ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Петербургский государственный университет путей сообщения Императора АлександраI»
(ФГБОУ ВО ПГУПС)

Петрозаводский филиал ПГУПС

ОДОБРЕНО
на заседании цикловой комиссии
протокол №_11_от_23.06.2017
Председатель цикловой комиссии:
_____(_____)

УТВЕРЖДАЮ
Начальник УМО
_____ А.В. Калько
«23» 06 2017г.

МЕТОДИЧЕСКИЕ УКАЗАНИЯ
по организации и проведению практических занятий

По МДК 02.03. Межсетевое взаимодействие в крупных и глобальных сетях

Специальность: 09.02.02 Компьютерные сети

Разработчик: преподаватель ПФ ПГУПС Усков Алексей Андреевич

2017г

Перечень практических занятий

1.Протокол межсетевого взаимодействия IP, протоколы маршрутизации
2.Изучение маршрутов следования информации в сети. Автономные системы
3.Изучение работы утилит ping, traceroute. Изучение протокола межсетевых управляющих сообщений ICMP.
4.Разработка схемы сети. Разбиение сети на подсети. Разработка схемы IP-адресации.
5.Базовая настройка маршрутизаторов. Настройка интерфейсов маршрутизаторов. Чтение конфигурации маршрутизатора. 4ч
6.Настройка статической маршрутизации 4ч
7.Настройка RIP маршрутизации 4ч
8.Настройка OSPF маршрутизации 4ч
9. Настройка BGP маршрутизации 4ч
10.Настройка удаленного доступа, удаленного управления 2ч
11.Настройка списков доступа 4ч
12.Настройка NAT-пула с перегрузкой и PAT 4ч
13.Настройка туннеля VPN GRE по схеме «точка-точка» 4ч
14.Настройка сетей VPN 4ч
15.Настройка IP телефонии 4ч

Усвоенные знания, освоенные умения, приобретенный практический опыт, формируемые элементы компетенций

Знания:

-технологии безопасности, протоколы авторизации, конфиденциальность и безопасность при работе в web;

Умения:

принимать меры по устранению возможных сбоев

Практический опыт:

-организации доступа к локальным и глобальным сетям;

Профессиональные и общие компетенции:

ПК 2.1. Администрировать локальные вычислительные сети и принимать меры по устранению возможных сбоев.

ПК 2.2. Администрировать сетевые ресурсы в информационных системах.

ПК 2.3. Обеспечивать сбор данных для анализа использования и функционирования программно-технических средств компьютерных сетей.

ПК 2.4. Взаимодействовать со специалистами смежного профиля при разработке методов, средств и технологий применения объектов профессиональной деятельности.

ОК 1.	Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.
ОК 2.	Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.
ОК 3.	Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.
ОК 4.	Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.
ОК 5.	Использовать информационно-коммуникационные технологии в профессиональной деятельности.
ОК 6.	Работать в коллективе и в команде, эффективно общаться с коллегами, руководством, потребителями.
ОК 7.	Брать на себя ответственность за работу членов команды (подчиненных), за результат выполненных заданий.
ОК 8.	Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.
ОК 9.	Ориентироваться в условиях частой смены технологий в профессиональной деятельности.

Практическое занятие №1

Тема: протокол межсетевого взаимодействия IP, протоколы маршрутизации

Цель: изучение заголовка IP, изучение протоколов маршрутизации

Исходные данные:
В папке packets файлы с захваченными пакетами.

Задание:

1. Запустить программу Wireshark. Выполнить захват пакетов. Изучить и описать поля заголовка IP, нескольких пакетов. Описать поля. Чем они отличаются, почему?
2. Изучить и описать содержимое файла rip_v1.cap. Какие протоколы нижележащих уровней использует протокол RIP?
3. Изучить и описать содержимое файла ospf.cap. Какие протоколы нижележащих уровней использует протокол OSPF?
4. Изучить и описать содержимое файла bgp.pcap. Описать содержимое OPEN Message, KEEPALIVE Message, UPDATE Message.

Практическое занятие №2

Тема: Изучение маршрутов следования информации в сети. Автономные системы

Задание:

1. С помощью tracert определить путь до сайта ya.ru
2. Определить IP адреса всех узлов.
3. Определить номера автономных систем (если это возможно).
4. Нарисовать схему маршрута с указанием IP адресов и номеров автономных систем.
5. Используя сайт указанный в разделе “Ссылки и литература”, узнать какие автономные системы зарегистрированы в г.Петрозаводск, сколько их, и кому они принадлежат.
6. Узнать IP адреса, и автономные системы в которых находятся сл. сайты: karelia.pro, karelia.ru, pgups-karelia.ru

Практическое занятие №3

Тема: Изучение работы утилит ping, traceroute. Изучение протокола межсетевых управляющих сообщений ICMP.

Задание:

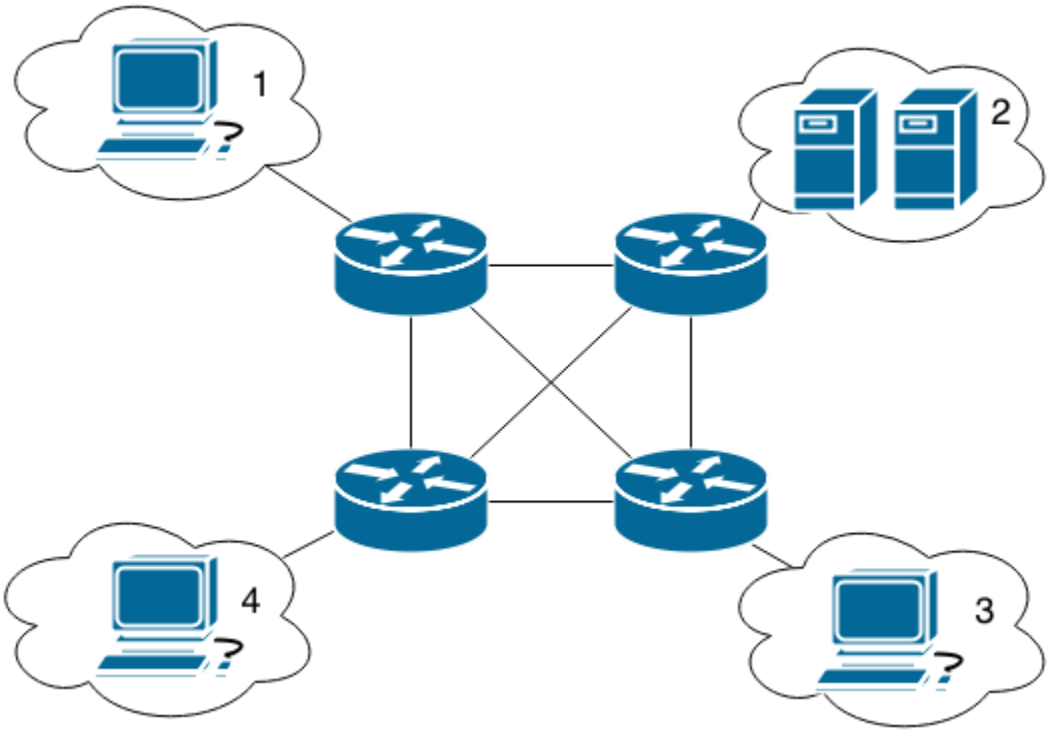
1. Открыть программу Wireshark, начать захват сетевого трафика.
2. Открыть командную строку. Выполнить команды ping, tracert. Команды выполнить к разным хостам например ping google.com, tracert ya.ru.
3. Остановить захват сетевого трафика. Выполнить фильтрацию полученного трафика, оставив только пакеты протокола ICMP.
4. Проанализировать пакеты ping, tracert. Изучить содержимое заголовков IP пакетов, содержимое ICMP заголовка.

Практическое занятие №4

Тема: Разработка схемы сети. Разбиение сети на подсети. Разработка схемы IP-адресации.

Задача:

Разработать корпоративную распределенную сеть передачи данных для некоторой организации. Организация имеет три офиса и центр обработки данных.



Необходимо разработать схему IP адресации, логическую схему сети. Во всех сетях количество хостов не превышает 254. Связь между офисами организована на основе L2 VPN каналов одним провайдером.
Сеть 192.168.0.0/24 - разбейте на подсети, для маршрутизаторов.
Сети 192.168.x.0/24, где x = 1,2,3,4 используйте для сетей офисов и центра обработки данных.

В отчете представить: схему IP адресации; схему сети.

Практическое занятие №5

Тема: Базовая настройка маршрутизаторов. Настройка интерфейсов маршрутизаторов. Чтение конфигурации маршрутизатора.

Задание:
На основе схемы IP адресации и логической схемы сети построить сеть в программе Cisco Packet Tracer. В качестве маршрутизаторов использовать 2811, добавляя модуль NM-2FE2W. В качестве коммутатора 2950-24. Сервера и компьютеры выбрать стандартные - Server-PT, PC-PT. Добавить коммутатор в каждую сеть. Добавить по три хоста в сети офисов 1,3,4. Для сети №2 (центра обработки данных) добавить три сервера.

