**МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ**

**Федеральное государственное бюджетное образовательное учреждение**

**высшего образования**

**«КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»**

**(ФГБОУ ВПО «КубГУ»)**

**Физико-технический факультет**

**Кафедра оптоэлектроники**

**КУРСОВОЙ ПРОЕКТ**

**ПРОЕКТИРОВАНИЕ МОДЕЛИ ВЗАИМОДЕЙСТВИЯ АВТОНОМНЫХ СИСТЕМ НА ОСНОВЕ JUNIPER**

Работу выполнил\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Нечитайло Роман Дмитриевич

Курс 3

Направление 11.03.02 Инфокоммуникационные технологии и системы связи

Научный руководитель

канд. физ.-мат. наук, доцент\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_А.С. Левченко

Нормоконтролер инженер\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_И.А. Прохорова

Краснодар 2017

**РЕФЕРАТ**

Курсовая работа 33 с., 8 рис., 2 табл., 7 источников.

ПАКЕТНАЯ ПЕРЕДАЧА ДАННЫХ, ДЕЙТАГРАММНЫЙ И ВИРТУАЛЬНЫЙ МЕТОДЫ ПАКЕТНОЙ КОММУТАЦИИ, БИЛЛИНГ, АУТЕНТИФИКАЦИЯ, МНОГОАДРЕСНОЕ ВЕЩАНИЕ

Объектом исследования данной курсовой работы является возможности моделирования сетей в среде GNS3 (Graphical Network Simulator-3).

Целью работы является моделирование части сети пакетной передачи данных интернет сервис-провайдера в эмуляционной среде на основе оборудования «Juniper».

В результате выполнения курсовой работы были изучены команды конфигурирования JunOS в эмуляционной среде GNS3, а также настройки фильтрации нежелательного трафика. В данной эмуляционной среде была собрана часть сети, состоящая из 2 роутеров, соединённых между собой, и находящихся в зонах TRUST и UNTRUST. К одному из роутеров подключён сервер и несколько компьютеров-клиентов. Для настройки передачи данных были использованы технологии статического NAT. Также был создан фильтр, не пропускающий нежелательный трафик на некоторые компьютеры-клиенты из зоны UNTRUST в зону TRUST.

**СОДЕРЖАНИЕ**

|  |  |
| --- | --- |
| Введение.……………………………………………………………………… |  4 |
| 1 Принципы пакетной передачи данных в совокупности с биллинговыми системами, многоадресным вещанием и аутентификацией.………………. |   5 |
| 1.1 Коммутация пакетов.…………………………………………………... |  5 |
| 1.2 Процесс передачи данных в сети с коммутацией пакетов.………….. |  6 |
| 1.3 Дейтаграммный метод пакетной коммутации……………………….. |  7 |
| 1.4 Виртуальный метод пакетной коммутации…………………………... |  7 |
| 1.5 Биллинговые системы для провайдеров……………………………… |  9 |
| 1.6 Многоадресное вещание ……………………………………………… | 12 |
| 1.7 Понятие аутентификации, её задачи и технологии………………….. | 13 |
| 1.8 Классификация методов аутентификации……………………………. | 14 |
| * 1. Сервер аутентификации………………………………………………..
 | 15 |
| 1.10 Основы работы сети провайдера по пакетной передаче данных….. | 15 |
| 2 Основы работы операционной системы JunOS в эмуляционной среде GNS3 ………………………............................................................................... | 18 |
| 2.1 Знакомство с JunOS в эмуляционной среде GNS3…………………... | 18 |
| 2.2 Фильтрация и политики операционной системы JunOS…………….. | 21 |
| 3 Практическая настройка сети с использованием NAT………….……….. | 24 |
| 4 Практическая настройка сети с использованием BGP…………………… | 28 |
| Заключение …………………………………………………………………… | 32 |
| Список использованных источников ……………………………………….. | 33 |

**ВВЕДЕНИЕ**

В настоящее время телекоммуникации, в частности компьютерные сети и телефония, приобретают всё большое значение для современного общества. В последнее время ярко выражена тенденция сближения различных видов сетей: глобальных и локальных компьютерных сетей, телекоммуникационных сетей других видов: телефонных, телевизионных, радиосетей.

Тема актуальна и может представлять интерес не только для специалистов в области телекоммуникаций, но и для широкого круга общественности. В современных условиях практически невозможно организовать построение сетей передачи данных без применения эмуляционных сред, в частности программы GNS3. Это симулятор сети передачи данных, выпускаемый фирмой Cisco Systems. Он позволяет делать работоспособные модели сети, настраивать маршрутизаторы и коммутаторы, взаимодействовать между несколькими пользователями.

При этом GNS3 позволяет создавать сложные макеты сетей, проверять на работоспособность топологии.

1. **Принципы пакетной передачи данных в совокупности с биллинговыми системами, многоадресным вещанием и аутентификацией**

**1.1 Коммутация пакетов**

Под коммутацией в сетях передачи данных понимается совокупность операций, обеспечивающих в узлах коммутации передачу информации между входными и выходными устройствами в соответствии с указанным адресом. При коммутации пакетов (КП) передаваемое сообщение разбивается на меньшие части, называемые пакетами, каждый из которых имеет установленную максимальную длину. Пакеты снабжаются служебной информацией, необходимой для доставки пакета, и передаются по сети.

