МИНИСТЕРСТВО ПО РАЗВИТИЮ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И КОММУНИКАЦИЙ РЕСПУБЛИКИ УЗБЕКИСТАН

ТАШКЕНТСКИЙ УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ИМЕНИ МУХАММАДА АЛ-ХОРАЗМИЙ

Кафедра «Кибербезопасности и криминалистики»

МЕТОДИЧЕСКОЕ ПОСОБИЕ

по выполнению лабораторных работ по дисциплине

"Безопасность сети"

для студентов бакалавриатуры (заочной и второй специальности) по направлению 5330300- "Информационная безопасность"", 5330500 – "Компьютерный инжиниринг" (компьютерный инжиниринг, ИТ - услуги), 5350100 – "Телекоммуникационные технологии" (телекоммуникации, мобильные системы)

Ташкент – 2022

В методической пособии рассматриваются такие вопросы, которые направлены на формирование практических знаний, умений и навыков по правильной планирование структуру сетей, регистрации и расследованию сетевых событий и инцидентов, на развитие самостоятельного мышления обучающихся, умения сопоставлять, анализировать вопросы реагирования и управления инцидентами информационной безопасности в сетевом уровне. Общей целью рассматриваемого пособия является оказание помощи в изучении процедур реагирования на инциденты сетевых структур организации и разработке предложений по совершенствованию системы управления информационной безопасностью.

Составитель:

Муминова С.Ш. — старший преподаватель кафедры «Кибербезопасность и криминалистика», ТУИТ

Рецензенты:

Насруллаев Н.Б. — директора Нурафшанского филиала Ташкентского университета информационных технологий имени Мухаммада ал-Хоразмий

Самаров Х.К — к.т.н, доцент кафедры «Обеспечение информационной безопасности», ТУИТ имени Мухаммад ал-Хоразмий

Методические указания рассмотрены и одобрены на заседании кафедры "Обеспечение информационной безопасности"
(___ _____ 2022 г. Протокол № _____)

Методические указания рекомендованы к печати на заседании научно-методического совета факультета "Информационная безопасность"
(___ _____ 2022 г. Протокол № _____)

Методические указания утверждены на Научно-методическом совете Ташкентского университета информационных технологий имени Мухаммада ал-Хоразмий
(___ _____ 2022 г. Протокол № _____)

ВВЕДЕНИЕ

В методическом пособии представлены вопросы ввиде лабораторных работ для установки базовых настроек безопасности на сетевых устройствах - Telnet, SSH, настройка Port Security на коммутаторах, анализ безопасности сетевых устройств, настройки протоколов STP, RSTP, LACP, PAgP, VTP, OSPF, RIP, EIGRP и BGP, настройка Access List (standard, extended), настройка NAT/PAT технологии, настройка протоколов SCP, SNMP и исследование лог файлов, а также настройка режима аутентификации в серверах AAA (RADIUS, TACACS+), анализ технологии безопасности - DHCP Snooping, анализ сетевой атаки ARP Poison, настройка технологии безопасности ASA, исследование протоколов PPTP, L2F, L2TP и IPSec, создание VPN сети в предприятиях, установка DMZ в сетевых маршрутизаторах, поиск и устранение проблем в сети. Troubleshooting, установка и настройка ПО Firewall, ПО IDS/IPS.

Курс «Безопасность сети» является предметом по специальности и преподается на 3 курсе обучения. Изучение данного курса требует знания и навыки по дисциплинам связанных с защитой информации, таких как «Основк кибербезопасности» и «Безопасность баз данных».

Методическое пособие состоит из таких компонентов, как тема практической работы, цель работы, порядок практической работы, задания для практической работы и контрольные вопросы.

В течение академического семестра студенты должны выполнять задания и представлять письменные отчеты на основе лабораторных рабочих инструкций. Каждый отчет, независимо от темы лабораторной работы, должен состоять из следующих компонентов:

1. Заглавная часть
2. Тема и цель работы.
3. Основная часть (последовательность выполненной работы)
4. Ответы на контрольные вопросы
5. Литература

ЛАБОРАТОРНАЯ РАБОТА №1
УСТАНОВКА ПЕРВИЧНЫХ НАСТРОЕК БЕЗОПАСНОСТИ НА СЕТЕВЫХ УСТРОЙСТВАХ

Цель работы: Изучение коммутационного устройства, его принцип работы, способы удалённого доступа, а также правила настройки показателей безопасности.

Краткая теоретические сведения

Есть несколько способов доступа к интерфейсу командной строки (CLI) устройств Cisco IOS. Ниже приведены наиболее распространенные методы:

- Консоль
- Telnet или SSH .
- порт AUX

Console port - Konsol porti это порт управления, который обеспечивает внешний доступ для настройки устройства Cisco. Преимущество использования консольного порта заключается в том, что к устройству можно получить доступ без настройки сетевых сервисов, например, в режиме начальной настройки сетевого устройства. Когда начальная настройка завершена, специальный компьютерный кабель (RS232) подключается к консольному порту устройства и выполняется настройка.

TELNET (terminal network) - это сетевой протокол для доступа к устройствам в сети. Современный стандарт протокола написан в RFC 854.

Функция протокола TELNET заключается в обеспечении взаимодействия между оконечными устройствами. Этот протокол используется для связи между терминалами.

Protokol Secureshell (SSH) - этот протокол обеспечивает безопасное (зашифрованное) соединение для управления удаленными устройствами. Для управления удаленными устройствами рекомендуется использовать протокол SSH вместо протокола Telnet. В локальных сетях Telnet можно использовать в

течение короткого времени. Telnet - это устаревший протокол, который позволяет, открыто передавать учетные данные (имена пользователей и пароли) между устройствами, так же как это происходит в виде незашифрованных защищенных данных. SSH обеспечивает защиту при подключении к удаленным устройствам. Надежно шифрует аутентификацию устройства (имя пользователя и пароль). Он также защищает данные, передаваемые между устройствами. SSH использует TCP-порт 22, Telnet использует TCP-порт 23.

Интерфейс командной строки (CLI) **AUX** - устаревший метод настройки сеанса, который подключается к вспомогательному порту маршрутизатора (AUX) через коммутируемое соединение на телефоне. Таким же образом, используя консольное соединение, вспомогательный метод также обеспечивает подключение вне сети и не требует настройки или сетевых служб. Если сетевые службы не работают, пульт дистанционного управления может получить доступ к коммутатору или маршрутизатору по телефонной линии.

Необходимые ресурсы:

– 1 коммутатор (операционная система Cisco 2960 Cisco IOS 15.0 (2), изображения);

– 1 ПК (операционная система для Windows 7, Vista или XP с терминалом эмулятора, например: TeraTerm, Patty);

– Console кабель для конфигурирования устройства Cisco IOS через консольный порт;

1. **Настройка базовых показателей для сетевого устройства**

1.1. Основными параметрами коммутатора: имя устройства, локальные пароли, баннер MOTD (сообщение, предупреждающее злоумышленника при доступе к устройству), адрес управления и настройка записей через Telnet.

а. Если файлы конфигурации не хранятся в NVRAM коммутатора, вы получите привилегию. Если строка изменилась на Switch>, **введите enable.**

```
Switch> enable
Switch #
```

b. Перейдите в режим глобальной конфигурации.

```
Switch # configure terminal
Switch (config) #
```

Строка снова изменилась, чтобы отобразить глобальный профиль конфигурации.

c. Назовите коммутатор.

```
Switch (config) # hostname S1
S1 (config) #
```

d. Настройка шифрования паролей.

```
S1 (config) # service password-encryption
S1 (config) #
```

e. Pass class как секретный пароль для доступа в режим Privilegirovan.

```
S1 (config) # enable secret class
S1 (config) #
```

f. Настройте баннер MOTD (сообщение, предупреждающее злоумышленника при доступе к устройству).

```
S1 (config) # banner motd #Запрещается доступ к устройству#
```

g. Убедитесь, что переходы в режимы установлены.

```
S1(config)# exit
S1# exit
```

Переключитесь из пользовательского режима в привилегированный. Введите **class**, когда будет предложено ввести пароль.

```
S1> enable
Password:
S1#
```

Примечание. Пароль не отображается в поле входа в систему.

i. Чтобы поместить IP-адрес коммутатора на переключатель SVI, перейдите в глобальный режим. Это позволяет дистанционно управлять коммутатором.

Перед переключением коммутатора на удаленный компьютер PC-A необходимо установить IP-адрес коммутатора на коммутатор S1. На основе конфигурации коммутатора коммутатор управляется через VLAN 1.

Установите IP-адрес 192.168.1.100 и сетевую маску 255.255.255.0 для внутреннего виртуального интерфейса (SVI) VLAN 1 коммутатора.

```
S1(config)# interface vlan1
S1(config-if)# ip address 192.168.1.100 255.255.255.0
S1(config-if)# no shutdown
S1(config-if)# exit
S1(config)#
```

2. Настройка конфигурации Console

Также вам необходимо ограничить доступ через порт **Console.** Основываясь на начальной конфигурации, все консольные подключения должны быть установлены без пароля. Команда logging synchronous введена для обеспечения непрерывности консольных сообщений.

```
S1 (config) # line console 0
S1 (config-line) # password cisco
S1 (config-line) # login
S1 (config-line) #exit
S1 (config) #
```

3. Настройка конфигурации Telnet

Чтобы разрешить доступ к коммутации через telnet, то есть пульт дистанционного управления, вам необходимо настроить виртуальный канал соединения (vty). Если вы не установили пароль vty, вы не сможете получить доступ к устройству через telnet.

```
S1 (config) # line vty 0 15
S1 (config-line) # password cisco
S1 (config-line) # login
S1 (config-line) # end
S1 #
```

Контрольные вопросы

1. В каком случае используется порт Console?
2. Зачем нужно настраивать канал VTY для коммутатора?
3. Как можно предотвратить передачу пароля в незашифрованном виде?
4. В каких целях используется протоколы Telnet и SSH?
5. Почему компьютеры имеют один и тот же сетевой адрес для доступа к устройствам?
6. Что означает командная строка vty 0 15?

ЛАБОРАТОРНАЯ РАБОТА № 2
НАСТРОЙКА PORT SECURITY НА КОММУТАТОРАХ

Цель работы: Освоение практических навыков по функцию коммутатора port – security, позволяющую обезопасить сеть от атак направленных на переполнение таблицы коммутации

Краткие теоретические сведения

Функция Port Security позволяет настроить какой-либо порт коммутатора так, чтобы доступ к сети через него мог осуществляться только определёнными устройствами. Устройства, которым разрешено подключаться к порту определяются по MAC-адресам. MAC-адреса могут быть изучены динамически или вручную настроены администратором сети. Помимо этого функция Port Security позволяет ограничивать количество изучаемых портом MAC-адресов, тем самым, ограничивая количество подключаемых к нему узлов. Также, данная функция ограждает коммутатор от атак, которые могут быть направлены на переполнение таблицы MAC адресов (Рис. 2.1).

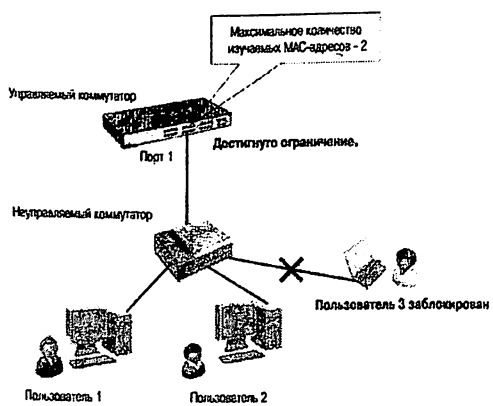


Рис. 2.1. Работа функции Port Security на коммутаторе

Существует два способа введения ограничений на MAC адреса:

1. Статический – когда администратор перечисляет, какие адреса разрешены

2. Динамический – когда администратор указывает, сколько адресов разрешено, а коммутатор обучается, запоминая, какие адреса в настоящий момент обращаются через указанный порт

Настройка режима реагирования на нарушения безопасности

Режимы реагирования на нарушение безопасности. Существует три способа реагирование на нарушение безопасности:

```
switch(config-if)# switchport port-security violation <protect | restrict | shutdown>
```

switchport port-security violation restrict - указывает режим реагирование на нарушение. Таким образом, если на данном интерфейсе одновременно «засветится» третий (неизвестный) MAC адрес, то все пакеты с этого адреса будут отбрасываться, при этом отправляется оповещение – syslog, SNMP trap, увеличивается счетчик нарушений (violetion counter).

switchport port-security violation shutdown- при выявлении нарушений переводит интерфейс в состояние error-disabled и выключает его. При этом отправляется оповещение SNMP trap, сообщение syslog и увеличивается счетчик нарушений (violation counter). Кстати, если интерфейс находится в состоянии error-disabled, то самым легким путем разблокировать его, является выключить и включить интерфейс (ввести в настройках интерфейса команду — «shutdown», а потом — «no shundown»).

Если же на интерфейсе введена команда — «**switchport port-security violation protect**», то при нарушениях, от неизвестного MAC адреса пакеты отбрасываются, но при этом никаких сообщений об ошибках не генерируется.

Какой именно способ выбрать дело каждого, но «switchport port-security violation restrict» является оптимальной для большинства случаев.

Последовательность выполнения задания

```
Switch>enable
Switch#configure terminal
Switch(config)#hostname Sw1
Sw1(config)#interface fa0/1
```

1. Устанавливаем порт в режим access

```
Sw1(config-if)#switchport mode access
```

2. Активируем port-security на порту

```
Sw1 (config-if)#switchport port-security
```

3. Устанавливаем динамическое определение secure-mac

```
Sw1 (config-if)#switchport port-security mac-address sticky
Sw1 (config-if)#exit
```

4. Устанавливаем статическое определение secure-mac

```
Sw1(config)#interface fastEthernet 0/2
Sw1(config-if)#switchport mode access
Sw1(config-if)#switchport port-security
Sw1(config-if)#switchport port-security mac-address 000B.BE9B.EE4A
Sw1(config-if)#end
```

5. Настройка режима реагирования на нарушения безопасности

```
Sw1(config)#interface fastEthernet 0/3
Sw1(config-if)#switchport mode access
Sw1(config-if)#switchport port-security
Sw1(config-if)#switchport port-security mac-address sticky
Sw1(config-if)#switchport port-security violation protect
Sw1(config-if)#end
```

6.Отключение неиспользуемых портов

```
Sw1(config)#interface range fastEthernet 0/5-24
Sw1(config-if-range)#shutdown
```

7. Устанавливаем максимальное количество secure-mac на порту

(это команда выполняется на коммутаторе Sw2)

```
Switch>enable
Switch#configure terminal
Switch(config)#hostname Sw2
Sw2(config)#interface fa0/4
Sw2(config-if)#switchport mode trunk
Sw2(config-if)#switchport port-security maximum 4
Sw2(config-if)#switchport port-security violation restrict
```

8. Проверяем результат

```
Switch#show port-security interface fa 0/1
Port Security : Enabled
Port Status : Secure-up
Violation Mode : Shutdown
Aging Time : 0 mins
Aging Type : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses : 1
Total MAC Addresses : 0
Configured MAC Addresses : 0
Sticky MAC Addresses : 0
Last Source Address:Vlan : 0001.63B4.E4A6:1
Security Violation Count : 0
```

9. Сохраняем конфигурацию

```
Switch#copy running-config startup-config
```

Задание:

Каждому студенты нужно выполнять лабораторные работы в среде Cisco Packet Tracer на основе приведенной выше информации и подготовить отчёт.

Контрольные вопросы:

1. Зачем нужно включать функцию безопасности порта на коммутаторе?
2. В чем заключается функция Port security?
3. Опишите основные атрибуты функция Port security.
4. Что такое MAC-адрес и как он определяется на устройствах?
5. Для чего в коммутаторе используется функция защиты порта?
6. В каких случаях используется максимальное количество N Secure-MAC?

7. Знаете ли вы какие-либо другие меры по обеспечению безопасности коммутатора?

ЛАБОРАТОРНАЯ РАБОТА № 3
АНАЛИЗ БЕЗОПАСНОСТИ СЕТЕВЫХ УСТРОЙСТВ

Цель работы: Освоение практических навыков по сбросу паролей на коммутаторах и маршрутизаторах Cisco.

Краткие теоретические сведения

Со всеми может произойти ситуация, когда забытый или потерянный пароль не позволяет получить доступ к оборудованию. Ниже мы рассмотрим, как сбросить пароль на маршрутизаторах и коммутаторах Cisco.

Стоит уточнить, что описанные способы подразумевают подключение к оборудованию только напрямую через консольный кабель. Поэтому стоит уделить внимание безопасности и сделать так, чтобы в серверную или помещение, где находится оборудование доступ имел только авторизованный персонал. Суть этих методов заключается в том, чтобы загрузиться без конфигурационного файла с забытым паролем, войти в привилегированный режим (**Privileged EXEC**), заменить новый конфигурационный файл на старый и поменять на нем все пароли.

Сброс пароля на маршрутизаторах Cisco

Для **броса пароля на маршрутизаторе cisco**, потребуется физический доступ к нему (подключение через консольный порт). В маршрутизаторе есть так называемый **конфигурационный регистр** – это переменная, хранящаяся в энергонезависимой памяти и управляющая процессом загрузки. Стандартное значение конфигурационного регистра для большинства маршрутизаторов «0x2102».

Если вы дошли хотя бы до уровня CCENT, вам должно быть известно такое понятие, как configuration register. Это 16-битный регистр, находящийся

в NVRAM-е, ответственный за последовательность загрузки маршрутизатора. А именно — откуда и в каком порядке маршрутизатор будет загружать свою операционную системы и файл настроек. Его дефолтное значение — 2102. Третья его цифра отвечает за файл настроек, четвёртая — за ОС. Наша цель — заставить маршрутизатор проигнорировать файл настроек при загрузке (именно в нём и находятся пароли) и открыть нам доступ к privileged mode. Этого мы добиваемся путём изменения третьего числа регистра на «4».

```
Router1#conf t
Router1(config)#enable password NewPassword
Router1(config)#enable secret NewPassword
Router1(config)#line vty 0 4
Router1(config-line)#password NewPassword
Router1(config-line)#login
Router1(config-line)#exit
Router1(config)#line console 0
Router1(config-line)#password NewPassword
Router1(config-line)#login
```

Теперь, когда мы сменили все пароли нам нужно вернуть старое значение конфигурационного регистра, введя из режима конфигурации команду **config-register 0x2102**

```
Router1(config)# config-register 0x2102
```

После этого сохраняем наш новый конфиг и перезагружаемся

```
Router1#copy running-config startup-config
Router1#reload
```

Когда роутер загрузится, то он возьмет сохраненный конфигурационный файл, с новыми паролями. Также, можно отключить возможность сброса пароля, используя команду **no service password-recovery**. Но как мы упомянули ранее, для этого метода восстановления требуется физический доступ к оборудованию.

Сброс пароля на коммутаторах Cisco Catalyst

Для того чтобы сбросить пароль на коммутаторе **Cisco Catalyst** нам также нужен физический доступ к оборудованию.

Подключаемся к свитчу консольным кабелем, выключаем его по питанию, а затем включаем, удерживая нажатой кнопку **Mode** на лицевой панели (рисунок 3.4.).

Рис. 3.4. Свитч (коммутатор), место нахождение кнопки «MODE».

Таким образом мы прервем обычный процесс загрузки.

```
Loading "flash:/c2960-lanbase-mz.122-25.FX.bin"...
##############################
Boot process terminated.
switch:
```

После этого мы вводим команды **flash_init** и **load_helper**. И теперь мы можем посмотреть содержимое нашей flash памяти, используя команду **dir flash:** (внимание – в конце команды должно стоять двоеточие)

```
switch: flash_init
Initializing Flash...
flashfs[0]: 3 files, 0 directories
flashfs[0]: 0 orphaned files, 0 orphaned directories
flashfs[0]: Total bytes: 64016384
flashfs[0]: Bytes used: 3059643
flashfs[0]: Bytes available: 60956741
flashfs[0]: flashfs fsck took 1 seconds.
...done Initializing Flash.
switch: load_helper
switch: dir flash:
Directory of flash:/

1   -rw-  3058048          c2950-i6q4l2-mz.121-22.EA4.bin
3   -rw-  979              config.text
2   -rw-  616              vlan.dat
60956741 bytes available (3059643 bytes used)
```

Мы видим содержимое нашей flash памяти и нам интересен файл **config.text** – файл конфигурации коммутатора. Сейчас нам нужно его переименовать, чтобы коммутатор загрузился без него. Делаем это командой **rename flash:config.text flash:config.old** и затем можно сделать проверку.

```
switch: rename flash:config.text flash:config.old
switch: dir.flash
Directory of flash:/
1   -rw-  3058048          c2950-i6q4l2-mz.121-22.EA4.bin
3   -rw-  979              config.old
2   -rw-  616              vlan.dat
60956741 bytes available (3059643 bytes used)
```

После этого возобновляем загрузку командой **boot**.

```
switch: boot
```

Коммутатор не найдет файл конфигурации и загрузится без него. Теперь входим в привилегированный режим, и переименовываем обратно наш конфиг, выполнив команду **rename flash:config.old flash:config.text**, а затем загружаем его командой **copy flash:config.text system:running-config**

```
Switch>en
Switch#rename flash:config.old flash:config.text
Switch#copy flash:config.text system:running-config
```

Теперь после того как конфигурация загружена мы можем задать новый пароль

```
Switch1#conf t
Switch1(config)#enable secret NewPassword
Switch1(config)#enable password NewPassword
Switch1 (config)#line vty 0 4
Switch1 (config-line)#password NewPassword
Switch1 (config-line)#login
Switch1 (config-line)#exit
Switch1 (config)#line console 0
Switch1 (config-line)#password NewPassword
Switch1 (config-line)#login
```

Задание:

Студенты выполняют лабораторные работы в среде Cisco Packet Tracer на основе приведенной выше материала. Нужно рассмотреть случаи забывания или утери паролей, установленных на коммутаторах и маршрутизаторах. Делает сброс паролей и установит новые пароли. Представляет отчет о проделанных работ.

Контрольные вопросы:

1. Инструменты безопасности сетевых устройств
2. Какие методы вы знаете, чтобы восстановить забытые пароли?
3. В каких случаях сбрасываются пароли или устанавливается новый пароль?
4. Какие типы памяти доступны на устройствах Cisco?

ЛАБОРАТОРНАЯ РАБОТА №4
НАСТРОЙКА ПРОТОКОЛОВ РЕЗЕРВИРОВАНИЯ – STP, RSTP И ПРОТОКОЛОВ АГРЕГИРОВАНИЯ – LACP, PAGP

Цель работы: Освоение практических навыков по настройке протоколов канального уровня STP, RSTP, LACP, PAGP.

Задание:

1. Задание по протоколам STP (spanning-tree protocol) и RSTP:

– Настройте и проверьте интерфейсы коммутаторов SW1, SW2 и SW3, как показано на рисунке 4.1;

– Настройка и тестирование коммутаторов согласно протоколу STP;

– Сделать каждый коммутатор корневым и изменить направление кадра;

– Проанализировать результаты каждой конфигурации коммутатора.

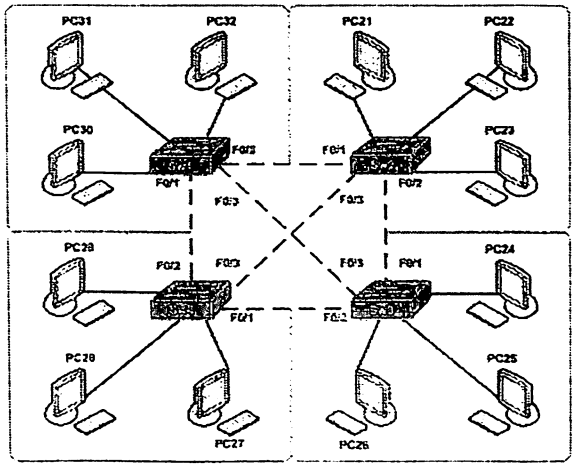


Рис. 4.1. Топология сети на основе протокола STP

2. Задание по настройке протоколов агрегирования LACP и PAGP

– Настройка и проверка интерфейсов коммутатора S1, S2 как показано на рисунке 4.9;
– Конфигурация агрегаций каналов с помощью протоколов LACP или PagP;
– Изучение функций команд написанные на каждом коммутаторе.

Краткое теоретическое сведения по первой задаче

Протокол STP - это протокол канального уровня модели OSI, основанный на стандарте IEEE 802.1d. Протокол STP был разработан в 1985 году Радиа Перлман. Протокол имеет следующие характеристики: PVSP +, RSTP, MSTP, SPM.

Основное назначение протокола STP - предотвращение образования петель (петель) в канале между несколькими коммутаторами, подключенными друг к другу в произвольной топологии в сети Ethernet. Протокол STP основан на создании логического дерева коммутаторов в сети. В верхней части дерева находится корневой коммутатор, а следующая ветвь - некорневые коммутаторы. Когда коммутаторы подключены друг к другу, можно физически соединить другие каналы, используя основной магистральный канал, но они будут логически автоматически заблокированы (рисунок 4.2). Процесс построения дерева состоит из следующих шагов:

- Выбор корневого переключателя;
- Выбор корневых портов;
- Выбор назначенных портов.

При выборе корневого коммутатора, который является основным в сети, коммутатор выбирается на основе минимального значения приоритета или значения его идентификатора. Здесь значение ID представляет MAC-адрес коммутатора, т. е. Наименьшее значение - это корневой коммутатор в сети. Коммутаторы отправляют друг другу кадры Hello BPDU каждые 2 секунды, чтобы определить, какой из них является корневым. Значения привилегий и идентификаторов идентификаторов снимков, полученных от соседей, сравниваются, и, если их значения выше, он перестает требовать корневую позицию и начинает рассылать сообщение Hello BPDU победителю. Нам нужно знать, что если привилегии равны при сравнении, то корневой коммутатор выбирается путем сравнения их идентификаторов.

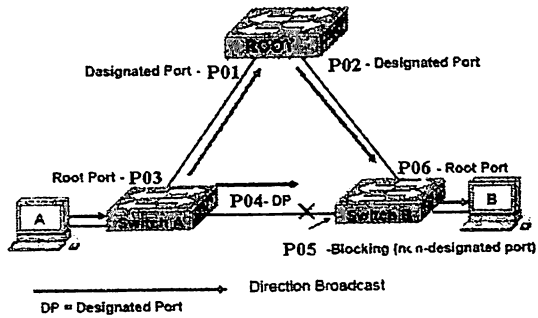


Рис. 4.2. Типы портов в протоколе STP

Протокол множественного связующего дерева (MSTP) определен в стандарте IEEE 802.1s и впоследствии дополнен IEEE 802.1Q-2003. Протокол MSTP - это улучшенная версия стандарта IEEE 802.1w (RSTP) для поддержки нескольких копий протокола STP. Это ускоряет работу сети и позволяет сбалансировать нагрузку на сеть, в которой настроена VLAN. 802.1s - это дополнение к MSTP 802.1Q.

