через провайдера ISP-1 (канал A). Если этот канал станет неработоспособным, например возникли проблемы с сетевым узлом или авария на транспортном уровне, или пропускная способность канала очень снизилась, и это привело к росту ошибок и потерь пакетов на канале, в этом случае трафик пользователей должен изменить маршрут и желательно без вмешательства администратора сети, тогда для выхода в интернет в нашем примере будем использовать канал C (провайдер ISP-2).

Такую задачу довольно трудно решить применяя только технологию PBR и традиционную маршрутизацию. Здесь нужна автоматизация процесса отслеживания состояния каналов провайдеров, перестроение правил PBR для разделения сетей и построения маршрутов. Технология SDN построена на принципе автоматизации процессов сбора данных, анализа и самостоятельного решения по выбору оптимального маршрута. Эту задачу, а также более сложные задачи, SDN может успешно решать, но применение этой технологии для уже функционирующей сети ограничено, так как связано с большими

финансовыми вложениями, требующими обновления телекоммуникационного оборудования и изменения принципов функционирования сети.

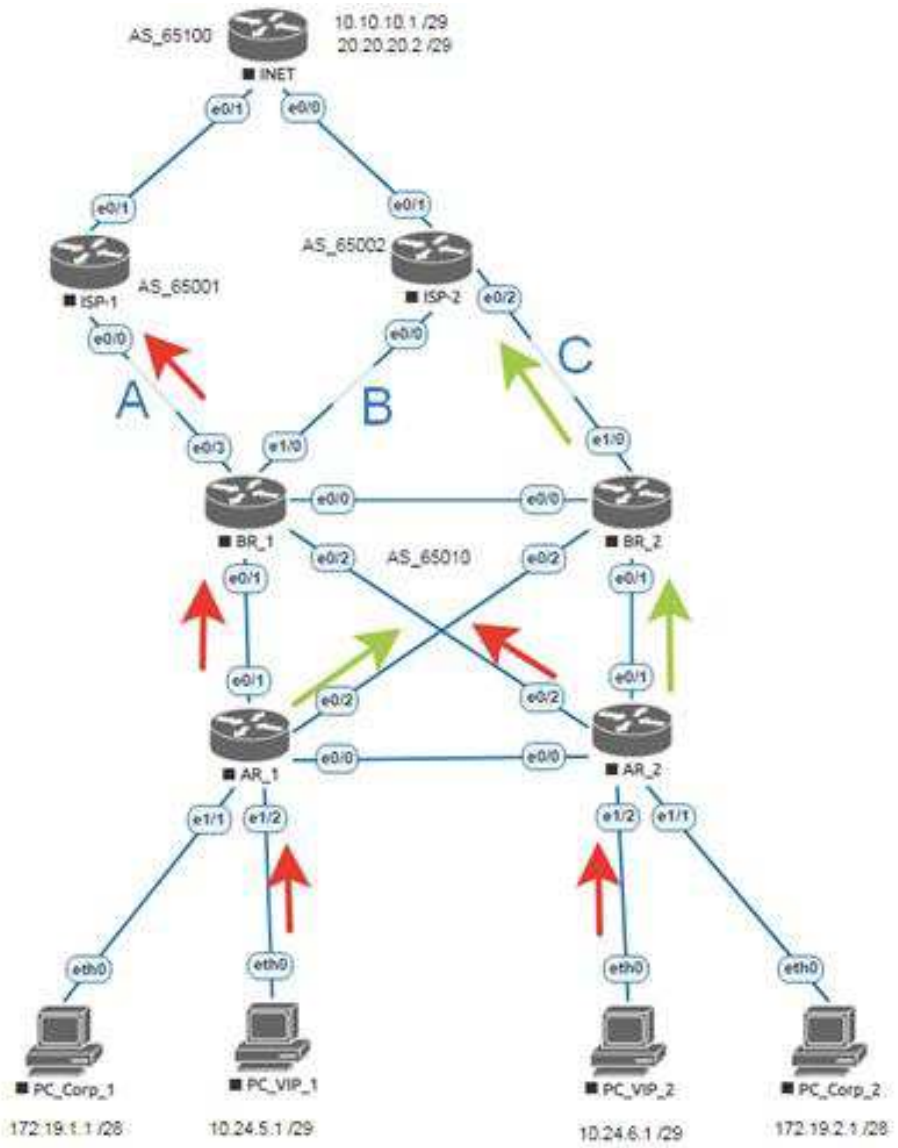

Рисунок 6. — Топология сети

Я хочу предложить альтернативный вариант для решения этой задачи, добавить автоматизации в процесс управления выбором лучшего маршрута, с учетом изменяющейся ситуации на СПД. Я планирую провести работу по разработке протокола, позволяющего между маршрутизаторами в пределах корпоративной СПД, автоматически строить и изменять политики влияющие на выбор лучшего маршрута, таким образом автоматически вносить коррективы в маршрутизацию трафика.

2 Проектирование метода

2.1 Практика настройки PBR на маршрутизаторах.

Для выполнения настройки технологии PBR, нужно пройти следующие шаги: 1) Выделить нужный трафик, например с помощью ACL. Если мы можем выделить интересующий нас трафик с помощью расширенного ACL, мы сможем его маршрутизировать, как нам будет угодно. 2) Создать карту политик, в ней для выбранного трафика назначить правила маршрутизации. 3) Назначить карту политик входному интерфейсу.

На примере топологии, представленной на рисунке №6, пройдем шаги по настройки PBR. Согласно исходным данным, наша AS_65010 имеет выход в сеть Интернет (10.10.10.0/29 и 20.20.20.0/29), через два граничных маршрутизатора BR1 и BR2, которые подключены к двум провайдерам ISP-1 и ISP-2, через три канала A, B и C. Граничный маршрутизатор BR1, имеет канал A, в сторону провайдера ISP-1 (входящим маршрутам назначается низкий приоритет *LocalPreference* 50), канал B ведет к провайдеру ISP-2 (для входящих маршрутов назначим *LP* 500). Граничный маршрутизатор BR2, имеет один канал C, к провайдеру ISP-2 (*LP* назначим 100).

В результате, с помощью протокола BGP установлена приоритезация для трех внешних каналов. Исходящий трафик сети AS_65010 следуя в Интернет, выберет канал B, с маршрутизатора BR1 через провайдера ISP-2. Поэтому маршрут от сети VIP-1 и VIP-2 в сторону Интернет будет строиться по схеме BR1 → ISP-2 (канал B) → Inet. Это подтверждает трассировка маршрута от сетей VIP-1 и VIP-2 до адресов 10.10.10.1 и 20.20.20.2.

```
1  10.24.5.6        - AR1 (gateway VIP-1)
2  192.168.14.1     - BR1
3  192.168.200.2    - ISP-2 (канал B)
4  *10.0.0.1        - INET

1  10.24.6.6        - AR2 (gateway VIP-2)
2  192.168.13.1     - BR1
3  192.168.200.2    - ISP-2 (канал B)
4  *10.0.0.1        - INET
```

Теперь внесем изменения в маршрут движения трафика для сетей VIP-1 и VIP-2 с помощью технологии PBR. Сделаем так, чтобы пользователи двигались

по схеме BR2 → ISP-2 (канал C) → Inet, новый маршрут отмечен зелеными стрелками. Для этого выполним следующие настройки:

1. AR1 является маршрутизатором доступа для сети 10.24.5.0/29. Создаем карту политик RM_PBR_VIP_1 для этой сети и назначим адресом NEXT_HOP адрес маршрутизатора BR2.

2. AR2 является маршрутизатором доступа для сети 10.24.6.0/29. Создаем карту политик RM_PBR_VIP_1 для этой сети и назначим адресом NEXT_HOP адрес маршрутизатора BR2.

3. На BR2 для сетей 10.24.5.0/29 и 10.24.6.0/29, создаем карту политик RM_PBR_VIP_1 и назначим адресом NEXT_HOP адрес маршрутизатора ISP-2. Снова проверяем трассировку маршрута от сетей VIP до адресов Интернет. Видим, что теперь маршрут строится через канал C.

```
1  10.24.5.6        - AR1 (gateway VIP-1)
2  192.168.24.1     - BR2
3  192.168.200.6    - ISP-2 (канал C)
4  *10.0.0.1        - INET

1  10.24.6.6        - AR2 (gateway VIP-2)
2  192.168.23.1     - BR2
3  192.168.200.6    - ISP-2 (канал C)
4  *10.0.0.1        - INET
```

Далее предположим, что канал C стал неработоспособен, тогда согласно настроенной маршрутизации трафик от сетей VIP-1 и VIP-2 до адресов Интернет пойдет по схеме BR1 → ISP-2 (канал B) → Inet. Мы можем вручную внести изменения в настройки PBR для изменения схемы движения, например так BR1 → ISP-1 (канал A) → Inet, новый маршрут отмечен красными стрелками.

Для этого выполним следующие настройки:

1. AR1, для RM_PBR_VIP_1, удаляем адрес NEXT_HOP ведущий к BR2, назначим адресом NEXT-HOP адрес маршрутизатора BR1.

2. AR2, для RM_PBR_VIP_1, удаляем адрес NEXT_HOP ведущий к BR2, назначим адресом NEXT-HOP адрес маршрутизатора BR1.

3. BR2, для входящих интерфейсов 0/1, 0/2, удалить привязку к RM_PBR_VIP_1.

4. На BR1 для сетей 10.24.5.0/29 и 10.24.6.0/29, создаем карту политик RM_PBR_VIP_1 и назначим адресом NEXT_HOP адрес маршрутизатора ISP-1. Тестируем новые настройки и видим что маршрут перестроился, трафик идет через канал А.

```
1   10.24.5.6          - AR1 (gateway VIP-1)
2   192.168.14.1       - BR1
3   192.168.100.2      - ISP-1 (канал А)
4   *10.0.0.5          - INET

1   10.24.6.6          - AR2 (gateway VIP-2)
2   192.168.13.1       - BR1
3   192.168.100.2      - ISP-1 (канал А)
4   *10.0.0.5          - INET
```

Если связь на канале С восстановится, то для перевода сетей VIP-1, VIP-2 обратно на канал С, придется вручную изменять правила PBR на маршрутизаторах AR1, AR2, BR1, BR2. Очевиден вывод, в текущей реализации технологии PBR есть немало ручной настройки, это значит что с увеличением масштаба, трудоемкость будет только расти. Можно предположить, что такие процессы, как мониторинг канала С, любые изменения топологии, а также настройка карты политики на перечисленных маршрутизаторах если автоматизировать, то это сделает PBR более управляемой и гибкой.

