

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ДОНСКОЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

Кафедра «Вычислительные системы и информационная безопасность»

**МЕТОДИЧЕСКИЕ УКАЗАНИЯ
ДЛЯ ВЫПОЛНЕНИЯ КОНТРОЛЬНОЙ РАБОТЫ
ПО ДИСЦИПЛИНЕ «АДМИНИСТРИРОВАНИЕ
ИНФОРМАЦИОННЫХ СИСТЕМ»**

Ростов-на-Дону
ДГТУ
2022

ВВЕДЕНИЕ

Под глобальной компьютерной сетью обычно понимают большую по размерам и территориально распределенную компьютерную сеть, которая обеспечивает функционирование множества сетевых сервисов для нужд большого количества пользователей, структурно состоящую из локальных компьютерных сетей, которые соединены между собой непосредственно или через инфраструктуру других телекоммуникационных провайдеров.

При решении задачи защиты информации в глобальной компьютерной сети на первом этапе необходимо составить релевантную модель угроз безопасности информации, определив актуальные угрозы для конкретного объекта защиты. При этом учитываются структурные и функциональные характеристики, присущие именно глобальным компьютерным сетям, например, - территориальная распределенность, большое количество пользователей и устройств, передача трафика через неконтролируемые компьютерные сети, применяемые сетевые технологии и некоторые другие характеристики.

В соответствии с определенными угрозами внедряются меры и средства защиты информации, которые рассматриваются в настоящем практикуме далее.

ВАРИАНТЫ ЗАДАНИЙ

Практические работы выполняются по **вариантам**: значения некоторых настраиваемых в заданиях параметров зависят от номера варианта.

Так, обозначение [N] в тексте задания означает, что при его выполнении данное обозначение должно быть заменено на две **последние цифры из номера зачетной книжки**.

Например, IP-адрес вида 192.168.[N].1 при номере зачетной книжки ...12 должен быть задан как 192.168.12.1, а IP-адрес вида 192.168.[N+3].1 должен быть задан, соответственно, как 192.168.15.1.

ПРАКТИЧЕСКАЯ РАБОТА № 1 СТАТИЧЕСКАЯ МАРШРУТИЗАЦИЯ

Цель работы

Изучить принципы организации и настройку статической маршрутизации между локальными сетями.

Теоретические сведения

1. Настраиваем статическую маршрутизацию на cisco router // Блог Go-to-EasyIt.com URL: <http://www.go-to-easyit.com/2011/05/cisco-router.html> (дата обращения: 20.05.2021).
-

2. Маршруты по умолчанию и их настройка // Лаборатория сетей CiscoLAB. URL: <http://www.ciscolab.ru/routing/7-nastroyka-marshrutov-po-umolchaniyu-ispolzuya-ip-komandy.html> (дата обращения: 20.05.2021).

Порядок выполнения работы

1. Подготовка схемы сети

- а. Соберите модель сети в соответствии со схемой на рисунке:

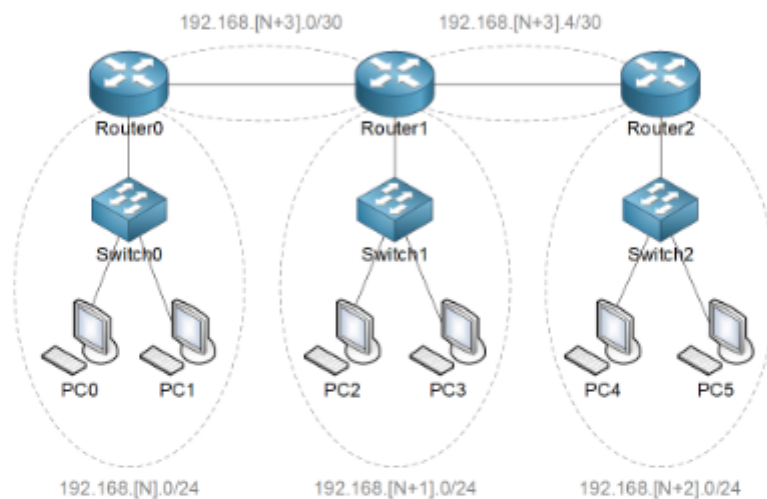


Схема модели сети

- б. На маршрутизаторах Router0 – Router2 с помощью команд вида
Router(config)#interface [тип] [номер]
Router(config-if)#ip address [IP-адрес] [маска]
Router(config-if)#no shutdown
назначьте интерфейсам IP-адреса из диапазонов IP-адресов подсетей в соответствии со схемой сети и включите их.
- с. Компьютерам PC0 – PC5 назначьте IP-адреса из диапазонов IP-адресов подсетей в соответствии со схемой сети.
- д. На компьютерах PC0 – PC5 установите в качестве шлюза по умолчанию (Default gateway) IP-адреса интерфейсов соответствующих маршрутизаторов Router0 – Router2.
- е. На маршрутизаторах Router0 – Router2, коммутаторах Switch0 – Switch2 и компьютерах PC0 – PC5 получите информацию о MAC-адресах и(или) IP-адресах активных интерфейсов, проанализируйте ее и **запишите в отчет** в виде таблицы со столбцами «Название устройства | Тип и номер интерфейса | MAC-адрес интерфейса | IP-адрес интерфейса».

2. Настройка статической маршрутизации

a. Проанализируйте топологию сети и в соответствии с количеством подсетей и их назначением составьте и **запишите в отчет** список маршрутов для маршрутизаторов Router0 – Router2, обеспечивающих доступность всех подсетей и узлов, в виде таблицы со столбцами «Название устройства | IP-адрес сети назначения | Маска сети назначения | Тип и номер интерфейса для отправки | IP-адрес для отправки».

b. На маршрутизаторах Router0 – Router2 с помощью команд вида
Router(config)#ip route [IP-адрес] [маска] [IP-адрес] или
Router(config)#ip route [IP-адрес] [маска] [тип интерфейса] [номер интерфейса]

c. На компьютерах PC0 – PC5, используя утилиту «Command Prompt», с помощью команды вида

PC>ping [IP-адрес]

проверьте доступность всех узлов внутри всех подсетей

d. На маршрутизаторах Router0 – Router2 с помощью команды

#show ip route

получите информацию о таблицах маршрутизации, проанализируйте ее и **запишите в отчет**.

Контрольные вопросы

1. Что такое маршрутизация?
2. Какие преимущества и недостатки у статической маршрутизации?
3. Какая структура у таблицы маршрутизации, как она формируется?
4. Какие источники и типы записей в таблице маршрутизации существуют, какой у них приоритет?
5. Что такое административное расстояние (дистанция) маршрута и какие значения оно (она) может принимать?
6. Что такое шлюз по умолчанию, с какой целью он задается?
7. Что такое маршрут по умолчанию, с какой целью он задается на маршрутизаторе?
8. Какие существуют способы задания маршрута по умолчанию на маршрутизаторе, в чем их отличия?

ПРАКТИЧЕСКАЯ РАБОТА № 2

RIP

Цель работы

Изучить настройку динамической маршрутизации с помощью дистанционно-векторного протокола RIP (англ. Routing Information Protocol, протокол маршрутной информации).

Теоретические сведения

1. Маршрутизация в Cisco // Точка обмена знаниями по UNIX/Linux-системам и системам с открытым исходным кодом URL: http://xgu.ru/wiki/Маршрутизация_в_Cisco (дата обращения: 20.05.2021).
2. RIP // Точка обмена знаниями по UNIX/Linux-системам и системам с открытым исходным кодом. URL: <http://xgu.ru/wiki/RIP> (дата обращения: 20.05.2021).
3. Configuring RIP // Сайт компании Cisco Systems. URL: http://www.cisco.com/c/en/us/td/docs/security/asa/asa82/configuration/guide/config/route_rip.html (дата обращения: 20.05.2021).