Последовательность выполнения работы:

Настройте базовые конфигурации для коммутаторов Sw1, Sw2, Sw3, Sw4 в соответствии с топологией, показанной на рисунке 4.3.

Среди коммутаторов в сетевой топологии, приведенной выше, главный корневой коммутатор (root) - это Sw1. Потому что в этой топологии Sw1 имеет наименьший значение MAC-адрес, чем другие коммутаторы. Поэтому мы видим, что все порты интерфейса ввода и вывода на коммутаторе Sw1 зеленые. Чтобы проверить это, используйте команду *Sw1#show spanning-tree*. В результате мы можем узнать *MAC-адрес 000D.BD2C.15B9* коммутатора Sw1 или главного коммутатора (*This bridge is the root*) (рисунок 4.4).

На рисунке. 4.5 видно что, после команды show spanning-tree на коммутаторе Sw2, по порту fastEthernet 0/4 определяется главный корневой коммутатор.

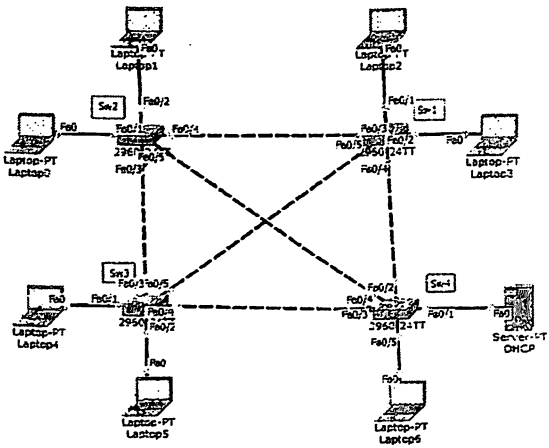


Рис. 4.3. Исследуемая сетевая структура

```
Sw1#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32769
              Address     000D.BD2C.15B9
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     000D.BD2C.15B9
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg FWD 19        128.1    P2p
Fa0/2            Desg FWD 19        128.2    P2p
Fa0/3            Desg FWD 19        128.3    P2p
Fa0/4            Desg FWD 19        128.4    P2p
Fa0/5            Desg FWD 19        128.5    P2p
```

Рис. 4.4. Результаты spanning-tree на Sw1

```
sw2#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32769
              Address     000D.BD2C.15B9
              Cost        19
              Port        4(FastEthernet0/4)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     00E0.A396.2B20
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg FWD 19        128.1    P2p
Fa0/3            Altn BLK 19        128.3    P2p
Fa0/4            Root FWD 19        128.4    P2p
Fa0/5            Altn BLK 19        128.5    P2p
Fa0/2            Desg FWD 19        128.2    P2p
```

Рис. 4.5. Результаты spanning-tree на Sw2

Краткое теоретическое сведения по второй задаче

Канал агрегации (англ. Link aggregation) - это технология, позволяющая объединить несколько физических каналов в один логический канал. Канал агрегации позволяет распределять трафик по логическому каналу по физическому каналу и обеспечивает резервное копирование одного или нескольких физических каналов в случае внутреннего события отказа в одном логическом канале. Эта технология позволяет увеличить пропускную способность и надежность канала. Топология сети показана на рисунке 4.7.

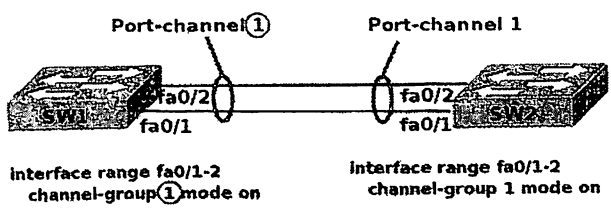


Рис. 4.7. Установление канала агрегации между коммутаторами

Общая информация о каналах агрегации

Каналы агрегации решают две проблемы:

– Увеличить пропускную способность канала

- Один из каналов обеспечивает резервное копирование при выходе из строя.

Агрегированные каналы могут быть созданы между двумя коммутаторами, коммутатором и маршрутизатором, коммутатором и хостом.

Для агрегирования каналов в Cisco можно использовать один из следующих трех вариантов:

- Стандартный протокол LACP (Link Aggregation Control Protocol);
- PAgP (протокол агрегации портов);
- Статическая агрегация, не использующая протокол.

Логический канал EtherChannel распределяет кадры по физическому каналу, представляет двоичный шаблон для адресной информации в кадре с цифровым символом и на первом этапе выбирает один из физических каналов в логическом канале. Распределение каналов EtherChannel основано на алгоритме хеширования Cisco.

Для настройки агрегации каналов на устройстве Cisco используются несколько терминов:

- EtherChannel - технология агрегирования каналов. Этот термин используется в Cisco для агрегирования каналов. EtherChannel используется для соединения коммутаторов, маршрутизаторов, серверов и клиентов друг с другом в локальной сети с помощью неэкранированной витой пары (UTP) или одно- и многоволоконных оптоволоконных кабелей.
- порт-канал - логический интерфейс, т.е. комбинация физических интерфейсов.
- channel-group - эта команда указывает, какой логический интерфейс находится в физическом интерфейсе и какой режим агрегации он использует.

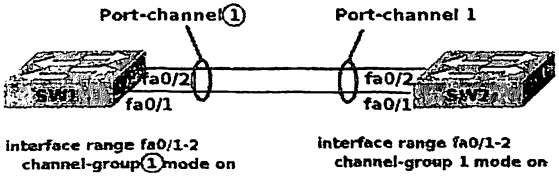


Рис. 4.8. Логический интерфейс порт-канал

В схеме номер, следующий за командой channel-group, представляет номер логического интерфейса Port-channel. Две стороны номера логического интерфейса агрегированного канала должны совпадать. Номер используется для различения разных групп портов на одном коммутаторе.

Команды channel-group

sw(config-if)# channel-group <channel-group-number> mode <<auto [non-silent] | desirable [non-silent] | on> | <active | passive>>

параметры команды:

- active — соединяет LACP;
- passive — Если идёт только сообщение LACP, соединяет LACP;
- desirable — соединяет PAgP;
- auto — Если идёт только сообщение PAgP, соединяет PAgP;
- on — соединяет только Etherchannel.

Настройка конфигурации EtherChannel на основе LACP

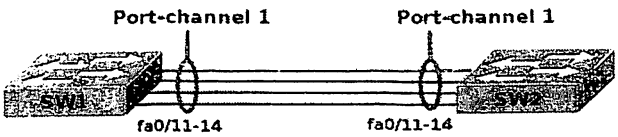


Рис. 4.9. EtherChannel на основе LACP

Перед настройкой агрегирования необходимо отключить физические интерфейсы. Достаточно отключить одну сторону

(например, выключена сторона sw1), после этого на обеих сторонах настраивается агрегация и подключаются интерфейсы.

Последовательность выполнения работы

Настройка EtherChannel на Sw1:

```
sw1(config)# interface range f0/11-14
sw1(config-if-range)# shutdown
sw1(config-if-range)# channel-group 1 mode active
Creating a port-channel interface Port-channel 1
```

Настройка EtherChannel на Sw2:

```
sw2(config)# interface range f0/11-14
sw2(config-if-range)# channel-group 1 mode passive
Creating a port-channel interface Port-channel 1
```

Соединение физических интерфейсов на sw1:

```
sw1(config)# interface range f0/11-14
sw1(config-if-range)# no shutdown
```

Информации о sw2 port-channel:

```
sw1#sh etherchannel port-channel
                Channel-group listing:
                ----------------------

Group: 1
----------

                Port-channels in the group:
                ---------------------------

Port-channel: Po1    (Primary Aggregator)

------------

Age of the Port-channel   = 0d:00h:14m:21s
Logical slot/port   = 1/3           Number of ports = 4
HotStandBy port = null
Port state          = Port-channel Ag-Inuse
Protocol            =   LACP
Port security       = Disabled

Ports in the Port-channel:

Index   Load   Port     EC state        No of bits
------+------+--------+---------------+-----------
  3     00     Fa0/11   Active              0
  0     00     Fa0/12   Active              0
  1     00     Fa0/13   Active              0
  2     00     Fa0/14   Active              0

Time since last port bundled:    0d:00h:01m:49s    Fa0/13
Time since last port Un-bundled: 0d:00h:04m:20s    Fa0/14
```

Настройка конфигурации EtherChannel на основе PAgP

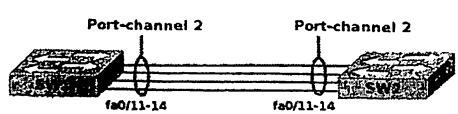


Рис. 4.10. EtherChannel на основе PAgP

Перед настройкой агрегирования необходимо отключить физические интерфейсы. Достаточно отключить одну сторону (например, выключена сторона sw1), после этого на обеих сторонах настраивается агрегация и подключаются интерфейсы.

Настройка EtherChannel на Sw1:

```
sw1(config)# interface range f0/11-14
sw1(config-if-range)# shutdown
sw1(config-if-range)# channel-group 2 mode desirable
Creating a port-channel interface Port-channel 2
```

Настройка EtherChannel на sw2:

```
sw2(config)# interface range f0/11-14
sw2(config-if-range)# channel-group 2 mode auto
Creating a port-channel interface Port-channel 2
```

Соединение физических интерфейсов на sw1:

```
sw1(config)# interface range f0/11-14
sw1(config-if-range)# no shut
```

Просмотр информации

Информация об Etherchannel

```
switch etherchannel summary
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator

        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------

2      Po2(SU)         PAgP      Fa0/11(P)   Fa0/12(P)   Fa0/13(P)
                                 Fa0/14(P)
```

Контрольные вопросы

1. Каковы функции протокола STP?
2. Что вы подразумеваете под корневым коммутатором в сети и как он выбирается?
3. Какие типы портов используются в протоколе STP и как они определены?

4. Каковы функции и типы каналов агрегации?
5. Каковы протоколы канального уровня?
6. Опишите протокол PAgP?
7. Опишите протокол LACP?

ЛАБОРАТОРНАЯ РАБОТА №5
НАСТРОЙКА ПРОТОКОЛА VTP

Цель работы: Освоение практических навыков по осуществлению маршрутизации между виртуальными локальными сетями (VLAN) созданный в локальном сети и принцип работы протокола VTP.

Задание:

- Настройте протокол VTP на построенном сети и объясните принцип работы (Рисунок 5.4);
- Проанализируйте результаты каждую конфигурацию коммутатора.

Краткие теоретические сведения

В коммутируемых объединённых сетях сети VLAN обеспечивают гибкость сегментации и организации. Сети VLAN позволяют сгруппировать устройства внутри локальной сети. Группа устройств в пределах сети VLAN взаимодействует так, будто устройства подключены с помощью одного провода. Сети VLAN основываются не на физических, а на логических подключениях.

Сети VLAN позволяют администратору производить сегментацию по функциям, проектным группам или областям применения, вне зависимости от физического расположения пользователя или устройства. Устройства в пределах сети VLAN работают таким образом, будто находятся в собственной

независимой сети, даже если делят одну общую инфраструктуру с другими VLAN. Любой порт коммутатора может принадлежать сети VLAN. Одноадресные, широковещательные и многоадресные пакеты пересылаются и рассылаются только к конечным станциям в пределах той сети VLAN, которая является источником этих пакетов. Каждая сеть VLAN считается отдельной логической сетью, и пакеты, адресованные станциям, не принадлежащим

Каждая VLAN в коммутируемой сети относится к какой-либо IP-сети; таким образом, в проекте VLAN нужно учитывать реализацию иерархической системы сетевой адресации. Иерархическая адресация подразумевает упорядоченное назначение номеров IP-сети сегментам или сетям VLAN с учетом работы сети в целом

Сети VLAN в основном бывают в двух разных диапазонах:

1. Стандарт – от 1 до 1005;
2. Расширенный – от 1006 до 4094.

Порты коммутатора по умолчанию прикрепляются к VLAN 1 (default vlan, native vlan = 1)

```
Switch# show vlan brief

VLAN Name                Status    Ports
---- ------------------- --------- -------------------------
1    default             active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                   Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                   Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                   Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                   Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                   Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                   Gi0/1, Gi0/2
1002 fddi-default        act/unsup
1003 token-ring-default  act/unsup
1004 fddinet-default     act/unsup
1005 trnet-default       act/unsup
```

Рис. 5.1. Список прикрепленных портов к VLAN 1

VLAN Trunking Protocol (VTP) — проприетарный протокол компании Cisco Systems, предназначенный для создания, удаления и переименования

VLANов на сетевых устройствах. Передавать информацию о том, какой порт находится в каком VLANe, он не может. Прежде всего, преимущества VLAN состоит в том, что он позволяет централизовано синхронизировать изменения в структуре VLAN сетей внутри VTP домена, что избавляет администратора сети от множества рутинной ручной работы по конфигурации каждого отдельного коммутатора. Коммутаторы, включенные в VTP домен, могут работать в трех режимах: клиент, сервер или «прозрачный» режим.

VTP коммутаторе имеется несколько режим настройки:

1. Server

В этом режиме можно создавать новые и вносить изменения в существующие VLAN'ы. Коммутатор будет обновлять свою базу VLAN'ов и сохранять информацию о настройках во Flash памяти в файле vlan.dat. Генерирует и передает сообщения как от других коммутаторов, работающих в режиме сервера, так и от клиентов

2. Client

Коммутатор в этом режиме будет передавать информацию о VLAN'ах полученную от других коммутаторов и синхронизировать свою базу VLAN при получении VTP обновлений. Настройки нельзя будет поменять через командную строку такого устройства.

3. Transparent

В данном режиме коммутатор будет передавать VTP информацию другим участникам, не синхронизируя свою базу и не генерируя собственные обновления. Настройки VLAN можно поменять лишь для локального коммутатора.

В VTP существует три типа сообщений:

1. Advertisement requests

Представляет из себя запрос от клиента к серверу на оповещение Summary Advertisement

2. Summary advertisements

Данное сообщение по умолчанию сервер отправляет каждые 5 минут или сразу же после изменения конфигурации.

3. Subset advertisements

Отправляется сразу же после изменения конфигурации VLAN, а также после запроса на оповещение.

Клиент, который получает новую версию базы данных VLAN от сервера, передает ее всем другим *trunk* портам, и если за ним находятся клиенты VTP и прозрачные каналы VTP, они также получат эти обновления.

Последовательность выполнения работы:

Создайте топологию, приведенную на рисунке 5.2. Выберите сами, какие коммутаторы в топологии: Client, Transparent, Server.

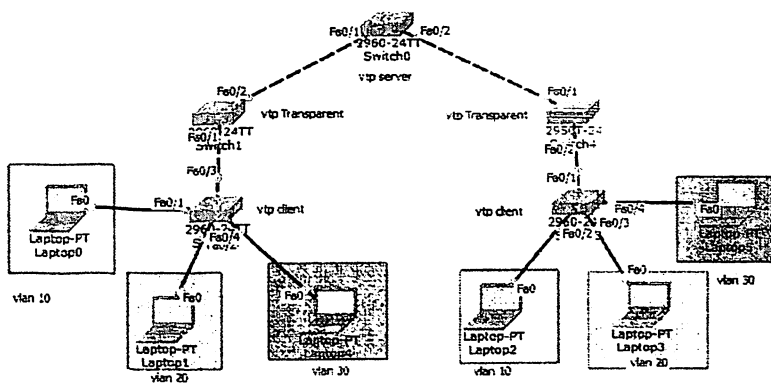


Рис. 5.2. Топология сети по VTP

VTP SERVER

```
Switch(config)#vtp version 2
Switch(config)#vtp mode server
Switch(config)#vtp domain tuit
Switch(config)#vtp password cisco
Switch(config)#vlan 10
Switch(config)#name student
Switch(config-vlan)#exit
Switch(config)#vlan 20
Switch(config)#name kafedra
Switch(config-vlan)#exit
```

```
Switch(config)#vlan 30
Switch(config-vlan)#name test
Switch(config-vlan)#exit
Switch(config)#interface range fastEth 0/1-2
Switch(config-if-range)#switchport mode trunk
```

VTP TRANSPARENT

```
Switch(config)#vtp version 2
Switch(config)#vtp mode transparent
Switch(config)#vtp domain tuit
Switch(config)#vtp password cisco
Switch(config)#vlan 10
Switch(config)#name student
Switch(config-vlan)#exit
Switch(config)#vlan 20
Switch(config)#name kafedra
Switch(config-vlan)#exit
Switch(config)#vlan 30
Switch(config-vlan)#name test
Switch(config-vlan)#exit
Switch(config)#interface fastEthernet 0/2
Switch(config-if-range)#switchport mode trunk
```

VTP client

```
Switch(config)#vtp version 2
Switch(config)#vtp mode client
Switch(config)#vtp domain tuit
Switch(config)#vtp password cisco
Switch(config)#interface fastEthernet 0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#exit
Switch(config)#interface fastEthernet 0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 20
Switch(config-if)#exit
Switch(config)#interface fastEthernet 0/4
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 30
Switch(config-if)#exit
```

```
Switch#show vtp status
VTP Version                     : 2
Configuration Revision          : 4
Maximum VLANs supported locally : 255
Number of existing VLANs        : 8
VTP Operating Mode              : Server
VTP Domain Name                 : cisco
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Enabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x07 0xF6 0xE7 0xAF 0xC2
```

Результаты Transparent switch

```
Switch#show vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 255
Number of existing VLANs        : 8
VTP Operating Mode              : Transparent
VTP Domain Name                 : cisco
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Enabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x38 0xB6 0x43 0xE9 0x2B
0xFC 0x64 0xC8
Configuration last modified by 0.0.0.0 at 3-1-93 00:00:32
```

Результаты Client switch

```
Switch#show vtp status
VTP Version                     : 2
Configuration Revision          : 4
Maximum VLANs supported locally : 255
Number of existing VLANs        : 8
VTP Operating Mode              : Client
VTP Domain Name                 : cisco
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Enabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x07 0xF6 0xE7 0xAF 0xC2
0xAC 0x69 0xAD
Configuration last modified by 0.0.0.0 at 3-1-93 00:55:58
```

Контрольные вопросы:

1. Каков диапазон адресов VLAN?
2. Что означает Client коммутатор в VTP?
3. Что такое Server коммутатор в VTP?
4. Что означает Transparent коммутатор в VTP?
5. Какой тип коммутаторов является основным инициатором?

ЛАБОРАТОРНАЯ РАБОТА №6
НАСТРОЙКА ДИНАМИЧЕСКОЙ МАРШРУТИЗАЦИИ НА ОСНОВЕ ПРОТОКОЛОВ OSPF, RIP, EIGRP И BGP

Цель работы: Освоение практических навыков по обеспечению безопасности в сети, построенный на протоколах маршрутизаций RIP, EIGRP, OSPF и BGP.

Задание:

1. Создайте топологию сети, построенной на основе протоколов динамической маршрутизации RIP, EIGRP, OSPF, BGP;
2. Настройте интерфейсы маршрутизаторов R1, R2 и R3;
3. Настройте аутентификацию информационного потока в каждом протоколе динамической маршрутизации
4. Изучите таблицу маршрутизации на каждом маршрутизаторе.

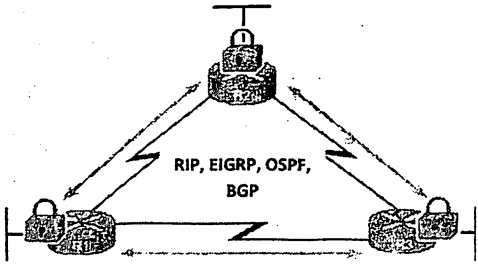


Рис. 6.1. Топология исследуемой сети

Краткие теоретические сведения

В IP-технологии процесс маршрутизации является одним из основных факторов, влияющих на эффективность и производительность сети в целом.

Понятие «маршрутизация» включает в себя несколько значений, одно из них — это передача информации от отправителя к получателю. В IT-среде маршрутизацией называется аппаратное вычисление маршрута движения

пакетов данных между сетями с использованием специального сетевого устройства – маршрутизатора.

Маршруты могут быть статическими и задаваться администратором сети, или динамическими и рассчитываться сетевыми устройствами по определенным алгоритмам (протоколам) маршрутизации, которые основаны на данных о топологии сети.

Протоколы динамической маршрутизации позволяют маршрутизаторам IP-сети автоматически создавать оптимальную таблицу маршрутизации (на основе выбранных критериев) и динамически изменять ее в соответствии с изменениями в топологии сети. Динамическая маршрутизация классифицируется следующим образом (рис. 6.2).

Рис.6.2. Классификация протоколов динамической маршрутизации

RIP. Протокол RIP основан на алгоритме удаленного вектора и широко используется. Использует простейшую метрику - количество промежуточных маршрутизаторов на принимающей стороне. Основным преимуществом протокола является то, что он прост в настройке и не требует высокой квалификации обслуживающего персонала. Протокол является открытым и

поддерживает сетевые устройства практически всех производителей сетевых устройств.

EIGRP. Протокол EIGRP Cisco Systems - это улучшенная версия исходной версии протокола IGRP. Протокол является гибридным и основан на алгоритме Diffusing-Update Algorithm (DUAL). Последняя версия EIGRP имеет функцию безопасности, которая не позволяет злоумышленникам записывать элементы таблицы маршрутизации и аутентифицирует их на основе ключа MD5

OSPF. Протокол динамической маршрутизации, который в настоящее время является относительно универсальным и удобным для настройки в корпоративных сетях, он находит самый короткий маршрут (Open Short-est Path First Protocol (OSPF)). Изначально протокол был разработан для работы в больших сетях со сложной топологией (до 65 536 маршрутизаторов). Он основан на алгоритме статуса канала связи и имеет высокую устойчивость к изменениям состояния сети.

BGP (англ. Border Gateway Protocol, протокол граничного шлюза) — протокол динамической маршрутизации.

Относится к классу протоколов маршрутизации внешнего шлюза (англ. EGP — External Gateway Protocol).

На текущий момент является основным протоколом динамической маршрутизации в сети Интернет.

Протокол BGP предназначен для обмена информацией о достижимости подсетей между автономными системами (АС, англ. AS — autonomous system), то есть группами маршрутизаторов под единым техническим и административным управлением, использующими протокол внутридоменной маршрутизации для определения маршрутов внутри себя и протокол междоменной маршрутизации для определения маршрутов доставки пакетов в другие АС. Передаваемая информация включает в себя список АС, к

которым имеется доступ через данную систему. Выбор наилучших маршрутов осуществляется исходя из правил, принятых в сети.

Последовательность выполнения работы:

по RIPv2 в среде GNS3

Нужно настроить обмен информацией между маршрутизаторами R1 и R2 на основе аутентификации и без аутентификации между другими маршрутизаторами и сравниваем различия между ними.

Конфигурация R1

```
Router(config)#hostname R1
R1(config)#router rip
R1(config-router)#version 2
R1(config-router)#no auto-summary
R1(config-router)#network 192.168.10.0
R1(config-router)#network 10.10.10.0
R1(config-router)#network 11.11.11.0
R1(config-router)#exit
R1(config)#key chain cisco
R1(config-keychain)#key 1
R1(config-keychain-key)#key-string cisco1
R1(config-keychain-key)#exit
R1(config-keychain)#exit
R1(config)#interface serial 0/0
R1(config-if)#ip rip authentication mode md5
R1(config-if)#ip rip authentication key-chain cisco
R1(config-if)#exit
```

Конфигурация R2

```
Router(config)#hostname R2
R2(config)#router rip
R2(config-router)#version 2
R2(config-router)#no auto-summary
R2(config-router)#network 192.168.20.0
R2(config-router)#network 10.10.10.0
R2(config-router)#network 12.12.12.0
R2(config-router)#exit
R2(config)#key chain cisco
```

```
R2(config-keychain)#key 1
R2(config-keychain-key)#key-string cisco1
R2(config-keychain-key)#exit

R2(config-keychain)#exit
R2(config)#interface serial 0/0
R2(config-if)#ip rip authentication mode md5
R2(config-if)#ip rip authentication key-chain cisco
R2(config-if)#exit
```

По протоколу EIGRP

Конфигурация R1

```
Router(config)#hostname R1
R1(config)#router eigrp 1
R1(config-router)#eigrp router-id 1.1.1.1
R1(config-router)#network 192.168.10.0 0.0.0.255
R1(config-router)#network 10.10.10.0 0.0.0.3
R1(config-router)#network 11.11.11.0 0.0.0.3
R1(config-router)#no auto-summary
R1(config-router)#exit
R1(config)#key chain EIGRP_KEY
R1(config-keychain)#key 1
R1(config-keychain-key)#key-string cisco
R1(config-keychain-key)#exit
R1(config-keychain)#exit
R1(config)#interface serial 0/3/0
R1(config-if)#ip authentication mode eigrp 1 md5
R1(config-if)#ip authentication key-chain eigrp 1 EIGRP_KEY
R1(config-if)#exit
```

Конфигурация R2

```
Router(config)#hostname R2
R2(config)#router eigrp 1
R2(config-router)#eigrp router-id 2.2.2.2
R2(config-router)#network 192.168.20.0 0.0.0.255
R2(config-router)#network 10.10.10.0 0.0.0.3
R2(config-router)#network 12.12.12.0 0.0.0.3
R2(config-router)#no auto-summary
R2(config-router)#exit
R2(config)#key chain EIGRP_KEY
R2(config-keychain)#key 1
R2(config-keychain-key)#key-string cisco
R2(config-keychain-key)#exit
R2(config-keychain)#exit
R2(config)#interface serial 0/3/0
```

```
R2(config-if)#ip authentication mode eigrp 1 md5
R2(config-if)#ip authentication key-chain eigrp 1 EIGRP_KEY
R2(config-if)#exit
```

Конфигурация R3

```
Router(config)#hostname R3
R3(config)#router eigrp 1
R3(config-router)#eigrp router-id 3.3.3.3
R3(config-router)#network 192.168.30.0 0.0.0.255
R3(config-router)#network 12.12.12.0 0.0.0.3
R3(config-router)#network 11.11.11.0 0.0.0.3
R3(config-router)#no auto-summary
```

По протоколу OSPF

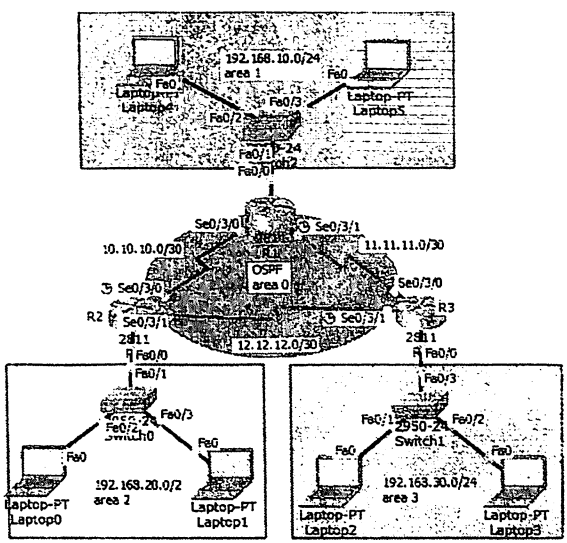


Рис.6.3. Топология сети на основе протокола OSPF.