Предлагается использовать механизм PBR, но при этом заменить большую часть ручной настройки. Формировать список заданных сетей с помощью ACL, только на одном роутере. Далее распространять ACL на все роутеры сети как служебную маршрутную информацию, и автоматически создавать правила политик. В случае если на сети происходят изменения топологии, каналы связи могут терять и восстанавливать активность, эти изменения должны учитываться и автоматически подстраивать карты политик, вычисляя новый путь для маршрутизации трафика.

2.2 Проектирование метода iPBR.

Выделим функции метода, которые нужно автоматизировать:

- Наблюдать за состоянием каналов связи между маршрутизаторами, каналов с провайдерами. Возможность отслеживать изменения топологии и принимать нужные меры, повысит гибкость работы протокола.
- Распространять маршрутную информацию между маршрутизаторами, чтобы каждый обладал актуальными данными. Необходимое условие для получения состояния сходимости сети.
- Создавать правила политик, а в случае изменения топологии сети иметь возможность автоматически внести поправки в правила политик. Это расширит возможности управления сетевым трафиком.

Путей для решения этих задач несколько. Современные протоколы маршрутизации обладают свойством расширения. Например, OSPF позволяет создать и использовать новый тип сообщения LSA-x, и с его помощью распространить между маршрутизаторами требуемую информацию. Или протокол BGP, он использует ручную настройку для взаимодействия с соседом, это готовый механизм организации и поддержания соседских отношений, а если его расширить новым блоком (*address-family*), то можно решить задачу распространения среди всех маршрутизаторов информации для построения правил карт политик. Есть третий путь, не использовать существующий протокол маршрутизации, а проектировать новый. Это более сложная и объемная задача. Пусть новый протокол будет намного проще существующих, но все равно придется подробно описать его структуру и функционал. Плюсом использования протоколов OSPF или BGP, для выполнения описанных задач автоматизации, является уже готовое решение типовых процессов, реализованное функционалом этих протоколов, остается лишь научить их передавать новую информацию для построения карт политик. Минусом будет, необходимость развертывания на реальной сети протокола OSPF или BGP. Это хоть и популярные протоколы, но не во всех случаях их используют. Задача проектирования нового протокола имеет дополнительную сложность. Чтобы экспериментально проверить работу разработанного протокола потребуется выполнить программирование всех его функций, что само по себе является

задачей повышенной сложности и не укладывается в рамки данной работы. Поэтому для автоматизации основных функций на базе технологии PBR, я использую функционал протокола BGP, с новым блоком ADDRESS-FAMILY. Новый метод будет называться iPBR (Intellectual Policy Based Routing).

2.2.1 Основные принципы работы метода iPBR.

Метод iPBR использует дистанционно-векторный принцип при распространении маршрутной информации.

ACL-список, будет содержать определенные сети адресов, к которым нужно применить особенный подход при маршрутизации. Чтобы метод iPBR мог отличить его от других ACL-списков, предлагается использовать в качестве имени iACL_x, где (x) это порядковый номер списка.

Данный iACL-список настраивается на граничном маршрутизаторе. Он называется граничный, потому что этот маршрутизатор для сетей из iACL-списка будет крайним в нашей автономной системе, после него следует либо точка назначения, либо трафик уйдет в другую автономную систему, например к провайдеру Интернет.

В методе iPBR вводится понятие END-HOP, это та самая точка назначения, куда будет строиться маршрут от сетей iACL-списка. Если обратится к рисунку №8, END-HOP будет адрес линковочной сети, находящийся на граничном маршрутизаторе, это адрес со стороны провайдера 192.168.100.2. Как будет показано далее, использование параметра END-HOP поможет вычислить лучший маршрут и назначить в карту политики параметр NEXT-HOP.

Маршрутизаторы выстраивают отношения соседства. Интерфейс будет в состояние STATE LISTEN если соседний маршрутизатор активен, и с ним можно обмениваться служебными сообщениями. В частности передавать и принимать информацию iACL_x и END-HOP необходимую для настройки карты политик. Интерфейс, через который направляется трафик в сторону END-HOP, устанавливается в состояние STATE FORWARD.

Маршрутизаторы обмениваются маршрутной информацией друг с другом. Маршрутизатор получив от соседа данные iACL_x и END-HOP обработает их, и программно сформирует iACL-лист. Используя данные таблицы маршрутизации вычислит лучший путь до END-HOP и на основании этого выберет адрес NEXT-HOP. Этих данных будет достаточно, чтобы автоматически сформировать карту политики. В результате данные для маршрутизации трафика сетей ACL-списка будут помещены в таблицу политик.

После того как все маршрутизаторы домена iPBR имеют актуальную информацию об ACL-списках, выбраны лучшие маршруты и сформированы правила политики. Остается только следить за состоянием каналов, быстро реагировать на изменения и вносить корректировку в правила политик.

2.2.2 Блок ADDRESS-FAMILY, для передачи маршрутной информации.

UPDATE - сообщение, в котором маршрутизатор передает своему соседу маршрутную информацию, которая имеет актуальную версию ACL-списка, адрес точки назначения END-HOP и значение метрики.

Маршрутизатор получивший это сообщение, использует содержащуюся в нем информацию, если она актуальна, для настройки таблицы политик. Данные этой таблицы позволяют применить к адресам находящимся в списке iACL особые правила маршрутизации.

Распространение маршрутной информации происходит с помощью протокола BGP, для этого создается новый блок ADDRESS-FAMILY, это отдельная группа которая будет передавать данные iPBR. В блоке ADDRESS-FAMILY нужно указать адреса соседей, которым будет передаваться маршрутная информация. Структура пакета BGP имеет секцию NLRI, она подходит для передачи параметров iPBR.

AFI - Address Family Identifiers. Поле сообщения BGP UPDATE, описывающее протокол сетевого уровня, адреса которого передаются в секции

NLRI. SAFI сообщает дополнительную информацию о типе NLRI. Например для AFI 1 (IP) SAFI может быть 1 (Unicast), 2 (Multicast), 128 (MPLS BGP VPN). SAFI является подтипом, характеризующим AFI.

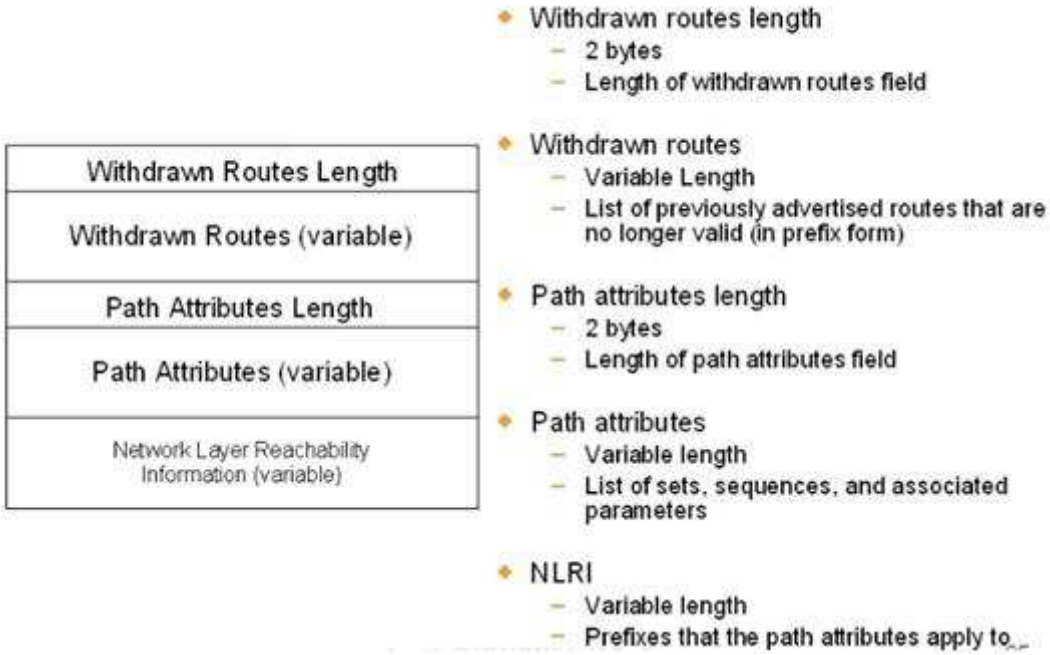

Рисунок 7. — Формат пакета UPDATE

Сообщение BGP обновления включает последовательность атрибутов пути, это характеристики описывающие маршрут. Атрибуты пути состоят из следующих полей: тип атрибута, состоит из двух полей, поле флага и поле кода типа атрибута; длина атрибута; значение атрибута [9].

Опциональные атрибуты не обязательно поддерживаются всеми реализациями протокола BGP, это может быть уникальный атрибут, используемый только в одной реализации протокола. В том случае, когда он поддерживается, он может быть передан BGP соседям.

Применяемый подход предполагает отделение основных параметров сеанса работы маршрутизатора от специфических параметров, присущих определенному ADDRESS FAMILY. Входные и выходные правила маршрутизации могут отличаться для различных AF. BGP маршрутизатор может быть настроен как отражатель маршрутов для одного AF или сразу нескольких AF. Префиксы могут независимо поступать из любых источников внутри каждого AF. Группы взаимодействующих узлов будут обслуживаться

внутри соответствующего AF, так как это касается генерации сообщений UPDATE [11].

Команды для семейства адресов AF, к этому типу могут быть отнесены два набора команд: Глобальные команды семейств адресов, это те команды, которые не зависят от конфигурации соседних узлов и влияют на работу по протоколу BGP определенного AF. Префиксы могут поступать от различных источников для AF, относящегося к этой категории. Вторая группа специфические команды семейств адресов для соседних узлов/группы узлов. Эти команды позволяют настроить правила работы с соседними узлом (узлами) или в группе взаимодействующих узлов с помощью списков преобразования, списков префиксов или карт маршрутов. Соседние узлы можно также конфигурировать как клиентов отражателя маршрутов или как дополнительных членов группы узлов. При этом соседние узлы должны быть явным образом "активированы" в целях разрешения обмена префиксами в рамках MBGP.

Чтобы разрешить использование определенного AF между соседними узлами, на BGP маршрутизаторе нужно задать команду ACTIVATE или перейти в режим конфигурации ADDRESS FAMILY. При этом соседние BGP узлы автоматически активируются для работы с IPv4. Для всех остальных AF соседние узлы следует активировать явным образом [16].

2.2.3 Использование механизма организации соседских отношений.

