Министерство образования и науки Российской Федерации
Вологодский государственный университет

Кафедра автоматики и вычислительной техники

ЗАЩИТА ИНФОРМАЦИИ

Методические указания к лабораторным работам

Факультет электроэнергетический

Направления подготовки бакалавриата	27.03.04 - Управление в технических системах 09.03.01 – Информатика и вычислительная техника 09.03.04 – Программная инженерия
Профили подготовки:	Управление и информатика в технических системах Программное обеспечение средств вычислительной техники и автоматизированных систем Разработка программно-информационных систем

Вологда
2014

УДК 681.374.1

Защита информации: методические указания к лабораторным работам. – Вологда: ВоГУ, 2014. – 31 с.

Приводятся методические указания к выполнению лабораторных работ по дисциплине с описанием разработанных программных комплексов. В начале каждой лабораторной работы приведен необходимый для выполнения работы теоретический материал, подробно описаны все действия, необходимые для изучения различных алгоритмов шифрования.

Утверждено редакционно-издательским советом ВоГУ

Составитель Е.Н. Давыдова, канд. техн. наук, доцент кафедры АВТ

Рецензент Г.А. Сазонова, канд. техн. наук, доцент каф. ИСиТ

ЛАБОРАТОРНАЯ РАБОТА № 1

НАСТРОЙКА ПАРОЛЕЙ, РЕЖИМОВ ПРИВИЛЕГИЙ В CISCO PACKET TRACER

1. ЦЕЛЬ РАБОТЫ:

1.1. Изучить режимы привилегий;
1.2. Изучить принцип настройки паролей.

2. ПОРЯДОК ПРОВЕДЕНИЯ РАБОТЫ

2.1. Изучить теоретический материал
2.2. Проделать практическое задание
2.3. Выполнить задания для самостоятельной работы
2.4. Оформить отчет
2.5 Защитить лабораторную работу

3. ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

Маршрутизаторы и коммутаторы Cisco можно конфигурировать с помощью интерфейса пользователя, исполняемого на консоли маршрутизатора или на терминале, а также через удаленный доступ. Перед тем как будет возможен ввод команд привилегированного режима, необходимо осуществить вход в маршрутизатор. В целях безопасности необходимо настраивать пароли и привилегии для пользователей, разграничивать доступ к режимам интерфейса пользователя, чтобы предотвратить несанкционированный доступ и не дать изменить настройки сетевого оборудования.

3.1.Режимы интерфейса пользователя

а) Пользовательский режим.

Switch>

Пользователям предоставляется возможность подключаться к коммутатору, маршрутизатору посредством консольного порта, telnet-сеанса, ssh-сеанса, в котором можно просматривать некоторую статистику и проводить самые простые операции вроде пинга. В этом режиме изменять конфигурацию не разрешается.

б) Привилегированный режим.

Switch> enable
password: [password]
Switch#

С помощью множества паролей можно разрешить различным группам пользователей доступ к разным наборам команд. В привилегированном режиме вы можете просмотреть всю информацию об устройстве.

3.2.Привилегии

Всего 16 уровней привилегий

– - уровень 0 – это команды disable, enable, exit, help и logout, которые работают во всех режимах

– - уровень 1 – это команды пользовательского режима, то есть как только вы попадаете на оборудование и увидите приглашение Router>, вы имеете уровень 1;

– - уровни 2-14 являются настраиваемыми уровнями привилегий пользователей;

– - уровень 15 – это команды привилегированного режима.

Уровень привилегий для команды задается с помощью команды privilege level глобальной конфигурации. Использование этой команды с префиксом по возвращает к уровню привилегий, заданному для соответствующей команды по умолчанию. Синтаксис команды следующий

privilege режим {level уровень команда | reset команда]

3.3.Описание

– режим – указывает режим конфигурации. Допустимыми значениями являются exec, configure, line, interface и другие режимы конфигурации маршрутизатора

– level уровень - назначает уровень привилегий от 0 до 15, связываемый с указанной командой

– команда – указывает команду, с которой связывается назначаемый уровень привилегий

– reset команда - восстанавливает уровень привилегий указанной команды.

3.4.Пароли

Команды enable password и enable secret позволяют ограничить доступ в привилегированный режим EXEC и запретить посторонним вносить изменения в настройки маршрутизатора. Пароль устанавливается с помощью следующих команд:

Router(config) # enable password [пароль]
Router(config) # enable secret [пароль]

Разница между командами enable password и enable secret состоит в том, что команда enable password по умолчанию зашифрована.

Существует несколько способов подключиться к устройству и настроить конфигурацию. Один из них – подключение компьютера к порту консоли устройства. Этот способ часто используется при первоначальной настройке.

Чтобы ввести пароль для доступа к консоли, сначала необходимо перейти в режим глобальной конфигурации. Затем ввести следующую команду:

Router(config) # line console 0
Router(config-line) # password [пароль]

Это помешает посторонним войти в пользовательский режим с порта консоли.

К подключенному к сети устройству можно получить доступ через сетевое соединение. Такой вариант называется подключением через виртуальный терминал. Для виртуального порта нужно настроить пароль.

Router(config) # line vty 0 4
Router(config-line) # password [пароль]

Можно проверить правильность пароля с помощью команды show running-config. Пароли хранятся в файле текущей конфигурации в формате незашифрованного текста. Можно включить шифрование всех паролей, которые хранятся в памяти маршрутизатора. Тогда посторонним будет сложнее их открыть. Команда service password encryption включает шифрование паролей.

Telnet – протокол незащищённый и передаёт пароль и данные в открытом виде. С помощью любого анализатора пакетов можно вычислить пароль. Поэтому рекомендуется использовать ssh.

Router(config)#hostname R0
Router(config)#ip domain-name cisco-dmn
Router(config)#crypto key generate rsa
Router(config)#line vty 0 4
Router(config-line)#transport input ssh

Имя хоста должно отличаться от Router, обязательно должно быть задано имя домена. Третьей строкой генерируется ключ и далее разрешается только ssh. Длина ключа должна быть более 768 бит, если вы желаете использовать ssh версии 2.

Сейчас принято настраивать доступы не через виртуальные терминалы, а командами #username и #aaa new-model. Для этого нужно выполнить:

Router(config)#aaa new-model
Router(config)#username admin password 1234

Первая команда служит для активации новой модели AAA (Authentication, Authorization, Accounting). Это нужно для того, чтобы была возможность использовать для аунтетификации на устройстве RADIUS или TACACS сервер. Если отдельно это не настроено, то будет использоваться локальная база пользователей, задаваемая командой username.

Прежде чем приступать к настройке, упомянем несколько полезных особенностей при работе с cisco CLI:

– Все команды в консоли можно сокращать. Главное, чтобы сокращение однозначно указывало на команду. Например, show running-config сокращается до sh run. Почему не до s r? Потому что s (в пользовательском режиме) может означать как команду show, так и команду ssh, и мы получим сообщение об ошибке % Ambiguous command: «s r» (неоднозначная команда).

