МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра космического приборостроения и систем связи

УТВЕРЖДАЮ
Проректор по учебной работе
_____О. Г. Локтионова
«06» 03 2023

ОСНОВЫ УПРАВЛЕНИЯ ИНФОКОММУНИКАЦИОННЫМИ СИСТЕМАМИ

Лабораторный практикум по инфокоммуникационным технологиям для студентов направлений подготовки и специальностей в области информационных и инфокоммуникационных технологий

Курск 2023

УДК 654:004.7 (075.8)

Составитель: А. А. Чуев

Рецензент
кандидат технических наук, доцент,
доцент кафедры программной инженерии
Т. Н. Конаныхина

Основы управления инфокоммуникационными системами: лабораторный практикум по инфокоммуникационным технологиям для студентов направлений подготовки и специальностей в области информационных и инфокоммуникационных технологий / Юго-Зап. гос. ун-т; сост.: А. А. Чуев. – Курск, 2023. – 39 с.

Лабораторный практикум содержит материалы и методические указания, необходимые для выполнения лабораторных работ по изучению некоторых методик и технологий управления инфокоммуникационными системами и телекоммуникационным трафиком.

Полученные знания в результате выполнения лабораторных работ дадут возможность углубить компетенции по проведению расчетов сетей и систем инфокоммуникаций с использованием стандартных методов, приемов и средств автоматизации проектирования, а также могут быть использованы в будущей профессиональной деятельности выпускника, связанной с сетевыми технологиями и администрированиям инфокоммуникационных систем.

Практикум предназначен для студентов, обучающихся по направлениям подготовки бакалавриата и специальностям, входящим в группы специальностей и направлений подготовки 10.00.00 Информационная безопасность, 11.00.00 Электроника, радиотехника и системы связи, при формировании компетенций, связанных с взаимодействием инфокоммуникационных устройств, работающих на канальном и сетевом уровнях модели ISO/OSI.

Текст печатается в авторской редакции

Подписано в печать 06.03.23. Формат 60x841/16.
Усл. печ. л. 2,26. Уч.-изд. 2,05. Тираж 100 экз. Заказ 67. Бесплатно.
Юго-Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94

СОДЕРЖАНИЕ

Лабораторная работа
СТАТИЧЕСКАЯ МАРШРУТИЗАЦИЯ.....4
Лабораторная работа
ВИРТУАЛЬНАЯ ЧАСТНАЯ СЕТЬ (VPN).....11
Лабораторная работа
ОРГАНИЗАЦИЯ ПРОСТЕЙШЕГО VPN-СЕРВЕРА 27
Лабораторная работа
РЕЗЕРВИРОВАНИЕ КАНАЛОВ 34
Приложение А.....37

Лабораторная работа
СТАТИЧЕСКАЯ МАРШРУТИЗАЦИЯ

Цель работы: изучение понятия маршрутизации, сути и принципов работы статической маршрутизации, принципов построения вычислительных сетей с использованием маршрутизаторов в сетевом эмуляторе Cisco Packet Tracer.

Краткие теоретические сведения

При небольшом количестве подсетей, как правило, используется статическая маршрутизация. Статические маршруты не меняются самим маршрутизатором. Данный тип маршрутизации потребляет мало вычислительных ресурсов и полезна в сетях, которые не имеют нескольких путей к адресату назначения. Если от маршрутизатора к маршрутизатору есть только один путь, то часто используют статическую маршрутизацию.

Рассмотрим типичные примеры конфигурирования сети с использованием статической маршрутизации. Предположим, что структура сети имеет вид, показанный на рисунке 1.1.

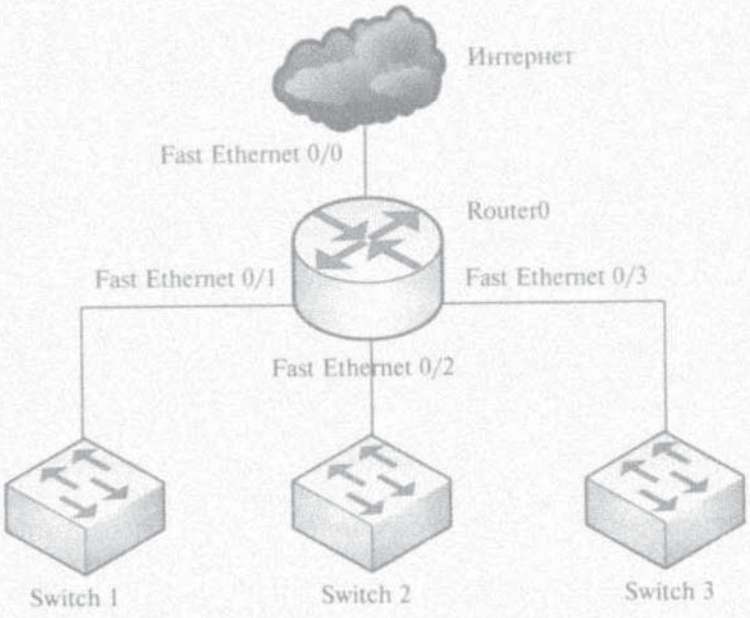

Рис.1.1. Структура сети

Из рисунка 1.1 следует, что сеть состоит их трех подсетей (это могут быть, например, три отдела предприятия). Разделения на подсети осуществляется с использованием маршрутизатора Router0, через него же

осуществляется доступ к сети Интернет. Каждая подсеть содержит коммутатор второго уровня емкостью 24 порта.

Предположим, что для адресации сети будет использоваться частный адрес 192.168.1.0/24, преобразование частных адресов в общедоступные будет осуществляться маршрутизатором в соответствии с протоколом NAT.

Каждая подсеть может содержать до 24 конечных узлов, плюс адрес интерфейса маршрутизатора, плюс два специальных адреса (для номера сети и широковещания), следовательно под адресацию узлов в каждой подсети необходимо отвести 5 разрядов (2^5=32). Оставшиеся 3 разряда четвертого байта можно использовать для адресации подсетей. Тогда маска подсети будет иметь вид: 11111111.11111111.11111111.11100000, или в десятичном формате: 255.255.255.224.

Тогда в нашей сети можно выделить 2^3=8 подсетей, из которых используем только три, а остальные можно оставить в резерве для будущее развития сети.

Подсетям назначим следующие адреса:

– 192.168.1.32/27;

– 192.168.1.64/27;

– 192.168.1.96/27.

Для конфигурирования статической маршрутизации в нашем примере портам маршрутизатора необходимо назначить сетевые адреса из диапазона адресного пространства перечисленных выше подсетей. Соответственно, порт FastEthernet, входящий в первую подсеть, получает адрес 192.168.1.33/27, во вторую – адрес 192.168.1.65/27, в третью – 192.168.1.97/27.

Компьютерам подсетей также необходимо задать соответствующие сетевые настройки. Этот процесс можно автоматизировать с применением протокола DHCP, или сконфигурировать конечные узлы вручную. В состав минимальных настроек узла входят: IP-адрес, маска подсети, а также адрес шлюза по умолчанию. В качестве шлюза по умолчанию в нашем примере для каждой из подсетей будет выступать маршрутизатор Router0, точнее, его интерфейс, включенный в подсеть.

Например, если конечные узлы работают под управлением ОС Windows, для конфигурирования необходимо зайти во вкладку «Подключение по локальной сети - Свойства» и выбрать пункт «Протокол

Интернета (TCP/IP)» (рисунок 1.2).

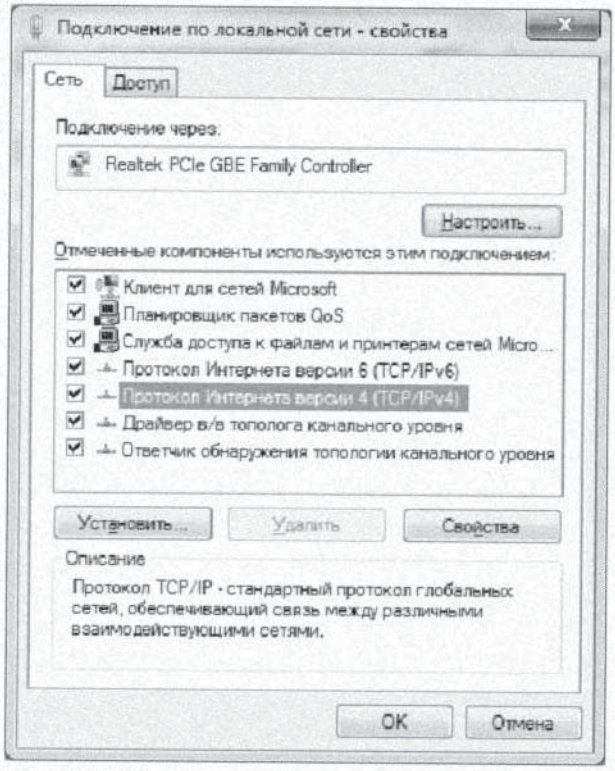

Рис.1.2. Конфигурирование конечного узла

В появившемся окне необходимо выделить пункт «Использовать следующий IP-адрес» и в соответствующие поля внести минимальную конфигурацию (рисунок 1.3).

