Лабораторная работа №6

Динамическая маршрутизация: RIP

Цель: на основе RIPv2 освоить базовые принципы конфигурирования протоколов динамической маршрутизации в локальных сетях.

1. Теоретические сведения

Routing Information Protocol (RIP) - это дистанционно-векторный протокол маршрутизации, который изначально был предназначен для сравнительно небольших и относительно однородных сетей, в которых справедливо допущение, что все каналы связи имеют примерно равную пропускную способность и примерно равную загрузку (типично для небольших локальных сетей). В этом случае число переходов является разумной метрикой для оценки стоимости продвижения пакетов по маршруту. Для выбора оптимального маршрута в протоколе используется алгоритм Белмана-Форда.

В RIP описание маршрутов хранится в специальной таблице, называемой **таблицей маршрутизации**. Каждая запись о маршруте включает в себя:

- IP-адрес сети (узла - *редко*) назначения;
- Метрику маршрута (от 1 до 15; число шагов до сети назначения);
- IP-адрес ближайшего маршрутизатора (gateway) по пути к сети назначения;
- Таймеры маршрута.

Первые два поля записи определяют термин - **«вектор расстояния»** (сеть назначения – определяет направление, а метрика – модуль вектора). Периодически каждый маршрутизатор посылает копию своей маршрутной таблицы всем соседям (маршрутизаторам), с которыми он непосредственно связан. Получатель (маршрутизатор) просматривает принятую таблицу. Если в ней присутствует новый маршрут, либо сообщение о более коротком маршруте, либо представлены изменения дистанции маршрута, то такие сведения получатель переносит в свою маршрутную таблицу.

Протокол RIP с течением времени перетерпел значительную эволюцию: от классового (classful) протокола маршрутизации (RIPv1) к бесклассовому протоколу RIP второй версии (RIPv2). Усовершенствования протокола RIPv2 включают в себя:

- способность переносить дополнительную информацию о маршрутизации пакетов;
- механизм аутентификации для обеспечения безопасного обновления таблиц маршрутизации;
- способность поддерживать маски подсетей.

Протокол RIP нацелен на предотвращение петель маршрутизации, по которым пакеты могли бы циркулировать неопределенно долго. Для этого максимально допустимое количество переходов на маршруте от отправителя к получателю ограничено значением 15. При получении от соседей таблицы маршрутизации метрика до всех сетей в ней увеличивается на единицу. Если метрика достигает значения 16, то маршрутная запись о такой сети удаляется и сеть считается недостижимой. Протокол RIP реализует и другие механизмы блокирующие распространение некорректных сведений о маршрутах. К ним можно отнести: расщепление горизонта, таймеры удержания информации и др.

В целом RIP является наиболее простым протоколом маршрутизации во внутренних сетях (относится к IGP). С него хорошо начинать изучение основных принципов динамической маршрутизации. Однако по сравнению с такими современными протоколам как EIGRP и OSPF протокол RIP значительно устарел, и в настоящее время он практически не используется.

2. Задание

Выполнять задание следует на основе варианта индивидуальных параметров, содержащихся в Приложении.

2.1. Обучающая часть с индивидуальными параметрами

1. Создайте новый проект CPT и добавьте в него первый маршрутизатор без сетевых интерфейсов.
2. Установите на маршрутизатор 2 интерфейса FastEthernet и 2 интерфейса GigabitEthernet.
3. На основе первого маршрутизатора создайте еще 3 его копии.
4. В **Приложении**, в соответствие в Вашим вариантом, даны диапазон IP-адресов для конфигурирования частных и служебных сетей. Частные сети используются для подключения конечных узлов, а служебные – для соединения маршрутизаторов между собой.
5. На основе 4-х маршрутизаторов постройте сеть с топологией, изображенной на рис. 1, и настройте ее в соответствии с параметрами Вашего варианта. В качестве названий маршрутизаторов используйте такой шаблон: <ФИО>-R<номер маршрутизатора> *(в названии маршрутизатора символы «<» и «>» писать не следует)*. Используя команду *hostname* задайте название каждому маршрутизатору. Маршрут по умолчанию и статические маршруты на маршрутизаторах задавать **не нужно**.

