Министерство образования Республики Беларусь
Учреждение образования
«Белорусский государственный университет
информатики и радиоэлектроники»

Факультет информационной безопасности

Кафедра защиты информации

Е. С. Белоусова

МАСШТАБИРОВАНИЕ ЛОКАЛЬНЫХ СЕТЕЙ. БЕЗОПАСНОСТЬ МЕЖДОМЕННОЙ МАРШРУТИЗАЦИИ. ЛАБОРАТОРНЫЙ ПРАКТИКУМ

Рекомендовано УМО по образованию в области информатики и радиоэлектроники в качестве учебно-методического пособия для специальности 1-98 01 02 «Защита информации в телекоммуникациях»

Минск БГУИР 2025

УДК 004.732(076.5)
ББК 32.973.202я73
Б43

Р е ц е н з е н т ы:

кафедра телекоммуникационных систем
учреждения образования
«Белорусская государственная академия связи»
(протокол № 7 от 17.01.2023);

заместитель генерального директора по науке
государственного научного учреждения
«Объединенный институт проблем информатики
Национальной академии наук Беларуси»
кандидат технических наук, доцент С. Н. Касанин

Белоусова, Е. С.

Б43 Масштабирование локальных сетей. Безопасность междоменной маршрутизации. Лабораторный практикум : учеб.-метод. пособие / Е. С. Белоусова. – Минск : БГУИР, 2025. – 132 с. : ил.

ISBN 978-985-543-724-7.

Состоит из восьми лабораторных работ, содержащих краткие теоретические сведения, описание хода выполнения лабораторного задания, вопросы для самоконтроля, ответы на которые оцениваются программной экспертной системой.

Предназначено для студентов, изучающих дисциплину «Защита информационных сетей».

УДК 004.732(076.5)
ББК 32.973.202я73

ISBN 978-985-543-724-7

СОДЕРЖАНИЕ

ЛАБОРАТОРНАЯ РАБОТА № 1
КОММУТАТОРЫ L3. ПРОТОКОЛ STP

Цель: изучить различия коммутаторов L2 и L3, версий протокола STP, овладеть навыками конфигурирования коммутаторов L3.

1.1 Теоретическая часть

Агрегирование, или агрегация, каналов (Link Aggregation) – технология, которая позволяет объединить несколько физических каналов в один логический. Такое объединение позволяет увеличивать пропускную способность и надежность канала. Агрегирование каналов может быть настроено между двумя коммутаторами, коммутатором и маршрутизатором [1].

Все избыточные связи в одном агрегированном канале остаются в рабочем состоянии, а имеющийся трафик распределяется между ними для достижения балансировки нагрузки. При отказе одной из линий, входящих в такой логический канал, трафик распределяется между оставшимися линиями.

Агрегирование каналов позволяет решить две задачи: повысить пропускную способность канала и обеспечить резерв на случай выхода из строя одного из каналов.

Большинство технологий агрегирования позволяют объединять только параллельные каналы, которые начинаются на одном и том же устройстве и заканчиваются на другом (рисунок 1.1). Если рассматривать избыточные соединения между коммутаторами, то без использования специальных технологий для агрегирования каналов передаваться данные будут только через один интерфейс. На рисунке 1.1 треугольником обозначены включенные порты коммутаторов, а кругом – выключенные. Такой вариант позволяет обеспечить резервирование каналов, но не дает возможности увеличить пропускную способность.

Технологии агрегирования каналов позволяют использовать все интерфейсы одновременно. При этом устройства контролируют распространение широковещательных кадров, предотвращая зацикливание и образование петли.

Петля коммутации (Bridging Loop, Switching Loop) – состояние в сети, при котором происходит бесконечная пересылка фреймов между коммутаторами, подключенными к одному и тому же сегменту сети. Например, если отправляется пакет ICMP с одного компьютера на другой, как правило, перед началом отправки необходимо узнать MAC-адрес получателя. Для этого создается ARP-пакет, который отправляется на все порты коммутатора, кроме исходящего.

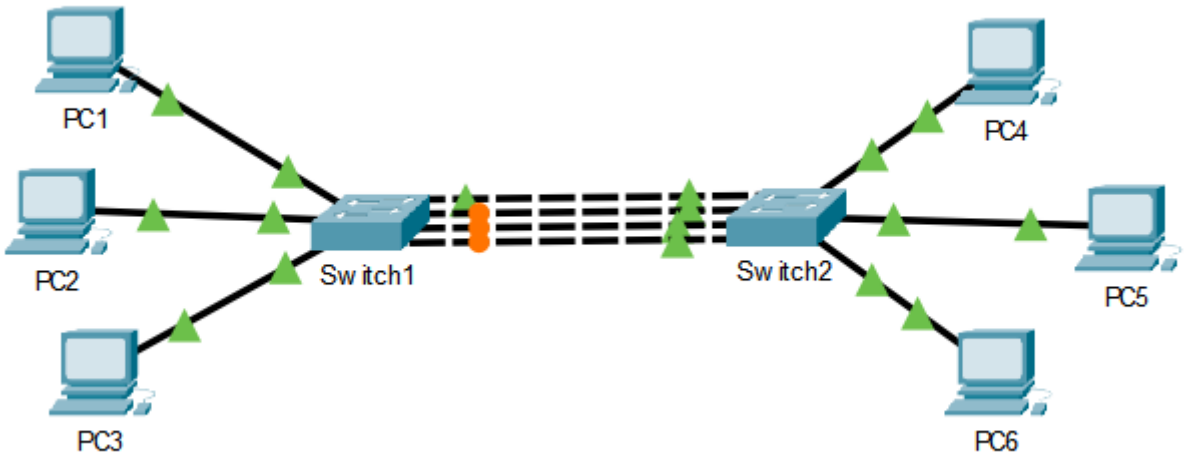

Рисунок 1.1 – Использование параллельных каналов
для соединения коммутаторов

Коммутатор, который получит данный пакет, также отправит его на другие порты. Полученный ARP будет отправлен на тот порт, с которого пришел первый ARP, т. к. он получен с другого порта и отдельным ARP-пакетом – для коммутатора это два разных кадра, и обрабатываются они независимо друг от друга. Первый коммутатор повторит действия, что приведет к образованию петли и перегрузке коммутатора. Следовательно, чем больше коммутаторов участвует в передаче, тем больше кадров будут создано, что приведет к быстрому отказу сети.

Предположим, что сеть Building1, представленную на рисунке 1.2, необходимо расширить, поэтому в сеть добавляется коммутатор Switch9, при этом резервируются каналы между коммутаторами Switch9 и Switch3. Если с компьютера PC20 будет отправлен ICMP-пакет, то сначала будет создан ARP-пакет, который будет пересылаться постоянно между коммутаторами Switch9 и Switch3, что приведет к перегрузке сети. Чтобы этого избежать, коммутатор при получении широковещательного фрейма через обычный интерфейс должен отправлять его в агрегированный канал только через один интерфейс. А при получении широковещательного фрейма из агрегированного канала не должен отправлять его назад.

При построении компьютерных сетей должны использоваться параллельные каналы между коммутаторами в целях агрегации и резервирования. Однако резервные каналы усложняют топологию и без должного управления могут привести к проблемам с подключением. Для управления резервными каналами необходимо реализовать такие протоколы и технологии, как протоколы STP и EtherChannel.

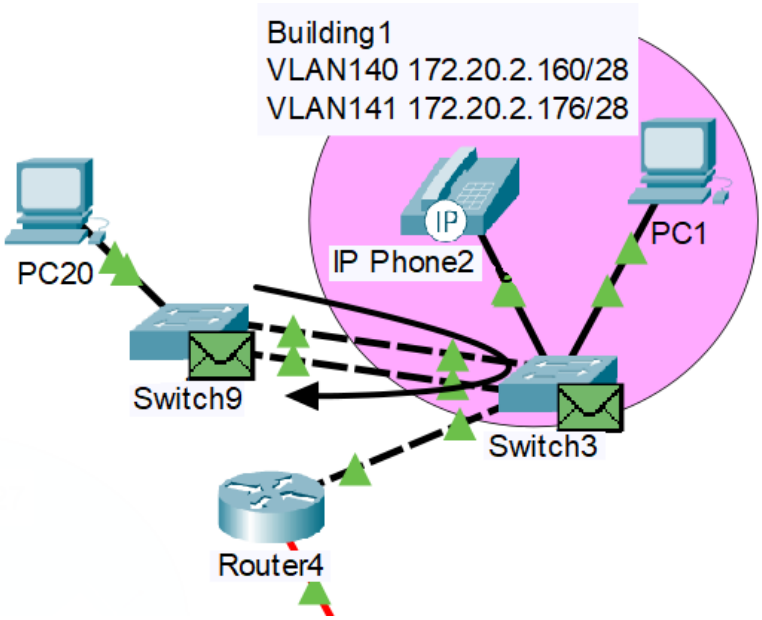

Рисунок 1.2 – Возникновение петли коммутации

STP (**Spanning Tree Protocol**) – сетевой протокол канального уровня, предназначенный для автоматического удаления циклов (петель коммутации) из топологии сети на канальном уровне в Ethernet-сетях [2].

Протокол STP делает топологию избыточной на физическом уровне, но при этом позволяет логически блокировать петли. Достигается это с помощью того, что STP отправляет сообщения BPDU и обнаруживает фактическую топологию сети, а затем, определяя роли коммутаторов и портов, часть портов блокирует так, чтобы в итоге получить топологию без петель.

Для того чтобы определить, какие порты будут заблокированы, а какие будут передавать данные, STP выполняет следующие действия:

– выбор корневого моста (Root Bridge);

– определение корневых портов (Root Port);

– определение выделенных (обозначенных) портов (Designated Port).

Для обмена информацией между собой коммутаторы используют специальные пакеты, называемые BPDU (Bridge Protocol Data Units). Пакеты BPDU бывают двух видов: конфигурационные (Configuration BPDU) и в виде уведомлений TCN (Topology Change Notification BPDU). Первые регулярно рассылаются корневым коммутатором (и ретранслируются остальными) и используются для построения топологии, вторые отсылаются в случае изменения топологии сети (при подключении/отключении устройств). Конфигурационные BPDU содержат несколько полей (рисунок 1.3) [3]:

– идентификатор протокола (Protocol Identifier) – 2-байтовое поле, равное нулю;

– версия STP-протокола (Protocol Version Identifier) – поле размером в 1 байт, значение которого равно нулю;

– тип BPDU (BPDU type) – 1 байт, который принимает значение «0», если это конфигурационный BPDU (CBPDU), или «1», если это TCN BPDU;

– флаги (Flags) – поле, в котором используется 1 байт для отображения изменения топологии (бит «1») и при подтверждении топологии (бит «8»);

– идентификатор корневого моста (Root Identifier) – поле, содержащее информацию о корневом коммутаторе, а именно его приоритет и MAC-адрес;

– расстояние до корневого моста (Root Path Cost) – поле, содержащее суммарную стоимость до корневого коммутатора, указывающую на скорость передачи (таблица 1.1);

– идентификатор моста (Bridge Identifier) – поле, содержащее данные (приоритет и MAC-адрес) коммутатора, который отправляет пакет;

– идентификатор порта (Port Identifier) – поле, содержащее идентификатор порта коммутатора, с которого отправляется данный пакет;

– время жизни сообщения (Message Age) – поле, содержащее временной интервал (в секундах), который необходим, чтобы распознать устаревшие кадры и удалить их. Его формирует корневой коммутатор и устанавливает в первоначальное значение «0». Далее каждый последующий коммутатор увеличивает это значение на время задержки. Как только это значение превысит максимальное пороговое значение, оно будет отброшено;

– максимальное время жизни сообщения (Max Age) – поле, отвечающее за максимальное время жизни, превысив которое, коммутатор отбрасывает кадр;

– время приветствия (Hello Time) – временной интервал, через который коммутатор посылает BPDU кадры (по умолчанию 2 секунды);

– задержка смены состояний (Forward Delay) – временной интервал, указывающий, сколько секунд порт коммутатора будет находиться в состоянии прослушивания и обучения.

CBPDU (Configuration Bridge Protocol Data Unit) – кадр, используемый для вычисления связующего дерева, когда значение поля «Тип BPDU» равно нулю.

TCNBPDU (Topology Change Notification Bridge Protocol Data Unit) – кадр, используемый для уведомления других об изменениях в топологии, когда значение поля «Тип BPDU» равно 1. Если в сети произошло какое-то изменение в топологии, коммутатор отправляет пакет BPDU со значением «1» в поле «Тип BPDU», далее будут отправляться пакеты BPDU со значением «0», чтобы заново перестроить дерево.

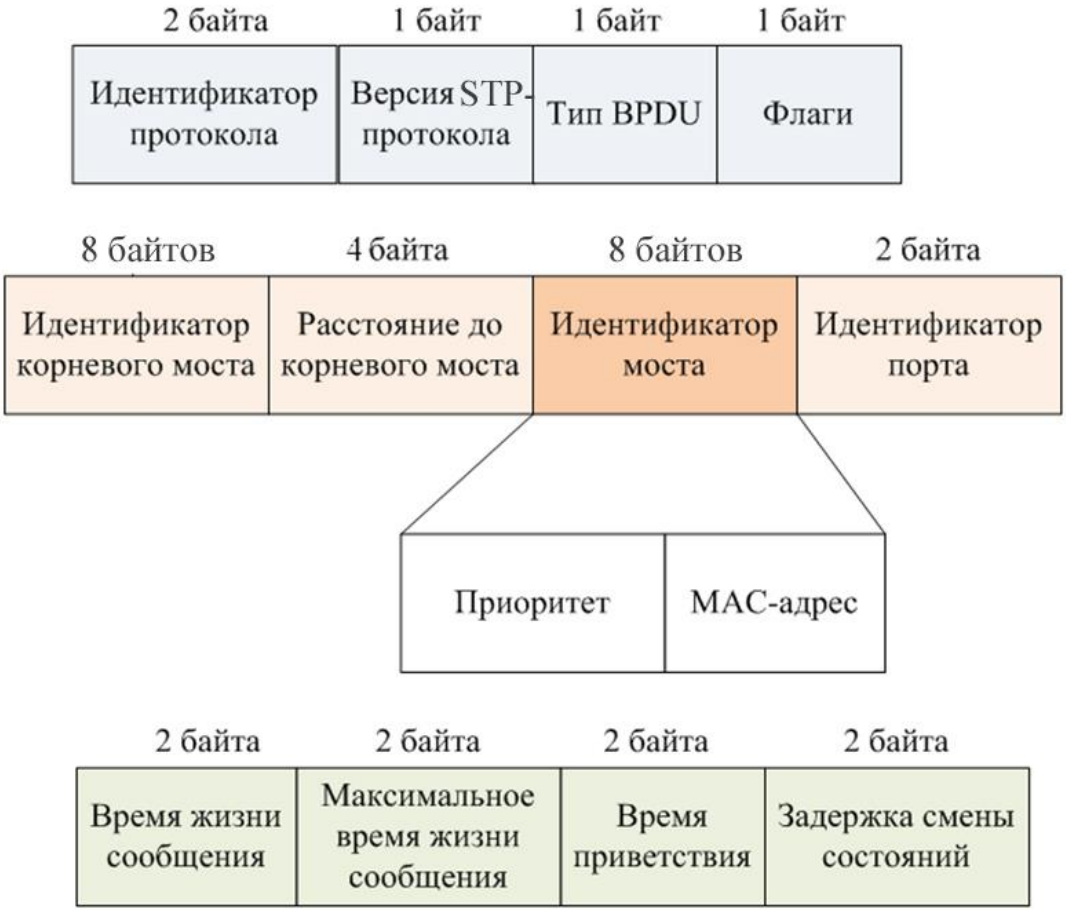

Рисунок 1.3 – Формат данных BPDU

Таблица 1.1 – Соответствие скорости канала и его стоимости

Скорость канала	Стоимость
10 Гбит/с	2
1 Гбит/с	4
100 Мбит/с	19
10 Мбит/с	100

Рассмотрим пример построения сети с использованием протокола STP (рисунок 1.4). В большинстве сетей Ethernet оконечные устройства, как правило, подключаются к коммутатору LAN второго уровня по принципу «точка – точка».

Коммутатор LAN второго уровня (L2) осуществляет коммутацию и фильтрацию только на основе MAC-адреса канального уровня модели OSI [4]. Коммутатор полностью прозрачен для сетевых протоколов и пользовательских приложений. Коммутатор L2 создает таблицу MAC-адресов, которую в дальнейшем использует для принятия решений о пересылке пакетов. В процессе передачи данных между независимыми IP-подсетями коммутаторы L2 полагаются на маршрутизаторы.

Коммутатор третьего уровня (L3) функционирует подобно коммутатору L2, но вместо использования только одного MAC-адреса второго уровня для принятия решений о пересылке коммутатор L3 может также использовать IP-адрес. Вместо того чтобы определять, какие MAC-адреса связаны с каждым из его портов, коммутатор третьего уровня может также установить, какие IP-адреса связаны с его интерфейсами. Это позволяет коммутатору L3 перенаправлять трафик по сети, в том числе используя данные об IP-адресе.

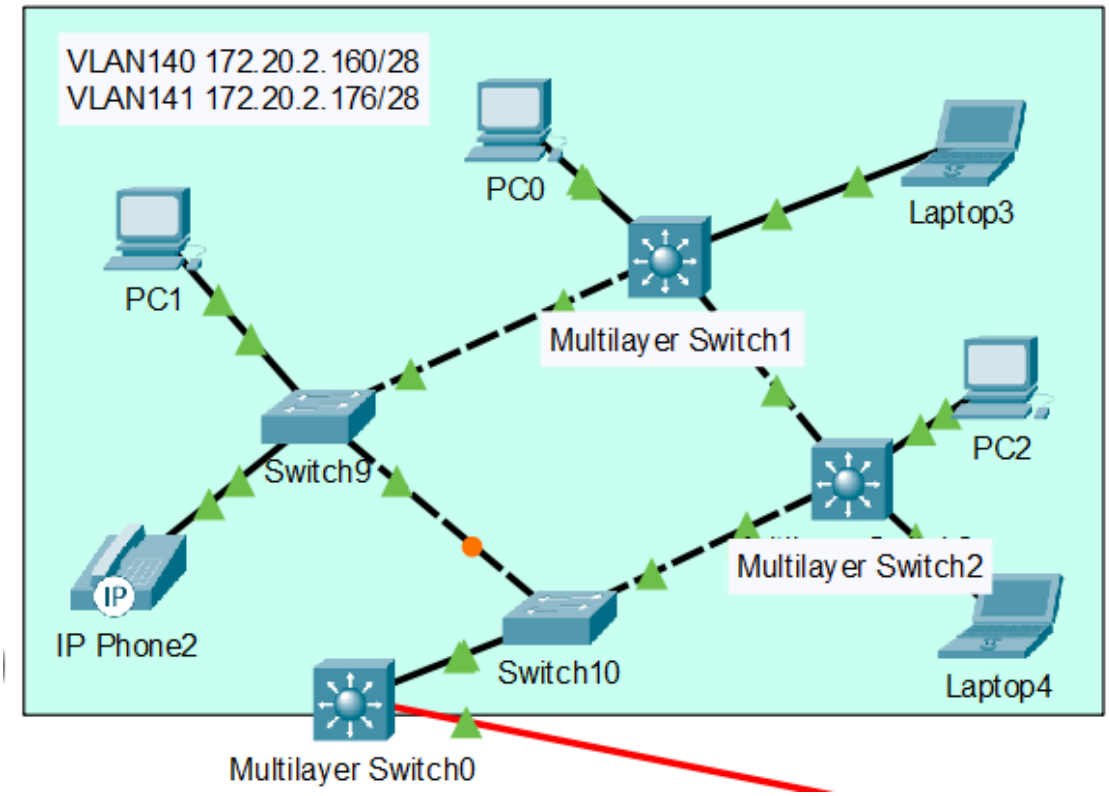

Рисунок 1.4 – Подключение коммутаторов L3 в сеть Building1

Коммутаторы L3 также могут выполнять функции маршрутизации третьего уровня, снижая необходимость установки выделенных маршрутизаторов в локальной сети. Поскольку в коммутаторах L3 установлено специальное аппаратное обеспечение для коммутации, они, как правило, могут направлять данные со скоростью самой коммутации.

С функциональной точки зрения коммутаторы третьего уровня представляют собой очень быстро работающие маршрутизаторы [5]. При обработке пакета они выполняют те же самые действия: используя информацию третьего уровня, определяют лучший путь передачи пакета, с помощью контрольной суммы проверяют целостность пакета и т. д. В то же время такие устройства полностью совместимы с традиционными маршрутизаторами и могут взаимодействовать с ними по стандартным протоколам маршрутизации.

Главное отличие маршрутизаторов и коммутаторов L3 заключается в архитектуре обработки пакетов. У традиционного маршрутизатора механизм этого процесса реализован программно, и он обычно функционирует на процессоре общего назначения. Ядро коммутаторов L3 осуществляет обработку пакетов на аппаратном уровне, а программная поддержка остается для процедур, которые напрямую не связаны с обработкой трафика: составления таблиц маршрутизации, поддержки функций управления и обработки пакетов в исключительных ситуациях (например, при реализация сложных фильтров). За счет перечисленных характеристик производительность коммутаторов L3 выше, чем у традиционных устройств, при меньшей стоимости и дополнительных функциональных возможностях. Хотя надо заметить, что многие современные модели маршрутизаторов имеют специальные чипы для ускоренной маршрутизации без использования ЦП и по производительности не уступают коммутаторам L3.

Благодаря анализу заголовков IP (или даже TCP/UDP) пакетов можно гибко устанавливать политику в сети, предусматривающую такие особенности обработки потока информации в локальной сети, как классы и качество обслуживания. С помощью коммутаторов L3 можно устанавливать приоритеты для трафика, выделять определенную ширину полосы пропускания и назначать величину задержки распространения конкретного вида трафика.

В отличие от традиционных маршрутизаторов, которые определяют конкретную подсеть только для одного интерфейса, коммутаторы L3 позволяют выделить в отдельную подсеть несколько интерфейсов коммутатора. Маршрутизация в коммутаторах L3 осуществляется над уровнем коммутации, что обеспечивает более гибкую и масштабируемую сетевую архитектуру.

Коммутаторы L3 поддерживают несколько различных типов интерфейсов. К основным типам относятся следующие:

– виртуальный интерфейс коммутатора (SVI) – логический интерфейс, связанный с виртуальной локальной сетью (VLAN);

– маршрутизируемый порт – физический порт на коммутаторе третьего уровня, настроенный на работу в качестве порта маршрутизатора;

– EtherChannel третьего уровня – логический интерфейс на устройстве Cisco, который связан с группой маршрутизируемых портов.

Интерфейс SVI для сети VLAN (VLAN1), используемой по умолчанию, должен быть активирован для обеспечения подключения IP-узла к коммутатору и возможности удаленного администрирования. Интерфейсы SVI также должны быть настроены для маршрутизации между сетями VLAN. Как уже упоминалось, SVI – это логические интерфейсы, настроенные для определенных сетей VLAN; для маршрутизации между двумя или более сетями VLAN каждая из них должна иметь отдельный активированный интерфейс SVI.

Маршрутизируемые порты позволяют коммутаторам L3 эффективно выступать в роли маршрутизаторов. Каждый порт на таком коммутаторе можно настроить в качестве одного из портов в независимой IP-сети.

Интерфейсы EtherChannel третьего уровня используются для объединения каналов Ethernet третьего уровня между устройствами, что позволяет агрегировать пропускную способность.

Рассмотрим пример подключения коммутаторов L3 к сети Building1 (см. рисунок 1.4). Коммутатор L3 может выполнять функции как коммутатора, так и маршрутизатора. На коммутаторах Multilayer Switch1 и Multilayer Switch2 реализованы только функции коммутации, на коммутаторе Multilayer Switch0 – функции коммутации и маршрутизации.

При конфигурации VLAN необходимо сначала создать VLAN с помощью команды `vlan номер_vlan`. Далее осуществляется конфигурация режимов интерфейсов. Для коммутатора Multilayer Switch1 на рисунке 1.4 использовались следующие команды:

```
Switch(config)#interface range FastEthernet0/1-2
Switch(config-if)# switchport access vlan 140
Switch(config-if)# switchport mode access
Switch(config)#interface range FastEthernet0/21-22
Switch(config-if)# switchport mode access
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk native vlan 142
```

Так как коммутатор L3 может выполнять функции маршрутизатора, то в конфигурации VLAN коммутатора Multilayer Switch0 нужно осуществить настройку IP-адреса. Настройка VLAN для коммутатора Multilayer Switch0 на рисунке 1.4 осуществлялась следующим образом:

```
Switch(config)#interface Vlan140
Switch(config-if)#ip address 172.20.2.161 255.255.255.240
```

Для настройки DHCP-сервера на коммутаторе Multilayer Switch0 используются команды, аналогичные командам на маршрутизаторе. Ниже представлена конфигурация DHCP сервера на коммутаторе Multilayer Switch0:

```
Switch(config)#ip dhcp pool VLAN140
Switch(dhcp-config)# network 172.20.2.160 255.255.255.240
Switch(dhcp-config)# default-router 172.20.2.161
Switch(dhcp-config)# dns-server 172.20.3.98
```

Для маршрутизации может использоваться любой протокол. Настройка протокола OSPF на коммутаторе Multilayer Switch0 осуществляется следующим образом:

```
Switch(config)#router ospf 115
Switch(config-router)# router-id 20.20.20.26
Switch(config-router)#network 172.20.3.112 0.0.0.15 area 20
Switch(config-router)#network 172.20.2.160 0.0.0.15 area 20
Switch(config-router)#network 172.20.2.176 0.0.0.15 area 20
```

На интерфейсах коммутатора Multilayer Switch0, подключенных к другим маршрутизаторам, также необходимо настроить адресацию и маршрутизацию:

```
Switch(config)#interface GigabitEthernet1/1/1
Switch(config-if)#no switchport
Switch(config-if)#ip address 172.20.0.194 255.255.255.252
Switch(config-if)#ip ospf 115 area 20
```

Как видно из рисунка 1.4, один из портов коммутаторов обозначен кругом (порт FastEthernet0/21 коммутатора Switch10). Если отправить ICMP-пакет, то из-за блокировки порта он пойдет не по кратчайшему пути, что увеличит время передачи. Это происходит из-за неверной конфигурации протокола. Для просмотра настроек протокола STP на коммутаторе необходимо ввести команду `show spanning-tree` (рисунок 1.5), в результате получаем информацию о данных корневого (Root ID) и текущего (Bridge ID) коммутаторов и статусы интерфейсов (Interface).

```
Switch#show spanning-tree vlan 142
VLAN0142
  Spanning tree enabled protocol ieee
  Root ID     Priority    4238
              Address     000C.851D.C984
              Cost        38
              Port        24(FastEthernet0/24)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    16526  (priority 16384 sys-id-ext 142)
              Address     0002.4AAA.246E
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/22           Altn BLK 19        128.22   P2p
Fa0/24           Root FWD 19        128.24   P2p
Po5              Desg FWD 9         128.29   Shr
```

Рисунок 1.5 – Просмотр настроек STP протокола на коммутаторе

По части данных корневого коммутатора можно понять, какой коммутатор является корневым, т. е. главным. Для этого в сети передаются BPDU-кадры, в которых в полях «Идентификатор корневого моста», «Расстояние до корневого моста» и «Идентификатор моста» содержится вся важная информация. Изначально коммутаторы в поле «Идентификатор корневого моста» записывают свой приоритет (по умолчанию 32768) и MAC-адрес. Коммутатор, который получит этот кадр, будет сравнивать свой «Идентификатор корневого моста» с полученным в BPDU-пакете. Если приоритет ниже, то с этого момента он будет ретранслировать его BPDU. В результате в сети останется только один коммутатор, который будет генерировать BPDU. Если приоритеты по умолчанию равны, коммутатор начинает опираться на MAC-адреса. И тот, у кого MAC-адрес меньше, становится главным.

В таблице интерфейсов (см. рисунок 1.5) записаны номера интерфейсов, их роли, статусы портов и прочее. Тип P2p говорит о том, что порт коммутатора подключен к другому коммутатору. Если указан тип Shared (Shr), то это означает, что порт подключен к нескольким коммутаторам. Один из интерфейсов имеет роль (режим) Designated (Desg), статус Forwarding (FWD), что говорит о том, что порты прошли все стадии и сейчас находятся в режиме пересылки. Другой интерфейс находится в роли Root, что говорит о кратчайшем пути к корневому коммутатору. Последний интерфейс находится в роли Alternate (Altn), запасной, а его статус Blocking (BLK) говорит о том, что порт заблокирован. Блокировка необходима для обрыва петли.

В поле «Расстояние до корневого моста» записывается стоимость пути. При создании BPDU, корневой коммутатор записывает туда ноль. Следующие коммутаторы начинают суммировать стоимость по таблице 1.1. В поле «Идентификатор моста» записываются приоритет и MAC-адрес самого коммутатора. При ретрансляции BPDU от коммутатора к коммутатору каждый записывает свой идентификатор в данное поле.

Когда коммутатор становится корневым, он сразу переводит все свои интерфейсы в роль Designated, обозначающую порт, который имеет самый короткий путь до корневого коммутатора. Остальные коммутаторы также вычисляют, через какой порт расстояние до корневого коммутатора будет наименьшим, и определяют свою роль как Root. При этом могут быть порты, которые не соединены с корневым коммутатором, тогда один из коммутаторов отключает данный порт. Для этого используется поле «Идентификатор моста», сравниваются приоритеты или, если они равны, сравнение происходит по MAC-адресам. Если у коммутатора MAC-адрес меньше, он переводит порт в роль Designated, а другой коммутатор – в роль Non-Designated (роль, при которой порту запрещено передавать какие-либо данные, но разрешено слушать, что происходит в сети, т. е. если в сети произойдет разрыв, он может включиться и работать, обеспечивая резервирование).

Кроме ролей у каждого порта есть следующие статусы:

– Blocking – блокировка, статус, в котором просматриваются пакеты BPDU и определяется состояние сети; в случае появления обрыва линии связи порт переходит в режим Listening;

– Listening – прослушивание, статус, в котором коммутатор отправляет и обрабатывает BPDU-кадры; если определено, что параметры отличаются, по истечении 15 секунд переходит в состояние Learning;

– Learning – обучение, статус, в котором коммутатор отправляет и обрабатывает BPDU-кадры, вносит изменения в таблицу коммутации; если получены данные имеют приоритет выше, чем у данного коммутатора, происходит переход в состояние Forwarding;

– Forwarding – продвижение, обмен служебной информацией и пользовательскими данными;

– Disable – отключение, физическое отключение порта, данные не передаются.

При построенном дереве корневой коммутатор передает BPDU-кадры другим коммутаторам, как показано на рисунке 1.6. В поле кадра Ethernet 802.3 указан широковещательный MAC-адрес (0180.C200.0000) в качестве адреса получателя. В полях BPDU в качестве стоимости пути указан «0», т. к. данный коммутатор является корневым.

Для установки приоритета на коммутаторе используется команда `spanning-tree vlan` *`номер`* `priority` *`число`*, в которой чем меньше число приоритета, тем приоритет выше.

Недостатком протокола STP является построение одного дерева для всей топологии, т. е. данный протокол не подходит для сетей с VLAN. В данном случае необходимо использовать протокол PVST (Per-VLAN Spanning Tree), который позволяет строить отдельное дерево для каждого VLAN. С появлением протокола 802.1Q PVST был модернизирован в протокол PVST+. В протоколе PVST+ к приоритету добавляется параметр **System ID Extension**, который содержит в себе номер VLAN. Например если VLAN имеет номер 1, то приоритет будет равняться 32768 + 1 = 32769, если VLAN имеет номер 10, то приоритет будет равняться 32768 + 10 = 32778.

Режим построения дерева PVST+ указывается командой `spanning-tree mode pvst`.

Для правильной работы сети необходимо, чтобы на всех коммутаторах был настроен одинаковый протокол.

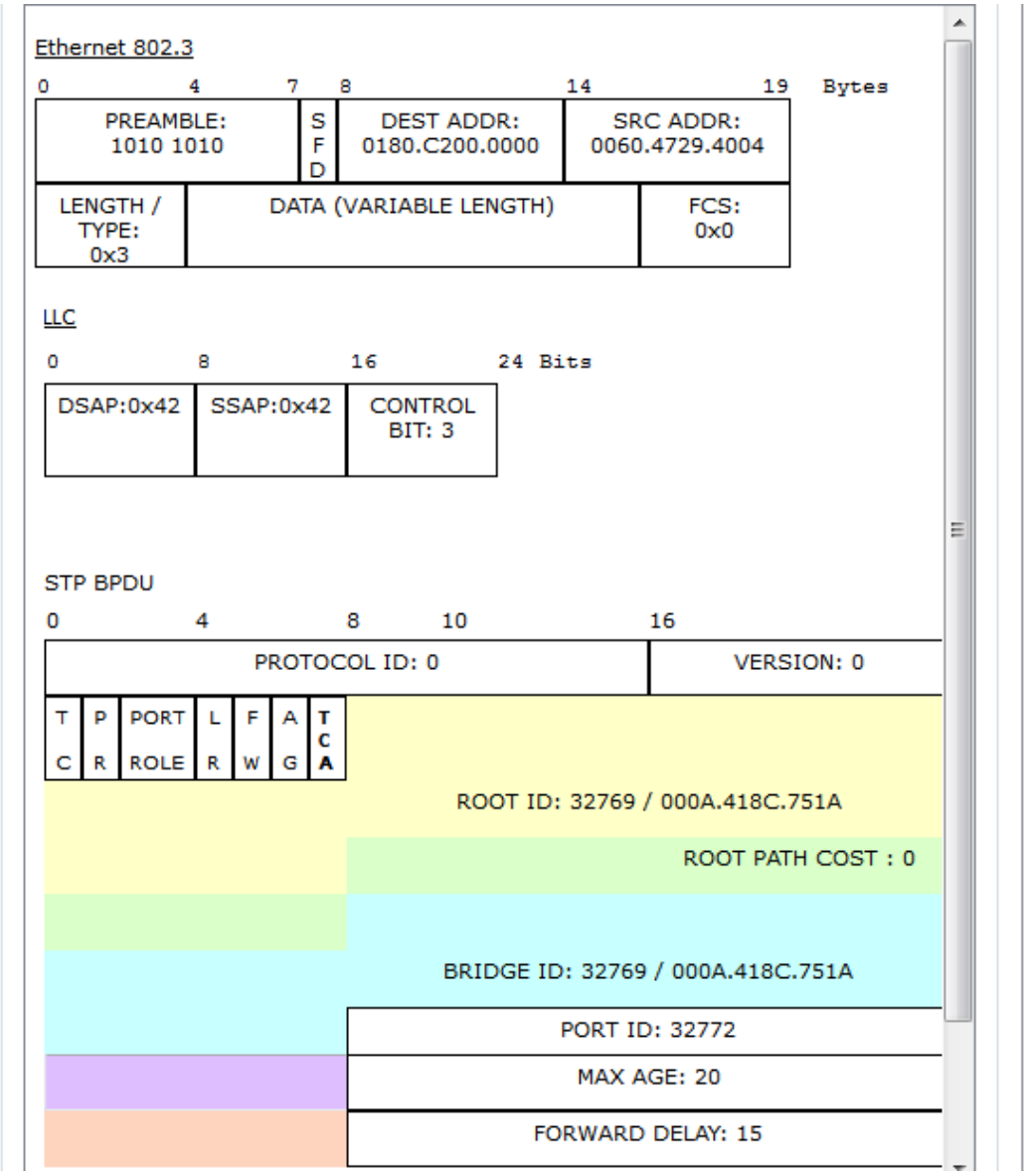

Рисунок 1.6 – Передача пакетов BPDU

В случае если в сети используется VLAN, то существует возможность создать для каждого VLAN своей корневой коммутатор. Для этого с помощью команды `spanning-tree vlan` *`номер`* `priority` *`число`* задаются необходимые приоритеты на каждом коммутаторе, которые и будут определять корневой коммутатор в VLAN. При этом чем больше VLAN в сети, тем больше информации будет получено после команды `show spanning-tree`. Для получения информации о построенном дереве для определенного VLAN можно использовать команду `show spanning-tree vlan` *`номер`*. Команда `show spanning-tree summary` показывает общую информацию, а именно в каком режиме работает коммутатор, для какого VLAN он является корневым, какие функции на нем включены, а также таблицу, содержащую имена VLAN и количество интерфейсов, находящихся в различных состояниях.

RSTP (Rapid Spanning Tree Protocol, быстрый STP) – версия протокола STP с ускоренной реконфигурацией дерева, использующаяся для исключения петель. Основное отличие данного протокола заключается в том, что все коммутаторы осуществляют отправку BPDU каждые 2 секунды по умолчанию. Если в протоколе STP коммутатор обнаруживает изменение топологии, он извещает корневой коммутатор, который, в свою очередь, требует от всех остальных очистить записи о текущей топологии в течение 15 секунд. Весь процесс перестройки дерева в этом случае может занять более 30 секунд в зависимости от размера сети. В протоколе RSTP обнаружение изменений в топологии влечет немедленную очистку записей. Также в RSTP есть еще одна роль порта, которая называется backup (резервный), который так же как и в роли alternate, не участвует в пересылке данных. Быстродействие протокола RSPT заключается в том, чтобы в случае отказа основного порта переключится на резервный. Для этого не нужно заново просчитывать топологию, необходимо просто переключиться на запасной порт.

Для переключения протокола RSTP используется команда `spanning-tree mode rapid-pvst`.

На рисунке 1.7 показан пример сети с VLAN, в которой используется протокол RSTP.

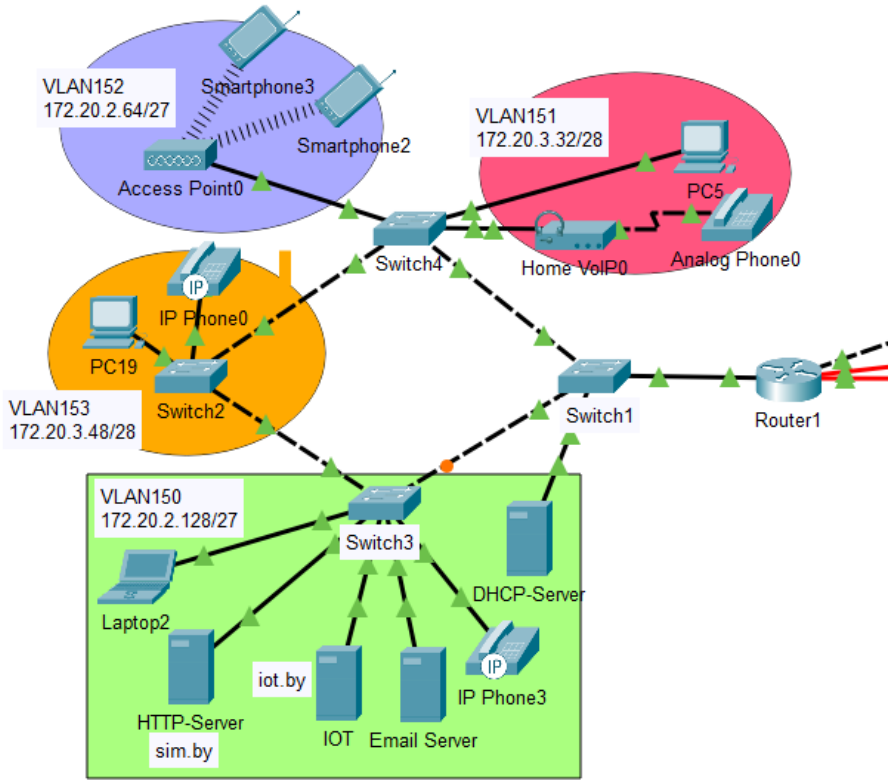

Рисунок 1.7 – Пример смоделированной сети с построением дерева на основе протокола RSTP

Для разрешения построения дерева только для определенных VLAN используется команда `spanning-tree vlan 1,150-154`.

В представленной выше команде указаны номера VLAN 150–153, настроенные для оконечных устройств, VLAN 154, соединяющий коммутаторы (Trunk), и VLAN 1, установленный на всех коммутаторах по умолчанию.

В случае если необходимо запретить построение деревьев для других VLAN, используется команда `no spanning-tree vlan 2-149`.

1.2 Лабораторное задание

Лабораторная работа выполняется на основе файла **Lab4-4.pkt** лабораторной работы № 4 лабораторного практикума «Маршрутизация в IPv4- и IPv6-сетях» [6]. До начала выполнения необходимо открыть сохраненный файл **Lab4-4.pkt** и проверить настройки IP-адресации: у всех устройств адресация должна соответствовать заданному IP-адресу из таблицы 1.2, должен использоваться протокол OSPFv2. В сети должны быть подсети с VLAN и беспроводным маршрутизатором, подсеть Building1, подсети с устройствами освещения, контроля температуры и дыма, видеонаблюдения, контроля доступа и пожаротушения, три сервера: на одном сервере должны отображаться состояния устройств освещения, контроля температуры и дыма (сервер iot.by на рисунке 1.8), на втором сервере должны отображаться состояния устройств видеонаблюдения, контроля доступа и пожаротушения (сервер camera.by на рисунке 1.8), на третьем – веб-сайт, разработанный в лабораторной работе № 5 лабораторного практикума «Основы построения локальных сетей» [10], доменное имя которого должно соответствовать фамилии студента. С любого устройства из любой подсети должен быть доступ к серверам.

В данной лабораторной работе необходимо организовать агрегирование каналов между коммутаторами с помощью протокола PVST для локальной сети Building1 и протокола RSTP для локальной сети с VLAN. По результатам выполнения данной лабораторной работы должна быть смоделирована сеть, аналогичная показанной на рисунке 1.8.

1 *Наблюдение петли коммутации*. Добавить в локальную сеть Building1 коммутатор и подключить к нему компьютер, на котором настроить IP-адресацию. Создать между коммутаторами два физических соединения, как показано на рисунке 1.2. Ввести на двух коммутаторах сети Building1 команду `no spanning-tree vlan 1`. Перейти в режим симуляции времени, установить в фильтре «Edit Filter» просмотр передачи пакетов ARP и ICMP, отправить ICMP-пакет с добавленного компьютера. Проследить за процессом передачи пакетов и заполнить таблицу 1.3. Сохранить файл под именем **LAB1-1.pkt**. Сделать вывод об особенностях передачи.

