

**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ
ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»**

МЕТОДИЧЕСКИЕ УКАЗАНИЯ
по выполнению лабораторных работ
по дисциплине «Проектирование элементов защищенных телекоммуникационных систем»
для студентов направления подготовки
10.03.01 Информационная безопасность
Направленность (профиль)
«Организация и технологии защиты информации (по отрасли или в сфере
профессиональной деятельности)»

Ставрополь,
2026

СОДЕРЖАНИЕ

Введение

Тема 1-2: Общие сведения о сетевых технологиях. Ethernet-совместимые технологии. Лабораторная работа № 1-4 «Основы конфигурирования в командной строке IOS»

Тема 3-4: Функции маршрутизаторов. Протоколы сетевого уровня. Лабораторная работа № 5-8 «Конфигурирование сетевых устройств фирмы Cisco»

Тема 5-6: Основы конфигурирования маршрутизаторов. Конфигурирование маршрутизации. Лабораторная работа № 9-12 «Меж сетевое экранирование с использованием технологий фирмы Cisco»

Тема 7: Сетевые фильтры. Лабораторная работа № 13-16 «Обнаружение сетевых компьютерных атак»

Тема 8: Безопасность коммутаторов. Лабораторная работа № 17-18 «Обнаружение комплексных компьютерных атак»

ВВЕДЕНИЕ

Целью изучения дисциплины «Проектирование элементов защищенных телекоммуникационных систем» является изучение методов и средств построения и эксплуатации сетевых технологий для обеспечения информационной безопасности на объекте, а также изучение основных подходов к разработке, реализации, эксплуатации, анализу, сопровождению и совершенствованию технологий защиты передачи информации, а также приобретение профессиональных компетенций будущего бакалавра по направлению подготовки 10.03.01 «Информационная безопасность».

Задачами дисциплины являются:

1. Обучение студентов систематизированным представлениям о принципах построения, функционирования и применения аппаратных средств современной вычислительной техники;
2. Изложение основных теоретических концепций, положенных в основу построения современных компьютеров, вычислительных систем, сетей и телекоммуникаций;
3. Подготовка к профессиональной деятельности по построению, проектированию и эксплуатации программно-аппаратных технологий защиты передачи информации.

2. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесённых с планируемыми результатами освоения образовательной программы

Код, формулировка компетенции	Код, формулировка индикатора	Планируемые результаты обучения по дисциплине (модулю), характеризующие этапы формирования компетенций, индикаторов
ПК-5 Способен проводить работы по установке и техническому обслуживанию защищённых технических средств обработки информации (06.034 В)	ИД-2 _{ПК-5} Способен к проведению работ по техническому обслуживанию защищённых технических средств обработки информации	-использует программные (программно-технические) средства защиты автоматизированных систем от несанкционированного доступа к информации и специальных программных воздействий на нее -применяет методы контроля защищенности информации от несанкционированного доступа и специальных программных воздействий

ПЛАНЫ ЛАБОРАТОРНЫХ РАБОТ

Лабораторная работа № 1-4

Тема 1-2: Общие сведения о сетевых технологиях Ethernet-совместимые технологии

Наименование задания: «Основы конфигурирования в командной строке IOS»

Цель: IOS.

Формируемые компетенции: ПК-5

Теоретическая часть:

Программа лабораторной работы

1. Cisco Packet Tracer.
2. Cisco GNS3.
3. Cisco IOS.

Основы моделирования компьютерной сети в Cisco Packet Tracer

Общие сведения о программе

Для освоения сетевых технологий и получения начального уровня навыков работы с сетевым оборудованием, фирмой Cisco был разработан программный продукт Cisco Packet Tracer.

Пакет Cisco Packet Tracer – это инструмент, предоставляющий возможность имитировать как работу некоторого набора сетевых устройств (маршрутизаторы, коммутаторы, точки беспроводного доступа, персональные компьютеры, сетевые принтеры, IP-телефоны и т. д.), так и сетевое взаимодействие между ними (распространение пакетов по сети).

Так как данное программное обеспечение лишь имитирует функционирование реальных устройств и сетевое взаимодействие между ними, то существуют определенные ограничения и условности в работе поддерживаемых устройств и сетевых протоколов (доступны не все команды Cisco IOS). Вместе с тем Packet Tracer предоставляет пользователю определенную возможность изменения аппаратной части имитируемых устройств, например, для маршрутизаторов и коммутаторов существует возможность установки дополнительных сетевых модулей (HWIC, WIC и NM), а для компьютеров – выбора сетевого адаптера с поддержкой той или иной среды передачи. В зависимости от типа устройства программа предоставляет определенные возможности по его конфигурированию и соответствующий набор программного обеспечения, например, для маршрутизаторов и коммутаторов единственное доступное ПО – это Cisco IOS, для ПК – это командная строка, простейший web-браузер и т. п.

Cisco Packet Tracer поддерживает два режима работы: режим реального времени (Real-Time Mode) и имитационный (Simulation Mode). В первом режиме пользователь работает с сетью в реальном масштабе времени. Режим имитации позволяет пользователю «замораживать» сеть, наблюдать перемещение данных по сети, изменение параметров IP-пакетов при прохождении их через сетевые устройства. Анализ событий, происходящих в сети, в этом режиме

позволяет изучать алгоритмы функционирования сетевых устройств и протоколов и обнаруживать узкие места и проблемы.

Помимо этого с помощью Cisco Packet Tracer пользователь может разработать не только логическую организацию сети, но и ее физическую модель, а, следовательно, получить навыки проектирования ее топологических связей. Схему компьютерной сети можно разрабатывать с учетом плана реально существующего здания или даже города, проектировать ее кабельную систему с учетом физических ограничений, таких как длина и тип прокладываемого кабеля или радиус зоны покрытия беспроводного сегмента сети.

Элементы пользовательского интерфейса

Главное окно программы Cisco Packet Tracer с основными элементами пользовательского интерфейса, обозначенными цифрами, представлено на рис. 1.1.

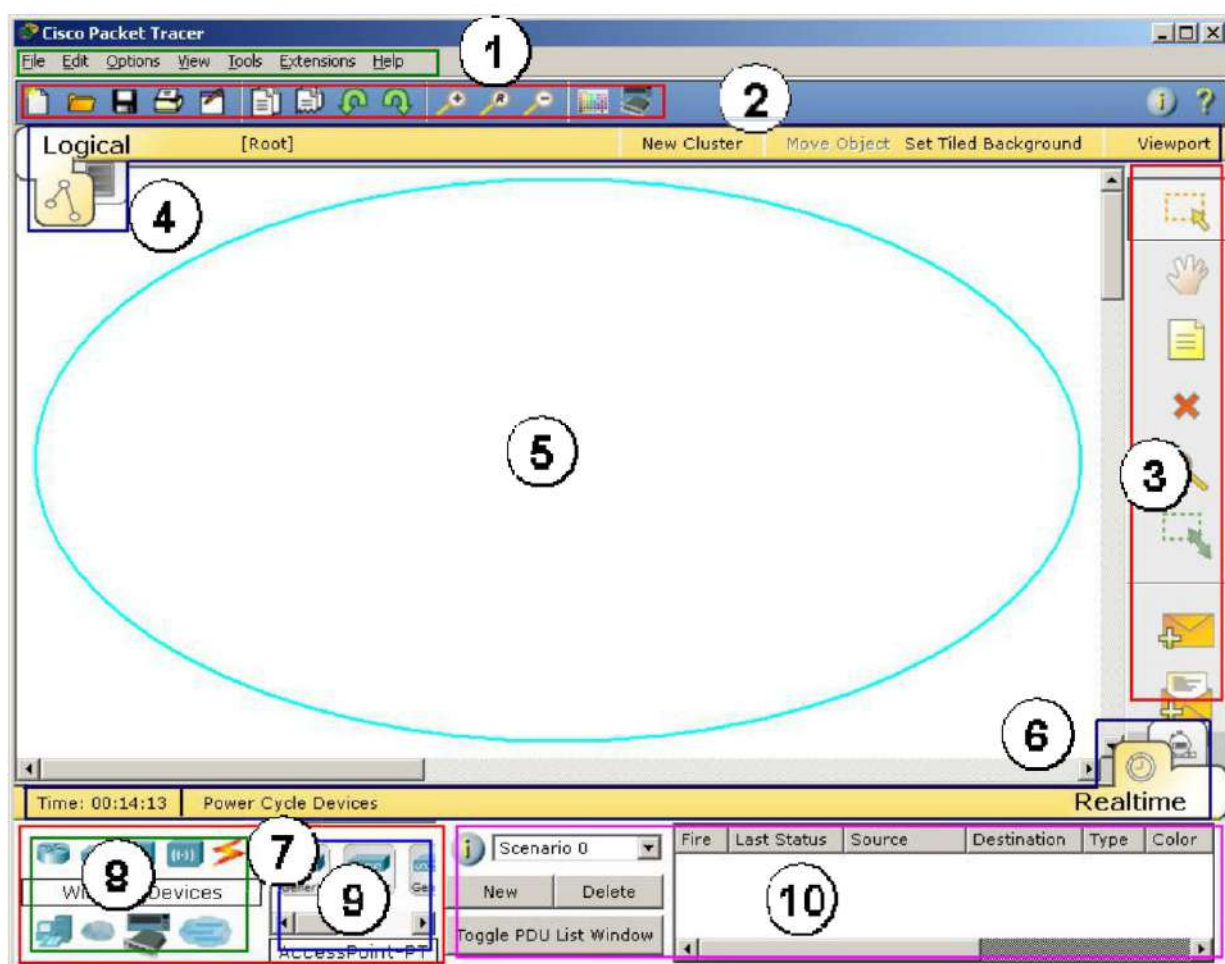


Рис. 1.1. Главное окно Cisco Packet Tracer

Пользовательский интерфейс программы включает в себя следующие элементы:

- Menu Bar (1) – меню с пунктами File, Edit, Options, View, Tools, Extensions, Help для доступа к функциям программы;
- Main Tool Bar (2) – панель инструментов, содержащая пиктограммы для доступа к часто используемым элементам меню;
- Common Tools Bar (3) – панель инструментов рабочей области: кнопки сверху вниз: Select, Move Layout, Place Note, Delete, Inspect, Resize Shape, Add Simple PDU и Add Complex PDU;
- Logical/Physical Workspace and Navigation Bar (4) – переключатель вида рабочей области: физический или логический. В зависимости от используемого вида на панели располагаются дополнительные кнопки: для логической схемы сети – кнопки для создания кластеров (New Cluster), позволяющих объединить устройства в один объект, и навигации между ними; для физического представления – кнопки, позволяющие создать новые объекты типа город, здание, серверная, и отобразить координатную сетку;
- Workspace (5) – основное рабочее пространство, в котором происходит создание сети, визуализация передачи сетевого трафика между устройствами и т. д.;
- Realtime/Simulation Bar (6) – переключатель между режимами Realtime и Simulation. В обоих режимах на соответствующей панели присутствуют часы, отображающие относительное время, и кнопка сброса питания (Power Cycle Devices). В режиме имитации добавляются кнопки управления сетевым трафиком (Play Controls): Back, Auto Capture/Play и Capture/Forward и кнопка Event List, позволяющая просматривать события в сети (отправку, получение пакетов и т. п.);
- Network Component Box (7) – область, в которой выбираются устройства и кабели для размещения их в рабочем пространстве. В ней в свою очередь находятся панели Device-Type Selection и Device-Specific Selection;
- Device-Type Selection Box (8) – панель выбора типа устройств и соединений, содержащая доступные типы устройств и кабелей в Packet Tracer;
- Device-Specific Selection Box (9) – панель выбора устройства, используемая для выбора конкретного устройства или соединения, необходимого для создания сети в рабочем пространстве. Вид панели изменяется в зависимости от выбранного типа устройств;

- User Created Packet Window (10) – окно управления сетевым трафиком пользовательского сценария.

Основные приемы создания схемы и конфигурирования устройств

Для создания логической схемы компьютерной сети необходимо добавить сетевые устройства в рабочую область. Чтобы это сделать, следует на панели выбора типа устройств (Device-Type Selection) указать категорию добавляемого устройства, затем пиктограмму необходимого устройства можно либо переместить с панели выбора конкретного устройства (Device-Specific Selection) в рабочую область, либо, выбрав ее, нажать левую кнопку мыши в рабочей области программы. На рис. 1.2 приведен пример, когда в качестве добавляемых устройств выбраны маршрутизаторы (Routers).



Рис. 1.2. Список устройств в категории Routers

Для быстрого создания нескольких экземпляров одного и того же устройства следует, удерживая кнопку Ctrl, нажать на пиктограмму устройства в области выбора конкретного устройства и отпустить кнопку Ctrl. После этого нажатие левой кнопки мыши в рабочей области будет приводить к добавлению нового устройства или соединения.

После того как устройства добавлены, их необходимо соединить друг с другом кабелем соответствующего типа. Выбор типа кабеля, осуществляется аналогично выбору устройства, используя категорию «соединения» (connections). Далее необходимо указать, какие два устройства будут соединены. При подключении кабеля программа попросит выбрать доступный порт. Существует специальный тип соединения, который автоматически выбирает тип кабеля, но с ним связаны определенные проблемы: при соединении пользователь не может указать порты, а программа сама выбирает их согласно приоритетам, например, если на маршрутизаторах есть

Serial и Ethernet порты, то предпочтительным будет соединение через Serial порты.

Как отмечалось ранее, у большинства добавляемых устройств может быть дополнительно сконфигурирована аппаратная часть. Кроме этого, Packet Tracer предоставляет интерфейс для конфигурирования сетевой части устройств (назначение IP-адресов, включение/выключение интерфейсов, назначение ID VLAN и т. п.). Для доступа к параметрам конфигурации устройства необходимо щелкнуть левой кнопкой мыши на его пиктограмме: появится окно с вкладками, содержимое которых зависит от типа выбранного устройства. Пример окна конфигурирования маршрутизатора приведен на рис. 1.3.

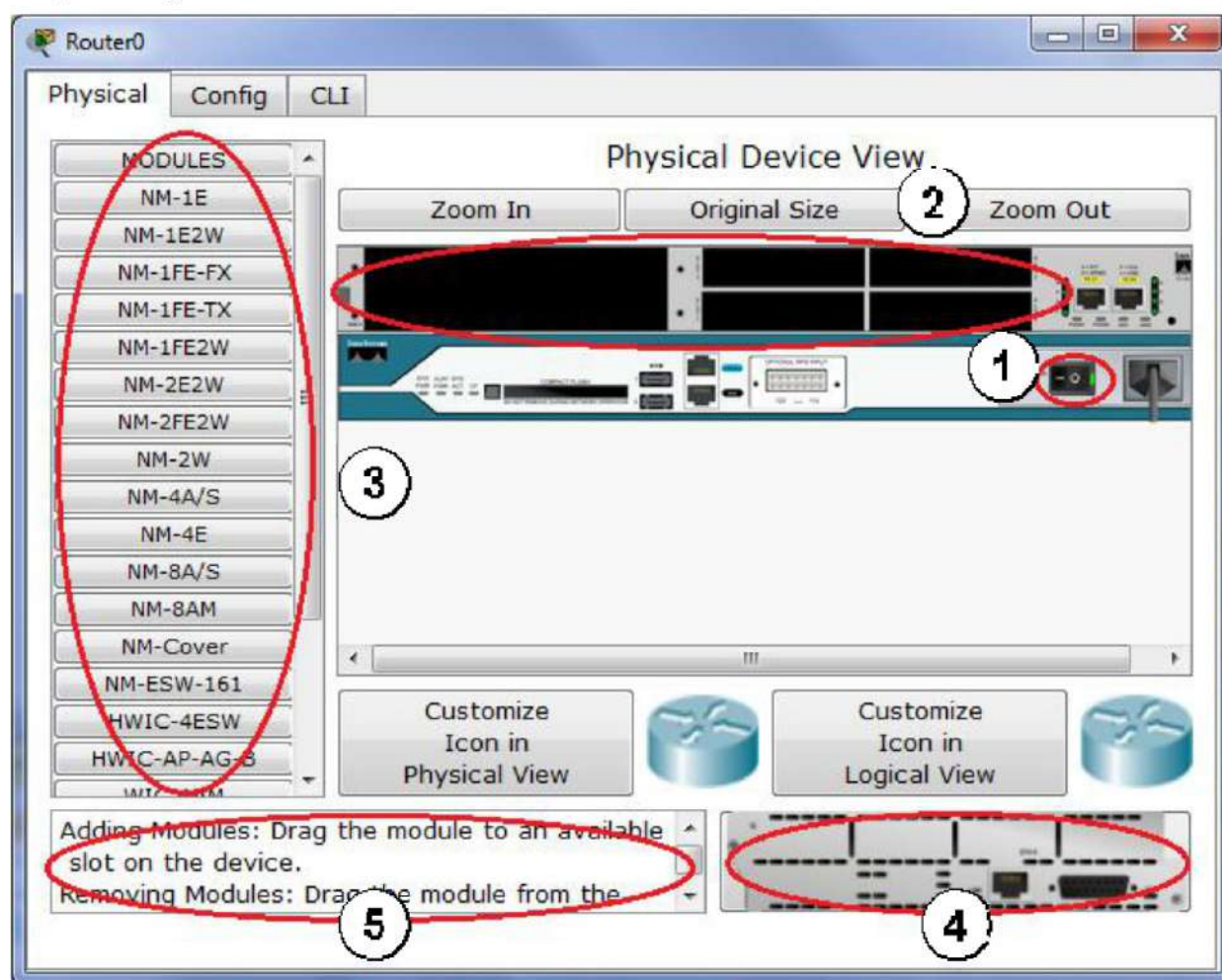


Рис. 1.3. Окно конфигурирования устройства, вкладка Physical

В зависимости от типа устройства могут присутствовать следующие вкладки: Physical, Config, CLI, Desktop.

На вкладке Physical (см. рис. 1.3) изображено устройство со слотами расширения, если таковые присутствуют в нем (2).

Выключатель питания (1) позволяет включить или выключить устройство. Если устройство включено, то нельзя изменить его аппаратную часть (добавить/удалить модули), если устройство выключено – нельзя получить доступ к вкладкам Config, CLI, Desktop. На вкладке может присутствовать список дополнительных модулей (3), поддерживаемых устройством. Если выбрать какой-либо модуль, то в нижней части вкладки будет отображено его краткое описание (5) и внешний вид (4). Для того чтобы добавить модуль в устройство, его необходимо переместить мышкой в соответствующий слот расширения из списка (3), либо из области внешнего вида модуля (4).

Вкладка Config позволяет настроить параметры функционирования устройства в целом, сетевых служб (DNS, DHCP, TFTP и т. п.) и его интерфейсов, не прибегая непосредственно к его штатным средствам настройки (например, для маршрутизатора). Пример вкладки Config для устройства Server0 приведен на рис. 1.4:

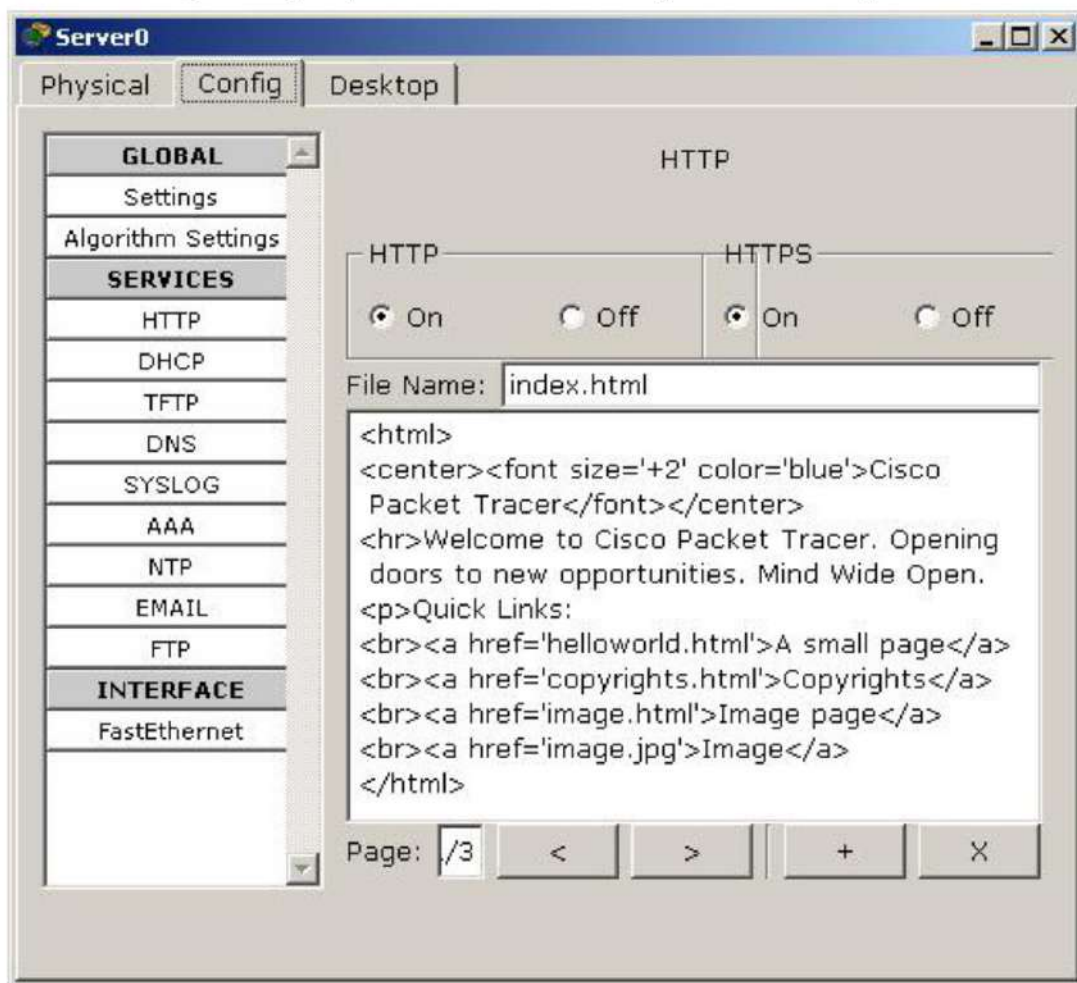


Рис. 1.4. Окно конфигурирования устройства, вкладка Config

Вкладка Desktop предоставляет доступ к программному обеспечению, доступному пользователю на конечном устройстве (PC, Server). На рис. 1.5 приведен пример вкладки Desktop для компьютера PC.



Рис. 1.5. ПО устройства, вкладка Desktop

Так как данное ПО является имитацией реальных утилит ОС, оно имеет упрощенный интерфейс и ограниченный набор функций, в основном ориентированный на работу с сетью, например, из 17 команд доступных в командной строке (Command Prompt) только 4 не имеют отношения к работе с сетью.

Для таких сетевых устройств как «Маршрутизатор» или «Коммутатор» вкладка Desktop заменяется на CLI, предоставляющую доступ пользователя к командной строке Cisco IOS. Набор доступных команд и параметров уступает их количеству на реальном устройстве: присутствуют основные, часто используемые команды, либо позволяющие освоить основные моменты тех или иных концепций и принципов, заложенных в работу сетей, сетевых протоколов и устройств.

Сводную информацию (состояние портов, IP- и MAC- адреса и т. п.) об устройстве, находящемся в рабочей области, можно получить, наведя на него указатель мышки. Кнопка Inspect (увеличительное стекло) на панели инструментов рабочей области также выводит определенную информацию об устройстве: в зависимости от типа устройства контекстное меню содержит различное количество пунктов.

Для удаления лишних устройств из рабочей области программы используется клавиша Delete (Del) или кнопка Delete на панели инструментов рабочей области.

Более подробную информацию по работе с программой и описание ее пользовательского интерфейса можно найти в справочной системе, поставляемой в виде набора html-страниц.

Эмулятор оборудования Cisco GNS3

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 (Dynamips), эмулятора ОС маршрутизаторов (Dynamips) и программы виртуализации хост-машин (модифицированный Qemu). GNS3 предоставляет графический интерфейс построения схемы сети и доступа к Dynamips, 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 виртуа-

лизации 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 (рис. 1.6). 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.

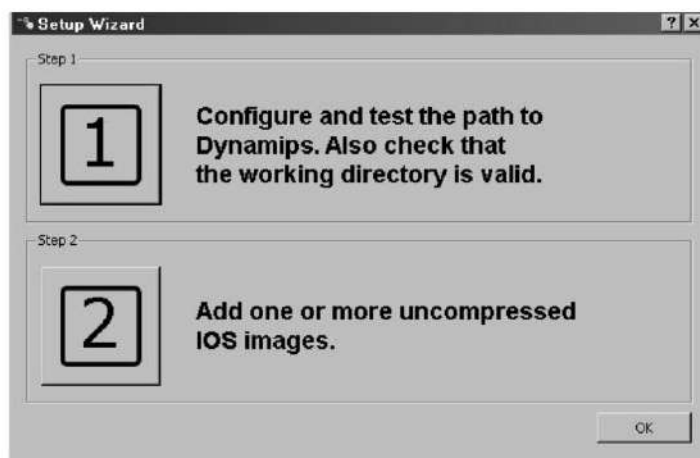


Рис. 1.6. Мастер настройки GNS3

При настройке программы в разделе General (рис. 1.7), прежде всего, указываются пути к каталогам хранения образов IOS различных устройств и пользовательских файлов-проектов.

В разделе Dynamips указываются параметры настройки эмулятора (рис. 1.8), 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.

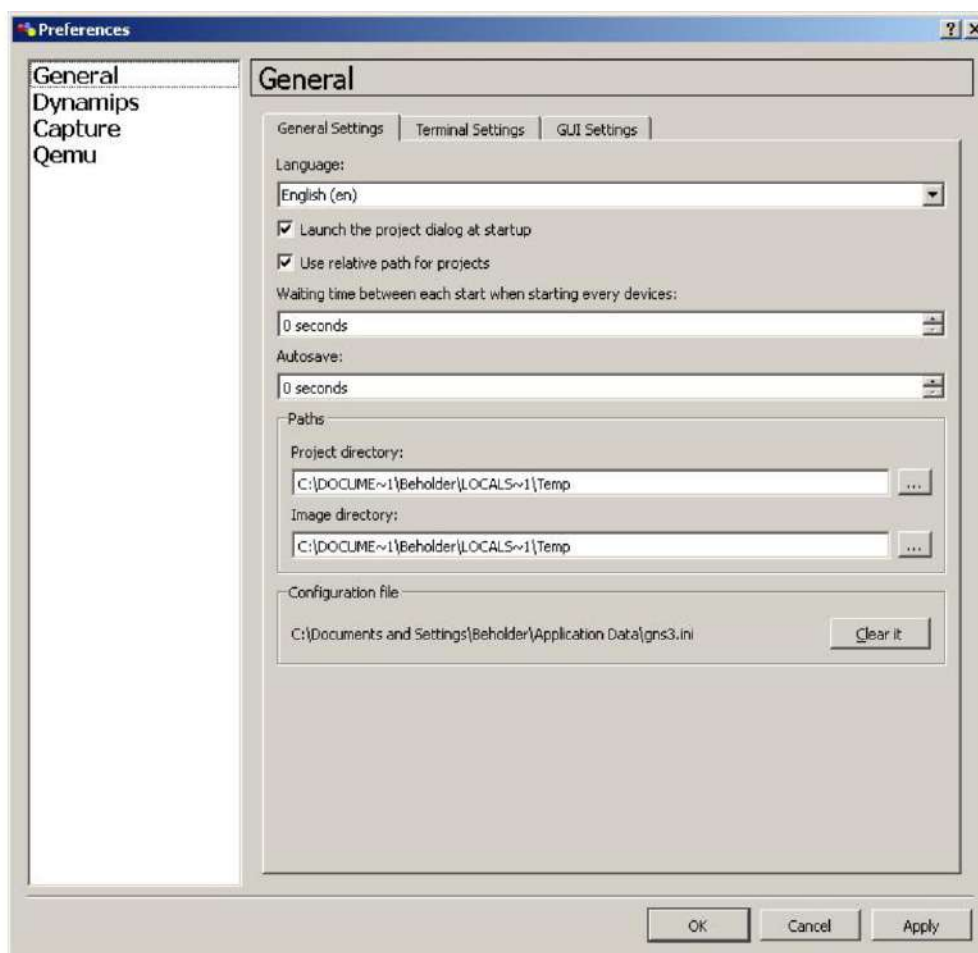


Рис. 1.7. Окно Preferences, раздел General

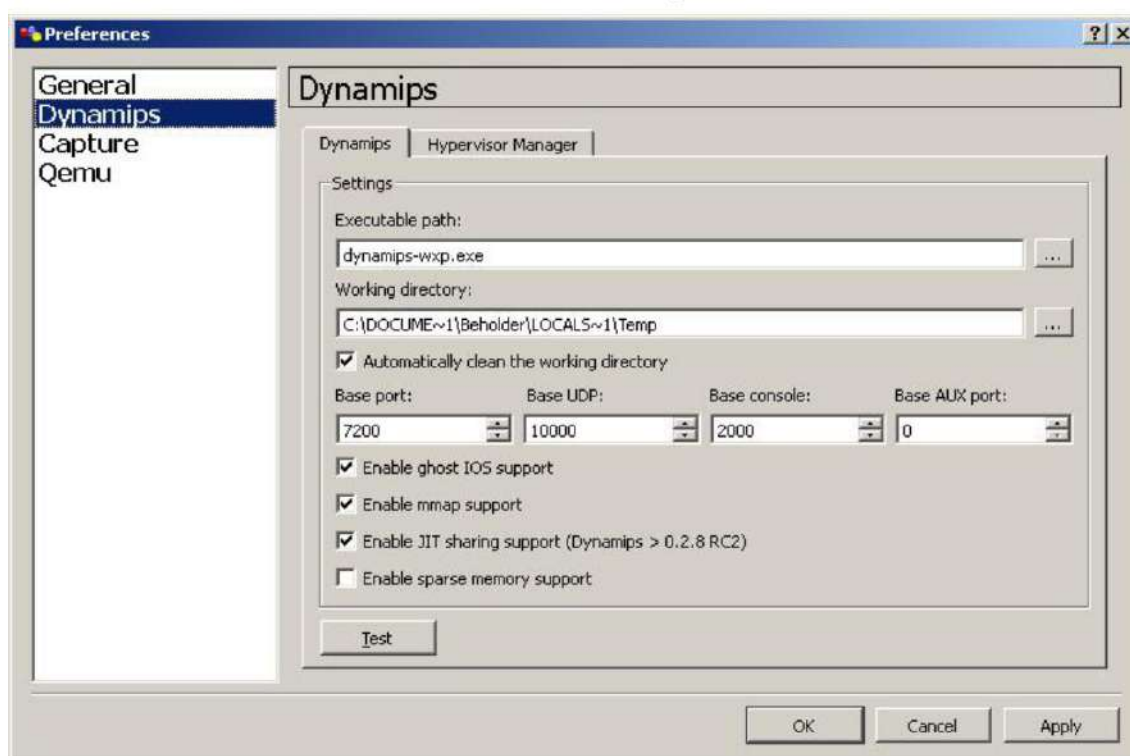


Рис. 1.8. Окно Preferences, раздел Dynamips

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 (рис. 1.9). Вкладка General Settings служит для настройки общих параметров программы: каталог для хранения временных файлов, пути к самой программе виртуализации Qemu, программе поддержки файлов-образов (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.