Порядок выполнения работы

1. Подготовка схемы сети

- а. Соберите модель сети в соответствии со схемой на рисунке:

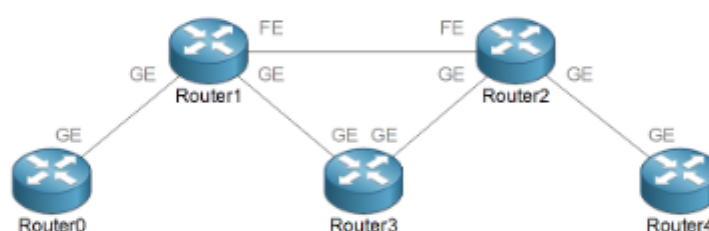


Схема модели сети

где GE – Gigabit Ethernet, FE – Fast Ethernet.

- б. На маршрутизаторах Router0 – Router4 с помощью команд вида
Router(config)#interface [тип] [номер]
Router(config-if)#ip address [IP-адрес] [маска]
Router(config-if)#no shutdown

назначьте интерфейсам IP-адреса из диапазонов IP-адресов подсетей с маской /24, полученных путем распределения одного диапазона IP-адресов вида 192.[N].0.0/18 на все требуемые подсети, и включите их.

- в. На маршрутизаторах Router0 и Router4 с помощью команд вида
Router(config)#interface loopback [номер]
Router(config-if)#ip address [IP-адрес] [маска]
создайте виртуальные loopback-интерфейсы, моделирующие подсети, подключенные к маршрутизаторам, и назначьте им IP-адреса из диапазонов IP-адресов вида 192.168.[N].0/24 и 192.168.[N+1].0/24 соответственно.

- д. На маршрутизаторах Router0 – Router4 получите информацию о MAC-адресах и IP-адресах активных интерфейсов (в том числе loopback-

интерфейсов), проанализируйте ее и запишите в отчет в виде таблицы со столбцами «Название устройства | Тип и номер интерфейса | MAC-адрес интерфейса | IP-адрес интерфейса».

2. Настройка динамической маршрутизации с помощью протокола RIP

a. На маршрутизаторах Router0 – Router4 с помощью команд

```
Router(config)#router rip
Router(config-router)#version 2
```

активируйте вторую версию протокола RIP.

Если при выполнении последующих заданий в таблице маршрутизации не появляются маршруты, информация о которых должна распространяться по протоколу RIP, то целесообразно перейти на первую версию протокола RIP.

b. На маршрутизаторах Router0 – Router4 с помощью команд вида

```
Router(config)#router rip
Router(config-router)#network [IP-адрес]
Router(config-router)#no auto-summary
```

активируйте маршрутизацию по протоколу RIP для соответствующих IP-адресов подсетей и отключите автосуммирование IP-адресов на границе маршрутизации.

c. На маршрутизаторах Router0 – Router4 с помощью команды

```
Router#show ip rip database
```

получите информацию об анонсируемых по протоколу RIP IP-адресах подсетей и проанализируйте ее.

d. На маршрутизаторах Router0 и Router4 с помощью команд вида

```
Router#ping
...
Target IP address: [IP-адрес]
...
Extended commands [n]: y
Source address or interface: [IP-адрес]
...
```

проверьте доступность узлов подсетей, смоделированных соответствующими виртуальными loopback-интерфейсами маршрутизаторов, между собой.

e. На маршрутизаторах Router0 – Router4 с помощью команды

```
Router#show ip protocols
```

проверьте настройки протокола RIP и проанализируйте их.

f. На маршрутизаторах Router0 – Router4 с помощью команды

```
Router#show ip route
```

получите информацию о таблицах маршрутизации, проанализируйте ее и **запишите в отчет.**

g. На маршрутизаторах Router0 и Router4 с помощью команд вида

```
Router#traceroute
...
Target IP address: [IP-адрес]
Source address: [IP-адрес]
...
```


получите информацию о маршруте сетевых пакетов между узлами подсетей, смоделированных соответствующими виртуальными loopback-интерфейсами маршрутизаторов.

h. На маршрутизаторе Router0 с помощью команд вида
Router#ping

```
...
Target IP address: [IP-адрес]
Repeat count [5]: 100
...
Extended commands [n]: y
Source address or interface: [IP-адрес]
...
```

запустите длительную проверку доступности подсети, смоделированной виртуальным loopback-интерфейсом маршрутизатора Router4, из подсети, смоделированной виртуальным loopback-интерфейсом маршрутизатора Router0.

i. Не дожидаясь отправки всех ICMP-запросов, на маршрутизаторе Router1 с помощью команд вида

```
Router(config)#interface [тип] [номер]
Router(config-if)#shutdown
```

выключите интерфейс, соединяющий его с маршрутизатором Router2.

j. Проанализируйте и **запишите в отчет** результаты проверки доступности подсети, смоделированной виртуальным loopback-интерфейсом маршрутизатора Router4, и по количеству недоставленных ICMP-запросов вычислите и **запишите в отчет** примерное время, за которое протокол RIP формирует новый маршрут.

3. Настройка «плавающего» статического маршрута

a. На маршрутизаторах Router1 и Router2 с помощью команд вида

```
Router(config)#router rip
Router(config-router)#no network [IP-адрес]
```

отключите маршрутизацию по протоколу RIP для соответствующих IP-адресов подсетей.

b. На маршрутизаторах Router1 и Router2 с помощью команд вида
Router(config)#ip route [IP-адрес] [маска] [IP-адрес] [административное расстояние]

создайте «плавающие» статические маршруты до сетей, смоделированных виртуальными loopback-интерфейсами маршрутизаторов Router0 и Router4, за счет задания для статических маршрутов значения административного расстояния, превышающего значение административного расстояния для маршрутов, сформированных протоколом RIP.

c. На маршрутизаторах Router1 и Router2 с помощью команд вида

```
Router(config)#router rip
Router(config-router)#redistribute static
```

активируйте распространение с помощью протокола RIP информации о статических маршрутах.

d. На маршрутизаторах Router0 – Router4 с помощью команды

```
Router#show ip route
```

получите информацию о таблицах маршрутизации, проанализируйте ее и убедитесь в том, что в ней отсутствует статический маршрут.

е. На маршрутизаторах Router0 и Router4 с помощью команд вида Router#traceroute

```
...
Target IP address: [IP-адрес]
Source address: [IP-адрес]
...
```

получите информацию о маршруте сетевых пакетов из подсети, смоделированной виртуальным loopback-интерфейсом маршрутизатора Router0, до подсети, смоделированной виртуальным loopback-интерфейсом маршрутизатора Router4, и наоборот, проанализируйте ее и убедитесь в том, что сетевые пакеты передаются через маршрутизатор Router3.

ф. На маршрутизаторе Router3 с помощью команд вида

```
Router(config)#interface [тип] [номер]
Router(config-if)#shutdown
```

отключите интерфейсы, соединяющие его с маршрутизаторами Router1 и Router2.

