

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ  
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ  
«СИБИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ  
ТЕЛЕКОММУНИКАЦИЙ И ИНФОРМАТИКИ»

Кафедра вычислительных систем

**Отчёт**  
по курсовому проекту по дисциплине  
“Сети ЭВМ и телекоммуникации”  
**Вариант № 2**

Выполнил:  
студент гр. ИП-514

\_\_\_\_\_ /Д.П. Сахарчук/  
подпись

Проверил:  
ст. п кафедры ВС

\_\_\_\_\_ /К.Е. Крамаренко/  
ОЦЕНКА, подпись

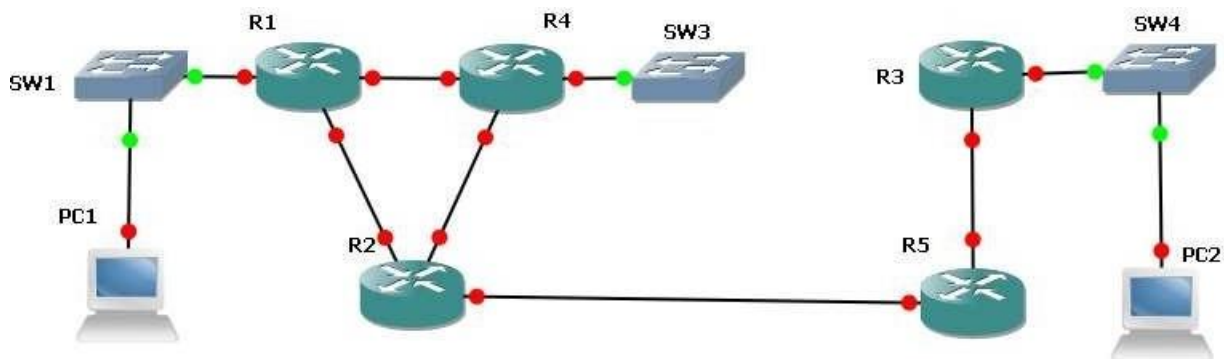
Новосибирск, 2018 г.

## Оглавление

1	Цель работы.....	3
2	Задания.....	3
3	Теоретические сведения .....	5
3.1	Используемые технологии и программное обеспечение .....	5
3.2	Используемые протоколы .....	6
4	Выполнение .....	9
4.1	Конфигурация сети .....	9
4.2	Конфигурация рабочей станции .....	9
4.3	Настройка маршрутизаторов сети .....	9
4.4	Конфигурация сервера .....	12
4.5	Настройка PIM_DM и IGMP .....	14
4.6	Настройка VLC .....	15
5	Вывод .....	19

## 1 Цель работы

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 2. Все каналы реализованы с использованием технологии Fast Ethernet.



*Рисунок 1– Схема связей сети*

Предприятию выделена сеть 10.2.0.0/16. Администратором сети (т.е. Вами) имеющаяся сеть разделена на необходимое количество подсетей. Маршрутизаторы реализуют протокол автоматического обмена таблицами маршрутизации RIP.

В сети имеется один сервер автоматической конфигурации сетевых параметров узлов DHCP (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). 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 Задания

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 решения (почему разделили сеть именно таким образом).

2. Установите операционную систему и программное обеспечение просмотра IpTV на рабочую станцию пользователя. Обоснуйте выбор операционной системы и программного 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 DHCP так, чтобы она обрабатывала запросы от клиентов из всех подсетей предприятия. Сделайте необходимые изменения в конфигурации маршрутизаторов (DHCP-relay, ip helper-address). Используя рабочую станцию и сетевой монитор приведите пример диалога, происходящего при получении сетевых настроек впервые и повторно.

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-DM. Продемонстрируйте работу этого протокола с использованием сетевого монитора.

### 3 Теоретические сведения

#### 3.1 Используемые технологии и программное обеспечение

- **IP TV** – это современная технология, позволяющая эффективно передавать телевизионный сигнал через сеть Интернет. Это полностью интерактивный сервис, функционирующий в Интернете. Данная технология позволяет получить идеальное качество изображения и звука, а также значительно расширить возможности телевидения путем добавления дополнительных сервисов. IPTV — вещание не имеет ограничения по количеству телеканалов и количеству транслируемого контента. Ограничения могут возникать лишь в пропускной способности сети оператора IPTV и интернет провайдера предоставляющих услуги конечному абоненту.
- **VLC** — бесплатный и свободный кроссплатформенный медиаплеер и медиаплатформа с открытым исходным кодом. VLC воспроизводит множество мультимедийных файлов, а также DVD, Audio CD, VCD и сетевые трансляции.
  - 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.
- **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.
- **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.
- **VirtualBox** – среда моделирования ЭВМ. Используется для эмулирования оконечных сетевых устройств или промежуточных устройств, реализованных на базе ЭВМ с архитектурой IBM/PC.
- **Windows Server 2008** — операционная система семейства Windows NT от компании Microsoft, предназначенная для работы на серверах

- **Ubuntu 16.04 LTS** - операционная система, основанная на Debian GNU/Linux. Основным разработчиком и спонсором является компания Canonical. В настоящее время проект активно развивается и поддерживается свободным сообществом.