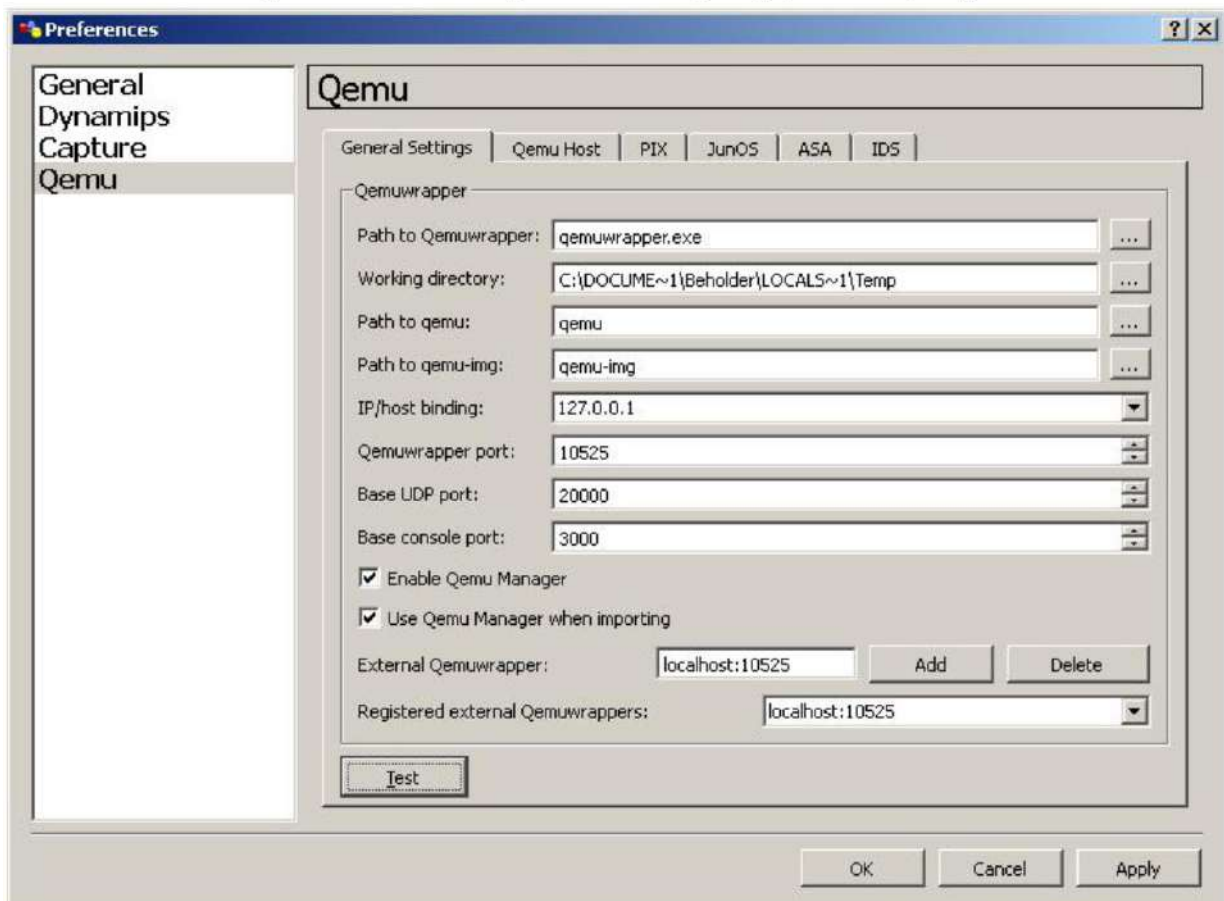


Рис. 1.9. Вкладка General Settings раздела Qemu

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 рис. 1.10: 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.

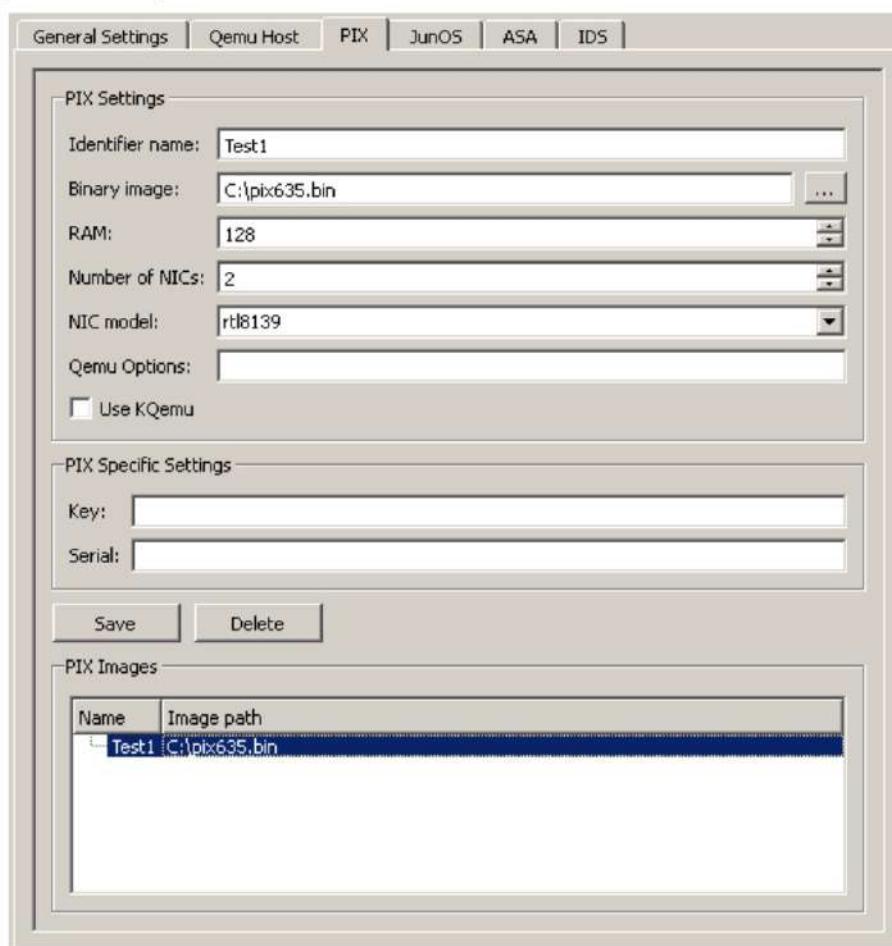


Рис. 1.10. Вкладка PIX раздела Qemu

Настройка конфигурационных параметров маршрутизаторов осуществляется через подпункт IOS images and hypervisors пункта Edit главного меню программы, а соответствующее диалоговое ок-

но содержит две вкладки IOS images и External hypervisors (рис. 1.11).

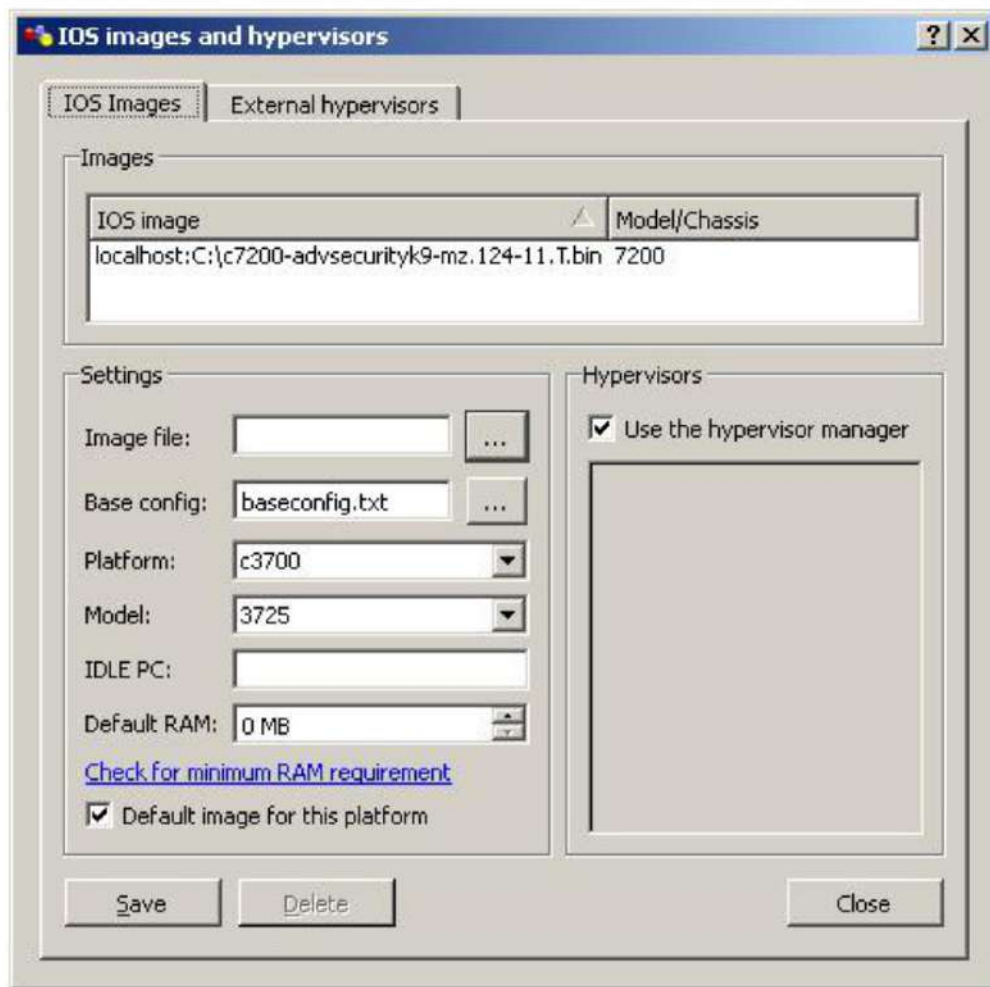


Рис. 1.11. Окно IOS images and hypervisors

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.

Основные приемы создания схемы и конфигурирования устройств

Главное окно программы GNS3, отображаемое по умолчанию, с элементами пользовательского интерфейса, обозначенными цифрами, приведено на рис. 1.12.

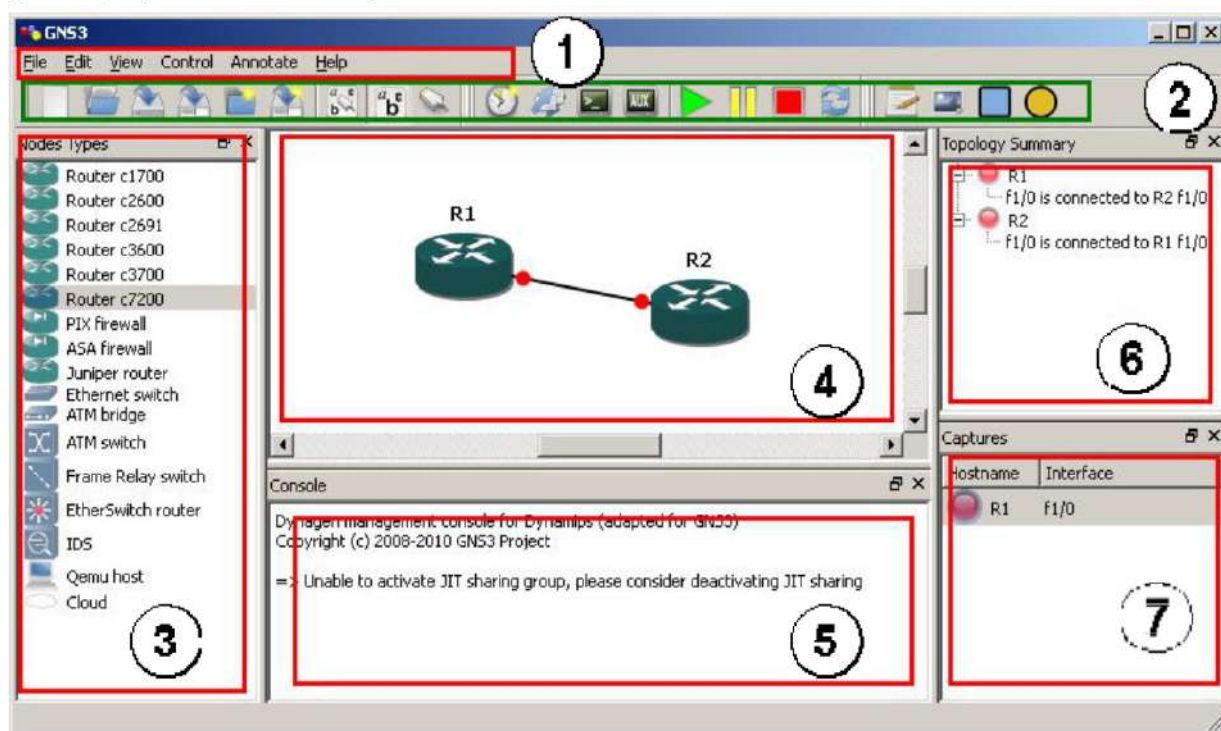


Рис. 1.12. Главное окно GNS3

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 рис. 1.13.



Рис. 1.13. 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 рис. 1.14.



Рис. 1.14. 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.

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 операци-

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.

Для того чтобы проводить эксперименты с различными возможностями ОС Cisco IOS, выполняя лабораторные работы, предлагается использовать программный пакет эмуляции сети Cisco Packet Tracer.

ВЫПОЛНИТЬ!

1. Запустить Cisco Packet Tracer.

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 рис. 1.15.

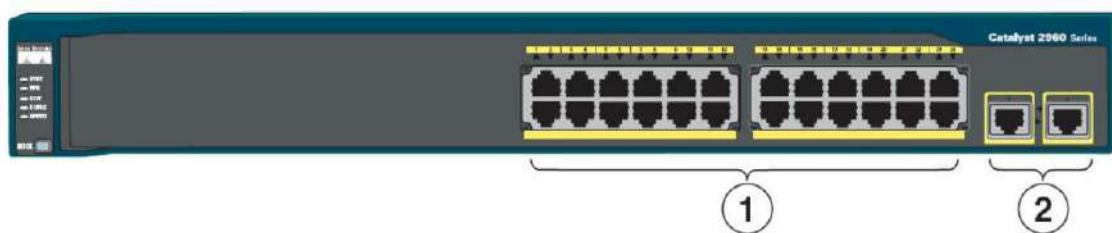


Рис. 1.15. Лицевая панель Catalyst 2960-24TT
(1 – 10/100 порты; 2 – 10/100/1000 порты)

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 онная система является общим ПО для широкого круга продуктов Cisco.

Список литературы, рекомендуемый к использованию по данной теме.

Основная: 1,2

Дополнительная: 1, 2,3

Интернет-ресурсы: 1, 2, 3, 4

Лабораторная работа № 5-8

Тема 3-4: Функции маршрутизаторов. Протоколы сетевого уровня

Наименование задания: «Конфигурирование сетевых устройств фирмы Cisco»

Цель: Cisco.

Формируемые компетенции: ПК-5

Теоретическая часть:

Конфигурирование коммутаторов

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 **vtty**.
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.

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 $1 \div 1000$ и расширенный – $1025 \div 4096$). 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 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 0/5
```

```
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 0/5 - 8
```

ВЫПОЛНИТЬ!

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

17. Назначить порты fa0/11 – 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 PC0–PC4, подсоединить их к соответствующим портам коммутатора, назначить им IP-адреса согласно схеме, приведенной на рис. 2.1.

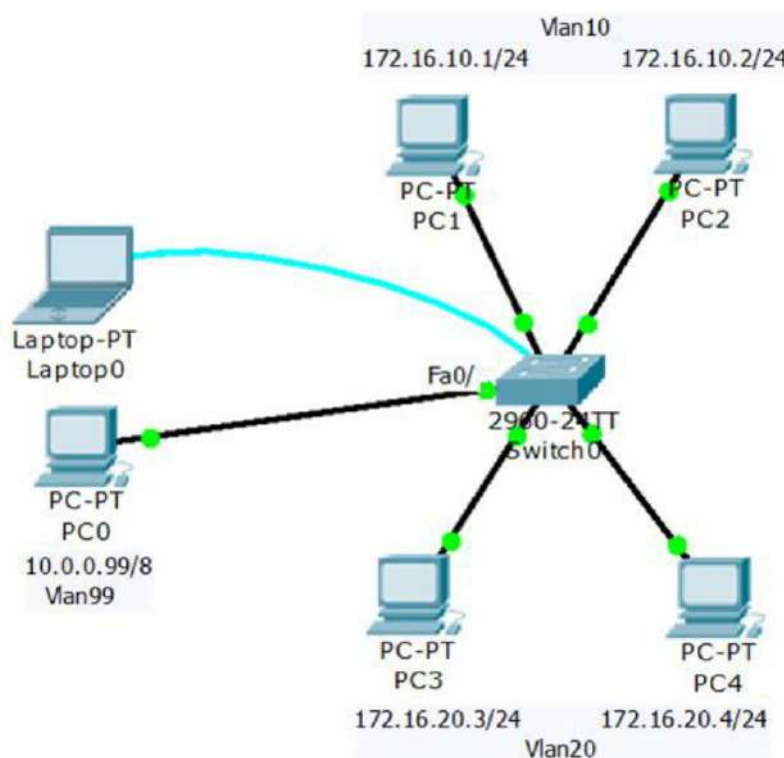


Рис. 2.1. Схема сети с VLAN99, VLAN10 и VLAN20

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 VLAN-сетей взаимодействие между компьютерами возможно, а между сетями нет.

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.

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 — динамиче-  
ские 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 fa1/17):

```
Switch(config)#mac-address-table static  
1111.2222.3333 vlan 99 int fa1/17.
```

ВЫПОЛНИТЬ!

32. Добавить статические записи о компьютерах PC2 и PC4.
33. Выполнить команды **ping** на PC1 в адрес PC2 и на PC3 в адрес PC4.
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 11-11-22-22-33-33 в Vlan номер 99 на интерфейсе fa1/17):

```
Switch(config)#no mac-address-table static  
1111.2222.3333 vlan 99 int fa1/17.
```

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 Port-security – функция коммутатора, позволяющая указать MAC-адреса узлов, которым разрешено передавать свои данные через определенный порт. После этого порт устройства не передает кадры, если MAC-адрес отправителя в них не относится к разрешенным.

Просмотр состояния функции port-security осуществляется с помощью команд:

Switch#show port-security — отображает общую информацию о функции port-security на интерфейсах коммутатора;

Switch#show port-security interface fa0/1 — отображает подробную информацию о функции port-security на указанном интерфейсе;

Switch#show port-security address — отображает информацию о записях таблицы разрешенных MAC-адресов функции port-security.

Для поддержки функции port-security на определенном интерфейсе коммутатора вначале необходимо явно перевести его в режим доступа (**Switch(config-if)#switchport mode access**), а затем использовать следующие команды:

Switch(config-if)#switchport port-security — включение защиты порта (соответственно, с префиксом **no** — выключение данной функции);

Switch(config-if)#switchport port-security maximum <N> — установка максимального числа адресов, одновременно используемых на порту, где N — число поддерживаемых на порту адресов (зависит от модели коммутатора), по умолчанию (если не использовать команду) устанавливается в 1;

Switch(config-if)#switchport port-security violation <action> — определяет действия в случае нарушения функции port-security. Параметр action может принимать следующие значения:

- **protect** — когда количество разрешенных MAC-адресов достигает максимального числа, настроенного на интерфейсе, кадры с неизвестным MAC-адресом отправителя отбрасываются до тех пор, пока администратором не будет удалено достаточное количество имеющихся MAC-адресов, чтобы их количество стало меньше максимального значения, или увеличено максимальное количество разрешенных адресов. Оповещений о нарушении безопасности в этом случае нет;

- **restrict** — аналогично предыдущему значению параметра, но в этом режиме при нарушении безопасности отправляются оповещение SNMP-trap, сообщение syslog и увеличивается счетчик нарушений (violation counter);

• **shutdown** — используется по умолчанию, нарушение безопасности приводит к тому, что интерфейс немедленно переводится в состояние **error-disabled**, отправляется SNMP-trap, сообщение syslog и увеличивается счетчик нарушений. Интерфейс коммутатора из состояния **error-disabled** можно вывести, введя последовательно команды **shutdown** и **no shutdown**;

Switch(config-if)#switchport port-sec mac-addr <MAC-адрес> — позволяет создать статическую запись для указанного MAC-адреса (параметр MAC-адрес указывается в нотации Cisco, например 1111.2222.3333). Если вместо адреса указать ключевое слово **sticky**, то коммутатор автоматически занесет адрес узла в конфигурацию при первом его появлении на интерфейсе и сделает эту запись статической. Если команду не использовать, то формируются динамические записи, которые при нарушении безопасности интерфейса будут удалены из таблицы функции port-security.

ВЫПОЛНИТЬ!

38. Справа от имеющейся схемы создать сеть, изображенную на рис. 2.2. Интерфейсы коммутатора FastEthernet с номерами с 1 по 5 назначить в VLAN10, с 6 по 10 — в VLAN20 и подключить Hub0 к Fa0/1, Server0 — к Fa0/2, Server1 — к Fa0/6.

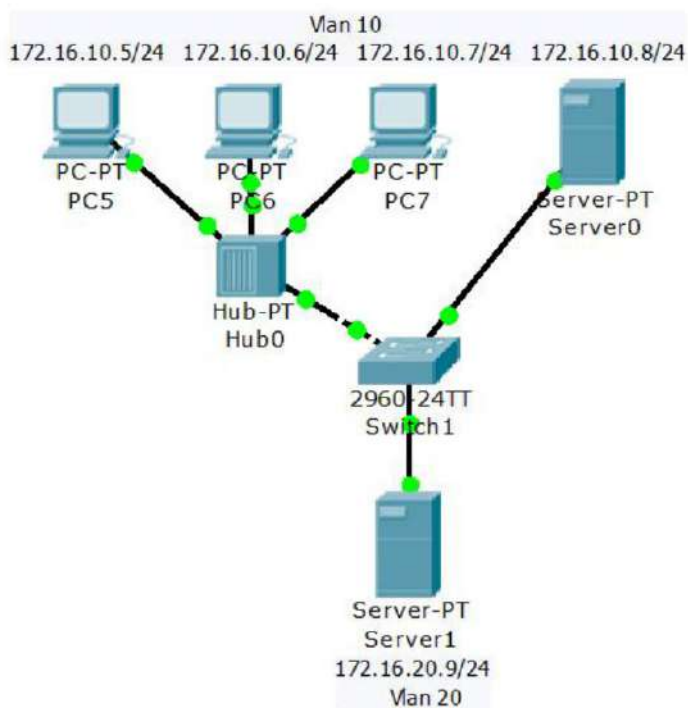


Рис. 2.2. Расширение имеющейся сети

ВЫПОЛНИТЬ!

39. Включить функцию port-security на интерфейсе FastEthernet0/1.
40. Задать на интерфейсе FastEthernet0/1 максимальное число MAC-адресов для функции port-security, равное трем.
41. Выполнить на PC5 команду **ping** в адрес узла Server0.
42. Проанализировать содержимое таблицы MAC-адресов port-security и таблицы коммутации.
43. Создать статическую запись port-security для узла PC6.
44. Выполнить команду создания статической записи port-security с параметром **sticky**.
45. Выполнить на PC7 команду **ping** в адрес узла Server0.
46. Проанализировать содержимое таблицы MAC-адресов и таблицы коммутации.
47. Отобразить общую информацию о конфигурации port-security и состоянии функции на интерфейсе FastEthernet0/1.
48. Сменить MAC-адрес сетевого адаптера на узле PC5. Если интерфейс FastEthernet0/1 коммутатора Switch1 не отключился (операция функции port-security по умолчанию), выполнить на PC5 команду **ping** в адрес узла Server0.
49. Проанализировать содержимое таблицы MAC-адресов port-security и таблицы коммутации.
50. Вывести информацию о состоянии интерфейса FastEthernet0/1 и вернуть его в рабочее состояние.
51. Выполнить на PC5 команду **ping** в адрес узла Server0.
52. Проанализировать содержимое таблицы MAC-адресов port-security и таблицы коммутации.
53. Убедиться в том, что Server0 доступен для узлов PC5, PC6, PC7.

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 ком-

мутаторах 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!

54. Соединить Switch0 и Switch1 друг с другом, используя для этого их интерфейсы GigabitEthernet1/1. У Вас должна получиться схема сети, представленная на рис. 2.3.

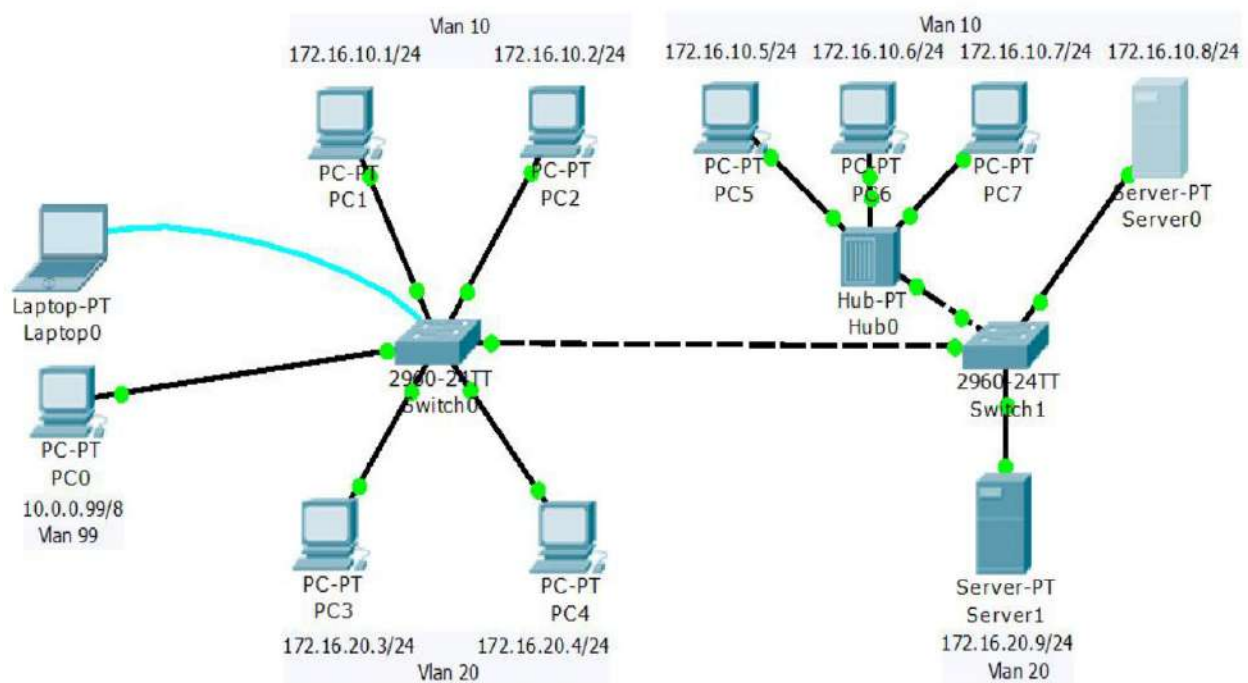


Рис. 2.3. Схема сети с магистральным каналом

ВЫПОЛНИТЬ!

55. 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|dot1Q>.
```

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>.
```

ВЫПОЛНИТЬ!

56. Перевести интерфейсы GigabitEthernet1/1 обоих коммутаторов в режим trunk.

57. Удалить неиспользуемые VLAN-сети из магистрального канала.

Для отображения информации о магистральных каналах используется команда привилегированного режима:

```
Switch#show interfaces trunk.
```

ВЫПОЛНИТЬ!

58. Вывести информацию о магистральных каналах коммутаторов.

Конфигурирование каналов EtherChannel

Для увеличения пропускной способности линий можно агрегировать несколько отдельных интерфейсов коммутатора в один логический порт (порт EtherChannel). Можно конфигурировать порты EtherChannel вручную или с помощью динамических прото-

колов. Протокол PAgP представляет собой фирменное решение фирмы Cisco, тогда как LACP (Link Aggregation Control Protocol – протокол управления агрегированием каналов) – стандартный протокол, определенный в спецификации IEEE 802.3ad. Кадры распределяются по отдельным портам, составляющим логический канал EtherChannel, с помощью алгоритма хеширования. В алгоритме могут использоваться IP-адреса отправителя, получателя, комбинации этих адресов, MAC-адреса отправителя и получателя или номера портов TCP/UDP в зависимости от аппаратной платформы и конфигурации оборудования.

Каналы EtherChannel могут быть статическими портами доступа или магистральными портами. Однако прежде чем формировать EtherChannel, всем объединяемым интерфейсам необходимо задать согласованную конфигурацию.

ВЫПОЛНИТЬ!

59. Добавить в схему сети линию связи между коммутаторами Switch0 и Switch1, используя их интерфейсы GigabitEthernet1/2.
60. Перевести интерфейсы GigabitEthernet1/2 обоих коммутаторов в режим trunk.
61. Удалить неиспользуемые VLAN-сети из созданного магистрального канала.
62. На коммутаторах Switch0 и Switch1 для интерфейсов Gi1/1 и Gi1/2 выполнить команду:
Switch(config-if)#channel-group 1 mode desirable. Данная команда создает канал EtherChannel с согласованием по протоколу PAgP.
63. Ответить на вопрос: какой интерфейс появился и привести его характеристики?

Для отображения информации о каналах EtherChannel используется команда привилегированного режима:

Switch#show etherchannel с возможностью указания дополнительных параметров.

ВЫПОЛНИТЬ!

64. Изучить возможности команды **show etherchannel**, вывести информацию о созданном канале EtherChannel и проанализировать параметры его функционирования.

Конфигурирование протокола STP

Протокол STP, основанный на стандарте мостового протокола IEEE 802.1D, обнаруживает и предотвращает формирование мостовых петель второго уровня. Параллельные маршруты в конфигурации сети могут существовать, но передача кадров допускается только по одному из них.

Коммутаторы сети запускают по одному экземпляру STP на каждую VLAN-сеть с помощью алгоритма PVST (Per-VLAN Spanning Tree – отдельные экземпляры распределенного связующего дерева для разных сетей VLAN). PVST-алгоритм требует использования между коммутаторами магистральных ISL-каналов.

Функционирование алгоритма STP и его конфигурирование на коммутаторах рассмотрим на примере упрощенной схемы сети и только для стандартной VLAN-сети с номером 1.

ВЫПОЛНИТЬ!

65. Сохранить текущую схему сети в файл для возможности ее использования в дальнейшем.

66. Создать схему сети, изображенную на рис. 2.4 (использовать интерфейсы FastEthernet).

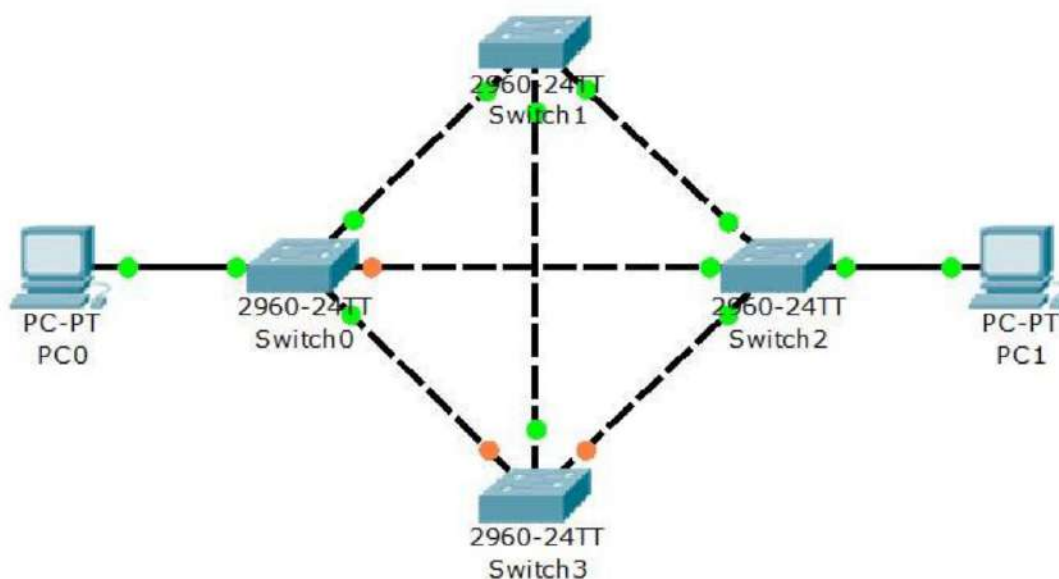


Рис. 2.4. Схема сети с избыточными линиями связи

Так как поддержка протокола связующего дерева включена по умолчанию, то по истечении некоторого времени, необходимого для отработки алгоритма STP, на графе Вашей сети будет построено связующее дерево и, несмотря на присутствующие физические петли, между любыми узлами в сети будет существовать единственный маршрут. Например, в сети, изображенной на рис. 2.4, между узлами PC0 и PC1 существует только один активный маршрут — через коммутаторы с номерами 0, 1 и 2 (в Packet Tracer заблокированные порты коммутаторов изображаются светло-коричневыми точками).

Для вывода информации о состоянии STP используются следующие команды привилегированного режима:

Switch#show spanning-tree active — на активных интерфейсах;

Switch#show spanning-tree detail — на всех интерфейсах;

Switch#show spanning-tree interface int-id — на указанном интерфейсе;

Switch#show spanning-tree vlan vlan-id — в указанной VLAN-сети;

Switch#show spanning-tree summary — вывод общей информации о состоянии STP.

ВЫПОЛНИТЬ!

67. Определить активное связующее дерево STP в Вашей сети.

Для конфигурирования протокола STP используются следующие команды режима глобального конфигурирования:

Switch(config)#spanning-tree vlan vlan-id — включение функции поддержки протокола STP (с префиксом **no** — отключение);

Switch(config)#spanning-tree mode {pvst | rapid-pvst} — выбор режима функционирования протокола;

Switch(config)#spanning-tree vlan vlan-id root {primary | secondary} — выбор основного (primary) и дополнительного (secondary) корневого коммутатора;

Switch(config)#spanning-tree vlan vlan-id priority priority – установка приоритета коммутатора, до-

пустимые значения параметра **priority** – 4096; 8192; 12288; 16384; 20480; 24576; 28672; 32768; 36864; 40960; 45056; 49152; 53248; 57344 и 61440 (по умолчанию – 32768).

Кроме приведенных есть и другие команды режимов глобального конфигурирования и конфигурирования интерфейсов, позволяющие более тонко настраивать функционирование протокола STP в сети, но их изучение выходит за рамки данного пособия.

ВЫПОЛНИТЬ!

68. Выбрать Switch3 дополнительным корневым коммутатором для расчета связующего дерева. Определить активное связующее дерево STP в сети.
69. Выбрать Switch1 основным корневым коммутатором для расчета связующего дерева. Определить активное связующее дерево STP в сети.
70. Установить приоритет для расчета связующего дерева на коммутаторе Switch2 – 20480. Определить активное связующее дерево STP в сети.
71. Удалить линию связи между коммутаторами Switch0 и Switch2. Определить приблизительное время расчета дерева по алгоритму PVST. Определить активное связующее дерево STP в сети.
72. Восстановить линию связи между коммутаторами Switch0 и Switch2. Установить на всех коммутаторах режим Rapid-PVST.
73. Удалить линию между коммутаторами Switch0 и Switch2. Определить приблизительное время расчета дерева по алгоритму Rapid-PVST.

Конфигурирование маршрутизаторов

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 комментария 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, RE-**

LEASE SOFTWARE (fc1)

**!Сокращенная версия IOS, которая используется в качестве загруз-
чика (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 (рис. 2.5):

Router>show processes.

```
Telnet localhost
Router>show processes
CPU utilization for five seconds: 0%/0%; one minute: 0%; five minutes: 0%
PID QTY PC Runtime (ms) Invoked uSecs Stacks TTY Process
1 Cwe 6002D4AC 0 3 0 5492/6000 0 Chunk Manager
2 Csp 6071B9B4 1000 346 2890 2536/3000 0 Load Meter
3 M* 0 3700 388 9536 8632/12000 0 Exec
4 Mwe 61F19FA0 0 1 023392/24000 0 EDDRI_MAIN
5 Lst 6002A800 352 174 2022 5260/6000 0 Check heaps
6 Cwe 60032DFC 0 2 0 5432/6000 0 Pool Manager
7 Mst 61048D04 0 2 0 5496/6000 0 Timers
8 Mwe 600E68B8 0 2 0 8492/9000 0 ATM AutoUC Perio
9 Mwe 600E6238 0 2 0 5492/6000 0 ATM UC Auto Crea
10 Mwe 6011B908 0 30 0 5672/6000 0 IPC Dynamic Cach
11 Mwe 6010FC7C 0 1 0 5548/6000 0 IPC Zone Manager
12 Mwe 6010F7BC 4 1792 2 5700/6000 0 IPC Periodic Tim
13 Mwe 6010F65C 4 1792 2 5524/6000 0 IPC Deferred Por
14 Mwe 6010F9BC 4 1 4000 5496/6000 0 IPC Seat Manager
15 Mwe 60112EEC 0 1 0 5560/6000 0 IPC BackPressure
16 Msi 60267240 20 1791 11 5304/6000 0 EnvMon
17 Mwe 6026E788 0 1 0 8520/9000 0 OIR Handler
18 Mwe 603157DC 0 1 023436/24000 0 Crash writer
19 Mwe 60BBD3C4 16 34 470 5300/6000 0 ARP Input
20 Mwe 60C250F4 0 2 0 5492/6000 0 ATM Idle Timer
21 Mwe 61003170 0 2 0 5484/6000 0 AAA high-capacit
--More--
```

Рис. 2.5. Просмотр информации о процессах

Router>show processes cpu.

```
Telnet localhost
Router>show processes cpu
CPU utilization for five seconds: 0%/0%; one minute: 0%; five minutes: 0%
PID Runtime (ms) Invoked uSecs 5Sec 1Min 5Min TTY Process
1 0 3 0 0.00% 0.00% 0.00% 0 Chunk Manager
2 1000 357 2801 0.08% 0.02% 0.04% 0 Load Meter
3 3780 401 9426 0.00% 0.10% 0.27% 0 Exec
4 0 1 0 0.00% 0.00% 0.00% 0 EDDRI_MAIN
5 356 180 1977 0.00% 0.01% 0.00% 0 Check heaps
6 0 2 0 0.00% 0.00% 0.00% 0 Pool Manager
7 0 2 0 0.00% 0.00% 0.00% 0 Timers
8 0 2 0 0.00% 0.00% 0.00% 0 ATM AutoUC Perio
9 0 2 0 0.00% 0.00% 0.00% 0 ATM UC Auto Crea
10 0 31 0 0.00% 0.00% 0.00% 0 IPC Dynamic Cach
11 0 1 0 0.00% 0.00% 0.00% 0 IPC Zone Manager
12 4 1845 2 0.00% 0.00% 0.00% 0 IPC Periodic Tim
13 4 1845 2 0.00% 0.00% 0.00% 0 IPC Deferred Por
14 4 1 4000 0.00% 0.00% 0.00% 0 IPC Seat Manager
15 0 1 0 0.00% 0.00% 0.00% 0 IPC BackPressure
16 20 1844 10 0.00% 0.00% 0.00% 0 EnvMon
17 0 1 0 0.00% 0.00% 0.00% 0 OIR Handler
18 0 1 0 0.00% 0.00% 0.00% 0 Crash writer
19 16 35 457 0.00% 0.00% 0.00% 0 ARP Input
20 0 2 0 0.00% 0.00% 0.00% 0 ATM Idle Timer
21 0 2 0 0.00% 0.00% 0.00% 0 AAA high-capacit
--More--
```

Рис. 2.6. Просмотр информации об использовании процессора

Список литературы, рекомендуемый к использованию по данной теме.

Основная: 1,2

Дополнительная: 1, 2,3

Интернет-ресурсы: 1, 2, 3, 4

Лабораторная работа № 9-12

Тема 5-6: Основы конфигурирования маршрутизаторов
Конфигурирование маршрутизации

Наименование задания: «Меж сетевое экранирование с использованием технологий фирмы Cisco»

Цель: Cisco.

Формируемые компетенции: ПК-5

Теоретическая часть:

Программа лабораторной работы

2. Zone-Based Policy Firewall.

3. Cisco PIX.

4. IPSec.

Списки доступа **Стандартные списки доступа**

Списки доступа (access lists) представляют собой общие критерии отбора, которые можно впоследствии применять при фильтрации дейтаграмм, для отбора маршрутов, определения приоритетного трафика и в других задачах.

Списки доступа, производящие отбор по IP-адресам, создаются командами access-list в режиме глобальной конфигурации, каждый список определяется номером – числом в диапазоне 0 ÷ 99 [11]. Каждая такая команда добавляет новый критерий отбора в список:

router (config) #access-list

<номер_списка><{deny|permit}>

<IP-адрес> [маска_шаблона] .

IP-адрес и маска шаблона записываются в десятично-точечной нотации, при этом в маске шаблона устанавливаются биты, значение которых в адресе следует игнорировать, остальные биты сбрасываются. При этом сетевая маска (netmask) и маска шаблона (wildcard) – это разные вещи. Например, чтобы строка списка сработала для всех узлов с адресами 1.16.124.xxx, адрес должен быть 1.16.124.0, а маска – 0.0.0.255, поскольку значения первых 24 бит жестко заданы, а значения последних 8 бит могут быть любыми. Как видно в этом случае маска шаблона является инверсией соответствующей сетевой маски. Однако маска шаблона в общем случае не связана с сетевой маской и даже может быть разрывной (содержать чередования нулей и единиц). Например, строка списка должна сработать для всех нечетных адресов в сети 1.2.3.0/24. Соответствующая комбинация адреса и маски шаблона: 1.2.3.1 0.0.0.254.

Комбинация «адрес – маска шаблона» вида 0.0.0.0 255.255.255.255 (то есть соответствующая всем возможным адресам) может быть записана в виде одного ключевого слова any. Если маска отсутствует, то речь идет об IP-адресе одного узла.

Операторы permit и deny определяют, соответственно, положительное (принять, пропустить, отправить, отобрать) или отрицательное (отбросить, отказать, игнорировать) будет принято реше-

ние при срабатывании данного критерия отбора. Например, если список используется при фильтрации дейтаграмм по адресу источника, то эти операторы определяют, пропустить или отбросить дейтаграмму, адрес источника которой удовлетворяет комбинации «адрес — маска шаблона». Если же список применяется для идентификации какой-либо категории трафика, то оператор `allow` отбирает трафик в эту категорию, а `deny` — нет.

Список доступа представляет собой последовательность из одного и более критериев отбора, имеющих одинаковый номер списка. Последовательность критериев имеет значение: маршрутизатор просматривает их по порядку; срабатывает первый критерий, в котором обнаружено соответствие образцу; оставшаяся часть списка игнорируется. Любые новые критерии добавляются только в конец списка. Удалить критерий нельзя, можно удалить только весь список. В конце списка неявно подразумевается критерий «отказать в любом случае» (`deny any`) — он срабатывает, если ни одного соответствия обнаружено не было.

Для аннулирования списка доступа следует ввести команду:
`router(config)#no access-list <номер_списка>.`

Чтобы применить список доступа для фильтрации пакетов, проходящих через определенный интерфейс, нужно в режиме конфигурации этого интерфейса ввести команду:

**`router(config-if)#ip access-group <номер_списка>
<{in|out}>.`**

Ключевое слово `in` или `out` определяет, будет ли список применяться к входящим или исходящим пактам соответственно. Входящими считаются пакеты, поступающие к интерфейсу из сети. Исходящие пакеты движутся в обратном направлении.

Только один список доступа может быть применен на конкретном интерфейсе для фильтрации входящих пакетов, и один — для исходящих. Соответственно, все необходимые критерии фильтрации должны быть сформулированы администратором внутри одного списка.

В стандартных списках доступа отбор пакетов производится по IP-адресу источника пакета.

ВЫПОЛНИТЬ!

1. Создать стандартный список доступа, разрешающий прохождения сетевых пакетов только для сетей

192.168.20.1/24 и 10.0.0.1/24. Для этого в глобальном контексте конфигурирования необходимо выполнить следующие команды:

```
router(config)#access-list 1 permit
192.168.20.1 0.0.0.255
router(config)#access-list 1 permit
10.0.0.1 0.0.0.255
router(config)#access-list 1 deny any any.
```

2. Применить созданный стандартный список доступа на вход одного из интерфейсов маршрутизатора.
3. С помощью команды **ping** проверить доступность компьютеров из сетей 192.168.20.1/24 и 10.0.0.1/24.
4. Аннулировать созданный стандартный список доступа.

Расширенные списки доступа

Кроме стандартных (standard) списков доступа существуют также расширенные (extended), имеющие большее количество параметров и предлагающие более богатые возможности для формирования критериев отбора.

Расширенные списки доступа создаются также с помощью команды access-list в режиме глобальной конфигурации, но номера этих списков лежат в диапазоне 100–199. Пример синтаксиса команды создания строки расширенного списка для контроля TCP-соединений:

```
router(config)#access-list<номер_списка><{deny|
permit}> tcp <IP-адрес_источника>
<маска_шаблона> [оператор
порт[порт]]<IP-адрес_получателя>
<маска_шаблона> [оператор
порт[порт]] [established]
```

Маски шаблона для адреса источника и узла назначения определяются так же, как и в стандартных списках.

Оператор при значении порта должен иметь одно из следующих значений: lt (меньше), gt (больше), eq (равно), neq (не равно), range (диапазон включительно). После оператора следует номер порта (или два номера порта в случае оператора range), к которому этот оператор применяется.

Комбинация оператор-порт, следующая сразу же за адресом источника, относится к портам источника. Соответственно, комбинация оператор-порт, которая следует сразу же за адресом получателя, относится к портам узла-получателя. Применение этих комбинаций позволяет отбирать пакеты не только по адресам мест отправки и назначения, но и по номерам TCP- или UDP-портов.

Кроме того, ключевое слово `established` определяет сегменты TCP, передаваемые в состоянии установленного соединения. Это значит, что строке, в которую включен параметр `established`, будут соответствовать только сегменты с установленным флагом ACK (или RST).

Пример: «запретить установление соединений с помощью протокола Telnet со всеми узлами сети 22.22.22.0 netmask 255.255.255.0 со стороны всех узлов Интернета, причем в обратном направлении все соединения должны устанавливаться; остальные TCP-соединения разрешены». Фильтр устанавливается для входящих сегментов со стороны Интернета (предположим, к Интернету маршрутизатор подключен через интерфейс FastEthernet 1/0).

```
router(config)#access-list 101 permit tcp any
                22.22.22.0 0.0.0.255 eq 23 established
router(config)#access-list 101 deny tcp any
                22.22.22.0 0.0.0.255 eq 23
router(config)#access-list 101 permit ip any any
router(config)#interface FastEthernet 1/0
router(config-if)#ip access-group 101 in.
```

Указание `ip` вместо `tcp` в команде `access-list` означает «все протоколы». Отметим, что в конце каждого списка доступа подразумевается `deny ip any any`, поэтому в предыдущем примере мы указали `permit ip any any` для разрешения произвольных пакетов, не попавших под предшествующие критерии.

Расширенный список с протоколом `ip` позволяет также производить отбор произвольных пакетов по адресу отправителя и по адресу получателя (в стандартных списках отбор производится только по адресу отправителя).

Критерии для отбора UDP-сообщений составляются аналогично TCP, при этом вместо `tcp` следует указать `udp`, а параметр `established`, конечно, не применим.

ВЫПОЛНИТЬ!

5. Создать расширенный список доступа, запрещающий установление соединений с помощью протокола HTTP со всеми узлами сети 192.168.20.0 netmask 255.255.255.0 со стороны всех узлов сети «Интернет», но разрешающий установление всех соединений в обратном направлении.
6. Применить созданный расширенный список доступа на вход одного из интерфейсов маршрутизатора.
7. Проверить работоспособность созданного расширенного списка, подключив к маршрутизатору две сети с Web-серверами и осуществив к ним поочередно запросы.

Контроль за ICMP-сообщениями может осуществляться с помощью критериев отбора типа:

```
router(config)#access-list<номер_списка>  
    <{deny|permit}> icmp <IP-адрес_источника>  
    <маска_шаблона>  
    <IP-адрес_назначения> <маска_шаблона>  
    [icmp-тип [icmp-код]].
```

Здесь icmp-тип и, если требуется уточнение, icmp-код определяют ICMP-сообщение.

Вообще, в расширенных списках можно работать с пакетами любого IP-протокола. Для этого после оператора deny/permit надо указать название протокола (ahp, esp, eigrp, gre, icmp, igmp, igrp, ipinip, ospf, tcp, udp) или его номер, которым он кодируется в поле Protocol заголовка пакета. Далее указываются адреса источника и узла назначения с масками и, возможно, дополнительные параметры, специфичные для данного протокола.

В конце команды **access-list** (расширенный) можно указать параметр **log**, тогда все случаи срабатывания данного критерия (то есть обнаружения пакета, соответствующего критерию), будут протоколироваться на консоль или как указано командой **logging**. После того, как протоколируется первый случай срабатывания, дальше сообщения посылаются каждые 5 минут с указанием числа срабатываний за отчетный период.

Просмотр имеющихся списков доступа (с указыванием числа срабатываний каждого критерия):

```
router#show access-lists.
```

ВЫПОЛНИТЬ!

8. Просмотреть число срабатываний каждого критерия из созданного списка доступа.

Более подробную статистику работы списков доступа можно получить, включив режим `ip accounting`. Режим включается в контексте конфигурирования интерфейса. Следующая команда включает режим учета случаев нарушения (то есть, пакетов, которые не были пропущены списком доступа на данном интерфейсе):

```
router(config-if)#ip accounting access-violations.
```

ВЫПОЛНИТЬ!

Просмотр накопленной статистики (с указанием адресов отправителей и получателей пакетов):

```
router#show ip accounting access-violations.
```

При конфигурировании запрещающих фильтров (в конце которых подразумевается `deny all`) администратор должен не забыть оставить «дверь» для сообщений протоколов маршрутизации, если они используются на конфигурируемом интерфейсе.

ВЫПОЛНИТЬ!

10. Выполнить несколько запросов к Web-серверам.
11. Просмотреть результаты работы команды **ping**.
12. Вывести на консоль накопленную статистику по учету случаев нарушений.
13. Аннулировать созданный расширенный список доступа.

Динамические обратные списки доступа

Недостатком списков доступа, применяемых для фильтрации трафика, является то, что они формируются администратором статически до начала работы. В итоге администратор вынужден закладывать в них разрешения «на все случаи жизни». Например, чтобы позволить узлам внутренней сети соединяться по Telnet с узлами Интернета, необходимо разрешить, во-первых, движение TCP-сегментов с любого порта изнутри на порт 23 снаружи; а во-вторых, для пропуска сегментов в обратном направлении необхо-

димо разрешить движение сегментов с порта 23 наружных узлов на любой порт внутренних, так как заранее не известно, какой клиентский порт будет использовать внутренний узел для открытия сеанса Telnet. Эти два списка доступа, для исходящих и входящих сегментов, никак не связаны друг с другом. В итоге злоумышленник, занявший порт 23 какого-либо внешнего узла, может отправлять сегменты на любой порт внутренних узлов, попадающих под список доступа. В случае с TCP проблема может быть частично решена установкой в списке доступа флага established, но для протокола UDP и это неприменимо.

Динамические обратные списки (reflexive access lists) предлагают способ решения проблемы. Они служат для автоматической фильтрации пакетов, следующих в обратном направлении относительно пакетов, пропущенных некоторым статическим списком. Динамические обратные списки открывают только те «двери», которые необходимо открыть для обслуживания данного конкретного сеанса обмена пакетами. В этом случае заранее формируется только один список, например список 120 «пропускать UDP-пакеты с любого порта внутри на порт 53 снаружи», а для пропуска пакетов в обратном направлении список 121 формируется динамически:

```
router(config)#access-list 120 permit udp any
any eq 53 reflect DNS_REPLIES
router(config)#access-list 121 evaluate
DNS_REPLIES
router(config)#interface FastEthernet 1/0
router(config-if)#ip access-group 120 out
router(config-if)#ip access-group 121 in
```

Приведенный выше пример работает следующим образом. Когда внутренний узел А посылает сообщение с клиентского порта 3456 на порт 53 некоторого внешнего узла В, то соответствующий сегмент пропускается в узел В согласно списку 120. Кроме того, узел А ожидает, что и ответное сообщение от В с порта 53 на А порт 3456 будет пропущено маршрутизатором. Для этого маршрутизатор динамически создает (дополняет) список доступа 121 обратный к списку 120. Точнее, критерий отбора, содержащий указание evaluate DNS_REPLIES, будет обратным критерию отбора, содержащему указание reflect DNS_REPLIES с учетом параметров данного конкретного сеанса — адресов А и В и номера порта 3456.

Иными словами, список 121 будет выглядеть: «пропускать UDP-пакеты с порта 53 узла В на порт 3456 узла А».

Динамически сформированный критерий отбора в списке 121 будет действовать до завершения сеанса между А и В. Завершение сеанса определяется таймером неактивности; кроме того, в TCP-сеансах отслеживаются сегменты с флагами FIN и RST. Таймер неактивности для всех динамических обратных списков устанавливается командой:

```
router(config)#ip reflexive-list timeout  
    <число_секунд>.
```

Кроме того, таймер для конкретного критерия может быть установлен с помощью параметра timeout:

```
router(config)#access-list 120 permit udp any  
    any eq 53 reflect DNS_REPLIES timeout 120.
```

Если одновременно с сеансом А – В будет установлен сеанс между узлами С и D, то в список 121 будет добавлен еще один критерий отбора, учитывающий параметры этого нового сеанса – адреса С и D и клиентский порт на узле С.

Необходимо понимать, что использование динамических обратных списков доступа несовместимо с приложениями, которые изменяют номера портов в процессе своей работы.

В заключение обсуждения списков доступа необходимо отметить такой очевидный факт, что использование списков доступа замедляет работу маршрутизатора. Чем больше и сложнее списки, тем меньше производительность маршрутизатора. То же относится и к фиксации событий в журналах.

ВЫПОЛНИТЬ!

14. Создать динамический обратный список доступа, предложенный выше в качестве примера, и осуществить его проверку, отправляя запросы к DNS-серверу.
15. Аннулировать созданные списки доступа.

В качестве примера предлагается реализовать схему сети, представленную на рис. 3.1.

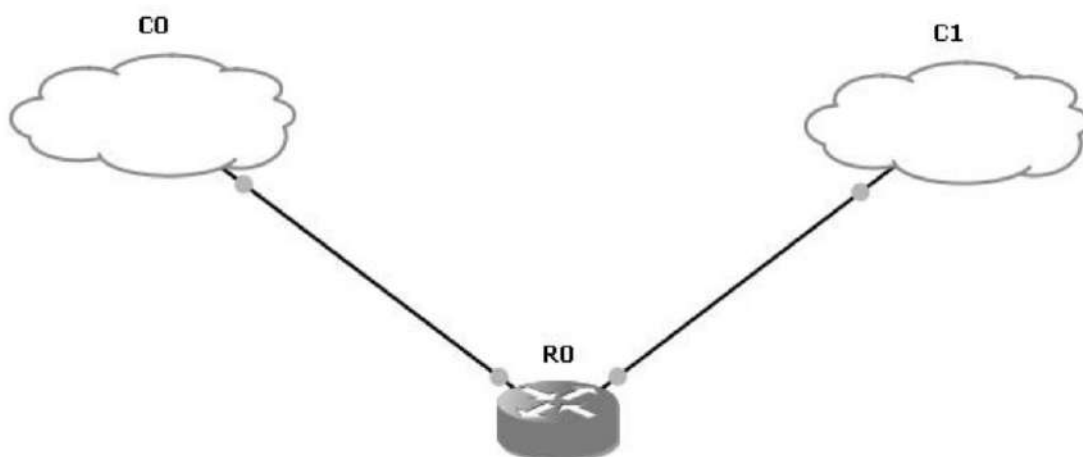


Рис. 3.1. Схема сети для примера использования расширенного списка доступа

Входные данные: C0 – сеть с диапазоном адресов 192.168.20.0/24; C1 – сеть с диапазоном адресов 10.0.0.0/8. Необходимо настроить маршрутизатор R0 таким образом, чтобы весь трафик из сети C0 в сеть C1 был запрещен, за исключением трафика функционирования WEB-сервера, имеющего IP-адрес 10.0.0.5.

Реализовать данную схему можно с помощью следующих команд:

```
Router>enable
```

```
Router#
```

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

```
Router#configuration terminal
```

!Переход в глобальный контекст конфигурирования.

```
Router(config)#access-list 101 permit tcp  
192.168.20.0 0.0.0.255 10.0.0.5 eq 80
```

!Задание расширенного списка доступа № 101, разрешающего прохождение IP-трафика со всех адресов сети 192.168.20.0/24 на порт 80 IP-адреса 10.0.0.5.

```
Router(config)#access-list 101 deny ip any any
```

!Запрет всего остального трафика.

```
Router(config)#interface FastEthernet 1/1
```

!Переход в контекст конфигурирования интерфейса FastEthernet 1/1, подключенного к сети C0.

```
Router(config-if)#ip address 192.168.20.2  
255.255.255.0
```

!Установка IP-адреса и маски сети.

```
Router(config-if)#ip access-group 101 in  
Router(config-if)#no shutdown
```

!Включение интерфейса.

```
Router(config-if)#exit
```

!Выход из контекста конфигурирования интерфейса FastEthernet 1/1, подключенного к сети C0.

```
Router(config)#interface FastEthernet 1/0
```

!Переход в контекст конфигурирования интерфейса FastEthernet 1/0.

```
Router(config-if)#ip address 10.0.0.2  
255.255.255.0
```

!Установка IP-адреса и маски сети.

```
Router(config-if)#no shutdown
```

!Включение интерфейса.

```
Router(config-if)#exit
```

ВЫПОЛНИТЬ!

- 16.Реализовать и проверить работоспособность приведенной схемы.

Настройка Zone-Based Policy Firewall

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 выполнении 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 рис. 3.2. 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.

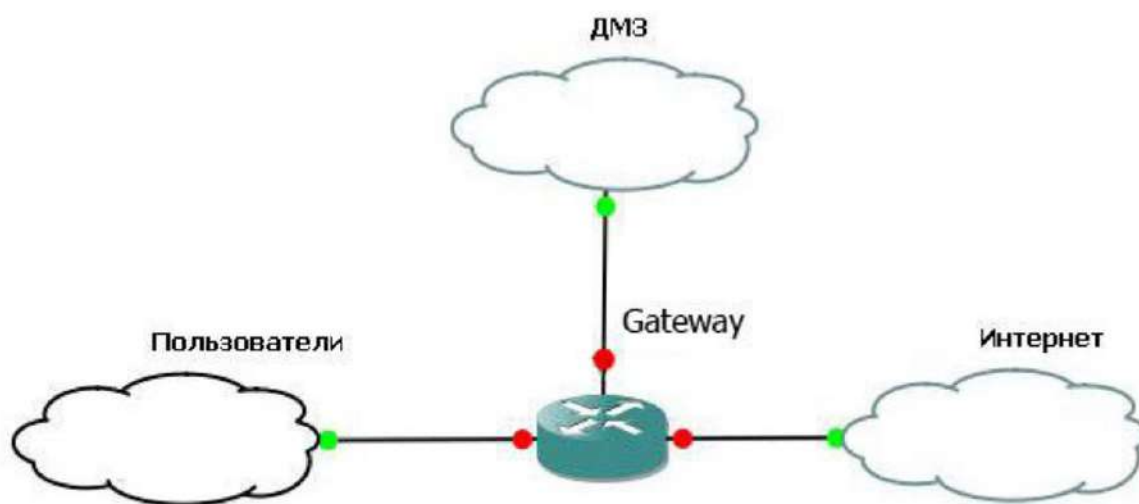


Рис. 3.2. Схема сети

ВЫПОЛНИТЬ!

1. Создать в GNS3 топологию сети, представленную выше (на рис. 3.2).
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 pop
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_http-  
ftp-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 inside-  
outside 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 web-  
server  
Gateway(config)#access-list 101 permit ip any  
host 172.16.0.4  
Gateway(config)#access-list 102 remark mail-  
server  
Gateway(config)#access-list 102 permit ip any  
host 172.16.0.5  
Gateway(config)#access-list 103 remark ftp-  
server  
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 web-
mail-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.
```

11. Проверить работоспособность созданной конфигурации.