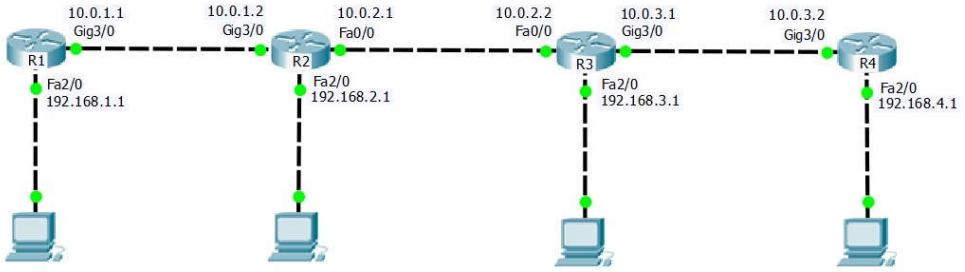

Рис. 1. Пример начальной конфигурация сети

6. Для включения протокола RIP на маршрутизаторе R2 в режиме глобального конфигурирования введите команду: *router rip*. По умолчанию в Cisco IOS она приводит к активации протокола RIPv1 и переходу в режим конфигурирования протокола маршрутизации. При этом приглашение Cisco IOS измениться следующим образом:

   R2(config-router)#

   Первая версия RIP работает только с классовыми сетями, т.е. она на различает подсети. В приведенном примере RIPv1 не сможет корректно анонсировать сети, подключенные к маршрутизатору R2, т.к. данный протокол не увидит различия между сетями 10.0.1.0 и 10.0.2.0, и будет сообщать соседям о сети 10.0.0.0, которая доступна ему через интерфейсы Gig3/0 и Fa0/0. Это приведет к неопределенности в продвижении пакетов и спровоцирует нестабильность работы всей сети в целом. Чтобы избежать такой ситуации необходимо либо изменить номера сетей (например Gig3/0 - 10.0.0.0 и Fa0/0 - 11.0.0.0), либо включить вторую версию протокола RIP, которая использует бесклассовую междоменную маршрутизацию.
7. Включите вторую версию протокола RIP на R2 введя в режиме конфигурирования протоколов маршрутизации команду: *version 2*.
8. Теперь следует указать протоколу RIP о каких сетях следует сообщать своим соседям. Это действие называется **анонсом сети**, а его выполнение производится командой *network* в режиме конфигурирования протоколов маршрутизации. Например, для анонса сети 192.168.1.0 следует указать команду:

   network 192.168.1.0

   При анонсе сети маска подсети не указывается. Маршрутизатор знает обо всех номерах подключенных к нему сетей и подсетей (для определения номера connected-сети

маршрутизатор с помощью логического «и» накладывает маску подсети на IP-адрес сетевого интерфейса). Если номер анонсируемой сети совпадает с номером одной из connected-сетей, то маска для анонсируемой сети в RIP-сообщение добавляется из конфигурации соответствующего сетевого интерфейса.

9. Анонсируйте остальные сети маршрутизатора R2. На этом активация протокола RIPv2 на маршрутизаторе R2 завершена. Сохраните рабочую конфигурацию маршрутизатора.
10. Переведите CPT в режим симуляции и настройте «Event List Filters» так, чтобы отслеживались только пакеты протокола RIP. На «Simulation Panel» нажмите кнопку «Forward» две раза, чтобы кадры с RIP-сообщениями достигли соседних сетевых узлов.
11. Щелкните на кадре, доставленном на R3, чтобы раскрылось окно «PDU Information». Изучите вкладку «OSI model» и ответьте на следующие вопросы:
    - Какой транспортный протокол используется для доставки RIP-сообщений?
    - Какой номер имеет сетевая служба обработки RIP-сообщений?
    - Какой групповой (multicast) адрес используется для рассылки RIP-сообщений?

    Откройте вкладку «Inbound PDU Details», изучите датаграмму и ответьте на следующие вопросы:
    - Как по структуре RIP-сообщения можно определить версию протокола, которому оно принадлежит?
    - Имеется ли в RIP-сообщении поле для указания версии протокола?
    - Информация о какой сети отсутствует в RIP-сообщении?