Конфигурация R1

```
R1(config)#router ospf 10
R1(config-router)#router-id 1.1.1.1
R1(config-router)#network 192.168.10.0 0.0.0.255 area 1
R1(config-router)#network 11.11.11.0 0.0.0.3 area 0
```

```
R1(config-router)#network 10.10.10.0 0.0.0.3 area 0
R1(config-router)#exit
R1(config)#router ospf 10
R1(config-router)#area 0 authentication message-digest
R1(config-router)#exit
R1(config)#interface serial 0/3/0
R1(config-if)#ip ospf message-digest-key 1 md5 cisco123
R1(config-if)#exit
```

Конфигурация R2

```
R2(config)#router ospf 10
R2(config-router)#router-id 2.2.2.2
R2(config-router)#network 10.10.10.0 0.0.0.3 area 0
R2(config-router)#network 12.12.12.0 0.0.0.3 area 0
R2(config-router)#network 192.168.20.0 0.0.0.255 area 2
R2(config-router)#exit
R2(config)#router ospf 10
R2(config-router)#area 0 authentication message-digest
R2(config-router)#exit
R2(config)#interface serial 0/3/0
R2(config-if)#ip ospf message-digest-key 1 md5 cisco123
R2(config-if)#exit
```

Конфигурация R3

```
R3(config)#router ospf 10
R3(config-router)#router-id 3.3.3.3
R3(config-router)#network 192.168.30.0 0.0.0.255 area 3
R3(config-router)#network 12.12.12.0 0.0.0.3 area 0
R3(config-router)#network 11.11.11.0 0.0.0.3 area 0
R3(config-router)#exit
```

По протоколу BGP

Введите IP-адреса компьютеров в соответствии с топологией, показанной на рисунке 6.4.

Конфигурация R1

```
R1(config)#router bgp 65100
R1(config-router)#bgp router-id 1.1.1.1
R1(config-router)#neighbor 172.16.0.2 remote-as 65200
R1(config-router)#neighbor 172.16.13.2 remote-as 65300
R1(config-router)#network 192.168.1.0 mask 255.255.255.0
R1(config-router)#exit
```

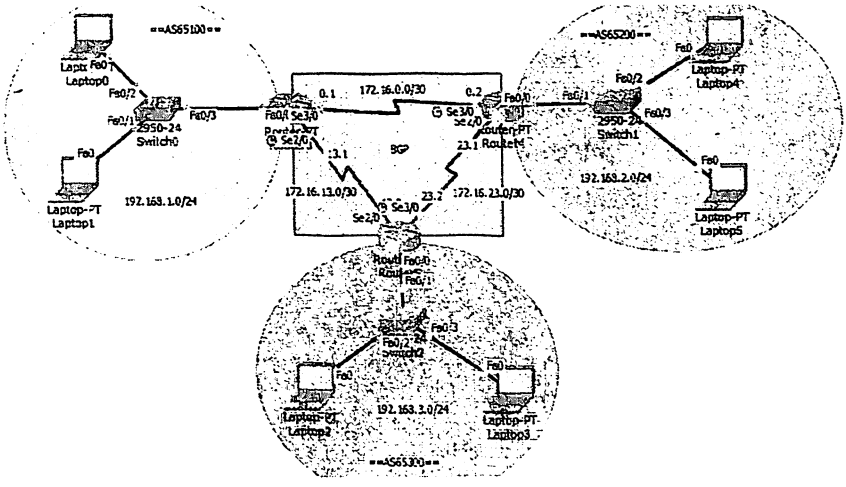


Рис.6.4. Топология сети на основе протокола BGP.

Конфигурация R2

```
R2(config)#router bgp 65200
R2(config-router)#bgp router-id 2.2.2.2
R2(config-router)#neighbor 172.16.0.1 remote-as 65100
R2(config-router)#neighbor 172.16.23.2 remote-as 65300
R2(config-router)#network 192.168.2.0 mask 255.255.255.0
R2(config-router)#exit
```

Конфигурация R2

```
R3(config)#router bgp 65300
R3(config-router)#bgp router-id 3.3.3.3
R3(config-router)#neighbor 172.16.13.1 remote-as 65100
R3(config-router)#neighbor 172.16.23.1 remote-as 65200
R3(config-router)#network 192.168.3.0 mask 255.255.255.0
R3(config-router)#exit
```

Контрольные вопросы

1. По какому алгоритму работает протокол RIP?
2. На каком основании протокол RIP рассчитывает метрики?
3. Каково административное расстояние протокола RIP?

4. В чем разница между протоколами RIPv1 и RIPv2?
5. По какому алгоритму работает протокол OSPF?
6. По какому алгоритму работает протокол EIGRP?
7. В чем преимущества протокола EIGRP?
8. Что вы подразумеваете под административной удаленностью?
9. Какие типы протоколов динамической маршрутизации?
10. В чем разница между динамической маршрутизацией и статической маршрутизацией?
11. Опишите протокол внешней маршрутизации BGP.
12. Каково административное расстояние протокола BGP.
13. По какому алгоритму работает протокол BGP?
14. Что вы подразумеваете под автономной системой?

ЛАБОРАТОРНАЯ РАБОТА №7
НАСТРОЙКИ СПИСКА ACL (STANDART, EXTENDED)

Цель работы: Изучение правил создания, настройки и проверки списков ACL, используемых в сетях передачи данных.

Краткие теоретические сведения:

Для фильтрации сетевого трафика ACL проверяет передачу или блокировку переданного пакета на интерфейсе маршрутизатора. Маршрутизатор проверяет каждый пакет и определяет, что делать с пакетом: передать или отбросить, на основе критериев, установленных в ACL.

Критерии ACL:

- Адрес трафика;
- Адрес получателя трафика;
- Протоколы высокого уровня.

IP ACL - это набор последовательных команд для блокировки и разрешения IP-пакетов. Маршрутизатор проверяет пакет индивидуально в соответствии с условиями ACL. Можно настроить следующие типы IP ACL:

- Стандартный ACL;
- расширенный ACL;
- dynamic ACL (замок и ключ);
- именованные ACL IP-списки;
- рефлексив ПКС;
- прокси - аутентификация;
- Турбо ACL.

Команда ACL по умолчанию выглядит так:

1. Стандартный ACL (только для зарегистрированных клиентов) управляет трафиком, сравнивая адреса IP-пакетов с адресами серверов пересылки.

Лучше всего разместить стандартный список ACL ближе к адресу получателя, так как это предотвратит попадание этого трафика в другие сети в интерфейсе, где используется ACL. Списки записей отмечены символическими именами или числами:

- Standart от 1 до 99;
- Extended от 100 до 999.

Стандартный список ACL

```
Router(config)#access-list < номер списка от 1 до 99> {permit | deny | remark}{address | any | host}[source-wildcard] [log]
```

- permit: разрешение;
- deny: отказ;
- remark: комментарий к списку работ;
- address: разрешить или запретить сеть;
- any: любое разрешение или отказ;

- host: разрешение или отказ хоста;
- source-wildcard: маска сети WildCardnet;
- log: разрешить регистрацию пакетов, которые проходят эту запись ACL.

Прикрепление к интерфейсу

```
Router(config-if)#ip access-group < наименование ACL или номер спискаi> {in | out}
```

- in: входящее направление;
- out: исходящее направление;

```
access-list access-list-number {permit|deny} {host|source source-wildcard|any}.
```

2. Расширенный список ACL

Расширенный ACL (только для зарегистрированных клиентов) управляет трафиком, сравнивая адреса IP-пакета с адресами отправителя и получателя. Можно четко указать производительность расширенного ACL. Расширенный список ACL фильтрует пакеты IPv4 по нескольким критериям:

- тип протокола;
- IPv4-адрес источника;
- IPv4-адрес получателя;
- TCP или UDP-порты источника;
- TCP или UDP порты приемника;
- Дополнительная информация о типе протокола для эффективного контроля.

Расширенный ACL (только для зарегистрированных клиентов) управляет трафиком, сравнивая адреса IP-пакета с адресами отправителя и получателя. Можно указать расширенную производительность ACL. Фильтрацию трафика можно использовать по следующим критериям:

- протокол;
- номер порта;

- значение DSCP;
- значение привилегии;
- состояние бита SYN.

Расширенная команда ACL выглядит так:

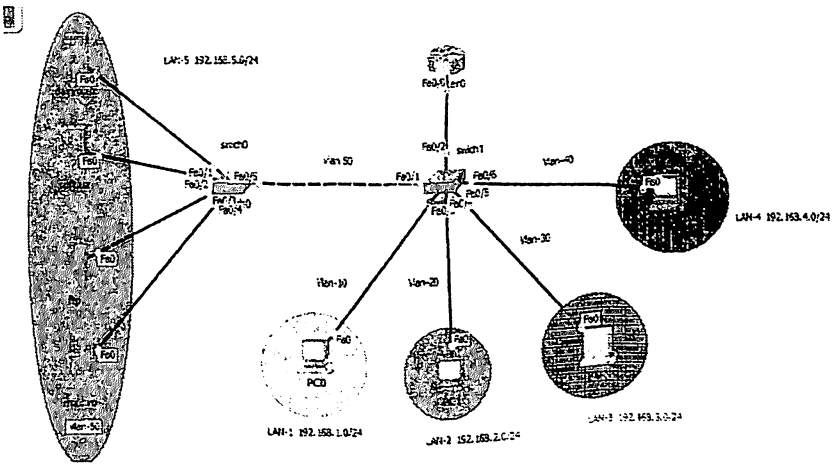


Рис. 7.1. Топология сети на основе расширенного списка ACL

Задача по расширенному списку ACL

Пинг со всех компьютеров на серверы, но:

1. Разрешить доступ к сайту daryo.uz с компьютеров в сети 192.168.1.0, ограничить доступ к другим серверам;

2. Разрешить доступ к сайту soft.uz для компьютеров в сети 192.168.2.0, ограничить доступ к другим серверам;

3. Компьютерам в сети 192.168.3.0 должен быть разрешен доступ к mail.ru, доступ к другим серверам должен быть ограничен;

4. Компьютерам в сети 192.168.3.0 должен быть разрешен доступ к ftp, доступ к другим серверам должен быть ограничен;

Для выполнения вышеуказанных условий мы используем расширенный ACL списка Assess.

Последовательность выполнения работы:

Присоединяем сервера к vlan 50

Конфигурация Switch 1

```
Switch>enable
Switch#conft
Switch(config)#hostname Sw1
Sw1 (config)#vlan 50
Sw1 (config-vlan)#exit
Sw1 (config)#interface range fastEthernet 0/1-4
Sw1 (config-if-range)#switchport mode access
Sw1 (config-if-range)#switchport access vlan 50
Sw1 (config-if-range)#exit
Sw1 (config)#int fa0/5
Sw1 (config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan 50
Switch(config-if)#exit
```

Конфигурация Switch 2

```
Switch>en
Switch#conf t
Switch(config)#hostname Sw2
Sw2 (config)#vlan 10
Sw2 (config-vlan)#vlan 20
Sw2(config-vlan)#vlan 30
Sw2(config-vlan)#vlan 40
Sw2 (config-vlan)#vlan 50
Sw2 (config-vlan)#exit
Sw2(config)# interface fastEthernet 0/1
Sw2(config-if)#switchport mode trunk
Sw2(config-if)#switchport trunk allowed vlan 50
Sw2(config-if)#exit
Sw2(config)# interface fastEthernet 0/3
Sw2(config-if)#switchport mode access
Sw2(config-if)#switchport access vlan 10
Sw2(config-if)#exit
Sw2(config)#interface fastEthernet 0/4
Sw2(config-if)#switchport mode access
Sw2(config-if)#switchport access vlan 20
Sw2(config-if)#exit
Sw2(config)# interface fastEthernet 0/5
Sw2(config-if)#switchport mode access
Sw2(config-if)#switchport access vlan 30
Sw2(config-if)#exit
Sw2(config)# interface fastEthernet 0/6
Sw2(config-if)#switchport mode access
```

```
Sw2(config-if)#switchport access vlan 40
Sw2(config-if)#exit
Sw2(config)# interface fastEthernet  0/2
Sw2(config-if)#switchport mode trunk
Sw2(config-if)#switchport trunk allowed vlan 10,20,30,40,50
Sw2(config-if)#exit
```

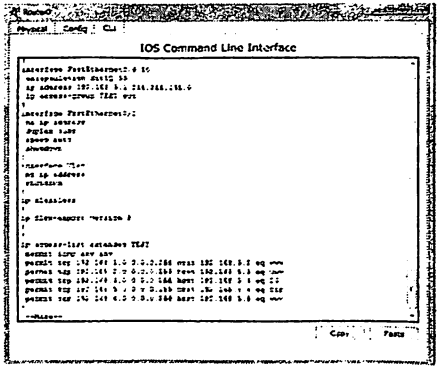
Конфигурация маршрутизатора

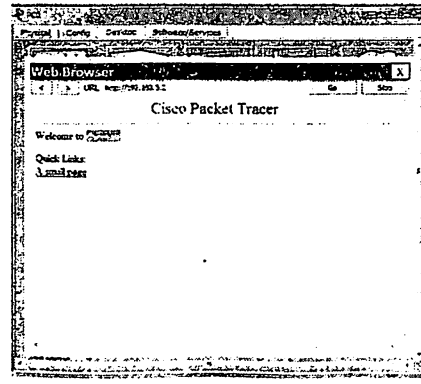
```
Router>en
Router#configure terminal
Router(config)#intfa 0/0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#intfa 0/0.10
Router(config-subif)#encapsulation dot1Q  10
Router(config-subif)#ip address 192.168.1.1 255.255.255.0
Router(config-subif)#exit
Router(config)#intfa 0/0.20
Router(config-subif)#encapsulation dot1Q  20
Router(config-subif)#ip address 192.168.2.1 255.255.255.0
Router(config-subif)#exit
Router(config)#intfa 0/0.30
Router(config-subif)#encapsulation dot1Q  30
Router(config-subif)#ip address 192.168.3.1 255.255.255.0
Router(config-subif)#exit
Router(config)#intfa 0/0.40
Router(config-subif)#encapsulation dot1Q  40
Router(config-subif)#ip address 192.168.4.1 255.255.255.0
Router(config-subif)#exit
Router(config)#intfa 0/0.50
Router(config-subif)#encapsulation dot1Q 50
Router(config-subif)#ip address 192.168.5.1 255.255.255.0
Router(config-subif)#exit
```

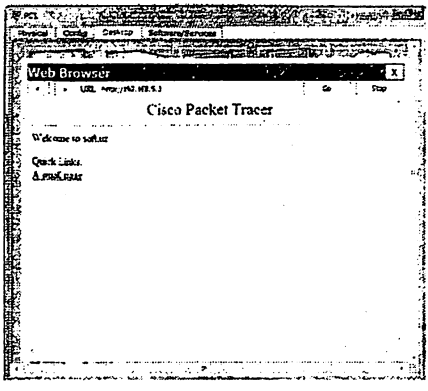
В маршрутизатор записывается следующие команды:

```
Router(config)#
Router(config)#ip access-list extended TEST
Router(config-ext-nacl)#permit icmp any any
Router(config-ext-nacl)#permit tcp 192.168.1.0 0.0.0.255 host 192.168.5.2 eq 80
Router(config-ext-nacl)#permit tcp 192.168.2.0 0.0.0.255 host 192.168.5.3 eq 80
Router(config-ext-nacl)#permit tcp 192.168.3.0 0.0.0.255 host 192.168.5.4 eq 20
Router(config-ext-nacl)#permit tcp 192.168.3.0 0.0.0.255 host 192.168.5.4 eq 21
Router(config-ext-nacl)#permit tcp 192.168.4.0 0.0.0.255 host 192.168.5.5 eq 80
Router(config-ext-nacl)#exit
```

```
Router(config)#intfastEthernet 0/0.50
Router(config-subif)#ip access-group TEST out
Router(config-subif)#exit
```







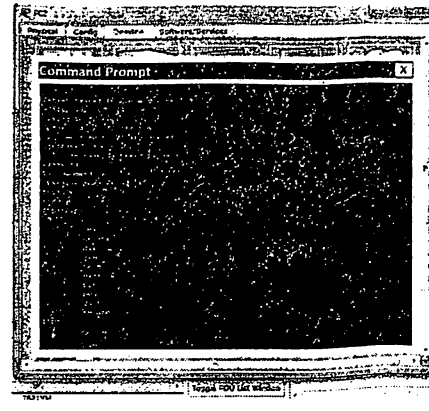


Рис. 7.2. Результаты тестирования топологии

Контрольные вопросы:

1. Что такое ACL?
2. Какие виды ACL существуют ?
3. В каких целях используют ACL?
4. Какая команда введется для того чтобы блокировать видео трафик?

5. Какая команда введется для того чтобы разрешить интернет трафик?
6. По каким критериям фильтруется трафик на списке ACL?

ЛАБОРАТОРНАЯ РАБОТА №8
НАСТРОЙКА ТЕХНОЛОГИИ NAT / PAT НА МАРШРУТИЗАТОРАХ

Цель работы: Изучение принципов и функций трансляции адресов (NAT) и получение практических навыков.

Краткие теоретические сведения

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

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

Принимая пакет от локального компьютера, роутер смотрит на IP-адрес назначения. Если это локальный адрес, то пакет пересылается другому локальному компьютеру. Если нет, то пакет надо переслать наружу в интернет. Но ведь обратным адресом в пакете указан локальный адрес компьютера, который из интернета будет недоступен. Поэтому роутер «на лету» транслирует (подменяет) обратный IP-адрес пакета на свой внешний (видимый из интернета) IP-адрес и меняет номер порта (чтобы различать ответные пакеты, адресованные разным локальным компьютерам). Комбинацию,

нужную для обратной подстановки, роутер сохраняет у себя во временной таблице. Через некоторое время после того, как клиент и сервер закончат обмениваться пакетами, роутер сотрёт у себя в таблице запись об n-м порте за сроком давности.

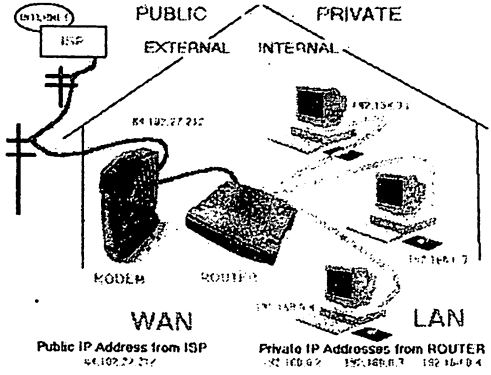


Рис. 8.1. Трансляция адресов

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

Существует 3 базовых концепции трансляции адресов:

- статическая (Static Network Address Translation),
- динамическая (Dynamic Address Translation),
- маскарадная (NAPT, NAT Overload, PAT).

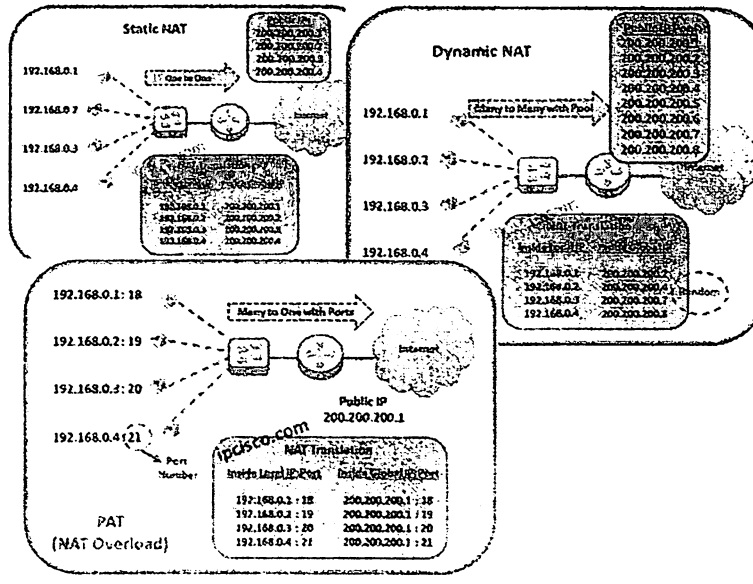


Рис. 8.2. Механизм трансляции адресов

Статический NAT — отображение незарегистрированного IP-адреса на зарегистрированный IP-адрес на основании один к одному. Особенно полезно, когда устройство должно быть доступным снаружи сети.

Динамический NAT — отображает незарегистрированный IP-адрес на зарегистрированный адрес из группы зарегистрированных IP-адресов. Динамический NAT также устанавливает непосредственное отображение между незарегистрированными и зарегистрированными адресами, но отображение может меняться в зависимости от зарегистрированного адреса, доступного в пуле адресов, во время коммуникации.

Перегруженный NAT (NAPT, NAT Overload, PAT, маскарадинг) — форма динамического NAT, который отображает несколько незарегистрированных адресов в единственный зарегистрированный IP-адрес, используя различные порты. Известен также как PAT (Port Address

Translation). При перегрузке каждый компьютер в частной сети транслируется в тот же самый адрес, но с различным номером порта.

Последовательность выполнения работы:

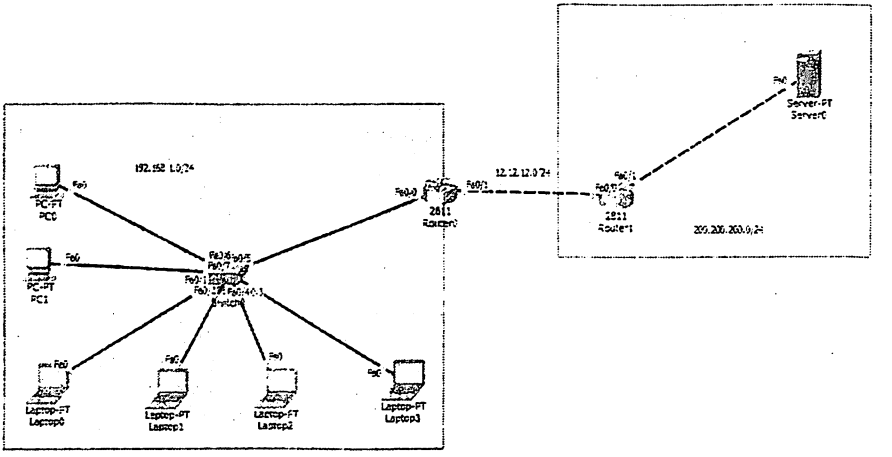


Рис. 8.3. Структура сети, построенный по PAT

```
Router1(config)#ip route 0.0.0.0  0.0.0.0  12.12.12.2
Router1(config)#ip nat pool nad_pat 195.158.1.1  195.158.1.4  netmask 255.255.255.240
Router1(config)#access-list 10 permit 192.168.1.0 0.0.0.255
Router1(config)#ip nat inside source list 10 pool nad_pat overload
Router1(config)#interface fastEthernet 0/0
Router1(config-if)#ip nat inside
Router1(config-if)#exit
Router1(config)#interface fastEthernet 0/1
Router(config-if)#ip nat outside
Router(config-if)#exit
Router(config)#end
Router#copy run startup-config
Конфигурация Router 2
Router(config)#ip route 0.0.0.0 0.0.0.0 12.12.12.1
```

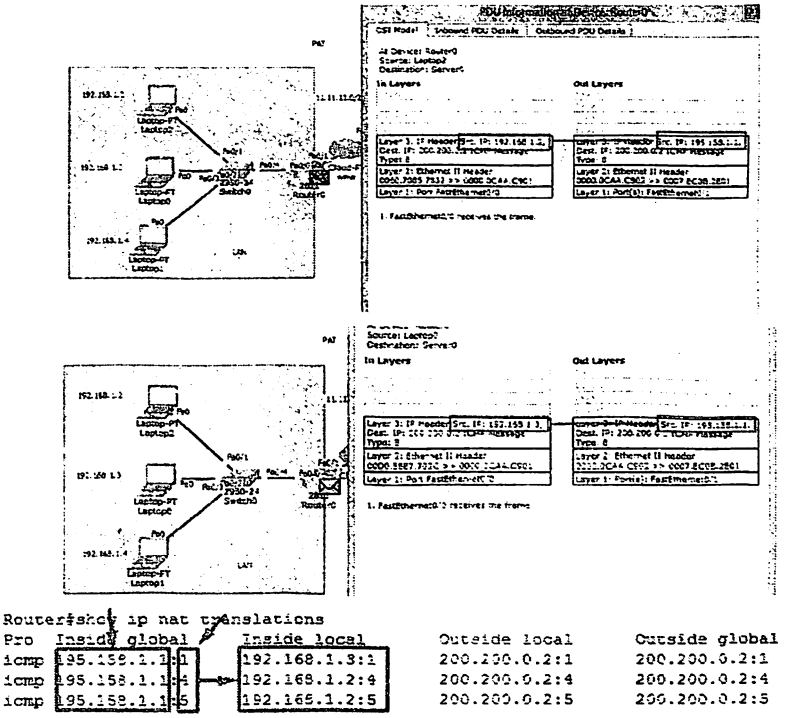


Рис. 8.4. Результаты по трансляции адресов

Все частные адреса в локальной сети будут передаваться через один общедоступный адрес 195.158.1.1, за исключением того, что порт отличается.

Задание:

- Создать структуру сети на Cisco packet tracer.
- Настроить и проверить интерфейсы каждого маршрутизатора R1, R2 в сети
- Настроить и проверить конфигурации сети по PAT
- Подготовить отчёт

Контрольные вопросы:

1. Какие существуют методы трансляции адресов (NAT)?
2. Чем статический NAT отличается от динамического NAT?

3. Объясните принцип работы PAT.
4. Какие типы адресов доступны в сети

ЛАБОРАТОРНАЯ РАБОТА № 9.
КОНФИГУРАЦИЯ ПРОТОКОЛОВ ЗАЩИТЫ СЕТИ SCP, SNMP И ИССЛЕДОВАНИЕ ЛОГ ФАЙЛОВ

Цель работы: Данная лабораторная работа предназначена для: освоения навыков конфигурации протоколов защиты сети SCP и SNMP, log файлов, а также конфигурации Syslog сервера.

Краткие теоретические сведения

Протоколы защиты сети SCP и SNMP

Ранее мы уже описали, что весьма опасно использовать **Telnet**, т.к. все данные передаются в открытом виде и злоумышленник может их с легкостью перехватить. В качестве альтернативы был предложен протокол **SSH**, который шифрует все по умолчанию. Аналогичная ситуация с **HTTP** и **HTTPS**.

Однако, при работе с сетевым оборудованием редко удается обойтись вышеуказанными протоколами. Ниже мы рассмотрим еще несколько популярных протоколов, а точнее их более защищенные версии.

SCP

Перед системными администраторами довольно часто возникает задача по обновлению прошивки оборудования. Для этого необходимо "закинуть" новую прошивку на устройство, что обычно делается с помощью **TFTP** или **FTP**-сервера. Технология стара как мир, да и подобный сервер разворачивается в несколько кликов.