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.



Рис. 3.3. 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 получают 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.

Аппаратная часть межсетевых экранов Cisco PIX

Межсетевые экраны Cisco PIX являются аппаратными устройствами, предназначенными для размещения как в серверной стойке, так и на стене (рис. 3.4).

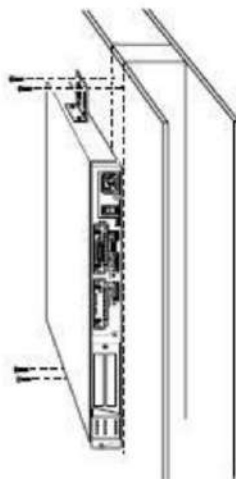


Рис. 3.4. Монтирование устройства Cisco PIX на стену

На лицевой панели устройства (рис. 3.5) расположены два индикатора: POWER (наличие питания) и ACTIVE (индикатор режима работоспособности устройства).



Рис. 3.5. Лицевая панель Cisco PIX 525

На задней панели устройства (рис. 3.6) расположены интерфейсы (рис. 3.7):

- 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.



Рис. 3.6. Задняя панель Cisco PIX 525

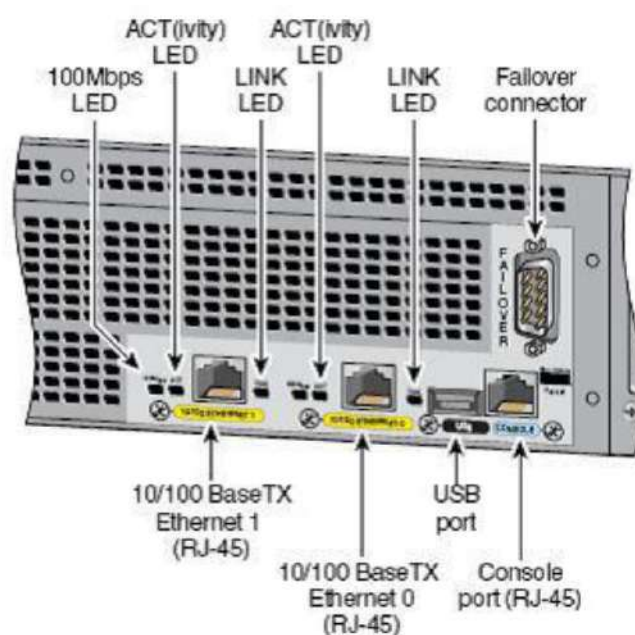


Рис. 3.7. Интерфейсы Cisco PIX 525

Список литературы, рекомендуемый к использованию по данной теме.

Основная: 1,2

Дополнительная: 1, 2,3

Интернет-ресурсы: 1, 2, 3, 4

Лабораторная работа № 13-16

Тема: «Обнаружение сетевых компьютерных атак»

Формируемые компетенции: ПК-5

Теоретическая часть:

Программа лабораторной работы

1. Cisco IDS Sensor.

2. Cisco IDS Sensor.

Настройка комплекса Cisco IDS Sensor

Назначение COA Cisco IDS Sensor

Система обнаружения атак (англ. Intrusion Detection System) – это программный или программно-аппаратный комплекс, предназначенный для выявления и по возможности предупреждения действий, угрожающих безопасности информационной системы.

Основными задачами, решаемыми с помощью систем обнаружения атак (СОА), являются:

- обнаружение атак (вторжений);
- прогнозирование возможных сценариев развития комплексных атак на основе выявления признаков начальных этапов атакующего воздействия;
- фиксация информации об источниках компьютерного нападения;
- получение информации об уязвимостях, использованных для компьютерного нападения.

В большинстве случаев СОА состоит из следующих компонентов:

- сенсорной подсистемы, предназначенной для сбора событий, связанных с безопасностью защищаемой сети или системы;
- подсистемы анализа, служащей для выявления комплексных компьютерных атак;
- информационного хранилища (базы данных), в котором накапливаются первичные события и результаты анализа;
- консоли управления, позволяющей конфигурировать СОА и просматривать выявленные подсистемой анализа инциденты.

В настоящее время существует ряд сетевых СОА фирмы Cisco Systems линейки 4200, предназначенных для сетей, работающих на технологии Fast Ethernet (рис. 4.1). Эти системы обладают общим программным обеспечением и различаются главным образом по производительности – пропускной способности:

- Cisco IDS 4210 – 45 Мб/с;
- Cisco IDS 4215 – 80 Мб/с;
- Cisco IDS 4230 – 100 Мб/с;
- Cisco IDS 4235 – 250 Мб/с;

- Cisco IDS 4250 – 500 Мб/с;
- Cisco IDS 4250 XL – 1000 Мб/с.



Рис. 4.1. Устройства линейки Cisco IDS 4200

На практическом занятии рассматривается модель Cisco IDS 4215 Sensor. Характеристики модели IDS-4215, обеспечивающие пропускную способность до 80 Мб/с: возможность сбора трафика с пяти сетевых интерфейсов, поддержка до 800 новых TCP-соединений в секунду, до 800 HTTP-соединений в секунду, средний размер пакета 445 байт.

Особенностями комплексов линейки 4200 являются:

- точность обнаружения атак, обусловленная применением сигнатурных алгоритмов;
- интеллектуальный анализ, основанный на применении аналитических алгоритмов обнаружения;
- простота и удобство администрирования при наличии трех интерфейсов администрирования;
- гибкость развертывания.

Наряду с традиционными сигнатурными алгоритмами в Cisco IDS используются и алгоритмы, отслеживающие аномалии в сетевом трафике и отклонения от нормального поведения сетевых приложений, что позволяет обнаруживать как известные, так и неизвестные атаки. С целью снижения числа ложных срабатываний, неизбежно возникающих при использовании аналитических алгоритмов, в комплексы интегрированы технологии корреляции событий безопасности: Cisco Threat Response, Threat Risk Rating и Meta Event Generator. Указанные технологии позволяют концентрировать внимание администраторов на наиболее критичных атаках.

Cisco IDS может также работать в режиме предотвращения атак, завершая сеанс атаки путем отключения соединений с опас-

ных IP-адресов, динамически изменяя списки доступа (Access Control Lists) на сетевом оборудовании.

Существуют три интерфейса администрирования Cisco IDS Sensor:

- интерфейс командной строки (CLI интерфейс) операционной системы устройства;
- графический интерфейс Cisco IDS Event Viewer (IEV), разработанный на языке Java для применения в ОС семейства Windows;
- графический интерфейс Cisco IDS Device Manager (IDM), основывающийся на использовании браузера.

Для защищенного обмена данными между администратором сети и сенсором применяется протокол Remote Data Exchange Protocol (RDEP) (начиная с версии 4.0). Протокол RDEP является разновидностью протокола HTTP и основывается на XML-конфигурации (TCP-порт 443). Безопасность передаваемых данных обеспечивается за счет использования протокола SSL (Secure Socket Layer). Для управления сенсором администратор должен задать имя устройства Cisco IDS Sensor и номер порта.

В сети COA может располагаться как перед, так и после межсетевого экрана. Установка COA перед межсетевым экраном позволяет обнаруживать все атаки, идущие на систему извне. Однако при этом не обнаруживается активность внутреннего нарушителя. Расположение COA за межсетевым экраном позволяет контролировать весь трафик, однако не будут фиксироваться те атаки, которые были отражены самим межсетевым экраном. Дополнительным преимуществом расположения COA за межсетевым экраном является уменьшение срабатываний COA.

Согласно рекомендациям производителя сенсор следует размещать в одном из следующих элементов сети (или в нескольких):

- на границе локальной сети и сети «Интернет», что позволит анализировать и контролировать весь трафик обмена внутренней сети с внешней;
- около шлюзов сторонних организации, к которым нет полного доверия;
- на границе между отдельными сегментами сети;
- около точек, используемых для модемной связи и связи с помощью технологий VPN и Wi-Fi.

Аппаратная часть COA Cisco IDS 4215 Sensor

COA Cisco IDS 4215 Sensor является аппаратным устройством, предназначенным для размещения в серверной стойке (рис. 4.2).

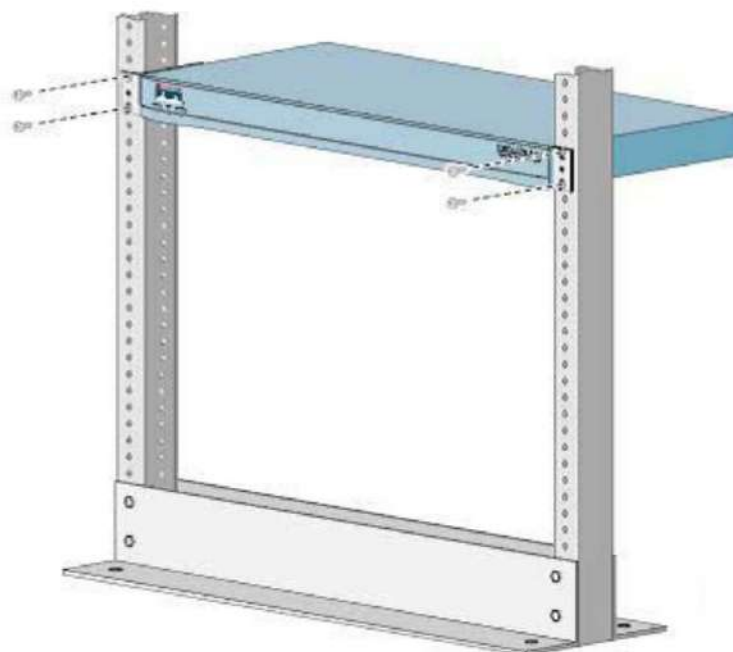


Рис. 4.2. Схема установки Cisco IDS 4215 Sensor в серверной стойке

На лицевой панели устройства (рис. 4.3) расположены три индикатора: POWER (наличие питания), ACT (индикатор режима работоспособности устройства) и NETWORK (индикатор наличия сетевого трафика в канале).



Рис. 4.3. Лицевая панель Cisco IDS 4215 Sensor

На задней панели устройства (рис. 4.4) расположен ряд интерфейсов (рис. 4.5):

- консольный порт для подключения к последовательному порту персонального компьютера с использованием коннектора RJ-45 и управления устройством в режиме командной строки;

- интерфейс FastEthernet0/1 для подключения устройства к анализируемому каналу передачи данных (интерфейс сенсора);
- интерфейс FastEthernet0/0 для управления устройством в режиме web-интерфейса;
- четыре дополнительных интерфейса типа FastEthernet для подключения анализируемых каналов передачи данных (функционируют в случае наличия дополнительно установленной карты типа 4FE) .



Рис. 4.4. Задняя панель Cisco IDS 4215 Sensor

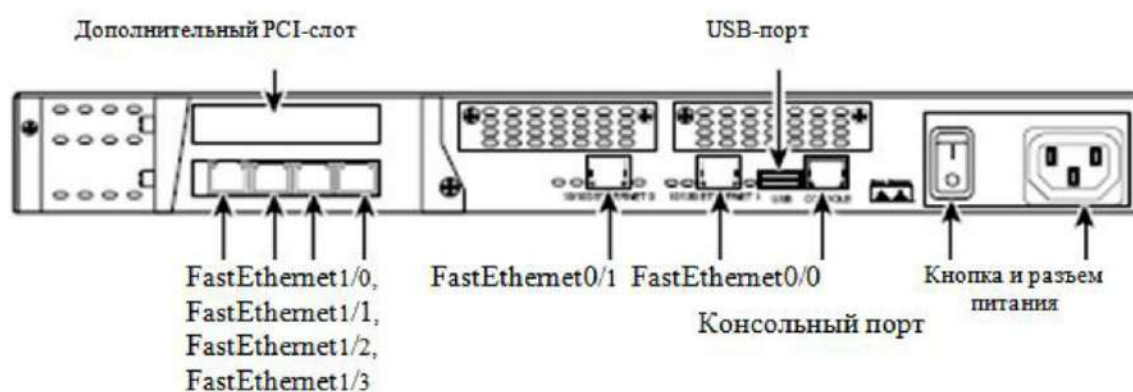


Рис. 4.5. Интерфейсы Cisco IDS 4215 Sensor

Интерфейс сенсора FastEthernet0/1 находится в режиме захвата пакетов (promiscuous mode), не имеет IP-адреса и не обнаруживается в сегменте сети.

Управляющий интерфейс FastEthernet0/0 должен иметь IP-адрес, быть видимым в сегменте сети. Для защиты управляющего канала связи применяется шифрование средствами службы SSH (при работе в режиме командной строки) и протокола SSL (в режиме web-интерфейса).

Внутри устройство представляет собой компьютер, оборудованный жестким магнитным диском с операционной системой Linux и специализированным программным обеспечением (рис. 4.6), а также оборудованный flash-картой памяти.

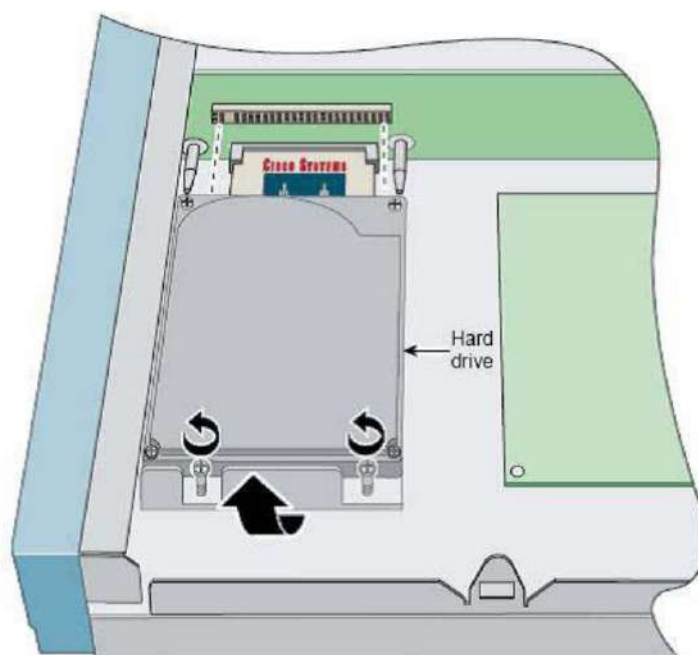


Рис. 4.6. Вид Cisco IDS 4215 Sensor со снятым кожухом

Предварительная настройка COA Cisco IDS Sensor в режиме командной строки

Рассмотрим некоторую организацию, в сети которой внедрено аппаратное устройство Cisco IDS Sensor с целью обнаружения компьютерных атак. Для имитации указанной сети развернем стенд на базе технологии виртуальных машин.

Основная ОС (рис. 4.7) будет имитировать работу администратора для конфигурирования Cisco IDS Sensor, она же будет использована для имитации атакующего воздействия. Оборудование Cisco IDS Sensor в учебных целях представлено виртуальным образом. Сетевое соединение выполняется с помощью виртуальной подсети VWNet1 (тип соединения – Host-only). Для имитации узла-«жертвы» может быть использована любая виртуальная система, подключенная к сети VWNet1.

В связи с тем что в основе Cisco IDS Sensor лежит операционная система Linux, для работы необходимы минимальные знания в области администрирования данной ОС. Для выполнения работы потребуется система VMware Player, образ Cisco IDS Sensor (предоставляется преподавателем в архиве `cisco_ids.rar`), сканер портов nmap (или его аналог), анализатор трафика Wireshark (или его аналог). Для имитации узла-«жертвы» может быть использована лю-

бая виртуальная система (например, ОС Windows 2003 Server), подключенная к сети VNet1.

Также может потребоваться система Java (TM) 2 Platform (файл с дистрибутивом – j2re-1_4_2_07-windows-i586-p.exe).

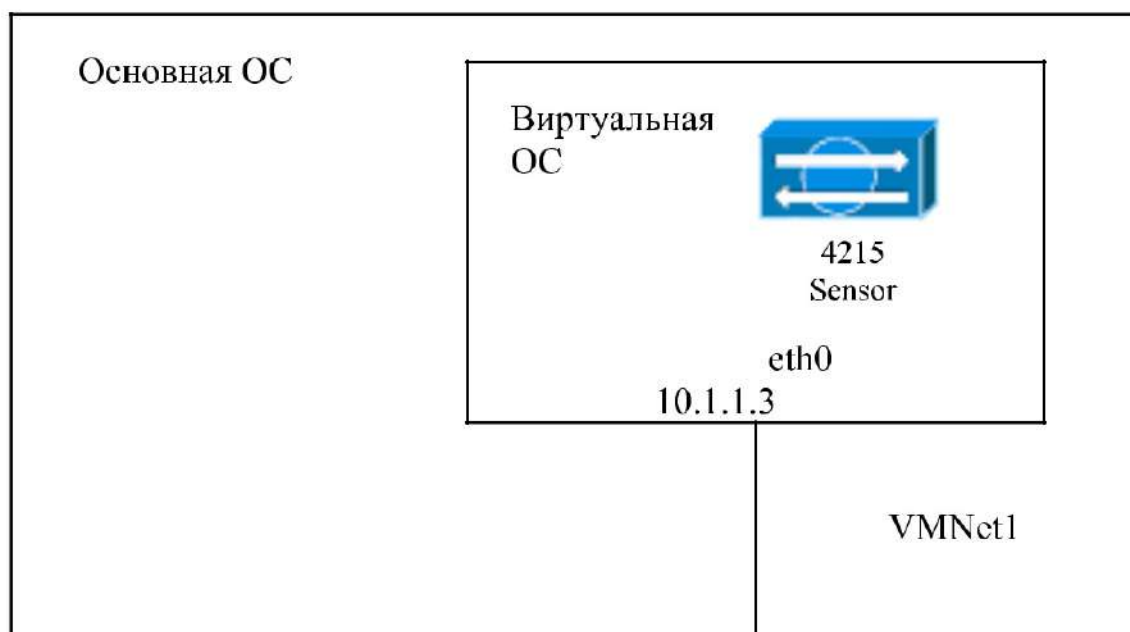


Рис. 4.7. Схема сетевого соединения Cisco IDS 4215 Sensor и основной ОС

Прежде чем работать с образом Cisco IDS Sensor, необходимо правильно настроить конфигурационный файл образа.

ВЫПОЛНИТЬ!

1. Запустить VMWare Player, открыть имеющийся образ Cisco IDS 4215 Sensor.
2. Настроить виртуальный сетевой адаптер на тип соединения Host-only.
3. В каталоге с образом найти файл с расширением .vmx (конфигурационный файл). Открыть его любым текстовым редактором.
4. Найти в файле строку bios440.filename= «...» и модифицировать ее в вид bios440.filename=«/Путь к каталогу с образом / CISCO_IDS4215_440. BIOS.ROM».
5. Проверьте наличие строк:
ethernet0.virtualDev = «e1000»
ethernet1.virtualDev = «e1000»
ethernet2.virtualDev = «e1000»
6. Сохранить конфигурационный файл.

Следующий этап работы состоит в настройке операционной системы Linux. Предполагается, что в устройстве должны быть три сетевых интерфейса: один для управления и два для анализа трафика.

ВЫПОЛНИТЬ!

7. Запустить виртуальную машину (Power on this Virtual Machine).
8. После загрузки системы и появления окна выбора способа загрузки выбрать Cisco IPS и нажать клавишу [e]. Далее выбрать вторую строку с надписью kernel и снова нажать [e].
9. Прокрутить строку влево, пока на экране не появится надпись init=loadrc.
10. Заменить значение loadrc на 1 (чтобы получилось init=1) (рис. 4.8).

```
[ Minimal BASH-like line editing is supported. For the first word, TAB
lists possible command completions. Anywhere else TAB lists the possible
completions of a device/filename. ESC at any time exits. ]
```

```
<800 rootrw=/dev/hda2 root=/dev/ram0 init=1_hda=flash nousb bigphysarea=16384
```

Рис. 4.8. Корректировка загрузки ОС Cisco IDS Sensor

11. Нажать [Enter] и затем клавишу [b] для начала загрузки.
12. Нажать [Enter] для перехода в режим правки.
13. Сменить раскладку клавиатуры на английскую. Ввести:
/loadrc
/etc/init.d/rc.init
touch /usr/share/zoneinfo/cidsZoneInfo.
14. Теперь необходимо выяснить значение быстродействия процессора, для чего ввести следующую команду:
cat /proc/cpuinfo.
15. Найти строку cpu MHz путем прокрутки списка вниз. Записать или запомнить значение (только целую часть, рис. 4.9).
16. Теперь нужно изменить функциональный файл аппаратного устройства (ids_functions). Для начала необходимо сделать резервную копию функционального файла аппаратного устройства на случай ошибочной настройки. Ввести:
cd /etc/init.d
cp ids_functions ids_functions.orig
vi ids_functions.

17. Прокрутить список вниз до строки 4215, что соответствует линии #252. Найти надпись:
`elif [[ 'isCPU 845' -eq $TRUE && ...`
`MODEL=$IDS4215`
18. Вместо значения 845 ввести ранее записанное значение быстродействия процессора (в примере – 1958, рис. 4.10).

```
EXT3-fs: mounted filesystem with ordered data mode.
Adding Swap: 594364k swap-space (priority -1)
-sh-2.05b# touch /usr/share/zoneinfo/cidsZoneInfo
-sh-2.05b# cat /proc/cpuinfo
processor       : 0
vendor_id      : GenuineIntel
cpu family     : 6
model          : 7
model name     : Intel(R) Core(TM)2 Duo CPU     P7350  @ 2.00GHz
stepping       : 6
cpu MHz        : 1958.897
cache size     : 64 KB
fdiv_bug       : no
hlt_bug        : no
f00f_bug       : no
coma_bug       : no
fpu            : yes
fpu_exception  : yes
cpuid level    : 10
wp             : yes
flags          : fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov
pat pse36 clflush dts acpi mmx fxsr sse sse2 ss pn1
bogomips       : 3919.05
-sh-2.05b# _
```

Рис. 4.9. Значение тактовой частоты процессора – 1958 МГц

```
if [ 'isFalconPresent' -eq 1 ]; then
    ACCELERATOR_TYPE=$FALCON_DEVICE
else
    ACCELERATOR_TYPE=$NONE
fi
export ACCELERATOR_TYPE

# Set the "HOST_TYPE"
# The Komodo+ uses the amd chip for the eobc, Mohawk uses a 498 Mhz cpu
# The default host type is PC
isKomodoPlatform
if [[ "$?" -eq 1 ]]; then
    HOST_TYPE=$KOMODO_HOST
elif [ 'isCPU 1958' -eq $TRUE ]; then
    HOST_TYPE=$MOHAWK_HOST
else
    HOST_TYPE=$PC_HOST
fi
export HOST_TYPE

# Set the "PLATFORM_TYPE"
# The default platform type is PC
if [[ ${HOST_TYPE} == ${KOMODO_HOST} || ${HOST_TYPE} == ${MOHAWK_HOST} ]]; th
    PLATFORM_TYPE=$BLADE_PLATFORM
```

Рис. 4.10. Изменение частоты процессора в ОС Cisco IDS Sensor

19. Найти две строки чуть ниже с надписями `DEFAULT_MGT_OS` и `DEFAULT_MGT_CIDS`. Изменить их следующим способом (рис. 4.11):

`DEFAULT_MGT_OS="ma0_0"`

`DEFAULT_MGT_CIDS="Management0/0"`.

```
MODEL=$IDS4215
BIGPHYS=16384
MEM_PAGES=${BIGPHYS}
DEFAULT_MGT_OS="ma0_0"
DEFAULT_MGT_CIDS="Management0/0"
```

Рис. 4.11. Настройки интерфейса управления ОС Cisco IDS Sensor

20. Сохранить и выйти из режима редактирования.
21. Теперь необходимо изменить конфигурационный файл сетевых интерфейсов. Для этого ввести следующие строки:
- ```
cd /usr/cids/idsRoot/etc
cp interface.conf interface.conf.orig
vi interface.conf
```
22. Прокрутить список вниз, пока на экране не появится второй раздел `IDS-4215`. Изменить строки следующим образом:
- ```
[models/IDS-4215/slots/1]
# lower slot
pci-bus=0
pci-device=17
[models/IDS-4215/slots/2]
# upper slot
pci-bus=0
pci-device=19
```
23. Прокрутить список еще ниже и изменить блок первого интерфейса `[models/IDS-4215/interfaces/1]` следующим образом:
- ```
[models/IDS-4215/interfaces/1]
built-in 10/100 TX mgmt interface, Intel 82559ER
was eth1 (int1) in 4.x
rightmost connector on front panel
labeled "Ethernet 1" on panel
name-template=Management0/0
pci-bus=0
```

```
pci-device= 17
pci-function=0
vendor-id=0x8086
device-id=0x100f
type=ge
mgmt-capable=yes
```

24. Изменить теперь второй интерфейс:

```
[models/IDS-4215/interfaces/2]
built-in 10/100 TX mgmt interface, Intel 82559ER
was eth0 (int0) in 4.x
leftmost connector labeled "Ethernet 0"
name-template= GigabitEthernet0/1
pci-bus=0
pci-device= 18
pci-function=0
vendor-id=0x8086
device-id= 0x100f
type=ge
sensing-capable=yes
tcp-reset-capable=yes
```

25. Создать третий интерфейс путем копирования второго и замены значений в строках, как показано ниже:

```
[models/IDS-4215/interfaces/3]
name-template=GigabitEthernet0/2
pci-bus=0
pci-device= 19
pci-function=0
vendor-id=0x8086
device-id=0x100f
type=ge
sensing-capable=yes
tcp-reset-capable=yes
```

26. Сохранить настройки, выйти из режима редактирования и перезагрузить ОС командой **reboot**.

27. На данном этапе необходимо изменить пароль учетным записям root, service и cisco при помощи команды **passwd <username>**.

28. В случае необходимости можно удалить имеющиеся пароли учетных записей cisco и service командой vi

/etc/passwd. Удалить в учетной записи cisco «крестик» для ее загрузки без пароля. Аналогично сделать с учетной записью service, которую необходимо также разблокировать командой: **passwd -u service**.

29. Сохранить настройки, выйти из режима редактирования и перезапустить устройство командой **reboot**.
30. Выбрать первый способ загрузки (Cisco IPS), и после того как система загрузится и попросит ввести регистрационные данные (sensor login), ввести cisco, а на запрос ввода пароля (password) – пароль, например pbdrc001A.
31. Задать пароль для режима service. Для этого ввести:  
**conf t**  
**username service pass <password> privy**  
**service**  
**exit**.
32. Теперь войти в систему с учетной записью service (пароль был установлен на предыдущем шаге). Для перехода в режим администратора (root) ввести **su -**.
33. Теперь открыть файл /usr/share/zoneinfo/cidsZoneInfo. Если не удастся открыть, то ввести touch /usr/share/zoneinfo/cidsZoneInfo. Без этого файла интерфейс командной строки CLI не будет доступен.
34. Завершить сеанс работы учетной записи service и войдите в систему, используя учетную запись cisco.

Следующий этап работы состоит в первоначальной настройке Cisco IDS 4215 Sensor, а именно в указании IP-адреса (10.1.1.3/24), при обращении к которому можно будет выполнять дальнейшие настройки из web-интерфейса.

### **ВЫПОЛНИТЬ!**

35. Ввести команду **setup** для перехода в режим системной конфигурации.
36. Нажать клавишу Пробел для перехода к вопросу Continue with configuration dialog? [yes]:. Ввести yes для продолжения.
37. При появлении строки Enter host name[sensor] ввести имя сенсора. По умолчанию имя сенсора – sensor. Можно

задать любое имя длиной до 256 символов без пробела и знака дефис. Нажать [Enter].

38. При появлении запроса Enter IP address[10.1.9.201] ввести 10.1.1.3/24 10.1.1.1. Где 10.1.1.3 – адрес IDS, /24 – маска 255.255.255.0, 10.1.1.1 – адрес шлюза.

39. При появлении запроса Enter telnet-server status [disabled] ввести enable. Ввести команду exit дважды до появления строки Use this configuration?[yes]. Ввести yes.

40. Перезагрузить с помощью команды **reset** и войти, используя учетную запись cisco.

41. Ввести команду **configure terminal** для перехода в режим конфигурирования терминала.

42. Последовательно ввести следующие команды (после ввода команды не забывайте нажимать [Enter]):

**service host** (для перехода в режим конфигурации),

**network-settings** (для перехода в режим конфигурирования сетевых параметров),

**show settings** (для вывода настроек на экран).

43. Для добавления нужной сети (10.1.1.1/24) в список доступа (ACL) необходимо сначала удалить из него адрес ненужной сети, а затем ввести адрес требуемой сети. Для этого ввести следующие команды:

**no access-list 1**

**access-list 10.1.1.1/24**

**exit.**

44. Затем необходимо вводить команду **exit** до тех пор, пока на экране не появится запрос на применение изменений Apply Changes:[yes]. Ввести yes.

45. При появлении запроса Continue with reboot?:[yes] ввести no.

46. Выйти из режима sensor(config)#, используя команду **exit**.

47. Установить дату и время. Для этого ввести:

**clock set hh:mm month day year** (например clock set 15:36 Jan 20 2010).

48. Для перезагрузки системы ввести команду **reset**.

49. Для проверки результатов (а именно того, что теперь возможна настройка Cisco IDS 4215 Sensor с помощью web-интерфейса) в адресной строке браузера основной ОС

ввести <https://10.1.1.3/>. Обратите внимание, что обмен осуществляется по защищенному каналу SSL (рис. 4.12).

50. При необходимости в системе VMware для сетевых интерфейсов сенсора произвести операцию Disconnect, затем Connect.



Рис. 4.12. Окно Web-интерфейса конфигурирования

### ***Настройка COA Cisco IDS Sensor в режиме Web-интерфейса***

На данном этапе работы предполагается выполнить основные настройки COA в режиме Web-интерфейса для обнаружения атак.

