Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Локтионова Оксана Геннадьевна
Должность: проректор по учебной работе
Дата подписания: 08.10.2026 18:50:45
Уникальный программный ключ:
0b817ca911e6668abb13a5d426d39e5f1c11eabbf73e943df4a4851fda56d089

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

УТВЕРЖДАЮ
Проректор по учебной работе
_____ О.Г. Локтионова
«16» 05 2024 г.

КОНФИГУРИРОВАНИЕ КОММУТАТОРОВ

Методические рекомендации по выполнению
лабораторной работы для студентов направления
подготовки 10.03.01 «Информационная безопасность»

Курск 2024

УДК 621.(076.1)

Составители: Е.М. Терещенко, В.В. Чуйкова

Рецензент

Доктор физико-математических наук, профессор кафедры Информационная безопасность *В.П. Добрица*

Конфигурирование коммутаторов: методические рекомендации по выполнению лабораторной работы / Юго-Зап. гос. ун-т; сост.: Е .М. Терещенко, В.В. Чуйкова – Курск, 2024. – 14 с.: ил. 3. – Библиогр.: с. 14.

Содержат сведения по вопросам конфигурирования коммутаторов в программном продукте Cisco GNS3. Указывается порядок выполнения лабораторной работы, правила содержание отчета.

Методические указания соответствуют требованиям программы, утвержденной учебно-методическим объединением по специальности.

Предназначены для студентов направления подготовки бакалавриата 10.03.01 Информационная безопасность.

Текст печатается в авторской редакции

Подписано в печать . Формат 60х84 1/16.
Усл.печ. л. 0,81. Уч.-изд. л. 0,74. Тираж 100 экз. Заказ. Бесплатно.
Юго-Западный государственный университет.
305040, г.Курск, ул. 50 лет Октября, 94.

1.1 Конфигурирование паролей на подключение к устройству

Пароли обеспечивают некоторый уровень защиты коммутатора, предотвращающий неавторизованное подключение к нему. Коммутаторы Catalyst стандартно имеют два уровня парольной защиты: пользовательский и привилегированный. Для обеспечения защиты устройства следует применять аутентификацию пользователя с использованием локальной базы коммутатора и шифрование паролей.

Пароль уровня пользователя предотвращает доступ неавторизованных лиц к интерфейсу командной строки (CLI) из Telnet- или консольного сеанса. Он настраивается для каждой линии подключения отдельно с помощью команд **password**, параметром которой является устанавливаемый пароль, и **login** без параметров. Команда **login** обеспечивает процесс аутентификации пользователя и является обязательной для линий подключения

IOS-коммутаторов. До тех пор, пока пароль не будет установлен или в конфигурации линии будет отсутствовать команда **login**, подключение по Telnet невозможно. Выбор той или иной линии для ее конфигурирования осуществляется с помощью команды режима глобального конфигурирования:

Switch(config)#line con 0 – для консольной линии,

Switch(config)#line vty 0 4 – для линий виртуального терминала в диапазоне номеров с 0 по 4.

ВЫПОЛНИТЬ!

1. В текущей конфигурации найти команды, устанавливающие пароли на линии **con** и **vty**.
2. Установить пароль **console** для линии **con0**.
3. Выйти из сеанса консоли с помощью команды **logout** и войти в новый сеанс, используя введенные данные аутентификации.

Пароль привилегированного режима предотвращает доступ неавторизованных лиц к соответствующему режиму, в котором могут вноситься изменения в конфигурацию коммутатора и осуществляться другие функции администрирования. Он задается с помощью команды enable secret, обеспечивающей его шифрование, устаревшая команда enable password не шифрует пароль и

оставлена для совместимости с программным обеспечением ранних версий, причем во второй команде пароль должен отличаться от устанавливаемого в первой.

ВЫПОЛНИТЬ!

4. В текущей конфигурации найти команды, устанавливающие пароль для входа в привилегированный режим.

Для того чтобы пароли не хранились в файле конфигурации в открытом виде, можно использовать встроенную службу шифрования, но учтите, что она не обеспечивает их шифрование, а призвана лишь усложнить чтение паролей с экрана. Указанная служба запускается командой: **service password-encryption.**

ВЫПОЛНИТЬ!

5. Запустить службу шифрования паролей и в текущей конфигурации найти команды, устанавливающие пароли.

Как упоминалось ранее, предпочтительнее применять аутентификацию пользователя с использованием локальной базы данных коммутатора, для чего сначала создаются записи локальной базы пользователей с помощью команды:

Switch(config)#username <имя> privilege <уровень> secret <пароль>.

Затем для каждой линии подключения к коммутатору указывается команда **login** с параметром локальной аутентификации:

Switch(config-line)#login local.

ВЫПОЛНИТЬ!

6. Создать запись в локальной базе данных аутентификации о пользователе **admin** с уровнем привилегий **0** и секретным паролем **cisco**.

7. Настроить линии **con0** и **vty0** – **vty4** на использование локальной аутентификации. Для отмены старых паролей можно использовать команду:

Switch(config-line)#no password.

8. Выйти из сеанса консоли и войти в новый сеанс, используя введенные данные аутентификации.

9. В текущей конфигурации найти команды, устанавливающие действующие на коммутаторе пароли.

10. Сохранить текущую конфигурацию.

1.2 Конфигурирование статических VLAN

Сети VLAN – это определенные внутри коммутаторов широковещательные домены, позволяющие внутри устройства второго уровня управлять широковещательными, групповыми, одноадресными рассылками, а также одноадресными рассылками с неизвестным получателем. Каждая сеть VLAN создается в локальной базе данных используемого коммутатора. Если в коммутаторе отсутствуют сведения о какой-либо VLAN-сети, то он не может передавать трафик для этой сети VLAN через свои порты. VLAN-сети создаются по номерам, при этом существует два диапазона, пригодных для использования VLAN-номеров (обычный диапазон 1 ÷ 1000 и расширенный – 1025 ÷ 4096). При создании VLAN-сети можно также назначить ей определенные атрибуты, такие как имя, тип и операционное состояние. По умолчанию на коммутаторе существуют предопределенные VLAN – их нельзя удалить или переименовать. Все физические порты устройства по умолчанию находятся в VLAN1, называемой стандартной сетью VLAN (default VLAN), поэтому ее в целях безопасности и не рекомендуют использовать. Для вывода краткой информации о VLAN служит команда:

Switch#show vlan-switch brief.

ВЫПОЛНИТЬ!

11. Вывести на экран информацию о VLAN, существующих в коммутаторе по умолчанию.

Процесс создания статических VLAN-сетей включает в себя несколько этапов. Во-первых, необходимо в режиме глобального конфигурирования (рекомендуется вместо режима конфигурирования базы данных VLAN) установить протокол VTP в прозрачный режим функционирования:

Switch#configure terminal

Switch(config)#vtp mode transparent.

ВЫПОЛНИТЬ!

12. Установить протокол VTP в прозрачный режим функционирования.

Во-вторых, создать собственно сеть VLAN и по желанию указать ее имя с помощью последовательности команд:

Switch(config)#vlan <номер> Switch(config-vlan)#name <имя> Switch(config-vlan)#end.

ВЫПОЛНИТЬ!

13. Создать две виртуальных локальных сети: с номерами 10 и 20 без имени и одну с номером 99 и именем – **Administration**.

14. Вывести на экран информацию о VLAN, существующих в коммутаторе.

В-третьих, необходимо назначить в созданные VLAN-сети физические порты коммутатора, для чего перейти в режим конфигурирования выбранного интерфейса, а затем перевести его в режим доступа и назначить его в соответствующую VLAN-сеть. Например, с помощью следующих команд порт FastEthernet 0/5 назначается в VLAN с номером 50:

Switch#configure terminal

Switch(config)#interface FastEthernet 1/5 Switch(config-if)#switchport mode access Switch(config-if)#switchport access vlan 50.

ВЫПОЛНИТЬ!

15. Назначить порт fa0/24 в VLAN с именем Administration.

Для выполнения некоторой последовательности команд одновременно для нескольких портов коммутатора можно использовать выбор диапазона портов, осуществляемый с помощью команды: **Switch(config)#interface range FastEthernet 1/5 - 8**

ВЫПОЛНИТЬ!

16. Назначить порты fa1/1 – fa0/10 в VLAN 10.

17. Назначить порты fa1/11 – fa0/20 в VLAN 20.
18. Сохранить текущую конфигурацию.
19. Вывести на экран информацию о VLAN, существующих в коммутаторе.
20. Добавить в схему сети компьютеры (VPCS) PC1–PC5, подсоединить их к соответствующим портам коммутатора, назначить им IP-адреса согласно схеме, приведенной на рисунке 1.

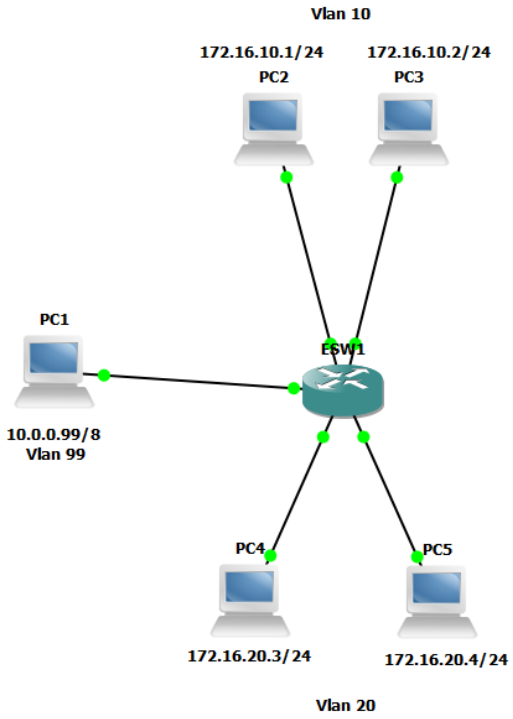

Рисунок 1 - Схема сети с VLAN99, VLAN10 и VLAN20

Состояние интерфейсов коммутатора на канальном и сетевом уровнях можно отобразить с помощью следующих команд соответственно (после параметра **interface** можно указать имя интерфейса для вывода информации только о его состоянии):

Switch#show interface
Switch#show interface switchport.
ВЫПОЛНИТЬ!

21. Используя приведенные команды, изучите параметры функционирования портов коммутатора, выясните различия в режимах работы портов, к которым подключены и не подключены компьютеры, а также портов, которые не настраивались Вами.

22. С помощью команды **ping** убедитесь, что в рамках VLANсетей взаимодействие между компьютерами возможно, а между сетями нет.

1.3 Конфигурирование IP-адреса административного управления

IP-адреса используются в коммутаторах второго уровня только в целях администрирования. Данный этап не является обязательным для функционирования коммутатора. В случае, если IP-адрес не был задан, единственным способом управления коммутатором является консольное соединение. Для конфигурирования IP-адреса используется последовательность команд:

Switch(config)#interface vlan <номер> Switch(config-if)#ip address <адрес> <маска> Switch(config-if)#exit.

ВЫПОЛНИТЬ!

23. Назначить административный IP-адрес 10.0.0.10/8 интерфейсу vlan99.

24. Сохранить текущую конфигурацию.

25. Используя команду **ping**, убедитесь, что PC0 может взаимодействовать с коммутатором.

26. Используя команду **telnet**, подключитесь с PC0 к коммутатору.

Для просмотра информации об административном интерфейсе можно использовать следующие команды:

Switch#show interface vlan <номер> Switch#show ip interface vlan <номер>.

ВЫПОЛНИТЬ!

27. Вывести информацию о настройках административного интерфейса vlan99.

Для просмотра краткой информации обо всех интерфейсах можно использовать команду:

Switch#show ip interface brief.

ВЫПОЛНИТЬ!

28. Вывести информацию об IP-интерфейсах коммутатора.

1.4 Работа с таблицей коммутации (CAM-таблица)

В таблице коммутации (switching table) содержатся MAC-адреса, номера VLAN и порты коммутатора, на которых эти адреса были определены автоматически или сконфигурированы статически. Просмотр содержимого таблицы коммутации осуществляется с помощью команд привилегированного режима:

Switch#show mac-address-table – все записи таблицы;

Switch#show mac-address-table dynamic – динамические записи;

Switch#show mac-address-table static – статических записи;

Switch#show mac-address-table interface – записи для указанного интерфейса.

ВЫПОЛНИТЬ!

29. Вывести содержимое таблицы коммутации коммутатора.
30. Выполнить команды **ping** на PC1 в адрес PC2 и на PC3 в адрес PC4.
31. Вывести содержимое таблицы коммутации коммутатора. Что изменилось?

Добавление статических записей в таблицу осуществляется с помощью команды режима глобального конфигурирования (пример приведен для MAC-адреса 11-11-22-22-33-33 в Vlan номер 99 на интерфейсе fa1/15):

Switch(config)#mac-address-table static
1111.2222.3333 vlan 99 int fa1/15.

ВЫПОЛНИТЬ!

32. Добавить статические записи о компьютерах PC2 и PC4.
33. Выполнить команды **ping** на PC2 в адрес PC3 и на PC4 в адрес PC5.
34. Вывести содержимое таблицы коммутации коммутатора.

Удаление динамических записей из таблицы коммутации осуществляется с помощью команды привилегированного режима: **Switch#clear mac-address-table dynamic,** а статических записей – с

помощью команды режима глобального конфигурирования (пример приведен для MAC-адреса 11-11-22-2233-33 в Vlan номер 99 на интерфейсе fa1/15):

Switch(config)#no mac-address-table static 1111.2222.3333 vlan 99 int fa1/15.

Очистка таблицы коммутации осуществляется с помощью команды привилегированного режима:

Switch#clear mac-address-table.

ВЫПОЛНИТЬ!

35. Удалить статическую запись о компьютере PC2 и вывести содержимое таблицы коммутации коммутатора.

36. Удалить динамические записи из таблицы коммутации и вывести содержимое таблицы коммутации коммутатора.

37. Очистить таблицу коммутации, убедиться в том, что в ней нет записей.

ВЫПОЛНИТЬ!

38. Справа от имеющейся схемы создать сеть, изображенную на рисуноке 2. Интерфейсыкоммутатора FastEthernet с номерами с 1 по 5 назначить в VLAN10, с 6 по 10 – в VLAN20 и подключить HUB1 к Fa1/1, Server0 – к Fa1/2, Server1 – к Fa1/6.

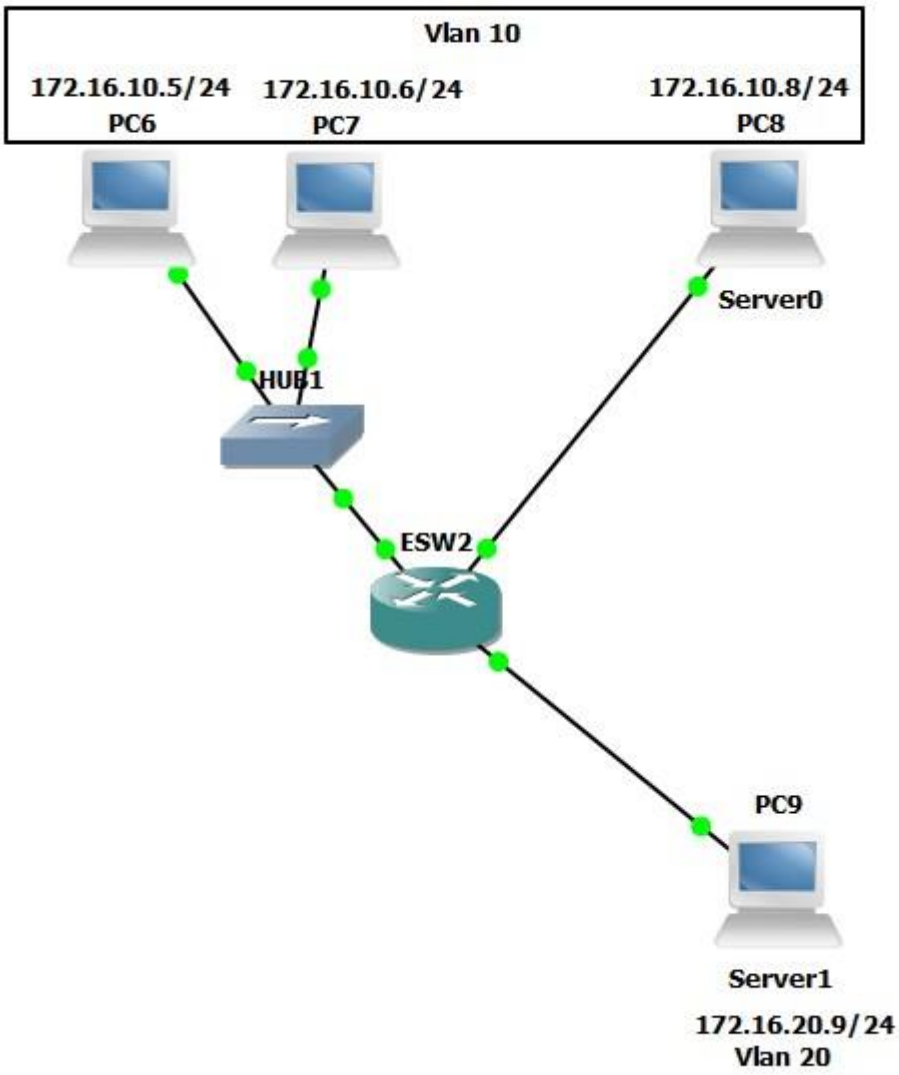

Рисунок 2 - Расширение имеющейся сети

1.6 Конфигурирование магистральных (транковых) линий

Дело в том, что VLAN-сети являются локальными в базе данных каждого коммутатора, и информация о принадлежности узлов к ним не передается между коммутаторами. Магистральные каналы (trunk links – транковые линии) обеспечивают VLAN-идентификацию для кадров, перемещающихся между коммутаторами сети. В коммутаторах фирмы Cisco имеются два механизма Ethernet-транкинга: протокол ISL и стандарт IEEE 802.1Q. Некоторые типы коммутаторов способны согласовывать параметры магистральных каналов. Магистральные каналы

стандартно транспортируют трафик от всех VLAN-сетей к коммутатору и от него, но могут быть настроены на поддержку трафика только определенной VLAN-сети.

ВЫПОЛНИТЬ!

39. Соединить ESW1 и ESW2 друг с другом, используя для этого их интерфейсы fa0/1. У Вас должна получиться схема сети, представленная на рисунке 3.

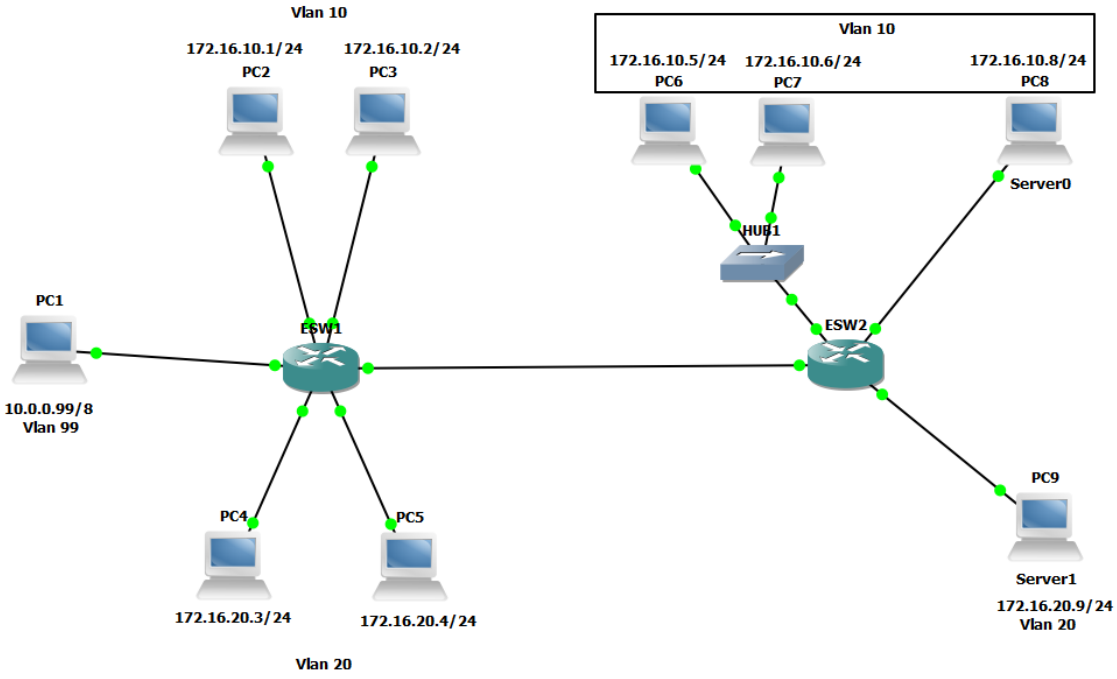

Рисунок 3 - Схема сети с магистральным каналом

ВЫПОЛНИТЬ!

40. Убедиться в том, что взаимодействие узлов, принадлежащих одной и той же VLAN-сети, невозможно, если они подключены к разным коммутаторам.

Для создания транка между коммутаторами необходимо выполнить для каждого интерфейса создаваемого канала описанную ниже последовательность действий (один из вариантов):

- перевести интерфейс в режим **trunk** с помощью команды:

Switch(config-if)#switchport mode trunk;

- указать метод инкапсуляции, используемый в канале, с помощью команды:

Switch(config-if)#switchport trunk encapsulation <negotiate|isl|dotlQ>.

Для некоторых коммутаторов стандартным методом инкапсуляции является ISL, используемый нами Catalyst-2960 поддерживает только лишь IEEE 802.1Q, поэтому данная команда в его ОС отсутствует, а при конфигурировании, например, Catalyst-3560 она необходима;

- удалить неиспользуемые VLAN-сети из магистрального канала вручную (необязательно, но рекомендуется) с помощью команды:

Switch(config-if)#switchport trunk allowed vlan remove <список>;

- в случае необходимости, добавить новые VLAN-сети в магистральный канал с помощью команды:

Switch(config-if)#switchport trunk allowed vlan add <список>.

Для отображения информации о магистральных каналах используется команда привилегированного режима: **Switch#show interfaces trunk.**

ВЫПОЛНИТЬ!

56. Вывести информацию о магистральных каналах коммутаторов.

Библиографический список

1. Защита информации в компьютерных сетях. Практический курс : учеб. пособие / А. Н. Андрончик, В. В. Богданов, Н. А. Домуховский [и др.] ; под ред. Н. И. Синадского. – Екатеринбург : УГТУ-УПИ, 2008. – 248 с.

2. Americas Headquarters Cisco Security MARS Initial Configuration and Upgrade Guide, Release 6.x. – USA : Cisco Systems, 2009. – 136 p.

3. Gary Hallen, G. Kellogg Security Monitoring with Cisco Security MARS. – USA : Cisco Press, 2007. – 335 p.

4. James Burton, Ido Dubrawsky, Vitaly Osipov Cisco Security Professional's Guide to Secure Intrusion Detection Systems. – USA : Syngress Publishing, 2003. – 673 p.

5. Installation Guide for the Cisco Secure PIX Firewall Version 5.2. [Электронный ресурс]. Режим доступа: http://www.cisco.com.

6. Install and Setup Guide for Cisco Security Monitoring Analysis and Response System. Release 4.3.x., 2008. [Электронный ресурс]. Режим доступа: http://www.cisco.com.

7. Стивенс У. Р. Протоколы TCP/IP. Практическое руководство / пер. с англ. – СПб. : БХВ-Петербург, 2003. – 672 с.

8. Кульгин М. Практика построения компьютерных сетей. Для профессионалов. – СПб. : Питер, 2001. – 320 с.

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

КОНФИГУРИРОВАНИЕ МАРШУТИЗАТОРОВ

Методические рекомендации по выполнению лабораторной работы для студентов направления подготовки 10.03.01 Информационная безопасность

Курск 2024

УДК 621.(076.1)

Составитель: Е.М. Терещенко, В.В.Чуйкова

Рецензент
Доктор физико-математических наук, профессор кафедры
Информационная безопасность *В.П. Добрица*

Конфигурирование маршрутизаторов: методические рекомендации по выполнению лабораторной работы / Юго-Зап. гос. ун-т; сост.: Е.М. Терещенко, В.В. Чуйкова – Курск, 2024. – 24 с.: ил. 12. – Библиогр.: с. 24.