г. На маршрутизаторах Router0 и Router4 с помощью команд вида Router#ping

```
...
Target IP address: [IP-адрес]
...
Extended commands [n]: y
Source address or interface: [IP-адрес]
...
```

проверьте доступность подсети, смоделированной виртуальным loopback-интерфейсом маршрутизатора Router4, из подсети, смоделированной виртуальным loopback-интерфейсом маршрутизатора Router0, и наоборот.

h. На маршрутизаторах Router0 и Router4 с помощью команды

```
Router#show ip route
```

получите информацию о таблицах маршрутизации, проанализируйте ее и **запишите в отчет**.

i. На маршрутизаторах Router0 и Router4 с помощью команд вида

```
Router#traceroute
...
Target IP address: [IP-адрес]
Source address: [IP-адрес]
...
```

получите информацию о маршруте сетевых пакетов между узлами подсетей, смоделированных соответствующими виртуальными loopback-интерфейсами маршрутизаторов.

Контрольные вопросы

1. Какие этапы работы у дистанционно-векторных алгоритмов маршрутизации?
2. Какие особенности применения, достоинства и недостатки у дистанционно-векторных протоколов маршрутизации?
3. Что такое метрика маршрута, какими свойствами она должна обладать и что может использоваться в ее качестве?
4. Что такое административное расстояние (дистанция) маршрута и какие значения оно (она) может принимать?
5. В чем отличие первой и второй версий протокола RIP?
6. Как передаются классовые и бесклассовые IP-адреса в случае применения первой версии протокола RIP?
7. Как передаются классовые и бесклассовые IP-адреса в случае применения второй версии протокола RIP?
8. Какие таймеры использует в своей работе протокол RIP?
9. Как протокол RIP адаптируется к изменениям состояния сети?
10. Какие в протоколе RIP существуют методы борьбы с ложными маршрутами?
11. Что такое суммирование маршрутов и с какой целью оно применяется?
12. Что такое «плавающий» статический маршрут и с какой целью он создается?

ПРАКТИЧЕСКАЯ РАБОТА № 3 EIGRP

Цель работы

Изучить настройку динамической маршрутизации с помощью дистанционно-векторного протокола EIGRP (англ. Enhanced Interior Gateway Routing Protocol, усовершенствованный внутренний протокол маршрутизации шлюзов).

Теоретические сведения

1. Маршрутизация в Cisco // Точка обмена знаниями по UNIX/Linux-системам и системам с открытым исходным кодом. URL: http://xgu.ru/wiki/Маршрутизация_в_Cisco (дата обращения: 20.05.2021).
2. EIGRP // Точка обмена знаниями по UNIX/Linux-системам и системам с открытым исходным кодом. URL: <http://xgu.ru/wiki/EIGRP> (дата обращения: 20.05.2021).
3. Протокол EIGRP (усовершенствованный внутренний протокол маршрутизации шлюзов) // Сайт компании Cisco Systems. URL:

http://www.cisco.com/cisco/web/support/RU/9/92/92088_eigrp-toc.html (дата обращения: 20.05.2021).

4. Как работает распределение нагрузки с неравной стоимостью путей (вариация) в IGRP и EIGRP? // Сайт компании Cisco Systems. URL: http://www.cisco.com/cisco/web/support/RU/9/92/92116_19.html (дата обращения: 20.05.2021).

5. Настройка предпочтительного маршрута посредством воздействия на метрики протокола EIGRP // Сайт компании Cisco Systems. URL: http://www.cisco.com/cisco/web/support/RU/9/92/92199_14.html (дата обращения: 20.05.2021).

6. Пример конфигурации проверки подлинности сообщений EIGRP // Сайт компании Cisco Systems. URL: http://www.cisco.com/cisco/web/support/RU/104/1041/1041955_eigrp-authentication.pdf (дата обращения: 20.05.2021).

Порядок выполнения работы

1. Подготовка схемы сети

- а. Соберите модель сети в соответствии со схемой на рисунке:

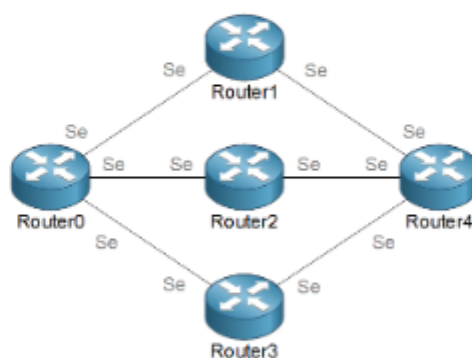


Схема модели сети

где Se – Serial.

- б. На маршрутизаторах Router0 – Router4 с помощью команд вида

```
Router(config)#interface [тип] [номер]
Router(config-if)#ip address [IP-адрес] [маска]
Router(config-if)#no shutdown
```

назначьте интерфейсам IP-адреса из диапазонов IP-адресов подсетей с маской /30, полученных путем распределения одного диапазона IP-адресов вида 192.168.[N].0/24 на все требуемые подсети, и включите их.

- с. На маршрутизаторах Router0 и Router4 с помощью команд вида

```
Router(config)#interface loopback [номер]
Router(config-if)#ip address [IP-адрес] [маска]
```

создайте виртуальные loopback-интерфейсы, моделирующие подсети, подключенные к маршрутизаторам, и назначьте им IP-адреса из диапазонов IP-адресов вида 192.168.[N+1].0/24 и 192.168.[N+2].0/24 соответственно.

d. На маршрутизаторах Router0 – Router4 получите информацию о MAC-адресах и IP-адресах активных интерфейсов (в том числе loopback-интерфейсов), проанализируйте ее и **запишите в отчет** в виде таблицы со столбцами «Название устройства | Тип и номер интерфейса | MAC-адрес интерфейса | IP-адрес интерфейса».

2. Настройка динамической маршрутизации с помощью протокола EIGRP

a. На маршрутизаторах Router0 – Router4 с помощью команд

```
Router(config)#router eigrp [номер автономной системы]
Router(config-router)#network [IP-адрес] [wildcard-маска]
Router(config-router)#no auto-summary
```

активируйте процесс динамической маршрутизации с помощью протокола EIGRP для автономной системы с указанным номером, активируйте протокол EIGRP на интерфейсах, IP-адреса которых входят в указанную подсеть, и отключите суммирование сетей на границе маршрутизации.

b. На маршрутизаторах Router0 и Router4 с помощью команд вида

```
Router#ping
...
Target IP address: [IP-адрес]
...
Extended commands [n]: y
Source address or interface: [IP-адрес]
...
```

проверьте доступность узлов подсетей, смоделированных соответствующими виртуальными loopback-интерфейсами маршрутизаторов, между собой.

c. На маршрутизаторах Router0 – Router4 с помощью команды

```
Router#show ip protocols
```

проверьте настройки протокола EIGRP и проанализируйте их.

d. На маршрутизаторах Router0 – Router4 с помощью команд вида

```
Router#show ip eigrp neighbors
```

получите информацию об отношениях смежности с соседними сетевыми устройствами и проанализируйте ее.

e. На маршрутизаторах Router0 – Router4 с помощью команд вида

```
Router#show ip eigrp topology
```

получите информацию о таблице топологии и проанализируйте ее.

f. На маршрутизаторах Router0 – Router4 с помощью команды

```
Router#show ip route
```

получите информацию о таблицах маршрутизации, проанализируйте ее и **запишите в отчет**.

г. В режиме симуляции, на маршрутизаторах Router0 и Router4 с помощью команд вида

```
Router#ping
...
Target IP address: [IP-адрес]
...
Extended commands [n]: y
Source address or interface: [IP-адрес]
...
```

проверьте доступность узлов подсетей, смоделированных соответствующими виртуальными loopback-интерфейсами маршрутизаторов, между собой и убедитесь в том, что для передачи сетевых пакетов в обе стороны используются различные маршруты.

