Министерство высшего образования и науки Российской федерации
Севастопольский государственный университет

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

Для выполнения лабораторных работ
по дисциплине «Сети передачи данных в территориально-распределенных информационных системах» для студентов очной и заочной форм обучения
направления 09.04.02 «Информационные системы и технологии»

Севастополь
2020

УДК 681.06 + 658.5

Методические указания к выполнению лабораторного практикума по дисциплине «Сети передачи данных в территориально-распределенных информационных системах» для студентов направления 09.04.02 очной и заочной форм обучения. / Разраб. К.В. Кротов. – Севастополь: Изд-во СевГУ, 2020. – 47 с.

Цель лабораторного практикума: ознакомление с основными методами и архитектурами организации объединенных сетей, основными способами настройки маршрутизаторов в глобальных сетях. Предназначено для студентов, обучающихся на направления 09.04.02.

Методические указания рассмотрены и утверждены на заседании кафедры Информационных систем. Протокол № 1 от 28 августа 2018 г.

Допущено учебно-методическим центром СевГУ в качестве методических указаний.

Рецензент: Корепанова Н.Л. канд. техн. наук, доц. каф. Информационных технологий и компьютерных систем.

СОДЕРЖАНИЕ

ОБЩИЕ ТРЕБОВАНИЯ К ВЫПОЛНЕНИЮ ЛАБОРАТОРНЫХ РАБОТ

1. ЦЕЛЬ И ЗАДАЧИ ЛАБОРАТОРНЫХ РАБОТ

Цель настоящих лабораторных работ состоит в исследовании способов организации топологий объединенных компьютерных сетей и способов конфигурирования устройств в объединенных сетях. Задачами выполнения лабораторных работ являются:

- углубленное изучение основных теоретических положений дисциплины «Сети передачи данных в территориально распределенных информационных системах».
- получение практических навыков по конфигурированию устройств в объединенных компьютерных сетях.

2. ОПИСАНИЕ ЛАБОРАТОРНОЙ УСТАНОВКИ

Объектом исследований в лабораторных работах являются способы организации объединенных компьютерных сетей и способы конфигурирования устройств в объединенных сетях. Лабораторная установка состоит из ПЭВМ, снабженной системой программирования Cisco Packet Tracer.

3. СОДЕРЖАНИЕ ОТЧЕТА

Отчеты по лабораторной работе оформляются каждым студентом индивидуально. Отчет должен включать: название и номер лабораторной работы; цель работы; краткие теоретические сведения; постановку задачи; реализацию задания с точки зрения определения IP-адресов, масок, таблиц маршрутизации и т.д., протоколы конфигурирования сетевых устройств, конфигурации сетевых устройств, как результаты выполнения последовательности команд администрирования, результаты обмена пакетами между сетевыми устройствами, подтверждающие работоспособность сформированной конфигурации.

4.ЗАДАНИЕ НА РАБОТУ

Задание выбирается в соответствии с вариантом, назначаемым преподавателем. Вариант задания предполагает определение топологии сети, для которой выполняется конфигурирование сетевых устройств, либо условия для формирования схемы адресации устройств в сети.

ЛАБОРАТОРНАЯ РАБОТА №1

Исследование возможностей, предоставленных IOS, по настройке интерфейсов маршрутизаторов.

1. Цель работы: изучить команды IOS, позволяющие выполнять настройку IP-адресов и протоколов канального уровня интерфейсов маршрутизаторов.

2. Теоретическое введение

Создание объединенной сети, работа с которой осуществляется в рамках данного цикла лабораторных работ, предполагает, прежде всего, формирование схемы IP-адресов компьютеров и узлов в сети. Необходимо отметить, что в рамках лабораторных работ осуществляется работа с сетью, которая объединяет несколько сетей с помощью маршрутизаторов, каждый из которых имеет один вход (порт) Ethernet для подключения локальной сети и два последовательных интерфейса Serial0 и Serial1 для соединения маршрутизаторов друг с другом.

Пример используемой для дальнейшей работы конфигурации сети представлен на рис. 1. В данном случае порт Ethernet0 обозначается E0, порты Serial0 и Serial1 – S0 и S1 соответственно.

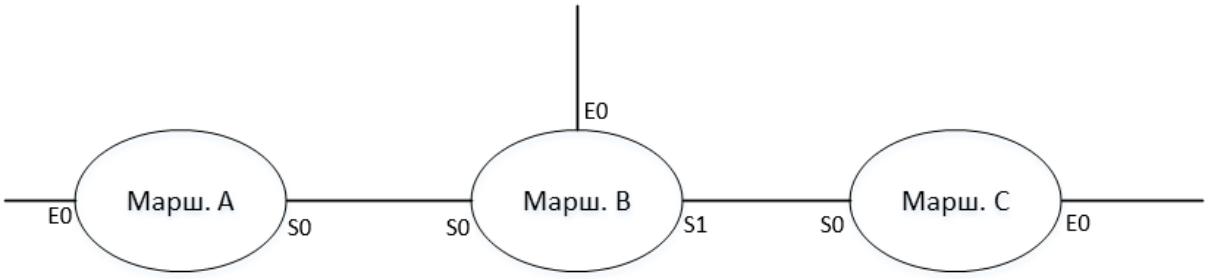


Рисунок 2.1 – Вид используемой конфигурации сети

В данном случае сеть объединяет три локальных сети, соединенных между собой последовательными линиями связи. При этом для сети A выделен IP-адрес 138.2.0.0, для сети B – 138.3.0.0, для сети C – 138.8.0.0. Конфигурирование маршрутизатора предусматривает, прежде всего, задание IP-адресов соответствующих интерфейсов, а уже во вторую очередь включение используемых на маршрутизаторе служб и протоколов. Первоначальное конфигурирование маршрутизатора может осуществляться в режиме ручного конфигурирования, предполагающего непосредственное определение всех требуемых параметров интерфейсов.

Конфигурирование маршрутизатора вручную предваряется переходом из пользовательского режима работы с этим устройством в привилегированный режим командой **enable**. После чего командой **config t** осуществляется переход непосредственно в режим конфигурирования. Действия в режиме настройки интерфейсов маршрутизаторов предполагают выполнение следующих шагов:

1) указание интерфейса, который будет настраиваться, командой **interface**.

2) задание описания использования данного интерфейса (например, LAN или WAN) с использованием команды **description**;

3) задание IP-адреса интерфейса и маски подсети (командой **IP address <адрес> <маска>**);

4) перевод интерфейса в активное состояние – включение интерфейса командой **no shutdown**;

5) после задания параметров интерфейсов маршрутизатора необходимо задать имя маршрутизатора с помощью команды **hostname <имя>** и выйти из режима конфигурирования, нажав **ctrl+z**.

Сохранение созданной конфигурации осуществляется командой **copy running-config startup-config**. В любой момент начальная или текущая (находящаяся в ОЗУ) конфигурация маршрутизатора может быть просмотрена командами **show running-config** или **startup-config** соответственно. Протокол диалога с IOS при ручном конфигурировании маршрутизатора выглядит следующим образом (для маршрутизатора A):

enable
conf t
interface Serial2/0
description LAN
IP address 138.2.0.2 255.255.255.252
encapsulation ppp
no shutdown
exit
interface Serial3/0
description LAN
IP address 138.2.0.5 255.255.255.252
encapsulation ppp
no shutdown
hostname RouterA
exit

Одновременно с настройкой логических адресов интерфейсов необходимо также осуществить настройку протокола канального уровня, с использованием которого осуществляется передача данных по последовательным линиям, соединяющим маршрутизаторы. Таким образом определяются протоколы, с использованием которых пакеты инкапсулируются в кадры для передачи.

Возможными вариантами являются протоколы X.25, PPP, HDLC. Задание протокола анального уровня осуществляется командой encapsulation <имя протокола>, вводимой в режиме конфигурирования интерфейсов маршрутизатора. Просмотр всех свойств интерфейса маршрутизатора, начиная с заданного в процессе настройки IP-адреса, протокола канального уровня, и заканчивая статистикой по количеству принятых и переданных через интерфейс пакетов, можно осуществить следующей командой:

show interface <имя интерфейса>.

Основополагающим моментом при настройке сети является выбор оптимального варианта распределения адресного пространства (IP-адресов) между хостами и маршрутизаторами в сети. Для задания адресов оптимальным образом необходима использовать маски переменной длины (VLSM). Настройка VLSM позволяет присвоить последовательным соединениям один вид маски, а локальной сети другой. При этом возрастает количество адресов в локальной сети (в данном случае последовательное соединение рассматривается также как локальная сеть), которые будут использованы. В классовой модели, где каждый интерфейс маршрутизатора предполагает работу со стандартной маской подсети, любой адрес распадается на адрес хоста и адрес сети. При этом границы такого разделения твердо определены. С помощью VLSM можно перенести разделитель этих двух компонент в любой разряд, задавая тем самым требуемое количество узлов в сети и изменяя количество бит в сетевом префиксе. Т.е. VLSM-маскирование не предполагает задания твердой границы между сетевым префиксом и адресом устройства. Эта граница может переноситься в зависимости от того сколько IP-адресов необходимо организовать в рамках сети (здесь необходимо помнить о зарезервированных для широковещательных рассылок адресах устройств). Таким образом, при реализации VLSM можно вообще отказаться от классового представления адреса и использовать, например, в сети класса B возможности класса C по организации ограниченного количества хостов.

Алгоритм VLSM:

1) Определить количество рабочих станций в подсети.

2) Определить количество бит, необходимых для адресации всех устройств.

$$B = \log_2 (N + 1);$$

где B – количество бит для адресации, N – количество рабочих станций.

3) Определить префикс сети.

4) Определить маску данной подсети.

5) Определить адрес подсети, наложив маску на суммарный адрес сети.

6) Задать IP-адреса устройств в подсети.

Пример реализации:

Суммарный адрес сети равен 172.16.14.0/24.

Выделим три подсети для адресации устройств по 30 устройств и еще три для подсетей «точка-точка» для связи коммутаторов с маршрутизатором.

Сеть 30 устройств.

1) N = 30;.
2) B = 5;
3) 172.16.14.0 0 0 | 0 0 0 0 0;
4) 255.255.255.224;
5) 172.16.14.32/27;
6) Устройства в сети будут адресоваться с адреса 172.16.14.33/27 до 172.16.14.62/27.

Остальные подсети рассчитываются таким же образом. Пример реализации представлен на рисунке 2.2.

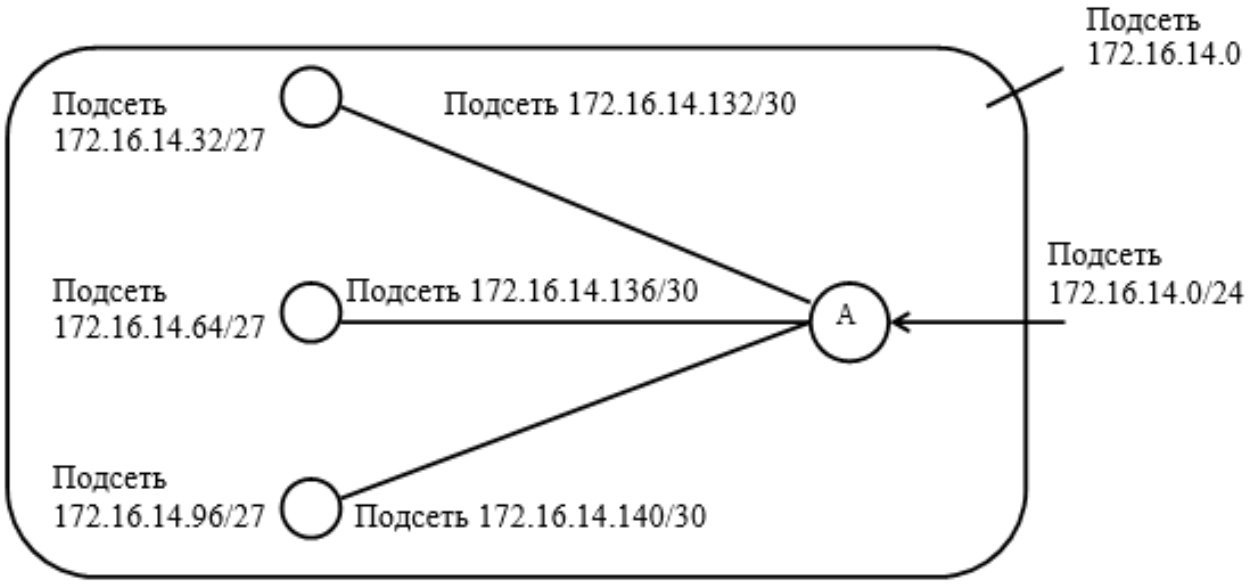


Рисунок 2.2 – Пример реализации VLSM маскирования

Например, для реализации последовательного соединения двух маршрутизаторов достаточно всего двух IP-адресов. При учете, что два адреса зарезервированы, размер маски составит /30. Аналогично, если необходимо выделит локальной сети 60 адресов, то маска для сетевого префикса локальной сети составит /26.

3. Варианты заданий

В зависимости от варианта необходимо осуществить настройку объединенной сети, определяя IP-адреса соответствующих интерфейсов маршрутизаторов.

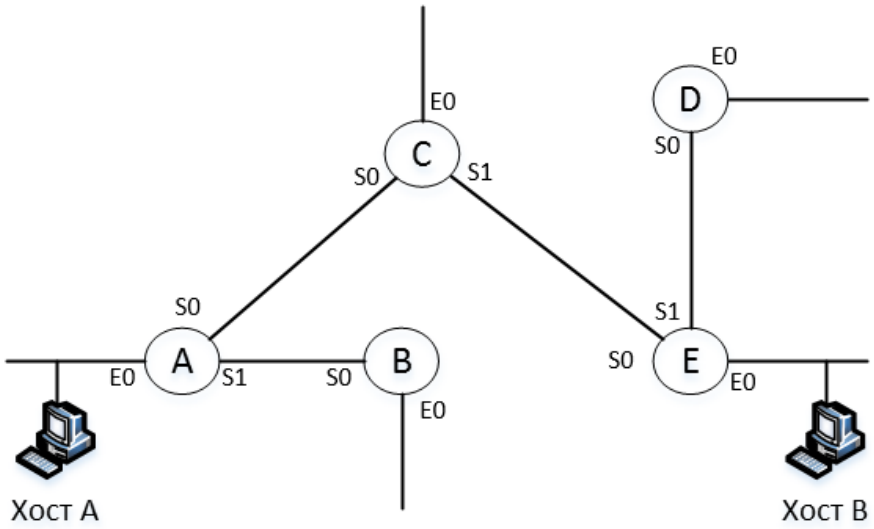
Для этого первоначально сформировать схему IP-адресации, при учете, что в каждой локальной сети необходимо выделить порядка 250 адресов, а для соединения маршрутизаторов необходимо использовать всего 2 адреса. Необходимо просмотреть стартовую конфигурацию каждого из маршрутизаторов, выполняя переход между ними, используя средства эмулятора работы IOS.