На маршрутизаторах:

- настроить имя устройства;
- настроить список локальных пользователей из двух пользователей - admin с самым высоким уровнем привелегий, и monitor с наименьшим уровнем привелегий. Настроить консольный порт для аутентификации по локальному списку пользователей. Пароли хранить в зашифрованном виде.
- настроить IP адресацию
- сохранить конфигурацию

На хостах, серверах:

- настроить IP адресацию, указать IP адрес шлюза

Для сдачи работы необходимо понимать что выводят сл. команды: show int имя_итерфейса; show ip interface brief; show users; show line.

* После выполнения и сдачи работы сделать резервную копию настроенной сети. Т.к. в дальнейшем из этой копии будут выполняться другие работы.

Практическое занятие №6

Тема: Настройка статической маршрутизации

Задание:

1. Настроить статическую маршрутизацию (для сети разработанной ранее).
2. Проверить настройку маршрутизации, выполнив команду ping из каждой подсети во все другие.

Для защиты работы:

- показать работающую маршрутизацию в программе Cisco Packet Tracer. Рассказать как и в какой последовательности настраивали маршрутизацию.
- знать команды просмотра таблицы маршрутизации
- уметь в программе Cisco Packet Tracer отслеживать путь трафика

Практическое занятие №7

Тема: Настройка RIP маршрутизации

Задание:

1. Настроить маршрутизацию по протоколу RIPv2 (для сети разработанной ранее).
2. Проверить настройку маршрутизации, выполнив команду ping из каждой подсети во все другие.

Для защиты работы:

- понимать, что такое протокол RIP для чего он нужен и как он работает
- показать работающую маршрутизацию в программе Cisco Packet Tracer. Рассказать как и в какой последовательности настраивали маршрутизацию.
- знать команды просмотра таблицы маршрутизации, команды просмотра настроек
- уметь в программе Cisco Packet Tracer отслеживать путь трафика

Практическое занятие №8

Тема: Настройка OSPF маршрутизации

Задание:

1. Настроить маршрутизацию по протоколу OSPF (для сети разработанной ранее).
2. Проверить настройку маршрутизации, выполнив команду ping из каждой подсети во все другие.

Для защиты работы:

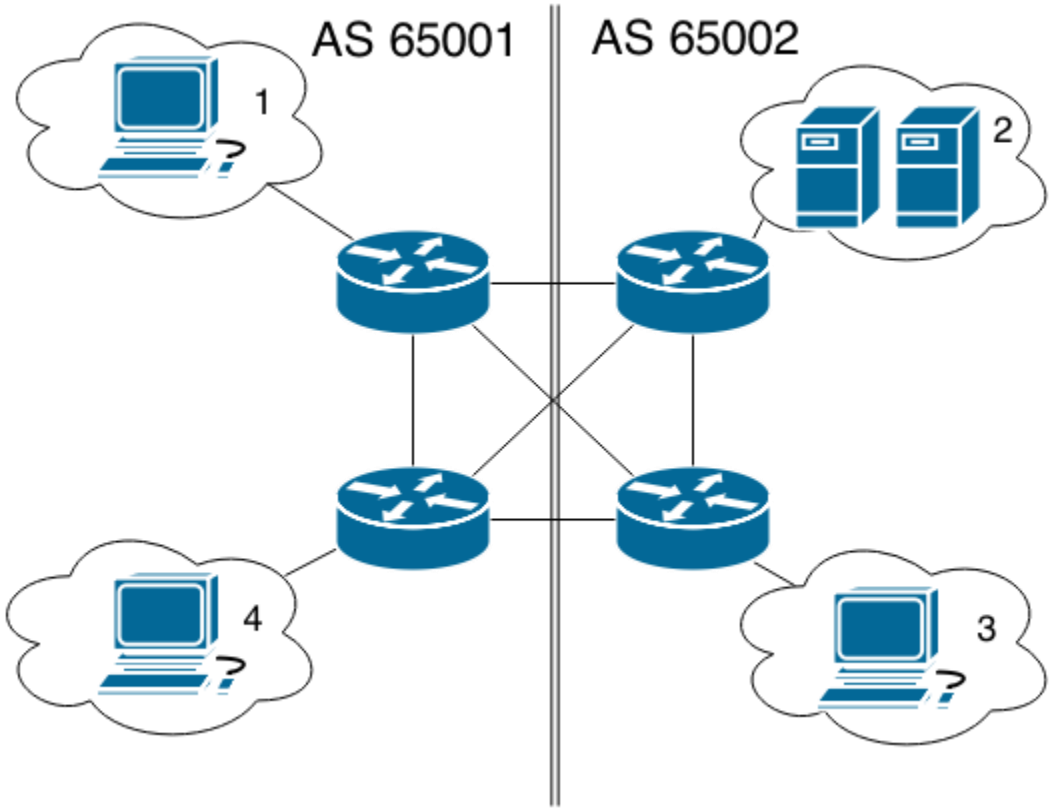
- понимать, что такое протокол OSPF для чего он нужен и как он работает
- показать работающую маршрутизацию в программе Cisco Packet Tracer. Рассказать, как и в какой последовательности настраивали маршрутизацию.
- знать команды просмотра таблицы маршрутизации, команды просмотра настроек
- уметь в программе Cisco Packet Tracer отслеживать путь трафика

Практическое занятие №9

Тема: Настройка BGP маршрутизации

Задание:

1. Настроить маршрутизацию по протоколу BGP (для сети разработанной ранее). В Cisco Packet Tracer не реализовано iBGP соседство, поэтому маршруты внутри одной автономной системы надо прописать статически. Поделить сеть на две автономные системы,можно, например, вот так:



2. Проверить настройку маршрутизации, выполнив команду ping из каждой подсети во все другие.

Для защиты работы:

- понимать, что такое протокол BGP для чего он нужен и как он работает
- показать работающую маршрутизацию в программе Cisco Packet Tracer. Рассказать, как и в какой последовательности настраивали

маршрутизацию.

- знать команды просмотра таблицы маршрутизации, команды просмотра настроек: show ip bgp, show ip bgp neighbors, show ip bgp summary.
- уметь в программе Cisco Packet Tracer отслеживать путь трафика

Практическое занятие №10

Тема: Настройка удаленного доступа, удаленного управления

Задание:

1. Настроить удаленный доступ по протоколам telnet, ssh на каждом маршрутизаторе (для схемы разработанной ранее). SSH настроить 2-ой версии, с количеством попыток входа - 2, и тайм-аутом - 60 секунд.
2. Проверить настройку удаленного доступа, выполнив удаленный вход на каждый маршрутизатор по протоколу telnet, ssh.

Для защиты работы:

- понимать, что такое протоколы telnet, ssh для чего они нужны и как работают
- показать возможности удаленного управления в программе Cisco Packet Tracer. Рассказать, как и в какой последовательности настраивали удаленный доступ.
- знать команды настройки удаленного доступа, команды просмотра пользователей устройства, команды просмотра состояния линий