    Изучите «PDU Information» кадров, доставленных на R1 и компьютер. Информация о какой сети отсутствует в этих RIP-сообщениях?
12. Закройте окно «PDU Information».
13. Нажмите кнопку «Forward» несколько (8-10) раз, и по данным окна «List Event» на «Simulation Panel» определите через какой интервал времени осуществляется отсылка RIP-сообщений?
14. Переключите CPT в режим реального времени.
15. Активируйте работу протокола RIPv2 на маршрутизаторах R1, R3, R4.
    Примечание! На всех маршрутизаторах должна быть запущена одинаковая версия протокола RIP.
16. Для просмотра таблицы маршрутизации в привилегированном режиме Cisco IOS выполните команду: *show ip route*. В примере после настройке протокола RIPv2 на всех маршрутизаторах вид таблицы маршрутизации на R2 представлен на рисунке 2.

```
R2#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter are
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/24 is subnetted, 3 subnets
C       10.0.1.0 is directly connected, GigabitEthernet3/0
C       10.0.2.0 is directly connected, FastEthernet0/0
R       10.0.3.0 [120/1] via 10.0.2.2, 00:00:05, FastEthernet0/0
R    192.168.1.0/24 [120/1] via 10.0.1.1, 00:00:07, GigabitEthernet3/0
C    192.168.2.0/24 is directly connected, FastEthernet2/0
R    192.168.3.0/24 [120/1] via 10.0.2.2, 00:00:05, FastEthernet0/0
R    192.168.4.0/24 [120/2] via 10.0.2.2, 00:00:05, FastEthernet0/0
```

Рис. 2. Таблица маршрутизации R2

В начале каждой маршрутной записи показан код протокола, на основе которого она была получена. Символ «C» - указывает на connected-сети, т.е. сети непосредственно подключенные к маршрутизатору. Символ «R» - указывает на маршрутные данные, полученные посредством обмена сообщениями по протоколу RIP.

Второе поле маршрутной записи содержит номер сети (подсети). В таблице маршрутизации записи группируются по номеру сети (классовая IP-адресация) и маске подсети. На рисунке 2 подсети: 10.0.1.0, 10.0.2.0, 10.0.3.0 относятся к одной сети класса A 10.0.0.0 и имеют одинаковую маску подсети 255.255.255.0 (/24).

В третьем поле маршрутной записи содержится «административное расстояние» (administrative distance - AD) и «метрика протокола маршрутизации» (metric - M). Для connected-сетей AD=1, а M=0. В Cisco IOS эти значения указываются в квадратных скобках – [AD/M]. В выводе команды *show ip route* значение [1/0] заменяется сообщением: «is directly connected». С помощью команды:

(config-router)#distance <значение административного расстояния от 1 до 255>

можно изменить административное расстояние протокола динамической маршрутизации на конфигурируемом устройстве.

В последующих полях маршрутной записи сообщается:

- об IP-адресе сетевого интерфейса, через который достижима заданная сеть *(кроме connected-сетей)*;
- время, прошедшее с момента обновления маршрутной информации (отсчитывается от момента прихода RIP-сообщения о заданной сети)*(этот параметр присутствует только у динамических записей таблицы маршрутизации)*;
- название сетевого интерфейса маршрутизатора, через который достижима заданная сеть.

Протокол RIP использует 4 таймера:

- **Update** – определяет период отправки маршрутной информации соседям. По умолчанию имеет значение 30 секунд. Таймер сбрасывается после отправки сообщения;
- **Invalid** – определяет период обновления маршрутной информации пришедшей из сети. Если обновление о маршруте не будет получено до истечения данного таймера, то маршрут до сети получит в таблице маршрутизации метрику 16, но не будет удален из нее. По умолчанию значение этого таймера равно 180 секунд. Invalid-таймер сбрасывается по приходу из сети нового RIP-сообщения о маршруте;
- **Holddown** – определяет период удержания маршрутной информации о недостижимой сети в таблице маршрутизации. До истечения данного таймера маршрут будет находиться в памяти для предотвращения образования маршрутной петли. По умолчанию равен 180 секундам. Таймер не является стандартным, добавлен в реализации Cisco;
- **Flush** – по умолчанию таймер равен 240 секундам, что на 60 больше, чем Invalid-таймер. Если данный таймер истечет до прихода обновления, то маршрут будет исключен из таблицы маршрутизации. Сбрасывается по приходу из сети нового RIP-сообщения о маршруте.