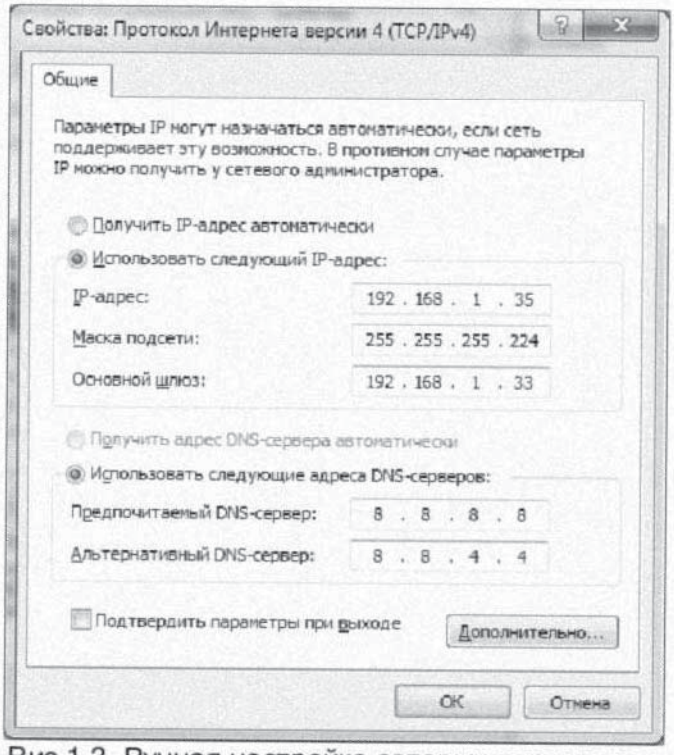

Рис.1.3. Ручная настройка сетевых параметров

На рисунке 1.3 представлен пример конфигурирования конечного узла, входящего в первую подсеть.

Конфигурирование интерфейсов маршрутизатора зависит от его модели. Например, для маршрутизатора Cisco набор команд конфигурирования будет иметь следующий вид:

`Router0>` **`enable`** – переход в привилегированный режим;

`Router0#` **`configure terminal`** – вход в режим глобального конфигурирования;

`Router0 (conf)#` **`interface fastEthernet 0/1`** – переход к конфигурированию конкретного интерфейса (в данном случае, интерфейса fastEthernet 0/1);

`Router0 (conf-if)#` **`ipaddress 192.168.1.33 255.255.255.224`** – назначение интерфейсу IP- адреса (с указанием маски).

Для того чтобы пакеты отправлялись во внешнюю сеть, пересылались на порт FastEthernet 0/0, необходимо прописать *маршрут по умолчанию*:

`Router0 (conf)#` **`interface fast ethernet 0/0`** ;

`Router0 (conf-if)#` **`ip route 0.0.0.0 0.0.0.0`** <адрес порта fast ethernet 0/0 или выходной интерфейс маршрутизатора>.

В обобщенном виде запись маршрутного правила (далее маршрута) можно представить так:

`ip route network netmask gateway`

Например, конкретная запись может быть представлена как:

`ip route 12.5.7.0 255.255.255.0 78.3.65.1` ,

где 12.5.7.0 – это адрес подсети (network), 255.255.255.0 – маска данной подсети (netmask), а 78.3.65.1 – адрес шлюза (gateway). Шлюз представляет собой маршрутизатор, на который посылается весь трафик, удовлетворяющий данному маршруту, т. е. имеющий адрес получателя пакетов входящий в указанную подсеть.

Конфигурирование статической маршрутизации в нашем простейшем примере можно считать законченным.

После настройки всех маршрутизаторов сети необходимо проверить связь между компьютерами командой *ping*, *traceroute*. Если связь есть – все настройки сделаны верно, в противном случае, чтобы убедиться в том, что маршрутизатор действительно правильно сконфигурирован и работает корректно, просмотрите таблицу маршрутизации роутера, используя команду *show* следующим образом:

```
Router0# show ip route
```

Пример успешного прохождения трафика показан на рисунке 1.4.

```
bash-3.2$ traceroute 10.0.0.100
traceroute to 10.0.0.100 (10.0.0.100), 64 hops max, 52 byte packets
 1  172.16.0.1 (172.16.0.1)  0.451 ms  0.181 ms  0.173 ms
 2  32.1.1.1 (32.1.1.1)  0.790 ms  0.571 ms  0.558 ms
 3  10.0.0.100 (10.0.0.100)  0.616 ms  0.514 ms  0.516 ms
bash-3.2$
```

Рис.1.4. Проверка связи между компьютерами командой traceroute

Исходные данные для выполнения лабораторной работы

Корпоративная сеть разбита на десять подсетей, из них в данный момент задействовано пять подсетей в пяти разных подразделениях организации.

Состав сети:

– три маршрутизатора;

– пять коммутаторов (по одному в каждом отделе на подсеть);

– один компьютер в каждой сети.

Задание на лабораторную работу

Внимание! Работа выполняется индивидуально. Номер варианта соответствует порядковому номеру студента в журнале преподавателя.

1. Изучить методические указания к лабораторной работе.

2. Рассчитать параметры подсетей и задать на компьютерах IP-адрес, маску и шлюз в каждой отдельной подсети. Исходный диапазон адресов зависит от варианта (табл. 1.1).

Табл. 1.1. Исходные данные для выполнения задания

Вар.	Диапазон адресов	Вар.	Диапазон адресов	Вар.	Диапазон адресов
1	15.0.0.0/8	11	18.0.0.0/8	21	35.0.0.0/8
2	46.30.0.0/16	12	18.46.0.0/16	22	30.28.0.0/16
3	16.0.0.0/8	13	19.25.0.0/16	23	15.28.0.0/16
4	28.46.0.0/16	14	16.10.0.0/16	24	28.15.0.0/16
5	46.19.0.0/16	15	17.0.0.0/8	25	25.30.0.0/16
6	19.0.0.0/8	16	20.20.0.0/16	26	30.0.0.0/8
7	28.0.0.0/8	17	8.28.0.0/16	27	46.15.0.0/16
8	20.30.0.0/16	18	26.0.0.0/8	28	28.18.0.0/16
9	16.30.0.0/16	19	25.28.0.0/16	29	30.30.0.0/16
10	20.0.0.0/8	20	15.15.0.0/16	30	20.19.0.0/16

3. Создать произвольную топологию сети, соединив маршрутизаторы с подсетями в любом порядке. При этом соединить

роутеры между собой напрямую.

4. Настроить статические маршруты так, чтобы компьютеры во всех подсетях были доступны друг другу.

5. Проверить работоспособность корпоративной сети командой ping. Проверять доступность следует между компьютерами, разделенными двумя маршрутизаторами.

6. Оформить отчет по лабораторной работе и подготовиться к его защите. Для подготовки рекомендуется ответить на контрольные вопросы.

Внимание! В отчете о выполнении работы все итерации выполнения задания должны быть подкреплены достаточным количеством скриншотов. На скриншотах требуется указать IP-адреса и другие настроенные параметры.

Контрольные вопросы и задания

1. Что такое маршрутизация?
2. На какие два вида делится маршрутизация?
3. В чем преимущества статической маршрутизации?
4. Дайте характеристику параметрам статической таблицы маршрутизации.
5. Какие этапы при установке устройства присущи маршрутизаторам компании Cisco, но отсутствуют у коммутаторов?
6. Какую из указанных ниже команд можно встретить в интерфейсе командной строки маршрутизатора, но не коммутатора?