Практическое занятие № 11

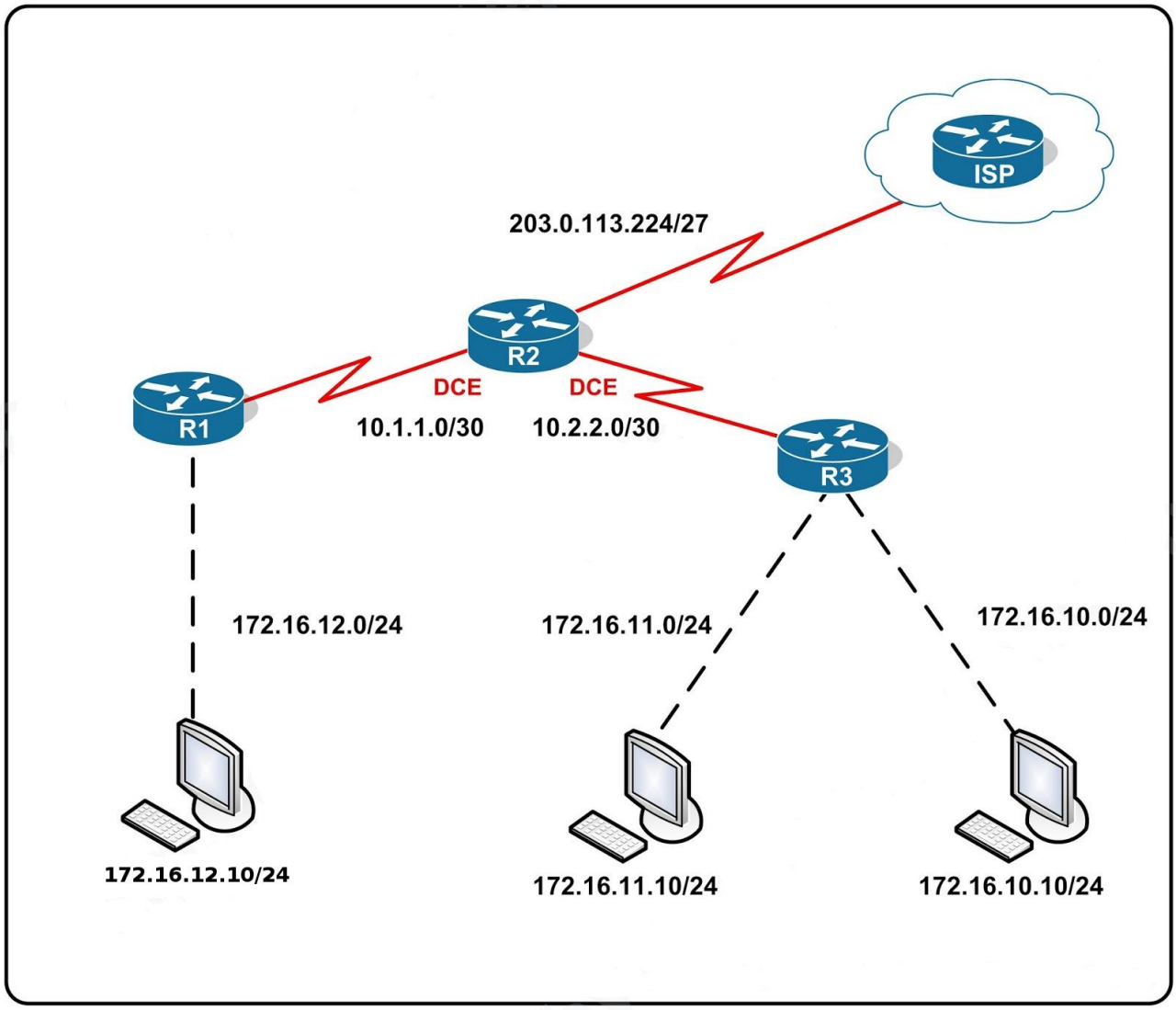
Тема: Настройка списков доступа
Цель выполнения работы: формирование профессиональных умений выполнять настройку списков доступа на маршрутизаторах и другом активном сетевом оборудовании

Постановка задачи или ситуации (если имеется):

Данная практическое занятие может быть выполнена на реальном оборудовании или в Cisco Packet Tracer. Все необходимые действия указаны в порядке их выполнения. Для начала необходимо построить сеть указанную на схеме. После схемы сети приведена схема адресации, адреса нужна назначать только когда это будет явно указано в порядке выполнения.

Исходные данные (если имеются)

Схема сети



План адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1	**S0/0**	**10.1.1.2**	**255.255.255.252**	**N/A**
	Fa0/0	**172.16.12.1**	**255.255.255.0**	**N/A**
R2	**S0/0**	**10.1.1.1**	**255.255.255.252**	**N/A**

	S0/1	**10.2.2.1**	**255.255.255.252**	**N/A**
	Lo0	**203.0.113.225**	**255.255.255.255**	**N/A**
R3	**S0/0**	**10.2.2.2**	**255.255.255.252**	**N/A**
	Fa0/0	**172.16.10.1**	**255.255.255.0**	**N/A**
	Fa0/1	**172.16.11.1**	**255.255.255.0**	**N/A**
PC1	**NIC**	**172.16.12.10**	**255.255.255.0**	**172.16.12.1**
PC2	**NIC**	**172.16.11.10**	**255.255.255.0**	**172.16.11.1**
PC3	**NIC**	**172.16.10.10**	**255.255.255.0**	**172.16.10.1**

Порядок выполнения

1. Настроить базовую конфигурацию оборудования

 Настроить hostname на маршрутизаторах.

 Отключить DNS lookup.

 Установитьпароль для EXEC mode

 Настроитьmessage-of-the-day banner.

 Установить пароль для console

2. Настроить адресацию оборудования согласно плана

 Настроить интерфейсы на**R1**, **R2** и **R3** согласно плана адресации.

 Проверить выполненные настройки командой**show ip interface brief**

 Настроить интерфейсы**PC1, PC2**, **PC3** и **Server** в соответствии с таблицей

 Сконфигурировать протокол динамической маршрутизации**OSPF** на **R1, R2** и **R3** для всех присутствующих сетей.

 Проверить выполненные настройки командой**ping**.

3. Настроить стандартные списки доступа

 На маршрутизаторе**R1** создать стандартный список доступа **STN_ACL_1**.

R1(config)#ip access-list standard STN_ACL_1

 Добавить правила запрещающие трафик из сети 172.16.11.0/24.

R1(config-std-nacl)#deny 172.16.11.0 0.0.0.255

 Добавить правило разрешающее остальной трафик

R1(config-std-nacl)#permit any

 Установить созданный список доступа**STN_ACL_1** на маршрутизаторе **R1** для входящего трафика через интерфейс **S0/1**

R1(config)#interface serial 0/1

R1(config-if)#ip access-group STN_ACL_1 in

R1(config-if)#end

R1#copy run start

 Проверить работу**ACL** при помощи команды **ping**, используя параметр **source**

R3#ping 172.16.12.1 source 172.16.11.1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 172.16.12.1, timeout is 2 seconds:

Packet sent with a source address of **172.16.11.1**

U.U.U

Success rate is 0 percent (**0/5**)

R3#ping 172.16.12.1 source 172.16.10.1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 172.16.12.1, timeout is 2 seconds:

Packet sent with a source address of **172.16.10.1**

!!!!!

Success rate is 100 percent (**5/5**), round-trip min/avg/max = 40/43/44 ms

 Просмотреть статистику работы**ACL** на **R1** при помощи команды **show access-lists**

R1# show access-lists

Standard IP access list STN_ACL_1

10 deny 172.16.11.0, wildcard bits 0.0.0.255 log (5 matches)

20 permit any (10 matches)

4. Настройка расширенных списков доступа

 На маршрутизаторе**R3** создать расширенный список доступа **EXT_ACL_1**.

R3(config)#ip access-list extended EXT_ACL_1

R3(config-ext-nacl)#deny ip 172.16.10.0 0.0.0.255 host 203.0.113.225

R3(config-ext-nacl)#permit ip any any

 Установить созданный список доступа**EXT_ACL_1** на маршрутизаторе **R3** для исходящего трафика через интерфейс **S0/0**

R3(config)#interface serial 0/0

R3(config-if)#ip access-group EXT_ACL_1 out

R3(config-if)#end

R3#copy run start

 Провфить работу **ACL** при помощи команды **ping**, используя параметр **source**

R3#ping 203.0.113.225 source 172.16.10.1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 203.0.113.225, timeout is 2 seconds:

Packet sent with a source address of **172.16.10.1**

U.U.U

Success rate is 0 percent (**0/5**)

 Просмотреть статистику работы**ACL** на **R3** при помощи команды **show access-lists**

R3# show access-lists

Extended IP access list EX_ACL_1

10 deny ip 172.16.10.0 0.0.0.255 host 203.0.113.225 (4 matches)

20 permit ip any any

5. Ограничение доступа к VTY при помощи ACL

 На маршрутизаторе**R2** создать стандартный список доступа **VTY_ACCESS_1**

R2(config)#ip access-list standard VTY_ACCESS_1

R2(config-std-nacl)#permit 172.16.12.0 0.0.0.255

 Установить ограничение доступа к**VTY** на маршрутизаторе **R2**

R2(config)#line vty 0 4

R2(config-line)#access-class VTY_ACCESS_1 in

 Проверить работу**ACL** при помощи команды **telnet**

R3# telnet 10.1.1.1

Trying 10.1.1.1 …

% Connection refused by remote host

R1# telnet 10.1.1.1 /source-interface f0/0

Trying 10.1.1.1 … Open

Unauthorized access strictly prohibited, violators will be prosecuted to the full extent of the law.

User Access Verification

Password:

Контрольные вопросы

1. Для чего применяются списки доступа?

2. Назовите особенности стандартных списков доступа

3. Назовите особенности расширенных списков доступа

4. Что подразумевается под «неявным запрещением» ?

5. Как обрабатываются правила в списках доступа содержащих множество правил?

Практическое занятие № 12

Тема: Настройка NAT-пула с перегрузкой и PAT
Цель выполнения работы: формирование профессиональных умений настраивать NAT на маршрутизаторах

Постановка задачи или ситуации:

По сценарию первой части лабораторной работы интернет-провайдер выделил вашей компании диапазон публичных IP-адресов 209.165.200.224/29. Благодаря этому компания получила шесть публичных IP-адресов. Перегрузка пула динамического NAT использует пул IP-адресов по модели «множество к множеству». Маршрутизатор использует первый IP-адрес в пуле и назначает подключения с помощью IP-адреса и уникального номера порта. После достижения на маршрутизаторе максимального количества преобразований для одного IP-адреса (для платформы и оборудования), используется следующий IP-адрес в пуле.