– Используйте клавишу Tab и знак вопроса. По нажатию Tab сокращенная команда дописывается до полной, а знак вопроса, следующий за командой, выводит список дальнейших возможностей и небольшую справку по ним.

– Используйте горячие клавиши в консоли:

Ctrl+A – Передвинуть курсор на начало строки

Ctrl+E – Передвинуть курсор на конец строки

Курсорные Up, Down – Перемещение по истории команд

Ctrl+W – Стереть предыдущее слово

Ctrl+U – Стереть всю линию

Ctrl+C – Выход из режима конфигурирования

Ctrl+Z – Применить текущую команду и выйти из режима конфигурирования

Ctrl+Shift+6 – Остановка длительных процессов (так называемый escape sequence)

4. ПРАКТИЧЕСКАЯ ЧАСТЬ

Кликом по компьютеру вызываем окно настройки, в котором нас интересует вкладка Desktop. Далее выбираем Terminal, где нам даётся выбор параметров.

Все параметры по умолчанию нас устраивают, и менять их не будем. Отвечаем no и видим приглашение:

Router>

Это стандартное совершенно для любой линейки cisco приглашение, которое характеризует пользовательский режим, в котором можно просматривать некоторую статистику и проводить самые простые операции вроде пинга. Ввод знака вопроса покажет список доступных команд. Просмотрим их:

```
Router>?
Exec commands:
  <1-99>      Session number to resume
  connect     Open a terminal connection
  disable     Turn off privileged commands
  disconnect  Disconnect an existing network connection
  enable      Turn on privileged commands
  exit        Exit from the EXEC
  logout      Exit from the EXEC
  ping        Send echo messages
  resume      Resume an active network connection
  show        Show running system information
  ssh         Open a secure shell client connection
  telnet      Open a telnet connection
  terminal    Set terminal line parameters
  traceroute  Trace route to destination
```

Гораздо большие возможности предоставляет режим привилегированный. Попасть в него можно, введя команду >enable. Теперь приглашение выглядит так:

Router#

Здесь список операций гораздо обширнее, в привилегированном режиме вы можете просмотреть всю информацию об устройстве. Просмотрим команды привилегированного режима:

```
Router#?
Exec commands:
  <1-99>      Session number to resume
  auto        Exec level Automation
  clear       Reset functions
  clock       Manage the system clock
  configure   Enter configuration mode
  connect     Open a terminal connection
  copy        Copy from one file to another
  debug       Debugging functions (see also 'undebug')
  delete      Delete a file
  dir         List files on a filesystem
  disable     Turn off privileged commands
  disconnect  Disconnect an existing network connection
  enable      Turn on privileged commands
  erase       Erase a filesystem
  exit        Exit from the EXEC
  logout      Exit from the EXEC
  mkdir       Create new directory
  more        Display the contents of a file
  no          Disable debugging informations
  ping        Send echo messages
```

Режим глобальной конфигурации активируется командой #configure terminal из привилегированного режима и демонстрирует такое приглашение:

Router(config)#

Настройка доступа по Telnet

Команда для перехода в режим конфигурации интерфейса FastEthernet 0/0: Router(config)# interface fa0/0

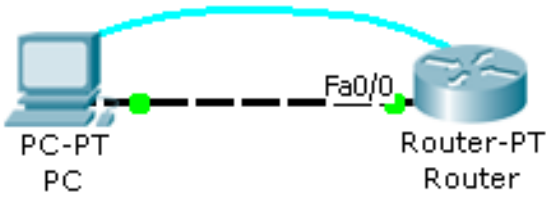
По умолчанию все интерфейсы отключены (состояние administratively down). Включаем интерфейс:

Router(config-if)#no shutdown

Настроим IP-адрес:

Router(config-if)#ip address 192.168.1.1 255.255.255.0

Подключаемся. Для этого надо использовать кроссоверный кабель.



Настраиваем IP-адрес компьютера через Desktop, затем пропингуем интерфейс маршрутизатора с PC. Соединение должно присутствовать.

Попробуйте установить соединение по протоколу Telnet

PC>telnet 192.168.1.1

К маршрутизатору не удалось подключиться, потому что соединение не настроено. Настроим его

Login = «admin», password = «1234»

Router(config)#aaa new-model

Router(config)#username admin password 1234

Первая команда служит для активации модели AAA (Authentication, Authorization, Accounting). Это нужно для того, чтобы была возможность использовать для аунтетификации на устройстве RADIUS или TACACS сервер. Если отдельно это не настроено, то будет использоваться локальная база пользователей, задаваемая командой username.

Проверим, можем ли мы подключиться по Telnet

```
PC>telnet 192.168.1.1
Trying 192.168.1.1 ...Open


User Access Verification

Username: admin
Password:
Router>
```

Это действительно так.

Просмотрим конфигурацию маршрутизатора

Router#show running-config

```
!
!
!
username admin password 0 1234
!
!
!
```

Видим, что пароль хранится в незашифрованном виде

Включим шифрование всех паролей, которые хранятся в памяти маршрутизатора

Router(config)#service password-encryption

```
!
!
!
username admin password 7 08701E1D5D
!
!
!
```