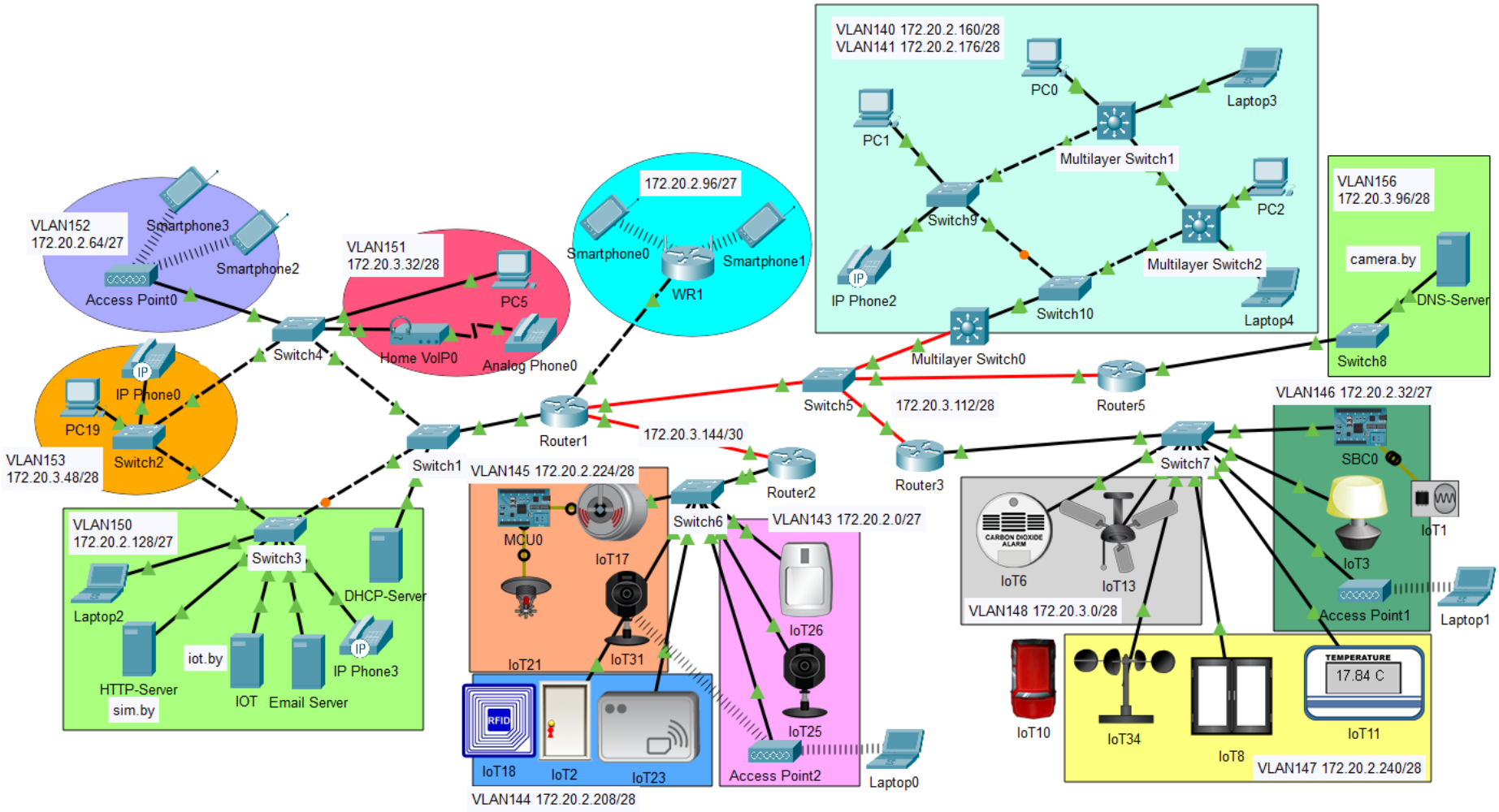

Рисунок 1.8 – Пример смоделированной сети

Таблица 1.2 – Исходные данные для смоделированной сети

Вторая цифра шифра	IP-адрес сети	Router-id	Номера VLAN для видеокамер, системы контроля доступа, пожаротушения, контроля дыма, освещения, температуры
0	172.16.0.0/20	10.10.10.10	80–85, 50–55
1	172.17.0.0/21	20.20.20.20	120–125, 150–155
2	172.18.0.0/22	30.30.30.30	230–235, 250–255
3	172.19.0.0/23	40.40.40.40	340–345, 350–355
4	172.21.0.0/22	15.15.15.15	455–460, 450–455
5	172.22.0.0/23	25.25.25.25	565–570, 550–555
6	172.23.0.0/24	35.35.35.35	675–680, 650–655
7	172.24.0.0/24	45.45.45.45	781–786, 750–755
8	172.30.0.0/21	13.13.13.13	890–895, 850–855
9	172.31.0.0/20	18.18.18.18	995–100, 950–955

Таблица 1.3 – Последовательность действий в смоделированной сети с коммутаторами при отправке ICMP-пакета

Номер шага	Отправитель	Получатель
1		
2		
3		

2 *Проверка построения дерева в смоделированной сети*. Добавить к построенной в пункте 1 сети Building1 еще два коммутатора L3 3560-24PS. Соединить коммутаторы в кольцо, к каждому коммутатору подключить по два компьютера (см. рисунок 1.8). Заменить маршрутизатор, соединяющий подсеть Building1 с другими сетями, на коммутатор L3 3650-24PS. Добавить в коммутатор L3 3650-24PS модули AC-POWER-SUPPLY и GLC-LH-SMD (рисунок 1.9). Настроить на добавленных коммутаторах L3 3560-24PS VLAN в соответствии с данными из таблицы 1.4. На коммутаторе L3 3650-24PS настроить IP-адресацию, маршрутизацию, VLAN. Ввести на всех коммутаторах сети Building1 команды `spanning-tree mode pvst` и `spanning-tree vlan` *`номер`*, в качестве номера VLAN указать значения VLAN1 и настроенные в подсети Building1 VLAN. Просмотреть на коммутаторах информацию о построенных деревьях, определить корневой коммутатор, заполнить таблицу 1.5. Сохранить файл под именем **LAB1-2.pkt**. Сделать вывод.

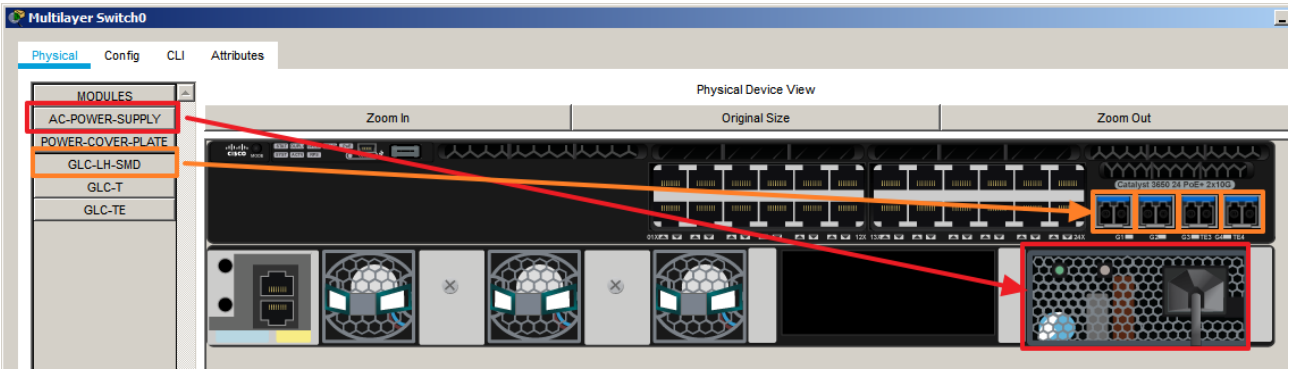

Рисунок 1.9 – Добавление моделей интерфейсов и блока питания в коммутатор L3 3650-24PS

Таблица 1.4 – Исходные данные для конфигурации

Третья цифра шифра	Номер VLAN для сети Building1		Приоритет
	access	trunk	
0	10	11	40960
1	100	101	36864
2	200	201	32768
3	300	301	28672
4	400	401	24576
5	500	501	4096
6	600	601	8192
7	700	701	12288
8	800	801	16384
9	900	901	20480

Таблица 1.5 – Данные коммутаторов

Имя коммутатора	Приоритет Root/MAC-адрес	Приоритет Bridge/MAC-адрес	Статусы/роли портов

3 *Процесс обмена данными между коммутаторами*. Перейти в режим симуляции. Установить в фильтре «Edit Filter» просмотр передачи только пакетов STP. Проследить передачи пакетов BPDU в сети и заполнить таблицу 1.6. Отразить в выводе, какой коммутатор по умолчанию стал корневым.

Таблица 1.6 – Описание процесса передачи BPDU-кадров

Номер шага	Отправитель	Получатель	Описание особенностей содержимого пакета
1			
2			

4 Настроить другой коммутатор в роли корневого (Multilayer Switch1 на рисунке 1.8). Используя команду `spanning-tree vlan` *`номер`* `priority` *`число`*, настроить приоритет для главного коммутатора (см. таблицу 1.4), для каждого последующего коммутатора уставить значение приоритета на 4096 больше значения приоритета, заданного в таблице 1.4. У каждого коммутатора должно быть разное значение приоритета. После внесения изменений заполнить таблицу по шаблону таблицы 1.5. Сохранить файл под именем **LAB1-4.pkt**.

5 Осуществить обрыв линии связи от корневого коммутатора таким образом, чтобы инициировать смену роли порта Blocking на Forwarding одного из коммутаторов (рисунок 1.10). Отправить ICMP-пакет с компьютера, подключенного к корневому коммутатору. Отразить в выводе, как быстро в подсети Building1 произошли изменения. Ликвидировать обрыв линии.

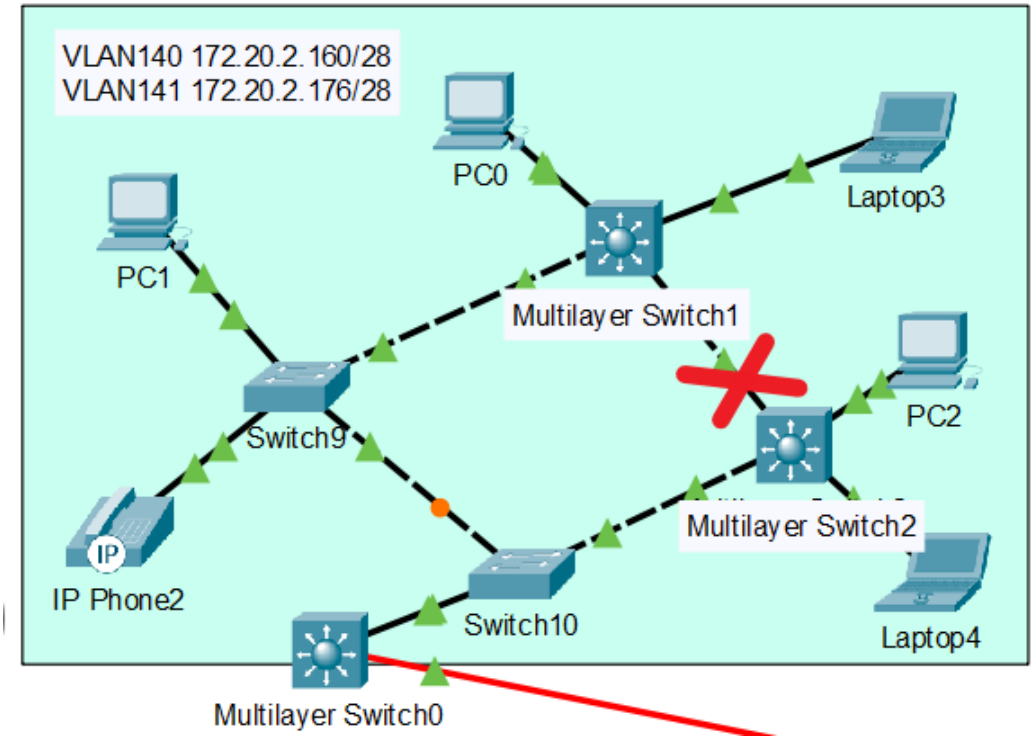

Рисунок 1.10 – Реализация обрыва линии
для наблюдения перестроения дерева STP

6 *Изучение работы протокола RSTP*. Настроить на всех коммутаторах в сетях с VLAN протокол RSTP. При необходимости добавить в подсеть коммутаторы, как показано на рисунках 1.7 и 1.8. Задать приоритет из таблицы 1.4 коммутатору, аналогичном коммутатору Switch4 на рисунке 1.8, для каждого последующего коммутатора установить значение приоритета на 4096 больше заданного значения приоритета. У каждого коммутатора должно быть разное значение приоритета. Разрешить построение дерева для настроенных в данной подсети VLAN. Просмотреть на коммутаторах информацию о построенных деревьях, определить корневой коммутатор. Заполнить таблицу по шаблону таблицы 1.5. Сохранить файл под именем **LAB1-6.pkt**.

7 Осуществить обрыв линии связи от корневого коммутатора. Отправить сообщение с компьютера. Отразить в выводе, что произошло в построенной сети, какие отличительные особенности работы протокола RSTP и PVST проявились в процессе. Ликвидировать обрыв линии.

1.3 Содержание отчета

1 Цель работы, исходные данные.

2 Результаты произведенных настроек (заполненные таблицы 1.3, 1.5, 1.6), результаты настроек из пунктов 1–7, изображение смоделированной сети.

3 Вывод по работе.

4 Ответы на контрольные вопросы.

1.4 Контрольные вопросы

1 Отличительные особенности коммутаторов L2, L3, маршрутизаторов.

2 Типы интерфейсов коммутаторов L3. Особенности конфигурации коммутаторов L3.

3 Определение и назначение агрегирования каналов.

4 Петля коммутации, причины образования.

5 Назначение протокола STP.

6 Механизм работы STP протокола.

7 Типы и содержание информации, которой обмениваются коммутаторы.

8 Формат данных BPDU-кадра.

9 Определение корневого коммутатора в автоматическом режиме работы протокола STP.

10 Состояние и роли портов коммутатора.

11 Отличия протоколов STP, PVST, PVST+, RSTP.

ЛАБОРАТОРНАЯ РАБОТА № 2
ТЕХНОЛОГИИ АГРЕГАЦИИ КАНАЛОВ

Цель: изучить технологии и методы агрегации каналов и балансировки нагрузки, овладеть навыками настройки статической агрегации каналов и агрегации по протоколам LACp и PAgP.

2.1 Теоретическая часть

Технологии агрегирования позволяют соединять разные устройства несколькими каналами связи (см. рисунок 1.1). Таким образом резервируется канал передачи данных и увеличивается пропускная способность. Подобную технологию иногда называют распределенным агрегированием каналов.

Избыточные соединения между коммутаторами без использования специальных технологий для агрегирования каналов чаще всего способствуют передаче данных хотя бы через один интерфейс, который, как правило, не заблокирован протоколом STP. Без использования STP такое избыточное соединение создаст петлю в сети. Такой вариант позволяет обеспечить резервирование каналов, но не дает возможности увеличить пропускную способность [1].

Технология агрегирования каналов позволяет использовать все интерфейсы одновременно. При этом устройства контролируют распространение широковещательных пакетов, чтобы не допустить образования петли коммутации. Для этого коммутатор при получении широковещательного кадра через обычный интерфейс отправляет его в агрегированный канал только через один интерфейс. А при получении широковещательного фрейма из агрегированного канала не отправляет его назад. При этом реальная загруженность конкретного интерфейса никак не учитывается. При неправильном выборе метода балансировки может сложиться ситуация, когда все данные будут передаваться только через один интерфейс, а остальные будут незадействованы.

Хотя агрегирование позволяет увеличить пропускную способность канала, иногда возникает проблема правильной балансировки нагрузки между интерфейсами в агрегированном канале, которая может осуществляться по следующим критериям: MAC-адресам, IP-адресам, портам отправителя или получателя и др.

Компанией Cisco разработана технология агрегирования каналов под названием Etherchannel, позволяющая объединять несколько физических соединений (каналов, портов) в единый логический интерфейс. При этом у других компаний технологии агрегирования называются по-другому, например, Huawei имеет технологию агрегирования Link Aggregation, D-Link – LAG.

В устройствах Cisco объединение каналов можно выполняться статически или динамически, т. е. с помощью специальных протоколов LACP и PAgP.

LACP (Link Aggregation Control Protocol) – открытый протокол, определяемый стандартом IEEE 802.3ad.

PAgP (Port Aggregation Protocol) – проприетарный протокол компании Cisco.

Использование LACP позволяет осуществить статическое или динамическое согласование настроек с удаленной стороной и избежать ошибок и петель в сети. Поддержка standby-интерфейсов позволяет агрегировать до 16 портов, 8 из которых будут активными, а остальные – в режиме standby (режим ожидания), в котором интерфейсы могут принимать пакеты, но не передавать их. При этом возможна дополнительная задержка при активации агрегированного канала или изменении его настроек.

Статическое агрегирование не вносит дополнительную задержку при активации агрегированного канала или изменении его настроек, при этом отсутствует согласование настроек с удаленной стороной. Не исключено, что ошибки в настройке могут привести к образованию петель.

Данные виды протоколов могут быть использованы при следующих условиях:

– все порты находятся в режиме Duplex;

– у всех интерфейсов одинаковая скорость;

– имеются одинаковые разрешенные VLAN;

– настроен одинаковый режим интерфейсов (access, trunk).

При настройке Etherchannel следует придерживаться следующих правил:

– для объединения в интерфейсах должны совпадать многие настройки: проще объединять их, когда они настроены по умолчанию, затем настраивать логический интерфейс;

– перед объединением интерфейсов лучше отключить их, что позволит избежать блокирования интерфейсов протоколом STP;

– для агрегирования рекомендуется выбирать количество кабелей в канале кратное двум;

– для удаления настройки EtherChannel достаточно удалить логический интерфейс.

Для включения протокола LACP необходимо выбранные интерфейсы объединить в канальную группу, для чего в настройках интерфейса указывается номер группы и режим с помощью команды `channel-group` *`номер группы`* `mode` *`режим`*.

Протокол LACP поддерживает три режима: on, active, passive. Отличие режимов в том, что режим active сразу активизирует протокол LACP, а режим passive включит LACP, если обнаружит LACP-сообщение от другого ком-

мутатора. Соответственно, чтобы агрегирование с помощью протокола LACP заработало сразу же, необходимо чтобы интерфейсы соседних коммутаторов были сразу установлены в режим on или active, либо один в active, а другой в passive. Например, чтобы настроить протокол LACP для интерфейсов fastEthernet 0/23-24 на коммутаторе Switch9 (рисунок 2.1), необходимо использовать следующие команды:

```
Switch9(config)#interface range fastEthernet 0/23-24
Switch9(config-if-range)#shutdown
Switch9(config-if-range)#switchport nonegotiate
Switch9(config-if-range)#channel-protocol lacp
Switch9(config-if-range)#channel-group 4 mode passive
Switch9(config-if-range)#no shutdown
```

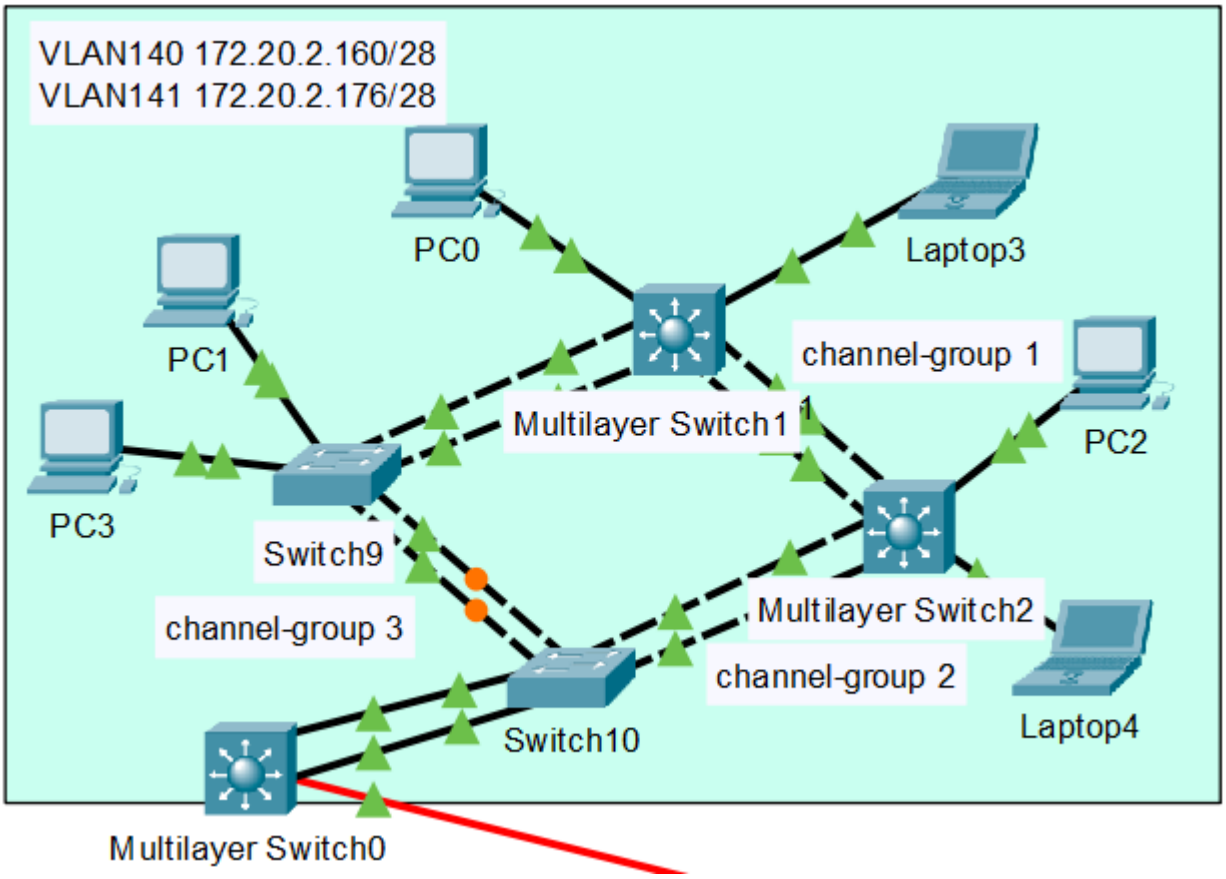

Рисунок 2.1 – Пример подсети с протоколом LACP

В результате выполнения команды `channel-group 4 mode passive` создается отдельный логический интерфейс port-channel 4, в настройки которого можно зайти с помощью команды `interface port-channel 4`.

Все действия, производимые в процессе настройки данного интерфейса, автоматически будут приводить к изменениям на физических портах.

В случае если в сети настроены VLAN, необходимо в конфигурации каждой канальной группы настроить режим trunk и указать номер native VLAN.

Конфигурация протокола LACP на коммутаторе L3 (MultiLayer Switch1 на рисунке 2.1) производится следующим образом:

```
Switch(config)#interface range fa0/23-24
Switch(config-if-range)# shutdown
Switch(config-if-range)# channel-protocol lacp
Switch(config-if-range)# channel-group 4 mode active
```

После ввода приведенных выше команд может появиться следующее сообщение:

```
%EC-5-CANNOT_BUNDLE2: Fa0/23 is not compatible with Po4
and will be suspended (native vlan of Fa0/23 is 142, Po4
id 1)
%EC-5-CANNOT_BUNDLE2: Fa0/24 is not compatible with Po4
and will be suspended (native vlan of Fa0/24 is 142, Po4
id 1)
```

Данное сообщение информирует о невозможности объединения интерфейсов Fa0/23 и Fa0/24 в логический интерфейс port-channel 4, т. к. на интерфейсах настроен native VLAN 142. Поэтому необходимо удалить VLAN 142 и указать его в конфигурации интерфейса port-channel 4 следующим образом:

```
Switch(config)#interface Port-channel4
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport trunk native vlan 142
```

После введения вышепредставленных команд осуществится объединение интерфейсов Fa0/23 и Fa0/24 в логический интерфейс port-channel 4, что можно проверить с помощью команд `show etherchannel port-channel` и `show etherchannel summary` (рисунок 2.2).

Между коммутаторами, настроенными в режимах active и passive, передаются LACP-пакеты (рисунок 2.3). Первый коммутатор отправляет LACP-сообщение, в Ethernet заголовке которого в поле Source MAC он записывает свой MAC-адрес, а в Destination MAC – широковещательный адрес

0180.C200.0002. Данное сообщение используется устройствами для синхронизации, сбора, агрегации, проверки активности и т. д. В кадре LACP в поля Actor System и Partner System записываются MAC-адреса виртуальных интерфейсов коммутаторов.

```
Port-channel: Po4    (Primary Aggregator)
------------

Age of the Port-channel   = 01d:00h:10m:38s
Logical slot/port   = 2/4          Number of ports = 2
GC                  = 0x00000000      HotStandBy port = null
Port state          = Port-channel
Protocol            =  LACP
Port Security       = Disabled

Ports in the Port-channel:

Index   Load   Port     EC state        No of bits
------+------+------+------------------+-----------
  0     00     Fa0/23   Passive            0
  0     00     Fa0/24   Passive            0
Time since last port bundled:    00d:00h:05m:16s    Fa0/24
Switch3#show etherchannel summary
Number of channel-groups in use: 2
Number of aggregators:           2

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------

3      Po3(SU)           LACP    Fa0/21(P) Fa0/22(P)
4      Po4(SU)           LACP    Fa0/23(P) Fa0/24(P)
```

Рисунок 2.2 – Пример результаты объединения интерфейсов в логический канал

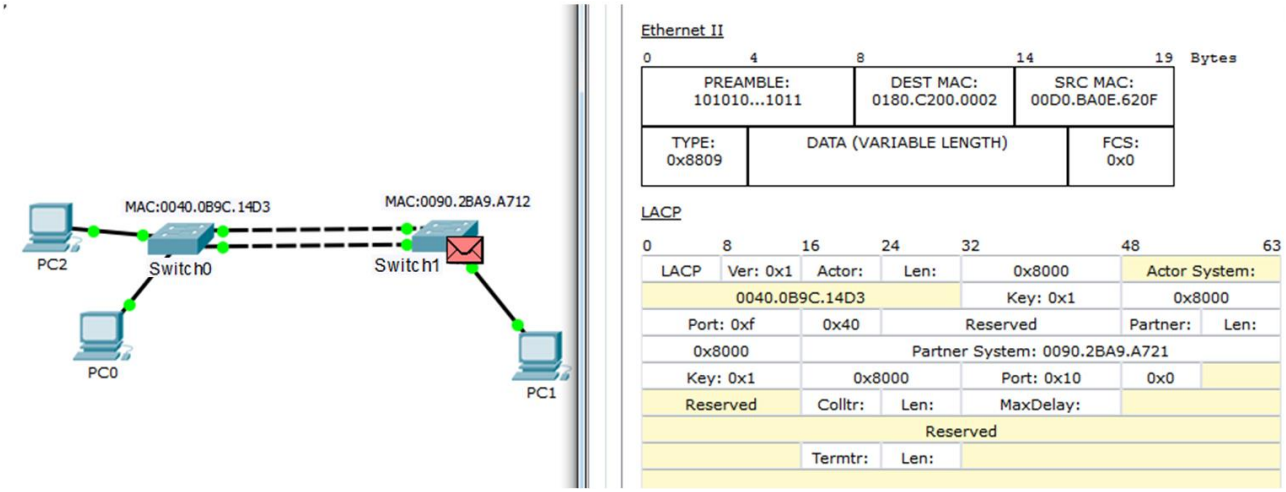

Рисунок 2.3 – Передача и содержание пакетов LACP

При создании агрегированного канала надо не забывать, что внутри него находятся физические интерфейсы, которые пропускают трафик. При этом иногда наблюдается ситуация, что весь трафик идет только по одному интерфейсу, а остальные не участвуют в передаче данных. Для этого используется балансировка нагрузки (Load Balance), которая по умолчанию работает исходя из MAC-адресов. При этом данный режим работы не всегда эффективен. Если, например, компьютер PC0 на рисунке 2.3 будет отправлять данные компьютеру PC1, то трафик будет проходить по первой линии связи. В то же время данные от компьютера PC2 к PC1 будут идти по второй. При этом все данные от PC1 к PC2 или PC0 будут проходить только по одному из путей, что приведет к неравномерной нагрузке в каналах. Поэтому иногда осуществляют настройку не по MAC-адресу источника, а по MAC-адресу назначения (Destination MAC), тогда данные и в обратном направлении (от PC1 к PC2 или PC0) будут передаваться по разным каналам.

Просмотреть состояние балансировки нагрузки на коммутаторе можно с помощью команды `show etherchannel load-balance`.

В зависимости от модели коммутатора могут поддерживаться следующие методы балансировки:

– по MAC-адресу отправителя (`src-mac`), MAC-адресу получателя (`dst-mac`) или с учетом обоих адресов (`src-dst-mac`);

– по IP-адресу отправителя (`src-ip`), IP-адресу получателя (`dst-ip`) или с учетом обоих адресов (`src-dst-ip`);

– по номеру порта отправителя, номеру порта получателя или с учетом обоих портов.

С помощью команды `port-channel load-balance` *вид* можно выбрать необходимый способ балансировки. Проверить правильность распределения нагрузки в логическом канале можно отправив любой пакет с разных оконечных устройств и проследив его прохождение через коммутаторы.

При включении протокола PAgP также используется три режима: on – включение PAgP, desirable – включение PAgP и отправка пакета PAgP, auto – включение в случае получения PAgP сообщение. Принцип работы схож с работой протокола LACP. Например, чтобы настроить протокол PAgP для интерфейсов FastEthernet 0/20-21 на коммутаторе Switch1 (рисунок 2.4), необходимо использовать следующие команды:

```
Switch1(config)#interface range fastEthernet 0/20-21
Switch1(config-if)#shutdown
Switch1(config-if)#channel-group 4 mode desirable
```

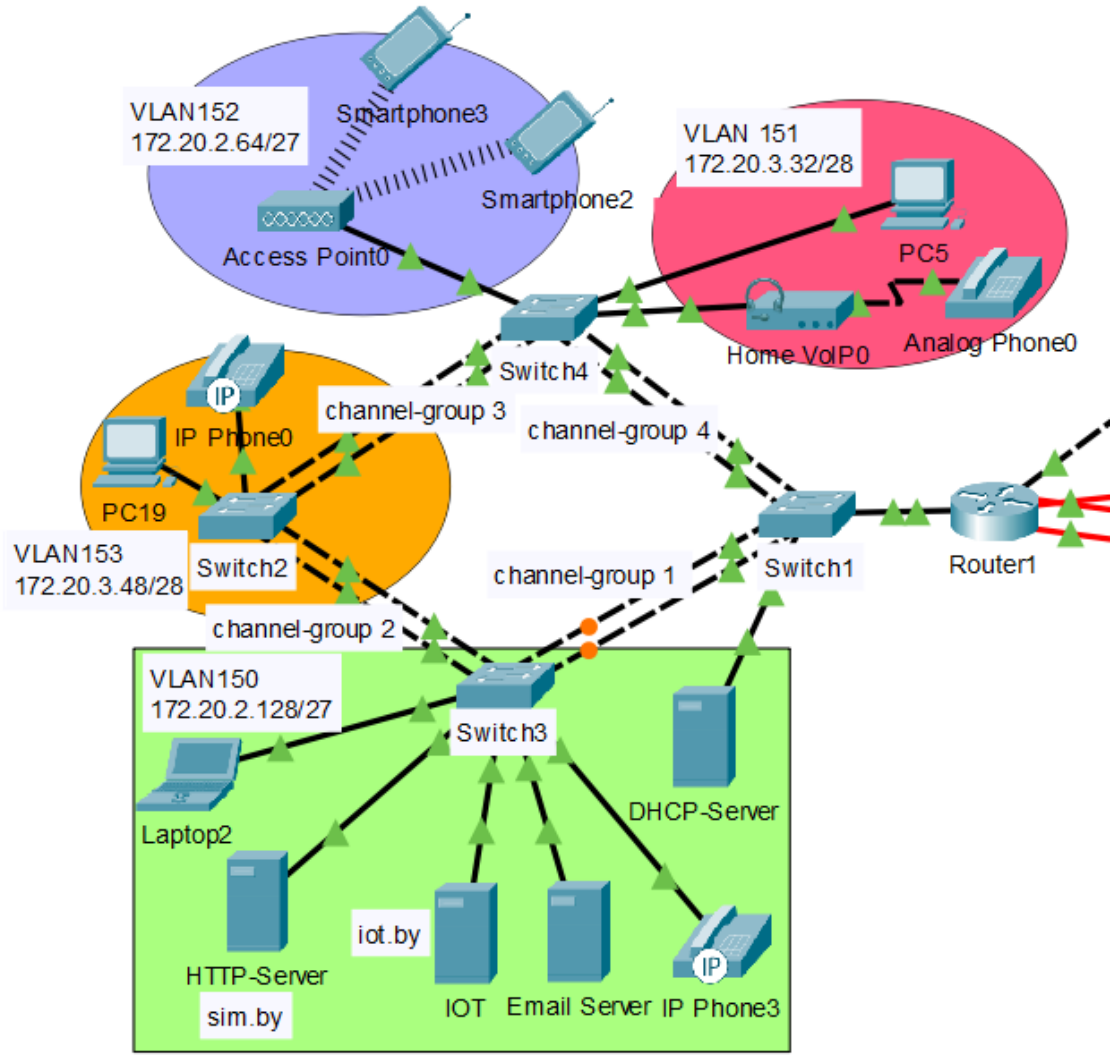

Рисунок 2.4 – Пример сети с агрегацией каналов по протоколу PAgP

Для соседнего коммутатора Switch1 настройка осуществляется следующим образом:

```
Switch4(config)#interface range fastEthernet 0/20-21
Switch4(config-if)#shutdown
Switch4(config-if)#channel-group 4 mode auto
Switch4(config-if)#no shutdown
```

Только после этого включается интерфейс на первом коммутаторе командой `no shutdown`. При получении PAgP-сообщения (рисунок 2.5) второй коммутатор меняет свой режим работы. В сообщении PAgP передается не только MAC-адрес соседнего коммутатора (поле Partner Device ID), но и имя устройства и порта, с которого осуществляется отправка сообщения. Как видно, основное отличие PAgP и LACP протокола состоит в структуре сообщений.

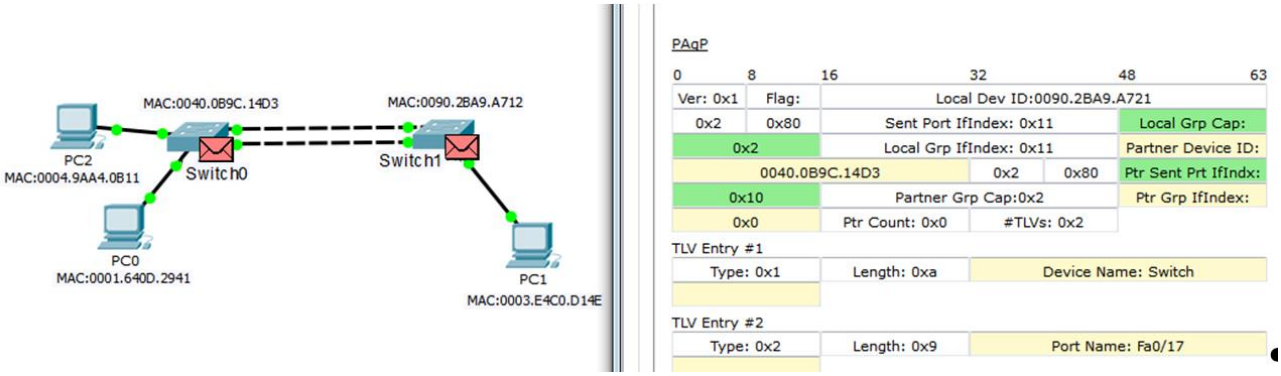

Рисунок 2.5 – Реализация протокола PAgP в смоделированной сети

Использование режима on в протоколах LACP и PAgP подразумевает ручную настройку объединения каналов без использования сообщений согласования и проверки. Обычно такой режим применяется для объединения физических каналов в логический при соединении двух маршрутизаторов, коммутаторов L3 или маршрутизатора с коммутатором. При использовании данного метода необходимо особенно внимательно проверять идентичность настроек интерфейсов. Или осуществить сброс настроек интерфейсов командой `default interface` *`номер_интерфейса`*.

На коммутаторе Switch10, соединенном с коммутатором L3 MultiLayer Switch0 двумя физическими каналами (см. рисунок 2.1), установлен протокол LACP в режиме on следующим образом:

```
Switch6(config)#interface range FastEthernet0/3-4
Switch6(config-if)# channel-group 5 mode on
```

Аналогичным образом осуществляется конфигурация протокола LACP в режиме on для интерфейсов GigabitEthernet1/0/1, GigabitEthernet1/0/2 на коммутаторе L3 MultiLayer Switch0. Для агрегации каналов на маршрутизаторах используются такие же принципы конфигурации, как и для коммутаторов.

Рассмотрим пример настройки агрегированного канала между маршрутизаторами Router1 и Router2 (рисунок 2.6). Сначала необходимо удалить IP-адреса интерфейсов, которые будут добавлены в агрегированный канал, а затем настроить IP-адрес для интерфейса port-channel, который будет использован для агрегирования. Также необходимо в конфигурации интерфейсов указать channel-group.

Так, в примере на рисунке 2.6 на маршрутизаторе Router1 интерфейс GigabitEthernet0/0/0 был изначально соединен с маршрутизатором Router2. Было решено увеличить пропускную способность данного соединения и использовать агрегирование.

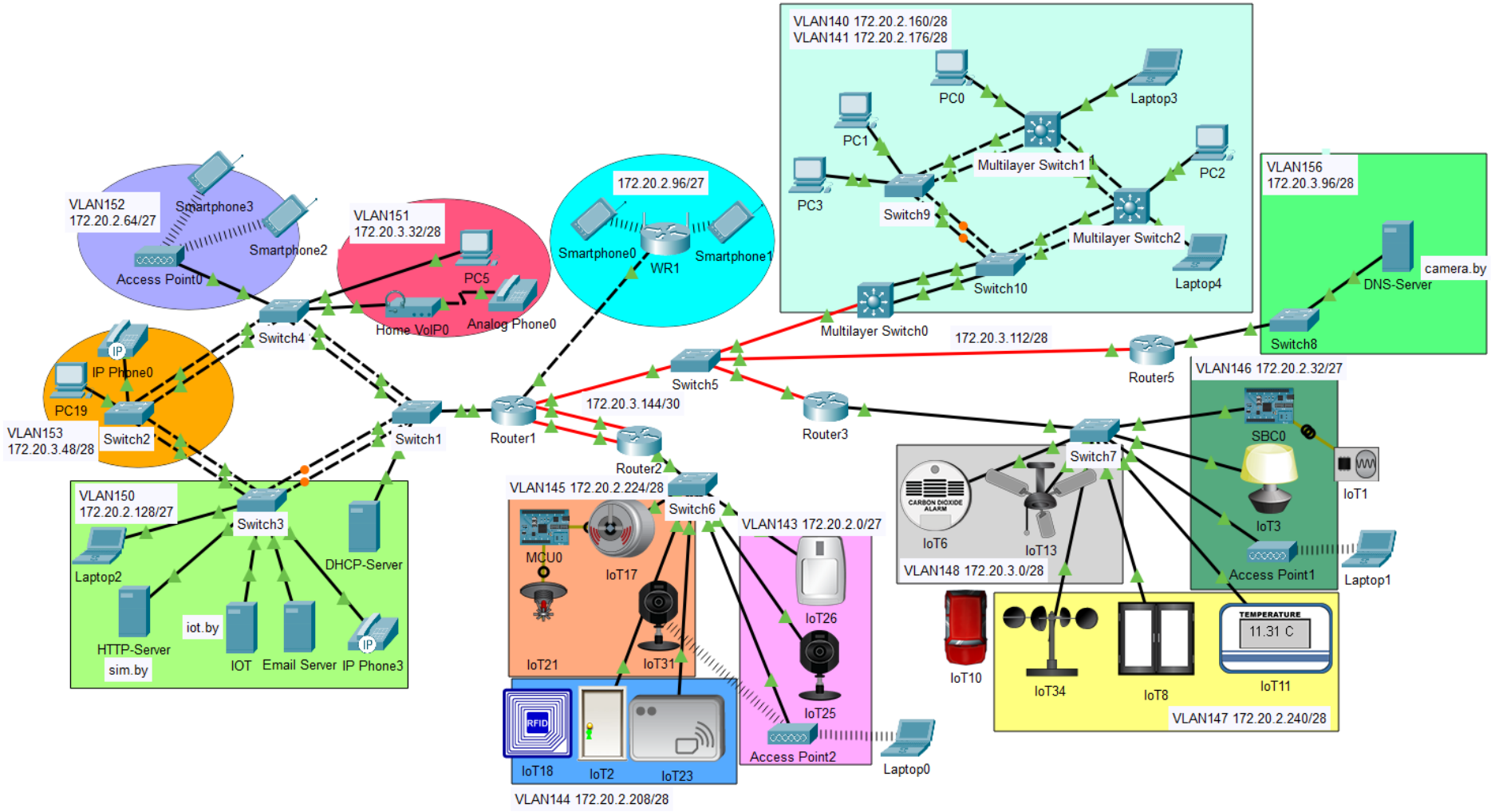

Рисунок 2.6 – Пример сети с агрегацией каналов

Таким образом, агрегация каналов на маршрутизаторе Router1 осуществляется следующим образом:

```
Router1(config)#interface GigabitEthernet0/0/0
Router1(config-if)#no ip address
Router1(config-if)#interface Port-channel1
Router1(config-if)#ip address 172.20.3.145
255.255.255.252
Router1(config-if)#interface GigabitEthernet0/0/0
Router1(config-if)#channel-group 1
Router1(config-if)#interface GigabitEthernet0/2/0
Router1(config-if)#channel-group 1
Router1(config-if)#port-channel load-balance src-ip
```

Проверить результат увеличение пропускной способности за счет агрегации каналов и правильности настройки логического интерфейса port-channel можно с помощью команды `show interfaces` *`тип_номер`* (рисунок 2.7).

```
Router1#show interfaces gigabitEthernet 0/0/0
GigabitEthernet0/0/0 is up, line protocol is up (connected)
  Hardware is Lance, address is 0003.e405.39c6 (bia 0003.e405.39c6)
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Full-duplex, 100Mb/s, media type is RJ45
  ARP type: ARPA, ARP Timeout 04:00:00,
  Last input 00:00:08, output 00:00:05, output hang never
Router1#show interfaces port-channel 1
Port-channel1 is up, line protocol is up (connected)
  Hardware is EtherChannel, address is 0010.11c1.5278 (bia 0010.11c1.5278)
  Internet address is 172.20.3.145/30
  MTU 1500 bytes, BW 2100000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Half-duplex, 2100Mb/s
  input flow-control is off, output flow-control is off
  Members in this channel: Gig0/0/0 ,Gig0/2/0
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:08, output 00:00:05, output hang never
```

Рисунок 2.7 – Проверка конфигурации агрегирования каналов на маршрутизаторе Router1

2.2 Лабораторное задание

Лабораторная работа выполняется на основе настроек, выполненных в лабораторной работе № 1 (файл **LAB1-6.pkt**). До начала выполнения необходимо открыть сохраненный файл **LAB1-6.pkt** и проверить настройки IP-

адресации: у всех устройств адресация должна соответствовать заданному IP-адресу из таблицы 1.2, маршрутизация должна быть настроена по протоколу OSPFv2. В сети должны быть подсети с VLAN, с беспроводным маршрутизатором, подсеть Building1, подсети с устройствами освещения, контроля температуры и дыма, видеонаблюдения, контроля доступа и пожаротушения, три сервера: на одном сервере должны отображаться состояния устройств освещения, контроля температуры и дыма (сервер iot.by на рисунке 1.8), на втором сервере должны отображаться состояния устройств видеонаблюдения, контроля доступа и пожаротушения (сервер camera.by на рисунке 1.8), на третьем – веб-сайт, разработанный в лабораторной работе № 5 лабораторного практикума «Основы построения локальных сетей» [10], доменное имя которого должно соответствовать фамилии студента. С любого устройства из любой подсети должен быть доступ к серверам. Агрегирование каналов между коммутаторами должно быть настроено с помощью протокола PVST для локальной сети Building1 и протокола RSTP для локальной сети с VLAN.