Выполнить настройку интерфейсов маршрутизаторов A, B, C, D, E в режиме ручного конфигурирования. В качестве протоколов канального уровня задать протокол PPP. Просмотреть рабочую конфигурацию каждого из маршрутизаторов и сохранить ее в качестве начальной для последующей загрузки.

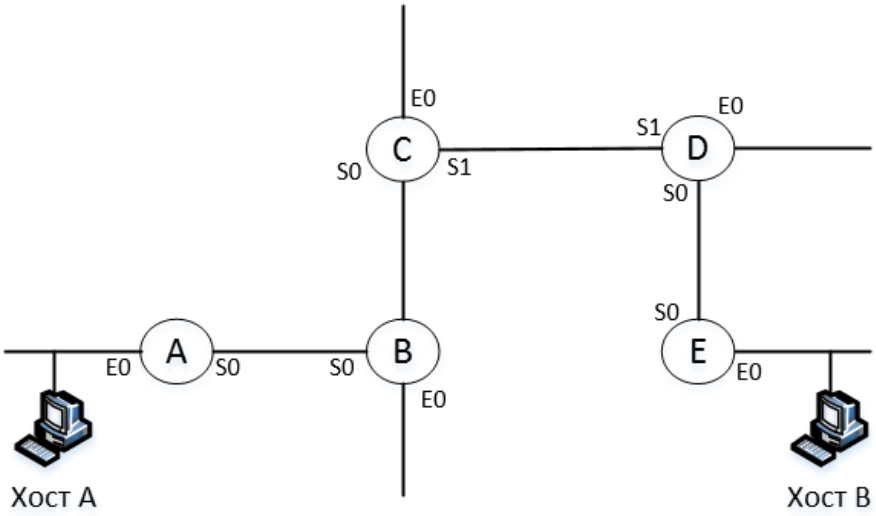
Просмотреть свойства интерфейсов маршрутизаторов.

Суммарный адрес сети: 192.168.0.0/16.

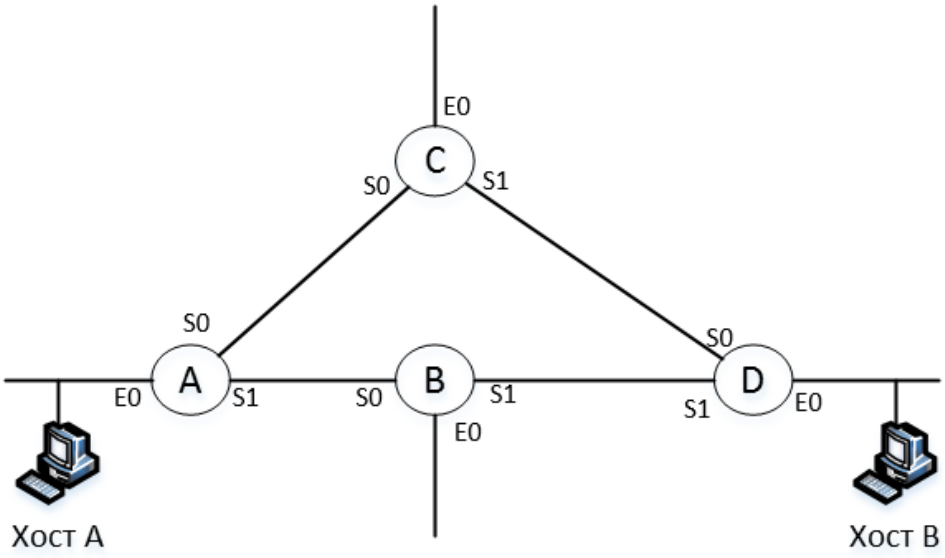
Вариант 1.



Вариант 2.



Вариант 3.



4. Содержание отчета

4.1 Цель работы.

4.2 Задание на работу с указанием схемы объединенной сети, настройка маршрутизаторов в которой осуществляется.

4.3 Распечатку стартовой конфигурации маршрутизаторов.

4.4 Распечатки протоколов настройки маршрутизаторов в диалоговом и ручном режимах настройки.

4.5 Распечатку рабочей конфигурации маршрутизаторов.

4.6 Распечатку свойств интерфейсов маршрутизаторов.

5. Контрольные вопросы.

5.1. В чем состоит отличие классовой схемы адресации от бесклассовой? Каким образом реализуется формирование бесклассовой схемы адресации?

5.2. Для чего в рамках лабораторной работы используется метод VLSM-маскирования?

5.3. В чем состоит алгоритм VLSM-маскирования?

5.4. На каком уровне эталонной модели функционирует протокол PPP и каковы его функции?

5.5. Какой вид имеет кадр протокола PPP?

5.6. Какова последовательность действий при конфигурировании интерфейсов маршрутизаторов и с использованием каких команд выполняется конфигурирование?

5.7. Каким образом при указании интерфейса маршрутизатора указывается, что он сформирован в соответствии с бесклассовой схемой адресации?

5.8. Почему при включении интерфейса маршрутизатора командой no shutdown маршрутизатор не изменяет его состояние на включено?

5.9. Какие образом просматривается текущая конфигурация маршрутизатора и какие параметры в ней указывают на бесклассовую схему адресации?

5.10. В чем состоит назначение основных параметров в распечатке конфигурации маршрутизатора?

5.11. Каким образом выполняется сохранение текущей конфигурации маршрутизатора?

ЛАБОРАТОРНАЯ РАБОТА №2

Исследование способов настройки таблиц статической и динамической маршрутизаций, представленных IOS CISCO.

1. Цель работы: изучить команды IOS CISCO, которые позволяют осуществлять настройку, просмотр и тестирование статических и динамических таблиц, формируемых протоколом EIGRP.

2. Теоретическое введение

Таблицы статической маршрутизации создаются и обновляются вручную. Администратор вручную маршрутизирует таблицы, когда топология объединенной сети изменяется. Одним из вариантов использования статической маршрутизации является условие, когда сеть достижима только по одному пути (тупиковая сеть).

Маршрутизаторы CISCO конфигурируются на применение статической маршрутизации с помощью команды **ip route**:

ip route сеть маска адрес [/интерфейс] [расстояние], где

Сеть – сетевой адрес сети или подсети получателя

Маска – маска подсети

Адрес – IP-адрес интерфейса маршрутизатора, следующего на пути следования пакета.

Интерфейс – название интерфейса, используемого для пересылки пакета (Ethernet0, Serial0, Serial1 для Cisco 2500),

Расстояние – административное расстояние.

Параметр административного расстояния представляет собой оценку надежности источника информации. Он выражается целым числом то 0 до 255 и определяется при учете настроенного протокола, выполняющего маршрутизацию (интерфейс прямого соединения – 0, статический маршрут – 1, EIGRP – 5, внешний BGP – 20, OSPF – 110, RIP – 120, EGP – 140 и т.д.).

Пример установления статического маршрута:

ip route 172.86.0.0 253.255.255.0 172.16.20.2

Т.о. для пересылки пакета в сеть 172.86.0.0 его необходимо переслать на интерфейс 172.16.20.2 ближайшего маршрутизатора.

Т.о., командой **ip route** определяются все маршруты (соответствующие строке в таблице маршрутизации), которые ведут в ту или иную сеть (т.е. интерфейсы маршрутизаторов, куда пересылаются пакеты для достижения той или иной сети).

Просмотр как начального вида таблиц статической маршрутизации, так и сконфигурированных маршрутов осуществляется командой **show ip route**, выполняемой на соответствующем маршрутизаторе. В результате отображается целевая сеть и IP-адрес интерфейса маршрутизатора на пути следования пакета.

Тестирование сконфигурированных путей следования пакетов осуществляется командой **ping**, генерируемой на некотором хосте, аргументом которой

является IP-адрес компьютера, куда пересылается пакет. Например, тестирование пути с хоста А на хост В в вариантах предыдущей лабораторной работы выполняется командой **ping 172.12.10.2**.

Настройка статических таблиц осуществляется в режиме конфигурирования маршрутизатора (вход по команде **config t**).

В случае, если необходимо переопределить статический маршрут соответствующая строка в таблице должна быть удалена, а таблица дополнена новым маршрутом. Удаление строки из таблицы маршрутизации выполняется в режиме конфигурирования маршрутизатора командой

no ip route <IP-адрес целевой сети>

Наряду со статической маршрутизацией, предполагающей использование таблиц, возможна также пересылка пакетов на IP-адрес сконфигурированного по умолчанию шлюза (маршрутизация по умолчанию). Таким образом, если в таблице маршрутизации нет соответствующего пути, пересылка осуществляется на маршрутизатор, выполняющий роль шлюза. Конфигурирование принятого по умолчанию шлюза (задание маршрута по умолчанию на маршрутизаторах CISCO) выполняется аналогично указанию путей при статической маршрутизации. Однако запись в таблице маршрутизации содержит нули в позициях IP-адреса сети и маски подсети. Указывается только IP-адрес интерфейса маршрутизатора, который будет выполнять роль шлюза.

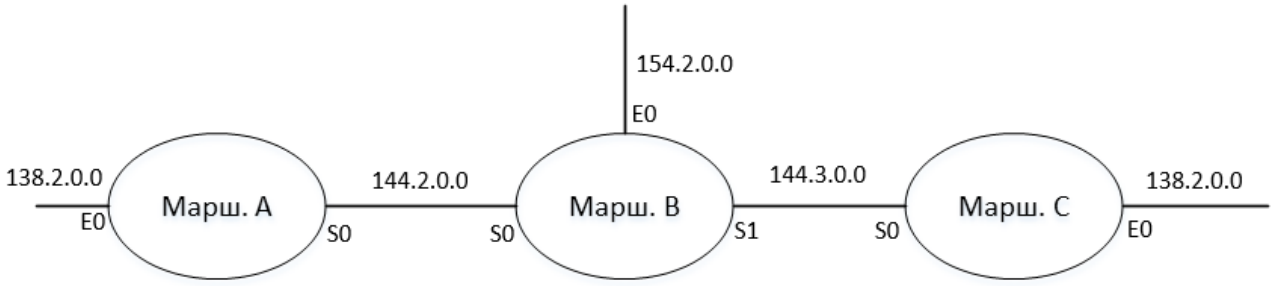


Рисунок 2.1 – Структура объединенной сети с маршрутизацией по умолчанию

Интерфейс S0 маршрутизатора В задается в таблице маршрутизации как интерфейс принятого шлюза для маршрутизатора А. Аналогично интерфейс S0 маршрутизатора С определяется как интерфейс принятого по умолчанию шлюза для маршрутизатора В.

Пример настройки маршрутизации по умолчанию

ip route 0.0.0.0 0.0.0.0 172.16.40.1

В противоположность статической маршрутизации динамическая маршрутизация предполагает обмен таблицами между маршрутизаторами. Протоколы динамической маршрутизации осуществляют определение наилучшего маршрута при учете количества транзитных участков до целевой сети (протоколы вектора расстояния) либо при учете пропускной способности каналов связи (протоколы маршрутизации по состоянию связи). При этом протоколы маршрутизации подразделяются на внутришлюзовые, функционирующие в рамках некоторой автономной системы, и на межшлюзовые, обеспечивающие обмен данными между автономными системами. В больших сетевых комплексах применяются алгоритмы маршрутизации, выявляющие маршрут на основе та-

ких критериев, как скорость (пропускная способность) и задержка линии. Алгоритмы маршрутизации по состоянию связи и некоторые гибридные протоколы при выборе маршрута учитывают именно эти критерии. Протокол EIGRP является гибридным протоколом, объединяющим преимущества маршрутизации по вектору расстояния и по состоянию связи.

Данный протокол является в настоящее время достаточно широко применимым на маршрутизаторах CISCO. Особенностью этого протокола является то, что на основе обмена информацией с соседями маршрутизатор строит базу данных топологии сети, в которой на основе определенных критериев выбираются наилучшие маршруты, заносимые в таблицу маршрутизации. В базе данных топологии может хранится до шести маршрутов к каждой целевой сети. Таким образом протокол EIGRP оперирует с тремя таблицами:

- таблица соседних маршрутизаторов;
- база данных о топологии сети;
- таблица маршрутизации.

При изменении таблицы маршрутизации EIGRP обменивается с соседями только этими изменениями, а не всеми таблицами целиком.

Включение протокола EIGRP на маршрутизаторе осуществляется командой:

router eigrp <номер_автономной_системы>,

где <*номер_автономной_системы*> с какими соседями, входящими в автономную систему, данный маршрутизатор может обмениваться маршрутами. Обмен возможен только между маршрутизаторами, входящими в одну автономную систему (имеющими одинаковый номер автономной системы).

Наряду с заданием использования протокола EIGRP на маршрутизаторе, необходимо определить IP-адреса сетей, с которыми протокол будет обмениваться таблицами. Для этого используется команда IOS:

network <IP-адрес сети>.

Часть <IP-адрес сети> определяет о какой сети будет передаваться информация о маршутизаторах, и только в интерфейсы, которые адресуются в сети с указываемым в команде Network сетевым адресом. Таким образом, протокол выполнения команд для настройки протокола EIGRP на маршрутизаторе A (рисунок 1) при условии, что он будет обмениваться информацией с соседями, выглядит следующим образом:

config t
router eigrp 200
network 138.2.0.0
network 144.2.0.0
^z
copy running – config startup – config

После выполнения указанных команд маршрутизаторы, на которых установлен протокол EIGRP обмениваются пакетами-приветствиями. Для контроля содержания таблицы соседних маршрутизаторов (соответствия номеров автономной системы) при известной схеме объединенной сети используется команда

show ip eigrp neighbors

Эта команда выдает список соседей, которые обмениваются информацией о маршрутах в рамках данной автономной системы. В случае, если список соседей не соответствует схеме сети, была допущена ошибка в задании номера автономной системы на одном из маршрутизаторов. Таким образом, указанная команда позволяет контролировать возможность обмена таблицами между соседними маршрутизаторами. После первоначального обмена таблицами протокол EIGRP осуществляет построение топологии сети. Контроль топологии сети и всех возможных маршрутов пересылки данных осуществляется командой **show ip eigrp topology**, а контроль процесса обмена пакетами между маршрутизаторами (число принятых и отправленных пакетов EIGRP) выполняется с использованием команды **show ip eigrp traffic**. Данная команда позволяет контролировать действительную рассылку пакетов обновлений путем увеличения соответствующих счетчиков. Просмотр же самой таблицы маршрутизации, построенной протоколом EIGRP, осуществляется командой **show ip route eigrp.**
Вход в режим отладки протокола EIGRP, в котором осуществляется отображение вида таблиц маршрутизации, которые отправляются другим маршрутизатором либо принимаются от них, реализуется командой **debug ip eigrp**. Выводится вид изменений в таблицах маршрутизации. На основе этих данных осуществляется последующее обновление таблиц на других маршрутизаторах.