Каждый пакет снабжается следующей служебной информацией (заголовком): коды начала и окончания пакета, адреса отправителя и получателя, номер пакета в сообщении, а также информация для контроля достоверности передаваемых данных в промежуточных узлах связи и в пункте назначения.

Множество пакетов одного и того же сообщения может передаваться одновременно. Приёмник в соответствии с заголовками пакетов выполняет сборку пакетов в исходное сообщение и отправляет его получателю. Благодаря возможности не накапливать сообщения целиком, в узлах коммутации не требуется внешних запоминающих устройств. Следовательно, можно вполне ограничиться оперативной памятью, а в случае её переполнения использовать различные механизмы задержки передаваемых пакетов в местах их генерации.

Части одного и того же сообщения могут в одно и то же время находиться в различных каналах связи. Возможна также ситуация, когда начало сообщения уже принято, его конец отправитель может ещё даже не передавать в канал.

При пакетной коммутации приходится находить компромиссное решение, удовлетворяющее двум противоречивым требованиям. Во-первых, это требование уменьшения задержки пакета в сети, обеспечиваемое уменьшением его длины. Во-вторых, это требование обеспечение повышения эффективности передачи информации, достигаемое, наоборот, увеличением длины пакета. В сети с пакетной коммутацией максимальный размер пакета устанавливается на основе 3-х факторов: распределение длин пакетов, характеристика среды передачи (главным образом, скорость передачи) и стоимость передачи. Для каждой передающей среды выбирается свой оптимальный размер пакета.

**1.2 Процесс передачи данных в сети с коммутацией пакетов**

Процесс передачи данных в сети с КП можно представить в виде следующей последовательности операций:

1. Вводимое в сеть сообщение разбивается на части - пакеты, содержащие адрес конечного пункта получателя.
2. В узле коммутации пакетов (КП) пакет запоминается в оперативной памяти (ОЗУ) и по адресу определяется канал, по которому он должен быть передан. Если этот канал связи с соседним узлом свободен, то пакет немедленно передается на соседний узел КП, в котором повторяется та же операция. Если канал связи с соседним узлом занят, то пакет может какое-то время храниться в ОЗУ до освобождения канала.
3. Сохраняемые пакеты помещаются в очередь по направлению передачи, причем длина очереди не превышает 3-4 пакета; если длина очереди превышает допустимую, пакеты стираются из ОЗУ и их передача должна быть повторена.

Пакеты, относящиеся к одному сообщению, могут передаваться по разным маршрутам в зависимости от того, по какому из них в данный момент они с наименьшей задержкой могут пойти к адресату. В связи с тем, что время прохождения по сети пакетов одного сообщения может быть различным (в зависимости от маршрута и задержки в узлах коммутации), порядок их перехода к получателю может не соответствовать порядку пакетов, поэтому необходимо сконфигурировать их в единое целое.

**1.3 Дейтаграммный метод пакетной коммутации**

Этот метод эффективен для передачи коротких сообщений. Он не требует громоздкой процедуры установления соединения между абонентами.

Термин "дейтаграмма" (датаграмма, datagram) применяют для обозначения самостоятельного пакета, движущегося по сети независимо от других пакетов. Пакеты доставляются получателю различными маршрутами. Эти маршруты определяются сложившейся динамической ситуаций на сети. Каждый пакет снабжается необходимым служебным маршрутным признаком, куда входит и адрес получателя.

Пакеты поступают на прием не в той последовательности, в которой они были переданы, поэтому приходится выполнять функции, связанные со сборкой пакетов. Получив дейтаграмму, узел коммутации направляет ее в сторону смежного узла, максимально приближенного к адресату. Когда смежный узел подтверждает получение пакета, узел коммутации стирает его в своей памяти. Если подтверждение не получено, узел коммутации отправляет пакет в другой смежный узел, и так до тех пор, пока пакет не будет отправлен.

Все узлы, окружающие данный узел коммутации, ранжируются по степени близости к адресату, и каждому присваивается ранг. Пакет сначала посылается в узел первого ранга, при неудаче - в узел второго ранга и так далее. Эта процедура называется алгоритмом маршрутизации. Существуют алгоритмы, когда узел передачи выбирается случайно, и тогда каждая дейтаграмма будет идти по случайной траектории.

**1.4 Виртуальный метод пакетной коммутации**

Этот метод предполагает предварительное установление маршрута передачи всего сообщения от отправителя до получателя с помощью специального служебного пакета - запроса вызова.

Для этого пакета выбирается маршрут, который в случае согласия получателя этого пакета на соединение закрепляется для прохождения по нему всего трафика. Пакет запроса на соединение как бы прокладывает через сеть путь, по которому пойдут все пакеты, относящиеся к этому вызову.

Метод называется виртуальным потому, что здесь не коммутируется реальный физический тракт (как, например, в телефонной сети), а устанавливается логическая связка между отправителем и получателем. То есть коммутируется виртуальный (воображаемый) тракт.

