ФЕДЕРАЛЬНОЕ АГЕНТСТВО СВЯЗИ

**Федеральное государственное
бюджетное образовательное учреждение высшего образования
«САНКТ-ПЕТЕРБУРГСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ
им. проф. М. А. БОНЧ-БРУЕВИЧА»**

**А. Б. Гольдштейн, А. В. Никитин,
А. А. Шкрыль, В. В. Фицов**

ТРАНСПОРТНЫЕ СЕТИ IP/MPLS

ТЕХНОЛОГИЯ И ПРОТОКОЛЫ

Лабораторный практикум

*Разработан в рамках договора между ОАО «Ростелеком» и СПбГУТ
на выполнение научно-исследовательских работ
по разработке учебно-методических комплексов с интерактивным обучением
по дисциплинам базовой кафедры «Инновационные технологии телекоммуникаций»
ОАО «Ростелеком» в СПбГУТ*

СПб ГУТ)))

**САНКТ-ПЕТЕРБУРГ
2016**

УДК 621.395(076)
ББК 32.882я73
Т65

Рецензенты:
заведующий кафедрой автоматической электросвязи,
профессор *А. П. Пшеничников* (МТУСИ),
доктор технических наук, профессор *Н. А. Соколов* (ЛО ЦНИИС)

Рекомендовано к печати
редакционно-издательским советом СПбГУТ

Гольдштейн, А. Б.

Т65 Транспортные сети IP/MPLS. Технология и протоколы : лабораторный практикум / А. Б. Гольдштейн, А. В. Никитин, А. А. Шкрыль, В. В. Фицов ; СПбГУТ. – СПб., 2016. – 63 с.

ISBN 978-5-89160-132-1

Написан в соответствии с рабочими программами дисциплин «Транспортные сети NGN» и «Инфокоммуникационные протоколы». Приведены методические рекомендации по выполнению лабораторных работ.

Предназначен для студентов, обучающихся по направлениям подготовки 11.03.02 «Инфокоммуникационные технологии и системы связи», 09.03.01 «Информатика и вычислительная техника».

УДК 621.395(076)
ББК 32.882я73

ISBN 978-5-89160-132-1

Предисловие

Инфокоммуникационные технологии проникли в нашу жизнь настолько глубоко, что мыслить дальнейшее развитие человечества вне контекста средств и технологий связи просто невозможно.

Национальная телекоммуникационная компания ПАО «Ростелеком» является не только ключевым игроком отечественной отрасли связи, но и образцом внедрения инновационных решений. Обеспечение бесперебойной работы крупнейших по своей протяженности сетей связи, расположившихся от Крайнего Севера до Ирана, от Лондона до Токио, является сложнейшей задачей, лежащей на наших сотрудниках. Подготовка специалистов, способных не только поддержать существующие процессы и досконально изучить используемые технологии, но и найти силы для поиска новых революционных решений – вот это и есть высшая цель, стоящая перед создателями актуального методического пособия.

Объединяя лучшее от практики и теории, авторы постарались максимально компактно и ярко изложить механизмы, протоколы и требования современных сетей IP/MPLS.

Руководство ПАО «Ростелеком» выражает признательность всему коллективу авторов за проведенную работу и желает всем слушателям укрепить свои знания и достойно встретить все вызовы профессиональной карьеры.

Вице-президент – Директор макрорегионального
филиала «Северо-Запад» ПАО «Ростелеком»
А. В. Балаценко

Лабораторная работа 1
ОЗНАКОМЛЕНИЕ С ТЕХНОЛОГИЕЙ MPLS

Цель лабораторной работы заключается в изучении пакетов с меткой MPLS, проверке передаваемого через зону коммутации MPLS трафика, а также процесса фрагментации в сетях IP/MPLS.

В результате выполнения лабораторной работы студент получит навык работы с программой Wireshark для перехвата и анализа пакетов MPLS, а также навык анализа топологии MPLS сети путем проверки настройки их сетевых интерфейсов.

Выполнение лабораторной работы

1. Запустить ярлык «Удаленная консоль». В открывшемся окне выбрать зону MPLS. Затем выбрать тот терминал-отправитель (Cm), рис. 1.1, с которого будет отправляться команда ***ping*** согласно варианту задания, указанному в табл. 1.1.

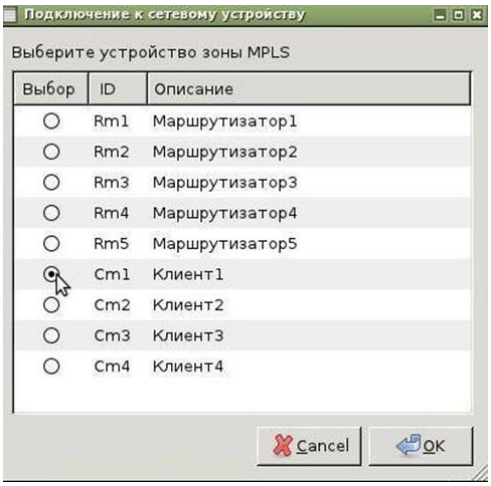


Рис. 1.1. Подключение к сетевому устройству

2. В открывшемся окне, как показано на рис. 1.2, ввести команду:

ping IP-адрес терминала-получателя

(где адрес терминала-получателя указан в табл. 1.1).

Рис. 1.2. Ввод команды ping

Таблица 1.1

Варианты заданий

Параметр	Номер варианта задания											
	1	2	3	4	5	6	7	8	9	10	11	12
Отправитель → получатель	Cm1 → Cm3	Cm3 → Cm1	Cm2 → Cm4	Cm4 → Cm2	Cm3 → Cm5	Cm5 → Cm3	Cm3 → Cm6	Cm6 → Cm3	Cm5 → Cm2	Cm2 → Cm5	Cm6 → Cm1	Cm1 → Cm6
Граничный маршрутизатор	Rm1	Rm3	Rm2	Rm4	Rm3	Rm5	Rm3	Rm6	Rm5	Rm2	Rm6	Rm1
Терминал-отправитель	Cm1	Cm3	Cm2	Cm4	Cm3	Cm5	Cm3	Cm6	Cm5	Cm2	Cm6	Cm1
Терминал-получатель	10.0.13.13	10.0.11.11	10.0.14.14	10.0.12.12	10.0.15.15	10.0.13.13	10.0.16.16	10.0.13.13	10.0.12.12	10.0.15.15	10.0.11.11	10.0.16.16
Интерфейс в сторону терминала	eth2	eth2	eth3	eth3	eth2	eth4	eth2	eth1	eth4	eth3	eth1	eth2
Интерфейс к транзитному маршрутизатору	eth1	eth1	eth2	Eth2	eth3	eth2	eth3	eth2	eth1	eth1	eth3	eth3
Транзитный маршрутизатор	Rm2	Rm2	Rm3	Rm3	Rm4	Rm4	Rm4	Rm4	Rm1	Rm1	Rm5	Rm5
Интерфейс на выходе транзитного маршрутизатора	eth2	eth1	eth3	eth1	eth1	eth2	eth4	eth2	eth1	eth3	eth1	eth3

3. Запустить программу «WireShark на сервере», используя ярлык на рабочем столе.

В открывшемся окне выбрать зону MPLS. Далее выбрать граничный маршрутизатор, рис. 1.3 (номер маршрутизатора (Rm) указан в табл. 1.1), с которого будет осуществляться снятие трассировки (отлов пакетов).

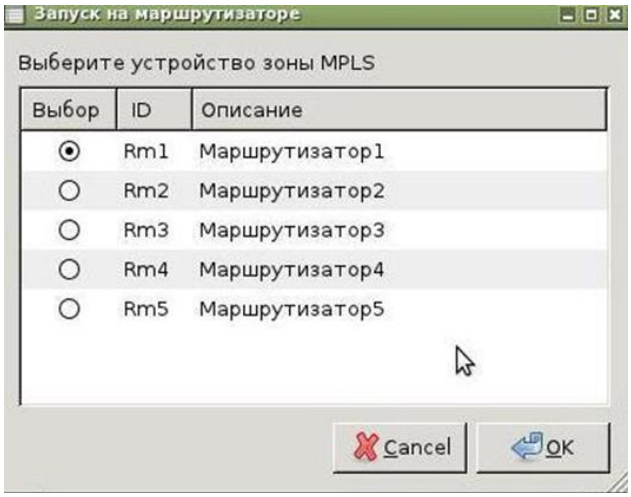


Рис. 1.3. Выбор граничного маршрутизатора

4. Выбрать интерфейс в сторону терминала (eth1-4), рис. 1.4, генерирующего запросы ping (в соответствии с вариантом задания, указанным в табл. 1.1). Убедиться, что в запросах и ответах отсутствуют метки MPLS. Для этого применить фильтр mpls и проверить то, что пакетов, использующих данную технологию, не обнаружено. Далее необходимо выбрать пакет, относящийся к запросу или ответу ping (используя фильтр icmp), и в нижней части окна посмотреть, какие технологии и протоколы применяются для его передачи.

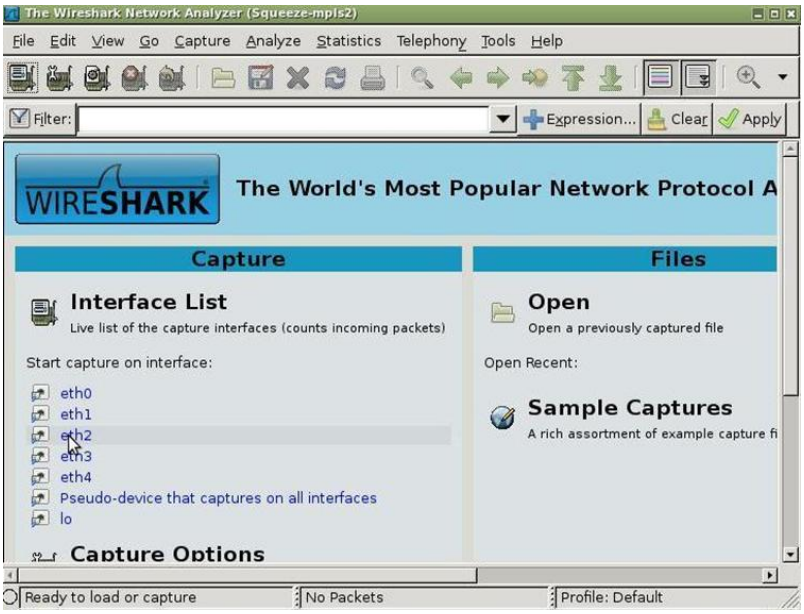


Рис. 1.4. Окно программы «WireShark на сервере»

5. Далее в программе «WireShark на сервере» необходимо выбрать интерфейс граничного маршрутизатора, ведущий к транзитному маршрутизатору. Для этого в выпадающем меню выбрать зону mpls, далее – граничный маршрутизатор в соответствии с вариантом в табл. 1.1. В запущенной программе в строке меню нажать ***Capture***, затем выбрать пункт ***Interfaces***. В открывшемся окне, показанном на рис. 1.5, указаны IP-адреса, которые соответствуют интерфейсам на маршрутизаторе и позволяют просмотреть маршрут. В правом верхнем углу нажать ***Stop***, выбрать интерфейс к транзитному маршрутизатору (согласно варианту, указанному в табл. 1), нажать ***Start***.

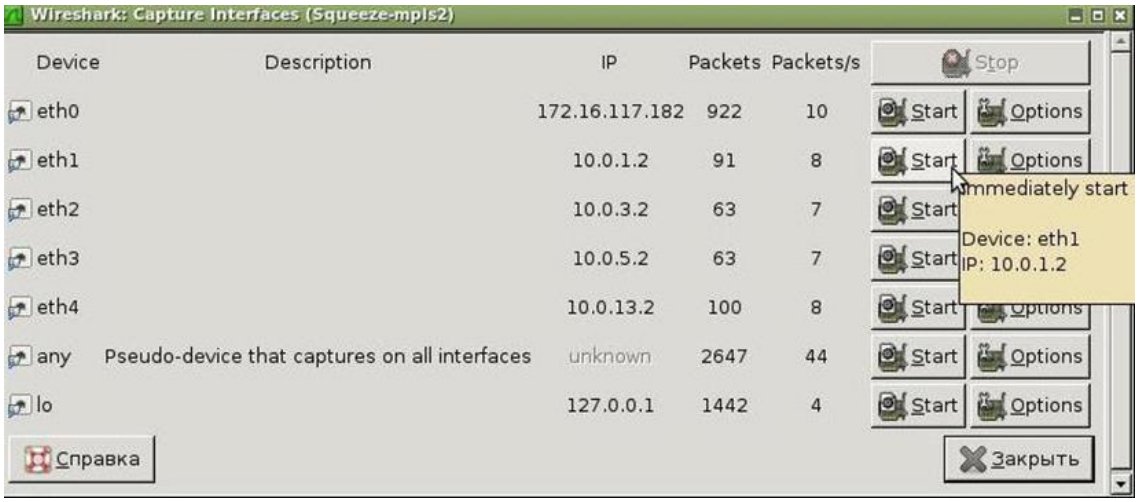


Рис. 1.5. Выбор интерфейса к транзитному маршрутизатору

6. Для поиска пересылаемых пакетов можно использовать фильтр, для этого в поле ***Filter*** ввести ***mpls*** и нажать ***Apply*** (рис. 1.6).

Найти отправляемые и получаемые пакеты (соответствующие IP-адресам клиентов отправителя и получателя), изучить их структуру.

В отчет следует выписать отличия между пакетами запросов и ответов, указать IP-адреса, поля технологии MPLS и их значения, также выписать выводы о использовании стека меток, приоритетного обслуживания и времени жизни.

7. Закрыть программу «WireShark на сервере».

8. Запустить снова программу «WireShark на сервере», выбрать зону MPLS, затем выбрать маршрутизатор, являющийся транзитным на пути следования пакета.

Выбрать интерфейс на выходе транзитного маршрутизатора, соответствующий варианту задания, указанному в табл. 1.1. Поставить в поле фильта ***mpls***. Выписать в отчет значения полей заголовка MPLS, сравнить с предыдущими и написать выводы о использовании меток и времени жизни.

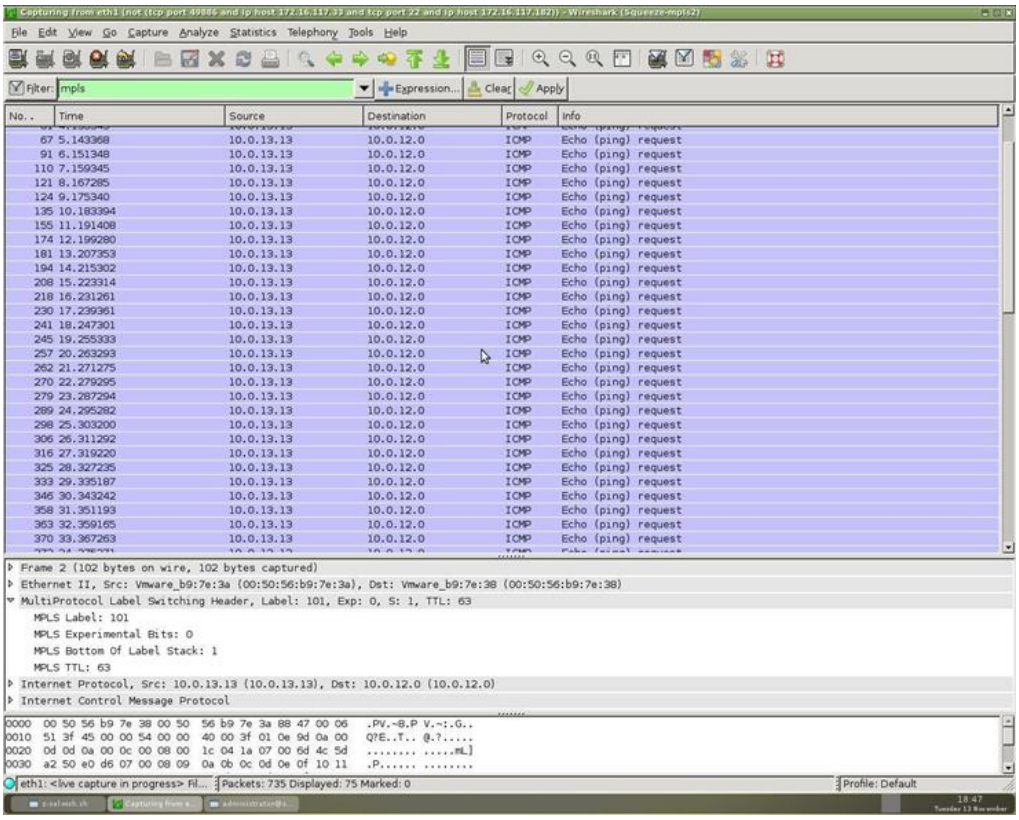


Рис. 1.6. Окно программы «WireShark». Фильтрация пакетов mpls.

9. В «Удаленной консоли» остановить выполнение команды «ping» сочетанием клавиш Ctrl + C.

10. В «Удаленной консоли» ввести команду:

ping IP-адрес терминала-получателя **-s 2000 -c 1**

Здесь параметр **«-s 2000»** устанавливает размер отправляемого пакета равным 2000, а «**-c 1**» устанавливает количество пакетов, равное 1. В результате будет отправлен запрос с превышением MTU (Maximum Transmission Unit – максимальный блок данных для канала), так как на маршрутизаторе установлен MTU, равный 1496.

11. В программе «WireShark на сервере» посмотреть переданные пакеты.

Из пакетов «request» или «reply» выписать в отчет значения параметров «identifier», а также количество фрагментов, на которые разбился пакет и их размер. На основании полученных данных посчитать суммарный размер пакета.

12. Закрыть программы «Удаленная консоль» и «WireShark на сервере».

Лабораторная работа 2
СОСТАВЛЕНИЕ ТАБЛИЦ КОММУТАЦИИ ПО МЕТКАМ

Цель лабораторной работы заключается в изучении принципа работы маршрутизаторов MPLS по таблицам коммутации меток.

В результате лабораторной работы студент получит навык назначения, анализа и переназначения меток на граничном и транзитном маршрутизаторах MPLS.

Таблица 2.1

Варианты заданий*

Вариант	Путь	Метка	Интерфейс на граничном маршрутизаторе	IP-адрес транзитного маршрутизатора	Граничный маршрутизатор	Транзитный маршрутизатор	IP-адрес терминала-получателя
1	1 → 3	100	eth1	10.0.1.2	1	2	10.0.13.13
2	3 → 1	100	eth1	10.0.3.2	3	2	10.0.11.11
3	2 → 4	200	eth2	10.0.3.3	2	3	10.0.14.14
4	4 → 2	200	eth2	10.0.4.3	4	3	10.0.12.12
5	3 → 6	300	eth3	10.0.4.4	3	4	10.0.16.16
6	6 → 3	300	eth2	10.0.5.4	6	4	10.0.13.13
7	1 → 4	400	eth3	10.0.2.5	1	5	10.0.14.14
8	4 → 1	400	eth1	10.0.6.5	4	5	10.0.11.11
9	1 → 6	500	eth3	10.0.2.5	1	5	10.0.16.16
10	6 → 1	500	eth3	10.0.7.5	6	5	10.0.11.11

*Если количество бригад нечетное, то последней бригаде необходимо выполнить пункты 1–10 для следующего варианта.

Выполнение лабораторной работы

1. Открыть ярлык «Удаленная консоль», расположенный на рабочем столе.

В открывшемся окне выбрать зону ***MPLS*** и граничный маршрутизатор, соответствующий варианту задания из табл. 2.1.

