ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«БЕЛГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ»
(Н И У « Б е л Г У »)

ИНСТИТУТ ИНЖЕНЕРНЫХ ТЕХНОЛОГИЙ И ЕСТЕСТВЕННЫХ НАУК

КАФЕДРА ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

ИССЛЕДОВАНИЕ ОСОБЕННОСТЕЙ МАРШРУТИЗАЦИИ UNICAST, BROADCAST И MULTICAST ТРАФИКА В ЛОКАЛЬНОЙ СЕТИ

Магистерская диссертация
обучающегося по направлению подготовки 11.04.02
Инфокоммуникационные технологии и системы связи,
магистерская программа «Системы и устройства радиотехники и связи»
очной формы обучения, группы 07001532
Буй Дык Хань

Научный руководитель
канд. тех. наук,
доцент кафедры
Информационно-
телекоммуникационных систем
и технологий НИУ «БелГУ»
Старовойт И. А.

Рецензент
канд. тех. наук,
доцент кафедры
информационных систем
НИУ«БелГУ»
Жихарев А. Г.

БЕЛГОРОД 2017

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Некоторое время назад, различные телекоммуникационные компании, такие как операторы подвижной связи, операторы кабельного телевидения, интернетпровайдеры, занимали разные сегменты рынка. Если первые из них предоставляли, в основном, услугу телефонии, вторые – вещательное телевидение, то последние специализировались на высокоскоростном доступе в Интернет. В настоящее время происходит конвергенция сетей, а инфокоммуникационные компании разрабатывают новые стратегии для успешного предоставления новых услуг в сетях следующих поколений. Процесс конвергенции связан с концепцией «тройная услуга» (англ. triple play), подразумевающей предоставление в одной сети одним провайдером услуг, которые можно разделить на три крупные категории – «голос», «видео» и «данные». Каждая категория фактически является крупной пакетной услугой: «голос» – IP-телефония, Skype, SIP-телефония; «видео» – IPTV, видео по запросу, потоковое P2P-видео; «данные» – передача файлов, электронная почта, обмен мгновенными сообщениями.

Трафик, генерируемый столь разнообразными услугами, пользующимися различной популярностью, различается не только по объему, но и чувствительностью к потерям пакетов, побитовой скоростью, временем передачи и пр. Потоковый (англ. streaming) трафик – это трафик реального времени с фиксированными скоростью и временем передачи. Выделяют два основных режима передачи потокового трафика – «точка – точка» и «точка – много точек»: одноадресный (англ. unicast) и многоадресный (англ. multicast) режимы передачи. Далее, для краткости, будем говорить о трех типах трафика – «одноадресный», «многоадресный» и «широковещательный».

Ввиду изложенного актуальной является задача разработки модели, методов анализа и расчета сетей с одноадресным, многоадресным и

широковещательным трафиком, предназначенных для исследования эффективности мультисервисных телекоммуникационных сетей с «тройной услугой».

Целью диссертационной работы является построение и анализ модели мультисервисной сети с тремя типами трафика – одноадресным, многоадресным и широковещательным, включая разработку методов анализа модели с многоадресным трафиком, а также точного и приближенного метода расчета отдельного звена сети с тремя типами трафика.

Сформулированная цель определила необходимость решения следующих научных задач:

1. Исследованы способы передачи данных в IP сетях. Изучены основные сведение о мультикастинге.
2. Изучены основные методы машрутизации группавых дейтаграмм.
3. Построение и анализ модели сети с типами трафика - одноадресным, многоадресным и широковещательным.

ГЛАВА 1 КЛАССИЧЕСКИЕ РЕШЕНИЯ IP - MULTICAST

При передаче данных в формате точка-многоточка, первой доступной технологией является IP-multicast. Данный подход описан в RFC 1112 и на сегодняшний день является стандартом множества индустрий:

- IP-TV – цифровое телевидение, подразумевающее доставку контента определённой группе получателей (подписчиков сервиса)
- IP – телефония аудиоконференции
- управление инфраструктурой предприятия – установка обновлений, проведение массовых изменений в локальных учётный записях пользователей.

В данной главе будут приведены принципы работы технологии IP-multicast и обоснование невозможности её использования для решения поставленной в диссертации задачи.

1.1 Основные сведения о мультикастинге

Технология IP-multicast обладает принципиальными отличиями от всем известных unicast и broadcast.

Unicast (одноадресная рассылка): один отправитель, один получатель (пример: запрос HTTP-странички у WEB-сервера). При передаче данных в режиме unicast используются классические алгоритмы маршрутизации. Данный вид передачи данных всегда базируется на использовании IP-адресов, описанных в RFC 6034 и RFC 2073.

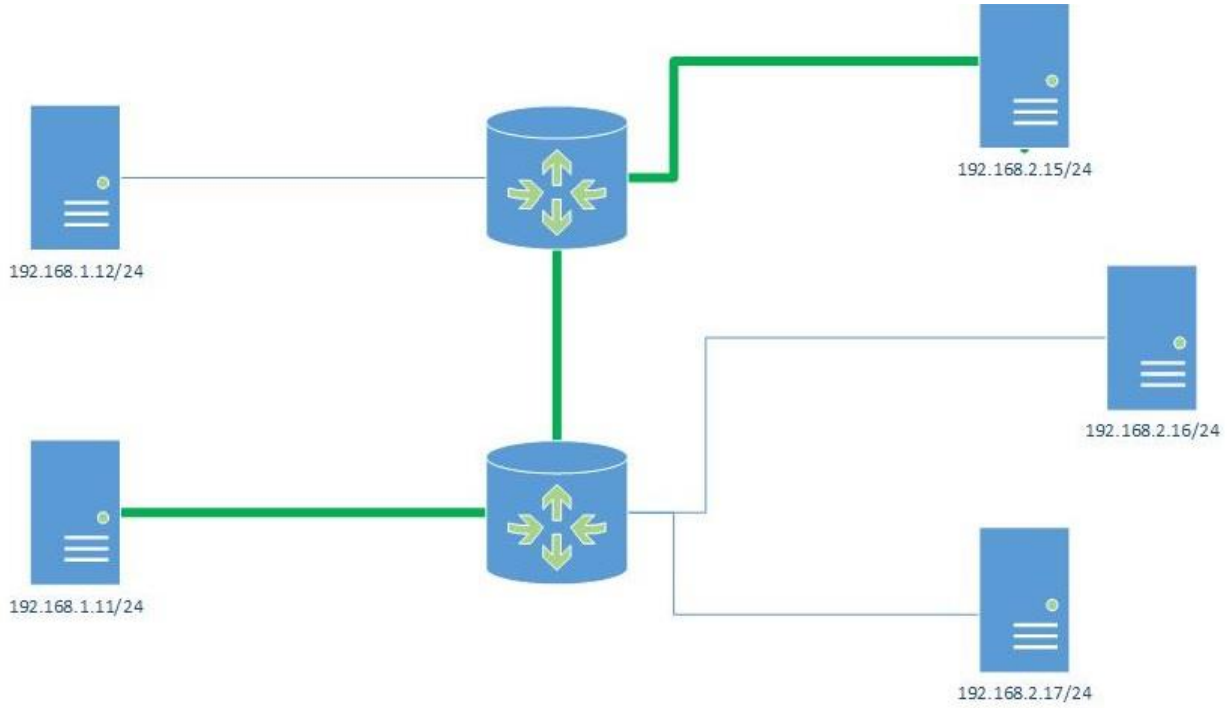

Рисунок 1.1 - Передача данных в формате точка-точка (unicast)

Broadcast (широковещательная рассылка) один отправитель, получатели все устройства в широковещательном сегменте (пример: ARP-запрос). В случае с broadcast (широковещательная передача), определённом в RFC 919, речь идёт о передаче данных от одного отправителя всем возможным получателям, а именно, всем активным (подключённым к сети) устройствам, имеющим адрес из той же подсети, что и отправитель. Отправитель в таком случае должен вести передачу на специально зарезервированный адрес, который определяется путём логической операции ИЛИ между битовым отрицанием маски подсети и адресом хоста, желающего начать передачу данных в режиме broadcast. Операцию получения broadcast адреса для определённой сети можно описать так: необходимо заменить каждый нулевой октет маски подсети на 255, например: маска 172.16.0.0, говорит о том, что областью широкого вещания (broadcast domain) для данной сети является адрес 172.16.255.255. Таким образом, отправив IP-пакет на адрес 172.16.255.255, его получит каждый хост из данной сети.

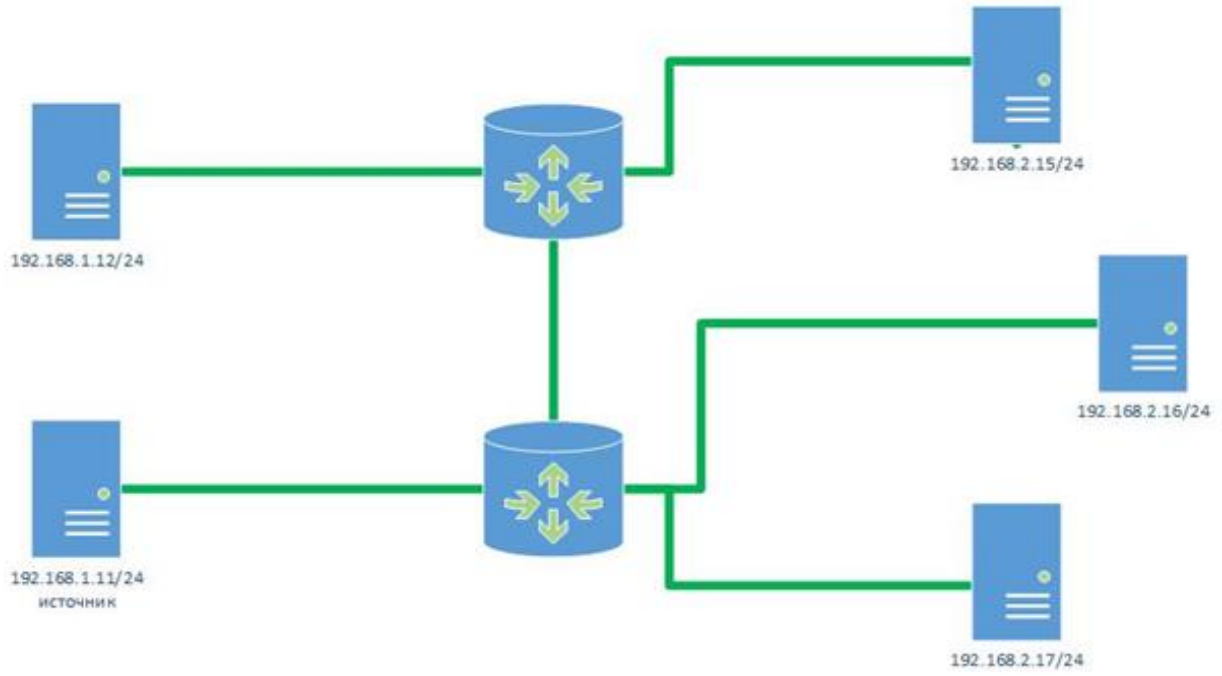

Рисунок 1.2 - Передача данных в формате от одного всем (broadcast)

Multicast (многоадресная рассылка) один отправитель, много получателей. (пример: IPTV). В случае же с multicast ситуация становиться значительно более интеллектуальной. IP-multicast подразумевает передачу данных определённой группе получателей – тех, что заинтересованы в получении определённой информации. Передача в таком случае ведётся на специальный адрес, определённый как IP-адрес группы D, а именно 224.0.0.0/4 (в случае IPv4) и . ff00::/8 (в случае IPv6).

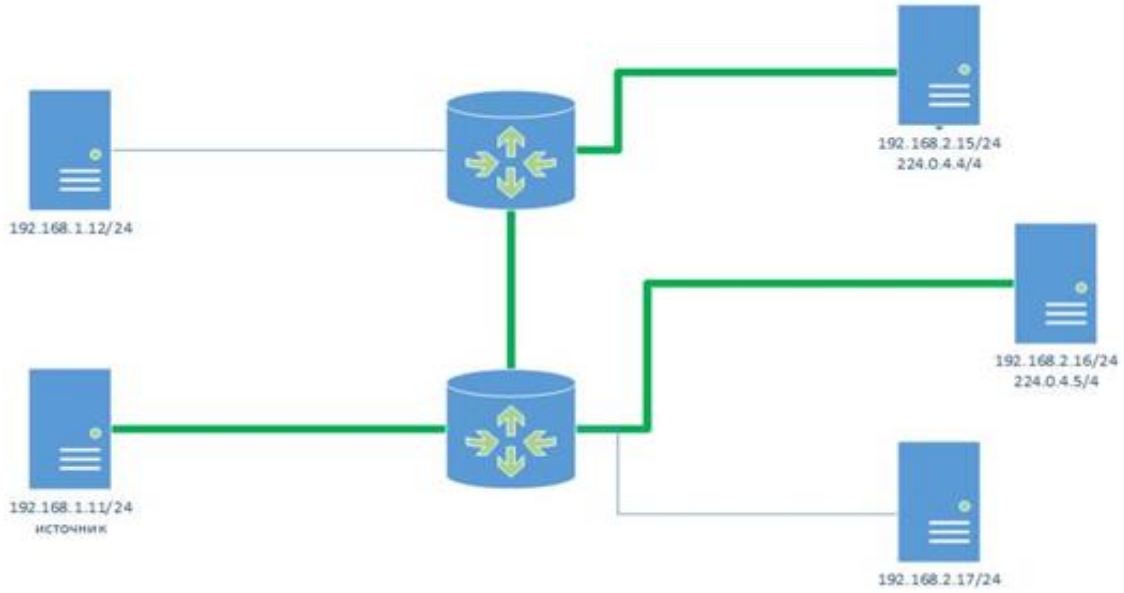

Рисунок 1.3 - Передача данных в формате точка-многоточка (multicast)

Multicast был разработан с целью снижения нагрузки на сеть путём снижения доли дублирующейся информации при передаче по сети. Иными словами, multicastреализует следующий подход: при наличии 20 получателей незачем передавать 20 пакетов, стоит передать лишь один, который, в свою очередь, будет дублироваться на промежуточных устройствах, если это необходимо. Такой подход при правильном использовании может значительно снизить нагрузку на сеть. Возьмем простой пример: Вы являетесь провайдером цифрового телевидения. Вы продали услугу Standard Definition Telefision (SDTV, стандартное разрешение телевидения). Необходимо предоставить её 20 абонентам: это фактически означает необходимость передачи 2 Мбит/с * 30 * 20 = 1200 Мбит/с (при условии вещания 30 каналов и необходимости 2 Мбит/с на канал). Наличие подобного канала связи является достаточно затратным мероприятием. Именно в связи с подобными потребностями и появился IP-multicast, позволяющий снизить нагрузку на канал. Разумеется, подобный подход подразумевает значительно более сложные механизмы, заложенные в основу процессов построения

multicast-групп и маршрутизации multicast-трафика. Базовые принципы работы технологии будут рассмотрены далее.

1.2 Преимущества групповой рассылки

Дейтаграмма, направленная на групповой адрес, должна быть доставлена всем участникам группы. В дальнейшем такие дейтаграммы будем называть групповыми. Получателей дейтаграмм с определенным групповым адресом будем называть членами данной группы.

Применения групповой рассылки дейтаграмм достаточно очевидны и перспективны: это рассылка новостей, трансляция радио- или видеопрограмм, дистанционное обучение, и т.п. Мультикастинг активно используется также и для передачи служебного трафика (маршрутной информации, сообщений службы точного времени и др.), а также для группового исполнения команд различными ЭВМ.

Групповая рассылка, по сравнению с индивидуальной, уменьшает нагрузку на сервер и на сеть.

Предположим, дейтаграмму следует отправить 500 получателям. Используя индивидуальную рассылку, отправитель должен сгенерировать 500 дейтаграмм, каждая из которых будет отправлена одному узлу. При мультикастинге отправитель создает одну дейтаграмму с групповым адресом назначения; по мере продвижения через сеть дейтаграмма будет дублироваться только на "развилках" маршрутов от отправителя к получателям.

Если развилок немного, например, все получатели в одной сети Ethernet, – экономия трафика будет 500-кратной. При этом сохраняются и вычислительные ресурсы промежуточных узлов.

1.3 Недостатки групповой рассылки

Недостатком групповой рассылки является очевидная невозможность использования на транспортном уровне протокола TCP. Использование протокола UDP (часто вместе с RTP) влечёт за собой все их недостатки: ненадежность доставки, отсутствие средств реагирования на заторы в сети и т.д.

Кроме того, в отдельных случаях при изменении маршрутов рассылки групповые дейтаграммы могут теряться и дублироваться, и это должно учитываться приложениями.

Построение составной сети с поддержкой мультикастинга является гораздо более сложной задачей, чем организация групповой рассылки в пределах одной IP-сети.

Для мультикастинга нужна специальная собственная маршрутизация.

Для продвижения групповых дейтаграмм от отправителя к получателям через систему сетей необходимо осуществлять маршрутизацию дейтаграмм. Однако по групповой дейтаграмме нельзя определить индивидуальные IP-адреса ее получателей, следовательно, использование обычной IP-маршрутизации и даже её принципов не имеет смысла. Поэтому для маршрутизации групповых дейтаграмм были разработаны специальные методы и протоколы маршрутизации, которые будут рассмотрены ниже.

Не все провайдеры Internet поддерживают мультикаст-связность.

1.4 Требования к сети, адресация

Для использования мультикаста, он должен поддерживаться в стеке TCP/IP сервера, клиентов и промежуточных маршрутизаторов. В LAN управлением мультикаст-группами занимается IGMP, в глобальной сети – PIM (Protocol Independent Multicast).

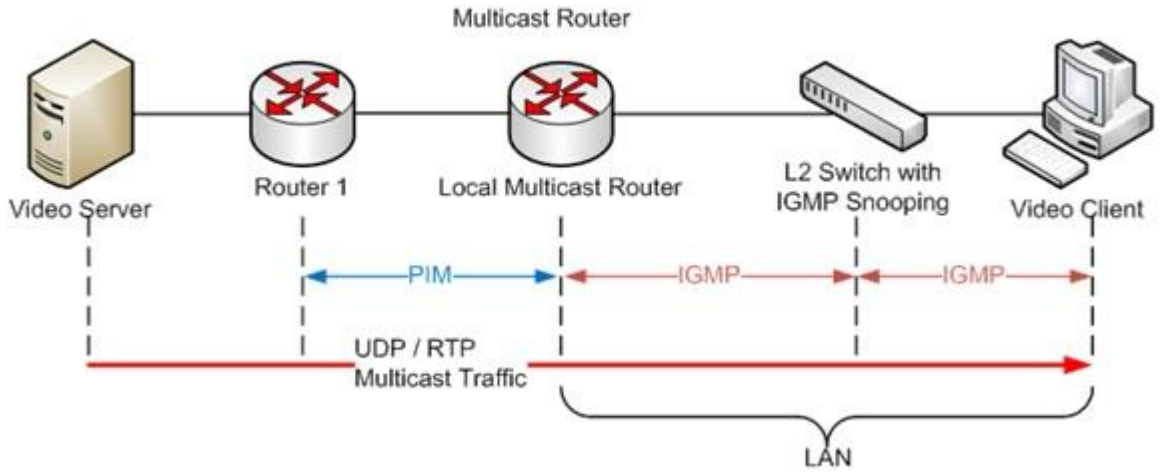

Рисунок 1.4 - Моделируемая сеть.

Для участия в мультикасте хост локальной сети должен иметь мультикаст программу (например, VideoClient). Чтобы коммутаторы посылали пакеты только нужным получателям (multicast), они должны поддерживать IGMP snooping. Без функции IGMP snooping коммутатор ретранслирует multicast трафик по всем своим портам и данные направляются всем устройствам сети, независимо от их вхождения в группы.