Содержат сведения по вопросам конфигурирования маршрутизаторов в программном продукте Cisco GNS3. Указывается порядок выполнения лабораторной работы, правила оформления отчета.

Методические указания соответствуют требованиям программы, утвержденной учебно-методическим объединением по специальности.

Предназначены для студентов направления подготовки бакалавриата 10.03.01 Информационная безопасность.

Текст печатается в авторской редакции

Подписано в печать . Формат 60x84 1/16.
Усл.печ. л. 1,40. Уч.-изд. л. 1,26. Тираж 100 экз. Заказ. Бесплатно.
Юго-Западный государственный университет.
305040, г.Курск, ул. 50 лет Октября, 94.

1 Получение сведений о маршрутизаторе и его работе

Просмотр информации о маршрутизаторе, такой как модель, объемы памяти, версия IOS, число и тип интерфейсов, выполняется по команде (ниже приведен пример вывода команды и комментарии к нему):

Router>show version
Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-JS-M), Version 12.0(3)T3, RELEASE SOFTWARE (fc1)
Copyright (c) 1986-1999 by cisco Systems, Inc.
Compiled Thu 15-Apr-99 17:05 by kpma
Image text-base: 0x80008088, data-base: 0x80C2D514

!Версия IOS, под управлением которой работает маршрутизатор.

ROM: System Bootstrap, Version 11.3(2)XA4, RELEASE SOFTWARE (fc1)

!Сокращенная версия IOS, которая используется в качестве загрузчика (Bootstrap) и находится в ПЗУ.

Router uptime is 0 minutes
System restarted by power-on
System image file is "flash:c2600-js-mz.120-3.T3.bin" !Файл с образом IOS, из которого система была загружена.

cisco 2621 (MPC860) processor (revision 0x101) with 24576K/8192K bytes of memory

!Модель маршрутизатора.

!Объем оперативной памяти – он выводится в виде двух чисел: объема процессорной памяти (24576 K) и памяти ввода-вывода (8192 K). Общий размер RAM равен их сумме.

Processor board ID JAB0402040J (2308906173)
M860 processor: part number 0, mask 49 Bridging software.
X.25 software, Version 3.0.0.
SuperLAT software copyright 1990 by Meridian Technology Corp).
TN3270 Emulation software.
Basic Rate ISDN software, Version 1.1.

2 FastEthernet/IEEE 802.3 interface(s)

2 Serial network interface(s)

32K bytes of non-volatile configuration memory. !Объем NVRAM.

8192K bytes of processor board System flash (Read/Write)

!Объем флэш-памяти.

Configuration register is 0x2102

!Значение конфигурационного регистра.

ВЫПОЛНИТЬ!

1. Запустить в GNS3 образ маршрутизатора серии 7200, добавив в его системный слот расширения slot0 модуль C7200-IO-2FE (два порта Fast Ethernet). Установить с ним консольное соединение.
2. Получить сведения о модели маршрутизатора, версии IOS, файле образа ОС, объеме памяти RAM, NVRAM, значении конфигурационного регистра.

Просмотр содержимого флэш-памяти:

Router>show flash

System flash directory:

File Length Name/status 1 6399468 c2600-dos-mz_120-4_T.bin

[6399532 bytes used, 1989076 available, 8388608 total]

8192K bytes of processor board System flash (Read/Write.

Мониторинг загрузки процессора (рисунок 1):

Router>show processes.

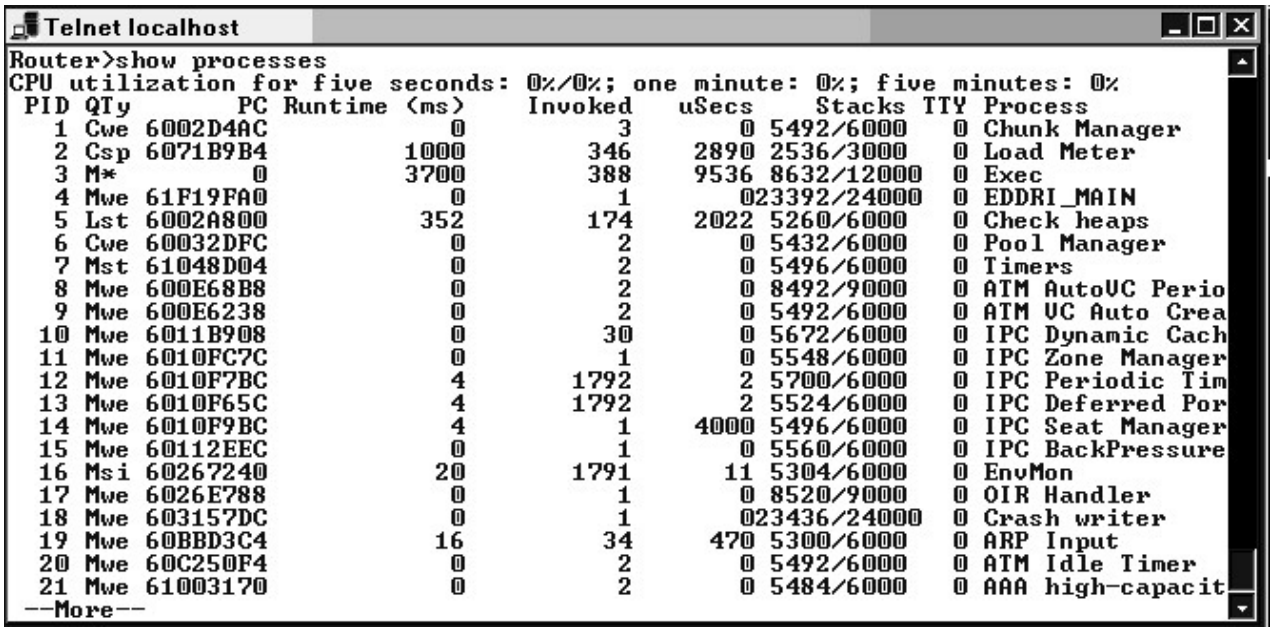

Рисунок 1 - Просмотр информации о процессах

Router>show processes cpu.

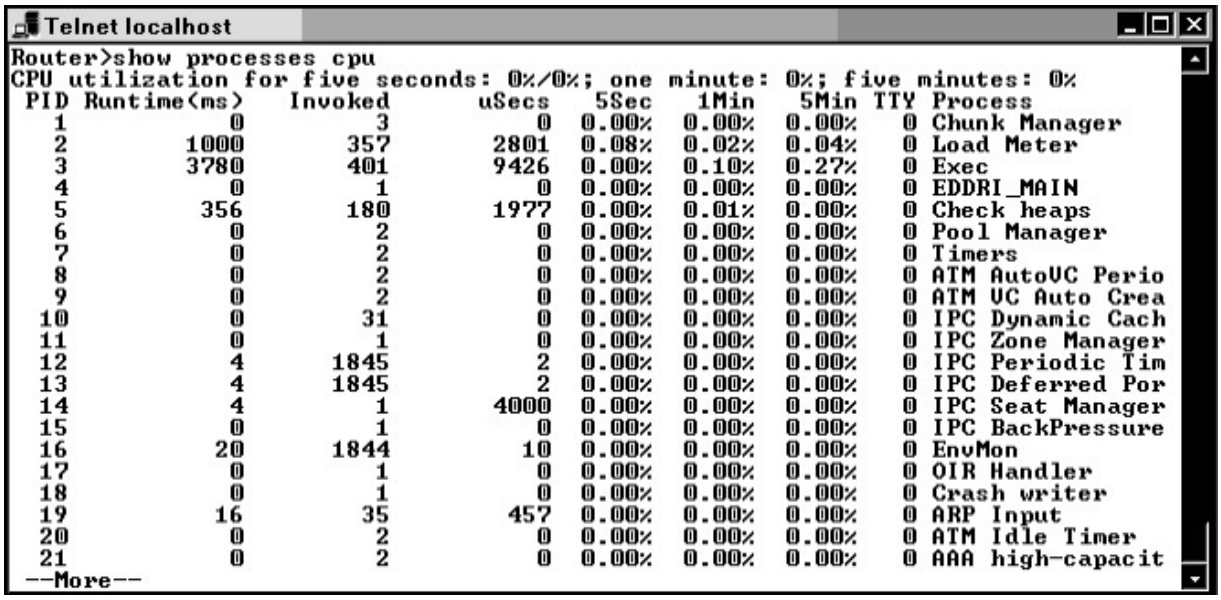

Рисунок 2 - Просмотр информации об использовании процессора

Router>show processes memory.

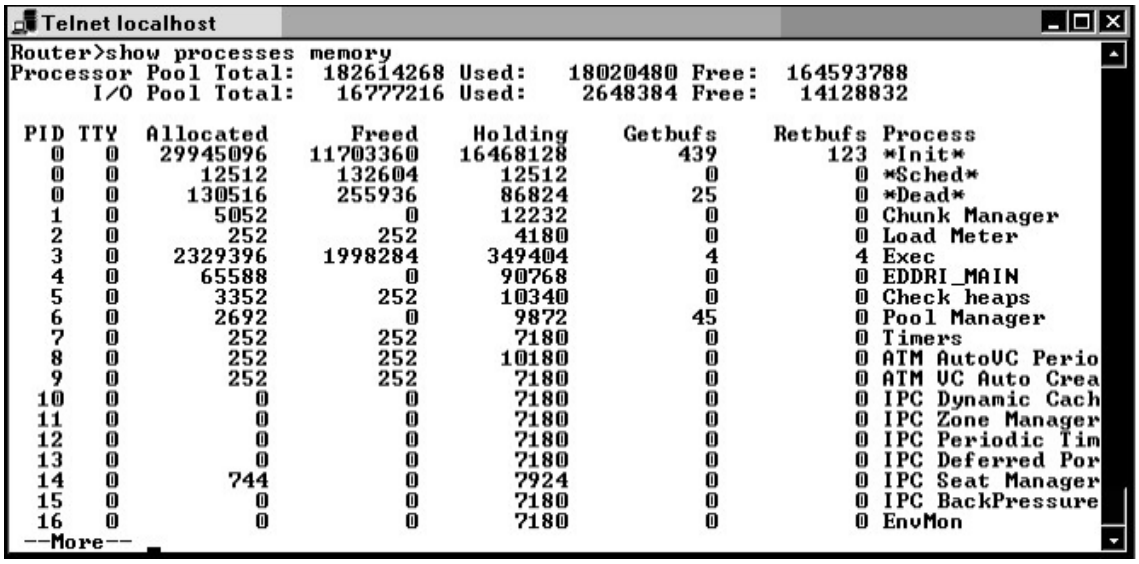

Рисунок 3 - Просмотр информации об использовании памяти

Второй вариант команды (рисунок 2) выводит более подробную информацию о загрузке процессора (показывает общую усредненную загрузку по каждому процессу за последние 5 секунд, 1 и 5 минут), а третий – о загрузке процессами оперативной памяти (рисунок 3).

Мониторинг общей загрузки памяти (рисунок 4):

Router>show memory.

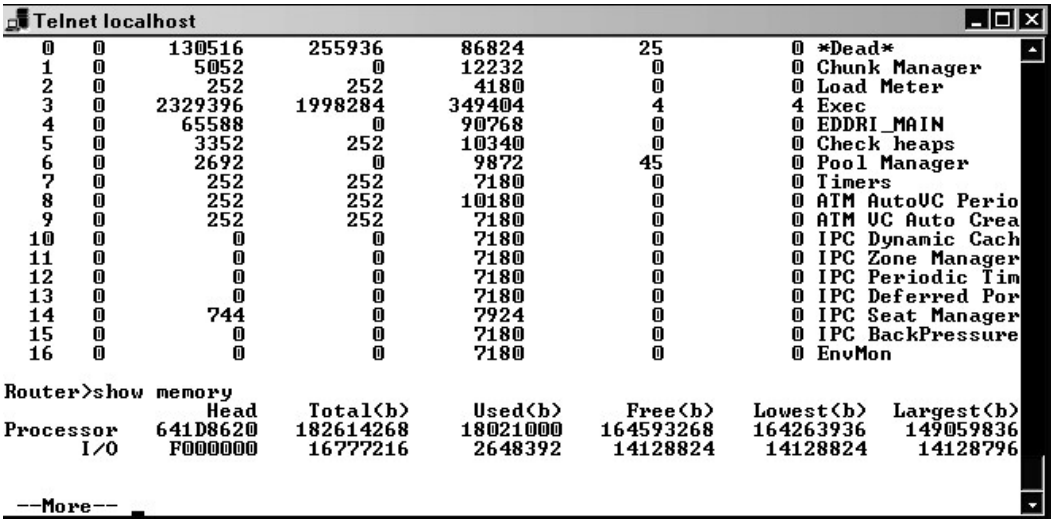

Рисунок 4 - Мониторинг общей загрузки памяти

Для каждого пула памяти (процессорного и ввода-вывода) указываются в байтах его объем (Total), объем памяти, используемой в настоящий момент (Used), объем свободной (Free),

а также наименьший объем памяти, когда-либо доступный для выделения из данного пула (Lowest), и размер наибольшего непрерывного блока, доступного для выделения в настоящий момент (Largest).

ВЫПОЛНИТЬ!

3. Получить сведения о используемых процессах, загрузке процессора и памяти.

2 Начальная конфигурация маршрутизатора

В данном пункте приведен набор команд первоначальной конфигурации маршрутизатора (рисунок 5). Для начала необходимо установить имя маршрутизатора, перейдя из пользовательского режима в режим администратора, открываемый командой **enable**, а затем в глобальный режим конфигурирования:

Router(config)#hostname <имя_маршрутизатора>.

Установить пароль администратора (пароль будет требоваться для выполнения команды **enable**):

lab1(config)#enable secret <enable>.

Отключить обращения в DNS (в том случае, если DNS-сервер не используется): **lab1(config)#no ip domain-lookup.**

Рисунок 5 – Начальная настройка маршрутизатора

Сконфигурировать консоль и виртуальные терминалы: отключить таймер неактивности и интерпретацию неизвестных команд как указаний открыть сеанс Telnet, включить режим синхронной регистрации:

lab1(config)#line con 0 lab1(config-line)#exec-timeout 0 0 lab1(config-line)#transport preferred none lab1(config-line)#logging synchronous.

Обратите внимание, что по умолчанию маршрутизатор выводит сообщения на консоль поверх ввода оператора, и чтобы продолжить ввод команды, оператор должен помнить, в каком

месте его прервали. При использовании команды **logging synchronous** после каждого выведенного сообщения маршрутизатор будет заново выводить часть команды, уже введенной оператором к моменту появления сообщения, и оператор может легко продолжить ввод.

Виртуальный терминал назначается оператору, подключившемуся к маршрутизатору по протоколу Telnet. На доступ через виртуальный терминал следует назначить пароль. Это делается командами:

lab1(config-line)#line vty 0 4 lab1(config-line)#login lab1(config-line)#password <password>.

Из соображений безопасности, если маршрутизатор напрямую подключен к публичным сетям, например Интернет, виртуальные терминалы рекомендуется заблокировать, а доступ к маршрутизатору осуществлять только по консольной линии.

ВЫПОЛНИТЬ!

4. Установить имя маршрутизатора и пароль на вход в привилегированный режим (lab1, enable).
5. Отключить обращения в DNS, таймер неактивности и интерпретацию неизвестных команд.
6. Включить режим синхронной регистрации.
7. Назначить пароль на доступ к маршрутизатору через виртуальный терминал (password).

3 Настройка интерфейсов

Для перехода в режим настройки необходимого интерфейса следует, находясь в глобальном режиме, выполнить команду: **lab1(config)#interface <имя_интерфейса>.**

По умолчанию все интерфейсы маршрутизатора выключены.

Интерфейс включается командой:

lab1(config-if)#no shutdown.

Работоспособность настроек физического и канального уровней можно проверить командой в контексте администратора: **lab1#show interface <имя_интерфейса>.**

Сообщения об изменении состояния физического и канального уровней любого интерфейса выводятся

маршрутизатором на консоль. Команда **show interface** также выводит сведения об используемом протоколе канального уровня, IP-адресе и статистику отправленных и полученных данных и ошибок.

Настройка IP-адреса интерфейса (рисунок 6) производится командой: **lab1(config-if)#ip address <адрес> <маска>.**

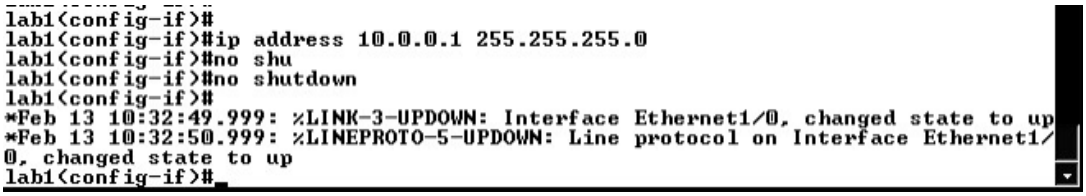

Рисунок 6 - Настройка IP-адреса интерфейса

Подробная информация о параметрах протокола IP (рисунок 7) доступна в контексте администратора по команде: **lab1#show ip interface <имя_интерфейса>.**

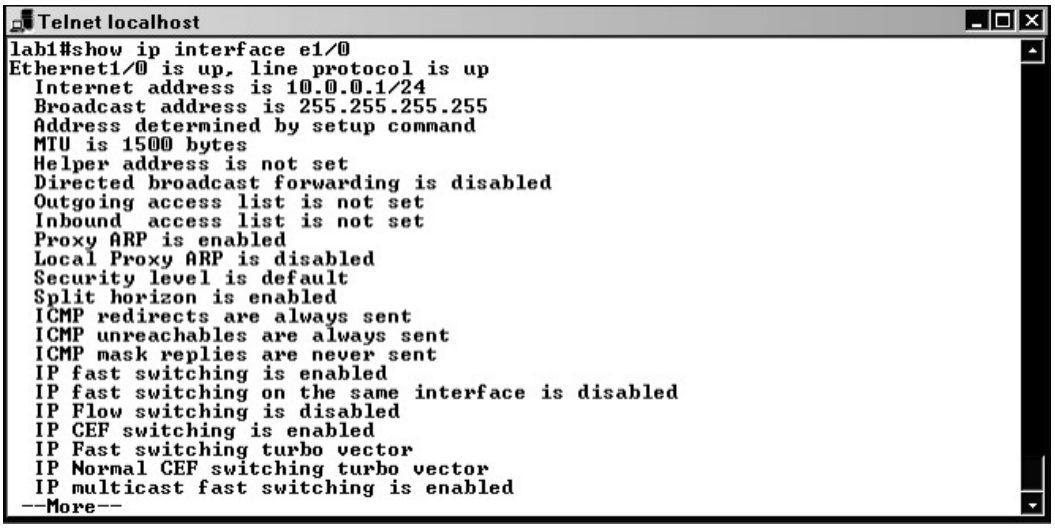

Рисунок 7 - Подробная информация о параметрах протокола IP

Краткая сводная таблица состояний IP-интерфейсов (рисунок 8):

lab1#show ip interface brief.

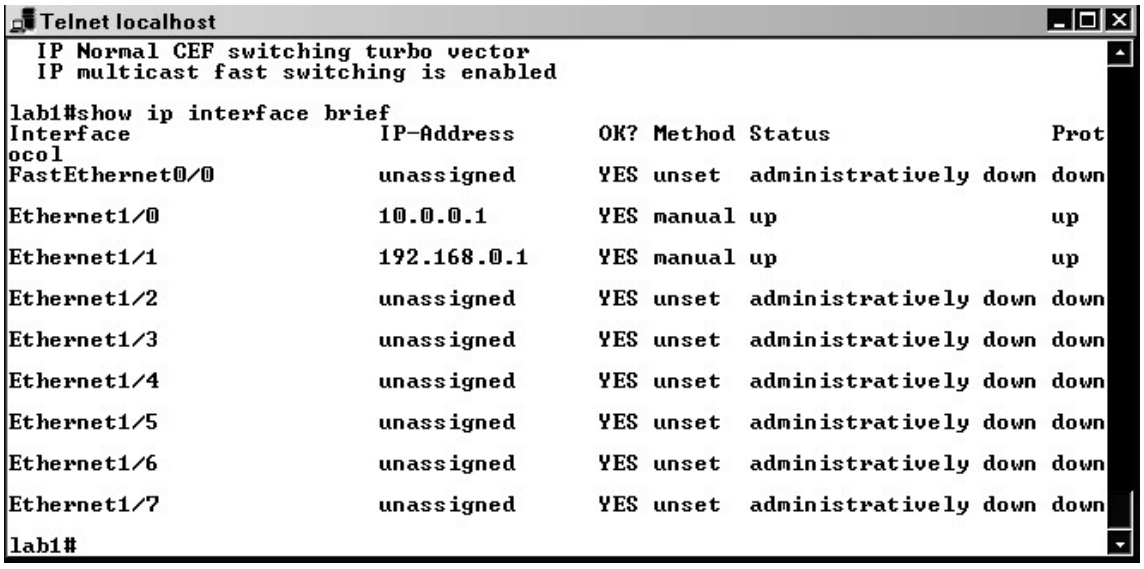

Рисунок 8 - Краткая сводная таблица состояний IP-интерфейсов

ВЫПОЛНИТЬ!

8. Произвести настройку интерфейсов FastEthernet 0/0 и FastEthernet 0/1 (192.168.0.1 и 10.0.0.1 со стандартными масками соответственно).

9. Изучить информацию о состоянии интерфейсов.

4 Назначение статических маршрутов

Маршруты, ведущие в сети, к которым маршрутизатор подключен непосредственно, автоматически добавляются в маршрутную таблицу после конфигурирования интерфейса при условии, что интерфейс работоспособен (line protocol up).

Для назначения дополнительных статических маршрутов в контексте глобальной конфигурации вводится команда (одна строка):

router(config)#ip route <IP-адрес> <маска> <интерфейс> <IP_адрес_следующего_маршрутизатора>.

Маршрут активен только тогда, когда следующий маршрутизатор достижим, то есть существует маршрут в сеть, где находится следующий маршрутизатор. Напротив, статический маршрут будет неактивен, если следующий маршрутизатор не достижим по разным причинам, например, когда его интерфейс находится в нерабочем состоянии.

Управление таблицей маршрутизации на маршрутизаторах в большой распределенной сети является сложной задачей. Поэтому часто используют специальные протоколы маршрутизации. Маршрут по умолчанию назначается командой:

router(config)#ip route 0.0.0.0 0.0.0.0 <интерфейс> <IP_адрес_следующего_маршрутизатора>.