2. Установить новую входящую метку. Для этого введем команду:

sudo mpls ilm add label gen XXX labelspace 0,

Здесь XXX – новая метка.

Чтобы убедиться, что новая метка добавлена, будем использовать команду для просмотра входящих меток (рис. 2.1):

sudo mpls ilm

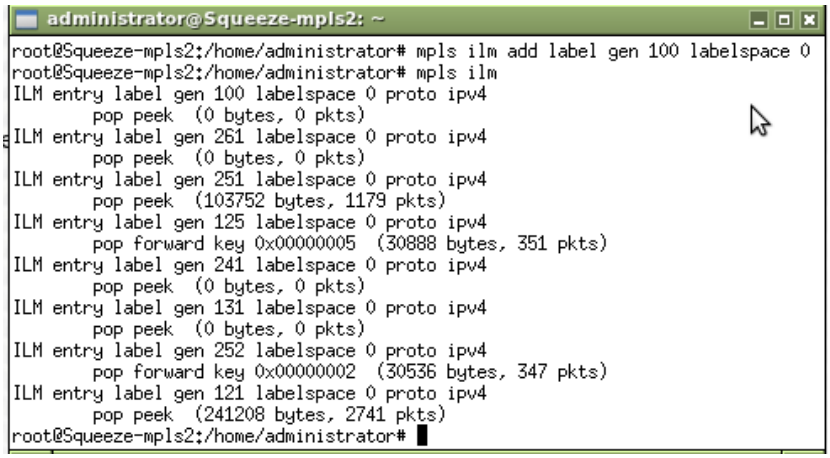


Рис. 2.1. Вывод команд установления новой метки
и ее просмотра

(Удалить *неверно введенную* метку можно командой: *mpls ilm del label gen XXX labelspace 0*.)

3. Установить новую исходящую метку до следующего маршрутизатора. Для этого введем команду:

sudo mpls nhlfe add key 0 instructions push gen XXX nexthop ethY ipv4 10.0.N.M

Здесь **XXX** – новая метка; **ethY** – интерфейс на граничном маршрутизаторе; **10.0.N.M** – IP-адрес транзитного маршрутизатора, все данные берутся из табл. 2.2.

Результат добавления новой метки появится на экране (рис. 2.2). Сформированный ключ имеет размер 4 байта и выводится в шестнадцатеричном виде (hex) 0xQQYYXXZZ, его необходимо записать в виде ***0xZZ.***

Для просмотра установленных меток используется команда:

sudo mpls nhlfe

(Удалить *ключ неверно введенной* метки можно командой: *mpls nhlfe del key 0xZZ instructions push gen XXX*).

4. Далее удалить существующий путь до терминала и добавить новый с использованием технологии MPLS. Для этого воспользоваться следующими командами с параметрами из табл. 2.2:

sudo ip route del 10.0.L.0/24

(где **10.0.L.0/24** – IP-адрес сети терминала-получателя);

sudo ip route add 10.0.L.0/24 via 10.0.N.M dev ethY mpls 0xZZ

(где **10.0.L.0/24** – IP-адрес сети терминала-получателя; **10.0.N.M** – IP-адрес транзитного маршрутизатора; **ethY** – интерфейс на граничном маршрутизаторе; **0xZZ** – ключ исходящей метки, полученный в предыдущем пункте).

Таблица 2.2

Пространство меток интерфейса

Вариант	Путь	Метка	Транзитный маршрутизатор	IP-адрес терминала-получателя	Пространство меток (labelspace)	Интерфейс для входящей метки	Интерфейс до следующего маршрутизатора	IP-адрес до следующего маршрутизатора
1	1 → 3	100	2	10.0.13.13	1	eth1	eth2	10.0.3.3
2	3 → 1	100	2	10.0.11.11	2	eth2	eth1	10.0.1.1
3	2 → 4	200	3	10.0.14.14	1	eth1	eth3	10.0.4.4
4	4 → 2	200	3	10.0.12.12	2	eth3	eth1	10.0.3.2
5	3 → 6	300	4	10.0.16.16	1	eth2	eth4	10.0.5.6
6	6 → 3	300	4	10.0.13.13	2	eth4	eth2	10.0.4.3
7	1 → 4	400	5	10.0.14.14	1	eth1	eth2	10.0.6.4
8	4 → 1	400	5	10.0.11.11	2	eth2	eth1	10.0.2.1
9	1 → 6	500	5	10.0.16.16	1	eth1	eth3	10.0.7.6
10	6 → 1	500	5	10.0.11.11	2	eth3	eth1	10.0.2.1

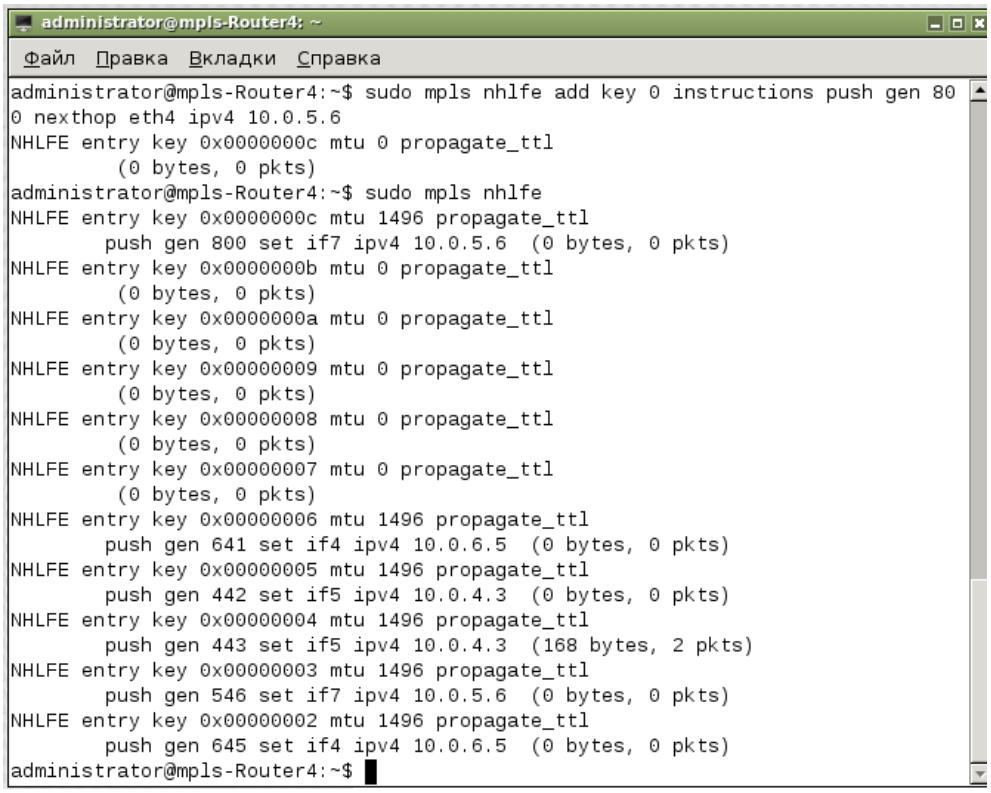


Рис. 2.2. Просмотр установленных меток

5. Закрыть и открыть «Удаленную консоль». В открывшемся окне выбрать зону MPLS и номер транзитного маршрутизатора, соответствующий варианту задания, указанному в табл. 2.2.

6. В данной части лабораторной работы на всех участках пути устанавливаются одинаковые метки, в связи с этим возможна ситуация, когда на маршрутизатор будут приходить одинаковые метки с разных интерфейсов, и будет невозможно определить дальнейшее направление для пересылки. Чтобы этого избежать, необходимо определить принадлежность интерфейса к пространству меток и указать какие метки в него входят.

Далее добавить в пространство меток ***K*** входящую метку **XXX**. Воспользуемся командой:

```
sudo mpls ilm add label gen XXX labelspace K
```

(где XXX – новая метка; ***labelspace K*** – пространство меток, соответствующее варианту задания).

Для контроля использовать команду для просмотра установленных входящих меток, которая использовалась ранее (п. 2):

```
sudo mpls ilm
```

7. Определить, что интерфейс **ethY** принадлежит к пространству меток ***K***. Ввести следующую команду:

```
sudo mpls labelspace set dev ethY labelspace K
```

(где ethY – интерфейс для входящей метки; ***labelspace K*** – пространство меток, соответствующее варианту задания).

8. Установить новую исходящую метку до следующего маршрутизатора, которая будет использоваться при пересылке пакетов. Введем команду (рис. 2.3):

```
sudo mpls nhlfe add key 0 instructions push gen XXX nexthop ethY ipv4 10.0.N.M
```

(где ***XXX*** – новая метка; ***ethY*** – интерфейс до следующего маршрутизатора; ***10.0.N.M*** – IP-адрес следующего маршрутизатора для пересылки, соответствующие вариантам задания).

Сформированный ключ необходимо записать в виде ***0xQQ***.

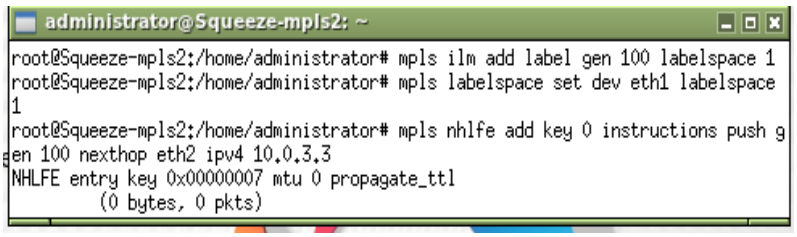


Рис. 2.3. Вывод команды mpls nhlfe add key

9. При использовании технологии MPLS решение о дальнейшей пересылке пакета осуществляется на основании входящей метки и интерфейса, поэтому для транзитных соединений необходимо ассоциировать входящую метку и исходящую. Воспользуемся командой:

sudo mpls xc add ilm_label gen XXX ilm_labelspace K nhlfe_key 0xQQ

(где ***XXX*** – новая метка, соответствующая вашему варианту; ***labelspace K*** – пространство меток, соответствующее варианту задания; ***0xQQ*** – ключ метки, полученный в предыдущем пункте).

Для проверки будем использовать команду просмотра пересылок меток (рис. 2.4):

sudo mpls xc

(Удалить *неверно введенную* метку можно командой: *mpls xc del ilm_label gen XXX ilm_labelspace 0*.)

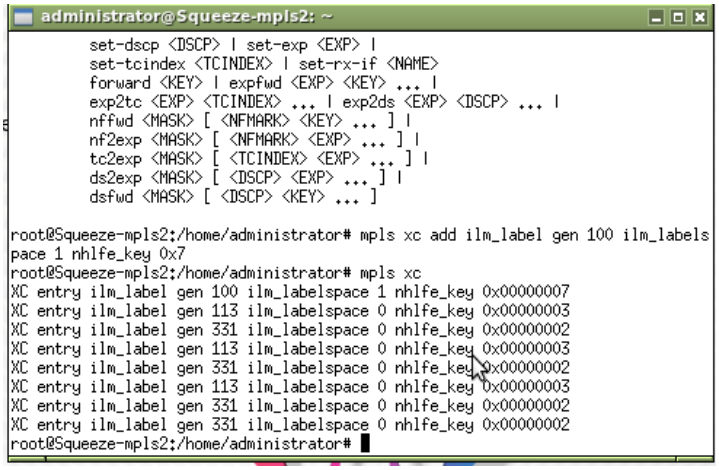


Рис. 2.4. Команда просмотра пересылок меток

10. Удалить существующий путь до клиента и добавить новый с использованием технологии MPLS, с помощью команд:

sudo ip route del 10.0.L.0/24

(где ***10.0.L.0/24*** – IP-адрес сети терминала-получателя);

sudo ip route add 10.0.L.0/24 via 10.0.N.M dev ethY mpls 0xQQ

(где ***10.0.L.0/24*** – IP-адрес сети терминала-получателя; ***10.0.N.M*** – IP-адрес следующего маршрутизатора для пересылки; ***ethY*** – используемый для пересылки интерфейс до следующего маршрутизатора; ***0xQQ*** – ключ исходящей метки, полученный в предыдущем пункте).

11. Закрыть и запустить заново «Удаленную консоль» на рабочем столе, выбрать терминал (соответствует первой цифре в столбце «Путь», табл. 2.3).

Запустить команду:

ping 10.0.N.M

(где ***10.0.N.M*** – IP-адрес терминала-получателя).

12. После того как обе бригады закончат установление меток на всем маршруте, необходимо проверить их в программе «WireShark». Для этого нужно запустить программу «WireShark на сервере», используя ярлык на рабочем столе.

Выбрать зону MPLS и граничный маршрутизатор, с которого будет осуществляться снятие трассировки (отлов пакетов). Затем выбрать интерфейс, участвующий в соединении (берется из табл. 2.1). В программе «WireShark» установить значение фильтра ***mpls.***

Посмотреть структуру пакетов и значение установленной метки.

13. Повторить п. 12 для транзитного маршрутизатора.

14. Закрыть программу «WireShark на сервере».

В «Удаленной консоли» остановить команду ***ping*** сочетанием клавиш ***Ctrl + C.***

Лабораторная работа 3
МЕТОД ТУННЕЛИРОВАНИЯ В СЕТИ MPLS

Цель лабораторной работы заключается в изучении стека меток и принципов действия MPLS-туннелей.

В результате лабораторной работы студент получит навык создания MPLS-туннелей с использованием стека меток.

Таблица 3.1

Варианты заданий

Вари-анты	Путь	Внешняя метка в стеке	Внутренняя метка в стеке	Граничный маршрути-затор (1)/ Интерфейс	Транзитный маршрутизатор (2)/ IP-адрес/ Интерфейс	Граничный маршрути затор (3)/ IP-адрес	Метка (до гранич-ного мар-шрутизатора (3)	IP-адрес терминала-получателя/ IP-адрес сети
1	1-2-3	110	100	1 /eth1	2 /10.0.1.2 /eth2	3 /10.0.3.3	122	10.0.13.13 /10.0.13.0
2	3-2-1	160	150	3 /eth1	2 /10.0.3.2 /eth1	1 /10.0.1.1	177	10.0.11.11 /10.0.11.0
3	3-4-5	210	200	3 /eth3	4 /10.0.4.4 /eth1	5 /10.0.6.5	222	10.0.15.15 /10.0.15.0
4	5-4-3	260	250	5 /eth2	4 /10.0.6.4 /eth2	3 /10.0.4.3	277	10.0.13.13 /10.0.13.0
5	1-5-6	310	300	1 /eth3	5 /10.0.2.5 /eth3	6 /10.0.7.6	322	10.0.16.16 /10.0.16.0
6	6-5-1	360	350	6 /eth3	5 /10.0.7.5 /eth1	1 /10.0.2.1	377	10.0.11.11 /10.0.11.0
7	2-3-4	410	400	2 /eth2	3 /10.0.3.3 /eth3	4 /10.0.4.4	422	10.0.14.14 /10.0.14.0
8	4-3-2	460	450	4 /eth2	3 /10.0.4.3 /eth1	2 /10.0.3.2	477	10.0.12.12 /10.0.12.0
9	2-1-6	510	500	2 /eth1	1 /10.0.1.2 /eth3	6 /10.0.2.6	522	10.0.16.16 /10.0.16.0
10	6-1-2	560	550	6 /eth4	1 /10.0.2.1 /eth1	2 /10.0.1.2	577	10.0.12.12 /10.0.12.0

Выполнение лабораторной работы

1. Для удаленного подключения к необходимому оборудованию нужно открыть ярлык «Удаленная консоль», расположенный на рабочем столе, и в открывшемся окне выбрать зону **MPLS**, тип и номер устройства, соответствующий варианту задания из табл. 3.1. Далее в работе данная процедура будет называться подключением к оборудованию.

Внимание! *В процессе выполнения лабораторной работы размер окна «Удаленная консоль» изменять нельзя, так как полноэкранный режим (или измененный размер окна) не позволяет вводить двухстрочные команды.*

Внимание! *В начале всех команд надо писать* ***sudo****.*

2. Для добавления меток на граничном маршрутизаторе (1) нужно к нему подключиться, в соответствии с вариантом в табл. 3.1, как показано на рис. 3.1.

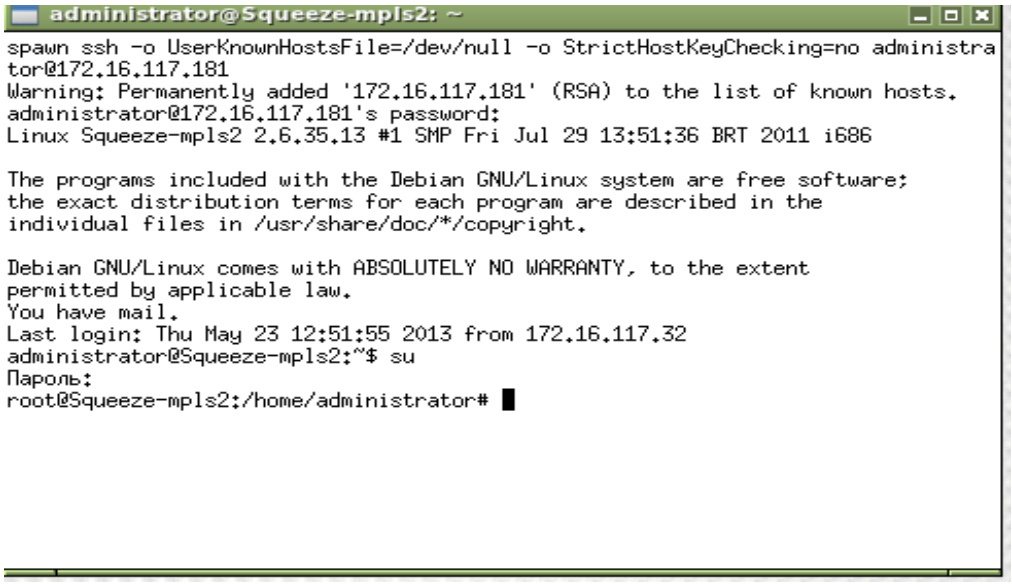


Рис. 3.1. Подключение к сетевому устройству

Чтобы закрепить интерфейс ***ethY*** за пространством меток **0**, нужно ввести команду:

```
sudo mpls labelspace set dev ethY labelspace 0
```

(где **ethY –** интерфейс на граничном маршрутизаторе; **labelspace 0** – пространство меток 0).

Для просмотра информации о пространствах меток используется команда:

```
sudo mpls labelspace
```

Вывод команды показан на рис. 3.2.

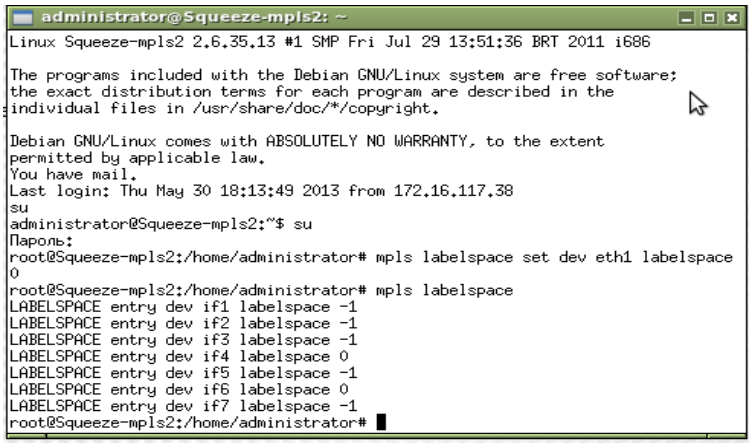


Рис. 3.2. Просмотр пространства меток

3. Далее следует установить новую исходящую метку (именно она будет использоваться для маршрутизации) до следующего маршрутизатора (2), табл. 3.1, командой:

sudo mpls nhlfe add key 0 instructions push gen XXX nexthop ethY ipv4 10.0.N.M

(где **XXX** – новая исходящая метка (*внешняя* метка в стеке) согласно табл. 3.1; **ethY** – интерфейс на граничном маршрутизаторе (1) в сторону транзитного маршрутизатора (2), который указан в табл. 3.1 в соответствии с вариантом; **10.0.N.M** – IP-адрес транзитного маршрутизатора (2) согласно варианту задания в табл. 3.1; **key 0** – параметр, который задается равным 0 для создания нового ключа исходящей метки).