Данные протоколы (TFTP и FTP) также нередко используются для резервного копирования конфигураций устройств. Наверняка большинству знакома команда вроде:

```
Router#copy running-config tftp:
```

Этой командой мы копируем текущую конфигурацию на удаленный TFTP-сервер.

Либо обратная ситуация, когда TFTP или FTP-сервер используется для восстановления конфигурации:

```
Router#copy tftp: running-config
```

И если в случае с прошивками нет ничего криминального, то при работе с конфигурациями совершенно недопустимо использовать незащищенный TFTP или FTP-сервер. По аналогии с Telnet, эти протоколы передают все данные в открытом виде, что позволяет злоумышленнику перехватить весьма ценную информацию - конфигурации ваших устройств. Для решения данной проблемы существует более защищенный протокол, такой как **SCP**.

SCP (secure copy) – протокол копирования файлов, который в качестве транспорта использует SSH (т.е. все передаваемые файлы шифруются). Для работы необходим **SCP-сервер**, которым может являться любой Linux дистрибутив с включенным SSH-сервером. Для Windows имеется специализированное программное обеспечение, например Solarwinds SFTP/SCP Server (доступна бесплатная версия). Сам процесс резервного копирования выглядит следующим образом:

```
Router#copy running-config scp://user:password@192.168.1.100/Cisco-
Conf/Router1.config
```

Данной командой мы копируем текущую конфигурацию на SCP-сервер с ip-адресом **192.168.1.100** в папку **Cisco-Conf**, а сам файл будет называться **Router1.config**. Для подключения к SCP-серверу используется логин и пароль, которые должны быть предварительно созданы на сервере. При этом вся передаваемая информация шифруется.

SNMP

SNMP – Simple Network Management Protocol. Если перевести дословно, то получится "простой протокол сетевого управления". Несмотря на название, данный протокол весьма редко используют именно для управления.

Наиболее частое применение SNMP - мониторинг. Температура процессора, загрузка канала, свободная оперативная память и так далее.

Существует три версии протокола: **SNMPv1, SNMPv2c** и **SNMPv3**. Не вдаваясь в подробности можно резюмировать, что до появления SNMPv3, главной проблемой SNMP была именно безопасность. Первые две версии протокола имеют очень слабый механизм аутентификации, по сути это лишь один пароль (строка сообщества), который передается в открытом виде. Это весьма серьезная уязвимость, которая позволяет злоумышленнику перехватить этот пароль, после чего он может получить всю необходимую информацию с устройства, на котором запущен SNMP. Если же вы используете SNMP для управления, то ситуация с безопасностью требует еще большего внимания.

Исследование log файлов

Если вы когда-нибудь посещали уроки Истории, то наверняка слышали фразу вроде: "Будущее невозможно без знаний о прошлом". Это очень глубокая мысль, которая имеет применение и в сфере информационной безопасности. В нашем случае в качестве учебника по истории будут выступать **Логи (logs)**. Их также называют журналом событий, файлом регистраций и т.д. Название не столь важно, а смысл один - записи о всех событиях в хронологическом порядке. Что конкретно подразумевается под "событиями" мы обсудим чуть позже.

Меня всегда удивляло, с какой халатностью относятся к логам многие системные администраторы. Их (логи) либо не собирают, либо просто не обращают на них внимания. А между тем, логи, это один из самых мощных инструментов как при поиске неисправностей (**troubleshooting**), так и при расследовании различных инцидентов (в том числе ИБ). Сколько было неудачных попыток доступа к маршрутизатору? Когда отключился порт fa0/1 и происходило ли это раньше? Когда произошло падение VPN-туннеля? Сколько прошло времени с перезагрузки устройства и связано ли это с

отключением электричества? Когда были внесены последние изменения в конфигурацию? На эти и многие другие вопросы мы можем ответить только обладая логами.

Логирование (**logging**) позволяет видеть практически все, что происходило в вашей сети. Согласитесь, что невозможно наблюдать за всем оборудованием в режиме реального времени, особенно если инциденты происходят в ночное время, а сеть исчисляется десятками коммутаторов и маршрутизаторов. Кроме того, периодический просмотр логов позволяет избежать проблем, которые могут случиться в будущем.

К сожалению сетевое оборудование Cisco (и других вендоров) имеет весьма ограниченное место для логов (буфер), что в свою очередь сказывается на временном промежутке, который может быть отражен в логах. При исчерпании размера буфера, самые старые логи просто удаляются. Кроме того, при перезагрузке устройства логи будут потеряны безвозвратно. Для решения данных проблем используются **Лог-серверы**, но обо всем по порядку.

Методы сбора логов

Всего существует 6 способов сбора логов с оборудования Cisco и не только. Рассмотрим их:

1) **Console Logging** – Вывод сообщений в консоль. Данный способ работает по умолчанию и выводит логи прямо в консоль устройства.

2) **Buffered Logging** – Сохранение логов в буфер устройства, т.е. RAM память.

3) **Terminal Logging** – Вывод логов в терминал, т.е. для Telnet или SSH сессий.

4) **Syslog сервер** – централизованный сбор логов по протоколу Syslog.

5) **SNMP Traps** – централизованный сбор логов по протоколу SNMP.

6) **AAA** – использование Accounting. Сбор логово касательно подключения к оборудованию и ввода команд. Мы уже рассматривали данный метод.

Каждый из способов обладает своими достоинствами и недостатками, поэтому необходимо использовать их вместе. Ниже мы рассмотрим некоторые аспекты этих методов.

Уровни логирования

Чуть выше мы сформулировали, что Логи это записи о всех событиях в хронологическом порядке. Но что является событием? Все зависит от уровня логирования. Именно он определяет, какую информацию необходимо отображать в логах. Всего существует 8 уровней логирования:

0 - Emergencies. События связанные с неработоспособностью системы.

1 - Alets. Сообщения о необходимости немедленного вмешательства.

2 - Critical. Критические события.

3 - Errors. Сообщения об ошибках.

4 - Warnings. Сообщения содержащие предупреждения.

5 - Notifications. Важные уведомления.

6 - Informational. Информационные сообщения.

7 - Debugging. Отладочные сообщения.

Данные уровни обладают наследственностью, т.е. выбрав уровень 7, вы будете получать сообщения всех уровней (от 0 до 7), а выбрав уровень 3 - только от 0 до 3. С осторожностью повышайте уровень логирования, поскольку чем выше уровень, тем больше нагрузка на CPU. К примеру, если через маршрутизатор идет "большой" трафик и процессор уже находится под высокой нагрузкой, то включив 7 уровень (Debugging) вы можете просто потерять управление над устройством.

В корпоративных сетях чаще всего применяется 6-ой (Informational) уровень логирования. Уровень 7 (Debugging) обычно используется при поиске неисправностей (troubleshooting), например для определения проблем с построением VPN туннеля.

Задание:

Лабораторная работа состоит из двух задач:

Задача №1

- Создайте сеть в соответствии с топологией, показанной на рисунке 9.1;
- На роутерах R1 и R2 включите SNMP. Здесь: ro community = public; rw community = private;
- На персональном компьютере откройте MIB browser и посмотрите название (hostname) роутеров R1 и R2;
- Просмотрите интерфейсы маршрутизатора R1 через браузер MIB;
- Просмотрите типы интерфейсов на маршрутизаторе R1 через браузер MIB;
- Просмотрите таблицу маршрутизации на маршрутизаторе R1 через браузер MIB;
- Переименуйте маршрутизатор R1 через браузер MIB;
- Повторите описанные выше действия для маршрутизатора R2.

Последовательность выполнения задачи №1

Топология сети имеет следующий вид (рисунок 9.1):

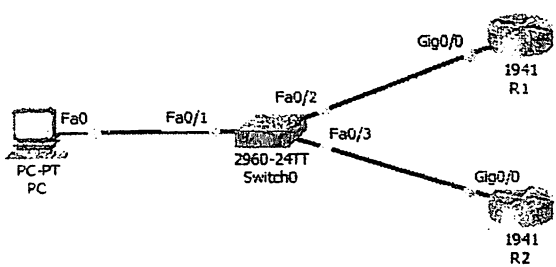


Рис.9.1. Топология для осуществления мониторинга сети на основе протокола SNMP.

Для включения SNMP на роутерах R1 и R2 вводятся следующие команды.

для роутера R1:

```
Router>en
Router#conf t
Router(config)#hostname R1
R1(config)#snmp-server community public ro
R1(config)#snmp-server community private rw
R1(config)#exit
```

для роутера R2:

```
Router>en
Router#conf t
Router(config)#hostname R2
R2(config)#snmp-server community public ro
R2(config)#snmp-server community private rw
R2(config)#exit
```

Процесс доступа к роутеру R1 с помощью персонального компьютера приведено на рисунке 9.2.

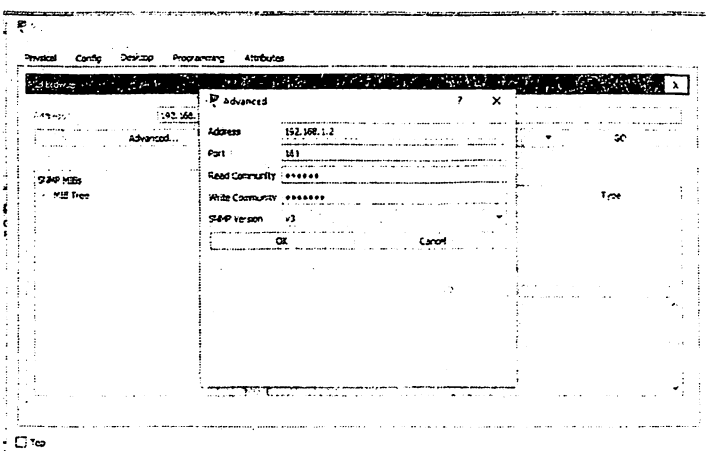


Рис. 9.2. Доступ к роутеру R1 с помощью MIB browser

Задача №2

- Настройте сервер SYSLOG в соответствии с топологией, показанной на рисунке 9.3.
- Установите соответствующие конфигурации, чтобы Router0 и Router1 могли записывать файлы журнала на сервер SYSLOG.

Последовательность выполнения задачи №2

Построим сеть по следующей топологии (рисунок 9.3):

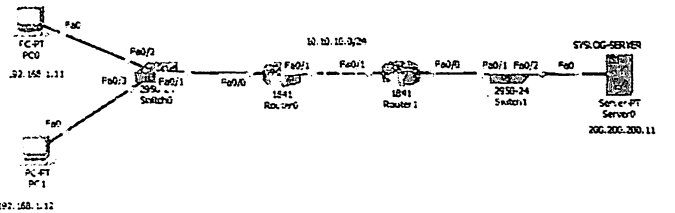


Рис. 9.3. Топология сети с установленным сервером SYSLOG

На Router0 (R1) и Router1 (R2) настраиваем ведение журнала на сервер SYSLOG и указываем уровень ведения журнала:

Для Router0:

```
R1(config)#logging host 200.200.200.11
R1(config)#logging trap debugging
```

Для Router1:

```
R2(config)#logging host 200.200.200.11
R2(config)#logging trap debugging
```

После отключим/включим некоторые интерфейсы маршрутизатора, потом проверим записи журнала на сервере SYSLOG (рисунок 9):

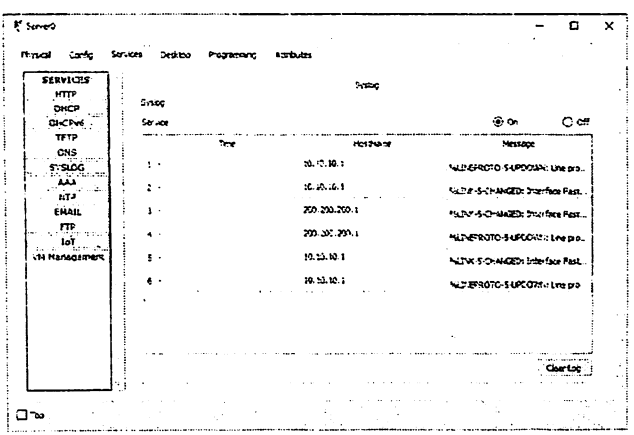


Рис. 9.4. Запись файлов журнала на сервер SYSLOG.

Контрольные вопросы:

1. Объясните назначение SCP протокола.
2. Принципы работы SCP протокола.
3. Назначение SNMP протокола.
4. Принципы работы SNMP протокола.
5. Для чего используются Логи (logs)?
6. Уровни логирования.

ЛАБОРАТОРНАЯ РАБОТА №10
НАСТРОЙКА РЕЖИМА АУТЕНТИФИКАЦИИ НА СЕРВЕРЕ . AAA (RADIUS, TACACS+)

Цель работы: Освоение теоретических знаний и практических навыков по протоколам аутентификации, авторизации и учета в сетях передачи данных.

Краткие теоретические сведения

Механизм AAA (Authentication, Authorization, Accounting) используется для описания процесса предоставления доступа и контроля над ним.

Аутентификация – сопоставление персоны (запроса) существующей учётной записи в системе безопасности. Осуществляется по логину, паролю, сертификату, смарт-карте и т.д.

Авторизация (проверка полномочий, уровня доступа) – сопоставление учётной записи в системе (и персоны, прошедшей аутентификацию) и определённых полномочий (или запрета на доступ).

Учёт – сбор данных об использовании пользователем ресурсов системы.

Одним из протоколов, реализующих AAA является, RADIUS (Remote Authentication Dial-In User Service).

Протокол RADIUS используется для осуществления проверки подлинности, авторизации и учета. RADIUS-клиент (обычно сервер удаленного доступа, VPN-сервер, точка доступа к беспроводной сети и т.п.) посылает учетные данные пользователя и параметры подключения в форме сообщения RADIUS на RADIUS-сервер. Сервер проверяет подлинность и авторизует запрос клиента, а затем посылает обратно ответное сообщение. Клиенты посылают на серверы также сообщения учета. Кроме того стандарт RADIUS поддерживает использование прокси-серверов. Прокси-сервер RADIUS – это компьютер, пересылающий RADIUS-сообщения между узлами, поддерживающими протокол RADIUS.

Для передачи сообщений RADIUS используется протокол UDP. Для сообщений проверки подлинности RADIUS используется UDP-порт 1812, а для сообщений учета – UDP-порт 1813. Некоторые серверы доступа к сети могут использовать UDP-порт 1645 для сообщений проверки подлинности RADIUS и UDP-порт 1646 для сообщений учета RADIUS.

Задание:

В данной работе необходимо:

– построить модель сети в соответствии со схемой, приведенной на рис 10.1;

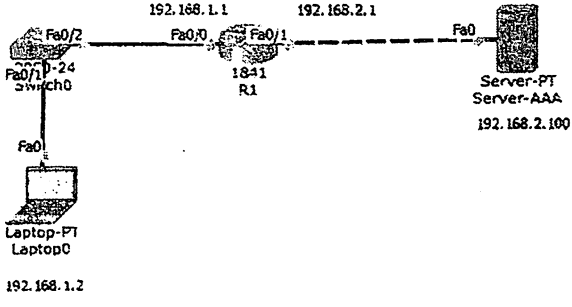


Рис. 10.1. Исследуемая сетевая структура

– Настройте сервер AAA так, чтобы его можно было подключить к компьютеру и маршрутизатору.;

– настроить AAA-клиент на маршрутизаторах

а) Настроить конфигурацию сервера по RADIUS;

б) Настроить конфигурацию сервера по TACACS+

– попытаться получить доступ к маршрутизатору посредством Telnet, используя неправильный пароль или имя пользования;

– попытаться получить доступ к маршрутизатору посредством Telnet, используя правильные имя пользователя и пароль.

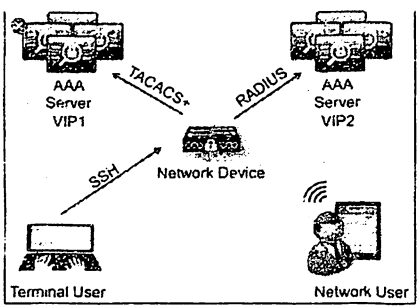


Рис 10.2. Механизм работы протоколов TACACS и RADIUS

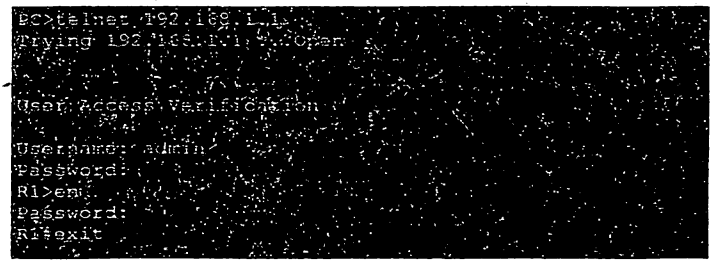
Методика выполнения

Конфигурация R1

```
Router>enable
Router#configure terminal
Router(config)# hostname R1
R1 (config)# enable secret 123456
R1(config)#username admin password admin
R1 (config)# aaa new-model
R1 (config)# radius-server host 192.168.2.100 key tuit
```

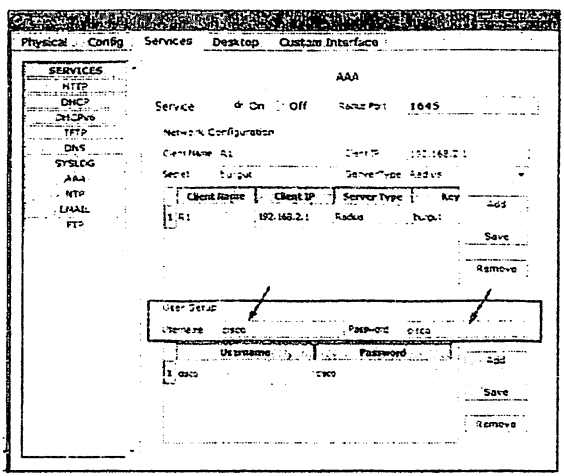
Для удаленного доступа к роутеру используется имя пользователя admin, пароль admin.

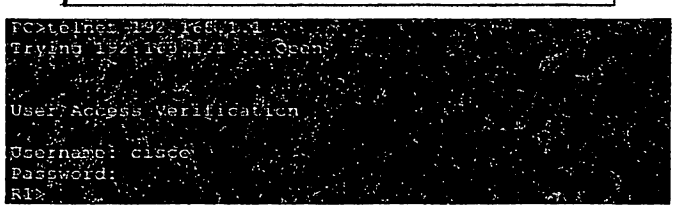
R1 (config)# aaa authentication login default local group radius



Если используется ***group radius***, то имя пользователя, показанное на рисунке, - **cisco**, а пароль вводится через **cisco.**

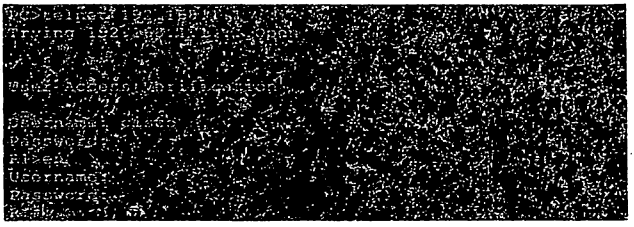
R1 (config)# aaa authentication login default group radius group radius





Паролем разрешения ***enable*** также можно управлять с помощью механизма AAA.

R1 (config)# aaa authentication enable default group radius enable



R1 (config)# aaa authentication enable default enable

Контрольные вопросы:

1. Что такое аутентификация?
2. Что такое авторизация?
3. Что такое идентификация?
4. Как расшифруется RADIUS?
5. Что такое учёт?
6. Какой протокол используется для передачи сообщений RADIUS ?
7. Какая функция у протокола UDP?

ЛАБОРАТОРНАЯ РАБОТА №11
ТЕХНОЛОГИЯ БЕЗОПАСНОСТИ – DHCP SNOOPING

Цель работы: Освоение теоретических знаний и практических навыков по настройке технологий безопасности DHCP Snooping.

Краткие теоретические сведения

DHCP Snooping - это технология безопасности уровня 2, встроенная в операционную систему работоспособного сетевого коммутатора, которая

отбрасывает трафик DHCP, определенный как неприемлемый. DHCP Snooping предотвращает несанкционированные (мошеннические) DHCP-серверы, предлагающие IP-адреса DHCP-клиентам. Функция DHCP Snooping выполняет следующие действия:

Проверяет сообщения DHCP из ненадежных источников и отфильтровывает недействительные сообщения.

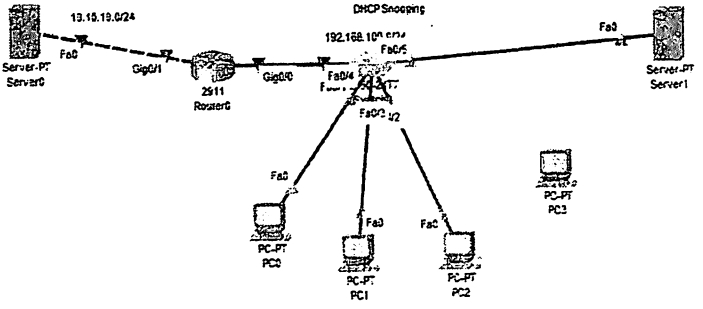
Создает и поддерживает базу данных привязки DHCP Snooping, которая содержит информацию о ненадежных хостах с арендованными IP-адресами.

Использует базу данных привязки DHCP Snooping для проверки последующих запросов от ненадежных хостов.

DHCP Snooping применим только к проводным пользователям. Как функция безопасности уровня доступа, она в основном включена на любом коммутаторе, содержащем порты доступа VLAN, обслуживаемой DHCP. При развертывании DHCP Snooping необходимо настроить доверенные порты (порты, через которые будут проходить допустимые сообщения DHCP-сервера), прежде чем включать DHCP Snooping в VLAN, которую вы хотите защитить. Это может быть реализовано как в интерфейсе CLI, так и в веб-интерфейсе. Команды CLI представлены в конфигурации DHCP Snooping на FS S3900 серии коммутаторах.

Последовательность выполнения работы:

1. Запуск симулятора Cisco packet tracer
2. Для выполнения лабораторной работы используем коммутатор cisco 2960 и маршрутизатор cisco 2911
3. Построить нижеприведенную топологию сети
4. Тестировать, выполненную топологию сети



1. Настройка SWITCHa:

```
Switch>
Switch>en
Switch#conf t
Switch(config)#ip dhcp snooping
Switch(config)#ip dhcp snooping vlan 1
Switch(config)#interface fastEthernet 0/5
Switch(config-if)#ip dhcp snooping trust
Switch(config-if)#ip dhcp snooping limit rate 2048
Switch(config-if) do wr
Switch(config)#end
```

2. Настройка ROUTERa:

```
continue with configuration dialog? [yes/no]: no
Router>enable
Router#conf t
Router(config)#interface gigabitEthernet 0/0
Router(config-if)#no shutdown
Router(config-if)#ip address 192.168.100.1 255.255.255.0
Router(config-if)#ip helper-address 10.10.10.10
Router(config-if)#ex
Router(config)#interface gigabitEthernet 0/1
Router(config-if)#no shutdown
Router(config-if)#ip address 10.10.10.1 255.255.255.0
Router(config-subif)#do wr
Router(config-subif)#exit
```

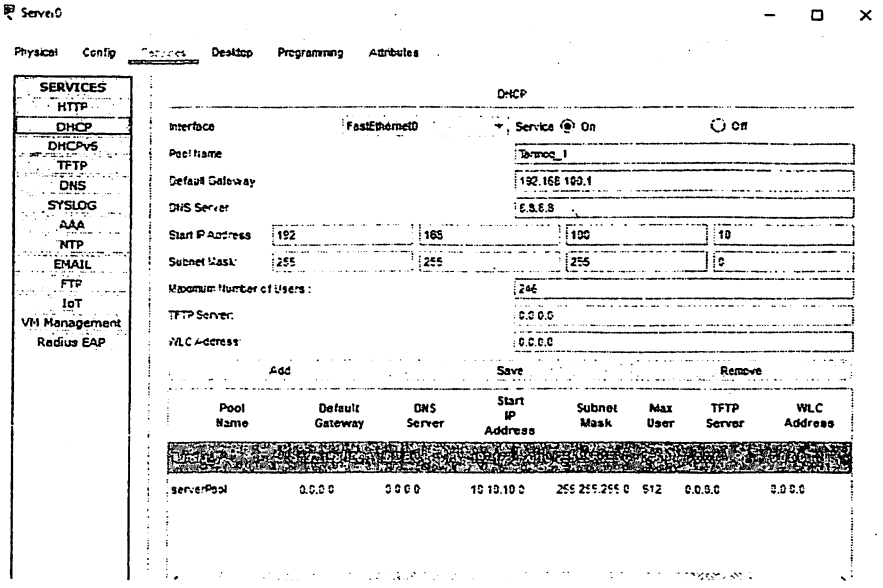


Рис. 11.1. Включить DHCP сервер

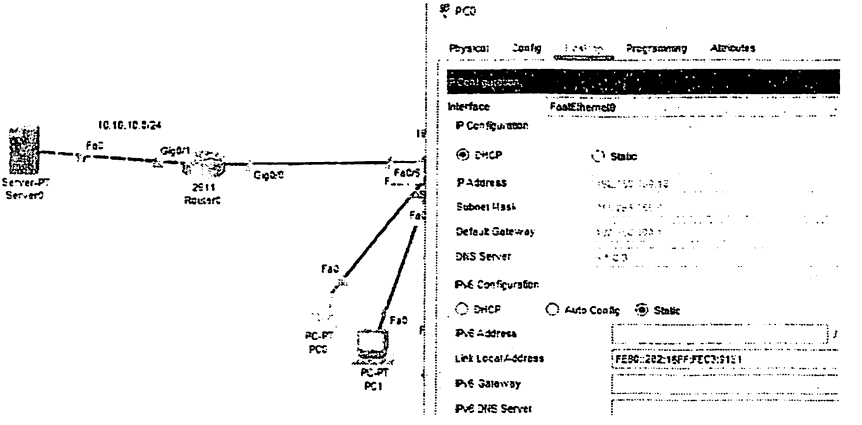


Рис. 11.2. Установить IP адреса на host

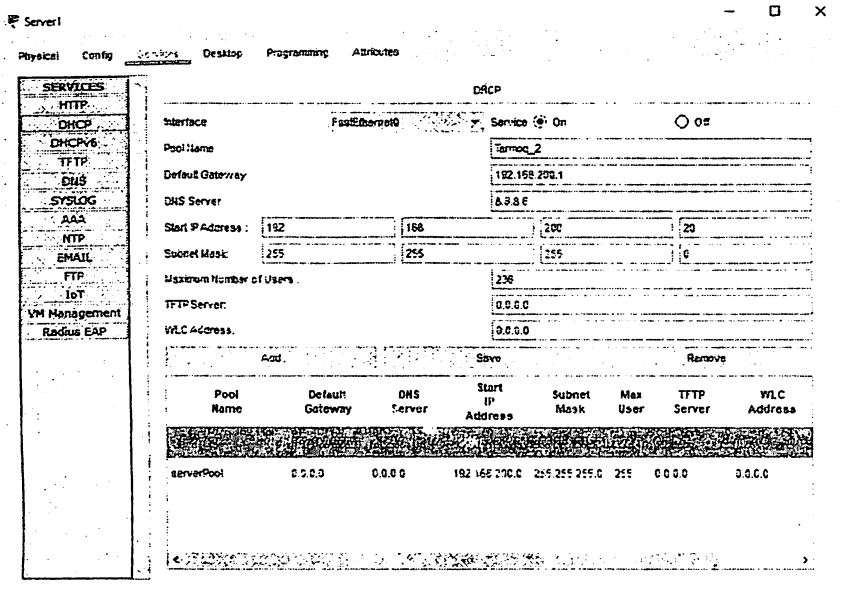


Рис. 11.3. Включить DHCP сервер на поддельном сервере.