Во второй части интернет-провайдер выделил вашей компании один IP-адрес, 209.165.201.18, для подключения к Интернету от маршрутизатора Gateway к сети интернет-провайдера. Для преобразования нескольких внутренних адресов в один пригодный для использования публичный адрес используйте преобразование адресов портов (PAT). Вы выполните тестирование, отображение и проверку осуществления всех преобразований и проанализируете статистику NAT/PAT для контроля процесса.

Исходные данные

Топология сети

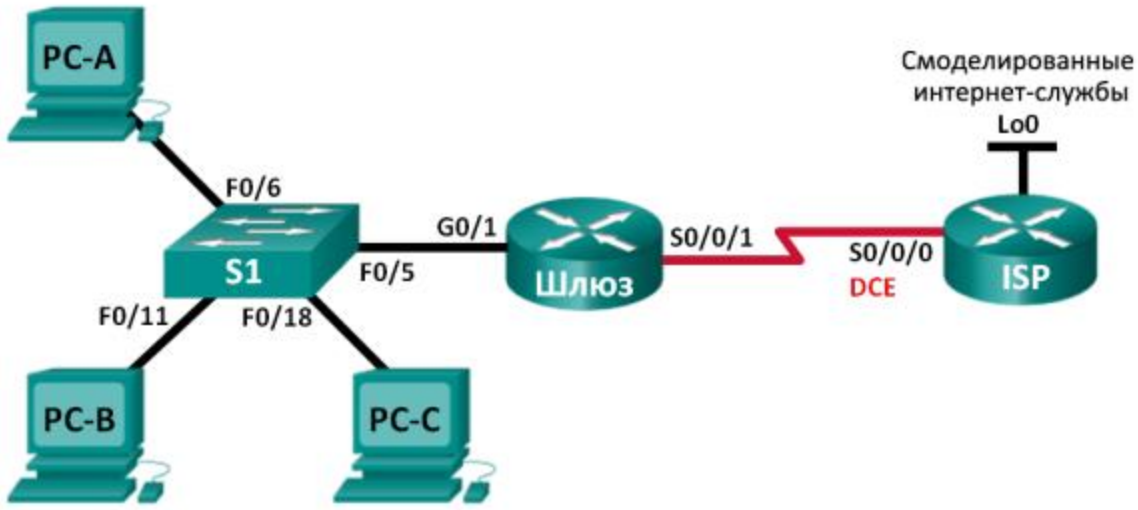


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
Gateway	G0/1	192.168.1.1	255.255.255.0	N/A
	S0/0/1	209.165.201.18	255.255.255.252	N/A
ISP	S0/0/0 (DCE)	209.165.201.17	255.255.255.252	N/A
	Lo0	192.31.7.1	255.255.255.255	N/A
PC-A	NIC	192.168.1.20	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.1.21	255.255.255.0	192.168.1.1
PC-C	NIC	192.168.1.22	255.255.255.0	192.168.1.1

Необходимые ресурсы:

- 2 маршрутизатора (Cisco 1941 под управлением ОС Cisco IOS 15.2(4) M3 (образ universal) или аналогичная модель);
- 1 коммутатор (Cisco 2960 под управлением ОС Cisco IOS 15.0(2), образ lanbasek9 или аналогичная модель);

- 3 компьютера (под управлением Windows 7, Vista или XP с программой эмуляции терминала, например Tera Term);
- консольные кабели для настройки устройств Cisco IOS через консольные порты;
- кабели Ethernet и последовательные кабели в соответствии с топологией.

Задачи

Часть 1. Построение сети и проверка подключения

Часть 2. Настройка и проверка NAT-пула с перегрузкой

Часть 3. Настройка и проверка преобразования PAT

Порядок выполнения

Часть 1: Построение сети и проверка подключения

В первой части вам предстоит настроить топологию сети и выполнить базовые настройки, например IP-адрес интерфейса, статическая маршрутизация, доступ к устройствам и пароли.

Шаг 1: Подключите кабели в сети в соответствии с топологией

Шаг 2: Настройте узлы ПК.

Шаг 3: Выполните инициализацию и перезагрузку маршрутизатора и коммутаторов.

Шаг 4: Настройте базовые параметры каждого маршрутизатора.

a. Отключите поиск DNS.

b. Настройте IP-адреса для маршрутизаторов, указанных в таблице адресации
c. Установите тактовую частоту на 128000 для всех последовательных интерфейсов DCE.
d. Присвойте имена устройствам в соответствии с топологией.
e. Назначьте cisco в качестве паролей консоли и VTY
f. Назначьте class в качестве зашифрованного пароля доступа к привилегированному режиму EXEC.

Шаг 5: Настройте статическую маршрутизацию.

a. Создайте статический маршрут от интернет-провайдера к маршрутизатору Gateway.
   ISP(config)# ip route 209.165.200.224 255.255.255.248 209.165.201.18

b. Создайте маршрут по умолчанию от маршрутизатора Gateway к маршрутизатору ISP
   Gateway(config)# ip route 0.0.0.0 0.0.0.0 209.165.201.17

Шаг 6: Проверьте сетевое соединение.

a. С узлов ПК отправьте эхо-запросы на интерфейс G0/1 на шлюзовом маршрутизаторе. Выявите и устраните неполадки, если эхо-запрос не проходит.
b. Проверьте настройку статических маршрутов на обоих маршрутизаторах.

Часть 2: Настройка и проверка NAT-пула с перегрузкой

Во второй части вам предстоит настроить маршрутизатор Gateway для преобразования IP-адреса из сети 192.168.1.0/24 в один из шести пригодных к использованию адресов в диапазоне 209.165.200.224/29.

Шаг 1: Создайте ACL-список, который соответствует диапазону частных IP-адресов локальной сети.

Для трансляции адресов из сети 192.168.1.0/24 используется ACL1.

Gateway(config)# access-list 1 permit 192.168.1.0 0.0.0.255

Шаг 2: Определите пул пригодных к использованию публичных IP-адресов.

Gateway(config)# ip nat pool public_access 209.165.200.225 209.165.200.230 netmask 255.255.255.248

Шаг 3: Определите соответствие в NAT внутреннего списка адресов источника и пула внешних адресов.

Gateway(config)# ip nat inside source list 1 pool public_access overload

Шаг 4: Задайте интерфейсы.

Выполните команды ip nat inside и ip nat outside на интерфейсах.

Gateway(config)# interface g0/1

Gateway(config-if)# ip nat inside

Gateway(config-if)# interface s0/0/1

Gateway(config-if)# ip nat outside

Шаг 5: Проверьте конфигурацию NAT-пула с перегрузкой.

a. Из каждого ПК отправьте эхо-запрос на адрес маршрутизатора интернет-провайдера — 192.31.7.1.
b. Отобразите статистику NAT по маршрутизатору Gateway.
   Gateway# show ip nat statistics
c. Отобразите преобразования NAT на маршрутизаторе Gateway.
   Gateway# show ip nat translations

Примечание. В зависимости от времени, истекшего с момента отправки эхо-запросов с каждого ПК, вы можете не увидеть все три преобразования. ICMP-преобразованиям характерны низкие значения лимита времени.

Сколько внутренних локальных IP-адресов указано в примере выходных данных выше?

Сколько указано внутренних глобальных IP-адресов?

Сколько номеров портов используется в паре с внутренними глобальными адресами

Что произойдёт в результате отправки эхо-запроса на внутренний локальный адрес компьютера PC-A от маршрутизатора интернет-провайдера? Почему?

Часть 3: Настройка и проверка преобразования PAT

В третьей части вам предстоит настроить PAT, используя интерфейс для определения внешних адресов вместо пула адресов. Не все команды из части 2 будут использоваться в части 3.

Шаг 1: Очистите преобразования NAT и статистику из маршрутизатора Gateway.

Шаг 2: Проверьте конфигурацию NAT.

a. Убедитесь, что статистика удалена.
b. Убедитесь, что внешние и внутренние интерфейсы настроены для преобразований NAT

c. Убедитесь, что ACL-список по-прежнему настроен для преобразований NAT.

Шаг 3: Удалите пул пригодных к использованию публичных IP-адресов.

Gateway(config)# no ip nat pool public_access 209.165.200.225 209.165.200.230 netmask 255.255.255.248

Шаг 4: Удалите NAT трансляцию между ACL-списком и пулом внешних адресов.

Gateway(config)# no ip nat inside source list 1 pool public_access overload

Шаг 5: Сопоставьте список источника с внешним интерфейсом.

Gateway(config)# ip nat inside source list 1 interface serial 0/0/1 overload

Шаг 6: Проверьте конфигурацию PAT.

a. Из каждого ПК отправьте эхо-запрос на адрес маршрутизатора интернет-провайдера — 192.31.7.1.
b. Отобразите статистику NAT по маршрутизатору Gateway.
   Gateway# show ip nat statistics

c. Отобразите преобразования NAT на Gateway.
   Gateway# show ip nat translations

Контрольные вопросы

1. Зачем используется NAT?