Результат добавления новой метки появится на экране, как показано на рис. 3.3. Сформированный ключ будет выведен на экран в форме 0x0000000Z, его необходимо записать в отчет, для удобства представив в виде 0xZ.

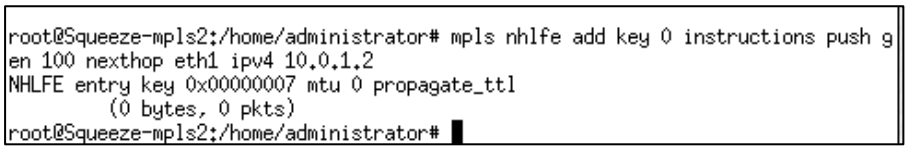


Рис. 3.3. Установление новой исходящей метки

Посмотрите установленные метки и проверьте добавление новой метки командой:

sudo mpls nhlfe

(Удалить *ключ неверно введенной* метки можно командой: *mpls nhlfe del key 0xZ instructions push gen XXX*.)

4. Для добавления в стек еще одной метки внутрь предыдущей метки нужно ввести команду:

sudo mpls nhlfe add key 0 instructions push gen BBB forward 0xZ

(где **0xZ** – ключ, полученный в п. 3; **BBB** – новая исходящая метка (*внутренняя* метка в стеке) согласно табл. 3.1; **key 0** – параметр, который задается равным 0 для создания нового ключа исходящей метки).

Результат добавления новой метки появится на экране аналогично п. 3, как это было показано на рис. 3.3. Сформированный ключ будет выведен на экран в форме 0x0000000Q, его необходимо записать в отчет, для удобства представив в виде 0xQ.

5. Далее следует удалить стандартный маршрут до сети, в которой находится терминал-получатель, командой:

sudo ip route del 10.0.L.0/24

(где **10.0.L.0** – IP-адрес сети терминала получателя; **/24** – указание маски подсети (единая для всех вариантов)).

Затем добавить новый маршрут до сети терминала-получателя с использованием технологии MPLS командой:

sudo ip route add 10.0.L.0/24 via 10.0.N.M dev ethY mpls 0xQ,

(где **10.0.L.0/24** – IP-адрес сети терминала-получателя; **10.0.N.M** – IP-адрес транзитного маршрутизатора (2) по табл. 3.1; **ethY** – интерфейс граничного маршрутизатора (1), используемый для пересылки до следующего маршрутизатора, согласно табл. 3.1; **0xQ** – полученный в п. 4 ключ исходящей метки).

Чтобы убедиться в добавлении нового пути до сети терминала-получателя, нужно ввести команду:

sudo ip route

Вывод команды показан на рис. 3.4.

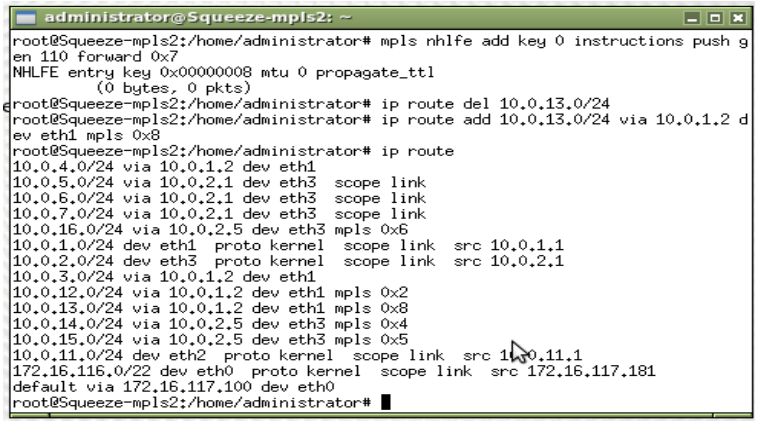


Рис. 3.4. Просмотр пути до сети терминала-получателя

6. Чтобы задать новую входящую метку на транзитном маршрутизаторе (2), следует к нему подключиться в соответствии с вариантом в табл. 3.1 и ввести команду:

sudo mpls ilm add label gen CCC labelspace 0

(где **CCC** – метка, внешняя в стеке, установленная на граничном маршрутизаторе (1), которая согласно варианту также указана в табл. 3.1).

(Удалить *неверно введенную* метку можно командой: *mpls ilm del label gen CCC labelspace 0.*)

7. Далее следует закрепить интерфейс **ethX** за пространством меток **0**, введя команду:

sudo mpls labelspace set dev ethX labelspace 0

(где **ethX** – интерфейс транзитного маршрутизатора (2) в сторону граничного маршрутизатора (3), табл. 3.1).

8. Чтобы установить новую исходящую метку (она станет новой внешней меткой) до следующего граничного маршрутизатора (3), табл. 3.1, нужно ввести команду:

sudo mpls nhlfe add key 0 instructions push gen DDD nexthop ethX ipv4 10.0.J.K

(где **DDD** – новая метка до следующего граничного маршрутизатора (3), табл. 3.1; **ethX** – интерфейс на транзитном маршрутизаторе (2) в сторону следующего граничного маршрутизатора (3); **10.0.J.K** – IP-адрес следующего граничного маршрутизатора (3); **key 0** – параметр, который задается равным 0, для создания нового ключа исходящей метки).

Результат добавления новой метки появится на экране. Сформированный ключ будет выведен на экран в форме 0x0000000P, его необходимо записать в отчет, для удобства представив в виде 0xP. Вывод команд из пп. 6–8 представлен на рис. 3.5.

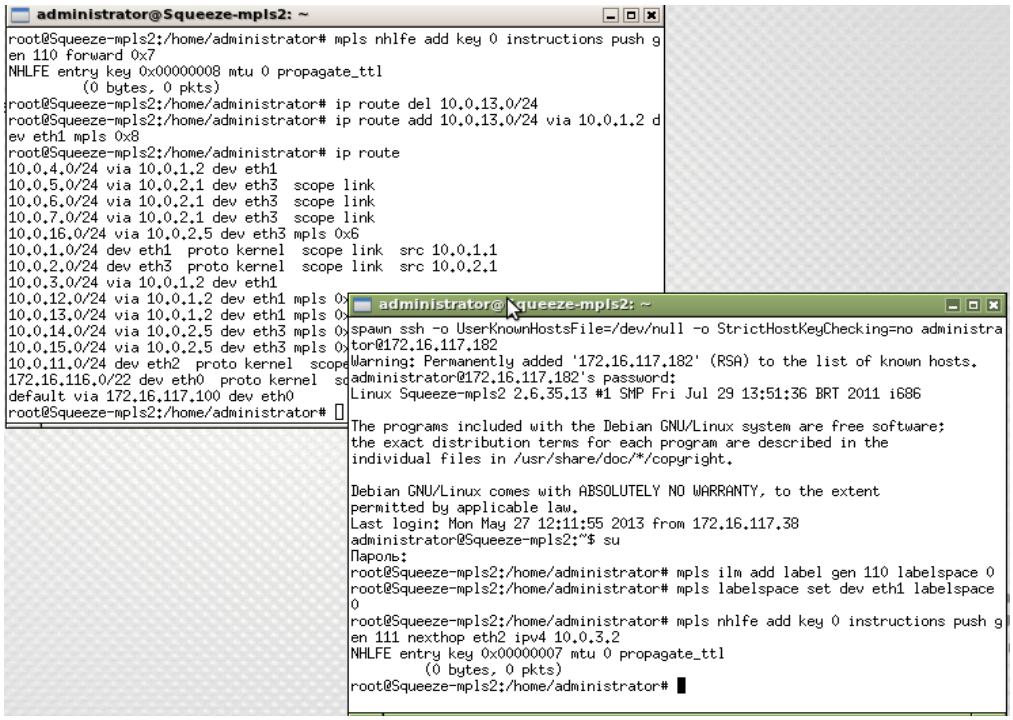


Рис. 3.5. Транзитный маршрутизатор:
установление меток; пространство меток

9. При использовании технологии MPLS решение о дальнейшей пересылке пакета осуществляется на основании входящей метки и интерфейса, поэтому для транзитных соединений необходимо связать входящую и исходящую метки командой:

```
sudo mpls xc add ilm_label gen CCC ilm_labelspace 0 nhlfe_key 0xP
```

(где **CCC** – метка, внешняя в стеке, установленная на граничном маршрутизаторе (1), по табл. 3.1; **labelspace 0** – пространство меток 0; **0xP** – ключ метки, полученный в п. 8).

(Удалить *неверно введенную* метку можно командой: *mpls xc del ilm_label gen CCC ilm_labelspace 0*.)

10. Далее нужно удалить стандартный маршрут до сети терминала-получателя командой:

```
ip route del 10.0.L.0/24
```

Затем добавить новый маршрут командой:

```
sudo ip route add 10.0.L.0/24 via 10.0.T.F dev ethX mpls 0xP
```

(где 0xP – сформированный ключ в п. 8.; **10.0.L.0/24** – IP-адрес сети терминала-получателя согласно табл. 3.1; **10.0.T.F** – IP-адрес граничного маршрутизатора (3), указанный в соответствии с вариантом в табл. 3.1; **eth X** – интерфейс транзитного маршрутизатора (2) в сторону следующего граничного маршрутизатора (3), указанный в табл. 3.1;

11. Далее следует установить новую входящую метку на следующем граничном маршрутизаторе (3), для чего нужно подключиться к нему и ввести команду:

```
sudo mpls ilm add label gen DDD labelspace 0
```

(где **DDD** – установленная исходящая метка на транзитном маршрутизаторе (2), указанная согласно варианту в табл. 3.1).

Эта команда удалит внешнюю метку в стеке.

12. Для удаления внутренней метки в стеке нужно ввести для нее аналогичную команду на граничном маршрутизаторе (3):

```
sudo mpls ilm add label gen BBB labelspace 0
```

(где **BBB** – установленная исходящая внутренняя метка на граничном маршрутизаторе (1), указанная согласно варианту в табл. 3.1).

Чтобы убедиться, что новая метка добавлена, нужно использовать команду для просмотра входящих меток:

```
sudo mpls ilm
```

Вывод команды показан на рис. 3.6.

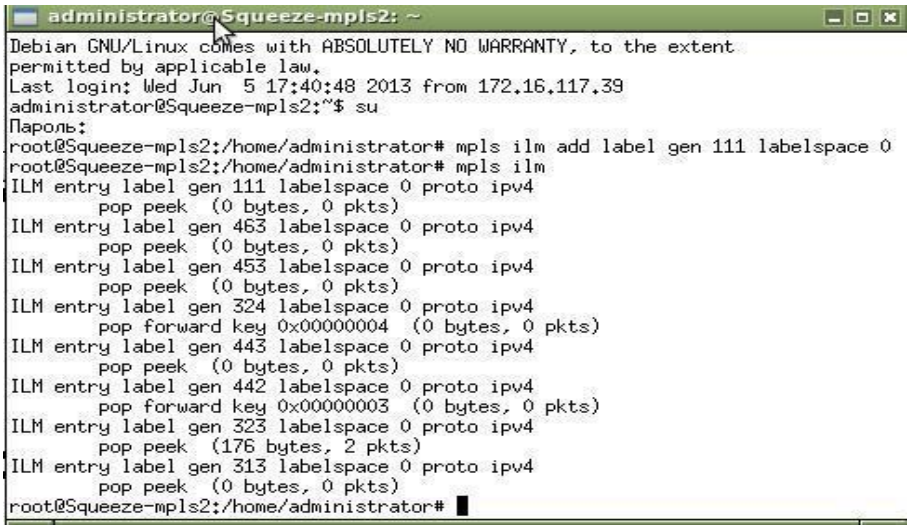


Рис. 3.6. Просмотр входящих меток

13. Чтобы проверить соединение с терминалом-получателем, нужно подключится к терминалу-источнику согласно табл. 3.1 (его номер выбирается по первой цифре столбца «Путь»), и ввести команду:

ping ip-адрес терминала-получателя

(ip-адрес терминала-получателя – по табл. 3.1).

14. Далее нужно свернуть окно удаленной консоли (чтобы тестовые пакеты продолжали отправляться терминалу-получателю вне зависимости от результата).

Затем запустить программу «WireShark на сервере», используя ярлык на рабочем столе. В открывшимся окне следует выбрать зону MPLS. Далее согласно варианту по табл. 3.1 указать граничный маршрутизатор (1), на котором будет осуществляться мониторинг передачи пакетов. Интерфейс для перехвата пакетов выбирается также по табл. 3.1.

Для поиска пакетов можно использовать фильтр, для этого в поле ***Filter*** надо ввести ***mpls*** (или ***icmp*** или ***ip.dst==****IP-адрес терминала получателя*), а затем нажать ***Apply***.

Нужно проверить наличие пакетов, убедиться, что это пакеты, сгенерированные командой в п. 12, и изучить структуру заголовков MPLS. **Значения полей MPLS следует выписать в отчет, проверить их соответствие вводным данным в табл. 3.1 и сделать выводы.**

15. Далее закрыть программу «*Wireshark* на сервере» и вновь открыть на транзитном маршрутизаторе (2), запустить перехват пакетов на интерфейсе согласно табл. 3.1.

Аналогично п. 13 выписать информацию в отчет.

16. Закрыть программу «*Wireshark* на сервере». Развернуть удаленную консоль с ping и сочетанием клавиш ***Ctrl + C*** остановить команду ***ping***. Закрыть «Удаленную консоль».

17. Подключиться к транзитному маршрутизатору (2) и удостоверить-ся, что он не знает, как обрабатывать внутреннюю метку в стеке, используя команду для просмотра входящих меток:

```
sudo mpls ilm
```

Следует убедиться, что в выводе команды не видно внутренней метки (которую можно было наблюдать в пп. 14 и 15).

Лабораторная работа 4
БЫСТРАЯ РЕМАРШРУТИЗАЦИЯ (FRR). ЗАЩИТА ЛИНИИ

Цель лабораторной работы заключается в изучении механизма защиты уязвимой линии в сети MPLS с использованием процедуры быстрой ремаршрутизации.

В результате выполнения лабораторной работы студент получит навык создания резервных маршрутов для защиты путей MPLS и научится анализировать характеристики переключения трафика с основного на резервный маршрут.

Таблица 4.1

Варианты заданий*

Вариант	R (1)	R (2)	Интерфейс на R (1)	IP-адрес R (2)	Метка	Key на R (2)	Интерфейс для отключения линии	Терминал-источник→ получатель и его IP-адрес
1	6	5	eth3	10.0.7.5	1000	0x2	eth2	6 → 4: 10.0.14.14
2	4	5	eth1	10.0.6.5	2000	0x3	–	4 → 6: 10.0.16.16
3	3	4	eth3	10.0.4.4	3000	0x2	eth6	3 → 5: 10.0.15.15
4	5	4	eth2	10.0.6.4	4000	0x4	–	5 → 3: 10.0.13.13
5	1	2	eth2	10.0.1.2	5000	0x3	eth5	1 → 3: 10.0.13.13
6	3	2	eth1	10.0.3.2	6000	0x2	–	3 → 1: 10.0.11.11
7	2	1	eth1	10.0.1.2	7000	0x5	eth4	2 → 5: 10.0.15.15
8	5	1	eth1	10.0.2.1	8000	0x2	–	5 → 2: 10.0.12.12
9	2	3	eth2	10.0.3.3	9000	0x4	eth5	2 → 4: 10.0.14.14
10	4	3	eth2	10.0.4.3	10000	0x3	–	4 → 2: 10.0.12.12

*Количество вариантов при выполнении работы должно быть четным! Если оно нечетное, то последней бригаде необходимо также выполнить работу за следующий вариант.

Выполнение лабораторной работы

1. Для удаленного подключения к граничному маршрутизатору (1) открыть ярлык «Удаленная консоль», расположенный на рабочем столе, в открывшемся окне выбрать зону **MPLS** и номер маршрутизатора (1), табл. 4.1, соответствующий варианту задания.

Так как обычная архитектура сети не подходит для выполнения данной лабораторной работы, необходимо добавить дополнительные связи между маршрутизаторами сети. Для этого следует запустить специальный скрипт:

```
sudo ./add_linkN
```

(где **N** номер варианта).

2. Создать резервный маршрут, чтобы в случае потери связи по основному маршруту переход на резервный маршрут осуществился как можно скорее.

Резервный маршрут будет двухсторонним, поэтому необходимо создать его сразу в обе стороны. В данной лабораторной работе одна бригада строит резервный маршрут в одну сторону, а другая – в другую.

Добавим новую исходящую метку до следующего маршрутизатора резервного маршрута, для этого воспользуемся командой добавления меток:

```
sudo mpls nhlfe change key 0x9 instructions push gen L nexthop ethY ipv4 10.0.N.M
```

(**L** – метка; **ethY** – интерфейс на маршрутизаторе (1); **10.0.N.M** – ip-адрес следующего маршрутизатора).

Для проверки добавления новой метки применить команду просмотра исходящих меток:

```
sudo mpls nhlfe
```

3. Для удаленного подключения к граничному маршрутизатору (2), необходимо открыть ярлык «Удаленная консоль», расположенный на рабочем столе, в открывшемся окне выбрать зону **MPLS** и номер маршрутизатора (2), табл. 4.1, соответствующий варианту задания.

Добавим на транзитном маршрутизаторе резервного маршрута новые входящие метки от соседних узлов резервного маршрута, которые будут принадлежать пространству меток 0:

```
sudo mpls ilm add label gen L labelspace 0
```

(где **L** – метка).

Для проверки добавления новой метки применить команду просмотра входящих меток:

```
sudo mpls ilm
```

Так как от маршрутизатора (2), табл. 4.1, до сети терминала-получателя уже установлена метка, то создавать новую не обязательно, можно воспользоваться уже установленной, поэтому выполним пересылку меток, используя команду пересылки меток:

```
sudo mpls xc add ilm_label gen L ilm_labelspace 0 nhlfe_key 0xK
```

(где **L** – метка, **0xK** – key, выбираются согласно табл. 4.1).

Для проверки добавления новой метки применить команду просмотра пересылаемых меток:

```
sudo mpls xc
```

4. Для удаленного подключения к граничному маршрутизатору (1), табл. 4.1, открыть ярлык «Удаленная консоль», расположенный на рабочем столе, в открывшемся окне выбрать зону **MPLS** и номер маршрутизатора (1), соответствующий варианту задания.

Запустить скрипт, обеспечивающий выполнение процедуры FRR, используя команду:

sudo ./frrN.sh

(где **N** – номер варианта).

Данное окно не следует закрывать, чтобы не прекращать выполнение скрипта!

5. Определить маршрут до терминала-получателя и записать его в отчет. Для этого открыть ярлык «Удаленная консоль», выбрать номер терминала-источника в соответствии с вариантом. Воспользоваться командой:

traceroute IP-адрес терминала-получателя

Проверить соединение между терминалами, используя команду:

ping IP-адрес терминала-получателя

Чтобы отследить количество пакетов, потерянное при изменении маршрута, выполнение команды ping останавливать не нужно!