В данной лабораторной работе необходимо организовать агрегирование каналов между коммутаторами и маршрутизаторами с помощью протоколов LACP и PAgP.

1 *Настройка протокола LACP в подсети Building1*. Создать между каждой парой коммутаторов в подсети Building1 по два физических соединения, как показано на рисунке 2.1. Настроить на коммутаторах протокол LACP, номера канальных групп и логических интерфейсов port-channel заданы в таблице 2.1. Проверить соединение. Вставить в отчет информацию о настройке LACP с двух коммутаторов. Сохранить файл под именем **LAB2-1.pkt**.

Таблица 2.1 – Исходные данные для настройки протоколов LACP и PAgP

Номер первой цифры шифра	Номера группы для LACP и PAgP	Метод балансировки
0	1, 2, 3, 4	По MAC-адресу получателя
1	2, 3, 4, 5	По IP-адресу отправителя
2	3, 4, 5, 6	По IP-адресу получателя
3	1, 4, 5, 6	По MAC-адресу отправителя и получателя
4	2, 4, 5, 6	По IP-адресу отправителя и получателя
5	2, 3, 5, 6	По IP-адресу отправителя и получателя
6	1, 2, 5, 6	По MAC-адресу отправителя и получателя
7	1, 2, 4, 5	По IP-адресу отправителя
8	1, 3, 4, 5	По MAC-адресу получателя
9	2, 3, 4, 6	По IP-адресу получателя

2 *Процесс передачи пакетов по протоколу LACP.* Перейти в режим симуляции времени, настроить фильтрацию на LACP-пакеты. Проследить за процессом передачи пакетов между любыми двумя коммутаторами и заполнить таблицу 2.2, определить, какие MAC-адреса используются в полях.

Таблица 2.2 – Содержимое пакета LACP

Номер шага	Содержимое заголовка Ethernet		Содержимое заголовка LACP	
	Destination MAC	Source MAC	Actor System	Partner System
1				
2				

3 *Настройка метода балансировки в соответствии с заданным шифром* (см. таблицу 2.1). Отобразить в отчете результат настройки балансировки нагрузки, осуществить отправку любого пакета с двух любых устройств и проверить правильность распределения по физическим каналам. Сохранить файл под именем **LAB2-3.pkt**.

4 *Настройка протокола PAgP в подсети с VLAN* (см. рисунок 2.4). Осуществить настройку протокола PAgP на всех коммутаторах подсети с VLAN (номера канальных групп и логических интерфейсов port-chanell заданны в таблице 2.1). Проверить соединение. Вставить в отчет информацию о настройке PAgP с двух коммутаторов. Сохранить файл под именем **LAB2-4.pkt**.

5 *Процесс передачи пакетов по протоколу PAgP*. Перейти в режим симуляции времени, настроить фильтрацию на PAgP-пакеты. Проследить за процессом передачи пакетов между коммутаторами и заполнить таблицу 2.3, определить, какие MAC-адреса используются в полях. Сделать вывод об особенностях передачи.

Таблица 2.3 – Содержимое пакета PAgP

Номер шага	Содержимое заголовка Ethernet		Содержимое заголовка PAgP			
	Destination MAC	Source MAC	Actor System	Partner System	Имя устройства	Порт
1						
2						

6 *Настройка метода балансировки в соответствии с заданным шифром на всех коммутаторах* (см. таблицу 2.1). Отобразить в отчете результат настройки балансировки нагрузки, осуществить отправку любого пакета с двух

любых устройств и проверить правильность распределения по физическим каналам. Сохранить файл под именем **LAB2-6.pkt**.

7 *Настройка агрегирования между маршрутизаторами*. Выбрать две пары маршрутизаторов и настроить на них агрегацию каналов и балансировку нагрузки (см. рисунок 2.6). Вставить в отчет информацию о настройке агрегации каналов на маршрутизаторах. Сохранить файл под именем **LAB2-7.pkt**.

2.3 Содержание отчета

1 Цель работы, исходные данные из таблицы 2.1.

2 Результаты произведенных настроек (заполненные таблицы 2.2 и 2.3, результаты произведенных настроек из пунктов 1–7), изображение смоделированной сети.

3 Вывод по работе.

4 Ответы на контрольные вопросы.

2.4 Контрольные вопросы

1 Назначение агрегации каналов.

2 Технологии и методы агрегации каналов, отличительные особенности.

3 Условия настройки агрегации на коммутаторах и основные правила.

4 Протокол LACP, механизм настройки и принцип работы.

5 Отличительные особенности LACP и PAgP.

6 Настройка протокола PAgP, особенности работы.

7 Методы балансировки нагрузки, особенности их настройки.

8 Конфигурация агрегации каналов между маршрутизаторами и коммутаторами.

ЛАБОРАТОРНАЯ РАБОТА № 3
ТРАНСЛЯЦИЯ СЕТЕВЫХ АДРЕСОВ

Цель работы: изучить назначение и принципы трансляции IP-адресов, овладеть навыками конфигурации статического и динамического NAT и PAT для одного и нескольких IP-адресов.

3.1 Теоретическая часть

NAT (Network Address Translation) – трансляция сетевых адресов, технология, которая позволяет преобразовывать (изменять) IP-адреса и порты в сетевых пакетах [7]. NAT чаще всего используется для осуществления доступа из корпоративной (частной) сети в интернет либо, наоборот, для доступа из интернета на какой-либо ресурс внутри сети. В таких сетях обычно используются частные IP-адреса, которые не маршрутизируются в интернете, и провайдеры должны отбрасывать пакеты с такими IP-адресами отправителей или получателей. Для преобразования частных адресов в глобальные (маршрутизируемые в интернете) и применяют NAT.

Помимо возможности доступа в глобальную сеть, NAT имеет еще несколько преимуществ. Так, например, трансляция сетевых адресов позволяет скрыть внутреннюю структуру сети и ограничить к ней доступ, что повышает безопасность. Также эта технология позволяет экономить глобальные IPv4-адреса, т. к. одним глобальным адресом в интернете может пользоваться множество устройств.

Частные адреса используются внутри организации для осуществления локального взаимодействия устройств. При этом частные IP-адреса не идентифицируют какую-либо отдельную компанию или организацию и их нельзя маршрутизировать через глобальную сеть. Чтобы разрешить устройству с частным IPv4-адресом получать доступ к устройствам и ресурсам за пределами локальной сети, частный адрес должен сначала быть преобразован в публичный адрес. Технология NAT обеспечивает преобразование частных адресов в публичные адреса. Это позволяет устройству с частным IPv4-адресом получать доступ к ресурсам за пределами корпоративной сети. NAT в сочетании с частными адресами IPv4 оказался полезным методом сохранения общедоступных адресов IPv4. Один общедоступный IPv4-адрес может использоваться сотнями и тысячами устройствами, каждое из которых имеет уникальный частный IPv4-адрес.

Маршрутизатор NAT обычно работает на границе сети, которая имеет только одно соединение с внешними сетями.

В терминологии NAT внутренняя сеть – это набор сетей, IP-адреса которых подлежат трансляции. Внешняя сеть относится ко всем другим сетям. При

использовании NAT IPv4-адреса имеют разные обозначения в зависимости от того, находятся ли они в частной или публичной сети, а также от того, является ли трафик входящим или исходящим.

Можно выделить четыре типа адресов в технологии NAT:

– внутренний локальный адрес;

– внутренний глобальный адрес;

– внешний локальный адрес;

– внешний глобальный адрес.

Внутренний адрес – адрес устройства, который транслируется с помощью NAT, **внешний адрес** – адрес устройства назначения. **Локальный адрес** – адрес во внутренней сети, **глобальный адрес** – адрес во внешней сети. На рисунке 3.1 компьютер имеет внутренний локальный адрес 192.168.20.20. С точки зрения компьютера веб-сервер имеет внешний адрес 220.0.45.20. Когда пакеты отправляются с компьютера на глобальный адрес веб-сервера, внутренний локальный адрес преобразуется в 226.200.125.52 (внутренний глобальный адрес). Адрес внешнего устройства не транслируется, потому что этот адрес является публичным IPv4-адресом.

Таким образом, компьютер имеет разные локальные и глобальные адреса, тогда как веб-сервер имеет один общедоступный адрес IPv4. С точки зрения веб-сервера сообщения пришло от внутреннего глобального адреса 226.200.125.52. В данном примере маршрутизатор Router1 является точкой разграничения между внутренней и внешней сетями, а также между локальными и глобальными адресами.

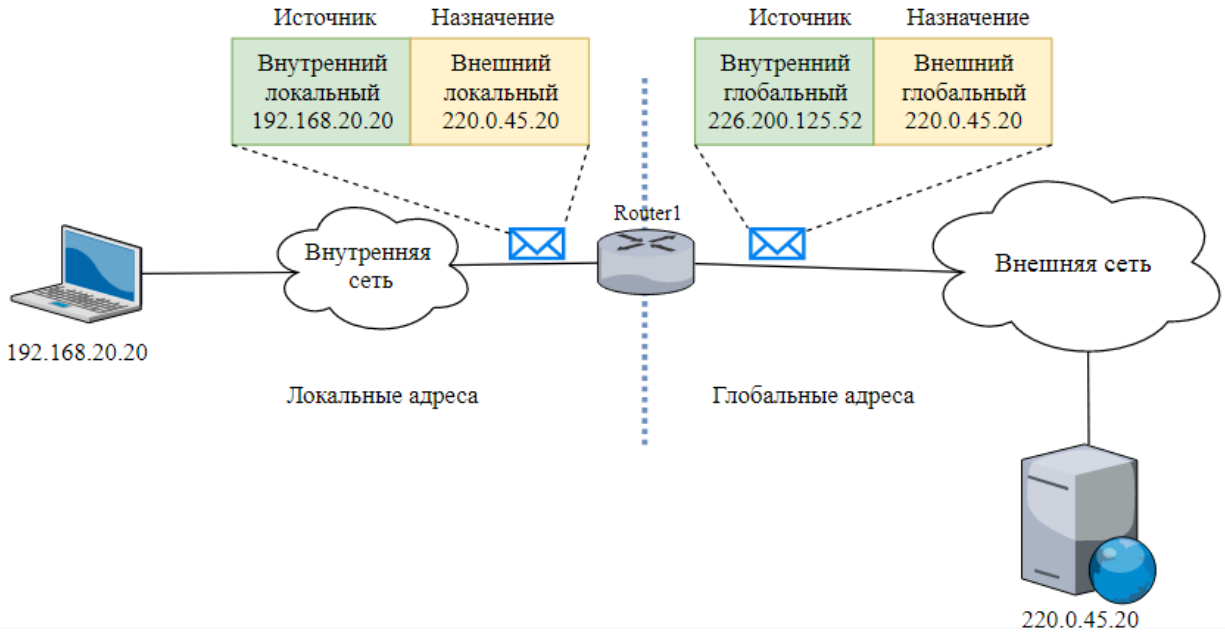

Рисунок 3.1 – Типы адресов в технологии NAT

Настройка NAT на маршрутизаторах включает в себя следующие шаги:

– назначение внутреннего (Inside) и внешнего (Outside) интерфейсов;

– определение IP-адресов для трансляции;

– выбор вида трансляции;

– проверка трансляции.

Существует три вида трансляции [8]:

– Static NAT (статический NAT) – преобразование IP-адреса один к одному, т. е. сопоставляется один адрес из внутренней сети с одним адресом из внешней сети;

– Dynamic NAT (динамический NAT) – преобразование внутреннего адреса(-ов) в один из группы внешних адресов;

– Port Address Translation (PAT), или Overloading – преобразование несколько внутренних адресов в один внешний.

При использовании статического NAT после отправки сообщения с устройства внутренней сети маршрутизатор преобразует внутренний локальный адрес во внутренний глобальный адрес. Статический NAT особенно полезен для веб-серверов или устройств, которые должны иметь постоянный адрес, доступный из глобальной сети. Также статический NAT может применяться для устройств, которые должны быть доступны для авторизованного персонала вне сети, например, доступ по SSH к настройкам сетевого оборудования. Основное требование при использование статического NAT – доступность достаточного количества адресов.

Динамический NAT использует пул публичных адресов и назначает их в порядке очереди. Когда внутреннее устройство запрашивает доступ к внешней сети, динамический NAT назначает доступный общедоступный IPv4-адрес из пула.

Port Address Translation (PAT), или Overloading, сопоставляет несколько частных адресов IPv4 с одним общедоступным адресом IPv4. В большинстве случаев домашние маршрутизаторы используют именно эту технологию трансляции IPv4-адресов. Интернет-провайдер назначает маршрутизатору один адрес, но несколько устройств, подключенных к одному домашнему маршрутизатору, могут одновременно иметь доступ к интернету.

Рассмотрим примеры конфигурации разных методов трансляции IPv4-адресов для сети (см. рисунок 2.6). В таблице 3.1 показано, что для внутренних подсетей используются частные IPv4-адреса, а для соединения маршрутизаторов – публичные. При отсутствии трансляции IPv4-адресов пакеты передаются без изменения адресов (рисунок 3.2). Рассмотрим пример конфигурации статического NAT для подсети с устройствами IoT.

Таблица 3.1 – Использование частных и публичных IPv4-адресов

Название подсети	Частные IP-адреса подсетей	Публичные IP-адреса подсетей	Вид NAT/PAT
VLAN 140	172.20.2.160/28	122.20.0.0/29	Динамический NAT
VLAN 141	172.20.2.176/28	122.20.0.8/29	
VLAN 142	172.20.2.192/28	122.20.0.16/29	
VLAN 143	172.20.2.0/27	122.20.0.24/29	Динамический PAT
VLAN 144	172.20.2.208/28		
VLAN 145	172.20.2.224/28		
VLAN 146	172.20.2.32/27	122.20.0.76/29	PAT
VLAN 147	172.20.2.240/28		
VLAN 148	172.20.3.0/28		
VLAN 150	172.20.2.128/27	122.20.0.48/29	Статический NAT
VLAN 151	172.20.3.32/28	122.20.0.73/29	PAT
VLAN 152	172.20.2.64/27		
VLAN 153	172.20.3.48/28		
VLAN 154	172.20.3.64/28		
VOIP	172.20.3.80/28		
VLAN 156	172.20.3.96/28	122.20.0.64/29	Статический NAT
WLAN	172.20.2.96/27	PAT 122.20.0.117/30	PAT
Router1 – Router2	172.20.3.144/30	122.20.0.112/30	–
Router1 – WR1	172.20.3.148/30	122.20.0.116/30	–
Router1 – Router3 – Router5 – MS0	172.20.3.112/28	122.20.0.72/29	–

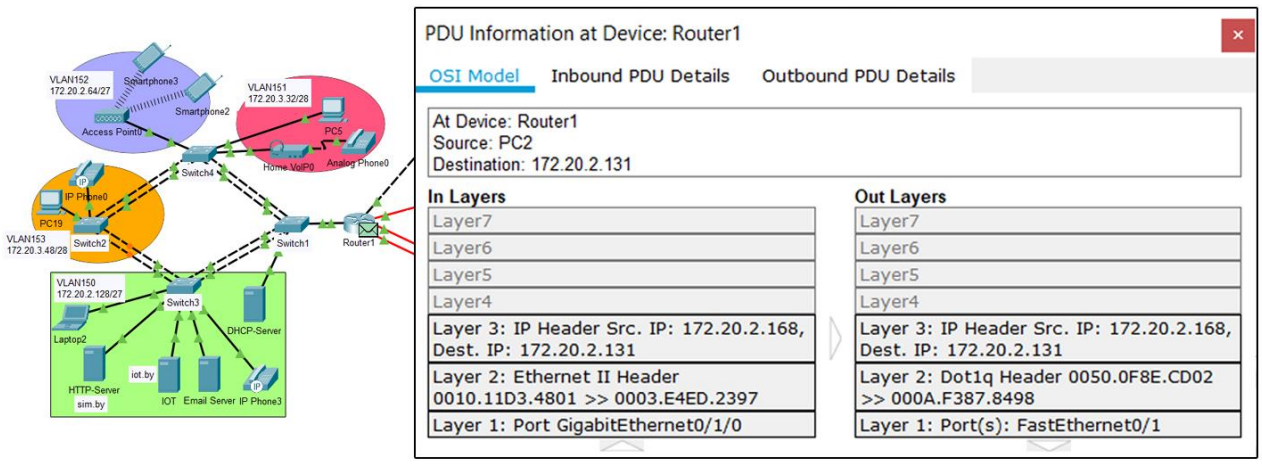

Рисунок 3.2 – Передача пакета в сети без трансляции IPv4-адреса

Для конфигурации статического NAT необходимо выполнить следующие действия:

– спланировать сопоставление внутренних локальных и внутренних глобальных IPv4-адресов (таблица 3.2);

– осуществить конфигурацию статического NAT с помощью команды `ip nat inside source static` *`Внутренний_локальный_адрес Внутренний_глобальный_адрес`*;

– определить, какие интерфейсы маршрутизатора относятся к внутренней сети;

– осуществить конфигурацию NAT на интерфейсах с указанием их подключения к внутренней сети с помощью команды `ip nat inside`;

– определить, какие интерфейсы маршрутизатора относятся к внешней сети;

– осуществить конфигурацию NAT на интерфейсах с указанием их подключения к внешней сети с помощью команды `ip nat outside`.

Таблица 3.2 – Сопоставление внутренних локальных и внутренних глобальных IPv4-адресов для подсети Building1

Наименование устройства	Внутренний локальный адрес	Внутренний глобальный адрес
HTTP-Server	172.20.2.133/27	122.20.0.50/29
IoT	172.20.2.131/27	122.20.0.51/29
Email Server	172.20.2.132/27	122.20.0.52/29
DHCP-Server	172.20.2.130/27	122.20.0.53/29

Представим пример конфигурации статического NAT для маршрутизатора Router1 (см. рисунок 3.2). Сначала в соответствии с таблицей 3.1 с помощью команд назначаем, какими внутренними глобальными IPv4-адресами будут заменяться внутренние локальные адреса:

```
Router1(config)#ip nat inside source static 172.20.2.133
122.20.0.50
Router1(config)#ip nat inside source static 172.20.2.131
122.20.0.51
Router1(config)#ip nat inside source static 172.20.2.132
122.20.0.52
Router1(config)#ip nat inside source static 172.20.2.130
122.20.0.53
```

Далее определяем, что интерфейс GigabitEthernet0/0 является внутренним, а интерфейсы GigabitEthernet0/2/0 и GigabitEthernet0/3/0 – внешними, на основе чего осуществляем настройку NAT с помощью следующих команд:

```
Router1(config)#interface GigabitEthernet0/0/0
Router1(config-if)#ip nat outside
Router1(config)#interface port-channel 1
Router1(config-if)#ip nat outside
Router1(config)#interface GigabitEthernet0/1.150
Router1(config-if)#ip nat inside
```

В результате анализа процесса передачи пакетов в режиме симуляции можно увидеть, что при передаче пакета из внутренней сети во внешнюю маршрутизатор осуществляет замену внутреннего локального IPv4-адреса 172.20.2.133 на внутренний глобальный адрес 122.20.0.50. При передаче пакета из внешней сети во внутреннюю маршрутизатор осуществляет обратную трансляцию IPv4-адреса (рисунок 3.3).

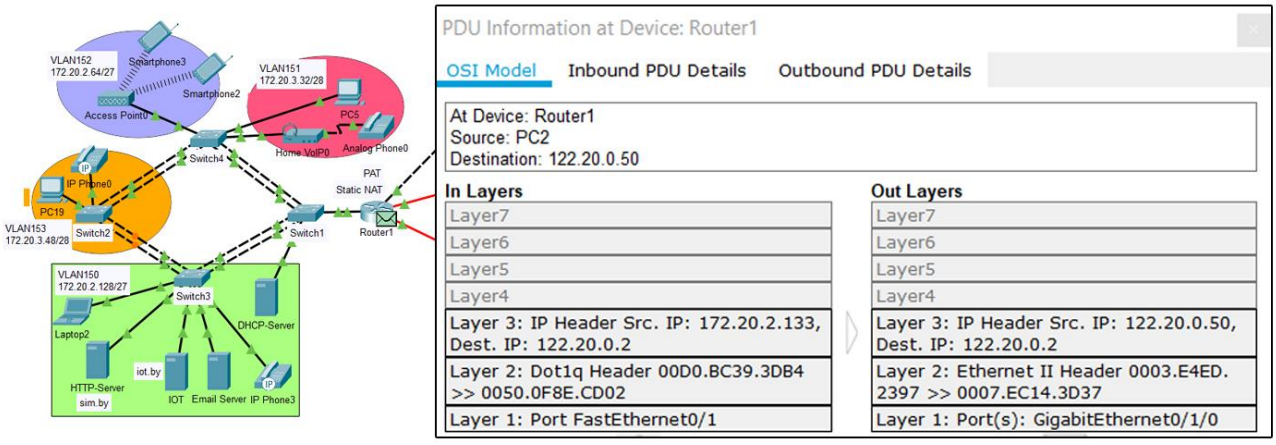

Рисунок 3.3 – Процесс замены внутреннего локального IPv4-адреса на внутренний глобальный адрес

Также проверить правильность конфигурации NAT можно с помощью команды `show ip nat translations`, результат которой представлен на рисунке 3.4. Как видно из рисунка, с помощью данной команды можно проверить трансляцию IPv4-адресов для всех пакетов, переданных маршрутизатором.

```
Router1#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
---  122.20.0.50       172.20.2.133       ---                ---
---  122.20.0.51       172.20.2.131       ---                ---
---  122.20.0.52       172.20.2.132       ---                ---
---  122.20.0.53       172.20.2.130       ---                ---
tcp 122.20.0.50:80     172.20.2.133:80    122.20.0.2:1029    122.20.0.2:1029
tcp 122.20.0.51:31000  172.20.2.131:31000 122.20.0.76:1024   122.20.0.76:1024
tcp 122.20.0.51:31000  172.20.2.131:31000 122.20.0.76:1025   122.20.0.76:1025
tcp 122.20.0.51:31000  172.20.2.131:31000 122.20.0.76:1026   122.20.0.76:1026
tcp 122.20.0.51:31000  172.20.2.131:31000 122.20.0.76:1027   122.20.0.76:1027
tcp 122.20.0.51:31000  172.20.2.131:31000 122.20.0.76:1028   122.20.0.76:1028
tcp 122.20.0.51:31000  172.20.2.131:31000 122.20.0.76:1029   122.20.0.76:1029
tcp 122.20.0.51:80     172.20.2.131:80    122.20.0.2:1025    122.20.0.2:1025
tcp 122.20.0.51:80     172.20.2.131:80    122.20.0.2:1026    122.20.0.2:1026
tcp 122.20.0.51:80     172.20.2.131:80    122.20.0.2:1027    122.20.0.2:1027
tcp 122.20.0.51:80     172.20.2.131:80    122.20.0.2:1028    122.20.0.2:1028
```

Рисунок 3.4 – Проверка трансляции IPv4-адресов для каждого переданного пакета маршрутизатора

С помощью команды `show ip nat statistics` можно получить краткую информацию о настроенных типах интерфейсов (внутренних и внешних) и общем количестве пакетов, подвергнутых трансляции (рисунок 3.5).

```
Router1#show ip nat statistics
Total translations: 15 (4 static, 11 dynamic, 11 extended)
Outside Interfaces: GigabitEthernet0/1/0 , FastEthernet1/0 , Port-channel1
Inside Interfaces: FastEthernet0/1.150 , FastEthernet0/1.151 , FastEthernet0/1.152 ,
FastEthernet0/1.153 , FastEthernet0/1.154
Hits: 1033  Misses: 1041
Expired translations: 0
Dynamic mappings:
```

Рисунок 3.5 – Краткая информация о конфигурации NAT

Для конфигурации динамического NAT необходимо выполнить следующие действия.

1 Определить пул адресов, которые будут использоваться для трансляции, с помощью команды `ip nat pool` *`имя_пула начальный_IP-адрес конечный_IP-адрес`* `netmask` *`маска_подсети`*. Пул адресов обычно является группой публичных адресов. Адреса определяются путем указания начального IP-адреса и конечного IP-адреса пула. С помощью netmask задается маска для указанных в команде адресов.

2 Конфигурация стандартного списка контроля доступа (ACL) для разрешения трансляции только тех адресов, которые будут указаны, с помощью

команды access-list *номер_ACL* permit *IP-адрес_внутренней_сети обратная_маска_внутренней_сети*.

3 Установить связь созданного ACL с пулом с помощью команды ip nat inside source list *номер_ACL* pool *имя_пула*. Эта конфигурация используется маршрутизатором для определения того, какие устройства (номер_ACL) какие адреса (имя_пула) получают.

4 Определить, какие интерфейсы маршрутизатора относятся к внутренней сети, осуществить конфигурацию NAT на интерфейсах с указанием их подключения к внутренней сети с помощью команды ip nat inside.

5 Определить, какие интерфейсы маршрутизатора относятся к внешней сети. Осуществить конфигурацию NAT на интерфейсах с указанием их подключения к внешней сети с помощью команды ip nat outside.

Для коммутатора L3 и VLAN 140 (см. рисунок 2.6) конфигурация динамического NAT производится с помощью следующих команд:

```
MS0(config)#access-list 40 permit 172.20.2.160 0.0.0.15
MS0(config)#ip nat pool NATvlan140 122.20.0.2 122.20.0.6
netmask 255.255.255.248
MS0(config)#ip nat inside source list 40 pool NATvlan140
```

В соответствии с представленными выше командами сначала осуществляется конфигурация списка контроля доступа ACL с номером 40, который предназначен для разрешения (permit) трансляции IPv4-адресов из подсети с адресом 172.20.2.160/28. Далее создается пул публичных IP-адресов под именем NATvlan140, в котором будут использоваться IPv4-адреса из диапазона 122.20.0.2–122.20.0.6. Также указывается маска подсети 122.20.0.0/29, соответствующая настроенному диапазону IP-адресов. Последняя команда предназначена для связи созданного ACL под номером 40 и пула NAT с именем NATvlan140. В случае необходимости динамической трансляции IP-адресов для других VLAN нужно добавить в список контроля доступа IP-адреса подсетей других VLAN или создать новый ACL и пул. Конфигурация динамического NAT на интерфейсах производится аналогично конфигурации статического NAT. Как правило, из маршрутизации OSPF удаляются частные IP-адреса локальных подсетей с помощью команды no network 172.20.2.160 0.0.0.15 area 20. Необходимо отметить, что для серверов предпочтительно настраивать отдельный статический NAT.

В результате произведенных конфигураций динамического NAT трансляция будет осуществляться, однако пакеты обратно приходить не будут, т. к. адрес подсети 122.20.0.0/29, указанный в пуле NAT, не маршрутизируется. Таким

образом, необходимо добавить IP-адрес 122.20.0.0/29 в маршрутизацию OSPF. Известно, что в пакетах OSPF передаются IP-адреса подсетей, если они подключены напрямую, т. е. настроены на интерфейсах маршрутизатора. Поэтому недостаточно только добавить IP-адрес 122.20.0.0/29 в маршрутизацию OSPF, также необходимо создать виртуальный интерфейс и назначить на нем IP-адрес из указанной подсети. Как правило, для этих целей используется интерфейс loopback или sub-интерфейс. Например, на коммутаторе L3 можно создать sub-интерфейс с IP-адресом 122.20.0.1/29 и добавить IP-адрес 122.20.0.0/29 в маршрутизацию OSPF, и только после этого данная подсеть будет добавлена в таблицы маршрутизации остальных маршрутизаторов.

Проверить правильность конфигурации NAT можно с помощью команды `show ip nat translations` (см. рисунок 3.4). Для очистки динамических записей NAT используется команда режима `clear ip nat translation *`.

В режиме реального времени проследить за корректностью трансляции можно с помощью команды `debug ip nat`, которая отображает информацию о результате трансляции IP-адреса в момент прохождения пакета через маршрутизатор (рисунок 3.6). Для отключения функции демонстрации процесса преобразования IP-адресов на маршрутизаторе используется команда `no debug ip nat`.

```
MS0#debug ip nat
IP NAT debugging is on
MS0#
NAT: s=172.20.2.163->122.20.0.2, d=122.20.0.66 [57]

NAT*: s=122.20.0.66, d=122.20.0.2->172.20.2.163 [657]

NAT: s=172.20.2.163->122.20.0.2, d=122.20.0.50 [58]

NAT*: s=122.20.0.50, d=122.20.0.2->172.20.2.163 [4]

NAT*: s=172.20.2.163->122.20.0.2, d=122.20.0.50 [59]

NAT*: s=172.20.2.163->122.20.0.2, d=122.20.0.50 [60]

NAT*: s=122.20.0.50, d=122.20.0.2->172.20.2.163 [5]

NAT*: s=172.20.2.163->122.20.0.2, d=122.20.0.50 [61]
```

Рисунок 3.6 – Отображение информации о трасляции IP-адресов

При трансляции PAT адреса сохраняются во внутреннем глобальном пуле, позволяя маршрутизатору использовать один внутренний глобальный адрес

для многих внутренних локальных адресов. Когда этот тип трансляции настроен, маршрутизатор сохраняет информацию из протоколов более высокого уровня, например, номера портов TCP или UDP, для преобразования внутреннего глобального адреса обратно в правильный внутренний локальный адрес. Общее количество внутренних адресов, которые можно преобразовать в один внешний адрес, теоретически может достигать 65 536.

Существует два способа настройки PAT в зависимости от выделяемого количества публичных IPv4-адресов: PAT для диапазона публичных IP-адресов (динамический PAT) и PAT для одного публичного IP-адреса (статический PAT). В случае если выдается более одного IPv4-адреса, принцип конфигурации PAT похож на конфигурацию динамического NAT, т. е. также создается пул. Рассмотрим необходимые действия для конфигурации PAT для диапазона публичных IP-адресов (динамический PAT).

1 Определить пул глобальных адресов, которые будут использоваться для трансляции, с помощью команды `ip nat pool` *`имя_пула начальный_IP-адрес конечный_IP-адрес netmask маска_подсети`*. Пул адресов обычно является группой публичных адресов. Адреса определяются путем указания начального IP-адреса и конечного IP-адреса пула. С помощью `netmask` указывается маска для подсети.

2 Конфигурация стандартного списка контроля доступа (ACL) для разрешения трансляции только тех адресов, которые будут указаны, с помощью команды `access-list` *`номер_ACL`* `permit` *`IP-адрес_внутренней_сети обратная_маска_внутренней_сети`*.

3 Установить связь созданного ACL с пулом и типом NAT с помощью команды `ip nat inside source list` *`номер_ACL`* `pool` *`имя_пула`* `overload`.

4 Определить, какие интерфейсы маршрутизатора относятся к внутренней сети, осуществить конфигурацию NAT на интерфейсах с указанием их подключения к внутренней сети с помощью команды `ip nat inside`.

5 Определить, какие интерфейсы маршрутизатора относятся к внешней сети. Осуществить конфигурацию NAT на интерфейсах с указанием их подключения к внешней сети с помощью команды `ip nat outside`.

Конфигурация PAT для диапазона публичных IP-адресов для маршрутизатора Router2 и VLAN 143 (см. рисунок 2.6) производилась следующим образом:

```
Router2(config)#ip nat pool NAT1 122.20.0.25 122.20.0.30
netmask 255.255.255.248
Router2(config)#access-list 20 permit 172.20.2.0 0.0.0.15
```

```
Router2(config)# ip nat inside source list 20 pool NAT1
overload
```

Конфигурация PAT на интерфейсах производится аналогично конфигурации статического или динамического NAT. Из маршрутизации OSPF исключается рассылка IPv4-адреса подсети 172.20.0.0/28, IPv4-адрес 122.20.0.25/29 присваивается sub-интерфейсу и добавляется в маршрутизацию OSPF.

В случае если выделяется один публичный IPv4-адрес (статический PAT), то принцип конфигурации PAT включает следующие этапы.

1 Конфигурация стандартного списка контроля доступа (ACL) для разрешения трансляции только тех адресов, которые будут указаны, с помощью команды `access-list` *`номер_ACL`* `permit` *`IP-адрес_внутренней_сети обратная_маска_внутренней_сети`*.

2 Конфигурация PAT с указанием номера списка контроля доступа и типа и номера интерфейса, IP-адрес которого будет использован для трансляции, с помощью команды `ip nat inside source list` *`номер_ACL`* `interface` *`тип_номер`* `overload`.

3 Определение интерфейсов маршрутизатора, которые относятся к внутренней сети, конфигурация NAT на интерфейсах с указанием их подключения к внутренней сети с помощью команды `ip nat inside`.

4 Определение интерфейсов маршрутизатора, которые относятся к внешней сети, конфигурация NAT на интерфейсах с указанием их подключения к внешней сети с помощью команды `ip nat outside`.

Конфигурация PAT для маршрутизатора Router1 и VLAN 151 (см. рисунок 2.6) производилась следующим образом:

```
Router1(config)# access-list 20 permit 172.20.3.32
0.0.0.15
Router1(config)# ip nat inside source list 20 interface
GigabitEthernet0/1/0 overload
```

Как видно из представленных выше команд, был создан список контроля доступа под номером 20, который разрешает трансляцию IPv4-адреса из подсети 172.20.0.32/28. Далее данный номер списка контроля доступа указывается в конфигурации NAT вместе с типом и номером интерфейса (GigabitEthernet0/1/0), IPv4-адрес которого использован в качестве внутреннего глобального адреса. Ключевое слово overload указывает на PAT.

3.2 Лабораторное задание

Лабораторная работа выполняется на основе настроек, выполненных в лабораторной работе № 2 (файл **LAB2-7.pkt**). До начала выполнения необходимо открыть сохраненный файл **LAB2-7.pkt** и проверить настройки IP-адресации: у всех устройств адресация должна соответствовать заданному IP-адресу из таблицы 1.2, маршрутизация должна быть настроена по протоколу OSPFv2. В сети должны быть подсети с VLAN и беспроводным маршрутизатором, подсеть Building1, подсети с устройствами освещения, контроля температуры и дыма, видеонаблюдения, контроля доступа и пожаротушения, три сервера: на одном сервере должны отображаться состояния устройств освещения, контроля температуры и дыма (сервер iot.by на рисунке 1.8), на втором сервере должны отображаться состояния устройств видеонаблюдения, контроля доступа и пожаротушения (сервер camera.by на рисунке 1.8), на третьем – веб-сайт, разработанный в лабораторной работе № 5 лабораторного практикума «Основы построения локальных сетей» [10], доменное имя которого должно соответствовать фамилии студента. С любого устройства из любой подсети должен быть доступ к серверам. Агрегирование каналов между коммутаторами должно быть настроено с помощью протокола PVST и LACP для локальной сети Building1 и протокола RSTP и PAgP для локальной сети с VLAN.

В данной практической работе необходимо осуществить конфигурацию статического и динамического NAT и PAT.

1 *Конфигурация публичных IPv4-адресов*. Осуществить настройку на внешних интерфейсах всех маршрутизаторов публичных IPv4-адресов в соответствии с исходными данными из таблицы 3.3. Заполнить таблицу 3.4 по аналогии с примером из таблицы 3.1. Представить в отчете изображение смоделированной подсети с подписями IPv4-адресов всех подсетей (рисунок 3.7).

Таблица 3.3 – Исходные данные для конфигурации публичных IP-адресов

Третья цифра шифра	IP-адрес публичной сети
0	160.60.2.0/25
1	152.85.85.0/25
2	21.51.10.0/25
3	123.192.2.0/25
4	52.17.10.0/25
5	36.65.14.0/25
6	43.200.58.0/25
7	124.58.1.0/25
8	70.15.6.0/25
9	69.59.73.0/25

Таблица 3.4 – Использование частных и публичных IPv4-адресов

Название подсети	Частные IP-адреса подсетей	Публичные IP-адреса подсетей	Вид NAT/PAT

2 *Конфигурация статического NAT*. Заполнить таблицу 3.5, отразить в ней сопоставление внутренних локальных и глобальных IPv4-адресов для всех серверов. Осуществить настройку статического NAT на маршрутизаторах, к которым подключены VLAN с серверами. Отразить в отчете результат успешной трансляции IPv4-адресов по примеру рисунка 3.2, а также результаты выполнения команд `show ip nat translations` и `show ip nat statistics`. Сохранить файл под именем **LAB3-1.pkt**.

Таблица 3.5 – Сопоставление внутренних локальных и глобальных IPv4-адресов для серверов

Наименование устройства	Внутренний локальный адрес	Внутренний глобальный адрес

3 Осуществить настройку динамического NAT для VLAN, подключенных к коммутатору L3. В качестве названия пула адресов, которые будут использованы для трансляции, использовать собственную фамилию. Отразить в отчете результат успешной трансляции IPv4-адресов (см. рисунки 3.2 и 3.5), а также результаты выполнения команд `show ip nat translations` и `show ip nat statistics`. Сохранить файл под именем **LAB3-2.pkt**.

4 Осуществить настройку PAT для диапазона публичных IP-адресов (динамический PAT) на маршрутизаторе, подключенном к подсетям VLAN с устройствами систем контроля дыма, освещения, температуры. Для пула публичных IP-адресов использовать адреса из таблицы 3.3. Для номера списка контроля доступа использовать последние две цифры шифра. Отразить в отчете результат успешной трансляции IPv4-адресов (см. рисунки 3.2 и 3.5), а также результаты выполнения команд `show ip nat translations` и `show ip nat statistics`. Сохранить файл под именем **LAB3-3.pkt**.

5 Осуществить настройку PAT для одного публичного IP-адреса (статический PAT) на маршрутизаторах, подключенных ко всем остальным подсетям VLAN, для которых в предыдущих пунктах не был настроен NAT или PAT.

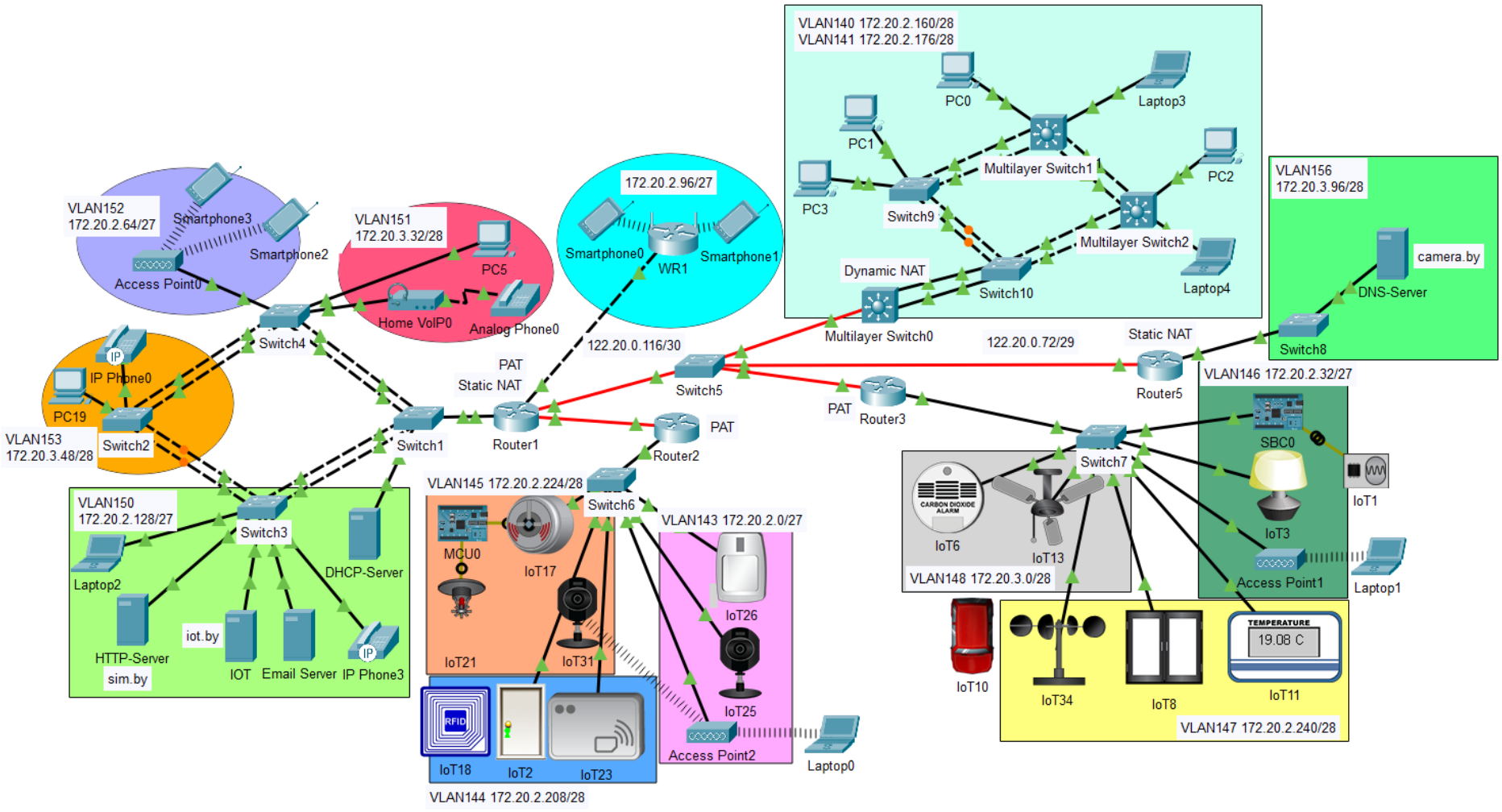

Рисунок 3.7 – Пример смоделированной сети с разными видами трансляции IPv4-адресов

Для номеров списков контроля доступа использовать последнюю цифру шифра. Отразить в отчете результат успешной трансляции IPv4-адресов (см. рисунки 3.2 и 3.5), а также результаты выполнения команд `show ip nat translations` и `show ip nat statistics`. Сохранить файл под именем **LAB3-4.pkt**.