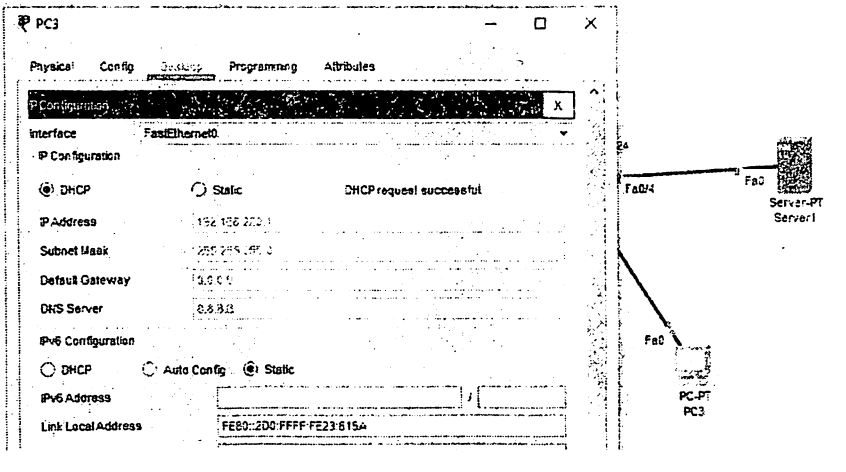


Рис. 11.4. Установить IP адреса на host с поддельного сервера.

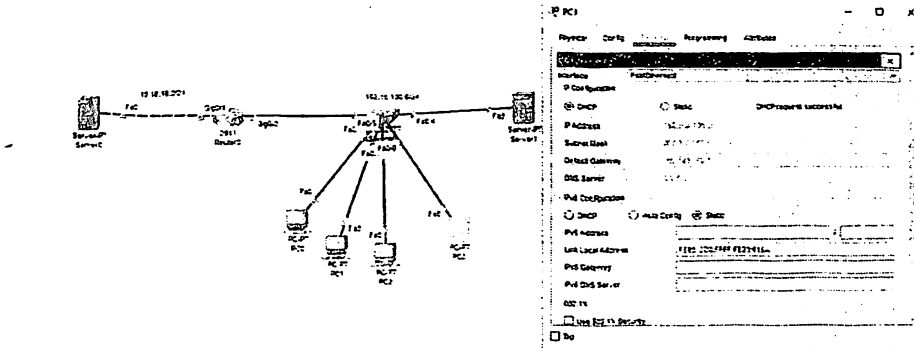


Рис. 11.5. После технологии DHCP Snooping установить IP адрес hosta с настоящего сервера.

Контрольные вопросы:

1. Что такое DHCP Snooping?
2. Какие уязвимости есть в технологии DHCP Snooping?
3. Объяснить сетевую атаку DHCP Snooping и методы предотвращения?

ЛАБОРАТОРНАЯ РАБОТА №12
АНАЛИЗ СЕТЕВЫХ АТАК: ARP-POISONING.

Цель работы: Совершенствование знаний о типах сетевых атак, таких как ARP-poisoning, и способах защиты от них.

Краткие теоретические сведения

ARP-spoofing (ARP-poisoning) — техника сетевой атаки, применяемая преимущественно в Ethernet, но возможная и в других, использующих протокол ARP сетях, основанная на использовании недостатков протокола ARP и позволяющая перехватывать трафик между узлами, которые

расположены в пределах одного широковещательного домена. Относится к числу spoofing-атак.

Протокол ARP предназначен для преобразования IP-адресов в MAC-адреса. Чаще всего речь идёт преобразовании в адреса Ethernet, но ARP используется и в сетях других технологий: Token Ring, FDDI и других.

Алгоритм работы ARP. Протокол может использоваться в следующих случаях (рис.12.1):

1. *Хост A* хочет передать IP-пакет *узлу B*, находящемуся с ним в одной сети;
2. *Хост A* хочет передать IP-пакет *узлу B*, находящемуся с ним в разных сетях, и пользуется для этого услугами *маршрутизатора R*.

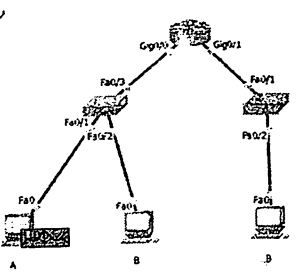


Рис.12.1. Использование протокола ARP

В любом из этих случае *узлом A* будет использоваться протокол ARP, только в первом случае для определения MAC-адреса *узла B*, а во втором — для определения MAC-адреса *маршрутизатора R*. В последнем случае пакет будет передан маршрутизатору для дальнейшей ретрансляции.

Далее для простоты рассматривается первый случай, когда информацией обмениваются узлы, находящиеся непосредственном в одной сети. (Случай когда пакет адресован узлу находящемуся за маршрутизатором отличается только тем, что в пакетах передаваемых после того как ARP-преобразование завершено, используется IP-адрес получателя, но MAC-адрес маршрутизатора, а не получателя(рис.12.2))

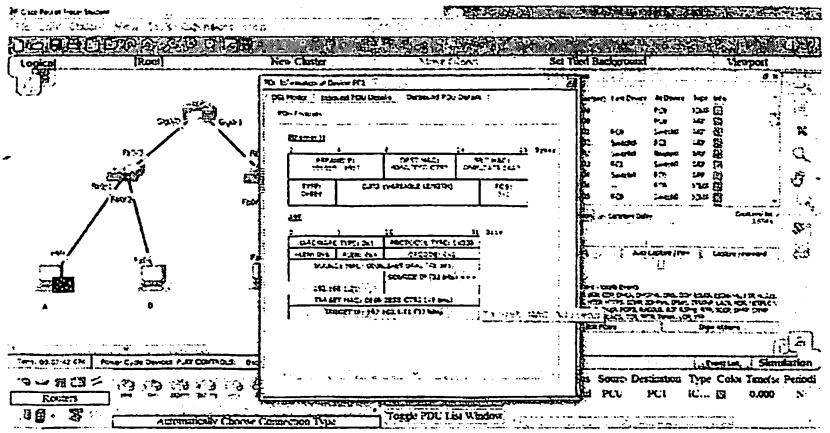


Рис.12.2. Преобразование MAC-адреса пакета

Проблемы ARP. Протокол ARP является абсолютно незащищённым. Он не обладает никакими способами проверки подлинности пакетов: как запросов, так и ответов. Ситуация становится ещё более сложной, когда может использоваться самопроизвольный ARP (gratuitous ARP).

Самопроизвольный ARP — такое поведение ARP, когда ARP-ответ присылается, когда в этом (с точки зрения получателя) нет особой необходимости. *Самопроизвольный ARP-ответ это пакет-ответ ARP, присланный без запроса.* Он применяется для определения конфликтов IP-адресов в сети: как только станция получает адрес по DHCP или адрес присваивается вручную, рассылается ARP-ответ gratuitous ARP.

Последовательность выполнения работы:

Включение защиты от спуфинга ARP.

```
Device> enable
Device# configure terminal
Device(config)# arp anti-spoofing
Device(config)# arp anti-spoofing unknown discard
```

Настройка защиты хоста

Настройка защиты хоста на порту позволяет порту отбрасывать неизвестные пакеты ARP. Настройте привязку IP-порта при настройке устройства на отбрасывание неизвестных пакетов ARP. Это позволяет пакету ARP этого IP-адреса лавировать на другие порты только через этот настроенный порт. Если ARP-пакет этого IP-адреса входит через другой порт, он будет отброшен.

```
Device> enable
Device# configure terminal
Device# host bind ip 192.168.5.13 ethernet 1/2
```

Настройка проверки согласованности MAC-адреса источника.

Чтобы настроить проверку согласованности MAC-адреса источника, выполните эту процедуру.

```
Device> enable
Device# configure terminal
Device# arp anti-spoofing valid-check
```

Настройка антиспуфинга шлюза.

Чтобы настроить антиспуфинг шлюза, выполните эту процедуру.

```
Device> enable
Device# configure terminal
Device# arp anti-spoofing deny-disguiser
```

Настройка порта доверия.

Чтобы настроить порт доверия, выполните эту процедуру.

```
Device> enable
Device# configure terminal
Device# interface fastEthernet (указать номер порта интерфейса)
Device# arp anti trust
```

Для отключения настройки порта доверия набираем команду:

```
Device# no arp anti trust
```

Настройка Anti-Flood Attack.

- Чтобы настроить атаку анти-флуда, выполните эту процедуру.

```
Device> enable
Device# configure terminal
Device(config)# arp anti-flood
Device(config)# arp anti-flood threshold (пороговое значение защиты от флуда ARP.
По умолчанию - 16 пакетов в секунду)
Device(config)# arp anti-flood action deny-arp {deny-all|deny-arp} ( Задает тип
отбрасываемых пакетов. deny-all : добавляет хост в черный список адресов и отбрасывает
все пакеты. deny-arp : отбрасывает только пакеты ARP)

Device(config)# arp anti-flood recover-time 100
Device(config)# arp anti-flood recover 00:00:00:00:32:33
Device# interface fastEthernet (указать номер порта интерфейса)
Device(config)# arp anti-flood threshold
```

Мониторинг ARP Snooping и Flood Attack.

Команды в следующей таблице можно использовать для отслеживания *ARP Snooping и Flood Attack.*

Таблица 12.1. Команды ARP Snooping и Flood Attack

Командование	Цель
show arp anti-snooping	Отображает конфигурацию ARP anti-snooping.
show arp anti-flood	Отображает конфигурацию ARP anti-flood и список злоумышленников
show arp anti interface	Отображает состояние интерфейса

Задание:

1. Создать сеть с тремя хостами и настроить базовые настройки.
2. Изучить как работает протокол ARP.
3. Изучить процесс ARP Snooping.
4. Настроить защиту от ARP Snooping.
5. Создать отчёт со скриншотами.

Вопросы:

1. Опишите функцию протокола ARP.
2. Как работает протокол ARP?
3. Какие атаки могут быть на протокол ARP?
4. Как можно защитится от ARP Snooping? Перечислите несколько способов.
5. Какой способ защиты эффективен?

ЛАБОРАТОРНАЯ РАБОТА №13
НАСТРОЙКА ТЕХНОЛОГИИ БЕЗОПАСНОСТИ

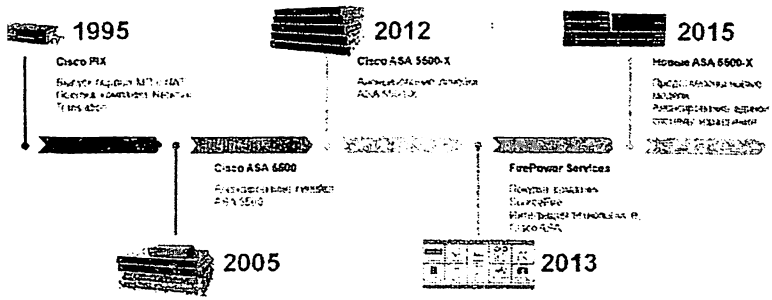
Цель работы: Освоение теоретических знаний и практических навыков по настройке технологий безопасности ASA

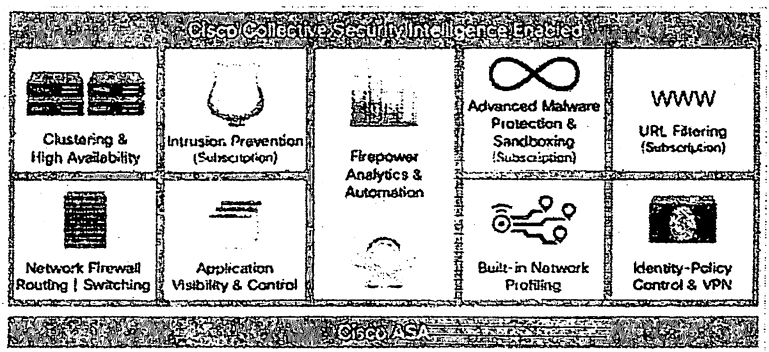
Краткие теоретические сведения

Cisco Systems — лидер мирового рынка межсетевых экранов по результатам исследований, например, по отчету за 2018 год от Frost&Sulivan. Самым известным продуктом компании в области безопасности является Cisco ASA.

Межсетевой экран Cisco ASA — преемник серии PIX, которые были первым файрволами Cisco и обеспечили превосходство компании в этом сегменте сетевых устройств. На инфографике представлена хронология основных событий.

Главным событием стало приобретение компании SourceFire — разработчика системы предотвращения вторжений (СПВ) Snort и антивируса AMP. Технологии компании были интегрированы в продукты линейки 5500-X и известны как сервисы FirePower. С тех пор устройства совершенствуются в механизмах защиты и удобстве управления.





Функциональные особенности

Cisco ASA представляет собой многофункциональное устройство обеспечения безопасности, совмещающее следующие технологии:

- Межсетевой экран нового поколения (NGFW);
- Система гранулярного мониторинга и контроля приложений (Cisco AVC);
- Система построения VPN-туннелей (site-to-site IPsec);
- Система предотвращения вторжений нового поколения (NGIPS);
- Система Advanced Malware Protection (AMP) с функциями ретроспективной защиты
- Фильтрация URL-адресов на основе репутации и алгоритмов классификации;
- Система управления уязвимостями и SIEM.

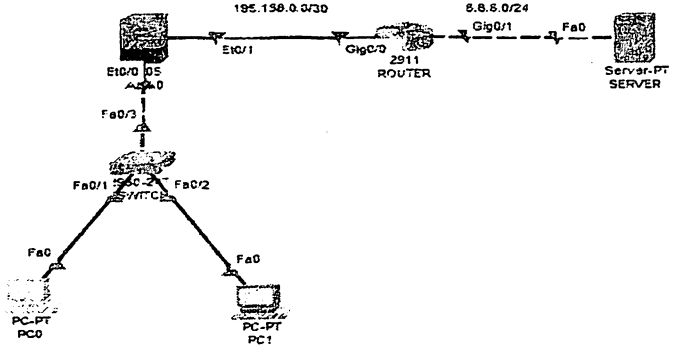
Последовательность выполнения работы:

1. Запуск симулятора Cisco packet tracer

2. Для выполнения лабораторной работы используем коммутатор cisco 2960, маршрутизатор cisco 2911, ASA0 5505 firewall, сервера и компьютеры

3. Построить нижеприведенную топологию сети

4. Тестировать, выполненную топологию сети



Команда для вышеприведенный топологии сети:

3. Команды для ASA0.

```
ciscoasa>en
ciscoasa#conf t
ciscoasa(config)#interface vlan 1
ciscoasa(config-if)#no ip address
ciscoasa(config-if)#ip address 192.168.100.1 255.255.255.0
ciscoasa(config-if)#exit
ciscoasa(config)#dhcpd address 192.168.100.22-192.168.100.50 inside
ciscoasa(config)#dhcpd dns 8.8.8.8
ciscoasa(config)#enable password salom
ciscoasa(config)#username elshod password admin
ciscoasa(config)#ssh 192.168.100.22 255.255.255.255 inside
ciscoasa(config)#ssh timeout 1
ciscoasa(config)#aaa authentication ssh console LOCAL
ciscoasa(config)#interface vlan 2
ciscoasa(config-if)# no ip address
ciscoasa(config-if)#ip address 195.158.0.2 255.255.255.252
```

```
ciscoasa(config-if)#exit
ciscoasa(config)#route outside 0.0.0.0 0.0.0.0 195.158.0.1
ciscoasa(config)#object network NET
ciscoasa(config-network-object)#subnet 192.168.100.0 255.255.255.0
ciscoasa(config-network-object)#nat (inside,outside) dynamic interface
ciscoasa(config-network-object)#ex
ciscoasa#conf t
ciscoasa(config)#access-list NAT extended permit icmp any any
ciscoasa(config)#access-group NAT in interface outside
```

4. Команды для ROUTERa.

```
continue with configuration dialog? [yes/no]: no
Router>enable
Router#conf t
Router(config)#interface gigabitEthernet 0/0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#hostname IP
IP(config)#interface gigabitEthernet 0/0
IP(config-if)#ip address 195.158.0.1 255.255.255.252
IP(config-if)#ex
IP(config)#interface gigabitEthernet 0/1
IP(config-if)#no shutdown
IP(config-if)#ip address 8.8.8.1 255.255.255.0
Router(config-if)#do wr
Router(config-if)#exit
```

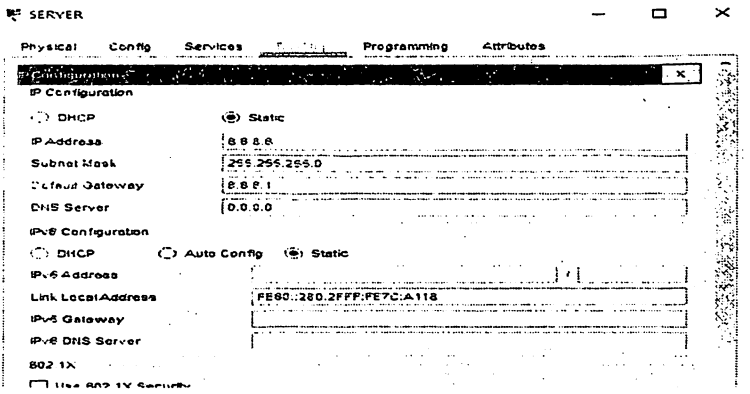


Рис. 13.1. Установить IP адрес серверу.

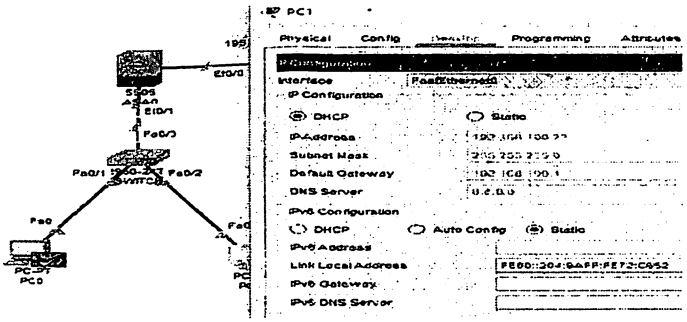


Рис. 13.2. Автоматическая установка IP адреса с ASA firewall компьютеру.

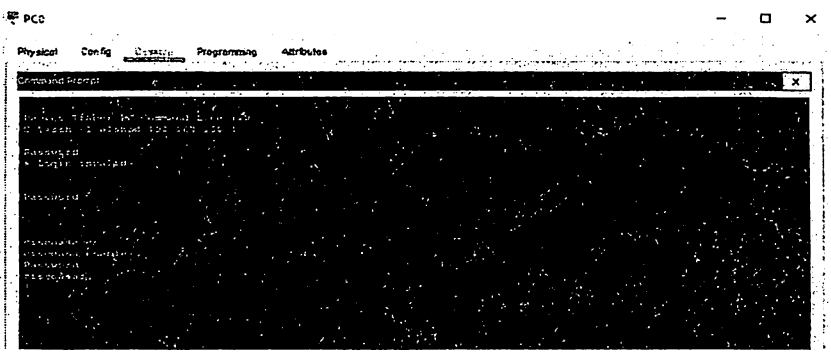


Рис. 13.3. Используя протокол SSH удаленное подключение firewally

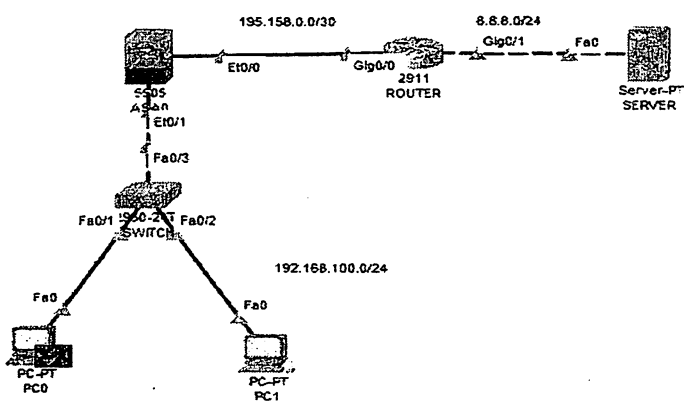


Рис. 13.4. Тестирование построенной топологии.

Задание:

Каждому студенты нужно выполнять лабораторные работы в среде Cisco Packet Tracer на основе приведенной выше информации и подготовить отчёт.

Контрольные вопросы:

1. Что такое технологии безопасности ASA?
2. Какие функциональные особенности есть в ASA?
3. Что такое NGFW?
4. Что такое Cisco AVC?
5. Что такое NGIPS?

ЛАБОРАТОРНАЯ РАБОТА №14
ИССЛЕДОВАНИЕ ПРОТОКОЛА PPTP, L2F, L2TP И IPSEC

Цель работы: Освоение теоретических знаний и практических навыков по исследованию протокола PPTP, L2F, L2TP И IPSec.

Краткие теоретические сведения

VPN (англ. Virtual Private Network - виртуальнаячастнаясеть) - логическая сеть, создаваемая поверх другой сети, например Internet. Несмотря на то, что коммуникации осуществляются по публичным сетям с использованием небезопасных протоколов, за счёт шифрования создаются закрытые от посторонних каналы. VPN позволяет объединить, например, несколько офисов организации в единую сеть с использованием для связи между ними не под контрольных каналов.

Сети VPN строятся с использованием протоколов туннелирования данных через сеть связи общего пользования Интернет, причем протоколы туннелирования обеспечивают шифрование данных и осуществляют их

сквозную передачу между пользователями. Как правило, на сегодняшний день для построения сетей VPN используются протоколы следующих уровней:

- Канальный уровень
- Сетевой уровень
- Транспортный уровень.

Протоколы для построения VPN-туннеля:

- PPTP
- L2TP /L2F
- IPSec

Point-to-Point Tunneling Protocol (PPTP) — один из старейших VPN протоколов, используемых до сих пор, изначально был разработан компанией Microsoft.

PPTP использует два соединения — одно для управления, другое для инкапсуляции данных. Первое работает с использованием TCP, в котором порт сервера 1723. Второе работает с помощью протокола GRE, который является транспортным протоколом (то есть заменой TCP/UDP). Этот факт мешает клиентам, находящимся за NAT, установить подключение с сервером, так как для них установление подключения точка-точка не представляется возможным по умолчанию. Однако, поскольку в протоколе GRE, что использует PPTP (а именно enhanced GRE), есть заголовок Call ID, маршрутизаторы, выполняющие натирование, могут идентифицировать и сопоставить GRE трафик, идущий от клиента локальной сети к внешнему серверу и наоборот. Это дает возможность клиентам за NAT установить подключение point-to-point и пользоваться протоколом GRE. Данная технология называется VPN PassTrough. Она поддерживается большим количеством современного клиентского сетевого оборудования.

PPTP поддерживается нативно на всех версиях Windows и большинстве других операционных систем. Несмотря на относительно высокую скорость, PPTP не слишком надежен: после обрыва соединения он не восстанавливается

так же быстро, как, например, OpenVPN. В настоящее время PPTP по существу устарел и Microsoft советует пользоваться другими VPN решениями. Мы также не советуем выбирать PPTP, если для вас важна безопасность и конфиденциальность.

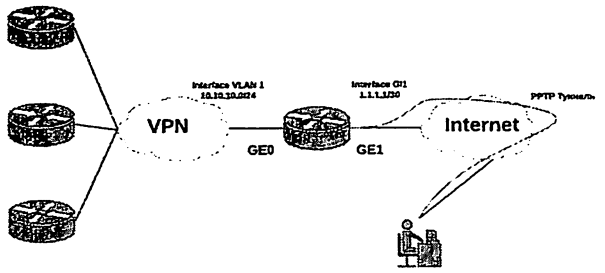
Конечно, если вы просто используете VPN для разблокировки контента, PPTP имеет место быть, однако, повторимся: есть более безопасные варианты, на которые стоит обратить внимание.

L2TP/ L2F. Layer 2 Tunneling Protocol (L2TP) был впервые предложен в 1999 году в качестве обновления протоколов L2F (Cisco) и PPTP (Microsoft). Поскольку L2TP сам по себе не обеспечивает шифрование или аутентификацию, часто с ним используется IPsec. L2TP в паре с IPsec поддерживается многими операционными системами, стандартизирован в RFC 3193. L2TP/IPsec считается безопасным и не имеет серьезных выявленных проблем (гораздо безопаснее, чем PPTP). L2TP/IPsec может использовать шифрование 3DES или AES, хотя, учитывая, что 3DES в настоящее время считается слабым шифром, он используется редко.

Последовательность выполнения работы:

1. Запуск симулятора Cisco packet tracer
2. Для выполнения лабораторной работы используем коммутатор cisco 2960 и маршрутизатор cisco 2911
3. Построить нижеприведенную топологию сети
4. Тестировать, выполненную топологию сети

Интерфейс VLAN 1 (подсеть 10.10.10.0/24) маршрутизируется в основной сети. Если мы «подключим» удаленных пользователей через PPTP туннель к данному VLAN и назначим адрес из диапазона 10.10.10.0/24, то, логично, что у них появится доступ ко всем сетевым ресурсам.



В данном случае аутентификация будет реализована через локальные аккаунты на маршрутизаторе Cisco. Однако, в соответствии с рекомендациями по безопасности, мы рекомендуем использовать внешний RADIUS сервер. PPTP всегда настраивается между сервером (маршрутизатором Cisco) и клиентом (рабочей станцией Windows). PPTP поддерживается маршрутизаторами Cisco, а МСЭ ASA, в свою очередь, не поддерживают терминирование туннеля на самом фаерволле.