а) команда clock rate;

б) команда ip address маска адрес;

в) команда ip address dhcp;

г) команда interface vlan 1

7. Чем отличаются интерфейсы командной строки маршрутизатора и коммутатора компании Cisco?
8. Какая из указанных ниже команд не покажет настройки IP-адресов и масок в устройстве?

а) show running-config;

б) show protocol тип номер;

в) show ip interface brief;

г) show version

9. Перечислите основные функции маршрутизатора в соответствии с уровнями модели OSI.
10. Перечислите основные технические характеристики

маршрутизаторов.

11. Приведите перечень протоколов маршрутизации и дайте им краткие характеристики.

Перечень необходимого материально-технического оборудования

Выполнение лабораторной работы предполагается в учебной лаборатории сетевых технологий кафедры космического приборостроения и систем связи. Учебная лаборатория должна быть оснащена:

– учебной мебелью (столы и стулья для обучающихся, в количестве не меньше списочного состава студентов, стол и стул для преподавателя);

– доской;

– учебными компьютерами (в количестве не менее 1 устройство на 2 студентов), с установленными операционной системой Windows, программным продуктом Cisco Packet Tracer и программным продуктом LibreOffice (для составления отчета о выполнении работы).

Лабораторная работа
ВИРТУАЛЬНАЯ ЧАСТНАЯ СЕТЬ (VPN)

Цель работы: изучение принципов работы технологии «Виртуальная частная сеть», приобретения навыков конфигурирования виртуальных соединений в операционной системе Cisco в сетевом эмуляторе Cisco Packet Tracer.

Краткие теоретические сведения

Основные понятия

Виртуальная частная сеть (VPN – Virtual Private Network) это логическая сеть, которая создается на базе общедоступной сети Интернет. Благодаря использованию средств криптографии уровень доверия к построенной логической сети не зависит от уровня доверия к сетям, на основе которых она построена, даже если коммуникация осуществляется по ненадежным публичным сетям. Огромное преимущество такой структуры в том, что ее создание на базе существующей сети значительно снижает расходы на покупку нового аппаратного обеспечения. VPN может гарантировать, что направляемый через Интернет трафик будет в безопасности, как будто передается внутри изолированной от локальной сети.

Концепция построения защищенных виртуальных частных сетей основывается на простой идее, которая заключается в следующем: если в глобальной сети есть два узла, которым необходимо обмениваться информацией (при этом важно обеспечить конфиденциальность и целостность данных), то между ними нужно создать виртуальный туннель. Туннель должен отвечать требованию чрезвычайной труднодоступности к нему всеми возможными внешними наблюдателями.

VPN может обеспечить соединения трех типов: «точка-точка», «точка-сеть», «сеть-сеть», которые также могу называться туннелем. Туннель создаётся в незащищённой сети, в качестве которой чаще всего выступает Интернет. Название «точка-точка» означает, что соединение устанавливается между двумя компьютерами, «сеть-сеть» – между двумя маршрутизаторами. В любом случае конечные устройства называются узлами. Каждый узел отвечает за кодирование информации перед отправкой в туннель и декодирование при приеме.

Независимо от используемого ПО, все VPN работают по следующим принципам:

а) Каждый из узлов идентифицирует друг друга перед созданием соединения, чтобы шифрованные данные передавались на нужный узел.

б) На обоих узлах необходимо наличие заранее настроенной политики безопасности, указывающей какие протоколы могут использоваться для шифрования и обеспечения целостности данных.

в) Узлы сверяют политики, чтобы договориться об используемых алгоритмах. Если этого не происходит то туннель не устанавливается.

г) Когда соглашение по применяемым алгоритмам достигнуто, создается ключ, в дальнейшем используемый в симметричном алгоритме для кодирования и декодирования данных.

Компоненты VPN

Виртуальная частная сеть состоит из четырех ключевых элементов, которые реализуют соответствие требованиям по безопасности, производительности и способности к взаимодействию с другими сетями: сервер VPN, алгоритм шифрования, система аутентификации, протокол VPN. Далее рассмотрим более подробно каждый из этих элементов.

Сервер VPN представляет собой компьютер или маршрутизатор, выступающий в роли конечного узла соединения VPN. Сервер должен иметь характеристики, достаточные для поддержки, ожидаемой на него нагрузки.

Алгоритм шифрования, используемый в виртуальных частных сетях должен быть достаточно мощным. Это единственное предъявляемое к нему требование, поэтому все стандартные и мощные алгоритмы могут эффективно использоваться при построении VPN. Выбор того или иного алгоритма зависит исключительно от предпочтений по программированию и назначения системы.

Система аутентификации VPN обязательно должна быть двухфакторной. Пользователи могут проходить аутентификацию с помощью пароля, электронного ключа или с помощью какого либо способа идентификации личности.

Протокол VPN оказывает влияние на общий уровень безопасности системы. Он определяет, каким образом виртуальная сеть взаимодействует с другими системами в Интернете, используется для

обмена ключами шифрования между конечными узлами, а также определяет уровень защищенности трафика. В случае слабой защиты трафика он может быть перехвачен и затем расшифрован, делая виртуальную частную сеть бесполезной.

Все существующие протоколы, защиты виртуальных сетей подразделяются на два вида и всегда работают в паре:

– протоколы, инкапсулирующие данные и формирующие VPN-соединение;

– протоколы, шифрующие данные внутри созданного туннеля.

IP Security

IP Security – это набор протоколов, разработанный как базовый протокол обеспечения безопасности на уровне IP-соединения. IPSec дополняет использующийся сейчас сетевой протокол IPv4 и является частью перспективного протокола IPv6. Возможности, предоставляемые IPSec, обеспечивают контроль доступа, криптографическое кодирование передаваемых пакетов, проверку их целостности и подлинности, защиту от повторных сообщений, конфиденциальность данных, аутентификацию источника, а также частичную защиту от анализа трафика.

Архитектура средств безопасности информационного обмена IPSec состоит из трех уровней (рис. 2.1).

На верхнем уровне расположены:

– протокол согласования параметров виртуального канала и управления ключами (ISAKMP), задачей которого является общее управление виртуальным соединением, в том числе согласование используемых алгоритмов криптозащиты, а также генерация и распределение ключевой информации;

– протокол аутентифицирующего заголовка (AH), выполняющий функции аутентификации источника данных, проверки подлинности и целостности после приема, а также защиты от навязывания повторных сообщений;

– протокол инкапсулирующей защиты содержимого (ESP) – обеспечивает криптографическое закрытие передаваемых пакетов сообщений и, при необходимости, может выполнять всех функции протокола аутентифицирующего заголовка (AH).