Для настройки на маршрутизаторе таймеров протокола RIP используется команда со следующим синтаксисом:

(config-router)#timers basic <update> <invalid> <holddown> <flush>

где <update>, <invalid>, <holddown>, <flush> - значения соответствующих таймеров в диапазоне от 1 до 4294967295 секунд.

17. Информация обо всех маршрутах, которые получил маршрутизатор по протоколу RIP, помещается в базу данных. Ее обзор можно сделать командой: *show ip rip database*.
18. Протестируйте прохождение пакетов между конечными узлами Вашей сети.
19. По умолчанию протокол RIP отправляет сообщения во все активные интерфейсы. Однако передача RIP-сообщений в среду, содержащую только конечные узлы, не имеет смысла, т.к. в ней нет RIP-клиентов (маршрутизаторов). Более того, RIP-трафик отнимает часть полосы пропускания у конечных узлов, которые обмениваются своими данными через

маршрутизатор. Заблокировать отправку RIP-сообщений через интерфейс, который связывает маршрутизатор с коммутируемой сетью, можно с помощью команды:

passive-interface <название интерфейса>

Например, к маршрутизатору R2 подключена сеть 192.168.1.0/24. Она содержит только конечные узлы и отправлять туда RIP-сообщения не нужно. Блокировать такую отправку можно командой:

R2(config-router)#passive-interface fa2/0

Определите в какие сети Вашей модели нет необходимости отправлять RIP-сообщения и переведите соответствующие интерфейсы маршрутизаторов в пассивное состояние.

20. Переведите CPT в режим симуляции, включите отслеживание пакетов только с RIP-сообщениями и понаблюдайте в каких направлениях распространяется трафик генерируемый протоколом RIP.
21. Добавьте в модель сети еще один пустой маршрутизатор и установите на него два GigabitEthernet-интерфейса. Измените топологию Вашей сети так как показано на рисунке 3.