1. Настройка ROUTERa:

```
vpdn enable  //Включаем VDPN (Virtual Private Dialup Network)
vpdn source-ip 1.1.1.1 //адрес используемый для входящих подключений
vpdn-group MerioNet //название группы
accept-dialin //разрешает маршрутизатору принимать подключение
protocol pptp //используемый протокол
virtual-template 1 //интерфейс, используемый для доступа
interface Virtual-Template1 //интерфейс используемый для клонирования
!описание  PPTP доступа
ip unnumbered Vlan1 //использование адреса, настроенного для VLAN 1
ip virtual-reassembly in
load-interval 30
peer default ip address pool PPTP-Pool //назначение сетевого адреса для клиентов в диапазоне, указанном в PPTP-
no keepalive
ppp encrypt mppe auto //Использование MPPE шифрования с автоматически указанной силой шифрования (40, 56 или 128 бит)
ppp authentication ms-chap ms-chap-v2 //настройка разрешенных способов методов аутентификации
ip local pool PPTP-Pool 10.10.10.90 10.10.10.100 //диапазон IP-адресов, которые могут получать клиенты
username RemoteUserMerionet password merionet //создание локального пароля и логина для подключения.
```

2. Настройка интерфейса:

```
interface GigabitEthernet1
description WAN Interface
ip address 1.1.1.1 255.255.255.252
interface Vlan1
description LAN Network
ip address 10.10.10.1 255.255.255.0
```

3. Подключить какой-нибудь клиент и проверьте работоспособность PPTP командами:

```
show users
show vpdn
```

Задание:

Каждому студенты нужно выполнять лабораторные работы в среде Cisco Packet Tracer на основе приведенной выше информации и подготовить отчёт.

Контрольные вопросы

1. Что такое PPTP?
2. Что такое L2F?
3. Что такое L2TP?
4. Что такое IPSec

ЛАБОРАТОРНАЯ РАБОТА №15
СОЗДАНИЕ VPN СЕТИ В ПРЕДПРИЯТИЯХ

Цель работы: Освоение теоретических знаний и практических навыков по создании VPN сетей в предприятиях

Краткие теоретические сведения

VPN – Virtual Private Network – виртуальная частная сеть. Это совокупность технологий, позволяющих обеспечить одно или несколько

сетевых соединений (логическую сеть) поверх другой сети (например, Интернет).

Расшифровка названия: сеть – объединение нескольких устройств каким-либо видом связи, позволяющее обмениваться информацией. Виртуальная – неосязаемая, не физическая, то есть не важно, по каким именно каналам связи она проложена. Физическая и логическая топологии могут как совпадать, так и отличаться. Частная – в эту сеть не может войти посторонний пользователь, там находятся только те, кому разрешили доступ. В частной сети надо маркировать участников и их трафик, чтобы отличить его от остальной, чужой информации. Также в такой сети обеспечивается защита данных криптографическими средствами, попросту говоря, шифруется. Приведем еще одно определение: VPN – это сервис, позволяющий защитить приватные данные при пользовании Интернетом.

Соединение VPN – это, так называемый, "туннель" между компьютером пользователя и компьютером-сервером. Каждый узел шифрует данные до их попадания в "туннель". Вы подключаетесь к VPN, система идентифицирует вашу сеть и начинает аутентификацию (сравнивает введенный пароль с паролем в своей базе данных). Далее сервер Вас авторизует, то есть предоставляет право на выполнение определенных действий: чтение почты, интернет-серфинг и т.д. После установления соединения весь трафик передается между вашим ПК и сервером в зашифрованном виде. Ваш ПК имеет IP-адрес, предоставленный интернет-провайдером. Этот IP блокирует доступ к некоторым сайтам. VPN сервер меняет ваш IP на свой. Уже с VPN-сервера все данные передаются к внешним ресурсам, которые вы запрашиваете. Теперь можно просматривать любые ресурсы и не быть отслеженным.

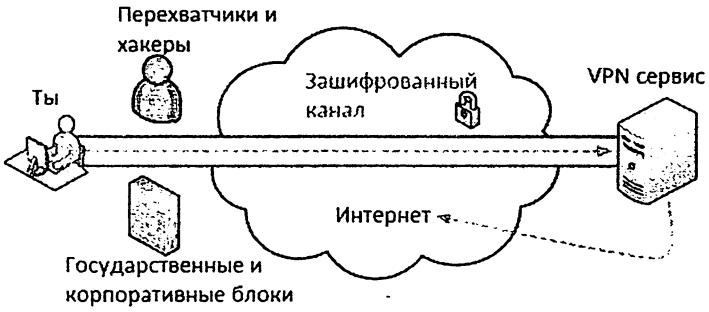


Рис. 15.1. Принцип работы VPN

Однако, следует помнить, что не вся информация шифруется. У разных VPN-провайдеров могут отличаться такие характеристики как степень шифрования, сокрытие факта подключения к серверу, хранение логов (журнал, в который сохраняется информация о посещаемых сайтах, реальный IP адреси т.п.) и сотрудничество при выдаче информации третьим лицам. Если VPN-провайдер вообще не записывает логи, то передавать третьим лицам просто нечего. А сокрытие факта подключения к серверу – уже более редкая услуга. При некорректном подключении или резком разрыве соединения может произойти утечка части данных. Решить проблему поможет технология Multihop VPN, которая предполагает соединение с сайтом сразу через несколько серверов.

Последовательность выполнения работы:

1. Запуск симулятора Cisco packet tracer
2. Построить нижеприведенную топологию сети
3. Тестировать, выполненную топологию сети

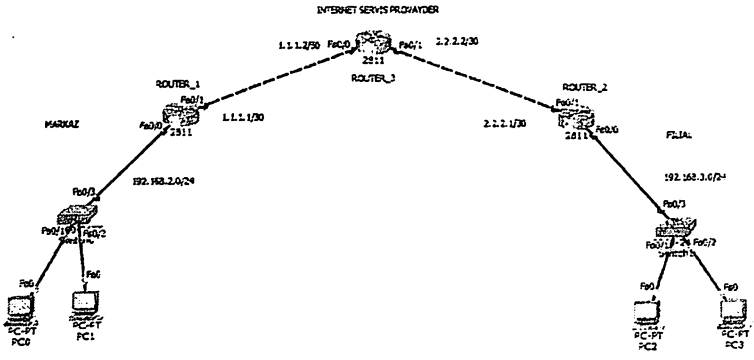


Рис. 15.2. Исследуемая топология сети

1. Команды в ROUTER_1.

```
Router>enable
Router#conf t
Router(config)#int fa 0/0
Router(config-if)#no shut
Router(config-if)#ip nat inside
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config)#int fa 0/1
Router(config-if)#no shut
Router(config-if)#ip address 1.1.1.1 255.255.255.252
Router(config-if)#ip nat outside
Router(config-if)#exit
Router(config)#ip access-list extended for-nat
Router(config-ext-nacl)#deny ip 192.168.2.0 0.0.0.255 192.168.3.0 0.0.0.255
Router(config-ext-nacl)#permit ip 192.168.2.0 0.0.0.255 any
Router(config-ext-nacl)#exit
Router(config)#ip nat inside source list for-nat int fa 0/1 overload
Router(config)#ip route 0.0.0.0 0.0.0.0 1.1.1.2
Router(config)#ip dhcp pool vl2
Router(dhcp-config)#network 192.168.2.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.2.1
Router(dhcp-config)#dns-server 8.8.8.8
Router(dhcp-config)#exit
Router(config)#crypto isakmp policy 1
Router(config-isakmp)#encryption aes
Router(config-isakmp)#hash md5
Router(config-isakmp)#authentication pre-share
Router(config-isakmp)#group 2
```

```
Router(config)#crypto isakmp key 123 address 2.2.2.1
Router(config)#crypto ipsec transform-set ts esp-aes esp-md5-hmac
Router(config)#ip access-list extended for-vpn
Router(config-ext-nacl)#permit ip 192.168.2.0 0.0.0.255 192.168.3.0 0.0.0.255
Router(config-ext-nacl)#exit
Router(config)#crypto map kriptokarta 10 ipsec-isakmp
Router(config-crypto-map)#match address for-vpn
Router(config-crypto-map)#set peer 2.2.2.1
Router(config-crypto-map)#set transform-set ts
Router(config-crypto-map)#exit
Router(config)#int fa 0/1
Router(config-if)#crypto map kriptokarta
*Jan 3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
Router(config-if)#exit (процесс построения VPN)
```

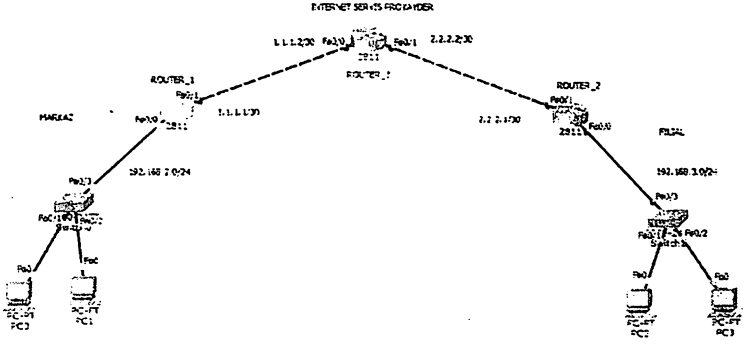


Рис. 15.3. Настройка ROUTER_1

2. Команды для ROUTER_2.

```
Router>enable
Router#conf t
Router(config)#int fa 0/0
Router(config-if)#no shut
Router(config-if)#ip nat inside
Router(config-if)#ip address 192.168.3.1 255.255.255.0
Router(config-if)#exit
Router(config)#int fa 0/1
Router(config-if)#no shut
Router(config-if)#ip address 2.2.2.1 255.255.255.0
Router(config-if)#ip nat outside
Router(config-if)#exit
Router(config)#ip access-list extended for-nat
Router(config-ext-nacl)#deny ip 192.168.3.0 0.0.0.255 192.168.2.0 0.0.0.255
```

```
Router(config-ext-nacl)#permit ip 192.168.3.0 0.0.0.255 any
Router(config-ext-nacl)#exit
Router(config)#ip nat inside source list for-nat int fa 0/1 overload
Router(config)#ip route 0.0.0.0 0.0.0.0 2.2.2.2
Router(config)#ip dhcp pool vl3
Router(dhcp-config)#network 192.168.3.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.3.1
Router(dhcp-config)#dns-server 8.8.8.8
Router(dhcp-config)#exit
Router(config)#crypto isakmp policy 1
Router(config-isakmp)#encryption aes
Router(config-isakmp)#hash md5
Router(config-isakmp)#authentication pre-share
Router(config-isakmp)#group 2
Router(config-isakmp)#exit
Router(config)#crypto isakmp key 123 address 1.1.1.1
Router(config)#crypto ipsec transform-set ts esp-aes esp-md5-hmac
Router(config)#ip access-list extended for-vpn
Router(config-ext-nacl)#permit ip 192.168.3.0 0.0.0.255 192.168.2.0 0.0.0.255
Router(config-ext-nacl)#exit
Router(config)#crypto map kriptokarta 10 ipsec-isakmp
Router(config-crypto-map)#match address for-vpn
Router(config-crypto-map)#set peer 1.1.1.1
Router(config-crypto-map)#set transform-set ts
Router(config-crypto-map)#exit
Router(config)#int fa 0/1
Router(config-if)#crypto map kriptokarta
*Jan 3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
Router(config-if)#exit
```

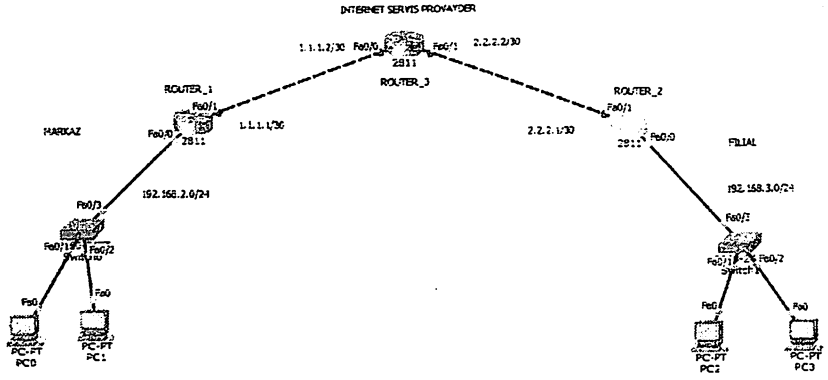


Рис. 15.4. Настройка ROUTER_2

3. Команды для ROUTER_3:

```
Router>enable
Router#conf t
Router(config)#int fa 0/0
Router(config-if)#no shut
Router(config-if)#ip address 1.1.1.2 255.255.255.252
Router(config)#int fa 0/1
Router(config-if)#no shut
Router(config-if)#ip address 2.2.2.2 255.255.255.0
Router(config-if)#exit
```

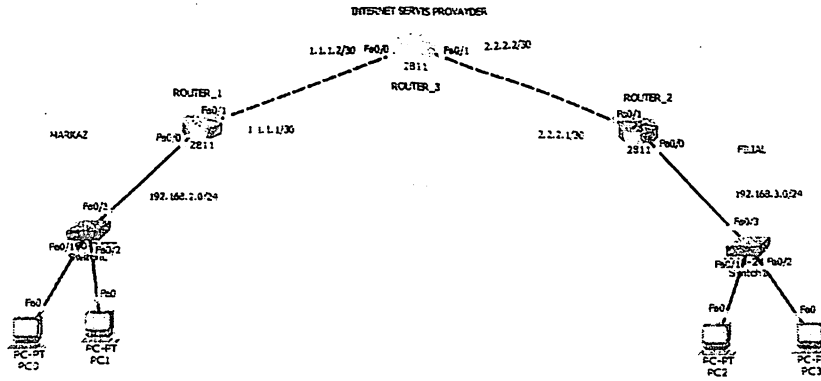


Рис. 15.5. Настройка ROUTER_3

4. Тестрировать, выполненную лабораторную работу, т.е. с PC0 на PC2 проверить с использованием протокола icmp.

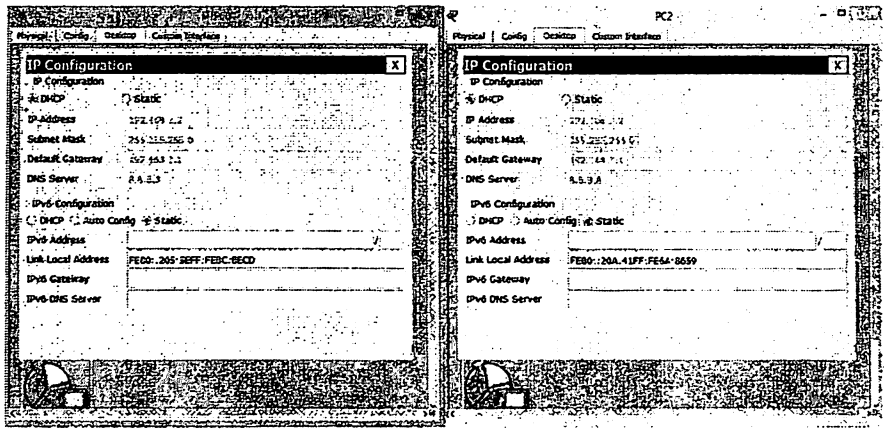


Рис. 15.6. IP адреса компьютеров PC0 va PC2

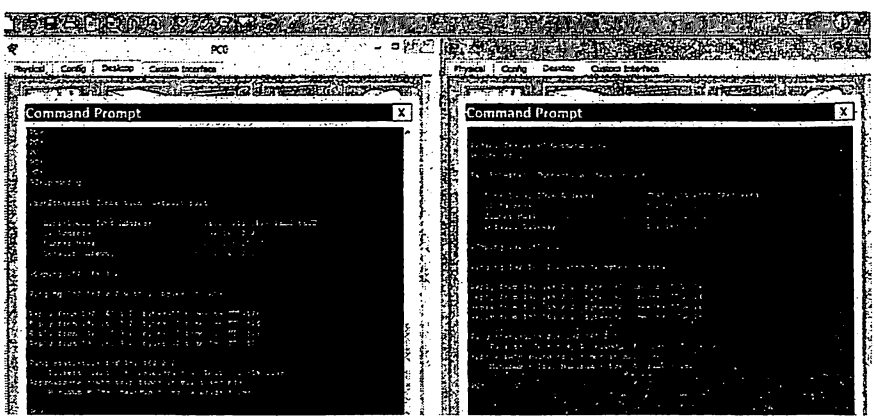


Рис. 15.7. Тестирование результатов

Чтобы увидеть статистику информации, отправленную через канал VPN используем следующую команду:

```
Show crypto ipsec sa
```

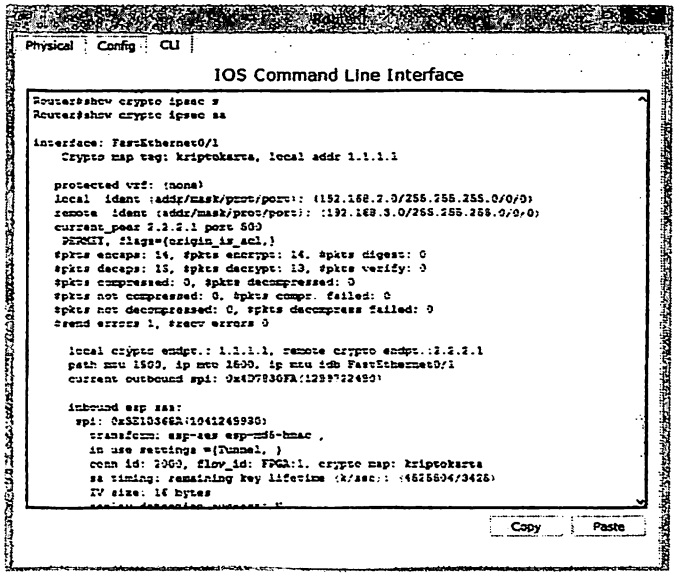
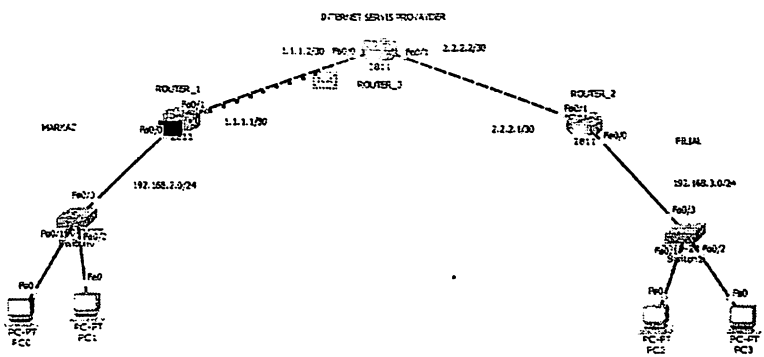


Рис. 15.8. Статистика информаций, отправляемая через канал VPN



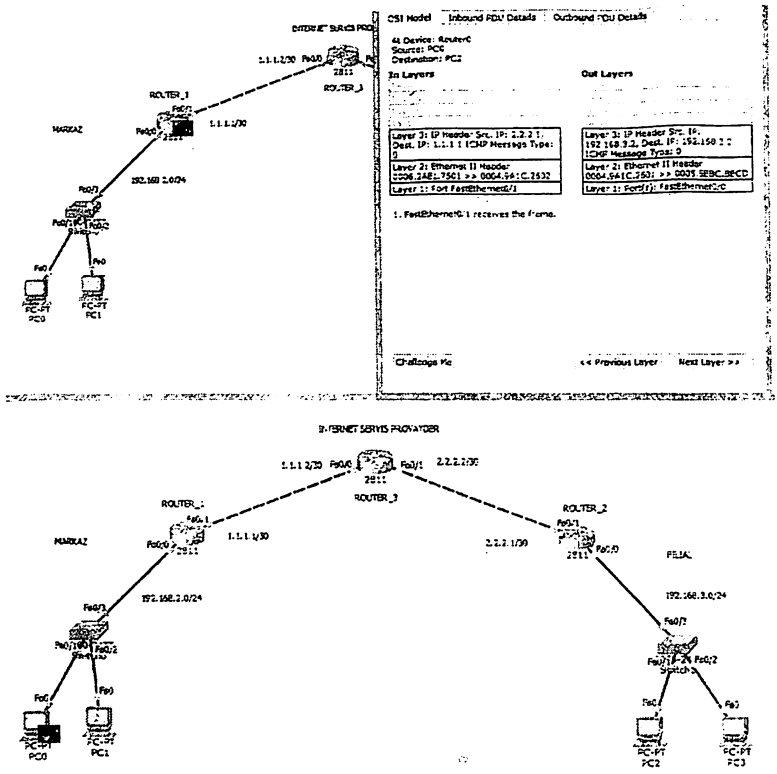


Рис. 15.9. Маршрут пакет, отправленная по топологии сети

Задание:

Каждому студенты нужно выполнять лабораторные работы в среде Cisco Packet Tracer на основе приведенной выше информации и подготовить отчёт.

Контрольные вопросы:

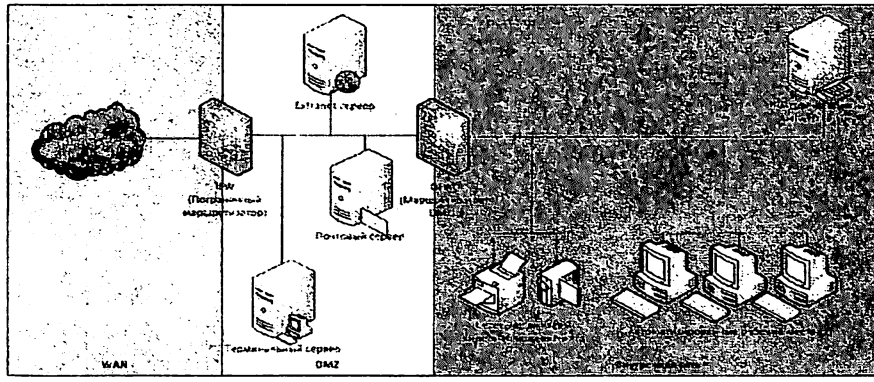
1. Что такое VPN?
2. Какой принцип работы VPN?
3. Какие протоколы используются в VPN?

ЛАБОРАТОРНАЯ РАБОТА №16
УСТАНОВКА DMZ В СЕТЕВЫХ МАРШРУТИЗАТОРАХ

Цель работы: Освоение теоретических знаний и практических навыков по установке DMZ в сетевых маршрутизаторах.

Краткие теоретические сведения:

DMZ является физическим или виртуальным сервером, служащим как буфер между локальной сетью и интернетом. Применяется для предоставления пользователям локальной сети услуг электронной почты, удалённых серверов, веб-приложений и других программ, которые требуют доступ во Всемирную паутину. Для доступа к внутренним ресурсам извне нужно пройти процедуру авторизации, попытка войти для не авторизованных пользователей успехом не увенчается. В большинстве случаев это настройка маршрутизатора.



Название происходит от английской аббревиатуры, обозначающей демилитаризованную зону как барьер между враждующими территориями. Эта технология применяется, когда вы создаёте домашний сервер, доступ к которому должен осуществляться с любого компьютера, подсоединённого к интернету. Настоящая демилитаризованная зона используется в больших

корпоративных сетя

модели роутеров пол

Последовательность выполнения работы:

1. Запуск симулятора Cisco packet tracer
2. Для выполнения лабораторной работы используем коммутатор cisco 2960 и маршрутизатор cisco 2911, ASA0 5505 firewall, компьютеры и сервер
3. Построить нижеприведенную топологию сети
4. Тестировать, выполненную топологию сети

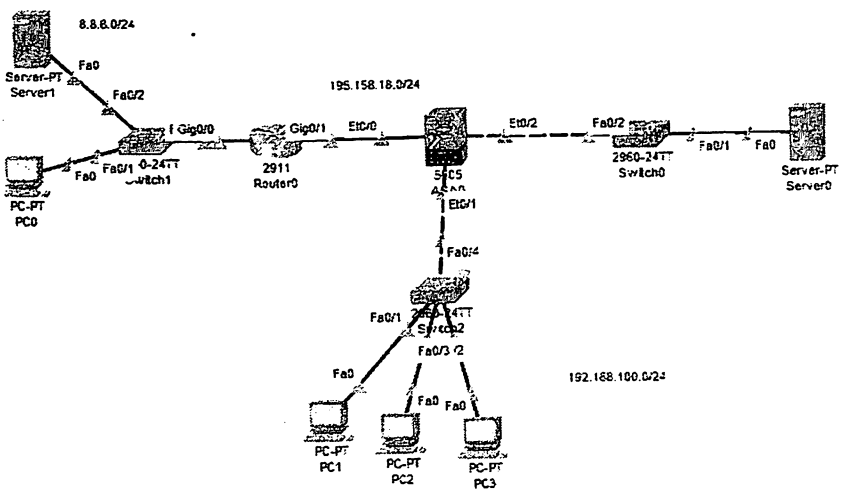


Рис. 16.1. Исследуемая топология сети

1. Команды на ASA0.

```
ciscoasa>en
ciscoasa#conf t
ciscoasa#no dhcpd enable inside
ciscoasa#no dhcpd address 192.168.1.5-192.168.1.36 inside
ciscoasa(config)#interface vlan 1
ciscoasa(config-if)#ip address 192.168.100.1 255.255.255.0
```

```
ciscoasa(config-if)#exit
ciscoasa(config)#dhcpd enable inside
ciscoasa(config)#dhcpd address 192.168.100.22-192.168.100.50 inside
ciscoasa(config)#dhcpd dns 8.8.8.8
ciscoasa(config)#interface vlan 2
ciscoasa(config-if)#ip address 195.158.18.18  255.255.255.0
ciscoasa(config-if)#exit
ciscoasa(config)#route outside 0.0.0.0 0.0.0.0 195.158.18.1
ciscoasa(config)#object network NAT
ciscoasa(config-network-object)#subnet 192.168.100.0 255.255.255.0
ciscoasa(config-network-object)#nat (inside,outside) dynamic outside
ciscoasa(config-network-object)#exit
ciscoasa(config)#class-map qoida
ciscoasa(config-if)#match default-inspection-traffic
ciscoasa(config-if)#exit
ciscoasa(config)#policy-map toplam
ciscoasa(config)#class qoida
ciscoasa(config)#inspect http
ciscoasa(config)#inspect icmp
ciscoasa(config)#exit
ciscoasa(config)#service-policy toplam global
ciscoasa(config)#exit
ciscoasa(config)#enable salom
ciscoasa(config)#username admin password tatu123
ciscoasa(config)#hostname ASA
ASA(config)#domain-name tatu.uz
ASA(config)#ssh 192.168.100.0 255.255.255.0 inside
ASA(config)#aaa authentication ssh console LOCAL
ASA(config)#aaa authentication telnet console LOCAL
ASA(config)#ssh 8.8.8.8 255.255.255.255 outside
ASA(config)#interface vlan 3
ASA(config-if)#no forward interface vlan 1
ASA(config-if)#nameif DMZ
ASA(config-if)#ip address 192.168.70.1 255.255.255.0
ASA(config-if)#exit
ASA(config)#interface vlan 3
ASA(config-if)#security-level 70
ASA(config-if)#exit
ASA(config)#object network DMZ
ASA(config-network-object)#nat (DMZ,outside) static 195.158.18.88
ASA(config-network-object)#exit
ASA#
ASA#conf t
ASA(config)#access-list DMZ permit icmp any host 195.158.18.88
ASA(config)#access-group DMZ in interface outside
ASA(config)#access-list DMZ permit tcp any host 195.158.10.88 eq www
ASA(config)#end
```

2. Команды на ROUTER.

```
continue with configuration dialog? [yes/no]: no
Router>enable
Router#conf t
Router(config)#interface gigabitEthernet 0/1
Router(config-if)#no shutdown
Router(config-if)#ip address 195.158.18.1 255.255.255.0
Router(config-if)#exit
Router(config)#interface gigabitEthernet 0/0
Router(config-if)#no shutdown
Router(config-if)#ip address 8.8.8.1 255.255.255.0
Router(config-if)#do wr
```

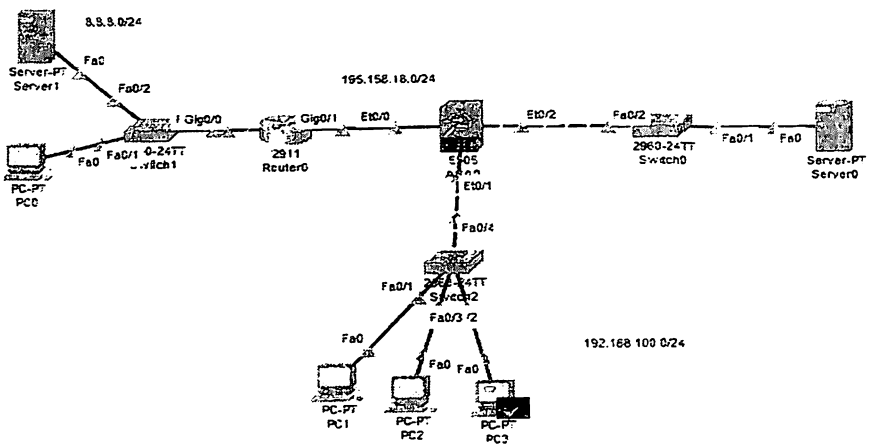


Рис. 16.2. Тестирование топологии сети

Задание:

Почледоветально сделать лабораторную работу по образцу и подготовить отчет.