В качестве транспортного протокола, BGP использует протокол TCP и порт 179, обеспечивающий надежную доставку. Поэтому протокол BGP предполагает, что его связь с соседом является надежной, и нет необходимости выполнять повторную посылку пакетов или реализовывать механизм восстановления ошибок. Два маршрутизатора, использующие протокол BGP устанавливают между собой TCP соединение, для этого они обмениваются сообщениями чтобы открыть и подтвердить параметры соединения. Протокол BGP рассылает сообщения KEEPALIVE, подобные Hello сообщениям, рассылаемым протоколами OSPF и EIGRP.

После того как между двумя маршрутизаторами установлено TCP соединение, каждый маршрутизатор отправляет соседу сообщение OPEN. Сосед получив такое сообщение отвечает на него сообщением KEEPALIVE, подтверждающим что сообщение OPEN получено. После этого соединение BGP считается установленным, и теперь можно обмениваться маршрутной информацией с помощью сообщений UPDATE. Пакеты KEEPALIVE посылаются для подтверждения существования соединения между BGP соседями, а пакеты NOTIFICATION посылаются в ответ на ошибки или специальные условия. При получении сообщения NOTIFICATION, соединение BGP закрывается немедленно. Сообщение NOTIFICATION включает код ошибки, а также данные соответствующие ошибке. Обмен сообщениями UPDATE, KEEPALIVE и NOTIFICATION происходит только когда соединение находится в состоянии ESTABLISHED. Сообщение KEEPALIVE состоит из заголовка и имеет длину 19 байт, по умолчанию рассылается каждые 60 секунд. Длина других сообщений может быть от 19 до 4096 байт. По умолчанию время задержки составляет 180 секунд. Состояние соседства двух маршрутизаторов BGP, может принимать следующие варианты:

- IDLE - соединение отсутствует;
- CONNECT - соединение;
- ACTIVE - активный;
- OPEN SENT - отправка сообщения OPEN;
- OPEN CONFIRM - подтверждение получения сообщения OPEN;
- ESTABLISHED - рабочий режим, соединение BGP между соседями установлено.

2.2.4 Механизм проверки состояния канала с ISP.

В нашем примере, каждый из маршрутизаторов BR, независимо и регулярно проводит тест состояния внешнего канала. В качестве теста можно предложить, отправлять каждые 10 секунд пакеты ICMP на публичный адрес, например 8.8.8.8, через свой внешний канал. С помощью технологии IP SLA

можно отслеживать процент потерь или задержку и на основе этого делать вывод о состоянии внешнего канала. Если ответа нет 20 секунд, то фиксируется событие, внешний канал считается потерянным, в этом случае маршрутизатор BR оповещает своих соседей из блока AF, а они распространяют информацию далее по всему домену iPBR, с целью внести корректировку в таблицу политик, чтоб данный END-HOP теперь не использовать.

Мониторинг потерянного канала с ISP не прекращается, нужно раз в 60 секунд отправлять пакеты ICMP на тестовый публичный адрес 8.8.8.8. После того как связь появится, маршрутизатор должен выполнить тест, подтверждающий надежность внешнего канала. Раз в 60 секунд, маршрутизатор отправляет 1000 icmp пакетов на адрес 8.8.8.8. Подобный тест выполняется подряд пять раз. В результате если после 300 секунд состояние внешнего канал показало удовлетворительный результат, суммарно потерь не более 5 пакетов и задержка менее 70 мс, то запускается процедура возврата трафика через этот маршрутизатор, формируется служебное сообщение и рассылается всем соседям домена iPBR, для изменения таблицы политик, так как теперь данный END-HOP можно использовать.

2.2.5 Порядок настройки метода iPBR.

Нужно вручную настроить ACL-списки и карты политики только на граничных маршрутизаторах. На остальных маршрутизаторах нужно: Активировать iPBR, задать ему номер процесса. Задать уникальный идентификатор маршрутизатора. Включить логирование событий.

Всю остальную работу, метод iPBR выполнит самостоятельно.

2.3 Пример настройки метода iPBR.

На рисунке №8 представлена топология тестовой сети. Используя эту схему выполним настройку iPBR. Данные для конфигурации маршрутизаторов возьмем из таблиц №1 и №2.

1. На граничных маршрутизаторах BR1 и BR2 в ручную настроены списки iACL

iACL-1 описывает трафик сети 10.1.1.0/24

iACL-2 описывает трафик сети 10.2.2.0/24

2. На граничном маршрутизаторе BR1 создана карта политики, она описывает условия:

для iACL-1 адрес NEXT-HOP 192.168.100.2 с метрикой 10

для iACL-2 адрес NEXT-HOP 192.168.100.2 с метрикой 100

3. На граничном маршрутизаторе BR2 создана карта политики, она описывает условия:

для iACL-1 адрес NEXT-HOP 192.168.200.6 с метрикой 100

для iACL-2 адрес NEXT-HOP 192.168.200.6 с метрикой 10

Таблица №1 (ip план каналов связи)

1	BR1 - ISP1	192.168.100.0 /30	BR1 +1	ISP1 +2
2	BR2 - ISP2	192.168.200.4 /30	BR2 +1	ISP2 +2
3	BR1 - BR2	10.10.12.0 /30	BR1 +1	BR2 +2
4	BR1 - TR3	10.10.13.0 /30	BR1 +1	TR3 +2
5	BR1 - TR4	10.10.14.0 /30	BR1 +1	TR4 +2
6	BR2 - TR3	10.10.23.0 /30	BR2 +1	TR3+2
7	BR2 - TR4	10.10.24.0 /30	BR2 +1	TR4 +2
8	TR3 - TR4	10.10.34.0 /30	TR3 +1	TR4 +2
9	TR3 - AR5	10.10.35.0 /30	TR3 +1	AR5 +2
10	TR3 - AR6	10.10.36.0 /30	TR3 +1	AR6 +2
11	TR3 - AR7	10.10.37.0 /30	TR3 +1	AR7 +2
12	TR4 - AR5	10.10.45.0 /30	TR4 +1	AR5 +2
13	TR4 - AR6	10.10.46.0 /30	TR4 +1	AR6 +2
14	TR4 - AR7	10.10.47.0 /30	TR4 +1	AR7 +2

Таблица №2 (ip план подключенных сетей)

1	AR5	10.1.1.0 /25	gi0/3	iACL_1
2	AR5	172.19.1.0 /26	gi0/4	
3	AR5	10.124.1.0 /25	gi0/5	
4	AR6	10.1.1.128 /25	gi0/3	iACL_1
5	AR6	10.2.2.0 /25	gi0/4	iACL_2
6	AR6	10.124.2.0 /25	gi0/5	
7	AR7	10.2.2.128 /25	gi0/3	iACL_2
8	AR7	172.19.3.0 /26	gi0/4	
9	AR7	10.124.3.0 /25	gi0/5	

4. BR1 должен отправить своим соседям (BR2, TR3 и TR4) маршрутную информацию, с помощью которой они создадут свои карты политики, маршрутная информация включает параметры:

сети из списка iACL-1, адрес END-HOP 192.168.100.2, метрика 10, версия 1

сети из списка iACL-2, адрес END-HOP 192.168.100.2, метрика 100, версия 1

5. BR2 должен отправить своим соседям (BR1, TR3 и TR4) маршрутную информацию, для настройки карт политик:

сети из списка iACL-1, адрес END-HOP 192.168.200.6, метрика 100, версия 1

сети из списка iACL-2, адрес END-HOP 192.168.200.6, метрика 10, версия 1

На граничном маршрутизаторе BR есть точка выхода, называется END-HOP, в нашем примере это стык с ISP, точек выхода END-HOP для трафика описанного в iACL-x, может быть несколько, выбор основной и резервной делается с помощью вручную заданной метрики, чем меньше значение метрики, тем выше ее приоритет.

В таблице описывающей правила политик для трафика iACL-x, будет две записи, первая запись с меньшей метрикой будет иметь статус активной, именно через указанный интерфейс будет ходить трафик для данного iACL-x, вторая запись имеет большую метрику и статус резервной.

Начиная с BR, маршрутная информация (МИ) автоматически распространяется среди всех маршрутизаторов домена iPBR.

Распространяемая МИ содержит номер актуальной версии, в результате все маршрутизаторы должны иметь одинаковую версию МИ, так обеспечивается сходимость на сети.

МИ передается между маршрутизаторами с помощью протокола BGP, для этого создается новый блок ADDRESS-FAMILY. Силами протокол BGP выполняется процедура определения и поддержания соседских отношений.

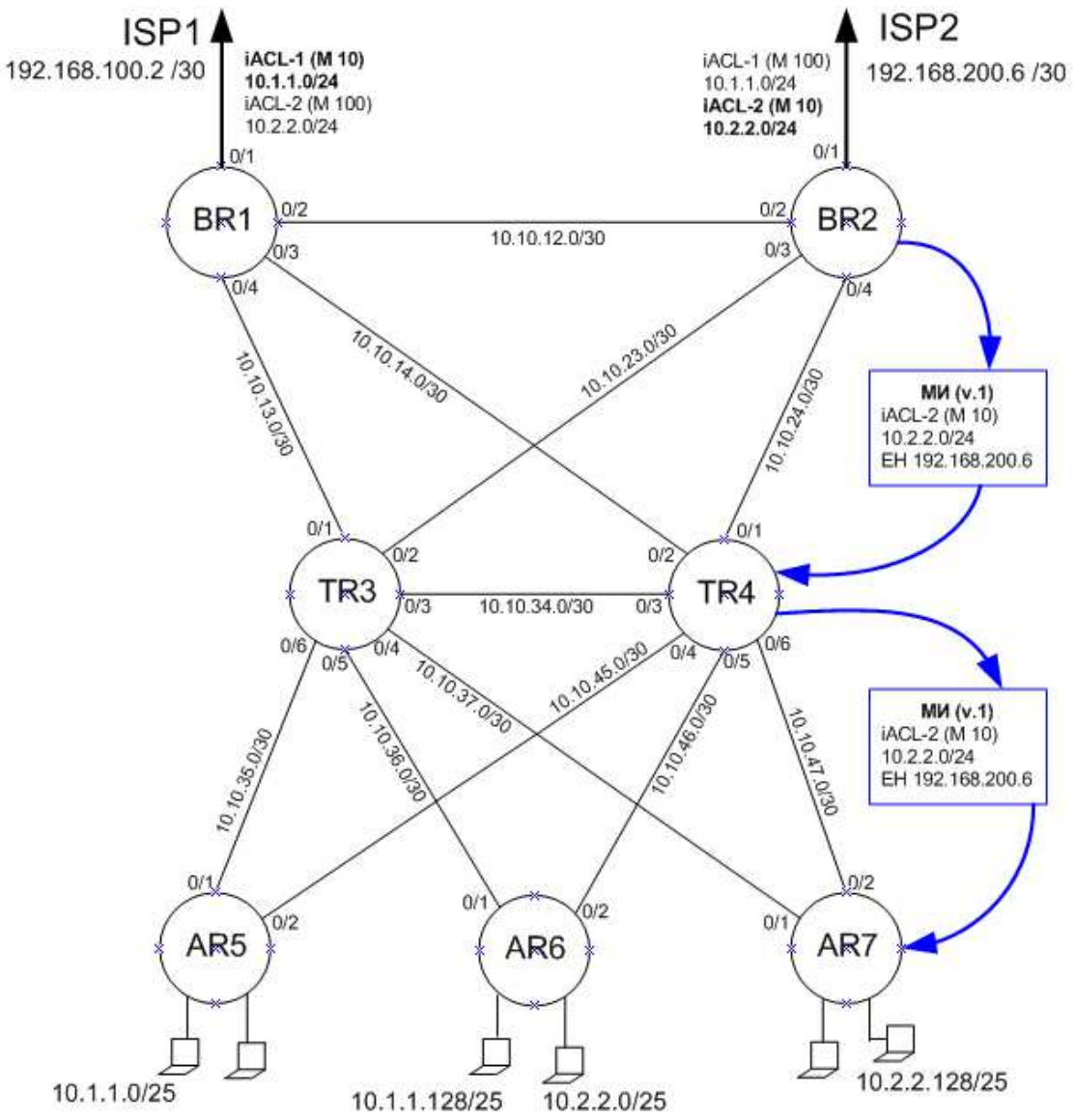

Рисунок 8. — Топология сети

2.3.1 Обмен маршрутной информацией.