Просмотреть таблицу маршрутов (рисунок 9) можно в контексте администратора по команде: **router#show ip route.**

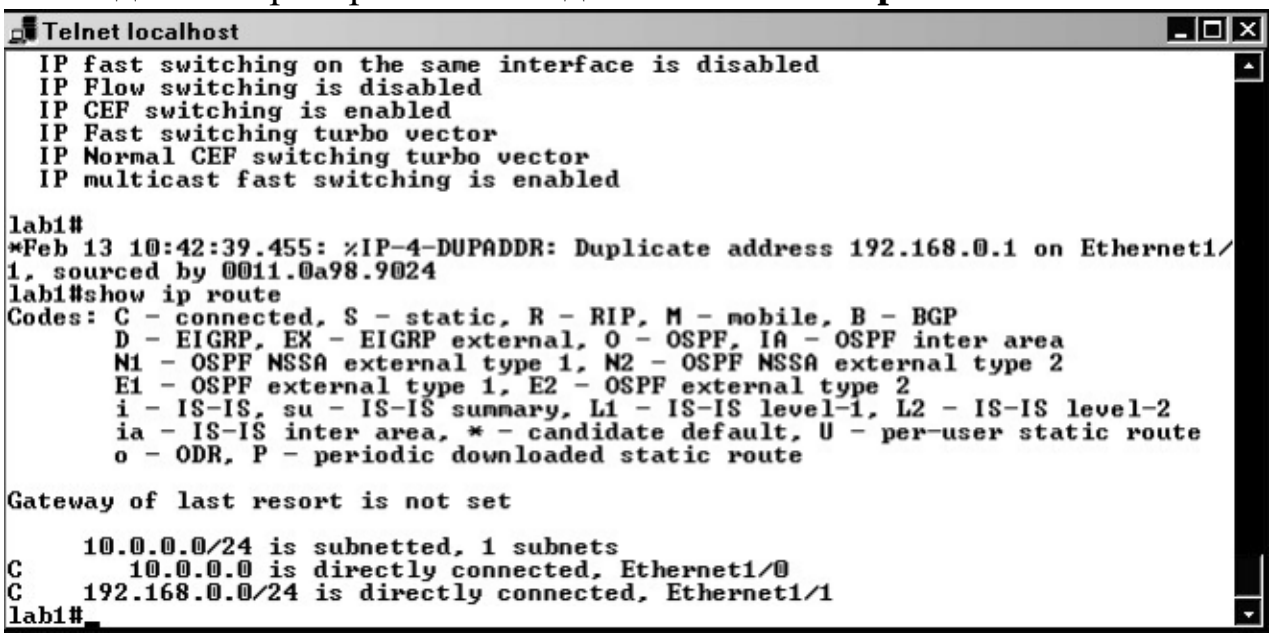

Рисунок 9 - Просмотр таблицы маршрутов

ВЫПОЛНИТЬ!

10. Добавить в схему сети такой же маршрутизатор. Соединить маршрутизаторы с использованием интерфейсов FastEthernet 0/1. Дать новому маршрутизатору имя lab2.

11. Произвести настройку интерфейсов FastEthernet 0/0 и FastEthernet 0/1 маршрутизатора lab2 (192.168.100.1 и 10.0.0.2 со стандартными масками соответственно) – в итоге должна получиться схема сети, изображенная на рисунке 10.

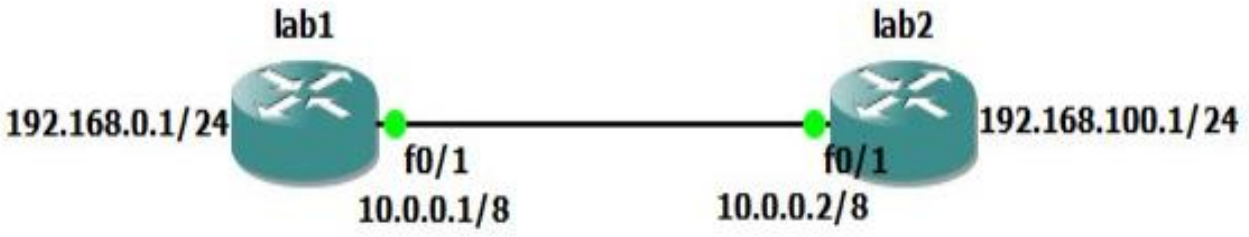

Рисунок 10 - Схема сети с двумя маршрутизаторами

ВЫПОЛНИТЬ!

12. На маршрутизаторе lab2 назначить статический маршрут к сети 192.168.0.0/24. Проверить достижимость 192.168.0.1.
13. Назначить для интерфейса FastEthernet 0/1 маршрутизатора lab1 маршрут по умолчанию. Проверить достижимость 192.168.100.1.
14. Изучить таблицу маршрутов на обоих маршрутизаторах.

5 Настройка точного времени

Часы маршрутизатора сбрасываются при перезагрузке или отключении питания. Старшие модели маршрутизаторов (7xxx и выше) оборудованы аппаратными часами (calendar), по которым программные часы устанавливаются после загрузки маршрутизатора [10]. В дальнейшем, говоря о часах, мы имеем ввиду только программные часы (clock) – именно их показания используются операционной системой, когда, например, ставятся метки времени в диагностических сообщениях.

Поскольку точное время исчисляется по Гринвичу, то предварительно следует установить часовой пояс (относительно Гринвича) и параметры перехода на летнее время (в случае необходимости): **lab1(config)#clock timezone <name> <offset> lab1(config)#clock summer-time <name> recurring.**

Текущее время на маршрутизаторе можно установить и отобразить с помощью следующих команд соответственно:

lab1#clock set <time> <day> <month> <year> и **lab1#show clock.**

ВЫПОЛНИТЬ

15. Произвести настройку текущего времени на маршрутизаторах lab1 и lab2.

В ряде случаев текущее время на маршрутизаторах необходимо синхронизировать с сервером точного времени, для этого используется протокол NTP.

Маршрутизаторы младших моделей (серии 800, 1700) поддерживают также упрощенную версию этого протокола – SNTP. Естественно, чтобы синхронизация была возможной, необходимо наличие связи с NTP-сервером.

В крупных корпоративных сетях обычно устанавливается собственный сервер точного времени, который синхронизируется от публичных серверов, расположенных в Интернете (списки таких серверов, а также программное обеспечение можно найти на сайте www.ntp.org), в иных случаях можно воспользоваться публичными NTP-серверами напрямую.

Серверы, подключенные непосредственно к источникам точного времени (атомным часам и т. п.), имеют статус stratum 1. Серверы, синхронизирующиеся от этих серверов, имеют статус stratum 2 и т. д. Отсутствие синхронизации обозначается в Cisco как stratum 16.

Маршрутизатор с синхронизированными часами может и сам выступать в роли NTP-сервера: **lab1(config)#ntp master <stratum>.**

Для синхронизации времени с сервером NTP на клиенте используется следующая команда (может быть задан один или несколько серверов): **lab1(config)#ntp server <IP-адрес_NTP_сервера>.**

Обратите внимание, что после настройки NTP, в конфигурационном файле появится команда **ntp clock-period**, содержащая информацию о неточности хода часов, которая обновляется маршрутизатором автоматически и редактировать ее не рекомендуется.

16.Для выполнения следующих упражнений Вам необходимо удалить линк между маршрутизаторами и подключить к ним два облака (Cloud), настроенные на loopback интерфейс вашего

компьютера. Loopback интерфейсу необходимо присвоить ip 10.0.0.5/8. Схема полученной сети представлена на рисунке 11.

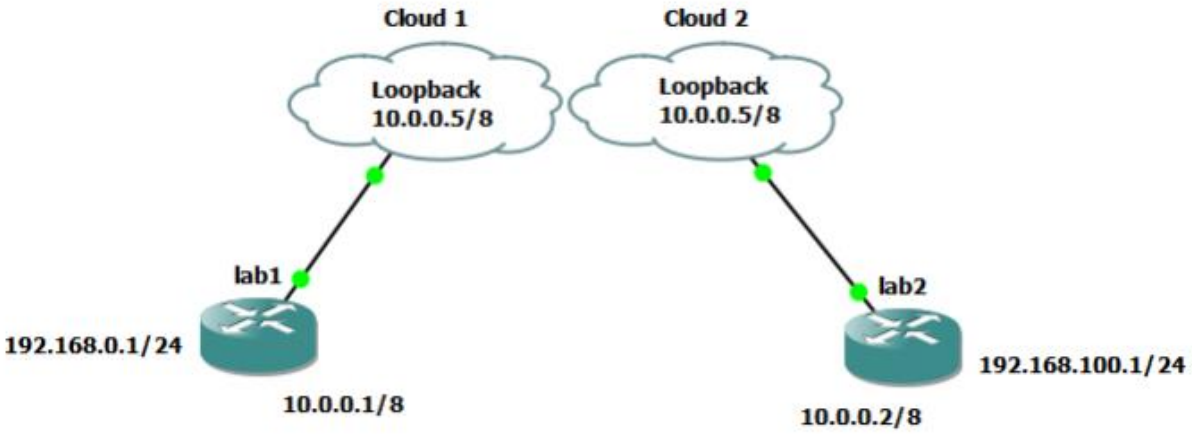

Рисунок 11 - «Улучшенная» схема сети с двумя маршрутизаторами

17. Произвести настройку сервера времени на маршрутизаторе lab1.

18. Настроить на маршрутизаторе lab2 синхронизацию времени с сервером.

Отобразить текущее состояние синхронизации по протоколу NTP можно с помощью команды: **lab1#show ntp status**

Clock is synchronized, stratum 3, reference is 217.107.53.5 ... (первая строка вывода говорит об успешной синхронизации), а параметры взаимодействия и ассоциации с NTP-серверами выводятся по команде:

lab1#show ntp associations или **lab1#show ntp associations detail.**

19.Захватить сетевой трафик, изучить процесс взаимодействия маршрутизаторов по протоколу NTP.

20. Проанализировать информацию о статусе и ассоциациях NTP на маршрутизаторах lab1 и lab2, сравнить результаты для lab1 и lab2.

Кроме клиент-серверных отношений протокол NTP предусматривает равноправные отношения (symmetric active mode), когда участники процесса учитывают показания часов друг друга и выполняют взаимную синхронизацию, соответствующая конфигурация определяется командой: **lab1(config)#ntp peer <IP-адрес_участника>.**

ВЫПОЛНИТЬ!

21. Настроить взаимную синхронизацию времени по протоколу NTP между lab1 и lab2 (не забудьте предварительно удалить предыдущие настройки NTP).

22. Захватить сетевой трафик, изучить процесс взаимодействия маршрутизаторов по протоколу NTP.

23. Проанализировать информацию о статусе и ассоциациях NTP на маршрутизаторах lab1 и lab2, сравнить результаты lab1 и lab2.

6 Конфигурирование протоколов управления оборудованием

При выполнении заданий данного параграфа используйте схему сети, изображенную на рисунке 11.

7 Сохранение и загрузка файлов конфигурации с использованием протоколов tftp и ftp

ВЫПОЛНИТЬ!

1. Запустить программу 3CDaemon, перейти на вкладку tftp сервера. Запустить захват трафика. В привилегированном режиме на маршрутизаторе lab1 выполнить команду **copy run tftp://10.0.0.5/router-lab1.cfg**. Подтвердить запросы маршрутизатора и дождаться окончания копирования.

2. В окне анализатора трафика найти пакеты, принадлежащие протоколу tftp. Какой транспортный протокол использует tftp? Каким образом передаются команды и содержимое файла?

3. Перейти в рабочий каталог tftp-сервера 3CDaemon (Посмотреть его расположение или изменить можно во вкладке

Configure TFTP Server). Найти только что скопированный файл и открыть его любым текстовым редактором. Этот файл содержит текущую конфигурацию устройства. Найти в файле параметры, установленные Вами в ходе лабораторной работы.

4. На маршрутизаторе lab1 удалить файл стартовой конфигурации (команда **erase startup-config**).

5. Загрузить сохраненный на сервере файл **router-lab1.cfg** в качестве файла стартовой конфигурации (команда **copy tftp: startup-config**).

6. Выполнить пункты 1 ÷ 5 для маршрутизатора lab2, используя протокол ftp. Для возможности сохранения файла конфигурации по протоколу ftp необходимо создать соответствующую учетную запись на сервере (рисунок 12). ***2.3.2. Доступ к маршрутизатору по протоколам Telnet и SSH***

ВЫПОЛНИТЬ!

7. На маршрутизаторах lab1 и lab2 создать учетную запись пользователя с именем **cisco**, паролем **secret** и уровнем привилегий **0**.

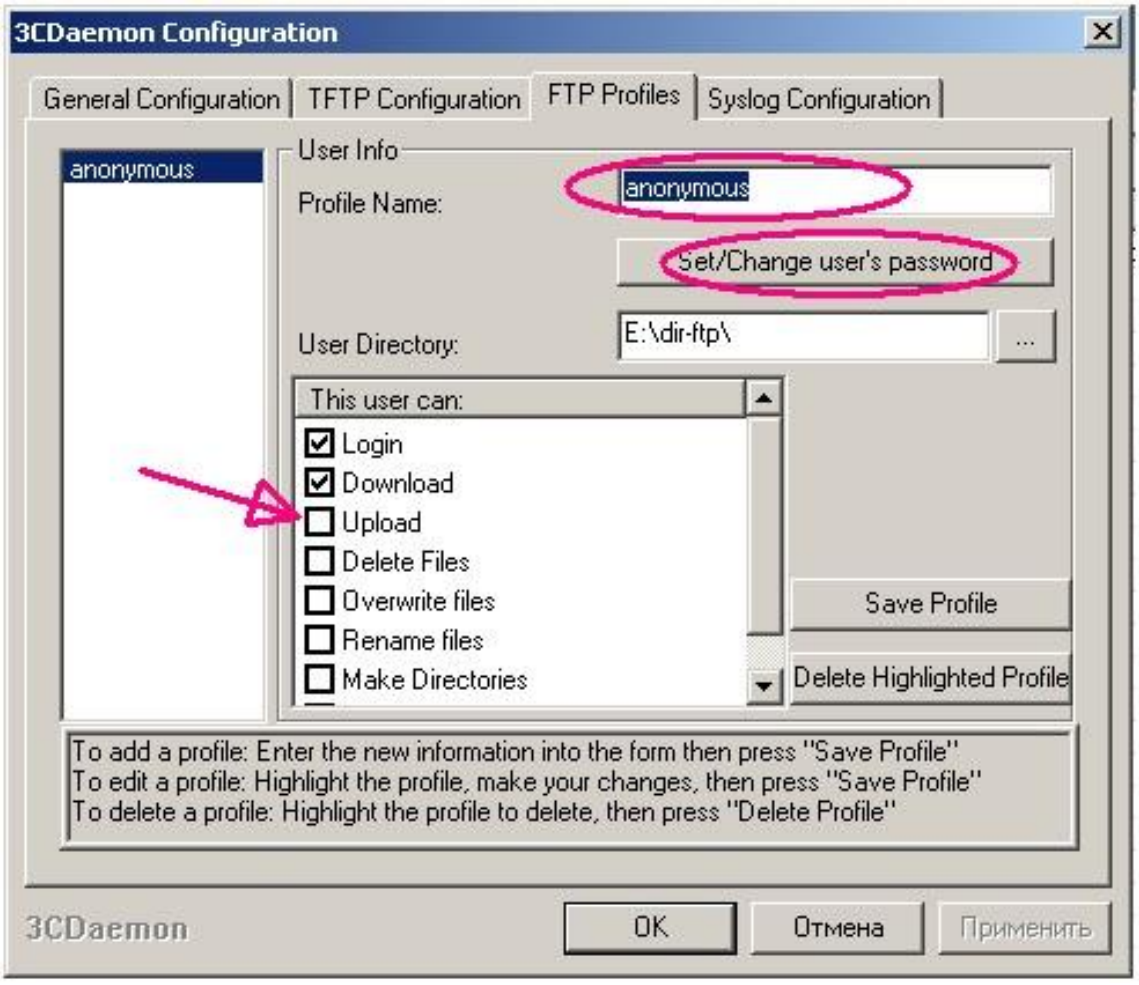

Рисунок 12 - Создание учетной записи на сервере FTP

8. На маршрутизаторах lab1 и lab2 установить пароль **enable** для входа в привилегированный режим.

9. На маршрутизаторах lab1 и lab2 сконфигурировать линии виртуальных терминалов vty0 ÷ vty4 на аутентификацию с использованием локальной базы устройства.

10. Подключиться к маршрутизатору lab1 по протоколу Telnet. В Wireshark проанализировать трафик сессии.

11. Указать на маршрутизаторе lab2 имя домена с помощью команды **ip domain-name <имя>**, где параметр **<имя>** – это имя произвольного домена, например, lab.net.

12. Сгенерировать ключ шифрования RSA длиной более 1024 бит с помощью команды **crypto key generate rsa**. После выполнения этой команды на маршрутизаторе начинает функционировать сервер SSH.

13. Подключиться к маршрутизатору lab2 по протоколу SSH, используя программу Putty (ярлык на рабочем столе).

В Wireshark проанализировать трафик сессии.

14. Установить для линий виртуальных терминалов маршрутизатора lab2 возможность подключения только с использованием протокола SSH, выполнив команду **transport input ssh**. Убедитесь, что подключение пользователя по протоколу Telnet сбрасывается маршрутизатором.

15. Отобразить и проанализировать с помощью команд **show ssh** и **show ip ssh** информацию о сессиях по протоколу SSH и настройках сервера SSH по умолчанию. ***2.3.3. Доступ к маршрутизатору по протоколу HTTP и HTTPS***

ВЫПОЛНИТЬ!

16. На маршрутизаторе lab1 сконфигурировать доступ по протоколу HTTP на аутентификацию с использованием локальной базы устройства с помощью команды **ip http authentication local**.

17. Проверить в текущей конфигурации маршрутизатора запущен ли HTTP-сервер (команда **ip http server**) и в случае необходимости запустить его. Подключиться к маршрутизатору по web-интерфейсу. В Wireshark проанализировать трафик сессии. Изучить возможности web-доступа по конфигурированию устройства.

18. Остановить на маршрутизаторе HTTP-сервер и запустить HTTPS-сервер (команда **ip http secure-server**). Подключиться к маршрутизатору по web-интерфейсу.

В Wireshark проанализировать трафик сессии.

8 Регистрация событий

Диагностические сообщения о системных событиях выводятся маршрутизатором по умолчанию только на консольную линию. Для того чтобы эти сообщения дублировались в виртуальные терминалы (то есть в telnet-соединения), в контексте администратора в соответствующем сеансе используется команда **lab1#terminal monitor.**

При конфигурировании линий виртуальных терминалов для этой цели выполняется команда **monitor**. Вывод сообщений можно направить также во внутренний буфер устройства или на syslogсервер. Направление в буфер: **lab1(config)#logging buffered <размер>.**

Буфер организован в виде очереди указанного размера (в байтах), самые старые сообщения удаляются из него при поступлении новых. Размер буфера по умолчанию – 4096 байт. Просмотр буфера (и параметров процесса регистрации событий): **lab1#show logging.**

Очистка буфера производится командой **lab1#clear logging.**

Пример отправки сообщений на syslog-сервер:

lab1(config)#logging <IP-адрес сервера> lab1(config)#logging facility local7 lab1(config)#logging trap debugging.

Последние две команды определяют источник сообщений (facility в терминах syslog, используется для определения способа обработки сообщений на сервере) и степень важности (debugging – минимальная) сообщений, протоколируемых в системном журнале.

По умолчанию диагностические сообщения имеют метки времени, которые отсчитываются с момента загрузки устройства (system uptime), поэтому для того чтобы время выводилось в обычном формате (дата, время суток), в конфигурации необходимо указать:

lab1(config)#service timestamps log datetime localtime
lab1(config)#service timestamps debug datetime locatime.

ВЫПОЛНИТЬ!

19. Реализовать вывод диагностических сообщений в виртуальный терминал.
20. Запустить syslog-сервер 3CDaemon.
21. Сконфигурировать маршрутизаторы lab1 и lab2 для отправки на сервер сообщений о **всех** системных событиях, указав различные источники для идентификации маршрутизаторов, например, для lab1 – local1, а для lab2 – local2.
22. Запустить захват сетевого трафика. На маршрутизаторах перейти в режим конфигурации интерфейса FastEthernet0/1, выключить его, а затем через некоторое время снова включить. Какие сообщения получил syslog сервер?

23. Сравнить диагностические сообщения, выводимые в виртуальном терминале и на syslog-сервере.

24. В анализаторе сетевого трафика найти пакеты, относящиеся к протоколу syslog. Какой транспортный протокол используется для их передачи? Какая информация содержится в этих пакетах? Какие механизмы позволяют отследить отправителя пакета, и насколько они надежны?

9 Протокол обнаружения соседних устройств CDP

Протокол CDP используется устройствами Cisco по умолчанию, поэтому в целях безопасности для запрета его функционирования на маршрутизаторе в целом в режиме глобальной конфигурации необходимо ввести команду **no cdp run**. Для использования протокола на конкретных интерфейсах устройства применяется команда **cdp enable** врежиме конфигурирования интерфейса. Параметры функционирования CDP отображаются командой **show cdp** в режиме глобального конфигурирования.

ВЫПОЛНИТЬ!

25. Убедиться, что команда **no cdp run** отсутствует в текущей конфигурации устройства (**show runningconfig**). Запросить у маршрутизатора lab1 информацию о его соседях: **show cdp neighbors**. Какие устройства и каким образом соединены с маршрутизатором? Какую опасность может представлять протокол CDP?

26. Отобразить и проанализировать параметры функционирования протокола CDP по умолчанию.

27. Выполнить команду **show cdp detail**. Какая информация из выведенного перечня была бы полезна для потенциального злоумышленника? Найти в выведенных параметрах IP-адреса соседних устройств.

28. На узле XP_VMnet2 захватить CDP-пакеты, передающиеся через его интерфейс локальной сети. Какой

транспорт используется протоколом CDP? С какой периодичностью передаются сообщения протокола?

10 Использование маршрутизатора в качестве DHCP-сервера

ВЫПОЛНИТЬ!

30. Для запуска на маршрутизаторе сервера DHCP необходимо перейти в режим глобальной конфигурации и включить его командой **service dhcp** (прекращение функционирования сервера производится, соответственно, командой **no service dhcp**). Запустить DHCP-сервер на маршрутизаторе lab1.

31. Создать пул с именем POOL10, из которого будет производиться раздача параметров функционирования клиентов. Для создания пула необходимо в режиме глобальной конфигурации ввести команду **ip dhcp pool <имя>**, где параметр <имя> – название пула, который используется при дальнейшей настройке. После выполнения команды устанавливается режим конфигурирования пула DHCP.

32. Указать сеть, из которой необходимо выдавать адреса, командой **network <сеть> <маска сети>** (используйте 10.0.0.0 255.0.0.0).

33. Указать шлюз по умолчанию для клиентов DHCP:

default-router <IP-адрес> (используйте адрес lab2).

34. Выйти из контекста конфигурации пула. Для настройки исключений DHCP в контексте глобального конфигурирования ввести команду

ip dhcp excluded-address <IP-low> <IP-high>, где IP-low – начальный адрес запрещенного диапазона, а IP-high – его конечный адрес. Данная команда для одной подсети может быть введена несколько раз. Настроить исключения таким образом, чтобы сервер выдавал клиентам адреса с 40 по 90 включительно, кроме адресов 60 ÷ 70 (последний байт адреса).

35. Запустить анализатор Wireshark. На узле XP_VMnet2 в настройках сетевого адаптера указать автоматическое получение IP-адреса. С помощью утилиты **ipconfig** определить, какие настройки получил клиент. Какой срок аренды IP-адреса

устанавливает сервер? В какой момент времени клиент отправит запрос на продление аренды адреса, если подключение к сети будет оставаться активным?

36. Проанализировать сессию захвата трафика. Найти все пакеты, относящиеся к протоколу DHCP. Какие типы DHCP-сообщений были использованы, какие значения установлены в полях адресов отправителя и получателя в кадре Ethernet и пакете IP? Какой транспортный протокол используется для передачи сообщений и какой идентификатор в нем указывает на сообщения протокола DHCP? Какая информация содержится непосредственно в DHCP-пакете?

37. На узле XP_VMnet2 с помощью команды **ipconfig** принудительно обновить адрес. В Wireshark определить, какие типы пакетов были использованы клиентом при обновлении параметров? Какие поля DHCP-пакетов заполнены и какие значения они имеют? Какой адрес получил узел XP_VMnet2 после обновления адреса?

38. С помощью команды **ipconfig** принудительно освободить адрес. В анализаторе трафика определить, какие типы пакетов были использованы при отказе от адреса. Какие поля DHCP-пакетов заполнены и какие значения они имеют?

39. Отключить сетевой адаптер и снова включить его. Какой IP-адрес получил узел XP_VMnet2?

40. На маршрутизаторе lab1 в привилегированном режиме просмотреть список адресов, выданных из пула в аренду (команда **show ip dhcp binding**). Какую информацию

об арендаторах хранит маршрутизатор? Посмотреть статистику работы сервера (команда **show ip dhcp server statistics**) и статистику пула адресов (команда **show ip dhcp pool**). Какие из выведенных параметров Вы можете интерпретировать?