Видим, что теперь пароль хранится в зашифрованном виде

Отменим команду создания пользователя admin

Router(config)#no username admin password 1234

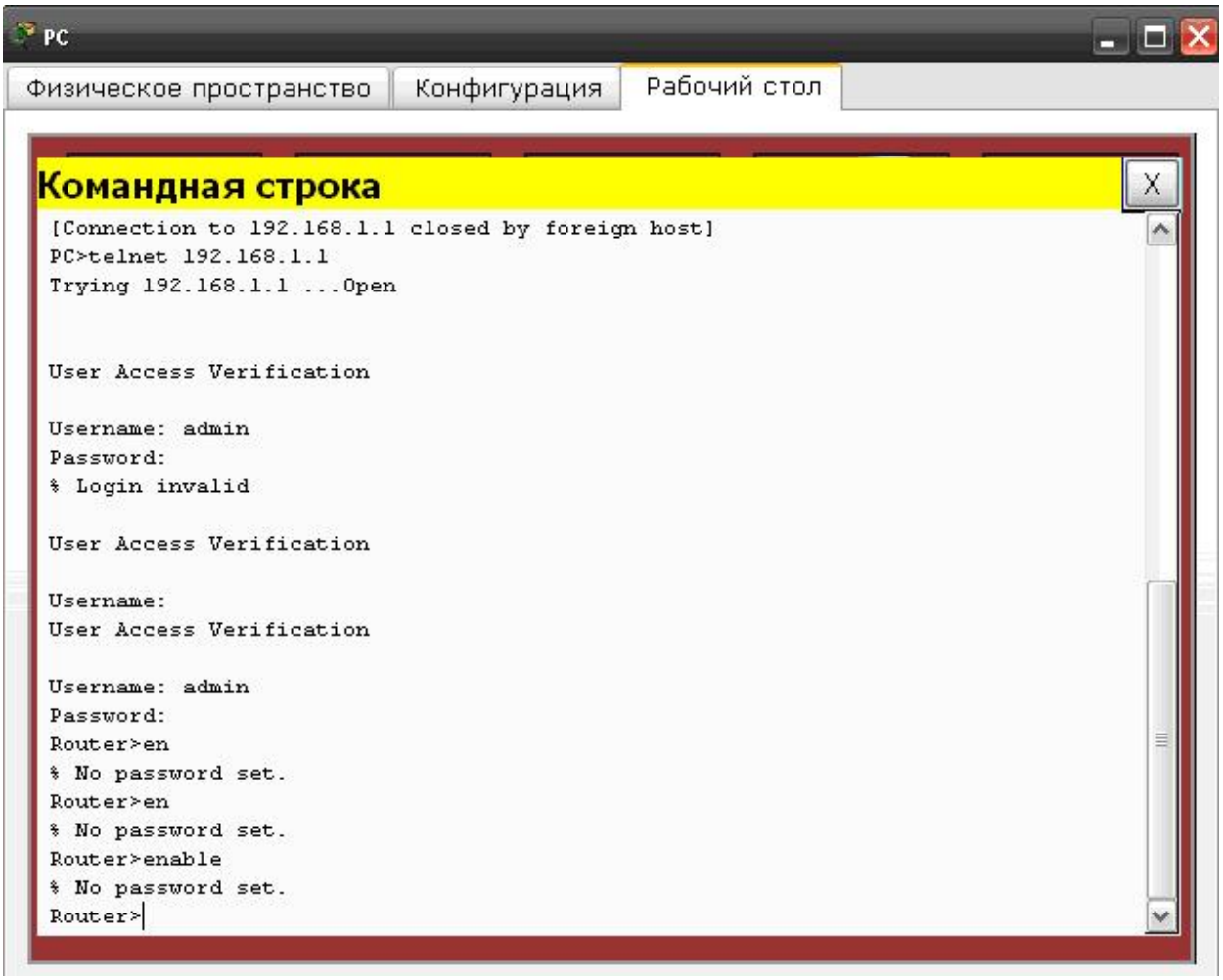
При настройке secret пароль хранится в зашифрованном виде в конфигурационном файле, а password – в открытом. Поэтому рекомендуется использование secret.

Router(config)#username admin secret 1234

```
!
username admin secret 5 $1$mERr$4dpRATIgxQacPVKOCfNV4/
!
!
!
```

Проверьте, что по-прежнему работает соединение по Telnet

Попробуйте перейти в привилегированный режим



Сделать это не получится, потому что удаленный доступ к привилегированному режиму не настроен.

Настроим его на маршрутизаторе в режиме конфигурации с помощь команды enable

Router(config)#enable secret cisco

```
PC>telnet 192.168.1.1
Trying 192.168.1.1 ...Open


User Access Verification

Username: admin
Password:
Router>enable
Password:
Router#
```

Настроим так, чтобы все пользователи, подключающиеся по Telnet, получали 15 уровень прав и попадали в привилегированный режим.

Для этого настроим виртуальные терминалы:

Router(config)#line vty 0 4

Router(config-line)#privilege level 15

Теперь, если попытаться зайти на маршрутизатор по Telnet, то автоматически попадаете в привилегированный режим уже без ввода пароля enable

```
PC>telnet 192.168.1.1
Trying 192.168.1.1 ...Open


User Access Verification

Username: admin
Password:
Router#
```

Если отменим команду с привилегиями, то при соединении по Telnet, будем попадать в пользовательский режим

Router(config-line)#no privilege level 15

```
PC>telnet 192.168.1.1
Trying 192.168.1.1 ...Open


User Access Verification

Username: admin
Password:
Router>
```

Создадим нового пользователя user и назначим ему привилегию второго уровня, которую создадим сами. Позволим этому пользователю использовать только команду show running-config

Router(config)#username user privilege 2 secret user

Router(config)#privilege exec level 2 show running-config

Router(config)#enable secret level 2 userpass

Присоединяемся к маршрутизотору по Telnet

При заходе в привилегированный режим с помощью enable необходимо указать уровень привилегии

```
PC>telnet 192.168.1.1
Trying 192.168.1.1 ...Open


User Access Verification

Username: user
Password:
Router>enable 2
Password:
Router#show running-config
Building configuration...

Current configuration : 941 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
!
!
```

Видим, что команда show running-config доступна

```
Router#conf t
             ^
% Invalid input detected at '^' marker.
```

А, например, команда перехода в режим глобальной конфигурации не доступна.

Router(config)#hostname R
R(config)#ip domain-name test
R(config)#crypto key generate rsa

```
PC>ssh -l admin 192.168.1.1
Open
Password:
R>
```

Доступ есть
Разрешим удаленный доступ только по ssh
R(config)#line vty 0 4
R(config-line)#transport input ssh
Просмотрим удаленный доступ с компьютера PC

```
PC>telnet 192.168.1.1
Trying 192.168.1.1 ...Open

[Connection to 192.168.1.1 closed by foreign host]
PC>ssh -l admin 192.168.1.1
Open
Password:
R>
```

Видим, что доступ по ssh есть, по telnet нет.

Просмотрите конфигурацию маршрутизатора

5. ЗАДАНИЕ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ

1. Настройте доступ по Telnet

Login = «test1», password = «test1»

Используйте такие команды, чтобы пароль хранился в памяти маршрутизатора в зашифрованном виде.

Проверьте соединение. Сделайте скриншот.

2. Настройте удаленный доступ к привилегированному режиму, используйте в качестве пароля «admin». Проверьте, сделайте скриншот.

3. Создайте нового пользователя user, используя для него пароль user, и назначьте ему привилегию третьего уровня. Позвольте этому пользователю использовать только команду show run. Проверьте, что доступна только эта команда. Сделайте скриншот.

4.Настройте удаленный доступ к роутеру по протоколу ssh

Задайте новое имя маршрутизатора R1

Имя домена Domain

Проверьте соединение. Сделайте скриншот.

5. Разрешите удаленное соединение только по протоколу ssh. Проверьте. Сделайте скриншот.

6. Создайте пользователя test2 с паролем test2, назначьте привилегию 15 уровня, чтобы этот пользователь попадал сразу в привилегированный режим. Проверьте. Сделайте скриншот.

6. СОДЕРЖАНИЕ ОТЧЁТА

Отчёт готовится в электронном виде. Отчёт содержит:

1. Скриншот топологии практической части.
2. Конфигурацию маршрутизатора.
3. Все введенные команды самостоятельного задания.
4. Все скриншоты, указанные в задании для самостоятельной работы.

ЛАБОРАТОРНАЯ РАБОТА № 2

НАСТРОЙКА СПИСКОВ КОНТРОЛЯ ДОСТУПА

1. ЦЕЛЬ РАБОТЫ:

1.1.Изучить стандартные списки контроля доступа;
1.2.Научиться выполнять настройку списков контроля доступа

2. ПОРЯДОК ПРОВЕДЕНИЯ РАБОТЫ

2.1. Изучить теоретический материал
2.2. Проделать практическое задание
2.3. Выполнить задания для самостоятельной работы
2.4. Оформить отчет
2.5 Защитить лабораторную работу

3. ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

ACL (Access Control List) — это набор текстовых выражений, которые что-то разрешают, либо что-то запрещают.