Контрольные вопросы:

1. Что такое DMZ?
2. Зачем в корпоративных сетях строят зоны DMZ?
3. Объяснить принцип работы DMZ?

ЛАБОРАТОРНАЯ РАБОТА №17
ПОИСК И УСТРАНЕНИЕ ПРОБЛЕМ В СЕТИ. TROUBLESHOOTING

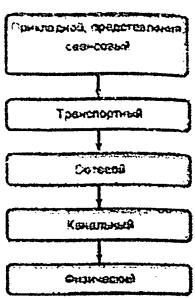
Цель работы: Освоение теоретических знаний и практических навыков по поиске и устранении проблем в сетевых устройств и сети

Краткие теоретические сведения

Успешно обнаружить и устранить сетевые неисправности может лишь тот, кому досконально известно, как должна работать сеть в нормальном режиме. Только при таком условии можно быстро распознать отклонение от нормы и диагностировать неполадку.

Хороший технический специалист сначала подробно изучит всю доступную ему информацию, постарается досконально разобраться в работе всех компонентов и научится правильно обращаться с ними. Опытные сетевые инженеры знают, что за серьезный сбой можно принять результат неправильного применения приложения или последствия так называемого «человеческого фактора».

Существует ряд структурированных методов поиска и устранения неполадок.



Снизу вверх	Всегда начинается на прикладном уровне и выполняется вниз по уровням до нижележащего уровня, на котором произошел сбой.	Больше подходит для решения более простых проблем, а также если есть подозрение, что проблемы связаны с аппаратными или пользовательскими, то есть с верхними уровнями.	Если в итоге выясняется, что проблема связана с нижними уровнями, происходит непродуктивная трата времени и усилий на верхнем или прикладном уровнях.

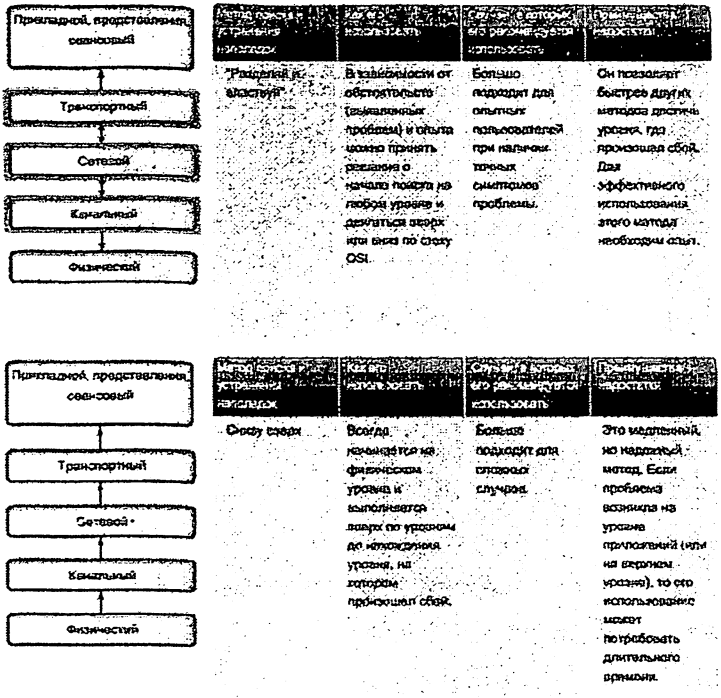


Рис. 17.1. Методы: сверху вниз, снизу вверх и "разделяй и властвуй"

Все эти структурированные методы предполагают многоуровневое строение сети. Примером многоуровневой сети является модель OSI, в которой все функции обмена данными строго поделены на семь уровней. При поиске и устранении неполадок в этой модели можно последовательно проверить работоспособность всех функций на каждом уровне, пока проблема не будет локализована.

Метод "сверху вниз" предполагает движение вниз с прикладного уровня. Проблема исследуется с точки зрения пользователя и приложения. Не работает только одно приложение или все приложения? Например, может ли пользователь при недоступности электронной почты обращаться к веб-страницам? Проявляются ли подобные явления на других рабочих станциях?

Метод "снизу вверх" предполагает движение с физического уровня к более высоким. На физическом уровне обследуются оборудование и проводные соединения. Не выпали ли кабели из гнезд? Если оборудование снабжено индикаторами, горят ли индикаторы?

При использовании метода "разделяй и властвуй" анализ начинается с одного из промежуточных уровней, после чего обследуются вышестоящие или нижестоящие уровни. Например, диагностику можно начать с сетевого уровня, проверив конфигурацию IP.

Последовательность выполнения работы:

1. Запуск симулятора Cisco packet-tracer
2. Для выполнения лабораторной работы используем коммутатор cisco 2960 и маршрутизатор cisco 2911 и компьютеры
3. Построить нижеприведенную топологию сети
4. Тестировать, выполненную топологию сети

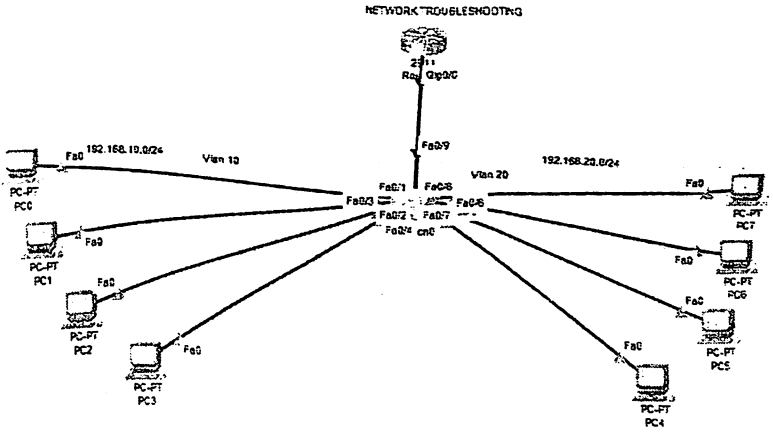


Рис. 17.2. Исследуемая сетевая структура

1. Команды на SWITCH.

```
Switch>en
Switch#conf t
Switch(config)#interface range fastEthernet 0/1-4
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 10
Switch(config-if-range)#ex
Switch(config)#interface range fastEthernet 0/5-8
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 20
Switch(config-if-range)#ex
Switch(config)#interface fastEthernet 0/9
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan 10
Switch(config-if)#do wr
```

2. Команды на ROUTER.

```
Router>en
Router#conf t
Router(config)#interface gigabitEthernet 0/0
Router(config-if)#no shutdown
Router(config-if)#ex
Router(config)#interface gigabitEthernet 0/0.10
Router(config-subif)#encapsulation dot1Q 10
Router(config-subif)#ip address 192.168.10.1 255.255.255.0
Router(config-subif)#ex
Router(config)#interface gigabitEthernet 0/0.20
Router(config-subif)#encapsulation dot1Q 20
Router(config-subif)#ip address 192.168.20.1 255.255.255.0
Router(config-subif)#ex
Router(config)#ip dhcp pool t1
Router(dhcp-config)#network 192.168.10.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.10.1
Router(dhcp-config)#ex
Router(config)#ip dhcp pool t2
Router(dhcp-config)#network 192.168.20.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.20.1
Router(dhcp-config)#do wr
```

Допущена ошибка при настройке топологии. Чтобы выяснить, где произошла ошибка, необходимо назначить статический IP-адрес одному хосту в каждом vlane и динамический IP-адрес остальным хостам.

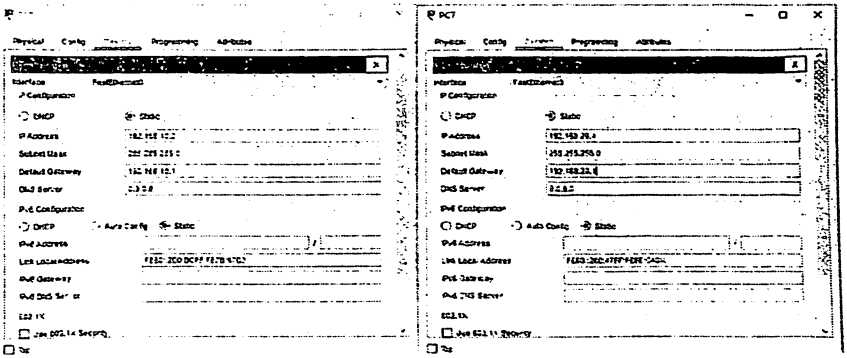


Рис. 17.3. Установка статического IP адреса хостам в Vlan 10 и Vlan 20

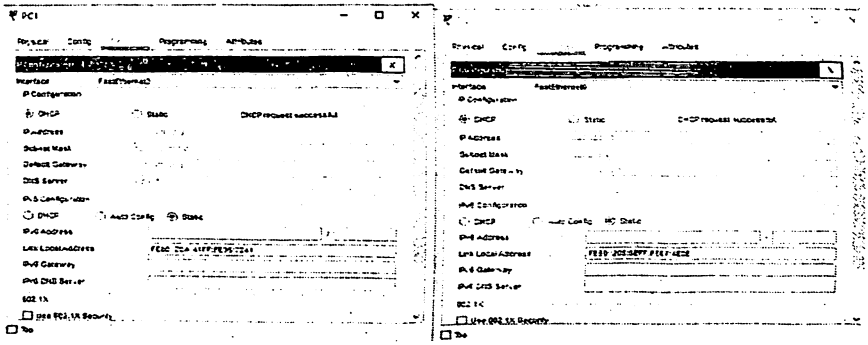


Рис. 17.4. Установка динамического IP адреса хостам в Vlan 10

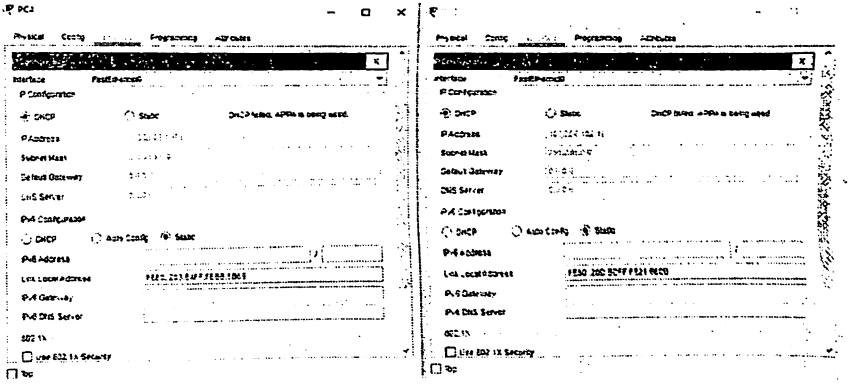


Рис. 17.5. Установка динамического IP адреса хостам в Vlan 20

Как видно из рисунков выше (рис. 17.4-17.5). Хосты на Vlan 10 получили IP-адрес, но хосты на Vlan 20 не получили IP-адрес. Поэтому нам нужно исправить эту ошибку, выяснив, почему vlan 20 не получил IP-адрес.

Следующие команды используются для диагностики проблем с коммутаторами и маршрутизаторами:

– **Команды коммутатора:**

Show vlan – просмотр vlan
Show vlan brief-
Show interface trunk-
Show ip arp-
Show mac-address-table-
Show ip interface brief show interface fastEthernet 0/1...

– **Команды маршрутизатора:**

Show ip arp-
Show dhcp lease-
Show ip dhcp pool-
Show ip dhcp binding-...

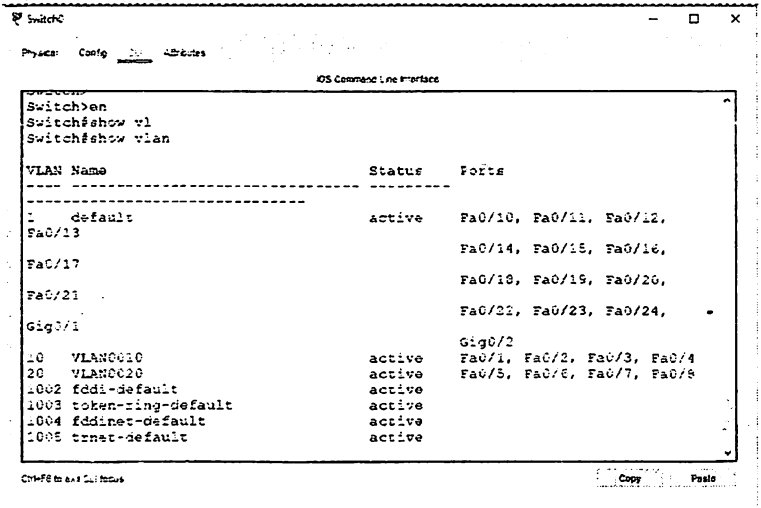


Рис. 17.6. Show vlan

С рисунка 17.6 видно, проблем с Vlanами нет.

```
Switch#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/9       on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/9       10

Port        Vlans allowed and active in management domain
Fa0/9       10

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/9       10
```

Рис. 17.7. Show interface trunk

Рисунок 17.7 показывает, что проблема в интерфейсе. При подключении vlan к trunk портам vlan 20 оставался неподключенным, поэтому служба DHCP не работала на хостах на vlan 20. Проблема решается следующим образом:

```
Switch#
Switch#conf t
Switch(config)#interface fastEthernet 0/9
Switch(config-if)#switchport trunk allowed vlan add 20
Switch(config-if)#
```

Тестирование для проверки устранения проблемы (рис. 17.8)

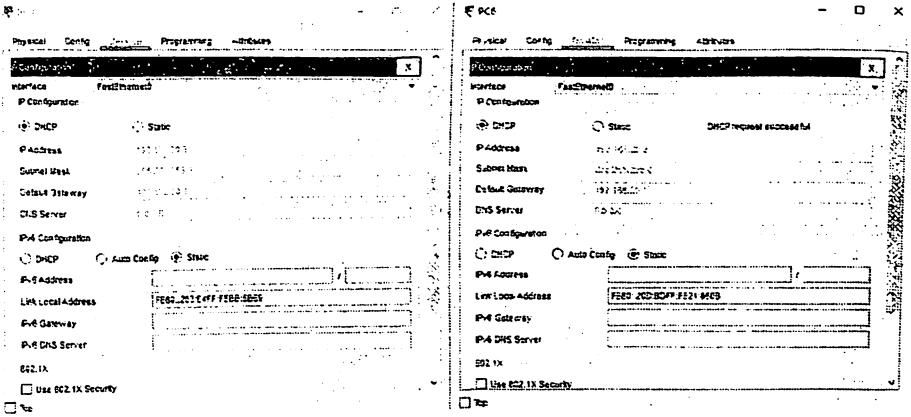


Рис.17.8 Тестирование результатов

Задание:

Каждому студенты нужно выполнять лабораторные работы в среде Cisco Packet Tracer на основе приведенной выше информации и подготовить отчёт.

Контрольные вопросы

1. Что такое Troubleshooting?
2. Какие методы есть в Troubleshooting?
3. Обьяснить метод «сверху-вниз»?
4. Обьяснить метод «снизу-вверх»?
5. Обьяснить метод «"разделяй и властвуй"»?

ЛАБОРАТОРНАЯ РАБОТА №18
УСТАНОВКА И НАСТРОЙКА ПО FIREWALL.

Цель работы: Освоение теоретических знаний и практических навыков по работе с межсетевым экраном на примере Kerio Control

Краткие теоретические сведения

Kerio Control (ранее назывался Kerio WinRoute Firewall и WinRoute Pro) — это программный межсетевой экран, разработанный компаниями Kerio Technologies и Tiny Software. Основными функциями программы являются: организация безопасного пользовательского доступа в Интернет, надежная сетевая защита ЛВС, экономия трафика и рабочего времени сотрудников за счёт ограничения нецелевого доступа к различным категориям веб-контента.

Последовательность выполнения работы:

Для установки Kerio Control Software Appliance нужно создать загрузочный носитель – флэшку или диск. В нашем случае флэшка создана с помощью программы UNetbootin.

1. Скачиваем Unetbootin и Kerio Control Software Appliance.

2. Форматируем в FAT32 средствами Windows (Рис.18.1).

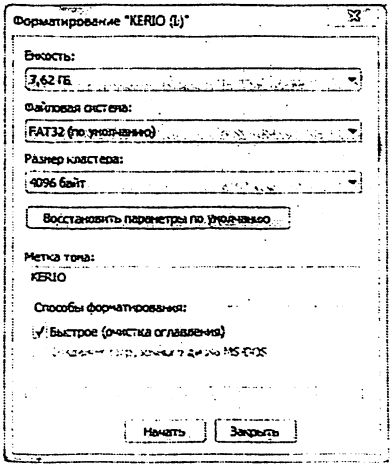


Рис. 18.1 Форматирование в FAT32 средствами Windows.

3. Запускаем UNetbootin и выбираем следующие настройки. Дистрибутив – не трогаем. Образ – Стандарт ISO, указываем путь к скаченному образу Kerio Control Software Appliance. Тип – Устройство USB, выбираем нужную флэшку и нажимаем ОК(Рис.18.2).

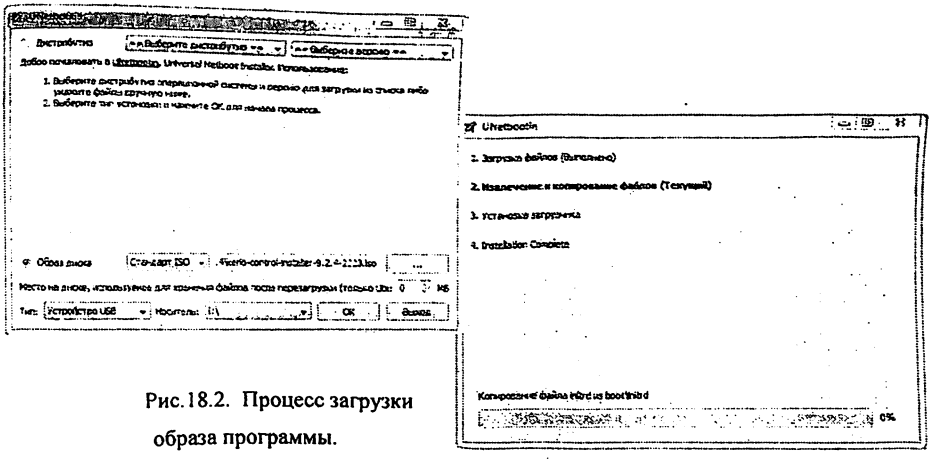


Рис.18.2. Процесс загрузки образа программы.

4. После некоторого времени создания, загрузочная флэшка готова. Жмем выход (Рис.18.3.).

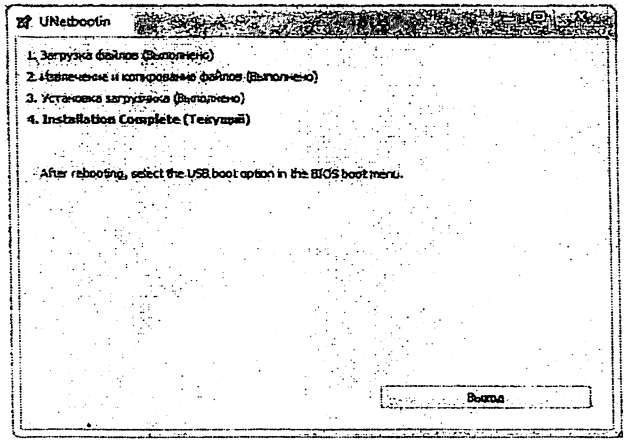


Рис.18.3. Процесс завершения загрузки образа.

На этом начинается процесс установки Kerio Control Software Appliance. На первом этапе нужно выбрать язык. После нужно прочитать лицензионное соглашение, затем принять её нажав F8. Далее потребуется ввести код подтверждения установки программы на жесткий диск. Нужно ввести код 135. Программа предупреждает о том, что жесткий диск будет отформатирован.

Сразу после завершения форматирования, начинается процесс установки программы. Ждем пока идет установка и система перезагрузится.

Чтобы завершить установку требуется перейти браузер по адресу: 10.10.10.1:4081/admin и задать пароль.

Пока этого делать не будем, а переходим в Конфигурацию сети в самом Kerio Control Software Appliance. На окне «Конфигурация сетевого интерфейса Ethernet" нужно отметить пробелом – «Назначить статический IP-адрес» и задать следующие значения.

IP-адрес: 192.168.1.250

Маска подсети: 255.255.255.0

5. После пятого этапа у нас повторно будет запрашиваться задать пароль. Но на этот раз по IP-адресу: 192.168.1.250. Затем в браузере переходим по адресу: https://192.168.1.250:4081/admin.

Браузер может сообщить что возникла проблема с сертификатом безопасности этого сайта. Нажимаем ниже – Продолжить открытие этого веб сайта и попадаем в мастер активации (Рис.18.4). Активируем Kerio Control Software Appliance который был куплен.

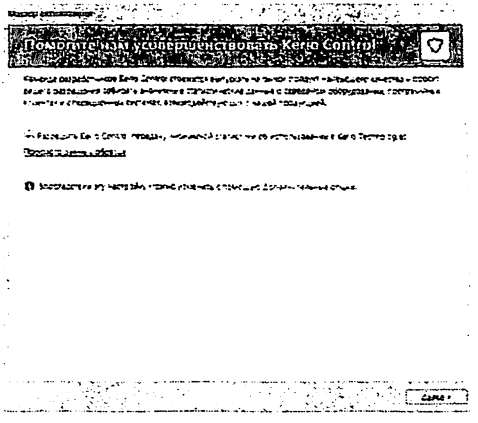


Рис. 18.4. Мастер активизации.

6. Вводим новый пароль администратора (Рис.18.4).

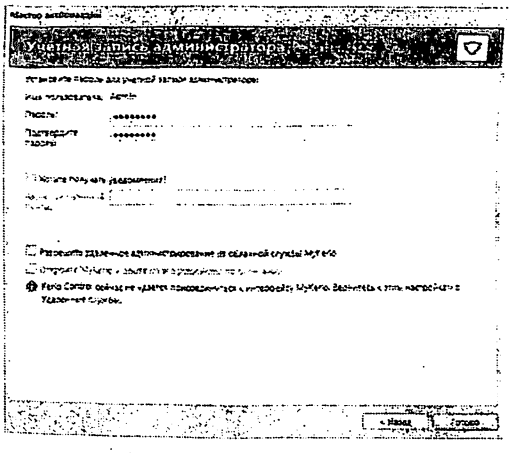


Рис.18.5. Процесс создания нового пароля.

7. Как процесс создания нового пароля завершится, начинается процесс авторизации (Рис.18.6).

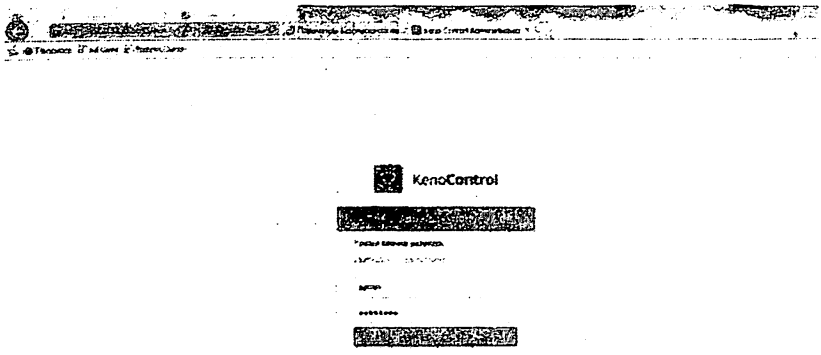


Рис.18.6. Процесс авторизации.

8. После авторизации, заходим в рабочую панель программы Kerio Control Software Appliance (Рис.18.7)

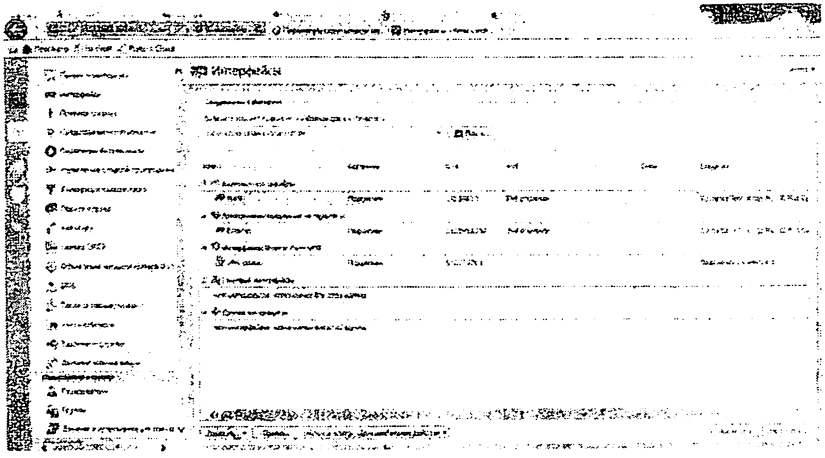


Рис.18.7. Рабочая панель Kerio Control Software Appliance.

9. Адрес внутренней сети надо изменить адрес 192.168.1.1. После смены IP нужно вводить https://192.168.1.1:4081/admin. Ниже на рисунке 18.8 приведена структурная схема подключения.