41. С помощью анализатора протоколов определить маршрут передачи пакетов при выполнении команды **ping** с узла XP_VMnet2 в адрес интерфейса FastEthernet 0/0 маршрутизатора lab1 (192.168.0.1).

Вопросы для проверки знаний

1. Какие VLAN существуют по умолчанию в коммутаторе и к каким из них принадлежат его интерфейсы?
2. Можно ли в сети с несколькими коммутаторами при конфигурировании VLAN обойтись без использования стандарта IEEE802.1Q?
3. Каково назначение функции Port Security?
4. В чем преимущество каналов EtherChannel?
5. Для чего необходим протокол STP?
6. Для чего и каким образом конфигурируются статические маршруты?
7. В каких случаях целесообразно использовать маршруты по умолчанию?
8. Каково назначение протокола CDP, в чем преимущества и недостатки его использования в сети?
9. Каковы основные возможности протокола управления сетью SNMP?
10. На основе каких протоколов можно получить удаленный доступ к командной строке IOS устройства, в чем преимущества и недостатки каждого из них?
11. Для какого количества сетей DHCP-сервер на маршрутизаторе может выдавать конфигурационные параметры клиентам?
12. В каких случаях на маршрутизаторах необходимо конфигурировать промежуточные агенты при использовании серверов DHCP?

Библиографический список

1. Защита информации в компьютерных сетях. Практический курс : учеб. пособие / А. Н. Андрончик, В. В. Богданов, Н. А. Домуховский [и др.] ; под ред. Н. И. Синадского. – Екатеринбург : УГТУ-УПИ, 2008. – 248 с.

2. Americas Headquarters Cisco Security MARS Initial Configuration and Upgrade Guide, Release 6.x. – USA : Cisco Systems, 2009. – 136 p.

3. Gary Hallen, G. Kellogg Security Monitoring with Cisco Security MARS. – USA : Cisco Press, 2007. – 335 p.

4. James Burton, Ido Dubrawsky, Vitaly Osipov Cisco Security Professional's Guide to Secure Intrusion Detection Systems. – USA : Syngress Publishing, 2003. – 673 p.

5. Installation Guide for the Cisco Secure PIX Firewall Version 5.2. [Электронный ресурс]. Режим доступа: http://www.cisco.com.

6. Install and Setup Guide for Cisco Security Monitoring Analysis and Response System. Release 4.3.x., 2008. [Электронный ресурс]. Режим доступа: http://www.cisco.com.

7. Стивенс У. Р. Протоколы TCP/IP. Практическое руководство / пер. с англ. – СПб. : БХВ-Петербург, 2003. – 672 с.

8. Кульгин М. Практика построения компьютерных сетей. Для профессионалов. – СПб. : Питер, 2001. – 320 с.

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

МЕЖСЕТЕВЫЕ ЭКРАНЫ CISCO PIX

Методические рекомендации по выполнению лабораторной работы для студентов направления подготовки 10.03.01 Информационная безопасность

Курск 2024

УДК 621.(076.1)

Составители: Е.М. Терещенко, В.В. Чуйкова

Рецензент

Доктор физико-математических наук, профессор кафедры Информационная безопасность» *В.П. Добрица*

Межсетевые экраны Cisco PIX: методические рекомендации по выполнению лабораторной работы / Юго-Зап. гос. ун-т; сост.: Е.М. Терещенко, В.В. Чуйкова. – Курск, 2024. – 17 с.: ил. 6. – Библиогр.: с. 17.

Содержат сведения по вопросам конфигурирования в программной среде Cisco GNS3. Указывается порядок выполнения лабораторной работы, правила оформления и содержание отчета.

Методические указания соответствуют требованиям программы, утвержденной учебно-методическим объединением по специальности.

Предназначены для студентов направления подготовки бакалавриата 10.03.01 Информационная безопасность.

Текст печатается в авторской редакции

Подписано в печать . Формат 60x84 1/16.
Усл.печ. л. 0,99. Уч.-изд. л. 0,89. Тираж 100 экз. Заказ. Бесплатно.
Юго-Западный государственный университет.
305040, г.Курск, ул. 50 лет Октября, 94.

1 Назначение межсетевых экранов Cisco PIX

Систему разграничения компьютерных сетей с различными политиками безопасности, реализующую правила информационного обмена между ними, называют межсетевым экраном (МЭ). Межсетевой экран – это локальное (однокомпонентное) или функционально-распределенное (многокомпонентное) программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в автоматизированную систему (АС) и/или исходящей из нее.

Существуют три сетевые зоны, с которыми работают межсетевые экраны: внутренняя, внешняя и демилитаризованная.

Внутренняя (inside) зона является так называемой доверительной зоной, к которой относятся устройства и конечные узлы закрытой сети. Обычно эти устройства и узлы подчиняются определенной политике безопасности при работе с другими сетями, относящимися к внешней зоне. Внешняя зона (outside) объединяет недоверенные (non-Trusted) сети. Демилитаризованная зона DMZ (De-Militarized Zone) является частью защищаемой сети, для которой устанавливаются особые правила безопасности. Обычно DMZ создается в случае необходимости размещения в сети серверов публичного доступа, например web-сервера. Основной функцией межсетевого экрана является защита узлов, находящихся во внутренней и демилитаризованных зонах от воздействий с узлов, расположенных во внешней зоне.

Линейкой устройств Cisco, предназначенных для решения задач межсетевого экранирования, является Cisco Secure PIX Firewall. В настоящее время пользователям предлагаются следующие модели аппаратно-программных межсетевых экранов Cisco Secure PIX Firewall – PIX 501, 506E, 515E, 525 и 535.

Рисунок 1 - Вид устройства Cisco PIX 525

Общим компонентом данных устройств является применение адаптивного алгоритма безопасности ASA. Cisco PIX Firewall является межсетевым экраном, использующим технологию пакетной фильтрации с запоминанием состояния (технология динамической фильтрации). Эта технология реализуется адаптивным алгоритмом безопасности (ASA – Adaptive Security Algorithm), основанным на концепции уровней безопасности (security levels). Уровень безопасности определяет степень доверия к тому или иному интерфейсу межсетевого экрана в зависимости от того, защищен он или нет относительно другого интерфейса. С помощью ASA осуществляется изоляция подключенных к межсетевому экрану сегментов сетей, поддерживаются так называемые периметры безопасности и контролируется трафик, проходящий между этими сегментами сетей.

Каждому интерфейсу Cisco PIX Firewall присваивается уровень безопасности от 0 до 100. Значение уровня 100 означает самый высокий уровень безопасности устройства. Этот уровень назначается по умолчанию интерфейсу, связанному с внутренней (inside) зоной. Без создания определенных разрешений узлы внешней зоны не получат доступ к внутренней зоне, тогда как узлы внутренней зоны имеют доступ к другим (внешним) зонам.

Значение уровня 0 устанавливает наименьший уровень безопасности. Назначается по умолчанию интерфейсу, связанному с внешней (outside) зоной. Так как 0 является самым низким значением, то за этим интерфейсом обычно находится самая незащищенная сеть, что позволяет ограничить доступ узлов этой сети к сетям, находящимся за другими интерфейсами без явного разрешения. Уровни безопасности от 1 до 99 назначаются другим

задействованным интерфейсам межсетевого экрана и определяют тип доступа, предоставляемый этим интерфейсам.

Уровни безопасности определяют поведение по умолчанию алгоритма следующим образом:

1) ASA разрешает соединения, исходящие от узлов, находящихся в защищаемой сети, то есть соединения с интерфейса с большим уровнем безопасности на интерфейсы с меньшим уровнем безопасности;

2) ASA запрещает соединения от узлов, находящихся в незащищенной сети, то есть соединения с интерфейса с меньшим уровнем безопасности на интерфейс с большим уровнем безопасности;

3) ASA запрещает соединения между узлами, находящимися в сетях, подключенных к интерфейсам с одинаковыми уровнями безопасности;

4) ASA разрешает соединения, идущие от узлов, находящихся в незащищенной сети, к узлам в защищенной сети (соединения с интерфейса с меньшим уровнем безопасности на интерфейс с большим уровнем безопасности) только в случае, если соблюдаются два условия:

- существует статическая трансляция для адреса назначения

(NAT static translation);

- задан список доступа (или conduit), разрешающий данное соединение.

Алгоритм ASA функционирует как динамический (stateful), ориентированный на соединение (connection-oriented) процесс, сохраняющий информацию о сессиях в таблице состояний (state table). Контроль трафика, проходящего через межсетевой экран, осуществляется путем применения политики безопасности и трансляции адресов к таблице состояний.

2 Аппаратная часть межсетевых экранов Cisco PIX

Межсетевые экраны Cisco PIX являются аппаратными устройствами, предназначенными для размещения как в серверной стойке, так и на стене (рисунок 2).

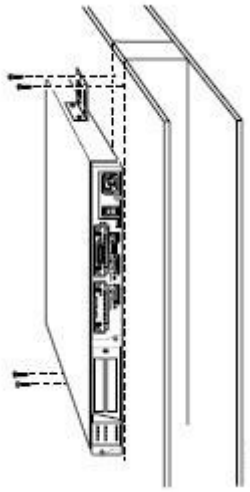

Рисунок 2 - Монтирование устройства Cisco PIX на стену

На лицевой панели устройства (рисунок 3) расположены два индикатора: POWER (наличие питания) и ACTIVE (индикатор режима работоспособности устройства).

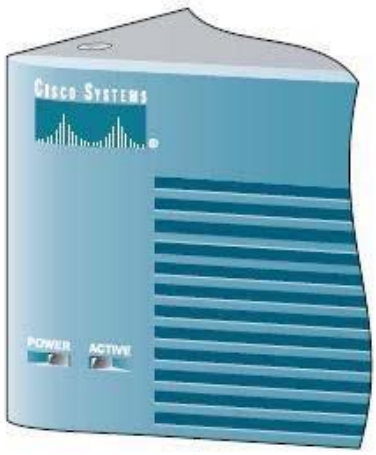

Рисунок 3 - Лицевая панель Cisco PIX 525

На задней панели устройства (рисунок 4) расположены интерфейсы (рисунок 5):

консольный порт для подключения к последовательному порту персонального компьютера с использованием коннектора RJ-45 и управления устройством в режиме командной строки; интерфейсы 100 BaseTX Ethernet0 и 100 BaseTX Ethernet1.

Рисунок 4 - Задняя панель Cisco PIX 525

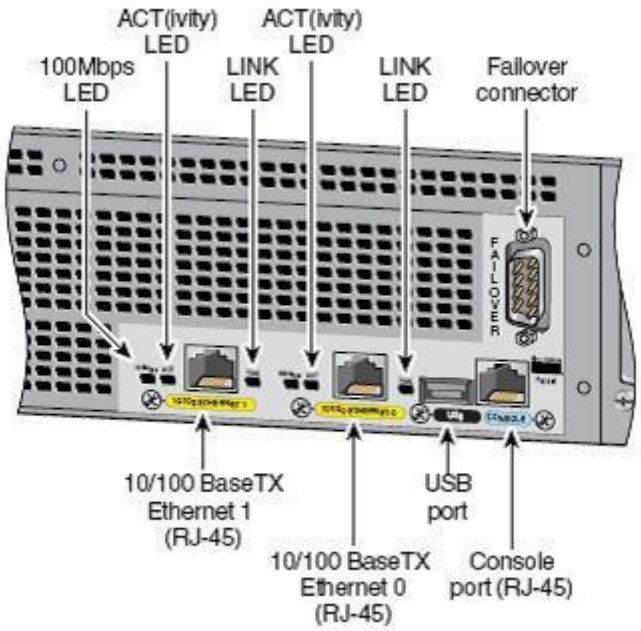

Рисунок 5 - Интерфейсы Cisco PIX 525

3 Базовые команды настройки Cisco PIX

Для начала работы с Cisco PIX определим минимальный набор команд для его настройки. К этим командам относятся: hostname, interface, ip address, route, nameif, security-level, nat, nat-control, global. С частью команд вы уже познакомились в разделе, посвященном настройке маршрутизаторов. Ниже приводится описание команд, специфичных для межсетевого экрана.

Nameif – эта команда предназначена для задания имени и уровня безопасности каждого интерфейса. По умолчанию первые два интерфейса имеют имена inside и outside. Команда имеет следующий синтаксис:

Nameif <интерфейс> <имя_интерфейса> <уровень_ безопасности>.

При первом включении Cisco PIX можно обратить внимание на то, что внутреннему (inside) и внешнему (outside) интерфейсам уже присвоены уровни безопасности: 100 – внутреннему, 0 – внешнему. При задании имен другим интерфейсам автоматически будет назначаться уровень безопасности 0, который в дальнейшем можно изменить.Команда выполняется в глобальном контексте конфигурирования:

PIX(config)#nameif ethernet0 outside security 0 PIX(config)#nameif ethernet1 inside security 100.

Команда clear xlate очищает таблицу трансляций, в результате чего происходит сброс всех существующих соединений, что позволяет изменить уровень безопасности интерфейса без ожидания закрытия существующих соединений.

ВЫПОЛНИТЬ!

1. Задать имена и уровни безопасности для интерфейсов межсетевого экрана.
2. Проверить возможность прохождения сетевых пакетов между интерфейсами межсетевого экрана.
3. Включить интерфейсы межсетевого экрана. По умолчанию все интерфейсы выключены, чтобы произвести их включение необходимо в контексте глобального конфигурирования выполнить команду interface.

Синтаксис команды: interface <интерфейс> <скорость> <состояние>.

Пример:

PIX(config)#interface ethernet0 auto shutdown.

4. Назначить интерфейсам межсетевого экрана IP-адреса. В межсетевых экранах, в отличие от маршрутизаторов, назначение IP-адреса сетевым интерфейсам выполняется в режиме глобального конфигурирования командой:

ip address <имя_интерфейса> <ip_адрес> <маска_сети>.

Пример:

PIX(config)#ip address outside 88.88.88.2 255.255.255.0.

4 Технология NAT

NAT (Network Address Translation) – трансляция адресов, позволяющая скрывать адреса сети от узлов, находящихся за Cisco PIX. При прохождении пакетов через Cisco PIX внутренние адреса сети перед выходом с внешнего интерфейса транслируются в другие адреса. NAT конфигурируется с помощью команд nat и global.

Когда исходящий пакет от узла, находящегося во внутренней зоне, попадает на Cisco PIX, на котором сконфигурирована система NAT, адрес источника пакета сравнивается с таблицей существующих трансляций. Если этого адреса источника нет в таблице, он транслируется в один из адресов пула и в таблице трансляций появляется новая запись для этого адреса источника. Пул выдаваемых адресов конфигурируется командой global. В результате этого происходит обновление таблицы трансляций, а пакет перенаправляется дальше. По истечении определенного времени (значение по умолчанию равно трем часам) запись в таблице трансляций для адреса источника, не пославшего ни одного пакета, очищается и адрес, выданный из пула, освобождается для использования другими узлами внутренней зоны.

Задание правил трансляции адресов исходящих пакетов для одного либо нескольких узлов осуществляется с помощью команды nat.

Синтаксис команды можно представить следующим образом: nat [(if_name)] nat_id address [netmask] [[tcp] tcp_max_conns [emb_limit] [norandomseq]]] [udp udp_max_conns], где:

- if_name – имя интерфейса, подключенного к сети, адреса которой необходимо транслировать;
- nat_id – число от 1 до 65535, соответствующее номеру пула глобальных адресов, в которые будут транслироваться внутренние адреса;
- address [netmask] – адрес, в который будет происходить трансляция;
- tcp_max_conns – максимальное число одновременных соединений, разрешенных узлам внутренней зоны. Соединения в

состоянии бездействия закрываются автоматически по истечении таймаута, задаваемого командой timeout conn;

- emb_limit – максимальное число незавершенных (embryonic) соединений. К незавершенным соединениям относятся те, которые еще не были до конца установлены между источником и назначением, например, при установке TCP-соединения между узлами;
- norandomseq – устанавливает необходимость при каждом новом соединении генерировать случайный initial sequence number (ISN). Связано это с тем, что TCP/IP стек некоторых ОС использует предсказуемые ISN, а это дает возможность злоумышленнику вклиниться в чужую сессию;
- udp_max_conns – максимальное число одновременных UDP-соединений, разрешенных каждому из узлов внутренней сети. UDP-соединения, находящиеся в состоянии бездействия, закрываются автоматически по истечении таймаута, задаваемого командой timeout conn.

Пример настройки службы NAT: PIX(config)#nat
(inside) 1 10.0.0.0 255.255.255.0. ВЫПОЛНИТЬ!

5. Настроить службу NAT на внутреннем интерфейсе межсетевого экрана.

В команде nat параметром nat_id (в примере – 1) указывается номер пула глобальных адресов, которые можно сконфигурировать командой global. Синтаксис:

global [(if_name)] nat_id {mapped_ip
[-mapped_ip] [netmask mapped_mask]} | interface, где:

- if_name – имя интерфейса, на котором необходимо использовать задаваемый пул глобальных адресов;
- mapped_ip [-mapped_ip] – один адрес либо диапазон адресов;
- netmask mapped_mask – задание маски для пула адресов в случае, если используются подсети. Если диапазон адресов с заданной маской покрывает несколько подсетей, то адрес подсети и широковещательный адрес подсети не выдаются для трансляции. Например, если задан диапазон адресов 192.168.0.20-192.168.0.140

и маска 255.255.255.128, то адрес второй подсети 192.168.0.128 и широковещательный адрес первой подсети 192.168.0.127 выдаваться не будут;

- interface – определяет использование PAT (Port Address Translation) на интерфейсе. Пример:

PIX(config)#nat (inside) 1 10.0.0.0 255.255.255.0
PIX(config)#global (outside) 1 192.168.0.3-
192.168.0.100

В этом примере сконфигурирован пул из 98 адресов (192.168.0.3-192.168.0.100) под номером 1, в которые будут транслироваться внутренние адреса узлов из сети 10.0.0.0 при прохождении сетевых пакетов через межсетевой экран.

Выдача адресов осуществляется динамически, начиная с начала диапазона и до его конца. В примере первым выданным адресом будет 192.168.0.3.

ВЫПОЛНИТЬ!

6. Выполнить конфигурацию пула глобальных адресов для внутреннего интерфейса межсетевого экрана.

Командой nat control включается одноименный режим. При работе в этом режиме пакеты, идущие из внутреннего (inside) интерфейса на внешний (outside), должны иметь сконфигурированное для них правило трансляции. То есть, каждый узел сети внутренней зоны может обмениваться данными с узлами сети внешней зоны, если заданы правила трансляции для этих внутренних узлов. Если на Cisco PIX приходит пакет от внутреннего узла, для которого не сконфигурировано правило трансляции, то этот пакет им не обрабатывается.

Режим nat control является выключенным по умолчанию. Поэтому Cisco PIX транслирует адрес источника пакета в любом случае.

ВЫПОЛНИТЬ!

7. Включить nat control режим и проверить возможность прохождения сетевых пакетов между интерфейсами устройства.
8. Выключить nat control режим.

Кроме команды nat существует команда static, с помощью которой осуществляется конфигурирование статической трансляции. Синтаксис команды:

PIX(config)# static (real_ifc, global_ifc)

{global_ip | interface} {real_ip [netmask mask]}, где:

- real_ifc – интерфейс, на который приходят пакеты, подлежащие трансляции;
- global_ifc – интерфейс, с которого уходит для дальнейшей маршрутизации транслированный пакет;
- global_ip – адрес, в который будет осуществляться трансляция;
- real_ip – адрес, который будет транслироваться. Пример:

PIX(config)#static (inside,outside) 192.168.100.10 10.10.10.10 netmask

255.255.255.255

Все пакеты, приходящие на адрес 192.168.100.10 будут передаваться на узел с адресом 10.10.10.10.

ВЫПОЛНИТЬ!

9. Сконфигурировать статическую трансляцию на внешнем интерфейсе межсетевого экрана.

10. С помощью программного сниффера проверить работу статической трансляции.

Команда fixup Cisco PIX предоставляет некоторые возможности глубокого анализа пакетов в межсетевых экранах PIX. Например, команда fixup protocol http приводит к тому, что PIX выполняет ряд действий, к которым относятся:

- ведение журналов, фиксирующих URL-запросы, содержащие команды GET;
- мониторинг URL-запросов при помощи средств N2H2 или

Websense;

- фильтрация опасных сценариев Java и ActiveX.

Для последних двух функций межсетевой экран должен быть сконфигурирован с командой filter. Пример команд для углубленного анализа трафика по основным протоколам: PIX(config)#fixup protocol ftp 21

PIX(config)#fixup protocol http 80

PIX(config)#fixup protocol h323 1720
PIX(config)#fixup protocol rsh 514
PIX(config)#fixup protocol smtp 25 PIX(config)# fixup protocol sqlnet 1521.

5 Настройка межсетевых экранов Cisco PIX

При выполнении работы осуществляется конфигурирование Cisco PIX Firewall для того, чтобы отделить и защитить корпоративную сеть от атак из сети «Интернет». Будем рассматривать внутреннюю сеть организации, содержащую Web-сервер, почтовый сервер и FTP-сервер, к которым имеют доступ пользователи сети «Интернет». Весь остальной доступ к узлам внутренней сети закрыт от внешних пользователей. Схема имитируемой сети показана на рисунок 3.8. Адресация серверов внутренней сети выполнена следующим образом:

- Web-сервер: внутренний адрес 192.168.0.4, Интернет-адрес 88.88.88.3;
- почтовый сервер: внутренний адрес 192.168.0.5, Интернет-адрес 88.88.88.4;
- FTP-сервер: внутренний адрес 192.168.0.6, Интернет-адрес 88.88.88.5.

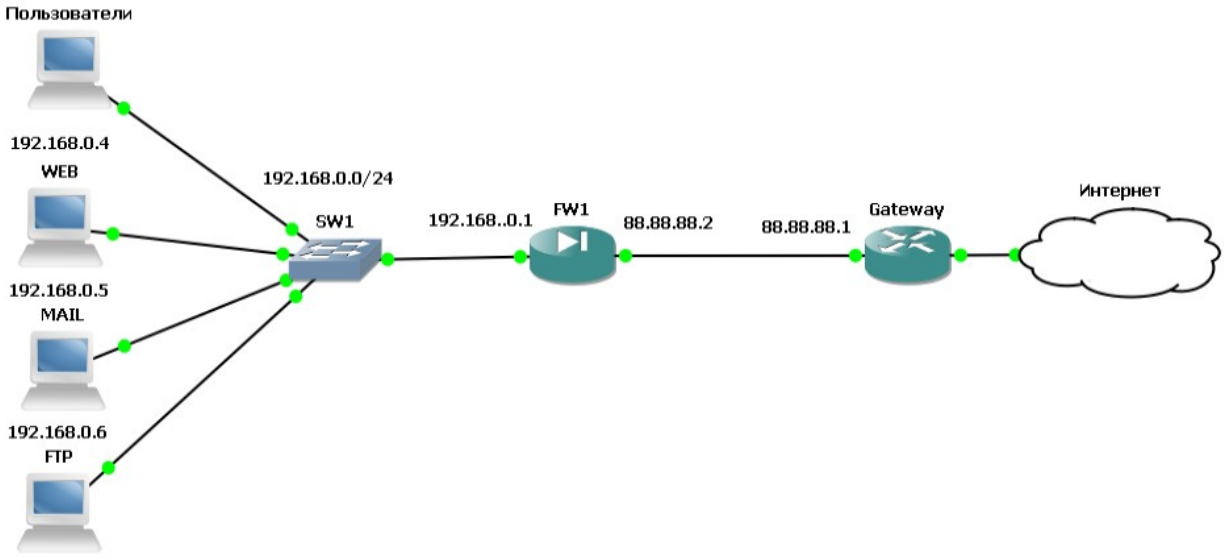

Рисунок 6 - Схема защиты сети

Всем пользователям внутренней сети разрешен неограниченный доступ в Интернет. Также пользователям разрешено выполнять команду ping до узлов в сети «Интернет», в то время как пользователям со стороны сети «Интернет» это запрещено. Провайдером выделен диапазон внешних адресов класса C: 88.88.88.0/24. Адреса 88.88.88.1 и 88.88.88.2 зарезервированы для внешнего маршрутизатора и внешнего интерфейса PIX (см. рисунок 6). Адреса диапазона 88.88.88.3 ÷ 88.88.88.5 отведены для серверов, а адреса 88.88.88.4 ÷ 88.88.88.14 зарезервированы для будущего использования, для пользователей внутренней сети выполняется процедура трансляции адресов.