Выход из режима просмотра рассылаемых обновлений таблиц возможен командой **undebug ip eigrp.**

Тестирование логических соединений, реализуемых протоколом EIGRP, осуществляется путем использования команды PING с указанием IP-адреса компьютера, куда пересылается пакет.

Особенностью использования команды PING является то, что она позволяет только констатировать факт достижимости компьютера, находящегося в удаленной сети. Однако она не позволяет контролировать маршрут достижения сети, который по ряду причин может быть не оптимальным (неправильная настойка интерфейсов маршрутизаторов, разрыв линии связи и т.д.). В этом случае для контроля движения пакета по конкретному маршруту (который должен быть оптимальным с точки зрения указанных выше критериев) используется команда **trace** с указанием IP-адреса целевого компьютера.

3. Методика выполнения работы

3.1 Осуществить просмотр начального вида статических таблиц маршрутизации. Определить с какими сетями соединен каждый маршрутизатор. Распечатать начальный вид статических таблиц маршрутизации.

3.2 С помощью команды PING осуществить отправку пакетов с компьютера «хост А» на маршрутизаторы А, В, С… и на «хост В». Прокомментировать выдаваемые после выполнения команды сообщения. Представить результаты рассылки пакетов с использованием команды PING различным получателям.

3.3 Осуществить настройку статических таблиц маршрутизации для маршрутизаторов объединенной сети. Представить вид полученных таблиц маршрутизации.

3.4 Командой PING путем рассылки пакетов с источника «хост А» на маршрутизаторы и на «хост В» выполнить тестирование полученных таблиц маршрутизации и правильность их функционирования. Представить результаты тестирования.

3.5 Осуществить удаление статических таблиц маршрутизации на каждом из маршрутизаторов. Представить вид таблиц маршрутизации после удаления из них маршрутов.

3.6 Осуществить настройку маршрутов по умолчанию (задать для каждого маршрутизатора принятый по умолчанию шлюз). При этом настройку маршрутов по умолчанию (выбор шлюзов) осуществлять в произвольном порядке. Осуществить тестирование полученных маршрутов путем пересылки пакетов между маршрутизаторами и между хостами А и В. Представить результат тестирования.

3.7 Осуществить удаление маршрутов по умолчанию из таблиц маршрутизации. Представить полученный вид таблиц.

3.8 Осуществить настройку протокола EIGRP на каждом из маршрутизаторов с указанием IP-адресов сетей, в которых он будет функционировать. Получить таблицу соседних маршрутизаторов на каждом из настраиваемых маршрутизаторов. Убедиться в правильности формирования автономной системы, соответствующей виду объединенной сети по варианту. Проконтролировать число принятых и отправленных пакетов на начальной стадии формирования базы данных топологии.

3.9 Получить вид базы данных топологии объединенной сети и вид таблицы маршрутизации (содержащей оптимальные маршруты). Прокомментировать критерии, в соответствии с которыми маршруты выбираются из БД топологии сети, и формат полученных таблиц. Осуществить тестирование протокола EIGRP при пересылке пакетов между компьютерами сети. Представить результат тестирования.

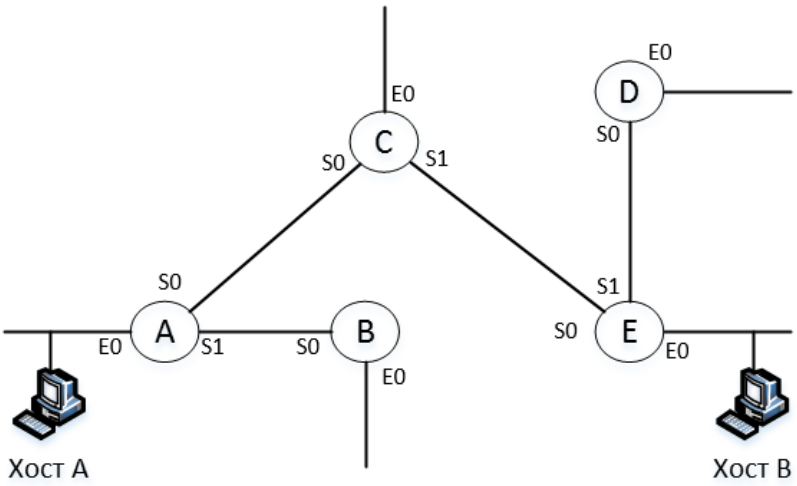
3.10 Войдя в режим конфигурирования, отключить интерфейс E0 на маршрутизаторе D. С помощью команды debug ip eigrp просмотреть вид таблицы маршрутизации, отсылаемой соседним маршрутизаторам. Проконтролировать изменение таблиц на других маршрутизаторах и число пакетов, задействованных для обмена. Предоставить полученный на маршрутизаторах вид таблиц.

3.11 В режиме конфигурирования подключить интерфейс E0 на маршрутизаторе D. Просмотреть вид таблицы маршрутизации, рассылаемой другим маршрутизаторам. Просмотреть изменения таблиц на других маршрутизаторах. Представить конечный вид таблиц на каждом их маршрутизаторов. Прокомментировать формат таблиц, рассылаемых маршрутизатором D. Проконтролировать изменение числа пакетов, используемых для обмена таблицами.

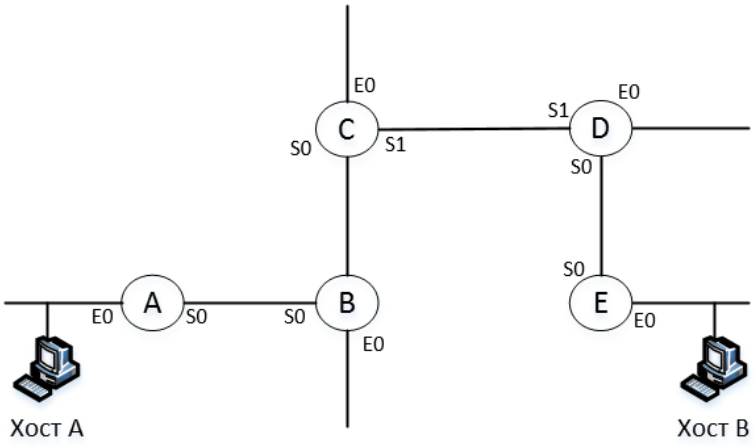
4. Варианты заданий

Настройка статических таблиц и протокола EIGRP на маршрутизаторах осуществляется для конкретного вида объединенной сети, который выбирается в соответствии с вариантом.

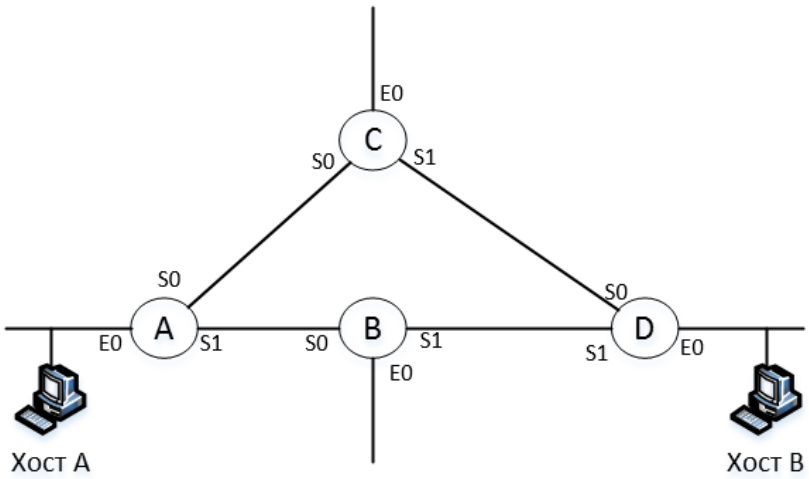
Вариант 1.



Вариант 2.



Вариант 3.



5. Содержание отчета

5.1 Цель работы.

5.2 Формулировки заданий на работу.

5.3 Распечатки протокола команд, реализуемых при выполнении задания.

5.4 Распечатка комментирующей выполнение пунктов задания информации (таблиц маршрутизации, сообщений IOS и т.д.).

5.5 Комментарии к ходу реализации заданий.

5.6 Выводы.

6. Контрольные вопросы

6.1. Информация о каких двух типах сетей хранится в таблице маршрутизации?

6.2. В чем заключаются правила формирования таблиц маршрутизации?

6.3. Каким образом выполняется конфигурирование статической таблицы маршрутизации?

6.4. В чем состоит назначение конфигурирования маршрутизации с использованием шлюзов по умолчанию?

6.5. Каким образом выполняется выбор в сети маршрутизатора, который будет настроен как шлюз по умолчанию?

6.6. К какому типу протоколов относится протокол EIGRP?

6.7. Каким образом протокол EIGRP формирует таблицы маршрутизации?

6.8. Каким образом протокол EIGRP контролирует неизменность топологии и каким образом он перестраивает таблицу маршрутизации при изменении топологии?

6.9. Каким образом по выполнению работы доказать к какому типу протоколов относиться протокол EIGRP?

6.10. В чем состоят причины образования петель маршрутизации в дистанционно-векторном протоколе?

6.11. Какой формат имеют сообщения, которыми обмениваются дистанционно-векторные протоколы при построении таблиц и их перестроении при изменении топологии?

6.12. В чем состоят технологии исключения петель маршрутизации в дистанционно-векторных протоколах?

ЛАБОРАТОРНАЯ РАБОТА №3

Исследование функционирования и настройки протокола OSPF при его работе в многозонных областях маршрутизации

1. Цель работы: исследование функционирования протокола OSPF в многозонных объединенных сетях.

2. Теоретическое введение

Протокол OSPF позволяет разбивать объединенные сети на отдельные области маршрутизации. С его работой в одной зоне маршрутизации связаны следующие понятия:

1) *Зона* – совокупность сетей и маршрутизаторов, имеющих один и тот же идентификатор зоны. Все маршрутизаторы в зоне характеризуются одной и той же информацией о состоянии канала.

2) *Соседи* – два маршрутизатора, имеющие интерфейсы в общей сети.

3) *База данных соседей* – список всех соседей, с которыми установлена двусторонняя связь.

4) *База данных состояния каналов* – список записей о состоянии каналов с другими маршрутизаторами сети (топологическая база данных).

5) *Таблица маршрутизации* – таблица, содержащая записи о маршрутах в сети.

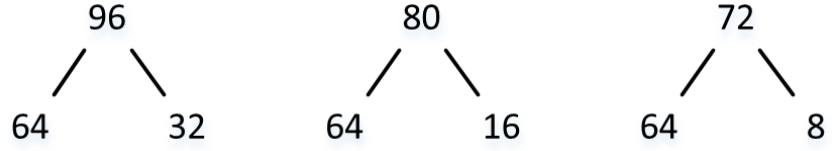
Протокол OSPF поддерживает следующие топологии сетей: широковещательная топология коллективного доступа, не широковещательная топология коллективного доступа, топология “точка-точка”.

Для реализации конфигурирования сети первоначально осуществляется разделение обобщенного сетевого префикса (обобщенного адреса) на части в соответствии с количеством устройств, которое должно быть выделено в каждой из подсетей. Для реализации разделения адресного пространства на части заданного размера используются технологии VLSM-маскирования и CIDR.

Использование VLSM для разделения адресного пространства

Разделить адресное пространство, определяемое суммарным адресом сети 192.168.0.0/24. на подсети с количеством устройств в них 96, 80, 72.

Разделим общее количество устройств на части, каждая из которых содержит количество устройств, кратное степени двойки:



64:

192.168.0.0 0 | 0 0 0 0 0 0

192.168.0.0 1 | 0 0 0 0 0 0

192.168.0.1 0 | 0 0 0 0 0 0

32:

192.168.0.1 1 0 | 0 0 0 0 0
16:
192.168.0.1 1 1 0 | 0 0 0 0
8:
192.168.0.1 1 1 1 0 | 0 0 0

Подсеть с 96 устройствами:
192.168.0.0/26
192.168.0.192/27
Подсеть с 80 устройствами:
192.168.0.64/26
192.168.0.224/28
Подсеть с 72 устройствами:
192.168.0.128/26
192.168.0.240/29

Остальные адреса, входящие в адресное пространство, выделяем на каналы точка-точка.

Использование CIDR для разделения адресного пространства

Разделить адресное пространство на подсети в следующем соотношении долей: 1/2, 1/4, 1/8, 1/8. Суммарный адрес сети: 138.0.0.0/24. Разбиение адресного пространства по технологии CIDR представлена на рисунке 2.1.

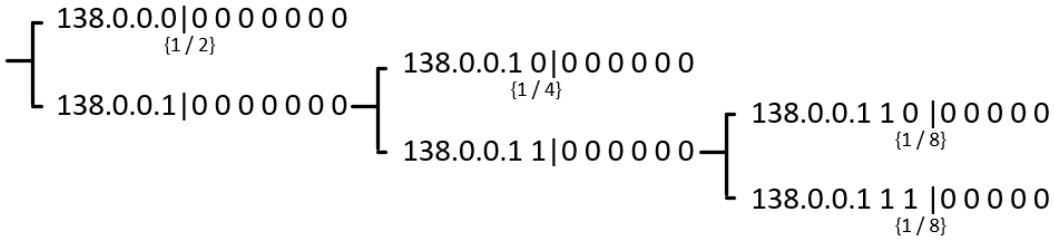


Рисунок 2.1 – Реализация технологии CIDR при разбиении адресного пространства

Конфигурирование OSPF в одной зоне предполагает выполнение следующих шагов:

1) Инициализировать потоки OSPF на маршрутизаторе с помощью команды:

router ospf <process_id>

Параметр <*process_id*> идентифицирует на маршрутизаторе процесс OSPF. Он необходим для связывания идентификаторов процессов на различных маршрутизаторах (более одного процесса OSPF на маршрутизаторе генерировать не рекомендуется).

2) Командой **network** определить сеть (сети), с которой OSPF будет работать (т.е. определиться сеть, которая будет являться частью объединенной OSPF-сети):

network <сеть> <маска> area <area_id>, где

Сеть – сетевой адрес сети.

Маска – инвертированная маска подсети.

<*Area_id*> – id зоны OSPF.

Значение адреса сети может быть или сетевым адресом, либо настроенным адресом интерфейса, из которого с использованием маски выделяется сетевой префикс. Обязательным параметрам команды **network** является параметр **area**, значение которого определяет номер зоны маршрутизации, в которой находится определяемая в network сеть.

Особенностью задания маски в команде network является то, что она инвертированная, т.е. групповые биты, имеющие значение “0”, обозначают соответствие, а “1” – отсутствие соответствия. При задании в качестве адреса в команде в **network** адрес интерфейса маршрутизатора, подключенного к этой сети, назначаемая маска имеет вид 0.0.0.0.

Пример настройки протокола OSPF на маршрутизаторе, к которому подключена сеть Ethernet и который передает данные по последовательному каналу (рисунок 1) представлен ниже.