В виртуальной сети абоненту-получателю направляется служебный пакет, прокладывающий виртуальное соединение. В каждом узле этот пакет оставляет распоряжение вида: пакеты k-го виртуального соединения, пришедшие из i-го канала, следует направлять в j-й канал. Тем самым виртуальное соединение существует только в памяти управляющего компьютера. Дойдя до абонента-получателя, служебный пакет запрашивает у него разрешение на передачу, сообщив, какой объем памяти понадобится для приема. Если его компьютер располагает такой памятью и свободен, то посылается согласие абоненту-отправителю на передачу сообщения. Получив подтверждение, абонент-отправитель приступает к передаче сообщения обычными пакетами.

Пакеты беспрепятственно проходят друг за другом по виртуальному соединению и в том же порядке попадают абоненту-получателю, где, освободившись от заголовков и концевиков, образуют передаваемое сообщение. Виртуальное соединение может существовать до тех пор, пока отправленный одним из абонентов специальный служебный пакет не сотрёт инструкции в узлах. Режим виртуальных соединений эффективен при передаче больших массивов информации.

Преимущества режима виртуальных соединений перед дейтаграммным заключается в обеспечении упорядоченности пакетов, поступающих в адрес получателя, и сравнительной простоте управления потоком данных вдоль маршрута в целях ограничения нагрузки в сети, в возможности предварительного резервирования ресурсов памяти на узлах коммутации.

К недостаткам следует отнести отсутствие воздействия изменившейся ситуации в сети на маршрут, который не корректируется до конца связи. Виртуальная сеть в значительно меньшей степени подвержена перегрузкам и зацикливанию пакетов, за что приходится платить худшим использованием каналов и большей чувствительностью к изменению топологии сети[6].

* 1. **Биллинговые системы для провайдеров**

Биллинг — это процесс выписывания счёта. Применительно к телекоммуникациям, это выставление счёта абоненту за пользование услугами. Биллинговая система, она же Автоматизированная Система Расчётов (АСР), —это подлежащая обязательной сертификации система. АСР — это очень важное для бизнеса приложение. АСР должна хранить в БД всех клиентов с их атрибутами (счёт, реквизиты, адрес, комментарии, баланс, тариф, квоты), обеспечивать работу сразу нескольких операторов, иметь пользовательский интерфейс для клиентов. Также Автоматизированная Система Расчётов должна обеспечивать генерацию отчётов любой детализации, что приводит к понятию многоуровневой базы данных (БД). Нужно соблюдать баланс между скоростью составления отчётов и нагрузкой на БД. Также АСР должна формировать счёт для каждого клиента согласно тарифу, производить тарификацию по предоставляемым услугам связи, а также обрабатывать и вводить в базу данных первичную информацию о предоставляемых услугах и их оплате.



Рисунок 1 – Зеркалирование

В случае аппаратных маршрутизаторов для сбора данных используется специальный протокол. Суть его в том, что через определённые промежутки времени будут отправляться данные о трафике на указанный в настройках хост. Специальные протоколы могут отправлять не полный поток данных, а с некой периодичностью усреднённые данные, экономя ресурсы и пропускную способность.



Рисунок 2 – Использование специальных протоколов

В случае, если провайдер является одним из доминирующих в стране либо крупном регионе, АСР должна уметь интерпретировать данные не только из своей сети, от своих устройств, но и предоставленные третьей стороной, со всеми параметрами и полями, которые важны всем втянутым операторам. Международный Союз Электросвязи (ITU) разработал универсальные стандарты, которых должны придерживаться разработчики систем биллинга.

Основные требования к комплексам такого уровня:

1. Модульность - дополнительный функционал добавляется в рамках той же самой системы. Для этого существуют унифицированные интерфейсы, медиаторы (промежуточные узлы), среды разработки.
2. Масштабируемость – при увеличении нагрузки не нужно менять программную составляющую, а необходимо лишь увеличить аппаратную мощь.
3. Резервирование, высокая устойчивость к сбоям – АСР работают на базе кластеров или в режиме «Hot/Backup», когда резервный сервер заменяет активный в случае его падения. Все данные находятся в хранилищах.
4. Время реакции. АСР должна в разумное время принять решение о действиях над абонентом (блокировка, ограничение скорости, увеличение скорости).

Оборудование, осуществляющее доставку и коммутацию звонка, формирует запись Call Detail Record (CDR) с некоторой периодичностью или после окончания вызова и передаёт биллинговой системе. Ну а она в свою очередь на основе этих данных формирует счёта. На рисунке 3 изображена мобильная сеть с DPI и биллинговой системой. Когда абонент с телефона выходит в интернет, он сначала регистрируется в мобильном ядре, а далее, получив IP-адрес, выходит в интернет. Все пакеты проходят через DPI. В такой ситуации и SGSN, и GGSN, и DPI могут генерировать CDR, выкладывать их в определённый каталог в хранилище, а биллинговая система будет их забирать и выкатывать счета на основе тарифов (дополнительные данные также содержатся в CDR). То есть в данном случае это будет информация не о времени и направлении звонка, а об объёме трафика и запрошенных ресурсах[7].



Рисунок 3 – Схема мобильной сети

* 1. **Многоадресное вещание**

Мультивещание, многоадресное вещание (англ. multicast — групповая передача) — форма широковещания, при которой адресом назначения сетевого пакета является мультикастная группа (один ко многим). Существует мультивещание на канальном, сетевом и прикладном уровнях.