### 3.2 Используемые протоколы

- **DHCP** — сетевой протокол, позволяющий компьютерам автоматически получать IP-адрес и другие параметры, необходимые для работы в сети TCP/IP. DHCP является клиент-серверным протоколом, то есть в его работе участвуют клиент DHCP и сервер DHCP. Передача данных производится при помощи UDP. По умолчанию запросы от клиента делаются на 67 порт к серверу, сервер в свою очередь отвечает на порт 68 к клиенту, выдавая адрес IP и другую необходимую информацию (сетевую маску, шлюз по умолчанию и серверы DNS). Сетевой администратор может задать диапазон адресов, распределяемых сервером среди компьютеров. Это позволяет избежать ручной настройки компьютеров сети и уменьшает количество ошибок.

- **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.

- **RTP (Real-time Transport Protocol)** – работает на уровне приложений (OSI - 7) и используется при передаче трафика реального времени.

- RTP переносит в своём заголовке данные, необходимые для

восстановления аудиоданных или видеоизображения в приёмном узле, а также данные о типе кодирования информации (JPEG, MPEG и т. п.). В заголовке данного протокола, в частности, передаются временная метка и номер пакета. Эти параметры позволяют при минимальных задержках определить порядок и момент декодирования каждого пакета, а также интерполировать потерянные пакеты.

- В протокол заложена возможность компенсации джиттера и обнаружения нарушения последовательности пакетов данных — типичных событий при передаче через IP-сети.
- RTP поддерживает передачу данных для нескольких адресатов через Multicast.
- **IGMP** — протокол управления групповой (multicast) передачей данных в сетях, основанных на протоколе IP. IGMP используется клиентским компьютером и соседними коммутаторами для соединения клиента и локального маршрутизатора, осуществляющего групповую передачу. Далее между локальным и удаленным маршрутизаторами используется PIM, с его помощью групповой трафик направляется от видеосервера к многочисленным клиентам групповой передачи.
  - IGMP реализован в виде серверной и клиентской частей, первая из которых выполняется на маршрутизаторе, вторая — в узле сети, получающем групповой трафик. Клиент посылает уведомление о принадлежности к какой-либо группе локальному маршрутизатору, в это время маршрутизатор находится в ожидании уведомлений и периодически рассылает клиентам запросы.
- **Protocol Independent Multicast (PIM)** — это группа протоколов, которые занимаются маршрутизацией мультикаст. И, хотя некоторые основы работы протоколов из этой группы одинаковы, каждый конкретный протокол работает по-разному. "Protocol independent" в названии протокола означает, что PIM может работать с unicast таблицей маршрутизации, независимо от того, как именно она заполнена. То есть, он может использовать, например, маршруты OSPF, EIGRP, статические маршруты и др. Кроме того, сам PIM не передает информацию о маршрутах, а строит дерево для передачи мультикаст трафика на основе таблицы маршрутизации unicast.
  - В PIM-DM информация об источнике и группе распространяется по

всему домену мультикаст. Выполняется это с помощью процедуры флудинга. Распространение информации об источнике и группе происходит независимо от того, есть ли в данный момент клиенты, которые хотят получать данные этой группы. Так как информация передается всем маршрутизаторам, то каждый маршрутизатор знает о существующих группах и источниках. И следовательно, когда появляется клиент, которых хочет получать трафик определенной группы, любой маршрутизатор в мультикаст домене знает где находится источник, который передает данные этой группы, и строит SPT-дерево к источнику.

- **RIP** — один из самых простых протоколов маршрутизации. Применяется в небольших компьютерных сетях, позволяет маршрутизаторам динамически обновлять маршрутную информацию (направление и дальность в хопх), получая её от соседних маршрутизаторов.



## 4 Выполнение

### 4.1 Конфигурация сети

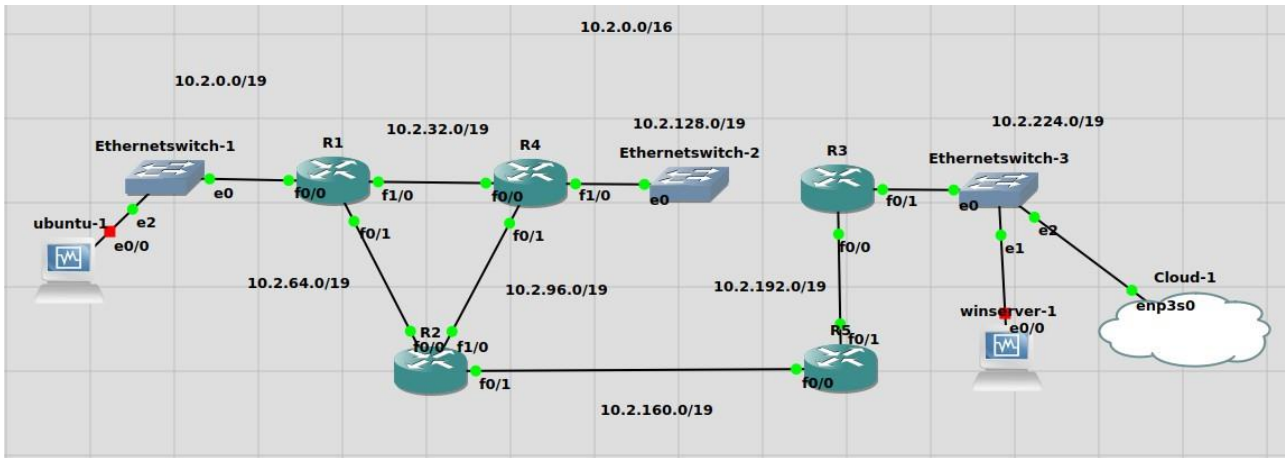


Рисунок 2. Сеть предприятия

На рисунке 2 изображена сконфигурированная сеть. Так как необходимо было разбить сети так, чтобы в сети с определенным коммутатором, было определённое количество рабочих станций, а именно :

- SW1 — 80
- SW2 — 520
- SW3 — 1997

То было принято решение разбить сети 19 маской, в результате в каждой сети возможно 8192 рабочих станций.