Рисунок 1.5 - Flooding трафик

Для работы мультикастинга необходима также групповая или широковещательная рассылка на уровне доступа к сети, поэтому мультикастинг-адресация может осуществляться и на IP- и на MAC-уровнях

Групповые адреса на уровне IP.

Для идентификации групп на сетевом уровне используются специальные адреса получателя. В IPv4 для мультивещания зарезервирована подсеть 224.0.0.0/4; это адреса из класса D в диапазоне 224.0.0.0 – 239.255.255.255. В IPv6 используются адреса FF00::/8. Адреса в диапазоне 224.0.0.0 – 238.255.255.255 предназначены для использования в масштабе Интернет. Адреса вида 239.X.X.X зарезервированы для внутреннего использования в частных сетях.

Некоторые из групповых адресов зарезервированы строго для специальных групп (см. RFC-1700). Например:

Таблица 1.1 - Мультикастинг адрес

Мультикастинг адрес	Описание
224.0.0.0 224.0.0.255	Local Network Control Block
224.0.0.0	Зарезервировано
224.0.0.1	Все системы данной субсети
224.0.0.2	Все маршрутизаторы данной субсети
224.0.0.4	Все DVMRP-маршрутизаторы
224.0.0.5-224.0.0.6	OSPF IGP (MOSPF) -маршрутизаторы
224.0.0.9	Маршрутизаторы RIP2
224.0.0.10	IGRP маршрутизаторы
224.0.0.251	Multicast DNS address
224.0.1.0 224.0.1.255	Internetwork Control Block
224.0.1.0	VMTP-группа менеджеров
224.0.1.1	получатели информации по NTP-network time
224.0.1.6	NSS - сервер имен
224.0.1.7	Audionews - audio news multicast (аудио служба
224.0.1.9	MTP (multicast transport protocol)
224.0.1.10	IETF-1-low-audio
224.0.1.11	IETF-1-audio
224.0.1.12	IETF-1-video
224.0.1.20	Любой частный эксперимент
224.0.1.24	microsoft-ds
224.1.0.0-	ST мультикастинг-группы
224.2.0.0-	Вызовы при мультимедиа- конференциях
232.0.0.0-	VMTP переходные группы

Групповые адреса на уровне MAC.

В MAC для мультикастинга IANA зарезервировала блок адресов в диапазоне от 01:00:5E:00:00:00 до 01:00:5E:7F:FF:FF. Первый байт адреса, равный 01, указывает на то, что адрес является мультикастным.

Данная схема резервирования адресного пространства позволяет использовать 23 бита MAC- адреса для идентификации группы рассылки при IP-мультикастинге (см. рис.).

IP адреса резервируются первыми 4 битами 1110 (см. рис 1.6). Область из 5 бит, отмеченная в IP - адресе 01111, не используется в формировании MAC-адреса.

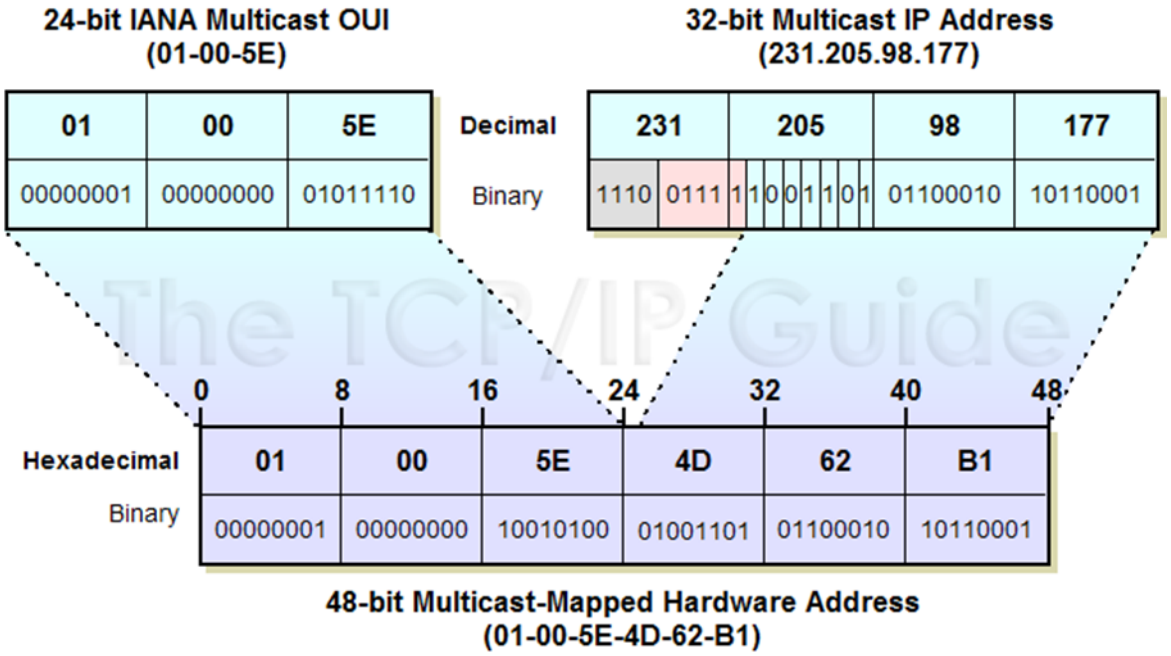

Рисунок 1.6 - Соотношение мультикастинговых MAC- и IP-адресов

Т.о. групповому IP-адресу 224.205.98.177 на уровне сети будет соответствовать MAC-адрес 01:00:5E:4D:62:B1 на уровне Ethernet.

Необходимо отметить, что это соответствие не является однозначным: IP-адреса с 224.205.98.177 до 239.205.98.177 и с 224.77.98.177 до 239.77.98.177 будут преобразованы в тот же MAC-адрес 01:00:5E:4D:62:B1.

Так как соотношение IP и MAC-адресов не является однозначным, драйверы должны обеспечивать специфичную обработку адресов с тем, чтобы интерфейсы получали только те кадры, которые действительно им предназначены.В Windows просмотреть arp таблицу и просмотреть членство в мультикастных группах можно командами arp –a и netsh interface ipv4 show joins; в Linux arp -a и netstat –g.

ГЛАВА 2 ОСНОВЫ О МАРШРУТИЗАЦИИ IP – MULTICAST

На основе описанной концепциидля стека TCP/IP был разработан ряд протоколов, с помощью которых можно организовать групповое вещание с различной степенью эффективности. Эти протоколы делятся на две категории.

- В первую входит один протокол — протокол IGMP, с помощью которого, во-первых, хосты сообщают о своем «желании»1 присоединиться к некоторой группе, во-вторых, маршрутизатор узнает о принадлежности хостов в непосредственно подключенных к нему подсетях к той или иной группе. Протокол IGMP работает в тесном взаимодействии с протоколами второй категории — протоколами маршрутизации группового вещания.
- Протоколы маршрутизации группового вещания необходимы для продвижения пакетов, несущих в себе информацию для групповых получателей, через сеть произвольной конфигурации. Эти протоколы — DVMRP, MOSPF, PIM — опираются на разные подходы, но в конечном итоге все они сводятся к построению графа, связывающего все хосты в определенной группе, причем между двумя хостами существует только один путь. Такой граф называют покрывающим деревом. Протоколы маршрутизации осуществляют постоянный мониторинг покрывающего дерева и время от времени отсекают те ветви дерева, которые из-за изменения состояния сети уже не ведут к членам той или иной группы.

Принципы маршрутизации трафика группового вещания

Среди принципов маршрутизации трафика группового вещания можно отметить:

- маршрутизацию на основе доменов
- учет плотности получателей группового трафика

• два подхода к построению маршрутного дерева.Два подхода к построению маршрутного дерева. Как и при решении задачи маршрутизации на основе индивидуальных адресов, в сети с групповым вещанием маршрутизаторы анализируют топологию сети, пытаясь найти кратчайшие пути доставки данных от источников к получателям. При этом все протоколы маршрутизации группового вещания используют один из следующих двух подходов.

• Концепция продвижения по реверсивному пути — это еще одна концепция, которую необходимо понять всем, кто реализует групповое вещание. Механизм, используемый для маршрутизации трафика группового вещания, в определенном аспекте является прямо противоположным (реверсивным) тому механизму, который применяется для продвижения обычного трафика на основе индивидуальных адресов. Концепция продвижения по реверсивному пути является главной при маршрутизации группового трафика независимо от того, какой протокол при этом использова.

Принципы работы multicast

В основу работы технологии multicast легли два основных принципа:

• возможность гибкого и масштабируемого управления multicast группами – для реализации динамического построения групп получателей.

• возможность маршрутизации multicast-пакетов – для обеспечения возможности автоматического построения эффективной таблицы маршрутизации multicast трафика.

На данном этапе, подходим к основополагающим протоколам стека технологий IP-multicast:

• IGMP (The Internet Group Management Protocol) – протокол управления multicast группами;

• PIM (Protocol Independent Multicast) – протокол маршрутизации multicast трафика.

Для маршрутизации multicast трафика существует специальный протокол PIM. В свою очередь PIM имеет два режима работы:

- PIM-DM (dense mode) или режим рассылки и отсечения;
- PIM-SM (sparse mode) или режим, при котором рассылка начинается только тогда, когда появляется запрос на членство в группе.

Сети класса D (224.0.0.0/4) зарезервированы для использования мультикастом. Адресное пространство рассматривается как "плоское", поскольку мультикастовые группы не разбиваются на подсети и не обязательно распределяются привычным иерархическим образом. Мультикастовые MAC-адреса формируются добавлением к "01-00-5e" последних 23-х битов идентификатора (IP-адреса) группы.

2.1 Протокол IGMP

Протокол IGMP играет в сети вспомогательную роль. Между роутерами, рассылающими мультикаст, и хостами, получающими его, работает Internet Group Membership Protocol (IGMP).

Протокол IGMP (Internet Group Management Protocol) предназначен для регистрации на маршрутизаторе членов групп, находящихся в непосредственно присоединенных к нему сетях (в LAN). Имея эту информацию, маршрутизатор может сообщать другим маршрутизаторам (с помощью протоколов групповой маршрутизации DVMRP, MOSPF, PIM, CBT) о необходимости пересылки ему дейтаграмм для групп.

Область рассылки IGMP-пакетов ограничена исключительно локальными линками. IGMP существует 3-х версий (1, 2 и 3).

- IGMP v1 - RFC-1112
- IGMP v2 - RFC-2236
- IGMP v3 - RFC-3376

IGMPv2

Типы сообщений IGMPv2:

- Membership Report - сообщает, что хост желает присоединиться к группе
- IGMPv1 Membership Report - для обратной совместимости с первой версией протокола
- Leave Group - сообщает, что хост покинул группу

Сообщение о членстве в группе адресуется мультикастовой группе с той целью, чтобы его получили все роутеры и другие члены группы в этом сегменте. Сообщения о прекращении членства рассылаются исключительно мультикастовой группе "все маршрутизаторы" (all routers, 224.0.0.2).

Маршрутизаторы могут отправлять в отдельную подсеть два типа запросов:

- General - общий запрос, для обнаружения членов любой группы; рассылается всем хостам (224.0.0.1)
- Group-specific - групповой запрос, отправляется на адрес группы с целью обнаружения членов этой группы

По-умолчанию общие запросы рассылаются каждые 60 секунд (значение меняется командой ip igmp query-interval). В запросе содержится величина максимального времени отклика (Max Response Time, по-умолчанию 10 секунд), показывающая, как долго маршрутизатор будет ожидать ответа. Маршрутизатор прекращает отправлять трафик группе по истечению трех таких интервалов.

Групповые запросы рассылаются в ответ на полученное сообщение о прекращении членства от члена группы. Запросы рассылает маршрутизатор, являющийся активным. Активным для отдельной подсети является маршрутизатор с наименьшим IP-адресом. Если другой маршрутизатор в подсети не слышит запросы от активного опрашивателя по истечению

заданного периода (по-умолчанию 120 секунд) - он принимает на себя эту роль. Этот интервал настраивается командой ip igmp query-timeout.

IGMPv1

IGMPv1 отличается от второй версии несколькими моментами:

- отсутствует сообщение о прекращении членства в группе;
- нет групповых запросов от маршрутизатора;
- таймер Max Response Time неизменно равен 10 секундам;
- выборы активного опрашивателя проводятся протоколом маршрутизации мультикаста.

Хосты с IGMPv2 распознают ответы версии IGMPv1 и будут отвечать на запросы IGMPv1 ответами этой же версии. Маршрутизатор IGMPv2 будет работать в режиме IGMPv1 до тех пор, пока в группе будет член IGMPv1.

IGMPv3

IGMPv3 предоставляет возможность групповых запросов и фильтрации в зависимости от источника трафика.

CGMP

Cisco Group Membership Protocol (CGMP) использовался для отправки сообщений о членстве в группах L2-коммутаторам с целью эффективного форварда группового трафика. В современных коммутаторах для этого используется IGMP Snooping.

Формат IGMP дейтаграммы

IGMP работает непосредственно поверх IP, и идентифицируется значением поля "Protocol" = 2 в заголовке IP-дейтаграммы.

По умолчанию мультикаст-дейтаграммы имеют значение поля TTL=1, что ограничивает их распространение одной субсетью.

Приложения могут увеличивать значение TTL. Первая дейтаграмма, тем не менее, всегда имеет TTL=1. Если получение этой дейтаграммы не

подтверждается сервером, посылается вторая - с TTL=2 и т.д. Попутно измеряется и число шагов между клиентом и сервером.

Для случая, когда число шагов не более 1 (для LAN), зарезервирован блок IP адресов 224.0.0.0 - 224.0.0.255. Маршрутизатор не обрабатывает пакеты с такими адресами.

За IP-заголовком в дейтаграмме следует сообщение IGMP:

0 7	15	23	31
Type	Max Response Time	Checksum	
Group Address			

- Type (8 бит) – тип сообщения, если начинается с 1, то это запрос, отправленный мультикастинг-маршрутизатором, с 2 указывает, что это отклик посланный узлом.
- Max Response Time (8 бит) – максимальное время отклика, задействовано только в сообщениях типа Membership Query (в IGMPv1 не использовалось и ставилось в 0).
- Checksum (16 бит) – контрольная сумма.
- Group Address (32 бита) – групповой IP-адрес.

Существуют следующие типы сообщений:

- Membership Query (Type=17) – запрос о наличии в сети членов групп (отправляется маршрутизатором). Запросы обо всех имеющихся группах – общие запросы – отправляются по адресу 224.0.0.1 ("всем узлам"); запросы о наличии членов определенной группы – частные запросы – отправляются по адресу этой группы.
- Membership Report (Type=22) – уведомление о наличии в сети члена группы (отправляется хостом – членом группы по адресу группы).
- Leave Group (Type=23) – уведомление об отсоединении хоста от группы (отправляется отсоединившимся хостом по адресу 224.0.0.2 – "всем маршрутизаторам").

2.2 Маршрутизация мультикаста

Для маршрутизации мультикаста есть пять IGP:

- Distance Vector Multicast Routing Protocol (DVMRP)
- Multicast OSPF (MOSPF)
- Core-based Trees (CBT)
- Protocol Independent Multicast Dense Mode (PIM-DM)
- Protocol Independent Multicast Sparse Mode (PIM-SM)

В IOS полностью поддерживается только PIM.

Групповые маршруты формируются из пар (источник, группа). Мультикаст всегда должен распространяться от источника. Для устранения петель протоколы маршрутизации мультикаста используют механизм reverse path forwarding, используя для ориентира адрес отправителя. Получив пакет из какого-либо интерфейса, маршрутизатор проверяет по своей маршрутной таблице, доступен ли отправитель пакета через этот интерфейс. Если да - пакет форвардится дальше, через другие интерфейсы (кроме того, с которого был получен), если нет - пакет отбрасывается.

"Плотный" (dense) против "разреженного" (sparse) режима

Топология, в которой на групповой трафик подписан большой процент хостов, зовется "плотной" (dense). Соответственно, "разреженная" (sparse) топология - относительно небольшое количество мультикастовых адресатов. В плотной топологии используются DVMRP, MOSPF и PIM-DM. В разреженной - CBT и PIM-SM.

Неявное против явного присоединения

Мультикастовое дерево маршрутизации строится исходя из неявных (implicit) либо явных (explicit) присоединений.

Неявные присоединения используются, когда дерево первоначально охватывает все роутеры в сети, а затем урезается только до тех сегментов, в

которых присутствуют интересующие хосты. Дерево (и рассылка трафика) снова охватывает всех, а затем снова обрезается на регулярной основе.

Явные присоединения используются для постепенного роста мультикастового дерева с целью включения в него всех нужных хостов.

Неявные присоединения применяются в DVMRP и PIM-DM; явные - в MOSPF, CBT и PIM-SM.

Дерево, строящиеся от источника, против общих деревьев

Корень деревьев, строящихся от источника (source-based), как ясно из названия, размещается непосредственно в источнике трафика мультикастовой гуппы, и далее деревья строятся в сторону получателей этой группы. Для каждой группы строится отдельное дерево.

Корень общих (shared) деревьев размещается на общем для множества мультикастовых групп роутере, размещенном в выгодной точке сети и зовущемся точкой рандеву (rendezvous point, RP). Общие деревья помечаются маршрутом (*, G).

Общие деревья, хотя и эффективны с точки зрения маршрутизации, не всегда предоставляют оптимальный маршрут от источника до получателя, т. к. весь трафик сперва проходит через RP. В протоколах плотной (dense) топологии используются деревья, строящиеся от источника, в разреженной (sparse) используются общие деревья.

Диапазоны

Для ограничения доступности группового трафика применяются мультикастовые диапазоны.

Диапазон на базе TTL устанавливает TTL-пороги на маршрутизирующих интерфейсах. Мультикастовые пакеты с TTL ниже порога не форвардятся

Административный диапазон устанавливает индивидуальные границы распространения группового трафика для источников из зарезервированной области (239.0.0.0/8).

2.2.1 Протокол PIM DM

PIM (Protocol Independent Multicast) – два протокола групповой маршрутизации (для плотного и разреженного расположения членов групп, соответственно dense mode и sparse mode), не зависящие от используемого протокола обычной маршрутизации.

PIM DM используется в системах сетей с большой плотностью получателей. Этот протокол реализует метод RPF с усечением (немодифицированный, то есть без доступа к внутренним таблицам протокола маршрутизации, вследствие чего достигается независимость от протокола маршрутизации). Необходимость периодической посылки "пробных" дейтаграмм не является существенным недостатком при плотном расположении получателей.

Протокол PIM DM прост в реализации и в настройке, предусмотрено взаимодействие с протоколом DVMRP.

В качестве недостатка отметим необходимость рассылать пробные дейтаграммы каждые 3 минуты, так как за это время истекает срок действия сообщения Prune.

Протокола PIM DM могут возникнуть две особые ситуации.

Ситуация 1 в PIM DM

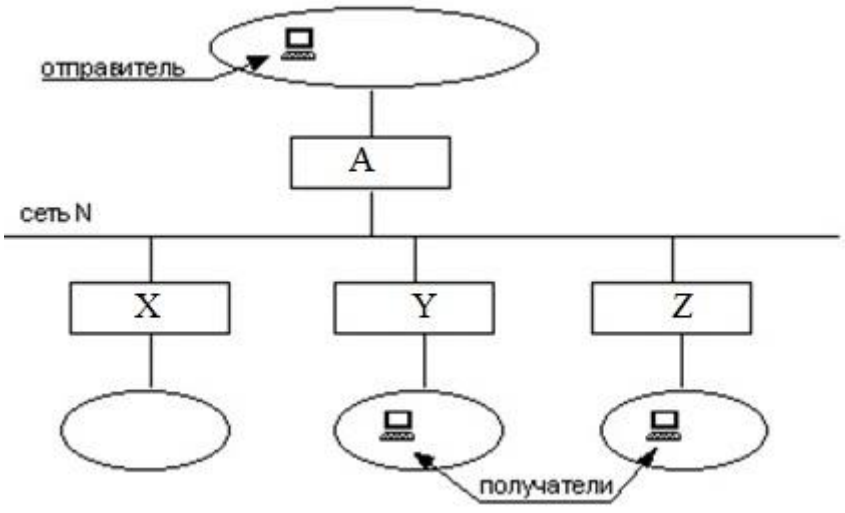

Рисунок 2.1 - Ситуация 1 в PIM DM

Несколько маршрутизаторов подключены к одной широковещательной сети N, которая через вышестоящий маршрутизатор X соединяется с системой сетей, в которой находится отправитель Y сетях,подключенных к маршрутизаторам Y и Z, находятся члены группы, а в сети, подключенной к маршрутизатору X – нет.