Ряд приложений, например, дистанционное обучение, рассылка почты, радио, видео по запросу, видеоконференцсвязь, поддерживают мультивещание. В одноадресной сети с каждым получателем устанавливается индивидуальное соединение даже при потреблении одного ресурса по общему маршруту. В многоадресной рассылке источник посылает единственный экземпляр данных по общему маршруту тем получателям, кто подписался на рассылку. Преимущество этого подхода: добавление новых пользователей не влечет за собой необходимость увеличения пропускной способности сети по общему маршруту до потребителей услуги. Соответственно, снижается нагрузка и на промежуточное оборудование.

При запуске на сервере приложения с поддержкой мультивещания, оно посылает в сеть уведомление, что соответствующая группа доступна для присоединения. Клиент, который хочет присоединиться к рассылке посылает уведомление об этом. Все промежуточные маршрутизаторы записывают, что за соответствующим маршрутом находится клиент соответствующей мультикастной группы. Поскольку состав группы со временем может меняться, вновь появившиеся и выбывшие члены группы динамически учитываются в построении путей маршрутизации. В локальной сети управлением мультикастными группами обычно занимается IGMP. Существует несколько алгоритмов и протоколов для построения мультивещательного дерева и опроса участников.

Чтобы технология работала, она должна поддерживаться сервером, клиентом и всеми промежуточными маршрутизаторами. Чтобы коммутаторы посылали пакеты только нужным получателям, они должны поддерживать IGMP snooping (у Cisco есть своя реализация — CGMP), иначе пакеты рассылаются широковещательно. Также нужно иметь в виду, что мультикаст может блокироваться межсетевыми экранами.

В IPv4 для мультивещания зарезервирована подсеть 224.0.0.0/4. Глобально маршрутизация разрешена только для подсетей 233.0.0.0/8 и 234.0.0.0/8. Но не все провайдеры поддерживают мультикаст-связность.

**1.7 Понятие аутентификации, её задачи и технологии**

Аутентификация — проверка подлинности предъявленного пользователем идентификатора. Аутентификация требуется при доступе к таким интернет-сервисам как электронная почта, платёжные системы, социальные сети, интернет-банкинг и так далее.

Задачами аутентификации являются установка доверительных отношений

пользователя и сервиса, выработка сессионного ключа, предоставление авторизованному пользователю прав доступа к необходимым ему ресурсам, а также максимальное затруднение использования полученных незаконным путём данных злоумышленниками.

Для различных типов ресурсов требуются различные технологии аутентификации. Если доступ осуществляется к информационным системам, содержащим информацию, разглашение которой не несёт существенных последствий, то минимальным требованием для аутентификации является использование многоразовых паролей. Если же на информационном ресурсе содержится информация, при модификации (либо уничтожении, либо копировании, либо блокировании) которой может быть нанесён значительный ущерб, то для аутентификации используются одноразовые пароли. Если же на сервере содержится конфиденциальная информация, то требуется строгая взаимная аутентификация пользователя и сервера.

* 1. **Классификация методов аутентификации**

Основные методы аутентификации:

1. Базовая аутентификация. При использовании данного вида аутентификации имя пользователя и пароль включаются в состав веб-запроса.
2. Дайджест-аутентификация. Пароль пользователя передается в хешированном виде. Он хэшируется всегда с добавлением произвольной строки символов, которая генерируется на каждое соединение заново.
3. Аутентификация с использованием протокола HTTPS. Это позволяет шифровать все данные, передаваемые между браузером и сервером, а не только имена пользователей и пароли.
4. Аутентификация по предъявлению цифрового сертификата. Механизмы аутентификации с применением цифровых сертификатов, как правило, используют протокол с запросом и ответом. Сервер аутентификации отправляет пользователю последовательность символов, так называемый запрос. В качестве ответа выступает запрос сервера аутентификации, подписанный с помощью закрытого ключа пользователя.
5. Отслеживание аутентификации самим пользователем.
6. Многофакторная аутентификация. Здесь используются несколько факторов аутентификации сразу.

**1.9 Сервер аутентификации**

Сервер аутентификации — это единый центр администрирования всех процессов проверки подлинности сразу для всех приложений, сервисов и ресурсов. Такие серверы поддерживают целый набор методов аутентификации. Каждый ресурс, использующий сервер аутентификации, может использовать метод, который требуется именно ему.

Администраторы серверов аутентификации получают единый интерфейс управления учетными данными пользователей, гибкие возможности по смене методов проверки подлинности.

Гибкость и лёгкость добавления новых методов проверки подлинности просто недостижима без сервера аутентификации. Сокращение времени на эти задачи настолько значительно, что позволяет говорить о быстроте ввода продукта в эксплуатацию как о конкурентном преимуществе. Ведь организация, предлагающая передовые технологические решения раньше остальных, заведомо более привлекательна для клиентов.

Доступность строгой аутентификации в виде специализированного программного обеспечения позволяет добавлять многофакторность для приложений, которые прежде не обладали подобным функционалом, без многочисленных доработок.

Практически все информационные системы, сервисы, приложения, не поддерживающие строгую аутентификацию, могут использовать возможности сервера аутентификации для доступа пользователей.