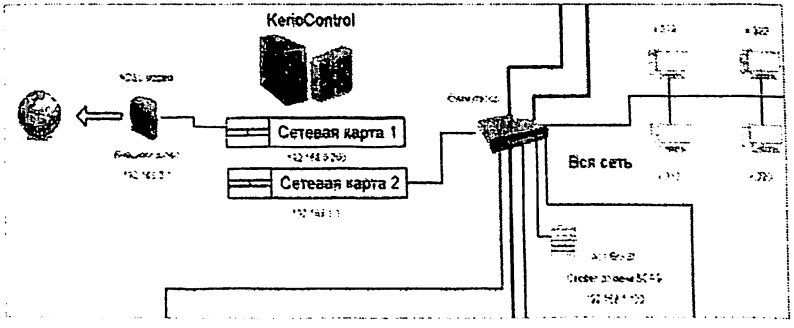


Рис.18.8. Структурная схема подключения.

10. Во вкладке интерфейсы выбираем свойства интерфейса Ethernet (Рис.18.9).

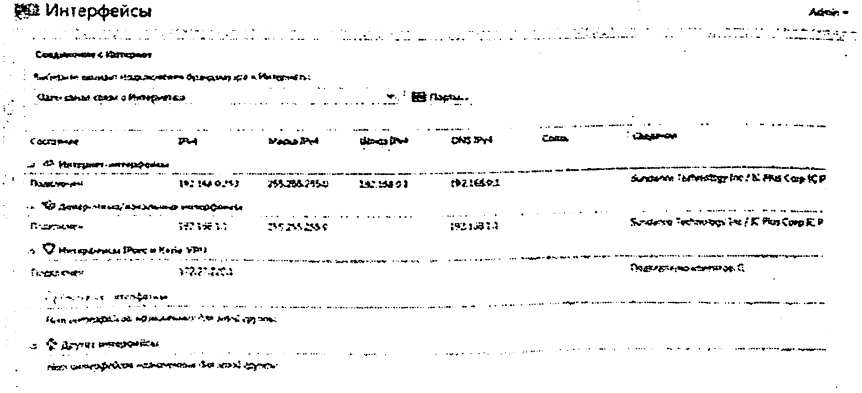


Рис.18.9. Свойства интерфейса Ethernet

11. Придумываем название типа «Внешняя сеть» или Интернет, по умолчанию написано WAN. Вводим вручную данные IP адреса, маску, шлюз и DNS, всё в одной подсети с модемом затем нажимаем «ОК» (Рис.18.10)

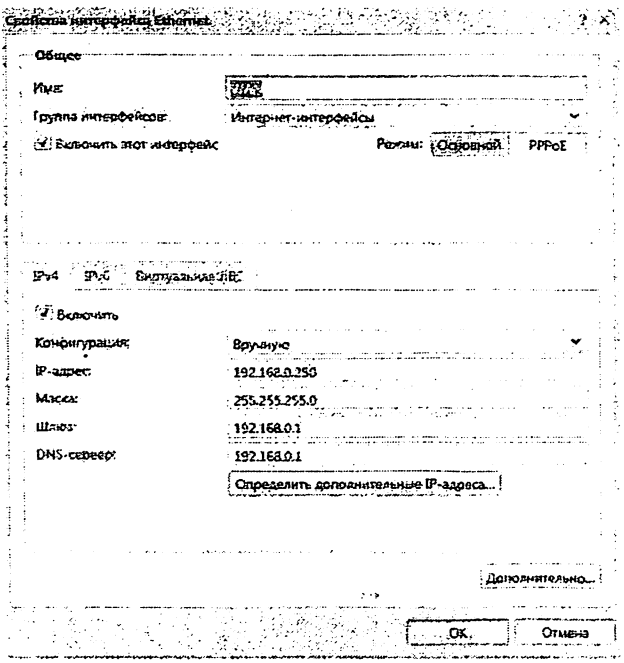


Рис.18.10. Процесс ввода общий параметров интерфейса Ethernet

12. Далее выбираем следующее подключение в пункте Доверенные/локальные интерфейсы – наша внутренняя сеть. Эти пункты в зависимости от версии Kerio Control Software Appliance могут называться по другому. Придумываем имя и вносим данные как на картинке ниже. Внешняя и внутренняя сеть не могут находится в одной подсети. Это не нужно забывать. DNS пишем от настроек Kerio Control Software Appliance. Шлюз не пишется. После ввода всех параметров нажимаем «ОК» (Рис.18.11).

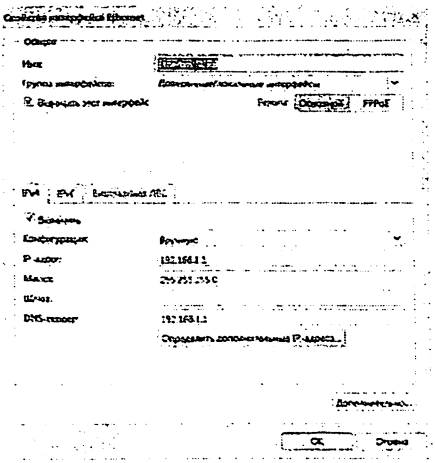


Рис.18.11. Процесс настройки параметров IPv4.

13. Нажимаем кнопку «Применить» в нижней правой части экрана, настройки активируются. Проверим подключение к Интернету. На панели мониторинга можно увидеть, что интернет работает (Рис.18.12.)

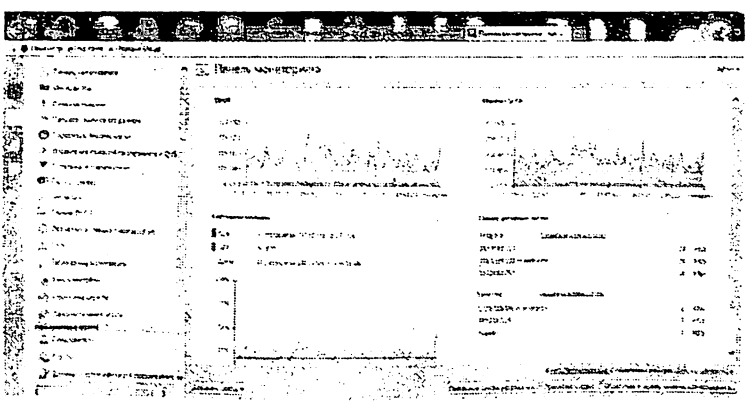


Рис.18.12. Процесс проверки соединения с интернетом на панели мониторинга.

Можно переходить к созданию правил трафика, фильтрации содержимого, посмотреть, кто скачивает торренты и перегружает сеть,

ограничить скорость или заблокировать. Kerio Control Software Appliance полноценно работает и в нем есть множество настроек. Тут каждый настраивает что кому нужно.

Открытие портов. Рассмотрим еще один важный момент – это открытие портов. До установки Kerio Control Software Appliance в модеме были проброшены порты на сервер. Так же изначально необходимые порты были открыты в самом сервере. Без этих портов специальная программа сервера не может нормально работать.

Рассмотрим открытие порта 4443. Модем HUAWEI HG532e, заходим в него, для этого в адресной строке браузера вводим 192.168.0.1. Переходим по вкладкам Advanced—>NAT—> Port Mapping и вносим данные как на рисунке 18.14 ниже.

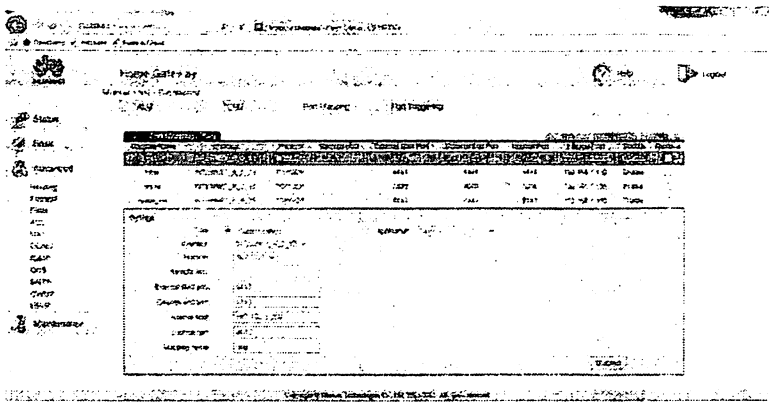


Рис.18.14. Настройка Port Mapping

Вводим следующие данные:

1. Наше подключение (в режиме роутера).
2. Протокол – TCP/UDP.
3. Remote host – ничего.
4. External start port/end port – 4443 (внешний порт).

5. Internal host – 192.168.0.250 (адрес внешней сетевой карты Kerio Control Software Appliance).

6. Internal port – 4443 (внутренний порт).

7. Mapping name – любое понятное имя.

Принцип действия таков, что обращение из интернета на внешний статический IP-адрес к порту 4443 будет переадресовано к внешней сетевой карте Kerio Control Software Appliance. Запрос с внешней сетевой карты перенаправлялся на внутреннюю сетевую карту и далее к нашему серверу на порт 4443 (Рис.18.15).

Это делается с помощью создания двух правил. Первое правило разрешает доступ извне, второе правило разрешает доступ изнутри.

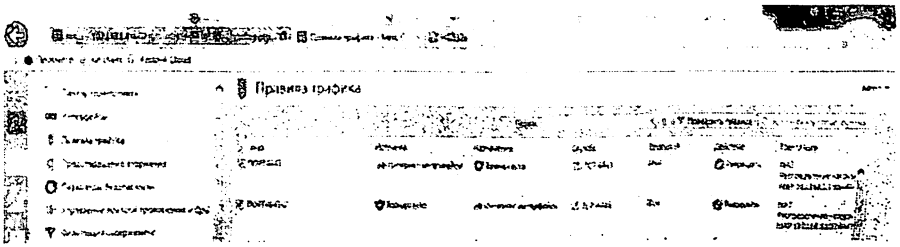


Рис.18.15. Процесс запроса с внешней сетевой карты.

Создаем эти два правила на вкладке «Правила трафика». Разница в пунктах источник и назначения. Служба – наш порт 4443. В пункте «Трансляция» делаем настройки как на рисунке 18.16. Отмечаем галочкой — «Адрес назначения» NAT и пишем там IP-адрес сервера назначения и нужный порт, затем нажимаем «ОК».

После ввода данных нажимаем применить. Проверяем, открылся ли порт в он-лайн сервисе (Рис.18.17).

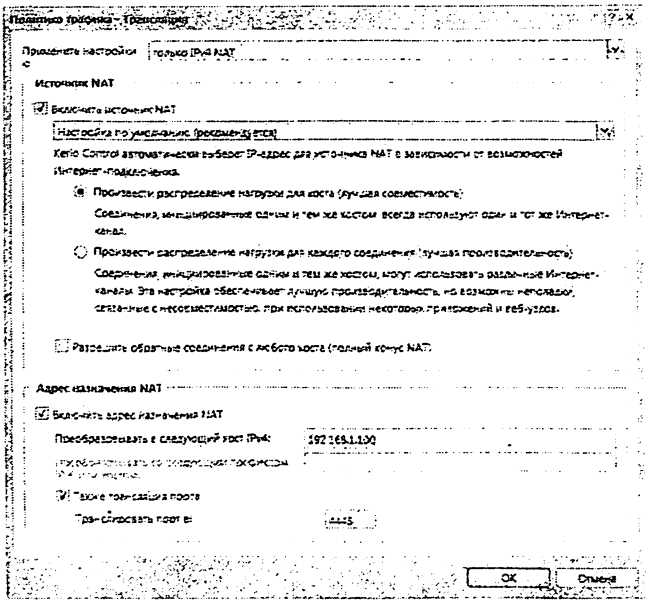


Рис.18.16. Настройка политики трафика.

Проверка порта

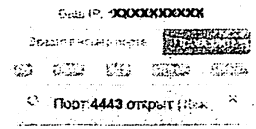


Рис.18.17. Процесс проверки порта.

Далее можно проверить службы сервера, для которых всё это делалось. Аналогичным способом можно открыть любой порт.

Задание:

Каждому студенты нужно выполнять лабораторные работы в среде Cisco Packet Tracer на основе приведенной выше информации и подготовить отчёт.

Контрольные вопросы:

1. Что такое Kerio Control?
2. Какие преимущества есть в Kerio Control?
3. Какие недостатки есть в Kerio Control?

ЛАБОРАТОРНАЯ РАБОТА №19
УСТАНОВКА И НАСТРОЙКА ПО IDS / IPS

Цель работы: Освоение теоретических знаний и практических навыков по установке и настройка технологий IPS / IDS.

Краткие теоретические сведения

Snort является свободно распространяемой программой с открытым исходным кодом под лицензией GPL. Изначально Snort был создан одним из известнейших людей в мире информационной безопасности, автором многих: книг Мартином Рошем в 1998 году. Основной причиной создания этой IDS было отсутствие на тот момент достаточно эффективного, тем более бесплатного, инструмента оповещения об атаках.

Программа совместима с ОС Windows и Linux. Все выявленные угрозы (список параметров подачи тревоги имеет тонкие настройки), записываются в лог-файл. Snort работает по принципу анализа пакетов транспортного уровня, поэтому для его использования, требуется перевод сетевой карты в специальный мониторный режим. Разработчики учитывали проблему потребления системных ресурсов системами класса IDS, поэтому Snort нетребовательна к железу и работает в фоновом режиме.

Поступив в SNORT, пакет последовательно проходит через декодеры, препроцессоры и только потом уже попадает в детектор, который начинает

применять правила. Задача декодеров сводится к тому, чтоб из протоколов канального уровня (Ethernet, 802.11, Token Ring...) «вытащить» данные сетевого и транспортного уровня (IP, TCP, UDP) (Рис.88).

Snort использует 'правила' (указанные в файлах 'правила'), чтобы знать какой трафик пропустить а какой задержать. Инструмент гибок, позволяя вам записывать новые правила и соблюдать их. Программа также имеет механизм обнаружения, который использует модульную сменную архитектуру, посредством чего определенные дополнения к программе могут быть добавлены или удалены из ' механизма обнаружения'.

Snort может работать в трех режимах:

1. Как пакетный снифер, подобно tcpdump;
2. Как регистратор пакета;
3. Как развитая система обнаружения вторжения.

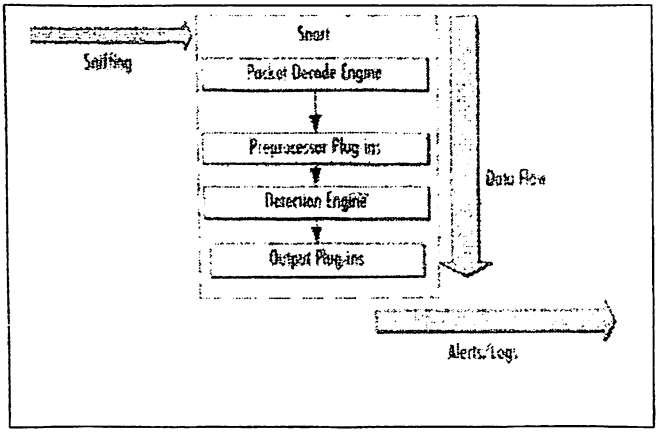


Рис.19.1. Принцип работы Snort

Последовательность выполнения работы:

Установка программы. Основной сайт для Snort - http://www.snort.org. Snort распространяется согласно лицензии GNU GPL автором Мартином

Рошом. После загрузки архива, нужно разархивировать его в каталог snort-1.7:

```
root @lord]# tar -zxvf snort-1.7.tar.gz
```

После загрузки libpcap, разархивируйте его подобным образом. Войдите в каталог libpacp, и выполните следующие шаги:

```
root @lord]# ./configure root @lord]# make
```

Теперь, нужно компилировать Snort. Для этого нужно войти в каталог, в котором находится Snort, и выполнить следующую команду:

```
root @lord]# ../configure --with-libpcap-includes=/path/to/libpcap/ {* in my case it was :
root@lord./configure--with-libpcap-includes=/home/dood/libpcap}
root @lord]# make root @lord]# make install
```

Snort теперь установлен на вашем компьютере. Теперь нужно создать директорию, в которой Snort будет хранить файлы регистрации:

```
root @lord]#mkdir /var/log/snort
```

И чтобы подтвердить где установлена программа нужно выполнить:

```
root @lord]# whereis snort
```

Архитектура Snort состоит из трех основных компонентов, которые могут быть описаны как:

1. *Дешифратор пакетов*: готовит перехваченные пакеты в форму типа данных, которые затем могут быть обработаны механизмом обнаружения. Дешифратор пакетов может регистрировать Ethernet, SLIP и PPP пакеты.

2. *Механизм Обнаружения*: анализирует и обрабатывает пакеты, поданные к нему "Дешифратором", основываясь на правилах Snort. Сменные модули могут быть включены в механизм обнаружения, чтобы увеличить функциональные возможности Snort.

3. *Logger/Alerter*: Регистратор позволяет вам регистрировать информацию, собранную дешифратором пакетов в удобочитаемом формате. По умолчанию файлы регистрации сохранены в каталоге :/var/log/Snort.

Механизм предупреждения посылает предупреждения к syslog, файлу, Unix sockets или базе данных. По умолчанию, все предупреждения сохранены в файле: /var/log/Snort/alerts.

1. Изучение программы и его режимы

В этом разделе мы обсудим концепции и команды SNORT в подробностях. Начнем с простой команды, которая отображает все ключи программы:

```
root@lord snort -?
```

Команда выдаст следующее:

```
-*> Snort! <*-
Version 1.7
By Martin Roesch (roesch@clark.net, www.snort.org)
USAGE: snort [-options]
Options:
-A Set alert mode: fast, full, or none (alert file alerts only)
'unsock' enables UNIX socket logging (experimental).
-a Display ARP packets
-b Log packets in tcpdump format (much faster!)
-c Use Rules File
-C Print out payloads with character data only (no hex)
-d Dump the Application Layer
-D Run Snort in background (daemon) mode
-e Display the second layer header info
-F Read BPF filters from file
-g Run snort gid as 'gname' user or uid after initialization
-h Home network =
-i Listen on interface
-l Log to directory
-n Exit after receiving packets
-N Turn off logging (alerts still work)
-o Change the rule testing order to Pass|Alert|Log
-O Obfuscate the logged IP addresses
-p Disable promiscuous mode sniffing
-P set explicit snaplen [sp? -ed.] of packet (default: 1514)
-q Quiet. Don't show banner and status report
```

```
-r Read and process tcpdump file
-s Log alert messages to syslog
```

Как уже говорилось, SNORT выполняется в трех различных режимах:

1. *Режим пакетного снифера :* Когда Snort работает в этом режиме, он читает и дешифрует все сетевые пакеты и формирует дамп к stdout (ваш экран). Для перевода Snort в режим сниффера используйте ключ

```
–v: root @lord]# ./snort –v
```

Обратите внимание что, в этом режиме он показывает только заголовки пакетов. Для просмотра заголовка + содержания пакета выполните:

```
root @lord]# ./snort -X
```

2. *Режим регистрации пакетов :* Этот режим записывает пакеты на диск и декодирует их в ASCII формат.

```
root @lord]# Snort -l < directory to log packets to >
```

3. *Режим обнаружения вторжения:* Сигнальные данные регистрируются механизмом обнаружения (по умолчанию файл называемый " alert" в каталоге регистрации, но можно через syslog, Winpop сообщения и т.д.) Каталог регистрации по умолчанию *-/var/log/snort* , может быть изменен, используя ключ "-l". Теперь рассмотрим типичную команду Snort для анализа пакета:

```
root @lord]# snort -v -d -e -i eth0 -h 192.168.3.0/24
```

Здесь, мы рассматриваем подсеть класса С в пределах от 192.168.3.0-192.168.3.255 (маска подсети: 255.255.255.0). Сделаем подробный разбор вышеупомянутой команды, чтобы понять, что она означает:

'*-v* ' : посылает подробный ответ на вашу консоль.

'*-d* ': формирует дамп декодированных данных прикладного уровня

'*-e* ': показывает декодированные Ethernet заголовки.

'*-i* ': определяет интерфейс, который будет проверен для анализа пакета.

'*-h* ': определяет сеть, которой нужно управлять.

В следующем примере мы заставим Snort генерировать предупреждения. Режимы предупреждения Snort состоят из трех основных групп (можно задавать свои):

a. Быстрый: записывает предупреждения в файл 'alert' в одну строку, так же как и в syslog.

b. Полный: записывает предупреждения в файл 'alert' с полным декодированным заголовком.

c. None: - не выдает предупреждения.Команда тогда изменится на следующую:

```
root @lord]# snort -v -d -e -i eth0 -h 192.168.3.0/24 -A fast
```

Чтобы посылать аварийные сообщения syslog, используйте ключ '*-s'* вместо этого.

Предупреждения появятся в */var/log/secure* или */var/log/messages*:

```
root @lord]# snort -v -d -e -i eth0 -h 192.168.3.0/24 –s
```

До сих пор все перехваченные и проанализированные пакеты показывались на вашем экране. Если вы хотите, чтобы Snort записывал их в ваш файл регистрации, вы должны использовать опцию *"-l"* и указать имя директории для записи логов (например */var/log/snort*):

```
root @lord]#snort -v -d -e -i eth0 -h 192.168.3.0/24 -A full -l /var/log/snort
```

Чтобы регистрировать пакеты в формате tcpdump и производить минимальные предупреждения, используйте ключ *-b*':

```
root @lord]#snort -b -i eth0 -A fast -h 192.168.3.0/24 -s -l /var/log/snort
```

В вышеупомянутых командах, Snort регистрирует все пакеты в вашем сегменте сети. Если вы хотите регистрировать только некоторые типы пакетов в зависимости от правил, используете ключ '*-c* '.

```
root @lord]# snort -b -i eth0 -A fast -h 192.168.5.0/24 -s -l /var/log/snort -c /snort-rule-
file.
```

Задание:

1. Установите SNORT и настройте правила.
2. Со второй ВМ используйте ping, посмотрите, как реагирует SNORT.
3. Используйте различные методы сканирования nmap (используйте -sS, -sT, -sN, -sU, -sX, -sF и посмотрите, как реагирует SNORT;
4. Со второй виртуальной машины произведите сканирование и проверьте, как работает правило.

Контрольные вопросы:

1. Что такое IDS?
2. Что такое сетевая система обнаружения вторжений?
3. Чем отличаются пассивные и активные IDS?
4. Что такое SNORT?
5. Какие задачи выполняет SNORT?
6. Как работают правила SNORT?
7. Как писать правила для SNORT?
8. Зачем писать собственные правила SNORT?
9. Зачем загружать обновление правил SNORT?
10. Как в SNORT создавать логи?

'*-i* ': определяет интерфейс, который будет проверен для анализа пакета.

'*-h* ': определяет сеть, которой нужно управлять.

В следующем примере мы заставим Snort генерировать предупреждения. Режимы предупреждения Snort состоят из трех основных групп (можно задавать свои):

a. Быстрый: записывает предупреждения в файл 'alert' в одну строку, так же как и в syslog.

b. Полный: записывает предупреждения в файл 'alert' с полным декодированным заголовком.

c. None: - не выдает предупреждения.Команда тогда изменится на следующую:

```
root @lord]# snort -v -d -e -i eth0 -h 192.168.3.0/24 -A fast
```

Чтобы посылать аварийные сообщения syslog, используйте ключ '*-s'* вместо этого.

Предупреждения появятся в */var/log/secure* или */var/log/messages*:

```
root @lord]# snort -v -d -e -i eth0 -h 192.168.3.0/24 –s
```

До сих пор все перехваченные и проанализированные пакеты показывались на вашем экране. Если вы хотите, чтобы Snort записывал их в ваш файл регистрации, вы должны использовать опцию *"-l"* и указать имя директории для записи логов (например */var/log/snort*):

```
root @lord]#snort -v -d -e -i eth0 -h 192.168.3.0/24 -A full -l /var/log/snort
```

Чтобы регистрировать пакеты в формате tcpdump и производить минимальные предупреждения, используйте ключ *-b*':

```
root @lord]#snort -b -i eth0 -A fast -h 192.168.3.0/24 -s -l /var/log/snort
```

В вышеупомянутых командах, Snort регистрирует все пакеты в вашем сегменте сети. Если вы хотите регистрировать только некоторые типы пакетов в зависимости от правил, используете ключ '*-c* '.

```
root @lord]# snort -b -i eth0 -A fast -h 192.168.5.0/24 -s -l /var/log/snort -c /snort-rule-file.
```

Задание:

1. Установите SNORT и настройте правила.
2. Со второй ВМ используйте ping, посмотрите, как реагирует SNORT.
3. Используйте различные методы сканирования nmap (используйте -sS, -sT, -sN, -sU, -sX, -sF и посмотрите, как реагирует SNORT;
4. Со второй виртуальной машины произведите сканирование и проверьте, как работает правило.

Контрольные вопросы:

1. Что такое IDS?
2. Что такое сетевая система обнаружения вторжений?
3. Чем отличаются пассивные и активные IDS?
4. Что такое SNORT?
5. Какие задачи выполняет SNORT?
6. Как работают правила SNORT?
7. Как писать правила для SNORT?
8. Зачем писать собственные правила SNORT?
9. Зачем загружать обновление правил SNORT?
10. Как в SNORT создавать логи?

Литература

1. Указ Президента Республики Узбекистан № ПФ 4947 «О стратегии дальнейшего развития Республики Узбекистан». № 6 (766). 7 февраля 2017 года.
2. Олифер В.Г., Олифер Н.А. "Безопасность компьютерных сетей" 2017 г.
3. Роджер А. Гримс "Взламываем хакера" Часть I. (Учимся у экспертов барьбе с хакерами).
4. Роджер А. Гримс "Взламываем хакера" Часть II. (Учимся у экспертов барьбе с хакерами).
5. Роджер А. Гримс "Взламываем хакера" Часть III. (Учимся у экспертов барьбе с хакерами).
6. Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. и др. Технические средства и методы защиты информации: Учебник для вузов / – М.: ООО «Издательство Машиностроение», 2009 – 508 с.
7. Нестеров С. А. Информационная безопасность и защита информации: Учеб.пособие. – СПб.: Изд-во Политехн. ун-та, 2009. – 126 с.
8. Чефранова А.О., Игнатов В.В., Уривский А.В. и др. Технология построения VPN: курс лекций: Учебное пособие.- Москва: Прометей, 2009. -180 с.
9. Шаньгин В. Ф. Защита информации в компьютерных системах и сетях - М: ДМК Пресс, 2012. - 596 с.

Интернет ресурсы

1. http://www.infotecs.ru/solutions/VPN/
2. http://hostinfo.ru/articles/501/
3. http://hamachi.ru.softonic.com/
4. ViPNet Администратор: Руководство администратора
5. ViPNet Координатор: Руководство администратора

Содержание

Формат 60x84 1/16. Печ.лист 7,75.
Заказ № 80. Тираж 15.
Отпечатано в «Редакционном издательском»
отделе при ТУИТ
г.Ташкент., ул. А.Темура, 108