### 4.2 Конфигурация рабочей станции

На рабочую станцию пользователя установлена Ubuntu 16.04 LTS. Эта ОС была выбрана благодаря невысоким системным требованиям и стабильной работе.

Для воспроизведения IP TV установлена программа VLC - бесплатный и свободный кроссплатформенный медиаплеер, способный воспроизводить сетевые трансляции (IP TV).

### 4.3 Настройка маршрутизаторов сети

Для настройки маршрутизаторов необходимо присвоить каждому

рабочему интерфейсу `ip` — адрес из соответствующего диапазона. Так же интерфейсы маршрутизаторов, которые выходят в локальные сети рабочих станции, имеют первый номер узла из этой сети.

```
R1#conf t
Enter configuration commands, one per line. End
R1(config)#int f0/0
R1(config-if)#ip add
R1(config-if)#ip address 10.2.0.1 255.255.224.0
R1(config-if)#no sh
R1(config-if)#
```

*Рисунок 3. Пример настройки интерфейса*

Для настройки маршрутизации в сети с помощью протокола динамической маршрутизации `rip`, необходимо выполнить следующие действия для его настройки на каждом маршрутизаторе приведенный на рисунке 4.

```
R1#conf t
Enter configuration commands, one pe
R1(config)#router rip
R1(config-router)#ver 2
R1(config-router)#netw
R1(config-router)#network 10.2.0.0
R1(config-router)#netw
R1(config-router)#network 10.2.32.0
R1(config-router)#network 10.2.64.0
```

*Рисунок 4. Настройка протокола динамической маршрутизации RIP*

На рисунке 5 показана работоспособности сети, `ping` происходит от R1 до R3.

```
R1#ping 10.2.224.1
Type escape sequence to a
Sending 5, 100-byte ICMP
!!!!
```

*Рисунок 4. Ping от R1 до R3*

На рисунке 6 показан пример общения маршрутизаторов по протоколу RIP.

Основные операции протокола RIP являются очень простыми и подчиняются описанным ниже весьма несложным правилам.

1. После загрузки маршрутизатора единственными известными ему маршрутами являются маршруты к сетям, к которым он непосредственно подключен.

2. Согласно протоколу RIP версии 1, маршрутизатор выполняет широковещательную рассылку информации обо всех известных ему сетях во все непосредственно подключенные сети. Применяемые при этом пакеты принято называть обновлениями или анонсами.
3. Маршрутизаторы RIP принимают широковещательные пакеты RIP. Это позволяет им получать от других маршрутизаторов такую информацию о сетях, которую они не могли бы получить самостоятельно.
4. Применяемая в протоколе RIP метрика представляет собой количество транзитных переходов (этот показатель можно неформально определить как количество маршрутизаторов в маршруте) и анонсируется в широковещательных рассылках RIP для каждой сети. Максимально допустимое количество транзитных переходов для RIP равно 15. Метрика 16 считается бесконечно большой.
5. Предполагается, что информация о любом маршруте, полученная от маршрутизатора RIP, касается маршрута, проходящего через этот маршрутизатор. Иными словами, если маршрутизатор А передает обновление маршрутизатору В, то маршрутизатор В предполагает, что в конце следующего транзитного перехода к сетям, включенным в это обновление, находится маршрутизатор А.
6. Обновления рассылаются через регулярные интервалы.

Протокол RIP версии 2 (который в основном определен в документе [RFC 2453](#)) позволяет устранить некоторые ограничения версии 1, но без внесения в сам протокол каких-либо кардинальных изменений. Ниже перечислены некоторые наиболее полезные усовершенствования, введенные в версии 2.

- **Поддержка VLSM.** Вместе с обновлениями RIP 2 передаются маски подсети.
- **Многоадресатные обновления.** Обновления передаются с помощью многоадресатной, а не широковещательной рассылки, поэтому сокращаются непроизводительные затраты процессорного времени в хостах, не участвующих в работе протокола RIP.
- **Поддержка аутентификации.** В маршрутизаторах, совместимых с требованиями RFC 2453, поддерживается аутентификация на основе открытого текста. (А в маршрутизаторах Cisco поддерживается также аутентификация с шифрованием по алгоритму MD5.)

```

▶ Frame 6: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on
▼ Ethernet II, Src: c2:01:27:36:00:01 (c2:01:27:36:00:01), Dst: IPv4mcast
  ▶ Destination: IPv4mcast_09 (01:00:5e:00:00:09)
  ▶ Source: c2:01:27:36:00:01 (c2:01:27:36:00:01)
  Type: IPv4 (0x0800)
▼ Internet Protocol Version 4, Src: 10.2.64.1, Dst: 224.0.0.9
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)
  Total Length: 92
  Identification: 0x0000 (0)
  ▶ Flags: 0x00
  Fragment offset: 0
  ▶ Time to live: 2
  Protocol: UDP (17)
  Header checksum: 0x8dc5 [validation disabled]
  [Header checksum status: Unverified]
  Source: 10.2.64.1
  Destination: 224.0.0.9
  [Source GeoIP: Unknown]
  [Destination GeoIP: Unknown]
▼ User Datagram Protocol, Src Port: 520, Dst Port: 520
  Source Port: 520
  Destination Port: 520
  Length: 72
  Checksum: 0x712c [unverified]
  [Checksum Status: Unverified]
  [Stream index: 0]
▼ Routing Information Protocol
  Command: Response (2)
  Version: RIPv2 (2)
  ▶ IP Address: 10.2.0.0, Metric: 1
  ▶ IP Address: 10.2.32.0, Metric: 1
  ▶ IP Address: 10.2.128.0, Metric: 2

```

*Рисунок 6. Рассылка известных маршрутов*

#### 4.4 Конфигурация сервера

На рабочую станцию, которая работает в качестве DHCP-сервера, установлена ОС Windows Server 2008.