Вышестоящий маршрутизатор X посылает в сеть N первую групповую дейтаграмму. Маршрутизатор X откликается сообщением Prune, однако отсекать сеть N от дерева рассылки нельзя, так как есть получатели в сетях Y и Z. Протокол предлагает следующее решение: маршрутизатор , получив Prune, запускает таймер. Маршрутизаторы Y и Z, прослушивая сеть, обнаруживают посланное узлом X Prune, и тут же один из них отправляет сообщение Join Маршрутизатор X, приняв Join, игнорирует предыдущий Prune. Если же за определенное время сообщение Join не будет принято, сеть N отрезается от дерева рассылки

Ситуация 2 в PIM DM

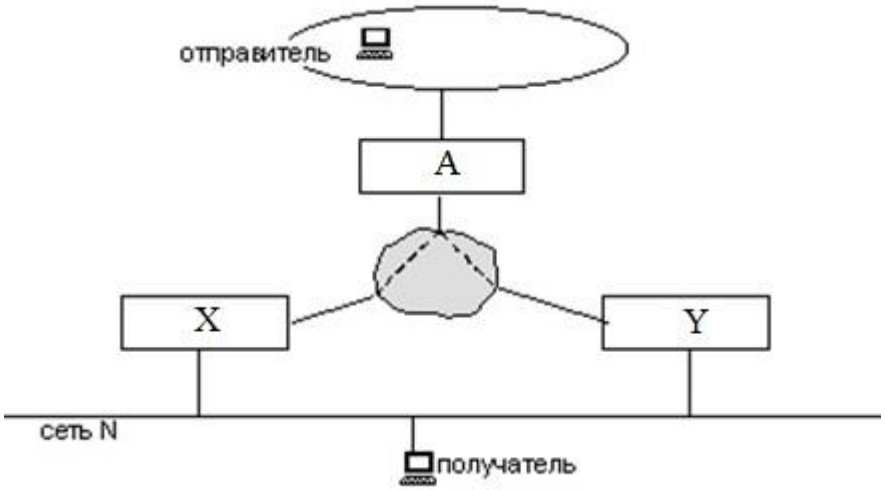

Рисунок 2.2 - Ситуация 2 в PIM DM

Вторая ситуация возникает, когда два маршрутизатора X и Y подключены к одной и той же клиентской сети N, в которой находится получатель.

Оба маршрутизатора будут отправлять групповые дейтаграммы в сеть N, так как им известно, что в ней находится получатель. Очевидно, что при этом создается избыточный трафик из лишних экземпляров дейтаграмм. Во избежание этого эффекта маршрутизатор, обнаружив, что в сети N действует конкурирующий маршрутизатор Y, также рассылающий групповые дейтаграммы от источника S в группу X, посылает сообщение Assert, содержащее расстояние от X до S. Конкурирующий узел Y, получив это сообщение, сравнивает расстояние от себя до S с указанным в сообщении, и если свое расстояние больше, то соответствующий интерфейс отрезается от дерева с помощью Prune. Аналогичным образом посылается и обрабатывается assert из Y в X. При равных расстояниях побеждает маршрутизатор с большим IP-адресом.

В PIM-DM (v2) используются пять типов сообщений (сообщения взяты из области садоводства, похоже, в связи с выращиванием мультикастовых деревьев):

- Hello
- Join/Prune (присоединение/обрезание)
- Graft (прививание)
- Graft-Ack (подтверждение прививания)
- Assert (утверждение)

По-умолчанию hello-пакеты рассылаются каждые 30 секунд (настраивается командой ip pim query-interval) во все PIMv2-интерфейсы. Время задержки (hold time) в каждом пакете выставлено в 3.5 hello-интервала (т. е. по-умолчанию 105 сек). В PIMv1-интерфейсы вместо хелло рассылаются запросы.

Сообщения об "обрезании" (prune) являются мультикастом от маршрутизаторов к группе 224.0.0.13. У каждого мультикастового маршрута есть два таймера: время нахождения в таблице и время устаревания (экспирации). Маршрут удаляется из таблицы, если для пары источник-

группа (S, G) не передается мультикастовый трафик в течение времени экспирации. "Обрезанные" интерфейсы не форвардят мультикаст 210 секунд, после чего трафик рассылается снова. Нижестоящий маршрутизатор должен снова запросить, чтобы его удалили из дерева.

Сообщение "прививания" (graft) отправляется юникастом вышестоящему соседу с целью снова присоединиться к мультикастовому дереву. Этот сосед включает передачу трафика в сторону просителя и отвечает сообщением "подтверждение прививания" (graft-ack).

Перед тем как отключить интерфейс при получении "обрезания" апстрим-роутер будет ждать 3 секунды. Что дает возможность другим роутерам, находящимся за отключаемым интерфейсом, так же увидеть запрос-"обрезание" (оно распространяется мультикастом всему сегменту) и организовать отмену обрезания "prune override". Отмена производится путем отправки вышестоящему роутеру нового сообщения о присоединении.

Маршрутизатор с наивысшим IP-адресом в групповом сегменте становится назначенным маршрутизатором (designated router, DR). DR является опрашивателем для IGMPv1 (т. к. непосредственно в IGMPv1 отсутствует процедура выборов опрашивателя).

Сообщения "утверждения" (assert) используются для назначения отправителя (forwarder) при наличии нескольких роутеров, имеющих маршрут из одного сегмента в другой. Отправителем становится маршрутизатор, объявляющий наиболее предпочтительный (определяется наименьшей административной дистанцией/наименьшей метрикой/наибольшим IP) юникастовый маршрут.

2.2.2 Протокол PIM-SM

Протокол PIM SM (Protocol Independent Multicast, Sparse mode) применяется для маршрутизации дейтаграмм для малочисленных групп,

члены которых находятся далеко друг от друга (в этом случае недостатки метода RPF с усечением становятся существенными).

Функционирование протокола можно кратко описать как метод CBT, переходящий в RPF. Вместо флудинга, как в PIM DM, в PIM SM выбирается один маршрутизатор, который будет хранить информацию о группах и источниках. Это обычный маршрутизатор PIM SM, который выполняет роль Rendezvous Point (RP). Все маршрутизаторы в домене PIM SM должны знать, кто выполняет роль RP. Маршрутизатор, в сети которого зарегистрировались члены группы, посылает в RP сообщение Join, которое обрабатывается промежуточными маршрутизаторами как в технологии CBT – таким образом формируется первоначальное дерево рассылки.

Отправитель дейтаграмм посылает в RP сообщения Register, в которых инкапсулируются групповые дейтаграммы. RP извлекает дейтаграммы из этих сообщений и рассылает их по сформированному дереву рассылки. Если отправитель работает достаточно интенсивно, то RP посылает в его сторону сообщение Join – то есть, отправитель становится членом группы и может рассылать групповые дейтаграммы по дереву непосредственно, минуя стадию туннелирования в точку рандеву.

Распространение групповых дейтаграмм по дереву рассылки осуществляется аналогично методу CBT: дейтаграмма рассылается через все интерфейсы, принадлежащие дереву.

Далее маршрутизатор может заметить, что интенсивность этого потока превышает некоторый установленный лимит. В этом случае маршрутизатор решает оптимизировать дерево рассылки. Он посылает сообщение Join к источнику следующей полученной им дейтаграммы, адресованной данной группе, а в точку рандеву посылается сообщение PruneТаким образом, дерево, изначально созданное вокруг точки рандеву, оптимизируется для данного источника.

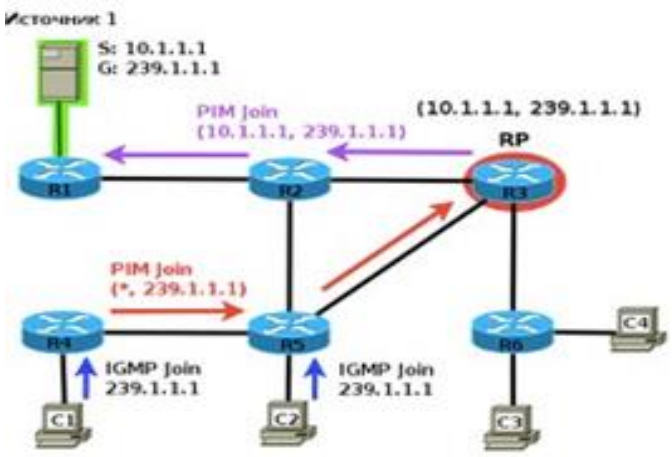

Рисунок 2.3 - Пример машрутиратор с пртоколом PIM-SM

Следует отметить, что переход к дереву, оптимизированному для источника, приводит к необходимости хранить и обрабатывать на маршрутизаторах большее количество служебной информации, что не всегда приемлемо, поэтому существует возможность отключения такого перехода.

Предусмотрен также обратный переход к дереву с корнем в точке рандеву. Он производится, если оптимизация дерева оказалась неоправданной

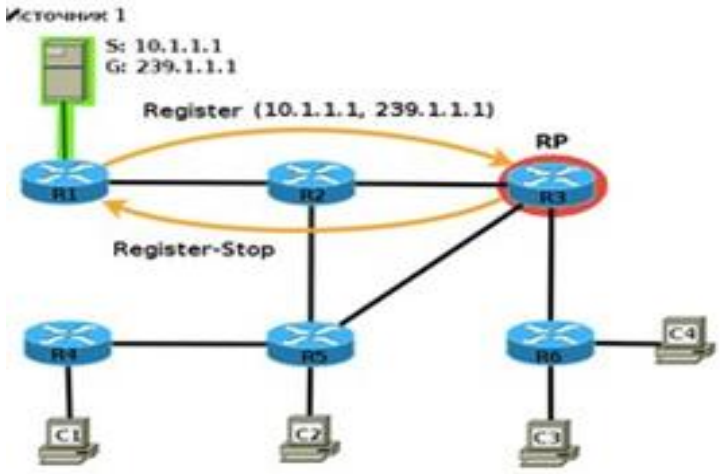

Рисунок 2.4 - Обратный переход к дереву с корнем в точке рандеву

В PIM-SM используются семь видов сообщений PIMv2:

- Hello
- Bootstrap (начальная загрузка)
- Candidate RP Advertisement (объявление RP-кандидата)
- Join/Prune
- Assert
- Register (регистрация)
- Register-stop (прекращение регистрации)

Здесь общее дерево строится от точки рандеву (rendezvous point, RP), определяемой одним из трех способов:

- Статические настройки на маршрутизаторах
- Стандартизованный протокол начальной загрузки (bootstrap)
- Механизм Auto-RP, являющийся собственностью Cisco

Auto-RP

Auto-RP является предшественником bootstrap-протокола и отличается от него несколькими моментами:

- Auto-RP является собственностью Cisco
- Вместо списка кандидатов используются т. н. RP-агенты, которые не выбираются из списка, а назначаются
- RP-агенты вместо рассылки RP-set привязывают группы к IP-адресам точек рандеву.
- В Auto-RP вместо 224.0.0.13 используются группы Cisco-RP-Announce (224.0.1.39) и Cisco-RP-Discovery (224.0.1.40)

Анонсы рассылаются каждые 60 секунд.

Общие деревья

Запись мультикастового маршрута в случае с общим деревом не привязана к конкретному источнику, вместо записи (S-источник, G-группа) используется (*, G). Перед присоединением к группе, маршрутизатор PIM-SM предпринимает ряд действий:

- Для интерфейса, требующего трафик для группы (исходя из запросов IGMP Join), создается маршрут (*, G)
- Затем проверяется таблица соответствия "группа-RP" для определения адреса точки рандеву для группы
- В юникастовой маршрутной таблице ищется путь к RP
- После чего точке рандеву отправляется сообщение Join/Prune с запросом о присоединении к группе

Вышестоящие маршрутизаторы после получения запроса на присоединение добавляют просителя в мультикастовое дерево для этой группы (если оно уже есть на этом маршрутизаторе), либо рассылают по направлению к RP свой собственный запрос на присоединение. Этот процесс продолжается до тех пор, пока запрос не попадет к маршрутизатору, включенному в дерево для этой группы, или пока не попадет к самой точке рандеву.

RP создает маршрут (*, G) для дерева даже в том случае, если источник трафика для группы неизвестен. Для поддержание дерева в актуальном состоянии сообщения "Join/Prune" рассылаются каждые 60 секунд (настраивается командой ip pim message-interval). Точно так же, как и в PIM-DM, в групповых сегментах используется "отмена обрезания" (prune overriding).

Регистрация источника и SPT (Shortest Path Tree)

Для правильной проверки RPF общие деревья, строящиеся в PIM-SM, должны быть однонаправлены, т. е. трафик должен идти от RP только вниз по дереву. Поэтому мультикастовый трафик от источника должен попадать в точку рандеву без использования общего дерева группы. Поэтому когда источник первоначально отправляет групповой трафик, маршрутизатор, к которому непосредственно подключен источник, инкапсулирует пакеты в register-сообщение и отправляет их юникастом в сторону RP. Таким образом удается избежать нарушения проверки RPF.

RP после получения трафика, инкапсулированного в register-сообщении, рассылает декапсулированный трафик вниз по дереву и записывает мультикастовый маршрут (S, G). После чего строит SPT до источника и отправляет сообщение "Register Stop" маршрутизатору, отправлявшему Register, чтобы тот перестал инкапсулировать мультикаст. Маршрутизаторы, к которым подключены непосредственные члены группы, могут также строить независимые SPT до источника, если обнаруживают в своей таблице лучший маршрут по сравнению с общим деревом.

По-умолчанию маршрутизатор Cisco будет переключаться на SPT при первой возможности. Командой ip pim spt-threshold (по-умолчанию 0) можно задать порог срабатывания (в kbps трафика группы). Предотвратить переключение на SPT можно, установив значение порога infinity.

2.2.3 Протокол DVMRP

Дистанционно-векторный протокол маршрутизации группового вещания (анг, Distance Vector Multicast Routing Protocol, DVMRP), описанный в спецификации RFC 1075, может быть характеризован с самых общих позиций следующим образом:

- как следует из его названия, он основан на дистанционно-векторном алгоритме и, следовательно, обладает всеми особенностями, свойственными данному алгоритму;
- является протокольно зависимым в том смысле, что для принятия решений о продвижении пакетов он не может использовать обычные таблицы маршрутизации.
- относится к классу протоколов плотного режима, использующих проверку продвижения по реверсивному пути;

Протокол DVMRT был одним из первых протоколов продвижения группового трафика в исследовательской сети MBone. Групповая

маршрутизация в ранней версии MBone была, в сущности, управляемой формой широковещания, когда пришедший пакет с групповым адресом передавался через все интерфейсы, кроме входного. Для борьбы с зацикливанием пакетов с групповыми адресами маршрутизаторы запоминали факт продвижения данного пакета и при его поступлении в следующий раз просто отбрасывали. Для сокращения бесполезного трафика в сети применялся протокол IGMP. С помощью этого протокола маршрутизаторы выясняли, имеются ли в непосредственно подключенных к нему сетях конечные узлы, принадлежащие к определенной группе, или нет. В том случае, когда маршрутизатор определял, что к некоторому интерфейсу подключена сеть, в которой нет членов группы, являющихся получателями группового пакета, он не передавал копию этого пакета чрез данный выходной интерфейс.

Недостатки DVMRP

- Эффективно работает в «плотно» населенных мультикаст-группами сетях (dense mode).
- Маршрутизатор должен хранить большое количество информации – пропорционально количеству источников – для каждого источника свое дерево
- В разряженных сетях (space mode) протокол DVMRP порождает много избыточного трафика: за счет затопления сети на этапы существования неусеченного дерева; за счет служебного трафика DV, требуеого для построения таблицы маршрутизации (протокол работает независимо от протокол обычной маршрутизации).

2.2.4 Протокол MOSPF

Протокол MOSPF (Multicast Open Shortest Path First: расширения протокола OSPF для группового вещания), протокол MOSPF описан в документе RFC 1584, опирается на обычные механизмы OSPF для поддержки группового вещания. MOSPF маршрутизаторы добавляют к информации о состоянии связей, распространяемой по протоколу OSPF, данные о членстве в группах узлов в непосредственно присоединенных сетях. Эти данные рассылаются по сети в дополнительном сообщении о членстве в группе. В результате помимо топологии связей, MOSPF-маршрутизаторам становится известно о наличии членов каждой из групп в каждой подсети области. На основании этой информации маршрутизатор находит дерево кратчайших путей для каждой группы. Это позволяет распространять групповые пакеты не широковещательно, а по кратчайшим путям от источника до подсетей, в которых есть активные члены группы.

Для получения данных о том, в какие группы входят конечные узлы в связанных с ним подсетях, MOSPF маршрутизатор использует запросы и ответы протокола IGMP. При каждом подключении узла к группе или исключении узла из группы маршрутизатор рассылает по сети новое сообщение о членстве в группе, так что можно считать, что протокол MOSPF задействует механизм явных уведомлений бб изменении состава групп и поэтому относится к группе протоколов разряженного режима. Кроме того, известные положительные свойства протокола OSPF устойчивое поведение при изменениях топологии сети, меньшие объемы служебного трафика по сравнению с протоколом RIP, а также возможность деления сети на области - полностью наследуются протоколом MOSPF, что делает его весьма привлекательным для применения в больших сетях.

Протокол MOSPF

- Каждый маршрутизатор выясняет по IGMP членство в группах непосредственно присоединенных сетях
- Эта информация рассылается в специальнных объявлениях Group Membership – состояние членства
- Каждый маршрутизатор находит дерево кратчайших маршрутов от себя до членов каждой группы – тот же недостаток, что т у DVMRP: для каждой группы своя таблица маршрутизации
- При изменении члества в группе маршрутизатор сразу же делает объявление о новом состоянии членства

ГЛАВА 3 РАЗРАБОТКИ МОДЕЛИ И МОДЕЛИРОВАНИИ MULTICAST НА ОБОРУДОВАНИИ CISCO

3.1 Выбор программного обеспечение для моделирования

В процессе изучения компьютерных сетей многие учащиеся сталкиваются с проблемой отсутствия нужного оборудования для получения практических навыков, изученной теории. Например, изучение принципов работы межсетевых устройств (концентраторов, коммутаторов, маршрутизаторов) и сетевых протоколов, используя только теорию понять можно, но практически увидеть нельзя.

Одним из решений в данном случае является применение программ моделирования компьютерной сети и имитации ее работы. Одной из подобных программ является Graphical Network Simulator 3. В процессе изучения была построена модель компьютерной сети с использованием межсетевых устройств — концентраторы и коммутаторы.

GNS3 (Graphical Network Simulator) - среда моделирования компьютерных сетей, использующих сетевое оборудование, функционирующее на базе процессоров с архитектурой MIPS. К таким сетевым устройствам относятся, в том числе, большинство сетевых коммутаторов и маршрутизаторов, производимых компанией CISCO

Свою историю среда GNS3 начинает с 2007 года, в котором Джереми Гроссман (Jeremy Grossman) занимался выполнением выпускной квалификационной работы и ему было необходимо создать среду моделирования компьютерных сетей. В основу создаваемого программного продукта легла разработка эмулятора MIPS устройств Dynamips и его графического интерфейса Dynagen.