Маршрутизатор получив пакет с МИ, должен проверить ее версию, если номер версии текущий или более старый, то такой пакет удаляется. Если номер версии свежий, то нужно обновить у себя данные, возможно что произошли изменения с составом сетей описанных в iACL-x или изменился статус доступности адреса END-HOP. После обработки такой пакет нужно отправить своим соседям, для обновления данных во всем домене.

Таблица соседства маршрутизатора BR1

№	Address	Interface	State	Holdtime	Uptime	END-HOP
1.	192.168.100.2	gi0/1	forward	5	01:38:42	192.168.100.2
2.	10.10.12.2	gi0/2	listen	10	02:40:16	-------
3.	10.10.14.2	gi0/3	listen	8	01:15:11	-------
4.	10.10.13.2	gi0/4	listen	14	02:22:25	-------

Распространение маршрутной информации (МИ) на уровне BR-TR:

1. Маршрутизатор BR2 получив МИ от BR1, вносит изменения в свою таблицу политик, трафик для iACL-1 с метрикой 10 нужно отправлять в порт gi0/2 в сторону BR1.

2. Маршрутизатор BR1 получив МИ от BR2, вносит изменения в свою таблицу политик, трафик для iACL-2 с метрикой 10 нужно отправлять в порт gi0/2 в сторону BR2.

3. Маршрутизатор TR3 получив МИ от BR1 и BR2 вносит изменения в свою таблицу политик, трафик для iACL-1 с метрикой 10 нужно отправлять в порт gi0/1 в сто, трафик для iACL-2 с метрикой 10 нужно отправлять в порт gi0/2 в сторону BR2.

4. Маршрутизатор TR4 получив МИ от BR1 и BR2 вносит изменения в свою таблицу политик, трафик для iACL-1 с метрикой 10 нужно отправлять в порт gi0/2 в сторону BR1, трафик для iACL-2 с метрикой 10 нужно отправлять в порт gi0/1 в сторону BR2.

Таблица соседства маршрутизатора BR2

№	Address	Interface	State	Holdtime	Uptime	END-HOP
1.	192.168.200.6	gi0/1	forward	9	02:35:52	192.168.200.6
2.	10.10.12.1	gi0/2	listen	18	01:31:25	-------
3.	10.10.23.2	gi0/3	listen	12	01:25:33	-------
4.	10.10.24.2	gi0/4	listen	15	02:32:23	-------

Распространение маршрутной информации (МИ) на уровне TR-AR:

1. Маршрутизатор AR5 получив МИ от TR3 и TR4 внесет изменения в свою таблицу политик, трафик для iACL-1 с метрикой 10 нужно отправлять в

порт gi0/1 в сторону TR3, трафик для iACL-2 (с метрикой 10 нужно отправлять в порт gi0/2 в сторону TR4.

2. Маршрутизатор AR6 получив МИ от TR3 и TR4 внесет изменения в свою таблицу политик, трафик для iACL-1 с метрикой 10 нужно отправлять в порт gi0/1 в сторону TR3, трафик для iACL-2 с метрикой 10 нужно отправлять в порт gi0/2 в сторону TR4.

3. Маршрутизатор AR7 получив МИ от TR3 и TR4 внесет изменения в свою таблицу политик, трафик для iACL-1 с метрикой 10 нужно отправлять в порт gi0/1 в сторону TR3, трафик для iACL-2 с метрикой 10 нужно отправлять в порт gi0/2 в сторону TR4.

Таблица соседства маршрутизатора TR3

№	Address	Interface	State	Holdtime	Uptime	END-HOP
1.	10.10.13.1	gi0/1	forward	10	02:35:52	192.168.100.2
2.	10.10.23.1	gi0/2	forward	3	01:31:25	192.168.200.6
3.	10.10.34.2	gi0/3	listen	12	01:21:23	-------
4.	10.10.37.2	gi0/4	listen	9	01:27:24	-------
5.	10.10.36.2	gi0/5	listen	17	01:29:25	-------
6.	10.10.35.2	gi0/6	listen	5	01:25:26	-------

Таблица соседства маршрутизатора TR4

№	Address	Interface	State	Holdtime	Uptime	END-HOP
1.	10.10.24.1	gi0/1	forward	6	02:45:52	192.168.200.6
2.	10.10.14.1	gi0/2	forward	7	01:21:25	192.168.100.2
3.	10.10.34.1	gi0/3	listen	12	01:33:52	-------
4.	10.10.45.2	gi0/4	listen	11	02:32:44	-------
5.	10.10.46.2	gi0/5	listen	14	02:30:33	-------
6.	10.10.47.2	gi0/6	listen	10	02:39:13	-------

Таблица соседства маршрутизатора AR5

№	Address	Interface	State	Holdtime	Uptime	END-HOP
1.	10.10.35.1	gi0/1	forward	19	02:35:52	192.168.100.2
2.	10.10.45.1	gi0/2	forward	11	01:31:25	192.168.200.6

Таблица соседства маршрутизатора AR6

№	Address	Interface	State	Holdtime	Uptime	END-HOP
1.	10.10.36.1	gi0/1	forward	12	01:52:12	192.168.100.2
2.	10.10.46.1	gi0/2	forward	17	01:51:55	192.168.200.6

Таблица соседства маршрутизатора AR7

№	Address	Interface	State	Holdtime	Uptime	END-HOP
1.	10.10.37.1	gi0/1	forward	5	02:51:12	192.168.100.2
2.	10.10.47.1	gi0/2	forward	8	02:31:45	192.168.200.6

Изменения о составе сетей описанных в iACL-x, можно выполнить только вручную на BR, после внесения изменений этот BR автоматически должен повысить номер версии МИ и разослать ее своим соседям, а те далее по всему домену.

2.3.2 Реакция iPBR при изменении топологии.

Нужно выполнять регулярный тест доступности канала с каждым ISP, для мониторинга работоспособности END-HOP, для этого отправляется пакет ICMP на публичный адрес 8.8.8.8 настроенный статикой через ISP, если пакеты перестают возвращаться, это значит что канал с ISP временно неработоспособен. Информацию об этом событии нужно распространить на все маршрутизаторы домена, версия МИ увеличивается и по домену распространяются данные, что для iACL-x нужно выполнить корректировку настройки RM и таблицы политик, в этом случае маршрутизатор получив пакет с обновленной МИ, для iACL-x в таблице политик меняется статус записи с активной на резервную, и увеличивается значение метрики до максимального 255, при этом статус резервной записи меняется на активный и трафик начинает ходить согласно новому правилу, перестраивается RM.

Мониторинг потерянного канала с ISP не прекращается, и когда пакеты ICMP начнут возвращаться, версию МИ увеличиваем и распространяем данные по домену, меняем настройки RM, в таблице политик для данного iACL-x актуализируются статусы записей, корректируется значение метрики.

Маршрутизатор BR выступает инициатором распространения МИ в следующих случаях, при этом изменения передаются по всему домену: при первоначальном запуске протокола; после ручного изменения состава сетей iACL-x на BR; при потери работоспособности канала с ISP; после восстановления канала с ISP.

Маршрутизаторы AR и TR могут инициировать распространение МИ, при потери или восстановлении активного канала связи, в зависимости от топологии СПД.

Таблица политик маршрутизатора BR1

№	iACL-x	END-HOP	NEXT-HOP	interface	metrica	status	version
1.	iACL-1	192.168.100.2	192.168.100.2	gi0/1	10	active	1
2.	iACL-1	192.168.200.6	10.10.2.2	gi0/2	100	rezerv	1
3.	iACL-2	192.168.100.2	192.168.100.2	gi0/1	100	rezerv	1
4.	iACL-2	192.168.200.6	10.10.2.2	gi0/2	10	active	1

Таблица политик маршрутизатора BR2

№	iACL-x	END-HOP	NEXT-HOP	interface	metrica	status	version
1.	iACL-1	192.168.100.2	10.10.1.1	gi0/2	10	active	1
2.	iACL-1	192.168.200.6	192.168.200.6	gi0/1	100	rezerv	1
3.	iACL-2	192.168.200.6	192.168.200.6	gi0/1	10	active	1
4.	iACL-2	192.168.100.2	10.10.1.1	gi0/2	100	rezerv	1

Таблица политик маршрутизатора TR3

№	iACL-x	END-HOP	NEXT-HOP	interface	metrica	status	version
1.	iACL-1	192.168.100.2	10.10.1.1	gi0/1	10	active	1
2.	iACL-2	192.168.200.6	10.10.2.2	gi0/2	10	active	1
3.	iACL-1	192.168.200.6	10.10.2.2	gi0/2	100	rezerv	1
4.	iACL-2	192.168.100.2	10.10.1.1	gi0/1	100	rezerv	1

Таблица политик маршрутизатора TR4

№	iACL-x	END-HOP	NEXT-HOP	interface	metrica	status	version
1.	iACL-1	192.168.100.2	10.10.1.1	gi0/2	10	active	1
2.	iACL-2	192.168.200.6	10.10.2.2	gi0/1	10	active	1
3.	iACL-1	192.168.200.6	10.10.2.2	gi0/1	100	rezerv	1
4.	iACL-2	192.168.100.2	10.10.1.1	gi0/2	100	rezerv	1