6. На терминале-источнике запустить Wireshark (используя ярлык «Wireshark на сервере»), при этом должны быть видны ICMP-пакеты.

7. (Только для вариантов 1, 3, 5, 7, 9!) Для удаленного подключения к граничному маршрутизатору (1) открыть ярлык «Удаленная консоль», расположенный на рабочем столе, в открывшемся окне выбрать зону **MPLS** и номер маршрутизатора (1) , соответствующий варианту задания.

Искусственно «разрушить» соединение между маршрутизатором (1) и маршрутизатором (2). Для этого полностью запретить прием пакетов на соответствующем интерфейсе маршрутизатора (1), используя команду:

sudo iptables -I INPUT -i ethX -j DROP

(где ethX – интерфейс для отключения линии).

8. После того как в выводе работы программы обеспечения работы процедуры FRR появится сообщение о смене маршрута, убедимся, что пакеты продолжают достигать получателя; по значению поля TTL определим, что путь стал на одну пересылку длиннее.

9. В запущенном в п. 6 Wireshark найти момент переключения на резерв по нарушению временных интервалов между отправлением пакетов ICMP (либо по сообщениям с ошибками). После этого нужно посчитать, сколько времени заняло переключение на резервный маршрут, и соотнести это время с межпакетным интервалом при нормальной передаче, с джиттером при нормальной передаче и с временем доставки пакета. Для расчета примерного времени доставки пакета разделить время двухсторонней задержки пополам. Сравнить время передачи пакетов по основному маршруту и по резервному маршруту. Полученные цифры и выводы выписать в отчет.

10. Остановить выполнение команды ping, в выводе команды определить количество потерянных пакетов. Снова определить маршрут до терминала-получателя, используя команду traceroute.

11. (Только для вариантов 1, 3, 5, 7, 9.)

Восстановить работоспособность линии с помощью команды (для этого разрешить прием и отправку пакетов на том же интерфейсе, что и в п. 6):

```
sudo iptables -I INPUT -i ethX -j ACCEPT
```

12. Повторить п. 9 для процесса возвращения трафика на основной маршрут. После этого можно остановить и закрыть wireshark.

13. После того как в выводе работы программы обеспечения работы процедуры FRR появится сообщение о возврате на основной маршрут, определить маршрут до терминала-получателя, используя команду traceroute. Записать маршрут в отчет и сделать вывод обо всех изменениях маршрута.

Лабораторная работа 5

ДИФФЕРЕНЦИАЛЬНОЕ ОБСЛУЖИВАНИЕ В СЕТИ MPLS

Цель лабораторной работы заключается в изучении принципов настройки и работы дифференцированного обслуживания трафика в MPLS.

В результате лабораторной работы студент получит навык создания видео-трансляции, назначения потоку данных значений приоритетного обслуживания, назначение значений приоритетного обслуживания на маршрутизаторах MPLS и научится анализировать параметры QoS для потоков данных переданных с различным качеством.

Таблица 5.1

Варианты заданий

Вариант	Терминал-источник (1) /IP-адрес /RTP порт	Терминал-источник (2) /IP-адрес /RTP порт	Терминал-получатель (3) /IP-адрес /RTP порт	Маршр. (1)	Маршр. (2) / IP-адр. /интерф.	Маршр. (3) / IP-адр.	DSCP (1)	DSCP (2)	Метка
1	1 /10.0.11.11 /5001	2 /10.0.12.12 /5002	3 /10.0.13.13 /5001/5002	1	2 /<10.0.1.2 /eth2>	3 /10.0.3.3	0x2e	0x1a	100
2	5 /10.0.15.15 /5005	4 /10.0.14.14 /5004	6 /10.0.16.16 /5005/5004	5	4 /<10.0.6.4 /eth4>	6 /10.0.5.6	0x2e	0x1a	200
3	4 /10.0.14.14 /5444	5 /10.0.15.15 /5555	6 /10.0.16.16 /5444/5555	4	5 /<10.0.6.5 /eth3>	6 /10.0.7.6	0x2e	0x1a	300
4	5 /10.0.15.15 /5055	4 /10.0.14.14 /5044	3 /10.0.13.13 /5055/5044	5	4 /<10.0.6.4 /eth2>	3 /10.0.4.3	0x2e	0x1a	400
5	2 /10.0.12.12 /5022	1 /10.0.11.11 /5011	5 /10.0.15.15 /5022/5011	2	1 /<10.0.1.1 /eth3>	5 /10.0.2.5	0x2e	0x1a	500

Выполнение лабораторной работы

1. Назначение приоритетов пакетам.

Differentiated Services Code Point (DSCP – точка кода дифференцированных услуг).

Поле в заголовке IP-пакета используется для классификации передаваемой информации. На основании значения данного поля IP-пакеты будут получать тот или иной класс обслуживания.

1.1. Для выполнения лабораторной работы необходимо изучить свой вариант в табл. 5.1 и на ее основе нарисовать схему, обязательно указывая все используемые терминалы и маршрутизаторов, а также их адреса, порты, метки и классы обслуживания. В качестве подсказки можно воспользоваться общей схемой сети MPLS в прил. 1.

1.2. Для удаленного подключения (далее подключения) открыть ярлык «Удаленная консоль», расположенный на рабочем столе, в открывшемся окне выбрать зону MPLS и номер необходимого устройства.

1.3. Чтобы установить на все исходящие пакеты от терминала-источника (1) нужное значение DSCP (1), подключиться к терминалу-источнику (1) согласно варианту в табл. 5.1. И выполнить команды:

```
sudo /sbin/iptables -t mangle -F
sudo /sbin/iptables -t mangle -A OUTPUT -j DSCP --set-dscp AxBC
```

(где AxBC – значение DSCP (1), класс трафика, устанавливаемый для пакетов, идущих от терминала источника (1)).

Если команды не работают, нужно переключиться в режим суперпользователя с помощью команды ***sudo su***. Пароль вводится преподавателем.

После этого нужно убедиться в успешном выполнении команд и свернуть удаленную консоль к терминалу-источнику до дальнейшего использования.

1.4. Аналогично п. 1.3 установить нужное значение DSCP (2) для пакетов от терминала источника (2) согласно варианту в табл. 5.1.

Обратите внимание, что параметру **AxBC** задается значение DSCP (2) – класс трафика, устанавливаемый для пакетов от терминала источника (2).

1.5. Чтобы задать всем потокам пакетов различные значения полей DSCP, нужно установить на все исходящие пакеты от терминала получателя (3) значение DCSP, равное 0. Для этого нужно проделать аналогичные п. 1.3 действия для терминала получателя (3) согласно варианту в табл. 5.1.

Обратите внимание что параметру **AxBC** назначается значение 0 – класс трафика, устанавливаемый для пакетов от терминала получателя (3).

На данном этапе на основании полей DSCP пакетам сетью будет предоставлен различный класс обслуживания.

1.6. Для исследования дифференциального обслуживания необходимо, чтобы поток информации от терминала источника (1) проходил по тому же участку пути, где проходит информация от терминала источника (2).

Чтобы маршрутизатор (1) терминала-источника (1) направил информацию к терминалу-получателю через маршрутизатор (2) терминала-источника (2), нужно подключиться к маршрутизатору (1) в соответствии с вариантом в табл. 5.1 и выполнить команду добавления статического маршрута:

```
sudo ip route add 10.0.1F.0/24 via 10.0.X.E dev eth1
```

(где **10.0.1F.0/24** – IP-адрес сети терминала получателя (3), где ***F*** – номер терминала-получателя (3) согласно варианту в табл. 5.1; ***10.0.****X.E* – IP-адрес маршрутизатора (2) терминала источника (2) на интерфейсе в сторону маршрутизатора (1) терминала источника (1) (X – цифра сети, E – номер маршрутизатора (2)).

1.7. Для проверки соединения с терминалом-получателем (3) нужно набрать команду:

ping IP

(где **IP** – адрес терминала получателя).

2. Назначение меток на маршрутизаторах.

Так как узлы сети MPLS анализируют заголовок MPLS, то для того чтобы они могли предоставлять различные классы обслуживания пакетам от различных источников, нужно использовать различные значения полей EXP заголовков MPLS. Поэтому необходимо, чтобы граничные маршрутизаторы (1), (3) устанавливали соответствие между значениями полей DSCP заголовка IP и EXP заголовка MPLS .

Таблица 5.2

Соответствие между параметрами классов обслуживания

TC_INDEX	EXP	DCSP
3	0x3	0xf
1	0x1	0x1a
5	0x5	0x3
2	0x2	0x2e
0	0x0	0x5
3	0x3	0x0
		0x0

Traffic Class (EXP) – поле заголовка MPLS, необходимое для реализации механизмов качества обслуживания и явного уведомления о перегрузке (ECN).

Explicit Congestion Notification (ECN, *явное уведомление о перегруженности*) – расширение протокола IP, позволяющее обеим сторонам в сети узнавать о возникновении затора на маршруте к заданному хосту или сети без отбрасывания пакетов.

TC_INDEX – фильтр, используемый для обеспечения механизмов качества обслуживания в ОС Linux.

2.1. Для задания новой исходящей метки до маршрутизатора (3) нужно подключиться к маршрутизатору (2) согласно варианту в табл. 5.1. Используя нижеуказанную команду, задать новую исходящую метку и одновременно с тем определить соответствие между DSCP заголовка IP, значением поля EXP заголовков MPLS и TC_INDEX, используемыми программными маршрутизаторами:

sudo mpls nhlfe add key 0 instructions ds2exp 0xf 0x1a 0x3 0x2e 0x5 0x0 0x0 exp2tc 0x3 0x1 0x5 0x2 0x0 0x3 push gen XXX nexthop ethY ipv4 10.0.N.M

(где [ds2exp 0xf 0x1a 0x3 0x2e 0x5 0x0 0x0 exp2tc 0x3 0x1 0x5 0x2 0x0 0x3] устанавливает соответствие между DCSP, EXP и TC_INDEX согласно табл. 5.2; **XXX** – новая исходящая метка в соответствии с вариантом в табл. 5.1; ***key 0*** – параметр, который мы задаем равным 0 для создания нового ключа исходящей метки; **ethY** – интерфейс на маршрутизаторе (1) в сторону маршрутизатора (3) по табл. 5.1; **10.0.N.M** – IP-адрес маршрутизатора (2) на интерфейсе в сторону маршрутизатора (3) по табл. 5.1;

Результат добавления новой метки появится на экране, как на рис. 5.1. Сформированный ключ будет выведен в форме 0x0000000Z, его необходимо записать в отчет, для удобства представив в виде 0xZ.

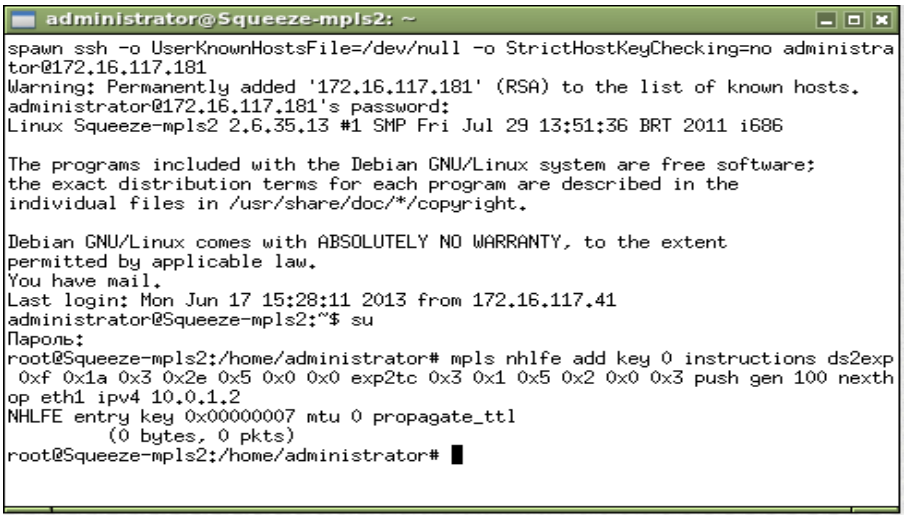


Рис. 5.1. Добавление новой метки

2.2. Чтобы произвести перевод FEC (Forwarding Equivalence Classes – классы эквивалентной пересылки) в исходящие метки (т. е. всем пакетам, поступающим на маршрутизатор (2) с одинаковым классом обслуживания присвоить исходящую метку XXX согласно табл. 5.1, назначенную в п. 2.1), нужно использовать команду:

sudo iptables -t mangle -A FORWARD -m dscp --dscp AxBC -j mpls --nhlfe 0xZ ,

(где **AxBC** – значение DSCP (1); **0xZ** – ключ, полученный в п. 2.1).

2.3. Для перевода FEC для терминала источника (2) нужно повторить команду из п. 2.2 с параметром **AxBC**, равным значениям DSCP (2) из табл. 5.1. Пример ввода команд показан на рис. 5.2.

```
root@Squeeze-mpls2:/home/administrator# iptables -t mangle -A FORWARD -m dscp --
dscp 0x1a -j mpls --nhlfe 0x7
root@Squeeze-mpls2:/home/administrator# iptables -t mangle -A FORWARD -m dscp --
dscp 0x2e -j mpls --nhlfe 0x7
root@Squeeze-mpls2:/home/administrator#
```

Рис. 5.2. Перевод FEC в исходящие метки для терминалов-источников

2.4. Для использования технологии MPLS нужно удалить на маршрутизаторе (2) существующий маршрут до сети терминала-получателя (3) командой:

sudo ip route del 10.0.L.0/24

(где **10.0.**L**.0** – адрес сети, в которой находится клиент-получатель (3); **/24** – указание маски подсети (единая для всех вариантов)).

А затем добавить новый маршрут с использованием технологии MPLS командой:

sudo ip route add 10.0.L.0/24 via 10.0.N.M mpls 0xZ

(где **10.0.L.0** – IP-адрес сети в которой находится клиент получатель (3); **/24** – указание маски подсети (единая для всех вариантов); **10.0.N.M** – IP-адрес маршрутизатора (3); **0xZ** – ключ, полученный в п. 2.1).

2.5. Чтобы обработать входящую метку от маршрутизатора (2) на маршрутизаторе (3), необходимо подключится к маршрутизатору (3) и ввести команду:

sudo mpls ilm add label gen XXX labelspace 0

(где XXX – метка, заданная в п. 2.1).

Для проверки добавления новой метки применить команду просмотра входящих меток:

sudo mpls ilm

Теперь сеть готова принимать пакеты и классифицировать их по классам обслуживания, далее необходимо настроить параметры обслуживания, такие как полоса пропускания, размер очереди и дисциплина обслуживания.

3. Настройка QoS на транзитном маршрутизаторе (2).

Сеть MPLS базируется на программных маршрутизаторах с ОС Linux, поэтому для настройки параметров качества обслуживания (описываются в начале лабораторной работы) используются механизмы управления качеством ОС Linux с помощью утилиты ***tc*** (traffic control).

3.1. Для настройки QoS на маршрутизаторе (2) следует подключиться к маршрутизатору (2) согласно варианту табл. 5.1 и перевести TCINDEX 1 в класс 1:11, TCINDEX 2 в класс 1:12 вводом команд:

sudo tc qdisc add dev ethY root handle 1: htb
sudo tc filter add dev ethY parent 1:0 protocol 0x8847 prio 1 tcindex mask 0xf shift 0 pass_on
sudo tc filter add dev ethY parent 1:0 protocol 0x8847 prio 1 handle 1 tcindex classid 1:11
sudo tc filter add dev ethY parent 1:0 protocol 0x8847 prio 1 handle 2 tcindex classid 1:12

(где **ethY** – интерфейс на маршрутизаторе (2) в сторону маршрутизатора (3), указанный в табл. 5.1).

3.2. Для ограничения максимальной полосы пропускания канала в сторону маршрутизатора (3) величиной в 900 кбит/с на маршрутизаторе (2) нужно применить команду:

tc class add dev ethY parent 1:0 classid 1:10 htb rate 900kbit

(где **ethY** – интерфейс на маршрутизаторе (2) в сторону маршрутизатора (3), указанный в табл. 5.1).

3.3. Для обеспечения гарантированной полосы пропускания для каждого класса обслуживания в 500 кбит/с для DSCP (2) и 300 кбит/с для DSCP (1) на маршрутизаторе (2) нужно ввести команды:

tc class add dev ethY parent 1:10 classid 1:11 htb rate 500kbit ceil 900kbit
tc class add dev ethY parent 1:10 classid 1:12 htb rate 300kbit ceil 900kbit

(где **ethY** – интерфейс на маршрутизаторе (2) в сторону маршрутизатора (3), указанный в табл. 5.1).

3.4. Для наглядности следует ограничить очередь на маршрутизаторе (2) до 5, используя команды:

sudo tc qdisc add dev ethY parent 1:11 handle 110: pfifo limit 5
sudo tc qdisc add dev ethY parent 1:12 handle 120: pfifo limit 5

(где **ethY** – интерфейс на маршрутизаторе (2) в сторону маршрутизатора (3), указанный в табл. 5.1).

3.5. Чтобы проверить соединение от терминала-источника (1) до терминала-получателя (3), как показано на рис. 5.3, нужно подключится к терминалу-источнику (1) согласно варианту в табл. 5.1 и ввести команду:

ping IP-адрес

(где **IP-адрес** является адресом терминала-получателя (1) согласно варианту в табл. 5.1).

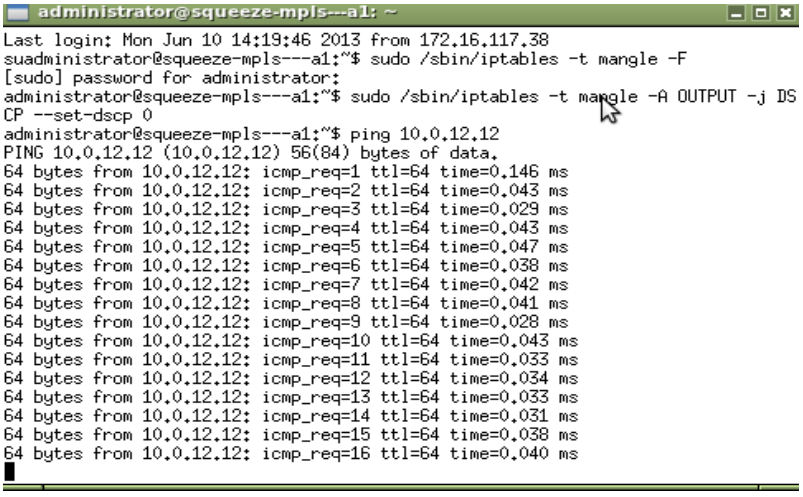


Рис. 5.3. Проверка соединения

3.6. Аналогично п. 3.5 следует проверить соединение от терминала-источника (2).

В итоге сеть способна принимать пакеты с различными значениями полей DCSP в заголовке IP, переводить их в соответствующие значения полей EXP заголовка MPLS и предоставлять заданное качество обслуживания.

4. Настройка видеотрансляции.

Для более наглядной демонстрации различий в качестве обслуживания следует транслировать от различных источников 2 одинаковых видеопотока с полосой пропускания в 500 кбит/с по сети, а на приемной стороне их просматривать и давать субъективную оценку.

Так как полоса пропускания канала, по которому будут проходить видеопотоки, ограничена величиной в 900 кбит/с, произойдет ухудшение качества воспроизводимого видео. Вследствие того что гарантированное качество обслуживания пакетов от одного источника выше, чем от другого, ухудшение видеопотока от одного источника будет сильнее, чем от другого.