Функционал ACL состоит в классификации трафика, нужно его проверить сначала, а потом что-то с ним сделать в зависимости от того, куда ACL применяется. ACL применяется везде, например:

- На интерфейсе: пакетная фильтрация
- На линии Telnet: ограничения доступа к маршрутизатору
- VPN: какой трафик нужно шифровать
- QoS: какой трафик обрабатывать приоритетнее
- NAT: какие адреса транслировать

Применительно к пакетной фильтрации, ACL размещаются на интерфейсах, сами они создаются независимо, а уже потом они применяются к интерфейсу. Как только вы его применили к интерфейсу, маршрутизатор начинает просматривать трафик входящий и исходящий. Тот трафик, который входит в маршрутизатор, называется входящим, тот который из него выходит — исходящий. Соответственно ACL размещаются на входящем или на исходящем направлении.

Список доступа можно применить либо на входящий трафик, тогда неугодные пакеты не будут даже попадать на маршрутизатор и, соответственно, дальше в сеть, либо на исходящий, тогда пакеты приходят на маршрутизатор, обрабатываются им, доходят до целевого интерфейса и только на нём удаляются. Стандартный список доступа проверяет только адрес отправителя. Расширенный - адрес отправителя, адрес получателя, а также порт. Стандартные ACL рекомендуется ставить как можно ближе к получателю (чтобы не порезать больше, чем нужно), а расширенные - ближе к отправителю (чтобы как можно раньше удалить нежелательный трафик).

ACL представляет собой набор текстовых выражений, в которых написано permit (разрешить) либо deny (запретить), и обработка ведется строго в том порядке, в котором заданы выражения. Соответственно когда пакет попадает на интерфейс, он проверяется на первое условие, если первое условие совпадает с пакетом, дальнейшая его обработка прекращается. Пакет либо перейдет дальше, либо уничтожится. **В каждом конце списка стоит неявный deny any (запретить весь трафик).**

ACL делятся на типы:

– Стандартные нумерованные списки доступа (Standart Numbered ACL)

– Расширенные нумерованные списки доступа (Extended Numbered ACL)

– Дополнительные нумерованные списки (1300-1999 - стандартные, 2000-2699 - расширенные)

– Именованные (Named ACL)

Рассмотрим стандартные и расширенные ACL

Сами ACL создаются отдельно, то есть это просто некий список, который создается в глобальном интерфейсе, потом он присваивается к интерфейсу и только тогда он и начинает работать. Необходимо помнить некоторые моменты, чтобы правильно настроить списки доступа:

– Обработка ведется строго в том порядке, в котором записаны условия;

– Если пакет совпал с условием, дальше он не обрабатывается;

– В конце каждого списка доступа стоит неявный deny any (запретить всё);

– Расширенные ACL нужно размещать как можно ближе к источнику, стандартные же как – можно ближе к получателю;

– Нельзя разместить более 1 списка доступа на интерфейс, на протокол, на направление;

– ACL не действует на трафик, сгенерированный самим маршрутизатором;

– Для фильтрации адресов используется WildCard маска.

WildCard-маска – это обратная маска. Берем шаблонное выражение: 255.255.255.255 и отнимаем от шаблона обычную маску 255.255.255.0, у нас получается маска 0.0.0.255, что является WildCard маской.

3.1.Стандартные списки доступа

Стандартные списки управления доступом используются при необходимости заблокировать или, наоборот, разрешить весь поток данных от какой-либо сети или хоста, а также отказать в доступе набору протоколов.

Стандартные списки управления доступом проверяют адреса источников для пакетов, которые могут быть обработаны маршрутизатором. В результате предоставляется доступ или отказывается в нем всему протоколу.

Для определения списка с номером используется стандартная команда установки конфигурации access-list. Она используется в командном режиме задания глобальной конфигурации.

Полная форма команды имеет вид:
Router(config)# ***access-list*** *номер-списка* {***permit*** **|** ***deny***} *source [log]*

Параметр	Описание
номер - списка	Номер списка управления доступом. Представляет собой десятичное целое число от 1 до 99 (для стандартных IP-списков)
deny	Отказ в доступе, если условие выполнено
permit	Разрешение доступа, если условие выполнено
source	Номер сети или хоста, с которого посылается пакет. Либо host IP, либо IP MASK, либо any
log (Необязательный)	Вызывает появление информационного сообщения о регистрации в системном журнале (logging message) пакета, который удовлетворяет ссылке, которая будет послана на консоль.

Для отображения на экране содержания всех списков используется команда ***show access-lists***. Она может использоваться и для отображения одного списка.

Команда ***ip access-group*** применяет уже существующий список управления доступом к конкретному интерфейсу. Команда имеет следующий формат: Router (config) # ***ip access-group*** *номер-списка* **in | out**

Параметр	Описание
номер-списка	Указывает номер списка управления доступом, который будет логически связан с данным интерфейсом
in | out	Показывает, к какому из интерфейсов будет применяться список управления доступом - к входному или выходному.

Для удаления списка необходимо сначала ввести команду: ***no ip accessgroup*** *номер-списка* для каждого интерфейса, на котором он использовался, а затем команду ***no access-list*** *номер-списка*.

Комбинация *«адрес – маска шаблона»* вида *0.0.0.0 255.255.255.255* – то есть соответствующая всем возможным адресам – может быть записана в виде отдельного ключевого слова ***any***. Если маску не указать в процессе настройки списка доступа, то это будет равносильно *0.0.0.0*, что соответствует одному узлу.

3.2.Расширенные списки доступа

Расширенные списки управления доступом используются чаще, чем стандартные, поскольку они обеспечивают большие возможности контроля.

Расширенные списки проверяют как адрес источника, так и адрес получателя. Они могут также проверять конкретные протоколы, номера портов и другие параметры. Это придает им большую гибкость в задании проверяемых условий.

Для одного списка можно определить несколько директив. Каждая из них должна ссылаться на имя или на номер, чтобы все они были связаны с одним и

тем же списком. Количество директив может быть произвольным и ограничено лишь объемом имеющейся памяти. Конечно, чем больше в списке директив, тем труднее понять работу списка и контролировать ее.

Номера расширенных списков находятся в диапазоне от 100 до 199.