ВЫПОЛНИТЬ!

11. Создать в GNS3 топологию сети, представленную на рисунок 36.

12. Произвести настройку Cisco PIX Firewall, выполнив следующие команды в контексте глобального конфигурирования:

PIX(config)#nameif ethernet0 outside security0
PIX(config)#nameif ethernet1 inside security100
PIX(config)#hostname pixfirewall
PIX(config)#fixup protocol ftp 21
PIX(config)#fixup protocol http 80

PIX(config)#fixup protocol h323 1720 PIX(config)#fixup protocol rsh 514

PIX(config)#fixup protocol smtp 25

PIX(config)#fixup protocol sqlnet 1521 PIX(config)#fixup protocol sip 5060 PIX(config)#names.

13. Создать ACL, разрешающий исходящие ICMP-запросы и ответы на них:

PIX(config)#access-list 100 permit icmp any any echo-reply

PIX(config)#access-list 100 permit icmp any any time-exceeded

PIX(config)#access-list 100 permit icmp any any unreachable. 14. Добавить разрешения для пользователей Интернет подключаться к Web-, Mail-, и FTP-серверам:

PIX(config)#access-list 100 permit tcp any host 88.88.88.3 eq www

PIX(config)#access-list 100 permit tcp any host 88.88.88.4 eq smtp

PIX(config)#access-list 100 permit tcp any host 88.88.88.5 eq ftp.

15. Включить режим ведения журналов:

PIX(config)#logging on

PIX(config)#no logging timestamp

PIX(config)#no logging standby

PIX(config)#no logging console PIX(config)#no logging monitor.

16. Установить режим сохранения сообщений об ошибках в локальном буфере:

PIX(config)#logging buffered errors.

17. Включить все интерфейсы (выключены по умолчанию):

PIX(config)#interface ethernet0 auto PIX(config)#interface ethernet1 auto.

18. Назначить IP-адреса сетевым интерфейсам:

PIX(config)#ip address outside 88.88.88.2 255.255.255.0

PIX(config)#ip address inside 192.168.0.1 255.255.255.0.

19. Определить пул трансляции адресов, которые используют внутренние узлы для выхода в Интернет:

PIX(config)#global (outside) 1 88.88.88.1588.88.88.253.

20. Определить адрес, который будет использоваться, когда выделенный пул адресов закончится:

PIX(config)#global (outside) 1 88.88.88.254.

21. Установить разрешение для всех внутренних узлов на использование NAT или PAT, определенные ранее:

PIX(config)#nat (inside) 1 0.0.0.0 0.0.0.0 0 0.

22. Задать статическую трансляцию для внутренних Web-, почтового и FTP-серверов, чтобы они были доступны из Интернета:

PIX(config)#static (inside,outside) 88.88.88.3 192.168.0.4 netmask 255.255.255.255 0 0

PIX(config)#static (inside,outside) 88.88.88.4 192.168.0.5 netmask 255.255.255.255 0 0

PIX(config)#static (inside,outside) 88.88.88.5 192.168.0.6 netmask 255.255.255.255 0 0.

23. Применить разработанный ACL с номером 100 к внешнему интерфейсу, выполнив в его контексте конфигурирования команду:

PIX(config)#access-group 100 in interface outside.

24. Назначить маршрут по умолчанию на маршрутизатор провайдера услуг Интернет командой в глобальном контексте конфигурирования:

PIX(config)#route outside 0.0.0.0 0.0.0.0

88.88.88.1 1.

25. Проверить работоспособность заданной конфигурации.

Библиографический список

1. Защита информации в компьютерных сетях. Практический курс : учеб. пособие / А. Н. Андрончик, В. В. Богданов, Н. А. Домуховский [и др.] ; под ред. Н. И. Синадского. – Екатеринбург : УГТУ-УПИ, 2008. – 248 с.

2. Americas Headquarters Cisco Security MARS Initial Configuration and Upgrade Guide, Release 6.x. – USA : Cisco Systems, 2009. – 136 p.

3. Gary Hallen, G. Kellogg Security Monitoring with Cisco Security MARS. – USA : Cisco Press, 2007. – 335 p.

4. James Burton, Ido Dubrawsky, Vitaly Osipov Cisco Security Professional's Guide to Secure Intrusion Detection Systems. – USA : Syngress Publishing, 2003. – 673 p.

5. Installation Guide for the Cisco Secure PIX Firewall Version 5.2. [Электронный ресурс]. Режим доступа: http://www.cisco.com.

6. Install and Setup Guide for Cisco Security Monitoring Analysis and Response System. Release 4.3.x., 2008. [Электронный ресурс]. Режим доступа: http://www.cisco.com.

7. Стивенс У. Р. Протоколы TCP/IP. Практическое руководство / пер. с англ. – СПб. : БХВ-Петербург, 2003. – 672 с.

8. Кульгин М. Практика построения компьютерных сетей. Для профессионалов. – СПб. : Питер, 2001. – 320 с.

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

НАСТРОЙКА ZONE-BASED POLICY FIREWALL

Методические рекомендации по выполнению лабораторной работы для студентов направления подготовки 10.03.01 Информационная безопасность

Курск 2024

УДК 621.(076.1)

Составители: Е.М. Терещенко, В.В.Чуйкова

Рецензент

Доктор физико-математических наук, профессор кафедры Информационная безопасность В.П. Добрица

Настройка Zone-Based Policy Firewall: методические рекомендации по выполнению лабораторной работы / Юго-Зап. гос. ун-т; сост.: Е.М. Терещенко, В.В. Чуйкова. – Курск, 2024. – 7 с.: ил. 1. – Библиогр.: с. 7.

Содержат сведения по вопросам конфигурирования межсетевого экрана в программной среде Cisco GNS3.

Указывается порядок выполнения лабораторной работы, правила оформления и содержание отчета.

Методические указания соответствуют требованиям программы, утвержденной учебно-методическим объединением по специальности.

Предназначены для студентов направления подготовки бакалавриата 10.03.01 Информационная безопасность.

Текст печатается в авторской редакции

Подписано в печать . Формат 60x84 1/16.
Усл.печ. л. 0,47. Уч.-изд. л. 0,42. Тираж 100 экз. Заказ. Бесплатно.
Юго-Западный государственный университет.
305040, г.Курск, ул. 50 лет Октября, 94.

ВВЕДЕНИЕ

Начиная с версии IOS 12.4, в маршрутизаторах появилась функция Zone-Based Policy Firewall, позволяющая производить настройку правил межсетевого экрана. Эта функция позволяет назначить интерфейсам маршрутизатора зоны безопасности и установить правила взаимодействия между ними.

Конфигурирование Zone-Based Policy Firewall заключается в выполнение следующих шагов:

1) назначить зоны межсетевого экрана;
2) определить возможность прохождения сетевого трафика между зонами;
3) включить существующие сетевые интерфейсы в созданные зоны;
4) определить классы, к которым будут применяться политики для пересечения пары зон;
5) определить политики для пар зон, регламентирующие производимые действия над проходящим сетевым трафиком; 6) применить политики для выбранных пар зон.

Рассмотрим настройку Zone-Based Policy Firewall для случая, представленного на рисунке 30. В демилитаризованной зоне (ДМЗ) с адресом 172.16.0.0/16 расположены: Web-сервер (172.16.0.4); почтовый сервер (172.16.0.5); FTP-сервер (172.16.0.6). Адрес внутренней сети (пользователи) 192.168.20.0/24. Внешний IP-адрес маршрутизатора 10.0.0.2, маска сети 255.0.0.0, внутренний – 192.168.20.2.

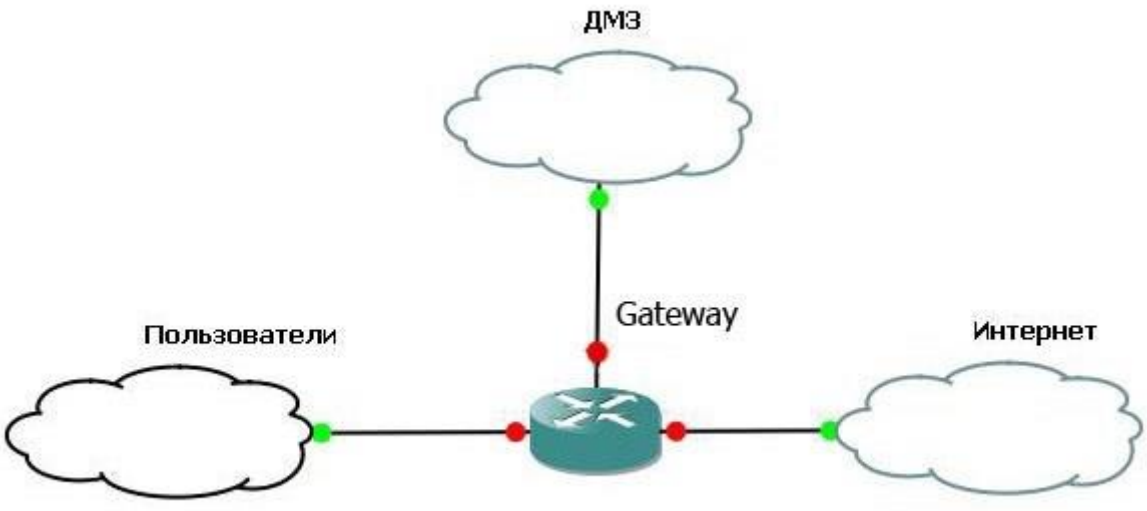

Рисунок 1 - Схема сети

ВЫПОЛНИТЬ!

1. **Создать в GNS3 топологию сети**, представленную выше (на рисунке 1).
2. **В режиме глобального конфигурирования** определить зоны безопасности. Для пользователей задать зону с именем inside, для Интернета – outside, для ДМЗ – DMZ.

```
Gateway(config)#zone security outside
Gateway(config-sec-zone)#description internet
Gateway(config-sec-zone)#exit
Gateway(config)#zone security inside
Gateway(config-sec-zone)# description intranet
Gateway(config-sec-zone)#exit
Gateway(config)#zone security dmz
Gateway(config-sec-zone)#description DMZ
Gateway(config-sec-zone)#exit.
```

3. **Назначить интерфейсы в зоны**. По умолчанию прохождения трафика между зонами запрещено.

Для зоны outside:

```
Gateway(config)#interface FastEthernet0/0
Gateway(config-if)#ip address 10.0.0.2 255.0.0.0
Gateway(config-if)#no shutdown
Gateway(config-if)#zone-member security outside
Gateway(config-if)#description outside
Gateway(config-if)#exit.
```

Для зоны inside:

```
Gateway(config)#interface FastEthernet0/1
Gateway(config-if)#ip address 192.168.20.2 255.255.255.0
Gateway(config-if)#no shutdown
Gateway(config-if)#zone-member security inside
Gateway(config-if)#description inside
Gateway(config-if)#exit.
```

Для зоны DMZ:

```
Gateway(config)#interface FastEthernet1/0
Gateway(config-if)#ip address 172.16.0.2 255.255.255.0
Gateway(config-if)#no shutdown
Gateway(config-if)#zone-member security dmz
Gateway(config-if)#description DMZ
Gateway(config-if)#exit.
```

4. **Определить протоколы**, по которым пользователям разрешено выходить в Интернет (http, ftp, smtp, pop3, dns, icmp).

```
Gateway(config)#class-map type inspect match-any cm_http-ftp-dns-smtp-pop3-icmp
```

Gateway(config-cmap)#match protocol http

Gateway(config-cmap)#match protocol ftp Gateway(config-cmap)#match protocol pop3

Gateway(config-cmap)#match protocol smtp

Gateway(config-cmap)#match protocol dns

Gateway(config-cmap)#match protocol icmp

Gateway(config-cmap)#exit.

5. Определить политики:

Gateway(config)#policy-map type inspect in-out

Gateway(config-pmap)#class type inspect cm_httpftp-dns-smtp-pop3-icmp

Gateway(config-pmap-c)#inspect

Gateway(config-pmap-c)#exit

Gateway(config-pmap)#exit.

6. Создать цепочку из пары зон inside → outside:

Gateway(config)#zone-pair security insideoutside source inside destination outside

Gateway(config-sec-zone-pair)#service-policy type inspect in-out

Gateway(config-sec-zone-pair)#exit.

7. Создать списки доступа для публичных серверов:

Gateway(config)#access-list 101 remark webserver

Gateway(config)#access-list 101 permit ip any host 172.16.0.4

Gateway(config)#access-list 102 remark mailserver

Gateway(config)#access-list 102 permit ip any host 172.16.0.5

Gateway(config)#access-list 103 remark ftpserver

Gateway(config)#access-list 103 permit ip any host 172.16.0.6.

8. Определить протоколы для доступа к серверам из внешней сети:

Gateway(config)#class-map type inspect match-all web

Gateway(config-cmap)#match access-group 101 Gateway(config-cmap)#match protocol http

Gateway(config-cmap)#exit

Gateway(config)#class-map type inspect match-all mail

Gateway(config-cmap)#match access-group 102

Gateway(config-cmap)#match protocol smtp

Gateway(config-cmap)#match protocol pop3

Gateway(config-cmap)#exit

Gateway(config)#class-map type inspect match-all ftp

Gateway(config-cmap)#match access-group 103

Gateway(config-cmap)#match protocol ftp

Gateway(config-cmap)#exit.

9. Задать политики для ДМЗ:

Gateway(config)#policy-map type inspect webmail-ftp-dmz
Gateway(config-pmap)#class type inspect web
Gateway(config-pmap-c)#inspect
Gateway(config-pmap-c)#exit
Gateway(config-pmap)#class type inspect mail
Gateway(config-pmap-c)#inspect
Gateway(config-pmap-c)#exit
Gateway(config-pmap)#class type inspect ftp
Gateway(config-pmap-c)#inspect
Gateway(config-pmap-c)#exit
Gateway(config-pmap)#exit.

10. Создать цепочку из пары зон outside → dmz:

Gateway(config)#zone-pair security out-dmz source outside destination dmz

Gateway(config-sec-zone-pair)#service-policy type inspect web-mail-ftp-dmz

Gateway(config-sec-zone-pair)#exit.

Проверить работоспособность созданной конфигурации.

Библиографический список

1. Защита информации в компьютерных сетях. Практический курс : учеб. пособие / А. Н. Андрончик, В. В. Богданов, Н. А. Домуховский [и др.] ; под ред. Н. И. Синадского. – Екатеринбург : УГТУ-УПИ, 2008. – 248 с.

2. Americas Headquarters Cisco Security MARS Initial Configuration and Upgrade Guide, Release 6.x. – USA : Cisco Systems, 2009. – 136 p.

3. Gary Hallen, G. Kellogg Security Monitoring with Cisco Security MARS. – USA : Cisco Press, 2007. – 335 p.

4. James Burton, Ido Dubrawsky, Vitaly Osipov Cisco Security Professional's Guide to Secure Intrusion Detection Systems. – USA : Syngress Publishing, 2003. – 673 p.

5. Installation Guide for the Cisco Secure PIX Firewall Version 5.2. [Электронный ресурс]. Режим доступа: http://www.cisco.com.

6. Install and Setup Guide for Cisco Security Monitoring Analysis and Response System. Release 4.3.x., 2008. [Электронный ресурс]. Режим доступа: http://www.cisco.com.

7. Стивенс У. Р. Протоколы TCP/IP. Практическое руководство / пер. с англ. – СПб. : БХВ-Петербург, 2003. – 672 с.

8. Кульгин М. Практика построения компьютерных сетей. Для профессионалов. – СПб. : Питер, 2001. – 320 с.

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

ОРГАНИЗАЦИЯ ЗАЩИЩЕННОГО КАНАЛА НА ОСНОВЕ IPSEC

Методические рекомендации по выполнению лабораторной работы для студентов направления подготовки 10.03.01 Информационная безопасность

Курск 2024

УДК 621.(076.1)

Составители: Е.М. Терещенко, В.В. Чуйкова

Рецензент

Доктор физико-математических наук, профессор кафедры
Информационная безопасность В.П. Добрица

Организация защищенного канала на основе IPSec :
методические рекомендации по выполнению лабораторной работы /
Юго-Зап. гос. ун-т; сост.: Е.М. Терещенко, В.В. Чуйкова. –
Курск, 2024. – 13 с.: ил. 3. – Библиогр.: с. 13.

Содержат сведения по вопросам работы в программном продукте Cisco GNS3. Указывается порядок выполнения лабораторной работы, правила оформления и содержание отчета. Методические указания соответствуют требованиям программы, утвержденной учебно-методическим объединением по специальности.

Предназначены для студентов направления подготовки бакалавриата 10.03.01 Информационная безопасность.

Текст печатается в авторской редакции

Подписано в печать . Формат 60x84 1/16.
Усл.печ. л. 0,76. Уч.-изд. л. 0,68. Тираж 100 экз. Заказ. Бесплатно.
Юго-Западный государственный университет.
305040, г.Курск, ул. 50 лет Октября, 94.

В качестве практической задачи предлагается настроить IPSec-туннель между двумя маршрутизаторами. Предполагается, что весь трафик, проходящий между маршрутизаторами, будет шифроваться на сетевом уровне, скрывая данные и адреса. Схема сети представлена на рисунок 1.

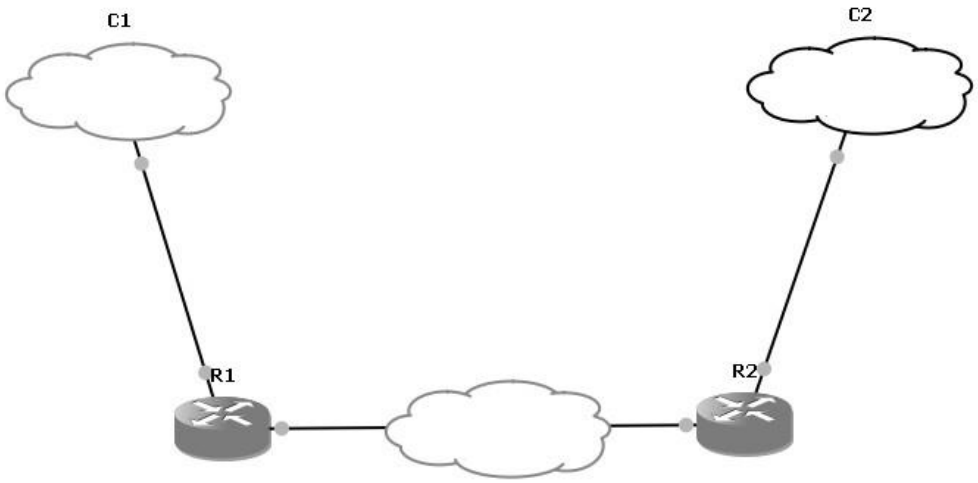

Рисунок 1 - Схема сети, состоящей из двух маршрутизаторов

Подробно рассмотрим настройку маршрутизатора R1. Настройка маршрутизатора R2 будет аналогичной. C1 – сеть с диапазоном IP-адресов 192.168.1.0/24. C2 – сеть с диапазоном IP-адресов 10.0.0.0/24. R1 – маршрутизатор, на котором задействованы два интерфейса: fa1/1 соединен с сетью C1 и имеет IP-адрес 192.168.1.1, fa1/0 соединен с маршрутизатором R2 и имеет IP-адрес 22.22.22.1. R2 – маршрутизатор, на котором задействованы также два интерфейса: fa1/1 соединен с сетью C2 и имеет IP-адрес 10.0.0.1, fa1/0 соединен с маршрутизатором R1 и имеет IP-адрес 22.22.22.2.

Первый шаг заключается в назначении маршрутов и настройке адресов интерфейсов. Для этого необходимо выполнить следующую последовательность команд:

Router>enable

!Переход в контекст администратора. По умолчанию пароль не установлен.

Router#configuration terminal

!Переход в глобальный контекст конфигурирования.

Router(config)#interface FastEthernet 1/1

!Переход в контекст конфигурирования интерфейса FastEthernet 1/1.

Router(config-if)#ip address 192.168.1.1 255.255.255.0

!Назначение IP-адреса и маски сети.

Router(config-if)#no shutdown

!Включение интерфейса.

Router(config-if)#exit

!Выход из контекста конфигурирования интерфейса FastEthernet 1/1.

Router(config)#interface FastEthernet 1/0

!Переход в контекст конфигурирования интерфейса FastEthernet 1/0.

Router(config-if)#ip address 22.22.22.1 255.255.255.0

!Назначение IP-адреса и маски сети.

Router(config-if)#no shutdown

!Включение интерфейса.

Router(config-if)#exit

Router(config)#ip route 0.0.0.0 0.0.0.0 fastethernet 1/1 22.22.22.2

!Указание маршрута по умолчанию.

ВЫПОЛНИТЬ!

1. Произвести первоначальную настройку интерфейсов.

IPSec предлагает стандартные способы аутентификации и шифрования соединений. В IPSec применяются открытые стандарты согласования ключей шифрования и управления соединениями. Технология IPSec предлагает методы, позволяющие сторонам «договориться» о согласованном использовании сервисов. Для указания согласуемыхпараметров в IPSec существуют ассоциации защиты.

Ассоциация защиты (SA) представляет собой согласованную политику или способ обработки данных, обмен которыми предполагается осуществлять между двумя устройствами. Например, согласуется алгоритм, используемый для шифрования

данных. Обе стороны могут применять один и тот же алгоритм как для шифрования, так и для дешифрования. Действующие параметры SA сохраняются в базе данных ассоциаций защиты (SA Database – SAD) обеих сторон.

Протокол IKE является гибридным протоколом, обеспечивающим аутентификацию сторон IPSec, согласование параметров ассоциаций защиты IKE и IPSec, а также выбор ключей для алгоритмов шифрования. Протокол IKE опирается на протоколы ISAKMP и Oakley, которые применяются для управления процессом создания и обработки ключей шифрования. IKE и ISAKMP, применительно к маршрутизаторам Cisco, будем рассматривать как синонимы.

Принцип работы IPSec можно представить в виде следующих шагов:

1. Начало процесса IPSec. Устройство, которому требуется шифровать трафик в соответствии с политикой защиты IPSec, согласованной сторонами IPSec, начинает IKE-процесс.
2. Первая фаза IKE. IKE-процесс выполняет аутентификацию сторон IPSec и ведет переговоры о параметрах ассоциаций защиты IKE, в результате чего создается защищенный канал для ведения переговоров о параметрах ассоциаций защиты IPSec в ходе второй фазы IKE.
3. Вторая фаза IKE. IKE-процесс ведет переговоры о параметрах ассоциации защиты IPSec и устанавливает соответствующие ассоциации защиты IPSec для устройств общающихся сторон.
4. Передача данных. Происходит обмен данными между общающимися сторонами IPSec, который основывается на параметрах IPSec и ключах, хранимых в базе данных ассоциаций защиты.
5. Завершение работы туннеля IPSec. Ассоциации защиты IPSec завершают свою работу либо в результате их удаления, либо по причине превышения предельного времени их существования.

Настройка IKE:

Router(config)#crypto isakmp enable

!Глобальная активизация IKE. Отменить IKE можно с помощью этой же команды, добавив в начало no.

Router(config)#crypto isakmp policy 100

!Задание политики IKE. Здесь 100 – это приоритет, который однозначно идентифицирует политику IKE. 1 – наивысший приоритет, 10000 – наименьший. Эта команда открывает контекст конфигурирования политики IKE, в котором можно устанавливать параметры IKE. Если в этом контексте не будет указана какая-либо команда, то для соответствующего параметра будет использоваться значение по умолчанию.

Router(config-isakmp)#hash md5

!Алгоритм хэширования сообщений – md5. Также можно использовать rsa.

Router(config-isakmp)#authentication pre-share

!Параметры обмена ключами – используем заранее согласованные ключи.