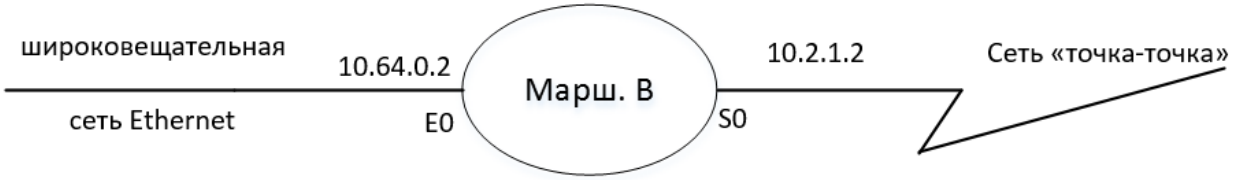


Рисунок 2.1 – Вид сети, настраиваемой в примере

```
interface e0/0
ip address    10.2.0.2   255.255.255.0
interface s0/0
ip address    10.2.1.2     255.255.255.252
router ospf 20
network 10.2.0.2   0.0.0.0       area    1
network 10.2.1.0     0.0.0.0      area    1
```

Проверка работоспособности OSPF при его функционировании в одной сети осуществляется с использованием следующих команд:

а) **show ip protocols** – отображает параметры метрик КС, таймер последнего обновления и т.д.

б) **show ip route** – отображает маршруты известные маршрутизатору, и источник информации об этих маршрутизаторах.

в) **show ip route ospf** – отображает только OSPF-маршруты, т.е. маршруты сформулированные OSPF.

г) **show ip ospf Interface <тип_интерфейса>** – выводит информацию об интерфейсе маршрутизатора. В частности, этой командой для ABR-маршрутизатора можно определить номера зон, в которых находятся его интерфейсы.

д) **show ip ospf neighbor** – отображает информацию (IP-адрес, режим обмена и т.д.) о соседних маршрутизаторах для протокола OSPF.

е) **show ip ospf database** – позволяет осуществлять просмотр таблицы топологии зоны маршрутизации.

Для снижения нагрузки на маршрутизаторы в объединенной сети осуществляется ее (сети) разбиение на зоны маршрутизации. При разбиении сети на

зоны могут быть введены следующие типы маршрутизаторов: внутренний маршрутизатор – маршрутизатор, интерфейсы которого находятся в одной зоне; магистральный маршрутизатор, осуществляющий передачу данных между зонами; граничный маршрутизатор – маршрутизатор, интерфейсы которого подключены к внешним (по отношению к данным) зонам. В соответствии с введенными типами маршрутизаторов настройки протокола OSPF позволяют определить следующие зоны:

1) стандартная зона – зона, работающая в соответствии с описанием функционирования протокола;

2) магистральная зона – зона, подключающая множество зон протокола OSPF и реализующая обмен между ними;

3) тупиковая зона – зона, не принимающая информации о маршрутах, являющихся внешними по отношению к данной автономной системе (АС);

4) полностью тупиковая зона – зона, которая не принимает внешние для данной АС маршруты, а также суммарные маршруты из других зон OSPF.

Настройка ABR по используемым командам соответствует настройке OSPF на внутреннем маршрутизаторе. Отличие состоит в том, что идентификаторы зон в команде **network** для различных интерфейсов ABR должны указываться разными. Например:

router ospf 50
network 10.2.1.2 0.0.0.0 area 1
network 10.64.0.2 0.0.0.0 area 0

В протоколе OSPF суммирование маршрутов по умолчанию отключено. Для настройки суммирования необходимо использовать команду area в следующем формате:

area < area_id >range < address > <mask>.

где параметры: *area_id* задает идентификатор зоны, для которой осуществляется суммирование маршрутов, *address* – суммарный IP-адрес, приведенный в соответствии с диапазоном адресов, *mask* – масса подсети, используемая для суммарного маршрута.

Пример реализации команды area для настройки суммирования маршрутов в сети, приведенной на рисунке 2.2, имеет вид:

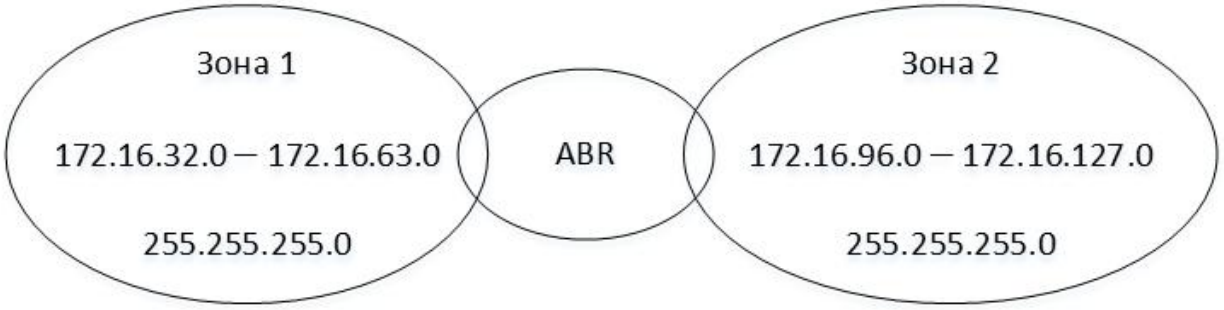


Рисунок 2.2 – Объединенная сеть с суммированием маршрутов

router ospf 50
network 172.16.96.1 0.0.0.0 area 0
network 172.16.32.1 0.0.0.0 area 1

area 0 range 172.16.96.0 255.255.224.0
area 1 range 172.16.32.0 255.255.224.0

Конфигурирование тупиковой или полностью тупиковой зоны осуществляется на маршрутизаторе ABR, запрещая тем самым передачу пакетов внутрь зоны. Оно выполняется в дополнение к определению сетей, находящихся в разных зонах. Формат команды area, конфигурирующий тупиковую или полностью тупиковую зону, имеет вид:

area < идентификатор зоны > stub – задание тупиковой зоны

area < идентификатор зоны > stub no summary – задание полностью тупиковой зоны

Параметр *no summary* является обязательным, он запрещает рассылку суммарных маршрутов в полностью тупиковые зоны.

3. Варианты заданий

Задание выполняется в соответствии с вариантами, называемых преподавателем.

Вариант 1

Реализовать топологию объединенной сети, представленную на рис. 3.1.

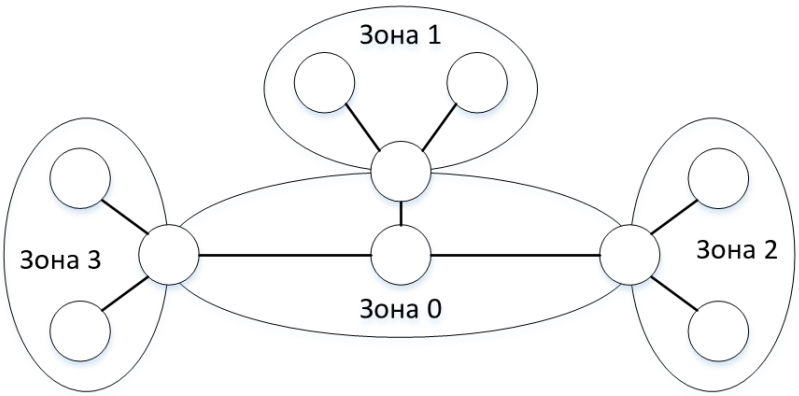


Рисунок 3.1 – Вид объединенной сети, подлежашей настроке.

В зоне 1 использовать сетевой префикс 172.16.1.0/24, адресное пространство которого поровну разделить между сетями, подключенным к внутренним маршрутизаторам. Для зоны 2 использовать префикс 172.16.2.0/24, зоны 3- 172.16.3.0/24, разделив адресное пространство по аналогии с зоной 1. Для зоны 0 использовать сетевой префикс 172.16.4.248/29. На внутренних маршрутизаторах и ABR настроить протоки OSPF. На ABR задать суммарные маршруты для других зон. Зоны 1 и 2 назначить стандартными, зону 3- частично тупиковой. Осуществить вывод всей вспомогательной информации о работе сети: таблица соседей, топологии (для каждого маршрутизатора), БД маршрутизации. Ко всем внутренним маршрутизаторам подключить по одному ПК.

Вариант 2.

Реализовать топологию объединенной сети в следующем виде, представленную на рис. 3.2.

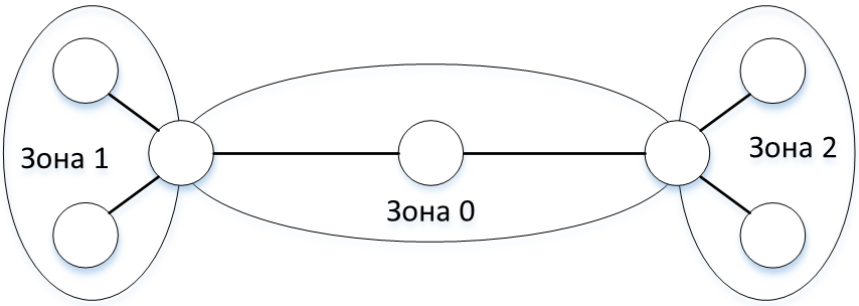


Рисунок 3.2 – Вид объединенной сети, подлежащей настройке.

В зоне 1 использовать сетевой префикс 172.16.1.0/24, адресное пространство которого поровну разделить между сетями, подключенными к внутреннему маршрутизатору. Для зоны 2 использовать префикс 172.16.2.0/24, разделив адресное пространство по аналогии с зоной 1. Для зоны 0 использовать сетевой префикс 172.16.4.248/29, адресуя только канала типа “точка-точка”. На внутренних маршрутизаторах и ABR построит протокол OSPF. На ABR задать суммарные маршруты для других зон. Зона 1 является стандартной, зона 2 конфигурируется как полностью тупиковая. Ко всем внутренним маршрутизаторам (за исключением магистрального) подключить по одному ПК. Осуществить вывод всей вспомогательной информации по функционированию протокола OSPF. Для каждого маршрутизатора (внутреннего и ABR) – таблицы соседей, топологии, маршрутизации, а также информация об интерфейсах.

Вариант 3

Реализовать топологию объединенной сети в следующем виде, представленную на рис. 3.3.

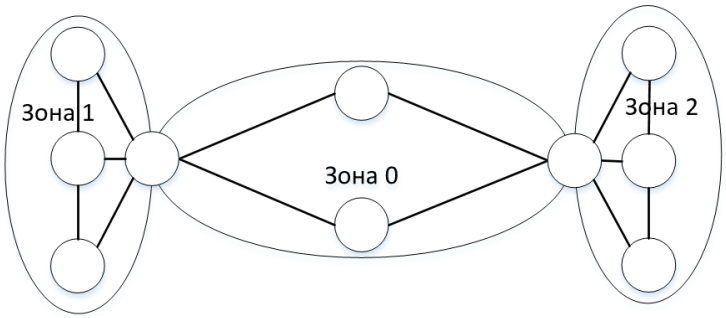


Рисунок 3.3 – Вид объединенной сети, подлежащей настройке.

В зоне 1 использовать сетевой префикс 172.16.1.64/26, для адресации внутренних сетей. Адресное пространство в зоне1 разделить поровну между тремя внутренними сетями. Для зоны 2 использовать префикс 172.16.1.128/24, для адресации внутренних сетей. Для зоны 0 использовать сетевой префикс 172.16.1.16/28, для адресации каналов “точка-точка”, связывающих магистральные маршрутизаторы объединенной сети.

На всех маршрутизаторах построить протокол OSPF, на ABR настроить суммирование маршрутов. Все зоны объединенной сети настроить. К внутренним маршрутизаторам подключить по одному ПК. Осуществить вывод всей вспомогательной информации по функционированию протокола (таблицы соседей, топологии, маршрутизации, а также информация об интерфейсах).

4. Содержание отчета

4.1 Цель работы;

4.2 Формулировки заданий на работу;

4.3 Распечатки протокола команд, реализуемых при выполнении задания;

4.4 Распечатка комментирующей выполнение пунктов задания информации (таблиц маршрутизации, сообщений IOS и т.д.);

4.5 Комментарии к ходу реализации заданий;

4.6 Выводы.

5. Контрольные вопросы

5.1. Каким образом VLSM-маскирование используется для разделения адресного пространства внутри зон маршрутизации?

5.2. Какие команды протокола OSPF используются при настройке этого протокола внутри зоны маршрутизации?

5.3. Какие типы зон маршрутизации поддерживаются протоколом OSPF?

5.4. Какой формат сообщений используется протоколом OSPF для обмена информацией с целью построения дерева топологии?

5.5. Каким образом протокол OSPF реализует построение дерева топологии (в чем заключается алгоритм построения дерева топологии в протоколе OSPF)?

5.6. Какой формат сообщений позволяет обмениваться информацией о суммарных маршрутах в протоколе OSPF?

5.7. Каким образом интерпретируются на маршрутизаторах других зон сообщения с указанием суммарного маршрута от граничного маршрутизатора одной из зон?

5.8. Каким образом в протоколе OSPF формируется информация о внешних по отношению к данной автономной системе сетях? Какой формат имеют сообщения с информацией о внешних по отношению к данной автономной системе сетях, формируемые протоколом OSPF?

5.9. Каким образом интерпретируются на маршрутизаторах сообщения с информацией о внешних по отношению к данной автономной системе сетях?

5.10. Каким образом необходимо выполнить конфигурирование маршрутизатора, выполняющего функции граничного маршрутизатора зоны маршрутизации?

5.11. Каким образом в протоколе OSPF выполняется конфигурирование суммарного маршрута?

5.12. Каким образом в протоколе OSPF выполняется конфигурирование тупиковых и полностью тупиковых зон?

5.13. Какие достоинства конфигурирования тупиковых и полностью тупиковых зон?

5.14. Какие условия должны быть выполнены, чтобы зона могла быть сконфигурирована как тупиковая?

ЛАБОРАТОРНАЯ РАБОТА № 4

Исследование возможностей протокола пограничной маршрутизации (BGP) по организации взаимодействия автономных систем в сети Интернет.

1. Цель работы: изучить средства IOS Cisco, предназначенные для настройки протокола BGP на граничных маршрутизаторах автономных систем сети Интернет. Изучить особенности взаимодействия протокола BGP и протоколов внутри шлюзовой маршрутизации, а также способы взаимодействия граничных маршрутизаторов автономных систем.

2. Теоретическое введение

Протокол BGP применяется в сетях Интернет-провайдеров. Он известен как протокол внешней маршрутизации IP. Он позволяет организовывать систему маршрутизации между автономными системами при обмене маршрутной информацией между ними. В частности, протокол BGP должен использоваться, когда при соединении нескольких провайдеров образуется точка входа в сеть Интернет. Имеется два типа BGP: внутренний BGP (iBGP) и внешний BGP (eBGP). Протокол iBGP позволяет осуществлять обмен между маршрутизаторами, на которых установлен протокол BGP, функционирующих в одной автономной системе. Такая ситуация складывается в случае, если несколько маршрутизаторов одной автономной системы связаны с другими автономными системами (несколькими) и они должны обмениваться друг с другом обновлениями таблиц (рисунок.2.1). Протокол eBGP служит для обмена информацией о маршрутизации между различными автономными системами.