3.3 Содержание отчета

1 Цель работы, исходные данные в соответствии с вариантом из таблицы 3.3, изображение смоделированной сети.

2 Результаты, полученные в результате выполнения пунктов 2–5, заполненные таблицы 3.4 и 3.5.

3 Вывод по работе.

4 Ответы на контрольные вопросы.

3.4 Контрольные вопросы

1 Определение и назначение технологии NAT. Типы адресов NAT.

2 Различия в видах трансляции IP-адресов.

3 Последовательность действий и примеры конфигурации статического NAT. Способы проверки конфигурации NAT.

4 Последовательность действий и примеры конфигурации динамического NAT.

5 Последовательность действий и примеры конфигурации PAT для диапазона публичных IP-адресов.

6 Последовательность действий и примеры конфигурации PAT для одного публичного IP-адреса.

ЛАБОРАТОРНАЯ РАБОТА № 4
СОВМЕСТНОЕ ИСПОЛЬЗОВАНИЕ ПРОТОКОЛОВ IPV4 И IPV6

Цель: изучить принципы трансляции IPv6 и методы совместного использования протоколов IPv4 и IPv6, овладеть навыками применения методов двойного стека, туннелирования и преобразования IP-адресов (NAT-PT) для объединения сетей IPv4 и IPv6.

4.1 Теоретическая часть

Целью внедрения протокола IPv6 является преодоление ограничения адресных ресурсов IPv4. Протокол IPv6 предлагает более обширный запас адресов, но при этом не является совместимым с протоколом IPv4. Это означает, что устройство, поддерживающее только IPv6, не может взаимодействовать с устройством IPv4, что существенно усложняет процесс перехода к протоколу IPv6 [9].

Другим фактором, объясняющим недостаточные темпы внедрения IPv6, является проблема, свойственная многим технологическим изменениям, которая заключается в том, что на начальных стадиях внедрения преимущества технологии (как технические, так и экономические) проявляются лишь в незначительной степени. После достижения критической точки ситуация радикально меняется в пользу новой технологии, и ее внедрение форсируется более естественными факторами. Такой критической точкой можно будет считать момент, когда подсоединение нового IPv6 устройства будет дешевле, чем устройства, поддерживающего протокол IPv4. Однако в настоящее время внедрение IPv6 означает инвестиции, которые не являются краткосрочно прибыльными.

Незначительный уровень внедрения также отрицательно влияет на общую осведомленность относительно IPv6, на отсутствие необходимого уровня квалификации и знаний в этой области, а также на недостаточно эффективный процесс разработки и улучшения оборудования через цикл реального использования и поддержки.

На сегодняшний день решением проблемы является совместное использование IPv4- и IPv6-протоколов. Можно выделить три основных метода совместного использования протоколов IPv4 и IPv6: двойной стек, туннелирование и трансляция IP-адресов.

Самым простым методом обеспечения совместимости между IPv4 и IPv6 является двойной стек (Dual stack). Его суть заключается в том, что на каждом узле сети, который работает с IPv6 и которому требуется взаимодействие с IPv4-сетями, устанавливается стек протокола IPv4, т. е. назначается IPv4-адрес (рисунок 4.1). Таким образом, данный узел может передавать данные устройствам, работающим с разными версиями протокола IP. Главным пре-

имуществом принципа двойного стека является относительная простота. При этом можно выделить следующие недостатки:

– для работы двойного стека необходимо, чтобы большинство промежуточных маршрутизаторов глобальной сети работали как с протоколом IPv4, так и с протоколом IPv6, т. е. на интерфейсах маршрутизаторов необходимо настроить две версии протокола IP (IPv4 и IPv6);

– для использования двойного стека системные администраторы должны установить соответствующие сетевые настройки на каждом узле, что требует дополнительных временных и финансовых затрат;

– применение данного метода повышает использование системных ресурсов промежуточных устройств сети и может замедлять их работу.

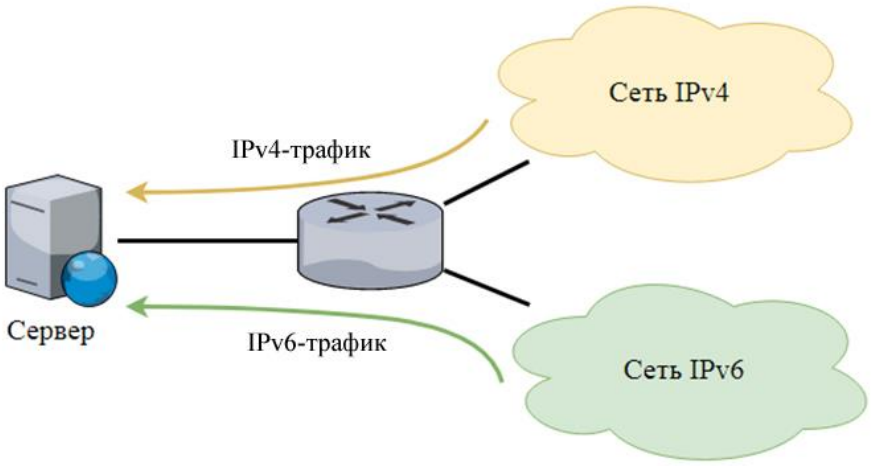

Рисунок 4.1 – Двойной стек

На рисунке 4.2 представлен пример схемы сети с применением двойного стека. В рассматриваемой сети в подсети Building1 и подсетях маршрутизаторов Router1 – Router4 и Router4 – Router3 настроена только IPv4-адресация. В остальных подсетях – IPv6. Для организации доступа пользователей подсети Building1 к серверу iot.by необходимо настроить IPv4-адресацию на сервере и sub-интерфейсе маршрутизатора Router1. В таблице 4.1 показана минимально необходимая IPv4-адресация для доступа пользователей подсети Building1 к серверу iot.by. В рассматриваемой сети настроены протоколы маршрутизации OSPFv3 для IPv6-подсетей и OSPFv2 для IPv4-подсетей.

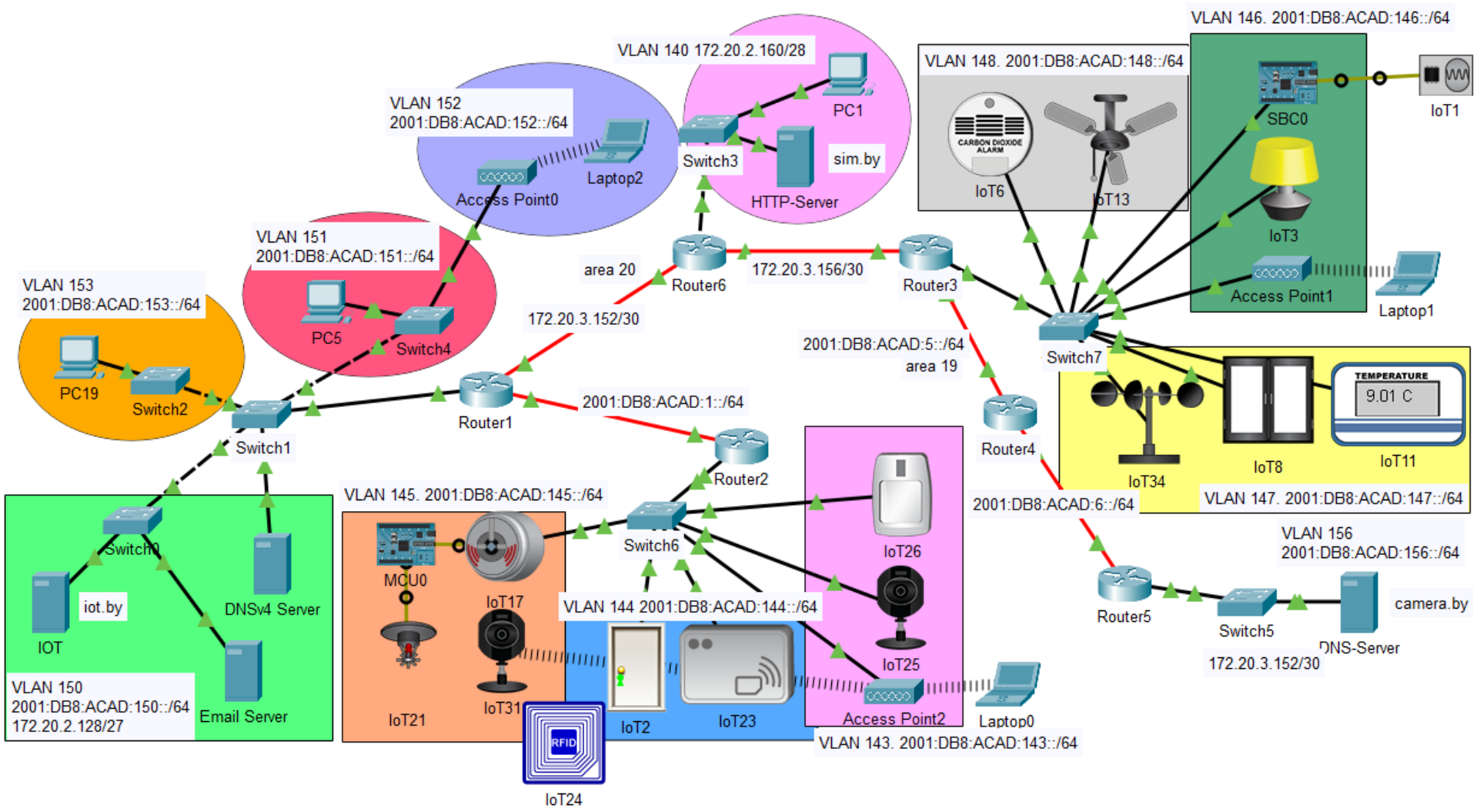

Рисунок 4.2 – Пример сети с применением двойного стека

Таблица 4.1 – IPv4- и IPv6-адресация для подсетей и вид преобразования адресов

Название подсети	IPv4-адреса подсетей	IPv6-адреса подсетей	Вид преобразования
VLAN 140	172.20.2.160/28	–	Dynamic NAT-PT
VLAN 143	–	2001:DB8:ACAD:143::/64	IPv6-туннель
VLAN 144	–	2001:DB8:ACAD:144::/64	
VLAN 145	–	2001:DB8:ACAD:145::/64	
VLAN 146	–	2001:DB8:ACAD:146::/64	IPv6-туннель
VLAN 147	–	2001:DB8:ACAD:147::/64	
VLAN 148	–	2001:DB8:ACAD:148::/64	
VLAN 150	172.20.2.128/27	2001:DB8:ACAD:150::/64	Двойной стек, IPv6-туннель
VLAN 151	–	2001:DB8:ACAD:151::/64	PAT NAT-PT, IPv4-mapped, IPv6-туннель
VLAN 152	–	2001:DB8:ACAD:152::/64	PAT NAT-PT, IPv6-туннель
VLAN 153	–	2001:DB8:ACAD:153::/64	
VLAN 156	–	2001:DB8:ACAD:156::/64	Static NAT-PT
Router1 – Router2	–	2001:DB8:ACAD:1::/64	–
Router1 – Router6	172.20.3.152/30	–	–
Router6 – Router3	172.20.3.156/30	–	–
Router4 – Router3	–	2001:DB8:ACAD:5::/64	–
Router4 – Router5	–	2001:DB8:ACAD:6::/64	–

На маршрутизаторе Router6 (см. рисунок 4.2) настроены три интерфейса следующим образом:

```
Router6(config)# interface GigabitEthernet0/0.400
Router6(config-if)#encapsulation dot1Q 400
Router6(config-if)#ip address 172.20.0.161 255.255.255.240
Router6(config)#interface GigabitEthernet0/0/0
Router6(config-if)# 172.20.3.154 255.255.255.252
Router6(config)#interface GigabitEthernet0/3/0
Router6(config-if)#ip address 172.20.3.158 255.255.255.252
```

Маршрутизация по протоколу OSPFv2 на маршрутизаторе настраивается следующим образом:

```
Router6(config)#router ospf 115
Router6(config-router)#router-id 20.20.20.26
Router6(config-router)#passive-interface FastEthernet0/0.140
Router6(config-router)#network 172.20.3.152 0.0.0.3 area 20
Router6(config-router)#network 172.20.3.156 0.0.0.3 area 20
Router6(config-router)#network 172.20.2.160 0.0.0.15 area 20
```

На маршрутизаторе Router1 настраивается IPv4- и IPv6-маршрутизация следующим образом:

```
Router1(config)#interface GigabitEthernet0/0/0
Router1(config-if)#ip address 172.20.3.153 255.255.255.252
Router1(config)#interface GigabitEthernet0/1.7
Router1(config-if)#encapsulation dot1Q 150
Router1(config-if)# ip address 172.20.2.129 255.255.255.224
Router1(config-if)#ipv6 address FE80::1 link-local
Router1(config-if)#ipv6 address 2001:DB8:ACAD:150::1/64
Router1(config-if)#ipv6 nd other-config-flag
Router1(config-if)#ipv6 ospf 115 area 20
Router1(config-if)#ipv6 dhcp server VLAN150
```

На остальных sub-интрефейсах и интерфейсе, подключенном к маршрутизатору Router2, настроена только IPv6-адресация. На маршрутизаторе Router1 должно быть настроено два протокола маршрутизации для OSPFv2 и OSPFv3.

```
Router1(config)#router ospf 115
Router1(config-router)#router-id 20.20.20.21
Router1(config-router)#network 172.20.3.152 0.0.0.3 area 20
Router1(config-router)#network 172.20.2.128 0.0.0.31 area 20
Router1(config)# ipv6 router ospf 115
Router1(config-router)# router-id 10.10.10.1
Router1(config-router)#passive-interface FastEthernet0/1.150
Router1(config-router)#passive-interface FastEthernet0/1.151
Router1(config-router)#passive-interface FastEthernet0/1.152
```

Необходимо отметить, что для IPv4-подсетей требуется создать отдельный DNS-сервер (DNSv4-Server на рисунке 4.2), IPv4-адрес которого указывать в сетевых настройках устройств подсети Building1. Это необходимо

для исключения ошибок в работе протокола DNS для IPv4 и IPv6. Таким образом, пользователи подсети Building1 могут получать доступ к серверу iot.by по протоколу IPv4, в то время как устройства IoT не могут передать данные на сервер, т. к. они находятся в IPv6-подсети, которая отделена от подсети сервера подсетью IPv4. В таком случае можно использовать механизм туннелирования.

Механизм туннелирования (рисунок 4.3) используется для частичного решения проблемы совместимости IPv4- и IPv6-протоколов. Он не может применяться для связи IPv6-узлов с IPv4-устройствами. Туннелирование предназначено для организации связи между IPv6-узлами или IPv6-сетями посредством существующей среды передачи данных, поддерживающей только версию протокола IPv4. Суть этого механизма заключается в том, что между сетями, работающими с IPv4, с помощью специальных конфигураций создается туннель. Пакеты, попадая на один конец этого туннеля, преобразовываются. Это преобразование заключается в инкапсулировании IPv6-пакетов в пакеты стандарта IPv4. На другой стороне туннеля происходит обратный процесс: из IPv4-пакетов извлекаются пакеты стандарта IPv6, которые затем обрабатываются маршрутизаторами как IPv6-пакеты.

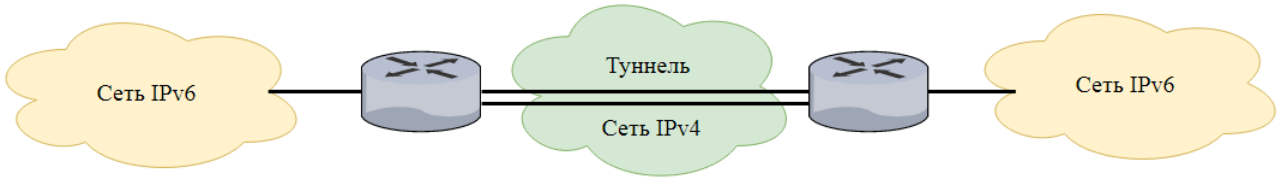

Рисунок 4.3 – Механизм туннелирования

Главным преимуществом этого метода является отсутствие необходимости устанавливать дополнительные настройки IPv6 на каждом промежуточном устройстве. Так для сети, построенной на основе протокола IPv6, достаточно создать несколько туннелей, связывающих ее с другими такими же сетями.

Создание туннеля производится следующим образом:

```
Router1(config)#interface tunnel номер
Router1(config-if)# ipv6 address IPv6-адрес/префикс
Router1(config-if)#ipv6 ospf номер area номер
Router1(config-if)#tunnel source интерфейс номер
Router1(config-if)#tunnel destination IPv4-адрес
```

Рассмотрим пример конфигурации туннелирования для сети, представленной на рисунке 4.2. Необходимо отметить, что в данной сети между маршрутизаторами Router1 – Router4 – Router3 настроена IPv4-адресация. При этом в

VLAN 106, 108, 400–406 настроена IPv6-адресация. Устройства IoT из подсетей VLAN 400–402 должны передавать данные на сервер camera.by, а устройства из подсетей VLAN 404–406 – на сервер iot.by. При этом IPv6-сети разделены подсетями IPv4. В данном случае целесообразно создать туннель IPv6 между маршрутизаторами Router1 – Router4 – Router3.

На маршрутизаторе Router1 туннель IPv6 настроен следующим образом:

```
Router1(config)#interface Tunnel150
Router1(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64
Router1(config-if)#ipv6 ospf 115 area 20
Router1(config-if)#tunnel source GigabitEthernet0/0/0
Router1(config-if)#tunnel destination 172.20.3.157
Router1(config-if)#tunnel mode ipv6ip
```

В данном примере команда `tunnel source` используется для обозначения источника, т. е. с какого интерфейса начинается туннелирование. Для маршрутизатора Router1 (см. рисунок 4.2) это интерфейс GigabitEthernet0/0/0, подключенный к маршрутизатору Router6. Команда `tunnel destination` показывает адрес назначения, а именно IPv4-адрес интерфейса маршрутизатора Router3.

Аналогичным образом происходит настройка на маршрутизаторе Router3:

```
Router3(config)#interface Tunnel150
Router3(config)#ipv6 address 2001:DB8:ACAD:2::2/64
Router3(config)# ipv6 ospf 115 area 20
Router3(config)#tunnel source GigabitEthernet0/0/0
Router3(config)#tunnel destination 172.20.3.153
Router3(config)#tunnel mode ipv6ip
```

В случае если настройки на маршрутизаторах произведены верно, то при отправке сообщения с компьютера из VLAN 151 на маршрутизаторе Router1 пакет будет дополнительно инкапсулирован в пакет IPv4 (рисунок 4.4), т. е. у сообщения будет не только адрес IPv6, но и IPv4. Правильная конфигурация IPv6-туннеля позволит всем IoT-устройствам передавать свои статусы на серверы (рисунок 4.5).

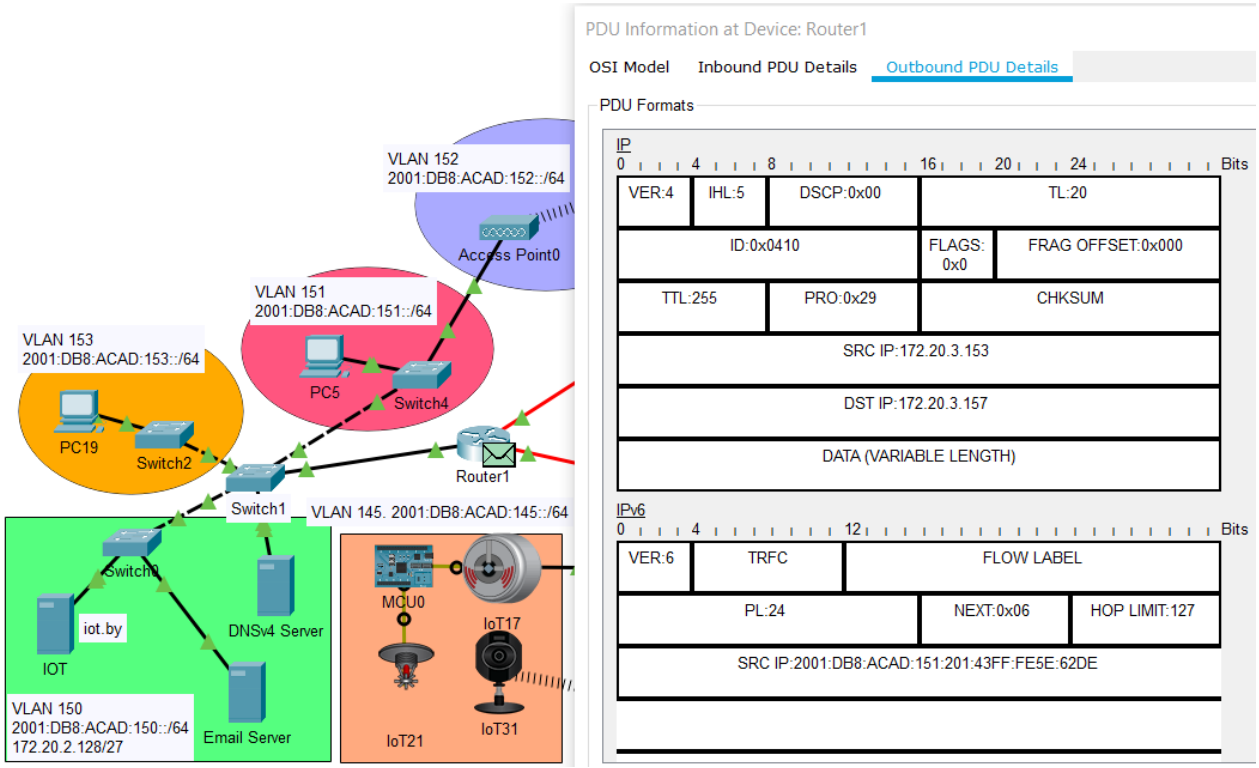

Рисунок 4.4 – Инкапсуляция пакета IPv6 в IPv4

Как было уже отмечено ранее, туннелирование предназначено для организации связи между IPv6-сетями, при этом пользователи сеть Building1, в которой настроена IPv4-адресация, не смогут получить доступ к IPv6-серверам camera.by и sim.by (см. рисунок 4.2). Для решения данной проблемы можно использовать преобразование (трансляцию) IP-адресов.

Преобразование адресов IPv6 в IPv4 называется NAT-PT (Network Address Translation – Protocol Translation). Другими словами, IPv6-пакет преобразовывается в пакет IPv4 и наоборот (рисунок 4.5).

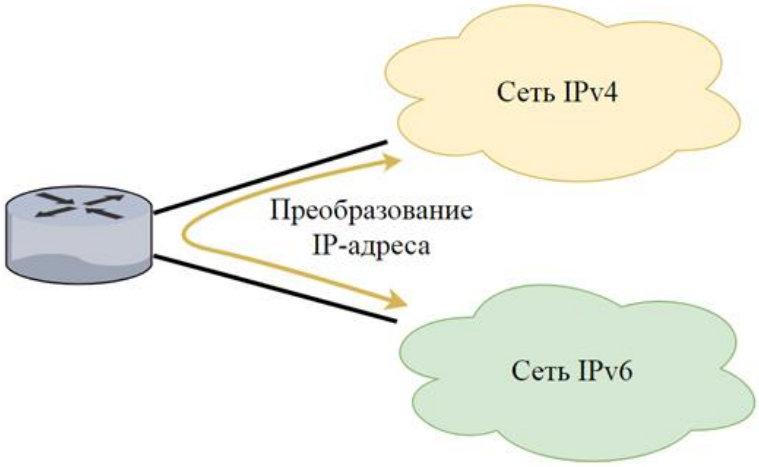

Рисунок 4.5 – Преобразование IP-адресов

Выделяют следующие типы NAT-PT:

– Static NAT-PT (статический NAT-PT) – преобразование одного IPv6-адреса в определенный уникальный IPv4-адрес, т. е. сопоставляется один IPv6-адрес с одним адресом IPv4 и наоборот;

– Dynamic NAT-PT (динамический NAT-PT) – преобразование диапазона IPv6-адресов в один из адресов заданного диапазона IPv4 и наоборот;

– Port Address Translation NAT-PT – преобразование нескольких IPv6-адресов в один IPv4-адрес внешнего интерфейса и наоборот;

– IPv4-mapped NAT-PT – для преобразования IPv4-адреса в адрес IPv6 используются 96 бит IPv6-адреса и 32 бита IPv4, преобразованные в шестнадцатеричную систему исчисления.

Для настройки статического преобразования IPv6-адресов в IPv4 необходимо использовать следующие команды:

```
Router(config)#ipv6 nat prefix IPv6-адрес/длина-префикса
Router(config)#ipv6 nat v4v6 source IPv4-адрес IPv6-адрес
Router(config)#ipv6 nat v6v4 source IPv6-адрес IPv4-адрес
Router(config)#interface номер_интерфейса
Router(config-if)#ipv6 nat
```

Командой `ipv6 nat prefix` *IPv6-адрес/длина-префикса* назначается IPv6-адрес, который будет использоваться для замены IPv4-адреса в передающем пакете. Для того чтобы преобразовывать конкретные IPv4-адреса источника сообщения в точный IPv6-адрес, используется команда `ipv6 nat v4v6 source`. Команда `ipv6 nat v6v4 source` указывает, что назначаемый IPv6-адрес источника будет заменяться IPv4-адресом, например, при поступлении пакета из сети IPv6 в сеть IPv4. Также необходимо включить преобразование IP-адресов на интерфейсах командой `ipv6 nat`.

Для того чтобы в пакетах, отправляемых из подсети Building1, представленной на рисунке 4.2, IPv4-адрес сервера заменялся на адрес IPv6, необходимо настроить преобразование IP-адресов на маршрутизаторах Router1 и Router3.

Например, на маршрутизаторе Router3 будем использовать статический NAT-PT для преобразования IPv6- и IPv4-адресов серверов camera.by (2001:DB8:ACAD:110::100/64) и sim.by (172.20.2.174). Для этого используются следующие команды:

```
Router3(config)#ipv6 nat v6v4 source
2001:DB8:ACAD:156::100 172.20.3.98
```

```
Router3(config)# ipv6 nat v6v4 source
2001:DB8:ACAD:141::100 172.20.2.174
Router3(config)#interface GigabitEthernet0/2/0
Router3(config-if)#ipv6 nat
```

Необходимо отметить, что IPv6- или IPv4-адреса, которые использовались для преобразования адресов серверов camera.by и sim.by не относятся ни к одной из подсетей в смоделированной сети. Таким образом, маршрутизаторы не имеют в таблицах маршрутизации записей о маршрутах к сети с IP-адресами 172.20.3.98 и 2001:DB8:ACAD:141::100. Поэтому необходимо назначить эти IP-адреса виртуальным или логическим интерфейсам маршрутизатора Router3 и добавить в конфигурацию маршрутизации OSPFv2 следующим образом:

```
Router3(config)#interface Loopback1
Router3(config-if)#ip address 172.20.3.98 255.255.255.255
Router3(config-if)#interface Loopback2
Router3(config-if)#no ip address
Router3(config-if)#ipv6 address 2001:DB8:ACAD:141::100/64
Router3(config-if)# ipv6 ospf 115 area 19
Router(config)#router ospf 115
Router(config-router)#network 172.20.3.96 0.0.0.15 area 20
```

В результате использования представленных выше команд в таблицы маршрутизации соседних маршрутизаторов появится запись о маршрутах к серверам camera.by и sim.by (рисунок 4.6).

```
Router6#show ip route ospf
     172.20.0.0/16 is variably subnetted, 5 subnets, 4 masks
O       172.20.2.128 [110/2] via 172.20.3.153, 01:40:19, GigabitEthernet0/0/0
O       172.20.3.98 [110/2] via 172.20.3.157, 00:06:43, GigabitEthernet0/3/0
```

```
Router4#show ipv6 route ospf
IPv6 Routing Table - 11 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
O   2001:DB8:ACAD:140::/96 [110/2]
     via FE80::3, GigabitEthernet0/2/0
O   2001:DB8:ACAD:141::100/128 [110/1]
     via FE80::3, GigabitEthernet0/2/0
```

Рисунок 4.6 – Таблицы маршрутизации на маршрутизаторах Router6 и Router4

Для конфигурации динамического NAT-PT необходимо выполнить следующие действия.

1 Определить пул IPv6-адресов, которые будут использоваться для трансляции, с помощью команды `ipv6 nat v4v6 pool` *`имя_пула начальный_IPv6-адрес конечный_IPv6-адрес`* `prefix-length 96`.

2 Определить префикс, который будет использоваться для преобразования, с помощью команды `ipv6 nat prefix` *`IPv6-адрес/префикс`*.

3 Настроить стандартный список контроля доступа (ACL) для разрешения трансляции только тех IPv4-адресов, которые будут указаны, с помощью команды `access-list` *`номер_ACL`* `permit` *`IPv4-адрес обратная_маска`*.

4 Установить связь созданного ACL с пулом с помощью команды `ipv6 nat v4v6 source list` *`номер_ACL`* `pool` *`имя_пула`*.

5 Определить, на каких интерфейсах маршрутизатора будет выполняться преобразование NAT-PT с помощью команды `ipv6 nat`.

Для преобразования IPv4-адресов из подсети Building1 настроим динамический NAT-PT на маршрутизаторе Router3 (см. рисунок 4.2) следующим образом:

```
Router3(config)#ipv6 nat v4v6 pool IPV6
2001:DB8:ACAD:140::2 2001:DB8:ACAD:140::6 prefix-length 96
Router3(config)#ipv6 nat prefix 2001:DB8:ACAD:140::/96
Router3(config)#access-list 4 permit 172.20.2.160
0.0.0.15
Router3(config)#ipv6 nat v4v6 source list 4 pool IPV6
Router3(config)#interface GigabitEthernet0/0/0
Router3(config-if)#ipv6 nat
```

Как показано на рисунке 4.7, при отправке сообщений из подсети Building1 на сервер camera.by преобразование IP-адресов осуществляется корректно, однако обратно в сеть Building1 сообщения не будут возвращаться, т. к. в таблице маршрутизации маршрутизатора Router4 нет записи о маршруте к подсети Building1, т. к. преобразованный IPv6-адрес 2001:DB8:ACAD:140::2 (см. рисунок 4.7) не относится ни к одной из подсетей. Поэтому необходимо IPv6-адрес подсети, используемый в динамическом NAT-PT, назначить какому-либо виртуальному интерфейсу маршрутизатора Router3, например, создать sub-интерфейс:

```
Router(config)#interface GigabitEthernet0/0.140
Router(config-subif)#encapsulation dot1Q 140
Router(config-subif)#no ip address
```

```
Router(config-subif)#ipv6 address 2001:DB8:ACAD:140::1/96
Router(config-subif)#ipv6 ospf 115 area 20
```

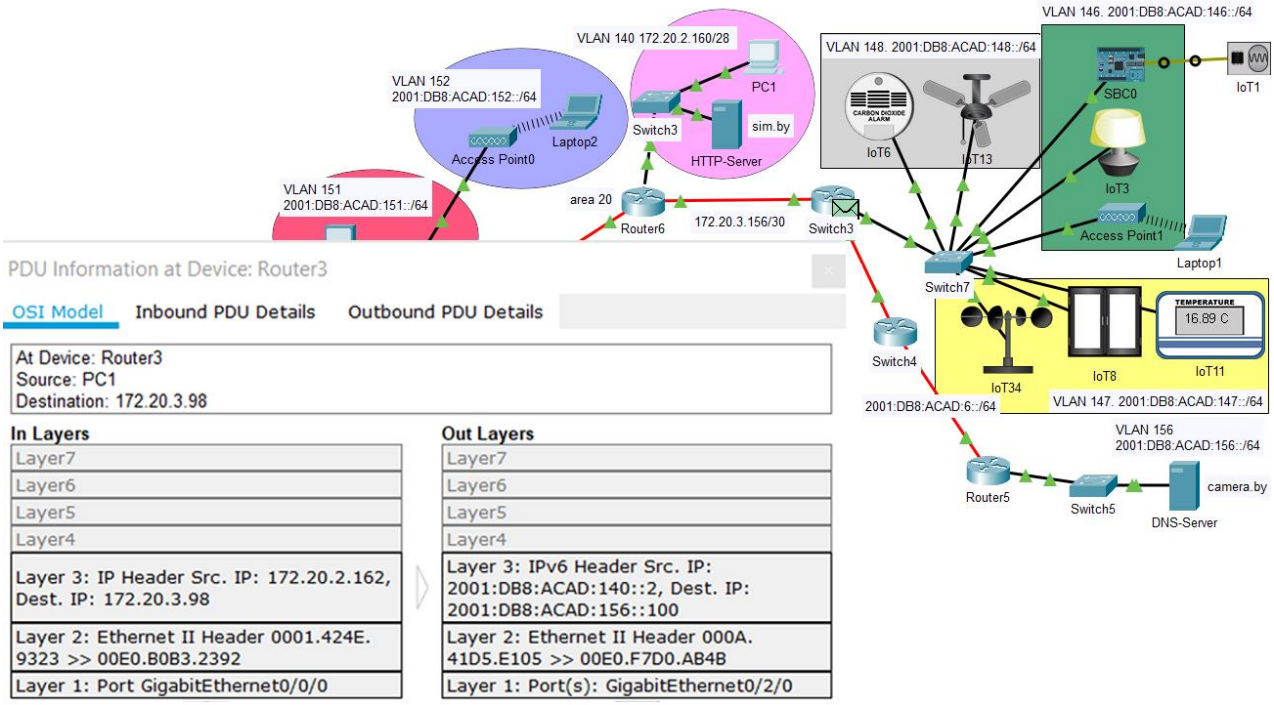

Рисунок 4.7 – Результат трасляции IP-адресов посредством конфигурации динамического и статического NAT-PT

В результате введенных команд, перезагрузки процесса OSPF на маршрутизаторах в таблице маршрутизации Router4 появится запись о маршруте к подсети 2001:DB8:ACAD:140::/96 (см. рисунок 4.6).

Процесс конфигурации PAT NAT-PT включает следующие этапы.

1 Конфигурация расширенного списка контроля доступа (ACL) для разрешения трансляции только тех IPv6-адресов, которые будут указаны, с помощью команд `ipv6 access-list` *`имя_ACL`* и `permit IPv6-`*`адрес/префикс`* `any`.

2 Конфигурация PAT с указанием номера списка контроля доступа и типа и номера интерфейса, IP-адрес которого будет использован для трансляции, с помощью команды `ipv6 nat v6v4 source list` *`номер_ACL`* `interface` *`тип_номер`* `overload`.

3 Определить, на каких интерфейсах маршрутизатора будет выполнять преобразование NAT-PT с помощью команды `ipv6 nat`.

Например, для доступа из подсети VLAN 151 к серверу sim.by в подсети Building1 настроим PAT NAT-PT на маршрутизаторе Router1 следующим образом:

```
Router1(config)#ipv6 access-list To-ipv4
```

```
Router1(config-ipv6-acl)#permit ipv6
2001:DB8:ACAD:151::/64 any
Router1(config)#ipv6 nat v6v4 source list To-ipv4
interface gigabitEthernet 0/0/0 overload
Router1(config)#interface fastEthernet 0/1.151
Router1(config-subif)#ipv6 nat
Router1(config)#interface gigabitEthernet 0/0/0
Router1(config-if)#ipv6 nat
```

Отметим, что дополнительно необходимо настроить статический NAT-PT для трансляции IPv6-адреса сервера sim.by и внести его IPv6-адрес в DNS для IPv6-подсетей. В результате будет осуществляться преобразование IPv6-адресов с помощью PAT NAT-PT, как показано на рисунке 4.8.

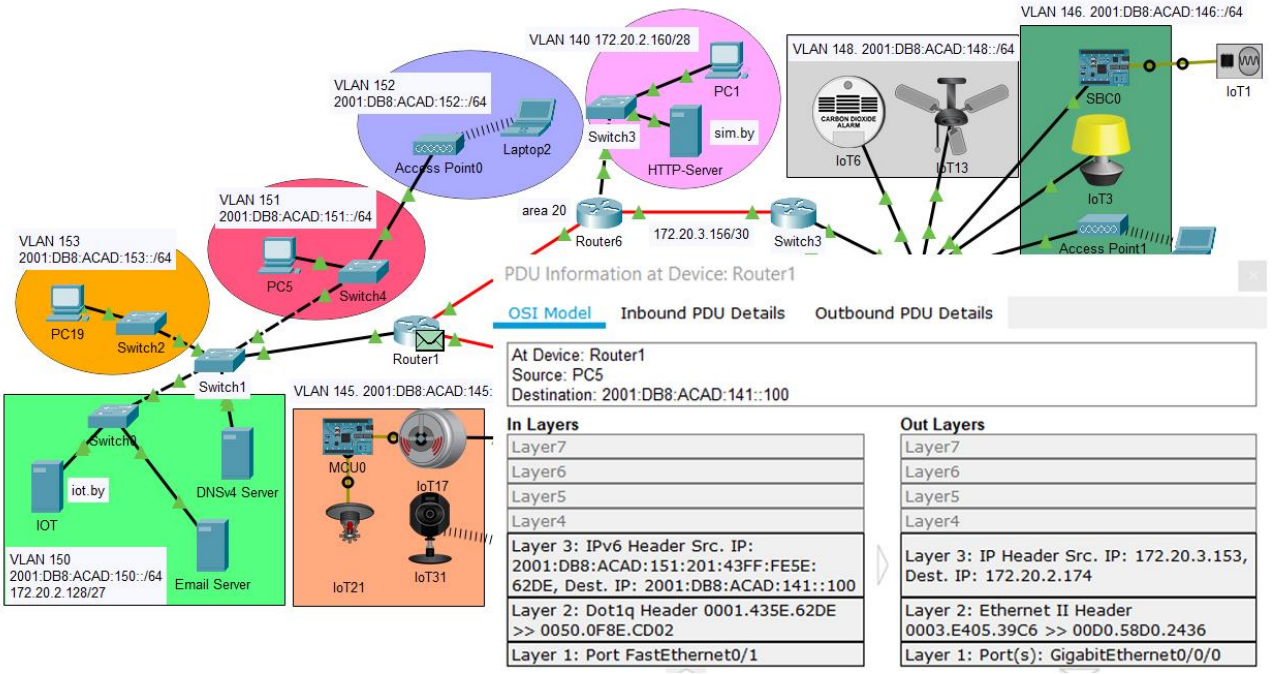

Рисунок 4.8 – Результат трасляции IPv6-адреса в IPv4 посредством PAT NAT-PT

Технология IPv4-mapped NAT-PT используется для упрощения удаленного доступа к конфигурации промежуточных устройств с помощью протоколов telnet или проверки соединения. Результат этого преобразования показан на рисунке 4.9. Для конфигурации IPv4-mapped NAT-PT реализуются следующие действия.

1 Конфигурация расширенного списка контроля доступа (ACL) для разрешения трансляции только тех IPv6-адресов, которые будут указаны, с помощью команд `ipv6 access-list` *`имя_ACL`* и `permit` *`IPv6-адрес/префикс`* `any`.

2 Определение префикса, который будет использоваться для преобразования, с помощью команды `ipv6 nat prefix` *`IPv6-адрес/префикс`*.

3 Конфигурация IPv4-mapped NAT-PT на интерфейсе с помощью команды `ipv6 nat prefix` *`IPv6-адрес/префикс`* `v4-mapped` *`имя_ACL`*.

4 Определение, на каких интерфейсах маршрутизатора будет выполняться преобразование NAT-PT, с помощью команды `ipv6 nat`.

Для конфигурации IPv4-mapped NAT-PT для VLAN 153 на маршрутизаторе Router1 использовались следующие команды:

```
Router1(config)#ipv6 access-list MAP
Router1(config-std-nacl)# permit ipv6
2001:DB8:ACAD:153::/64 any
Router1(config)# ipv6 nat prefix 2001:DB8:ACAD:142::/96
Router1(config)#interface FastEthernet0/1.153
Router1(config-if)# ipv6 nat prefix
2001:DB8:ACAD:142::/96 v4-mapped MAP
Router1(config-subif)#ipv6 nat
```

Ввиду того, что на маршрутизаторе Router1 на интерфейсе gigabitEthernet 0/0/0 настроен PAT NAT-PT, необходимо в созданный ранее список ACL To-ipv4 добавить разрешения доступа к NAT с помощью следующих команд:

```
Router1(config)#ipv6 access-list To-ipv4
Router1(config-ipv6-acl)#permit ipv6
2001:DB8:ACAD:153::/64 any
```

Таким образом, IPv6-адрес источника будет преобразоваться с помощью PAT NAT-PT, а адрес назначения – с помощью IPv4-mapped NAT-PT. Для проверки работы IPv4-mapped NAT-PT отправим ICMP сообщение с компьютера PC0 на компьютер PC3 (см. рисунок 4.6) с помощью команды `ping` или `ssh`, например, `ssh -l admin 2001:DB8:ACAD:142::172.20.2.173`. В данной команде первые 96 битов представлены IPv6-адресом, остальные 32 бита – IPv4-адресом, соответствующим IPv4-адресу коммутатора Switch3 в подсети Building1. В результате последние 32 бита переводятся в шестнадцатеричную систему исчисления и образуется IPv6-адрес. Таким образом можно отправить ICMP сообщение из IPv6-подсети на любое устройство в IPv4-подсети.