Таблица политик маршрутизатора AR5

№	iACL-x	END-HOP	NEXT-HOP	interface	metrica	status	version

1.	iACL-1	192.168.100.2	10.10.1.1	gi0/1	10	active	1
2.	iACL-1	192.168.200.6	10.10.2.2	gi0/2	100	rezerv	1

Таблица политик маршрутизатора AR6

№	iACL-x	END-HOP	NEXT-HOP	interface	metrica	status	version
1.	iACL-1	192.168.100.2	10.10.1.1	gi0/1	10	active	1
2.	iACL-2	192.168.200.6	10.10.2.2	gi0/2	10	active	1
3.	iACL-1	192.168.200.6	10.10.2.2	gi0/2	100	rezerv	1
4.	iACL-2	192.168.100.2	10.10.1.1	gi0/1	100	rezerv	1

Таблица политик маршрутизатора AR7

№	iACL-x	END-HOP	NEXT-HOP	interface	metrica	status	version
1.	iACL-2	192.168.200.6	10.10.2.2	gi0/2	10	active	1
2.	iACL-2	192.168.100.2	10.10.1.1	gi0/1	100	rezerv	1

На TR3 канал связи в сторону BR1 стал неактивным. Интерфейс Gi0/1, был в состоянии STATE FORWARD, через него выполнялась маршрутизация для сетей из списка iACL_1. Из таблицы соседства этот интерфейс будет исключен, до восстановления связи с маршрутизатором BR1. Если при этом маршрутизатор BR1 в работе и канал с ISP1 активен, то таблицы соседства и политик на маршрутизаторе TR3 поменяют свой вид. Теперь трафик для сетей из списка iACL_1 пойдет через маршрутизатор TR4, на TR3 в таблице соседства интерфейс в сторону TR4 поменяет статус на STATE FORWARD. Выбор в пользу TR4 был выполнен на основе анализа таблицы маршрутизации, так как лучший путь до адреса END-HOP 192.168.100.2, для TR3 теперь строится именно через TR4.

Таблица соседства маршрутизатора TR3

№	Address	Interface	State	Holdtime	Uptime	END-HOP
1.	10.10.23.1	gi0/2	forward	3	02:41:15	192.168.200.6
2.	10.10.34.2	gi0/3	forward	12	02:31:33	192.168.100.2
3.	10.10.37.2	gi0/4	listen	9	02:57:14	-------
4.	10.10.36.2	gi0/5	listen	17	02:39:45	-------
5.	10.10.35.2	gi0/6	listen	5	02:45:46	-------

Таблица политик маршрутизатора TR3

№	iACL-x	END-HOP	NEXT-HOP	interface	metrica	status	version
1.	iACL-1	192.168.100.2	10.10.1.1	gi0/3	10	active	2

2.	iACL-2	192.168.200.6	10.10.2.2	gi0/2	10	active	1
3.	iACL-1	192.168.200.6	10.10.2.2	gi0/2	100	rezerv	1
4.	iACL-2	192.168.100.2	10.10.1.1	gi0/3	100	rezerv	2

Изменение состояния основного линка на TR3, будет интересно для соседей AR5, AR6, AR7. Поэтому маршрутизатор TR3 сформирует служебное сообщение, с обновленной версией маршрутной информации для списка iACL_1 и END-HOP 192.168.100.2

Маршрутизаторы AR5, AR6, AR7 получив это сообщение, внесут изменения в таблицу политик. Согласно таблицы маршрутизации для построения лучшего пути до END-HOP 192.168.100.2 нужно выбрать новый интерфейс Gi0/2, ведущий к TR4.

Таблица соседства маршрутизатора AR5

№	Address	Interface	State	Holdtime	Uptime	END-HOP
1.	10.10.45.1	gi0/2	forward	19	02:35:52	192.168.100.2
2.	10.10.45.1	gi0/2	forward	11	01:31:25	192.168.200.6

Таблица политик маршрутизатора AR5

№	iACL-x	END-HOP	NEXT-HOP	interface	metrica	status	version
1.	iACL-1	192.168.100.2	10.10.1.1	gi0/2	10	active	2
2.	iACL-1	192.168.200.6	10.10.2.2	gi0/2	100	rezerv	1

Таблица соседства маршрутизатора AR6

№	Address	Interface	State	Holdtime	Uptime	END-HOP
1.	10.10.46.1	gi0/2	forward	12	01:52:12	192.168.100.2
2.	10.10.46.1	gi0/2	forward	17	01:51:55	192.168.200.6

Таблица политик маршрутизатора AR6

№	iACL-x	END-HOP	NEXT-HOP	interface	metrica	status	version
1.	iACL-1	192.168.100.2	10.10.1.1	gi0/2	10	active	2
2.	iACL-2	192.168.200.6	10.10.2.2	gi0/2	10	active	1
3.	iACL-1	192.168.200.6	10.10.2.2	gi0/2	100	rezerv	1
4.	iACL-2	192.168.100.2	10.10.1.1	gi0/2	100	rezerv	2

Таблица соседства маршрутизатора AR7

№	Address	Interface	State	Holdtime	Uptime	END-HOP
1.	10.10.47.1	gi0/2	forward	5	02:51:12	192.168.100.2

2.	10.10.47.1	gi0/2	forward	8	02:31:45	192.168.200.6

Таблица политик маршрутизатора AR7

№	iACL-x	END-HOP	NEXT-HOP	interface	metrica	status	version
1.	iACL-2	192.168.200.6	10.10.2.2	gi0/2	10	active	1
2.	iACL-2	192.168.100.2	10.10.1.1	gi0/2	100	rezerv	2

Следующий вариант, когда на TR3 канал связи в сторону TR4 стал неактивным. Этот интерфейс Gi0/3, был в состоянии STATE LISTEN. Интерфейс будет удален из таблицы соседства. В связи с тем что, состояние соседства со стороны TR3 было STATE LISTEN, он никому не будет рассылать служебное сообщения, чтобы не дублировать информацию.

На TR3 канал связи в сторону AR5 стал неактивным. Этот интерфейс Gi0/6, был в состоянии STATE LISTEN. Интерфейс будет удален из таблицы соседства. В связи с тем что, состояние соседства со стороны TR3 было STATE LISTEN, он никому не будет рассылать сообщения, чтобы не дублировать информацию. Подобное поведение повторяется для каналов связи с AR6 и AR7.

На AR5 канал связи в сторону TR3 стал неактивным. Этот интерфейс Gi0/1, был в состоянии STATE FORWARD, для сетей из списка iACL_1. Интерфейс будет удален из таблицы соседства. Используя данные таблицы маршрутизации, в качестве нового интерфейса для форвардинга трафика выбирается Gi0/2, так как лучшая метрика пути до END-HOP 192.168.100.2, строится через роутер TR4, в соответствии с этим меняется таблица соседства и политик. Далее сообщение об изменении топологии не передается, потому что у маршрутизатора AR5 больше нет соседей в состоянии STATE LISTEN, которым могла бы быть интересна информация о потере линка с TR3.

Таблица соседства маршрутизатора AR5

№	Address	Interface	State	Holdtime	Uptime	END-HOP
1.	10.10.45.1	gi0/2	forward	19	02:35:52	192.168.100.2
2.	10.10.45.1	gi0/2	forward	11	01:31:25	192.168.200.6

Таблица политик маршрутизатора AR5

№	iACL-x	END-HOP	NEXT-HOP	interface	metrica	status	version
1.	iACL-1	192.168.100.2	10.10.1.1	gi0/2	10	active	1
2.	iACL-1	192.168.200.6	10.10.2.2	gi0/2	100	rezerv	1

3 Описание реализации метода.

3.1 Описание варианта реализации iPBR.

На данном этапе завершена теоретическая проработка метода iPBR. Для выполнения тестирования его работы, можно выбрать расширенный пакет программ маршрутизации Quagga, который обеспечивает реализацию протоколов маршрутизации, основанных на TCP/IP.

Quagga - пакет программ, реализующих протоколы маршрутизации, основанных на TCP/IP и поддерживает такие протоколы как RIPv2, OSPFv2, OSPFv3, BGP. Quagga использует расширенную программную архитектуру для того, чтобы предоставить качественный механизм маршрутизации [17].

Традиционное программное обеспечение маршрутизации сделано как одна программа, которая обеспечивает все функциональные возможности протокола маршрутизации. Quagga использует несколько другой подход. Каждый протокол маршрутизации обслуживается отдельным демоном, с последующим формированием таблиц маршрутизации. Одновременно работать могут несколько разных демонов в сообществе с управляющим демоном zebra.

Каждый демон имеет свой собственный файл конфигурации и терминальный интерфейс. Когда Вы конфигурируете статический маршрут, это должно быть сделано в файле конфигурации zebra, а при конфигурировании маршрутов BGP - в файле конфигурации bgpd.

Zebra - это программа управления процессом маршрутизации. Она обеспечивает обновления таблицы маршрутизации ядра, поиск интерфейса и распределение маршрутов между различными демонами маршрутизации [19].

Начальные команды конфигурирования:

Установить имя хоста.

Command: hostname hostname {}

Установить пароль на vty. Если пароль не установлен, vty не будет принимать подключения.

Command: password password {}

Установить пароль на режим enable.

Command: enable password password {}

Переход в режим конфигурации.

Command: configure terminal {}

Показывает текущую версию Quagga и информацию по хосту.

Command: show version {}

Установить значение таймаута для VTY.