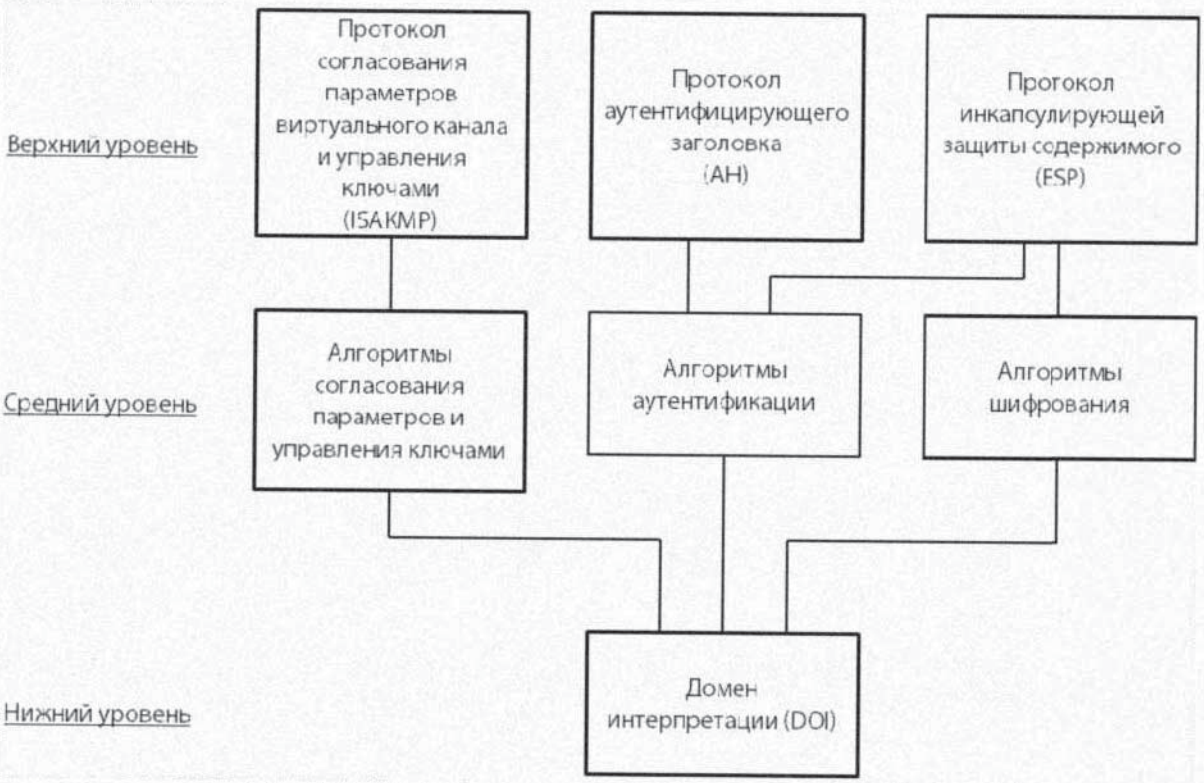

Рис.2.1. Архитектура средств безопасности IPSec

Средний уровень архитектуры средств безопасности IPSec составляют алгоритмы шифрования и аутентификации, используемые в протоколах аутентифицирующего заголовка (AH) и инкапсулирующей защиты содержимого (ESP). Также к этому уровню относятся алгоритмы согласования параметров и управления ключами, применяемые в протоколе ISAKMP. Протоколы защиты виртуального канала верхнего уровня архитектуры IPSec (AH и ESP) не зависят от конкретных криптографических алгоритмов, а значит в них могут применяться любые методы аутентификации, типы ключей (несимметричные или симметричные), алгоритмы шифрования и распределения ключей.

Из-за независимости алгоритмов протоколов AH и ESP требуется предварительное согласование набора применяемых алгоритмов и их параметров, поддерживаемых взаимодействующими сторонами. Эта функция возлагается на протокол ISAKMP, который контролирует создание взаимодействующими сторонами общего контекста безопасности (SA) при формировании защищённого виртуального канала. Затем используются элементы созданного контекста, такие как ключи и алгоритмы.

Нижний уровень архитектуры IPSec состоит из домена интерпретации (DOI), который хранит сведения об используемых в IPSec протоколах и алгоритмах, их параметрах, протокольных идентификаторах

и т.п. Существование DOI необходимо из-за возможности использования в IPSec алгоритмов и протоколов, изначально не предназначенных для этой архитектуры и именно домен интерпретации обеспечивает их совместную работу. Для того чтобы в качестве алгоритмов аутентификации и шифрования в протоколах AH и ESP можно было использовать алгоритмы, соответствующие национальным стандартам, их необходимо зарегистрировать в DOI.

В настоящий момент для протоколов AH и ESP зарегистрировано два стандартных алгоритма аутентификации: HMAC-MD5 (Hashed Message Authentication Code – Message Digest version 5) и HMAC-SHA1 (Hashed Message Authentication Code – Secure Hash Algorithm version 1). Это алгоритмы аутентификации с секретным ключом. Если секретный ключ известен только принимающей и передающей сторонам, это обеспечит аутентификацию источника данных и целостность пакетов, пересылаемых между сторонами. Для обеспечения совместимости работы оборудования по умолчанию на начальной стадии реализации протокола IPSec принято использовать алгоритм аутентификации HMAC-MD5.

Протоколы AH и ESP поддерживают работу в двух режимах:

– туннельном, при котором IP-пакеты защищаются целиком вместе с заголовками;

– транспортном, обеспечивающим полную защиту только содержимого IP-пакетов.

Основным режимом является туннельный. При работе в этом режиме каждый обычный IP-пакет помещается в конверт IPSec целиком в криптозащищенном виде, а тот, в свою очередь, инкапсулируется в другой IP-пакет. Туннельный режим обычно реализуют на специально выделенных защитных шлюзах, в роли которых могут выступать маршрутизаторы или межсетевые экраны. Туннелирование IP-пакетов полностью прозрачно для обычных компьютеров в локальных сетях, являющихся держателями туннелей.

В транспортном режиме в конверт IPSec в криптозащищённом виде помещается только содержимое исходного IP-пакета и к полученному конверту добавляется исходный IP-заголовок. Соответственно в транспортном режиме заголовок IPSec размещается между IP-заголовком и транспортным (TCP или UDP) заголовками обычного IP-пакета. Транспортный режим быстрее туннельного и разработан для применения

на оконечных системах. Данный режим может применяться на шлюзах для защиты внутренних связей между одноранговыми сетями. Работа в транспортном режиме отражается на всех системах, входящих в группу защищенного взаимодействия, и в большинстве случаев требует перепрограммирования сетевых приложений.

Настройка протокола безопасности IPSec

Устройства Cisco для поддержки VPN используют набор протоколов IPSec, играющего сегодня роль промышленного стандарта обеспечения широких возможностей VPN. Действия IPSec основаны на целом ряде технологических решений и методов шифрования, но обобщенно их можно представить в виде пяти этапов, описанных ниже (рис.2.2).

Первый этап «Начало процесса IPSec». Этап начинается с создания на каждом узле контекста безопасности. Затем этот контекст реализуется в виде команд конфигурации интерфейсов устройств на каждой стороне IPSec. В маршрутизаторах Cisco для определения трафика, подлежащего шифрованию, используют списки доступа, которые реализуют политику шифрования. Когда подлежащий шифрованию трафик генерируется клиентом IPSec или проходит через него, клиент инициирует следующий этап процесса, начиная первую фазу IKE.

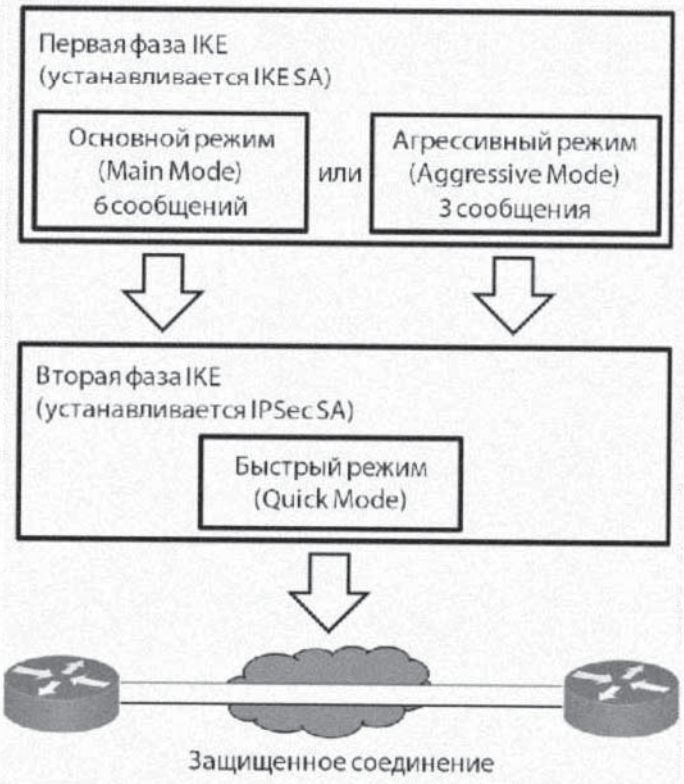

Рис.2.2. Этапы работы IPSec (фазы IKE)

Второй этап «Первая фаза IKE». Обмен данными на этом этапе необходим для аутентификации сторон IPSec и создания защищенного канала между сторонами, позволяющего начать обмен IKE. В ходе первой фазы IKE выполняются следующие действия.

а) Для обеспечения защиты обмена IKE проводятся переговоры о согласовании политики контекстов безопасности IKE между сторонами. Контекст IKE получает согласованные параметры и является двусторонним.

б) В результате аутентифицированного обмена Диффи–Хеллмана, выбирается общий секретный ключ для использования в алгоритмах шифрования IPSec.

в) Выполняется аутентификация и обеспечивается защита обеих сторон IPSec.