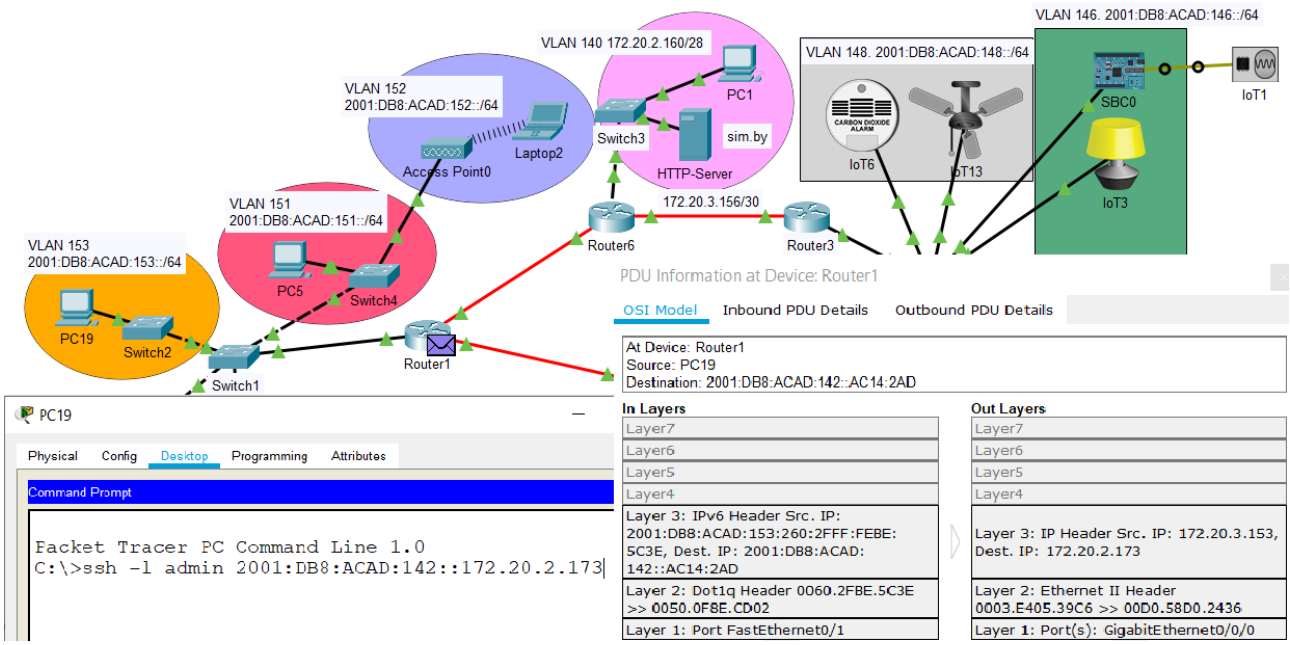

Рисунок 4.9 – Результат преобразования посредством IPv4-mapped NAT-PT

4.2 Лабораторное задание

Лабораторная работа выполняется на основе настроек, выполненных в лабораторной работе № 8 лабораторного практикума «Маршрутизация в IPv4- и IPv6-сетях» [6], файл **Lab8-1.pkt**. До начала выполнения необходимо открыть сохраненный файл **Lab8-1.pkt** и проверить настройки IPv6-адресации: у всех устройств адресация должна соответствовать заданному IP-адресу из таблицы 4.2, маршрутизация должна быть настроена по протоколу OSPFv3. В сети должны быть подсети с VLAN, подсеть Building1, подсети с устройствами освещения, контроля температуры и дыма, видеонаблюдения, контроля доступа и пожаротушения, три сервера: на одном сервере должны отображаться состояния устройств освещения, контроля температуры и дыма (сервер iot.by на рисунке 4.2), на втором сервере должны отображаться состояния устройств видеонаблюдения, контроля доступа и пожаротушения (сервер camera.by на рисунке 4.2), на третьем – веб-сайт, разработанный в лабораторной работе № 5 лабораторного практикума «Основы построения локальных сетей» [10], доменное имя которого должно соответствовать фамилии студента. С любого устройства из любой подсети должен быть доступ к серверам.

В данной лабораторной работе необходимо настроить двойной стек, IPv6-туннель и разные виды NAT-PT для объединения сетей IPv4 и IPv6.

1 Преобразовать топологию сети, удалить соединения между маршрутизаторами по примеру рисунка 4.10. Во всей сети должна быть одна область OSPFv3. На маршрутизаторе, подключенном к подсети Building1, удалить

IPv6-маршрутизацию, IPv6-адресацию и IPv6-рассылку OSPF, используя следующие команды:

```
Router(config)#no ipv6 router ospf номер
Router(config)#no ipv6 unicast-routing
Router(config)#interface номер
Router(config-if)#no ipv6 address
```

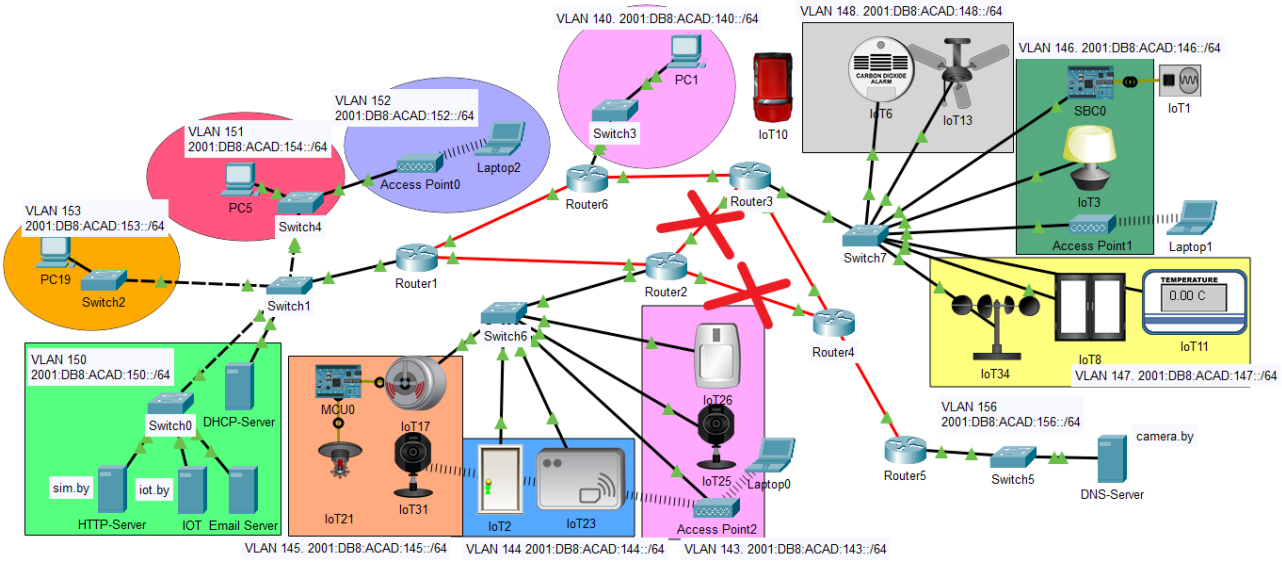

Рисунок 4.10 – Пример смоделированной сети с преобразованной топологией

В подсети Building1 и на подключенных к ней маршрутизаторах настроить IPv4-адресацию и маршрутизацию OSPFv2 (маршрутизаторы Router1, Router3 и Router6 на рисунке 4.2) в соответствии с исходными данными в таблице 4.2. Организовать доступ пользователей данной сети к серверу iot.by путем настройки двойного стека на сервере iot.by и на подключенном к его подсети маршрутизаторе (маршрутизатор Router1 на рисунке 4.2). Добавить в подсеть сервера iot.by DNSv4-сервер, настроить его IPv4-адрес в DHCP подсети Building1. Проверить правильность настроек: осуществить проверку соединения с любого устройства из подсети Building1 к серверу iot.by через браузер по доменному имени. В отчете представить заполненную таблицу 4.3 (см. таблицу 4.1 в качестве примера) и результаты настройки двойного стека и маршрутизации на маршрутизаторе, подключенном к подсети Building1, и соседнем маршрутизаторе (маршрутизаторы Router1 и Router3 на рисунке 4.2). Сохранить файл под именем **LAB4-1.pkt**.

Таблица 4.2 – Исходные данные для IPv6- и IPv4-адресации

Третья цифра шифра	IPv6-адрес	Вторая цифра шифра	IPv4-адрес сети
0	2001:EDA:50::/48	0	172.16.0.0/20
1	2001:ADA:41::/48	1	172.17.0.0/21
2	2001:ABA:12::/48	2	172.18.0.0/22
3	2001:CED:33::/48	3	172.19.0.0/23
4	2001:DED:54::/48	4	172.21.0.0/22
5	2001:FEF:85::/48	5	172.22.0.0/23
6	2001:CEF:96::/48	6	172.23.0.0/24
7	2001:DEC:47::/48	7	172.24.0.0/24
8	2001:CAC:28::/48	8	172.30.0.0/21
9	2001:DAD:79::/48	9	172.31.0.0/20

Таблица 4.3 – IPv4- и IPv6-адресация для смоделированной сети и виды преобразования адресов

Название подсети	IPv4-адреса подсетей	IPv6-адреса подсетей	Вид преобразования

2 Осуществить настройку IPv6-туннеля на маршрутизаторах, находящихся на границе IPv4-сети (маршрутизаторы Router1, Router3 на рисунке 4.2). Номер интерфейса туннеля должен соответствовать шифру студента. Представить в отчете результаты настройки туннелей на маршрутизаторах и показать, что на серверах iot.by и camera.by отражаются IoT устройства. Сохранить файл под именем **LAB4-2.pkt**.

3 *Наблюдение инкапсуляции IPv6-пакета в IPv4.* Получить доступ с устройства в IPv6-подсети к серверам iot.by и camera.by так, чтобы пакеты проходили через IPv6-туннель. Представить в отчете результаты инкапсуляции IPv6-пакетов в IPv4 (см. пример на рисунке 4.4).

4 *Настройка статического и динамического NAT-PT.* Для доступа к серверам с IPv6-адресацией из IPv4-подсетей настроить статический NAT-PT. Для организации доступа из подсети Building1 к серверу camera.by настроить динамический NAT-PT (см. рисунок 4.7). Отразить в отчете результаты конфигурации статического и динамического NAT-PT на маршрутизаторе и результат трансляции IP-адресов по примеру рисунка 4.7. Сохранить файл под именем **LAB4-4.pkt**.

5 Перенести в подсеть Building1 сервер с веб-сайтом, разработанным в лабораторной работе № 5 лабораторного практикума «Основы построения локальных сетей» [10], доменное имя и IPv6-адрес которого должны соответствовать фамилии студента. Организовать доступ из любого VLAN к добавленному серверу посредством PAT NAT-PT. Отразить в отчете результаты конфигурации PAT NAT-PT на маршрутизаторе и результат трансляции IP-адресов (см. пример на рисунке 4.8). Сохранить файл под именем **LAB4-5.pkt**.

6 Организовать возможность отправки ICMP пакетов и подключения по протоколу SSH с любого устройство в VLAN в IPv4-подсети посредством IPv4-mapped NAT-PT. Отразить в отчете результаты конфигурации IPv4-mapped NAT-PT на маршрутизаторе и результат трансляции IP-адресов (см. пример на рисунке 4.9). Сохранить файл под именем **LAB4-6.pkt**.

4.3 Содержание отчета

1 Цель работы, исходные данные.

2 Результаты произведенных настроек (результаты настроек из пунктов 1–6), изображение смоделированной сети.

3 Вывод по работе.

4 Ответы на контрольные вопросы.

4.4 Контрольные вопросы

1 Проблемы совместимости IPv6- и IPv4-сетей.

2 Описание методов совместного использования IPv4- и IPv6-протоколов.

3 Описание метода двойного стека, его достоинства и недостатки, принципы настройки.

4 Описание механизма туннелирования, его достоинства и недостатки, принципы настройки.

5 Назначение и типы NAT-PT. Пример конфигурации статического NAT-PT.

6 Отличительные особенности конфигурации статического и динамического NAT-PT.

7 Последовательность действий и пример конфигурации PAT NAT-PT.

8 Назначение IPv4-mapped NAT-PT. Последовательность действий и пример конфигурации IPv4-mapped NAT-PT.

ЛАБОРАТОРНАЯ РАБОТА № 5
МАРШРУТИЗАЦИЯ В ГЛОБАЛЬНЫХ СЕТЯХ

Цель: изучить протокол маршрутизации глобальных сетей BGP, перераспределение маршрутов в разных протоколах маршрутизации.

5.1 Теоретическая часть

Глобальная сеть (WAN – Wide Area Network) – система связанных между собой информационных сетей, предоставляющих доступ региональным сетям и оконечным устройствам, расположенным на расстоянии друг от друга.

Основная функция глобальной сети заключается в обеспечении взаимосвязи информационных сетей, маршрутизации трафика между ними, поддержании оптимальной пропускной способности.

Доступ к глобальной сети предоставляется операторами связи, которые выделяют каналы определенной пропускной способности по установленному тарифному плану для подключения удаленных сетей и устройств. Если для подключения к глобальной сети организации требуется канал связи, то физическое подключение (арендованная линия) арендуется у оператора связи, что подразумевает предоставление предустановленного канала связи глобальной сети, идущего от заказчика к сети оператора связи.

Различают следующие типы операторов связи:

– Tier 1 ISP – провайдер, который имеет доступ ко всей региональной таблице маршрутизации исключительно через пиринговые взаимоотношения, не должен оплачивать транзит трафика;

– Tier 2 ISP – оператор, покупающий и продающий транзитный трафик в пределах интернет-региона;

– Tier 3 ISP – оператор, который для доступа к сети Интернет использует исключительно каналы, которые покупает у других операторов.

Пиринговые взаимоотношения (от англ. peering – взаимодействие) – соглашение интернет-операторов об обмене трафиком между своими сетями, а также техническое взаимодействие, реализующее указанное соглашение: соединение сетей и обмен информацией о сетевых маршрутах по протоколу BGP [11].

Транзит трафика – это услуга по предоставлению широкополосного доступа в глобальную сеть для операторов связи через оптические сети передачи данных другого оператора на платной основе.

С апреля 2012 г. услуги пиринга в Республике Беларусь оказывает республиканское унитарное предприятие «Национальный центр обмена трафиком» (НЦОТ) [12].

Для учета всех сетей операторов введены автономные системы.

Автономная система (AS – Autonomous System) – система сетей и сетевых устройств, управляемых одним или несколькими операторами, имеющими единую политику маршрутизации с глобальной сетью [13]. Номера автономных систем представляют собой 16-битные (выделялись до 2007 г.) или 32-битные номера, которые выделяются локальными (LIR – Local Internet Registry) или региональными интернет-регистраторами (RIR – Regional Internet Registry).

Выделяют пять основных региональных регистраторов [14]:

– American Registry for Internet Numbers (ARIN) – обслуживает сети Северной Америки;

– RIPE Network Coordination Centre (RIPE NCC) – обслуживает сети стран Европы, Ближнего Востока, Центральной Азии;

– Asia-Pacific Network Information Centre (APNIC) – обслуживает сети Азии, Тихоокеанского региона;

– Latin American and Caribbean Internet Addresses Registry (LACNIC) – обслуживает сети Латинской Америки, Карибского региона;

– African Network Information Centre (AfriNIC) – обслуживает сети Африканского континента.

Как правило, статус локальных регистраторов имеют различные государственные и частные провайдеры.

Для регистрации автономной системы LIR или RIR необходимо предоставить следующую информацию:

– реквизиты организации;

– сведения (номера) о других автономных системах (минимум двух), которые готовы взаимодействовать с регистрируемой AS (как правило, это AS операторов, которые предоставляют свои каналы связи);

– запрос определенного количества публичных IP-адресов;

– описание технических характеристик подключаемой сети с указанием оборудования, которое будет обслуживать AS.

Таким образом, на сегодняшний день существует огромное количество автономных сетей, которые можно просмотреть в различных базах, например, на сайте организации IANA.

Для маршрутизации трафика между автономными системами используется протокол BGP, который представляет собой протокол динамической маршрутизации с передачей карты маршрутов всем остальным маршрутизаторам в других автономных системах.

Протокол BGP может использоваться как для внутренней маршрутизации, в таком случае его называют IGP (Interior Gateway Protocols), или IBGP (Internal BGP), так и для внешней – EGP (Exterior Gateway Protocol), или EBGP (External BGP). Принцип работы IBGP похож на алгоритм SPF в протоколе

OSPF. Протокол EBGP основан на формировании метрик, включающих различные атрибуты для построения оптимального маршрута.

Маршрутизатор, подключенный к глобальной сети (пограничный маршрутизатор), сообщает своим соседям, какие сети и автономные системы доступны через него. Обмен подобной информацией позволяет пограничным маршрутизаторам занести в таблицу маршрутизации записи о сетях, находящихся в других AS. При необходимости эта информация потом распространяется внутри автономной системы с помощью протоколов внутренней маршрутизации (OSPF, EIGRP, RIP).

Принципиальным отличием внешней маршрутизации от внутренней является наличие маршрутной политики, т. е. при расчете маршрута рассматриваются не только метрики и математические расчеты, но и множество других атрибутов. Алгоритмы расчета метрик в дистанционно-векторных протоколах и состояния каналов являются непригодными для глобальной маршрутизации, т. к. каждый узел передачи данных должен определять метрики и состояния самостоятельно, не полагаясь на расчет соседним устройством.

В протоколе BGP используется подход под названием «вектор пути», который, в отличие от вектора расстояний, содержит адрес сети и список атрибутов пути, описывающих различные характеристики маршрута от маршрутизатора-отправителя в указанную сеть.

Список атрибутов пути:

– AS_PATH – список номеров AS, через которые должен пройти пакет на пути в указанную сеть;

– NEXT_HOP – IP-адрес следующего маршрутизатора на пути достижения сети назначения;

– ORIGIN – обязательный атрибут, указывающий источник информации о маршруте: 0 – информация о достижимости сети получена от протокола внутренней маршрутизации или введена администратором; 1 – информация о достижимости сети получена от протокола внешней маршрутизации; 2 – INCOMPLETE – информация получена из перераспределения, например, из RIP в OSPF, а затем в BGP;

– MULTI_EXIT_DISC – необязательный атрибут, указывающий на приоритет использования объявляющего маршрутизатора для достижения через него анонсируемой сети, т. е. фактически это метрика маршрута с точки зрения анонсирующего маршрут BGP-маршрутизатора. Используется не само значение, а разница значений, когда несколько маршрутизаторов одной AS объявляют о достижимости через себя одной и той же сети, предоставляя получателям несколько вариантов маршрутов в эту сеть. Пакеты в объявляемую сеть будут посылаться через маршрутизатор, отправивший меньшее значение MULTI_EXIT_DISC;

– LOCAL_PREF – дополнительный атрибут, устанавливающий для данной AS приоритет данного маршрута среди всех маршрутов к заявленной сети;

– ATOMIC_AGGREGATE и AGGREGATOR – необязательные атрибуты, связанные с операциями агрегирования нескольких маршрутов в один.

Атрибут AS_PATH используется:

– для обнаружения петель: если номер одной и той же AS встречается в AS_PATH дважды, значит, маршрут неверно построен;

– для вычисления метрики маршрута: метрикой является число AS, через которые должен пройти пакет в сеть назначения;

– для применения маршрутной политики: если AS_PATH содержит номера недоступных AS, то данный маршрут исключается из рассмотрения.

Отличие IBGP от EBGP состоит в том, что при объявлении маршрута соседнему маршрутизатору, находящемуся в той же AS, маршрутизатор не должен добавлять в AS_PATH номер своей автономной системы. Если номер AS будет добавлен и соседний маршрутизатор анонсирует этот маршрут далее, то одна и та же AS будет указана в атрибуте AS_PATH дважды, что приведет к образованию петли.

Также для исключения петель используются серверы маршрутной информации (аналог выделенного маршрутизатора в OSPF), которые обслуживают группу BGP-маршрутизаторов. Принцип работы сервера маршрутной информации заключается в получении маршрутов от одного маршрутизатора группы и их рассылке другим маршрутизаторам. Маршрутные серверы также применяются для уменьшения числа соединений, в случае когда в одной физической сети находится много BGP-маршрутизаторов из различных AS (например, в точке обмена трафиком).

Точка обмена трафиком (IXP – Internet Exchange Point) – сетевая инфраструктура, посредством которой производится обмен сетевым трафиком, пропуск трафика между различными провайдерами без загрузки внешних магистральных каналов (например, в пределах одного региона, города или страны).

Маршрутизатор использует три базы данных (таблица 5.1) и две политики: политику приема маршрутов и политику анонсирования маршрутов. Для обработки маршрутов в базах данных в соответствии с имеющимися политиками маршрутизатор выполняет процедуру под названием «процесс отбора» (Decision Process), состоящую из следующих этапов [15]:

1 Для полученных маршрутов из базы данных ADJ-RIBS-IN в соответствии с политикой приема вычисляется приоритет и значение атрибута LOCAL_PREF, в результате некоторые маршруты могут быть признаны неприемлемыми.

2 Для каждой сети из всех имеющихся вариантов выбирается маршрут с бóльшим приоритетом, который заносится в базу LOC-RIB и таблицу маршрутизации.

3 Из LocRIB выбираются маршруты, соответствующие политике анонсирования, и результат помещается в базу Adj-RIBsOut, содержимое которой рассылается соседям.

Таблица 5.1 – Базы данных RIB (Routing Information Base) протокола BGP

Название	Описание
ADJ-RIBS-IN	Содержит маршрутную информацию, которая получена из сообщений UPDATE
LOC-RIB	Содержит локальную маршрутную информацию, которую маршрутизатор, руководствуясь маршрутной политикой, отобрал из ADJ-RIBS-IN
ADJ-RIBS-OUT	Содержит информацию, которую локальный маршрутизатор отобрал для рассылки соседям с помощью сообщений UPDATE

Отбор маршрутов из базы ADJ-RIBS-IN может производиться по следующим критериям:

– регулярное выражение для значения AS_PATH (частные случаи: номер конечной AS маршрута, AS соседа, от которого получен маршрут);

– адрес сети, в которую ведет маршрут;

– адрес соседа, приславшего информацию о маршруте;

– происхождение маршрута (атрибут ORIGIN).

К маршруту, удовлетворяющему установленному критерию, можно применить следующие политики:

– не принимать маршрут, удалить из ADJ-RIBS-IN;

– установить административный вес маршрута;

– установить значение атрибута LOCAL_PREF;

– установить маршрут в качестве маршрута по умолчанию.

Если после выполнения первого этапа отбора в базе ADJ-RIBS-IN имеется несколько альтернативных маршрутов, ведущих в одну сеть назначения, то отбор лучшего из них производится на втором этапе исходя из следующих критериев:

– наибольшее административное расстояние;

– наибольшее значение LOCAL_PREF;

– кратчайший AS_PATH (маршрут, порожденный в локальной AS, имеет самый короткий путь, а значит, пустое значение атрибута AS_PATH);

– наименьшее значение ORIGIN;

– наименьшее значение MULTI_EXIT_DISC;

– маршрут, полученный по EBGP, против маршрута, полученного по IBGP;

– если все маршруты получены по IBGP, то маршрут выбирается через ближайшего соседа;

– маршрут, полученный от BGP-соседа с наименьшим идентификатором (IP-адресом).

Критерии последовательно применяются в указанном порядке, пока не останется единственный маршрут.

Отбор маршрутов в базу ADJ-RIBS-OUT может производиться по следующим критериям:

– регулярное выражение для значения AS_PATH (номер конечной AS маршрута, AS соседа, от которого получен маршрут);

– адрес сети, в которую ведет маршрут;

– адрес соседа, которому этот маршрут объявляется;

– происхождение маршрута (атрибут ORIGIN).

К маршруту, соответствующему установленному критерию, можно применить следующие политики:

– не объявлять маршрут;

– не устанавливать значение MULTI_EXIT_DISC, установить указанное значение, взять в качестве значения метрику маршрута из IGP;

– произвести агрегирование сетей;

– модифицировать AS_PATH;

– заменить маршрут на маршрут по умолчанию.

В протоколе BGP используются следующие типы сообщений [13]:

– OPEN – посылается после установления TCP-соединения, ответом на которое является сообщение KEEPALIVE, если вторая сторона согласна стать соседом; иначе посылается сообщение NOTIFICATION с кодом, поясняющим причину отказа;

– KEEPALIVE – предназначено для подтверждения согласия на установление соседских отношений, а также для мониторинга активности открытого соединения: BGP-соседи обмениваются KEEPALIVE-сообщениями через определенные интервалы времени;

– UPDATE – предназначено для анонсирования и отзыва маршрутов. После установления соединения с помощью сообщений UPDATE пересылаются все маршруты, которые маршрутизатор хочет объявить соседу, после чего пересылаются только данные о добавленных или удаленных маршрутах по мере их появления;

– NOTIFICATION – используется для информирования соседа о причине закрытия соединения.

Как правило, протокол BGP настраивается на маршрутизаторе, подключаемом к глобальной сети, следующим образом:

```
router bgp номер_AS
network адрес_выданного_блока_IP-адресов mask маска_блока
network адрес_подключенной_сети mask маска
neighbor адрес_BGP-маршрутизатора_первого_провайдера
neighbor адрес_BGP-маршрутизатора_второго_провайдера
```

Рассмотрим пример конфигурации протокола BGP для сети, смоделированной в лабораторной работе № 3 (см. рисунок 2.6), которую назовем MTS. К сети MTS с номером автономной системы 25106 подключены автономные системы Beltelecom (AS6697) с маршрутизацией RIP, RETN (AS9002) с маршрутизацией EIGRP, BeCloud (AS60330) с маршрутизацией OSPF. Краткая структурная схема сети представлена на рисунке 5.1. На рисунке 5.2 представлена расширенная схема данной сети.

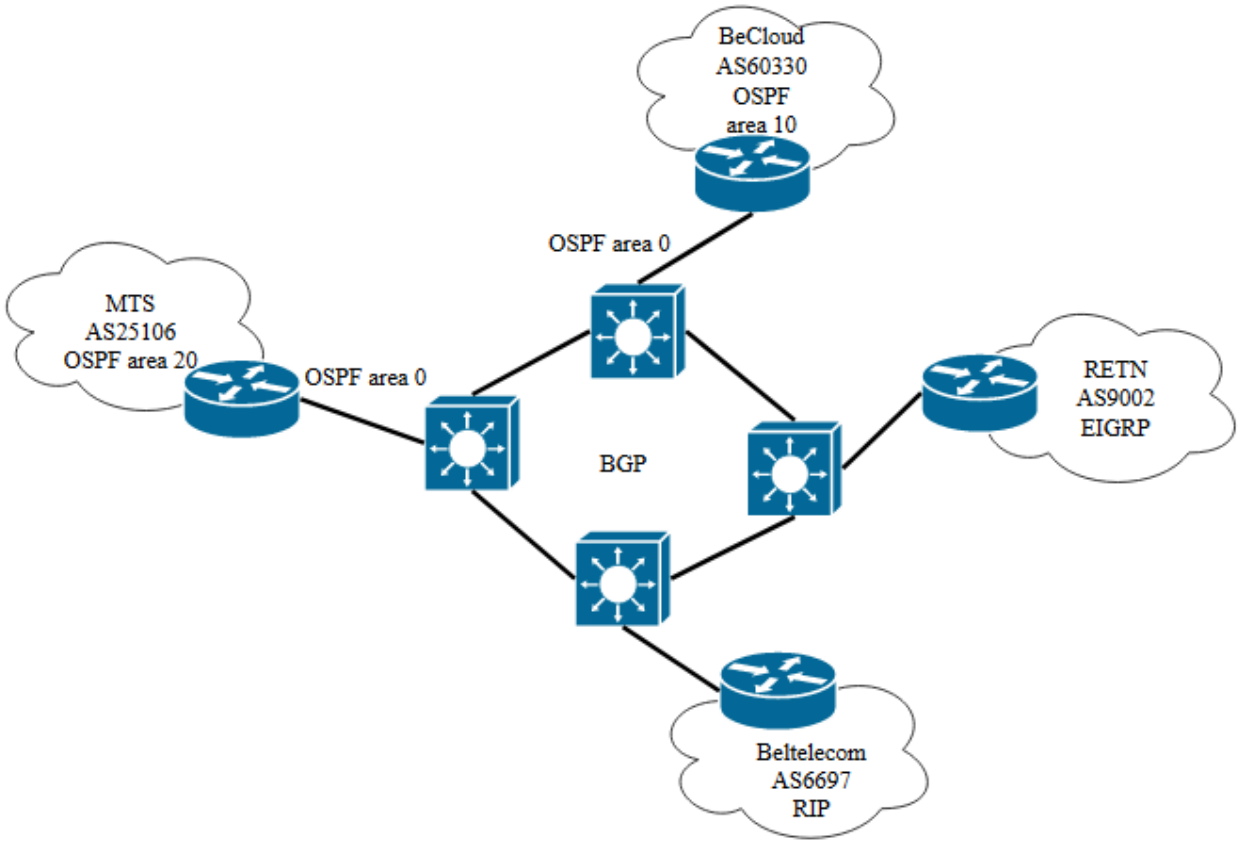

Рисунок 5.1 – Структурная схема соединения сетей

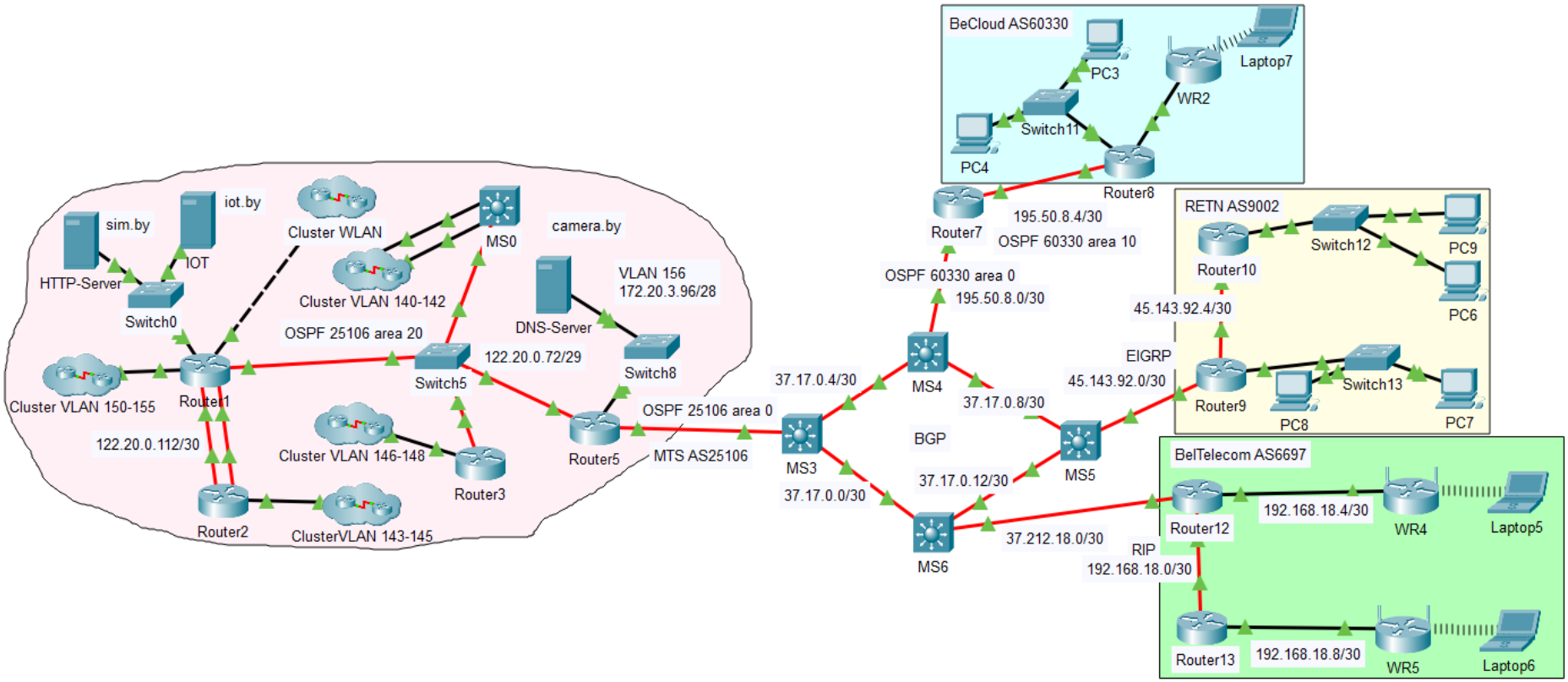

Рисунок 5.2 – Расширенная схема сети с применением протокола BGP

Все сети соединяются посредством подсетей из коммутаторов L3 с маршрутизацией BGP. Подсети Building1 (VLAN 140–142), WLAN, VLAN 150–155, VLAN 143–145, VLAN 146–148 сгруппированы в кластеры в сети MTS. Для создания кластера необходимо выделить группу объектов, которые будут принадлежать одному кластеру и нажать кнопку New Cluster (рисунок 5.3). В результате вместо данных объектов появится облако, нажав на которое можно перейти к содержимому кластера. В случае если объекты нужно вернуть из кластера на главную рабочую область, их необходимо выделить, нажать на кнопку Move object и во всплывающем меню выбрать Move to Root (рисунок 5.4). Таким образом, с помощью кластеров можно компактно представить большую сеть.

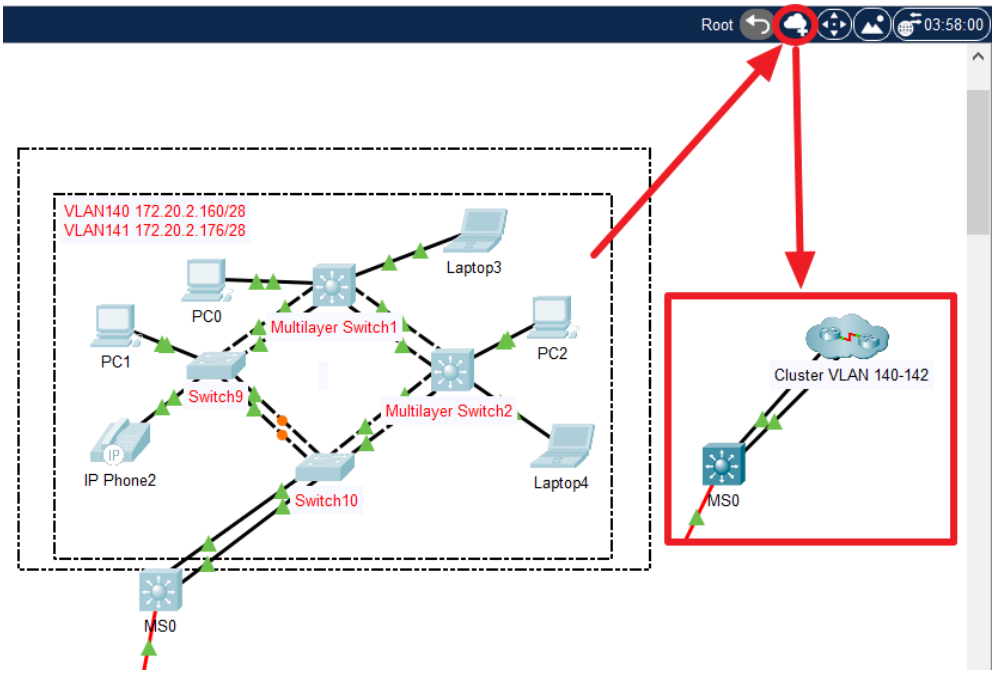

Рисунок 5.3 – Добавление объектов в кластер

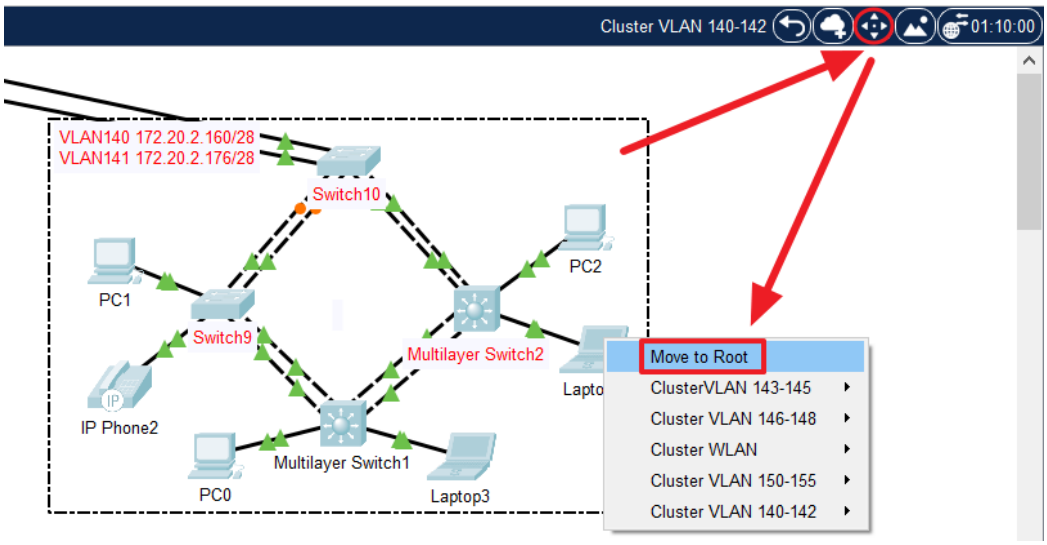

Рисунок 5.4 – Перемещение объекта на главную рабочую область

В сети на рисунках 5.1, 5.2 присутствует четыре автономные системы (AS25106, AS6697, AS9002, AS60330). Рассмотрим пример конфигурации BGP-протокола на коммутаторе L3 MS3 для AS25106. Необходимо отметить, что на коммутаторе L3 MS3 настроен протокол OSPF со значением Process ID, равным 25106, и областью 0. Также на маршрутизаторе Router5 настроено административное суммирование маршрутов к подсетям между маршрутизаторами в AS25106, подсети Building1 (VLAN 140–142), WLAN, VLAN 150–155, VLAN 143–145, VLAN 146–148. Для конфигурации протокола BGP использовались следующие команды:

```
SW3(config)#router bgp 25106
SW3(config-router)#neighbor 37.17.0.6 remote-as 60330
SW3(config-router)#neighbor 37.17.0.2 remote-as 6697
SW3(config-router)#network 37.17.0.4 mask 255.255.255.252
SW3(config-router)#network 37.17.0.0 mask 255.255.255.252
SW3(config-router)#network 134.17.215.0 mask 255.255.255.252
SW3(config-router)#redistribute ospf 25106
```

Аналогичным образом осуществляется конфигурация BGP-протокола на остальных коммутаторах L3. Как видно из представленных выше команд, для согласования работы протокола OSPF и BGP использовалось перераспределение маршрутов из OSPF в BGP. Аналогично было активировано перераспределение из BGP в OSPF в конфигурации маршрутизации OSPF. При этом, если в OSPF настроена передача маршрута по умолчанию в области, то конфигурация перераспределения маршрутов из BGP в OSPF является излишней, т. к. значительно увеличится размер таблиц маршрутизации.

Между маршрутизатором Router7 и коммутатором L3 MS4 настроена маршрутизация по протоколу OSPF со значением Process ID, равным 60330, и областью 0 и перераспределение маршрутов из BGP в OSPF и обратно.

Необходимо отметить, что магистральная область настраивается между коммутатором L3 и маршрутизатором, подключенным к нему, между остальными маршрутизаторами настраивается транзитная область.

Правильность настройки протокола BGP можно проверить с помощью команды `show ip route`, `show ip bgp neighbors`, `sh ip bgp summary`.

На коммутаторе L3 кроме конфигурации протокола маршрутизации BGP настраивается протокол EIGRP, в котором необходимо предусмотреть перераспределение маршрутов из BGP с помощью команды `redistribute bgp 9002 metric 1000000 10 255 1 65355`. Обратное перераспределение

осуществляется в конфигурации протокола BGP с помощью команды `redistribute eigrp 9002`.

Для осуществления перераспределения между протоколами RIP и BGP используются аналогичные команды, представленные выше. Однако ограничения среды моделирования Cisco PT не позволяют осуществлять перераспределение между протоколами RIP и BGP. Для передачи маршрутов к сетям AS6697 на коммутаторе L3 в протоколе BGP была настроена сеть 37.212.18.0/30. На маршрутизаторе Router12 настроено преобразование частных IP-адресов с помощью трансляции PAT в IP-адрес 37.212.18.2.

5.2 Лабораторное задание

Лабораторная работа выполняется на основе настроек, выполненных в лабораторной работе № 3 (файл **LAB3-3.pkt**). До начала выполнения необходимо открыть сохраненный файл **LAB3-3.pkt** и проверить настройки IP-адресации: у всех устройств адресация должна соответствовать заданным IP-адресам из таблиц 1.2 и 3.3, маршрутизация должна быть настроена по протоколу OSPFv2 со значением Process ID, равным номеру шифра студента, и значением области больше 1. В сети должны быть подсети с VLAN, подсеть с беспроводным маршрутизатором, подсеть Building1, подсети с устройствами освещения, контроля температуры и дыма, видеонаблюдения, контроля доступа и пожаротушения, три сервера: на одном сервере должны отображаться состояния устройств освещения, контроля температуры и дыма (сервер iot.by на рисунке 3.7), на втором сервере должны отображаться состояния устройств видеонаблюдения, контроля доступа и пожаротушения (сервер camera.by на рисунке 3.7), на третьем – веб-сайт, разработанный в лабораторной работе № 5 лабораторного практикума «Основы построения локальных сетей» [10], доменное имя которого должно соответствовать фамилии студента. С любого устройства из любой подсети должен быть доступ к серверам. В сети должны работать различные технологии в соответствии с заданиями лабораторной работы № 3. Агрегирование каналов между коммутаторами должно быть настроено с помощью протокола PVST и LACP для локальной сети Building1 и протокола RSTP и PAgP для локальной сети с VLAN.

