Федеральное государственное образовательное бюджетное учреждение высшего профессионального образования

«Сибирский государственный университет телекоммуникаций и информатики»

(ФГОБУ ВПО «СибГУТИ»)

Кафедра вычислительных систем (ВС) СибГУТИ

Отчёт

по курсовому проекту по дисциплине

«Сети ЭВМ и телекоммуникации»
Вариант №9

Выполнил:
студент группы ИП-713
Михеев Н.А.

Проверил:
старший преподаватель
кафедры ВС
Крамаренко К.Е.

Новосибирск, 2020 г.

Оглавление

1. Задание на курсовой проект

На предприятии имеется три сети, объединённых при помощи пяти маршрутизаторов. Для организации связи внутри сетей используются коммутаторы: SW1, SW3, SW4. Схема соединения маршрутизаторов представлена на рисунке 1. Все каналы реализованы с использованием технологии Fast Ethernet.

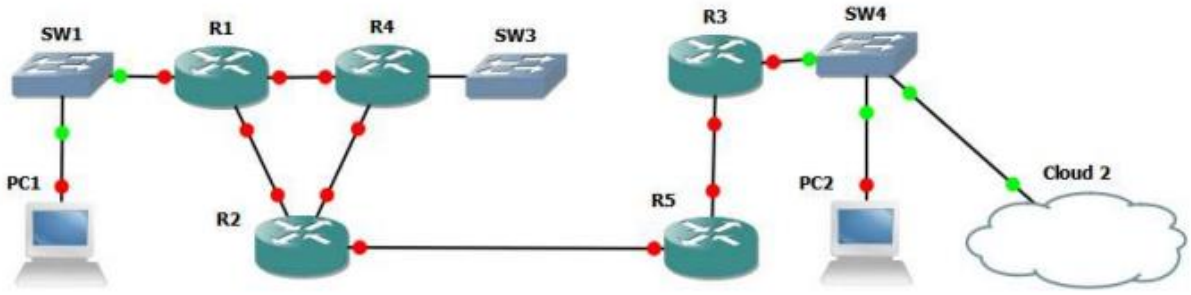

Рисунок 1 – Схема связей сети

Предприятию выделена сеть 10.9.0.0/16. Администратором сети (т.е. Вами) имеющаяся сеть разделена на необходимое количество подсетей. Маршрутизаторы реализуют протокол автоматического обмена таблицами маршрутизации OSPF. В сети имеется один сервер системы имен DNS (на компьютере PC2). Указанный сервер функционирует под управлением операционной системы Microsoft Windows Server (версия не ниже 2003). Компьютер PC2 выступает источником многоадресной рассылки видеопотока (один канал, транслируется бесконечно). Для рекурсивных запросов DNS использует сервер физической сети. Для доступа к этой сети компьютер PC2 либо оснащается дополнительным сетевым интерфейсом, либо реализует IP-алиас. Компьютер PC1 – пользовательская рабочая станция. Он может подключаться к произвольной сети (в процессе отладки сети должна быть проверена его работоспособность во всех сетях предприятия). Указанный компьютер используется для просмотра видеопотока.

2. Постановка задачи

1. Рассчитайте схему деления имеющейся сети на подсети исходя из следующего количества компьютеров в каждой из них: SW1 – (день Вашего рождения * количество полных лет Вам на текущий момент), SW3 – (номер Вашей группы + месяц Вашего рождения), SW4 – (год Вашего рождения). Приведите обоснование своего решение (почему разделили сеть именно таким образом).

2. Установите операционную систему и программное обеспечение просмотра IpTV на рабочую станцию пользователя. Обоснуйте выбор операционной системы и програмного обеспечения для просмотра IpTV.
3. Сконфигурируйте маршрутизаторы сети так, чтобы они имели связь к непосредственно подключенными сетями. Продемонстрируйте работоспособность текущей конфигурации (с использованием ping).

4. Настройте маршрутизаторы на использование протокола динамической маршрутизации. Используя сетевой монитор Wireshark приведите структуру пакетов, используемых протоколом динамической маршрутизации для своего функционирования. Объясните какой тип пакета для чего используется в рамках реализации протокола

5. Установите на сервере PC2 операционную систему. Сконфигурируйте службу DNS так, чтобы она обрабатывала запросы от клиентов для одной зоны (имя зоны выбирается самостоятельно). Для обработки рекурсивных запросов настройте сервер так, чтобы он ретранслировал их на внешний DNS. Используя рабочую станцию и сетевой монитор приведите пример диалога, происходящего при получении DNS запросов и ответом на них.

6. Установите на сервере VLC media player и настройте его так, чтобы он осуществлял многоадресную рассылку видеопотока (содержание видеопотока выбирается произвольно и передается непрерывно «в цикле»).

7. Используя сетевой монитор Wireshark продемонстрируйте работу протокола IGMP.

8. Сконфигурируйте маршрутизаторы для передачи многоадресного трафика. В качестве протокола динамической маршрутизации многоадресного трафика используйте протокол PIM-SM. Продемонстрируйте работу этого протокола с использованием сетевого монитора.

3. Описание используемых технологий и протоколов

- **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 из популярных 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.

- **OSPF —** Популярным протоколом динамической маршрутизации в локальных сетях ЭВМ. Протокол был разработан IETF в 1988 году. Последняя версия протокола представлена в RFC 23284.

  Протокол OSPF имеет меньшее время сходимости, чем протокол RIP. Кроме того, OSPF изначально учитывает описание сетей с помощью масок переменной длинны (VLSM).

  Протокол OSPF относится к протоколам состояния каналов. Основная идея протоколов этого класса состоит в том, что маршрутизаторы рассылают информацию о состоянии своих каналов и ретранслируют сообщения о состоянии каналов других маршрутизаторов. В результате каждый маршрутизатор отвечает только за собственные каналы, но имеет информацию о состоянии каналов всех своих соседей.

  Собрав информацию от своих соседей маршрутизатор самостоятельно строит свое видение топологии сети и выбирает кратчайшие маршруты до всех известных ему сетей. Поиск маршрутов в OSPF производится с помощью алгоритма Дейкстра.

  Следует отметить, что протокол OSPF поддерживает три типа сетей: широковещательные (Ethernet, Token Ring), точка-точка (T1, E1) и сети с множественным доступом (Frame Relay). Далее в этой лабораторной работе рассматривается работа протокола OSPF только в широковещательных сетях.