Router(config-isakmp)#exit

!Выход из контекста конфигурирования политики IKE.

Router(config)#crypto isakmp key 12345 address 22.22.22.2

!Выбор общих ключей аутентификации. Ключ следует определять каждый раз, когда в политике IKE указывается использование заранее согласованных общих ключей. Здесь 12345 – общий ключ. Для задания ключа можно использовать любую буквенноцифровую комбинацию длиной до 128 бит. Значения общих ключей должны быть одинаковы в устройствах обеих сторон. Address – задание IP-адреса другой стороны, может использоваться также и имя хоста, если вместо address подставить hostname.

ВЫПОЛНИТЬ!

2. Произвести настройку IKE.

Следующим шагом производится настройка IPSec.

Router(config)#crypto ipsec transform-set r1 esp-des esp-md5-hmac

!Определение набора преобразований, представляющего собой совокупность конкретных алгоритмов IPSec, с помощью которых реализуется политика защиты для выбранного трафика. В рамках ассоциации защиты IKE выполняются операции

согласования, в результате чего стороны соглашаются использовать конкретный набор преобразований для защиты потока данных. Набор преобразований определяется с помощью команды глобальной конфигурации crypto ipsec transform-set, активизирующей конфигурационный контекст cfg-crypto-trans. Параметры команды:

Router(config)#crypto ipsec transform-set
<набор> <преобразование>

В примере: набор – r1; преобразование esp-des – преобразование ESP, использующее шифр DES (56 бит); esp-md5-hmac – преобразование ESP с аутентификацией HMAC-MD5; используется в комбинации с esp-des и esp-3des для обеспечения целостности пакетов ESP.

Router(cfg-crypto-trans)#exit

!Выход из конфигурационного контекста cfg-crypto-trans.

Router(config)#crypto map r1map 100 ipsec-isakmp

!Настройка криптографической карты. Здесь r1map – имя карты, 100 – порядковый номер (приоритет), ipsec-isakmp – требование использовать IKE при создании ассоциаций защиты IPSec для трафика, определяемого новой записью криптографической карты. При вводе данной команды открывается контекст конфигурирования криптографической карты.

Router(config-crypto-map)#set peer 22.22.22.2 !Идентификация IPSec-партнера с помощью IP-адреса или имени хоста. Можно указать несколько адресов для реализации стратегии резервирования.

Router(config-crypto-map)#set transform-set r1

!Указание списка наборов преобразований. Здесь – r1.

Router(config-crypto-map)#match address 151

!Идентификация расширенного списка доступа, используемого криптографической картой. Здесь 151 – номер списка.

Router(config-crypto-map)#exit

!Выход из контекста конфигурирования криптографической карты.

Router(config)#interface FastEthernet 1/0

!Переход в контекст конфигурирования интерфейса FastEthernet 1/0.

Router(config-if)#ip access-group 101 in

!Указание на использование списка доступа № 101 для контроля входного трафика на этом интерфейсе.

Router(config-if)#crypto map r1map

!Применение набора записей криптографической карты к этому интерфейсу.

Router(config-if)#exit

!Выход из контекста конфигурирования интерфейса.

ВЫПОЛНИТЬ!

3. Провести настройку IPSec.

Заключительным шагом является настройка списков доступа.

Router(config)#access-list 101 permit ahp host
22.22.22.2 host 22.22.22.1

!Задание расширенного списка доступа № 101, разрешающего входящий трафик протокола AHP с удаленного маршрутизатора.

Router(config)#access-list 101 permit esp host
22.22.22.2 host 22.22.22.1

!Задание расширенного списка доступа № 101, разрешающего входящий трафик протокола ESP с удаленного маршрутизатора.

Router(config)#access-list 101 permit udp host
22.22.22.2 host 22.22.22.1 eq isakmp

!Задание расширенного списка доступа № 101, разрешающего входящий трафик протокола UDP с удаленного маршрутизатора на порт isakmp.

Router(config)#access-list 151 permit ip
192.168.1.0 0.0.0.255 10.0.0.0 0.0.0.255

!Задание расширенного списка доступа № 151, разрешающего прохождение IP-трафика со всех адресов сети 192.168.1.0/24 на все адреса сети 10.0.0.0/24.

Router(config)#access-list 151 deny ip any any

!Запрет всего остального IP-трафика.

Router(config)#exit

!Завершение конфигурирования.

ВЫПОЛНИТЬ!

4. Произвести настройку списков доступа для лабораторной работы. Для второго маршрутизатора R2 настройка будет такой же. Ниже приведен список команд.

Router#show ip interface
FastEthernet1/0 is up, line protocol is up
Internet address is 22.22.22.2/24
Broadcast address is 255.255.255.255
Outgoing access list is not set
Inbound access list is not set
FastEthernet1/1 is up, line protocol is up
Internet address is 10.0.0.1/24
Broadcast address is 255.255.255.255
Outgoing access list is not set
Inbound access list is not set
Router(config)#crypto isakmp enable
Router(config)#crypto isakmp policy 100
Router(config-isakmp)#hash md5
Router(config-isakmp)#authentication pre-share
Router(config)#crypto isakmp key 12345 address 22.22.22.1
Router(config)#crypto ipsec transform-set r2 esp-des esp-md5-hmac
Router(cfg-crypto-trans)#exit
Router(config)#crypto ipsec transform-set r2 esp-des esp-md5-hmac
Router(cfg-crypto-trans)#exit Router(config)#crypto map r2map 100 ipsec-isakmp Router(config-crypto-map)#set peer 22.22.22.1 Router(config-crypto-map)#set transform-set r2 Router(config-crypto-map)#match address 151 Router(config-crypto-map)#exit
Router(config)#int fa 1/0
Router(config-if)#ip access-group 101 in
Router(config-if)#crypto map r2map
Router(config-if)#exit
Router(config)#access-list 101 permit ahp host 22.22.22.1 host 22.22.22.2

Router(config)#access-list 101 permit esp host 22.22.22.1 host 22.22.22.2

Router(config)#access-list 101 permit udp host 22.22.22.1 host 22.22.22.2 eq isakmp

Router(config)#access-list 151 permit ip 10.0.0.0 0.0.0.255 192.168.1.0 0.0.0.255

Router(config)#access-list 151 deny ip any any

Router(config)#exit

Сконфигурировав маршрутизаторы с помощью представленных выше команд, мы получим шифрованный IPSec-туннель. На рисунках показан трафик с включенным шифрованием (рисунок 2) и без шифрования (рисунок 3).

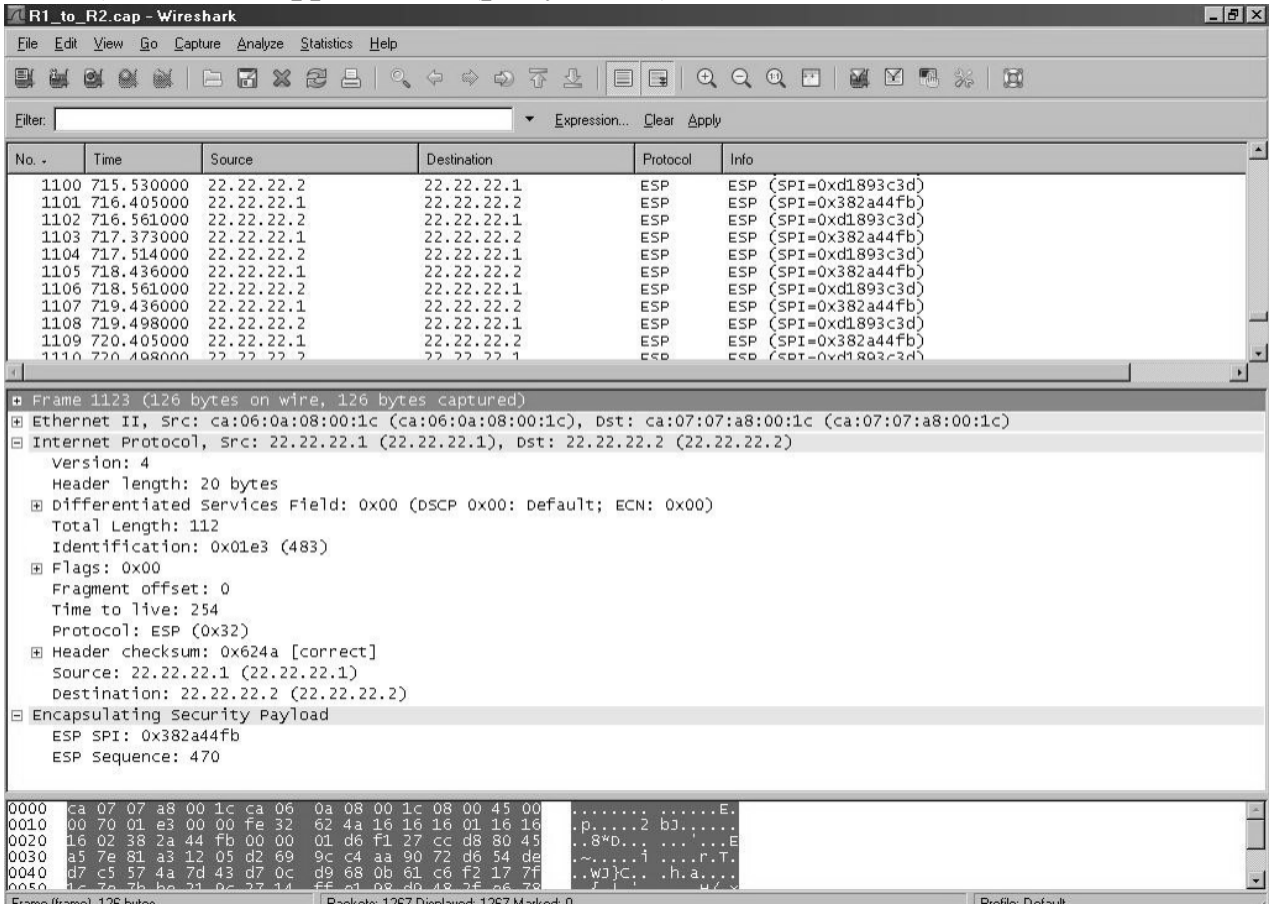

Рисунок 2 - Вид зашифрованного трафика

ВЫПОЛНИТЬ!

5. Произвести настройку второго маршрутизатора.

6. Проверить с помощью захвата трафика работу шифрованного туннеля.

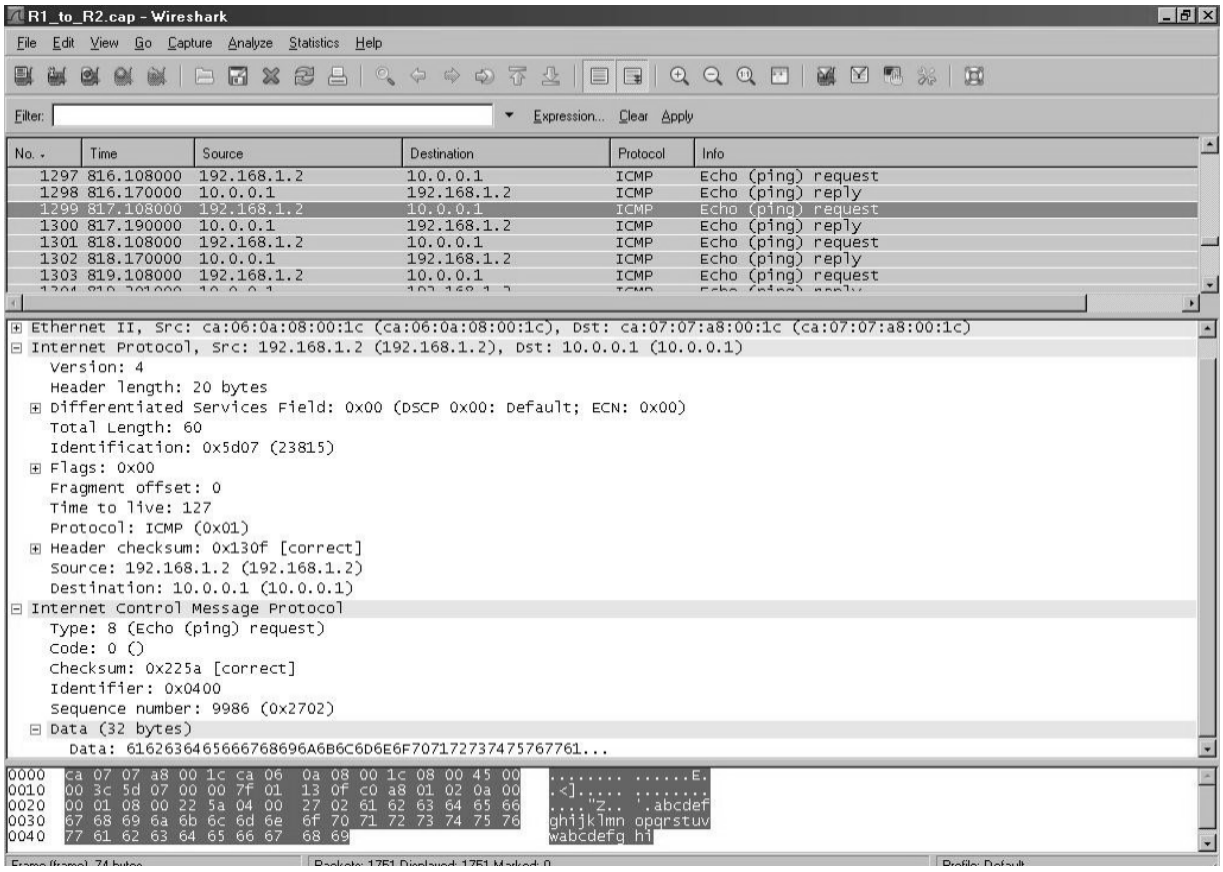

Рисунок 3 - Вид трафика без шифрования

Вопросы для проверки знаний:

1. В чем состоит ограничение при использовании стандартных списков доступа?
2. Какие сетевые протоколы поддерживаются при создании правил расширенных списков доступа?
3. В чем состоит преимущество использования динамических обратных списков доступа перед другими?
4. Объяснить понятие уровня безопасности интерфейса Cisco PIX Firewall.
5. Назвать виды NAT и дать им краткую характеристику.
6. Назвать преимущества использования технологии NAT при подключении к открытым сетям.
7. Какова роль протокола IKE при организации IPSec-туннеля?

Библиографический список

1. Защита информации в компьютерных сетях. Практический курс : учеб. пособие / А. Н. Андрончик, В. В. Богданов, Н. А. Домуховский [и др.] ; под ред. Н. И. Синадского. – Екатеринбург : УГТУ-УПИ, 2008. – 248 с.

2. Americas Headquarters Cisco Security MARS Initial Configuration and Upgrade Guide, Release 6.x. – USA : Cisco Systems, 2009. – 136 p.

3. Gary Hallen, G. Kellogg Security Monitoring with Cisco Security MARS. – USA : Cisco Press, 2007. – 335 p.

4. James Burton, Ido Dubrawsky, Vitaly Osipov Cisco Security Professional's Guide to Secure Intrusion Detection Systems. – USA : Syngress Publishing, 2003. – 673 p.

5. Installation Guide for the Cisco Secure PIX Firewall Version 5.2. [Электронный ресурс]. Режим доступа: http://www.cisco.com.

6. Install and Setup Guide for Cisco Security Monitoring Analysis and Response System. Release 4.3.x., 2008. [Электронный ресурс]. Режим доступа: http://www.cisco.com.

7. Стивенс У. Р. Протоколы TCP/IP. Практическое руководство / пер. с англ. – СПб. : БХВ-Петербург, 2003. – 672 с.

8. Кульгин М. Практика построения компьютерных сетей. Для профессионалов. – СПб. : Питер, 2001. – 320 с.

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

ЭМУЛЯТОР ОБОРУДОВАНИЯ CISCO GNS3

Методические рекомендации по выполнению лабораторной работы для студентов направления подготовки 10.03.01 Информационная безопасность

Курск 2024

УДК 621.(076.1)

Составитель: Е.М. Терещенко, В.В.Чуйкова

Рецензент
Доктор физико-математических наук, профессор кафедры
Информационная безопасность *В.П. Добрица*

Эмулятор оборудования Cisco GNS3: методические рекомендации по выполнению лабораторной работы / Юго-Зап. гос. ун-т; сост.: Е.М. Терещенко, В.В.Чуйкова – Курск, 2024. – 26 с.: ил. 13. – Библиогр. 8 : с. 27.

Содержат сведения по вопросам работы в программном продукте Cisco GNS3. Указывается порядок выполнения лабораторной работы, правила выполнения отчета.

Методические указания соответствуют требованиям программы, утвержденной учебно-методическим объединением по специальности.

Предназначены для студентов направления подготовки бакалавриата 10.03.01 Информационная безопасность.

Текст печатается в авторской редакции

Подписано в печать . Формат 60x84 1/16.
Усл.печ. л. 1,57. Уч.-изд. л. 1,42. Тираж 100 экз. Заказ. Бесплатно.
Юго-Западный государственный университет.
305040, г.Курск, ул. 50 лет Октября, 94.

1.1 Общие сведения о пакете, установка и его настройка

Одной из альтернатив программному продукту Cisco Packet Tracer является интегрированная среда GNS3. Она базируется на проекте Dynamips, целью которого была разработка эмулятора маршрутизаторов фирмы Cisco серии 7200. Позже в эмулятор была добавлена поддержка еще нескольких серий маршрутизаторов той же фирмы, построенных на базе процессоров MIPS и PowerPC. Так как в основе GNS3 лежит эмулятор, то в отличие от Packet Tracer, имитирующего работу ОС устройства, GNS3 использует реальные образы ОС Cisco IOS. В более новых версиях продукта добавлена поддержка ОС Cisco PIX, Cisco IDS, виртуальных образов ОС обычных компьютеров.

Среда эмуляции состоит из четырех компонентов: графического интерфейса (собственно GNS3), консоли управления гипервизором (Dynagen), эмулятора ОС маршрутизаторов (Dynamips) и программы виртуализации хост-машин (модифицированный Qemu). GNS3 предоставляет графический интерфейс построения схемы сети и доступа к Dynagen, Dynamips и Qemu, обеспечивает управление образами узлов и проектом в целом. Эмулятор маршрутизатора, как следует из названия, обеспечивает эмуляцию работы ОС устройства, то есть, исполнение кода IOS, функционирование подключаемых модулей и сетевых соединений. Программа виртуализации обеспечивает работу «пользовательских» машин, Cisco PIX, IDS, а также их сетевое взаимодействие с маршрутизаторами.

GNS3 существует в версии для ОС семейства Windows и Linux (внешний вид программы и структура конфигурационных файлов одинаковы). Установка пакета производится стандартным образом для той или иной ОС. После завершения установки автоматически запускается мастер настройки программы (рисунок 1). При отказе пользователя от работы с мастером начальной настройки, доступ к конфигурационным параметрам осуществляется через подпункты Preferences… и IOS images and hypervisors пункта Edit меню программы.

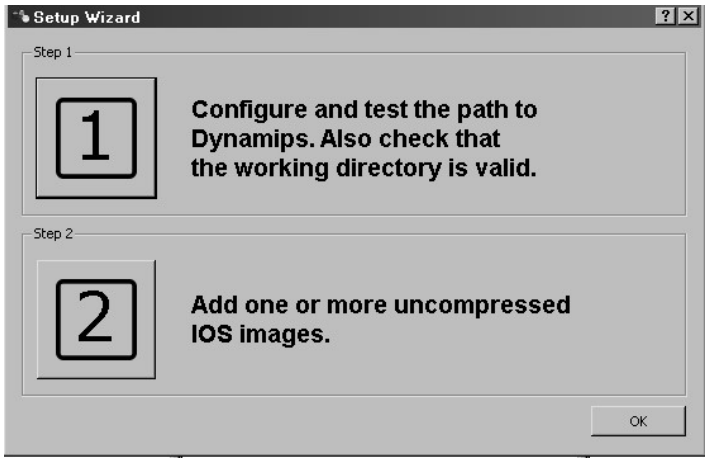

Рисунок 1 - Мастер настройки GNS3

При настройке программы в разделе General (рисунок 2), прежде всего, указываются пути к каталогам хранения образов IOS различных устройств и пользовательских файлов-проектов.

В разделе Dynamips указываются параметры настройки эмулятора (рисунок 3), среди которых основными являются: имена исполняемого файла эмулятора и рабочего каталога для хранения временных файлов. В подавляющем большинстве случаев дополнительные параметры можно оставить без изменений. Перед первым запуском программы и после внесения изменений желательно нажать кнопку Test для проверки правильности функционирования эмулятора.

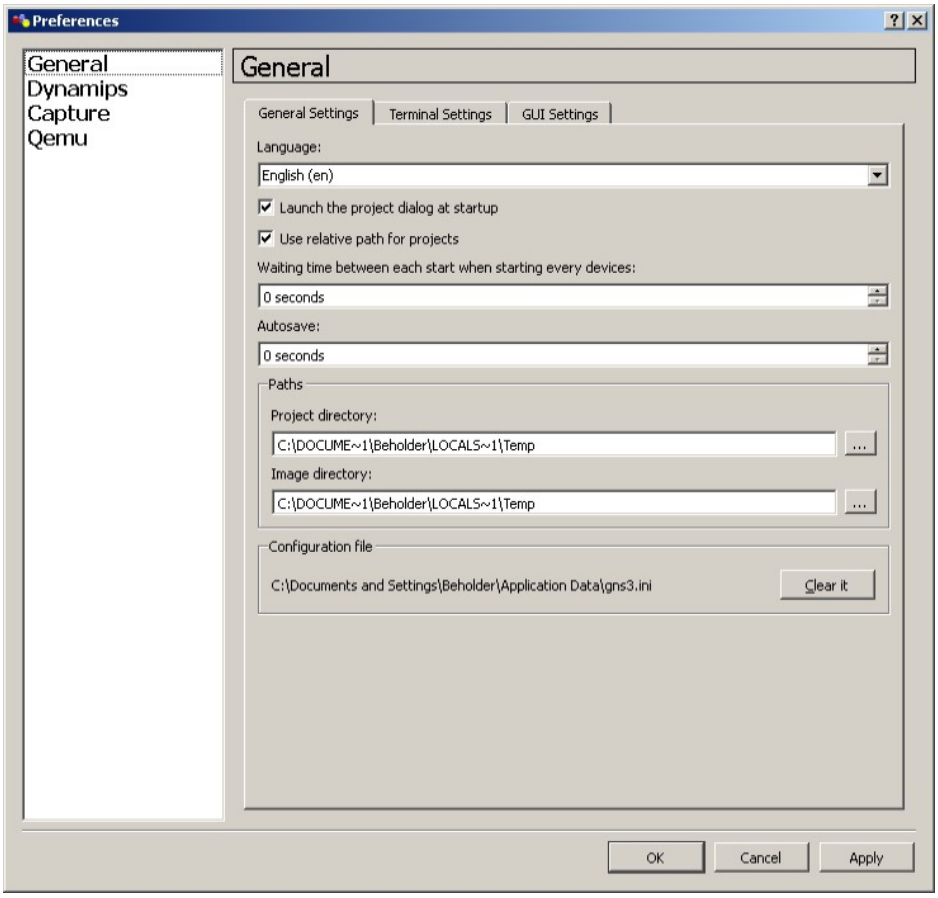

Рисунок 2 - Окно Preferences, раздел General

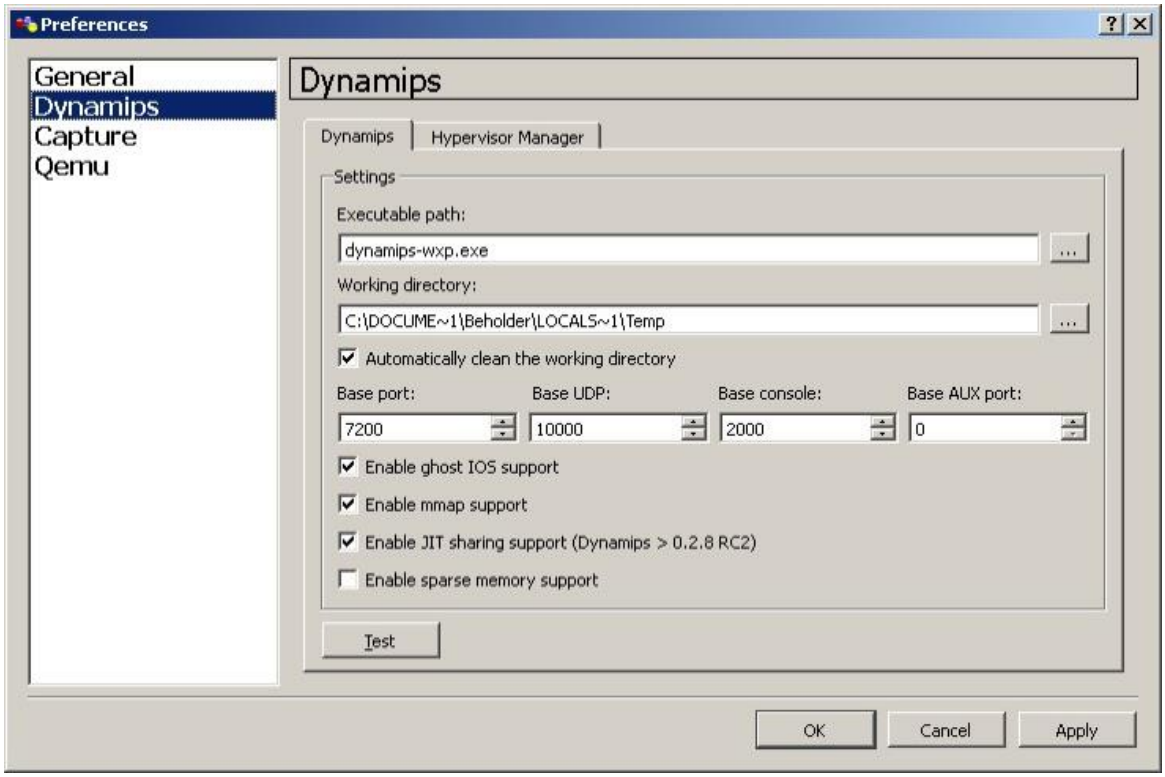

Рисунок 3 - Окно Preferences, раздел Dynamips

В разделе Capture окна настроек указываются: программа, используемая для захвата и анализа сетевого трафика, а также каталог, в котором будут сохраняться файлы с дампами трафика. Обычно для этих целей используется программа Wireshark, которая предварительно должна быть установлена на компьютере.