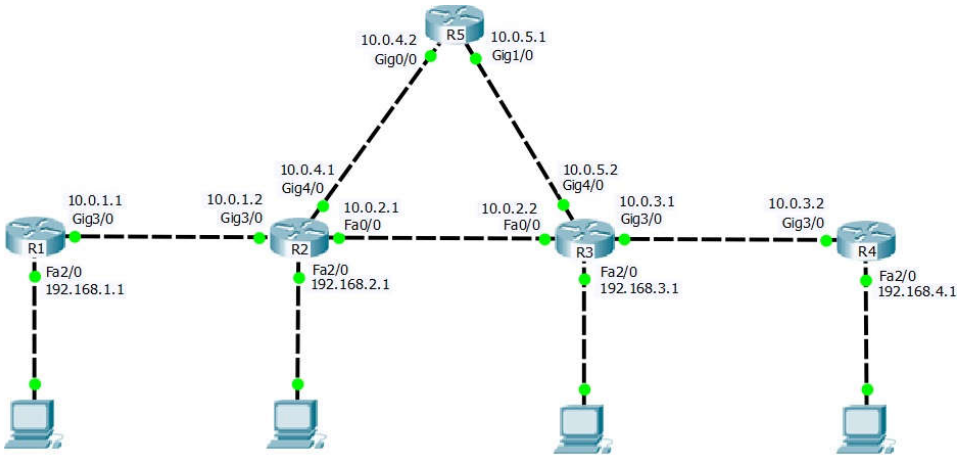

Рис. 3. Модифицированная топология сети

22. Выполните настройку протокола RIP на пятом маршрутизаторе сети и верните CPT в режим реального времени.
23. Протестируйте прохождение пакетов между узлами крайних сетей. В рассматриваемом примере ими являются сети 192.168.1.0/24 и 192.168.4.0/24 (рис. 3). Каким должен быть маршрут пересылки пакетов (из возможных), чтобы время доставки было минимальным? Каким участком маршрута определяется максимальная скорость передачи данных по нему?
24. С помощью команды *tracert* определите маршрут следования *icmp*-пакетов. Этот маршрут соответствует определенному Вами? Почему на участке между маршрутизаторами R2 и R3 данные при передаче данных предпочтение отдается интерфейсу FastEthernet, а не GigabitEthernet?
25. С помощью команды *ping* с ключом *–n 1000* запустите тестирование соединения между крайними сетями. Разорвите соединение между R2 и R3 через интерфейс FastEthernet и отследите какое количество пакетов будет потеряно при восстановлении обмена данными через пятый маршрутизатор по протоколу RIP. Прервите команду *ping*, нажав ^C. Выполните команду tracert и проследите каким стал маршрут передачи данных между крайними сетями. Исследуйте таблицу маршрутизации на R1 и определите количество переходов до сети, которая находится за R4. Восстановите связь между маршрутизаторами R2 и R3 через FastEthernet. Еще раз запросите таблицу маршрутизации на R1 и посмотрите как изменится метрика до сети, которая находится за R4.

26. В протоколе RIPv2 реализована возможность авторизации поступающих обновлений от соседних маршрутизаторов. Сделано это для повышения безопасности, а также для фильтрации обновлений старой версии RIP. Существуют 2 режима авторизации:
    - с установкой пароля открытым текстом;
    - с использованием хэша MD5.

    На обоих маршрутизаторах настраивается один и тот же пароль. Однако в первом случае пароль передается между маршрутизаторами по сети открытым текстом (то есть не шифрованный) и может быть легко раскрыт любым сниффером. Во втором случае пароль по сети вообще не передается. Вместо этого оба маршрутизатора на основе специального алгоритма (хэш-функции) и пароля генерируют последовательность, которая называется цифровым отпечатком или хэш. При доставке пакета с обновлением сравнивается хэш, содержащийся в сообщении, с хэш, который был вычислен на маршрутизаторе. Если они совпадают, то пакет обновления принимается. В противном случае он уничтожается.

    В симуляторе CPT авторизация в протоколе RIP не реализована, но она работает на оборудовании Cisco.

    Для настройки авторизации необходимо установить цепочку ключей, которые будут содержать пароли. Для повышения безопасности можно настроить “срок действия” каждого пароля. Например:

    R1(config)# key chain <название_цепочки>
    R1(config-keychain)# key <номер>
    R1(config-keychain-key)# key-string <пароль>

    Теперь на интерфейсе, на котором запущен RIP, включается аутентификация. Для этого указывается созданная цепочка ключей:

    R1(config-if)# ip rip authentication mode <text | md5>
    R1(config-if)#ip rip authentication key-chain <название_цепочки>

27. Подключите к маршрутизатору R1 коммутатор и организуйте сеть конечных абонентов с тремя VLAN. IP-адреса узлам каждой VLAN назначьте с помощью протокола DHCP, сервер которого организуйте на маршрутизаторе. С помощью технологии ACL заблокируйте взаимодействие VLAN между собой, но разрешите обмен данными с внешними (по отношению к R1) сетями. Настройте протокол RIP на маршрутизаторе R1, чтобы о сетях VLAN узнали остальные маршрутизаторы Вашей сети. Протестируйте работу сети.
28. Продемонстрируйте работоспособную модель Вашей сети преподавателю и сохраните ее в файле с именем **LabNet-06(Фамилия-группа)-task-1.pkt** для последующего отчета по лабораторной работе.

2.2. Самостоятельная работа

1. Создайте новый проект CPT и скопируйте в него сеть из проекта **LabNet-05(Фамилия-группа)-task3.pkt**, построенную в соответствие в вариантом индивидуальных параметров.
2. Дополните сеть ПРЕДПРИЯТИЯ еще двумя локальными сетями аналогично сети, представленной на рисунке 4. Для адресации узлов сетей назначения и интерфейсов маршрутизаторов в служебных сетях используйте индивидуальные параметры, соответствующей Вашему варианту и приведенные в **Приложении**. В качестве адреса DNS-сервера для узлов локальных сетей ПРЕДПРИЯТИЯ следует указать IP-адрес внутреннего DNS-сервера. Внутренний DNS-сервер ПРЕДПРИЯТИЯ должен содержать ссылки на домены ресурсов сети ИНТЕРНЕТ, разрешение имен которых производится на внешнем DNS-сервере.