### ***ВЫПОЛНИТЬ!***

51. Перейти по адресу интерфейса управления сенсора <https://10.1.1.3>.

52. В графическом интерфейсе Cisco IDS Device Manager зарегистрироваться с учетной записью cisco. Откроется окно Cisco IDM 5.1 (рис. 4.13).

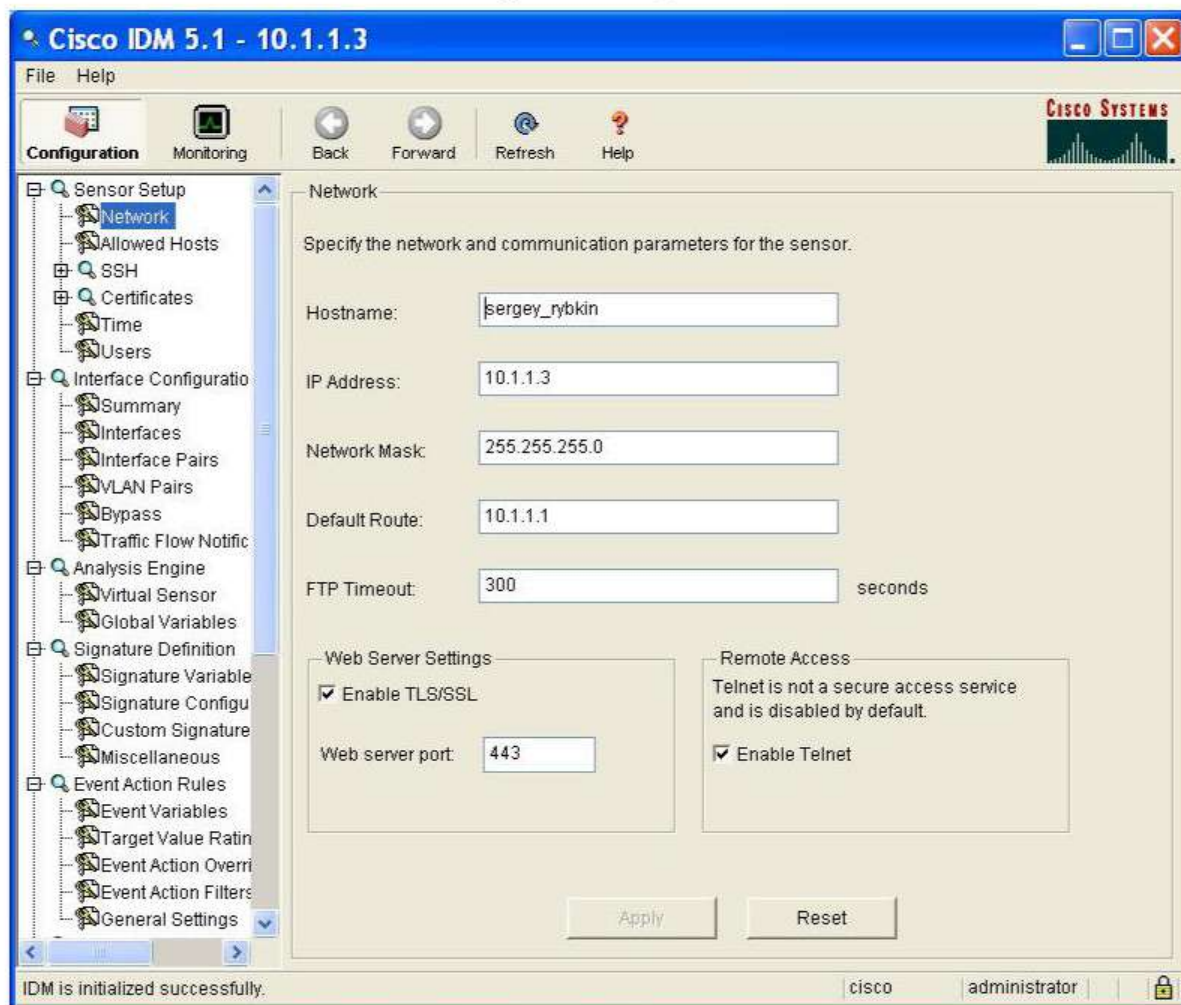


Рис. 4.13. Окно Cisco IDM 5.1

Если графический интерфейс не запускается, то необходимо в основной ОС установить систему Java (TM) 2 Platform (файл j2re-1\_4\_2\_07-windows-i586-p.exe). В случае появления ошибки о нехватке памяти следует открыть панель управления – Control Panel (нажать правой кнопкой мыши на иконке Java (TM) 2 Platform в строке состояния и выбрать пункт Open Control Panel). В открывшемся окне на вкладке Advanced в строке Java Runtime Parameters ввести -Xmx256m и нажать Apply (рис. 4.14). После перезапустить интерфейс (закрывать все окна и заново перейти по ссылке <https://10.1.1.3>).

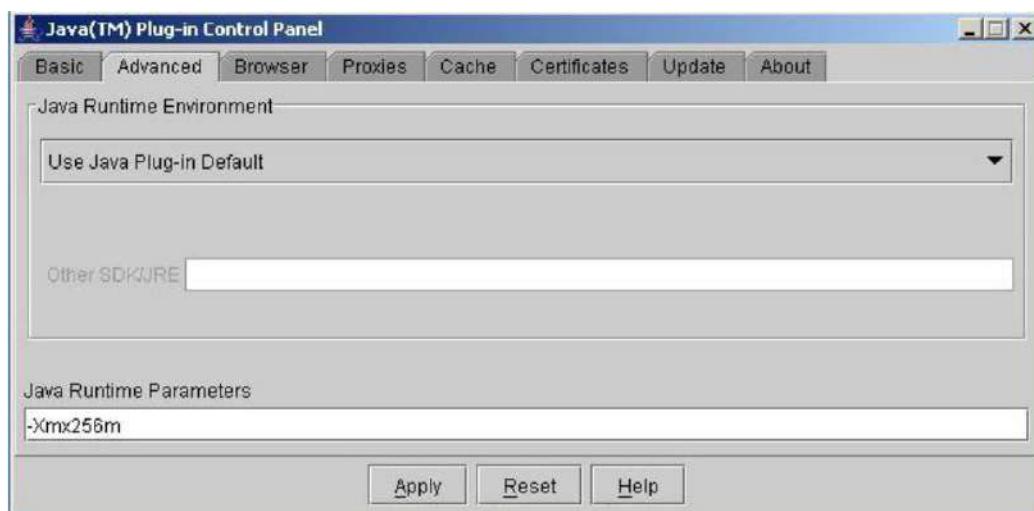


Рис. 4.14. Увеличение объема оперативной памяти для Java

Выполним настройку сетевых интерфейсов.

53. В разделе Configuration (рис. 4.15) выбрать пункт Interface Configuration → Interfaces. Поменять статус обоих интерфейсов GigabitEthernet0/1 и GigabitEthernet0/2 на Enabled (Включенный).

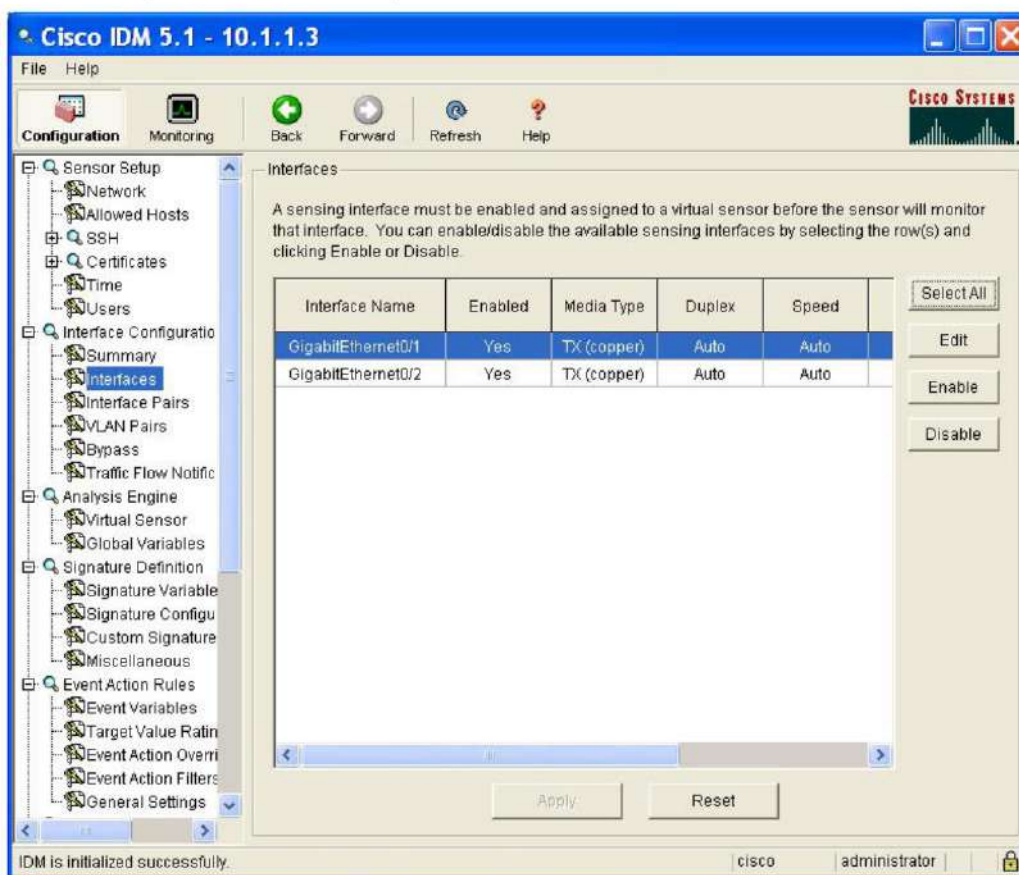


Рис. 4.15. Включение сетевых интерфейсов

54. В разделе Configuration выберите Analysis Engine → Virtual Sensor → Edit. Поменять статус интерфейсов GigabitEthernet0/1 и GigabitEthernet0/2, работающих в режиме захвата пакетов, на Assigned (Назначенный, рис. 4.16).

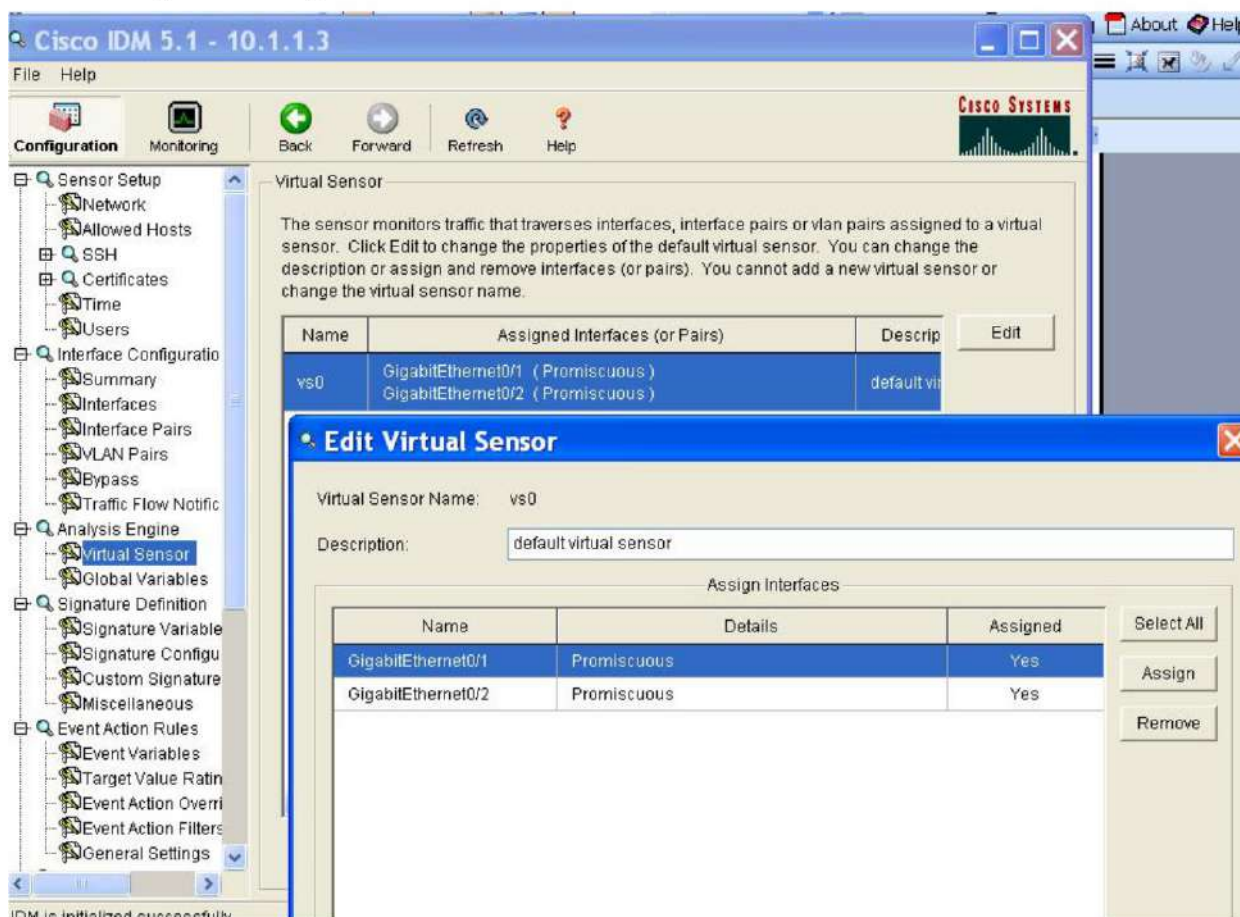


Рис. 4.16. Настройка интерфейсов сенсора

## Обнаружение компьютерных атак на узлы сети с использованием комплекса Cisco IDS Sensor

### *Сигнатуры компьютерных атак COA Cisco IDS Sensor*

Процесс выявления опасной активности в сети заключается в том, что COA Cisco IDS 4215 Sensor анализируется трафик сети, который сравнивается с сигнатурами, содержащимися в базе знаний. Если при анализе трафика сети находятся совпадения в базе сигнатур, то COA формируются сигналы тревоги, которые затем могут быть записаны в журнал, переданы аппаратному устройству Cisco MARS и по почте и т. п.

Сигнатуры COA основываются на информационном наполнении (content-based) или на контексте (context-based).

Сигнатуры Content-based предназначены для выявления атакующего воздействия, содержащегося в полезной нагрузке пакета, например строки URL-запроса.

Сигнатуры Context-based предназначены для выявления атак по заголовкам пакетов в определенных полях или по определенному смещению в пределах пакета.

В рассматриваемой COA существуют четыре основных класса сигнатур:

- исследовательские (reconnaissance);
- информационные (informational);
- сигнатуры доступа (access);
- отказ в обслуживании (denial of service).

Исследовательские — класс сигнатур, позволяющий обнаружить начальный этап компьютерной атаки — исследование атакуемой сети. К таким атакам относятся DNS-атака, сканирование узлов и портов, и т. п.

Информационные — класс сигнатур, позволяющий обнаружить второй этап атакующего воздействия — получение информации об атакуемой системе (например, определение типа и версии системы, сетевых служб).

Сигнатуры доступа — класс сигнатур, позволяющий определить факт несанкционированного доступа в компьютерную систему.

Отказ в обслуживании — класс сигнатур, позволяющий обнаружить типы атак, направленных на нарушение работоспособности устройств в сети.

Структура сигнатуры зависит от количества пакетов, которые должны быть проанализированы. Сигнатуры могут быть атомарными или составными. Сигнатура называется атомарной, если при обнаружении анализируется отдельный пакет без учета его взаимосвязи с иными пакетами, и составной, если при обнаружении анализируется множество пакетов. При обнаружении сенсором первого пакета, который является потенциальной атакой, он анализирует информацию из следующих пакетов.

Например, в случае SYN-атаки отправляется единственный пакет с установленным SYN-флагом без завершения процедуры установления TCP-соединения. Для анализа требуется единственный SYN-пакет вне последовательности. В случае Windows Locator

атаки для обнаружения требуется больше чем один пакет, СОА опознает первый пакет последовательности, пометит его как подозрительный и будет отслеживать дальнейшие совпадения с известными последовательностями, используемыми для данной атаки.

Все сигнатуры делятся на серии от 1000 до 11000. Данное деление помогает администратору быстрее определить, чем вызвана произошедшая атака. Ниже приведен список некоторых серий сигнатур СОА Cisco IDS 4215 Sensor:

- 1000 – охватывает сигнатуры, которые анализируют информацию IP-заголовков;
- 2000 – охватывает сигнатуры, анализирующие информацию, передаваемую по протоколу ICMP;
- 3000 – TCP-порты;
- 4000 – UDP-порты;
- 5000 – HTTP-трафик;
- 6000 – сигнатуры мультипротокола;
- 7000 – ARP-протокола;
- 8000 – сигнатуры сопоставления строк и др.

Также различают следующие типы сигнатур:

- General Connection (общего подключения);
- String (строковые);
- ACL (списка контроля доступа).

Сигнатуры типа General охватывают следующие серии сигнатур: 1000, 2000, 5000 и 6000. В зависимости от типа атаки General-сигнатуры ищут отклонения в известном типе трафика. Например, удостоверяется, правильно ли ведет себя определенный протокол, или «полезная» информация в пакетах только выглядит правильной. Пример General-сигнатуры: 1037-TCP FRAG SYN FIN Host Sweep. Эта сигнатура вызывается, когда последовательность TCP-пакетов с SYN- и FIN- набором флагов отправлена множеству узлов с тем же самым портом адресата. Одновременное наличие флагов SYN и FIN является недопустимым.

Сигнатуры типа Connection охватывают 3000 и 4000 серии. Они анализируют трафик UDP-портов и TCP-соединений. Пример Connection-сигнатуры: 3001-TCP Port Sweep. Данная сигнатура действует тогда, когда последовательность TCP-подключений определена на аппаратном устройстве ко многим портам. Диапазон портов – меньше чем 1024.

Сигнатуры типа String универсальны и контролируют строки (текст) в пределах пакетов, которые считаются важными. Пример string-сигнатуры: 8000:2303-Telnet-+ + (Telnet сеанс инициализирован, и введена команда «++»).

Сигнатуры ACL применяются для анализа трафика с целью выявления деятельности, связанной с попытками обхода списков контроля доступа на маршрутизаторах. Эти сигнатуры относятся к серии 10000. Пример ACL-сигнатуры: 10000:1001-IP-Spoof Interface 2.

На рис. 4.17 изображен фрагмент окна с сигнатурами серии 2000, выделена сигнатура 2000-ICMP Echo Reply, которая срабатывает на исходящий ICMP эхо-ответ.

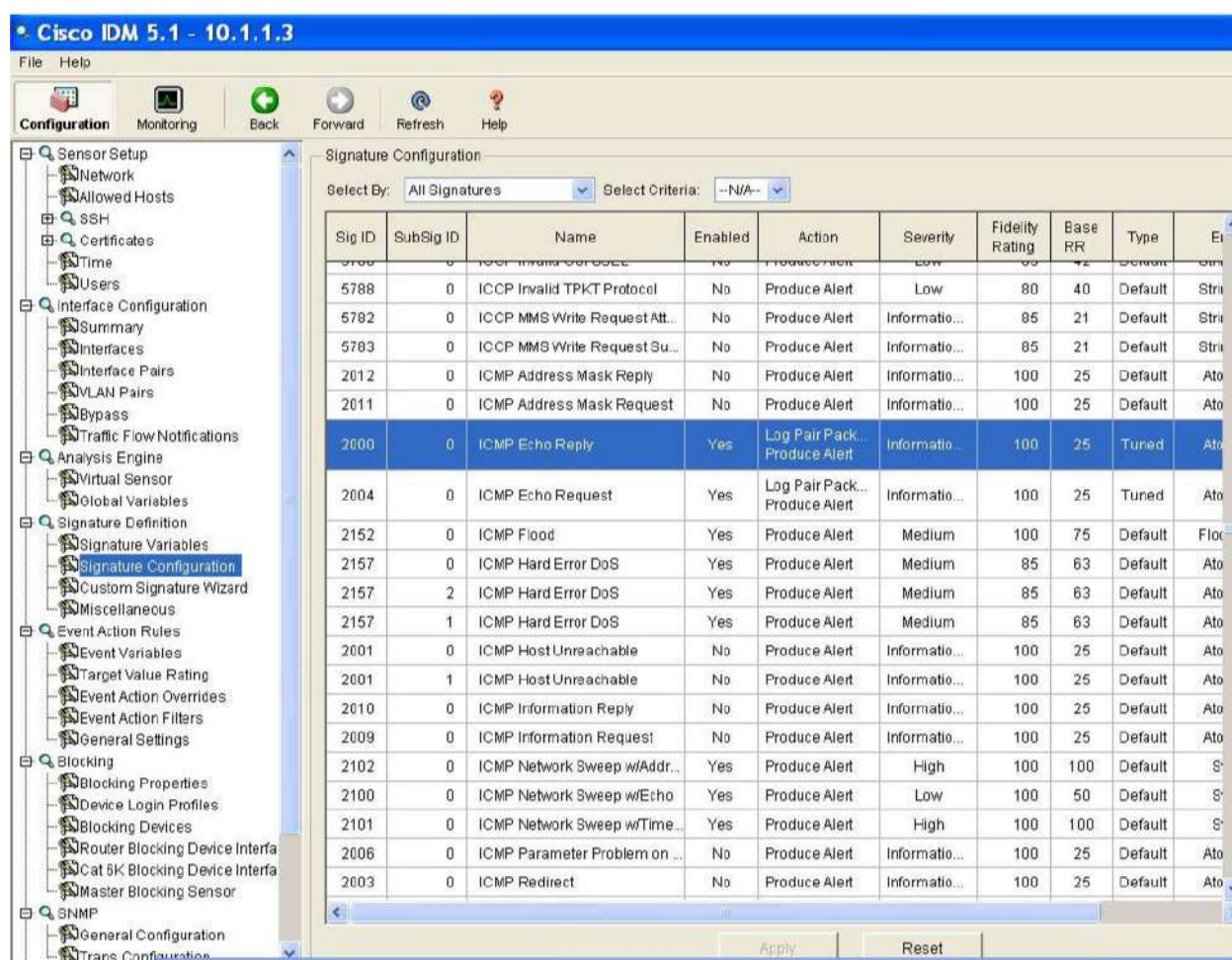


Рис. 4.17. Фрагмент окна настройки сигнатур обнаружения

По результатам анализа СОА выдает предупреждения (Alarm), каждому из которых назначен уровень тревоги: низкий (Low, 3), средний (Medium, 4), и высокий (High, 5). Также предупреждения могут быть еще двух уровней – неиспользуемый (None, 1) и информационный (Informational, 2).

Кроме того, используются служебные тревожные сообщения (сигнатуры 900-999). В частности, требует внимания сигнатура 993-Missed Packet Count. Появление данного сигнала тревоги связано с пропуском пакетов при анализе, что свидетельствует о загруженности СОА.

### ***ВЫПОЛНИТЬ!***

1. Найти следующие сигнатуры обнаружения атак:

- 2000-ICMP Echo Reply;
- 2004-ICMP Echo Request;
- 3002-TCP SYN Port Sweep.

### ***Обнаружение атак исследования сетевой топологии***

Выполним обнаружение двух атак, относящихся к классу исследовательских – ICMP-сканирование узла и SYN-сканирование портов. ICMP-сканирование выполним с помощью штатной утилиты ping, для сканирования портов будет использован сканер nmap.

**Список литературы, рекомендуемый к использованию по данной теме.**

*Основная:* 1,2

*Дополнительная:* 1, 2,3

*Интернет-ресурсы:* 1, 2, 3, 4

## Лабораторная работа № 17-18

### Тема 7: Сетевые фильтры

**Наименование темы:** «Обнаружение комплексных компьютерных атак»

**Формируемые компетенции:** ПК-5

**Теоретическая часть:**

#### *Программа лабораторной работы*

1. Cisco MARS.
2. Cisco Security Agent Cisco MARS.

### **Обнаружение компьютерных атак на узлы сети с использованием комплекса Cisco MARS**

#### ***Назначение комплекса Cisco MARS***

Система мониторинга, анализа и ответной реакции Cisco MARS (Cisco Security Monitoring, Analysis and Response System) является комплексным средством управления информационной безопасностью, позволяющим осуществлять обнаружение и отражение компьютерных атак. Система Cisco MARS выполняет на основе обнаружения атак изоляцию элементов, нарушающих нормальную работу сети. Кроме того, система обеспечивает анализ соответствия существующей политики безопасности организации и имеющихся нормативных документов.

Одна из основных задач Cisco MARS — централизованный сбор и преобразование предоставляемых сетевыми устройствами, сетевыми и узловыми сенсорами СОА данных о злонамеренной активности в удобную для анализа форму с целью устранения подтвержденных нарушений политики безопасности с учетом их приоритетов.

В качестве источников данных Cisco MARS могут выступать:

- сетевые устройства (маршрутизаторы и коммутаторы);
- средства защиты информации (межсетевые экраны, системы обнаружения атак, сканеры уязвимостей и антивирусные программы);
- сетевые узлы (серверы под управлением ОС Windows, Solaris и Linux);
- серверы приложений (базы данных, Web-серверы и серверы аутентификации);
- программы обработки сетевого трафика (Cisco NetFlow).

После сбора данные о событиях упорядочиваются в соответствии с топологической схемой, конфигурациями обнаруженных устройств, а также сходными типами атак. Сходные события объединяются в сеансы.

Для выявления нарушений политики безопасности вводятся системные и пользовательские правила, которые с учетом корреля-

ции событий применяются ко множеству сеансов. Cisco MARS поставляется с полным набором предварительно заданных правил, которые обновляются компанией Cisco Systems. Правила определяют большое количество комплексных атак. Вместе с тем предоставляется возможность создания в графической среде пользовательских правил.

Cisco MARS позволяет администраторам быстро определять все охваченные атакой объекты, вплоть до MAC-адресов как атакующих, так и атакованных узлов. Функция ответной реакции обнаруживает расположенные на пути атаки доступные устройства защиты и автоматически генерирует для них необходимые команды, которые пользователь может выполнить для отражения атаки.

С целью сокращения объема анализируемых администратором данных о событиях безопасности и назначения приоритетов ответных действий применяются функция корреляции событий и интерактивная инструментальная панель управления безопасностью. На панель выводится графическая информация о топологической схеме сети с отображением атак, их путей и подробных данных.

Кроме этого Cisco MARS предоставляет возможность создания отчетов. Имеются более 80 стандартных отчетов, а также генератор отчетов, позволяющий изменять существующие и создавать новые. Примерами отчетов являются:

- отчет по пользователям;
- подробные сведения по пользователям;
- подробные сведения о конечном узле;
- отчет первой десятки нарушений со стороны конечных узлов и пользователей и т. п.

Cisco MARS устанавливается в сети TCP/IP, выполняя передачу и прием системных журналов и запросов SNMP. Управление Cisco MARS осуществляется с помощью защищенного web-интерфейса.

Системы Cisco MARS являются надежными устройствами, оптимизированными для сбора больших объемов информации о событиях безопасности со скоростью свыше 10000 событий в секунду или свыше 300000 событий Cisco NetFlow в секунду.

## ***Аппаратная часть комплекса Cisco MARS***

Комплекс Cisco MARS является аппаратным устройством, выпускаемым в различных конфигурациях: 20, 50, 100, 100е, 200, GC, GCM и иных, основное отличие которых состоит в количестве процессоров и в объеме запоминающего устройства. Так Cisco MARS 20 имеет один процессор и жесткий диск объемом 120 Гб, а Cisco MARS 200 и выше обладают двумя процессорами и RAID-массивом объемом 1 Тб.

Более подробно рассмотрим комплекс Cisco MARS 20. Устройство предназначено для размещения в серверной стойке (рис. 5.1).

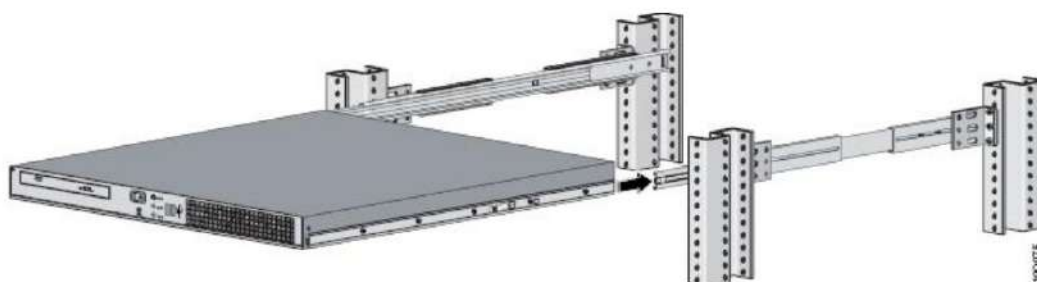


Рис. 5.1. Схема установки Cisco MARS 20 в серверной стойке

На лицевой панели устройства (рис. 5.2) расположены: устройство чтения DVD-дисков и кнопка открытия (1, 2), кнопка включения питания и индикатор (3, 4), отверстия для крепежа (5) и кнопка сброса (6).

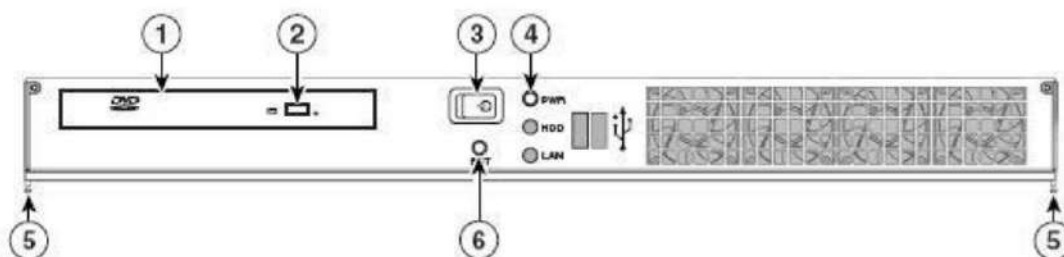


Рис. 5.2. Лицевая панель Cisco MARS 20

На задней панели устройства (рис. 5.3) расположены: разъемы для подключения клавиатуры и «мыши» (1, 2); порты – параллельный (3), модемный (6, 7), VGA (10), последовательный (11), USB (12, 13); разъем и кнопка питания (8, 9); два сетевых интерфейса типа FastEthernet (4, 5).