Эмуляция дополнительных сетевых устройств осуществляется программой виртуализации Qemu, параметры которой задаются в соответствующем разделе диалогового окна настроек (рисунок 4). Вкладка General Settings служит для настройки общих параметров программы: каталог для хранения временных файлов, пути к самой программе виртуализации Qemu, программе поддержки файловобразов (Qemu-Img) и программе взаимодействия с GNS3 (QemuWrapper). Для проверки работоспособности эмулятора следует нажать кнопку Test: в случае корректной работы будет выдано соответствующее сообщение. Остальные вкладки данного раздела связаны с настройками конкретных эмулируемых устройств.

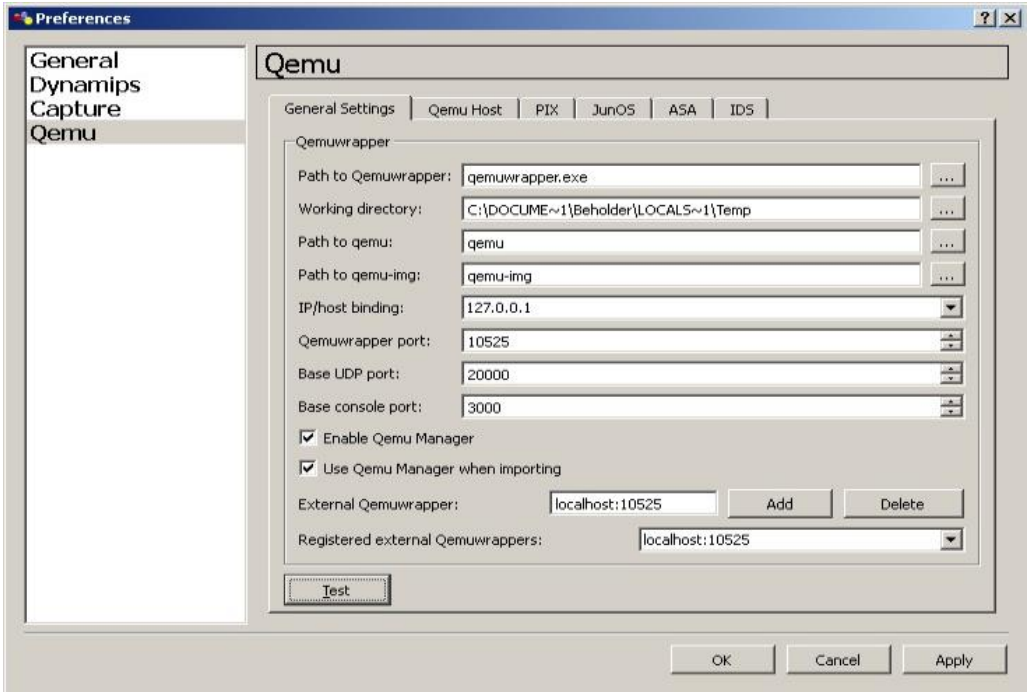

Рисунок 4 - Вкладка General Settings раздела Qemu

На вкладках поддерживаемых устройств указываются: идентификатор (некоторое имя), имя файла образа (исключение ASA, для которого задаются файлы ядра и initrd), объем оперативной памяти, количество сетевых интерфейсов и их тип

(модель), в зависимости от эмулируемого устройства дополнительные настройки и опции для запуска Qemu.

Пример конфигурации устройства PIX приведен на рисунок 5: идентификационное имя устройства Test1, используемый файл образа – pix635.bin, расположенный в корневом каталоге диска C:, 128 Мб оперативной памяти, два сетевых адаптера модели rtl8139, далее следуют специфичные для PIX параметры Key и Serial. Текущая конфигурация устройства может быть сохранена (кнопка Save), при добавлении устройства в состав сети, будет предложено выбрать имя добавляемого устройства; для удаления сохраненной конфигурации служит кнопка Delete.

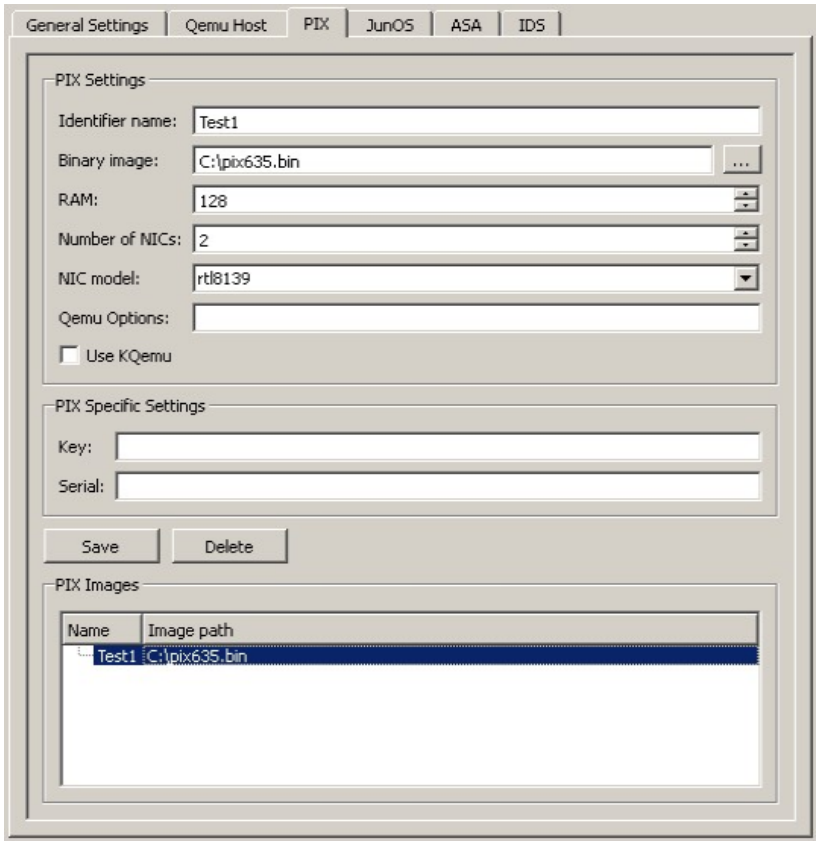

Рисунок 5 - Вкладка PIX раздела Qemu

Настройка конфигурационных параметров маршрутизаторов осуществляется через подпункт IOS images and hypervisors пункта Edit главного меню программы, а соответствующее диалоговое окно содержит две вкладки IOS images и External hypervisors (рисунок 6).

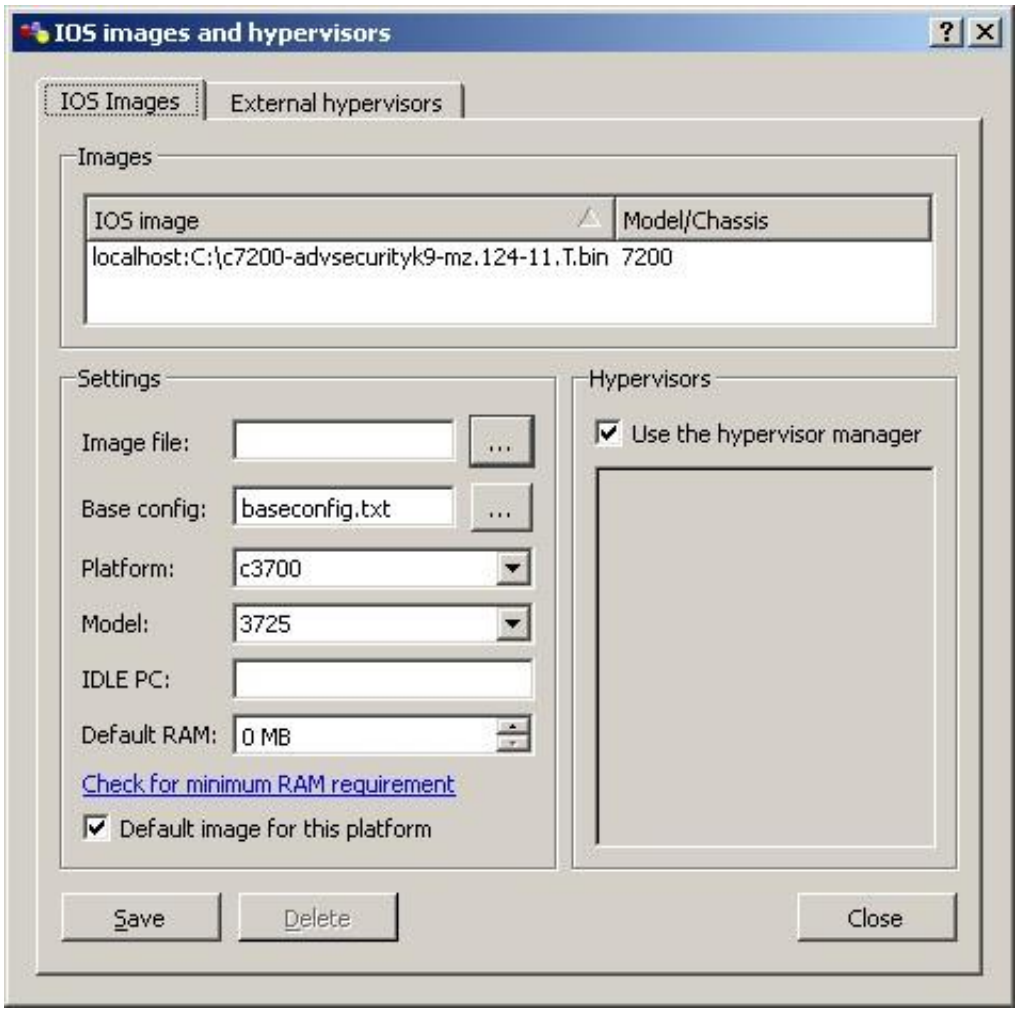

Рисунок 6 - Окно IOS images and hypervisors

Вкладка External hypervisors предназначена для настройки взаимодействия с программой dynamips, исполняющейся на другом компьютере (то есть возможна ситуация, когда пакет GNS3 запущен на одном сетевом узле, а гипервизор dynamips с соответствующими образами устройств функционирует на другом).

На вкладке IOS Images осуществляется управление конфигурациями маршрутизаторов. При конфигурировании эмулируемого устройства необходимо указать:

- имя файла образа IOS с полным путем к нему в строке ввода

Image file;

- имя файла базовой конфигурации (текстовый файл с набором команд IOS) в строке ввода Base config;
- платформу (серию) устройства в строке ввода Platform;
- конкретную модель устройства в строке ввода Model;

• поле IDLE PC не заполняется (вычисляется автоматически с использованием контекстного меню);

• объем памяти по умолчанию в строке ввода Default RAM.

При включенном (состояние по умолчанию) пункте Use the hypervisor manager на панели Hypervisors будет использован локальный гипервизор, а при выключенном данном пункте внешний гипервизор выбирается из списка, расположенного ниже на этой же панели. Список формируется автоматически при настройке внешних гипервизоров на вкладке External hypervisors.

1.2 Основные приемы создания схемы и конфигурирования устройств

Главное окно программы GNS3, отображаемое по умолчанию, с элементами пользовательского интерфейса, обозначенными цифрами, приведено на рисунке 7.

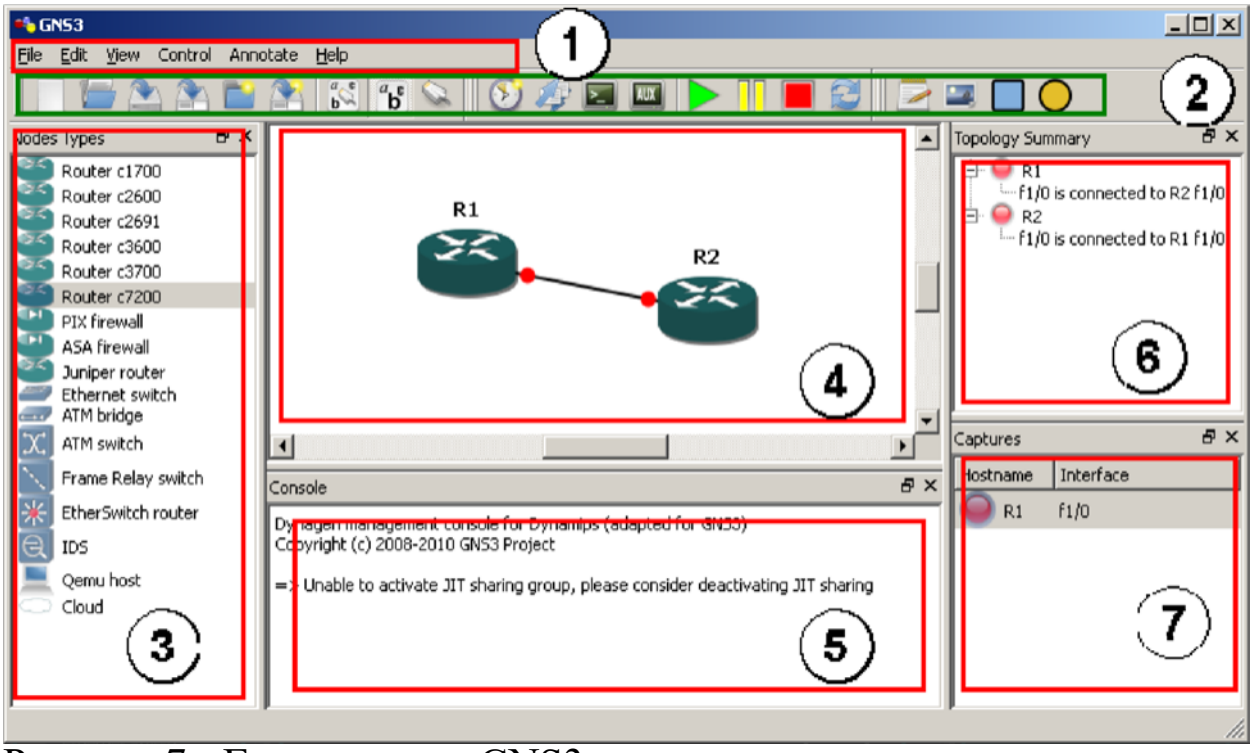

Рисунок 7 - Главное окно GNS3

Пользовательский интерфейс программы состоит из следующих основных элементов:

- меню программы (1);
- панель инструментов, содержащая ярлыки для быстрого доступа к часто используемым элементам меню программы (2);
- окно выбора типа сетевого устройства (3);
- окно логической схемы эмулируемой компьютерной сети (рабочая область) (4);
- окно консоли управления эмулятором маршрутизаторов (5);
- окно топологии сети, отображающее состояние объектов сети и связи между ними (6);
- окно управления захватом трафика, отображающее точки съема сетевого трафика (7).

Чтобы добавить устройство в схему сети необходимо из области выбора устройства переместить соответствующий объект в рабочую область. Если для данного типа устройств предусмотрено несколько конфигураций и ни одна из них не указана как конфигурация по умолчанию, то программа предложит выбрать желаемую из списка имеющихся.

Находящееся в рабочей области устройство можно перемещать с помощью левой кнопки мышки, нажатой на его пиктограмме. Нажатие правой кнопки мышки вызывает контекстное меню, которое зависит от типа устройства. Пример контекстного меню для маршрутизатора приведен на рисунке 8.

Рисунок 8 - Контекстное меню маршрутизатора

Для всех типов устройств в контекстном меню определен пункт Configure, при выборе которого появляется диалоговое окно, позволяющее произвести дополнительную настройку устройства. Пример диалогового окна с дополнительными настройками для маршрутизатора приведен на рисунке 9.

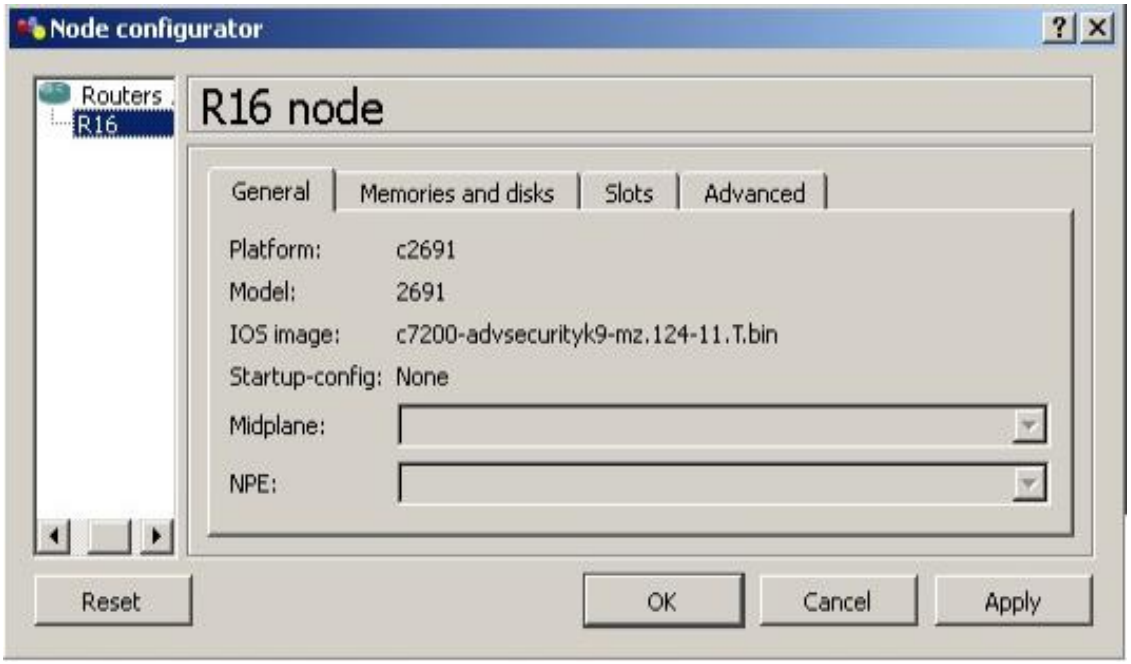

Рисунок 9 - Окно дополнительных параметров настройки устройства

Диалоговое окно для устройства маршрутизатор имеет четыре вкладки:

- General содержит общую информацию об устройстве и используемом образе IOS;
- Memories and disks задает размер памяти RAM, доступной на устройстве, размер NVRAM, а также размер дисков, если таковые есть в устройстве;
- Slots используется наиболее часто. На этой вкладке можно выбрать, какие сетевые модули, и в какие доступные слоты устройства будут подключены;
- Advanced – на вкладке можно задать значение конфигурационного регистра (управляющего загрузкой маршрутизатора), размер области исполнения, процент памяти, зарезервированный под буферы ввода-вывода.

Среди объектов, расположенных в окне сетевых устройств, есть объект Cloud (Облако), позволяющий осуществлять сетевое взаимодействие между объектами, функционирующими в среде GNS, и «внешними» по отношению к ним сетевыми узлами. В частности, Облако может быть «подключено» напрямую к реальному или виртуальному сетевому интерфейсу, что дает

возможность включить в состав эмулируемой сети реальные компьютеры или виртуальные образы ОС, например, VMware.

Для построения сетевых связей между устройствами, входящими в состав эмулируемой сети, необходимо в панели инструментов выбрать ярлык Add link, после нажатия на который, появится контекстное меню с выбором типа физического соединения (Ethernet, Serial и т. п.). После выбора типа соединения программа переходит в режим построения физических связей, курсор принимает вид крестика, и любое нажатие левой клавишей мыши на объект схемы осуществляет подключение соответствующего устройства к соединению, а повторное нажатие отключает его. Последовательное нажатие на двух различных устройствах, приводит к созданию соединения между ними. Для выхода из режима построения физических связей необходимо еще раз нажать на ярлык Add link. Среди поддерживаемых типов соединений есть тип Manual, при выборе которого пользователь может указывать между какими портами (интерфейсами) устройств следует установить соединение.

Устройства и соединения из текущей схемы компьютерной сети удаляются однотипным образом: либо из контекстного меню, либо с помощью клавиши Delete.

1.3 Операционная система Cisco IOS

На сегодняшний день одним из ведущих игроков на рынке программно-аппаратных комплексов для организации защиты периметра компьютерных сетей является корпорация Cisco, которая разработала межсетевую операционную систему, поддерживаемую не только оборудованием самой фирмы Cisco, но и продуктами других ведущих производителей сетевого оборудования. Межсетевая операционная система Cisco IOS (Cisco Internetwork Operating System) обеспечивает высокий уровень сетевых возможностей, защищенности сети, качества сервисных услуг, простоты использования и управляемости сетевым оборудованием. Данная операционная система является общим ПО для широкого круга продуктов Cisco.

Операционная система Cisco IOS устанавливается на маршрутизаторы таких корпораций, как, например, Compaq и Hewlett Packard. Cisco планирует дальнейшее расширение возможностей IOS и распространение этой системы на всю сетевую отрасль. Поэтому изучение возможностей оборудования Cisco является актуальной задачей на сегодняшний день.

1.3.1 Способы подключения к устройству

Устройство Catalyst серии 2960 является коммутатором, который обеспечивает доступ к сети конечных пользователей, а также предоставляет расширенные функции. Коммутаторы этой серии поставляются с различной плотностью портов и некоторыми отличиями в скоростях передачи портов и разъемах, характерных для передающей среды. Один из продуктов этой серии обеспечивает связь на уровне 10/100/1000 Мбит/с с использованием медных кабелей. Внешний вид устройства изображен на рисунок 10.