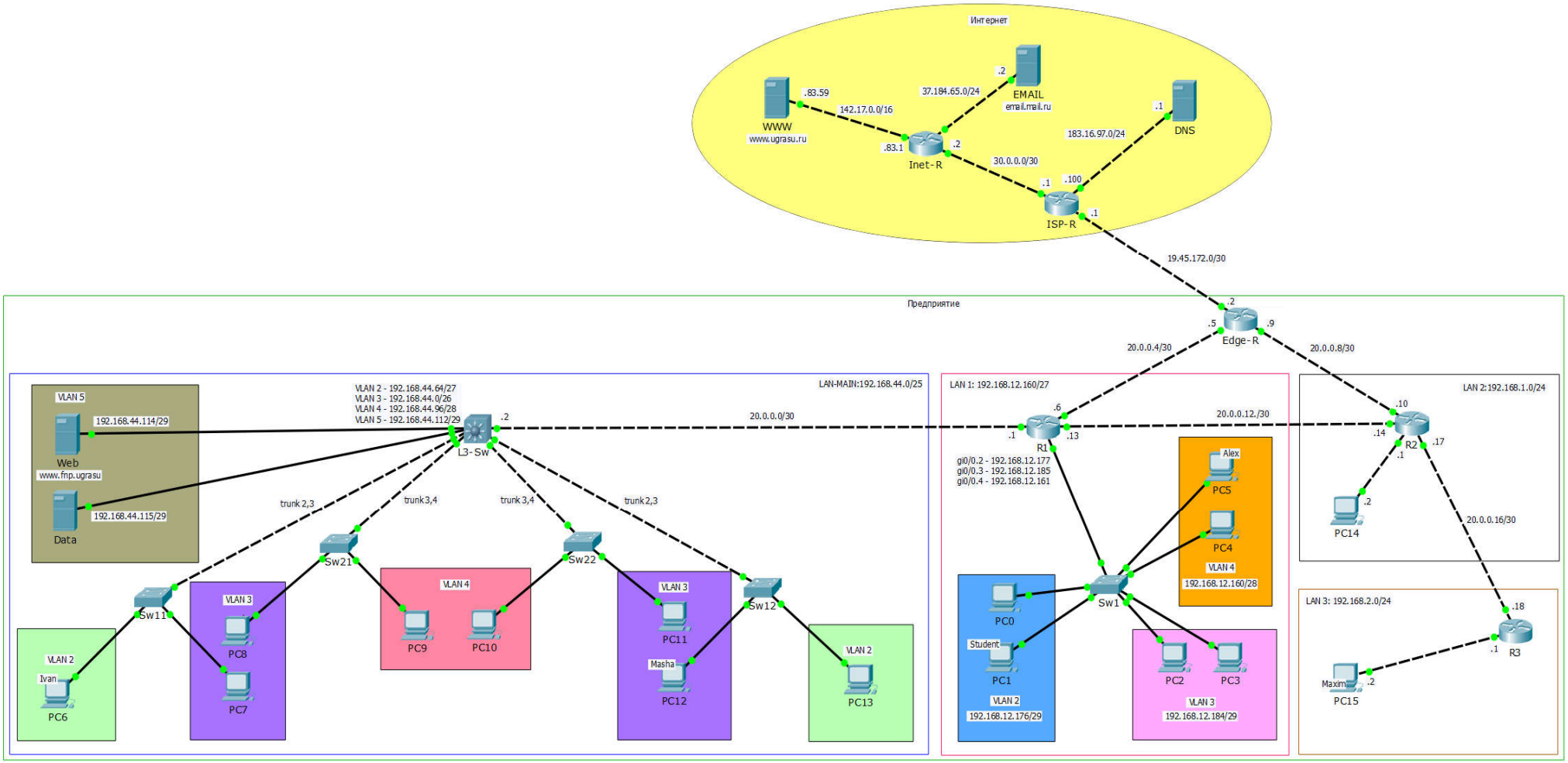

Рис. 4. Примерная структура сети ПРЕДПРИЯТИЯ

3. Удалите на всех маршрутизаторах ПРЕДПРИЯТИЯ статические маршруты, в том числе, маршруты по умолчанию и агрегирующие маршруты.
4. Настройте на маршрутизаторах предприятия протокол RIPv2.
5. Настройте пассивные интерфейсы маршрутизаторов ПРЕДПРИЯТИЯ. На пограничном маршрутизаторе (Edge-R)(рис. 4) интерфейс в сторону сети Интернет также следует сделать пассивным, т.е. маршрутизаторы сети Интернет не должны располагать сведениями о внутренних сетях ПРЕДПРИЯТИЯ.
6. Для доступа к сетям ПРЕДПРИЯТИЯ используйте на маршрутизаторах ИНТЕРНЕТ статические маршруты по умолчанию.
7. На пограничном маршрутизаторе ПРЕДПРИЯТИЯ (Edge-R) создайте статический маршрут по умолчания, направленный в сеть Интернет.
8. Далее на этом маршрутизаторе в режиме конфигурирования протокола RIP выполните команду

   default-information originate

   Она приведет к распространения маршрута по умолчанию на все остальным маршрутизаторы ПРЕДПРИЯТИЯ. Таким образом, каждый из них будет знать куда посылать пакеты, когда адрес сети назначения отличается от адресов сетей ПРЕДПРИЯТИЯ. После выполнения, указанной выше команды, посмотрите как изменилась таблица маршрутизации на сетевых устройствах ПРЕДПРИЯТИЯ? Как помечается маршрут по умолчания, если он получен по протоколу RIP?
9. Протестируйте доступ к Web-ресурсам ПРЕДПРИЯТИЯ и сети ИНТЕРНЕТ. Возможен ли доступ к http-серверу ПРЕДПРИЯТИЯ из сети ИНТЕРНЕТ?
10. Настройте несколько Email-браузеров внутри предприятия для работы через почтовый сервер, который находится в сети ИНТЕРНЕТ. Протестируйте почтовый обмен сообщениями.