3. Настройка метрик маршрутизации протокола EIGRP

а. На маршрутизаторах Router0 – Router4 с помощью команды вида Router#show interface [тип] [номер] получите информацию о состоянии интерфейсов, проанализируйте ее и **запишите в отчет** в виде таблицы со столбцами «Название устройства | Тип и номер интерфейса | Пропускная способность | Задержка».

б. Для маршрутизатора Router0 рассчитайте характеристики маршрутов до подсети, смоделированной виртуальным loopback-интерфейсом маршрутизатора Router4, проанализируйте их и **запишите в отчет** в виде таблицы со столбцами «Названия устройств, через которые проходит маршрут | Объявленное расстояние (Advertised Distance) | Возможное расстояние (Feasible Distance) | Выполнение критерия возможного состояния (Feasible Condition) | Статус маршрута | Статус соседнего устройства».

с. На маршрутизаторах Router0 и Router4 с помощью команд вида Router#traceroute

```
...
Target IP address: [IP-адрес]
Source address: [IP-адрес]
...
```

получите информацию о маршруте сетевых пакетов из подсети, смоделированной виртуальным loopback-интерфейсом маршрутизатора Router0, до подсети, смоделированной виртуальным loopback-интерфейсом маршрутизатора Router4, и наоборот и проанализируйте ее.

д. На маршрутизаторах Router0 – Router4 с помощью команд вида Router(config)#interface [тип] [номер]
Router(config-if)#bandwidth [значение]
Router(config-if)#delay [значение]
настройте параметры интерфейсов таким образом, чтобы от маршрутизатора Router0 до подсети, смоделированной виртуальным loopback-интерфейсом маршрутизатора Router4, был только один основной и один резервный маршрут.

е. На маршрутизаторах Router0 – Router4 с помощью команды вида Router#show interface [тип] [номер]

получите информацию о состоянии интерфейсов, проанализируйте ее и **запишите в отчет** в виде таблицы со столбцами «Название устройства | Тип и номер интерфейса | Пропускная способность | Задержка».

f. Для маршрутизатора Router0 рассчитайте характеристики маршрутов до подсети, смоделированной виртуальным loopback-интерфейсом маршрутизатора Router4, проанализируйте их и **запишите в отчет** в виде таблицы со столбцами «Названия устройств, через которые проходит маршрут | Объявленное расстояние (Advertised Distance) | Возможное расстояние (Feasible Distance) | Выполнение критерия возможного состояния (Feasible Condition) | Статус маршрута | Статус соседнего устройства»

g. На маршрутизаторах Router0 и Router4 с помощью команд вида Router#traceroute

```
...
Target IP address: [IP-адрес]
Source address: [IP-адрес]
...
```

получите информацию о маршруте сетевых пакетов из подсети, смоделированной виртуальным loopback-интерфейсом маршрутизатора Router0, до подсети, смоделированной виртуальным loopback-интерфейсом маршрутизатора Router4, и наоборот и проанализируйте ее.

h. На маршрутизаторах Router0 – Router4 с помощью команд вида Router#show ip eigrp topology

получите информацию о таблице топологии и проанализируйте ее.

i. На маршрутизаторах Router0 – Router4 с помощью команд вида Router#show ip eigrp topology all-links

получите информацию о полной таблице топологии и проанализируйте ее.

j. На маршрутизаторах Router0 – Router4 с помощью команды Router#show ip route

получите информацию о таблицах маршрутизации, проанализируйте ее и **запишите в отчет**.

4. Настройка аутентификации сетевых устройств в протоколе EIGRP

a. На маршрутизаторе Router0 с помощью команд вида

```
Router(config)#key chain [имя]
Router(config-keychain)#key [идентификатор]
Router(config-keychain-key)#key-string [строка]
```

создайте цепочку ключей, создайте ключ, задайте ему идентификатор и установите ключевую строку.

b. На маршрутизаторе Router0 с помощью команд вида

```
Router(config)#interface [тип] [номер]
Router(config-if)#ip authentication mode eigrp [номер] md5
Router(config-if)#ip authentication key-chain eigrp [номер] [имя]
```

активируйте на интерфейсе, соединяющим его с маршрутизатором Router1, аутентификацию сетевых устройств и установите цепочку ключей.

c. На маршрутизаторах Router0 и Router1 с помощью команд вида

Router#show ip eigrp neighbors

получите информацию об отношениях смежности с соседними сетевыми устройствами, проанализируйте ее и **запишите в отчет**.

д. На маршрутизаторе Router1 с помощью команд вида

Router(config)#key chain [имя]

Router(config-keychain)#key [идентификатор]

Router(config-keychain-key)#key-string [строка]

создайте цепочку ключей, создайте ключ, задайте ему идентификатор и установите ключевую строку, совпадающую с ключевой строкой, установленной в ключевой цепочке маршрутизатора Router0.

е. На маршрутизаторе Router1 с помощью команд вида

Router(config)#interface [тип] [номер]

Router(config-if)#ip authentication mode eigrp [номер] md5

Router(config-if)#ip authentication key-chain eigrp [номер] [имя]

активируйте на интерфейсе, соединяющим его с маршрутизатором Router0, аутентификацию сетевых устройств и установите цепочку ключей.

ф. На маршрутизаторах Router0 и Router1 с помощью команд вида

Router#show ip eigrp neighbors

получите информацию об отношениях смежности с соседними сетевыми устройствами, проанализируйте ее и **запишите в отчет**.

Контрольные вопросы

1. Что такое wildcard-маска, как она формируется и для чего применяется?
2. Какие особенности применения, достоинства и недостатки у протокола EIGRP?
3. Какие типы сообщений в своей работе использует протокол EIGRP?
4. Какие таблицы в своей работе использует протокол EIGRP, как они формируются?
5. Какие таймеры в своей работе использует протокол EIGRP?
6. Как протокол EIGRP вычисляет метрику маршрута?
7. Как в протоколе EIGRP происходит обновление маршрутов?
8. Как протокол EIGRP определяет основные и резервные маршруты?
9. Что такое расщепление горизонта и с какой целью оно применяется?
10. Что такое обратный запрет и с какой целью он применяется?
11. Что такое балансировка нагрузки и с какой целью она применяется?
12. Как в протоколе EIGRP происходит балансировка нагрузки между маршрутами с одинаковой метрикой?
13. Как в протоколе EIGRP происходит балансировка нагрузки между маршрутами с разной метрикой?
14. Что такое суммирование маршрутов и с какой целью оно применяется?

15. С какой целью в протоколе EIGRP применяется проверка подлинности сообщений (аутентификация сетевых устройств)?

16. Как в протоколе EIGRP реализована проверка подлинности сообщений (аутентификация сетевых устройств)?

ПРАКТИЧЕСКАЯ РАБОТА № 4

OSPF

Цель работы

Изучить настройку динамической маршрутизации в одной и нескольких областях с помощью протокола состояния каналов связи OSPF (англ. Open Shortest Path First, протокол маршрутизации с определением кратчайшего пути).

Теоретические сведения

1. OSPF // Точка обмена знаниями по UNIX/Linux-системам и системам с открытым исходным кодом. URL: <http://xgu.ru/wiki/OSPF> (дата обращения: 20.05.2021).

2. Руководство по проектированию OSPF // Сайт компании Cisco Systems. URL: http://www.cisco.com/cisco/web/support/RU/9/92/92027_1.html (дата обращения: 20.05.2021).

3. OSPF в Cisco // Точка обмена знаниями по UNIX/Linux-системам и системам с открытым исходным кодом. URL: http://xgu.ru/wiki/OSPF_в_Cisco (дата обращения: 20.05.2021).