- **Протокол PIM-SM** версия разряженного режима PIM-SM **(Protocol Independent Multicast — Sparse Mode).** Главной особенностью протокола PIM-SM является то, что он рассчитан на работу в разряженном режиме, то есть он посылает групповые пакеты только по явному запросу получателя. Для доставки данных каждой конкретной группе получателей протокол PIM-SM строит одно разделяемое дерево, общее для всех источников этой группы. Вершина разделяемого дерева не может располагаться в источнике, так как источников может быть несколько. В качестве вершины разделяемого дерева используется специально выделенный для этой цели маршрутизатор, выполняющий функции точки встречи (RP). Все маршрутизаторы в пределах домена PIM-SM должны обладать согласованной информацией о расположении точки встречи. Различные группы могут иметь как одну и ту же, так и разные точки встречи. Самым распространенным и, возможно, самым простым способом конфигурирования локальных (в пределах одного домена PIM-SM) точек встречи является назначение их статически среди множества

маршрутизаторов данного домена. Это приводит к весьма определенной конфигурации и позволяет в дальнейшем легче находить ошибки, чем при других подходах. Для получателей каждой конкретной группы и источников, вещающих на эту группу, маршрутизатор точки встречи является посредником, который связывает их между собой. Процесс доставки протоколом PIM-SM группового трафика от источника к получателям, принадлежащим некоторой группе, может быть представлен трехэтапным: построение разделяемого дерева с вершиной в точке встречи, которое описывает пути доставки групповых пакетов между точкой встречи и членами данной группы. Это дерево называют также деревом точки встречи (Rendezvous Point Tree, RPT); построение дерева кратчайшего пути (Shortest Path Tree, SPT), которое будет достав лять пакеты между источником данной группы и точкой встречи; построение набора SPT-деревьев, которые ради повышения эффективности будут использованы для доставки пакетов непосредственно между источником и каждым из получателей группы.

- **DNS**

Служба Доменных Имен предназначена для того, чтобы машины, работающие в Internet, могли по доменному имени узнать IP-адрес нужной им машины, а также некоторую другую информацию; а по IP-номеру могли узнать доменное имя машины.

Служба Доменных Имен была разработана для именования машин в глобальной сети. Основной особенностью глобальной сети является распределенное администрирование, когда один администратор физически не может уследить за выделением имен. Поэтому Служба Доменных Имен функционирует на принципе делегирования полномочий.

Каждая машина либо знает ответ на вопрос, либо знает кого спросить. При правильном функционировании система замкнута, т.е. если запрошенная информация имеется у кого-либо, то она будет найдена и сообщена клиенту, либо, если вопрос не имеет ответа, клиент получит сообщение о невозможности получения ответа на вопрос.

Каждый клиент знает своего сервера; обычно указывается не один, а несколько серверов - если первый не отвечает, клиент обращается ко второму и так далее до исчерпания списка. В принципе неважно, к какому серверу обращаться - они дают (должны давать при правильном функционировании)

одинаковые ответы на любой запрос. Поэтому для ускорения работы обычно указывают ближайший. Следует помнить, что на одной машине могут функционировать одновременно Name-сервер и программы-клиенты; поэтому если на машине запущен Name-сервер, то в качестве Name-сервера на ней должен быть прописан "я сам".

Имеется некий домен верхнего уровня, обозначаемый точкой: "." Имеется девять серверов (как минимум), которые отвечают за эту зону. Они не знают ни одного доменного имени - они только авторизуют серверы верхних зон. Серверы верхних зон тоже гнушаются хранить информацию о конкретных машинах и передают это право нижележащим серверам. Тут уже появляются первые упоминания о конкретных машинах, равно как и происходит авторизация нижележащих серверов.

- **UDP**

UDP (User Datagram Protocol) — один из ключевых элементов TCP/IP, набора сетевых протоколов для Интернета. С UDP компьютерные приложения могут посылать сообщения другим хостам по IP-сети без необходимости предварительного сообщения для установки специальных каналов передачи или путей данных.

UDP использует простую модель передачи, без неявных «рукопожатий» для обеспечения надёжности, упорядочивания или целостности данных. Таким образом, UDP предоставляет ненадёжный сервис, и датаграммы могут прийти не по порядку, дублироваться или вовсе исчезнуть без следа. UDP подразумевает, что проверка ошибок и исправление либо не нужны, либо должны исполняться в приложении. Чувствительные ко времени приложения часто используют UDP, так как предпочтительнее сбросить пакеты, чем ждать задержавшиеся пакеты, что может оказаться невозможным в системах реального времени. При необходимости исправления ошибок на сетевом уровне интерфейса приложение может задействовать TCP или SCTP, разработанные для этой цели.

Природа UDP как протокола без сохранения состояния также полезна для серверов, отвечающих на небольшие запросы от огромного числа клиентов, например, DNS и потоковые мультимедийные приложения вроде IPTV, Voice over IP, протоколы туннелирования IP и многие онлайн-игры.

- **IGMP**

Протокол группового управления в Интернете (Internet Group Management Protocol, IGMP), разработанный в 1989 году, используется исключительно при

взаимодействии непосредственно связанных друг с другом маршрутизатора и хоста, когда последний вы

ступает (или желает выступать) в роли получателя трафика группового вещания.

К основным функциям протокола IGMP относятся оповещение маршрутизатора о желании хоста быть включенным в группу и опрос членов группы.

Оповещение маршрутизатора о желании хоста быть включенным в группу. Чтобы стать получателем групповых данных, узел должен «выразить» свою заинтересованность маршрутизатору, к которому непосредственно подсоединена его сеть. Для этого хост должен установить взаимодействие с маршрутизатором по протоколу IGMP Версия IGMP для

хоста непосредственно зависит от типа операционной системы, установленной на хосте.

Так, ранние версии Windows (Windows 95) поддерживали только версию IGMPvl, более поздние (Windows 2000) — версию IGMPv2, а начиная с Windows XP поддерживается версия IGMPv3. Протоколы IGMPv2 и IGMPv3 поддерживаются во многих версиях Mac OS, Linux, UNIX-подобных операционных системах.

Опрос членов группы. Для выполнения этой функции один из маршрутизаторов локальной сети выбирается доминирующим. Доминирующий маршрутизатор средствами протокола IGMP периодически опрашивает все системы (групповой адрес 224.0.0.1) в непосредственно присоединенных к нему подсетях, проверяя, активны ли члены всех известных ему групп. Остальные (невыбранные) маршрутизаторы прослушивают сеть, и если обнаруживают отсутствие сообщений-запросов в течение некоторого периода (обычно 250 секунд), то повторяют процедуру выбора нового доминирующего маршрутизатора.

В IGMPv2 определено три типа сообщений:

1. *Запрос о членстве (membership query).* С помощью этого сообщения маршрутизатор пытается узнать, в каких группах состоят хосты в локальной сети, присоединенной к ка кому-либо его интерфейсу. Запрос о членстве существует в двух вариантах: в одном из них маршрутизатор делает общий запрос обо всех группах, в другом его интересует информация только о какой-то конкретной группе, адрес которой указывается в запросе.

2. *Отчет о членстве (membership report).* Этим сообщением хосты отвечают маршрутизатору, который послал в сеть запрос о членстве. В сообщении содержится информация об адресе группы, в которой они состоят.

Маршрутизатор, являясь членом всех групп, получает сообщения, направленные на любой групповой адрес. Для маршрутизатора, получающего ответные сообщения, важен только факт наличия членов той или иной группы (групп), а не принадлежность конкретных хостов конкретным группам. Этот факт будет использован другими маршрутизаторами сети для продвижения пакетов группового вещания в ту часть сети, за которую «отвечает» данный маршрутизатор. Отчет о членстве хост может послать не только в ответ на запрос маршрутизатора, но и по собственной инициативе, когда он пытается присоединиться к определенной группе.