2. В чём заключаются преимущества PAT?
3. Как работает статический NAT?
4. Как работает динамический NAT?

Практическое занятие № 13

Тема: Настройка туннеля VPN GRE по схеме «точка-точка»
Цель выполнения работы: формирование профессиональных умений по настройке туннеля VPN GRE на маршрутизаторах

Теория

1. Книга Дж. Бони Руководство по Cisco IOS. Глава 13 Специальные темы IP-конфигурирования. Раздел Туннели, страница 322.

Постановка задачи или ситуации:

Задачи:

Часть 1. Базовая настройка устройств

Часть 2. Настройка туннеля GRE

Часть 3. Включение маршрутизации через туннель GRE

Универсальная инкапсуляция при маршрутизации (GRE) — это протокол туннелирования, способный инкапсулировать различные протоколы сетевого уровня между двумя объектами по общедоступной сети, например, в Интернете.

GRE можно использовать с:

- подключением сети IPv6 по сетям IPv4

- пакетами групповой рассылки, например, OSPF, EIGRP и приложениями потоковой передачи данных

В этой практической работе необходимо настроить незашифрованный туннель GRE VPN «точка- точка» и убедиться, что сетевой трафик использует туннель. Также будет нужно настроить протокол маршрутизации OSPF внутри туннеля GRE VPN. Туннель GRE существует между маршрутизаторами WEST и EAST в области 0 OSPF. Интернет-провайдер не знает о туннеле GRE. Для связи между маршрутизаторами WEST и EAST и интернет-провайдером применяются статические маршруты по умолчанию.

Необходимые ресурсы:

• 3 маршрутизатора (Cisco 1941 под управлением ОС Cisco IOS 15.2(4) M3 (образ universal) или аналогичная модель);

• 2 коммутатора (Cisco 2960 под управлением ОС Cisco IOS 15.0(2), (образ lanbasek9) или аналогичная модель);

• 2 ПК (под управлением ОС Windows 7, Vista или XP с программой эмуляции терминала, например Tera Term);

• консольные кабели для настройки устройств Cisco IOS через порты консоли;

• кабели Ethernet и последовательные кабели в соответствии с топологией.

Исходные данные

Топология

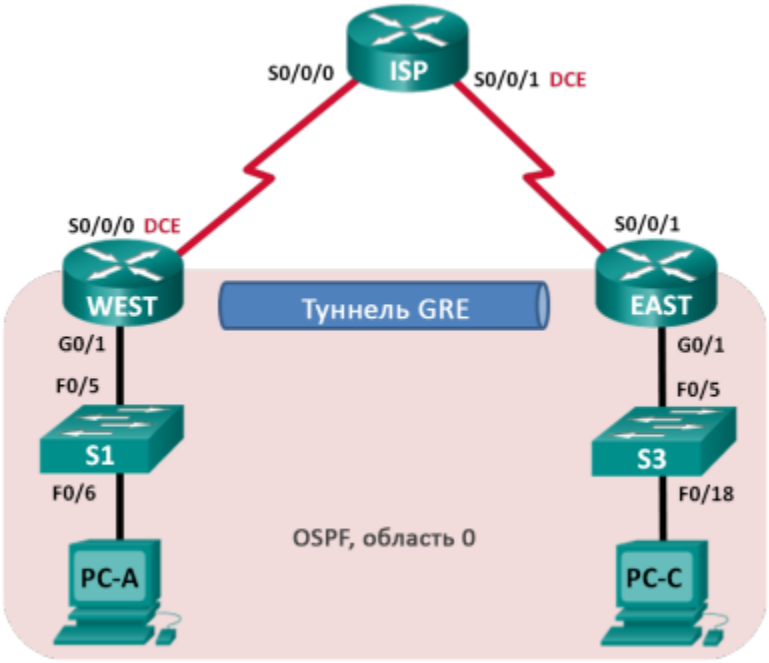


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
WEST	G0/1	172.16.1.1	255.255.255.0	Недоступно
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	Недоступно
	Tunnel0	172.16.12.1	255.255.255.252	Недоступно
ISP	S0/0/0	10.1.1.2	255.255.255.252	Недоступно
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	Недоступно
EAST	G0/1	172.16.2.1	255.255.255.0	Недоступно
	S0/0/1	10.2.2.1	255.255.255.252	Недоступно
	Tunnel0	172.16.12.2	255.255.255.252	Недоступно
PC-A	NIC	172.16.1.3	255.255.255.0	172.16.1.1
PC-C	NIC	172.16.2.3	255.255.255.0	172.16.2.1

Порядок выполнения

Часть 1: Базовая настройка устройств

В части 1 вам предстоит настроить топологию сети и базовые параметры маршрутизатора, например, IP-адреса интерфейсов, маршрутизацию, доступ к устройствам и пароли.

Шаг 1: Подключите кабели в сети в соответствии с топологией.

Шаг 2: Выполните инициализацию и перезагрузку маршрутизаторов и коммутаторов.

Шаг 3: Произведите базовую настройку маршрутизаторов.

a. Отключите поиск DNS
b. Назначьте имена устройств.
c. Зашифруйте незашифрованные пароли
d. Создайте баннерное сообщение дня (MOTD) для предупреждения пользователей о запрете несанкционированного доступа.
e. Назначьте class в качестве зашифрованного пароля доступа к привилегированному режиму.
f. Назначьте cisco в качестве пароля для консоли и виртуального терминала VTY и активируйте учётную запись.
g. Настройте ведение журнала состояния консоли на синхронный режим (*в cisco packet tracer этого не сделать).
h. Примените IP-адреса к интерфейсам Serial и Gigabit Ethernet в соответствии с таблицей адресации и активируйте физические интерфейсы. На данном этапе не настраивайте интерфейсы Tunnel0.
i. Настройте тактовую частоту на 128000 для всех последовательных интерфейсов DCE.

Шаг 4: Настройте маршруты по умолчанию к маршрутизатору интернет-провайдера.

WEST(config)# ip route 0.0.0.0 0.0.0.0 10.1.1.2

EAST(config)# ip route 0.0.0.0 0.0.0.0 10.2.2.2

Шаг 5: Настройте компьютеры.

Настройте IP-адреса и шлюзы по умолчанию на всех ПК в соответствии с таблицей адресации

Шаг 6: Проверьте соединение.

На данный момент компьютеры не могут отправлять друг другу эхо-запросы. Каждый ПК должен получать ответ на эхо-запрос от своего шлюза по умолчанию. Маршрутизаторы могут отправлять эхо- запросы на последовательные интерфейсы других маршрутизаторов в топологии. Если это не так, устраните неполадки и убедитесь в наличии связи.

Шаг 7: Сохраните текущую конфигурацию.

Часть 2: Настройка туннеля GRE

В части 2 необходимо настроить туннель GRE между маршрутизаторами WEST и EAST.

Шаг 1: Настройка интерфейса туннеля GRE.

a. Настройте интерфейс туннеля на маршрутизаторе WEST. Используйте S0/0/0 на маршрутизаторе WEST в качестве интерфейс источника туннеля и 10.2.2.1 как назначение туннеля на маршрутизаторе EAST.
   WEST(config)# interface tunnel 0

   WEST(config-if)# ip address 172.16.12.1 255.255.255.252

   WEST(config-if)# tunnel source s0/0/0

   WEST(config-if)# tunnel destination 10.2.2.1

b. Настройте интерфейс туннеля на маршрутизаторе EAST. Используйте S0/0/1 на маршрутизаторе EAST в качестве интерфейс источника туннеля и 10.1.1.1 как назначение туннеля на маршрутизаторе WEST.
   EAST(config)# interface tunnel 0

   EAST(config-if)# ip address 172.16.12.2 255.255.255.252

   EAST(config-if)# tunnel source 10.2.2.1

   EAST(config-if)# tunnel destination 10.1.1.1

Шаг 2: Убедитесь, что туннель GRE работает.

a. Проверьте состояние интерфейса туннеля на маршрутизаторах WEST и EAST.
   WEST# show ip interface brief

```
Interface                  IP-Address      OK? Method Status                Protocol
Embedded-Service-Engine0/0 unassigned      YES unset  administratively down down
GigabitEthernet0/0         unassigned      YES unset  administratively down down
GigabitEthernet0/1         172.16.1.1      YES manual up                    up
Serial0/0/0                10.1.1.1        YES manual up                    up
Serial0/0/1                unassigned      YES unset  administratively down down
Tunnel0                    172.16.12.1     YES manual up                    up
```