Полный формат команды ***access-list*** имеет следующий вид:

Router(config)# ***access-list*** *номер-списка {**permit** | **deny**} протокол IP-адрес_источника маска-шаблон [оператор порт] IP-адрес_получателя маска-шаблон [оператор порт] [established]*

Параметр	Описание
номер-списка	Указывает список, используются номера от 100 до 199
permit | deny	Указывает на то, разрешает ли данная позиция доступ к указанному адресу
протокол	Используемый протокол, например IP, TCP, UDP, ICMP, IGRP
IP-адрес_источника и IP-адрес_получателя	Указывает адреса источника и получателя
Маска -источника и маска -получателя	Шаблон маски, нули указывают позиции, которые должны соответствовать заданным условиям, в то время как единицы указывают позиции, значение которых не влияет на доступ
оператор порт	it, gt, eq, neq (меньше чем, больше чем, равно, не равно) и номер порта
established	Разрешает прохождение TCP-потока, если он использует установленное соединение (т.е. если бит АСК в заголовке сегмента установлен)

Связать созданный расширенный список с выходным или входным интерфейсом можно также командой ***ip access-group***.

Router(config)# ***ip access-group*** *номер-списка **{in | out}***

Некоторые часто используемые зарезервированные номера портов приведены в таблице.

Номер порта	Ключевое слово	Описание	Протокол
1-4		Не назначено	
20	FTP-DATA	FTP(данные)	TCP
21	FTP	FTP	TCP
23	TELNET	Терминальное соединение	TCP
25	SMTP	SMTP	TCP
42	NAMESERVER	Сервер имен	UDP
53	DOMAIN	DNS	TCP/UDP
69	TFTP	TFTP	UDP
70		Gopher	TCP/IP
80		WWW	TCP
133-159		Не назначены	
160-223		Зарезервированы	
161		FNP	UDP
224-241		Не назначены	
242-255		Не назначены	

Утилиты ***ping*** и ***traceroоute*** используют для отправки эхо-пакетов протокол ICMP. Для ограничения работы данных утилит необходимо в списках доступа устанавливать ограничения на работу протокола ***icmp***.

Просмотр имеющихся списков доступа: router# ***show access-lists***

Пример. *Необходимо запретить установление соединений с помощью протокола telnet со всеми хостами сети 1.16.195.0 netmask 255.255.255.0 со стороны всех хостов Интернета, причем в обратном направлении все соединения должны устанавливаться; остальные TCP-соединения разрешены.*

Фильтр устанавливается для входящих сегментов со стороны Интернета (предположим, что к Интернету маршрутизатор подключен через ин-

терфейс S0):

Router(config)# access-list 100 permit tcp any 1.16.195.0 0.0.0.255 eq 23 established

Router(config)# access-list 100 deny tcp any 1.16.195.0 0.0.0.255 eq 23

Router(config)# access-list 100 permit ip any any

Router(config)# interface se0

Router(config-if)# ip access-group 100 in

Указание ***ip*** в команде ***access-list*** означает «все протоколы». В конце каждого списка доступа по умолчанию подразумевается ***deny ip any any***, поэтому в примере мы указали ***permit ip any any***. Таким образом, наше правило срабатывает раньше и пропускает все пакеты, не попавшие по предшествующие его критерии.

Подробную статистику работы списков доступа можно получить, включив режим ***ip accounting***: Router(config-if)# ***ip accounting access-violations***

Просмотр накопленной статистики (с указанием адресов отправителей и получателей датаграмм): router# ***show ip accounting access-violations***

4. ПРАКТИЧЕСКАЯ ЧАСТЬ

4.1.Настройка стандартных списков контроля доступа

1. Откройте файл

Напомним, стандартные списки необходимо размещать как можно ближе к получателю

2. Создайте список, разрешающий доступ на PC2 только с PC0

Создайте список с номером 1

Router(config)#access-list 1 permit 192.168.1.2

в конце списка стоит неявный deny any

Закрепляем его за интерфейсом fa1/0

Router(config)#int fa1/0

Список будет действовать на исходящем направлении

Router(config-if)#ip access-group 1 out

3. Просмотрите созданный список
Router#show access-lists

```
Standard IP access list 1
    permit host 192.168.1.2
```

Видим, что созданный список стандартный с номером 1

4. Проверьте работу списка
Пропингуйте PC2 со всех устройств в сети
Так как в конце списка стоит неявный deny any (запретить весь трафик), пинги на PC2 должны проходить только с компьютера PC0, убедитесь в этом

5. Удалите список
Зайдите на интерфейс, на котором закреплен список
Router(config)#int fa1/0
Удалите список с интерфейса
Router(config-if)#no ip access-group 1 out
Удалите сам список
Router(config-if)#no access-list 1

6. Проверьте, что список удален командой *show access-lists*

7. Разрешим доступ к серверу из подсети 192.168.1.0
Router(config)#access-list 2 permit 192.168.1.0 0.0.0.255
Router(config)#int fa6/0
Router(config-if)#ip access-group 2 out

8. Проверьте работу списка пропинговав сервер с компьютеров PC0, PC1 и PC2
С компьютера PC2 пинг не пройдет

```
PC>ping 10.10.1.2

Pinging 10.10.1.2 with 32 bytes of data:

Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.

Ping statistics for 10.10.1.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

9. Удалите список, используя команды *no ip access-group* и *no access-list*

4.2.Расширенные списки доступа

1. Разрешите доступ компьютера PC0 к ftp серверу, а компьютеру PC1 запретите доступ

По умолчанию на сервере в Cisco Packet Tracer уже поднят FTP- сервер с логином и паролем **cisco**. Проверьте это с PC1:

```
PC>ftp 10.10.1.2
Trying to connect...10.10.1.2
Connected to 10.10.1.2
220- Welcome to PT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>
```

Доступ к ftp-серверу есть.

Создайте два правила на 20 и 21 порты. Эти порты отвечают за передачу данных по FTP.

В конце добавьте правило, разрешающее все остальным устройствам доступ к ftp-серверу

Router(config)#access-list 111 permit tcp host 192.168.1.2 host 10.10.1.2 eq 20
Router(config)#access-list 111 permit tcp host 192.168.1.2 host 10.10.1.2 eq 21
Router(config)#access-list 111 permit ip any any
Router(config)#int fa0/0
Router(config-if)#ip access-group 111 in

2. Проверьте соединение ftp-сервера и компьютеров

Проверка связи с сервером с PC0