После такого сообщения хост может рассчитывать на то, что трафик для этой группы действительно будет доставляться в сеть, к которой этот хост принадлежит.

3. *Покинуть группу (leave group).* Это сообщение хост может использовать, чтобы сигнализировать «своему» маршрутизатору о желании покинуть определенную группу, в которой он до этого состоял. Получив это сообщение, маршрутизатор посылает специфический запрос о членстве членам только этой конкретной группы, и если не получает на него ответа (что говорит от том, что это последний хост в группе), то перестает передавать трафик группового вещания для этой группы. Слово «может» означает в данном случае,

что хост может быть исключен из группы, просто не отвечая маршрутизатору на запрос о членстве (такой подход реализован в протоколе IGMP vl). Тогда маршрутизатор будет

продолжать передавать нежелательный трафик группового вещания до тех пор, пока не истечет некоторый период времени с момента поступления последнего отчета о членстве.

Такой подход может значительно удлинить период скрытого нахождения хоста в состоянии выхода из группы, что снижает эффективность работы сети.

4. Реализация

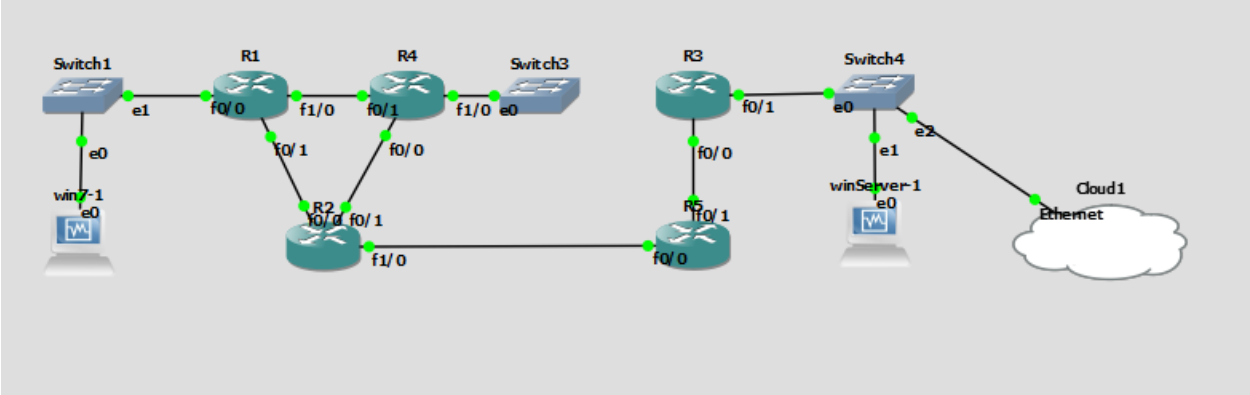

Рис. 2 – готовая конфигурация в gns3

Расчет схемы деления имеющейся сети на подсети

Для SW1 – 4 * 21 = 84 устройства, выбрана маска длиной 24 бита;

SW3 – 713 + 5 = 718 устройств, выбрана маска длиной 22 бита;

SW4 – 1999 устройств, соответствующая маска длиной в 21 бит.

Для удобства настройки маршрутизаторов их интерфейсам были присвоены последовательные ip адреса.

Чтобы адреса подсетей коммутаторов не накладывались на адреса между маршрутизаторами и не перекрывались между собой было решено использовать для третьего октета первый бит + последний бит определяющий адрес подсети:

64 + 1 = 65 для SW1

64 + 10 = 74 для SW3

64 + 12 = 76 для SW4

При такой конфигурации каждая подсеть будет иметь достаточное количество ip адресов с небольшим запасом и с учётом того, что некоторые ip адреса будут гарантировано заняты под адрес шлюза и служебные нужды.

Настройка рабочей станции пользователя

В работе используется ОС Microsoft Windows 7, Microsoft Windows Server 2008 R2.

В качестве ПО для просмотра и трансляции IPTV была выбрана программа VLC Media Player от Videolan

Программа работает на большинстве современных операционных систем и мобильных платформ, в частности Android, iOS, Tizen и Windows 10 Mobile.

Плеер VLC можно использовать в качестве сервера для трансляции потока аудио/видео по сети (поддерживает протоколы IPv4 и IPv6). Для воспроизведения файлов мультимедиа не требуется установка дополнительных кодеков, они уже «встроены» в программу. VLC может воспроизводить DVD и потоковое незашифрованное (без DRM) видео (IPTV) и интернет-радио. Также программа может записывать потоковое аудио/видео на компьютер. VLC воспроизводит испорченные файлы — например, с повреждёнными индексами.