В дальнейшем среда GNS3 получила широкое распространение и теперь является одним изпопулярных сред для изучения компьютерных сетей и отработки различных промышленных решений.

В текущей версии для своего функционирования среда GNS3 использует следующее программное обеспечение:

• WinPCAP – системный драйвер и библиотека функций, позволяющая получить доступ к сетевым интерфейсам физического компьютера и передаваемой/получаемой информации по ним. Используется для анализа трафика, передаваемого по сети;

• Wireshark – графический анализатор сетевого трафика. Позволяет наглядно отобразить подробнейшую информацию о сетевом трафике. Используется как внутри среды GNS3, так и позволяет анализировать трафик с реальной компьютерной сети (считывая его с физических интерфейсов с помощью драйвера WinPCAP);

• Dynamips – среда моделирования сетевых устройств, реализованных на базе процессоров с MIPS архитектурой. Для своего функционирования требует наличие образов операционных систем iOS сетевых устройств CISCO. Допускает выполнение и иных операционных систем.

• VCPS, VirtualBox, QEMU – среды моделирования ЭВМ. Используются для эмулирования оконечных сетевых устройств или промежуточных устройств, реализованных на базе ЭВМ с архитектурой IBM/PC;

• SolarWinds Response – среда для анализа сетевого трафика. Используется для графического отображения информации, подготовленной Wireshark;

• SuperPUTTY – система виртуальных терминалов. Позволяет подключаться к сетевым устройствам для управления ими.

• Cpulimit – средство ограничения объемов потребления процессорного времени.

3.2 Маршрутизатор Cisco 3725

Маршрутизатор – это устройство, которое определяет более приемлемый путь для передачи данных из одной сети в другую. Устройство работает на третьем уровне модели OSI/ISO (сетевом). Для определения лучшего пути маршрутизатор использует таблицы маршрутизации и протоколы, которые реализуют алгоритмы маршрутизации.

В 1984 году была основана американская компания Cisco Systems, которая занимается разработкой и продажей сетевого оборудования. На рынке компанией представлен широкий спектр сетевого оборудования, и клиент имеет возможность закупить все необходимое сетевое оборудование исключительно у Cisco Systems.

Помимо сетевого оборудования Cisco Systems создала многоуровневую разветвленную систему сертификации инженеров по компьютерным сетям.

Благодаря тому, что экзамены этой системы проверяют знание не только продукции Cisco, но и знание сетевых технологий, многие организации, даже работающие на сетевом оборудовании других фирм, признают ценность профессиональных сертификатов Cisco. В частности, сертификация на уровне эксперта (CCIE) является одной из самых известных и уважаемых в компьютерной индустрии.

Рассмотрим характеристики маршрутизаторов Cisco 3725

Таблица 3.1: Технические характеристики маршрутизатора Cisco 3725

Технические характеристики	Cisco 3725
WAN-интерфейсы	Два 10/100 BASE-T
LAN-интерфейсы	Управляемый коммутатор на 8 портов 10/100 BASE-T
Аналоговый модемный порт V.92	Один
Порты USB 2.0	2 порта
Консольный порт	1, скорость до 115.2 Кбит/с
AUX-порт	1, скорость до 115.2 Кбит/с
ОЗУ(RAM)	Синхронный двухсторонний модуль памяти (DIMM) SDRAM (1 слот DIMM) по умолчанию 128 МБ максимум 384 МБ
Flash-память	Внешняя съемная flash-память формата Compact Flash, по умолчанию 32 МБ максимум 128 МБ

• LAN (Local Area Network) - интерфейс – это интерфейс, отвечающий за выход в локальную сеть.

• WAN (Wide Area Network) интерфейс – это внешний интерфейс маршрутизатора, используется для подключения к провайдеру или оборудованию доступа к провайдеру

• AUX (auxiliary, вспомогательный) порт необходим для подключения вспомогательного оборудования.После настройки подключения вспомогательное оборудование можно использовать как резервное.

• Консольный порт – порт, который используется для настройки оборудования с помощью управляющего терминала (консоли).В качестве консоли может выступать обычный компьютер.

Таблица 3.2 - Особенности маршрутизации в маршрутизаторе Cisco 3725

Особенности маршрутизации	Cisco 3725
Рекомендуемое количество пользователей	50
Поддержка технологий маршрутизации	Протокол динамической конфигурации узла (DHCP). Динамическая поддержка доменной системы имен. Сетевой протокол туннелирования канального уровня (L2TP). Технология трансляции порта адреса (PAT) скоростной пересылки Cisco (CEF). Асинхронный режим передачи данных по протоколу «точка-точка» (PPPoA). Протокол двухточечного соединения по сети Ethernet (PPPoE). Протокол связующего дерева (802.1d, STP).
Протоколы маршрутизации	BGP, EIGRP, OSPF, RIPv1, RIPv2
Машрутизируемые протоколы	IPv4, IPv6, IPX, IBM SNA, AppleTalk

• DHCP – сетевой протокол, позволяющий компьютерам автоматически получать IP-адрес и другие параметры, необходимые для работы в сети TCP/IP.DNS – это протокол, при помощи которого символьные имена преобразуются в IP-адреса и наоборот.

• L2TP – сетевой протокол туннелирования канального уровня в компьютерных сетях, использующийся для поддержки виртуальных частных сетей.

• PAT – технология трансляции сетевого адреса взависимости от TCP/UDP - порта получателя (частный случай NAT).

• PPPoE – туннелирующий протокол, который позволяет настраивать (или инкапсулировать) IP или другие протоколы, которые настраиваются на PPP (Point to point protocol) через соединение Ethernet.

• STP – сетевой протокол. Основной задачей STP является устранение петель в топологии произвольной сети Ethernet, в которой есть один или более сетевых мостов, связанных избыточными соединениями. STP решает эту задачу, автоматически блокируя соединения,

которые в данный момент для полной связности коммутаторов являются избыточными.

- IPX – протокол сетевого уровня модели OSI в стеке протоколов SPX.Он предназначен для передачи датаграмм, являясь неориентированным на соединение (так же, как IP), и обеспечивает связь между NetWare-серверами и конечными станциями.
- SNA – системная сетевая архитектура, разработанная компанией IBM в 1974 году. Представляет собой общее описание структуры, форматов, протоколов, используемых для передачи информации между программами IBM и оборудованием.
- AppleTalk – стек протоколов, разработанный Apple Computer. Он был изначально включен в Macintosh (1984), сейчас компания отказалась от него в пользу TCP/IP.

Рассмотрим более подробно маршрутизатор Cisco 3725

Рисунок 3.1 - Обозначение световых маршрутизатора Cisco 3725

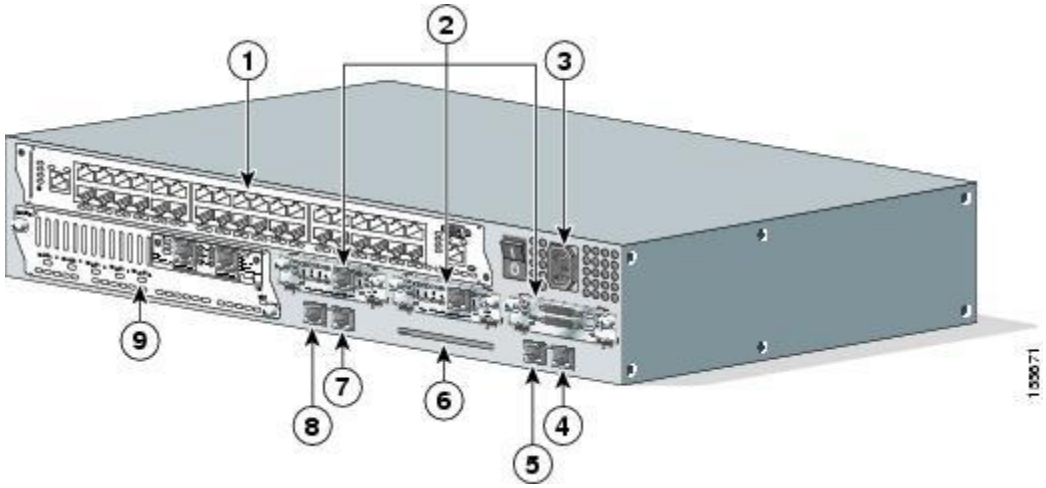

Рисунок 3.2 - Задняя панель маршрутизатора Cisco 3725

Таблица 3.3: Задняя панель маршрутизатора Cisco 3725

№	Наименование
1	Слоты интерфейсных плат
2	Сетевые модули
3	Источник питания
4	Вспомогательный порт
5	Консольный порт
6	Компактный слот для вспышки
7	FastEthernet 0/0
8	FastEthernet 0/1

3.3 Экспериментальные результаты моделирования

Мультиадресная рассылка IP — это технология, предназначенная для экономии пропускной способности. Она сокращает объем трафика за счет параллельной доставки одного информационного потока тысячам корпоративных получателей и домовладений. В числе приложений, которые получат преимущества при использовании мультиадресной рассылки видеоконференции, корпоративные коммуникации, дистанционное обучение и распространение программного обеспечения, котировок акций и новостей. В этом документе рассматриваются основы конфигурации мультиадресной рассылки для различных сетевых сценариев.

Для настройка multicast воьмём небольшую сети:

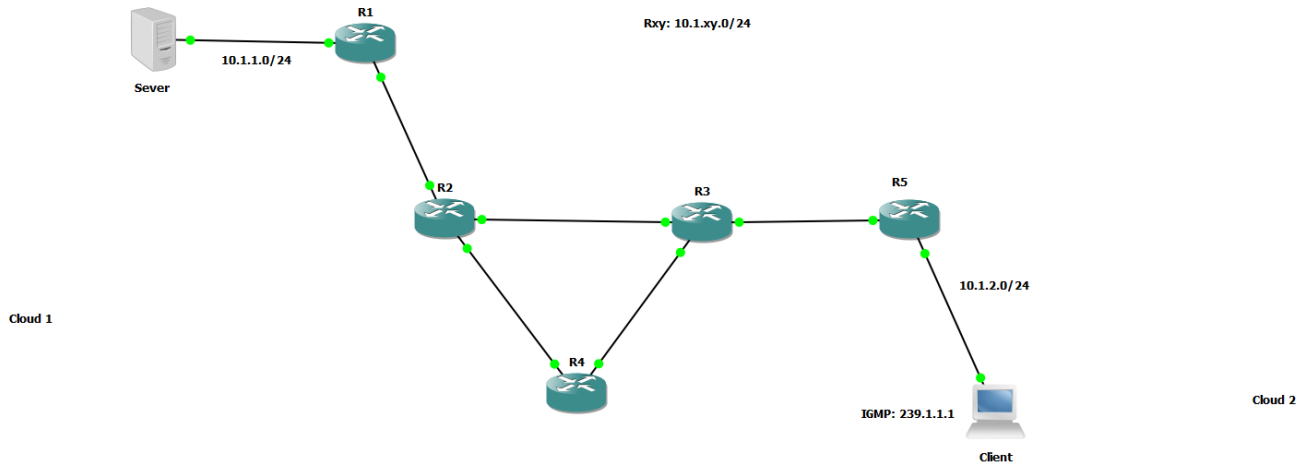

Рисунок 3.3 - Моделируемая сеть.

На рисунке выше представлена упрощённая схема сети провайдера и небольших клиентов. В сети оператора использовано пять маршрутизатора для обеспечения простейшей отказоустойчивости. R1, R2, R3, R4 и R5 – cisco 3725. R1 и R5: два FastEthernet интерфейса.

R2, R3 и R4: три FastEthernet интерфейса.

Сети клиентов представлены одним маршрутизатором для простоты. Клиент (Multicast Client, 10.1.2.0/24) и сервер (Multicast Server, 10.1.1.0/24), который будет транслировать сигнал в мультикастовый адрес 239.1.1.1.

Из теории видно, что принадлежность того или иного клиента к определенной группе «вещания» отслеживается протоколом IGMP (Internet Group Management Protocol). Передача multicast работает по протоколу PIM (Protocol Independent Multicast). Этот протокол составляет свою таблицу маршрутизации multicast на основе обычной таблицы маршрутизации. Есть 3 режима работы данного протокола:

- *dence mode* – когда маршрут прокладывается непосредственно от источника до получателя (предложение вещания потоков, зарегистрированных на роутере, идет всем, а затем отсекаются те, кому оно не нужно);
- *sparce mode* – маршрут прокладывается только до так называемой точки рандеву RP (Rendezvous point). Трансляция потока начинается, только если есть запрос от клиента;
- *sparce - dence mode* – смешанный режим.

Пповерка с режим dense-mode протокола PIM.

Конфигурации IP (проверка router 2, router 3)

Для Router 2:

Ping 255.255.255.255

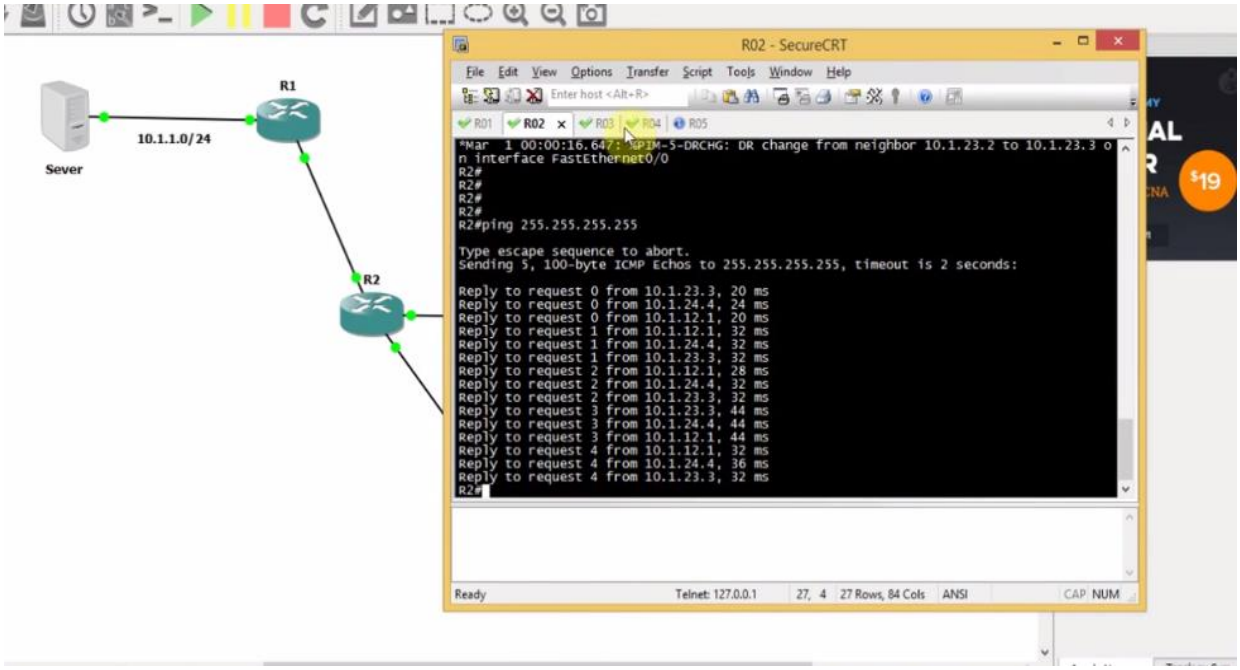

Рисунок 3.4 - Конфигурации IP (Router_2)

Для router 3:

Ping 255.255.255.255

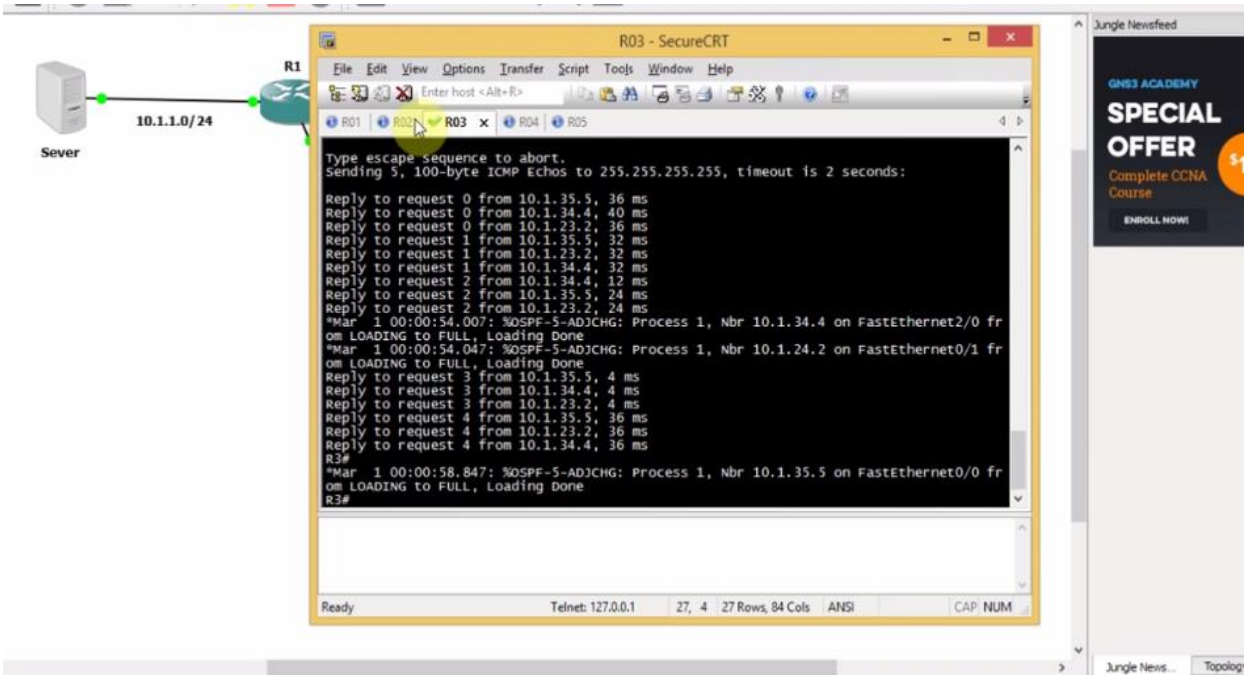

Рисунок 3.5 - Конфигурации IP (Router_3)

Конфигурации IGP (проверка router 1, router 5)