   EAST# show ip interface brief

```
Interface                  IP-Address      OK? Method Status                Protocol
Embedded-Service-Engine0/0 unassigned      YES unset  administratively down down
GigabitEthernet0/0         unassigned      YES unset  administratively down down
GigabitEthernet0/1         172.16.2.1      YES manual up                    up
Serial0/0/0                unassigned      YES unset  administratively down down
Serial0/0/1                10.2.2.1        YES manual up                    up
Tunnel0                    172.16.12.2     YES manual up                    up
```

b. С помощью команды show interfaces tunnel 0 проверьте протокол туннелирования, источник туннеля и назначение туннеля, используемые в этом туннеле. Какой протокол туннелирования используется? Какие IP-адреса источника и назначения туннеля связаны с туннелем GRE на каждом маршрутизаторе?
c. Отправьте эхо-запрос по туннелю из маршрутизатора WEST на маршрутизатор EAST с использованием IP-адреса интерфейса туннеля.
   WEST# ping 172.16.12.2

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.12.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/34/36 ms
```

d. С помощью команды **traceroute** на маршрутизаторе WEST определите тракт к интерфейсу туннеля на маршрутизаторе EAST. Укажите путь до маршрутизатора EAST.
e. Отправьте эхо-запрос и сделайте трассировку маршрута через туннель от маршрутизатора EAST к маршрутизатору WEST с использованием IP-адреса интерфейса туннеля. Укажите путь от маршрутизатора EAST до маршрутизатора WEST? С какими интерфейсами связаны эти IP-адреса? Почему?
f. Команды ping и traceroute должны успешно выполняться. Если это не так, устраните неполадки и перейдите к следующей части.

Часть 3: Включение маршрутизации через туннель GRE

В части 3 необходимо настроить протокол маршрутизации OSPF таким образом, чтобы локальные сети (LAN) на маршрутизаторах WEST и EAST могли обмениваться данными с помощью туннеля GRE.

После установления туннеля GRE можно реализовать протокол маршрутизации. Для туннелирования GRE команда network будет включать сеть IP туннеля, а не сеть, связанную с последовательным интерфейсом. точно так же, как и с другими интерфейсами, например, Serial и Ethernet. Следует помнить, что маршрутизатор ISP в этом процессе маршрутизации не участвует.

Шаг 1: Настройка маршрутизации по протоколу OSPF для области 0 по туннелю.

a. Настройте идентификатор процесса OSPF 1, используя область 0 на маршрутизаторе WEST для сетей 172.16.1.0/24 и 172.16.12.0/24.
   WEST(config)# router ospf 1

   WEST(config-router)# network 172.16.1.0 0.0.0.255 area 0

   WEST(config-router)# network 172.16.12.0 0.0.0.3 area 0

b. Настройте идентификатор процесса OSPF 1, используя область 0 на маршрутизаторе EAST для сетей 172.16.2.0/24 и 172.16.12.0/24.
   EAST(config)# router ospf 1

   EAST(config-router)# network 172.16.2.0 0.0.0.255 area 0

   EAST(config-router)# network 172.16.12.0 0.0.0.3 area 0

Шаг 2: Проверка маршрутизации OSPF.

a. Отправьте с маршрутизатора WEST команду show ip route для проверки маршрута к локальной сети 172.16.2.0/24 на маршрутизаторе EAST. Какой выходной интерфейс и IP-адрес используются для связи с сетью 172.16.2.0/24?
   WEST# show ip route

   …

```
      10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        10.1.1.0/30 is directly connected, Serial0/0/0
L        10.1.1.1/32 is directly connected, Serial0/0/0
      172.16.0.0/16 is variably subnetted, 5 subnets, 3 masks
C        172.16.1.0/24 is directly connected, GigabitEthernet0/1
L        172.16.1.1/32 is directly connected, GigabitEthernet0/1
O        172.16.2.0/24 [110/1001] via 172.16.12.2, 00:00:07, Tunnel0
C        172.16.12.0/30 is directly connected, Tunnel0
L        172.16.12.1/32 is directly connected, Tunnel0
```

b. Отправьте с маршрутизатора EAST команду для проверки маршрута к локальной сети 172.16.1.0/24 на маршрутизаторе WEST. Какой выходной интерфейс и IP-адрес используются для связи с сетью 172.16.1.0/24?

Шаг 3: Проверьте связь между конечными устройствами.

a. Отправьте эхо-запрос с ПК A на ПК C. Эхо-запрос должен пройти успешно. Если это не так, устраните неполадки и убедитесь в наличии связи между конечными узлами.
b. Запустите трассировку от ПК A к ПК C. Каков путь от ПК A до ПК C?

Контрольные вопросы

1. Какие еще настройки необходимы для создания защищенного туннеля GRE?
2. Если вы добавили дополнительные локальные сети к маршрутизатору WEST или EAST, то что нужно сделать, чтобы сеть использовала туннель GRE для трафика?

Практическое занятие № 14

Тема: Настройка сетей VPN
Цель выполнения работы: формирование профессиональных умений по настройке сетей VPN на маршрутизаторах

Постановка задачи или ситуации:

В этом задании необходимо на двух маршрутизаторах настроить поддержку межузловой сети VPN с использованием IPsec для трафика, проходящего между их соответствующими локальными сетями. IPsec-трафик VPN будет проходить через другой маршрутизатор, который не знает об использовании VPN. IPsec обеспечивает передачу конфиденциальной информации в защищённом режиме по незащищённым сетям, таким как Интернет. IPsec действует как протокол сетевого уровня, обеспечивая защиту и аутентификацию IP пакетов между участвующими в связи устройствами IPsec (равноправными узлами), такими как маршрутизаторы Cisco.

Задачи

Часть 0. Базовая настройка сети

Часть 1. Включение функций безопасности

Часть 2. Настройка параметров IPsec на маршрутизаторе R1

Часть 3. Настройка параметров IPsec на маршрутизаторе R3

Часть 4. Проверка работы VPN IPsec

Исходные данные (если имеются)

Топология

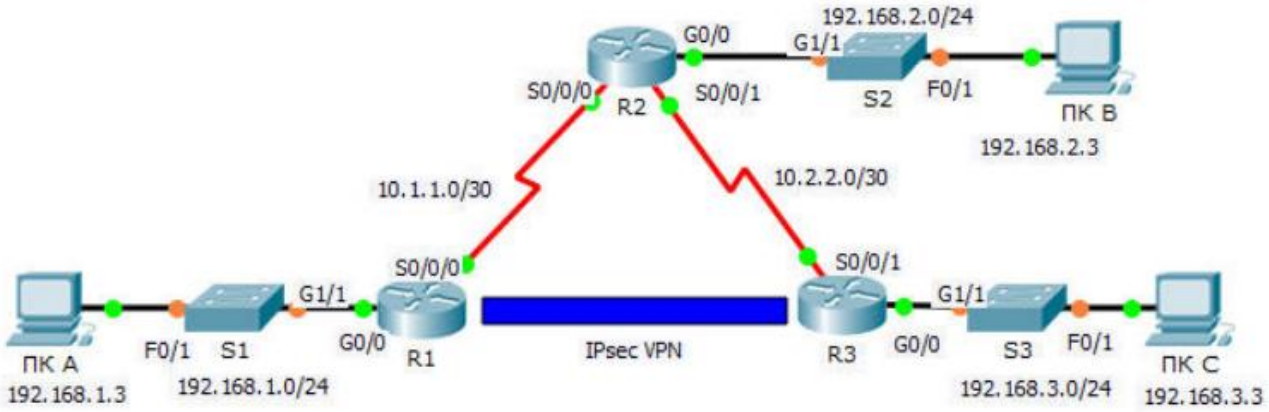


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1	G0/0	192.168.1.1	255.255.255.0	Недоступно
	S0/0/0	10.1.1.2	255.255.255.252	Недоступно
R2	G0/0	192.168.2.1	255.255.255.0	Недоступно
	S0/0/0	10.1.1.1	255.255.255.252	Недоступно
	S0/0/1	10.2.2.1	255.255.255.252	Недоступно
R3	G0/0	192.168.3.1	255.255.255.0	Недоступно
	S0/0/1	10.2.2.2	255.255.255.252	Недоступно
ПК A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
ПК B	NIC	192.168.2.3	255.255.255.0	192.168.2.1
ПК C	NIC	192.168.3.3	255.255.255.0	192.168.3.1

Параметры политики 1 фазы ISAKMP

Параметры		R1	R3
Метод распространения ключей	Вручную или с помощью **ISAKMP**	ISAKMP	ISAKMP
Алгоритм шифрования	**DES**, 3DES или AES	AES	AES
Алгоритм хеширования	MD5 или **SHA-1**	SHA-1	SHA-1
Метод аутентификации	Общие ключи или **RSA**	pre-share	pre-share
Обмен ключами	Группа DH **1**, 2 или 5	DH 2	DH 2
Время жизни IKE SA	86400 секунд или меньше	86400	86400
Ключ ISAKMP		cisco	cisco

Параметры по умолчанию выделены **полужирным** шрифтом. Другие параметры необходимо указать явным образом.

Параметры политики 2 фазы IPsec

Параметры	R1	R3
Набор преобразований	VPN-SET	VPN-SET
Имя узла пира	R3	R1
IP-адрес пира	10.2.2.2	10.1.1.2
Сеть, трафик которой шифруется	192.168.1.0/24	192.168.3.0/24
Имя для криптографического сопоставления (crypto map)	VPN-MAP	VPN-MAP
Установка SA	ipsec-isakmp	ipsec-isakmp

Порядок выполнения

Часть 0. Базовая настройка сети.

Шаг 1. Настройте адресацию согласно таблице адресации

Шаг 2. Настройте статическую маршрутизацию

Шаг 3. Проверьте настройки, выполнив ping от PC-A до PC-B, PC-C.

Часть 1: Включение функций безопасности

Шаг 1: Активируйте модуль securityk9.

Для выполнения этого задания должна быть включена лицензия пакета технологий обеспечения безопасности (Security) на маршрутизаторах R1 и R3.

a. Введите команду show version в пользовательском или привилегированном режиме, чтобы убедиться, что лицензия пакета технологий безопасности активирована.