```
PC>ftp 10.10.1.2
Trying to connect...10.10.1.2
Connected to 10.10.1.2
220- Welcome to PT Ftp server
```

Связь есть

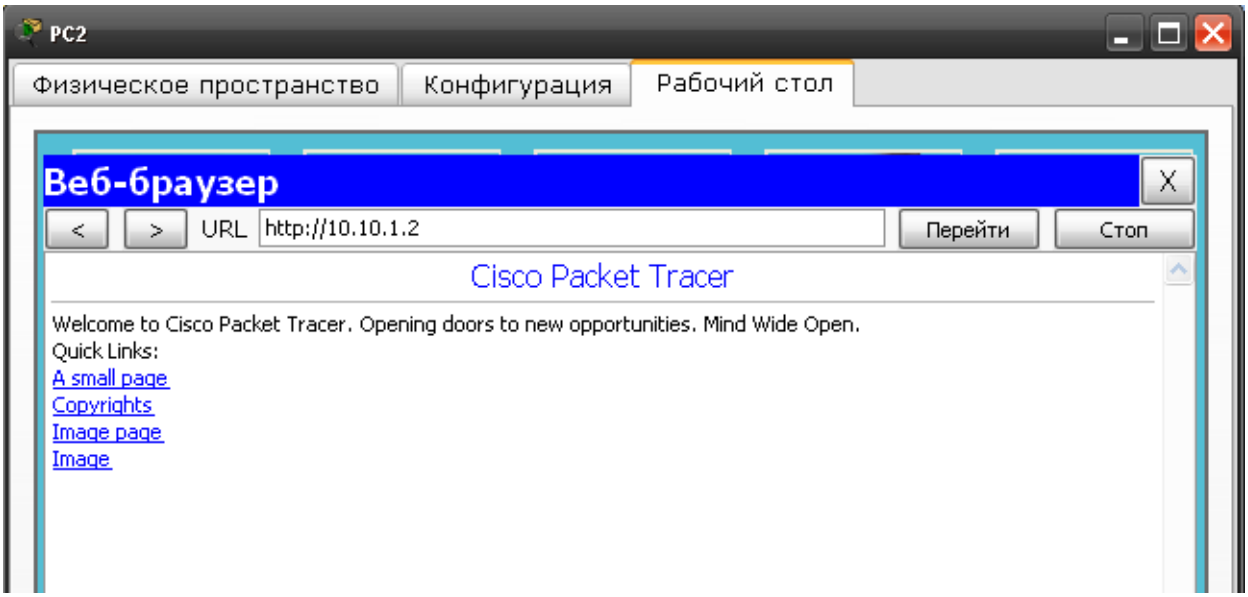
Проверка связи с сервером с PC1

```
PC>ftp 10.10.1.2
Trying to connect...10.10.1.2

%Error opening ftp://10.10.1.2/ (Timed out)
.



Packet Tracer PC Command Line 1.0
PC>(Disconnecting from ftp server)



Packet Tracer PC Command Line 1.0
```

Доступа к ftp серверу нет

3. Запретите обращение с компьютера PC2 на web-сервер

Проверьте, что связь с web-сервером есть. Зайдите на PC2 выберите вкладку Рабочий стол, зайдите в веб-браузер и введите ip-адрес сервера.



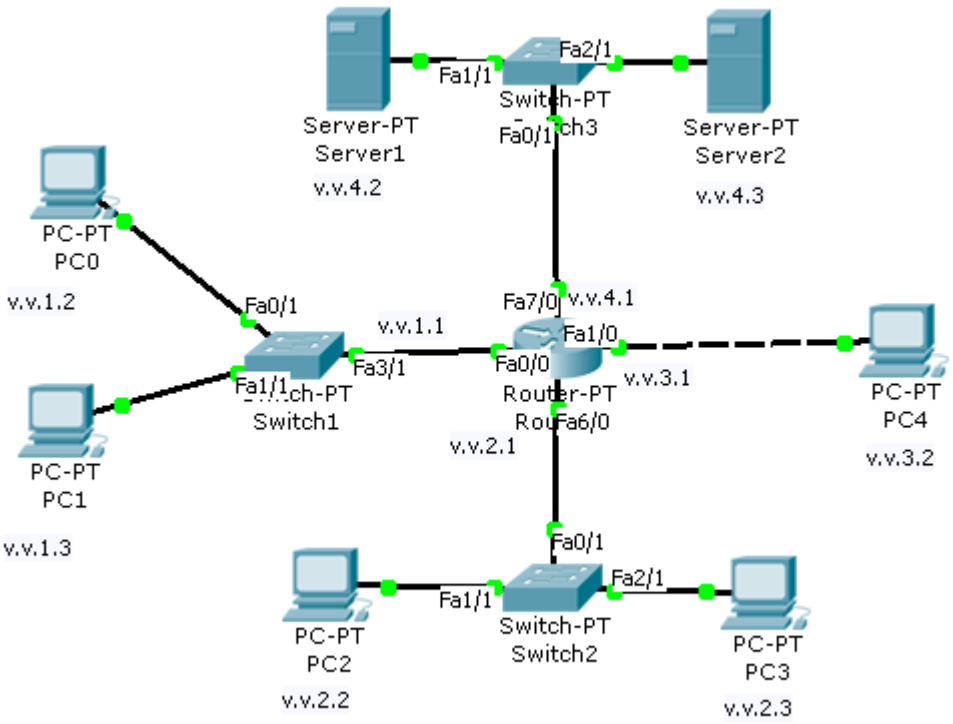
Router(config)#access-list 110 deny tcp host 192.168.2.2 host 10.10.1.2 eq 80
Router(config)#int fa1/0
Router(config-if)#ip access-group 110 in

Попробуйте связаться с web-сервером снова. Соединение должно отсутствовать.

5. ЗАДАНИЕ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ

Постройте в Packet Tracer топологию, представленную на рисунке.

Задайте ip-адреса компьютерам согласно рисунку, v – это номер варианта. Все маски 255.255.255.0.



Выполните задания, используя стандартные списки контроля доступа

1. Разрешите доступ с PC0 на PC4, а с PC1 запретите. Проверьте настройку списка, пропинговав компьютеры.

2. Запретите доступ с PC2 на подсеть v.v.1.0, затем проверьте настройку, пропинговав с PC2 на PC0 и с PC3 на PC0

3. Разрешите доступ с PC3 на Server1 и Server2, а с Pc2 запретите.

Пропингуйте устройства.

4. Просмотрите списки с помощью команды *show access-lists,* сделайте скриншот.

5. Удалите все списки, используя команды *no ip access-group* и *no access-list.*

Выполните задания, используя расширенные списки контроля доступа

1. Разрешите доступ только на Server1 с подсети v.v.1.0

Проверьте работу списка

2. Запретите с Server1 посылать icmp пакеты только на PC4, разрешите передачу данных по протоколу ip на все остальные устройства.

Проверьте работу списка

3. Разрешите доступ с PC4 только на PC2 и PC0

Проверьте работу списка

Объясните, почему не пингуется PC0 с PC4.

4. Разрешите доступ на ftp – сервер Server1 с PC2, а с PC3 разрешите доступ на web – сервер Server2. Разрешите доступ с PC2 на PC4, разрешите передачу icmp пакетов с подсети 20.20.2.0 на все устройства

Проверьте работу списка

5. Просмотрите списки с помощью команды *show access-lists,* сделайте скриншот.

6. СОДЕРЖАНИЕ ОТЧЁТА

Отчёт готовится в электронном виде. Отчёт содержит:

1. Скриншот топологий практической части.
2. Скриншоты всех созданных списков.
3. Скриншот топологии самостоятельного задания с адресами своего варианта.
4. Все введенные команды самостоятельного задания.
5. Все скриншоты, указанные в задании для самостоятельной работы.

ЛАБОРАТОРНАЯ РАБОТА № 3

НАСТРОЙКА VLAN

1. ЦЕЛЬ РАБОТЫ:

1.1.Изучить понятие виртуальных сетей.

1.2.Научиться настраивать виртуальные сети.

2. ПОРЯДОК ПРОВЕДЕНИЯ РАБОТЫ

2.1. Изучить теоретический материал

2.2. Проделать практическое задание

2.3. Выполнить задания для самостоятельной работы

2.4. Оформить отчет

2.5 Защитить лабораторную работу

3. ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

По умолчанию на каждом порту коммутатора в устройствах Cisco имеется сеть VLAN1 или VLAN управления. Сеть управления не может быть удалена, однако могут быть созданы дополнительные сети VLAN и этим альтернативным VLAN могут быть дополнительно назначены порты.

Типы портов в терминологии Cisco:

access port — порт принадлежащий одному VLAN'у и передающий нетегированный трафик

trunk port — порт передающий тегированный трафик одного или нескольких VLAN'ов

Создание VLAN'а и задание имени для него:
sw1(config) # ***vlan*** *номер-vlan*
sw1(config-vlan) # ***name*** *имя-vlan*
Настройка access портов
Назначение порта коммутатора в VLAN:
sw1(config) # ***interface*** *порт*
sw1(config-if) # ***switchport mode access***
sw1(config-if) # ***switchport access vlan*** *номер-vlan*
Назначение диапазона портов в vlan:
sw1(config) # ***interface range*** *порт-порт*
sw1(config-if-range) # ***switchport mode access***
sw1(config-if) # ***switchport access vlan*** *номер-vlan*
Просмотр информации о VLAN'ах:
sw1# show vlan brief
Для того чтобы передать через порт трафик нескольких VLAN, порт переводится в режим транка.
Настройка транка
sw1(config) # ***interface*** *порт*
sw1(config-if) # ***switchport mode trunk***
По умолчанию в транке разрешены все VLAN. Можно ограничить перечень VLAN, которые могут передаваться через конкретный транк.
sw1(config) # ***interface*** *порт*
sw1(config-if) # ***switchport trunk allowed vlan*** *диапазон номеров vlan*
Настройка VLAN на маршрутизаторах Cisco

Для логических подынтерфейсов необходимо указывать то, что интерфейс будет получать тегированный трафик и указывать номер VLAN, соответствующий этому интерфейсу. Это задается командой в режиме настройки подынтерфейса:
*R1(config-if)#****encapsulation dot1q*** *номер-vlan*
Создание логического подынтерфейса для VLAN :
*R1(config)#i****nterface*** *порт*
*R1(config-if)#****encapsulation dot1q*** *номер подынтерфейса*
*R1(config-if)#****ip address*** *подынтерфейса маска*
Соответствие номера подынтерфейса и номера VLAN не является обязательным условием. Однако обычно номера подынтерфейсов задаются именно таким образом, чтобы упростить администрирование.

4. ПРАКТИЧЕСКАЯ ЧАСТЬ

4.1.Настройка VLAN

1. Откройте файл

2. Настроим Switch1

Сначала создадим два vlan: vlan 10 и vlan 20 и назовем их firstvlan и secondvlan соответственно.