В лабораторной работе необходимо расширить смоделированную в лабораторной работе № 3 сеть и настроить согласованную работу протоколов маршрутизации OSPF, RIP, EIGRP, BGP.

1 *Подключение сети NET1*. В смоделированную сеть из лабораторной работы № 3, добавить четыре коммутатора L3, которые соединить в кольцевую топологию (рисунок 5.5). Между коммутаторами настроить публичные IP-адреса, выделенные из заданного IP-адреса (таблица 5.2). Один из коммута-

торов L3 подключить к маршрутизатору смоделированной ранее сети (NET1 на рисунке 5.5).

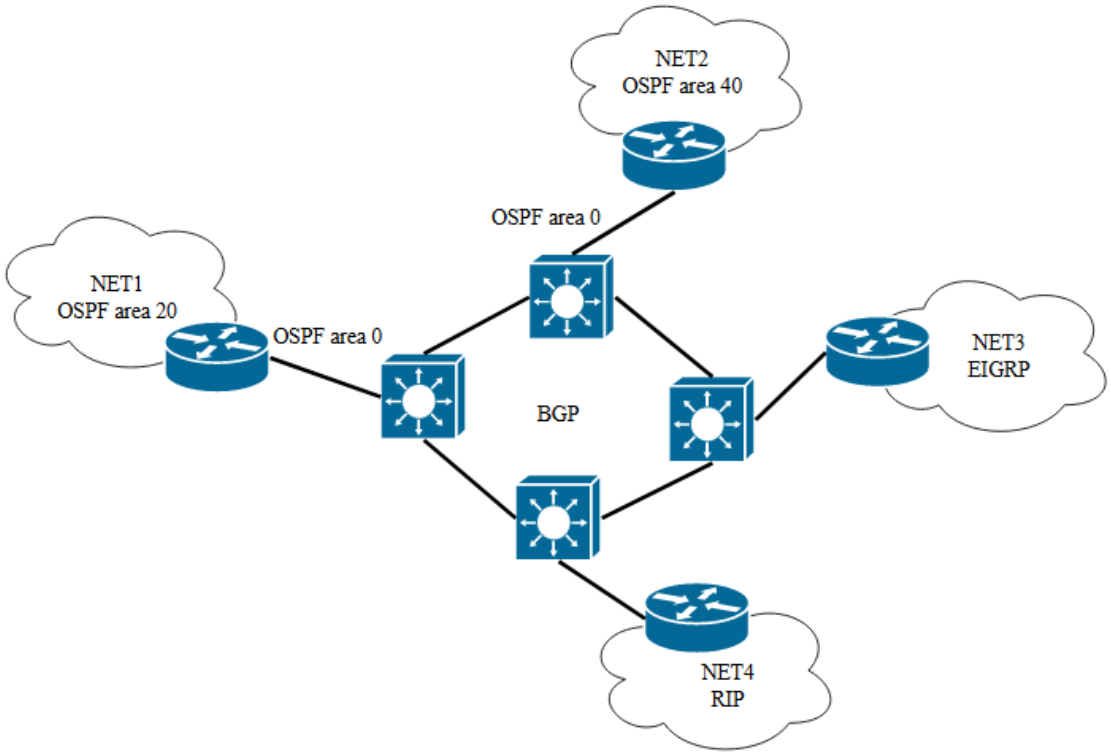

Рисунок 5.5 – Структурная схема сети, требуемой для моделирования

Таблица 5.2 – Исходные данные для конфигурации публичных IP-адресов в сетях

Номер первой цифры шифра	Публичные IP-адреса для подсетей			
	NET1	NET2	NET3	NET4
0	178.175.0.0/18	64.37.44.0/23	23.156.32.0/24	74.116.58.0/24
1	204.79.86.0/23	76.8.36.0/24	50.21.237.0/24	64.114.78.0/24
2	199.0.80.0/20	38.75.80.0/22	96.1.244.0/22	75.154.144.0/22
3	200.49.4.0/22	199.16.251.0/24	154.20.0.0/16	142.169.76.0/22
4	1.70.0.0/16	66.249.145.0/24	199.175.31.0/24	204.174.146.0/24
5	62.115.192.0/19	2.22.72.0/22	209.44.105.0/24	8.21.39.0/24
6	41.79.200.0/24	38.102.69.0/24	12.129.102.0/23	199.106.40.0/21
7	103.68.35.0/24	66.54.125.0/24	72.51.10.0/24	104.36.148.0/23
8	5.178.16.0/21	41.221.218.0/23	139.123.232.0/24	23.133.112.0/24
9	128.9.28.0/23	115.126.41.0/24	23.137.80.0/24	102.23.100.0/22

IP-адрес для подсети NET1, соединяющей коммутатор L3 и пограничный маршрутизатор сети NET1, выделить из заданного IP-адреса в таблице 5.2.

В сети NET1 должен работать протокол OSPF со значением Process ID, равным номеру шифра студента, и значением области 20. Настроить между подключенным коммутатором L3 и пограничным маршрутизатором сети NET1 протокол OSPF со значением Process ID, равным номеру шифра студента, и значением области, равным 0. На пограничном маршрутизаторе сети NET1 настроить административное суммирование по протоколу OSPF. В отчете представить таблицу маршрутизации на подключенном к сети NET1 коммутаторе L3, в которой видны суммарные маршруты OSPF к подсетям NET1. На коммутаторе L3, подключенном к сети NET1, настроить маршрут по умолчанию в глобальную сеть, который будет передаваться по протоколу OSPF в подсети NET1.

2 *Подключение сети NET2*. Ко второму коммутатору L3 подключить подсеть NET2, в которой должны быть коммутатор L2, два проводных маршрутизатора, один беспроводной маршрутизатор, минимум три оконечных устройства (см. рисунок 5.1). В подсети NET2 организовать автоматическую раздачу частных IP-адресов оконечным устройствам в соответствии с заданным в таблице 5.3 IP-адресом. Публичный IP-адрес для подсетей, соединяющих коммутатор L3 и внутренние маршрутизаторы сети NET2, выделить из заданного в таблице 5.3 IP-адреса. Настроить на маршрутизаторе в подсети NET2 и подключенном к нему коммутаторе L3 протокол маршрутизации OSPF с областью 0, для остальных маршрутизаторов сети NET2 настроить протокол OSPF с областью 40. В отчете представить таблицу маршрутизации на подключенном к сети NET2 коммутаторе L3, в которой видны маршруты, переданные по протоколу OSPF.

Таблица 5.3 – Исходные данные для конфигурации частных IP-адресов в сетях

Номер второй цифры шифра	Частные IP-адреса для подсетей		BGP
	NET2	NET3	
0	192.168.0.0/24	192.168.1.0/24	213.163.99.0/24
1	192.168.10.0/24	192.168.11.0/24	207.209.184.0/21
2	192.168.20.0/24	192.168.21.0/24	204.152.185.0/24
3	192.168.30.0/24	192.168.31.0/24	64.76.0.0/21
4	192.168.40.0/24	192.168.41.0/24	202.38.121.0/24
5	192.168.50.0/24	192.168.51.0/24	62.115.248.0/21
6	192.168.60.0/24	192.168.61.0/24	129.134.131.0/24
7	192.168.70.0/24	192.168.71.0/24	128.42.0.0/16
8	192.168.80.0/24	192.168.81.0/24	148.201.0.0/16
9	192.168.90.0/24	192.168.91.0/24	198.32.16.0/24

3 *Подключение сети NET3.* К третьему коммутатору L3 подключить подсеть NET3, в которой должны быть два маршрутизатора и не меньше трех оконечных устройств (см. рисунок 5.1). В подсети NET3 организовать автоматическую раздачу частных IP-адресов оконечным устройствам в соответствии с заданным в таблице 5.3 IP-адресом. IP-адрес для подсетей, соединяющих коммутатор L3 и внутренние маршрутизаторы сети NET3, выделить из IP-адреса, заданного в таблице 5.2. Настроить на маршрутизаторе в подсети NET3 и подключенном к нему коммутаторе L3 протокол маршрутизации EIGRP. В отчете представить таблицу маршрутизации на подключенном к сети NET3 коммутаторе L3, в которой видны маршруты, переданные по протоколу EIGRP.

4 *Подключение сети NET4.* К четвертому коммутатору L3 подключить подсеть NET4, в которой должны быть два проводных и два беспроводных маршрутизатора, а также не меньше двух оконечных устройств (см. рисунок 5.1). В подсети NET4 организовать автоматическую раздачу частных IP-адресов оконечным устройствам в соответствии с IP-адресом, заданным в таблице 5.3. Публичный IP-адрес для подсети, соединяющей коммутатор L3 и внутренний маршрутизатор сети NET4, выделить из IP-адреса, заданного в таблице 5.2. Настроить в сети NET4 протокол RIP. В отчете представить таблицу маршрутизации на подключенном к сети NET4 коммутаторе L3, в котором видны маршруты, переданные по протоколу RIP.

5 *Конфигурация протокола BGP на коммутаторах L3*. Для каждой подсети (см. рисунок 5.5) использовать номера автономных систем, заданные в таблице 5.4. Настроить перераспределение маршрутов из других протоколов в BGP и обратно. Проверить таблицы маршрутизации всех коммутаторов L3 и проследить, чтобы в них были перераспределенные маршруты из других протоколов и маршруты BGP. Представить в отчете таблицы маршрутизации всех добавленных коммутаторов L3, а также результаты команд `show ip route`, `show ip bgp neighbors`, `sh ip bgp summary` на одном из коммутаторов L3. Сохранить файл под именем **LAB5-1.pkt**.

Таблица 5.4 – Номера автономных систем для подсетей в смоделированной сети

Номер третьей цифры шифра	Номера автономных систем для подсетей			
	NET1	NET2	NET3	NET4
0	5414	5576	6843	8661
1	174	286	577	1220
2	1239	1251	1280	2635

Продолжение таблицы 5.4

Номер третьей цифры шифра	Номера автономных систем для подсетей			
	NET1	NET2	NET3	NET4
3	2924	3257	3273	3549
4	3257	3300	3460	3717
5	701	714	766	1299
6	37461	37612	37665	63293
7	6	8	10	12
8	2708	2904	3073	3141
9	20	21	22	23

5.3 Содержание отчета

1 Цель работы, исходные данные из таблиц 5.2–5.4.

2 Результаты произведенных настроек из пунктов 1–5, изображение смоделированной сети.

3 Вывод по работе.

4 Ответы на контрольные вопросы.

5.4 Контрольные вопросы

1 Организация доступа к глобальной сети, типы операторов связи.

2 Автономная система, ее регистрация, типы регистраторов.

3 Принципы функционирования протокола BGP для внутренней и внешней маршрутизации.

4 Список атрибутов BGP, расчет метрики.

5 Процесс отбора маршрутов по протоколу BGP, базы данных BGP.

6 Типы сообщений BGP.

7 Принцип конфигурации BGP и перераспределения маршрутов из других протоколов.

ЛАБОРАТОРНАЯ РАБОТА № 6
ДОМЕННЫЕ ЗОНЫ. АУТЕНТИФИКАЦИЯ В МАРШРУТИЗАЦИИ

Цель: изучить принципы построения доменных зон, процесса обмена сообщениями между DNS-серверами, уметь конфигурировать аутентификацию между устройствами.

6.1 Теоретическая часть

Доменная зона (домен) – область иерархического пространства доменных имен глобальной сети, которая обозначается уникальным доменным именем.

Доменное имя – символьное (буквенно-цифровое) обозначение, сформированное в соответствии с международными правилами адресации сети Интернет, предназначенное для поименованного обращения к интернет-ресурсу и связанное при его делегировании с определенным сетевым адресом [16].

Протокол DNS необходим не только для преобразования доменного имени в IP-адрес и наоборот, но и для поиска доменного имени в иерархической распределенной системе хранения и обработки информации о доменных зонах. Такая распределенная система доменных зон очень важна в глобальной сети, т. к. на одном сервере не могут храниться соответствия всех доменных имен и их IP-адресов.

Существуют доменные зоны, принадлежащие определенным организациям.

Распределение доменных имен в доменных зонах образует дерево имен со следующим уровнями (рисунок 6.1):

– нулевой уровень, или корневой домен, обозначается точкой, которая обычно не указывается, регистратором корневого домена является организация ICANN;

– первый уровень, или национальные (региональные) домены, или Top-Level Domain (TLD), принадлежат государственным организациям или крупным корпорациям, так, например, администратором национальной доменной зоны .by является Оперативно-аналитический центр при Президенте Республики Беларусь, а доменов .net и .com – компания VeriSign;

– второй уровень, или Second-Level Domain (SLD), домены отражают название организации, владеющей веб-ресурсом, или тематику ресурса, регистраторами в Республике Беларусь являются ООО «Белорусские облачные технологии» (becloud.by), ООО «Надежные программы» (hoster.by), ООО «Открытый контакт» (www.domain.by) и др.;

– третий уровень, или поддомены, представляют собой расширения доменного имени, необходимы для функционального расширения веб-ресурсов, обозначают дочерние веб-ресурсы.

Редко можно встретить доменные имена, включающие четвертый и последующие уровни.

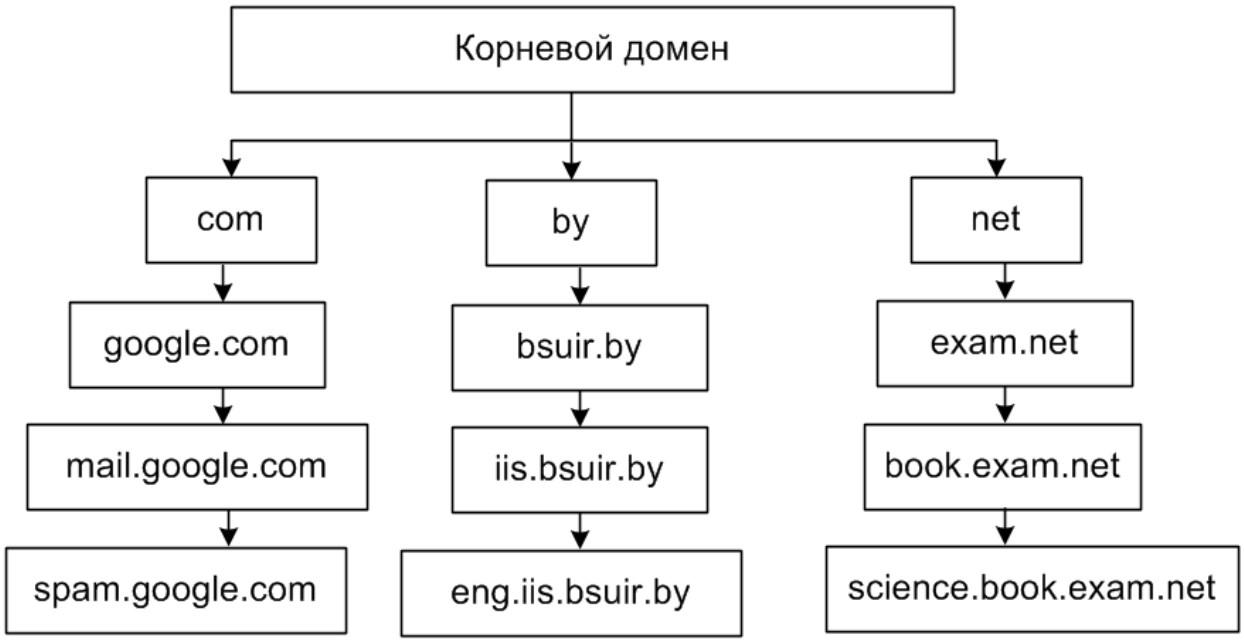

Рисунок 6.1 – Пример дерева доменных имен

Таким образом, корневая доменная зона содержит записи всех доменных зон первого уровня, а доменные зоны первого уровня содержат зарегистрированные в них домены второго уровня и т. д.

В инфраструктуре системы доменных имен выделяют следующие компоненты:

– дерево серверов DNS;

– клиент DNS, ПО, генерирующее запросы DNS на оконечном устройстве;

– DNS-резолвер, или сервер разрешения имен DNS, предназначенный для получения запросов от клиента и выполняющий поиск необходимого IP-адреса в дереве доменных имен.

Для регистрации доменного имени сервера в глобальной сети необходимо зарегистрировать его у регистратора доменных имен, например, hoster.by. Перед регистрацией можно проверить, свободно ли доменное имя в интернет-пространстве на сайте регистратора доменных имен или с помощью утилиты nslookup (рисунок 6.2). Регистрация доменного имени является платной услугой, оформляется на определенный период. После покупки и активации доменного имени необходимо приобрести хостинг-пространство (ресурсы для размещения веб-сайта).

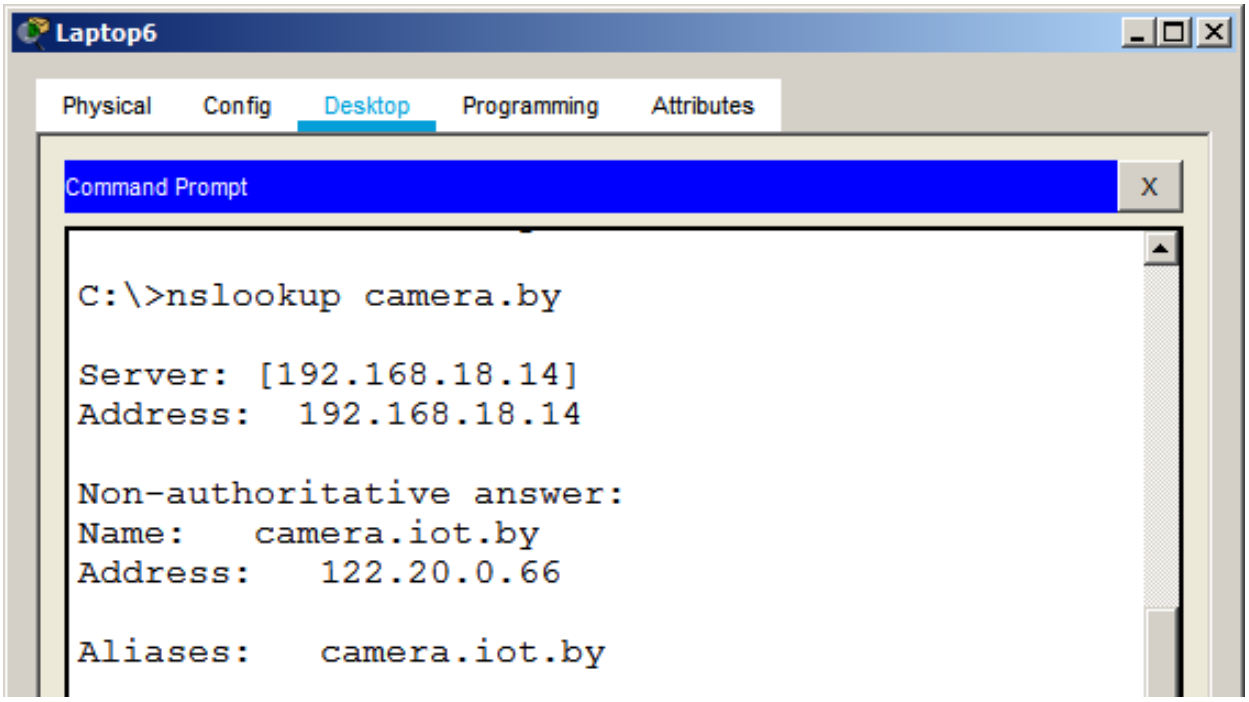

Рисунок 6.2 – Использование утилиты nslookup для проверки доменного имени camera.by

В конфигурации практически любого устройства указывается IP-адрес первичного (приватного, внутреннего) и вторичного (публичного, внешнего) DNS-серверов. Как правило, первичный DNS-сервер – это сервер организации или интернет-провайдера, является DNS-резолвером, и в случае, если он недоступен, то DNS-запросы отправляются на вторичный DNS-сервер. Наиболее популярным публичным DNS-резолвером является Google Public DNS, который имеет IP-адрес 8.8.8.8.

К основным функциям DNS-резолвера относятся:

– рекурсия – модель обработки запросов DNS-сервером, при которой осуществляется поиск доменных имен посредством обращения к другим DNS-серверам;

– кеширование – временное хранение в памяти DNS-сервера информации, получаемой в DNS-ответах;

– TTL (Time to Live) – предельно допустимое время кеширования, содержится в поле TTL рекурсной записи.

Рассмотрим вышеописанные свойства на примере. Если пользователь вводит в браузере доменное имя iis.bsuir.by, сначала проверяется кеш DNS. Дополнительно проверить кеш DNS можно с помощью команды `ipconfig /displaydns` в командной строке ОС Windows (рисунок 6.3). Очистка DNS-кеша осуществляется с помощью команды `ipconfig /flushdns`.

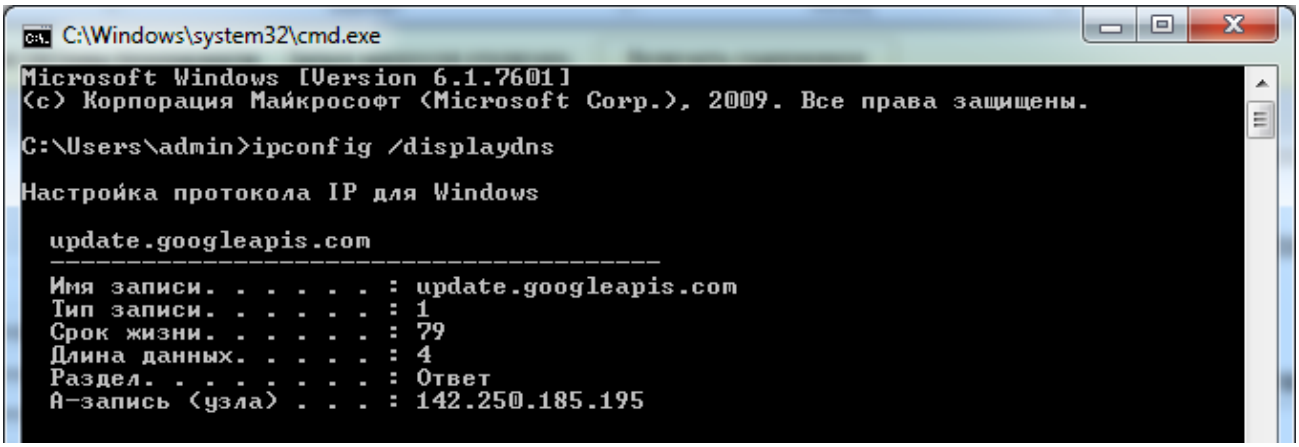

Рисунок 6.3 – Просмотр кеша DNS оконечного утройства

В случае если к ресурсу iis.bsuir.by пользователь обращается впервые, то формируется DNS-запрос к DNS-резолверу. Если первичный сервер, IP-адрес которого внесен в сетевые настройки, будет недоступен или не будет иметь запись о запрашиваемом ресурсе, формируется запрос ко вторичному DNS-серверу. Когда к DNS-резолверу поступает запрос от клиента, он проверяет свой кеш. В случае если в кеше нет записи о доменном имени iis.bsuir.by, то DNS-резолвер формирует запрос к DNS-серверу в корневом домене, который находится в регионе страны, например, домене .by. Как правило, корневой сервер имеет информацию об IP-адресах TLD-серверов в домене .by, IP-адрес одного из них и отправляется DNS-резолверу. Получив ответ от корневого сервера, DNS-резолвер формирует новый запрос к TLD-серверу в домене .by. TLD-сервер по доменному имени определяет IP-адрес авторитетного сервера имен (Authoritative Name Server), который имеет базу данных для доменных имен bsuir.by. Авторитетным сервером имен является DNS-сервер, который удовлетворяет запросы из своих собственных баз данных без необходимости ссылаться на другой DNS-сервер. Получая ответ от TLD-сервера, DNS-резолвер направляет запрос авторитетному серверу. Если сервер находит в базе данных доменное имя iis.bsuir.by, то он возвращает его IP-адрес DNS-резолверу. Если доменное имя не существует в глобальной сети, то будет отправлен отрицательный ответ. DNS-резолвер сохраняет полученную информацию в своем кеше и передает клиенту.

Для настройки DNS-серверов используются следующие основные типы записей [17]:

– A Record – указывает на точное соответствие IPv4-адреса и доменного имени сервера;

– AAAA (IPv6 Address Record) – указывает на точное соответствие IPv6-адреса и доменного имени сервера;

– NS (Name Server) – указывает на DNS-сервер для данного домена, обычно для стабильной работы домена указывается не менее двух NS-записей, т. к. в случае недоступности одного из DNS-серверов запрос отправляется на другой DNS-сервер;

– CNAME (Canonical Name Record) – каноническая запись имени, используется для перенаправления на другое доменное имя;

– MX (Mail Exchange) – указывает сервер обмена почтой для данного домена;

– SOA (Start of Authority) – начальная запись зоны, указывает местоположение эталонной записи о домене, содержит в себе контактную информацию лица, ответственного за данную зону, время кеширования информации на серверах и данные о взаимодействии DNS.

В программе Cisco Packet Tracer запись SOA содержит следующие параметры:

– имя домена;

– имя первичного DNS-сервера (Primary Name Server) в домене;

– Minimum TTL – определяет минимальное «время жизни» записей в кеше DNS;

– Retry Time – время ожидания вторичным сервером перед тем, как повторить попытку опроса доступности первичного сервера, если предыдущая попытка оказалась неудачной;

– Expire Time – время, в течение которого вторичный сервер обслуживает домен, в случае недоступности первичного севера;

– Refresh Time – время опроса вторичным сервером доступности первичного;

– Mail Box – почтовый адрес администратора доменной зоны.

Порядок записей в базе данных DNS-серверов не имеет значения за одним исключением: запись SOA должна идти первой. Дальнейшие записи считаются относящимися к той же зоне, пока не встретится новая запись SOA. Как правило, после записи зоны указывают записи DNS-серверов, а остальные записи располагают по алфавиту.

Рассмотрим пример организации DNS для сети на рисунке 6.4. В подсети BelTelecom размещен локальный DNS-сервер (Local DNS-server), IP-адрес которого выдается по DHCP всем оконечным устройствам в подсетях MTS, Becloud, RENT, BelTelecom. На локальном DNS-сервере настроена рекурсия к корневому серверу (ROOT DNS-server), который находится в подсети RENT.

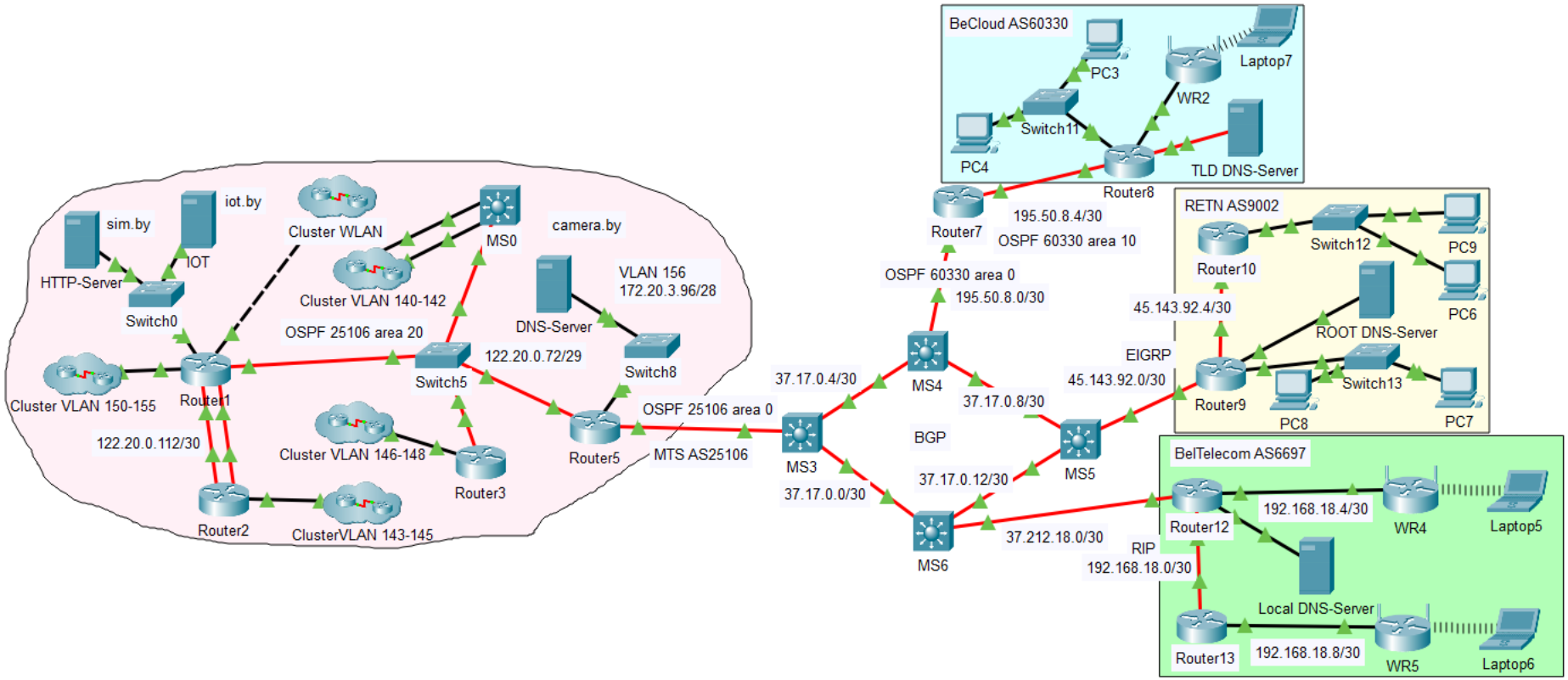

Рисунок 6.4 – Модель сети с доменной зоной .by

Для конфигурации рекурсии в службе DNS Local DNS-server создаются две записи:

– запись NS (Name Server), которая указывает на DNS-сервер ROOT для домена .by;

– запись A Record, которая указывает на точное соответствие IPv4-адреса и доменного имени сервера ROOT.

На корневом сервере ROOT DNS-server настраивается рекурсия к доменам iot через TLD-сервер, для этого создаются четыре записи в DNS службе ROOT DNS-server (рисунок 6.5).

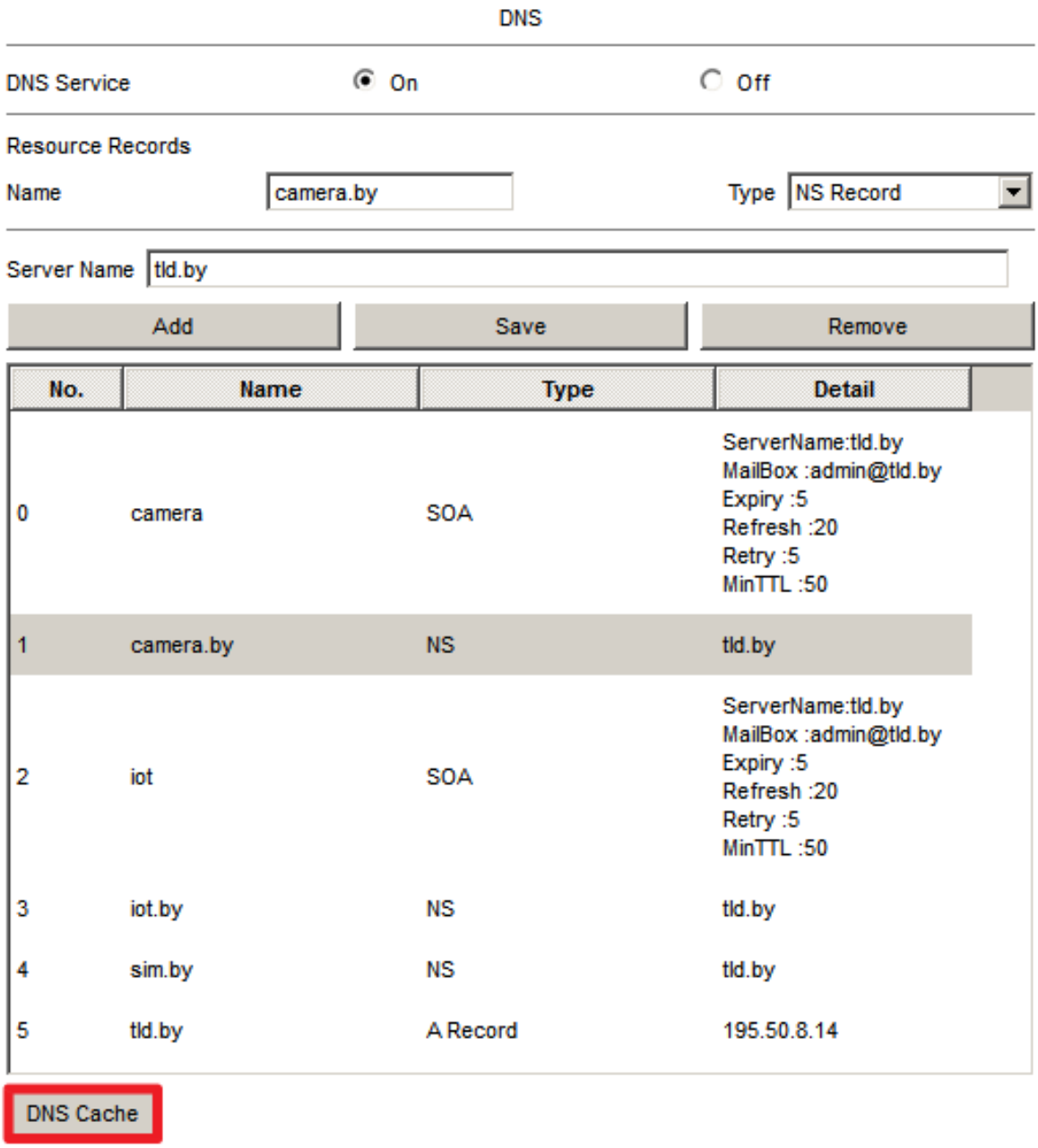

Рисунок 6.5 – Конфигурация записей SOA, NS, A Record на ROOT DNS-сервере

Для параметров Minimum TTL, Retry Time, Expire Time, Refresh Time заданы достаточно короткие интервалы времени. Также в записи SOA указан e-mail, который создан на TLD-сервере. В результате получения ответов от TLD-сервера соответствие IP-адресов и доменных имен вносится в кеш корневого сервера, который можно просмотреть, нажав кнопку DNS Cache. Пример содержимого кеша корневого сервера представлен на рисунке 6.6.

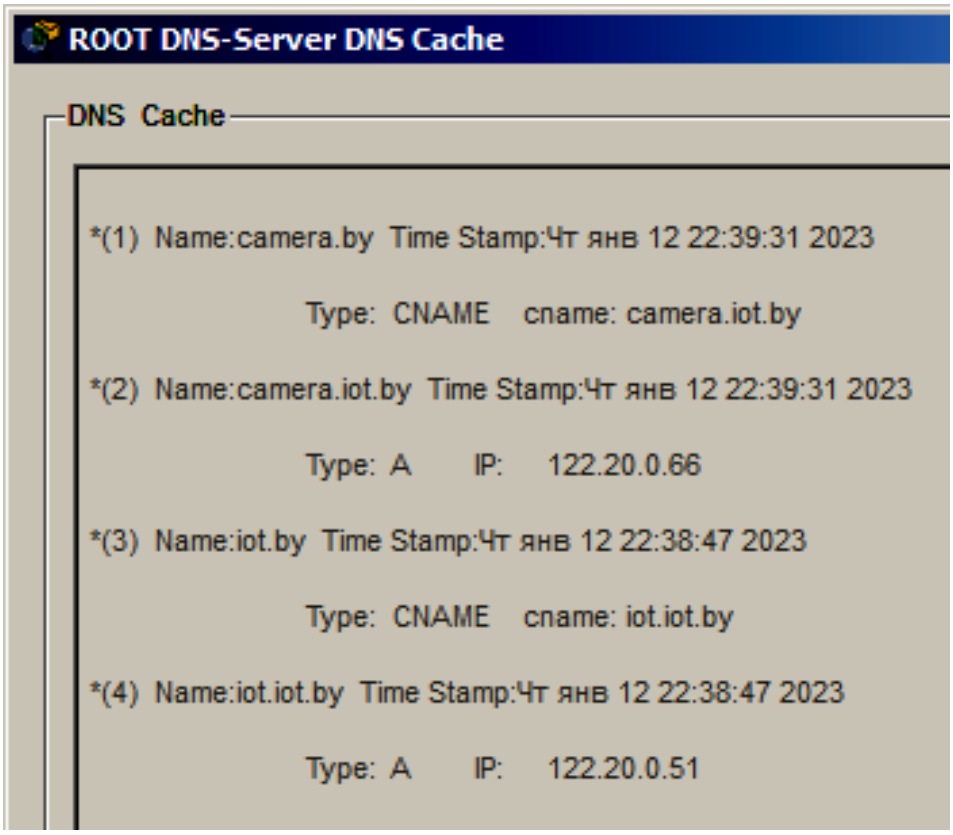

Рисунок 6.6 – Кеш корневого сервера ROOT DNS-server

TLD-сервер располагается в автономной системе BeCloud (AS60330) (см. рисунок 6.4), на нем с помощью четырех записей настроена рекурсия к авторитарному серверу camera.by:

– SOA-запись с названием authority для авторитарного DNS-сервера authority.iot.by, которая содержит адрес электронной почты администратора на сервере iot.by и представленные выше значения временных параметров;

– две записи NS (Name Server), которые указывают на авторитарный DNS-сервер authority.iot.by для доменов iot.by и camera.by;

– запись A Record, которая указывает на точное соответствие IPv4-адреса и доменного имени авторитарного сервера.

Авторитарный сервер реализован на сервере camera.by, на котором настроены записи A Record для доменных имен ROOT, iot.by, camera.by. Доменное имя iot.by в конфигурации авторитарного сервера с помощью

CNAME-записи заменяется на iot.iot.by, для которого создана отдельная запись A Record.

Таким образом, при получении доступа к серверу camera.by с какого-либо устройства в подсети BelTelecom AS6697, будет генерироваться DNS-запрос к серверу Local DNS-server, т. к. его IPv4-адрес выдается по DHCP и сохраняется в сетевых настройках данного устройства. Local DNS-server проверяет свой кеш: если в нем нет записей о требуемом домене, он обращается к корневому серверу ROOT в соответствии с записями NS и A Record, формируя рекурсивный запрос к корневому серверу. Запрос от Local DNS-server на корневом сервере проверяется сначала в кеше, а потом в базе данных. В соответствии с записями SOA для домена camera определяется TLD-сервер и его IP-адрес (запись A Record). Когда запрос приходит на TLD-сервер, также проверяются записи NS для доменного имени camera.by, определяется авторитарный сервер, проверяется запись SOA для авторитарного сервера и определяется его IPv4-адрес по записи A Record. При получении запроса авторитарный сервер в соответствии с записью CNAME определяет, что домен camera.by стал доменом третьего уровня в домене iot.by, и в DNS-ответе выдает IPv4-адрес для доменного имени camera.iot.by в соответствии с записью A Record. Этот DNS-ответ кешируется на всех ROOT-, TLD-, Local DNS-серверах. Кеш всех DNS-серверов можно просмотреть, нажав кнопку DNS Cache (см. рисунки 6.5, 6.6). При вводе команды `nslookup iot.by` на оконечном сервере подсети BelTelecom AS6697 будет получена информация о доменном имени camera.iot.by (см. рисунок 6.2).

Одной из уязвимостей протокола DNS является отсутствие проверки ответов от рекурсивных DNS-серверов на валидность. Эта уязвимость может быть использована нарушителем для реализации кибератаки «отравление кеша». Нарушитель отправляет на рекурсивные DNS-серверы неверное соответствие доменного имени и IP-адреса, в качестве последнего указывая IP-адрес своего сервера. Таким образом, в кеше рекурсивного DNS-сервера будет храниться неверная запись, которая будет выдаваться в ответах на запросы от других серверов, что приведет к перенаправлению пользователей на нелегитимный сервер, а следовательно, к дезинформации пользователей или краже персональных данных. Поэтому рекомендуется использовать протокол DNSSEC.

DNSSEC (Domain Name System Security Extensions) – усовершенствованный протокол DNS, выполняющий все его функции с проверкой достоверности ответов DNS и подлинности DNS-серверов посредством цифровой подписи.

В каждой доменной зоне есть пара ключей: закрытый и открытый. Закрытый ключ используется для подписи данных в сообщении DNS. На его основе генерируются цифровые подписи. Открытый ключ зоны свободно распростра-

няется среди других доменных зон. Любой рекурсивный сервер получает открытый ключ и использует его для проверки подлинности данных DNS. Если подлинность подтверждается, то данные считаются настоящими и далее передаются внутри доменной зоны. Если подпись не проходит проверку подлинности, то предполагается попытка «отравления» кеша, внутри зоны передается ошибка.

Процесс аутентификации также важен при маршрутизации. Например, маршрутизация может быть нарушена в результате фальсификации информации, передаваемой в сообщениях протоколов маршрутизации. Информация о фальсифицированной маршрутизации обычно может использоваться для того, чтобы заставить маршрутизаторы дезинформировать друг друга, что может привести к кибератакам типа «отказ в обслуживании» (DoS) или перенаправить трафик по нелегитимному маршруту. Можно выделить следующие последствия фальсификации маршрутной информации:

– перенаправление трафика для создания петель маршрутизации;

– перенаправление трафика для его мониторинга;

– перенаправление трафика для его блокировки.

Протоколы RIP, EGRP, OSPF и BGP поддерживают аутентификацию на основе использования криптографических алгоритмов и без шифрования. Кроме того, аутентификация может быть настроена двумя способами:

– с использованием цепочки ключей;

– на основе аутентификации соседа.