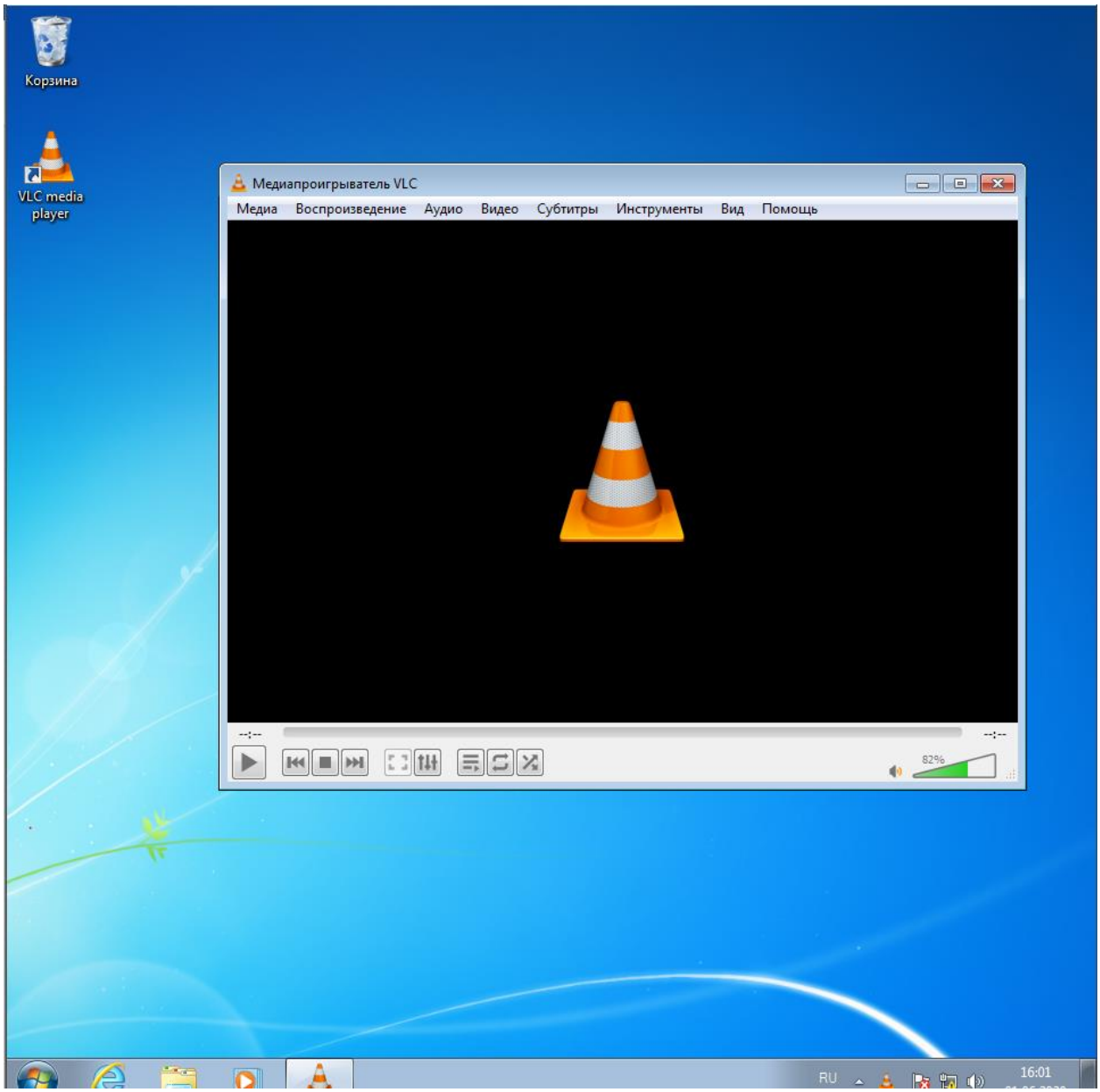

Рис.3 – VLC Media Player на клиентской виртуальной машине

Настройка маршрутизаторов сети

Для динамической маршрутизации был применен протокол OSPF на всех маршрутизаторах

```
R1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     20.0.0.0/32 is subnetted, 1 subnets
S       20.20.20.20 is directly connected, FastEthernet0/1
     10.0.0.0/8 is variably subnetted, 10 subnets, 2 masks
O       10.9.3.0/24 [110/11] via 10.9.4.2, 00:24:11, FastEthernet1/0
C       10.9.2.0/24 is directly connected, FastEthernet0/1
O       10.9.6.0/24 [110/21] via 10.9.2.2, 00:24:01, FastEthernet0/1
O       10.9.5.0/24 [110/11] via 10.9.2.2, 00:24:01, FastEthernet0/1
C       10.9.4.0/24 is directly connected, FastEthernet1/0
O       10.9.20.1/32 [110/22] via 10.9.2.2, 00:24:02, FastEthernet0/1
S       10.9.20.0/24 is directly connected, FastEthernet0/1
C       10.9.65.0/24 is directly connected, FastEthernet0/0
O       10.9.74.0/24 [110/2] via 10.9.4.2, 00:24:12, FastEthernet1/0
O       10.9.76.0/24 [110/31] via 10.9.2.2, 00:24:02, FastEthernet0/1
R1#
```

Рис.4 – вариант настроенной сети по протоколу OSPF на R1

210	308.398525	10.9.2.1	224.0.0.5	OSPF	122 LS Update
211	308.419977	10.9.2.1	224.0.0.5	OSPF	94 LS Update
212	308.774040	10.9.2.1	224.0.0.5	OSPF	94 Hello Packet
213	309.804028	10.9.2.2	224.0.0.5	OSPF	122 LS Update
216	310.898385	10.9.2.2	224.0.0.5	OSPF	98 LS Acknowledge
218	312.325348	10.9.2.1	224.0.0.5	OSPF	78 LS Acknowledge
220	316.508855	10.9.2.2	224.0.0.5	OSPF	94 Hello Packet
222	317.141893	10.9.2.2	224.0.0.5	OSPF	122 LS Update
223	317.195525	10.9.2.2	224.0.0.5	OSPF	94 LS Update
224	318.279171	10.9.2.1	224.0.0.5	OSPF	94 Hello Packet
225	319.631017	10.9.2.1	224.0.0.5	OSPF	98 LS Acknowledge
227	320.006533	10.9.2.2	224.0.0.5	OSPF	110 LS Update
228	320.060178	10.9.2.2	224.0.0.5	OSPF	94 LS Update
230	322.517128	10.9.2.1	224.0.0.5	OSPF	98 LS Acknowledge
232	325.501749	10.9.2.2	224.0.0.5	OSPF	94 Hello Packet

Рис.5 – Hello-Пакеты OSPF

Итак, я включил OSPF на R1, и он начал каждые 10 секунд отправлять Hello-пакеты. Включив OSPF на R2 - проследил как будут устанавливаться отношения соседства. Сначала происходит Link State Update – обновление состояния канала, посылается по групповому адресу на один транзитный участок. И далее идет Link State Acknowledge - подтверждение получение пакета Link State Update.