Для router 1: Show ip ro

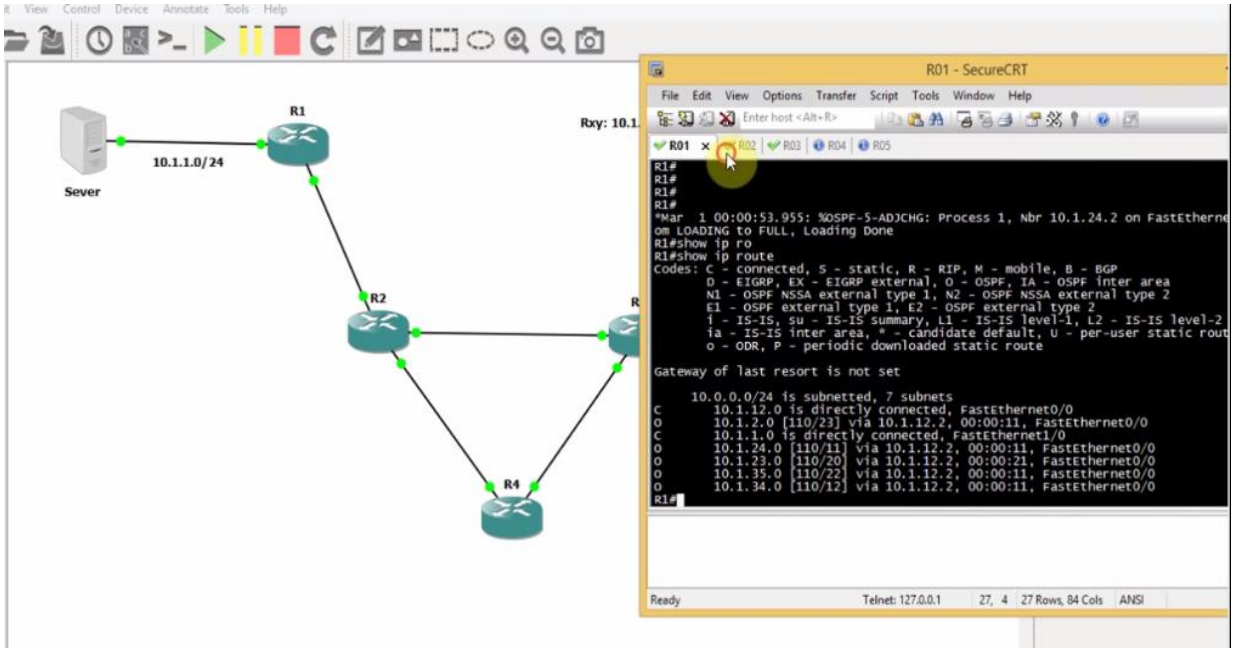

Рисунок 3.6 – Таблицы марршрутизации Router_1

Router_1: Ping 10.1.2.0

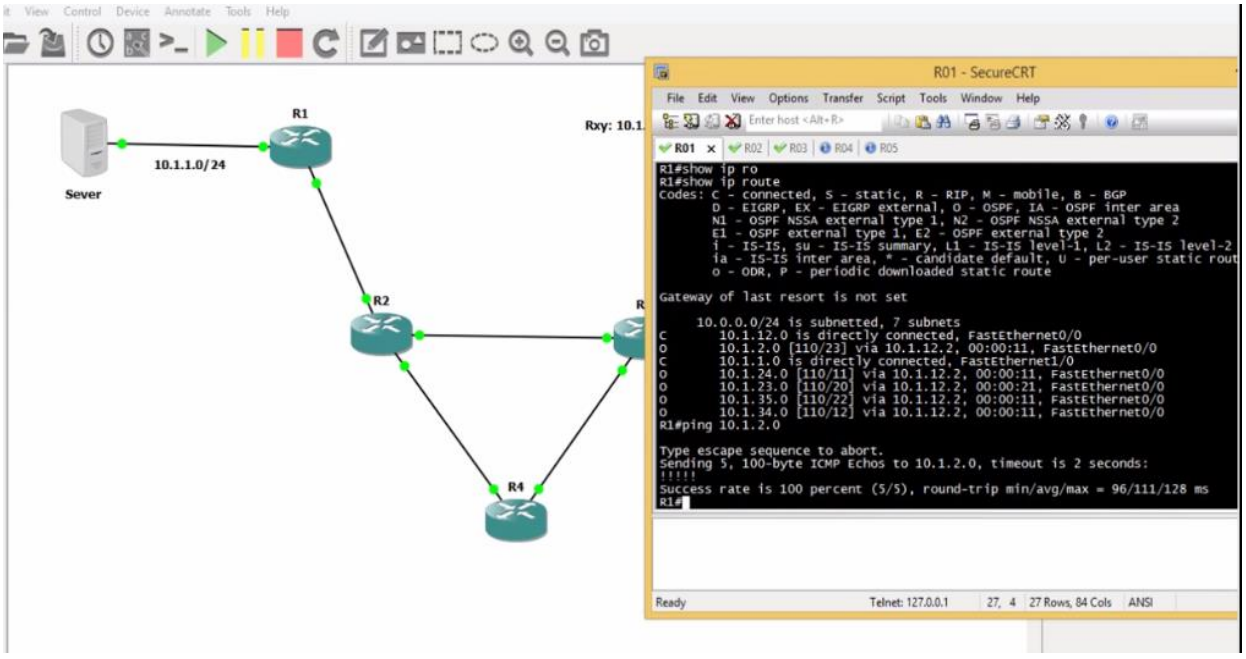

Рисунок 3.7 - Проверка соединение между router_1 и Client

Для router 5: Show ip ro

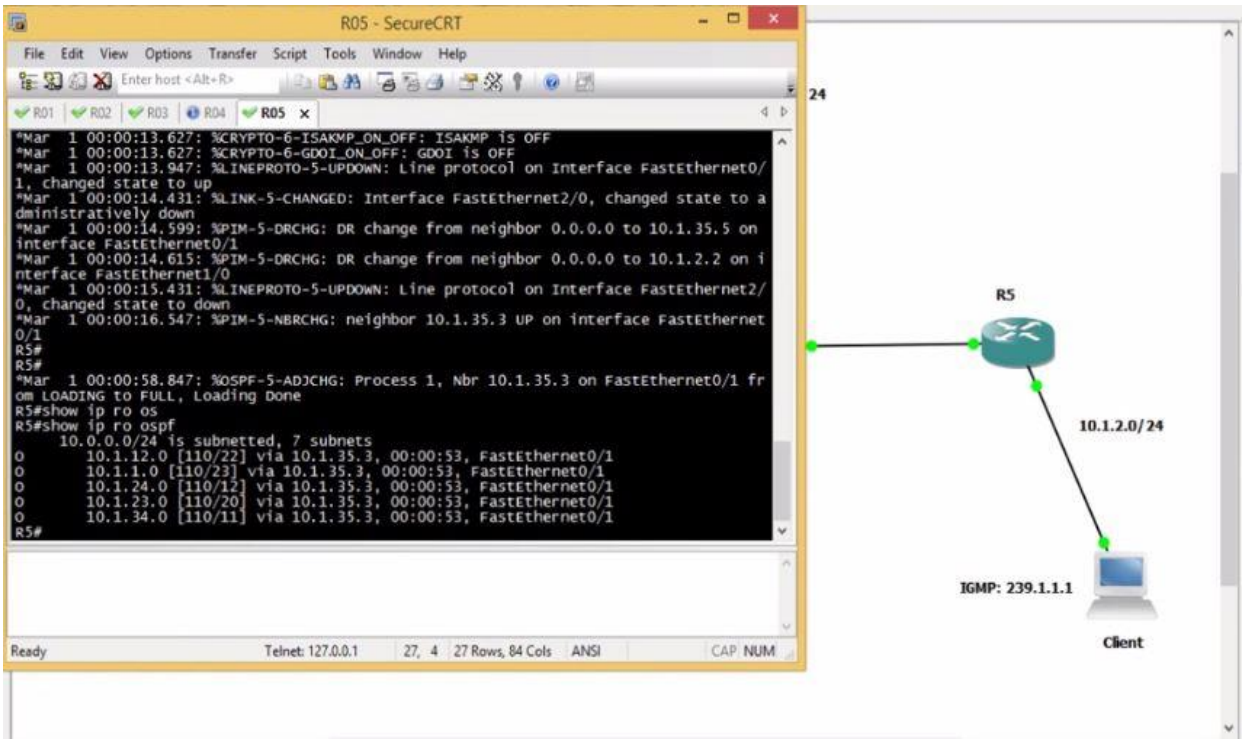

Рисунок 3.8 - Таблицы марршрутизации Router_5)

Router_5: Ping 10.1.1.0

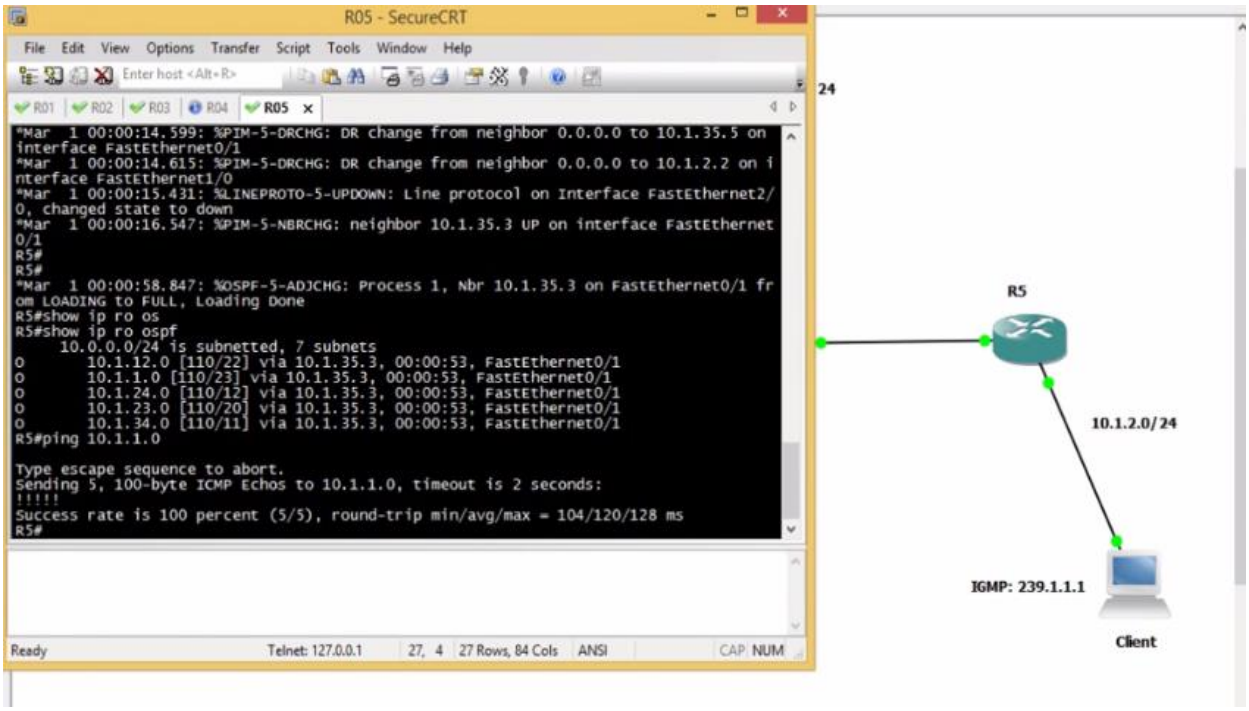

Рисунок 3.9 - Проверка соединение между router_5 и Server

Конфигурации multicast

Для проверки сигнализации приемника: Выполните команду «show ip igmp groups» на первом вышестоящем маршрутизаторе для проверки присоединения интерфейса к группе.

Router_5 : Show run | se igmp

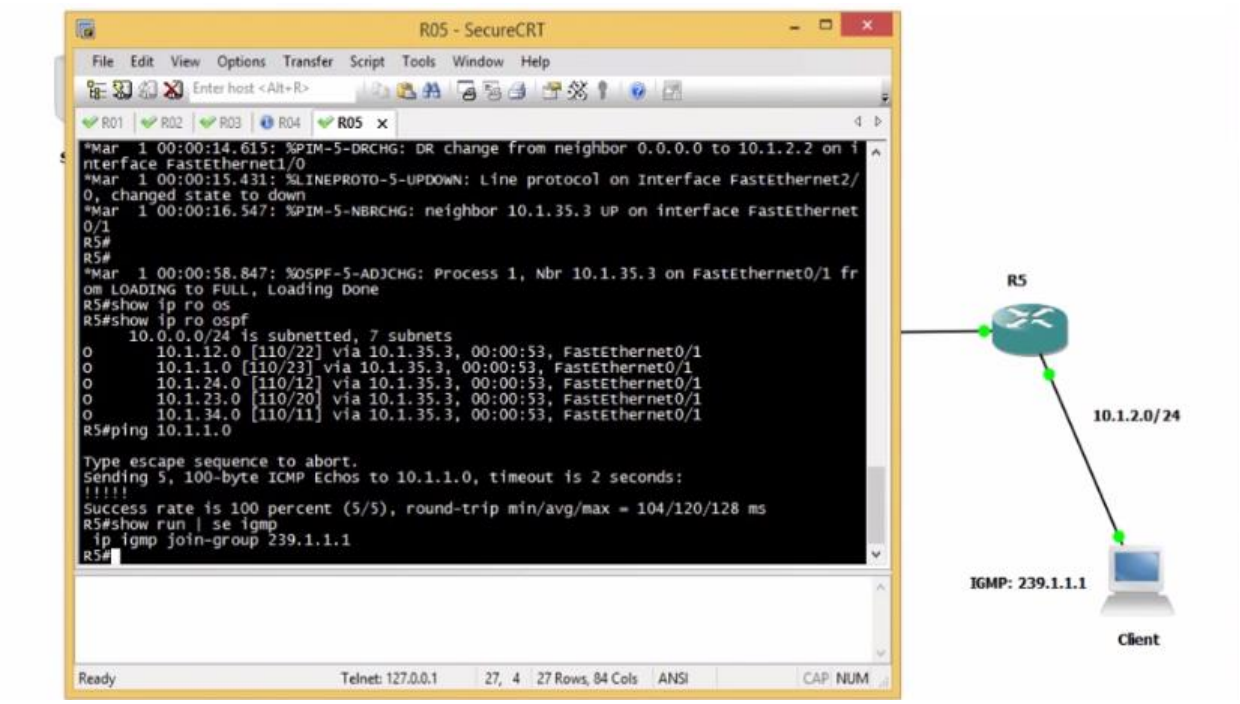

Рисунок 3.10 - Проверки сигнализации приемника (router_5)

Выполните команду «ping» для проверки доступности хоста и первого вышестоящего маршрутизатора.

Router 1: Ping ip

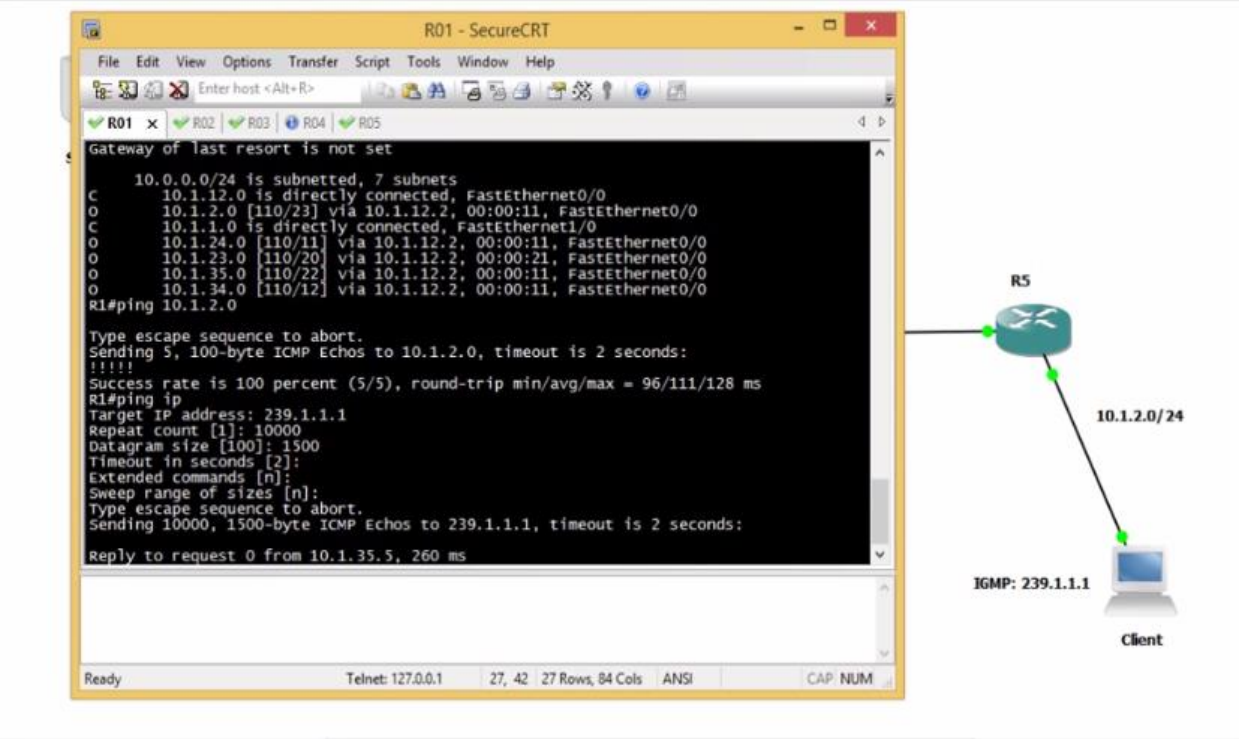

Рисунок 3.11 - Проверки сигнализации передачи(router_1)

Командой «show ip mroute» можно посмотреть таблицу маршрутизации multicast.Router 5: Show ip mro

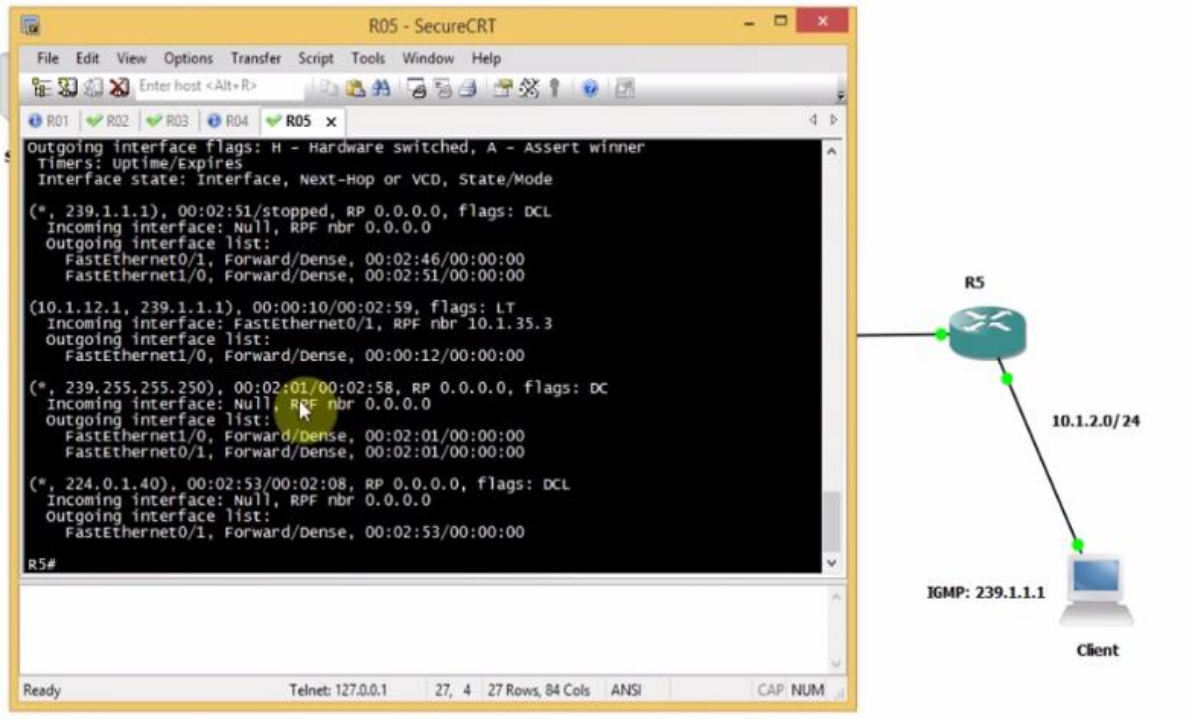

Рисунок 3.12 - Маршрутизации multicast (router_5)

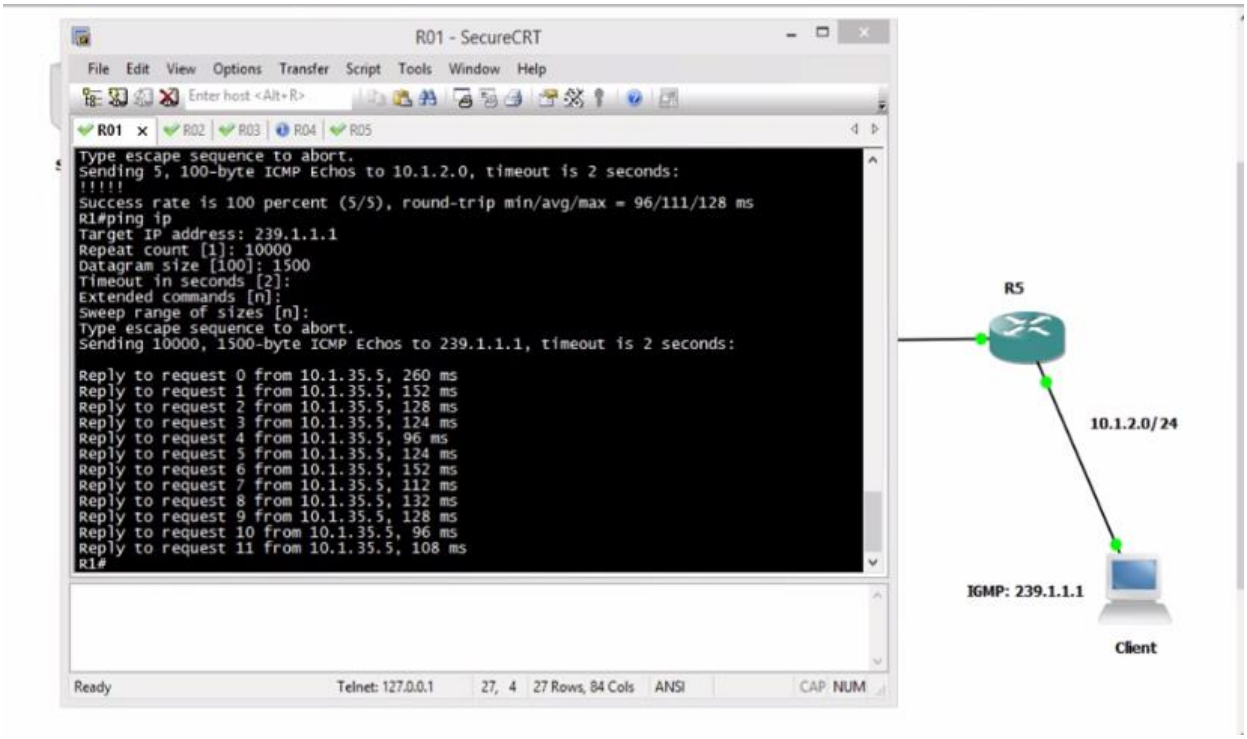

Рисунок 3.13 Маршрутизации multicast (router_1)

Ping server к client

Команда «Ipconfig» используется для отображения текущих настроек протокола TCP/IP и для обновления некоторых параметров, задаваемых при автоматическом конфигурировании сетевых интерфейсов при использовании протокола Dynamic Host Configuration Protocol (DHCP)..