Command: exec-timeout minute {}

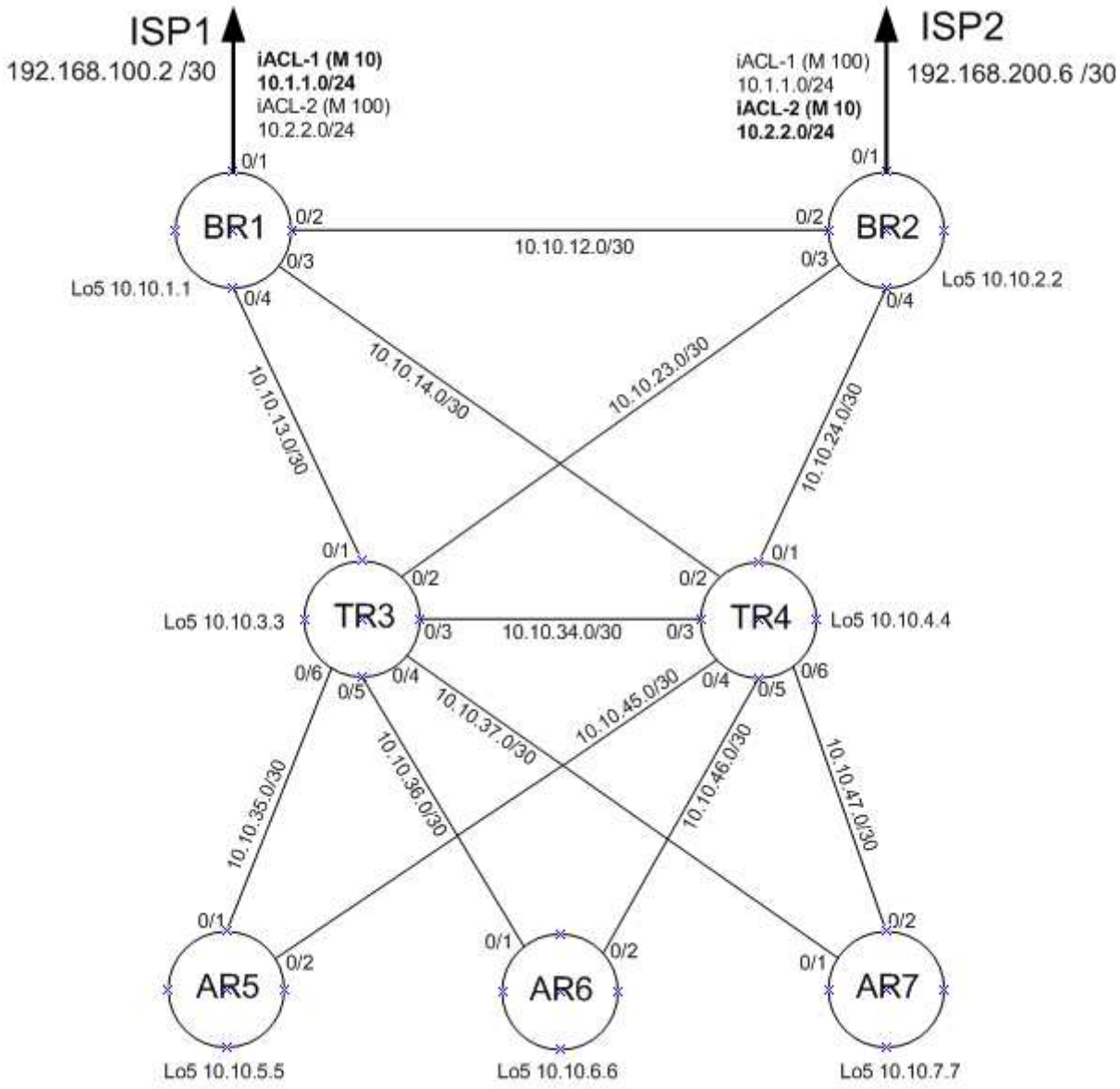

Рисунок 9. — Топология сети

Потребуется построить тестовую сеть на виртуальных машинах под управлением операционной системой Linux Ubuntu. Согласно представленной схеме, сеть будет состоять из семи виртуальных машин. И на каждой будет установлена программа Quagga, которая позволит выполнить настройку протоколов маршрутизации OSPF и BGP. Таким образом мы получим функционирующую распределенную автономную систему. Потребуется добавить еще две виртуальные машины, которые будут играть роль провайдеров Интернет, ISP1 и ISP2.

Далее нужно реализовать с помощью функционала программного комплекса Quagga, возможность передавать маршрутную информацию протокола iPBR, между маршрутизаторами нашей автономной системы.

Полноценное тестирование функционала разработанного метода с помощью программного обеспечения Quagga достаточно трудоемко. Для этого потребуется создать отдельный скриптовый механизм, позволяющий принимать и обрабатывать UPDATE сообщения с данными новой ADDRESS-FAMILY, а далее взаимодействовать с основным модулем Zebra, отвечающим за работу маршрутизатора. Осложняется это тем, что нужно разбираться с кодом многочисленных файлов ПО Quagga.

В текущей ситуации, можно предложить упрощенный прототип реализации метода iPBR, основанный на работе скриптов. Механизм PBR в Linux можно организовать с помощью IPTABLES, тут можно хранить правила для обработки определенного трафика. На данный момент на указанных виртуальных машинах настроено и запущено ПО Quagga, созданы файлы конфигурации протоколов OSPF и BGP, в результате мы имеем связанность и установленные соседские отношения по BGP. Но маршрутизаторы, кроме граничных ничего не знают о политиках маршрутизации. Запускаем скрипт на граничном маршрутизаторе с помощью планировщика задач с интервалом один раз в минуту. Задача скрипта выгрузить из системы набор правил политик маршрутизации, то есть скрипт читает данные из IPTABLES. Эти данные кодируются в стандарт Base64. Теперь эти данные нужно передать соседнему

маршрутизатору, на котором скрипт сможет их декодировать и вставить в IPTABLES, таким образом сформировав правило политики маршрутизации. Отсюда возникает задача передачи этой маршрутной информации. На этом этапе скрипт начинает взаимодействовать с ПО Quagga. С помощью протокола TELNET скрипт может подключиться к демону Quagga. Нужно сформировать сообщение UPDATE, их может потребоваться несколько, для передачи всех правил политик, используя атрибут BGP Extended Community, для этих сообщений будет назначен общий групповой признак. На маршрутизаторе получившем эту маршрутную информацию, скрипт выполнит парсинг данных о правилах политик, далее данные будут декодированы, и в результате мы получим строку для добавления правила в IPTABLES.

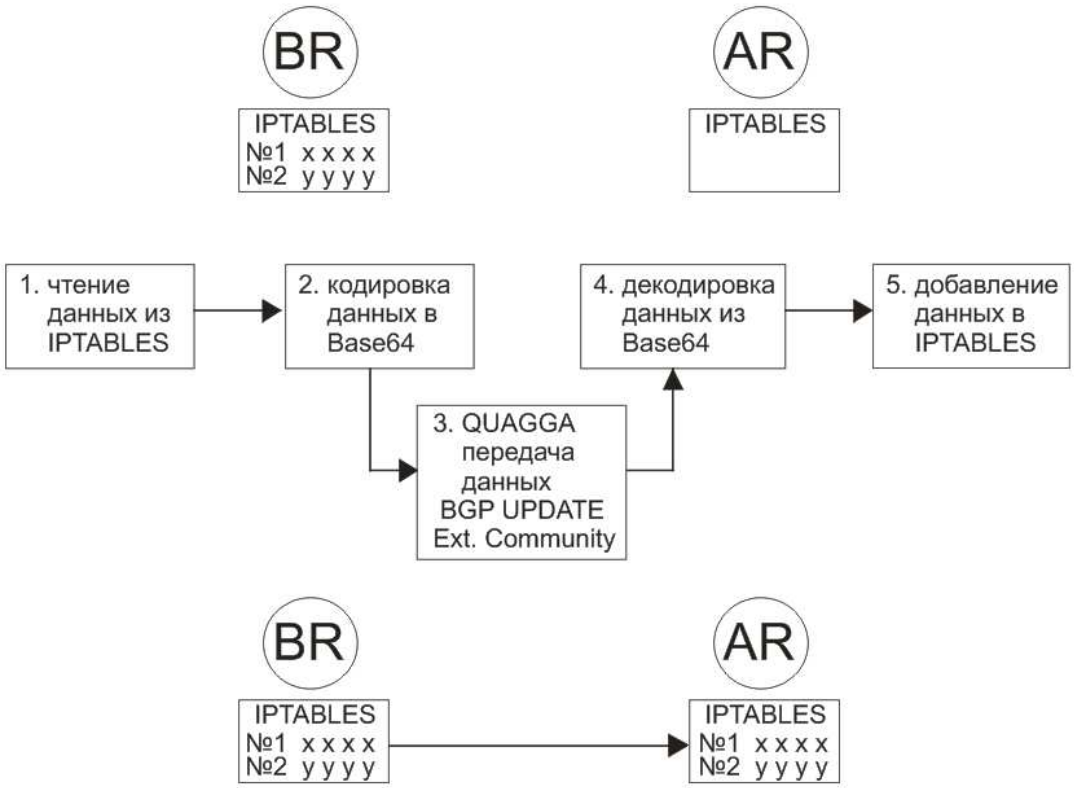

Рисунок 10. — Обмен маршрутной информацией

10.10.1.1 /32	адрес Loopback интерфейса маршрутизатора BR1
10.10.2.2 /32	адрес Loopback интерфейса маршрутизатора BR2
10.10.3.3 /32	адрес Loopback интерфейса маршрутизатора TR3
10.10.4.4 /32	адрес Loopback интерфейса маршрутизатора TR4
10.10.5.5 /32	адрес Loopback интерфейса маршрутизатора AR5
10.10.6.6 /32	адрес Loopback интерфейса маршрутизатора AR6

10.10.7.7 /32 адрес Loopback интерфейса маршрутизатора AR7

На маршрутизаторе BR1 вручную созданы списки доступа ACL и таблица политик RM

```
!
route-map RM_iPBR_iACL-1 permit 10
 match ip address iACL-1
 set ip next-hop 192.168.100.2                адрес ISP1
!
route-map RM_iPBR_iACL-2 permit 10
 match ip address iACL-2
 set ip next-hop 192.168.100.2                адрес ISP1
!
ip access-list standard iACL-1
 permit 10.1.1.0 0.0.0.255
 deny   any
!
ip access-list standard iACL-2
 permit 10.2.2.0 0.0.0.255
 deny   any
!
```

Маршрутизатор BR1 передает своим соседям маршрутную информацию, которая размещается в служебном сообщении BGP-UPDATE в секции NLRI, ADDRESS-FAMILY iPBR

Структура первого UPDATE-сообщения, которое отправляет BR1 своим соседям:

```
!
route-map RM_iPBR_iACL-1 permit 10
  match ip address iACL-1
  set ip next-hop 10.10.1.1                   адрес Loopback интерфейса на BR1
!
ip access-list standard iACL-1
  permit 10.1.1.0 0.0.0.255
  deny   any
!
```

version 1 номер версии маршрутной информации

metrica 10 метрика к адресу END-HOP через BR1 лучше чем через BR2

Данные сообщения в кодировке ASCII

cm91dGUtbWFwIFJNX2lQQlJfaUFDTC0xIHBlcm1pdCAxMAogIG1hdGNoIGlwI
GFkZHJlc3MgaUFDTC0xCiAgc2V0IGlwIG5leHQtaG9wIDEwLjEwLjEuMQohCm
lwIGFjY2Vzcy1saXN0IHN0YW5kYXJkIGlBQ0wtMQogIHBlcm1pdCAxMC4xLjE

uMCAwLjAuMC4yNTUKICBkZW55ICAgYW55CiEKdmVyc2lvbiAxCm1ldHJpY
2EgMTA=

Структура второго UPDATE-сообщения, которое отправляет BR1 своим соседям:

```
!
route-map RM_iPBR_iACL-2 permit 10
  match ip address iACL-2
  set ip next-hop 10.10.1.1                    адрес Loopback интерфейса на BR1
!
 ip access-list standard iACL-2
  permit 10.2.2.0 0.0.0.255
  deny   any
!
version 1            номер версии маршрутной информации
metrica 100          метрика к адресу END-HOP через BR1 хуже чем через BR2
```