г) Формируется защищенный туннель для ведения переговоров о параметрах второй фазы IKE.

Третий этап «Вторая фаза IKE (QuickMode)». На этом этапе происходит согласование параметров контекста безопасности IPSec для создания IPSec-туннеля. В этой фазе выполняются следующая последовательность действий.

а) Ведутся переговоры о параметрах IPSec SA, защищаемых существующим контекстом безопасности IKE.

б) Устанавливаются контексты безопасности IPSec.

в) Периодически возобновляются переговоры о контекстах безопасности IPSec, что обеспечивает более надежную защиту.

г) При необходимости может выполняться дополнительный обмен Диффи–Хеллмана.

Вторая фаза IKE проходит только в быстром режиме, после того как в результате первой фазы IKE формируется защищенный туннель. После чего ведутся переговоры о согласованной политике IPSec, извлекается общий секретный материал для работы алгоритмами защиты IPSec и создаются IPSec SA. В быстром режиме выполняется обмен оказиями, которые используются для того, чтобы гарантировать создание уникальных секретных ключей и не допустить проведения атак воспроизведения, в результате которых злоумышленник мог бы создать «фальшивые» контексты безопасности.

Четвертый этап «Передача данных». После завершения второй фазы

IKE и создания IPSec SA в быстром режиме, начинается передача трафика по туннелю IPSec, связывающему стороны. Пакеты шифруются и дешифруются с помощью алгоритмов шифрования и ключей, указанных контекстом безопасности IPSec. IPSec SA задает также предел времени своего существования в килобайтах передаваемых данных или в секундах. Контекст безопасности имеет специальный счетчик, значение которого уменьшается на единицу за каждую секунду или после передачи каждого килобайта данных.

Пятый этап «Завершение работы туннеля IPSec». Контексты безопасности IPSec завершают свою работу либо по причине их удаления, либо потому, что оказывается превышен предел времени их существования. После прекращения работы контекстов, соответствующие им ключи также становятся недействительными. Если для потока данных требуются новые IPSec SA, в рамках протокола IKE снова инициируется обмен второй фазы, а при необходимости, и первой. В результате успешного их завершения создаются новые ассоциации защиты и новые ключи. Новые ассоциации защиты могут создаваться и до истечения времени существования предыдущих, чтобы поток данных мог двигаться непрерывно. Обычно проведение переговоров второй фазы требуется чаще, чем переговоров первой фазы.

Порядок выполнения лабораторной работы

В процессе настройки средств Cisco IOS для использования заранее согласованных ключей IKE в маршрутизаторах Cisco должны быть решены следующих четыре задачи.

Задача 1. Подготовка к использованию IPSec. Для успешного построения сети IPSec прежде чем приступить непосредственно к настройке маршрутизаторов, требуется предварительное планирование. Оно должно начинаться с определения контекста безопасности IPSec на основе требований общей политики защиты компании. В процессе планирования выполняются следующие основные шаги.

Шаг 1. Определение политики IKE взаимодействия сторон IPSec (первая фаза IKE), в зависимости от числа сторон и их размещения.

Шаг 2. Определение политики IPSec для учета параметров сторон IPSec (вторая фаза IKE), в частности IP–адресов и режимов IPSec.

Шаг 3. Проверка текущей конфигурации с помощью команд write terminal, show isakmp, show crypto map и других команд show.

Шаг 4. Проверка работоспособности сети при деактивированных средствах шифрования (с помощью команды ping к месту назначения).

Шаг 5. Проверка того, что списки доступа, определяющие фильтрацию пакетов, разрешают движение трафика IPSec.

Задача 2. Настройка IKE. Следующей задачей настройки IPSec явля-ется выбор параметров IKE в соответствии с той информацией о сети, которая была выяснена ранее. Процесс настройки IKE состоит из следующих шагов.

Шаг 1. Первым шагом настройки IKE является его активизация. Активизировать IKE глобально можно с помощью команды crypto isakmp enable, отменить использование IKE – с помощью той же команды с префиксом no. По умолчанию протокол IKE активизирован. Необходимость активизировать IKE для каждого интерфейса маршрутизатора отсутсвует, т. к. протокол активизируется глобально для всех интерфейсов. Если какие либо интерфейсы не используются IPSec, IKE на них можно отключить с помощью операторов списка доступа, запрещающих использование UDP-порта 500 (тем самым обеспечивается защита от атак блокирования сервиса).

Шаг 2. Создание политик IKE. Следующим шагом настройки IKE является определение набора политик IKE, используемых при создании связей IKE между сторонами IPSec. Политика определяет набор параметров, необходимых для построения ISAKMP-туннеля, через который затем будут передаваться параметры основного IPSec-туннеля. Политика указывает используемый алгоритм шифрования, алгоритм хеширования, метод аутентификации и параметры обмена ключами. Все используемые элементы политики IKE перечислены в таблице 2.1. Настройка политики IKE на маршрутизаторе Cisco представлена на рисунке 2.3.

Табл.2.1. Политика IKE для двух маршрутизаторов

Параметр	Значение для маршрутизатора 1	Значение для маршрутизатора 2
Алгоритм шифрования сообщений	3DES	3DES
Алгоритм гарантии целостности (алгоритм хэширования) сообщений	MD5	MD5
Метод аутентификации сторон	Согласованный ключ (pre-shared key)	Согласованный ключ (pre-shared key)

Параметры обмена ключами (идентификатор группы Диффи–Хеллмана)	Группа 2 (1024–битовый вариант алгоритма Диффи– Хеллмана)	Группа 2 (1024–битовый вариант алгоритма Диффи–Хеллмана)
Предел времени существования ассоциаций защиты, установленных с помощью ISAKMP	86400 (по умолчанию)	86400 (по умолчанию)
IP–адрес стороны IPSec	91.240.210.120	185.22.174.42

```
router1(config)#crypto isakmp policy 1
router1(config-isakmp)#encryption 3des
router1(config-isakmp)#hash md5
router1(config-isakmp)#authentication pre-share
router1(config-isakmp)#group 2
router1(config-isakmp)#lifetime 86000
router1(config-isakmp)#exit
router1(config)#
```

Рис.2.3. Настройка политики IKE на маршрутизаторе

Шаг 3. После настройки политики происходит создание согласованного ранее pre-shared key, и который был указан в методе аутентификации, и указывается адрес роутера, с которым создается VPN-соединение. Данные настройки производятся командой: crypto isakmp key cisco address 185.22.174.42.

Шаг 4. Завершающим этапов второй задачи является проверка конфигурации IKE с помощью команды show crypto isakmp policy (рис. 2.4).

```
router1#show crypto isakmp policy
Global IKE policy
Protection suite of priority 1
        encryption algorithm:   Three key triple DES
        hash algorithm:         Message Digest 5
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               86400 seconds, no volume limit
```

Рис.2.4. Проверка настроенной конфигурации IKE

Задача 3. Настройка IPSec. Следующей задачей настройки IPSec в Cisco IOS является установка ранее определенных параметров шифрования и хеширования IPSec. Действия, которые необходимо выполнить для этого в маршрутизаторах Cisco, являются следующими.

Шаг 1. Определение набора преобразований, т.е совокупности конкретных алгоритмов IPSec, с помощью которых реализуется политика защиты для выбранного трафика. В рамках контекста безопасности IKE выполняются операции согласования (в ходе второй фазы IKE, быстрый режим), в результате которых стороны соглашаются использовать

конкретный набор преобразований для защиты потока данных.

Набор преобразований объединяет следующие элементы IPSec:

– механизм шифрования данных: преобразование ESP;

– режим IPSec (транспортный или туннельный).

Набор преобразований устанавливается с помощью команды глобальной конфигурации crypto ipsec transform-set, активизирующей конфигурационный режим crypto–transform. Для удаления набора преобразований, используется так же команда с префиксом no.

Данные настройки производятся командой: crypto ipsec transform-set TS esp-3des esp-md5-hmac.

Шаг 2. Установка глобальных пределов существования ассоциации защиты IPSec. Пределы существования ассоциаций защиты IPSec указывают, как долго они останутся действительными и когда потребуется их переустановка. ПО Cisco IOS поддерживает глобальное значение предела существования, применимого сразу ко всем криптографическим картам. Это значение можно изменить соответствующей записью криптогра-фической карты. Чтобы обеспечить непрерывность потока данных перед тем как контекст безопасности прекратит свое существование, проводятся переговоры о создании нового.