В client использовании команда «ipconfig»

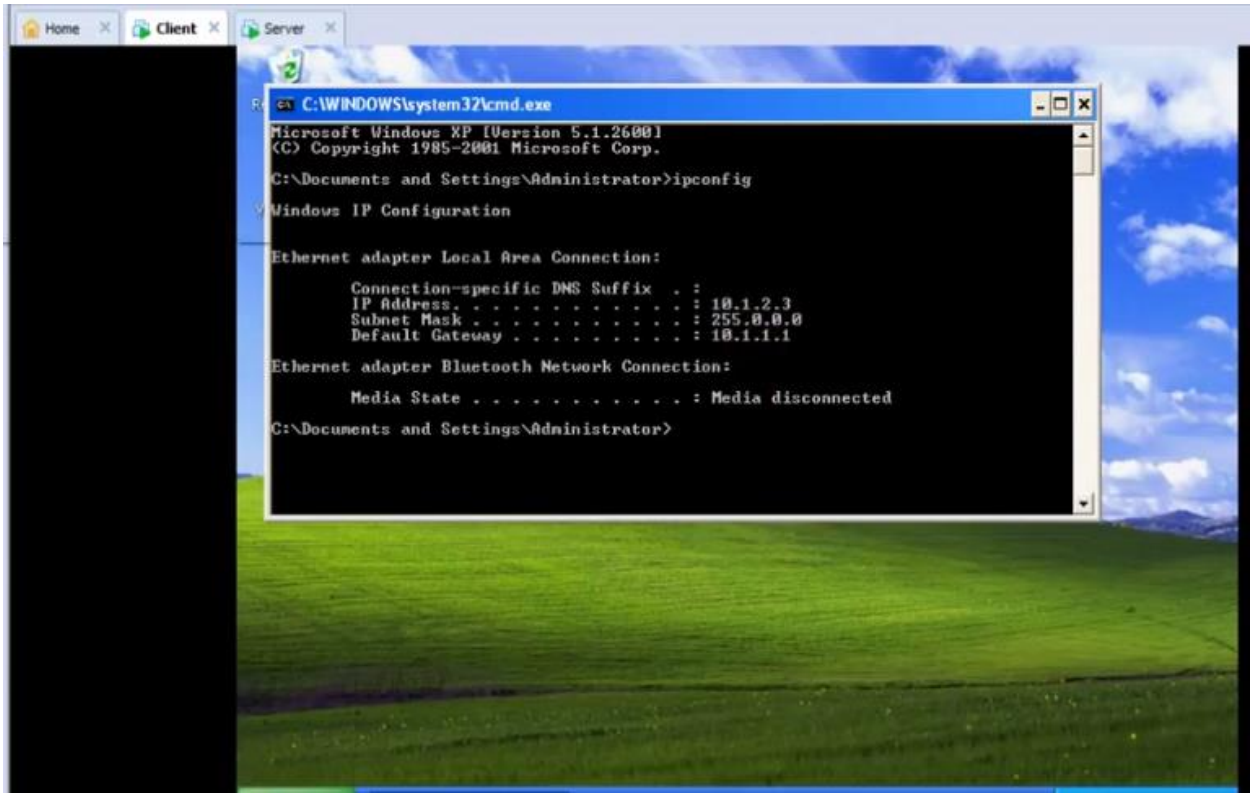

Рисунок 3.14 - IP адрес в Multicast Client

IP address client: 10.1.2.3

В server: ping 10.1.2.3

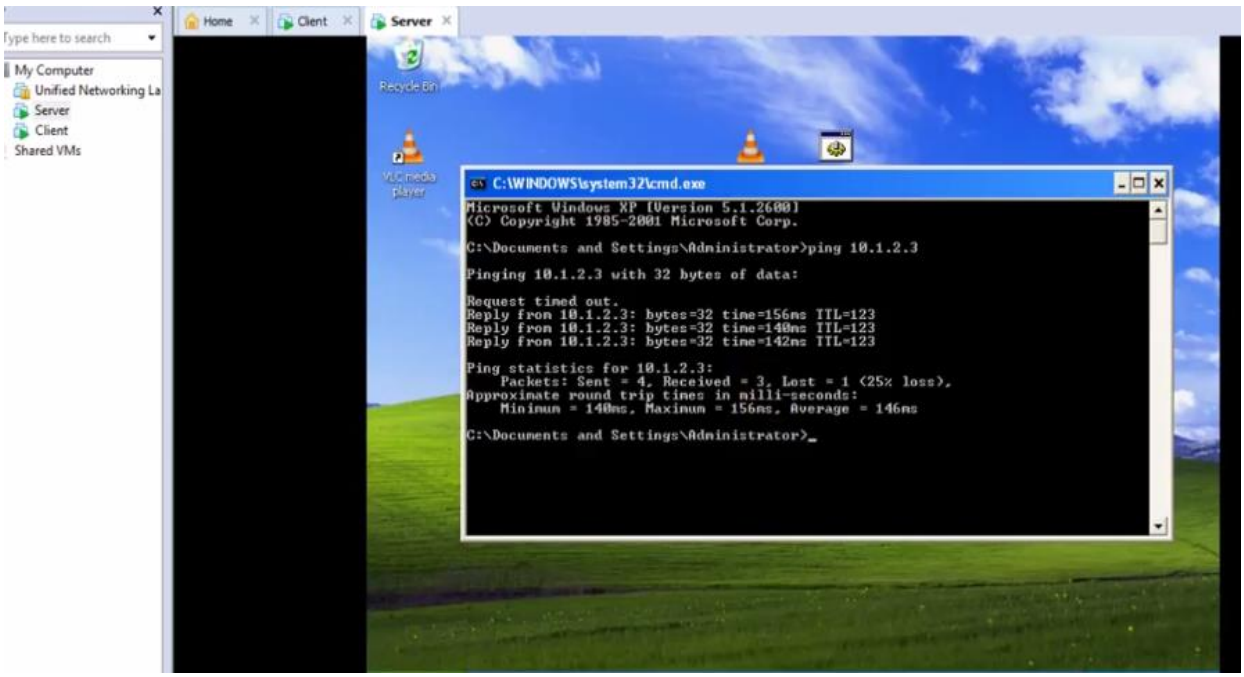

Рисунок 3.15 - Проверка соединение между Server и Client

Зайдем на Multicast Server и настроим вещание файла .avi в плеере VLC. Открываем программу. Появится следующее окно:

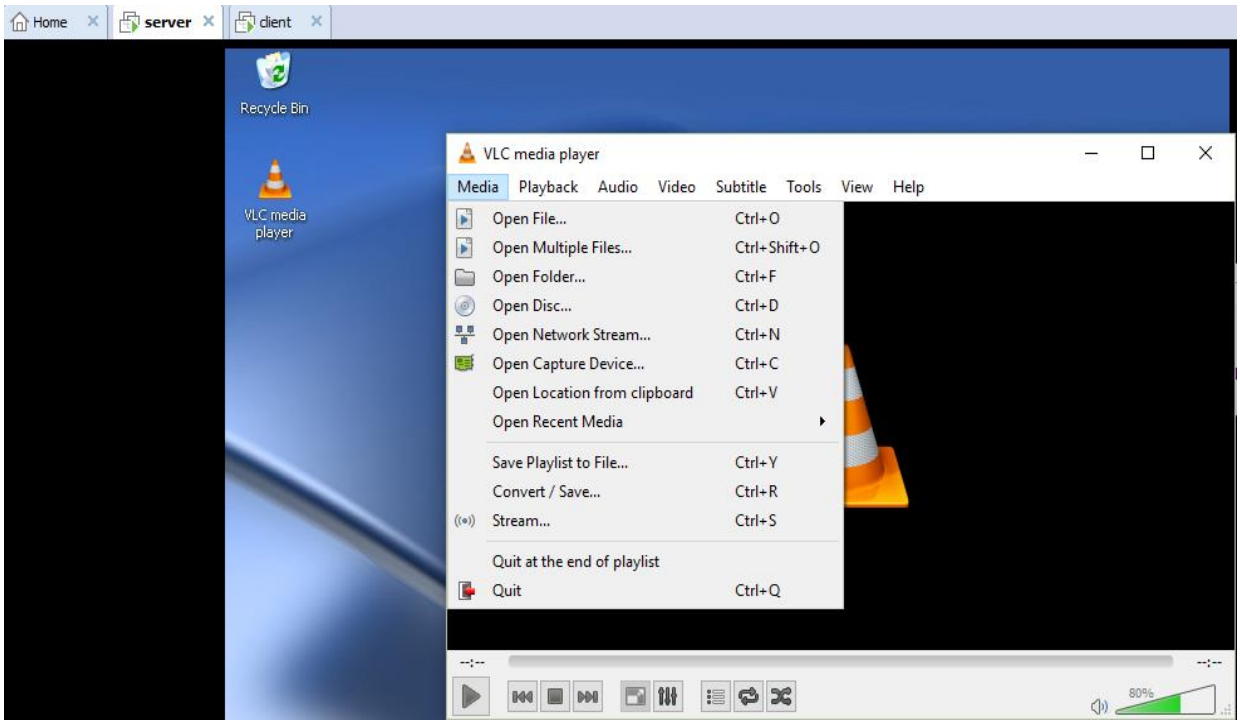

Рисунок 3.17 - Программа VLC media player на компьютере Server.

Выбираем «Media» - «Steam» Откроется следующее окно:

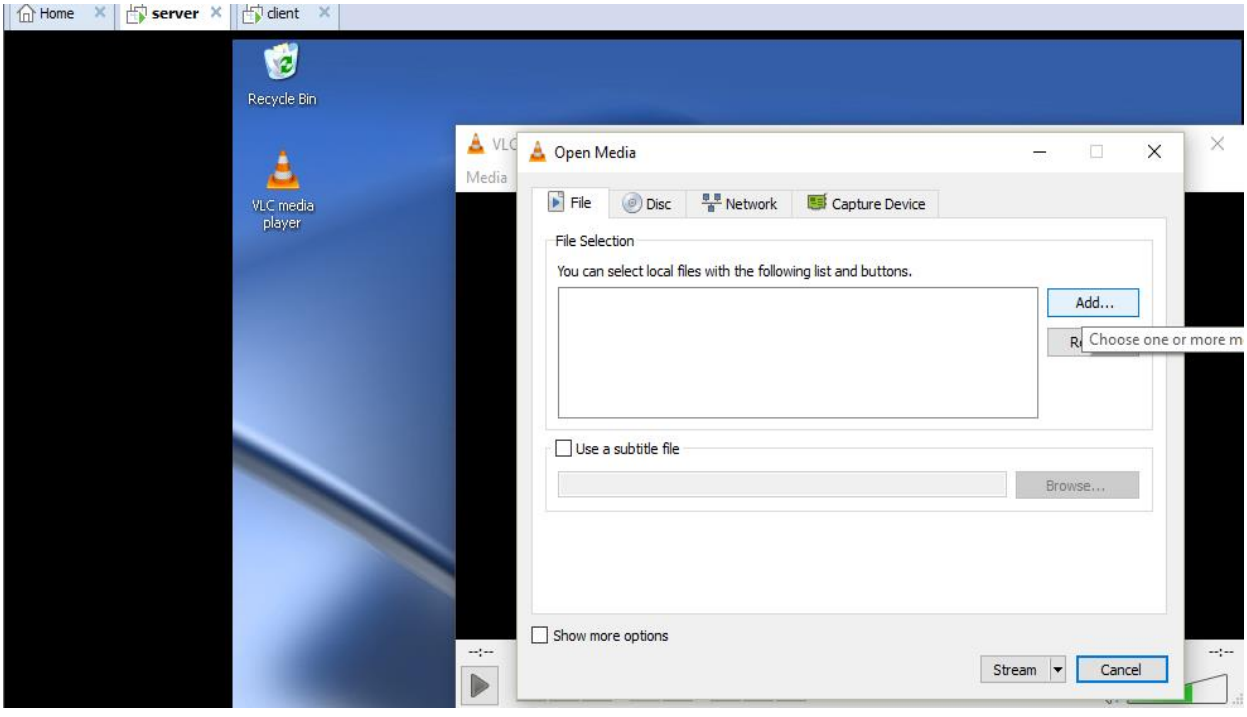

Рисунок 3.18 - Интерфейс потоковое вещание

Здесь остаемся на вкладке «File». Нажимаем на «Add». В появившемся окне выбираем файл .avi и нажимаем «Open». Файл появится в списке:

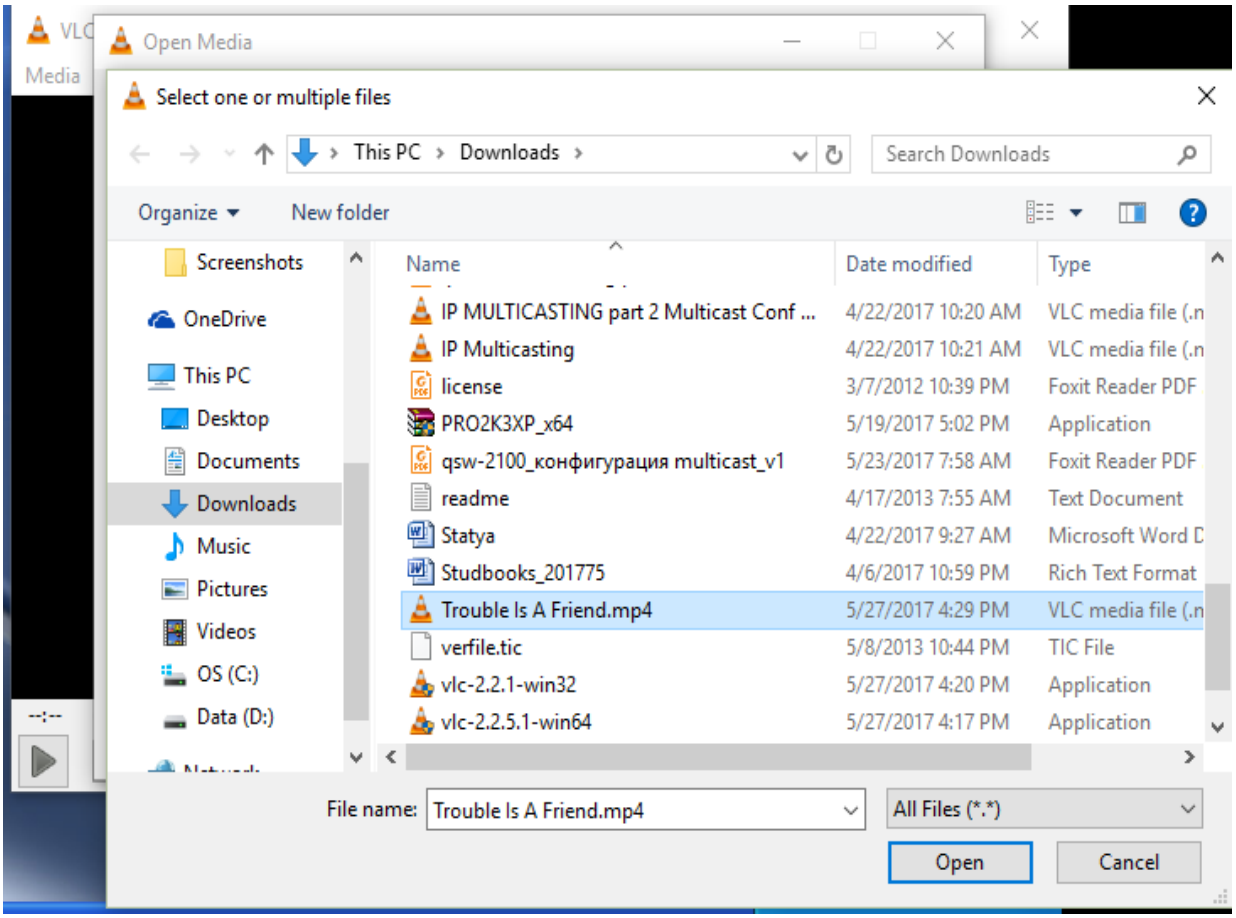

Рисунок 3.19 - Выбор файл .avi для потоковое вещание

Внизу справа, из выпадающего меню выбираем пункт «Stream».