Данные сообщения в кодировке ASCII

cm91dGUtbWFwIFJNX2lQQlJfaUFDTC0yIHBlcm1pdCAxMAogIG1hdGNoIGlwI
GFkZHJlc3MgaUFDTC0yCiAgc2V0IGlwIG5leHQtaG9wIDEwLjEwLjEuMQohCi
BpcCBhY2Nlc3MtbGlzdCBzdGFuZGFyZCBpQUNMLTIKICBwZXJtaXQgMTAu
Mi4yLjAgMC4wLjAuMjU1CiAgZGVueSAgIGFueQohCnZlcnNpb24gMQptZXRya
WNhIDEwMA==

На маршрутизаторе BR2 вручную созданы списки доступа ACL и таблица политик RM

```
!
route-map RM_iPBR_iACL-1 permit 10
 match ip address iACL-1
 set ip next-hop 192.168.200.6                 адрес ISP2
!
route-map RM_iPBR_iACL-2 permit 10
 match ip address iACL-2
 set ip next-hop 192.168.200.6                 адрес ISP2
!
ip access-list standard iACL-1
 permit 10.1.1.0 0.0.0.255
 deny   any
!
ip access-list standard iACL-2
 permit 10.2.2.0 0.0.0.255
 deny   any
!
```

Маршрутизатор BR2 передает своим соседям маршрутную информацию, которая размещается в служебном сообщении BGP-UPDATE в секции NLRI, ADDRESS-FAMILY iPBR

Структура первого UPDATE-сообщения, которое отправляет BR2 своим соседям:

```
!
route-map RM_iPBR_iACL-1 permit 10
  match ip address iACL-1
  set ip next-hop 10.10.2.2                адрес Loopback интерфейса на BR2
!
ip access-list standard iACL-1
  permit 10.1.1.0 0.0.0.255
  deny   any
!
version 1                    номер версии маршрутной информации
metrica 100                  метрика к END-HOP через BR2 хуже чем через BR1
```

Данные сообщения в кодировке ASCII

cm91dGUtbWFwIFJNX2lQQlJfaUFDTC0xIHBlcm1pdCAxMAogIG1hdGNoIGlwI
GFkZHJlc3MgaUFDTC0xCiAgc2V0IGlwIG5leHQtaG9wIDEwLjEwLjIuMgohCml
wIGFjY2Vzcy1saXN0IHN0YW5kYXJkIGlBQ0wtMQogIHBlcm1pdCAxMC4xLjE
uMCAwLjAuMC4yNTUKICBkZW55ICAgYW55CiEKdmVyc2lvbiAxCm1ldHJpY
2EgMTAw

Структура второго UPDATE-сообщения, которое отправляет BR2 своим соседям:

```
!
route-map RM_iPBR_iACL-2 permit 10
  match ip address iACL-2
  set ip next-hop 10.10.2.2                адрес Loopback интерфейса на BR2
!
ip access-list standard iACL-2
  permit 10.2.2.0 0.0.0.255
  deny   any
!
version 1                    номер версии маршрутной информации
metrica 10                   метрика к END-HOP через BR2 лучше чем через BR1
```

Данные сообщения в кодировке ASCII

cm91dGUtbWFwIFJNX2lQQlJfaUFDTC0yIHBlcm1pdCAxMAogIG1hdGNoIGlwI
GFkZHJlc3MgaUFDTC0yCiAgc2V0IGlwIG5leHQtaG9wIDEwLjEwLjIuMgohCml

wIGFjY2Vzcy1saXN0IHN0YW5kYXJkIGlBQ0wtMgogIHBlcm1pdCAxMC4yLjIu
MCAwLjAuMC4yNTUKICBkZW55ICAgYW55CiEKdmVyc2lvbiAxCm1ldHJpY2
EgMTA=

Порядок обработки полученной маршрутной информации:

Проверить, что в полученном UPDATE-сообщении, номер версии МИ актуален, если в сообщении номер выше, чем текущий номер в таблице политик маршрутизатора, то такое сообщение обрабатывается. Если номер равен или ниже, чем текущий номер в таблице политик маршрутизатора, то такое UPDATE-сообщение удаляется.

Проверяются данные блока iACL в сообщении, если данные отличаются от настроек на маршрутизаторе, то их нужно добавить в конфигурацию маршрутизатора.

Обрабатывается блок данных RM в сообщении, если данные отличаются от настроек на маршрутизаторе, то их нужно добавить в конфигурацию маршрутизатора.

На основе данных о метрике маршрута к адресу END-HOP в UPDATE-сообщении, трафик попадающий под условия описанные в iACL, будет маршрутизироваться в сторону маршрутизатора с меньшей метрикой к адресу END-HOP, при условии что данный маршрутизатор активен. В противном случае выбирается маршрутизатор с большей метрикой к адресу END-HOP.

В результате обработки UPDATE-сообщения, маршрутизатор добавит в свой конфигурационный файл данные о списке сетей iACL, и сформируется RM для этого списка, где в качестве NEXT-HOP будет указан адрес Loopback интерфейса BR1 или BR2, для которого задана меньшая метрика до адреса END-HOP.

Созданный RM нужно применить к интерфейсам соседей маршрутизаторов, указанных в блоке ADRESS-FAMILY iPBR в настройках протокола BGP.

3.2 Конфигурационные файлы в сокращенном виде.

Конфигурация маршрутизатора BR1

```
interface Loopback10
 ip address 10.10.1.1 255.255.255.255
router iPBR 10
 router-id 10.10.1.1
```

```
!
interface gi0/1
 description Link-to-ISP1
 ip address 192.168.100.1 255.255.255.252
!
interface gi0/2
 description Link-to-BR2
 ip address 10.10.12.1 255.255.255.252
!
interface gi0/3
 description Link-to-TR4
 ip address 10.10.14.1 255.255.255.252
!
interface gi0/4
 description Link-to-TR3
 ip address 10.10.13.1 255.255.255.252
!

address-family ipv4
  neighbor IBGP next-hop-self
  neighbor IBGP send-community both
  neighbor 10.10.2.2 activate
  neighbor 10.10.3.3 activate
  neighbor 10.10.4.4 activate
  neighbor 10.10.5.5 activate
  neighbor 10.10.6.6 activate
  neighbor 10.10.7.7 activate
  no auto-summary
  no synchronization
 exit-address-family
 address-family iPBR
  neighbor IBGP send-community both
  neighbor IBGP next-hop-self
  neighbor 10.10.2.2 activate
  neighbor 10.10.3.3 activate
  neighbor 10.10.4.4 activate
 exit-address-family
 log-adjacency-changes
 interface gi0/2
 interface gi0/3
 interface gi0/4
!
router bgp 65535
 bgp router-id 10.10.1.1
 bgp log-neighbor-changes
 neighbor IBGP peer-group
 neighbor IBGP remote-as 65535
 neighbor IBGP update-source Loopback10
 neighbor IBGP version 4
 neighbor 10.10.2.2 peer-group IBGP
 neighbor 10.10.3.3 peer-group IBGP
 neighbor 10.10.4.4 peer-group IBGP
 neighbor 10.10.5.5 peer-group IBGP
 neighbor 10.10.6.6 peer-group IBGP
 neighbor 10.10.7.7 peer-group IBGP
!
route-map RM_iPBR_iACL-1 permit 10
 match ip address iACL-1
 set ip next-hop 192.168.100.2
!
route-map RM_iPBR_iACL-2 permit 10
 match ip address iACL-2
 set ip next-hop 192.168.100.2
!
ip access-list standard iACL-1
 permit 10.1.1.0 0.0.0.255
 deny   any
!
ip access-list standard iACL-2
 permit 10.2.2.0 0.0.0.255
 deny   any
!
```

Конфигурация маршрутизатора TR3

```
interface Loopback10
 ip address 10.10.3.3 255.255.255.255
!
interface gi0/1
 description Link-to-BR1
 ip address 10.10.13.2 255.255.255.252
!
interface gi0/2
router iPBR 10
 router-id 10.10.3.3
 log-adjacency-changes
 interface gi0/3
 interface gi0/4
 interface gi0/5
 interface gi0/6
!
```

```
 description Link-to-BR2
 ip address 10.10.23.2 255.255.255.252
!
interface gi0/3
 description Link-to-TR4
 ip address 10.10.34.1 255.255.255.252
!
interface gi0/4
 description Link-to-AR7
 ip address 10.10.37.1 255.255.255.252
!
interface gi0/5
 description Link-to-AR6
 ip address 10.10.36.1 255.255.255.252
!
interface gi0/6
 description Link-to-AR5
 ip address 10.10.35.1 255.255.255.252
  neighbor 10.10.4.4 activate
  neighbor 10.10.5.5 activate
  neighbor 10.10.6.6 activate
  neighbor 10.10.7.7 activate
  no auto-summary
  no synchronization
 exit-address-family
 address-family iPBR
  neighbor IBGP send-community both
router bgp 65535
 bgp router-id 10.10.3.3
 bgp log-neighbor-changes
 neighbor IBGP peer-group
 neighbor IBGP remote-as 65535
 neighbor IBGP update-source Loopback10
 neighbor IBGP version 4
 neighbor 10.10.1.1 peer-group IBGP
 neighbor 10.10.2.2 peer-group IBGP
 neighbor 10.10.4.4 peer-group IBGP
 neighbor 10.10.5.5 peer-group IBGP
 neighbor 10.10.6.6 peer-group IBGP
 neighbor 10.10.7.7 peer-group IBGP
 address-family ipv4
  neighbor IBGP next-hop-self
  neighbor IBGP send-community both
  neighbor 10.10.1.1 activate
  neighbor 10.10.2.2 activate
  neighbor IBGP next-hop-self
  neighbor 10.10.1.1 activate
  neighbor 10.10.2.2 activate
  neighbor 10.10.4.4 activate
  neighbor 10.10.5.5 activate
  neighbor 10.10.6.6 activate
  neighbor 10.10.7.7 activate
 exit-address-family
```