Так как, внутри автономной системы маршрутизация осуществляется с использованием внутри шлюзовых протоколов (IGRP, EIGRP, OSPF и т.д.), а обмен между автономными системами осуществляется с использованием протокола BGP, то на граничных маршрутизаторах эти протоколы функционируют вместе и обмениваются друг с другом информацией посредством редистрибуции таблиц. В тоже время, пересылка пакетов за границы автономной системы может быть осуществлена путем задания граничного маршрутизатора в качестве принятого по умолчанию шлюза для всех внутренних маршрутизаторов автономной системы. В этом случае, все пакеты, направляемые за границы системы переправляются на граничный маршрутизатор, выполняющий их передачу в другую автономную систему. При этом, если в автономной системе имеется несколько маршрутизаторов (в частности, два), поддерживающих протокол BGP и являющихся шлюзами по умолчанию, связанными с более, чем одной автономной системой, необходимо выполнить настройку обмена таблицами между ними (настройки iBGP-взаимодействия). В случае параллельного функционирования IGP и EGP

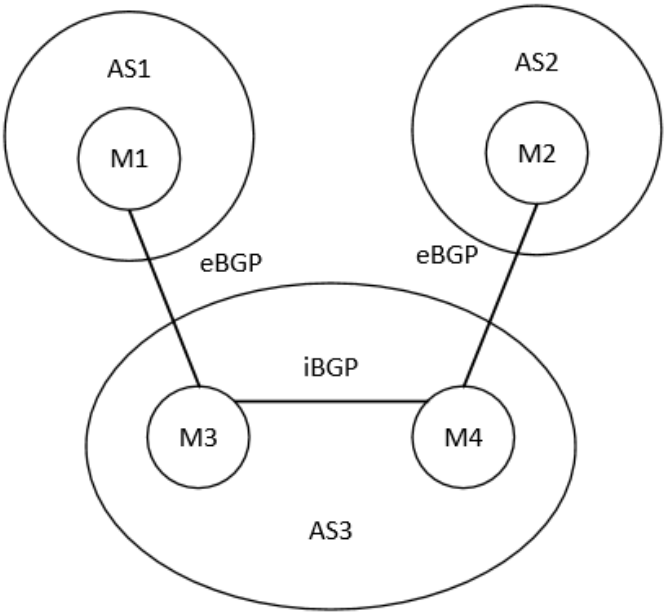


Рисунок 2.1 – Обобщенная организация объединенной сети с использованием iBGP и eBGP маршрутизаторов.

протоколов на маршрутизаторах устанавливать iBGP-взаимодействие между двумя маршрутизаторами нет необходимости.

В случае редистрибуции таблиц маршрутов IGP-протокол (IGRP, OSPF, EIGRP) сам распространит информацию об изменении маршрутов по всей автономной системе.

В результате информация об изменении маршрутов дойдет и до второго маршрутизатора с BGP, функционирующего в рамках этой автономной системы.

3. Настройка протокола BGP на маршрутизаторе

Процесс конфигурирования протокола BGP состоит из трех этапов: разрешение маршрутизатору исполнять протокол BGP, идентификации одноранговых маршрутизаторов, выполняющих функции EBGP обмена с другими автономными системами, идентификации маршрутизаторов, выполняющих функции iBGP обмена внутри своей автономной системы. Последний шаг процесса настройки является необходимым в случае, если граничные маршрутизаторы с протоколами BGP выполняют функции принятых по умолчанию шлюзов для внутри шлюзовых маршрутизаторов в своей автономной системе. При этом настройка шлюза по умолчанию для внутренних маршрутизаторов труда не представляет (см. материал работы № 2) Включение протокола BGP на маршрутизаторе осуществляется командой router bgp, выполняемой в режиме конфигурирования, аргументом которой является номер автономной системы, в которой функционирует маршрутизатор.

router bgp <номер_автономной_системы>

Естественно, что при настройке BGP и EIGRP на одном маршрутизаторе номер автономной системы должен совпадать.

Процесс дальнейшей настройки маршрутизаторов поясняет рис. 3.1 Т.к. М3 и М4 являются принятыми по умолчанию шлюзами для М5 и М6 соответственно (т.е. реализованы статические маршруты), то информация об изменениях в сетях, подключенных к М5 и М6 на шлюзы передаваться не будет. В тоже время изменения на интерфейсах Е0 маршрутизаторов М3 и М4 (131.8.22.7 и 131.8.22.4 соответственно) будут влиять на маршрутную информацию протокола BGP, поэтому их сетевые IP-адреса необходимо указать в команде network после включения протокола BGP. Т.е. информация о сети 131.8.0.0 будет включаться в пакеты обмена протокола BGP между автономными системами.

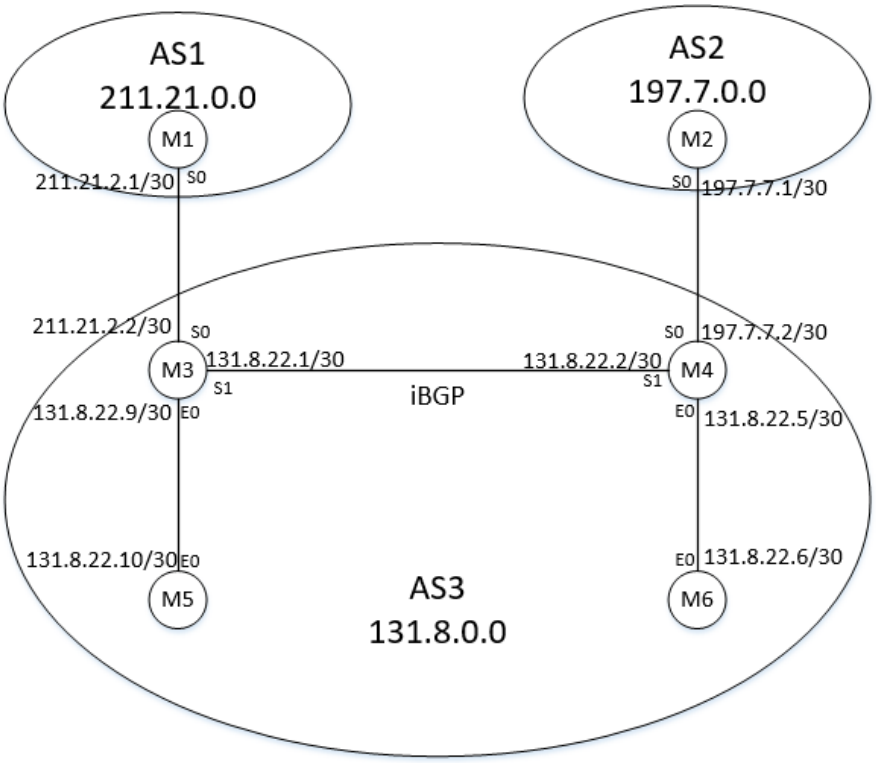


Рисунок 3.1 – Структура объединенной сети при настройке IBGP и EBGP протоколов

Идентификация одноранговых маршрутизаторов (выполняющих функции IBGP или EBGP) осуществляется с помощью команды конфигурирования маршрутизации:

neighbor <IP-адрес_интерфейса_соседнего_маршрутизатора>
remote-as <номер_автономной_системы>

Если номер автономной системы (АС), заданный после remote-as в команде Neighbor совпадает с номером АС, заданным в команде глобального конфигурирования router bgp, то этот маршрутизатор (с указанным в neighbor IP) считается внутренним одноранговым BGP углом (IBGP). Если номер АС, заданный в команде **neighbor** отличается от номера АС, определенного в команде **router bgp**, то команда **neighbor** определяет внешний одноранговый BGP маршрутизатор.

В случае, если необходимо прокомментировать какой IP-адрес принадлежит тому или иному маршрутизатору (внутреннему или внешнему маршрутизатору BGP) может быть использовано ключевое слово description с указанием комментария в команде **neighbor**.

Если маршрутизатор М3 является настроенным маршрутизатором IBGP для маршрутизатора М4 (М4 пересылает обновления таблиц на М3) и есть линия связи между этими маршрутизаторами, то на М4 должен быть настроен статический маршрут до М3. Однако в этом случае будут по этому каналу связи пересылаться и пакеты данных на М3. Чтобы исключить пересылку данных по линии связи, соединяющей М4 и М3, можно использовать расширение списка доступа.

Если внутренние маршрутизаторы BGP не соединены друг с другом линией связи, то при конфигурировании обмена информацией между ними задается интерфейс кольца обратной связи (в рамках данной лабораторной работы этот вопрос не рассматривается).

Обмен между внутренними маршрутизаторами BGP конфигурируется в случае, если эти маршрутизаторы являются принятыми по умолчанию шлюзами для других маршрутизаторов автономной системы (М3 – шлюз для М5, М4 – шлюз для М6). В этом случае пересылка пакетов из АС1 и АС2 в подсети АС3 (рисунок 3.1) осуществляется также с использованием статических маршрутов. Т.е. на маршрутизаторах М3 и М4 наряду с настройкой протокола BGP для обмена с другими АС осуществляется настройка статических маршрутов к подсетям своей автономной системы.

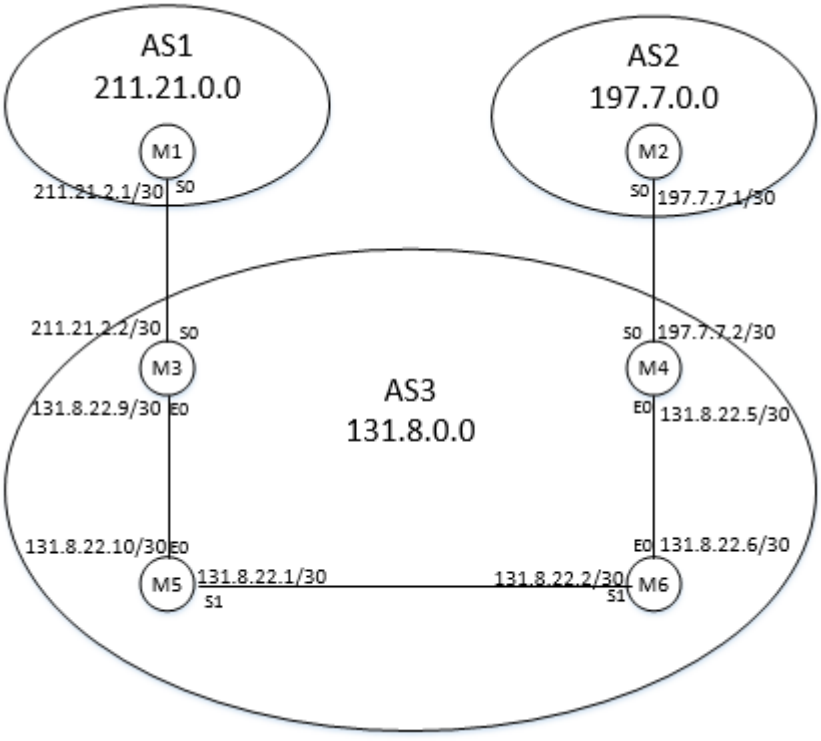


Рисунок 3.2 – Структура объединенной сети при настройке EBGP протокола и статической маршрутизации

Соединение между маршрутизаторами М3 и М4 используется для передачи информации об обновлении таблиц протокола BGP и пакетов данных. Передача пакетов из АС1 в АС2 через АС3 может осуществляться с использованием статических маршрутов от М3 через М5, М6 и М4 (т.е. необходима настройка статических маршрутов). Таким образом, необходима редистрибуция статических маршрутов в динамические таблицы (в таблицы М3 для пересылки

из АС1 в АС2 и в таблицы М4 для пересылки из АС2 в АС1) протокола BGP. Например, если из АС1 передан маршрут на М4 по протоколу BGP и на М4 есть путь через М2 (АС2) до этой сети, то пересылка пакетов от М4 возможна (М4 – граничная точка выхода в другую область). При обмене обновлениями между М3 и М4 этот маршрут должен быть занесен в обновленную таблицу маршрутов протокола BGP. Однако, этого не произойдет в случае, если маршрутизатор М3 (протокол BGP) не знает путь до точки выхода в АС2 (маршрутизатор М4). Чтобы обновить таблицу протокола BGP необходимо явно определить путь до М4, а это осуществляется редистрибуцией статических маршрутов.

В соответствие с этим определяется особенность настройки М3 и М4 – сначала формируются статические маршруты, затем выполняется настройка протокола BGP, в процессе конфигурирования которого необходимость редистрибуции статических маршрутов задается командой redistribute static.

В соответствии с введенными выше командами настройки протокола BGP при учете, что маршрутизатор М3 является принятым по умолчанию шлюзом для маршрутизатора М5 (рисунок 3.1) и он обменивается пакетами обновления с М4, а пакеты данных перемещаются с использованием статических маршрутов, процесс конфигурирования маршрутизатора М3 буде выглядеть следующим образом:

config t
router bgp 3
network 131.8.0.0
neighbor 211.21.2.1 remote-as 1
neighbor 211.21.2.1 description Internet connection
neighbor 131.8.2.1 remote-as 3
neighbor 131.8.2.1 description IBGP connection
^z
copy running – config startup – config

Аналогичным образом настраивается маршрутизатор М4, М1 и М2 настраиваются также, но без задания обмена таблицами внутри области.

В случае, если протокол BGP действует на маршрутизаторе совместно с каким-либо внутри шлюзовым протоколом (например EIGRP) нет необходимости настраивать обмен таблицами между IBGP – маршрутизаторами. В этом случае, выполнив редистрибуцию обновлений таблиц протокола BGP в протокол EIGRP, можно быть уверенным, что сам протокол EIGRP выполнит рассылку обновлений таблиц по всей сети. При выполнении редистрибуции маршрутов из одного внутри шлюзового протокола в другой (например, из RIP в EIGRP) возникает проблема согласования метрик, вычисляемых разными протоколами. Для согласования метрик протокола EIGRP используется специальная команда IOS Cisco.

Однако при редистрибуции протоколов BGP и EIGRP о согласовании метрик вести речь не совсем корректно. Т.к. EIGRP учитывает полосу пропускания линии связи, задержки и т.д. при выборе маршрута внутри автономной системы. Протокол BGP учитывает при выборе маршрута число автономных

систем до целевой сети. Поэтому редистрибуция таблиц одного протокола в другой предусматривает занесение в эти таблицы маршрутов, которые до этого в них отсутствовали. А протокол BGP играет роль точки выхода из автономной системы (в сеть Интернет).