Настройка Windows Server

В качестве роли для сервера была установлена роль DNS – сервера

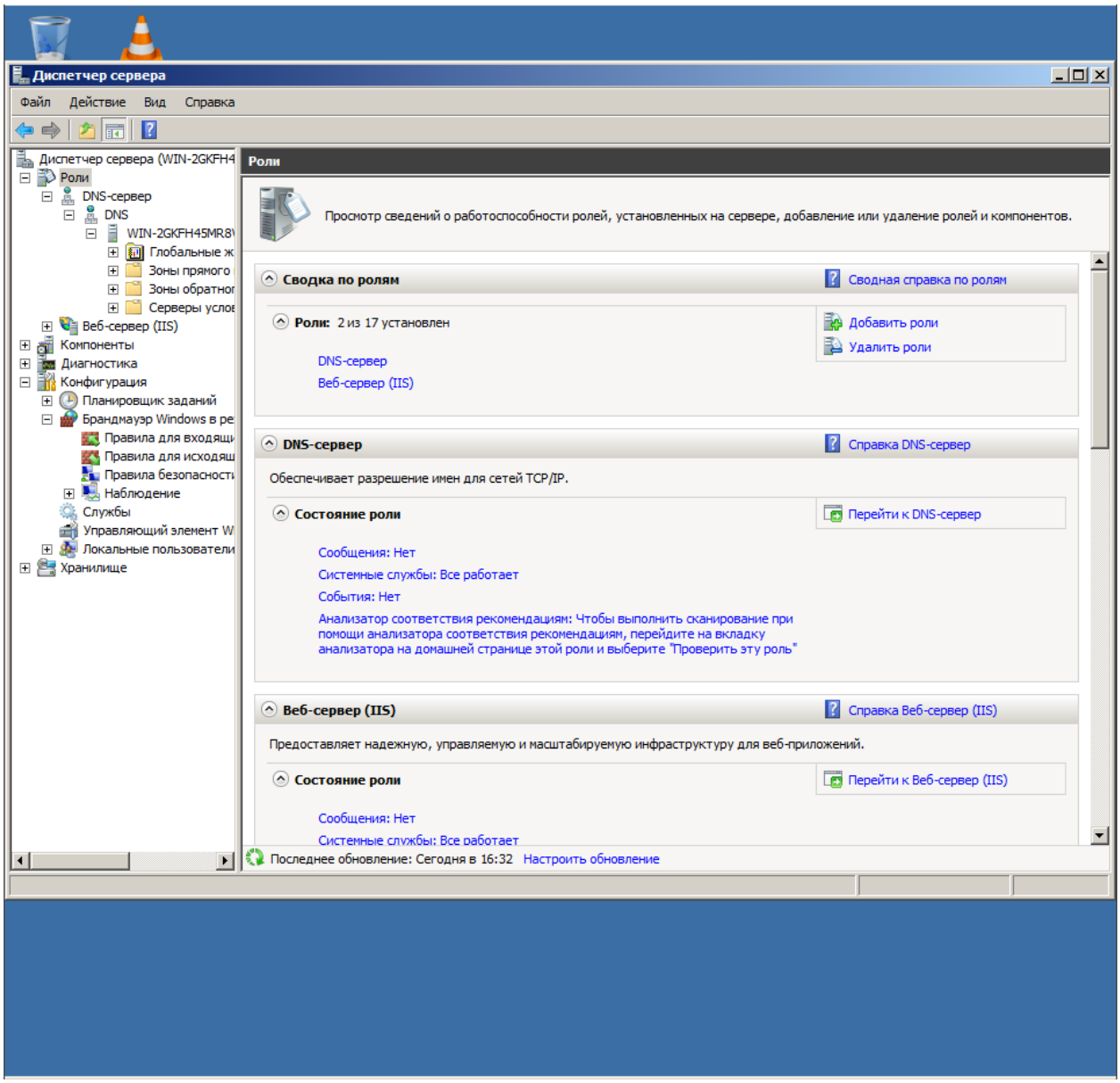

Рис. 6 – обзор ролей сервера

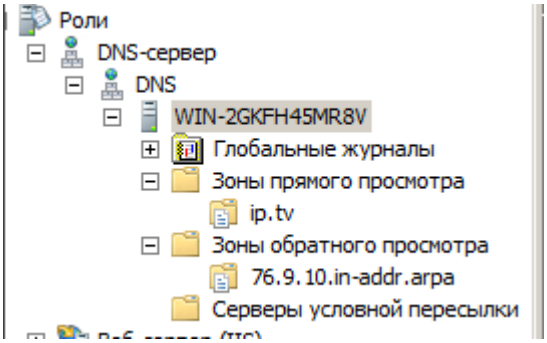

Рис.7 – для работы были прописаны зоны прямого и обратного просмотра на сервере

Настройка многоадресной рассылки потока и протокола PIM-SM

В качестве ПО вещания IPTV была выбрана программа VLC Media Player.

Переходим к настройке sparse-mode протокола PIM. Для этого режима необходимо выбрать так называемую точку рандеву (Rendezvous point). Пусть для этих целей служит R2. В качестве IP-адреса точки будем использовать loopback0.

Запускаем VLC Media Player на Windows Server 2008 и выбираем видеофайл для трансляции.