При конфигурации аутентификации с использованием цепочки ключей выполняются следующие действия:

1) имя цепочки ключей задается с помощью команды `key chain имя_цепочки`;

2) создается ключ и указывается его идентификатор, значение и тип шифрования (HMAC-MD5, HMAC-SHA1-12, MD5, SHA-1 и др.) с помощью команд

```
key номер
send-id идентификатор_отправляемого_ключа
recv-id идентификатор_получаемого_ключа
send-lifetime время_действия_отправляемого_ключа
accept-lifetime время_действия_получаемого_ключа
key-string значение_ключа
cryptographic-algorithm тип;
```

3) указывается название ключа в конфигурации протокола BGP с помощью команд

```
router bgp номер_AS
neighbor IP-адрес_соседа remote-as номер_AS_соседа key-
chain имя_цепочки
```

При использовании аутентификации соседа в конфигурации протокола BGP задается пароль с указанием IP-адреса соседа следующим образом:

```
router bgp номер_AS
neighbor IP-адрес_соседа remote-as номер_AS_соседа
neighbor IP-адрес_соседа password тип_шифрования значе-
ние_ключа
```

В представленных выше командах в качестве параметра `тип_шифрования` может использоваться значение `clear` (без шифрования) или `encrypted` (хеширование MD5). У двух соседних устройств должны быть настроены одинаковые типы шифрования и ключи, иначе аутентификация не будет пройдена успешно.

В результате реализации конфигурации аутентификации соседа на двух соединенных устройствах к каждому TCP-сегменту (для протокола BGP), который отправляется соседу, будет добавляться значение MD5-хеша, вычисляемое на основе следующих данных:

– IP-адрес отправителя, IP-адрес получателя, номер протокола, размер сегмента;

– заголовок TCP;

– данные сегмента TCP;

– указанный ключ шифрования.

Для предотвращения атак перенаправления трафика в протоколе маршрутизации OSPF используется проверка подлинности. После настройки аутентификации на маршрутизаторе проверяется источник каждого полученного пакета обновления маршрутизации. Это достигается путем обмена ключом аутентификации, который известен как источнику, так и получателю информации.

Протокол OSPF поддерживает три типа аутентификации:

– Null – это метод, установленный по умолчанию, который означает, что для OSPF аутентификация не используется;

– простая аутентификация по паролю, который отправляется в виде открытого текста в обновлении;

– MD5-аутентификация – пароль шифруется алгоритмом MD5.

На рисунке 6.7 показано, как используется аутентификация MD5 для двух соседних маршрутизаторов OSPF. Сначала маршрутизатор Router1 объединяет

сообщение маршрутизации с предварительно общим секретным ключом и вычисляет подпись, используя алгоритм MD5. Подпись также известна как хеш-значение.

Далее маршрутизатор Router1 добавляет подпись к сообщению маршрутизации и отправляет его к маршрутизатору Router2. Алгоритм MD5 не шифрует сообщение, поэтому его содержание открыто. Маршрутизатор Router2 открывает пакет, предварительно объединяет сообщение маршрутизации с общим секретным ключом и вычисляет подпись с использованием алгоритма MD5. Если подписи совпадают, то маршрутизатор Router2 принимает обновление маршрутизации. Если подписи не совпадают, то маршрутизатор Router2 не использует полученную информацию для обновления.

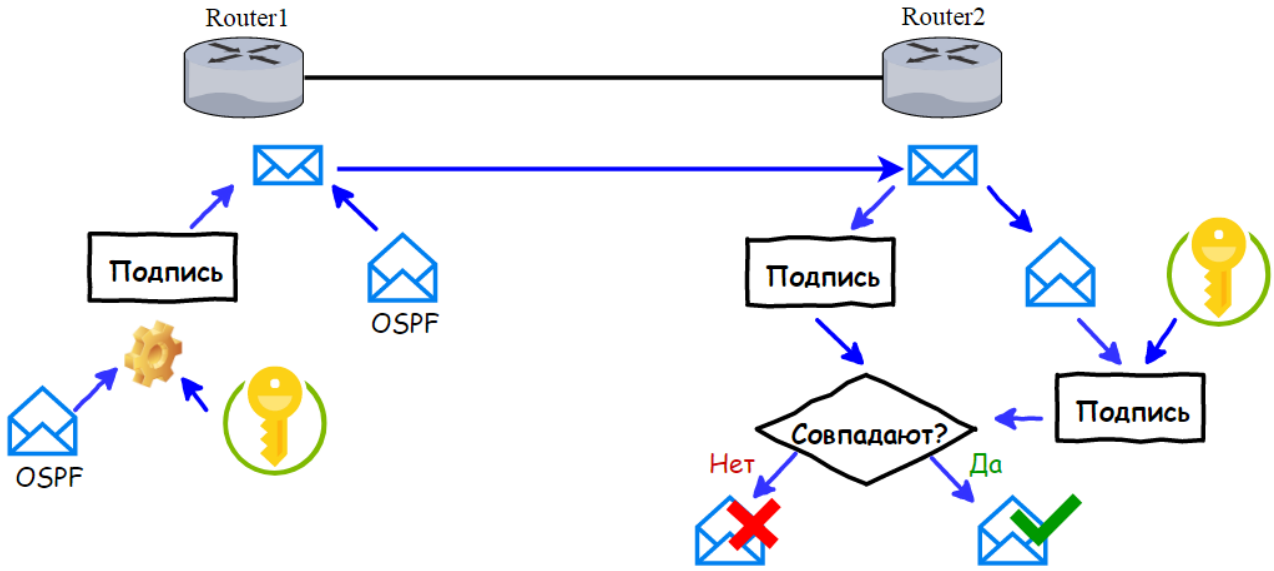

Рисунок 6.7 – Механизм аутентификации MD5

OSPF поддерживает аутентификацию протокола маршрутизации с использованием MD5. Аутентификация MD5 может быть включена как для всех интерфейсов (глобальная аутентификация), так и для каждого интерфейса отдельно (локальная аутентификация). Для включения глобальной аутентификации OSPF MD5 необходимо в режиме конфигурации маршрутизатора использовать команду `area area-id authentication message-digest` для указания области. В режиме конфигурации интерфейса также необходимо настроить аутентификацию командой `ip ospf message-digest-key` *`ключ`* `md5` *`пароль`*.

Для обеспечения большей гибкости теперь можно настроить локальную аутентификацию. В этом случае аутентификации MD5 активируется на каждом интерфейсе командами `ip ospf message-digest-key` *`ключ`* `md5` *`пароль`* и `ip ospf authentication message-digest`.

Глобальная аутентификация и локальная аутентификация OSPF MD5 могут использоваться на одном маршрутизаторе. Однако настройка локальной аутентификации переопределяет глобальную. Пароли аутентификации MD5 не обязательно должны быть одинаковыми во всей области, однако между соседями они должны быть одинаковыми.

Рассмотрим пример конфигурации аутентификации по протоколу OSPF в сети MTS AS25106 (см. рисунок 6.4). Для областей 0 и 20 настроена глобальная аутентификация OSPF MD5. Конфигурация аутентификации на Router5 осуществляется следующим образом:

```
Router5(config)#router ospf 25106
Router5(config-router)# area 20 authentication message-digest
Router5(config-router)# area 0 authentication message-digest
Router5(config-router)#interface GigabitEthernet0/1/0
Router5(config-if)#shutdown
Router5(config-if)#ip ospf message-digest-key 1 md5 25106
Router5(config-if)#no shutdown
Router5(config-if)#interface GigabitEthernet0/0/0
Router5(config-if)#shutdown
Router5(config-if)#ip ospf message-digest-key 1 md5 25106-20
Router5(config-if)#no shutdown
```

Как видно из представленных выше команд, для каждой области задается разный ключ в конфигурации интерфейсов. Важно использовать эти ключи при настройке глобальной аутентификации на соседних устройствах.

Для мониторинга правильности передачи сообщений аутентификации между настроенными устройствами используется команда `debug ip ospf events`. Если на Router5 ввести команду `debug ip ospf events`, можно увидеть процесс передачи сообщений по протоколу OSPF. На рисунке 6.8 представлены оповещения, которые показывают, что в результате отправки настроенного ключа аутентификации на интерфейсе GigabitEthernet 0/1/0 от соседнего устройства был получен ответ о несовпадении ключей. Это значит, что в процессе настройки были указаны разные ключи в команде `ip ospf message-digest-key`. В случае если ключи на устройствах настроены верно, будут отражаться сообщения о передаче пакетов OSPF (рисунок 6.9). Для отключения функции мониторинга процесса передачи сообщений OSPF используется команда `no debug ip ospf events` или `no debug all`.

```
21:39:57: OSPF: Send with youngest Key 1

21:39:57: OSPF: Interface GigabitEthernet0/1/0 going Up

21:39:57: OSPF: Rcv pkt from  134.17.215.1, GigabitEthernet0/1/0
: Mismatch Authentication Key - Message Digest Key 1
```

Рисунок 6.8 – Результат неверной конфигурации глобальной аутентификации OSPF MD5 для области 0

```
00:21:49: OSPF: Send with youngest Key 1

00:21:49: OSPF: Interface GigabitEthernet1/0/1 going Up

00:21:49: OSPF: Rcv hello from 66.66.66.66 area 0 from
GigabitEthernet1/0/1 194.62.64.114

00:21:49: OSPF: End of hello processing

00:21:59: OSPF: Rcv hello from 66.66.66.66 area 0 from
GigabitEthernet1/0/1 194.62.64.114

00:21:59: OSPF: 2 Way Communication to 66.66.66.66 on
GigabitEthernet1/0/1, state 2WAY
```

Рисунок 6.9 – Часть информации о результате обмена сообщениями OSPF между маршрутизатором Router5 и коммутатором L3 MS3

Для проверки настройки аутентификации на интерфейсе маршрутизатора используется команда `show ip ospf interface имя_номер`. В результате выполнения данной команды можно убедиться, что аутентификация включена и используется ключ с номером 1 (рисунок 6.10).

```
Router5# show ip ospf interface gigabitEthernet 0/1/0

GigabitEthernet0/1/0 is up, line protocol is up
  Internet address is 134.17.215.2/30, Area 0
  Process ID 25106, Router ID 20.20.20.25, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 20.20.20.25, Interface address 134.17.215.2
  Backup Designated Router (ID) 3.3.3.3, Interface address 134.17.215.1
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:01
  Index 3/3, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 3.3.3.3  (Backup Designated Router)
  Suppress hello for 0 neighbor(s)
  Message digest authentication enabled
    Youngest key id is 1
```

Рисунок 6.10 – Результат проверки настройки глобальной аутентификации OSPF MD5

Для настройки локальной аутентификации OSPF MD5 на каждом интерфейсе на маршрутизаторе Router7, соединенном с коммутатором L3 MS4 (см. рисунок 6.4), используются следующие команды:

```
Router7(config)#interface GigabitEthernet0/0/0
Router7(config-if)#shutdown
Router7(config-if)#ip ospf authentication message-digest
Router7(config-if)#ip ospf message-digest-key 1 md5 60330
Router7(config-if)#no shutdown
```

Проверить правильность настройки также можно, используя команду `show ip ospf interface` *имя_номер*.

Между маршрутизаторами Router12, Router13 и коммутатором MS6 (см. рисунок 6.4) настроен протокол RIP. Для аутентификации маршрутизаторов, работающих по протоколу RIP, также используется конфигурация цепочки ключей, аналогичная протоколу BGP. Ключи протокола RIP могут быть зашифрованы с помощью алгоритма MD5. Отличие настройки цепочки ключей для протокола RIP заключается в том, что она активируется на интерфейсах соседних маршрутизаторов следующим образом:

```
interface имя_номер
ip rip authentication mode md5
ip rip authentication key-chain имя_цепочки
```

Между маршрутизаторами Router9, Router10 и коммутатором MS5 (см. рисунок 6.4) работает протокол EIGRP. Аутентификация соседних устройств в протоколе EIGRP также осуществляется посредством конфигурации цепочки ключей. Существует возможность их хеширования с помощью алгоритма MD5. Конфигурация цепочки ключей в EIGRP осуществляется аналогично конфигурации в BGP, за исключением того, что активация ключей осуществляется на интерфейсах соседних устройств следующим образом:

```
ip authentication mode eigrp номер_AS md5
ip authentication key-chain eigrp номер_AS имя_цепочки
```

Рассмотрим пример конфигурации аутентификации в EIGRP для маршрутизатора Router9 (см. рисунок 6.4):

```
Router9(config)#key chain keyEIGRP
Router9(config-keychain)# key 1
```

```
Router9(config-keychain-key)# key-string EIGRP9002
Router9(config-keychain-key)#interface Gig0/1/0
Router9(config-if)#shutdown
Router9(config-if)#ip authentication mode eigrp 9002 md5
Router9(config-if)#ip authentication key-chain eigrp 9002
keyEIGRP
Router9(config-if)#no shutdown
```

С помощью команды `debug eigrp packets` можно проследить процесс аутентификации. На рисунке 6.11 показан процесс неуспешной аутентификации, на рисунке 6.12 – успешной. Для отключения функции мониторинга процесса передачи сообщений аутентификации EIGRP используется команда `no debug eigrp packets` или `no debug all`.

```
EIGRP: Sending HELLO on GigabitEthernet1/1/4
  AS 51365, Flags 0x0, Seq 95/0 idbQ 0/0 iidbQ un/rely 0/0

EIGRP: Received packet with MD5 authentication, key id = -1

EIGRP: Received HELLO on GigabitEthernet1/1/4 nbr 194.62.64.106
  AS 51365, Flags 0x0, Seq 111/0 idbQ 0/0
 EIGRP: GigabitEthernet1/1/4 : ignored packet from 194.62.64.106, opcode = HELLO
(missing authentication)
```

Рисунок 6.11 – Результат неуспешной аутентификации по протоколу EIGRP

```
EIGRP: Received packet with MD5 authentication, key id = 1

EIGRP: Received HELLO on GigabitEthernet0/1/0 nbr 45.143.92.1
  AS 9002, Flags 0x0, Seq 113/0 idbQ 0/0

%DUAL-5-NBRCHANGE: IP-EIGRP 9002: Neighbor 45.143.92.1 (GigabitEthernet0/1/0)
is up: new adjacency
```

Рисунок 6.12 – Результат успешной аутентификации по протоколу EIGRP

6.2 Лабораторное задание

Лабораторная работа выполняется на основе настроек, выполненных в лабораторной работе № 5 (файл **LAB5-1.pkt**). До начала выполнения необходимо открыть сохраненный файл **LAB5-1.pkt** и проверить настройки IP-адресации (см. таблицы 1.2, 3.3, 5.2, 5.3): маршрутизация должна быть настроена по протоколу BGP, номера автономных систем должны соответствовать номерам из таблицы 5.4. В автономных системах должна быть настроена маршрутизация по протоколам OSPF, RIP, EIGRP. В лабораторной работе необходимо расширить смоделированную в лабораторной работе № 5 сеть в соответствии со следующими заданиями.

1 Добавить в подсеть NET4 локальный DNS-сервер (Local DNS-server) (см. рисунок 6.4). IP-адрес сервера следует выдавать по DHCP всем оконечным устройствам в сетях NET1, NET2, NET3, NET4. Настроить на локальном DNS-сервере рекурсию к корневому серверу (ROOT DNS-server), который следует добавить в сеть NET3.

2 На корневом сервере создать SOA-записи для поддоменов camera и iot и рекурсию к TLD DNS-серверу. TLD DNS-сервер добавить в сеть NET2, на нем настроить рекурсию к авторитетному серверу authority.iot.by, реализовать его на сервере camera.by в подсети NET1. Создать учетные записи электронной почты, которые указывались в SOA-записях.

3 В службе DNS сервера authority.iot.by заменить доменное имя iot.by на iot.iot.by, camera.by на camera.iot.by. Для других доменных имен (ROOT и др.) создать A Record записи.

4 С любых оконечных устройств в сетях NET1, NET2, NET3, NET4 реализовать команду `nslookup` для доменных имен ROOT, iot.by, camera.by и представить результаты в отчете.

В отчете также представить результаты конфигурации Local DNS-сервера, ROOT DNS-сервера, TLD DNS-сервера и других DNS на серверах. Сохранить файл под именем **LAB6-2.pkt**.

5 Настроить глобальную аутентификацию во всей сети NET1, в том числе между пограничным маршрутизатором сети NET1 и подключенным к ней коммутатором L3. В качестве ключа использовать номер автономной системы сети NET1. Отобразить в отчете результаты успешной аутентификации OSPF на пограничном маршрутизаторе сети NET1. Сохранить файл под именем **LAB6-3.pkt**.

6 Настроить локальную аутентификацию на маршрутизаторах сети NET2 и на подключенном к данной сети коммутаторе L3. В качестве ключа использовать номер автономной системы. Отобразить в отчете результаты успешной аутентификации OSPF на пограничном маршрутизаторе сети NET2. Сохранить файл под именем **LAB6-4.pkt**.

7 Настроить аутентификацию EIGRP для маршрутизаторов в сети NET3 и подключенном к ним коммутаторе L3. В качестве названия цепочки ключей использовать фамилию выполняющего задание студента. Значение ключа должно быть равно номеру автономной системы для EIGRP. Отобразить в отчете результаты успешной аутентификации EIGRP. Сохранить файл под именем **LAB6-5.pkt**.

8 *Проверка правильности настроек.* В смоделированной сети любое устройство должно получать доступ ко всем серверам, на серверах iot.by и camera.by должны отображаться все зарегистрированные на них устройства. Должны правильно функционировать серверы электронной почты. В отчете

представить изображение смоделированной сети с подписями IP-адресов и автономных систем всех подключаемых сетей.

6.3 Содержание отчета

1 Цель работы.

2 Результаты произведенных настроек из пунктов 1–8, изображение смоделированной сети.

3 Вывод по работе.

4 Ответы на контрольные вопросы.

6.4 Контрольные вопросы

1 Доменное имя и домен. Распределение доменных имен.

2 Компоненты системы доменных имен. Этапы регистрации доменного имени.

3 Процесс обмена сообщения между серверами разных уровней.

4 DNSSEC. Команда `nslookup`.

5 Функции DNS-резолвера. Типы записей.

6 Способы конфигурации различных DNS-серверов.

7 Назначение аутентификации на маршрутизаторах глобальной сети.

8 Типы аутентификации протокола OSPF. Процесс аутентификации по протоколу OSPF.

9 Способы настройки аутентификации по протоколу OSPF и RIP.

10 Настройка аутентификации в протоколах EIGRP и BGP.

ЛАБОРАТОРНАЯ РАБОТА № 7
МЕЖСЕТЕВОЕ ЭКРАНИРОВАНИЕ. СПИСКИ КОНТРОЛЯ ДОСТУПА

Цель: изучить типы и принципы организации списков контроля доступа, овладеть практическими навыками конфигурации стандартных и расширенных списков контроля доступа.

7.1 Теоретическая часть

Межсетевое экранирование – это комплекс аппаратных, программных средств и их комбинаций для управления потоком сетевого трафика, предотвращения угроз и несанкционированного доступа, анализа уязвимостей в соответствии с требованиями безопасности [18].

Межсетевые экраны – это оборудование, программное обеспечение или их комбинация для управления, инспекции и фильтрации потока сетевого трафика между внешними и внутренними локальными сетями (доверенными и ненадежными) с помощью предварительно настроенных правил или фильтров на основе требований безопасности.

Межсетевое экранирование основано на инспектировании трафика в различных системах фильтрации, в которых настроены правила блокировки и пропуска пакетов.

Системы фильтрации классифицируют в зависимости от способа анализа содержимого пакета при его прохождении через сетевое оборудование.

1 Канальная фильтрация – анализ заголовков канального уровня модели OSI, а именно полей заголовков, содержащих информацию о MAC-адресах и идентификаторах VLAN. Такие системы используются в коммутаторах L2.

2 Сетевая фильтрация, или пакетные фильтры (Packet Filtering Firewall, L3 Firewall) – анализ заголовков сетевого и транспортного уровней модели OSI, а именно полей заголовков, содержащих информацию об IP-адресах и портах в TCP- и UDP-заголовках. Такие системы используются в стандартных или в расширенных списках контроля доступа, настраиваемых на межсетевых экранах и маршрутизаторах.

3 Сеансовая фильтрация (Circuit-level Firewall) является развитием сетевой фильтрации с возможностью создания виртуального соединения от внешнего IP-адреса для исключения прямого соединения из внутренней сети. Сеансовая фильтрация реализуется за счет использования технологий NAT.

4 Фильтрация с контролем состояния (Stateful Inspection Firewall) основана на подробном анализе заголовков транспортного уровня и отслеживании типов пакетов TCP, их порядковых номеров и других параметров, которые реги-

стрируются в таблице исходящих TCP-соединений, соответствующих каждой сессии.

5 Прикладная фильтрация (Application-level Gateway, L7 Firewall), анализирует содержимое всех заголовков всех уровней модели OSI и передаваемые данные, сочетает в себе функции всех вышеперечисленных способов фильтрации и обеспечивает дополнительные возможности, такие как аутентификация и авторизация пользователей, разграничение доступа к ресурсам, антивирусная проверка передаваемых данных, фильтрация по URL (веб-фильтрация), фильтрация используемых приложений, отслеживание и предотвращение DDoS-атак и др.

Прикладная фильтрация используется в следующих типах межсетевых экранов [19]:

– прокси-фаервол (Proxy Firewall) – программное устройство на сервере в любом месте локальной сети для аутентификации и авторизации пользователей для доступа во внешнюю сеть или другие сегменты сети, осуществляет сеансовую фильтрацию и/или фильтрацию с контролем состояния;

– UTM (Unified Threat Management) – программное или программно-аппаратное устройство, внутри которого установлено несколько различных систем фильтрации (антивирус, системы обнаружения и предотвращения вторжений (IDS/IPS), веб-фильтрация и прочее), которые последовательно анализируют проходящий через устройство трафик и принимают решение в соответствии с заданными правилами о пропуске, блокировке или дополнительной проверке;

– межсетевые экраны нового поколения (Next-generation Firewall, NGFW) – программное или программно-аппаратное устройство, являющееся развитием UTM с дополнительными функциями и возможностями, такими как поддержка технологий облачной песочницы, контроль производительности и пропускной способности сети

Для сетевой и сеансовой фильтрации используются списки контроля доступа.

Списки контроля доступа (Access Control List, ACL) – это набор правил, которые устанавливают критерии проверки определенных заголовков и советующие действия над пакетом при совпадении указанных в правилах критериев с содержимым заголовков. При настройке ACL разрешаются или запрещаются IP-пакеты (при этом возможен анализ IP-пакета по типу пакета). Также ACL можно настроить для различных сетевых протоколов. В основном применение списков доступа рассматривают для реализации сетевой фильтрации. Списки доступа позволяют создавать правила управления трафиком, по которым будет происходить межсетевое взаимодействие как в локальных, так и в глобальных сетях.

Применительно к сетевой фильтрации на маршрутизаторах разные ACL создаются независимо и применяются к определенным интерфейсам, после че-

го маршрутизатор анализирует входящий и исходящий трафик только на указанном интерфейсе. Тот трафик, который приходит на интерфейс маршрутизатора, называется входящим, тот, который выходит, – исходящим. Соответственно ACL могут размещаться на входящем или на исходящем направлении интерфейса.

Рассмотрим принцип работы ACL на примере сети, представленной на рисунке 7.1.

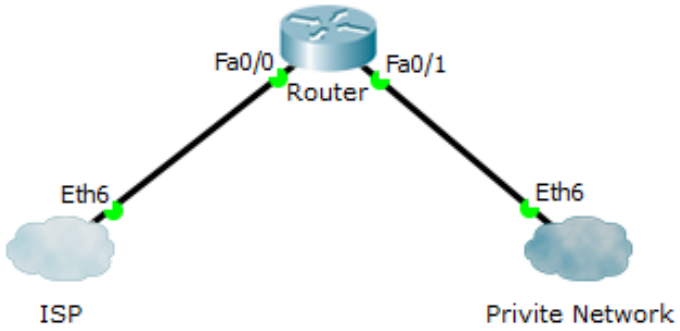

Рисунок 7.1 – Пример соединения локальной сети
с сетью провайдера интернет-услуг ISP

Когда из частной сети на интерфейс маршрутизатора Fa0/1 приходит пакет, маршрутизатор проверяет, есть ли ACL на исходящем направлении интерфейса Fa0/1 или нет. Если он есть, то дальше анализ пакета ведется по правилам списка контроля доступа строго в том порядке, в котором записаны правила. Если маршрутизатор обнаруживает совпадение указанных в правиле параметров (IP-адреса, номера портов) с содержимым заголовков анализируемого пакета, то проверяется соответствующее данному правилу действие (запретить или разрешить прохождение данного пакета). Если списка контроля доступа нет – пакет проходит без всяких ограничений на интерфейс Fa0/0. Перед тем как отправить пакет маршрутизатор проверяет наличие ACL на исходящем направлении интерфейса Fa0/0. Например, на интерфейсе Fa0/0 есть ACL с правилом запрета устройствам из локальной сети доступа в глобальную сеть. Как правило, такие ACL являются некорректными, хотя работают технически верно: для реализации правил такого ACL маршрутизатором были потрачены вычислительные ресурсы на две проверки данного пакета на интерфейсе Fa0/1 и Fa0/0. Поэтому корректным считается конфигурация ACL с учетом экономии ресурсов сетевых устройств. Если ACL с правилом блокировки доступа к глобальной сети внутренним устройствам настроен на входящем направлении интерфейса Fa0/1, то пакет будет сразу заблокирован, таким образом, не потребуется его дополнительная обработка (проверка таблицы маршрутизации, передача данных на интерфейс Fa0/0 и проверка ACL на данном интерфейсе). Существует нестрогое правило, в соответствии с которым расширенные ACL нужно размещать как можно ближе к источнику, стандартные – как можно ближе к получателю.

Существует два основных типа списков доступа: стандартные (standart) и расширенные (extended). В конфигурации оборудования Cisco списки контроля доступа могут задаваться по именам или номерам, при этом номера с 1 по 99 используются для стандартных ACL, номера с 100 по 199, с 2000 по 2699 – для расширенных ACL. Различия между стандартными и расширенными ACL заключаются в возможности фильтровать пакеты не только по IP-адресу, но и по другим различным параметрам.

Стандартные списки обрабатывают только входящие IP-адреса источников и ищут соответствия в правилах, в которых указаны IP-адреса отправителя. Расширенные списки работают с IP-адресами источников и отправителей одновременно и дополнительно проверяют протоколы транспортного и других уровней модели OSI по номерам портов или протоколу.

Работа списка доступа напрямую зависит от порядка следования правил в этом списке, где в каждой строке записано правило обработки трафика [8]. Все правила списка просматриваются по порядку с первого до последнего, но как только было найдено первое соответствие, просмотр завершается, т. е. если для пришедшего пакета было найдено правило, под которое он подпадает, остальные правила проверяться не будут. Если пакет не подпал ни под одно из правил, то включается правило, указанное по умолчанию в самом конце ACL.

Для создания списков контроля доступа используются следующие правила:

– обработка правил списков контроля доступа ведется строго в том порядке, в котором они записаны;

– при условии совпадения содержимого заголовков пакета с критериями в правиле выполняется указанное в данном правиле действие, следующие далее правила не используются для проверки;

– в конце каждого списка контроля доступа находится скрытое правило полного запрета (deny any), установленное по умолчанию;

– расширенные ACL нужно размещать как можно ближе к источнику, стандартные – ближе к получателю;

– нельзя размещать более одного списка контроля доступа на одном интерфейсе, протоколе, направлении;

– правила списков доступа не действуют на трафик, сгенерированный самим маршрутизатором;

– для указания IP-адресов в правилах также используется обратная маска.

Для того чтобы создать стандартный список доступа, необходимо выполнить следующие этапы:

– создать список контроля доступа;

– составить правила обработки трафика;

– применить список доступа к интерфейсу устройства на вход или выход.

Рассмотрим пример создания списка контроля доступа на маршрутизаторе Router1 для подсети с VLAN на рисунке 7.2. Перед конфигурацией списков контроля доступа составляют примерный план (таблица 7.1), учитывая политику безопасности организации.

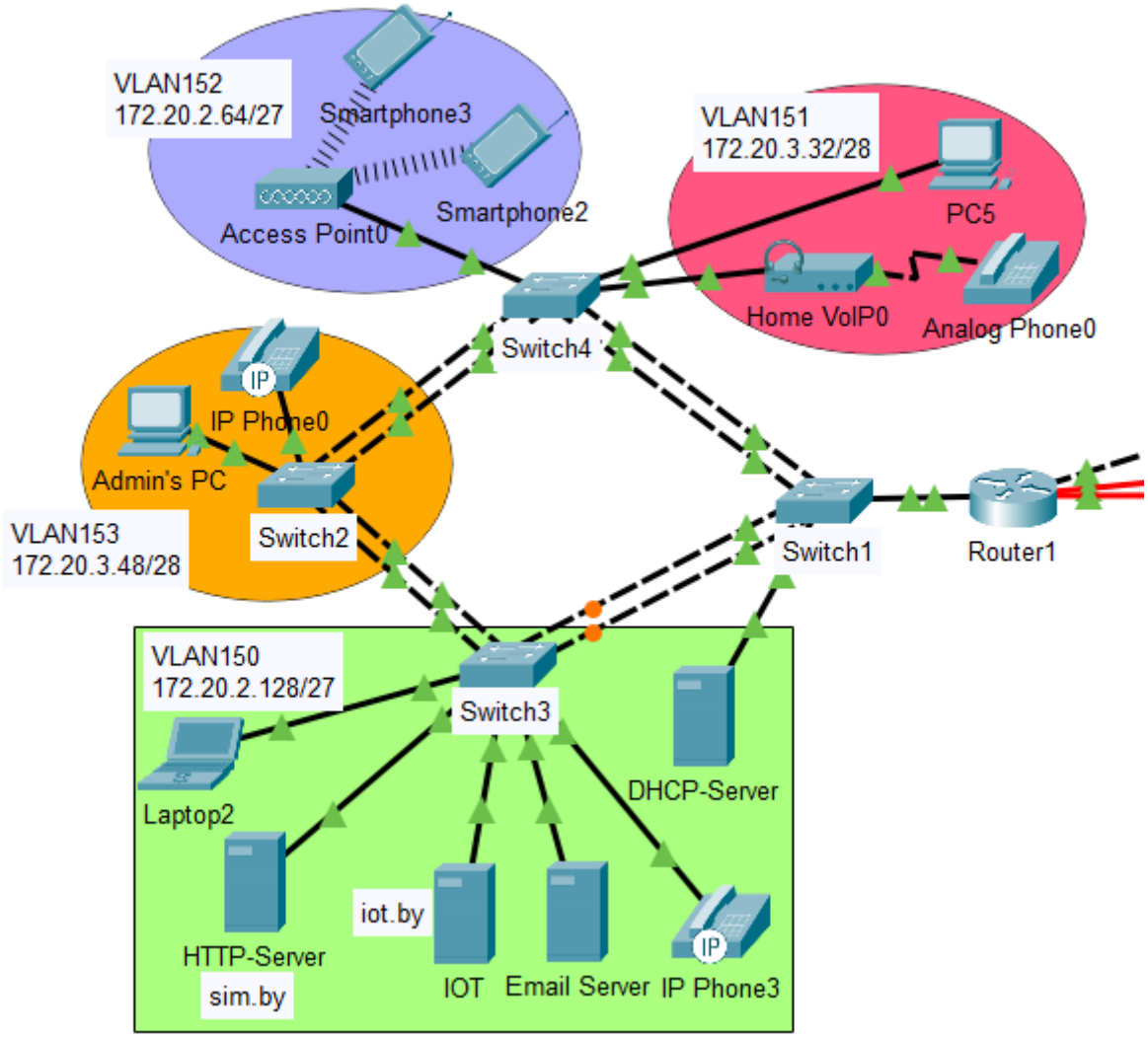

Рисунок 7.2 – Пример конфигурации стандартных ACL

Таблица 7.1 – Примерный план конфигурации стандартных списков контроля доступа

Название/ номер списка доступа	Разрешить/ запретить доступ	Адресация		Интерфейс маршрутизатора	
		IP-адрес устройства/ сети	Обратная маска	Название	Направление
SSH	permit	172.20.3.50	–	VTY	in
	deny	any	–		
1	deny	172.20.2.64/27	0.0.0.15	FastEthernet 0/1.150–151, 0/1.153–154	out
	permit	any	–		
ForIOT	permit	172.20.3.50 172.20.3.34	–	FastEthernet 1/1.204	out
	deny	any	–		

Например, в соответствии с политикой безопасности требуется организовать доступ по SSH ко всем сетевых устройствам только для компьютера администратора. Для этого будет создан список контроля доступа SSH (см. таблицу 7.1). Также потребуется запретить доступ из подсети VLAN 152 в VLAN 150–151, VLAN 153–154, VLAN 200 и к серверу iot.by (ACL 1). Доступ к серверу iot.by разрешить только компьютеру администратора и компьютеру PC5 (ACL ForIOT).

Составление плана конфигурации стандартных списков контроля доступа (см. таблицу 7.1) позволяет исключить ошибки в настройке. После составления плана можно перейти к конфигурации списков контроля доступа. На первом этапе создается стандартный список контроля доступа с использованием имени или номера. Так, например, для создания списка контроля доступа SSH используется команда `ip access-list standard SSH`.

Для создания списка контроля доступа под номером 152 используется команда `ip access-list standard 1`.

При вводе правил в списке контроля доступа на втором этапе могут использоваться следующие параметры:

– действия: запретить (deny), разрешить (permit);

– адрес сети с обратной маской (например, 192.168.2.0, 0.0.0.255), IP-адрес устройства (192.168.2.1) или указатель любого адреса (any).

Правила для стандартного списка доступа под именем ForIOT разрешают доступ к серверу iot.by только устройствам с IP-адресами 172.20.3.50 и 172.20.3.34. Данное правило создается следующим образом:

```
Router1(config)#ip access-list standard ForIOT
Router1(config-std-nacl)#permit 172.20.3.50
Router1(config-std-nacl)#permit 172.20.3.34
Router1(config-std-nacl)#deny any
```

Последнее правило для представленного выше стандартного списка контроля доступа под именем ForIOT должно разрешать остальной трафик.

На третьем этапе на каждом интерфейсе должен быть активирован список контроля доступа или для входящих пакетов, или для исходящих пакетов. Каждый список работает только с тем интерфейсом, к которому он был применен, и не действует на остальные интерфейсы устройства, если он не указан в их настройках. Один список контроля доступа может быть применен к разным интерфейсам. Активация списка доступа на интерфейсе осуществляется следующими командами:

```
Router1(config-std-nacl)#interface FastEthernet1/1.204
Router1(config-subif)# ip access-group ForIOT out
```

В данном случае к sub-интерфейсу FastEthernet1/1.204, к которому подключен сервер iot.by, применили список контроля доступа на исходящем направлении интерфейса (out).

В списке контроля доступа, созданном под номером 1, прописываются следующие правила:

```
Router1(config)#access-list 1 deny 172.20.2.64 0.0.0.15
Router1(config)#access-list 1 permit any
Router1(config)#interface FastEthernet0/1.154
Router1(config-subif)# ip access-group 1 out
```

Для просмотра созданных списков доступа используется команда `show access-lists`. Для удаления списка доступа применяется команда `no ip access-list` *`тип_списка номер_списка(имя)`*. Для удаления списка доступа на интерфейсе используется команда `no ip access-group` *`номер_списка(имя) направление`*.

Для безопасности удаленного администрирования сетевого оборудования целесообразно создавать списки контроля доступа к линиям VTY.

Рассмотрим пример создания стандартного списка контроля доступа под название SSH (см. таблицу 7.1). Сначала необходимо создать стандартный ACL с именем SSH с помощью команды `ip access-list standard SSH`.

Далее создается правило разрешения доступа устройству с IP-адресом 172.20.0.42: `permit 172.20.3.50`.

Следующая команда устанавливает запрет на все остальные виды трафика: `deny any`.

В режим настройки интерфейса Telnet созданный ACL добавляется на входящее направление:

```
Router1(config)#line vty 0 15
Router1(config-line)#access-class SSH in
```

Создание расширенных списков контроля доступа отличается тем, что в правилах после указания действия (permit или deny) должен находиться параметр протокола (IP, TCP, UDP, ICMP и др.), который указывает, должна ли выполняться проверка всех пакетов IP или только пакетов с определенными заголовками (ICMP, TCP или UDP). Также можно задать проверку определенных номеров портов протоколов TCP или UDP.

Создание расширенного списка контроля доступа также возможно с указанием имени или номера. Например, создание ACL с номером 100 производится с помощью команды `ip access-list extended 100`.

Для указания номеров портов в правиле доступа указываются обозначения, представленные в таблице 7.2. Распространенные протоколы и соответствующие им стандартные номера портов приведены в таблице 7.3 (может указываться номер порта или ключевое имя).

Таблица 7.2 – Список обозначений правил для фильтрации трафика по портам

Обозначение	Действие
lt n	Все номера портов, меньшие чем n
gt n	Все номера портов, большие чем n
eq n	Порт n
neq n	Все порты за исключением n
range n m	Все порты от n до m включительно

Таблица 7.3 – Номера портов для протоколов и их обозначение в командах

Номер порта	Протокол	Приложение	Ключевое слово в команде access_list
20	TCP	FTP	data ftp_data
21	TCP	Управление сервером FTP	ftp
22	TCP	SSH	ssh
23	TCP	Telnet	telnet
25	TCP	SMTP	smtp
53	UDP, TCP	DNS	domain
67, 68	UDP	DHCP	nameserver
69	UDP	TFTP	tftp
80	TCP	HTTP	www
110	TCP	POP3	pop3
161	UDP	SNMP	snmp

Рассмотрим пример конфигурации списка контроля доступа на Router5 для запрета всем устройствам доступа по протоколу HTTP к серверу camera.by с IP-адресом 172.20.3.98 (см. рисунок 6.4). Доступ будет разрешен только по протоколу HTTPS компьютеру администратора с IP-адресом 122.20.0.54:

```
Router5(config)#ip access-list extended ForCameraBY
Router5(config-ext-nacl)#permit tcp host 122.20.0.54 host
172.20.3.98 eq 443
Router5(config-ext-nacl)#deny ip any any
```

Необходимо отметить, что на сервер camera.by данные о статусе IoT-устройств передаются по протоколу TCP с номером порта 31000, и для них также должно быть создано разрешающее правило контроля доступа. Также должны учитываться другие протоколы, которые нужны для правильной работы сети: OSPF, Radius, TACACS+, SSH, DNS и др.

При добавлении новых правил в список контроля доступа ForCameraBY необходимо помнить, что они сохраняются последовательно, т. е. в случае если необходимо добавить правило `permit tcp 122.20.0.24 0.0.0.7 host 172.20.3.98 eq 31000`, разрешающее доступ устройств систем контроля доступа, пожаротушения и видеонаблюдения к серверу camera.by, оно сохранится после правила `deny tcp any any`, установленного в списке контроля доступа ForCameraBY ранее. В таком случае данное правило никогда не будет выполнено, т. к. при проверке параметров пакета на соответствие правилам ACL проверка осуществляется последовательно (сверху вниз).

Таким образом, для правильной работы ACL нужно использовать номер правила в списке контроля доступа:

```
Router5(config-ext-nacl)#11   permit   tcp   122.20.0.24
0.0.0.7 host 172.20.3.98 eq 31000
```

Выделяют динамические (Dynamic ACL) и рефлексивные (Reflexive ACL) списки доступа [19]. Динамический ACL позволяет ограничивать доступ к серверам из внешней сети. Например, когда на маршрутизаторе, который подключен к какому-то серверу, необходимо закрыть доступ из внешней сети, но в то же время есть несколько пользователей, которым дожен быть разрешен доступ к серверу. Для этого настраивается динамический список контроля доступа на входящем направлении, а дальше пользователям, которым разрешен доступ, необходимо подключиться к данному устройству через Telnet, в результате чего динамический ACL открывает доступ к серверу, и пользователь может осуществлять доступ по протоколу HTTP или HTTPS. По умолчанию через 10 минут это соединение закрывается, и пользователь будет вынужден еще раз выполнить авторизацию по протоколу Telnet, чтобы подключиться к серверу.

Рефлексивные ACL работают следующим образом: доступ блокируется полностью (deny any), при этом формируется еще один специальный ACL, который анализирует параметры пользовательских соединений, сгенерированных из локальной сети, и для них игнорирует правило блокировки трафика. В результате пользователи из сети Интернет не смогут установить соединение, но на запросы пользователей, соединения которых сгенерированы в локальной сети, будут приходить ответы. Рефлексивные списки доступа обеспечивают повышенную защиту. Например, когда пользователь в локальной сети отправляет TCP-запрос во внешнюю сеть, для того чтобы пришел TCP-ответ от внешнего сервера, должно устанавливаться соединение. Если соединение не установлено, пакеты из внешней сети будут блокироваться. Но при этом такой открытой сессией и ее параметрами может воспользоваться нарушитель для проникновения в частную сеть.

7.2 Лабораторное задание

Лабораторная работа выполняется на основе настроек, выполненных в лабораторной работе № 6 (файл **LAB6-5.pkt**). До начала выполнения необходимо открыть сохраненный файл **LAB6-5.pkt** и проверить настройки IP-адресации (см. таблицы 1.2, 3.3, 5.2, 5.3): маршрутизация должна быть настроена по протоколу BGP, номера автономных систем должны соответствовать данным из таблицы 5.4. В автономных системах должны быть настроены маршрутизация и аутентификация по протоколам OSPF, RIP, EIGRP. Топология сети должна соответствовать рисунку 6.4. В данной лабораторной работе необ-

ходимо настроить стандартные и расширенные списки контроля доступа в соответствии со следующими заданиями.

1 Осуществить конфигурацию стандартных списков контроля доступа на маршрутизаторе (Router 1 на рисунке 6.4), подключенном к VLAN с оконечными устройствами (см. таблицу 1.2), в соответствии со следующими ниже условиями.

1.1 Организовать доступ по SSH только для одного устройства (Admin) из первого указанного в таблице 1.2 VLAN ко всем коммутаторам подсетей VLAN и маршрутизаторам сети NET1. Версия протокола SSH – 2. Аутентификацию подключений по SSH к маршрутизаторам на сервере camera.by проводить по протоколам Radius или TACACS+, для коммутаторов использовать локальную аутентификацию. Остальным устройствам запретить доступ по SSH к маршрутизаторам и коммутаторам. Заполнить таблицу 7.4, определив необходимые IP-адреса и интерфейсы.