11. После отладки и тестирования модели сети продемонстрируйте ее работоспособность преподавателю и сохраните в файле **LabNet-06(Фамилия-группа)-task-2.pkt** для последующего отчета по лабораторной работе.

3. Подготовка отчета, представление и оценка работы

Структура отчета

В качестве отчета по заданию необходимо предоставить готовый проект Cisco Packet Tracer. В рабочей области проекта нужно текстовыми метками указать логины и пароли, которые были задействован при настройке или требуются для использования какого-либо устройства или сетевой службы. В отчете (файлах, направляемых на Eluniver) оценивается точность названий, для которых в задании определен шаблон или уникальное значение, параметры настройки сетевого оборудования.

Загрузку проектов на сайт Eluniver следует выполнять после демонстрации задания преподавателю. Желательно загружать все файлы одновременно.

Представление и защита работы

Представлением работы является ее демонстрация преподавателю. В ходе представления преподаватель может задать вопрос по любому пункту задания или попросить выполнить какие-либо построения на основе навыков, полученных при разработке проекта. Оценка за представление задания выставляется на основе работоспособности проекта, правильности ответа студента на вопросы по проекту и готовности выполнить дополнительное задание без использования методического материала.

Защита работы заключается в ответе на два контрольных вопроса, выбранных произвольно преподавателем из списка контрольных вопросов (п. 4). Оценивается детальность и точность

ответа. Во время ответа пользоваться методическим материалом нельзя. Возможность ответа на контрольные вопросы дается студенту после представления задания.