Далее необходимо запустить параллельно или последовательно 3 программы VLC: на терминале-источнике (1) – пп. 4.1–4.4, терминале-источнике (2) – п. 4.6, терминале-получателе (3) – п. 4.7.

VLC media player – межплатформенный проигрыватель, может быть использован в качестве сервера для трансляции потока аудио/видео по сети (поддерживает протоколы IPv4 и IPv6). Не требует установки дополнительных кодеков, а также воспроизводит потоковое незашифрованное (без DRM) видео (IPTV) и интернет-радио. Предоставляет возможность записи потокового аудио/видео на компьютер.

4.1. Для удаленного подключения к терминалу-источнику видеопотока (1) необходимо открыть ярлык «VLC», расположенный на рабочем столе, в открывшемся окне выбрать зону MPLS и номер необходимого терминала согласно варианту, указанному в табл. 5.1.

Видеотрансляция производится с помощью медиа-проигрывателя VLC, который помимо ярлыка можно локально (либо удаленно) запустить командой:

vlc (либо: **ssh -X administrator@**IP-адрес терминала **vlc**)

4.2. Чтобы начать потоковое вещание в открывшемся окне медиа-проигрывателя, как показано на рис. 5.4, необходимо выбрать «***Медиа»***, затем «***Потоковое вещание».***

Для выбора видео для трансляции в открывшемся окне настройки потокового вещания в области «Выбор файлов» нажать ***«Добавить»***. Готовый файл с видео находится в директории:

Computer – / – media – _mp4.mpg

Для его выбора, как это показано на рис. 5.4, следует нажать «***Open***».

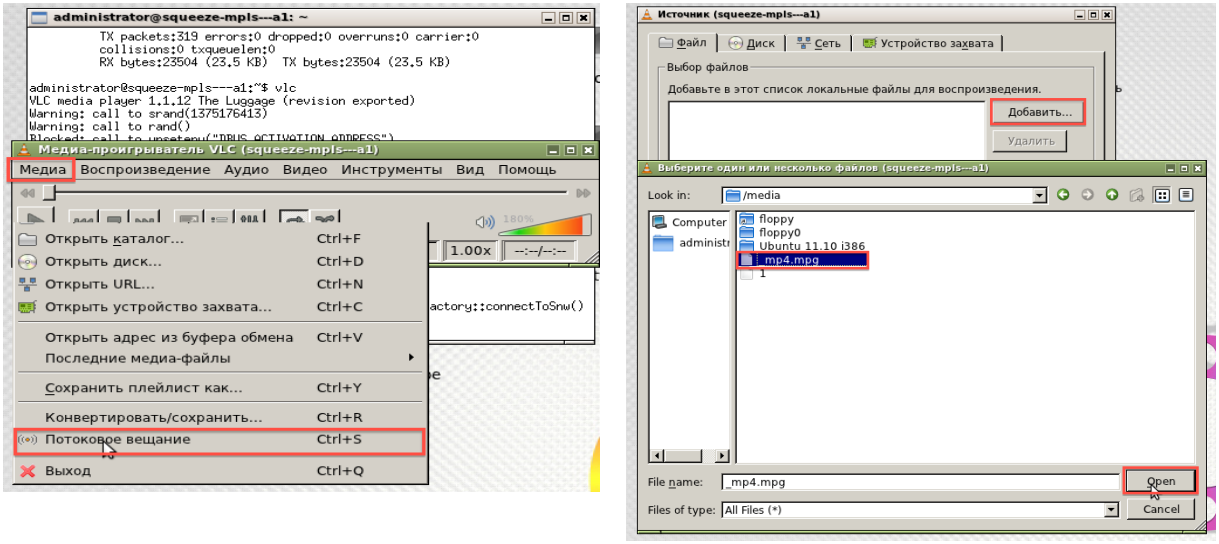


Рис. 5.4. Настройка и Окно потокового вещания

4.3. Чтобы настроить параметры трансляции, нужно нажать ***«Поток»***. После чего в качестве источника указывается видеофайл: /media/_mp4.mpg. Нажимаем ***«Следующий»*** для перехода в настройки пути назначения, как на рис. 5.5.

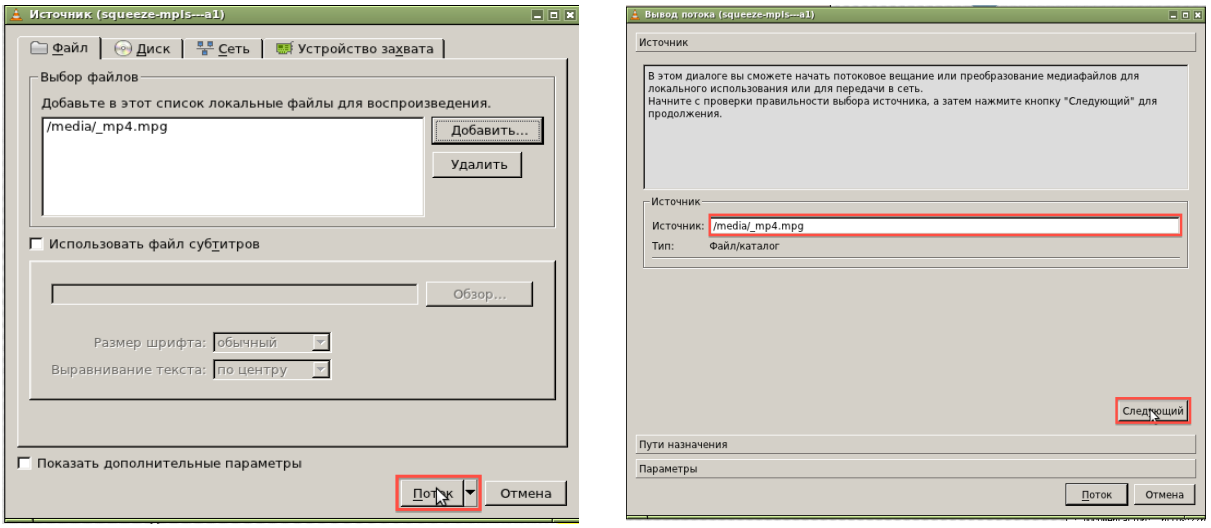


Рис. 5.5. Настройка параметров трансляции

4.4. Для выбора метода передачи во вкладке «Файлы» следует выбрать «***RTP/MPEG Transport stream***» и нажать ***«Добавить»***. Последовательность действий изображена на рис. 5.6. В поле «Адрес» нужно ввести **IP-адрес терминала получателя видеоинформации**, «Базовый порт» 5XXX для терминала источника (1) согласно варианту в табл. 5.1. Для проверки настройки видео и звука, как показано на рис. 5.6, необходимо во вкладке «Профиль» выбрать: ***Video→H.264+AAC (MP4)***.

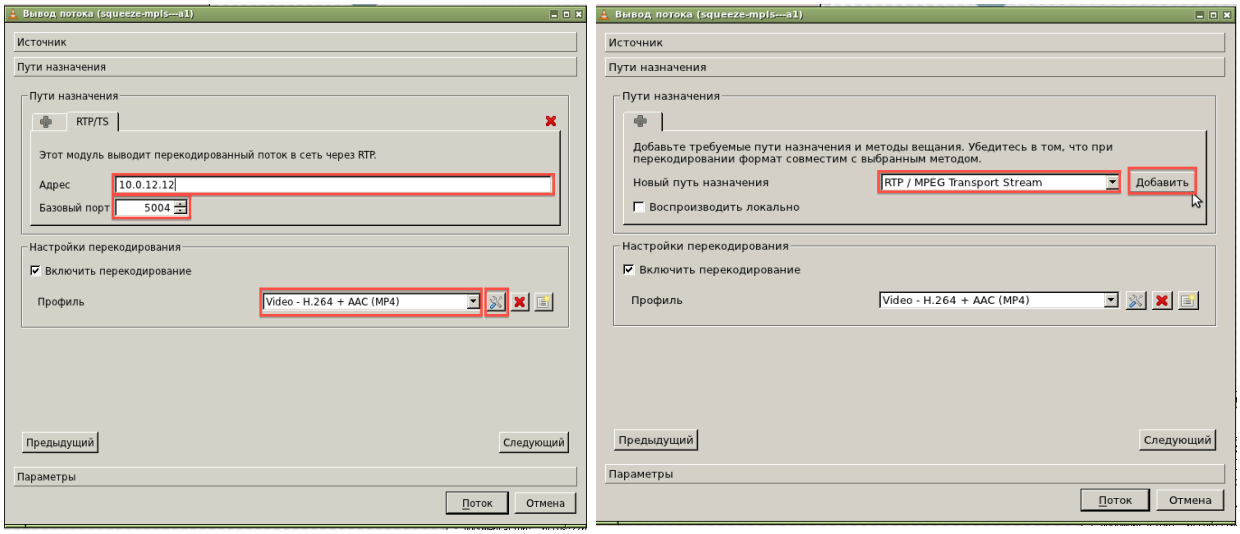


Рис. 5.6. Выбор метода передачи

Далее сохранить параметры и начать трансляцию видеофайла, для этого нажать ***«Поток»***, как показано на рис. 5.6. После окончания видеофайла трансляция начнется повторно сама (в противном случае необходимо нажать клавишу play).

4.5. (Выполнение пункта необязательно.) Чтобы проверить настройки профиля, нужно нажать на значок ***«Изменить выделенный профиль»*** (находится с вкладкой профиль).

Таблица 5.3

Параметры видеопотока

Параметр	Значение
Инкапсуляция	MPEG-1
Видео-кодек	MPEG-1
Частота кадров	25 к/с
Битрейт	500 кбит/с
Ширина	320
Высота	280

Параметр «Инкапсуляция» настраивается во вкладке «Инкапсуляция», все остальные параметры – во вкладке «Видео-кодек». Настройка параметра показана на рис. 5.7.

4.6. Для запуска видеотрансляции с терминала источника (2) согласно варианту в табл. 5.1 следует запустить на нем VLC и для него повторить пп. 4.1–4.4, изменив при этом значение «Базовый порт» на 5XXX для терминала источника (2) согласно варианту в табл. 5.1.

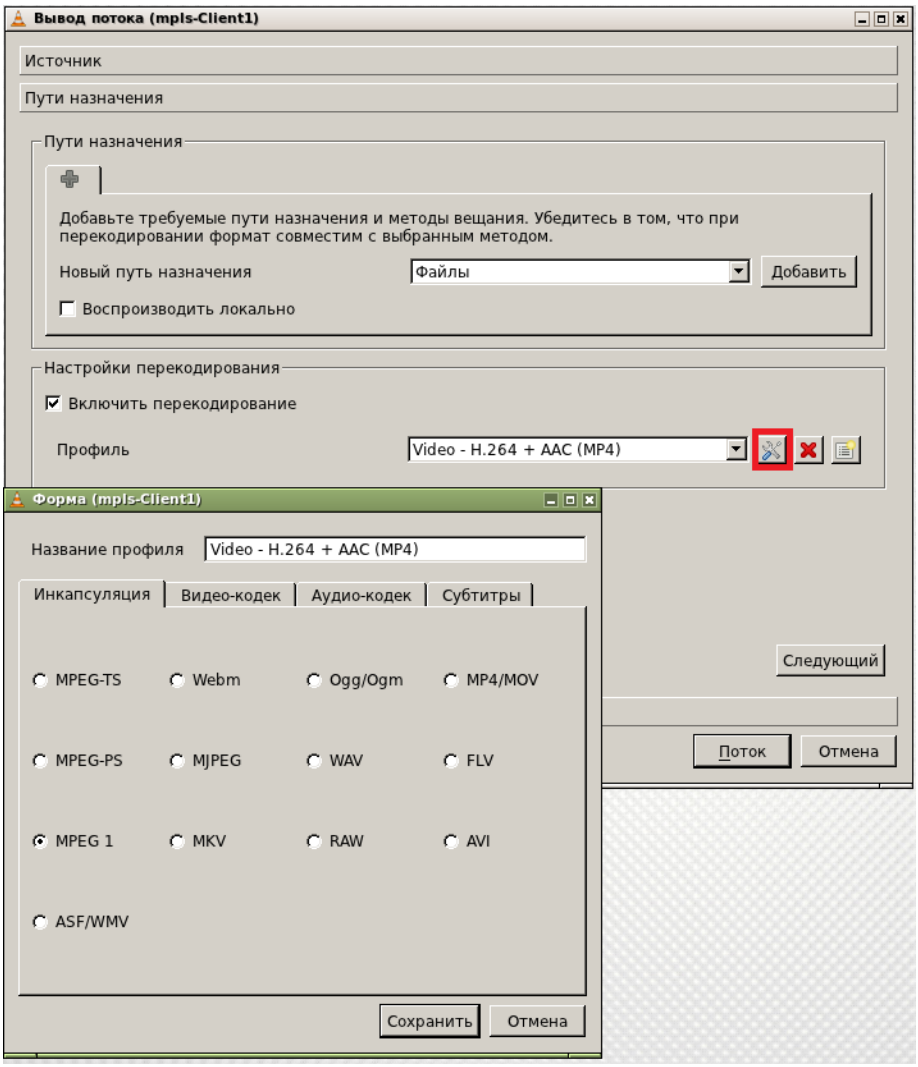


Рис. 5.7. Настройка параметра «Инкапсуляция»

4.7. Для просмотра видеопотоков на терминале-получателе (3) согласно варианту в табл. 5.1 следует запустить на нем VLC (п. 4.1), после чего в открывшемся окне медиапроигрывателя выбрать «***Медиа***», затем ***«Открыть URL»***, как показано на рис. 5.8. В поле «Введите сетевой адрес» ввести: ***rtp://@:****5XXX* (в соответствии с табл. 5.1 для терминала-получателя (3)). Затем отметить галочкой «***Показать доп. параметры»*** и «***Параллельно воспроизводить другой медиафайл»***, в поле «Другой файл» ввести: ***rtp://@:****5XXX* (в соответствии с табл. 5.1 для терминала получателя (3)). Далее нажать «Воспроизвести». Данные действия продемострированны на рис. 5.8. Для каждого из видеопотоков будет открыто отдельное окно, как это показано на рис. 5.9.

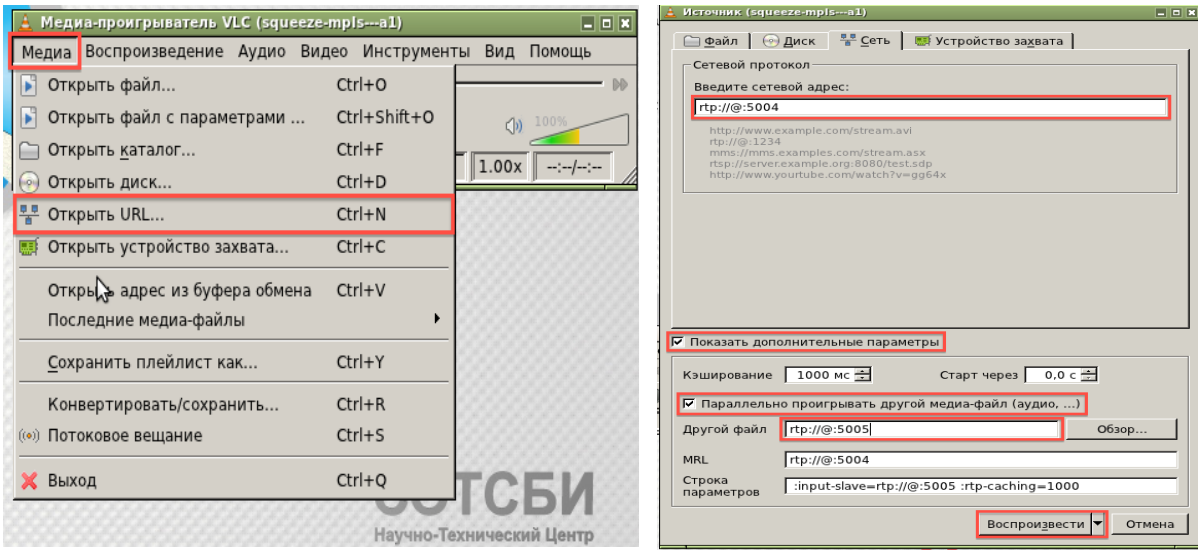


Рис. 5.8. Окно медиапроигрывателя и ввод сетевого адреса

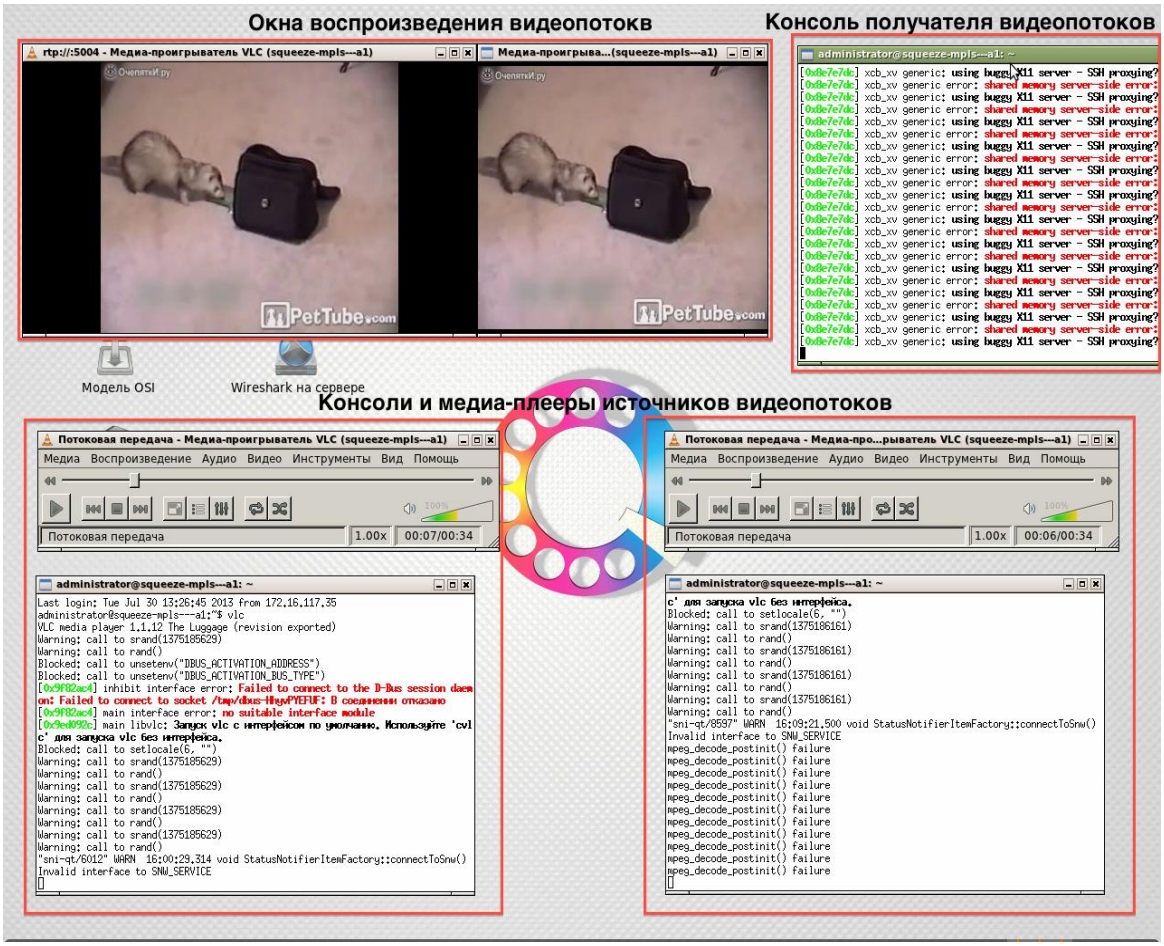


Рис. 5.9. Воспроизводимые видео

4.8. В завершение работы дать оценку качеству воспроизводимого видео, сделать выводы и занести их в отчет.