Конфигурация маршрутизатора AR5

```
interface Loopback10
 ip address 10.10.5.5 255.255.255.255
!
interface gi0/1
 description Link-to-TR3
 ip address 10.10.35.2 255.255.255.252
!
interface gi0/2
 description Link-to-TR4
 ip address 10.10.45.2 255.255.255.252
!
interface gi0/3
 description Link-to-iACL-1
 ip address 10.1.1.1 255.255.255.128
!
interface gi0/3
 description Link-to-LAN-1
 ip address 172.19.1.1 255.255.255.192
 neighbor IBGP remote-as 65535
 neighbor IBGP update-source Loopback10
 neighbor IBGP version 4
 neighbor 10.10.1.1 peer-group IBGP
 neighbor 10.10.2.2 peer-group IBGP
 neighbor 10.10.3.3 peer-group IBGP
 neighbor 10.10.4.4 peer-group IBGP
 neighbor 10.10.6.6 peer-group IBGP
 neighbor 10.10.7.7 peer-group IBGP
 address-family ipv4
  neighbor IBGP next-hop-self
  neighbor IBGP send-community both
  neighbor 10.10.1.1 activate
  neighbor 10.10.2.2 activate
  neighbor 10.10.3.3 activate
  neighbor 10.10.4.4 activate
  neighbor 10.10.6.6 activate
  neighbor 10.10.7.7 activate
```

```
!
interface gi0/3
 description Link-to-LAN-2
 ip address 10.124.1.1 255.255.255.128
!
router iPBR 10
 router-id 10.10.5.5
 log-adjacency-changes
 interface gi0/3
!
router bgp 65535
 bgp router-id 10.10.5.5
 bgp log-neighbor-changes
 neighbor IBGP peer-group
 no auto-summary
 no synchronization
exit-address-family
address-family iPBR
 neighbor IBGP send-community both
 neighbor IBGP next-hop-self
 neighbor 10.10.1.1 activate
 neighbor 10.10.2.2 activate
 neighbor 10.10.3.3 activate
 neighbor 10.10.4.4 activate
 neighbor 10.10.6.6 activate
 neighbor 10.10.7.7 activate
exit-address-family
```

ЗАКЛЮЧЕНИЕ

Современные корпоративные сети это сложный механизм, который динамически растет и изменяется, в соответствии с теми требованиями, которые ставят новые задачи бизнеса. Запуск новых сервисных приложений может потребовать малых или больших изменений конфигурации сетевого оборудования. При этом существующие сервисы должны продолжать работать стабильно и эффективно. Инженер отвечающий за работу корпоративной сети, может выбирать различные технологии, позволяющие выполнять управление трафиком, которые можно комбинировать друг с другом решая сложные задачи и повышая эффективность работы сети.

Возможность внедрения в процесс управления сетью элементов автоматизации, позволяет более гибко реагировать на меняющуюся ситуацию. Более быстро применять готовые скрипты повышающие эффективность передачи данных по сети. Программно определяемые сети сводят к минимуму работу инженера по ручному конфигурированию сетевых устройств. В сетях SDN процессы управления, развития и контроля полностью автоматизированы.

Поэтому в сравнении с классическими протоколами управления передачей трафика, возможности сетей SDN обеспечить безотказную и высоко производительную работу значительно выше.

В этой дипломной работе, ставилась цель, внести элемент автоматизации в существующий механизм. За основу была взята технология Policy Base Routing (PBR). Это эффективный инструмент, но применимость его ограничена, поскольку все настройки необходимо выполнять вручную. Поэтому для повышения гибкости и масштабируемости, предлагается часть функций технологии PBR автоматизировать. Новой реализации дано название iPBR (Intelectual Policy Base Routing). Метод iPBR, должен положительно решать эти трудности, за счет автоматизации функций:

1. Наблюдать за состоянием каналов связи между маршрутизаторами и каналов с провайдерами.

2. Распространять маршрутную информацию между маршрутизаторами, чтобы каждый из них обладал актуальными данными, это необходимое условие для получения состояния сходимости на сети.

3. Автоматически создавать правила политик для маршрутизации трафика, а в случае изменения топологии автоматически вносить изменения.

Основные принципы работы метода iPBR:

1. iPBR использует дистанционно-векторный принцип передачи маршрутной информации.

2. iACL список доступа содержит определенные сети, к которым нужно применить особый подход при построении маршрута движения пакета.

3. Данный iACL список настраивается только на граничном маршрутизаторе.

4. Термин граничный маршрутизатор, нужно понимать, что данный маршрутизатор для сетей из списка доступа iACL, будет крайним, а далее идет или пункт назначения или трафик уходит в соседнюю автономную систему, например в Интернет.

5. Вводится понятие END-HOP, это точка назначения, для сетей из списка доступа iACL, в случае если трафик уходит в Интернет, то это адрес на стороне провайдера.

6. Используя адрес END-HOP выполняется вычисление лучшего маршрута и выбирается NEXT-HOP для формирования правила политики.

7. Маршрутизаторы выстраивают соседские отношения, интерфейс через который будет идти трафик в сторону END-HOP, имеет статус ACTIVE, запасной интерфейс если такой существует будет находится в резерве, его статус REZERV.

8. Маршрутизаторы обмениваются маршрутной информацией через служебные сообщения UPDATE, получив такой пакет, сперва нужно проверить его версию, если версия старая, то такой пакет уничтожается, если версия новая то информацию нужно обработать, и если требуется то внести изменения в правила политик или в состав сетей из списка подступа iACL.

9. Распространение маршрутной информации происходит с помощью протокола BGP, для этого создается новый блок ADDRESS-FAMILY, это отдельная группа которая будет передавать данные протокола iPBR. В настройка блока ADDRESS-FAMILY указываются адреса соседних маршрутизаторов, между которыми распространяется маршрутная информация iPBR. Структура пакета BGP имеет секцию NLRI, она подходит для передачи параметров iPBR.

10. Когда маршрутизатор доступа AR, получает служебный пакет от BR, он согласно содержащейся в пакете информации, автоматически создает у себя список доступа используя данные таблицы маршрутизации вычисляет значение NEXT-HOP, как лучше добраться до указанной в пакете END-HOP и после этого автоматически формирует правило политики для маршрутизации сетей из данного списка доступа.

12. После того как все маршрутизаторы домена имеют актуальную информацию о списках доступа, выбраны лучшие маршруты и сформированы правила политики, остается только следить за состоянием каналов, быстро реагировать на изменения топологии и вносить корректировку в правила политик.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Куроуз, Д. Компьютерные сети. Нисходящий подход / Д. Куроуз, К. Росс - Москва, 2016. - 912 с.
2. Дибров, М.В. Маршрутизаторы : учебное пособие / М.В. Дибров. - Красноярск, 2008. - 389 с.
3. Олифер, В. Компьютерные сети. Принципы, технологии, протоколы : учебник для вузов / В. Олифер, Н. Олифер - Питер, 2016. - 992 с.
4. Сандул, Г. Возможности технологии Cisco IOS IP SLA. [Электронный ресурс] / Сандул, Г. – 2007. – Режим доступа: https://www.securitylab.ru/analytics/309557.php
5. Хан, А. Policy Based Routing (PBR) в примерах. [Электронный ресурс] / Хан, А. – 2013. – Режим доступа: http://www.ciscolab.ru/routing/29-policy-based-routing-pbr-v-primerah.html
6. Самойленко, Н. Cisco PBR [Электронный ресурс] / Самойленко, Н. – 2014. – Режим доступа: http://xgu.ru/wiki/Cisco_PBR
7. Введение в Cisco OER/PfR [Электронный ресурс] – 2011. – Режим доступа: http://www.anticisco.ru/blogs/2011/05/введение-в-cisco-oerpfr/
8. Смелянский, Р. Программно-конфигурируемые сети [Электронный ресурс] / Смелянский, Р. – Электрон. журн. – 2012. – Режим доступа: https://www.osp.ru/os/2012/09/13032491
9. RFC 1771. Rekhter Y. / A Border Gateway Protocol 4 (BGP-4) / Y. Rekhter, T. Li. – Network Working Group, 1995. – 57 p
10. RFC 2328. Moy J. / OSPF Version 2 / J. Moy. – Network Working Group, 1998. – 244 p.
11. Руденко, И. Маршрутизаторы CISCO для IP–сетей. Пер. с англ. / И. Руденко, Tsunami Computing. – М.: КУДИЦ–ОБРАЗ, 2003. – 656 с.
12. RFC 1247. Moy J. / OSPF Version 2 / J. Moy. – Network Working Group, 1991. – 189 p.
13. Cisco IOS IP Routing Protocols Configuration Guide Release 12.4 / Cisco Systems, Inc., 2006. – 880 p.
14. Cisco IOS Interface and Hardware Configuration Guide Release 12.4 / Cisco Systems, Inc., 2006. – 864 p.
15. Cisco IOS IP Addressing Services Command Reference Release 12.4 / Cisco Systems, Inc., 2006. – 322 p.
16. Хелеби, С. Принципы маршрутизации в Internet, 2-е издание. /С. Хелеби, Д. Мак-Ферсон - Издательский дом «Вильямс», 2001. — 448 с.
17. Перевод руководства от Quagga [Электронный ресурс] – 2004. – Режим доступа: https://www.opennet.ru/base/net/zebra_doc.txt.html

18. Таблица маршрутизации в Quagga [Электронный ресурс] – 2016. – Режим доступа: https://habr.com/ru/post/306084/
19. Протокол BGP в Quagga [Электронный ресурс] – 2016. – Режим доступа: https://habr.com/ru/post/310736/
20. Campus LAN and Wireless LAN. Solution Design Guide – 2020. – 76 p.

Федеральное государственное автономное
образовательное учреждение
высшего образования
«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Институт космических и информационных технологий
институт

Вычислительная техника
кафедра

УТВЕРЖДАЮ
Заведующий кафедрой ВТ

_____ О.В. Непомнящий
подпись инициалы, фамилия
« 18 » 06 2021 г.

МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ

Методы управления маршрутизацией на основе политик
тема

09.04.01 Информатика и вычислительная техника
код и наименование направления

09.04.01.05 Сети ЭВМ и телекоммуникации
код и наименование магистерской программы

Научный руководитель Коршун 11.06.21 доцент, канд. физ.-мат. наук К.В. Коршун
подпись, дата должность, ученая степень инициалы, фамилия

Выпускник _____ 11.06.21 И.А. Дрокин
подпись, дата инициалы, фамилия

Рецензент 11.06.21 Генеральный директор ООО "Интертакс" М.В. Алексеев
подпись, дата должность, ученая степень инициалы, фамилия

Нормоконтролер Коршун 11.06.21 К.В. Коршун
подпись, дата инициалы, фамилия

Красноярск 2021