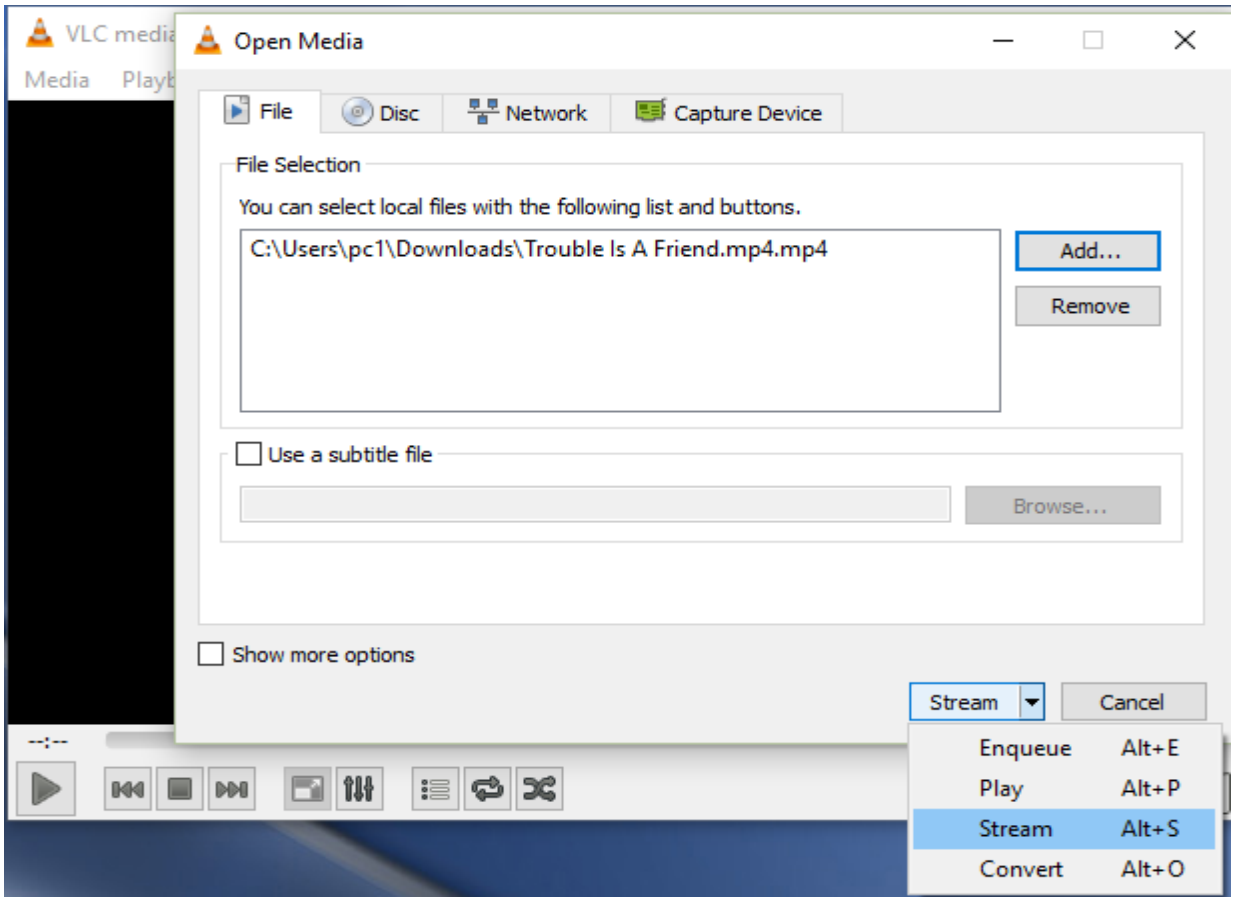

Рисунок 3.20 - VLC потоковое вещание

В этом окне выключаем перекодирование.В закладке «Destination Setup» (Пункт назначения) из выпадающего меню выбираем пункт «RTP Audio/Video Profile» и нажимаем «Add».

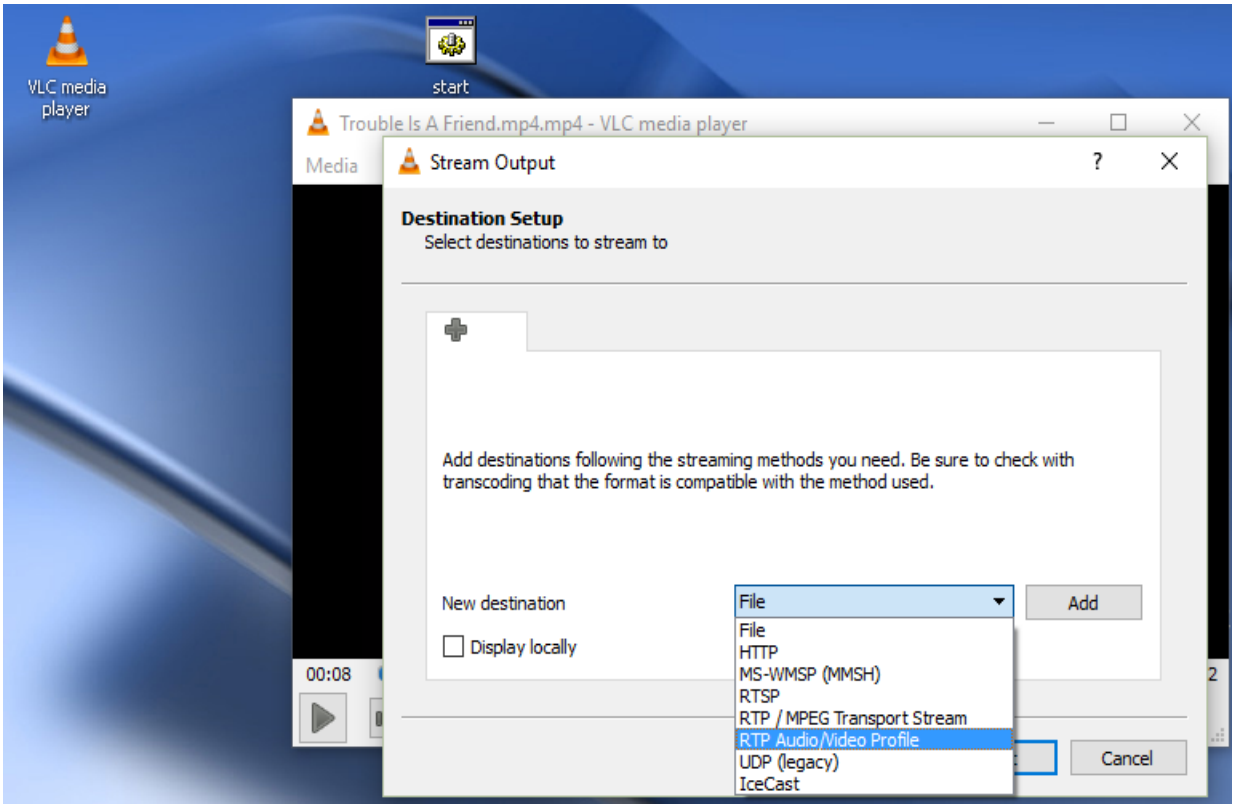

Рисунок 3.21 - Настройка назначение

Откроется новая закладка на этой же странице:

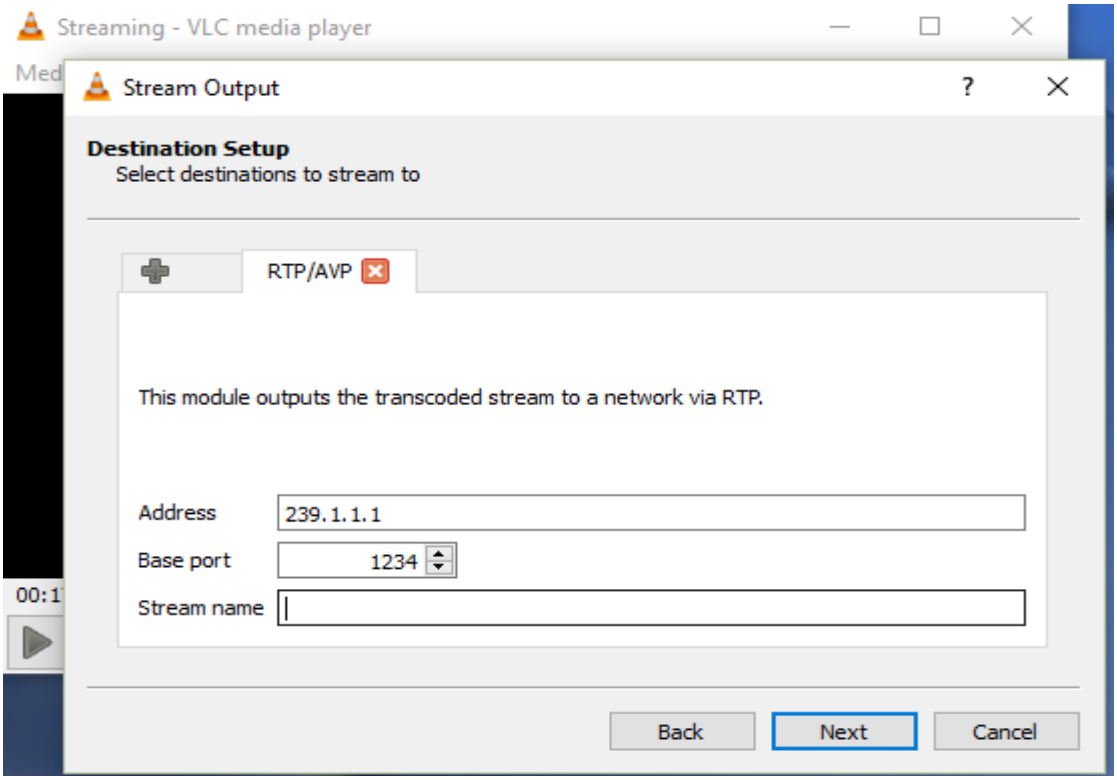

Рисунок 3.22 - Multicast адрес назначение

В этой вкладке указываем multicast адрес, в который будет транслироваться файл. Порт можно оставить по умолчанию.

Поток (Stream) настроен. Теперь перейдем на Multicast Client и примем его. Для этого, открываем VLC на компьютере клиента:

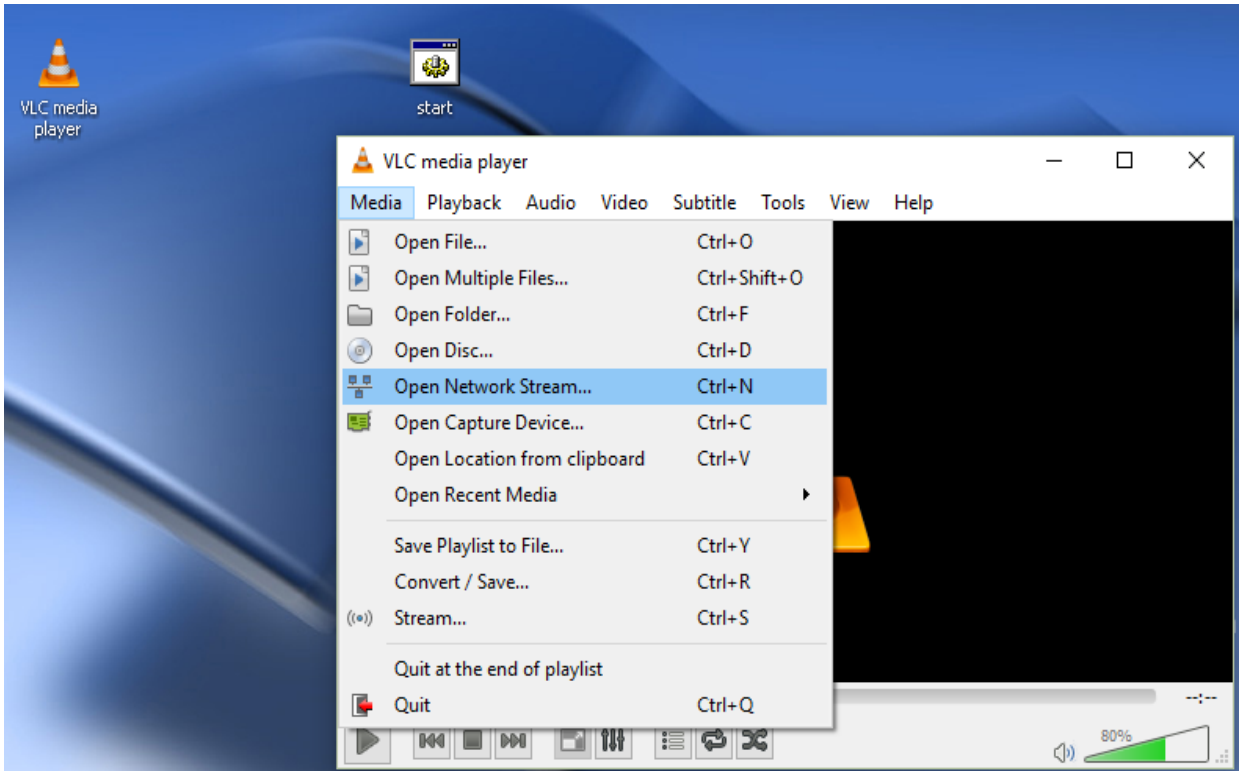

Рисунок 3.23 - Программа VLC media player на компьютере клиента

В пункте меню «Media» из выпадающего списка выбираем «Open Network Stream». Появится окно:

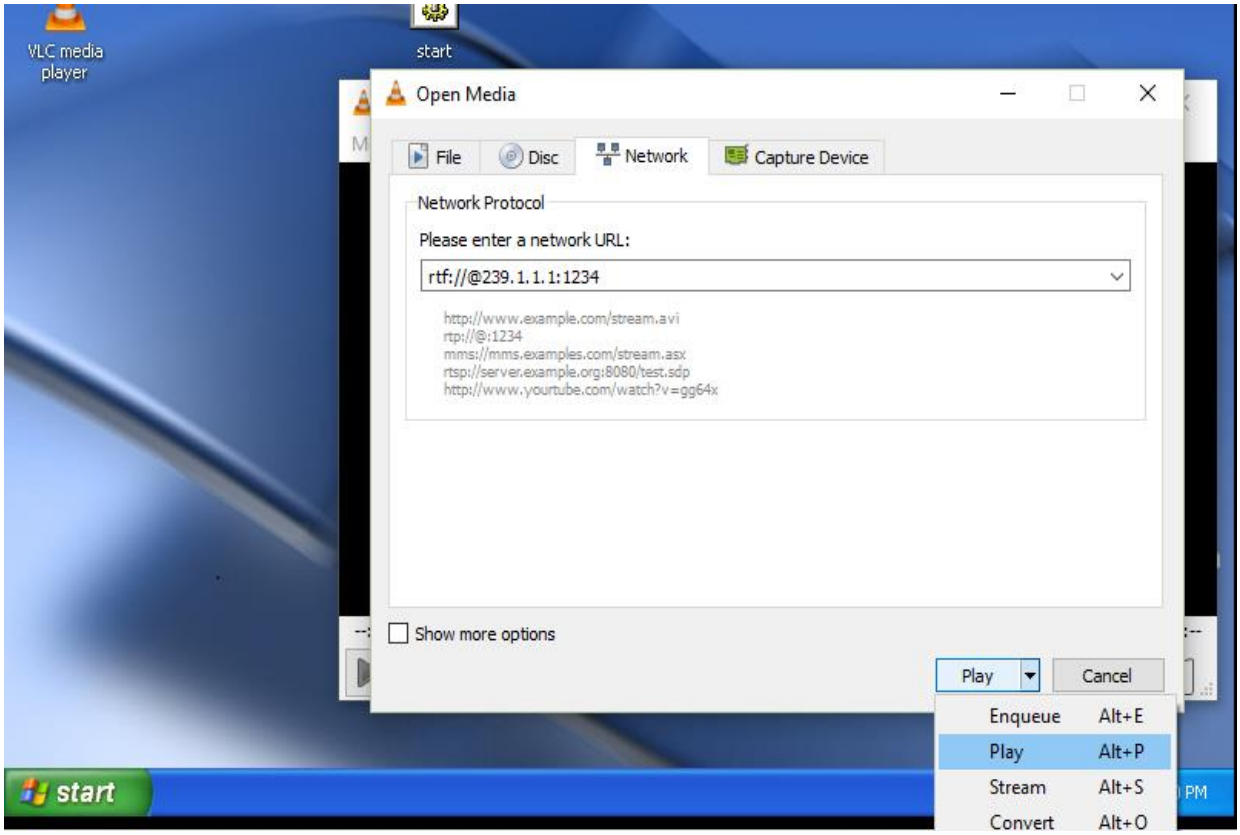

Рисунок 3.24 - Открытый сетевой поток

Вводим адрес потока multicast и порт, выбираем из выпадающего меню внизу справа «Play».

Проверку dense-mode закончили.

Переходим к настройке sparse-mode протокола PIM. Для этого режима необходимо выбрать так называемую точку рандеву (RP (Rendezvous point)). Пусть для этих целей служит Router_2. В качестве IP-адреса точки будем использовать loopback 0. Так же нам надо будет дописать статические маршруты, чтобы другие роутеры знали, как добраться до RP.(см. Приложение А)

Перейдем к проверкам. Снова заходим на Multicast Server, включаем потоковое вещание, возвращаемся на Multicast Client и смотрим результат.

Multicast Server:

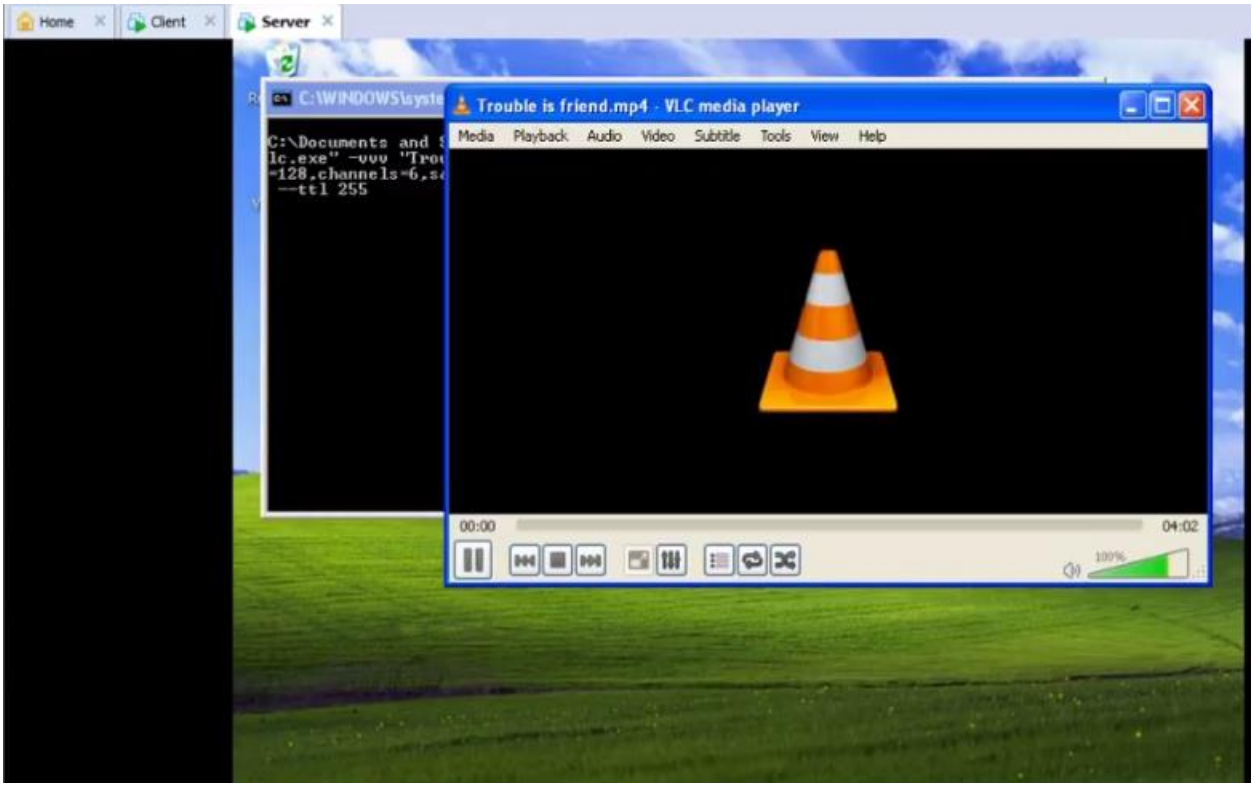

Рисунок 3.25 - Включаем потоковое вещание на компьютере Server

Multicast Client:

Рисунок 3.26 - Экспериментальные результаты на компьютере Client

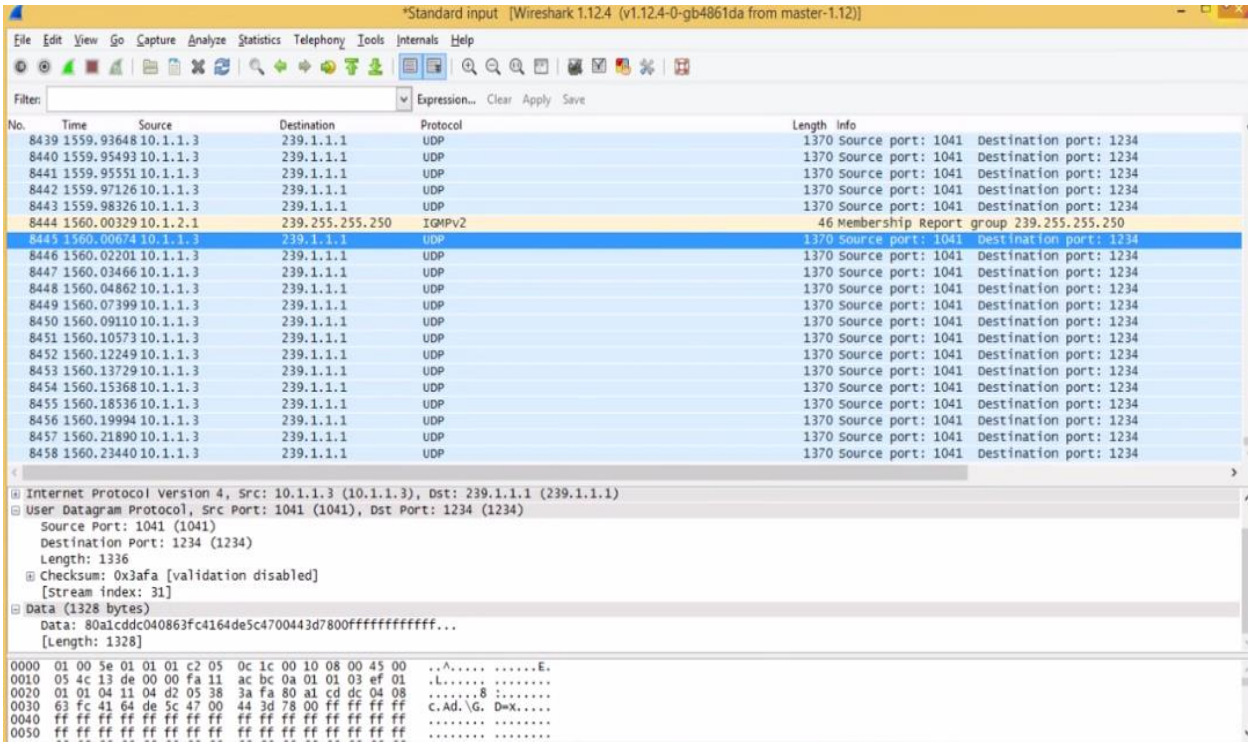

Рисунок 3.27 - Результаты испытаний с помощью Wireshark.