В случае, если на маршрутизаторе функционируют параллельно два протокола, настраивать маршрутизатор IBGP нет необходимости и ориентированный протокол конфигурирования BGP на маршрутизаторе будет иметь следующий вид:

config t
router bgp 3
network 131.8.0.0
neighbor 211.21.2.1 remote-as 1
neighbor 211.21.2.1 description Internet connection
^z
copy running – config startup – config

Настройка редистрибуции таблиц протоколов BGP и EIGRP выполняется уже после конфигурирования этих протоколов на маршрутизаторах с использованием следующей команды:

redistribute <имя_протокола> <номер_автономной_системы>

В этом случае протокол настройки редистрибуции таблиц протоколов BGP и EIGRP ориентировочно может выглядеть следующим образом:

conifg t
router bgp 3
redistribute eigrp 3
router eigrp 3
redistribute bgp 3
^z
copy running – config startup – config

После выполненной настройки обновленные маршруты EIGRP прописываются в таблицах маршрутизации BGP и наоборот.

4. Методика выполнения работы

4.1. Осуществляется построение схемы объединенной сети. Выполняется IP-адресация интерфейсов маршрутизаторов в соответствии со схемой. При этом подсети AC1 адресуются с использованием сетевого адреса 138.8.0.0. подсети AC2 адресуются с использованием сетевого адреса 190.21.0.0, подсети AC3 - 180.2.0.0.

4.2. Маршрутизаторы 1,2,6,8 являются граничными маршрутизаторами для автономных систем AC1, AC2 и Ac3 соответственно. Они задаются в качестве принятых по умолчанию шлюзов для всех остальных маршрутизаторов. В тоже время на маршрутизаторах 1, 2, 6, 8 задаются статические маршруты ко всем остальным маршрутизаторам соответствующих автономных систем. На маршрутизаторах 1 и 2 задаются статические маршруты друг к другу.

4.3. На маршрутизаторах 1,2, 6, 8 осуществляется настройка протокола BGP, при этом на маршрутизаторах 1 и 2 предусматривается обмен обновлениями таблиц маршрутизации внутри автономных систем (настройки IBGP маршрутизаторов). На всех указанных маршрутизаторах выполняется редистрибуция статических маршрутов в таблицы протокола BGP. Выполнить первоначальный просмотр таблиц маршрутов протокола BGP до выполнения редистрибуции и после нее.

4.4. Выполнить тестирование сформированных протоколом BGP таблиц, переслав пакет:

Вариант 1 с маршрутизатора 3 (АС1) на маршрутизатор 9 (в АС3)
Вариант 2 с маршрутизатора 3 (АС1) на маршрутизатор 11

4.5. Отключить на маршрутизаторе 2 интерфейс E0. Просмотреть вид таблицы маршрутизации, которая будет рассылаться IBGP и EBGP маршрутизаторам, с помощью команды debug ip bgp. Прокомментировать последующее изменение таблиц на маршрутизаторах 1,6,8. Уделить внимание контролю обмена изменениями таблиц между маршрутизаторами IBGP в АС1.

4.6. Подключить интерфейс E0 маршрутизатора 2. Просмотреть вид таблицы маршрутизации, рассылаемой маршрутизатором 2 всем другим BGP-маршрутизаторам. Проконтролировать изменения таблиц на маршрутизаторах 1,6,8. Осуществить пересылку пакета:

Вариант 1 с маршрутизатора 7 на маршрутизатор 4
Вариант 2 с маршрутизатора 11 на маршрутизатор 3

4.7. Представить распечатки протоколов выполнения каждого пункта задания.

4.8. Изменить схему объединенной сети, используемой в первой части задания. Для этого отключить интерфейсы S1 на маршрутизаторах 3 и 4. Полученный вид схемы объединенной сети выбирается по вариантам. Аналогичным образом назначить подсетям АС1 адреса с использованием сетевого адреса 138.8.0.0, подсетям АС2 назначить адреса с использованием адреса 190.21.0.0, подсетям АС3 – с использованием адреса 180.2.0.0.

4.9. Выполнить настройку на каждом маршрутизаторе автономных систем АС1, АС2, АС3 протокола EIGRP. Получить вид таблиц маршрутизации на каждом из маршрутизаторов автономных систем. Протестировать правильность построения таблиц путем пересылки пакетов внутри автономных систем:

Вариант 1 пересылка пакетов с маршрутизатора № 3 на маршрутизатор № 2

Вариант 2 пересылка пакетов с маршрутизатора № 3 на маршрутизатор № 1

4.10. выполнить настройку протокола BGP на граничных маршрутизаторах автономных систем – 1,2,6,8. Получить вид таблиц маршрутизации протокола BGP на этих узлах. Выполнить редистрибуцию таблиц протокола EIGRP в протокол BGP и наоборот. Получить вид таблиц маршрутизации протоколов EIGRP и BGP. Сравнить таблицы с их первоначальной формой. Проследить распространение внешних маршрутов протокола BGP по маршрутизаторам автономных систем посредством протокола EIGRP.

4.11. Протестировать функционирование протоколов EIGRP и BGP на маршрутизаторах путем пересылки пакетов:

Вариант 1 с маршрутизатора 3 автономной системы №1 на маршрутизатор 9 в АС № 3.

Вариант 2 с маршрутизатора 3 в АС1 на маршрутизатор 11 в АС3

4.12. Отключить интерфейс E0 маршрутизатора №9. Проконтролировать изменение таблиц маршрутизации на этом маршрутизаторе и получить вид таблиц, рассылаемых протоколом EIGRP другим маршрутизаторам Ас. Проконтролировать изменение таблиц протокола BGP на маршрутизаторе:

Вариант 1 № 8, с последующим изменением таблиц BGP на маршрутизаторах №1, №2 и №6 в АС2.

Вариант 2 № 6, с последующим изменением таблиц BGP на маршрутизаторах №1, №2 и №8 в АС3.

Проконтролировать последующие изменения таблиц маршрутизации протокола EIGRP на маршрутизаторах:

Вариант 1 № 7 в АС 2

Вариант 2 № 11 в АС 3

после отключения интерфейса E0 маршрутизатора №9.

4.13. Подключить интерфейс E0 маршрутизатора 9. Проконтролировать изменение таблиц маршрутизации протоколов EIGRP и BGP

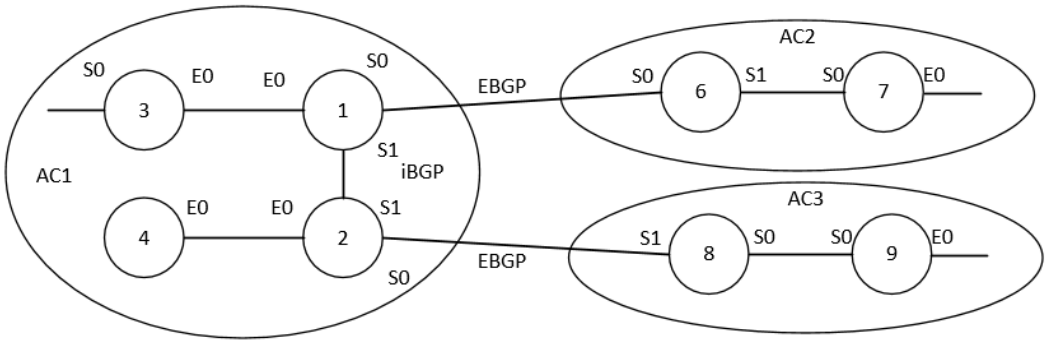
5. Варианты заданий

Задание на работу включает в себя две части. Первая часть предусматривает совместную настройку граничных маршрутизаторов как принятых по умолчанию шлюзов и конфигурирование на них протокола BGP. Вторая часть задания предусматривает настройку на граничных маршрутизаторах автономной системы совместной работы протоколов BGP и EIGRP.

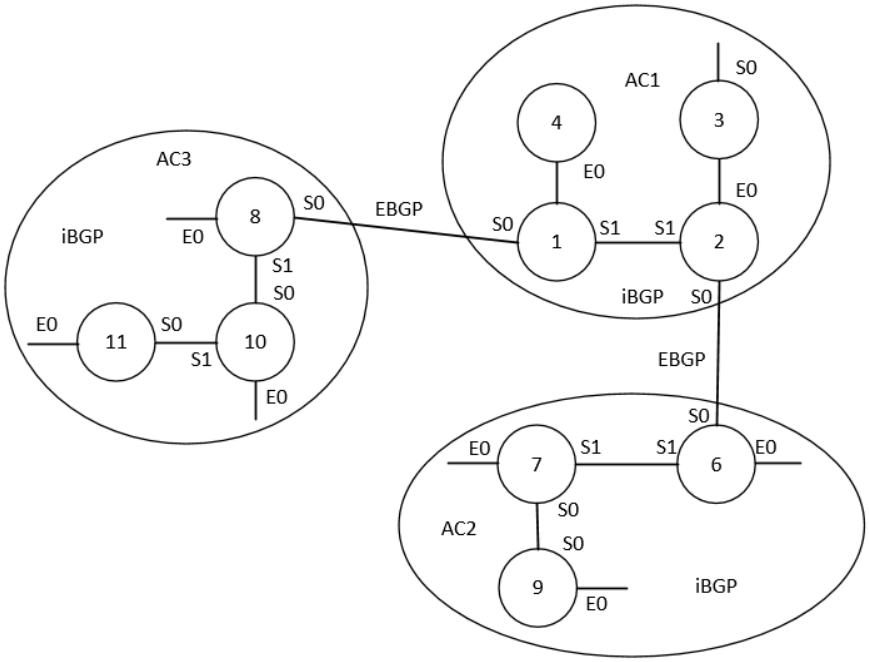
Часть1

Настройка статических маршрутов и протокола BGP на граничных маршрутизаторах.

Вариант 1.

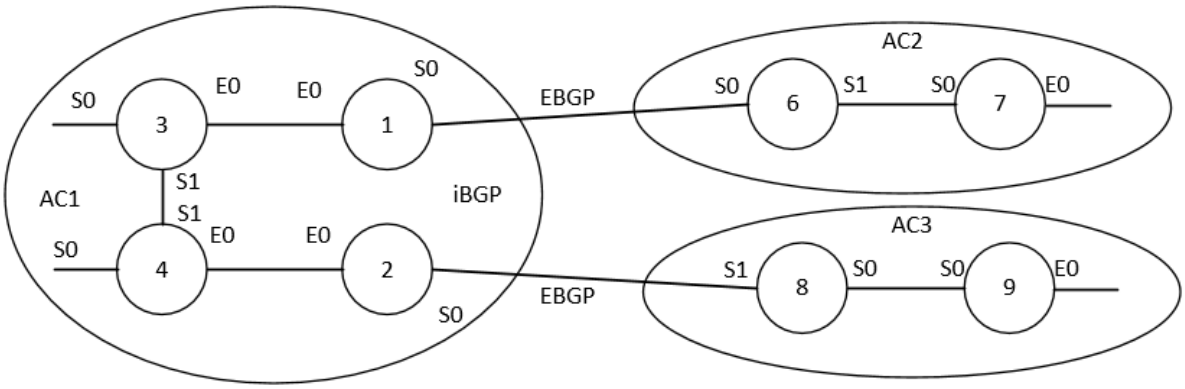


Вариант 2.

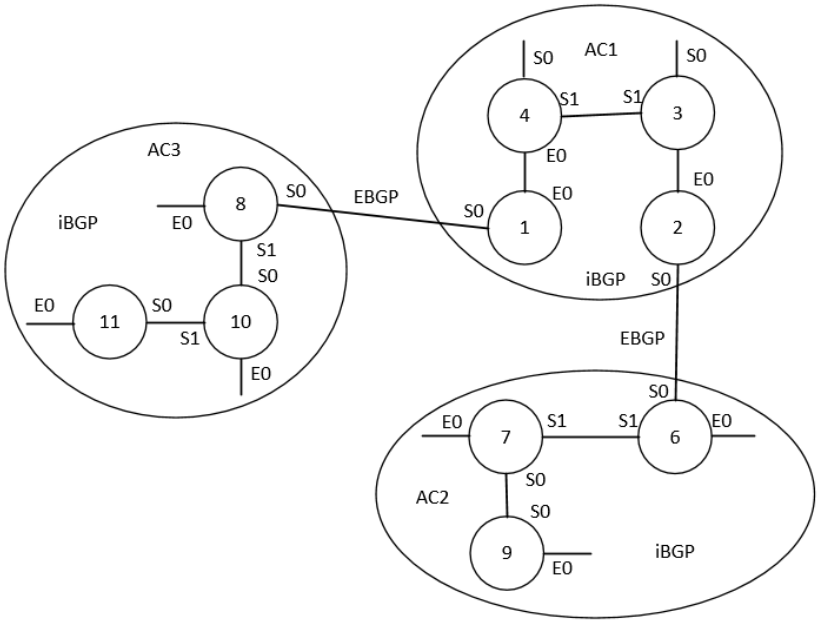


Часть 2

Вариант 1.



Вариант 2.



6. Содержание отчета

6.1 Цель работы.

6.2 Формулировка пунктов задания, распечатка протоколов реализации команд по выполнению пунктов задания. Распечатка служебной информации IOS Cisco, которая позволяет контролировать действительное выполнение пунктов задания.

6.3 Выводы.

7. Контрольные вопросы

7.1. В чем состоит назначение протокола BGP?

7.2.Какие граничные маршрутизаторы автономной системы могут являются BGP соседями?

7.3. В чем состоят функции маршрутизаторов, реализующих IBGP и EBGP режимы работы?

7.4. Какие команды реализуют настройку маршрутизатора с протоколом BGP, функционирующего в IBGP и EBGP режимах.

7.5. В чем состоит отличие функционирования маршрутизатора в IBGP-режиме от функционирования маршрутизатора в EBGP-режиме?

7.6. В том случае, если два граничных маршрутизатора одной автономной системы не соединены каналом связи, как осуществляется распространение внешней маршрутной информации через эту автономную систему?

7.7. В чем заключается понятие редистрибуции маршрутов между протоколами маршрутизации и для каких целей она используется при функционировании протокола BGP?

7.8. Почему в автономной системе, граничные маршрутизаторы которой соединены каналом связи, возможно не использовать внутришлюзовый протокол?

7.9. Каким образом в протоколе реализуется настройка суммарного маршрута для автономной системы?

ЛАБОРАТОРНАЯ РАБОТА № 5

Исследование возможностей, предоставляемых IOS Cisco по оптимизации рассылки таблиц маршрутизации по сети

1. Цель работы: изучить возможности, предоставляемые списками доступа IOS Cisco, которые позволяют осуществить оптимизацию рассылки обновлений таблиц маршрутизации по сети.