```
-----------------------------------------------------------------
Technology    Technology-package          Technology-package
              Current       Type          Next reboot
-----------------------------------------------------------------
ipbase        ipbasek9      Permanent     ipbasek9
security      None          None          None
uc            None          None          None
data          None          None          None
```

b. Если это не так, активируйте модуль securityk9 для следующей загрузки маршрутизатора, примите лицензию, сохраните настройку и перезагрузите маршрутизатор.
R1(config)# **license boot module c2900 technology-package securityk9**

R1(config)# **end**

R1# **copy running-config startup-config**

R1# **reload**

c. После перезагрузки снова выполните команду show version для проверки активации лицензии пакета технологий безопасности.

```
Technology Package License Information for Module:'c2900'

-----------------------------------------------------------------
Technology    Technology-package          Technology-package
              Current       Type          Next reboot
-----------------------------------------------------------------
ipbase        ipbasek9      Permanent     ipbasek9
security      securityk9    Evaluation    securityk9
uc            None          None          None
data          None          None          None
```

d. Повторите шаги 1a-1c для маршрутизатора R3.

Часть 2: Настройте параметры IPsec на маршрутизаторе R1

Шаг 1: Проверьте связь.

Отправьте эхо-запрос с ПК A на ПК C.

Шаг 2: Определите интересующий трафик на маршрутизаторе R1.

Настройте ACL-список 110 таким образом, чтобы определить трафик из локальной сети на маршрутизаторе **R1** до локальной сети на маршрутизаторе **R3** как интересующий. Данный интересующий трафик будет активировать VPN IPsec при наличии трафика между локальными сетями маршрутизаторов **R1** и **R3**. Весь остальной трафик, передаваемый из этих локальных сетей, шифроваться не будет. Помните о действии неявного запрета «deny any» и о том, что добавлять данное правило в список не требуется.

R1(config)# **access-list 110 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255**

Шаг 3: Настройте параметры 1 фазы ISAKMP на маршрутизаторе R1.

Настройте на маршрутизаторе **R1** свойства криптографической политики ISAKMP **10**, а также общий ключ шифрования **cisco**. Конкретные параметры, подлежащие настройке, приведены в таблице настроек 1 фазы ISAKMP. Значения по умолчанию настраивать не нужно, поэтому требуется настроить только шифрование, способ обмена ключами и метод DH.

R1(config)# **crypto isakmp policy 10**

R1(config-isakmp)# **encryption aes**

R1(config-isakmp)# **authentication pre-share**

R1(config-isakmp)# **group 2**

R1(config-isakmp)# **exit**

R1(config)# **crypto isakmp key cisco address 10.2.2.2**

Шаг 4: Настройте параметры 2 фазы ISAKMP на маршрутизаторе R1.

Создайте набор преобразований (transform-set) **VPN-SET** для использования **esp-3des** и **esp-shahmac**. Затем создайте криптографическое сопоставление (crypto map) **VPN-MAP**, которое связывает вместе все параметры 2 фазы. Используйте порядковый номер **10** и определите его в качестве сопоставления **ipsec-isakmp.**

R1(config)# **crypto ipsec transform-set VPN-SET esp-3des esp-sha-hmac**

R1(config)# **crypto map VPN-MAP 10 ipsec-isakmp**

R1(config-crypto-map)# **description VPN connection to R3**

R1(config-crypto-map)# **set peer 10.2.2.2**

R1(config-crypto-map)# **set transform-set VPN-SET**

R1(config-crypto-map)# **match address 110**

R1(config-crypto-map)# **exit**

Шаг 5: Настройте криптографическое сопоставление для исходящего интерфейса.

Наконец, привяжите криптографическое сопоставление **VPN-MAP** к исходящему интерфейсу Serial 0/0/0.

R1(config)# **interface S0/0/0**

R1(config-if)# **crypto map VPN-MAP**

Часть 3: Настройка параметров IPsec на маршрутизаторе R3

Шаг 1: Настройте маршрутизатор R3 для поддержки сети VPN между площадками с маршрутизатором R1.

Теперь настройте параметры передачи на обоих направлениях маршрутизатора **R3**. Настройте ACL- список 110 так, чтобы определить трафик из локальной сети маршрутизатора **R3** до локальной сети маршрутизатора **R1** как интересующий.

R3(config)# **access-list 110 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255**

Шаг 2: Настройте параметры 1 фазы ISAKMP на маршрутизаторе R3.

Настройте на маршрутизаторе **R3** свойства криптографической политики ISAKMP **10**, а также общий ключ шифрования **cisco**.

R3(config)# **crypto isakmp policy 10**

R3(config-isakmp)# **encryption aes**

R3(config-isakmp)# **authentication pre-share**

R3(config-isakmp)# **group 2**

R3(config-isakmp)# **exit**

R3(config)# **crypto isakmp key cisco address 10.1.1.2**

Шаг 3: Настройте параметры 2 фазы ISAKMP на маршрутизаторе R1.

Аналогично действиям для маршрутизатора **R1**, создайте набор преобразований (transform-set) **VPN-SET** для **esp-3des** и **esp-sha-hmac**. Затем создайте криптографическое сопоставление (crypto map) **VPN-MAP**, которое связывает вместе все параметры 2 фазы. Используйте порядковый номер **10** и определите его в качестве сопоставления **ipsec-isakmp**.

R3(config)# **crypto ipsec transform-set VPN-SET esp-3des esp-sha-hmac**

R3(config)# **crypto map VPN-MAP 10 ipsec-isakmp**

R3(config-crypto-map)# **description VPN connection to R1**

R3(config-crypto-map)# **set peer 10.1.1.2**

R3(config-crypto-map)# **set transform-set VPN-SET**

R3(config-crypto-map)# **match address 110**

R3(config-crypto-map)# **exit**

Шаг 4: Настройте криптографическое сопоставление для исходящего интерфейса.

Наконец, привяжите криптографическое сопоставление VPN-MAP к исходящему интерфейсу Serial 0/0/1.

R3(config)# **interface S0/0/1**

R3(config-if)# **crypto map VPN-MAP**

Часть 4: Проверка работы VPN по IPsec

Шаг 1: Проверьте туннель до прохождения по нему интересующего трафика.

Введите команду **show crypto ipsec sa** на маршрутизаторе **R1**. Обратите внимание, что количество всех пакетов (инкапсулированных, зашифрованных, декапсулированных и дешифрованных) равно 0

R1# show crypto ipsec sa

```
interface: Serial0/0/0
    Crypto map tag: VPN-MAP, local addr 10.1.1.2

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
   remote  ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
   current_peer 10.2.2.2 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
   #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 0, #recv errors 0

     local crypto endpt.: 10.1.1.2, remote crypto endpt.:10.2.2.2
     path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
     current outbound spi: 0x0(0)
<Данные опущены>
```

Шаг 2: Создание интересующего трафика.

Отправьте на компьютер ПК С эхо-запрос от компьютера ПК А

Шаг 3: Проверьте туннель после прохождения интересующего трафика.

На маршрутизаторе R1 повторно введите команду **show crypto ipsec sa.** Теперь обратите внимание, что количество пакетов стало больше 0. Это означает, что туннель сети VPN по IPsec работает.

R1# show crypto ipsec sa