Внутри устройство представляет собой компьютер, оборудованный жестким магнитным диском с операционной системой Linux и специализированным программным обеспечением.

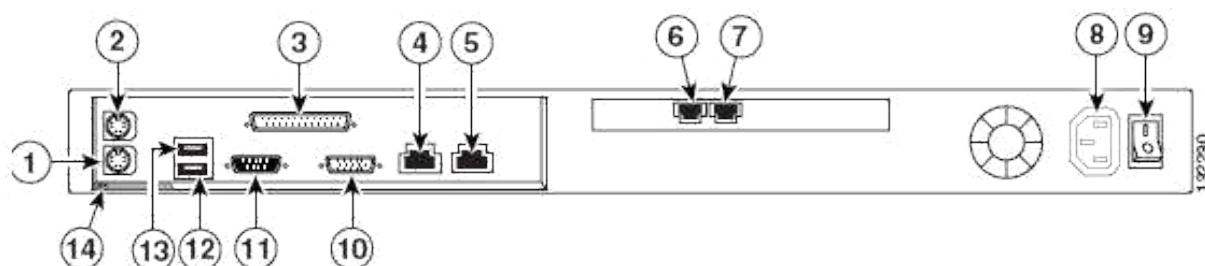


Рис. 5.3. Задняя панель Cisco MARS 20

### *Структура лабораторного стенда*

Для изучения средств обнаружения комплексных атак рассмотрим некоторую организацию, использующую web-сервер, развернутый на базе Microsoft Internet Information Server в среде операционной системы Windows 2003 Server. Для обнаружения компьютерных атак в сеть внедрено аппаратное устройство Cisco MARS, которое в качестве входных данных использует события, генерируемые COA Cisco IDS Sensor, выполняющей мониторинг сетевого трафика, и службой Snare, осуществляющей анализ журналов web-сервера IIS, функционирующего в ОС Windows 2003 Server (рис. 5.4).

Также в сети функционируют две рабочие станции ОС Windows XP, одна из них предназначена для администрирования комплексом Cisco MARS и COA Cisco IDS Sensor, другая имитирует стороннего наблюдателя (злоумышленника). В сети действуют две подсети: технологическая (192.168.10.0/24) и управляющая (10.0.0.0/24). В технологической подсети расположен защищаемый web-сервер, к ней подключены сенсорные интерфейсы Cisco IDS Sensor и интерфейс сбора событий Cisco MARS. Для имитации некоторых атакующих воздействий сервер ОС Windows 2003 Server будет заменяться на рабочую станцию ОС Windows XP, а также атакующий компьютер. В управляющей подсети присутствует рабочая станция ОС Windows XP, к ней подключены интерфейсы управления Cisco MARS и Cisco IDS Sensor. Атакующий компьютер представлен рабочими станциями ОС Windows XP или ОС Linux OpenSUSE, имеющими два сетевых интерфейса – один

для подключения в технологическую сеть, другой – для управляющей сети.

Для развертывания данной сети предложен виртуальный стенд, состоящий из четырех виртуальных образов и двух виртуальных сетей VMware. Основная ОС имитирует компьютер администратора.

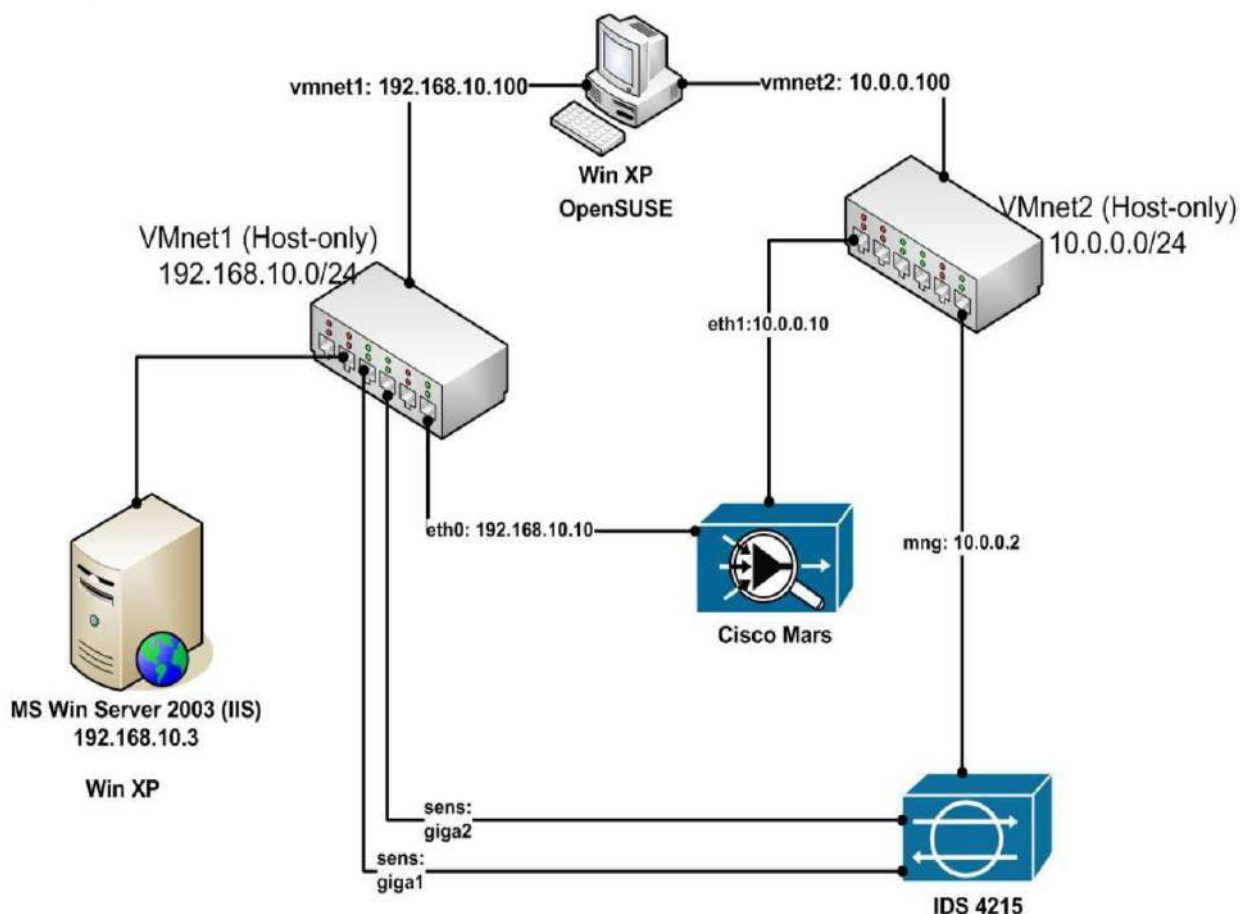


Рис. 5.4. Структура имитируемой сети

Технологическая подсеть подключена к виртуальной сети VMnet1, управляющая – к сети VMnet2.

Для выполнения работы понадобится следующее ПО:

- виртуальный образ комплекса Cisco MARS (версия 6.0.3);
- виртуальный образ COA Cisco IDS Sensor 4215 (используется образ, настроенный в процессе выполнения задания по п. п. 4.1.3, 4.1.4);
- виртуальный образ ОС MS Windows 2003 Server;
- виртуальный образ ОС MS Windows XP;
- виртуальный образ ОС Linux OpenSUSE;
- дистрибутив SnareIISSetup-1.1.exe;
- дистрибутив SnareSetup-3.1.7-MultiArch.exe;

- дополнение для построения графиков в web-интерфейсе SVGView.exe.

В составе стенда присутствуют следующие образы операционных систем:

- образ ОС Windows 2003 Server с одним сетевым интерфейсом, подключенным к подсети VMnet1 192.168.10.0/24 (IP-адрес 192.168.10.3);

- образ ОС Windows XP с одним сетевым интерфейсом, подключенным к подсети VMnet1 192.168.10.0/24 (IP-адрес 192.168.10.3);

- образ ОС Windows XP с двумя сетевыми интерфейсами, подключенными к подсети VMnet1 192.168.10.0/24 (IP-адрес 192.168.10.100) и к подсети VMnet2 10.0.0.0/24 (IP-адрес 10.0.0.100);

- образ ОС Linux OpenSUSE с одним сетевым интерфейсом, подключенным к подсети VMnet1 192.168.10.0/24 (IP-адрес 192.168.10.100);

- образ Cisco MARS с двумя сетевыми интерфейсами, подключенными к подсети VMnet1 192.168.10.0/24 (IP-адрес 192.168.10.10) и к подсети VMnet2 10.0.0.0/24 (IP-адрес 10.0.0.10);

- образ Cisco IDS Sensor с тремя сетевыми интерфейсами, один подключен к подсети VMnet2 10.0.0.0/24 (IP-адрес 10.0.0.2), два подключены к подсети VMnet1 для захвата трафика и не имеют собственного IP-адреса. Потребуется перенастройка.

### ***Настройка ОС Windows 2003 Server***

#### **ВЫПОЛНИТЬ!**

1. Настроить IP-адрес 192.168.10.3, маска 255.255.255.0. Установить MAC-адрес 000C29F734A2. Для этого необходимо в «Диспетчере устройств» в разделе «Сетевые адаптеры» выбрать сетевой адаптер, из контекстного меню «Свойства» выбрать «Дополнительно – Сетевой адрес». Присвоить значение 000C29F734A2 (рис. 5.5).
2. Установить web-сервер базе Microsoft Internet Information Server (IIS). Выбрать «Пуск – Программы – Администрирование – Управление ролями» – «Добавить или убрать роль» – Сервер приложений (IIS, ASP.NET) (рис. 5.6).

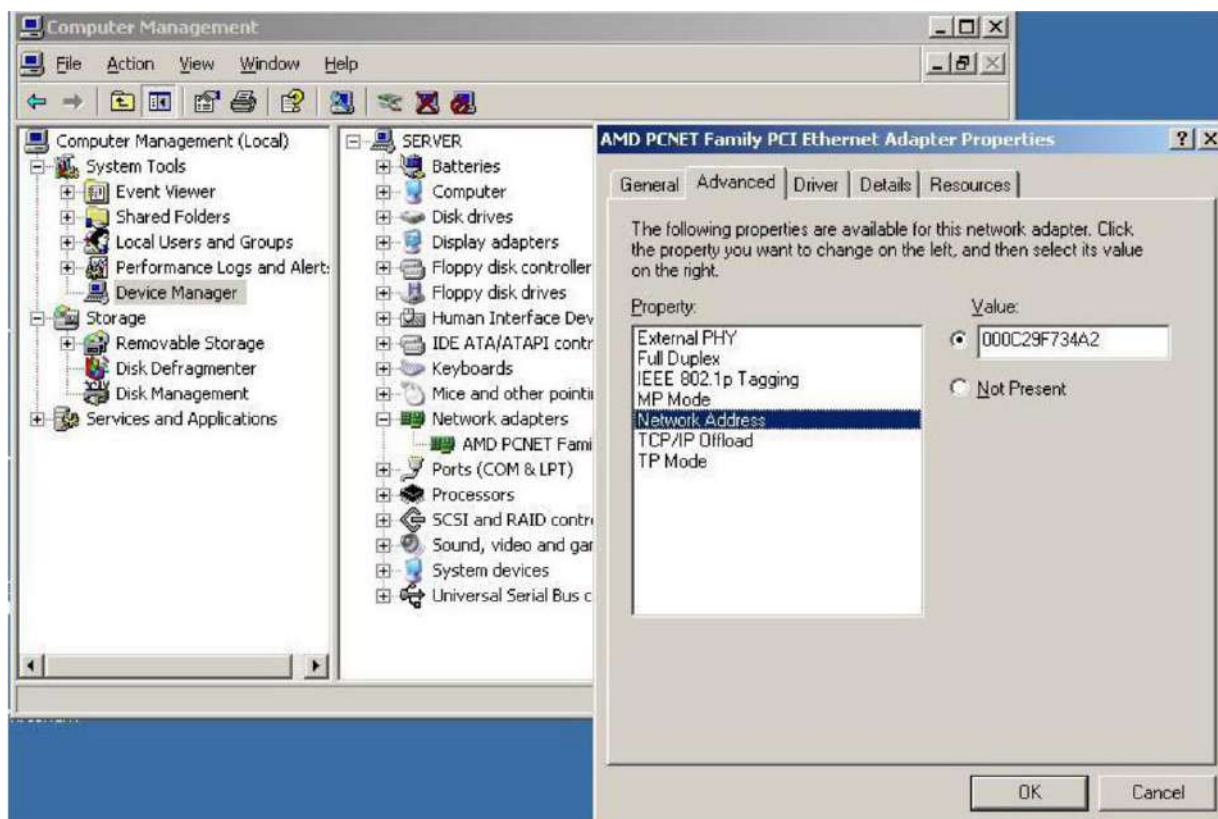


Рис. 5.5. Окно настройки MAC-адреса

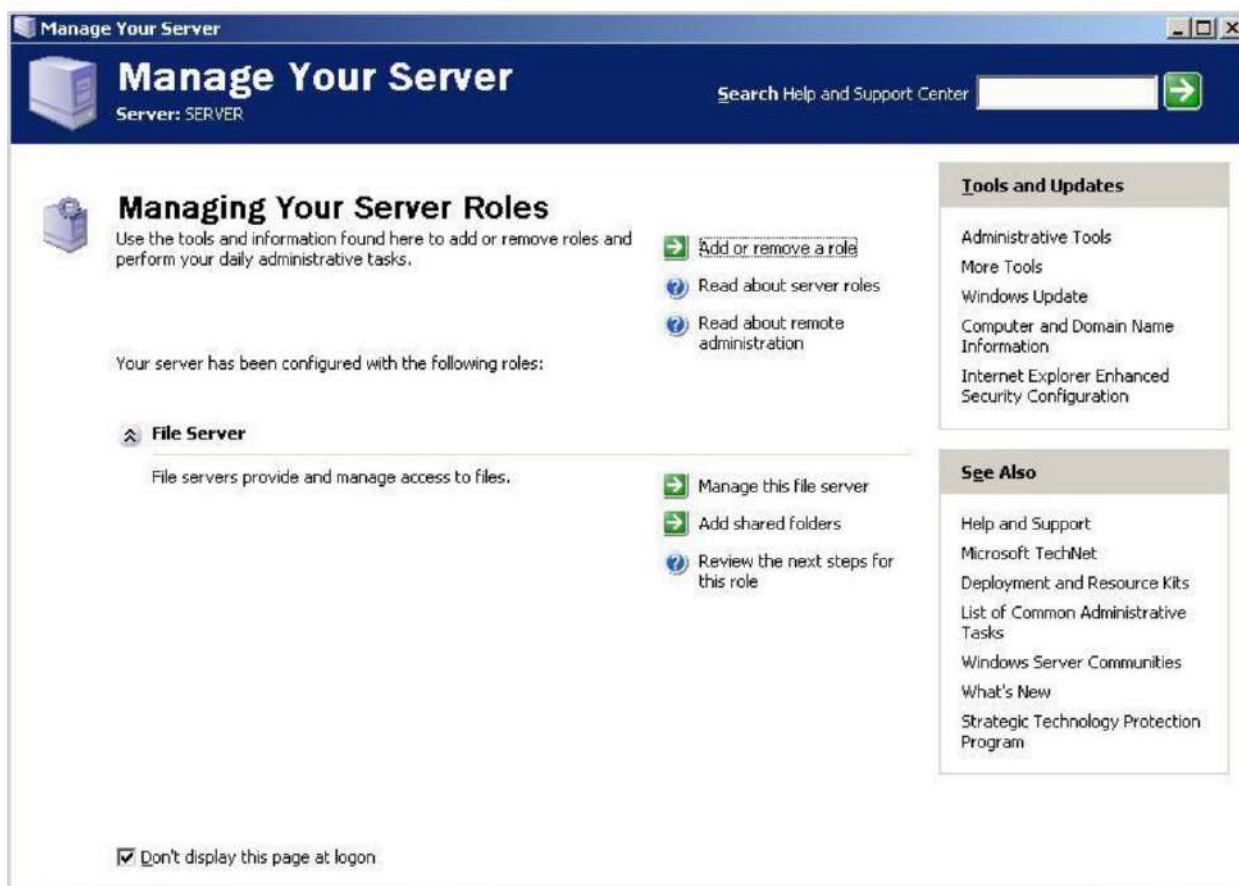


Рис. 5.6. Окно установки web-сервера

3. Проверить работоспособность установленного web-сервера, указав в web-браузере основной ОС адрес `http://192.168.10.3`.
4. Установить и настроить службу Snare для сбора информации из системных журналов ОС Windows и ее пересылки на комплекс Cisco MARS. Для этого необходимо запустить `SnareSetup-3.1.7-MultiArch.exe`. После установки необходимо выбрать «Все программы – InterSect Alliance – Snare for Windows». В меню Network Configuration установить следующие настройки (рис. 5.7):
  - Override detected DNS Name with – 192.168.10.3;
  - Destination Snare Server address – 192.168.10.10;
  - Destination Port – 514;
  - Allow SNARE to automatically set audit configuration;
  - Allow SNARE to automatically set file audit configuration;
  - Enable SYSLOG Header.Применить настройки Apply the Latest Audit Configuration.

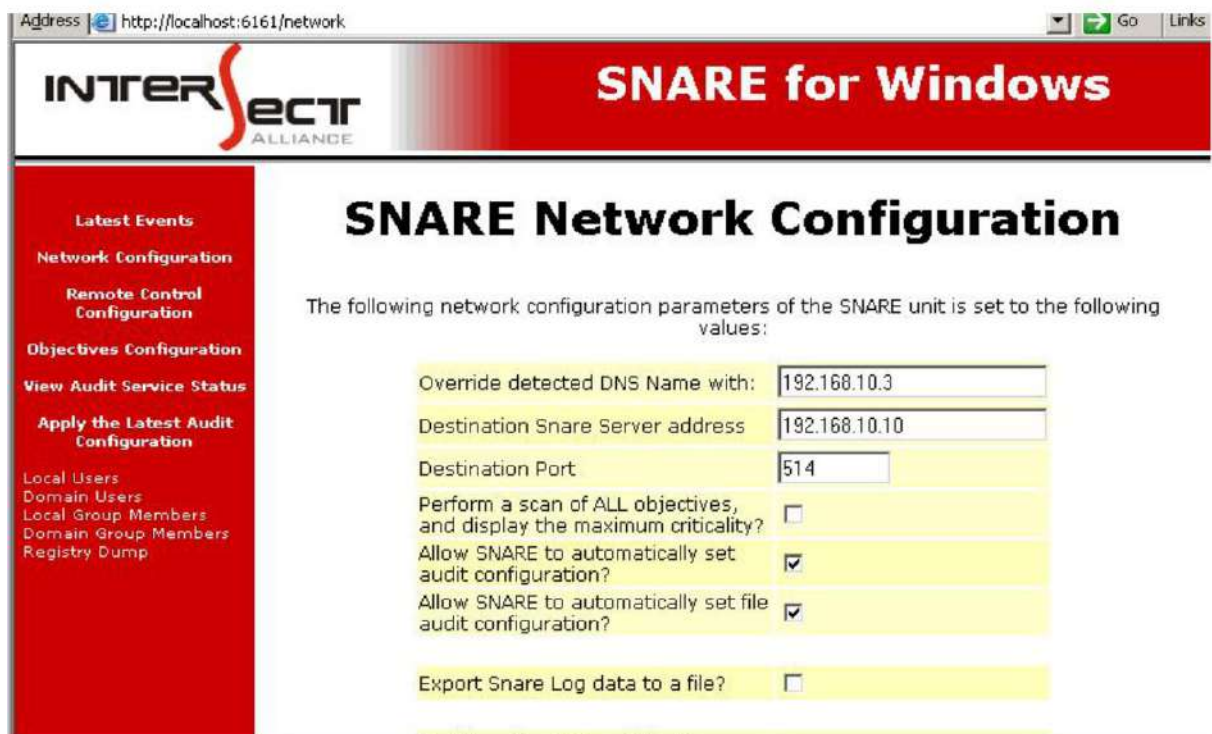


Рис. 5.7. Окно настройки службы Snare

5. Установить и настроить службу SnareIIS для отправки журналов на комплекс Cisco MARS. Для этого запустить `SnareIISSetup-1.1.exe`. Для настройки выбрать «Пуск – Все программы – InterSect Alliance – Audit Configuration».

В графе Target Host установить IP-адрес Cisco MARS (192.168.10.10). В графе Log Directory задать путь до каталога, где будут храниться журналы (log-файлы). По умолчанию – это каталог C:\LogFiles. В графе Destination необходимо выбрать тип – Syslog (рис. 5.8).

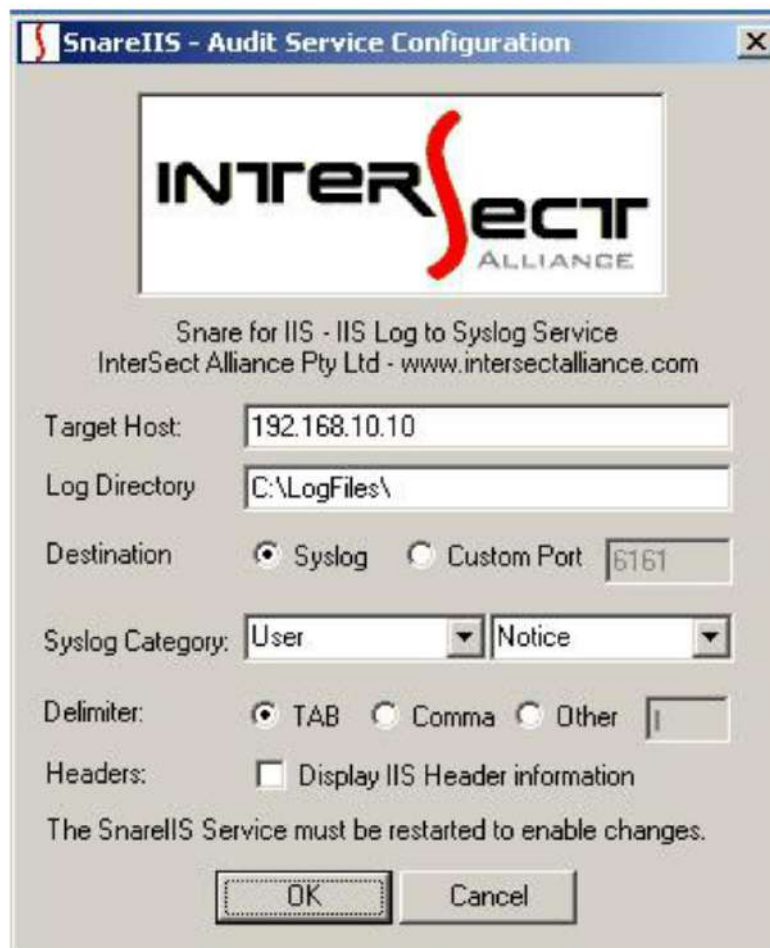


Рис. 5.8. Окно пастройки службы SnareIIS

6. Настроить web-сервер на ведение журналов. Для этого в окне Internet Service Manager выбрать пункт Web site, затем выбрать Свойства объекта Default Web Site. В поле Active log format выбрать W3C Extended Log File Format (рис. 5.9).
7. В пункте Properties... выполнить настройки ежедневного ведения журналов в каталог по умолчанию (рис. 5.10).
8. Убедиться, что службы Snare и SnareIIS запущены. Это можно сделать с помощью Диспетчера устройств во вкладке «Процессы» (должны присутствовать процессы SnareIIS.exe и SnareCore.exe).

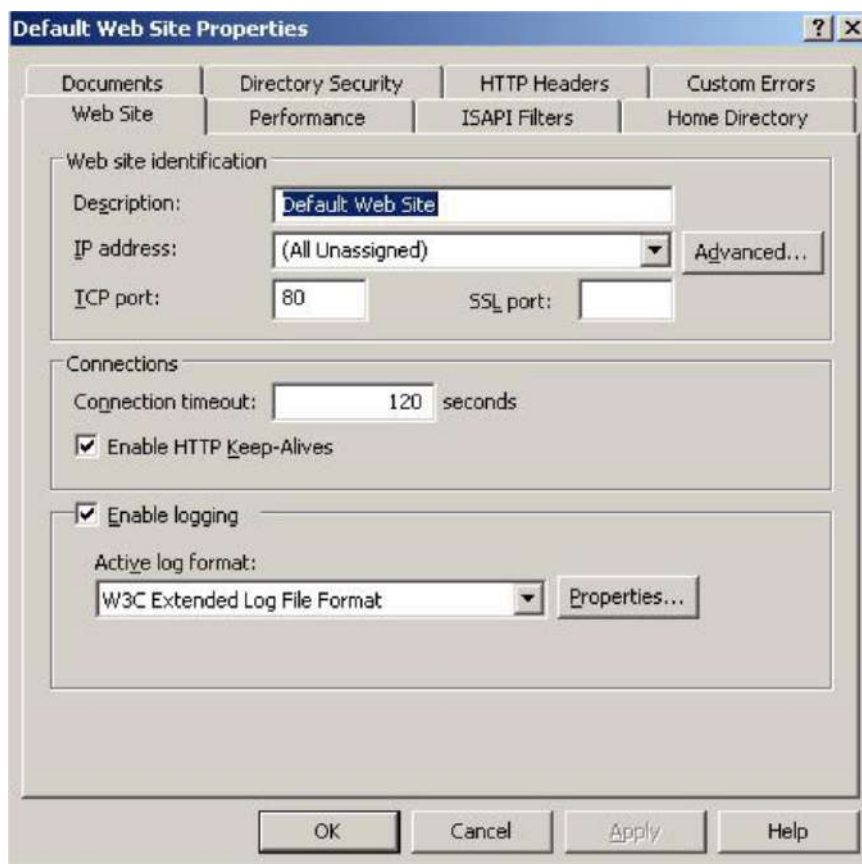


Рис. 5.9. Настройка web-сервера на ведение журнала

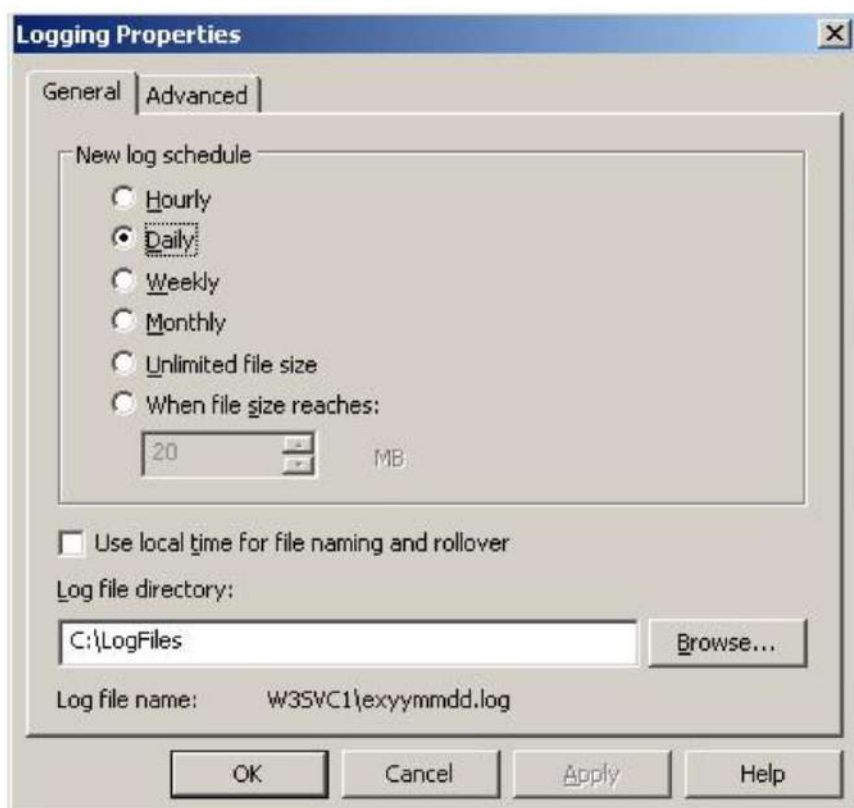


Рис. 5.10. Настройка службы ведения журнала

## Настройка сетевых интерфейсов Cisco MARS

### ВЫПОЛНИТЬ!

9. Открыть имеющийся образ Cisco MARS. В настройках виртуального образа убедиться, что один сетевой интерфейс Network Adapter принадлежит сети VMnet1, а другой Network Adapter2 – сети VMnet2.
10. Запустить образ, после загрузки системы ввести имя учетной записи администратора (по умолчанию padmin) и пароль (padmin).
11. Настроить IP-адреса следующим образом: для двух Ethernet-интерфейсов (eth0 и eth1) комплекса Cisco MARS – адрес 192.168.10.10 для сетевого интерфейса eth0 и адрес 10.0.0.10 для интерфейса eth1. Для этого необходимо ввести команду `ifconfig eth0 192.168.10.10 255.255.0.0` и нажать Enter. На вопрос о перезагрузке виртуальной машины с целью применения изменений, ввести Yes. После перезагрузки ОС Cisco MARS повторить настройку для сетевого интерфейса eth1. Пример настроенных интерфейсов приведен на рис. 5.11. Остальные настройки, такие как dns, host-name, gateway, route можно оставить по умолчанию.

```
[padmin]# ifconfig
eth0 Link encap:Ethernet HWaddr 00:0C:29:09:E9:78
 inet addr:192.168.10.10 Bcast:192.168.10.255 Mask:255.255.255.0
 inet6 addr: fe80::20c:29ff:fe09:e978/64 Scope:Link
 UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
 RX packets:0 errors:0 dropped:0 overruns:0 frame:0
 TX packets:9 errors:0 dropped:0 overruns:0 carrier:0
 collisions:0 txqueuelen:1000
 RX bytes:0 (0.0 b) TX bytes:546 (546.0 b)
 Interrupt:185 Base address:0x2000

eth1 Link encap:Ethernet HWaddr 00:0C:29:09:E9:82
 inet addr:10.0.0.10 Bcast:10.0.0.255 Mask:255.255.255.0
 inet6 addr: fe80::20c:29ff:fe09:e982/64 Scope:Link
 UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
 RX packets:0 errors:0 dropped:0 overruns:0 frame:0
 TX packets:12 errors:0 dropped:0 overruns:0 carrier:0
 collisions:0 txqueuelen:1000
 RX bytes:0 (0.0 b) TX bytes:672 (672.0 b)
 Interrupt:169 Base address:0x2000

[padmin]# _
```

Рис. 5.11. Настройка сетевых интерфейсов Cisco MARS

12. Из основной ОС командой **ping** убедиться в правильной настройке сетевых параметров, а именно, в возможности

получить ICMP-ответ от каждого из сетевых интерфейсов комплекса Cisco MARS. После чего проверить доступность

web-интерфейса комплекса: <https://192.168.10.10> или <https://10.0.0.10>. Обязательно указывать режим https, а не http.