Для работы DHCP-сервера в системе необходимо настроить роль, для этого используется «Мастер настройки сервера» (рис. 8), который установит необходимое ПО для работы. После требуется создать области, для этой цели также имеется «Мастер создания области». В процессе создания надо указать уникальное имя области, описание, диапазон IP-адресов, маску, срок действия аренды адреса, а также можно указать дополнительные параметры:

исключенные IP-адреса, адреса маршрутизатора (шлюз), DNS-сервера и др.

Для предприятия необходимо создать область для каждой подсети (SW1, SW2 и SW3). Для каждой подсети заданы соответствующие диапазоны адресов, маски и шлюзы. Так как запросы к DHCP-серверу и обратно отправляются широковещательно (т.е. дальше своего широковещательного домена запросы не уходят), в каждой из подсетей настроен ретранслятор, который, получив DHCP-запрос, отправляет его серверу (одноадресная рассылка). После обработки сервер отправляет ответ ретранслятору, который пересылает его соответствующему клиенту. При получении сетевых настроек впервые между клиентом и сервером происходит «диалог» из 4-х сообщений.

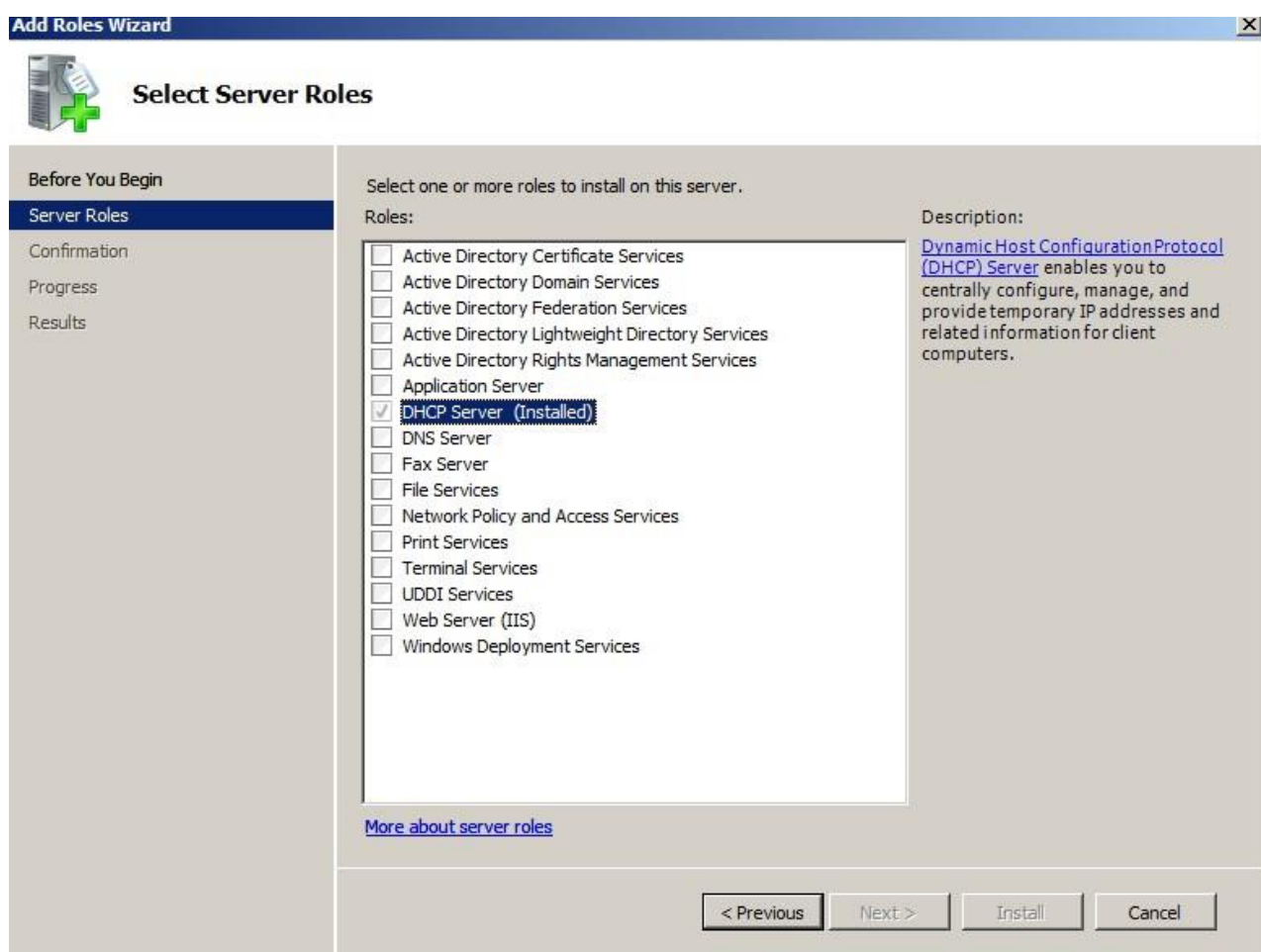


Рисунок 7. Мастер настройки сервера



Рисунок 8. Настройка пула адресов

Scope [10.2.0.0] Pool 0.0	** Active **
Scope [10.2.128.0] Pool 128.0	** Active **
Scope [10.2.224.0] Pool 224.0	** Active **

Рисунок 9. Сконфигурированные пулы

На рисунке 11 показан пример общения DHCP — протокола.