```
Switch1(config)#vlan 10
Switch1(config-vlan)#name firstvlan
Switch1(config-vlan)#vlan 20
Switch1(config-vlan)#name secondvlan
```

3. Просмотрим созданные vlan

```
Switch1#show vlan brief
```

```
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa1/1, Fa2/1, Fa3/1
                                                Fa4/1, Fa5/1
10   firstvlan                        active
20   secondvlan                       active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

В результате выполнения команды на экране появится таблица: номера vlan – первый столбец, название vlan - второй столбец, состояние vlan (работает он в данный момент или нет) – третий столбец, порты, принадлежащие к данному vlan – четвертый столбец. Видим, что на коммутаторе настроено 7 vlan, 5 по умолчанию и 2 мы создали сами. Все порты коммутатора по умолчанию принадлежат vlan 1.

3. Укажем, что порты fa1/1, fa2/1 аксесс порты, а также к каким vlan они являются портами доступа

Заходим сначала на интерфейс fa1/1

```
Switch1(config)#int fa1/1
```

Указываем, что этот порт это аксесс порт

```
Switch1(config-if)#switchport mode access
```

Укажем, что этот порт относится к vlan 10

```
Switch1(config-if)#switchport access vlan 10
```

Зайдем на интерфейс fa2/1 и проделаем те же шаги

```
Switch1(config)#int fa2/1
Switch1(config-if)#switchport mode access
Switch1(config-if)#switchport access vlan 20
```

3. Просмотрим vlan

Switch1#show vlan brief

```
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa4/1, Fa5/1
10   firstvlan                        active    Fa1/1
20   secondvlan                       active    Fa2/1
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

Видим, что порты доступа относятся к нужным нам vlan

4. Настроим порт fa3/1 для передачи трафика сразу нескольких vlan-ов по одной линии между коммутаторами

Заходим сначала на интерфейс fa3/1

Switch1(config)#int fa3/1

Указываем, что этот порт это транковый порт

Switch1(config-if)#switchport mode trunk

Укажем данные каких vlan будет пропускать этот порт

Сначала настроим так, чтобы пропускались данные всех vlan

Switch1(config-if)#switchport trunk allowed vlan all

Просмотрим конфигурациюSwitch1

Switch1(config)#show run

```
interface FastEthernet0/1
!
interface FastEthernet1/1
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet2/1
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet3/1
 switchport mode trunk
!
interface FastEthernet4/1
!
interface FastEthernet5/1
!
interface Vlan1
 no ip address
 shutdown
!
```

5. Настроим таким же образом Switch2 и просмотрим конфигурацию Switch2

Switch2(config)#show run

6. Пропингуем компьютеры, находящиеся в vlan 10

PC1>ping 192.168.10.2

Пинг прошел

7. Пропингуем компьютеры, находящиеся в vlan 20

PC3>ping 192.168.20.2

Пинг прошел, то есть трафик наших vlan свободно ходит между коммутаторами

8. Пропингуем компьютеры, находящиеся в разных vlan

PC2>ping 192.168.20.2

Пинг не прошел

9. На интерфейсах fa3/1 разрешим передачу трафика, относящегося к vlan 20, закроем трафик, относящийся к vlan 10

Зайдем на интерфейс fa3/1

Switch1(config)#int fa3/1

Разрешим передачу только трафика vlan 20

Switch1(config-if)#switchport trunk allowed vlan 20

Проделаем аналогичные действия на Switch2

Switch2(config)#int fa3/1

Switch2(config-if)#switchport trunk allowed vlan 20

10. Попробуем пропинговать компьютеры vlan 20

PC3>ping 192.168.20.2

Пинг прошел

Попробуем пропинговать компьютеры vlan 10

PC1>ping 192.168.10.2

Пинг не прошел, проходит трафик относящийся только к vlan 20

4.2.Маршрутизация между vlan

1. Откроем файл

2. Switch#show vlan bri

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa1/1, Fa2/1, Fa3/1
                                                 Fa4/1, Fa5/1
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

Видим, что есть только стандартные vlan и все порты принадлежат vlan 1

3. Создадим 3 vlan
Switch(config)#vlan 2
Switch(config-if)#vlan 3
Switch(config-if)#vlan 4

4. Просмотрим созданные vlan
Switch#show vlan bri

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa1/1, Fa2/1, Fa3/1
                                                 Fa4/1, Fa5/1
2    VLAN0002                          active
3    VLAN0003                          active
4    VLAN0004                          active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

Просмотрев, увидим, что появились 3 новых vlan

5. Настроим порты fa1/1, fa2/1, fa3/1
Switch(config)#fa1/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 2
Таким же образом настроим порты fa2/1, fa3/1

6. Просмотрим
Switch#show vlan bri

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa4/1, Fa5/1
2    VLAN0002                          active    Fa1/1
3    VLAN0003                          active    Fa2/1
4    VLAN0004                          active    Fa3/1
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

Видим, что порты принадлежат нужным нам vlan

7. Настроим интерфейс fa0/1
Switch(config)#fa0/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan all
Просмотрим настройку трнкового порта
Switch#show int trunk