4. Configuring OSPF Authentication on a Virtual Link // Сайт компании Cisco Systems. URL: <http://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/8313-27.html> (дата обращения: 20.05.2021).

Порядок выполнения работы

1. Подготовка схемы сети

- а. Соберите модель сети в соответствии со схемой на рис. 4.1:



Рис. 4.1. Схема модели сети

b. На маршрутизаторах Router0 – Router5 с помощью команд вида
Router(config)#interface loopback [номер]
Router(config-if)#ip address [IP-адрес] [маска]
создайте виртуальные loopback-интерфейсы и назначьте им IP-адреса для идентификации маршрутизаторов в процессе работы протокола OSPF.

c. На маршрутизаторах Router0 – Router2 назначьте интерфейсам, входящим согласно схеме сети в одну область, IP-адреса из диапазонов IP-адресов подсетей с маской /30, полученных путем распределения одного диапазона IP-адресов вида [N].1.0.0/24 на все подсети.

d. На маршрутизаторах Router3 – Router5 назначьте интерфейсам, входящим согласно схеме сети в одну область, IP-адреса из диапазонов IP-адресов подсетей с маской /30, полученных путем распределения одного диапазона IP-адресов вида [N].2.0.0/24 на все подсети.

e. На маршрутизаторах Router0 – Router5 получите информацию о MAC-адресах и IP-адресах активных интерфейсов (в том числе loopback-интерфейсов), проанализируйте ее и запишите в отчет в виде таблицы со столбцами «Название устройства | Тип и номер интерфейса | MAC-адрес интерфейса | IP-адрес интерфейса».

2. Настройка динамической маршрутизации в одной области с помощью протокола OSPF

a. На маршрутизаторах Router0 – Router5 с помощью команд вида
Router(config)#router OSPF [идентификатор процесса]
Router(config-router)#network [IP-адрес] [wildcard-маска] area [номер]
запустите процесс OSPF и назначьте интерфейсам номера областей в соответствии со схемой сети.

b. На маршрутизаторах Router0 – Router5 с помощью команды
Router#show ip ospf neighbor
получите информацию о состоянии всех соседних маршрутизаторов и проанализируйте ее.

c. На маршрутизаторах Router0 – Router5 с помощью команды и подкоманд Router#show ip ospf database ...
определите какую информацию о работе протокола OSPF можно получить, получите и проанализируйте ее.

d. На маршрутизаторах Router0 – Router5 с помощью команды и подкоманд
Router#show ip ospf interface [тип] [номер]
получите полную информацию об интерфейсах маршрутизатора, участвующих в работе протокола OSPF и проанализируйте ее.

e. На маршрутизаторах Router0 – Router5 с помощью команды
Router#show ip route
получите информацию о таблицах маршрутизации, проанализируйте ее и запишите в отчет.

3. Подготовка схемы сети

- a. Соберите модель сети в соответствии со схемой на рис. 4.2:

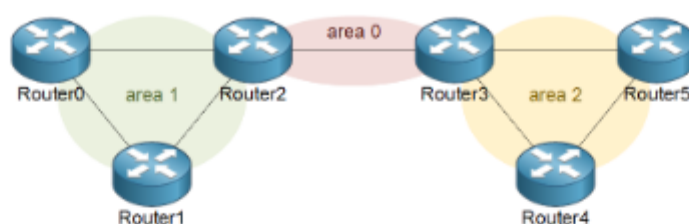


Рис. 4.2. Схема модели сети

b. На маршрутизаторах Router2 и Router3 назначьте интерфейсам, входящим согласно схеме сети, в одну область, IP-адреса из диапазонов IP-адресов подсетей с маской /30, полученных путем распределения одного диапазона IP-адресов вида [N].0.0.0/24 на все подсети.

c. На маршрутизаторах Router0 – Router5 получите информацию о MAC-адресах и IP-адресах активных интерфейсов (в том числе loopback-интерфейсов), проанализируйте ее и запишите в отчет в виде таблицы со столбцами «Название устройства | Тип и номер интерфейса | MAC-адрес интерфейса | IP-адрес интерфейса».

4. Настройка динамической маршрутизации в нескольких областях с помощью протокола OSPF

a. На маршрутизаторах Router2 и Router3 с помощью команд вида Router(config)#router OSPF [идентификатор процесса] Router(config-router)#network [IP-адрес] [wildcard-маска] area 0 активируйте процесс OSPF и назначьте интерфейсам номера областей в соответствии со схемой сети.

b. На маршрутизаторах Router3 и Router4 с помощью команды Router#show ip ospf neighbor получите информацию о состоянии всех соседних маршрутизаторов и проанализируйте ее.

c. На маршрутизаторах Router3 и Router4 с помощью команды и подкоманд Router#show ip ospf database ... определите какую информацию о работе протокола OSPF можно получить, получите и проанализируйте ее.

d. На маршрутизаторах Router3 и Router4 с помощью команды и подкоманд Router#show ip ospf interface [тип] [номер] получите полную информацию об интерфейсах маршрутизатора, участвующих в работе протокола OSPF и проанализируйте ее.

e. На маршрутизаторах Router3 и Router4 с помощью команды

Router#show ip route

получите информацию о таблицах маршрутизации, проанализируйте ее и запишите в отчет.

5. Настройка суммирования маршрутов

а. На пограничных маршрутизаторах областей №1-2 с помощью команды вида

Router(config-router)#area номер range [IP-адрес] [маска]

за счет использования маски подсети настройте в направлении магистрали (области №0) суммирование всех маршрутов соответствующих областей IP-адресами с маской /24.

б. На маршрутизаторах Router1 – Router6 с помощью команды

Router#show ip route

получите информацию о таблицах маршрутизации, проанализируйте ее изменения и запишите в отчет.

6. Настройка простой аутентификации

а. На маршрутизаторах области №1 с помощью команды вида

Router(config-router)#area [номер области] authentication

активируйте простую аутентификацию.

б. На маршрутизаторах области №1 с помощью команды вида

Router(config-if)#ip ospf authentication-key [ключ]

настройте на интерфейсах ключи для простой аутентификации.

с. На маршрутизаторах области №1 с помощью команды вида

Router#show ip ospf interface [тип] [номер]

получите информацию об интерфейсах, отнесенных к области №1 и проанализируйте ее.

д. На маршрутизаторах области №1 с помощью команды

Router#show ip ospf neighbor

получите информацию о состоянии всех соседних маршрутизаторов и проанализируйте ее.

7. Настройка криптографической аутентификации

а. На маршрутизаторах области №2 с помощью команды вида

Router(config-router)#area [номер] authentication message-digest

активируйте криптографическую аутентификацию.

б. На маршрутизаторах области №2 с помощью команды вида

Router(config-if)#ip ospf message-digest-key [идентификатор] md5 [ключ]

настройте на интерфейсах ключи для криптографической аутентификации.

с. На маршрутизаторах области №2 с помощью команды вида

Router#show ip ospf interface [тип] [номер]

получите информацию об интерфейсах, отнесенных к области №2 и проанализируйте ее.

д. На маршрутизаторах области №2 с помощью команды

Router#show ip ospf neighbor

получите информацию о состоянии всех соседних маршрутизаторов и проанализируйте ее.

8. Подготовка схемы сети

- а. Соберите модель сети в соответствии со схемой на рис. 4.3:



Рис. 4.3. Схема модели сети

б. На маршрутизаторах Router6 – Router9 назначьте интерфейсам, входящим согласно схеме сети, в одну область, IP-адреса из диапазонов IP-адресов подсетей с маской /30, полученных путем распределения одного диапазона IP-адресов вида [N+1].0.0.0/24 на все подсети.