Таблица 7.4 – Настройка стандартных списков контроля доступа

Название/ номер списка доступа	Разрешить/ запретить доступ	Адресация		Интерфейс маршрутизатора	
		IP-адрес устройства/ сети	Обратная маска	Название	Направление

1.2 В подсети с VLAN добавить беспроводную точку доступа (при ее отсутствии) и создать отдельный VLAN для устройств, подключаемых к ней (подсеть VLAN 152 на рисунке 7.2). Запретить доступ всем устройствам, подключаемым к точке доступа, доступ к другим VLAN и серверу iot.by. Разрешить доступ к внешней сети и всем остальным серверам. Заполнить таблицу 7.4, определив необходимые IP-адреса и интерфейсы.

1.3 Разрешить доступ к серверу iot.by только двум оконечным устройствам из разных VLAN (например, на рисунке 7.2 Admin’s PC и PC5). Всем остальным устройствам доступ запретить. Заполнить таблицу 7.4, определив необходимые IP-адреса и интерфейсы.

1.4 При составлении списков контроля доступа учитывать необходимость правильности работы по протоколам DNS, Radius, TACACS. Устройства систем контроля дыма, освещения, температуры должны передавать свои данные на сервер iot.by. При необходимости подкорректировать составленную таблицу 7.4

и реализованные настройки списков контроля доступа на маршрутизаторе (Router 1 на рисунке 7.2), подключенном к VLAN, с оконечными устройствами из таблицы 1.2.

1.5 Проверить правильность настройки списков контроля доступа с помощью команд `ping` и `ssh` с разных устройств сети. Представить результат учета подключения по SSH на Radius или TACACS+ сервере. При условии правильной настройки представить информацию команды `show access-lists` в отчете. Сохранить файл под именем **LAB7-1.pkt**.

2 Осуществить конфигурацию расширенных списков контроля доступа на пограничном маршрутизаторе сети NET1 (Router 5 на рисунке 6.4) в соответствии со следующими ниже условиями.

2.1 Разрешить доступ по DNS к серверу camera.by только TLD DNS-серверу, остальным устройствам из внешней сети запретить доступ по DNS в сеть NET1. Заполнить таблицу 7.5, определив необходимые IP-адреса и интерфейсы.

2.2 Запретить доступ всем устройствам из внешней сети к серверу camera.by (см. рисунок 6.4). Разрешить доступ по HTTPS к серверу camera.by компьютеру администратора (Admin), выбранному в пункте 1.1 данной лабораторной работы, остальным оконечным устройствам из других подсетей и сетей доступ запретить. Разрешить доступ по HTTPS к серверу с доменным именем «фамилия студента» всем устройствам из внешних сетей. Заполнить таблицу 7.5, определив необходимые IP-адреса и интерфейсы.

2.3 Разрешить доступ к службе FTP сервера camera.by всем устройствам из сети NET2 и компьютеру администратора, остальным устройствам из других подсетей и из внешней сети запретить доступ. Заполнить таблицу 7.5, определив необходимые IP-адреса и интерфейсы.

Таблица 7.5 – Настройка стандартных списков контроля доступа

Название списка доступа	Разрешить/ запретить доступ	Протокол / номер порта	Адресация		Название и направление интерфейса
			IP-адрес / обратная маска отправителя	IP-адрес получателя	

2.4 Запретить доступ за пределы сети NET1 всем устройствам из подсетей VLAN и Building1 по всем протоколам, кроме HTTPS. Разрешить доступ

устройствам из подсетей VLAN и Building1 за пределы сети NET1 только по протоколу HTTPS.

2.5 Запретить прохождение всех остальных типов пакетов в сеть NET1 (ICMP, TFTP, SSH, TELNET, DHCP) из внешних сетей. При необходимости добавить в списки контроля доступа разрешающие правила для осуществления соединений, необходимых в представленных выше заданиях.

2.6 При составлении списков контроля доступа учитывать необходимость правильной работы по протоколам OSPF, DNS, Radius, TACACS, SSH. Устройства систем контроля доступа, пожаротушения и видеонаблюдения должны передавать свои данные на сервер camera.by. При необходимости скорректировать составленную таблицу 7.5 и реализованные настройки списков контроля доступа на пограничном маршрутизаторе сети NET1.

2.7 Проверить правильность настройки списков контроля доступа с помощью подключений к разным сервисам из списка контроля доступа с разных компьютеров. При условии правильной настройки скопировать информацию результата выполнения команд `show access-lists` и `show running-config` на пограничном маршрутизаторе в сети NET1. Сохранить файл под именем **LAB7-2.pkt**.

7.3 Содержание отчета

1 Цель работы.

2 Результаты произведенных настроек (заполненные таблицы 7.4 и 7.5, результаты произведенных настроек из пунктов 1–2), изображение смоделированной сети.

3 Вывод по работе.

4 Ответы на контрольные вопросы.

7.4 Контрольные вопросы

1 Назначение и принцип работы ACL.

2 Типы ACL и их отличия.

3 Отличительные особенности настройки стандартных и расширенных списков контроля доступа. Примеры конфигурации стандартных и расширенных ACL.

4 Номера портов для разных видов протоколов.

5 Динамические и рефлексивные списки доступа.

6 Межсетевое экранирование.

7 Типы систем фильтрации.

ЛАБОРАТОРНАЯ РАБОТА № 8
ДЕМИЛИТАРИЗОВАННЫЕ ЗОНЫ

Цель: изучить принципы организации демилитаризованных зон, овладеть навыками конфигурации межсетевых экранов и ограничением доступа к внутренним сетям.

8.1 Теоретическая часть

Корпоративные сети можно разделить на следующие зоны: внешняя сеть (подключение к WAN), демилитаризованная зона (ДМЗ, DMZ), внутренняя сеть. В свою очередь каждая из этих зон может включать в себя несколько сегментов. В зависимости от масштабов предприятия и вида его деятельности определяется оптимальный подход к сегментированию сети.

Демилитаризованная зона (ДМЗ, DMZ) – это подсеть корпоративной сети, содержащая ресурсы, к которым могут получать доступ пользователи из внешней сети.

Внутренняя сеть – совокупность локальных сетей с едиными правилами распределения IP-адресов. Пользователями данной сети являются сотрудники организации. Во внутренней сети осуществляется подключение рабочих станций сотрудников, внутренних серверов и устройств. Во внутренней сети применяются соответствующие меры контроля, политики безопасности.

Возможны следующие варианты организации корпоративных сетей [20]:

– плоская сеть;

– сеть с одним пограничным устройством и демилитаризованной зоной;

– сеть с двумя пограничными устройствами и демилитаризованной зоной;

– разделение сети на Front-End и Back-End.

При реализации варианта «плоская сеть» (рисунок 8.1) все устройства организации находятся в одной общей сети (внутренняя сеть). Внутренняя сеть подключена к внешней сети посредством пограничного маршрутизатора или межсетевого экрана.

Такой вариант организации сети является по сравнению с другими наиболее простым в реализации и наименее затратным по стоимости оборудования и труда специалистов, однако он обеспечивает минимальный уровень безопасности. При получении нарушителем несанкционированного доступа к пограничному маршрутизатору или межсетевому экрану происходит нарушение безопасности всей внутренней сети.

В DMZ осуществляется подключение серверов, обеспечивающих работу таких сервисов, как DNS, HTTP, FTP, e-mail и др. За счет использования DMZ такие серверы изолированы и имеют ограниченный доступ во внутреннюю сеть, при этом обеспечивают свободный доступ пользователям из внешней сети. Таким образом, наличие DMZ-зоны затрудняет нарушителю прямой доступ к внутренней сети организации.

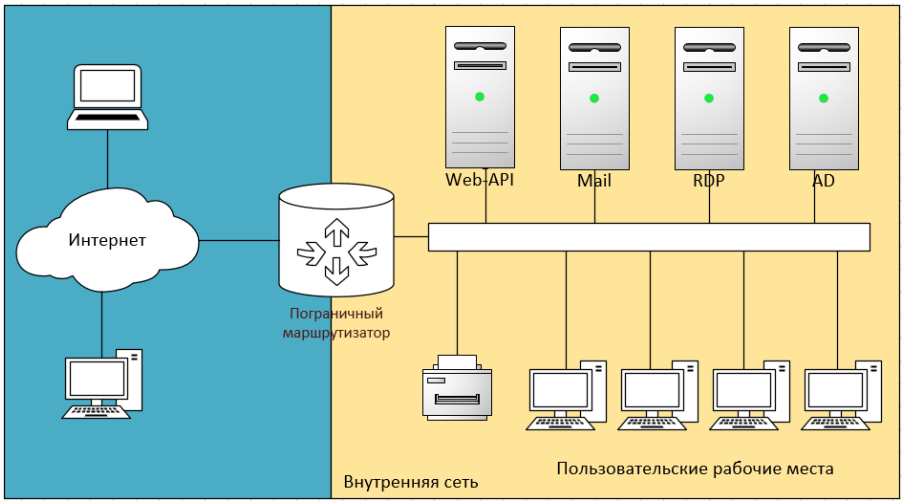

Рисунок 8.1 – Топология плоской сети

При построении DMZ с одним межсетевым экраном требует наличия минимум трех сетевых интерфейсов для соединения с WAN, LAN и DMZ. Для большей защищенности рекомендуется использовать два межсетевых экрана (рисунок 8.2). Первый межсетевой экран используется на внешнем периметре сети и служит только для направления трафика в DMZ, второй – обслуживает трафик из DMZ во внутреннюю сеть. Такой подход считается более безопасным, т. к. он создает два отдельных независимых периметра сети.

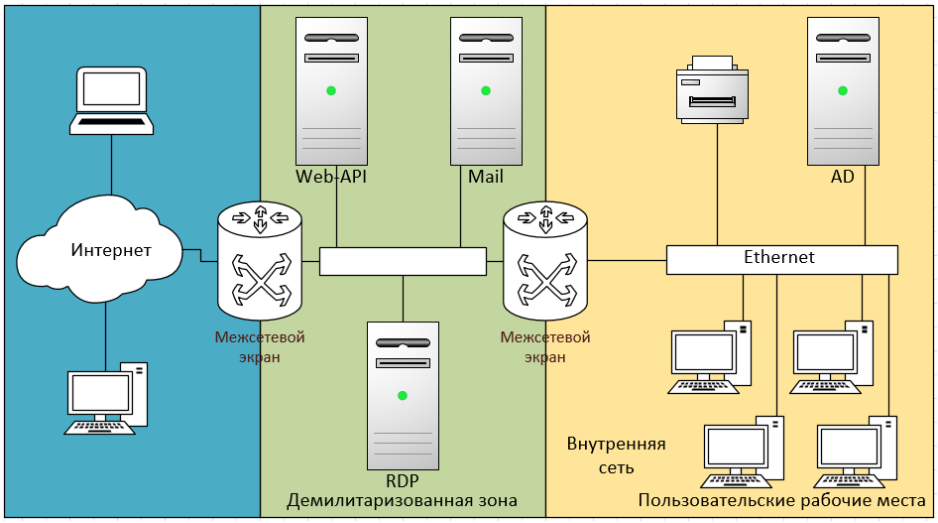

Рисунок 8.2 – Топология сети с DMZ и двумя межсетевыми экранами

Таким образом, построение сети с демилитаризованной зоной позволяет существенно повысить безопасность внутренней сети. При этом необходимо учитывать, что эксплуатация уязвимостей серверов в ДМЗ может привести к нарушению безопасности во внутренней сети при взаимодействии пользователей внутренней сети с серверами из DMZ. Решением данной проблемы является использование разделения сети на Front-End и Back-End, которые располагаются на отдельных серверах в DMZ и внутренней сети соответственно. Серверы в

Front-End осуществляют взаимодействие с внешними пользователями, серверы в Back-End необходимы для взаимодействия с внутренними пользователями. Для взаимодействия Front-End и Back-End на внутреннем межсетевом экране создаются правила, разрешающие инициацию подключений от Front-End к Back-End с дополнительной фильтрацией трафика.

Рассмотрим пример построения сети с DMZ на основе межсетевого экрана Cisco ASA 5505.

Межсетевой экран Cisco ASA 5505 – многофункциональное программно-аппаратное устройство защиты ресурсов локальной сети от внешних атак.

Основные функции межсетевого экрана Cisco ASA 5505:

– статическая, динамическая маршрутизация;

– поддержка коммутации и маршрутизации более 4000 VLAN;

– ограниченное управление качеством обслуживания (QoS);

– статический, динамический NAT, PAT;

– глубокий анализ содержимого пакетов;

– обнаружение угроз (сканирования и DoS атак);

– инспектирование трафика;

– конфигурация демилитаризованной зоны (DMZ);

– поддержка различных видов VPN-туннелей;

– управление и конфигурация посредством графического (GUI, Graphical User Interface) и командного (CLI, Command Line Interface) интерфейса;

– интегрированный графический менеджер Cisco Adaptive Security Device Manager (ASDM);

– поддержка Power over Ethernet (PoE) и др.

При организации сетей с межсетевым экраном Cisco ASA (рисунок 8.3) осуществляется разделение на внутреннюю сеть (INSIDE), сеть с демилитаризованной зоной (DMZ), внешнюю сеть (OUTSIDE), для каждой из которых создается VLAN.

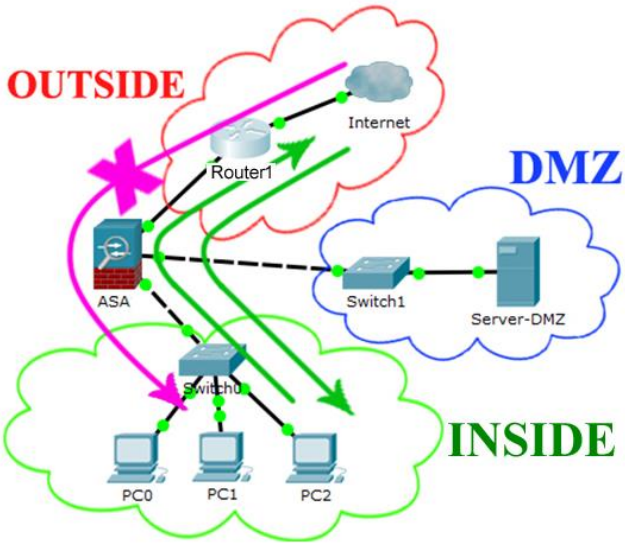

Рисунок 8.3 – Организация сети при использовании межсетевого экрана Cisco ASA

Несмотря на наличие графического интерфейса, базовая конфигурация межсетевого экрана Cisco ASA 5505 производится через интерфейс CLI. Пароль по умолчанию не настроен, поэтому при аутентификации его вводить не нужно, но необходимо настроить новый пароль при первом подключении.

Базовые команды для межсетевого экрана Cisco ASA 5505 практически не отличаются от команд для других сетевых устройств Cisco. В Cisco Packet Tracer функции межсетевого экрана Cisco ASA 5505 существенно ограничены. Например, индивидуальное имя устройства и установка пароля для привилегированного режима настраиваются следующими командами:

```
ciscoasa(config)#hostname ASA60330
ASA60330(config)#enable password пароль
```

Для очистки файла конфигурации используется следующая команда:

```
ASA60330#write erase
ASA60330#reload
```

По умолчанию межсетевой экран Cisco ASA имеет два VLAN, которые назначены для внешнего и внутреннего интерфейса (рисунок 8.4). VLAN1 активирован на всех интерфейсах, кроме Ethernet0/0, для VLAN1 назначен IP-адрес и настроен DHCP-сервер, что необходимо для получения доступа к настройкам межсетевого экрана по Telnet или SSH. Рекомендуется не использовать конфигурацию по умолчанию в процессе эксплуатации межсетевого экрана, поэтому необходимо сначала удалить все настроенные по умолчанию IP-адреса и DHCP.

По умолчанию на межсетевом экране Cisco ASA активирована ограниченная лицензия, которая позволяет создать только три VLAN. Для активации расширенной лицензии Security Plus необходимо ввести ключ активации, который можно узнать с помощью команды `show activation-key`. На рисунке 8.5 представлен результат выполнения команды `show activation-key`, который позволяет скопировать значение ключа, а также убедиться, что разрешено создание только трех VLAN и многие функции ограничены. После ввода значения ключа в команде `activation-key` и перезагрузки межсетевого экрана будет доступно создание двадцати VLAN. Пример активации ключа [21]:

```
ASA60330#activation-key 0x4B43A861 0xD7AC9273 0xCE41D420
0x689B019A 0xD68E69E7
```

```
ciscoasa#show running-config
: Saved
:
ASA Version 8.4(2)
!
hostname ciscoasa
names
!
interface Ethernet0/0
 switchport access vlan 2
!
interface Ethernet0/1
!
--Часть конфигурации пропущена
!
interface Ethernet0/7
!
interface Vlan1
 nameif inside
 security-level 100
 ip address 192.168.1.1 255.255.255.0
interface Vlan2
 nameif outside
 security-level 0
 ip address dhcp
!
telnet timeout 5
ssh timeout 5
!
dhcpd auto_config outside
!
dhcpd address 192.168.1.5-192.168.1.36 inside
dhcpd enable inside
```

Рисунок 8.4 – Базовая конфигурация межсетевого экрана Cisco ASA 5505

```
ASA60330#show activation-key
Serial Number:  JMX153636GB-
Running Permanent Activation Key: 0x48255441 0xCE934E94 0x57A9C9AD 0x1E37965E 0x0C0D2EC4

Licensed features for this platform:
Maximum Physical Interfaces       : 8              perpetual
VLANs                             : 3              DMZ Restricted
Dual ISPs                         : Disabled       perpetual
VLAN Trunk Ports                  : 0              perpetual
Inside Hosts                      : 10             perpetual
Failover                          : Disabled       perpetual
VPN-DES                           : Enabled        perpetual
VPN-3DES-AES                      : Enabled        perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 10             perpetual
Total VPN Peers                   : 25             perpetual
Shared License                    : Disabled       perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
```

Рисунок 8.5 – Проверка функциональности лицензии межсетевого экрана Cisco ASA

Рассмотрим пример конфигурации межсетевого экрана ASA60330 в сети BeCloud (рисунок 8.6), на котором организуем подключение двух VLAN и DMZ. Настройка VLAN осуществляется с помощью следующих команд:

```
ASA60330(config)#interface Vlan1
ASA60330(config-if)#no nameif
ASA60330(config-if)#no security-level
ASA60330(config-if)#no ip address
ASA60330(config-if)#interface Vlan2
ASA60330(config-if)#no nameif
ASA60330(config-if)#no security-level
ASA60330(config-if)#no ip address
ASA60330(config-if)#interface Vlan10
ASA60330(config-if)#nameif inside1
ASA60330(config-if)#security-level 100
ASA60330(config-if)#ip address 192.168.10.1 255.255.255.0
ASA60330(config-if)#no shutdown
ASA60330(config-if)#interface Vlan11
ASA60330(config-if)#nameif inside2
ASA60330(config-if)#security-level 100
ASA60330(config-if)#ip address 192.168.11.1 255.255.255.0
ASA60330(config-if)#no shutdown
ASA60330(config-if)#interface Vlan13
ASA60330(config-if)#nameif outside
ASA60330(config-if)#security-level 0
ASA60330(config-if)#ip address 195.50.8.6 255.255.255.252
ASA60330(config-if)#no shutdown
```

Параметр security level (уровень безопасности) – это число от 0 до 100, которое позволяет сравнить два интерфейса и определить, для какого из них уровень безопасности трафика выше. Обычно для внутренних сетей устанавливается уровень безопасности больше, чем для внешних, т. е. с интерфейса с бóльшим уровнем безопасности на интерфейс с меньшим уровнем безопасности трафик пропускается, сессия запоминается, обратно пропускаются только ответы по этим сессиям – такой трафик называется инспектированным. Трафик, идущий во внутреннюю сеть, по умолчанию запрещен.

Параметр nameif (имя интерфейса) позволяет использовать в настройках не физическое наименование интерфейса, а его имя, которое определяет тип сети (INSIDE, OUTSIDE, DMZ и т. д.).

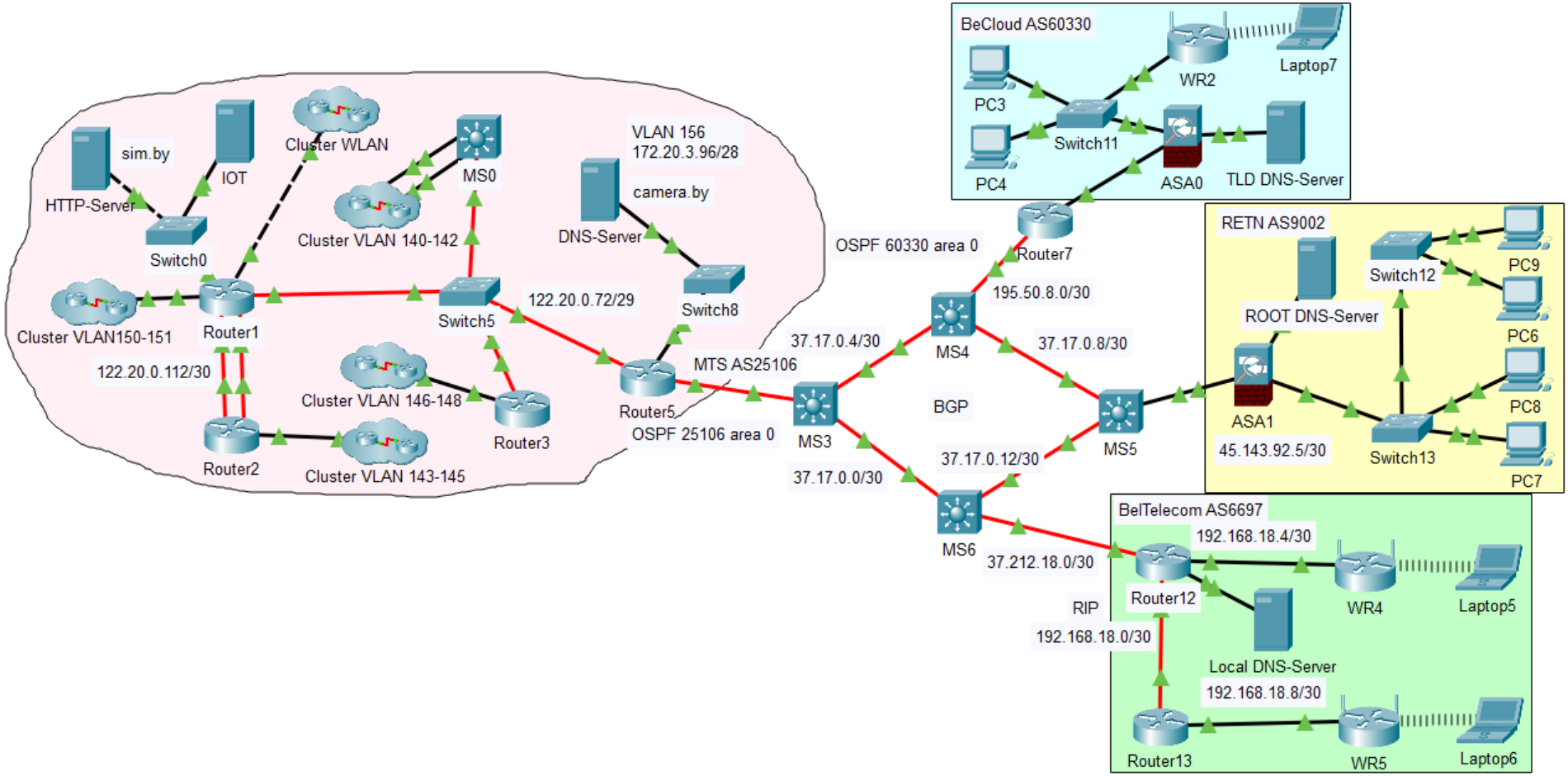

Рисунок 8.6 – Модель сети с межсетевым экранированием

Созданные VLAN необходимо активировать на интерфейсах следующим образом:

```
ASA60330(config)#interface Ethernet0/0
ASA60330(config-if)#switchport access vlan 13
ASA60330(config-if)#interface Ethernet0/1
ASA60330(config-if)#switchport mode trunk
ASA60330(config-if)#switchport trunk allowed vlan 10-11
```

Для настройки маршрутизации по умолчанию используется команда `route` *`имя_внешнего_интерфейса`* `0.0.0.0 0.0.0.0` *`IP-адрес_следующего_перехода`*, для настройки маршрута по умолчанию из внутренней сети во внешнюю в качестве имени интерфейса указывается название для внутренней сети (OUTSIDE).

Для включения DHCP-службы на межсетевом экране Cisco ASA используются следующие команды:

```
dhcpd address диапазон_IP название_VLAN_внутренней сети
dhcpd dns IP-адрес interface название_VLAN_внутренней сети
dhcpd enable inside
```

Межсетевой экран Cisco ASA разделяет конфигурацию на объектную часть, которая определяет преобразуемую сеть, и фактические параметры команды `nat`. Эти части находятся в двух разных местах конфигурации.

Настройка статического преобразования внутренних адресов (NAT) производится командами

```
object network имя
host IP-адрес
nat (название_VLAN_внутренней_сети, название_VLAN_внешней_сети) static IP-адрес
```

Настройка преобразования внутренних адресов (PAT) производится командами

```
object network имя
subnet IP-адрес_подсети маска_сети
nat (название VLAN внутренней_сети,
название_VLAN_внешней_сети) dynamic interface
```

Например, для конфигурации DHCP и NAT для VLAN11 на межсетевом экране ASA60330 в сети BeCloud (см. рисунок 8.6) используются следующие команды:

```
ASA60330(config)#dhcpd address 192.168.11.50-
192.168.11.70 inside2
ASA60330(config)#dhcpd dns 37.212.18.5 interface inside2
ASA60330(config)#dhcpd enable inside2
ASA60330(config)#object network NAT-VLAN11
ASA60330(config-network-object)# subnet 192.168.11.0
255.255.255.0
ASA60330(config-network-object)#nat (inside2,outside)
dynamic interface
```

Для ограничения входящего трафика во внутренней сети необходимо, чтобы исходящий трафик, инициированный из внутренней сети, пропускался во внешнюю сеть и обратно. Все пакеты из внешней сети запрещаются. Например, с компьютера PC4 во VLAN11 (см. рисунок 8.6) отправляется запрос во внешнюю сеть. Когда сервер в сети Интернет получит данный запрос, он должен ответить на него. Этот ответ должен быть пропущен межсетевым экраном. Если же из внешней сети приходят неинициированные из внутренней сети запросы, они должны блокироваться (если не настроены разрешающие ACL). Данная политика может быть осуществлена с помощью следующих команд:

```
class-map название_карты_классов
match default-inspection-traffic
policy-map название_карты_политики
class название_карты_классов
inspect протокол
service-policy название_карты_политики global
```

Для создания политик безопасности на устройстве Cisco ASA сначала создается карта классов, которая определяет, какой тип трафика будет обрабатываться. Команда `match default-inspection-traffic` устанавливает инспектирование всего проходящего через межсетевой экран трафика. Далее создается политика для определения действий над трафиком, которая применяется для созданной карты классов. Команда `inspect` определяет действие инспектирования трафика определенного протокола (DNS, FTP, HTTP и др.). Команда `service-policy` определяет, на какой (входящий и/или исходящий) трафик будет действовать политика (параметр `global` определяет действия для всего проходящего трафика). Например, для конфигурации функции инспектирования трафика HTTP и DNS на межсетевом экране ASA60330 в сети BeCloud (см. рисунок 8.6) используются следующие команды:

```
ASA60330(config)#class-map INSPECT
ASA60330(config-cmap)#match default-inspection-traffic
ASA60330(config-cmap)#policy-map gl-pol
ASA60330(config-pmap)#class INSPECT
```

```
ASA60330(config-pmap-c)#inspect dns
ASA60330(config-pmap-c)#inspect http
ASA60330(config-pmap-c)#service-policy gl-pol global
```

Для удаленного доступа к настройкам межсетевого экрана Cisco ASA используется протокол SSH. Первоначально необходимо настроить авторизацию пользователя и определить для него пароль. Это осуществляется следующим образом:

```
username имя password пароль
aaa authentication ssh console LOCAL
```

Для разрешения SSH-подключений с любого устройства во внутренней сети и с удаленного управляющего устройства во внешней сети используются следующие команды:

```
ssh IP-адрес_внутренней_сети маска_сети название_сети
ssh timeout время
```

Для настройки демилитаризованной зоны сети используется отдельный VLAN и уровень защиты ниже, чем для внутренней сети. Пример создания демилитаризованной зоны для сети BeCloud:

```
ASA60330(config-if)#interface Vlan12
ASA60330(config-if)#nameif DMZ
ASA60330(config-if)#security-level 50
ASA60330(config-if)#ip address 192.168.12.1 255.255.255.0
ASA60330(config-if)#no shutdown
```

К интерфейсу, к которому подключается демилитаризованная зона, прикрепляется созданный VLAN.

```
ASA60330(config)#interface Ethernet0/2
ASA60330(config-if)# switchport access vlan 12
```

Демилитаризованная зона используется для размещения в ней общедоступных сервисов, к которым организовывается доступ как из внешней, так и из внутренней сети. При этом трафик из демилитаризованной зоны не должен поступать во внутреннюю сеть, чтобы исключить возможные атаки. Для выполнения этих условий необходимо создать расширенные ACL. Например, в сети BeCloud есть TLD-сервер, к которому по протоколу DNS обращается сервер ROOT. Также на данном сервере активирована электронная почта. На основе этого составляются разрешающие правила ACL, и ACL активируется на внешнем интерфейсе:

```
ASA60330(config)#access-list OUTSIDE-DMZ extended permit
tcp any host 195.50.8.6 eq 25
ASA60330(config)#access-list OUTSIDE-DMZ extended permit
tcp any host 195.50.8.14 eq 110
ASA60330(config)#access-list OUTSIDE-DMZ extended permit
udp host 45.143.92.9 host 195.50.8.14 eq 53
ASA60330(config)#access-group OUTSIDE-DMZ in interface
outside
```

Команда `show interface ip brief` используется для отображения состояния всех интерфейсов. Информация по интерфейсам VLAN 3-го уровня может быть получена при выполнении команды `show ip address`. С помощью команды `show switch vlan` могут быть получены данные о внутренних и внешних сетях VLAN и назначенных портах. С помощью команды `show route` можно убедиться, что статический маршрут по умолчанию присутствует в таблице маршрутизации ASA. Команда `show nat` используется для просмотра преобразованных и непреобразованных элементов. Команда `show access-list` позволяет просмотреть созданные на межсетевом экране ACL.

8.2 Лабораторное задание

Лабораторная работа выполняется на основе настроек, выполненных в лабораторной работе № 7 (файл **LAB7-2.pkt**). До начала выполнения необходимо открыть сохраненный файл **LAB7-2.pkt** и проверить настройки IP-адресации (см. таблицы 1.2, 3.3, 5.2, 5.3): маршрутизация должна быть настроена по протоколу BGP, номера автономных систем должны соответствовать заданию из таблицы 5.4. В автономных системах должны быть настроены маршрутизация и аутентификация по протоколам OSPF, RIP, EIGRP. Топология сети должна соответствовать рисунку 8.6. На пограничном маршрутизаторе сети NET1 должны быть настроены стандартные и расширенные списки контроля доступа в соответствии с заданиями лабораторной работы № 7. В данной лабораторной работе необходимо настроить межсетевые экраны для сетей NET2 и NET3, в которых организовать демилитаризованные зоны.

1 Заменить пограничный маршрутизатор в сети NET2 на межсетевой экран Cisco ASA 5505 (см. рисунок 8.6).

1.1 Для межсетевого экрана в сети NET2 настроить два VLAN, в одном VLAN должны быть два компьютера, получающие IP-адреса по DHCP, во втором – беспроводной маршрутизатор, получающий IP-адреса по DHCP, к которому подключено два оконечных устройства. Номера VLAN и IP-адреса для них заданы в таблице 8.1. Номер VLAN для внешней сети увеличить на 1. Настроить PAT для созданных VLAN и маршрут по умолчанию.

Таблица 8.1 – Исходные данные для конфигурации сетей NET2 и NET3

Номер второй цифры шифра	Сеть NET2		Сеть NET3	
	Номер VLAN	IP-адрес	Номер VLAN	IP-адрес
1	12 13	192.168.12.0/24 192.168.13.0/24	20 21	192.168.20.0/24 192.168.21.0/24
2	22 23	192.168.22.0/24 192.168.23.0/24	30 31	192.168.30.0/24 192.168.31.0/24
3	32 33	192.168.32.0/24 192.168.33.0/24	40 41	192.168.40.0/24 192.168.41.0/24
4	42 43	192.168.42.0/24 192.168.43.0/24	50 51	192.168.50.0/24 192.168.51.0/24
5	52 53	192.168.52.0/24 192.168.53.0/24	60 61	192.168.60.0/24 192.168.61.0/24
6	62 63	192.168.62.0/24 192.168.63.0/24	70 71	192.168.70.0/24 192.168.71.0/24
7	72 73	192.168.72.0/24 192.168.73.0/24	80 81	192.168.80.0/24 192.168.81.0/24
8	82 83	192.168.82.0/24 192.168.83.0/24	90 91	192.168.90.0/24 192.168.91.0/24
9	92 93	192.168.92.0/24 192.168.93.0/24	100 101	192.168.100.0/24 192.168.101.0/24
0	102 103	192.168.102.0/24 192.168.103.0/24	110 111	192.168.110.0/24 192.168.111.0/24

1.2 Настроить демилитаризованную зону для межсетевого экрана в сети NET2, поместить в нее сервер TLD. Для сервера TLD настроить статический NAT. Установить уровень безопасности для демилитаризованной зоны, равный 60. Настроить инспектирование трафика HTTP и DNS.

1.3 Настроить списки контроля доступа к серверу в DMZ, в которых указать размещающие правила для DNS-запросов от ROOT и авторитарного сервера, для HTTPS и для протоколов, соответствующих e-mail. Остальное запретить.

1.4 Настроить доступ по SSH к межсетевому экрану сети NET2 из одного любого VLAN сети NET2 и компьютера администратора из сети NET1. В отчете представить результат настройки и проверку подключения по протоколу SSH с компьютера администратора из сети NET1 и двух компьютеров из разных VLAN подсети NET2.

1.5 В отчете представить результаты выполнения команд `show interface ip brief`, `show ip address`, `show switch vlan`, `show route`, `show nat`, `show access-list` для межсетевого экрана в сети NET2. Сохранить файл под именем **LAB8-1.pkt.**

2 Заменить пограничный маршрутизатор в сети NET3 на межсетевой экран Cisco ASA 5505 (см. рисунок 8.6).

2.1 Для межсетевого экрана в сети NET3 настроить два VLAN, в каждом из которых должно быть по два оконечных устройства, получающих IP-адреса по DHCP. Номера VLAN и IP-адреса для них заданы в таблице 8.1. Номер VLAN для внешней сети увеличить на 1. Настроить PAT для созданных VLAN.

2.2 Настроить демилитаризованную зону для межсетевого экрана в сети NET3, поместить в нее сервер ROOT. Для сервера ROOT настроить статический NAT. Установить уровень безопасности для демилитаризованной зоны, равный 70. Настроить инспектирование трафика HTTP и DNS.

2.3 Настроить списки контроля доступа к серверу в DMZ, в которых указать размещающие правила для DNS-запросов от TLD и Local DNS Server, для HTTPS, для протоколов, соответствующих e-mail. Остальное запретить.

2.4 Настроить доступ по SSH к межсетевому экрану сети NET3 из одного любого VLAN сети NET3 и компьютера администратора из сети NET1. В отчете представить результат настройки и проверку подключения по протоколу SSH с компьютера администратора из сети NET1 и двух компьютеров из разных VLAN подсети NET3.

2.5 В отчете представить результаты команд `show interface ip brief`, `show ip address`, `show switch vlan`, `show route`, `show nat`, `show access-list` для межсетевого экрана в сети NET3.

3 Удостовериться в правильности работы сети путем получения доступа с разных устройств разных сетей ко всем серверам. При возникновении ошибок внести исправления в конфигурацию устройств без нарушения требований заданий лабораторных работ № 1–8. Сохранить файл под именем **LAB8-2.pkt**.

8.3 Содержание отчета

1 Цель работы.

2 Результаты произведенных настроек в пунктах 1–3, изображение смоделированной сети.

3 Вывод по работе.

4 Ответы на контрольные вопросы.

8.4 Контрольные вопросы

1 Назначение демилитаризованной зоны.

2 Функции межсетевых экранов.

3 Базовая конфигурация межсетевых экранов.

4 Особенности конфигурации VLAN на межсетевых экранах.

5 Конфигурация DHCP и NAT на межсетевых экранах.

6 Принцип конфигурации демилитаризованной зоны.

7 Принцип инспектирования трафика и его конфигурация на межсетевых экранах.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Самойленко, Н. Агрегирование каналов [Электронный ресурс] / Н. Самойленко. – 2023. – Режим доступа: http://xgu.ru/wiki/Агрегирование_каналов.

2. STP [Электронный ресурс]. – 2023. – Режим доступа: http://xgu.ru/wiki/STP.

3. Основы компьютерных сетей. Тема № 7. Протокол связующего дерева: STP [Электронный ресурс]. – 2023. – Режим доступа: https://habr.com/ru/post/321132.

4. Протокол разрешения адресов (ARP). Коммутация [Электронный ресурс]. – 2023. – Режим доступа: https://spravochnick.ru/lektoriy/protokol-razresheniya-adresov-arp-kommutaciya.

5. Коммутаторы 3-го уровня [Электронный ресурс]. – 2023. – Режим доступа: http://www.xnets.ru/plugins/content/content.php?content.196.

6. Белоусова, Е. С. Маршрутизация в IPv4- и IPv6-сетях. Лабораторный практикум : учеб.-метод. пособие / Е. С. Белоусова. – Минск : БГУИР, 2022. – 102 с.

7. Преобразование сетевых адресов NAT [Электронный ресурс]. – 2023. – Режим доступа: http://dvboyarkin.ru/wp-content/uploads/2015/05/1. Metodichka_ Cisco_Packet_Tracer.pdf.

8. Гудюшкина, А. А. Система фильтрации трафика в компьютерной сети организации [Электронный ресурс] / А. А. Гудюшкина, Е. Б. Стариченко. – 2023. – Режим доступа: https://core.ac.uk/download/46138613.pdf.

9. Раздел 3. Сетевые службы [Электронный ресурс]. – 2023. – Режим доступа: https://studfile.net/preview/3250670/page:5.

10. Белоусова, Е. С. Основы построения локальных сетей. Лабораторный практикум : учеб.-метод. пособие / Е. С. Белоусова. – Минск : БГУИР, 2020. – 191 с.

11. Ребязина, В. А. Сетевые формы взаимодействия российских компаний в сфере информационно-коммуникационных технологий / В. А. Ребязина, Ю. Л. Владимиров // Журн. социологии и социал. антропологии. – 2012. – № 5, т. 15. – С. 281–293.

12. Обмен национальным трафиком [Электронный ресурс] / Республиканское унитарное предприятие «Национальный центр обмена трафиком». – 2023. – Режим доступа: https://ncot.by/ru/services/by-ix.

13. Нечаев, А. Н. Особенности функционирования и основные свойства протокола динамической маршрутизации BGP / А. Н. Нечаев, В. С. Авербах // Изв. ин-та систем управления СГЭУ. – 2011. – № 1 (2). – С. 255–258.

14. Колесников, А. В. Красная кнопка интернета / А. В. Колесников // Индекс безопасности. – 2015. – № 4 (115), т. 21. – С. 53–66.

15. Алиев, И. М. Управление внутридоменной маршрутизацией в глобальных сетях / И. М. Алиев, Л. Э. Керимова // Системы управления и информ. технологии. – 2010. – № 1 (39). – С. 112–116.

16. Семёнова, Т. В. Доменное имя как объект гражданских прав / Т. В. Семёнова // Правовая защита интеллектуальной собственности: проблемы теории и практики : материалы Междунар. науч.-практ. конф., 28 мая 2021 г. – С. 121–130.

17. Туманов, С. А. Средства тестирования информационной системы на проникновение / С. А. Туманов // Докл. Томск. гос. ун-та систем управления и радиоэлектроники. – 2015. – № 2 (36). – С. 73–79.

18. СТБ 34.101.73-2017. Информационные технологии. Методы и средства безопасности. Межсетевые экраны. Общие требования. – Введ. 01–01–18. – Минск, 2017.

19. ACL: списки контроля доступа в Cisco IOS [Электронный ресурс]. – 2023. – Режим доступа: https://habr.com/ru/post/121806.

20. Обзор вариантов организации доступа к сервисам корпоративной сети из Интернета [Электронный ресурс]. – 2023. – Режим доступа: https://habr.com/ru/post/302068.

21. Руки дошли: продолжаем про ASA [Электронный ресурс]. – 2023. – Режим доступа: https://habr.com/ru/post/80414.

Св. план 2023, поз. 25

Учебное издание

Белоусова Елена Сергеевна

МАСШТАБИРОВАНИЕ ЛОКАЛЬНЫХ СЕТЕЙ. БЕЗОПАСНОСТЬ МЕЖДОМЕННОЙ МАРШРУТИЗАЦИИ. ЛАБОРАТОРНЫЙ ПРАКТИКУМ

УЧЕБНО-МЕТОДИЧЕСКОЕ ПОСОБИЕ

Редактор *С. Г. Девдера*
Корректор *Е. Н. Батурчик*
Компьютерная правка, оригинал-макет *Е. Г. Бабичева*

Подписано в печать 12.03.2025. Формат 60×84 1/16. Бумага офсетная. Гарнитура «Таймс».
Отпечатано на ризографе. Усл. печ. л. 7,79. Уч.-изд. л. 8,2. Тираж 30 экз. Заказ 37.

Издатель и полиграфическое исполнение: учреждение образования
«Белорусский государственный университет информатики и радиоэлектроники».
Свидетельство о государственной регистрации издателя, изготовителя,
распространителя печатных изданий №1/238 от 24.03.2014,
№2/113 от 07.04.2014, №3/615 от 07.04.2014.
Ул. П. Бровки, 6, 220013, г. Минск