Структура оценки лабораторной работы

№	Вид оценки	Максимальный балл
1.	Выполнение задания «Обучающей части»	25
2.	Выполнение задания «Самостоятельной работы»	25
3.	Отчет по «Обучающей части»	10
4.	Отчет по «Самостоятельной работе»	10
5.	Контрольный вопрос 1	15
6.	Контрольный вопрос 2	15
	Итого:	**100**

4. Контрольные вопросы

1. Какая метрика используется в протоколе RIP?
2. Какое допущение использовано при выборе метрики протокола RIP?
3. Можно ли на основе метрики протокола RIP оптимизировать таблицу маршрутизации по загруженности сетевых интерфейсов маршрутизатора? Почету?
4. Какой транспортный протокол используется для доставки RIP-сообщений?
5. Какой номер имеет сетевая служба обработки RIP-сообщений?
6. Какой групповой (multicast) адрес используется для рассылки RIP-сообщений?
7. Как по структуре RIP-сообщения можно определить версию протокола, которому оно принадлежит?
8. Имеется ли в RIP-сообщении поле для указания версии протокола?
9. Информация о какой сети отсутствует в RIP-сообщении?
10. Как определить протокол, с помощью которого создана запись в таблице маршрутизации?
11. Как административное расстояние влияет на построение таблицы маршрутизации? Приведите пример.
12. Какое административное расстояние имеет протокол RIP?
13. Каким образом вычисляется метрика маршрутной записи по протоколу RIP?
14. На какие значения административного расстояния и метрики указывает сообщение: «is directly connected»?
15. Как можно изменить значение административного расстояния протокола динамической маршрутизации в Cisco IOS?
16. На что указывает поле времени в маршрутной записи?
17. Могут ли в таблице маршрутизации содержаться записи о маршрутах с метрикой 16?
18. Что такое маршрутная петля? Приведите пример.
19. Какой таймер протокола RIP способствует устранению в сети маршрутной петли?
20. Invalid-таймер устанавливается для маршрутной таблицы в целом или для каждой маршрутной записи по отдельности?
21. Какова структура базы данных протокола RIP?
22. Каким образом можно заблокировать отправку RIP-сообщений через отдельный сетевой интерфейс маршрутизатора?
23. В каком режиме Cisco IOS выполняется команда *passive-interface*?
24. Каким участком маршрута определяется максимальная скорость передачи данных по нему?
25. Почему на участке между маршрутизаторами R2 и R3 данные при передаче данных предпочтение отдается интерфейсу FastEthernet, а не GigabitEthernet?
26. Зависит ли метрика протокола RIP от пропускной способности канала связи?

27. Зависит ли метрика протокола RIP от задержках на сетевых интерфейсах маршрутизаторов?
28. В чем различие между административным расстоянием протокола маршрутизации и его метрикой?
29. Какие команды Cisco IOS используются для настройки цепочки ключей для авторизации приема RIP-сообщений?
30. Какие виды авторизации поддерживает протокол RIPv2?

Приложение. Варианты индивидуальных параметров к заданиям

	Диапазон частных IP-адресов	Диапазон IP-адресов для служебных сетей
1.	192.168.32.0/22	10.56.48.0/28
2.	192.168.158.0/25	10.35.134.128/27
3.	192.168.13.192/26	10.2.5.128/25
4.	192.168.59.128/27	10.126.0.0/28
5.	192.168.11.224/27	10.92.67.128/27
6.	192.168.34.0/26	10.99.38.0/28
7.	192.168.34.0/23	10.93.64.192/26
8.	192.168.44.64/27	10.28.167.224/27
9.	192.168.0.128/25	10.0.0.192/26
10.	192.168.30.0/23	10.26.94.128/27
11.	192.168.37.128/26	10.68.19.0/28
12.	192.168.62/25	10.29.144.64/26
13.	192.168.25.0/25	10.18.90.192/26
14.	192.168.0.192/27	10.0.0.0/23
15.	192.168.200.0/26	10.95.73.0/28
16.	192.168.12.0/22	10.205.16.0/21
17.	192.168.58.192/27	10.105.16.0/27
18.	192.168.75.0/25	10.45.168.0/25
19.	192.168.40.0/23	10.26.12.192/28
20.	192.168.5.128/25	10.26.77.128/27
21.	192.168.0.0/21	10.28.101.0/26
22.	192.168.36.192/26	10.183.17.128/25
23.	192.168.64.0/21	10.0.9.0/26
24.	192.168.90.128/25	10.118.0.64/26
25.	192.35.1.64/26	10.92.0.32/27