7	25.104962	0.0.0.0	255.255.255.255	DHCP	342 DHCP Request	- Transaction ID 0x98305351
8	25.173703	10.2.0.1	10.2.0.10	DHCP	342 DHCP ACK	- Transaction ID 0x98305351

Рисунок 10. Пример общения DHCP

Также необходимо настроить dhcp-relay на интерфейсах маршрутизаторов, на которые приходят dhcp — запросы командой «*ip helper-address 10.2.224.2*».

## 4.5 Настройка PIM\_DM и IGMP

Для настройка PIM\_DM происходит следующим образом (рис. 11). Также при необходимости необходимо явно указать, что данный интерфейс входит в группу «*ip igmp join-group 224.1.1.1*».

```

R1#conf t
Enter configuration commands, one
R1(config)#ip mu
R1(config)#ip multicast-r
R1(config)#ip multicast-routing
R1(config)#int f0/0
R1(config-if)#ip ig
R1(config-if)#ip pim
R1(config-if)#ip pim de
R1(config-if)#ip pim dense-mode |

```

Рисунок 11. Настройка PIM\_DM

13.463426	10.2.160.1	224.0.0.1	IGMPv2	60 Membership Query, general
15.105366	c2:02:27:45:00:01	CDP/VTP/DTP/PAGP/UD...	CDP	352 Device ID: R2 Port ID: FastEthernet0/1
15.457785	10.2.160.1	224.1.1.1	IGMPv2	60 Membership Report group 224.1.1.1
19.506111	10.2.160.2	224.0.0.13	PIMv2	68 Hello
20.009493	c2:02:27:45:00:01	c2:02:27:45:00:01	LOOP	60 Reply
20.502802	c2:05:27:73:00:00	c2:05:27:73:00:00	LOOP	60 Reply
20.613684	10.2.160.2	224.0.0.9	RIPv2	86 Response
24.309494	10.2.160.2	224.0.1.40	IGMPv2	60 Membership Report group 224.0.1.40