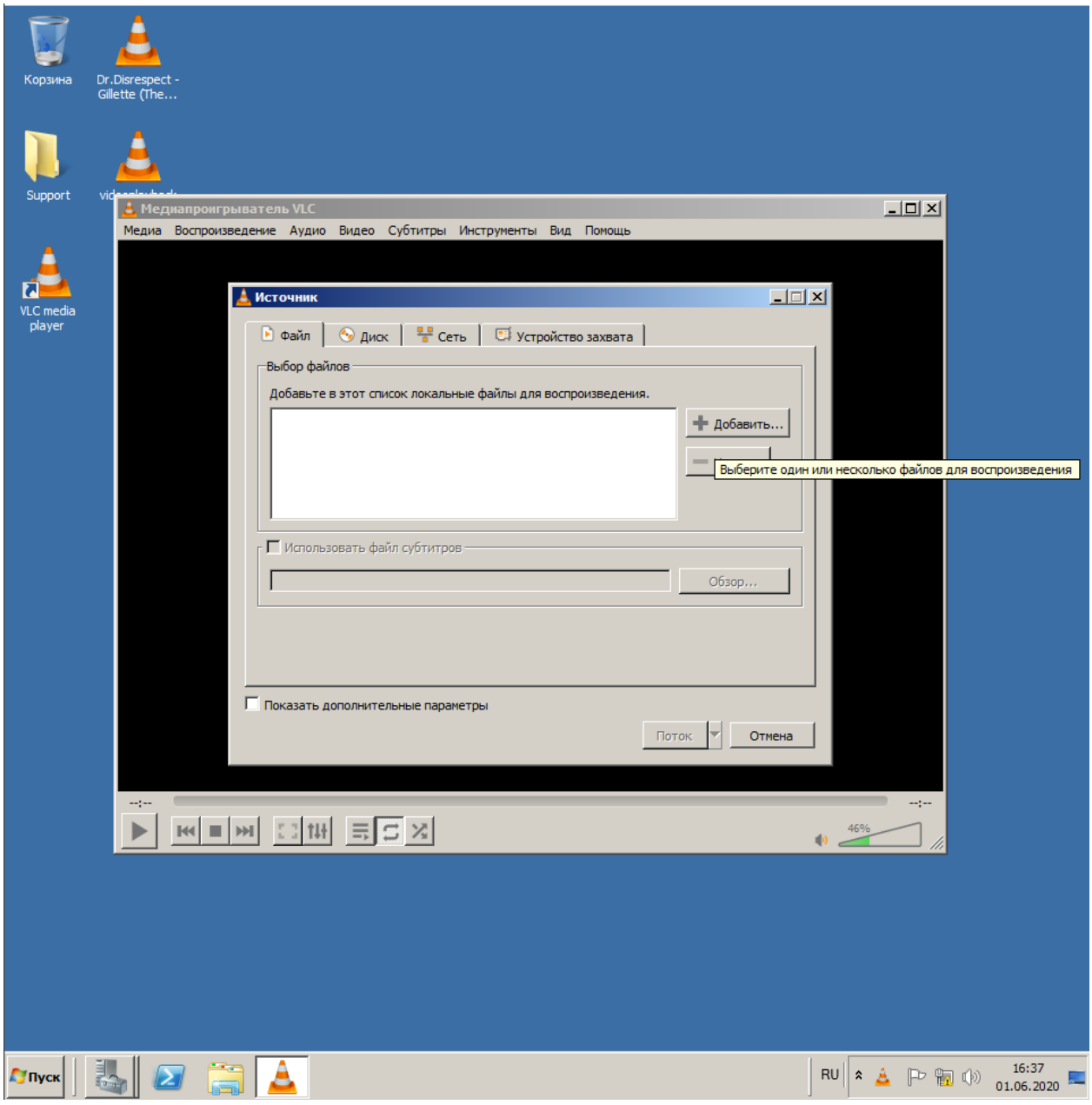

Рис.8 – Выбор файла, который будем транслировать

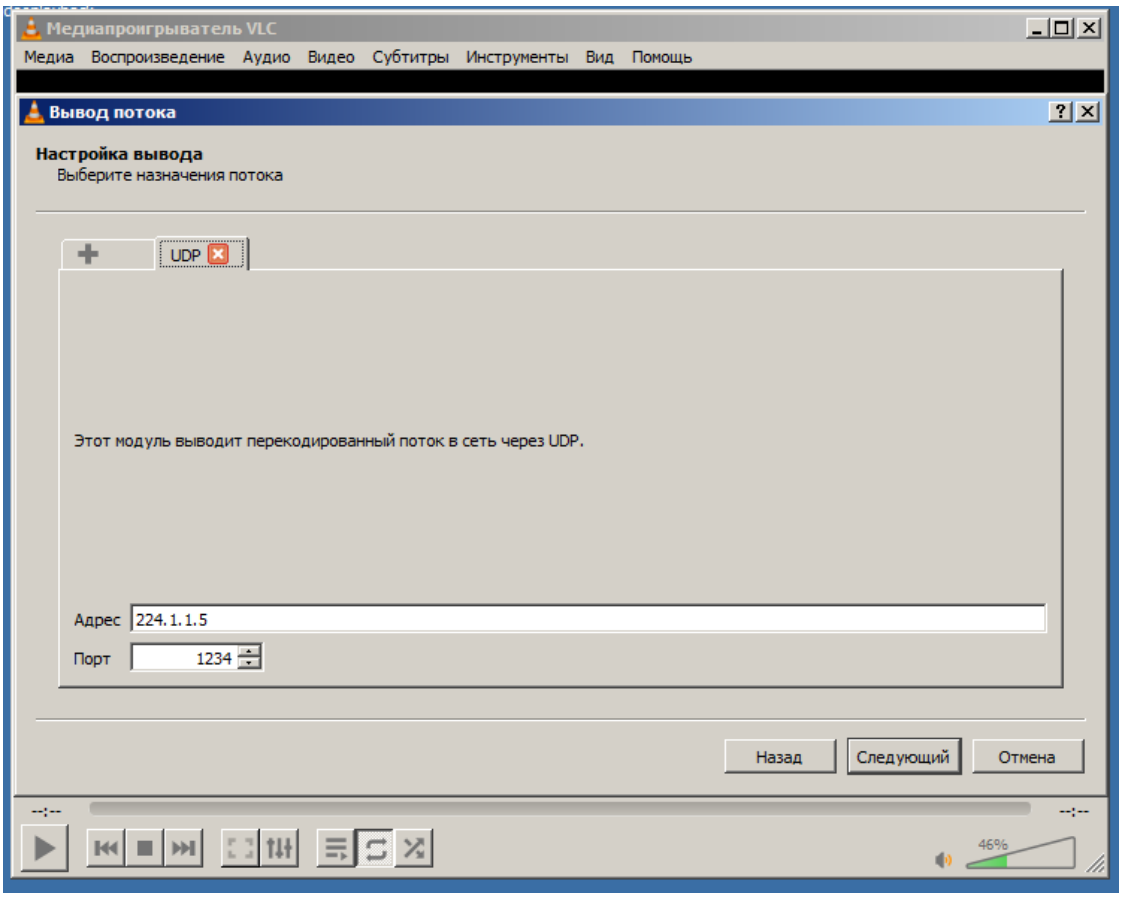

Рис.9 – настойка вывода потока

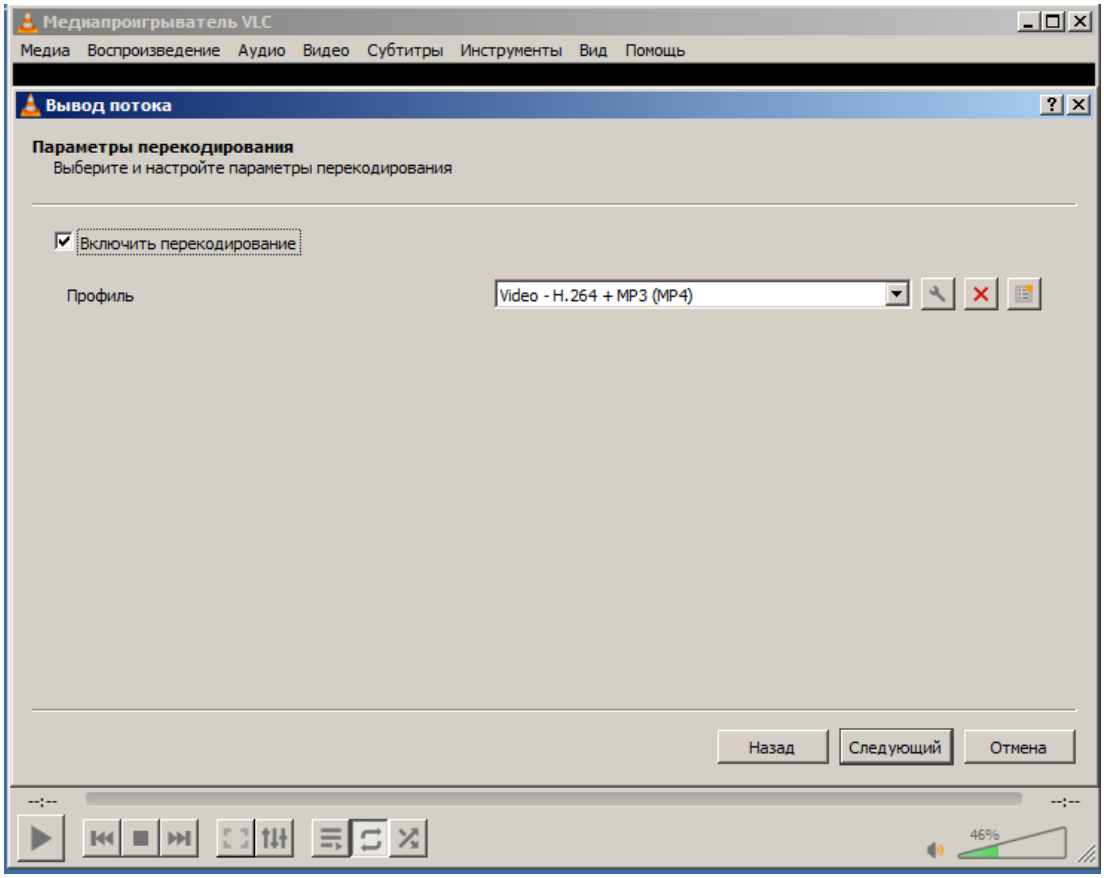

Рис.10 – включение кодировщика для оптимизации качества