с. На маршрутизаторах Router6 – Router9 с помощью команд вида
Router(config)#interface loopback [номер]
Router(config-if)#ip address [IP-адрес] [маска]
создайте виртуальные loopback-интерфейсы и назначьте им IP-адреса для идентификации маршрутизаторов в процессе работы протокола OSPF.

д. На маршрутизаторах Router6 – Router9 получите информацию о MAC-адресах и IP-адресах активных интерфейсов (в том числе loopback-интерфейсов), проанализируйте ее и **запишите в отчет** в виде таблицы со столбцами «Название устройства | Тип и номер интерфейса | MAC-адрес интерфейса | IP-адрес интерфейса».

На маршрутизаторах Router7 – Router18 с помощью команд вида

```
Router(config)#router OSPF [идентификатор процесса]
Router(config-router)#network [IP-адрес] [wildcard-маска] area [номер]
```

активируйте процесс OSPF и назначьте интерфейсам номера областей в соответствии со схемой сети.

9. Подключение области к магистральной через виртуальный канал

а. На маршрутизаторах Router7 и Router8 с помощью команды вида
Router(config-router)#area [номер] virtual-link [идентификатор]
создайте виртуальный канал для подключения области №2, не имеющей физического подключения к магистральной (области №0).

б. На маршрутизаторах Router7 и Router8 с помощью команды
Router#show ip ospf virtual-links
получите информацию о виртуальных каналах, проанализируйте ее и **запишите в отчет**.

с. На маршрутизаторах Router7 и Router8 с помощью команды
Router#show ip route
получите информацию о таблицах маршрутизации, проанализируйте и **запишите в отчет**.

Контрольные вопросы

1. Какие этапы работы у алгоритма маршрутизации, основанного на состоянии связей?
2. Какие особенности применения, достоинства и недостатки у протоколов маршрутизации, основанных на алгоритме состояния связей?
3. Как в протоколе OSPF происходит выбор идентификатора маршрутизатора?
4. Как в протоколе OSPF происходит установка отношений соседства?
5. Что такое и как в протоколе OSPF выбираются выделенный маршрутизатор (DR) и резервный выделенный маршрутизатор (BDR)?
6. Какие в протоколе OSPF существуют типы областей (зон)?
7. Какие относительно работы протокола OSPF существуют типы маршрутизаторов?
8. Какие в протоколе OSPF существуют типы объявлений о состоянии канала (LSA)?
9. Как в протоколе OSPF происходит построение и поддержание базы данных о состоянии связей сети (LSDB)?
10. Какие в протоколе OSPF применяются метрики маршрута?
11. Как в протоколе OSPF реализовано нахождение оптимальных маршрутов?
12. Как в протоколе OSPF происходит генерация таблицы маршрутизации?
13. Что такое суммирование маршрутов и с какой целью оно применяется?
14. Как к магистральной области может быть подключена область, физически с ней не связанная?
15. Для чего и какие виды аутентификации применяются в протоколе OSPF?

ПРАКТИЧЕСКАЯ РАБОТА № 5 BGP

Цель работы

Изучить настройку маршрутизации между автономными системами с помощью протокола BGP (англ. Border Gateway Protocol, протокол граничного шлюза).

Теоретические сведения

1. BGP // Точка обмена знаниями по UNIX/Linux-системам и системам с открытым исходным кодом. URL: <http://xgu.ru/wiki/BGP> (дата обращения: 20.05.2021).

2. BGP в Cisco // Точка обмена знаниями по UNIX/Linux-системам и системам с открытым исходным кодом. URL: http://xgu.ru/wiki/BGP_в_Cisco (дата обращения: 20.05.2021).

3. Руководства по настройке совместимых систем: Руководство по конфигурации BGP // Сайт компании Cisco Systems. URL: https://www.cisco.com/c/ru_ru/support/docs/ip/border-gateway-protocol-bgp/17612-bgp.html (дата обращения: 20.05.2021).

4. Практические примеры BGP // Сайт компании Cisco Systems. URL: https://www.cisco.com/c/ru_ru/support/docs/ip/border-gateway-protocol-bgp/26634-bgp-toc.html (дата обращения: 20.05.2021).

5. BGP: часто задаваемые вопросы // Сайт компании Cisco Systems. URL: https://www.cisco.com/cisco/web/support/RU/9/92/92044_bgpfaq_5816.html (дата обращения: 20.05.2021).

Порядок выполнения работы

1. Подготовка схемы сети

- а. Соберите модель сети в соответствии со схемой на рисунке:

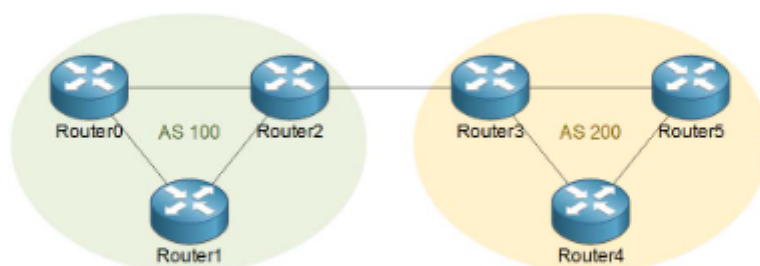


Схема модели сети

б. На маршрутизаторах Router0 – Router5 с помощью команд вида
`Router(config)#interface loopback [номер]`
`Router(config-if)#ip address [IP-адрес] [маска]`
создайте виртуальные loopback-интерфейсы и назначьте им IP-адреса для идентификации маршрутизаторов.

с. На маршрутизаторах Router0 – Router2, входящих согласно схеме сети, в одну автономную систему, назначьте интерфейсам IP-адреса из диапазонов IP-адресов подсетей, полученных путем распределения одного диапазона IP-адресов вида [N].100.0.0/24 на все подсети.

д. На маршрутизаторах Router3 – Router5, входящих согласно схеме сети, в одну автономную систему, назначьте интерфейсам IP-адреса из диапазонов IP-адресов подсетей, полученных путем распределения одного диапазона IP-адресов вида [N].200.0.0/24 на все подсети.

е. На маршрутизаторах Router2 и Router3 назначьте соединяющим их между собой интерфейсам IP-адреса с маской /30 для обеспечения возможности маршрутизации.

ф. На маршрутизаторах Router0 – Router5 получите информацию о MAC-адресах и IP-адресах активных интерфейсов (в том числе loopback-интерфейсов), проанализируйте ее и **запишите в отчет** в виде таблицы со столбцами «Название устройства | Тип и номер интерфейса | MAC-адрес интерфейса | IP-адрес интерфейса».

г. На маршрутизаторах Router1 – Router6 настройте динамическую маршрутизацию внутри каждой автономной системы с помощью протокола OSPF.

h. На маршрутизаторах Router0 – Router5 с помощью команды Router#show ip route получите информацию о таблицах маршрутизации, проанализируйте ее и **запишите в отчет**.

2. Настройка распространения маршрутов между автономными системами

а. На пограничных маршрутизаторах автономных систем Router2 и Router3 с помощью команд вида

```
Router(config)#router bgp [номер]  
Router(config-router)#neighbor [IP-адрес] remote-as [номер]
```

присвойте каждому маршрутизатору номер автономной системы в соответствии со схемой сети и активируйте сессии BGP между соседними пограничными маршрутизаторами.

б. На пограничном маршрутизаторе автономной системы Router2 с помощью команд вида

```
Router(config)#router bgp [номер]  
Router(config-router)#network [номер] mask [маска]
```

сформируйте списки IP-адресов подсетей, информация о которых будет распространяться с помощью протокола BGP.