Рисунок 12. Пример PIM\_DM и IGMP

## 4.6 Настройка VLC

Настройка vlc как источника раздачи показана на рисунках 13 — 16

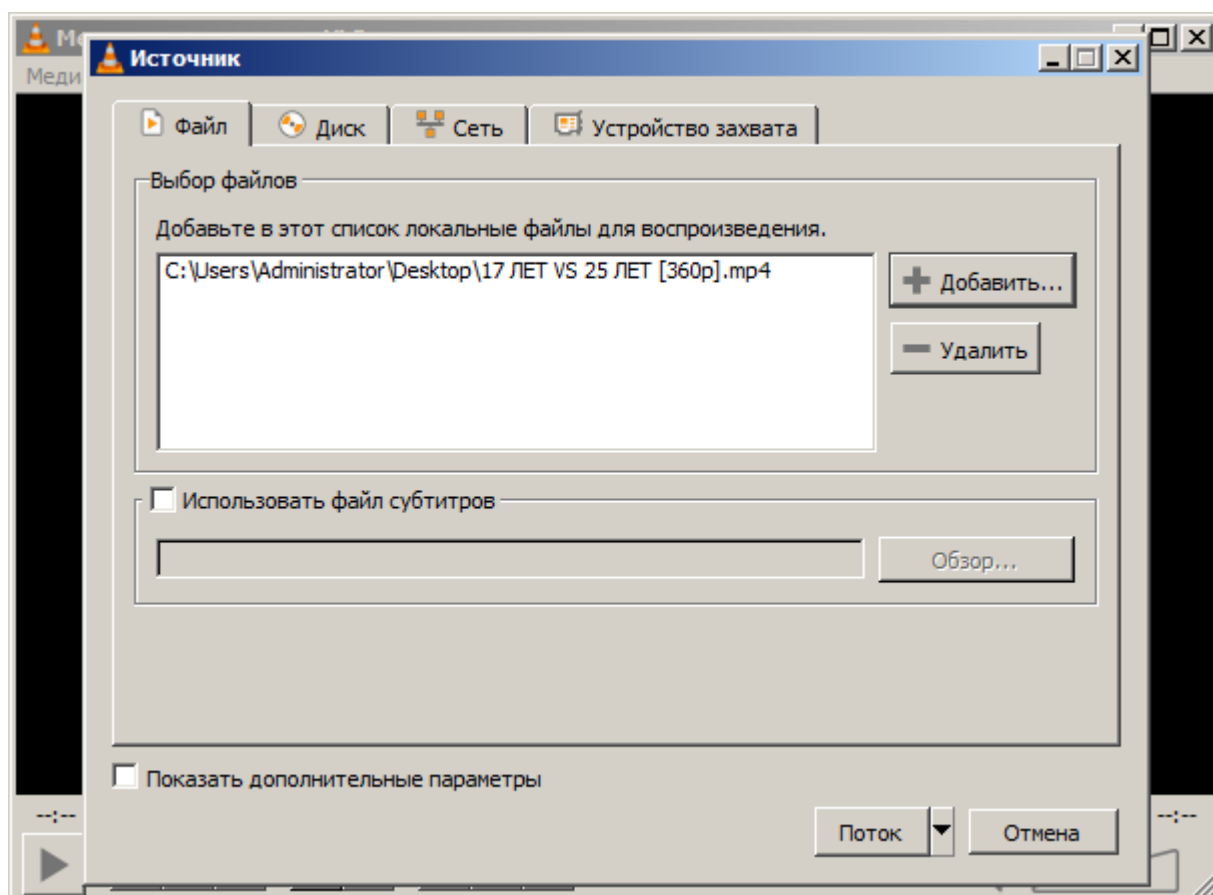


Рисунок 13. Выбор файла для передачи

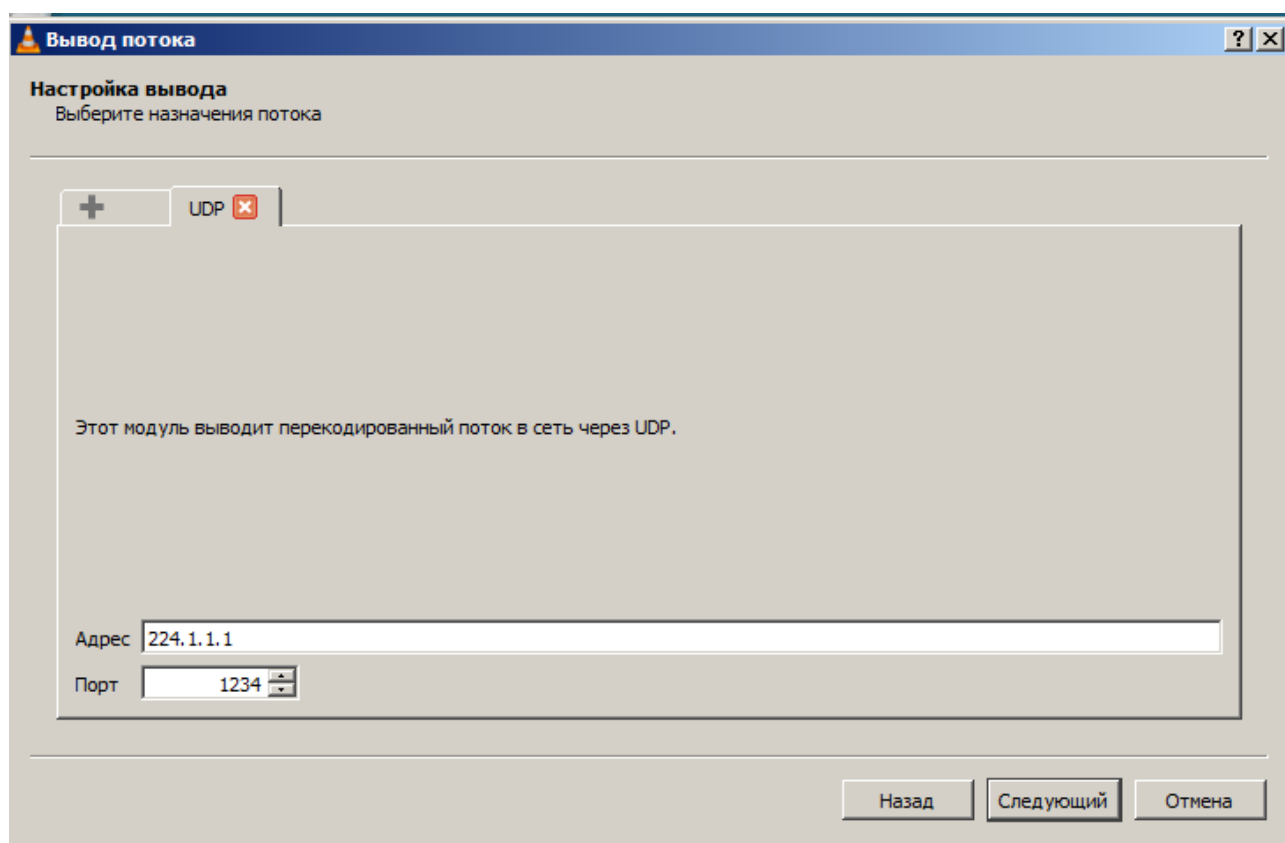