* 1. **Основы работы сети провайдера по пакетной передаче данных**

Для описания основы работы сети провайдера по пакетной передаче данных до конечного пользователя по оптоволоконной телекоммуникационной сети в качестве примера будет взята технология IPTV (Internet Protocol Television). Это современная технология, позволяющая эффективно передавать телевизионный сигнал через сеть Интернет. При описании работы будут учитываться функциональные назначения биллинга, сервера аутентификации и многоадресное вещание. На рисунке 4 изображена часть сети провайдера. Каждый клиент желает посмотреть платную телепередачу на одном и том же ресурсе. При этом для просмотра трансляции каждому из них необходимо ввести свои логин и пароль.



Рисунок 4 – Часть сети провайдера

Каждый клиент проходит процедуру аутентификации для получения доступа в сеть Интернет, благодаря которой происходит подтверждение личности каждого клиента. При этом начинает свою работу Автоматизированная Система Расчётов. Она начинает формировать счёт для каждого клиента согласно тарифу, производит тарификацию по предоставляемым услугам связи, а также обрабатывает и вводит в базу данных первичную информацию о предоставляемых услугах и их оплате. После успешного прохождения авторизации каждый клиент получает возможность просматривать желаемую телепередачу. На коммутаторе все 4 порта должны быть в одном VLAN. Трафик приходит на коммутатор и по умолчанию рассылается во все порты одного VLAN'а. Значит все клиенты получают этот трафик. При этом клиенты и сервер не обязательно должны иметь адреса из одной подсети и пинговать друг друга — достаточно, чтобы они были в одном широковещательном домене. Три клиента становятся членами одной мультикастовой группы, и при этом любой из них может войти и выйти из неё. В данном случае от сервера-источника приходит только одна копия трафика на коммутатор, а не по отдельной копии для каждого клиента.

1. **Основы работы операционной системы JunOS в эмуляционной среде GNS3**

**2.1 Знакомство с JunOS в эмуляционной среде GNS3**

В сетевом оборудовании пакетной передачи данных для управления и настройки существует специальная, предназначенная для этого, операционная система. Компания Juniper, занимающаяся производством и продажей такого оборудования, выпустила программное обеспечение, названное JunOS, под которой в настоящий момент и работают все их устройства сети. Данная ОС имеет множество различных версий. Это обусловлено наличием оборудования разного типа: коммутаторы, роутеры, серверное оборудование, а также стеком протоколов, настройка которых возможна.

Специалисты должны обладать знаниями и навыками, позволяющими им работать с сетями операторского класса, а также разрабатывать и обслуживать сети предприятий. Для удаленной тренировки таких специалистов в настоящее время часто используется программа- симулятор GNS3. Данная эмуляционная среда дает возможность виртуально создавать сети пакетной передачи данных различного уровня сложности. Также разработчики программы GNS3 смогли адаптировать JunOS на своей платформе, в следствие чего появилась возможность использовать эту операционную систему для эмулирования работы оборудования Juniper.

Работа с командной строкой в JunOS разделяется на два режима: эксплуатационный режим и режим конфигурирования. Эксплуатационный режим (Operational mode) – это режим для просмотра информации посредством команды show, отслеживания ошибок через команды monitor, ping, test, traceroute (рисунок 5). Данный режим в командной строке обозначается символом « > ».

root@% cli

root> tracerout [ip- адрес]



Рисунок 5­ – Структура команд

Режим конфигурирования (Configuration mode) – это режим, в котором происходит непосредственно настройка устройства. Любое подключение и отключение протоколов происходит именно в этом режиме. В консоли он обозначается символом «#». В данный контекст можно попасть с помощью введения команд в экcплуатационном режиме configure или edit.

 root> configure

[edit]

 root#

Работа устройства осуществляется за счет уже прописанной конфигурации, которая сохранена в памяти оборудования. Такая конфигурация называется действующей. Однако, существует и другая конфигурация- кандидат, используемая для настройки устройства в настоящее время. В данной конфигурации происходит изменение настроек и подключение протоколов. Любая настройка протоколов в данной конфигурации происходит через команду edit, как показано на рисунке 6 [1].



Рисунок 6 – Структура команды Edit

Данная команда обозначает переход с одного уровня настройки протокола на другой. Таким образом существует несколько вариантов захода на определенный уровень. Первый вариант включает в себя поочередное прописывание команды edit на каждом уровне, пока не будет достигнут тот, который необходим. К примеру, необходимо достичь уровня настройки соседа в протоколе bgp.

 root> configure

[edit]

 root# edit protocols bgp

[edit protocols bgp]

 root# edit group «название группы»

[edit protocols bgp group «название группы»]

 root# edit neighbor [ip адрес]

[edit protocols bgp group «название группы» neighbor [ip адрес]

Удобство данного варианта заключается в том, что при использовании команды exit на любом уровне конфигурирования протокола произойдет выход на предыдущий уровень настройки.

 root# edit neighbor [ip адрес]

[edit protocols bgp group «название группы» neighbor [ip адрес]]

 root# exit

[edit protocols bgp group «название группы»]

 root#

Таким образом это облегчает лавирование между уровнями если идет настройка только одного протокола. Второй способ заключается в возможности быстрого перехода на определенный, нужный, уровень настройки. Существуют ситуации, в которых нужно быстро сделать исправление или добавить запись только на одном уровне протокола. В этом случае это наиболее удобный вариант перехода.

 root# edit protocols bgp group «название группы» neighbor [ip адрес]

[edit protocols bgp group «название группы» neighbor [ip адрес]]

 root#

При использовании команды exit консоль автоматически переходит на изначальный уровень в режиме конфигурирования[2].