4.9. Дополнительно определить влияние настраиваемых параметров на субъективное восприятие видеокартинки.

Лабораторная работа 6

НАСТРОЙКА СТАТИЧЕСКИХ ПУТЕЙ MPLS (LSP) (НА ОБОРУДОВАНИИ HUAWEI)

Цель лабораторной работы заключается в изучении ручной настройки назначения меток MPLS на маршрутизаторах Huawei.

В результате выполнения лабораторной работы студент получит навык назначения и обработки меток MPLS на сетевом оборудовании Huawei.

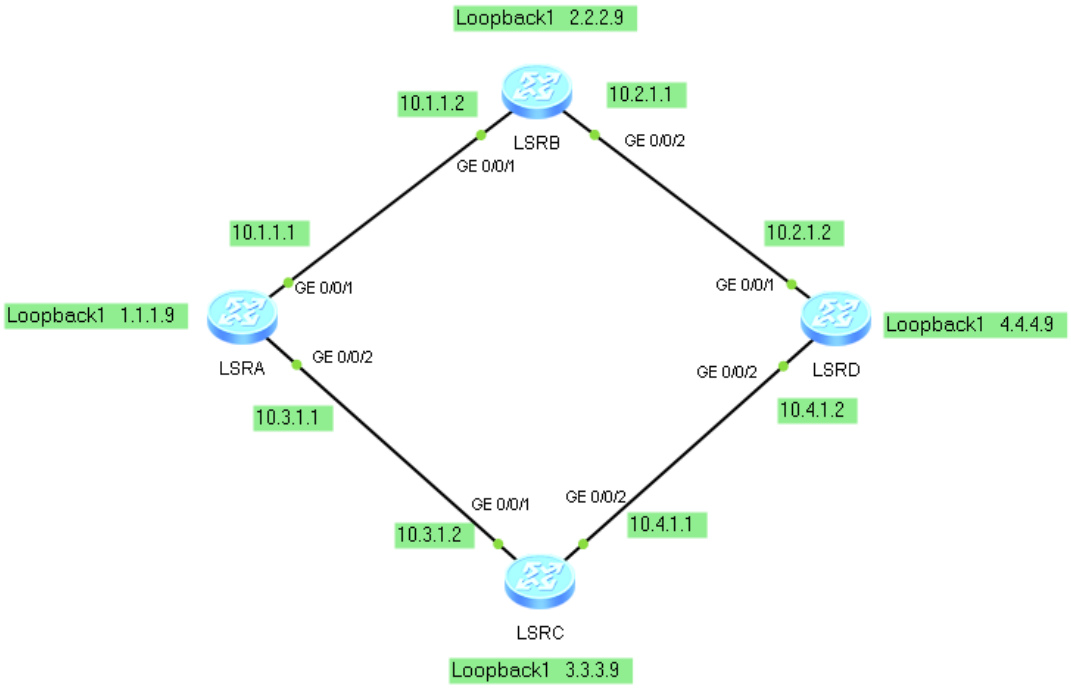


Рис. 6.1. Схема маршрутизаторов MPLS

Двунаправленные LSP расположены между LSRA и LSRD. LSP между LSRA и LSRD: LSRA → LSRB → LSRD. Между LSRD и LSRA: LSRD → LSRC → LSRA (рис. 6.1).

Выполнение лабораторной работы

1. *Предварительная настройка*.

Сначала провести предварительную настройку сетевого оборудования в соответствии со схемой на рис. 6.1. Для этого нужно сконфигурировать IP-адреса на реальных интерфейсах и на LoopBack (при этом LoopBack используются в качестве уникальных адресов LSR), а также настроить протокол маршрутизации OSPF.

В случае если работа выполняется в эмуляторе eNSP, можно использовать 4 маршрутизатора AR1220 (на которых задаем интерфейсы, как показано на рис. 6.1). Соединить их линией типа Copper. Выделить курсором

всю схему, нажать Start Device и подождать, пока не загорятся зеленые огоньки. Для последующей настройки кликнуть двойным нажатием левой клавишей мыши на изображение маршрутизатора.

В случае если работа выполняется на оборудовании Huawei, согласовать устройства, которые будут задействованы в схеме, с преподавателем, соединить их кабелем и подключиться к ним с использованием ярлыка «Удаленная консоль», Huawei → модель устройства (например, NE40E-01).

1.1. Настроить IP-адреса.

1.1.1. Получить права конфигурации устройства:

```
<Huawei> system-view
```

1.1.2. Пункт выполняется только при работе в эмуляторе eNSP.

Для удобства присвоить роутеру имя, например LSRA, следующей командой:

```
[Huawei] sysname LSRx_Model
```

1.1.3. Настроить GE 0/0/1 и 0/0/2 на маршрутизаторе и все остальные маршрутизаторы таким же способом:

```
[LSRx_Model] interface GigabitEthernet 0/0/1
[LSRx_Model-GigabitEthernet 0/0/1] ip address 10.1.1.1 30
[LSRx_Model-GigabitEthernet 0/0/1] interface GigabitEthernet 0/0/2
[LSRx_Model-GigabitEthernet 0/0/2] ip address 10.3.1.1 30
```

1.1.4. Далее установить на каждый из маршрутизаторов интерфейс LoopBack1 для LSR-ID:

```
[LSRx_Model-GigabitEthernet 0/0/1] interface LoopBack1
[LSRx_Model-LoopBack1] ip address 1.1.1.9 32
```

Затем установить на каждый из маршрутизаторов интерфейс LoopBack2 для объявлении уникальной маршрутной информации в протоколе OSPF:

```
[LSRx_Model-LoopBack1] interface LoopBack2
[LSRx_Model-LoopBack1] ip address X.X.X.X 32
```

(где **X** является номером варианта).

1.1.5. *В случае если работа выполняется в эмуляторе eNSP* для отключения вывода информации о служебных событиях (например, о включении интерфейса) ввести команду:

```
[LSRx_Model] undo t m
```

1.2. Настроить протоколы OSPF.

Для всех маршрутизаторов:

```
[LSRx_Model] ospf 1
[LSRx_Model-ospf-1]area 0
```

Для LSRA:

[LSRA_Model-ospf-1-area-0.0.0.0] **network 1.1.1.9 0.0.0.0**
[LSRA_Model-ospf-1-area-0.0.0.0] **network 10.1.1.0 0.0.0.3**
[LSRA_Model-ospf-1-area-0.0.0.0] **network 10.3.1.0 0.0.0.3**

Для LSRB:

[LSRB_Model-ospf-1-area-0.0.0.0] **network 2.2.2.9 0.0.0.0**
[LSRB_Model-ospf-1-area-0.0.0.0] **network 10.1.1.0 0.0.0.3**
[LSRB_Model-ospf-1-area-0.0.0.0] **network 10.2.1.0 0.0.0.3**

Для LSRC:

[LSRC_Model-ospf-1-area-0.0.0.0] **network 3.3.3.9 0.0.0.0**
[LSRC_Model-ospf-1-area-0.0.0.0] **network 10.3.1.0 0.0.0.3**
[LSRC_Model-ospf-1-area-0.0.0.0] **network 10.4.1.0 0.0.0.3**

Для LSRD:

[LSRD_Model-ospf-1-area-0.0.0.0] **network 4.4.4.9 0.0.0.0**
[LSRD_Model-ospf-1-area-0.0.0.0] **network 10.2.1.0 0.0.0.3**
[LSRD_Model-ospf-1-area-0.0.0.0] **network 10.4.1.0 0.0.0.3**

Для всех маршрутизаторов после настройки конфигурации зайти в маршрутизатор, чтобы посмотреть информацию о доступных сетях и маршрутизаторах (рис. 6.2):

[LSRx_Model] **display ip routing-table**

```
<LSRA>sys
Enter system view, return user view with Ctrl+Z.
[LSRA]display ip rout
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 12        Routes : 13

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

        1.1.1.9/32  Direct  0    0           D   127.0.0.1       LoopBack1
        2.2.2.9/32  OSPF    10   1           D   10.1.1.2        GigabitEthernet
0/0/1
        3.3.3.9/32  OSPF    10   1           D   10.3.1.2        GigabitEthernet
0/0/2
        4.4.4.9/32  OSPF    10   2           D   10.1.1.2        GigabitEthernet
0/0/1
                    OSPF    10   2           D   10.3.1.2        GigabitEthernet
0/0/2
       10.1.1.0/30  Direct  0    0           D   10.1.1.1        GigabitEthernet
0/0/1
       10.1.1.1/32  Direct  0    0           D   127.0.0.1       GigabitEthernet
0/0/1
       10.2.1.0/30  OSPF    10   2           D   10.1.1.2        GigabitEthernet
0/0/1
       10.3.1.0/30  Direct  0    0           D   10.3.1.1        GigabitEthernet
0/0/2
       10.3.1.1/32  Direct  0    0           D   127.0.0.1       GigabitEthernet
0/0/2
       10.4.1.0/30  OSPF    10   2           D   10.3.1.2        GigabitEthernet
0/0/2
      127.0.0.0/8   Direct  0    0           D   127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
```

Рис. 6.2. Таблица маршрутизации LSRA

Nexthop или исходящий интерфейс статического LSP на 4.4.4.9/32 от LSRA до LSRD определяется на основании таблицы маршрутизации. В этом примере IP-адрес следующего nexthop 10.1.1.2/30 (рис. 6.3).

```
<LSRD>sys
Enter system view, return user view with Ctrl+Z.
[LSRD]display ip rout
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 12        Routes : 13

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

        1.1.1.9/32  OSPF    10   2           D   10.2.1.1        GigabitEthernet
0/0/1
                    OSPF    10   2           D   10.4.1.1        GigabitEthernet
0/0/2
        2.2.2.9/32  OSPF    10   1           D   10.2.1.1        GigabitEthernet
0/0/1
        3.3.3.9/32  OSPF    10   1           D   10.4.1.1        GigabitEthernet
0/0/2
        4.4.4.9/32  Direct  0    0           D   127.0.0.1       LoopBack1
       10.1.1.0/30  OSPF    10   2           D   10.2.1.1        GigabitEthernet
0/0/1
       10.2.1.0/30  Direct  0    0           D   10.2.1.2        GigabitEthernet
0/0/1
       10.2.1.2/32  Direct  0    0           D   127.0.0.1       GigabitEthernet
0/0/1
       10.3.1.0/30  OSPF    10   2           D   10.4.1.1        GigabitEthernet
0/0/2
       10.4.1.0/30  Direct  0    0           D   10.4.1.2        GigabitEthernet
0/0/2
       10.4.1.2/32  Direct  0    0           D   127.0.0.1       GigabitEthernet
0/0/2
      127.0.0.0/8   Direct  0    0           D   127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
```

Рис. 6.3. Таблица маршрутизации LSRD

Nexthop или исходящий интерфейс статического LSP на 1.1.1.9/32 от LSRD до LSRA определяется на основании таблицы маршрутизации. В этом примере приведен IP-адрес следующего nexthop 10.4.1.1/30.

2. *Глобальная настройка MPLS.*

2.1. Настроить индетификатор LSR.

Конфигурация MPLS для каждого маршрутизатора (рис. 6.4):

[LSRx_Model**]mpls lsr-id IP_loopback**

(где **IP_loopback** – IP-адрес, указанный на LoopBack1 данного маршрутизатора),

[LSRx_Model]**mpls**

```
<LSRA>sys
Enter system view, return user view with Ctrl+Z.
[LSRA]mpls lsr-id 1.1.1.9
[LSRA]mpls
Info: Mpls starting, please wait... OK!
[LSRA-mpls]
Jul 29 2013 19:31:20-08:00 LSRA DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011.5.2
5.191.3.1 configurations have been changed. The current change number is 2, the
change loop count is 0, and the maximum number of records is 4095.
[LSRA-mpls]q
[LSRA]
```

Рис. 6.4. Запуск MPLS

2.2. Настроить MPLS на интерфейсах.

Настроить базовые функции MPLS непосредственно для каждого интерфейса (на примере LSRA проделать то же самое):

[LSRx_Model] **interface GigabitEthernet 0/0/1**
[LSRx_Model-GigabitEthernet 0/0/1]**mpls**
[LSRx_Model-GigabitEthernet 0/0/1]**interface GigabitEthernet 0/0/2**
[LSRx_Model-GigabitEthernet 0/0/2]**mpls**

2.3. Настроить LSP на LSRA.

Задать LSP от LSRA до LSRD. Конфигурация ingress-router (роутер, который является источником для заданного LSP) следующая:

[LSRA_Model]**static-lsp ingress RAtoRD destination 4.4.4.9 32 nexthop 10.1.1.2 out-label 20**

Так как источником является роутер LSRA, задать параметр ingress, пункт назначения, nexthop к транзитному маршрутизатору и выходную метку.

2.4. Настроить LSP на LSRB.

Конфигурация транзитного маршрутизатора LSRB:

[LSRB_Model]**static-lsp transit RAtoRD incoming-interface gigabiteethernet0/0/1 in-label 20 nexthop 10.2.1.2 out-label 40**

Здесь указывается входной интерфейс, входная метка из предыдущего пункта, nexthop к LSRD и выходная метка.

2.5. Настроить LSP на LSRD.

Конфигурация egress-router (роутер, который является пунктом назначения LSP):

[LSRD_Model]**static-lsp egress RAtoRD incoming-interface gigabiteethernet0/0/1 in-label 40**

Указать, что это egress router, входной интерфейс и входная метка.

2.6. Просмотреть информацию о LSP на LSRA.

Чтобы убедиться, что LSP поднят, зайти в LSRA и выполнить команду (рис. 6.5):

[LSRD_Model]**display mpls lsp**

```
[LSRA]display mpls lsp
------------------------------------------------------------------------------


                LSP Information: STATIC LSP
------------------------------------------------------------------------------
FEC                 In/Out Label  In/Out IF                      Vrf Name
4.4.4.9/32          NULL/20       -/GE0/0/1
[LSRA]display mpls static-lsp
TOTAL           :  1       STATIC LSP(S)
UP              :  1       STATIC LSP(S)
DOWN            :  0       STATIC LSP(S)
Name                FEC                I/O Label    I/O If                Status

RAtoRD              4.4.4.9/32         NULL/20      -/GE0/0/1             Up
```

Рис. 6.5. Пути MPLS

В поле total видим, что есть один LSP, а в поле UP – что он поднят.

2.7. Настроить LSP от LSRD к LSRA.

LSP должен быть двунаправленным. Для этого выполнить задания по пп. 2.3– 2.6, при этом источником будет LSRD, транзитным – LSRC, а конечным – LSRA:

[LSRD_Model]**static-lsp ingress RDtoRA destination 1.1.1.9 32 nexthop 10.4.1.1 out-label 30**

[LSRC_Model]**static-lsp transit RDtoRA incoming-interface gigabiteethernet0/0/2 in-label 30 nexthop 10.3.1.1 out-label 60**

[LSRD_Model]**static-lsp egress RDtoRA incoming-interface gigabiteethernet 0/0/2 in-label 60**

2.8. Проверить доступность LSP.

Нужно проверить, действительна ли конфигурация и доступен ли созданный LSP. Для этого достаточно «пропинговать» LSRA (рис. 6.6):

[LSRD_Model]**ping lsp ip 1.1.1.9 32**

```
[LSRD]ping lsp ip 1.1.1.9 32
  LSP PING FEC: IPV4 PREFIX 1.1.1.9/32/ : 100  data bytes, press CTRL_C to break
    Reply from 1.1.1.9: bytes=100 Sequence=1 time=270 ms
    Reply from 1.1.1.9: bytes=100 Sequence=2 time=90 ms
    Reply from 1.1.1.9: bytes=100 Sequence=3 time=60 ms
    Reply from 1.1.1.9: bytes=100 Sequence=4 time=60 ms
    Reply from 1.1.1.9: bytes=100 Sequence=5 time=40 ms

  --- FEC: IPV4 PREFIX 1.1.1.9/32 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 40/104/270 ms
```

Рис. 6.6. Проверка работоспособности пути (LSP)

2.9. Просмотреть информацию о статусе LSP на LSRD.

Чтобы узнать статус и подробную информацию LSP, воспользоваться следующей командой (для любого LSR), рис. 6.7:

[LSRD_Model]**display mpls static-lsp**

```
[LSRD]display mpls static-lsp
TOTAL          :  2       STATIC LSP(S)
UP             :  2       STATIC LSP(S)
DOWN           :  0       STATIC LSP(S)
Name               FEC                I/O Label    I/O If                Status

RAtoRD             -/-                40/NULL      GE0/0/1/-             Up

RDtoRA             1.1.1.9/32         NULL/30      -/GE0/0/2             Up
```

Рис. 6.7. Статус путей (LSP)

На рис. 6.7 показано, что подняты два LSP, но так как команда выполняется на LSRD, поле FEC на пути RAtoRD не заполнено (подумайте, почему так, попробуйте сделать то же самое на LSRA).

2.10. Просмотреть информацию о метках LSP на LSRD:

[LSRD_Model]**display mpls static-lsp verbose**

На рис. 6.8 показаны входящие и исходящие метки и интерфейсы и представлена подробная информация о LSP. На ее основе составить отчет о созданных LSP и их характеристиках.

```
[LSRD]display mpls static-lsp verbose
No              :  1
LSP-Name        :  RAtoRD
LSR-Type        :  Egress
FEC             :  -/-
In-Label        :  40
Out-Label       :  NULL
In-Interface    :  GigabitEthernet0/0/1
Out-Interface   :  -
NextHop         :  -
Static-Lsp Type:  Normal
Lsp Status      :  Up

No              :  2
LSP-Name        :  RDtoRA
LSR-Type        :  Ingress
FEC             :  1.1.1.9/32
In-Label        :  NULL
Out-Label       :  30
In-Interface    :  -
Out-Interface   :  GigabitEthernet0/0/2
NextHop         :  10.4.1.1
Static-Lsp Type:  Normal
Lsp Status      :  Up
```

Рис. 6.8. Параметры путей (LSP)

Лабораторная работа 7

РАЗЛИЧНАЯ МАРШРУТИЗАЦИЯ В ПРЯМОМ И ОБРАТНОМ НАПРАВЛЕНИЯХ MPLS

Цель лабораторной работы заключается в изучении использования различных путей LSP для передачи трафика в сети MPLS.

В результате выполнения лабораторной работы студент получит навык создания индивидуальных LSP-путей для передачи определенного трафика.

Таблица 7.1

Варианты заданий

Вариант	Терминал-отправитель (Cm)	IP-адрес терминала получателя	Маршрутизатор (1)	Интерфейс в сторону терминала	Маршрутизатор (2)	Интерфейс к следующему маршрутизатору	IP-адрес следующего маршрутизатора
1	1	10.0.13.13	1	eth2	2	eth1	10.0.1.2
2	2	10.0.14.14	2	eth3	3	eth2	10.0.3.3
3	3	10.0.15.15	3	eth2	4	eth3	10.0.4.4
4	3	10.0.16.16	3	eth2	4	eth3	10.0.4.4
5	4	10.0.11.11	4	eth3	5	eth1	10.0.6.4
6	5	10.0.12.12	5	eth4	1	eth1	10.0.2.5
7	6	10.0.11.11	6	eth1	5	eth3	10.0.7.6
8	5	10.0.11.11	5	eth4	6	eth3	10.0.7.5
9	2	10.0.13.13	2	eth3	4	eth4	10.0.9.4

Выполнение лабораторной работы

1. Открыть ярлык «Удаленная консоль», расположенный на рабочем столе.