2. Теоретическое введение

Для снижения загруженности сети (оптимизации загрузки сети) могут использоваться списки доступа. Списки доступа фильтруют пакеты в соответствии с некоторыми условиями. Если пакет отвечает определенным условиям, он либо пропускается далее, либо отбрасывается. С использованием списков доступа можно оптимизировать процесс рассылки таблиц маршрутизации по сети. В случае перезагруженности сети (которая может контролироваться с использованием протокола SNMP путем просмотра выходных очередей на маршрутизаторах) рассылка таблиц маршрутизации может быть временно прекращена, а затем вновь возобновлена при разгрузке сети. Особенностью использования списков доступа для этих целей является то, что необходимо фильтровать только пакеты протоколов маршрутизации. Данная задача решается с использованием расширенных списков доступа. Механизм построения расширенных списков доступа достаточно сложен, поэтому его понимание лучше начать с исследования способов формирования стандартных списков доступа.

Возможности стандартных списков доступа довольно ограничены. Они способны выполнить отбор только по исходному адресу входящего или исходящего пакета.

Стандартный список доступа представляет собой последовательность операторов **access-list**, содержащих опции **permit** или **deny**. В случае указания опции permit предполагается дальнейшая пересылка пакетов, удовлетворяющих условиям фильтрации. При этом опция **deny** осуществляется отключением пакета, удовлетворяющего условиям, сформированным в списке доступа. Если с интерфейсом маршрутизатора сопоставлен список доступа, просматривается каждая строка списка по порядку, пока не будет обнаружено соответствие тому или иному критерию (отклонять или не отклонять). Если соответствие какому-либо критерию не найдено (отклонять или не отклонять) пакет отбрасывается вообще. Для того чтобы этого не происходило, и пакеты, не удовлетворяющие условиям, пересылались дальше оператор (команда) **access-list** должна содержать опцию permit с указанием в этой команде вместо конкретного IP-адреса исходного компьютера опции **any.**

Общий формат создания списка доступа (команды формирования списка доступа) имеет следующий вид:

access-list <номер_списка_доступа> < deny\ permit ><исходный адрес\ any> (маска_шаблона_исходного_адреса)

Параметр «*номер_списка_доступа*» - это целое число от 1 до 99. Если необходимо обозначить определенное количество адресов узлов в некоторой сети, пакеты от которых подвергаются фильтрации, необходимо добавить «*маску_шаблона_исходного_адреса*».

Пример создания списка доступа может выглядеть следующим образом:

access-list 1 deny 192.168.0.0 0.0.255.255
access-list 1 deny 192.161.0.0 0.0.15.255
access-list 1 permit any

Данный синтаксис создания списков доступа позволяет отклонять пакеты, приходящие от всех компьютеров сети 192.168.0.0 и от 2^{12} компьютеров, находящихся в сети 192.161.0.0. последняя команда **access-list 1** с опцией **permit any** означает, что все остальные пакеты должны быть пересланы по назначению.

Связывание того или иного списка доступа с определенным интерфейсом осуществляется с использованием команды

ip access-group <номер_списка_доступа> [in\out],

которую администратору необходимо ввести после задания номера интерфейса маршрутизатора в команде interface.

Таким образом, протокол настройки интерфейса маршрутизатора на блокировании пакетов, поступающих от определенных сетей, выглядит следующим образом:

conf t
access-list 1 deny 192.168.0.0 0.0.255.255
access-list 1 deny 192.161.0.0 0.0.15.255
access-list 1 permit any
interface s0/0
ip access-group 1 in
^z

В данном случае будут отфильтровываться все пакеты, поступающие на интерфейс s0/0 от указанных сетей.

В отличие от стандартных списков доступа расширенные списки доступа позволяют выполнять отбор не только по исходным IP-адресам, но и по протоколам (в частности, протоколам маршрутизации) и по целевым адресам. Т.е. расширенные списки доступа позволяют осуществлять отбор по более широкому набору критериев. Каждый интерфейс может иметь две группы доступа (**access-group**): одну для входящих пакетов и одну для исходящих пакетов. Наибольшее различие между стандартными и расширенными списками доступа заключается в их синтаксической структуре. Синтаксис настройки расширенных списков доступа следующий:

access-list<номер_списка_доступа> [deny\permit] <протокол> <исходный_адрес маска_шаблона_исходного_адреса | any> <целевой_адрес маска_шаблона_целевого_адреса | any > [опции_протокола], где:

«*Номер_списка_доступа*» - целое число в диапазоне от 100 до 199;

deny\permit – условие, действующее для данной строки списка доступа;

Протокол – указание определенного протокола (возможные варианты: EIGRP, ICMP, IGRP, IP, OSPF, TCP и UDP);

Исходный_адрес маска_шаблона_исходного_адреса – IP-адрес сети и маска шаблона, определяющая диапазон адресов компьютеров, по которым осуществляется фильтрация (ключевое слово any обозначает любой исходный IP-адрес);

Целевой_адрес маски_шаблона_целевого_адреса – интерпретируется по аналогии с настройками для исходного адреса;

В качестве *опций_протокола* задается опция log, которая включает режим протоколирования для списка доступа.

В рамках данной лабораторной работы изучается только применение списков доступа для оптимизации распространения таблиц маршрутизации, т.е для фильтрации пакетов протоколов маршрутизации.

Если список доступа предназначен для того, чтобы определенные виды транспорта не передавались по сети, его (список) следует разместить как можно ближе к источнику нежелательного трафика (т.е. не передавать пакеты по магистрали только затем, чтобы в конце концов их выбросить).

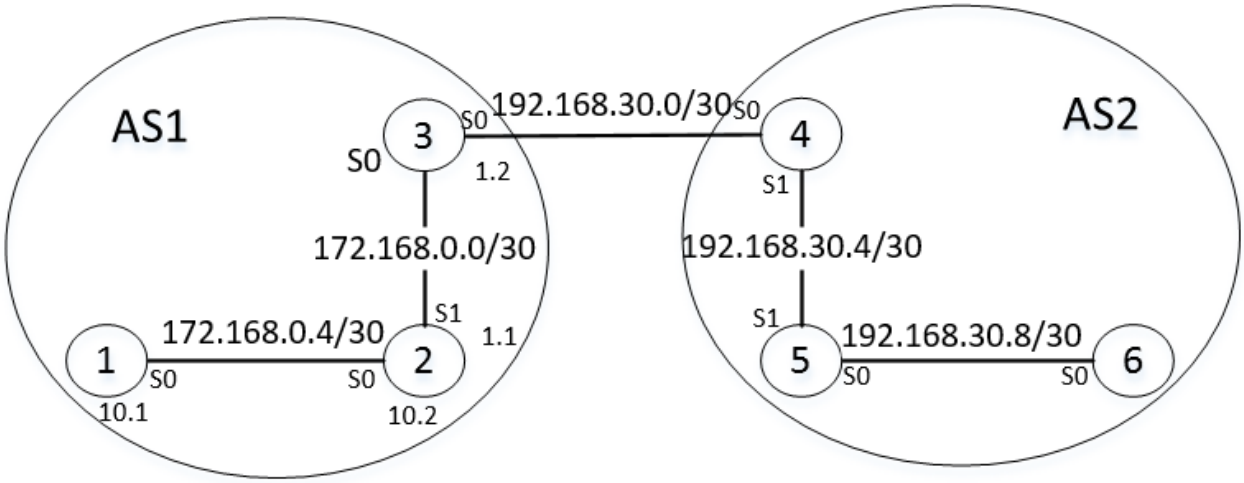


Рисунок 2.1 – Конфигурация объединенной сети с автономными областями

Например, если необходимо запретить рассылку таблиц маршрутизации между маршрутизаторами внутри автономных систем (рисунок 1) необходимо настроить списки таким образом, чтобы ограничивать рассылку пакетов на каждом входе каждого маршрутизатора. Для этого может быть использована опция **out** в команде **ip access-group**.

В том же случае, если необходимо разрешить рассылку пакетов маршрутизации внутри автономных систем, но запретить обмен изменениями в таблицах между автономными системами, возможно связать список доступа, запрещающий прием пакетов, с входами S1 маршрутизаторов 2 и 4, использовав при этом опцию **in** команды **ip access-group**.

Ориентированный протокол настройки маршрутизатора (например, маршрутизатора 5 в AS2) при запрете рассылки таблиц по AS2 будет выглядеть следующим образом:

```
en
conf t
```

```
access-list 1 deny eigrp 191.26.0.0 | 0.0.255.255 any
interface S0/0
ip access-group 1 out
access-list 2 deny eigrp 168.12.0.0 | 0.0.255.255 any
interface S1/0
ip access-group 2 out
^z
```

В данном случае сетевой IP-адрес (исходный адрес) 191.26.0.0 принадлежит интерфейсу S0/0 маршрутизатора 5 (выходной интерфейс при рассылке пакетов обновлений таблиц). Исходный адрес 168.12.0.0 (выходной адрес при рассылке пакетов с таблицами маршрутизации) принадлежит интерфейсу S1/0 маршрутизатора 5.

Ориентировочный протокол настройки списка доступа на маршрутизаторе 4 в AS2 (интерфейс S0/0-целевой интерфейс для принимаемых пакетов маршрутизации), запрещающий пересылку пакетов с изменениями в таблицах маршрутизации, выглядит следующим образом (маршрутизатор 4 – граничный маршрутизатор):

```
enable
conf t
access-list 1 deny eigrp any 168.22.0.0 0.0.255.255
int S0/0
ip access-group 1 in
^z
```

3. Методика выполнения работы

В качестве структуры сети, исследуемой в данной лабораторной работе, при формировании списков доступа используется сеть, представленная во второй части задания к лабораторной работе № 2 (структура сети выбирается в соответствии с вариантом).

Необходимо реализовать следующие пункты задания:

3.1. Запретить пересылку пакетов между маршрутизаторами 1,3 и маршрутизаторами 2,4. Друг с другом (1 с 3 и 2 с 4) маршрутизаторы обмениваются пакетами могут. Используя команду PING проконтролировать правильное функционирование списков доступа (проконтролировать, действительно ли посланные пакеты отклоняются, а не пересылаются в соответствующую сеть), настроенных соответственно на маршрутизаторах 1 и 3, 2 и 4.

3.2. Отменить использование списков доступа на маршрутизаторах 1 и 3, 2 и 4. Проконтролировать возможность пересылки пакетов между маршрутизаторами с использованием команды PING.

3.3. Настроить на каждом из маршрутизаторов расширенные списки доступа таким образом, чтобы запретить рассылку обновлений таблиц маршрутизации протокола EIGRP. Используя команду shutdown, отключить интерфейсы S0 на маршрутизаторах 3 и 4. Проконтролировать таблицы маршрутизации на

маршрутизаторах 1 и 2, выяснить, что эти таблицы остались в прежнем состоянии.

3.4. Отменить действие расширенных списков доступа для рассылки сообщений протокола EIGRP. Проконтролировать изменение таблиц на маршрутизаторах 1 и 2, связанные с отключением интерфейсов S0 на маршрутизаторах 3 и 4. также проконтролировать изменение таблиц на маршрутизаторах 6 и 8.

3.5. Настроить на маршрутизаторах 1 и 2 списки доступа таким образом, чтобы они обменивались таблицами с маршрутизаторами 3 и 4, но не распространяли изменения в таблицах в другие автономные системы (запретить рассылку пакетов EIGRP через интерфейсы S0 на маршрутизаторах 1 и 2). Подключить интерфейсы S0 маршрутизаторов 3 и 4.Проконтролировать изменение таблиц на маршрутизаторах 1 и 2. Проконтролировать правильность функционирования списков доступа, убедившись в неизменности таблиц на маршрутизаторах 6 и 8.

3.6. Отключить списки доступа на интерфейсах S0 маршрутизаторов 1 и 2, убедится в изменении таблиц на маршрутизаторах 6 и 8.

3.7. Настроить распространение таблиц маршрутизации от маршрутизатора 3 к сети, образованной маршрутизаторами:

Вариант 1 4 и 2;

Вариант 2 1 и 4.

4. Содержание отчета

4.1 Цель работы.

4.2 Формулировка пунктов задания, распечатка протоколов реализации команд по выполнению пунктов задания. Распечатка служебной информации IOS Cisco, которая позволяет контролировать действительное выполнение пунктов задания.

4.3 Выводы.

5. Контрольные вопросы

5.1. В чем состоит отличие стандартных и расширенных списков доступа?

5.2. В чем состоит назначение списков доступа?

5.3. Какими командами реализуется настройка списков доступа?

5.4. На каких уровнях эталонной модели функционируют стандартные и расширенные списки доступа и какой они при этом имеют формат?

5.5. Каким образом должен быть задан список доступа, чтобы он обеспечивал фильтрацию пользовательских пакетов (только пакетов пользователей) из локальной сети?

5.6. Каким образом должен быть задан список доступа, чтобы он обеспечивал фильтрацию таблиц маршрутизации от соседнего маршрутизатора?

5.7. Как выполняется привязка списка доступа к маршрутизатору?

ЛАБОРАТОРНАЯ РАБОТА №6

Исследование технологии преобразования адресов в объединенных сетях (технология NAT).

1.Цель работы: Исследование способов маршрутизации с использованием трансляции адресов.

2.Теоретическое введение

NAT (от англ. Network Address Translation — «преобразование сетевых адресов») — это механизм в сетях TCP/IP, позволяющий преобразовывать IP-адреса транзитных пакетов. Также имеет названия IP Masquerading, Network Masquerading и Native Address Translation.

Функционирование:

Преобразование адресов методом NAT может производиться почти любым маршрутизирующим устройством — маршрутизатором, сервером доступа, межсетевым экраном. Суть механизма состоит в замене адреса источника (source) при прохождении пакета в одну сторону и обратной замене адреса назначения (destination) в ответном пакете. Наряду с адресами source/destination могут также заменяться номера портов source/destination.

Помимо source NAT (предоставления пользователям локальной сети с внутренними адресами доступа к сети Интернет) часто применяется также destination NAT, когда обращения извне транслируются межсетевым экраном на сервер в локальной сети, имеющий внутренний адрес и потому недоступный извне сети непосредственно (без NAT).

Существует 3 базовых концепции трансляции адресов: статическая (Static Network Address Translation), динамическая (Dynamic Address Translation), маскарадная (NAPT, PAT).