13. Для построения графиков в web-интерфейсе, необходимо в основной ОС установить дополнение для построения графиков – SVGView.exe. После этого перезапустить web-браузер Internet Explorer. При успешном доступе установка SVGView.exe будет предложена автоматически. Если web-браузер будет блокировать попытку сохранения, то необходимо в верхней части экрана нажать появившееся уведомление.

### ***Настройка сетевого взаимодействия устройств Cisco IDS Sensor, Cisco MARS и сервера Windows 2003 Server***

#### **ВЫПОЛНИТЬ!**

14. Открыть и запустить ранее настроенный образ COA Cisco IDS Sensor.

15. В режиме командной строки перенастроить IP-адрес интерфейса управления на 10.0.0.2 (см. п. 4.1.3).

16. Добавить IP-адрес устройства Cisco MARS в конфигурацию COA Cisco IDS Sensor для их связи по протоколу SSH. Для этого воспользоваться web-интерфейсом Cisco IDS Sensor. В окне Configuration выбрать Sensor Setup – Certificates → Trusted Hosts. Нажать Add и ввести IP-адрес Cisco MARS – 10.0.0.10.

17. Настроить Windows 2003 Server для передачи от него информации в комплекс Cisco MARS и отображения сервера при построении схемы сети. Для этого в ОС Windows Server 2003 необходимо обратиться к web-интерфейсу Cisco MARS по адресу <https://10.0.0.10>.

18. В web-интерфейсе перейти по вкладкам Admin – Security and Monitor Devices – Add. В списке Device Type выбрать Add SW Security apps on a new host.
19. В появившемся окне в параметрах Device Name и IP addresses ввести в первом параметре Server и во втором – 192.168.10.3. В параметре Operating System выбрать Windows. Затем нажать Logging Info.
20. В новом окне выбрать Windows 2003 Server. В параметре logging mechanism выбрать Receive. Нажать кнопку Submit.
21. Добавить в параметр Interface IP Address and Network Mask IP-адрес ОС Windows Server 2003 – 192.168.10.3/32. Чтобы применить новые параметры нажать кнопку Apply.
22. Во вкладке Reporting Applications выбрать раздел Generic Web Server Generic. Нажать Add, выбрать Windows Web Log format, затем указать W3C\_EXTENDED\_LOG.
23. Последовательно нажать Submit, Done и Activate для сохранения и применения новых настроек.
24. Зайти на web-интерфейс ОС Cisco IDS 4215. Перейти по вкладкам Admin – Security and Monitor Devices – Add.
25. В списке Device Type выбрать Cisco IDS 4.0. В параметрах Device Name и IP Addresses установить значения ids4215 и 10.0.0.2. Параметр Access type установить в значение SSL. Ввести имя учетной записи cisco и пароль (например, Qwe12345). В параметре Monitored Networks добавить сеть 192.168.10.0 с маской 255.255.255.0. Для сохранения и применения настроек нажать последовательно Submit и Activate.
26. Для отображения устройств с ОС Windows 2003 Server и Cisco IDS Sensor на схеме сети в ОС Cisco MARS следует последовательно зайти на вкладки Admin – Security and Monitor Devices и убрать «Облако» напротив каждого из устройств. Для применения настроек нажать Active.

## ***Создание сигнатуры компьютерной атаки в COA Cisco IDS Sensor***

В данном параграфе вернемся к созданию сигнатур в COA Cisco IDS Sensor и введем сигнатуру обнаружения доступа к Web-серверу.

### ***ВЫПОЛНИТЬ!***

27. В браузере основной ОС задать адрес интерфейса управления сенсора <https://10.0.0.2> (см. п. 4.1.4).
28. В графическом интерфейсе Cisco IDS Device Manager зарегистрироваться учетной записью cisco.
29. В окне Cisco IDM 5.1 (рис. 4.17) выбрать раздел Signature Configuration. Нажать кнопку Add для добавления сигнатуры.
30. Задать имя сигнатуры и указать область ее действия (рис. 5.12) – эта сигнатура будет связана с определенным IP-адресом (Engine → Atomic IP). Указать действие, которое будет осуществляться при ее обнаружении – перехват сетевого пакета (Event Action → Produce Verbose Alert).
31. Назначить IP-адрес (рис. 5.13), при обращении к которому будет срабатывать сигнатура (Specify IP Addr Options → IP Addresses Options → IP Addresses → Specify Destination IP Addresses = 192.168.10.3).
32. Подтвердить ввод кнопкой ОК.
33. Включить запись всех пакетов для IP-адреса 192.168.10.3, для этого перейти в окно Monitoring, в разделе IP Logging добавить запись, в которой указать IP-адрес и определить время захвата (например, 10 минут) (рис. 5.14).

**Edit Signature**

| Name                                                     | Value                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|----------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Signature ID:                                            | 60000                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| SubSignature ID:                                         | 0                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <input checked="" type="checkbox"/> Alert Severity:      | Medium                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <input checked="" type="checkbox"/> Sig Fidelity Rating: | 75                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <input checked="" type="checkbox"/> Promiscuous Delta:   | 0                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <input checked="" type="checkbox"/> Sig Description:     | <div> <div> <div><input checked="" type="checkbox"/> Signature Name:</div> <div>passwd_site</div> </div> <div> <div><input checked="" type="checkbox"/> Alert Notes:</div> <div>My Sig Info</div> </div> <div> <div><input checked="" type="checkbox"/> User Comments:</div> <div>Sig Comment</div> </div> <div> <div><input checked="" type="checkbox"/> Alert Traits:</div> <div>0</div> </div> <div> <div><input checked="" type="checkbox"/> Release:</div> <div>custom</div> </div> </div> |
| <input checked="" type="checkbox"/> Engine:              | Atomic IP                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|                                                          | <div> <div><input checked="" type="checkbox"/> Event Action:</div> <div> <div>Produce Verbose Alert</div> <div>Request Block Connection</div> <div>Request Block Host</div> <div>Request SNMP Trap</div> <div>Reset TCP Connection</div> </div> </div>                                                                                                                                                                                                                                          |

☒ Parameter uses the Default Value. Click the icon to edit the value.  
☒ Parameter uses a User-Defined Value. Click the icon to restore the default value.

OK Cancel Help

Рис. 5.12. Окно создания сигнатур COA Cisco IDS Sensor

☒ Specify IP Addr Options: Yes

☒ IP Address Options: IP Addresses

Specify Source IP Addresses: No

☒ Specify Destination IP Addresses: Yes

Destination IP Address Range: 192.168.10.3

Рис. 5.13. Фрагмент окна создания сигнатур

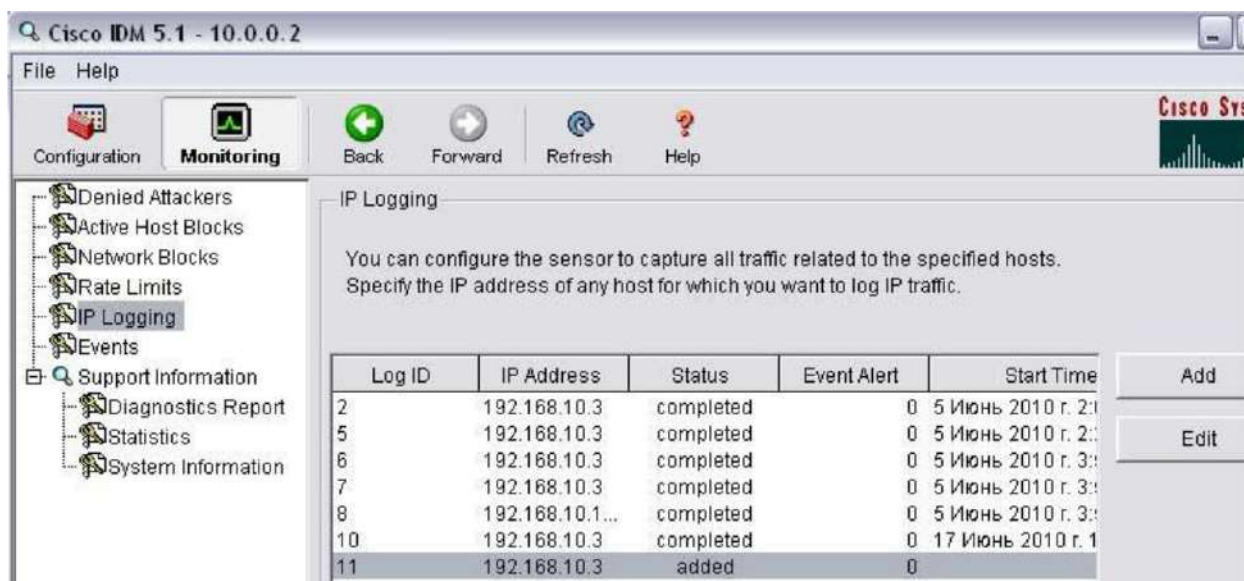


Рис. 5.14. Фрагмент окна регистрации событий

### *Имитация и обнаружение атакующего воздействия*

#### **ВЫПОЛНИТЬ!**

34. С целью имитации атакующего воздействия, обнаруживаемого созданной сигнатурой, в web-браузере основной ОС перейти по адресу web-сервера <http://192.168.10.3>.
35. Произвести сканирование IP-адреса web-сервера с помощью программы Nmap (например, `nmap.exe -v -A -p 10-1024 192.168.10.3`).
36. Проанализировать сетевой трафик, полученный в результате мониторинга. Для этого фрагмент трафика сохранить на диске (Monitoring → IP Logging → Stop → Download).
37. Отобразить результаты срабатываний сигнатур (Monitoring → Events → Show all events currently stored on the sensor).
38. Найти результаты обнаружения атаки типа сканирование портов (рис. 5.15), а также созданной сигнатуры (рис. 5.16).



Рис. 5.15. Событие типа сканирование портов

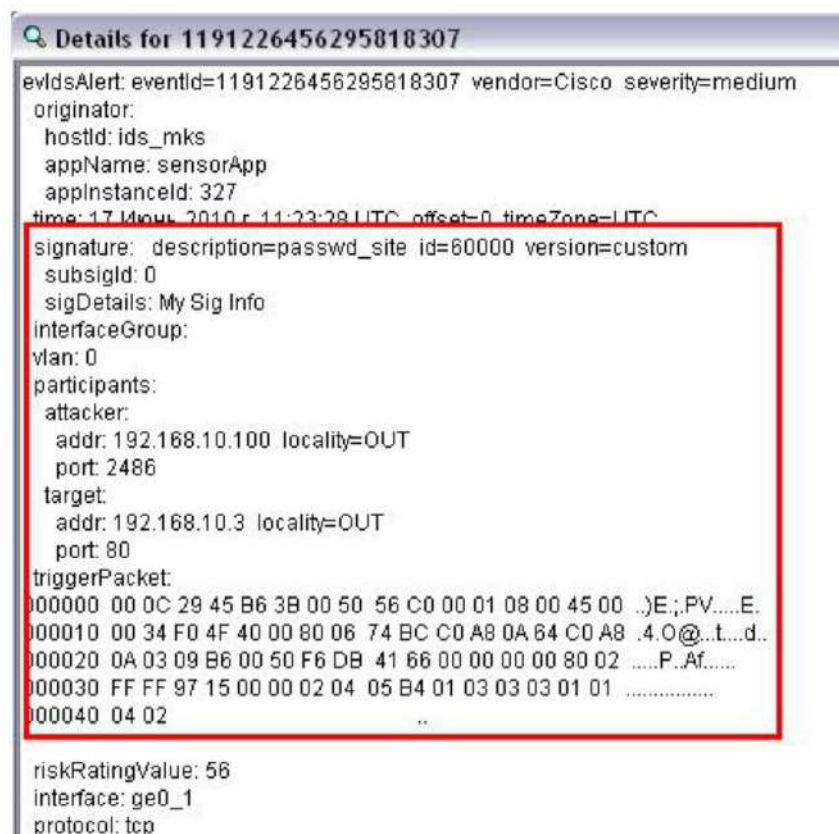


Рис. 5.16. Событие обнаружения созданной сигнатуры

39. Подключиться из основной ОС к web-интерфейсу Cisco MARS.

40. Включить режим просмотра событий (вкладка Query/Reports). Задать условия для построения отчета (период, тип событий, источник) и нажать Submit Inline. По умолчанию выводятся все события за последние 10 минут (рис. 5.17).

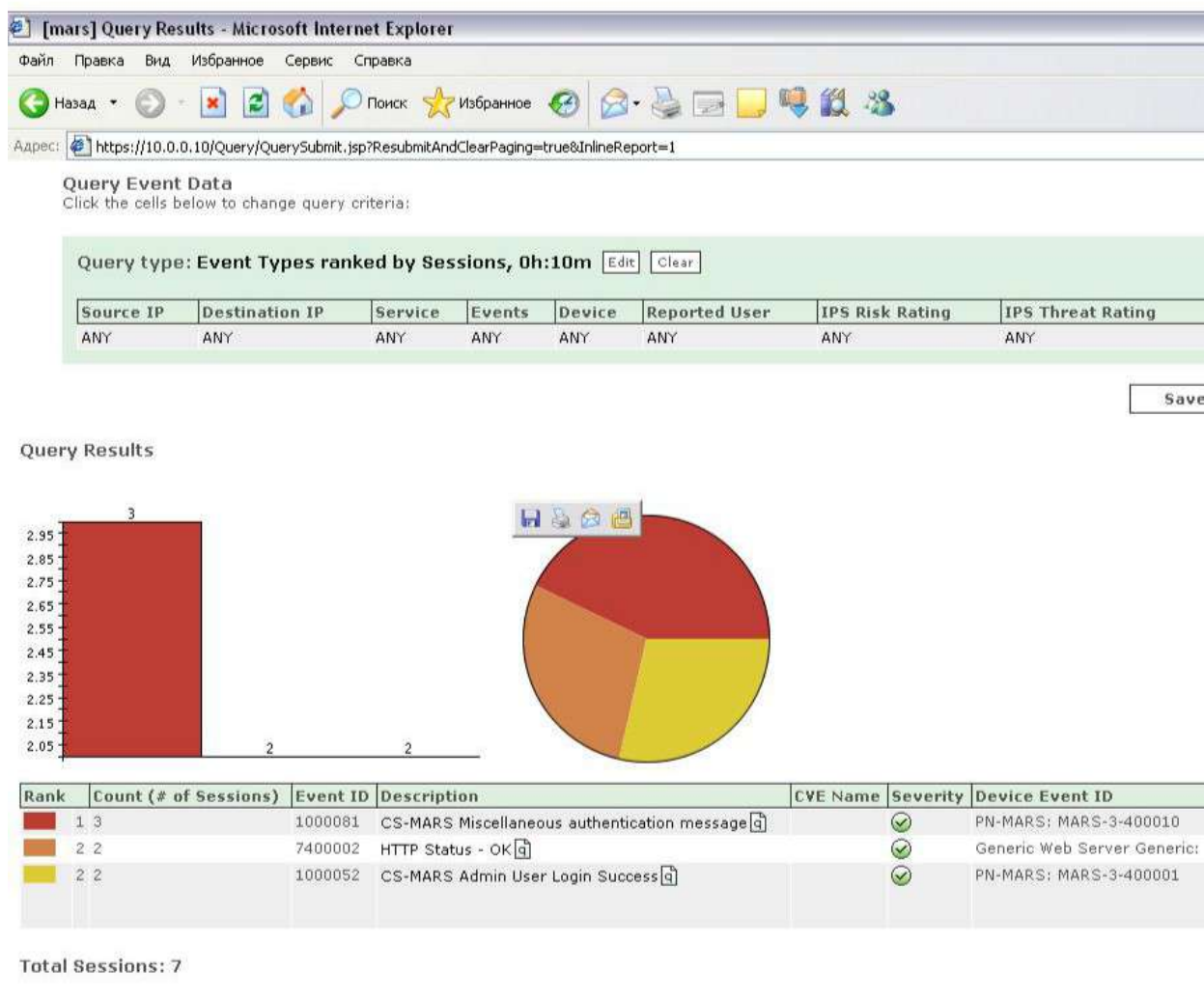


Рис. 5.17. Режим просмотра событий

41. Включить режим просмотра инцидентов (вкладка Incidents). Инцидент – это событие, которое соответствует правилу (Rules). Сработавшие правила отображаются на диаграмме атак (вкладка Summary) (рис. 5.18). При выборе определенного Incident ID откроется окно с подробным описанием данного инцидента (источник, атакуемый, описание инцидента) (рис. 5.19).

42. В отчете по данной работе привести снимки экранов инцидентов, связанных с функционированием атакуемого web-сервера.

The screenshot shows the Cisco MARS web interface in Microsoft Internet Explorer. The browser address bar shows <https://10.0.0.10/incidents/index.jsp>. The page title is "[mars] Incidents - Microsoft Internet Explorer". The Cisco logo is visible in the top left. The navigation bar includes links for SUMMARY, INCIDENTS, QUERY / REPORTS, RULES, and MANAGEMENT. The INCIDENTS tab is selected, showing a sub-header for "CS-MARS Standalone: mars v6.0". The page indicates the user is Administrator (dnadmin) and shows the date Jun 25, 2010 9:00 AM. Below the navigation bar, there are fields for Incident ID and Session ID. A section titled "Recent Incidents for Last" with a dropdown set to "One Year" is followed by a "View" button. Below this, there are filters for "All Severities" and "All Rules". The main table lists incidents with columns: Incident ID, Event Type, Matched Rule, Action, Time, and Path. The table contains 8 rows of incident data.

| Incident ID | Event Type                            | Matched Rule                                   | Action | Time                                                        | Path |
|-------------|---------------------------------------|------------------------------------------------|--------|-------------------------------------------------------------|------|
| I:1511372   | Inactive CS-MARS reporting device     | System Rule: Inactive CS-MARS Reporting Device |        | Jun 18, 2010 11:00:02 AM YEKST                              |      |
| I:1511371   | Inactive CS-MARS reporting device     | System Rule: Inactive CS-MARS Reporting Device |        | Jun 18, 2010 10:00:01 AM YEKST                              |      |
| I:907595    | TCP SYN Port Sweep                    | System Rule: Scans: Stealth                    |        | Jun 3, 2010 2:34:59 PM YEKST - Jun 3, 2010 2:36:29 PM YEKST |      |
| I:907595    | TCP SYN Port Sweep                    | System Rule: Scans: Stealth                    |        | Jun 3, 2010 2:29:59 PM YEKST - Jun 3, 2010 2:30:59 PM YEKST |      |
| I:907594    | TCP SYN Port Sweep                    | System Rule: Scans: Stealth                    |        | Jun 3, 2010 2:29:29 PM YEKST                                |      |
| I:907593    | Inactive CS-MARS reporting device     | System Rule: Inactive CS-MARS Reporting Device |        | Jun 3, 2010 2:00:01 PM YEKST                                |      |
| I:907592    | Inactive CS-MARS reporting device     | System Rule: Inactive CS-MARS Reporting Device |        | Jun 3, 2010 1:00:05 PM YEKST                                |      |
| I:907591    | HTTP Status - Not Found               | Web-server (Local)                             |        | Jun 3, 2010 11:40:07 AM YEKST                               |      |
| I:403775    | CS-MARS dnadmin User Password Changed | System Rule: Modify Network Config             |        | Jun 2, 2010 10:44:24 AM YEKST                               |      |

Рис. 5.18. Окно инцидентов

The screenshot shows the Cisco MARS web interface in Microsoft Internet Explorer, displaying the details for incident 907595. The browser address bar shows [https://10.0.0.10/incidents/IncidentDetails.jsp?Incident\\_Id=907595](https://10.0.0.10/incidents/IncidentDetails.jsp?Incident_Id=907595). The page title is "[mars] Incident Details - Microsoft Internet Explorer". The Cisco logo is visible in the top left. The navigation bar includes links for SUMMARY, INCIDENTS, QUERY / REPORTS, RULES, and MANAGEMENT. The INCIDENTS tab is selected, showing a sub-header for "CS-MARS Standalone: mars v6.0". The page indicates the user is Administrator (dnadmin) and shows the date Jun 25, 2010 9:00 AM. Below the navigation bar, there are fields for Incident ID and Session ID. A section titled "Recent Incidents for Last" with a dropdown set to "One Year" is followed by a "View" button. Below this, there are filters for "All Severities" and "All Rules". The main table lists incidents with columns: Incident ID, Event Type, Matched Rule, Action, Time, and Path. The table contains 8 rows of incident data.

Incident ID: 907595

Time Range: 0h : 10m

Action: None  
Provider: Cisco

Description: This rule detects highly suspicious scans that are performed by sending malformed TCP/IP packets with an intent to discover host and application characteristics such as OS name, OS version etc. A vulnerability assessment tool such as Nmap can generate such scans. The source of the scans, if from inside the trusted network, must be investigated to see if it is from an authorized source. A MARS appliance may be performing such a test as part of false positive analysis.

| Offset | Open | Source IP | Destination IP | Service Name | Event                                                          | Device | Reported User | IPS Risk Rating | IPS Threat Rating | Keyword | Severity | Count | Close | Operation |
|--------|------|-----------|----------------|--------------|----------------------------------------------------------------|--------|---------------|-----------------|-------------------|---------|----------|-------|-------|-----------|
| 1      |      | ANY       | ANY            | ANY          | Probe/PortSweep/Stealth, Probe/FromScanner, Probe/Host/Stealth | ANY    | None          | ANY             | ANY               | ANY     | ANY      | 1     |       |           |

Expand All Collapse All

| Offset | Session / Incident ID | Event Type         | Source IP / Port | Destination IP / Port | Protocol | Time                         | Reporting Device | Reported User | Path / Mitigate | Tune                  |
|--------|-----------------------|--------------------|------------------|-----------------------|----------|------------------------------|------------------|---------------|-----------------|-----------------------|
| 1      |                       | TCP SYN Port Sweep | 192.168.10.100   | 3837                  | TCP      | Jun 3, 2010 2:29:59 PM YEKST | ids_mks          |               |                 | False Positive Tuning |
| 1      | S:807744, I:907595    | TCP SYN Port Sweep | 192.168.10.100   | 3860                  | TCP      | Jun 3, 2010 2:29:59 PM YEKST | ids_mks          |               |                 | False Positive Tuning |
| 1      | S:807752, I:907595    | TCP SYN Port Sweep | 192.168.10.100   | 4655                  | TCP      | Jun 3, 2010 2:30:59 PM YEKST | ids_mks          |               |                 | False Positive Tuning |
| 1      | S:807748, I:907595    | TCP SYN Port Sweep | 192.168.10.100   | 4192                  | TCP      | Jun 3, 2010 2:30:29 PM YEKST | ids_mks          |               |                 | False Positive Tuning |
| 1      | S:807750, I:907595    | TCP SYN Port Sweep | 192.168.10.100   | 4786                  | TCP      | Jun 3, 2010 2:30:59 PM YEKST | ids_mks          |               |                 | False Positive Tuning |
| 1      | S:807743, I:907595    | TCP SYN Port Sweep | 192.168.10.100   | 3837                  | TCP      | Jun 3, 2010 2:29:59 PM YEKST | ids_mks          |               |                 | False Positive Tuning |
| 1      | S:807745, I:907595    | TCP SYN Port Sweep | 192.168.10.100   | 4087                  | TCP      | Jun 3, 2010 2:29:59 PM YEKST | ids_mks          |               |                 | False Positive Tuning |
| 1      | S:807751, I:907595    | TCP SYN Port Sweep | 192.168.10.100   | 4553                  | TCP      | Jun 3, 2010 2:30:59 PM YEKST | ids_mks          |               |                 | False Positive Tuning |
| 1      | S:807748, I:907595    | TCP SYN Port Sweep | 192.168.10.100   | 4324                  | TCP      | Jun 3, 2010 2:30:29 PM YEKST | ids_mks          |               |                 | False Positive Tuning |

Copyright © 2003-2009 Cisco Systems, Inc. All rights reserved.

Summary :: Incidents :: Query / Reports :: Rules :: Management :: Admin :: Help

Рис. 5.19. Детализированное описание инцидента

## **Обнаружение компьютерных атак на узлы сети с использованием COA Cisco Security Agent и Cisco MARS**

### ***Назначение COA Cisco Security Agent***

Cisco Security Agent (CSA) – это система предотвращения атак на уровне узла (HIPS), предназначенная для серверных систем и настольных компьютеров в ОС Windows, Solaris и Linux. CSA состоит из двух основных частей: центра управления (Management Center) и агентов (Agents). CSA использует агентов для применения настроенных на центральном сервере политик информационной безопасности.

Агент, внедренный в ОС, выполняет множество ролей, предотвращая как известные, так и неизвестные атаки, включая следующие функции: защиту от вредоносных программ (путем контроля приложений, целостности файлов и каталогов, доступа к сети и т. п.), защиту информации от утечки (через USB-порты, DVD-RW, внешние устройства, сеть, буфер обмена).

Центр управления – Management Center (MC) – выполняет настройку агентов и политик, централизованный сбор отчетов. Для его работы требуется ОС Windows Server. В качестве базы данных используется Microsoft SQL. Все функции по управлению агентами осуществляется через консоль управления, которая является частью Cisco Works VPN Management Solution (VMS) и выглядит также, как и другие утилиты управления от фирмы Cisco. Конфигурация выполняется через Web-браузер по защищенному протоколу SSL.

Также важными составными компонентами Management Center являются просмотр событий и создание отчетов.

Как только агент обнаруживает нарушение политики безопасности, он сразу же посылает сообщение консоли управления для централизованного просмотра событий и создания отчетов. В определенные интервалы времени агент запрашивает центр управления об изменениях политики безопасности.

### ***Структура лабораторного стенда***

Для изучения средств обнаружения атак, направленных на узлы, рассмотрим некоторую сеть, в которой установлен подлежащий защите сервер на базе ОС Windows 2003 Server. На данный сервер

установлен агент CSA. В сети также развернут MC и Cisco MARS для выявления комплексных компьютерных атак.

Для развертывания данной сети предложен виртуальный стенд, состоящий из трех виртуальных образов и двух виртуальных сетей VMware. Также задействуется и основная ОС (рис. 5.20).

Технологическая подсеть подключена к виртуальной сети VMnet1, управляющая – к сети VMnet2. Основная ОС имеет два виртуальных сетевых интерфейса (IP-адреса 192.168.10.100 и 10.0.0.100).

Для выполнения работы понадобится следующее ПО:

- виртуальный образ комплекса Cisco MARS (версия 6.0.3);
- виртуальный образ ОС Windows 2003 Server с установленными MC CSA и агентом, который устанавливается автоматически при установке MC CSA.

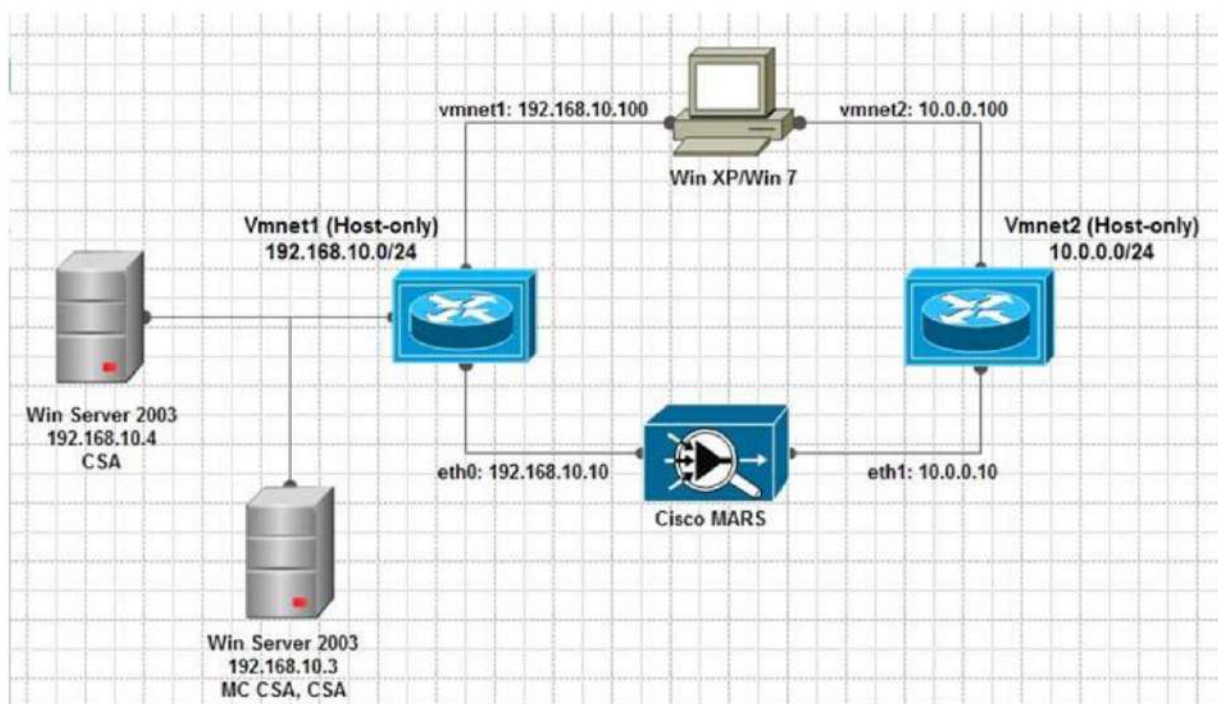


Рис. 5.20. Структура имитируемой сети

В составе стенда присутствуют следующие образы операционных систем:

- образ ОС Windows 2003 Server с установленным MC CSA с одним сетевым интерфейсом, подключенным к подсети VMnet1 192.168.10.0/24 (IP-адрес 192.168.10.3);
- образ ОС Windows 2003 Server с установленным агентом CSA с одним сетевым интерфейсом, подключенным к подсети VMnet1 192.168.10.0/24 (IP-адрес 192.168.10.4);

**Список литературы, рекомендуемый к использованию по данной теме.**

*Основная:* 1,2

*Дополнительная:* 1, 2,3

*Интернет-ресурсы:* 1, 2, 3, 4

**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ  
ФЕДЕРАЦИИ  
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ  
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ  
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»**

**МЕТОДИЧЕСКИЕ УКАЗАНИЯ**

для обучающихся по организации и проведению самостоятельной работы  
по дисциплине «Проектирование элементов защищенных телекоммуникационных  
систем» для студентов направления подготовки  
10.03.01 Информационная безопасность  
направленность (профиль) «Организация и технологии защиты информации (по отрасли  
или в сфере профессиональной деятельности)»

Ставрополь,  
2026

## **СОДЕРЖАНИЕ**

1. Общая характеристика самостоятельной работы студента
2. Технологическая карта самостоятельной работы студента
3. Самостоятельное изучение тем лекций
4. Паспорт фонда оценочных средств для проверки самостоятельной работы
5. Список рекомендуемой литературы

## **ВВЕДЕНИЕ**

Целью изучения дисциплины «Проектирование элементов защищенных телекоммуникационных систем» является изучение методов и средств построения и эксплуатации сетевых технологий для обеспечения информационной безопасности на объекте, а также изучение основных подходов к разработке, реализации, эксплуатации, анализу, сопровождению и совершенствованию технологий защиты передачи информации, а также приобретение профессиональных компетенций будущего бакалавра по направлению подготовки 10.03.01 Информационная безопасность.