Глобальные значения пределов существования для ассоциаций защиты IPSec изменяются с помощью команды конфигурации crypto ipsec security–association lifetime. Для восстановления стандартного значение предела существования используется та же команда с префиксом no.

Команда задается следующим образом: crypto ipsec security-association lifetime seconds 86400.

Шаг 3. Создание списков шифрованного доступа. Следующим шагом настройки IPSec является создание списков access-list, которые используются для определения трафика IP, защищаемого (или не защищаемого) средствами IPSec. Списки доступа применяются для:

– выбора исходящего трафика, подлежащего шифрованию средствами IPSec;

– обработки входящего трафика на предмет выявления трафика IPSec;

– выявления и фильтрации входящего трафика, подлежащего защите средствами IPSec;

– удовлетворения запросов создания ассоциаций защиты IPSec в процессе согласования IKE.

Настройка перечисленных параметров приведена на рисунке 2.5, где создается access-list FOR-VPN, а затем в список шифрованного доступа вносится запись сетей source и destination с wildcard масками.

```
router1(config)# ip access-list extended FOR-VPN
router1(config-ext-nacl)# permit ip 192.168.1.0 0.0.0.128
192.168.1.128 0.0.0.128
router1(config-ext-nacl)#exit
```

Рис.2.5. Создание списков шифрованного доступа

Шаг 4. Создание криптографических карт. При создании криптографических карт, с помощью средств IPSec можно установить контексты безопасности для потоков данных, подлежащих шифрованию.

Записи криптографических карт определяют параметры контекстов безопасности IPSec, связывая следующие элементы конфигурации:

– трафик, защищаемый средствами IPSec (списком шифрованного доступа), и степень детализации трафика, защищаемого набором ассоциаций защиты;

– пункт назначения, куда направляется трафик IPSec;

– локальный адрес, использующийся для трафика IPSec;

– тип защиты IPSec, применяемый к указанному трафику (наборы преобразований);

– способ создания контекстов безопасности: создание вручную или посредством IKE.

Последовательность команд, с помощью которых создается криптографическая карта и задаются вышеперечисленные настройки, представлена на рисунке 2.6.

```
router1(config)# crypto map CMAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
router1(config-crypto-map)# set peer 185.22.174.42
router1(config-crypto-map)# set transform-set TS
router1(config-crypto-map)# match address FOR-VPN
router1(config-crypto-map)# exit
```

Рис.2.6. Создание криптографической карты

Шаг 5. Применение криптографических карт к интерфейсам. Этот шаг заключается в привязке к интерфейсу в режиме конфигурации криптографической карты с помощью команды cryptomap. Данная операция приведена на рисунке 2.7. Сразу после применения

криптографической карты маршрутизатор выводит сообщение о том, что протокол ISAKMP активирован.

В таблице 4 представлены элементы политики IPSec использованные для настройки VPN-туннеля.

```
router1(config)# int GigEthernet 0/0
router1(config-if)#crypto map CMAP
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
router1(config-if)#exit
```

Рис.2.7. Применение созданной криптографической карты к интерфейсу GigabitEthernet 0/0

Таблица 4 – Элементы политики IPSec

Параметр	Значение для стороны A	Значение для стороны B
Набор преобразований	esp–3des, esp–md5–hmac	esp–3des, esp–md5–hmac
Режим IPSec	Туннельный	Туннельный
Алгоритм хэширования	MD5	MD5
Имя удаленного хоста	router1	router2
Интерфейс	GigabitEthernet0/0	GigabitEthernet0/0
IP–адрес удаленной стороны	185.22.174.42	91.240.210.120
IP–адрес хостов, которые должны быть защищены	192.168.1.0/25	192.168.1.128/25
Тип трафика для шифрования	TCP	TCP
Установка ассоциаций защиты	ipsec–isakmp	ipsec–isakmp

Задача 4. Тестирование и контроль IPSec. Завершающей задачей процесса настройки IPSec для работы с общими ключами является проверка текущих установок и функциональных возможностей IPSec.

Команда show crypto isakmp policy используют для проверки настроенных параметры политики IKE. Применение команды было показано на рисунке A. Команда show crypto isakmp sa отображает параметры всех текущих ассоциаций защиты IKE (рис.2.8).

```
Router1#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state      conn-id    slot   status
94.240.210.120  185.22.174.42   QM_IDLE    1073       0      ACTIVE

IPv6 Crypto ISAKMP SA
```

Рис.2.8. Параметры текущих ассоциаций защиты IKE

Команда clear crypto isakmp режима глобального конфигурирования служит для очистки активных соединений IKE. Команда задается следующим образом: clear crypto isakmp [id–соединения], где id–соединения идентифицирует соединение, которое требуется очистить.

Если значение параметра не указано, будут очищены все существующие соединения.

Команда show crypto ipsec sa режима предназначена для вывода текущей конфигурации IPSec. Здесь показаны все параметры текущих IPSec-соединений, включая количество зашифрованных и расшифрованных пакетов.

Задание на лабораторную работу

Внимание! Работа выполняется в подгруппах по 2 студента. При настройке устройств локальные IP-адреса выбрать на свое усмотрение из «серого» диапазона адресов, глобальные IP-адреса составить по схеме 94.205.А.Б. и 185.112.А.Б, буквы А и Б заменить на порядковые номера в журнале преподавателя выполняющих работу студентов.

1. Изучить методические указания к лабораторной работе.

2. Построить схему, состоящую из двух изолированных локальных сетей (число компьютеров в каждой из локальной сетей соответствует последней цифре номера зачетной книжки выполняющих работу студентов). Локальные сети объединить между собой при помощи трех маршрутизаторов. Всем устройствам и интерфейсам назначить IP-адреса. Примерный вид схемы представлен на рисунке 2.9.

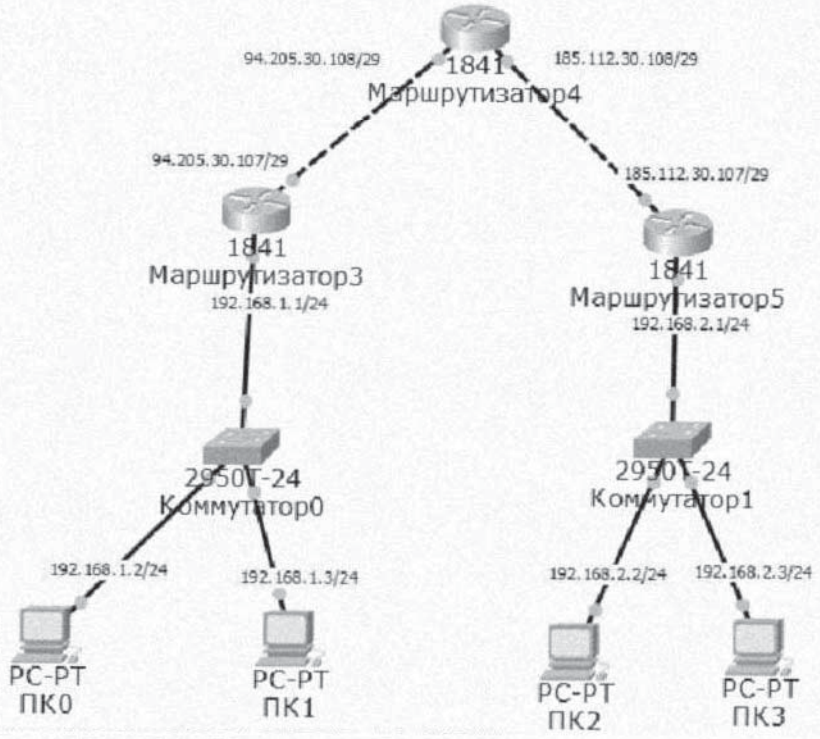

Рис. 2.9. Пример схемы для выполнения работы

3. Построить VPN-соединение между двумя сетями. Каждый этап при выполнении данного пункта и последующих, отобразить на

скриншотах.

4. Определить политику IKE для создаваемого соединения.

5. Установить параметры шифрования и хеширования IPSec.

6. Проверить произведенные настройки и отобразить настроенную конфигурацию IPSec.

7. Проверить взаимную доступность устройств из разных сетей. Использовать команду, которая однозначно доказывала бы функционирование виртуального туннеля между сетями.