[edit protocols bgp group «название группы» neighbor [ip адрес]]

 root#exit

[edit]

 root#

**2.2 Фильтрация и политики операционной системы JunOS**

В сетевом оборудовании пакетной передачи данных для управления и настройки существует специальная, предназначенная для этого, операционная система. Компания Juniper, занимающаяся производством и продажей такого оборудования, выпустила программное обеспечение, названное JunOS, под которой в настоящий момент и работают все их устройства сети. Данная ОС имеет множество различных версий. Это обусловлено наличием оборудования разного типа: коммутаторы, роутеры, серверное оборудование, а также стеком протоколов, настройка которых возможна.

Фильтром называется механизм, применимый для фильтрации пакетов на входе в маршрутизатор и выполняющий определённые действия. Чаще всего это принять либо отбросить пакет в зависимости от выбранных свойств пакета.

Пример структуры фильтра:

R1# show firewall filter test

interface-specific;

term 1 {

from {

«условие совпадения»;

}

then

{

«условие действия\_1»;

«условие действия\_2»;

}

}

term 2 {

«условие действия\_3»;

}

[edit]

Все фильтры делятся на части, называемые term. Каждый term имеет своё название и содержит свой набор действий, применимых к пакету. Сначала, после параметра from, выставляется условие. Потом указывается действие, которое необходимо выполнить при выполнении заданного условия. В фильтре так же содержится второй term, который вступает в действие, в случае невыполнения условий, заданных в первом.

Каждый term содержит условия совпадения и действия, которые надо выполнить в результате совпадения условий. Все term выполняются строго по порядку, до выполнения одного из действий. Как только у нас сработал один из term, фильтр прекращает свою работу. Чтобы выполнить несколько term подряд, необходимо добавить специальное действие: «next term».

Существуют несколько основных команд-действий в структуре фильтра:

1. Discard – отбрасывание пакета без отсылки ICMP уведомления.
2. Reject – отбрасывание пакета с отсылкой ICMP уведомления.
3. Count «имя файла» – посчитать пакет с записью в специально создаваемый файл.
4. Log – залогировать пакет в файл логирования.

Политики используются для управления маршрутами на сети, изменения стандартного поведения протоколов динамической маршрутизации. Политики являются очень гибким механизмом для осуществления маршрутизации пакетов, и применяются уже не на интерфейс, а в самых различных местах в конфигурации оборудования Juniper Network.

Общая структура политик:

R1# show policy-options

policy-statement test {

term 1 {

from «условие совпадения»;

then «условие действия»;

}

term 2 {

from {

«условие совпадения»;

}

then {

«условие действия»;

}

}

}

[edit]

R1#

Как видно из примера, политика тоже состоит из частей, называемых term. Каждый term содержит условия совпадения и действия, выполняемые в результате совпадения условий. Если в каком-либо разделе конфигурации присутствует цепочка политик, то при выполнении одной из политик перехода к следующей не будет осуществлено, если не указать специальное действие «next term» [3].

1. **Практическая настройка сети с использованием NAT**

Схема, изображенная на рисунке 7, представляет собой часть сети провайдера, состоящую из 2 роутеров, свитча и компьютеров-клиентов.



Рисунок 7 – Схема построения сети

Таблица 1 – Исходные данные для сети с использованием статического NAT

|  |  |  |  |
| --- | --- | --- | --- |
| Устройство | Интерфейс | Ip- адрес | Маска |
|  | Em0 | 10.24.0.3 | 255.255.255.224 |
| Router1 | Em1 | 10.24.32.3 | 255.255.255.224 |
|  | Loopback 0 | 10.10.10.10 | 255.255.0.0 |
|  | Em0 | 10.24.32.4 | 255.255.255.224 |
| Router2 | Em1 | 10.24.64.3 | 255.255.255.224 |
|  | Loopback 0 | 11.11.11.11 | 255.255.0.0 |
| PC1 | Fe 0/0 | 10.24.0.4 | 255.255.255.224 |
| PC2 | Fe 0/0 | 10.24.0.5 | 255.255.255.224 |
| PC3 | Fe 0/0 | 10.24.0.6 | 255.255.255.224 |
| PC4 | Fe 0/0 | 10.24.0.7 | 255.255.255.224 |
| PC5 | Fe 0/0 | 10.24.64.4 | 255.255.255.224 |

В качестве примера построена сеть с использованием одного из трёх видов NAT, статического NAT, который можно настроить на оборудовании Juniper. Статический NAT позволяет осуществить соединение с двух сторон, в отличие от NAT источника и NAT назначения[4].