```
interface: Serial0/0/0
    Crypto map tag: VPN-MAP, local addr 10.1.1.2

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
   remote  ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
   current_peer 10.2.2.2 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 3, #pkts encrypt: 3, #pkts digest: 0
   #pkts decaps: 3, #pkts decrypt: 3, #pkts verify: 0
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 1, #recv errors 0

     local crypto endpt.: 10.1.1.2, remote crypto endpt.:10.2.2.2
     path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
     current outbound spi: 0x0A496941(172583233)
<Данные опущены>
```

Шаг 4: Создание не интересующего трафика.

Отправьте на ПК B эхо-запрос от ПК A.

Шаг 5: Проверка туннеля.

На маршрутизаторе R1 повторно введите команду **show crypto ipsec sa**. Наконец, обратите внимание, что количество пакетов не изменилось. Это означает, что не интересующий трафик не шифруется.

Контрольные вопросы

1. Для чего используется VPN?
2. Функции VPN-шлюза?
3. Требования к защищенному каналу?
4. Методы организации защищенного канала?
5. Что такое IPSec?
6. Режимы в IPSec?

Практическое занятие № 15

Тема: Настройка IP телефонии
Цель выполнения работы: формирование профессиональных умений по настройке IP телефонии

Исходные данные

Топология

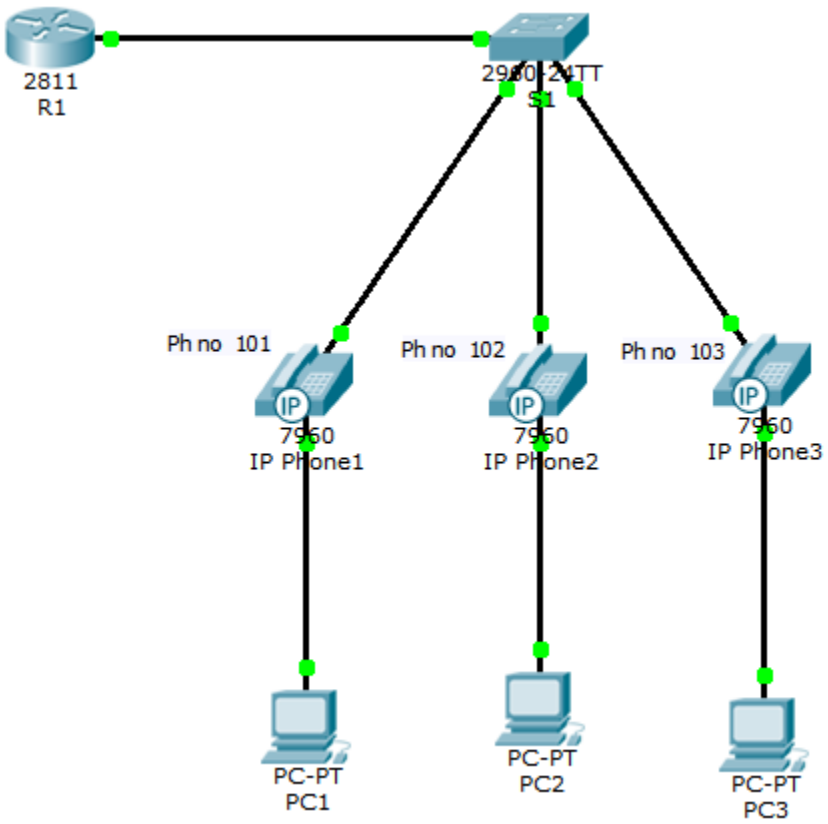


Таблица адресации

Устройство	Интерфейс	Подключен к	Адрес
R1	fa0/0	Fa0/1 (S1)	

	fa0/0.10	Fa0/1 (S1)	192.168.10.1/24
	fa0/0.20	Fa0/1 (S1)	192.168.20.1/24
	fa0/0.99	Fa0/1 (S1)	192.168.99.1/24
S1	fa0/1	Fa0/0 (R1)	
	fa0/2	IP Phone 1	
	fa0/3	IP Phone 2	
	fa0/4	IP Phone 3	
	Vlan99		192.168.99.10/24

Таблица VLAN

Номер	Имя	Описание
10	Data	Для потока данных от рабочих станций
20	Voice	Для потока данных IP телефонии
99	Management	Для управления

Маршрутизатор 2811

Коммутатор 2960

IP Phone

PC

Порядок выполнения

Часть 1. Базовая конфигурация.

Шаг 1. Собрать топологию.

Шаг 2. Настроить PC как DHCP-клиенты .

Часть 2. Настройка коммутатора

Шаг 1. Задать vlan на коммутаторе

S1(config)#vlan 10

S1(config-vlan)name Data

S1(config)#vlan 20

S1(config-vlan)name Voice

S1(config)#vlan 99

S1(config-vlan)name Management

S1(config)#int vlan 99

S1(config-if)#ip add 192.168.99.10 255.255.255.0

S1(config-if)#no sh

S1(config-if)#exit

S1(config)#ip default-gateway 192.168.99.1

Шаг 2. Настроить интерфейсы на коммутаторе

S1(config)#int fa0/1

S1(config-if)#switchport mode trunk

S1(config-if)#switchport trunk native vlan 99

S1(config-if)#no sh

S1(config)#int range fa0/2-4

S1(config-if-range)#switchport mode access

S1(config-if-range)#switchport access vlan 10

S1(config-if-range)#switchport voice vlan 20

S1(config-if-range)#no sh

Шаг 3. Настроить маршрутизатор

Настроить интерфейсы:

R1(config)#int fa0/0

R1(config-if)#no sh

R1(config)#int fa0/0.10

R1(config-subif)#encapsulation dot1Q 10

R1(config-subif)#ip add 192.168.10.1 255.255.255.0

R1(config)#int fa0/0.20

R1(config-subif)#encapsulation dot1Q 20

R1(config-subif)#ip add 192.168.20.1 255.255.255.0

R1(config)#int fa0/0.99

R1(config-subif)#encapsulation dot1Q 99 native

R1(config-subif)#ip add 192.168.99.1 255.255.255.0

Настроить DHCP сервер:

R1(config)# ip dhcp excluded-address 192.168.10.1 192.168.10.9

R1(config)# ip dhcp excluded-address 192.168.20.1 192.168.20.9

R1(config)#ip dhcp pool Data

R1(dhcp-config)#network 192.168.10.0 255.255.255.0

R1(dhcp-config)#default-router 192.168.10.1

R1(config)#ip dhcp pool Voice

R1(dhcp-config)#network 192.168.20.0 255.255.255.0

R1(dhcp-config)#default-router 192.168.20.1

R1(dhcp-config)#option 150 ip 192.168.20.1

Настроить Call Manager Express:

R1(config)# telephony-service

R1(config-telephony)# max-ephones 3

R1(config-telephony)#max-dn 3
R1(config-telephony)#ip source-address 192.168.20.1 port 2000

R1(config)# ephone-dn 1
R1(config-ephone-dn)# number 101

R1(config)# ephone-dn 2
R1(config-ephone-dn)# number 102

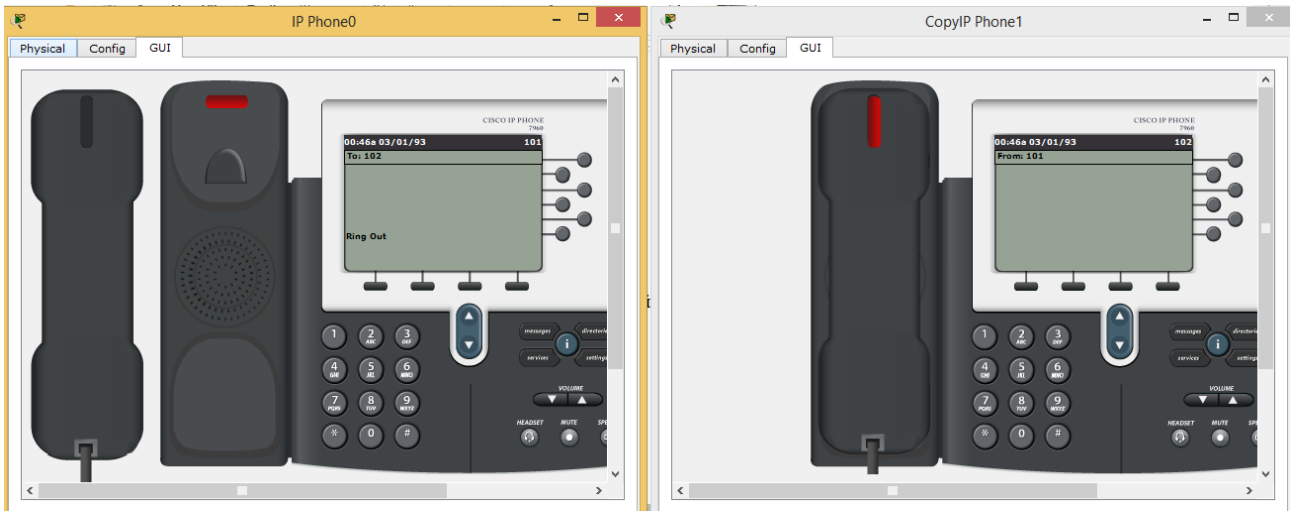
```
R1(config)# ephone-dn 3
R1(config-ephone-dn)# number 103

R1(config)# ephone 1
R1(config-ephone)#type 7960
R1(config-ephone)#button 1:1

R1(config)# ephone 2
R1(config-ephone)#type 7960
R1(config-ephone)#button 1:2

R1(config)# ephone 3
R1(config-ephone)#type 7960
```

R1(config-ephone)#button 1:3

Часть 3. Проверить конфигурацию.

Шаг 1. Проверить конфигурацию телефонов на маршрутизаторе командой: sh ephone.

Шаг 2. Выполнить тестовые звонки



Контрольные вопросы

1. Как расшифровывается VoIP?