с. На пограничном маршрутизаторе автономной системы Router3 с помощью команд вида

```
Router(config)#router bgp [номер]  
Router(config-router)#redistribute [тип]
```

перераспределите распространение информации о маршрутах, полученных с помощью протокола OSPF, по протоколу BGP.

д. На маршрутизаторах Router2 и Router3 с помощью команды

```
Router#show ip route
```

получите информацию о таблицах маршрутизации, проанализируйте ее и **запишите в отчет**.

3. Настройка распространения маршрутов внутри автономных систем

а. На пограничном маршрутизаторе автономной системы Router2 с помощью команд вида

```
Router(config)#ip route [IP-адрес] [маска] [IP-адрес]
Router(config)#router ospf [номер]
Router(config-router)#default-information originate
```

сформируйте статический маршрут до соседнего пограничного маршрутизатора автономной системы и перераспределите распространение информации о нем с помощью протокола OSPF.

б. На пограничном маршрутизаторе автономной системы Router3 с помощью команд вида

```
Router(config)#router ospf [номер]
Router(config-router)#redistribute bgp [номер] subnets
```

перераспределите распространение информации о маршрутах, полученных с помощью протокола BGP, по протоколу OSPF.

с. На маршрутизаторах Router0 – Router5 с помощью команды `Router#show ip route` получите информацию о таблицах маршрутизации, проанализируйте ее и запишите в отчет.

Контрольные вопросы

1. Что такое автономная система, для чего она создается, как нумеруется и кем управляется?
2. Какое назначение, принципы работы и настройки у протокола BGP?
3. Как в протоколе BGP происходит установка отношений соседства?
4. Какие относительно работы протокола BGP существуют типы маршрутизаторов?
5. Как в протоколе BGP происходит построение таблицы маршрутизации?
6. Как в протоколе BGP происходит перераспределение маршрутов?
7. Как в протоколе BGP происходит управление маршрутами?

ПРАКТИЧЕСКАЯ РАБОТА № 6 NAT

Цель работы

Изучить настройку службы NAT (англ. Network Address Translation, трансляция сетевых адресов).

Теоретические сведения

1. Cisco NAT // Точка обмена знаниями по UNIX/Linux-системам и системам с открытым исходным кодом. URL: http://xgu.ru/wiki/Cisco_NAT (дата обращения: 20.05.2021).

2. Настройка трансляции сетевых адресов: Начало работы
// Сайт компании Cisco Systems. URL: http://www.cisco.com/cisco/web/support/RU/9/92/92026_12.html (дата обращения: 20.05.2021).

Порядок выполнения работы

1. Подготовка схемы сети

- а. Соберите модель сети в соответствии со схемой на рисунке:

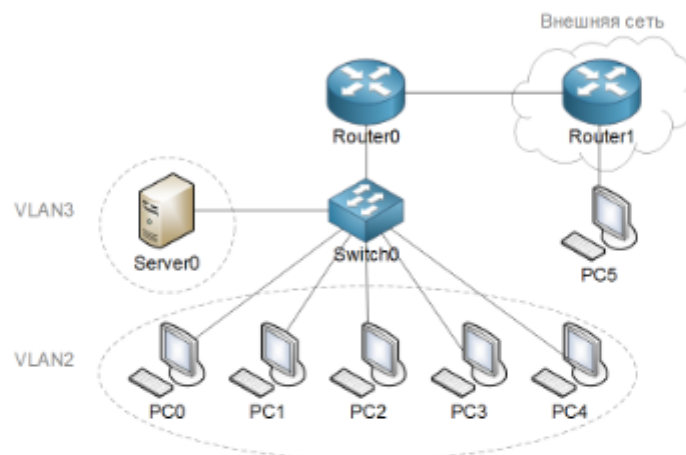


Схема модели сети

б. На маршрутизаторах Router0 – Router1, компьютерах PC0 – PC5 и сервере Server0 назначьте интерфейсам, входящим согласно схеме сети, в одну подсеть, IP-адреса из диапазонов IP-адресов подсетей, полученных путем распределения одного диапазона IP-адресов вида [N].0.0.0/8 на все подсети.

с. На маршрутизаторе Router0 настройте маршрутизацию между виртуальными локальными сетями VLAN2 и VLAN3 по схеме «маршрутизатор на привязи».

д. На маршрутизаторе Router0 с помощью команды вида
`Router(config)#ip route [IP-адрес] [маска] [IP-адрес]`
создайте маршрут «по умолчанию» для всего трафика.

е. На маршрутизаторах Router0 и Router1 маршрутизацию между сетями, которые к ним подключены, не настраивайте.

ф. На маршрутизаторах Router0 и Router1, коммутаторе Switch0, компьютерах PC0 – PC5 и сервере Server0 получите информацию о MAC-адресах и(или) IP-адресах активных интерфейсов, проанализируйте ее и **запишите в отчет** в виде таблицы со столбцами «Название устройства | Тип и номер интерфейса | MAC-адрес интерфейса | IP-адрес интерфейса».

g. На маршрутизаторах Router0 и Router1 с помощью команды Router#show ip route получите информацию о таблицах маршрутизации, проанализируйте ее и запишите в отчет.

Таким образом, должна получиться схема сети, в которой маршрутизатор Router1 и компьютер PC5 моделируют внешнюю сеть, а маршрутизатор Router0, коммутатор Switch0, компьютеры PC0 – PC4 и сервер Server0 моделируют локальную сеть, при этом маршрутизатору Router0 на внешний интерфейс назначен уникальный глобальный IP-адрес, а частные IP-адреса локальной сети в таблицу маршрутизации маршрутизаторов Router0 и Router1 не попадают.

2. Настройка перегруженной NAT

a. На маршрутизаторе Router0 с помощью команды вида

```
Router(config)#interface [тип] [номер]
Router(config-if)#ip nat outside
```

установите исходящий интерфейс для службы NAT.

b. На маршрутизаторе Router0 с помощью команды вида

```
Router(config)#interface [тип] [номер]
Router(config-if)#ip nat inside
```

определите входящие для службы NAT интерфейсы (подынтерфейсы).

c. На маршрутизаторе Router0 с помощью команды вида

```
Router(config)#ip access-list standart [имя]
Router(config-std-nacl)#permit [IP-адрес] [wildcard-маска]
```

сформируйте список контроля доступа, содержащий IP-адреса сетей, которые должны быть заменены службой NAT на глобальный IP-адрес.

d. На маршрутизаторе Router0 с помощью команды вида

```
Router(config)#ip nat inside source list [имя] interface [имя]
[номер] overload
```

создайте правило трансляции.

e. На компьютерах PC0 – PC4 и сервере Server0, используя утилиту «Command Prompt», с помощью команды вида

```
PC>ping [IP-адрес]
```

проверьте доступность компьютера PC5.

f. На маршрутизаторе Router0 с помощью команды

```
Router#show ip nat translations
```

получите информацию о трансляциях, проанализируйте ее и запишите в отчет.

3. Настройка статической NAT

a. На сервере Server0 запустите службу HTTP и, по желанию, с помощью языка гипертекстовой разметки HTML отредактируйте содержимое страниц, размещенных на HTTP-сервере.

b. На маршрутизаторе Router0 с помощью команды вида

```
Router(config)#ip nat inside source static tcp [IP-адрес] [номер
порта] [IP-адрес] [номер порта]
```

создайте статическое правило трансляции.

с. На компьютере PC5, используя утилиту «Web Browser», проверьте доступность содержимого HTTP-сервера Server0 (веб-сайта), обратившись к нему по IP-адресу и номеру порта.