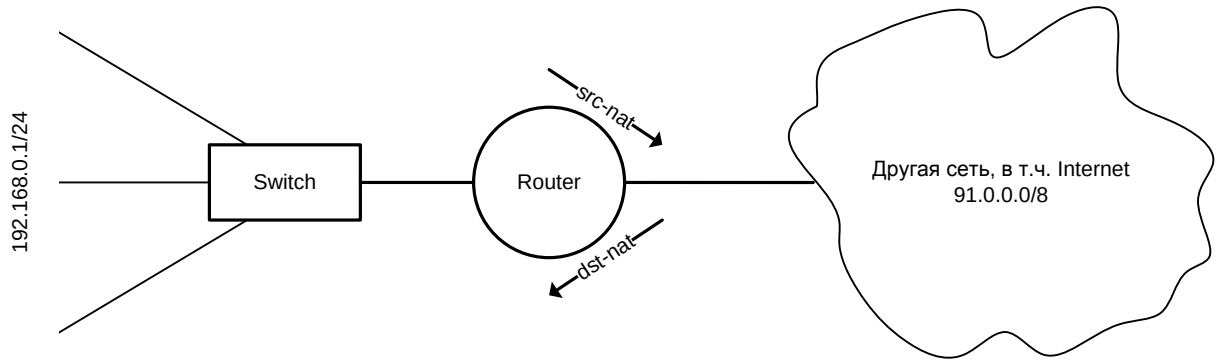


Рисунок 2.1 – Трансляция адресов локальной сети в глобальные адреса с использованием концепции SNAT

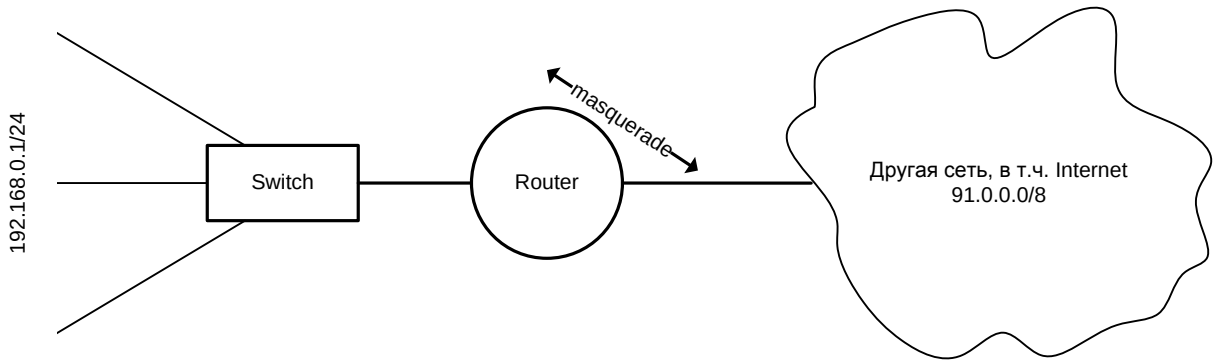


Рисунок 2.2 – Трансляция адресов локальной сети в глобальные адреса с использование концепции MASQUERADE

Преимущества:

NAT выполняет две важных функции.

Позволяет сэкономить IP-адреса, транслируя несколько внутренних IP-адресов в один внешний публичный IP-адрес (или в несколько, но меньшим количеством, чем внутренних).

Позволяет предотвратить или ограничить обращение снаружи ко внутренним хостам, оставляя возможность обращения изнутри наружу. При инициации соединения изнутри сети создаётся трансляция. Ответные пакеты, поступающие снаружи, соответствуют созданной трансляции и поэтому пропускаются. Если для пакетов, поступающих снаружи, соответствующей трансляции не существует (а она может быть созданной при инициации соединения или статической), они не пропускаются.

Недостатки:

Не все протоколы могут «преодолеть» NAT. Некоторые не в состоянии работать, если на пути между взаимодействующими хостами есть трансляция адресов. Некоторые межсетевые экраны, осуществляющие трансляцию IP-адресов, могут исправить этот недостаток, соответствующим образом заменяя IP-адреса не только в заголовках IP, но и на более высоких уровнях (например, в командах протокола FTP).

Из-за трансляции адресов «много в один» появляются дополнительные сложности с идентификацией пользователей и необходимость хранить полные логи трансляций.

DoS со стороны узла, осуществляющего NAT — если NAT используется для подключения многих пользователей к одному и тому же сервису, это может вызвать иллюзию DoS атаки на сервис (множество успешных и неуспешных попыток). Например, избыточное количество пользователей ICQ за NAT’ом приводит к проблеме подключения некоторых пользователей из-за превышения допустимой скорости коннектов к серверу. Частичным решением проблемы является использование пула адресов (группы адресов), для которых осуществляется трансляция.

Сложности в работе с пиринговыми сетями, в которых необходимо не только инициировать исходящие соединения, но также принимать входящие.

Существует несколько типов NAT.

1. Static NAT — статический NAT задает однозначное соответствие одного адреса другому. Иными словами, при прохождении через маршрутизатор, адрес(а) меняются на строго заданный адрес, один-к-одному. (к примеру 10.1.1.1 всегда заменяется на 11.1.1.1 и обратно, но никогда на 12.1.1.1). Запись о такой трансляции хранится неограниченно долго, пока есть строчка в конфиге.

2. Dynamic NAT — при прохождении через маршрутизатор, новый адрес выбирается динамически из некоторого куска адресов, называемого пулом (англ. pool). Запись о трансляции хранится некоторое время, чтобы ответные пакеты могли быть доставлены адресату. Если в течение некоторого времени трафик по этой трансляции отсутствует, трансляция удаляется и адрес возвращается в пул. Если требуется создать трансляцию, а свободных адресов в пуле нет, то пакет отбрасывается. Иными словами, хорошо бы, чтобы число внутренних адресов было ненамного больше числа адресов в пуле, иначе высока вероятность проблем с доступом наружу.

Примеры:

Задание: Имеется две сети, объединенные двумя маршрутизаторами. IP адреса первой сети 192.168.0.0/24, второй – 192.168.1.0/24. Произвести настройку маршрутизации используя dst-nat и src-nat, чтобы был возможен доступ из одной сети в другую. Для глобальной сети использовать адреса 172.18.16.0/30. Использовать Маршрутизаторы Cisco 2505. Выбор Коммутаторов произвести самостоятельно.

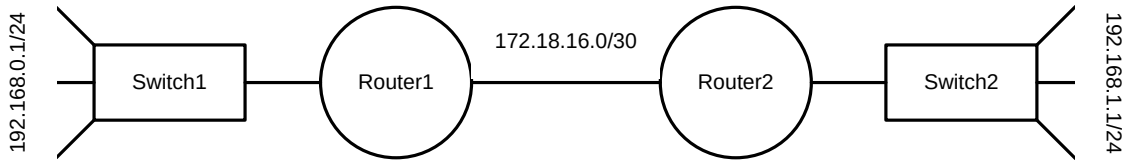


Рисунок 2.3 – Статический режим функционирования NAT

Создадим в Cisco Packet Tracer, данную топологию и выполним конфигурирование роутера 1. Конфигурировать будем динамический NAT.

Router>enable	Установка привилегированного режима
Router#configure terminal	Переход в режим конфигурирования
Router#hostname router1	Задание имени хоста
Router(config)#interface Ethernet0/0	Переход к конфигурированию интерфейса Ethernet 0/0

Router(config-if)#ip address 192.168.0.1 255.255.255.0	Установка адреса 192.168.0.1 с маской 255.255.255.0
Router(config-if)#ip nat inside	Сообщить роутеру, что данный интерфейс для локальной сети
Router(config-if)#no shutdown	Запуск интерфейса
Router(config-if)#exit	Выход из конфигурирования интерфейса
Router(config)#interface Serial2/0	Конфигурирование интерфейса Serial 0, посредством которого происходит доступ к глобальной сети
Router(config-if)#ip address 172.18.16.1 255.255.255.252	Задание IP адреса и маски по условию
Router(config-if)#no shutdown	Запуск интерфейса
Router(config-if)#exit	Выход
Router(config)#ip nat pool Net171 11.1.1.10 11.1.1.20 netmask 255.255.255.0	Создаем пул из адресов, указывая стартовый и конечный адрес
Router(config)#access-list 1 permit 192.168.0.0 0.0.0.255	Добавление списка доступа для локальных хостов
Router(config)# ip nat inside source list 1 pool Net171	Установка трансляции адресов из локальной сети в глобальную
Router(config)# ip nat outside source list 1 pool Net171	Установка трансляции адресов из глобальной сети в локальную
Router(config)#router rip	Переход в режим редактирования протокола RIP
Router(config-router)#network 192.168.0.0	Задание сетей для протокола RIP (внутренняя сеть)
Router(config-router)#network 172.18.16.0	Задание сетей для протокола RIP (внешняя сеть)
Router(config)#ip nat translations	Вывод списка трансляций

Таким же образом выполняется конфигурирование второго роутера.

Конфигурирование рабочих станций: станциям назначаются адреса из подсетей, которым они принадлежат, затем проверяется связь между рабочими станциями одной сети и другой.

Нередки ситуации, когда внутри корпоративной сети есть сервер, доступ которому извне по статическому внешнему адресу жизненно необходим. В таком случае, можно выставить его прямиком в Интернет, назначив глобальный адрес. Но часто это не очень удобно, например, по соображениям безопасности. И в таких случаях нам на помощь приходит статический NAT.

Он создает двустороннюю и постоянную трансляцию. Так что наш хост всегда будет доступен по одному внешнему адресу и эта трансляция никогда не вылетит из таблицы трансляций по таймауту. Трансляцию создаем следующей командой:

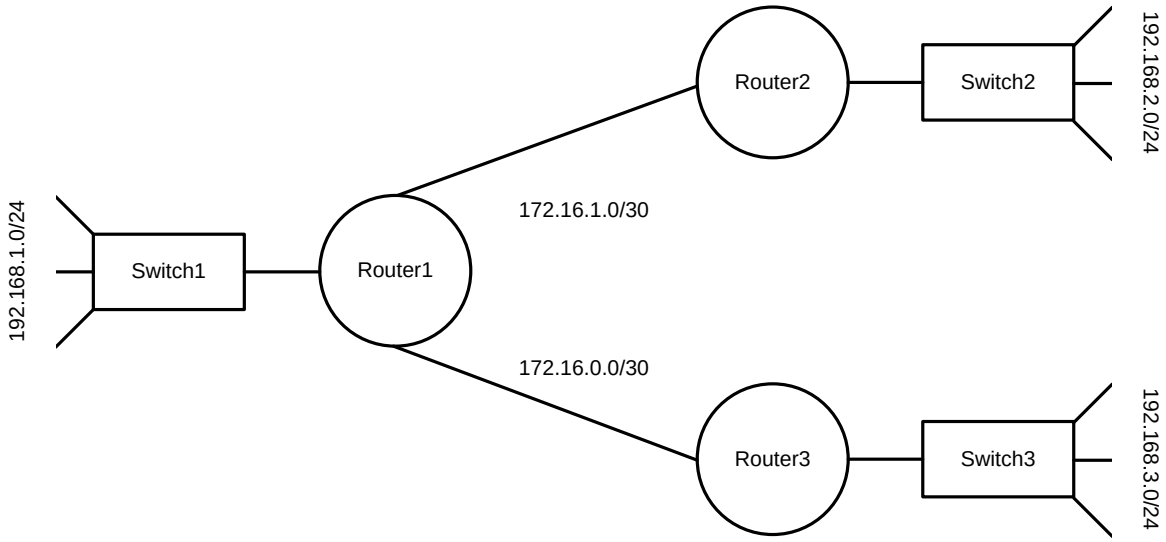
ip nat inside source static 192.168.1.0 11.1.1.21

3. ПРОГРАММА РАБОТЫ

Задание выбирается в соответствии с вариантом, назначаемым преподавателем.

Смоделировать схему в Cisco Packet Tracer.

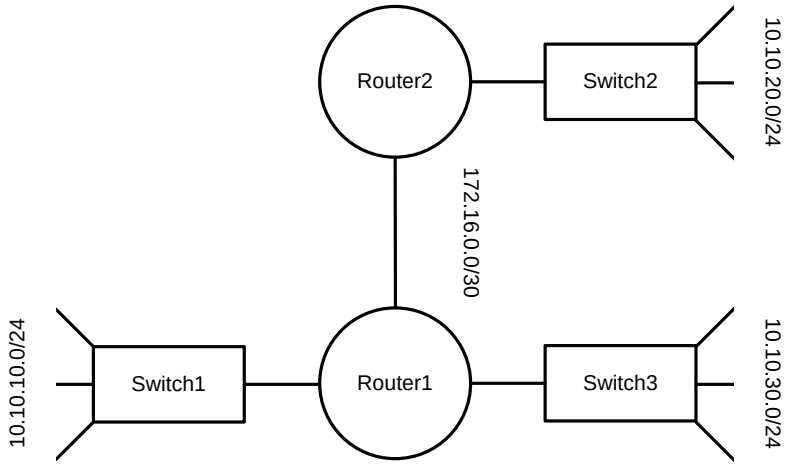
1 Вариант.



Магистраль между Router1 и Router2 основана на Serial интерфейсе. Сконфигурировать NAT на данной магистрали в статическом режиме работы.

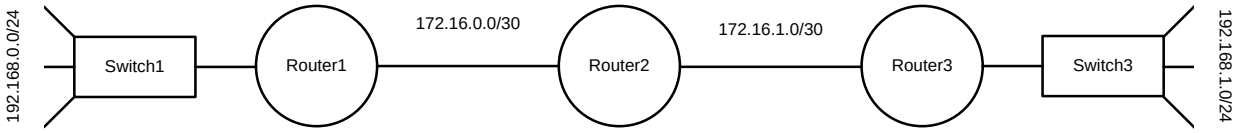
Магистраль между Router1 и Router3 основана на Ethernet. Конфигурирование NAT выполнить по схеме с использованием списков доступа.

2 Вариант.



Магистраль между Router1 и Router2 основана на Serial интерфейсе. Конфигурацию NAT для сетей 10.10.10.0/24 и 10.10.30.0/24 выполнить на основе статической схемы, конфигурирование NAT между маршрутизаторами выполнить на основе списков доступа.

3 Вариант.



Магистраль между Router1 и Router2 основана на Ethernet интерфейсе, магистраль Router2, Router3 – на Serial интерфейсе.

Выполнить конфигурирование NAT в статическом режиме для сетей 172.16.0.0/24 и 172.16.1.0/30. Конфигурирование NAT для внутренних сетей произвести по схеме со списками доступа.

4. Контрольные вопросы

4.1. В чем состоит назначение технологии NAT при функционировании сети?

4.2. В чем состоят отличия режимов функционирования NAT?

4.3. Какие режимы конфигурирования маршрутизаторов позволяют использовать NAT для трансляции адресов?

4.4. Какой порядок выполнения команд при конфигурировании NAT в статическом режиме?

4.5. Какой порядок выполнения команд при конфигурировании NAT с использованием списков доступа?

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1.Леммл Т., Портер Д. CCNA: Cisco Certified Network Associate. Учебное руководство. – М.: Издательство “Лори”, 2000. – 615 с.

2.Леинванд А., Пински Б. Конфигурирование маршрутизаторов Cisco. – М.: Издательство “Вильямс”, 2001. – 360 с.

3. Леммл Т. Настройка маршрутизаторов Cisco. – М.: Издательство “Лори”, 2001. - 33 с.

4. Пасет К., Тир Д. Создание масштабируемых сетей Cisco, - М.: Издательство ”Вильямс”, 2002. – 787 с.

5. Хелеби С., Мас – Ферсон Д. Принципы маршрутизации в Internet. – М.: Издательство “Вильямс”, 2001. – 445 с.