Настройка интерфейсов стоит в очередности сразу после аутентификации, т. е. подключения имени и пароля. Для обоих роутеров аутентификация производится одинаково.

 root> configure

 root# set system host-name user

 root# set system root-authentication plain text password

New password: admin1

Retype new password: admin1

Начальная настройка включает настройку IP адресации с помощью протокола IPv4, а также настройки логических интерфейсов Loopback.

 Router1# edit interface em0

[edit interfaces em0]

 Router1# set unit 0 family inet address 10.24.0.3/19

 Router1# exit

[edit]

 Router1# edit interface em1

[edit interfaces em1]

 Router1# set unit 0 family inet address 10.24.32.3 /19

 Router1# exit

 Router2# edit interface em0

[edit interfaces em0]

 Router2# set unit 0 family inet address 10.24.32.4/19

 Router2# exit

[edit]

 Router2# edit interface em1

[edit interfaces em1]

 Router2# set unit 0 family inet address 10.24.64.3 /19

 Router2# exit

 Router1>configure

[edit]

 Router1#edit interfaces lo0

[edit interfaces lo0]

 Router1#set unit 0 family inet address 10.10.10.10/16

 Router2>configure

[edit]

 Router2#edit interfaces lo0

[edit interfaces lo0]

 Router2#set unit 0 family inet address 11.11.11.11/16

Настроим метод сетевой трансляции адресов на Router1, при прохождении пакетов из зоны Untrust в зону Trust на клиентские компьютеры. Нужна настройка свода правил.

 Router1#edit security nat static

[edit security nat static]

 Router1#set rule-set rs1 from zone untrust

 Router1#set rule-set rs1 rule r1 match destination-address 10.24.32.3/19

 Router1#set rule-set rs1 rule r1 then static-nat prefix 10.24.0.4/19

Далее нужно указать интерфейс и его адрес, на котором будет происходить смена адреса назначения посредством команды set proxy-arp interface «номер интерфейса» address «адрес интерфейса» [5].

[edit security nat]

 Router1# set proxy-arp interface em1 address 10.24.32.3

Затем, в конфигурационном режиме в контексте настройки security нужно настроить зону и адрес хоста, к которому будет осуществляться подключение.

[edit security]

 Router1# set zones security-zone trust address-book address PC1 10.24.0.4/19

 Router1# set zones security-zone trust address-book address PC2 10.24.0.5/19

 Router1# set zones security-zone trust address-book address PC3 10.24.0.6/19

Настройка двух правил политики: из зоны Untrust в Trust и из зоны Trust в зону Untrust для PC1:

[edit security policies from-zone untrust to-zone trust]

 Router1# set policy server-access match source-address any destination-address PC1 application any

 Router1# set policy server-access then permit

[edit security policies from-zone trust to-zone untrust]

 Router1# set policy permit-all match source-address PC1 destination-address any application any

 Router1# set policy permit-all then permit

Настроим фильтрацию пакетов на Router1 так, чтобы пакеты с PC4 не были доставлены на PC1 и применим фильтр на интерфейс:

 Router#1 set term block-some-packets1 from source-address 10.24.0.7/19 destination-address 10.24.0.4/19 then discard

Router#1 set interfaces em0 unit 0 family inet filter output filter-in

1. **Практическая настройка сети с использованием eBGP**

На примере части сети, изображенной на рисунке 8, будут рассмотрены основы работы протокола граничного шлюза BGP на роутерах фирмы Juniper.



Рисунок 8 – Схема сети с использованием протокола eBGP

Таблица 2 – Исходная данные для построения сети на основе протокола eBGP

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Устройство | AS | Интерфейсы | IP-адрес | Маска |
| JUNOS1 | 11 | Loopback 0 | 10.10.10.10 | 255.255.255.0 |
|  |  | Em0 | 10.24.0.3 | 255.255.0.0 |
| JUNOS2 | 12 | Loopback 0 | 11.11.11.11 | 255.255.255.0 |
|  |  | Em0 | 11.24.0.4 | 255.255.0.0 |

Настройка интерфейсов стоит в очередности сразу после аутентификации, т. е. подключения имени и пароля.

root> configure

 root# set system host-name user

 root# set system root-authentication plain text password

New password: admin1

Retype new password: admin1

Настройки интерфейсов и самой настройки протокола BGPv4.

 JUNOS1# edit interface em0

[edit interface em0]

 JUNOS1# set unit 0 family inet address 10.24.0.3/16

JUNOS2# edit interface em0

[edit interface em0]

 JUNOS2# set unit 0 family inet address 11.24.0.4/16

Далее нужно настроить логические интерфейсы и присвоить им определенные IP-адреса, воспользовавшись уже знакомой командой set unit 0 family inet address [адрес/маска].

 JUNOS1>configure

 JUNOS1#edit interfaces lo0

[edit interfaces lo0]

 JUNOS1#set unit 0 family inet address 10.10.10.10/24

 JUNOS2>configure

 JUNOS2#edit interfaces lo0

[edit interfaces lo0]

 JUNOS2#set unit 0 family inet address 11.11.11.11/24

Таким образом все интерфейсы, которые были нужны для корректной работы протокола граничного шлюза BGP, были настроены.