Внимание! В процессе выполнения лабораторной работы размер окна «Удаленная консоль» изменять нельзя.

В открывшемся окне выбрать зону MPLS и номер терминала отправителя (Cm), соответствующий варианту задания из табл. 7.1.

Студентам с номерами вариантов 8 и 9 в открывшемся окне набрать команду:

```
sh add_link
```

Данная команда добавляет маршрут до терминала-получателя.

2. Всем бригадам ввести команду:

ping [IP-адрес терминала-получателя].

Соответствующий варианту IP-адрес терминала-получателя указан в табл. 7.1.

3. Запустить программу «WireShark на сервере», используя ярлык на рабочем столе. В открывшемся окне выбрать зону ***MPLS***. Далее указать

маршрутизатор (1), соответствующий номеру варианта из табл. 7.1, с которого будет осуществляться снятие трассировки (отлов пакетов). Номер маршрутизатора (Rm) также указан в табл. 7.1. В соответствии с вариантом задания выбрать интерфейс в сторону терминала (***eth1-4***), генерирующий запросы ***ping***.

4. Найти отправляемые пакеты, изучить их структуру и отметить на схеме отчета, используется ли на этом участке технология MPLS или иная (обозначить нужные участки стрелками с названием используемой технологии).

5. Далее в программе «WireShark на сервере» выбрать интерфейс к следующему маршрутизатору (2), соответствующему вашему варианту по табл. 7.1. Для этого в строке меню следует нажать ***Capture***, а затем выбрать пункт ***Interfaces***. В открывшемся окне указаны IP-адреса, которые соответствуют интерфейсам на маршрутизаторе и позволяют просмотреть маршрут.

Прежде чем выбрать интерфейс к следующему маршрутизатору (2), в правом верхнем углу нажать ***Stop,*** затем, изменив интерфейс согласно своему варианту, указанному в табл. 7.1, нажать ***Start***.

6. Повторить п. 4. Для поиска пакетов можно использовать фильтр, для этого в поле ***Filter*** надо ввести ***mpls***, а затем нажать ***Apply***.

7. Следует отличать свои пакеты от пакетов других бригад, используя ***Sourse IP*** и ***Destination IP.***

8. Закрыть программу «WireShark на сервере».

9. Запустить снова программу «WireShark на сервере», выбрать зону **MPLS** и указать маршрутизатор (2) на пути следования пакета. Номер маршрутизатора (Rm) указан в табл. 7.1.

Выбрать интерфейс к следующему маршрутизатору, соответствующий варианту задания. Далее повторить п. 4.

10. Закрыть программу «WireShark на сервере».

Сочетанием клавиш Ctrl + C остановить команду ping. Закрыть «Удаленную консоль».

11. Открыть ярлык «Удаленная консоль». В открывшемся окне выбрать зону **MPLS**. Затем указать маршрутизатор (1) согласно варианту задания, приведенному в табл. 7.1.

Студентам с номерами вариантов 1, 2, 4 и 6 ввести команду:

```
sh add_link
```

Данная команда добавляет маршрут до терминала-получателя.

12. Удалить существующий путь до терминала-получателя и добавить новый путь без MPLS. Для этого воспользоваться следующими командами:

ip route del 10.0.L.0/24

(где **10.0.L.0/24** – IP-адрес сети терминала-получателя),

ip route add 10.0.L.0/24 via 10.0.N.M dev ethY

(где **10.0.L.0/24** – IP-адрес сети терминала-получателя; **10.0.N.M** – IP-адрес следующего маршрутизатора (2); ***ethY*** – интерфейс на маршрутизаторе (1) в сторону маршрутизатора (2)).

Команда, используемая для просмотра нового пути до терминала:

ip route

13. Аналогично сделанному в пп. 2–11 просмотреть весь путь своего варианта задания и записать в отчет изменения.

Лабораторная работа 8

ПРОТОКОЛ РАСПРЕДЕЛЕНИЯ МЕТОК LDP (НА ОБОРУДОВАНИИ HUAWEI)

Цель лабораторной работы заключается в изучении протокола распределения меток LDP и его настройке на маршрутизаторах MPLS.

В результате выполнения лабораторной работы студент получит навык настройки MPLS с использованием протокола LDP на сетевом оборудовании Huawei.

Таблица 8.1

Варианты заданий

Вариант	Название	Настраиваемый интерфейс	LSR ID (IP-адрес маршрутизатора)	Интерфейсы к соседним устройствам	IP-адрес получателя (для ping)
1	Маршрутизатор NE40E-03	GigabitEthernet2/0/0	10.255.255.1	GigabitEthernet2/0/0 GigabitEthernet2/1/0	10.255.255.2
2	Маршрутизатор NE40E-03	GigabitEthernet2/1/0	10.255.255.1	GigabitEthernet2/0/0 GigabitEthernet2/1/0	10.255.255.3
3	Маршрутизатор NE40E-02	GigabitEthernet2/0/0	10.255.255.3	GigabitEthernet2/0/0 GigabitEthernet3/0/10 GigabitEthernet2/0/8	10.255.255.1
4	Маршрутизатор NE40E-02	GigabitEthernet3/0/10	10.255.255.3	GigabitEthernet2/0/0 GigabitEthernet3/0/10 GigabitEthernet2/0/8	10.255.255.4
5	Маршрутизатор NE40E-01	GigabitEthernet2/0/0	10.255.255.2	GigabitEthernet2/0/0 GigabitEthernet2/1/0 GigabitEthernet2/0/8	10.255.255.1
6	Маршрутизатор NE40E-01	GigabitEthernet2/1/0	10.255.255.2	GigabitEthernet2/0/0 GigabitEthernet2/1/0 GigabitEthernet2/0/8	10.255.255.4
7	Коммутатор S93-01	vlanif 777	10.255.255.4	GigabitEthernet2/0/0 GigabitEthernet2/1/0	10.255.255.2
8	Коммутатор S93-01	vlanif 888	10.255.255.4	GigabitEthernet2/0/0 GigabitEthernet2/1/0	10.255.255.3

Выполнение лабораторной работы

1. На рабочем столе открыть ярлык «Удаленная консоль». Выбрать имитационную зону ***Huawei***, затем выбрать устройство (рис. 8.1) согласно варианту задания из табл. 8.1.

2. Перейти в режим конфигурации интерфейсов. Для этого ввести команду:

```
<NE40E-03>system-view
[NE40E-03]
```

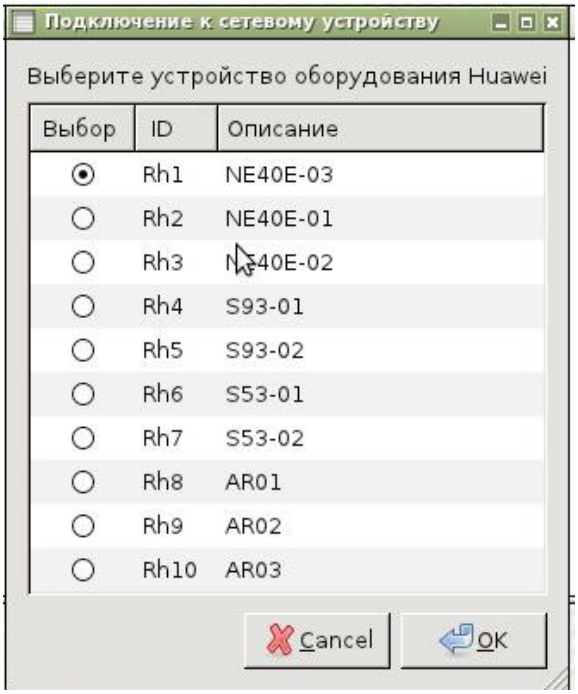


Рис. 8.1. Выбор устройства

3. Для запуска MPLS сначала задать IP-адрес для MPLS LSR:

[NE40E-03] **mpls lsr-id A.B.C.D.**

(где ***A.B.C.D.*** – LSR ID, берется согласно варианту задания из табл. 8.1).

Подключить MPLS глобально. Для этого ввести команду:

[NE40E-03] **mpls**

Для выхода из настроек MPLS ввести: ***quit***

Далее включить протокол LDP, используя команду:

[NE40E-03] **mpls ldp**

Для выхода из настроек протокола использовать команду: ***quit***

Для просмотра текущей конфигурации устройства использовать команду:

[NE40E-03] **display current-configuration**

Воспользоваться выводом команды, который показан на рис. 8.2, чтобы убедиться, что на устройстве используется технология MPLS.

Кроме того, если необходимо, можно посмотреть список интерфейсов, их идентификаторов и настроенных на них IP-адресов командой:

[NE40E-03] **display ip interface brief**

Нарисовать схему сетевого окружения оборудования по полученному варианту в табл. 8.1 и согласовать действующие или настраиваемые в будущем IP-адреса с другими бригадами. Отметьте IP-адреса и номера интерфейсов на схеме. В случае если IP-адрес уже задан на настраиваемом

интерфейсе и соответствует плану, повторно его настраивать в п. 4.2 не нужно. Однако в п. 4.2 следует включить mpls и mpls ldp.

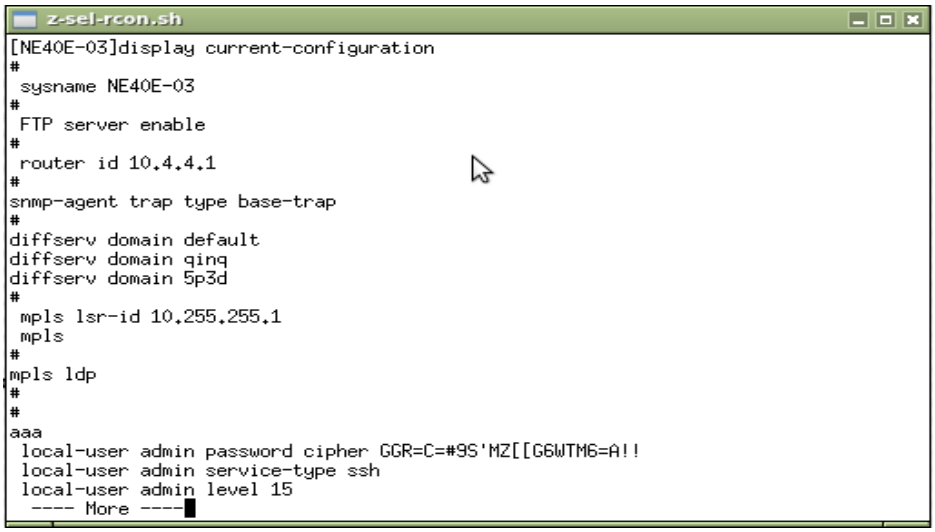


Рис. 8.2. Просмотр текущей конфигурации устройства

4. Провести настройку интерфейса. Для этого ввести серию команд:

4.1. (*Пункт выполняется только при настройке на коммутаторе S93 или S53*). Для последующей задачи IP-адреса настроить порты к смежным сетевым устройствам на использование VLAN:

[S93-01] **vlan ID-vlan**

(где ID-VLAN – это номер VLAN из табл. 8.1, например 777 для варианта 7);

[S93-01-vlan111] **port ID-интерфейса**

(где **ID интерфейса** соответствует идентификатору порта/интерфейса на данном устройстве, например, «***GigabitEthernet 2/0/0»***, ведущего к соседним устройствам из табл. 8.1);

[S93-01-vlan111]**quit**
[S93-01] **interface** ID-интерфейса

(где **ID-интерфейса** соответствует идентификатору порта/интерфейса на данном устройстве, например «***GigabitEthernet 2/0/0»***, ведущего к соседним устройствам из табл. 8.1);

[S93-01-GigabitEthernet2/0/0] **port link-type access**

4.2. Для обеспечения связи на сетевом уровне на выбранных портах нужно настроить IP-адреса вводом следующих команд:

[NE40E-03] interface ID-интерфейса

(где **ID-интерфейса** для маршрутизатора соответствует идентификатору порта/интерфейса на данном устройстве, например «***GigabitEthernet 2/0/0»***,

а для коммутатора – идентификатору логического интерфейса для определенной виртуальной локальной сети (VLAN), например «***vlanif 777***», где 777 соответствует номеру VLAN**.**

Настроить IP-адрес на интерфейсе командой:

[NE40E-03-GigabitEthernet2/0/0] ip address IP-адрес 24

(где **IP-адрес** указывается в соответствии с табл. 8.1).

4.3. Для включения технологии MPLS на интерфейсе необходимо применить команду:

[NE40E-03-GigabitEthernet2/0/0] mpls

Следующим шагом задать использование протокола LDP на интерфейсе командой:

[NE40E-03-GigabitEthernet2/0/0] **mpls ldp**

Выйти из режима конфигурации интерфейса командой:

[NE40E-03-GigabitEthernet2/0/0] **quit**

5. Проверку MPLS LDP осуществить командой (рис. 8.3):

[NE40E-03] **display mpls ldp**

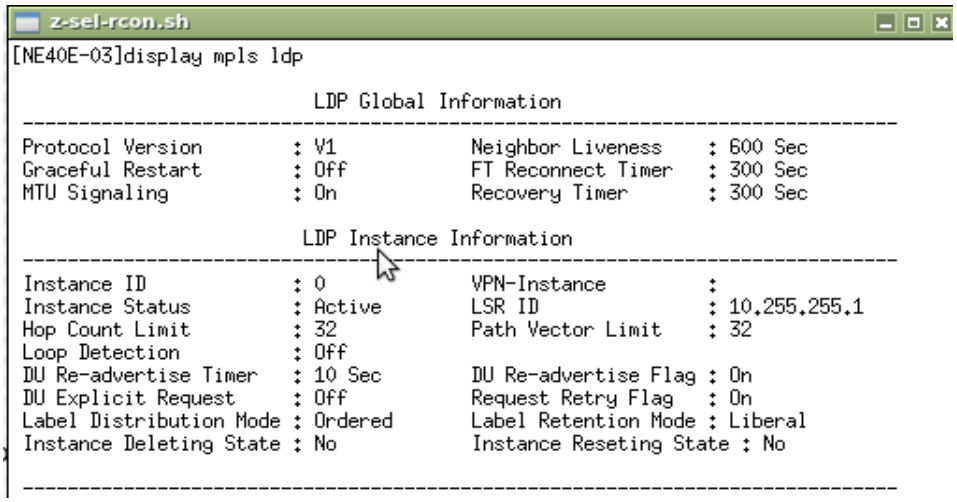


Рис. 8.3. Проверка MPLS LDP

Проверку состояния интерфейсов, на которых используется MPLS, осуществить командой:

[NE40E-03] **display mpls interface**

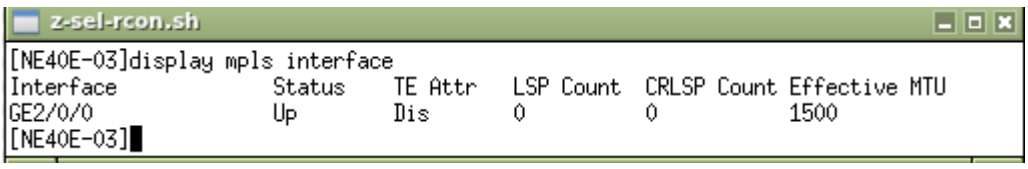


Рис. 8.4. Вывод команды display mpls interface

В случае если данные об использовании MPLS на интерфейсе не выводятся, проверить, как выполнен п. 4.

Проверка доступности соседних MPLS-маршрутизаторов осуществляется командой :

[NE40E-03] display mpls ldp peer

Далее проверить соединение с другим устройством с помощью команды:

[NE40E-03] ping lsp ip A’.B’.C’.D’ **24**

(где **A’.B’.C’.D’** – IP-адрес получателя).

6. Отключить использование MPLS и протокола LDP на интерфейсе. Для этого в режиме конфигурации интерфейса ввести команды:

[NE40E-03-GigabitEthernet2/0/0] **undo mpls**
[NE40E-03-GigabitEthernet2/0/0] **undo mpls ldp**

Бригады 1, 3, 5, 7 должны отключить использование MPLS на устройствах глобально и MPLS LSR. Для этого ввести команды:

[NE40E-03] **undo mpls**
[NE40E-03] **undo mpls lsr**

Лабораторная работа 9

ПРОТОКОЛ ДВУНАПРАВЛЕННОГО ОБНАРУЖЕНИЯ ОШИБОК ПРОДВИЖЕНИЯ BFD В MPLS (НА ОБОРУДОВАНИИ HUAWEI)

Цель лабораторной работы заключается в изучении протокола обнаружения ошибок BFD и его использования в MPLS-сетях.

В результате выполнения лабораторной работы студент получит навык настройки BFD на сетевом оборудовании Huawei для его использования в MPLS-сетях.

Протокол двунаправленного обнаружения ошибок продвижения (Bidirectional Forwarding Detection – BFD) разработан как более простая альтернатива протоколу LSP Ping для постоянного мониторинга состояния пути LSP.

Такой постоянный мониторинг требуется для определения отказа на основном пути, для своевременного переключения на резервный путь. Такой механизм должен быстро выявлять отказ, но не перегружать сеть тестовыми сообщениями. Например, протокол LSP Ping постоянно тестирования состояния пути путем периодической отправки сообщений Echo Requst. Однако их обработка трудоемка, так как требует сравнения значения FEC в каждом запросе со значением из базы данных. Протокол BFD проще, чем LSP Ping, но не способен локализовать отказавший элемент сети.

Выполнение лабораторной работы

1. Создать сеть с топологией, приведенной на рис. 9.1.

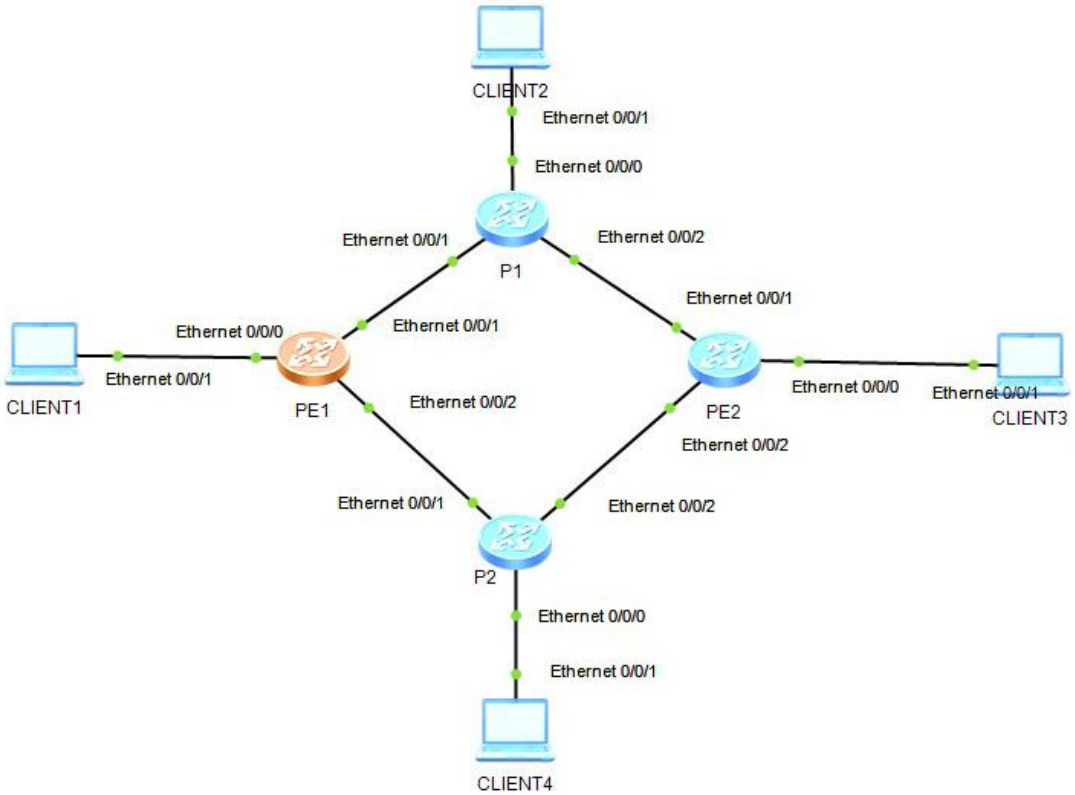


Рис. 9.1. Топология сети MPLS

Таблица IP-адресов на интерфейсах маршрутизаторов (табл. 9.1) соответствует схеме рис. 9.1.