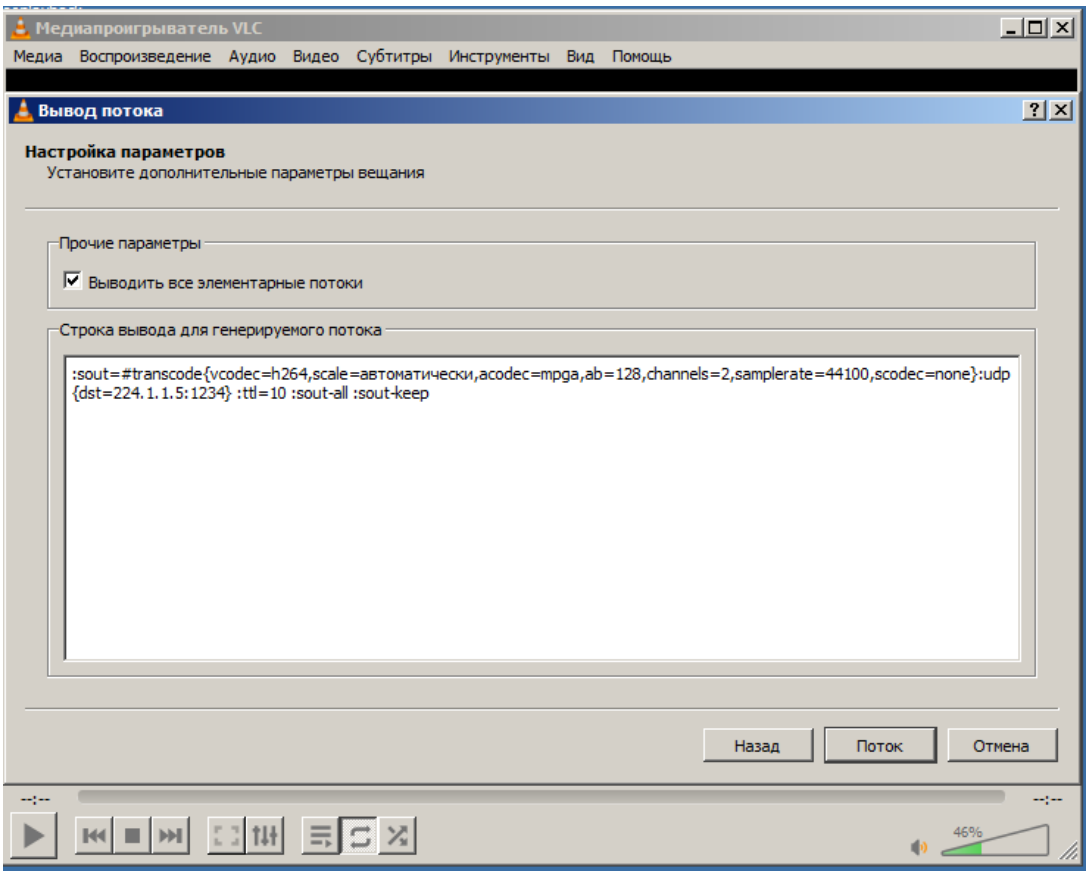

Рис.11 – ввод дополнительных параметров трансляции

Обязательным является добавление параметра времени жизни Time to Live: 10, так как по умолчанию стоит -1, из-за чего пакеты могут не доходить до клиента.