8. Отобразить полную конфигурацию маршрутизатора.

9. Изобразить структурную схему построенного соединения с указанием используемых адресов, использованных устройств и интерфейсов, алгоритмов шифрования и гарантии целостности, параметров обмена ключами.

10. Оформить отчет по лабораторной работе и подготовиться к его защите. Для подготовки рекомендуется ответить на контрольные вопросы.

Внимание! В отчете о выполнении работы все итерации выполнения задания должны быть подкреплены достаточным количеством скриншотов. На скриншотах требуется указать IP-адреса и другие настроенные параметры.

Контрольные вопросы и задания

1. В чем основная суть технологий виртуальных частных сетей?
2. Из каких компонентов состоит VPN?
3. Опишите принцип работы технологии виртуальных частных сетей.
4. Что подразумевается под понятием инкапсуляции?
5. Какие операции производятся с пакетом данных при движении через туннель?
6. На какие типы делятся протоколы по способу передачи данных в туннеле?
7. Чем отличаются туннельный и транспортный режим работы AH и ESP?
8. Поясните суть понятий аутентификации и шифрования.

Перечень необходимого материально-технического оборудования

Выполнение лабораторной работы предполагается в учебной лаборатории сетевых технологий кафедры космического приборостроения

и систем связи. Учебная лаборатория должна быть оснащена:

– учебной мебелью (столы и стулья для обучающихся, в количестве не меньше списочного состава студентов, стол и стул для преподавателя);

– доской;

– учебными компьютерами (в количестве не менее 1 устройство на 2 студентов), с установленными операционной системой Windows, программным продуктом Cisco Packet Tracer и программным продуктом LibreOffice (для составления отчета о выполнении работы).

Лабораторная работа
ОРГАНИЗАЦИЯ ПРОСТЕЙШЕГО VPN-СЕРВЕРА

Цель работы: закрепление принципов работы технологии «Виртуальная частная сеть», приобретения навыков конфигурирования PPTP-сервера с помощью Ubuntu и использования PPTP-соединения.

Краткие теоретические сведения

Ubuntu – это дистрибутив Linux

Ubuntu – это дистрибутив Linux, построенный на базе другого дистрибутива Linux – Debian, и распространяющийся под свободной лицензией GNU/GPL.

Ubuntu ориентирована на удобство и простоту использования. Она включает широко распространённое использование утилиты sudo, которая позволяет пользователям выполнять администраторские задачи, не запуская потенциально опасную сессию суперпользователя.

Главные особенности дистрибутива Ubuntu:

1. Стабильность работы – систему часто используют на высоко нагруженных серверах. ОС не требует частых перезагрузок устройства, даже в случаи обновлений, установки или удаления программ.

2. Полностью бесплатная ОС – установка происходит в несколько кликов, в сети полно версий для бесплатного скачивания, не нужно вводить никаких ключей, можно использовать на множестве компьютеров одновременно.

3. Быстрая установка – с появлением новых версий установка Ubuntu все упрощается, чем привлекает неопытных пользователей. Основное ПО и драйвера устанавливаются сразу и практически автоматично, в итоге вы получаете готовую к работе ОС. Кроме того предлагается автоматическое обновление.

4. Предсказуемость обновления системы – каждый новый релиз выходит с периодичностью в 6 месяцев, пользователи всегда имеют доступ к свежим версиям ОС.

VPS/VDS – виртуальный сервер

Понятия VDS и VPS ничем друг от друга не отличаются и используются для определения услуги виртуального выделенного сервера.

Обычно их используют вместе, чтобы не путать пользователей. VPS/VDS – аббревиатура от Virtual Private Server/Virtual Dedicated Server. Эти термины развивались параллельно и служат для обозначения одной и той же услуги.

Виртуальный выделенный сервер – это одна из разновидностей услуги хостинга. Хостинг – это услуга, при которой компания размещает на своих серверах информацию о сайтах. Сервер – это специальное мощное вычислительное устройство. Существует несколько видов хостинга.

1. Виртуальный. Это самый простой и дешевый тип. Если сравнивать хостинг с домом, то виртуальный можно представить в виде коммунальной квартиры. У каждого жильца (клиента) есть отдельная комната, но кухня и ванная общие (клиенты пользуются общими ресурсами).

2. Виртуальный выделенный сервер VPS/VDS. Когда на обычном физическом сервере создают множество виртуальных серверов, эмулирующих работу физического. Этот вид хостинга можно представить в виде многоэтажного дома. У каждого жильца (клиента) есть собственная квартира со всеми удобствами (выделенные CPU, RAM), а еще он может сделать практически любой ремонт (root-доступ).

3. Выделенные серверы. Самый дорогой вид хостинга. Когда в аренду сдается целый физический сервер. Этот вид можно представить в виде большого частного дома, где нет соседей (других клиентов) и еще больше свободы для ремонта.

Сравнение основных параметров трех видов хостинга приведено в таблице 3.1.

Табл. 3.1. Параметры видов хостинга

Услуга	VPS/VDS	Выделенный сервер	Виртуальный хостинг
Root-доступ	Да	Да	Нет
Выделенный IP-адрес	Да	Да	Нет (можно заказать)
Один клиент на сервере	Нет	Да	Нет
Цена, руб./мес.	от 158	от 4167	от 144

Порядок настройки VPN-сервера

С помощью терминала установить необходимые пакеты для работы с PPTP. Для установки понадобятся права root пользователя или sudo:

```
sudo su
apt-get install ppp pptpd // Установка пакета PPTP
```

После окончания установки, понадобится отредактировать несколько файлов. Для изменения файлов можно пользоваться любым удобным способом, хоть nano, хоть визуальными редакторами.

Далее необходимо определиться с локальной подсетью для клиентов VPN. Нужно выбрать диапазон из любой подсети, которая не маршрутизируется в интернете:

10.0.0.0/8
172.16.0.0/12
192.0.2.0/24
192.88.99.0/24
192.168.0.0/16
198.18.0.0/15
224.0.0.0/4
240.0.0.0/4
100.64.0.0/10

Следующим шагом нужно открыть файл /etc/pptpd.conf, в котором нужно найти и раскоментировать (если вдруг закоментированы) строки localip и remoteip, затем прописать свою IP адресацию.

```
localip 172.16.0.1 // IP-адрес из выбранной подсети, который будет являться локальным шлюзом для клиентов VPN
remoteip 172.16.0.2-254 // диапазон IP-адресов для назначения клиентам VPN
```

Если на вашей виртуальной машине несколько внешних IP-адресов, то нужно указать конкретный IP, по которому будет доступно подключение к VPN-серверу. Для этого в конце файла нужно добавить:

```
listen внешний_ip
```

Следующим шагом будет открытие файла /etc/ppp/pptpd-options и приводим его к виду (без комментариев):

```
name pptpd
refuse-pap
nobsdcomp
require-mschap-v2 // делаем обязательным шифрование
require-mppe-128
ms-dns 8.8.8.8 // указываем конкретные DNS, которые будут использоваться при подключении через VPN
```

```
ms-dns 8.8.4.4
proxyarp
novjccomp
nodefaultroute
lock
nobsdcomp
mtu 1400
mru 1400
auth
require-mppe
```

Далее открываем стандартный файл /etc/sysctl.conf, находим и раскоментируем строку:

```
net.ipv4.ip_forward=1
```

Данное действие сделает возможным выход клиентов в интернет через VPN-сервер.

Добавляем необходимые правила в iptables:

```
iptables -A INPUT -p gre -j ACCEPT
iptables -A INPUT -m tcp -p tcp --dport 1723 -j ACCEPT
iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
```

Обратите внимание, что eth0 – имя вашего сетевого интерфейса. Вы можете узнать его с помощью команды ifconfig

Если вам необходимо, чтобы была локальная сеть между клиентами, подключенными к VPN, добавьте следующие правила в iptables:

```
iptables --table nat --append POSTROUTING --out-interface
ppp0 -j MASQUERADE
iptables -I INPUT -s 172.16.0.0/24 -i ppp0 -j ACCEPT
iptables --append FORWARD --in-interface eth0 -j ACCEPT
```

Обратите внимание, что 172.16.0.0/24 – локальная подсеть, которую вы себе выбрали, а ppp0 – имя pptp интерфейса.