Таблица 9.1

Настройка IP-адресов

Маршрутизатор	Интерфейс	IP-адрес/маска подсети
PE1	Ethernet 0/0/0	1.1.1.9/30
	Ethernet 0/0/1	10.1.1.1/30
	Ethernet 0/0/2	10.1.2.1/30
PE2	Ethernet 0/0/0	4.4.4.9/30
	Ethernet 0/0/1	10.1.5.1/30
	Ethernet 0/0/2	10.1.4.1/30
P1	Ethernet 0/0/0	2.2.2.9/30
	Ethernet 0/0/1	10.1.1.2/30
	Ethernet 0/0/2	10.1.5.2/30
P2	Ethernet 0/0/0	3.3.3.9/30
	Ethernet 0/0/1	0.1.2.2/30
	Ethernet 0/0/2	10.1.4.2/30

2. Для того чтобы попасть в консоль маршрутизатора LSR_A, необходимо два раза нажать на него левой кнопкой мыши.

Для удобства дальнейшей настройки маршрутизатора отключить терминальные сообщения командой:

<Huawei> **undo terminal monitor**

Для перехода в режим системных настроек ввести команду:

<Huawei>**system view**

Для удобства работы в консоли с несколькими маршрутизаторами задать имя маршрутизатора командой:

[Huawei]**sys PE1**

3. Далее для настройки ip-адресов на соответствующих интерфейсах перейти к настройке необходимого интерфейса (например, Ethernet 0/0/0) командой:

[PE1]**interface Ethernet 0/0/0**

В режиме настройки интерфейса задать соответствующий ему по табл. 1 IP-адрес и маску сети командой:

[PE1-Ethernet0/0/0]**ip address 1.1.1.9 255.255.255.0**

Для настройки следующего интерфейса покинуть данный интерфейс с помощью команды:

[PE1-Ethernet0/0/0]**quit**

Таким образом необходимо настроить все оставшиеся интерфейсы и маршрутизаторы в соответствии с табл. 8.1 и заданной топологией сети на рис. 8.1.

4. Настроить MPLS LDP на маршрутизаторах.

Перейти к системным настройкам маршрутизатора P1 командой:

```
<P1> system view
```

Задание адреса для MPLS LSR с помощью команды:

```
[P1]mpls lsr-id 2.2.2.9
```

Подключить опцию MPLS на данном маршрутизаторе глобально командой:

```
[P1]mpls
```

Покинуть режим глобальной настройки MPLS командой:

```
[P1-mpls]q
```

Далее настроить MPLS непосредственно на интерфейсах, войти в режим настройки интерфейса командой:

```
[P1]interface Ethernet 0/0/1
```

Подключить MPLS на данном интерфейсе командой:

```
[P1-Ethernet0/0/1]mpls
```

Выйти из режима настройки интерфейса командой:

```
[P1-Ethernet0/0/1]quit
```

Аналогично подключить MPLS на интерфейсе Ethernet 0/0/2 данного маршрутизатора, а также подключить MPLS на интерфейсах оставшихся маршрутизаторов.

5. Подключить протокол LDP.

Перейти к режиму настройки командой:

```
<P1>system view
```

Подключить на маршрутизаторе протокол BFD на маршрутизаторе командой:

[P1]mpls ldp – подключение протокола LDP

Подключить протокол BFD командой:

```
[P1]bfd
```

Покинуть режим настройки командой:

```
[P1-bfd]quit
```

6. С помощью следующей команды задать параметры BFD сессии для динамического LSP интерфейса Ethernet 0/0/2:

[P1]**bfd lto4 bind ldp-lsp peer-ip 3.3.3.9 nexthope 10.1.5.1 interface Ethernet 0/0/2**

Аналогично для интерфейса Ethernet0/0/1 задать параметры BFD сессии:

[P1]**bfd lto4 bind ldp-lsp peer-ip 3.3.3.9 nexthop 10.1.1.1 interface Ethernet 0/0/1**

Протокол BFD является однонаправленным. Активировать прием прямой и обратной связи командами:

[P1-bfd-lsp-session-lto4]**discriminator local 1** – активация исходящего сигнала
[P1-bfd-lsp-session-lto4]**discriminator remote 2** – разделение входящего сигнала

Изменить статус интерфейса в таблице состояний LDP:

[P1-bfd-lsp-session-lto4]**process-pst**

Запустить конфигурацию сессии командой:

[P1-bfd-lsp-session-lto4]**commit**

Выйти из режима настройки командой:

[P1-bfd-lsp-session-lto4]**quit**

7. Для P2 выполнить следующие действия:
– подключить протокол BFD командой:

[P2]**bfd**

– покинуть режим настройки с помощью команды:

[P1 -mpls-ldp]**quit**

– задать имя удаленного маршрутизатора для LDP сессии командой:

[P1]**mpls ldp remote-peer P2**

– задать IP-адрес удаленного маршрутизатора командой:

[P1-mpls-ldp-remote-lsrc]**remote-ip 3.3.3.9**

– покинуть режим настройки с помощью команды:

[P1-mpls-ldp-remote-lsrc]**quit**

Аналогично для P2 подключить MPLS на маршрутизаторах PE1, PE2 с учетом значений IP-адресов из табл. 8.1.

8. Подключить протокол BFD. Для P2 выполнить следующие дйствия:
– задать ip-адрес удаленного маршрутизатора с помощью команды:

[P2]**bfd 4lot bind peer-ip 2.2.2.9**

– активировать прием прямой и обратной связи:

[P2-bfd-session-4lot]**discriminator local 2**
[P2-bfd-session-4lot]**discriminator remote 1**

– запустить конфигурацию командой:

[P2-bfd-session-4lot]**commit**

– покинуть режим настройки:

[P2-bfd-session-4lot]**q**

9. Подключить протокол OSPF командой:

[P1]**ospf 1**

Дальнейшими командами подключить сети, в которых будет использован данный протокол:

[P1-ospf-1]**area 0.0.0.0**
[P1-ospf-1-area-0.0.0.0]**network 2.2.2.9 0.0.0.255**
[P1-ospf-1-area-0.0.0.0]**network 10.1.5.0 0.0.0.3**
[P1-ospf-1-area-0.0.0.0]**network 10.1.1.0 0.0.0.3**
[P1-ospf-1-area-0.0.0.0]**quit**
[P1-ospf-1]**quit**

Аналогично подключить протокол OSPF на остальных маршрутизаторах с учетом используемых сетей.

10. Произвести вывод информации об установленных сессиях протокола BFD (рис. 9.2) с помощью команды:

[P2]**display bfd session all verbose**

Выписать основные параметры в соответствии с бланком.

```
[P2]display bfd session all verbose
--------------------------------------------------------------------------------
Session MIndex : 256        (Multi Hop) State : Down      Name : 4lot
--------------------------------------------------------------------------------
  Local Discriminator     : 2                 Remote Discriminator    : 1
  Session Detect Mode     : Asynchronous Mode Without Echo Function
  BFD Bind Type           : Peer IP Address
  Bind Session Type       : Static
  Bind Peer IP Address    : 2.2.2.9
  Bind Interface          : -
  Track Interface         : -
  FSM Board Id            : 0                 TOS-EXP                 : 7
  Min Tx Interval (ms)    : 1000              Min Rx Interval (ms)    : 1000
  Actual Tx Interval (ms) : 2100              Actual Rx Interval (ms) : 2100
  Local Detect Multi      : 3                 Detect Interval (ms)    : -
  Echo Passive            : Disable           Acl Number              : -
  Destination Port        : 3784              TTL                     : 254
  Proc Interface Status   : Disable           Process PST             : Disable
  WTR Interval (ms)       : -                 Local Demand Mode       : Disable
  Active Multi            : -
  Last Local Diagnostic   : No Diagnostic
  Bind Application        : No Application Bind
  Session TX TmrID        : 1033              Session Detect TmrID    : -
  Session Init TmrID      : -                 Session WTR TmrID       : -
  Session Echo Tx TmrID   : -
  PDT Index               : FSM-0 | RCV-0 | IF-0 | TOKEN-0
  Session Description     : -
--------------------------------------------------------------------------------

    Total UP/DOWN Session Number : 0/1
```

Рис. 9.2. Анализ формата пакетов BFD

11. На панели инструментов нажать левой кнопкой мыши два раза на значок «capture data» (рис. 9.3).

Рис. 9.3. Панель инструментов

Выбрать P1 и Ethernet 0/0/1 (рис. 9.4), запустить Wireshark.

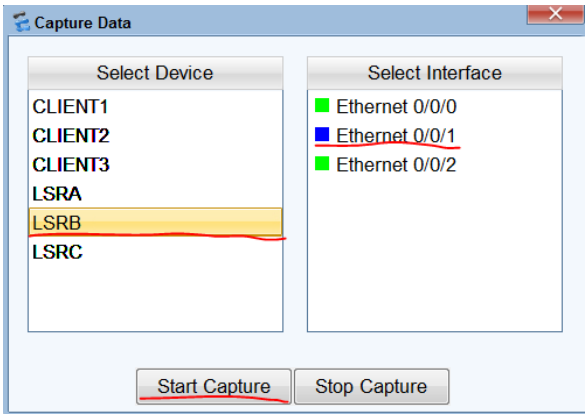


Рис. 9.4. Окно программы

В Wireshark найти пакеты передачи BFD (рис. 9.5).

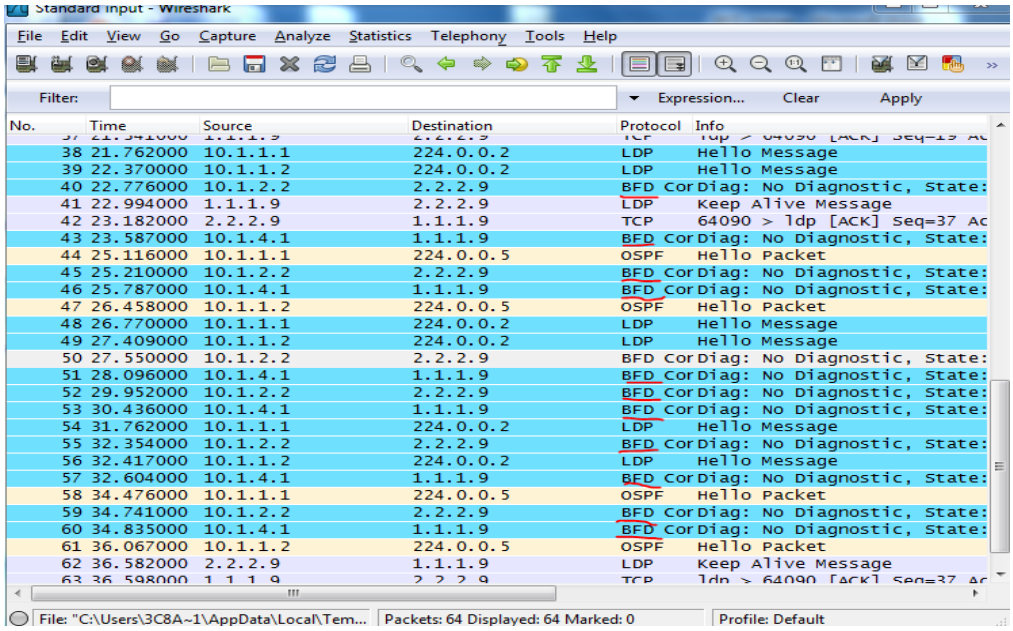


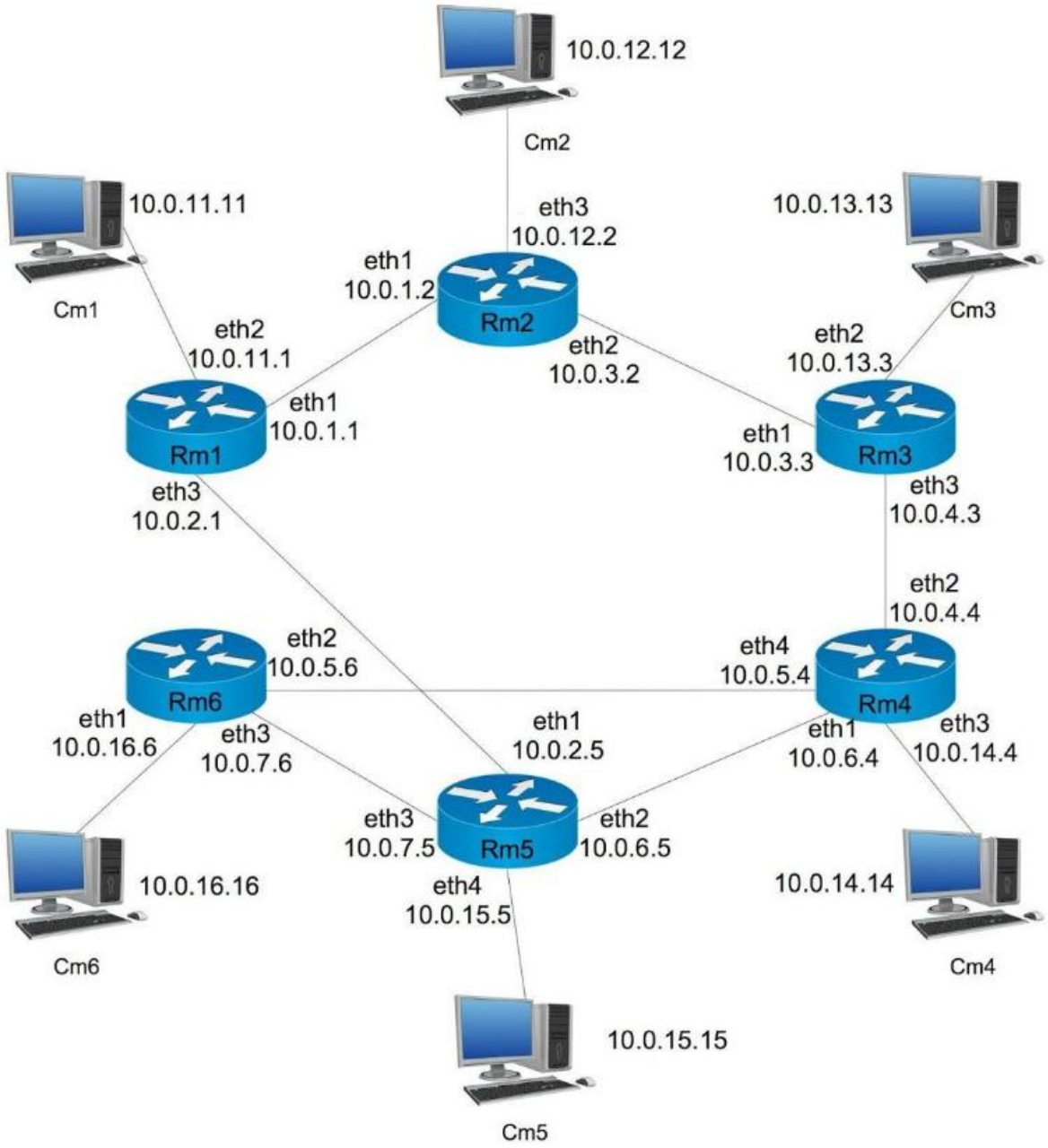
Рис. 9.5. Пакеты протоколов OSPF, LDP, BFD

В отчете записать:

1) для чего нужен протокол BFD;
2) какие поля встречаются в пакетах BFD;
3) зачем используется протокол OSPF при настройке MPLS.

Приложение 1

СХЕМА MPLS



Приложение 2

СКРИПТ ПЕРЕХОДА НА РЕЗЕРВНЫЙ МАРШРУТ И ВОЗВРАЩЕНИЕ НА ОСНОВНОЙ МАРШРУТ

Пример скрипта (Rm6) с пояснениями (для лабораторной работы 4)

df=1 – используется основной маршрут

while ["1" = "1"] ; – бесконечный цикл

do

sleep 0.0001 – пауза между циклами (может заменить фразу цикл)

st=`sudo ping -c 1 -I eth2 -w 0.05 -s 1 10.0.5.4 | grep "100% packet loss\|Host Unreacable"` – проверка состояния линии, для этого посылается 1 запрос ping с интерфейса eth2 размером 1 байт, время ожидания ответа 50 мс (минимальный размер пакета необходим, чтобы увеличить скорость его прохождения и не «загружать» сеть; время ожидания ответа минимально, чтобы в кратчайшие сроки суметь обнаружить неисправность), поиск в выводе команды фразы "100% packet loss\|Host Unreacable", которая появляется, если ответ на запрос не будет получен

if [! -z "$st"] ; then – если фраза найдена (т. е. линия недоступна)

if [$df = 1] ; then – и используется основной маршрут, тогда

df=0 ; – основной маршрут недоступен, необходимо использование резервного маршрута

echo Link down – alternative route – вывод сообщения о переходе на резервный маршрут

ip route del 10.0.14.0/24 – удаление основного маршрута

ip route add 10.0.14.0/24 via 10.0.7.5 dev eth3 mpls 0x7 – добавление резервного маршрута

fi – (пусто) когда недоступен основной маршрут и установлен резервный, никаких изменений не производится

fi

if [-z "$st"] ; then – если фраза не найдена

if [$df = 0] ; then – и если используется резервный маршрут

df=1 ; – основной маршрут доступен, необходимо выполнить переход на него

echo Link up – default route – вывод сообщения о переходе на основной маршрут

ip route del 10.0.14.0/24 – удаление резервного маршрута

ip route add 10.0.14.0/24 via 10.0.5.4 mpls 0x3 – добавление основного маршрута

fi – (пусто) когда доступен основной маршрут и установлен основной, никаких изменений не производится

fi

done

Список литературы

1. *Гольдштейн, А. Б.* Технология и протоколы MPLS / А. Б. Гольдштейн, Б. С. Гольдштейн. – СПб. : BHV, 2005. – ISBN 5-8206-0126-2.

2. *Гольдштейн, А. Б.* Транспортные сети IP/MPLS. Технология и протоколы : учеб. пособие / А. Б. Гольдштейн, А. В. Никитин, А. А. Шкрыль ; СПбГУТ. – СПб., 2016. – ISBN 978-5-8-160-129-1.

Содержание

Гольдштейн Александр Борисович
Никитин Алексей Владимирович
Шкрыль Александр Александрович
Фицов Вадим Владленович

ТРАНСПОРТНЫЕ СЕТИ IP/MPLS

Технология и протоколы

Лабораторный практикум

Редактор *И. И. Щенсняк*
Компьютерная верстка *Н. А. Ефремовой*

План издания 2016 г., п. 31 б

Подписано к печати 06.04.2016
Объем 4,0 усл.-печ. л. Тираж 30 экз. Заказ 639
Редакционно-издательский отдел СПбГУТ
191186 СПб., наб. р. Мойки, 61

Отпечатано в СПбГУТ