Рисунок 14. Выбор адреса для вещания

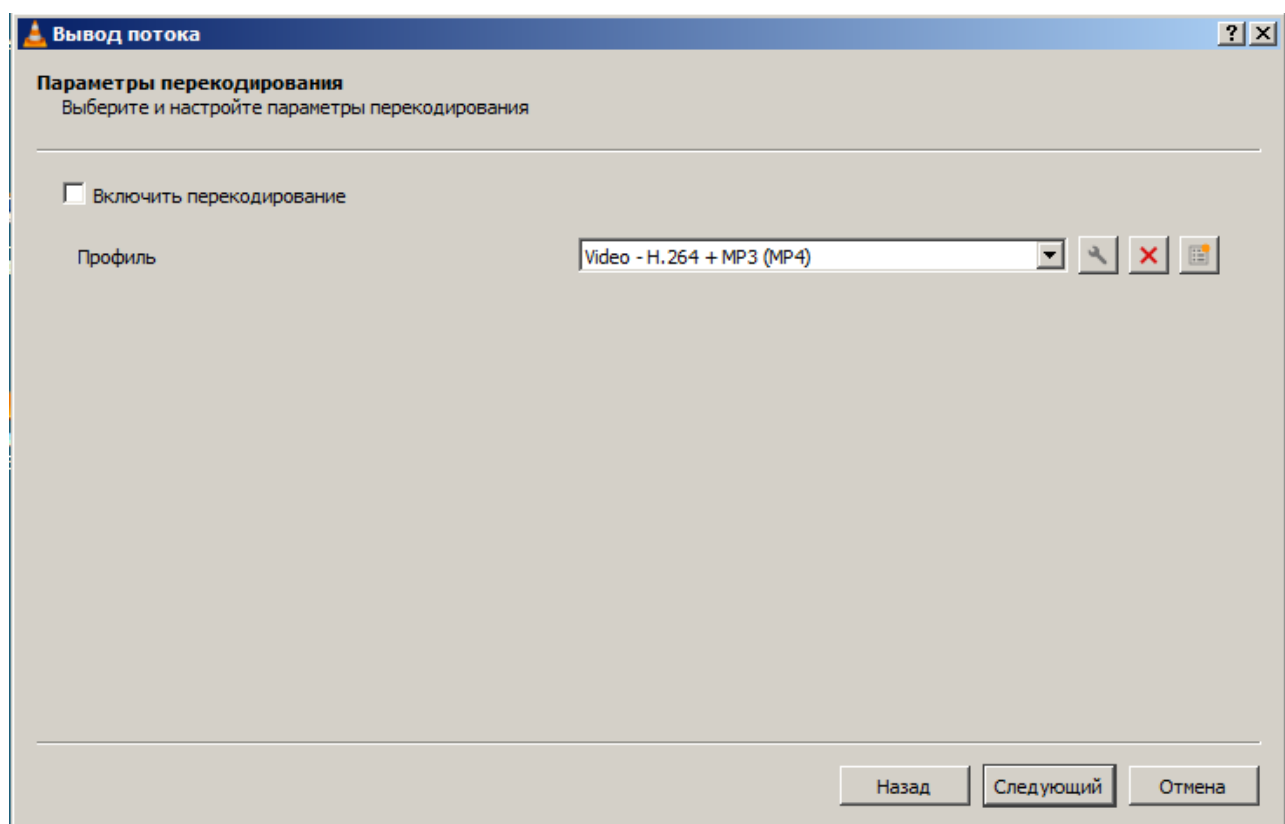


Рисунок 15. Параметры кодирования



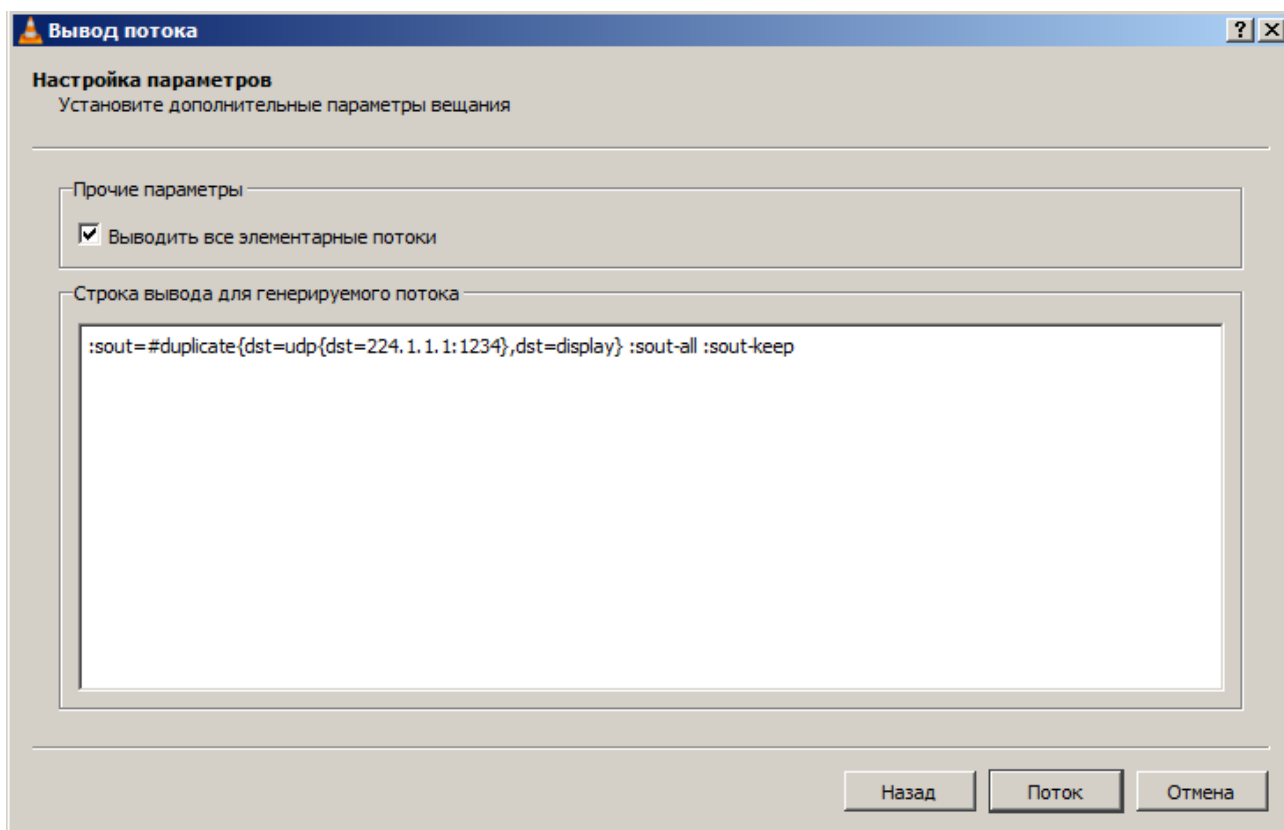


Рисунок 16. Настройки вещания

Настройка VLC как клиента показана на рисунке 17.