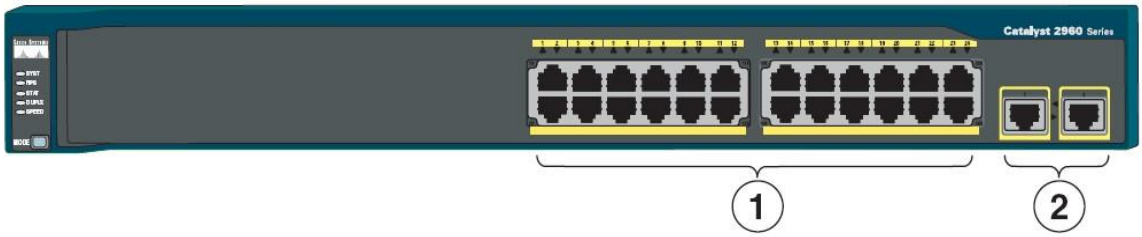

Рисунок - 10 Лицевая панель Catalyst 2960-24TT
(1 – 10/100 порты; 2 – 10/100/1000 порты)

Данный коммутатор допускает развертывание гигабитового канала к уровню доступа сети. Коммутаторы серии 2960 обеспечивают перенаправление пакетов второго уровня, а также обладают множеством таких же возможностей, что и коммутаторы Catalyst серии XL: установка магистрального соединения и создание EtherChannel-каналов. Кроме того, коммутаторы этой серии добавляют функции безопасности третьего и четвертого уровней с использованием списков доступа (Access Control Lists – ACL) для VLAN-сетей, а также улучшенную классификацию и

планирование качества обслуживания, основанные на информации третьего и четвертого уровней.

Коммутатор, как правило, настраивается в командной строке ОС Cisco IOS. Подсоединение к нему осуществляется по протоколу Telnet на IP-адрес любого из его сетевых интерфейсов или с помощью любой терминальной программы через последовательный порт компьютера, связанный с консольным портом устройства (рисунок 11).

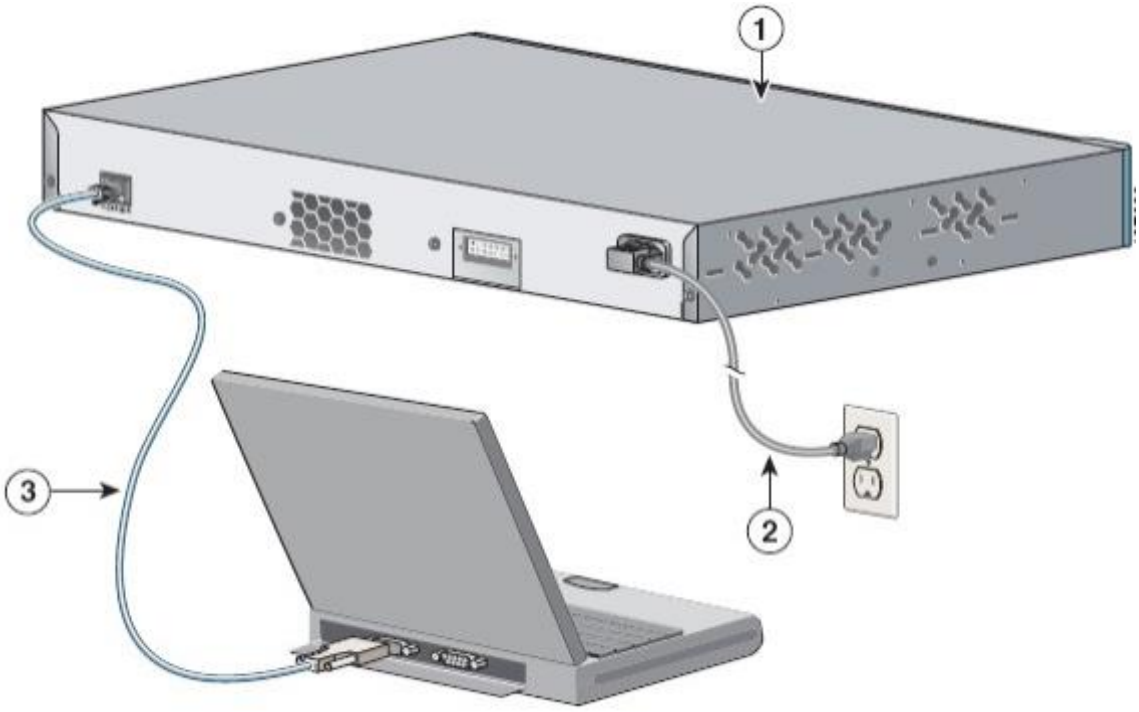

Рисунок - 11 Подключение по консольному кабелю

На рисунок 11 изображена схема подключения по консольному порту: на тыльной стороне коммутатора Catalyst серии 2960 (1) расположены силовой разъем для подключения шнура питания (2) и консольный порт (3), обеспечивающий подключение к COM-порту компьютера администратора посредством кабеля RJ-45-to-DB-9.

Последний способ предпочтительнее, потому что в процессе настройки оборудования могут измениться параметры физического порта или административного IP-интерфейса, что приведет к потере соединения, установленного по протоколу Telnet.

ВЫПОЛНИТЬ!

1. В GNS3 переместить на рабочую область устройство Cisco 3725 и подключить модуль NM-16ESW.

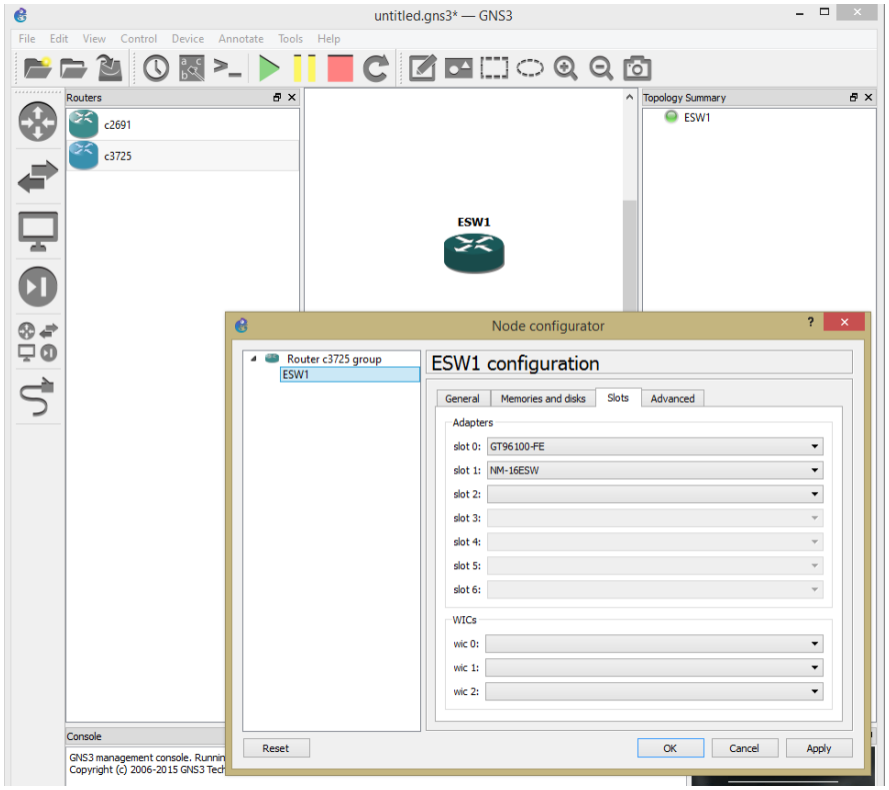

Рисунок 12 – Добавление устройства

GNS3 не имеет полноценной поддержки эмуляции L2 коммутаторов, поэтому вместо образа 2960 используется образ 3750.

Следует иметь в виду, что аварийное отключение консоли не регистрируется оборудованием, и сеанс остается в том состоянии, в котором находился на момент отключения. При повторном подключении пользователь окажется в том же контексте (если только не сработал автоматический выход в контекст пользователя по таймеру неактивности). Напротив, при разрыве Telnet-соединения коммутатор закрывает сеанс работы.

1.3.2. Контексты командной строки

В операционной системе Cisco IOS имеются два основных пользовательских режима для администрирования коммутатора и

несколько других режимов, позволяющих контролировать конфигурацию устройства. В дополнение к различным режимам программное обеспечение Cisco ISO обеспечивает такие функции, как интерактивная справка и редактирование командной строки, которые позволяют взаимодействовать с коммутатором в административных целях.

1) Пользовательский EXEC-режим.

Switch>

Пользователям предоставляется возможность подключаться к коммутатору посредством консольного порта или Telnet-сеанса. Стандартно при первоначальном доступе к коммутатору пользователь входит в пользовательский EXEC-режим (user EXEC), в котором предоставляется ограниченный набор команд. При подключении к коммутатору может потребоваться пароль пользовательского уровня.

ВЫПОЛНИТЬ!

2. На компьютере Laptop 1 в закладке Desktop запустить приложение Terminal с параметрами по умолчанию. Нажмите [Enter] для входа в пользовательский режим.

2) Привилегированный EXEC-режим.

Switch> enable Switch#

После того как пользователь получает доступ к пользовательскому EXEC-режиму, можно применить команду enable для входа в привилегированный EXEC-режим (privileged EXEC), который предоставляет полный доступ ко всем командам ОС. Для того чтобы покинуть привилегированный EXEC-режим, используется команда disable (возврат в пользовательский режим) или exit.

ВЫПОЛНИТЬ!

3. Перейти в привилегированный режим.

3) Конфигурационный режим.

Switch#configure terminal Switch(config)#

Войти в конфигурационный режим можно из привилегированного EXEC-режима. В режиме конфигурации можно вводить любые команды для настройки функций коммутатора, которые доступны в программном образе

операционной системы IOS. Любая команда конфигурации вступает в действие немедленно после ввода (а не после возврата в контекст администратора).

Конфигурационный режим организован иерархически. Режим глобальной конфигурации (global configuration mode) содержит команды, которые влияют на коммутатор в целом. В режиме конфигурирования интерфейса (interface configuration mode) администратору предоставляются команды, позволяющие настраивать интерфейсы коммутатора в зависимости от настраиваемого ресурса.

Для перехода со специфического уровня конфигурирования на более общий вводится команда exit. Для того чтобы покинуть режим глобальной конфигурации и вернуться в привилегированный EXEC-режим необходимо ввести команду exit. Для того чтобы покинуть любой конфигурационный режим и вернуться в привилегированный EXEC-режим, применяется команда end или комбинация клавиш [Ctrl]+[z].

Вид приглашения командной строки в контекстах конфигурирования, которые будут встречаться наиболее часто: Switch(config)# – глобальный;

Switch(config-if)# – интерфейса;

Switch(config-line)# – терминальной линии.

ВЫПОЛНИТЬ!

5. Перейти в режим глобального конфигурирования и обратно в привилегированный.

4) Режим конфигурирования базы данных VLAN-сетей (устаревший, использовать не рекомендуется).

Switch# vlan database Switch(vlan)#

Перейти в указанный режим можно из привилегированного EXEC-режима. После ввода команды появится приглашение режима конфигурирования базы данных VLAN-сетей (vlan database mode). В данном режиме с помощью команд vlan (и/или vtp) конфигурируются и модифицируются VLAN- и VTP-параметры. После внесения изменений в базу данных VLAN они не вступят в

действие до тех пор, пока не будет введена команда apply для активизации изменений в базе данных или команда exit, которая позволяет активизировать изменения и покинуть режим. Команда abort отменяет какие-либо сделанные изменения в базе данных и позволяет покинуть рассматриваемый режим конфигурирования. Кроме того, существует возможность просмотреть текущее состояние базы данных и предполагаемые изменения, используя команды группы show.

Необходимо запомнить вид приглашений командной строки (изображены в прямоугольнках) во всех вышеуказанных контекстах и команды перехода из контекста в контекст (изображены над стрелками), это поможет при настройке коммутатора (рисунок 1.18).

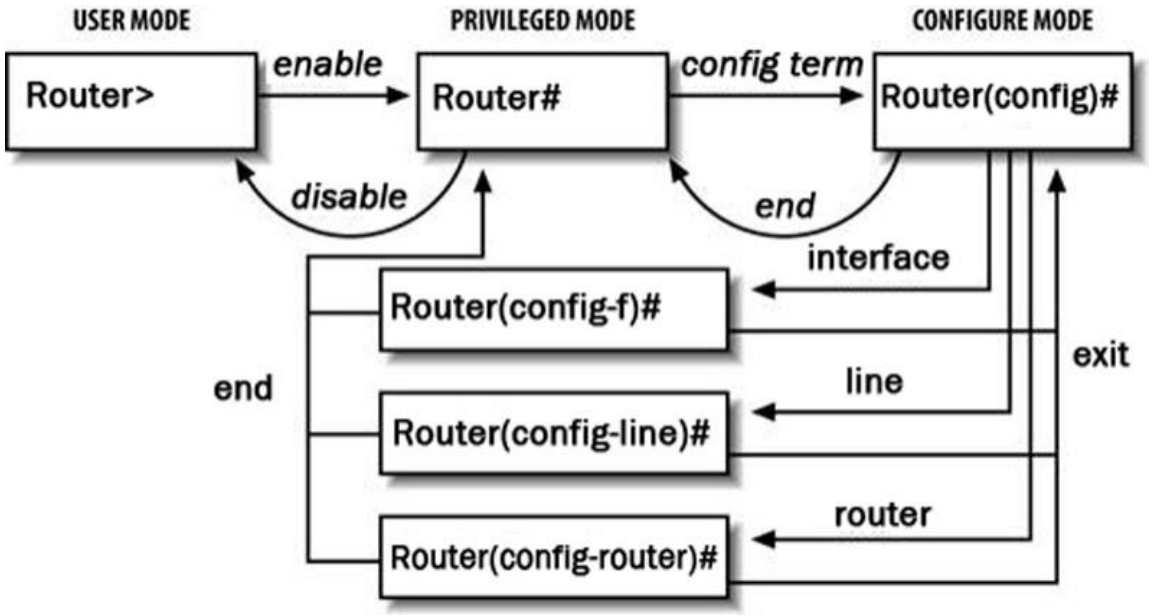

Рисунок 13 - Схема контекстов Cisco IOS (пример для маршрутизатора)

ВЫПОЛНИТЬ!

6. Осуществить переход в представленные контексты Cisco IOS.
7. Просмотреть список команд каждого контекста с помощью команды ?.

1.3.3 Ввод команд

Команды IOS вводятся в соответствующем режиме (режим EXEC, глобальной конфигурации, конфигурации интерфейса, подинтерфейса, режим конфигурирования базы данных VLAN-сетей и т. д.). Для активизации какой либо функции или параметра следует напечатать собственно команду и ее опции и нажать [Enter]. Отмена любой команды (отключение опции или режима, включаемых командой, снятие или удаление параметров, назначаемых командой) производится исполнением этой же команды, набранной с префиксом no, например:

Switch(config-if)#shutdown – отключить интерфейс;

Switch(config-if)#no shutdown – включить интерфейс. Команды и параметры можно сокращать и вводить в виде нескольких букв, количество которых достаточно для того, чтобы аббревиатура не была двусмысленной. Например, для того чтобы войти в режим конфигурации интерфейса FastEthernet 0/0, команду interface FastEthernet 0/0 можно ввести в сокращенном виде: int fa0/0.

Сокращенные команды можно вывести в полном виде последующим нажатием клавиши [Tab]. Название команды расширяется до ее полной формы, если сокращение не является двусмысленным.

Для выполнения в режиме глобального конфигурирования (не покидая его) команд привилегированного EXEC-режима используется команда do, параметром которой является конечная команда.

В случае некорректного синтаксиса команды, возвращается сообщение об ошибке «Invalid input detected at '^' marker» (обнаружена ошибка в позиции маркера '^'). Знак ^ появляется ниже соответствующего символа командной строки, в позиции которого обнаружена синтаксическая ошибка.

Редактировать текст в командной строке можно, перемещая курсор с помощью клавиш [стрелка вправо] и [стрелка влево]. Если вводятся дополнительные символы, то знаки справа сдвигаются.

Для внесения изменений можно использовать клавишу [Backspace].

ВЫПОЛНИТЬ!

8. Выполнить в привилегированном EXEC-режиме несколько команд группы show, используя сокращенную запись команд.

9. Выполнить в режиме глобального конфигурирования несколько команд группы show, используя команду do.

1.3.4. Контекстная справка

Чтобы получить дополнительную информацию о командах используется команда ? (знак вопроса), причем, в любой позиции командной строки. Если в строке напечатан только знак вопроса, будут отображены все возможные для данного режима команды. Знак вопроса может вводиться в любой позиции после команды, ключевого слова или параметра. Знак вопроса, введенный после пробела, позволяет отобразить все доступные ключевые слова или параметры. Если знак вопроса вводится без пробела после другого слова, отображаются все доступные команды, начинающиеся с данной подстроки. Эта функция может быть полезной в случае, когда сокращенная команда является двусмысленной или воспринимается как ошибочная:

router#? – список всех команд данного контекста с комментариями;

router#co? – список всех слов в этом контексте, начинающихся на «co»;

router#conf ? – список всех параметров, которые могут следовать за командой config.

ВЫПОЛНИТЬ!

10. Выполнить несколько команд группы show, используя встроенную справочную систему.

1.3.5 Хронологический список команд

Ранее введенные команды для возможности быстрого повторного вызова помещаются в буфер. Размер буфера (журнала команд) для текущего терминального сеанса, определяется следующей командой:

Switch# terminal history size N, где N – число запоминаемых команд.

Для установки размера журнала всех сеансов на линии используется команда:

Switch(config-line)# history size N.

Для повторного вызова ранее введенных команд в любом режиме работы интерфейса командной строки служат клавиши [стрелка вверх] (предыдущая) и [стрелка вниз] (следующая). Вызванные из хронологического списка команды можно редактировать как введенные с клавиатуры. С помощью команды show history на экране отображается журнал записанных команд.

ВЫПОЛНИТЬ!

11. Осуществить настройку истории команд терминального сеанса, назначив буферу максимально возможный размер.

12. Просмотреть хронологический список команд каждого контекста.

1.3.6 Просмотр, сохранение и загрузка конфигурации

При загрузке коммутатора или маршрутизатора IOS считывает команды конфигурации из памяти NVRAM, где они хранятся в виде текстового файла. Конфигурация, сохраненная в NVRAM, называется начальной или стартовой (startup config). Таким образом, при загрузке ОС в оперативной памяти устройства создается копия начальной конфигурации – текущая или рабочая конфигурация (running config). В процессе работы устройства администратор может вводить дополнительные конфигурационные команды, в результате чего текущая конфигурация становится отличной от начальной.

Просмотр начальной и текущей конфигураций коммутатора производится в контексте администратора с помощью команд:

Switch#show startup-config Switch#show running-config. Стоит отметить, что вывод последней команды полностью описывает текущую конфигурацию устройства. Однако многие параметры коммутатора имеют значения по умолчанию и если

администратор не менял эти значения, они в конфигурации не отображаются.

ВЫПОЛНИТЬ!

13. Сравнить начальную и текущую конфигурации коммутатора.

Для того чтобы при последующей загрузке коммутатора не потерять все внесенные изменения в конфигурации устройства, необходимо скопировать текущую конфигурацию коммутатора в стартовую с помощью команды:

Switch#copy running-config startup-config.

ВЫПОЛНИТЬ!

14. Сохранить текущую конфигурацию коммутатора.

Конфигурация устройства может сохраняться на TFTP-, FTP- или WEB-сервере либо загружаться с этих серверов. Для этого надо знать IP-адрес сервера и имя сохраняемого или загружаемого файла, они будут запрошены после ввода команды. Для перезагрузки ОС коммутатора используется команда: Switch#reload.

ВЫПОЛНИТЬ!

15. Перезагрузить ОС коммутатора.

1.3.7 Просмотр информации о коммутаторе

При начальном запуске или при перезагрузке процедура POST выводит диагностические и информационные сообщения, если во время тестирования POST обнаруживаются ошибки, они выводятся на консоль. После успешного завершения POST на коммутаторе Catalyst 2960 появится приглашение для запуска программы начальной конфигурации коммутатора (Packet Tracer работает иначе). Программа автоматической установки может использоваться для задания IP-параметров коммутатора, имени хоста и кластера, паролей, а также для создания конфигурации по умолчанию. Позднее можно будет использовать интерфейс командной строки для изменения конфигурации.

ВЫПОЛНИТЬ!

16. Внимательно изучить вывод данных начальной загрузки коммутатора и ответить на вопросы.

– Модель коммутатора?
– Процессор?
– Базовый MAC-адрес?
– Версия Cisco IOS?
– Имя и расположение файла образа ОС?
– Количество интерфейсов Fast Ethernet?
– Количество интерфейсов Gigabit Ethernet?

17. С помощью команды show version вывести информацию о коммутаторе (команда выполняется как в пользовательском, так и в привилегированном режиме). Сравнить вывод команды с информацией, выводимой при загрузке устройства.

1.3.8 Создание начальной конфигурации

Как отмечалось ранее, программа начальной конфигурации (команда setup) предоставляет быстрый метод конфигурирования устройства Cisco:

Switch#setup.

Для создания более сложных и специализированных конфигураций необходимо использовать интерфейс командной строки, войдя в режим конфигурации терминала.

ВЫПОЛНИТЬ!

18. Произвести начальную настройку с использованием команды setup, ответив на все вопросы по мере их появления, как показано ниже:

Continue with configuration dialog? [yes/no]: yes
Would you like to enter basic management setup? [yes/no]: no
First,would you like to see the current interface summary[yes]:no
Enter host name [Switch]: 2960
Enter enable secret: enable Enter
enable password: pass
Enter virtual terminal password: terminal

Configure SNMP Network Management? [no]:no Do you want to configure Vlan1 interface? [no]:no

Do you want to configure FastEthernet0/1 interface? [no]:no Do you want to configure FastEthernet0/2 interface? [no]:no …

Do you want to configure FastEthernet0/24 interface? [no]:no Do you want to configure GigabitEthernet1/1 interface? [no]:no

Do you want to configure GigabitEthernet1/2 interface? [no]:no

Would you like to enable as a cluster command switch? [yes/no]:no

19. По завершении создания начальной конфигурации команда setup выведет содержимое сгенерированного файла на экран и предложит сохранить в память NVRAM – выбрав вариант (2), сохранить результаты своей работы. Новая подсказка системы 2960# свидетельствует о том, что изменения вступили в силу.

20. Отобразить текущую и стартовую конфигурации.

21. Внимательно изучить содержимое файлов конфигурации и проверить результат работы команды setup.

22. Перезагрузить ОС коммутатора.

Вопросы для проверки знаний

1. Какие существуют способы подключения к сетевому оборудованию для управления им?
2. Какие существуют контексты командной строки IOS и каковы возможности администрирования каждого из них?
3. Каково назначение конфигурационных файлов сетевых устройств фирмы Cisco?
4. Для чего используется команда Setup?

Библиографический список

1. Защита информации в компьютерных сетях. Практический курс : учеб. пособие / А. Н. Андрончик, В. В. Богданов, Н. А. Домуховский [и др.] ; под ред. Н. И. Синадского. – Екатеринбург : УГТУ-УПИ, 2008. – 248 с.

2. Americas Headquarters Cisco Security MARS Initial Configuration and Upgrade Guide, Release 6.x. – USA : Cisco Systems, 2009. – 136 p.

3. Gary Hallen, G. Kellogg Security Monitoring with Cisco Security MARS. – USA : Cisco Press, 2007. – 335 p.

4. James Burton, Ido Dubrawsky, Vitaly Osipov Cisco Security Professional's Guide to Secure Intrusion Detection Systems. – USA : Syngress Publishing, 2003. – 673 p.

5. Installation Guide for the Cisco Secure PIX Firewall Version 5.2. [Электронный ресурс]. Режим доступа: http://www.cisco.com.

6. Install and Setup Guide for Cisco Security Monitoring Analysis and Response System. Release 4.3.x., 2008. [Электронный ресурс]. Режим доступа: http://www.cisco.com.

7. Стивенс У. Р. Протоколы TCP/IP. Практическое руководство / пер. с англ. – СПб. : БХВ-Петербург, 2003. – 672 с.

8. Кульгин М. Практика построения компьютерных сетей. Для профессионалов. – СПб. : Питер, 2001. – 320 с.