Задачами дисциплины являются:

1. Обучение студентов систематизированным представлениям о принципах построения, функционирования и применения аппаратных средств современной вычислительной техники;
2. Изложение основных теоретических концепций, положенных в основу построения современных компьютеров, вычислительных систем, сетей и телекоммуникаций;
3. Подготовка к профессиональной деятельности по построению, проектированию и эксплуатации программно-аппаратных технологий защиты передачи информации..

### **1. Общая характеристика самостоятельной работы студента при изучении дисциплины**

Основными видами учебной работы по достижению результатов освоения дисциплины являются лекции, лабораторные работы и самостоятельная работа студентов (СРС).

На лекциях раскрываются основные положения и понятия курса, формируются знания в области способов и средств защиты телекоммуникационных систем. На лабораторных работах формируются умения и навыки, необходимые для решения задач профессиональной деятельности.

Приступая к изучению учебной дисциплины, необходимо ознакомиться с учебной программой, получить в библиотеке рекомендованные учебные пособия, а также получить у ведущего преподавателя в электронном виде конспекты лекций, методические рекомендации к лабораторным работам и тестовые, завести новую тетрадь для конспектирования лекций и выполнения лабораторных работ.

Для изучения дисциплины предлагается список основной и дополнительной литературы. Основная литература предназначена для обязательного изучения, дополнительная – поможет более глубоко освоить отдельные вопросы, подготовить исследовательские задания и выполнить задания для самостоятельной работы.

В ходе лекционных занятий студент обязан осуществлять конспектирование учебного материала, особое внимание, обращая на категории, формулировки, раскрывающие содержание тех или иных

понятий, физических явлений, процессов, эффектов. В рабочих конспектах желательно оставлять поля, на которых следует делать пометки из рекомендованной литературы, дополнять материал прослушанной лекции, формулировать научные выводы и практические рекомендации. Студент имеет право задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

Самостоятельная работа студентов над материалом учебной дисциплины является неотъемлемой частью учебного процесса и должна предполагать углубление знания учебного материала, излагаемого на аудиторных занятиях, и приобретение дополнительных знаний по отдельным вопросам самостоятельно.

Основными видами самостоятельной работы курсантов по учебной дисциплине являются:

- самостоятельное изучение учебного материала по заданным темам;
- подготовка к лабораторным работам и подготовка к собеседованию по результатам работы.

Основными методами самостоятельной работы студентов являются:

1) для овладения знаниями:

- чтение текста (конспекта лекций, учебника, дополнительной литературы) и конспектирование текста;
- работа с нормативными документами;
- поиск информации в Интернет;

2) для закрепления и систематизации знаний:

- работа с конспектом лекции (обработка текста);
- повторная работа над учебным материалом (учебника, дополнительной литературы, слайдами);
- составление плана и тезисов ответа или графическое изображение структуры ответа;
- составление таблиц для систематизации учебного материала;
- изучение нормативных документов;
- ответы на контрольные вопросы;

3) для формирования умений:

- подготовка к лабораторным занятиям;
- решение задач и лабораторным заданием;
- подготовка отчетов по лабораторным занятиям;
- рефлексивный анализ профессиональных умений.

В случае пропуска учебного занятия студент может воспользоваться содержанием различных блоков учебно-методического комплекса (лекции, лабораторные занятия, контрольные вопросы и тесты) для самоподготовки и освоения темы. Для самоконтроля необходимо использовать вопросы и задания, предлагаемые к лабораторным занятиям, а также варианты тестовых заданий.

## 2. Технологическая карта самостоятельной работы студента

| Коды реализуемых компетенций, индикатора(ов) | Вид деятельности студентов                            | Средства и технологии оценки  | Объем часов, в том числе |                                    |       |
|----------------------------------------------|-------------------------------------------------------|-------------------------------|--------------------------|------------------------------------|-------|
|                                              |                                                       |                               | СРС                      | Контактная работа с преподавателем | Всего |
| 7 семестр                                    |                                                       |                               |                          |                                    |       |
| ПК-5 ИД-2                                    | Подготовка к лабораторной работе                      | Собеседование                 | 8.00                     | 2.00                               | 10.00 |
| ПК-5 ИД-2                                    | Подготовка к лекции                                   | Конспект                      | 10.00                    | 2.00                               | 12.00 |
| ПК-5 ИД-2                                    | Подготовка доклада                                    | Доклад                        | 8.00                     | 2.00                               | 10.00 |
| ПК-5 ИД-2                                    | Самостоятельное изучение литературы                   | Конспект                      | 10.00                    | 2.00                               | 12.00 |
| ПК-5 ИД-2                                    | Самостоятельное выполнение заданий по заданным темам. | Конспект.<br>Письменный отчет | 8.00                     | 2.00                               | 10.00 |
| Итого за 7 семестр                           |                                                       |                               | 44.00                    | 10.00                              | 54.00 |
| Итого                                        |                                                       |                               | 44.00                    | 10.00                              | 54.00 |

## 3. Порядок выполнения самостоятельной работы

### 3.1 Методические рекомендации по изучению теоретического материала

Комплексное изучение предлагаемой студентам учебной дисциплины «Проектирование элементов защищенных телекоммуникационных систем» предполагает овладение материалами лекций, учебников, программы, творческую работу студентов в ходе проведения лабораторных работ, а также систематическое выполнение заданий для самостоятельной работы.

В ходе лекций раскрываются основные вопросы в рамках рассматриваемых тем, делаются акценты на наиболее сложные и интересные положения изучаемого материала, которые должны быть приняты студентами во внимание. Материалы лекций являются основой для подготовки студентов к лабораторным работам.

#### **Работа с конспектом лекций**

Просмотрите конспект сразу после занятий. Отметьте материал конспекта лекций, который вызывает затруднения для понимания. Попытайтесь найти ответы на затруднительные вопросы, используя предлагаемую литературу. Если самостоятельно не удалось разобраться в материале, сформулируйте вопросы и обратитесь на текущей консультации или на ближайшей лекции за помощью к преподавателю.

Каждую неделю отводите время для повторения пройденного материала, проверяя свои знания, умения и навыки по контрольным вопросам и тестам.

## ***Выполнение лабораторных работ по дисциплине «Проектирование элементов защищенных телекоммуникационных систем»***

На первом занятии получите у преподавателя задания по курсу, планы подготовки к лабораторным работам. Обзаведитесь всем необходимым методическим обеспечением.

Перед лабораторными работами изучите теорию вопроса, предполагаемого к исследованию, ознакомьтесь с опытом других исследователей в этом направлении.

Целью лабораторных работ является:

- закрепление методов приложения теории к решению лабораторных задач анализа и синтеза психологического знания;
- проверка уровня понимания студентами вопросов, рассмотренных на лекциях и по учебной литературе, степени и качества усвоения материала;
- обучение навыкам освоения методики эксперимента и работы с нормативно-справочной литературой;
- восполнение пробелов в пройденной теоретической части курса и оказание помощи в его усвоении.

### *3.2 Методические рекомендации по написанию и оформлению доклада*

#### 1. Общие положения

1.1. Доклад, как вид самостоятельной работы в учебном процессе, способствует формированию навыков исследовательской работы, расширяет познавательные интересы, учит критически мыслить.

1.2. При написании доклада по заданной теме студент составляет план, подбирает основные источники.

1.3. В процессе работы с источниками систематизирует полученные сведения, делает выводы и обобщения.

1.4. К докладу по крупной теме могут привлекать несколько студентов, между которыми распределяются вопросы выступления.

#### 2. Выбор темы доклада

2.1. Тематика доклада обычно определяется преподавателем, но в определении темы инициативу может проявить и студент.

2.2. Прежде чем выбрать тему доклада, автору необходимо выявить свой интерес, определить, над какой проблемой он хотел бы поработать, более глубоко ее изучить.

#### 3. Этапы работы над докладом

3.1. Формулирование темы, причем она должна быть не только актуальной по своему значению, но и оригинальной, интересной по содержанию.

3.2. Подбор и изучение основных источников по теме (как правильно, при разработке доклада используется не менее 8-10 различных

источников).

3.3. Составление списка использованных источников.

3.4. Обработка и систематизация информации

3.5. Разработка плана доклада.

3.6. Написание доклада.

3.7. Публичное выступление с результатами исследования.

4. Структура доклада:

- титульный лист

- оглавление (в нем последовательно излагаются названия пунктов доклада, указываются страницы, с которых начинается каждый пункт);

- введение (формулирует суть исследуемой проблемы, обосновывается выбор темы, определяются ее значимость и актуальность, указываются цель и задачи доклада, дается характеристика используемой литературы);

- основная часть (каждый раздел ее, доказательно раскрывая отдельную проблему или одну из ее сторон, логически является продолжением предыдущего; в основной части могут быть представлены таблицы, графики, схемы);

- заключение (подводятся итоги или дается обобщенный вывод по теме доклада, предлагаются рекомендации);

- список использованных источников

5. Структура и содержание доклада

5.1. Введение - это вступительная часть научно-исследовательской работы. Автор должен приложить все усилия, чтобы в этом небольшом по объему разделе показать актуальность темы, раскрыть практическую значимость ее, определить цели и задачи эксперимента или его фрагмента.

5.2. Основная часть. В ней раскрывается содержание доклада. Как правило, основная часть состоит из теоретического и практического разделов. В теоретическом разделе раскрываются история и теория исследуемой проблемы, дается критический анализ литературы и показывается позиция автора. В практическом разделе излагаются методы, ход, и результаты самостоятельно проведенного эксперимента или фрагмента.

В основной части могут быть также представлены схемы, диаграммы, таблицы, рисунки и т.д.

5.3. В заключении содержатся итоги работы, выводы, к которым пришел автор, и рекомендации. Заключение должно быть кратким, обязательным и соответствовать поставленным задачам.

5.4. Список использованных источников представляет собой перечень использованных книг, статей, фамилии авторов приводятся в алфавитном порядке, при этом все источники даются под общей нумерацией литературы. В исходных данных источника указываются фамилия и инициалы автора, название работы, место и год издания.

5.5. Приложение к докладу оформляются на отдельных листах,

причем каждое должно иметь свой тематический заголовок и номер, который пишется в правом верхнем углу, например: «Приложение 1»

#### 6. Требования к оформлению доклада

6.1. Объем доклада может колебаться в пределах 5-15 печатных страниц; все приложения к работе не входят в ее объем.

6.2. Доклад должен быть выполнен грамотно, с соблюдением культуры изложения.

6.3. Обязательно должны иметься ссылки на используемую литературу.

6.4. Должна быть соблюдена последовательность написания библиографического аппарата.

#### 7. Критерии оценки доклада

- актуальность темы исследования;
- соответствие содержания теме;
- глубина проработки материала; правильность и полнота использования источников;
- соответствие оформления доклада стандартам.

По усмотрению преподавателя доклады могут быть представлены на семинарах, научно-практических конференциях, а также использоваться как зачетные работы по пройденным темам.

### *3.3 Методические рекомендации по конспектированию первоисточников*

Изучение и анализ литературных источников является обязательным видом самостоятельной работы студентов. Изучение литературы по избранной теме имеет своей задачей проследить характер постановки и решения определенной проблемы различными авторами, аргументацию их выводов и обобщений, провести анализ и систематизировать полученный материал на основе собственного осмысления с целью выяснения современного состояния вопроса.

Проработка отобранного материала обязательно должна идти с одновременным ведением записей прочитанного и своих замечаний. Запись может иметь как форму конспекта, так и выписок, а также картотеку положений, тезисов, идей, методик, что в дальнейшем облегчит классификацию и систематизацию полученного материала. Такого рода записи являются лучшим способом накопления и первичной обработки материал, одной из обязательных форм организации умственного труда.

**Планом** удобно пользоваться при подготовке к устному выступлению по выбранной теме. Каждый пункт плана должен раскрывать одну из сторон избранной темы, а весь план должен охватывать ее целиком.

**Тезисы** предполагают сжатое изложение основных положений текста в форме утверждения или отрицания. Они являются более совершенной формой записей и представляют основу для дискуссии. К тому же их легко запомнить.

**Конспектирование** – процесс мысленной переработки и письменной фиксации информации, в виде краткого изложения основного содержания, смысла какого-либо текста.

Результат конспектирования – запись, позволяющая конспектирующему немедленно или через некоторый срок с нужной полнотой восстановить полученную информацию. Конспект в переводе с латыни означает «обзор». По существу его и составлять надо как обзор, содержащий основные мысли текста без подробностей и второстепенных деталей. Конспект носит индивидуализированный характер: он рассчитан на самого автора и поэтому может оказаться малопонятным для других.

Для того чтобы осуществлять этот вид работы, в каждом конкретном случае необходимо грамотно решить следующие задачи:

1. Сориентироваться в общей композиции текста (уметь определить вступление, основную часть, заключение).
2. Увидеть логико-смысловую канву сообщения, понять систему изложения автором информации в целом, а также ход развития каждой отдельной мысли.
3. Выявить «ключевые» мысли, т. е. основные смысловые вехи, на которые «нанизано» все содержание текста.
4. Определить детализирующую информацию.
5. Лаконично сформулировать основную информацию, не перенося на письмо все целиком и дословно.

Во всяком научном тексте содержится информация 2-х видов: основная и вспомогательная. Основной является информация, имеющая наиболее существенное значение для раскрытия содержания темы или вопроса. К ней относятся: определения научных понятий, формулировки законов, теоретических принципов и т. д. Назначение вспомогательной информации – помочь читателю лучше усвоить предлагаемый материал. К этому типу информации относятся разного рода комментарии. Основную – записываем как можно полнее, вспомогательную, как правило, опускаем. Содержание конспектирования составляет переработка основной информации в целях ее обобщения и сокращения. Обобщить – значит представить ее в более общей, схематической форме, в виде тезисов, выводов, отдельных заголовков, изложения основных результатов и т. п. Читая, мы интуитивно используем некоторые слова и фразы в качестве опорных. Такие опорные слова и фразы называются ключевыми. Ключевые слова и фразы несут основную смысловую и эмоциональную нагрузку содержания текста.

Выбор ключевых слов – это первый этап смыслового свертывания, смыслового сжатия материала.

Важными требованиями к конспекту являются наглядность и обозримость записей и такое их расположение, которое давало бы возможность уяснить логические связи и иерархию понятий.

**По форме конспекты подразделяются на формализованные и**

**графические.**

**1. Формализованные** (все записи вносятся в заранее подготовленные таблицы).

Это удобно, во-первых, при конспектировании материалов, когда перечень характеристик описываемых предметов или явлений более или менее постоянен, во-вторых, при подготовке единого конспекта по нескольким источникам. Особенно если есть необходимость сравнения отдельных данных. Разновидностью формализованного конспекта является запись, составленная в форме ответов на заранее подготовленные вопросы, обеспечивающие исчерпывающие характеристики однотипных предметов или явлений.

**2. Графические** (элементы конспектируемой работы располагаются в таком виде, при котором видна иерархия понятий и взаимосвязь между ними).

По каждой работе может быть не один, а несколько графических конспектов, отображающих книгу в целом и отдельные ее части. Ведение графического конспекта - наиболее совершенный способ изображения внутренней структуры книги, а сам этот процесс помогает усвоению ее содержания.

Можно выделить следующие основные **типы конспектов: плановый, текстуальный, сводный, тематический.**

**Плановый** – легко получить с помощью предварительно сделанного плана произведения, каждому вопросу плана отвечает определенная часть конспекта:

а) вопросно-ответный (на пункты плана, выраженные в вопросительной форме, конспект дает точные ответы);

б) схематичный плановый конспект (отражает логическую структуру и взаимосвязь отдельных положений).

**Текстуальный** – это конспект, созданный в основном из цитат.

**Сводный конспект** – сочетает выписки, цитаты, иногда тезисы; часть его текста может быть снабжена планом.

**Тематический** – дает более или менее исчерпывающий ответ (в зависимости из числа привлеченных источников и другого материала, например, своих же записей) на поставленный вопрос – тему: обзорный; хронологический.

Роль конспекта – чисто учебная: он помогает зафиксировать основные понятия и положения первичного текста и в нужный момент их воспроизвести, например, при написании реферата или подготовке к экзамену.

**Способы конспектирования.**

- **Тезисы** – это кратко сформулированные основные мысли, положения изучаемого материала. Тезисы лаконично выражают суть читаемого, дают возможность раскрыть содержание. Приступая к освоению записи в виде тезисов, полезно в самом тексте отмечать места, наиболее четко

формулирующие основную мысль, которую автор доказывает (если, конечно, это не библиотечная книга). Часто такой отбор облегчается шрифтовым выделением, сделанным в самом тексте.

- **Линейно-последовательная запись текста.** При конспектировании линейно – последовательным способом целесообразно использование плакатно-оформительских средств, которые включают в себя следующие:

- сдвиг текста конспекта по горизонтали, по вертикали;
- выделение жирным (или другим) шрифтом особо значимых слов;
- использование различных цветов;
- подчеркивание;
- заключение в рамку главной информации.

- **Способ «вопросов – ответов».** Он заключается в том, что, поделив страницу тетради пополам вертикальной чертой, конспектирующий в левой части страницы самостоятельно формулирует вопросы или проблемы, затронутые в данном тексте, а в правой части дает ответы на них.

Одна из модификаций способа «вопросов – ответов» - таблица, где место вопроса занимает формулировка проблемы, поднятой автором (лектором), а место ответа – решение данной проблемы. Иногда в таблице могут появиться и дополнительные графы: например, «мое мнение» и т. п.

- **Схема с фрагментами** – способ конспектирования, позволяющий ярче выявить структуру текста, - при этом фрагменты текста (опорные слова, словосочетания, пояснения всякого рода) в сочетании с графикой помогают созданию рационально - лаконичного конспекта.

- **Простая схема** – способ конспектирования, близкий к схеме с фрагментами, объяснений к которой конспектирующий не пишет, но должен уметь давать их устно. Этот способ требует высокой квалификации конспектирующего. В противном случае такой конспект нельзя будет использовать.

- **Параллельный способ** конспектирования. Конспект оформляется на двух листах параллельно или один лист делится вертикальной чертой пополам и записи делаются в правой и в левой части листа.

**Однако** лучше использовать разные способы конспектирования для записи одного и того же материала.

**Комбинированный конспект** – вершина овладения рациональным конспектированием. При этом умело используются все перечисленные способы, сочетая их в одном конспекте (один из видов конспекта свободно перетекает в другой в зависимости от конспектируемого текста, от желания и умения конспектирующего). Именно при комбинированном конспекте более всего проявляется уровень подготовки и индивидуальность студента.

Принципы составления конспекта прочитанного.

1. Записать все выходные данные источника: автор, название, год и место издания. Если текст взят из периодического издания (газеты или журнала), то записать его название, год, месяц, номер, число, место издания.

2. Выделить поля слева или справа, можно с обеих сторон. Слева на

полях отмечаются страницы оригинала, структурные разделы статьи или книги (названия параграфов, подзаголовки и т. п.), формулируются основные проблемы. Справа – способы фиксации прочитанной информации.

Один из видов чтения – углубленное – предполагает глубокое усвоение прочитанного и часто сохранение информации в целях последующего обращения к ней. Эффективность такого чтения повышается, если прочитанное зафиксировано не только в памяти, но и на бумаге. Психологи утверждают, что записанное лучше и полнее усваивается, прочнее откладывается в памяти. Установлено, что если прочитать 1000 слов и затем записать 50, подытоживающих прочитанное, то коэффициент усвоения будет выше, чем, если прочитать 10000 слов, не записав ни одного. Кроме того, при записи прочитанного формируется навык свертывания информации. И, наконец, чередование чтения и записывания уменьшает усталость, повышает работоспособность и производительность умственного труда.

#### 1. Резюмирование.

Резюме – краткий итог прочитанного, содержащий его оценку. Резюме характеризует основные выводы книги, главные итоги.

Выбор языковых средств для построения резюме-выводов подчинен основной задаче свертывания информации: минимум языковых средств – максимум информации. Это обычно одно – три четких, кратких, выразительных предложения, раскрывающих, по мнению автора, самую суть описываемого объекта.

#### 2. Аннотация.

Аннотация – краткая обобщенная характеристика печатной работы (книги, статьи), включающая иногда и его оценку. Это наискратчайшее изложение содержания первичного документа, дающее общее представление о теме.

Основное ее назначение – дать некоторое представление о книге (статье, научной работе) с тем, чтобы рекомендовать ее определенному кругу читателей или воспользоваться своими записями при выполнении работы исследовательского, реферативного характера. Поэтому аннотации не требуется изложения содержания произведения, в ней лишь перечисляются вопросы, которые освещены в первоисточнике (содержание этих вопросов не раскрывается). Аннотация отвечает на вопрос: «О чем говорится в первичном тексте?», дает представление только о главной теме и перечне вопросов, затрагиваемых в тексте первоисточника.

Текст аннотации не стандартизирован. В научной литературе можно встретить различные требования к составлению аннотаций. Например, текст справочной аннотации может включать следующие сведения:

- тип и название аннотируемого документа (монография, диссертация, сборник, статья и т. п.)
- задачи, поставленные автором аннотируемого документа

- метод, которым пользовался автор (эксперимент, сравнительный анализ, компиляция других источников)
- принадлежность автора к определенной научной школе или направлению
- структуру аннотируемого документа
- предмет и тему произведения, основные положения и выводы автора
- характеристику вспомогательных иллюстративных материалов, дополнений, приложений, справочного аппарата, включая указатели и библиографию.

#### **4.1 Вопросы для собеседования по лабораторным работам**

##### **Лабораторная работа 1. Основы конфигурирования в командной строке IOS.**

###### ***Базовый уровень:***

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?

###### ***Повышенный уровень:***

3. Каково назначение конфигурационных файлов сетевых устройств фирмы Cisco?
4. Для чего используется команда Setup?

##### **Лабораторная работа 2. Конфигурирование сетевых устройств фирмы Cisco.**

###### ***Базовый уровень:***

5. Какие VLAN существуют по умолчанию в коммутаторе и к каким из них принадлежат его интерфейсы?
6. Можно ли в сети с несколькими коммутаторами при конфигурировании VLAN обойтись без использования стандарта IEEE802.1Q?
7. Каково назначение функции Port Security?
8. В чем преимущество каналов EtherChannel?
9. Для чего необходим протокол STP?
10. Может ли администратор каким-либо образом повлиять на расчет покрывающего дерева в сети?
11. Для чего и каким образом конфигурируются статические маршруты?
12. В каких случаях целесообразно использовать маршруты по умолчанию?

13. Каково назначение протокола CDP, в чем преимущества и недостатки его использования в сети?

14. Каковы основные возможности протокола управления сетью SNMP?

***Повышенный уровень:***

15. На основе каких протоколов можно получить удаленный доступ к командной строке IOS устройства, в чем преимущества и недостатки каждого из них?

16. Для какого количества сетей DHCP-сервер на маршрутизаторе может выдавать конфигурационные параметры клиентам?

17. В каких случаях на маршрутизаторах необходимо конфигурировать промежуточные агенты при использовании серверов DHCP?

**Лабораторная работа 3. Межсетевое экранирование с использованием технологий фирмы Cisco**

***Базовый уровень:***

18. В чем состоит ограничение при использовании стандартных списков доступа?

19. Какие сетевые протоколы поддерживаются при создании правил расширенных списков доступа?

20. В чем состоит преимущество использования динамических обратных списков доступа перед другими?

***Повышенный уровень:***

21. Объяснить понятие уровня безопасности интерфейса Cisco PIX Firewall.

22. Назвать виды NAT и дать им краткую характеристику.

23. Назвать преимущества использования технологии NAT при подключении к открытым сетям.

24. Какова роль протокола IKE при организации IPSec-туннеля?

**Лабораторная работа 4. Обнаружение сетевых компьютерных атак**

***Базовый уровень:***

25. Какие задачи решаются с помощью COA?

26. Для чего предназначен компонент COA – сенсорная подсистема?

27. Какую функцию выполняют интегрированные в сенсор технологии Cisco Threat Response, Threat Risk Rating и Meta Event Generator?

***Повышенный уровень:***

28. Перечислите элементы сети, где согласно рекомендациям производителя следует размещать сенсор.

29. Опишите структуру сигнатуры.
30. Назовите существующие в сенсоре классы сигнатур.

## **Лабораторная работа 5. Обнаружение комплексных компьютерных атак**

### ***Базовый уровень:***

31. Перечислите основные задачи, решаемые с помощью Cisco MARS?
32. Что может выступать в качестве источников данных Cisco MARS?
33. Назовите примеры отчетов, создаваемых Cisco MARS.

### ***Повышенный уровень:***

34. Каким образом осуществляется просмотр событий, зафиксированных Cisco MARS?
35. Какие функции выполняет Cisco Security Agent?
36. Для чего предназначен MC CSA?

## **4.2. Вопросы для собеседования по самостоятельному изучению программного продукта Cisco Packet Tracer**

### ***Базовый уровень:***

- 1) Какая плата расширения обеспечивает функционал встроенной точки доступа?
- 2) Какая плата расширения предоставляет однопортовое последовательное подключение к удаленным офисам или устаревшим серийным сетевым устройствам?
- 3) Как называется высокопроизводительный модуль с 4-мя коммутационными портами Ethernet под разъем RJ-45?
- 4) Перечислите сетевые карты, позволяющие подключаться к WAN сетям?
- 5) Какой тип интерфейса следует выбрать при создании кластера?
- 6) Назовите модели коммутаторов третьего уровня?
- 7) Какой тип кабеля следует использовать при соединении роутеров между собой?
- 8) Укажите серии магистральных маршрутизаторов.
- 9) В каких случаях используется интерфейс SERIAL?
- 10) Как организовать связь двух магистральных маршрутизаторов?
- 11) Перечислите все возможные режимы работы программы Cisco Paket Tracer?
- 12) Назовите модели коммутаторов второго уровня?
- 13) Перечислите все типы связей, используемых в Cisco Paket Tracer и укажите их назначение

## **4.3. Вопросы для собеседования по самостоятельному изучению тем**

## **дисциплины**

### **Базовый уровень:**

- 1) Для чего создаются виртуальные локальные сети? Их достоинства?
- 2) Как связываются между собой VLAN и порты коммутатора?
- 3) Как обеспечивается общение между узлами разных виртуальных сетей?
- 4) Как обеспечивается управление виртуальными локальными сетями?

### **Перечень литературы необходимый для освоения дисциплины**

#### **Основная литература:**

Голиков, А. М. Основы проектирования защищенных телекоммуникационных систем : учебное пособие для специалитета: 10.05.02 Информационная безопасность телекоммуникационных систем. Курс лекций, компьютерный практикум, компьютерные лабораторные работы и задание на самостоятельную работу / А. М. Голиков. — Томск : Томский государственный университет систем управления и радиоэлектроники, 2016. — 396 с. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/72158.html>

Пятибратов, А. П. Вычислительные машины, сети и телекоммуникационные системы : учебное пособие / А. П. Пятибратов, Л. П. Гудыно, А. А. Кириченко. — Москва : Евразийский открытый институт, 2009. — 292 с. — ISBN 978-5-374-00108-2. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/10644.html>

#### **Дополнительная литература:**

Никифоров, С.Н. Защита информации. Защита от внешних вторжений Электронный ресурс : учебное пособие / С.Н. Никифоров. - Санкт-Петербург : Санкт-Петербургский государственный архитектурно-строительный университет, ЭБС АСВ, 2017. - 84 с. - Книга находится в базовой версии ЭБС IPRbooks. - ISBN 978-5-9227-0757-2

Олифер, В. Г. Компьютерные сети : принципы, технологии, протоколы : учеб. пособие для вузов / В. Г. Олифер, Н. А. Олифер. - 4-е изд. - СПб. [и др.] : Питер, 2014. - 944 с. : ил. - (Учебник для вузов). - Гриф: Рек. МО. -

Библиогр.: с. 917. - Алф. указ.: с. 918-943. - ISBN 978-5-469-00004-8

Тарасюк, М. В. Защищенные информационные технологии : Проектирование и применение / М. В. Тарасюк. - М. : СОЛОН-Пресс, 2004. - 192 с. : ил. - (Аспекты защиты). - Библиогр.: с. 180-181. - Глоссарий: с. 182-186. - ISBN 5-98003-143-X

**Интернет-ресурсы:**

Cisco.com – Официальный сайт компании Cisco Systems: сайт. – URL: [http:// cisco.com](http://cisco.com)

WikiSec.ru – энциклопедия информационной безопасности: сайт. – URL: [http:// wikisec.ru](http://wikisec.ru)

Информационный портал по безопасности SecurityLab.ru, новости, статьи, обзор уязвимостей, вирусов и мнения аналитиков: сайт. – URL: <http://securitylab.ru>

[www.biblioclub.ru](http://www.biblioclub.ru) - Электронная библиотечная система «Университетская библиотека онлайн»

[www.eLibrary.ru](http://www.eLibrary.ru) - Научная электронная библиотека

[www.iprbookshop.ru](http://www.iprbookshop.ru) - Электронно-библиотечная система IPRbooks