Для сохранения iptables, выполните команду:

```
iptables-save > /etc/iptables.up.rules
```

Переходим в файл /etc/network/interfaces и в конце добавляем строку:

```
pre-up iptables-restore < /etc/iptables.up.rules
```

Данное действие нужно выполнить, чтобы правила iptables не сбрасывались после перезапуска машины.

Далее создадим пользователей для подключения к VPN–серверу в файле /etc/ppp/chap-secrets

```
user1          pptpd   password1     "*"
user2          pptpd   password2     "172.16.0.2"
```

где `user1` – имя пользователя

`password1` – пароль пользователя

`"*"` – локальный IP будет выдаваться из пула, указанного в файле /etc/pptpd.conf

`"172.16.0.2"` – пользователю будет присвоен указанный ip адрес.

Перезапускаем сервис pptpd для применения новых настроек:

```
service pptpd restart
```

Настройка PPTP сервера в Ubuntu Server закончена, можно пробовать подключиться. В качестве протокола проверки подлинности обязательно нужно указывать mschapv2 и обязательно нужно включать шифрование, иначе сервер не разрешит подключение.

Задание на лабораторную работу

Внимание! Работа выполняется студентами в подгруппах по 2 человека. Вариант определяется персонально преподавателям.

1. Изучить методические указания к лабораторной работе.
2. Установить на виртуальную машину дистрибутив Ubuntu (версии не ниже 14.04) без графического интерфейса. Если работа выполняется с использованием VPS, то нужно убедиться, что хостер не использует систему виртуализации openvz (не лишним будет уточнить у хостера включены ли модули ppp в ядре виртуальной машины).
3. Установить необходимые пакеты для работы с PPTP.
4. Произвести настройку сервера согласно инструкции. Адреса локальной сети и количество пользователей выбрать в соответствии с выданным преподавателем заданием (табл. 3.2).

Имена пользователей задать по схеме userAAA, где AAA – первые буквы от фамилии, имени, отчества авторов отчета на английском языке (для первых двух созданных пользователей) и комбинация из любых трех букв английского алфавита (для третьего и четвертого созданных пользователей).

5. Проверить работоспособность сервера с помощью сервисов определения IP-адреса в сети Интернет (показать адрес до подключения к VPN и после).
6. Проверить работоспособность сервера с помощью сетевых

анализаторов – устройства, подключенные к виртуальной частной сети, должны определять друг друга.

Табл.3.2. Варианты задания

	Адрес сети	Количество пользователей для подключения
1	10.0.0.0/26	3
2	172.16.0.0/24	4
3	192.168.91.0/25	3
4	10.168.125.0/24	4
5	172.16.0.128/25	3
6	10.168.43.128/27	4
7	10.0.1.0/26	3
8	10.168.43.0/27	4
9	172.16.91.0/24	3
10	192.168.15.128/25	4
11	10.168.58.128/25	3
12	10.0.1.128/26	4
13	10.91.100.0/24	3
14	192.168.15.128/26	4

7. Оформить отчет по лабораторной работе и подготовиться к его защите. Для подготовки рекомендуется ответить на контрольные вопросы.

Внимание! В отчете о выполнении работы все значимые этапы выполнения задания должны быть подкреплены достаточным количеством скриншотов. Для процедуры защиты:

1. Предусмотреть возможность подключения к VPN-серверу преподавателя с логином kpiss-swsu и паролем 01122021.

2. Быть готовым продемонстрировать работу сервера на компьютере, с помощью программы Advanced IP Scanner, и на смартфоне, с помощью любого анализатора локальной сети. В процессе работы программы должны отображаться все устройства, подключенные в данный момент к виртуальной сети.

3. Продемонстрировать IP-адрес устройства в сети Интернет до подключения к VPN-серверу и после.

Контрольные вопросы и задания

1. В чем основная суть технологий виртуальных частных сетей?
2. Из каких компонентов состоит VPN?
3. Какой протокол туннельного соединения использовался в работе?
4. На какие типы делятся протоколы по способу передачи данных в туннеле?

Перечень необходимого материально-технического оборудования

Выполнение лабораторной работы предполагается в учебной лаборатории сетевых технологий кафедры космического приборостроения и систем связи. Учебная лаборатория должна быть оснащена:

– учебной мебелью (столы и стулья для обучающихся, в количестве не меньше списочного состава студентов, стол и стул для преподавателя);

– доской;

– учебными компьютерами (в количестве не менее 2 устройство на 2 студентов), с установленными операционной системой Ubuntu, операционной системой Windows, программным продуктом Advanced IP Scanner (либо любым другим сетевым анализатором) и программным продуктом LibreOffice (для составления отчета о выполнении работы).

Приложение А

Форма отчета обучающегося о выполненной лабораторной работе

МИНОБРНАУКИ РОССИИ

Юго-Западный государственный университет

Кафедра космического приборостроения и систем связи

ОТЧЁТ

по выполнению лабораторной работы

«Планирование адресного пространства локальной сети»

по дисциплине «Основы сетевых технологий»

Выполнил: студент группы ИТ-91б
Иванов М.О.

Проверил: ст.преподаватель кафедры КПиСС
Чуев А.А.

_____ «____»_____2023 г.

(подпись)

работа защищена на_____баллов

Курск 2023

Приложение А

Форма отчета обучающегося о выполненной лабораторной работе

Целью работы является освоение принципов и методик разделения адресного пространства локальной сети на подсети; получение практических навыков разделения сетей на нужное количество подсетей нужного (различного) размера.

1.1 Индивидуальное задание

1. Сгенерировать индивидуальный IP-адрес и префикс подсети (суперсети).

2. Определить основные параметры заданной подсети:

а) адрес узла в точечно-двоичной нотации;

б) класс сетевого адреса (традиционный);

в) маску подсети (или суперсети, если префикс оказался меньше традиционного для класса) в точечно-десятичной нотации;

г) шаблон для выделения адресов узлов в подсети (в суперсети);

д) количество узлов в подсети (суперсети);

е) IP-адрес подсети (суперсети);

ж) IP-адрес шлюза;

з) IP-адрес первого узла в подсети;

и) IP-адрес последнего узла в подсети;

к) IP-адрес широковещательных сообщений для данной подсети.

3. Используя схему сети предприятия, приведенную на рисунке 1, а также, информацию о количестве компьютеров в отделах предприятия, заданную вариантом (таблица 1), разбить заданную сеть на подсети.

Таблица 1 – Исходные данные сети предприятия

Вариант	Исходная сеть (блок адресов)	Количество компьютеров в отделах		
		А	Б	В
7	126.61.74.0 /23	8	61	17

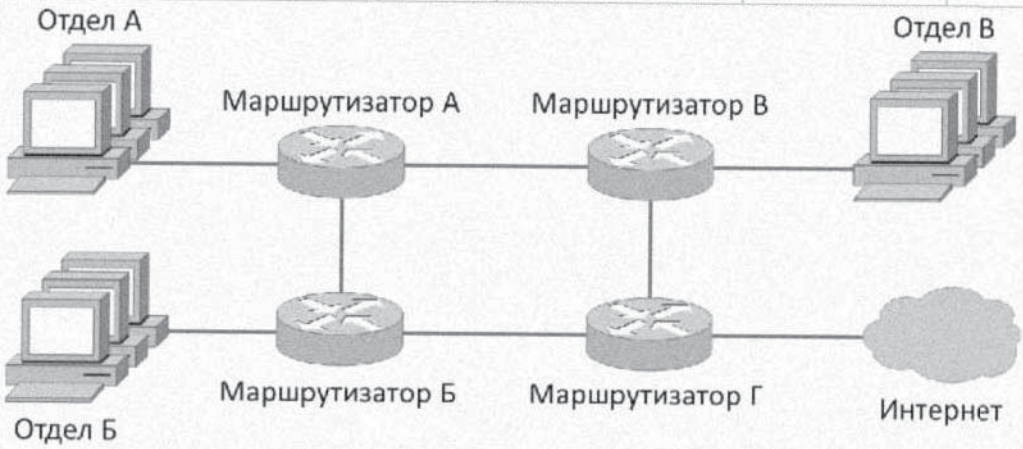

Рисунок 1 – Схема сети предприятия

Приложение А

Форма отчета обучающегося о выполненной лабораторной работе

1.2 Ход работы

……

Вывод