д. На маршрутизаторе Router0 с помощью команды Router#show ip nat translations получите информацию о трансляциях, проанализируйте ее и запишите в отчет.

Контрольные вопросы

1. Что такое NAT, вследствие каких причин и с какой целью она применяется?
2. Какие принципы работы у службы NAT?
3. Какие типы NAT существуют и в каких случаях они применяются?
4. Что такое список контроля доступа, в каком виде он хранится, с какой целью и на каких устройствах применяется?

ПРАКТИЧЕСКАЯ РАБОТА № 7 WI-FI

Цель работы

Изучить настройку беспроводной сети на базе стандарта IEEE 802.11 (англ. Wireless Fidelity, Wi-Fi).

Теоретические сведения

1. Технологии // Wireless Life - Мобильность жизни
URL: <http://wi-life.ru/tehnologii> (дата обращения: 20.05.2021).

Порядок выполнения работы

1. Подготовка схемы сети

- а. Соберите модель сети в соответствии со схемой на рис. 7.1:



Рис. 7.1. Схема модели сети

б. На маршрутизаторе Router0 и компьютере PC0, в том числе, с помощью команд вида

```
Router(config)#interface [тип] [номер]
Router(config-if)#ip address [IP-адрес] [маска]
Router(config-if)#no shutdown
```

назначьте соединяющим их интерфейсам IP-адреса из диапазона IP-адресов вида 100.100.[N].0/30, и включите их.

с. На маршрутизаторе Router0 настройте службу NAT для трансляции IP-адресов сетевых устройств, которые будут подключены к сети Wi-Fi точки доступа Access Point0.

д. На маршрутизаторе Router0 настройте DHCP-сервер для выдачи сетевых параметров сетевым устройствам, которые будут подключены к сети Wi-Fi точки доступа Access Point0, в том числе IP-адресов из диапазона IP-адресов вида 192.168.[N].0/24.

е. На маршрутизаторе Router0, компьютере PC0, ноутбуке Laptop0, планшете Tablet PC0 и смартфоне Smartphone0 получите информацию о MAC-адресах и IP-адресах активных интерфейсов, проанализируйте ее и **запишите в отчет** в виде таблицы со столбцами «Название устройства | Тип и номер интерфейса | MAC-адрес интерфейса | IP-адрес интерфейса».

2. Настройка сети Wi-Fi на точке доступа

а. На точке доступа Access Point0 задайте имя сети вида «WiFiNetwork[N]», выберите канал, тип аутентификации, алгоритм шифрования, установите пароль и эти параметры **запишите в отчет**.

б. На ноутбуке Laptop0, планшете Tablet PC0 и смартфоне Smartphone0 настройте беспроводные интерфейсы для подключения к сети Wi-Fi точки доступа Access Point0.

с. На ноутбуке Laptop0, планшете Tablet PC0 и смартфоне Smartphone0, используя утилиту «Command Prompt», с помощью команды вида PC>ping [IP-адрес]

проверьте доступность компьютера PC0.

3. Подготовка схемы сети

а. Соберите модель сети в соответствии со схемой на рис. 7.2:

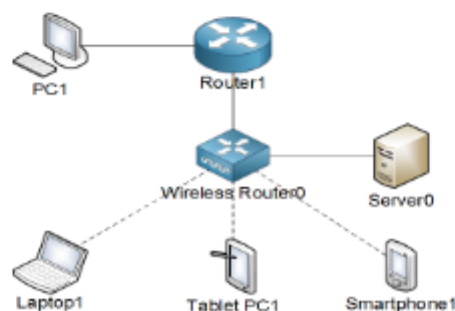


Рис. 7.2. Схема модели сети

б. На беспроводном маршрутизаторе Wireless Router0, сервере Server0, маршрутизаторе Router1 и компьютере PC1, в том числе, с помощью команд вида

```
Router(config)#interface [тип] [номер]
Router(config-if)#ip address [IP-адрес] [маска]
Router(config-if)#no shutdown
```

назначьте соединяющим их интерфейсам IP-адреса из диапазона IP-адресов вида 200.200.[N].0/30, и включите их.

с. На беспроводном маршрутизаторе Wireless Router0 установите в качестве шлюза по умолчанию (Default gateway) IP-адрес соответствующего интерфейса маршрутизатора Router0.

д. На маршрутизаторе Router1, беспроводном маршрутизаторе Wireless Router0, сервере Server0, компьютере PC1, ноутбуке Laptop1, планшете Tablet PC1 и смартфоне Smartphone1 получите информацию о MAC-адресах и IP-адресах активных интерфейсов, проанализируйте ее и **запишите в отчет** в виде таблицы со столбцами «Название устройства | Тип и номер интерфейса | MAC-адрес интерфейса | IP-адрес интерфейса».

4. Настройка сети Wi-Fi на беспроводном маршрутизаторе

а. На беспроводном маршрутизаторе Wireless Router0, используя графический пользовательский интерфейс (GUI), на вкладке «Setup – Basic Setup» назначьте IP-адрес, маску и шлюз по-умолчанию (Default gateway), настройте DHCP-сервер для выдачи сетевых параметров сетевым устройствам, которые будут подключены к сети Wi-Fi беспроводного маршрутизатора Wireless Router0, в том числе IP-адресов из диапазона IP-адресов вида 192.168.[N+1].0/24, и зарезервируйте один выдаваемый IP-адрес за сервером Server0.

б. На беспроводном маршрутизаторе Wireless Router0, используя графический пользовательский интерфейс (GUI), на вкладке «Wireless – Basic Wireless Settings» выберите режим Wi-Fi, задайте имя сети вида «WiFiNetwork[N+1]», выберите частотный диапазон и канал и эти параметры **запишите в отчет**.

с. На беспроводном маршрутизаторе Wireless Router0, используя графический пользовательский интерфейс (GUI), на вкладке «Wireless – Wireless Security» выберите режим безопасности, алгоритм шифрования, установите пароль и эти параметры **запишите в отчет**.

д. На ноутбуке Laptop1, планшете Tablet PC1 и смартфоне Smartphone1 настройте беспроводные интерфейсы для подключения к сети Wi-Fi беспроводного маршрутизатора Wireless Router0.

е. На сервере Server1, ноутбуке Laptop1, планшете Tablet PC1 и смартфоне Smartphone1, используя утилиту «Command Prompt», с помощью команды вида

```
PC>ping [IP-адрес]
```

проверьте доступность компьютера PC1.

f. На компьютере PC1, используя утилиту «Web Browser», убедитесь в том, что содержимое HTTP-сервера Server0 (веб-сайт) не доступно, обратившись к нему по IP-адресу (и номеру порта).

g. На беспроводном маршрутизаторе Wireless Router0, используя графический пользовательский интерфейс (GUI), на вкладке «Application & Gaming – Single Port Forwarding» настройте проброс порта службы HTTP на внутренний IP-адрес сервера Server0.

h. На компьютере PC1, используя утилиту «Web Browser», проверьте доступность содержимого HTTP-сервера Server0 (веб-сайта), обратившись к нему по IP-адресу (и номеру порта).

Контрольные вопросы

1. Какие стандарты и режимы Wi-Fi существуют, в чем их особенности и какие у них характеристики?
2. Какие частотные полосы и каналы Wi-Fi существуют, какие у них характеристики?
3. Какое назначение и принципы работы у точки доступа?
4. Какие режимы работы точек доступа существуют, в чем их особенности и какое у них назначение?
5. Какое назначение и принципы работы у беспроводного маршрутизатора?