В данной сети имеются две автономные системы, обозначенные AS 10 и AS 11. В каждой из них имеется маршрутизатор, исполняющий роль внешнего шлюза. Так как сеть, не имеет внутри своих автономных систем несколько устройств, то настройка протокола граничного шлюза BGP будет ограничена настройкой протокола eBGP.

Для настройки данного протокола нужно зайти в его конфигурацию посредством команды edit protocols bgp и в контексте этого режима задать номер автономной системы и идентификатор роутера. Для этого будут использоваться команды set local-as и set local-address соответственно. За идентификатор маршрутизаторов будет взят номер их логических интерфейсов.

[edit]

 JUNOS1# edit protocols bgp

[edit protocols bgp]

 JUNOS1# set local-as 11

 JUNOS1# set local-address 10.24.0.3

[edit]

 JUNOS2# edit protocols bgp

[edit protocols bgp]

 JUNOS2# set local-as 12

 JUNOS2# set local-address 11.24.0.4

Теперь необходимо описать соседний маршрутизатор с которыми будет происходить обмен маршрутной информацией посредством протокола граничного шлюза BGP. В операционной системе JunOS все соседние роутеры объединяются в группы, которым присваиваются общие свойства. Создание таких групп происходит через команду edit group «название группы» в режиме конфигурирования данного протокола.

[edit protocols bgp]

 JUNOS1#edit group main

[edit protocols bgp]

 JUNOS2#edit group main

Таким образом, на обоих маршрутизаторах была создана группа под названием main. В контексте настройки группы обязательно должно быть указано с помощью команды set type «external/internal», что за тип соседства будет использоваться в ней, то есть какой протокол динамической маршрутизации будет использован, eBGP или iBGP.

[edit protocols bgp group main]

 JUNOS1#set type external

[edit protocols bgp group main]

 JUNOS2#set type external

Последующее добавление информации о соседних маршрутизаторах и автономных системах производится путем введения команды edit neighbor. В информацию о соседнем роутере входит номер его автономной системы, а также его идентификатор.

[edit protocols bgp group main]

 JUNOS1#edit neighbor 11.24.0.4

[edit protocols bgp group main neighbor 11.24.0.4]

 JUNOS1#set peer-as 12

[edit protocols bgp group main]

 JUNOS1#edit neighbor 11.24.0.4

[edit protocols bgp group main neighbor 11.11.11.11]

 JUNOS1#set peer-as 12

[edit protocols bgp group main]

 JUNOS2#edit neighbor 10.24.0.3

[edit protocols bgp group main neighbor 10.24.0.3]

 JUNOS2#set peer-as 11

[edit protocols bgp group main]

 JUNOS2#edit neighbor 10.10.10.10

[edit protocols bgp group main neighbor 10.10.10.10]

 JUNOS2#set peer-as 11

**ЗАКЛЮЧЕНИЕ**

Была изучена и описана основа работы сети провайдера по пакетной передаче данных до конечного пользователя по оптоволоконной телекоммуникационной сети с учётом функционального назначения биллинга, сервера аутентификации и многоадресного вещания. Выяснено, что пользователи подключаются к свитчам доступа, которые подключены к свитчу агрегации, к которому подключены роутеры. Они соединены между собой и организовывают внутреннюю сеть провайдера, в которую пользователи получают доступ с помощью сервера аутентификации.

Также настроена точка рандеву, в которую удалённо приходят несколько видеоканалов по протоколу PIM. Из точки рандеву осуществляется мультикаст вещание видеопотока до телевизионных приставок пользователе й, при этом разрешённые в политике фильтрации MAC-адреса соответствуют распространённому оборудованию провайдера.

Практически в среде GNS3 на основе роутеров Juniper была собрана часть сети, состоящая из 2 роутеров, соединённых между собой, использующих статический NAT для реализации возможности выхода в интернет. Диапазон IP-адресов внутренней сети 10.24.0.0 – 10.24.31.0. Диапазон IP-адресов внешней сети 10.24.32.0 – 10.24.64.0. Также сеть провайдера была объединена с помощью протокола external BGP, вторая сеть выполняет роль удалённого ресурса.

**Список использоВАННыХ иСтОЧНИКОВ**

1 Juniper Networks. ACX Series Universal Access Router Configuration Guide, Inc. 1133 Innovation Way Sunnyvale, California 2015, – 12 p.

2 Питер Саусвик. Juniper networks warrior/ П. Саусвик. – O’Reilly Media, 2012, – 400 p.

3 Сэм Хелеби. Принципы маршрутизации в интернет, 2-ое изд./ Д. Мк- Ферсон, С. Хелеби. Издательский дом "Вильяме" Cisco Press, 2000, – 404 с.

4 Джонатан Луней. Auomating JunOS administration/ Д. Луней, С. Смит. – O’Reilly Media, may 2016, – 684 p.

 5 Дуглас Ричард Хэнкс. Juniper MX series/ Д. Р. Хэнкс, Х. Рэйнольдс. –O’Reilly Media, 2012, – 902 p.

6 Э. Таненбаум. Компьютерные сети. СПб. : – Питер, 2003, – 992 с.

7 Eucariot. Немного о биллинговых системах для провайдеров 07 апреля 2013 // URL: http://telekomza.ru/2013/04/07/nemnogo-o-billingovyx-sistemax-dlya-provajderov/ [21 апреля 2017]