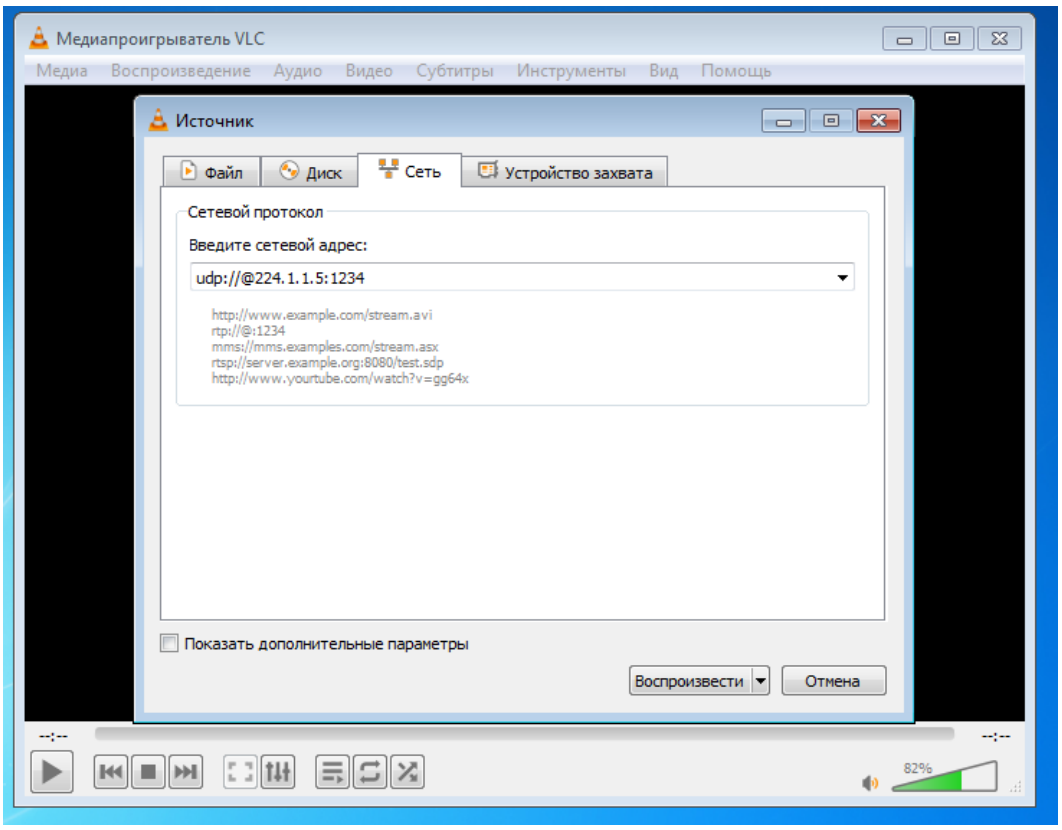

Рис.12 – старт просмотра на клиенте

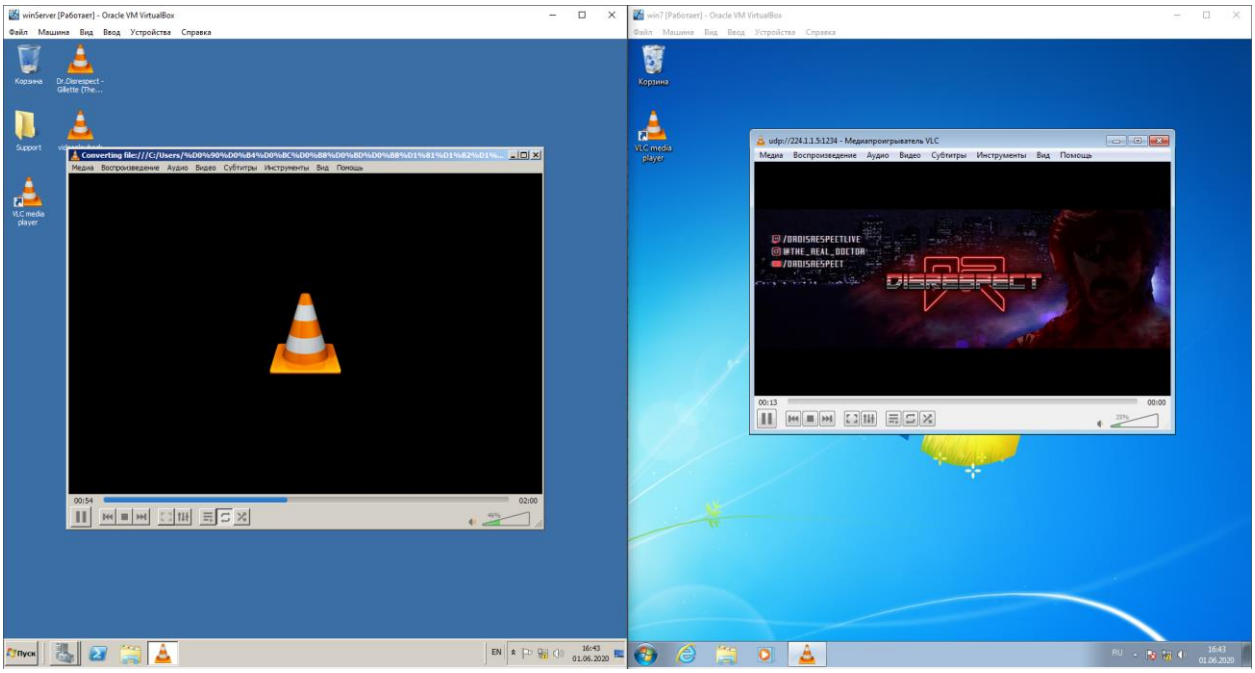

Рис.13 – произошел мгновенный старт видео на клиенте

```
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report,
       Z - Multicast Tunnel, z - MDT-data group sender,
       Y - Joined MDT-data group, y - Sending to MDT-data group
Outgoing interface flags: H - Hardware switched, A - Assert winner
 Timers: Uptime/Expires
 Interface state: Interface, Next-Hop or VCD, State/Mode

(*, 239.255.255.250), 00:59:30/00:02:21, RP 10.9.6.1, flags: SJC
  Incoming interface: FastEthernet0/1, RPF nbr 10.9.2.2
  Outgoing interface list:
    FastEthernet0/0, Forward/Sparse, 00:59:30/00:02:21

(*, 224.1.1.5), 00:00:56/stopped, RP 10.9.20.1, flags: SJC
  Incoming interface: FastEthernet0/1, RPF nbr 10.9.2.2
  Outgoing interface list:
    FastEthernet0/0, Forward/Sparse, 00:00:56/00:02:25

(10.9.76.2, 224.1.1.5), 00:00:58/00:02:59, flags: JT
  Incoming interface: FastEthernet0/1, RPF nbr 10.9.2.2
  Outgoing interface list:
    FastEthernet0/0, Forward/Sparse, 00:00:58/00:02:23

(*, 224.0.1.40), 01:00:41/00:02:27, RP 10.9.6.1, flags: SJCL
  Incoming interface: FastEthernet0/1, RPF nbr 10.9.2.2
  Outgoing interface list:
    FastEthernet0/0, Forward/Sparse, 01:00:41/00:02:26
```

Рис.14 – таблица мультикаст маршрутизации на одном из роутеров

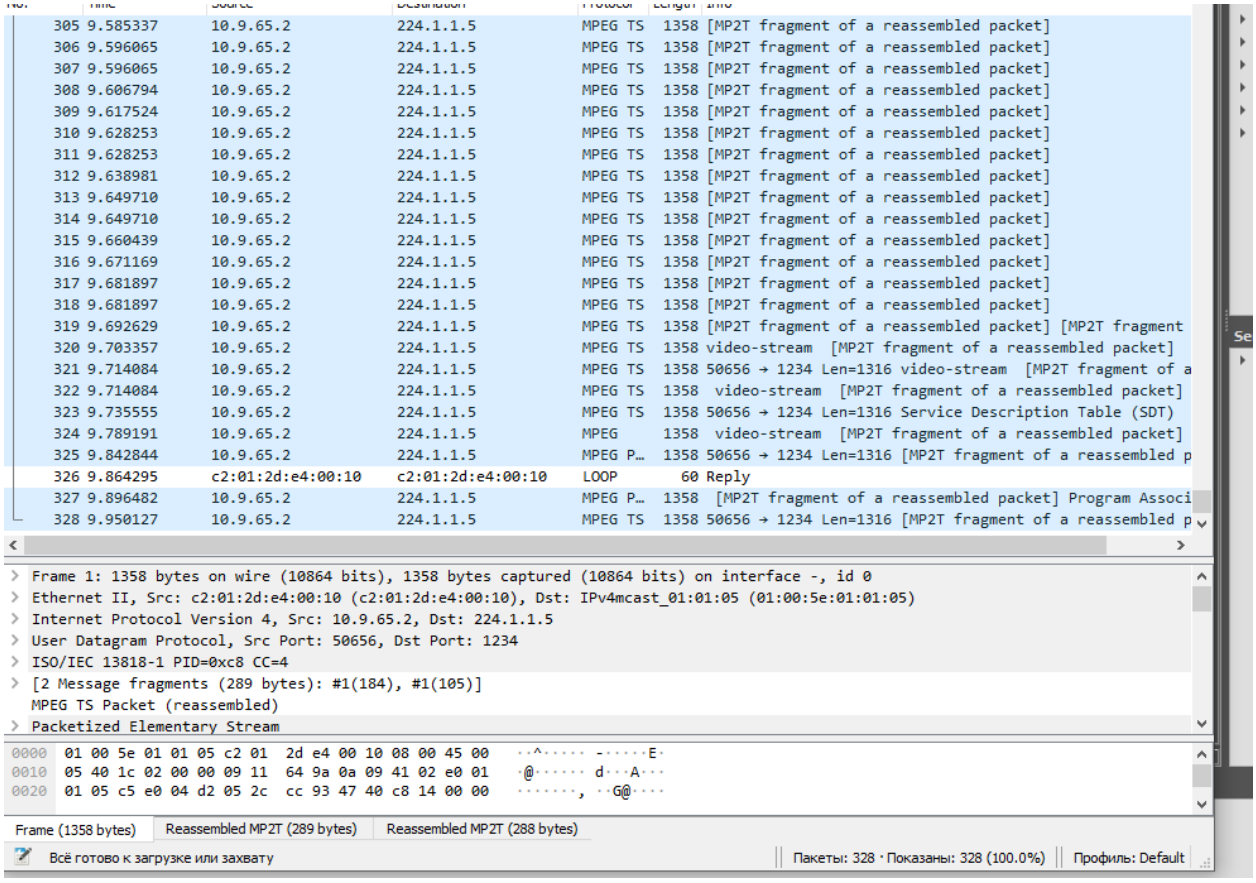

Рис.15 – мониторинг работы протокола через wireshark

5. Вывод

В ходе выполнения данной работы мною были получены практические знания по настройке сети с использованием IPTV, установке необходимого клиентского программного обеспечения, настройки динамической маршрутизации OSPF, конфигурирования DHCP-сервера.