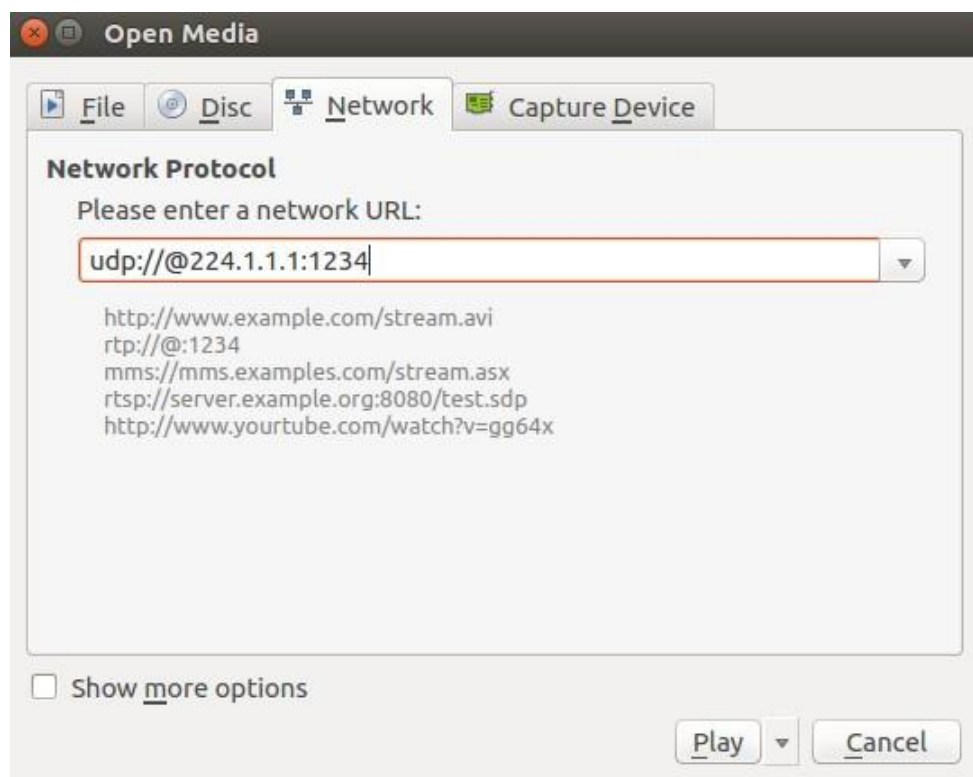


Рисунок 17. Настройка клиента VLC

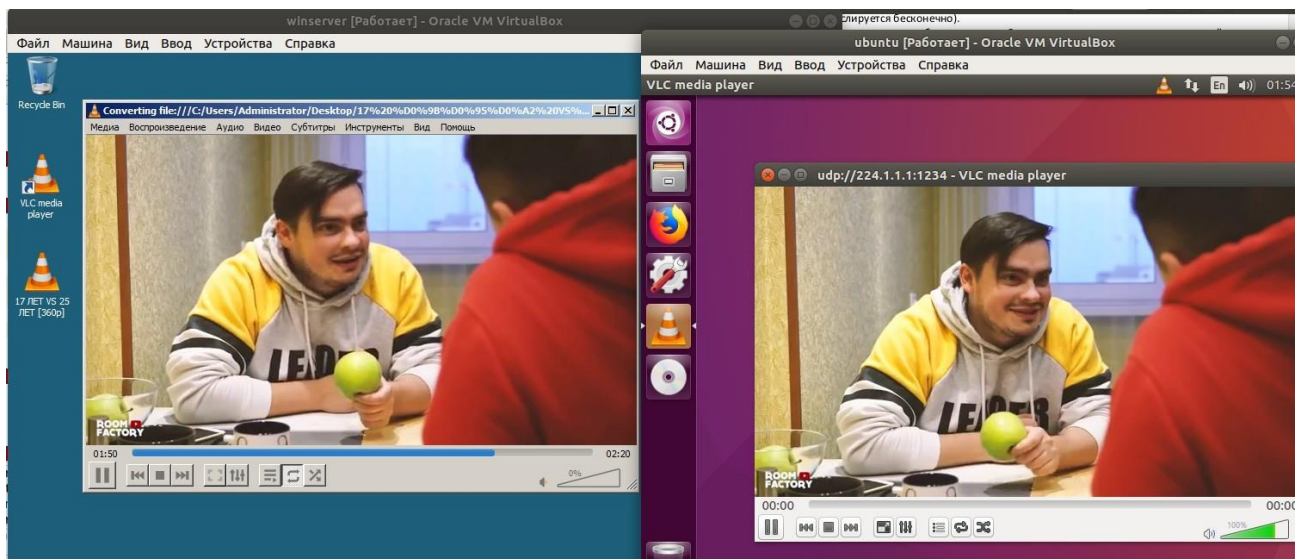


Рисунок 18. Вещание передачи

На рисунке 18 показана передача видео — файла с помощью VLC. Так же стоит заметить, что при необходимости нужно выставить TTL на источнике, необходимый для доставки до клиента.

## **5 Вывод**

В ходе выполнения данной работы мною были получены практические знания по настройке сети, в которой осуществляется многоадресная рассылка видеопотока, по настройке протокола динамической маршрутизации OSPF, по конфигурированию автоматического получения параметров сети с использованием DHCP.