ЗАКЛЮЧЕНИЕ

В ходе выполнения работы анализ способы передачи данных в групповой рассылки, рассмотренны преимущества групповой рассылки, анализ протоколов маршрутизации. Представлены их характеристики. Так же был рассмотрены протокол маршрутизации IP Multicast: ICMP, PIM DM и PIM SM.

Были рассмотренны протоколы внутридоменной маршрутизации DVMRP, MOSPF.

В ходе выполнения работы в среде GNS3 была разработана имитационная модель сети с тремя типами трафика – одноадресным, многоадресным и широковещательным.

Упрощенная настройка всех протоколов маршрутизации была наглядно продемонстрирована на оборудовании Cisco. В работа программы Graphical Network Simulator 3 - симулятора сети передачи данных, выпускаемой фирмой Cisco Systems. Программа позволяет делать работоспособные модели сети, настраивать с помощью команд Cisco IOS маршрутизаторы и коммутаторы.

Так же в ходе работе рассмотрены маршрутизатор Cisco Systems серии 3725, его внутренние компоненты и возможности.

Анализ полученных результатов показал, что IGMP – протокол управления multicast группами, PIM – протокол маршрутизации multicast трафика.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Деарт В.Ю. Мультисервисные сети связи. Протоколы и системы управления сеансами (Softswitch/IMS) [Текст] // Учебное пособие. — М.: Инсвязьиздат. 2011. - 198с

2. Абдель-Джалил,Дж.Н.
Алгоритмы межпроцессорного взаимодействия в отказоустойчивых многопроцессорных системах [Текст] / Дж.Н.Абдель-Джалил, Э.И.Ватутин, И.В.Зотов, А.А.Иванов // Методы и системы обработки информации. Муром, 2004. С. 117-125.

3. Артамонов, Г.Т. Топология регулярных вычислительных сетей и сред [Текст] / Г.Т.Артамонов. -М.: Радио и связь, 1985. 192 с.

4. Архитектура и синтез параллельных логических мультимикроконтроллеров [Текст] / И.В.Зотов, В.С.Титов, В.И.Штейнберг -Курск: КурскГТУ, 2006. 359 с.

5. Chen, C.-L. A fault-tolerant routing scheme for meshes with nonconvex faults [Текст] / Chun-Lung Chen, Ge-Ming Chiu // IEEE Transactions on Parallel and Distributed Systems. 2001. Vol. 12, №5. P.467-475.

6. Кондрашин А.А. IPTV– современная интерактивная цифровая технология [Текст] / А.А. Кондрашин, В.В. Слепцов, А.Н. Лямин // Новые материалы и технологии НМТ-2010. Т. 2. Материалы Всерос. научно-техн. конф. М.: МАТИ-РГТУ им. К.Э. Циолковского, 2010. С. 118.

7. Барсков А.Г. ТВ в сетях IP [Текст] / А.Г. Барсков // Сети и системы связи. 2004. №11 - С. 62-68.

8. Весоловский Кшиштоф. Системы подвижной радиосвязи [Текст] // Горячая линия – Телеком, 2006. - 536 с.

9. Баишрин Г.П. Лекции по математической теории телетрафика [Текст] / Г.П. Баишрин // Учебное пособие. Изд. 3 дораб. и доп. - М.: Изд-во РУДН, 2009. -342 с

10. Гудкова Н.А., Лузгачев М.В. Модели разделения ресурсов звена мультисервисной сети с эластичным трафиком [Текст] // T-Comm - Телекоммуникации и Транспорт. М.: Издательский дом Медиа Паблишер. - 2010. - № 7. - С. 22-24.

11. Деарт В.Ю. Мультисервисные сети связи. Транспортные сети и сети доступа [Текст] // М.: Инсвязьиздат, 2007. – С.166.

12. Адресация в IP-сетях [Электронный ресурс]/ Режим доступа - http://www.intuit.ru — ИНТУИТ — Национальный открытый университет, (Дата обращения 26.05.2017)

13. Величко В.В., Субботин Е.А., Шувалов В.П.Телекоммуникационные системы и сети: Учебное пособие. В 3-х томах. Том 3. - Мультисервисные сети, 2005. – 592 с.

14. Травин, М.Г. Вейвлеты для инженеров [Текст] / М.Г. Травин, В.М. Терешко, Г.А. Травин. – Белгород: издательско-полиграфический центр «ПОЛИТЕРРА», 2007. – 423с.

15. Кааранен Х, Ахтиайнен А. Сети UMTS. Архитектура, мобильность, сервисы [Текст] // М: Техносфера. - 2007. - 464 с

16. Кучерявый А.Е., Цуприков А.JI. Сети связи следующего поколения [Текст] // М.: ФГУП ЦНИИС, 2006. -280 с.

17. Наумов В.А., Самуилов К.Е., ЯркинаН.В. Теория телетрафика мультисервисных сетей. Монография [Текст] // М.: Изд-во РУДН, 2007. -191 с.

18. Плаксина О.Н., Яркина Н.В. Приближенный метод расчета характеристик звена мультисервисной сети связи [Текст] // Тезисы докладов Всероссийской конференции по проблемам математики, информатики, физики и химии. М.: РУДН, 2008. -С. 85

19. Росляков А.В., Самсонов М.Ю. Сети следующего поколения NGN [Текст] // М.: Эко-Трендз.- 2009. - 424 с

20. Рыков В.В. Сети обслуживания прозрачных требований [Текст] // Автоматика и телемеханика. 2001. №5. С. 147-158.

21. Рыков В. В., Самуилов К. Е. К анализу вероятностей блокировок ресурсов сети с динамическими многоадресными соединениями [Текст] // Электросвязь. 2000. - № 10. - С. 27-30.

22. Самуилов К. Е. Метод расчета вероятностных характеристик модели сети с многоадресными соединениями [Текст] // Вестник РУДН. Серия «Прикладная и компьютерная математика». 2003. - Т.2,№1.

23. Самуилов К. Е., Яркина Н. В. Модель звена мультисервисной сети с одноадресными и многоадресными соединениями [Текст] // Вестник РУДН. Серия «Прикладная и компьютерная математика». 2003. - Т. 2, № 1.-С. 32-43.

24. Сегайер А., Цитович И.И. Построение моделей мультисервисных сетей [Текст] // Электросвязь. 2009. № 9. С. 54-57.

25. Степанов С.Н. Основы телетрафика мультисервисных сетей [Текст] // М.: Эко-Трендз, 2010. 392 с.

26. Тихвинский В.О., Терентьев С.В., Юрчук А.Б. Сети мобильной связи LTE: технологии и архитектура [Текст] // М.: Эко-Трендз. 2010. - 284 с.

27. Цитович И.И. Устойчивые модели трафика мультисервисных сетей [Текст] // Тр. НРТОРЭС им. А.С. Попова. Вып.: LX-2. М.: Инсвязьиздат. - 2005. -Т 2. - С. 271-273.

28. Цитович И.И., Албхаиси Осама. Анализ тенденций внедрения принципов коммутации пакетов в корпоративных сетях [Текст] // T-Comm: Телекоммуникации и транспорт - 2009. - № S1. - С. 54-56.

29. Bain A., Kelly F., Key P. Fair Internet traffic integration: network flow models and analysis // Annals of Telecommunication. -2004.-Vol. 59, No. 11-12.-P. 1338-1352.

30. Замятина О.М. Моделирование сетей: учебное пособие [Текст] / О.М. Замятина: Томский политехнический университет – Томск: Изд-во Томского политехнического ниверситета, 2011. – 168 с.

31. Лоу А.М., Кельтон В.Д. Имитационное моделирование. Классика CS [Текст] – 3-е изд. – СПб.: Питер; Киев: Издательская группа BHV, 2005. – 847 с.

32. Программа сетевой академии Cisco CCNA 3 и 4. Вспомогательное руководство.: Пер. с англ. [Текст] / – М.: ООО «ИД Вильямс», 2007. – 994 с.

33. Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2010-2015. White paper. - February, 2011. pp. 18-31

34. Cisco Visual Networking Index: Forecast and Methodology, 2009-2014. White paper. - June, 2010. pp. 78-86.

35. Cisco CDA Visual Quality Experience Application User Guide, Release 3.0.-2008. pp. 27-49.

36. Cisco Visual Networking Index: Forecast and Methodology, 2009-2014. White paper. - June, 2010

37. Hens F.J., Caballero G.M. Triple Play: Building the converged network for IP, VoIP and IPTV. Wiley. -2008. - 416 p.

ПРИЛОЖЕНИЕ А

В среде GNS3 необходимо разработать сеть, состоящую из 5 маршрутизаторов.В общей сети необходимо реализовать 7 статических маршрута.

10.1.1.0/24

10.1.12.0/24

10.1.23.0/24

10.1.24.0/24

10.1.34.0/24

10.1.35.0/24

Построение маршрутизатор с Dence mode.

Router_1:

R1>en

R1#conf t

R1(config)#hostname Router_1

Router_1(config)#ip multicast-routing – глобально включаем маршрутизацию multicast;

Router_1(config)#int fa 1/0

Router_1(config-if)#ip address 10.10.1.1 255.255.255.250

Router_1(config-if)#ip pim dense-mode – включаем нужный режим на интерфейсе;

Router_1(config-if)#no sh

Router_1(config-if)#exit

Router_1(config)#int fa 0/0

Router_1(config-if)#ip address 10.1.12.1 255.255.255.250

Router_1(config-if)#ip pim dense-mode

Router_1(config-if)#no sh

Router_1(config-if)#exit

Router_1(config)#ip route 10.1.2.0 255.255.255.0 10.1.12.2 – прописываем статический маршрут для обеспечения обычной сетевой доступности между клиентом и сервером;

Router_1(config)#exit

Router_1#wr

Router_1#

Router_2:

R2>en

R2#conf t

R2(config)#hostname Router_2

Router_2(config)#ip multicast-routing

Router_2(config)#int fa 0/1

Router_2(config-if)#ip address 10.1.12.2 255.255.255.250

Router_2(config-if)#ip pim dense-mode

Router_2(config-if)#no sh

Router_2(config-if)#exit

Router_2(config)#int fa 0/0

Router_2(config-if)#ip address 10.1.23.2 255.255.255.250

Router_2(config-if)#ip pim dense-mode

Router_2(config-if)#no sh

Router_2(config-if)#exit

Router_2(config)#int fa 1/0

Router_2(config-if)#ip address 10.1.24.2 255.255.255.250

Router_2(config-if)#ip pim dense-mode

Router_2(config-if)#no sh

Router_2(config-if)#exit

Router_2(config)#ip route 10.1.1.0 255.255.255.0 10.1.12.1

Router_2(config)#ip route 10.1.2.0 255.255.255.0 10.1.23.3

```
Router_2(config)#exit
Router_2#wr
Router_2#
```

Router_3:

```
R3>en
R3#conf t
R3(config)#hostname Router_3
Router_3(config)#ip multicast-routing
Router_3(config)#int fa 0/1
Router_3(config-if)#ip address 10.1.23.3 255.255.255.250
Router_3(config-if)#ip pim dense-mode
Router_3(config-if)#no sh
Router_3(config-if)#exit
Router_3(config)#int fa 2/0
Router_3(config-if)#ip address 10.1.34.3 255.255.255.250
Router_3(config-if)#ip pim dense-mode
Router_3(config-if)#no sh
Router_3(config-if)#exit
Router_3(config)#int fa 0/0
Router_3(config-if)#ip address 10.1.35.3 255.255.255.250
Router_3(config-if)#ip pim dense-mode
Router_3(config-if)#no sh
Router_3(config-if)#exit
Router_3(config)#ip route 10.1.1.0 255.255.255.0 10.1.23.2
Router_3(config)#ip route 10.1.2.0 255.255.255.0 10.1.35.5
Router_3(config)#exit
Router_3#wr
```

Router_3#

Router_4:

R4>en

R4#conf t

R4(config)#hostname Router_4

Router_4(config)#ip multicast-routing

Router_4(config)#int fa 1/0

Router_4(config-if)#ip address 10.1.24.4 255.255.255.250

Router_4(config-if)#ip pim dense-mode

Router_4(config-if)#no sh

Router_4(config-if)#exit

Router_4(config)#int fa 2/0

Router_4(config-if)#ip address 10.1.34.4 255.255.255.250

Router_4(config-if)#ip pim dense-mode

Router_4(config-if)#no sh

Router_4(config-if)#exit

Router_4(config)#ip route 10.1.1.0 255.255.255.0 10.1.24.2

Router_4(config)#ip route 10.1.2.0 255.255.255.0 10.1.34.3

Router_4(config)#exit

Router_4#wr

Router_4#

Router_5:

R5>en

R5#conf t

R5(config)#hostname Router_5

Router_5(config)#ip multicast-routing

Router_5(config)#int fa 0/1

Router_5(config-if)#ip address 10.1.35.5 255.255.255.250

Router_5(config-if)#ip pim dense-mode

Router_5(config-if)#no sh

Router_5(config-if)#exit

Router_5(config)#int fa 1/0

Router_5(config-if)#ip address 10.1.2.5 255.255.255.250

Router_5(config-if)#ip pim dense-mode

Router_3(config-if)#no sh

Router_5(config-if)#exit

Router_5(config)#ip route 10.1.1.0 255.255.255.0 10.1.35.3

Router_5(config)#exit

Router_5#wr

Router_5#

Построение маршрутизатор с sparse-mode

Итак, начнем с роутера Router 2.

Router_2>en

Router_2#conf t

Router_2(config)#int loopback 0 – создаем интерфейс;

Router_2(config-if)#ip address 20.20.20.20 255.255.255.255 – назначаем ему IP-адрес;

Router_2(config-if)#exit

Router_2(config)#access-list 1 permit 224.1.1.0 0.0.0.255 – создаем список доступа, чтобы проходил только наш поток;

Router_2(config)#ip pim rp-address 20.20.20.20 1 – прописываем адрес RP и привязываем к нему список доступа;

Router_2(config)#int fa 0/0

Router_2(config-if)#ip pim sparse-mode – запускаем нужный режим на интерфейсе;

Router_2(config-if)#exit

Router_2(config)#int fa 0/1

Router_2(config-if)#ip pim sparse-mode

Router_2(config-if)#exit

Router_2(config)#int fa 1/0

Router_2(config-if)#ip pim sparse-mode

Router_2(config-if)#exit

Router_2(config)#exit

Router_2#wr

Router_2#

Переходим к роутеру Router 1

Router_1>en

Router_1#conf t

Router_1(config)#ip route 20.20.20.20 255.255.255.255 10.1.12.2 – прописываем статический маршрут до RP;

Router_1(config)#access-list 1 permit 224.1.1.0 0.0.0.255

Router_1(config)#ip pim rp-address 20.20.20.20 1 – прописываем адрес RP и привязываем к нему список доступа;

Router_1(config)#int fa 0/0

Router_1(config-if)#ip pim sparse-mode

Router_1(config-if)#exit

Router_1(config)#int fa 1/0

Router_1(config-if)#ip pim sparse-mode

Router_1(config-if)#exit

Router_1(config)#exit

Router_1#wr

Router_3.

```
Router_3>en
Router_3#conf t
Router_3(config)#ip route 20.20.20.20 255.255.255.255 10.1.23.2
Router_3(config)#access-list 1 permit 224.1.1.0 0.0.0.255
Router_3(config)#ip pim rp-address 20.20.20.20 1
Router_3(config)#int fa 0/0
Router_3(config-if)#ip pim sparse-mode
Router_3(config-if)#exit
Router_3(config)#int fa 2/0
Router_3(config-if)#ip pim sparse-mode
Router_3(config-if)#exit
Router_3(config)#int fa 0/1
Router_3(config-if)#ip pim sparse-mode
Router_3(config-if)#exit
Router_3(config)#exit
Router_3#wr
Router_3#
```

Router_4.

```
Router_4>en
Router_4#conf t
Router_4(config)#ip route 20.20.20.20 255.255.255.255 10.1.24.2
Router_4(config)#access-list 1 permit 224.1.1.0 0.0.0.255
Router_4(config)#ip pim rp-address 20.20.20.20 1
Router_4(config)#int fa 1/0
Router_4(config-if)#ip pim sparse-mode
Router_4(config-if)#exit
Router_4(config)#int fa 2/0
```

```
Router_4(config-if)#ip pim sparse-mode
Router_4(config-if)#exit
Router_4(config)#exit
Router_4#wr
Router_4#
```

Router_5.

```
Router_5>en
Router_5#conf t
Router_5(config)#ip route 20.20.20.20 255.255.255.255 10.1.35.3
Router_5(config)#access-list 1 permit 224.1.1.0 0.0.0.255
Router_5(config)#ip pim rp-address 20.20.20.20 1
Router_5(config)#int fa 0/1
Router_5(config-if)#ip pim sparse-mode
Router_5(config-if)#exit
Router_5(config)#int fa 1/0
Router_5(config-if)#ip pim sparse-mode
Router_5(config-if)#exit
Router_5(config)#exit
Router_5#wr
Router_5#
```