```
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/1       1-1005

Port        Vlans allowed and active in management domain
Fa0/1       1,2,3,4

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,2,3,4
```

Видим, что этот vlan будет пропускать трафик всех vlan

8. Чтобы обеспечить маршрутизацию между vlan, необходимо настроить субинтерфейсы на маршрутизаторе

Зайдем на интерфейс fa0/0 и уберем ip-адрес
Router(config)#int fa0/0
Router(config-if)#no ip address

Настроим субинтерфейсы
Router(config)#int fa0/0.2
Router(config-subif)#encapsulation dot1Q 2
Router(config-subif)#ip addr 1.1.2.1 255.255.255.0

Router(config)#int fa0/0.3
Router(config-subif)#enapsulation dot1Q 3
Router(config-subif)#ip addr 1.1.3.1 255.255.255.0
Аналогично настроим третий субинтерфейс

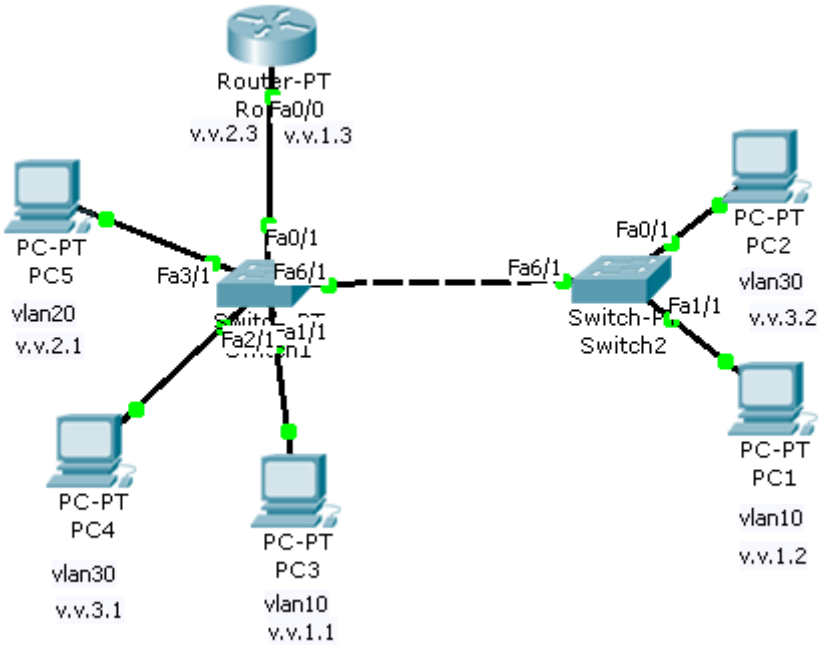
9. Просмотрим созданные субинтерфейсы
Router#show ip int brief

```
Interface              IP-Address      OK? Method Status                Protocol

FastEthernet0/0        unassigned      YES manual up                    up

FastEthernet0/0.2      1.1.2.1         YES manual up                    up

FastEthernet0/0.3      1.1.3.1         YES manual up                    up

FastEthernet0/0.4      1.1.4.1         YES manual up                    up

FastEthernet1/0        unassigned      YES unset  administratively down down

Serial2/0              unassigned      YES unset  administratively down down
```

10. Настроим основные шлюзы для компьютеров
Для PC1 шлюз 1.1.2.1
PC2 шлюз 1.1.3.1
PC3 шлюз 1.1.4.1
Теперь все компьютеры можно пропинговать. Проверьте это.

5. ЗАДАНИЕ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ

1. Построить в Packet Tracer топологию, представленную на рисунке. Необходимо обеспечить передачу трафика между 10 и 20 vlan



Задайте ip-адреса компьютерам согласно рисунку, v – это номер варианта. Все маски 255.255.255.0.

2. Создайте vlan`ы и настройте интерфесы коммутаторов для соответствующих vlan.

Настройте транковые порты: между коммутаторами для передачи трафика всех vlan между коммутатором и роутером для передачи трафика 10 и 20 vlan

3. Просмотрите созданные vlan, используя команту *show vlan brief* . Сделайте скриншот.

4. Необходимо обеспечить маршрутизацию трафика между vlan 10 и vlan 20. Для этого настройте субинтерфейсы на маршрутизаторе. Просмотрите созданные субинтерфейсы используя команту *show ip int brief.* Сделайте скриншот.

Затем настройте шлюзы для компьютеров соответствующих vlan.

5. Пропингуйте компьютеры, находящиеся в одном vlan.

Затем пропингуйте компьютеры из vlan 10 в vlan 20. Сделайте скриншоты.

Пропингуйте компьютеры из vlan 10 в vlan 30, рассмотрите результаты, поясните их.

6. Просмотрите конфигурацию коммутаторов, используя команду *show run.* Сделайте скриншоты.

6. СОДЕРЖАНИЕ ОТЧЁТА

Отчёт готовится в электронном виде. Отчёт содержит:

1. Скриншоты топологий практической части.
2. Конфигурации коммутаторов.
3. Скриншот топологии самостоятельного задания с адресами своего варианта.
4. Все введенные команды самостоятельного задания.
5. Все скриншоты, указанные в задании для самостоятельной работы.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Суконщиков, А.А., Методы и средства защиты компьютерной информации: учебное пособие / А.А. Суконщиков, Е.Н. Давыдова. – Вологда: ВоГТУ, 2008. - 132с.

2. Мельников, В.П. Информационная безопасность и защиты информации: учеб. пособие для вузов / В.П. Мельников, С.А. Клейманов, А.М. Петраков; под ред. С.А. Клейманова. – 3-е изд., стер. – М.: Academia, 2008. – 330 с.

Подписано в печать 15.05.2014.	Усл. печ. л. 1,9	Тираж 15 экз.
Печать офсетная.	Бумага писчая.	Заказ №____.

Отпечатано: РИО ВоГУ, г. Вологда, ул. С. Орлова, 6